PRZEGLĄD KONSTYTUCYJNY, 2/2023, s. 75–111
https://doi.org/10.4467/25442031PKO.23.011.18277
www.ejournals.eu/Przeglad-Konstytucyjny

MARCIN ROJSZCZAK

Konstytucjonalizacja prawa do ochrony danych osobowych – proces trwający czy zakończony?

1. Wstęp

W 2022 r. obchodzona była 25. rocznica uchwalenia oraz wejścia w życie Konstytucji RP[1]. Z jednej strony ćwierć wieku w historii państw i narodów to okres bardzo krótki, niepozwalający w pełni ocenić skutków zachodzących procesów społeczno-gospodarczych, a przez to i wyrokować, czy wprowadzone rozwiązania ustrojowe w sposób trwały zabezpieczyły prawidłowy rozwój struktur państwa. Z drugiej jednak 25 lat to okres wystarczający, aby dokonać oceny skuteczności ustanowienia niektórych, zwłaszcza nowych instytucji prawnych.

Przyjęcie w 1997 r. ustawy zasadniczej stanowiło zakończenie istotnego etapu transformacji ustrojowej. Nowy akt konstytucyjny przyczynił się do wzmocnienia demokratycznego państwa prawa, ale również miał fundamentalne znaczenie dla budowy społeczeństwa obywatelskiego.

Polska Konstytucja – czego niestety dzisiaj często nie doceniamy – to również akt nowoczesny, a przez to odpowiadający na wyzwania współczesności.

[1] Niniejszy artykuł stanowi rozszerzoną wersję referatu, przedstawionego podczas seminarium naukowego pt. „Konstytucja wobec wyzwań nowych technologii", zorganizowanego 13 stycznia 2023 r. na Wydziale Administracji i Nauk Społecznych Politechniki Warszawskiej. Autor serdecznie dziękuje organizatorowi wydarzenia dr. Radosławowi Puchcie, a także wszystkim uczestnikom za zgłoszenie cennych uwag, które wpłynęły na finalny kształt artykułu.

Przykładem są przepisy ustanawiające szczególne prawa jednostki dotyczące ochrony informacji jej dotyczących – niemające odpowiednika we wcześniejszych krajowych przepisach konstytucyjnych, ale również w ustawach zasadniczych wielu innych państw europejskich. Regulacje te – ustanawiające nowe publiczne prawo podmiotowe – są dzisiaj niemal powszechnie określane terminem „prawo do ochrony danych osobowych". Jednak w 1997 r. ochrona danych osobowych była obszarem dopiero rozpoznawanym przez prawodawców. Dość powiedzieć, że zaledwie dwa lata wcześniej prawodawca unijny (wspólnotowy) zdecydował o przyjęciu pierwszej regulacji dotyczącej tego obszaru – dyrektywy 95/46/WE[2] – która przez ponad 20 lat jej obowiązywania ukształtowała i niemal „zmonopolizowała" myślenie o konstrukcji i treści prawa do ochrony danych w europejskim modelu prawnym[3].

W trzeciej dekadzie XXI w. ochrona danych osobowych jest jednym z centralnych zagadnień wpływających na rozwój nowoczesnych usług cyfrowych. Unijne prawo stanowione w tym zakresie jest uznawane za najbardziej kompleksowe oraz nowoczesne, stanowiące przykład dla innych prawodawców, jak zapewnić skuteczną ochronę praw podstawowych przed zagrożeniami związanymi z rozwojem globalnego rynku danych[4].

Wraz z wejściem w życie rozporządzenia 2016/679 (RODO)[5] zakończony został – zapoczątkowany Traktatem z Lizbony[6] – proces reformy unijnego modelu ochrony danych. Zastąpienie dyrektywy 95/46/WE stosowanym wprost rozporządzeniem stanowiło także silny impuls dla opracowania nowej generacji przepisów regulujących funkcjonowanie rynku cyfrowego.

Zatem gdy Konstytucja RP była przyjmowana, ochrona danych osobowych w prawie UE nie miała statusu prawa podstawowego, a regulacje jej dotyczące były stanowione na podstawie kompetencji dotyczących współpracy

2 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. UE L 281 z 23.11.1995, s. 31, ze zm.

3 Chociaż oczywiście należy pamiętać, że historycznie pierwszym ponadnarodowym aktem ustanawiającym zasady dotyczące ochrony danych osobowych była Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28 stycznia 1981 r., Dz.U. z 2003 r. Nr 3, poz. 25.

4 Zob. np. J.P. Albrecht, *How the GDPR...*; G. Greenleaf, *The influence...*; M.L. Rustad, T.H. Koenig, *Towards...*

5 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE L 119 z 4.05.2016, s. 1, ze zm.

6 Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 grudnia 2007 r., Dz.Urz. UE C 306 z 17.12.2007, s. 1.

gospodarczej[7]. Dzisiaj – 25 lat później – to prawo UE, w szczególności Karta praw podstawowych (dalej: KPP) oraz bogate orzecznictwo Trybunału Sprawiedliwości, wyznacza standard ochrony danych osobowych obowiązujący w państwach członkowskich.

Wykładnia Trybunału Sprawiedliwości w wielu przypadkach nie tylko pomogła wyjaśnić praktyczne wątpliwości związane ze stosowaniem stosunkowo nowych regulacji dotyczących ochrony danych osobowych, ale wielokrotnie stanowiła również narzędzie kształtowania rynku cyfrowego. Taki skutek wywarły między innymi wyroki w sprawach *Google Spain*[8] (prawo do bycia zapomnianym), *Wirtschaftsakademie Schleswig-Holstein*[9] (przetwarzanie danych w mediach społecznościowych) czy *GC*[10] (terytorialny zakres stosowania unijnego prawa ochrony danych).

Jednocześnie krajowy sąd konstytucyjny – mimo dużej aktywności i bogactwa orzecznictwa wzmacniającego ochronę praw podstawowych – stosunkowo rzadko zajmował się rozstrzyganiem zawiłości kształtowanej dopiero co praktyki stosowania przepisów o ochronie danych. A gdy już to robił, wzorcem kontroli nie był samodzielnie stosowany art. 51 Konstytucji RP, ale raczej standard zrekonstruowany na podstawie kompleksu norm konstytucyjnych – obejmujący zazwyczaj także prawo do prywatności (art. 47 Konstytucji RP).

W efekcie w tym samym czasie, gdy Trybunał Sprawiedliwości, a także sądy konstytucyjne innych państw[11] prowadziły dialog wyjaśniający różne aspekty konstrukcyjne prawa ochrony danych, polskie orzecznictwo konstytucyjne niezmiennie postrzegało ochronę danych osobowych wyłącznie jako konkretyzację obowiązków związanych z poszanowaniem prywatności jednostki.

Skutkiem była – stosunkowo wąska – optyka definiowania strony przedmiotowej tego prawa, koncentrująca się na uwypuklaniu zagrożeń dla prywatności związanych z przetwarzaniem danych w systemach informatycznych.

[7] Formalną podstawą przyjęcia dyrektywy 95/46/WE był ówczesny art. 100a Traktatu ustanawiającego Wspólnotę Europejską (obecnie art. 114 Traktatu o Unii Europejskiej, dalej: TUE), a więc przepis kompetencyjny dotyczący harmonizacji rynku wewnętrznego.

[8] Wyrok TSUE z 13 maja 2014 r., C-131/12, *Google Spain SL i Google Inc.* przeciwko *Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi*, ECLI:EU:C:2014:317.

[9] Wyrok TSUE z 5 czerwca 2018 r., C-210/16, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* przeciwko *Wirtschaftsakademie Schleswig-Holstein GmbH*, ECLI:EU:C:2018:388.

[10] Wyrok TSUE z 24 września 2019 r., C-136/17, *GC i in.* przeciwko *Commission nationale de l'informatique et des libertés (CNIL)*, ECLI:EU:C:2019:773.

[11] Zob. np. C. Rauchegger, *National...*

Tak rozumiana ochrona danych osobowych była zatem redukowana do roli prawa akcesoryjnego względem ogólniejszego – prawa do prywatności.

Na tym tle uwagę zwraca akceptowany niemal powszechnie w dogmatyce prawa pogląd, że skutkiem wejścia w życie Konstytucji RP z 1997 r. była konstytucjonalizacja prawa do ochrony danych osobowych[12]. Jego zwolennicy, wyjaśniając elementy konstrukcyjne tak rozumianego prawa, chętnie korzystają przy tym z siatki pojęciowej wprowadzonej w prawie UE, jednocześnie obcej polskim przepisom konstytucyjnym. Ignorują tym samym, że pojęcia te (w tym także sam termin „dane osobowe") mają swoje legalne definicje, a ich bezkrytyczne odnoszenie do gwarancji konstytucyjnych musi co najmniej tworzyć niejasności interpretacyjne.

Autor niniejszego artykułu formułuje tezę, że Konstytucja RP z 1997 r. w istocie nie skutkowała konstytucjonalizacją prawa do ochrony danych osobowych – rozumianą jako wprowadzenie do systematyki praw podstawowych wynikających z ustawy zasadniczej samodzielnego prawa podmiotowego, konstrukcyjnie zbliżonego do prawa ustanowionego w unijnym modelu prawnym. Ustrojodawca ustanowił natomiast szczególne prawo jednostki do ochrony niektórych kategorii informacji jej dotyczących przed dostępem przez organy władzy publicznej. W tym zakresie (częściowo) zabezpieczył zatem autonomię informacyjną jednostki. Prawo to – chociaż *explicite* odnoszące się do pozyskiwania i przetwarzania niektórych kategorii informacji – jest jednak podmiotowo i przedmiotowe inne, niż prawo do ochrony danych osobowych w kształcie wynikającym z art. 8 KPP. Opiera się także na innej ochronie instytucjonalnej, ale przede wszystkim zostało zbudowane na innym *ratio legis*. Zamiarem ustrojodawcy nie było wprowadzenie nowego, samodzielnego prawa podmiotowego, lecz wyłącznie ustanowienie normy szczególnej, chroniącej jednostkę przed niektórymi rodzajami nadużyć wertykalnych dotyczących jej sfery życia prywatnego[13]. Dlatego chociaż na gruncie Karty praw podstawowych prawo do prywatności i prawo do ochrony danych osobowych mogą być rozpatrywane jako dwa odrębne i samodzielne prawa podmiotowe, to relacja taka nie występuje w ujęciu polskich

[12] Por. np. M. Sakowska-Baryła, *Konstytucjonalizacja...*, s. 127 oraz K. Łachowska, *Ochrona...*, s. 132. Rację ma Mariusz Polok, dostrzegając fragmentaryczność regulacji konstytucyjnej, co jednak tłumaczy celowym działaniem prawodawcy, który „ograniczył swoje działania legislacyjne jedynie do najważniejszych grup interesów" – M. Polok, *Bezpieczeństwo...*, s. 78.

[13] Szerzej na temat przebiegu prac dotyczących treści i redakcji art. 51 prowadzonych w ramach Komisji Konstytucyjnego Zgromadzenia Narodowego – M. Wild, w: *Konstytucja...*, komentarz do art. 51, nb 9–14.

przepisów konstytucyjnych, w których obie normy, realizując tożsamy cel, służą ochronie tej samej sfery – życia prywatnego jednostki.

Na skutek inkorporacji prawa UE do prawodawstwa państw członkowskich prawo do ochrony danych osobowych stało się częścią krajowego porządku prawnego. Ma ono swoją legalną definicję, zbudowaną na określonej siatce pojęciowej i związanej z nią bogatym orzecznictwem sądowym. Prawo to nie powinno być jednak utożsamiane z prawem zagwarantowanym w kompleksie norm wynikających z art. 51 Konstytucji RP.

W niniejszym artykule przedstawiono porównanie unijnego prawa do ochrony danych (którego źródłem jest art. 8 KPP) oraz krajowych gwarancji dotyczących autonomii informacyjnej jednostki (art. 51 Konstytucji RP). Takie komparatystyczne ujęcie problemu – w zamierzeniu autora – ma pozwolić nie tylko na zidentyfikowanie wielu błędnych, ale powtarzanych w piśmiennictwie, tez dotyczących zakresu stosowania art. 51 Konstytucji RP, ale również ustalenia, czy przywołany zespół norm konstytucyjnych może stanowić wzorzec kontroli do oceny dopuszczalności stosowania wielu nowoczesnych (i intruzywnych) form ingerencji w prawa podstawowe, także tych wykorzystywanych przez podmioty publiczne (np. analityka big data, masowe profilowanie użytkowników itp.). Przedstawione wnioski mogą okazać się pomocne w dyskusji na temat kierunków przyszłej ewolucji krajowych przepisów konstytucyjnych w obszarze ochrony danych osobowych.

2. Konstytucjonalizacja ochrony danych w prawie UE

2.1. Geneza prawa do ochrony danych

Tradycyjnie włączenie ochrony danych osobowych do katalogu praw podstawowych UE łączy się dopiero z wejściem w życie Traktatu z Lizbony, którego mocą państwa członkowskie nadały Karcie praw podstawowych moc równą traktatom. Oczywiście również przed wprowadzeniem reformy lizbońskiej Trybunał Sprawiedliwości wielokrotnie wypowiadał się co do roli i znaczenia danych osobowych[14], a także podkreślał znaczenie poszanowania praw podstawowych jako nieprzekraczalnej bariery określającej ramy funkcjonowania Unii Europejskiej[15].

[14] M. O'Neill, *The Issue...*
[15] A. Tizzano, *The Role...*

Na tym tle warto pamiętać, że sama Karta – pierwotnie przyjęta w 2000 r. jako dokument wyznaczający kierunek działań instytucji UE – już w swojej pierwszej wersji definiowała prawo do ochrony danych jako odrębne prawo podmiotowe. Przyjęty wówczas sposób zdefiniowania nowego prawa funkcjonuje do dzisiaj i *de facto* w późniejszym czasie stał się również wzorem dla reformy Konwencji nr 108 Rady Europy[16]. Treść Karty w tym zakresie wypełniała dyspozycję art. 286 obowiązującego wówczas Traktatu ustanawiającego Wspólnotę Europejską (dalej: TWE). W efekcie, szukając daty, od której należy mówić o rozpoczęciu procesu konstytucjonalizacji prawa do ochrony danych w unijnym (wspólnotowym) porządku prawnym, należy wskazać na 1 stycznia 1999 r. – a więc datę, od której zgodnie z art. 286 ust. 1 unijne przepisy o ochronie danych miały zastosowanie do instytucji i organów ustanowionych w traktatach.

Prawo do ochrony danych osobowych zostało zagwarantowane nie tylko w Karcie praw podstawowych, ale także – jako jedne z niewielu[17] – wprost i niezależnie wprowadzone także bezpośrednio w Traktacie o funkcjonowaniu Unii Europejskiej (dalej: TFUE). Zgodnie z art. 16 TFUE (stanowiącym rozszerzenie obowiązującego wcześniej art. 286 TWE) każdy ma prawo do ochrony danych osobowych, które go dotyczą. Chociaż w wersji polskiej istnieją różnice w tłumaczeniu między art. 16 ust. 1 TFUE a art. 8 ust. 1 KPP, normy te mają identyczne brzmienie w tekstach oryginalnych.

Na tym tle warto także wyjaśnić powód, dla którego zdecydowano się na niejako powtórzenie tego samego przepisu w dwóch aktach prawnych – zaliczanych w hierarchii źródeł prawa do tej samej kategorii prawa pierwotnego. Jest nim oczywiście potrzeba ustanowienia czytelnej normy kompetencyjnej, stanowiącej podstawę dla przyjęcia unijnych przepisów o ochronie danych[18]. Wcześniejsze regulacje (w szczególności dyrektywa 95/46/WE), wprowadzane były na podstawie ogólnej normy dotyczącej współpracy gospodarczej (harmonizacji rynku wewnętrznego). Wraz z likwidacją podziału na trzy filary integracji reforma lizbońska umożliwiła przyjęcie nowej treści art. 16 TFUE, w której poza zdefiniowaniem prawa do ochrony danych,

[16] Formalnie zmodernizowana treść traktatu została przyjęta jako Protokół zmieniający Konwencję nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych – C. de Terwangne, *Council of Europe...*

[17] Do tego typu wyjątków należą np. prawo dostępu do informacji publicznej w zakresie działania UE (art. 15 TUE), prawo do przemieszczania się (art. 21 TUE) czy prawo do głosowania w wyborach lokalnych (art. 22 TUE).

[18] Trzeba pamiętać, że Karta praw podstawowych, zgodnie z jej art. 51 ust. 2, nie rozszerza *per se* kompetencji przyznanych Unii w traktatach.

ustanowiono również normę kompetencyjną dla przyjęcia horyzontalnych przepisów o ochronie danych. Wydaje się jednak bardziej zasadne, aby państwa członkowskie w konstrukcji art. 16 ust. 1 TFUE wprost odwołały się do wykładni prawa wynikającego z Karty praw podstawowych – co pozwoliłoby rozstrzygnąć wątpliwości na temat wpływu klauzuli derogacyjnej wynikającej z Karty na zakres stosowania prawa opisanego w art. 16 ust. 1 TFUE[19].

2.2. Zakres przedmiotowy i podmiotowy

Zespół norm wynikających z art. 8 KPP definiuje ogólne prawo, przyznane wszystkim osobom znajdującym się pod ochroną przepisów prawa UE (a więc nie tylko obywatelom państw członkowskich) do ochrony danych osobowych ich dotyczących – obejmujące także prawo dostępu do danych oraz ich sprostowania. Obowiązek poszanowania tego prawa nie został przy tym ograniczony wyłącznie do organów publicznych. Co więcej, w treści art. 8 ust. 2 KPP doprecyzowano także najważniejsze zasady przetwarzania danych – takie jak zasada legalności, rzetelności oraz ograniczenia celu.

Zestawiając art. 8 KPP z innymi prawami i wolnościami przewidzianymi w Karcie, uwagę zwraca stosunkowo duża szczegółowość tej normy. Autorzy Karty nie poprzestali wszakże na zdefiniowaniu praw jednostki, ale również wskazali najważniejsze obowiązki, które należy łączyć z ich poszanowaniem. Taka konstrukcja przepisu wynikała przede wszystkim z potrzeby wyznaczenia najważniejszych elementów konstrukcyjnych nowego prawa, które nie miało *de facto* odpowiednika w funkcjonujących wówczas przepisach konstytucyjnych państw członkowskich. Jak wskazano w poprzedniej sekcji, w czasach pracy nad treścią Karty ujęcie prawa do ochrony danych jako odrębnego prawa podmiotowego stanowiło *novum* na tle dominującego w tamtym czasie poglądu, że prawo to należy postrzegać jako prawo zależne względem ochrony prywatności[20]. Ponieważ zaś zakres prawa do prywatności przewidziany w Karcie był tożsamy z zagwarantowanym w przepisach Europejskiej Konwencji Praw Człowieka, a wszystkie państwa członkowskie UE były w czasie powstawania Karty stronami tej

[19] Na tym tle zgłaszać można przecież wątpliwości co do skutków Protokołu brytyjskiego, który przecież dotyczy wyłącznie ograniczenia kognicji Trybunału Sprawiedliwości oraz sądów krajowych w odniesieniu do praw wynikających z Karty praw podstawowych, a nie Traktatu o funkcjonowaniu Unii Europejskiej.

[20] W tym zakresie wystarczy przytoczyć pełne tytuły Konwencji 108 oraz dyrektywy 95/46/WE – w których ochronę danych osobowych wprost zdefiniowano jako *lex specialis* względem prawa do prywatności.

konwencji – wykładnia Europejskiego Trybunału Praw Człowieka dotycząca treści i dopuszczalnej ingerencji w prawo do prywatności na gruncie konwencyjnym mogła być również wprost zastosowana na potrzeby interpretacji tożsamej normy wprowadzonej w Karcie (co zresztą wynika bezpośrednio z art. 52 ust. 3 KPP). Prawo do ochrony danych osobowych nie miało odpowiednika w Europejskiej Konwencji Praw Człowieka. Pamiętając, że z perspektywy prawa UE Konwencja nie wyznacza maksymalnego standardu ochrony praw podstawowych, lecz standard minimalny, należy jednocześnie zauważyć, że prawodawca unijny, przyjmując odrębne i samodzielne prawo do ochrony danych, ustanowił wyższy standard ochrony praw jednostek niż wynikający z postanowień konwencyjnych.

Wraz z rozwojem usług cyfrowych, a także ze wzrostem możliwości technicznych dotyczących masowego przetwarzania informacji, pojęcie „dane osobowe" zaczęło być intepretowane w sposób rozszerzający, w efekcie czego zaczęło ono obejmować kolejne grupy informacji. Dlatego dzisiaj nie ma już wątpliwości, że do danych osobowych – w zależności od danej sytuacji faktycznej – należy zaliczyć nie tylko wykorzystywany przez użytkownika identyfikator internetowy, ale również profil automatycznie stworzony przez dostawcę usług czy zmienny dynamicznie adres IP[21]. Obecnie Trybunał Sprawiedliwości rozważa, czy logi komputerowe (tworzone w celu prowadzenia czynności wsparcia technicznego) także można zaklasyfikować do kategorii danych osobowych[22]. W efekcie coraz częściej w piśmiennictwie wskazuje się na ryzyko, że prawo ochrony danych wkrótce może stać się „prawem wszystkiego"[23]. W tym zakresie także widać podobieństwa do prawa do prywatności, w odniesieniu do którego podobne zastrzeżenia formułowano kilkadziesiąt lat wcześniej[24].

Z pojęciem danych osobowych ściśle związany jest termin ich przetwarzania, pozwalający wyznaczyć administratora danych, a więc głównego adresata obowiązków przewidzianych w unijnym prawie ochrony danych. Prawo UE nigdy nie zawierało enumeratywnie wskazanych czynności przetwarzania danych. W istocie przetwarzaniem jest zarówno wykonywanie aktywnych operacji na danych, jak i czynności pasywnych – niezwiązanych z ich odczytaniem czy przekształceniem – takich jak przechowywanie. Co

[21] Wyrok TSUE z 19 października 2016 r., C-582/14, *Patrick Breyer* przeciwko *RFN*, ECLI:EU:C:2016:779.

[22] Wniosek o wydanie orzeczenia w trybie prejudycjalnym z 21 września 2021 r. złożony przez Itä-Suomen hallinto-oikeus (Finlandia), C-579/21.

[23] N. Purtova, *The law...*

[24] T. Gerety, *Redefining...*

przy tym istotne, administratorem danych jest nie tyle podmiot, który dane przetwarza, ale ten, który podejmuje decyzję o ich przetwarzaniu. Innymi słowy, administratorem jest osoba ustalająca cele i formy przetwarzania, z inicjatywy której przetwarzanie jest prowadzone. Administrator nie musi przy tym nawet mieć dostępu do danych, wystarczy że jest podmiotem podejmującym decyzję o ich gromadzeniu. To kluczowa obserwacja, wyjaśnia bowiem, dlaczego poszukiwanie odpowiedzialności za ochronę danych wyłącznie w gronie podmiotów, które mają do nich bezpośredni dostęp, jest błędne. W rozumieniu prawa unijnego najpełniejszy obowiązek w zakresie ochrony danych ma podmiot, który decyduje o ich gromadzeniu – to on bowiem ustala, w jaki sposób dane będą gromadzone, kto będzie miał do nich dostęp i jaki jest dopuszczalny cel ich przetwarzania. Ten podmiot jest też później adresatem żądań osób, których dane są przetwarzane.

Z problematyką prawnej ochrony danych osobowych nierozerwalnie związane jest również zagadnienie anonimizacji danych. Dane anonimowe z definicji nie pozwalają na identyfikację podmiotu danych, a więc ich przetwarzanie odbywa się poza reżimem prawnym przeznaczonym dla danych osobowych[25]. Dlatego operacja anonimizacji danych (pozbawienie ich cech pozwalających na identyfikację osób fizycznych) to narzędzie stosowane do zwiększenia możliwości komercyjnego wykorzystania dużych zbiorów danych, które w innym wypadku nie mogłyby przedmiotem swobodnego obrotu. Jednocześnie w ostatnich latach coraz więcej uwagi poświęcane jest technikom deanonimizacji – pozwalającym na ponowną identyfikację osób w zbiorze, który wcześniej uznany za prawidłowo zanonimizowany[26]. Rozwój techniki umożliwił bowiem identyfikowanie osób także w danych anonimowych, prowadząc tym samym do dyskusji o zakresie przydatności uznawania jakichkolwiek danych dotyczących jednostek za prawdziwie anonimowe[27].

Istotna różnica między konstrukcją prawa do prywatności (art. 7) a prawa do ochrony danych (art. 8) – w kształcie wynikającym z Karty praw podstawowych – związana jest z uwzględnieniem w treści tej drugiej normy wymogu powołania niezależnego nadzoru, stojącego na straży przestrzegania zasad związanych z ochroną praw jednostek. W ten sposób prawodawca unijny stworzył instytucjonalny komponent, uzupełniający treść materialnego prawa do ochrony danych osobowych. To w istocie jedyny przykład,

[25] Zob. motyw 26 rozporządzenia 2016/679; szerzej M. Siwicki, *Anonimizacja...*

[26] P. Ohm, *Broken...*

[27] M. Rojszczak, *Definicja...*

gdy bezpośrednio w przepisach Karty wskazano instrument instytucjonalny, którego istnienie jest niezbędne do zapewnienia poszanowania konkretnego prawa osobistego.

2.3. Istota prawa do ochrony danych

Zdefiniowane w Karcie prawo do ochrony danych osobowych nie jest prawem absolutnym. Jego stosowanie może podlegać ograniczeniom, pod warunkiem że ograniczenia te zostaną wprowadzone ustawą, a nadto będą szanowały jego istotę, pozostając przy tym w zgodzie z zasadą proporcjonalności i konieczności. Wszelkie ograniczenia muszą także w sposób rzeczywisty przyczyniać się do realizacji uznanego celu funkcjonowania państwa demokratycznego.

Podczas badania dopuszczalności wprowadzenia określonego ograniczenia w przestrzeń praw podstawowych, tradycyjnie w pierwszej kolejności ocenie podlega test zgodności z prawem oraz proporcjonalności. Abstrahując od konstrukcji samego testu proporcjonalności (definiowanego nieco odmiennie w poszczególnych modelach prawnych, ale też np. przez Europejski Trybunał Praw Człowieka[28]), nie ulega wątpliwości, że jego fundamentalnym etapem jest potwierdzenie, iż badany środek w najmniej intruzyjny sposób wkracza w prawa jednostki. Innymi słowy, zamierzony cel nie może być osiągnięty z wykorzystaniem innego, mniej inwazyjnego środka.

Nie wolno jednak tracić z pola widzenia tego, że niezależnie od oceny proporcjonalności istotne jest również potwierdzenie, iż badany środek nie narusza samej istoty prawa podstawowego, a więc tej jego części, która podlega ochronie w każdych warunkach. W doktrynie wskazuje się, że istota prawa podstawowego może być definiowana w sposób relatywny lub absolutny[29]. W tym pierwszym wypadku istota prawa wyznaczana jest w kontekście badanego stanu faktycznego, a więc jest zależna od okoliczności danej sprawy, w której ingerencja ma nastąpić (lub nastąpiła)[30]. Z kolei zgodnie z koncepcją absolutną istota prawa jest niezmienna i wyznacza nieprzekraczalną granicę dla ingerencji w prawo jednostki. Dostrzegając, że autorzy art. 52 ust. 1 KPP odrębnie zdefiniowali test proporcjonalności

[28] J. Gerards, *How to improve...*

[29] B. Banaszak, w: *Konstytucja...*, komentarz do art. 31, nb 17.

[30] Dlatego też część komentatorów wskazuje, że takie definiowanie istoty prawa podstawowego w rzeczywistości zbliża ten instrument do testu proporcjonalności. Zob. np. L. Bosek, M. Szydło, w: *Konstytucja...*, komentarz do art. 31, nb 140–141.

oraz warunek poszanowania istoty prawa podstawowego, staje się jasne, że opowiedzieli się w ten sposób za definiowaniem istoty praw podstawowych w sposób absolutny.

Celem ochrony tak rozumianej istoty prawa podstawowego jest zapewnienie, aby każdy środek, który faktycznie pozbawia jednostkę zagwarantowanego jej prawa, był uznawany za niedopuszczalny, bez konieczności przeprowadzania tekstu proporcjonalności, a więc niezależnie również od tego, jak ważny cel realizuje. Dlatego Koen Lenaerts trafnie uznał, że badając ograniczenia dla praw wynikających z Karty, w pierwszej kolejności należy potwierdzić, że badany środek nie narusza istoty prawa podstawowego. W tym zakresie można więc mówić o swoistym teście „poszanowania istoty prawa podstawowego"[31].

Tak rozumiana istota prawa jest więc rodzajem prawa absolutnego, stanowiącego komponent zasadniczego prawa podmiotowego. W zakresie prawnej ochrony prywatności jest to zatem koncepcja zbieżna z tą formułowaną przez Andrzeja Kopffa jeszcze w latach 70. XX w., bazującą na wydzieleniu z konstrukcji prawa podmiotowego obszaru stanowiącego nienaruszalną przestrzeń wolności jednostki (wg propozycji Kopffa była nią „sfera intymności życia osobistego")[32].

Na tym tle nie przekonuje wywód Andrzeja Wróbla, utożsamiającego absolutny charakter niektórych praw podstawowych z nienaruszalnym (absolutnym) charakterem istoty pozostałych praw (które *per se* charakteru absolutnego nie mają). Na potwierdzenie swojej tezy wskazuje on, że Trybunał Sprawiedliwości w swoim orzecznictwie niekiedy przychylał się do koncepcji relatywnego wyznaczania istoty praw podstawowych[33]. W tym zakresie wskazuje, że Trybunał uznawał prawo do wolności wypowiedzi za niemające charakteru absolutnego, inaczej niż prawo do życia czy zakaz stosowania tortur i nieludzkiego lub poniżającego traktowania[34]. Andrzej Wróbel dostrzega, że przywołane przez niego rozważania Trybunału Sprawiedliwości dotyczą praw zagwarantowanych w Europejskiej Konwencji Praw Człowieka, w której określone są przecież prawa o charakterze absolutnym (do których zalicza się powołane prawo do życia oraz zakaz tortur i nieludzkiego lub poniżającego traktowania)[35]. Badając różnice między

31 K. Lenaerts, *Limits...*

32 A. Kopff, *Koncepcja...*

33 A. Wróbel, w: *Karta...*, komentarz do art. 52, nb 18.

34 Wyrok TSUE z 12 czerwca 2003 r., C-112/00, *Eugen Schmidberger, Internationale Transporte und Planzüge* przeciwko *Republice Austrii*, ECLI:EU:C:2003:333, pkt 80.

35 M.K. Addo, N. Grief, *Does Article 3...*; H. Battjes, *In Search...*

poszczególnymi prawami zagwarantowanymi w Konwencji, Trybunał Sprawiedliwości nie tyle przychylił się do koncepcji relatywnej, ale potwierdził, że w odniesieniu do niektórych praw ustanowienie jakichkolwiek ograniczeń jest prawnie niedopuszczalne. W tym zakresie warto pamiętać, że także w orzecznictwie Europejskiego Trybunału Praw Człowieka odnaleźć można bezpośrednie odniesienia do potrzeby poszanowania istoty praw podstawowych, a więc wyznaczenia swoistego rdzenia tego typu praw, którym należy przyznać ochronę absolutną[36].

Czytelne zdefiniowanie istoty prawa podstawowego ma więc fundamentalne znaczenie nie tylko dla oceny dopuszczalności działań podejmowanych przez organy władzy publicznej, ale również dla potwierdzenia, że badane prawo ma charakter faktycznie samodzielny. Zatem ustalenie istoty unijnego prawa do ochrony danych może pomóc wskazać, czy prawo to jest faktycznie odrębnym prawem podmiotowym, a nie wyłącznie rodzajem prawa akcesoryjnego, służącego uzupełnieniu gwarancji dotyczących prawnej ochrony prywatności.

Trybunał Sprawiedliwości podjął tę problematykę przy okazji badania dyrektywy retencyjnej, wskazując, że badane wówczas przepisy nie naruszają istoty prawa do prywatności, ponieważ nie pozwalają na przechwytywanie treści wymienianej korespondencji elektronicznej[37]. Trybunał wskazał w ten sposób, że nieukierunkowane (hurtowe) gromadzenie dużej części (a potencjalnie całości) treści korespondencji to środek, którego nie można pogodzić z poszanowaniem gwarancji wynikających z Karty praw podstawowych – prowadziłby bowiem do naruszenia istoty prawa do prywatności[38]. W odniesieniu do tych samych regulacji Trybunał Sprawiedliwości uznał, że nie doszło do naruszenia istoty prawa do ochrony danych osobowych, ponieważ dostawcy usług, na których nałożono obowiązek gromadzenia metadanych z łączności elektronicznej, zostali zobowiązani do przestrzegania konkretnych zasad w zakresie zabezpieczenia procesu przetwarzania danych[39]. *A contrario* można uznać, że do naruszenia istoty prawa do ochrony danych doszłoby w razie przetwarzania danych osobowych realizowanego

[36] Zob. np. wyrok ETPC z 23 czerwca 2016 r., 20261/12, *Baka* przeciwko *Węgrom*, pkt 121.

[37] Wyrok TSUE z 8 kwietnia 2014 r., C-293/12 i C-594/12, *Digital Rights Ireland Ltd* przeciwko *Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.*, ECLI:EU:C:2014:238, pkt 39.

[38] Analogicznie w wyroku TSUE z 6 października 2015 r., C-362/14, *Maximillian Schrems* przeciwko *Data Protection Commissioner*, ECLI:EU:C:2015:650, pkt 94.

[39] Wyrok TSUE w sprawie *Digital Rights Ireland*, pkt 40.

w sposób niechroniący „przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą" tych informacji.

W ten sposób Trybunał Sprawiedliwości wyjaśnił, że celem (istotą) prawa do prywatności jest ochrona jednostki przed swobodnym i pełnym wglądem w jej sprawy osobiste. Dlatego żaden środek – nawet spełniający kryterium proporcjonalności – nie może zostać uznany za zgodny z prawem UE, jeżeli wprowadza ograniczenia tak daleko idące, że tworzy z prawa do prywatności jedynie miraż, skorupę wydrążoną z wolności dostępnych dla ogółu społeczeństwa. Z kolei w odniesieniu do ochrony danych osobowych Trybunał podkreślił znaczenie ustanowienia elementarnych zasad przetwarzania danych ograniczających ryzyko błędów prowadzących do ich uszkodzenia czy zniszczenia. W takim rozumieniu naruszenie prawa do ochrony danych (także istoty tego prawa) może w ogóle nie skutkować negatywnymi konsekwencjami w zakresie prywatności jednostki[40].

2.4. Ochrona danych w orzecznictwie Trybunału Sprawiedliwości

Chociaż Trybunał Sprawiedliwości w sposób czytelny wyjaśnił różnicę między ochroną prywatności a ochroną danych osobowych, to jednocześnie w swoim orzecznictwie stosunkowo rzadko jako wzorzec kontroli stosował samodzielnie art. 8 KPP. Najczęściej w sprawach, w których przedmiotem oceny była dopuszczalność stosowania nowoczesnych technik przetwarzania danych, Trybunał rekonstruował standard oceny, stosując łącznie art. 7 i 8 KPP.

Jednocześnie argumentacja prezentowana w poszczególnych orzeczeniach wskazuje, że w ocenie Trybunału – przynajmniej w pewnym zakresie – rozdzielenie ochrony prywatności od ochrony danych osobowych jest w praktyce niemożliwe. Przykładem może być opinia wydana w sprawie projektowanej umowy UE i Kanady dotyczącej transferu danych o pasażerach lotniczych (*passegner name records*, PNR). Trybunał uznał w niej, że transfer taki (obejmujący co do zasady także dane osobowe) stanowi ingerencję w prawo do prywatności. Doszedł do takiego wniosku, ponieważ – jak stwierdził – prawo to „odnosi się do wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej"[41]. W ten sposób Trybunał zdefiniował ochronę danych jako komponent prawa do prywatności.

[40] Szerzej M. Brkan, *The Essence...*

[41] Opinia 1/15 TSUE z 26 lipca 2017 r., w sprawie projektu umowy między Kanadą a Unią Europejską o przekazywaniu danych dotyczących przelotu pasażera, ECLI:EU:C:2017:592, pkt 122.

Podobny wniosek płynie z analizy stanowiska przedstawionego w wyroku sprawie *Google Spain*, w którym Trybunał podkreślił, że wykładnia unijnych przepisów o ochronie danych, „w zakresie, w jakim regulują one kwestię przetwarzania danych osobowych mogących naruszyć podstawowe wolności, **a w szczególności prawo do prywatności** [wyróżnienie – M.R.], musi być bezwzględnie dokonywana z punktu widzenia praw podstawowych”[42]. W ten sposób Trybunał Sprawiedliwości ponownie podkreślił doniosłość ochrony danych osobowych z uwagi na jej związek z prawem do prywatności.

W efekcie Trybunał w grupie wyroków dotyczących różnych aspektów przetwarzania danych stosował łącznie wzorzec kontroli zrekonstruowany z norm art. 7 i 8 KPP. Dotyczy to m.in. wyroków dotyczących retencji danych[43], prawa do bycia zapomnianym[44], przetwarzania danych wrażliwych[45] czy algorytmicznego przetwarzania danych o pasażerach[46]. Nawet w sprawach dotyczących wprost ważności decyzji Komisji dotyczących transgranicznego przekazywania danych do państw trzecich, wzorcem kontroli były zawsze art. 7 i 8 KPP stosowane łącznie[47]. Trybunał opierał swoje wyrokowanie na standardzie wywodzonym z art. 8 KPP jedynie w sprawach dotyczących technicznych aspektów przetwarzania danych – np. roli organów nadzorczych[48] czy zgodności przetwarzania z zasadą określonego celu[49].

[42] Wyrok TSUE w sprawie *Google Spain SL*, pkt 68.

[43] Zob. np. wyrok TSUE z 21 grudnia 2016 r., C-203/15 i C-698/15, *Tele2 Sverige AB* przeciwko *Post-och telestyrelsen* oraz *Secretary of State for the Home Department* przeciwko *Tomowi Watsonowi i in.*, ECLI:EU:C:2016:970; wyrok TSUE z 6 października 2020 r., C-623/17, *Privacy International* przeciwko *Secretary of State for Foreign and Commonwealth Affairs i in.*, ECLI:EU:C:2020:790; wyrok TSUE z 6 października 2020 r., C-511/18, C-512/18 i C-520/18, *La Quadrature du Net i in.* przeciwko *Premier ministre i in.*, ECLI:EU:C:2020:791

[44] Wyrok TSUE w sprawie *Google Spain SL*, pkt 97; także wyrok TSUE w sprawie *GC*, pkt 44.

[45] Wyrok TSUE z 1 sierpnia 2022 r., C-184/20, *OT* przeciwko *Vyriausioji tarnybinės etikos komisija*, ECLI:EU:C:2022:601, pkt 126.

[46] Wyrok TSUE z 21 czerwca 2022 r., C-817/19, *Ligue des droits humains* przeciwko *Conseil des ministres*, ECLI:EU:C:2022:491.

[47] W szczególności dotyczy to wyroków skutkujących uchyleniem decyzji Komisji stanowiących podstawę do realizacji dwóch kluczowych programów transatlantyckiej wymiany danych osobowych – programu Bezpieczna przystań (ang. *Safe Habour*) oraz Tarcza prywatności (*Privacy Shield*). Zob. wyrok TSUE z 6 października 2015 r., C-362/14, *Maximillian Schrems* przeciwko *Data Protection Commissioner*, ECLI:EU:C:2015:650 oraz wyrok TSUE z 16 lipca 2020 r., C-311/18, *Data Protection Commissioner* przeciwko *Facebook Ireland i Maximillian Schrems*, ECLI:EU:C:2020:559.

[48] Wyrok TSUE z 9 marca 2010 r., C-518/07, *Komisja* przeciwko *Niemcom*, ECLI:EU:C:2010:125; wyrok TSUE z 8 kwietnia 2014 r., C-288/12, *Komisja* przeciwko *Węgrom*, ECLI:EU:C:2014:237.

[49] Wyrok TSUE w sprawie *Wirtschaftsakademie Schleswig-Holstein*.

Co więcej, chociaż Trybunał Sprawiedliwości historycznie stwierdzał niezgodność z prawem UE określonych przepisów lub praktyki krajowej z uwagi na naruszenie istoty prawa do prywatności[50], to dotychczas taka sytuacja nigdy nie wystąpiła w przypadku naruszenia istoty prawa do ochrony danych. Częściowo wynika to ze specyfiki regulacji dotyczących ochrony danych – które są stosowane zaledwie od kilkudziesięciu lat, a znaczące kontrowersje dotyczące ich wykładni pojawiły się wraz z dynamicznym rozwojem rynku cyfrowego (a więc w ostatnich kilkunastu latach). Jednocześnie jednak wydaje się, że ciągłe przedstawianie przedmiotu i zakresu prawa do ochrony danych niejako w kontekście prawa do prywatności stanowi przeszkodę dla zapewnienia skutecznej realizacji praw jednostek w cyberprzestrzeni[51]. Stałe badanie poszczególnych aspektów ochrony danych w kontekście naruszeń prawa do prywatności przesuwa bowiem na dalszy plan obowiązki związane z bezpieczeństwem przetwarzanych danych – co nie jest zgodne z pierwotną intencją prawodawcy, związaną z ustanowieniem dwóch odrębnych i niezależnych praw podmiotowych.

3. Ochrona danych w krajowych przepisach konstytucyjnych

3.1. Zakres przedmiotowy i podmiotowy

Inaczej niż w przypadku Karty praw podstawowych, w redakcji art. 51 Konstytucji RP nie wprowadzono ogólnego prawa do ochrony danych, podlegającego uszczegółowieniu w kolejnych ustępach przywołanego przepisu. Polski ustrojodawca w art. 51 zawarł natomiast zespół norm, które *de facto* ustanawiają odrębne prawa – różniące się zarówno zakresem przedmiotowym, jak i podmiotowym.

Źródłem ogólnego prawa do ochrony danych nie jest z pewnością art. 51 ust. 1 Konstytucji RP, zgodnie z którym nikt nie może być zobowiązany inaczej niż w ustawie do ujawniania informacji go dotyczących. Chociaż z zakazu tego bez problemu można zrekonstruować prawo podmiotowe – to jego zakresem objęte będzie uprawnienie do nieujawniania informacji na swój temat, nie zaś prawo do ochrony danych, które (w sposób legalny) zostały

[50] Zob. wyrok w sprawie *Maximillian Schrems* przeciwko *Data Protection Commissioner* (tzw. Schrems I), w którym Trybunał wskazał, że badane przepisy decyzji KE naruszają zarówno istotę prawa do prywatności (pkt 94 wyroku) jak i prawa do skutecznej ochrony prawnej (art. 95).

[51] Na tym tle zob. także trafne uwagi: J. Kokott, C. Sobotta, *The distinction...*

przekazane do dalszego przetwarzania. Ustrojodawca skoncentrował się zatem na uszczegółowieniu gwarancji związanych z prywatnością jednostki i tak też ta norma jest powszechnie interpretowana zarówno w doktrynie[52], jak i judykaturze[53].

Chociaż zakres art. 51 ust. 1 Konstytucji RP nie został *explicite* ograniczony wyłącznie do podmiotów publicznych, to jednak z uwagi na systematykę wskazanej normy – odnoszącej się do „obowiązku ujawniania" informacji – jej zastosowanie do przypadków gromadzenia informacji przez podmioty publiczne wydaje się naturalne[54]. Przepis ten nie wprowadza zatem ograniczeń w przekazywaniu informacji według uznania jednostki (np. na podstawie udzielonej zgody czy zawartej umowy) ani nie ustanawia wyraźnego zakazu dla pozyskiwania tzw. danych wrażliwych[55].

W istocie w badanej regulacji w ogóle brak bezpośredniego odniesienia do terminu „dane osobowe". W rozumieniu art. 51 ust. 1 Konstytucji RP nie ma zatem znaczenia, jakie informacje miałaby ujawnić jednostka, w szczególności czy spełniają one definicję danych osobowych (a więc czy razem z informacjami już posiadanymi przez podmiot pozwalają na – nawet pośrednią – identyfikację danej osoby). Słusznie w literaturze wskazuje się, że taka wykładnia powinna prowadzić do wniosku, że również ujawnianie informacji zanonimizowanych (lub w sposób anonimowy) mieści się w hipotezie omawianej normy[56]. W tym zakresie przez pojęcie danych anonimowych należy rozumieć takie informacje, które nie pozwalają na zidentyfikowanie podmiotów danych. W praktyce trudno założyć, aby proces gromadzenia danych (oparty na legalnej podstawie prawnej) był prowadzony w sposób anonimowy.

---

52 Zob. w szczególności argumentację przedstawioną w komentarzach do Konstytucji RP napisanych pod red. B. Banaszaka (Warszawa 2012), L. Garlickiego i M. Zubika (Warszawa 2016), M. Safjana i L. Boska (Warszawa 2016) czy P. Tulei (Warszawa 2019).

53 Zob. szerzej na temat relacji między art. 47 i 51 Konstytucji RP w wyroku TK z 19 czerwca 2018 r., SK 19/17, OTK-A 2018, poz. 42 oraz w przywołanym w nim orzecznictwie.

54 M. Wild w swojej argumentacji idzie jednak dalej, wskazując, że to wyłącznie organy władzy publicznej są adresatem wskazanej normy. Odmienne stanowisko prezentuje K. Wygoda, sprzeciwiając się przyjęciu, że podmioty niepubliczne w ogóle nie podlegają ograniczeniom wynikającym z art. 51. Zob. M. Wild, w: *Konstytucja...*, komentarz do art. 51, nb 15; K. Wygoda, *Prawo...*, s. 56.

55 Chociaż sam Trybunał Konstytucyjny wykorzystywał w swoim orzecznictwie termin „dane wrażliwe" do określenia informacji szczególnie chronionych – zob. zamiast wielu: wyrok TK z 18 grudnia 2014 r., K 33/13, OTK-A 2014, nr 11, poz. 120 i przywołane w nim orzecznictwo.

56 Tak M. Wild, w: *Konstytucja...*, komentarz do art. 31, nb 18–20.

Współcześnie ujawnianie informacji organom publicznym coraz częściej nie polega na przekazywaniu ich urzędnikowi do protokołu, ale na masowym ich gromadzeniu w sposób automatyczny. Przykładowym mechanizmem pozyskiwania tego typu informacji mogą być na przykład publiczne aplikacje mobilne, które coraz częściej są preferowanym także przez obywateli sposobem komunikacji z administracją i korzystania z e-usług publicznych. Dość powiedzieć, że wiele tego typu produktów wymaga do prawidłowego działania różnego rodzaju uprawnień, w tym na przykład związanych z dostępem do listy zainstalowanych na urządzeniu (np. telefonie) aplikacji. Prowadzi to do wątpliwości, czy dostęp do tego typu danych powinien być zaklasyfikowany jako „ujawnianie informacji o osobie" w rozumieniu art. 51 ust. 1 Konstytucji RP[57]. Ocena ta może ulec zmianie po uwzględnieniu faktu, że dzięki wykorzystaniu odpowiednio dużej bazy danych oraz wyłącznie na podstawie listy zainstalowanych aplikacji i częstotliwości ich używania można z wysokim poziomem ufności wnioskować o intymnych kwestiach dotyczących użytkownika, w tym o jego o orientacji seksualnej[58]. Nie sposób jednak założyć, aby każdy podmiot (w tym publiczny), który gromadzi informacje techniczne, np. związane z listą aplikacji zainstalowanych na urządzeniu abonenckim, zamierzał prowadzić analizy ujawniające szczególne kategorie danych (dane wrażliwe).

Obserwacja ta prowadzi do odrębnego problemu, jakim jest kwestia ujawniania (a następnie przetwarzania) tzw. danych wrażliwych. Mikołaj Wild zaznacza, że informacje tego typu na gruncie art. 51 Konstytucji RP „objęte są szczególną ochroną konstytucyjną"[59]. Dane wrażliwe to pojęcie wprost zaczerpnięte z prawa UE, gdzie oznaczają szczególny zbiór informacji, w tym dotyczących pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych, przynależności wyznaniowej lub związkowej, a także danych o stanie zdrowia, kodzie genetycznym, nałogach

[57] Podobne wątpliwości w zakresie stosowania unijnego prawa do ochrony danych dotyczą – nadal nierozstrzygniętego – sporu o to, czy numer rejestracyjny samochodu należy uznać za dane osobowe. Chociaż większość doktryny przychyla się do stanowiska, że numer rejestracyjny jest (lub w konkretnym przypadku – może być) informacją o osobie fizycznej, to pogląd ten nie znajduje aprobaty w orzecznictwie sądów administracyjnych – por. np. wyrok NSA z 3 listopada 2022 r., III OSK 1522/21, LEX nr 3429658: „dane dotyczące rzeczy nie stanowią [danych osobowych – przyp. M.K.], jeżeli zidentyfikowanie posiadacza tej rzeczy możne być dokonane tylko poprzez dostęp do odpowiednich rejestrów lub katalogów".

[58] M. Rojszczak, *Definicja...*, s. 123. Szerzej o profilowaniu użytkowników na podstawie (meta) danych opisujących sposób korzystania przez nich z aplikacji mobilnych – S. Zhao i in., *User...*

[59] M. Wild, w: *Konstytucja...*, komentarz do art. 51, nb 34.

czy życiu seksualnym[60]. W prawie UE przewidziano domyślny zakaz przetwarzania tego typu informacji, od którego ustanowiono zamknięty katalog wąskich wyjątków. Co do zasady przepisy Konstytucji RP nie zawierają równoważnej normy *explicite* zakazującej przetwarzania danych wrażliwych ani nawet określającej katalog tego typu danych. O ile możliwe jest poszukiwanie konstytucyjnej definicji „danych wrażliwych" w odniesieniu do wolności sumienia czy prawa do prywatności, to w ten sposób trudno byłoby odtworzyć stosowany standard równoważny temu istniejącemu na gruncie prawa UE. Zasadne natomiast byłoby postulowanie, że – z braku bardziej szczegółowej definicji – przez pojęcie danych wrażliwych należy rozumieć dane ujawniające „światopogląd, przekonania religijne lub wyznanie" (por. art. 53 ust. 7 Konstytucji RP)[61].

Ponieważ ustrojodawca ograniczył wprowadzony przez siebie zakaz wyłącznie do przypadków „ujawniania" informacji, powstają wątpliwości, na ile regulacja ta ogranicza także swobodne przetwarzanie informacji dotyczących jednostki pozyskanych w inny sposób (np. od innych podmiotów). Zręb tego typu regulacji można odnaleźć w art. 52 ust. 2 Konstytucji RP, zgodnie z którym władze publiczne mogą „pozyskiwać, gromadzić i udostępniać" wyłącznie takie informacje o obywatelach, które są niezbędne w demokratycznym państwie prawnym. Norma ta nie stanowi jednak rozwinięcia art. 51 ust. 1 Konstytucji RP, bo *de facto* zakreśla zarówno inny krąg podmiotów uprawnionych (wyłącznie obywatele), jak i zobowiązanych (organy publiczne). Abstrahując od powodów, dla których poszanowanie wartości państwa demokratycznego miałoby wyznaczać granicę dla działań organów publicznych wyłącznie względem osób posiadających polskie obywatelstwo[62], uwagę zwraca również stosunkowo wąski katalog reglamentowanych czynności przetwarzania. Niejasności budzą także użyte pojęcia – np. odrębne wyszczególnienie „pozyskiwania" danych, obok ich „gromadzenia". Jeżeli – w ocenie ustrojodawcy – istnieje możliwość pozyskania informacji

[60] Do 2018 r. w polskim systemie prawnym tożsamą definicję można było odnaleźć w art. 27 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych. W efekcie kwestia dopuszczalności przetwarzania danych wrażliwych przez organy władzy publicznej była badana na podstawie standardu konstytucyjnego uzupełnionego tą regulacją ustawową – zob. np. wyrok TK z 20 stycznia 2015 r., K 39/12, OTK-A 2015, nr 1, poz. 2.

[61] Por. też wyrok TK z 11 maja 2007 r., K 2/07, OTK-A 2007, nr 5, poz. 48.

[62] Na ten temat także Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r., K 23/11, OTK-A 2014, nr 7, poz. 80: „Mając na uwadze przede wszystkim art. 30 i art. 37 ust. 1 Konstytucji trzeba przyjmować – jako założenie wyjściowe – jednakowy standard ingerencji w konstytucyjne wolności oraz prawa, bez względu na to, czy ich podmiot ma obywatelstwo polskie".

o jednostkach, które nie jest jednocześnie ich gromadzeniem, to wydaje się, że taki wniosek powinien być uwzględniony w redakcji innych przepisów ustawy zasadniczej (por. treść art. 51 ust. 5 Konstytucji RP, w którym brak „pozyskiwania" danych).

Stosunkowo wąski zakres zakazu w art. 51 ust 2 Konstytucji RP pozostaje zatem bez wpływu na możliwość dalszego przetwarzania danych, np. w celu ujawnienia (odkrycia) nowych (nieznanych wcześniej) faktów z wykorzystaniem rozbudowanych algorytmów, takich jak big data. A więc nie wprowadza on czytelnych ograniczeń związanych z profilowaniem użytkowników, która to technika jest przecież coraz częściej stosowana również przez organy publiczne[63].

Ustanowionym zakazom towarzyszą szczególne prawa jednostki – w szczególności prawo do informacji (na gruncie Konstytucji RP nazwane prawem dostępu do dokumentów i zbiorów danych), a także prawo żądania sprostowania oraz usunięcia informacji nieprawdziwych lub zgromadzonych w sposób bezprawny. Również w tym wypadku ustrojodawca nie uniknął jednak kontrowersji terminologicznych – np. ograniczając prawo do informacji wyłącznie do urzędowych dokumentów i zbiorów danych. W świetle definicji stosowanej na gruncie procedury cywilnej dokumenty urzędowe to takie, które zostały sporządzone we właściwej formie przez powołane do tego organy[64], co implikuje wytworzenie ich przez te organy. Taka interpretacja pozbawiałaby ochrony w odniesieniu do informacji, które organ posiada, ale których nie wytworzył. Czyniłoby zatem przywołany przepis nieprzydatnym do osiągnięcia celu, dla którego został wprowadzony – a nie jest nim przecież rozumiana abstrakcyjnie kontrola legalności działań organów władzy publicznej, ale ochrona autonomii informacyjnej jednostki, definiowanej jako prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących siebie oraz prawo do kontrolowania, które z tych informacji znajdą się w dyspozycji innych podmiotów[65].

Na tym tle Paweł Sarnecki zbyt pochopnie wskazuje, że obowiązek sprostowania informacji jest adresowany do administratora danych – czego przecież z treści komentowanego przepisu wyczytać nie sposób[66]. Wniosek taki byłby prawdziwy na gruncie unijnego prawa do sprostowania informacji

63 B. Szafrański, *Realizacja...*

64 A. Mendrek, *Pojęcie...*, s. 27–44.

65 Wyrok TK z 20 czerwca 2005 r., K 4/04, OTK-A 2005, nr 6, poz. 64.

66 P. Sarnecki, w: *Konstytucja...*, komentarz do art. 51, nb 3.

(stanowiącego komponent prawa do ochrony danych)[67], jednak w odniesieniu do regulacji konstytucyjnej po stronie zobowiązanej należy wskazać raczej każdy podmiot przetwarzający informacje (a więc nie tylko administratora)[68].

Do czasu wejścia w życie rozporządzenia 2016/679 krajowa ustawa o ochronie danych była wskazywana jako akt zarówno stanowiący transpozycję unijnej dyrektywy 95/46/WE oraz określający zasady wykonywania praw przewidzianych w art. 51 Konstytucji RP. Jednak w obecnym porządku prawnym to rozporządzenie 2016/679 określa zasady wykonywania unijnego prawa do ochrony danych. Jest przy tym jasne, że celem przyjęcia przez prawodawcę unijnego nowego rozporządzenia nie była szczegółowa regulacja praw i obowiązków, o których mowa w polskiej Konstytucji. Trudno zatem przyjąć, że rozporządzenie 2016/679 uzupełnia polski system prawny o regulacje podkonstytucyjne, o których mowa w poszczególnych ustępach art. 51 ustawy zasadniczej – a więc że z perspektywy przepisów konstytucyjnych pełni tą samą funkcję, którą wcześniej realizowała ustawa o ochronie danych osobowych. Prowadzi to do wniosku, z uwagi na brak szczegółowej regulacji ustawowej, że prawo do sprostowania (wynikające z art. 51 ust. 4 Konstytucji RP) może być wykonywane przez jednostkę względem każdego podmiotu dokonującego takiego przetwarzania, a nie tylko administratora danych (jak jest to przyjęte w prawie UE).

Ustrojodawca, ustanawiając prawo do sprostowania i usunięcia informacji (art. 51 ust. 4 Konstytucji RP), ograniczył jego stosowanie wyłącznie do przypadków przetwarzania informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Co do zasady oznacza to, że konstytucyjne „prawo do usunięcia danych" ma znacząco węższy zakres niż tożsame prawo wynikające z regulacji UE[69]. Nie obejmuje bowiem (naj-

[67] Por. art. 16 rozporządzenia 2016/679. Sądy krajowe również nie kwestionują, że żądanie sprostowania (wywodzone z tego rozporządzenia) może być wykonywane przez osoby, których dane dotyczą, i kierowane jest do administratorów danych, a nie dowolnych podmiotów – zob. np. wyrok WSA w Warszawie z 6 maja 2022 r., II SA/Wa 3238/21, LEX nr 3413849.

[68] Co oczywiście prowadzi także do pytań o bezpośredni skutek horyzontalny badanego przepisu, zwłaszcza w sytuacji, gdy – o czym szerzej w dalszej części artykułu – w obecnym porządku prawnym brak regulacji podkonstytucyjnych w sposób kompleksowy regulujących materię ochrony danych osobowych. Na brak skutku horyzontalnego badanej regulacji wskazuje m.in. M. Wild, w: *Konstytucja...*, komentarz do art. 51, nb 46, dowodząc, że omawiana regulacja odnosi się wyłącznie do urzędowych dokumentów i zbiorów danych.

[69] Chociaż pierwotnie zakres stosowania prawa do usunięcia danych (prawo do bycia zapomnianym) był wywodzony głównie z orzecznictwa Trybunału Sprawiedliwości (zob. np. wyrok TSUE w sprawie *Google Spain*), to obecnie (w szerszym zakresie) jest gwarantowane przez art. 17 rozporządzenia 2016/679. Szerzej o prawie do bycia zapomnianym – T. Grzegory, *Pamięć...*, s. 58–68; M. Rojszczak, *Analiza...*, s. 30–41.

częstszych) przypadków, gdy dane, które pierwotnie zostały zgromadzone w sposób legalny, obecnie nie są już potrzebne do osiągnięcia zamierzonego celu przetwarzania. Wątpliwości budzi także warunek sprzeczności z ustawą – który wszakże nie jest tożsamy z gromadzeniem informacji bez podstawy prawnej[70]. O ile na gruncie prawa UE nie ma wątpliwości, że samodzielną podstawą żądania usunięcia danych jest ich zgromadzenie bez podstawy prawnej[71], to w przypadku przywołanej normy konstytucyjnej postulat taki może budzić wątpliwości – zwłaszcza w odniesieniu do podmiotów zobowiązanych (przetwarzających informacje) nienależących do kręgu organów publicznych.

W zestawieniu zakresu przedmiotowego i podmiotowego prawa do ochrony danych (wynikającego z art. 8 KPP) oraz kompleksu gwarancji wprowadzonych w krajowych przepisach konstytucyjnych dostrzegalny jest również brak w tych drugich czytelnego odniesienia do nakazu przetwarzania informacji zgodnie z prawnie dopuszczalnym celem ich zgromadzenia. Prawo UE wyklucza sytuacje, gdy administrator danych (podmiot przetwarzający) samodzielnie zmienia cel przetwarzania pozyskanych wcześniej danych. Zakaz taki wynika wprost z przyjętej redakcji art. 8 KPP. Regulacje konstytucyjne takiego ograniczenia nie wprowadzają. Oznacza to, że praktyka ponownego wykorzystania danych przez organy publiczne do realizacji innego, prawnie uzasadnionego celu nie będzie prowadziła do naruszenia przywołanej normy konstytucyjnej. Dość powiedzieć, że w przypadku prawa UE brak poszanowania zasady ograniczonego celu stanowiło samodzielną podstawę dla uznania przez Trybunał Sprawiedliwości niezgodności badanych przepisów z Kartą praw podstawowych[72].

Różnice między unijnym a krajowym modelem ochrony danych są dostrzegalne zwłaszcza w odniesieniu do hybrydowych zagrożeń dla prywatności użytkowników online – tj. takich zagrożeń, które wymykają się tradycyjnie stosowanemu (i coraz częściej nieaktualnemu) podziałowi na zagrożenia wertykalne i horyzontalne. Z perspektywy prawa UE ten podział nie wpływa na zakres praw jednostki, ponieważ gwarancje związane z ochroną danych nie zostały zróżnicowane względem tożsamości podmiotu gromadzącego czy przetwarzającego informacje. Z kolei redakcja art. 51 Konstytucji RP

[70] Innymi słowy, „sprzeczność" – rozumiana jako działanie *explicite* naruszające obowiązującą normę prawną – nie jest jedynym przypadkiem bezprawności przetwarzania danych osobowych, co zresztą wynika również wprost z rozporządzenia 2016/679.

[71] Por. art. 17 ust. 1 lit. d rozporządzenia 2016/679.

[72] Zob. argumentację Trybunału przedstawioną w wyroku w sprawie *Ligue des droits humains*.

powoduje, że zarówno zakres konkretnych gwarancji (w wymiarze zakresu gromadzonych informacji oraz dopuszczalnych form ich przetwarzania), jak też kręgi podmiotów uprawnionych i zobowiązanych różnią się w poszczególnych ustępach przywołanej regulacji.

Nie ulega wątpliwości, że redakcja przepisu jest efektem przekonania ustrojodawcy o szczególnym charakterze ryzyka związanego z gromadzeniem przez organy władzy publicznej nadmiarowych informacji dotyczących jednostek. Jednocześnie jednak, w warunkach zglobalizowanego rynku danych, opartego w dużej mierze na masowym gromadzeniu informacji przez podmioty prywatne, zdefiniowane w ten sposób gwarancje konstytucyjne mogą okazać się niewystarczające do skutecznej ochrony praw podstawowych.

3.2. Relacja z prawem do prywatności

Na gruncie polskich przepisów konstytucyjnych zestaw gwarancji wprowadzonych w art. 51 nie tworzy odrębnego, całościowego prawa do ochrony danych osobowych – ale wzmacnia prawa jednostki w obszarze ochrony jej prywatności, co do zasady zagwarantowane już w art. 47 Konstytucji RP. Na prawidłowość takiego wniosku wskazuje Bogusław Banaszak, który – bazując na wykładni Trybunału Konstytucyjnego[73] – dowodzi, że w kontekście polskich przepisów konstytucyjnych prywatność nie tylko jest pojęciem szerszym niż ochrona danych osobowych, ale również, że jest źródłem szczególnych praw jednostki w zakresie dotyczących jej danych[74].

Dlatego w doktrynie prawa powszechnie wskazuje się, że chociaż art. 51 Konstytucji RP nie obejmuje wielu ingerencji horyzontalnych (a także niektórych wertykalnych) – to tego typu przypadki oceniane mogą być na zgodność z ogólniejszym art. 47. W takim ujęciu art. 51 nie ustanawia zatem prawa do ochrony danych (w rozumieniu całościowej, samodzielnej regulacji – na wzór prawa wprowadzonego w prawie UE), ale służy doprecyzowaniu niektórych gwarancji wynikających z ochrony prywatności – dotyczących głównie (ale nie jedynie) ochrony autonomii informacyjnej przed działaniami organów władzy publicznej[75]. Taka interpretacja znajduje potwierdzenie w orzecznictwie Trybunału Konstytucyjnego, który wskazuje, że „[a]rt. 51

[73] Por. wyrok TK z 19 maja 1998 r., U 5/97, OTK 1998, nr 4, poz. 46.

[74] B. Banaszak, w: *Konstytucja...*, komentarz do art. 51, nb 2.

[75] W tym zakresie zob. także wyrok TK z 22 lipca 2014 r., K 25/13, OTK-A 2014, nr 7, poz. 76: „w większości orzeczeń [TK] prezentowany był pogląd, że norma wysłowiona w art. 51 ust. 2 Konstytucji nie ma charakteru całkowicie samodzielnego".

Konstytucji stanowi szczególny środek ochrony tych samych wartości, które chronione są za pośrednictwem art. 47 Konstytucji”[76], a także że ochrona danych osobowych stanowi „konkretyzację prawa do prywatności w aspektach proceduralnych”[77].

Przedstawiony pogląd wymaga szerszego komentarza. Treść prawa ustanowionego w art. 47 Konstytucji RP jest tożsama nie tylko z art. 7 KPP, ale jest również zbliżona do art. 8 ust. 1 EKPC. W Konwencji nie zdefiniowano odrębnie prawa do ochrony danych, co jest zrozumiałe, uwzględniając, że powstała w czasach przed erą komputeryzacji, a jej kształt odzwierciedlał powojenne wyobrażenie o celach ustanawiania ponadnarodowego systemu ochrony praw człowieka (nakierowanego na ochronę przez zagrożeniami wertykalnymi). Brak odrębnej regulacji *explicite* dotyczące ochrony danych osobowych nie stanowił przeszkody do uznania przez Europejski Trybunał Praw Człowieka, że gwarancje dotyczące ochrony danych wynikają wprost z prawa do prywatności. W ten sposób z rozszerzającej wykładni Trybunału wynika, że na gruncie Konwencji jednostka może poszukiwać ochrony między innymi w przypadkach gromadzenia danych nadmiarowych[78], w sposób nierzetelny[79] lub przez okres dłuższy niż wymagany do realizacji prawnie uzasadnionego celu[80].

Co więcej, chociaż Konwencja co do zasady nakłada obowiązki na państwa, nie są to wyłącznie obowiązki negatywne (dotyczące powstrzymania się od nieuprawnionej ingerencji). Trybunał w licznych orzeczeniach wskazał, że zapewnienie praw i wolności wynikających z Konwencji wymaga również odpowiedniego ukształtowania prawa krajowego, w sposób zapewniający poszanowanie praw jednostek w relacjach horyzontalnych[81]. W ten sposób wskazywał potrzebę wprowadzenia odpowiednich regulacji krajowych chroniących przed nadużyciami związanymi z przetwarzaniem danych osobowych także przez podmioty prywatne, których źródłem jest art. 8 ust. 1 EKPC, a więc prawo do prywatności[82].

[76] Wyrok TK z 13 grudnia 2011 r., K 33/08, OTK-A 2011, nr 10, poz. 116.

[77] Wyrok TK z 19 maja 1998 r., U 5/97.

[78] Wyrok ETPC z 4 grudnia 2008 r., 30562/04 i 30566/04, *S. i Marper* przeciwko *Wielkiej Brytanii*, pkt 103.

[79] Wyrok ETPC z 18 listopada 2008 r., 22427/04, *Cemalettin Canlı* przeciwko *Turcji*, pkt 35.

[80] Postanowienie ETPC z 4 czerwca 2013 r., 7841/08 i 57900/12, *Peruzzo i Martens* przeciwko *RFN*, pkt 46.

[81] A.R. Mowbray, *The development...*

[82] Zob. np. wyrok ETPC z 12 listopada 2013 r., 5786/08, *Söderman* przeciwko *Szwecji*, pkt 88–89. Odniesienie do relacji między obowiązkami negatywnymi a pozytywnymi państw szerzej w wyroku ETPC z 5 września 2017 r., 61496/08, *Bărbulescu* przeciwko *Rumunii*, pkt 112.

Skoro Europejski Trybunał Praw Człowieka wyinterpretował z konwencyjnego prawa do prywatności obowiązki związane z ochroną danych osobowych, to *per analogiam* podobna wykładnia może być zastosowana na gruncie polskich przepisów konstytucyjnych. W takim ujęciu możliwe byłoby nawet postulowanie, że art. 51 Konstytucji RP w istocie nie wprowadza nowej treści normatywnej, której nie można wyinterpretować z innych gwarancji konstytucyjnych (w szczególności z art. 47 Konstytucji RP).

Próba zredukowania art. 51 Konstytucji RP wyłącznie do roli prawa akcesoryjnego względem prawa do prywatności musi jednak budzić zastrzeżenia. Wszak norma ta obejmuje również przypadki ujawniania informacji o jednostce pozostające bez związku z jej sferą życia prywatnego. Jednak i w tym zakresie Trybunał Konstytucyjny wskazywał, że taka szeroka wykładnia autonomii informacyjnej, obejmująca każde informacje osobowe, również te indyferentne z punktu widzenia prywatności jednostki – jest zgodna ze „współczesnym rozumieniem sfery życia prywatnego”[83]. Innymi słowy, że nawet ochrona danych niezwiązanych z prywatnością jednostki łączy się ze sferą jej życia prywatnego – i jako taka jest objęta zakresem stosowania art. 47 Konstytucji RP.

W ocenie Trybunału art. 51 Konstytucji RP należy postrzegać jako normę pomagającą wyodrębnić niektóre typu naruszeń ze względu na „częstotliwość, uporczywość i typowość wkraczania w prywatność przez władzę publiczną”[84]. Celem przyjętej redakcji przepisu jest natomiast ułatwienie dostrzeżenia pojawiających się naruszeń i uproszczenie dowodu, że takie wykroczenie nastąpiło.

Rekapitulując dotychczasowe stanowisko Trybunału Konstytucyjnego, Monika Florczak-Wątor podkreśla, że „[a]rtykuł 51 statuuje prawo do ochrony danych osobowych, które jest jednym z przejawów prawa do ochrony prywatności”[85]. Teza ta zatem nie tylko aprobuje pogląd (dominujący również w orzecznictwie Trybunału) o całkowitym podporządkowaniu art. 51 celom art. 47, ale dodatkowo postuluje, że na gruncie norm konstytucyjnych uzasadnione jest twierdzenie o ustanowieniu „prawa do ochrony danych”. I chociaż także Trybunał wskazywał art. 51 jako źródło konstytucyjnego prawa do ochrony danych osobowych[86], to jednocześnie należy pamiętać, że norma ta nie dosyć, że *de facto* nie operuje terminem „dane osobowe” (i nie

[83] Wyrok TK z 12 listopada 2002 r., SK 40/01, OTK-A 2002, nr 6, poz. 81.
[84] Wyrok TK z 20 listopada.2002 r., K 41/02, OTK-A 2002 nr 6, poz. 83.
[85] M. Florczak-Wątor, w: *Konstytucja...*, komentarz do art. 51.
[86] Zob. np. wyrok TK z 25 listopada 2021 r., Kp 2/19, OTK-A 2022, poz. 6.

odwołuje się do siatki pojęciowej związanej z tym pojęciem), to ponadto ustanawia zestaw odrębnych gwarancji, nietworzących jednego, spójnego prawa podstawowego.

Argumenty za brakiem samodzielnego charakteru art. 51 Konstytucji RP można również odnaleźć, badając istotę tego prawa (zestawu praw) – a więc tej nienaruszalnej wiązki uprawnień, których ograniczenie jest niedopuszczalne i to niezależnie od zaistniałych okoliczności. Przyjmując dominujący w nauce pogląd, że art. 51 konkretyzuje gwarancje wynikające z art. 47, oraz podążając za wykładnią Trybunału Konstytucyjnego, pojawia się trudność w ustaleniu istoty konstytucyjnego prawa do ochrony danych osobowych, możliwego do wyznaczenia i niezwiązanego ze sferą życia prywatnego jednostki. W rzeczywistości, chociaż Trybunał wielokrotnie podejmował problematykę zarówno istoty praw podstawowych jako całości[87], jak i poszczególnych gwarancji konstytucyjnych[88], to w jego orzecznictwie brak wykładni dotyczącej *stricte* istoty prawa (praw) zredagowanych w poszczególnych ustępach art. 51 Konstytucji RP.

Rozważania te prowadzą do wniosku, że o ile w modelu unijnym prawo do ochrony danych osobowych co do zasady koncentruje się na zapewnieniu bezpiecznego przetwarzania tych danych, to w ujęciu polskich przepisów konstytucyjnych jest ono ściśle skorelowane z autonomią informacyjną – służąc celom ochrony prywatności jednostki, takim jak kontrola ujawniania i procesu gromadzenia informacji, bez odniesienia do wymagań związanych z ich bezpiecznym i rzetelnym przetwarzaniem[89].

Na tym tle Krzysztof Wygoda zaznaczył jednak, że dostrzegalna w orzecznictwie Trybunału Konstytucyjnego bliska relacja między art. 47 i art. 51 „nie jest do końca tożsama z uznaniem ochrony informacji o osobach wyłącznie za zespół zasad techniczne chroniących prywatność”[90]. W jego ocenie istnieje przestrzeń do uznania ochrony danych za samodzielne prawo podmiotowe, a mianowicie w przypadkach, gdy przetwarzaniu podlegają dane dostępne publicznie. Jak się wydaje, wskazuje on tym samym na ochronną funkcję art. 51 ust. 2 Konstytucji RP w zakresie, w jakim norma ta stoi na

[87] Zob. wyrok TK z 30 września 2008 r., K 44/07, OTK-A 2008, nr 7, poz. 126 i przywołane w nim orzecznictwo.

[88] W kontekście prawa własności zob. np. wyrok TK z 12 stycznia 1999 r., P 2/98, OTK 1999, nr 1, poz. 2.

[89] Trafność tego wniosku potwierdza m.in. analiza orzecznictwa Trybunału Sprawiedliwości UE i polskiego Trybunału Konstytucyjnego wydanego w sprawach dotyczących ochrony danych osobowych pracowników – M. Barański, *Ochrona...*

[90] K. Wygoda, *Prawo...*, s. 50.

przeszkodzie w gromadzeniu przez organy publiczne informacji dostępnych publicznie w sposób naruszający warunek niezbędności w państwie demokratycznym. Warto jednak zauważyć, że i w tym wypadku prawo to *de facto* służy ochronie autonomii informacyjnej jednostki (kontroli sfery jej życia prywatnego), a nie *stricte* zabezpieczeniu procesu przetwarzania danych osobowych.

3.3. Skutki reformy przepisów z 2018 r. dla czytelności standardu konstytucyjnego

Omawiając standard konstytucyjny dotyczący autonomii informacyjnej oraz przetwarzania danych osobowych, nie sposób pominąć wyjaśnienia skutków reformy krajowych przepisów o ochronie danych – będących bezpośrednią konsekwencją przyjęcia przez prawodawcę unijnego w 2016 r. nowego pakietu regulacyjnego, składającego się w szczególności z rozporządzenia 2016/679 oraz dyrektywy 2016/680 (tzw. dyrektywa policyjna)[91].

Obowiązująca wcześniej – przez niemal 30 lat – ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (dalej: u.o.d.o. z 1997 r.), stanowiąca transpozycję dyrektywy 95/46/WE, była aktem prawnym kompleksowo omawiającym prawa i obowiązki związane z przetwarzaniem danych osobowych i to także w dziedzinach znajdujących się poza zakresem stosowania prawa UE[92]. Dlatego też Sąd Najwyższy w swoim orzecznictwie wskazywał na regulacje tej ustawy jako służące realizacji gwarancji wprowadzonych w art. 51 Konstytucji RP[93]. W ten sposób dowodził, że prawo do rzetelnej informacji o gromadzeniu i przetwarzaniu danych (art. 51 ust. 2) oraz prawo do żądania sprostowania oraz usunięcia danych nieprawdziwych

[91] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 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 uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. UE L 119 z 4.05.2016, s. 89, ze zm.

[92] W istocie art. 1 ust. 1 u.o.d.o. z 1997 r. wprowadzał publiczne prawo podmiotowe do ochrony danych osobowych („każdy ma prawo do ochrony dotyczących go danych osobowych"). Obecnie w dziedzinach znajdujących się poza zakresem stosowania prawa UE brak równoważnej regulacji krajowej. Istnieją wszakże przepisy, które jako *lex specialis* służą szczególnej regulacji kwestii ochrony danych. Przykładem jest regulacja wprowadzona w art. 4 ust. 2 ustawy z 6 stycznia 2005 r. o mniejszościach narodowych i etnicznych oraz o języku regionalnym, którą P. Fajgielski opisuje jednak jako superfluum ustawowe z uwagi na treść art. 51 ust. 1 Konstytucji RP. P. Fajgielski, *Ogólne...*, komentarz do ustawy o ochronie danych osobowych, s. 216.

[93] Postanowienie SN z 14 czerwca 2000 r., V CKN 1119/00, OSNC 2002, nr 4, poz. 49.

(art. 51 ust. 4) należy odczytywać w kontekście obowiązującego wówczas art. 26 ust. 1 u.o.d.o. z 1997 r.[94] Prowadziło to do wniosku, że w ocenie sądu gwarancje konstytucyjne winny być konkretyzowane w postaci obowiązku gromadzenia i przetwarzania danych „wyłącznie w oznaczonych i legalnych celach, z dbałością o ich merytoryczną poprawność [...] oraz dostosowanie jej zakresu do celu przetwarzania, a także przechowywane nie dłużej niż jest to niezbędne ze względu na cel przetwarzania"[95].

W ten sposób Sąd Najwyższy powiązał art. 51 Konstytucji RP z podstawowymi zasadami ochrony danych osobowych zdefiniowanymi w prawie UE, tj. zasadą zgodności z prawem, rzetelności i przejrzystości, ograniczonego celu, prawidłowości oraz ograniczenia przechowywania. Jeśli w stanie prawnym obowiązującym do 2018 r. taka wykładnia obowiązujących przepisów była możliwa, to obecnie – wraz z wejściem w życie rozporządzenia 2016/679 oraz nowej ustawy z 10 maja 2018 r. o ochronie danych osobowych[96] – jest już problematyczna. Trudno bowiem uznać, aby rozporządzenie 2016/679 stanowiło regulację ustawową, o której mowa w poszczególnych ustępach art. 51 Konstytucji RP. Abstrahując od sporu dotyczącego hierarchii źródeł prawa, wątpliwość ta wynika także z obserwacji, że w polskim modelu prawnym rozporządzenie 2016/679 jest stosowane wyłącznie do przetwarzania objętego prawem UE – nie obejmuje zatem całości przetwarzania objętego dyspozycją art. 51 Konstytucji RP[97].

W efekcie ocena działalności organu publicznego, który, realizując zadania wyłączone z zakresu stosowania prawa UE, nie przetwarza danych zgodnie z zasadą ograniczonego celu, rzetelności czy przejrzystości, nie może być dokonana na gruncie rozporządzenia 2016/679. Problem ten dostrzegł niedawno Naczelny Sąd Administracyjny, ustalając źródła kompetencji Prezesa Urzędu Ochrony Danych Osobowych do kontrolowania czynności przetwarzania prowadzonych przez Instytut Pamięci Narodowej[98]. Na tym tle wskazał, że uznanie, iż działalność Instytutu znajduje się poza zakresem prawa Unii, prowadzi do wyłączenia jej spod regulacji także rozporządzenia 2016/679. To z kolei prowadziłoby do wniosku, że dane znajdujące się w rejestrach Instytutu pozostają poza jakąkolwiek kontrolą organów właściwych w dziedzinie ochrony danych osobowych, czyniąc gwarancje przewidziane

[94] Dziś jest to art. 5 rozporządzenia 2016/679.

[95] Wyrok SN z 11 lutego 2015 r., I CSK 868/14, www.sn.pl.

[96] Dz.U. z 2018 r. poz. 1000 tekst pierw.; Dz.U. z 2019 r. poz. 1781 tekst jedn.

[97] Należy pamiętać, że taki skutek przyjęcia nowej regulacji był wskazywany już w trakcie procedowania ustawy – zob. np. A. Grzelak, *O przedmiotowym...*

[98] Wyrok NSA z 25 sierpnia 2020 r., I OSK 3325/19, orzeczenia.nsa.gov.pl.

w art. 51 ust. 4 Konstytucji RP nierealizowalnymi. Konstatacja taka wynika z faktu, że w odniesieniu do danych niepełnych lub nieprawdziwych brak byłoby jakiegokolwiek trybu ich weryfikacji. Wskazany problem dotyczy w istocie całości działalności realizowanej przez organy publiczne, która pozostaje poza zakresem stosowania prawa UE. W takim wypadku reforma unijnych przepisów o ochronie danych (a raczej wadliwe dostosowanie krajowego prawodawstwa do zmieniającego się otoczenia prawnego) skutkowała znaczącym obniżeniem standardów ochrony praw zagwarantowanych w art. 51 Konstytucji RP.

Jednak problem ten dotyczy nie tylko przypadków, gdy organy państwa działają poza zakresem stosowania prawa UE. Obok ogólnego rozporządzenia o ochronie danych, drugim kluczowym aktem prawa UE dotyczącym ochrony danych osobowych jest dyrektywa policyjna. Akt ten reguluje kwestie przetwarzania danych przez organy publiczne w dziedzinie prawa karnego. Polski ustawodawca dokonał transpozycji przepisów rozporządzenia 2016/679, wprowadzając ustawę z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[99]. Jednocześnie jednak na podstawie art. 3 pkt 2 wskazanej ustawy wyłączył z jej zakresu stosowania przetwarzanie prowadzone w dziedzinie bezpieczeństwa narodowego, „w tym w ramach realizacji zadań ustawowych Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego". Regulacja ta była szeroko krytykowana już w trakcie prac prawodawczych, prowadziła bowiem do wyłączenia z zakresu stosowania ustawy działalności niektórych organów państwa realizujących typowe funkcje policyjne (np. Centralnego Biura Antykorupcyjnego – w zakresie walki z przestępczością korupcyjną), w efekcie czego przetwarzanie danych przez nie prowadzone znalazło się *de facto* w próżni prawnej. Skutkiem przyjęcia takiego rozwiązania jest kolejna trudność w odniesieniu art. 51 ust. 3 Konstytucji RP do działalności organów publicznych, których działalność została (wadliwie i z naruszeniem prawa UE) wyłączona z zakresu stosowania krajowych przepisów ustawowych implementujących dyrektywę policyjną.

Powyższe obserwacje prowadzą do wniosku, że o ile w przypadku ewolucji unijnego prawodawstwa dostrzec można wyraźną konsekwencję prawodawcy prowadzącą do zbudowania koherentnego modelu regulacyjnego,

[99] Dz.U. z 2019 r. poz. 125 tekst pierw.; Dz.U. z 2023 r. poz. 1206 tekst jedn. ze zm.

o tyle na gruncie przepisów *stricte* krajowych polski prawodawca nie tyle pozostaje bierny, ale nawet podejmuje działania utrudniające wypracowanie czytelnego standardu w zakresie prawa do ochrony danych – a w efekcie nadania konstytucyjnym gwarancjom przewidzianym w art. 51 rzeczywistego znaczenia z perspektywy ochrony praw jednostek.

3.4. Potrzeba i kierunek zmian na przykładzie ClearView AI

Oceniając znaczenie gwarancji ustanowionych w art. 51 Konstytucji RP dla przestrzeni ochrony praw podstawowych, na pierwszy plan należy wysunąć stosunkowo wąski zakres przedmiotowy i podmiotowy przywołanej regulacji, który dodatkowo nie został uzupełniony czytelnymi przepisami podkonstytucyjnymi. W efekcie w znacznej części przypadków wykorzystania nowoczesnych technik przetwarzania danych, granice dopuszczalnej ingerencji wyznaczają nie standardy konstytucyjne, ale normy prawa UE. Co więcej, unijne prawo ochrony danych – z uwagi na jego ponadnarodowy charakter – wydaje się również skuteczniejszym narzędziem oddziaływania na praktyki stosowane przez usługodawców na zglobalizowanym rynku danych.

Ustrojodawca, ustanawiając art. 51 Konstytucji RP, zamierzał wzmocnić ochronę jednostki przede wszystkim przed zagrożeniami wertykalnymi. Abstrahując od kwestii, na ile cel ten został w redakcji przepisu czytelnie i spójnie wyrażony, wydaje się, że w związku z postępującymi przemianami technologicznymi ponownej analizy wymaga nie tyle adekwatność przyjętych środków, ale aktualność motywów uzasadniających ich ustanowienie. Współcześnie coraz trudniej bowiem dokonać jasnego podziału naruszeń ochrony danych względem źródła ich pochodzenia, a więc na zagrożenia o *stricte* horyzontalnym i wertykalnym charakterze.

Odbiorcami nowoczesnych usług cyfrowych są coraz częściej także podmioty publiczne. Co więcej, usługi tego typu mogą być świadczone w obszarach do niedawna zastrzeżonych dla organów państwa – takich jak bezpieczeństwo publiczne czy walka z poważną przestępczością. W efekcie trwanie przy odmiennych standardach wyznaczających zakres ingerencji w autonomię informacyjną w zależności od tożsamości podmiotu zobowiązanego *de facto* osłabia prawa jednostki, zamiast je wzmacniać.

Przykładem może być szeroko komentowany w ostatnich miesiącach *casus* systemu ClearView AI. System ten (czy raczej usługa świadczona w modelu chmury obliczeniowej) oferuje możliwość niemal natychmiastowego identyfikowania osób znajdujących się na wskazanych przez operatora (użytkownika systemu) zdjęciach (nagraniach wideo). ClearView AI

pozwala zatem w czasie rzeczywistym ustalać tożsamość osób, np. zarejestrowanych przez lotniskowy monitoring czy przemieszczających się w przestrzeni publicznej. Przewagę konkurencyjną produktu stanowią jednak nie same algorytmy przetwarzania obrazu i rozpoznawania twarzy (oparte na systemach uczenia maszynowego), ale olbrzymia baza danych zawierająca – według deklaracji producenta – ponad 20 mld zdjęć. Zdjęcia te zostały pozyskane z publicznie dostępnych źródeł (głównie mediów społecznościowych). ClearView AI to zatem doskonały przykład narzędzia służącego zarówno celom komercyjnego profilowania użytkowników, jak i realizacji zadań z obszaru bezpieczeństwa publicznego. W rzeczywistości sama firma wskazuje, że jej głównymi klientami są organy ścigania i służby specjalne[100]. Wiarygodność tej informacji wzmacniają doniesienia o wykorzystaniu systemu przez służby ukraińskie do identyfikacji sprawców zbrodni wojennych dokonanych w trakcie wojny z Rosją[101].

Ponieważ dane, na których bazuje ClearView AI, zostały zgromadzone bez zgody osób zainteresowanych, legalność przetwarzania jest kwestionowana na gruncie prawa UE[102]. W październiku 2022 r. francuski organ ochrony danych (CNIL) jako pierwszy[103] nałożył na producenta systemu wysoką[104] karę finansową za naruszenie praw osób, których dane są przetwarzane – powołując się przy tym na rozszerzony, tzw. terytorialny zakres stosowania unijnego prawa ochrony danych[105]. Kluczowe dla rozstrzygnięcia CNIL było jednak potwierdzenie, że czynności związane z eksploatacją ClearView AI wchodzą w zakres przedmiotowy stosowania rozporządzenia 2016/679, a więc że działania usługodawcy mogą być uznane za przetwarzanie danych osobowych.

100 K. Hill, *The Secretive...*

101 P. Dave, J. Dastin, *Ukraine...*

102 I.N. Rezende, *Facial...*

103 Kolejna decyzja została wydana 13 lipca 2022 r. przez grecki organ ochrony danych – zob. European Data Protection Board, *Hellenic DPA fines Clearview AI 20 million euros*, 20 lipca 2022 r., < https://edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en >, dostęp: 14 grudnia 2022 r. Własną decyzję 26 maja 2022 r. wydał także brytyjski ICO, nakazując ClearView AI usunięcie danych Brytyjczyków oraz nakładając karę administracyjną w wysokości 7,5 mln funtów, < https://ico.org.uk/action-weve-taken/enforcement/clearview-ai-inc-mpn/ >, dostęp: 14 grudnia 2022 r.

104 W rzeczywistości jest to maksymalna kara dopuszczalna na podstawie przepisów rozporządzenia 2016/679 – 20 mln euro.

105 Commission Nationale de l'Informatique et des Libertés, Délibération SAN-2022-019 du 17 octobre 2022, < https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859?isSuggest=true >, dostęp: 14 grudnia 2022 r. (CNIL udostępnił także wersję anglojęzyczną).

Przenosząc powyższe rozważania na grunt polskich przepisów konstytucyjnych, w pierwszej kolejności należy wyjaśnić, czy przetwarzanie realizowane w ramach usług takich jak ClearView AI w ogóle objęte jest zakresem stosowania art. 51 Konstytucji RP. Oczywiście nawet negatywna odpowiedź nie wyklucza możliwości ochrony praw jednostki na podstawie standardu wynikającego z art. 47 Konstytucji RP (ochrona prywatności). Jednak ocena taka może pomóc w ustaleniu, czy art. 51 faktycznie – jak wskazywał Trybunał Konstytucyjny – „ułatwia dostrzeżenie pojawiających się naruszeń" w obszarze autonomii informacyjnej jednostki.

Przykład ClearView AI obrazuje ograniczenia obecnej redakcji art. 51 ust. 1 – w szczególności niepotrzebne zawężenie tej normy wyłącznie do przypadków „ujawniania" informacji przez jednostkę. Przetwarzanie danych publicznie dostępnych (ujawnionych wcześniej i dobrowolnie) z pewnością nie skutkuje naruszeniem zakazu ustanowionego w przywołanej normie. Jednocześnie nie ma wątpliwości, że jednostka, publikując dane w mediach społecznościowych (w szczególności – swoje zdjęcie), nie godziła się na wykorzystanie tych informacji przez prywatny podmiot w prowadzonej przez niego działalności gospodarczej.

Idąc dalej, jeśli wydaje się jasne, że zbudowanie systemu takiego jak ClearView AI (bazującego na masowym gromadzeniu i przetwarzaniu danych osobowych) bezpośrednio przez polskie organy publiczne byłoby trudne do pogodzenia z poszanowaniem standardu wynikającego z art. 51 ust. 2 Konstytucji RP, to ocena ta nie byłaby już tak oczywista w przypadku, gdy organ publiczny do realizacji swoich zadań wykorzystałby tożsamą usługę, ale zbudowaną i utrzymywaną przez podmiot prywatny (np. zagranicznego usługodawcę). W takim stanie faktycznym możliwe byłoby dowodzenie braku wypełnienia warunku „pozyskiwania lub gromadzenia danych", o którym mowa w art. 52 ust. 2 Konstytucji RP – co czyniłoby *de facto* gwarancję wynikającą z tej normy zależną już nie tylko od tożsamości podmiotu zobowiązanego, ale technicznego sposobu przetwarzania danych (który przecież dla podmiotu danych w większości przypadków pozostaje nieznany). Wskazane niejasności nie występowałyby, gdyby hipoteza art. 52 ust. 2 Konstytucji RP odnosiła się ogólnie do „przetwarzania danych", a nie konkretnych, enumeratywnie wskazanych czynności podejmowanych przez zobowiązanego, oraz nie zawężała strony podmiotowej wyłącznie do organów „władzy publicznej" (zamiast tego wiążąc ustanawiane ograniczenie z wykonywaniem zadań publicznych).

Pozostałe prawa i obowiązki, skonkretyzowane w dalszych ustępach art. 51 Konstytucji RP, również wydają się nie tworzyć czytelnego standardu

chroniącego przed nadużyciami związanymi z nadmiarowym przetwarzaniem informacji lub przetwarzaniem ich niezgodnie z wolą jednostki. W szczególności trudno postulować, aby informacje publikowane przez samych użytkowników były nieprawdziwe lub niepełne; z kolei żądanie ich usunięcia ze względu na niezgodność z ustawą napotykają na przeszkodę w postaci braku rzeczonej ustawy (przepisów podkonstytucyjnych – jak wcześniej wskazano – w wielu przypadkach brak). W obecnym stanie prawnym nie sposób nawet wskazać, do kogo żądanie tego typu miałoby być adresowane – czy do podmiotu publicznego korzystającego z ClearView AI czy bezpośrednio do dostawcy usługi czy platformy analitycznej (producenta systemu). Z tego samego powodu w badanym przypadku normą o znaczeniu *de facto* ornamentacyjnym pozostaje art. 51 ust. 5 Konstytucji RP.

Powyższe wątpliwości dotyczące adekwatności zakazów ustanowionych w art. 51 Konstytucji RP do przeciwdziałania nowoczesnym formom nadużyć w obszarze przetwarzania danych można odnieść do wielu współczesnych przypadków tzw. prywatyzacji bezpieczeństwa publicznego, których charakterystycznym elementem jest powierzanie podmiotom prywatnym realizacji zadań wcześniej wykonywanych samodzielnie przez organy publiczne.

4. Podsumowanie

W trzeciej dekadzie XXI w. ochrona danych osobowych coraz częściej zaliczana jest do grupy praw podstawowych o fundamentalnym znaczeniu dla budowy i rozwoju nowoczesnych społeczeństw, opartych na wiedzy i informacji. Jednocześnie z uwagi na stosunkowo krótki czas, jaki upłynął od ustanowienia pierwszych prawnych regulacji ustanawiających podmiotowe prawo jednostki do ochrony danych jej dotyczących, kwestia zarówno charakteru tego prawa, jak i jego zakresu przedmiotowego czy podmiotowego, jest nadal przedmiotem licznych dyskusji.

Nie ma wątpliwości, że autorzy Konstytucji RP trafnie rozpoznali potrzebę objęcia ochroną regulacjami ustawy zasadniczej także przypadków wkraczania w autonomię informacyjną jednostki. Przyjęta redakcja art. 51 stanowiła *novum* nie tylko na tle wcześniejszych regulacji ustrojowych, ale również przepisów konstytucyjnych innych państw europejskich. Odniesienie się do zagadnień dotyczących ochrony danych w odrębnej jednostce redakcyjnej pozwoliło na podkreślenie niektórych praw i obowiązków związanych z gromadzeniem i przetwarzaniem danych osobowych. Ustrojodawca nie zdecydował się jednak na bardziej wyraźne wyodrębnienie prawa do

ochrony danych jako samodzielnego prawa podmiotowego. W tym zakresie nie ustanowił również spójnego, koherentnego prawa podmiotowego, wyznaczającego jasne i czytelne granice stosowania, co byłoby z korzyścią zarówno dla podmiotów uprawnionych, jak i zobowiązanych.

Dwadzieścia pięć lat, jakie upłynęło od przyjęcia obecnej Konstytucji RP, to okres wystarczający, aby zdecydować się na pierwsze podsumowania i rekomendacje. Przedstawiona w niniejszym artykule analiza treści art. 51 na tle unijnego prawa do ochrony danych ma właśnie służyć takiemu celowi – stanowić głos w dyskusji nad potrzebą i zasadnością czytelniejszego wyodrębnienia w krajowych przepisach konstytucyjnych prawa do ochrony danych jako samodzielnego prawa podmiotowego, ukierunkowanego na ochronę jednostek nie tyle przed naruszeniami prywatności, ile skutkami nieprawidłowego przetwarzania danych ich dotyczących.

W czasach głębokiego kryzysu rządów prawa – prowadzącego także do kwestionowania prawidłowości obsadzenia najważniejszych instytucji wymiaru sprawiedliwości, w tym Trybunału Konstytucyjnego[106] i Sądu Najwyższego[107] – dyskusja na temat zasadności wprowadzania zmian ustrojowych, zwłaszcza w obszarze podstawowych praw i wolności, może wydawać się przedwczesna. Tym bardziej że – jak można słusznie argumentować – gdyby Trybunał Konstytucyjny w ostatnich latach skutecznie wypełniał swoją rolę ustrojową, spójna wykładnia orzecznicza mogłaby wyeliminować wiele dostrzeżonych w niniejszym artykule wątpliwości interpretacyjnych.

Niestety, trwający kryzys wokół Trybunału Konstytucyjnego powoduje, że coraz częściej prymat w zakresie wyznaczania standardów ochrony praw jednostek w Polsce pełni obecnie Trybunał Sprawiedliwości UE. Obserwacja ta jest także prawdziwa w dziedzinie ochrony danych osobowych. Dość powiedzieć, że to właśnie Trybunał Sprawiedliwości uchylił przepisy stanowiące podstawę funkcjonowania Centralnego Rejestru Beneficjentów Rzeczywistych Ministerstwa Finansów – i to z powodu nieproporcjonalnej ingerencji w prawo do prywatności i prawo do ochrony danych[108]. Dla porównania w ciągu ostatnich siedmiu lat Trybunał Konstytucyjny rozpoznał łącznie 18 spraw, w których wzorzec kontroli obejmował również przepisy art. 51 Konstytucji RP – przy czym w zdecydowanej większości (11) sprawy

[106] Wyrok ETPC z 7 maja 2021 r., 4907/18, *Xero Flor* przeciwko *Polsce*.

[107] Wyrok ETPC z 3 lutego 2022 r., 1469/20, *Advance Pharma* przeciwko *Polsce*.

[108] Wyrok TSUE z 22 listopada 2022 r., C-37/20 i C-601/20, *WM i Sovim SA* przeciwko *Luxembourg Business Registers*, ECLI:EU:C:2022:912.

te zostały umorzone[109] (w tym postępowania zainicjowane wnioskami Rzecznika Praw Obywatelskich dotyczące zbadania zgodności z Konstytucją RP przepisów ustawy inwigilacyjnej[110], a także ustawy antyterrorystycznej[111]). Ostatni wyrok, w którym Trybunał zajmował się kwestią ingerencji w autonomię informacyjną, został wydany 25 listopada 2021 r. W wyroku tym Trybunał przychylił się do wniosku Prezydenta Rzeczypospolitej i uznał przepisy rozszerzające zakres oświadczeń o stanie majątkowym składanych przez osoby pełniące funkcje publiczne za niezgodne m.in. z art. 51 ust. 2 Konstytucji RP[112]. To znamienne, że w czasie, gdy Trybunał Sprawiedliwości UE swoimi wyrokami chronił społeczeństwo przed nadmierną ingerencją ze strony organów publicznych w sferę prywatności, polski Trybunał Konstytucyjny wydawał orzeczenia, w których *de facto* koncentrował się na ochronie praw przedstawicieli władzy.

Usieciowione społeczeństwo, funkcjonujące na co dzień w cyfrowej gospodarce i korzystające z usług e-administracji, to „nowa rzeczywistość", także dla prawodawców. Ochrona danych to nie chwilowa moda czy przemijający trend, który wkrótce zejdzie z agendy ważnych problemów społecznych. Dlatego dyskusja nad skutecznymi narzędziami, także prawnymi, kształtującymi środowisko regulacyjne w sposób pozwalający realizować cele i aspiracje jednostek, to temat, który warto i trzeba podejmować także (a może – zwłaszcza) w czasach trwającego kryzysu ustrojowego.

Abstract

The article presents arguments for the need to further improve of the Polish constitutional provisions establishing guarantees in the area of personal data protection. To this end, the development and current framework of EU data protection law and the national guarantees of the individual's informational autonomy introduced in the Polish Constitution are presented. Against this background, the author argues that the Polish Constitution, although it provides certain guarantees related to the protection of information concerning an individual, is not in fact a source of a coherent, consistent and independent public subjective right to the protection of personal data. The author considers whether the examined set of constitutional

[109] Statystyki z 14 grudnia 2022 r. wg danych dostępnych w Internetowym Portalu Orzeczeń TK, < https://ipo.trybunal.gov.pl/ >.

[110] Postanowienie TK z 22 marca 2018 r., K 9/16, OTK-A 2018, poz. 21.

[111] Postanowienie TK z 6 czerwca 2018 r., K 35/16, OTK-A 2018, poz. 39.

[112] Wyrok TK z 25 listopada 2021 r., Kp 2/19, OTK-A 2022, poz. 6.

norms can constitute a control model for assessing the permissibility of using many modern (and intrusive) forms of interference with fundamental rights, including those used by public entities – in this regard, he discusses in detail the case of the ClearView AI system. Particular attention is paid to the impact of the recent reform of the sub-constitutional provisions on the protection of personal data on the legibility and effectiveness of constitutional guarantees of the informational autonomy of the individual.

Keywords: protection of personal data, information autonomy, the right to privacy, the essence of fundamental rights.

MARCIN ROJSZCZAK https://orcid.org/0000-0003-2037-4301
Adiunkt na Wydziale Administracji Nauk Społecznych Politechniki Warszawskiej.

Bibliografia

Addo M.K., Grief N., *Does Article 3 of The European Convention on Human Rights Enshrine Absolute Rights?*, „European Journal of International Law" 1998, t. 9, nr 3.

Albrecht J.P., *How the GDPR Will Change the World*, „European Data Protection Law Review" 2016, t. 2, nr 3.

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej*, Warszawa 2012.

Barański M., *Ochrona danych osobowych pracowników w orzecznictwie Trybunału Konstytucyjnego oraz Trybunału Sprawiedliwości*, „Państwo i Prawo" 2022, z. 1.

Battjes H., *In Search of a Fair Balance: The Absolute Character of the Prohibition of* Refoulement *under Article 3 ECHR Reassessed*, „Leiden Journal of International Law" 2009, t. 22, nr 3.

Bosek L., Szydło M., w: *Konstytucja RP*, t. 1, *Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016.

Brkan M., *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, „German Law Journal" 2019, t. 20, nr 6.

Dave P., Dastin J., *Ukraine has started using Clearview AI's facial recognition during war*, Reuters, 14 marca 2022 r., < https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/ >, dostęp: 14 grudnia 2022 r.

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2022.

Florczak-Wątor M., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2019.

Gerards J., *How to improve the necessity test of the European Court of Human Rights*, „International Journal of Constitutional Law" 2013, t. 11, nr 2.

Gerety T., *Redefining Privacy*, „Harvard Civil Rights-Civil Liberties Law Review" 1997, nr 2.

Greenleaf G., *The influence of European data privacy standards outside Europe: implications for globalization of Convention 108*, „International Data Privacy Law" 2012, t. 2, nr 2.

Grzegory T., *Pamięć absolutna czy kontrolowana amnezja – wybrane problemy prawne regulacji „prawa do bycia zapomnianym" w ogólnym rozporządzeniu o ochronie danych (dodatek MoP 20/2016)*, „Monitor Prawniczy" 2016, nr 20.

Grzelak A., *O przedmiotowym zakresie stosowania RODO*, „ABI Expert" 2017, nr 3.

Hill K., *The Secretive Company That Might End Privacy as We Know It*, The New York Times (18.01.2020 r.), < https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html >, dostęp: 14 grudnia 2022 r.

Kokott J., Sobotta C., *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, „International Data Privacy Law" 2013, t. 3, nr 4.

Kopff A., *Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1972, t. 20.

Lenaerts K., *Limits on Limitations: The Essence of Fundamental Rights in the EU*, „German Law Journal" 2019, t. 20, nr 6.

Łachowska K., *Ochrona danych osobowych w prawie polskim i unijnym*, w: *Ochrona danych osobowych w prawie publicznym*, red. M. Jędrzejczak, Warszawa 2021.

Mendrek A., *Pojęcie dokumentu urzędowego – zagadnienia wybrane*, „Polski Proces Cywilny" 2018, nr 3.

Mowbray A.R., *The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights*, Oxford, Portland, OR 2004.

Ohm P., *Broken Promises of Privacy Responding to the Surprising Failure of Anonymization*, „UCLA Law Review" 2009, t. 57.

O'Neill M., *The Issue of Data Protection and Data Security in the (Pre-Lisbon) EU Third Pillar*, „Journal of Contemporary European Research" 2010, t. 6, nr 2.

Polok M., *Bezpieczeństwo danych osobowych*, Warszawa 2008.

Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, „Law, Innovation and Technology" 2018, t. 10, nr 1.

Rauchegger C., *National Constitutional Courts as Guardians of the Charter: A Comparative Appraisal of the German Federal Constitutional Court's* Right to Be Forgotten *Judgments*, „Cambridge Yearbook of European Legal Studies" 2020, t. 22.

Rezende I.N., *Facial recognition in police hands: Assessing the 'Clearview case' from a European perspective*, „New Journal of European Criminal Law" 2020, t. 11, nr 3.

Rustad M.L., Koenig T.H., *Towards a Global Data Privacy Standard*, „Florida Law Review" 2019, t. 71.

Rojszczak M., *Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE*, „Prawo Mediów Elektronicznych" 2017, nr 3.

Rojszczak M., *Definicja i granice prawnej ochrony prywatności w epoce analityki big data*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2019, t. 81, nr 1.

Sakowska-Baryła M., *Konstytucjonalizacja prawa do ochrony danych osobowych w Polsce*, „Przegląd Prawa Konstytucyjnego" 2016, t. 32, nr 4.

Sarnecki P., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. L. Garlicki, M. Zubik, Warszawa 2016.

Siwicki M., *Anonimizacja jako narzędzie służące ochronie danych osobowych*, „Przegląd Sejmowy" 2022, nr 2.

Szafrański B., *Realizacja zadań publicznych a Big Data*, w: *Internet. Publiczne bazy danych i Big Data*, red. G. Szpor, Warszawa 2014.

Tizzano A., *The Role of the ECJ in the Protection of Fundamental Rights*, w: *Continuity and Change in EU Law: Essays in Honour of Sir Francis Jacobs*, red. A. Arnull, P. Eeckhout, T. Tridimas, Oxford 2008.

de Terwangne C., *Council of Europe convention 108+: A modernised international treaty for the protection of personal data*, „Computer Law & Security Review" 2021, t. 40.

Wild M., w: *Konstytucja RP*, t. 1, *Komentarz do art. 1–86*, red. M. Safjan, L. Bosek, Warszawa 2016.

Wróbel A., w: *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, Warszawa 2020.

Wygoda K., *Prawo do ochrony danych osobowych w Konstytucji RP*, w: *Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2022.

Zhao S. i in., *User profiling from their use of smartphone applications: A survey*, „Pervasive and Mobile Computing" 2019, t. 59.