ANALIZA RYZYKA W OCHRONIE DANYCH OSOBOWYCH

Andrzej Krasuski, Przemysław Siembida

PRAWO W PRAKTYCE

Wolters Kluwer

ANALIZA RYZYKA W OCHRONIE DANYCH OSOBOWYCH

Andrzej Krasuski, Przemysław Siembida

PRAWO W PRAKTYCE

Wolters Kluwer

WARSZAWA 2022

Stan prawny na 10 sierpnia 2022 r.

Recenzenci
Dr hab. Paweł Fajgielski, prof. KUL
Prof. dr hab. Andrzej Powałowski

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Ołówek

Opracowanie redakcyjne
JustLuk

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

Poszczególne części napisali:

Andrzej Krasuski – Wstęp, rozdziały I, II, III, VI, Zakończenie
Przemysław Siembida – rozdziały IV, V

ISBN 978-83-8286-718-3 *ISBN PDF-a: 978-83-8328-016-5*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

1. Akty normatywne

1.1. Źródła prawa krajowego

k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2022 r. poz. 1360 ze zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm. i sprost.)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735 ze zm.)
p.p.s.a.	– ustawa z 25.07.2022 r. – Prawo o ustroju sądów administracyjnych (Dz.U. z 2022 r. poz. 329 ze zm.)
pr. wod.	– ustawa z 20.07.2017 r. – Prawo wodne (Dz.U. z 2021 r. poz. 2233 ze zm.)
u.k.s.c.	– ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 ze zm.)
u.o.d.o.	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.i.n.	– ustawa z 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742 ze zm.)

1.2. Źródła prawa unijnego

decyzja 1082/2013/UE	– decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z 22.10.2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE (Dz.Urz. UE L 293, s. 1, sprost.)

decyzja 1313/2013/UE	– decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z 17.12.2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.Urz. UE L 347, s. 924, ze zm.)
dyrektywa 2004/49/WE	– dyrektywa 2004/49/WE Parlamentu Europejskiego i Rady z 29.04.2004 r. w sprawie bezpieczeństwa kolei wspólnotowych oraz zmieniająca dyrektywę Rady 95/18/WE w sprawie przyznawania licencji przedsiębiorstwom kolejowym, oraz dyrektywę 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej i pobierania opłat za użytkowanie infrastruktury kolejowej oraz certyfikację w zakresie bezpieczeństwa (Dz.Urz. UE L 164, s. 44, ze zm.) – akt uchylony
dyrektywa 2007/60/WE	– dyrektywa 2007/60/WE Parlamentu Europejskiego i Rady z 23.10.2007 r. w sprawie oceny ryzyka powodziowego i zarządzania nim (Dz.Urz. UE L 288, s. 27)
dyrektywa 2008/114/WE	– dyrektywa Rady 2008/114/WE z 8.12.2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz.Urz. UE L 345, s. 75)
dyrektywa 2012/18/UE	– dyrektywa Parlamentu Europejskiego i Rady 2012/18/UE z 4.07.2012 r. w sprawie kontroli zagrożeń poważnymi awariami związanymi z substancjami niebezpiecznymi, zmieniająca, a następnie uchylająca dyrektywę Rady 96/82/WE (Dz.Urz. UE L 197, s. 1)
dyrektywa 2016/798	– dyrektywa 2016/798/WE Parlamentu Europejskiego i Rady UE z 11.05.2016 r. w sprawie bezpieczeństwa kolei (Dz.Urz. UE L 138, s. 102, ze zm.)
dyrektywa 2016/1148	– dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)
EKPCz	– Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 4.11.1950 r. zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.)
KPP UE	– Karta Praw Podstawowych Unii Europejskiej (2007/C 303/01) (Dz.Urz. UE C 303 z 2007 r., s. 1, ze sprost.)

RODO lub rozporządzenie 2016/679	– 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. UE L 119, s. 1, ze zm.)
rozporządzenie 178/2002	– rozporządzenie (WE) nr 178/2002 Parlamentu Europejskiego i Rady z 28.01.2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (Dz.Urz. UE L 31, s. 1, ze zm.)
rozporządzenie 611/2013	– rozporządzenie Komisji (UE) nr 611/2013 z 24.06.2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz.Urz. UE L 173, s. 2)
rozporządzenie 2018/151	– rozporządzenie wykonawcze Komisji (UE) 2018/151 z 30.01.2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia czy incydent ma istotny wpływ (Dz.Urz. UE L 26, s. 48, ze zm.)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 47)
TUE	– Traktat o Unii Europejskiej (wersja skonsolidowana 2016) (Dz.Urz. UE C 202, s. 13)

1.3. Wytyczne i zalecenia

Wytyczne GrArt. 29 WP 248v1	– Wytyczne Gr. Art. 29 dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679, ang. Guidelines on Data Protection Impact Assessment (DPIA)

	and determining whether processing is „likely to result in a high risk" for the purposes of Regulation 2016/679, z 4.04.2017 r., WP 248 (zaktualizowane w 4.10.2017 r., WP 248v1) (https://ec.europa.eu/newsroom/article29/items/611236/en, dostęp: 30.07.2022 r.)
Wytyczne GrArt. 29 WP 250v1	– Wytyczne Gr. Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, z 3.10.2017 r., WP 250 (zaktualizowane 6.02.2018 r., WP 250v1) (https://ec.europa.eu/newsroom/article29/items/612052/en, dostęp: 30.07.2022 r.)
Wytyczne GrArt. 29 WP 253	– Wytyczne Grupy Roboczej Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia 2016/679 z 3.10.2017 r., WP 253 (https://ec.europa.eu/newsroom/article29/items/611237/en, dostęp: 30.07.2022 r.)

1.4. Normy techniczne

ISO 19510	– ISO 19510 – ISO/IEC-19510 (Information technology – Object Management Group Business Process Model and Notation)
ISO 27000	– ISO 27000 – PN-ISO/IEC-27000 (Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia)
ISO 27001	– ISO 27001 – PN-ISO/IEC-27001 (Technika informatyczna – Techniki bezpieczeństwa – Wytyczne do zintegrowanego wdrożenia)
ISO 27002	– ISO 27002 – PN-ISO/IEC-27002 (Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczenia informacji)
ISO 27005	– ISO 27005 – PN-ISO/IEC-27005 (Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji)
ISO 27018	– ISO 27018 – PN-ISO/IEC-27018 (Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII)

ISO 29134	– ISO 29134 – PN-ISO/IEC-29134 (Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące oceny skutków dla prywatności)
ISO 29151	– ISO 29151 – PN-ISO/IEC-29151 (Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady ochrony informacji o identyfikowalnych osobach)
ISO 31010	– ISO 31010 – PN-EN IEC-31010 (Zarządzanie ryzykiem – Techniki oceny ryzyka)
ISO 9001	– ISO 9001 – PN-EN ISO-9001 (Systemy zarządzania jakością – Wymagania)

2. Czasopisma i publikatory

Apel.-W-wa	– Apelacja – Sąd Apelacyjny w Warszawie
CBOSA	– Centralna Baza Orzeczeń Sądów Administracyjnych
ONSA	– Orzecznictwo Naczelnego Sądu Administracyjnego
ONSAiWSA	– Orzecznictwo Naczelnego Sądu Administracyjnego i wojewódzkich sądów administracyjnych
OSNC	– Orzecznictwo Sądu Najwyższego. Izba Cywilna
OSNCP	– Orzecznictwo Sądu Najwyższego. Izba Cywilna (od 1962 r. do końca 1994 r.)
OSNP	– Orzecznictwo Sądu Najwyższego. Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych
OTK	– Orzecznictwo Trybunału Konstytucyjnego
OTK-A	– Orzecznictwo Trybunału Konstytucyjnego; zbiór urzędowy, Seria A
OTK ZU	– Orzecznictwo Trybunału Konstytucyjnego Zbiór Urzędowy
PiP	– Państwo i Prawo
PUG	– Przegląd Ustawodawstwa Gospodarczego

3. Organy i instytucje

ABW	– Agencja Bezpieczeństwa Wewnętrznego
ANSSI	– (fr. Agence nationale de la sécurité des systèmes d'information) Francuska Krajowa Agencja Bezpieczeństwa Systemów Informatycznych

CNIL	– (fr. The Commission nationale de l'informatique et des libertés) Krajowa Komisja Informatyki i Swobód – francuski organ regulacyjny
CSIRT	– (ang. Computer Security Incident Response Team) Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (np. CSIRT MON)
ENISA	– (ang. The European Union Agency for Cybersecurity) Agencja Unii Europejskiej do spraw Cyberbezpieczeństwa
EROD	– Europejska Rada Ochrony Danych
ETPCz	– Europejski Trybunał Praw Człowieka
FREE	– (ang. Fundamental Rights Experts Europe Group) Europejska Grupa Ekspertów ds. Praw Podstawowych
GIODO	– Generalny Inspektor Ochrony Danych Osobowych zastąpiony przez Prezesa UODO
GPDP	– (wł. Garante per la protezione dei dati personali) Gwarant ochrony danych osobowych – włoski organ regulacyjny
Grupa Robocza/ Gr. Art. 29	– Grupa Robocza ds. Ochrony Danych Osobowych, powołana na mocy art. 29 dyrektywy 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. WE L 281, s. 31, ze zm.) – akt uchylony
ICO	– (ang. Information Commissioner's Office) Brytyjskie Biuro Rzecznika Informacji
IOD	– Inspektor Ochrony Danych
ISO	– International Organisation for Standarisation (Międzynarodowa Organizacja Normalizacyjna)
NASK	– Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy
NIST	– National Institute of Standards and Technology (amerykański Narodowy Instytut ds. Standardów i Technologii)
NSA	– Naczelny Sąd Administracyjny
OMG	– Object Management Group
SA	– sąd apelacyjny
SN	– Sąd Najwyższy
TK	– Trybunał Konstytucyjny
TS	– Trybunał Sprawiedliwości

TSUE	– Trybunał Sprawiedliwości Unii Europejskiej
UKE	– Urząd Komunikacji Elektronicznej
UODO	– Urząd Ochrony Danych Osobowych
WSA	– wojewódzki sąd administracyjny
ZFODO	– Związek Firm Ochrony Danych Osobowych

4. Inne

BIP	– Biuletyn Informacji Publicznej
EOG	– Europejski Obszar Gospodarczy
iss.	– *issue* (pol. wydanie)
proces DPiA	– ocena skutków planowanych operacji przetwarzania dla ochrony danych osobowych

WPROWADZENIE

W RODO prawodawca unijny wprowadził model konkretyzacji obowiązków prawnych w oparciu o kryterium ryzyka. Nie zdefiniował jednak pojęcia „ryzyko", nie określił również sposobu jego identyfikacji oraz ustalenia jego skali. Ryzyko jako kryterium konkretyzacji obowiązków prawnych przewidziane zostało również w innych obszarach regulacji prawnej, w tym m.in. w regulacji ochrony zdrowia publicznego, bezpieczeństwa żywności, zarządzania kryzysowego, cyberbezpieczeństwa oraz zwalczania przestępczości.

Artykuł 83 Konstytucji RP formułuje obowiązek przestrzegania prawa Rzeczypospolitej Polskiej. Organy administracji oraz sądy przy wydawaniu rozstrzygnięć są zobowiązane do brania pod uwagę nie tylko przepisów ustaw i rozporządzeń, ale również przepisów Konstytucji RP, powinny także uwzględniać, czy działania obywatela były zgodne z prawem. Obowiązek przestrzegania przepisów prawa należy postrzegać również z punktu widzenia zasady równości wobec prawa. Zgodnie z art. 32 ust. 1 i art. 83 Konstytucji RP wszyscy są wobec prawa równi, wszyscy mają prawo do równego traktowania przez władze publiczne i każdy ma obowiązek przestrzegania prawa Rzeczypospolitej Polskiej. Ponadto z ogólnej zasady państwa demokratycznego – wyrażonej w art. 2 Konstytucji RP – wynika, że obowiązki prawne powinny być formułowane w sposób zrozumiały dla obywateli.

Obowiązek przestrzegania prawa, o którym mowa w art. 83 Konstytucji RP, należy rozpatrywać w kontekście możliwości zapoznania się z obowiązkami prawnymi wynikającymi z norm prawnych określonych w odpowiednich przepisach prawa. Każdy obywatel powinien

zatem mieć możliwość zrozumienia obowiązujących go przepisów prawa. Jest to możliwe wówczas, gdy przepis prawa jest sformułowany w sposób przejrzysty, wystarczająco szczegółowy i zrozumiały. W innej sytuacji nie powinno się w państwie demokratycznym oczekiwać przestrzegania prawa przez jego adresatów.

Obowiązek prawny może wynikać wprost z normy prawnej zawartej w określonym przepisie bez konieczności zrelatywizowania tego obowiązku do konkretnej sytuacji objętego hipotezą normy prawnej zawartej w tym przepisie. W pewnych przypadkach ustawodawca przewidział konieczność konkretyzacji obowiązków prawnych. Konkretyzacja ta może odbywać się poprzez indywidualny akt administracyjny organu administracji publicznej bądź za pośrednictwem kryterium konkretyzacji wskazanych wprost w przepisach prawa. W tym drugim przypadku akt konkretyzacji obowiązku prawnego, jak również wykonania skonkretyzowanego obowiązku prawnego spoczywa na adresacie normy prawnej.

Takim kryterium konkretyzacji może być ryzyko. W tym przypadku zakres obowiązku prawnego konkretyzowany jest przez adresata normy prawnej poprzez odniesienie tego obowiązku do ryzyka. Ustawodawca określa w akcie normatywnym cel postępowania z ryzykiem, który będzie związany z jego zmniejszeniem.

Przedmiotem niniejszej monografii jest przedstawienie analizy zastosowania przez prawodawcę unijnego w RODO modelu konkretyzacji obowiązków prawnych opartych na kryterium ryzyka naruszenia praw lub wolności osób fizycznych. W publikacji zostały omówione m.in. przyczyny wprowadzenia norm prawnych opartych na analizie ryzyka, jak również ocena zasadności wprowadzenia tych norm prawnych, z uwzględnieniem uwarunkowań przetwarzania danych osobowych, w tym zagrożeń z tym związanych. Monografia zawiera także wyjaśnienie znaczenia pojęcia „ryzyko" oraz odniesienie prawodawcy unijnego do ryzyka naruszenia praw lub wolności osób fizycznych, których dane osobowe są przetwarzane. Omówiona została metodyka identyfikacji ryzyka naruszenia praw lub wolności osób fizycznych, jak również sposób zarządzania ryzykiem. Zastosowanie tej metodyki

jest procesem złożonym, wymagającym wiedzy z zakresu rachunku prawdopodobieństwa, a także zarządzania procesami biznesowymi w organizacji. Analizie poddane zostało zagadnienie, czy przeniesienie przez prawodawcę unijnego na administratora i podmiot przetwarzający odpowiedzialności za konkretyzację obowiązków prawnych, jak również ich wykonanie jest prawnie usprawiedliwione. W związku z tym ocenione zostało, czy potrzebne jest przeprowadzenie zmian legislacyjnych, w postaci wniosków *de lege ferenda*. W tym kontekście istotne jest ustalenie, jakie cechy powinien spełniać adresat wymogu konkretyzacji obowiązków prawnych za pośrednictwem kryterium ryzyka. Wykonanie aktu konkretyzacji obowiązków prawnych w oparciu o kryterium ryzyka naruszenia praw lub wolności osób fizycznych, a następnie skonkretyzowanych obowiązków prawnych podlega ocenie przez Prezesa Urzędu Ochrony Danych Osobowych, jako krajowego organu nadzoru nad ochroną danych osobowych. W związku z tym w publikacji zostały omówione kompetencje tego organu w zakresie prowadzenia postępowań odnoszących się do ryzyka naruszenia praw lub wolności osób fizycznych. Przedstawiono także zasady postępowania przed Prezesem UODO, w kontekście uprawnień strony tego postępowania. Monografia analizuje również rolę sądownictwa administracyjnego w kontekście stosowania modelu regulacji polegającego na konkretyzacji obowiązków prawnych, przez podmioty zobowiązane, za pomocą kryterium ryzyka.

Monografia składa się z sześciu rozdziałów.

W rozdziale I została omówiona istota obowiązku prawnego oraz przedstawiono modele konkretyzacji obowiązków prawnych. Wyjaśniona została definicja ryzyka. Ponadto omówione zostało zastosowanie modelu konkretyzacji obowiązków prawnych w oparciu o kryterium ryzyka w wybranych obszarach regulacji.

Rozdział II dotyczy metody badania konkretyzacji obowiązków prawnych ustalanych w oparciu o kryterium ryzyka. W ramach tego rozdziału omówione zostały przyczyny zastosowania modelu badawczego, przedstawiona została metoda badań naukowych oraz zastosowana została normatywna teoria wykładni.

Rozdział III jest poświęcony regulacji ryzyka naruszenia praw lub wolności osób fizycznych. W rozdziale tym została przedstawiona regulacja ryzyka w RODO oraz akt konkretyzacji obowiązku prawnego na podstawie kryterium ryzyka naruszenia praw lub wolności osób fizycznych i jego wykonanie. Zaprezentowano ujęcie podmiotowe i przedmiotowe ryzyka naruszenia praw lub wolności osób fizycznych. Ponadto w rozdziale tym omówione zostały prawa i wolności osób fizycznych, których dotyczy ryzyko ze wskazaniem różnych źródeł prawnych.

W rozdziale IV zostały omówione metody identyfikacji ryzyka naruszenia praw lub wolności osób fizycznych. W ramach tego rozdziału wyjaśniono znaczenie podejścia procesowego dla identyfikacji i zarządzania ryzykiem. Przedstawione zostały modele i mapy procesów oraz omówiono metodykę analizowania ryzyka. Omówione zostały iteracje, wykorzystanie audytu do zarządzania przetwarzaniem danych osobowych opartego na ryzyku, kontekst oraz szacowanie ryzyka.

Rozdział V został poświęcony postępowaniu z ryzykiem naruszenia praw lub wolności osób fizycznych. Wyjaśniono, na czym polega analiza ryzyka, w tym również jego ewaluacja. Ponadto wyjaśnione zostały sposoby modyfikowania ryzyka. W rozdziale tym omówiono sposób wyznaczania poziomu realizacji zabezpieczeń, jak również sposób oceny poziomu realizacji zabezpieczeń. Przedstawione zostało także zagadnienie rejestrowania, raportowania i akceptowania ryzyka.

Rozdziały IV i V zostały opracowane przez inż. Przemysława Siembidę.

Rozdział VI dotyczy nadzoru administracyjnoprawnego wykonywania obowiązków prawnych w oparciu o kryterium ryzyka naruszenia praw lub wolności osób fizycznych. W rozdziale tym omówione zostały kompetencje Prezesa UODO do prowadzenia postępowań, w których rozstrzygnięcie oparte jest na analizie ryzyka naruszenia praw lub wolności osób fizycznych. Analizie poddana została zdol-

ność prawna Prezesa UODO, a także kompetencja szczególna tego organu do prowadzenia postępowań administracyjnych, w których jest uwzględniana analiza ryzyka. Zważywszy, że postępowanie administracyjne jest postępowaniem, w którym pozycja strony postępowania i organu administracji publicznej nie są równe, w rozdziale tym zostały omówione zasady postępowania przed Prezesem UODO i ich znaczenie dla wyrównania relacji pomiędzy tym organem a stronami postępowania. Zagadnienia te zaprezentowano w odniesieniu do konkretnych spraw rozstrzyganych w aktach administracyjnych Prezesa UODO. Przedstawione zostały również środki odwoławcze od rozstrzygnięć tego organu, mając na względzie wyłączenie zasady dwuinstancyjności. Omówiona została także prawomocność i egzekwowalność orzeczeń sądów administracyjnych w sprawach skarg na decyzje i postanowienia Prezesa UODO.

W Zakończeniu zostały przedstawione refleksje prawne na temat dopuszczalności stosowania w prawie konstrukcji konkretyzacji obowiązków prawnych, w których prawodawca unijny przenosi na zobowiązanego wymóg dokonania konkretyzacji w oparciu o niedookreślone kryteria konkretyzacji. Zagadnienie to zostało omówione w kontekście praw i obowiązków określonych w Konstytucji RP, w tym wynikającego z art. 83 Konstytucji RP obowiązku do przestrzegania prawa obowiązującego w Rzeczypospolitej Polskiej. Problematyka ta została omówiona z punktu widzenia podmiotów zobowiązanych do dokonania konkretyzacji obowiązków prawnych i wykonania tych obowiązków, jak również statusu prawnego i kompetencji Prezesa UODO, jako organu administracji publicznej. Uwzględniona została również rola sądownictwa administracyjnego w tym zakresie. Szerokie ujęcie tego zagadnienia legło u podstaw odpowiedzi na pytanie, czy w aktualnym stanie prawnym konieczne są zmiany *de lege ferenda*.

Monografia uwzględnia stan prawny na 10.08.2022 r.

dr hab. Andrzej Krasuski, prof. UJD

Warszawa, sierpień 2022 r.

Rozdział I

REGULOWANIE OBOWIĄZKÓW PRAWNYCH W OPARCIU O KRYTERIUM RYZYKA

1. Sposoby konkretyzacji obowiązków w prawie

Pojęcie obowiązku prawnego łączy się z pojęciem sytuacji prawnej czy sytuacji konkretnego podmiotu wyznaczonej przez obowiązujące normy prawne, tj. normy ustanowione we właściwym trybie lub uznane za obowiązujące przez organy państwa, w których to normach w sposób jednoznaczny i bezpośredni nakazuje się podmiotom, do których są skierowane, aby w pewnych okolicznościach zachowały się w ten, a nie inny sposób. Narzędziem służącym do opisywania sytuacji, w której znajdują się adresaci normy prawnej z uwagi na jej treść, jest pojęcie stosunku prawnego. Charakterystyka przedmiotu tego stosunku obejmuje zachowania, których jego strony mogą od siebie oczekiwać[1].

Obowiązek w znaczeniu prawnym oznacza konieczność zachowania się w odpowiedni sposób, co wynika z nakazu albo zakazu określonego w normie prawnej. Obowiązek prawny sprowadza się więc najczęściej do tego, że przepis prawa ustanawia dla danego podmiotu nakaz lub zakaz określonego zachowania się (działania lub

[1] F. Longchamps de Bérier, *O pojęciu stosunku prawnego w prawie administracyjnym*, „Acta Universitatis Wratislaviensis" 1964/12(19), s. 45.

zaniechania)[2]. Niezastosowanie się do nakazu lub zakazu wytwarza stan niewypełnienia obowiązku uregulowanego przez prawo[3].

Zachowanie będące przedmiotem obowiązku wynikające z określonej normy prawnej może być nakazane lub zakazane. Oznacza to, że może wystąpić obowiązek pozytywny lub negatywny[4]. Obowiązek prawny nie musi sprowadzać się do prostych nakazów lub zakazów. Obowiązek prawny stanowi uwarunkowane przez zawarte w normach prawa żądanie i zagwarantowaną przez przymus państwowy konieczność określonego zachowania się[5].

Obowiązek prawny stanowi zatem uwarunkowane przez zawarte w normach prawa żądanie i zagwarantowaną przez przymus państwowy konieczność określonego zachowania się[6].

W literaturze przedmiotu podkreśla się, że czyn może polegać na jakimś działaniu lub zaniechaniu, a w przypadku gdy norma nie określa czynu formalnie, lecz wskazuje, jaki stan rzeczy ma być przez adresata normy zrealizowany, czyn może składać się ze złożonego zespołu działań i zaniechań[7].

Wyodrębniając części składowe pojęcia prawnego obowiązku, można wskazać na następujące zależności:

1) zachodzi tu brak możności wyboru określonego postępowania przez adresata obowiązku, przeciwnie, istnieje nakaz lub zakaz określonego postępowania;
2) obowiązek zawsze wynika z prawa w znaczeniu przedmiotowym, inaczej mówiąc, nie ma obowiązku bez normy;
3) w przypadku sporu konieczność wskazania podstawy prawnej, z której wynika określony obowiązek, ciąży na organie państwowym żądającym wykonania tego obowiązku przez obywatela;

---

[2] Wyrok WSA w Warszawie z 14.02.2017 r., IV SA/Wa 2461/16, LEX nr 2288716.
[3] Wyrok WSA w Warszawie z 23.11.2015 r., IV SA/Wa 2538/15, LEX nr 2030777.
[4] Wyrok WSA w Warszawie z 13.01.2016 r., IV SA/Wa 2609/15, LEX nr 2045690.
[5] Wyrok WSA w Warszawie z 7.12.2021 r., IV SA/Wa 1376/21, LEX nr 3308562.
[6] Wyrok NSA z 16.04.2019 r., II OSK 1409/17, LEX nr 2678388.
[7] Z. Ziembiński, *Logiczne podstawy prawoznawstwa*, Warszawa 1966, s. 99.

4) na państwie ciąży powinność podjęcia starań w celu zapewnienia realizacji obowiązków. Z sytuacjami, w których niewypełnienie obowiązku powinno pociągać za sobą ujemne skutki, mamy do czynienia zaś wówczas, gdy dany przepis prawa nakazuje wiązanie ujemnych skutków prawnych z każdym przypadkiem niewypełnienia danego obowiązku[8].

Pojęcie obowiązku jako zachowania nakazanego lub zakazanego przez normę prawną może być odniesione już do sytuacji, gdy określone zachowanie jest nakazane lub zakazane przez samą normę prawną, bez konieczności jego zrelatywizowania do sytuacji pewnego podmiotu i powiązania go z uprawnieniem przysługującym temu podmiotowi[9].

W określonych przypadkach ustawodawca, przy ustalaniu norm prawnych, przyjmuje, że powołanie się na wynikające z tych norm uprawnienia i odpowiadające im obowiązki prawne wymaga ich uprzedniej konkretyzacji. Konkretyzacja ta jest możliwa w dwojaki sposób.

Po pierwsze, za pośrednictwem indywidualnego aktu, skierowanego do tego podmiotu, który pozostaje stroną stosunku materialnoprawnego ustalonego w normie wymagającej konkretyzacji. W tym przypadku organ administracji publicznej, działając w oparciu o normę zadaniową i kompetencyjną, konkretyzuje obowiązek prawny w indywidualnym akcie administracyjnym, wydanym w trybie określonym w Kodeksie postępowania administracyjnego lub w przepisie szczególnym.

Po drugie, za pośrednictwem kryteriów dotyczących cech samego obowiązku prawnego lub uprawnienia, któremu ten obowiązek odpowiada. Obowiązek trzeba postrzegać jako powinność jednej ze stron zachowania się w określony sposób, zaspokajający prawnie chroniony interes jego drugiej strony. W stosunkach prywatnoprawnych stroną, która może oczekiwać zaspokojenia swojego interesu przez

[8] Wyrok WSA w Warszawie z 13.01.2016 r., IV SA/Wa 2609/15, LEX nr 2045690.

[9] M. Romańska, *Postępowanie egzekucyjne i zabezpieczające w administracji*, Warszawa 2021, s. 18.

oczekiwane zachowanie innej osoby, jest podmiot prawa prywatnego, w stosunkach administracyjnoprawnych stroną tą jest organ reprezentujący interes społeczny. Celem postępowania administracyjnego jest w takim przypadku skonkretyzowanie sytuacji prawnej, tj. praw i obowiązków, oznaczonego podmiotu, w drodze decyzji[10].

Takim kryterium może być ryzyko. W tym przypadku zakres obowiązku prawnego konkretyzowany jest poprzez adresata normy prawnej poprzez odniesienie tego obowiązku do ryzyka. Ustawodawca określa w akcie normatywnym cel postępowania z ryzykiem, który będzie związany z jego zmniejszeniem.

2. Definicja terminu „ryzyko"

Pojęcie ryzyka wywodzi się z języka włoskiego (wł. *risico*), w którym oznacza przede wszystkim przedsięwzięcie, którego wynik jest nieznany albo niepewny, lub możliwość, że coś się uda albo nie uda[11], czy też inaczej stan, w którym rezultat osiągnięty w przyszłości jest nieznany, ale można zidentyfikować jego przyszłe alternatywy, przy założeniu, że szanse wystąpienia możliwych alternatyw są znane[12].

W semantyce tego słowa dostrzega się również to, że ryzyko jest raczej wyborem, a nie nieuchronnym przeznaczeniem[13].

Zdefiniowanie ryzyka jest zadaniem złożonym. Potoczne rozumienie pojęcia „ryzyko" jest wieloznaczne. Według *Słownika języka polskiego* pojęcie to rozumiane jest jako „możliwość, że coś się nie uda" albo jako „przedsięwzięcie, którego wynik jest niepewny", albo „odważenie

[10] Zob. wyrok NSA z 13.02.2018 r., II OSK 1824/17, LEX nr 2477162.

[11] *Hedging i nowoczesne usługi finansowe*, red. nauk. M. Biegański, A. Janc, Poznań 2001, s. 9.

[12] J. Głuchowski, *Leksykon finansów*, Warszawa 2021, s. 266.

[13] K. Czerwonka, M. Cież, M. Kowal, *Ryzyko*, Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Ryzyko#cite_note-1 (dostęp: 21.02.2022 r.).

się na takie niebezpieczeństwo”[14]. W literaturze przedmiotu dostrzega się różny wymiar ryzyka w zależności od kontekstu, w którym ryzyko to występuje[15]. W definiowaniu ryzyka można z jednej strony eksponować jego skutki, z drugiej zaś – nieosiągnięcie zamierzonego celu[16]. Ryzyko postrzegane jest bowiem jako prawdopodobieństwo wystąpienia sytuacji odmiennej od oczekiwanej[17]. Na prawdopodobieństwo wystąpienia określonego zdarzenia w kontekście zbudowania definicji „ryzyka” wskazano przykładowo w Glosariuszu terminów dotyczących kontroli i audytu w administracji publicznej[18]. W pojęciu ryzyka może zawierać się niedobór informacji o poszczególnych elementach relacji przyczyna–skutek, przez co ryzyko można również określać jako deficyt informacji o możliwości osiągnięcia określonego celu lub celów[19].

W kontekście prowadzonej działalności[20], w tym działalności gospodarczej, ryzyko powinno definiować się w dwojaki sposób. Z jednej strony ryzyko można postrzegać jako możliwość nieosiągnięcia zakładanego efektu[21]. W tym kontekście ryzyko postrzegane jest jako zagro-

---

[14] W. Doroszewski, *Słownik języka polskiego*, https://doroszewski.pwn.pl/ (dostęp: 15.01.2022 r.).

[15] P. Kokot-Stępień, *Identyfikacja ryzyka jako kluczowy element zarządzania ryzykiem w przedsiębiorstwie*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego” nr 855, „Finanse, Rynki Finansowe, Ubezpieczenia” 2015/74, t. 1, s. 533.

[16] A. Zachorowska [w:] *Zarządzanie ryzykiem inwestycyjnym* [w:] *Wybrane procesy zarządzania w przedsiębiorstwach i instytucjach publicznych*, red. D. Wielgórka, Częstochowa 2013, s. 11.

[17] K. Czerwonka, M. Cież, M. Kowal, *Ryzyko…*

[18] *Glosariusz terminów dotyczących kontroli i audytu w administracji publicznej*, Warszawa 2005, s. 34, tinyurl.com/MF-ryzyko (dostęp: 22.01.2022 r.).

[19] T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Warszawa 2008, s. 54.

[20] W literaturze przedmiotu wskazano na „ryzyko” jako element systemu zarządzania zarówno w działalności podmiotów publicznych, jak i prywatnych (A. Cieślik [w:] M. Jagielski, *Dokumentacja ochrony danych osobowych ze wzorami*, Warszawa 2019, s. 61).

[21] Ch. Poszwiński proponuje postrzeganie i ocenę ryzyka w relacji do niepożądanego rezultatu danej czynności. Wskazuje na zależność pomiędzy zwiększaniem się zakresu przetwarzanych danych osobowych a wzrostem ryzyka. Autor ten nie dostrzega jednak szerszego ujęcia ryzyka, w tym także jako szansy dającej możliwość uzyskania efektu odmiennego od oczekiwanego (Ch. Poszwiński, *Podejście oparte na ryzyku w procesie przetwarzania danych osobowych*, Wrocław 2021, s. 31).

żenie. Z drugiej strony – jako szansę dającą możliwość uzyskania efektu odmiennego od oczekiwanego. W tym przypadku ryzyko postrzegane jest w ujęciu negatywnym albo pozytywnym[22], tzn. jako zagrożenie lub szansa[23]. W ujęciu negatywnym ryzyko rozumiane jest jako możliwość poniesienia straty bądź nieosiągnięcia zakładanego celu[24].

Zagrożenie jest to możliwość wystąpienia określonych strat, ustalana dla sytuacji powstałej po zajściu pojedynczego zdarzenia niepożądanego w rozpatrywanym systemie człowiek–technika–środowisko. Jest to sytuacja niebezpieczna, w której występuje obiekt mogący doznać szkody lub obiekt, który może ponieść stratę w efekcie uaktywnienia się niebezpieczeństwa. Strata odnoszona jest do przedmiotów, które w wyniku niebezpiecznego zdarzenia mogą ulec uszkodzeniu lub zniszczeniu. Z kolei szkoda lub krzywda odnosi się do człowieka[25].

Zagrożenie może być spowodowane różnymi przyczynami:

1) wpływem czynników środowiska o charakterze negatywnym;
2) błędami człowieka, w tym błędami sterowania w odniesieniu do urządzeń;
3) wadliwym działaniem urządzenia, na skutek uszkodzeń jego podzespołów.

W niektórych stanowiskach prezentowanych w literaturze przedmiotu powyższe cechy ryzyka mogą wystąpić jednocześnie, tzn. ryzyko określane jest jako zagrożenie nieosiągnięcia zamierzonych celów lub prawdopodobieństwo wystąpienia negatywnych skutków[26].

---

[22] Na pozytywne ujęcie ryzyka jako szansy wskazują także E. Bielak-Jomaa, D. Lubasz [w:] *Analiza ryzyka i bezpieczeństwo danych w kancelariach prawnych*, red. D. Lubasz, Warszawa 2021, s. 29.

[23] K. Jajuga, *Koncepcja ryzyka i proces zarządzania ryzykiem – wprowadzenie* [w:] *Zarządzanie ryzykiem*, red. K. Jajuga, Warszawa 2009, s. 5 i 6.

[24] A. Zachorowska, Z. Ostraszewska, *Procesy decyzyjne podmiotów gospodarczych w warunkach ryzyka i niepewności* [w:] *Wybrane problemy zarządzania w podmiotach gospodarczych*, red. Z. Ostraszewska, A. Wójcik-Mazur, Częstochowa 2012, s. 10.

[25] A. Terelak-Tymczyna, *Zarządzanie bezpieczeństwem*, Szczecin 2014.

[26] M. Borusiński, A. Lipczyński, *Pojęcie, rodzaje oraz zarządzanie ryzykiem bankowym*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej" 2013/3(7), s. 29.

W ramach ujęcia pozytywnego przedsiębiorca uzyskuje zwiększoną korzyść, obejmującą premię za podejmowane ryzyko[27]. W ujęciu pozytywnym ryzyka, tzn. uwzględniając jego pozytywną rolę, przedsiębiorca ma możliwość uzyskania większych korzyści, podejmując działalność obarczoną tym ryzykiem.

W ujęciu ryzyka jako zagrożenia przedsiębiorca podejmuje środki zaradcze mające na celu jego zmniejszenie[28]. Środki zaradcze, zastosowane w sposób usystematyzowany jako pakiet działań dążących do osiągnięcia zamierzonego stanu bezpieczeństwa, nazywa się zarządzaniem bezpieczeństwem. Bezpieczeństwo jest pojęciem przeciwnym do pojęcia ryzyka. Jest to stan braku zagrożenia. Skuteczność działań na rzecz bezpieczeństwa jest wyrażana stopniem obniżenia poziomu ryzyka[29]. Działania te dążą do minimalizacji prawdopodobieństwa wystąpienia zdarzeń niepożądanych oraz stwarzają możliwość do jego kontrolowania i monitorowania poprzez identyfikację zagrożeń oraz ocenę występującego ryzyka. Zarządzanie bezpieczeństwem jest to identyfikacja, ocena i ustalenie priorytetów wystąpienia ryzyka poprzez takie koordynowanie działaniami w przedsiębiorstwie, aby zminimalizować, monitorować i kontrolować prawdopodobieństwo wystąpienia zjawisk niepożądanych[30].

W odniesieniu do transportu kolejowego prawodawca unijny zdefiniował ryzyko w art. 3 dyrektywy 2004/49/WE[31] jako częstotliwość wypadków i incydentów prowadzących do szkody (spowodowanej zagrożeniem) oraz stopień powagi tej szkody. Ryzyko to potencjalna

[27] K. Jajuga, *Koncepcja ryzyka*…, s. 14.

[28] P. Kokot-Stępień, *Identyfikacja ryzyka*…, s. 533.

[29] E. Wyraz, M. Szkoda, *Wymagania formalnoprawne oceny ryzyka w transporcie*, „Autobusy” 2017/12, s. 1431.

[30] A. Terelak-Tymczyna, *Zarządzanie bezpieczeństwem*…

[31] Na podstawie art. 34 dyrektywy 2016/798 utraciła moc dyrektywa 2004/49/WE. W pkt 2 załącznika III do dyrektywy 2016/798 zawarta została definicja „oceny ryzyka”. Zgodnie z nią jest to ustrukturyzowane podejście do oceny ryzyka związanego z utrzymaniem pojazdów, w tym ryzyka wynikającego bezpośrednio z procesów operacyjnych i działań innych organizacji lub osób, oraz określanie właściwych środków kontroli ryzyka.

możliwość urealnienia się zagrożenia[32]. Ryzyko zdefiniowane zostało również jako kombinacja prawdopodobieństwa aktywizacji zagrożenia w zdarzeniu niepożądanym i spowodowanych w związku z tym strat (szkód). Najczęściej jest to iloczyn poziomu prawdopodobieństwa aktywizacji zagrożenia w zdarzeniu niepożądanym i poziomu spowodowanych w związki z tym strat (szkód)[33].

Ryzyko jest to możliwość pojawienia się określonych strat (szkód) w rozważanym systemie człowiek–technika–otoczenie w określonym czasie jego funkcjonowania. W tym kontekście ryzyko można rozpatrywać na dwa sposoby. Po pierwsze, poprzez zastosowanie definicji dystrybucyjnej, w której ryzyko jest związane z wielkością możliwego rozkładu wyników. Po drugie, poprzez zastosowanie definicji parametrycznej, związanej z prawdopodobieństwem powstania straty i jej wielkości.

Można także wyróżnić trzy rodzaje definicji ryzyka, zwane definicjami parametrycznymi. Po pierwsze, ryzyko odnosi się do prawdopodobieństwa powstania straty. Po drugie, ryzyko jest tym większe, im większa może być strata w wyniku podjętego działania. Po trzecie, ryzyko jest to iloczyn prawdopodobieństwa poniesienia straty i jej wielkości. Ryzyko = (szansa zaistnienia, czyli prawdopodobieństwo) × (konsekwencje – czyli strata)[34]. Ryzyko jest scenariuszem opisującym zdarzenie i jego konsekwencje, oszacowanym pod względem powagi i prawdopodobieństwa jego wystąpienia[35].

W celu dalszych rozważań zostało przyjęte rozumienie ryzyka w znaczeniu negatywnym, jako prawdopodobieństwo wystąpienia zagrożenia w zdarzeniu niepożądanym i powstałych w związku z tym negatywnych skutków dla człowieka lub rzeczy. Zagrożenie to zbiór

[32] M. Jedynak, S. Młynarski, A. Sowa, *Ryzyko i jego miary w transporcie kolejowym*, „Logistyka" 2015/6, s. 1071–1085.

[33] A. Kadziński, A. Gill, *Integracja pojęć* [w:] *Zintegrowany system bezpieczeństwa transportu*, t. 2, *Uwarunkowania rozwoju integracji systemów bezpieczeństwa transportu*, red. R. Krystek, Warszawa 2009, s. 285–288.

[34] A. Terelak-Tymczyna, *Zarządzanie bezpieczeństwem…*

[35] Zob. Wytyczne GrArt. 29 WP 248v1, s. 7.

uwarunkowań, jakie mogą doprowadzić do wystąpienia ciągu zdarzeń wpływających niekorzystnie na ludzi, obiekty i ich otoczenie[36]. W kontekście analizy ryzyka w RODO należy zawęzić powyższe rozumienie tego pojęcia do prawdopodobieństwa wystąpienia zagrożenia w zdarzeniu niepożądanym i powstałych w związku z tym negatywnych skutków dla człowieka[37].

3. Zastosowanie konstrukcji konkretyzacji obowiązków prawnych w oparciu o kryterium ryzyka w wybranych aktach prawnych

Prawodawca unijny **oparł RODO na ryzyku w dwóch aspektach**. Po pierwsze, ryzyko występuje jako jedno z kryteriów wykorzystywanych do konkretyzacji obowiązku prawnego administratora do wdrożenia środków technicznych i organizacyjnych w zakresie bezpieczeństwa przetwarzania danych osobowych. Po drugie, ryzyko, przy uwzględnieniu jego skali, wykorzystywane jest do określenia obowiązków administratora związanych z naruszeniem danych osobowych, jak również ze złożeniem wniosku w sprawie przeprowadzenia procesu konsultacji w trybie art. 36 RODO[38].

Prawodawca unijny powiązał obowiązki prawne związane z zapewnieniem bezpieczeństwa przetwarzania danych osobowych m.in. z ryzykiem naruszenia praw i wolności osób fizycznych, których dane dotyczą. Prawodawca unijny nie definiuje ryzyka w RODO, nadając mu jednocześnie znaczenie normatywne, jak również nie określa kryteriów jego ustalania. Obowiązkiem adresata normy prawnej jest

[36] M. Jedynak, S. Młynarski, A. Sowa, *Ryzyko…*

[37] M. Gumularz. T. Izydorczyk podobnie wskazują na stan mogący negatywnie, wpływać na człowieka, którego dane osobowe są przetwarzane (zob. M. Gumularz. T. Izydorczyk [w:] *Ochrona danych osobowych. Ocena ryzyka i skutków. Metody i praktyczne przykłady*, red. M. Gumularz, T. Izydorczyk, Warszawa 2021, s. 45).

[38] Por. E. Bielak-Jomaa, D. Lubasz [w:] *Analiza ryzyka…*, red. D. Lubasz, s. 35. Autorzy ci co prawda nie dokonują takiego wyróżnienia, ale wskazują na zagadnienia, które mieszczą się w ramach wyróżnionych aspektów.

w takim przypadku wdrożenie odpowiedniej metodyki kwalifikacji ryzyka i jego oceny. Dopiero na tej podstawie możliwe jest skonkretyzowanie obowiązku prawnego, polegającego na zastosowaniu odpowiednich środków technicznych i organizacyjnych, które mają na celu zmniejszenie tego ryzyka. Także w tym przypadku prawodawca unijny nie określa, jakie czynności faktyczne i prawne powinny zostać podjęte. Wdrażane środki techniczne powinny być natomiast adekwatne do stwierdzonego ryzyka naruszenia praw i wolności osób fizycznych. Zgodnie z art. 32 ust. 1 RODO jednym z czynników, jakie należy brać pod uwagę przy doborze właściwych środków technicznych i organizacyjnych, jest stan wiedzy technicznej, który powinno się oceniać z uwzględnieniem warunków rynkowych, w szczególności dostępności i akceptowalności rynkowej danego rozwiązania technicznego W tym zakresie pomocne może być posługiwanie się dedykowanymi normami technicznymi[39]. Przykładowo ENISA w wytycznych dotyczących bezpieczeństwa przetwarzania danych osobowych z 2016 r.[40], z uwzględnieniem normy PN-EN ISO/IEC 27001:2017-06 (w wersji z 2013 r.) oraz RODO, w ramach kontroli dostępu i uwierzytelniania rekomenduje stosowanie mechanizmu uwierzytelnia dwuetapowego dla systemów obejmujących dostęp do danych osobowych. Zgodnie z podejściem opartym na ryzyku, wynikającym m.in. z art. 25 ust. 1 rozporządzenia 2016/679, wybór odpowiedniego środka uwierzytelniania powinien opierać się na ocenie ryzyka realizowanej za jej pomocą transakcji lub usługi[41]. Punktem odniesienia do wdrożenia odpowiednich środków technicznych i organizacyjnych mogą być również rekomendacje instytutów standaryzacyjnych znajdujących się poza obszarem Unii Europejskiej, w tym np. Narodo-

[39] Szerzej na temat pojęcia „norma techniczna" – zob. A. Krasuski, *Chmura obliczeniowa. Prawne aspekty zastosowania*, Warszawa 2018, s. 157.

[40] Guidelines for SMEs on the security of personal data processing, https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personaldata-processing.

[41] Przykładowo Norma PN-ISO/IEC 29115:2017-07 („Technika informatyczna – Techniki bezpieczeństwa – Ramy uzasadnionej pewności poziomów uwierzytelnienia"), podobnie jak motywy 75 czy 85 rozporządzenia 2016/679, wskazuje możliwe konsekwencje i skutki niepowodzenia uwierzytelnienia w zależności od zastosowanego poziomu, m.in. nieuprawnione ujawnienie poufnych informacji czy strata finansowa.

wego Instytutu Standaryzacji i Technologii (ang. National Institute of Standards and Technology, NIST)[42]. Również Prezes UODO wskazuje, że dobór właściwego środka uwierzytelniającego powinien być poprzedzony analizą ryzyka i poddawany ciągłym przeglądom[43]. Wykonanie obowiązku prawnego wynikającego z normy prawnej określonej w RODO, a dotyczącej bezpieczeństwa przetwarzania danych osobowych, jest procesem złożonym dla adresata normy, z której obowiązek ten wynika. Jest to także proces złożony dla Prezesa UODO w kontekście oceny wykonania tego obowiązku.

Podmioty, które przetwarzają dane osobowe, zobowiązane są na podstawie RODO nie tylko do zapewnienia zgodności z obowiązkiem, określonym w tym rozporządzeniu 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[44].

Konkretyzacja obowiązków prawnych zawartych w normach za pośrednictwem kryteriów o charakterze normatywnym w skutkach różni się od samoregulacji, co wynika z następujących względów: cechą samoregulacji, w tym wyrażającą się poprzez tworzenie kodeksów postępowania, jest dobrowolność postępowania, która nie występuje w przypadku konkretyzacji obowiązku prawnego. W literaturze przedmiotu wskazuje się, że zarówno bowiem źródło powstania ko-

[42] Zob. NIST 800-63B: Wytyczne dotyczące tożsamości cyfrowej: uwierzytelnianie i zarządzanie cyklem życia aplikacji (ang. Digital Identity Guidelines: Authentication and Lifecycle Management) [3], https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf (dostęp: 25.02.2022 r.).

[43] Zob. decyzja Prezesa UODO z 10.09.2019 r., ZSPR.421.2.2019, https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 (dostęp: 1.08.2022 r.).

[44] Wyrok WSA w Warszawie z 3.09.2020 r., II SA/Wa 2559/19, LEX nr 3077973.

deksów postępowania, jak i ich stosowanie i kontrola przestrzegania zawartych w nim norm są oparte na dobrowolnym przyjęciu przez sygnatariuszy kodeksu postępowania[45]. Tego rodzaju dobrowolnie przyjmowane regulacje, z jednej strony umożliwiają doprecyzowanie ogólnych przepisów prawa, z drugiej zaś – uzupełniają obowiązujące prawo tam, gdzie brak regulacji szczegółowych[46].

W prawie unijnym ryzyko jako kryterium konkretyzacji obowiązku prawnego zostało również przewidziane w innych obszarach regulacji niż ochrona danych osobowych. Przykładowo należy wskazać na regulacje unijne dotyczące **obszaru ochrony zdrowia publicznego**, w tym na decyzję 1082/2013/UE. Jeśli weźmiemy pod uwagę cechy decyzji jako aktu prawa wtórnego, jest to akt prawny wiążący co do wszystkich przepisów w nich zawartych, zaś wykonywanie decyzji nie może być ograniczane aktami prawa krajowego. Jej adresatem może być każdy podmiot prawa (państwa członkowskie, przedsiębiorcy czy inne podmioty prawa). Jeżeli decyzja jest adresowana do państw członkowskich, to wiąże wszystkie organy państwa. W związku z powyższym decyzja może kreować obowiązki prawne dla państw członkowskich.

Przedmiot decyzji 1082/2013/UE obejmuje określenie zasad współpracy i koordynacji między państwami członkowskimi, aby usprawnić zapobieganie rozprzestrzenianiu się przez granice państw członkowskich poważnych chorób u ludzi i wspieranie kontroli tego rozprzestrzeniania się oraz zwalczanie innych poważnych transgranicznych zagrożeń zdrowia, w celu przyczynienia się do wysokiego poziomu ochrony zdrowia publicznego w Unii[47]. Jak wynika z motywu 21 tej decyzji, państwa członkowskie odpowiadają za zarządzanie na szczeblu krajowym kryzysami w dziedzinie zdrowia publicznego. Jednak środki podejmowane indywidualnie przez państwa członkowskie mogą zaszkodzić interesom innych państw członkow-

[45] M. Sieradzka [w:] *Komentarz do dyrektywy 2005/29/WE o nieuczciwych praktykach rynkowych* [w:] M. Sieradzka, *Ustawa o przeciwdziałaniu nieuczciwym praktykom rynkowym. Komentarz*, Warszawa 2008, art. 2.

[46] A. Mokrysz-Olszyńska, *Swoboda promocji a ochrona przed nieuczciwymi praktykami handlowymi w projektach prawa Unii Europejskiej*, PiP 2005/2, s. 57.

[47] Zob. art. 1 ust. 2 decyzji 1082/2013/UE.

skich, jeśli będą niespójne ze sobą lub oparte na rozbieżnych ocenach ryzyka. Cel koordynacji reagowania na poziomie unijnym powinien zatem dążyć do zagwarantowania m.in. tego, że środki podejmowane na poziomie krajowym będą proporcjonalne i ograniczone do ryzyka dla zdrowia publicznego związanego z poważnymi transgranicznymi zagrożeniami zdrowia i że nie będą sprzeczne z prawami i zobowiązaniami określonymi TFUE, takimi jak dotyczące ograniczenia swobody podróżowania i handlu.

Prawodawca unijny wprowadził w decyzji 1082/2013/UE definicję „środka ochrony zdrowia publicznego"[48]. Definicja ta dotyczy decyzji lub czynności umożliwiających realizację celów w postaci zwalczania poważnego ryzyka dla zdrowia publicznego lub zmniejszanie ich wpływu na zdrowie publiczne. Określony w tej decyzji obowiązek prawny do podejmowania przez państwa członkowskie czynności w zakresie koordynacji działań w zakresie reagowania krajowego na poważne transgraniczne zagrożenie zdrowia, jak również w zakresie komunikacji w zakresie ryzyka i sytuacji kryzysowych, wymaga konkretyzacji za pośrednictwem kryterium ryzyka[49].

Kształtowanie obowiązków prawnych w prawie unijnym poprzez odwołanie do kryterium ryzyka ma miejsce również w regulacjach prawnych dotyczących **bezpieczeństwa żywności**. W tym zakresie należy wskazać na rozporządzenie 178/2002, które nakłada na przedsiębiorstwa spożywcze m.in. obowiązek zastosowania środków, jakie w skutkach będą odpowiednie do zapobiegnięcia ryzyka dla konsumenta związanego z żywnością[50]. Podobna regulacja została przewidziana dla podmiotów działających na rynku pasz[51]. Na przykładzie tego rozporządzenia można dostrzec złożoność regulacji dotyczącej stosowania kryterium ryzyka, w tym definicji ryzyka, jak również definicji powiązanych, co przyczynia się do stopnia skomplikowania aktu konkretyzacji obowiązku prawnego w zakresie konkretyzacji

[48] Art. 3 pkt f decyzji 1082/2013/UE.
[49] Zob. art. 11 ust. 1 decyzji 1082/2013/UE.
[50] Zob. art. 19 ust. 3 rozporządzenia 178/2002.
[51] Zob. art. 20 ust. 3 rozporządzenia 178/2002.

obowiązku prawnego w zakresie zastosowania adekwatnych środków technicznych i organizacyjnych i jego konkretyzacji.

Rozporządzenie 178/2002 zawiera definicję ryzyka, określonego jako niebezpieczeństwo zaistnienia negatywnych skutków dla zdrowia oraz dotkliwość takich skutków w następstwie zagrożenia[52]. Ponadto w rozporządzeniu 178/2002 prawodawca unijny definicjami legalnymi objął pojęcie „analiza ryzyka", jak również poszczególne elementy definicji analizy ryzyka. Za „analizę ryzyka" prawodawca unijny uznał proces składający się z trzech powiązanych elementów: oceny ryzyka, zarządzania ryzykiem i informowania o ryzyku[53]. Z kolei „ocena ryzyka" to proces wsparty naukowo, składający się z czterech etapów: identyfikacji zagrożenia, charakterystyki niebezpieczeństwa, oceny ekspozycji i charakterystyki ryzyka[54]. Pojęcie „zarządzanie ryzykiem" oznacza proces różniący się od oceny ryzyka, polegający na zbadaniu alternatywy polityki w porozumieniu z zainteresowanymi stronami, wzięciu pod uwagę oceny ryzyka i innych prawnie uzasadnionych czynników, i w razie potrzeby – na wybraniu stosownych sposobów zapobiegania i kontroli[55]. Z zastosowania definicji zarządzania ryzykiem wynika, że zakres zastosowanych środków zaradczych ma być adekwatny do zidentyfikowanego ryzyka. Miernikiem konkretnego obowiązku prawnego jest wynik przeprowadzonej analizy ryzyka. Z kolei pojęcie „informowanie o ryzyku" zostało zdefiniowane jako interaktywna wymiana informacji i opinii podczas procesu analizy ryzyka, dotycząca zagrożeń i ryzyka, czynników związanych z ryzykiem i postrzeganiem ryzyka, między oceniającymi ryzyko, zarządzającymi ryzykiem, konsumentami, przedsiębiorstwami paszowymi i spożywczymi, środowiskiem naukowym i innymi zainteresowanymi stronami, z uwzględnieniem wyjaśnienia wniosków z oceny ryzyka i powodów decyzji w zakresie zarządzania ryzykiem.

[52] Zob. art. 3 pkt 9 rozporządzenia 178/2002.
[53] Zob. art. 3 pkt 10 rozporządzenia 178/2002.
[54] Zob. art. 3 pkt 11 rozporządzenia 178/2002.
[55] Zob. art. 3 pkt 12 rozporządzenia 178/2002.

Powiązanie konkretyzacji obowiązku prawnego polegającego na zastosowaniu środków zaradczych z ryzykiem jest odzwierciedlone także w przepisach unijnych odnoszących się do **zarządzania kryzysowego, jak również zwalczania przestępczości**. Działania te dotyczą m.in. zarządzania ryzykiem związanym z funkcjonowaniem infrastruktury krytycznej, zagrożenia powodziowego, użycia niebezpiecznych substancji czy przeciwdziałaniem aktom terroryzmu. W tym kontekście należy wskazać na dyrektywę 2008/114/WE, dotyczącą procedury rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz wspólnego podejścia państw członkowskich do oceny potrzeb w zakresie poprawy ochrony takiej infrastruktury w celu lepszej ochrony ludności. W ramach procedury wskazano na konieczność opracowywania przez państwa członkowskie planów ochrony infrastruktury, dokonywania analizowania ryzyka oraz rozpoznawania, selekcji i ustalenia hierarchii ważności środków przeciwdziałania. W art. 2 lit. e dyrektywy 2008/114/WE prawodawca unijny zawarł definicję ochrony, zgodnie z którą pojęcie to obejmuje wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków. Zamiarem ustawodawcy unijnego było zatem powiązanie rodzaju i zakresu działań dotyczących infrastruktury krytycznej w zakresie, w jakim działania te będą adekwatne do stwierdzonego ryzyka, aby co najmniej minimalizować jego wystąpienie. Konkretyzacja obowiązku prawnego wymaga analizy ryzyka. Pojęcie to zostało zdefiniowane w art. 2 lit. c dyrektywy 2008/114/WE i oznacza uwzględnianie stosownych metod postępowania w przypadku zaistnienia zagrożeń, aby ocenić słabe punkty i potencjalne skutki zakłócenia lub zniszczenia infrastruktury krytycznej.

Regulacje unijne w zakresie ochrony infrastruktury krytycznej, przewidziane w dyrektywie 2008/114/WE, zostały implementowane do polskiego porządku prawnego w ustawie o zarządzaniu kryzysowym. Jako ochronę infrastruktury krytycznej należy rozumieć działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom, oraz ograniczenia i neutra-

lizacji ich skutków, a także szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie[56].

Ustawa o zarządzaniu kryzysowym przewiduje tworzenie Krajowego Planu Zarządzania Kryzysowego oraz wojewódzkich, powiatowych i gminnych planów zarządzania kryzysowego. Obejmują one m.in. ochronę infrastruktury krytycznej i przyjęcie Narodowego Programu Ochrony Infrastruktury Krytycznej[57]. W ustawie tej ustawodawca powiązał konkretyzację obowiązku prawnego z kryterium ryzyka w ramach regulacji dotyczącej tych planów zarządzania kryzysowego. Ich integralnym elementem muszą być m.in. charakterystyki zagrożeń oraz oceny ryzyka ich wystąpienia (w tym dotyczące infrastruktury krytycznej), a także mapy ryzyka i mapy zagrożeń. Na potrzeby Krajowego Planu Zarządzania Kryzysowego ministrowie kierujący działami administracji rządowej, kierownicy urzędów centralnych oraz wojewodowie sporządzają raport o zagrożeniach bezpieczeństwa narodowego. Raport taki powinien również zawierać analizy najważniejszych zagrożeń przez stworzenie mapy ryzyka. Sposoby realizacji powyższych obowiązków zostały wskazane w rozporządzeniu Rady Ministrów[58].

W obszarze prawnej regulacji zarządzania kryzysowego należy także wskazać na dyrektywę 2007/60/WE, w której prawodawca unijny określił ramy prawne dla oceny ryzyka powodziowego i zarządzania nim. W oparciu o zidentyfikowane ryzyko określane są środki mające na celu ograniczenie negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej, związanych z powodziami na terytorium Unii Europejskiej. W motywie 11 preambuły dyrektywy wskazuje się, że na pewnych

[56] Zob. art. 3 pkt 3 ustawy z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U. z 2022 r. poz. 261 ze zm.).

[57] Zob. art. 5 ustawy o zarządzaniu kryzysowym.

[58] Zob. rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz.U. Nr 83, poz. 542) i rozporządzenie Rady Ministrów z 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz.U. Nr 83, poz. 541).

obszarach Unii Europejskiej ryzyko powodziowe może zostać uznane za nieznaczne, przykładowo na obszarach słabo zaludnionych, niezaludnionych lub obszarach o ograniczonej wartości gospodarczej lub ekologicznej. W każdym obszarze dorzecza lub w każdej jednostce zarządzającej powinno się ocenić ryzyko powodziowe i konieczność dalszych działań, takich jak ocena możliwości łagodzenia skutków powodzi. Zgodnie z art. 2 pkt 2 dyrektywy 2007/60/WE ryzyko powodziowe to kombinacja prawdopodobieństwa wystąpienia powodzi i związanych z powodzią potencjalnych negatywnych konsekwencji dla zdrowia ludzkiego, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej. Wpływ na ustalone ryzyko mają plany zarządzania ryzykiem powodziowym, określone w rozdziale IV dyrektywy 2007/60/WE. Państwa członkowskie zostały zobligowane do opracowania planów zarządzania ryzykiem powodziowym obejmujących wnioski z oceny ryzyka, mapy ryzyka powodziowego i zestawienie środków służących osiągnięciu odpowiednich celów zarządzania ryzykiem powodziowym.

Transpozycja dyrektywy 2007/60/WE do polskiego porządku prawnego nastąpiła za sprawą ustawy – Prawo wodne. Zarządzanie ryzykiem powodziowym uregulowane zostało w rozdziale 1 działu IV tej ustawy. Jako cel zarządzania ryzykiem powodziowym w ustawie – Prawo wodne wskazano ograniczenie potencjalnych negatywnych skutków powodzi dla życia i zdrowia ludzi, środowiska, dziedzictwa kulturowego oraz działalności gospodarczej[59]. Jako ryzyko powodziowe wskazano kombinację prawdopodobieństwa wystąpienia powodzi i negatywnych skutków powodzi, a jako czynnik niezbędny do prowadzenia ochrony przed powodziami wskazano mapy ryzyka powodziowego oraz plany zarządzania ryzykiem powodziowym[60]. Wskazano sposób oceny ryzyka, tzn. prawdopodobieństwo powinno zostać oszacowane w oparciu o dane historyczne[61], a negatywne skutki odniesione do szeregu określonych parametrów. Przewidziano dwa poziomy analizy ryzyka powodziowego: wstępną ocenę ryzyka

[59] Zob. art. 16 pkt 4 pr. wod.
[60] Zob. art. 16 pkt 48 pr. wod.
[61] Zob. art. 371 pr. wod.