Uniwersytet Łódzki
Wydział Prawa i Administracji
Katedra Prawa Gospodarczego i Handlowego

mgr Magdalena Czaplińska

Problematyka odpowiedzialności cywilnej przedsiębiorcy w związku z przetwarzaniem danych osobowych

rozprawa doktorska przygotowana pod kierunkiem
dr hab. Szymona Byczko prof. UŁ

Łódź, 2023r.

SPIS TREŚCI

Wykaz najczęściej używanych skrótów

Akty prawne

AI ACT – Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie stucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, 21.04. 2021, (COM/2021/206 final)
dyrektywa 95/46/WE – Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 95.281.31 ze zm.)
Dz.U. – Dziennik Ustaw
Dz.Urz. UE L – Dziennik Urzędowy Unii Europejskiej
EKPC – Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. 1993 nr 61 poz. 284)
k.c. – ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2022 r. poz. 1360)
Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
Konwencja nr 108 RE – Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. 2003, nr 3, poz. 25)
k.p.c. – ustawa z 17.11.1964 r. – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805)
k.p.p. – Karta praw podstawowych Unii Europejskiej (wersja skonsolidowana: Dz.Urz. C 202 z 7.06.2016 r., s. 391)
k.z. – rozporządzenie Prezydenta Rzeczypospolitej z 27.10.1933 r. – Kodeks zobowiązań (Dz.U. Nr 82, poz. 598 ze zm.)
p.t. – ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2022 r., poz. 1648 ze zm.)
pr. bank. – ustawa z 29.08.1997 r. – Prawo bankowe (Dz.U. z 2020 r. poz. 1896 ze zm.)
PUODO – Prezes Urzędu Ochrony Danych Osobowych, organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10.05.2018 r. o ochronie danych osobowych w miejsce Generalnego Inspektora Ochrony Danych Osobowych (GIODO).
RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04,2016 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)
SCC – standardowe klauzule umowne (*standard contractual clauses*)
SUODO - ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 723).
TUE – Traktat o Unii Europejskiej z 7.02.1992 r. (wersja skonsolidowana: Dz.Urz. UE z 2010 r. C 83)
TFUE – Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz. Urz. UE z 2016 C 202)
UODO – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U.2019.1781)
u.p.a.p.p. – ustawa o prawach autorskich i prawach pokrewnych z 4.02.1994 r. (Dz.U. z 2019 r. poz. 1231)
Wytyczne 01/2021 EROD – Wytyczne Europejskiej Rady Ochrony Danych 01/2021 w sprawie przykładów zgłoszeń naruszeń ochrony danych

Czasopisma, publikatory

EPS – Europejski Przegląd Sądowy
MoP – Monitor Prawniczy
NP – Nowe Prawo

ONSA – Orzecznictwo Naczelnego Sądu Administracyjnego
ONSAiWSA – Orzecznictwo Naczelnego Sądu Administracyjnego i Wojewódzkich Sądów Administracyjnych
OSNC – Orzecznictwo Sądu Najwyższego. Izba cywilna
OSP – Orzecznictwo Sądów Polskich
OTK – Orzecznictwo Trybunału Konstytucyjnego
OTK-A – Orzecznictwo Trybunału Konstytucyjnego. Zbiór Urzędowy, Seria A
OTK-ZU – Orzecznictwo Trybunału Konstytucyjnego. Zbiór Urzędowy
PiP – Państwo i Prawo
PPH – Przegląd Prawa Handlowego
RPEiS – Ruch Prawniczy, Ekonomiczny i Socjologiczny
ZNUJ PPWI - Prace z Prawa Własności Intelektualnej (ZNUJ PPWI) wydawane są w ramach Zeszytów Naukowych Uniwersytetu Jagiellońskiego

Instytucje

EROD – Europejska Rada Ochrony Danych
NSA – Naczelny Sąd Administracyjny
PE i Rada (UE) – Parlament Europejski i Rada Unii Europejskiej
SA – Sąd Apelacyjny
SN – Sąd Najwyższy
SO – Sąd Okręgowy
SR – Sąd Rejonowy
TK – Trybunał Konstytucyjny
WSA – Wojewódzki Sąd Administracyjny

Wstęp

Zagadnienia wprowadzające

Dane stanowią jedną z cech charakterystycznych gospodarki cyfrowej i określane są mianem nowej waluty. Dawniej wartość ekonomiczna była ściśle powiązana z wytwarzaniem dóbr i usług. Obecnie wartość tę mogą generować dane: osobowe, nieosobowe, prywatne, publiczne, komercyjne, należące do administracji, dobrowolne, wrażliwe i niewrażliwe. Ilość danych nieustannie rośnie. Stanowią one cenne źródło, które może przynieść zysk, jeżeli zostanie odpowiednio zmonetyzowane. Rozwój gospodarki opartej na danych tworzy wiele nowych możliwości. Wykorzystanie danych wpływa na wzrost produktywności przedsiębiorstw, obniżenie kosztów, sprawniejszą transformację cyfrową wszystkich sektorów rynku, a nawet może przyczynić się do rozwiązania problemów natury ekonomicznej czy społecznej. Co więcej, cyfryzacja dokonuje zmiany łańcucha wartości, otwierając możliwości dla nowych obszarów biznesowych[1]. Znaczną część tych wartości stanowią dane osobowe, będące tym segmentem systemu gospodarczego, który wraz z biegiem czasu odgrywa coraz znaczniejszą rolę w działalności przedsiębiorstw. Dzieje się tak dlatego, że funkcjonowanie współczesnych, globalnych gospodarek w znaczący sposób odbiega od gospodarczych doświadczeń poprzednich pokoleń. Wiąże się z to pytaniem, czy wypracowane normy, sposoby zarządzania, dobre praktyki są jeszcze dostosowane do wymogów rynków, które weszły na drogę gwałtownego postępu technologicznego, szerokiego wykorzystania kapitału ludzkiego, globalnej dyfuzji wiedzy[2]. W takich warunkach dla podnoszenia wartości przedsiębiorstwa kluczowe jest zagadnienie roli regulacji prawnych. Podobnie jak własność przemysłowa, której rozwiązania prawne odnośnie ochrony danych, od czasów Konwencji paryskiej[3] były szansą na zdobycie konkurencyjnej pozycji i zwiększenie innowacyjności, tak obecnie ochrona danych osobowych odgrywa istotną rolę w zdobywaniu przewagi rynkowej. W dobie gospodarki opartej na informacji konieczna jest nie tylko analiza sposobu wykorzystywania informacji, w

[1] Program otwierania danych na lata 2012-2027 https://www.gov.pl/web/cyfryzacja/program-otwierania-danych-na-lata-2021-2027.

[2] Małgorzata Niklewicz-Pijaczyńska, *Własność przemysłowa w prawie i ekonomii oraz praktyce gospodarczej* [w:] *Własność w prawie i gospodarce*, red. U. Kalina-Prasznic, Wrocław 2017, s. 98.

[3] Konwencja Związkowa Paryska z dnia 20.03.1883 r. o ochronie własności przemysłowej, przejrzana w Brukseli dnia 14.12.1900 r., w Waszyngtonie 2.06.1911 r. i w Hadze 6.11.1925 r. (ratyfikowana zgodnie z ustawą z dnia 17.03.1931 r.), (Dz.U. 1932 Nr 2, poz. 8).

tym danych osobowych, ale również zidentyfikowanie ryzyka związanego z ich przetwarzaniem oraz wynikających z tego konsekwencji prawnych. Zagadnienia te są istotne zarówno z perspektywy teorii, jak i praktyki prawniczej.

W dotychczasowym dorobku nauki prawa nie ma kompleksowego opracowania o charakterze monografii, dotyczącego cywilnej odpowiedzialności przedsiębiorcy z tytułu przetwarzania danych osobowych. W publikacjach naukowych z zakresu ochrony danych osobowych jest ona uwzględniana jedynie jako jedno z wielu zagadnień szczegółowych. Autorzy: B. Łukańko, R. Strugała, M. Gumularz czy K. Biczysko-Pudełko poprzestają zwykle na omówieniu wybranych problemów, dotyczących odpowiedzialności podmiotów uczestniczących w systemie ochrony danych osobowych lub wybranych narzędzi ochrony danych osobowych.

Regułą jest to, że obowiązki i uprawnienia przypisane uczestnikom systemu ochrony danych osobowych związane są z charakterem przetwarzania danych osobowych, a w przypadku przetwarzania danych osobowych nie w celach osobistych, lecz zarobkowych, reguły poszanowania zasad ochrony danych osobowych przypisane są przedsiębiorcom. Potrzeba analizy odpowiedzialności związanej z przetwarzaniem danych osobowych uzasadniona jest zatem ciągłym rozwojem nowoczesnych technologii i wzrostem świadomości co do wagi danych osobowych. Rozwój nowych technologii wiąże się ze stale narastającą ilością problemów prawnych, których główną przyczyną jest nienadążanie krajowego oraz unijnego prawodawstwa za nowymi wyzwaniami, związanymi także z postępującą globalizacją. Gwałtowny rozwój systemów i sieci informatycznych spowodował, że przetwarzanie danych stało się znacznie tańsze, a tym samym bardziej powszechne. Zarówno przedsiębiorcy, jak i organy publiczne na niespotykaną dotąd skalę wykorzystują do wykonywania powierzonych im zadań zgromadzone dane osobowe, przetwarzane w coraz bardziej zaawansowany sposób. Ponieważ ochrona danych osobowych stanowi jeden z podstawowych aspektów prawa do prywatności, opisane zjawiska niewątpliwie mogą tę prywatność naruszać. W dobie rewolucji informatycznej obywatele zaczynają bowiem tracić możliwość wpływu na procesy zbierania i przechowywania informacji ich dotyczących[4]. Zjawiska te skłaniają do refleksji nad zastosowaniem dotychczasowego dorobku prawa do nowych regulacji, mających wpływ na prywatność i ochronę danych osobowych.

[4] S. Kotecka-Kral, *Sądowe środki ochrony prawnej i jurysdykcja krajowa w zakresie spraw związanych z ochroną danych osobowych na mocy rozporządzenia 2016/679* [w:] *Ars in vita. Ars in iure. Księga Jubileuszowa dedykowana Profesorowi Januszowi Jankowskiemu*, red. A. Barańska, S. Cieślak, Warszawa 2018, s. 829–856.

Niejednokrotnie można mieć wrażenie, że tradycyjne rozwiązania prawne zdają się nie nadążać za potrzebami gospodarki. Jest to jednak twierdzenie z perspektywy prawnej deprecjonujące ich istotę dla rozwoju rynku. Wiele przykładów rozwiązań stosowanych obecnie w prawie cywilnym ma swoją genezę w instytucjach prawa rzymskiego (np. *lex Aquilia)*, co pozwala postawić tezę, że cywilnoprawne konstrukcje ochrony prywatności mogą okazać się wystarczające w obliczu zmian związanych z rozwojem systemów informatycznych oraz zautomatyzowaniem operacji przetwarzania danych.

Problematyka ochrony danych osobowych jest przedmiotem analiz w nauce prawa, zwłaszcza teraz, po wejściu w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych[5] oraz ustawy z dnia 10.05.2018 r. o ochronie danych osobowych[6]. Zagadnienia dotyczące danych osobowych były przedmiotem badań naukowych także w okresie poprzedzającym, gdy podstawowymi aktami normatywnymi regulującymi tę problematykę były: Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[7] oraz ustawa z dnia 29.08.1997 r. o ochronie danych osobowych[8], zwana dalej SUODO. Jak wykazane zostanie w dalszej części pracy dorobek wypracowany na gruncie dyrektywy 95/46 jest w części wykorzystywany obecnie.

Celem RODO jest zwiększenie kontroli osób fizycznych nad ich danymi osobowymi. RODO poszerza zakres niektórych praw uregulowanych dotychczas w dyrektywie 95/46/WE i przyznaje osobom, których dane dotyczą, nowe prawa. RODO określa zasady przetwarzania danych osobowych i nakłada nowe obowiązki na administratorów danych i podmioty przetwarzające, zwiększając ich odpowiedzialność za przetwarzanie[9]. Zgodność z RODO to dynamiczny proces, który wymaga takiego podejścia, aby dopasować systemy, zasady i

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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).
[6] Ustawa z dnia 10.10.2018 r. o ochronie danych osobowych (tekst jedn. Dz.U. z 2019 r., poz. 1781).
[7] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 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).
[8] Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r., poz. 922).
[9] M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 64.

procedury przetwarzania danych do wybranego celu[10]. Tym celem jest zapewnienie obywatelom UE większej kontroli nad danymi osobowymi, przy równoczesnym obarczeniu podmiotów zobowiązanych do stosowania RODO większą odpowiedzialnością, zapisaną w ogólnych zasadach, takich jak przejrzystość i rozliczalność. Aby zrealizować to zadanie, niezbędna jest harmonizacja praktyk i zasad dotyczących gromadzenia danych, które w 27 państwach członkowskich są różne[11].

Pozycja przedsiębiorcy jako podmiotu zobowiązanego wynika z faktu, że RODO dotyczy wyłącznie sfery działalności zarobkowej. Zgodnie z motywem 18 RODO rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową, co oznacza związanie obowiązkami wynikającymi z RODO przedsiębiorców. Poza zakresem zastosowania RODO znajdują się dane nieosobowe, czyli dane elektroniczne inne niż dane osobowe zdefiniowane w przepisach RODO, których zasady przetwarzania określa Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[12]. Przedsiębiorca realizuje obowiązki wynikające z RODO obok przepisów dotyczących prowadzonej przez niego działalności gospodarczej. Jego odpowiedzialność na gruncie RODO kształtuje się zatem niezależnie od tych przepisów, z tym zastrzeżeniem, że przepisy te wpływają na jej zakres wtedy, gdy wykonywanie konkretnych obowiązków prawnych dotyczy przetwarzania danych osobowych. W sytuacji, w której przedmiotem realizacji obowiązku prawnego jest przetwarzanie danych osobowych, sposób wykonania tego obowiązku może bowiem wpływać na ocenę poprawności zastosowania przepisów o ich ochronie. Obowiązki wynikające z RODO muszą być tym samym brane pod uwagę w trakcie wykonywania czynności prawnych z udziałem przedsiębiorców. Współstosowanie przepisów prawnych w tym obszarze może prowadzić do komplikacji natury podmiotowej i przedmiotowej. Nie sposób bowiem jednoznacznie wydzielić tych płaszczyzn, tj. gospodarczej i prawa ochrony danych osobowych, w ramach których funkcjonują przedsiębiorcy, co przekłada na się na złożoność zagadnienia odpowiedzialności cywilnej. Tezę o złożoności

[10] S. Breen, K. Ouazzane, P. Patel, *GDPR: Is your consent valid?*, „Business Information Review" 2020/37(1), pp. 19–24, https://journals-1sagepub-1com 144m4e89l02bc.han3.lib.uni.lodz.pl/doi/full/10.1177/0266382120903254

[11] A. Cool, *Impossible, unknowable, accountable: Dramas and dilemmas of data law Social Studies of Science*, „Social Studies of Science" 2019/49/4, s. 503–530, https://journals-1sagepub-1com-144m4e89l02bc.han3.lib.uni.lodz.pl/doi/full/10.1177/0306312719846557

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz. L 303 z 28.11.2018).

zagadnienia odpowiedzialności cywilnej na gruncie RODO wzmacniają argumenty dotyczące tego, że podmioty zobowiązane na gruncie przepisów o ochronie danych osobowych mogę występować jednocześnie w kilku rolach – nie tylko jako administratorzy, ale także jako współadministratorzy oraz podmioty przetwarzające. Wielość ról po stronie podmiotów zobowiązanych wpływa na problemy praktyczne przy rozgraniczaniu statusów i kompetencji, wynikających ze stosowania przepisów RODO.

Nie bez znaczenia dla omawianego zagadnienia jest fakt, że prawo ochrony danych osobowych przed RODO także korzystało z ochrony prawnej na gruncie regulacji, dotyczących ochrony dóbr osobistych, wizerunku, tajemnicy przedsiębiorstwa, co wiąże się z pojęciem prywatności, wynikającym m.in. z art. 51 Konstytucji RP. Ma to wpływ na obecny stan prawny i będzie szerzej omówione w niniejszej pracy. Ochrona danych jest nierozerwalnie związana z wieloma innymi prawami obywateli – między innymi z tajemnicą korespondencji, wolnością wypowiedzi i zgromadzeń, ochroną osobowości, wolnością zrzeszania się, wolnością przemieszczania się i ochroną mieszkania, co ma znaczenie dla realizacji obowiązków, wynikających z przepisów o ochronie danych, czego dowodzą omawiane w dalszej części pracy orzeczenia sądowe. W ramach wykonywania działalności RODO nakłada na przedsiębiorcę szereg obowiązków. Mają one charakter w części obowiązków wynikających wprost z przepisów prawa, a w części organizacyjny**,** ponieważ w ramach obowiązków wynikających z konieczności zapewnienia zgodności z RODO przedsiębiorca musi zdecydować o wyborze odpowiednich środków organizacyjnych i technicznych, których wdrożenie gwarantować będzie ochronę danych osobowych. Środki te ujęte powinny być w dokumentach wewnętrznych – takich jak np. polityki, a w stosunku do pracowników reguły takie powinny zostać wdrożone w ramach regulaminu pracy lub innych instrukcji, stanowiących element regulacji wewnętrznych pracodawcy, z którymi – zgodnie z art. 104^3 kp[13] – pracownik musi zostać zaznajomiony. Analogicznie jak na gruncie SUODO, w stosunku do dokumentacji obowiązek wdrożenia przez administratora systemu ochrony danych osobowych oznacza nie tylko opublikowanie i zapoznanie osób upoważnionych do przetwarzania danych osobowych z treścią dokumentacji, składającej się na ten system. Wdrożenie powinno obejmować także zobowiązanie osób upoważnionych do przetwarzania danych do stosowania określonych środków organizacyjnych i technicznych – jeżeli to od ich aktywności zależy ich skuteczne stosowanie. Tylko w ten sposób rezultat polegający na stosowaniu środków (opisanych w

[13] Ustawa z dnia 26.06.1974 r. – Kodeks pracy (Dz.U. z 2022 r., poz. 1510 ze zm.).

dokumentacji) może zostać osiągnięty[14].

Regulaminy lub instrukcje wydawane przed przedsiębiorcę w zakresie wdrożenia RODO, które dotyczą wyboru zastosowania odpowiednich środków organizacyjnych i technicznych, mogą odnosić się do wszystkich osób fizycznych, tj. zatrudnionych przez przedsiębiorcę pracowników, osób współpracujących. Poza zakresem kompetencji regulacyjnych przedsiębiorcy znajdują się te obowiązki, których realizacja wynika wprost z przepisów prawa. Na gruncie RODO takim obszarem będą objęte np. żądania dostępowe do danych, których źródłem jest m.in. art. 51 Konstytucji RP stanowiący, że prawo do żądania danych osobowych od osoby wskazanej przepisami, zobowiązujące ją do udzielenia informacji o sobie, będzie skuteczne tylko wtedy, gdy będzie to wynikać z ustawowego uregulowania. Ustawowe umocowanie do żądania danych wyklucza nałożenie takiego obowiązku na osobę w drodze aktów wewnętrznych (np. instrukcji, regulaminów, statutów organizacyjnych, regulaminów i zarządzeń), nawet gdyby były to akty wydawane przez centralne organy administracji państwowej. W literaturze podnosi się również, że źródłem zobowiązania do ujawniania informacji o osobie nie mogą być także akty wewnątrzzakładowe, tj. regulaminy pracy, układy zbiorowe pracy czy – w sposób oczywisty – normy deontologiczne lub normy prawa zwyczajowego[15]. Z powyżej omawianych zagadnień wynika, że podstawa prawna obowiązków dotyczących systemu ochrony danych osobowych nie jest dla uczestników tego systemu jednolita, co ma znaczenie dla problematyki dotyczącej odpowiedzialności. Dodatkowo zastosowanie konkretnych obowiązków prawnych w każdej z możliwych konfiguracji podmiotowych, jako że wszystkie wymienione podmioty – tj. pracownicy, współpracujący, kontrahenci mogą być uczestnikami systemu ochrony danych osobowych, stanowić może samodzielne źródło powstania odpowiedzialności odszkodowawczej przedsiębiorcy. Tym samym zasadne wydaje się dokonanie analizy i omówienie zakresu obowiązków przedsiębiorcy oraz osób, biorących udział w procesie przetwarzania danych i ich konsekwencji prawnych zarówno dla przedsiębiorcy, jak i dla podmiotu danych. Skutki prawne stosowania RODO będą wynikać z roli, jaką przedsiębiorca pełni w przetwarzaniu danych osobowych na gruncie przepisów o ochronie danych osobowych, co w niniejszej pracy zestawione zostanie także z przepisami Kodeksu cywilnego[16] z uwagi na znajdujące się w ustawie o ochronie danych osobowych odesłanie do stosowania jej przepisów.

[14] P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2017.
[15] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 121.
[16] Ustawa z dnia 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2022 r., poz. 1360 ze zm.)

Istotne jest, aby w tym miejscu zasygnalizować, że z perspektywy ponad trzech lat stosowania RODO nie brakuje ocen, iż przepisy dotyczące danych osobowych są skomplikowane i biurokratyczne, ich znaczenie nie zawsze jest oczywiste, a ochrona danych osobowych często niepotrzebnie utrudnia życie codzienne[17]. Kwestią budzącą poważne wątpliwości, jest zakres stosowania RODO, który jest na tyle szeroki, że można pod niego podciągnąć niemal wszystko. Praktycznie każda forma interakcji międzyludzkiej ujawniającej informacje o innych osobach, niezależnie od sposobu ich ujawniania, może podlegać przepisom RODO, kształtującego instytucje prawa, które mogą wywoływać trudności interpretacyjne i być różnie oceniane (np. rozbieżności w orzecznictwie sądowym w zakresie uznania tablic rejestracyjnych za dane osobowe). Z perspektywy czasu, który upłynął od rozpoczęcia obowiązywania RODO i obserwacji praktyki jego stosowania, za istotne uznać należy argumenty zawarte w opinii rzecznika generalnego TSUE Michala Bobeka w sprawie C-245/20, sprowadzające się do stwierdzenia, że albo Trybunał, albo tym bardziej prawodawca Unii mogą być pewnego dnia zmuszeni do ponownego przeanalizowania zakresu RODO. Obecne podejście stopniowo przekształca RODO w jedne z najbardziej *de facto* lekceważonych ram prawnych w prawie Unii. Nie było to intencją prawodawcy. Jest to raczej naturalny produkt uboczny zbyt szerokiego zakresu stosowania RODO, powodujący, że wiele osób nie ma świadomości, że ich działania również podlegają przepisom RODO. A to oznacza, że zakres RODO powinien zostać ograniczony pod względem materialnym[18].

Pogląd ten stanowi przykład wypowiedzi odnoszącej się do problematyki stosowania art. 2 RODO, który formułuje zakres obowiązywania rozporządzenia, stwierdzając, że: „niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych". Cytowany przepis wyodrębnia dwa sposoby przetwarzania danych podlegające przepisom RODO:

1. przetwarzanie w sposób całkowicie lub częściowo zautomatyzowany bez względu na to, czy owo przetwarzanie jest związane z koniecznością umieszczenia danych w zbiorze danych, oraz
2. przetwarzanie inne niż zautomatyzowane, pod warunkiem że dane stanowią część zbioru danych lub mają stanowić część zbioru.

[17] Wykład prof. Niko Härtinga na konferencji Stowarzyszenia Niemieckich Inspektorów Ochrony Danych na temat ochrony danych osobowych, Monachium, 27.10.2021 r.
[18] Opinia rzecznika generalnego TSUE Michala Bobeka w sprawie w sprawie C-245/20.

Oznacza to, że każde przetwarzanie danych – niewyłączone spod obowiązywania RODO przepisem szczególnym lub art. 2 ust. 2 rozporządzenia – całkowicie lub częściowo zautomatyzowane podlegać będzie przepisom rozporządzenia, bez względu na to, czy będzie to przetwarzanie w systemach teleinformatycznych, czy np. wideorejestratorach samochodowych, kamerach zainstalowanych na dronach. W przypadku przetwarzania danych innego niż zautomatyzowane (manualne) ochroną objęte jest przetwarzanie danych w zbiorze danych lub w jego w części. Przy tak określonych warunkach objęcia ochroną kluczowe staje się istnienie zbioru danych osobowych i przyporządkowanie danych do zbioru w danym momencie bądź w przyszłości („mają" one stanowić część zbioru). Nie będą zatem podlegać ochronie dane nieuporządkowane w formie zbioru danych bądź dane pojedyncze, co wynika także z treści motywu 15 preambuły do RODO.

Biorąc pod uwagę rys historyczny prac nad RODO, zakres materialny jego stosowania wydaje się poprzedzony szeroką analizą, ponieważ przesłanki rozpoczęcia prac nad nowym aktem europejskim w zakresie ochrony danych szczegółowo zostały wyliczone w preambule uzasadnienia do projektu RODO. Wśród nich znalazły się: konieczność wzmocnienia i doprecyzowania praw osób, których dane dotyczą oraz obowiązków podmiotów przetwarzających dane, oraz uregulowanie kwestii nieznajdujących odzwierciedlenia w dyrektywie 95/46/WE, a wynikających z szybkiego rozwoju nowych technologii (zwłaszcza Internetu) i postępującej globalizacji, której skutkiem jest wzrost zbierania i wymiany danych osobowych. Ponadto podkreślona została potrzeba ujednolicenia przepisów z zakresu ochrony danych osobowych, gwarantująca większą pewność prawną, spójność i stabilność zasad ochrony, w szczególności w kontekście międzynarodowego przekazywania danych osobowych, stanowiącego istotny element działalności prowadzonej zarówno przez podmioty prywatne, jak i publiczne. Ten drugi argument podnoszony był w szczególności przez podmioty sektora prywatnego, które zwracały uwagę, że zróżnicowanie następuje w sposobie interpretacji przepisów, a związku z tym w zakresie ochrony danych w poszczególnych państwach członkowskich. Dawało to wrażenie rozdrobnienia ochrony danych, które uniemożliwiało swobodny przepływ danych w UE, stanowiło przeszkodę w prowadzeniu działalności gospodarczej, zakłócało konkurencję i utrudniało organom wykonywanie ich obowiązków wynikających z przepisów unijnych, a także powodowało osłabienie ochrony przysługującej osobom fizycznym. Z tego też względu organy unijne zdecydowały się na przyjęcie aktu prawnego gwarantującego we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw i obowiązków administratorów i podmiotów przetwarzających oraz spójność funkcjonowania organów nadzorczych w ramach skutecznej

współpracy tychże organów z różnych państw członkowskich, w tym możliwość wymierzania równoważnych kar[19].

Zagadnienie materialnego ograniczenia stosowania RODO jest jednak dyskutowane od lat. Działania w sprawie postulowanych powyżej ograniczeń mogą wynikać z faktu, że głosy zalecające ostrożniejsze podejście do pojęć danych osobowych i przetwarzania były już wcześniej podnoszone przez Grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołaną na podstawie art. 29 dyrektywy 95/46/WE. W opinii w/w Grupy Roboczej w sprawie pojęcia danych osobowych zauważone zostało, że „sam fakt, iż dana sytuacja może zostać uznana za wiążącą się z «przetwarzaniem danych osobowych» w świetle definicji, nie przesądza o stosowaniu przepisów dyrektywy [95/46], w szczególności przepisów art. 3"[20]. W opinii tej podkreślone zostało, że „nie należy nadmiernie rozszerzać zakresu przepisów dotyczących ochrony danych", a nawet przewidziane zostało, iż „mechaniczne stosowanie wszystkich przepisów dyrektywy" może prowadzić do „zbyt uciążliwych lub nawet absurdalnych rezultatów"[21]. Zdaniem rzecznika generalnego TSUE w sprawie C-245/20 tym, czego należałoby być może wymagać, jest co najmniej modyfikacja lub jakiekolwiek inne przetwarzanie w sensie „wartości dodanej" do danych osobowych, o których mowa, lub „uczciwego korzystania" z tych danych. Ewentualnie lub w związku z tym należałoby położyć większy nacisk na pojęcie zautomatyzowanych sposobów, które wykluczałyby wszelkie inne formy zwykłego ujawnienia informacji za pomocą sposobów niezautomatyzowanych, czy to ustnie, czy też poprzez zwykły wgląd w dokument pisemny[22]. W tym miejscu podkreślenia wymaga, że z uwagi na szerokie pojęcie danych osobowych, o czym będzie mowa w dalszej części pracy, poprzez odniesienie np. do problemu danych numerycznych, tj. tablic rejestracyjnych, konieczne jest objęcie tym zakresem także innych form udostępnienia wykraczające poza dokument pisemny. Dodanie takiego lub jakiegokolwiek innego podobnego kryterium progowego mogłoby być użyteczne dla ponownego ukierunkowania przepisów o ochronie danych na działania, które powinny być w pierwszej kolejności objęte tymi przepisami, przy jednoczesnym pominięciu przypadkowych, incydentalnych lub minimalnych sposobów wykorzystania danych osobowych, które w przeciwnym razie musiałyby zmierzyć się z pełnymi konsekwencjami

[19] E. Kulesza [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,* red. *D.* Dörre-Kolasa, Warszawa 2017.
[20] Opinia Grupy Roboczej art. 29 (01248/07/PL WP 136, 20.06.2007 r., s. 4–5.
[21] Opinia rzecznika generalnego TSUE Michala Bobeka w sprawie w sprawie C-245/20/.
[22] Opinia rzecznika generalnego TSUE Michala Bobeka w sprawie w sprawie C-245/20/.

prawnymi oraz z mocą praw i obowiązków wynikających z RODO[23].

Nie bez znaczenia dla omawianego problemu jest fakt, że w 2020 r. Komisja Europejska przeprowadziła przegląd RODO po dwóch latach jego stosowania. Choć w raporcie wskazała na pewne problemy, to uznała, że za wcześnie jest, by mówić o ewentualnych zmianach i uznała, że RODO wzmacnia pozycję obywatela, zapewniając szereg praw związanych z ochroną danych osobowych oraz tworzy nowy europejski system zarządzania i egzekwowania tych przepisów. W sprawozdaniu stwierdzono, że RODO okazało się elastyczne pod względem wspierania rozwiązań cyfrowych w nieprzewidzianych okolicznościach, takich jak kryzys związany z koronawirusem. Ponadto coraz więcej państw członkowskich dostosowuje wewnętrzne przepisy do ogólnego rozporządzenia o ochronie danych osobowych. Z analiz Komisji Europejskiej wynika również, że przedsiębiorstwa coraz częściej postrzegają dostosowanie organizacji do przepisów o ochronie danych osobowych jako silną przewagę konkurencyjną. RODO daje osobom fizycznym możliwe do egzekwowania prawa, takie jak prawo dostępu do danych, ich sprostowania, usunięcia, prawo do sprzeciwu i prawo do przenoszenia danych. RODO daje osobom fizycznym większą podmiotowość, jeśli chodzi o decydowanie, co dzieje się z ich danymi w związku z transformacją cyfrową[24].

W kontekście omawianych problemów podkreślenia wymaga, że według wyników opublikowanej w czerwcu tego roku ankiety przeprowadzonej przez Agencję Praw Podstawowych Unii Europejskiej, 69 proc. ludności UE w wieku powyżej 16 lat słyszało o RODO, a 71 proc. osób słyszało o swoim krajowym organie ochrony danych[25]. Wynik ankiet na takim poziomie potwierdza tezę, że ochrona danych osobowych staje się znaczącym elementem bieżących stosunków gospodarczych i społecznych. To nie oznacza, że RODO jest aktem, który w ogólnym odbiorze społecznym i gospodarczym standaryzuje wynikające z niego obowiązki, co stanowić może źródło oceny tego aktu, jako aktu sprawiającego trudności w praktycznym zastosowaniu. Praktyka stosowania RODO unaocznia bowiem problemy w interpretacji przepisów na szczeblu krajowym państw członkowskich, czego wyrazem są pytania prejudycjalne kierowane przez sądy do TSUE. Wśród podnoszonych zagadnień problemowych widoczne są zagadnienia związane z realizacją praw osób, których dane dotyczą, czy wykonywaniem funkcji IOD oraz pojęciem szkody i jej przesłanek, które są kluczowe dla niniejszej pracy. Może to prowadzić do wniosku, że być może w przyszłości

[23] Opinia rzecznika generalnego TSUE Michala Bobeka w sprawie w sprawie C-245/20/.

[24] Raport Komisji Europejskiej: https://biz.legalis.pl/rodo-wzmacnia-pozycje-obywateli-i-jest-dostosowane-do-potrzeb-ery-cyfrowej/

[25] Raport Komisji Europejskiej: https://biz.legalis.pl/rodo-wzmacnia-pozycje-obywateli-i-jest-dostosowane-do-potrzeb-ery-cyfrowej/

zakres materialny RODO zostanie ograniczony lub zmodyfikowany, ponieważ profesjonalnym podmiotom trudno jest w praktyce stosować jego przepisy. Dopóki jednak takie działania nie miały miejsca, RODO powinno podlegać ocenie w kształcie, w jakim zostało uchwalone. W związku z zarysowanymi powyżej problemami niniejsza praca doktorska została przygotowana według schematu opisującego podstawowe zagadnienia odpowiedzialności cywilnej, zakres obowiązków poszczególnych uczestników systemu ochrony danych osobowych i ich konsekwencje w obszarze odpowiedzialności na gruncie Kodeksu cywilnego i RODO. Poza przedmiotem badań niniejszej pracy pozostają, z uwagi na obszerność zagadnień prawnych które ich dotyczą, kwestie realizacji praw podmiotów danych oraz odpowiedzialności Inspektora Ochrony Danych.

ROZDZIAŁ I.

Zarys historyczny prawa ochrony danych osobowych

Zarys historyczny prawa ochrony danych osobowych i pojęcie danych osobowych

W polskiej myśli naukowej problematyka danych osobowych podnoszona była już od lat 70. XX wieku w publikacjach A. Mrózek[26] i J. Kosik.[27] Na gruncie prawa cywilnego była w tym czasie analizowana jak dobra osobiste. Powstanie pierwszych regulacji dotyczących prywatności i ochrony danych osobowych było konsekwencją postępującego rozwoju technologii – najpierw fotografii, a następnie postępu w digitalizacji i komputerowym przetwarzaniu informacji. Prawo człowieka do ochrony jego danych osobowych zaczęło się rozwijać wraz z początkiem automatycznego przetwarzania danych. W 1978r. J. Kosik pisał, że żyjemy w czasie drugiej rewolucji przemysłowej, nazywanej informacyjną, bądź ściślej naukowo - techniczną, a informacja stała się dziś, bardziej niż kiedykolwiek w przeszłości, centralnym ogniwem w wielu procesach. Informacja o ludziach i rzeczach, podmiotach i przedmiotach otaczającego świata stanowi potęgę. Kto ma najwięcej informacji, kto może z niej w pełni korzystać, by działać w pożądanych kierunkach, ten ma w ręku narzędzia do podejmowania decyzji w podstawowych sprawach społeczeństwa i jednostki [28]. Według A. Mrózka informacja może być traktowana jako pewna wiedza posiadająca znaczenie dla jakiegoś rozstrzygnięcia (ujęcie ciągnące ku płaszczyźnie pragmatycznej) oraz jako ustalone w drodze konwencji znaczenie wyodrębnionych komunikatów (jest to ujęcie semantyczne)[29].

Wydaje się, że przedstawione wyżej poglądy pomimo upływu czasu nie straciły na znaczeniu. Zwiększa się dostępność nowych technologii, a korzystanie z nich zyskuje na znaczeniu w przestrzeni publicznej i prywatnej[30], co wywiera wpływ na zakres gromadzenia i przetwarzania informacji. Zgodnie ze *Słownikiem języka polskiego* informacja to „to, co powiedziano lub napisano o kimś lub o czymś, także zakomunikowanie czegoś", „dział informacyjny urzędu, instytucji", „dane przetwarzane przez komputer"[31]. Złożoność zagadnienia informacji wiąże się z faktem, że informacje nie tworząc jednolitej kategorii podlegają licznym podziałom. Biorąc pod uwagę ich przedmiot, można wyróżnić m.in. informacje odnoszące się do osób, rzeczy, zjawisk i procesów. Jeśli dotyczą one

[26] A. Mrózek, *Prawno-polityczne konsekwencje wdrożenia ADP w ramach aparatu państwa burżuazyjnego (na przykładzie państw zachodnich)*, Toruń 1978
[27] J. Kosik, *Technika komputerowa w ewidencji ludności a ochrona cywilnoprawna człowieka*, Wrocław 1978.
[28] J. Kosik, *Technika komputerowa...*, s. 9.
[29] A. Mrózek, *Prawno-polityczne konsekwencje...*, s. 25
[30] M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 19.
[31] https://sjp.pwn.pl/sjp/informacja;2466189.html

zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych, są one określane jako „dane osobowe”[32].

Zagadnienie ochrony danych osobowych sięga XIX wieku. W Polsce pierwsze regulacje prawne pojawiły się w latach 70. XX wieku w ustawie z dnia 10.04.1974 r. o ewidencji ludności i dowodach osobistych. Na gruncie prawa międzynarodowego dokumentem, który jako pierwszy odniósł się do tematu ochrony danych osobowych była Rezolucja 34/169 Zgromadzenia Ogólnego ONZ[33]. Dane osobowe ujęte są tam jako dane o życiu prywatnym pozyskiwane przez ograny ścigania. Powszechna definicja danych osobowych po raz pierwszy została sformułowana w Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju z 23.09.1980r. w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami[34]. W dokumencie tym dane osobowe zostały zdefiniowane jako informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Ponadto wymieniono zasady, jakimi należy się kierować podczas przetwarzania danych. Zgodnie z rekomendacją przy przetwarzaniu danych osobowych należy kierować się zasadami: ograniczonego pozyskiwania, adekwatności, ograniczonego użytkowania, celowości, indywidualnego udziału, otwartości i zasadą odpowiedzialności. Rekomendacja OECD nie była jednak dokumentem wiążącym. Pierwszym aktem wiążącym była Konwencja nr 108 Rady Europy podpisana 28.01.1981r. w Strasburgu[35]. Oddziaływała ona jedynie w sferze publiczno-prawnej, nie wywołując skutków prawnych po stronie obywateli państw, które ją ratyfikowały. Zachęcała do wydania odpowiednich przepisów, ukierunkowując prace legislacyjne. Kolejnym dokumentem poruszającym kwestię bezpieczeństwa danych osobowych była Rezolucja 45/95 Zgromadzenia Ogólnego ONZ[36]. Zawierała ona zasady, którymi powinni kierować się prawodawcy krajowi podczas sporządzania aktów prawnych dotyczących ochrony danych osobowych. Do zasad tych zaliczano: zasadę legalności i rzetelności, zasadę celowości, zasadę dokładności, dostępności, niedyskryminacji i zasadę bezpieczeństwa.[37]

Wraz z reformą lizbońską[38] państwa członkowskie zdecydowały się na wzmocnienie gwarancji związanych z prawami podstawowymi, w tym także z ochroną prywatności oraz

[32] M. Błażewski, J. Behr, *Środki prawne ochrony danych osobowych*, Wrocław 2018, s. 20.
[33] Rezolucja 34/169 Zgromadzenia Ogólnego ONZ z 17.12.1979 r.: Kodeks Postępowania Funkcjonariuszy Porządku Prawnego.
[34] Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 23.09.1980 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami
[35] Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. 2003, nr 3, poz. 25).
[36] Rezolucja 45/95 Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych z 26.06.1985r.
[37] P. Jatkiewicz, *Ochrona danych osobowych Teoria i praktyka*, Warszawa 2015, s. 11-14.
[38] Wprowadzona przez: Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, sporządzony w Lizbonie 13.12.2007 r. (Dz.Urz. UE C 306 z 17.12.2007).

danych osobowych, poprzez nadanie Karcie Praw Podstawowych[39] mocy równej traktatom. W rezultacie zarówno prawo do prywatności (art. 7 k.p.p.), jak i ochrona danych osobowych (art. 8 k.p.p.) uzyskały status praw podstawowych w UE. Prawo materialne wynikające z art. 8 ust. 1 i 2 k.p.p. zostało uzupełnione normą wynikającą z art. 8 ust. 3, zgodnie z którą „przestrzeganie tych zasad podlega kontroli niezależnego organu". Jednocześnie, do Traktatu o funkcjonowaniu Unii Europejskiej[40] wprowadzono nowy przepis kompetencyjny, stanowiący podstawę dla działań prawodawczych Unii Europejskiej w budowaniu wspólnej przestrzeni przetwarzania danych. Zgodnie z art. 16 ust. 1 TFUE, każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Przepis art. 16 ust. 2 stanowi podstawę do przyjęcia aktów prawa wtórnego, regulujących zasady dotyczące ochrony prywatności w związku z przetwarzaniem danych osobowych na terenie Unii Europejskiej[41].

Pojęcie danych osobowych po raz pierwszy zdefiniowane zostało w dyrektywie 95/46/WE, w której art. 2 wprowadził do prawa unijnego ich definicję jako wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą). Przez osobę możliwą do zidentyfikowania należy rozumieć osobę, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość.

Także na gruncie prawa polskiego ochronę danych osobowych uznaje się za prawo autonomiczne lub za element (wymiar) prawa do prywatności[42], a prawo do prywatności wiąże się prawem do autonomii informacyjnej jednostki. Ochrona danych osobowych i prywatność jako jednostki jurydyczne współcześnie stanowią instytucje od siebie niezależne, gdyż ochrona danych osobowych stanowi dziś osobną dziedzinę prawa. Prawo do prywatności oraz ochrona danych osobowych i prawo do ochrony danych osobowych nie są tożsamymi przedmiotami ochrony, choć pozostają w bliskim związku przedmiotowym i funkcjonalnym, a ich ścisłe zależności uwidaczniają się zwłaszcza w sprawach, w których odmawia się dostępu do informacji ze względu na „prywatność danych" i możliwość zidentyfikowania osoby, której one dotyczą. Reżim ochrony prawa do prywatności i reżim ochrony danych osobowych są wobec siebie niezależne. Niewątpliwie dochodzi przy tym do wzajemnych relacji i

[39] Karta Praw Podstawowych Unii Europejskiej (wersja skonsolidowana: Dz.Urz. C 202 z 7.06.2016 r., s. 391).
[40] Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz. Urz. UE z 2016 C 202).
[41] M. Rojszczak, *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne* IKAR 2018/4s. 73.
[42] P. Sobczyk, *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze" 2009/9/1, s. 299–317.

oddziaływania tych reżimów, w określonych bowiem sytuacjach faktycznych przetwarzanie danych osobowych może spowodować naruszenie dobra osobistego w postaci prawa do prywatności, albo ochrona prawa do prywatności będzie wymagała sprzeciwienia się wykorzystaniu danych osobowych"[43].

W orzecznictwie używa się co najmniej kilku określeń odnoszących się do prawnej ochrony prywatności. I tak mówi się o: prawie do prywatności, prywatności jako wolności, autonomii informacyjnej jednostki, prywatności informacyjnej oraz prawie do tożsamości informacyjnej, a także prawie do ochrony danych osobowych. Najszerszym pojęciem jest oczywiście prawo do ochrony prywatności, które jest uregulowane w art. 47 Konstytucji RP i zgodnie z poglądami Trybunału Konstytucyjnego obejmuje ochroną wielopoziomową sieć dóbr osobistych. Z kolei autonomia informacyjna jest przez Trybunał Konstytucyjny utożsamiana z regulacją art. 51 Konstytucji RP i rozumiana jako pozostawienie każdej osobie swobody w określeniu sfery dostępności dla innych wiedzy o sobie. Należy przy tym zaznaczyć, że wbrew literalnemu brzmieniu, w tak rozumianej autonomii nie zawiera się jedynie aspekt kontroli nad danymi, ale również ograniczenia dostępu do danych. Prywatność informacyjna jest z kolei identyfikowana jako aspekt dotyczący informacji z art. 47, a także art. 51 Konstytucji RP. Tożsamość informacyjna dotyczy kontroli nad informacjami istotnymi dla odrębności osoby[44].

Pojęcie prywatności jest złożonym zagadnieniem różnie definiowanym w porządkach prawnych, co wynika z ich tradycji, względów społecznych, a także różnic kulturowych. Prawo do prywatności jest zatem wartością korzystającą z ochrony prawnej w Stanach Zjednoczonych. To właśnie tam, jeszcze w XIX wieku, S.D. Warren i L.D. Brandeis w słynnym artykule *The Right to Privacy* przedstawili spójną, doktrynalną próbę opisu tego prawa na poziomie normatywnym. Jednak zakres tej ochrony na poziomie konstytucyjnym jest w USA węższy niż w Europie, chociażby z tego powodu, że Karta Praw Podstawowych nie przewiduje prawa do prywatności, a sama koncepcja jego konstytucyjnej podstawy od samego początku budziła zastrzeżenia, podobnie jak argumenty, których Sąd Najwyższy użył, identyfikując tę podstawę. W konsekwencji „prywatność" w amerykańskim porządku konstytucyjnym ogranicza się do ochrony przed ingerencją (wyłącznie) władzy państwowej, przede wszystkim w sferę życia rodzinnego, w sprawy małżeńskie i życie seksualne człowieka. Nie obejmuje natomiast innych

[43] M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej*, Warszawa 2022, s. 472
[44] K. Łakomiec, *Prawo do ochrony prywatności w kontekście informacji o stanie zdrowia Autoreferat rozprawy doktorskiej, napisanej pod kierunkiem prof. dr. hab. Marka Zubika*, 2018, s. 3.

sfer, w kontekście europejskim kojarzonych z prawem do poszanowania życia prywatnego, w szczególności ochrony godności człowieka[45].

Kontrastem jest podejście do zagadnienia prywatności, prezentowane w Chinach. Jedną z najbardziej popularnych definicji prywatności jest ta, zgodnie z którą prywatność to prawo osoby fizycznej, wolne od publicznej i jakiejkolwiek innej ingerencji w jej sprawy osobiste, odnoszące się jedynie do tej jednostki i informacji na jej temat. Twórcy tej definicji pozycjonują prywatność jako wywodzącą się z równowagi między jednostką a społeczeństwem i pozwalającą jednostce na przeżywanie w spokoju swoich wewnętrznych emocji, ponieważ istnienie prawa do prywatności jest ściśle związane z funkcjonowaniem duchowej sfery życia ludzkiego.

W Indiach prawo do prywatności czy prawo do ochrony danych osobowych nie są w konstytucji osobom pozostającym pod ich jurysdykcją przyznane wprost. W praktyce stosowania prawa, prawo do prywatności pośrednio odczytuje się z art. 19 ust. 1 lit. a oraz art. 21 indyjskiej konstytucji. Z uwagi na fakt, że indyjska konstytucja nie przyznaje wprost prawa do ochrony prywatności bądź autonomii informacyjnej jednostki, już od lat 70. XX w. indyjski Sąd Najwyższy w swoim orzecznictwie sankcjonuje istnienie tego prawa, opierając je na wynikającej z art. 19 wolności słowa i wolności osobistej przyznanej przez art. 21 konstytucji. I tak w 1975 r. Sąd Najwyższy, ponownie rozpoznając kwestię istnienia bądź nieistnienia gwarancji prawa do prywatności w indyjskiej konstytucji, posiłkował się anglosaską koncepcją prawa do prywatności jako prawa do bycia pozostawionemu samemu sobie (*right to be alone)*. Konstytucja Japonii nie odnosi się wprost do ochrony prawa do prywatności bądź ochrony danych osobowych. Dotychczasowe orzecznictwo sądów powszechnych poszukuje tych praw w art. 13 ustawy zasadniczej, który stanowi: „Wszystkich obywateli szanuje się jako jednostki ludzkie. Ich prawa do życia, wolności i dążenia do szczęścia, o ile nie pozostają w sprzeczności z dobrem publicznym, brane są w najwyższym stopniu pod uwagę w działalności ustawodawczej i innych poczynaniach państwa". Już w 1964 r. wskazywano na ochronę prywatności jako prawa wynikającego z konstytucji Japonii, podkreślając, że podanie informacji na temat osoby fizycznej do publicznej wiadomości stanowi naruszenie jej prywatności[46].

[45] J. Skrzydło, *Wolność słowa w orzecznictwie Sądu Najwyższego Stanów Zjednoczonych i Europejskiego Trybunału Praw Człowieka Analiza porównawcza*, Toruń 2013, s. 209

[46] M. Abu Gholeh, D. Kuźnicka-Błaszkowska, *Ochrona danych osobowych w wybranych państwach Azji*, Wrocław 2019, s. 93.

Wracając na grunt europejskiego porządku prawnego w zakresie zagadnienia autonomii informacyjnej warte podkreślenia jest, że po raz pierwszy zasadę tą w swym orzecznictwie sformułował i rozwinął niemiecki Federalny Trybunał Konstytucyjny w orzeczeniu z 15.12.1983 r., 1BvR 209/83[47]. Ustalił on, że „w warunkach nowoczesnego przetwarzania danych", Konstytucja Republiki Federalnej Niemiec chroni jednostkę przed „nieograniczonym gromadzeniem, używaniem i przekazywaniem jej danych osobowych". Konstytucja gwarantuje również „prawo jednostki do zasadniczo samodzielnego stanowienia o ujawnianiu i używaniu jej danych osobowych"[48].

W Rzeczypospolitej Polskiej zagadnieniem tym zajął się Trybunał Konstytucyjny w swoim orzecznictwie[49], wywodząc w nich, że zasada autonomii informacyjnej obejmuje dwa kluczowe elementy, tj.: a) prawo do samodzielnego decydowania o ujawnianiu innym informacji na swój temat oraz b) prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów.

Prawo do prywatności ma wysoką rangę w ramach systemu funkcjonującego w Unii Europejskiej. Jednym z filarów tego systemu jest Karta Praw Podstawowych Unii Europejskiej[50]. Istotne jest przy tym, że zgodnie z art. 6 ust. 1 Traktatu o Unii Europejskiej[51] uznano, że Karta Praw Podstawowych ma taką samą wartość prawną jak Traktaty[52]. Zatem moc prawna postanowień Karty Praw Podstawowych Unii Europejskiej jest równa prawu pierwotnemu Unii Europejskiej[53]. Zgodnie z art. 8 ust. 1 Karty Praw Podstawowych Unii Europejskiej każdy ma prawo do ochrony danych osobowych, które go dotyczą. Przepis ust. 2 tego artykułu precyzuje, że dane muszą być przetwarzane rzetelnie, w określonych celach i jedynie za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Artykuł 8 ust. 1 Europejskiej Konwencji Praw Człowieka[54] statuuje prawo do

[47] orzeczenie Federalnego Trybunału Konstytucyjnego z 15.12.1983 r., 1BvR 209/83

[48] J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych* [w:] *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, Wrocław 2014, s. 154.

[49] Wyrok TK z 24.06.1997 r., sygn. K. 21/96, OTK ZU nr 2/1997, poz. 23; wyrok TK z 11.04.2000 r., sygn. K. 15/98, OTK ZU nr 3/2000, poz. 86; wyrok TK z 19.02.2002 r., sygn. U 3/01, OTK ZU nr 1/A/2002, poz. 3; wyrok TK z 12.11.2002 r., sygn. SK 40/01, OTK ZU nr 6/A/2002, poz. 81; wyrok TK z 20.11.2002 r., sygn. K 41/02, OTK ZU nr 6/A/2002, poz. 83; wyrok TK z 20.06.2005 r., sygn. K 4/04 OTK ZU nr 6/A/2005, poz. 64.

[50] Karta Praw Podstawowych Unii Europejskiej z dnia 12.12.2007 r. (Dz.Urz. UE z 2007 r. C 303, s. 1).

[51] Traktat o Unii Europejskiej z dnia 7.02.1992 r., wersja skonsolidowana (Dz.Urz. UE z 2010 r. C 83 s. 13).

[52] Z tym że w przypadku Polski i Wielkiej Brytanii postanowienie to ulega modyfikacji wynikającej z przyjęcia Protokołu nr 7 w sprawie stosowania Karty Praw Podstawowych Unii Europejskiej do Polski i Zjednoczonego Królestwa (inaczej: protokół brytyjski). Szerzej zob. M. Jabłoński, J. Węgrzyn, J. Rzucidło, *Znaczenie Protokołu nr 7 do Traktatu z Lizbony dla procesów integracyjnych w Unii Europejskiej*, „Przegląd Prawa i Administracji" nr 2011/86, s. 67 i n.

[53] A. Wyrozumska, *Znaczenie prawne zmiany statusu Karty Praw Podstawowych Unii Europejskiej*, „Przegląd Sejmowy" 2008/2(85)/, s. 28.

[54] Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U.1993.61.284).

poszanowania życia prywatnego, a w przepisie ust. 2 zakazuje władzy publicznej ingerowania w to prawo za wyjątkiem przypadków przewidzianych w ustawie i koniecznych w demokratycznym społeczeństwie w sytuacjach wskazanych w Konwencji. Na poziomie krajowym o wadze obu wskazanych praw decydują art. 47 i 51 Konstytucji RP, które chronią odpowiednio prawo do prywatności oraz prawo do ochrony danych osobowych.

W Karcie Praw Podstawowych Unii Europejskiej postanowiono także, że każdy ma prawo dostępu do zebranych danych, które go dotyczą i prawo do spowodowania ich sprostowania. Ustanowiono także, że przestrzeganie tych zasad podlega kontroli niezależnego organu. Nie oznacza to jednak, że społeczność międzynarodowa uznała, iż ochrona danych osobowych nie zasługuje na szczególną uwagę. Pamiętać przecież trzeba, że prawo to swój początek bierze w prawie do prywatności[55].

W tym miejscu należy dodać, że prawo do prywatności jest nieco starsze, gdyż odpowiadało na wcześniejsze zagrożenia prywatności, ochrona danych osobowych powstała później jako odpowiedź na rozwój technologii informatycznych – świadczą o tym już same nazwy przepisów prawa chroniącego dane osobowe. Konwencja nr 108 Rady Europy z 28.1.1981r. w swojej nazwie ma określenie mówiące o związku z automatycznym, tj. komputerowym przetwarzaniem[56]. Jednocześnie podkreślić trzeba, że prawo do prywatności, jako osobna kategoria jurydyczna, ma dość krótką historię. Po raz pierwszy to pojęcie pojawiło się pod koniec XIX wieku w piśmiennictwie amerykańskim. Wcześniej funkcjonowało w języku potocznym i można uznać, że od najwcześniejszego okresu rozwoju prawa było zakorzenione w świadomości człowieka. Według definicji prywatności sformułowanej w polskim piśmiennictwie prawniczym dobrem osobistym w postaci życia prywatnego jest wszystko to, co ze względu na uzasadnione odizolowanie się jednostki od ogółu służy jej do rozwoju fizycznej i psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej.

Trudność w zdefiniowaniu pojęcia „prywatność" wynika również z tego, że jest ono wspólne dla wielu dziedzin i dyscyplin prawa, wśród nich prawa konstytucyjnego, cywilnego (w tym prawa autorskiego i wynalazczego), administracyjnego, karnego. W praktyce analiza tego terminu może być przede wszystkim inspirowana przez orzecznictwo. Orzekając, sądy oceniają, czy określone czyny spowodowały naruszenie sfery prywatności lub też mogły jej zagrażać. Wnioskowanie to opiera się na rozważanych w określonej sytuacji konfliktach wartości. Dlatego autorzy, próbując definiować prawo do prywatności, na ogół wskazują

[55] J. Rzucidło, *Prawo do prywatności...*, s. 158.
[56] L. Kępa, *Ochrona danych osobowych przewodnik dla przedsiębiorców*, Warszawa 2018, s. 4.

rodzaje naruszeń, przed którymi prawo chroni jednostkę[57]. Taki też schemat oceny obowiązków przez pryzmat definiowania naruszeń, dokonywany przez orzecznictwo został przyjęty w dalszej części pracy.

Zauważyć warto, że na gruncie prawa wspólnotowego przez długi czas nie definiowano prawa do informacji oraz prawa jednostki do ochrony jej danych osobowych. Prawo do informacji zostało wyartykułowane w prawie pierwotnym Unii Europejskiej niezależnie od znajdujących się tam gwarancji dotyczących wolności wypowiedzi. Traktaty założycielskie nie zawierały w swej treści zapisów odnoszących się do wolności i praw jednostki. Stan taki doprowadził do ukształtowania się tzw. prawa pretoriańskiego, którego podstawą było oparcie działań organów Unii Europejskiej na standardach wynikających z orzecznictwa Europejskiego Trybunału Praw Człowieka, wydawanych na podstawie Konwencji o ochronie praw człowieka i podstawowych wolności jako aktu prawa międzynarodowego[58].

Historycznie po dyrektywie 95/46/WE zagadnienie danych osobowych kształtowane było przez regulacje omówione poniżej.

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[59]. Głównym celem rozporządzenia jest zapewnienie zarówno efektywnej zgodności z regułami rządzącymi ochroną podstawowych praw i wolności osób fizycznych oraz swobodnego przepływu danych osobowych między Państwami Członkowskimi a instytucjami i organami wspólnotowymi, jak i między instytucjami i organami wspólnotowymi do celów związanych z wykorzystaniem ich kompetencji. Rozporządzenie znajduje zastosowanie do przetwarzania danych osobowych przez wszystkie instytucje i organy wspólnotowe, o ile takie przetwarzanie jest przeprowadzane podczas wykonywania czynności całkowicie lub częściowo podlegających prawu wspólnotowemu. Rozporządzenie reguluje ogólne zasady legalności przetwarzania danych osobowych, prawa osoby, której dane dotyczą, oraz powołuje urząd Europejskiego Rzecznika Ochrony Danych. Następnie przyjęte zostały przez Komisję 25.01.2012 r założenia zmian regulacji, w tym wniosek dotyczący rozporządzenia zawierającego ogólne regulacje w zakresie ochrony danych oraz wniosek dotyczący dyrektywy zawierającej szczególne regulacje

[57] M. Sakowska- Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 26–27.
[58] M. Jabłoński, K. Wygoda, *Dostęp do informacji i jego granice*, Wrocław 2000, s. 101.
[59] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18.12.2000 r.o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz. Urz. L 008, z 12.01.2001).

dotyczące ochrony danych dla sektora odpowiedzialnego za egzekwowanie prawa. W związku z tymi działaniami zaplanowano zastąpienie dyrektywy 95/46/WE rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych, jako aktem, obowiązującym bezpośrednio w krajach członkowskich, bez potrzeby wydawania aktów prawnych wdrażających je do porządku krajowego. Zakładając taką pełną harmonizację prawa materialnego w ramach UE, dopuszczono odrębność w zakresie przetwarzania danych osobowych przez właściwe organy w celu zapobiegania, dochodzenia, wykrywania lub ścigania przestępstw lub wykonywania sankcji karnych i swobodnego przepływu tych danych –uregulowaną dyrektywą[60].

Zwieńczeniem powyższych prac jest RODO i zawarte w nim pojęcie danych osobowych, wprost zdefiniowane w art. 4 pkt 1 RODO jako wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"), przy czym możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Jednocześnie, jak prawodawca unijny argumentuje w motywie 26 preambuły RODO zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych, przy czym spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. W rzeczonym motywie wskazuje się, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Nadto aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji,

[60] B. Konieczna-Drzewiecka, *Inspektor ochrony danych w strukturze i funkcjonowaniu naczelnego organu administracji publicznej*, Warszawa 2019, s. 20-21.

które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować.

Definicja danych osobowych

Po omówieniu zagadnień ogólnych prawa ochrony danych osobowych zasadne jest dokonanie bliższej analizy pojęcia danych osobowych. Zasadniczo RODO, w ślad za dyrektywą 95/46/WE, kwalifikuje jako dane osobowe wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"). W odniesieniu do osoby możliwej do zidentyfikowania RODO modyfikuje katalog kryteriów pozwalających na jej identyfikację, rozszerzając je o znaczniki o charakterze elektronicznym (dane o lokalizacji, identyfikator internetowy). Taki kierunek zmian nie jest przypadkowy – postęp technologiczny oraz związane z nim pojawienie się w obrocie nowych narzędzi umożliwiających identyfikację osoby, której dane dotyczą, wymusił na unijnym prawodawcy aktualizację przykładowych atrybutów identyfikacyjnych. U podstaw regulacji RODO legła przy tym nie tylko postępująca cyfryzacja społeczeństwa, ale także uwarunkowania prawne, w tym m.in. tendencja orzecznicza Trybunału Sprawiedliwości UE czy opiniotwórcza rola podmiotów wyspecjalizowanych w zagadnieniach ochrony danych osobowych. Na gruncie RODO utrzymano zatem prezentowaną i przyjętą w dyrektywie 95/46 koncepcję szerokiej definicji danych osobowych, która ma swoje źródło jeszcze w Konwencji 108. W konsekwencji nie jest możliwe określenie zamkniętego katalogu informacji o danych osobowych. Pozostaje to także w istotnym związku z celami regulacyjnymi RODO, wskazanymi w art. 1 oraz motywach 10, 11, 13 i 14. W definicji z art. 4 pkt 1 RODO wyróżniono trzy kumulatywne przesłanki kwalifikacyjne pojęcia danych osobowych 1) wszelkie informacje, 2) dotyczące osoby fizycznej, 3) zidentyfikowanej lub możliwej do zidentyfikowania. Przesłanki te wymagają kolejnego omówienia.

Termin „wszelkie informacje" należy interpretować w sposób szeroki, oddający perspektywę ochronną przepisów RODO i jego cele. Jak wskazuje Grupa Robocza Art. 29 w opinii 4/2007 wydanej na gruncie analogicznie brzmiącej w tej części definicji danych osobowych w dyrektywie 95/46, dla oceny osobowego wymiaru informacji nie ma znaczenia czy mają one charakter obiektywny czy subiektywny, jak również irrelewantne jest w jaki sposób są utrwalone, w szczególności na jakim nośniku.

Druga przesłanka rozstrzyga o konieczności istnienia relacji pomiędzy określonego rodzaju informacją a osobą fizyczną. Przesłanka ta odgrywa istotną rolę przy ustalaniu zakresu

przedmiotowego pojęcia danych osobowych, szczególnie w odniesieniu do nowych technologii. Informacje muszą bowiem dotyczyć określonej osoby fizycznej, de lege lata – być „o (...) osobie fizycznej" (niem. Personenbeziehbarkeit). Związek ten musi mieć charakter merytoryczny. Jak podkreśla bowiem Grupa Robocza Art. 29 w opinii 4/2007 w sprawie pojęcia danych osobowych: „informacja dotyczy osoby, jeżeli jest ona na temat tej osoby". Musi zatem istnieć związek między informacją a osobą fizyczną, który podlega ocenie przez pryzmat treści, celu lub skutku. Stopień powiązania może jednak być różny w poszczególnych stanach faktycznych. Związek pomiędzy informacją a osobą fizyczną, do której informacja ta się odnosi, może mieć zarówno charakter osobowy, jak i rzeczowy (majątkowy), tj. referujący się do majątku, wykorzystywanych urządzeń itp. Podkreślić należy, że związek ten nie może mieć jednak wyłącznie charakteru statystycznego, ponieważ nie pozwala wtedy na identyfikację[61]. Co istotne, aby stanowić „dane osobowe" informacja nie musi być prawdziwa, ani sprawdzona.

Przepisy dotyczące ochrony danych uwzględniają ewentualność, że informacje nie są prawdziwe i zapewniają osobie, której dotyczą dane, prawo dostępu do informacji i zakwestionowania ich przy pomocy odpowiednich środków. Jest także tak, że w wielu innych przypadkach ustalenie, że dane informacje „dotyczą" pewnej osoby może jednak nie być tak łatwe. W niektórych przypadkach dane przekazują przede wszystkim informacje o przedmiotach, a nie o osobach. Przedmioty te należą zazwyczaj do kogoś, podlegają wpływowi działania pewnych osób lub wywierają na nie pewien wpływ, lub też pozostają w pewnego rodzaju sąsiedztwie fizycznym lub geograficznym w stosunku do osób lub należących do nich przedmiotów. Można wtedy uznać, że informacje dotyczą tych osób lub przedmiotów jedynie pośrednio. Przykładem takiej sytuacji jest wartość danego domu, która stanowi informację o przedmiocie. Przepisy dotyczące ochrony danych nie znajdą zastosowania, jeżeli informacja taka zostanie wykorzystana wyłącznie w celu ilustracji poziomu cen nieruchomości w pewnej dzielnicy. Jednakże w pewnych okolicznościach taka informacja może również zostać uznana za dane osobowe. Dom jest dobrem należącym do pewnego właściciela i jako taki może zostać na przykład uwzględniony przy ustaleniu wysokości zobowiązań podatkowych tej osoby. W tym kontekście informację taką należy niewątpliwie uznać za dane osobowe. Rejestr serwisu samochodu prowadzony przez

[61] D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, MoP 2021/23.

mechanika lub warsztat zawiera informacje o samochodzie, przebiegu, datach przeglądów technicznych, usterkach technicznych i stanie materialnym. Informacje te są powiązane w rejestrze z numerem tablicy rejestracyjnej i numerem silnika, które z kolei mogą zostać powiązane z właścicielem. Jeżeli warsztat powiąże pojazd z jego właścicielem w celu wystawienia faktury, informacje „dotyczą" właściciela lub kierowcy. Jeżeli powiąże się informacje z mechanikiem, który pracował przy samochodzie, w celu ustalenia wydajności jego pracy, informacja ta będzie również „dotyczyła" mechanika[62].

Trzecia przesłanka kwalifikacyjna pojęcia danych osobowych wymaga, aby informacja dotyczyła osoby fizycznej „zidentyfikowanej lub możliwej do zidentyfikowania". Wiążą się z tym różne zagadnienia. Ogólnie rzecz biorąc, można uważać osobę fizyczną za „zidentyfikowaną", jeśli w grupie osób można ją odróżnić od wszystkich pozostałych członków grupy. Osoba fizyczna jest też „możliwa do zidentyfikowania", jeżeli, mimo że nie została jeszcze zidentyfikowana, taka identyfikacja jest możliwa (na co wskazuje słowo „możliwa"). Ta druga możliwość jest więc w praktyce zasadniczym warunkiem przesądzającym o tym, czy informacje odpowiadają kryteriom trzeciego składnika. Identyfikacji dokonuje się zazwyczaj dzięki poszczególnym informacjom, które można nazwać „czynnikami identyfikującymi" i które wiążą się w sposób szczególny i bliski z daną osobą. Przykładem mogą być cechy wyglądu zewnętrznego osoby, takie jak wzrost, kolor włosów, ubranie, itp., lub pewne cechy tej osoby niedostrzegalne w pierwszej chwili, takie jak zawód, stanowisko, nazwisko[63].
Oznacza to, że możliwość identyfikacji i zasięg pojęcia identyfikacji w kontekście relacji do osoby fizycznej jest najbardziej problematyczną w zastosowaniu i budzącą potencjalnie najwięcej sporów przesłanką definicji pojęcia danych osobowych[64].

Na przestrzeni kilku ostatnich lat stosowania RODO ujawnił się szereg wątpliwości i rozbieżności co do kwalifikowania określonych informacji jako danych osobowych. Choć ideą RODO było zapewnienie jednolitości w stosowaniu przepisów o ochronie danych osobowych, to zróżnicowany katalog czynników spowodował, że w praktycznym wymiarze widoczny jest niejednolity sposób podchodzenia do kwalifikowania poszczególnych informacji jako danych osobowych[65]. Nie budzi wątpliwości, że danymi osobowymi będą takie informacje jak: imię, nazwisko, PESEL czy numer dokumentu identyfikującego daną osobę, jak np. dowód tożsamości czy paszport, lub zazwyczaj adres. Problematyczną kwestią natomiast są takie

[62] Opinia Grupy Roboczej Art. 29 nr 4/2007.
[63] Opinia Grupy Roboczej Art. 29 nr 4/2007.
[64] D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych*...
[65] D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych*...

informacje jak adres IP komputera i adres poczty elektronicznej. Nie ulega wątpliwości, że ocena, czy dana informacja stanowi dane osobowe, musi być dokonywana w konkretnych przypadkach, z uwzględnieniem ich specyfiki.

Przykładem na zobrazowanie tej tezy może być fakt, że na tle przepisów dyrektywy 95/46/WE TSUE uznał, że danymi osobowymi są m.in. nazwisko osoby w połączeniu z jej numerem telefonu lub informacjami dotyczącymi jej warunków pracy czy sposobu spędzania wolnego czasu oraz informacja, że osoba na skutek doznanego urazu stopy korzystała ze zwolnienia lekarskiego (sprawa C-101/01). W/w orzeczenie dotyczyło B. Lindqvist, która była pracownikiem najemnym jako sprzątaczka oraz pełniła funkcję katechetki w parafii Alseda (Szwecja). B. Lindqvist uczęszczała na kurs informatyczny, w ramach którego miała w szczególności stworzyć stronę domową w Internecie. Pod koniec 1998 r. utworzyła ona w domu, na swoim osobistym komputerze, strony internetowe mające ułatwić uzyskanie potrzebnych informacji parafianom przygotowującym się do bierzmowania. Na jej wniosek administrator strony Kościoła Szwecji utworzył linki pomiędzy utworzonymi przez nią stronami i stroną Kościoła. Utworzone przez nią strony zawierały informacje na temat jej osoby oraz na temat osiemnastu jej kolegów z parafii, obejmujące całe brzmienie ich nazwisk lub w niektórych przypadkach tylko ich imiona. Ponadto B. Lindqvist z pewną dozą humoru opisała funkcje pełnione przez jej kolegów oraz sposób spędzania przez nich wolnego czasu. W kilku przypadkach zamieściła informacje o ich sytuacji rodzinnej, numer telefonu i inne dane. Dodatkowo wskazała, że jedna z jej koleżanek doznała urazu stopy i w związku z tym przebywała na zwolnieniu lekarskim w niepełnym wymiarze. B. Lindqvist nie poinformowała tych osób o istnieniu rzeczonych stron, ani nie uzyskała uprzednio ich zgody na opublikowanie danych, ani też nie zgłosiła swoich działań do Datainspektion (instytucji publicznej zajmującej się ochroną danych przekazywanych drogą informatyczną). Wyżej opisany stan faktyczny stał się podstawą sformułowania przez sąd krajowy pytania czy operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków, np. numeru telefonu lub informacji dotyczących ich warunków pracy i sposobów spędzania wolnego czasu, stanowi „przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany" w rozumieniu art. 3 ust. 1 dyrektywy 95/46. Na tak postawione zagadnienie TSUE odpowiedział twierdząco, uznając że danymi osobowymi są informacje, takie jak te, które były umieszczane przez B. Lindqvist[66].

[66] Wyrok Trybunału z 6.11.2003 r. numer sprawy = C-101/01 https://curia.europa.eu/juris/document/document.jsf;jsessionid=F27690A268783F62CDAECF275D795D60?text=&docid=48382&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=828974

W innym orzeczeniu TSUE uznał za dane osobowe nazwiska osób i ich roczne dochody. Wyrok w tej sprawie został wydany na skutek pytania prawnego dotyczącego tego, czy przepisy o ochronie danych osobowych, należy interpretować w ten sposób, że stoją na przeszkodzie regulacji krajowej nakładającej na organy państwowe obowiązek gromadzenia i komunikowania danych na temat dochodów do celów publikacji nazwisk i dochodów pracowników (połączone sprawy C-465/00, C-138/01 i C-139/01)[67]. W sprawie sporu pomiędzy Tietosuojavaltuutettu (inspektorem ochrony danych osobowych) a Tietosuojalautakunta (komisją ds. ochrony danych) w przedmiocie działań związanych z przetwarzaniem danych osobowych dokonywanych przez spółki Satakunnan Markkinapörssi Oy i Satamedia Oy TSUE uznał za dane osobowe dane dotyczące dochodów z działalności zarobkowej i kapitału, a także majątku osoby fizycznej (sprawa C-73/07)[68]. Rozstrzygnięcie tej sprawy zapadło w stanie faktycznym, w którym w/w firmy pobierały od instytucji publicznych jawne dane dotyczące dochodów oraz opodatkowania 1,2 mln fińskich obywateli, by następnie używać ich w celach marketingowych. W innej sprawie Trybunał uznał, że zbiory władz publicznych obejmujące dane osobowe, które zawierają jedynie materiał informacyjny już upowszechniony przez media, należą do zakresu zastosowania dyrektywy, dlatego imię i nazwisko uznane zostało za dane osobowe obok daty i miejsca urodzenia, płci, narodowości, stanu cywilnego, historii wjazdów i opuszczania terytorium danego państwa, statusu pobytu, szczegółów dotyczących kolejnych paszportów, meldunków, oznaczenia urzędów i służb przekazujących dane (wyrok wydany w sprawie C-524/06)[69].

Problem kwalifikowania informacji jako dane osobowe widoczny był także w literaturze i doktrynie sprzed RODO, w których w/w problematyka była podnoszona wielokrotnie, czego wyrazem jest poniższa analiza poglądów i stanowisk.

Zgodnie z poglądami piśmiennictwa informacje o osobie poczętej mają charakter danych osobowych. W przypadku ich ochrony będą traktowane jako dane dotyczące matki, czy jej stanu zdrowia, aż do momentu narodzin[70]. Za dane osobowe można uważać sam numer PESEL lub imię i nazwisko, danymi osobowymi nie będzie natomiast sam numer domu czy nazwa ulicy. Regułą w kwalifikowaniu informacji jako danych osobowych jest to, że w pewnych okolicznościach pewne dane będą danymi osobowymi, a w innych nie. Zagadnienie

[67] Wyrok Trybunału z dnia 20.05.2003 r. https://curia.europa.eu/juris/document/document.jsf?text=&docid=48330&pageIndex=0&doclang=PL&mode=lst&dir=&occ=first&part=1&cid=832537

[68] Zob. https://archiwum.giodo.gov.pl/pl/1520141/4558

[69] M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, str. 66

[70] M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej*, Warszawa 2022, str. 353

to podniesione zostało w wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z 3.03.2009r.[71], który dotyczył decyzji Generalnego Inspektora Ochrony Danych Osobowych, uznającej iż danymi osobowymi nie są imię i nazwisko w zestawieniu ze szkołą i klasą, umieszczone pod zdjęciem sprzed wielu lat. Organ nadzoru w tym przypadku uznał, że identyfikacja skarżącego nie jest możliwa bez nadmiernych kosztów i czasu. W uzasadnieniu decyzji stwierdził, iż dostęp do danych jest ograniczony do grupy osób zarejestrowanych na portalu Nasza Klasa, co skutkuje tym, że prawa skarżącego nie zostały naruszone. Zdaniem Sądu w tej sprawie o tym, czy mamy do czynienia z danymi osobowymi, decydują nie tylko wiadomości dotyczące aktualnej sytuacji osoby fizycznej, ale także informacje odnoszące się do tego, co robiła i kim była w przeszłości. Wojewódzki Sąd Administracyjny zważył, że „zgodnie z treścią art. 6 ust. 2 SUODO o tym, czy mamy do czynienia z danymi osobowymi, decydują nie tylko wiadomości dotyczące aktualnej sytuacji osoby fizycznej, ale także informacje odnoszące się do tego, co robiła i kim była w przeszłości. Oznacza to, że również takie dane podlegają ochronie przewidzianej w ustawie o ochronie danych osobowych. Może się zdarzyć, że w pewnych okolicznościach pewne dane będą danymi osobowymi, a w innych nie. Zgodnie z orzeczeniem WSA z 8.06.2017r. o tym, czy określona informacja ma charakter danych osobowych, czy też nie, decyduje jej przydatność do ustalenia tożsamości osoby, której ta informacja dotyczy. Jeżeli komunikat można powiązać z konkretną osobą fizyczną, wówczas jego treść należy uznać za dane osobowe[72]. Tożsamość oznacza cechy, które stanowią o tym, kim dana osoba jest. Na tak rozumianą tożsamość składa się nie tylko to, kim się jest obecnie, ale także to, kim się było, a nawet zamierzenia na przyszłość, wszystko to powoduje, że dana osoba różni się od innej[73]. W innym wyroku WSA stwierdził, że pojęcie "dane osobowe" na gruncie prawa polskiego obejmuje wszelkie informacje dotyczące osoby fizycznej, jeśli możliwe jest określenie jej tożsamości i zidentyfikowanie. Dane osobowe to zespół wiadomości (komunikatów) o konkretnym człowieku na tyle zintegrowany, że pozwala na jego zindywidualizowanie. Obejmuje co najmniej informacje niezbędne do identyfikacji (imię, nazwisko, miejsce zamieszkania), jednakże do tego się nie ogranicza, bowiem mieszczą się w nim również dalsze informacje, wzmacniające stopień identyfikacji[74].

Danymi osobowymi nie są dane osób zmarłych[75]. Pojęciem osoby fizycznej w prawie określa się człowieka uczestniczącego w stosunkach prawnych, który posiada tzw. zdolność

[71] Wyrok w sprawie o sygn. akt II SA/Wa 1495/08.
[72] M. Krawczyk, *Ochrona danych w Internecie* [w:] *Współczesne wyzwania cyfryzacji*, s.187.
[73] Wyrok WSA w Warszawie z 3.03.2009 r., sygn. akt II SA/Wa 1495/08.
[74] Wyrok WSA w Warszawie z 8.06.2017 r., sygn. akt II SA/Wa 1414/16.
[75] P. Jatkiewicz, *Ochrona danych osobowych. Teoria i praktyka*, Warszawa 2015, s. 25

prawną – może być podmiotem praw i obowiązków. Zgodnie z utrwalonym w orzecznictwie i doktrynie poglądem, zdolność prawna osoby fizycznej ustaje w chwili jej śmierci, tylko do tego czasu trwają i podlegają ochronie wszystkie osobiste prawa jednostki[76]. Zmarły nie może być podmiotem praw i obowiązków w stosunkach prawnych, nie może być zatem uznany za osobę fizyczną. W opinii organu doradczego – Grupy Roboczej ds. ochrony danych powołanej na mocy Artykułu 29[77] zwrócono również uwagę, że administrator może nie być w stanie stwierdzić, czy osoba, której dane dotyczą, nadal żyje, a nawet jeżeli ustalenie tego jest możliwe, informacje o osobach nieżyjących można przetwarzać bez rozróżnienia według takich samych procedur, co informacje o osobach żyjących. W praktyce administratorowi będzie zwykle łatwiej przetworzyć dane o osobach nieżyjących w sposób wymagany przez przepisy o ochronie danych osobowych niż podzielić dane na dwie osobne kategorie. Trzeba jednak zauważyć, że w szczególnych przypadkach dane osób zmarłych mogą jednocześnie dotyczyć osób żyjących – taki charakter będą miały na przykład informacje o chorobach genetycznych przekazywanych z rodzica na dziecko. W takim przypadku dane osobowe dotyczące zmarłego rodzica mogą pośrednio (jako dane dotyczące żyjącego dziecka) zostać objęte przepisami o ochronie danych osobowych[78]. Dane anonimowe, np. zebrane do celów statystycznych, również nie są danymi osobowymi[79]. Adres e-mail, jeśli zawiera w nazwie imię i nazwisko i np. nazwę pracodawcy, również będzie stanowił dane osobowe, jeśli pozwoli na identyfikację konkretnej osoby.

Problematyczna sytuacja może zaistnieć w przypadku nicku, którym użytkownik posługuje się w Internecie. Większość administratorów traktuje nicki tak, jakby były danymi osobowymi. Może się, bowiem zdarzyć sytuacja, w której użytkownik sam opublikuje swoje dane osobowe pod swoim nickiem[80]. Problem kwalifikowania nicku jako informacji prawnie chronionej podniesiony został w sprawie zakończonej wyrokiem SN z 11.03.2008 r.[81] Stan faktyczny tej sprawy dotyczył użycia w wypowiedziach pracownika portalu sprzedażowego - serwisu aukcyjnego sformułowań przypisujących jego użytkownikowi nieuczciwość, kłamstwa, interesowność i prywatę. Istotą sporu w tej sprawie była ocena działań portalu w kontekście tego, czy komentarze formułowane w następstwie zawieszenia konta użytkownika o treści krytykującej styl wypowiedzi pod adresem innych użytkowników i administratorów,

[76] Wyrok SN z 17.07.1997 r., sygn. akt III CKN 149/97, OSP 2000/4/63
[77] Opinia Grupy Roboczej Art. 29 nr 4/2007 w sprawie pojęcia danych osobowych.
[78] N. Zawadzka, https://portalodo.com/ochrona-danych-osobowych-osob-zmarlych/
[79] A. Boboli, M. Borkiewicz, K. Koszewicz, G. Leśniewski, *Ochrona danych osobowych w dziale IT*, Wrocław 2017, s. 39.
[80] M. Brzozowska, *Ochrona danych osobowych w sieci*, Wrocław 2012, s. 36
[81] Wyrok SN z 11.03.2008r , sygn. akt II CSK 539/07

zarzucającej zniechęcanie użytkowników do wygłaszania własnych poglądów, nieuczciwość i prywatę – przedkładanie własnych interesów nad interesy innych podmiotów, mogły naruszać jego dobre imię. Sąd Okręgowy, mając na uwadze okoliczności faktyczne niniejszej sprawy, uznał powództwo powoda o ochronę dóbr osobistych za uzasadnione w świetle przesłanek wynikających z art. 23 k.c. i 24 k.c. w związku z art. 448 k.c. Sąd Okręgowy w tej sprawie stwierdził, że dobre imię jest chronione na wielu polach aktywności życiowej człowieka i nie można co do zasady wyłączyć takiej ochrony w przypadku działalności danej osoby w środowisku internetowym. Zwrócił uwagę na fakt, że uwarunkowania społeczne zmieniają się, obrót internetowy zyskuje na znaczeniu i stale zwiększają się możliwości jego wykorzystania. Dzięki Internetowi można nie tylko korzystać z interaktywności mediów, zbierać informacje, korespondować, wymieniać poglądy z wieloma osobami, regulować zobowiązania, ale i uczestniczyć w obrocie handlowym. Niektóre z tych form aktywności internetowej wiążą się z korzystaniem z nazwy użytkownika, która zastępuje wtedy nazwisko lub nazwę danego podmiotu. Sytuacja ta – zdaniem Sądu - może wiązać się z budowaniem „image" danego podmiotu (choćby dzięki systemowi komentarzy w serwisie internetowym) natomiast wypowiedzi, które przypisują podmiotowi posługującemu się określoną nazwą użytkownika zachowania nieuczciwe, czy niegodziwe godzą w dobre imię osoby występującej pod określoną nazwą. W ocenie Sądu, nazwa użytkownika może mieć znaczenie zbliżone do pseudonimu, którym dana osoba posługuje się np. w działalności artystycznej. To podobieństwo skłania do przyznania ochrony nazwie użytkownika zbliżonej do tej, którą ma zagwarantowany w prawie polskim pseudonim. W konsekwencji Sąd Okręgowy stwierdził, że nie znajduje argumentów aby odmówić ochrony dobrego imienia osoby posługującej się nazwą użytkownika w Internecie. Dobre imię stanowi zewnętrzny wymiar czci, musi być rozumiane szeroko i może być powiązane z używaną w obrocie nazwą użytkownika. Zdaniem Sądu Okręgowego, takie spojrzenie na nazwę użytkownika odpowiada duchowi czasu, pozwala skorzystać z otwartej formuły dóbr osobistych przyjętej w polskim ustawodawstwie, dostosowując ją do szybko następujących zmian społecznych związanych z postępem techniki. Sąd Okręgowy wyraził też pogląd, że w miarę zwiększania się ilości usług świadczonych internetowo może okazać się, że znaczenie nazwy użytkownika będzie dla poszczególnych osób równie ważne jak nazwisko. Sąd Apelacyjny nie podzielił poglądów Sądu pierwszej instancji, że nazwa użytkownika serwisu internetowego jest dobrem osobistym osoby fizycznej podlegającym ochronie na podstawie art. 24 k.c. Sąd wyjaśnił, że nazwa użytkownika inaczej login, to słowo stosowane do określenia identyfikatora używanego w systemach komputerowych. Login jest ciągiem znaków przypisanych użytkownikowi bądź programowi. Zdaniem Sądu, nazwa użytkownika

łączy się jedynie z faktem przydzielenia powodowi konta w serwisie aukcyjnym ma charakter techniczny – służy do indywidualizacji operacji (składanie ofert, sprzedaż, kupno itp.). Sąd podkreślił również, że nazwa użytkownika nie wiąże się z osobowością człowieka, nie wyraża wartości uznanych powszechnie w społeczeństwie, a w konsekwencji nie może zostać uznana za dobro osobiste w rozumieniu przepisu art. 23 i następnych kodeksu cywilnego. Wyrok Sądu Apelacyjnego został poddany kontroli instancyjnej, w wyniku której SN zajął odmienne stanowisko i stwierdził, że nie można podzielić poglądu Sądu Odwoławczego, że nazwa użytkownika serwisu aukcyjnego nie podlega ochronie prawnej. W uzasadnieniu wyroku SN podniósł, że nazwa użytkownika, którą posługuje się osoba fizyczna korzystająca z serwisu aukcyjnego pełni różne funkcje. Po pierwsze, utworzenie nazwy użytkownika jest niezbędne do rejestracji w serwisie i uzyskania własnego konta, w konsekwencji do uczestniczenia w aukcjach zarówno jako nabywca jak i sprzedawca. Po drugie nazwa umożliwia użytkownikowi zalogowanie się do serwisu. W procesie logowania użytkownik podaje parę identyfikatorów, tj. nazwę i hasło. Dopiero po prawidłowym wprowadzeniu identyfikatorów użytkownik uzyskuje dostęp do serwisu. Po trzecie nazwa identyfikuje daną osobę fizyczną w środowisku internetowym, w tym konkretnym wypadku w środowisku osób korzystających z usług serwisu sprzedażowego. Dana osoba fizyczna jest rozpoznawana jako użytkownik posługujący się konkretną nazwą. Nie można zgodzić się ze stanowiskiem Sądu Apelacyjnego, że nazwa użytkownika ma wyłącznie charakter techniczny i służy do indywidualizacji operacji. Przeciwnie, nazwa indywidualizuje osobą, która korzysta z serwisu aukcyjnego, składa ofertę, jest stroną konkretnej umowy sprzedaży, wystawia lub otrzymuje komentarz określonej treści, prowadzi korespondencję z innymi użytkownikami. Niekiedy już samo wzięcie udziału w aukcji przez użytkownika posługującego się konkretną nazwą może stanowić źródło informacji dla pozostałych uczestników, którzy wiedzą, że dany użytkownik zwykle bierze udział w aukcjach danego typu, licytuje tylko do pewnej kwoty, tylko w określone dni, w określony sposób, nie konkuruje z użytkownikami posługującymi się określonymi nazwami, że użytkownik ten jest rzetelny, sprawnie i bezzwłocznie przeprowadza transakcje, itp. Z pewnością zatem można powiedzieć, że nazwa użytkownika identyfikuje konkretną osobę fizyczną. Przenosząc te rozważania na grunt ochrony danych osobowych, nick jest informacją, która może identyfikować osobę.

Działalność w Internecie jako aktywność objęta w stosunku do pewnej kategorii informacji ochroną na gruncie regulacji dotyczących danych osobowych wybrzmiała także w orzeczeniu Wojewódzkiego Sądu Administracyjnego w Warszawie, tj. w wyroku z 7.10.2011 r., w którym Sąd stwierdził, że zamiar wytoczenia powództwa autorowi obraźliwego wpisu w

Internecie nie wystarczy, by od administratora żądać wydania danych osobowych użytkownika, który podpisał się nickiem. W przywołanej sprawie administrator odmówił udostępnienia danych osobowych użytkownika, który znieważył w Internecie członka zarządu spółki, powołując się na tajemnicę telekomunikacyjną. Wojewódzki Sąd Administracyjny w Warszawie przyznał rację administratorowi, argumentując swoje stanowisko tym, iż sam zamiar wytoczenia powództwa nie jest wystarczającą przesłanką do udostępnienia danych osobowych. Zdaniem sądu zamiar taki trzeba uprawdopodobnić, wstępując na drogę sądową, składając pozew lub prywatny akt oskarżenia[82].

Kwestia oceny informacji w kategoriach uznania jej za dane osobowe jest podstawowym zagadnieniem dla rozważanego problemu odpowiedzialności. Uznanie informacji za mającej cechy danych osobowych warunkuje dokonywanie analizy, czy określone działania z ich udziałem mają podstawy prawne, a ich skutkiem nie jest naruszenia obowiązującego prawa. Kwalifikowanie konkretnych informacji jako danych osobowych nie jest jednak w praktyce jednoznaczne. W pierwszej kolejności zagadnienie to ilustruje to analiza numeru IP jako danych osobowych Co prawda sam adres IP komputera nie wystarcza do wskazania osoby, która z niego korzystała, ale w zestawieniu z innymi informacjami pozwala przypuszczać, że jej tożsamość można ustalić.

Omawianie zagadnienia identyfikalności poprzez adres IP (ang. *Internet Protocol Address*) rozpocząć należy od wskazania, że adres IP jest to liczba nadawana interfejsowi, grupie interfejsów (ang. *broadcast, multicast*), bądź całej sieci komputerowej opartej na protokole IP, służąca identyfikacji elementów warstwy trzeciej modelu OSI – w obrębie sieci oraz poza nią (tzw. adres publiczny). Adres IP nie jest „numerem rejestracyjnym" komputera – nie identyfikuje jednoznacznie fizycznego urządzenia – może się dowolnie zmieniać (np. przy każdym wejściu do sieci Internetu) jak również kilka urządzeń może dzielić jeden publiczny adres IP. Ustalenie prawdziwego adresu IP użytkownika, do którego następowała transmisja w danym czasie jest możliwe dla systemu/sieci odpornej na przypadki tzw. IP spoofingu – na podstawie historycznych zapisów systemowych[83]. Każde urządzenie (komputer) w sieci IP musi mieć przyporządkowany adres IP. W ramach jednej podsieci adres IP musi być unikalny dla każdego urządzenia. Adres ten służy do identyfikacji urządzenia w sieci. Dzięki temu unikalnemu numerowi komputer może być rozpoznawany przez inne komputery w sieci. Można w przybliżeniu określić adres IP np. serwera, pod który podłączony jest komputer oraz operatora i drogę jaką pokonuje np. pakiet danych wysłanych pod wskazany adres. Adres IP

[82] Wyrok WSA w Warszawie z 7.10.2011r. sygn.akt II SA/Wa 364/11.
[83] Wikipedia, wolna encyklopedia, hasło: adres IP.

nie występuje samodzielnie. Zazwyczaj odnoszą się do niego inne informacje, które stwarzają realną możliwość identyfikacji osoby korzystającej z sieci.

„Możliwość identyfikacji", o której mowa w definicji danych osobowych, dokonywana jest w doktrynie i piśmiennictwie przez pryzmat sporu do tego, czy należy oceniać ją:

- subiektywnie, tj. z uwzględnieniem tylko tych sposobów identyfikacji, do jakich dostęp ma aktualny administrator danych, czy też
- obiektywnie – tj. z uwzględnieniem wszystkich potencjalnych sposobów identyfikacji, jakie są dostępne (także dla podmiotów trzecich).

W opinii 4/2007 z 2007r. Grupa robocza uznała adresy IP za dane dotyczące osoby możliwej do zidentyfikowania. Grupa ta stwierdziła, że „dostawcy dostępu do Internetu i administratorzy sieci lokalnych mogą, używając sposobów, jakimi można się posłużyć, zidentyfikować użytkowników Internetu, którym przydzielili adresy IP, ponieważ systematycznie „rejestrują" oni w pliku datę, godzinę, czas trwania i dynamiczne adresy IP przydzielone użytkownikom Internetu. To samo można powiedzieć o dostawcach usług internetowych prowadzących rejestr na serwerze http. W takich przypadkach można niewątpliwie mówić o danych osobowych. Zwłaszcza w przypadkach, gdy przetwarzanie adresów IP ma na celu zidentyfikowanie użytkowników komputera (na przykład przez posiadaczy praw autorskich w celu ścigania użytkowników za pogwałcenie praw autorskich), administrator przewiduje, że „sposoby, jakimi można się posłużyć" w celu zidentyfikowania osoby mogą się stać dostępne, na przykład w drodze sądowej (w przeciwnym razie gromadzenie danych nie miałoby sensu), i że w związku z tym informacje te należy uważać za dane osobowe. Szczególny przypadek stanowią niektóre rodzaje adresów IP, które w pewnych okolicznościach nie pozwalają na zidentyfikowanie użytkownika z różnych względów technicznych i organizacyjnych. Przykładem mogą być adresy IP przypisane do komputera w kawiarni internetowej, gdzie identyfikacja użytkownika nie jest wymagana. Można by twierdzić, że dane dotyczące użycia komputera X w pewnym przedziale czasowym nie pozwalają na zidentyfikowanie osoby „przy użyciu sposobów, jakimi można się posłużyć", i że w związku z tym nie stanowią one danych osobowych. Jednakże należy odnotować, że dostawcy usług internetowych nie wiedzą najczęściej, czy dany adres IP pozwala na zidentyfikowanie, i że w związku z tym przetwarzają oni dane związane z takim adresem IP w taki sam sposób, jak informacje związane z adresami IP użytkowników zarejestrowanych i możliwych do zidentyfikowania. Dlatego też poza przypadkiem, gdy dostawca usług internetowych może stwierdzić z całkowitą pewnością, że dane dotyczą użytkowników niemożliwych do

zidentyfikowania, musi on ze względów bezpieczeństwa traktować wszystkie informacje związane z adresem IP jako dane osobowe[84].

Na gruncie polskim w sprawie numerów IP WSA wypowiadał się w wyroku z 3.02.2010 r., pod rządami starej ustawy o ochronie danych osobowych, według której za osobę możliwą do zidentyfikowania uważa się osobę, której tożsamość można określić bezpośrednio lub pośrednio. Użyty przez ustawodawcę w art. 6 ust. 2 SUODO przysłówek "pośrednio" powoduje, iż identyfikacja osoby może nastąpić również na podstawie zestawienia różnych informacji pozwalających określić jej tożsamość. Taka sytuacja zaistniała w rozpoznawanej sprawie. Z akt sprawy wynikało bowiem, iż uczestnik postępowania posiadał informacje o dacie logowania, pseudonimach osób dokonujących tej czynności i treści dokonanych wpisów. W ocenie Sądu, powyższe informacje, zestawione z numerami IP umożliwiały jednoznaczne określenie tożsamości osób, które naruszyły dobra osobiste uczestnika postępowania. Zdaniem Sądu w tej sprawie dane osobowe obejmują wszelkie informacje dotyczące osoby fizycznej, o ile możliwe jest zidentyfikowanie tej osoby. Zgodnie z powyższym orzeczeniem adres IP stanowi dane osobowe, gdy jest na stałe przypisany do określonego urządzenia, użytkowanego przez określony podmiot. Ta zależność powoduje, iż w określonych sytuacjach istnieje możliwość identyfikacji tego podmiotu, a taka sytuacja miała miejsce w rozpoznawanej sprawie. W ocenie Sądu identyfikacja tej osoby nie musi być związana z nadmiernymi kosztami, czasem lub działaniami[85].

W wyroku wydanym 19.10.2016 r. w sprawie C-582/14, tj przed rozpoczęciem stosowania RODO Trybunał Sprawiedliwości Unii Europejskiej orzekł, że adresy IP mogą być danymi osobowymi. W stanie faktycznym rozpoznawanym w tej sprawie rząd niemiecki postulował przyjęcie teorii subiektywnej i podnosił, że adresy IP zbierane („logowane") przez strony rządowe nie są danymi osobowymi, ponieważ na ich podstawie administrator strony internetowej nie może samodzielnie ustalić nazwiska czy też adresu właściciela określonego adresu IP. Takie dane są zwykle w wyłącznym posiadaniu dostawcy usługi dostępu do Internetu (ISP), a administrator strony internetowej nie ma do nich dostępu. Trybunał przychylił się pośrednio do teorii subiektywnej, stwierdził jednak, że prawo niemieckie prawdopodobnie umożliwia administratorowi strony internetowej – w szczególności w przypadku ataku hakerskiego – zwrócenie się do odpowiednich organów, które mogą nakazać dostawcy dostępu do Internetu ujawnienie tożsamości właściciela danego adresu IP. Jednocześnie, zgodnie z

[84] Grupa robocza Art. 29, opinia nr 4/2007.
[85] Wyrok WSA w Warszawie z 3.02.2010 r., sygn. akt II SA/Wa 1598/09, I OSK 1079/10; J. Barta, R. Markiewicz, *Ochrona danych osobowych – komentarz*, Kraków 2002, s. 315.

motywem 26 dyrektywy 95/46/WE, przy ustalaniu, czy istnieje „możliwość identyfikacji", należy brać pod uwagę „wszystkie środki, których podjęcie przez administratora lub jakąkolwiek osobę trzecią jest – racjonalnie rzecz biorąc – prawdopodobne"). Jeśli istnieją środki, których zastosowanie przez administratora w celu identyfikacji osoby kryjącej się za danym adresem IP jest racjonalnie prawdopodobne, adresy IP należy – zdaniem Trybunału – uznać za dane osobowe[86]. Trybunał rozstrzygnął zatem, że dynamiczny adres IP stanowi wobec dostawcy usług medialnych dane osobowe, w sytuacji gdy dostawca ten dysponuje środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu. W ocenie Trybunału nie miałoby to miejsca w przypadku, gdyby identyfikacja osoby, której dane dotyczą, była zakazana prawem lub niewykonalna w praktyce. Za P. Litwińskim należy powtórzyć, że stanowiska Trybunału, wyrażonego w powyższym wyroku na tle dyrektywy 95/4625 „nie można automatycznie przenosić na stan prawny istniejący na gruncie rozporządzenia ogólnego. Definicja danych osobowych wynikająca z art. 4 pkt 1 rozporządzenia zawiera bowiem nowy element, nieznany dyrektywie – element uzasadnionego prawdopodobieństwa"[87].

O złożoności zagadnień faktycznych i prawnych, związanych z IP świadczy przyjmująca inną argumentację wydana w aktualnym stanie prawnym decyzja Prezesa UODO z 2021 r. (poddana kontroli instancyjnej przed WSA w sprawie II SA/Wa 3993/21), która stwierdza m.in., że informacją dotyczącą osoby jest zarówno informacja odnosząca się do niej wprost, jak i taka, która odnosi się bezpośrednio do przedmiotów czy urządzeń, ale poprzez możliwość powiązania tych przedmiotów czy urządzeń z określoną osobą pośrednio stanowi informację także o niej samej. Adres IP jest unikatowym numerem przyporządkowanym urządzeniom sieci komputerowych. Jest zatem informacją dotyczącą komputera, a nie konkretnej osoby fizycznej, zwłaszcza wtedy gdy możliwe jest współużyczenie jednego adresu IP przez wielu użytkowników w ramach sieci lokalnej. Tam, gdzie adres IP jest na dłuższy okres lub na stałe przypisany do konkretnego urządzenia, a urządzenie to przypisane jest konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową, jest to bowiem informacja umożliwiająca identyfikację konkretnej osoby fizycznej[88]. W związku z powyższym, w ocenie Prezesa UODO zarówno adres IP, jak również ID plików cookies, z

[86] Wyrok TSUE z 19.10.2016 r. w sprawie C-582/14.
[87] E. Kuczkowska, Glosa aprobująca do wyroku WSA w Warszawie z 13.04.2021 r., sygn. akt II SA/WA 1898/20
[88] Wyrok NSA z 19.05.2011 r., sygn. akt I OSK 1079/10.

uwagi na uzasadnione prawdopodobieństwo zidentyfikowania w powiązaniu z tymi danymi, stanowią dane osobowe.

Analizowana powyżej decyzja Prezesa UODO bez wątpienia odnosi się do jednej z bardziej paradoksalnych kwestii współczesnego przetwarzania danych osobowych za pośrednictwem stron internetowych. Z jednej strony bowiem bez plików cookies z tychże stron sprawnie dla użytkownika korzystać się właściwie nie da, z drugiej strony powracającą jest kwestia tego, z jakich plików cookies korzystanie jest rzeczywiście niezbędne, a na jakie ich użycie nieodzowna jest zgoda. Ponadto niezwykle istotne jest to, jak ta zgoda jest wyrażana i czy faktycznie współczesna praktyka niekończących się treści zgód i oświadczeń, które użytkownicy „odklikują" dość mechanicznie (bywa, ze bez żadnej refleksji) w istocie zapewnia im samodecydowanie i autonomię informacyjną. Praktyka stosowania plików cookies wciąż nie doczekała się jednoznacznej regulacji. Trudno dziś mówić o przejrzystych unormowaniach w tym względzie, tym bardziej doniosła okazuje się praktyka orzecznicza organów nadzorczych. Niestety wciąż mamy tu do czynienia z dwoma reżimami prawnymi, gdzie niezwykle trudno sensownie połączyć praktykę wynikającą z zastosowania przepisów Prawa telekomunikacyjnego oraz prawa unijnego, gdzie jeszcze czekamy na rozporządzenie ePrivacy, a już musimy stosować się do reżimów RODO. Nie ma wątpliwości, że użytkownik strony internetowej musi być poinformowany o tym, że dana witryna korzysta z plików cookie, a dopiero po uzyskaniu takiej informacji, powinien wyrazić zgodę na ich zastosowanie. Informacja o instalowaniu plików cookie ma być przekazana zanim zaczną one działać, sporne jednak być może, czy na tym etapie mamy do czynienia z danymi osobowymi, a przynajmniej czy za każdym razem tak można kwalifikować informacje o użytkowniku, skoro – jak wynika z ustaleń organu w innych decyzjach - adres IP może nie być danymi osobowymi[89].

W ustawie o ochronie danych osobowych z 1997 r., tj. sprzed RODO art. 6 ust. 3 stanowił, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Natomiast na gruncie RODO czynnikami, które należy brać pod uwagę przy identyfikowaniu danej osoby są: koszt i czas potrzebne do zidentyfikowania osoby oraz technologia dostępna w momencie przetwarzania danych. O postępie technologicznym stanowi motyw 26 preambuły do RODO, w którym unijny legislator określił, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane. To

[89] M. Sakowska-Baryła https://www.prawo.pl/biznes/wazny-wyrok-wsa-nie-kazde-cookies-jest-dana-osobowa,512328.html

zatem, czy dana informacja stanowi dane osobowe, czy jednak nimi nie jest, uzależnione jest od konkretnych okoliczności stanu faktycznego – od tego, kto informacją dysponuje oraz z jakimi danymi może ją zestawić. Informacja, która po połączeniu jej z innymi informacjami pozwoli na identyfikację osoby fizycznej, ma status danych osobowych.

Podsumowując zagadnienie IP, stwierdzić należy, że RODO nie rozstrzyga, czy same identyfikatory internetowe, takie jak adresy IP, czy identyfikatory plików cookies powinny zawsze być traktowane jako dane osobowe, czy jako jeden z czynników („śladów"), które mogą pozwolić na identyfikację osoby fizycznej. W motywie 30 RODO stwierdza się bowiem, że ich wykorzystanie może skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób. W art. 4 pkt 1 RODO stanowi zaś, że możliwa do zidentyfikowania osoba fizyczna, to taka którą można bezpośrednio lub pośrednio zidentyfikować w szczególności na podstawie identyfikatora internetowego. Test możliwości identyfikacji osoby fizycznej przewidziano w motywie 26 RODO, który wskazuje, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, o których była już mowa, tj. takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny

W świetle powyższego nie ma podstaw, by uznać, że adres IP – niezależnie od tego, czy jest adresem stałym (statycznym), czy zmiennym (dynamicznym) oraz niezależnie od tego, kto jest jego dysponentem i jakie istnieją możliwości wykorzystania go w celu identyfikacji osoby fizycznej, należy zawsze traktować jako daną osobową.

O problemach interpretacyjnych dotyczących zagadnienia subiektywnych i obiektywnych możliwości technicznych identyfikacji osoby poprzez zestawienie informacji o niej stanowią także nasze inne krajowe rozstrzygnięcia sądowe. Przykładem ilustrującym tą problematykę jest spór sądowy, dotyczący innych niż IP informacji i sposobu zakwalifikowania ich jako danych dotyczących użytkownika i danych dotyczących transmisji, który powstał w stanie faktycznym związanym z udzieleniem informacji przez przedsiębiorcę telekomunikacyjnego nie bezpośrednio abonentce – stronie umowy oświadczenie usług

telekomunikacyjnych, ale wykonującemu z jej numeru telefonu połączenie rozmówcy, powołującemu się na udzieloną w tym zakresie zgodę abonentki. Istotą tej spawy stało się rozstrzygnięcie zasadności zarzutu związanego z naruszeniem przez operatora sieci komórkowej obowiązku zachowania tajemnicy telekomunikacyjnej i konieczność oceny, czy doszło do ujawnienia danych dotyczących użytkownika w postaci nazwy usługi abonamentowej. Sąd I instancji przyjął w tej sprawie, że nazwa usługi abonamentowej może w sposób pośredni identyfikować osobę, ponieważ identyfikacja użytkownika jest możliwa poprzez zespolenie nazwy usługi abonamentowej i pozostałych danych udzielanych osobie dzwoniącej, jak data transmisji danych internetowych, czas transmisji, ich ilość. Połączenie wszystkich uzyskanych parametrów może doprowadzić do uzyskania wiedzy na temat numeru telefonicznego, a przez to do identyfikacji osoby, która jest właścicielem tego numeru. W ocenie Sądu informacja o nazwie usługi abonamentowej pozwala więc na zidentyfikowanie w sposób pośredni osoby fizycznej, przez co stanowi dane dotyczące użytkownika podlegające ochronie. Nie ma znaczenia zdaniem Sądu I instancji, czy uzyskujący dane ma możliwości techniczne ich „powiązania" z określoną osobą. W ocenie Sądu Apelacyjnego Sąd I instancji wadliwie zakwalifikował informację o nazwie usługi abonamentowej jako daną dotyczącą użytkownika. Sąd odwoławczy nie podzielił poglądu Sądu I instancji, że informacje obejmujące nazwę usługi abonamentowej, datę transmisji danych internetowych, ich ilość i czas transmisji, pozwalają osobie trzeciej na zidentyfikowanie w sposób pośredni innej osoby fizycznej. Zidentyfikowanie osoby na podstawie powyższych informacji wymagałoby bowiem nadmiernych kosztów, czasu i działań. Zajmując stanowisko w przedmiocie skargi kasacyjnej w tej sprawie, Sąd Najwyższy stwierdził, że Sąd Apelacyjny nie wyjaśnił jednak, które dane miał na myśli, ani nie podał argumentacji prowadzącej do takiej konkluzji. Brak powyższych ustaleń i ocen uniemożliwiał dokonanie kontroli kasacyjnej zaskarżonego wyroku, tym bardziej, że sposób zakwalifikowania ujawnionych przez powoda informacji jako danych dotyczących użytkownika lub danych transmisyjnych, był między stronami sporny. Z uzasadnienia objętego skargą kasacyjną wyroku nie wynika także, czy Sąd odwoławczy jako dane dotyczące użytkownika postrzegał wyłącznie nazwę usługi abonamentowej, co do której wyraził stanowisko, że nie stanowiła „danej osobowej", czy też do kategorii tej zaliczył także inne informacje wskazane w uzasadnieniu decyzji Prezesa UKE z 27.12.2012 r., co do których się nie wypowiedział. Niejasne też było, czy ze sformułowania „zakres ujawnionych danych winien być ograniczony jedynie do danych transmisyjnych" miałoby wynikać, że wszystkie ujawnione dane, poza nazwą usługi abonamentowej, zaliczył do tej kategorii, czy też uznał, że ujawniono jedynie dane zaliczone do danych transmisyjnych w uzasadnieniu decyzji, a więc:

informację o ilości przesłanych w określonym dniu danych i godzinach nawiązywania połączeń oraz informację o braku połączeń z Internetem w danym dniu i nawiązywaniu w tym dniu połączeń z numerami komórkowymi. Sąd Najwyższy wskazał, że ponownie rozpoznając sprawę, Sąd odwoławczy powinien dokonać oceny prawnej, czy i które z ujawnionych przez powoda informacji stanowią przedmiot tajemnicy telekomunikacyjnej, a w szczególności, czy poszczególne informacje można zaliczyć do kategorii „danych dotyczących użytkownika" lub „danych transmisyjnych"[90]. Zarówno pod rządami starych przepisów jak i zgodnie z RODO informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań, czyli a contrario informacje, które bez nadzwyczajnego wysiłku, bez nieproporcjonalnie dużych nakładów dają się „powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, również zasługują na zaliczenie ich do kategorii danych osobowych. W omawianej sprawie identyfikacja użytkownika była możliwa poprzez zespolenie nazwy usługi abonamentowej i pozostałych danych udzielanych osobie dzwoniącej, takich jak data transmisji danych internetowych, czas transmisji, ich ilość. Połączenie wszystkich uzyskanych parametrów mogło doprowadzić do uzyskania wiedzy na temat numeru telefonicznego, a przez to do identyfikacji osoby, która jest właścicielem tego numeru. Nie miało zatem znaczenia zdaniem Sądu I instancji, czy uzyskujący dane ma możliwości techniczne ich „powiązania" z określoną osobą. Nie tyle subiektywnie, ile obiektywnie oceniane możliwości techniczne są w takim przypadku wyznacznikiem statusu uzyskanych danych. W analizowanym orzeczeniu Sąd podjął się także oceny zakresu przedmiotowego tajemnicy telekomunikacyjnej, określonej w art. 159 ust. 1 p.t.[91], uznając, że dane dotyczące użytkownika mogą odnosić się do strony umowy o świadczenie usług telekomunikacyjnych lub osoby żądającej świadczenia takiej usługi, a więc definicja użytkownika jest szersza niż definicja abonenta (art. 2 pkt 1 i pkt 49 PT). Tajemnicą są objęte dane dotyczące użytkowników przekazywane w sieci telekomunikacyjnej, a także dane o użytkownikach występujące w związku z ustanowieniem stosunku prawnego między użytkownikiem a przedsiębiorcą oraz w związku z korzystaniem z usług. Część tych danych, w zależności od tego, jakiej kategorii użytkowników dotyczą oraz kto nimi dysponuje, będzie danymi osobowymi. W konsekwencji Sąd przyjął, że w piśmiennictwie trafnie zauważa się, że ponieważ art. 159 ust. 1 pkt 1 p.t. nie ogranicza przedmiotowego zakresu danych dotyczących użytkowników do danych osobowych, a do

[90] Wyrok SA w Warszawie z 1.07.2020 r., sygn. akt VII AGa 245/19.
[91] Ustawa z dnia 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800).

zakresu tajemnicy telekomunikacyjnej należy zaliczyć też inne dane o użytkownikach oprócz danych osobowych, nawet jeżeli dla przedsiębiorcy telekomunikacyjnego nie mają one charakteru osobowego. Dane dotyczące użytkownika mogą obejmować zatem również inne dane. Dotyczy to sytuacji, gdy użytkownika nie da się zidentyfikować co do tożsamości w myśl przepisów ustawy o ochronie danych osobowych, ale przedsiębiorca telekomunikacyjny może uzyskać zindywidualizowane informacje o użytkowniku w związku z wykonywaniem usług. Okoliczność zatem, że określone dane, czy też informacje nie mogą zostać uznane za dane osobowe w rozumieniu ustawy o ochronie danych osobowych, nie oznacza, że nie są objęte tajemnicą telekomunikacyjną w rozumieniu art. 159 ust. 1 p.t.[92]

Powyższe rozważania prowadzą do wniosku, że kwalifikowanie informacji jako danych osobowych jest zależne od okoliczności faktycznych konkretnego przypadku, a poddanie ich ochronie prawnej zależne od przepisów, które stanowią podstawę formułowanych roszczeń. Omawiany wyrok pokazuje, że odpowiadając na pytanie, czy określone identyfikatory internetowe stanowią dane osobowe, należy wziąć pod uwagę „wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo", że zostaną wykorzystane przez administratora lub inną osobę w celu zidentyfikowania osoby fizycznej. Miarą uzasadnionego prawdopodobieństwa wykorzystania danego sposobu identyfikacji powinny być zaś „wszelkie obiektywne czynniki", do których prawodawca unijny w szczególności zalicza „koszt i czas potrzebne do zidentyfikowania" osoby fizycznej, „technologię dostępną w momencie przetwarzania danych" i „postęp technologiczny". Nie powinna mieć przy tym rozstrzygającego znaczenia możliwość dokonania samoidentyfikacji przez osobę, której dane dotyczą.

Kolejnym problematycznym zagadnieniem w zakresie uznania informacji za dane osobowe jest numer telefonu. Problem ten ilustruje sprawa rozpoznawana przez Sąd WSA w Warszawie[93] w stanie faktycznym, którego istotą sporu było to, że w związku z nabyciem pakietu danych (numerów telefonu, wytypowanych na podstawie kryterium geograficznego) od innego podmiotu – Spółka pozyskała numer telefonu wnioskodawcy, a wnioskodawca skierował do Spółki żądanie dostarczenia mu kopii jego danych, a także udzielenia informacji o źródle pozyskania tych danych. Spółka udzieliła wnioskodawcy pisemnej odpowiedzi, w której odmówiła realizacji jego żądań, gdyż – w jej opinii – numer telefonu nie stanowi danych osobowych. W tym stanie rzeczy wnioskodawca złożył skargę do PUODO na

[92] Wyrok SA w Warszawie z 1.07.2020 r., sygn. akt VII AGa 245/19.
[93] Wyrok WSA w Warszawie z 13.04.2021 r., sygn. akt II SA/Wa 1898/20.

przetwarzanie jego danych osobowych przez Spółkę. Zdaniem wnioskodawcy nieprawidłowości w procesie przetwarzania polegały na przetwarzaniu jego danych osobowych, w szczególności numeru telefonu, bez podstawy prawnej oraz niezrealizowaniu żądań udzielenia informacji o źródle pozyskania danych i przekazania mu kopii przetwarzanych danych. Po przeprowadzeniu postępowania PUODO udzielił Spółce upomnienia za odmowę realizacji żądania wnioskodawcy dotyczącego udzielenia mu informacji o źródle pozyskania danych osobowych oraz kopii jego danych osobowych. Dodatkowo nakazał Spółce usunięcie danych osobowych wnioskodawcy, gdyż – zdaniem PUODO – przetwarzała je bez podstawy prawnej. Sąd zajął w tej sprawie stanowisko, zgodnie z którym przy weryfikacji, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki. Jak przypomniał Sąd, Grupa Robocza ds. ochrony danych, powołana na mocy art. 29, w Opinii 4/2007 zajmuje stanowisko, że „krajowe organy ds. ochrony danych osobowych zetknęły się ze sprawami, w których administrator twierdził, że przetwarza jedynie niekompletne informacje bez jakiejkolwiek wzmianki o nazwisku lub innym bezpośrednim czynniku identyfikującym i przekonywał, że dane nie powinny być uważane za dane osobowe i nie powinny podlegać przepisom dotyczącym ochrony danych osobowych. Jednak przetwarzanie takich informacji ma sens jedynie wtedy, jeżeli umożliwia zidentyfikowanie konkretnych osób i zastosowanie wobec nich określonego sposobu traktowania. W przypadkach, gdy celem przetwarzania jest identyfikacja osób, można przypuszczać, że administratorzy lub inne zainteresowane osoby dysponują sposobami, jakimi można się posłużyć" w celu zidentyfikowania osoby, której dane dotyczą. Twierdzenie, że osoby nie są możliwe do zidentyfikowania, podczas gdy celem przetwarzania danych jest właśnie ich identyfikacja, zawierałoby wewnętrzną sprzeczność. Dlatego informacje takie należy uważać za dotyczące osób możliwych do zidentyfikowania, a przetwarzanie ich powinno podlegać przepisom dotyczącym ochrony danych". W dalszej części uzasadnienia wyroku Sąd stwierdził, że danymi osobowymi mogą być informacje, które nie identyfikują konkretnej osoby, lecz jest możliwe – przy ich pomocy i wykorzystaniu nieznacznych środków – zidentyfikowanie konkretnej osoby. Zdaniem Sądu w tej sprawie tego rodzaju charakteru nie ma sam numer telefonu – nieprzypisany do konkretnej osoby, w ramach zbioru informacji posiadanych przez podmiot dysponujący tymi danymi, bądź w łatwy sposób pozyskiwalnymi. Niektóre dane – w zależności od ich powiązania z innym zbiorem informacji o osobach - mogą w pewnych sytuacjach stanowić dane osobowe bądź nimi nie być. Numer telefonu może być wyłącznie podstawą dla podjęcia określonych czynności w celu identyfikacji posiadacza

numeru – abonenta lub osoby, która faktycznie używa danego numeru[94]. Sam numer telefonu w większości przypadków (tj. z wyjątkiem sytuacji, gdy administrator danych - dysponent informacji – będzie miał również inne informacje, które umożliwiają identyfikację osoby fizycznej) nie będzie stanowił danych osobowych. Możliwość identyfikowania osoby fizycznej – jak już powiedziano – należy odnosić do określenia tożsamości konkretnej osoby fizycznej na podstawie posiadanych lub ewentualnie możliwych do uzyskania informacji. Nie można natomiast odnosić tego pojęcia do podejmowania działań zmierzających dopiero do ustalenia (uzyskania) informacji, które mogą stanowić dane osobowe (identyfikować konkretną osobę fizyczną)[95].

Danymi osobowymi mogą być informacje przedstawione z wykorzystaniem słów, liczb (numerów), dźwięków czy obrazów. Nie ulega wątpliwości, że informacja dotycząca numeru telefonu, która stanowi w istocie pewien zbiór cyfr, nie wskazuje tożsamości konkretnej osoby, ani też na podstawie tej danej nie jest możliwe natychmiastowe ustalenie tożsamości osoby. Natomiast kwestią, która wymaga rozważenia, jest to, czy na podstawie numeru telefonu można bezpośrednio lub pośrednio zidentyfikować daną osobę. Co do kwestii identyfikowania osoby fizycznej warto jeszcze wskazać, że w doktrynie prezentowany jest pogląd, iż możliwość identyfikowania na gruncie definicji danych osobowych zawartej w RODO należy odnosić do określenia tożsamości konkretnej osoby fizycznej na podstawie posiadanych lub ewentualnie możliwych do uzyskania informacji, a nie do podejmowania działań zmierzających dopiero do uzyskania informacji, które mogą stanowić dane osobowe[96]. Analiza powyższych rozważań prowadzi do wniosku, że zestawienie numeru telefonu z innymi danymi odnoszącymi się do konkretnej osoby pozwala na zidentyfikowanie tej osoby, a zatem uzasadniona była konstatacja prezentowana przez Sąd, że numer telefonu jest daną osobową. W świetle powyższego należy stwierdzić, że na podstawie numeru telefonu można zidentyfikować konkretną osobę, gdy numer ten zostanie zestawiony z innymi informacjami odnoszącymi się do osoby fizycznej, której dane dotyczą. Zagadnienie to nie ma znaczenia w sytuacji ocenienia numeru telefonu, którego abonentem nie jest osoba fizyczna.

Innym zagadnieniem dotyczącym problematyki oceny informacji jako danych osobowych jest przykład numerów rejestracyjnych. W orzecznictwie sądów administracyjnych

[94] Wyrok WSA w Warszawie z 13.04.2021 r., sygn. akt II SA/Wa 1898/20.
[95] P. Barta, M. Kawecki, *Rozporządzenie UE*..., red. P. Litwiński.
[96] P. Barta, M. Kawecki, *Rozporządzenie UE*..., red. P. Litwiński, komentarz do art. 4 https://sip-1legalis-1pl-1v27i8rcf003d.han3.lib.uni.lodz.pl/document-view.seam?documentId=mjxw62zogi3damzxgaztsnzoobqxalrtgq4dgnbsgi3q&refSource=toc

wykształciły się dwa poglądy na temat tego, czy numer rejestracyjny pojazdu jest daną osobową.

Pierwszy pogląd zakłada, że numer rejestracyjny służy przede wszystkim identyfikacji pojazdu i do niego jest przypisany. Z tych samych pojazdów korzystają bowiem często różne osoby, w różnych miejscach, są one niejednokrotnie rejestrowane na więcej niż jeden podmiot. Zatem w takich sytuacjach nie da się powiązać pojazdu z określoną osobą w sposób łatwy i niewymagający nadzwyczajnych nakładów. Numer rejestracyjny identyfikuje pojazd, a nie osobę. Podobna opinia prezentowana jest również w doktrynie, gdzie przyjmuje się, że statusu danych osobowych z reguły nie mają informacje odnoszone np. do numerów rejestracyjnych samochodów[97] oraz w polskim orzecznictwie[98]. Drugi natomiast pogląd uznaje, że numer rejestracyjny pojazdu może prowadzić do identyfikacji osoby, a zatem stanowi on dane osobowe w rozumieniu art. 6 ust.1 SUODO. Taka argumentacja wynika z wyroków Wojewódzkiego Sądu Administracyjnego w Warszawie[99]. W świetle tak prezentowanych stanowisk przyjąć należy, że co do zasady numery rejestracyjne pojazdu same w sobie nie stanowią danych osobowych. Istnieją jednak sytuacje, kiedy mając na uwadze całokształt okoliczności towarzyszących, uznać można, iż sama informacja zawarta na tablicy pojazdu (np. spersonalizowany numer lub numer umieszczony na unikatowym egzemplarzu pojazdu) pozwala przypisać ją do jego zindywidualizowanego właściciela bądź posiadacza.

Na przykładzie powyższych analiz widoczne jest, że o zakwalifikowaniu konkretnej informacji jako danej osobowej przesądza każdorazowo analiza stanu faktycznego sprawy i przyporządkowanie go do trzech przesłanek wyznaczających definicję danej osobowej. W piśmiennictwie podnoszony jest w związku z tym problem zjawiska tzw. relatywizacji pojęcia danych osobowych, które odnosi się do możliwości różnego kwalifikowania takiej samej informacji z punktu widzenia definicji danych osobowych w zależności od tego, jaki podmiot tę informację przetwarza, jakimi środkami identyfikacji dysponuje, jakie jeszcze inne informacje przetwarza itp. Zjawisko to miało swoje źródło m.in. w motywie 26 Dyrektywy 95/46 oraz w definicji pojęcia danych osobowych, zawartej w art. 6 SUODO, stanowiącym, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Stanowisko, że nie mają charakteru danych

---

[97] J. Barta, P. Fajgielski, R. Markiewicz, *Ustawa o ochronie danych osobowych, Komentarz*, LEX 2015.

[98] Wyrok NSA z 11.04.2019 r., sygn. akt I OSK 1240/17; wyrok NSA z 28.96.2019 r. I OSK 2063/17; wyrok WSA w Gliwicach z 31.10.2018 r., sygn. akt II SA/GL 593/17; wyrok WSA w Krakowie z 2.02.2017 r., sygn. akt II SA/Kr 1457/16; wyrok WSA w Krakowie z 20.03.2014 r., sygn. akt II SA/Kr 127/14.

[99] Wyrok WSA w Warszawie z 9.04.2013 r., sygn. akt II SA/Wa 211/13; wyrok z 25.04.2014 r., sygn. akt II SA/Wa 30/14 (CBOSA).

osobowych informacje, przy których ustalenie tożsamości osoby wymaga nieproporcjonalnie dużego nakładu czasu, pracy czy kosztów, wyrażone zostało również w raporcie wyjaśniającym do Konwencji 108 oraz w rekomendacjach Komitetu Ministrów Rady Europy, tj. rekomendacji na temat udostępniania danych osobowych będących w dyspozycji instytucji publicznych oraz rekomendacji w sprawie ochrony danych osobowych wykorzystywanych dla potrzeb płatności oraz innych analogicznych operacji. Na gruncie RODO prawodawca unijny do koncepcji relatywnego charakteru danych osobowych nawiązał w motywie 26 wskazując, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (ang. *reasonably likely*, niem. *nach allgemeinem Ermessen wahrscheinlich),* w stosunku do których istnieje uzasadnione prawdopodobieństwo (ang. *reasonably likely*, niem. *nach allgemeinem Ermessen wahrscheinlich),* iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. W relacji do motywów dyrektywy 95/46 nastąpiła zatem widoczna zmiana, której znaczenie należy rozważyć w kontekście jej wpływu na zasięg pojęcia danych osobowych. W motywie 26 dyrektywy 95/46 wskazywano bowiem, że w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie (racjonalnie prawdopodobne) sposoby, jakimi może posłużyć się administrator lub inna osoba w celu zidentyfikowania owej osoby. W RODO pojawia się natomiast nowy element, zgodnie z którym wszelkie racjonalnie (rozsądnie) prawdopodobne sposoby należy oceniać dodatkowo przez pryzmat uzasadnionego prawdopodobieństwa ich wykorzystania przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej[100].

Z perspektywy odpowiedzialności za naruszenie przepisów o ochronie danych osobowych zagadnienie pojęcia jakie informacje są danymi osobowymi jest kluczowe, dlatego kwalifikowanie konkretnych informacji jako danych osobowych powinno być zależne wyłącznie od spełnienia omawianych przesłanek. Na gruncie RODO aktualnie problematyczne jest rozumienie przesłanki definicji danych osobowych. Wynikająca z art. 4 pkt 1 rozporządzenia definicja zawiera bowiem nowy element, nieznany dyrektywie – element uzasadnionego prawdopodobieństwa. Z uwagi jednak na wypracowane w doktrynie na gruncie

[100] D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych*...

Dyrektywy rozumienie pojęcia danych osobowych zasadnym dla praktyki wydaje się kontynuowanie tego dorobku, zwłaszcza że istota prawa do ochrony danych osobowych nie uległa zmianie. W tym miejscu podkreślić należy, doniosłość tezy, że proces kwalifikacji identyfikatora powinien realizować obowiązek stosowania tzw. „klauzuli rozsądku" wypowiedzianej w wyroku Trybunału Sprawiedliwości Unii Europejskiej z 19.10.2016 r. w sprawie C-582/14 Breyer vs Niemcy[101]. W wyroku tym (pkt 42) odwołano się do motywu 26 dyrektywy 95/46 wskazując, że „w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może, racjonalnie rzecz biorąc, posłużyć się (ang. wers. jęz.: all the means likely reasonably to be used – przyp. Sądu) administrator danych lub inna osoba w celu zidentyfikowania owej osoby". Następnie natomiast stwierdzono (pkt 43), że „w zakresie, w jakim wskazany wyżej motyw odnosi się do sposobów, jakimi mogą, racjonalnie rzecz biorąc, posłużyć się zarówno administrator danych, jak i inna osoba, brzmienie tego motywu sugeruje, że aby dane mogły zostać uznane za dane osobowe w rozumieniu art. 2 lit. a) wspomnianej dyrektywy, nie jest wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, musiały znajdować się w rękach tylko jednej osoby". Trybunał zaznaczył jednak również, że „należy (...) ustalić, czy możliwość połączenia informacji z owymi dodatkowymi informacjami może racjonalnie rzecz biorąc, zostać zastosowana w celu zidentyfikowania osoby, której dane dotyczą". Odwołując się do opinii rzecznika generalnego, Trybunał wskazał, że „nie miałoby to miejsca w przypadku, gdyby identyfikacja osoby, której dane dotyczą, była zakazana prawem lub niewykonalna w praktyce, przykładowo z powodu okoliczności, że wiąże się ona z nadmiernym nakładem czasu, kosztów i pracy ludzkiej, tak że ryzyko identyfikacji wydaje się w rzeczywistości znikome. Takie rozumienie przywołanej „klauzuli rozsądku" powinno być brane pod uwagę podczas oceny elementu aktualnej definicji danych osobowych jakim jest uzasadnione prawdopodobieństwo.

Pojęcie przedsiębiorcy

Kluczowe dla niniejszej pracy jest ustalenie kto w procesie przetwarzania danych odpowiada za zgodność przetwarzania z przepisami. Uznanie kto jaką rolę pełni na gruncie RODO jest równoznaczne z przypisaniem konkretnych obowiązków. Zagadnienia analizowane w pracy ograniczają się do badania konsekwencji prawnych działań przedsiębiorcy, a nie wszystkich podmiotów, którym przypisana jest rola administratora lub podmiotu

[101] Wyrok Trybunału Sprawiedliwości Unii Europejskiej z 19.10.2016 r. w sprawie C-582/14 Breyer vs Niemcy.

przetwarzającego, dlatego w pierwszej kolejności konieczne jest zdefiniowanie pojęcia „przedsiębiorca" na gruncie prawa krajowego i europejskiego. Obowiązki przedsiębiorcy jako administratora i podmiotu przetwarzającego omówione zostaną w dalszych rozdziałach pracy.

Polski system prawa nie zawiera uniwersalnej definicji pojęcia przedsiębiorcy, która byłaby stosowana w sposób jednolity w ramach wszystkich aktów normatywnych posługujących się tym terminem. W wielu aktach prawnych możemy spotkać różniące się między sobą normatywne definicje pojęcia „przedsiębiorca". W ten sposób ustawodawca, poszerzając bądź też zawężając zakres definicyjny omawianego terminu, dostosowuje go konstrukcyjnie do specyfiki stosunków uregulowanych danym aktem normatywnym[102]. Do czasu wprowadzenia definicji ustawowej przedsiębiorcy, dla ich oznaczenia w stosunkach cywilnoprawnych funkcjonowało głównie określenie „kupiec" lub inne pojęcia, zależnie od rodzaju dokonywanych czynności, np. osoby fizycznej, dłużnika, właściciela[103]. Pojęcia kupca i przedsiębiorcy występowały w polskim prawie już w okresie międzywojennym, przy czym zasadnicza różnica między nimi polegała na tym, że pojęcie kupca zostało ustawowo zdefiniowane, a przedsiębiorcy – nie[104]. W latach 30. XX w. wprowadzony został termin „jednostka gospodarcza" – w art. 1 rozporządzenia Prezydenta RP z 24.10.1934 r. – Prawo upadłościowe (Dz.U. z 1991 r. Nr 118, poz. 512) i w art. 1 rozporządzenia Prezydenta RP z 24.10.1934 r. – Prawo o postępowaniu układowem (Dz.U. Nr 93, poz. 836). Następnie pojęcie kupca zdefiniował w kodeksie handlowych z 1934 r. art. 2, stanowiąc, że kupcem jest ten, kto we własnym imieniu prowadzi przedsiębiorstwo zarobkowe. Pojęcie kupca (choć bez określenia, co znaczy) znajdowało się więc w przepisach obowiązujących aż do końca 2000 r. z uwagi na fakt, że w przepisach wprowadzających kodeks cywilny (art. VI) utrzymano w mocy niektóre przepisy Kodeksu handlowego z 1934 r., uchylając wprawdzie cały kodeks, a więc i art. 2 definiujący kupca, ale pozostawiając w mocy między innymi takie przepisy, które posługiwały się pojęciem kupca lub kupca rejestrowego w odniesieniu do pozostawionych spółek handlowych (przepisy o firmie, prokurze, rejestrze handlowym).

Po kilkudziesięciu latach, tj. pod koniec lat 80., ustawodawca Ustawą o działalności gospodarczej z 1988 r. w art. 2 wprowadzona została definicja podmiotu gospodarczego, zastąpiona od stycznia 2001 r. definicją przedsiębiorcy zawartą w ustawie Prawo działalności

[102] I. Gancarz, *Pojęcie przedsiębiorcy w zakresie antykonkurencyjnych praktyk na tle art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej*, Wrocław 2012, s. 114.
[103] S. Dmowski, R. Trzaskowski, [w:] *Kodeks cywilny. Komentarz. Księga pierwsza, część ogólna*, t. 1, Warszawa 2014, s. 216.
[104] Rozporządzenie Prezydenta RP z 27.6.1934 r. – Kodeks handlowy (Dz.U. Nr 57 poz. 502), data uchylenia: 1.1.2001 r.; zob. M. Allerhand, *Kodeks handlowy: komentarz*, Lwów 1935, s. 5–6.

gospodarczej z 19.11.1999 r. w art. 2 ust. 1 i 2. Pojęcie przedsiębiorcy w prawie polskim przeszło zatem ewolucyjną drogę od pierwszych aktów prawnych zawierających regulacje z zakresu działalności gospodarczej, gdzie przedsiębiorca nazywany był podmiotem gospodarczym, do wprowadzenia do prawa polskiego definicji przedsiębiorcy. Przepisy pierwszego polskiego aktu normatywnego regulującego problematykę działalności gospodarczej, tj. rozporządzenia Prezydenta Rzeczypospolitej z 7.06.1927 r. o prawie przemysłowem, posługiwały się pojęciem „przemysłowca (art. 39, 113, 125) i „przedsiębiorca" (art. 29, 42), używając w swej treści tych terminów niekiedy zamiennie, nie podając ich ustawowej definicji. Pojęciem przedsiębiorcy, także bez bliższego wyjaśnienia treści zaproponowanej definicji, posługiwały się już przepisy ustawy z 2.08.1926 r. o zwalczaniu nieuczciwej konkurencji. Po definicji przedsiębiorcy z 1999 r. kolejne jej określenie przyniosła ustawa z 2.07.2004 r. o swobodzie działalności gospodarczej, a całkiem odmiennie od niego ustawodawca uregulował to pojęcie w ustawie z dnia 6.03.2018 r. – Prawo przedsiębiorców.

Zdaniem niektórych z autorów art. 4 u.p.p. powiela częściowo regulacje obowiązujące wcześniej w art. 4 u.s.d.g. zarówno w zakresie kategorii podmiotów, jak również wymogu wykonywania działalności gospodarczej, stąd zarówno orzecznictwo, jak i wszelkie interpretacje urzędowe wydane na gruncie przywołanego przepisu ustawy o swobodzie działalności gospodarczej, podobnie jak piśmiennictwo, zachowują swoją aktualność w stosunku do art. 4 u.p.p. w zakresie, w jakim tyczą się tych elementów[105]. Zdaniem niektórych z autorów art. 4 u.p.p. powiela częściowo regulacje obowiązujące wcześniej w art. 4 u.s.d.g. zarówno w zakresie kategorii podmiotów, jak również wymogu wykonywania działalności gospodarczej, stąd zarówno orzecznictwo, jak i wszelkie interpretacje urzędowe wydane na gruncie przywołanego przepisu ustawy o swobodzie działalności gospodarczej, podobnie jak piśmiennictwo, zachowują swoją aktualność w stosunku do art. 4 u.p.p. w zakresie, w jakim tyczą się tych elementów[106]. Według W.J. Katnera negatywnie należy jednak ocenić pominięcie cechy zawodowości (profesjonalizmu) wśród cech przedsiębiorcy w Prawie Przedsiębiorców. Podobnej krytyce poddane zostało umieszczenie warunku prowadzenia działalności we własnym imieniu w definicji działalności gospodarczej, a nie jak dotychczas w definicji przedsiębiorcy[107].

[105] A. Pietrzak, *Prawo przedsiębiorców. Komentarz*, Warszawa 2019.
[106] A. Pietrzak, *Prawo przedsiębiorców*...
[107] W. J. Katner Zakres tzw. konstytucji biznesu. Kontrowersje wokół pojęcia przedsiębiorcy w ustawie - Prawo przedsiębiorców z 2018 r. PPH 2019/1/5-10

Począwszy od pierwszej ustawy z 1988 r. o działalności gospodarczej[108], definiującej podmiot gospodarczy, określenie przedsiębiorcy zawierało stronę podmiotową, czyli wskazanie podmiotów prawa, które mogą być przedsiębiorcami, stronę przedmiotową, czyli to, co stanowi sobą działalność gospodarcza oraz odrębnie cechy przedsiębiorcy. Posiadanie tych cech decydowało o tym, że prowadzona działalność gospodarcza była wykonywana przez podmiot, który można określić mianem przedsiębiorcy. Cechy przedsiębiorcy określiła szczegółowo ustawa z 1999 r. – Prawo działalności gospodarczej i powtórzyła ustawa z 2004 r. o swobodzie działalności gospodarczej. Z punktu widzenia podmiotowego mogła to więc być osoba fizyczna, osoba prawna i jednostka organizacyjna niemająca osobowości prawnej, ale mająca przyznaną ustawowo zdolność prawną (czyli każdy podmiot prawa cywilnego), która prowadziła określoną działalność gospodarczą we własnym imieniu, w sposób zorganizowany, zarobkowy, ciągły i zawodowy. Cechy te musiały wystąpić łącznie[109].

W Kodeksie cywilnym definicja przedsiębiorcy funkcjonuje od 24.04.2003 r.[110]. Zgodnie z art. 43 [1] k.c. za przedsiębiorcę uważa się osobę fizyczną, osobę prawną i jednostkę organizacyjną, o której mowa w art. 33^1 § 1 k.c. (czyli tzw. niepełną osobę prawną) prowadzącą we własnym imieniu działalność gospodarczą lub zawodową (art. 43^1). Z kolei, w obowiązującej od.08.2004 r. ustawie o swobodzie działalności gospodarczej za przedsiębiorcę uznawało się takie same podmioty, jak według Kodeksu cywilnego, wykonujące we własnym imieniu działalność gospodarczą (art. 4 ust. 1). W przeciwieństwie do Kodeksu cywilnego ustawa określała dalsze cechy, które musi spełnić podmiot prawa, aby stać się przedsiębiorcą, a także wskazywała, co oznacza wymaganie prowadzenia działalności gospodarczej (art. 2). Zdaniem W.J. Katnera w opracowaniach cywilistycznych zauważalne jest ignorowanie ustawy z 2004 r. i dość wątpliwe tłumaczenie pojęcia działalności gospodarczej, ale skoro Kodeks cywilny używa tego pojęcia, a go nie definiuje, to trzeba sięgnąć do przepisów, które to czynią. Według W.J. Katnera były nimi przepisy ustawy z 2004 r. Tam też znajdowały się opuszczone w Kodeksie cywilnym, a niezbędne cechy przedsiębiorcy, czyli zarobkowy cel oraz wykonywanie działalności w sposób zorganizowany i ciągły. Nie można przecież poważnie uważać, że można musieć spełnić określone cechy, żeby być przedsiębiorcą dla celów rejestru w KRS i ewentualnie innych celów publicznoprawnych, a nie musieć ich mieć, a i tak być przedsiębiorcą w obrocie cywilnoprawnym. Biorąc za przykład spółkę kapitałową, to przecież

[108] Ustawa z dnia 23.12.1988 r. o działalności gospodarczej (Dz.U. 1988 nr 41 poz. 324).
[109] W.J. Katner, *Zakres tzw. konstytucji biznesu. Kontrowersje wokół pojęcia przedsiębiorcy w ustawie - Prawo przedsiębiorców z 2018 r.*, PPH 2019/1/5-10.
[110] Ustawa z dnia 14.02.2003 r. o zmianie ustawy - Kodeks cywilny oraz niektórych innych ustaw.

ona – wprawdzie zawsze wpisana do rejestru przedsiębiorców (art. 36 ustawy o KRS) – nie będzie przedsiębiorcą, jeśli nie spełni cech go dotyczących (np. będzie utworzona dla celów niezarobkowych – *non profit*). Będzie zaś podmiotem prawa (osobą prawną) według art. 1 k.c. i będzie występować jako podmiot prawa cywilnego (np. w umowach)[111].

Działalność gospodarcza jest faktem obiektywnym, stąd za trafne uznać należy oceny jakie w stosunku do aktualnego brzmienia definicji przedsiębiorcy, wynikającej z ustawy z dnia 6.03.2018 r. – Prawo przedsiębiorców, formułuje W.J. Katner. Dowodzi on m.in, że ustawodawca pomieszał pojęcie przedsiębiorcy z tym, czym się on zajmuje. Zdaniem tego Autora jeżeli według art. 5 u.p.p. działalność bagatelna, o której stanowi ten przepis, nie jest gospodarcza, to chyba ustawodawca nie zdawał sobie sprawy, że faktom nie da się zaprzeczyć przez tzw. zaklęcia ustawowe albo tzw. dobre intencje. Dlatego, mimo wprowadzonego przepisu, działalność bagatelna i tak będzie działalnością gospodarczą, ponieważ będzie dotyczyć czynności, które obiektywnie są gospodarcze, a to, że nie spowoduje obowiązku złożenia wniosku o wpis do Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG) ma dla pojęć działalności gospodarczej i przedsiębiorcy wtórne znaczenie. Podkreślić należy, że w ewidencji rejestruje się osoby fizyczne, jako przedsiębiorców i od tego zależy ich legalne funkcjonowanie w obrocie. Ustawa zatem całkowicie myli osobę przedsiębiorcy z prowadzoną przez niego działalnością, gdyż ona nie wystarczy, żeby być przedsiębiorcą. Należało zatem w nowych przepisach zostawić dotychczasowe, tradycyjne jak już można powiedzieć, wyodrębnienie działalności gospodarczej, przedmiotowo koniecznej do wyróżnienia przedsiębiorcy od cech osoby, która chce się mienić przedsiębiorcą podmiotowo[112]. Takie reguły budowania definicji przedsiębiorcy mogły ujednolicić rozumienie tego pojęcia w całym systemie prawa, dlatego że formułowanie pojęć i określeń właściwych tylko ustaw, w których występują oraz posługiwania się tymi samymi terminami w różnych znaczeniach prowadzi do tworzenia bałaganu terminologicznego, powodującego niezrozumienie przez adresatów (w ogromnej większości niebędących prawnikami) norm prawnych – dlaczego to samo pojęcie co chwilę znaczy coś innego[113]. W tym miejscu podkreślenia wymaga, że próby ujednolicenia rozumienia pojęcia przedsiębiorcy nie ułatwia fakt, że w obowiązującym stanie prawnym definicje przedsiębiorcy występują ponadto m.in. w:

[111] W.J.Katner, *Pojęcie przedsiębiorcy – polemika*, PPH 2007/4/41-44.
[112] W.J. Katner, *Zakres tzw. konstytucji biznesu...*, PPH 2019/1/5–10.
[113] W.J. Katner, *Pojęcie przedsiębiorcy – polemika...*

– art. 3 ust. 1 pkt 3 ustawy z 30.06.2000 r. – Prawo własności przemysłowej, gdzie przez przedsiębiorcę rozumie się osobę prowadzącą w celach zarobkowych działalność wytwórczą, budowlaną, handlową lub usługową;
– art. 2 ustawy z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji, stanowiącym, że przedsiębiorcami, w rozumieniu ustawy, są osoby fizyczne, osoby prawne oraz jednostki organizacyjne niemające osobowości prawnej, które prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową, uczestniczą w działalności gospodarczej;
– art. 4 pkt 1 ustawy z 16.02.2007 r. o ochronie konkurencji i konsumentów, który stanowi, że przez przedsiębiorcę rozumie się przedsiębiorcę w rozumieniu przepisów Prawa przedsiębiorców, a także: osobę fizyczną, osobę prawną oraz jednostkę organizacyjną niemającą osobowości prawnej, której ustawa przyznaje zdolność prawną, organizującą lub świadczącą usługi o charakterze użyteczności publicznej, które nie są działalnością gospodarczą w rozumieniu przepisów Prawa przedsiębiorców, jak również osobę fizyczną wykonującą zawód we własnym imieniu i na własny rachunek lub prowadzącą działalność w ramach wykonywania takiego zawodu oraz osobę fizyczną, która ma kontrolę nad co najmniej jednym przedsiębiorcą, choćby nie prowadziła działalności gospodarczej w rozumieniu przepisów Prawa przedsiębiorców, jeżeli podejmuje dalsze działania podlegające kontroli koncentracji, a także związek przedsiębiorców;
– art. 2 pkt 1 ustawy z 23.08.2007 r. o przeciwdziałaniu nieuczciwym praktykom rynkowym, gdzie przez przedsiębiorcę rozumie się osoby fizyczne, osoby prawne oraz jednostki organizacyjne nieposiadające osobowości prawnej, które prowadzą działalność gospodarczą lub zawodową, nawet jeżeli działalność ta nie ma charakteru zorganizowanego i ciągłego, a także osoby działające w ich imieniu lub na ich rzecz[114].

W systemie prawa występuje zatem wiele określeń pojęcia przedsiębiorca. Zdaniem komentatorów nie pomagają apele o zaprzestanie uznawania przedsiębiorcy za pojęcie, które można różnie rozumieć w kolejnych ustawach. Podkreślić trzeba, że w opublikowanym w 2009 r. projekcie księgi pierwszej nowego Kodeksu cywilnego dostrzeżono wady dotychczasowej regulacji przedsiębiorący w Kodeksie i zaproponowano nowe rozumienie przedsiębiorcy, ale prezentuje się ono jeszcze gorzej niż według obowiązującego art. 43^1k.c.[115].

Także na gruncie RODO pojęcie przedsiębiorcy ma charakter autonomiczny, wpisując się w swoistą plagę niejednolitości interpretacyjnych, która po części wynika z konieczności przejęcia regulacji UE, która nie odwołuje się do polskich przepisów. Dlatego zgodnie z

[114] A. Pietrzak, *Prawo przedsiębiorców,* WKP 2019.
[115] W.J. Katner, *Prawo gospodarcze i handlowe*, Warszawa 2020 s. 64.

poczynioną na wstępie niniejszego rozdziału uwagą dla analizy zagadnień omawianych w pracy istotne jest ustalenie rozumienia przedsiębiorcy na gruncie przepisów RODO i ocena tego jak omawiane pojęcie należy rozumieć w kontekście jego definicji funkcjonującej w prawie UE, którego częścią jest RODO.

RODO zawiera własną definicję, wskazując w art. 4 pkt. 18 RODO jako przedsiębiorcę osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą. Definicja przyjęta w art. 4 pkt 18 RODO składa się z elementu podmiotowego (przedsiębiorcą jest osoba fizyczna lub prawna) oraz przedmiotowego („prowadząca działalność gospodarczą"). Ustawodawca dookreślił, że nie ma znaczenia forma prawna podmiotu prowadzącego działalność gospodarczą, a pojęcie to obejmuje również spółki osobowe i „zrzeszenia" (organizacje inne niż spółki), które prowadzą „regularną działalność gospodarczą[116].

Polska wersja językowa art. 4 pkt 18 RODO istotnie różni się od innych wersji, a zwłaszcza angielskiej i niemieckiej, definiując pojęcia, które nie oznaczają „przedsiębiorcy", lecz „przedsiębiorstwo". Jest to o tyle ważne dla pracy, że odpowiedzialność ponosi przedsiębiorca, a nie przedsiębiorstwo. W wersji angielskiej RODO użyto terminu *enterprise* podobnie w wersji francuskiej (*entreprise),* niemieckiej (*Unternehmen)* i hiszpańskiej (*empresa).* Należy zatem uznać, że pojęcie to należy interpretować w ten sposób, iż odnosi się ono zarówno do podmiotu prowadzącego działalność gospodarczą, jak i do samego zespołu składników tworzących przedsiębiorstwo. To, że istnieją rozbieżności w brzmieniu RODO pomiędzy polskim tekstem oficjalnym i innymi wersjami językowymi, zasadniczo skłania do uwzględnienia wszystkich wersji językowych[117]. Na przykład art. 40 ust. 1 RODO w wersji polskiej posługuje się terminem „przedsiębiorstwo", podczas gdy w wersji angielskiej użyto – zdefiniowanego w komentowanym tu przepisie – terminu *enterprise*. Podobnie jest w przypadku art. 42. Wydaje się, że również art. 83 ust. 4–6 RODO należy rozumieć jako odnoszący się do przedsiębiorcy w rozumieniu art. 4 pkt 18 RODO, choć nie jest to oczywiste, bo np. wersja angielska posługuje się w tym przypadku terminem *undertaking*, a nie *enterprises*, ale za to wersja niemiecka używa w tym przypadku terminu *Unternehmen*[118]. W taki sposób wypowiada się część doktryny i zgodnie z tymi stanowiskami różnica ta ma bardzo istotne konsekwencje, ponieważ omawiana definicja powinna mieć znaczenie głównie

[116] M. Górski [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 587.
[117] Zob. wyrok TSWE z 12.11.1969 r., 29/69, *Stauder v. Miasto Ulm*, ECLI:EU:C:1969:57; analogicznie wyrok z 5.12.1967 r., 19/67, *Bestuur der Sociale Verzekeringsbank v. J.H. van der Vecht*, ECLI:EU:C:1967:49.
[118] M. Górski [w:] *Ogólne rozporządzenie...*, red. M. Sakowska-Baryła, s. 587.

na potrzeby stosowania art. 83 ust. 4–6, które regulują wysokość administracyjnych kar pieniężnych, przewidując liczenie ich jako określony procent obrotu przedsiębiorstwa, a nie przedsiębiorcy. Użyte pojęcia mają istotne znaczenie praktyczne, a brak precyzji ustawodawcy generuje wątpliwości interpretacyjne dotyczące ich prawidłowego stosowania. Posługiwanie się zatem w polskiej wersji językowej pojęciem przedsiębiorcy prowadzi do problemów ze stosowaniem art. 83 ust. 4–6 komentowanego aktu prawnego. Definicja, która miała uprościć wykładnię wskazanych przepisów, według wskazanych powyżej opinii, zupełnie by się do tego nie nadawała. Prowadzi to do wniosku, że w polskiej wersji językowej rozporządzenia ogólnego pojawił się błąd w tłumaczeniu i art. 4 pkt 18 zamiast wyjaśniać pojęcie przedsiębiorstwa, definiuje pojęcie przedsiębiorcy[119].

Prezentowane powyżej poglądy nie odnoszą się do tego, że użyte w art. 40 i 42 RODO pojęcia nawiązują do występującej w prawie UE definicji małego i średniego przedsiębiorstwa, które są wykorzystywane dla celów statystycznych, rachunkowości sprawozdawczej oraz przydziału środków pomocowych (zalecenie Komisji z 6.5.2003 r. dotyczące definicji przedsiębiorstw mikro, małych i średnich C (2003). W literaturze proponuje się wykorzystanie tej definicji na potrzeby prawa konsumenckiego[120]. Ponadto pojęcia małego i średniego przedsiębiorstwa pojawiają się także w aktach prawa wtórnego (por. niżej), przykładowo: rozporządzenie nr 68/2001, 70/2001, 2204/2002 na temat wspólnotowego pojęcia małego i średniego przedsiębiorstwa. Pomijają one fakt, że centralnym pojęciem całego prawa gospodarczego UE jest przedsiębiorstwo[121], a w prawie krajowym to pojęcie przedsiębiorcy ma bogatą historię, co zostało wcześniej już zasygnalizowane. W piśmiennictwie podnoszone jest, że w prawie UE przyjmuje się szeroką i funkcjonalną definicję terminu „przedsiębiorca", obejmującą wszelkie podmioty, niezależnie od ich formy prawnej czy statusu określonego prawem wewnętrznym państwa członkowskiego, w tym również organy i instytucje publiczne, o ile wykonują one swobodę przedsiębiorczości lub świadczenia usług w rozumieniu TFUE[122].

W konsekwencji rozumienie pojęcia przedsiębiorca, które funkcjonujące w europejskim systemie prawa na potrzeby RODO może być źródłem problemów interpretacyjnych podobnych do tych, które obserwowane są w stosunku do pojęcia przedsiębiorcy w polskim porządku prawnym. Konieczne jest zatem podjęcie próby dalszej analizy przyczyn tłumaczenia tych pojęć w sposób przyjęty w polskiej wersji językowej. I tak

[119] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, L. Dominik, Warszawa 2017, Komentarz do art. 4
[120] M. Brożyna, *Konsumenckie prawo do odwołania umowy*, Warszawa 2021
[121] M. Brożyna, *Konsumenckie prawo do odwołania umowy*, Warszawa 2021.
[122] M. Etel, *Pojęcie przedsiębiorcy*, Warszawa 2012,s. 99–114.

w pierwszej kolejności podnieść należy, że posługiwanie się w niej pojęciem przedsiębiorstwa w art. 83 ust. 3 i 4, umieszczonym w rozdzielę VIII pt. środki ochrony prawnej, odpowiedzialność i sankcje dotyczy wyłącznie określeń wymiaru administracyjnej kary pieniężnej referującej w zależności od rodzaju naruszenia do wysokości 2–4 proc. całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Takie tłumaczenie pojęcia przedsiębiorstwo koresponduje z motywem 150 RODO, który wskazuje, że jeżeli administracyjna kara pieniężna jest nakładana na przedsiębiorstwo, to pojęcie przedsiębiorstwa należy rozumieć zgodnie z art. 101 i 102 TFUE. W komentarzu do polskiej ustawy o ochronie danych osobowych (późniejszej w stosunku do prezentowanych wcześniej stanowisk) problem nieścisłości pojęć w art. 83 ust. 4–6 RODO i motywie 150 podniesiony został w sposób prezentujący oba pojęcia zamiennie z jednoczesnym wskazaniem, że Grupa Robocza Art. 29 zwraca uwagę na to, że w przypadku nakładania kary na podmiot będący przedsiębiorcą, organ nadzorczy powinien uznać za przedsiębiorcę taki podmiot, który jest przedsiębiorcą w rozumieniu orzecznictwa TSUE wydanego na gruncie art. 101 i 102 TFUE[123], czyli podmiot zaangażowany w prowadzenie działalności gospodarczej niezależnie od jego statusu prawnego i formy jego finansowania[124].

Oceniając omawiane stanowiska dotyczące błędu w tłumaczeniu wersji polskiej RODO, stwierdzić należy, że nie podejmują one analizy tego, że najistotniejszą konsekwencją prawną przestrzegania zgodności przetwarzania danych jest prawna odpowiedzialność za przestrzeganie obowiązków, wynikających z prawa o ochronie danych osobowych. Odpowiedzialność zaś może być przypisana jedynie podmiotowi, który zgodnie z obowiązującym prawem posiada zdolność prawną i zdolność do czynności prawnych, której nie posiada przedsiębiorstwo. W doktrynie brak jest zatem stanowisk analizujących poprawność tłumaczenia z perspektywy zagadnień omawianych w pracy, gdzie posłużenie się definicją przedsiębiorcy, nie przedsiębiorstwa w zestawieniu z obowiązkami administratora lub podmiotu przetwarzającego ma znaczenie dla zagadnień dotyczących ponoszenia odpowiedzialności .

Przechodząc dalej do analizy pojęcia „przedsiębiorca" na gruncie RODO, powiedzieć należy, że omawiana definicja wyróżnia dwie grupy podmiotów, które mogą być zakwalifikowane jako przedsiębiorcy. W pierwszej znalazły się osoby fizyczne, osoby prawne oraz spółki osobowe, a w drugiej zrzeszenia. O ile do zakwalifikowania pierwszej grupy jako

[123] Zob. wyrok TSWE z 23.4.1991 r., C-41/90, *Höfner i Elser p. Macrotron GmbH*, EU:C:1991:161; Wytyczne WP 253, s. 6.
[124] *Ustawa o ochronie danych osobowych. Komentarz*, red. M. Czerniawski, M. Kawecki, Warszawa 2019.

przedsiębiorców wystarczające jest prowadzenie działalności gospodarczej, o tyle druga grupa musi prowadzić taką działalność w sposób regularny. Zarówno pierwsza, jak i druga kategoria dla uznania jej za przedsiębiorcę musi spełniać kumulatywnie dwie przesłanki. Po pierwsze, należeć do określonego grona podmiotów, a po drugie, prowadzić działalność gospodarczą albo regularną działalność gospodarczą[125].

Artykuł 4 pkt. 18 RODO pojęciem przedsiębiorca obejmuje osoby fizyczne lub prawne prowadzące działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą. O ile pojęcia osoby fizycznej lub prawnej, jak również spółki osobowej nie rodzą wielkich trudności w ich interpretacji na gruncie polskich i unijnych przepisów, o tyle dalszego doprecyzowania wymagają w szczególności pojęcia „zrzeszenia" (ang. *associations)* na gruncie polskich przepisów oraz (regularnej) „działalności gospodarczej" w rozumieniu nadanym mu przez przepisy unijne. Uwzględniając angielskojęzyczną wersję RODO i przenosząc pojęcie „zrzeszenia" na grunt polskich przepisów, należałoby przyjąć, że są nim objęte w szczególności stowarzyszenia. Obywatele polscy mają, zgodnie z art. 1 ust. 1 u.p.st.[126] prawo zrzeszania się w stowarzyszeniach. Zgodnie z art. 34 cytowanej ustawy, stowarzyszenia mogą prowadzić działalność gospodarczą. Zakresem zastosowania tego pojęcia mogą być objęte również stowarzyszenia międzynarodowe (art. 5) i związki stowarzyszeń (art. 22). Element „zrzeszenia" zawarty jest w definicji spółdzielni z art. 1 § 1 u.p.sp.[127]. Zgodnie z art. 67 cytowanej ustawy spółdzielnie prowadzą działalność gospodarczą. Obie z powyższych kategorii podmiotów zyskują osobowość prawną z chwilą wpisu do KRS. Definicją przedsiębiorcy na gruncie RODO mogą być objęte zrzeszenia tworzone na podstawie odrębnych przepisów, np. społeczno-zawodowe organizacje rolników, o których mowa w art. 3 u.s.z.o.r.[128], które zgodnie z art. 12 u.s.z.o.r. ustawy mogą prowadzić działalność gospodarczą[129].

Pojęcie zrzeszenia musi oznaczać inne podmioty niż osoby fizyczne, osoby prawne oraz spółki osobowe, których dotyczy pierwsza część komentowanego przepisu. Jednocześnie należy dążyć do takiej wykładni pojęcia przedsiębiorcy, by objąć nim wszystkie podmioty, które zgodnie z prawem poszczególnych państw członkowskich mogą wykonywać działalność gospodarczą. Biorąc powyższe pod uwagę, przez pojęcie zrzeszenia należy rozumieć inne niż

[125] *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D.Lubasz.
[126] Ustawa z dnia 7.04.1989 r. – Prawo o stowarzyszeniach (Dz.U. 2020 poz. 2261).
[127] Ustawa z dnia 16.09.1982 r. – Prawo spółdzielcze (Dz.U. 2021 poz. 648).
[128] Ustawa z dnia 8.10.1982 r. o społeczno- zawodowych organizacjach rolników (Dz.U. 2022 poz. 281).
[129] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021.

spółki osobowe jednostki organizacyjne niebędące osobami prawnymi, którym przepisy poszczególnych państw członkowskich przyznają zdolność prawną. Na gruncie prawa polskiego chodzić będzie o tzw. ułomne osoby prawne w rozumieniu przepisu art. 33^1 § 1 k.c., jednak inne niż spółki osobowe, które są osobno wymienione w art. 4 pkt 18. Zgodnie z zaproponowaną wykładnią zrzeszeniami w rozumieniu tego wspólnoty mieszkaniowe, co wynika z art. 6 ustawy z 24.06.1994 r. o własności lokali[130] jeżeli czerpią zyski np. z wynajmu części wspólnych nieruchomości.

W tym miejscu pojawia się problem, jak na gruncie przepisu art. 4 pkt 18 zakwalifikować spółkę cywilną. Czy powinna ona należeć do pierwszej grupy podmiotów, a więc osób prawnych, osób fizycznych i spółek osobowych, czy też do drugiej w postaci zrzeszeń? Przede wszystkim należy podkreślić, że spółka cywilna jest jedynie stosunkiem obligacyjnym i nie tworzy osobnego bytu prawnego, co podkreślił Sąd Najwyższy w postanowieniu z 24.10.2003r.[131], argumentując, że: „Obecnie spółka cywilna jest nadal związkiem osób niemającym podmiotowości prawnej, ale o jawnej dla osób trzecich strukturze podmiotowej". Nie należy zatem dokonywać kwalifikacji spółek cywilnych pod pojęcie zrzeszeń. Pod tym pojęciem rozumiane są bowiem tzw. ułomne osoby prawne, z wyłączeniem spółek osobowych. Spółki cywilne nie posiadają tymczasem zdolności prawnej. Poszukując rozwiązania problemu prawidłowej kwalifikacji spółek cywilnych, należy uznać, że umowa spółki cywilnej w rozumieniu art. 860 § 1 k.c. może być zawarta zarówno przez osoby fizyczne, osoby prawne, jak i jednostki organizacyjne niebędące osobami prawnymi, którym przepisy poszczególnych państw członkowskich przyznają zdolność prawną. Spółka cywilna korzysta w obrocie w istocie z podmiotowości prawnej swoich wspólników, którzy reprezentują spółkę i w ten sposób zarządzają majątkiem wspólników, który ma charakter wspólności łącznej. Skoro zatem stronami umowy spółki cywilnej mogą być podmioty z obu grup wyróżnionych na gruncie przepisu art. 4 pkt 18, na których podmiotowości prawnej oparta jest następnie możliwość działania spółki cywilnej w obrocie, to najlepszym kierunkiem wykładni wydaje się uzależnienie kwalifikacji poszczególnych spółek cywilnych od tego, kto w danym przypadku jest ich wspólnikiem. Jeżeli będą to osoby fizyczne, osoby prawne lub spółki osobowe, wówczas taka spółka cywilna powinna być traktowana na równi z nimi i dla kwalifikacji pod przepis art. 4 pkt 18 musi prowadzić działalność gospodarczą. W sytuacji natomiast, gdy wspólnikami danej spółki cywilnej będą zrzeszenia, powinna ona prowadzić regularną działalność gospodarczą, by zostać uznaną za przedsiębiorcę na gruncie

[130] *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D.Lubasz.
[131] Postanowienie SN z 24.10.2003 r., sygn. akt III CZP 67/039, LEX nr 131935

rozporządzenia ogólnego. Mogą zdarzyć się sytuacje, gdy wspólnicy spółki cywilnej będą należeć do różnych grup podmiotów wskazanych w przepisie art. 4 pkt 18. Wówczas ocena powinna być dokonywana na gruncie konkretnego stanu faktycznego po zbadaniu, do której z grup podmiotów bliżej jest danej spółce cywilnej. Przy tej ocenie należy brać pod uwagę wielkość udziałów wspólników z poszczególnych grup podmiotów[132].

Z punktu widzenia tematu pracy istotne w tym miejscu pozostaje, że dla kwalifikowania podmiotowych konstrukcji prawnych w kategoriach przedsiębiorców związanych RODO ważna jest zawarta tam w art. 82 ust.4, zasada która stanowi, że jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. O ile konstrukcja solidarnej odpowiedzialności wspólników spółki cywilnej za jej zobowiązania, wynikająca z art. 864 k.c. koresponduje z regulacją art. 82 ust. 4 RODO, o tyle kwalifikowanie jako zrzeszeń podmiotów działających w ramach np. umów o współdziałanie nie zwierających regulacji np. umownej odpowiedzialności solidarnej może prowadzić do trudności interpretacyjnych oceny wiążących ich stosunków prawnych oraz zastosowania art. 82 ust.4.

W prowadzonych rozważaniach problematycznym zagadnieniem pozostaje kwestia kwalifikacji prawnej podmiotów działających w ramach umów o współdziałanie takich jak konsorcjum, meta-konsorcjum, *pool*, *joint venture* i wynikająca z faktu braku kryteriów normatywnych, które pozwalałyby uznać je za jednostki organizacyjne. Ustawodawca, tak jak w przypadku osób prawnych w art. 33^1 k.c., stanowiącym podstawę normatywną do zaliczania do podmiotów prawa cywilnego jednostek organizacyjnych niebędących osobami prawnymi, którym ustawa przyznaje zdolność prawną, posłużył się normatywną metodą regulacji. W konsekwencji otwarta pozostaje kwestia differentia specifica jednostek organizacyjnych nieposiadających zdolności prawnej oraz kryteriów, którymi powinien kierować się ustawodawca, przyznając niektórym z nich zdolność prawną. Problem ten widoczny jest szczególnie w przypadku zjawisk zachodzących w rzeczywistości społecznej jakim są umowy o współdziałanie. Pojęcie „umów o współdziałanie" odnosi się do czynności prawnych, które można umiejscowić w systemie prawa pomiędzy typowymi umowami zobowiązaniowymi (art. 353 § 1 k.c.) a umowami powołującymi odrębne podmioty prawa cywilnego. Zalicza się do

[132] *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D.Lubasz.

nich rozmaite formy współdziałania, takie jak spółka cywilna, konsorcjum, meta-konsorcjum, pool, joint venture czy spółka cicha[133].

Pojęcie konsorcjum przez długi czas nie występowało w języku prawnym, choć jednocześnie dość często używano go w doktrynie i orzecznictwie dla opisywania umów zawieranych przez przedsiębiorców dla łącznej realizacji zadań gospodarczych. Brak podmiotowości prawnej konsorcjum powoduje, że jedyną spółką, z którą można porównać te konstrukcję, jest spółka uregulowana w art. 860 i n. k.c., czyli spółka cywilna[134]. Konsorcjum ma charakter zbliżony do spółki, lecz sposób współdziałania i cel są odmienne. Zamiast *affectio societatis*, typowego dla spółek i polegającego na woli związania się dla realizacji wspólnego celu8, w konsorcjum mamy do czynienia raczej z działaniem komplementarnym, podobnym do umów o podwykonawstwo. Uczestnicy konsorcjum wykluczają także możliwość budowania stosunków majątkowych zbliżonych do spółki cywilnej. Brak jest w nim majątku wspólnego, konsorcjum nie osiąga zysku dzielonego pomiędzy uczestników[135].

W praktyce odpowiedzialność w przypadku konsorcjum jest tylko zbliżona do odpowiedzialności wspólnika w spółce cywilnej[136], generalnie przyznaje się jednak, że konsorcjum niekoniecznie musi oznaczać podtyp spółki cywilnej, mimo (dość złudnego) podobieństwa obu konstrukcji. Co ciekawe, badania prawnoporównawcze wskazują na to, że podobna sytuacja ma miejsce w innych porządkach prawnych[137]. W świetle powyższego ocena kwalifikacji prawnej konsorcjum jako jednostki organizacyjnej w rozumieniu art. 4 pkt. 18 RODO i zobowiązanej jako administrator lub podmiot przetwarzający nie wydaje się możliwa bez każdorazowej analizy treści stosunku prawnego powołującego konsorcjum.

Zestawiając powyższe rozważania z definicją przedsiębiorcy na gruncie prawa polskiego, dochodzimy do wniosku, że aby zrzeszenia mogły być uznane za przedsiębiorcę na gruncie przepisu art. 4 pkt 18, muszą prowadzić regularną działalność gospodarczą. Prawodawca unijny dla tej kategorii podmiotów dodał zatem dodatkowy element do definicji przedsiębiorcy w postaci regularności prowadzenia działalności gospodarczej. Przedstawiciele doktryny opowiadają się za stanowiskiem, że omawiane pojęcie przedsiębiorcy należy rozumieć w kontekście jego autonomicznej definicji funkcjonującej w prawie UE, którego częścią jest RODO, nie zaś poprzez odniesienia do definicji funkcjonujących w prawie polskim

[133] M. Klaja, *O potrzebie regulacji umów o współdziałanie*, PPE 2019/4/49.
[134] Sz. Byczko, *Uwagi o charakterze prawnym konsorcjum*, „Studia PrawnoEkonomiczne" 2021/121.
[135] Sz. Byczko, *Konsorcjum w orzecznictwie Sądu Najwyższego*. *Księga jubileuszowa ku czci Prof. W.J. Katnera*, Łódź 2022, s. 120.
[136] Sz. Byczko, *Consortia in Central And Easten Europe*, Gdańsk 2019, s. 93.
[137] Sz. Byczko, *Konsorcjum w orzecznictwie*..., s. 121.

(art. 43^1 k.c. czy art. 4 prawa przedsiębiorców). Niedopuszczalność dekodowania pojęć używanych w prawie UE, w braku odesłań do prawa krajowego, jest ugruntowana w orzecznictwie Trybunału Sprawiedliwości[138]. Inni podnoszą także, że kategoria przedsiębiorców w rozumieniu UE zdecydowanie wykracza poza ramy definicyjne określane prawem krajowym. Państwa członkowskie są zatem na mocy regulacji unijnych zmuszone do dokonywania indywidualnej oceny każdego stanu faktycznego i to na jej podstawie winny dokonywać kwalifikacji podmiotów do kategorii przedsiębiorców, oczywiście w sytuacjach, kiedy czynią to na potrzeby realizacji norm unijnych[139].

W tym miejscu dla porządku dodać należy, że pojęcie działalności gospodarczej zawarte jest w art. 75 TFUE, który jednak nie precyzuje jego znaczenia. Jak wskazuje się w literaturze, w orzecznictwie TSUE i piśmiennictwie, powszechnie działalność gospodarczą utożsamia się z przedsiębiorczością i świadczeniem usług. Przyjmuje się bowiem, że działalność gospodarcza to wykonywanie przedsiębiorczości i świadczenie usług[140]. Zgodnie z orzecznictwem ETS, każda działalność polegająca na oferowaniu towarów i usług na danym rynku stanowi działalność gospodarczą[141]. Artykuł 57 TFUE, stanowi, że „usługami w rozumieniu Traktatów są świadczenia wykonywane zwykle za wynagrodzeniem w zakresie, w jakim nie są objęte postanowieniami o swobodnym przepływie towarów, kapitału i osób".

Przetwarzanie danych osobowych dotyczących osób fizycznych prowadzących działalność gospodarczą

Innym istotnym zagadnieniem dotyczącym omawianych problemów jest kwestia przetwarzania danych osobowych dotyczących osób fizycznych prowadzących działalność gospodarczą. Obecnie nie ma wątpliwości, że RODO stosuje się do przetwarzania danych osobowych dotyczących osób fizycznych prowadzących działalność gospodarczą. Zagadnienie to nie było jednoznaczne przed RODO z uwagi brak jednolitości stanowisk piśmiennictwa w tym zakresie. Część autorów opowiadała się za uznaniem danych o działalności gospodarczej za dane osobowe, chociażby z racji tego, iż w wielu sytuacjach prowadzą do identyfikacji konkretnych osób[142].

[138] M. Górski; zob. np. wyrok TSWE z 18.02.1970 r., 38/69, *Komisja v. Włochy*, ECLI:EU:C:1970:11.
[139] P. Litwiński *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021.
[140] P. Litwiński *Ogólne rozporządzenie...*; por. M. Etel, *Pojęcie przedsiębiorcy...*, s. 99.
[141] Wyrok ETS z 18.6.1998 r. w sprawie C-35/96, *Komisja przeciwko Włochom*, Legalis.
[142] A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 25; J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 347.

Inne stanowisko zaprezentował Generalny Inspektor Ochrony Danych Osobowych, według, którego ustawa o ochronie danych osobowych nie miała zastosowania do przetwarzania informacji o podmiotach gospodarczych. Stanowisko to zostało także podzielone przez NSA w wyroku z 28.11.2002 r.[143], w którym Sąd uznał, że osoba decydująca się na prowadzenie działalności gospodarczej godzi się na ograniczenie swojego prawa do prywatności. Kluczowe jednak znaczenie dla rozwiązania przedstawionego problemu miała nowelizacja ustawy z dnia 19.11.1999 r. – Prawo o działalności gospodarczej (Dz. U. Nr 101, poz. 1178, ze zm.)[144], na mocy której dodano art. 7a, wyłączający spod ochrony wynikającej z ustawy o ochronie danych osobowych, dane zawarte w ewidencji działalności gospodarczej. Przepis ten wyraźnie rozstrzygnął kwestię budzącą wcześniejsze wątpliwości. Komentatorzy w tamtym czasie wskazywali na niefortunność tego rozwiązania, wskazując na korzystniejsze regulacje polegające na dopuszczeniu przetwarzania danych o przedsiębiorcach będących osobami fizycznymi w zakresie związanym z prowadzoną przez te podmioty działalnością gospodarczą na nieco łagodniejszych zasadach[145].

Stosowanie RODO wobec osób prawnych i jednostek organizacyjnych

Kolejnym zagadnieniem istotnym dla zagadnień omawianej pracy jest zakres ochrony jakie RODO przyznaje osobom prawnym i jednostkom organizacyjnym mającym zdolność prawną, a nieposiadającym osobowości prawnej. W motywie 14 stwierdzono, że „rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw (zgodnie z angielską wersją *undertaking*) będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. W literaturze przedmiotu wskazuje się jednak, że w pewnym (ograniczonym) zakresie informacje dotyczące osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej prowadzących działalność gospodarczą (przedsiębiorców) mogą być chronione chociażby na podstawie konstrukcji tajemnicy przedsiębiorstwa[146]. Stanowisko w tym przedmiocie zajął także Trybunał Sprawiedliwości w sprawach połączonych C-92/09 oraz

[143] II SA 3389/01, MoP 2003/3, poz. 99.
[144] Ustawa z dnia 19.11.1999 r. – Prawo o działalności gospodarczej (Dz.U. Nr 101, poz. 1178, ze zm.).
[145] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 349; także P. Fajgielski, *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną* [w:] *Dysfunkcje publicznego prawa gospodarczego*, red. E. Kruk, G. Lubeńczuk, M. Zdyb, Warszawa 2018, s. 65–74.
[146] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*) [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2021, s. 108.

C-93/09[147], stwierdzając, że osoby prawne mogą się powoływać na ochronę z art. 7 i 8 KPP w odniesieniu do identyfikacji osobowej właśnie wtedy, gdy nazwa oficjalna osoby prawnej identyfikuje jedną lub więcej osób fizycznych. Także w opinii Grupy Roboczej Art. 29 zawarta została konstatacja, że jeżeli kryteria „treść", „cel" lub „skutek" pozwalają na uznanie informacji o osobie prawnej lub o przedsiębiorstwie za „dotyczącą" osoby fizycznej, należy uznać je za dane osobowe i stosować przepisy o ochronie danych osobowych[148]. Zdaniem komentatorów rozporządzenie nie odnosi się w żaden szczególny sposób do danych osób fizycznych prowadzących działalność gospodarczą. Niewątpliwie dane te mieszczą się w zakresie desygnatów wyznaczonych przez definicję zawartą w art. 4 pkt 1 RODO. Należy zatem podzielić zapatrywanie wyrażone w literaturze, iż RODO znajduje w całości zastosowanie do przetwarzania danych osobowych dotyczących osób fizycznych prowadzących działalność gospodarczą i nie istnieją żadne podstawy do wyodrębniania danych osobowych osób fizycznych prowadzących działalność gospodarczą spośród uniwersum danych osobowych objętych jego zastosowaniem[149]. Brak przyznania ochrony danym osobowym osób prawnych dotyczących firmy, formy oraz danych kontaktowych nie oznacza, że RODO nie dotyczy administratora lub podmiotu przetwarzającego, który jest przedsiębiorcą i ma status osoby prawnej.

Kontynuując rozważania na temat ochrony przyznanej przez RODO osobom prawnym i jednostkom organizacyjnym, należy zwrócić uwagę na prezentowany w doktrynie głos wskazujący na walor praktyczny występowania w definicji z art. 4 ust. 18 RODO kategorii administratorów - przedsiębiorców niebędących osobami fizycznymi, prawnymi lub organami publicznymi w aspekcie odpowiedzialności cywilnej. W tym zakresie A. Sobczyk jako przykład z sektora prywatnego podaje ułomne osoby prawne (osobowe spółki handlowe, spółki kapitałowe w organizacji) oraz podnosi problem wprowadzonej w RODO definicji grupy przedsiębiorstw. Według RODO grupa przedsiębiorstw określana jest jako przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane, co w ocenie A. Sobczyka spełnia definicję nie tylko jednostki organizacyjnej, ale wręcz organizacji, która składa się z osób prawnych. Tym samym zasadne jest przyjęcie, że grupa przedsiębiorstw lub jej krajowe odpowiedniki mogą być administratorami danych osobowych, [150] które to stanowisko może stanowić o początku dyskusji w doktrynie na temat statusu grupy przedsiębiorstw jako formy

[147] Wyrok TS w sprawach połączonych C-92/09 oraz C-93/09
[148] Opinia 4/2007 Grupy Roboczej Art 29 w sprawie pojęcia danych osobowych z 20.06.2007 r. WP 136, s. 24
[149] *Rozporządzenie UE*, red. P. Litiwński, komentarz do art. 4 pkt 1, Nb 10
[150] A. Sobczyk, *RODO. Rozproszona władza publiczna*, Kraków 2020, s. 109.

omawianej instytucji zrzeszenia, zwłaszcza po nowelizacji k.s.h. dotyczącej przepisów holdingowych.

Powyższe rozważania można podsumować stwierdzeniem, że wyłączenie określonych podmiotów z zakresu podmiotowego definicji "przedsiębiorcy" nie będzie zawsze oznaczać wyłączenia ich z zakresu podmiotów zobowiązanych do stosowania RODO. Posiadanie statusu przedsiębiorcy będzie jednak zawsze wiązało się z przypisaniem roli administratora lub podmiotu przetwarzającego z uwagi na fakt, że rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową. Kryterium prowadzenia działalności gospodarczej związane z definicją przedsiębiorcy w ujęciu europejskim i krajowym warunkuje, że przetwarzanie danych osobowych przez przedsiębiorcę objęte jest RODO. Stany faktyczne związane z celem i sposobem przetwarzania danych osobowych będą na gruncie RODO decydować o przypisaniu przedsiębiorcy określonej roli administratora lub podmiotu przetwarzającego. Z wyjątkiem przypadków, kiedy status administratora przyznawany jest konkretnemu podmiotowi bezpośrednio w przepisach prawa UE albo prawa państwa członkowskiego, kwalifikacji danego podmiotu jako „administratora" dokonuje się na podstawie ustaleń faktycznych, a więc całokształtu okoliczności przetwarzania danych osobowych w danym przypadku. Skoro zakwalifikowanie konkretnego podmiotu jako administratora uzależnione jest wyłącznie od okoliczności faktycznych podkreślenia wymaga, że uzyskanie tego statusu nie jest możliwe poprzez postanowienia umowne ani też czynność jednostronną, z której wynikałoby nadanie danemu podmiotowi takiego statusu[151]. Uznanie zaś, że konkretny podmiot jest administratorem, jest równoznaczne z przypisaniem mu szeregu obowiązków określonych w RODO oraz odpowiedzialności za przetwarzanie danych dokonywanych przez ten podmiot samodzielnie, jak również za pośrednictwem jego personelu oraz podmiotów wobec niego zewnętrznych. W pewnym zakresie także te podmioty ponoszą odpowiedzialność; nie jest to jednak odpowiedzialność tożsama z odpowiedzialnością administratora. Ogólnie, w zakresie przetwarzania danych osobowych administrator odpowiada nie tylko za własne działania i decyzje i ponosi konsekwencje nie tylko swoich działań i zaniechań, ale także innych podmiotów, których przybrał do dokonywanego w jego imieniu i na jego rzecz przetwarzania danych osobowych (Opinia 1/2010 Grupy Roboczej Art. 29). Najistotniejszą konsekwencją prawną bycia administratorem jest prawna odpowiedzialność za przestrzeganie obowiązków wynikających z prawa o ochronie danych osobowych. Status ten

[151] M. Sakowska-Baryła [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 96.

może przysługiwać jedynie podmiotowi, który zgodnie z obowiązującym prawem może być pociągnięty do odpowiedzialności prawnej, a więc posiadającemu zdolność prawną[152].

[152] M. Sakowska-Baryła [w:] *Ogólne rozporządzenie o ochronie*..., red. M. Sakowska-Baryła, s.104.

ROZDZIAŁ II.

Koncepcja odpowiedzialności cywilnej prawa do ochrony danych osobowych

Zasady ochrony danych osobowych na gruncie Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 roku w sprawie ochrony osób fizycznych

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych w art. 23 zobowiązywała państwa członkowskie do zapewnienia, aby każda osoba, która w wyniku niezgodnej z prawem operacji przetwarzania danych poniosła szkodę, uzyskała odszkodowanie, wskazując jednocześnie, że administrator danych może zastać zwolniony od tej odpowiedzialności w całości lub w części, jeżeli udowodni, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę. W motywie 18 dyrektywy 95/46/WE podkreślone zostało, że aby nie dopuścić do pozbawienia jednostek ochrony, do której mają prawo na mocy niniejszej dyrektywy, wszelkie przetwarzanie danych osobowych we Wspólnocie musi być przeprowadzane zgodnie z ustawodawstwem jednego z Państw Członkowskich. W dalszej części w motywie 55 wskazano, że na wypadek nieprzestrzegania przez administratora danych praw osób, których dane dotyczą, ustawodawstwa krajowe muszą przewidywać odpowiednie środki zaskarżenia. Szkody, jakie osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych, zgodnie z tym motywem muszą być wyrównane przez administratora danych, który może być zwolniony z odpowiedzialności w przypadku udowodnienia, że szkoda nie powstała z jego winy, szczególnie wówczas gdy stwierdzi wystąpienie winy po stronie osoby, której dane dotyczą lub w przypadku siły wyższej. Zgodnie z postanowieniami dyrektywy 95/46/WE należy nakładać sankcje na każdą osobę, podlegającą prawu prywatnemu lub publicznemu, która nie spełnia wymagań wynikających z przyjętych krajowych przepisów wprowadzonych na podstawie niniejszej dyrektywy.

Kluczowe znaczenie dla standardu ochrony prawa do prywatności i danych osobowych wyznaczonego w dyrektywie 95/46/WE miała zatem konkretyzacja wskazanej regulacji dokonana w drodze implementacji krajowej i wypracowanego na jej podstawie orzecznictwa. Dyrektywa jako akt prawa wtórnego Unii Europejskiej dawała państwom członkowskim podstawę do uszczegółowienia zakresu ochrony danych osobowych poprzez postanowienia, których celem powinno było być ich respektowanie przez wiele podmiotów zapewniających różny poziom, zakres i stopień ochrony prywatności. Implementacja dyrektywy 95/46/WE

pozwalała w obszarze odpowiedzialności na objęcie ochroną odpowiedniej na gruncie krajowym liczby sytuacji i stanów prawnych, które wraz ze zmianami technologicznymi powinny takiej ochronie podlegać. Z uwagi na odrębności przepisów krajowych funkcjonujących w różnych tradycjach i kulturach prawnych takie działanie nie mogło służyć jednak ujednoliceniu zasad ochrony. Zagadnienie braku spójności na poziomie wspólnotowym zasad odpowiedzialności oraz potrzeby ujednolicenia przepisów, gwarantującej większą pewność prawną, spójność i stabilność zasad ochrony podnoszone było już w publikacjach dotyczących idei stworzenia europejskiego Kodeksu cywilnego[153].

Analizę zagadnienia zasad ochrony danych osobowych w okresie obowiązywania dyrektywy 95/46/WE na gruncie krajowym należy rozpocząć zatem od zaprezentowania regulacji stosowania sankcji cywilnych za naruszenia przepisów o ochronie danych osobowych w poprzednio obowiązującym stanie prawnym.

Polska ustawa, implementując do naszego porządku prawnego dyrektywę 95/46/WE, nie przewidywała żadnych przepisów szczególnych, odnoszących się do cywilnoprawnej odpowiedzialności administratora danych. Brak wyraźnego zakresu i konkretnej sankcji wskazywać mógł na niepewność takiej ochrony i możliwość nadużyć, gdyby nie praktyka która odpowiedzialność administratora opierała na normach Kodeksu cywilnego.

W piśmiennictwie pojawiły się w konsekwencji tego głosy, że „kwestia kompensacji szkody majątkowej, spowodowanej naruszeniem przepisów o ochronie danych osobowych, wydawała się w okresie obowiązywania Dyrektywy jasna. Znajdowały tu bowiem zastosowanie ogólne zasady odpowiedzialności deliktowej. Natomiast problematyka naprawienia szkody niemajątkowej była złożona, ponieważ w polskim prawie cywilnym naprawienie szkody niemajątkowej przewidują przepisy odnoszące się do ochrony dóbr osobistych oraz szkód na osobie, co powodowało, że zastosowanie ogólnej odpowiedzialności deliktowej miało miejsce w przypadku kompensacji szkód niemajątkowych, niemieszczących się w hipotezach norm statuujących ochronę dóbr osobistych”[154].

Inni przedstawiciele doktryny stoją na stanowisku, że „oferowana przez prawo cywilne ochrona ochrony w razie naruszeń dóbr osobistych, w tym sfery prywatności i tożsamości ma jednak charakter następczy – następuje jedynie w sytuacji, w której dobro osobiste zostało zagrożone cudzym działaniem (zob. art. 23 i art. 24 k.c.). Te klasyczne cywilnoprawne instrumenty ochrony dóbr osobistych w dobie postępującej komputeryzacji i wskazywanych

[153] J. Pisuliński, *Kilka pytań o europejski kodeks cywilny*, „Transformacje prawa prywatnego” 2006/2, s. 99–106.
[154] F. Morawski *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według ogólnego. Rozporządzenia o ochronie danych osobowych*, „Acta Iuris Stetinensis” 2019/2/26.

już niebezpieczeństw dla prywatności jednostki okazały się niewystarczające. Konstrukcja prawa do ochrony danych osobowych z założenia ma gwarantować uprawnienia o charakterze prewencyjnym (zapobiegawczym), których celem jest niedopuszczenie do powstawania zagrożeń"[155]. W ślad za przedstawicielami doktryny wskazać można, że w dobie nowych rozwiązań technologicznych niewystarczające okazały się klasyczne cywilnoprawne instrumenty ochrony dóbr osobistych, które nie wywierały skutku prewencyjnego, a miały zastosowanie dopiero w chwili samego zagrożenia[156].

Powyższe poglądy powinny zostać uzupełnione o pogląd, że Kodeks cywilny zawiera konstrukcje, których zastosowanie może spełnić oczekiwania wskazywane w prezentowanych poglądach, kwestionujących znaczenie dla ochrony danych osobowych obowiązujących jeszcze przed RODO regulacji. Na uzasadnienie podnoszonej tezy wskazać należy art. 439 k.c., który stanowi, że ten komu wskutek zachowania się innej osoby zagraża bezpośrednio szkoda, może żądać, ażeby osoba ta przedsięwzięła środki niezbędne do odwrócenia grożącego niebezpieczeństwa oraz art. 24 k.c., który formułuje roszczenie o zaniechanie naruszeń w następującym brzmieniu: „ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne".

Artykuł 439 k.c. wprowadził do polskiego systemu prawa cywilnego instytucję statuującą generalne roszczenie prewencyjne – skargę prewencyjną, umożliwiającą osobie bezpośrednio zagrożonej szkodą domaganie się od podmiotu odpowiedzialnego za stan takiego zagrożenia, aby przedsięwziął on środki niezbędne dla odwrócenia grożącego niebezpieczeństwa, a w razie potrzeby dał także odpowiednie zabezpieczenie Z treści powołanego przepisu wynika przede wszystkim to, że wzorem innych przypadków odpowiedzialności uregulowanych w Tytule VI Księgi Trzeciej Kodeksu cywilnego roszczenie bezpośrednio zagrożonego szkodą względem odpowiedzialnego za stan takiego zagrożenia powstaje z mocy samego prawa. Fakt, że szkoda nie jest przesłanką uregulowanej w ten sposób odpowiedzialności cywilnej, powoduje, iż nie przybiera ona postaci odpowiedzialności odszkodowawczej. Elementem ujawniającym jednak związek tej odpowiedzialności z reżimem odpowiedzialności odszkodowawczej *ex delicto* jest to, iż – jak się powszechnie przyjmuje – skarga przewidziana w art. 439 k.c. przysługuje tylko w przypadku, w którym stan zagrożenia szkodą prawie na pewno zmierza do przekształcenia się w stan wyrządzenia szkody

[155] M. Sakowska-Baryła, *Prawo do ochrony...*, s. 41.

[156] S. Kotecka-Kral, *Sądowe środki ochrony prawnej i jurysdykcja krajowa w zakresie spraw związanych z ochroną danych osobowych na mocy rozporządzenia. Księga Jubileuszowa dedykowana Profesorowi Januszowi Jankowskiemu*, „Ars in vita. Ars in iure" 2016/679, s. 829–856.

(poszkodowania), do której naprawienia zastosowanie znajdzie jedna z podstaw odpowiedzialności odszkodowawczej z tytułu czynów niedozwolonych.[157] Zgodnie z przyjętą praktyką zastosowanie powyższych przepisów ma miejsce w sytuacjach zagrożenia, tj. zanim jeszcze doszło do naruszenia. R. Kasprzyk twierdził, że celem art. 439 k.c. jest wyposażenie osoby, która jest zagrożona wyrządzeniem szkody w roszczenie skuteczne przeciwko każdemu grożącemu. Artykuł ten stanowi zatem podstawę normatywną do wymuszania ogólnych obowiązków właściwego zachowania się, które przybierają skonkretyzowaną postać obowiązku przedsięwzięcia środków niezbędnych w celu odwrócenia grożącego niebezpieczeństwa[158].

W piśmiennictwie podkreślano, że nie każde sprzeczne z ustawą przetwarzanie danych osobowych stanowiło pod rządami starych przepisów jednocześnie naruszenie dóbr osobistych osoby, której dane są przetwarzane, a zakres pojęciowy dóbr osobistych i danych osobowych nie był tożsamy[159]. Tym samym nie każde naruszenie przepisów o ochronie danych osobowych naruszało sferę prywatności osoby, której dane są przetwarzane. W doktrynie wskazywało się, że pomiędzy ochroną prywatności a ochroną danych osobowych zachodził stosunek krzyżowania się[160]. Niektórzy przedstawiciele doktryny wręcz wskazywali, że wszystkie dane dotyczące osoby zidentyfikowanej lub możliwej do zidentyfikowania zawierają się w sferze prywatności tej osoby o tyle, o ile można te dane powiązać z konkretną osobą[161]. Pojawiały się także głosy, by ogólnie uznać dane osobowe za kolejne nowe dobro osobiste[162].

Powyższe stanowiska nie powinny pozostawać bez wpływu na interpretację obecnie obowiązujących przepisów. Prawo do ochrony danych osobowych było i nadal jest wyrazem ochrony godności osoby ludzkiej i jej prawa do postępowania zgodnie ze swoim sumieniem. Ochrona danych osobowych koresponduje z wolnością osobistą i chroni pewne jej aspekty w sytuacji zagrożeń stwarzanych przez nowoczesne technologie. Celem ochrony jest zagwarantowanie decydowania w sferze informacji przez jednostkę, a zarazem zapewnienie realizacji jej prawnie chronionego interesu do zachowania prywatności i intymności[163].

---

[157] Z. Banaszczyk, *Możliwość zastosowania art. 439 k.c. w odniesieniu do przypadków sprowadzenia stanu bezpośredniego niebezpieczeństwa wyrządzenia szkody niezgodnym z prawem wykonywaniem władzy publicznej* [w:] *Non omne quod licet honestum est. Studia z prawa cywilnego i handlowego w 50-lecie pracy naukowej Profesora Wojciecha Jana Katnera*, Warszawa 2022, s. 72

[158] R. Kasprzyk, *Podstawa roszczenia prewencyjnego*, „Palestra" 1989 nr 3/375, t. 33, s. 28.

[159] F. Morawski, *Odpowiedzialność cywilna administratora...*

[160] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych*, Warszawa 2015, s. 143.

[161] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych*, Warszawa 2015, s. 143.

[162] F. Morawski, *Odpowiedzialność cywilna administratora*... ,za: T.A.J. Banyś, J. Łuczak, *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, Wrocław 2013, s. 352.

[163] B. Drzewiecka-Konieczna, *Inspektor ochrony danych w strukturze i funkcjonowaniu naczelnego organu administracji publicznej*, Warszawa 2019, s. 11.

Takie rozumienie prawa do ochrony danych osobowych wymaga analizy zagadnienia jak zasady ochrony danych osobowych, wynikające z Dyrektywy wpływają na nowy porządek prawny, związany z rozpoczęciem stosowania RODO. Analiza taka dokonana zostanie w dalszej części pracy. W tym miejscu podkreślenia wymaga natomiast, że w motywach RODO mamy odniesienie do rozumienia pojęcia szkody i zasad odpowiedzialności określone w sposób nawiązujący do postanowień Dyrektywy. Dlatego dla pełnego obrazu badanego problemu konieczne jest dla porządku omówienie pojęć dóbr osobistych i prywatności i ich rozumienia pod rządami przepisów SUODO.

Pojęcie dóbr osobistych i prywatności

Analiza pojęcia danych osobowych dokonana w rozdziale I z uwagi na postawione powyżej tezy stosunku krzyżowania się ochrony danych osobowych z dobrami osobistymi i ochroną prywatności wymaga uzupełnienia o analizę także tych pojęć z perspektywy ich wspólnych cech**.**

W pierwszej kolejności powiedzieć należy, że dla ochrony dóbr osobistych szczególne znaczenie ma Powszechna Deklaracja Praw Człowieka uchwalona przez Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych dnia 10.12.1948 r [164], która stanowi, że:

1. każdy człowiek ma prawo do życia, wolności i bezpieczeństwa swojej osoby;
2. nikt nie może pozostawać w stanie niewolnictwa lub służebności; niewolnictwo i handel niewolnikami we wszystkich formach będą zakazane;
3. nikt nie może być poddany torturom lub okrutnemu, nieludzkiemu albo upokarzającemu traktowaniu lub karaniu;
4. każdy człowiek ma prawo do wolności myśli, sumienia i religii; prawo to obejmuje wolność zmiany religii lub wiary oraz wolność głoszenia swej religii lub wiary, bądź indywidualnie, bądź wespół z innymi ludźmi, publicznie lub prywatnie poprzez nauczanie, praktykowanie, uprawianie kultu i praktyk religijnych;
5. każdy człowiek ma prawo do wolności poglądów i swobodnego ich wyrażania; prawo to obejmuje swobodę posiadania niezależnych poglądów, poszukiwania, otrzymywania

[164] Trzecia Sesja Ogólnego Zgromadzenia ONZ, obradująca w Paryżu, uchwaliła 10.12.1948 r. Powszechną Deklarację Praw Człowieka. Dokument ten stanowi niewątpliwie jedno z największych i najtrwalszych osiągnięć ONZ. Przetłumaczona na większość języków świata Powszechna Deklaracja Praw Człowieka zbiera oraz porządkuje osiągnięcia i postulaty człowieka, który od wielu setek lat toczy nieskończoną jeszcze walkę o swoją wolność i swoją godność.

i rozpowszechniania informacji i idei wszelkimi środkami, bez względu na granice [165]. Zgodnie z art. 12 Powszechnej Deklaracji Praw Człowieka „nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu”[7]. Podobna teza została sformułowana w art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych w myśl którego: „nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. Każdy ma prawo do ochrony prawnej przed tego rodzaju integracjami i zamachami”[8] .

Przywołane powyżej postanowienia uniwersalnych systemów praw człowieka silnie wpływały na twórców systemów w poszczególnych państwach. W rozdziale I pracy część z nich została omówiona, dlatego w tym miejscu warto te rozważania uzupełnić jedynie o twierdzenie, że prawo do prywatności znalazło swoje miejsce niemal w każdym z nich.

Należy powiedzieć również o: (Pan)Amerykańskiej Konwencji Praw Człowieka, sporządzonej w San José 22.11.1969 r. Oddziałuje ona na obszar krajów Ameryki Południowej oraz wysp karaibskich, stąd też konwencję nazywa się niekiedy latynosko-karaibską. Prawo do prywatności uregulowane zostało w niej w art. 11, który stanowi, że każdy ma prawo do poszanowania jego honoru oraz uznania jego godności. Ponadto nikt nie może być obiektem samowolnej lub niewłaściwej ingerencji w jego życie prywatne, rodzinne, mir domowy, korespondencję albo bezprawnych ataków na jego honor lub reputację. Każdemu przyznano ponadto prawo do ochrony prawnej przed taką ingerencją lub atakami.

Podstawą funkcjonowania omawianych zagadnień na kontynencie afrykańskim jest Afrykańska Karta Praw Człowieka i Ludów, która weszła w życie 21.10.1986 r. Nie przewidziano w niej wprost prawa do prywatności, ale zawiera ona takie postanowienia, które owe prawo pozwalają wyinterpretować. Dla porządku wypada także przytoczyć regulacje obowiązujące w systemie stworzonym pod auspicjami Ligi Państw Arabskich, z których najistotniejsza jest Deklaracja Praw Człowieka w Islamie z 5.08.1990 r. W tymże akcie prawnym w art. 18 potwierdzono prawo każdego do prywatności w prowadzeniu swoich spraw osobistych, we własnym domu, wśród rodziny, z poszanowaniem własności i osobistych relacji. Zabroniono przy tym szpiegowania jednostki, poddawania jej nadzorowi czy oczerniania

[165] I. Lewandowska-Malec, *Dobra osobiste na tle prawa międzynarodowego*, Warszawa 2017, https://sip-1legalis-1pl-1v27i8rcf003d.han3.lib.uni.lodz.pl/document-full.seam?documentId=mjxw62zogi3damjxgm3tknzogezq&refSource=toc#tabs-metrical-info

dobrego imienia. Ustalono, że państwo ma obowiązek chronić jednostki przed samowolną ingerencją. Z prawem tym skorelowano nienaruszalność miru domowego Deklaracja nie ma jednak mocy wiążącej.

Odmienny charakter ma Arabska Karta Praw Człowieka z 22.05.2004 r. Dokument ten po wielu latach od uchwalenia pierwotnej wersji (w 1994 r.) wszedł w życie 15.03.2008 r. W art. 21 tego aktu prawnego stwierdzono, że nikt nie może zostać poddany niezgodnemu z prawem naruszeniu prywatności, życia rodzinnego, miru domowego i korespondencji oraz bezprawnemu atakowi na jego honor i reputację. Ponadto w art. 16 pkt 8 zawarto szczególną regulację, na wypadek oskarżenia danej osoby o popełnienie przestępstwa. Stosownie do tej jednostki redakcyjnej ma jej zostać w takim wypadku zapewnione bezpieczeństwo i prywatność[166].

Na poziomie krajowym uregulowanie w przedmiocie ochrony dóbr osobistych zostało ukonstytuowanie art. 30 Konstytucji RP. W myśl treści art. 30 „przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych." Jego rezultatem jest art. 31 ust. 2 zgodnie z którym „każdy jest obowiązany szanować wolności i prawa innych. Nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje, a ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw"[167].

Konstytucja RP proklamuje poszanowanie godności już na wstępie – w Preambule, wzywając wszystkich ją stosujących, aby czynili to, dbając o zachowanie przyrodzonej godności człowieka, ponadto w art. 233 ust. 1 szczególnie akcentuje rangę godności człowieka poprzez bezwzględny zakaz jej ograniczania w razie wprowadzenia stanu nadzwyczajnego. To wskazanie na zasadę godności w Preambule Konstytucji RP, a następnie w art. 30 otwierającym katalog konstytucyjnych wolności i praw jednostki w przywołanym wyżej ujęciu, jako najważniejszej i wzorcowej wartości, w której są one zakotwiczone, ma istotne znaczenie także z perspektywy charakteru Konstytucji RP jako szczególnego aktu prawnego. Konstytucja RP bowiem – jak dowodzi A. Młynarska-Sobaczewska – stanowi źródło oraz reguluje granice władzy w państwie, a jednocześnie jej treść odzwierciedla „system operacyjny wspólnoty

[166] J. Rzucidło, *Prawo do prywatności...*, s. 156
[167] I. Lewandowska-Malec, *Dobra osobiste...*

podporządkowanej tej regulacji". Konstytucyjna zasada godności człowieka współcześnie jest uznana za centralną kategorię systemu prawnego. Przynależy ona człowiekowi niezależnie od jakichkolwiek jego cech, właściwości czy sposobu postępowania. To kategoria aksjologiczno-ontyczna, która jako aksjomatyczna cecha każdego człowieka przysługuje mu właśnie z racji bycia człowiekiem i ani nie wymaga uprzedniego zdobycia, ani nie może zostać przez człowieka utracona. Odróżnia ją to od godności osobowościowej, która zależy od posiadania określonych cech lub właściwości i którą można utracić[168].

Z pojęciem godności związana jest konstytucjonalizacja konstrukcji dóbr osobistych jak nazywa ją M. Safjan, który w ustawie zasadniczej upatruje źródła wszystkich tych dóbr, a konkretnie w art. 30 stanowiącym o niezbywalnej godności osobowej człowieka. Jej odpowiednikiem na gruncie Kodeksu cywilnego ma być ogólne prawo osobistości. Poszczególne dobra są, zdaniem Autora, wycinkami tego ogólnego prawa. Natomiast o ich wspólnym korzeniu świadczyć może ich zachodzenie na siebie, przecinanie się ich zakresów[169]. Powołując wspomniany powyżej pogląd jako jedno ze stanowisk monistycznej koncepcji praw podmiotowych, zasygnalizować w tym miejscu należy fakt sporu doktrynalnego omawianej koncepcji z ideą pluralistyczną i podkreślić, że pojęcie dobra osobistego można odnaleźć w wielu aktach normatywnych, jednak w żadnym z nich nie znajdziemy wyjaśnienia, czym one w istocie są.

Dla porządku przypomnieć w tym miejscu należy, że w literaturze prawniczej dobra osobiste są traktowane także jako wartości niemajątkowe, związane z osobowością człowieka, uznawane powszechnie w danym społeczeństwie[170]. W prawie polskim nie funkcjonuje zatem ich legalna definicja. Z pewnością nie można tak traktować art. 23 k.c., który stanowi, że w szczególności są nimi zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, dodając jednocześnie, że pozostają one pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Istotne jest, że doktryna prawa cywilnego zajęła się dogłębnie analizowaniem, czym są dobra osobiste. Jednakże powstałe definicje różnią się od siebie[171], zależnie od tego, czy dany autor przyjął

[168] M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej*, Warszawa 2022, s. 311.
[169] M. Safjan, *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych*, KPP 2002/1, s. 244.
[170] A. Szpunar, *Ochrona dóbr osobistych*, Warszawa 1979, s. 106.
[171] F. Zoll wyróżnił sześć kryteriów, dzięki którym można określić prawa osobiste, a mianowicie: brak przedmiotu, nierozerwalna więź z podmiotem, dla którego istnieją, mogą mieć wartość niemajątkową, niemożność ustawowego określenia ich rozciągłości, ich treść łączy się czasem ze sferą innych praw podmiotowych, a także są prawami jednolitymi, a nie sumą uprawnień przysługujących człowiekowi (zob: F. Zoll, *Prawa osobiste w zarysie ze stanowiska prawa prywatnego austriackiego*, „Czasopismo Prawnicze i Ekonomiczne", Kraków 1903,

rozumienie obiektywne czy subiektywne. Sięgając zaś do orzecznictwa, możemy w nim znaleźć definicję dóbr osobistych wypracowaną przez Sąd Najwyższy, np. w wyroku z 10.6.1977 r.[172], w którym zdefuniowano, że dobro osobiste to ogół czynników mających na celu zapewnienie obywatelowi rozwoju jego osobowości, ochronę jego egzystencji i zapewnienie mu prawa do korzystania z tych dóbr, które są dostępne na danym etapie rozwoju społeczno-ekonomicznego społeczeństwa, a które sprzyjają zachowaniu cech odrębności i związaniu ze społeczeństwem, w którym żyje.

Dla analizowanych w pracy zagadnień kwestią zasadniczą jesst problem konieczności oddzielenia samego dobra osobistego od konstrukcji, na której zasadza się jego ochrona. Nie wystarczy przecież naruszenie samego dobra, by domagać się ochrony prawnej. Działanie naruszyciela może być bowiem sankcjonowane przez normę prawną. Dopiero wtargnięcie w głębszą sferę zrodzi odpowiedzialność cywilną. W zakresie dóbr osobistych w polskiej doktrynie wyróżnić można dwa opozycyjne względem siebie stanowiska. Dominujący pogląd opiera się na konstrukcji bezwzględnych praw podmiotowych, natomiast według drugiego ochrona realizuje się za pomocą ustanowionych nakazów i zakazów postępowania[173].

Na potrzeby niniejszej pracy przyjęta została koncepcja krzyżowania się praw do ochrony dóbr osobistych i danych osobowych, co oznacza, że poczynione rozważania o dobrach osobistych wymagają uzupełnienia o analizę jaki charakter ma przewidziane przez RODO prawo do ochrony danych. W ślad za prezentowanymi poglądami uznać należy, że prawo to jest szczególnym rodzajem bezwzględnego prawa podmiotowego o charakterze niemajątkowym. Taki charakter praw do danych niewątpliwie przyczynia się do ochrony dobra osobistego, jakim są dane osobowe. W ślad za głoszonymi już wcześniej stanowiskami zasygnalizować w tym miejscu należy, że może okazać się to jednak niewystarczające dla urzeczywistnienia postulatów dotyczących nowych modeli gospodarki opartej na danych. Przede wszystkim dzisiejszy model prawa do danych nie tworzy odpowiednich ram prawnych dla „komercjalizacji" danych, która jest podstawą dla koncepcji zakładających np. generowanie pasywnego przychodu z tytułu wykorzystywania danych osobowych. Tak rozumiana

s. 557). S. Grzybowski wypracował własną definicję dóbr osobistych, zgodnie z którą są to niemajątkowe, indywidualne wartości świata uczuć, stanu życia psychicznego człowieka, a ich przedmiot stanowi ludzkie uczucie, niezmącony stan życia psychicznego (zob.: S. Grzybowski, *Ochrona dóbr osobistych*, Warszawa 1957, s. 78; S. Grzybowski, *Prawo cywilne*, Kraków 1969, s. 135). J. Sadomski uznaje je za elementy systemu prawnego, który trzeba według niego rozumieć możliwie szeroko. W tym kontekście należ więc uwzględnić także uzasadnienia orzeczeń sądowych, poglądy nauki, wyobrażenia potoczne utrwalone w normach moralnych i obyczajowych społeczeństwa (zob.: J. Sadomski, *Konflikt zasad – ochrona dóbr osobistych a wolność prasy*, Warszawa 2008, s. 60).

[172] Wyrok SN z 10.6.1977 r., sygn. akt II CR 187/77.

[173] I. Lewandowska-Malec, *Dobra osobiste*...

komercjalizacja danych może wymagać wyraźniejszego prawnego zdefiniowania majątkowych praw do danych osobowych. Prowadziłoby to do tzw. dualizmu praw, który w odniesieniu do dóbr niematerialnych nie byłby jednak niczym nowym. Prawa własności intelektualnej również przewidują równoległe istnienie praw o charakterze majątkowym oraz niemajątkowym. Zbyt wąskie rozumienie prawa do danych osobowych oraz ograniczanie go wyłącznie do wymiaru niemajątkowego może być niewystarczające dla realizacji niektórych modeli *data economy*. To oznacza, że w dalszej perspektywie czasowej konieczne może okazać się uznanie charakteru majątkowego prawa do danych osobowych do czego może doprowadzić dalszy rozwój doktryny prawa ochrony danych osobowych w kierunku identyfikowania w ramach istniejących regulacji danych osobowych uprawnień o charakterze majątkowym[174].

Komplementarność pojęć prywatność i dane osobowych

Przechodząc do zagadnienia wzajemnego uzupełnienia się prywatności i praw ochrony danych osobowych, w pierwszej kolejności podkreślić trzeba wspólną cechę prywatności i danych osobowych, jaką jest identyfikowalność jednostki, bez której nie można mówić ani o prywatności, ani o danych osobowych. Dla stwierdzenia, że w danym przypadku mamy do czynienia z prywatnością konkretnego człowieka bądź z jej naruszeniem, konieczna jest możliwość identyfikacji przez inne osoby, a ten czynnik właśnie jest decydujący także dla zaliczenia informacji do kategorii danych osobowych. Takie rozpisanie prywatności na kategorie danych osobowych, które dotyczą poszczególnych jej aspektów, wiąże się ze stwierdzeniem, że w każdym z tych obszarów dysponowanie danymi osobowymi będzie odbywało się na zasadach wynikających z przepisów o ochronie danych osobowych, określających procedury postępowania z danymi osobowymi – z RODO na czele. Dane osobowe mieszczą się w zakresie prywatności, a celem regulacji z zakresu ochrony danych osobowych jest ochrona prywatności w rozumieniu art. 47 Konstytucji RP[175].

Zagrożenie „prywatności" przez dłuższy czas było uważane za główny przedmiot i cel ochrony danych osobowych. Prekursorami terminu „prawa do prywatności" jak to już zostało wskazane wcześniej są prawnicy amerykańscy Samuel D. Warren i Louis D. Brandeis, którzy opublikowali w 1890 r. artykuł „*The right to privacy*", w którym dowodzili, że „istnieje wspólna, niewyrażona *expressis verbis* podstawa, którą jest prawo do prywatności służące ochronie nienaruszalnej osobowości". Następnie niektórzy autorzy zaczęli przedmiot ochrony danych traktować szerzej, dostrzegając w nim instrument kontroli procesów informacyjnych

[174] Podobnie: K. Wojdyło, K. Żukowska, K. Romanowska, adwokat w: Wardyński i Wspólnicy.
[175] M. Sakowska-Baryła, *Ochrona danych osobowych a dostęp do informacji publicznej*, Warszawa 2022, s. 580.

oraz narzędzie eliminowania negatywnych społecznie następstw automatycznego przetwarzania danych. W toczących się dyskusjach na temat celu ochrony danych, np. w literaturze amerykańskiej wysunięto pogląd, iż jej celem jest zabezpieczenie prywatności rozumianej jako prawo do pozostawiania w samotności (right to be let alone, right to withdraw). Wskazywano, że warunkiem zabezpieczenia prywatności jest wyznaczenie sfery, obszaru, do którego nikt z zewnątrz nie powinien mieć dostępu. Obszar ten miał pozostać do wyłącznej dyspozycji jednostki, zarówno w stosunku do osób, instytucji prywatnych, jak i do państwa. W konsekwencji pogląd ten doprowadził do rozwinięcia tzw. teorii sfer, zgodnie z którą zachowania człowieka można uporządkować według skali: intymne-prywatne-publiczne. A. Kopff podjął próbę utożsamiania pojęcia prawa do prywatności z pojęciem „sfery życia osobistego", w ramach których wyróżnił: sferę intymności, prywatności i powszechnej dostępności [176]. Trudności pojawiły się jednak w związku z próbami określenia poszczególnych sfer. To w konsekwencji doprowadziło do sformułowania poglądu o „relatywności sfery prywatności". Chodziło o to, że niektóre informacje mogą mieć charakter publiczny lub prywatny w zależności od tego, kto się nimi posługuje i dla jakich celów. Stwierdzono zatem, że sfery są zrelatywizowane do poszczególnych partnerów, z którymi jednostka jest w kontakcie. Wyodrębnione sfery okazały się mało przydatne dla określenia calu i przedmiotu ochrony danych.

Oprócz teorii sferycznej w literaturze[177] prezentowano również koncepcje skupiające się bardziej na zakresie ochrony. Inne próby określenia przedmiotu i celu ochrony danych, także nawiązujące do prywatności, opierały się na analizie społecznych struktur informacyjnych i rolach, w jakich występuje człowiek w społeczeństwie. Ich założeniem było to, że jednostka, pełniąc określoną rolę społeczna, decyduje się na przekazanie określonych informacji, przy czym inny krąg informacji udostępni np. partnerowi, inne informacje jako pacjent, inne jako podatnik. Wskazywano, że prywatność oznacza zabezpieczenie takiego stanu, aby charakterystyczne dla określonych ról społecznych informacje, nie były dostępne bez zgody jednostki innym podmiotom.

---

[176] A. Kopff, *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1971/20, s. 31 i n. Obszar intymności (sfera informacji intymnych) obejmuje te wszystkie przejawy zachowania jednostki, które powinny być całkowicie niedostępne. Obszar prywatności (sfera informacji prywatnych) to obszar, który dostępny jest tylko częściowo i pod pewnymi warunkami innym osobom lub instytucjom. Sfera publiczna to obszar zachowań jednostki w pełni dostępnych dla innych podmiotów (zob. A. Mrózek, *Ustawowe prawo ochrony danych*, Toruń 1981, s. 44).

[177] N. Brieskorn, *Ochrona danych osobowych a zagrożenia prywatności* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999. Koncepcja ta wymieniała: 1) teorię ról i mozaiki, która różnicowała informacje funkcjonalnie – w zależności od pozycji społecznej, 2) teorię autonomicznej prezentacji – definiującą sferę prywatną poprzez zakres samodzielności w prezentowaniu własnej osoby w otoczeniu oraz 3) teorię komunikowania – w której w sferze prywatnej przedmiotem ochrony jest nienaruszalność procesu komunikacji.

Reasumując, według W. Steinmülera: „przez prywatność rozumieć należy: nierównomierny rozdział informacji na temat jednostki w środowisku [oraz] przyporządkowanie poszczególnych zbiorów informacji poszczególnym partnerom". Samo użycie terminu „prywatność" nie przesądzało jeszcze, że chodzi o problematykę ochrony danych[178].

Prywatność można definiować na wiele sposobów, czego przykładem jest analiza tego pojęcia na gruncie różnych porządków prawnych dokonana we wcześniejszych fragmentach pracy. Na gruncie krajowym w ujęciu wąskim prywatność to stan, w którego ramach jednostka decyduje o zakresie i zasięgu informacji udostępnianych i zakomunikowanych innym osobom. W szerokim zaś to stan, w którym jednostka podejmuje decyzje dotyczące jej osoby bez ingerencji osób trzecich. Mariusz Jabłoński opisuje prywatność jako sumę wielu wartości składających się na rozumienie autonomiczności jednostki żyjącej w określonej rzeczywistości wobec innych jednostek, a także ich wspólnot oraz samego państwa i jego funkcjonariuszy[179]. Jaonna Braciak zauważa zaś, że prywatność jest ściśle związana z pojęciem interesu własnego jednostki, jej dobra oraz z aktywnością podejmowaną przez jednostkę na rzecz ochrony tego dobra, w przeciwieństwie do aktywności podejmowanej dla dobra wszystkich. Prywatność obejmuje sferę aspiracji, dążności oraz tych rodzajów aktywności, które nie podlegają zewnętrznej kontroli; stąd bywa definiowana jako przestrzeń wolnego poruszania się, bądź jako domena autonomicznej aktywności, wolnej od kontroli szerszych grup[180].

Pewnej kategoryzacji definicji prywatności podjął się K. Motyka. Wyróżnił cztery podstawowe typy definiowania prywatności, które znajdują odzwierciedlenie w wyżej przytoczonych stanowiskach:

1. Prywatność jako prawo do bycia pozostawionym w spokoju;
2. Prywatność jako prawo do kontroli informacji na swój temat;
3. Prywatność jako kontrola dostępu do osoby;
4. Prywatność jako autonomia jednostki.

Autor prezentuje także podejście redukcjonistyczne do prywatności. Sprowadza się ono w istocie do eliminacji pojęcia prywatności i w to miejsce korzystania z takich utrwalonych pojęć, jak: tajemnica korespondencji, nietykalność mieszkania, ochrona własności, nietykalność osobista itp. J. Rzucidło uważa, że o ile można się zgodzić z twierdzeniem, iż

[178] B. Konieczna-Drzewiecka, *Inspektor ochrony danych...*, s. 13
[179] M. Jabłoński, *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej*, „Przegląd Prawa i Administracji" 2007/86, s. 280.
[180] J. Braciak, *Prawo do prywatności* [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002, s. 278.

przez pojęcie prywatności rozumieć można tak wiele różnorodnych zjawisk, że niekiedy mają one ze sobą niewiele wspólnego, o tyle nie można funkcjonować bez tego pojęcia, zwłaszcza w obliczu braku sprecyzowanej regulacji dla jakiejś dziedziny aktywności jednostki, którą niekiedy intuicyjnie można zakwalifikować do sfery życia prywatnego, unormowanie takie jest niezbędne. Bez pojęcia prywatność sfera ta pozostaje bez jakiejkolwiek ochrony lub też by objąć ją ochroną, trzeba byłoby co najmniej przeprowadzić bardziej lub mniej skomplikowany proces wykładni prawa.

W literaturze[181] podnosi się, że omawiane w niniejszym opracowaniu prawo uległo jurydyzacji jako wyraz coraz bardziej upowszechniającego się poczucia indywidualności, odrębności i niepowtarzalności jednostki. Z drugiej jednak strony nie sposób pominąć innego trendu, który występował niejako obok tego pierwszego, o którym była już mowa wcześniej w pracy. M. Jagielski, wskazując na źródło konstytucjonalizacji ochrony prywatności, stwierdził, że znaczenie prawa do prywatności wyrosło niejako z ustawodawstwa zwykłego. To na poziomie ustawowym było ono kształtowane i tam też pojawiały się określone instrumenty ochrony. Dopiero z czasem ranga tego prawa urosła na tyle, by znaleźć się w aktach rangi konstytucyjnej (czy pewnych szczególnych aktach prawa międzynarodowego). Co ważne, pomimo że ustawodawca traktował prawo do prywatności jako „nowe prawo", to już na poziomie ustaw zasadniczych zyskało ono miejsce obok takich klasycznych instytucji jak ochrona tajemnicy korespondencji, nienaruszalność mieszkania, czy ochrona dobrego mienia[182].

Relacja pomiędzy prywatnością, dobrami osobistymi a danymi osobowymi

Prawo do ochrony danych osobowych pozostaje w relacji z prywatnością i dobrami osobistymi, wywierając wpływ na wspólne obszary regulacji dotyczących w/w pojęć. W konsekwencji prowadzi to do krzyżowania się różnych reżimów prawnych, co skutkuje koniecznością ustalenia ich wzajemnej specyfiki. W poniżej prezentowanym orzecznictwie sprzed RODO przyjmuje się, że pomiędzy prawem do prywatności a prawem do ochrony danych osobowych istnieje ścisły związek, a co za tym idzie naruszenie ochrony danych osobowych często pociąga za sobą naruszenie prawa do prywatności. Jak stwierdził TK w sprawie pośrednio dotyczącej ochrony danych osobowych, „prawo do prywatności, statuowane

[181] A. Mednis, *Prawo do prywatności a interes publiczny*, Warszawa 2006, s. 79.
[182] J. Rzucidło, *Prawo do prywatności...*, s. 153

w art. 47[183], zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51[184]. Ten ostatni, rozbudowany przepis, odwołując się aż pięciokrotnie do warunku legalności – *expressis verbis* w ust. 1, 3, 4 i 5 oraz pośrednio przez powołanie się na zasadę demokratycznego państwa prawnego w ust. 2 – stanowi też konkretyzację prawa do prywatności w aspektach proceduralnych"[185].

Trybunał Konstytucyjny wydał powyższe orzeczenie rozponając zagadnienie zgodności z prawem przepisów, zobowiązujących do uwidocznienia w zaświadczeniu lekarskim numeru statystycznego choroby. Stwierdził w konsekwencji przeprowadzonego badania wprost, że prawo do ochrony danych osobowych stanowi szczególny instrument ochrony życia prywatnego. Jest zatem wyspecjalizowanym środkiem ochrony tych samych wartości, które chronione są przez prawo do prywatności. Prywatność dotyczy również ochrony informacji dotyczących określonego podmiotu, co „gwarantuje m.in. pewien stan niezależności, w ramach którego jednostka może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu"[186].

Jakub Rzucidło, omawiając powyższe orzeczenie, stwierdził, że można kwestionować prawidłowość rozumowania, zgodnie z którym między regulacjami prawa do prywatności i prawa do ochrony danych osobowych zachodzi stosunek krzyżowania, przy czym są to „reżimy wzajemnie niezależne". Zdaniem Autora takie stanowisko nie prowadzi w żadnym wypadku do wzmocnienia roli prawa do ochrony danych osobowych, dlatego że nadaje się mu niejako niezależny status. Z drugiej zaś strony jasne powinno już być, że prawo do prywatności nie daje się „sprowadzić jedynie do ochrony danych osobowych"[187]. Pogląd ten stoi w sprzeczności z prezentowaną wcześniej tezą o wzajemnym krzyżowaniu się omawianych praw która aktualnie dominuje w piśmiennictwie dotyczącym ich relacji.

W doktrynie na ogół przyjmuje się, że prywatność odnosi się m.in. do ochrony informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu. Istnienie prawa do prywatności w polskim porządku prawnym

[183] art. 47 Konstytucji RP „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym"
[184] art. 51 Konstytucji RP „1.Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa
[185] Wyrok TK z 19.05.1998 r., U 5/97, OTK.
[186] Wyrok TK z 12.11.2002 r., SK 40/01, OTK/
[187] J. Rzucidło, *Prawo do prywatności...*, s. 165.

znalazło potwierdzenie w orzecznictwie Sądu Najwyższego[188], który odniósł koncepcję ochrony dóbr osobistych (art. 23 i 24 kc) do sfery życia prywatnego i sfery intymności. Na istotny związek prawa do prywatności oraz do ochrony danych osobowych wskazał także Trybunał Konstytucyjny m.in. w orzeczeniu z 24.06.1997 r. w sprawie o sygn. K. 21/96, powołując się na swe ustabilizowane orzecznictwo, według którego zasada demokratycznego państwa prawnego obejmuje swym zakresem także pewne treści materialne, w szczególności powiązane z prawami i wolnościami jednostki. Trybunał uznał, że art. 1 uprzednio obowiązujących przepisów konstytucyjnych dawał podstawę do sformułowania konstytucyjnego prawa do prywatności, rozumianego m.in. jako prawo do zachowania w tajemnicy informacji o swoim życiu prywatnym[189].

Jak argumentuje Sąd Najwyższy w sprawie dotyczącej roszczeń opartych na naruszeniu danych osobowych i dóbr osobistych wynikających z braku aktualizacji informacji o kredytobiorcy w systemie informacji kredytowej „prawo do ochrony danych osobowych, ujęte w art. 51 Konstytucji RP, wiąże się ściśle ze sferą poszanowania prywatności, swobody i integralności człowieka. Łączy w sobie prawo do rzetelnej informacji o ich gromadzeniu i przetwarzaniu z prawem do żądania sprostowania oraz usunięcia danych nieprawdziwych. Prawo do ochrony danych osobowych jest wywodzone w piśmiennictwie z takich dóbr osobistych, jak godność człowieka oraz prawo do prywatności. W ten sam sposób kwalifikuje je Trybunał Konstytucyjny, w którego orzecznictwie utrwalił się pogląd, że art. 47 i art. 51 Konstytucji RP chronią tę samą wartość konstytucyjną – sferę prywatności[190]. Autonomia informacyjna stanowi istotny element składowy prawa do prywatności i oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby oraz prawo do sprawowania kontroli nad tymi informacjami znajdującymi się w posiadaniu innych podmiotów[191]. Prywatność obejmuje także ochronę informacji dotyczących określonego podmiotu [192], w tym informacji dotyczących jego sytuacji finansowej[193].

W innym wyrok, wydanym w podobnym stanie faktycznym, tj. dotyczącym oceny skutków prawnych raportu, z którego wynikało, że powódka była niesolidną klientką banku, Sąd Najwyższy[194] zwrócił uwagę na konieczność wykładania przepisów ustawy o ochronie

[188] Orzeczenie SN z 8.04.1994 r., sygn. akt III ARN 18/94.
[189] Orzeczenie TK z 24.06.1997 r. w sprawie o sygn. akt K. 21/96, OTK ZU Nr 2/1997, poz. 23, s. 225.
[190] Wyrok SN z 11.02.2015 r., sygn. akt I CSK 868/14.
[191] Wyroki TK z: 19.02.2002 r., sygn. akt U 3/01, OTK-A 2002/1/3; z 20.11.2002 r., sygn. akt K 41/02, OTK-A 2002/6/83; z 13.12.2011 r., sygn. akt K 33/08, OTK-A 2011/10/116.
[192] Wyrok TK z 12.11.2002 r., sygn. akt SK 40/01, OTK-A 2002/6/81.
[193] Orzeczenie TK z 24.06.1997 r., sygn. akt K 21/96, OTK 1997/2/23.
[194] Wyrok SN z 15.02.2008 r., sygn. akt I CSK 358/07.

danych osobowych z uwzględnieniem zaleceń dyrektywy 95/46/WE. W jej części wstępnej podkreślono, że systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi i muszą szanować podstawowe prawa i wolności osób fizycznych, a szczególnie prawo do prywatności. Jeżeli w wyniku nienależytej dbałości o interesy osoby, której dane osobowe są gromadzone i przetwarzane, nastąpiło wkroczenie w sferę wartości o charakterze niemajątkowym, wiążących się z osobowością człowieka, uznanych powszechnie w społeczeństwie, to poza środkami administracyjnymi przewidzianymi w ustawie o ochronie danych osobowych pokrzywdzony może sięgnąć również po możliwości obrony przewidziane w art. 24 k.c[195].

W literaturze sprzed RODO wskazywano, że prawo do ochrony danych osobowych ma co najmniej dwa aspekty: prywatnoprawny oraz publicznoprawny. Gdy idzie o ten pierwszy, to chodzi przede wszystkim o osobisty stosunek występujący pomiędzy osobą fizyczną a danymi jej dotyczącymi. Dane osobowe są zatem w tym aspekcie chronione podobnie jak dobra osobiste[196]. Dlatego też osobom fizycznym może przysługiwać ochrona danych osobowych na podstawie przepisów Kodeksu cywilnego, Kodeksu pracy czy Kodeksu karnego[197]. Możliwych jest w tym zakresie kilka podejść. Szerokie ujęcie zakłada, że autonomia informacyjna jednostki jest dobrem osobistym i przy rygorystycznym założeniu, że każde bezprawne posłużenie się danymi narusza takie prawo, należy przyjąć, że chronione są dane osobowe. Natomiast przy przyjęciu mniej intensywnej ochrony i akceptacji stanowiska zrelatywizowanego, z naruszeniem wyżej wskazanego dobra mielibyśmy do czynienia tylko wówczas, gdy nieuprawnione wkroczenie naruszyłoby stan niezakłóconego spokoju fizycznego osoby będącej ofiarą naruszenia.

Ponadto możliwe jest jeszcze inne ujęcie danych osobowych, nie w kategorii dobra osobistego, ale w kategorii własnościowej (czy w kategoriach własnościowych). I znowu można tutaj wyróżnić dwa ujęcia. W najszerszym, przedmiotem ochrony są same dane osobowe, których właścicielem jest ten człowiek, którego one dotyczą. Złagodzone stanowisko zakłada zaś, że to status własnościowy, władztwo sprawowane nad danymi przez osobę, której dane dotyczą (połączone niekiedy z poufnością), stanowi przedmiot ochrony. Opowiadając się za Autorami – J. Bartą, P. Fajgielskim, R. Markiewiczem, którzy powyższe koncepcje wyszczególnili, wypada przyjąć tę nawiązującą do powszechnej ochrony dóbr osobistych i to w rygorystycznym ujęciu. Wydaje się, że przyjęcie mniej rygorystycznej koncepcji byłoby

[195] Wyrok SN z 11.02.2015 r. sygn. akt I CSK 868/14; D. Lubasz, A. Szkurłat, *Relatywizacja pojęcia danych*....
[196] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych...*, s. 289 291
[197] A. Drozd, *Ustawa o ochronie danych osobowych*, Warszawa 2006, s. 152–153.

nader kłopotliwe, jeśli idzie o przeprowadzenie dowodu w zakresie ustalenia zakłócenia stanu spokoju, co implikuje stwierdzenie, że jest to „prawo niemajątkowe, ściśle związane z osobą. Wyklucza to w istocie obrót tym prawem, możliwość zrzeczenia się go, jak też uczynienie go przedmiotem dziedziczenia. Niemajątkowy charakter prawa nie odbiera jednak możliwości osiągania korzyści majątkowych przez jego wykonywanie[198].

Przyjmując na potrzeby pracy ten pogląd jako argument przemawiający za jego słusznością, w pierwszej kolejności podkreślić należy, że istotę prawa do ochrony danych wskazuje punkt 7 preambuły RODO, który stanowi, że osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi. Prawo do ochrony danych osobowych ma więc służyć przede wszystkim zapewnieniu podmiotom danych kontroli nad ich danymi. Szczegółową treść tego prawa definiują instrumenty ochronne przewidziane przez RODO. Instrumenty te polegają m.in. na zagwarantowanym prawie do informacji o przetwarzanych danych, prawie kontroli, ale również prawie do sprzeciwu względem przetwarzania danych. Wiele z tych uprawnień jest zbliżonych do wiązki praw występujących również w klasycznych konstrukcjach prawa własności. Istnieją jednak również istotne różnice.

Przede wszystkim elementem uprawnień wynikających z RODO nie jest uprawnienie do wyłącznego posiadania danych osobowych (*ius possidendi*). RODO odnosi się jedynie do prawa do „ochrony" danych, gwarantując podmiotowi danych możliwość kontroli nad danymi, jednak nie regulując kwestii ich własności. Te same dane mogą być jednocześnie przetwarzane przez różne podmioty. W wielu przypadkach podmioty te będą mogły przetwarzać dane bez zgody podmiotu danych, a niekiedy również bez jego wiedzy. Prawo do ochrony danych nie przewiduje również typowego dla prawa własności uprawnienia do wyłącznego pobierania pożytków z przedmiotu własności (ius utendi et fruendi). Dane mogą być wykorzystywane zarobkowo przez inne niż podmiot danych podmioty, bez konieczności zapewnienia podmiotowi danych korzyści z wykorzystywania jego danych. Istotnemu ograniczeniu podlega również klasyczne uprawnienie do dysponowania rzeczą (*ius disponendi*). Jakkolwiek poszczególne dane osobowe mogą być przekazywane przez podmiot danych do innych podmiotów, to nie ma możliwości zbycia całości prawa do ochrony danych osobowych. Zarówno z teoretycznego, jak i praktycznego punktu widzenia istotne jest ustalenie, czy wiązka uprawnień do ochrony danych przewidziana przez RODO ma charakter prawa majątkowego czy też prawa niemajątkowego. Wydaje się, że brakuje w RODO mechanizmów, które gwarantowałyby podmiotowi danych swoiste władztwo i kontrolę nad

[198] J. Rzucidło, *Prawo do prywatności...*, s. 168.

korzyściami ekonomicznymi płynącymi z danych osobowych. To nie interes ekonomiczny podmiotu danych jest podstawowym przedmiotem zainteresowania i ochrony RODO. Z tego punktu widzenia przewidziane przez RODO prawo do ochrony danych jest zbliżone raczej do praw niemajątkowych niż praw o charakterze majątkowym, o czym była mowa we wcześniejszym fragmencie pracy. Potwierdza to także motyw 4 preambuły RODO, zgodnie z którym prawo do ochrony danych należy postrzegać w kontekście jego funkcji społecznej[199].

Praktyczne znaczenie omawianego powyżej rozróżnienia wynika w kontekście prawa polskiego przede wszystkim z art. 44 k.c., zgodnie z którym mieniem jest własność i inne prawa majątkowe. Prawa niemajątkowe nie będą składnikiem mienia i zgodnie z powszechnym w doktrynie zapatrywaniem nie mogą być również dziedziczone oraz zbywalne. Przyjęcie, że prawo do ochrony danych nie ma charakteru majątkowego, musiałoby konsekwentnie oznaczać, że prawo to nie jest składnikiem mienia, nie podlega dziedziczeniu oraz nie może być zbyte. Takie właśnie podejście zaczyna być również obecne w polskiej praktyce.

Dobrym tego przykładem jest interpretacja podatkowa z 21.02.2020 r., w której Dyrektor Krajowej Informacji Skarbowej (sygn. 0113-KDIPT2-3.4011.717.2019.1.PR) odmówił zakwalifikowania przychodów z czasowego udostępnienia danych osobowych jako przychodów z praw majątkowych. Przedstawił stanowisko, zgodnie z którym dane osobowe stanowią prawa niemajątkowe i ewentualne przychody z rozporządzania danymi osobowymi należy traktować jako przychody „z innych źródeł". W ramach tego podejścia dane osobowe są kwalifikowane jako dobro osobiste, a ewentualne prawa odnoszące się do tych danych są niemajątkowymi prawami osobistymi. Prawa osobiste to prawa przysługujące osobie fizycznej lub prawnej w celu ochrony jej dóbr osobistych. W tym przypadku chronionym dobrem osobistym jest sfera prywatności człowieka, której immanentnym elementem pozostają dane osobowe podmiotu danych[200].

Naruszenie dóbr osobistych a naruszenie danych osobowych w orzecznictwie

Omawiane zagadnienia relacji prawa do prywatności, dóbr osobistych i danych osobowych prowadzą do wniosku, że w zakresie odpowiedzialności na gruncie poprzednich regulacji prawnych w pierwszej kolejności znaczenie miał fakt, czy naruszenie danych osobowych powodowało także naruszenie dóbr osobistych. Odpowiedzialność na podstawie

[199] K. Wojdyło, praktyka prawa nowych technologii kancelarii Wardyński i Wspólnicy, Katarzyna Żukowska, adwokat, Karolina Romanowska, adwokat, praktyka ochrony danych osobowych kancelarii Wardyński i Wspólnicy, https://codozasady.pl/p/czym-jest-prawo-do-danych-osobowych
[200] K. Wojdyło, praktyka prawa...

dyrektywy 95/46/WE oraz ustawy o ochronie danych osobowych z 1997 r. oparta była na ogólnych regułach odpowiedzialności cywilnej albo w reżimie ochrony dóbr osobistych, o ile w danym konkretnym stanie faktycznym naruszenie ochrony danych osobowych godzi w dobra osobiste osoby, której dane są przetwarzane, albo na ogólnych zasadach odpowiedzialności deliktowej. Kwestia kwalifikowania w orzecznictwie naruszenia obowiązków wynikających z przetwarzania danych osobowych jako naruszenia dóbr osobistych miała istotne znaczenie dla omawianego zagadnienia. Zasadne jest zatem dokonanie w tym miejscu przeglądu zarówno polskiego, jak i zagranicznego dorobku orzeczniczego, zwłaszcza że w zakresie możliwości uznania za naruszenie dobra osobistego działania polegającego na nieprawidłowym, w rozumieniu ustawy o ochronie danych osobowych z 1997 r. (w okresie do 24.05.2018 r.) i ogólnego rozporządzenia o ochronie danych osobowych (w okresie od 25.05.2018 r.) przetwarzaniu danych osobowych sądy wypowiadały się wielokrotnie.

Już w orzecznictwie sądowym z lat 70. XX wieku, kiedy w Polsce brak było regulacji dotyczących ochrony danych osobowych (pierwsze ustawy, np. niemiecka federalna ustawa o ochronie danych osobowych pochodzą z lat 70. XX wieku), polskie sądy analizowały takie kwestie, jak ujawnienie informacji o stanie zdrowia (wezwanie chorego do poradni dermatologicznej jako podejrzanego o chorobę weneryczną), czy też wpisanie do książki zdrowia pacjenta informacji o rozpoznaniu konkretnej choroby psychicznej w sytuacji, gdy diagnoza nie potwierdziła się. W nowszym orzecznictwie Sąd Najwyższy przyjął natomiast, że „pracodawca nie narusza dóbr osobistych pracownika (art. 23 k.c., art. 47 i art. 51 ust. 1 i 2 Konstytucji RP), zobowiązując go zgodnie z postanowieniami regulaminu przyznawania zapomóg z zakładowego funduszu świadczeń socjalnych do złożenia zaświadczenia o zarobkach uzyskiwanych u drugiego pracodawcy“[201].

Podkreślenia wymaga, że przepis art. 23 k.c. nie zawiera ustawowej definicji dobra osobistego, a jedynie przykładowy, a więc otwarty katalog dóbr osobistych. Obecnie nie ulega wątpliwości, że do tego katalogu zaliczane są również prawo do prywatności[202], jak i prawo do ochrony danych osobowych[203]. Przesądza o tym również ranga obu powyższych wartości w systemie prawnym. Jak już zostało wskazane mają one swoje źródło zarówno w Konstytucji RP RP, jak i Europejskiej Karcie Praw Podstawowych UE oraz Europejskiej Konwencji Praw Człowieka. Nie można mieć też wątpliwości, że obie te wartości niemajątkowe wiążą się ściśle

[201] B. Łukańko, *Uchybienie przepisom o ochronie danych osobowych jako naruszenie dobra osobistego – analiza na przykładzie orzecznictwa Sądu Najwyższego*, „Studia Prawnoustrojowe UWM” 2019/46, s. 247.
[202] P. Księżak [w:] *Kodeks cywilny. Komentarz. Część ogólna*, red. M. Pyziak-Szafnicka, P. Księżak, uwagi 107 i n. do art. 23.
[203] *Kodeks cywilny. Komentarz...*, red. M. Pyziak-Szafnicka, P. Księżak, uwagi 115 do art. 23.

z osobowością człowieka i są powszechnie uznane w społeczeństwie. Podkreślane jest to w orzecznictwie. Sąd Najwyższy akcentuje w swoich wyrokach, w tym w omawianym wcześniej już wyroku w sprawie I CSK 358/07, że prawo do ochrony danych osobowych, rzetelnej informacji o ich gromadzeniu i przetwarzaniu nie tylko jest gwarantowane konstytucyjnie, ale wywodzi się bezpośrednio z takich dóbr osobistych, jak godność człowieka i prawo do prywatności. Zdaniem Sądu Najwyższego zgodne z prawem zbieranie danych osobowych oraz przejrzyste informowanie o tym fakcie podmiot danych ma na celu ochronę godności oraz poczucia pewności i bezpieczeństwa. W przypadku naruszenia zasad przetwarzania danych osobowych wartości te są naruszone. Dobro osobiste w postaci prawa do ochrony danych osobowych tj. zgodnego z prawem i przejrzystego ich przetwarzania odgrywa zatem niezwykle istotną rolę[204].

Prawo do prywatności należy do kluczowych dóbr osobistych jednostki, chociaż nie zostało wprost wymienione w art. 23 k.c. Tak wywodzi Sąd Apelacyjny, rozstrzygając sprawę dotyczącą roszczeń wynikających z faktu opublikowania na łamach czasopisma listu w sprawie zaprzestania wydawania czasopisma, w którym bezprawnie podane zostały pełne dane osobowe i adresowe powoda i podniesione zostały zarzuty stosowania gróźb i nieuczciwych praktyk rynkowych. Zdaniem Sądu składnikiem i pochodną prawa do prywatności jest niejawność: danych adresowych człowieka, informacji o jego stanie zdrowia i realiach życia rodzinnego, intymnych szczegółów dotyczących sfery erotycznej itd. Pierwotnym (początkowym) dysponentem powyższych informacji może być jedynie podmiot, którego one dotyczą. Złamaniem zasady prywatności owych danych jest zaś ich upublicznienie, przy czym o ile dochodzi do niego za zgodą i przy udziale samego zainteresowanego, to nie sposób ocenić takiego zachowania co do zasady jako bezprawne. Oczywiście istotny w takiej sytuacji jest zakres analizowanego upublicznienia; nie można bowiem w pełni wykluczyć bezprawności szerokiego upublicznienia danych ujawnionych wcześniej w zakresie znacząco mniejszym (upublicznienie wobec wybranych odbiorców)[205]. To oznacza, że zakres upublicznienia danych ma znaczenie dla oceny wagi ich naruszenia.

W innej sprawie dotyczącej naruszenia dóbr osobistych związanych z niedopełnieniem wszystkich ciążących na Banku obowiązków, zgłoszenia z opóźnieniem w rejestrze informacji o wypowiedzeniu, a w konsekwencji nękania powoda propozycjami zawarcia umów dotyczących produktów bankowych Sąd stwierdził, że samo naruszenie przepisów ustawy o

[204] Wyrok SN z 15.02.2008 r., sygn. akt I CSK 358/07
[205] Wyrok SA w Białymstoku - I Wydział Cywilny z 13.09.2017, sygn. akt r. I ACa 236/17.

ochronie danych osobowych nie stanowi jeszcze o naruszeniu dóbr osobistych powoda[206]. W przedmiotowej sprawie wyrok zapadł w stanie faktycznym, w którym powód powoływał się na naruszenie przez pozwanego przepisów ustawy z 29.08.1997 r. o ochronie danych osobowych polegające na braku realizacji jego wniosków składanych w trybie art. 32 ust. 1 pkt. 1-5a w zw. z art. 33 w przedmiocie usunięcia danych osobowych. Z analizy przedstawionej przez powoda podstawy faktycznej żądania wynika, że dobrami osobistymi, które mogłyby ulec naruszeniu w toku sprawy, były: prawo do prywatności oraz dobre imię powoda jako klienta banku.
W ocenie Sądu Apelacyjnego powód nie wykazał, by owe dobra osobiste zostały naruszone, wskazując jednocześnie, że w czasach nachalnego marketingu i wszechobecnej reklamy, odebranie w okresie 3 miesięcy (czyli 91 dni) około 20–30 telefonów oferujących produkty bankowe stanowi normalny element życia codziennego. Rozmowę taką można w sposób stanowczy przerwać na samym wstępie, można również zablokować wyświetlający się numer telefonu. Odnosząc się zaś do oceny zarzutu naruszenia dobra osobistego w postaci dobrego imienia powoda jako klienta banku, Sąd stwierdził, że w żaden sposób nie zostało wykazane, że do takiego naruszenia doszło, z uwagi na fakt, że – jak przyznała sama pozwana – powód regularnie uiszczał swe należności, a jego historia kredytowa była – jak to zostało określone – idealna. Też i w żaden sposób nie ucierpiało dobre imię powoda jako klienta banku wskutek tego, że niespornie ujawnienie aktualnych danych powoda w rejestrze nastąpiło z opóźnieniem, co wyniknęło z systemowo technicznych systemów przetwarzania informacji[207]. W omawianej sprawie Sąd odniósł pojęcie prywatności do intensywności telefonicznych działań marketingowych oceniając, że naruszenie prawa prywatności miałoby miejsce, gdyby powód w sposób ciągły zmuszany był do odbioru połączeń telefonicznych, w ramach których telemarketerzy w sposób nachalny, mimo sprzeciwów odbiorcy, przedstawialiby oferty marketingowe produktów bankowych. Owe połączenia musiałyby występować w sposób ciągły, zakłócający zwykły rytm dzisiejszego życia codziennego.

Inaczej koncepcję intensywności działań reklamowych, wykonywanych w tradycyjnej formie pisemnej jako ingerujących w prywatność jednostki Sąd oceniał w orzeczeniu wydanym w sprawie sygn. akt VI ACa 223/16[208]. W pierwszej kolejności Sąd uznał, że zawarty w art. 23 k.c. katalog dóbr osobistych jest jedynie przykładowym ich wyliczeniem, dlatego sądowi pozostawiono decyzję odnośnie tego, czy określone zachowanie można uznać za bezprawne i jednocześnie naruszające cudze dobra osobiste. Zdaniem Sądu w tej sprawie zachowaniem,

[206] Wyrok SA - I Wydział Cywilny z 24.05.2018 r., sygn. akt I ACa 1202/17.
[207] Wyrok SA - I Wydział Cywilny z 24.05.2018 r., sygn. akt I ACa 1202/17.
[208] Wyrok SA w Warszawie – V Wydział Cywilny z 17.05.2017, sygn. akt VI ACa 223/16.

które należało uznać za bezprawne i naruszające cudze dobra osobiste było wysyłanie, nie chcianej przez adresata korespondencji reklamowej. W ocenie Sądu kierowanie do kogokolwiek skierowanych bezpośrednio do niego komunikatów, których otrzymywania osoba ta sobie nie życzy stanowi naruszenie dobra osobistego w postaci swobody korespondencji. Wolność ta nie ogranicza się bowiem, zdaniem sądu pierwszej instancji, do wolności korespondowania, ale obejmuje także prawo do tego, by nie otrzymywać korespondencji niechcianej, zwłaszcza gdy adresat wyraźnie powiadomi nadawcę o tym, że nie życzy sobie jej otrzymywania. Równolegle takie postępowanie może zostać uznane za naruszenie prawa do prywatności. Przesyłanie korespondencji bezpośrednio adresowanej, w odróżnieniu od tzw. przesyłek bezadresowych jest bowiem równoznaczne z faktem, że kierujący przesyłki dysponuje informacją co do sposobu skontaktowania się z daną osobą, która to informacja – podobnie jak informacja o miejscu zamieszkania – należy do sfery prywatności. Sąd zwrócił w tej sprawie jednocześnie uwagę, że źródłem roszczenia powoda nie był fakt naruszenia przez pozwaną obowiązków wynikających z przepisów o ochronie danych osobowych, a fakt naruszenia jego dóbr osobistych poprzez przesyłanie mu nie zamówionych informacji handlowych.

W ocenie Sądu tego rodzaju działanie stanowiło naruszenie dóbr osobistych powoda w postaci swobody korespondencji i prawa do prywatności, dlatego należało przyjąć, że pozwana dopuściła się naruszenia dóbr osobistych powoda. Według Sądu działaniem naruszającym w prezentowanym stanie faktycznym dobra osobiste nie było przetwarzanie danych osobowych, a przesyłanie na adres powoda korespondencji, której otrzymywania od pozwanej powód sobie nie życzył. W ocenie Sądu pozwana nie może zatem wywodzić, że fakt działania przez nią na podstawie umów „powierzenia przetwarzania danych osobowych" wyłącza bezprawność naruszenia dobra osobistego powoda. Powoływanie się przez pozwaną na art. 31 ust.1 i 2 SUODO wynika, zdaniem Sądu Okręgowego z błędnego założenia, jakoby źródłem naruszenia dóbr osobistych powoda było przetwarzanie jego danych. W ocenie Sądu wykorzystywanie takich danych do przesyłania korespondencji nie stanowi samo przez się „przetwarzania danych osobowych" w rozumieniu ustawy. Argumentacja Sądu została wywiedziona z tego, że kwestia przesyłania niezamówionych informacji handlowych nie podlegała nawet bezpośrednio regulacji tej ustawy, bo była ona regulowana ustawą z dnia 18.07.2013 r. „o świadczeniu usług drogą elektroniczną", która w art. 10 ust. 1 wprowadzała wprost zakaz takiej działalności. W dalszej części orzeczenia Sąd stwierdził, że z przepisu tego wprost wynikała bezprawność przesyłania niezamówionej informacji handlowej. Dlatego ewentualne obalenie przez pozwaną domniemania bezprawności naruszenia dóbr osobistych

powoda wymagałoby wykazania przez nią, że powód udzielił zgody na przesyłanie mu informacji handlowych. Oświadczenie administratora danych osobowych nie jest wystarczającym dowodem – poświadcza ono, że administrator taką zgodę uzyskał, nie zaś, iż powód jej udzielił. Natomiast w sytuacji gdy powód temu zaprzecza, samo tylko twierdzenie administratora danych to zbyt mało, by okoliczność tę uznać za udowodnioną. W rezultacie uznano, że działanie pozwanej stanowiło bezprawne naruszenie dóbr osobistych powoda[209].

Przedstawione powyżej stanowisko Sądu co do rozumienia pojęcia przetwarzania danych uległoby zapewne weryfikacji, gdyby przedmiotem jego rozważań była definicja przetwarzania ze SUODO. Zgodnie bowiem z art. 7 SUODO przetwarzaniem danych osobowych były jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Takie rozumienie operacji przetwarzania danych na gruncie RODO, które przecież w dacie wydawania omawianego orzeczenia weszło już w życie i oczekiwało na rozpoczęcie jego stosowania nie uległo znaczącej zmianie. Powyższe dowodzi wątpliwości co do poprawności oceny Sądu w przedmiocie braku stwierdzenia naruszenia danych osobowych. To nie wpływa na rozstrzygniecie co do naruszenia dóbr osobistych, mając na względzie fakt, że ocena pojęcia dobro osobiste pozostawione jest do analizy Sądu *ad casu*. Istotność omawianego rozstrzygnięcia polega na odmiennym w stosunku poprzednio omawianego wyroku rozumieniu intensywności działań, których skutkiem jest naruszenie prywatności.

Uznanie jako naruszenie prawa do prywatności rozpowszechnienia adresu powódki potwierdzone zostało w innym orzeczeniu Sądu[210]. W sprawie tej doszło do zaniedbania pozwanego, które doprowadziło do ujawnienia danych powódki, co uprawniało ją do skorzystania ze środków ochrony prawnej przewidzianych w art. 24 § 1 k.c. Zdaniem Sądu upublicznienie danych osobowych naruszyło konkretne dobro osobiste powódki w postaci prawa do prywatności. Prawo to – choć niewymienione w art. 23 k.c. – co podkreślał Sąd jest chronionym prawnie dobrem osobistym. Katalog wskazanych w tym przepisie dóbr osobistych ma charakter otwarty i jest uzupełniany przed doktrynę oraz judykaturę. Z punktu widzenia prawa cywilnego szeroko rozumiane prawo do prywatności obejmuje m.in. dane osobowe i prawo dysponowania swoimi danymi osobowymi[211]. Argumentacja Sądu w tej sprawie koresponduje ze stanowiskiem Trybunału Konstytucyjnego,

[209] Wyrok SA w Warszawie - V Wydział Cywilny z 17.05.2017 r. VI ACa 223/16.
[210] Wyrok SA w Białymstoku – I Wydział Cywilny z 15.03.2017 r., sygn. akt I ACa 599/16.
[211] Wyrok SN z 24.06.2014 r., sygn. akt I CSK 532/13.

który podnosi, że z Konstytucji RP wynika, że każdy ma prawo do ochrony życia prywatnego i nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby (art. 47 i art. 51 ust. 1 Konstytucji RP). Ochrona życia prywatnego obejmuje także autonomię informacyjną, oznaczającą prawo do samodzielnego decydowania o ujawnieniu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów[212].

Analiza wskazanego powyżej orzecznictwa pozwala na postawienie tezy, że nie każde uchybienie przepisom o ochronie danych osobowych będzie jednoznaczne z naruszeniem dóbr osobistych - są to dwa odrębne reżimy prawne. Taka kwalifikacja każdorazowo będzie uzależniona od oceny przedmiotu, charakteru i skutków danego uchybienia. Jeżeli w wyniku nienależytej dbałości o interesy osoby, której dane osobowe zostały przetworzone, zostaną naruszone także uznane powszechnie w społeczeństwie wartości o charakterze niemajątkowym, takiej osobie – poza środkami przewidzianymi w ustawie o ochronie danych osobowych – przysługiwać będą również środki ochrony prawnej z art. 24 k.c.

W tym miejscu dodać warto, że w odniesieniu do osób publicznych zakres udzielonej im ochrony dóbr osobistych, w szczególności prawa do prywatności, doznaje większych ograniczeń niż w przypadku osób „niepublicznych". Osoby publiczne muszą liczyć się z większym zainteresowaniem opinii publicznej, co ma wpływ także na zakres ochrony prawa do prywatności. Analiza orzecznictwa Sądu Najwyższego czy Europejskiego Trybunału Praw Człowieka dotycząca konfliktu wartości w postaci prawa do prywatności (art. 47 Konstytucji RP oraz art. 8 EKPC) z prawem do swobody wypowiedzi (art. 54 Konstytucji RP oraz art. 10 EKPC) prowadzi do wniosku, że dawany jest prymat zasadzie swobody wypowiedzi, gdy sprawa będąca przedmiotem wypowiedzi dotyczy kwestii publicznych, budzących zainteresowanie publiczne[213]. Wolność wypowiedzi nie ma jednak charakteru bezwzględnego i jest ograniczona m.in. ze względu na potrzebę ochrony praw innych osób. W odniesieniu do osób publicznych zakres udzielanej im ochrony dóbr osobistych, w szczególności prawa do prywatności może być ograniczony wtedy, gdy wiąże się to z ich działalnością publiczną[214].

Kwestię ujawnienia danych w kontekście oceny czy doszło do naruszenia danych osobowych lub dóbr osobistych Sąd rozpoznawał także w poniższych wyrokach, uznając, że innym naruszeniem dóbr osobistych związanym z danymi osobowymi jest w ocenie Sądu[215]

[212] Wyrok TK z 20.04.2002 r., sygn. akt K 41/02.
[213] Uzasadnienie wyroku SN z 16.12.2014 r., sygn. akt III CSK 52/14 i wskazane tam orzecznictwo.
[214] Wyrok SN z 28.10.2016 r., sygn. akt I CSK 695/15.
[215] Wyrok SR – Wrocław Śródmieście we Wrocławiu z 9.10.2018 r., sygn. akt VIII C 16/18.

omyłkowe oraz nieumyślne ujęcie w wykazie akcjonariuszy posiadających ponad 5% głosów na walnym zgromadzeniu spółki publicznej właściciela akcji, do którego należy mniej niż 5% głosów oraz ujawnienie danych takiej osoby w raporcie bieżącym. Z autonomii informacyjnej wynika prawo jednostki do decydowania zarówno o zakresie, jak i treści informacji, jakie dostępne będą podmiotom trzecim, w szczególności stanowić będą przedmiot publicznego udostępnienia za pośrednictwem środków masowego przekazu. Autonomia informacyjna zakłada daleko posuniętą swobodę jednostki w zakresie decyzji, które informacje jej dotyczące są dostępne osobom trzecim, w tym szerszej kategorii odbiorców (opinii publicznej). W tym kontekście podanie w publikacji imienia i nazwiska danej osoby co do zasady narusza jej prawo do prywatności, jeżeli nie wyraziła zgody na ich ujawnienie. Jednakże nie każda informacja dotycząca określonej osoby będzie informacją z dziedziny jej życia osobistego. Informacje dotyczące pracy danej osoby mogą się do takiej sfery zaliczać, ale to nie oznacza, że każda taka informacja stanowi wkroczenie w życie prywatne, naruszenie prywatności. Ocena zależeć będzie od całego kontekstu i okoliczności sprawy, a przede wszystkim od tego, jaka konkretnie informacja i komu została podana (ujawniona)[216].

Według uchwały Sądu Najwyższego z 16.07.1993 r.[217] prywatność człowieka obejmuje w szczególności zdarzenia związane z życiem rodzinnym, seksualnym, stanem zdrowia, przeszłością, sytuacją majątkową, w tym z uzyskiwanymi dochodami. Sąd Najwyższy wskazał w niej, że ujawnienie przez pracodawcę bez zgody pracownika wysokości jego pensji może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 k.c. Sąd uznał też, że zaliczenie prawa do wynagrodzenia do sfery prywatności pracownika zależy od kilku czynników. Chodzi tu m.in. o zwyczaje panujące w konkretnym zakładzie, jego wielkość, panujące stosunki społeczne oraz gospodarcze. Należy jednak uznać, że pracodawca bezwzględnie powinien wstrzymać się z ujawnianiem wysokości zarobków podwładnego, jeśli ten wyraźnie się na to nie zgadza (wyraża sprzeciw).

Odmienne zapatrywania judykatury należą do rzadkości, ale zostały wyrażone np. w wyroku z 14.11.2003 r. Sądu Apelacyjnego w Poznaniu[218]. Z perspektywy zagadnienia krzyżowania sią praw istotne jest, że w orzeczeniu tym Sąd uznał, że stan majątku i dane o tym majątku nie należą do kategorii dóbr osobistych chronionych w trybie art. 23 i art. 24 k.c. oraz art. 448 k.c. Dane o stanie majątku podlegają ochronie na podstawie ustawy z dnia 29.08.1997 r. o ochronie danych osobowych w razie ujawnienia danych osobowych w sposób

[216] Wyrok SA w Krakowie – I Wydział Cywilny z 12.06.2014 r., sygn. akt I ACa 507/14.
[217] Uchwała SN z 16.11.1993 r., sygn. akt I PZP 28/93.
[218] Wyrok SA w Poznaniu z 14.11.2003 r., sygn. akt I ACa 1062/03.

sprzeczny z ustawą i dlatego należy się odwołać do przepisu art. 415 k.c., który wyraża ogólną regułę odpowiedzialności deliktowej.

Z innej perspektywy publikowaniem danych zajmował się Sąd Apelacyjny w wyroku rozstrzygającym zagadnienie krzyżowania się praw dostępu do informacji publicznej, dóbr osobistych i ochrony danych osobowych, który dotyczył opublikowania na stronie internetowej organu publicznego niezanonimizowanych danych osobowych bez wiedzy i woli osoby, której one dotyczyły. Sąd uznał, że doszło do naruszenia dobra osobistego tej osoby, potwierdzając odrębność reżimu ochrony dóbr osobistych i danych osobowych. W sprawie tej Sąd[219] stwierdził, że dobrami osobistymi, które nie są wymieniane w mającym charakter otwarty katalogu kodeksowym, są prawo do prywatności i prawo do ochrony danych osobowych.
Ze względu na rozwój technologiczny i zjawisko „społeczeństwa informacyjnego", w którym wzrastają możliwości technicznego ingerowania w prywatność innych, dobra te zasługują na szczególną ochronę. Przy ocenie, czy nastąpiło wkroczenie w dziedziną chronionego prawem życia prywatnego, nie należy pojęcia tego absolutyzować, bowiem ze względu na stopień swojej ogólności, wymaga ono wykładni przy uwzględnieniu konkretnych okoliczności charakteryzujących daną sytuację. Reżim ochrony prawa do prywatności mieszczący się w ramach powszechnych dóbr osobistych (oparty na przepisach Konstytucji RP i przepisach prawa cywilnego) i reżim ochrony danych osobowych (oparty na przepisach Konstytucji RP oraz ustawy o ochronie danych osobowych), są wobec siebie niezależne.

W tym postępowaniu pozwany podnosił, że ustawa o ochronie danych osobowych przewiduje szczegółowy administracyjnoprawny tryb uprawniający jednostkę do ochrony jej danych osobowych przed ich nieuprawnionym przetwarzaniem i jest on czymś zupełnie innym niż ochrona dóbr osobistych na gruncie prawa cywilnego. W ocenie Sądu istotnie tryb administracyjnoprawny ochrony danych osobowych jest alternatywnym do cywilnoprawnego trybu ochrony danych osobowych w drodze roszczenia o naruszenie dóbr osobistych w postaci prawa do prywatności. Te dwa tryby są od siebie niezależne i nie wykluczają się. Uprawnionym do wyboru jednego z tych trybów lub każdego z nich jest osoba, której dane osobowe zostały użyte w sposób niezgodny z przepisami ustawy o ochronie danych osobowych, bądź której bezprawne upublicznienie danych osobowych naruszyło jej dobra osobiste określone w Kodeksie cywilnym.

Sąd zaaprobował stanowisko, że ustawa o ochronie danych osobowych nie reguluje wpływu przetwarzanych informacji i ich treści pod kątem ewentualnego naruszenia dóbr

[219] Wyrok SA w Gdańsku - I Wydział Cywilny z 18.02.2015 r., sygn. akt I ACa 785/14.

osobistych. W tym zakresie zastosowanie mają przepisy art. 23 i art. 24 k.c., co oznacza, że naruszenie zakazu rozpowszechniania danych osobowych nie jest automatycznie równoznaczne z bezprawnym naruszeniem dóbr osobistych. Prowadzi to do konkluzji, że fakt przetworzenia danych osobowych bez zgody zainteresowanego nie przesądza sam przez się o naruszeniu dóbr osobistych i podstawie do uzyskania ochrony na podstawie art. 23 i 24 k.c.[220] Podobne stanowisko zostało zaaprobowane w innym orzeczeniu, dotyczącym braku przekazania informacji o wygaśnięciu zobowiązań powoda do BIK, co spowodowało, że powodowi odmówiono udzielenia kredytu w innym banku, uniemożliwiając mu sfinalizowanie umowy zakupu sprzętu komputerowego, Sąd stwierdził, że uchybienie przepisom o ochronie danych osobowych nie w każdym wypadku musi prowadzić do naruszenia dóbr osobistych, konieczne jest więc zawsze poddanie ocenie przedmiotu, charakteru i skutków tego uchybienia. Zagadnienie to podsumowuje prezentowane już wcześniej stanowisko Sądu Najwyższego wskazujące, że jeżeli w wyniku nienależytej dbałości o interesy osoby której dane osobowe są gromadzone i przetwarzane następuje wkroczenie w sferę wartości o charakterze niemajątkowym, wiążących się z osobowością człowieka, uznanych powszechnie w społeczeństwie, to poza środkami administracyjnymi przewidzianymi w ustawie o ochronie danych osobowych pokrzywdzony może sięgnąć również po możliwości obrony przewidziane w art. 24 k.c.[221]

Na zjawisko krzyżowania się pojęć dobra osobiste i dane osobowe zwraca uwagę także orzecznictwo dotyczące takich informacji jak: nazwisko, sfera życia intymnego czy wizerunek, uznając, że innym dobrem osobistym w rozumieniu art. 23 k.c., które podlega ochronie prawnej jest nazwisko, a jego naruszenie lub zagrożenie naruszeniem jest podstawą roszczenia przewidzianego przepisem art. 24 k.c.. Imię i nazwisko identyfikuje bowiem osobę fizyczną, jako podmiot praw i obowiązków i jednocześnie określa tożsamość tego podmiotu. Nie można uznać jednak, że jest także jedynym - jeżeli w ogóle - wyznacznikiem określającym tożsamość etniczną osoby, do której przynależne są te dane.

Niewątpliwie takim wyznacznikiem nie jest imię danej osoby. Przewidziana ochrona dobra osobistego, jakimi są imię i nazwisko, nie ogranicza się tylko do zakazu naruszania tego dobra, ale i pozytywnego obowiązku używania pełnych danych osobowych identyfikujących daną osobę, przede wszystkim jednak to nazwisko określa tożsamość danej osoby[222]. Zgodnie z wyraźnym brzmieniem art. 23 k.c.

[220] Wyrok SA w Warszawie – I Wydział Cywilny z 25.11.2016 r., sygn. akt I ACa 1565/15.
[221] Wyrok SN – Izba Cywilna z 11.02.2015 r., sygn. akt I CSK 868/14.
[222] Wyrok SA w Szczecinie – I Wydział Cywilny z 17.03.2015 r., sygn. akt I ACa 868/14.

nazwisko człowieka stanowi jego dobro osobiste. Podobnie należy traktować imię, które łącznie z nazwiskiem, określa tożsamość osoby fizycznej. Nazwisko, ujmowane jako potwierdzenie przynależności danej osoby do rodziny, z której się wywodzi dany człowiek, stanowi jednocześnie podstawę identyfikacji danej osoby w społeczeństwie[223].

Do kategorii dóbr osobistych podlegających wyjątkowo ścisłej rygorystycznej ochronie należy sfera życia intymnego (seksualnego), jako składnik prawa do prywatności i integralności osobistej. Ochronie takiej podlegają także preferowane przez daną osobę poglądy i zachowania należące do szeroko pojętej etyki seksualnej. Do uznania naruszenia dobra osobistego wystarczające jest subiektywne poczucie dyskomfortu po stronie poszkodowanego, wynikające z bezprawnego wykroczenia w sferę jego życia intymnego poprzez publiczne przypisanie mu wyznawania określonego światopoglądu, obejmującego preferowane w tej sferze życia zasady etyki[224].

Odrębną kategorią dóbr osobistych jest wizerunek. Przez pojęcie wizerunku należy rozumieć każdą podobiznę bez względu na technikę wykonania, a więc fotografię, rysunek, wycinankę sylwetki, film, przekaz telewizyjny bądź przekaz wideo, a zatem jest nim niewątpliwie zdjęcie[225]. Zgodnie z orzeczeniem wydanym w sprawie I ACa 1452/13[226] pojęcie wizerunku obejmuje dostrzegalne, fizyczne cechy człowieka, tworzące jego wygląd i pozwalające na identyfikację osoby wśród ludzi jako obraz fizyczny, portret, rozpoznawalną podobiznę. Wymóg rozpoznawalności należy wiązać wyłącznie z formą przedstawienia danej osoby, a więc taką, która pozwala na ustalenie osobistych cech danej osoby w chwili sporządzania fotografii. Wymogu rozpoznawalności nie można wiązać z podobieństwem wizerunku z okresu edukacji szkolnej z aktualnym wizerunkiem danej osoby. W sprawie tej roszczenie powoda zostało oparte na podstawie wynikającej m.in. z prawa autorskiego i ustawy o ochronie danych osobowych, w konsekwencji czego Sąd stwierdził, że dla zastosowania art. 81 ust. 2 pkt 2 u.p.a.p.p. rozstrzygające znaczenie ma ustalenie w strukturze przedstawienia relacji między wizerunkiem osoby domagającej się ochrony a pozostałymi elementami jego treści. Co za tym idzie rozpowszechnianie wizerunku nie wymaga zezwolenia, jeśli stanowi on jedynie element akcydentalny lub akcesoryjny przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia. Zdjęcia klasowe utrwalają pewne zgromadzenie, w skład którego wchodzą osoby uczęszczające do tej samej klasy, a przy

[223] Wyrok SO we Wrocławiu – I Wydział Cywilny z 30.01.2014 r., sygn. akt I C 411/13.
[224] Wyrok SA w Poznaniu – I Wydział Cywilny z 21.10.2015 r., sygn. akt I ACa 475/15.
[225] Wyrok SA w Katowicach – I Wydział Cywilny z 28.05.2015 r., sygn. akt I ACa 158/15.
[226] Wyrok SA we Wrocławiu – I Wydział Cywilny z 30.01.2014 r., sygn. akt I ACa 1452/13.

tym wizerunek każdego z uczniów ma ten charakter, iż stanowi jedynie element akcesoryjny, którego usunięcie nie zmieniło by ani przedmiotu, ani charakteru przedstawienia. A co za tym idzie ich przetwarzanie również odbywa się w granicach prawa.

Odnosząc się do oceny roszczenia opartego na naruszeniu danych osobowych, Sąd uznał, że zakres ochrony wynikający z przepisów ustawy o ochronie danych osobowych, a przy tym przepisów, które nie odnoszą się do stosunków cywilnoprawnych, jest odmienny. To, że żądanie powoda zaniechania przetwarzania jego danych osobowych zostało uwzględnione nie oznacza, iż publikacja jego wizerunku stanowi naruszenie przepisów ustawy o prawie autorskim i prawach pokrewnych. Dane osobowe stanowią bowiem zbiór informacji na temat danej osoby pozwalających na jej identyfikację. Taki charakter ma umieszczenie w serwisie zdjęcia z wizerunkiem powoda wraz z oznaczeniem jego imienia i nazwiska. Domaganie się jedynie ochrony naruszonego wizerunku jednoznacznie wskazuje na odmienność tych stanów faktycznych. Nie można zatem przypisywać orzeczeniu sądu administracyjnego niejako prejudycjalnego charakteru dla rozstrzygnięcia niniejszej sprawy[227].

W tym miejscu podkreślenia wymaga, że takie podejście jak to prezentowane w orzeczeniu pod rządami RODO nie będzie mogło być uznane za poprawne z uwagi na regulacje art. 92 UODO, o której będzie mowa w dalszej części pracy. O aktualnej zmianie podejścia do relacji pomiędzy zdarzeniami, kwalifikowanymi jako naruszenie na gruncie prawa administracyjnego i prawa cywilnego świadczy także sprawa zawisła przed WSA w Warszawie za sygn. akt II SA/Wa 1801/20[228]. Stan faktyczny rozstrzygnięcia w tej sprawie stanowiły okoliczności, związane z kwestionowaniem przez skarżącego praktyki polegającej na tym, że kierowca autobusu prosił o podanie na głos imienia i nazwiska przez posiadacza biletu, by zweryfikować czy jest uprawniony do przejazdu, a następnie sam czytał te informacje na głos. W wyniku rozpoznania sprawy Sąd stwierdził, że przepisy RODO nie znajdują zastosowania do wszelkich przypadków przetwarzania danych osobowych (formą przetwarzania jest ich upublicznienie – tak art. 4 pkt 3 RODO), lecz tylko gdy chodzi o te, objęte zakresem danej regulacji. Zdaniem Sądu wobec przywołanych uwarunkowań uzasadniony jest wniosek, że – wobec wyartykułowanych celów przyjęcia RODO i treści jego regulacji wstępnych – akt ten dotyczy zdarzeń związanych z przetwarzaniem informacji (gromadzenie, transfer itp.) gdzie możliwe jest mechaniczne odnajdywanie informacji o osobach – ich danych osobowych – w szczególności w ramach systemów teleinformatycznych. Nie dotyczy ono zaś zdarzeń, pozostających w związku z ujawnieniem (a więc przetworzeniem) danych osobowych, w

[227] Wyrok SA we Wrocławiu – I Wydział Cywilny z 30.01.2014 r., sygn. akt I ACa 1452/13.
[228] Wyrok WSA w Warszawie z 11.05.2021 r., sygn. akt II SA/Wa 1801/20.

innych sytuacjach – np. możliwości poznania imienia i nazwiska określonej osoby, wobec głośnego jego wypowiedzenia (przez kierowcę czy pasażera autobusu), nawet gdy znajduje się ono równocześnie w określonym zbiorze informacji (liście pasażerów), choćby prowadzono ją w formie elektronicznej.

Inna ocena mogłaby dotyczyć przypadku, w którym określone informacje upowszechniane byłyby w takiej postaci, że technicznie możliwe byłoby ich niekontrolowane gromadzenie przez osoby nieuprawnione – bez wiedzy zainteresowanych. Sytuacja taka – bezspornie – nie miała jednak miejsca w rozpatrywanej sprawie. Według Sądu, co ma znaczenie dla rozpatrywanego w tym momencie pracy zagadnienia, jeżeli – według twierdzeń wnioskodawcy – wobec nieuprawnionej praktyki Spółki posługiwanie się przez realizujących na jej rzecz przewozy kierowców danymi osobowymi pasażerów w celu ich identyfikacji, doszło do naruszenia jego praw osobistych, np. prawa do prywatności, poszkodowanemu przysługują stosowne roszczenia względem sprawcy naruszeń. Właściwymi do rozstrzygania spraw w danym zakresie są sądy powszechne.

Istotne dla omawianego zagadnienia jest także orzeczenie Sądu Okręgowego w Warszawie z 12.03.2020 r.[229] rozstrzygające zakres ochrony przysługującej powodowi w następstwie upublicznienia zdjęcia przedmiotu należącego do powoda, nie zaś jego podobizny z perspektywy prawnoautorskiej i ochrony danych osobowych. W wyroku tym Sąd argumentuje, że „wiedza o powodzie, jako właścicielu pojazdu (...) przedstawionego na zdjęciu jest wiedzą niszową, ograniczoną do kręgu osób znających powoda osobiście. Przedmiot ten nie ma takiej siły identyfikacyjnej, która pozwalałaby utożsamić powszechnie, przez każdego przeciętnego odbiorcę powoda i jego pojazd, tak aby przez publikację obrazu tego pojazdu «przebijała» podobizna powoda. Siła skojarzenia przedmiotu i jego właściciela jest zbyt wątła, by przy najszerszym rozumieniu prawa do wizerunku przeciętny, nieznający uprzednio powoda osobiście odbiorca mógł utożsamić (...) z powodem". W orzeczeniu tym powołana została argumentacja dotycząca omawianego w pracy stanowiska Trybunału Sprawiedliwości UE wyrażonego w wyroku z 19.10.2016 r. (C – 582/14).

Analizowane rozstrzygnięcia podsumować można twierdzeniem, że w orzecznictwie Sądu Najwyższego przyjmuje się, iż prawo do dysponowania swoimi danymi osobowymi, będące emanacją tzw. autonomii informacyjnej jednostki, stanowi element dobra osobistego jakim jest prywatność. Argumentacja Sądu Najwyższego odwołuje się przy tym do orzecznictwa Trybunału Konstytucyjnego, który w omawianych wcześniej rozstrzygnięciach

[229] Wyrok SO w Warszawie z 12.03.2020 r., sygn. akt I C 214/19.

oraz w wyroku z 20.04.2002 r., sygn. akt K 41/0218, wyjaśnił, że ochrona życia prywatnego, gwarantowana w art. 41 Konstytucji RP, obejmuje także autonomię informacyjną (art. 51 Konstytucji RP), oznaczającą prawo do samodzielnego decydowania o ujawnieniu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów. Trybunał Konstytucyjny podkreślił, że autonomia informacyjna, której wyodrębnienie normatywne z całości ochrony prywatności przewiduje art. 51 Konstytucji RP, jest uzasadniona częstotliwością, uporczywością i typowością wkraczania w prywatność przez władzę publiczną. Trybunał Konstytucyjny stwierdził również, że normatywne wyodrębnienie w art. 51 ust. 2 Konstytucji RP odrębnego zakazu uprościło przedmiot dowodu, że takie wkroczenie nastąpiło.

Zagadnienie stosunku prawa ochrony danych osobowych do ochrony dóbr osobistych także stało się przedmiotem orzeczeń Sądu Najwyższego. Ich prezentację rozpocząć trzeba od wyroku Sądu Najwyższego z 28.04.2004 r.[230], w którym wskazano, że relacja pomiędzy powszechną ochroną dóbr osobistych a ochroną danych osobowych nie jest oczywista. Sąd Najwyższy podkreślił, że trafne są w jego ocenie poglądy doktryny wskazujące, że ustawa o ochronie danych osobowych nie zawiera żadnych odniesień ani do powszechnych dóbr osobistych w ogólności, ani np. do prawa do prywatności, jak również na to, że także Konstytucja nie łączy ochrony danych osobowych z prawem do prywatności, poświęcając tym kwestiom odrębne przepisy (art. 47 i 51)[231].

Jak uznał Sąd Najwyższy, „dane osobowe nie są tożsame z dobrami osobistymi, chociaż pewne ich rodzaje mogą złożyć się na elementy tożsamości i prywatności”[232]. W konsekwencji „naruszenie przepisów dotyczących ochrony danych osobowych może uzasadniać również ochronę przewidzianą w art. 23 i 24 k.c., o ile doprowadziło do naruszenia dóbr osobistych. Jednakże dane osobowe nie są tożsame z dobrami osobistymi”[233]. Dane osobowe nie są tożsame z dobrami osobistymi, chociaż pewne ich rodzaje mogą złożyć się na elementy tożsamości i prywatności[234] (por. wyrok Sądu Najwyższego z 13.12.2018 r., I CSK 690/17). Innymi słowy z samego naruszenia zasad przetwarzania danych osobowych nie wynika skutek w postaci naruszenia dobra osobistego. Jeżeli źródłem roszczenia o ochronę dóbr niemajątkowych jest czyn polegający na naruszeniu zasad przetwarzania danych osobowych to na powodzie, oprócz

[230] Wyrok SN z 28.04.2004 r., sygn. akt III CK 442/0219.
[231] B. Łukańko, *Uchybienie przepisom o ochronie danych osobowych jako naruszenie dobra osobistego – analiza na przykładzie orzecznictwa Sądu Najwyższego*, UWM 2019, s. 249.
[232] Wyrok SN z 13.12.2018 r., sygn akt. I CSK 690/17.
[233] Wyrok SA w Warszawie z 18.09.2019 r., sygn. akt VI ACa 254/18.
[234] Wyrok SN z 13.12.2018 r., sygn. akt I CSK 690/17.

wykazania zajścia takiego naruszenia, spoczywa obowiązek wskazania dobra osobistego naruszonego tym czynem oraz wykazania tego naruszenia[235].

Autonomia informacyjna jednostki nie jest nieograniczona. Ustawodawca przesądza bowiem o konieczności ujawnienia przez podmiot danych informacji dotyczących jego osoby w pewnych okolicznościach. Taka powinność musi jednak wynikać z przepisu ustawowego. Jak stwierdził TK w uzasadnieniu wyroku z 17.6.2008 r., autonomia informacyjna jednostki obejmuje prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, jak również prawo do sprawowania kontroli nad tymi danymi, jeśli znajdują się one w posiadaniu innych podmiotów. Elementem tak rozumianej autonomii informacyjnej jest zatem także prawo dostępu do danych osobowych oraz towarzyszące mu uprawnienia, m.in. prawo do sprostowania czy usunięcia danych osobowych. Pogląd ten należy podzielić. Trudno sobie bowiem wyobrazić realizację autonomii informacyjnej człowieka bez zapewnienia mu możliwości wykonywania kontroli nad przetwarzaniem przez inne podmioty informacji dotyczących jego osoby. Zakres przedmiotowy autonomii informacyjnej obejmuje informacje dotyczące osoby fizycznej. Jak podkreśla się w orzecznictwie, są to zarówno dane o charakterze ściśle personalnym (osobowym), jak i informacje dotyczące majątku i sfery ekonomicznej jednostki[236].

Zasady ochrony danych osobowych na gruncie RODO – zagadnienie podstaw prawnych naprawienia szkody

RODO w sposób znaczący zmieniło zagadnienia dotyczące odpowiedzialności, w tym odpowiedzialności cywilnej. Wprowadziło odrębne przesłanki naprawienia szkody, formułując ich zasady w art. 79 i 82 i n., zaś w art. 92 UODO doprecyzowano, że „w zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23.04.1964 r. – Kodeks cywilny".

W myśl art. 79 ust. 1 RODO bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77 RODO, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jego danych

[235] Wyrok SO w Warszawie z 12.03.2020 r., sygn. akt I C 214/19.
[236] M. Kuba, *Zasada przejrzystości przetwarzania danych osobowych jako instrument ochrony autonomii informacyjnej pracownika*, MOPR 2020/12.

osobowych z naruszeniem niniejszego rozporządzenia. Zgodnie natomiast z art. 82 ust. 1 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

W piśmiennictwie podnoszone jest, że konstrukcja odpowiedzialności odszkodowawczej z RODO skłania do refleksji, że obecny stan regulacji prywatnoprawnej na poziomie Unii świadczy o trudnościach w harmonizacji czy ujednolicaniu przepisów w tym zakresie. Po pierwsze, podstawową metodą regulacji są dyrektywy (przede wszystkim dyrektywy w zakresie prawa konsumenckiego – prawa umów) dające państwom członkowskim szansę wdrożenia przepisów koherentnych z ich systemami prawnymi (nawet w ramach dyrektyw maksymalnych). Po drugie, brak jest kompleksowej regulacji materii odpowiedzialności odszkodowawczej na poziomie unijnym. Najbardziej istotna w tym zakresie wydaje się regulacja odpowiedzialności za produkt niebezpieczny, a do tej pory nie udało się kompleksowo uregulować w prawie unijnym kwestii odpowiedzialności odszkodowawczej, i to zarówno w ramach reżimu umownego, jak i pozaumownego.

Biorąc pod uwagę przedstawiony zarys stanu *aquis communautaire* w zakresie prawa prywatnego, wątpliwości może budzić zamieszczenie materii odpowiedzialności odszkodowawczej w rozporządzeniu ogólnym. Wątpliwości związane z regulacją art. 82 RODO wynikają przede wszystkim z problemu umiejscowienia regulacji rozporządzenia ogólnego w kontekście przepisów prywatnoprawnych państw członkowskich. W tym zakresie możliwe są następujące rozwiązania:

1. regulację art. 82 RODO należy umiejscowić w ramach jednego z dwóch reżimów odpowiedzialności odszkodowawczej: deliktowego lub kontraktowego;
2. regulacja art. 82 RODO stanowi samodzielny i wyczerpujący reżim odpowiedzialności odszkodowawczej niezależny od krajowych regulacji prywatnoprawnych[237].

W literaturze wskazuje się również, że wykładnia art. 82 RODO musi uwzględniać kontekst przepisów prawa krajowego (polskiego). Jest to istotne z (co najmniej) dwóch względów. Po pierwsze dlatego, że art. 82 RODO nie reguluje wszystkich istotnych kwestii. Po drugie, art., 92 UODO, tj . przepis krajowy odwołuje się do przepisów RODO. W tym zakresie istotne jest zestawienie trzech przepisów tj. ar. 79 i 82 RODO z art. 92 UODO [238]. W tym miejscu podkreślenia wymaga, że barierą ujednolicenia analizowanych zagadnień odpowiedzialności

[237] M. Gumularz, *Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, EPS 2017/5/140, s. 31–36.
[238] M.Gumularz [w:] *Meritum. Ochrona danych osobowych*, red. Dominik Lubasz, Warszawa 2021, s. 512.

na szczeblu europejskim są odmienności między systemami prawnymi państw członkowskich. Jako ich przykład w literaturze podaje się różne stanowiska, jakie poszczególne systemy prawne zajmują w kwestii obowiązków przedkontraktowych, w tym obowiązku zachowania stron zgodnie z zasadą dobrej wiary, i odpowiedzialności za zerwanie rokowań, w kwestii ustalenia treści praw i obowiązków stron, w tym istnienia dodatkowych obowiązków, wynikających z zasad dobrej wiary, jak obowiązek udzielania informacji, obowiązek współpracy itd., w kwestii przyczyn i skutków niewykonania zobowiązania, w tym znaczenia siły wyższej i niemożliwości świadczenia dla ustalenia odpowiedzialności dłużnika, czy mośliwości żądania realnego wykonania zobowiązania[239].

Kształtowanie się zasady odesłania do przepisów krajowych

Artykuł 92 UODO pierowtnie miał mieć inny kształt niż ostatecznie przyjęty. Zgodnie z projektem ustawy przedstawionym przez Ministerstwo Cyfryzacji z dnia 12.09.2017 r.[240] zagadnienia odpowiedzialności cywilnej regulować miał projektowany rozdział 8 ustawy, stanowiący, że :

Artykuł 78.1. Każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać, zaniechania tego działania a także może żądać ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. 2. Wystąpienie z roszczeniem, o którym mowa w ust. 1, nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. 3. W zakresie nieuregulowanym rozporządzeniem 2016/679 oraz niniejszą ustawą dochodzenie roszczeń, o których mowa w ust. 1, następuje na zasadach określonych przepisami Kodeksu cywilnego. Artykuł 79.1. Do postępowania w sprawach roszczeń dochodzonych na podstawie art. 78, w zakresie nieuregulowanym niniejszą ustawą, stosuje się przepisy Kodeksu postępowania cywilnego.

W uzasadnieniu do projektu ustawy została przedstawiona następująca argumentacja na poparcie projektowanych regulacji. Realizacja normy kompetencyjnej wskazanej w art. 79 ust. 1 RODO nie może naruszać bezpośrednio skutecznej normy wyrażonej w art. 82 RODO (tj. nie może ograniczać dochodzenia roszczeń, bazując na tej podstawie prawnej). Zgodnie z treścią art. 82 ust. 1 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego RODO, ma prawo uzyskać od administratora lub podmiotu

[239] J. Pisuliński Kilka pytań o europejski kodeks cywilny Transformacje prawa prywatnego 2/2006, str. 99-106
[240] Zob. https://odoserwis.pl/a/1149/projekt-ustawy-o-ochronie-danych-osobowych-z-dnia-12-wrzesnia-2017-r

przetwarzającego odszkodowanie za poniesioną szkodę. W art. 82 ust. 1 RODO chodzi więc o roszczenia majątkowe (art. 82 ust. 5 mówi o „zapłacie" odszkodowania), które można dochodzić w razie zaistnienia szkody majątkowej lub niemajątkowej[241]. W doktrynie i orzecznictwie, nie budzi wątpliwości, iż naruszenie danych osobowych nie zawsze stanowi jednocześnie naruszenie dóbr osobistych. Artykuł 23 k.c. zawiera otwarty katalog dóbr osobistych. Natomiast dane osobowe ujmowane są jako kategoria dobra osobistego – prywatności. Dane osobowe nie mają więc charakteru samoistnego dobra osobistego[242]. Jednocześnie w piśmiennictwie podkreśla się, że „prywatność jest pojęciem wieloznacznym, trudnym do zdefiniowania. W wyjaśnieniach doktryny dotyczących istoty prywatności zwraca się zwłaszcza uwagę na aspekt poszanowania prawa człowieka do odosobnienia się, pozostawienia w spokoju, co przekłada się na ujęcie prywatności jako obszaru niedostępności, wolnego od ingerencji zewnętrznej, stwarzającego warunki do swobodnego kształtowania własnego życia i rozwoju własnej osobowości. Wskazuje się również, w nawiązaniu do przepisów konstytucyjnych, że za istotny komponent prywatności należy uznać autonomię człowieka w decydowaniu o swoim życiu osobistym (art. 47 Konstytucji RP), a także autonomię informacyjną"[243].

Z uzasadnienia projektu ustawy wynika, że przedstawione rozumienie dobra osobistego tj. prywatności rodzi ryzyko wąskiego ujęcia w jej ramach danych osobowych (m.in. pojawia się wątpliwość czy w ramach art. 24 § 1 k.c. można żądać, ażeby osoba, która dopuściła się naruszenia np. odmówiła wydania kopii danych, dopełniła czynności potrzebnych do usunięcia jego skutków). W związku z tym projektodawca zdecydował się na wprowadzenie regulacji odrębnej w art. 78 ust. 1 projektu, dającej wyraźną cywilnoprawną podstawę roszczeń o charakterze niemajątkowym. Dochodzenie roszczeń powiązano z naruszeniem praw podmiotów danych wynikających z przepisów o ochronie danych osobowych (nie tylko RODO). W ten sposób, bez potrzeby definiowania dobra osobistego (danych osobowych) skonstruowano podstawę dochodzenia cywilnoprawnych roszczeń niemajątkowych w razie naruszenia praw przysługujących na podstawie przepisów o ochronie danych osobowych. Należy zwrócić w tym miejscu uwagę, iż art. 78 ust. 1 projektu dotyczył wyłącznie dokonanego

[241] M. Gumularz, *Wpływ regulacji odpowiedzialności...*
[242] P. Sobolewski, *Kodeks cywilny. Komentarz*, t. 1, *Przepisy wprowadzające. Część ogólna. Własność i inne prawa rzeczowe*, red. K. Osajda, Warszawa 2017;; P. Machnikowski, *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski red., Warszawa 2016, komentarz do art. 23 k.c., teza 2.
[243] J. Panowicz-Lipska, *Kodeks cywilny. Komentarz. Księga I. Część ogólna*, red. J. Gutowski, Warszawa 2016, komentarz do art. 23 k.c., teza 13.

naruszenia praw przysługujących na mocy przepisów o ochronie danych osobowych. W tej sytuacji przysługiwać miało roszczenie o:

- zaniechanie tego działania;
- to, aby ten kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków[244].

Rządowy projekt ustawy nr 2410[245], który wpłynął do Sejmu 5.04.2018 r. zawierał jako propozycję wdrożenia do polskiego porządku prawnego regulację art. 79 RODO przepis o treści uchwalonego art. 92 UODO, który stanowi wyłącznie o odpowiednim stosowaniu przepisów k.c. (odpowiadający w swej treści projektowanemu art. 79 ust.1, bez uwzględnienia projektowanego art. 78). Z uzasadnienia w/w projektu wynikało już inne podejście do konieczności wprowadzenia wyraźnej cywilnoprawnej podstawy roszczeń o charakterze niemajątkowych. Powtórzona w nim została argumentacja, że rozporządzenie nie wymaga wprowadzenia do systemu prawa państwa członkowskiego nowego środka na płaszczyźnie prawa materialnego, jeżeli obowiązujące przepisy mogą stanowić skuteczną podstawę roszczeń związanych z naruszeniem ogólnego rozporządzenia (czy ogólnie przepisów o ochronie danych osobowych). Zwrócono uwagę, iż realizacja normy kompetencyjnej wskazanej w art. 79 ust. 1 RODO nie może naruszać bezpośrednio skutecznej normy wyrażonej w art. 82 RODO (tj. nie może ograniczać dochodzenia roszczeń bazując na tej podstawie prawnej).

Zgodnie z treścią art. 82 ust. 1 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego RODO, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Podobnie jak w poprzednim uzasadnieniu projektu wskazano, że w art. 82 ust. 1 RODO chodzi więc o roszczenia majątkowe (art. 82 ust. 5 RODO mówi o „zapłacie" odszkodowania), które można dochodzić w razie zaistnienia szkody majątkowej lub niemajątkowej i powołano stanowisko M. Gumularza. Argumentację dotyczącą projektowanych poprzednio roszczeń pominięto, a problem został podsumowany jedynie stwierdzeniem, że projektowane regulacje dotyczą roszczeń odszkodowawczych, które mogą być realizowane w przypadku poniesienia szkody majątkowej lub niemajątkowej w wyniku naruszenia przepisów RODO na podstawie art. 82

[244] Zob. https://legislacja.rcl.gov.pl/docs//2/12302950/12457664/12457665/dokument308360.pdf
[245] Zob. https://www.sejm.gov.pl/sejm8.nsf/PrzebiegProc.xsp?nr=2410

RODO. Dodane zostało, że projektowane przepisy mają charakter porządkowy i przesądzają cywilnoprawny tryb dochodzenia roszczeń wskazanych w projekcie[246].

Środek ochrony prawnej – art. 79 RODO

Poza zakresem regulacji RODO państwa członkowskie mają, co do zasady, swobodę regulacji, z zastrzeżeniem, że nie mogą one w ten sposób naruszać celu rozporządzenia. Obowiązek prawodawczy poza zakresem zastosowania RODO może wynikać z jego treści, np. art. 79 RODO, w związku z koniecznością zapewnienia efektywności tej regulacji. Zgodnie z motywem 8 RODO, w zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – jeśli jest to niezbędne, aby krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swojego prawa krajowego. Przedstawiony motyw podkreśla ograniczenie kompetencji prawodawczej państw członkowskich w ramach objętych zakresem rozporządzenia ogólnego[247].

Wbrew ostatecznemu stanowisku ustawodawcy, który wyszedł z założenia, że odesłanie do Kodeksu cywilnego zamyka temat roszczeń odszkodowawczych, które mogą być realizowane w przypadku poniesienia szkody majątkowej lub niemajątkowej w wyniku naruszenia przepisów RODO w doktrynie widoczne są poglądy przeciwne. Podnoszą one, że RODO, regulując kwestie dochodzenia roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych w art. 79 i 82, nie czyni tego w sposób wyczerpujący. Artykuł 79 ust. 1 RODO wymaga od państw członkowskich, aby w ich systemach prawnych istniały skuteczne środki ochrony prawnej przed sądem, w przypadku gdy podmiot danych uzna, że prawa przysługujące mu na mocy RODO zostały naruszone w wyniku przetwarzania jego danych osobowych z naruszeniem przepisów tego rozporządzenia. Polski ustawodawca nie zdecydował się na wprowadzenie do systemu prawa nowego środka na płaszczyźnie prawa materialnego, rozstrzygnął jednak, że uzupełnieniem unijnych przepisów dotyczących roszczeń podmiotu danych będzie regulacja Kodeksu cywilnego[248].

W literaturze podkreśla się, że art. 79 ust. 1 RODO:

1. obejmuje swoim zakresem (przede wszystkim w aspekcie proceduralnym) konieczność zapewnienia skutecznego mechanizmu dochodzenia roszczeń odszkodowawczych z tytułu naruszenia przepisów ogólnego rozporządzenia na podstawie art. 82 RODO;

[246] Zob. https://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=2410
[247] M. Gumularz, *Wpływ regulacji odpowiedzialności...*
[248] N. Zawadzka [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, komentarz do art. 92.

2. nie wyklucza wprowadzenia na płaszczyźnie prawa materialnego innych (niż roszczenie odszkodowawcze z art. 82 RODO) podstaw dochodzenia roszczeń;
3. nie wymusza wprowadzenia do systemu prawa państwa członkowskiego nowego środka na płaszczyźnie materialnoprawnej, jeżeli obowiązujące przepisy mogą stanowić podstawę roszczeń opartych na naruszeniu ogólnego rozporządzenia w relacji: podmiot danych – administrator danych/procesor, a jednocześnie stanowią skuteczny środek ochrony prawnej w tym zakresie. Podnoszone są tym samym argumenty dla uzasadnienia tezy, że obowiązujące przepisy mogą stanowić podstawę roszczeń opartych na naruszeniu ogólnego rozporządzenia.

Celem uzasadnienia tezy o relacjach M. Gumularz zwraca uwagę, że jako uzupełnienie roszczenia odszkodowawczego (za szkodę majątkową lub niemajątkową) w związku z naruszeniem ogólnego rozporządzenia w relacji podmiot danych – administrator/procesor można traktować roszczenia niemajątkowe, które w związku z naruszeniem dóbr osobistych (np. prawa do prywatności) można dochodzić na podstawie art. 24 § 1 zdania 1–2 k.c.[249].

Podobnego zdania jest W. Kotschy , według którego art. 79 RODO wskazuje, że:

1. postępowania wprowadzone przez państwa członkowskie jako wypełnienie obowiązków z art. 77 i 78 RODO powinny być „skutecznym środkiem prawnym" w rozumieniu art. 47 KPP;
2. w sytuacji, gdy skarga nie może być wniesiona przed organ nadzorczy, zgodnie z RODO, państwa członkowskie muszą wprowadzić „skuteczny środek prawny" poza postępowaniami wprowadzonymi jako wypełnienie obowiązków z art. 77 i 78 RODO;
3. nie jest wymagane wprowadzenie dodatkowego w stosunku do tego z art. 77 i 78 RODO środka prawnego gwarantującego bezpośredni dostęp do sądu[250].

Z innej perspektywy przedstawia to zagadnienie S. Kotecka-Kral, twierdząc, że poprzez środek ochrony prawnej podmiot danych może żądać od administratora lub procesora konkretnego działania lub jego zaprzestania, w tym także odszkodowania, o którym mowa w osobnym art. 82 RODO. Środkiem ochrony prawnej będzie powództwo zmierzające do nakazania działania lub zaniechania lub usunięcia skutków naruszenia. Nieuprawnione jest zawężanie zastosowania art. 79 RODO do roszczeń o charakterze wyłącznie odszkodowawczym (art. 82 RODO). W ramach omawianego środka ochrony prawnej będzie można dochodzić także roszczeń o charakterze prewencyjnym. Istotne znaczenie z punktu

[249] M. Gumularz, *Wpływ regulacji odpowiedzialności...*, s. 35-36

[250] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021, komentarz do art. 82.

widzenia osób, których dane dotyczą, ma fakt oderwania podstawy potencjalnych roszczeń opartych na art. 79 RODO od naruszenia dóbr osobistych, w tym zwłaszcza prawa do prywatności i oparcia ich na naruszeniu praw zagwarantowanych przepisami RODO.

Ogólne rozporządzenie o ochronie danych przewiduje oddzielną regulację w przypadku poniesienia przez podmiot danych szkody majątkowej lub niemajątkowej w wyniku naruszenia przepisów rozporządzenia przez administratora lub podmiot przetwarzający (art. 82 RODO). Podstawy materialnoprawnej roszczeń, które mogą być dochodzone na podstawie art. 79 RODO, należy więc upatrywać przede wszystkim w przepisach RODO, zwłaszcza zawartych w jego rozdziale III, ustanawiającym m.in. obowiązki informacyjne administratora wobec podmiotu danych i prawa podmiotu danych, np. dostępu do danych, do sprostowania danych, do usunięcia danych, do ograniczenia przetwarzania danych czy do przenoszenia danych. Jeśli administrator nie realizuje praw podmiotów danych związanych z przetwarzaniem danych osobowych, podmioty danych mogą przed sądem dochodzić swoich praw, niezależnie od uprawnienia przewidzianego w art. 77 RODO (skarga do organu nadzorczego). Organ nadzorczy, zgodnie z treścią art. 58 ust. 2 lit. c RODO, może z własnej inicjatywy, jak również na skutek wniesionej skargi, nakazać administratorowi lub podmiotowi przetwarzającemu spełnienie żądania osoby, której dane dotyczą, wynikającego z praw przysługujących jej na mocy ogólnego rozporządzenia o ochronie danych (a także aktów delegowanych i wykonawczych przyjęte na mocy RODO oraz prawa państwa członkowskiego doprecyzowującego RODO). S. Kotecka-Kral uważa, że w przypadku obowiązywania materialnoprawnej podstawy roszczenia w prawie krajowym również można z niej skorzystać przy inicjowaniu na podstawie art. 79 RODO postępowania sądowego. Z pewnością mieścić się tu będą roszczenia związane z ochroną dóbr osobistych, w szczególności z ochroną prywatności[251]. To oznacza, że w tym zakresie podziela pogląd M. Gumularza.

Rozważając dalej dotychczasowe piśmiennictwo w tym temacie wskazać należy także na następujące poglądy. W odróżnieniu od art. 82 RODO, który kształtuje samodzielną podstawę roszczeń odszkodowawczych (por. komentarz do art. 82), art. 79 RODO stanowi więc wyłącznie normę kompetencyjną (w obecnym stanie prawnym odsyłającą do przepisów Kodeksu cywilnego w zakresie ochrony dóbr osobistych), która nie może być traktowana jako bezpośrednia podstawa do dochodzenia roszczeń. Jak twierdzi M. Świerczyński art. 79 ust. 2 RODO odnosi się (choć nie wynika to wprost z jego brzmienia) do postępowania cywilnego. Dotyczy zatem tylko drogi cywilnej zaskarżania aktów naruszenia ochrony danych osobowych

[251] S. Kotecka-Kral, *Sądowe środki ochrony...*, s. 829-856.

do sądu (art. 79 RODO), a nie skargi do organu nadzorczego (art. 77 RODO). Oba postępowania mają charakter niezależny i osobie, której dane są przetwarzane, służy prawo wyboru zastosowania jednego z nich lub też obu. Zdaniem M. Świerczyńskiego postępowanie z art. 79 RODO nie jest nowym trybem sądowo-administracyjnym i należałoby wiązać je na płaszczyźnie polskiego prawa materialnego z roszczeniami o naruszenie dóbr osobistych z art. 24 k.c. bez wprowadzania dodatkowego (trzeciego) trybu dochodzenia roszczeń[252]. Wydaje się, że decydujące znaczenie dla oceny prezentowanych powyżej stanowisk wykształtuje dopiero praktyka formułowania roszczeń i ich ocena sądowa.

Podstawa prawna dochodzenia roszczeń z art. 82 RODO

Przepisy art. 82 RODO mają charakter *stricte* prywatnoprawny i dotyczą horyzontalnej relacji pomiędzy administratorem lub podmiotem przetwarzającym dane a podmiotem danych. Prawodawca unijny w art. 82 RODO ustanowił samodzielną podstawę roszczeń odszkodowawczych, związanych z przetwarzaniem danych osobowych z naruszeniem przepisów RODO; brak takiej podstawy prawnej w prawie krajowym nie pozbawia zatem podmiotu danych prawa do żądania odszkodowania. Roszczenia odszkodowawcze z art. 82 RODO mogą być dochodzone równolegle ze środkami ochrony prawnej przewidzianymi w art. 77 RODO (skarga do organu nadzorczego) i art. 79 RODO (sądowy środek ochrony prawnej przeciwko administratorowi lub podmiotowi przetwarzającemu)[253].

Według poglądów prezentowanych w piśmiennictwie przesłankami odpowiedzialności z art. 82 RODO są:

1. poniesienie przez osobę, której dane dotyczą, szkody majątkowej lub niemajątkowej;
2. naruszenie przez administratora lub podmiot przetwarzający przepisów RODO (w tym aktów delegowanych, wykonawczych lub przepisów prawa krajowego przyjętych na mocy przepisów RODO);
3. zaistnienie związku przyczynowego pomiędzy szkodą a naruszeniem;
4. wina po stronie administratora lub procesora (a contrario art. 82 ust. 3 RODO)[254].

Jak wskazuje się w literaturze, przesłanki te są zbliżone do tych z art. 415 k.c. z tym że w ramach odpowiedzialności deliktowej w Kodeksu cywilnego nie ma, co do zasady, domniemania winy. Co istotne, podobnie jak to ma (co do zasady) miejsce w obrębie

[252] *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021
[253] S.Kotecka-Kral, *Sądowe środki ochrony...*, s. 829-856.
[254] P. Zawadzka-Filipczyk, D. Jarmużek, E. Jagiełło-Jaroszewska, *RODO. Ochrona danych...*, s. 1049–1050; podobnie G. Zanfir-Fortuna, [w:] *The EU General Data Protection Regulation*, s. 1175–1176.

odpowiedzialności deliktowej, kwestia nastawienia psychicznego sprawcy czynu (umyślność lub nieumyślność) jest irrelewantna na tle art. 82 RODO[255]. Należy przyjąć, że o ile nie ukształtuje się swoiste rozumienie (na poziomie prawa unijnego) przesłanki winy i związku przyczynowego, o tyle wydaje się, że w tym zakresie możliwe jest ostrożne odwołanie się do rozumienia kształtowanego w obrębie prawa deliktów w zakresie nienaruszającym celu rozporządzenia ogólnego. Jak jednocześnie uważa M. Gumularz, stosowanie do art. 82 RODO i przepisów Kodeksu cywilnego o czynach niedozwolonych (art. 415 i n. k.c.) będzie rodzić wątpliwości przede wszystkim w odniesieniu do art. 429 k.c. Dodatkowo wątpliwości może budzić stosowanie przepisów wyłączających winę i bezprawność (np. stan wyższej konieczności) oraz stosowanie przepisów o podżeganiu i pomocnictwie (art. 422 k.c.). Wydaje się, że regulacja art. 429 k.c. nie daje się pogodzić z treścią art. 82 ust. 3 RODO. Okolicznością wyłączającą odpowiedzialność zgodnie z art. 82 ust. 3 RODO jest brak winy za zdarzenie powodujące szkodę, a nie brak winy w wyborze[256]. Należy również powiedzieć, że w art. 82 RODO nie ma odwołania do naruszenia dóbr osobistych, jak również nie określono rodzajów roszczeń odszkodowawczych.

Na gruncie polskich przepisów w przypadku szkody niemajątkowej przysługują poszkodowanemu roszczenia majątkowe i niemajątkowe. Jak zasadnie argumentuje M. Gumularz,[257] chociaż art. 82 RODO nie odwołuje się do przesłanki naruszenia dobra osobistego, to jednak powstanie szkody niemajątkowej, o której mowa w tym przepisie, siłą rzeczy będzie [na gruncie obowiązujących obecnie przepisów – przyp. aut.] konsekwencją naruszenia dobra osobistego"[258].

Artykuł 82 ust. 1 RODO nie odnosi się do stosunku obligacyjnego łączącego osobę, która poniosła szkodę, z administratorem lub podmiotem przetwarzającym, który miałby być źródłem odpowiedzialności odszkodowawczej. Z tego względu należy zgodzić się ze stanowiskiem, że regulacji art. 82 RODO bliżej jest do reżimu odpowiedzialności deliktowej. Jednak z uwagi na okoliczność, że przepis ten nie stanowi kompleksowej regulacji zasad tej odpowiedzialności, przepisy Kodeksu cywilnego można stosować w zakresie w nim nieuregulowanym (np. dotyczących kwestii przedawnienia roszczeń odszkodowawczych) lub szczątkowo uregulowanym (np. w odniesieniu do rodzajów roszczeń odszkodowawczych czy okoliczności wyłączających winę). Stosowanie przepisów o deliktach możliwe jest wyłącznie

[255] P. Zawadzka-Filipczyk, D. Jarmużek, E. Jagiełło-Jaroszewska, *RODO. Ochrona danych...*, s. 1050.
[256] M. Gumularz [w:] *Ustawa o ochronie...*, red. M. Gumularz, K. Kozieł, P. Kozik, s. 438.
[257] M. Gumularz, *Wpływ regulacjiw ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, EPS 2017/5, s. 34.
[258] *Ogólne rozporządzenie o ochronie...*, red. P. Litwiński.

w zakresie nieuregulowanym w art. 82 RODO, tj. poza kwestią przesłanek odpowiedzialności, solidarnej odpowiedzialności administratora i procesora oraz roszczeń regresowych między tymi podmiotami[259].

Do omawianej powyżej przesłanki winy odnosi się przepis ust. 3 artykułu 82 RODO, w którym przewidziane zostało zwolnienie z odpowiedzialności odszkodowawczej. Zgodnie z tym przepisem, administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności odszkodowawczej, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie (wynikające z działania bądź zaniechania), które doprowadziło do powstania szkody. Oznacza to, że odpowiedzialność odszkodowawcza została oparta na zasadzie winy. Pojęcie winy obejmuje zarówno winę umyślną (zamiar bezpośredni lub zamiar ewentualny), jak i winę nieumyślną (lekkomyślność lub niedbalstwo)"[260].

W piśmiennictwie wyrażane są także inne poglądy, co do przesłanek odpowiedzialności, które wskazując na następujące okoliczności. Mając świadomość tego, że poszczególne normy wynikające z RODO mogą być adresowane wyłącznie do administratora, inne zaś – do podmiotów przetwarzających, można odnieść wrażenie, że uregulowana w art. 82 RODO odpowiedzialność uzależniona jest zawsze od bezprawności. Oznaczałoby to, że warunkiem odpowiedzialności zarówno administratora, jak i podmiotu przetwarzającego, jest naruszenie tych reguł dotyczących przetwarzania danych osobowych, które adresowane są do tego z podmiotów, który miałby zostać pociągnięty do odpowiedzialności. Takie założenie nie byłoby właściwe. W treści RODO doprecyzowano, że o ile podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające (lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom), o tyle administrator uczestniczący w przetwarzaniu odpowiada za „szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie". Taka treść przytoczonego przepisu wydaje się z kolei oznaczać, że administrator zlecający przetwarzanie danych podmiotowi trzeciemu (podmiotowi przetwarzającemu) odpowiada za szkody wyrządzone w wyniku bezprawnego (sprzecznego z normami adresowanymi bezpośrednio do tego podmiotu) przetwarzania danych osobowych przez ten podmiot[261].

[259] S. Kotecka-Kral, *Sądowe środki...*, s. 829–856.
[260] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 648.
[261] R. Strugała, *RODO a odpowiedzialność odszkodowawcza. Podstawowe problemy odpowiedzialności za szkodę spowodowaną nieprawidłowym przetwarzaniem danych osobowych*, „Monitor Prawniczy" 2018/17.

Zdaniem D. Klimas i P. Wróbel odpowiedzialność na gruncie RODO oparta jest na zasadzie winy, nie na zasadzie ryzyka. W rezultacie tego administrator nie musi już wykazywać na przykład faktu działania siły wyższej lub wystąpienia innego zdarzenia, nad którym nie mógł mieć kontroli, którego nie mógł przewidzieć, ani nad nim zapanować. Jednocześnie według poglądów cytowanych Autorów należy pamiętać, że wina administratora nie musi polegać na jego umyślnym działaniu, ale także na zaniechaniu oraz specyficznej dla RODO odpowiedzialności związanej z błędnym wyborem (winą w wyborze) lub nieprawidłowym nadzorem nad procesorem.[262] Stanowisko takie należy przyjąć, dlatego że w polskiej wersji językowej pojawia się słowo „wina" zamiast „odpowiedzialność", którego prawidłowe zastosowanie wskazywałoby na oparcie odpowiedzialności na zasadzie ryzyka. Nie budzi wątpliwości fakt, że zakres semantyczny tych słów znacząco różni się, a „udowodnienie braku winy" jest zdecydowanie węższym znaczeniowo wyrażeniem niż „udowodnienie braku odpowiedzialności". Należy podkreślić, że tłumaczenie art. 23 dyrektywy 95/46 formułującego zasady odpowiedzialności administratora nie zawierało omyłki terminologicznej. Błąd ten niesie za sobą poważne konsekwencje w określaniu granic odpowiedzialności znacząco je zawyżając[263].

To stanowisko doktryny wymaga komentarza sprowadzającego się do stwierdzenia, że takie kategoryczne rozumienie sytuacji prawnej, w której zastąpienie w tłumaczeniu słowa „wina" na „odpowiedzialność", wskazywałoby na oparcie odpowiedzialności na zasadzie ryzyka jest mylne. Zasady odpowiedzialności mają za zadanie wyjaśnić sens społeczny i mechanizm działania przepisów, według których odpowiedzialność za szkodę ponosi dany podmiot. W sferze czynów niedozwolonych możemy wyróżnić odpowiedzialność opartą na zasadzie winy i odpowiedzialność, która powstaje niezależnie od winy, jako sam skutek. Oprócz zasady winy występuje więc zasada ryzyka i zasada słuszności, które pełnią rolę uzupełniającą, dlatego odpowiedzialność może być oparta na różnych zasadach i jest przez to znaczeniowo szerszym pojęciem niż pojęcie winy.

Zdaniem A. Błaszczyńskiej podkreślenia wymaga, że odpowiedzialność administratora (i analogicznie wprowadzona w RODO po raz pierwszy – odpowiedzialność podmiotu przetwarzającego) została na gruncie RODO w sposób znaczący ograniczona względem dyrektywy 95/46/WE. Nowa regulacja wprowadza zmiany na gruncie RODO w stosunku do dotychczasowego stanu prawnego i relacji wobec Kodeksu cywilnego. Zarówno

[262] D. Klimas, P. Wróbel [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017, s. 107.
[263] D. Klimas, P. Wróbel [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, *Reforma ochrony...*, s. 110.

administrator, jak i podmiot przetwarzający mogą się uwolnić od odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody. Prawodawca unijny zdecydował się zatem na bardzo daleko idące ograniczenie odpowiedzialności tych podmiotów, co może być krytykowane. Dotychczas w dyrektywie 95/46/WE przewidywano jedynie zwykłą, niekwalifikowaną przesłankę odpowiedzialności administratora. To rozwiązanie zostało powielone w projekcie RODO w którym w art. 77 ust. 3 stanowiono, że: „administrator oraz podmiot przetwarzający mogą uwolnić się od odpowiedzialności odszkodowawczej w całości lub w części, jeżeli udowodnią, że nie są odpowiedzialni za zdarzenie, które doprowadziło do powstania szkody". Zdaniem tej Autorki w odniesieniu do obecnie obowiązującego stanu prawnego, zważywszy na sprzeczności w zakresie przesłanki odpowiedzialności między dyrektywą 95/46/WE a zasadami ogólnymi Kodeksu cywilnego, które wymagają dla zaistnienia odpowiedzialności na gruncie art. 415 k.c. oraz 448 k.c. zawinienia, stan prawny przynajmniej w polskim porządku prawnym nie ulegnie zmianie. Zmiana zasadnicza dokona się jednak w zupełnie innym, ale niezwykle doniosłym aspekcie, mianowicie prawodawca unijny wprowadza do RODO domniemania winy administratora oraz podmiotu przetwarzającego, przenosząc na nich ciężar dowodu, że winy nie ponoszą[264]. Konieczność ustanowienia takiego domniemania wynika z faktu, że wykazanie odpowiedzialności (a tym bardziej winy) administratora jest niejednokrotnie bardzo utrudnione. Administrator ma bowiem większą wiedzę o okolicznościach przetwarzania przez niego danych osobowych, zaś osoba poszkodowana może ich w ogóle nie znać i nawet nie mieć możliwości ich poznać[265].

W tym miejscu po raz kolejny należy zwrócić uwagę na kwestię błędnego tłumaczenia polskiej wersji językowej ogólnego rozporządzenia[266]. Motyw 146 RODO w polskiej wersji językowej stanowi, że administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności, jeżeli udowodnią, „że szkoda w żadnym razie nie powstała z ich winy". Natomiast w wersji angielskiej ten sam fragment stanowi *if it proves that it is not in any way responsible for the damage.* Fragment ten powinien być raczej tłumaczony w ten sposób, że administrator i podmiot przetwarzający powinni być zwolnieni z odpowiedzialności, „jeśli udowodnią, że w żadnym wypadku nie są odpowiedzialni za szkodę". Podobnie błędnie został przetłumaczony art. 82 ust. 3 RODO.

---

[264] A. Błaszczyńska [w:] *Realizacja praw osób, których dane dotyczą*, red. B. Fischer, M.Sakowska-Baryła, Wrocław 2017, s. 415.
[265] A. Błaszczyńska [w:] *Realizacja praw...*, s. 414.
[266] Por. D. Klimas, P. Wróbel, *Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia*, Legalis.

W świetle analizy innych wersji językowych RODO (angielskiej, niemieckiej, włoskiej) należy dojść do wniosku, że w polskim tłumaczeniu błędnie stwierdzono, że uwolnienie od odpowiedzialności cywilnoprawnej wymaga dowiedzenia braku winy w tym naruszeniu. Użycie słowa „wina" w polskim tłumaczeniu należy ocenić jako całkowicie dowolne i nieuzasadnione. Wniosek taki wynika także z wykładni celowościowej ogólnego rozporządzenia. Z motywów 3, 10 i 11 RODO wynika jasno, że celem ogólnego rozporządzenia jest zharmonizowanie, ujednolicenie i zapewnienie jednakowo wysokiego stopnia ochrony danych osobowych we wszystkich państwach członkowskich. Edyta Bielak-Jomaa wskazuje wręcz, że nowe podejście RODO statuuje oparcie przetwarzania danych osobowych na ryzyku. Co więcej, nawet dyrektywa 95/46/WE zobowiązywała państwa członkowskie do przyjęcia lub dostosowania mechanizmów kompensacji szkód powstałych w wyniku naruszenia przepisów o ochronie danych osobowych, wskazując jednocześnie, że należy przewidzieć możliwość zwolnienia administratora od odpowiedzialności, jeśli wykaże, że jego działanie nie było bezprawne[267].

Przedstawione poglądy doktryny wskazują na rozumienie przesłanek odpowiedzialności zgodnie z literalnym brzemieniem przepisu, bez przesądzenia ostatecznego modelu odpowiedzialności wobec wadliwego jego tłumaczenia. Tym samym tracą z pola widzenia złożoność tego zagadnienia. Znaczenie zasady ryzyka lub zasady winy, co do której przedstawiciele doktryny wyrażają wątpliwości interpretacyjne jeżeli chodzi o stosowanie RODO na gruncie Kodeksu cywilnego nie jest równe. Wina jest ogólna podstawą odpowiedzialności w tym sensie, że jeżeli przepis szczególny nie stanowi inaczej, to odpowiedzialność z tytułu czynów niedozwolonych można wywodzić wyłącznie z art. 415 k.c. Przepis ten stanowi generalną klauzulę odpowiedzialności *ex delicto*. Usprawiedliwianie takiego rozwiązania nie nastręcza żadnych trudności z punktu widzenia moralnego i społecznego. Odpowiedzialność na zasadzie winy bowiem rozumie się sama przez się, naganność postępowania tłumaczy wszystko. Nie wymaga zatem bliższego uzasadnienia uczynienie z niej generalnej podstawy odpowiedzialności *ex delicto*. Miejsce zasady ryzyka w systemie prawa polskiego jest zupełnie inne. Jak wspomniano wyżej ma ona charakter samodzielny. Wprawdzie zasada ryzyka znajduje zastosowanie tylko w wypadkach ściśle przewidzianych w ustawie, jednakże stanowi tylko dla nich wyłączną podstawę odpowiedzialności[268]. Nie można w toku tych rozważań pomijać zagadnienia obiektywizacji winy oraz użytecznej na gruncie RODO instytucji winy anonimowej.

[267] F. Morawski, *Odpowiedzialność cywilna administratora*...
[268] B. Lewaszkiewicz-Petrykowska, *Wyrządzenie szkody przez kilka osób*, Warszawa 1978, s. 49.

Odesłanie do przepisów krajowych – skutki prawne i znaczenie

Powyższe rozważania skłaniają do analizy zagadnienia odpowiedzialności w dalszej części pracy, zwłaszcza że w omawianych powyżej przepisach zawiera się szereg kwestii, które muszą być uzupełnione w drodze wyinterpretowania z przepisów prawa krajowego. Należy zauważyć, że o ile prawodawca uwzględnił kwestię odpowiedzialności cywilnej administratora i podmiotu przetwarzającego wobec osób, których dane dotyczą, to nie objął swoją regulacją np. wszystkich relacji kontraktowych pomiędzy administratorem a podmiotem przetwarzającym lub innymi podmiotami (np. subprocesorami, IOD).

RODO nie różnicuje zasad odpowiedzialności administratora za szkody spowodowane własnym działaniem od zasad odpowiedzialności w przypadku zlecenia przetwarzania danych osobowych podmiotowi trzeciemu w sytuacji działania lub zaniechania przetwarzania naruszającego rozporządzenie. Wskazanie jako przesłanki zwolnienia z odpowiedzialności wykazania braku winy nie odzwierciedla w pełni problemów dotyczących zasad odpowiedzialności administratora. Inaczej na gruncie rozwiązań krajowych kształtuje się jego sytuacja prawna w przypadku powstania szkody w następstwie działania będącego jego udziałem, a inaczej w przypadku, gdy jako profesjonalista wybiera inny profesjonalny podmiot do świadczenia usług w jego imieniu i na jego rzecz. Rozwiązaniem w takich przypadkach będzie zapewne stosowanie reguły z art. 92 ustawy o ochronie danych osobowych, która stanowi, że w zakresie nieuregulowanym rozporządzeniem 2016/679, do roszczeń z tytułu naruszenia przepisów o ochronie danych osobowych, o których mowa w art. 79 i art. 82 tego rozporządzenia, stosuje się przepisy ustawy z dnia 23.04.1964 r. - Kodeks cywilny. Problem współstosowania RODO i Kodeksu cywilnego pojawił się w głosach doktryny, które zwracają uwagę, że „RODO nie zawiera wyczerpującej regulacji, np. co do przedawnienia roszczeń i proponuje się też stosowanie np. art. 422 k.c., 429 k.c."[269]

W tym miejscu wspomnieć warto, że odsyłanie do stosowania innych przepisów – ulokowanych w innym miejscu danego aktu prawnego lub w innym akcie prawnym –polegające na nakazaniu „zachowania" określonych przepisów, różni się od, także często stosowanej w legislacji, metody opartej na formule, iż dopuszczalne jest stosowanie innych przepisów (odpowiednio lub wprost) „w zakresie nieuregulowanym" we wskazanych przepisach albo jeżeli wskazane przepisy „nie stanowią inaczej". W tym wypadku stosowanie tych innych przepisów jest dozwolone tylko wówczas, gdy hipoteza (dyspozycja) żadnego z nich nie

[269] M. Gumularz, *Wpływ regulacji....*, s. 35.

pokrywa się –choćby w części –z hipotezą (dyspozycją) przepisów, do których się odsyła; jeżeli tak jest, przepisy te „stanowią inaczej", co uniemożliwia sięgnięcie do odesłania[270].

Ustawodawca, odsyłając do innej grupy przepisów, pragnie regulować określoną grupę stosunków prawnych tak samo, jak to następuje w przepisach, do których decyduje się odsyłać. Musi zatem godzić się z tym, że normy w odesłaniu podlegają zmianom. W piśmiennictwie dotyczącym problematyki przepisów odsyłających wskazuje się, że odesłanie może mieć charakter statyczny lub dynamiczny[271]. W ujęciu dynamicznym odesłanie uwzględnia wszelkie zmiany, jakich dokonano w przepisie odesłanym, ujęcie statyczne obejmuje jedynie jego pierwotne znaczenie. Rozważania te, podnoszone na kanwie zasad techniki prawodawczej (§ 156 i n. załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20.06.2002 r. w sprawie zasad techniki prawodawczej), powołują się na domniemanie dynamicznego charakteru odesłania. Zgodnie z § 159 rozporządzenia z 20.06.2002 r. odesłanie ma charakter dynamiczny, ponieważ odesłanie statyczne (§ 160) wymaga doprecyzowania przez wskazanie, że określone regulacje stosuje się w brzmieniu z określonej daty, ustalonym określonym aktem normatywnym.

Zawarta w art. 92 ustawy o ochronie danych osobowych formuła stosowania przepisów Kodeksu cywilnego skłania w pierwszej kolejności do refleksji, które z przepisów Kodeksu cywilnego znajdują zastosowanie do przypadków naruszenia przepisów o ochronie danych wprost, a które odpowiednio. Tadeusz Żyznowski w glosie do uchwały Sądu Najwyższego[272] stwierdził, że „odpowiednie" stosowanie przepisów prawa jest czynnością jednolitą o charakterze jednolitym. W literaturze wyodrębnia się trzy grupy sytuacji – w zależności od uzyskiwanego rezultatu – odpowiedniego stosowania przepisów prawa. Do pierwszej grupy należą te, w których odpowiednie stosowanie polega na stosowaniu odpowiednich przepisów bez żadnych modyfikacji. Do drugich zaliczono te, w których odpowiednie przepisy mają być stosowane z pewnymi modyfikacjami. Wreszcie trzecia grupa obejmuje te przepisy, które ze względu na ich bezprzedmiotowość lub sprzeczność z przepisami ustanowionymi dla tych stosunków, do których miały być stosowane odpowiednio, nie mogą być w ogóle stosowane.

Biorąc pod uwagę wątpliwości doktryny dotyczące zasad odpowiedzialności deliktowej i odpowiedniego stosowania art. 415 k.c., art. 422 k.c., czy art. 429 k.c., w niniejszej pracy postawiona zostanie teza, że odpowiedzialność za naruszenie przepisów o ochronie

[270] Uchwała SN z 4.09.2009 r., III CZP 62/09.
[271] S. Wronkowska, M. Zieliński, *Zasady techniki prawodawczej. Komentarz*, Warszawa 1997, s. 177 oraz M. Hauser, *Przepisy odsyłające. Zagadnienia ogólne*, Przegląd Legislacyjny 2003/4, s. 81–82.
[272] T. Żyznowski, Glosa do uchwały Sądu Najwyższego z 29.10.1991 r. (III CZP 109/ 91), „Przegląd Sądowy" 1992/5/6.

danych osobowych może mieć charakter zarówno odpowiedzialności kontraktowej, wynikającej z umowy, jak i wynikającej z innych zdarzeń, z którymi RODO lub ustawa łączą odpowiedzialność, co stanowi o deliktowym charakterze możliwej odpowiedzialności. Powyższa teza implikuje dokonanie analizy instytucji odpowiedzialności odszkodowawczej oraz analizy naruszenia obowiązków podmiotów, biorących udział w procesach przetwarzania danych, jako źródła zdarzenia szkodzącego (zdarzenia, z którym ustawa wiąże odpowiedzialność za szkodę wyrządzoną innej osobie).

W tym miejscu warto podkreślić, że mimo faktu posiadania przez reżim odpowiedzialności kontaktowej i deliktowej wspólnych cech wykazują one daleko idące różnice w zakresie domniemań, zasad odpowiedzialności, przyczyny, dla której doszło do szkody oraz rodzajów roszczeń, z którymi może wystąpić poszkodowany. To komplikuje ocenę odpowiedzialności przedsiębiorcy na gruncie RODO i utrudnia zadanie dotyczące utworzenia zbioru przypadków, co do których można zastosować dany rodzaj odpowiedzialności. W kodeksie cywilnym występuje jedność podstawowych założeń i zasad odpowiedzialności. Obowiązują wspólne przepisy dla świadczeń odszkodowawczych. Ostrość przeciwstawienia obu reżimów odpowiedzialności ulega dalszemu złagodzeniu, gdy weźmie się pod uwagę, że oba systemy nie wyłączają się wzajemnie. Przeciwnie wyrządzenie szkody przez naruszenie zobowiązania może jednocześnie stanowić czyn niedozwolony i pociągać za sobą odpowiedzialność deliktową[273]. To prowadzić będzie do zastosowania instytucji zbiegu podstaw odpowiedzialności z art. 443 k.c. Odpowiedzialność deliktowa jest szersza, ponieważ reżim kontraktowy nie może zostać rozciągnięty na szkody niemajątkowe. Argument dotyczący istotnego ograniczenia w tym zakresie i tym samym uznania reżimu *ex delicto* za korzystniejszy dla poszkodowanego nabiera jednak innego znaczenia np. w świetle regulacji art. 474 k.c.

Innym przykładem ważnym dla powyższych rozważań jest ocena możliwości zastosowania art. 435 k.c. Przyjmując głoszone w piśmiennictwie tezy, że współcześnie trudno znaleźć zakład pracy, w którym nie są wykorzystywane energia elektryczna, paliwa płynne lub energia cieplna, mające źródło w siłach przyrody, uznać należy, że nie oznacza to, że nie ma wątpliwości, czy intencją ustawodawcy nie było związanie zaostrzonej odpowiedzialności z jakimkolwiek przejawem wykorzystania w działalności przedsiębiorstwa sił przyrody.
W obecnym brzmieniu przepis art. 435 § 1 k.c. jest wysoce nieprecyzyjny i na jego podstawie niezwykle trudno sformułować przejrzyste kryteria, na podstawie których można by w konkretnej sytuacji w prosty sposób dokonać przyporządkowania danego przedsiębiorstwa lub

[273] T. Pajor, *Odpowiedzialność dłużnika za niewykonanie zobowiązania*, Warszawa 1982, s. 33.

zakładu do kategorii wprawianych bądź nie wprawianych w ruch za pomocą sił przyrody. W zasadzie każde przedsiębiorstwo w swojej działalności wykorzystuje przetworzone siły przyrody, choćby energię elektryczną. Nie budzi i nigdy nie budziło wątpliwości, że sama taka okoliczność jest dalece niewystarczająca dla kategoryzacji prowadzących takie przedsiębiorstwa, jako podlegających pod reżim art. 435 § 1 k.c.[274]

Dokonując w tym miejscu uproszczenia na potrzeby pracy, przyjąć należy założenie, że elektroniczne nośniki danych osobowych korzystając z energii elektrycznej, czynią z przedsiębiorcy ich używającego podmiot, któremu można przypisać odpowiedzialność także na takiej podstawie. W doktrynie przeważa pogląd, że przez określenie „ruch przedsiębiorstwa" należy rozumieć kompleks faktów prowadzących do ujawnienia stwarzanego przez przedsiębiorstwo niebezpieczeństwa. Ponadto do wyrządzenia szkody przez ruch przedsiębiorstwa dochodzi zarówno wtedy, gdy szkoda jest bezpośrednim skutkiem użycia sił przyrody i pozostaje w adekwatnym związku przyczynowym z niebezpieczeństwem wynikającym z zastosowania tych sił jak i wtedy, gdy pozostaje w związku tylko z samym ruchem przedsiębiorstwa lub zakładu jako całości. Dlatego też nie jest konieczne, by szkodę spowodowało konkretne urządzenie wprawiane w ruch siłami przyrody. Wystarczy, by istniał adekwatny związek przyczynowy między funkcjonowaniem przedsiębiorstwa jako całości a powstałą szkodą[275].

Jak słusznie zauważył J. Łopuski, stosowanie urządzeń wprawianych w ruch za pomocą sił przyrody uległo upowszechnieniu, rozwój cywilizacji przynosi coraz to nowe postacie zagrożeń, natężenie niebezpieczeństwa ulega zróżnicowaniu, wobec czego należy rozważyć, czy niebezpieczeństwo stwarzane przez działalność wprawianą w ruch za pomocą sił przyrody ma nadal charakter szczególny, uzasadniający w każdym przypadku wprowadzenie odpowiedzialności na zasadzie ryzyka[276]. To zagadnienie będzie analizowane w części pracy dotyczącej odpowiedzialności za przetwarzanie danych z użyciem SI.

Na potrzeby niniejszej pracy postawiona zostanie także teza, że zbyt daleko idącym uproszczeniem jest wywodzenie zasad odpowiedzialności z tłumaczenia RODO bez badania charakteru i rodzaju świadczenia, z którym związane jest powstanie szkody. Ustalenie zakresu stosowania i reżimu odpowiedzialności wymagać będzie udzielenia także odpowiedzi m.in. na

[274] M. Zelek, *O kryteriach kwalifikacji przedsiębiorstwa lub zakładu jako wprawianego w ruch za pomocą sił przyrody (art. 435 § 1 k.c.)*, PS 2019/3, s. 70-83.
[275] M.P. Ziemiak, M. Karolak, *Odpowiedzialność za szkody wyrządzone przez przedsiębiorstwo wprawiane w ruch za pomocą sił przyrody (art. 435 k.c.). Rozważania de lege lata i de lege ferenda na kanwie orzecznictwa sądowego i poglądów Profesora Jana Łopuskiego*, „Prawo i Więź" 2020/3, s. 70.
[276] M.P. Ziemiak, M. Karolak, *Odpowiedzialność za szkody...*, s. 65.

następujące zagadnienia: czy reżim odpowiedzialności kontraktowej stosuje się we wszystkich przypadkach do wszystkich zobowiązań, czy tylko do pewnej grupy oraz czy stosuje do stosuje się on do wszystkich rodzajów naruszeń zobowiązania. W zakresie odpowiedzialności delikotwej niezbędna będzie analiza źródła obowiązku odszkodowawczego.

ROZDZIAŁ III.

Zagadnienia ogólne dotyczące odpowiedzialności odszkodowawczej przedsiębiorcy za naruszenie danych osobowych

Pojęcie odpowiedzialności odszkodowawczej i prawnej

Analiza odpowiedzialności przedsiębiorców biorących udział w przetwarzaniu danych osobowych wymaga omówienia zagadnień ogólnych dotyczących odpowiedzialności odszkodowawczej, zgodnie z powszechnie dokonywaną klasyfikacją odpowiedzialności według kryterium źródła powstania zobowiązania (*ex contractu, ex delicto*), co stanowić będzie punkt wyjścia do dalszych rozważań na temat podstaw odpowiedzialności przedsiębiorcy, występującego na gruncie RODO w roli administratora lub podmiotu przetwarzającego. W rozdziale tym omówione zostaną zasady odpowiedzialności oraz charakter świadczeń. Będzie miało to znaczenie dla dalszych wywodów, które dotyczyć będą istoty obowiązków wynikających z RODO i wynikających z nich skutków prawnych oraz zagadnień dotyczących okoliczności, na które może powoływać się administrator lub podmiot przetwarzający w celu uniknięcia odpowiedzialności. W odrębnym rozdziale omówione zostaną też założenia odpowiedzialności za przetwarzanie danych osobowych z wykorzystaniem systemów SI.

Rozważania na temat odpowiedzialności rozpocząć należy od zaprezentowania poglądu, według którego przez odpowiedzialność rozumieć należy dopuszczalność zastosowania przymusu w celu wyegzekwowania należnego świadczenia, czyli w celu realizacji wierzytelności jako wiązki uprawnień. Świadczenie, czyli – mówiąc potocznie – „tego, do czego zobowiązany jest dłużnik" jest podstawowym dla istoty zobowiązania pojęciem. W nauce mówi się, że świadczenie jest wyznaczone treścią zobowiązania do określonego zachowania się dłużnika względem wierzyciela. Sytuację prawną dłużnika określa, od strony spoczywających na nim obowiązków, pojęcie długu, który stanowi zespół obowiązków dłużnika względem wierzyciela. Rozróżnienie długu i odpowiedzialności jest dziełem niemieckiej nauki prawa. O ile dług wiąże się z obowiązkiem określonego zachowania się – spełnienia świadczenia – i jest niejako korelatem wierzytelności przysługującej uprawnionemu (wierzycielowi), o tyle odpowiedzialność polega na możliwości wyegzekwowania tego świadczenia przy zaangażowaniu przymusu zaoferowanego uprawnionemu przez państwo. Istnienie odpowiedzialności zapewnia „pokrycie" dla długu. Jak

wskazują niektórzy autorzy niemieccy – „odpowiedzialność przydaje długowi ziemskiej ciężkości”[277].

Na gruncie prawa prywatnego odpowiedzialność jest ważnym uzupełnieniem każdej konstrukcji prawnej. Odpowiedzialność odszkodowawcza jest uznawana za filar prawa cywilnego[278].

Pojęcie odpowiedzialności w prawie ma charakter interdyscyplinarny. Wyróżnia się przede wszystkim odpowiedzialność cywilną, karną, administracyjną, dyscyplinarną. Poza prawem cywilnym i karnym odpowiedzialność występuje w różnych innych gałęziach prawa, w szczególności w prawie konstytucyjnym, administracyjnym, finansowym oraz w prawie pracy. Próby konstruowania ogólnego pojęcia odpowiedzialności podejmowane były przede wszystkim przez przedstawicieli teorii prawa[279]. Celem odpowiedzialności jest wskazanie osoby odpowiedzialnej za powstałą szkodę oraz ustalenie wysokości i zakresu należnego od niej odszkodowania. Te dwa elementy: wskazanie odpowiedzialnego za szkodę oraz zobowiązanie go do jej wyrównania są charakterystyczne zarówno dla odpowiedzialności deliktowej, jak i kontraktowej[280]. Różne rodzaje odpowiedzialności łączy jedna cecha wspólna – świadczenia zmierzające do naprawienia szkody, czyli najogólniej ujmując, zaspokojenia uszczerbku powstałego w dobrach jednej osoby (określanej mianem poszkodowanego) przez inny podmiot[281]. Istnienie odpowiedzialności wzmacnia, a czasem wręcz umożliwia realizację podstawowych funkcji prawa. Kwestia w jaki sposób dłużnik odpowiada za spełnienie świadczenia ma decydujące znaczenia dla wartości ekonomicznej zobowiązania. Ukształtowanie odpowiedzialności za dług ma doniosłą wagę praktyczną.[282] Bez odpowiedzialności często trudno byłoby osiągnąć rzeczywisty, obiektywny skutek, rezultat istnienia jakiejś instytucji czy normy prawnej[283]. Doktryna wyróżnia trzy podstawowe funkcje

[277] *Prawo cywilne – część ogólna. System Prawa Prywatnego*, red. M. Safjan, t. 1, Warszawa 2012, s. 964.
[278] A. Stelmachowski, *Wstęp o teorii prawa cywilnego*, Warszawa 1969, s. 243. Szerzej na temat odpowiedzialności odszkodowawczej: A. Doliwa, *Zobowiązania*, Warszawa 2006, s. 106–109 oraz W. Warkałło, *Odpowiedzialność odszkodowawcza. Funkcje, rodzaje, granice*, Warszawa 1972.
[279] B. Kucharski, *Świadczenie ubezpieczyciela w umowie ubezpieczenia mienia*, Warszawa 2019, s. 29.
[280] Sz. Byczko, *Świadczenie pieniężne ubezpieczyciela na tle pojęcia odpowiedzialności cywilnoprawnej, Prawo prywatne wobec wyzwań współczesności. Księga pamiątkowa dedykowana Profesorowi Leszkowi Ogiegle*, red. Mariusz Fras, Piotr Ślęzak, Łodź 2017.
[281] M. Kaliński, *Szkoda na mieniu i jej naprawienie*, Warszawa 2011, s. 1.
[282] W. Czachórski, *Zobowiązania, Zarys wykładu*, Warszawa 1999, s. 63.
[283] M. Czech, *Umowa powierzenia przetwarzania danych osobowych*, Białystok 2020, s. 293; https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/8735/1/M_Czech_Umowa_powierzenia_przetwarzania_danych_osobowych.pdf

odpowiedzialności odszkodowawczej, tj. kompensacyjną, represyjną i prewencyjno-wychowawczą[284].

Analizując treść pojęcie odpowiedzialności odszkodowawczej należy ustosunkować się do terminu „odpowiedzialność prawna", przez którą rozumie się „ujemne następstwa prawne, przewidziane dla jakiegoś podmiotu w związku ze ziszczeniem się pewnych zdarzeń kwalifikowanych negatywnie przez system prawny[285]. W piśmiennictwie wyrażono pogląd, że odpowiedzialność jest to zasada ponoszenia przez podmiot przewidzianych prawem ujemnych konsekwencji za zdarzenia lub stany rzeczy podlegające ujemnej kwalifikacji normatywnej i przypisywane prawnie określonemu podmiotowi w danym porządku prawnym[286]. Zdaniem T. Dybowskiego konstrukcjom cywilnoprawnym najbardziej odpowiada ta definicja. Pogląd ten łączący pojęcie odpowiedzialności z ujemnymi konsekwencjami pewnego zachowania zaaprobował Sz. Byczko[287].

W ramach odpowiedzialności prawnej mieści się odpowiedzialność cywilna, na wieloznaczność której zwraca uwagę – za R. Longchamps de Berierem – A. Stelmachowski, przyjmując ostatecznie, iż oznacza ona sytuację, w której mamy do czynienia ze „zobowiązaniem określonego podmiotu, zagrożonym sankcją cywilną". Zobowiązaniu temu odpowiada po stronie uprawnionego możliwość domagania się jego przymusowego zaspokojenia za pomocą organów państwowych lub przez samopomoc w przypadkach przewidzianych przepisami szczególnymi. Konstrukcja ta jest koherentna ze strukturą zobowiązania, według której – co do zasady – w zobowiązaniu po stronie dłużnika mamy do czynienia z długiem oraz odpowiedzialnością. Nie ma wystarczających podstaw, aby wyłączać z zakresu pojęcia odpowiedzialności cywilnej przymusowe wykonanie zobowiązania (pogląd taki eksponuje znaczenie sankcji), a nawet – jak się wydaje – wykonanie dobrowolne, gdy zobowiązaniu towarzyszy możliwość uruchomienia takiej sankcji. Dłużnik, świadcząc zgodnie z treścią zobowiązania, także realizuje swoją odpowiedzialność; wyjątek stanowią sytuacje, gdy w strukturze zobowiązania nie występuje możliwość uruchomienia przymusu w celu jego realizacji, a mimo to dochodzi do jego dobrowolnego wykonania (jest tak w przypadku

[284] B. Więzowska, *Odpowiedzialność cywilna na zasadzie słuszności*, Warszawa 2009, LEX. Szerzej na temat funkcji odpowiedzialności cywilnej: W. Czachórski, *Zasady i funkcje odpowiedzialności cywilnej według kodeksu cywilnego – ich ewolucja* [w:] *Studia z prawa zobowiązań*, red. Z. Radwański, Warszawa–Poznań 1979.
[285] Przywołuję tu definicję zaproponowaną w pierwszym wydaniu podręcznika prawa cywilnego napisanym tuż po transformacji ustrojowej – zob. Z. Radwański, *Zobowiązania – część ogólna*, Warszawa 1995, s. 39.
[286] T. Dybowski [w:] *System Prawa Prywatnego*, t. 3, *Prawo rzeczowe*, Warszawa 2007, s. 166; K. Zagrobelny, O *okolicznościach kształtujących odpowiedzialność odszkodowawczą dłużnika* [w:] *Odpowiedzialność w prawie cywilnym*, red. P. Machnikowski, „Prawo" 2006/300, s. 273; W. Lang, *Struktura odpowiedzialności prawnej*, „Prawo" 1968/8, s. 12.
[287] Sz. Byczko, *Świadczenie pieniężne...*, także B. Kucharski, *Świadczenie ubezpieczyciela...*, s. 29.

zobowiązań naturalnych). Dlatego zamieszczanie w definicji pojęcia odpowiedzialności prawnej kwalifikatorów wskazujących na negatywną ocenę jakichś zdarzeń lub stanów rzeczy nie wydaje się prawidłowe[288].

Wieloznaczność odpowiedzialność cywilnej mieszczącej się w ramach odpowiedzialności prawnej była dostrzegana przez R. Longchamps de Beriera, który wskazywał, że termin odpowiedzialność służyć może jako określenie:

1. Rozmiaru świadczenia (np. odpowiedzialność ograniczona rachunkowo).
2. Subiektywnego warunku powstania zobowiązania (np. odpowiedzialność za winę).
3. Obowiązków w ramach zobowiązania (np. odpowiedzialność z tytułu rękojmi).
4. Właściwości, że majątek dłużnika jest gwarancją spełnienia przezeń świadczeń[289].

Odpowiedzialność odszkodowawcza występuje wszędzie tam, gdzie dłużnik w ramach sankcji przewidzianej przez prawo zobowiązany jest do świadczenia polegającego na naprawieniu uszczerbku, jakiego doznała inna osoba na skutek tego, że prawnie chronione dobra i interesy tej drugiej osoby zostały naruszone[290].

W doktrynie dominuje stanowisko, zgodnie z którym odpowiedzialność odszkodowawcza jest zawsze odpowiedzialnością cywilną. Innymi słowy termin odpowiedzialność odszkodowawcza jest węższy niż odpowiedzialność cywilna. Jak stwierdził A. Szpunar, ogólne zasady rządzące określeniem odszkodowania za szkodę majątkową są te same bez względu na to, jakie było źródło powstania tego obowiązku[291].

Zdaniem M. Kalińskiego przypadki odpowiedzialności odszkodowawczej stanowią niewątpliwie najistotniejszy element odpowiedzialności cywilnej. Nie przesądza to jednak, czy odpowiedzialność cywilna obejmuje wszystkie sytuacje, w których mamy do czynienia ze świadczeniem odszkodowawczym, czyli zakresy omawianych pojęć się krzyżują. Pogląd o krzyżowaniu się pojęć oparto na założeniu, że zawarcie regulacji odszkodowawczych w unormowaniach zaliczanych np. do prawa administracyjnego, wymusza przyjęcie jakoby odpowiedzialność odszkodowawcza była pojęciem wykraczającym poza normy odpowiedzialności cywilnej[292].

Powyższe rozważania mają znaczenie dla zagadnień objętych pracą z uwagi na fakt, że zakres praw i obowiązków uczestników systemu ochrony danych osobowych należy do

[288] M. Kaliński, *Odpowiedzialność odszkodowawcza* [w:] *Szkoda na mieniu i jej naprawienie*, red. Olejniczak, M. Kaliński, Warszawa 2011, s. 3–4.
[289] B. Kucharski, *Świadczenie ubezpieczyciela...*, s. 30.
[290] A. Stelmachowski, *Wstęp do teorii prawa cywilnego*, Warszawa 1984, s. 314.
[291] A. Szpunar, Odszkodowanie za szkodę majątkową. Szkoda na mieniu i osobie, Bydgoszcz 1998 s. 13.
[292] M. Kaliński, *Szkoda na mieniu..*, Warszawa 2011 s. 7.

regulacji łączących elementy administracyjnoprawne i cywilnoprawne. Szczegółowa analiza charakteru obowiązków wynikających z prawa ochrony danych osobowych w tym zakresie nie jest w niniejszej pracy możliwa, ale na takie rozumienie obowiązków wskazują m.in. poglądy A. Sobczyka, który ocenia charakter tych obowiązków w relacjach podmiotów prywatnych w taki sposób, że twierdzi, iż administrator bez względu na formę prawną i panujące w nim stosunki właścicielskie wykonuje akty władzy publicznej[293].

W ślad za A. Piskorz-Ryn powtórzyć należy, że na problem istnienia regulacji łączących elementy administracyjnoprawne i cywilnoprawne zwracano uwagę w piśmiennictwie od dawna, właściwie od zarania prawa administracyjnego. Jerzy Stefan Langrod podkreślał, że administracja żyje niejako „podwójnym życiem" prawnym, będąc poddana zarówno prawu administracyjnemu, jak i prawu cywilnemu. Z tego względu odróżniamy trzy sfery prawne, jedną – wyłącznego zastosowania prawa administracyjnego, drugą – wyłącznego zastosowania prawa cywilnego, oraz trzecią – sferę graniczną, gdzie krzyżują się oba reżimy, obejmującą punkty styku ich ingerencji. Dla trzeciej sfery prawnej Franciszek Longchamps używał określenia „prawo pogranicza". Tadeusz Kuta posługiwał się zaś pojęciem „instrumentu mieszanego". O „instytucjach mieszanych" pisał też Jerzy Starościak. Twierdził on, że „Normy prawa administracyjnego wkraczają w dziedzinę regulowaną przed ich wydaniem wyłącznie przez prawo cywilne, przekształcając instytucje tego prawa: z jednej strony «uadministracyjniając» te instytucje, a z drugiej same się «cywilizują»". Autor ten pisał również, „o polach środkowych znajdujących się równocześnie pod równoważnym wpływem regulacji administracyjnej i cywilnej". Dowodził ponadto, że pozostają konstrukcje prawne będące jednoczesnym i równoważnym tworem obu tych działów prawa [294].

Obecnie mamy do czynienia z coraz szerszym wpływem przepisów administracyjnych na odpowiedzialność cywilną, czego oprócz RODO doskonałym przykładem jest choćby dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15.05.2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE – MIFID II[295]. W przypadku tego aktu nie powinno ulegać wątpliwości, że celem publicznoprawnych unormowań ustanawiających obowiązki informacyjne i ostrzegawcze wobec klienta jest ochrona jego interesów. Funkcją tych obowiązków jest wyposażenie klienta w wiedzę ułatwiającą mu podjęcie racjonalnej decyzji inwestycyjnej na podstawie rzetelnych informacji na temat usługi maklerskiej lub instrumentu finansowego. Naruszenie tych

[293] A. Sobczyk, *RODO. Rozproszona władza publiczna*, Kraków 2020, s. 118.
[294] A. Piskorz-Ryń, *Ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2018, s. 22
[295] Dz. Urz. UE L 173 z 12.06.2014, s. 349.

unormowań może być podstawą odpowiedzialności odszkodowawczej firmy inwestycyjnej na podstawie art. 415 k.c., jeśli spełnione zostaną pozostałe przesłanki tej odpowiedzialności[296]. Wydaje się zatem, że pojęcie odpowiedzialności na gruncie RODO może wykraczać poza ramy cywilnoprawne i także na podstawie tego aktu można dokonywać analizy cywilnoprawnej skutków naruszenia publicznoprawnych unormowań dotyczących np. obowiązków informacyjnych rozważając przede wszystkim ewentualną odpowiedzialność deliktową na podstawie art. 415 k.c.

W tym miejscu zasadne jest zatem przywołanie przekonywującej dla założeń pracy tezy M. Kalińskiego, że normy prawne dotyczące obowiązku naprawienia szkody rozsiane są po aktach prawnych zaliczanych do różnych dziedzin prawa, jednakże ustalenie treści stosunku odszkodowawczego powinno następować zawsze z uwzględnieniem zawartych w art. 361–363 k.c. ogólnych norm dotyczących zapłaty odszkodowania. Z tych względów stosunek odszkodowawczy ma charakter cywilnoprawny, a odpowiedzialność odszkodowawczą należy uznać za element odpowiedzialności cywilnej[297]. Teza ta ma znaczenie dla przedmiotu pracy z uwagi na analizowane zagadnienia obowiązków prawnych oraz stosunków prawnych łączących uczestników systemu ochrony danych osobowych.

W pierwszej kolejności analizy wymaga zatem pojęcie stosunku prawnego (a także stosunku cywilnoprawnego) w takim kontekście, iż omawiane pojęcie służy do określenia sytuacji prawnej podmiotu (w tym uczestników systemu ochrony danych osobowych), wyznaczonego treścią normy prawnej. Ze względu na obowiązywanie generalnej i abstrakcyjnej normy prawnej, stosunek prawny opisuje więc, jako wynikające z tej normy prawnej powinne zachowanie się podmiotu. Pojęcie to wyjaśnia zatem, czy i która z norm prawnych może znaleźć zastosowanie w danej sytuacji, i w odniesieniu do jakiego podmiotu[298]. Przenosząc powyższe na grunt pracy wskazać należy, że określenie stosunków prawnych uczestników systemu ochrony danych osobowych ma podstawowe znaczenie dla zagadnienia ich odpowiedzialności. Istotne jest tutaj podkreślenie, że stosunkiem prawnym jest każdy rodzaj zależności pomiędzy ludźmi lub ich organizacjami, jeśli jest on wyznaczony przez normę prawną, a różnorodność modeli tych stosunków związana jest z wyodrębnianiem poszczególnych dyscyplin prawniczych i gałęzi prawa[299]. Konstrukcja stosunku prawnego

[296] T. Sójka, *Cywilnoprawne ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym*, Warszawa 2016, s. 189.
[297] M. Kaliński, *Szkoda na mieniu...*, s. 9.
[298] *Prawo cywilne – część ogólna. System Prawa Prywatnego*, red. M. Safjan, t. 1, Warszawa 2012. s. 936; Z. Ziembiński, *Problemy podstawowe prawoznawstwa*, Warszawa 2022, s. 334–336.
[299] W. Lang, J. Wróblewski, S. Zawadzki, *Teoria państwa prawa*, Warszawa 1986, s. 382.

służy do normatywnej kwalifikacji zachowań określonych podmiotów i wynikających z nich powiązań o charakterze uprawnieniowo-zobowiązaniowym, których celem jest określenie uprawnień i obowiązków tych podmiotów oraz skutków prawnych wynikających z łączących ich relacji[300]. Stosunek prawny kształtują pewne jego elementy konstytutywne obejmujące podmioty stosunku prawnego, jego przedmiot i treść, a także fakty prawne[301]. Podmiotami stosunku prawnego są podmioty będące adresatami norm regulujących ten stosunek, które występują w nim jako uprawnione lub zobowiązane do określonego zachowania się względem innych osób – uczestników tego samego stosunku prawnego[302]. Przedmiotem stosunku prawnego jest określone zachowanie, przedmiot, materialny lub dobro niematerialne bądź prawa, których dotyczą obowiązki i uprawnienia między stronami[303].

W dalszej kolejności powiedzieć należy, że pojęcie stosunku prawnego – wyrażające podstawową zależność między podmiotami prawa – nie jest wyłącznie pojęciem teoretycznym. Stanowi ono jednocześnie termin przynależny zarówno językowi prawniczemu, jak i prawnemu. Treść stosunku prawnego stanowią uprawnienia i obowiązki jego podmiotów (stron)[304]. Fakty prawne natomiast to takie okoliczności (zdarzenia, stany rzeczy), z którymi przepisy prawa wiążą powstanie, zmianę lub wygaśnięcie stosunku prawnego, obejmujące szereg kategorii działań konwencjonalnych i niekonwencjonalnych, dozwolonych i niedozwolonych, zależnych i niezależnych od ludzkiej aktywności[305]. Według takiego schematu klasyfikować można zachowania uprawnionych i podmiotów zobowiązanych do zapewniania realizacji prawa do ochrony danych osobowych[306].

Źródła odpowiedzialności odszkodowawczej

Wiesław Lang przed sformułowaniem swojej definicji odpowiedzialności analizował odpowiedzialność na gruncie różnych gałęzi prawa. W prawie cywilnym wyróżnia trzy jej postaci, a mianowicie:

1. odpowiedzialność dłużnika za wykonanie zobowiązania;
2. odpowiedzialność kontraktową z tytułu niewykonania zobowiązania;
3. odpowiedzialność deliktową za szkodę wyrządzoną czynem niedozwolonym.

[300] A. Korybski, L. Leszczyński, A. Pieniążek, *Wstęp do prawoznawstwa*, Lublin 2007, s. 181.
[301] W. Lang, J. Wróblewski, S. Zawadzki, *Teoria państwa…*, s. 379.
[302] A. Korybski, L. Leszczyński, A. Pieniążek, *Wstęp do prawoznawstwa*, Lublin 2007, s. 181.
[303] T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa*, Warszawa 2021, s. 143.
[304] T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa…*, s. 146.
[305] W. Lang, J. Wróblewski, S. Zawadzki, *Teoria państwa…*, s. 381.
[306] M. Sakowska-Baryła, *Ochrona danych osobowych...*, s. 60.

Pierwszą z postaci odpowiedzialności W. Lang określa jako pierwotną, wynikającą bezpośrednio z treści czynności prawnej będącej źródłem zobowiązania i przeciwstawia odpowiedzialności kontraktowej za szkodę spowodowaną niewykonaniem lub nienależytym wykonaniem zobowiązania[307].

Odpowiedzialność cywilnoprawna uczestników systemu ochrony danych osobowych może mieć dwie podstawy – zarówno *ex contractu*, jak i *ex delicto*, stąd wynika potrzeba ich analizy.

Pochodzący jeszcze z prawa rzymskiego podział źródeł odpowiedzialności odszkodowawczej (*ex contractu – ex delicto*) uznano w toku rozwoju prawa za niewystarczający, co było przyczyną uzupełniania go o nowe kategorie. Wyrazem tej tendencji było wymienienie w art. 1 k.z., jako źródeł zobowiązań oświadczeń woli, czynów i innych zdarzeń. Chociaż Kodeks cywilny nie przejął tego unormowania, nie ulegało wątpliwości, iż nie wprowadził on w omawianym zakresie istotnych zmian, a zarazem unormowanie w art. 415 i n. oraz art. 471 i n. k.c. reguł odpowiedzialności odszkodowawczej deliktowej i kontraktowej nie może być uważane za regulację wyczerpującą. Wskazywano, iż poza tymi dwoma reżimami istnieje co najmniej trzecie źródło odpowiedzialności, określając je mianem wynikającego „bezpośrednio z ustawy"[308]. Podobnie jak czynność prawna oraz czyn niedozwolony w polskim prawie prywatnym źródłem zobowiązania jest bezpodstawne wzbogacenie. Precyzyjniej można powiedzieć, że źródłem zobowiązania, którego stronami są zubożony (dłużnik) oraz wzbogacony (wierzyciel), jest uzyskanie bez podstawy prawnej przez wzbogaconego korzyści majątkowej kosztem zubożonego. Trzeba zasygnalizować, że szczególnym przypadkiem bezpodstawnego wzbogacenia jest nienależne świadczenie, a dokładniej – uzyskanie świadczenia nienależnego[309].

Zdaniem T. Pajora odpowiedzialność odszkodowawcza dłużnika należy do węzłowych instytucji prawa obligacyjnego. Splatają się tu zagadnienia obrotu umownego i odpowiedzialności za wyrządzoną szkodę. Sprawia to, że wspomniana instytucja ma doniosłe znaczenie teoretyczne i praktyczne. Polskie prawo należy do systemów wyodrębniających szczególny reżim odpowiedzialności odszkodowawczej dłużnika. Tradycyjne rozróżnienie między odpowiedzialnością deliktową i kontaktową zostało utrzymane. W związku z tym mówi się o dwóch systemach lub reżimach odpowiedzialności, między którymi zachodzą dość istotne

[307] W. Lang, *O strukturze odpowiedzialności prawnej*, ZNUMK 1968/31, s. 10; B. Kucharski, *Świadczenia ubezpieczyciela*..., s. 32.
[308] W. Warkałło, *Odpowiedzialność*..., s. 107.
[309] *Prawo zobowiązań – część ogólna. System Prawa Prywatnego*, red. A. Olejniczak, t. 6, Warszawa 2009, s. 208.

różnice co do rozwiązań szczegółowych. W Kodeksie cywilnym występuje jedność podstawowych założeń i zasad odpowiedzialności. Obowiązują zatem wspólne przepisy dla świadczeń odszkodowawczych. Ostrość przeciwstawienia obu reżimów odpowiedzialności ulega dalszemu złagodzeniu, gdy weźmie się pod uwagę, że oba systemy nie wyłączają się wzajemnie. Przeciwnie, wyrządzenie szkody przez naruszenie zobowiązania może jednocześnie stanowić czyn niedozwolony i pociągać za sobą odpowiedzialność deliktową[310].

Odróżnienie odpowiedzialności kontraktowej od deliktowej odpowiedzialności za szkodę opiera się na tym, że odpowiedzialność kontraktowa obejmuje wypadki, w których podmiotem odpowiedzialnym za szkodę jest dłużnik, poszkodowanym zaś wierzyciel, a źródłem szkody fakt, że zobowiązanie, jakie ciążyło na dłużniku względem wierzyciela, zanim doszło do powstania szkody, nie zostało wykonane bądź zostało wprawdzie wykonane, lecz nienależycie (art. 471 k.c.). Odpowiedzialność deliktowa obejmuje natomiast wypadki, w których wyrządzenie szkody stanowi lub mogłoby stanowić samoistne źródło powstania obowiązku naprawienia szkody także między osobami, których do tej pory żaden stosunek zobowiązaniowy nie łączył (art. 415 i n. k.c.)[311].

Prawo polskie dopuszcza zbieg odpowiedzialności, ale to nie uzasadnia tezy, że każde lub niemal każde naruszenie zobowiązania jest deliktem i rodzi odpowiedzialność z art. 415 k.c. Zbieg odpowiedzialności może mieć miejsce wówczas, gdy czyn stanowiący nienależyte wykonanie zobowiązania narusza zarazem obowiązek powszechny. Trzeba jednak zaznaczyć, że zgodnie ze stanowiskiem Sądu Najwyższego ukształtowanym w latach 50. XX wieku[312] chodzi tylko o taki obowiązek którego naruszenie mogłoby nastąpić również poza istniejących stosunkiem obligacyjnym. Odpowiedzialność ta nie byłaby natomiast uzasadniona jeżeli miałaby opierać się jedynie na fakcie, że nienależyte spełnienie świadczenia narusza ogólną powinność prawidłowego wykonania zobowiązania. Powinność ta bowiem nie wprowadza niczego nowego ponad to co już wynika z treści wiążącego dłużnika stosunku, a przeciwnie dopiero w tej treści znajduje konkretyzację. Jeżeli więc nie następuje naruszenie dwu różnych w swej istocie obowiązków to i przyjęcie zbiegu odpowiedzialności nie byłoby uzasadnione. Odmienne stanowisko oznaczałoby akceptację całkiem szczególnego deliktu który sprowadzały się do naruszenia zobowiązania[313].

---

[310] T. Pajor, *Odpowiedzialność dłużnika*..., s. 33.
[311] J. Rezler, *O odpowiedzialności kontraktowej w jej stosunku do odpowiedzialności deliktowej – inaczej*, „Palestra" 31/10–11(358–359), s. 86–103.
[312] Za T. Pajorem: orzeczenie 7 sędziów SN z 30 X/13 XI 1954 (OSN 1955, poz. 51) a zwłaszcza uchwała Izby Cywilnej SN z 26.10.1956 r., OSN 1957, poz. 1 [w:] *Odpowiedzialność dłużnika...*
[313] T. Pajor, *Odpowiedzialność dłużnika...*, s. 56–57.

Zagadnienie zbiegu odpowiedzialności stanowi wciąż przedmiot rozbieżności interpretacyjnych. Zgodnie np. z orzeczeniem Sądu Najwyższego w sprawie I CSK 687/12 niewykonanie zobowiązania samo przez się nie może być uznane za działanie bezprawne w rozumieniu art. 415 k.c. Taka jego kwalifikacja jest uzasadniona tylko wtedy, gdy jednocześnie następuje naruszenie obowiązku powszechnego, ciążącego na każdym podmiocie. W takim wypadku Kodeks cywilny dopuszcza zbieg roszczenia z tytułu niewykonania lub nienależytego wykonania zobowiązania i roszczenia z tytułu czynu niedozwolonego, pozostawiając poszkodowanemu wybór jednego z tych roszczeń (art. 443 k.c.)[314]. Zgodnie zaś z wyrokiem SN z 7.10.2020 r.[315] okoliczność, że pozwany nie wykonał zobowiązania wynikającego z umowy, w świetle art. 443 k.c., nie wyłącza roszczenia o naprawienie szkody z tytułu czynu niedozwolonego. Zbieg odpowiedzialności kontraktowej z deliktową zachodzi wtedy, gdy dłużnik nie tylko nie wykonuje lub nienależycie wykonuje swoje zobowiązanie umowne, lecz jednocześnie narusza nakaz lub zakaz zobowiązujący go niezależnie od istniejącego między stronami stosunku prawnego i jego postępowanie ma wówczas charakter deliktu cywilnego. Zgodnie zaś z orzeczeniem Sądu Najwyższego w sprawie I CSK 687/12 niewykonanie zobowiązania samo przez się nie może być uznane za działanie bezprawne w rozumieniu art. 415 k.c. Taka jego kwalifikacja jest uzasadniona tylko wtedy, gdy jednocześnie następuje naruszenie obowiązku powszechnego, ciążącego na każdym podmiocie. W takim wypadku Kodeks cywilny dopuszcza zbieg roszczenia z tytułu niewykonania lub nienależytego wykonania zobowiązania i roszczenia z tytułu czynu niedozwolonego, pozostawiając poszkodowanemu wybór jednego z tych roszczeń (art. 443 k.c.)[316].

Z perspektywy RODO zagadnienie zbiegu odpowiedzialności będzie przedmiotem analizy złożonych stosunków prawnych, w których uczestniczy kilka podmiotów. Polska doktryna stoi na stanowisku, że odpowiedzialność za szkodę z art. 82 RODO zbliżona jest do konstrukcji odpowiedzialności z tytułu czynów niedozwolonych[317]. W sytuacji jednak, kiedy między stronami występuje umowa, której zasadniczym elementem jest przetwarzanie danych osobowych, wówczas bezprawna operacja na danych osobowych może być naruszeniem umowy, a tym samym stanowić dodatkową podstawę odpowiedzialności obok odpowiedzialności deliktowej.

[314] Wyrok z 19.09.2013 r., sygn. akt I CSK 687/12, niepubl.
[315] Wyrok SN z 7.10.2020 r., sygn. akt V CSK 603/18; wyrok SN z 28.04.1964 r., sygn. akt II CR 540/63, OSPiKA 1965, poz. 197.
[316] Wyrok z 19.09.2013 r., sygn. akt I CSK 687/12, niepubl.
[317] A. Pązik, *Szkoda wynikająca* …, s. 132—133; M. Gumularz, *Wpływ regulacji...*, s. 32—33.

Normy prawne wiążące uczestników systemu ochrony danych osobowych będą podlegały także analizie w kontekście konkurencyjności reżimów odpowiedzialności odszkodowawczej, zwłaszcza że w prawie polskim nie sposób sformułować generalnego poglądu, że któryś z nich jest korzystniejszy dla poszkodowanego. Zakres odpowiedzialności i wygoda dochodzenia naprawienia szkody w obu reżimach przedstawiają się różnie, co może prowadzić w konkretnych wypadkach do znacznych różnic w atrakcyjności każdego z reżimów dla dłużnika i wierzyciela[318]. Zdaniem W. Czachórskiego gdyby jeden i ten sam stan faktyczny mógł teoretycznie podlegać ocenie zarówno norm jednego jak i drugiego reżimu, okazałoby się, że w jednych punktach dogodniejszym z nich dla poszkodowanego jest reżim kontraktowy gdy w innych właśnie reżim deliktowy[319]. W. Czachórski był przeciwnikiem możliwości skorzystania z obydwu reżimów odpowiedzialności jednocześnie wskazując, że wybór dokonany przez poszkodowanego automatycznie wyklucza możliwość skorzystania z reżimu konkurencyjnego[320]. W przypadku zbiegu odpowiedzialności możliwe są zatem trzy rozwiązania: prymat odpowiedzialności deliktowej (z którym do czynienia mamy w przypadkach określonych w art. 435 i 436 k.c.), prymat odpowiedzialności kontraktowej (poprzez porozumienie stron zawarte na podstawie art. 443 k.c.) albo konkurencja roszczeń opartych na obydwu z tych podstaw, w którym to przypadku to do poszkodowanego należy prawo wyboru reżimu, w jakim będzie dochodził odszkodowania za doznany przez niego uszczerbek [321].

W przypadku RODO ze zbiegiem będziemy mieli do czynienia w sytuacji, kiedy przedsiębiorca, będący administratorem lub podmiotem przetwarzającym nie wywiąże się z obowiązków nałożonych na niego umową, a jednocześnie jego zachowanie stanowić będzie naruszenie zasad współżycia społecznego bądź innej normy obowiązującej niezależnie od stosunku obligacyjnego, którego jest stroną. Praktycznym przykładem takich naruszeń będzie wykorzystywanie danych osobowych zebranych od klienta na podstawie umowy w celu sprzecznym z wykonaniem umowy, czyli celem dla którego zostały one przekazane, albo wykraczającym poza ten cel, np. w celu realizacji innej umowy. Innym przykładem w takim przypadku będzie naruszenie podstawy prawnej przetwarzania danych osobowych, przepisu prawa dopuszczającego przetwarzanie poza postanowieniami umowy, tj. np. przepisy

[318] E. Łętowska, *Zbieg norm w prawie cywilnym*, Warszawa 2002, s. 87.
[319] W. Czachórski, *Zbieg odpowiedzialności według kodeksu zobowiązań*, Warszawa 1960, s. 50.
[320] W. Czachórski, *Odpowiedzialność kontraktowa i jej stosunek do odpowiedzialności deliktowej wg KC*, „Nowe Prawo" 1964/10, s. 958.
[321] J. Gudowski, G. Bieniek, Komentarz do art. 443 [w:] *Kodeks cywilny. Komentarz*, red. J. Gudowski, t. 3, *Zobowiązania. Część ogólna*, LEX.

podatkowe albo w przypadku, gdy została udzielona zgoda na przetwarzanie danych z jej naruszeniem, np. w zakresie działań marketingowych.

Cechą wspólną, łączącą poszczególne reżimy odpowiedzialności, jest obowiązek naprawienia szkody. Systematyka kodeksowa uzasadnia tezę o jednolitości reguł rządzących ustaleniem odszkodowania, niezależnie od reżimu, w ramach którego powstał taki obowiązek; wszelkie odstępstwa w tym zakresie muszą wynikać z ustawy lub czynności prawnej. Powoduje ona także, iż cele obowiązku naprawienia szkody, do których dochodzimy w wyniku wykładni art. 361–363 k.c., znajdują zastosowanie w odniesieniu do poszczególnych przypadków unormowanych w ramach każdego z reżimów[322]. Przyjęta w k.c. konstrukcja prowadzi do ujednolicenia systemu odpowiedzialności odszkodowawczej i stanowi wyraz dążenia do zacierania różnic między poszczególnymi reżimami[323].

Przenosząc powyższe rozważania na grunt RODO w tym miejscu wyszczególnić należy zdarzenia, z którymi przepisy mogą wiązać powstanie odpowiedzialności. Takim zdarzeniem, z którym może być związana odpowiedzialność za szkodę, będziemy mogli mieć do czynienia np. w przypadku naruszenia przepisów RODO dotyczących:

1. obowiązku uzyskania zgody od opiekuna dziecka poniżej 16 roku życia w przypadku oferowania dziecku usług społeczeństwa informacyjnego (art. 8 RODO);
2. przetwarzania niewymagającego identyfikacji (art. 11 RODO);
3. realizacji praw osób których dane dotyczą (art. 15 – 22 RODO)
4. obowiązku uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 RODO);
5. obowiązku uregulowania odpowiedzialności współadministratorów (art. 26 RODO);
6. obowiązku wyznaczenia przedstawiciela na terenie Unii przez administratora lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii (art. 27 RODO);
7. obowiązku administratora odpowiedniego uregulowania relacji z podmiotem przetwarzającym, przestrzegania przez podmiot przetwarzający obowiązków umownych i wynikających z przepisów RODO (art. 28 RODO)
8. obowiązku przetwarzania z upoważnienia administratora lub podmiotu przetwarzającego i na jego polecenie (art. 29 RODO);

[322] M. Kaliński, *Prawo zobowiązań – część ogólna. System Prawa Prywatnego*, t. 6, s. 21.
[323] M. Kaliński, *Prawo zobowiązań...*, s. 20.

9. obowiązku rejestrowania czynności przetwarzania (art. 30 RODO);
10. obowiązku współpracy z organem nadzorczym (art. 31 RODO);
11. obowiązku wdrożenia odpowiednich środków technicznych i organizacyjnych (art. 32 RODO);
12. obowiązku zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu; obowiązku dokumentowania naruszeń ochrony danych osobowych (art. 33 RODO);
13. obowiązku zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 RODO);
14. obowiązku dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych (art. 35 RODO) oraz obowiązku przeprowadzenia uprzednich konsultacji z organem nadzorczym (art. 36 RODO);
15. obowiązku wyznaczenia inspektora ochrony danych (art. 37 RODO), statusu inspektora ochrony danych (art. 38 RODO) oraz wypełniania zadań inspektora ochrony danych (art. 39 RODO);

Ponadto takimi zdarzeniami może być naruszenia obowiązków administratora i podmiotu przetwarzającego wynikających z przepisów o certyfikacji (art. 42 i 43 RODO), obowiązków podmiotu certyfikującego (art. 42 i 43 RODO) lub obowiązków podmiotu monitorującego, o których mowa w art. 41 ust 4 RODO. Z uwagi na brak funkcjonowania w krajowym porządku prawnym praktyki stosowania systemu certyfikacji i monitorowania obowiązki w tym zakresie nie będą stanowiły przedmiotu późniejszych analiz.

Niezależnie od wyszczególnionych powyżej obowiązków źródłem szkody może być niewykonanie lub nienależyte wykonania zobowiązania umownego. Relację umowną uczestników systemu ochrony danych osobowych rozpatrywać możemy głównie jako stosunek prawny pomiędzy administratorem a podmiotem przetwarzającym. Zagadnienia związane z charakterem świadczeń wspomnianych wyżej podmiotów będą przedmiotem rozważań w kolejnych rozdziałach pracy.

Poza przedmiotem badań niniejszej pracy pozostają, z uwagi na obszerność zagadnień prawnych które ich dotyczą, kwestie realizacji praw podmiotów danych.

Odpowiedzialność deliktowa – ogólna charakterystyka

Etymologicznie czyn niedozwolony oznacza czyn zakazany, zachowanie zabronione przez prawo. Tak też używany jest w języku potocznym. Od takiego rozumienia określania czyn niedozwolony musimy się odciąć od razu na wstępie naszych rozważań. Potoczne

znaczenie tego terminu niewiele ma wspólnego z zakresem, jakie polskie prawo cywilne temu pojęciu nadaje[324].

Odpowiedzialność deliktowa to rodzaj stosunku cywilnoprawnego, w ramach którego jeden podmiot (ponoszący odpowiedzialność) jest obciążony obowiązkiem naprawienia szkody dotykającej innego zindywidualizowanego podmiotu (poszkodowanego)[325].

Czyn niedozwolony (delikt) jest tradycyjnie uznawany za zdarzenie prawne, z którego wystąpieniem łączy się powstanie zobowiązania opiewającego na świadczenie, którego treścią jest naprawienie szkody (*in natura* albo przez zapłatę odszkodowania pieniężnego). Takie ujęcie uzasadnia włączenie do treści pojęcia deliktu nie tylko zdarzenia szkodzącego (zdarzenia, z którym ustawa wiąże odpowiedzialność za szkodę wyrządzoną innej osobie), ale także związku przyczynowego oraz samej szkody. Powszechnie wyróżniane przesłanki odpowiedzialności deliktowej– tj. zdarzenie szkodzące, szkoda oraz łączący je związek przyczynowy – konstrukcyjnie są więc nie tylko przesłankami odpowiedzialności deliktowej, lecz także elementami deliktu, rozumianego jako pewien stan faktyczny. W tak ujętej strukturze czynu niedozwolonego (odpowiedzialności deliktowej) uniwersalne, tj. powtarzalne, są jedynie niektóre elementy (przesłanki). Szkoda oraz związek przyczynowy między nią i zdarzeniem szkodzącym to nieodłączne elementy każdego czynu niedozwolonego i bez ich wystąpienia nie może dojść do powstania odpowiedzialności. Podobnie jest z trzecim wyróżnionym wyżej elementem – zdarzeniem szkodzącym. Zdarzenia te – w zależności od konkretnej podstawy odpowiedzialności– różnią się jednak zasadniczo. *De lege lata* ustawodawstwo polskie kształtuje je tak, że znajdują się wśród nich zarówno czyny człowieka (osoby odpowiadającej za szkodę lub bezpośredniego sprawcy, za którego odpowiada ktoś inny), jak i zdarzenia niestanowiące zachowania ludzi (np. ruch pojazdu, o którym mowa w art. 436 k.c. czy ruch przedsiębiorstwa w rozumieniu art. 435 k.c.). Pozwala to na wyróżnienie dalszych elementów deliktu (przesłanek odpowiedzialności deliktowej), tym razem charakterystycznych dla konkretnej podstawy odpowiedzialności, jak np. wina czy bezprawność zachowania składającego się na zdarzenie szkodzące[326].

Nie można zadowolić się stwierdzeniem, że termin „czyny niedozwolone" stanowią zbiorczą nazwę dla wszystkich wypadków, w których wyrządzenie szkody jest samodzielnym

[324] B. Lewszkiewicz-Petrykowska, *Wyrządzenie szkody przez kilka osób*, Warszawa 1978, s. 45.
[325] M. Kaliński, *Prawo zobowiązań...*, s. 12; M. Kaliński, *Szkoda na mieniu...*, s. 1 i n.; por. A. Śmieja [w:] *System Prawa Prywatnego...*, red. A. Olejniczak, s. 356.
[326] R. Strugała, *Dobra i interesy chronione w strukturze czynu niedozwolonego*, Warszawa 2019, https://sip-1legalis-1pl-1v27i8rcf003d.han3.lib.uni.lodz.pl/document-full.seam?documentId=mjxw62zogi3damrsga3dembohe&refSource=toc

źródłem zobowiązania. Pojęcie czynu niedozwolonego ma charakter obiektywny, ponieważ odwołuje się do obiektywnie zaistniałego stanu faktycznego[327]. Delikt określony w ustawie musi stanowić pewien „delikt – typ". To znaczy, że jego opis powinien pozostawać na takim stopniu ogólności, aby obejmował on ochroną deliktową zamierzony przez ustawodawcę typ aktywności lub rodzaj działań. Jednocześnie nie może on być zbyt szczegółowy, aby nie prowadził do zbytniego zawężenia możliwości nałożenia obowiązku naprawienia szkody na jej sprawcę w obszarach, w których wprowadzenie kompensacji jest pożądane[328]. Przepisy o czynach niedozwolonych tworzą zespół norm o charakterze ochronnym. Chodzi o ochronę przez niepożądaną szkodą, czyli taką, która w założeniu nie może być akceptowana ani przez poszkodowanego, ani przez porządek prawny[329].

Przepisy RODO stanowią samodzielną podstawę konstruowania stosownego roszczenia. Pytaniem jest natomiast to, jakie podmioty na mocy art. 82 RODO są uprawnione do dochodzenia roszczeń z tytułu szkody spowodowanej naruszeniem przepisów o ochronie danych osobowych. Zagadnieniu temu została poświęcona uwaga w dokrynie i tak co do określenia katalogu podmiotów uprawnionych z art. 82 RODO, pojawiają się trzy stanowiska:

1. mogą to być wyłącznie osoby, których dane dotyczą;
2. poza podmiotami z pkt 1, uprawnienia z art. 82 RODO przysługują również pozostałym osobom fizycznym;
3. poza podmiotami z pkt 1 i 2, na art. 82 RODO mogą się powołać także osoby prawne[330].

Marcin Górski uważa, że nie ma znaczenia dla roszczenia odszkodowawczego z tytułu art. 82 RODO, czy poszkodowany jest podmiotem danych, czy też inną osobą. Jednakże Autor ten zauważa, że z praktycznego punktu widzenia trudno jest wyobrazić sobie sytuację, aby na ten przepis powoływała się inna osoba niż ta, której dane dotyczą[331].

W doktrynie podjęto rozważania, czy roszczenie to ma charakter deliktowy, czy związane jest z odpowiedzialnością kontraktową. Biorąc pod uwagę naturę roszczenia, jego samodzielny charakter, niezależny od więzi o charakterze względnym, należy zgodzić się ze stanowiskiem, zgodnie z którym roszczenie z art. 82 RODO jest roszczeniem deliktowym. Na podstawie RODO można określić podstawowe jego przesłanki, choć zakres regulacji jest

[327] B. Lewaszkiewicz- Petrykowska, *Wina jako przesłanka odpowiedzialności z tytułu czynów niedozwolonych*, „Studia Prawno-Ekonomiczne" 1969/2, s. 45.
[328] J. Kuźmicka-Sulikowska, *Zasady odpowiedzialności deliktowej w świetle nowych tendencji w ustawodawstwie polskim*, Warszawa 2011, s. 451–452.
[329] B. Lewszkiewicz-Petrykowska, *Wina jako okoliczność*...
[330] W. Lamik, *Środki cywilnoprawne ochrony danych osobowych*. Rozprawa doktorska, Wrocław 2022 s. 217.
[331] M. Górski [w:] *Ogólne rozporządzenie o ochronie*..., red. M. Sakowska-Baryła, Warszawa 2018.

ograniczony i odnosi się tylko do niektórych elementów odpowiedzialności, pozostałe pozostawiając regulacji prawa krajowego[332].

Odnosząc się do przesłanki szkody, ustawodawca unijny ujmuje ją w art. 82 ust. 1 RODO jako „szkodę majątkową lub niemajątkową, jednocześnie wskazując w motywie 146. preambuły, że pojęcie szkody należy interpretować szeroko, w sposób w pełni odzwierciedlający cele rozporządzenia, a osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesione szkody, o czym będzie mowa w dalszej części pracy.

Problematyka związku przyczynowego nie została szczegółowo podjęta ani w art. 82 RODO, ani w preambule rozporządzenia. Konieczność istnienia takiego związku wynika jednak wprost z brzmienia omawianego przepisu RODO. Nie wskazano natomiast w żaden sposób, za jaką koncepcją przyczynowości opowiada się unijny legislator[333]. Określenie zasady odpowiedzialności z art. 82 RODO jest problematyczne, o czym będzie mowa w dalszej części pracy.

Odpowiedzialność kontraktowa – ogólna charakterystyka

Ogólną podstawą odpowiedzialności kontraktowej wprowadza Kodeks cywilny w artykule 471 k.c. Jak można zauważyć użyte w tym przepisie określenia niewykonanie i nienależyte wykonanie obejmują w zasadzie wszystkie postacie naruszenia więzi obligacyjnej. Oznacza to, że w prawie polskim odpowiedzialność kontraktowa może powstać w razie każdego naruszenia zobowiązania i nie jest ograniczona do poszczególnych, wskazanych w ustawie przypadków powstania odpowiedzialności kontraktowej. Nie wystarcza samo naruszenie więzi obligacyjnych. Roszczenie odszkodowawcze może przysługiwać wierzycielowi tylko wówczas gdy z naruszenia tego wynika szkoda. W związku z tym można wyróżnić trzy podstawowe przesłanki odpowiedzialności dłużnika, którymi są niewykonanie lub nienależyte wykonanie zobowiązania, szkoda, związek przyczynowy między niewykonaniem lub nienależytym wykonaniem zobowiązania szkodą. Jak wynika z artykułu 471 k.c. niewykonanie lub nienależyte wykonanie zobowiązania musi być następstwem okoliczności za które dłużnik odpowiada. Obowiązek odszkodowawczy dłużnika jest więc bezpośrednio sankcją naruszenia powinności obligacyjnych i wynikłej z tego szkody. Istotne znaczenie ma przyczyna naruszenia zobowiązania. Obowiązek odszkodowawczy powstaje, gdy jest nią okoliczność za którą dłużnik odpowiada. Stąd do dalszych przesłanek

[332] M. Jagielska, M. Jagielski, *W poszukiwaniu prawa właściwego dla cywilnoprawnych roszczeń odszkodowawczych,* „Problemy Prawa Prywatnego Międzynarodowego" 2021/28, s. 55.
[333] M. Jagielska, M. Jagielski, *W poszukiwaniu prawa...*, s. 58.

odpowiedzialności kontraktowej w prawie polskim należy zaliczyć istnienie okoliczności, za które dłużnik ponosi odpowiedzialność, oraz związek przyczynowy między przynajmniej jedną z takich okoliczności a niewykonaniem lub nienależytym wykonaniem zobowiązania[334].

Według art. 471 kc, i do niego się ograniczając, przyjęte jest domniemanie odpowiedzialności dłużnika, a jej wyłączenie, jak już było wspomniane musi wynikać z udowodnionych okoliczności wyłączających tę odpowiedzialność.

Mimo więc, że ustawodawca nie używa pojęcia winy dla wskazania razie jej braku nieodpowiedzialności dłużnika, to na gruncie Kodeksu cywilnego dominuje pogląd o przesłance winy w tkwiącej w art. 471 kc. Wprawdzie próbuje się twierdzić, że są to poglądy starsze i jakby nieaktualne, to jednak są one obecne w bieżącym orzecznictwie i u większości współczesnych autorów opowiadających się za utrzymaniem takiego uregulowania[335].

Według ujęcia klasycznego, do którego nawiązuje art. 353 k.c. zobowiązanie przedstawia się od strony dłużnika jako powinność spełnienia świadczenia, od strony wierzyciela zaś, jako skierowane do dłużnika roszczenia o spełnienie świadczenia. W ramach tego modelu pojęcie zobowiązania można scharakteryzować następującymi cechami: konkretyzacją podmiotów i treści, korelacją praw i obowiązków stron, ograniczeniem w czasie oraz istnieniem źródła więzi prawnej między stronami[336].

Zdaniem Sz. Byczko „zgodnie z powszechnie przyjętym stanowiskiem doktryny przedmiotem każdego stosunku cywilnoprawnego, a co za tym idzie także umowy, jest zachowanie się jego podmiotów (świadczenie), czasem zalicza się do tego przedmiotu także pewne obiekty, których to zachowanie dotyczy. Niezależnie od tego, jaką wagę nadamy tym obiektom, należy zgodzić się z poglądem W. Katnera, zgodnie z którym wprawdzie nie ważą one na ocenie zachowania stron, ale jednak bez nich wiele zachowań „wisiałoby w powietrzu" nie mając żadnego rzeczywistego punktu odniesienia. Przedmiotem stosunku prawnego są zachowania się podmiotów tego stosunku – ale zazwyczaj zrelatywizowane wobec konkretnych rzeczy lub elementów stanu faktycznego (lub innych podmiotów prawa)[337].

Istotą stosunku zobowiązaniowego jest obciążająca dłużnika powinność spełnienia świadczenia wierzycielowi. Jeżeli dłużnik nie spełnia świadczenia (lub spełnia je nienależycie) wierzyciel może domagać się przymusowego świadczenia. W przypadku, gdy uzyskanie

[334] T. Pajor, *Odpowiedzialność dłużnika...*, s. 35–36.
[335] W.J. Katner [w:] *Współczesne problemy prawa zobowiązań*, Warszawa 2015, s. 290.
[336] T. Pajor, *Odpowiedzialność dłużnika...*, s. 45.
[337] S. Byczko, *Interes ubezpieczeniowy aspekty prawne*, Warszawa 2013 s. 77.

świadczenia w drodze przymusowej egzekucji jest niemożliwe bądź gdy uzyskanie świadczenia in natura z powodu, np. nadmiernego opóźnienia utraci dla wierzyciela znaczenie, wierzytelność przekształca się w roszczenie o naprawienie szkody wynikłej z niewykonania zobowiązania[338].

Zakres zastosowania reguł odpowiedzialności kontraktowej wyznacza treść artykułu 471 k.c. Przepis ten odnosi się do sytuacji, gdy szkoda wynikła z niewykonania lub nienależytego wykonania zobowiązania. Między poszkodowanym a osobą odpowiedzialną musi zatem istnieć stosunek obligacyjny. Okoliczność, że wymienione podmioty łączy zobowiązanie, w ramach którego doszło do wyrządzenia szkody stanowi kryterium wyróżniające dla przypadków objętych odpowiedzialnością *ex contractu* [339].

W literaturze podnoszone są też głosy odmienne w stosunku do prezentowanych we wcześniejszych fragmentach pracy tj., że analiza przesłanek odpowiedzialności wynikających z art. 82 RODO oraz z art. 471 k.c. prowadzi do wniosku, że występuje tu (przynajmniej *prima facie*) większy stopień podobieństwa niż między pierwszą z wymienionych norm a art. 415 k.c. Artykuł 82 RODO znajduje bowiem zastosowanie w odniesieniu do zachowania, które: 1) jest bezprawne (w sensie naruszenia norm wymienionego rozporządzenia) i 2) pozostaje w związku przyczynowym ze 3) szkodą majątkową bądź niemajątkową. Jeśli poszkodowanemu uda się dowieść wystąpienia tych trzech okoliczności, to administrator lub osoba przetwarzająca dane musi wykazać, iż nie ponosi winy (domniemanie winy). Artykuł 471 k.c. uzależnia zaś odpowiedzialność odszkodowawczą od 1) bezprawności (w sensie: niewykonania lub nienależytego wykonania zobowiązania) zachowania pozostającego w 2) związku przyczynowym ze 3) szkodą majątkową. Zawinienie (okoliczności, za które dłużnik ponosi odpowiedzialność) również jest objęte domniemaniem. Co więcej, choć odpowiedzialność odszkodowawcza przewidziana w art. 471 k.c. jest określana jako kontraktowa, to z punktu widzenia brzmienia wymienionej normy podstawą tej odpowiedzialności może być także naruszenie zobowiązań wynikających z innych źródeł niż umowa bądź czynność prawna. Biorąc to pod uwagę, można teoretycznie przyjąć, że naruszenie przepisów RODO może być uznane za niewykonanie (nienależyte wykonanie) zobowiązania w rozumieniu art. 471 k.c. (w

[338] T.A. Filipiak, J.Mojek, M. Nazar, E.Niezbecka, *Zarys prawa cywilnego*, Lublin 2002 s. 366.
[339] T. Pajor, *Odpowiedzialność dłużnika...*, s. 42

tym kontekście byłoby to niewykonanie zobowiązania starannej ochrony danych osobowych)[340].

Na gruncie RODO najbardziej wyraźnym przykładem regulacji kontraktowych jest relacja administrator – podmiot przetwarzający, o których będzie mowa szczegółowo w dalszej części pracy.

Szkoda

Umiejscowienie unormowania dotyczącego naprawienia szkody w art. 361–363 k.c. stanowi regulację wspólną dla obu reżimów odszkodowawczych[341]. RODO w art. 82 w ust. 1, 2 i 3 posługuje się pojęciem szkody, wyznaczając zasadę odpowiedzialności administratora i podmiotu przetwarzającego w sposób, określony poniżej:

1. każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2. każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem poleceniami administratora lub wbrew takim poleceniom.

W ust. 4 i 5 art. 82 RODO zawarte jest określenie odszkodowanie w celu określenia zasad odpowiedzialności solidarnej i roszczeń regresowych w sposób, określony poniżej:

1. jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.
2. administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym

[340] A. Pązik, *Szkoda wynikająca z naruszenia przepisów RODO. Wybrane problemy*, ZNUJ PPWI 2020/3, s. 127–146.
[341] *Prawo zobowiązań – część ogólna. System Prawa Prywatnego – suplement do tomu 6*, red. A. Olejniczak, Warszawa 2010.

przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2.

W języku prawnym oraz prawniczym wyróżnia się szkodę majątkową i niemajątkową (zwaną także zamiennie krzywdą, szkodą niematerialną, czy krzywdą niemajątkową). Podział na szkodę majątkową i niemajątkową stanowi najwyższy szczebel klasyfikacji pojęcia szkody według kryterium przedmiotu oddziaływania zdarzenia szkodzącego na sferę dóbr poszkodowanego. W tym ujęciu użycie kwalifikatora nawiązującego do pojęcia majątku ma swój walor tylko o tyle, o ile rozumie się je w znaczeniu węższym, to znaczy jako ogół aktywów majątkowych służących poszkodowanemu. Chociaż określenie to nie jest wolne od tautologii, to jednak przybliża w sposób intuicyjny sens sformułowania „szkoda majątkowa”[342].

Ze względu na granicę treści zobowiązania tylko szkody wynikłe z niespełnienia lub nienależytego spełnienia świadczenia podlegają naprawieniu na podstawie przepisów reżimu kontraktowego. Formułując tę myśl nieco inaczej można powiedzieć, że reżim ten stosuje się jedynie do uszczerbków pozostających w ścisłym, funkcjonalnym związku z wykonywaniem zobowiązania. Jeżeli zaś wyrządzenie szkody nastąpiło wskutek naruszenia obowiązków powszechnych przy okazji ich wykonywania, w grę może wchodzić jedynie deliktowa odpowiedzialność sprawcy[343].

Istota szkody jako przesłanki odpowiedzialności cywilnej wyraża się w zasadzie: jak długo nie ma szkody, tak długo nie ma obowiązku jej naprawienia, w konsekwencji nie ma też odpowiedzialności cywilnej. Odpowiedzialność deliktowa w razie istnienia stosunku zobowiązaniowego zachodzi jedynie wtedy, gdy szkoda jest następstwem takiego działania lub zaniechania sprawcy, które stanowi samoistne, tzn. niezależne od zakresu istniejącego zobowiązania, naruszenie ogólnie obowiązującego przepisu prawa bądź zasad współżycia społecznego[344].

Szkodę majątkową stanowi różnica między obecnym stanem majątku poszkodowanego a stanem, jaki zaistniałby, gdyby nie nastąpiło zdarzenie, które doprowadziło do wystąpienia tej różnicy. Ta metoda określania szkody, zwana dyferencyjną, polega na hipotetycznym odtworzeniu najbardziej prawdopodobnego przebiegu zdarzeń bez uwzględnienia szkody i ustaleniu jego wpływu na stan majątkowy poszkodowanego, a następnie porównaniu go ze

[342] M. Kaliński, *Szkoda…*, s. 208-209.
[343] T. Pajor, *Odpowiedzialność dłużnika...*, s. 50
[344] Zob. M.Serwach, *Odpowiedzialność cywilna w teorii i w praktyce – najnowsze tendencje i kierunki zmian*, „Rozprawy Ubezpieczeniowe” 2009/1/6, http:/rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/

stanem powstałym wskutek tego zdarzenia. Stopień prawdopodobieństwa takiego przebiegu zdarzeń powinien być tak wysoki, że w świetle wiedzy i zasad doświadczenia życiowego wyklucza możliwość przyjęcia, że bieg zdarzeń byłby inny. Ustalenie tej różnicy następuje z uwzględnieniem tego, że szkodą jest każdy uszczerbek w dobrach prawnie chronionych, z którym ustawa wiąże powstanie odpowiedzialności odszkodowawcze[345].

Artykuł 82 RODO posługuje się odmienną od kodeksowej aparaturą pojęciową. Mowa w nim między innymi o szkodzie majątkowej i odszkodowaniu za nią, podczas gdy Kodeks cywilny posługuje się na określenie takiej szkody i kompensaty za nią pojęciem krzywdy i zadośćuczynienia – zob. art. 445 k.c. czy art. 448 k.c. Szkoda związana z przetwarzaniem danych osobowych może być więc zarówno szkodą majątkową (w przeważającym zakresie), jak i szkodą niemajątkową (w rzadszych przypadkach). Zagadnienie szkody niemajątkowej w obszarze ochrony danych osobowych wciąż budzi kontrowersje. Dotyczy to zwłaszcza krzywdy rozumianej jako utrata kontroli nad danymi osobowymi, czego przykładem jest wyrok Sądu Najwyższego Zjednoczonego Królestwa z 10.11.2021 r. w sprawie Lloyd v. Google (UKSC 2019/0213)[346]. Wskazana sprawa związana była z zarzutem, które Lloyd sformułował w ramach powództwa przedstawicielskiego[347] przeciwko Google w imieniu około 4 milionów osób, twierdząc, że Google bezprawnie przetwarzał dane przeglądarki bezpośrednio z urządzeń mobilnych użytkowników bez ich zgody. Zdaniem Lloyd Google korzystał z tak zwanego „obejścia Safari", aby dokonać ustawień prywatności w celu śledzenia plików cookie na potrzeby reklamy ukierunkowanej. W toku postepowania w wyniku kontroli instancyjnej sformułowane zostały w tej sprawie zagadnienia problemowe, skierowane do Supreme Court dotyczące tego, czy roszczenie odszkodowawcze może być rozpatrywane w okolicznościach, w których nie poniesiono żadnej straty pieniężnej, szkody lub cierpienia, w wyniku czego wnioskodawcy mogą wnieść powództwo tylko o „utratę kontroli" nad swoimi danymi? W ich konsekwencji Sąd uznał, że przy właściwej wykładni pojęcie „szkody" musi oznaczać szkodę materialną (taką jak strata finansowa) lub cierpienie psychiczne, a nie tylko samo niezgodne z

[345] Wyrok SN z 23.11.2018 r., sygn. akt II CSK 682/17.
[346] Wyrok dostępny na stronie internetowej https://www.supremecourt.uk/cases/uksc-2019-0213.html, a istotne komentarze w tej sprawi dostępne na przykład: https://www.pinsentmasons.com/out-law/analysis/lloyd-v-google-supreme-court-representative-action oraz https://verfassungsblog.de/lloyd-privacy/
[347] Powództwo przedstawicielskie jest formą postępowania sądowego typu „opt-out", które jest wnoszone w imieniu wszystkich członków określonej kategorii powodów, o ile nie zrezygnują. Procedura wnoszenia powództwa w charakterze powództwa przedstawicielskiego jest zawarta w zasadzie 19.6 k.p.c., która wymaga, aby powództwo takie mogło zostać wniesione przez lub przeciwko przedstawicielowi innych osób, które mają „ten sam interes" w powództwie

prawem przetwarzanie. W związku z tym roszczenia na podstawie na tej podstawie podnoszone wymagają dowodu straty finansowej lub trudności, aby znaleźć uzasadnienie prawne do powództwa.

W piśmiennictwie jako przykłady szkód wyrządzonych administratorom danych przez podmioty przetwarzające i podprzetwarzające wskazywane są straty finansowe, utrata wiarygodności, utrata pozycji na rynku, utrata klientów, zmniejszenie lub utrata dochodów, zasobów własnych. W zakresie szkód wyrządzonych na skutek przetwarzania danych w dobrach osób, których przetwarzane dane dotyczą, podnoszone jest, że mogą częściej niż w poprzednim przypadku wystąpić szkody niemajątkowe. Może to być np. ciężki uszczerbek na zdrowiu (wywołany np. długotrwałym stresem i poczuciem braku bezpieczeństwa z powodu wycieku danych z systemu bankowości elektronicznej) czy też utrata dobrego imienia (np. na skutek popełnionych oszustw w związku z kradzieżą tożsamości)[348]. Według UODO szkodą jest ujawnienie danych osobowych, a w szczególności takich danych, jak numer ewidencyjny PESEL wraz z imieniem i nazwiskiem oraz informacjami o stanie finansowym / majątkowym ponieważ może zostać wykorzystane lub powodować np. ograniczenie możliwości korzystania z praw obywatelskich i usług kierowanych do ogółu obywateli (np. głosowania w ramach budżetu obywatelskiego, internetowej rejestracji wizyt w urzędach itp.); osoby trzecie mogą podjąć próbę uzyskania pożyczek w instytucjach pozabankowych z użyciem danych osoby dotkniętej naruszeniem, np. przez internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości; osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o stanie zdrowia osoby dotkniętej naruszeniem, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać potwierdzając swoją tożsamość za pomocą numeru PESEL; osoby trzecie mogą podjąć próbę zawarcia na szkodę osoby dotkniętej naruszeniem umów cywilnoprawnych[349].

Rozważając dalej wątek przykładów szkód, wskazać także należy na decyzję PUODO,[350] w której podniesione zostało, że ujawnienie numeru PESEL wraz z imieniem i nazwiskiem ze względu na możliwe doniosłe negatywne konsekwencje dla osoby fizycznej może powodować duży stres lub dyskomfort, związany z możliwością materializacji negatywnych zagrożeń (w postaci np. straty finansowej, czy kradzieży tożsamości), zaburzając poczucie bezpieczeństwa takiej osoby, podobnie jak ujawnienie danych behawioralnych.

[348] M. Czech, *Umowa powierzenia...*, s. 302.
[349] Decyzja UODO DKN.5131.3.2021.
[350] Decyzja UODO DS.523.3908.2021.PR.KM.1414.

Jednak poziom stresu lub dyskomfortu osoby fizycznej w związku z ujawnieniem numeru PESEL jest znacznie wyższy niż przy ujawnieniu takich danych jak dane dotyczące lokalizacji (GPS), identyfikatory sieciowe (cookies itp.), przeszukiwane zasoby internetowe. Dotkliwość ujawnienia danych w postaci numeru PESEL wraz z imieniem i nazwiskiem jest porównywalna, jak w przypadku ujawnienia „danych finansowych" (które również zostały ujawnione w wyniku przedmiotowego naruszenia), czy danych „szczególnie chronionych" (decyzja UODO). PESEL, czyli jedenastocyfrowy symbol numeryczny, jednoznacznie identyfikujący osoby fizyczne, zawierający m.in.: ich datę urodzenia oraz oznaczenie płci, a więc informacje ściśle powiązane ze sferą prywatną tych osób. Takie konsekwencje. mogą być kwalifikowane w kategorii szkody.

W orzecznictwie problem szkody na gruncie RODO był analizowany incydentalnie. Na potrzeby pracy warto wskazać na orzeczenia, które wydane zostały na gruncie poprzednio obowiązujących przepisów, ale w cytowanych fragmentach pozostają aktualne. Jak zauważono zatem w wyrok Sądu Apelacyjnego w Łodzi „jako niewielki zakres naruszenia prywatności, nie powodujący negatywnych skutków w sferze przeżyć psychicznych, uznawane jest naruszenie, które powoduje brak jakichkolwiek niekorzystnych następstw naruszenia dobra osobistego w świecie zewnętrznym. Takim naruszeniem jest działanie, polegające na tym, że przez kilkanaście godzin zawierające dane pismo było dostępne dla osób trzecich, a na skutek protestu powódki, pismo od razu zostało zdjęte przez pozwanego, który w kolejnym piśmie wyjaśnił powódce cel swojego postępowania. Ustawodawca nie wprowadził żadnych kryteriów, jakimi powinien kierować się sąd przy ustalaniu wysokości należnego poszkodowanemu zadośćuczynienia, ograniczając się jedynie do stwierdzenia, iż ma być ono „odpowiednie". Już z powyższego wynika zatem, że pojęcie „sumy odpowiedniej" jest pojęciem o charakterze niedookreślonym. Kryteriami, którymi należy kierować się przy ustalaniu wysokości zadośćuczynienia pieniężnego za naruszenie dóbr osobistych. są m.in.: rodzaj naruszonych dóbr osobistych, forma naruszenia, stopień nasilenia i czas trwania ujemnych przeżyć psychicznych spowodowanych naruszeniem i wpływ naruszenia na społeczną pozycję pokrzywdzonego, a także rodzaj i stopień winy sprawcy szkody z uwzględnieniem, iż nie pozostaje bez znaczenia także cel, który zamierzał osiągnąć sprawca podejmując działanie naruszające dobra osobiste[351].

Innego przykładu oceny żądania zasądzenia zadośćuczynienia dostarcza orzeczenie Sądu, w którym podkreślone zostało, że brak jest podstaw do uznania, że powód wskutek

[351] Wyrok SA w Łodzi – I Wydział Cywilny z 17.12.2015 r., sygn. akt I ACa 806/15.

przesyłania mu nie zamówionej informacji handlowej doznał krzywdy, której naprawienie mogłoby nastąpić w drodze zapłaty zadośćuczynienia w żądanej przez niego kwocie. Zdaniem Sądu na podstawie uzasadnienia pozwu nie sposób jest bowiem stwierdzić, na czym tak krzywda miałaby polegać (nawet nie sposób jest podać przykład tego jaką konkretnie krzywdę mogłoby wyrządzić samo otrzymywanie na adres poczty elektronicznej nie zamówionej informacji handlowej). Sam fakt, że działanie takie narusza dobra osobiste nie oznacza, że jest ono jednocześnie źródłem krzywdy. (…) Powód w żaden sposób nie odnosi się zatem do krzywdy jaką miałaby mu przynieść działalność pozwanej, wskazując co najwyżej na koszty postępowania wywołane jej działaniem, a więc należność nie objętą roszczeniem zgłoszonym w niniejszej sprawie. Argumentacja powoda wskazuje wprost, że traktuje on żądaną od pozwanej kwotę w kategoriach „kary" za niewłaściwe postępowanie pozwanej, nie zaś zadośćuczynienia za faktycznie doznaną przez niego krzywdę. Stanowisko to koreluje z podnoszonym także przez powoda w uzasadnianiu roszczenia o zadośćuczynienie faktem, że powód uprzednio domagał się zapłaty od pozwanej różnych kwot w zamian za nie wszczynanie przeciwko niej postępowań, bez wskazania, że kwoty te mają stanowić zadośćuczynienie ani nawet, że czuje się pokrzywdzony działaniami pozwanej[352].

W doktrynie zauważa się, że pojęciu szkody na tle przepisów rozporządzenia należy nadać autonomiczne znaczenie,[353] które nie musi odpowiadać rozumieniu szkody utrwalonemu na gruncie krajowych porządków prawnych. Takie podejście może jednak rodzić trudności interpretacyjne pojęcia szkody i problemy praktyczne. Faktem jest, że pojęcie to może być kształtowane przez orzecznictwo TSUE, ale Trybunał nie wypracował do tej pory definicji szkody odnoszącej się do odpowiedzialności za naruszenie przepisów chroniących dane osobowe. Sytuacja ta zapewne ulegnie zmianie w związku z orzeczeniem niemieckiego Federalnego Trybunału Konstytucyjnego, który nakazał sądowi niższej instancji (Sąd Rejonowy w Goslar) zwrócenie się do TSUE z pytaniem prawnym, czy już drobne naruszenie RODO może stanowić podstawę odszkodowania za szkody niematerialne na podstawie art. 82. Powstaje jednak pytanie, na ile dotychczasowe orzecznictwo TSUE w przedmiocie pojęcia szkody, w tym szkody spowodowanej naruszeniem danych osobowych, może znaleźć zastosowanie dla roszczenia z art. 82 RODO, zwłaszcza biorąc pod uwagę zawartą w preambule dyrektywę przyznawania pełnego i skutecznego odszkodowania. Wydaje się raczej, że sądy krajowe — przynajmniej tak długo, jak długo kwestia ta nie zostanie rozstrzygnięta przez TSUE

[352] Wyrok SA w Warszawie – V Wydział Cywilny z 17.05.2017 r., sygn. akt VI ACa 223/16.
[353] A. Pązik, *Szkoda wynikająca...*, s. 133—134.

— będą interpretować pojęcie szkody zgodnie z prawem wewnętrznym[354]. W chwili obecnej najwięcej rozbieżności w orzecznictwie sądów krajowych wywołuje kwestia rekompensaty szkód o charakterze niematerialnym, a zwłaszcza tego, czy dla przyznania odszkodowania wystarczy samo naruszenie RODO, czy też musi wystąpić jakiś uszczerbek na dobrach podmiotu domagającego się ochrony. Na najbardziej rygorystycznym stanowisku stoją w tym względzie sądy niemieckie i austriackie, wskazując na konieczność zaistnienia obiektywnego naruszenia jakiegoś prawnie chronionego dobra. Sądy niderlandzkie są mniej wymagające w tym względzie, przyznając odszkodowanie, mimo że szkoda nie może być precyzyjnie określona i może mieć stosunkowo niewielki zakres, natomiast sądy angielskie w ogóle takiego powiązania nie wymagają, przyznając rekompensatę za sam fakt naruszenia regulacji chroniącej dane osobowe. W tym ostatnim przypadku rozstrzygnięcie zapadło co prawda na tle dyrektywy 95/46, niemniej jednak w doktrynie podkreśla się, że stanowisko to nie powinno ulec zmianie na tle RODO[355]. Z punktu widzenia odpowiedniego stosowania k.c. do RODO wskazać należy na celowość rozumienia odszkodowania w sposób typowy dla każdego porządku prawnego krajowego.

W kwestii tego, czy na gruncie art. 82 RODO samo naruszenie RODO prowadzi już do roszczenia przeciwko administratorowi danych, czy też musi również istnieć wyraźnie wymierna szkoda najszerzej wypowiadają się, obok omawianej sprawy Lioyd v Google także sądy niemieckie. Wcześniejsze orzecznictwo niemieckie (do roku 2018) przyznawało zadośćuczynienie za szkody niemajątkowe tylko w przypadku poważnych naruszeń dóbr osobistych, co wynikało wprost ze starej wersji ustawy o ochronie danych osobowych. Obecnie nie ma jednolitego orzecznictwa. Wyższy Sąd Krajowy we Frankfurcie (OLG Frankfurt 13 U 206/20 z 02.03.2022 r.) uznał że warunkiem roszczenia odszkodowawczego na podstawie art. 82 RODO jest udowodnienie konkretnej (w tym niemajątkowej) szkody „Wymóg udowodnienia rzeczywiście poniesionej szkody jest zatem niezbędny także co do istoty, aby uniknąć mnożenia się roszczeń o odszkodowanie we wszystkich przypadkach naruszenia ochrony danych - które w rzeczywistości nie ma żadnych konsekwencji dla osoby, której dane dotyczą". Podobne stanowisko zajął Sąd Krajowy w Lipsku (LG Leipzig 03 O 1268/21 z 23.12.2021 r.). „Samo naruszenie RODO nie jest wystarczające do wniesienia roszczenia o odszkodowanie. Osoba dotknięta naruszeniem ochrony danych musi raczej doznać zauważalnej niekorzyści. Musi istnieć obiektywnie zrozumiałe naruszenie dóbr osobistych o określonej wadze. Szkoda musi mieć określone znaczenie." Również w opinii Wyższego Sądu Krajowego

[354] M. Jagielska, M. Jagielski, *W poszukiwaniu prawa...*, s. 58.
[355] M. Jagielska, M. Jagielski, *W poszukiwaniu prawa...*, s. 57.

w Dreźnie (4 U 760/19 z 11.06.2019 r.) „art. 82 RODO nie może być rozumiany w ten sposób, że każda indywidualnie postrzegana niedogodność lub każde błahe naruszenie wizerunku lub reputacji danej osoby może uzasadniać roszczenie o odszkodowanie niemajątkowe.” Są też stanowiska odmienne. Sąd Okręgowy w Karlsruhe (4 O 67/20 z 09.02.2021 r.) uznaje, że „w przeciwieństwie do starego prawa nie jest obecnie konieczne poważne naruszenie dóbr osobistych do dochodzenia szkody niemajątkowej”. Wyższy Sąd Krajowy w Kolonii przyznał powodowi 500 euro, ponieważ ten odczuwał "stres i zmartwienie" jedynie z powodu spóźnionych informacji (15 U 137/21). Nie sposób zaznaczyć, że taki wymiar odszkodowania ma symboliczną wartość. Federalny Sąd Pracy stwierdził w kontekście sporu z zakresu prawa pracy, że roszczenie o odszkodowanie niemajątkowe na podstawie RODO nie wymaga od poszkodowanego wykazania poniesionej szkody wykraczającej poza naruszenie RODO [8 AZR 253/20 (A)][356]. Zagadnienie pojęcia szkody stało się także przedmiotem pytania prejudycjalnego do TSUE szeroko omówionego w dalszej części pracy.

Rodzaje świadczeń

Innym zagadnieniem istotnym z punktu widzenia omawianych zagadnień ogólnych dotyczących odpowiedzialności jest to, czy reguły dotyczące wykonania zobowiązania można odnieść do oceny naruszenia obowiązków powszechnych wynikających z RODO. W tym miejscu podkreślenia wymaga, że ze względu na zasadę swobody umów i wynikający z niej brak *numerus clausus* typów stosunku obligacyjnych, kształt możliwych świadczeń nie da się określić z góry w sposób wyczerpujący. W związku z tym w każdym wypadku konieczne jest przede wszystkim badanie konkretnego zobowiązania i określenie świadczenia, które dany dłużnik powinien spełnić. Różnorodność i zmienność treści zobowiązania nie wyklucza jednak operowania dla celów analizy prawniczej pewnymi rodzajami świadczeń. Ich klasyfikacje przeprowadzane są przez uwzględnieniu wielu różnych kryteriów. Sama ustawa wprowadza rozróżnienie między świadczeniami polegającymi na działaniu i na zaniechaniu. Przede wszystkim wskazuje się, że podział ten pozwala sprecyzować przedmiot stron, a co za tym idzie określić na czym polega niewykonanie zobowiązania w poszczególnych wypadkach. Przy zobowiązaniach rezultatu niewykonanie zachodzi, gdy oznaczony rezultat nie został osiągnięty. W zakresie zobowiązań starannego działania o niewykonaniu stanowi niedołożenie staranności, do której dłużnik był zobowiązany. Co do pozostałych konsekwencji omawianej klasyfikacji

[356] T. Borys, *Ochrona danych osobowych / GDPR / RODO / DSGVO*, https://www.linkedin.com/in/tomasz-borys-32725915a/recent-activity/all/

brak jest zgodności poglądów. Według poglądu przeważającego podział na zobowiązania rezultatu i starannego działania nie wpływa na podstawę odpowiedzialności kontraktowej która zawsze pozostaje oparta na zasadzie winy. Podział wywiera natomiast wpływ na rozkład ciężaru dowodu przesłanek tej odpowiedzialności[357].

Podział ten jest istotny także dlatego, że temat kryteriów przedmiotowych, stanowiących podstawę odpowiedzialności deliktowej z art. 415 k.c. jest przedmiotem dyskusji w piśmiennictwie[358], która koncentruje się wokół problemu zakwalifikowania kryteriów należytej staranności jako przesłanki ponoszenia odpowiedzialności za czyn własny.

Podstawowym sposobem wykonania zobowiązania jest spełnienie świadczenia, tj. takie zachowanie dłużnika, które odpowiada treści zobowiązania. W typowej sytuacji zobowiązanie zostanie wykonane, gdy dłużnik świadczył do rąk osoby uprawnionej, we właściwym miejscu i we właściwym czasie. Te trzy elementy modalne są typowym probierzem prawidłowości wykonania zobowiązania, jednak nie stanowią żadnej zamkniętej listy. Zachowanie dłużnika powinno odpowiadać dalszym elementom treści zobowiązania, w tym uwzględniać wskazane w art. 354 § 1 k.c. zasady współżycia społecznego, społeczno-gospodarczy cel zobowiązania oraz uwzględniać ustalone zwyczaje. Artykuł 355 k.c. nakłada na dłużnika obowiązek działania z należytą starannością[359].

Pogląd odnajdujący w ramach konstrukcji odpowiedzialności deliktowej reguły staranności na przestrzeni lat zyskał sobie licznych zwolenników[360], tak jak przeciwny tej tezie postulat, że art. 355 k.c. i zawarte w jego treści standardy należytej staranności dotyczą jedynie reżimu kontraktowego a nie deliktowego[361]. Wątpliwości związane z kierunkiem rozstrzygnięcia powyższej dyskusji potęguje fakt, że charakter świadczeń objętych obowiązkami, wynikającymi z ochrony danych osobowych nie jest jednolity. Takie głosy były podnoszone już w okresie obowiązywania dyrektywy 95/46/WE. I tak zdaniem B. van Alsenoya, aby w pełni zrozumieć odpowiedzialność administratora danych w dyrektywie 95/46/WE, konieczne jest najpierw ustalenie istoty jego obowiązków. Te z kolei dzieliły się na dwie podstawowe kategorie:

---

[357] T. Pajor, *Odpowiedzialność dłużnika...*, s. 69-73.
[358] T. Nowakowski, *Reguły staranności a odpowiedzialność deliktowa – glosa do wyroku Sądu Apelacyjnego w Łodzi z dnia 30.01.2018. (I AC A 727/17)*, „Palestra" 2020/11.
[359] *Prawo zobowiązań – część ogólna...*, red. A. Olejniczak.
[360] B. Lewaszkiewicz-Petrykowska, *Wina jako przesłanka...*, s. 97; A. Szpunar, *Czyny niedozwolone w kodeksie cywilnym*, „Studia Cywilistyczne" 1970/15, s. 54.
[361] P. Machnikowski [w:] *System prawa prywatnego*, t. 6, *Prawo zobowiązań – część ogólna*, red. A. Olejniczak, Warszawa 2014, s. 401–403; M. Gutowski [w:] *Kodeks cywilny – komentarz*, red. M. Gutowski, Warszawa 2016, t. 2, s. 1257; Z. Banaszczyk, P. Granecki, *O istocie należytej staranności*, „Palestra" 2002/7–8, s. 24.

1. obowiązek co do osiągnięcia konkretnego rezultatu (np. zgodnie z art. 6 ust. 1 lit. b) dyrektywy, który stanowi, że dane osobowe muszą być gromadzone do określonych, jednoznacznych i legalnych celów oraz nie mogą być poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem);
2. obowiązek podjęcia uzasadnionych starań dla osiągnięcia konkretnego celu (np. art. 6 ust. 1 lit. d) dyrektywy, zgodnie z którym administrator danych musiał podjąć „wszelkie uzasadnione" działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane).

Tym samym charakter obowiązku administratora powinien być precyzowany w świetle konkretnego brzmienia każdego przepisu[362], co dla analiz dokonywanych w pracy ma podstawowe znaczenie.

Okoliczności, za które dłużnik odpowiada na gruncie odpowiedzialności kontraktowej

Obowiązek odszkodowawczy dłużnika nie jest bezpośrednio sankcją naruszenia stosunku zobowiązaniowego i wynikłej z tego szkody. Istotne znaczenie ma przyczyna naruszenia zobowiązania. Obowiązek odszkodowawczy powstaje gdy jest nim okoliczność, za którą dłużnik odpowiada. Stąd też do dalszych przesłanek odpowiedzialności kontraktowej w prawie polskim należy zaliczyć: istnienie okoliczności za które dłużnik ponosi odpowiedzialność oraz związek przyczynowy między przynajmniej jedną z tych okoliczności a niewykonaniem lub nienależytym wykonaniem zobowiązania. Odnośnie do dwóch ostatnich przesłanek można ze sformułowań artykułu 471 k.c. wnioskować, że ciężar ich udowodnienia nie spoczywa na poszkodowanym wierzycielu, a przeciwnie do dłużnika należy wykazanie ich braku. Ustawodawca wprowadza więc domniemanie, że będące przyczyną szkody naruszenie zobowiązania jest następstwem okoliczności, za które dłużnik odpowiada. Dla zwolnienia się od obowiązku odszkodowawczego dłużnik musi to domniemanie obalić, wykazując, że niewykonanie lub nienależyte wykonanie zobowiązania jest następstwem okoliczności, za które odpowiedzialności nie ponosi. Jak można zauważyć sformułowanie końcowej części artykułu 471 k.c. nie wyjaśnia ani zasady odpowiedzialności dłużnika, ani też treści dowodu zwalniającego. Taka redakcja przepisu nie stanowi jednak usterki. Art. 471 k.c. nie precyzuje wspomnianych kwestii, gdyż nie mogą być one z góry jednolicie rozstrzygnięte. To, za co dłużnik w konkretnym wypadku odpowiada, oraz jakimi dowodami może się zwolnić, określa

[362] B. Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability*, „Intersentia" 2019/6, s. 85; W. Lamik, *Środki cywilnoprawne ochrony...*, s. 196.

przede wszystkim treść czynności prawnej będącej źródłem zobowiązania, oraz przepisy właściwe dla danego stosunku prawnego. Dopiero w braku szczegółowych postanowień czynności prawnej lub ustawy znajdują zastosowanie ogólne reguły Kodeksu wskazujące, za jakie okoliczności dłużnik ponosi odpowiedzialność (artykuł 472-474 k.c.**)**. Jednakże nawet w myśl tych reguł ogólnych odpowiedzialność dłużnika nie opiera się na jednej zasadzie. Ramową formułę o okolicznościach za które dłużnik odpowiada należy rozumieć jako odesłanie do tych wszystkich postanowień ustawowych lub umownych, które w danym wypadku określają zasady odpowiedzialności dłużnika. Na tle powyższej charakterystyki unormowania polskiego nasuwa się spostrzeżenie, że przy kształtowaniu zasad odpowiedzialności kontraktowej ustawodawca położył główny nacisk na jej funkcję kompensacyjną. Odpowiedzialność ta nie stanowi w prawie polskim bezpośredniej sankcji naruszenia zobowiązania. Regułą jest, że wierzyciel może dochodzić odszkodowania dopiero wówczas, gdy naruszenie wynikło z winy dłużnika. Na kompensacyjny charakter omawianej odpowiedzialności dodatkowo wskazuje stosowanie do niej ogólnych przepisów o naprawieniu szkody jak również dopuszczalność zbiegu odpowiedzialności zgodnie z art. 443 k.c. [363].

Przyjmując winę jako regułę dochodzenia odszkodowania, podkreślić trzeba, że winę należy rozpatrywać według normatywnej koncepcji jej zarzucalności. Tezę tę rozwinęła w prawie polskim B. Lewaszkiewicz-Petrykowska czyniąc to na gruncie odpowiedzialności z tytułu czynów niedozwolonych. Oznacza to, że osobie odpowiedzialnej (dłużnikowi) stawia się zarzut nagannego zachowania. Żeby to uczynić muszą zostać spełnione przesłanki subiektywne i obiektywne winy[364]. Prawidłowe określenie winy możliwe jest tylko na gruncie teorii normatywnej. Zgodnie z nią wina stanowi ujemną ocenę całokształtu postępowania określonej osoby, wydaną na podstawie oceny stanu psychicznego tejże osoby i istniejących norm. Wina polega na możliwości uczynienia zarzutu, którego treścią jest stwierdzenie naganności postępowania. Ujęcie winy jako zarzucalności pozwala na posługiwanie się tym terminem jednolicie w stosunku do całego systemu prawa, przy jednoczesnym zagwarantowaniu zachowania niezbędnych odrębności występujących w każdej dziedzinie[365].

Przenosząc powyższe rozważania na grunt ochrony danych osobowych, podnieść należy, że co do przesłanek zawinienia na gruncie ochrony danych osobowych wypowiadały się sądy. Ciekawej ilustracji dostarcza jedno z orzeczeń, w którym wskazane zostało, że o

[363] T. Pajor, *Odpowiedzialność dłużnika...* s. 35-39.
[364] W.J. Katner [w:] *Współczense problemy prawa zobowiązań*, Warszawa 2015, s. 291
[365] B. Lewaszkiewicz-Petrykowska, *Wina jako podstawa...*, t. 2, s. 87.

zawinionym działaniu można mówić dopiero od momentu, gdy do pozwanego dotarła informacja, że powód nie życzy sobie otrzymywania informacji handlowych. Do tego momentu bowiem przyjąć należało, że pozwany miał prawo działać w zaufaniu do swego kontrahenta, który zapewnił ją o dopuszczalności użycia przedstawionej bazy adresowej do przesyłania wiadomości reklamowych. Już w momencie otrzymania pierwszego pisma od powoda, otrzymanie którego pozwany potwierdził, pozwany uzyskał wiadomość, że powód nie życzy sobie otrzymywania od niej korespondencji handlowej. Od tego momentu nie mógł się zatem pozwany powoływać na działanie w dobrej wierze i zaufaniu do kontrahenta, i to niezależnie od tego, na czyje zlecenie kieruje do pozwanego korespondencję. W konsekwencji wysyłanie przez pozwanego informacji handlowych po dacie otrzymania sprzeciwu powoda uznać należy za działanie zawinione. O winie pozwanego świadczy przy tym dodatkowo fakt, że jak wynika z treści odpowiedzi na pozew pozwany zaakceptował fakt zgłoszenia przez powoda sprzeciwu co do otrzymywania korespondencji od spółki z o.o. i usunął jego adres z listy adresów, na które przesyłana była korespondencja. Przesyłanie nie zamówionej korespondencji zostało jednak wznowione po otrzymaniu kolejnej bazy danych zawierającej adres powoda, co, zdaniem Sądu, świadczy co najmniej o niedbalstwie polegającym na nie sprawdzeniu otrzymanej bazy pod kątem tego, czy nie zawiera ona adresów osób, co do których pozwany wiedział, że nie życzą sobie otrzymywania korespondencji[366].

W wyroku wydanym po rozpoczęciu stosowania RODO Sąd wskazał, że przekazanie przez ubezpieczyciela dodatkowych danych powódki numeru (PESEL i numeru telefonu właściciela pojazdu) wykraczało poza upoważnienie ustawowe wynikające z przepisów: art. 29 ust. 6 ustawy z dnia 11.09.2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (tekst jedn.: Dz.U. z 2020 r., poz. 895) oraz art. 44 ust. 1 pkt 4 ustawy z dnia 22.06.1997 r. Prawo o ruchu drogowym (tekst jedn.: Dz.U. z 2020 r., poz. 110), a więc było bezprawne. Pozwanemu towarzystwu ubezpieczeń przypisać można było winę subiektywną w opisanym wyżej znaczeniu z uwagi na fakt, że regulacje prawne dotyczącej ochrony danych osobowych (ochrony dóbr osobistych) powinny być znane przedstawicielom pozwanego, dokonującym przekazania dokumentacji szkodowej poszkodowanemu w kolizji drogowej, skoro pozwany zajmuje się profesjonalnie działalnością w zakresie ubezpieczeń, obejmującą m.in. likwidację szkód[367].

[366] Wyrok SA w Warszawie – V Wydział Cywilny z 17.05.2017 r., sygn. akt VI ACa 223/16.
[367] Wyrok SO w Warszawie z 6.08.2020 r., sygn. akt XXV C 2596/19.

Okoliczności, za które dłużnik odpowiada na gruncie odpowiedzialności deliktowej

Prawo cywilne zna trzy podstawy odpowiedzialności z tytułu czynów niedozwolonych, a mianowicie zasady winy, zasadę ryzyka oraz odpowiedzialność opartą na zasadach współżycia społecznego, tradycyjnie zwaną zasadą słuszności. W ślad za wcześniej poczynionym omówieniem pojęcia winy, dla porządku w tym miejscu wskazać należy tylko, że nie zostało ono w Kodeksie cywilnym zdefiniowane. Tekst art. 415 k.c. powtarza dosłownie sformułowanie dawanego art. 134 k.z., który z kolei pozostawał pod wpływem formuły art. 1382 k.c. franc. Jeszcze w czasie debat nad projektem Kodeksu zobowiązań nie było bynajmniej oczywiste, czy w treści przepisu, wyrażającego generalną formułę deliktu nie powinna znaleźć się wyraźna wzmianka o bezprawności postępowania sprawcy. Prócz tego miało zostać wskazane, że czyn sprawcy powinien być subiektywnie negatywny. W ślad za prawem francuskim ograniczono się jednak jedynie do wskazania, że czyn sprawcy ma mieć znamiona „winy". Rozumiano tym samym, że ma być on obiektywnie i subiektywnie zasługujący na ujemną ocenę. Słowo „wina" obejmuje w tym przypadku oba aspekty. Nie budzi wątpliwości, że pojęcie winy uwzględnia dwa elementy składowe: obiektywny (bezprawność) i subiektywny (wadliwość zachowania się sprawcy, podmiotowa, subiektywna)[368].

Według zdecydowanie dominującego w polskiej cywilistyce poglądu art. 415 k.c. uzależnia odpowiedzialność za szkodę wyrządzoną przez czyn własny od bezprawności postępowania będącego źródłem szkody. Bezprawność, rozumiana w sposób przyjęty poniżej, stanowi również przesłankę odpowiedzialności na podstawie przepisu art. 430 i 429 k.c. oraz art. 427, 431 czy art. 72 k.c. W przeciwieństwie do art. 415 k.c., o powstaniu odpowiedzialności na podstawie art. 427 oraz 429 czy art. 430 k.c. decyduje, rzecz jasna, kwalifikacja (jako bezprawnego) postępowania nie osoby ponoszącej odpowiedzialność, ale osób trzecich, za które ona odpowiada[369]. Na gruncie RODO takie przypadki mogą dotyczyć relacji, w których przedsiębiorca występuje jako administrator lub podmiot przetwarzający, a zdarzenie szkodzące jest wynikiem działania pracownika, współpracownika lub dalszy podmiot przetwarzający. Nie wpływa to jednak na sposób rozumienia samego pojęcia bezprawności – nie zmienia się ono w porównaniu ze znaczeniem tego pojęcia przyjmowanym przy wykładni art. 415 k.c.

W nowszej literaturze zamiast o bezprawności pisze się raczej „o obiektywnej nieprawidłowości postępowania", z którego wynikła szkoda. Taka terminologia nie niesie ze sobą zmiany w sposobie rozumienia omawianej tutaj przesłanki odpowiedzialności.

[368] W. Czachórski, *Zobowiązania. Zarys wykładu*, Warszawa 1994, s. 189–191.
[369] R. Strugała, *Dobra i interesy chronione w strukturze czynu niedozwolonego*, Warszawa 2019.

Przeciwnie, jest ona wyrazem akceptacji dla znaczenia przypisywanego jej powszechnienie w doktrynie i orzecznictwie. Współcześnie bowiem słowo „bezprawność" w coraz mniejszym stopniu oddaje treść, jaką nadaje się temu terminowi w nauce i judykaturze. Treść ta ujmowana jest szeroko. Za bezprawne w rozumieniu art. 415 k.c. powszechnie uznaje się postępowanie odpowiedzialnego za szkodę zarówno wówczas, gdy jest ono sprzeczne z normami prawa stanowionego (nakazami i zakazami wynikającymi z przepisów różnych gałęzi prawa), jak również wtedy, gdy narusza ono normy moralne, nazywane zasadami współżycia społecznego czy dobrymi obyczajami[370].

Podstawowe znaczenie dla możności przypisania sprawcy szkody odpowiedzialności odszkodowawczej opartej na art. 415 k.c. ma zatem określenie zdarzenia, za które podmiotowi przypisywana jest odpowiedzialność (czyn sprawcy). Czynem tym może być działanie, jak i zaniechanie, a za bezprawne należy kwalifikować czyny zakazane przez przepisy prawne, bez względu na ich źródła, mające charakter abstrakcyjny, nakładające powszechny obowiązek określonego zachowania, a więc nakazując lub zakazując generalnie oznaczonym podmiotom określonych zachowań w określonych sytuacjach. Za bezprawne uznaje się także zachowania sprzeczne z zasadami współżycia społecznego albo dobrymi obyczajami, a więc sprzeczne z normami moralnymi powszechnie akceptowanymi w całym społeczeństwie lub grupie społecznej. Działanie (zaniechanie) sprawcy musi być przy tym zawinione. Przez winę rozumieć zaś należy możność postawienia danej osobie zarzutu, że nie zachowała się prawidłowo (tj. zgodnie z prawem i zasadami współżycia społecznego), chociaż mogła i powinna tak się zachować. Innymi słowy, że w konkretnej sytuacji dopuściła się ona nagannej decyzji odnoszącej się do podjętego przez niego bezprawnego czynu. Takie ujmowanie winy stanowi konsekwencję posługiwania się na gruncie prawa cywilnego kategoriami analogicznymi do pojęcia winy w prawie karnym, a jednocześnie dominacji koncepcji normatywnej winy[371].

Istota zasady ryzyka sprowadza się do nałożenia na dłużnika odpowiedzialności odszkodowawczej niezależnej od istnienia po jego stronie winy i bezprawności, co oznacza, że dowód braku winy nie zwalnia go z odpowiedzialności. Równocześnie drugą cechą odpowiedzialności na zasadzie ryzyka, jest jej wyłączenie w ustawowo wymienionych przypadkach, określanych mianem okoliczności egzoneracyjnych. Triada okoliczności

[370] R. Strugała, *Dobra i interesy...*

[371] B. Lewaszkiewicz-Petrykowska, *Wina jako podstawa...*, s. 88; Z. Radwański, *Zobowiązania...*, s. 198; W. Czachórski, *Zobowiązania...*, s. 204; Z. Banaszczyk [w:] *Kodeks cywilny*, t. 1, komentarz 2015 do artykułów 1-449, s. 1215.

wyłączających odpowiedzialność na podstawie art. 435 k.c. dotyczy przypadku powstania szkody wskutek siły wyższej albo wyłącznie z winy poszkodowanego lub osoby trzeciej, za którą nie ponosi odpowiedzialności. Odpowiedzialność na zasadzie ryzyka jest surowsza od odpowiedzialności na zasadzie winy w tym sensie, że surowsze są przesłanki tej odpowiedzialności. RODO nie odnosi się do zasad odpowiedzialności w omawianym rozumieniu.

Zasada słuszności wprowadza wyjątek od reguły ustanawiającej obowiązek naprawienia szkody wynikłej wyłącznie z bezprawnego postępowania sprawcy, ale jej brak zastosowania w zakresie odpowiedzialności z tytułu naruszenia przepisów o ochronie danych osobowych nie budzi w piśmiennictwie dyskusji w przeciwieństwie do tego, jakie rozbieżności stanowisk prezentowane są w stosunku do dwóch wcześniej omówionych zasad, o czym będzie mowa także w dalszej części pracy.

Związek przyczynowy

Problematyka związku przyczynowego nie została szczegółowo podjęta ani w art. 82 RODO, ani w preambule rozporządzenia. Konieczność istnienia takiego związku wynika jednak wprost z brzmienia art. 82 RODO. Tak jak już zostało podniesione wcześniej nie RODO nie wskazuje w żaden sposób, za jaką koncepcją przyczynowości opowiada się unijny legislator[372]. Należy więc sięgnąć do zasad ogólnych wynikających z Kodeksu cywilnego.

Odpowiedzialność za czyn własny noszący znamiona winy obciąża sprawcę, gdy między czynem tym a szkodą zostanie ustalony związek przyczynowy[373]. Związek przyczynowy, który zachodzi pomiędzy niewykonaniem lub nienależytym wykonaniem zobowiązania a szkodą jest także przesłanką odpowiedzialności kontraktowej.

Polska koncepcja związku przyczynowego jako przesłanki odpowiedzialności określonego podmiotu została szeroko przebadana w piśmiennictwie. Zauważalny jest tutaj wpływ tradycji prawa germańskiego. Jest bezsporne w doktrynie i judykaturze, że badanie kauzalne ma dwie fazy. W doktrynie eksponowana jest myśl, że test warunku koniecznego charakterystyczny dla teorii równowartości warunków pozwala stwierdzić, czy między zdarzeniem a szkodą zachodzi obiektywna zależność. W tym celu analizie poddawana jest indywidualna sytuacja, a więc przyczynowość określonego zdarzenia w odniesieniu do

[372] M. Jagielska, M. Jagielski, *W poszukiwaniu prawa...*, s. 57–58.
[373] W. Czachórski, *Zobowiązania...*, s. 189–191.

konkretnej szkody. W przypadku wystąpienia związku przyczynowego wieloczłonowego zależność przyczynowa musi zachodzić pomiędzy poszczególnymi ogniwami[374].

Przy rozważeniu związku przyczynowego należy pamiętać, że przyjmowana przez prawo teoria przyczynowości jest jednocześnie teorią odpowiedzialności, służącą temu celowi, aby określonej osobie przypisać oznaczoną szkodę. Sprawę tę trzeba mieć stale na uwadze, w szczególności zaś, wówczas, gdy rozgranicza się sfery odpowiedzialności różnych osób[375].

Związek przyczynowy jest niezbędną przesłanką odpowiedzialności cywilnej, a jednocześnie stanowi jej ustawowe ograniczenie. Zobowiązany nie odpowiada za wszystkie negatywne skutki swojego działania lub zaniechania, ale jedynie za normalne ich następstwa, a także za zdarzenia od woli ludzkiej niezależne, o ile ustawa łączy z nimi obowiązek odszkodowawczy (art. 361 § 1 k.c.) Określone następstwo ma zatem charakter normalny, gdy w danym układzie stosunków i warunków oraz w zwyczajnym biegu rzeczy, bez zaistnienia szczególnych okoliczności, szkoda jest zwykłym następstwem określonego zdarzenia[376]. W granicach zwykłego przebiegu zdarzeń odpowiedzialność za szkodę może powodować nie tylko przyczyna bezpośrednia, lecz także dalsza pośrednia, chyba że pozostaje w tak luźnym związku przyczynowym, iż jej uwzględnienie wykraczałoby poza normalną prawidłowość zjawisk, ocenianą według wskazanych uprzednio kryteriów doświadczenia życiowego i aktualnego stanu wiedzy[377]. Analogiczne twierdzenie jest zawarte np. w wyroku Sądu Apelacyjnego z 22.09.2005 r.[378]

Należy podzielić wyrażane wielokrotnie w orzecznictwie Sądu Najwyższego stanowisko, że na gruncie art. 361 § 1 k.c. obojętne jest, czy związek przyczynowy ma charakter bezpośredni, czy pośredni, oraz czy jest to związek przyczynowy złożony, wieloczłonowy, z tym że odpowiedzialność cywilną uzasadnia jedynie taki związek przyczynowy wieloczłonowy, w którym między poszczególnymi ogniwami zachodzi normalna zależność przyczynowa, a więc każde ogniwo tego związku podlega ocenie z perspektywy przyczynowości adekwatnej. Związek przyczynowy może zatem występować jako normalny również wtedy, gdy pewne zdarzenie stworzyło warunki do powstania innych zdarzeń, z których dopiero ostatnie stało się bezpośrednią przyczyną szkody. Koncepcja adekwatnego związku przyczynowego zakłada, że określona szkoda może być skutkiem wielu zdarzeń oraz

[374] E. Bagińska, *Odpowiedzialność deliktowa w razie niepewności związku przyczynowego. Studium prawnoporównawcze*, Gdańsk 2013, s. 38
[375] B. Lewaszkiewicz-Petrykowska, *Wina poszkodowanego…*
[376] Wyrok SN z 26.09.2006 r., sygn. akt II CK 372/05.
[377] Wyrok z 28.02.2006 r., sygn. akt III CSK 135/05.
[378] Wyrok SA z 22.09.2005 r., I ACa 197/05 wraz z aprobującą glosą M. Niedośpiał (OSA 2007, nr 3, poz. 88).

że normalne następstwa badanej przyczyny mogą być zarówno bezpośrednie, jak i pośrednie i pozostawać w relacjach wieloczłonowych, a w takiej sytuacji ocenie z perspektywy kryterium normalności podlega zależność wielu czynników kauzalnych w ich wzajemnych powiązaniach. Ustalenie zaś, że zachodzi normalny związek przyczynowy wymaga zbadania, czy gdyby dane zdarzenie nie wystąpiło, powstałby określony skutek (warunek *conditio sine qua non*), oraz czy pojawienie się przyczyny badanego rodzaju zwiększa prawdopodobieństwo wystąpienia rozpatrywanego skutku przez jej współistnienie i współdziałanie z innymi czynnikami. Jeżeli odpowiedź na te pytania okaże się twierdząca, będzie to równoznaczne z wystąpieniem normalnego związku przyczynowego. Dla oceny istnienia związku przyczynowego jako kategorii obiektywnej nie ma przy tym znaczenia, z jakich powodów osoba poszkodowana wskazała jako przyczynę szkody określone zdarzenie, a nie inne zdarzenie, które pozostawało w ciągu przyczyn lub stanowiło współprzyczynę szkody. Okoliczności te mogą być ewentualnie rozważane przy ocenie wysokości roszczenia odszkodowawczego na podstawie zasad ogólnych. Przy ustalaniu związku przyczynowego jako jednej z przesłanek odpowiedzialności odszkodowawczej decydujące znaczenie ma natomiast to, czy i jaką szkodę spowodowało bezprawne zdarzenie wskazane przez powoda jako podstawa faktyczna tego roszczenia. Zgodnie z utrwalonym w judykaturze poglądem przy ocenie, czy istnieje normalny związek przyczynowy między szkodą a zdarzeniem, które ją spowodowało, trzeba brać pod uwagę całokształt okoliczności sprawy, doświadczenie życiowe i zasady nauki. Zachodzi on wówczas, gdy w danym układzie stosunków i warunków oraz w zwyczajnym biegu rzeczy szkoda jest typowym następstwem danego zdarzenia[379].

Źródła stosunku prawnego na gruncie przepisów o ochronie danych osobowych

Dokonane powyżej wyszczególnienie przesłanek odpowiedzialności odszkodowawczej i okoliczności, za które w myśl ogólnych przepisów ustawy ponosi odpowiedzialność, pozwala wyznaczyć dalszy plan rozważań dotyczących zakresu odpowiedzialności przedsiębiorcy uczestniczącego w systemie ochrony danych osobowych w różnych wariantach podmiotowych, który jest ściśle powiązany z zakresem obowiązków nałożonych na te podmioty. W tym celu w pierwszej kolejności konieczne jest dokonanie analizy źródeł obowiązku odszkodowawczego na gruncie przepisów o ochronie danych osobowych.

[379] Wyrok SN z 10.04.2000 r., sygn. akt V CKN 28/00, LEX nr 52426; wyrok SA w Poznaniu z 20.03.2013 r., sygn. akt I ACa 122/13.

Analiza obowiązku odszkodowawczego i zależności pomiędzy uczestnikami systemu ochrony danych osobowych wyznaczonych przez normy prawne, nie będzie możliwa bez omówienia zagadnienia dotyczącego tego jakie w polskim porządku prawnym miejsce zajmują regulacje RODO i dyrektywy 95/46/WE.

RODO oraz dyrektywa 95/46/WE stanowią źródła prawa wtórnego Unii Europejskiej (klasyfikowane, gwoli ścisłości, odpowiednio jako rozporządzenie unijne i dyrektywa unijna) i są one jednocześnie uznawane za część porządku prawnego poszczególnych państw członkowskich Unii Europejskiej (w tym polskiego porządku prawnego). Warto zwrócić uwagę, że miejsce prawa wtórnego Unii Europejskiej w polskim porządku prawnym wyznacza art. 91 ust. 3 Konstytucji RP.

Mając na względzie wskazany przepis, należy uznać, że zarówno RODO (jako rozporządzenie unijne), jak i dyrektywa 95/46/WE (jako dyrektywa unijna) stanowią – z perspektywy polskiego porządku prawnego – takie źródła prawa powszechnie obowiązującego, które mają szczególną rangę w hierarchii źródeł prawa i pierwszeństwo w przypadku kolizji z ustawami. Co przy tym istotne, RODO – tak jak i wszystkie inne rozporządzenia unijne – dla swojej skuteczności nie wymaga uchwalenia żadnej ustawy implementującej i może być w pełnym zakresie bezpośrednio stosowane. Dyrektywy unijne z kolei (również dyrektywa 95/46/WE) wymagają z założenia uchwalenia odpowiednich ustaw implementujących, odzwierciedlających ogólny standard regulacji w nich zawarty[380]. Dla porządku przypomnienia wymaga, że po akcesji Polski do Unii Europejskiej regulacją prawa krajowego – współistniejącą w polskim porządku prawnym z przepisami dyrektywy 95/46/WE i odzwierciedlającą standardy w niej zawarte – stała się ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych.

Stosownie do art. 288 TFUE rozporządzenie ma zasięg ogólny, wiąże w całości, co do wszystkich zawartych w nim postanowień, i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Ze swej natury staje się ono częścią krajowych systemów prawnych bez potrzeby dokonywania jakichkolwiek czynności transpozycyjnych i wywiera skutki bezpośrednie w stosunku do jednostek. Rozporządzenia obejmują wertykalny i horyzontalny skutek bez wyjątku. Również taki charakter ma ogólne rozporządzenie o ochronie danych, które uchyliło dyrektywę 95/46/WE, przejmując jego rolę aktu harmonizującego prawo ochrony danych osobowych w państwach członkowskich. Z punktu widzenia ogólnego rozporządzenia zakazane stanie się stosowanie rozwiązań nieprzewidzianych w rozporządzeniu i

[380] M. Pisz, *Konstytucyjne i ustawowe uwarunkowania ochrony danych osobowych w polskim porządku prawnym* [w:] *RODO. Przewodnik dla adwokatów i aplikantów adwokackich*, red. A. Mednis, Warszawa 2018.

niepozostawionych w nim wyraźnie do uregulowania w prawie krajowym. Jednak ogólne rozporządzenie o ochronie danych nie wprowadza pełnej harmonizacji, rozumianej jako pełne (zupełne) ukształtowanie regulacji danego obszaru przedmiotowego, bez dopuszczalności stosowania regulacji krajowych. Przeciwieństwem harmonizacji pełnej jest harmonizacja częściowa, w której pozostawia się państwom członkowskim większą lub mniejszą aktywność w danej dziedzinie po wejściu w życie aktu harmonizującego. W ramach takiej harmonizacji częściowej, której przykładem jest ogólne rozporządzenie o ochronie danych, w enumeratywnie określonych sytuacjach pozostawia się państwu możliwość wyboru kierowania się w ustalonych kwestiach przedmiotowych regulacjami unijnymi lub regulacjami krajowymi (harmonizacja fakultatywna) [381]. Są nimi na przykład:

- delegacja zawarta w art. 6 ust. 2 i 3 RODO, która pozwala na zachowanie lub wydanie bardziej szczegółowych przepisów prawa krajowego, gdy przetwarzanie ma być oparte na przesłance niezbędności do wypełnienia obowiązku prawnego ciążącego na administratorze lub przesłance niezbędności do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- delegacja zawarta w art. 23 RODO, która pozwala na ograniczanie zakresu niektórych obowiązków i praw wynikających z RODO w przypadku, gdy ograniczenie takie służy ważnym celom leżącym w ogólnym interesie publicznym;
- delegacja zawarta w art. 88, który upoważnia państwa członkowskie do objęcia szczególną, doprecyzowującą RODO regulacją stosunków pracy w celu zapewnienia ochrony praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem;
- delegacja zawarta w art. 85 dotyczącym możliwości wydania przepisów krajowych pozwalających pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji;
- delegacja zawarta w art. 8 ust. 1 poświęconemu warunkom wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego przewidującego „widełki, w ramach których państwa członkowskie mogą określić wiek dziecka, do którego odnosi się wskazana regulacja ochronna (13—16 lat);

[381] G. Sibiga, *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia*, MoP 2016/20.

- delegacja zawarta w art. 9 ust. 4, który pozwala państwom członkowskim na podniesienie poziomu ochrony w przypadku danych genetycznych, biometrycznych i dotyczących zdrowia[382].

Nawet w sytuacji wyboru przez państwo opcji wprowadzenia przepisów krajowych akt harmonizujący może ingerować w kształt tych przepisów. Akt harmonizujący może bowiem ustanawiać wymogi wobec regulacji prawnej państwa członkowskiego. Co ważne, w przypadku ogólnego rozporządzenia przewidziano również możliwość włączenia elementów rozporządzenia do przepisów krajowych, jeżeli będzie to niezbędne dla zachowania spójności i zrozumiałości przepisów dla osób, do których mają zastosowanie. Nawet w kwestii podlegającej harmonizacji w drodze rozporządzenia może dojść do nałożenia obowiązku na państwo członkowskie określenia w prawie krajowym sposobu i formy realizacji wymagań z rozporządzenia. Jednocześnie w prawie krajowym mogą występować przepisy, które ze względu na hierarchiczną budowę źródeł prawa w tym państwie, będą obowiązywać równolegle do regulacji unijnych. W polskim prawodawstwie problem ten dotyczy przepisów Konstytucji RP zawierających gwarancje ochrony danych osobowych[383].

Istotne w kontekście powyższych rozważań jest stanowisko doktryny stwierdzające, że fakt wejścia w życie i stosowania RODO powoduje, że niknie nie tylko potrzeba tworzenia norm prawa krajowego regulujących objętą nim problematykę, ale pojawia się zakaz stosowania rozwiązań sprzecznych z rozporządzeniem[384]. Powyższe nie wyeliminuje jednak wszystkich różnic, mogących w pewnym zakresie ograniczyć prowadzoną współpracę. Przykładem może być tutaj art. 61 ust. 7 RODO zgodnie z którym organy nadzorcze mogą uzgodnić zasady dokonywania wzajemnego zwrotu konkretnych wydatków poniesionych w wyniku świadczonej wzajemnej pomocy w wyjątkowych okolicznościach[385].

W rozważaniach dotyczących źródeł stosunku prawnego, wynikającego z przepisów o ochronie danych osobowych nie sposób pominąć przepisów dotyczących aktów prawa pochodnego UE przyjmowanych przez instytucje i organy UE, wśród których podstawowym przepisem traktatowym jest art. 288 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Oprócz wiążących prawnie rozporządzeń, dyrektyw i decyzji, w przepisie tym wymienia się jako akty prawa pochodnego również zalecenia i opinie, przy czym – zgodnie z art. 288 ust. 5

[382] M. Jagielska, M. Jagielski, *W poszukiwaniu prawa...*, s. 56
[383] G. Sibiga, *Dopuszczalny zakres...*
[384] M. Kawecki, *The proccessing of personal data by law offices after the new EU regulation on the protection of personal data has become effectice*, „Przegląd Prawno-Ekonomiczny" 2013/23 s. 13.
[385] M. Kawecki, *Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Warszawa 2017, s. 258

TFUE – w sposób wyraźny stwierdza się, że nie mają one charakteru wiążącego. W art. 288 TFUE nie ujęto jednak całej grupy tzw. aktów nienazwanych, które, z jednej strony, łączy to, że są aktami formalnie niewiążącymi, ale z drugiej – są instrumentami tzw. harmonizacji miękkiej, ponieważ wskazują one pewien kierunek zarówno dla prawodawcy unijnego, jak i krajowego, a także dla podmiotów stosujących prawo. Wszystkie te akty (czyli zalecenia i opinie oraz inne akty nienazwane) zbiorczo można określić jako *soft law* (tzw. miękkie prawo), które to pojęcie nie jest zdefiniowane w systemie ustrojowym UE, chociaż pojawia się w dokumentach unijnych.

Trzeba przy tym zauważyć, że art. 288 TFUE nie definiuje pojęcia zalecenia i opinii w sposób, w jaki czyni to w odniesieniu do dyrektyw i rozporządzeń, ale wymienia pewną istotną cechę łączącą te dwa dokumenty, czyli brak mocy wiążącej prawnie. Nie są to jednak pojęcia, które mogą być używane zamiennie, bowiem w istocie akty te powinny pełnić nieco inne zadania. Katalog aktów typu soft law jest otwarty, przy czym do nazw aktów nie należy przywiązywać szczególnej wagi, bowiem same nazwy bywają stosowane zamiennie, a niektóre mogą być wręcz mylne. *Soft law* nie jest wynalazkiem systemu prawnego UE. Jest mocno zakorzenione we współpracy międzynarodowej, w prawie międzynarodowym publicznym – tam celem tego typu aktów jest zachęcenie określonych podmiotów do konkretnego postępowania, bez wywoływania wiążących skutków prawnych, co bywa naturalnie krytykowane w doktrynie. W prawie UE obecnie tego typu akty mogą być przyjmowane w każdej dziedzinie, niekiedy służąc obejściu formalnych procedur, gdy brak jest konsensusu czy kompetencji w danym obszarze. Chociaż proces przyjmowania tych aktów bywa nieprzejrzysty, to naturalnie w ostatnich latach liczba przyjmowanych aktów tego rodzaju również w UE znacząco wzrosła, czego przyczyn upatruje się w kilku czynnikach. Jednym z nich jest to, że określanie pewnych niewiążących reguł postępowania czy wytycznych interpretacyjnych w tej formie dużo słabiej ingeruje w porządki prawne państw członkowskich, co ma znaczenie również ze względu na treść art. 296 ak. 1 TFUE[386].

W dotychczasowej swej działalności Europejska Rada Ochrony Danych, realizując swe podstawowe zadanie związane z zapewnieniem spójnego stosowania RODO (art. 70 ust. 1 *ab initio)*, wydawała w głównej mierze wytyczne (ang. *guidelines)*. Dopiero w przypadku dokumentu precyzującego wymogi wynikające z wyroku TSUE w sprawie *Schrems II* doszło do wydania zaleceń (ang. *recommendations)*. Znajduje to swe oparcie (podobnie zresztą jak w przypadku wydawanych przez Radę wytycznych) w art. 70 ust. 1 lit. e) RODO. Zgodnie z tym

[386] A. Grzelak, *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych*, MoP 2021/23.

przepisem EROD „z własnej inicjatywy lub na wniosek jednego ze swoich członków lub Komisji bada wszelkie kwestie dotyczące stosowania RODO i wydaje wytyczne, zalecenia oraz określa najlepsze praktyki, by zachęcić do spójnego stosowania RODO. Przepisy RODO, ale również m.in. regulamin wewnętrzny Rady, nie dają jednoznacznej odpowiedzi na pytanie o różnice, jakie występują pomiędzy wytycznymi a zaleceniami. Wydaje się jednak, że biorąc pod uwagę w szczególności brzmienie art. 288 TFUE oraz dostępną w tym zakresie literaturę, należy zalecenia EROD traktować jako akty prawnie niewiążące.

Zalecenia są adresowane do podmiotów zewnętrznych w stosunku do instytucji unijnych, przy czym podmiotami tymi mogą być zarówno państwa członkowskie (w tym przypadku przypominają one swym charakterem niewiążące dyrektywy), jak również podmioty prywatne (w tym przypadku – jak ma to miejsce w odniesieniu do zaleceń EROD – przypominają one swym charakterem wytyczne lub inne dokumenty dające się pomieścić w grupie aktów prawa miękkiego, *soft law)*. Zresztą zalecenia wydawane przez inne niż EROD instytucje unijne tytułowane są w praktyce w różny sposób, w tym np. jako „wytyczne" lub „standardy dobrych praktyk". Wskazuje to na zbliżony pod względem prawnym charakter zaleceń oraz wytycznych EROD. Odnosząc się do znaczenia słownikowego, przez „zalecenie" („zalecenia") rozumieć należy polecenie, wskazanie, rekomendowanie, doradzanie pewnego postępowania jako korzystnego dla określonego podmiotu lub oczekiwanego od niego. Co ciekawe, Prezes Urzędu Ochrony Danych Osobowych posługuje się w kontekście zaleceń wydawanych przez EROD terminem „wskazówki", które odpowiada słownikowemu znaczeniu tego pojęcia.

Wydanie przez EROD zaleceń – biorąc pod uwagę jej podstawowe zadania – będzie zatem służyło doprecyzowaniu zakresu obowiązywania lub sposobu stosowania aktu prawnie wiążącego Unii, tj. ogólnego rozporządzenia o ochronie danych. Pomimo też braku wiążącego charakteru, zalecenia (oraz wytyczne) EROD mają istotny wpływ na praktykę. Pozwalają one bowiem administratorom danych oraz podmiotom przetwarzającym przewidzieć, w jaki sposób właściwe organy nadzorcze wchodzące w skład EROD będą postępować w przyszłości, interpretując i egzekwując stosowanie RODO. Pod względem funkcjonalnym można tym samym traktować zalecenia EROD jako swoiste źródło prawa, wpływające na zachowania organów nadzorczych oraz adresatów tychże zaleceń, tj. administratorów oraz podmioty przetwarzające. W razie zaś braku zastosowania się do nich – mogące skutkować negatywnymi konsekwencjami dla tych adresatów, chyba że mogą oni zrealizować obowiązki wynikające z

przepisów RODO w inny sposób niż wynikający z zaleceń, pozostający jednak w zgodności z tymi przepisami[387].

Prawna regulacja ochrony danych osobowych w Unii Europejskiej nie ogranicza się jedynie do przepisów RODO oraz krajowych ustaw uzupełniających RODO, ale obejmuje również inne akty normatywne, z których część stanowią akty delegowane i decyzje wykonawcze. Uchwalenie rozporządzeń i dyrektyw unijnych jest zadaniem Parlamentu Europejskiego i Rady, natomiast wydawanie aktów normatywnych „niższego rzędu" stanowi zasadnie Komisji Europejskiej. Uzupełnieniem regulacji prawnych są różnego rodzaju dokumenty (opinie, zalecenia, wytyczne) tworzone przez inne organy, w tym EROD, Europejskiego Inspektora Ochrony Danych Osobowych oraz krajowe organy nadzorcze[388].

Analizując zagadnienie źródeł prawa w ochronie danych osobowych, nie sposób pominąć instytucji kodeksów postępowania. Jest to dobrowolne narzędzie, przewidziane przez RODO, uszczegóławiające stosowanie przepisów o ochronie danych osobowych przez administratorów i podmioty przetwarzające z konkretnego sektora. Mogą być one wręcz pewnego rodzaju szczegółową instrukcją, zbiorem zasad, które sprawią, że administrator przystępujący do takiej inicjatywy i stosujący się do postanowień takiego dokumentu będzie miał większą pewność działania zgodnie z RODO. Kodeksy mają bowiem uszczegóławiać wiele kwestii i podpowiadać administratorom m.in.: jak mają postępować przy zbieraniu danych, jak podchodzić do realizacji obowiązków informacyjnych i praw osób, których dane przetwarzają, czy jakie środki techniczne i organizacyjne powinny w ich branży zastosowane, by zapewnić odpowiedni poziom ochrony danych.

Z inicjatywą opracowania kodeksu i przedłożenia go Prezesowi Urzędu Ochrony Danych Osobowych w celu jego zatwierdzenia mogą wystąpić zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające. Do wniosku dołącza się informację o przeprowadzonych konsultacjach oraz ich wyniku. UODO dokonuje oceny przedstawionego projektu. Podczas tej oceny może się on kontaktować z przedstawicielami organizacji, które przygotowały projekt kodeksu postępowania, w celu uzyskania wyjaśnień czy dodatkowych odpowiedzi[389]. Charakter takich kodeksów dobrych praktyk jest rozpracowany choćby na przykładzie reguł obowiązujących na giełdach papierów wartościowych

[387] D. Karwala, *Znaczenie soft law dla transferów danych osobowych do państw trzecich na przykładzie zaleceń EROD*, MoP 2020/01.
[388] P. Fajgielski, *Rola Europejskiego Inspektora Ochrony Danych w kształtowaniu i wykładni przepisów o ochronie danych osobowych*, MoP 2021/23.
[389] Zob. https://uodo.gov.pl/pl/138/1858

W chwili obecnej dwa kodeksy postępowania zostały pozytywnie zaopiniowane przez UODO w branży medycznej, a jeden z nich został przez UODO zaakceptowany. Z punktu widzenia zagadnień omawianych w przedmiotowej pracy istotne są ich postanowienia doprecyzowujące obowiązki administratora dotyczące np.:

- zasady minimalizacji danych o treści „przetwarzane przez PWDL dane osobowe Pacjenta muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów w jakich są przetwarzane PWDL, przetwarzając dane osobowe w celach zdrowotnych, może potencjalnie przetwarzać zakres danych osobowych wykraczający poza minimalny zakres danych obowiązkowo zawartych w Dokumentacji medycznej zgodnie z przepisami prawa polskiego. Co do zasady gromadzenie danych obejmujących adres e-mail lub numer telefonu jest adekwatne do celów zdrowotnych, mimo że nie są to dane minimalne, wymagane przez przepisy prawa;
- zakresu stosowania środków organizacyjnych w ramach procedury weryfikacji tożsamości o treści: „Weryfikacji tożsamości Pacjenta dokonuje się poprzez kontrolę okazanego przez Pacjenta dokumentu potwierdzającego tożsamość zawierającego co najmniej zdjęcie, imię i nazwisko oraz PESEL lub w przypadku jego braku inny numer jednoznacznie identyfikujący Pacjenta. Dokumentem potwierdzającym tożsamość jest w szczególności: dowód osobisty, legitymacja studencka, legitymacja szkolna, prawo jazdy, paszport lub inny dokument urzędowy ze zdjęciem. PWDL może utrwalić informację o: dacie dokonania weryfikacji tożsamości oraz rodzaju dokumentu, na podstawie którego została ona dokonana w przypadku, gdy w PWDL jest więcej osób o tym samym imieniu i nazwisku – numerze PESEL osoby okazującej dowód tożsamości, jeżeli został nadany, a w przypadku osób, które nie mają nadanego numeru PESEL - rodzaju i numerze dokumentu potwierdzającego tożsamość.

Kodeksy postepowania powstają także na poziomie europejskim[390]. Z perspektywy zagadnień omawianych w pracy istotne jest to, że naruszenie zasad kodeksu postepowania, będzie mogło być kwalifikowane jako działanie bezprawne.

Związanie Sądu decyzjami Prezesa UODO

Dla rozważanych problemów odpowiedzialności w szczególności okoliczności, dotyczących stwierdzenia ewentualnej bezprawności fundamentalne znaczenie ma instytucja związania sądu decyzjami Prezesa UODO wynikająca z art. 94 ustawy o ochronie danych

[390] Zob. dpb.europa.eu/our-work-tools/accountability-tools/register-codes-conduct-amendments-and-extensions-art-4011_pl

osobowych. Zgodnie z tym przepisem o wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, o którym mowa w art. 79 lub art. 82 rozporządzenia 2016/679, sąd zawiadamia niezwłocznie Prezesa Urzędu. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych, która toczy się przed Prezesem Urzędu lub sądem administracyjnym albo została zakończona. Prezes Urzędu niezwłocznie informuje sąd również o wszczęciu każdego postępowania w sprawie dotyczącej tego samego naruszenia.

Jak stwierdził ustawodawca w uzasadnieniu projektu ustawy o ochronie danych osobowych, „[c]elem wprowadzenia przedmiotowych regulacji do projektu jest udrożnienie i przyspieszenie komunikacji pomiędzy sądami powszechnymi a Prezesem Urzędu. Należy zwrócić uwagę, iż wniesienie pozwu w sprawach, o których mowa w projekcie, obliguje sąd – przed którym toczy się postępowanie – do zawiadomienia Prezesa Urzędu. W ocenie projektodawcy ważnym do wskazania jest również, że wprowadzenie do projektu wskazanych regulacji nie ma wpływu na toczące się obecnie postępowania”[391].

Zgodnie z art. 97 ustawy o ochronie danych osobowych ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów.

Omówione wyżej regulacje wprowadzają zasadę związania sądu w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych (na podstawie art. 79 RODO, na podstawie przepisów dotyczących ochrony dóbr osobistych, lub na podstawie art. 82 RODO jako samodzielnej podstawy prawnej) ustaleniami prawomocnej decyzji PUODO o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku (wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 cyt. ustawy) co do stwierdzenia naruszenia tych przepisów. Zasada ukształtowana w tym przepisie ogranicza się do faktu zaistnienia naruszenia przepisów o ochronie danych osobowych i rodzaju naruszenia. Innymi słowy, sąd powszechny będzie

[391] Uzasadnienie projektu UODO, Druk sejmowy VIII kadencji Nr 2410, s. 41; P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Legalis, https://sip-1legalis-1pl-1v27i8rcf0b57.han3.lib.uni.lodz.pl/document-view.seam?documentId=mjxw62zogi3damrqgm4dgnboobqxalrugmydknbzge4a&refSource=toc#tabs-metrical-info

związany tylko takimi ustaleniami zawartymi w prawomocnej decyzji PUODO, które stwierdzają naruszenie przepisów o ochronie danych osobowych o ochronie danych osobowych (nie będzie mógł samodzielnie badać tego zagadnienia). Natomiast w sytuacji, gdy w decyzji lub wyroku sądu administracyjnego zostanie ustalone, że nie doszło do naruszenia przepisów o ochronie danych osobowych, to tego rodzaju ustalenia nie będą dla sądu powszechnego wiążące[392]. W literaturze wskazuje się również, że „związanie sądu cywilnego dotyczy wszystkich szczebli sądownictwa cywilnego – sądów powszechnych (SO – zgodnie z art. 93 ustawy o ochronie danych osobowych), ale też SN”[393]. Wypada również zauważyć, że przepis art. 97 UODO jest podobny w brzmieniu do art. 11 KPC, który stanowi, że "[u]stalenia wydanego w postępowaniu karnym prawomocnego wyroku skazującego co do popełnienia przestępstwa wiążą sąd w postępowaniu cywilnym". Analogicznie jak w przypadku art. 11 KPC należy przyjąć, że zakres związania prawomocnych wyroków skazujących (tu: prawomocnych decyzji o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnych orzeczeń sądu administracyjnego) dotyczy ustaleń co do okoliczności popełnienia przestępstwa (tu: okoliczności naruszenia ochrony danych osobowych) zawartych w sentencji wyroku (wyr. SN z 2.2.2012 r., II CSK 330/11, Legalis)[394].

Związanie sądu powszechnego decyzją Prezesa Urzędu Ochrony Danych Osobowych o stwierdzeniu naruszenia przepisów o ochronie danych osobowych budzi uzasadnione wątpliwości co do zgodności z konstytucyjnym prawem podmiotowym do sądu. W piśmiennictwie podnoszone jest, że gdy mamy do czynienia z potencjalną hierarchiczną niezgodnością norm prawnych (norma ustawowa ingeruje w treść konstytucyjnej) należy przeprowadzić test proporcjonalności zgodnie z art. 31 ust. 3 Konstytucji RP i ocenić, czy ograniczenie prawa do niezawisłego sądu oraz sprawiedliwego rozpatrzenia sprawy przez mechanizm określony w art. 97 UODO jest proporcjonalne dla realizacji interesu publicznego tj. zasady pewności i jednolitości stosowania prawa. Odnosząc się do kolejnych elementów testu proporcjonalności zgodnie z art. 31 ust. 3 Konstytucji RP, należy stanąć na stanowisku, że art. 97 UODO:

1. zachowuje ustawową formę ograniczenia;

[392] M. Szwast, *Związanie sądu powszechnego decyzją Prezesa Urzędu Ochrony Danych Osobowych o stwierdzeniu naruszenia przepisów o ochronie danych osobowych* [w:] *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2019*, red. G. Sibiga, MoP, 2019/22, s. 81.
[393] B. Gubernat, S. Szczepaniak [w:] *Ustawa o ochronie danych osobowych*, red. M. Kawecki, M. Czerniawski, s. 282, Warszawa 2019.
[394] P. Litwiński, *Ustawa o ochronie danych osobowych, Komentarz*, Warszawa 2016.

2. nie narusza istoty prawa do sądu, albowiem nie wyklucza całkowicie możliwości obrony pozwanego w postępowaniu o naprawienie szkody i zadośćuczynienie krzywdy;
3. został wprowadzony dla realizacji interesu publicznego tj. zasady pewności i jednolitości stosowania prawa, który mieści się w zakresie przesłanki „porządku publicznego" wymienionej w art. 31 ust. 3 Konstytucji RP;
4. jest przydatny dla realizacji celów zakładanych przez ustawodawcę mających umocowanie konstytucyjne albowiem uniemożliwia funkcjonowanie w obrocie prawnym dwóch rozstrzygnięć w różny sposób kwalifikujących naruszenie przepisów o ochronie danych osobowych;
5. jest konieczny albowiem cel tego przepisu nie jest możliwy do osiągnięcia przy zastosowaniu innego środka, nakładającego mniejsze ograniczenia na prawa i wolności jednostki.

Natomiast na ostatnim – szóstym – etapie badania proporcjonalności regulacji ograniczającej prawa i wolności konstytucyjne ocenia się, czy uszczerbek dla tych praw i wolności, jaki wiąże się z badanym ograniczeniem, został odpowiednio wyważony z efektami wprowadzonej regulacji (tzw. proporcjonalność *sensu stricto*). Kryterium to zakłada, że ograniczenia konstytucyjnych praw podmiotowych nie mogą w sposób nieadekwatny nakładać ciężarów na podmioty praw i wolności.

Jak wskazuje Trybunał Konstytucyjny[395] – ograniczenia te powinny „pozostawać w bezpośrednim związku i odpowiedniej proporcji do nałożonych ciężarów". W konsekwencji art. 97 UODO nie spełnia tego ostatniego kryterium testu proporcjonalności. Tę konkretną kolizję norm: prawa do sprawiedliwego rozpatrzenia sprawy przez niezawisły sąd z zasadą pewności i jednolitości stosowania prawa należy rozstrzygnąć na korzyść tych pierwszych norm konstytucyjnych. Wynika to w pierwszej kolejności z okoliczności, że nieproporcjonalne jest związanie niezawisłego sądu powszechnego ustaleniami decyzji PUODO, który nie jest organem mającym charakter w pełni niezależny, co wykazano wyżej. W tej sytuacji ustawodawca wyłącza istotę sprawowania władzy sądzenia i minimum samodzielności jurysdykcyjnej sądu na rzecz rozstrzygnięcia organu administracji publicznej. Zakłada też z góry, że pozwany administrator danych osobowych albo podmiot przetwarzający nie mogą się bronić w postępowaniu cywilnym przed powództwem osoby, której dane osobowe naruszono w zakresie naruszenia przez siebie przepisów o ochronie tych danych. Argument o zapewnieniu przez art. 97 UODO zasady jednolitości stosowania prawa i pewności prawa jest ważny,

[395] Wyroki TK: z 22.10.2013 r., SK 14/11; z 3.5.2002 r., SK 32/01; z 11.6.2002 r., SK 5/02.

niemniej w prawie polskim występuje szereg rozwiązań, które dopuszczają różną ocenę tego samego stanu faktycznego z punktu widzenia norm prawnych przez różne ośrodki orzekania[396].

Wyrażane są opinie, że nasze krajowe regulacje naruszają konstytucyjne prawo do niezawisłego sądu. Jeśli bowiem prezes UODO zajmie się sprawą dotyczącą tego samego naruszenia, to sąd musi zawiesić postępowanie. Ustalenia dokonane przez prezesa UODO w prawomocnej decyzji są wiążące dla sądu co do stwierdzenia naruszenia przepisów. RODO dało nam więc nowe prawne narzędzia, Celem polskiego rozwiązania było zapewnienie jednolitego merytorycznie orzecznictwa w sprawach ochrony danych osobowych. Należy jednak uznać, że to niewystarczający argument, aby pozbawiać sądy możliwości szybkiego oraz w pełni samodzielnego i niezależnego orzekania w tych sprawach[397].

Zagadnienie związania sądu budzi problemy interpretacyjne także w innych państwach członkowskich, o czym świadczy pytanie prejudycjalne węgierskiego sądu z 20.08.2021 r. zawisłe za sygn. akt C-132/21 przed Trybunałem Sprawiedliwości Unii Europejskiej. W tej sprawie Sąd powziął wątpliwość co do tego, czy dopuszczalne jest równoległe rozpatrywanie przez różne sądy środków prawnych dotyczących tego samego naruszenia zasad przetwarzania danych osobowych. Równoległe wykonywanie środków ochrony prawnej może bowiem prowadzić do wydania sprzecznych ze sobą decyzji dotyczących identycznych okoliczności faktycznych. Wątpliwości Sądu były wynikiem okoliczności związanych ze skierowaniem przez podmiot danych wniosków, tj. wniosku o udostępnienie danych do administratora, a następnie wniosku do organu nadzorczego o stwierdzenie, że nie realizując wniosku, zgodnie z oczekiwaniami podmiotu danych administrator działał niezgodnie z prawem, czego skutkiem powinno być nakazanie wykonania wniosku zgodnie z żądaniem podmiotu danych. Sąd ten zwrócił się zatem do TSUE z pytaniami prejudycjalnymi, zmierzającymi do potwierdzenia wykładni, zgodnie z którą w przypadku, gdy w odniesieniu do tego samego naruszenia organ nadzorczy prowadzi lub przeprowadził postępowanie, decyzja tego organu w tej sprawie, a także rozstrzygnięcie sprawującego nad nim kontrolę sądu administracyjnego, posiadają pierwszeństwo w ustaleniu zaistnienia naruszenia i że w tych postępowaniach administracyjnych i sądowo-administracyjnych rozstrzygnięcia sądów cywilnych zapadłe na podstawie art. 79 rozporządzenia 2016/679 nie są wiążące.

W pytaniach Sąd stwierdził, że do rozstrzygnięcia niniejszego sporu konieczne jest w odniesieniu do stwierdzenia istnienia naruszenia dokonanie rozgraniczenia kompetencji organu nadzorczego, sądu administracyjnego, który kontroluje decyzję tego organu, i sądu cywilnego

[396] M. Szwast, *Związanie sądu...*
[397] Zob. https://prawo.gazetaprawna.pl/artykuly/1485435,baza-pesel-poczta-polska-postepowanie-uodo.html

działającego na podstawie art. 79 rozporządzenia 2016/679. W tym celu należy mieć na uwadze, że jeśli pierwszeństwo nie zostanie przyznane organowi nadzorczemu, sąd odsyłający, przestrzegając zasadę pewności prawa, będzie musiał uznać za wiążące rozstrzygnięcie sądu cywilnego zawarte w prawomocnym wyroku i nie będzie mógł dokonać własnej oceny zgodności z prawem decyzji administracyjnej co do istnienia naruszenia, co w praktyce oznaczałoby pozbawienie treści kompetencji przyznanej w art. 78 rozporządzenia 2016/679.[398]

W wyroku z 12.01.2023 r. wydanym w tej sprawie TSUE przypomniał kluczowe regulacje zawarte w art. 77, 78 i 79 rozporządzenia 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Zgodnie z art. 77 bez uszczerbku dla innych środków administracyjnych lub środków ochrony prawnej przed sądem każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza niniejsze rozporządzenie. W myśl art. 78 bez uszczerbku dla innych administracyjnych lub pozasądowych środków ochrony prawnej każda osoba fizyczna lub prawna ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej. Natomiast stosownie do art. 79 bez uszczerbku dla dostępnych administracyjnych lub pozasądowych środków ochrony prawnej, w tym prawa do wniesienia skargi do organu nadzorczego zgodnie z art. 77, każda osoba, której dane dotyczą, ma prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna ona, że prawa przysługujące jej na mocy niniejszego rozporządzenia zostały naruszone w wyniku przetwarzania jej danych osobowych z naruszeniem niniejszego rozporządzenia.

TSUE uznał, że przepisy rozporządzenia 2016/679 oferują różne środki ochrony prawnej osobom powołującym się na naruszenie przepisów tego rozporządzenia, przy czym każdy z tych środków odwoławczych powinien być dostępny „bez uszczerbku" dla pozostałych. Rozporządzenie 2016/679 nie przewiduje pierwszeństwa lub wyłączności ani żadnej zasady nadrzędności oceny dokonanej przez organ lub sądy w odniesieniu do istnienia naruszenia praw przyznanych przez to rozporządzenie. Zapewnienie wielości środków odwoławczych wzmacnia cel rozporządzenia polegający na zagwarantowaniu każdej zainteresowanej osobie, która uzna, że jej prawa wynikające z tego rozporządzenia zostały

[398] Oznaczenie sądu odsyłającego: Fővárosi Törvényszék (sąd dla miasta stołecznego Budapeszt, Węgry)
Data wydania postanowienia o wystąpieniu z wnioskiem o wydanie orzeczenia w trybie prejudycjalnym: 2.03.2021 r. Strona skarżąca: BE Druga strona postępowania: Nemzeti Adatvédelmi és Információszabadság Hatóság (krajowy organ ochrony danych i wolności informacji, Węgry) Fővárosi Törvényszék (sąd dla miasta stołecznego Budapeszt, Węgry).

naruszone, prawa do skutecznego środka prawnego przed sądem.[399] To oznacza, że żaden z nich nie ma pierwszeństwa i to państwo członkowskie musi zapewnić spójność ich stosowania.

W prawie węgierskim system środków ochrony prawnej został skonstruowany w taki sposób, że środki ochrony prawnej przewidziane w art. 78 ust. 1 i art. 79 ust. 1 rozporządzenia są od siebie niezależne. Nie można zatem wykluczyć, że orzeczenia wydane przez te dwa sądy będą ze sobą sprzeczne, jedno stwierdzające naruszenie przepisów rozporządzenia, a drugie – brak takiego naruszenia. W takim przypadku istnienie dwóch sprzecznych ze sobą orzeczeń podważałoby cel rozporządzenia, polegający na zapewnieniu spójnego i jednolitego w całej Unii stosowania przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Do państw członkowskich należy zatem określenie takich zasad powiązania tych środków ochrony prawnej, by zapewnić skuteczność ochrony praw gwarantowanych przez to rozporządzenie, spójne i jednolite stosowanie jego przepisów, a także prawo do skutecznego środka prawnego przed sądem.

W prawie polskim środki ochrony w razie naruszenia zasad przetwarzania danych osobowych również uregulowane są dwutorowo. Na gruncie art. 60 ustawy z 10.05.2018 r. o ochronie danych osobowych postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych jest prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych. W postępowaniu tym przysługuje prawo do wniesienia skargi do sądu administracyjnego. Niezależnie jednak od powyższego stosownie do art. 92 i n. ustawy możliwe jest dochodzenie roszczeń z tytułu naruszenia danych osobowych w procesie cywilnym przed sądem okręgowym. Polski ustawodawca rozwiązał problem kolizji środków ochrony uprawnionego w ten sposób, że o wniesieniu pozwu oraz prawomocnym orzeczeniu kończącym postępowanie w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych sąd zawiadamia niezwłocznie Prezesa Urzędu. Prezes Urzędu zawiadomiony o toczącym się postępowaniu niezwłocznie informuje sąd o każdej sprawie dotyczącej tego samego naruszenia przepisów o ochronie danych osobowych. Sąd umarza postępowanie w zakresie, w jakim prawomocna decyzja Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocny wyrok sądu administracyjnego, uwzględnia roszczenie dochodzone przed sądem. Zarazem ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku

[399]https://curia.europa.eu/juris/document/document.jsf;jsessionid=41F251870D5D7FA7A0122DA2590ADD04?text=&docid=269145&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=332155; https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-01/cp230003pl.pdf;

sądu administracyjnego, wiążą sąd cywilny w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych[400].

Pojęcie naruszenia na gruncie RODO

Po dokonaniu analizy zagadnień dotyczących naruszeń przepisów o ochronie danych należy dokonać analizy kolejnego zagadnienia, jakim jest odrębna kategoria zdarzenia szkodzącego, czyli naruszenie ochrony danych osobowych. Naruszenie przepisów o ochronie danych osobowych nie jest pojęciem tożsamym z naruszeniem ochrony danych osobowych. Istotne jest także to, że naruszenie przepisów nie jest pojęciem zdefiniowanym w RODO, a naruszenie ochrony danych osobowych w RODO zostało zdefiniowane. O naruszeniach przepisów o ochronie danych stanowi motyw 146 preambuły RODO, zgodnie z którym przetwarzanie dokonywane w sposób naruszający RODO obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy RODO oraz prawo państwa członkowskiego doprecyzowujące RODO. Podmiot danych może zatem wykorzystać przysługujący mu środek ochrony prawnej także w przypadku naruszenia przez administratora lub podmiot przetwarzający krajowych przepisów o ochronie danych osobistych[401].

Naruszenie ochrony danych osobowych definiowane jest jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Uregulowanie w RODO norm dotyczących naruszenia powoduje doniosłe konsekwencje. W ich wyniku mamy bowiem do czynienia ze współistnieniem w systemie prawnym polskich przepisów dotyczących naruszenia prawa oraz przepisów ogólnego rozporządzenia o ochronie danych dotyczącego tej materii w zakresie dotyczącym przetwarzania naruszającego RODO i naruszenia ochrony danych osobowych. O naruszeniu ochrony danych osobowych można mówić wówczas, gdy spełnione są kumulatywnie dwa zawarte w tej definicji warunki. Po pierwsze, dojść musi do naruszenia bezpieczeństwa. Po drugie, musi wystąpić skutek w postaci przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego

[400] *T. Partyk, Sądowe środki ochrony danych osobowych mogą być stosowane równolegle. Omówienie wyroku TS z dnia 12 stycznia 2023 r., C-132/21 (X)*, LEX/el. 2023; https://sip-1lex-1pl-1heg2dlkx07f8.han3.lib.uni.lodz.pl/#/publication/151426113/partyk-tomasz-sadowe-srodki-ochrony-danych-osobowych-moga-byc-stosowane-rownolegle-omowienie...?keyword=C-132~2F21%20&cm=STOP (dostęp: 2023-06-21 14:12)

[401] S. Kotecka-Kral, *Sądowe środki ochrony prawnej*..., s. 829–856.

dostępu do danych osobowych przesłanych, przechowywanych lub w inny sposób przetwarzanych. Fakt, że warunkiem zaistnienia naruszenia ochrony danych osobowych jest wystąpienie naruszenia bezpieczeństwa, prowadzi do wniosku, iż nie każde naruszenie zasad przetwarzania danych osobowych będzie kwalifikowało się jako naruszenie zdefiniowane w art. 4 pkt 12 RODO[402]. Naruszenie innych obowiązków wynikających z RODO, np. obowiązków informacyjnych[403], nie mieści się zatem w pojęciu naruszenia bezpieczeństwa i nie może być uznane za naruszenie ochrony danych osobowych

W tym miejscu konieczne jest zatem wskazanie konkretnych przykładów naruszeń ochrony danych. Nie jest to jednak oczywiste, o czy świadczy fakt, że EROD w toku swoich prac zajęła się tym zagadnieniem i podczas 58. posiedzenia plenarnego w dniu 14.12.2021 r. zaakceptowała ostateczną wersję Wytycznych w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych.

Dokument ten uzupełnia wytyczne Grupy Roboczej Art. 29, dotyczące zgłaszania naruszeń ochrony danych osobowych poprzez wprowadzenie bardziej ukierunkowanych na praktyki wytycznych i zaleceń. Najnowsze wytyczne mają pomóc administratorom w podejmowaniu decyzji o tym, jak postępować w przypadku naruszeń ochrony danych i jakie czynniki należy wziąć pod uwagę podczas oceny ryzyka. Wytyczne zawierają praktyczne przykłady naruszeń, wskazując np. w przykładzie 8 jako naruszenie „eksfiltrację danych biznesowych przez byłego pracownika". W omawianym przykładzie mowa jest o sytuacji, w której w okresie wypowiedzenia pracownik przedsiębiorstwa kopiuje dane handlowe z bazy danych przedsiębiorstwa, do której ma prawo dostępu, po to aby wypełniać swoje obowiązki. Kilka miesięcy później, po rezygnacji z pracy, wykorzystuje on uzyskane w ten sposób dane (głównie podstawowe dane kontaktowe) w celu skontaktowania się z klientami przedsiębiorstwa w celu przyciągnięcia ich do nowego pracodawcy. Chociaż jedyny cel byłego pracownika, który złośliwie skopiował dane, może ograniczać się do zdobycia danych kontaktowych klientów do własnych celów handlowych, administrator nie ma kompetencji do uznania, że ryzyko dla osób, których dane dotyczą, jest niskie, ponieważ administrator nie ma żadnej gwarancji co do intencji pracownika. Tak więc, podczas gdy konsekwencje naruszenia mogą być ograniczone do narażenia osób, których dane dotyczą, na niechciany marketing ze

[402] J. Błachut, S. Dudzik, *Naruszenie ochrony danych osobowych. Problematyka prawna*, „Przegląd Konstytucyjny" 2021/3, s. 10.
[403] P. Fajgielski, *Ogólne rozporządzenie o ochronie danych osobowych, ustawa o ochronie danych osobowych, Komentarz*, Warszawa 2018, s. 130.

strony byłego pracownika, nie jest wykluczone, że może dojść do innego, poważniejszego naruszenia tych danych.

Przykład nr 15 przedstawiony w Wytycznych Europejskiej Rady Ochrony Danych 01/2021 w sprawie przykładów zgłoszeń naruszeń ochrony danych, wersja 1.0 dowodzi, że naruszenie polegać może na wysłaniu drogą elektroniczną do 15 nieuprawnionych odbiorców listy 15 gości hotelowych zawierającą ich dane osobowe w zakresie nazwisk, adresów e-mail oraz preferencji żywnościowych (w przypadku dwóch gości). Przykład nr 16 przedstawiony w Wytycznych EROD 01/2021 dotyczy sytuacji, gdy grupa ubezpieczeniowa w ramach oferowania ubezpieczenia samochodowego wysłała do niewłaściwego odbiorcy korespondencję zawierającą dane osobowe w postaci imienia, nazwiska, adresu, daty urodzenia, numeru tablicy rejestracyjnej oraz klasyfikację stawki ubezpieczenia w bieżącym i przyszłym roku. W wytycznych wskazuje się, że niewłaściwy odbiorca powinien zostać poinformowany, że nie może wykorzystywać odczytanych informacji, a mimo tego należy również naruszenie zgłosić organowi nadzorczemu. Innym zobrazowaniem naruszenia ochrony danych osobowych jest przykład nr 12, czyli kradzież papierowego dziennika z ośrodka odwykowego, w którym to znajdowały się m. in. dane zdrowotne pacjentów przyjętych do placówki.

Analiza decyzji krajowego organu nadzorczego prowadzi do wniosku, że naruszenie w rozumieniu RODO może polegać na posiadaniu przez byłego pracownika Banku, któremu nie odebrano po zakończeniu stosunku pracy dostępu do Platformy Usług Elektronicznych ZUS (PUE ZUS), nieuprawnionego dostępu do tejże platformy, w wyniku czego mógł on przeglądać znajdujące się na profilu płatnika dane pracowników Banku w zakresie ich imion i nazwisk, nr PESEL, adresu zamieszkania lub pobytu oraz informacji o zwolnieniach lekarskich stanowiących dane dotyczące zdrowia[404].

Powyższe stanowisko potwierdzają rozważania Sądu Okręgowego w Elblągu, który w wyroku z 24.03.2021 r.[405] uznał, że „zachowanie powódki, polegające na uzyskaniu bezprawnego dostępu do danych osobowych klientów ZUS, pozostające bez związku z wykonywanymi obowiązkami pracowniczymi, było działaniem celowym i świadomym i jako takie wypełniło przesłanki ciężkiego naruszenia podstawowych obowiązków pracowniczych. Podkreślić należy, że powódka została przeszkolona przez pracodawcę do wykonywania swoich obowiązków, wielokrotnie składała oświadczenia na piśmie potwierdzające znajomość

[404] Decyzja Prezesa UODO z 19.01.2022 znak sprawy DKN.5131.33.2021 https://uodo.gov.pl/decyzje/DKN.5131.33.2021
[405] Wyrok z 24.03.2021 r. w sprawie o sygn.akt IV Pa 10/21.

dokumentów dotyczących przetwarzania danych osobowych oraz bezpieczeństwa informacji w ZUS, wielokrotnie uczestniczyła w szkoleniach dotyczących przestrzegania przepisów o ochronie danych osobowych, posiadała wiedzę o konsekwencjach świadomego naruszenia ochrony danych osobowych, a mimo to swoim zachowaniem naruszyła przepisy nie tylko wewnątrzzakładowe takie jak „Polityka bezpieczeństwa informacji w Zakładzie Ubezpieczeń Społecznych" i „Regulamin pracy Zakładu Ubezpieczeń Społecznych", ale również art. 4 pkt 12 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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)".

Inna grupą naruszeń są obowiązki wynikające z konieczności przestrzegania zasad bezpieczeństwa. Naruszeniem jest niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania, brak regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, które mają na celu zapewnienie bezpieczeństwa danych osobowych (decyzja PUODO z 9.12.2021 r. DKN.5130.2559.2020). Innym naruszeniem jest niewdrożenie odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych przy użyciu przenośnych pamięci zewnętrznych, zapewniających bezpieczeństwo zapisanych tam danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, co skutkowało utratą przenośnej pamięci zewnętrznej z danymi osobowymi, zapisanymi na niej w sposób niezabezpieczony (decyzja PUODO z 13.07.2021 r. DKN.5131.22.2021). Kolejnym rodzajem naruszeń jest zagubienie dokumentacji zawierającej dane osobowe (decyzja PUODO z 14.10.2021r DKN.5131.16.2021 r.), czy wysłanie pocztą elektroniczną do niewłaściwego odbiorcy danych osobowych w postaci imienia i nazwiska oraz oferty ubezpieczenia zawierającą dane osobowe w postaci: imię, nazwisko, nr PESEL, miejscowość, kod pocztowy, informację o przedmiocie ubezpieczenia (dom), informację o produkcie ubezpieczeniowym […], sumę ubezpieczenia/sumę gwarancyjną w kwocie 300 000 zł i 200 000 zł stosownie do wariantu oraz wysokość składki (decyzja PUODO z 21.06.2021 r. DKN.5131.3.2021). Podsumowując analizę naruszeń identyfikowanych w ramach aktualnych działań prowadzonych przez UODO wsakzać należy, że znacząca ich część dotyczy obowiązków związanych z bezpieczeństwem danych.

ROZDZIAŁ IV.

Obowiązki administratora i jego odpowiedzialność

Pojęcie administratora

Pojęcie administratora zdefiniowane zostało w art. 4 pkt 7 RODO poprzez wskazanie, że oznacza ono osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Definicja ta jest zbieżna z pojęciem administratora danych zawartym w poprzednio obowiązującym stanie prawnym, w którym w art. 7 pkt 4 UODO wskazywano na dwa konstrukcyjne elementy tego pojęcia: decydowanie o celach przetwarzania danych osobowych oraz decydowanie o środkach przetwarzania danych. Aktualność poglądów wypracowanych na gruncie poprzednio obowiązujących przepisów nie jest aktualnie sporna. Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych[406], podobnie jak RODO, zakładała prawie pełną swobodę co do statusu prawnego administratora, dlatego odwołanie się do wypowiedzi doktryny i judykatury, poczynionych na gruncie s.u.o.d.o. pozwala ocenić, czego można spodziewać się w trakcie stosowania samego RODO[407]. Zgodnie z definicją zawartą w art. 7 pkt 4 SUODO „ilekroć w ustawie jest mowa o: administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o której mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych". Przepis ten odwołuje się w swojej treści do art. 3 SUODO z 1997 r., który określał zakres podmiotowy stosowania jej przepisów - potencjalnie więc każdy podmiot, który objęty został zakresem podmiotowym ustawy, może zostać uznany za administratora danych, o ile - jednocześnie - decyduje o celach i środkach przetwarzania danych.[408]" Tak więc, aby uznać dany podmiot za administratora danych wymagane jest kumulatywne spełnienie dwóch przesłanek. Po pierwsze, trzeba należeć do którejś z kategorii podmiotów wskazanych w art. 3 UODO, po drugie, konieczne jest sprawowanie swoistego

[406] Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 723).
[407] K. Wygoda [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO*, Wrocław 2018, s. 17.
[408] P. Litwiński, *Administrator danych osobowych* [w:] *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009, LEX.

władztwa w procesie przetwarzania danych osobowych polegającego na decydowaniu o celach i środkach przetwarzania danych[409].

Ewolucja pojęcia administratora – od administratora zbioru danych w Konwencji nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, przez administratora danych w dyrektywie 95/46/WE, do administratora w RODO – podąża w kierunku uproszczenia pojęcia i skoncentrowania się na aspekcie zgodnego z prawem przetwarzania danych osobowych[410]. W opinii Grupy Roboczej art. 29 nr 1/2010 wskazuje się, że podstawową i najważniejszą rolą administratora danych jest określenie, kto odpowiada za zgodność z zasadami ochrony danych i w jaki sposób osoby, których dane dotyczą, mogą w praktyce wykonywać swoje prawa. W konsekwencji, biorąc pod uwagę brzmienie art. 4 pkt 7 RODO, nadal w ślad za wytycznymi Grupy Roboczej art. 29 można wskazywać, że definicja administratora składa się z trzech elementów:

1. personalnego: „osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot";
2. kontrolnego: określanego również mianem kontroli pluralistycznej z uwagi na użycie sformułowania „samodzielnie lub wspólnie z innymi";
3. podstawowego: elementu odróżniającego administratora od innych podmiotów – „ustala cele i sposoby przetwarzania danych osobowych"[411].

Takie rozumienie definicji potwierdza także dorobek orzecznictwa w zakresie dotyczącym administratora wypracowany w poprzednim stanie prawnym w tym m.in: wyrok NSA z 18.08.2016 r., sygn. akt I OSK 864/16[412]; wyrok NSA z 03.12.2015 r., sygn. akt I OSK

[409] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 53

[410] A. Mednis, *Prawna ochrona danych osobowych*,Warszawa 1995, s. 20–21; Grupa Robocza Art. 29, opinia 1/2010.

[411] A. Nerka, *Organizacja związkowa jako administrator – wybrane zagadnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społeczne" 2020/27/4.

[412] Według wyroku: w relacji podmiot prowadzący platformę ogłoszeń o pracę a pracodawca administratorem danych w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych kandydata do pracy jest pracodawca jako podmiot decydujący o celach i środkach przetwarzania danych osobowych. Status administratora danych nie wynika z samego faktu posiadania danych, ale ze sprawowania faktycznej kontroli nad ich przetwarzaniem, obejmującej dwa wspomniane elementy – decydowanie o celach i środkach przetwarzania danych.

1166/14[413]; wyrok NSA z 21.02.2014 r., sygn. akt I OSK 2445/12[414]; wyrok NSA z 14.03.2013 r., sygn. akt I OSK 1059/12[415].

Według prezentowanych powyżej poglądów na sprawowanie władztwa nad przetwarzanymi danymi składają się łącznie wchodzące w skład definicji administratora danych osobowych elementy, a więc decydowanie o celach i środkach przetwarzania danych osobowych. Podkreślić jednakże należy, że posiadania przymiotu administratora danych osobowych nie można utożsamiać z faktycznym posiadaniem danych - podstawowym kryterium odróżniającym administratora danych osobowych od innych podmiotów przetwarzających dane jest bowiem sprawowanie faktycznej kontroli nad przetwarzaniem danych, a więc decydowanie o celach i środkach przetwarzania, nie zaś faktyczne dysponowanie nimi – faktyczne ich przetwarzanie, które może zostać powierzone innemu podmiotowi. Na tę właśnie okoliczność zwrócił uwagę Naczelny Sąd Administracyjny w wyroku z 30.01.2002 r., II SA 1098/01,- w ocenie sądu, za administratora danych osobowych nie można uznać „każdego dysponenta danych". Administratorem danych osobowych „nie jest (...) każdy dysponent danych osobowych (...) Jest nim ten, kto decyduje o celach i środkach

[413] Według wyroku: nawet jednorazowe pozyskanie danych osobowych, tylko w jednym celu przez podmiot, który spełnia warunki, aby zostać uznanym za administratora, w rozumieniu art. 7 pkt 4 u.o.d.o., nakłada na niego obowiązki wobec osoby, której dane są przetwarzane, co miało miejsce w tej sprawie wobec pozyskania przez Spółkę danych osobowych z rejestru publicznego i wykorzystywania ich poprzez skierowanie do podmiotu danych propozycji odkupu posiadanych przez niego akcji.

[414] Według wyroku: administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych, to nie powinno budzić wątpliwości, że w każdej sytuacji, w której struktura organizacyjna administratora danych jest wieloosobowa, powinien on w ramach tej struktury wyznaczyć osobę fizyczną odpowiedzialną za wykonywanie czynności nadzorczych, powierzając jej obowiązki administratora bezpieczeństwa informacji, i to niezależnie od tego, czy administrator danych jest organem, jednostką organizacyjną, podmiotem czy osobą prawną. Zdaniem GIODO, wykonywanie przez administratora danych czynności administratora bezpieczeństwa informacji możliwe jest jedynie wówczas, gdy administrator danych jest osobą fizyczną. Jednak w przedmiotowej sprawie tak nie jest, gdyż kontrolowany nie był osobą fizyczną. W takiej sytuacji Spółka, jako administrator danych, powinna była wyznaczyć osobę fizyczną, która byłaby odpowiedzialna za proces bezpieczeństwa informacji i nadzór nad przestrzeganiem zasad ochrony.

[415] Według wyroku: obowiązki nałożone ustawą o ochronie danych osobowych mają zastosowanie do administratorów danych osobowych niezależnie od tego, jakie dane osobowe przetwarzają, w jakich celach i zbiorach, jak również ilości tych zbiorów. Nie ma znaczenia również fakt, czy administrator wykorzystuje do przetwarzania danych systemy informatyczne, czy dokonuje tych czynności w formie papierowej. W wyroku tym wobec sporu co do tego komu przysługuje status administratora Sąd stwierdził także, że administratorem danych członków wspólnoty mieszkaniowej jest Wspólnota, przez co spoczywają na niej obowiązki wynikające z ustawy o ochronie danych osobowych. Zarząd wspólnoty działa jako jej organ, a zarządca nieruchomości pełni rolę podmiotu, któremu administrator danych powierzył ich przetwarzanie. Zarówno Wspólnota, jak i zarządca są wobec tego zobligowani stosować wymagania odnoszące się do zabezpieczenia danych. Tym samym powierzenie innemu podmiotowi na podstawie art. 31 ust. 1 ustawy o ochronie danych osobowych przetwarzania danych osobowych w zakresie i celu określonym w tej umowie nie zwalnia Wspólnoty z obowiązków wynikających z art. 36 ust. 2 i 3 tej ustawy.

przetwarzania, przy czym zasadnicze znaczenie ma rodzaj i charakter nadanych przez prawo kompetencji z zakresu spraw publicznych”[416].

Sąd argumentował, że gdyby za administratora danych uznać każdego dysponenta danych pewne sfery ochrony danych osobowych znalazłyby się poza prawną ochroną. Sfera ochrony dotyczy bowiem nie tylko tych działań, które są dokonywane na podstawie ustawy o ochronie danych osobowych. W grę wchodzi także ochrona np. na podstawie przepisów o zwalczaniu nieuczciwej konkurencji, ochrona cywilnoprawna, ochrona karna itp. Między innymi dlatego Sąd Najwyższy rozróżnił administratora i administrującego danymi osobowymi[417]. Za administratora uznał jedynie ten podmiot, który decyduje o celach i środkach przetwarzania danych (art. 7 pkt 4 ustawy), natomiast administrującym jest taki podmiot, który zarządza, zawiaduje zbiorem danych lub danymi. Pojęcie administrującego ma więc szersze znaczenie. Może być nim zarówno administrator, jak i ten kto takiej roli nie pełni. Administratorem nie jest więc każdy dysponent danych osobowych[418]. Jest nim ten, kto decyduje o celach i środkach przetwarzania, przy czym zasadnicze znaczenie ma rodzaj i charakter nadanych przez prawo kompetencji z zakresu spraw publicznych[419].

W podobnym duchu wypowiedział się również Sąd Najwyższy w postanowieniu z 11.12.2001 r.[420], w którym rozróżnił administratora i administrującego danymi osobowymi. Za administratora uznał jedynie ten podmiot, który decyduje o celach i środkach przetwarzania danych, natomiast administrującym jest taki podmiot, który „zarządza, zawiaduje zbiorem danych lub danymi”[421].

---

[416] w/w orzeczenie zapadło w stanie faktycznym dotyczącym skargi Spółki na działania jej byłego członka zarządu, który uniemożliwiał przeniesienie danych osobowych Spółki do jej nowej siedziby. W następstwie działań organu nadzorczego były członek zarządu wydał Spółce część dokumentów z wyjątkiem zapisu elektronicznego na twardej części dysku oraz comiesięcznych archiwizacji danych osobowych Spółki przechowywanych, zgodnie z § 7 celów Strategii i Polityki Zabezpieczenia Systemów Informatycznych, w kasie pancernej. Kasa pancerna znajdowała się mieszkaniu byłego członka zarządu, który początkowo był związany z inną spółką, która korzystała z jego zasobów mieszkaniowych, a w końcowej fazie postepowania pozostawał także poza strukturą tej innej spółki. Z uwagi na fakt, że nie został on uznany za administratora danych, bowiem taki status w tej sprawie posiadała wyłączenie Spółka, w której były członek zarządu pełnił funkcję organu, nie mógł być w trakcie postępowania stroną decyzji kontrolnej. W sprawie tej wybrzmiało, że obawę skarżącego o zapewnienie właściwej ochrony danych osobowych trzeba jednocześnie pogodzić z konstytucyjnym prawem do prywatności, której naruszeniem byłaby zdaniem Sądu możliwość przeszukania pomieszczeń prywatnych u osoby fizycznej, którą podejrzewano jedynie o wykorzystanie danych osobowych, w taką osobą był właśnie były członek zarządu.

[417] Zob. postanowienie SN z 11.12.2001 r., sygn. akt II KKN 438/00, OSNKW 2001 nr 3–4, poz. 33. a

[418] J. Barta, R. Markiewicz, *Ochrona danych osobowych Komentarz*, Kraków 2001, s. 307.

[419] J. Barta, R. Markiewicz, *Ochrona danych...*, s. 306

[420] Wyrok dotyczył stanu faktycznego, w którym przyjmujący zlecenie dokonania akcji promocyjnej zbierał w jej toku dane osobowe, będąc jednocześnie zobowiązanym do zniszczenia pozostałej po losowaniu korespondencji w terminie 2 miesięcy po zakończeniu promocji. Zobowiązanie to przyjmujący zlecenie wykonał w sposób nieprawidłowy przekazując podmiotowi zewnętrznemu usługę zniszczenia dokumentacji bez zastrzeżenia jej tajności i tym samym umożliwiając jej udostępnienie w toku procedury niszczenia osobom nieupoważnionym (zob. postanowienie SN z 11.12.2001 r., sygn. akt II KKN 438/00).

[421] P. Litwiński, *Administrator danych...*

W piśmiennictwie słusznie uznaje się, że decydowanie o celach i środkach przetwarzania powinno być rozumiane jako faktyczne podejmowanie we własnym imieniu i na własną rzecz decyzji o tym, w jakim celu i w jaki sposób przetwarzane są dane osobowe. Zasadniczo decyzja co do określoności celów przetwarzania spoczywa na administratorze w takim zakresie, w jakim leży to w granicach jego swobodnej decyzji, a nie jest narzucone przez przepisy prawa, które mogą wyznaczać pewne „dalsze" cele przetwarzania danych osobowych. Tak się dzieje na podstawie art. 5 ust. 1 lit. b RODO, który wprost wskazuje, że dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, które nie jest uznawane w myśl art. 89 ust. 1 RODO, jest niezgodne z pierwotnymi celami. Przepis ten pokazuje właśnie, że administrator może być pozbawiony możliwości samodzielnego określania celów przetwarzania, gdy wynikają one bezpośrednio z przepisów prawa[422].

Podkreślić należy, że SUODO posługiwała się określeniem „administrator danych" dla oznaczenia podmiotów odpowiedzialnych za procedury postępowania z danymi osobowymi. Administratorem danych jest ten podmiot, który ponosi odpowiedzialność za przetwarzanie danych.[423] Z punktu widzenia zasad dotyczących przetwarzania danych osobowych i obowiązków nakładanych przez te przepisy administrator danych był podmiotem kluczowym. Na gruncie RODO występuje tożsame rozumienie roli administratora, o czym świadczą stanowiska prezentowane w aktualnym orzecznictwie takie jak to, że zasada rozliczalności bazuje na prawnej odpowiedzialności administratora za właściwe wypełnianie obowiązków i nakłada na niego obowiązek wykazania zarówno przed organem nadzorczym, jak i przed podmiotem danych, dowodów na przestrzeganie wszystkich zasad przetwarzania danych[424] oraz takie, że administrator ma znaczną swobodę w zakresie stosowanych zabezpieczeń, jednocześnie jednak ponosi odpowiedzialność za naruszenie przepisów o ochronie danych osobowych. Z zasady rozliczalności wprost wynika, że to administrator danych powinien wykazać, a zatem udowodnić, że przestrzega przepisów określonych w art. 5 ust. 1 RODO[425].

Decydowanie o celach i środkach przetwarzania danych oznacza faktyczne podejmowanie decyzji w odniesieniu do przetwarzanych danych osobowych oraz

[422] A. Nerka, *Organizacja związkowa jako administrator – wybrane zagadnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2020/27/4, s. 259–270.
[423] A. Mednis, *Administrator danych i podmiot przetwarzający dane na zlecenie – status prawny, zakres praw i obowiązków, problemy definicyjne* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009, s. 80.
[424] Wyrok WSA w Warszawie z 10.02.2021 r., sygn. II SA/Wa 2378/20.
[425] Wyrok WSA w Warszawie z 26.08.2020 r., sygn. II SA/Wa 2826/19.

samodzielność w podejmowaniu tych decyzji, ale aby być zaliczonym do administratorów danych nie jest konieczne fizyczne dysponowanie danymi. Nie sposób in abstracto wyznaczyć katalogu takich celów i środków. Oczywiste jest, że „cele i środki przetwarzania" wynikać będą ze specyfiki działalności administratora danych. Trudno wskazać środki przetwarzania danych bez oznaczenia tego, kim jest administrator danych i na czym polega jego działalność, zwłaszcza że w ramach działalności przedsiębiorcy wykonywane są różne czynności związane z przetwarzaniem danych np. gromadzenie danych, wprowadzanie ich do systemów informatycznych, katalogów baz danych, następnie ich odczyt, zmiana bądź usuwanie[426]. Pojęcie to odnosi się do sposobów, form oraz organizacji przetwarzania danych. Nie ogranicza się natomiast do jego finansowania. W kontekście owych środków przetwarzania należy podnieść, że administrator danych nie musi być właścicielem wszystkich, czy też poszczególnych elementów infrastruktury służącej do przetwarzania danych, posługując się pojęciem środków przetwarzania powinniśmy mieć na uwadze całość procesów przetwarzania w obszarze infrastruktury, oprogramowania, a także organizacji.[427]

O decydowaniu przez konkretny podmiot o celach i środkach przetwarzania danych osobowych wnioskujemy zwykle z okoliczności faktycznych. Zdaniem Grupy Roboczej Art. 29 w przypadku słowa określa należy przyjrzeć się konkretnym operacjom przetwarzania i zrozumieć, kto je określa, odpowiadając przede wszystkim na danym etapie na pytania „dlaczego dane przetwarzanie ma miejsce? kto je rozpoczął?"[428] Takie rozumienie powielają także wytyczne EROD 7/2020 wydane na gruncie RODO, które podkreślają, że pojęcia administratora i podmiotu przetwarzającego są pojęciami funkcjonalnymi: ich celem jest podział obowiązków stosownie do rzeczywistych ról stron. Oznacza to, że status prawny podmiotu jako „administratora " lub „podmiotu przetwarzającego" należy zasadniczo określać na podstawie jego rzeczywistych działań w konkretnej sytuacji, a nie na formalnym wyznaczeniu podmiotu jako „administratora danych" lub „podmiotu przetwarzającego" (np. w umowie). W konsekwencji podział ról powinien zazwyczaj wynikać z analizy elementów stanu faktycznego lub okoliczności sprawy i jako taki nie podlega uzgodnieniom. Pojęcia administratora i podmiotu przetwarzającego są również pojęciami autonomicznymi w tym sensie, że chociaż zewnętrzne źródła prawne mogą być pomocne w ustaleniu, kto jest

[426] M. Ganczar, *Obowiązki przedsiębiorców w zakresie gromadzenia, przetwarzania i udostępniania danych osobowych* [w:] *Człowiek z perspektywy biznesu*, Lublin 2009, s. 126.
[427] A. Krasuski, *Dane osobowe w obrocie tradycyjnymi elektronicznym. Praktyczne problemy*, Warszawa 2012, s. 120.
[428] Opinia 1/2010 Grupy Roboczej art. 29 w sprawie pojęć administratora danych i przetwarzającego, przyjęta 16.02.2010 r., http://www.giodo.gov.pl/1520057/id_art/3595/j/pl

administratorem danych, interpretacji należy dokonywać przede wszystkim zgodnie z przepisami dotyczącymi ochrony danych. Z wytycznych należy wnioskować, że koncepcja administratora nie powinna kolidować z pojęciami z innych dziedzin prawa, takimi np. jak twórca lub posiadacz praw w prawach własności intelektualnej lub prawie konkurencji, choć różne pojęcia i różne ich zakresy mogą się na siebie nakładać. Jednocześnie temu wzajemnemu współstosowaniu powinno służyć wzięcie pod uwagę podstawowego celu przypisania konkretnemu podmiotowi roli administratora, jakim jest zapewnienie rozliczalności i skuteczna, kompleksowa ochrona danych osobowych.

W tym kontekście pojęcie administratora powinno być: interpretowane w sposób dostatecznie szeroki, sprzyjający jak najbardziej efektywnej i kompletnej ochronie osób, których dane dotyczą, aby zapewnić pełne działanie unijnego prawa o ochronie danych, aby uniknąć luk i zapobiegać możliwemu obchodzeniu przepisów[429].

Jako przykłady z praktyki uznania konkretnych podmiotów za administratorów wskazać można na te, które zawarte są w opinii 1/2010 Grupy Roboczej Art. 29 i wytycznych 7/2020. I tak w przypadku przekazywania komunikatu zawierającego dane osobowe przy pomocy urządzeń telekomunikacyjnych lub poczty elektronicznej, których wyłącznym przeznaczeniem jest przekazywanie takich komunikatów, za administratora danych osobowych zawartych w takim komunikacie uważać się będzie osobę, od której komunikat wychodzi, nie zaś osobę wykonującą usługę w zakresie transmisji danych. Zatem w sytuacji, gdy zgodnie z umową podmiot X świadczy usługi reklamy komercyjnej dla klientów podmiotu Y i jest przetwarzającym, ale postanawia wykorzystać bazę danych klientów Y również w celu promowania produktów innych klientów, decyzja, aby dołączyć dodatkowy cel do celu, w którym przekazano dane osobowe, zmienia X w administratora danych dla tych celów[430].

Inny przykład może dotyczyć następującego stanu faktycznego. Przedsiębiorstwo ABC chce zrozumieć, którzy konsumenci będą najbardziej zainteresowani jego produktami. Dostawca usług XYZ jest agencją zajmującą się badaniami rynku, która gromadziła informacje na temat upodobań konsumentów za pomocą różnych kwestionariuszy dotyczących szerokiej gamy produktów i usług. Dostawca usług XYZ zebrał i przeanalizował te dane niezależnie, zgodnie z własną metodologią, nie otrzymując żadnych instrukcji od przedsiębiorstwa ABC. Aby dostarczyć usługę, o którą zwróciło się przedsiębiorstwo ABC, dostawca usług XYZ wygeneruje informacje statystyczne, ale zrobi to bez otrzymania jakichkolwiek dalszych

[429] M. Sakowska-Baryła, *Administrator i podmiot przetwarzający w wytycznych 07/2020 EROD*, dodatek MoP 23/2021/23.
[430] Wytyczne 7/2020 EROD , s.19.

instrukcji dotyczących tego, które dane osobowe należy przetwarzać lub jak je przetwarzać w celu wygenerowania tych statystyk. W tym przypadku dostawca usług XYZ pełni funkcję jedynego administratora i przetwarza dane osobowe do celów badania rynku, samodzielnie określając sposoby osiągnięcia tego celu[431].

Pojęcie administratora ma zasadnicze znaczenie w stosowaniu przepisów o ochronie danych osobowych, w tym także z punktu widzenia analizowanych w pracy zagadnień. Ustalenie kto jest administratorem jest bowiem równoznaczne ze wskazaniem, kto w rozważanym przypadku odpowiada za zgodność przetwarzania danych z zasadami ich ochrony, wyrażonymi w RODO i innych przepisach o ochronie danych osobowych. Ten kto decyduje o tym w jakim celu dane są zbierane i w jaki sposób przetwarzane może bowiem ponieść konsekwencje prawne braku zgodności swojego zachowania z prawem. W związku z tym, że pojęcie administratora jest pojęciem funkcjonalnym, opiera się ono raczej na analizie okoliczności faktycznych niż analizie formalnej. W celu ułatwienia analizy można zastosować pewne zasady postępowania i praktyczne założenia, aby ukierunkować i uprościć proces. W większości sytuacji „organ ustalający" można łatwo i jasno identyfikować przez odniesienie do okoliczności prawnych lub faktycznych, z których normalnie może wynikać faktyczny „wpływ", o ile inne elementy nie wskazują inaczej. Można wyróżnić dwie kategorie sytuacji: (1) administrowanie wynikające z przepisów prawnych; oraz (2) administrowanie wynikające z faktycznego wpływu[432].

W tym miejscu warto poczynić odniesienie, że funkcjonalne rozumienie pojęcia administratora, wykazuje podobieństwo do pojęcia znanego z art. 435 k.c., w którym z „prowadzenia na własny rachunek" uczyniono kryterium oznaczające osobę odpowiedzialną za szkody wyrządzone przez ruch przedsiębiorstw poruszanych siłami przyrody. Zgodnie z poglądami B. Lewaszkiewicz-Petrykowskiej prowadzenie na własny rachunek najszerzej pojęte polega na możliwości wpływania na losy przedsiębiorstwa, kierowania jego pracą, wydawania wiążących poleceń, sprawowania nadzoru i kontroli , rozstrzygania o celu i sposobie ruchu. Wszystkie te cechy mogą łącznie występować u prowadzącego. Odpowiedzialną jest jednak nie osoba prowadząca w ogóle, ale osoba prowadząca przedsiębiorstwo „na własny rachunek". Będzie to więc osoba, która nie tylko posiada wyłączną możliwość decydowania o naturze funkcjonowania przedsiębiorstwa, ale nadto władzę tę wykonuje we własnym imieniu i dla siebie. Jest to osoba ponosząca nieuchronnie związane z funkcjonowaniem przedsiębiorstwa ryzyko gospodarcze, obciążona

[431] Wytyczne 7/2020 EROD, s.19.
[432] Wytyczne 7/2020 EROD, s.12.

konsekwencjami własnej działalności gospodarczej oraz posiadająca samodzielny bilans zysków i strat. Oczywiście, wszystkie te przymioty muszą istnieć w chwili wyrządzenia szkody. Moment ten bowiem jest decydujący dla podmiotu odpowiedzialnego[433].

Problem przypisywania statusu administratora był wielokrotnie podejmowany zarówno w doktrynie, jak i w orzecznictwie[434]. Zwykle przyjmuje się, że zidentyfikowanie roli danego podmiotu wymaga oceny sytuacji przez pryzmat przesłanek wynikających z definicji administratora. Na gruncie art. 4 pkt 7 RODO pojęcie administratora oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi podmiotami ustala cele i sposoby przetwarzania danych osobowych, przy czym prawodawca europejski dopuszcza możliwość określenia celów i sposobów przetwarzania w prawie Unii lub w prawie państwa członkowskiego. W takim wypadku administrator może zostać wyznaczony również w prawie Unii lub w prawie państwa członkowskiego. Konkretne kryteria jego wyznaczenia mogą zostać określone wprost w przepisach. Dla porządku należy dodać, że status administratora może uzyskać podmiot przetwarzający dane w imieniu innej osoby (procesor) w sytuacji wskazanej w art. 28 ust. 10 RODO, czyli w razie naruszenia przepisów o ochronie danych przy określaniu celów i sposobów przetwarzania uznaje się go za administratora w stosunku do tego przetwarzania. Dopuszczona przez przepisy RODO możliwość wyznaczenia administratora w przepisach krajowych lub prawie Unii, a także ustalenia kryteriów jego wyznaczenia, gdy cele i sposoby przetwarzania ustalane są także na poziomie tych przepisów, zakłada istnienie sytuacji, w której kontrola nad celami i sposobami przetwarzania wynika z wyraźnych kompetencji przewidzianych przez prawo. W takim przypadku przepisy mogą jednoznacznie wskazywać, który podmiot pełni funkcję administratora, ale też status ten może wynikać pośrednio z przyznanych danemu podmiotowi zadań.

W polskim porządku prawnym znajdują się przykłady regulacji przypisujących określonemu podmiotowi status administratora, lub przekazujących określonemu podmiotowi zadania związane z przetwarzaniem, z którego wynika taki status. Można tu wskazać, że ustawa o Policji przyznaje w stosunku do niektórych zbiorów status administratora danych Komendantowi Głównemu Policji, a ustawa o Krajowym Rejestrze Karnym – Ministrowi

[433] B. Lewaszkiewicz-Petrykowska, *Zakres odpowiedzialności na zasadzie ryzyka prowadzącego na własny rachunek przedsiębiorstwo wprawiane w ruch za pomocą sił przyrody art. 435 k.c.*, RPEiS 1968/30, s. 49–68; https://repozytorium.amu.edu.pl/bitstream/10593/18389/1/006%20BIRUTA%20LEWASZKIEWICZ-PETRYKOWSKA.pdf

[434] A. Nerka, *Organizacja związkowa jako administrator – wybrane zagadnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2020/27/4: s. 259–270.

Sprawiedliwości w stosunku do danych zgromadzonych w Rejestrze[435]. W ustawie o Służbie Więziennej administratorem danych osobowych przetwarzanych przez Inspektorat Wewnętrzny Służby Więziennej jest Szef IWSW[436]. Częściej jednak ma miejsce sytuacja, w której przepisy prawa, zamiast bezpośrednio wyznaczyć administratora danych lub określić kryteria jego wyznaczania, ustalają zadanie lub nakładają na kogoś obowiązek gromadzenia i przetwarzania niektórych danych. W takim przypadku określenie, kto jest administratorem, wynika z przepisów prawa[437].

Podsumowując powyższe rozważania wskazać należy, że status konkretnego podmiotu jako administratora danych osobowych może wynikać:

- bezpośrednio z przepisów prawa,
- z interpretacji przepisów prawa (np. pracodawca jest administratorem danych osobowych pracowników),
- z dokonywanych przez Prezesa Urzędu Ochrony Danych Osobowych interpretacji prawa takich, np. jak: administratorem danych przetwarzanych w związku z działalnością biblioteczną jest uniwersytet, w ramach którego działa biblioteka[438], czy takich np., że w następstwie gromadzenia przez radę rodziców danych rodziców, którzy dokonali wpłat administratorem tych danych będzie szkoła, pomimo tego, że działanie rady rodziców regulują art. 83 i 84 ustawy z dnia 14.12.2016 r. – Prawo oświatowe[439].

Powyższe uprawnienie PUODO wynika ze statusu i kompetencji organu nadzorczego określonych w RODO, w ramach których dokonywanie oficjalnej interpretacji prawa w zakresie ochrony danych osobowych (w rozumieniu RODO) leży po stronie Prezesa UODO. Zgodnie z RODO jest to wyłączną kompetencją organów nadzorczych krajów członkowskich oraz Europejskiej Rady Ochrony Danych. Tym samym UODO jest jedynym organem umocowanym prawnie do wydawania wytycznych i interpretowania w tym zakresie przepisów prawa.

W literaturze prezentowane jest stanowisko, że pośród elementów definicji administratora danych najwięcej kontrowersji i wątpliwości interpretacyjnych wywołuje „ustalanie" celów i sposobów przetwarzania danych. Należy zauważyć, iż tam, gdzie w dyrektywie 95/46/WE i w RODO w tekstach oryginalnych występuje to samo słowo, a mianowicie determines, w tłumaczeniach tych aktów prawnych na język polski występują

[435] A. Nerka, *Organizacja związkowa...*, s. 259–270.
[436] Artykuł 23v ustawy z 9.04.2010 r. o służbie więziennej.
[437] Wytyczne 7/2020 EROD.
[438] Zob. https://uodo.gov.pl/pl/494/2354
[439] Zob. https://uodo.gov.pl/pl/494/2419

dwa różne słowa, a mianowicie „określa" w dyrektywie 95/46/WE oraz „ustala" w RODO. Wydaje się jednak, iż z uwagi na dominujące znaczenie dla wykładni tekstu oryginalnego wspomniane różnice nie powinny mieć żadnego wpływu na meritum, co pozwala na wykorzystanie wykładni tego elementu, ukształtowanej począwszy od lat 90. XX wieku[440].

W przypadku gdy administrator został wyraźnie wyznaczony przez prawo, będzie to miało decydujące znaczenie dla ustalenia, kto działa jako administrator. Oznacza to, że ustawodawca wyznaczył jako administratora podmiot, który ma rzeczywistą zdolność do sprawowania kontroli. W niektórych państwach przepisy prawa krajowego przewidują, że organy publiczne odpowiadają za przetwarzanie danych osobowych w ramach swoich obowiązków. Pracowników, którzy mają dostęp do danych osobowych w organizacji, zasadniczo nie uważa się za „administratorów" ani „podmioty przetwarzające", lecz raczej za „osoby działające z upoważnienia administratora lub podmiotu przetwarzającego" w rozumieniu art. 29 RODO. Częściej ma jednak miejsce sytuacja, w której przepisy prawa, zamiast bezpośrednio wyznaczyć administratora danych lub określić kryteria jego wyznaczania, ustalają zadanie lub nakładają na kogoś obowiązek gromadzenia i przetwarzania niektórych danych. W takim przypadku określenie, kto jest administratorem, wynika z mocy prawa. Administratorem będzie zazwyczaj podmiot wyznaczony przez prawo do realizacji tego celu, tego zadania publicznego. Tak może być na przykład w przypadku podmiotu, któremu powierzono pewne zadania publiczne (np. zabezpieczenie społeczne), których nie można wypełnić bez zgromadzenia przynajmniej niektórych danych osobowych, i który tworzy bazę danych lub rejestr w celu realizacji tych zadań publicznych. W takim przypadku określenie, kto jest administratorem – choć pośrednio – wynika z normy prawnej. Ogólniej mówiąc, prawo może również nakładać na podmioty publiczne lub prywatne obowiązek zatrzymywania lub przekazywania określonych danych. Podmioty te byłyby wówczas zazwyczaj uznawane za administratorów w odniesieniu do przetwarzania, które jest niezbędne do wykonania tego obowiązku[441].

Zgodnie ze stanowiskiem wyrażonym w opinii 1/2010 Grupy Roboczej art. 29 zdolność „ustalania" może zostać nadana z mocy prawa i zwykle będzie wynikać z analizy elementów faktycznych lub okoliczności danego przypadku – należy przyjrzeć się konkretnym operacjom przetwarzania i zrozumieć, kto je określa, odpowiadając na pierwszym etapie na pytania: dlaczego dane przetwarzanie ma miejsce? I kto je rozpoczął?. Bycie administratorem danych

[440] D. Dorre Kolasa, *Administrator danych osobowych w zbiorowym prawie zatrudnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019/26/4, s. 371.
[441] Wytyczne 7/2020 EROD.

wynika zatem przede wszystkim z okoliczności faktycznej, w której podmiot podjął decyzję o przetwarzaniu danych osobowych dla własnych celów[442]. W takim przypadku należy przyjrzeć się konkretnym operacjom przetwarzania i zrozumieć, kto je ustala, biorąc pod uwagę w pierwszej kolejności następujące kwestie: „dlaczego dane są przetwarzane?" oraz „kto zdecydował, że dane powinny być przetwarzane w określonym celu?"[443]

Także wytyczne 07/2020 EROD pojęcia administratora i podmiotu przetwarzającego określają jako „pojęcia funkcjonalne", które mają na celu przypisanie odpowiedzialności zgodnie z rzeczywistymi rolami stron, co oznacza, że status prawny „administratora" lub „podmiotu przetwarzającego" musi, co do zasady, być określony przez jego rzeczywistą działalność w określonej sytuacji, a nie opierać się na formalnym lub umownym nadaniu ról podmiotom uczestniczącym w procesach przetwarzania danych osobowych. Potwierdza to trafność interpretacji, według której określenie statusu podmiotowego następuje na podstawie analizy stanu faktycznego. Z tym stanem faktycznym związane są natomiast określone przepisami prawa obowiązki oraz innego rodzaju konsekwencje prawne.

Jak wskazuje EROD w wytycznych 07/2020 – pierwszy element konstrukcyjny odnosi się do typu jednostki, która może być administratorem. Ów typ jednostki i jego uwarunkowania o charakterze prawnym, w tym cywilnym, administracyjnym, finansowym, kształtowany jest jednak przede wszystkim przez prawo krajowe. Nie przeczy to stanowisku EROD, że pojęcia administratora i podmiotu przetwarzającego są pojęciami autonomicznymi, bo sens tej autonomii odnosi się do obszaru unijnego prawa do ochrony danych osobowych. Natomiast zewnętrzne, w tym krajowe, źródła prawne powinny móc pomóc w ustaleniu, kto właściwie jest administratorem i kto może w sposób efektywny udźwignąć ciężar związanych z tym statusem obowiązków. W tych okolicznościach uzasadnione jest zadanie pytania o przywołaną już „zdolność" rzeczywistego wykonywania obowiązków administratora czy podmiotu przetwarzającego. Na tym tle uzasadnione jest twierdzenie, że administratorów należy poszukiwać wśród podmiotów, które są zdolne do ponoszenia odpowiedzialności i którym przysługuje zdolność prawna. Zabiegiem częstym pozostaje natomiast ustalanie statusu administratora na podstawie norm kompetencyjnych, a więc przepisów, które określają kompetencje danego podmiotu, do których wykonywania niezbędne jest przetwarzanie danych osobowych[444].

[442] D. Dorre-Kolasa, *Administrator danych osobowych...*, s. 367–388.
[443] Wytyczne 7/2020 EROD.
[444] M. Sakowska- Baryła, *Administrator i podmiot przetwarzający w wytycznych 07/2020 EROD*, MoP 2021/23.

Określenie „celu" przetwarzania powinno się odnosić do oczekiwanego i zamierzonego rezultatu[445]. Dla zapewnienia zgodności z RODO, tj. z art. 5 ust. 1 pkt b, cel ten powinien być konkretny, wyraźny i prawnie uzasadniony. Co do zasady – dane nie powinny być przetwarzane dalej w sposób niezgodny z tymi pierwotnymi celami. Określanie „sposobów" należy interpretować szeroko. Mieszczą się w tym kwestie zarówno techniczne, jak i organizacyjne (np. rodzaj sprzętu, oprogramowania, stosowana forma zabezpieczenia przed dostępem osób nieupoważnionych, utratą danych), które niekiedy mogą być scedowane na podmioty przetwarzające dane w imieniu administratora, tzw. podmioty przetwarzające. Zasadnicze elementy określania „sposobów, tj. zakresu danych osobowych («jakie dane», «jakich podmiotów danych»), okresu przetwarzania danych, a także tego, kto ma dostęp do przetwarzanych danych", w tradycyjny i nieodłączny sposób określa wyłącznie administrator danych[446].

Jeśli administrowanie nie wynika z norm prawnych, statusu administratora należy poszukiwać na podstawie oceny okoliczności faktycznych związanych z przetwarzaniem. Aby stwierdzić, czy dany podmiot ma decydujący wpływ na przetwarzanie danych osobowych, należy wziąć pod uwagę wszystkie istotne okoliczności faktyczne. Potrzeba oceny faktów oznacza również, że rola administratora nie wynika z charakteru podmiotu przetwarzającego dane, ale z jego konkretnych działań w określonym kontekście. Innymi słowy, ten sam podmiot może działać jednocześnie jako administrator w przypadku niektórych operacji przetwarzania danych i jako przetwarzający w przypadku innych tego rodzaju operacji, a to czy kwalifikuje się jako administrator, czy przetwarzający należy oceniać w odniesieniu do każdej konkretnej czynności przetwarzania danych. W praktyce niektóre działania związane z przetwarzaniem można uznać za powiązane w sposób naturalny z rolą lub działalnością podmiotu, co ostatecznie pociąga za sobą odpowiedzialność z punktu widzenia ochrony danych. Może to wynikać z bardziej ogólnych przepisów prawnych lub z utrwalonej praktyki prawnej w różnych dziedzinach (prawo cywilne, prawo handlowe, prawo pracy itd.). W takim przypadku w zidentyfikowaniu administratora pomogą istniejące tradycyjne role i wiedza specjalistyczna, które zwykle wiążą się z pewną odpowiedzialnością: będzie nim na przykład pracodawca w odniesieniu do przetwarzania danych osobowych dotyczących jego pracowników, wydawca przetwarzający dane osobowe swoich abonentów lub stowarzyszenie przetwarzające dane osobowe swoich członków lub osób wspierających. Gdy podmiot angażuje się w przetwarzanie

[445] Opinia 1/2010 Grupy Roboczej Art. 29, s. 14.
[446] D. Dorre-Kolasa, *Administrator danych osobowych*..., s. 367–388.

danych osobowych w ramach interakcji z własnymi pracownikami, klientami lub członkami, to zazwyczaj to ten podmiot określa cel i sposoby przetwarzania i w związku z tym działa jako administrator w rozumieniu RODO[447].

W praktyce nierzadko są spotykane sytuacje trudne do jednoznacznej oceny, który z podmiotów jest administratorem danych, a który przetwarzającym. Skomplikowanym przypadkiem z życia codziennego może być np. przystąpienie pracodawcy do programu oferowanego przez podmiot świadczący usługi sportowo-rekreacyjne i zawarcie umowy o świadczenie usług przez dany podmiot dla pracowników pracodawcy. Pracodawca jako administrator danych pracowników jest zobowiązany do przekazania określonych w umowie danych po to, by pracownicy jako członkowie programu benefitowego otrzymali karty wstępu do obiektów usługodawcy. W takich sytuacjach, po przekazaniu danych pracodawca staje się przetwarzającym, natomiast administratorem danych uczestników programu sportowo-rekreacyjnego jest podmiot świadczący usługę, który określa jaki zakres danych osobowych jest niezbędny dla wystawienia takich kart i ich rozliczenia z podmiotami współpracującymi. Takich przypadków, gdy administrator danych jest jednocześnie przetwarzającym (i w odwrotnej konfiguracji) oraz gdy trudno jest jednoznacznie stwierdzić, który z podmiotów jest faktycznie administratorem, a który przetwarzającym, jest wiele, dlatego każdy stosunek prawny tego typu wymaga indywidualnej oceny okoliczności, stanowiących podstawę przetwarzania danych osobowych.

Współadministrowanie

RODO wprowadza nowe podejście rozumienia procesu przetwarzania danych dokonywanego przez kilku administratorów, wprowadzając definicję współadministrowania, zawartą w art. 26 RODO, zgodnie z którą – jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, tzn. wspólnie o nich decydują, to są współadministratorami. W definicji administratora danych funkcjonującej na gruncie dyrektywy 95/46/WE występowała możliwość, by administrator samodzielnie lub wspólnie z innymi podmiotami określał cele i sposoby przetwarzania danych. Brakowało jej natomiast w definicji administratora danych osobowych wynikającej z polskiej ustawy, gdzie ustawodawca posługiwał się liczbą pojedynczą[448]. Z definicji, zawartej w art. 26 RODO należy wywieść, że status współadministratorów konkretnym podmiotom może zostać przypisany wtedy, gdy zostaną łącznie spełnione następujące warunki:

[447] Wytyczne 7/2020 EROD, s.13.
[448] M. Czech, *Umowa powierzenia...*, s. 198.

- co najmniej 2 podmioty są administratorami (ADO) w rozumieniu RODO,
- co najmniej 2 podmioty wspólnie ustalają cele przetwarzania,
- co najmniej 2 podmioty wspólnie ustalają sposoby przetwarzania (w rozumieniu organizacyjnym i technicznym).

Współadministrowanie nie jest zależne od konieczności wystąpienia uprzedniej konkretnej przyczyny czy podstawy prawnej wspólnego przetwarzania danych osobowych. Zaistnienie relacji współadministrowania jest uzależnione od wystąpienia kumulatywnie dwóch przesłanek, tj. określenia przez dwóch odrębnych administratorów wspólnego celu i sposobu przetwarzania danych osobowych. Wspólne ustalanie przez co najmniej dwóch administratorów celów i sposobów przetwarzania stanowi konstytutywną cechę pozwalającą twierdzić, że w danym przypadku mamy do czynienia ze współadministrowaniem. Istotą współadministrowania jest podejmowanie decyzji w zakresie celów i sposobów przetwarzania, a nie sam udział więcej niż jednego podmiotu w procesie przetwarzania.

Specyfika relacji współadministrowania polega przede wszystkim na tym, że administratorzy wspólnie ustalają cele i sposoby przetwarzania, a także wspólnie realizują obowiązki wynikające z przepisów RODO i podejmują procesy przetwarzania. W konsekwencji za pozbawioną uzasadnienia należy uznać praktykę wskazywania w umowie, że mocą wzajemnych uzgodnień nadany został jej stronom status współadministratora. Skoro fakt współadministrowania wynika z konkretnego stanu faktycznego, jaki łączy dwóch administratorów, to nie ma podstaw do uznania, że regulacje umowne będą kształtowały taką rolę administratorów w stosunku do danych osobowych będących przedmiotem operacji przetwarzania. Tym samym nazwanie stron umowy współadministratorami nie będzie decydujące w określeniu statusu prawnego danego podmiotu, zwłaszcza w przypadku, gdy faktyczna relacja stron umowy wyraźnie wskazuje, że mamy do czynienia np. z powierzeniem przetwarzania danych albo z niezależnym osobnym działaniem różnych „samodzielnych" administratorów, pomimo że w umowie błędnie obie strony nazywa się współadministratorami[449].

Praktycznym przykładem obrazującym relację polegającą na współadministrowaniu danymi osobowymi jest sytuacja opisana w Opinii 1/2010 Grupy Roboczej Art. 39[450], gdzie podmiot świadczący usługi rekrutacji X współpracował z przedsiębiorcą poszukującym

[449] M. Czaplińska, *Dokumentowanie współadministrowania danymi osobowymi*, LEX/el. 2018; https://sip-1lex-1pl-1heg2dlkx07f8.han3.lib.uni.lodz.pl/#/publication/470111308/czaplinska-magdalena-dokumentowanie-wspoladministrowania-danymi-osobowymi?keyword=czapli%C5%84ska&cm=SREST (dostęp: 2023-06-21).
[450] Opinia 1/2010 Grupy Roboczej Art. 29, s. 21.

pracowników Y. Podmioty zawarły umowę, zgodnie z którą firma X jako przetwarzający przetwarza dane osobowe kandydatów w imieniu firmy Y będącej administratorem danych. Jednocześnie jednak podmiot X jest administratorem danych osób poszukujących pracy, stanowiących zbiór globalny, a nie tylko danych z CV przekazywanych przez przedsiębiorcę Y. Zdaniem przedstawicieli Grupy art. 29, pomimo umownego przypisania roli przetwarzającego, podmiot X należy uznać za wspólnie administrującą danymi z przedsiębiorcą Y, w zakresie danych z rekrutacji w przedsiębiorstwie Y.

W kwestii współadministrowania wypowiedział się także TSUE w sprawie *Fashion ID GmbH & Co.KG przeciwko Verbraucherzentrale NRW eV oraz Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein przeciwko Wirtschaftsakademie Schleswig-Holstein GmbH.*

W pierwszym wyroku TSUE wyjaśnił, że operator witryny internetowej uczestniczy w określaniu celów (i sposobów) przetwarzania danych, umieszczając w witrynie internetowej wtyczkę społecznościową, aby zoptymalizować reklamy swoich towarów poprzez uczynienie ich bardziej widocznymi w sieci społecznościowej. Trybunał uznał, że przedmiotowe operacje przetwarzania zostały przeprowadzone w interesie gospodarczym zarówno operatora witryny internetowej, jak i dostawcy wtyczki społecznościowej.

W drugim wyroku, jak zauważył TSUE, przetwarzanie danych osobowych poprzez statystyki odwiedzających fanpage ma w szczególności pozwolić Facebookowi na poprawę jego systemu reklam, jakie emituje on za pośrednictwem swego portalu, a administratorowi fanpage'a na uzyskanie statystyk do celów zarządzania promocją jego działalności. Każdy podmiot w tym przypadku realizuje swój własny interes, ale obie strony uczestniczą w określaniu celów (i sposobów) przetwarzania danych osobowych w odniesieniu do osób odwiedzających fanpage'a. Przykładem praktycznym współadministrowania mogą być także relacje wynikające ze spółki cywilnej, czy konsorcjum, w których istotę wpisane jest współdziałanie, co na gruncie RODO oznacza wspólne określenie celów i sposobów działania w obszarze przetwarzanych tam danych osobowych, np., w sferze działań organizacyjnych, związanych ze wspólną obsługą korespondencji, czy działaniami promocyjnymi.

Współadministrowanie jest możliwe także w ramach grupy przedsiębiorstw w rozumieniu art. 4 ust. 19 RODO, który stanowi, że grupa przedsiębiorstw oznacza „przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane". W grupie przedsiębiorstw współadministrowanie może występować w wybranych procesach biznesowych. Jeżeli dochodzi zatem do wspólnego decydowania o celach i sposobach przetwarzania danych osobowych, to można przyjąć, że w tej części stosunków biznesowych

wyłączone zostaje sprawowanie kontroli przez jedno przedsiębiorstwo nad innym. W relacji współadministrowania brak jest charakterystycznych dla grupy przedsiębiorstw działań dotyczących kontroli, z uwagi na fakt, że podejmowanie decyzji co do celu i sposobu przetwarzania danych osobowych dokonywane jest wspólnie przez administratorów, którymi są niezależnie poszczególne podmioty z grupy. W pozostałych procesach biznesowych, innych niż te, które objęte są współadministrowaniem, możliwe jest określenie stosunków biznesowych w sposób pozostawiający relację przedsiębiorstwo sprawujące kontrolę, czyli przedsiębiorstwo wpływające na podejmowane decyzje – przedsiębiorstwo przez nie kontrolowane, czyli przedsiębiorstwo pozbawione możliwości kontrolowania innych. W praktyce trudności współadministrowania w takiej formule mogą być związane z koniecznością precyzyjnego określenia faz procesów biznesowych wspólnych w rozumieniu współadministrowania danymi i ich oddzielenia od tych etapów przetwarzania danych osobowych, co do których nie będzie możliwe wspólne decydowanie o sposobach i celach przetwarzania, bo mogą nie być one spójne organizacyjnie, wizerunkowo, a nawet finansowo.

W praktyce stosunek współadministrowania będzie można w stosunku do pewnych procesów przetwarzania identyfikować także w przypadku działania grupy spółek, która zgodnie z obowiązującym od.10.2022 r. art. 4 § 1 pkt 51 k.s.h. definiowana jest jako – spółka dominująca i spółka albo spółki zależne, będące spółkami kapitałowymi, kierujące się zgodnie z uchwałą o uczestnictwie w grupie spółek wspólną strategią w celu realizacji wspólnego interesu (interes grupy spółek), uzasadniającą sprawowanie przez spółkę dominującą jednolitego kierownictwa nad spółką zależną albo spółkami zależnymi. Do tej pory w Krajowym Rejestrze Sądowym nie zarejestrowano jednak formalnie żadnej grupy spółek na gruncie nowego prawa holdingowego, co wpływa istotnie na ograniczenia możliwości prowadzenie badań nad praktyką stosowania tych nowych rozwiązań prawnych[451].

Istotą współadministrowania jest podejmowanie decyzji w zakresie celów i sposobów przetwarzania, a nie sam udział więcej niż jednego podmiotu w procesie przetwarzania. Specyfika relacji współadministrowania polega przede wszystkim na tym, że administratorzy wspólnie ustalają cele i sposoby przetwarzania, a także wspólnie realizują obowiązki wynikające z przepisów RODO i podejmują procesy przetwarzania. Tym samym nie dochodzi między tymi podmiotami do powierzenia ani udostępnienia danych, ponieważ

451 Zamiar wprowadzenia prostej spółki akcyjnej spotkał się ze zdecydowaną krytyką przeważającej części doktryny (zob. A. Kappes, *Prosta spółka akcyjna - czy rzeczywiście prosta i czy potrzebna? Uwagi do projektu nowelizacji Kodeksu spółek handlowych, wprowadzającego prostą spółkę akcyjną (projektowane art. 300(1) – 300(121) k.s.h.*, PPH 2018/5, s. 10 i n.).

przetwarzają dane wspólnie, w ramach ustalonych celów. W takim przypadku konieczne jest spełnienie obowiązku wynikającego z art. 26 ust. 1 RODO, który stanowi, że „w drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą". Wspólne ustalanie celów i sposobów przetwarzania wynikające z omawianego przepisu nakazuje dokonanie odpowiedniego podziału obowiązków w relacjach wynikających ze sfery wewnętrznej działania współadministratorów oraz w relacjach wynikających ze sfery zewnętrznej działania współadministratorów, tj. w relacjach dotyczących osób, których dane dotyczą, podmiotów przetwarzających, organów nadzoru i sądów.

Współadministratorzy mają obowiązek dokonać formalnego podziału obowiązków oraz odpowiedzialności za ich realizację w zakresie (określającym przynajmniej wykonywanie praw) osób, których dane dotyczą, i obowiązków informacyjnych. Takie działanie jest konieczne, po pierwsze po to, aby obronić się przed zarzutem, że administrator nie wypełnił swoich obowiązków, czym stwarzał zagrożenie naruszenia praw osób, których dane dotyczą, a po drugie, aby ograniczyć własne ryzyko związane z odpowiedzialnością za działania innego administratora. Potwierdza to motyw 79 RODO który wskazuje, że „ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora." Na bazie w/w motywu preambuły RODO podjęto próbę określenia kryteriów odpowiedzialności współadministratorów dotyczących wypełniania obowiązków wynikających z RODO. Chodzi tu o przejrzysty i transparentny podział zadań i obowiązków, zagwarantowanie rozliczalności przez każdego ze współadministratorów, precyzja ustaleń, zgodność ustaleń ze stanem faktycznym i rzeczywistymi ramami współpracy[452].

[452] K. Witkowska-Nowakowska [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 614.

Z regulacji art. 26 RODO wynika, że obowiązkiem współadministratorów jest co najmniej dokonanie odpowiedniego podziału obowiązków w relacjach wynikających ze sfery zewnętrznej działania współadministratorów, tj. w relacjach dotyczących osób, których dane dotyczą, podmiotów przetwarzających, organów nadzoru i sądów. W konsekwencji w drodze wspólnych uzgodnień współadministratorzy powinni dążyć do możliwie precyzyjnego określenia zadań i obowiązków każdego z nich, aby w każdym z procesów przetwarzania danych osobowych składających się na wspólny projekt możliwe było sprawne zrealizowanie ich praw. Podział uzgodnień powinien być zdeterminowany czynnościami faktycznymi przydzielonymi każdej ze stron. Nie sposób bowiem zaakceptować praktyki, w której realizując różne procesy przetwarzania składające się na wspólny cel, podmioty przyjmują na siebie np. tożsame obowiązki informacyjne. Podobnie należy ocenić sytuację, w której każdy z administratorów, posiadając odmiennie uregulowany we własnym systemie ochrony danych osobowych sposób komunikowania o zgłoszonych prawach osób, których dane dotyczą, przyjmie do wykonania w ramach uzgodnień procedury drugiego administratora, których zastosowanie ze względów organizacyjnych i technicznych nie będzie mogło zostać wykonane w praktyce. W pierwszej kolejności zatem najważniejsze z punktu widzenia roli administratorów pozostających w relacji współadministrowania jest określenie celu przetwarzania danych. Z punktu widzenia praktycznego powinno to się odbyć poprzez wskazanie konkretnych procesów przetwarzania danych, którymi dla przykładu mogą być np. wspólne akcje marketingowe, działania informacyjne o usługach i produktach, newsletter.

W art. 26 RODO prawodawca posługuje się określeniem „uzgodnienia", co odczytywać można jako formę wewnętrznych ustaleń między administratorami, nieprzybierającego jednak postaci sformalizowanego porozumienia między podmiotami publicznymi lub umowy między podmiotami prywatnymi albo między podmiotem publicznym a prywatnym. Uzgodnienia powinny być określone w „przejrzysty sposób," co tłumaczyć można jako wymóg jasnego i jednoznacznego wskazania obowiązków i związanej z nimi odpowiedzialności[453]. W praktyce stosunek współadministrowania zwykle znajduje oparcie w postanowieniach umownych, w których strony określają zakres swoich uprawnień i obowiązków, ustalając cele i sposoby współdziałania, które przekładają się na ustalenie celów i sposobów przetwarzania danych osobowych[454].

[453] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...*, s. 330.
[454] M. Sakowska-Baryła, *Ogólne rozporządzenie...*, s. 298.

W konsekwencji należy przyjąć, że w praktyce zakres ustaleń dotyczących współadministrowania powinien odnosić się do obowiązków administratorów i uwzględnić takie działania jak:

- analiza obecnego i przyszłego procesu biznesowego;
- wskazanie poszczególnych zadań związanych z przetwarzaniem wraz z określeniem administratorów zaangażowanych w poszczególne fazy przetwarzania,
- zbadanie podstaw legalności przetwarzania danych,
- analiza procesów przetwarzania pod kątem udokumentowania kwestii związanych z rejestrem czynności przetwarzania, przeglądem wdrożonych środków organizacyjno-technicznych i ich uaktualnianiem
- wybór środków technicznych dotyczących infrastruktury IT i bezpieczeństwa danych,
- rozkład obowiązków dotyczących klauzul informacyjnych,
- zakres powierzenia przetwarzania danych osobowych i związany z tym audyt standardów przetwarzania danych u podmiotów przetwarzających,
- zasady udzielania zgód na podpowierzenie i dokumentowania takich zgód,
- sposób realizacji praw osób, których dane dotyczą,
- wykonywanie obowiązków informacyjnych wobec osób, których dane dotyczą, oraz ich odbiorców w sytuacji wykonania praw m.in. do sprostowania, usunięcia, uzupełnienia, kopii danych, przeniesienia danych,
- szacowanie ryzyka i dokonywanie oceny ryzyka,
- zgłaszanie incydentów i naruszeń,
- rejestr naruszeń,
- zasady wydawania i ewidencjonowania upoważnień i poleceń przetwarzania danych,
- procedury usuwania naruszeń i podejmowanych działań naprawczych,
- procedury wykonywania obowiązków administracyjnych wobec organu nadzoru,
- relacje dotyczące dochodzenia roszczeń cywilnych,
- obrona interesów w sprawach wynikających z realizacji praw osób, których dane dotyczą,
- zasady rozpatrywania roszczeń pomiędzy współadministratorami
- zasady postępowania w przypadku ewentualnych transferów danych do państw trzecich, z uwzględnieniem koniecznych do zastosowania dodatkowych mechanizmów ochrony.

Artykuł 26 RODO nie wskazuje zakresu dokumentowania uzgodnień, ale stanowi, że zasady uzgodnień pomiędzy współadministratorami powinny być udostępniane osobom, których dane

dotyczą. Osoby te muszą zostać poinformowane o wszystkich administratorach, którzy wspólnie decydują o celach i sposobach przetwarzania danych. RODO nie przesądza o formie udostępnienia ww. informacji, jednak wydaje się, że powinna być ona adekwatna do formy zbierania danych oraz kompatybilna ze sposobem przekazywania osobie, której dane dotyczą, innych informacji wymaganych przez RODO, m.in. na mocy art. 13 lub 14 RODO[455].

RODO stanowi o udostepnieniu zasadniczej treści uzgodnień osobom, których dane dotyczą, RODO nie określa jednak wprost, o które uzgodnienia tu chodzi. W tym stanie rzeczy zasadne wydaje się uznawać za zasadnicze te elementy uzgodnień, które pozwalają osobie, której dane dotyczą, zorientować się w okolicznościach przetwarzania jej danych osobowych przez współadministratorów, a w konsekwencji zrealizować przysługujące jej prawa – zarówno te, które wynikają z rozdziału III RODO, jak i takie, które wyprowadzić można z pozostałych przepisów tego rozporządzenia, jak również z innych przepisów prawa. Powinny być to miedzy innymi uzgodnienia, które umożliwiają podmiotowi danych w razie potrzeby zrealizować prawo do wniesienia skargi do organu nadzorczego oraz roszczenia o charakterze cywilnoprawnym wynikające z art. 79 i 82 RODO, jak i z innych przepisów pozwalających jednostce na dochodzenie jej praw.

Biorąc pod uwagę treść art. 26 RODO, za zasadnicza uznać należy te cześć uzgodnień pomiędzy administratorami, która ujawnia ich tożsamość, cele i sposoby przetwarzania danych, a także zakresy ich odpowiedzialności dotyczącej wypełniania obowiązków wynikających z tego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw[456].

Artykuł 26 RODO wydaje się wyraźnie zatem akcentować konieczność osiągnięcia porozumienia, konsensusu, a więc żaden ze współadministratorów nie może narzucić drugiemu wyboru celów i sposobów przetwarzania. To wyklucza sytuację powstania współadministrowania, gdy akt woli wynika jedynie pośrednio (ale w sposób dostateczny) z zachowania, które zmierza do innego celu, tj. per factia concludentia. Do tej pory nie wypracowana została przez judykaturę ocena tego jakie rodzaje zachowań w przedmiocie współadministrowania mogą z uwagi na dany układ sytuacyjny stanowić wyraz oświadczenia woli, mimo że same te zachowania (lub ich wytwory) w oderwaniu od kontekstu nie miałyby tego znaczenia. W orzeczeniach, które dotyczą innych stanów faktycznych nie znajdujemy

[455] M. Czaplińska, *Dokumentowanie współadministrowania...*
[456] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 298.

odniesień do omawianego zagadnienia. W kontekście najnowszego orzecznictwa TSUE[457] należy jednak zwrócić uwagę na wykładnię samego pojęcia „wspólnie ustala." Dla zaistnienia takiego działania nie jest konieczne, aby wszystkie decyzje o celach i sposobach przetwarzania na drodze wspólnych ustaleń. Do uznania za współadministratorów wystarczyć więc może np. niezależne od siebie podejmowanie decyzji co do poszczególnych operacji składających się na większy proces przetwarzania danych osobowych[458].

Powyższe zagadnienia mają doniosłe znaczenie dla oceny poprawności stosowania przepisów. Z Wytycznych 7/2020 EROD wynika, że współadministratorzy w przejrzysty sposób określają i uzgadniają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO. Określenie zakresu ich odpowiedzialności dotyczy w szczególności wykonywania przez osoby, których dane dotyczą, przysługujących im praw oraz obowiązków w odniesieniu do udzielania informacji. Oprócz tego podział odpowiedzialności powinien obejmować inne obowiązki administratora, takie jak obowiązki dotyczące ogólnych zasad ochrony danych, podstawy prawnej, środków bezpieczeństwa, obowiązku powiadamiania o naruszeniu ochrony danych, oceny skutków dla ochrony danych, korzystania z usług podmiotów przetwarzających, przekazywania danych do państw trzecich oraz kontaktów z osobami, których dane dotyczą, i organami nadzorczymi. Każdy współadministrator ma obowiązek zapewnić, że posiada podstawę prawną do przetwarzania danych oraz że dane nie są dalej przetwarzane w sposób niezgodny z celami, dla których zostały pierwotnie zgromadzone przez administratora udostępniającego dane[459].

Dla określenia odpowiedzialności poszczególnych współadministratorów podstawą powinien być stan faktyczny i działania dokonywane przez nich w rzeczywistości. Naruszenie powyższych obowiązków naraża współadministratorów na odpowiedzialność z art. 83 ust. 4 RODO. Treść uzgodnień pomiędzy współadministratorami nie jest dla organu nadzorczego wiążąca i podlega ocenie przez ten organ. W przypadku rozbieżności pomiędzy treścią

[457] Sprawa C-210/16, w której Trybunał uznał, że: „administrator fanpage'a prowadzonego na *Facebooku,* taki jak *Wirtschaftsakademie*, uczestniczy, podejmując działania polegające na ustaleniu parametrów zależnych w szczególności od jego użytkowników docelowych, jak również od celów w zakresie zarządzania lub promocji jego działalności, w określeniu celów i sposobów przetwarzania danych osobowych osób odwiedzających jego „fanpage'a", czy sprawa C-40/17, *Fashion ID*, dotycząca odpowiedzialności za przetwarzanie danych wynikające z umieszczenia przycisku „Lubię to" *Facebooka* na własnej stronie internetowej, Trybunał potwierdził model „pluralistycznej kontroli" przetwarzania danych osobowych przez administratorów. Podkreślił także, że do uznania, iż mamy do czynienia ze wspólnym określaniem celów i sposobów, może wystarczyć, że konkretne określanie ma miejsce tylko przez część czasu trwania przetwarzania i, że przetwarzanie danych w różnych celach przez różnych administratorów (także gdy są określane w różnym czasie bądź równolegle, niezależnie od siebie) może w określonych sytuacjach konstytuować jedno, wspólne przetwarzanie danych osobowych

[458] M. Czerniawski, *Instytucja współadministrowania a pojęcie „ustalania" celów i sposobów przetwarzania danych osobowych – zarys problemu* [w:] *Rok RODO,* Warszawa 2019, s. 13–20.

[459] Wytyczne 7/2020 EROD.

uzgodnień a stanem faktycznym rozstrzygnięcie organu powinno być oparte na ustaleniach faktycznych i ocenie wszelkich istotnych okoliczności konkretnej operacji przetwarzania danych, a więc na podstawie rzeczywistego zakresu obowiązków poszczególnych współadministratorów. W kontekście ewentualnej odpowiedzialności za naruszenie przepisów o ochronie danych osobowych powinna być więc oceniana rzeczywista funkcja pełniona przez poszczególnych współadministratorów przy przetwarzaniu danych osobowych, a nie ich wzajemne ustalenia[460]. Brak omawianych powyżej uzgodnień może stanowić zarzut naruszenia przepisów o ochronie danych i prowadzić do odpowiedzialności.

Obowiązki dokumentacyjne administratora

Posiadanie statusu administratora nakłada szereg obowiązków, dotyczących zorganizowania procesu przetwarzania danych, realizacji praw osób, których dane dotyczą i odpowiedzialności za naruszenia w tym zakresie.

Przede wszystkim przetwarzanie danych powinno następować zgodnie z prawem, przy zastosowaniu odpowiednich środków organizacyjnych i technicznych zapewniających ochronę przed udostępnieniem osobom nieupoważnionym, uszkodzeniem lub zniszczeniem[461]. Status administratora ma walor funkcjonalny – dostarcza kryteriów określenia, kto kontroluje procesy przetwarzania danych. Innymi słowy, określenie kto jest administratorem w procesie przetwarzania danych, stanowi pierwszy krok do ustalenia, kto w danym przypadku odpowiada za zgodność przetwarzania danych osobowych z przepisami prawa, w tym za realizację wynikających z nich zasad, wprowadzenie należytych zabezpieczeń oraz zapewnienie wykonywania uprawnień przez osoby, których dane dotyczą. Ustalenie, że konkretny podmiot jest administratorem, jest równoznaczne z przypisaniem mu szeregu obowiązków określonych w RODO oraz odpowiedzialności za przetwarzanie danych dokonywanych przez ten podmiot samodzielnie, jak również za pośrednictwem jego personelu oraz podmiotów wobec niego zewnętrznych. W zakresie przetwarzania danych osobowych administrator odpowiada nie tylko za własne działania i decyzje oraz zaniechania, ale także innych podmiotów, które wybrał do dokonywanego w jego imieniu i na jego rzecz przetwarzania danych osobowych.

Obowiązki administratora nie mają jednolitego charakteru. Część z nich dotyczy sfery wewnętrznej działania organizacji, część relacji wynikających z powierzenia przetwarzania

[460] M. Czerniawski, Glosa do wyroku TSUE z 5.6.2018 r., C-210/16, *Wirtachtsakademie Scheswig-Holstein GmbH*, LEX

[461] M. Ganczar, *Obowiązki administracji publicznej w zakresie ochrony danych osobowych* [w:] *Ochrona danych osobowych skuteczność regulacji*, Warszawa 2009 r. s. 121.

danych i relacji z podmiotami danych. Jeszcze inne obowiązki dotyczą obsługi naruszenia, praw podmiotu danych, czy kontaktu z organem nadzoru .

Omówienie obowiązków administratora danych osobowych rozpocząć należy od sfery wewnętrznej działania administratora i przedstawienia zagadnienia podstawowego jakim jest obowiązek wykazania realizacji zasad zawartych w art. 5 RODO, tj. wykazanie zasady rozliczalności. W art. 5 ust. 2 RODO wyraźnie wprowadza się zasadę rozliczalności, co oznacza, że: – administrator jest odpowiedzialny za przestrzeganie zasad określonych w art. 5 ust. 1 RODO oraz że – administrator musi być w stanie wykazać przestrzeganie zasad określonych w art. 5 ust. 1 RODO. Zasada ta została opisana w kontekście danych już w opinii Grupy Roboczej Art. 29 z 13.07.2010[462], w której Grupa robocza Art. 29 zauważa, że zasada rozliczalności jako taka nie jest nowa. Jej wyraźne uznanie można zauważyć w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD) dotyczących ochrony prywatności przyjętych w 1980 r. Zgodnie z zawartą w nich zasadą rozliczalności: „Administrator danych powinien odpowiadać za przestrzeganie środków, które nadają skuteczność (istotnym) zasadom wymienionym powyżej".

W tym miejscu wspomnieć należy, że Organizacja Współpracy Gospodarczej i Rozwoju jest autorem licznych dokumentów omawiających zasady postepowania z danymi, takich jak „Przewodnik OECD w sprawie ochrony prywatności i transgranicznego przepływu danych osobowych", gdzie określone zostały zasady dotyczące prywatności i danych osobowych[463], których zachowanie ma wpływ na omawianą zasadę. Celem włączenia zasady rozliczalności do RODO i uczynienia jej główną zasadą było podkreślenie, że administratorzy muszą wdrożyć odpowiednie i skuteczne środki oraz być w stanie wykazać zgodność z przepisami. Zasada rozliczalności została doprecyzowana w art. 24 RODO, który stanowi, że administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z przepisami RODO i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Zasada rozliczalności znajduje również odzwierciedlenie w art. 28 RODO, w którym określono obowiązki administratora podczas korzystania z usług podmiotu przetwarzającego. Zasada rozliczalności jest skierowana bezpośrednio do administratora. Niektóre z bardziej szczegółowych przepisów dotyczą jednak zarówno administratorów, jak i podmiotów przetwarzających, np. przepisy dotyczące uprawnień organów nadzorczych

[462] Opinia 00062/10/PL WP 173.

[463] M. Ganczar, *Obowiązki przedsiębiorców w zakresie gromadzenia, przetwarzania i udostępniania danych osobowych* [w:] *Prawo do prywatności w kontekście prowadzenia działalności gospodarczej* [w:] *Człowiek z perspektywy biznesu*, red K. Machowicz, Lublin 2009 s. 121.

zawarte w art. 58 RODO. Zarówno administratorzy, jak i podmioty przetwarzające mogą podlegać karze pieniężnej w przypadku naruszenia dotyczących ich obowiązków przewidzianych w RODO. Oba te podmioty ponoszą bezpośrednią odpowiedzialność względem organów nadzorczych z tytułu obowiązku przechowywania i dostarczania na żądanie odpowiedniej dokumentacji, współpracy w przypadku prowadzenia postępowania i wykonywania rozkazów administracyjnych. Jednocześnie należy wskazać, że podmioty przetwarzające muszą zawsze stosować się do instrukcji administratora i działać wyłącznie na ich podstawie[464].

Jak zauważa P. Fajgielski „zgodnie z określoną w art. 5 ust. 2 RODO zasadą rozliczalności (ang. accountability) administrator jest odpowiedzialny za przestrzeganie omówionych wcześniej zasad dotyczących przetwarzania danych i musi być w stanie wykazać realizację tego obowiązku. W literaturze wskazuje się na podstawowy charakter zasady rozliczalności stanowiącej na kanwie RODO całkowicie nowe rozwiązanie.[465] Katalog zasad przetwarzania danych zawarty w rozporządzeniu jest swoistym odpowiednikiem wyliczenia obowiązków ciążących na administratorze[466]. Zasada rozliczalności nakłada bowiem na administratorów i podmioty przetwarzające odpowiedzialność za przestrzeganie przepisów dotyczących przetwarzania danych oraz wymaga, aby podmioty te były w stanie to wykazać. Oznacza to nową jakość w systemie ochrony danych osobowych, polegającą na proaktywnym podejściu administratorów do przetwarzania danych w celu wykazania realizacji zasady rozliczalności, czyli w gruncie rzeczy wszystkich zasad wyszczególnionych w art. 5 ust. 1 RODO[467]. W tym miejscu warto dodać, że istotę rozliczalności poprawnie regulowała definicja zamieszczona w nieobowiązującym już rozporządzeniu MSWiA z 29.04.2004 r.[468], zgodnie z którą rozliczalność to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi (par. 2 pkt 7 przywołanego aktu prawnego).

Stwierdzenie, że administrator powinien być w stanie wykazać przestrzeganie zasad, odczytywać można jako nałożenie na administratora ciężaru dowodowego w zakresie przestrzegania zasad przetwarzania danych. W razie sporu z osobą, której dane dotyczą, albo z organem nadzorczym, administrator powinien być w stanie przedstawić dowody na to, że

[464] Wytyczne 7/2020 EROD.
[465] P. Drobek [w:] E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych*, Warszawa 2018, komentarz do art. 5.
[466] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...*, s. 143.
[467] A. Nerka [w:] *Ogólne rozporządzenie...*, red. M. Sakowska-Baryła, s. 147.
[468] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).

przestrzega zasad. Dowodami takimi mogą być dokumenty dotyczące przetwarzania i ochrony danych. Dlatego też, pomimo braku wyraźnego wymogu wynikającego z przepisów komentowanego rozporządzenia, zasadne wydaje się prowadzenie dokumentacji przetwarzania danych, obejmującej wskazanie działań, jakie zostały podjęte dla zapewnienia zgodności przetwarzania i ochrony danych z wymogami określonymi w rozporządzeniu (np. przeprowadzonej analizy ryzyka i doboru odpowiednich zabezpieczeń)[469]. Rozumienie zasady rozliczalności powinno następować w taki sposób, że prawodawca przerzuca ciężar z organu na administratora, który będzie musiał wykazywać, że jego działania w zakresie przetwarzania danych osobowych są zgodne z przepisami RODO. Należy to rozumieć jako „obowiązek aktywnego działania, wykazywania inicjatywy, bez oczekiwania na skargi i wnioski klientów lub zarzuty i rekomendacje organów nadzorczych"[470].

Zgodnie z nowym podejściem RODO nie zawiera generalnych wytycznych ani co do struktury dokumentacji, ani co do sposobu jej prowadzenia, ani – w końcu – co do jej merytorycznej treści. Swoboda, jaką pozostawiono administratorom i podmiotom przetwarzającym w zakresie zapewnienia ochrony danych osobowych, przejawia się między innymi w tym, że mogą one nie tylko samodzielnie kształtować, ale także opisywać stosowane metody przetwarzania danych osobowych, związane z nimi procedury, jak również zastosowane zabezpieczenia techniczne i organizacyjne. Chodzi o to, by opracowywane dokumenty mogły być jak najbardziej praktyczne, dostosowane do potrzeb konkretnego podmiotu. Idzie też o to, by ograniczyć przypadki tworzenia dokumentów zbędnych, takich, które w kontekście skali i sposobu przetwarzania danych przez dany podmiot nie są użyteczne[471].

Wymagania nakładane na administratorów przez RODO są tak ukształtowane, że prowadzenie odpowiedniej dokumentacji jest nie tylko konieczne, ale też celowe. Z tego punktu widzenia zawarte w RODO regulacje można podzielić na dwa rodzaje. Pierwsze to takie, w których wskazano obowiązki, z których wprost wynika konieczność opracowania pewnych konkretnych dokumentów[472].

Prezes Urzędu Ochrony Danych Osobowych podaje tu następujące przypadki:

1. prowadzenie rejestru czynności przetwarzania i zakres rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;

[469] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...*, s. 157.
[470] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego*, Warszawa 2016.
[471] M. Jagielski, *Dokumentacja ochrony danych ze wzorami*, Warszawa 2019, s. 15.
[472] M. Jagielski, *Dokumentacja ochrony…*, s. 16

2. zgłaszanie naruszenia ochrony danych do organu nadzorczego (UODO) – art. 33 ust. 3 RODO;
3. prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
4. zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7 RODO[473].

Cechą charakterystyczną powyższych rozwiązań jest to, że RODO wskazuje przy ich pomocy konkretne treści, które adresat jest zobowiązany opracować. W tym zakresie sporządzenie dokumentu staje się koniecznością, gdyż w przeciwnym wypadku administrator lub podmiot przetwarzający nie zrealizowałby nałożonego nań konkretnego obowiązku.

Przypadek drugi to sytuacja, gdy RODO, określając w sposób ogólny zasady i wymagania, którym musi odpowiadać przetwarzanie danych osobowych, tak je formułuje, że ich wykonanie nie będzie możliwe albo bardzo utrudnione, jeśli nie obejmie opracowania stosownych dokumentów. Kluczową rolę w tym względzie odgrywa wyrażona w art. 5 ust. 2 RODO zasada rozliczalności[474].

Obowiązki w zakresie bezpieczeństwa danych

Idea rozliczalności została rozwinięta i doprecyzowana w art. 24 ust. 1 RODO. Przepis ten nakłada na administratorów obowiązek wdrożenia takich środków technicznych i organizacyjnych, które zapewnią, że przetwarzanie będzie odbywało się zgodnie z rozporządzeniem i administratorzy będą w stanie to wykazać. Realizując wskazany obowiązek, administratorzy powinni uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, a także mają obowiązek poddawania przeglądom i uaktualniania zastosowanych środków, jeśli tylko zajdzie taka potrzeba. Powyższy przepis, analogicznie do art. 5 ust. 2 RODO, nie nakłada wprost obowiązku przygotowania konkretnych dokumentacji, jednak nie ulega wątpliwości, że nie można zrealizować wskazanych w nim zaleceń, unikając tworzenia dokumentów[475].

Inną regulacją doprecyzowującą art. 5 RODO jest art. 32 ust. 1 RODO, z którego wynika, że administrator jest zobowiązany do zastosowania środków technicznych

[473] *UODO, Dokumentacja przetwarzania danych osobowych zgodnie z RODO*; https://uodo.gov.pl/ pl/138/273 (dostęp: 21.02.2019 r.).
[474] M. Jagielski, *Dokumentacja ochrony*… , s. 16–17.
[475] M. Jagielski, *Dokumentacja ochrony*… , s. 17.

i organizacyjnych odpowiadających ryzyku naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Przepis precyzuje, że decydując o środkach technicznych i organizacyjnych należy wziąć pod uwagę stan wiedzy technicznej, koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze. Z przytoczonego przepisu wynika, że ustalenie odpowiednich środków technicznych i organizacyjnych jest procesem dwuetapowym. W pierwszej kolejności istotne jest określenie poziomu ryzyka, jakie wiąże się z przetwarzaniem danych osobowych przy uwzględnieniu kryteriów wskazanych w art. 32 RODO, a następnie należy ustalić, jakie środki techniczne i organizacyjne będą odpowiednie, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Ustalenia te, w stosownym przypadku zgodnie z lit. b)[476] i d)[477], powinny obejmować środki takie, jak zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Artykuł 32 ust. 2 RODO stanowi, że oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych[478].

Unijne rozporządzenie nakłada zatem na administratora i podmiot obowiązek dokonania oceny ryzyka, jakie wiąże się z przetwarzaniem danych, i przyjęcia zabezpieczeń odpowiednich do stopnia tego ryzyka. W rozporządzeniu nie przewidziano przepisów wykonawczych, które precyzowałyby wymagania dotyczące zabezpieczeń, a jedynie możliwość wydawania wspomnianych wcześniej instrumentów o charakterze *soft law,* np. w postaci zatwierdzonych kodeksów postępowania czy wytycznych. Brak wyraźnych unormowań prawnych określających rodzaje technicznych i organizacyjnych środków zabezpieczenia danych skłania do poszukiwania wskazówek, które mogą być pomocne administratorom do spełnienia wymogów ogólnie uregulowanych w komentowanym rozporządzeniu. Tego rodzaju

[476] Tj. administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

[477] Tj. administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

[478] Decyzja UODO z 21.04.2021 r., znak sprawy DKN.5130.3114.2020.

wskazówek dostarczyć mogą normy techniczne odnoszące się do zabezpieczenia informacji. W obecnym stanie prawnym można zatem spodziewać się wzrostu zainteresowania, a co za tym idzie zwiększenia znaczenia norm technicznych. Warto jednak podkreślić, że stosowanie tego rodzaju norm jest dobrowolne i nie stanowi wymogu określonego przepisami prawa[479].

Powyższe regulacje oznaczają zatem, że pod rządami RODO mamy do czynienia z odejściem od dotychczasowego formalnego i zasadniczo reaktywnego modelu ochrony danych na rzecz podejścia dynamicznego opartego na modelu ochrony proaktywnej, prewencyjnej, o zindywidualizowanym charakterze, bez nałożonych bezpośrednio przez prawodawcę unijnego formalnych obowiązków w zakresie techniczno-organizacyjnych rozwiązań, na których powinno być oparte przetwarzanie[480].

Praktycznym przykładem problemu dokumentowania obowiązku dokonania oceny ryzyka naruszenia praw lub wolności osób fizycznych jest stanowisko Wojewódzkiego Sądu Administracyjnego w Warszawie zawarte w wyroku o sygnaturze II SA/Wa 2826/19 z 26.08.2020 r. W wyroku tym Sąd uznał, że „czynności o charakterze techniczno – organizacyjnym leżą w gestii administratora danych osobowych, ale nie mogą być dobierane w sposób całkowicie swobodny i dobrowolny, bez uwzględnienia stopnia ryzyka oraz charakteru chronionych danych osobowych", Podkreślenia wymaga w tym momencie, że sklasyfikowanie i zdefiniowanie ryzyka jest bardzo trudne ze względu na dużą ilość odnoszących się do niego określeń i budowę jego znaczenia na podstawie składników zmieniających się w zależności od konkretnego przypadku[481]. Na zmianę okoliczności istotnych dla oceny ryzyka będą miały takie zdarzenia jak: zmiany organizacyjne, zmiany środków technicznych (np. wprowadzenie nowego oprogramowania), praca zdalna, wprowadzenie prewencyjnej kontroli pracowników na obecność w ich organizmach alkoholu lub środków działających podobnie do alkoholu.

Obowiązki wynikające z zasady legalności, rzetelności i przejrzystości przetwarzania danych

Administrator odpowiedzialny jest za spełnienie obowiązków, odnoszących się do przestrzegania zasad rzetelności i przejrzystości przetwarzania danych wobec osoby, której

[479] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...,* s. 371. Szerzej na temat relacji między normami technicznymi a normami prawnymi por. B. Fischer, *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*, Warszawa 2017, s. 75 i n.
[480] B. Fischer, *Pojęcie analizy ryzyka przy przetwarzaniu danych osobowych* [w:] B.Fisher, *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia*, MoP 2014/9.
[481] B. Fischer, *Pojęcie analizy ryzyka...*

dane dotyczą, zasady zgodności z prawem przetwarzania danych osobowych, konieczności spełnienia obowiązku informacyjnego wobec osób, których dane będą przetwarzane oraz, co kluczowe, do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO, w tym by zapewnić ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem danych osobowych. Ponadto powyższe działania administrator musi być w stanie wykazać zgodnie z zasadą rozliczalności wyrażoną w art. 5 ust. 2 RODO.

Naczelną zasadą obowiązującą administratora przy przetwarzaniu danych osobowych jest wyrażona w art. 5 ust. 1 pkt a) RODO zasada legalności i rzetelności, zgodnie z którą przetwarzane musi odbywać się z sposób zgodny z prawem i zarazem rzetelny. Wynika z niej, iż administrator zobowiązany jest do prowadzenia wszelkich operacji na danych osobowych w sposób zgodny z powszechnie obowiązującymi przepisami prawa, i to nie tylko z zakresu ochrony danych osobowych, ale także obejmujących inne gałęzie prawa. Podstawy legalności uregulowane w samym rozporządzeniu RODO zawarte zostały odpowiednio w art. 6[482] (odnoszący się do przetwarzania danych zwykłych) i art. 9[483] RODO

[482] Artykuł 6 Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden z poniższych warunków:
a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

[483] Artykuł 9 1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
2. Ustęp 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:
a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych,

(odnoszący się do przetwarzania danych szczególnej kategorii). Wymieniają one w sposób enumeratywny podstawy prawne do przetwarzania danych osobowych, gwarantując by przetwarzanie danych odpowiadało przesłance zgodności z prawem.

Z zasady rozliczalności wynika także, że dane osobowe powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Administrator powinien zatem pozyskiwać tylko te dane osobowe, które są niezbędne z punktu widzenia założonego przez siebie celu obiektywnie uzasadniającego zbieranie określonych danych. Powyższa zasada oznacza, że nieuprawnione na gruncie przepisów o ochronie danych osobowych jest zbieranie danych nadmiarowych tj. niemających dla administratora znaczenia z punktu widzenia osiągnięcia przez niego celu, jaki z założenia ma służyć zbieraniu i dalszemu przetwarzaniu danych osobowych. Powyższa zasada oznacza także, że w świetle regulacji RODO zabronione jest zbieranie danych na tzw. „wszelki wypadek" czy „na zapas", tj. w zakresie i w ilościach nadmiernych w stosunku do realizowanego celu. Omawiana zasada wymusza zatem na administratorze dokonanie analizy, jakie kategorie danych powinny być bezwzględnie zbierane dla ustalonego wcześniej celu, a które dane pozostają irrelewantne z punktu widzenia celu i interesu administratora.

światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;
i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Obowiązki informacyjne wobec podmiotu danych

Inną formą realizacji zasady rzetelności i przejrzystości są obowiązki informacyjne wobec podmiotu danych. Rozpoczęcie procesu przetwarzania danych osobowych w ramach określonej czynności to moment, w którym aktualizuje się obowiązek informacyjny, o jakim mowa w art. 13 i 14 RODO, a jaki winien spełnić administrator wobec osób fizycznych, których dane będą podlegały przetwarzaniu. Prawo do wiedzy o tym, kto, w jakim celu i na jakiej podstawie przetwarza dane osobowe osoby, której dane dotyczą jest jednym z podstawowych praw wynikających z RODO[484] oraz fundamentalnym elementem ochrony danych osobowych. Realizuje bowiem zasadę przejrzystości, która wynika z art. 5 ust. 1 lit. a RODO i ma gwarantować zapewnienie podmiotowi danych kontroli nad tym, kto, na jakiej podstawie, i w jakim celu przetwarza jego dane osobowe. Poinformowanie osoby, której dane dotyczą o przetwarzaniu jej danych osobowych w przypadku, gdy administrator pozyskuje te dane od innego podmiotu, niż podmiot danych jest szczególnie istotne pod kątem zapewnienia realizacji prawa osoby do ochrony jej danych[485] i spełnienia zasady przejrzystości. Jednocześnie wykonanie tego obowiązku ma zagwarantować poszanowanie prawa do prywatności oraz prawa do autonomii informacyjnej jednostki. Brak realizacji obowiązku informacyjnego czyni bowiem iluzorycznym sprawowanie kontroli nad informacjami wykorzystywanymi przez inny podmiot, co jest esencją prawa do autonomii informacyjnej. W sytuacji, gdy administrator nie poda podmiotowi danych informacji o przetwarzaniu jego danych osobowych, uprawniony nie wiedząc, że jego dane osobowe są przetwarzane, pozbawiony jest możności skorzystania z przysługujących mu na mocy RODO uprawnień dotyczących kontroli przetwarzania danych, tj. prawa dostępu do danych, prawa do ich sprostowania oraz żądania ich usunięcia, prawo do ograniczenia przetwarzania, jak również prawa do sprzeciwu. W związku z powyższym, administrator powinien przekazać podmiotowi danych informacje m.in. dotyczące:

- swojej tożsamości i swoich danych kontaktowych oraz, gdy ma to zastosowanie, tożsamości i danych kontaktowych swojego przedstawiciela;
- gdy ma to zastosowanie – danych kontaktowych inspektora ochrony danych;
- celów przetwarzania, do których mają posłużyć dane osobowe, oraz podstawy prawnej przetwarzania;
- kategorii odnośnych danych osobowych;
- odbiorców danych osobowych lub kategorii odbiorców, jeżeli istnieją;

[484] M. Gawroński, *Prawo do informacji o danych osobowych i obowiązek informacyjny*, LEX/el. 2018.
[485] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679...*

- okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;
- prawa do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz prawa do wniesienia sprzeciwu wobec przetwarzania, a także prawa do przenoszenia danych;
- prawa wniesienia skargi do organu nadzorczego;
- źródła pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych.

Dotychczasowe regulacje prawa do ochrony danych osobowych zawarte w aktach prawa międzynarodowego, przede wszystkim we wcześniejszych niż RODO aktach europejskich, a w szczególności Konwencji 108 i dyrektywie 95/46/WE, pozwalają wskazać na pewne standardy ochrony interesów jednostki w związku z przetwarzaniem jej danych osobowych, do których obok określenia zasad przetwarzania danych oraz zapewnienia nadzoru nad systemem ochrony danych osobowych przez niezależny organ (lub organy) wyposażony w kompetencje w indywidualnych sprawach, każdorazowo należy przyznanie osobie, której dane dotyczą, uprawnień pozwalających na kontrolowanie operacji wykonywanych z użyciem jej danych osobowych.

Standardy te zostały zachowane także na gruncie RODO, tyle tylko, że wraz z rozwojem technicznym, a także na skutek obserwacji praktyki stosowania dotychczasowych przepisów prawa ochrony danych osobowych oraz działań uczestników obrotu prawnego ich dookreślenie nastąpiło w sposób, mający na celu dostosowanie do zmieniających się realiów technicznych i potrzeb[486]. Spełnienie przez administratora obowiązku informacyjnego wobec podmiotu danych ma więc nadal doniosłe znaczenie dla ochrony danych osobowych. Z jednej strony umożliwia osobie, której dane dotyczą kontrolę nad przetwarzaniem jej danych osobowych, z drugiej zaś pozwala administratorowi wykazać rzetelność i przejrzystość przetwarzania danych wobec osoby, której dane dotyczą. Niedopełnienie obowiązku informacyjnego pozbawia możności skorzystania z praw przysługujących na mocy RODO[487].

Zasada prywatności w fazie projektowania oraz domyślnej ochrony danych

Kontynuując rozważania o obowiązkach wynikających wprost z RODO, powiedzieć trzeba, że do innej kategorii obowiązków administratora należą obowiązki z art. 25 RODO,

[486] B. Fischer, M. Sakowska-Baryła, *Realizacja praw osób, których dane dotyczą*, Wrocław 2017, s. 18.
[487] Zob. https://panoptykon.org/poczta-musielismy-sluchac-premiera

który stanowi wprowadza do regulacji prawnej ochrony danych osobowych obowiązek uwzględnienia ochrony danych osobowych w fazie projektowania oraz domyślnej ochrony danych.

W ust. 1 określone zostały czynniki i okoliczności, jakie administrator powinien uwzględnić przy wdrażaniu zabezpieczeń mających na celu realizację ochrony danych w fazie projektowania, ust. 2 określa wymagania odnoszące się do domyślnej ochrony danych, natomiast w ust. 3 wskazano jeden ze sposobów umożliwiających wykazanie wywiązywania się z wskazanych powyżej obowiązków. Artykuł 25 RODO stanowi nowy element regulacji, niemający odpowiednika w dyrektywie 95/46/WE. Zarówno wymóg zapewnienia ochrony prywatności w fazie projektowania, jak też wymóg domyślnej ochrony danych były traktowane w kategoriach dobrych praktyk ochrony danych, natomiast nie miały charakteru wymogów prawnych, wynikających z przepisów prawa unijnego. Również SUODO nie zawierała przepisów nakładających obowiązek uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych[488].

Obowiązki związane z obsługą naruszeń

Odrębnym od omawianych powyżej obowiązków jest obowiązek administratora dotyczący obsługi naruszenia ochrony danych osobowych w tym, jego zgłoszenia do PUODO. Jak już zostało wcześniej wskazane przepisy RODO zobowiązują zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. W RODO ustanowiono wymóg przyjęcia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych, co z kolei ma decydujące znaczenie dla ustalenia, czy w danym przypadku obowiązek zgłoszenia naruszenia ma zastosowanie. Oznacza to, że zdolność do zapobiegania naruszeniom w przypadkach, w których jest to możliwe, oraz zdolność do niezwłocznego reagowania na naruszenia w sytuacjach, w których mimo to dojdzie do ich wystąpienia, stanowią kluczowy element każdej polityki w zakresie bezpieczeństwa danych.

Pojęcie naruszenia ochrony danych osobowych zgodnie z RODO definiowane jest jako „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego

[488] P. Fajgielski, *Komentarz do rozporządzenia nr 2016/679*..., s. 322.

dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych". To, co należy rozumieć pod pojęciem „zniszczenia" danych osobowych, powinno być stosunkowo jasne: pojęcie to odnosi się do sytuacji, w której dane już nie istnieją lub przestały istnieć w postaci, w której administrator mógłby je w jakikolwiek sposób wykorzystać. Znaczenie pojęcia „uszkodzenie" również powinno być stosunkowo oczywiste: odnosi się ono do sytuacji, w której dane osobowe zostały zmodyfikowane, zniekształcone lub przestały być kompletne. Jeżeli chodzi o pojęcie „utraty" danych osobowych, należy interpretować je jako odnoszące się do sytuacji, w której dane mogą nadal istnieć, ale administrator utracił nad nimi kontrolę, nie posiada już do nich dostępu lub nie znajduje się już w ich posiadaniu. Nieuprawnione lub niezgodne z prawem przetwarzanie może oznaczać ujawnienie (lub udostępnienie) danych osobowych odbiorcom, którzy nie są upoważnieni do ich otrzymania (lub do uzyskania do nich dostępu), lub jakąkolwiek inną formę przetwarzania skutkującą naruszeniem przepisów RODO

Zagadnienie to było przedmiotem opinii Grupy Roboczej Art. 29. Zgodnie z tą opinią zgłaszanie naruszeń wiąże się z szeregiem korzyści. Zgłaszając naruszenie organowi nadzorczemu, administratorzy mogą zasięgnąć opinii tego organu w kwestii tego, czy w danym przypadku należy przekazać stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. Organ nadzorczy może nakazać administratorowi, aby poinformował odpowiednie osoby fizyczne o naruszeniu. Zawiadomienie osób fizycznych o naruszeniu zapewnia administratorowi możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie osoby te mogą podjąć, aby uchronić się przed potencjalnymi skutkami naruszenia. Każdy plan reagowania na naruszenia powinien koncentrować się przede wszystkim na zapewnieniu ochrony osobom fizycznym i ich danym osobowym. Dlatego też mechanizm zgłaszania naruszeń powinien być postrzegany jako narzędzie przyczyniające się do poprawy przestrzegania przepisów w zakresie ochrony danych osobowych.

O doniosłości obowiązków zgłaszania naruszeń świadczy fakt, że 14.12.2021 r. Europejska Rada Ochrony Danych (EROD) przyjęła wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych. Wytyczne te uzupełniają wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych, wprowadzając bardziej praktyczne wskazówki i zalecenia. Dokument ten ma na celu pomoc administratorom danych w podjęciu decyzji, jak postępować w przypadku naruszenia ochrony danych i jakie czynniki wziąć pod uwagę podczas oceny ryzyka. Wytyczne zawierają spis najczęściej występujących przypadków naruszeń ochrony danych, takich jak: ataki ransomware; ataki

polegające na eksfiltracji danych oraz przypadki zgubionych lub skradzionych urządzeń i dokumentów w formie papierowej – opracowane na podstawie doświadczenia organów nadzorczych. W poszczególnych kategoriach wytyczne przedstawiają najbardziej typowe dobre lub złe praktyki, porady dotyczące identyfikacji i oceny ryzyka, podkreślają czynniki, na które należy zwrócić szczególną uwagę, a także informują, w jakich przypadkach administrator powinien powiadomić o naruszeniu organ nadzorczy i/lub powiadomić o nim osoby, których dane dotyczą[489].

Charakterystyka obowiązków administratora i ich konsekwencje prawne

Naruszenie ochrony danych osobowych, o którym była mowa powyżej, nie jest pojęciem tożsamym z pojęciem naruszenia przepisów o ochronie danych osobowych. Naruszenie przepisów o ochronie danych osobowych związane jest z naruszeniem obowiązków administratora. Źródeł obowiązków administratora należy upatrywać w zadaniach nałożonych na niego w RODO, w ustawach krajowych (np. ustawa o ochronie danych osobowych), w czynnościach wykonywanych przez niego w ramach prowadzonej działalności na podstawie np. decyzji administracyjnych Prezesa UODO, czy w ramach umów zawartych z podmiotem przetwarzającym. Na gruncie krajowym mogą one wynikać także, np. z ustawy o ochronie danych osobowych, z ustawy o zmianie niektórych ustaw w związku z rozpoczęciem stosowania RODO, z ustawy o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021–2027, z ustawy o kasach zapomogowo-pożyczkowych.

Charakter obowiązków administratora nie jest jednolity. Obowiązki administratora pogrupować można na takie, których skutek ma wpływ na:

1. stosunki wewnątrz organizacji;
2. relacje z podmiotem danych;
3. obowiązki dokumentacyjne w relacjach z podmiotami trzecimi lub organem nadzoru.

Różnorodność obszarów aktywności administratora niezbędnej do zapewienia zgodności z prawem skutkuje uznaniem, że źródeł jego obowiązków należy upatrywać w przepisach prawa, czynności prawnej lub akcie administracyjnym. Wpływa to na ustalenie istoty obowiązków administratora.

W pierwszej kolejności obowiązki administratora można podzielić według zasady, że część z nich to obowiązki związane z osiągnięciem konkretnego rezultatu, a część to obowiązki

[489] Zob. https://uodo.gov.pl/pl/138/1857

podjęcia uzasadnionych starań, co do osiągnięcia konkretnego celu. Do pierwszej grupy zaliczyć można dla przykładu zasadę legalności przetwarzania danych osobowych, która polega na zapewnieniu zgodności z prawem operacji przetwarzania danych, co oznacza nie tylko konieczność spełnienia przesłanek legalności przetwarzania danych, które zostały określone w art. 6 i 9 RODO, ale także zachowania zasady legalności celu przetwarzania, co oznacza obowiązek gromadzenia danych do określonych, jednoznacznych i zgodnych z prawem celów oraz zakaz poddawania ich przetwarzaniu w sposób niezgodny z celem. Innym przykładem są obowiązki informacyjne, których realizacja następuje w sposób określający m.in. ich treść (art. 13, art. 14 RODO), czy obowiązek przetwarzania danych osobowych na podstawie upoważnienia (art. 29 RODO).

Druga grupa obowiązków dotyczy działań, które powinny być podjęte w formie starań określanych w przepisach jako „wszelkie rozsądne działania", podejmowane „w miarę możliwości" dotyczących zapewnienia np. usuwania lub poprawiania nieprawidłowych lub niekompletnych danych (art. 5 ust. 1 lit. d RODO), czy wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO (art. 24 RODO). Tutaj administrator musi sam dokonać wyboru środków, których wprowadzenie w systemie ochrony danych osobowych zapewni uznanie na etapie np. postępowania sądowego, że ich zastosowanie było odpowiednie do zidentyfikowanego ryzyka, możliwości organizacyjnych i infrastrukturalnych. Kolejnym obowiązkiem z tej grupy jest art. 32 RODO, w stosunku, do którego w doktrynie pojawiają się głosy, że przetwarzając dane osobowe nigdy nie będzie możliwe osiągniecia stanu, kiedy to przetwarzanie nie będzie za sobą pociągało ryzyka naruszenia ochrony danych osobowych. Do tego celu można jedynie dążyć, próbując osiągnąć jak najwyższy stopień bezpieczeństwa[490].

Zgodnie z prezentowanymi już wcześniej poglądami przedmiotem stosunku prawnego jest określone zachowanie, przedmiot, materialny lub dobro niematerialne bądź prawa, których dotyczą obowiązki i uprawnienia między stronami. W zagadnieniach dotyczących danych osobowych odpowiedzialność należy traktować jako konsekwencje prawne realizujące się po stronie podmiotu, który ma zgodnie z wolą ustawodawcy ponosić skutki prawne określonego zdarzenia przejawiające się w obowiązku naprawienia szkody, dlatego konieczne jest ustalenie treści stosunku prawnego uczestników systemu ochrony danych osobowych i scharakteryzowanie jakie uprawnienia i obowiązki wiążą jego podmioty (strony). Powyższe powinno zostać uwzględniać regułę, że dłużnik obowiązany jest do staranności ogólnie

[490] T. Izydorczyk, *Meritum, Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020, s. 271.

wymaganej w stosunkach danego rodzaju (należyta staranność), którą w zakresie prowadzonej przez niego działalności gospodarczej określa się przy uwzględnieniu zawodowego charakteru tej działalności. Nie przesądzając w tym momencie, który z poglądów doktryny na temat zasad odpowiedzialności na gruncie RODO jest prawidłowy konieczne jest w tym momencie dokonanie na potrzeby pracy charakterystyki obowiązków administratora według tej zasady.

Z uwagi na brak w RODO modelu starannego profesjonalisty w kontekście przetwarzania danych osobowych niezgodnie z prawem, indywidualizacji w tym zakresie powinniśmy dokonać poprzez analizę decyzji oraz orzeczeń odnoszących się do oceny sposobu wykonania przepisów prawa, mając na względzie, że takie wypracowane zostały np. na w stosunku do lekarza. Stanowisko Sądu Najwyższego w tej materii wskazuje, że w przypadkach szkody wyrządzonej przez lekarza wzorzec staranności wyznaczany jest przez wiele indywidualnych czynników, takich jak: „kwalifikacje (specjalizacja, stopień naukowy), posiadane doświadczenie ogólne i przy wykonywaniu określonych zabiegów medycznych, charakter i zakres dokształcania się w pogłębianiu wiedzy medycznej i poznawaniu nowych metod leczenia”[491].

Na gruncie RODO kryteria kwalifikacji takie jak doświadczenie, wiedza odnoszą się, np. do obowiązku weryfikacji Inspektora Ochrony Danych, czy podmiotu przetwarzającego. Nie odnoszą się bezpośrednio do obowiązków obciążających uczestników systemu ochrony danych, co nie oznacza jednak, że nie należy się nimi kierować. Na gruncie SUODO w art. 26 wskazane zostało, że w działaniach mających na celu realizację przetwarzania danych osobowych, administrator danych przetwarzający je, powinien dołożyć należytej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności był zobowiązany zapewnić, aby dane były przetwarzane zgodnie z prawem[492]. Właściwie cały art. 26 SUODO, wyznaczając główne zasady postępowania przy przetwarzaniu danych osobowych, ujmował je w formę podstawowych obowiązków, których musiał zawsze przestrzegać administrator danych. Był on odpowiedzialny nie tylko za samo przetwarzanie danych, w wąskim znaczeniu, ale także za jakość danych, co wymagało od administratora dołożenia szczególnej staranności w celu ochrony interesów osób, których dane dotyczą[493].

Administrator danych przetwarzający dane powinien był dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, w szczególności był zobowiązany

[491] Wyrok SN z 10.2.2010 r., sygn. akt V CSK 287/09.
[492] M. Ganczar, *Obowiązki przedsiębiorców w zakresie gromadzenia, przetwarzania i udostępniania danych osobowych* [w:] *Człowiek z perspektywy biznesu*, red. K. Machowicz, Lublin 2009, s. 118–130.
[493] Wyrok NSA z 7.08.2008 r., I OSK 1218/07, LEX nr 513794.

zapewnić, aby dane te były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane[494]. Wzorzec normatywny należytej staranności związany jest z zakresem i naturą obowiązków nałożonych na administratora na gruncie RODO i przepisów krajowych, które wskazują bezsprzecznie na profesjonalny charakter prowadzonej przez niego działalności w zakresie przestrzegania przepisów dotyczących ochrony danych osobowych. Stad wymóg rzetelności przetwarzania można nadal odnosić do zasady szczególnej staranności (art. 355 k.c.)[495] lub do reguł „staranności zawodowej"[496]. Przez należytą staranność należy rozumieć „obiektywnie istniejący wzorzec postępowania stworzony w celu jak najlepszego, poprawnego wykonywania zobowiązań, a jednocześnie zabezpieczający interesy zobowiązanych przez odniesienie treści staranności do danego rodzaju stosunków"[497]. Niezachowanie tak rozumianej staranności jest równoznaczne z niewykonaniem lub nienależytym wykonaniem zobowiązania[498]. Stan ten należy utożsamić ze względną bezprawnością zachowania dłużnika [499]. Dopiero stwierdzenie, że dłużnik nie zachował należytej staranności, otwiera drogę do badania, czy dłużnikowi można przypisać winę[500]. Poza tym wydaje się, ze zasadę rzetelności przetwarzania danych osobowych należy interpretować dynamicznie, ponieważ ocena profesjonalnego podejścia do ochrony danych osobowych powinna uwzględniać zmiany technologiczne dotyczące stosowanych środków przetwarzania i zabezpieczania danych[501]. Obiektywizacja wzorca staranności zakłada posługiwanie się pewnym modelem postepowania dłużnika w ramach istniejącego stosunku zobowiązaniowego, który jest następnie porównywany z zachowaniem dłużnika na tle konkretnej sytuacji. Konstruowanie miernika obiektywnego i zewnętrznego nie wyklucza jednak możliwości uwzględnienia konkretnych okoliczności i uwarunkowań, niezależnych od dłużnika, w jakich

[494] Wyrok WSA w Warszawie z 27.02.2004 r., II SA 291/03, LEX nr 569664.
[495] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych*..., s. 468
[496] A. Drozd, *Ustawa o ochronie danych osobowych*, 2006, s. 152–153.
[497] Z. Banaszczyk, P. Granecki, *O istocie należytej...*, s. 19. Podobnie, jak się wydaje, P. Machnikowski [w:] *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, nb 6–8, komentarz do art. 355/
[498] Z. Banaszczyk, P. Granecki, *O istocie należytej...*, s. 15; G. Domański, *Z problematyki podstawowych...*, s. 147; I. Karasek-Wojciechowicz [w:] *Zobowiązania. Przepisy ogólne…*, red. P. Machnikowski, nb 6 komentarz do art. 355; A. Opalski, K. Oplustil, *Niedochowanie należytej staranności jako przesłanka odpowiedzialności cywilnoprawnej zarządców spółek kapitałowych*, „Przegląd Prawa Handlowego" 2013/ 3, s. 14; M. Romanowski, *Zobowiązania rezultatu i starannego działania w umowach o prace badawcze*, „Studia Iuridica Lubinensia", 2010/14/77–92, s. 26.
[499] Z. Banaszczyk, P. Granecki, *O istocie należytej...*, s. 17; podobnie: I. Karasek-Wojciechowicz [w:] *Zobowiązania. Przepisy ogólne…*, nb 6, 10, komentarz do art. 355. Inaczej M. Krajewski, który twierdząc, że niezachowanie należytej staranności świadczy o bezprawności zachowania dłużnika, stanowczo wzbrania się przed utożsamieniem tego stanu rzeczy z uchybieniem świadczeniu. Autor ten uznał, że „utożsamienie świadczenia i dołożenia należytej staranności nie jest w żadnym wypadku poprawne" (zob. M. Krajewski, *Niezachowanie należytej staranności...*, s. 43).
[500] Z. Banaszczyk, P. Granecki, *O istocie należytej...*, s. 18; tak też M. Krajewski, *Niezachowanie należytej staranności...*, s. 41.
[501] A. Nerka [w:] *Ogólne rozporządzenie*..., red. M. Sakowska-Baryła, s. 141.

musiał on podejmować działania zmierzające do wykonania zobowiązania.[502] W tym stanie rzeczy w praktyce konieczne będzie konstruowanie miernika obiektywnie należytego wykonywania. W obecnym stanie prawnym zapewne wyjściowo bazować trzeba będzie na wcześniejszych (wzorcach, zasadach) miarach staranności wykonywania zadań przez administratora bezpieczeństwa informacji. Z czasem natomiast konkretyzacja miary należytej staranności odnosić się będzie już wyłącznie do tej oczekiwanej przez inspektora ochrony danych i powszechnie, obiektywnie przyjmowanych okoliczności poprzedzających wystąpienie naruszenia, czyli natężenia staranności podmiotów zobowiązanych w zakresie realizacji obowiązków wynikających z RODO i uniknięcia tym samym naruszenia i jego następstw – a zatem stopnia odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO[503].

Mając na względzie fakt, że przy ustalaniu wzorca należytego zachowania dłużnika trzeba uwzględnić pewne pozaprawne reguły postępowania w oznaczony sposób w określonej sytuacji, utrwalone i powszechnie akceptowane w danej branży, do której przynależą obie strony stosunku obligacyjnego podstawę do rozważania o powinności określonych zachowań mogą stanowić wskazywane przez organ nadzoru[504] w decyzjach środki zaradcze – (lub) naprawcze. Takimi działaniami jest stosowanie środków bezpieczeństwa, w celu zminimalizowania ryzyka ponownego wystąpienia naruszenia w przyszłości, takich jak dodatkowe szkolenia pracowników, aktualizacje baz danych, zobowiązywanie osoby nieuprawnione, które weszły w posiadanie dokumentów, do trwałego i bezpowrotnego usunięcia danych i potwierdzenia braku ich nieuprawnionego wykorzystania. Administratorzy wdrażali też środki bezpieczeństwa w postaci np. wymuszenia dwukrotnego podania adresu do korespondencji w formularzu lub szyfrowania wiadomości. W ramach działań naprawczych administratorzy zlecali wykonanie audytów informatycznych firmom zewnętrznym, przeprowadzali testy systemów w środowisku deweloperskim, a także przeprowadzali analizę nadawanych uprawnień. W istotę działalności gospodarczej wkomponowane jest wymaganie posiadania niezbędnej wiedzy fachowej, obejmującej nie tylko czysto formalne kwalifikacje, ale także doświadczenie wynikające z praktyki zawodowej oraz ustalone zwyczajowo standardy wymagań, co oznacza, że o tym, czy na tle konkretnych okoliczności można osobie

[502] M. Safjan [w:] *Kodeks cywilny*, t. 1, red. K. Pietrzykowski, Warszawa 2018, komentarz do art. 355, uwaga 4 w części I oraz uwaga 4 w części II.
[503] M. Górski [w:] *Ogólne rozporządzenie o ochronie...*, red. Sakowska-Baryła, s. 588.
[504] Sprawozdanie Prezesa UODO

zobowiązanej postawić zarzut braku należytej staranności w dopełnieniu obowiązków, decyduje nie tylko niezgodność jego postępowania z modelem, lecz także uwarunkowana doświadczeniem życiowym możliwość i powinność przewidywania następstw swoich działań.

Pojęcie naruszenia obowiązków dotyczących ochrony danych osobowych i naruszenia danych osobowych przez administratora w świetle orzecznictwa i decyzji organu nadzoru

Także z orzecznictwa dotyczącego zagadnień ochrony prywatności i danych osobowych można wywieść w jaki sposób judykatura interpretuje w praktyce naruszenie obowiązków. Zgodnie z wyrokiem Sądu Apelacyjnego w Białymstoku z 15.03.2017 r. w sprawie I ACa 599/16 odpowiedzialność z tytułu danych osobowych wynikać może z nieprawidłowego zabezpieczenia danych. W rozpatrywanym w tej sprawie stanie faktycznym Sąd orzekł, że w sytuacji, gdy pozew został doręczony na prywatny adres pozwanego, winien on był czuwać nad tym, by dane tam zawarte nie zostały ujawnione i rozpowszechnione. Tymczasem treść pozwu – wysłanego na „domowy" adres pozwanego – trafiła do redakcji portalu internetowego i została wykorzystana w sposób naruszający dobra osobiste powódki.

Zdaniem Sądu brak winy umyślnej w postaci świadomego, bądź rozmyślnego działania pozwanego nie wyłącza jego odpowiedzialności za niedochowanie szczególnej staranności we właściwym zabezpieczeniu danych osobowych powódki, zwłaszcza że naruszenie danych osobowych polegało także na publikacji pozwu, przez co doszło do ujawnienia danych osobowych**.** W opisywanej sprawie opublikowanie danych osobowych powódki, w szczególności jej adresu zamieszkania – nie było związane z jej działalnością publiczną, w związku z czym stanowiło bezprawne naruszenie jej prawa do prywatności. Z uwagi na charakter działalności publicznej powódki (działalność polityczna, powiązana z konkretną partią polityczną) ochrona prywatności przede wszystkim w postaci adresu zamieszkania jest niezwykle istotna, gdyż skala potencjalnych utrudnień i zagrożeń jest znaczna. Upublicznienie adresu takiej osoby stwarza wysokie ryzyko napływu osób zainteresowanych i petentów, ale także osób wrogo nastawionych z uwagi na przynależność partyjną. Sama powódka wskazywała, że upublicznienie jej adresu skutkowało tym, że była w nocy nękana domofonem.

Zdaniem Sądu Apelacyjnego, tego typu dobro osobiste (adres) w przypadku osoby publicznej jest szczególnie ważne, bowiem stanowi niekiedy ostatnią barierę, która chroni resztki prywatności. Dla każdej osoby – ale nabiera to szczególnego znaczenia w przypadku osoby publicznej – dom jest miejscem wyjątkowym, swego rodzaju azylem, miejscem gdzie można wypocząć i zachować swobodę. Nie jest ani społecznie pożądanym, ani też uzasadnionym innymi racjami, naruszanie tej sfery i burzenie spokoju oraz poczucia

bezpieczeństwa. Prawo do nieupubliczniania swego adresu zamieszkania stanowi pewne niezbędne minimum prawa do prywatności osoby publicznej[505].

Jako inne naruszenie wskazywane jest także wywieszenie na tablicy ogłoszeń w budynku pisma, w którym podano imię, nazwisko i adres powódki, bez jej zgody, co spowodowało ujawnienie osobom trzecim jej danych osobowych, a przez to naruszyło jej prawo do prywatności. Spółdzielnia nie wykazała, by w tym zakresie jej działanie nie było bezprawne, a cel, dla którego pozwana dokonała publicznego wywieszenia pisma, nie wymagał, by pismo zawierało dane osobowe powódki. Zdaniem Sądu mieszkańcy bloku przy ul. (...) nie musieli bowiem znać tych danych, by zrozumieć stanowisko spółdzielni w zakresie sporu interesującego większą grupę członków spółdzielni[506].

Kolejnym przykładem naruszenia jest wydanie dokumentu osobistego (będącego dokumentem stwierdzającym tożsamość) i prawa jazdy, osobie podającej się za powoda, w konsekwencji czego doszło do „zawłaszczenia" tożsamości powoda, czemu towarzyszyło również wykorzystanie innych informacji indywidualizujących powoda, w tym także jego adresu, daty urodzenia itp.[507]

Naruszeniem obowiązków, wynikających z przepisów ustawy o ochronie danych osobowych było także niezaktualizowanie danych w bazie służącej weryfikacji wiarygodności kredytowej, które spowodowało, że dana osoba w kontaktach z bankami prezentowana była jako osoba nie dającą gwarancji rzetelnego wywiązywania się ze zobowiązań kredytowych, co przełożyło się na odmowę udzielania mu kredytu przez bank i uprawnia pokrzywdzonego do skorzystania ze środków przewidzianych w art. 24 § 1 k.c. Z uwagi na powszechność korzystania w codziennym życiu z różnorodnych usług kredytowych, ograniczenie dostępu do tych usług w wyniku wytworzenia obrazu powoda jako niewiarygodnego klienta, naruszało jego godność, narażając go na traktowanie przez banki jako osoby o wątpliwej wiarygodności i niezrozumiałe dla niego odmowy udzielenia kredytu .[508]

W orzecznictwie opartym o roszczenia formułowane na podstawie RODO naruszenia charakteryzowane są głównie jako nieuprawnione ujawnienia danych. I tak np. w wyroku Sądu Okręgowego Warszawa – Praga w Warszawie z 17.03.2022 r. w sprawie sygn. akt II C 1228/19[509] jako naruszenie zidentyfikowane zostało omyłkowe udostepnienie danych osobowych klientów, które powstało wskutek błędu pracownika Spółki, polegającego na

[505] Wyrok SA w Białymstoku z 15.03.2017 r., sygn. 1kt I ACa 599/16.
[506] Wyrok SA w Łodzi - I Wydział Cywilny z 17.12.2015 r., sygn. akt I ACa 806/15.
[507] Wyrok SO we Wrocławiu – I Wydział Cywilny z 30.01.2014 r., sygn. akt I C 411/13.
[508] Wyrok SN – Izba Cywilna z 11.02.2015 r., sygn. akt I CSK 868/14.
[509] Wyrok SA Warszawa-Praga w Warszawie z 17.03.2022r. w sprawie sygn. akt II C 1228/19.

wysłaniu pliku z załącznikiem zawierającym dane osobowe innych klientów. W wyroku Sądu Okręgowego Warszawa – Praga w Warszawie z 19.12.2021 r. w sprawie sygn. akt II C 1169/19[510] wskazane zostało, że Spółka ponosi odpowiedzialnościcci za błędy popełnione przez osoby, które świadczą dla niej prace lub usługi, takie jak w tej sprawie, w której pracownica pozwanej podjęła błędne działania, skutkujące przekazaniem danych osobowych wielu klientów osobie nieuprawnionej do ich pozyskania.

Z perspektywy organu nadzorczego naruszenia wiążą się zwykle z innym zakresem aktywności uczestników systemu ochrony danych osobowych. W dotychczasowych decyzjach UODO jako przyczyny naruszeń w pierwszej kolejności wskazywany jest dobór nieskutecznych zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz brak regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych objętych naruszeniem, w szczególności w zakresie podatności, błędów oraz możliwych skutków dla tych systemów. Jako dalsze naruszenia podnoszone jest przetwarzanie danych osobowych w sposób niezapewniający odpowiedniego bezpieczeństwa danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Zdaniem organu jest to wynikiem braku wdrożenia odpowiednich środków technicznych i organizacyjnych, a w konsekwencji, braku możliwości wykazania przestrzegania zasady „integralności i poufności", co stanowi o naruszeniu zasady „rozliczalności" wyrażonej w art. 5 ust. 2 RODO.

Organ nadzoru podkreśla w swoich decyzjach konieczność okresowego weryfikowania wdrożonych środków technicznych i organizacyjnych oraz regularnego prowadzenia audytów, które stanowią w jego opinii przejaw wdrożenia przez administratora odpowiednich środków technicznych i organizacyjnych. Jako obowiązki administratora wskazywane jest głównie to, że administrator powinien podjąć skuteczne działania zapewniające ochronę osobom fizycznym i ich danym osobowym, które z jednej strony pozwolą na kontrolę skuteczności dotychczasowych rozwiązań, a z drugiej ocenę modyfikacji i usprawnień służących zapobieżeniu nieprawidłowościom.

Prowadzi to do konkluzji, że wdrożenie odpowiednich środków technicznych i organizacyjnych ma charakter działania ciągłego. Określając najczęściej zgłaszane naruszenia organ wskazuje na nieprawidłowe zaadresowanie lub zapakowanie korespondencji (w formie tradycyjnej lub

[510] Wyroku SO Warszawa-Praga w Warszawie z 19.12.2021r. w sprawie sygn. akt II C 1169/19.

elektronicznej) – co powoduje udostępnienie danych osobowych osobom nieuprawnionym. Naruszenia te powstawały najczęściej w wyniku błędu pracownika administratora danych. Źródłem naruszenia stawały się także błędy już na etapie gromadzenia danych adresowych, gdy niedoszli adresaci przesyłek wskazywali administratorom nieprawidłowe adresy do korespondencji. Jako równie częsta grupa naruszeń zidentyfikowane jest udostępnienie danych niewłaściwej osobie – do tego typu naruszeń dochodziło m.in. w konsekwencji wydawania dokumentów (np. zaświadczeń i deklaracji podatkowych) osobom bez uprawnień do ich otrzymania lub omyłkowych zaksięgowań przelewów. Naruszeniem uznany został także nieuprawniony dostęp do baz danych. Do tych naruszeń dochodziło wskutek błędów oprogramowania ujawniających się po aktualizacji, braku regularnych testów bezpieczeństwa w kierunku wykrycia podatności systemu oraz nieprawidłowego nadawania uprawnień. Podobnie zakwalifikowane zostało zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej lub nośnika danych. Do tego typu naruszeń dochodziło przeważnie wskutek opieszałości pracowników[511].

Kontynuując analizę zagadnienia naruszeń podnieść należy, że w decyzji z 8.06.2021 r.[512] jako inny obowiązek administratora, za który ponosi on odpowiedzialność wskazany został prawidłowy nadzór nad pracownikami. Jak podał Prezes UODO w omawianej decyzji Spółka broniła się podnosząc, że badane przez organ opóźnienia były wynikiem nieumyślnych błędów pracowników kancelarii odpowiedzialnych za wysyłkę korespondencji, w tym korespondencji dotyczącej naruszeń danych osobowych kierowanej do Prezesa UODO. Błędy polegały np. na niewpisaniu korespondencji do książki nadawczej, czego efektem był jej zwrot przez operatora pocztowego. Z uwagi, że postępowanie dotyczyło zdarzeń z 2020 r., Spółka wyjaśniła, że członkowie zespołu pracowali w trybie zdalnym, a w związku ze stanem zagrożenia epidemicznego ogłoszonym w Polsce, a najbliższym możliwym terminem do wysłania zawiadomień o naruszeniu pocztą tradycyjną był poniedziałek. Spółka przyznała się też do przypadku, gdy pracownik przygotowujący zawiadomienie o naruszeniu ochrony danych osobowych popełnił oczywistą omyłkę pisarską w dacie stwierdzenia naruszenia. Prezes UODO nie uznał jednak, że takie okoliczności stojące za opóźnieniami mogą stanowić podstawę umorzenia postępowania lub odstąpienia od nałożenia kary. Prezes UODO podkreślił, że błędy pracowników Spółki w tym zakresie świadczą właśnie o nieprawidłowym zorganizowaniu przez Spółkę procesu powiadamiania Prezesa UODO o naruszeniach danych osobowych, tym bardziej, że Spółka na żadnym etapie postępowania nie wykazała, aby

[511] Sprawozdanie Prezesa UODO.
[512] Decyzja UODO, znak sprawy DKN.5131.10.2020.

sprawowała odpowiedni nadzór nad tym procesem, a w szczególności nad pracownikami kancelarii odpowiedzialnymi za wysyłkę tej korespondencji.

W innej decyzji[513] UODO wskazuje, że w RODO ustanowiono wymóg zobowiązujący administratora do wdrożenia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osoby, których dane dotyczą. W RODO stwierdzono również, że to, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Wiąże się to z nałożeniem na administratora obowiązku utrzymania zdolności do terminowego „stwierdzania" wystąpienia wszelkich naruszeń, aby zapewnić możliwość podjęcia stosownych działań także osobie, której dane dotyczą.

Zagadnienia szczególne dotyczące deliktowej odpowiedzialności administratora

Rozważania na temat aktualnych problemów prawnych związanych z zagadnieniem odpowiedzialności administratora rozpocząć należy od syntetycznego przypomnienia stanu prawnego sprzed RODO. Zgodnie zatem z art. 22 i 23 dyrektywy państwa członkowskie miały zapewnić każdej osobie prawo do korzystania ze środków prawnych w związku z naruszeniem praw zagwarantowanych jej przez przepisy krajowe dotyczące przetwarzania danych. Środki te miały być niezależne od narzędzi administracyjnoprawnych, a także funkcjonowania organu nadzorczego. Administrator danych co do zasady ponosił odpowiedzialność za wszelkie szkody spowodowane niezgodnym z prawem przetwarzaniem danych osobowych. Państwa członkowskie miały zapewnić, aby każda osoba, która poniosła szkodę na skutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi dyrektywą, mogła uzyskać od administratora danych odszkodowanie za poniesioną szkodę. Administrator danych mógł zostać zwolniony od tej odpowiedzialności w całości lub w części, jeżeli udowodnił, że nie jest odpowiedzialny za zdarzenie, które spowodowało szkodę. W ramach ustalania zakresu odpowiedzialności w art. 23 dyrektywy należy odnieść się do motywu 55, który stanowi, że „szkody, jakie osoba może ponieść wskutek niezgodnego z prawem przetwarzania danych, muszą być wyrównane przez administratora danych, który może być zwolniony z odpowiedzialności w przypadku udowodnienia, że szkoda nie powstała z jego winy, szczególnie wówczas gdy stwierdzi wystąpienie winy po stronie osoby, której dane

[513] Decyzja UODO z 22.04.2021 r., znak sprawy DKN.5130.3114.2020.

dotyczą lub w przypadku siły wyższej". To oznaczało, że wyłączenia, na które mógł powołać się administrator danych, aby uniknąć odpowiedzialności za powstałą szkodę dotyczyły okoliczności:

1. wystąpienia winy po stronie osoby, której dane dotyczą, lub
2. przypadku wystąpienia siły wyższej.

Nie wszystkie wersje językowe Dyrektywy zostały przetłumaczone przez państwa członkowskie tak jak wersja polska z użyciem pojęcia winy. Zdaniem M. Thompsona różne wersje językowe art. 23 ust. 2 dyrektywy nie dotyczą przypisania administratorowi danych winy, a tego, czy można przypisać mu zaistnienie pewnych faktów. [514] W związku z powyższym administrator danych mógł zostać zwolniony z odpowiedzialności kiedy wykazał łączenie spełnienie trzech przesłanek:

1. wystąpienie zdarzenia,
2. wystąpienie szkody,
3. zdarzenia nie można było przypisać administratorowi.

Kwestia odpowiedzialności w RODO jest uregulowana w sposób odbiegający od regulacji Kodeksu cywilnego. Zagadnienie wzajemnych relacji i współstosowania RODO z przepisami krajowym może budzić wątpliwości interpretacyjne, dlatego wymaga dogłębnej analizy. O złożoności tych zagadnień świadczą problemy prawne, które stały się już przedmiotem pytań prejudycjalnych do TSUE w sprawach m.in. C 687/21 i C 741/21. W pierwszej z nich, tj. w sprawie BL przeciwko *Saturn Electro-Handelsgesellschaft mbH Hagen* (Saturn) znany jest stan faktyczny stanowiący podstawę złożonych pytań.

Zgodnie z materiałami dostępnymi na stronie TSUE stan faktyczny w tej sprawie dotyczył zdarzenia związanego z błędem pracownika popełnionym podczas wydawania towaru w jednym ze sklepów sieci Saturn. Błąd ten polegał na wydaniu nieuprawnionemu klientowi danych innej osoby (powoda) i wynikał z tego, że w trakcie procesu wydawania towaru klient ten przepchnął się do przodu, a w wyniku nieuwagi pracowników wydano mu zarówno zamówiony towar powoda, jak również dokumenty, które powód przekazał tym pracownikom. Klient oddalił się od punktu wydawania sprzętu razem z towarem i dokumentami powoda. Po wykryciu błędu przez kierownika punktu, udało się w ciągu pół godziny odzyskać sprzęt oraz dokumenty, które zostały niezwłocznie przekazane powodowi. Powód wytoczył powództwo sklepowi, domagając się zadośćuczynienia na podstawie art. 82 RODO z tytułu powstania

[514] M. Thompson, *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, Vanderbilt Journal of Entertainment & Technology Law, 2016/18/4; University of Hong Kong Faculty of Law Research Paper 2015/045, s. 810; W. Lamik, *Środki cywilnoprawne ochrony...*

szkody niemajątkowej. Sklep stanął na stanowisku, że nie doszło do naruszenia przepisów o ochronie danych osobowych, jak również nie wystąpiła żadna szkoda po stronie klienta. Nawet przy założeniu, że nastąpiło naruszenie ochrony danych osobowych, to nie było ono istotne. Nie potwierdzono również tego, aby osoba nieuprawniona posłużyła się danymi osobowymi powoda.

Sąd rejonowy w Hagen, który skierował do TSUE pytania prejudycjalne, stanął na stanowisku, że jeżeli przyjmie się, że szkoda niemajątkowa klienta powstała już momencie przekazania dokumentów zawierających jego dane osobowe osobie trzeciej, powinno być przyznane odszkodowanie. Na podstawie powyższego stanu faktycznego Sąd w Hagen zadał TSUE aż siedem pytań prejudycjalnych o treści:

1. czy przepis dotyczący odszkodowania zawarty w art. 82 RODO jest bezskuteczny z uwagi na brak określoności skutków prawnych, jakie należy orzec w przypadku naprawienia szkody niematerialnej?
2. czy do przyznania odszkodowania konieczne jest stwierdzenie – oprócz nieuprawnionego ujawnienia danych osobowych nieuprawnionej osobie trzeciej – wystąpienia szkody niemajątkowej, która musi być wykazana przez osobę dochodzącą tego odszkodowania?
3. czy przypadkowe ujawnienie (tj. w wyniku pomyłki pracowników przedsiębiorstwa) danych osobowych podmiotu danych (takich jak imię i nazwisko, adres, zawód, dochód, pracodawca) osobie trzeciej w postaci wydrukowanego dokumentu papierowego, jest wystarczające do stwierdzenia, że doszło do naruszenia RODO?
4. jeżeli przedsiębiorca przypadkowo udostępni za pośrednictwem swoich pracowników dane – wprowadzone do zautomatyzowanego systemu przetwarzania danych – nieuprawnionej osobie trzeciej w formie wydruku, to czy to przypadkowe ujawnienie osobie trzeciej kwalifikuje się jako niezgodne z prawem dalsze przetwarzanie (w związku z art. 2 ust. 1, art. 5 ust. 1 lit. f), art. 6 ust. 1 i art. 24 RODO)?
5. czy szkoda niemajątkowa w rozumieniu art. 82 RODO występuje już w przypadku, gdy osoba trzecia, która otrzymała dokument z danymi osobowymi, nie przyjęła do wiadomości tych danych przed zwróceniem tego dokumentu, czy też dla szkody niemajątkowej w myśl przytoczonego przepisu wystarczy dyskomfort osoby, której dane osobowe zostały dalej przekazane niezgodnie z prawem, ponieważ przy każdym nieuprawnionym ujawnieniu danych osobowych istnieje niedająca się wykluczyć możliwość, że dane te mogą być mimo wszystko dalej rozpowszechniane wśród nieznanej liczby osób lub nawet nadużywane?
6. za jak poważne należy uznać naruszenie, w sytuacji gdy niezamierzonemu dalszemu przekazaniu osobie trzeciej należy zapobiegać poprzez lepszą kontrolę pracowników

zatrudnionych w przedsiębiorstwie lub lepszą organizację bezpieczeństwa danych, np. poprzez oddzielną obsługę wydawania towarów i dokumentacji dotyczącej umowy (zwłaszcza co do finansowania) za pomocą osobnego pokwitowania wydania lub poprzez dalsze przekazanie wewnątrz przedsiębiorstwa personelowi wydającemu towar – bez angażowania klienta, któremu wręczono wydrukowane dokumenty, w tym upoważnienie do odbioru (w związku z art. 32 ust. 1 lit. b) i ust. 2 oraz art. 4 pkt 7 RODO)?

7. czy naprawienie szkody niemajątkowej oznacza zasądzenie kary jak w przypadku kary umownej?

W drugim postępowaniu, tj. w sprawie C 741/21 w zasobach TSUE nie można odnaleźć żadnych informacji co do stanu faktycznego tej sprawy. Tym samym konieczne jest poprzestanie na przedstawieniu wyłącznie pytań prejudycjalnych. Zatem niemiecki *Landgericht Saarbrücken* w sprawie GP przeciwko *juris GmbH* w dniu 1.12.2021 r. złożył wniosek o wydanie orzeczenia w trybie prejudycjalnym, na podstawie którego TSUE powinien udzielić odpowiedzi na następujące pytania:

1. czy pojęcie szkody niemajątkowej w art. 82 ust. 1 RODO należy interpretować w świetle motywu 85 i motywu 146 zd. 3 tego rozporządzenia w ten sposób, że obejmuje ono każde naruszenie podlegającej ochronie sytuacji prawnej niezależnie od pozostałych skutków i wagi tego naruszenia?
2. czy odpowiedzialność odszkodowawczą na podstawie art. 82 ust. 3 RODO wyłącza okoliczność, że przyczyną naruszenia jest w konkretnym przypadku błąd ludzki osoby działającej z upoważnienia, o której mowa w art. 29 RODO?
3. czy przy określaniu wysokości odszkodowania za szkody niemajątkowe dozwolone (względnie wymagane) jest oparcie się na kryteriach określonych w art. 83 RODO, w szczególności w art. 83 ust. 2 i ust. 5 RODO?
4. czy odszkodowanie należy ustalać dla każdego indywidualnego naruszenia czy też obejmuje się kilka – co najmniej kilka podobnych – naruszeń sankcją łącznego odszkodowania, które nie jest określane poprzez zsumowanie indywidualnych kwot, lecz jest oparte na własnej ocenie całościowej?

W kolejnej sprawie C-340/21 zakresem pytania prejudycjalnego jest zagadnienie czy niezgodny z prawem dostęp osób trzecich do danych osobowych pociąga za sobą odpowiedzialność administratora za domniemaną winę i może prowadzić do powstania podlegającej naprawieniu szkody niemajątkowej. Tan faktyczny niniejszej sprawy dotyczył okoliczności związanej z rozpowszechnieniem przez bułgarskie media informacji na temat nieuprawnionego dostępu do systemu informatycznego bułgarskiej narodowej agencji

przychodów skarbowych (NAP). W Internecie opublikowano różne informacje podatkowe i ubezpieczeniowe milionów osób. Szereg osób, w tym V.B., wniosło powództwa przeciwko NAP o zasądzenie odszkodowania za szkodę niemajątkową wyrażającą się w niepokoju i obawach, że jej dane osobowe mogą zostać wykorzystane w sposób nieuczciwy w przyszłości. Zdaniem V.B., NAP naruszyła przepisy krajowe oraz obowiązek podjęcia odpowiednich środków w celu zapewnienia odpowiednich standardów bezpieczeństwa przy przetwarzaniu danych osobowych jako administrator. Sąd pierwszej instancji oddalił powództwo, uznając, że agencja nie ponosi winy za ujawnienie danych, że ciężar dowodu co do odpowiedniego charakteru przyjętych środków spoczywa na V.B., i że żadna szkoda niemajątkowa nie podlega naprawieniu.

Rozpatrujący środek zaskarżenia Najwyższy Sąd Administracyjny zwrócił się do TSUE z pytaniami prejudycjalnymi dotyczącymi wykładni ogólnego rozporządzenia o ochronie danych w celu określenia warunków przyznania odszkodowania za szkodę niemajątkową osobie, której dane osobowe, będące w posiadaniu agencji publicznej, zostały opublikowane w Internecie w wyniku ataku hakerskiego.

W przedstawionej 27.04.2023 r. opinii rzecznik generalny Giovanni Pitruzzella stwierdził, że na administratorze spoczywa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rzeczonym rozporządzeniem. Odpowiedni charakter tych środków należy określić z uwzględnieniem natury, zakresu stosowania, kontekstu i celów przetwarzania oraz prawdopodobieństwa i wagi ryzyka naruszenia praw i wolności osób fizycznych, na podstawie oceny każdego przypadku z osobna.

W pierwszej kolejności rzecznik generalny uznał, że wystąpienie „naruszenia danych osobowych” nie jest wystarczające samo w sobie do stwierdzenia, że wdrożone przez administratora środki techniczne i organizacyjne nie były „odpowiednie” dla zapewnienia ochrony danych. Dokonując wyboru środków, administrator musi wziąć pod uwagę szereg czynników, w tym „stan wiedzy technicznej”, który pozwala na ograniczenie poziomu technologicznego wdrażanych środków do tego, co jest racjonalnie możliwe w chwili przyjęcia środków, a także koszty wdrożenia. Wybór administratora podlega ewentualnej sądowej kontroli zgodności. Ocena odpowiedniego charakteru środków musi opierać się na równowadze między interesami osoby, której dane dotyczą a interesami finansowymi i możliwościami technologicznymi administratora, z poszanowaniem ogólnej zasady proporcjonalności.

W drugiej kolejności rzecznik generalny sprecyzował, że oceniając, czy środki techniczne i organizacyjne są odpowiednie, sąd krajowy musi przeprowadzić kontrolę, która

obejmuje konkretną analizę zarówno treści tych środków, jak i sposobu ich wdrożenia oraz praktycznych skutków. Kontrola sądowa powinna zatem uwzględniać wszystkie czynniki zawarte w rozporządzeniu. Wśród owych czynników przyjęcie kodeksów postępowania lub systemów certyfikacji może stanowić przydatny element oceny w celu wywiązania się z ciężaru dowodu i związanej z tym kontroli sądowej. To na administratorze spoczywa ciężar udowodnienia, że rzeczywiście przyjął środki przewidziane w kodeksie postępowania, podczas gdy certyfikacja stanowi sama w sobie dowód zgodności z rozporządzeniem dokonanych operacji przetwarzania. Ze względu na to, że środki muszą być w razie potrzeby poddawane przeglądom i uaktualniane, sąd powinien również wziąć pod uwagę tę okoliczność.

W trzeciej kolejności rzecznik generalny wyjaśnił, że ciężar dowodu w odniesieniu do odpowiedniego charakteru środków spoczywa na administratorze. Zgodnie z zasadą autonomii proceduralnej do wewnętrznego porządku prawnego każdego państwa członkowskiego należy określenie dopuszczalnych metod dowodowych i ich mocy dowodowej, w tym środków dowodowych.

W czwartej kolejności okoliczność, że naruszenia rozporządzenia dopuściła się osoba trzecia nie stanowi sama w sobie podstawy zwolnienia administratora z odpowiedzialności. Aby administrator mógł zostać zwolniony z odpowiedzialności, musi on udowodnić za pomocą wysokiego standardu dowodu, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody. Niezgodne z prawem przetwarzania danych osobowych może w istocie przemawiać za uznaniem zaostrzonego charakteru odpowiedzialności z tytułu domniemanej winy. Wynika z tego możliwość przedstawienia przez administratora dowodu zwalniającego z odpowiedzialności.

Wreszcie, zdaniem rzecznika generalnego, szkoda polegająca na obawie przed potencjalnym nieuczciwym wykorzystaniem w przyszłości danych osobowych, której istnienie wykazała osoba, której dane dotyczą, może stanowić szkodę niemajątkową uprawniającą do odszkodowania. Osoba, której dane dotyczą, winna wykazać, iż poniosła rzeczywistą i pewną szkodę emocjonalną, a nie zwykłą trudność lub niedogodność[515]. Opinia rzecznika generalnego nie jest wiążąca dla TSUE. Orzeczenie, które zapadnie w tej sprawie będzie miało kluczowy charakter dla rozpatrywanych zagadnień, a na naszym gruncie krajowym dostarczy argumentów dotyczących trwających sporów co do zasad odpowiedzialności, wynikających z m.in. z wątpliwości dotyczących poprawności tłumaczeń.

[515] Komunikat prasowy TSUE z 27.04.23, nr 67/23, https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-04/cp230067pl.pdf

Poza zagadnieniami zawartymi w pytaniach prejudycjalnych na gruncie relacji RODO a przepisy krajowe występuje szereg dalszych wątpliwości interpretacyjnych. Stosując przepisy RODO, należy mieć na uwadze, że celem tego rozporządzenia (wyrażonym w art. 1 ust. 2) jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych oraz że ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych (zdanie pierwsze motywu 1 preambuły). W przypadku jakichkolwiek wątpliwości np. co do wykonania obowiązków przez administratorów – nie tylko w sytuacji, gdy doszło do naruszenia ochrony danych osobowych, ale też przy opracowywaniu technicznych i organizacyjnych środków bezpieczeństwa mających im zapobiegać – należy w pierwszej kolejności brać pod uwagę te wartości. Stosownie do art. 82 RODO odpowiedzialność odszkodowawcza administratora uzależniona jest od spełnienia następujących przesłanek:

- poniesienia przez podmiot danych szkody majątkowej lub niemajątkowej,
- zdarzenia, w wyniku którego doszło do powstania szkody (przetwarzanie danych osobowych przez administratora lub procesora naruszające rozporządzenie ogólne lub akty delegowane i wykonawcze przyjęte na mocy ogólnego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące rozporządzenie,
- związku pomiędzy szkodą a naruszeniem ogólnego rozporządzenia,

Spornym zagadnieniem jest przesłanka winy jako okoliczności wyłączającej odpowiedzialność za naruszenie przepisów, co wpływa na rozkład ciężaru dowodowego i stawia jako problemowe zagadnienia, czy administrator chcąc uniknąć odpowiedzialności powinien wykazywać, że:

- nie był administratorem w odniesieniu do przetwarzania, które naruszyło RODO
- naruszenia dopuścił się podmiot przetwarzający działający poza lub wbrew zgodnym z prawem poleceniom administratora
- nie było naruszenia RODO / innych przepisów prawa

Budzi to wątpliwości interpretacyjne, ponieważ nie każde naruszenie ochrony danych osobowych powoduje uszczerbek w dobrach osoby, które dane dotyczą. Aby pokazać zależność pomiędzy naruszeniem ochrony danych a szkodą należy się skupić w pierwszej kolejności na rozumieniu pojęcia szkody, które nie zostało zdefiniowane w RODO w taki sposób jak zdefiniowane zostało naruszenie.

Z RODO wynika, że pojęcie szkody należy rozumieć szeroko i w tym zakresie możemy się posłużyć np. motywem 75 RODO, zgodnie z którym przetwarzania danych osobowych mogące prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, występują w szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą

tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową. Kwestia rozumienia pojęcia szkody i naruszenia warunkującego jej naprawienie szczególnie w kontekście związanym z utratą kontroli nad danymi stała się przedmiotem analizy w toku postępowań sądowych prowadzonych przed innymi państwami członkowskimi już na gruncie starych przepisów[516].

Zgodnie z RODO w motywie 85 RODO wskazane zostało, że przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi.

Kwestia rozumienia pojęcia szkody niemajątkowej stała się przedmiotem rozstrzygnięcia TSUE w sprawie C-300/21 | Österreichische Post, wydanego na konwie stanu faktycznego, w którym od 2017 r. Österreichische Post gromadziła informacje na temat preferencji politycznych ludności Austrii. Za pomocą algorytmu uwzględniającego różne kryteria społeczne i demograficzne określiła ona „adresy grup docelowych". Zebrane w ten sposób dane skłoniły Österreichische Post do ustalenia, że konkretny obywatel miał wysokie preferencje względem określonej austriackiej partii politycznej. Przetwarzane dane nie zostały jednak przekazane osobom trzecim. Wspomniany obywatel, który nie udzielił zgody na przetwarzanie swoich danych osobowych, twierdzi, że ustalenie szczególnej preferencji dla danej partii wywołało u niego wielkie wzburzenie, utratę zaufania, a także poczucie upokorzenia. Z tytułu odszkodowania za szkodę niemajątkową, którą miał ponieść, dochodzi przed sądami austriackimi kwoty 1000 euro. Austriacki Sąd Najwyższy wyraził wątpliwości co do zakresu prawa do odszkodowania, które ogólne rozporządzenie o ochronie danych (RODO) przewiduje w wypadku szkody majątkowej lub niemajątkowej z powodu naruszenia tego rozporządzenia. Sąd ten zwrócił się do TSUE z pytaniem, czy samo naruszenie RODO jest wystarczające do przyznania tego prawa i czy odszkodowanie jest możliwe tylko wtedy, gdy przekroczony zostanie pewien próg wagi poniesionej szkody niemajątkowej. Zmierza również do ustalenia, jakie są wymagania prawa Unii co do ustalenia kwoty odszkodowania.

W wyroku z 4.05.2023 r. TSUE[517] orzekł w pierwszej kolejności, że prawo do odszkodowania przewidziane w RODO jest podporządkowane, w jednoznaczny sposób, trzem

[516] Sprawa Lloyd przeciwko Google EWCA Civ 1599; wyrok dostępny na: https://www.supremecourt.uk/cases/uksc-2019-0213.html, a istotne komentarze w tej sprawie dostępne na: https://www.pinsentmasons.com/out-law/analysis/lloyd-v-google-supreme-court-representative-action oraz https://verfassungsblog.de/lloyd-privacy/

[517] Wyrok TSUE z 4.05.2023 r., C-300/21.

kumulatywnym przesłankom: naruszenie RODO, szkoda majątkowa lub niemajątkowa wynikająca z tego naruszenia i związek przyczynowy między szkodą a naruszeniem. Stąd każde naruszenie RODO, samo w sobie, nie rodzi prawa do odszkodowania. Inna wykładnia byłaby sprzeczna z wyraźnym brzmieniem RODO. Ponadto zgodnie z motywami RODO dotyczącymi prawa do odszkodowania, naruszenie RODO niekoniecznie musi prowadzić do powstania szkody, a dla uzasadnienia prawa do odszkodowania musi istnieć związek przyczynowy między danym naruszeniem a poniesioną szkodą. Tym samym powództwo odszkodowawcze odróżnia się od innych środków odwoławczych przewidzianych w RODO, w szczególności tych, które pozwalają nakładać administracyjne kary pieniężne, w odniesieniu do których to środków wykazanie wyrządzenia indywidualnej szkody nie jest konieczne.

W drugiej kolejności TSUE stwierdził, że prawo do odszkodowania nie jest zastrzeżone dla szkód majątkowych osiągających określoną wagę. RODO nie wspomina o takim wymogu i takie ograniczenie zaprzeczałoby szerokiej koncepcji pojęcia „szkody" przyjętej przez prawodawcę Unii. Poza tym uzależnienie odszkodowania za szkodę niemajątkową od określonego progu wagi mogłoby zaszkodzić spójności systemu ustanowionego przez RODO. Wyznaczanie takiego progu, od którego zależałaby możliwość uzyskania odszkodowania, mogłoby ulegać wahaniom w zależności od oceny sądu rozpatrującego sprawę.

W trzeciej i ostatniej kolejności, odnośnie do zasad dotyczących oszacowania odszkodowania TSUE zaznaczył, że RODO nie zawiera przepisów mających taki przedmiot. Do porządku prawnego każdego państwa członkowskiego należy zatem określenie zasad mających na celu zapewnienie podmiotom prawa ochrony uprawnień wynikających z RODO, a w szczególności kryteriów pozwalających na określenie zakresu odszkodowania należnego w tych ramach, z zastrzeżeniem poszanowania zasad równoważności i skuteczności. W tym aspekcie TSUE podkreślił funkcję kompensacyjną prawa do odszkodowania przewidzianego w RODO i przypomniał, że ten instrument ma zapewnić pełne i skuteczne odszkodowanie za poniesioną szkodę[518].

Odrębną grupą zagadnień wymagających interpretacji, które nie wynikają wprost z RODO są zagadnienia dotyczące relacji administrator - podwładny, czyli np. zastosowanie art. 430 k.c. w sytuacji, gdy pomimo wdrożenia odpowiednich środków organizacyjnych i technicznych osoba, której powierzono wykonanie czynności doprowadza do powstania szkody poprzez wykorzystanie do własnych celów danych osobowych. W takich przypadkach redefinicji na potrzeby RODO będzie wymagało określenie obowiązku stosowania się do

[518] Wyrok TSUE z 4.05.2023 r., C-300/21.

wskazówek oraz zakresu powierzonej czynności, której wykonywanie doprowadziło do powstania szkody.

Kolejny obszar problemowy wiąże się z tym, że w systemie ochrony danych osobowych większość zadań związanych z przetwarzaniem danych osobowych wykonywana jest nie tylko wyłącznie bezpośrednio na podstawie powszechnie obowiązujących przepisów prawa, ale i procedur wewnętrznych. Odbywa się to bez konieczności uzyskiwania kolejnych decyzji przedsiębiorcy, czy zarządu jako organu osoby prawnej. Ich rola sprowadza się do prawidłowego ustanowienia i wprowadzenia procedur wewnętrznych, których naruszenie przez personel może spowodować szkodę. Szkoda może powstać także całkowicie niezależnie od ustanowionych procedur, a wynikać ze złej organizacji osoby prawnej, złej jakości pracy, gdzie często nie można wskazać konkretnej osoby odpowiedzialnej za szkodę. W takich sytuacjach koncepcja „winy bezimiennej", „organizacyjnej" może mieć praktyczne zastosowanie[519]. Zastosowanie tej konstrukcji ma na celu ustalenie sprawstwa niezindywidualizowanej osoby z grupy ludzi[520].

Zagadnienia szczególne dotyczące odpowiedzialności współadministratorów

Inny obszar zagadnień problemowych związany jest ze stosowaniem wspólnej odpowiedzialności przez współadministratorów. W tym zakresie stanowisko zajął M. Gumularz, który zwraca uwagę na możliwość wystąpienia następujących sytuacji, względem jakich mogą pojawić się wątpliwości co do solidarnej odpowiedzialności współadministratorów. W tym miejscu dla porządku wskazania wymaga, że do przyjęcia solidarności biernej, jak i czynnej konieczne jest stwoerdzenie dla niej tytułu. Zobowiązanie jest solidarne jedynie wówczas, gdy to wynika z ustawy lub czynności prawnej.

Zdaniem M.Gumularza z perspektywy art. 26 RODO możemy postawić jako problematyczną tezę, czy odpowiedzialność solidarną może rodzić:

1. niezawarcie lub nieprawidłowa treść uzgodnień z art. 26 ust. 1 RODO?
2. naruszenie przez jednego ze współadministratorów uzgodnień z art. 26 ust. 1 RODO (np. przetwarzanie danych osobowych w sposób sprzeczny z celami, które były przedmiotem uzgodnień).

[519] S. Kaczyńska, *Zarządzający portem lotniczym jako podmiot prawa publicznego i prywatnego. Wybrane zagadnienia*, Warszawa 2016, https://sip-1legalis-1pl-1v27i8rcf1fd1.han3.lib.uni.lodz.pl/document-full.seam?documentId=mjxw62zogi2dkmjugq4timjog4&refSource=toc#tabs-metrical-info
[520] S. Kaczyńska, *Zarządzający portem*...

Autor ten uważa, że w pierwszym przypadku taka odpowiedzialność wystąpi, gdyż w przeciwnym wypadku podmiot danych zostałby pozbawiony ochrony cywilnoprawnej W drugim stanie faktycznym M. Gumularz twierdzi, że możliwe jest pociągnięcie do odpowiedzialności współadministratora, który nie naruszył uzgodnień, gdy szkoda powstała w wyniku jego zawinionego zachowania. Stanowisko to wzmacnia treść art. 371 k.c., w myśl którego działania i zaniechania jednego z dłużników solidarnych nie mogą szkodzić współdłużnikom[521]. Istotny dla oceny analizowanych zagadnień będzie także art. 375 § 1 k.c., skutkującym tym, że podmiot, który odpowiada w sposób solidarny na podstawie art. 82 ust. 4 RODO (administrator lub podmiot przetwarzający), może podnosić względem zgłaszającego roszczenie (tj. co do zasady osoby, której dane dotyczą) zarzuty, które przysługują mu osobiście względem podmiotu danych, a także te, które ze względu na sposób powstania lub treść zobowiązania są wspólne dla pozostałych administratorów lub procesorów.

Zagadnienia szczególne dotyczące kontraktowej odpowiedzialności administratora

W obszarze odpowiedzialności kontraktowej zagadnienia problemowe koncentrują się wokół tego, że obowiązek odszkodowawczy dłużnika nie jest zawsze bezpośrednio sankcją naruszenia powinności obligacyjnych i wynikłej z tego szkody. Istotne znaczenie ma przyczyna naruszenia zobowiązania. Obowiązek odszkodowawczy powstaje, gdy szkoda jest wynikiem okoliczności, za którą dłużnik odpowiada. To za co dłużnik w konkretnym wypadku odpowiada i jakimi dowodami może się zwolnić określa przede wszystkim treść czynności prawnej będącej źródłem zobowiązania oraz przepisy właściwe dla danego stosunku prawnego. Dopiero w braku poszczególnych postanowień czynności prawnej lub ustawy znajdują zastosowanie ogólne reguły Kodeksu wskazujące za jakie okoliczności dłużnik ponosi odpowiedzialność[522].

Przyjmując, że źródłem zobowiązań na gruncie RODO są zdarzenia cywilnoprawne, a najczęściej są to czynności prawne takie jak umowy, nie można pomijać faktu, że niektóre z nich powstają w drodze czynności jednostronnych. Dzieje się tak w przypadku umów adhezyjnych, których istotę wyznaczają m.in. uczciwe warunki umowy, czy dobra wiara przedsiębiorcy. Zgodnie z poglądami doktryny ogólne kryteria oceny nieuczciwego charakteru warunków umowy, zwłaszcza w przypadku działalności zapewniającej usługi o charakterze powszechnym, muszą być uzupełnione środkami umożliwiającymi dokonanie ogólnej oceny różnych interesów. Stanowi to element oceny działania w dobrej wierze, przy dokonywaniu

[521] M. Gumularz, *Meritum...*, s. 518.
[522] T. Pajor, *Odpowiedzialność dłużnika...* s. 35–36.

oceny której będzie brana pod uwagę zwłaszcza siła pozycji przetargowej stron umowy.[523] W kontekście RODO interesy stron takich umów będę wymagały analizy obowiązków uczestników systemu ochrony danych osobowych.

Źródłem zobowiązań mogą być także akty administracyjne oraz orzeczenia sądowe jeżeli stanowią źródło powstania stosunku obligacyjnego. Dzieje się tak, gdy mają one charakter konstytutywny – powstanie zobowiązania jest bezpośrednim skutkiem tego zdarzenia. Dodatkowo stosunki zobowiązaniowe mogą powstać także wskutek innych zdarzeń, z którymi norma prawna łączy skutek w postaci powstania stosunku obligacyjnego[524]. W relacjach wynikających z RODO akty wewnętrzne, czy jednostronne czynności mogą być źródłem zobowiązań w ramach stosunków wewnętrznych, np. w stosunku do pracowników.

Reżim odpowiedzialności kontraktowej rozciąga się na wszystkie stosunki obligacyjne, dlatego bliższe określenie jego zakresu wymaga zbadania, jak szeroko ujmuje się samo pojęcie zobowiązania. Chodzi zwłaszcza o wskazanie kryteriów pozwalających odróżnić zobowiązania od tak zwanych obowiązków powszechnych ciążących na wszystkich przedmiotach obrotów prawnego. Według ujęcia klasycznego do którego nawiązuje artykuł 353 k.c. zobowiązanie przedstawia się od strony dłużnika jako powinność spełnienia świadczenia, od strony wierzyciela zaś, jako skierowane do dłużnika roszczenie o spełnienie świadczenia. W ramach tego modelu pojęcie zobowiązania można scharakteryzować następującymi cechami: konkretyzacją podmiotów i treści, korelacją praw i obowiązków stron, ograniczeniem w czasie oraz istnieniem źródła więzi prawnej między stronami. Ze względu na granicę treści zobowiązania tylko szkody wynikłe z niespełnienia lub nienależytego spełnienia świadczenia podlegają naprawieniu na podstawie przepisów reżimu kontraktowego.

Formułując tę myśl nieco inaczej można powiedzieć, że reżim ten stosuje się jedynie do uszczerbków pozostających w ścisłym, funkcjonalnym związku z wykonywaniem zobowiązania. Według T. Pajora oznacza to, że jeżeli wyrządzenie szkody nastąpiło wskutek naruszenia obowiązków powszechnych przy okazji wykonywania zobowiązania, w grę może wchodzić jedynie deliktowa odpowiedzialność sprawcy[525]. W takim przypadku nie możemy jednak nie rozważać instytucji zbiegu odpowiedzialności z art. 443 k.c. W literaturze przedmiotu wskazuje się zazwyczaj, że z przepisu tego wynika, iż jako zasadę przyjąć trzeba

[523] M. Ganczar, M. Pyter, *Rejestr klauzul niedozwolonych jako źródło prawa administracyjnego i cywilnego*, *Źródła prawa administracyjnego a ochrona praw i wolności obywateli*, Warszawa 2014 s. 205.
[524] A. Olejniczak [w:] *Kodeks cywilny. Komentarz*, t. 3, *Zobowiązania. Część ogólna*, red. A. Kidyba, Warszawa 2014 s. 33.
[525] T. Pajor, *Odpowiedzialność dłużnika...*, s. 45–50.

równorzędność tych roszczeń[526] w sensie swobodnej konkurencji pomiędzy nimi[527]. Zazwyczaj twierdzi się, że dokonanie wyboru należy tu do poszkodowanego[528].

Zagadnienie samo w sobie zawiera niezwykle duży potencjał problemów zarówno na gruncie prawa materialnego, jak i procesowego. Wiąże się to nie tylko z możliwością samodzielnej, dyskrecjonalnej oceny przez sąd podstawy prawnej dochodzonego roszczenia, lecz także zagadnieniem ustalenia granicy ingerencji przez organ procesowy w przedmiocie podstawy faktycznej i ewentualnej modyfikacji podstawy prawnej. Kontrowersje w tym wypadku wiążą się z ustaleniem, co faktycznie wchodzi w podstawę powództwa, która nie może podlegać zmianom dokonanym przez organ procesowy (takim jak sąd)[529].

W przypadku zobowiązania istotne jest, że w ramach swobody umów strony mogą wprowadzać dopuszczalne prawnie modyfikacje umowne, wpływające na zakres odpowiedzialności stron, który to problem poddany zostanie analizie w kolejnym rozdziale pracy.

Zagadnienia szczególne dotyczące odpowiedzialności w relacji z podmiotem danych

Zagadnienie odpowiedzialności administratora na gruncie RODO wymaga także dokonania jego oceny z perspektywy podmiotu danych, tj. osoby, której dane dotyczą w przypadku naruszenia ochrony danych osobowych W tym zakresie istotne jest, że w motywie 85 preambuły RODO wyjaśniono, że „przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie

[526] M. Safjan [w:] *Kodeks cywilny…*, s. 1416; A. Ohanowicz, *Zbieg norm w kodeksie cywilnym*, PiP 1965/2, s. 190; A. Szpunar, *Zbieg roszczeń odszkodowawczych*, RPEiS 1974/1, s. 38. Na tym tle podkreśla się, że brak uzasadnienia dla twierdzeń, jakoby odpowiedzialność kontraktowa zawsze wykluczała deliktową bądź na odwrót (zob. A. Ohanowicz, *Zbieg norm w kodeksie cywilnym* [w:] A Ohanowicz, *Wybór prac*, Warszawa 2007, s. 277). Pojawiają się jednak także poglądy odmienne, w myśl których poszkodowany powinien wywodzić swe roszczenia w pierwszym rzędzie z łączącego go z drugą stroną stosunku zobowiązaniowego i dopiero w jego braku może oprzeć je na reżimie deliktowym (zob. Z. Banaszczyk, P. Granecki, *O istocie należytej staranności*, Palestra 2000/7–8, s. 12–13)

[527] W. Dubis [w:] *Kodeks cywilny. Komentarz…*, s. 747.

[528] A. Śmieja [w:] *System prawa prywatnego…*, s. 659; G. Bieniek [w:] *Komentarz do kodeksu cywilnego. Księga trzecia. Zobowiązania*, t. 1, red. G. Bieniek, Warszawa 2005, s. 448; M. Safjan [w:] *Kodeks cywilny…*, s. 1418; W. Dubis [w:] *Kodeks cywilny. Komentarz…*, s. 748; E. Łętowska [w:] *System prawa prywatnego*, t. 1, *Prawo cywilne — część ogólna*, red. M. Safjan, Warszawa 2007, s. 547; A. Ohanowicz, *Zbieg norm w kodeksie cywilnym*, „Nowe Prawo" 1966/12, s. 1504; wyrok SN z 4.08.2005 r., sygn. akt III CK 701/04, Lex nr 371489. Odmiennie, jak się wydaje, M. Sośniak, który nie wspomina nic o wyborze przysługującemu poszkodowanemu, lecz zakłada, że o zastosowaniu określonych uregulowań decyduje organ orzekający w procesie odszkodowawczym (zob. M. Sośniak [w:] *Prawo cywilne*, red. S. Grzybowski, Warszawa 1972, s. 198).

[529] Ł. Błaszczak, J. Kuźmicka–Sulikowska, *Zbieg roszczeń ex contractu i ex delicto na tle art. 443 k.c. w ujęciu materialnoprawnym i procesowym*, „Transformacje Prawa Prywatnego" 2013/3, s. 6.

tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki".

Z kolei w motywie 86 preambuły RODO wskazano, że „administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania".

Zawiadamiając bez zbędnej zwłoki podmiot danych, administrator umożliwia osobie podjęcie niezbędnych działań zapobiegawczych w celu ochrony praw lub wolności przed negatywnymi skutkami naruszenia. Art. 34 ust. 1 i 2 RODO ma na celu nie tylko zapewnienie możliwie najskuteczniejszej ochrony podstawowych praw lub wolności podmiotów danych, ale także realizację zasady przejrzystości, która wynika z art. 5 ust. 1 lit. a) RODO[530]. Właściwe wywiązanie się z obowiązku określonego w art. 34 RODO ma zapewnić osobom, których dane dotyczą - szybką i przejrzystą informację o naruszeniu ochrony ich danych osobowych wraz z opisem możliwych konsekwencji naruszenia ochrony danych osobowych oraz środków, które mogą one podjąć w celu zminimalizowania jego ewentualnych negatywnych skutków. Postępując zgodnie z prawem i wykazując dbałość o interesy osoby, której dane dotyczą, administrator powinien bez zbędnej zwłoki zapewnić osobie, której dane dotyczą, możliwość jak najlepszej ochrony przez nią jej danych osobowych. Dla osiągnięcia tego celu niezbędne

[530] W. Chomiczewski [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak- Jomaa, D. Lubasz, Warszawa 2018, s. 34

jest przynajmniej wskazanie tych informacji, które wymienione są w art. 34 ust. 2 RODO. W konsekwencji podejmując decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osoby, której dane dotyczą, w praktyce administrator pozbawia tę osobę, przekazanej bez zbędnej zwłoki, rzetelnej informacji o naruszeniu i możliwości przeciwdziałania potencjalnym szkodom. Sytuacje, gdy dane osobowe przetwarzane są bez wiedzy podmiotu danych, choć istnieje obowiązek wynikający z art. 13 oraz 14 RODO informowania go o fakcie przetwarzania danych osobowych, a do tego, że dane przetwarzane są bezprawnie, ingeruje w poczucie pewności i bezpieczeństwa jednostki. Podważa to jednocześnie prawo do autonomii informacyjnej, czyli decydowania o tym, kto i jakie dane osobowe na nasz temat przetwarza. Znaczenie prawa do autonomii informacyjnej jest podkreślane w orzecznictwie Trybunału Konstytucyjnego, który zwraca uwagę, że prawo do obejmuje m.in. kontrolę nad informacjami, jeżeli znajdują się one w posiadaniu innych podmiotów[531]. Naruszenie zatem zasad przetwarzania danych osobowych, w tym legalnego ich przetwarzania i realizacji obowiązków informacyjnych, ingeruje na poziomie dóbr osobistych w prawo do ochrony danych osobowych, prawo do autonomii informacyjnej oraz prawo do prywatności. Dodatkowo może naruszać godność osoby. Przewidziana zatem w RODO ochrona danych osobowych jest jedynie częścią większej całości systemu ochrony opisanych na wstępie praw podstawowych człowieka. Naruszenie RODO, które wywołuje ingerencję w wartości niemajątkowe, ma swoje konsekwencje na gruncie art. 23 i 24 k.c.[532], szczególnie w kontekście problemu podstaw prawnych formułowania roszczeń o naprawienie szkody niemajątkowej bazując wyłącznie na RODO, o czym będzie mowa także w dalszej części pracy.

Zagadnienie naruszenia przepisów i naruszenia ochrony danych wymaga rozważenia kwestii, czy uprawnienie podmiotu danych z art. 79 RODO aktualizować będzie się wyłącznie w przypadku jednoczesnego naruszenia przepisów regulujących prawa podmiotu danych oraz innych przepisów rozporządzenia, tj. tych dotyczących praw i obowiązków podmiotów przetwarzających i administratorów, czy być może wystarczy w tym zakresie naruszenie praw podmiotów danych. Otóż mając na względzie fakt, iż w zdecydowanej większości przypadków naruszenie praw osób, których dane dotyczą samo w sobie stanowić będzie naruszenie przepisów rozporządzenia, samo naruszenie przepisów regulujących prawa osób, których dane dotyczą, będzie stanowić podstawę do skorzystania ze środka unormowanego w art. 79 RODO, choć z praktycznego punktu widzenia istotna zdaje się być w tym zakresie uwaga, że często

[531] Wyroki TK z 19.02.2002 r., U 3/01, OTK ZU z 2002, nr 1/A, poz. 3; wyrok z 20.11.2002 r., sygn. akt K 41/02.
[532] Zob. https://panoptykon.org/poczta-musielismy-sluchac-premiera

naruszenie praw podmiotów danych skorelowane będzie z naruszeniem przez administratora czy przetwarzającego ich obowiązków. Z analogiczną sytuacją będziemy mieć do czynienia także wówczas, gdy naruszone zostaną co prawda zasady przetwarzania danych osobowych, czy też przepisy regulujące zasady dopuszczalności przetwarzania, albowiem w praktyce powyższe skutkować będzie naruszeniem ogólnego prawa podmiotu danych do ochrony jego danych osobowych. Jak bowiem słusznie zauważa P. Fajgielski przyjęcie przeciwnego wniosku prowadziłoby do pozbawienia osoby której dane dotyczą, możliwości skorzystania ze środka o którym mowa w art. 79 rozporządzenia np. w sytuacji gdy administrator przetwarzał dane bezprawnie lub naruszył zasadę adekwatności poprzez zbieranie zbyt dużej ilości danych. Nadto też należy podkreślić, że uprawnienie to aktualizować będzie się nie tylko w przypadku naruszenia *stricte* przepisów rozporządzenia ogólnego o ochronie danych osobowych, ale także naruszenia przepisów aktów delegowanych i wykonawczych przyjętych na jego podstawie oraz prawa państwa członkowskiego, które doprecyzowuje jego postanowienia – o czym wprost stanowi motyw 146 RODO. Z tego typu naruszeniem będziemy mieć do czynienia np. w sytuacji niezgodności działań administratora z aktem wykonawczym określającym techniczne standardy mechanizmów certyfikacji, wydanym przez KE na podstawie art. 43 ust. 9 RODO[533].

Obowiązek notyfikacji naruszenia organowi nadzorczemu i zawiadomienie osób, których dane dotyczą z perspektywy odpowiedzialności odszkodowawczej należy rozpatrywać także w kontekście instytucji przyczynienia się do powstania szkody. Zgodnie z art. 362 k.c. jeżeli poszkodowany przyczynił się do powstania lub zwiększenia szkody, obowiązek jej naprawienia ulega odpowiedniemu zmniejszeniu, stosownie do okoliczności, a zwłaszcza do stopnia winy obu stron (art. 362 k.c.). W poprzednim stanie prawnym, na podstawie art. 158 § 2 k.z. z 1933 r., obowiązującego do 1.01.1965 r. przewidywano, że jeżeli poszkodowany przyczynił się do wyrządzenia szkody, odszkodowanie ulega odpowiedniemu zmniejszeniu. Jeszcze na gruncie regulacji art. 158 § 2 k.z. wypracowane zostały cztery stanowiska dotyczące kwestii przyczynienia się[534].

Przenosząc powyższe rozważania na grunt ochrony danych osobowych brak zawiadomienia przez administratora organu nadzoru może być argumentem służącym podniesieniu powyższego zarzutu. W stosunku do administratora argumentacja w tym zakresie mogłaby być budowana poprzez podnoszenie braku zastosowania się do nakazów organu

[533] K. Biczysko-Pudełko, *Cywilnoprawna odpowiedzialność dostawcy usług cloud computing w świetle przepisów rozporządzenia ogólnego o ochronie danych osobowych – wybrane problemy 2021*, https://sip-1legalis-1pl-1v27i8rcf1fd1.han3.lib.uni.lodz.pl/document-full.seam?documentId=mjxw62zogi3damzwgmztqmzohe

[534] Sz. Krajnik, A. Ornowska, *Przyczynienie się do powstania szkody w prawie cywilnym oraz jego aspekty prawnokarne*, „Studia Iuridica Toruniensia" 2011/8.

nadzoru w toku postępowania wyjaśniającego, których zastosowanie mogłoby mieć wpływ na powstanie szkody. W relacji z podmiotem danych możliwymi do wykorzystania byłyby argumenty związane z działaniami, które w ramach zawiadomienia o naruszeniu, wskazują na okoliczności związane ze skutkami naruszenia i działaniami, których podjęcie przez podmiot danych może takim skutkom zapobiec. Do takich działań mogą zaliczać się wskazywane w zawiadomieniu przez administratora zalecenia zachowania ostrożności w sytuacji odbierania połączeń telefonicznych od nieznanych numerów telefonów, ignorowania nieoczekiwanych wiadomości e-mail lub SMS, w szczególności od nieznanych nadawców oraz nie otwierania nieznanych załączników, nie używania linków do stron internetowych otrzymanych od nieznanych nadawców w wiadomościach e-mail lub SMS-ach, zachowania ostrożność przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu, czy założenia konto w systemie informacji kredytowej lub gospodarczej w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem.

Omówione wyżej okoliczności będą musiały zostać uwzględnione w teoriach przyczynienia się do powstania szkody w danych osobowych, zwłaszcza problematyka przyczynienia się poszkodowanego do powstania lub zwiększenia szkody od kilkudziesięciu już lat budzi spory w doktrynie i judykaturze, które nie zakończyły się dotąd wypracowaniem jednej wspólnej koncepcji pojmowania tej instytucji.

ROZDZIAŁ V.
Obowiązku podmiotu przetwarzającego i jego odpowiedzialność

Pojęcie podmiotu przetwarzającego

Określenie „podmiot przetwarzający" (ang. *processor*, niem. *Auftragsverarbeiter*) zgodnie z definicją legalną, zawartą w art. 4 pkt 8 RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Z tej definicji wynika, że podmiotem przetwarzającym może być zarówno podmiot prywatny (osoba fizyczna, osoba prawna, jednostka organizacyjna mająca zdolność prawną, ale nieposiadająca osobowości prawnej), jak i publiczny (organ administracji publicznej, inny podmiot publiczny)[535].

Na gruncie dyrektywy 95/46/WE, w art. 2 lit. e wskazywano, że „przetwarzający" oznaczał osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ przetwarzający dane osobowe w imieniu administratora danych. Natomiast w przepisach SUODO w art. 31 wskazywano, że administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Co do zasady więc konstrukcja podmiotu, który w imieniu i na rzecz administratora może przetwarzać dane osobowe, nie jest nową regulacją wprowadzaną przepisami RODO. W poprzednim stanie prawnym dla określenia podmiotu przetwarzającego dane na zlecenie w praktyce posługiwano się różnymi określeniami, w tym przetwarzający, podmiot przetwarzający, procesor[536].

Podmiot przetwarzający pojawia się w procesie przetwarzania danych osobowych, gdy mamy do czynienia z powierzeniem przetwarzania. Obecnie jest ono powszechne zarówno w sektorze prywatnym, jak i w sektorze publicznym. Podmiot przetwarzający wykonuje czynności przetwarzania danych dla administratora, realizując jego cele i potrzeby – w jego imieniu i na jego rzecz. Administrator nie ma bowiem obowiązku samodzielnego wykonywania czynności na danych osobowych, nie musi też fizycznie ich posiadać ani samodzielnie realizować określonych przez siebie celów przetwarzania. Może zlecić te działania innej osobie, innemu podmiotowi. Powierzenie przetwarzania jest oczywistą konsekwencją wielu usług outsourcingowych, w obrębie których przetwarzanie danych osobowych jest nie tyle istotą zlecenia, co oczywistym elementem kontraktowanej usługi, np. zewnętrzna obsługa

[535] P. Fajgielski, *Ogólne rozporządzenie o ochronnie*..., s. 342.
[536] A. Mednis, *Administrator danych*..., s. 83; M. Sakowska-Baryła, *Prawo do ochrony danych*..., s. 157.

prawna, obsługa księgowa, prowadzenie rekrutacji przez portal internetowy, pośrednictwo ubezpieczeniowe i bankowe[537], akcje marketingowe i rozsyłanie newslettera[538].

Jak z tego wynika, występowanie podmiotu przetwarzającego w procesie przetwarzania danych osobowych uzależnione jest od decyzji administratora, który może zdecydować o przetwarzaniu danych w ramach własnej organizacji, na przykład przez pracowników upoważnionych do przetwarzania danych pod jego bezpośrednim zwierzchnictwem, lub przekazać całość bądź część działań w zakresie przetwarzania danych organizacji zewnętrznej tj. pomiotowi odrębnemu prawnie działającemu w jego imieniu[539].

Klasyfikowanie podmiotów odpowiednio jako: „administrator" i „podmiot przetwarzający" ma charakter obiektywny i następuje w związku z konkretnymi okolicznościami, podejmowanymi decyzjami gospodarczymi, oceną, kto w tych okolicznościach podejmuje decyzje co do celu przetwarzania danych osobowych oraz sposobów, jakimi się ono odbywa[540]. Tak określonej relacji nie zmienia umowne ustalenie statusu podmiotów uczestniczących w procesach przetwarzania danych osobowych, choć w praktyce pojawiają się próby oznaczania w umowie, kto w danym stosunku jest administratorem, a kto podmiotem przetwarzającym, bez względu na to, kto rzeczywiście decyduje o celach przetwarzania danych, na czyją rzecz i w czyim imieniu się to odbywa. Praktykę tę należy ocenić negatywnie jako niezgodą z prawem[541]. Treść umowy okazuje się nie być ostatecznym i miarodajnym środkiem rozstrzygającym o statusie podmiotów uczestniczących w przetwarzaniu danych osobowych.

Wniosek ten wypływa m.in. z analizy decyzji GIODO, w której stwierdzono, że jeżeli w umowie pomiędzy podmiotami wskazano jeden z podmiotów jako administratora danych, a drugiego jako podmiot, któremu powierzono przetwarzanie danych, nie przesądza o tym, kto rzeczywiście jest administratorem tych danych. Jeżeli zarówno z innych postanowień umowy jak i samego procesu przetwarzania danych wynika, iż podmiot wskazany w umowie jako ten, któremu powierzono przetwarzanie danych, w rzeczywistości decyduje o celach i sposobach, należy uznać iż administratorem danych jest właśnie ten podmiot[542]. W przedmiotowej sprawie

---

[537] E. Kulesza, *Agent nie jest administratorem*...; E. Kulesza, *Zlecenie przetwarzania informacji*...; P. Babiarz, *Dopuszczalność zlecania przez bank*, „Monitor Prawniczy" 2000/10, s. 634 i n.

[538] T. Izydorczyk, *ADO w konkursach i loteriach*..., s. 41–43; zob. M. Sakowska-Baryła [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 104.

[539] Opinia 1/2010 Grupy Roboczej Art. 29, s. 27; *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 223.

[540] M. Sakowska-Baryła [w:] *Ogólne rozporządzenie….,* s. 107

[541] G. Sibiga, *Powierzenie przetwarzania danych osobowych w obrocie gospodarczym* [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, Warszawa 2013, s.105–106.

[542] Decyzja GIODO z 15.07.2015 r., DIS/DEC 594/15/62961, Legalis nr 1336609.

istotą sporu było określenie poprawności stosowanej umowy powierzenia przetwarzania danych związanej z umową, której przedmiotem było świadczenie usług na rzecz pracowników klienta w ramach programu korzyści pracowniczych przez partnerów Spółki oraz Spółkę W umowie sprzed kontroli podmiotem przetwarzającym określona została błędnie rzeczona Spółka, w sytuacji w której z konstrukcji stosunku prawnego wynikało, że to ona a nie pracodawca decyduje o celach i sposobach przetwarzania danych osobowych pracowników klienta.

W tym miejscu konieczne jest podkreślenie, że rozstrzyganie o statusie podmiotów uczestniczących w przetwarzaniu danych i analiza pod tym kątem umowy nie może pomijać zagadnienia wykładni oświadczeń woli, która zgodnie z art. 65 k.c. dokonywana jest na trzech poziomach.

Pierwszy poziom rzeczonej wykładni wyznaczany jest przez dosłowne brzmienie umowy, drugi zdeterminowany jest przez treść odczytywaną przy zastosowaniu reguł interpretacyjnych wyrażonych w art. 65 § 1 k.c., trzeci zaś polega na ustaleniu znaczenia oświadczeń woli przez odwołanie do zgodnego zamiaru i celu umowy (art. 65 § 2 k.c.). Zasadom wykładni ustalonym w art. 65 § 2 k.c. podlega także kwalifikacja prawna umowy wyrażona nadaną jej przez strony nazwą, a interpretacja oświadczeń woli stron służy ustaleniu charakteru umowy. W doktrynie i judykaturze dominuje stanowisko, że na gruncie art. 65 k.c. zastosowanie znajduje kombinowana metoda wykładni oparta na kryteriach obiektywnych i subiektywnych[543].

Relacja administrator – podmiot przetwarzający

Relacji administrator – podmiot przetwarzający dotyczy art. 28 RODO, który w ust. 1 stanowi, że jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Obowiązek ten odnosi się on do sytuacji przed zawarciem umowy i nie jest on obowiązkiem wobec drugiej strony umowy. Celem art. 28 ust. 1 RODO, poza zapewnieniem zgodności z RODO jest ochrona prawa osób, których dane dotyczą. Elementami, które należy wziąć pod uwagę, w ramach weryfikacji gwarancji, o których mowa w przepisie są: wiedza

[543] Uchwała SN z 29.06.1995 r., sygn. akt III CZP 66/95, OSNC 1995/12/168; wyrok SN z 8.10.2004 r., sygn. akt V CK 670/03, OSNC 2005/9/162; wyrok SN z 29.04.2009 r., sygn. akt II CSK 614/08; wyrok SN z 15.10.2010 r., sygn. akt V CSK 36/10.

fachowa podmiotu przetwarzającego (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń ochrony danych); wiarygodność podmiotu przetwarzającego; zasoby podmiotu przetwarzającego oraz stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub mechanizmu certyfikacji[544].

W praktyce, jeżeli administrator angażuje podmiot przetwarzający w przetwarzanie w jego imieniu, często oznacza to, że podmiot przetwarzający będzie miał możliwość samodzielnego podejmowania pewnych decyzji co do sposobu przetwarzania. EROD uznaje, że podmiot przetwarzający może mieć pewien margines swobody, aby mógł podejmować pewne decyzje w odniesieniu do przetwarzania. W tym kontekście potrzebne są wytycznych wyjaśniające, jak duży wpływ na „dlaczego" i „jak" może mieć uznanie podmiotu za administratora i w jakim zakresie podmiot przetwarzający może samodzielnie podejmować decyzje[545]. Pytanie brzmi, gdzie wytyczyć granicę między decyzjami zastrzeżonymi dla administratora a decyzjami, które może podejmować podmiot przetwarzający według własnego uznania. Decyzje dotyczące celu przetwarzania danych są oczywiście zawsze podejmowane przez administratora.

Jeśli chodzi o określenie sposobów przetwarzania, można dokonać rozróżnienia między istotnymi sposobami przetwarzania a sposobami innymi niż istotne. „Istotne sposoby przetwarzania" są z natury zastrzeżone dla administratora, podczas gdy sposoby przetwarzania inne niż istotne mogą być również określane przez podmiot przetwarzający. „Istotne sposoby przetwarzania" to sposoby przetwarzania, które są ściśle związane z celem i zakresem przetwarzania, takie jak rodzaj przetwarzanych danych osobowych („jakie dane będą przetwarzane?"), czas trwania przetwarzania („jak długo będą przetwarzane?"), kategorie odbiorców („kto będzie miał do nich dostęp?") oraz kategorie osób, których dane dotyczą („czyje dane osobowe są przetwarzane?"). Wraz z celem przetwarzania danych, podstawowe sposoby przetwarzania są również ściśle powiązane z kwestią, czy przetwarzanie danych jest zgodne z prawem, niezbędne i proporcjonalne. „Sposoby przetwarzania inne niż istotne" dotyczą bardziej praktycznych aspektów wdrażania, takich jak wybór konkretnego rodzaju sprzętu lub oprogramowania lub szczegółowych środków bezpieczeństwa, których wybór może pozostać w gestii podmiotu przetwarzającego[546].

Realizacja omawianego obowiązku zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych powiązana jest z art. 32 ust. 1 lit. d)

[544] Wytyczne 7/2020 EROD, s. 35
[545] Wytyczne 7/2020 EROD., s.16
[546] Wytyczne 7/2020 EROD., s.16

RODO, z którego wynika obowiązek regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Dokonywanie przeglądów i aktualizacja wdrożonych rozwiązań jest także wymogiem sformułowanym wprost w art. 24 ust. 1 RODO, a także wynika z art. 25 ust. 1 RODO, kreującego obowiązek zapewnienia ochrony prywatności w fazie projektowania (privacy by design) i nakładającego na administratora zobowiązanie do wdrożenia odpowiednich środków technicznych zarówno w fazie określania sposobów przetwarzania, jak i w fazie samego przetwarzania. Weryfikacja realizacji w/w obowiązków w relacji powierzenia przetwarzania danych wiąże się z art. 28 ust. 3 lit. h) RODO. Z przepisu tego wynika bowiem, że umowa powierzenia przetwarzania danych osobowych powinna uszczegółowić to, że podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji. Przepis ten daje administratorowi narzędzia zapewniające, że proces przetwarzania danych podlegających powierzeniu będzie zgodny z przepisami RODO, a administrator uniknie odpowiedzialności za ich naruszenie.

W celu zapewnienia nadzoru administrator może prowadzić audyt i inspekcje, o których mowa w art. 28 ust. 3 lit. h) RODO. Realizację w/w obowiązku, należy traktować jako jeden z istotniejszych środków bezpieczeństwa, jakie powinien zastosować administrator w celu prawidłowego wywiązania się ze swoich obowiązków wynikających z art. 32 ust. 1 RODO. Administrator powinien bowiem w czasie korzystania przez niego z usług podmiotu przetwarzającego dysponować wiedzą, czy i w jaki sposób podmiot, któremu powierzył przetwarzanie danych osobowych, spełnia wymogi określone w RODO Brak realizacji audytów, w tym inspekcji, w podmiocie przetwarzającym oznacza naruszenie przepisu art. RODO. Przepis ten obliguje do wdrażania odpowiednich środków technicznych i organizacyjnych, nie tylko przy określaniu sposobów przetwarzania, ale także w czasie samego przetwarzania. Ciągłość wpisana w analizowany obowiązek może więc w praktyce przejawiać się m.in. w konieczności zapewnienia regularnego monitoringu zastosowanych zabezpieczeń oraz prowadzenia stałego nadzoru nad podmiotem przetwarzającym

Z perspektywy podmiotu przetwarzającego relację z administratorem wyznacza ust. 2 art. 28 RODO, który stanowi, że podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.. W przepisie tym określono zatem warunki korzystania z tych usług, czyli albo uzyskanie zgody

szczegółowej (gdy jest konkretny podmiot będący podwykonawcą przetwarzającego), albo zgody ogólnej o charakterze blankietowym (gdy nie wiadomo jeszcze na tym etapie kto będzie podprzetwarzającym). Prawodawca w treści art. 28 ust. 4 wymaga, aby podprzetwarzający również zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych (wybór odpowiedniego podmiotu), jak też, by przestrzegał tych samych obowiązków co podmiot przetwarzający w relacji z administratorem[547]. Rozważania na temat powyższych zagadnień zostaną rozwinięte w dalszej części pracy.

Obowiązki administratora i podmiotu przetwarzającego wdrożenia odpowiednich środków organizacyjnych i technicznych w praktyce orzeczniczej

Kwestia wdrożenia odpowiednich środków organizacyjnych i technicznych w praktyce budzi spore wątpliwości zwłaszcza co do technicznej formy realizacji obowiązków w tym zakresie oraz sposobu ich dokumentowania. Warto tu zwrócić uwagę na istotne stanowisko UODO zawarte w decyzji z 19.01.2022 r.[548] dotyczące zasad prowadzenia audytów, wskazujące, że długotrwała współpraca stron, nie poparta okresowym, systematycznym przeprowadzaniem audytów bądź inspekcji nie gwarantuje, iż podmiot przetwarzający zrealizuje w sposób prawidłowy zadania wymagane przepisami prawa oraz wynikające z zawartej umowy powierzenia. Dotychczasowa, pozytywnie oceniana współpraca stanowić może jedynie punkt wyjścia przy dokonywaniu weryfikacji, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Wymóg określony art. 28 ust. 1 RODO bezwzględnie obowiązuje bowiem każdego administratora danych, który w ramach prowadzonej działalności korzysta z zasobów lub usług podmiotu przetwarzającego podczas przetwarzania danych osobowych. Samo podpisanie umowy powierzenia przetwarzania danych osobowych bez dokonania odpowiedniej oceny podmiotu przetwarzającego nie może być uznane jako realizacja obowiązku przeprowadzenia postępowania weryfikującego podmiot przetwarzający pod kątem spełnienia przez niego wymogów RODO. Z obowiązku przeprowadzenia takiej oceny nie zwalnia również fakt wieloletniej współpracy i korzystania z usług danego podmiotu przetwarzającego przed dniem 25.05.2018 r., tj. przed rozpoczęciem stosowania RODO.

[547] M. Kwiatkowska-Cylke [w:] *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 241.
[548] Decyzja Prezesa UODO z 19.01.2022 r., DKN.5130.2215.2020, https://uodo.gov.pl/decyzje/DKN.5130.2215.2020.

Takie rozumienie obowiązków nałożonych na administratora znajduje potwierdzenie również w wyroku Wojewódzkiego Sądu Administracyjnego z 3.09.2020 r.[549] Sąd orzekł w nim, że: „Rozporządzenie 2016/679 wprowadziło podejście, w którym zarządzanie ryzykiem jest fundamentem działań związanych z ochroną danych osobowych i ma charakter ciągłego procesu. Podmioty przetwarzające dane osobowe zobligowane są nie tylko do zapewnienia zgodności z wytycznymi ww. rozporządzenia poprzez jednorazowe wdrożenie organizacyjnych i technicznych środków bezpieczeństwa, ale również do zapewnienia ciągłości monitorowania poziomu zagrożeń oraz zapewnienia rozliczalności w zakresie poziomu oraz adekwatności wprowadzonych zabezpieczeń. Oznacza to, że koniecznością staje się możliwość udowodnienia przed organem nadzorczym, że wprowadzone rozwiązania, mające na celu zapewnienie bezpieczeństwa danych osobowych, są adekwatne do poziomu ryzyka, jak również uwzględniają charakter danej organizacji oraz wykorzystywanych mechanizmów przetwarzania danych osobowych. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka. Konsekwencją takiej orientacji jest rezygnacja z list wymagań, w zakresie bezpieczeństwa narzuconych przez prawodawcę, na rzecz samodzielnego doboru zabezpieczeń na podstawie analizy zagrożeń. Administratorom nie wskazuje się konkretnych środków i procedur w zakresie bezpieczeństwa. Administrator samodzielnie ma przeprowadzić szczegółową analizę prowadzonych procesów przetwarzania danych i dokonać oceny ryzyka, a następnie zastosować takie środki i procedury, które będą adekwatne do oszacowanego ryzyka.” Podobne stanowisko prezentowane jest w wyroku Wojewódzkiego Sądu Administracyjnego z 26.08.2020 r.[550], w którym zawarte zostało stwierdzenie m.in., że art. 32 rozporządzenia 2016/679 „nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością.” Ponadto Sąd podkreślił również, że „przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą

[549] Wyrok WSA w Warszawie z 3.09.2020 r., sygn. akt II SA/Wa 2559/19.
[550] Wyrok WSA w Warszawie z 26.08.2020 r., sygn. II SA/Wa 2826/19.

musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest, aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka."

Analiza aktualnego orzecznictwa pozwala wywnioskować, że prawodawca w treści RODO podniósł rangę regulacji dotyczącej bezpieczeństwa przetwarzania danych do poziomu zasady przewodniej, co jest spójne ze stanowiskiem zaproponowanym na gruncie nauki prawa, iż z treści art. 32 RODO wynika, że w razie naruszenia fizycznej lub technicznej ochrony danych, ich integralności i/lub poufności – środki techniczne i organizacyjne zapewniały zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich. Chodzi więc o jak najszybsze przywrócenie możliwości dostępu do danych osobom upoważnionym, jak również przywrócenie im możliwości dokonywania operacji na danych[551].

Charakter umowy powierzenia

Zasadą z ust. 3 art. 28 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Umowa w sprawie powierzenia przetwarzania danych innemu podmiotowi nie została w przepisach RODO sprecyzowana co do jej rodzaju. RODO nie wskazuje jaki charakter prawny ma umowa powierzenia przetwarzania danych. Brak także szczególnej regulacji tej umowy w przepisach prawa cywilnego. Ten stan prawny zostawia swobodę wyboru, ale wydaje się, że aktualność zachowuje w związku z tym teza przedstawiona w piśmiennictwie na gruncie ustawy o ochronie danych osobowych z 1997 r.[552], że umowa powierzająca przetwarzanie danych osobowych powinna być kwalifikowana jako umowa o świadczenie usług, nienormowana w sposób szczególny[553]. Bazując na przepisach SUODO przyjmowano, że umowa taka zazwyczaj będzie miała charakter umowy o świadczenie usług, do której odpowiednio stosuje się przepisy dotyczące umowy zlecenia – art. 750 k.c.[554] Pomimo bardzo okrojonej regulacji art. 750 k.c. uważa się, że umowy te należą do najczęściej zawieranych w obrocie, ponieważ dotykają

[551] *Rozporządzenie...*, red. P. Litwiński, Legalis.
[552] Ustawa z 29.08.1997 r. o ochronie danych osobowych (tekst. jedn. Dz.U. 2018 poz. 723).
[553] R. Golat, *Przekazywanie przez pracodawców przetwarzania danych osobowych innym podmiotom*, „Służba Pracownicza" 2011/8, s. 11–14.
[554] J. Barta, P. Fajgielski. R. Markiewicz, *Ochrona danych osobowych...*, s. 508.

niemal wszystkich sfer życia społecznego i gospodarczego[555]. Świadczenie usług występuje w przypadku wszelkich umów obligujących do dokonywania czynności faktycznych (jednorazowych, wielokrotnych, w tym wykonywanych stale) lub do dokonania powiązanych funkcjonalnie czynności faktycznych i prawnych (np. umowy o świadczenie pomocy prawnej, zarządzanie przedsiębiorstwem, majątkiem lub nieruchomością)[556].

Podkreślenia w tym miejscu wymaga, że w literaturze prezentowane są poglądy**,** że przedmiotem tej umowy są usługi publiczne w postaci wykonywania władztwa nad prawami podmiotów trzecich do ich danych**.** Takie stanowisko prezentuje A. Sobczyk, podnosząc w swoich wypowiedziach, że uzasadnieniem dla jego poglądu jest następująca argumentacja. W literaturze trudno jest znaleźć wypowiedzi na temat tego, czym właściwie jest umowa powierzenia przetwarzania danych. Jeśli wsłuchać się w wypowiedzi komentatorów to można dojść do wniosku, że nie budzi niczyich wątpliwości to, że umowa ta jest umową prawa cywilnego. Przyjmując taki punkt widzenia, należałoby stwierdzić według cytowanego Autora, że umowa powierzenia przetwarzania danych osobowych jest umową nazwaną prawa cywilnego. Taki punkt widzenia ma jednak liczne słabości, w których najpoważniejszą jest taka, że nie analizujemy przedmiotu tej umowy. Pewne jest jedynie to, że jej przedmiotem jest „usługa" w zakresie przetwarzania danych a nie usługa polegająca na zaspokojeniu potrzeb podmiotu, będącego administratorem. Te ostatnie wykonywane są na podstawie tzw. umów głównych np. obsługi księgowej, kadrowej itp.

Zresztą, analizując przedmiot owej umowy, należy mieć na względzie, że zgodnie z art. 29 ust. 3 RODO podstawą powierzenia może być inny instrument prawny niż umowa. Nie wchodząc w szczegóły trzeba przyjąć, że musi tu chodzić albo o obowiązek wynikający wprost z prawa lub z indywidualnego aktu administracyjnego. Zasadne jest więc przyjęcie założenia, że przedmiot i charakter owej umowy musi być ostatecznie taki sam jak instrumentu prawnego. Kluczowe dla ustalenia charakteru prawnego umowy powierzenia jest ustalenie, co administrator powierza. Analiza RODO dostarcza argumentów za tym, że istotą umowy powierzenia danych osobowych jest delegowanie na podmiot przetwarzający uprawnień oraz przenoszenie publicznoprawnych obowiązków, które w stosunku do podmiotu danych ma administrator. Warto podkreślić, że administrator nie posiada uprawnień własnych do danych osobowych. Administrator dokonuje jedynie ingerencji w prawa innych osób (autonomię informacyjną) na podstawie norm kompetencyjnych z art. 6 i 9 RODO. Upraszczając,

[555] R. Morek, M. Raczkowski [w:] *Kodeks cywilny. Komentarz,* red. K. Osajda, Warszawa 2018, Legalis.
[556] M. Czech, *Umowa powierzenia…*, s. 175.

administrator dokonuje czynności na cudzych danych czasem wbrew podmiotowi danych, a czasem za jego zgodą, tj. poprzez ustalenie celu i sposobu przetwarzania danych osobowych osób trzecich.

W myśl tego stanowiska administrator dokonuje aktu władztwa publicznego. Przyznając taką kompetencję administratorowi, RODO nakłada na niego szereg obowiązków publicznych, takich jak zapewnienie bezpieczeństwa, obowiązki informacyjne, obowiązek przenoszenia danych itd. Ponadto poddaje administratora nadzorowi publicznemu i karom administracyjnym, co jest typowym rozwiązaniem dla przypadków delegowania kompetencji na podmioty nie będące częścią administracji państwowej. Z tej perspektywy istotą umowy powierzenia przetwarzania danych osobowych jest przeniesienie uprawień administratora danych na inny podmiot, zresztą znajdujący się pod władzą administratora. M. Czech nie precyzuje, czy uznaje w tej sytuacji możliwość zastosowania art. 474 k.c, ale uważa, że ten ostatni nie dość iż ma prawo do wydawania poleceń, to także prawo do kontroli.
Jest to drugi aspekt umowy powierzenia, czyli poddanie się władzy. Uprawnienia administratora danych osobowych w stosunku do podmiotu przetwarzającego nie wynikają bowiem z umowy, ale z prawa. Wraz z „powierzeniem władzy" na podmiot przetwarzający przechodzą co najmniej niektóre obowiązki publiczne, z obowiązkiem zapewnienia bezpieczeństwa na czele. Nie jest to więc umowa o świadczenie usług prywatnych. Jeśli już, to przedmiotem tej umowy są usługi publiczne w postaci wykonywania władztwa nad prawami podmiotów trzecich do ich danych**.** Istotą tej umowy – w odróżnieniu od umowy głównej – jest więc delegacja kompetencji administratora oraz poddanie się jego władztwu. A takie umowy nazywa się umowami prawa publicznego. Umowy takie mają podobny skutek jak jednostronne akty administracyjne. Powyższe wyjaśnia zresztą, że powierzenie może nastąpić czasem na podstawie „innego instrumentu prawnego" (art. 28 ust. 3 RODO)[557].

Prezentowany powyżej pogląd należy zestawić z koncepcją, że specyfika umowy powierzenia przetwarzania danych osobowych, w tym jej akcesoryjny charakter, nie pozwalają na jednoznaczne umiejscowienie jej w klasycznych systematyzacjach umów, co wskazuje na niejednolity charakter prawny umów tego typu. Powoduje to konieczność indywidualnej oceny okoliczności, w jakich ma funkcjonować umowa. W oparciu o przyjęty w nauce prawa prywatnego katalog przesłanek stanowiących warunki prawne umowy nienazwanej należy

[557] Zob. https://sobczyk.com.pl/umowa-powierzenia-przetwarzania-danych-osobowych-a-kary-umowne/; podobnie A. Sobczyk, *RODO. Rozproszona władza publiczna*, Kraków 2019.

uznać, że w kontekście aktualnej regulacji zawartej w treści art. 28 RODO umowę powierzenia należy zakwalifikować do kategorii umów nienazwanych.

Zgodnie z opracowanym przez J. W. Katnera katalogiem przesłanek stanowiących warunki prawne umowy nienazwanej, których łączne spełnienie stanowi o tym, że dany stosunek prawny stanowi umowę nienazwaną można mówić w przypadku:

1. dwustronnej czynności prawnej, będącej ważną umową;
2. braku jej nazwania, choć to nazwanie nie musi wystąpić wprost przez jakiś tytuł, pojęcie itp., może wynikać z kontekstu lub opisania;
3. braku określenia *essentialia negotii* takiej umowy w Kodeksu cywilnego lub w innej ustawie, mimo że mogą być tam umieszczone wskazania, co umowa ma w swej treści zawierać;
4. braku tożsamości umowy z umową nazwaną albo takiego prawdopodobieństwa, które wskazuje na rodzaj umowy nazwanej;
5. określenia stron umowy, jej przedmiotu i treści, w tym zwłaszcza praw i obowiązków stron;
6. pozostawania w zgodzie z porządkiem prawnym, tzn. w zgodności kreowanego stosunku prawnego (jego treści i celu) z jego właściwościami (naturą), ustawami i zasadami słuszności, jak też dobrymi obyczajami (nazywanymi obecnie w art. 353^1 k.c. zasadami współżycia społecznego)[558].

Analiza tych przesłanek w kontekście umowy powierzenia przetwarzania danych osobowych prowadzi do wniosku, że umowa powierzenia przetwarzania danych osobowych ze swej natury jest dwustronną czynnością prawną. Stanowi ważną umowę, bo podstawą prawną jest przepis prawa przewidujący jej zawarcie w przypadku „zlecania" przetwarzania danych osobowych podmiotowi innemu niż administrator. Nazwa umowy nie wynika z aktualnie obowiązujących przepisów prawa przedmiotowej, jest raczej wytworem zarówno rozwijającej się nauki jak i praktyki w obszarze ochrony danych osobowych. Nie jest to umowa tożsama lub podobna do umowy nazwanej. Określenie stron umowy, przedmiotu i treści, praw i obowiązków stron wynika z treści art. 28 RODO, przy czym jedne w sposób literalny, a inne wymagają wyinterpretowania. Kwestia najtrudniejszą do rozstrzygnięcia jest czy umowa ta zawiera elementy przedmiotowo istotne dla umowy powierzenia przetwarzania danych osobowych, bez których nie można mówić o tej umowie, czy jedynie wskazania co taka umowa ma zawierać w swojej treści. W treści art. 28 ust. 3 RODO wymienia obligatoryjne elementy umowy powierzenia przetwarzania danych osobowych. Stronom nie pozostawiono możliwości rezygnacji z tych elementów. W literaturze podkreśla się z powołaniem na doktrynę niemiecką,

[558] W.J. Katner [w:] *System Prawa Prywatnego*, red. W.J. Katner, t. 9, *Prawo zobowiązań – umowy nienazwane*, Warszawa 2015, s. 13.

że jeżeli odpowiednia umowa jest sprzeczna z wytycznymi przewidzianymi w art. 28 RODO oraz gdy brak jest alternatywnej podstawy w postaci innego instrumentu prawnego, powierzenie przetwarzania danych jest bezskuteczne z uwagi na brak koniecznej podstawy prawnej[559]. Na gruncie prawa krajowego generalnie przyjmuje się, że umowa pozbawiona essentialia negotti jest nieważna, a taka umowa nie podlega zmianom – w tym np. uzupełnieniom[560].To oznacza, że wymienione w art. 28 RODO elementy umowy kwalifikuje jako *essentialia negotii* umowy[561]. W przypadku braku wymienionych elementów umowa, po pierwsze nie spełnia wymogów wynikających z przepisów prawa, a po drugie nie pozwala na prawidłowe wykonanie zobowiązania[562].

Ponadto zgodnie z klasycznymi na gruncie prawa cywilnego podziałami umów, umowa powierzenia przetwarzania danych osobowych została zakwalifikowana jako zobowiązująca (kształtuje zobowiązanie na mocy art. 353 §1 k.c. i nie stanowi rozporządzenia), dwustronnie zobowiązująca (a dokładniej wzajemna), w pewnych okolicznościach może mieć charakter umowy konsensualnej, a w innych realnej. Uzasadnieniem dla stanowiska, że umowa przetwarzania danych osobowych jest umową konsensualną, za czym opowiada się A. Krasuski i D. Skolimowska[563] jest fakt, że przedmiotowa umowa zawierana jest w konsekwencji złożenia zgodnych oświadczeń woli stron, a nie ma konieczności wręczenia rzeczy. Jeżeli jednak umowa jest skonstruowana w taki sposób, że zbiór danych musi być wydany podmiotowi przetwarzającemu, (np. w formie nośnika z danymi, czy to papierowego czy elektronicznego), aby mógł on realizować zobowiązanie, umowa taka w drodze wspólnych uzgodnień będzie miała charakter umowy realnej. Umowa powierzenia przetwarzania jest też umową odpłatną, ponadto może być umową swobodnie negocjowaną i adhezyjną. W praktyce doniosłym jest akcesoryjny charakter umowy – jest ona zawsze umową związaną z umową zasadniczą, nie występuje w obrocie samodzielnie[564].

Oceniając powyższe poglądy, stwierdzić należy, że uznanie umowy powierzenia przetwarzania danych za umowę, której przedmiotem są usługi publiczne jest istotnym głosem w dyskusji dotyczącej charakteru RODO jako aktu i jego miejsca w porządku prawnym. Prezentowana w tym zakresie argumentacja nie odnosi się jednak do tego, że nie zmieniając istoty tej umowy jako umowy cywilnoprawnej w ślad za tym stanowiskiem możemy przyjąć,

[559] K. Witkowska-Nowakowska [w:] *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, komentarz do art. 28.
[560] M.in. wyrok SO w Łodzi z 27.04.2017 r., sygn. akt III Ca 119/17.
[561] M. Sakowska-Baryła [w:] *Ogólne...*, red. M. Sakowska Baryła, s. 320.
[562] M. Czech, *Umowa powierzenia...*
[563] A. Krasuski, D. Skolimowska, *Dane osobowe w przedsiębiorstwie*, Warszawa 2007, s. 130.
[564] M. Czech, *Umowa powierzenia...*, s. 327.

że umowa powierzenia przetwarzania danych może rodzić także skutki na gruncie prawa publicznego. Dominującą w tym zakresie jest jednak wykładnia, która związana jest z tym, że na gruncie obowiązujących aktów prawa krajowego (np. art. 429 k.c., art. 124 k.p., art. 6a pr. bank.) powierzenie kojarzone jest z przekazaniem czegoś przez jeden podmiot innemu podmiotowi, „zleceniem" określonych czynności, przeniesieniem wykonywania obowiązków lub praw z jednego podmiotu, by w jego imieniu wykonywał je inny podmiot, co czyni w sektorze prywatnym z umowy powierzenia umowę cywilnoprawną. Obrona tezy, że administrator nie będący podmiotem publicznym jest podmiotem (organem) administrującym i jako taki wykonuje zadania i funkcje publiczne (ingeruje w prawa i wolności jednostek w imię dobra wspólnego), co nie zmienia jego prywatnego charakteru wymagałaby w niniejszej pracy rozstrzygania kwestii skutków prawnych stosowania innego instrumentu prawnego, co pozostaje poza zakresem prowadzonych rozważań.

Umowa powierzenia przetwarzania danych powinna mieć formę pisemną bez zastrzeżonego szczególnego rygoru niedochowania formy. Wymóg spisania postanowień dotyczących powierzenia przetwarzania służyć ma nie tylko celom dowodowym, ale ma przyczynić się do jasnego określenia zakresu uprawnień i obowiązków stron umowy lub podmiotów, których dotyczy inny akt prawny (zarówno administratora, jak i podmiotu, któremu powierzono przetwarzanie). Prawodawca unijny nie ogranicza swobody jedynie do tradycyjnej postaci papierowej, ale przewiduje również możliwość sporządzenia dokumentu w postaci elektronicznej. Wykładnia prowadząca do uznania, że prawodawca wymaga zachowania zarówno formy pisemnej (dokumentu w postaci papierowej), jak (równocześnie) postaci elektronicznej, nie wydaje się prawidłowa. Wydaje się, iż należy przyjąć za wystarczające, aby postanowienia umowy zostały spisane, a sposób ich utrwalenia może przybrać postać papierową lub elektroniczną. Taką interpretację zdają się potwierdzać inne wersje językowe rozporządzenia (ang. *shall be in writing, including in electronic form,* niem. *ist schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann*)[565].

W RODO określenie „forma elektroniczna" pojawiło się także w motywie 58, gdzie jako formę elektroniczną przekazania informacji rozumie się na przykład stronę internetową. Należy zatem wskazaną w art. 28 RODO formę elektroniczną zawarcia umowy powierzenia utożsamiać z formą dokumentową. Do zachowania dokumentowej formy czynności prawnej (tu zawarcia umowy powierzenia) wystarcza zgodnie z przepisami Kodeksu cywilnego złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby

[565] Zob. P. Fajgielski,.....

składającej oświadczenie. Dokumentem jest nośnik informacji umożliwiający zapoznanie się z jej treścią (art. 77^2 i 77^3 k.c.).

Obowiązki podmiotu przetwarzającego

Po omówieniu zagadnienia charakteru umowy należy przyjrzeć się obowiązkom podmiotu przetwarzającego, które można podzielić na dwie grupy. Pierwsza grupa, to obowiązki wynikające ze stosunku powierzenia skoncentrowane wokół relacji tego podmiotu z administratorem. Wynikają one w głównej mierze z art. 28 RODO. Warto przy tym zwrócić uwagę na specyficzną konstrukcję art. 28 ust. 3 zd. 2, w którym określono szereg obowiązków ciążących na podmiocie przetwarzającym względem administratora. W tym przepisie zostały one ukształtowane jako obligatoryjne, które zastrzeżone mają być w umowie lub w „innym instrumencie prawnym" stanowiących podstawę powierzenia. Wyliczenie to nie ma charakteru zamkniętego. To egzemplifikacja, ale jednocześnie obowiązki stanowiące pewien minimalny próg. Zasadniczo wynikają one z RODO, a jednocześnie – zgodnie z art. 28 ust. 3 zd. 2 – muszą wynikać z umowy lub innego aktu będącego podstawą powierzenia przetwarzania danych[566].

W tej grupie obowiązków znajdują się te, które ściśle związane z pozycją administratora i w treści których wymaga się od przetwarzającego podlegania poleceniom administratora. Do obowiązków tych należy wymóg przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO) oraz wymóg usunięcia lub zwrotu wszelkich danych osobowych i ich istniejących kopii po zakończeniu umowy zależnie od decyzji administratora (art. 28 ust. 3 lit. g RODO). Dalsze obowiązki dotyczą zapewnienia bezpieczeństwa przetwarzanych danych, stanowiące pierwotnie obowiązki administratora, ale ze względu na dokonanie powierzenia będące pochodną obowiązków administratora. Wśród nich jest zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy (art. 28 ust. 3 lit. b RODO), podejmowanie wszelkich środków wymaganych na mocy art. 32 RODO (art. 28 ust. 3 lit. c RODO), jak również przestrzeganie warunków korzystania z usług innego podmiotu przetwarzającego (art. 28 ust. 3 lit. d RODO). Kolejne obowiązki dotyczą wspierania administratora w realizacji jego zobowiązań wynikających z przepisów prawa, w tym: pomoc administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw, poprzez odpowiednie środki techniczne i organizacyjne (art. 28 ust. 3 lit. e RODO), pomoc administratorowi w wywiązywaniu się z

[566] M. Sakowska-Baryła [w:] *Czy jesteśmy gotowi…*, s. 107.

obowiązków określonych w art. 32–36 (art. 28 ust. 3 lit. f RODO), jak również udzielanie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków, w tym umożliwianie administratorowi przeprowadzanie audytów, w tym inspekcji i przyczynianie się do nich[567].

Druga grupa obowiązków to te, które zgodnie z treścią RODO są nakładane na podmiot przetwarzających bezpośrednio w przepisach tego rozporządzenia. Podkreślić bowiem należy, że RODO adresatem swoich przepisów stosunkowo często, obok administratora, czyni równocześnie podmiot przetwarzający. Co więcej, obowiązki podmiotu przetwarzającego często bywają tożsame lub bardzo zbliżone do obowiązków administratora. Wypada tu wspomnieć choćby o obowiązkach dotyczących zabezpieczenia danych (art. 32 RODO), zapewnienia współpracy z organem nadzorczym (art. 31 RODO), wyznaczenia inspektora ochrony danych (art. 37–39 RODO), przekazywania danych do państw trzecich lub organizacji międzynarodowych (art. 44–50 RODO). Można tu także wskazać na adresowanie bezpośrednio do podmiotu przetwarzającego przepisów RODO dotyczących kwestii korzystania z kodeksów postępowań i certyfikacji (art. 40–43), dopuszczalność zastosowania przez organ nadzorczy uprawnień w zakresie prowadzonych postępowań (art. 58), w tym nakładania administracyjnych kar pieniężnych (art. 83)[568].

Powyższe rozważania uzasadniają twierdzenie, że przepisy RODO kształtują dwie kategorie obowiązków ciążących na procesorze w związku z przetwarzaniem danych. Pierwsza kategoria obejmuje obowiązki procesora, które powinny wynikać z umowy powierzenia zawartej z administratorem (art. 28 RODO). Do drugiej kategorii można zaliczyć samodzielne obowiązki procesora, tj. te, których bezpośrednim źródłem są przepisy RODO. Będą należeć do niej następujące obowiązki:

1. niekorzystania z usług innego podmiotu przetwarzającego bez zgody administratora (art. 28 ust. 2 RODO);
2. przetwarzania danych wyłącznie na polecenie administratora (art. 29 RODO);
3. prowadzenia rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 2 RODO);
4. współpracy z organem nadzorczym (art. 31 RODO);
5. zapewnienia bezpieczeństwa przetwarzania (32 RODO);

[567] M. Czech, *Powierzenie przetwarzania...* s. 235.
[568] M. Sakowska-Baryła [w:] *Czy jesteśmy gotowi…*, s. 107.

6. niezwłocznego zgłoszenia administratorowi naruszenia ochrony danych osobowych (art. 33 ust. 2 RODO);
7. powołania inspektora ochrony danych (art. 37 ust. 1 RODO).

Wymagania dotyczące treści umowy lub innego instrumentu prawnego

Artykuł 28 RODO określa wymagania dotyczące treści umowy lub innego instrumentu prawnego stanowiącego podstawę powierzenia przetwarzania oraz wskazuje obowiązki stron umowy, w tym w szczególności obowiązki podmiotu przetwarzającego, które powinny być zawarte w umowie lub innym instrumencie prawnym[569]. W praktyce oznacza to, że w sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora.

Postrzegając przetwarzanie danych osobowych przez pryzmat całego RODO, w pełni uzasadniony jest wymóg zawarcia stosunkowo szczegółowego opisu przetwarzania w umowie powierzenia. Kompleksowe zawarcie w tej umowie elementów wynikających z art. 28 ust. 3 RODO ma na celu bowiem zapewnienie precyzyjnego ustalenia granic działania podmiotu

[569] Wymagania odnoszące się do treści obejmują konieczność określenia w umowie (lub innym instrumencie prawnym) następujących kwestii:
1) przedmiotu i czasu trwania przetwarzania;
2) charakteru i celu przetwarzania;
3) rodzaju danych osobowych oraz kategorie osób, których dane dotyczą;
4) obowiązków i praw administratora.
W dalszej części art. 28 RODO stanowi, że podmiot przetwarzający:
a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

przetwarzającego, co stanowi podstawę umowy powierzenia ze względu na związanie podmiotu przetwarzającego z celem ustalonym przez administratora.

Mechanika współpracy z podmiotem przetwarzającym powinna wyglądać tak, że przed rozpoczęciem współpracy podmiot przetwarzający dostaje od administratora polecenie dokonania oceny ryzyka dotyczące środków organizacyjnych i technicznych. Po dokonaniu takiej oceny podmiot przetwarzający powinien wraz z administratorem wpisać środki organizacyjne i techniczne do umowy i uszczegółowić zasady wzajemnej współpracy w trakcie trwania umowy. Ostatnim etapem negocjacji w sprawie powierzenia są regulacje dotyczące zakończenia umowy. Po zakończeniu przetwarzania w imieniu administratora, podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych.

W praktyce istotne jest także, aby w sposób skonkretyzowany określony został zakres powierzenia i jego skutki. Jako wadliwe działanie wskazane zostało przez UODO[570] zawieranie umowy powierzenia, w sposób niewystarczająco doprecyzowujący te zagadnienia. Zdaniem UODO określenie, że „podmiot przetwarzający w ramach świadczenia usługi hostingowej przetwarzał będzie powierzone dane osobowe zwykłe obejmujące zbiory danych osobowych niezbędne do wykonywania prac w systemie informatycznym na rzecz administratora" oznacza, że administrator nie wskazał kategorii osób, których dane dotyczą, wymaganych przez art. 28 ust. 3 RODO. Posłużył się jedynie pojęciem zbioru danych osobowych. Stosując wykładnię celowościową należy wskazać, że w tym kontekście „rodzaj danych", również wymagany ww. przepisem, odnosi się do informacji dotyczącej charakterystyki określonej, znanej administratorowi, grupy podmiotów danych osobowych, które w umowie powierzenia nie zostały wskazane.

Opisując przetwarzanie danych, umowa powinna również odwoływać się do ich kategorii, jeśli można je doprecyzować. O ile w przypadku przetwarzania danych związanych np. z usługą poczty elektronicznej, trudno jest jednoznacznie taki zakres wskazać, o tyle w przypadku przetwarzania danych w celach związanych z funkcjonowaniem platformy szkoleniowej, informacje takie, jako możliwe do określenia, powinny być zawarte.

Zgodnie z art. 28 ust. 3 pkt a) RODO umowa powierzenia przetwarzania danych stanowi m.in., że podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora. W związku z obowiązkiem określonym w akapicie

[570] Decyzja UODO z 11.02.2021 r., znak sprawy: DKN.5130.2024.2020.

pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych. W ocenie organu nadzoru umowa powierzenia powinna zawierać przynajmniej ogólne sformułowanie zobowiązujące podmiot przetwarzający do działania wyłącznie na udokumentowane polecenie administratora. O ile w pewnym stopniu element ten można wyinterpretować z § 3 pkt 3 umowy głównej, zgodnie z którym *„*zgłoszenia usterek związanych z usługami hostingowymi, w tym ich niedostępność, dokonywane będą pisemnie, faksem lub pocztą elektroniczną*”,* o tyle w ocenie według Prezesa UODO wskazane postanowienie umowy jest niewystarczające.

Jak wskazuje się w literaturze przedmiotu, w praktyce obowiązki wynikające z art. 28 ust. 3 pkt a-h RODO będą wymagać skonkretyzowania w sposób adekwatny do zadań, operacji przetwarzania, zaplecza logistycznego, kategorii danych i osób, których dane dotyczą, ram czasowych i terytorialnych powierzonego przetwarzania.[571] Nie można w zapominać, że zgodnie z art. 353 [1] k.c. strony mają swobodę w zakresie treści wymaganych postanowień. Prawodawca ustalił w treści art. 28 ust. 3 pkt a-h RODO sferę obowiązków podmiotu przetwarzającego, jako minimalne wymagania. To oznacza, że sposób realizowana obowiązków podmiotu przetwarzającego może być przedmiotem ustaleń stron, np. w kwestii uregulowania uprawnień kontrolnych administratora nad przetwarzaniem powierzonych danych przez podmiot przetwarzający, czy zasad współpracy stron np. w kontekście audytów, w tym ram prowadzenia działań sprawdzających przez administratora, zasad dostępu do informacji o sposobach przetwarzania danych przez przetwarzającego i stosowanych przez niego zabezpieczeniach. Ustalenie zasad partycypacji podmiotu przetwarzającego w realizacji tych zadań ma szczególnie istotne znaczenie z perspektywy administratora, rozliczanego przez organ nadzorczy z ich realizacji.

Słusznie podkreśla się, że ze zobowiązaniem podmiotu przetwarzającego do wsparcia w wykonywaniu opisanych powyżej obowiązków współgrają normy adresowane bezpośrednio do tego podmiotu, mieszczące się w art. 32–36 RODO. W konsekwencji, poza nałożeniem na podmiot przetwarzający obowiązku zastosowania odpowiednich środków bezpieczeństwa wynikającego z art. 32 RODO, wskazać należy w tym aspekcie na zobowiązanie podmiotu przetwarzającego do obowiązków implikujących konieczność przeprowadzenia kompleksowej, rzetelnej i wyczerpującej analizy procesów przetwarzania i całego kontekstu, w jakim to przetwarzanie się odbywa. Do takiego całościowego zbadania danego procesu

[571] *Ogólne...*, red. M. Sakowska-Baryła, s. 324.

przetwarzania niezbędne jest uzyskanie przez administratora szeregu informacji, w tym m.in. w zakresie stosowanych środków bezpieczeństwa, certyfikacji w określonych obszarach, zidentyfikowanych po stronie podmiotu przetwarzającego zagrożeń i ryzyk związanych z przetwarzaniem[572].

Standardowe klauzule umowne

W motywie 81 preambuły RODO wskazane zaostało, że administrator i podmiot przetwarzający mogą postanowić skorzystać z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez Komisję albo które zostały przyjęte przez organ nadzorczy zgodnie z mechanizmem spójności, a następnie przyjęte przez Komisję. Zgodnie z treścią ust. 6 art. 28 RODO, postanowienia umów dotyczących powierzenia mogą opierać się na standardowych klauzulach w całości lub w części, co oznacza, że jeżeli podmioty zdecydują się na wykorzystanie standardowych klauzul, to nie będą musiały przyjmować wszystkich wzorcowych klauzul, ale będą mogły również dokonać wyboru tych spośród standardowych klauzul, które im odpowiadają[573].

Motyw 109 preambuły RODO wskazuje, że możliwość korzystania ze standardowych klauzul ochrony danych nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi ani nie naruszają podstawowych praw lub wolności osób.

Pierwszymi standardowymi klauzulami umownymi wydanymi na gruncie RODO były duńskie standardowe klauzule umowne. Po wydanej przez Europejską Radę Ochrony Danych w lipcu 2019 r. opinii w sprawie projektu standardowych klauzul umownych (ang. *standard contractual clauses* – SCC) dla umów między administratorami a podmiotami przetwarzającymi dane, przedstawionego do zaopiniowania przez EROD przez duński organ nadzorczy, ostateczny tekst klauzul, przyjęty przez tenże organ, został opublikowany w prowadzonym przez EROD Rejestrze decyzji wydanych przez organy nadzorcze i sądy w przedmiocie kwestii rozstrzyganych w ramach mechanizmu spójności. Standardowa umowa z podmiotem przetwarzającym została przyjęta przez duński organ nadzorczy w związku z art. 28 ust. 8 RODO i ma na celu wsparcie organizacji w spełnieniu wymogów określonych w art. 28 ust. 3 i 4, biorąc pod uwagę okoliczność, że umowa między administratorem a podmiotem

[572] K. Witkowska-Nowakowska, *Komentarz do art. 28 RODO*…, s. 642–643.
[573] P. Fajgielski, *Ogólne rozporządzenie o ochronie...*, s. 347.

przetwarzającym nie może jedynie powielać zapisów RODO, ale powinna je dodatkowo uściślać, np. w związku ze wsparciem, którego podmiot przetwarzający udziela administratorowi.

Możliwość użytkowania standardowych klauzul umownych przyjętych przez organ nadzorczy nie przekreśla możliwości dodawania przez strony innych klauzul lub dalszych zabezpieczeń, pod warunkiem, że nie będą one stać (pośrednio lub bezpośrednio) w sprzeczności z przyjętymi klauzulami i nie będą stanowiły uszczerbku dla fundamentalnych praw i wolności osób, których dane dotyczą. Klauzule są narzędziem, którego należy używać „takimi, jakimi są", tj. strony umowy, która zawiera zmodyfikowaną wersję klauzul, nie są uznawane za stosujące przyjęte standardowe klauzule umowne. Przeciwnie, w zakresie w jakim organizacje te zdecydują się na wykorzystanie standardowych zapisów, duński organ nadzorczy, na przykład w związku z inspekcją, nie zbada tych zapisów szczegółowo[574].

W tym miejscu dodać należy, że w kwietniu 2020 r. szwedzki organ nadzorczy uznał, iż duńskie standardowe klauzule umowne przetwarzania danych osobowych mogą być stosowane również w Szwecji. Z możliwości, jaką daje art. 28 ust. 8 RODO polskie organ nadzoru jeszcze nie skorzystał.

Analiza standardowych klauzul umownych przyjętych przez duński organ nadzoru prowadzi do wniosku, że wszystkie zagadnienia dotyczące przetwarzania powinny zostać zawarte w umowie, a w odniesieniu do każdej kategorii przetwarzania należy wypełnić załączniki. Klauzule te są wyrazem bardzo daleko posuniętego formalizmu umów, nie tylko z uwagi na szczegółowość tych załączników, ale także fakt rozumienia polecenia przetwarzania w taki sposób, że jego udokumentowana treść ma zostać wpisana wprost do umowy. W zakresie polecenia zgodnie z klauzulami umowę powierzenia należy uzupełnić o postanowienia, które regulowałyby sytuację niezgodnych z prawem poleceń administratora, co oznacza, że umowa powinna zawierać postanowienia, co do tego, co się dzieje np. z terminem wykonania przedmiotu umowy, jeżeli administrator otrzyma od podmiotu przetwarzającego informację, że polecenie przetwarzania nie jest zgodne z prawem.

Z punktu widzenia zasad odpowiedzialności konieczne jest podkreślenie, że zgodnie ze standardowymi klauzulami umownymi podmiot przetwarzający jest odpowiedzialny nie tylko za nałożenie na podwykonawcę podmiotu przetwarzającego dane wymogu, aby spełniał on co najmniej obowiązki, którym podlega podmiot przetwarzający zgodnie z tymi klauzulami i przepisami ogólnego rozporządzenia o ochronie danych, ale podmiot przetwarzający ma

[574] Newsletter dla IOD, UODO 2020/2.

obowiązek uzgodnić z podwykonawcą podmiotu przetwarzającego dane klauzulę dotyczącą beneficjenta będącego osobą trzecią. Standardowe klauzule umowne zakładają, że jeżeli – w przypadku upadłości podmiotu przetwarzającego – administrator danych jest beneficjentem będącym osobą trzecią w stosunku do umowy z podwykonawcą przetwarzania ma prawo wyegzekwować tę umowę od podwykonawcy przetwarzania zaangażowanego przez podmiot przetwarzający, np. umożliwić administratorowi danych polecenie podwykonawcy przetwarzania usunięcia lub zwrotu danych osobowych.

Stopień szczegółowości standardowych klauzul umownych i zaprojektowanych załączników skłania do refleksji, że jest to jednak na tyle elastyczny wzór umowy, że w zasadzie można go stosować w oderwaniu od umowy głównej i może on stanowić odrębny byt, jeżeli nie w znaczeniu prawnym to w znaczeniu praktycznym, tzn. jako umowa, której negocjowanie nie jest konieczne w każdym przypadku zmiany umowy głównej. W tym miejscu wskazać należy, że zgodnie z założeniami RODO umowa powierzenia przetwarzania danych ma charakter umowy akcesoryjnej w stosunku do umowy głównej.

W dniu 4.06.2021 r. wydana została decyzja wykonawcza Komisji Europejskiej w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia PE (UE)[575] oraz art. 29 ust. 7 rozporządzenia PE (UE) 2018/1725 – decyzja 2021/915[576]. W dniu 4.06.2021 r. wydana została także decyzja wykonawcza Komisji Europejskiej w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (Dz. U. UE. L. z 2021 r. Nr 199, str. 31) – decyzja 2021/914[577].

W tym miejscu zaznaczyć należy, że ze względu na ograniczony temat pracy problem podstaw prawnych legalności transferu danych nie został objęty badaniem.

Przechodząc zatem do analizy decyzji wykonawczej w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi podkreślić należy, że

[575] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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. L 119 z 4.5.2016).

[576] Decyzja wykonawcza Komisji (UE) 2021/915 z 4.06.2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725, (Dz.Urz. L 199 z 7.6.2021);
https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32021D0915&from=EN

[577] Decyzja wykonawcza Komisji (UE) 2021/914 z 4.06.2021 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, Dz.U. L 199 z 7.6.2021, str. 31—61;
https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32021D0914&from=PL

zgodnie z jej treścią w motywie 6 powtórzony został motyw 109 RODO. W myśl motywu 10 standardowych klauzul umownych (z decyzji wykonawczej 2021/915) nie można stosować jako standardowych klauzul umownych do celów rozdziału V rozporządzenia PE UE – 2016/679, co oznacza, że SCC nie nadają się do legalizacji transferu danych poza EOG.

Motyw 12 zakłada, że klauzule podlegają okresowej ocenie zgodnie z art. 97 RODO. Na podstawie art. 1 wprowadzona została zaś zasada, że standardowe klauzule spełniają wymogi dotyczące umów zawieranych między administratorami a podmiotami przetwarzającymi określone w art. 28 ust. 3 i 4 rozporządzenia (UE) 2016/679, co stanowi o pewność zgodności treści wzorca umowy z wymogami RODO. Artykuł 2 przewiduje możliwość stosowania klauzul (tylko) w umowach pomiędzy administratorami a podmiotami przetwarzającymi.

Struktura decyzji zbudowana jest na schemacie:

- Sekcja I (klauzule 1–5) reguluje klauzule ogólne;
- Sekcja II (klauzule 6–9) reguluje obowiązki stron;
- Sekcja III (klauzula 10) zawiera postanowienia końcowe.

Odpowiednio do tej struktury skonstruowane są załączniki:

- Załącznik I przewiduje wykaz stron;
- Załącznik II – opis przetwarzania;
- Załącznik III – środki techniczne i organizacyjne (opcjonalnie);
- Załącznik IV – wykaz podmiotów podprzetwarzających.

Zgodnie z założeniem niezmienności klauzul w decyzji zawarte zostało zobowiązanie stron do niezmieniania klauzul z wyjątkiem dodawania informacji do załączników lub aktualizowania zawartych w nich informacji oraz postanowienie, że SCC można umieszczać w treści umowy o szerszym zakresie (np. umowy głównej), jak też dodawać inne klauzule lub dodatkowe zabezpieczenia, o ile bezpośrednio lub pośrednio nie będą sprzeczne z SCC ani nie będą naruszały podstawowych praw lub wolności osób.

Według wspólnej opinii EIOD i EROD 1/2021[578] klauzule sprzeczne z SCC to takie, które podważają lub negatywnie wpływają na obowiązki określone w SCC lub uniemożliwiają przestrzeganie obowiązków określonych w SCC. Na przykład klauzule zezwalające podmiotom przetwarzającym na wykorzystywanie danych do własnych celów. Zgodnie z klauzulą 4 przyjęte zostało pierwszeństwo SCC w razie sprzeczności z postanowieniami

[578] Wspólna opinia EROD i EIOD1/2021 dotycząca decyzji wykonawczej Komisji Europejskiej w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_pl.pdf

powiązanych umów między stronami. Przystąpienie do SCC uregulowane zostało według zasady, że każdy podmiot niebędący stroną SCC może za zgodą wszystkich stron przystąpić do SCC jako administrator lub podmiot przetwarzający, wypełniając załączniki i podpisując załącznik I, stając się przez to stroną klauzul zgodnie z jego rolą określoną w załączniku I (klauzula 5). Klauzula 7 dotycząca obowiązków stron wskazuje na pełną odpowiedzialność za subprocesora (art. 28 ust. 4 RODO *in fine*) oraz obowiązek powiadomienia administratora o niewywiązaniu się subprocesora z jego zobowiązań umownych. W dalszej części stanowi, że procesor uzgadnia z subprocesorem klauzulę dotyczącą beneficjenta będącego osobą trzecią, zgodnie z którą, jeżeli podmiot przetwarzający przestanie istnieć faktycznie lub formalnie lub stanie się niewypłacalny, administrator ma prawo rozwiązać umowę z subprocesorem i nakazać mu usunięcie lub zwrot danych osobowych.

Charakter świadczeń podmiotu przetwarzającego

Zgodnie z przeważającym poglądem doktryny, o czym była mowa wcześniej umowa powierzenia przetwarzania jest umową o świadczenie usług. Należy poprzeć to stanowisko jednocześnie zaznaczając wewnętrzną niejednolitość w ramach umowy tego typu, ponieważ z praktyki zawierania umów powierzenia można odnieść wrażenie, że część z nich będzie miała charakter umowy o świadczenie usług z wyraźnymi elementami umowy zlecenia, a część (choć zdecydowanie mniejsza) – charakter umowy o świadczenie usług z wyraźnymi elementami umowy o dzieło. Trzeba zwrócić uwagę przede wszystkim na fakt, że przedmiotem umowy powierzenia przetwarzania danych osobowych jest świadczenie polegające na przetwarzaniu danych.

Natomiast przetwarzanie to nie tylko czynności faktyczne, ale również czynności prawne. Czynnością prawną w zakresie pojęcia przetwarzania danych osobowych będzie podpowierzenie (dalsze powierzenie) przetwarzania danych, które następuje w drodze umowy z podwykonawcą (tzw. podprzetwarzającym). Powyższa konstatacja wymaga dokonania oceny tego, czy do konkretnej umowy powierzenia przetwarzania danych osobowych należy stosować odpowiednio przepisy o zleceniu, czy też dana umowa jest jednak bardziej podobna do umowy o dzieło. Rozstrzygnięcie tego zagadnienia wymaga każdorazowej analizy przedmiot umowy, a dokładniej oceny tego, jakie operacje wchodzące w zakres przetwarzania danych osobowych będzie obejmowała umowa. W przypadku gdy administrator danych powierza np. takie czynności jak zbieranie, przechowywanie, porządkowanie, powielanie danych, to z uwagi na fakt, że są to czynności traktowane jako staranne działanie, to faktycznie przepisy o zleceniu są bardziej odpowiednie biorąc pod uwagę, że jest to umowa starannego działania i nie oczekuje

się by strona odpowiadała za efekt swoich działań. Umowa powierzenia stanowi w tym przypadku umowę o świadczenie usług z wyraźnymi elementami umowy zlecenia. Natomiast w przypadku, kiedy umowa powierzenia jest integralną częścią umowy np. na usługę niszczenia czy to dokumentów w formie papierowej, czy też elektronicznych nośników informacji, dotyczy ona rezultatu działania przetwarzającego – chodzi o efekt usunięcia danych. Ten rodzaj operacji dokonywanych na danych powinien być rozpatrywany w kategorii dzieła jako umowy rezultatu, a nie zlecenia, jako starannego działania podmiotu świadczącego usługi niszczenia dokumentów. W takiej sytuacji umowa powierzenia może być rozpatrywana jako umowa o świadczenie usług z wyraźnymi elementami umowy zlecenia. Skłania to również do sformułowania wniosku, że charakter umowy powierzenia w głównej mierze jest zależny od umowy zasadniczej, z którą jest związana. Jeśli umowa zasadnicza jest umową starannego działania i ma cechy zlecenia (np. archiwizacja akt osobowych pracowników, wynajęcie miejsca na serwerze), to umowa powierzenia również ma ten charakter[579].

Odpowiedzialność deliktowa podmiotu przetwarzającego

Odpowiedzialność podmiotu przetwarzającego ma istotne znaczenie praktyczne, dlatego że to właśnie jego działania, a nie bezpośrednie działania administratora pozyskującego dane osobowe, stają się często źródłem ryzyka powstania szkody. Zgodnie z art. 82 ust. 2 RODO podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Podmiot przetwarzający zostaje zwolniony z odpowiedzialności, jeżeli udowodni, „że w żaden sposób nie ponosi winy" za zdarzenie, które doprowadziło do powstania szkody.

W pierwszej kolejności z powyższej regulacji wywieść należy, że odpowiedzialność podmiotu przetwarzającego jest odpowiedzialnością deliktową, podobną do odpowiedzialności administratora, którą analizowano w niniejszej pracy. Z ust. 1 art. 82 RODO wynika, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. RODO nie definiuje pojęcia każda osoba, ale odnosi się wielokrotnie wprost do pojęcia osoba fizyczna, np. w art. 4 pkt 1, 4, 5, 13, 14, 15, art. 6 ust. 1 lit. d, art. 9 ust. 1, ust. 2 lit. c . Treść tego przepisu nie ogranicza pojęcia „każda osoba"

[579] M. Czech, *Umowa powierzenia*… s. 177.

wyłączenie do relacji podmiot przetwarzający – podmiot danych. To oznacza, że osoba prawna nie została wyłączona z możliwości powołania się na ten przepis[580], który może stanowić podstawę prawną dochodzenia roszczeń w relacji podmiot przetwarzający – administrator. Mając na uwadze wcześniejsze rozważania dotyczące konstruowania na tej podstawie przesłanek deliktu wskazać w tym miejscu należy, że aby doszło do powstania odpowiedzialności konieczne jest:

1. poniesienie przez osobę, której dane dotyczą, szkody majątkowej lub niemajątkowej;
2. naruszenie przez administratora lub podmiot przetwarzający przepisów RODO;
3. zaistnienie związku przyczynowego między naruszeniem a szkodą;
4. wina po stronie administratora lub podmiotu przetwarzającego.

Podmiot przetwarzający odpowiada zatem za szkody spowodowane przetwarzaniem naruszającym przepisy, gdy:

1. nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające, czyli art. 28 ust. 2 RODO, który stanowi, że podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora oraz art. 30 ust. 2 RODO, który stanowi, że każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania danych;
2. działał poza zgodnymi z prawem instrukcjami administratora;
3. działał wbrew zgodnym z prawem instrukcjom administratora.

Zgodnie z przedstawionymi wyżej punktami podmiot przetwarzający chcąc uniknąć odpowiedzialności powinien wykazywać, że:

- działał stosownie do zgodnych z prawem poleceń administratora,
- nie doszło do naruszenia obowiązków nakładanych bezpośrednio na podmiot przetwarzający,

Podkreślenia wymaga, że zakres odpowiedzialności podmiotu przetwarzającego, wynikający z art. 82 RODO jest węższy niż administratora, ponieważ obejmuje tylko szkody wynikające z niedopełnienia przez niego zobowiązań wynikających z przepisów RODO lub naruszenia postanowień umowy powierzenia danych łączących go z administratorem.

W relacji zewnętrznej, tj. wobec podmiotu danych odpowiedzialność deliktowa podmiotu przetwarzającego kształtuje się w tożsamy sposób, z tym zastrzeżeniem, że zgodnie z art. 82 ust. 4 administrator i podmiot przetwarzający odpowiadają za szkodę spowodowaną

[580] W. Lamik, *Środki cywilnoprawne...*, s. 220.

przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania, o czym będzie mowa w dalszej części pracy.

Odpowiedzialność kontraktowa podmiotu przetwarzającego

Niezależnie od odpowiedzialności deliktowej podmiot przetwarzający może ponosić odpowiedzialność kontraktową. Tego rodzaju odpowiedzialności nie przewiduje RODO, stąd jej zastosowanie będzie możliwe na podstawie przepisów prawa krajowego. Zgodnie z art. 471 k.c., dłużnik zobowiązany jest do naprawienia szkody, jaką wyrządził wierzycielowi poprzez nieprawidłowe wykonanie zobowiązania, chyba że nastąpiło to w wyniku okoliczności, za które nie odpowiada. Gdy ani czynność prawna, ani przepis szczególny nie stanowią inaczej, okoliczności te – zgodnie z art. 472 k.c. – sprowadzają się do winy dłużnika (ściślej mówiąc zawinionego zachowania dłużnika), a gdy dłużnik nie spełnia zobowiązania osobiście, lecz posługuje się osobami trzecimi albo też powierza im wykonanie stosunku obligacyjnego – także do winy jego pomocników (art. 474 k.c.).

Dłużnik odpowiada – na podstawie art. 474 k.c. – za działania i zaniechania swych pomocników bez względu na to, czy podlegają jego kierownictwu, czy też zachowują swobodę działania. Nie jest także istotne, czy wspomniane osoby uzyskują z tytułu pomocy w wykonaniu zobowiązania jakąś korzyść, czy działają nieodpłatnie. Artykuł 474 k.c. nie dotyczy natomiast tych, którzy spełniają świadczenie bez zgody dłużnika (oczywiście, o ile wierzyciel takie świadczenie przyjmie). Ponadto, na gruncie odpowiedzialności kontraktowej regułę stanowi prawo żądania przez wierzyciela pełnego odszkodowania, wyznaczanego w zasadzie przez wartość szkody (*damnum emergens i lucrum cessans* – art. 361 § 2 k.c.), ta zaś powinna być z kolei normalnym następstwem niewykonania lub nienależytego wykonania stosunku obligacyjnego (adekwatny związek przyczynowy) Przedstawione powyżej zasady odpowiedzialności odszkodowawczej z art. 471 k.c. są podstawowym modelem odpowiedzialności kontraktowej, tworzonym z mocy samego prawa w braku przepisu szczególnego, który wprowadzałby odstępstwa, a także wobec milczenia stron w tej materii.

Na gruncie RODO do powstania odpowiedzialności kontraktowej może dojść w sytuacji naruszenia postanowienia łączącej strony umowy powierzenia przetwarzania danych, co wyłącza z kręgu osób, których ta odpowiedzialność dotyczy podmiot danych. Przesłankami tego rodzaju odpowiedzialności są: niewykonanie lub nieprawidłowe wykonania zobowiązania, powstanie szkody i związek przyczynowy pomiędzy niewykonaniem lub nieprawidłowym wykonaniem zobowiązania a wystąpieniem szkody. Zgodnie z poczynionymi wcześniej

rozważaniami niewykonanie lub nieprawidłowe wykonanie zobowiązania zależne będzie od zakresu obowiązków stron umowy powierzenia przetwarzania danych. Zakres tych obowiązków wyznacza określenie celu i charakteru przetwarzania oraz rodzaju danych osobowych, co sprowadzać się powinno do doprecyzowania, jakie kategorie danych i po co zostały powierzone do przetwarzania, a także w jaki sposób mają być przetwarzane. Podkreślenia w tym miejscu wymaga, że prawodawca unijny umieścił te same obowiązki w odrębnych przepisach – tj. zarówno w art. 28 ust. 3 RODO określającym obligatoryjne elementy umowy powierzenia zawieranej z administratorem oraz w innych przepisach określających wprost obowiązki procesora. W związku z tym, uzasadniona wydaje się argumentacja, że w zakresie obowiązków wymienionych w art. 28 ust. 3 RODO (które jednocześnie nie zostały powtórzone w przepisach odrębnych), procesor będzie ponosił wyłącznie odpowiedzialność umowną (naruszenie umowy w tym zakresie nie będzie bowiem zawsze prowadziło do naruszenia przepisów RODO). Źródłem tych obowiązków jest bowiem umowa powierzenia. Przykładowo naruszenie obowiązku pomocy administratorowi w wywiązywaniu się z praw podmiotów danych określonego w art. 28 ust. 3 f RODO, nie musi prowadzić do naruszenia obowiązku realizacji praw podmiotów danych przez administratora, jeżeli będzie on w stanie zrealizować je bez pomocy procesora[581].

Modyfikacje umowne odpowiedzialności kontraktowej

Jak już wspomniano, przepisy szczególne lub klauzule umowne mogą wprowadzać do reguł wyznaczanych przez model podstawowy odpowiedzialności kontraktowej różnego rodzaju odstępstwa, i to nie tylko co do okoliczności, za jakie odpowiada dłużnik, lecz również co do rodzaju szkód kontraktowych podlegających naprawieniu, a także wysokości odszkodowania, co będzie stanowiło przedmiot poniższych rozważań.

Biorąc pod uwagę zakres i wagę obowiązków, które winny zostać zawarte w umowie powierzenia przetwarzania danych nie budzi w praktyce wątpliwości fakt stosowania przez strony mechanizmów egzekucji wzajemnych praw w postaci np. kar umownych. Bezsporne jest, że w zakresie nieuregulowanym w art. 28 RODO strony umowy powierzenia przetwarzania danych wiąże swoboda kontraktowania. Z art. 472 Kodeksu cywilnego, wynika, że strony (zgodnie z zasadą swobody umów) mogą w umowie zmienić zakres odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązania. Jeżeli bowiem

[581] M. Gumularz, P.Kozik, *Odpowiedzialność administracyjna...*

z przepisu ustawy lub odpowiedniego postanowienia umownego nie wynika nic innego, dłużnik odpowiedzialny jest za niezachowanie należytej staranności.

Artykuł 472 k.c. dopuszcza modyfikację umowną i strony mogą wprowadzić do umowy odpowiedzialność opartą na zasadzie winy umyślnej albo tylko za rażące niedbalstwo i winę umyślną, co pozwala, by odpowiedzialność odszkodowawcza była w pewnych przypadkach całkowicie wyłączona. Odpowiedzialność wyłącznie za szkodę wyrządzoną umyślnie wyłącza odpowiedzialność dłużnika za rażące niedbalstwo. Zmniejszenie odpowiedzialności dłużnika ma jednak swoją granicę, którą jest art. 473 § 2 Kodeksu cywilnego. Przepis ten stanowi, że nieważne jest zastrzeżenie wyłączające odpowiedzialność za szkodę wyrządzoną umyślnie. Swoboda kontraktowania nie oznacza zatem zupełnej dowolności w kształtowaniu regulacji umownych

Próby ustalenia, jak kształtują się w zakresie granice swobody umów, nasuwają pytania, czy dopuszczalne jest, aby strony – w stosunkach między sobą – zmieniły charakter związku przyczynowego jako przesłanki odpowiedzialności z art. 471 k.c., w szczególności zaś uzgodniły, że dłużnik będzie odpowiadał także za takie szkody, które nie stanowią normalnego następstwa nieprawidłowego wykonania zobowiązania (odejście od teorii adekwatnego związku przyczynowego). Klauzule umowne mogą wprowadzać do reguł wyznaczanych przez model podstawowy różnego rodzaju odstępstwa, i to nie tylko co do okoliczności, za jakie odpowiada dłużnik. Z art. 361 § 2 k.c. wynika, że strony zobowiązania mają do tego prawo . Jeżeli więc strony w umowie nie zawrą innego postanowienia, wówczas naprawienie szkody będzie obejmowało straty oraz utracone korzyści - jest to zasada pełnego odszkodowania. Jeśli zaś w umowie strony zmodyfikują zakres uszczerbku podlegającego naprawieniu (np. poprzez ograniczenie odpowiedzialności do poniesionych strat, wyłączając utracone korzyści) oraz metodę obliczenia wartości uszczerbku (ograniczenie kwoty, do której odpowiada dłużnik), naprawienie szkody będzie obejmowało jedynie to, co w umowie postanowiono. Odpowiedzialność odszkodowawcza dłużnika, a raczej jej ograniczenie może wynikać z samej ustawy, np. art. 362 k.c. stanowi, że jeśli poszkodowany przyczynił się do powstania lub zwiększenia szkody, odpowiedzialność dłużnika będzie mniejsza. To zagadnienie było przedmiotem rozważań w niniejszej pracy w zakresie dotyczącym obsługi naruszenia ochrony danych osobowych.

Rozważając zagadnienie dopuszczalnych prawnie modyfikacji umownych, nie sposób pominąć instytucji klauzule indemnifikacyjne, które w polskiej literaturze, określa się je jako zastrzeżenia umowne, mocą których jedna ze stron zobowiązuje się zabezpieczyć, chronić i zwolnić w razie konieczności drugą stronę z poniesienia wskazanych w klauzuli strat, którymi

zazwyczaj są wszelkiego rodzaju zobowiązania, koszty czy odszkodowania[582]. W tym miejscu wskazać należy na częste praktyki rynkowe, proponujące w umowach powierzenia przetwarzania danych modyfikacje zasad odpowiedzialności RODO. Ich skutkiem ma być zgodnie z intencją strony proponującej takie rozwiązania zwolnienie z odpowiedzialności w przypadku zaistnienia umówionych okoliczności, w których szkoda powstała lub przeniesienie kary administracyjnej na kontrahenta umowy.

Problematyczne w takich przypadkach jest to, że różnorodność obowiązków stron umowy powierzenia niejednokrotnie wyklucza precyzyjne wyznaczenie zakresu odpowiedzialności względem różnego rodzaju zdarzeń, których wystąpienie zabezpieczać mają modyfikacje umowne. W zakresie zabezpieczeń ryzyka związanego z nałożeniem kary administracyjnej wątpliwości, co do skuteczności takich postanowień wynikają z tego, że podstawą przeniesienia kary jest np. stwierdzenie naruszenia postanowień umowy powierzenia przetwarzania danych bez jednoczesnego określenia o jakie naruszenie chodzi oraz w jakich warunkach ono powstaje.

Problemy interpretacyjne co do rzeczywistej intencji stron umowy może generować zatem postanowienie umowne, że w każdym przypadku nałożenia kary administracyjnej podmiot przetwarzający będzie zobowiązany do jej uiszczenia. Jest to kłopotliwe o tyle, że taka sytuacja może mieć miejsce także w przypadku, gdy naruszenie powstało w warunkach zależności od działań kontrahenta, na które przetwarzający nie miał wpływu. Podobnie problemów interpretacyjnych mogą dostarczyć modyfikacje umowne dotyczące wyłączenia odpowiedzialności podmiotu przetwarzającego za realizację wszelkich poleceń administratora, obowiązek informowania o roszczeniach i postępowaniach oraz obowiązek współdziałania w obronie przed roszczeniami.

W przypadku klauzul takich jak omawiane powyżej trzeba mieć na względzie, że rdzeniem toczącej się w polskim piśmiennictwie dyskusji jest związanie podstaw konstrukcji klauzul indemnifikacyjnych albo z dyspozycją przepisu art. 391 k.c. , albo z art. 392 k.c., co nawiązuje do spornej kwestii — tj. ustalenia tego, co jest istotą świadczenia wynikającego z umów gwarancyjnych. Część autorów opowiada się za koncepcją, w myśl której pierwotnym obowiązkiem gwaranta jest powstrzymanie wierzyciela przed dochodzeniem określonego świadczenia od dłużnika; inni z kolei opowiadają się za pierwotnym charakterem odszkodowawczego zobowiązania gwaranta, uznając je za podstawowy model umowy

[582] A.M. Juranek, *Klauzule indemnifikacyjne jako szczególny mechanizm modyfikacji odpowiedzialności kontraktowej przez alokację ryzyka a kwestia akcesoryjnych zastrzeżeń umownych zabezpieczających ich wykonanie*, „Transformacje prawa prywatnego" 2020/4.

gwarancyjnej w prawie polskim, a więc również właściwy względem klauzuli indemnifikacyjnej.

Strony mogą oczywiście inaczej ukształtować treść zobowiązania indemnifikacyjnego w umowie, w szczególności przez przyjęcie, że dłużnik będzie zobowiązany do podejmowania wszystkich działań mających ochronić wierzyciela przed szkodą, zastrzegając w razie nieosiągnięcia tego celu jego odpowiedzialność na zasadach ogólnych (art. 471 k.c.), albo też tak, że na dłużniku spoczywał będzie nie tylko obowiązek podejmowania działań ochronnych wobec ryzyka poniesienia szkody przez wierzyciela, ale że jego odpowiedzialność zostanie rozszerzona także na zagwarantowanie niewystąpienia szkody w ogóle. Zagadnienia te będą musiały zostać poddane ocenie w kontekście warunków, w jakich omawiane klauzule mają na celu ujęcie całkowicie innego rozkład ciężaru odpowiedzialności, aniżeli wynikałoby to z przepisów prawa, co dokonywane jest poprzez określenie która ze stron stosunku obligacyjnego poniesie ciężar ekonomiczny wystąpienia określonego zdarzenia.

Realizacja obowiązków podmiotu przetwarzającego w orzecznictwie

Zagadnienie realizacji obowiązków ciążących na administratorze danych w związku z powierzeniem przetwarzania danych osobowych był przedmiotem rozstrzygnięcia organu nadzoru w decyzji z 17.12.2020 r.[583]. W decyzji tej Prezes UODO poświęcił uwagę ocenie współpracy między KSSIP a podmiotem przetwarzającym odnosząc się do zasad i zakresu współpracy i odpowiedzialności stron umowy powierzenia. Podnoszona w decyzji argumentacja, pomimo jej skutku, jakim była administracyjna kara pieniężna, wskazuje na kierunek interpelacji przez organ nadzoru obowiązków stron umowy, co może mieć w przyszłości znaczenie dla przesłanek odpowiedzialności cywilnej, dlatego wymaga z uwagi na temat pracy jej szczegółowego omówienia.

W analizowanym rozstrzygnięciu Prezes UODO uznał, że administrator – KSSIP nie zapewnił bezpieczeństwa danych (poprzez niezastosowanie odpowiednich środków technicznych i organizacyjnych służących poufności przetwarzania, brak testowania i oceny skuteczności tych środków oraz niewłaściwe uwzględnienie ryzyka związanego ze zmianami w procesie przetwarzania danych), co było spowodowane niezgodnością z przepisami RODO zawartej umowy powierzenia oraz zakresem odpowiedzialności stron tej umowy. Zagadnieniem, wpływającym na obowiązki stron umowy, na jakie zwrócił uwagę Prezes UODO, jest język komunikacji między stronami umowy powierzenia. Administrator

[583] Decyzja prezesa UODO z 17.12.2020 r. znak DKN.5130.1354.2020.

posługiwał się określoną nomenklaturą i oznaczeniami (np. baza danych „stara" platforma szkoleniowa, platforma e-learning, baza szkoleniowa), która dla dostawcy usług hostingowych, z uwagi na charakter świadczonej usługi, w opinii procesora, była nieprawidłowa i niezrozumiała. Rodziło to problemy interpretacyjne i oznaczało oczekiwanie administratora do wykonywania przez podmiot przetwarzający czynności poza określone w umowie. Przepisy RODO, jak wskazano w komentowanej decyzji, dają pewną swobodę w zakresie kształtowania relacji między administratorem a podmiotem przetwarzającym.

Należy więc oczekiwać, że administrator wypracuje model współpracy z podmiotem przetwarzającym, który będzie zapewniał przetwarzanie zgodne z przepisami o ochronie danych osobowych, a w szczególności będzie umożliwiał realizację zasady rozliczalności wyrażoną w art. 5 ust. 2 RODO. O ile zatem strony umowy ustaliły kanały komunikacji oraz wyznaczyły osoby wykonujące czynności związane z realizacją umowy, o tyle osoby wskazane przez KSSiP nadal nie miały świadomości, jak kształtują się prawa i obowiązki pomiędzy administratorem a podmiotem przetwarzającym.

Uprawniona jest konstatacja, że osoby wyznaczone do kontaktu z podmiotem przetwarzającym powinny zostać uprzednio poinformowane o zakresie usług świadczonych przez podmiot przetwarzający i o obowiązkach leżących po stronie administratora. Treść porozumienia natomiast nie powinna budzić wątpliwości, a zatem strony powinny używać i posługiwać się pojęciami zrozumiałymi dla obu stron, co może skutecznie minimalizować ryzyko naruszenia ochrony danych osobowych Brak współpracy na poziomie poprawnej komunikacji, błędne polecenia wydawane podmiotowi przetwarzającemu, fałszywa ocena ról, zadań i zakresu obowiązków określonych w umowie powierzenia prowadziły w tej sprawie w konsekwencji do braku właściwej, odpowiedzialnej weryfikacji tego, czy zlecona czynność została wykonana, i czy została wykonana prawidłowo[584].

Prezes UODO stwierdził w tej decyzji także, że relacja z podmiotem przetwarzającym nie oznacza obowiązku ciągłego monitorowania stosowanych rozwiązań. Jednakże, zdaniem PUODO istotne jest, by administrator w ramach realizacji obowiązków wynikających z rozporządzenia 2016/679 dokonywał cyklicznej weryfikacji, czy w używanych rozwiązaniach technicznych i organizacyjnych nie stwierdzono słabości mogących wpłynąć na ryzyko naruszenia praw lub wolności osób, których dane dotyczą, a fakt przetwarzania danych przez

[584] E. Bielak-Jomaa, *Realizacja obowiązków administratora danych w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialność podmiotu przetwarzającego oraz model współpracy między tymi podmiotami Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 11 .02. 2021 r., DKN.5130.2024.2020* [w:] „Gdańskie Studia Prawnicze" 2021/4(52), Rok XXV, s. 175–188.

podmiot przetwarzający tej odpowiedzialności z administratora nie zdejmuje. Z uwagi na zaskarżenie decyzji stanowisko stron w tej sprawie podlegało dalszej argumentacji, w toku której administrator podawał, że nie jest prawidłowe zapatrywanie organu, że powierzenie przez nią czynności przetwarzania danych osobowych wyspecjalizowanym firmom, nie miało żadnego wpływu na odpowiedzialność skarżącej za naruszenie i powtórzył, że ewentualna odpowiedzialność skarżącej powinna być rozpatrywana w kontekście art. 28 ust. 1 rozporządzenia. W konsekwencji powyższego podnosił, że odpowiedzi na pytanie, czy gwarancje udzielone Spółce jako administratorowi danych przez podmioty przetwarzające były wystarczające, aby uzasadnić skorzystanie przez nią z ich usług. Skarżąca podała, że zapewniła odpowiedni stopień bezpieczeństwa danych klientów (uwzględniając przy tym ryzyko naruszenia praw lub wolności osób fizycznych) właśnie poprzez powierzenie czynności przetwarzania danych osobowych, mających czysto techniczny charakter (tj. przechowywanie danych na serwerach) firmom wyspecjalizowanym w tym zakresie.

W ocenie organu korzystanie w procesie przetwarzania danych osobowych ze wsparcia ze strony profesjonalnego podmiotu przetwarzającego, określane „transferem ryzyka", nie implikuje wcale stanu „przeniesienia odpowiedzialności" z administratora na podmiot przetwarzający w zakresie obowiązków ciążących na nim na mocy przepisów RODO, a odnosi się do stanu ich kooperacji określonej na gruncie art. 28 ust. 3 lit. c) RODO i ponoszonej na zasadzie wzajemnej odpowiedzialności za bezpieczeństwo procesów przetwarzania danych osobowych.

W świetle art. 32 ust. 1 RODO odpowiedzialność administratora za zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez powierzenie ich przetwarzania podmiotowi przetwarzającemu nie zostaje wyłączona. Przyjęcie odmiennej interpretacji przepisu prowadziłoby do błędnego wniosku, że w momencie zawarcia umowy powierzenia danych osobowych, administrator staje się de facto wyłączony spod przepisów RODO zobowiązujących go do zapewnienia bezpieczeństwa przetwarzanych danych. Zdaniem organu nadzoru fakt przetwarzania danych osobowych przez podmiot przetwarzający na podstawie umowy powierzenia przetwarzania danych osobowych nie zdejmuje z administratora odpowiedzialności za wdrożenie odpowiednich środków technicznych i organizacyjnych, odpowiadających ryzyku zaistnienia naruszenia praw lub wolności osób fizycznych. Innymi słowy, na gruncie tego przepisu zobowiązania administratora i podmiotu przetwarzającego do zapewniania bezpieczeństwa przetwarzania danych osobowych pozostają od siebie niezależne, a ich wykonanie przez wskazane podmioty nie ma charakteru alternatywnego, co w konsekwencji prowadzić musi do konstatacji, iż nie zachodzi wyłączenie odpowiedzialności

administratora za zapewnienie bezpieczeństwa przetwarzania danych osobowych poprzez powierzenie ich przetwarzania podmiotowi przetwarzającemu.

Według rozpoznającego omawianą powyżej sprawę Sądu WSA w Warszawie rozważenie zasadniczej w tej sprawie kwestii ewentualnego rozłożenia ciężaru odpowiedzialności podmiotów biorących udział w procesie przetwarzania danych osobowych (administratora danych i podmiotu przetwarzającego) wymagało jednak ustalenia zakresu przypisanych każdemu z nich, określonych w rozporządzeniu obowiązków związanych z przetwarzaniem. Zdaniem Sądu było oczywiste, że gdy administrator danych przetwarzając dane osobowe nie korzysta z usług innego podmiotu - podmiotu przetwarzającego, na nim spoczywa pełna odpowiedzialność za przestrzeganie przepisów mających zapewniać bezpieczeństwo tych danych. Inaczej wygląda sytuacja, jeżeli w procesie przetwarzania danych biorą udział dwa podmioty: administrator i podmiot przetwarzający.

Podmiot przetwarzający, to w rozumieniu art. 4 pkt 8 RODO osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Administrator może więc posłużyć się zastępcą, który wykonuje za niego, w jego imieniu czynności przetwarzania. Zastępca (reprezentant) administratora jest odrębnym podmiotem prawa, działającym za reprezentowanego, na podstawie umocowania udzielonego w zawartej z administratorem umowie o powierzeniu przetwarzania. Jeżeli czynności przetwarzania wykonuje podmiot przetwarzający, a nie administrator, to co do zasady do działania tego zastępcy należałoby odnosić przepisy określające obowiązki związane z przetwarzaniem. RODO rozkłada jednakże te obowiązki pomiędzy administratora i podmiot przetwarzający, co oznacza, że administrator powierzając przetwarzanie danych innemu podmiotowi nie jest zwolniony całkowicie z odpowiedzialności za niedopełnienie prawnych wymagań dotyczących przetwarzania.

Przepisy rozporządzenia kierują niektóre obowiązki do administratora danych (art. 5 ust. 2), inne zaś są adresowane jednocześnie do administratora i do podmiotu przetwarzającego (art. 32 ust. 1 i 2). Ponadto podmiot przetwarzający ma odrębne obowiązki w tym zakresie (art. 28 rozporządzenia). Co prawda te obowiązki podmiotu przetwarzającego powinny być umieszczone w zawartej między stronami umowie o przetwarzanie danych. Niemniej jednak obligatoryjne dla stron wprowadzenie ich do umowy nie odbiera im charakteru publicznoprawnego, nie czyni obowiązkami wyłącznie obligacyjnymi, co ma oczywiście zasadnicze znaczenie dla określenia odpowiedzialności za ich naruszenie i co znajduje potwierdzenie w art. 83 ust. 4 lit. a rozporządzenia. Podmiot przetwarzający jest obowiązany do współdziałania z administratorem, a nawet do udzielania mu pomocy w wywiązywaniu się

z jego obowiązków określonych w art. 32–36 (art. 28 rozporządzenia). Nałożenie zarówno na administratora, jak i na podmiot przetwarzający dość ogólnego obowiązku zapewnienia bezpieczeństwa danych (art. 32 ust. 1) nie implikuje konieczności podejmowania przez te podmioty działań tego samego rodzaju i nie rodzi po ich stronie odpowiedzialności za naruszenia, niezależnie od tego, któremu z nich można je przypisać. Nie ma tu mowy o jakimkolwiek solidarnym, w rozumieniu prawnym wykonywaniu przez strony obowiązków dotyczących zapewnienia bezpieczeństwa przetwarzania danych i solidarnej odpowiedzialności za naruszenie tych obowiązków.

W omawianej sprawie zdaniem Wojewódzkiego Sądu Administracyjnego w Warszawie punktem odniesienia dla konkretyzacji obowiązków kierowanych do administratora i do podmiotu przetwarzającego (np. art. 32 ust. 1) są ich prawnie wyznaczone funkcje. Według rozporządzenia funkcją administratora danych jest samodzielne lub wspólnie z innymi ustalanie celów i sposobów przetwarzania danych osobowych (art. 4 pkt 7 rozporządzenia). Do podmiotu przetwarzającego należy natomiast przetwarzanie danych osobowych w imieniu administratora (art. 4 pkt 8). Prowadzi to do wniosku, że na każdym z tych podmiotów ciążą obowiązki dotyczące zakresu ich indywidualnego uczestnictwa w procesie przetwarzania danych. Ta teza znajduje potwierdzenie w piśmiennictwie. W komentarzu do art. 5 ust. 2 rozporządzenia formułującego ogólną zasadę odpowiedzialności administratora danych za przestrzeganie przepisów rozporządzenia dotyczących przetwarzania danych osobowych wyrażono pogląd, że w przypadku powierzenia przetwarzania danych osobowych, obowiązki wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia odpowiedniego stopnia bezpieczeństwa odpowiadającego ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia spoczywają na podmiocie przetwarzającym[585].

Przedstawione rozważania uzasadniają stwierdzenie, że w przypadku powierzenia przetwarzania danych podmiotowi przetwarzającemu egzekwowanie odpowiedzialności za naruszenia powstałe w procesie przetwarzania nie może nie brać pod uwagę obowiązków obu podmiotów uczestniczących w przetwarzaniu i nie uwzględniać ich indywidualnego przyczynienia się do powstania naruszenia. Świadczą o tym również określone w rozporządzeniu zasady nakładania administracyjnych kar pieniężnych za naruszenie przepisów rozporządzenia (art. 83). Tej odpowiedzialności administracyjnej podlegają administrator danych i podmiot przetwarzający. Jedna z dyrektyw nakładania tych kar stanowi, że podjęcie

[585] *Ogólne rozporządzenie o ochronie danych osobowych Ustawa o ochronie danych osobowych Wybrane przepisy sektorowe. Komentarz,* red. P. Litwiński, Warszawa 2021, s. 164.

decyzji o nałożeniu kary i ustaleniu jej wysokości wymaga zwrócenia uwagi w każdym indywidualnym przypadku na stopień odpowiedzialności administratora lub podmiotu przetwarzającego, z uwzględnieniem środków technicznych organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 (art. 83 ust. 2 lit. d).

W sprawie tej Sąd uznał, że administrator danych, nie posiadając organizacyjnych czy technicznych możliwości prawidłowego, zgodnego z wymogami prawnymi przetwarzania danych, powierzył te czynności innemu podmiotowi, wyspecjalizowanemu w tej materii. Niejako wyręczył się w tym zakresie podmiotem przetwarzającym. Dokonując prawidłowego (niezakwestionowanego przez organ nadzoru) wyboru tego podmiotu, mógł mieć więc zaufanie do jego działania, wsparte znajomością ciążących na nim obowiązków określonych omawianym rozporządzeniem oraz wynikających z umowy o powierzenie przetwarzania danych. Mocą tej umowy podmiot przetwarzający zobowiązał się wobec administratora danych m.in. do stosowania odpowiednich technicznych, fizycznych oraz organizacyjnych środków bezpieczeństwa w celu ochrony powierzonych danych, sprawowania nadzoru nad bezpieczeństwem danych przez cały okres ich powierzenia i wreszcie do zgłaszania administratorowi bez zbędnej zwłoki faktycznego lub podejrzanego naruszenia ochrony danych.

Dokonanie prawidłowego wyboru podmiotu przetwarzającego dane nie zwalnia administratora całkowicie z obowiązków związanych z przetwarzaniem danych i z odpowiedzialności za ich naruszenie. Nie pozwala jednak na egzekwowanie od administratora całej odpowiedzialności za naruszenie przepisów prawa prowadzących do naruszenia ochrony danych osobowych, powstałego z przyczyn leżących po stronie podmiotu przetwarzającego. Zgadzając się z organem, że administrator nie wykazał się znaczącą aktywnością w działaniach zmierzających do zweryfikowania informacji o prawdopodobnym naruszeniu ochrony danych osobowych, trzeba zauważyć, że w okolicznościach faktycznych sprawy jego możliwości działania były ograniczone, poza wywieraniem nacisku na podmiot przetwarzający. Nie wydaje się bowiem, aby administrator miał techniczne czy organizacyjne możliwości, pozwalające mu na własną rękę skontrolować funkcjonowanie zabezpieczeń serwera, z którego wyciekły dane.

W innej części wyroku Sąd odnosi się do zakresu odpowiedzialności administratora na zasadzie winy w wyborze, wskazując, że według niego w tej sprawie naruszenie ochrony danych nastąpiło z przyczyn leżących po stronie podmiotu przetwarzającego. Naruszeniem w rozumieniu art. 4 pkt 12 rozporządzenia jest bowiem stworzenie nieuprawionego dostępu do danych, a to nastąpiło wskutek błędu pracownika podmiotu przetwarzającego. Organ w żaden sposób nie wykazał, że istnieje związek przyczynowo - skutkowy pomiędzy tym błędem, a

zarzucanym administratorowi naruszeniem obowiązków wskazanych w decyzji o nałożeniu kary administracyjnej, które według tego, co już powiedziano należy interpretować zgodne z funkcją administratora jako podmiotu ustalającego cele i sposoby przetwarzania danych. Rozumowanie organu sprowadza się do przyporządkowania (subsumcji) ustalonego stanu faktycznego, ograniczonego do działania administratora pod określone przepisy rozporządzenia, regulujące obowiązki związane z przetwarzaniem danych osobowych, z pominięciem faktu, że te przepisy odnoszą się nie tylko do administratora danych i że ze stanu faktycznego wynika oczywisty udział podmiotu przetwarzającego w powstaniu naruszenia ochrony danych osobowych. Zdaniem Sądu przypisana administratorowi opieszałość w stwierdzeniu naruszenia ochrony danych mogła się ewentualnie przyczynić do powstania szkody w wyniku powstałego naruszenia, a nie do powstania samego naruszenia.[586]

Pomimo faktu, że omawiana sprawa była rozpoznawana pod kątem wyłącznie odpowiedzialności administracyjnej zagadnienia w niej poruszane wykraczają swoją problematyką poza tą materię. Świadczy o tym m.in. glosa E. Bielak-Jomaa, w której Autorka twierdzi, że trudno podzielać opinię organu nadzoru, że procesor, który zarządzał zasobami serwerowymi, nie ponosi żadnej winy, a więc także odpowiedzialności za wyciek danych. W przedstawionej sprawie działania podmiotu przetwarzającego określić można jako bierne zachowanie. Wykonywał on działania ograniczone do poleceń administratora, odmawiając wykonania polecenia lub żądając jego doprecyzowania, w sytuacji gdy były one niejasne albo nieprecyzyjne. W jej ocenie, takie zaangażowanie podmiotu przetwarzającego, w tej konkretnie sprawie, nie spełniało obowiązku udzielania pomocy, o którego zobowiązany jest podmiot przetwarzający na mocy art. 28 ust. 3 lit. f RODO[587]. Stan faktyczny tej sprawy i poruszone przez Sąd zagadnienia prowadzą do refleksji, że poza odpowiedzialnością administracyjną w sprawie tej rozważać odpowiedzialność cywilną i administratora i podmiotu przetwarzającego.

Ocena relacji podmiot przetwarzający – administrator także przed wejściem w życie RODO stanowiła przedmiot kontroli sądowej. Dla przykładu w wyroku Sądu Najwyższego[588] zawarte zostało stwierdzenie, że nie po to w szczególnej ustawie, jaką jest ustawa z 29.08.1997 r. o ochronie danych osobowych przewidziane zostały drobiazgowe regulacje, mające gwarantować kontrahentom firm telekomunikacyjnym ochronę ich danych, żeby można uwolnić się od odpowiedzialności cywilnej przez zastosowanie ogólnego przepisu, jakim jest art. 429 k.c. Z tego wynika, że administrator danych osobowych, będący firmą

[586] Wyrok WSA w Warszawie z 5.10.2021, sygn. akt II SA/Wa 528/21.
[587] E. Bielak-Jomaa, *Realizacja obowiązków...*, s. 175–188.
[588] Wyrok SN – Izba Cywilna z 01.06.2017, sygn. akt I CSK 597/16.

telekomunikacyjną odpowiada na podstawie art. 415 k.c. za własną winę wobec klienta - strony umowy o świadczenie usług telekomunikacyjnych, jeżeli nadużył zaufania tego klienta, powierzając bez jego zgody i wiedzy wykonywanie części umówionych usług osobie trzeciej - profesjonalnej firmie, która dopuściła do przetworzenia przez nieupoważnione osoby danych strony umowy i umieszczenia ich w ogólnie dostępnym portalu internetowym, przez co naruszone zostały jej dobra osobiste (art. 23 k.c.). Przedsiębiorca telekomunikacyjny będący administratorem danych osobowych odpowiada za szkodę wyrządzoną klientowi – stronie umowy o świadczenie usług telekomunikacyjnych, jeżeli w sposób zawiniony nadużył jego zaufania, powierzając bez jego zgody i wiedzy wykonywanie części umówionych usług innemu przedsiębiorcy (art. 415 k.c). Przepis art. 429 k.c. nie ma w takiej sytuacji zastosowania[589].
Administrator danych osobowych będący firmą telekomunikacyjną odpowiada na podstawie art. 415 k.c. za własną winę wobec klienta – strony umowy o świadczenie usług telekomunikacyjnych, jeżeli nadużył zaufania tego klienta, powierzając bez jego zgody i wiedzy wykonywanie części umówionych usług osobie trzeciej - profesjonalnej firmie, która dopuściła do przetworzenia przez nieupoważnione osoby danych strony umowy i umieszczenia ich w ogólnie dostępnym portalu internetowym, przez co naruszone zostały jej dobra osobiste (art. 23 k.c.); w tym zakresie nie ma zastosowania wyłączenie odpowiedzialności administratora na podstawie art. 429 k.c.[590].

Dalsze podmioty przetwarzające

Ze względu na to, że w praktyce często występują sytuacje dalszego powierzenia przetwarzania danych rodzi to pytanie o relacje podmiotów przetwarzających i dalszych podmiotów przetwarzających. Udział w procesie przetwarzania danych osobowych podmiotu określanego często jako „subprocesor" lub „dalszy przetwarzający" czy „podprocesor" wynika z tego, że usługobiorcy przy realizacji zleceń lub usług korzystają z podwykonawców, powierzając im w jakimś zakresie przetwarzanie danych osobowych, które uprzednio administrator powierzył do przetwarzania podmiotowi przetwarzającemu. Subprocesor to tzw. inny podmiot przetwarzający, a więc w praktyce podwykonawca wykonawcy (podmiotu przetwarzającego), który przy wykonywaniu usługi przetwarza dane osobowe w imieniu i na rzecz administratora.

W praktyce w tej samej relacji powierzenia po stronie podmiotów przetwarzających faktycznie może wystąpić więcej niż jeden podmiot – pierwotny wykonawca (podmiot

[589] Biuletyn SN 2017/9; OSNC zb.dod. 2017/D/73.
[590] OSP 2018/10/98.

przetwarzający) i jego podwykonawca (subprocesor), a nawet łańcuszek dalszych subprocesorów, a więc podwykonawcy podwykonawców. Subprocesor dokonuje przetwarzania danych w imieniu administratora, z tym zastrzeżeniem, że podstawą tego przetwarzania pozostaje stosunek prawny (umowa) łączący go z pierwotnym podmiotem przetwarzającym.

RODO w art. 28 wymaga, by w umowie powierzenia lub innym akcie (tzw. innym instrumencie prawnym), uregulować tzw. podpowierzenie przetwarzania danych, jeśli ma ono miejsce. Konstruowanie umowy powierzenia wymaga zatem, aby już na tym etapie dokonać pewnych rozstrzygnięć co do podwykonawstwa właśnie. Zgodnie z art. 28 ust. 2 RODO podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Dopuszczalność podpowierzenia jest zależna od woli pierwotnie powierzającego dane, dlatego kwestia zgody na podpowierzenie jest kluczowa - musi być ona uprzednia względem podpowierzenia. Zgoda może być zawarta bezpośrednio z umowie powierzenia albo stanowić odrębny dokument, a jeśli zgody nie wyrażono w umowie, umowa powinna określać zasady wystąpienia o zgodę i zasady zgłoszenia sprzeciwu. Umowa powinna precyzować, czym sprzeciw skutkuje w konkretnych okolicznościach.

Zasadniczym powodem potrzeby uregulowania zagadnień dotyczących podpowierzenia przetwarzania danych jest potrzeba jasnego określenia relacji zachodzących między podmiotem przetwarzającym a dalszym podmiotem przetwarzającymi. Zawarcie umowy z subprocesorem ma zapobiec obniżeniu poziomu ochrony wskutek faktycznego wykonywania czynności przetwarzania przez inne podmioty niż administrator i osoby mu bezpośrednio podległe oraz podmiot przetwarzający.

Podmiot, któremu dane zostały podpowierzone, powinien spełniać te same standardy ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym. Umowa lub innym instrument prawny wymaga uregulowania następujących kwestii:

1. przedmiotu i czasu trwania przetwarzania;
2. charakteru i celu przetwarzania;
3. rodzaju danych osobowych oraz kategorie osób, których dane dotyczą;
4. obowiązków i praw administratora.

Zasady odpowiedzialności dotyczące dalszych podmiotów przetwarzających

W relacjach dotyczących podpowierzenia RODO dokonuje modyfikacji zasad odpowiedzialności, do których przywykliśmy na gruncie regulacji wynikających z Kodeksu cywilnego. W myśl art. 28 ust. 4 RODO, jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3 RODO, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

Odpowiedzialność podmiotu przetwarzającego według tak skonstruowanych zasad nie kształtuje się na wzór art. 429 k.c. – tj. tak, że od odpowiedzialności podmiot przetwarzający zwalniałoby wykazanie braku winy w wyborze podmiotu dalszego przetwarzającego. Z tego powodu istotnym pozostaje, aby zabezpieczyć dalsze powierzenia przetwarzania danych osobowych także w sposób gwarantujący możliwość dochodzenia roszczeń regresowych, o których mowa w art. 82 RODO[591].

Artykuł 28 ust. 10 RODO przewiduje konsekwencje naruszenia przez podmiot przetwarzający przepisów rozporządzenia w zakresie określenia celów i sposobów przetwarzania danych. Podejmowanie decyzji o celach i sposobach przetwarzania danych jest znamienną cechą administratora danych i jego uprawnieniem. Jeżeli w tę sferę bezprawnie ingeruje podmiot przetwarzający, wchodząc w zakres zastrzeżony administratorowi, to komentowany przepis nakazuje uznać podmiot przetwarzający za administratora w odniesieniu do tego przetwarzania. Oznacza to, że podmiot przetwarzający odpowiada w tym zakresie za naruszenie przepisów komentowanego rozporządzenia tak jak administrator. W komentowanym przepisie stwierdzono, że taka konstrukcja pozostaje „bez uszczerbku dla art. 82, 83 i 84", co oznacza, że to podmiot przetwarzający może odpowiadać niezależnie od odpowiedzialności administratora w zakresie prawa osoby, której dane dotyczą, do

[591] M. Czaplińska *Naprawienie szkody z tytułu naruszenia RODO* [w:] *D. Dörre-Kolasa* (red.), Ochrona danych osobowych w zatrudnieniu, Warszawa 2020, s. 444-446

odszkodowania i odpowiedzialności odszkodowawczej (art. 82); odpowiedzialności w postaci administracyjnych kar pieniężnych (art. 83) oraz innych sankcji (np. karnych) za naruszenie obowiązków wynikających z rozporządzenia (art. 84).

Z punktu widzenia administratora podmiot przetwarzający realizuje czynności zlecone przez administratora po to, aby wesprzeć go w realizacji jego celów przetwarzania. Celem jego aktywności nie jest zatem, co do zasady, uzyskiwanie korzyści wynikającej bezpośrednio z przetwarzania danych osobowych (realizacja własnych celów przetwarzania), ale wykonanie usługi, za co może otrzymać wynagrodzenie[592]. Podmiot przetwarzający nie może zatem przetwarzać danych inaczej niż zgodnie z poleceniami administratora. Podmiot przetwarzający narusza RODO, jeśli wykracza poza polecenia administratora i zaczyna ustalać własne cele i sposoby przetwarzania. Procesor będzie wtedy uważany za administratora danych w odniesieniu do tego przetwarzania i może podlegać sankcjom za przekroczenie instrukcji administratora.

Role administratora i podmiotu przetwarzającego wydają się być precyzyjnie rozgraniczone. W rzeczywistości często dochodzi jednak do sytuacji, w których te role trudno jednoznacznie przypisać. Coraz częściej pojawiają się modele, w których rola poszczególnych podmiotów ma charakter hybrydowy. Stanowi to wyzwanie dla modelu, który został zbudowany wokół założenia podporządkowanej roli podmiotu przetwarzającego wobec celów przetwarzania ustalanych przez administratora. Dostrzegana jest coraz wyraźniejsza tendencja podmiotów przetwarzających do realizowania, przy okazji przetwarzania danych w imieniu administratora, własnych celów przetwarzania. Tendencję tę można wiązać z rozwojem nowoczesnych technologii, m.in. opartych na uczeniu maszynowym, które często bazują na danych w tym znaczeniu, że ich doskonalenie i rozwijanie wymaga dużej ilości danych. Podmiot przetwarzający ma często uprzywilejowany dostęp do dużych zbiorów danych które potencjalnie mógłby wykorzystać we własnych celach. Z reguły nie może tego jednak zrobić, ponieważ jest ograniczony rolą, jaką pełni w stosunku do tych danych. Rozporządzenie ogólnie nie wyklucza osiągania przez podmiot przetwarzający korzyści wynikających wprost z przetwarzania danych. Warunkiem osiągania tych korzyści jest jednak, aby były one bezpośrednim następstwem realizowania zadań dla administratora. Przetwarzanie danych przez podmiot przetwarzający musi się bowiem zawsze mieścić w przedmiotowych i czasowych ramach wyznaczonych przez administratora. Podmiot przetwarzający może zatem czerpać własne korzyści z przetwarzania danych w imieniu administratora, jednak nie może w celu ich

[592] S. Kowalski, *Zakres swobody podmiotu przetwarzającego przy przetwarzaniu danych osobowych*, MoP 2020/23.

osiągnięcia podejmować dodatkowych czynności przetwarzania danych, które są zbędne z perspektywy realizacji celów administratora, a służą jedynie lub przede wszystkim realizacji celów podmiotu przetwarzającego[593].

Roszczenie regresowe

Zgodnie z art. 82 ust. 4 RODO administrator i podmiot przetwarzający odpowiadają za całą szkodę wobec podmiotu danych, co stanowi modyfikację zasady regresu według Kodeksu cywilnego. Z instytucją odpowiedzialności solidarnej administratora lub podmiotu przetwarzającego ściśle związane jest roszczenie regresowe, o którym mowa w art. 82 ust. 5 RODO. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 art. 82 rozporządzenia ogólnego zapłacił odszkodowanie za wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2 RODO. Jednoznacznie z tego wynika że, jeżeli w efekcie postępowania sądowego przedsiębiorca został zobowiązany i uiścił odszkodowanie za całą wyrządzoną szkodę, a w przetwarzanie były zaangażowane także inne podmioty, to może on żądać od takich podmiotów zwrotu części wypłaconego odszkodowania, przy czym istotne jest zastrzeżenie, że przedmiotowe roszczenie regresowe będzie dotyczyło zwrotu części odszkodowania, za które ponoszą one odpowiedzialność w myśl art. 82 ust. 4 RODO.

W odniesieniu do tak sformułowanej normy art. 82 ust. 4 rozporządzenia ogólnego o ochronie danych A. Błaszczyńska wyraziła opinię, iż powyższy przepis może być jednak w pewnym sensie uznany za wadliwy, a to z tego względu, że wskazuje jako uprawnionego do roszczeń regresowych wyłącznie podmiot, który „zapłacił odszkodowanie za całą wyrządzoną szkodę". Oznaczałoby to – w ocenie wspomnianej Autorki – iż ten, kto zapłacił kwotę odszkodowania wyższą w stosunku do stopienia jego zawinienia, ale niepełną, nie może dochodzić roszczeń regresowych. Z drugiej strony takie ujęcie sprawy może być uważane za celowe z uwagi na fakt, że wymusza na naruszycielu całościowe zadośćuczynienie roszczeniom poszkodowanego w celu uzyskania uprawnienia do regresu[594].

[593] S. Kowalski, *Zakres swobody...*
[594] K. Biczysko-Pudełko, *Cywilnoprawna odpowiedzialność...*

Zgodnie z art. 441 k.c., jeżeli kilka osób ponosi odpowiedzialność za szkodę wyrządzoną czynem niedozwolonym, ich odpowiedzialność jest solidarna. Jeżeli szkoda była wynikiem działania lub zaniechania kilku osób, ten, kto szkodę naprawił, może żądać od pozostałych zwrotu odpowiedniej części zależnie od okoliczności, a zwłaszcza od winy danej osoby oraz od stopnia, w jakim przyczyniła się do powstania szkody. Ten, kto naprawił szkodę, za którą jest odpowiedzialny mimo braku winy, ma zwrotne roszczenie do sprawcy, jeżeli szkoda powstała z winy sprawcy. W przypadku regresu pomiędzy współsprawcami szkody zakres roszczenia jest uzależniony od okoliczności, wśród których szczególnie istotne (chociaż nie wyłączne) znaczenie ma stopień winy danej osoby oraz stopień, w jakim przyczyniła się ona do powstania szkody. Każda z tych okoliczności może mieć znaczenie samodzielne i niezależne od drugiej – identyczny stopień zawinienia nie wyklucza różnic w ocenie stopnia przyczynienia się współsprawcy według reguł adekwatnego związku przyczynowego.

Poza ramami tej pracy pozostają wymagające szczegółowych analiz zagadnienia sprowadzające się pytań, które w praktyce będą wymagały rozstrzygnięcia, takich jak:

1. Czy pełny regres osoby odpowiedzialnej mimo braku winy, o którym mowa w art. 441 § 3 k.c., jest możliwy tylko wtedy, gdy po stronie adresata roszczenia – bezpośredniego sprawcy szkody – zachodzi nie tylko wyłączność winy, ale również wyłączność przyczyny w wyrządzeniu szkody, np. podmiot przetwarzający wyłącznie winny?
2. W przypadku dalszego rozpowszechnienia danych, bezprawnie ujawnionych przez administratora czy odpowiedzialność razem z administratorem poniesie każdy podmiot, który rozpowszechnia te dane?
3. Czy administrator będzie odpowiadał za szkodę / krzywdę, która powstała w wyniku dalszego rozpowszechniania danych?

Zagadnienia szczególne dotyczące odpowiedzialności podmiotu przetwarzającego

Analizując zakres odpowiedzialności deliktowej podmiotu przetwarzającego, stwierdzić należy, że został on ukształtowanego w sposób odmienny od zasad odpowiedzialności administratora poprzez ograniczenie odpowiedzialności do przypadków niedopełnienia obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające lub w sytuacjach, gdy podmiot przetwarzający działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. RODO nie zawiera definicji instrukcji, o których mowa w art. 82 ust. 2 RODO. Przede wszystkim nie rozstrzyga tego, czy omawianymi instrukcjami mogą być postanowienia umowy Zgodnie z zasadą swobody umów administrator w relacji z podmiotem przetwarzającym ma możliwość wprowadzenia do umowy

postanowień doprecyzowujących sposób wykonawczy wykonywania obowiązku: podejmowania wszelkich środków wymaganych na mocy art. 32 RODO; pomagania administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III; pomagania administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO; udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w artykule 28 RODO oraz umożliwiania administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynienia się do nich[595].

Administrator danych nie będzie odpowiadał na podstawie RODO za naruszenie przez procesora – wynikających z umowy powierzenia – obowiązków względem administratora danych, jeżeli nie będzie to prowadziło do naruszenia przepisów ochrony danych przez samego administratora. np. nieudzielenie pomocy przy realizacji praw podmiotów danych, jeżeli administrator w tym zakresie samodzielnie zrealizuje te obowiązki. Inaczej jednak jego odpowiedzialność w tym zakresie będzie kształtować się na gruncie art. 474 k.c.

Oczywiście nie można także wykluczyć sytuacji, w której administrator i procesor będą odpowiadać samodzielnie, za naruszenie wynikające z działania lub zaniechania procesora np. w przypadku bezprawnego ujawnienia danych osobowych przez procesora. Jednocześnie należy przyjąć, że administrator nie będzie odpowiadał za naruszenia samodzielnych obowiązków procesora, których treść nie została objęta art. 28 ust. 3 RODO (np. prowadzenie przez procesora rejestru przetwarzań, o którym mowa w art. 32 ust. 2 RODO). Jak to zostało wskazane wyżej, na procesorów nałożone zostały pewne obowiązki wynikające wprost z przepisów RODO, które jednocześnie nie są obligatoryjnymi elementami umowy powierzenia. W zakresie wskazanych obowiązków (nie pokrywających się z tymi określonymi w art. 28 ust. 3 RODO), administrator nie ma bowiem możliwości skontrolowania tego, czy procesor wywiązuje się ze swoich obowiązków.

Co istotne, w RODO brak jest przepisów wprost wyłączających odpowiedzialność administratora za działania lub zaniechania procesora np. w sytuacji spełnienia wymogu o którym mowa w art. 28 ust. 1 RODO tj. korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą [596]. Zagadnieniem nierozstrzygniętym w tym zakresie jest to

[595] M.Czaplińska, *Naprawienie szkody z tytułu naruszenia RODO*….
[596] M.Gumularz, P.Kozik, *Odpowiedzialność administracyjna*...

w jaki sposób stan prawny, wynikający z RODO zestawić w praktyce współstosowania przepisów art. 429 i 474 k.c.

Obok zagadnienia czy postanowienia umowy są instrukcjami administratora możliwe jest sformułowanie kolejnych problemów, których rozstrzygnięcia nie znajdziemy wprost w RODO, takich jak:

- które polecenia na podstawie zakresu informacji posiadanych przez procesora, należy ocenić jako legalne?
- co gdy podmiot przetwarzający działał zgodnie z niezgodnymi z prawem instrukcjami administratora w świetle art. 28 ust. 3 RODO, który stanowi, że w związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych oraz jaki standard winy obowiązuje w tym zakresie subiektywny czy obiektywny?
- jaki jest stosunek art. 28 ust. 3 RODO do braku winy w art. 82 ust. 3 RODO?
- czy podmiot przetwarzający odpowiada za bezprawne przetwarzanie, jeżeli naruszenie przepisów RODO nastąpiło tylko po stronie administratora?
- co gdy podmiot przetwarzający działał poza lub wbrew instrukcjom administratora, ale były one niezgodne z prawem?

Zakres faktycznej odpowiedzialności kontraktowej administratora, współadministratora i procesora jest pochodną podziału obowiązków i odpowiedzialności, dokonanego w ramach umowy powierzenia między administratorem a podmiotem przetwarzającym, zawartej zgodnie z art. 28 RODO lub też w ramach wspólnych uzgodnień współadministratorów dokonanych na podstawie art. 26 RODO.[597]. W zakresie stosunku prawnego, jakim jest powierzenie przetwarzania danych osobowych, odpowiedzialność *ex contractu* występić może nie tylko w takiej relacji jak wymieniona powyżej. Odpowiedzialność kontraktową ponosić może podmiot przetwarzający wobec administratora, albo też podmiot podprzetwarzający wobec podmiotu przetwarzającego. Przykładów nienależytego wykonania umowy powierzenia, które mogą spowodować szkodę jest dużo. Przede wszystkim podmiot przetwarzający naraża się na odpowiedzialność poprzez spowodowanie szkody, nie realizując poleceń administratora lub wychodząc poza ich zakres, nie stosując lub stosując niewłaściwe środki zabezpieczania danych osobowych, wybierając podmiot podprzetwarzający niezapewniający stosownych gwarancji lub podpowierzając przetwarzanie danych osobowych bez zgody administratora[598]. W

[597] K. Biczysko-Pudełko, *Cywilnoprawna odpowiedzialność...*
[598] M.Czech, *Umowa powierzenia...*, s. 297.

kontekście przepisów RODO odpowiedzialność kontraktowa pojawia się w treści art. 28 ust. 4 RODO. Dotyczy on możliwości korzystania przez podmiot przetwarzający z podwykonawców (podpowierzenie przetwarzania danych osobowych) i nakłada obowiązek zawarcia umowy pomiędzy podmiotem przetwarzającym a podprzetwarzającym. Jest to stosunek prawny w którym zachodzi trójstopniowy łańcuch powierzenia (administrator danych powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu, a ten „podzleca" przetwarzanie podmiotowi podprzetwarzającemu).

W sytuacji gdy administrator poniósłby szkodę, prawodawca postanowił, że jeżeli podmiot podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, to pełna odpowiedzialność wobec administratora za wypełnienie obowiązków kolejnego podmiotu przetwarzającego (nazywanego podprzetwarzającym) będzie spoczywać na pierwotnym podmiocie przetwarzającym. Z uwagi na fakt, że podmioty w łańcuchu powierzeń łączą umowy, będzie miał tu zastosowanie reżim odpowiedzialności kontraktowej. W związku z tym mamy do czynienia z odpowiedzialnością za inne osoby i odnieść się należy do treści art. 474 k.c., który stanowi, że dłużnik odpowiedzialny jest jak za własne działanie lub zaniechanie za działania i zaniechania osób, z których pomocą zobowiązanie wykonywa, jak również osób, którym wykonanie zobowiązania powierza. Gdyby natomiast podmiotu przetwarzającego z podprzetwarzającym nie łączyło zobowiązanie ze stosunku umownego (co byłoby de facto niezgodne z treścią art. 28 ust. 4 RODO), podstawą prawną naprawienia szkody poniesionej przez administratora byłby art. 429 k.c., stanowiący, że kto powierza wykonanie czynności drugiemu, ten jest odpowiedzialny za szkodę wyrządzoną przez sprawcę przy wykonywaniu powierzonej mu czynności, chyba że nie ponosi winy w wyborze albo że wykonanie czynności powierzył osobie, przedsiębiorstwu lub zakładowi, które w zakresie swej działalności zawodowej trudnią się wykonywaniem takich czynności. Wina w wyborze i zawarte w tym przepisie domniemanie winy powierzającego zmienia klasyczny rozkład ciężaru dowodu, czyli jest odstępstwem od art. 6 k.c., co ułatwia sytuację osoby poszkodowanej. Warto też zauważyć, że art. 429 k.c. nie zwalnia z odpowiedzialności bezpośredniego sprawcy szkody, bowiem może on odpowiadać na zasadzie przewidzianej w art. 415 k.c. Tak więc nie można tu wyłączyć konstrukcji odpowiedzialności solidarnej na podstawie art. 441 k.c.[599]

[599] M. Czech, *Umowa powierzenia...*,s. 298.

ROZDZIAŁ VI.

Odpowiedzialność przedsiębiorcy za przetwarzanie danych osobowych z wykorzystaniem systemów sztucznej inteligencji

Pojęcie sztucznej inteligencji

Tradycyjnie za twórców pojęcia sztuczna inteligencja (ang. *artificial intelligence*) uważa się J. McCarthiego, M. Minskiego, N. Rochestera i C. Shannona, którzy użyli tego terminu w tytule swojego projektu badawczego, przedstawionego w 1955 r. Problematyka sztucznej inteligencji (zwanej dalej: SI) stanowi zatem przedmiot zainteresowania nauki już od ponad 70 lat[600] i znalazła się w głównym nurcie zainteresowania wielu dziedzin nauki – w tym nauk technicznych, społecznych, medycynie czy nauk prawnych. Sztuczna inteligencja wywrze, jak należy przypuszczać, największy wpływ na: szybkość obrotu i szablonowość stosunków prawnohandlowych, a także transparentność i bezpieczeństwo obrotu oraz trwałość stosunków prawnych.[601] Jest to technologia najszybciej rozwijająca się na świecie. Wzrost jej znaczenia wiąże się zatem z koniecznością znalezienia rozwiązań prawnych i etycznych, które zminimalizują możliwe negatywne aspekty jej rozwoju. W opracowaniach prawniczych poświęconych sztucznej inteligencji (w skrócie SI) często nie definiuje się tego pojęcia, przyjmując zapewne, nieco intuicyjnie, że czytelnik mniej więcej wie, co należy przez to rozumieć, a może dlatego, że nie wypracowano jeszcze powszechnie akceptowalnej definicji tego pojęcia. [602] Sztuczna inteligencja wymyka się już na samym początku próbom stworzenia zamkniętej definicji, ponieważ rozwija się w takim tempie i w tak wielu kierunkach, często pod zasłoną trudnych do zrozumienia technologii, że analiza jej przy użyciu aparatu pojęciowego zaczerpniętego z klasycznego wykładu prawa jest niezwykle trudna[603].

Według informatycznej definicji „sztuczna inteligencja" to określenie programu komputerowego, który zamiast wykonywać listę dokładnych instrukcji wykorzystuje zaawansowane modele statystyczne do tego, żeby rozwiązać zadanie. „Inteligencja" w tym przypadku oznacza, że program – na podstawie zbioru danych zawierającego przykłady zadań i poprawne odpowiedzi – sam znajduje występujące między nimi zależności (wzorce)[604].

---

[600] M. Rojszczak, *Prawne aspekty systemów sztucznej inteligencji – zarys problemu* [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019.

[601] M.P. Wiórek [w:] *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie*, t. 1, red. M. Dumkiewicz, K. Kopaczyńska–Pieczniak, J. Szczotka Jerzy, Warszawa 2020.

[602] M.P. Wiórek [w:] *Sto lat polskiego*...

[603] E. Kurowska–Tober, Ł. Czynienik, M. Koniarska, Aspekty prawne sztucznej inteligencji – zarys problematyki, MoP 2019/21.

[604] Zob. https://panoptykon.org/sztuczna-inteligencja-non-fiction.

Interdyscyplinarnym określeniem SI może być inteligencja inna niż naturalna, ponieważ do stworzenia SI można dojść poprzez algorytmy uczenia maszynowego, mogą być to algorytmy skonfigurowane z urządzeniem, np. pojazd autonomiczny lub poprzez modyfikacje ludzkiego ciała, poprzez emulacje ludzkiego mózgu (np. implanty wszczepiane do mózgu) lub przeniesienie imitacji ludzkiego mózgu do komputera. W ujęciu prawnym pojęcie SI przybiera odrębną postać terminologiczną. W badaniach nad rozwojem sztucznej inteligencji, stosowane są również inne terminy, w tym:

- „agent oprogramowania",
- inteligentny agent,
- elektroniczny agent,
- komputerowy agent,
- autonomiczny agent,
- robot zwany również agentem sprzętowym[605].

Uczenie maszynowe a SI

W definiowaniu SI panuje relatywizm w zależności od tego czy patrzymy na SI jako na dziedzinę z zakresu etyki czy prawa. W praktyce pojęciem tym jest nazywanych szereg rożnych zastosowań, często związanych z systemami uczenia maszynowego (ang. *machine learning*, ML). Uczenie maszynowe to jednak termin szerszy niż sztuczna inteligencja i obejmuje wszystkie rozwiązania bazujące na algorytmach zdolnych do budowania własnych wniosków na podstawie dostępnych informacji.[606] Prowadzi to do tego, że niekiedy opisywane są zastosowania nowych technologii, które ściśle rzecz ujmując, nie mają (jeszcze) nic wspólnego ze sztuczną inteligencją, ale stanowią, pod względem rozwoju technologicznego, etap ją poprzedzający (choć rozwiązania te mogą występować równolegle z rozwiązaniami stanowiącymi zalążek sztucznej inteligencji)[607].

Błędem byłaby jednak próba zrównania systemów uczenia maszynowego z systemami sztucznej inteligencji. Te drugie postrzegane są jako kolejny etap ewolucji następujący po uczeniu maszynowym. Tak jak cechą charakterystyczną dla systemów ML jest zdolność do odkrywania wiedzy, tak wyróżnikiem systemów SI jest zdolność do podejmowania samodzielnych decyzji.[608] Z kolei, w ramach systemów sztucznej inteligencji, a więc

[605] A. Krauski, *Status prawny sztucznego agenta. Podstawy prawne. Sztuczny agent i jego znaczenie dla rozwoju sztucznej inteligencji*, Warszawa 2020.
[606] M. Rojszczak, *Prawne aspekty*...
[607] M.P. Wiórek [w:] *Sto lat polskiego*...
[608] M. Rojszczak, *Prawne aspekty*...

informatycznych systemów autonomicznych stworzonych do realizacji określonego celu i posiadających zdolność do podejmowania samodzielnych decyzji, służących do jego osiągnięcia, wyróżnia się słabą oraz silną SI. O ile słaba sztuczna inteligencja jest zdolna do podejmowania samodzielnych decyzji, o tyle silną sztuczną inteligencję cechuje samoświadomość, zdolność do samostanowienia i zdolności poznawcze.

W różnego rodzaju opracowaniach pojawia się też niejednoznaczne pojęcie superinteligencji, które niekiedy i w pewnym uproszczeniu, używane jest jako swego rodzaju synonim sztucznej inteligencji (również wtedy pisze się o silnej i słabej superinteligencji). Inni autorzy stopniują sztuczną inteligencję, poczynając od sztucznej wąskiej inteligencji (*Artificial Narrow Intelligence*), stanowiącej odpowiednik słabej SI, przez sztuczną ogólną inteligencję (*Artificial General Intelligence*), która dorównuje człowiekowi, po właśnie wspomnianą sztuczną superinteligencję (*Artificial Superinteligence)* która będąc najwyższym stopniem rozwoju SI, przewyższa człowieka pod każdym względem.[609] Takie zróżnicowanie pojęć SI ma swoje uzasadnienie dla przyjęcia koncepcji gradacji poziomów odpowiedzialności i jej zasad, o czym będzie mowa w dalszej części pracy.

Dane osobowe w SI

Nie ma wątpliwości, że efektywne wykorzystanie danych na potrzeby sztucznej inteligencji (SI) uzależnione jest od szerokiego dostępu do jak najlepszych danych. Możliwości systemów SI powodują, że granica między danymi osobowymi i nieosobowymi przesuwa się, co wymusza inwentaryzowanie posiadanych danych oraz stosowanie adekwatnych metod ich wykorzystania i udostępniania. Przepływy danych, łączenie danych z różnych źródeł, agregowanie czy tworzenie zbiorów uwzględnia obydwa rodzaje danych, a linia podziału jest często nieoczywista. Wskazują na to przykłady, na których opierano się przy pracach nad rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1807 w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, gdzie dane generowane przez nowoczesne samochody wskazywano w uzasadnieniu tego aktu jako przykład danych nieosobowych. Natomiast przy pracach nad rozporządzeniem w sprawie prywatności i łączności elektronicznej, tzw. *e-privacy*, ten sam przykład wskazywano jako zagrożenie dla prywatności[610]. Zbiorczym elementem wspólnym dla sztucznej inteligencji są zatem dane, w

[609] M.P. Wiórek [w:] *Sto lat polskiego...*

[610] B. Fischer, *Prawne uwarunkowania wykorzystania danych nieosobowych przez sztuczną inteligencję – zagadnienia podstawowe* [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2022, s. 181

tym dane osobowe. Sztuczna inteligencja korzysta z danych i na podstawie ich analiz się uczy, wykorzystując coraz to bardziej złożone zbiory danych, pochodzące z coraz to nowszych źródeł. Jest to możliwe dlatego, że w cyfrowym świecie e-usług bardzo wiele informacji przekazywanych jest dobrowolnie, niejednokrotnie, w imię wygody – z jedynie pozorną gwarancją bezpieczeństwa[611].

Z tego względu wyzwaniami prawnymi dla SI jest zapewnienie jakości danych, które cechować powinien walor ich niedyskryminacyjnego charakteru oraz braku tzw. „przechyłu algorytmicznego", rozumianego potocznie jako okoliczność, że sztuczna inteligencja, jak człowiek, jest podatna na skrzywienia poznawcze. Istotne jest także zapewnienie ich legalności, jeżeli chodzi o dane osobowe lub dane objęte prawem własności intelektualnej oraz różnorodności, bo algorytmy wykorzystują dane o charakterze historycznym, tj. zmiennym w czasie. Uczenie się sztucznej inteligencji jest związane z przetwarzaniem danych osobowych poprzez wykorzystanie ich jako cyfrowej reprezentacji zjawisk. Działanie SI, przynajmniej w najczęstszym typie opartym na uczeniu maszynowym, wymaga korzystania z danych w taki sposób, że z jednej strony dane (zanonimizowane) są potrzebne już na etapie stworzenia określonej SI (konstruowania i uczenia); z drugiej – działanie autonomiczne możliwe jest wyłącznie wtedy, gdy system SI ma bezpośredni, w czasie rzeczywistym, dostęp do informacji. Myśląc o wykorzystaniu danych osobowych w SI możemy wskazać jako źródła ich pochodzenia np. odczyty z różnych systemów monitorowania, rejestrów i baz danych lub możemy mówić o danych jako o np. o zapisach mowy ludzkiej, tekście lub obrazach. Dane mogą mieć różną gęstość lub dynamikę zmian w czasie. Mogą też pochodzić z różnych źródeł i wymagać skomplikowanej integracji.[612]

W każdym z przypadków przetwarzania danych osobowych trzeba brać pod uwagę konieczność zastosowania się do zasad ochrony danych osobowych, które określają przepisy RODO, a także uzupełniających tę regulację unormowań krajowych – w Polsce na czele z przepisami ustawy UODO. Należy też pamiętać, że to, czy mamy do czynienia z danymi osobowymi zwykle zależy od kontekstu, w jakim występuje konkretna informacja. W działalności komercyjnej istotne są te dane osobowe, które mogą być pozyskane i wykorzystywane w rozwiązaniach bazujących na SI we wszystkich sferach aktywności

[611] B. Fischer, *Prawo do prywatności i pewności prawa przy wykorzystaniu instrumentów samoregulacyjnych w związku z przetwarzaniem danych jednostki w systemach rozproszonych* [w:] *Władza – obywatele – informacja. Ku nowemu porządkowi prawnemu. Księga pamiątkowa ku czci Teresy Górzyńskiej*, red. I. Lipowicz, Warszawa 2014, s. 273.

[612] Polityka rozwoju sztucznej inteligencji w Polsce. Założenia do strategii AI w Polsce. Plan działania Ministerstwa Polityka rozwoju sztucznej inteligencji.

gospodarczej. W obszarze zainteresowania będą głównie takie informacje o osobie fizycznej, jak jej wizerunek, głos, lokalizacja, wykorzystywane przez nią sygnały łączności bezprzewodowej, czy informacje identyfikujące ją pośrednio takie, jak np. numer rejestracyjny pojazdu. Nie bez znaczenia są tu także takie dane, które można wywodzić z kontekstu, w jakim są zbierane lub okoliczności, w jakich występuje konkretna osoba fizyczna. Chodzić tu może na przykład o hobby, sposób spędzania wolnego czasu, relacje towarzyskie czy rodzinne. Każda z tak określonych informacji może by zakwalifikowana do kategorii „dane osobowe" o ile dotyczy zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, ponieważ tylko takie informacje stanowią dane osobowe[613] na gruncie RODO.

Tak jak zostało powiedziane powyżej kwalifikacja konkretnych informacji jako „dane osobowe" w znacznej mierze ma charakter kontekstowy, stąd ich katalog nigdy nie będzie zupełny, ponieważ o tym, czy w określonym przypadku możliwe jest zidentyfikowanie osoby fizycznej decydują różne czynniki, do których coraz częściej należy dostępna technologia. „Osobowy" charakter informacji właściwie nie może być z góry przypisany żadnej kategorii, a zaliczenie informacji do „danych osobowych", wynika z kontekstu, w jakim się pojawiają.[614] Założenie takie uzasadnia także treść motywu 26 RODO, w którym wskazuje się, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby, w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. W ślad za wywodem rzeczonego motywu, aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. W przypadku wykorzystywania danych przy użyciu SI wszystkie te kwestie są bardzo istotne, chociażby z tej racji, że obraz, dźwięk, czy inne pozyskane informacje mogą być różnej jakości, albo mogą mieć walor historyczny. Z punktu widzenia prowadzonych w pracy rozważań ustalenia w tym właśnie względzie mają charakter kluczowy. Jeśli bowiem

[613] Zgodnie z art. 4 pkt 1 tego rozporządzenia „dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej ("osobie, której dane dotyczą"), przy czym – w przepisie tym przybliża się, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

[614] A. Mednis, *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, PiP 1997/6, s. 35.

przetwarzanie danych przez SI dotyczy informacji, które nie mają charakteru osobowego lub odnosi się do informacji anonimowych, niecelowe jest wkraczanie na grunt rozważań z zakresu ochrony danych osobowych, ponieważ w tym przypadku przepisy z tego obszaru nie mają zastosowania.

Przywołany już motyw 26 RODO przybliża tę kwestię, wskazując wprost, że zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Należy przy tym jednak wziąć pod uwagę, że odwołanie we wspomnianym motywie 26 RODO do kryterium „postępu technologicznego" pozwala jednocześnie uznać, że zakres pojęcia „dane osobowe" może być zmienny w czasie i informacje, których obecnie nie jesteśmy w stanie połączyć z konkretną osobą wraz z rozwojem i dostępem do nowych technologii potencjalnie mogą pozwolić na identyfikację osób fizycznych, a co za tym idzie dać podstawę do analiz z zakresu ochrony danych osobowych[615].

Założenia dotyczące uregulowania zasad korzystania z SI – rys historyczny

W ostatnich latach możemy obserwować prawdziwy „wysyp" założeń, polityk, strategii czy wytycznych na temat szeroko rozumianej sztucznej inteligencji. Dokumenty te dotyczą rozmaitych zagadnień, począwszy od prognozowania potencjalnego wpływu sztucznej inteligencji na rozwój ekonomiczny społeczeństwa (np. problem likwidowania niektórych zawodów albo wprowadzenia tzw. podatku od robotów), przez kwestie etyczne, aż do omawiania wybranych problemów prawnych związanych ze sztuczną inteligencją. Powstają one zarówno z inspiracji rządów poszczególnych państw, jak również są opracowywane przez wyspecjalizowane ciała kolegialne oraz instytuty badawcze. Trend ten jest widoczny zarówno na poziomie lokalnym, jak i regionalnym[616].

Prace podejmowane w ramach tych działań koncentrują się wokół zagadnień dotyczących definicji sztucznej inteligencji, zasad etycznych oraz zagadnień odpowiedzialności. I tak na początku.02.2017 w Parlamencie Europejskim odbyło się seminarium poświęcone rozwojowi robotyki oraz sztucznej inteligencji. W jego trakcie uczestnicy analizowali raport *Świat robotów w kontekście wyzwań prawa cywilnego*. Znalazły

[615] A. Konert, M. Sakowska-Baryła, *Prawne uregulowania w zakresie używania bezzałogowych statków powietrznych przez media*, International Journal of Legal Studies 2020/8/2.
[616] E. Kurowska-Tober, Ł. Czynienik, M. Koniarska, *Aspekty prawne*...

się w nim zapisy dotyczące najważniejszych zagadnień związanych z wyzwaniami, jakie niesie rozwój robotyki oraz sztucznej inteligencji m. in. w obszarze prawa cywilnego.
Efektem tego seminarium jest uchwalona 16.02.2017 r. Rezolucja Parlamentu Europejskiego zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki (2015/2103)[617]. Istotne jest, że rezolucja PE na pierwszym miejscu spośród zasad i wartości, które winny być brane pod uwagę przy projektowaniu nowego prawa cywilnego z zakresu robotyki, wymienia prawa Asimova[618].

Jak wskazano we wprowadzeniu do rezolucji, jednym z powodów jej opracowania stało się przekonanie, że: „ludzkość stoi obecnie u progu ery, w której coraz bardziej zaawansowane roboty, androidy, komputery i inne wcielenia sztucznej inteligencji wydają się dawać początek nowej rewolucji przemysłowej, która prawdopodobnie nie ominie żadnej warstwy społecznej". Tym samym, w ocenie twórców tej rezolucji, obecnie za zasadne uznać należy podjęcie takich działań, aby „przepisy uwzględniały prawne i etyczne implikacje i skutki tych zmian bez hamownia innowacji".

Rozwój sztucznej inteligencji (ang. *artificial intelligence*– AI) i robotyki w ostatnich latach uświadomił potrzebę stworzenia ram prawnych odpowiednich dla tego nowego zjawiska. Dyskusja na ten temat jest już dość zaawansowana. W literaturze wskazuje się najważniejsze obszary, w których refleksja jest najbardziej potrzebna. Za najpilniejsze uważa się poszukiwanie etycznych fundamentów dla dalszej ekspansji AI oraz konieczność wypracowania nowych rozwiązań odnoszących się do prawa cywilnego. Pojazdy autonomiczne, roboty medyczne czy programy doradcze stawiają fundamentalne pytania o odpowiedzialność cywilną (np. odnoszące się do winy). Z kolei rozwój automatycznych, inteligentnych systemów zawierania umów każe w nowy sposób spojrzeć na wiele podstawowych zasad i utrwalonych instytucji prawa kontraktów (takich jak np. świadomość, wola, błąd, podstęp, wykładnia umowy, dobra wiara AI)[619].

W rezolucji 2015/2103 dostrzeżono także potrzebę „zbadania, przeanalizowania i rozważenia konsekwencji prawnych", jakie może nieść ze sobą „nadanie robotom specjalnego

[617] P. . Stylec-Szromek, *Sztuczna Inteligencja – prawo, odpowiedzialność, etyka*, „Zeszyty Naukowe. Organizacja i Zarządzanie. Politechnika Śląska, 2018/123, s. 501–509.
[618] Prawa Asimova to zespół reguł wymyślonych w latach 40. i uzupełnionych w latach 80. Ubiegłego stulecia przez amerykańskiego pisarza *science fiction* Isaaca Asimova. Prawa Asimova początkowo traktowano bardzo poważnie. Niektórzy uważają, że swoją popularność zawdzięczają one temu, iż były remedium na tzw. kompleks Frankensteina, czyli obecny u jednostek i grup społecznych strach przed sztucznymi tworami człowieka, będącymi rezultatem rozwijającej się technologii (zwłaszcza tymi przypominającymi pod pewnymi względami ludzi). Kompleks Frankensteina to obawa, że uwolnią się one spod kontroli swych twórców i obrócą przeciwko człowiekowi (zob. P. Księżak, S. Wojtczak, *Prawa Asimova, czyli science fiction jako fundament nowego prawa cywilnego*, „Forum Prawnicze" 2020/4/60).
[619] P. Księżak, S. Wojtczak, *Prawa Asimova...*

statusu prawnego w perspektywie długoterminowej" i nadanie przynajmniej tym najbardziej rozwiniętym robotom autonomicznym „statusu osób elektronicznych odpowiedzialnych za naprawienie wszelkich szkód, jakie mogłyby wyrządzić, oraz ewentualnie stosowanie osobowości elektronicznej w przypadku podejmowania przez roboty autonomicznej decyzji lub ich niezależnych interakcji z osobami trzecimi", co w rzeczywistości mogłoby sprowadzać się do stworzenia nowej kategorii prawnej o specyficznych dla niej cechach i implikacjach.[620] Zagadnienie to było najszerzej komentowane w przestrzeni medialnej.

Dyskurs dotyczący możliwości przyznania robotom (sztucznej inteligencji) osobowości prawnej miał swój początek jeszcze w latach 80. ubiegłego stulecia Od tego też czasu w doktrynie prezentowane są zupełnie różne koncepcje co do powyższego, od tych najbardziej sceptycznych począwszy, przez te umiarkowanie aprobujące, a na tych wręcz nawołujących do przyznania robotom osobowości prawnej skończywszy[621].

Zdaniem niektórych z komentatorów w aktualnym stanie prawnym, brak zdolności sztucznego agenta do bycia stroną stosunków prawnych, powoduje występowanie licznych barier prawnych. Sztucznemu agentowi powinien zostać przyznany status podmiotu prawnego, ze względu na potrzebę zrealizowania dwóch celów. Po pierwsze, przyznanie sztucznemu agentowi podmiotowości prawnej ma umożliwić zalegalizowanie sposobu zastosowania sztucznego agenta w obrocie prawnym, w tym poprzez uwzględnienie zdolności do bycia stroną stosunków faktycznych i prawnych podczas ich działalności w imieniu i na rzecz człowieka. Po drugie, przyznanie sztucznemu agentowi podmiotowości prawnej będzie prowadziło do dzielenia się odpowiedzialnością za szkody wyrządzone działaniem lub zaniechaniem sztucznego agenta, przez użytkownika sztucznego agenta z producentem i projektantem (programistą)[622].

Rozważania prawne na temat przyznania podmiotowości SI idą w dwóch kierunkach. Pierwsza grupa rozważań w tym przedmiocie sprawdza się do analizy prawnych form zabezpieczenia obrotu prawnego z udziałem sztucznych agentów poprzez powiązanie ich z koncepcją uznania SI za przedmiot, a nie podmiot prawa, np. na zasadzie analogii do prawa rzymskiego i instytucji *peculium*, która w dużym uproszczeniu była majątkiem, który niewolnik otrzymywał od swojego właściciela i którym mógł samodzielnie zarządzać[623].

[620] K. Biczysko-Pudełko, D. Szostek, *Koncepcje dotyczące osobowości...*
[621] K. Biczysko-Pudełko, D. Szostek, *Koncepcje dotyczące osobowości...*
[622] A. Krauski, *Status prawny sztucznego agenta. Podstawy prawne. Postulowana konstrukcja prawna sztucznego agenta*, Warszawa 2020.
[623] K. Biczysko-Pudełko, D. Szostek, *Koncepcje dotyczące osobowości...*

Druga grupa rozważań uwzględnia przyznanie SI podmiotowości prawnej wskazując na następujące możliwe konstrukcje prawne, w ramach których sztuczny agent posiada status podmiotu prawnego:

1. Sztuczny agent jako osoba fizyczna;
2. Sztuczny agent jako posłaniec;
3. Sztuczny agent jako osoba małoletnia;
4. Sztuczny agent jako elektroniczna osoba prawna;
5. Sztuczny agent jako osoba fizyczna, za która odpowiedzialność ponosi osoba prawna;
6. Sztuczny agent jako pełnomocnik zarządu spółki kapitałowej[624].

Podmiotowość prawna SI a RODO

Zagadnienie czy SI ma być podmiotem, czy przedmiotem obrotu prawnego może mieć istotne znaczenie także dla zastosowania regulacji RODO. Uznanie sztucznego agenta za podmiot prawa, któremu należy przypisać odpowiadający osobie fizycznej status prawny, pozwalałby na rozwiązanie problemu ustalenia statusu prawnego podmiotów przetwarzających dane osobowe. Zgodnie z art. 4 pkt 7 RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie UE lub w prawie państwa członkowskiego, to również w prawie UE lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania. Definicja „administratora" przewidziana w art. 4 pkt 7 RODO jest przykładem definicji równościowej. Zatem przetwarzanie danych osobowych w sferze aktywności sztucznego agenta pozostającej poza kontrolą ze strony użytkownika, wymagałoby ustalenia celów przetwarzania danych osobowych oraz środków wykorzystywanych do przetwarzania, przypisanych do sztucznego agenta. Dopiero wówczas spełnione zostałyby kryteria przyznania sztucznemu agentowi statusu „administratora"[625].

Inaczej sytuacja przedstawiałaby się w przypadku uznania, że sztuczny agent przetwarza dane osobowe w ramach celów przetwarzania ustalonych przez użytkownika. Wówczas co do zasady można byłoby rozważyć relację pomiędzy użytkownikiem jako administratorem a sztucznym agentem jako podmiotem przetwarzającym. W praktyce jednak do ustalenia statusu powierzenia przetwarzania danych osobowych wymagany byłby akt

[624] A. Krauski, *Status prawny sztucznego agenta*...
[625] A. Krauski, *Status prawny sztucznego agenta*...

formalny w postaci umowy powierzenia przetwarzania danych, wskazanej w art. 28 ust. 1 RODO, której treść określona została w art. 28 ust. 3 RODO. Taka umowa nie mogłaby zostać skutecznie zawarta, ze względu na wymóg zgodnych oświadczeń woli stron, ponieważ w sferze aktywności sztucznego agenta, pozostającej poza kontrolą człowieka, człowiek nie byłby w stanie ustalić zamiaru sztucznego agenta.

Kolejny problem dotyczy możliwości egzekwowania od sztucznego agenta obowiązków określonych w RODO, w tym zarówno przykładowo w zakresie zrealizowania uprawnień wobec osoby fizycznej, które określone zostały w dziale III RODO, jak również w zakresie zabezpieczenia danych osobowych. Sztuczny agent nie mógłby być także, przynajmniej od strony praktycznej (pomimo uznania za stronę postępowania administracyjnego w rozumieniu art. 28 k.p.a.), stroną postępowań administracyjnych przed Prezesem UODO, w tym m.in. w zakresie nakładania przez organ ten decyzji mających wpływ na przetwarzanie danych osobowych, w tym również w zakresie nakładania kar pieniężnych. Tak więc przyjęcie fikcji prawnej, uznającej sztucznego agenta za osobę fizyczną, nie rozwiązałoby problemów przetwarzania danych osobowych z wykorzystaniem sztucznego agenta[626].

Koncepcje statusu prawnego SI w projektach dokumentów unijnych

Organy takie jak: Rada Europy w swoich opracowaniach czy Parlament Europejski w Rezolucji 2018/C252/25[627] nie odniosły się wprost do oceny statusu prawnego sztucznego agenta z punktu widzenia tego, czy jest przedmiotem czy też podmiotem stosunku prawnego. Niemniej w motywie AF Rezolucji 2018/C252/25 Parlament Europejski stwierdził, że w przypadku, gdy robot może podejmować niezależnie decyzje, tradycyjne przepisy nie będą wystarczające do ustalenia odpowiedzialności prawnej za szkody spowodowane przez robota, ponieważ na ich podstawie nie będzie możliwe określenie strony odpowiedzialnej za zapewnienie odszkodowania oraz żądanie od niej naprawienia wyrządzonej szkody.
Innymi słowy Parlament Europejski uznał, że w przypadku, gdy w wyniku działania sztucznego agenta w sposób autonomiczny, człowiek traci nad nim kontrolę, człowiek (np. użytkownik sztucznego agenta) nie powinien ponosić odpowiedzialności na dotychczasowych zasadach. Jeżeli człowiek miałby nie odpowiadać za szkody wyrządzone przez sztucznego agenta, to – z

[626] A. Krauski, *Status prawny sztucznego agenta...*
[627] Rezolucja Parlamentu Europejskiego z 16.02.2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, 2018/C252/25, (Dz.Urz. UE C z 18.07.2018).

uwagi na to, że prawo do odszkodowania nie może zostać usunięte z porządku prawnego – przyjąć należy, że Parlament Europejski założył określenie innego kręgu podmiotów odpowiedzialnych za powstałą szkodę, w tym także nie wykluczając odpowiedzialności sztucznego agenta samodzielnie bądź solidarnie[628].

Komisja Europejska w raporcie z 2019 r.[629] przedstawiła stanowisko dopuszczające przyznanie szczególnej podmiotowości prawnej sztucznym agentom, w zakresie obejmującym przyznanie odpowiedzialności. Jednocześnie Komisja Europejska podkreśliła praktyczne problemy związane z przyznaniem tego statusu w kontekście skutecznego dochodzenia roszczeń odszkodowawczych. Do problemów tych zalicza m.in. konieczność powiązania z takim statusem środków finansowych, co z kolej prowadziłoby do określenia limitu odpowiedzialności odszkodowawczej. Argument ten nie jest jednak przekonywający, w przypadku uznania, że pierwotna suma funduszy powiązanych ze sztucznym agentem, powinna zostać uzupełniona, bądź w określonych przypadkach podwyższona[630].

Niewątpliwie kwestia przyznania sztucznej inteligencji osobowości prawnej jest jednym z najważniejszych pytań, przed którymi staje obecnie doktryna prawa. W październiku 2017 r. świat obiegła informacja, że Arabia Saudyjska przyznała obywatelstwo humanoidalnemu robotowi *Sophia*. Przy czym podkreślenia wymaga, że *Sophia*, choć robiąca duże wrażenie, to raczej stosunkowo prosty robot, jeśli możemy tak mówić, biorąc pod uwagę niezwykle skomplikowane algorytmy, które stoją za jego funkcjonalnościami. To właściwie dość zaawansowany chatbot, który prowadzi rozmowę, naśladując ludzką formę komunikacji. Co istotne, ta niewątpliwie historyczna decyzja Arabii Saudyjskiej miała tak naprawdę wymiar propagandowy. Od tej pory we wszystkich encyklopediach to właśnie ten kraj będzie wymieniany jako pierwszy, który zdecydował się na przyznanie obywatelstwa robotowi. Równocześnie jednak za tą niewątpliwie przełomową decyzją nie poszły żadne deklaracje co do statusu prawnego nowego obywatela, jego osobowości prawnej, zdolności do zaciągania zobowiązań, bycia podmiotem praw, reguł dziedziczenia itd.[631]

W dyskusji nad sztuczną inteligencją istotne jest, że na chwilę obecną poza Unią Europejską brak jest szerszego forum, które byłoby w stanie przyjąć ponadnarodowe regulacje w tym obszarze. Wyjątkiem może tu być konieczność uregulowania dopuszczalności użycia broni wykorzystującej sztuczną inteligencję. Zagrożenie, jakie dla ludzkości może mieć

[628] A. Krasuski, *Status prawny sztucznego agenta...*
[629] Expert Group on Liability and New Technologies, *Report on Liability for Artificial Intelligence and Other Emerging Digital Technologies*, European Commission 2019.
[630] A. Krasuski, *Status prawny sztucznego agenta...*
[631] E. Kurowska-Tober, Ł. Czynienik, M. Koniarska, *Aspekty prawne...*

zastosowanie w walce konwencjonalnej np. w pełni zautomatyzowanych dronów (zdalnie kierowane bezzałogowe systemy powietrzne – BSP), które samodzielne dokonują wyboru celu oraz podejmują decyzję o jego likwidacji, może być przyczynkiem do powstania międzynarodowych regulacji w tym obszarze. Przykładem może tu być podpisany 27.01.1967 r. układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej łącznie z Księżycem i innymi ciałami niebieskimi, zwany też Traktatem o przestrzeni kosmicznej[632]. Na jego mocy państwa-sygnatariusze zobowiązały się nie umieszczać broni nuklearnej bądź innej broni masowego rażenia na orbicie okołoziemskiej, na Księżycu ani gdziekolwiek indziej w przestrzeni kosmicznej. Wśród 108 sygnatariuszy znaczna ich większość nie dysponuje potencjałem ekonomicznym czy militarnym, aby wykorzystać przestrzeń kosmiczną do działań zbrojnych. Niemniej przykład ten pokazuje, jak stymulująco na sferę regulacji prawnych potrafią oddziaływać określone zagadnienia[633].

Problematykę regulacyjną sztucznej inteligencji dostrzeżono w UE także, m.in. w kluczowych z tej perspektywy komunikatach wydanych przez Komisję Europejską[634]. W dokumentach tych przedstawiona została wizja dotycząca sztucznej inteligencji wspierająca „tworzenie w Europie etycznych, pewnych i najnowocześniejszych rozwiązań w zakresie SI" oparta na trzech filarach:

1. zwiększenie inwestycji publicznych i prywatnych w SI w celu jej szerszego rozpowszechnienia;
2. przygotowanie się na zmiany społeczno-gospodarcze oraz
3. zapewnienie odpowiednich ram etycznych i prawnych, aby wzmocnić wartości europejskie.

Pierwszym z efektów zaplanowanych przez Komisję działań było powołanie grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji, którym w pierwszej kolejności powierzono zadanie opracowania wytycznych w zakresie etyki dotyczącej godnej zaufania sztucznej inteligencji, a następnie zaleceń dotyczących polityki i inwestycji.

W opracowanych w kwietniu 2019 r. wytycznych Grupa ekspertów wskazała na konieczność stworzenia warunków dla rozwoju w Europie humanocentrycznej sztucznej

---

[632] Układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej, łącznie z Księżycem i innymi ciałami niebieskimi**,** sporządzony w Moskwie, Londynie, i Waszyngtonie dnia 27.01.1967 r. zwany też Traktatem o przestrzeni kosmicznej (Dz.U. 1968 nr 14 poz. 82).

[633] E. Kurowska-Tober, Ł. Czynienik, M. Koniarska, *Aspekty prawne...*

[634] Komunikaty Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komunikatu Regionów: *Sztuczna inteligencja dla Europy*, 25.04.2018, COM/2018/237 final; *Skoordynowany plan w sprawie sztucznej inteligencji*, 7.12.2018, COM/2018/795 final; *Biała Księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania*, 19.02.2020, COM/2020/65 final.

inteligencji przede wszystkim poprzez nadanie jej cechy „godnej zaufania" sztucznej inteligencji. Powinna posiadać ona trzy cechy, które muszą charakteryzować wyposażony w nią system przez cały jego cykl życia:

1. powinna być zgodna z prawem, tj. przestrzegać wszystkich obowiązujących przepisów ustawowych i wykonawczych;
2. powinna być etyczna, zapewniając zgodność z zasadami i wartościami etycznymi oraz
3. powinna być solidna zarówno z technicznego, jak i ze społecznego punktu widzenia, ponieważ systemy SI mogą wywoływać niezamierzone szkody nawet wówczas, gdy korzysta się z nich w dobrej wierze[635].

Zagadnienia dotyczące odpowiedzialności

Wydaje się, że w świetle prezentowanych wcześniej stanowisk (i wątpliwości) uznanie zwolenników koncepcji przyznania SI osobowości prawnej zapewniałaby bezpieczeństwo obrotu prawnego, zarówno z punktu widzenia osób korzystających ze SI, jak również przez osoby trzecie, które jako uczestnicy obrotu prawnego wchodzą w interakcje z SI. Taka koncepcja być może uprościłaby także rozważania na temat odpowiedzialności. Zapewnienie odpowiednich standardów ochrony w obszarze SI nie jest jednak zagadnieniem, które może zostać ograniczone tylko do jednej koncepcji. Znajduje to potwierdzenie w sprawozdaniu Komisji Europejskiej, w którym wskazane zostało m.in., że „nowe wyzwania w zakresie bezpieczeństwa stwarzają również nowe wyzwania w zakresie odpowiedzialności. Należy uwzględnić te wyzwania, aby zapewnić taki sam poziom ochrony, z jakiego korzystają poszkodowani w kontekście tradycyjnych technologii, przy jednoczesnym utrzymaniu równowagi w stosunku do potrzeb innowacji technologicznych[636].

Sprawę komplikuje przede wszystkim to, czy o sztucznej inteligencji mówimy w ujęciu tylko narzędzia, za pomocą którego określony podmiot wykonuje swoje zadania, czy chodzi o przypadki inteligentnego robota, czy wysokiej automatyzacji. Definiując koncepcję inteligentnych robotów odniesienia należy szukać w rezolucji Parlamentu Europejskiego z dnia 16.02.2017 r. charakteryzującej inteligentne roboty jako systemy, które posiadają takie cechy jak zdobywanie autonomii za pomocą czujników lub wymiany danych z otoczeniem (wzajemne

[635] D.Lubasz [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020.
[636] M. Jankowska, *Podmiotowość prawna sztucznej inteligencji*? [w:] *O czym mówią prawnicy, mówiąc o podmiotowości*, red. A. Bielska-Brodziak, Katowice 2015, s. 171 i n.; P. Księżak, *Zdolność prawna sztucznej inteligencji (AI)* [w:] *Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej*, red. W. Robaczyński, Łódź 2017, s. 63 i n.; K. Biczysko-Pudełko, D. Szostek, *Koncepcje dotyczące osobowości prawnej robotów – zagadnienia wybrane*, „Prawo Mediów Elektronicznych" 2019/2.

połączenia) oraz wymiany i analizy tych danych oraz zdolność samokształcenia na podstawie zdobytego doświadczenia i interakcji z otoczeniem.

Do określenia wysokiej automatyzacji posłużyć można się pięciostopniową skalą klasyfikacji Society of Automotive Engineers (SAE), według której wysoka automatyzacja zachodzi wtedy, gdy proces jest w pełni prowadzony przez system w założonych warunkach (poziom 4) oraz w przypadku automatyzacji pełnej, która ma miejsce wtedy, gdy system realizuje wszystkie funkcje danego procesu, w każdych warunkach (poziom 5). Dla zagadnienia odpowiedzialności ważne jest to, że w przypadku wysokiej automatyzacji podstawowym problemem jest konieczność „kontroli sztucznej inteligencji". Istotą sztucznej inteligencji na odpowiednio wysokim poziomie autonomiczności jest bowiem jej oderwanie od procesów decyzyjnych podejmowanych przez człowieka[637], czego najlepszym przykładem są autonomiczne pojazdy.

Jak słusznie zauważa P. Stylec-Szromek, zagadnienie odpowiedzialności SI obejmuje zatem dwa wątki. Po pierwsze chodzi o odpowiedzialność ponoszoną za aktywność maszyn oraz jej skutki. Zawsze w wypadku powstania szkody spowodowanej przez maszynę, bez względu na to czy dysponuje ona SI czy nie, będziemy poszukiwać odpowiedzialności konstruktora lub osób, w których dyspozycji pozostaje robot. W sytuacji normalnego użytkowania robota w pierwszej kolejności odpowiedzialność ponosić powinien ten, kto robota wytworzył, i np. wprowadził do niego wadliwy kod. Natomiast drugi aspekt to ewentualna odpowiedzialność samej maszyny w sytuacji, gdy robot działa samodzielnie oraz w sprzeczności z założeniami jego twórcy[638].

W przypadku każdego systemu korzystającego z technik uczenia maszynowego do grona podmiotów odpowiedzialnych można zaliczyć producenta, operatora (podmiot odpowiedzialny za jego działanie) oraz trenera (podmiot mający wpływ na odpowiednie przygotowanie systemu do pracy). Istotne w przypadku takich systemów jest, że w zależności od stopnia swobody systemu w podejmowaniu własnych decyzji oraz czasu jego eksploatacji, ciężar odpowiedzialności będzie przesuwał się z producenta na operatora, a następnie z operatora na trenera. Wyważenie odpowiedzialności między tymi stronami jest zadaniem skomplikowanym i najczęściej niemożliwym z perspektywy osoby poszkodowanej. Także z punktu widzenia podmiotów profesjonalnie zajmujących się produkcją oraz dostarczaniem agentów inteligentnych stan, w którym zakres ich odpowiedzialności jest nieznany i może być

[637] W. Robaczyński, *Sztuczna inteligencja – przedmiot badań czy podmiot kontrolowany*, „Kontrola państwowa" 2022/67/6(407), s. 8–29.
[638] E. Kurowska-Tober, Ł. Czynienik, M. Koniarska, *Aspekty prawne sztucznej*...

zmienny w czasie w trudny do przewidzenia dla nich sposób, wydaje się nieakceptowalny. Propozycję rozwiązania powyższego problemu przedstawił A. Chłopecki, posiłkując się pojęciem faktycznego dysponenta SI. Oparcie odpowiedzialności na dysponencie pozwoliłoby przenieść część jej ciężaru z producenta, a jednocześnie uwzględnić okoliczność wielości dysponentów. Nieprzekonująca jest jednak argumentacja tego Autora dotycząca możliwych proponowanych rozstrzygnięć konfliktu interesów między dysponentami. Z pewnością wprowadzenie domniemania prawnego, że dysponentów tej samej SI traktuje się jako działających wspólnie, nie prowadziłoby do wyjaśnienia licznych wątpliwości interpretacyjnych[639].

W tym miejscu można postawić tezę, że odpowiedzialność za sztuczną inteligencję nie powinna się różnić od odpowiedzialności na zasadach ogólnych. Dopóki sztuczna inteligencja działa w granicach przewidywalnego kontekstu i błędu, który może być udziałem człowieka, to jej odpowiedzialność nie powinna być oparta na innych warunkach. Jeżeli działalność SI wychodziłaby poza granice przewidywalnego kontekstu, czy błąd sztucznej inteligencji byłby takim błędem, którego człowiek by na pewno nie popełnił, to wtedy inne zasady odpowiedzialności miałby swoje uzasadnienie.

W literaturze pojawiają się głosy, że w prawie odszkodowawczym potencjalna podmiotowość sztucznej inteligencji może ułatwić prawną ocenę określonych stanów faktycznych. Takie podejście, choć na pierwszy rzut oka atrakcyjne, wiąże się jednak z wieloma potencjalnymi trudnościami, dotyczącymi m.in. konieczności stworzenia dla sztucznej inteligencji miary należytej staranności (art. 355 k.c.). W literaturze można także spotkać wypowiedzi, w świetle których podmiotowość sztucznej inteligencji miałaby w przyszłości wyrażać się w zawieraniu umów i wykonywaniu zobowiązań[640].

Problem podmiotowości prawnej budzi skrajne stanowiska w doktrynie. G. Bar twierdzi, że ciekawym i wartym rozważenia pomysłem jest przedstawiona przez PE koncepcja „elektronicznej osoby prawnej", zgodnie, z którą „najbardziej rozwiniętym robotom autonomicznym można byłoby nadać status osób elektronicznych odpowiedzialnych za naprawianie wszelkich szkód, jakie mogłyby wyrządzić". Konstrukcja prawna osobowości elektronicznej miałaby także zastosowanie w przypadkach podejmowania przez roboty autonomicznych decyzji lub ich niezależnych interakcji z osobami trzecimi.[641] M.

[639] M. Rojszczak, *Prawne aspekty*...
[640] W. Robaczyński, *Sztuczna inteligencja*..
[641] G. Bar, *Robot personhood, czyli po co nam antropocentryczna sztuczna inteligencja*? [w:] *Prawo sztucznej inteligencji*..., red. L. Lai, M. Świerczyński, pkt 6.

Wałachowska jest zdania, że póki co należy przede wszystkim wykorzystywać rozwiązania już istniejące., takie np. odpowiedzialność za produkt niebezpieczny w rozumieniu art. 449 [1]i n. k.c.[642]. Wielu autorów odnosi się do upodmiotowienia AI sceptycznie, uznając je za niemożliwe, zbędne lub co najmniej przedwczesne. Wyraźnie przeciwko takiej możliwości, także w odniesieniu do zaawansowanej sztucznej inteligencji, wypowiedział się M Uliasz. Autor uzasadnia to brakiem autonomicznego interesu i woli, przypominającej wolę człowieka. Jego zdaniem należy przyjąć, że „nawet silna (ogólna) sztuczna inteligencja nie spełnia materialnych warunków przyznania zdolności prawnej, które były przestrzegane dotychczas w prawodawstwie[643]. Podobne stanowisko prezentuje A. Kappes, który twierdzi, że zasadniczym argumentem przeciwko przyznaniu AI podmiotowości prawnej jest ten, że sztuczna inteligencja jest przedmiotem stosunku cywilnoprawnego. Jest to nie do pogodzenia z możliwością bycia podmiotem tego stosunku. Można być bowiem albo podmiotem, albo przedmiotem prawa, względnie stosunku prawnego (alternatywa rozłączna)[644].

Istotne rozważania w zakresie odpowiedzialności za szkody dokonane przez SI zawiera przywoływana już wcześnie Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019–2027. Zgodnie z powyższym dokumentem, Polska opowiada się za koncepcją supremacji człowieka nad systemami SI, a co za tym idzie: odpowiedzialnością ludzką osobistą lub osób prawnych, których człowiek jest założycielem i zarządcą.

W zagadnieniach dotyczących SI istotny jest także problem jakie ryzyka niesie stosowanie SI, dlatego problemem są zasady odpowiedzialności i to na ile SI jest w stanie się uczyć w związku z gromadzeniem danych. Mechanizmy SI nie są w stanie jeszcze zastąpić człowieka. Dokumenty UE wskazują na to, że mechanizmy mają człowieka wspierać, a nie zastępować, co powinno mieć wpływ na przyjmowane konstrukcje prawne. Zaawansowane systemy SI generują ryzyko wyrządzenia szkody, polegające na tym, że system się pomyli lub nie podejmie prawidłowej decyzji. Pojawia się pytanie kto i na jakich zasadach powinien odpowiadać, zwłaszcza że w przypadku SI zachodzi konieczności równoważenia interesu podmiotu, który wdraża, rozwija i użytkuje systemy, w którym implementowane są tego typu rozwiązania SI, a z drugiej strony równoważenia interesu społecznego związanego z możliwościami jakie dają algorytmy sztucznej inteligencji.

---

[642] M. Wałachowska [w:] *Prawo sztucznej inteligencji…*, red. L. Lai, M. Świerczyński.

[643] M. Uliasz, *Sztuczna inteligencja jako sztuczna osoba prawna* [w:] *Sztuczna inteligencja, blockchain...,* red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek.

[644] A. Kappes, *Podmiotowość prawna sztucznej inteligencji. Rzeczywista potrzeba czy kreacjonizm prawniczy?* [w:] *Non omne quod licet honestum est. Studia z prawa cywilnego i handlowego w 50-lecie pracy naukowej Profesora Wojciecha Jana Katnera*, red. U. Promińska, S. Byczko, A. Kappes, B. Kucharski, Warszawa 2022, s. 332.

Obecnie w Komisji prawnej PE aktywnie podchodzi się do tematu SI. Problemy omówione powyżej zostały dostrzeżone zostały w projekcie rezolucji Parlamentu UE z 4.05.2020 r. o odpowiedzialności cywilnej za działania systemów sztucznej inteligencji[645], a 5.10.2020 r. przedstawione zostało sprawozdanie z zaleceniami dla Komisji modyfikujące zasady z 4.05.2020 r. Intensywność prac oraz kolejne zmiany projektu wskazują na wzmożenie dyskusji m.in nad kształtowaniem odpowiedzialności za działania sztucznej inteligencji. Kompleksowe regulacje ogólne odpowiedzialności nadal pozostają jednak wyzwaniem.

Do tej pory za takie całościowe próby regulacji tego tematu można uznać propozycje zawarte m.in. w rezolucji Parlamentu Europejskiego z dnia 16.02.2017 r. zawierającej zalecania dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, w której rozważane były jako alternatywna dla modelu odpowiedzialności opartej na zasadzie winy modele odpowiedzialności deliktowej oparte na zasadzie ryzyka, zasadzie zarządzania ryzykiem oraz odpowiedzialności gwarancyjno-repartycyjnej.

Parlament Europejski zaznaczył w rezolucji z 16.02.2017 r., że podejście zakładające zarządzanie ryzykiem nie skupia się na osobie, „która działała w sposób niedbały", jako ponoszącej odpowiedzialność indywidualną, ale na osobie, która może, w określonych okolicznościach, zminimalizować ryzyko i podjąć działania w odniesieniu do negatywnych skutków (pkt 55). Po wskazaniu ostatecznie odpowiedzialnych stron ich odpowiedzialność powinna zasadniczo być proporcjonalna do poziomu instrukcji, jakie wydano robotowi, i stopnia jego autonomii, a zatem im dany robot ma większą zdolność uczenia się lub większą autonomię i im dłużej trwało „szkolenie" robota, tym większa odpowiedzialność powinna spoczywać na osobie prowadzącej szkolenie, z tym zastrzeżeniem, że – poszukując osoby, która jest rzeczywiście odpowiedzialna za szkodliwe zachowanie robota – nie należy mylić umiejętności wynikających ze „szkolenia" robota z umiejętnościami zależącymi ściśle od zdolności robota do samodzielnego uczenia się; zauważa, że przynajmniej na obecnym etapie odpowiedzialność musi spoczywać na człowieku, a nie na robocie (pkt 56). W zaleceniach Parlamentu zwrócono również uwagę na możliwość, iż rozwiązaniem złożonego problemu ustalania odpowiedzialności za szkody spowodowane przez coraz bardziej autonomiczne roboty może być ubezpieczenie obowiązkowe, na wzór ubezpieczeń samochodowych. Taki

[645] Rezolucja Parlamentu Europejskiego z 20.10.2020 r. z zaleceniami dla Komisji w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)).

system ubezpieczeń mógłby zostać uzupełniony funduszem, aby można było naprawiać szkody w przypadkach, które nie są objęte ubezpieczeniem (pkt 57–58).[646]

W projekcie rezolucji Parlamentu Europejskiego z 4.05.2020 r. ze zmianami z 5.10.2020 r., w szczegółowych zaleceniach dla przygotowujących projekt rozporządzenia PE i Rady w sprawie odpowiedzialności za działania systemów sztucznej inteligencji zawarta została proponowana treść rozporządzenia, zawierająca regulacje dotyczące odpowiedzialności. Modyfikuje ona dotychczasowe koncepcje, wprowadzając dwa modele odpowiedzialności w zależności od rodzaju systemu SI, który został zastosowany. Projektodawca proponuje wydzielenie zasad odpowiedzialności dla systemów wysokiego ryzyka. Definiuje wysokie ryzyko jako znaczącą potencjalną możliwość wyrządzenia przez autonomicznie działający system sztucznej inteligencji losowo występujących szkód jednej osobie lub większej liczbie osób w taki sposób, że niemożliwe jest wcześniejsze przewidzenie wystąpienia tych szkód. Znacząca potencjalna możliwość zależy od wzajemnego stosunku pomiędzy powagą ewentualnej szkody, prawdopodobieństwem, że ryzyko się zmaterializuje oraz sposobem użycia systemu sztucznej inteligencji. W załączniku do rozporządzenia podana została lista systemów SI obarczonych wysokim ryzykiem, wyszczególniająca dla przykładu np. bezzałogowe statki powietrzne w rozumieniu art. 3 ust. 30 rozporządzenia (UE) 2018/1139, których wzmożoną powszechność użycia obserwujemy aktualnie na co dzień. Już na tym etapie wyszczególnienia systemów pojawiły się wątpliwości interpretacyjne jak klasyfikować niektóre z rozwiązań, np. oprogramowanie saas dla elektrowni.

Dlatego w projekcie z 5.10.2020 r. zatwierdzono, że samo oprogramowanie może być traktowane jako system sztucznej inteligencji na potrzeby odpowiedzialności. Odpowiedzialność na zasadzie ryzyka w projekcie rozporządzenia przypisana jest tym samym podmiotowi wdrażającemu działanie systemu SI obarczonego wysokim ryzykiem, który nie może się zwolnić od odpowiedzialności wykazując należytą staranność oraz powołując się na autonomiczny charakter SI i którego obowiązkiem jest zawarcie w tym zakresie ubezpieczenia od odpowiedzialności. Podmiot wdrażający zdefiniowany jest jako osoba, która decyduje o życiu sztucznej inteligencji oraz kontroluje zagrożenia wynikające z użycia i korzystania z działania jej systemu. Takie ujęcie nie pozwala na wyjaśnienie zasad odpowiedzialności w sytuacji, gdy w procesie związanym z użyciem SI oprócz podmiotu wdrażającego występują

[646] L. Bosek, *Perspektywy rozwoju odpowiedzialności cywilnej za inteligentne roboty*, „Forum Prawnicze" 2019/2/(52).

inne etapy użycia systemów SI i inne podmioty takie jak producent, podmiot kontrolujący, czy użytkownik. W projekcie z 5.10.2020 r projektodawca odstąpił od koncepcji przypisania odpowiedzialności podmiotowi wdrażającemu i posłużył się nomenklaturą operatora, wyróżniając dwie jego kategorie fronted operatora i innego operatora – backend operatora.

W zakresie pojęcia szkody podlegającej kompensacji projekt skupia się na szkodzie majątkowej na mieniu i na osobie, którą definiuje jako negatywny wpływ na życie, zdrowie, nienaruszalność cielesną lub stan posiadania osoby fizycznej lub prawnej za wyjątkiem szkód niemajątkowych. W tym zakresie znacząco różni się od zakresu obowiązku naprawienia szkody na gruncie RODO, które obejmuje pojęciem szkody także szkodę niemajątkową, tym samym wyłączając z obowiązku naprawienia szkody sytuacje np. naruszenia prywatności w wyniku działania systemów SI. Szkody na osobie podlegające według projektu rozporządzenia kompensacji zostały precyzyjnie określone poprzez wskazanie, że w przypadku śmierci szkodą są koszty leczenia przed śmiercią, koszty pochówku, ograniczenia możliwości zarobkowania, zwiększenia potrzeb, koszty utrzymania osoby trzeciej. W przypadku uszczerbku na zdrowiu w zakres szkody według projektu rozporządzenia wchodzi zwrot kosztów leczenia oraz utrata możliwości zarobkowania. Projekt wprowadza limity odpowiedzialności ujęte jako ograniczenia odpowiedzialności za szkodę na mieniu do 8 mln euro, a w przypadku szkody na osobie do 20 mln euro, przy czym w projekcie z 5.10.2020 znacznie zredukowano kwoty odpowiednio do 2 i 10 mln euro przy jednoczesnym obowiązku wykupienia na tą kwotę polisy ubezpieczeniowej. Projekt rozporządzenia wprowadza oddzielne regulacje zasad przedawnienia dla systemów obarczonych wysokim ryzykiem[647].

Do projektów rozwiązań dotyczących zasad odpowiedzialności za SI w kwietniu 2021 r. dołączają zaproponowane przez Komisję pierwsze w historii ramy prawne dotyczące sztucznej inteligencji, które zgodnie z założeniami mają uwzględniać wszystkie zagrożenia związane z AI i pozycjonować Europę jako światowego lidera, jeśli chodzi o godną zaufania AI. W pakiecie zaprezentowanym przez Komisję znalazł się wniosek dotyczący rozporządzenia ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt o sztucznej inteligencji, AI ACT)[648].

[647] Zob. https://www.europarl.europa.eu/doceo/document/A-9-2020-0178_PL.html#_section2

[648] Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie stucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, 21.04. 2021, (COM/2021/206 final)
https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

Zakres projektu rozporządzenia AI ACT obejmuje przede wszystkim problematykę zakazanych praktyk w zakresie AI, wprowadza podział systemów AI z równoczesnym nałożeniem wielu obowiązków na AI wysokiego ryzyka (jak kwestia oceny zgodności, dokumentacji, przejrzystości, obowiązek informacyjny, utworzenie systemu zarządzania ryzykiem, obowiązki importerów, dystrybutorów, obowiązek automatycznego rejestrowania zdarzeń itd.), regulacje dotyczące notyfikacji i organów notyfikujących, a także zasady tworzenia norm, oceny zgodności przez Komisję Europejską (delegacja do wydawania przepisów wykonawczych), utworzenie Europejskiej Rady do spraw Sztucznej Inteligencji. Co istotne omawiany projekt wprowadza zmiany w wielu dyrektywach, rozszerzając ich zakres obowiązywania także na systemy AI, nakładając przy tym dodatkowe obowiązki wynikające z projektu rozporządzenia i rozszerzając zasady odpowiedzialności wynikające z poszczególnych dyrektyw również na systemy AI[649]. Podmiotowy zakres zastosowania AI ACT definiowany jest poprzez określenie, że:

1. „dostawca" oznacza osobę fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które opracowują system sztucznej inteligencji lub zlecają jego opracowanie w celu wprowadzenia go do obrotu lub oddania go do użytku pod własną nazwą handlową lub własnym znakiem towarowym –odpłatnie lub nieodpłatnie;
2. „użytkownik" oznacza osobą fizyczną lub prawną, organ publiczny, agencję lub inny podmiot, które korzystają z systemu sztucznej inteligencji pod swoją kontrolą, z wyjątkiem sytuacji, gdy system sztucznej inteligencji jest wykorzystywany w ramach osobistej działalności pozazawodowej;
3. „importer" oznacza dowolną osobę fizyczną lub prawną mającą siedzibę w Unii, która wprowadza do obrotu lub oddaje do użytku system sztucznej inteligencji opatrzony nazwą handlową lub znakiem towarowym osoby fizycznej lub prawnej mającej siedzibę poza granicami Unii;
4. „dystrybutor" oznacza dowolną osobę fizyczną lub prawną w łańcuchu dostaw, inną niż dostawca lub importer, która udostępnia system sztucznej inteligencji na rynku unijnym bez zmiany jego właściwości;
5. „operator" oznacza dostawcę, użytkownika, upoważnionego przedstawiciela, importera i dystrybutora.

[649] D. Szostek, *To nie takie proste. System odpowiedzialności za algorytmy, w tym AI, z perspektywy prawa unijnego* [w:] *Prawo sztucznej inteligencji i nowych technologii 2*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2022, s. 128.

Głównym założeniem AI ACT jest zdefiniowanie sztucznej inteligencja wysokiego ryzyka jako działania w poniższych obszarach:

- identyfikacja biometryczna i kategoryzacja osób fizycznych;
- infrastruktury krytyczne (np. transport), które mogą zagrażać życiu i zdrowiu obywateli;
- edukacja lub szkolenie zawodowe –decydowanie o dostępie do edukacji i zawodowym przebiegu czyjegoś życia (np. punktacja egzaminów);
- zatrudnienie, zarządzanie pracownikami i dostęp do samozatrudnienia (np. oprogramowanie do sortowania CV w procedurach rekrutacyjnych);
- podstawowe usługi prywatne i publiczne (np. ocena kredytowa uniemożliwiająca obywatelom uzyskanie pożyczki);
- egzekwowanie prawa, które może ingerować w prawa podstawowe ludzi (np. ocena wiarygodności dowodów);
- zarządzanie migracją, azylem i kontrolą granic (np. weryfikacja autentyczności dokumentów podróży);
- wymiar sprawiedliwości i procesy demokratyczne (np. systemy AI mające na celu wspomaganie organu sądowego w badaniu i interpretacji faktów oraz prawa).

Systemy sztucznej inteligencji wysokiego ryzyka muszą spełniać wymagania ustanowione w Rozdziale 2 AI ACT określone jako:

1. system zarządzania ryzykiem stanowiący ciągły, iteracyjny proces realizowany przez cały cykl życia systemu, wymagający regularnej, systematycznej aktualizacji;
2. testowanie systemu AI w celu zidentyfikowania ryzyk i określenia odpowiednich środków łagodzących oraz sprawdzenia, czy system działa konsekwentnie zgodnie z zamierzonym celem;
3. system zarządzania jakością (udokumentowany w formie pisemnych zasad, procedur i instrukcji);
4. wymogi dotyczące danych i zarządzania nimi: zbiory danych treningowych, walidacyjnych i testowych podlegają odpowiednim praktykom w zakresie zarządzania danymi; wymóg, aby wszystkie zestawy danych szkoleniowych, walidacyjnych i testowych były kompletne, wolne od błędów i reprezentatywne;
5. dokumentacja techniczna dla systemu sztucznej inteligencji wysokiego ryzyka sporządza się przed wprowadzeniem danego systemu do obrotu lub oddaniem go do użytku oraz dokonuje się jej aktualizacji – tzw. rozliczalność. Zawiera ona co najmniej elementy określone w Załączniku IV (w tym dotycząca architektury systemu, algorytmów i specyfikacji modelu) – tzw. Wyjaśnialność;

6. rejestry zdarzeń – funkcja umożliwiająca automatyczne rejestrowanie zdarzeń podczas działania tych systemów; musi zapewniać, w całym cyklu życia systemu sztucznej inteligencji, poziom identyfikowalności jego funkcjonowania odpowiedni do przeznaczenia systemu;
7. przejrzystość i udostępnianie informacji użytkownikom:
   - umożliwienie użytkownikom interpretacji wyników działania systemu i ich właściwe wykorzystanie;
   - dostarczenie użytkownikom instrukcji obsługi w odpowiednim formacie cyfrowym lub innym formacie zawierającą zwięzłe, kompletne, poprawne i jasne informacje, które są istotne, dostępne i zrozumiałe dla użytkowników;
8. nadzór ze strony człowieka: uwzględnienie odpowiednich narzędzi interfejsu człowiek-maszyna, aby w okresie wykorzystywania systemu sztucznej inteligencji wysokiego ryzyka mogły je skutecznie nadzorować osoby fizyczne;
9. dokładność, solidność i cyberbezpieczeństwo:
   - poziomy dokładności i odpowiednie wskaźniki dokładności systemów sztucznej inteligencji wysokiego ryzyka deklaruje się w dołączonych do nich instrukcjach obsługi
   - odporność na błędy, usterki lub niespójności, które mogą wystąpić w systemie lub w środowisku, w którym działa system, w szczególności w wyniku interakcji z osobami fizycznymi lub innymi systemami;
   - solidność systemów sztucznej inteligencji wysokiego ryzyka można osiągnąć dzięki rozwiązaniom technicznym gwarantującym redundancję, które mogą obejmować plany zakładające dostępność systemu zapasowego lub plany zapewniające przejście systemu w stan bezpieczny (tzw. *fail-safe*);
   - rozwiązania techniczne mające na celu eliminowanie podatności charakterystycznych dla sztucznej inteligencji obejmują, w stosownych przypadkach, środki służące zapobieganiu atakom mającym na celu manipulowanie zbiorem danych treningowych, danym wejściowym, które mają na celu spowodowanie błędu w modelu („niepożądane przykłady”), lub wadom modelu, a także środki służące weryfikacji działania systemu pod kątem tych zagrożeń

W dniu 11.11.2022 r. upubliczniona została nowa wersja projektu AI ACT, wprowadzająca zmiany w stosunku do dwóch poprzednich wersji. W nowej wersji zmodyfikowana została definicja systemu sztucznej inteligencji i aktualnie uwzględnia ona elementy autonomii, jaką posiada AI.

Omawiane powyżej projekty dowodzą tego, że kwestia odpowiedzialności wciąż stanowi jedną z najważniejszych barier na drodze do korzystania ze sztucznej inteligencji. Problem ten nadal dostrzega Komisja Europejska, która w 28.09.2022 r. złożyła wniosek dotyczący Dyrektywy w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji. We wniosku tym podniesione zostało, że obowiązujące przepisy krajowe dotyczące odpowiedzialności, w szczególności opartej na zasadzie winy, nie są dopasowane do rozpatrywania roszczeń z tytułu odpowiedzialności za szkody spowodowane przez produkty i usługi oparte na sztucznej inteligencji. Zgodnie z tymi przepisami poszkodowani muszą udowodnić bezprawne działanie lub zaniechanie osoby, która spowodowała szkodę. Cechy szczególne sztucznej inteligencji, w tym jej złożoność, autonomia i brak przejrzystości (tzw. efekt czarnej skrzynki), mogą sprawić, że zidentyfikowanie osoby ponoszącej odpowiedzialność i udowodnienie spełnienia wymogów uznania roszczenia odszkodowawczego może być dla poszkodowanych trudne lub nadmiernie kosztowne. Poszkodowani ubiegający się o odszkodowanie mogą w szczególności ponieść bardzo wysokie koszty wstępne i uczestniczyć w znacznie dłuższym postępowaniu sądowym niż miałoby miejsce w sprawach niezwiązanych ze sztuczną inteligencją. Może to zatem powstrzymać poszkodowanych przed ubieganiem się o odszkodowanie.

Powyższy wniosek stanowi uzupełnienie innych elementów polityki Komisji Europejskiej w dziedzinie sztucznej inteligencji opartych na zapobiegawczych wymogach regulacyjnych i nadzorczych, do których należą akt w sprawie AI, RODO, akt o usługach cyfrowych oraz prawo Unii w zakresie niedyskryminacji i równego traktowania. Jego celem nie jest ustanowienie ani harmonizacja obowiązków dochowania należytej staranności lub odpowiedzialności różnych podmiotów, których działalność jest regulowana na podstawie tych aktów prawnych. Wniosek nie ma prowadzić także do powstania nowych roszczeń z tytułu odpowiedzialności oraz nie wpływać na wyłączenia odpowiedzialności na mocy tych innych aktów prawnych. Wniosek wprowadza wyłącznie zmniejszenie ciężaru dowodu dla osób, które poniosły szkody spowodowane przez systemy sztucznej inteligencji w przypadku roszczeń, które mogą być oparte na prawie krajowym lub na tych innych aktach prawa Unii. Jako uzupełnienie tych elementów, wniosek zapewnia ochronę prawa osoby poszkodowanej do dochodzenia odszkodowania na podstawie prawa prywatnego[650].

[650] Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), 28.09.2022, COM/2022/496 final;
https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52022PC0496&from=PL

Omawiana powyżej regulacja ma mieć zastosowanie do pozaumownych cywilnoprawnych roszczeń z tytułu szkód spowodowanych przez system sztucznej inteligencji, w przypadku, gdy dochodzi się ich w ramach systemów odpowiedzialności opartych na zasadzie winy. Przewiduje, że osoby dochodzące odszkodowania będą miały możliwość uzyskania informacji na temat systemów sztucznej inteligencji wysokiego ryzyka, które mają być rejestrowane/dokumentowane zgodnie z aktem w sprawie AI. Ponadto domniemania wzruszalne zapewnią, aby ciężar dowodu spoczywający na osobach dochodzących odszkodowania za szkody spowodowane przez systemy sztucznej inteligencji był bardziej racjonalny i aby ich uzasadnione roszczenia z tytułu odpowiedzialności mogły zostać uznane.

Problematyczne zagadnienia osobowości prawnej SI i jej odpowiedzialności na tle Kodeksu cywilnego

W dyskusji nad sztuczną inteligencją na poziomie UE pojawiły się propozycje, na razie czysto teoretyczne, uznawania jej za samodzielny podmiot wyposażony zarówno w zdolność prawną, jak i zdolność do czynności prawnych. W chwili obecnej dokonywanie istotnych zmian regulacyjnych dotyczących SI, choć postulowane przez część doktryny nie jest celowe. Z jednej strony bowiem, nie da się przewidzieć kierunku rozwoju świata cyfrowego, z drugiej, wprowadzanie nowych rozwiązań prawnych naruszałoby pewność i stabilność prawa, co nie jest pożądane biorąc pod uwagę złożoności racji, interesów i wartości, które towarzyszą upowszechnianiu SI. Ponadto na dzień dzisiejszy problemy i wątpliwości powstające na tle odpowiedzialności za SI nie są nowe, choć na pewno występują w znacznie większym natężeniu. Istnieje zatem możliwość wykorzystania dotychczasowego dorobku prawnego.

Nie wydaje się, że *de lege lata* możliwe jest uznanie odrębnej „osobowości" systemu sztucznej inteligencji. Kłóciłoby się to, między innymi, z istotą odpowiedzialności cywilnej, w szczególności opartej na zasadzie winy. Przecież, aby zastosowanie miał art. 415 k.c. konieczne jest nie tylko działanie sprzeczne z prawem, ale także wykazanie subiektywnego elementu winy, a więc takiej nieprawidłowości w postępowaniu, z powodu której można komuś postawić zarzut. Tymczasem trudno sobie, przynajmniej obecnie, wyobrazić, jakieś psychologiczne „nastawienie" systemu do czynu, nie wiadomo, w jaki sposób ocenić choćby umyślność czy nieumyślność działania. Poza tym nie byłoby jasne, w jaki sposób zbudować wzorzec należytej staranności przewidziany w art 355 k.c. Skoro mówimy o pewnym systemie kodów czy algorytmach, wprawdzie uczących się, ale wszak – przynajmniej na początku – kontrolowanych

przez człowieka, koncepcja odrębnego bytu AI w sensie prawnym, traci sens w świetle cywilnoprawnych reguł odpowiedzialności odszkodowawczej[651].

W naszym porządku prawnym rozwiązanie oparte na podmiotowości prawnej SI nie będzie możliwe także ze względu na definicje pojęć zdolności prawnej i zdolności do czynności prawnej.

Na obecnym etapie rozwoju sztucznej inteligencji, zakładając, że tzw. mocna inteligencja pozostaje na razie w sferze teorii – nie ma ona ani własnej woli, ani własnego interesu. Zarówno za jednym, jak i drugim stoi pierwotnie wpisany algorytm, programowanie wbudowane przez twórcę maszyny. Jakbyśmy nie byli pod wrażeniem jej mocy obliczeniowych, szybkości reakcji, trafności decyzji, są to jedynie wyniki niezwykle zaawansowanego technologicznie systemu informatycznego. Jak twierdzi M. Uliasz „stanowi ona przedmiot a nie podmiot. Jest wytworzona przez człowieka pośrednio lub bezpośrednio, aby służyć człowiekowi jako narzędzie w celu ułatwiania i wspomagania jego aktywności"[652].

Twórcy Polityki Rozwoju Sztucznej Inteligencji w Polsce na lata 2019–2027 przygotowanej przez Ministerstwo Cyfryzacji wyraźnie podkreślają znaczenie koncepcji sztucznej inteligencji zorientowanej na człowieka i jego środowisko (*Human Centric Approach*), której celem jest dążenie do tego, aby wartości ludzkie były kluczowe dla sposobu, w jaki systemy sztucznej inteligencji są opracowywane, wdrażane, wykorzystywane i monitorowane. Polska stoi na stanowisku i popiera kraje, które odmawiają nadania systemom sztucznej inteligencji statusu obywatelstwa lub osobowości prawnej. Koncepcja osobowości prawnej SI według Polityki Rozwoju Sztucznej Inteligencji w Polsce jest sprzeczna z wyżej wskazaną ideą koncepcji sztucznej inteligencji zorientowanej na człowieka. Polska opowiada się za koncepcją supremacji człowieka nad systemami SI. Jak wyraźnie zostało podkreślone w Załączniku nr 3 Polityki Rozwoju Sztucznej Inteligencji w Polsce, należy przeciwstawić się działaniom zmierzającym do nadania osobowości prawnej sztucznej inteligencji[653].

Taki stan faktyczny rozwoju technologicznego SI pozostawia aktualnie poza obszarem analizy koncepcje przyznania SI podmiotowości prawnej, które dyskutowane są na literaturze przedmiotu i dotyczą np. konstrukcji, zgodnie z którą szatą dla osobowości prawnej SI byłoby prawo spółek alternatywnie dla nowej kategorii osób, czyli alternatywnie dla innej koncepcji, tzw. elektronicznej osoby prawnej.

---

[651] . Wachowska, *Odpowiedzialność za sztuczną inteligencję* [w:] *Prawo sztucznej inteligencji*... red. L.Lai, M. Świerczyński.

[652] M. Uliasz, *Sztuczna inteligencja jako sztuczna osoba prawna* [w:] *Sztuczna inteligencja, blockchain...*, pod red. K. Flagi-Gieruszyńskiej, J. Gołaczyńskiego, D. Szostka, s. 31.

[653] Polityka Rozwoju Sztucznej Inteligencji w Polsce na lata 2019–2027.

Poza tematem podmiotowości prawnej podnieść należy, że w dyskusji dotyczącej SI sygnalizowane są także inne rodzaje zagadnień problemowych łączących się z tematem odpowiedzialności. Podstawowym z nich jest zakresem takiej odpowiedzialności, tj. pytania o to jak ustalić granicę pomiędzy tymi systemami, które mają zdolność działania w danym zakresie, i tymi które nie mają. W ramach prowadzonych w tym obszarze rozważań pojawia się postulat, że być może rozwiązaniem dla tego problemu jest właściwe rozłożenie ciężaru dowodu. Wraz ze wzrastającą wszechstronnością robotów (systemów) można by przejść od ciężaru dowodu, że robot (system) powinien był działać, spoczywającego na osobie formułującej roszczenia, do ciężaru dowodu, że robot (system) nie musiał działać, spoczywającego na podmiocie odpowiedzialnym za robota (system). Wtedy pozostają do rozwiązania jeszcze inne problemy, tj. czy robot (system) ma obowiązek reagować na ryzyko skrzywdzenia każdej osoby bez względu na jej położenie i prawa, jakie ma ona w stosunku do robota (systemu) itd.?

Kolejne pytanie to, czy katalog takich osób należałoby przy użyciu jakiegoś kryterium ograniczyć, a jeśli tak, to według jakiego (bliskość w przestrzeni czy pod względem stosunków o charakterze prawnym, czy może wg kryterium wieku itd. Inna kwestia do rozważenia to, czy odpowiedzialność ta powinna być analogiczna do dotychczas funkcjonującej odpowiedzialności na zasadach ogólnych za szkodę majątkową i niemajątkową, odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny, odpowiedzialności za szkodę wyrządzoną przez zwierzęta, odpowiedzialności za szkodę spowodowaną przez mechaniczny środek. komunikacji poruszany za pomocą sił przyrody.

Zdaniem P. Księżaka i S. Wojtczak odpowiedzialność taka powinna być nieograniczona w czasie i przechodzić na kolejne podmioty sprawujące nadzór nad robotem (systemem) albo być współdzielona na rożnych zasadach (solidarna odpowiedzialność producenta i użytkownika, gwarancyjna odpowiedzialność zakładu ubezpieczeń, pomocnicza odpowiedzialność funduszu gwarancyjnego, serwisanta, operatora lub właściciela). Jeszcze inny obszar wątpliwości dotyczy samego pojęcia szkody. Zdaniem wspomnianych Autorów szkoda ta może obejmować zarówno dobra osobiste człowieka, jak i jego majątek – w tym oczywiście również inne roboty. Przesłanki tej odpowiedzialności zapewne (tak jak w wypadku szkód wyrządzonych przez produkt niebezpieczny, ruch przedsiębiorstwa czy pojazdów mechanicznych) muszą abstrahować od elementów subiektywnych (tj. winy), choć ze względu na autonomiczność robota (zwłaszcza sterowanego przez silną AI) nie jest to kwestia oczywista. Nie ma powodów, by w zakresie odpowiedzialności za szkody wyrządzone przez robota (systemy) przyjmować *a priori* absolutną odpowiedzialność niezależną od takich

okoliczności jak wina, czy przyczynienie się poszkodowanego. Na gruncie prawa w ogóle pojęcie winy (podobnie jak pojęcie związku przyczynowego) i tak będzie prawdopodobnie wymagało przemyślenia, w miarę jak w życiu społecznym i obrocie prawnym coraz częściej i w coraz większym zakresie będą uczestniczyć roboty.

Kolejnym problemem jest odpowiedzialność cywilna za nienależyte wykonanie zobowiązania lub z tytułu rękojmi czy gwarancji. W przypadku zachowania robota polegającego wyłącznie na niewykonaniu polecenia człowieka (przy niewystąpieniu szkody) trudno znaleźć uzasadnienie dla jakichś innych reżimów odpowiedzialności, ale przedmiotem dyskusji może stać się to, czy taka odpowiedzialność powinna być ograniczona w czasie, ewentualnie jak długo powinna trwać[654].

Z punktu widzenia odpowiedzialności cywilnej w literaturze podnoszone jest także to, czy człowiek będzie miał obowiązek wspomagać się SI, jeśli zapewni to wyższy standard działania. Jako przykład ilustrujący to zagadnienie podawany jest lekarz, który jest krótkowidzem: dla każdego jest oczywiste, że powinien nosić okulary albo szkła kontaktowe. W takim przypadku standard jego należytej staranności odniesiemy do osoby dobrze widzącej, dlatego powstaje pytanie, czy tak samo odnosić to będzie trzeba do wspomagania innymi technologiami znacznie bardziej rozwiniętymi, gdy nie chodzić będzie tylko o naprawienie pewnych chorób czy niepełnosprawności i przywrócenie ich do poziomu naturalnego, ale o poprawienie zdolności leczenia? Właśnie na płaszczyźnie medycyny te problemy będą szybko i jaskrawo widoczne: jeżeli będą istniały narzędzia usprawniające pracę lekarza do poziomu nadludzkiego to spojrzenie na zagadnienie od strony pacjenta może prowadzić do wniosku, że ta nowa technologia kształtuje nowy standard, do którego – pod rygorem odpowiedzialności co najmniej cywilnej – każdy będzie musiał się dostosować[655].

RODO a SI

Tradycyjna definicja prawa do prywatności jako „prawa do nie bycia widzianym" (ang. *right not to be seen)* oscyluje wokół pojęć takich jak widoczność i pozostawanie w ukryciu. Pomimo upływu czasu nie traci ona na aktualności także w czasach technologicznego przełomu, kiedy to w centrum zainteresowania znajdują się dane, w tym dane dotyczące osób fizycznych. W ciągu ostatnich dziesięcioleci to właśnie dane stały się najcenniejszym zasobem napędzającym gospodarkę. Jednak działania w zakresie wypracowania efektywnych rozwiązań

[654] P. Księżak, S. Wojtczak, *Prawa Asimova*...
[655] P. Księżak, *Prawo cyborgów. Wprowadzenie w problematykę*, „Przegląd Prawniczy Allehardа" 2021/4/2(8).

prawnych, które w sposób kompleksowy regulowałyby sposoby korzystania z nich, w tym efektywnie mitygowałyby nieskrępowaną monetyzację praktyk naruszających prawa podmiotów danych oraz zagrażających integralności społeczeństwa, przebiegają w tempie odwrotnie proporcjonalnym do prędkości rozwoju samej technologii.

Wątpliwości dotyczące przetwarzania danych z wykorzystaniem algorytmów, w tym profilowania oraz zautomatyzowanego podejmowania decyzji, budzą w szczególności kwestie związane z obserwowanymi w ostatnich latach niepokojącymi zjawiskami, takimi jak: powszechność funkcjonowania i trudności w weryfikacji tzw. skrzywień algorytmicznych (ang. *algorithmic bias*), Wnioski wyciągane na podstawie zautomatyzowanej analizy dużych zbiorów danych mogą okazać się bardzo zaskakujące także dla samych podmiotów danych, jako że mogą one ujawniać informacje (w tym predykcje) dotyczące jednostek, co do których one same nie miały wiedzy. Co więcej, może okazać się, że wnioskowanie zostało przeprowadzone błędnie, a informacje uzyskane na jego podstawie są nieprawdziwe. Z uwagi na brak przejrzystości w zakresie przetwarzania danych, w tym zastosowania algorytmów, podmioty te często pozostają nieświadome istnienia tych wypaczeń i wywieranych przez nie skutków, albo mając już ich świadomość, nie mają możliwości skorzystania z rzetelnej procedury ich weryfikacji (tzw. *algorithmic due process)* i co za tym idzie – pozbawione są możliwości kontestowania rezultatów operacji przeprowadzanych z wykorzystaniem dotyczących ich danych, nawet jeśli wnioskowanie jest obiektywnie błędne, dyskryminujące czy też w inny sposób narusza ich prawa.

Jednym z głównych celów RODO było zaadresowanie problemów opisanych powyżej, co miało doprowadzić do umocnienia autonomii podmiotów danych. Intencją legislatorów było stworzenie nowych ram ochrony danych osobowych osób fizycznych, które poprzez wprowadzenie nowych uprawnień oraz środków ochrony podmiotów danych dawałyby nadzieję na stawienie efektywnego oporu naciskom ze strony ekspansywnie rozwijającej się technologii[656].

W kontekście technologicznym dla SI podstawową konsekwencją konieczności zastosowania RODO jest zapewnienie legalności przetwarzania danych, czyli zachowanie przede wszystkim wynikających z RODO podstaw prawnych przetwarzania danych osobowych oraz realizacja prawa do podlegania decyzji podjętej w sposób niezautomatyzowany. Możliwość wyrażenia sprzeciwu wobec decyzji podjętych w sposób automatyczny podobnie jak implementacja odpowiednich reguł etycznych to priorytety, które powinny być

[656] K. Alama-Maruta, *Algorytmiczne przetwarzanie danych na gruncie RODO – uwagi krytyczne oraz kierunki działań w celu poprawy standardów przetwarzania danych oraz ochrony prywatności*, MoP 2020/20.

przestrzegane na każdym etapie wykorzystania SI tj. przez projektantów, deweloperów, podmioty wdrażające oraz podmioty posługujące się sztuczną inteligencją. Zbiory danych przetwarzanych w systemach SI, zwłaszcza te zawierające szczególne kategorie danych osobowych, powodują, że posiadanie tak różnorodnej wiedzy na temat konkretnego podmiotu danych może powodować, iż mogą one być wykorzystywane nie tylko do tego, by np. systemy bankowe oceniały jego zdolność kredytową, ale również do tego, żeby kreować jego wybory czy też podejmowane decyzje.[657] W procesie projektowania rozwiązań z wykorzystaniem SI określenie celu przetwarzania danych powinno nastąpić w takiej formie, aby wykluczyć takie przypadki, gdy jego zmiana wpływa na prawa i obowiązki osób, których dane dotyczą. Konieczne w tym zakresie jest działanie polegające na zminimalizowaniu ryzyka stronniczości czy dyskryminacji lub błędów w systemach SI.

Głównym zagrożeniem sztucznej inteligencji dla realizacji RODO może być trudność w zrozumieniu mechanizmów jej działania, dlatego znaczna część prac podejmowanych przy projektowaniu rozwiązań z wykorzystaniem SI powinna polegać na wyjaśnieniu mechanizmów jej działania. Bez wyjaśnienia zasad działania algorytmów nie będzie możliwe spełnienie poprawnie obowiązków prawnych. Jeżeli wyjaśnienie zasad działania sztucznej inteligencji będzie prowadziło do wskazania na jakich danych oparta została sztuczna inteligencja jakie dane przetworzyła i jaką decyzje na ich podstawie podjęła będziemy wiedzieć czy jej działanie spełnia warunki legalności

Kwestia danych osobowych w systemach wykorzystujących SI jest i będzie jeszcze przez dłuższy czas kontrowersyjna z uwagi projektowane rozwiązania dotyczące podmiotowości SI oraz zasad odpowiedzialności i istniejące już wymagania prawne, które należy stosować do danych, w tym danych osobowych. Brak jasnego podziału obowiązków podmiotów biorących udział w tworzeniu i korzystaniu z systemów SI oraz trwająca dyskusja nad koncepcją podmiotowości prawnej SI komplikuje stosowanie przepisów RODO.

Obecnie wydaje się, że na każdym etapie działania SI zgodność z przepisami RODO dotyczyć powinna przede wszystkim wykonania obowiązków zapewnienia legalności danych oraz zastosowania zasad rozliczalności danych zwłaszcza w zakresie ograniczenia przechowywania danych, czyli retencji tych danych oraz ich minimalizacji. Ma to znaczenie z uwagi na fakt, że w przypadku automatycznego podejmowania decyzji, osobie, której dane dotyczą, przysługuje prawo wyrażenia sprzeciwu, które technicznie trzeba będzie wykonać.

[657] M. Jakubik, T. Świętnicki, *RODO* [w:] *IT: sztuczna inteligencja a dane osobowe – czy RODO definiuje AI oraz ML?*, LEX 2020.

Projektowanie systemów SI musi uwzględniać także realizację innych praw osób, których dane dotyczą, takich jak np. prawo do sprostowania, uzupełnienia czy dostępu do danych.

Działania w obszarze SI wynikające z RODO powinny zatem dotyczyć przekazania osobom, których dane dotyczą, informacji o automatycznym podejmowaniu decyzji, w tym właśnie o profilowaniu, oraz informacji o zasadach ich podejmowania, jednocześnie zaznaczając konsekwencje tego przetwarzania dla osoby, której dane dotyczą, zgodnie z art. 13 lub 14 RODO, w zależności od kogo pochodzą dane osobowe. W pewnych sytuacjach osoba, której dane są przetwarzane, ma prawo do tego, aby w ogóle nie podlegać decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu danych, w tym na profilowaniu, a wtedy administrator danych musi szukać podstawy, aby mimo wszystko taką decyzję zastosować, np. będzie musiał wykazać, że jest to niezbędne do wykonania umowy zawartej pomiędzy administratorem danych a osobą, której dane dotyczą, oraz szukać pozwolenia na takie działanie w przepisach prawa czy też pobrać od osoby, której dane przetwarza, wyraźną zgodę, na której będzie opierać się decyzja[658].

Systemy wykorzystujące działania SI powinny zatem zostać tak zaprojektowane, aby zmiana podstawy prawnej przetwarzania danych mogła być nie tylko odnotowana, ale żeby mogła być weryfikowalna także w późniejszym dowolnym terminie.

Obecnie z perspektywy konstrukcji mechanizmów opartych na sztucznej inteligencji kluczowe będzie zapewnienie zgodności z zasadami przetwarzania, które wyznaczają ogólne ramy dopuszczalności wykorzystywania danych zawarte w art. 5 RODO, zasadzie rzetelności, celowości, proporcjonalności przetwarzania danych, *privacy by design* i *privacy by default*, rozliczalności, przejrzystości, bezpieczeństwa danych i zarządzania ryzykiem. W sytuacji gdy do porządku prawnego wejdą projektowane rozwiązania w zakresie odpowiedzialności w/w zasady zostaną uzupełnione o nowe obowiązki[659].

Pomimo że przepisy ogólnego rozporządzenia o ochronie danych nie odnoszą się wprost do systemów sztucznej inteligencji, to jak najbardziej znajdują one zastosowanie do tych systemów, o ile w ich ramach przetwarzane są dane osobowe. RODO jest tym obszarem prawa, którego zastosowanie w przypadku SI jest wyzwaniem praktycznym. Obowiązki wynikające z RODO dotyczą wszystkich podmiotów biorących udział w technologii SI, poczynając od etapu jej tworzenia, poprzez korzystanie i dalsze doskonalenie, niezależnie od statusu jaki tym podmiotom przysługuje na gruncie RODO, tj. niezależnie od tego czy są administratorem, czy podmiotem przetwarzającym. Wskazać tu należy choćby na obowiązki

[658] M. Jakubik, T. Świętnicki, *RODO* [w:] *IT: sztuczna inteligencja...*
[659] D. Lubasz W. Chomiczewski, *Privacy by Design a sztuczna inteligencja*, MoP 2020/20.

wynikające z art. 24, 25 i 32 RODO. Wszystkie one zakładają dokonanie analizy ryzyka naruszenia praw i wolności osoby fizycznej związane z przetwarzaniem danych osobowych, z uwzględnieniem charakteru, zakresu, kontekstu i celu przetwarzania danych osobowych, a następnie wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Wśród środków tych muszą znaleźć się odpowiednie polityki ochrony danych osobowych, zabezpieczenia informatyczne i fizyczne, dokumentacja techniczna i organizacyjna, a więc standardy, które pozwolą zabezpieczyć dane osobowe i wykazać to zabezpieczenie.

Istotną cechą systemów SI, w tym tych opartych na uczeniu się maszyn, jest to, że wykorzystują one bardzo duże ilości danych. Dane wykorzystywane są w procesie tworzenia modelu – aby system dobrze nauczył się wykonywać jakieś zadanie (np. rozpoznawać twarze), musi zdobyć doświadczenie, czyli przeanalizować bardzo wiele danych (w przypadku rozpoznawania twarzy – obrazów). W zależności od tego, jakie zadanie system SI ma wykonywać, w procesie szkolenia mogą być wykorzystywane dane osobowe (np. jeśli system ma służyć do rozpoznawania twarzy lub do analizy CV pod kątem przydatności kandydata do pracy). Zatem z punktu widzenia prawa ochrony danych osobowych istotne jest nie tylko tworzenie nowych danych o osobach fizycznych lub podejmowanie decyzji przez system SI wobec osób fizycznych (tj. wynik działania systemu SI), ale także proces szkolenia i testowania systemu, ponieważ na tym etapie także mogą być przetwarzane dane osobowe[660].

RODO – jako regulacja neutralna technologicznie – nie odnosi się wprost do systemów SI, dlatego głównym problemem w realizacji RODO pozostaje trudność w zrozumieniu mechanizmów działania SI oraz występowanie błędów, wynikających z wadliwych danych dostarczonych programowi na etapie jego konstruowania i uczenia się.

Pierwszy ze wskazanych powyżej problemów ma wpływ na przede wszystkim na realizację obowiązków informacyjnych oraz na stosowanie mechanizmu profilowania. Art. 13 ust. 2 lit. f oraz 14 ust. 2 lit. g RODO wymaga, by administrator przekazał osobie, której dane dotyczą, m.in. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Błędy wynikające z wadliwych danych mogą powodować problem dyskryminacji przy automatycznym przetwarzaniu danych. Motyw 71 preambuły RODO stanowi m.in., że:

[660] K. Syska, *Ocena odpowiedniości przepisów RODO do zapewnienia przejrzystości działania systemów AI – wybrane zagadnienia*, MoP 2020/23.

„Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji – mogącej obejmować określone środki – która ocenia jej czynniki osobowe, opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa, jak na przykład automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej. Do takiego przetwarzania zalicza się «profilowanie», które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji".

Motyw 60 RODO stanowi natomiast, że udzielanie informacji o profilowaniu jest częścią obowiązków administratora dotyczących przejrzystości na mocy art. 5 ust. 1 lit. a. Osoba, której dane dotyczą, ma prawo do uzyskania informacji od administratora na temat profilowania a w pewnych okolicznościach także prawo do sprzeciwu wobec „profilowaniu", niezależnie od tego, czy ma miejsce wyłącznie zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach na podstawie profilowania[661].

Systemy SI często dokonują szczegółowego profilowania osób fizycznych, identyfikując preferencje, cechy charakteru, czy inne informacje na temat tych osób. Osoby, których dane dotyczą, mogą nie mieć świadomości tego, jak szczegółowe, lub jak bardzo ingerujące w prywatność jest takie profilowanie. Poza tym systemy SI mogą tworzyć nowe kategorie informacji o osobach, których dane dotyczą – różnego rodzaju prognozy co do tych osób, ich przewidywane preferencje, zdolności, zainteresowania, informacje o sytuacji życiowej, itp. Jeżeli osoba nie ma świadomości, że takie informacje jej dotyczące są tworzone i wykorzystywane przez systemy SI, to nie ma nad takim przetwarzaniem kontroli. Jeśli osoby, których dane dotyczą, dysponowałyby informacjami o tym, jakiego rodzaju informacje o nich są przetwarzane przez system SI i czego dotyczą decyzje tego systemu takie jak prognozy,

[661] Grupa Robocza Art. 29: wytyczne 251 dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania dla celów rozporządzenia 2016/679.

rekomendacje lub klasyfikacje to osoby te zyskałyby większą kontrolę nad swoimi danymi. Dzięki większej świadomości osoby, których dane dotyczą, mogłyby także korzystać ze swoich praw, np. sprzeciwu wobec przetwarzania ich danych. Ponadto, jeśli osoby, których dotyczą decyzje podejmowane przez systemy SI lub przy wsparciu tych systemów SI, otrzymywałyby wyjaśnienia powodów tych decyzji, to mogłyby skuteczniej kwestionować takie decyzje lub miałyby większe szanse na kontrolowanie, czy nie dochodzi do dyskryminacji[662].

W tym miejscu trzeba postawić tezę, że prace podejmowane przy projektowaniu rozwiązań z wykorzystaniem SI powinny polegać przede wszystkim na wyjaśnieniu mechanizmów jej działania. Oczywiście wyjaśnienie, dlaczego SI podejmuje określoną decyzję, może być trudne, a nawet niemożliwe, chociażby z uwagi na to, że projektanci SI, aby zdobyć przewagę konkurencyjną, budują własne sieci, według własnych, autorskich koncepcji, które zachowują w tajemnicy. Bez wyjaśnienia jednak zasad działania algorytmów nie będzie możliwe spełnienie poprawnie obowiązków prawnych. Jeżeli wyjaśnienie zasad działania sztucznej inteligencji będzie prowadziło do wskazania na jakich danych oparta została sztuczna inteligencja jakie dane przetworzyła i jaką decyzje na ich podstawie podjęła będziemy wiedzieć czy jej działanie spełnia warunki legalności.

W związku z tak postawioną tezą należy rozważyć, jakie obowiązki dotyczące informowania o zautomatyzowanym podejmowaniu decyzji oraz kwestii wyjaśniania decyzji podejmowanych w sposób całkowicie zautomatyzowany wynikają z przepisów RODO i jak te obowiązki mogą być zastosowane do systemów SI.

Przepisy RODO przewidują szczególne obowiązki – także w zakresie przejrzystości – dotyczące decyzji podejmowanych w sposób całkowicie zautomatyzowany, jeśli takie decyzje wywołują wobec osób fizycznych skutki prawne lub w podobny sposób istotnie na nie wpływają (art. 22 ust. 1 RODO). Nawet jeśli proces podejmowania decyzji nie ma wpływu na prawa osób, może on nadal wchodzić w zakres art. 22, jeżeli wywoła skutek równoważny lub w podobny sposób znaczący. Innymi słowy nawet w przypadku braku zmian w prawach lub obowiązkach, wpływ na osobę, której dane dotyczą, mógłby w dalszym ciągu być wystarczająco duży, aby wymagała ona ochrony na podstawie tego przepisu.

Dlatego w RODO pojawia się fraza „w podobny sposób" do wyrażenia „istotnie wpływa", co oznacza, że próg istotności musi być podobny do progu decyzji wywołującej skutek prawny[663]. Jeśli chodzi o kryterium wywoływania skutków prawnych, to wskazuje się tu przykładowo na skutki w postaci rozwiązania umowy, udzielenia lub odmowy udzielenia określonego

[662] K. Syska, *Ocena odpowiedniości*..
[663] Grupa robocza Art. 29: wytyczne 251...

świadczenia społecznego, odmowy wjazdu na terytorium danego państwa. Jeśli chodzi o kryterium podobnego istotnego wpływu na osoby, których decyzje dotyczą, organy nadzorcze wskazują na decyzje, które wywierają wpływ na sytuację finansową, stan zdrowia i możliwość korzystania ze świadczeń zdrowotnych, szanse na zatrudnienie, dostęp do kształcenia, czy też zachowanie się osoby. Natomiast jako przykład wpływu nieistotnego podaje się rekomendowanie przez system programów telewizyjnych na podstawie nawyków widza[664].

Należy zatem już na tym etapie podkreślić, że szczególne obowiązki wynikające z RODO dotyczące zautomatyzowanych decyzji nie dotyczą wszystkich zautomatyzowanych decyzji, ale tylko takich decyzji, które są podejmowane w sposób całkowicie zautomatyzowany, oraz które jednocześnie wywołują skutki prawne lub inny istotny wpływ na osobę, której dane dotyczą. W związku z tym decyzje podejmowane przez systemy SI będą podlegały pod szczególne przepisy RODO, tylko jeśli system SI będzie podejmował takie decyzje autonomicznie (bez udziału człowieka) i decyzje te będą wywoływały skutki prawne lub w podobny sposób istotnie wpływały na osoby, których dane dotyczą.

W zakresie obowiązków informacyjnych zastosowanie w tym przypadku będzie miał cytowany wcześniej art. 13 ust. 2 lit. f oraz 14 ust. 2 lit. g RODO, które stanowią, że administrator danych ma obowiązek przekazać osobie, której dane dotyczą, informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W katalogu informacji zawartych w w/w przepisach nie ma wyjaśnienia powodów podjęcia konkretnej decyzji przez system SI, o takim prawie jest mowa tylko w motywie art. 71 RODO jako o prawie do uzyskania wyjaśnienia co do decyzji podjętej w sposób zautomatyzowany. Ta różnica jest powodem wątpliwości interpretacyjnych co do tego, czy w RODO przewidziane jest prawo do uzyskania wyjaśnienia powodów podjęcia konkretnej decyzji w sposób zautomatyzowany (np. przez system SI). Wątpliwości w tym zakresie są przedmiotem rozważań m.in. organów nadzoru, co stanowi o istotności problemu zakresu obowiązku informacyjnego, którego wykonanie trzeba pogodzić z innymi przepisami, w szczególności dotyczącymi ochrony prawno-autorskiej systemu SI[665].

Sposób wykonania takiego obowiązku prawnego będzie budził kontrowersje, dlatego na tym etapie za dobrą praktykę w tym względzie poczytać można działania podjęte w ostatnim

[664] K. Syska, *Ocena odpowiedniości*...
[665] K. Syska, *Ocena odpowiedniości*...

czasie przez podmioty doradcze takie jak Grupa robocza Art. 29 RODO, która po wielu miesiącach różnych interpretacji wskazała, nie wdając się w analizę technologiczną, że w zakresie profilowania w sieci przez tzw. ciasteczka[666] obowiązek uzyskania zgody dotyczy ciasteczek wykorzystywanych w celu:

- śledzenia aktywności użytkowników przez wtyczki portali społecznościowych (tzw. *social plug-in tracking cookies*),
- dostarczania reklamy behawioralnej przez osoby trzecie (m.in. pozwalające na regulowanie częstotliwości wysyłanych reklam, dokumentowanie odsłon, wykrywanie tzw. „nieuczciwych kliknięć", generowanych przez boty),
- dostarczania informacji statystycznych pozwalających m.in. na pomiar oglądalności stron,
- monitorowania przez pracodawców wykorzystania Internetu przez pracowników do celów prywatnych.

Kończąc omawianie problematyki RODO w systemach SI stwierdzić należy, że z RODO nie wynika wprost wymóg przedstawiania wyjaśnienia podstaw (powodów) konkretnej decyzji podjętej w sposób całkowicie zautomatyzowany (przez system SI). Istotnym argumentem jest to, że takie uprawnienie nie wynika z przepisów RODO, a tylko z motywu, który nie ma mocy obowiązującej.

RODO nie zapewnia zatem wystarczającej ochrony przed zagrożeniami wynikającymi ze stosowania systemów SI. Być może w przyszłości w związku z wprowadzeniem regulacji prawnych dotyczących systemów SI nastąpi modyfikacja obowiązków informacyjnych w kierunku każdej zautomatyzowanej decyzji, a w ich zakres będzie wchodzić wyjaśnienie przyczyn jej podjęcia.

Obecnie w piśmiennictwie formułowane są stanowiska, które sceptycznie oceniają dotychczasowe regulacje. Zdaniem K. Alama-Maruty skuteczność instrumentów prawnych

[666] „Cookies" nie jest potocznym określeniem, ani skrótem jakiejś wieloczłonowej technicznej nazwy protokołu sieciowego. Taką nazwę nadał „ciasteczkom" w 1994 r. ich pomysłodawca Lou Montulli, zatrudniony jako programista w Netscape Communications. Dopiero na potrzeby zgłoszenia patentowego stworzone zostało określenie „HTTP State Management Mechanism" (tłum. „Mechanizm HTTP Zarządzania Statusem"). Patent na to rozwiązanie został zarejestrowany pod numerem US5774670A, zaś prawa z rejestracji obowiązywały do 2015 r[666]. Od tego czasu rozwiązanie to znajduje się w domenie publicznej i może być wykorzystywane swobodnie przez każdego. W dużym uproszczeniu, pliki cookies to bardzo małe pliki tekstowe, zapisywane na komputerze użytkownika przez przeglądarkę internetową w trakcie sesji surfowania w Sieci. Zawierają one niewielką liczbę danych, dzięki którym serwery internetowe mogą m.in. identyfikować użytkownika, a także śledzić jego aktywność w przeglądarce (np. kliknięcia, logowania, wpisywane dane). Proces ten odbywa się w pamięci wyszukiwarki internetowej i jest co do zasady niewidoczny dla zwykłego użytkownika.

przedstawionych w RODO, mających na celu zagwarantowanie podmiotom możliwości rzeczywistej kontroli i zarządzania danymi, które poddawane są operacjom z wykorzystaniem algorytmów ocenić należy krytycznie.

W obecnym stanie prawnym mamy do czynienia z sytuacją, w której nawet jeśli podmioty danych są świadome swoich zagwarantowanych w rozporządzeniu praw (co swoją drogą nadal nie stanowi sytuacji powszechnej) oraz dążą do ich egzekwowania, nadal natykają się na problemy, które utrudniają lub wręcz uniemożliwiają ich dochodzenie. Wśród nich wskazać można m.in.:

1. ukrywanie pełnego zakresu oraz konsekwencji algorytmicznego przetwarzania danych przez administratorów, którzy często próbują uniknąć wypełniania obowiązków związanych z zasadą przejrzystości i rzetelności przetwarzania, oraz uchylają się przed dostarczaniem podmiotom informacji dotyczących profilowania i algorytmicznego przetwarzania danych w możliwie najskuteczniejszy sposób. W ocenie wspomnianej wyżej Autorki, administratorzy nadal mają możliwość wykorzystywania nieświadomości podmiotów z powodu braku wystarczająco precyzyjnie sformułowanych obowiązków w zakresie sposobu dostarczania informacji dotyczących algorytmicznego przetwarzania danych zarówno przed jego rozpoczęciem, jak i w trakcie jego trwania, które dawałyby gwarancję skutecznego dotarcia takich informacji do świadomości odbiorcy;
2. powszechność wykorzystywania zgody jako podstawy algorytmicznego przetwarzania danych, połączoną z brakiem przestrzegania wymagań prawnych dotyczących jej skuteczności;
3. brak precyzyjnego sformułowania wymagań w zakresie treści wyjaśnień decyzji dostarczanych na żądanie podmiotów danych, które dostarczałyby istotnych dla podmiotu informacji w zakresie konkretnych operacji i co za tym idzie, gwarantowałyby możliwość ewentualnego skutecznego kontestowania decyzji;
4. utrudnienie możliwości skutecznego podważania decyzji z powodu braku obowiązku włączenia neutralnego arbitra do procesu jej weryfikacji. Zgodnie z wytycznymi WP251rev.01, procedura ta może zostać przeprowadzona wewnętrznie przez organizację, która podjęła określoną decyzję.

Powstaje zatem uzasadniona wątpliwość co do rzetelności takiej procedury, dodatkowo demotywując podmioty danych do skorzystania z niej[667].

[667] K. Alama-Maruta, *Algorytmiczne przetwarzanie danych na gruncie RODO – uwagi krytyczne oraz kierunki działań w celu poprawy standardów przetwarzania danych oraz ochrony prywatności*, MoP 2020/20.

Koncepcje odpowiedzialności za SI na gruncie Kodeksu cywilnego

Najważniejszym problemem prawnym związanym z rozwojem SI jest zagadnienie odpowiedzialności za szkody, które mogą powstać w związku z jej działalnością. Systemy SI, nie tylko te zaawansowane, generują ryzyko wyrządzenia szkody, polegające na tym, że system się pomyli lub nie podejmie prawidłowej decyzji, dlatego pojawia się zatem pytanie kto i na jakich zasadach powinien odpowiadać. W wypadku działania autonomicznego pojawiają się problemy, których nie można rozwiązać wprost przy zastosowaniu dotychczasowych regulacji, ale jak to zostało wskazane na wstępie aktualnie jesteśmy na etapie automatyzacji nie autonomiczności SI.

Trudno mówić tym samym, że SI mogłaby ponosić odpowiedzialność, bo jej zdolności do ponoszenia odpowiedzialności nie można oprzeć na własnej osobowości prawnej. Naturalniejszą koncepcją jest odpowiedzialność na zasadzie winy podmiotu, który wdraża rozwiązania lub wykorzystuje algorytmy w swojej działalności. Nie ma możliwości przypisania winy algorytmowi, bo nie można mówić o subiektywnym nastawieniu do czynu, ale można się zastanowić czy nie skorzystanie z narządzi SI w sytuacji łatwości ich zastosowania nie może być poczytywane jako wina. Można przyjąć koncepcję, że przedmioty, w których inkorporowane są algorytmy SI uznaje się za produkty niebezpieczne i w tym zakresie obciążyć surowszą odpowiedzialnością obiektywną producenta tego rodzaju urządzeń.

Normy odpowiedzialności cywilnej wiążą odpowiedzialność za produkt z producentem, ograniczając ją jednak do sytuacji, gdy wykazano wadliwość produktu (art. 449 ze zn. 1 § 3 k.c.). Jest to odpowiedzialność na zasadzie ryzyka, a więc co do zasady do jej zaistnienia niewymagane jest wykazanie winy po stronie podmiotu zobowiązanego (producenta). Prawodawca określił jednak przesłanki pozwalające na uchylenie się od odpowiedzialności. W szczególności producent nie odpowiada za wyrządzoną szkodę, gdy nie można było przewidzieć niebezpiecznych właściwości produktu, uwzględniając stan nauki i techniki w chwili wprowadzenia produktu do obrotu (art. 449 ze zn. 3 § 2 k.c.). Uznanie, że system SI działa wadliwie – w sposób niebezpieczny, nie odnosi się w żaden sposób do jakości jego pracy. Trudno przyjąć, aby wadliwie działał system, który doszedł do błędnych wniosków, ponieważ inne nie mogły być zbudowane na podstawie dostępnych danych. Podobnych trudności dostarcza próba oceny czy działanie badanego systemu było prawidłowe, uwzględniając stan nauki i techniki z chwili wprowadzenia produktu do obrotu.

W przypadku SI problemem może być nawet wskazanie, kiedy system został „wyprodukowany" oraz „wprowadzony do obrotu". Jak trafnie wskazuje się w literaturze,

wiązanie odpowiedzialności producenta z decyzją podjętą przez niego w chwili wprowadzenia produktu do obrotu i wyłącznie na podstawie dostępnych wówczas danych nie pozwala na odpowiednie zabezpieczenie interesów użytkowników produktów, będących już w obrocie[668]. Systemy SI powinny spełniać kryterium bezpieczeństwa nie tylko w momencie wprowadzenia do obrotu, lecz także w trakcie całego okresu eksploatacji. Producent powinien ponosić odpowiedzialność za wady technologii cyfrowych pojawiające się także po wprowadzeniu produktu do obrotu, nawet jeżeli szkoda była następstwem zmian zachodzących po wprowadzeniu produktu do obrotu, o ile wciąż sprawował kontrolę nad produktem, jego aktualizacjami lub aktualizacjami technologii, w które produkt jest wyposażony.

Dodatkowe wątpliwości wynikają z przyjętej w polskim prawodawstwie definicji produktu. Zgodnie z normą wskazaną w art. 449 ze zn. 1 § 2 k.c. za produkt uważa się rzecz ruchomą, zwierzęta oraz energię elektryczną. Powstaje problem, czy system informatyczny może zostać uznany za produkt, zwłaszcza w przypadku, gdy nie jest on zapisany na nośniku danych, a funkcjonuje w rozproszonej sieci informatycznej (takiej jak Internet). W niektórych przypadkach SI jest częścią rzeczy ruchomej (np. pojazd autonomiczny) lub do prawidłowego działania wymaga interakcji z rzeczą ruchomą (np. systemy diagnostyki medycznej). Nie jest to jednak normą i bez trudu można wskazać przypadki, gdy systemy tego typu funkcjonują wyłącznie jako usługa w sieci Internet (np. tzw. inteligentne boty, systemy analityki *Big Data* itp.). W takim przypadku agenci tego typu mogą być traktowani wyłącznie jako dobro niematerialne. To zaś z kolei prowadzi do ich wyłączenia z reżimu odpowiedzialności za produkt niebezpieczny[669].

Odpowiedzialność za sztuczną inteligencję nie powinna się zatem różnić od odpowiedzialności na zasadach ogólnych, dopóki sztuczna inteligencja działa w granicach przewidywalnego kontekstu i błędu, który może być udziałem człowieka. Jeżeli działalność SI wychodziłaby poza granice przewidywalnego kontekstu, czy błąd sztucznej inteligencji byłby takim błędem, którego człowiek by na pewno nie popełnił to wtedy inne zasady odpowiedzialności miałby swoje uzasadnienie.

Dopóki określone urządzenie jest wyłącznie narzędziem np. w rękach lekarza, zasady odpowiedzialności nie są (co do zasady) zróżnicowane w zależności od złożoności tego urządzenia. Bez względu zatem na to, czy narzędzie w rękach lekarza to zwykły stetoskop czy zaawansowany komputer, odpowiedzialność kształtuje się na zasadach ogólnych. Oczywiście złożoność systemu wspomagającego lekarza może rzutować pośrednio na tę odpowiedzialność,

[668] M. Rojszczak, *Prawne aspekty*...
[669] M. Rojszczak, *Prawne aspekty*...

np. wpływając na określenie poziomu wymaganej staranności albo na krąg osób odpowiedzialnych (bezpośrednio i regresowo), jednakże wyłaniające się na tym tle problemy nadal pozostają jakościowo takie same. Dlatego na obecnym etapie rozwoju robotów i w zakresie ich praktycznego wykorzystania co do zasady pojawiające się ewentualnie problemy można rozwiązać, stosując wprost istniejące w tym zakresie przepisy i bazując na dotychczasowym dorobku judykatury i doktryny. Jeśli zatem np. lekarz dopuści się błędu na skutek niedochowania należytej staranności w obsłudze robota albo dojdzie do wadliwego działania maszyny, które można powiązać z brakiem należytego nadzoru nad jej funkcjonowaniem przez personel odpowiedzialność będzie kształtować się według reguł ogólnych[670].

W zagadnieniu odpowiedzialności przedsiębiorcy wykorzystującego systemy SI chodzi o odpowiedzialność ponoszoną za aktywność maszyn oraz jej skutki. „Zawsze w wypadku powstania szkody spowodowanej przez maszynę, bez względu na to czy dysponuje ona SI czy nie, będziemy poszukiwać odpowiedzialności konstruktora lub osób, w których dyspozycji pozostaje robot. W sytuacji normalnego użytkowania robota w pierwszej kolejności odpowiedzialność ponosić powinien ten, kto robota wytworzył, i np. wprowadził do niego wadliwy kod"[671].

Pojawia się jednak pytanie, czy do odpowiedzialności za SI można zastosować odpowiedzialność z art. 435 k.c., zgodnie z którym prowadzący na własny rachunek przedsiębiorstwo lub zakład wprawiany w ruch za pomocą sił przyrody ponosi odpowiedzialność za szkodę na osobie lub mieniu, wyrządzoną przez ruch przedsiębiorstwa lub zakładu. System SI wchodzić może w skład przedsiębiorstwa i wówczas odpowiedzialnym byłby podmiot je prowadzący, w razie wykazania, że szkoda powstała w związku z ruchem przedsiębiorstwa.

Zdaniem M. Wałachowskiej w przypadku szkód wyrządzonych przy leczeniu koncepcja ta nie mogłaby według niektórych poglądów jednak znaleźć zastosowania - ponieważ np. podmiot leczniczy prowadzący szpital nie może być uznany za podmiot prowadzący przedsiębiorstwo w rozumieniu art. 435 k.c.[672] Zagadnienie kwalifikowania podmiotów leczniczych jako podmioty prowadzące przedsiębiorstwo w rozumieniu art. 435 k.c. wywołuje duże rozbieżności w ocenach dokonywanych przez Sądy. Na poparcie prezentowanej tezy M.

[670] P. Księżak [w:] *Organizacja systemu ochrony zdrowia. System Prawa Medycznego*, red. D. Bach-Golecka Warszawa 2020.
[671] E. Kurowska-Tober, Ł. Czynienik, M. Koniarska, *Aspekty prawne...*
[672] M. Wałachowska [w:] *Prawo sztucznej inteligencji...* red. L.Lai, M. Świerczyński.

Wałachowska powołała odnoszący się do problemtyki tego zagadnienia wyrok Sądu Najwyższego – Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z dnia 21.09.2017 r. I PK 272/16.

Doktryna i orzecznictwo wykształciły dość niejednoznaczne przesłanki kwalifikowania przedsiębiorstwa jako wprawianego w ruch za pomocą sił przyrody. Mówi się zatem o tym, że ocena musi uwzględniać „istotę działalności" oraz to, czy możliwe byłoby osiągnięcie celów zakładu bez użycia sił przyrody. W nadal przywoływanym w orzecznictwie i piśmiennictwie wyroku z 12.7.1977 r. Sąd Najwyższy wyjaśnił, że podczas ustalania zakresu stosowania art. 435 k.c. należy brać pod uwagę trzy elementy: stopień zagrożenia ze strony stosowanych urządzeń, stopień komplikacji przy przetwarzaniu energii elementarnej na pracę oraz ogólny poziom techniki. Łatwo zauważyć, że w rzeczywistości przepis art. 435 k.c. milczy na temat tak opisywanych przesłanek. Przepis powstał w czasach, gdy tylko nieliczne przedsiębiorstwa wprawiane były w ruch za pomocą sił przyrody i dotyczyło to przedsiębiorstw dużych, które stwarzały istotne niebezpieczeństwo (kopalnie, huty, fabryki). Większość przedsiębiorstw jeszcze niedawno mogła realizować swoje zadania bez użycia sił przyrody, które miały wprawdzie charakter bardzo ważny, ale jedynie wspierający, a nie warunkujący działalność.

Hipoteza przepisu jest jednak całkowicie nieadekwatna do współczesności; anachronizm przepisu staje się szczególnie widoczny w wypadku wszelkich przedsiębiorstw działających w Internecie, tych, których działalność opiera się na przetwarzaniu danych w komputerach i oczywiście tych, które wykorzystują sztuczną inteligencję. Podstawą funkcjonowania takich przedsiębiorstw jest energia elektryczna i jej wykorzystanie jest warunkiem *sine qua non* działania tego przedsiębiorstwa. Nie jest możliwe działanie wyszukiwarki Google, serwisu Facebook czy Twitter bez wykorzystania sił przyrody. W judykaturze zmierza się zatem – wbrew dosłownemu brzmieniu ustawy – do przyjęcia, że art. 435 k.c. dotyczy tylko tych przedsiębiorstw, które nie tylko są wprawiane za pomocą sił przyrody, ale też stwarzają – poprzez wykorzystanie tych sił – szczególne niebezpieczeństwo. Takie ujęcie wydaje się zrozumiałe i odpowiadające celowi przepisu, jednak zdaje się pozostawać w sprzeczności z konsekwentnie przyjmowanym poglądem, że – w razie przesądzenia, że określone przedsiębiorstwo jest wprawiane w ruch za pomocą sił przyrody, zakresem art. 435 k.c. są objęte również takie szkody, które powstały bez jakiegokolwiek związku z wykorzystaniem sił przyrody i szczególnym niebezpieczeństwem (czego akademickim przykładem jest odpowiedzialność przewoźnika kolejowego na podstawie art. 435 k.c. za skutki poślizgnięcia się pasażera na nieodśnieżonym peronie dworca kolejowego). Zarazem wiązanie działania całego przedsiębiorstwa (a nie wycinka tej działalności, jakim jest

samo zdarzenie szkodzące) ze szczególnym niebezpieczeństwem jest też dyskusyjne, bo nie wynika wcale z brzmienia ustawy i po prostu przyjmuje inny punkt wyjścia niż uczynił to ustawodawca, który odnosi się do wykorzystania sił przyrody, nie zaś do intensywności potencjalnych szkód. Co gorsza, wprowadzona dodatkowa przesłanka „szczególnego niebezpieczeństwa" jest – mówiąc oględnie – dość niejednoznaczna. W wypadku przedsiębiorstw opartych na działaniu Internetu zdefiniowanie poważnego niebezpieczeństwa szkody (w tym szkody niemajątkowej) wydaje się być bardzo trudne[673].

Powyższe rozważania można podsumować twierdzeniem, że systemy SI, którymi posługują się aktualnie ludzie, nadal są jedynie narzędziami, choć coraz bardziej zaawansowanymi, a problemy, które te rozwiązania przynoszą można nadal rozwiązywać w dotychczasowy sposób z wykorzystaniem istniejących konstrukcji prawnych[674].

[673] P. Księżak [w:] *Organizacja systemu ochrony zdrowia...*, red. D. Bach-Golecka.
[674] P. Księżak, *Zdolność prawna sztucznej inteligencji (AI)* [w:] *Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej*, red. W. Robaczyński, Łódź 2017

Podsumowanie

Obowiązki podmiotów, biorących udział w systemie ochrony danych osobowych nie są jednolite. Tak jak nie są jednolite reguły ich dokumentowania, wynikające głównie z omawianej w pracy zasady rozliczalności. Zgodnie z prezentowanymi poglądami: „odpowiedzialność" (ang. *responsibility*) i rozliczalność (ang. *accountability*) to dwie strony tego samego medalu i są istotnymi składnikami dobrego zarządzania[675], a im szczegółowiej administrator dokumentuje poszanowanie przepisów RODO, tym trudniej przypisać mu odpowiedzialność administracyjną lub cywilną[676].

Nie są jednolite także stosunki prawne, z których wynikają obowiązki, co wyklucza możliwość formułowania tezy, że ich naruszenie na gruncie RODO rodzi konsekwencje zastosowania wyłączenie jednego rodzaju odpowiedzialności. Standaryzowanie odpowiedzialności poprzez przyjęcie jednej ogólnej konstrukcji odpowiedzialności zgodnie z tym założeniem nie jest prawidłowe, mimo że dotychczasowe wypowiedzi piśmiennictwa takie założenie zdają się przyjmować jako zasadne, koncentrując argumentację wokół przesądzenia czy jest to odpowiedzialność deliktowa oparta na zasadzie ryzyka czy na zasadzie winy, o czym będzie mowa szczegółowo w dalszej części podsumowania.

Dla omawianego w pracy zagadnienia odpowiedzialności istotne znaczenie ma fakt, że w okresie sprzed RODO nasz porządek prawny nie przewidywał żadnych przepisów szczególnych, odnoszących się do cywilnoprawnej odpowiedzialności administratora danych, pomimo tego, że dyrektywa 95/46 zakładała, iż państwa członkowskie mogą wprowadzić do przepisów środek prawny ochrony danych osobowych. Taki stan rzeczy doprowadził do dyskusji nad relacją między regulacjami prawa do prywatności i prawa do ochrony danych osobowych.

Zasadnie w piśmiennictwie podnoszono, że nie każde sprzeczne z ustawą przetwarzanie danych osobowych stanowiło pod rządami starych przepisów jednocześnie naruszenie dóbr osobistych osoby, której dane są przetwarzane, a zakres pojęciowy dóbr osobistych i danych osobowych nie był tożsamy. W piśmiennictwie stosunkowo szeroko dyskutowane było zagadnienie przysługujących uprawnionym roszczeń, które to zagadnienia pozostaje aktualne obecnie. Aktualność tego problemu wynika z faktu, że także na gruncie RODO nie został wprowadzony do porządku prawnego środek ochrony prawnej, co czyni zagadnienia roszczeń

[675] Opinia 3/2010 w sprawie zasady rozliczalności (WP 173).
[676] M. Krzysztofek, *Ochrona danych...*, s. 55.

odszkodowawczych ograniczonym do art. 82 RODO i przepisów odsyłających do k.c.. To wymaga odniesienia się do tych stanowisk z perspektywy badań, dokonywanych w toku pracy.

Podsumowanie stanowisk piśmiennictwa dotyczących powyższych zagadnień i ich wpływu na badania pracy poprzedzić należy ogólnym stwierdzeniem, że przed wejściem w życie RODO możliwość naprawienia szkody spowodowanej naruszeniem reguł przetwarzania danych osobowych opierano na przepisach Kodeksu cywilnego o odpowiedzialności deliktowej. Była to konsekwencja tego, że art. 23 obowiązującej 24.05.2018 r. dyrektywy 95/46/WE zawierał ogólną regulację dotyczącą odpowiedzialności cywilnoprawnej stanowiąc, że państwa członkowskie zapewniają, iż każdej osobie, która poniosła szkodę wskutek niezgodnej z prawem operacji przetwarzania danych lub innej czynności niezgodnej z przepisami krajowymi przyjętymi zgodnie z niniejszą dyrektywą, przysługuje od administratora danych odszkodowanie za poniesioną szkodę. Polski ustawodawca nie dokonał implementacji tego przepisu w ustawie o ochronie danych osobowych, lecz przyjął, że obowiązują tu przepisy ogólne, czyli regulacje Kodeksu cywilnego o deliktach. W piśmiennictwie wskazano, że był to nieprawidłowy sposób implementacji, gdyż podstawą odpowiedzialności deliktowej w prawie polskim jest wina, a dyrektywa zakładała odpowiedzialność bez tej przesłanki. Następstwem wadliwej implementacji dyrektywy było poszukiwanie ochrony w ramach instytucji dóbr osobistych i takie rozwiązanie przyjęto w dominującej linii orzeczniczej sądów polskich na gruncie stanu prawnego, poprzedzającego rozpoczęcie stosowania RODO. Podobne rozwiązanie przyjęto także w orzecznictwie niemieckim i zaaprobowano w niemieckim piśmiennictwie prawniczym[677].

Skutkowało to tym, że ochrona danych osobowych była powiązana z dobrami osobistymi. To oznaczało, że ten, czyje dobro osobiste zostało zagrożone cudzym działaniem, mógł żądać zaniechania tego działania, chyba, że nie było ono bezprawne. W razie dokonanego naruszenia mógł on też żądać, aby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności, aby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na gruncie Kodeksu cywilnego, w przypadku szkody niemajątkowej (krzywdy), oprócz dochodzenia roszczeń majątkowych (zadośćuczynienia) możliwe było także dochodzenie roszczeń o charakterze niemajątkowym na podstawie art. 24 § 1 zdania 1–2 k.c. (niemajątkowa ochrona dóbr osobistych) – zakładając, że wystąpienie szkody niemajątkowej na gruncie Kodeksu cywilnego uzależnione było od naruszenia dobra osobistego.

[677] B. Łukańko, *Uchybienie przepisom o ochronie danych osobowych*, „Studia Prawnoustrojowe UWM" 2019.

Do omawiania problematyki zagadnienia roszczeń przysługujących podmiotom danych po wejściu w życie RODO istotna pozostaje odpowiedź na pytanie, czy obowiązujące obecnie przepisy modyfikują dotychczasowy charakter roszczeń. Poniżej zaprezentowane zostaną stanowiska piśmiennictwa w tej sprawie.

Rozporządzenie ogólne definiuje dane osobowe w art. 4 pkt 1 jako „informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej", a w katalogu otwartym wymienia ich przykłady, m.in. imię, nazwisko czy też czynniki określające fizjologiczną tożsamość osoby. Niektóre elementy tego zbioru pojawiają się także w otwartym katalogu z art. 23 polskiego k.c. jako dobra osobiste osoby fizycznej. Wynika z tego, że chociaż przedmiot obu pojęć może być identyczny, np. wizerunek czy imię i nazwisko danej osoby, o tyle nie znaczy to, że oba pojęcia są sobie tożsame i na gruncie prawa równorzędne[678]. Zarówno samo RODO, jak i projekty aktów mu towarzyszących przynoszą gruntowne (choć charakterystyczne raczej dla ewolucji niż rewolucji) zmiany w zakresie praw podmiotów przetwarzanych danych osobowych i korespondujących z nimi obowiązków podmiotów procesujących te dane[679]. Choć RODO wskazuje na prawo do odszkodowania zarówno za szkodę majątkową, jak i niemajątkową, to nie jest jasny charakter tego roszczenia. Kolejne ustępy art. 82 RODO wskazują raczej na roszczenie majątkowe (w szczególności art. 82 ust. 5 mówi o „zapłacie odszkodowania"), jednakże w doktrynie pojawiają się stanowiska, że ust. 4 tego przepisu ustanawia zasadę pełnego odszkodowania, tj. także świadczonego *in natura*, a potwierdzać ma to także motyw Nr 146 mówiący o „pełnym i skutecznym odszkodowaniu".

RODO ogranicza przyznane odszkodowanie do charakteru majątkowego roszczenia, pozbawiając podmiot danych prawa żądania np. usunięcia skutków naruszenia przepisów o ochronie danych osobowych.[680]

Inne prezentowane w piśmiennictwie poglądy wskazują, że w tym kontekście należy zwrócić uwagę na kwestie szczegółowe i specyficzne dla regulacji rozporządzenia ogólnego. Po pierwsze, dochodzenie roszczeń z powołaniem się na wystąpienie szkody niemajątkowej związane jest w obrębie przepisów o deliktach z naruszeniem (jako przesłanką) dóbr osobistych (art. 24 § 1 zdanie trzecie w związku z art. 445, 446 § 4 oraz 448 k.c.), o czym nie ma mowy w art. 82 rodo. Po drugie, należy zwrócić uwagę, że rozporządzenie ogólne nie przesądza wyraźnie charakteru roszczeń odszkodowawczych. W polskim systemie prawnym uszczerbek

[678] P. Wróbel, *Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia*, PME 2017/4.
[679] P. Wróbel, *Ogólne rozporządzenie*...
[680] P. Wróbel, *Ogólne rozporządzenie*...

o charakterze niemajątkowym może rodzić roszczenia zarówno niemajątkowe, jak i majątkowe. Artykuł 82 ust. 1 rodo wskazuje ogólnie na roszczenie odszkodowawcze i to zarówno w odniesieniu do szkody majątkowej, jak i niemajątkowej. Natomiast w art. 82 ust. 5 rodo wyraźnie odwołano się do zapłaty odszkodowania. Niemniej, w związku z zasadą pełnego odszkodowania (wyrażoną w art. 82 ust. 4 rodo) nie można wykluczyć żądania odszkodowania *in natura*. W konsekwencji możliwe byłoby ostrożne stosowanie art. 363 k.c., który w przypadku szkody majątkowej daje możliwość wyboru pomiędzy roszczeniem pieniężnym i *in natura*. Natomiast w przypadku szkody niemajątkowej (krzywdy) możliwe będzie stosowanie art. 448 k.c. w zakresie roszczeń majątkowych (zapłata odszkodowania).[681]

Kolejny pogląd wskazuje, że art. 82 RODO zawiera regulację „samodzielną", „całkowitą i wyczerpującą", mającą zastosowanie wówczas „gdy szkoda jest wynikiem naruszenia przepisów rozporządzenia" i dalszych regulacji, o których mowa w motywie 146 preambuły do RODO. „Należy traktować ją w polskim porządku prawnym jako regulację lex specialis, wyłączającą stosowanie zasad ogólnych k.c. na podstawie reguły lex specialis derogat legi generali". Podkreśla się, że od 25.05.2018 r. nie można już stosować w przypadku naruszenia regulacji o ochronie danych osobowych przepisów Kodeksu cywilnego w zakresie odpowiedzialności odszkodowawczej. Trzeba jednak podkreślić, że odpowiedzialność cywilnoprawna z tytułu naruszenia regulacji RODO i odpowiedzialność z tytułu naruszenia dobra osobistego wskutek nieprawidłowego przetwarzania danych osobowych nie są tożsame. Inny może być np. zobowiązany do naprawienia szkody. Trafnie wskazywano w orzecznictwie niemieckim, na gruncie dyrektywy 95/46/WE, iż roszczenia z tytułu naruszenia ogólnego dobra osobistego mogą występować tam, gdzie brak jest kompleksowej regulacji tyczącej odpowiedzialności cywilnoprawnej w przepisach o ochronie danych osobowych. Niewątpliwie zatem roszczenia z zakresu ochrony dóbr osobistych znajdą zastosowanie przy przetwarzaniu danych osobowych poza zakresem zastosowania RODO określonym w art. 2 ust. 2 lit a) i c) ogólnego rozporządzenia. Tyczyć to będzie np. przetwarzania danych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze, czy też przetwarzania danych osoby prawnej (motyw 14 preambuły). Tam, gdzie prawodawca (unijny) uregulował roszczenie jednostki identyczne pod względem przesłanek i skutków, co wymaga zbadania w

[681] M.Gumularz, *Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, EPS 2017/5, s. 31–36.

okolicznościach konkretnej sprawy, na stosowanie krajowych przepisów o ochronie dóbr osobistych nie będzie już miejsca[682].

Problemem, który w tym miejscu powinien być zatem postawiony jest pytanie, czy w zakresie (szkody niemajątkowej – krzywdy) możliwe jest aktualnie także skonstruowanie roszczeń niemajątkowych.

Na tak postawione pytanie M. Gumularz odpowiada, że taki mechanizm należy dopuścić też w świetle art. 82 rodo. Chociaż art. 82 nie odwołuje się do przesłanki naruszenia dobra osobistego, to jednak powstanie szkody niemajątkowej, o której mowa w tym przepisie, siłą rzeczy będzie konsekwencją naruszenia dobra osobistego. W praktyce trudno będzie wykazać, że doszło do powstania szkody niemajątkowej bez odwołania się i uzasadnienia, iż jest ona efektem ingerencji w dobra osobiste podmiotu danych. Nawet gdyby przyjąć, że konstrukcja szkody niemajątkowej na tle rozporządzenia ogólnego jest całkowicie oderwana od kwestii naruszenia dobra osobistego podmiotu danych (tj. bez konieczności wykazywania tej przesłanki), to i tak na zasadzie analogii (w interesie podmiotu danych) należałoby dopuścić możliwość skorzystania z art. 24 § 1 zdania 1–2 k.c.

Bernard Łukańko uznał, że powyższy pogląd tworzący z roszczenia z art. 82 RODO (w zakresie odpowiedzialności odszkodowawczej za szkodę niemajątkową) swoistą hybrydę z regulacją art. 24 § 1 zd. 1–2 k.c., nie wydaje się natomiast trafny także z uwagi na fakt, że krytycznie na temat uznania roszczeń określonych w art. 79 ust. 1 i art. 82 ust. 1 RODO za roszczenia z zakresu ochrony dóbr osobistych wypowiedziała się Naczelna Rada Adwokacka w opinii z dnia 26.09.2017 r. do projektu ustawy o ochronie danych osobowych i projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych przygotowanej przez P. Litwińskiego[683].

Problem formułowania roszczeń w zakresie szkody niemajątkowej wyłącznie w oparciu o RODO wydaje się być tematem, który wymaga dalszych rozważań i rozstrzygnięć sądów, których na obecnym etapie w tym zakresie nie mamy. Wszystkie krajowe orzeczenia analizowane w niniejszej pracy z perspektywy odpowiedzialności cywilnej, a jest ich jeszcze stosunkowo niewiele, nie dotyczą takich sytuacji. W każdym z nich bowiem roszczenia takie oparte zostały o podstawę prawną z Kodeksu cywilnego, Szansą na pozyskanie argumentów do

[682] P. Wróbel, *Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia*, PME 2017/4.
[683] Opinia z dnia 26.09.2017 r. do projektu ustawy o ochronie danych osobowych i projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych przygotowanej przez P. Litwińskiego; http://www.adwokatura.pl/admin/wgrane_pliki/file-20170910-opinia-ws- -ochrony-danych-mec-litwinski-mcyf-147-u-10-17-20817.pdf

dalszej dyskusji mogą być pytania prejudycjalne złożone do TSUE, które omówione zostały w pracy.

Podsumowując zagadnienia dotyczące tematu pracy, stwierdzić należy, że na żadnym etapie prowadzonych w piśmiennictwie analiz nie jest przedmiotem badań zagadnienie, dotyczące obowiązków umownych podmiotów biorących udział w systemie ochrony danych osobowych i ich konsekwencji, chociaż samo RODO takie instytucje prawa jako umowa powierzenia przetwarzania danych osobowych lub umowa o współadministrowanie reguluje swoim zakresem. To stanowiło podstawę do próby ich charakterystyki, która doprowadziła m.in. do tezy, stawianej w pracy, że odpowiedzialność za naruszenie przepisów o ochronie danych osobowych może mieć charakter zarówno odpowiedzialności kontraktowej, wynikającej z umowy, jak i wynikającej z innych zdarzeń, z którymi RODO lub ustawa łączą odpowiedzialność, co stanowi o deliktowym charakterze możliwej odpowiedzialności.

W tym zakresie zwrócić należy uwagę na poglądy, które stanowią, że art. 82 RODO nie odwołuje się – jako do przesłanki odpowiedzialności – do istniejącej już pomiędzy stronami relacji obligacyjnej, której naruszenie mogłoby stanowić źródło obowiązku naprawienia szkody (majątkowej lub niemajątkowej). Bliżej art. 82 do konstrukcji odpowiedzialności odszkodowawczej z tytułu czynów niedozwolonych. Stosownie do art. 82 rodo odpowiedzialność odszkodowawcza administratora danych lub procesora względem podmiotu danych uzależniona jest od spełnienia następujących przesłanek:

- poniesienia przez podmiot danych szkody majątkowej lub niemajątkowej,
- zdarzenia, w wyniku którego doszło do powstania szkody (przetwarzanie danych osobowych przez administratora lub procesora naruszające rozporządzenie ogólne lub akty delegowane i wykonawcze przyjęte na mocy ogólnego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące rozporządzenie),
- związku pomiędzy szkodą a naruszeniem ogólnego rozporządzenia,
- winy w naruszeniu ogólnego rozporządzenia.

Wymienione powyżej przesłanki są zbliżone do tych z art. 415 k.c., z tym że w ramach odpowiedzialności deliktowej w Kodeksie cywilnym brak, co do zasady, domniemania winy[684]. Odpowiedzialność cywilna przewidziana w art. 82 RODO ma charakter czysto odszkodowawczy, tymczasem wskazany wyżej polski akt prawny przewiduje kilka niezależnych środków ochrony, tj. żądanie zaniechania działania, usunięcia skutków, zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy na wskazany cel społeczny, a

[684] M. Gumularz, *Wpływ regulacji...*

także odszkodowania za wyrządzenie szkody majątkowej. Są to więc dwa oddzielne i niezależne reżimy odpowiedzialności deliktowej[685].

W piśmiennictwie słusznie podniesiony zostaje problem, że stosowanie przepisów o odpowiedzialności cywilnej w połączeniu z tymi dotyczącymi ochrony danych osobowych stanowi problem zarówno dla podmiotów dochodzących swoich praw, jak i w praktyce sądowej. Bez wątpienia nasili się już teraz spotykane zamienne stosowanie pojęć z obu dziedzin, a nawet łączenie skutków z odrębnych przecież gałęzi prawa. W perspektywie omawianych niedociągnięć regulacyjnych RODO, np. w aspekcie braku odpowiednich norm kolizyjnych dla prawa materialnego, jawi się kolejne istotne zagadnienie. Regulacja dotycząca ochrony dóbr osobistych w Kodeksie cywilnym jest już dobrze znana, powszechnie stosowana i przede wszystkim kompletna. Co prawda dochodzenie praw na podstawie art. 24 k.c. wiąże się z rezygnacją z pewnych, bezsprzecznie ważnych, ułatwień dla podmiotu przetwarzanych danych, takich jak np. przesunięcie ciężaru dowodu na administratora danych czy też przemienna właściwość sądów właściwych do rozpoznania sprawy, jednakże potencjalny powód zyskuje większą pewność, jak może się potoczyć jego sprawa, ponieważ zastosowane zostaną dobrze znane mechanizmy ochrony dóbr osobistych powiązane z ogólnymi przepisami dotyczącymi odpowiedzialności deliktowej[686].

W tym miejscu istotne jest zasygnalizowanie problemu praktycznego istotnego dla oceny zasadności przyjętej powyżej konstrukcji prawnej. Domniemanie winy administratora lub podmiotu przetwarzającego ma znaczenie dla rozkładu ciężaru dowodowego w okolicznościach, w których dokumentacja systemu ochrony danych osobowych nie posiada waloru ogólnodostępności, a w sektorze publicznym jawności. Takie stanowisko potwierdzają poniższe orzeczenia.

Przypadki żądania udostępnienia Polityki bezpieczeństwa na podstawie ustawy o dostępie do informacji publicznej były przedmiotem orzeczeń sądów administracyjnych. W wyroku z 8.12.2005 r. Wojewódzki Sąd Administracyjny w Warszawie[687] wskazał, że biorąc pod uwagę wymaganą przepisami prawa zawartość polityki bezpieczeństwa nie powinna być ona udostępniana publicznie. W ocenie WSA, elementy polityki bezpieczeństwa mają charakter informacji niejawnych i w związku z tym ich udostępnienie podlega ograniczeniu,

[685] P. Wróbel, Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia, PME 2017, Nr 4
[686] P. Wróbel, Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia, PME 2017, Nr 4
[687] Wyrok WSA w Warszawie z 8.12.2005 r., sygn. akt II SA/WA 1539/05, publik. LexPolonica, „Rzeczpospolita" 2005/289, s. C5.

zgodnie z art. 5 ust. 1 ustawy o dostępie do informacji publicznej. W wyroku z 26.10.2015 r.[688] w odniesieniu do innego wniosku o udostępnienie informacji publicznej Sąd uznał, że „dokument Polityka Bezpieczeństwa Systemu Informatycznego PESEL-SAD wersja (...) podlega szczególnej ochronie, jako że jego ujawnienie może mieć szkodliwy wpływ na wykonywanie zadań m.in. w zakresie właśnie bezpieczeństwa publicznego, czy wymiaru sprawiedliwości (…) nieuprawniony dostęp do żądanego dokumentu, mógłby nieść ze sobą zagrożenie dla praw i wolności obywateli, ich bowiem dane osobowe w tym systemie, którego dotyczy dokument, są przetwarzane w ramach wykonywania ustawowych zadań".

Jeśli chodzi o kwestię relacji danych/informacji żądanych we wniosku a pojęcia tzw. dokumentów wewnętrznych pismo organu (jak i odpowiedź na skargę) nie jest przekonywujące. Zdaniem sądu takie dane jak liczba zgłoszeń/incydentów, wszczętych postępowań, rejestry i analizy nie są danymi technicznymi, tylko danymi polityki bezpieczeństwa stosowanej w podmiocie publicznym, finansowanym ze środków publicznych, stanowiącymi zatem informację publiczną. W orzecznictwie przyjmuje się bowiem, że dokumenty tzw. polityki bezpieczeństwa, w tym systemów stosowanych przez organy władzy publicznej są informacjami publicznymi[689].

Wskazuje się wprawdzie, że dokumentacja o charakterze wewnętrznym bądź technicznym może nie być nośnikiem informacji publicznej (waloru takiej informacji nie mają np. informacje techniczne, dotyczące np. sposobu funkcjonowania danego narzędzia użytkowanego przez organ, informacje techniczne wskazujące na częstotliwość logowania się do danego narzędzia, czy przedstawiających okresy aktywności lub zmniejszonej aktywności w systemie teleinformatycznym organu), ale podkreśla się jednocześnie, że granica oceny tego co jest dokumentem wewnętrznym, a co informacją publiczną, chronioną przez przepisy ustawy, jest bardzo płynna[690]. Takie stanowisko wyrażane jest także obecnie, czego przykładem jest wyrok WSA w Łodzi z 12.02.2019 r.[691], w którym stwierdzone zostało, że jak podkreśla Prezes UODO, prowadzone przez administratorów i przetwarzających rejestry pozwalają im usystematyzować wykonywane czynności oraz całościowo spojrzeć na wykonywane operacje przetwarzania danych osobowych pod względem zgodności m.in. z

[688] Wyrok WSA w Warszawie z 26.10.2015 r., sygn. akt II SA/Wa 1135/15, CBOSA
[689] Por. wyroki NSA z 23.07.2014 r., I OSK 2769/13 oraz 24.01.2018 r., I OSK 323/16; CBOSA.
[690] Por. wyrok NSA z 10.01.2014 r. I OSK 2254/13, CBOSA.
[691] Wyrok WSA w Łodzi z 12.02.2019 r., sygn. akt II SAB/Łd 181/18, CBOSA

wymaganiami prawnymi[692]. Rejestry mają ponadto ułatwić organowi nadzorczemu kontrolę wszystkich procesów przetwarzania danych w organizacji.

W kontekście obowiązku określonego w art. 30 ust. 1 RODO przyjąć należy, że czynności przetwarzania to zespół powiązanych ze sobą operacji na danych, wykonywanych przez jedną lub kilka osób, które można określić w sposób zbiorczy, w związku z celem, w jakim te czynności są podejmowane. Rejestr z kolei to opis poszczególnych zespołów operacji związanych zbiorczo z realizacją określonego celu przetwarzania. Rejestr kategorii czynności stanowi natomiast krótszą formę rejestru czynności przetwarzania i w odróżnieniu od rejestru czynności nie musi zawierać celów przetwarzania, opisu kategorii osób, których dane dotyczą, kategorii danych osobowych oraz kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione. Zdaniem Sądu powyższe przepisy i rozważania potwierdzają prawidłowość stanowiska organu, według którego prowadzone rejestry czynności przetwarzania oraz rejestry kategorii czynności przetwarzania nie stanowią informacji publicznej, lecz stanowią dokument o charakterze wewnętrznym – organizacyjnym i porządkowym. Warto bowiem zaznaczyć, że założeniem ustawy o dostępie do informacji publicznej było zapewnienie w drodze dostępu do informacji publicznej społecznej kontroli nad działalnością m.in. organów administracji publicznej[693]. Cel ten winien być każdorazowo uwzględniany przy ocenie czy dana informacja ma charakter informacji publicznej. W przedmiotowej sprawie celem prowadzenia rejestrów jest, co zostało już wspomniane, usystematyzowanie wykonywanych operacji przetwarzania danych osobowych pod względem zgodności z wymaganiami prawnymi. Powyższa okoliczność przesądza o wewnętrznym i organizacyjnym charakterze wspomnianych rejestrów.

Oczywiste jest, że będące przyczyną szkody naruszenie może być następstwem okoliczności, które swoje źródło wywodzą z procedur, przyjętych przez administratora, za których prawidłowe działanie on odpowiada. Brak dostępu do tych procedur ocenę tych okoliczności istotnie utrudnia, a wręcz uniemożliwia, co powinno być brane pod uwagę w kontekście skuteczności dochodzenia roszczeń. Przyjęcie konstrukcji domniemania winy spowoduje, że ciężar udowodnienia okoliczności bezprawności naruszenia nie spoczywać będzie na podmiocie danych a przeciwnie – do administratora należeć będzie wykazanie jej braku.

Wyżej wymienione zagadnienia skłaniają komentatorów do refleksji, że nie można również wykluczyć, że ze względu na powiązanie pomiędzy kwestią ochrony dóbr osobistych

[692] Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określnego w art. 30 ust. 1 i 2 RODO, dostępne na www.uodo.gov.pl.
[693] Por. wyrok NSA z 4.08.2015 r., I OSK 1645/14, Lex nr 1770329.

a konstrukcją szkody niemajątkowej w obrębie art. 82 RODO – w praktyce stosowania tego przepisu – ukształtuje się nowe dobro osobiste związane z szerszą (niż w ramach wąsko ujętego prawa do prywatności) potrzebą ochrony danych osobowych. Padają nawet głosy, że należałoby się także zastanowić nad znowelizowaniem w tym kierunku art. 23 k.c., co w konsekwencji:

- rozwiązałoby to problem charakteru prawnego i istoty szkody niemajątkowej związanej z naruszeniem ogólnego rozporządzenia w ramach art. 82 RODO (szkoda niemajątkowa z tytułu naruszenia rozporządzenia ogólnego zostałaby wprost powiązana z naruszeniem dóbr osobistych i nim uzasadniona – jak w innych przypadkach w polskim prawie);
- przesądziłoby to możliwość szerokiego stosowania roszczeń niemajątkowych w razie naruszenia rozporządzenia ogólnego, w zakresie, w jakim nie dałoby się tego naruszenia zakwalifikować w ramach naruszenia prawa do prywatności;
- stanowiłoby to dodatkowe uzasadnienie możliwości podnoszenia roszczeń niemajątkowych poprzez stosowanie art. 82 RODO w zw. z art. 24 § 1 zdania 1–2 k.c., o czym była mowa powyżej;
- dałoby to podstawę możliwości szerszej ochrony przed naruszeniami rozporządzenia ogólnego niż wyłącznie w ramach ochrony dobra osobistego – prawa do prywatności (możliwe jest naruszenie rozporządzenia ogólnego niebędące jednocześnie naruszeniem dobra osobistego w postaci prawa do prywatności);
- mogłoby to wpłynąć nie tylko na wykładnię i stosowanie art. 82 RODO, o czym była mowa powyżej. W ten sposób możliwe byłoby nawet konstruowanie w ramach art. 24 § 1 zdania 1–2 k.c. szerokiej gamy roszczeń, np. w związku z naruszeniem prawa do uzyskania kopii danych, bez potrzeby odwoływania się do pojęcia szkody majątkowej lub niemajątkowej, lecz z uwzględnieniem roszczeń wywodzonych wprost z naruszenia dobra osobistego[694].

W doktrynie, na gruncie art. 82 RODO, trafnie unika się nawiązywania do pojęcia ochrony dóbr osobistych, a posługuje się pojęciem naruszenia dóbr niemajątkowych. Mimo tych uwag stwierdzić trzeba, że podobnie jak miało to miejsce na gruncie przepisów poprzednio obowiązujących, art. 82 RODO nie wyklucza zbiegu roszczeń wynikających z tego samego zdarzenia. Tym samym, co do zasady, aktualne pozostaje dotychczasowe stanowisko Sądu

[694] M. Gumularz, *Wpływ regulacji...*

Najwyższego uznające, że niezgodne z przepisami przetwarzanie danych osobowych może w konkretnym przypadku prowadzić do naruszenia dóbr osobistych i stosowania art. 23 i n. k.c.

Gdy naruszone zostanie jedno z dóbr osobistych, uprawnionemu przysługiwać będzie, po spełnieniu przesłanek prawa krajowego, roszczenie o zaniechanie działania, o usunięcie i złożenie oświadczenia określonej treści, a także prawo do żądania zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny. w sytuacji, gdy w okolicznościach konkretnej sprawy zdarzenie polegające na przetwarzaniu danych osobowych dokonanym niezgodnie z obowiązującymi przepisami prawa naruszy dobro osobiste, jakim jest prawo do prywatności, którego elementem jest prawo do samostanowienia informacyjnego, to uprawnionemu przysługują przewidziane w Kodeksie cywilnym roszczenia w zakresie ochrony dóbr osobistych. Stanowisko to zachowuje, co do zasady, ze względu na treść motywu 146 zd. 4 preambuły do RODO, aktualność także po wejściu w życie ogólnego rozporządzenia, które wprawdzie w sposób kompleksowy i wyczerpujący oraz bezpośrednio obowiązujący we wszystkich państwach członkowskich reguluje kwestię odpowiedzialności cywilnoprawnej za naruszenie przepisów rozporządzenia, ale zgodnie z wyrażonym w piśmiennictwie stanowiskiem nie wyklucza zbiegu roszczeń i naruszenia przez konkretne zdarzenie określonego dobra osobistego[695].

Dla zachowania kompletności podsumowania podkreślić należy, że w piśmiennictwie, jak zostało już to wskazane wcześniej, nie ma jednolitych poglądów co do zasad ponoszenia odpowiedzialności na gruncie RODO.

W ramach analizy zagadnienia zasad odpowiedzialności pojawiają się w piśmiennictwie poglądy, szeroko prezentowane już w pracy (m.in. D. Klimas, A. Błaszczyńska), i te, które wymagają w tym miejscu zaprezentowania dla kompletności rozważań. Zatem jak twierdzi R. Strugała w kontekście wykładni historycznej bardziej zasadna wydaje się być ocena co do konieczności wykluczenia odpowiedzialności administratora lub przetwarzającego na zasadzie winy. Powracając bowiem do przepisów dyrektywy 95/46/WE, przypomnieć należy, że w art. 23 ust. 2 dyrektywy – którego odzwierciedlenie w ramach przepisów rozporządzenia ogólnego o ochronie danych osobowych stanowi art. 82 – posługiwano się formułą „braku dowodu odpowiedzialności". Zdaniem K. Biczysko-Pudełko w RODO w sposób zupełnie dowolny, niczym nieuzasadniony i to w odróżnieniu od innych wersji językowych rozporządzenia, od tego typu sformułowania odstąpiono, zastępując je wzmianką o „dowodzie braku winy". Co

[695] B. Łukańko, *Uchybienie przepisom o ochronie danych osobowych*, Studia Prawnoustrojowe UWM 2019.

więcej, przytoczone w motywie 55 preambuły dyrektywy 95/46/WE przykładowe okoliczności zwalniające z odpowiedzialności odszkodowawczej (tj. siła wyższa oraz winy osoby, której dane dotyczą) pozwały przyjąć, że odpowiedzialność ta ukształtowana była na wzór tejże odpowiedzialności, którą to w polskiej terminologii prawniczej określa się mianem odpowiedzialności na zasadzie ryzyka. Wykładnia historyczna tychże przepisów każe postawić wniosek, że intencją ustawodawcy unijnego nie było wprowadzenie zmian w zasadach odpowiedzialności odszkodowawczej przewidzianej w RODO w stosunku do tego, co obowiązywało w ramach przepisów dyrektywy 95/46/WE. Wreszcie zdaniem Autorki uznać należy, że za koncepcją odpowiedzialności odszkodowawczej opartej za zasadzie ryzyka w ramach przepisów RODO przemawia także wykładnia celowościowa. Jeżeli weźmie się pod uwagę fakt, że polskie tłumaczenie RODO w zakresie przesłanki winy stanowi niechlubny wyjątek od innych wersji językowych – jak np. angielskiej, niemieckiej czy włoskiej – a celem RODO jest ujednolicenie systemu ochrony danych osobowych w całej UE oraz zharmonizowanie, ujednolicenie i zapewnienie wysokiego stopnia ochrony danych osobowych we wszystkich państwach UE (co wynika chociażby z motywu 3, 10 i 11 preambuły RODO) to wątpliwości nie powinna budzić ocena co do braku możliwości uznania, że odpowiedzialność na gruncie RODO oparta jest o zasadę winy[696].

Za przyjęciem odpowiedzialności na zasadzie ryzyka opowiada się także B. Marcinkowski twierdząc, że w tym kontekście dostrzec można podobieństwo regulacji ochrony danych osobowych z regułami odpowiedzialności za wypadki komunikacyjne w ruchu lądowym czy morskim. Przykładowo, Prawidło 2 Konwencji w sprawie międzynarodowych przepisów o zapobieganiu zderzeniom na morzu[697] zatytułowane „Odpowiedzialność" stanowi, iż żadne z postanowień niniejszych prawideł nie zwalnia statku lub jego armatora, kapitana bądź załogi od następstw jakiegokolwiek zaniedbania przestrzegania niniejszych prawideł lub zaniedbania zachowania środków ostrożności, których może wymagać zarówno zwykła praktyka morska, jak i szczególne okoliczności danego wypadku, a przy interpretowaniu i stosowaniu rzeczonych prawideł należy uwzględniać wszystkie niebezpieczeństwa żeglugi i zderzenia oraz wszelkie szczególne okoliczności, łącznie z możliwościami danych statków, które w celu uniknięcia bezpośredniego niebezpieczeństwa mogą uczynić konieczne odstąpienie od niniejszych prawideł. Owe postanowienia, nakładające na ich adresata nie tylko określony poziom staranności, ale też przewidywania zdarzeń i ich konsekwencji z

[696] K. Biczysko-Pudełko, *Cywilnoprawna odpowiedzialność dostawcy*...
[697] Konwencja COLEG 72, sporządzona w Londynie w dniu 20.10.1972 r. (Dz.U. z 1977 r., Nr 15, poz. 61).

uwzględnieniem kontekstu (szczególnych okoliczności danego wypadku), są w swej istocie zbliżone do przywoływanej wcześniej regulacji art. 32 ust. 1 RODO („Bezpieczeństwo przetwarzania"), zgodnie z którym administrator i podmiot przetwarzający – uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze – wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. W obu zatem przypadkach konieczne jest dokonanie oceny i projekcji ewentualnych, przyszłych ryzyk i zagrożeń oraz zastosowanie środków odpowiednich[698].

Zestawiając powyższe z przeprowadzonym badaniem charakteru obowiązków administratora i podmiotu przetwarzającego, których znacząca część polega na wykazaniu rozliczalności poprzez realizację aktów staranności w obszarze np. bezpieczeństwa danych, odpowiedzialność na zasadzie ryzyka wydaje się surowsza od odpowiedzialności na zasadzie winy w tym sensie, że surowsze są w takim przypadku przesłanki tej odpowiedzialności. Oceniając okoliczności wyłączające odpowiedzialność w kontekście przyczyn naruszeń przepisów o ochronie danych i naruszeń ochrony danych, które przeanalizowane zostały w pracy na podstawie dostępnego orzecznictwa, uznać należy, że ich rozumienie bliższe jest zasadzie winy.

W takim kierunku – wydaje się – podążają także opinie rzeczników wydawane w sprawach pytań prejudycjalnych do TSUE. Do zasady winy odnoszą się także projektowane w Dyrektywie w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji regulacje ustanawiające wspólne zasady dotyczące:

- ujawniania dowodów dotyczących systemów AI wysokiego ryzyka, aby umożliwić powodowi uzasadnienie pozaumownego cywilnoprawnego roszczenia odszkodowawczego opartego na zasadzie winy;
- ciężaru dowodu w przypadku pozaumownych cywilnoprawnych roszczeń odszkodowawczych opartych na zasadzie winy wnoszonych do sądów krajowych z tytułu szkód spowodowanych przez system sztucznej inteligencji.

[698] B. Marcinkowski, *Incydent, wina i kara. Problem granic odpowiedzialności administratora i procesora*. Manuskrypt.

Wykaz literatury

Abu Gholeh M., Kuźnicka-Błaszkowska D., *Ochrona danych osobowych w wybranych państwach Azji*, Wrocław 2019

Alama-Maruta K., *Algorytmiczne przetwarzanie danych na gruncie RODO – uwagi krytyczne oraz kierunki działań w celu poprawy standardów przetwarzania danych oraz ochrony prywatności*, MoP 2020/20

Babiarz P., *Dopuszczalność zlecania przez bank*, „Monitor Prawniczy" 2000/10

Bagińska E., *Odpowiedzialność deliktowa w razie niepewności związku przyczynowego. Studium prawnoporównawcze*, Gdańsk 2013

Banaszczyk Z. [w:] *Kodeks cywilny*, t. 1, komentarz 2015 do artykułów 1-449

Banaszczyk Z., *Możliwość zastosowania art. 439 k.c. w odniesieniu do przypadków sprowadzenia stanu bezpośredniego niebezpieczeństwa wyrządzenia szkody niezgodnym z prawem wykonywaniem władzy publicznej* [w:] *Non omne quod licet honestum est. Studia z prawa cywilnego i handlowego w 50-lecie pracy naukowej Profesora Wojciecha Jana Katnera*, Warszawa 2022

Banaszczyk Z., Granecki P., *O istocie należytej staranności*, „Palestra" 2002/7–8

Banyś T.A.J., Łuczak J., *Ochrona danych osobowych w praktyce. Jak uniknąć błędów i ich konsekwencji prawnych*, Wrocław 2013

Bar G., *Robot personhood, czyli po co nam antropocentryczna sztuczna inteligencja*? [w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński, Warszawa 2020

Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2017

Barta J., Markiewicz R., *Ochrona danych osobowych – komentarz*, Kraków 2002

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2015

Biczysko-Pudełko K., Cywilnoprawna odpowiedzialność dostawcy usług cloud computing w świetle przepisów rozporządzenia ogólnego o ochronie danych osobowych – wybrane problemy 2021

Biczysko-Pudełko K., Szostek D., *Koncepcje dotyczące osobowości prawnej robotów – zagadnienia wybrane*, „Prawo Mediów Elektronicznych" 2019/2

Bielak-Jomaa E., *Realizacja obowiązków administratora danych w związku z powierzeniem przetwarzania danych osobowych, odpowiedzialność podmiotu przetwarzającego oraz model współpracy między tymi podmiotami Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 11 .02. 2021 r., DKN.5130.2024.2020* [w:] „Gdańskie Studia Prawnicze" 2021/4(52), Rok XXV

Bieniek G. [w:] *Komentarz do kodeksu cywilnego. Księga trzecia. Zobowiązania*, t. 1, red. G. Bieniek, Warszawa 2005

Błachut J., Dudzik S., *Naruszenie ochrony danych osobowych. Problematyka prawna*, „Przegląd Konstytucyjny" 2021/3

Błaszczak Ł., Kuźmicka–Sulikowska J., *Zbieg roszczeń ex contractu ex delicto na tle art. 443 k.c. w ujęciu materialnoprawnym i procesowym*, „Transformacje Prawa Prywatnego" 2013/3

Chomiczewski W. [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak- Jomaa, D. Lubasz, Warszawa 2018

Błaszczyńska A. [w:] *Realizacja praw osób, których dane dotyczą*, red. B. Fischer, M.Sakowska-Baryła, Wrocław 2017

Błażewski M., Behr, J., *Środki prawne ochrony danych osobowych*, Wrocław 2018Boboli A., Borkiewicz M., Koszewicz K., Leśniewski G., *Ochrona danych osobowych w dziale IT*, Wrocław 2017

Bosek L., *Perspektywy rozwoju odpowiedzialności cywilnej za inteligentne roboty*, „Forum Prawnicze" 2019/2/(52)
Braciak J., *Prawo do prywatności* [w:] *Prawa i wolności obywatelskie w Konstytucji RP*, red. B. Banaszak, A. Preisner, Warszawa 2002
Brieskorn N., *Ochrona danych osobowych a zagrożenia prywatności* [w:] *Ochrona danych osobowych*, red. M. Wyrzykowski, Warszawa 1999
Breen S., Ouazzane K., Patel P., *GDPR: Is your consent valid?*, „Business Information Review" 2020/37(1)
Brożyna M., *Konsumenckie prawo do odwołania umowy*, Warszawa 2021
Brzozowska M., *Ochrona danych osobowych w sieci*, Wrocław 2012
Byczko Sz., *Consortia in Central And Easten Europe*, Gdańsk 2019
Byczko Sz., *Interes ubezpieczeniowy aspekty prawne*, Warszawa 2013
Byczko Sz., *Konsorcjum w orzecznictwie Sądu Najwyższego. Księga jubileuszowa ku czci Prof. W.J. Katnera*, Łódź 2022
Byczko Sz., *Świadczenie pieniężne ubezpieczyciela na tle pojęcia odpowiedzialności cywilnoprawnej, Prawo prywatne wobec wyzwań współczesności. Księga pamiątkowa dedykowana Profesorowi Leszkowi Ogiegle*, red. Mariusz Fras, Piotr Ślęzak, Łodź 2017
Byczko Sz., *Uwagi o charakterze prawnym konsorcjum*, „Studia Prawno-Ekonomiczne" 2021/121
Cool A., *Impossible, unknowable, accountable: Dramas and dilemmas of data law Social Stu* R. *dies of Science*, „Social Studies of Science" 2019/49/4
Czachórski W., *Odpowiedzialność kontraktowa i jej stosunek do odpowiedzialności deliktowej wg KC*, „Nowe Prawo" 1964/10
Czachórski W., *Zasady i funkcje odpowiedzialności cywilnej według kodeksu cywilnego – ich ewolucja* [w:] *Studia z prawa zobowiązań*, red. Z. Radwański, Warszawa–Poznań 1979
Czachórski W., *Zbieg odpowiedzialności według kodeksu zobowiązań*, Warszawa 1960
Czachórski W., *Zobowiązania. Zarys wykładu*, Warszawa 1994
Czaplińska M. , *Dokumentowanie współadministrowania danymi osobowymi*, LEX 2018
Czaplińska M. *Naprawienie szkody z tytułu naruszenia RODO* [w:] *D. Dörre-Kolasa* (red.), Ochrona danych osobowych w zatrudnieniu, Warszawa 2020
Czech M., *Umowa powierzenia przetwarzania danych osobowych*, Białystok 2020
Czerniawski M., Glosa do wyroku TSUE z 5.6.2018 r., C-210/16, *Wirtachtsakademie Scheswig-Holstein GmbH*, LEX
Czerniawski M., *Instytucja współadministrowania a pojęcie „ustalania" celów i sposobów przetwarzania danych osobowych – zarys problemu* [w:] *Rok RODO*, Warszawa 2019
Dmowski S. , Trzaskowski R. [w:] *Kodeks cywilny. Komentarz. Księga pierwsza, część ogólna*, t. 1, Warszawa 2014
Doliwa A., *Zobowiązania*, Warszawa 2006
Drobek P. [w:] E. Bielak-Jomaa, D. Lubasz, *RODO. Ogólne rozporządzenie o ochronie danych*, Warszawa 2018, komentarz do art. 5
Dorre Kolasa D., *Administrator danych osobowych w zbiorowym prawie zatrudnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społecznej" 2019/26/4
Drozd A., *Ustawa o ochronie danych osobowych*, Warszawa 2006
Drzewiecka-Konieczna B., *Inspektor ochrony danych w strukturze i funkcjonowaniu naczelnego organu administracji publicznej*, Warszawa 2019
Dybowski T. [w:] *System Prawa Prywatnego*, t. 3, *Prawo rzeczowe*, Warszawa 2007
Etel M., *Pojęcie przedsiębiorcy*, Warszawa 2012
Fajgielski P., *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych*) [w:]

Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2021
Fajgielski P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018
Fajgielski P., *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną* [w:] *Dysfunkcje publicznego prawa gospodarczego*, red. E. Kruk, G. Lubeńczuk, M. Zdyb, Warszawa 2018
Fajgielski P., *Rola Europejskiego Inspektora Ochrony Danych w kształtowaniu i wykładni przepisów o ochronie danych osobowych*, MoP 2021/23
Fischer B., *Pojęcie analizy ryzyka przy przetwarzaniu danych osobowych* [w:] B.Fisher, *Podział odpowiedzialności za chmurowe przetwarzanie danych osobowych z uwzględnieniem kształtowania regulacji umownych – wybrane zagadnienia*, MoP 2014/9
Fischer B., *Prawne aspekty norm technicznych. Normalizacja jako wsparcie legislacji administracyjnej*, Warszawa 2017
Fischer B., *Prawne uwarunkowania wykorzystania danych nieosobowych przez sztuczną inteligencję – zagadnienia podstawowe* [w:] *Prawo sztucznej inteligencji i nowych technologii*, red. B. Fischer, A. Pązik, M. Świerczyński, Warszawa 2022
Fischer B., *Prawo do prywatności i pewności prawa przy wykorzystaniu instrumentów samoregulacyjnych w związku z przetwarzaniem danych jednostki w systemach rozproszonych* [w:] *Władza – obywatele – informacja. Ku nowemu porządkowi prawnemu. Księga pamiątkowa ku czci Teresy Górzyńskiej*, red. I. Lipowicz, Warszawa 2014
Fischer B., Sakowska-Baryła M., *Realizacja praw osób, których dane dotyczą*, Wrocław 2017
Filipiak T.A., Mojek J., Nazar M., Niezbecka E., *Zarys prawa cywilnego*, Lublin 2002
Grzelak A., *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych*, MoP 2021/23
Gubernat B., Szczepaniak S. [w:] *Ustawa o ochronie danych osobowych*, red. M. Kawecki, M. Czerniawski, s. 282, Warszawa 2019
Gancarz I., *Pojęcie przedsiębiorcy w zakresie antykonkurencyjnych praktyk na tle art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej*, Wrocław 2012
Ganczar M., *Obowiązki administracji publicznej w zakresie ochrony danych osobowych* [w:] *Ochrona danych osobowych skuteczność regulacji*, Warszawa 2009
Ganczar M., *Obowiązki przedsiębiorców w zakresie gromadzenia, przetwarzania i udostępniania danych osobowych* [w:] *Człowiek z perspektywy biznesu*, red K. Machowicz Lublin 2009
Ganczar M., Pyter M., *Rejestr klauzul niedozwolonych jako źródło prawa administracyjnego i cywilnego, Źródła prawa administracyjnego a ochrona praw i wolności obywateli*, Warszawa 2014
Gawroński M., *Prawo do informacji o danych osobowych i obowiązek informacyjny*, LEX/el. 2018
Górski M. [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018
Golat R., *Przekazywanie przez pracodawców przetwarzania danych osobowych innym podmiotom*, „Służba Pracownicza" 2011/8
Grzybowski S., *Ochrona dóbr osobistych*, Warszawa 1957
Grzybowski S., *Prawo cywilne*, Kraków 1969
Gumularz M. [w:] *Meritum. Ochrona danych osobowych*, red. Dominik Lubasz, Warszawa 2021
Gumularz M., *Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, EPS 2017/5/140

Gumularz M., *Wpływ regulacjiw ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich*, EPS 2017/5
Gudowski J., Bieniek G., Komentarz do art. 443 [w:] *Kodeks cywilny. Komentarz*, red. J. Gudowski, t. 3, *Zobowiązania. Część ogólna*, LEX.
Gutowski M. [w:] *Kodeks cywilny – komentarz*, red. M. Gutowski, Warszawa 2016, t. 2
Härting N., Wykład na konferencji Stowarzyszenia Niemieckich Inspektorów Ochrony Danych na temat ochrony danych osobowych, Monachium, 27.10.2021
Hauser M., *Przepisy odsyłające. Zagadnienia ogólne*, Przegląd Legislacyjny 2003/4
Jagielska M., Jagielski M., *W poszukiwaniu prawa właściwego dla cywilnoprawnych roszczeń odszkodowawczych,* „Problemy Prawa Prywatnego Międzynarodowego" 2021/28
Jankowska M., *Podmiotowość prawna sztucznej inteligencji*? [w:] *O czym mówią prawnicy, mówiąc o podmiotowości*, red. A. Bielska-Brodziak, Katowice 2015
Juranek A.M., *Klauzule indemnifikacyjne jako szczególny mechanizm modyfikacji odpowiedzialności kontraktowej przez alokację ryzyka a kwestia akcesoryjnych zastrzeżeń umownych zabezpieczających ich wykonanie*, „Transformacje prawa prywatnego" 2020/4
Izydorczyk T., *Meritum, Ochrona danych osobowych*, red. D. Lubasz, Warszawa 2020
Jakubik M., T. Świętnicki, *RODO* [w:] *IT: sztuczna inteligencja a dane osobowe – czy RODO definiuje AI oraz ML?*, LEX 2020
Jatkiewicz P., *Ochrona danych osobowych Teoria i praktyka*, Warszawa 2015
Jabłoński M., *Prywatność jako przesłanka ograniczenia dostępu do informacji publicznej*, „Przegląd Prawa i Administracji" 2007/86
Jabłoński M., Węgrzyn J., Rzucidło J., *Znaczenie Protokołu nr 7 do Traktatu z Lizbony dla procesów integracyjnych w Unii Europejskiej*, „Przegląd Prawa i Administracji" 2011/86
Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice*, Wrocław 2000
Jagielski M., *Dokumentacja ochrony danych ze wzorami*, Warszawa 2019
Jatkiewicz P., *Ochrona danych osobowych. Teoria i praktyka*, Warszawa 2015
Kaczyńska S., *Zarządzający portem lotniczym jako podmiot prawa publicznego i prywatnego. Wybrane zagadnienia*, Warszawa 2016
Kaliński M., *Odpowiedzialność odszkodowawcza* [w:] *Szkoda na mieniu i jej naprawienie*, red. Olejniczak, M. Kaliński, Warszawa 2011
Kaliński M., *Prawo zobowiązań – część ogólna. System Prawa Prywatnego*, t. 6
Kappes A., *Podmiotowość prawna sztucznej inteligencji. Rzeczywista potrzeba czy kreacjonizm prawniczy?* [w:] *Non omne quod licet honestum est. Studia z prawa cywilnego i handlowego w 50-lecie pracy naukowej Profesora Wojciecha Jana Katnera*, red. U. Promińska, S. Byczko, A. Kappes, B. Kucharski, Warszawa 2022
Kappes A., *Prosta spółka akcyjna - czy rzeczywiście prosta i czy potrzebna? Uwagi do projektu nowelizacji Kodeksu spółek handlowych, wprowadzającego prostą spółkę akcyjną (projektowane art. 300(1) –300(121) k.s.h.*, PPH 2018/5
Karwala D., *Znaczenie soft law dla transferów danych osobowych do państw trzecich na przykładzie zaleceń EROD*, MoP 2020/01
Kasprzyk R., *Podstawa roszczenia prewencyjnego*, „Palestra" 19893/375/33
Katner W.J., *Pojęcie przedsiębiorcy – polemika*, PPH 2007/4/41–44
Katner W.J., *Prawo gospodarcze i handlowe*, Warszawa 2020
Katner W.J. [w:] *System Prawa Prywatnego*, red. W.J. Katner, t. 9, *Prawo zobowiązań – umowy nienazwane*, Warszawa 2015
Katner W.J. [w:] *Współczesne problemy prawa zobowiązań*, Warszawa 2015
Katner W.J., *Zakres tzw. konstytucji biznesu. Kontrowersje wokół pojęcia przedsiębiorcy w ustawie - Prawo przedsiębiorców z 2018 r.*, PPH 2019/1/5–10

Kawecki M., *Reforma ochrony danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Warszawa 2017
Kawecki M., *The proccessing of personal data by law offices after the new EU regulation on the protection of personal data has become effectice*, „Przegląd Prawno-Ekonomiczny" 2013/23
Kępa L., *Ochrona danych osobowych przewodnik dla przedsiębiorców*, Warszawa 2018
Klaja M., *O potrzebie regulacji umów o współdziałanie*, PPE 2019/4/49
Klimas D., Wróbel P., *Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia*
Klimas D., Wróbel P. [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda, *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017
Konert A., Sakowska-Baryła M., *Prawne uregulowania w zakresie używania bezzałogowych statków powietrznych przez media*, International Journal of Legal Studies 2020/8/2
Konieczna-Drzewiecka B., *Inspektor ochrony danych w strukturze i funkcjonowaniu naczelnego organu administracji publicznej*, Warszawa 2019
Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne" 1971/20
Korybski A., Leszczyński L., Pieniążek A., *Wstęp do prawoznawstwa*, Lublin 2007
Kosik J., *Technika komputerowa w ewidencji ludności a ochrona cywilnoprawna człowieka*, Wrocław 1978.
Kotecka-Kral S., *Sądowe środki ochrony prawnej i jurysdykcja krajowa w zakresie spraw związanych z ochroną danych osobowych na mocy rozporządzenia 2016/679* [w:] *Ars in vita. Ars in iure. Księga Jubileuszowa dedykowana Profesorowi Januszowi Jankowskiemu*, red. A. Barańska, S. Cieślak, Warszawa 2018
Kowalski S., *Zakres swobody podmiotu przetwarzającego przy przetwarzaniu danych osobowych*, MoP 2020/23
Krajnik Sz., A. Ornowska, *Przyczynienie się do powstania szkody w prawie cywilnym oraz jego aspekty prawnokarne*, „Studia Iuridica Toruniensia" 2011/8
Krasuski A., *Dane osobowe w obrocie tradycyjnymi elektronicznym. Praktyczne problemy*, Warszawa 2012
Krasuski A., *Status prawny sztucznego agenta. Podstawy prawne. Sztuczny agent i jego znaczenie dla rozwoju sztucznej inteligencji*, Warszawa 2020
Krasuski A., Skolimowska D., *Dane osobowe w przedsiębiorstwie*, Warszawa 2007
Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego*, Warszawa 2016
Księżak P. [w:] *Kodeks cywilny. Komentarz. Część ogólna*, red. M. Pyziak-Szafnicka, P. Księżak, uwagi 107 i n. do art. 23.
Księżak P. [w:] *Kodeks cywilny. Komentarz. Część ogólna*, red. M. Pyziak-Szafnicka, P. Księżak, uwagi 115 do art. 23
Księżak P. [w:] *Organizacja systemu ochrony zdrowia. System Prawa Medycznego*, red. D. Bach-Golecka Warszawa 2020
Księżak P., *Prawo cyborgów. Wprowadzenie w problematykę*, „Przegląd Prawniczy Alleharda" 2021/4/2(8)
Księżak P., *Zdolność prawna sztucznej inteligencji (AI)* [w:] *Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej*, red. W. Robaczyński, Łódź 2017

Księżak P., *Zdolność prawna sztucznej inteligencji (AI)* [w:] *Czynić postęp w prawie. Księga jubileuszowa dedykowana Profesor Birucie Lewaszkiewicz-Petrykowskiej,* red. W. Robaczyński, Łódź 2017
Księżak P., Wojtczak S., *Prawa Asimova, czyli science fiction jako fundament nowego prawa cywilnego*, „Forum Prawnicze" 2020/4/60
Kuba M., *Zasada przejrzystości przetwarzania danych osobowych jako instrument ochrony autonomii informacyjnej pracownika,* MOPR 2020/12
Kuczkowska E., Glosa aprobująca do wyroku WSA w Warszawie z 13.04.2021 r., sygn. akt II SA/WA 1898/20
Kucharski B., *Świadczenie ubezpieczyciela w umowie ubezpieczenia mienia*, Warszawa 2019
Kulesza E. [w:] *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, red. D.* Dörre-Kolasa, Warszawa 2017
Kurowska–Tober E., Czynienik Ł., Koniarska M., *Aspekty prawne sztucznej inteligencji – zarys problematyki*, MoP 2019/21
Kuźmicka-Sulikowska J., *Zasady odpowiedzialności deliktowej w świetle nowych tendencji w ustawodawstwie polskim,* Warszawa 2011
Lang W., *O strukturze odpowiedzialności prawnej*, ZNUMK 1968/31
Lang W., *Struktura odpowiedzialności prawnej*, „Prawo" 1968/8
Lang W., Wróblewski J., Zawadzki S., *Teoria państwa prawa*, Warszawa 1986
Lamik W., *Środki cywilnoprawne ochrony danych osobowych*. Rozprawa doktorska, Wrocław 2022
Lewaszkiewicz-Petrykowska B., *Wina jako przesłanka odpowiedzialności z tytułu czynów niedozwolonych*, „Studia Prawno-Ekonomiczne" 1969/2
Lewszkiewicz-Petrykowska B., *Wyrządzenie szkody przez kilka osób*, Warszawa 1978
Lewaszkiewicz-Petrykowska B., *Zakres odpowiedzialności na zasadzie ryzyka prowadzącego*
Lewandowska-Malec I., *Dobra osobiste na tle prawa międzynarodowego*, Warszawa 2017
Lewaszkiewicz-Petrykowska B., *Wyrządzenie szkody przez kilka osób*, Warszawa 1978
Litwiński P., *Administrator danych osobowych* [w:] *Ochrona danych osobowych w ogólnym postępowaniu administracyjnym*, Warszawa 2009, LEX
Litwiński P., *Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz*, red. P. Litwiński, Warszawa 2021
Litwiński P., *Ustawa o ochronie danych osobowych, Komentarz*, Warszawa 2016
Lubasz D.[w:] *Prawo sztucznej inteligencji*, red. L. Lai, M. Świerczyński,
Lubasz D., Chomiczewski W., *Privacy by Design a sztuczna inteligencja*, MoP 2020/20
Lubasz D., Szkurłat A., *Relatywizacja pojęcia danych osobowych w świetle orzecznictwa polskich sądów administracyjnych i powszechnych*, MoP 2021/23
Łakomiec K., *Prawo do ochrony prywatności w kontekście informacji o stanie zdrowia Autoreferat rozprawy doktorskiej, napisanej pod kierunkiem prof. dr. hab. Marka Zubika*, Warszawa 2018
Łętowska E. [w:] *System prawa prywatnego*, t. 1, *Prawo cywilne — część ogólna*, red. M. Safjan, Warszawa 2007
Łętowska E., *Zbieg norm w prawie cywilnym*, Warszawa 2002
Łukańko B., *Uchybienie przepisom o ochronie danych osobowych jako naruszenie dobra osobistego – analiza na przykładzie orzecznictwa Sądu Najwyższego*, „Studia Prawnoustrojowe UWM" 2019/46
Machnikowski P., *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski red., Warszawa 2016, komentarz do art. 23 k.c., teza 2
Machnikowski P. [w:] *System prawa prywatneg*o, t. 6, *Prawo zobowiązań – część ogólna*, red. A. Olejniczak, Warszawa 2014

Marcinkowski B., *Incydent, wina i kara. Problem granic odpowiedzialności administratora i procesora*. Manuskrypt.
Mednis A., *Administrator danych i podmiot przetwarzający dane na zlecenie – status prawny, zakres praw i obowiązków, problemy definicyjne* [w:] *Ochrona danych osobowych. Skuteczność regulacji*, red. G. Szpor, Warszawa 2009
Mednis A., *Ochrona danych osobowych w konwencji Rady Europy i dyrektywie Unii Europejskiej*, PiP 1997/6
Mednis A., *Prawna ochrona danych osobowych*,Warszawa 1995
Mednis A., *Prawo do prywatności a interes publiczny*, Warszawa 2006
Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999
Morawski F., *Odpowiedzialność cywilna administratora danych osobowych i podmiotu przetwarzającego według ogólnego. Rozporządzenia o ochronie danych osobowych*, „Acta Iuris Stetinensis" 2019/2/26
Morek R., Raczkowski M. [w:] *Kodeks cywilny. Komentarz*, red. K. Osajda, Warszawa 2018, Legalis.
Mrózek A., *Prawno-polityczne konsekwencje wdrożenia ADP w ramach aparatu państwa burżuazyjnego (na przykładzie państw zachodnich)*, Toruń 1978
Mrózek A., *Ustawowe prawo ochrony danych*, Toruń 1981
Nerka A., *Organizacja związkowa jako administrator – wybrane zagadnienia*, „Studia z Zakresu Prawa Pracy i Polityki Społeczne" 2020/27/4
Niklewicz-Pijaczyńska M. , *Własność przemysłowa w prawie i ekonomii oraz praktyce gospodarczej* [w:] *Własność w prawie i gospodarce*, red. U. Kalina-Prasznic, Wrocław 2017
Nowakowski T., *Reguły staranności a odpowiedzialność deliktowa – glosa do wyroku Sądu Apelacyjnego w Łodzi z dnia 30.01.2018. (I AC A 727/17)*, „Palestra" 2020/11
Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, red. M. Sakowska-Baryła, Warszawa 2018
Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Wybrane przepisy sektorowe. Komentarz, red. P. Litwiński, Warszawa 2021
Ohanowicz A., *Zbieg norm w kodeksie cywilnym*, „Nowe Prawo" 1966/12
Ohanowicz A., *Zbieg norm w kodeksie cywilnym*, PiP 1965/2
Ohanowicz A., *Zbieg norm w kodeksie cywilnym* [w:] A Ohanowicz, *Wybór prac*, Warszawa 2007
Olejniczak A. [w:] *Kodeks cywilny. Komentarz*, t. 3, *Zobowiązania. Część ogólna*, red. A. Kidyba, Warszawa 2014
Opalski A., Oplustil K., *Niedochowanie należytej staranności jako przesłanka odpowiedzialności cywilnoprawnej zarządców spółek kapitałowych*, „Przegląd Prawa Handlowego" 2013/3
Panowicz-Lipska J., *Kodeks cywilny. Komentarz. Księga I. Część ogólna*, red. J. Gutowski, Warszawa 2016, komentarz do art. 23 k.c., teza 13
Pązik A., *Szkoda wynikająca z naruszenia przepisów RODO. Wybrane problemy*, ZNUJ PPWI 2020/3
Partyk T., *Sądowe środki ochrony danych osobowych mogą być stosowane równolegle. Omówienie wyroku TS z dnia 12 stycznia 2023 r., C-132/21 (X)*, LEX/el. 2023;
Pietrzak A., *Prawo przedsiębiorców. Komentarz*, Warszawa 2019
Piskorz-Ryń A., *Ponowne wykorzystywanie informacji sektora publicznego*, Warszawa 2018
Pisuliński J., *Kilka pytań o europejski kodeks cywilny*, „Transformacje prawa prywatnego"
Publiczne prawo gospodarcze. System Prawa Administracyjnego, t. 8A, red. R. Hauser, Z. Niewiadomski, A. Wróbel, Warszawa 2013

Pisz M., *Konstytucyjne i ustawowe uwarunkowania ochrony danych osobowych w polskim porządku prawnym* [w:] *RODO. Przewodnik dla adwokatów i aplikantów adwokackich*, red. A. Mednis, Warszawa 2018
Rezler J., *O odpowiedzialności kontraktowej w jej stosunku do odpowiedzialności deliktowej – inaczej*, „Palestra" 31/10–11(358–359)
Robaczyński W., *Sztuczna inteligencja – przedmiot badań czy podmiot kontrolowany*, „Kontrola państwowa" 2022/67/6(407)
Rojszczak M., *Prawne aspekty systemów sztucznej inteligencji – zarys problemu* [w:] *Sztuczna inteligencja, blockchain, cyberbezpieczeństwo oraz dane osobowe. Zagadnienia wybrane*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Warszawa 2019
Rojszczak M., *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne* iKAR 2018/4
Romanowski M. *Zobowiązania rezultatu i starannego działania w umowach o prace badawcze*, „Studia Iuridica Lubinensia", 2010/14/77–92
Rzucidło J., *Prawo do prywatności i ochrona danych osobowych* [w:] *Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym*, Wrocław 2014
Sadomski J., *Konflikt zasad – ochrona dóbr osobistych a wolność prasy*, Warszawa 2008
Safjan M., *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych*, KPP 2002/1
Sakowska-Baryła M., *Administrator i podmiot przetwarzający w wytycznych 07/2020 EROD*, dodatek MoP 23/2021/23
Sakowska-Baryła M., *Dostęp do informacji publicznej a ochrona danych osobowych*, Warszawa 2022
Sakowska-Baryła M. [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018
Sakowska-Baryła M., *Ochrona danych osobowych a dostęp do informacji publicznej*, Warszawa 2022
Sakowska- Baryła M., *Prawo do ochrony danych osobowych*, Wrocław 2015
Serwach M., *Odpowiedzialność cywilna w teorii i w praktyce – najnowsze tendencje i kierunki zmian*, „Rozprawy Ubezpieczeniowe" 2009/1/6
Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia*, MoP 2016/20
Sibiga G., *Powierzenie przetwarzania danych osobowych w obrocie gospodarczym* [w:] *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, red. A. Mednis, Warszawa 2013
Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003
Skrzydło J., *Wolność słowa w orzecznictwie Sądu Najwyższego Stanów Zjednoczonych i Europejskiego Trybunału Praw Człowieka Analiza porównawcza*, Toruń 2013
Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty Prawnicze" 2009/9/1
Sobczyk A., *RODO. Rozproszona władza publiczna*, Kraków 2020
Sobolewski P. , *Kodeks cywilny. Komentarz*, t. 1, *Przepisy wprowadzające. Część ogólna. Własność i inne prawa rzeczowe*, red. K. Osajda, Warszawa 2017
M. Sośniak M. [w:] *Prawo cywilne*, red. S. Grzybowski, Warszawa 1972
Sójka T., *Cywilnoprawne ochrona inwestorów korzystających z usług maklerskich na rynku kapitałowym*, Warszawa 2016
Stawecki T., Winczorek P., *Wstęp do prawoznawstwa*, Warszawa 2021

Stelmachowski A., *Wstęp o teorii prawa cywilnego*, Warszawa 1969
Stelmachowski A., *Wstęp do teorii prawa cywilnego*, Warszawa 1984
Strugała R., *Dobra i interesy chronione w strukturze czynu niedozwolonego*, Warszawa 2019
Strugała R., *RODO a odpowiedzialność odszkodowawcza. Podstawowe problemy odpowiedzialności za szkodę spowodowaną nieprawidłowym przetwarzaniem danych osobowych*, „Monitor Prawniczy" 2018/17
Stylec-Szromek P., *Sztuczna Inteligencja – prawo, odpowiedzialność, etyka*, „Zeszyty Naukowe. Organizacja i Zarządzanie. Politechnika Śląska, 2018/123
Syska K., *Ocena odpowiedniości przepisów RODO do zapewnienia przejrzystości działania systemów AI – wybrane zagadnienia*, MoP 2020/23
Szpunar A., *Ochrona dóbr osobistych*, Warszawa 1979
Szpunar, *Odszkodowanie za szkodę majątkową. Szkoda na mieniu i osobie*, Bydgoszcz 1998
Szpunar A., *Czyny niedozwolone w kodeksie cywilnym*, „Studia Cywilistyczne" 1970/15
Szpunar A., *Zbieg roszczeń odszkodowawczych*, RPEiS 1974/1
Szwast M., *Związanie sądu powszechnego decyzją Prezesa Urzędu Ochrony Danych Osobowych o stwierdzeniu naruszenia przepisów o ochronie danych osobowych* [w:] *Polskie przepisy o ochronie danych osobowych. Aktualne problemy prawnej ochrony danych osobowych 2019*, red. G. Sibiga, MoP, 2019/22
Thompson M., *Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries*, Vanderbilt Journal of Entertainment & Technology Law, 2016/18/4
Van Alsenoy B., *Data Protection Law in the EU: Roles, Responsibilities and Liability*, „Intersentia" 2019/6
Warkałło W., *Odpowiedzialność odszkodowawcza. Funkcje, rodzaje, granice*, Warszawa 1972
Więzowska B., *Odpowiedzialność cywilna na zasadzie słuszności*, Warszawa 2009, LEX
Witkowska-Nowakowska K. [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018
Wiórek M.P. [w:] *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie*, t. 1, red. M. Dumkiewicz, K. Kopaczyńska–Pieczniak, J. Szczotka Jerzy, Warszawa 2020
Wronkowska S., Zieliński M., *Zasady techniki prawodawczej. Komentarz*, Warszawa 1997
Wróbel P., *Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia*, PME 2017/4
Wygoda K. [w:] Jabłoński M., Sakowska-Baryła M., Wygoda K., *Czy jesteśmy gotowi na stosowanie RODO*, Wrocław 2018
Wyrozumska A., *Znaczenie prawne zmiany statusu Karty Praw Podstawowych Unii Europejskiej*, „Przegląd Sejmowy" 2008/2(85)
Zagrobelny K., O *okolicznościach kształtujących odpowiedzialność odszkodowawczą dłużnika* [w:] *Odpowiedzialność w prawie cywilnym*, red. P. Machnikowski, „Prawo" 2006/300
Zawadzka N. [w:] *Ustawa o ochronie danych osobowych. Komentarz*, red. D. Lubasz, Warszawa 2019, komentarz do art. 92
Zanfir-Fortuna G., [w:] *The EU General Data Protection Regulation*
Ziembiński Z., *Problemy podstawowe prawoznawstwa*, Warszawa 2022
Zoll F., *Prawa osobiste w zarysie ze stanowiska prawa prywatnego austriackiego*, „Czasopismo Prawnicze i Ekonomiczne", Kraków 1903
Zelek M., *O kryteriach kwalifikacji przedsiębiorstwa lub zakładu jako wprawianego w ruch za pomocą sił przyrody (art. 435 § 1 k.c.)*, PS 2019/3
Ziemiak M.P., Karolak M., *Odpowiedzialność za szkody wyrządzone przez przedsiębiorstwo wprawiane w ruch za pomocą sił przyrody (art. 435 k.c.). Rozważania de lege lata i de lege ferenda na kanwie orzecznictwa sądowego i poglądów Profesora Jana Łopuskiego*, „Prawo i Więź" 2020/3

Żyznowski T., Glosa do uchwały Sądu Najwyższego z 29.10.1991 r. (III CZP 109/ 91), „Przegląd Sądowy" 1992/5/6

Wykaz orzecznictwa

Europejski Trybunał Sprawiedliwości/Trybunał Sprawiedliwości Unii Europejskiej

Wyrok ETS z 5.12.1967 r. w sprawie 19/67, *Bestuur der Sociale Verzekeringsbank v. J.H. van der Vecht*, ECLI:EU:C:1967:49.
Wyrok ETS z 12.11.1969 r. w sprawie 29/69, *Stauder v. Miasto Ulm*, ECLI:EU:C:1969:57.
Wyrok ETS z 18.02.1970 r. w sprawie 38/69, *Komisja v. Włochy*, ECLI:EU:C:1970:11.
Wyrok ETS z 23.4.1991 r., C-41/90, *Höfner i Elser p. Macrotron GmbH*, EU:C:1991:161.
Wyrok ETS z 18.6.1998 r. w sprawie C-35/96, *Komisja przeciwko Włochom*, Legalis.
Wyrok TSUE z 6.11.2003 r. w sprawie C-101/01.
Wyrok TSUE z 19.10.2016 r. w sprawie C-582/14, *Breyer vs Niemcy*.
Wyrok TSUE z 4.05.2023 r. w sprawie C-300/21.

Trybunał Konstytucyjny

Wyrok TK z 24.06.1997 r., sygn. akt K. 21/96, OTK ZU 1997/3/23.
Wyrok TK z 19.05.1998 r., sygn. akt U 5/97, OTK.
Wyrok TK z 11.04.2000 r., sygn. akt K. 15/98, OTK ZU 2000/3/86.
Wyrok TK z 19.02.2002 r., sygn. akt U 3/01, OTK-A 2002/1/3.
Wyrok TK z 20.04.2002 r., sygn. akt K 41/02.
Wyrok TK z 12.11.2002 r., sygn. akt SK 40/01, OTK-A 2002/6/81.
Wyrok TK z 20.11.2002 r., sygn. akt K 41/02, OTK-A 2002/6/83.
Wyrok TK z 20.06.2005 r., sygn. akt K 4/04 OTK-A 2005/6/64.
Wyrok TK z 13.12.2011 r., sygn. akt K 33/08, OTK-A 2011/10/116.
Orzeczenie TK z 24.06.1997 r., sygn. akt K 21/96, OTK 1997/2/23.
Wyrok TK z 22.10.2013 r., sygn. akt SK 14/11.
Wyrok TK z 5.2002 r., sygn.. akt SK 32/01.
Wyrok TK z 11.6.2002 r., sygn. akt SK 5/02.

Sądy powszechne

Uchwała SN z 16.11.1993 r., sygn. akt I PZP 28/93.
Uchwała SN z 29.06.1995 r., sygn. akt III CZP 66/95, OSNC 1995/12/168.
Uchwała SN z 4.09.2009 r., III CZP 62/09.
Wyrok SN z 28.04.1964 r., sygn. akt II CR 540/63, OSPiKA 1965, poz. 197.
Wyrok SN z 10.06.1977 r., sygn. akt II CR 187/77.
Wyrok SN z 17.07.1997 r., sygn. akt III CKN 149/97, OSP 2000/4/63.
Wyrok SN z 10.04.2000 r., sygn. akt V CKN 28/00, LEX nr 52426.
Wyrok SN z 28.04.2004 r., sygn. akt III CK 442/0219.
Wyrok SN z 8.10.2004 r., sygn. akt V CK 670/03, OSNC 2005/9/162.
Wyrok SN z 4.08.2005 r., sygn. akt III CK 701/04, LEX nr 371489.
Wyrok SN z 28.02.2006 r., sygn. akt III CSK 135/05.
Wyrok SN z 26.09.2006 r., sygn. akt II CK 372/05.
Wyrok SN z 15.02.2008 r., sygn. akt I CSK 358/07.
Wyrok SN z 11.03.2008 r., sygn. akt II CSK 539/07
Wyrok SN z 29.04.2009 r., sygn. akt II CSK 614/08.
Wyrok SN z 10.02.2010 r., sygn. akt V CSK 287/09.
Wyrok SN z 15.10.2010 r., sygn. akt V CSK 36/10.

Wyrok SN z 19.09.2013 r., sygn. akt I CSK 687/12, niepubl.
Wyrok SN z 24.06.2014 r., sygn. akt I CSK 532/13.
Wyrok SN z 11.02.2015 r., sygn. akt I CSK 868/14.
Wyrok SN z 16.12.2014 r., sygn. akt III CSK 52/14.
Wyrok SN z 28.10.2016 r., sygn. akt I CSK 695/15.
Wyrok SN z 1.06.2017 r., sygn. akt I CSK 597/16.
Wyrok SN z 13.12.2018 r., sygn. akt I CSK 690/17.
Wyrok SN z 23.11.2018 r., sygn. akt II CSK 682/17.
Wyrok SN z 7.10.2020 r., sygn. akt V CSK 603/18.
Postanowienie SN z 11.12.2001 r., sygn. akt II KKN 438/00, OSNKW 2001/3–4/33.
Postanowienie SN z 24.10.2003 r., sygn. akt III CZP 67/039.
Orzeczenie SN z 8.04.1994 r., sygn. akt III ARN 18/94.
Wyrok SA w Białymstoku – I Wydział Cywilny z 15.03.2017 r., sygn. akt I ACa 599/16.
Wyrok SA w Białymstoku – I Wydział Cywilny z 13.09.2017 r., sygn. akt r. I ACa 236/17.
Wyrok SA w Gdańsku – I Wydział Cywilny z 18.02.2015 r., sygn. akt I ACa 785/14.
Wyrok SA w Katowicach – I Wydział Cywilny z 28.05.2015 r., sygn. akt I ACa 158/15.
Wyrok SA w Katowicach – I Wydział Cywilny z 24.05.2018 r., sygn. akt I ACa 1202/17.
Wyrok SA w Krakowie – I Wydział Cywilny z 12.06.2014 r., sygn. akt I ACa 507/14.
Wyrok SA w Łodzi – I Wydział Cywilny z 17.12.2015 r., sygn. akt I ACa 806/15.
Wyrok SA w Łodzi – I Wydział Cywilny z 17.12.2015 r., sygn. akt I ACa 806/15.
Wyrok SA w Poznaniu z 14.11.2003 r., sygn. akt I ACa 1062/03.
Wyrok SA w Poznaniu z 22.09.2005 r., I ACa 197/05, wraz z aprobującą glosą M. Niedośpiał (OSA 2007/3/88).
Wyrok SA w Poznaniu z 20.03.2013 r., sygn. akt I ACa 122/13.
Wyrok SA w Poznaniu – I Wydział Cywilny z 21.10.2015 r., sygn. akt I ACa 475/15.
Wyrok SA w Szczecinie – I Wydział Cywilny z 17.03.2015 r., sygn. akt I ACa 868/14.
Wyrok SA w Warszawie – I Wydział Cywilny z 25.11.2016 r., sygn. akt I ACa 1565/15.
Wyrok SA w Warszawie – V Wydział Cywilny z 17.05.2017 r., sygn. akt VI ACa 223/16.
Wyrok SA w Warszawie z 18.09.2019 r., sygn. akt VI ACa 254/18.
Wyrok SA w Warszawie z 1.07.2020 r., sygn. akt VII AGa 245/19.
Wyrok SA Warszawa-Praga w Warszawie z 17.03.2022 r., sygn. akt II C 1228/19.
Wyrok SA we Wrocławiu – I Wydział Cywilny z 30.01.2014 r., sygn. akt I ACa 1452/13.
Wyrok SO w Elblągu z 24.03.2021 r., sygn. akt IV Pa 10/21.
Wyrok SO w Łodzi z 27.04.2017 r., sygn. akt III Ca 119/17.
Wyrok SO w Warszawie z 12.03.2020 r., sygn. akt I C 214/19.
Wyrok SO w Warszawie z 6.08.2020 r., sygn. akt XXV C 2596/19.
Wyroku SO Warszawa-Praga w Warszawie z 19.12.2021 r., sygn. akt II C 1169/19.
Wyrok SO we Wrocławiu – I Wydział Cywilny z 30.01.2014 r., sygn. akt I C 411/13.
Wyrok SR – Wrocław Śródmieście we Wrocławiu z 9.10.2018 r., sygn. akt VIII C 16/18.

Sądy administracyjne
Wyrok NSA z 7.08.2008 r., sygn. akt I OSK 1218/07, LEX nr 513794.
Wyrok NSA z 19.05.2011 r., sygn. akt I OSK 1079/10, CBOSA.
Wyrok NSA z 10.01.2014 r., sygn. akt I OSK 2254/13, CBOSA.
Wyrok NSA z 23.07.2014 r., sygn. akt I OSK 2769/13, CBOSA.
Wyrok NSA z 24.01.2018 r., sygn. akt I OSK 323/16, CBOSA.
Wyrok NSA z 11.04.2019 r., sygn. akt I OSK 1240/17, CBOSA.
Wyrok NSA z 28.06.2019 r., sygn. akt I OSK 2063/17, CBOSA.
Wyrok WSA w Gliwicach z 31.10.2018 r., sygn. akt II SA/Gl 593/17, CBOSA.
Wyrok WSA w Krakowie z 20.03.2014 r., sygn. akt II SA/Kr 127/14, CBOSA.

Wyrok WSA w Krakowie z 2.02.2017 r., sygn. akt II SA/Kr 1457/16, CBOSA.
Wyrok WSA w Łodzi z 12.02.2019 r., sygn. akt II SAB/Łd 181/18, CBOSA.
Wyrok WSA w Warszawie z 27.02.2004 r., sygn. akt II SA 291/03, LEX nr 569664.
Wyrok WSA w Warszawie z 8.12.2005 r., sygn. akt II SA/WA 1539/05, publik. LexPolonica, „Rzeczpospolita" 2005/289, s. C5.
Wyrok WSA w Warszawie z 3.03.2009 r., sygn. akt II SA/Wa 1495/08, CBOSA.
Wyrok WSA w Warszawie z 3.02.2010 r., sygn. akt II SA/Wa 1598/09, CBOSA.
Wyrok WSA w Warszawie z 7.10.2011 r., sygn. akt II SA/Wa 364/11, CBOSA.
Wyrok WSA w Warszawie z 9.04.2013 r., sygn. akt II SA/Wa 211/13, CBOSA.
Wyrok WSA w Warszawie z 25.04.2014 r., sygn. akt II SA/Wa 30/14, CBOSA.
Wyrok WSA w Warszawie z 26.10.2015 r., sygn. akt II SA/Wa 1135/15, CBOSA.
Wyrok WSA w Warszawie z 8.06.2017 r., sygn. akt II SA/Wa 1414/16, CBOSA.
Wyrok WSA w Warszawie z 26.08.2020 r., sygn. II SA/Wa 2826/19, CBOSA.
Wyrok WSA w Warszawie z 3.09.2020 r., sygn. akt II SA/Wa 2559/19, CBOSA.
Wyrok WSA w Warszawie z 10.02.2021 r., sygn. akt II SA/Wa 2378/20, CBOSA.
Wyrok WSA w Warszawie z 13.04.2021 r., sygn. akt II SA/Wa 1898/20, CBOSA.
Wyrok WSA w Warszawie z 11.05.2021 r., sygn. akt II SA/Wa 1801/20, CBOSA.
Wyrok WSA w Warszawie z 5.10.2021 r., sygn. akt II SA/Wa 528/21, CBOSA.

Inne

Decyzja GIODO z 15.07.2015 r., DIS/DEC 594/15/62961, Legalis nr 1336609.
Decyzja Prezesa UODO z 17.12.2020 r., znak sprawy DKN.5130.1354.2020.
Decyzja Prezesa UODO z 11.02.2021 r., znak sprawy DKN.5130.2024.2020.
Decyzja Prezesa UODO z 21.04.2021 r., znak sprawy DKN.5130.3114.2020.
Decyzja Prezesa UODO z 22.04.2021 r., znak sprawy DKN.5130.3114.2020.
Decyzja Prezesa UODO z 19.01.2022 r., znak sprawy DKN.5130.2215.2020
Decyzja Prezesa UODO z 19.01.2022 r., znak sprawy DKN.5131.33.2021

Wykaz aktów prawnych

Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz. Urz. UE z 2016 C 202)

Karta Praw Podstawowych Unii Europejskiej (wersja skonsolidowana: Dz.Urz. C 202 z 7.06.2016 r., s. 391)

Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U.1993.61.284).

Konwencja Związkowa Paryska z dnia 20.03.1883 r. o ochronie własności przemysłowej, przejrzana w Brukseli dnia 14.12.1900 r., w Waszyngtonie 2.06.1911 r. i w Hadze 6.11.1925 r. (ratyfikowana zgodnie z ustawą z dnia 17.03.1931 r.), (Dz.U. 1932 Nr 2, poz. 8).

Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. 2003, nr 3, poz. 25)

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24.10.1995 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)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 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)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz. L 303 z 28.11.2018)

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych *(Dz. Urz. L 008, z 12.01.2001).*

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie stucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii, 21.04. 2021, (COM/2021/206 final)

Rezolucja 34/169 Zgromadzenia Ogólnego ONZ z 17.12.1979 r.: Kodeks Postępowania Funkcjonariuszy Porządku Prawnego.

Rezolucja Parlamentu Europejskiego z 16.02.2017 r. zawierająca zalecenia dla Komisji w sprawie przepisów prawa cywilnego dotyczących robotyki, 2018/C252/25 (Dz.Urz. UE C z 18.07.2018)

Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 23.09.1980 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami

Decyzja wykonawcza Komisji (UE) 2021/915 z 4.06.2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725, (Dz.Urz. L 199 z 7.6.2021);

Komunikaty Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komunikatu Regionów: *Sztuczna inteligencja dla Europy*, 25.04.2018, COM/2018/237 final; *Skoordynowany plan w sprawie sztucznej inteligencji*, 7.12.2018, COM/2018/795 final; *Biała Księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania*, 19.02.2020, COM/2020/65 final.

Układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej, łącznie z Księżycem i innymi ciałami niebieskimi, sporządzony w Moskwie, Londynie, i Waszyngtonie dnia 27.01.1967 r. zwany też Traktatem o przestrzeni kosmicznej (Dz.U. 1968 nr 14 poz. 82).

Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję), 28.09.2022, COM/2022/496 final;

Ustawa z dnia 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2022 r., poz. 1360 ze zm.)

Ustawa z dnia 26.06.1974 r. – Kodeks pracy (Dz.U. z 2022 r., poz. 1510 ze zm.).

Ustawa z dnia 8.10.1982 r. o społeczno- zawodowych organizacjach rolników (Dz.U. 2022 poz. 281).

Ustawa z dnia 16.09.1982 r. – Prawo spółdzielcze (Dz.U. 2021 poz. 648).

Ustawa z dnia 23.12.1988 r. o działalności gospodarczej (Dz.U. 1988 nr 41 poz. 324).

Ustawa z dnia 7.04.1989 r. – Prawo o stowarzyszeniach (Dz.U. 2020 poz. 2261).

Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych (Dz.U. 2018 poz. 723).

Ustawa z dnia 19.11.1999 r. – Prawo o działalności gospodarczej (Dz.U. Nr 101, poz. 1178, ze zm.).
Ustawa z dnia 14.02.2003 r. o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw (Dz.U. nr 49, poz. 408).
Ustawa z dnia 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r. Nr 171, poz. 1800).
Ustawa z dnia 10.10.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r., poz. 1781).
Rozporządzenie Prezydenta RP z 27.6.1934 r. – Kodeks handlowy (Dz.U. Nr 57 poz. 502), data uchylenia: 1.1.2001 r.; zob. M. Allerhand, *Kodeks handlowy: komentarz*, Lwów 1935, s. 5–6.
Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29.04.2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).