PME
4/2017

PRAWO Mediów Elektronicznych

www.ksiegarnia.beck.pl

ISSN 2082-100x

Cena 65 zł (w tym 5% VAT)

C·H·BECK

PME

4/2017

Adres redakcji:
Uniwersytet Wrocławski, Wydział Prawa, Administracji i Ekonomii,
Centrum Badań Problemów Prawnych i Ekonomicznych
Komunikacji Elektronicznej
ul. Uniwersytecka 22/26, 51-145 Wrocław
e-mail: pme@beck.pl

C·H·BECK

Wydawca:
Wydawnictwo C.H. Beck
ul. Bonifraterska 17
00-203 Warszawa

tel.: 22 33 77 600
fax: 22 33 77 602
www.czasopisma.beck.pl

Nakład: 250 egz.

Spis treści

Contents

C·H·BECK

Szanowni Państwo,

z przyjemnością przedstawiam czwarty numer kwartalnika Prawo Mediów Elektronicznych w 2017 r. Obejmuje on swoim zakresem teksty dotyczące ochrony danych osobowych, w szczególności problemów, które się pojawiają w związku z wejściem w życie unijnego rozporządzenia ogólnego o ochronie danych osobowych (RODO). Przykładowo są to artykuły: *G. Sibigi* na temat skargi do organu nadzorczego według RODO; *D*. *Sybilskiego* o ponownym wykorzystaniu informacji sektora publicznego w kontekście konieczności zapewnienia ochrony danych osobowych według RODO oraz *M. Bieniasa* o zasadzie ograniczenia przechowywania danych na gruncie RODO. Niniejszy numer zawiera także opracowania dotyczące tzw. trollingu prawnoautorskiego jako formy nadużycia prawa podmiotowego (*A. Skibińskiej*), a także artykuł *J. Adamczyk* o nowych formach szczególnych czynności prawnych w Kodeksie cywilnym w zakresie dokumentowej i elektronicznej w kontekście rozporządzenia e-IDAS. W tym wydaniu zamieszczono także sprawozdanie z konferencji naukowej Legal Innovation, która odbyła się we Wrocławiu 21–22.4.2017 r.

Zapraszam do publikacji na łamach Prawa Mediów Elektronicznych oraz do kontaktu z nami pod adresem: pme@beck.pl.

Zachęcam do lektury,
prof. dr hab. *Jacek Gołaczyński*

Sprawozdanie: Międzynarodowa Konferencja Naukowa Legal Innovation, Wrocław, 21–22.4.2017 r.

dr *Maria Kaczorowska*[1]

Rozwój nowoczesnych technologii, znajdujących coraz szersze zastosowanie w wymiarze sprawiedliwości i administracji publicznej, wpływa w istotny sposób na kształt praktyki prawniczej. Informatyzacja postępowań sądowych i funkcjonowania urzędów, wykorzystanie nowych metod komunikacji elektronicznej oraz narzędzi informatycznych prowadzą do przyspieszenia procedur i ułatwienia dostępu do informacji prawnej, przyczyniając się do usprawnienia wykonywania zawodów prawniczych. Postęp technologiczny niesie ze sobą również liczne wyzwania dla uczestników obrotu prawnego, związane m.in. z ochroną danych osobowych czy udostępnianiem informacji publicznej.

Okazję do omówienia dotychczasowych osiągnięć i aktualnych tendencji rozwojowych w dziedzinie innowacyjnych rozwiązań technologicznych wykorzystywanych w sądownictwie i działalności organów administracji publicznej w Polsce i w innych krajach europejskich, a także problemów praktycznych uwidaczniających się na tle procesów informatyzacji stanowiła Międzynarodowa Konferencja Naukowa *Legal Innovation*, która odbyła się 21–22.4.2017 r. na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego. Konferencja została zorganizowana przez Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej (CBKE) działające na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz Sąd Apelacyjny we Wrocławiu we współpracy z Federacją Adwokatur Europejskich (*Fédération des Barreaux d'Europe*), Okręgową Izbą Radców Prawnych we Wrocławiu i Okręgową Radą Adwokacką we Wrocławiu. Obrady zgromadziły przedstawicieli nauki prawa, sędziów, adwokatów, radców prawnych i prawników zagranicznych.

Prezentowane podczas konferencji referaty zostały przygotowane przez specjalistów z dziedziny prawa nowych technologii, reprezentujących krajowe i zagraniczne ośrodki naukowe, takich jak Prof. em. Dr. Dr. h.c. *Wolfgang Kilian* (Uniwersytet Leibniza w Hanowerze), Prof. Dr. *Andreas Wiebe* (Uniwersytet im. Georga Augusta w Getyndze), doc. JUDr. *Radim Polčák*, Ph.D. (Uniwersytet Masaryka w Brnie), Dr. *Zsolt Balogh* (Uniwersytet Korwina w Budapeszcie), Dr. *Katalin Balogh* (Katolicki Uniwersytet w Leuven), dr hab. *Michał Bernaczyk* (Uniwersytet Wrocławski), prof. USz dr hab. *Kinga Flaga-Gieruszyńska* (Uniwersytet Szczeciński), prof. dr hab. *Jacek Gołaczyński* (Uniwersytet Wrocławski), prof. UO dr hab. *Dariusz Szostek* (Uniwersytet Opolski), dr *Wojciech Wiewiórowski* (zastępca Europejskiego Inspektora Ochrony Danych Osobowych), a także dr inż. *Kajetan Wojsyk* (Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie). Przewidziane zostały również wystąpienia polskich i zagranicznych prawników praktyków.

Rozpoczęcie obrad konferencji poprzedziło uroczyste otwarcie wystawy z okazji 35-lecia Okręgowej Izby Radców Prawnych we Wrocławiu. Celem wystawy była popularyzacja wiedzy o zasadach wykonywania zawodu radcy prawnego jako zawodu zaufania publicznego w Polsce.

Panele tematyczne objęte programem konferencji zostały poświęcone zagadnieniom technologii informatycznych wspierających pracę prawników oraz aktualnym zmianom w branży prawniczej:

- wykorzystaniu e-usług w pracy prawnika;
- ochronie danych osobowych i dostępowi do informacji publicznej;
- funkcjonowaniu elektronicznych biur podawczych w wybranych krajach, a także
- zastosowaniu technologii komunikacyjno-informacyjnych w postępowaniach sądowym i administracyjnym.

Ponadto zorganizowano warsztaty dotyczące usług chmury obliczeniowej (*cloud computing*).

W ramach podejmowanych w pierwszej części obrad konferencji rozważań nad kierunkami wykorzystania najnowszych rozwiązań technologicznych w praktyce prawniczej zwrócono uwagę na rolę, jaką w usprawnieniu postępowań sądowych odgrywają systemy elektronicznej rejestracji rozpraw i innowacyjne technologie głosowe służące do transkrypcji mowy. Znaczącym ułatwieniem w codziennej pracy profesjonalnych pełnomocników, a także sędziów jest ponadto możliwość korzystania z systemów informacji o prawie, oferujących dostęp do dokumentów prawnych, aktualizowanych pod kątem powołanych przepisów. Wśród poruszonych w referatach zagadnień uwzględnione zostały także praktyczne aspekty e-dowodów. Przybliżono ponadto regulację postępowania arbitrażowego w prawie litewskim.

[1] Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

W wystąpieniach poświęconych problematyce danych osobowych omówiono kwestie ochrony danych osobowych przy międzynarodowej wymianie informacji dotyczących postępowań karnych, jak również poddano analizie nową regulację rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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[2] z uwzględnieniem wynikających z niej wymagań dla systemów informatycznych. Zagadnienie dostępu do informacji publicznej zostało rozwinięte w referacie na temat dostępu do państwowych baz danych i oprogramowania oraz ich ponownego wykorzystywania w prawie polskim.

Kolejny panel pozwolił na skonfrontowanie założeń dalszej informatyzacji polskiego postępowania cywilnego, obejmującej umożliwienie składania pism procesowych za pośrednictwem elektronicznego biura podawczego[3], z doświadczeniami w zakresie wdrażania analogicznych rozwiązań w obcych porządkach prawnych – w Niemczech, we Włoszech, w Hiszpanii i we Francji. Nowe rozwiązania oparte na elektronicznej komunikacji z sądem mają służyć podniesieniu sprawności i efektywności postępowań sądowych. Podjęto również rozważania nad potencjalnymi korzyściami i zagrożeniami związanymi z upowszechnieniem się usług rejestrowanego doręczania elektronicznego.

Problematyka wykorzystania chmury obliczeniowej w działalności kancelarii prawnych w Polsce, UE i USA została przybliżona w ramach warsztatów, które przeprowadzili *Tomasz Grzegory* (Google) i adw. *Xawery Konarski* (Kancelaria Traple Konarski Podrecki i Wspólnicy). Technologia chmury, ciesząca się obecnie coraz większą popularnością, opiera się na przechowywaniu informacji na serwerach zewnętrznych i dostarczaniu ich jako usługi na życzenie klientów, co skutkuje zwiększeniem możliwości przetwarzania danych oraz obniżeniem kosztów funkcjonowania przedsiębiorstw. Jak zaznaczono, dostawcy usług chmurowych zapewniają klientowi autonomię w zarządzaniu dostępem do zasobów chmury.

Postępy w dziedzinie informatyzacji postępowań sądowych i rozwoju administracji elektronicznej (*e-government*) zostały przedstawione na przykładzie rozwiązań stosowanych w Polsce, a także m.in. na Węgrzech, w Bułgarii, Niemczech, Rumunii, jak również Australii. Jednym z poruszonych zagadnień o doniosłym znaczeniu z punktu widzenia usług świadczonych przez profesjonalnych pełnomocników było poświadczanie za zgodność z oryginałem dokumentów elektronicznych w postępowaniu sądowym i sądowoadministracyjnym. Problemy praktyczne mogą wiązać się z kwalifikacją dokumentów elektronicznych jako mających walor oryginału – spełniających kryteria autentyczności i integralności. W tym kontekście podkreślono wpływ rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (rozporządzenia eIDAS)[4], znajdującego zastosowanie w UE od 1.7.2016 r., na wykorzystywane metody identyfikacji elektronicznej. W obecnym stanie prawnym wprowadzona została m.in. zastępowalność podpisu własnoręcznego kwalifikowanym podpisem elektronicznym w skali europejskiej. Przedmiotem rozważań była ponadto rola interoperacyjności i uporządkowania rejestrów publicznych w funkcjonowaniu administracji elektronicznej. Współcześnie warunkiem efektywnej realizacji zadań przez podmioty publiczne jest zapewnienie wzajemnego współdziałania systemów teleinformatycznych, w których są prowadzone rejestry publiczne, i sprawnej wymiany danych między rejestrami.

Bogaty program konferencji *Legal Innovation*, uwzględniający analizę aktualnych trendów w dziedzinie wykorzystania nowych technologii w służbie wymiaru sprawiedliwości i administracji publicznej, pozwolił na podjęcie przez uczestników szerokiej dyskusji nad optymalnymi sposobami wdrażania nowatorskich rozwiązań technologicznych w celu faktycznej poprawy jakości usług oferowanych przez prawników.

Możliwość wymiany poglądów na temat zastosowań innowacyjnych technologii w dziedzinie prawa umów elektronicznych, prawa mediów elektronicznych, e-sądownictwa czy handlu elektronicznego przewidziano również dla młodych adeptów prawa w ramach Studencko-Doktoranckiego Panelu Międzynarodowej Konferencji Naukowej *Legal Innovation – Young Researchers*, zorganizowanego 20.4.2017 r.

[2] Dz.Urz. UE L Nr 119, s. 1.

[3] Możliwość wnoszenia pism procesowych drogą elektroniczną i dokonywania doręczeń elektronicznych przewidziano w ustawie z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. poz. 1311 ze zm.), która weszła w życie 8.9.2016 r. Zgodnie z art. 20 tej nowelizacji w okresie trzech lat od jej wejścia w życie dokonanie wyboru wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe oraz dalsze wnoszenie tych pism za pośrednictwem tego systemu jest dopuszczalne, jeżeli ze względów technicznych, leżących po stronie sądu, jest to możliwe. W powyższym terminie wszystkie sądy powinny umożliwić stronom wnoszenie pism procesowych za pomocą aplikacji „Elektroniczne Biuro Podawcze".

[4] Dz.Urz. UE L Nr 257, s. 73.

Skarga do organu nadzorczego oraz jej rozpatrzenie według ogólnego rozporządzenia o ochronie danych. Postępowanie w przedmiocie skargi osoby, której dane dotyczą

dr *Grzegorz Sibiga*[1]

Z punktu widzenia osoby, której dane dotyczą (podmiotu danych), istota regulacji prawnej ochrony danych osobowych sprowadza się do przyznania jej prawa do ochrony własnych danych osobowych. Taka osoba realizuje swoje uprawnienia wobec administratora jej danych, a gdy okaże się to nieskuteczne, ma prawo złożenia skargi do niezależnego organu administracyjnego ds. ochrony danych osobowych (organu nadzorczego). Zadaniem organu jest rozpatrzenie skargi, po to żeby w sytuacji stwierdzenia naruszenia prawa do ochrony danych doprowadzić środkami administracyjnymi do realizacji prawa. W tekście przedstawiam regulacje w tym zakresie zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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)[2], porównując je do dotychczasowych rozwiązań, obowiązujących do 25.5.2018 r., znajdujących się w dyrektywie 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[3] oraz w wykonującej dyrektywę polskiej ustawie z 29.8.2997 r. o ochronie danych osobowych[4].

Uwagi wstępne

W administracyjnoprawnej ochronie danych osobowych kluczowe znaczenie ma powiązanie prawa osoby fizycznej do ochrony jej danych osobowych (jako istoty regulacji[5]) z funkcjonowaniem organu administracyjnego właściwego w sprawach ochrony danych osobowych (organu nadzorczego), który, posługując się prawnymi formami działania administracji, w tym aktami administracyjnymi, zapewnia realizację tego prawa. W tym kontekście ochrona osoby, której dane dotyczą, polega również na tym, że może ona się zwrócić do organu nadzorczego o rozpatrzenie indywidualnej sprawy dotyczącej jej prawa do ochrony swoich danych osobowych. Chodzi o sytuację, gdy podmiot danych uważa, że naruszono jego prawo do ochrony danych i domaga się reakcji organu ds. ochrony danych polegającej na przywróceniu realizacji uprawnienia określonego prawem. Organ nadzorczy posiada zaś niezbędne kompetencje do stwierdzenia zasadności żądania podmiotu danych, a gdy potwierdzi naruszenia prawa, pozostaje uprawniony do skutecznej interwencji przywracającej stan zgodny z przepisami prawa.

Dlatego też instytucja skargi do organu ds. ochrony danych osobowych oraz obowiązek jej rozpatrzenia pełni jedną z podstawowych funkcji dla osoby, której dane dotyczą. Przyjęcie konstrukcji administracyjnoprawnej procesowej ochrony prawa do ochrony danych osobowych powinno w założeniu być korzystne dla skarżącego (osoby której dane dotyczą). Działania organu ds. ochrony danych osobowych (jako organu administracji publicznej prowadzącego postępowanie administracyjne) nie mogą się bowiem ograniczać do roli swoistego arbitra w sporze między osobą, której dane dotyczą, oraz adresatem obowiązków ochrony danych (przede wszystkim administratorem), ale powinny charakteryzować się aktywnością, wyspecjalizowanym działaniem i szerokim zakresem kompetencji. Organ, opierając się na zasadzie oficjalności, ustala stan faktyczny w zakresie przetwarzania danych osobowych, a w przypadku stwierdzenia naruszenia ochrony danych osobowych dobiera adekwatny środek korygujący naruszenie. W założeniu postępowanie organu nadzorczego powinno zakończyć się szybciej niż sprawa sądowa.

Tak ukształtowany mechanizm ochrony administracyjnoprawnej stanowi realizację postulatu, w tym wyrażonego w polskiej doktrynie już od 1980 r., aby organy administracji publicznej wyposażyć w kompetencje do władczego określania sytuacji prawnej jednostki w zakresie jej danych osobowych, co „stwarza konieczność zapewnienia odpowiedniej procedury kontrolnej, w związku z możliwością zniekształcenia informacji lub naruszenia sfery życia prywatnego”[6].

[1] Autor jest kierownikiem Zakładu Prawa Administracyjnego w Instytucie Nauk Prawnych PAN oraz adwokatem.

[2] Dz.Urz. UE L Nr 119, s. 1; dalej jako: ogólne rozporządzenie lub RODO.

[3] Dz.Urz. UE L Nr 281; dalej jako: dyrektywa 95/46/WE.

[4] T.j. Dz.U. z 2016 r. poz. 922 ze zm.; dalej jako: OchronaDanychU.

[5] Prawo każdej osoby do ochrony danych jej dotyczących przyznaje art. 16 ust. 1 Traktatu o Funkcjonowaniu Unii Europejskiej (TFUE). Również w jednym z pierwszych przepisów ogólnego rozporządzenia stwierdzono, że celem nowej regulacji unijnej jest ochrona podstawowych praw i wolności osób fizycznych, w szczególności ich prawa do ochrony danych osobowych (art. 1 ust. 2).

[6] *I. Lipowicz*, Decyzje administracyjne w związku z funkcjonowaniem rządowych systemów informatycznych, [w:] materiały konferencji „Nowe zjawiska w administracji”, Kozubnik 1980, maszynopis powielony, s. 11.

Warunek ten spełniały od 1997 r. polskie przepisy o ochronie danych osobowych, które przyznały kompetencje Generalnemu Inspektorowi Ochrony Danych Osobowych (GIODO) do załatwiania w drodze decyzji administracyjnej skarg osób, których dane dotyczą[7]. Mimo to nadal zgłaszane są propozycje dalszego wzmocnienia administracyjnoprawnej ochrony danych osobowych, nawet wbrew woli człowieka, którego dane dotyczą, gdy naruszenie zasad ochrony danych osobowych – choćby następowało za jego zgodą – stanowi naruszenie jego godności[8].

Podstawy prawne skargi do organu nadzorczego oraz postępowania w tym przedmiocie

W ogólnym rozporządzeniu regulacje dotyczące skargi do organu nadzorczego znajdują się w dwóch grupach przepisów, które dotyczą:

1) środków ochrony prawnej, tj. art. 77, 78 i 80 oraz motywy 141–145 preambuły,
2) zadań organu nadzorczego, tj. art. 57 ust. 1 lit. f, ust. 2–4 RODO.

Pomimo lakoniczności regulacji w tym zakresie znajdującej się w rozporządzeniu ogólnym została ona i tak rozbudowana w porównaniu z przepisami dyrektywy 95/46/WE. W art. 28 ust. 4 zd. 1 dyrektywy 95/46/WE przewiduje się jedynie, że zadaniem organu nadzorczego jest rozpatrywanie skarg podmiotów danych oraz organizacji reprezentujących te podmioty w zakresie ochrony ich praw i wolności dotyczących przetwarzania danych osobowych. Skarżący powinien zostać poinformowany przez organ o wyniku rozpatrzenia sprawy.

Odrębnym zadaniem określonym w art. 28 ust. 4 zd. 3 dyrektywy 95/46/WE jest rozpatrywanie skarg złożonych przez „dowolną osobę" (*any person*) w zakresie kontroli legalności przetwarzania danych osobowych, gdy przepisy krajowe – na mocy art. 13 tej dyrektywy – ograniczają zakres praw i obowiązków określonych w dyrektywie.

Znacznie szerzej problem skarg podmiotów danych, czy też rozpatrywania spraw żądań podmiotu danych w zakresie przetwarzania jego danych osobowych, został uregulowany w uchwalonej w 1997 r. ustawie o ochronie danych osobowych. Zagadnieniu temu poświęconych zostało kilka przepisów rozproszonych w dwóch rozdziałach ustawy, tj. art. 12 pkt 2 oraz art. 18 ust. 1 (Rozdział 2 pt. Organ ochrony danych osobowych) oraz art. 32 ust. 2 (w zw. z ust. 1 pkt 7), art. 32 ust. 3a (w zw. z ust. 1 pkt 9) i art. 35 ust. 2 (w zw. z ust. 1) (Rozdział 4 pt. Prawa osób, których dane dotyczą). Zgodnie z art. 12 pkt 1 OchronaDanychU rozpatrywanie skarg stało się podstawowym zadaniem organu ds. ochrony danych osobowych (GIODO) związanym z wydawaniem decyzji administracyjnych, z czego wynika, że żądanie osoby, której dane dotyczą, kreuje indywidualną sprawę administracyjną rozstrzyganą przez organ władczo w drodze decyzji. Do postępowań prowadzonych przez GIODO zastosowanie znajdują przepisy Kodeksu postępowania administracyjnego z odmiennościami wynikającymi z samej ustawy o ochronie danych osobowych. Kontrolę organu w sprawach indywidualnych sprawuje natomiast sąd administracyjny.

Przedmiot i charakter postępowania

Zgodnie z art. 77 ust. 1 RODO przedmiotem skargi podmiotu danych do organu nadzorczego jest przetwarzanie danych osobowych skarżącego z naruszeniem przepisów ogólnego rozporządzenia. W motywie 141 RODO środki ochrony prawnej (środek administracyjny i środek sądowy) odnosi się do sytuacji, gdy osoba uznaje, że jej uprawnienia wynikające z ogólnego rozporządzenia są naruszane. Wynika to także pośrednio z motywu 142 RODO (zd. 1) dotyczącego umocowania przez osobę organizacji społecznej do działania w jej imieniu w postępowaniu przed organem nadzorczym, ponieważ występuje to w sytuacji „jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z rozporządzenia". Z punktu widzenia osoby, której dane dotyczą, skarga do organu nadzorczego służy więc przede wszystkim wykonaniu prawa do ochrony danych osobowych poprzez działanie organu nadzorczego, jeżeli do realizacji uprawnień w tym względzie nie doszło wcześniej poprzez działania adresatów obowiązków (przede wszystkim administratora). Zwraca się jednak uwagę na możliwość objęcia skargą każdego naruszenia przepisów ogólnego rozporządzenia, jeżeli odnosi się ono do danych osobowych skarżącego[9]. Z drugiej strony przedmiotem skargi nie może być jakiekolwiek naruszenie przepisów ogólnego rozporządzenia, które nie ma bezpośredniego związku z przetwarzaniem danych osobowych zainteresowanego.

Należy także zwrócić uwagę, że w ogólnym rozporządzeniu już wprost jest mowa o prawie podmiotu danych do wniesienia skargi do organu nadzorczego w przedmiocie przetwarzania własnych danych osobowych. Stanowi to zmianę w porównaniu z dotychczasowymi regulacjami dyrektywy 95/46/WE oraz ustawy o ochronie danych osobowych. Według polskiej ustawy rozpatrywanie skarg jest

[7] Na ten temat zob. *G. Sibiga*, Administracyjnoprawna ochrona prawa do ochrony danych osobowych w wyniku skargi osoby, której dane dotyczą – geneza i ewolucja polskich rozwiązań, [w:] *P. Kostański*, *P. Podrecki*, *T. Targosz* (red.), *Experienta docet*. Księga jubileuszowa ofiarowana Pani Profesor Elżbiecie Traple, Warszawa 2017, s. 1393 i n.

[8] *I. Lipowicz*, Ochrona danych osobowych na rozdrożu, [w:] *G. Szpor* (red.), Prawne problemy informatyzacji administracji, Warszawa 2008, s. 16–17.

[9] *R. Jay*, Guide to the General Data Protection Regulation, A Companion to Data Protection Law and Practice (4th edition), London 2017, s. 287.

jedynie zadaniem organu ochrony danych, z czego dopiero odkodowujemy uprawnienie w tym względzie osób, których dane dotyczą (art. 12 pkt 2 OchronaDanychU). Również w art. 28 ust. 4 dyrektywy 95/46/WE wprowadzono jedynie zadanie organu nadzorczego polegające na rozpatrywaniu wpływających do niego skarg.

Korelatem realizacji prawa podmiotu danych do złożenia skargi staje się obowiązek organu nadzorczego załatwienia sprawy ze skargi[10]. W art. 77 RODO nie określono formy, w jakiej organ załatwia sprawę, przewidując jedynie obowiązek poinformowania skarżącego „o postępach i efektach rozpatrywania skargi". Potencjalnie takie rozwiązanie daje dużą swobodę prawodawcy krajowemu w ukształtowaniu prawnych form działania organu nadzorczego i związanego z nimi zakończenia prowadzonego postępowania. Bez względu na przyjęte rozwiązanie organ nadzorczy zawsze pozostaje zobowiązany do merytorycznego załatwienia sprawy indywidualnej ze skargi i podlega w tym zakresie kontroli sądu. W takim wypadku organ, kończąc postępowanie, stwierdza naruszenie ogólnego rozporządzenia i stosuje środek korygujący albo też nie stwierdza takiego naruszenia.

Osobiście skłaniam się do wniosku, że najpełniej realizuje zasady ogólnego rozporządzenia, szczególnie w kontekście prawnych form działania polskich organów administracji publicznej, zakończenie przez organ nadzorczy postępowania poprzez władcze i konkretyzująco-jednostkowe decydowanie o rozpatrzeniu skargi osoby, której dane dotyczą. Przede wszystkim wynika to z rozwiązań dotyczących sądowej kontroli rozpatrywania skarg przez organ nadzorczy. Artykuł 78 ust. 1 RODO przyznaje m.in. podmiotowi danych (skarżącemu) „prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącej decyzji organu nadzorczego jej dotyczącej". W motywie 141 RODO wyjaśnia się, że środek sądowy przysługuje skarżącemu, „jeżeli organ nadzorczy nie reaguje na skargę, częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby". Biorąc to pod uwagę, należy przyjąć, że w ramach konkretyzacji następuje badanie przez organ skargi pod względem formalnym (czego wynikiem może być odrzucenie skargi) oraz pod względem merytorycznym (tutaj wynikiem może być oddalenie skargi). Mimo że w przepisach dotyczących skargi (art. 77 RODO) oraz sądowej kontroli jej rozpatrywania (art. 78 RODO) nie wskazuje się w nich przedmiotu rozstrzygnięcia (czy nawet rodzajów rozstrzygnięć) uwzględniających skargę, wydaje się, że wówczas organ nadzorczy korzysta ze swoich kompetencji naprawczych określonych w art. 58 ust. 2 RODO. Korzystanie z tych kompetencji naprawczych pozwoli na proporcjonalną reakcję na naruszenie w konkretnej sprawie w ten sposób, że usunięty zostanie stan naruszenia prawa do ochrony danych osobowych, a w przypadku nałożenia kary pieniężnej zrealizowana zostanie dodatkowo także funkcja odstraszająca (art. 83 ust. 1 w zw. z art. 58 ust. 2 lit. i RODO). Wobec powyższego sprawę ze skargi podmiotu danych powinniśmy kwalifikować jako indywidualną sprawę administracyjną. Pojęcie sprawy administracyjnej jest bowiem definiowane jako możliwość konkretyzacji wzajemnych uprawnień i obowiązków stron stosunku administracyjnoprawnego, którymi w tym przypadku są organ nadzorczy, składająca skargę osoba, której dane dotyczą, oraz podmiot naruszający zdaniem skarżącego przepisy rozporządzenia (administrator lub podmiot przetwarzający). W polskim porządku prawnym najwłaściwszą formą realizacji tak rozumianych kompetencji przez organ nadzorczy jest akt administracyjny (decyzja administracyjna).

W tym kontekście nieco mylące może być użycie zwrotu „skarga" (zarówno w ogólnym rozporządzeniu, jak i w ustawie o ochronie danych osobowych), które w Kodeksie postępowania administracyjnego występuje jako powszechny środek prawny przysługujący każdemu i dotyczy w szczególności zaniedbania lub nienależytego wykonywania zadań przez właściwe organy albo przez ich pracowników, naruszenia praworządności lub interesów skarżących, a także przewlekłego lub biurokratycznego załatwiania sprawy. Po otrzymaniu skargi organ przeprowadza postępowanie uproszczone, które kończy, zawiadamiając skarżącego o sposobie załatwienia skargi. Tymczasem w sprawie w przedmiocie ochrony danych osobowych ze swojego wniosku („skargi") osoba, której dane dotyczą, właśnie ze względu na przysługujące jej prawo do ochrony danych ma interes prawny w żądaniu rozstrzygnięcia sprawy przez organ nadzorczy. Nie mamy więc do czynienia z postępowaniem uproszczonym, ale z typowym postępowaniem jurysdykcyjnym kończonym decyzją administracyjną. Takie rozumienie konstrukcji skargi osoby, której dane dotyczą, znalazło potwierdzenie w stanowiskach judykatury na gruncie ustawy o ochronie danych osobowych[11].

Od skargi podmiotu danych w zakresie przetwarzania jego danych osobowych należy odróżnić inne skargi na naruszenia ochrony danych osobowych. Osoba, której dane dotyczą, niezależnie od wniosku (skargi) dotyczącego jej prawa do ochrony danych osobowych może także składać do organu nadzorczego (tak jak do każdego organu administracji publicznej) skargi na inne naruszenia przepisów o ochronie danych osobowych. To samo uprawnienie przysługuje zresztą

[10] W niniejszym tekście nie omawiam problematyki szczególnych sytuacji prowadzenia postępowania w ramach mechanizmu współpracy (organów nadzorczych) przez wiodący organ nadzorczy oraz organy nadzorcze, których sprawa dotyczy. Na ten temat zob. *M. Piech*, One-stop-shop. Mechanizmy podejmowania decyzji w sprawie transgranicznego przetwarzania danych osobowych w UE, [w:] *G. Sibiga* (red.), Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016, Warszawa 2016, s. 82 i n.

[11] Zob. wyrok NSA z 28.8.2009 r., I OSK 1521/08, Legalis; wyrok WSA w Warszawie z 20.1.2012 r., II SA/Wa 1671/11, Legalis, oraz postanowienie WSA w Warszawie z 17.9.2008 r., II SA/Wa 335/08, Legalis.

każdej innej osobie. W takim wypadku znajdą zastosowanie przepisy działu VIII Kodeksu postępowania administracyjnego dotyczącego skarg i wniosków (art. 221 KPA i n.).

Uprawniony do wniesienia skargi i uczestnictwa w postępowaniu

W art. 77 RODO wskazuje się wyłącznie środki ochrony prawnej przysługujące osobie, której dane dotyczą. Nie określa się zatem sytuacji procesowej innych osób, nawet gdy ich interesu prawnego będzie dotyczyło postępowanie wszczęte w wyniku skargi. W przypadku gdy organ nadzorczy władczo rozstrzyga sprawę aktem administracyjnym, a więc gdy postępowanie ma charakter postępowania administracyjnego jurysdykcyjnego, jego drugą stroną będzie administrator (w mniejszym stopniu podmiot przetwarzający), który dokonuje przetwarzania objętego skargą.

Ponieważ postępowanie jest wszczynane na wniosek, jedynym uprawnionym do jego zainicjowania będzie osoba, której dane dotyczą, przynajmniej taka konkluzja wynika z treści art. 77 ust. 1 oraz art. 57 ust. 1 lit. f RODO. Powyższe rozwiązanie przyjęte w ogólnym rozporządzeniu odbiega od obecnie obowiązującego w ustawie o ochronie danych osobowych. Zgodnie z art. 18 ust. 1 OchronaDanychU w przypadku naruszenia przepisów o ochronie danych osobowych GIODO z urzędu lub na wniosek „osoby zainteresowanej", w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem. W doktrynie konstrukcję skargi na gruncie ustawy o ochronie danych osobowych odnosi się do wniosków osób, których dane dotyczą[12]. Jednak ustawodawca posłużył się szerszą kategorią „osoby zainteresowanej", które z pewnością obejmuje swoim zakresem każdą osobę, czyjego interesu prawnego dotyczy postępowanie[13]. Przykładowo do tej kategorii w orzecznictwie sądów administracyjnych zaliczono podmioty, które żądają – z powołaniem się na przepisy o ochronie danych osobowych – udostępnienia im danych osobowych osób trzecich[14].

W pewnym zakresie również dyrektywa 95/46/WE przewiduje skuteczne złożenie skargi do organu przez innego skarżącego niż osoba, której dane dotyczą. W art. 28 ust. 4 dyrektywy 95/46/WE rozróżnia się skargę osoby, której dane są przetwarzane, oraz skargę „dowolnej osoby" (*any person*), w szczególności w zakresie legalności przetwarzania danych, gdy przepisy krajowe ograniczają zakres praw i obowiązków określonych w tej dyrektywie. W każdym z tych dwóch przypadków na organie spoczywa obowiązek rozpatrzenia sprawy oraz poinformowania skarżącego: „o wyniku sprawy" (gdy skarżącym jest podmiot danych) lub „o przeprowadzeniu kontroli" (gdy skarżącym jest inna osoba).

Ogólne rozporządzenie przyznaje szczególne uprawnienia procesowe – poza podmiotem danych (skarżącym) – jedynie organizacjom społecznym, które łącznie spełniają trzy warunki: nie mają charakteru zarobkowego, ich cele statutowe mieszczą się w interesie publicznym oraz „działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych". Według art. 80 ust. 1 RODO takie organizacje mogą zostać umocowane przez podmiot danych (skarżącego) do działania w jego imieniu w postępowaniu przez organem nadzorczym, a następnie w postępowaniu sądowym (kontrolnym wobec organu nadzorczego). Uprawnienie w tym zakresie obejmuje samo złożenie skargi oraz realizowanie w tym postępowaniu uprawnień podmiotu danych. Występuje trudność z bezpośrednim przeniesieniem tego rozwiązania do polskiego postępowania administracyjnego, ponieważ zgodnie z art. 33 § 1 KPA pełnomocnikiem w postępowaniu administracyjnym może być jedynie osoba fizyczna mająca pełną zdolność do czynności prawnych. Należy jednak dążyć do zapewnienia komplementarności przepisu przewidującego szczególną rolę organizacji w postępowaniu oraz zasad prowadzenia postępowania administracyjnego, choćby poprzez umożliwienie udziału tej organizacji w postępowaniu.

Niezależnie od tego art. 80 ust. 2 RODO stanowi, że przepisy krajowe mogą umożliwiać tym organizacjom samodzielne prawo wniesienia skargi do organu nadzorczego i wykonywania uprawnień w postępowaniu, „jeżeli uznają, że w wyniku przetwarzania naruszone zostały prawa osoby, której dane dotyczą, wynikające z niniejszego rozporządzenia". Należy zwrócić uwagę, że regulacja znajdująca się w art. 80 ust. 2 RODO znacząco różni się od art. 31 KPA określającego sytuację prawną organizacji społecznej w polskim postępowaniu administracyjnym jurysdykcyjnym. Istota rozwiązania unijnego polega na przyznaniu organizacji uprawnienia do złożenia skargi do organu nadzorczego (w sytuacji naruszenia praw podmiotu danych określonego w RODO), co oznacza, że organizacja ma prawo skutecznie żądać merytorycznego rozstrzygnięcia wniesionej przez nią sprawy, a w trakcie postępowania będzie przysługiwał jej status strony w tym postępowaniu. Rolą organu nadzorczego nie jest wstępne rozstrzyganie o wszczęciu postępowania na wniosek organizacji, ale rozstrzygnięcie merytoryczne każdego wniosku organizacji dotyczącego naruszenia prawa osoby, której dane dotyczą. Postępowanie wnioskowe w takim wypadku jest wszczęte w dniu doręczenia organowi nadzorczemu żądania

[12] *E. Kulesza*, Pozycja i uprawnienia Generalnego Inspektora Ochrony Danych Osobowych w świetle ustawy ochronie danych osobowych. Uwagi *de lege lata* i *de lege ferenda*, Przegląd Sejmowy 1999, Nr 5, s. 16–17.

[13] Na temat pojęcia osoby zainteresowanej w rozumieniu art. 18 ust. 1 OchronaDanychU zob. *C. Martysz*, Zakres stosowania kodeksu postępowania administracyjnego w ustawie o ochronie danych osobowych, [w:] *G. Szpor* (red.), Przetwarzanie i ochrona danych, Katowice 1998, s. 35; *G. Sibiga*, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s. 129 i n.

[14] Zob. np. wyrok NSA z 21.8.2013 r., I OSK 1666/12, Legalis.

organizacji spełniającego warunki określone w art. 80 ust. 2 w zw. z ust. 1 RODO. Decyzja o wprowadzeniu takiej szczególnej konstrukcji procesowej należy jednak do prawodawcy krajowego.

Od skargi podmiotu danych w zakresie przetwarzania jego danych osobowych należy odróżnić skargi innych osób na naruszenia ochrony danych osobowych. Zresztą skarżącym w tym rozumieniu może być też sama osoba, której dane dotyczą. Może ona bowiem niezależnie od wniosku (skargi) dotyczących jej prawa do ochrony danych osobowych składać także do organu (GIODO) skargi na inne naruszenia przepisów o ochronie danych osobowych. Dopiero wówczas dojdzie do zastosowania przepisów działu VIII Kodeksu postępowania administracyjnego dotyczącego skarg i wniosków (art. 221 KPA i n.). Zresztą taką skargę w przedmiocie ochrony danych osobowych może złożyć do organu każdy zainteresowany, a jeżeli sprawa nie będzie dotyczyła jego danych osobowych lub z innych powodów nie będzie miał interesu prawnego w jej rozpatrzeniu, należy ją traktować jako skargę, o której mowa w dziale VIII Kodeksu postępowania administracyjnego.

Wybór środka dochodzenia prawa

Osobie, której dane dotyczą, przyznano w ogólnym rozporządzeniu niezależne od siebie środki ochrony związane z naruszeniem jej praw określonych w rozporządzeniu i mające służyć realizacji tych praw:

1) skargę do organu nadzorczego na przetwarzanie jej danych osobowych z naruszeniem rozporządzenia (art. 77 RODO), a następnie zainicjowanie sądowej kontroli dotyczącej decyzji organu nadzorczego lub jego bezczynności (art. 78 RODO);
2) środek ochrony przed sądem na naruszenie jej praw przysługujących na podstawie ogólnego rozporządzenia w wyniku przetwarzania danych osobowych sprzecznego z tym rozporządzeniem (art. 79 RODO)[15].

Dla podmiotu danych przewidziano zatem wybór między dwoma środkami ochrony prawnej: administracyjnym oraz sądowym. Każdy z tych środków służy realizacji prawa do ochrony danych osobowych (w sytuacji gdy doszło do jego naruszenia), a prawodawca unijny podkreśla, że zastosowanie jednego z tych środków pozostaje bez uszczerbku do skorzystania z drugiego (art. 77 ust. 1 oraz art. 79 ust. 1 RODO)[16]. Wydaje się jednak, że prawodawca krajowy powinien w ten sposób ukształtować procedurę, aby zapobiegać możliwości występowania w obrocie dwóch „konkurencyjnych" wobec siebie orzeczeń (sądowego i administracyjnego), które mają tożsamy przedmiot związany z prawem do ochrony danych osobowych.

Warunek wyczerpania środków prawnych przed złożeniem skargi

W przypadku skargi na niewykonanie przez administratora uprawnienia osoby, której dane dotyczą, w art. 77 oraz 57 ust. 1 lit. f RODO wprost nie wymaga się od tej osoby wcześniejszego złożenia żądania wobec samego administratora.

Powyższa kwestia została uregulowana odmiennie w ustawie ochronie danych osobowych. W polskiej ustawie przyjęto bowiem konstrukcję, że w pierwszej kolejności osoba, której dane dotyczą, realizuje swoje uprawnienia, składając żądania do administratora jej danych. Dopiero gdy administrator nie wykona tych żądań, podmiot danych składa wniosek do GIODO, który rozstrzyga merytorycznie sprawę (art. 35 ust. 2 OchronaDanychU). Wyjątkowo to sam administrator, który otrzymał żądanie, musi je przekazać do GIODO, gdy negatywnie rozpatrzył to żądanie, co wyręcza osobę, której dane dotyczą, od potrzeby samodzielnego wniesienia skargi go organu. Powyższy szczególny tryb dotyczy żądania podmiotu danych: zaprzestania przetwarzania danych osobowych ze względu na jego szczególną sytuację oraz ponownego indywidualnego rozpatrzenia jego sprawy rozstrzygniętej z naruszeniem zakazu automatyzacji (art. 32 ust. 2 i 3a OchronaDanychU).

Pomimo braku stosowanej regulacji w art. 77 oraz 57 ust. 1 lit. f RODO moim zdaniem z przepisów ogólnego rozporządzenia wynika warunek skuteczności skargi polegający na uprzednim wyczerpaniu środków prawnych wobec administratora, jeżeli taki środek przysługuje. Na uprawnienia podmiotu danych określone w art. 15–21 RODO składają się bowiem dwa elementy: materialny i formalny. Element materialny określa treść określonego uprawnienia, natomiast formalny wymaga, aby osoba zwróciła się o realizację swojego prawa do administratora. Z naruszeniem ogólnego rozporządzenia mamy do czynienia dopiero w sytuacji, gdy nie dojdzie do realizacji uprawnienia mimo łącznego spełnienia tych dwóch elementów. Pośrednio warunek uprzedniego wyczerpania środka wobec administratora potwierdzają formalne wymogi negatywnej odpowiedzi tego administratora na żądanie podmiotu danych (gdy takie żądanie zostanie złożone). Według art. 12 ust. 4 RODO w takiej odpowiedzi zawiadamiającej o niepodjęciu żądanych działań administrator musi w szczególności poinformować o możliwości wnie-

[15] Odrębnie od środka sądowego, o którym mowa w art. 79 RODO, w art. 82 RODO przewiduje się uprawnienie odszkodowawcze wobec administratora lub podmiotu przetwarzającego przyznane każdej osoby, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia ogólnego rozporządzenia.

[16] Dopuszczalny przedmiot powództwa, o którym mowa w art. 79 RODO, wydaje się węższy niż skargi, ponieważ odnosi się on do naruszenia praw powoda określonych w RODO, podczas gdy skarga dotyczy każdego naruszenia RODO w zakresie przetwarzania danych osobowych skarżącego. Zob. *R. Jay*, Guide to the General…, s. 293.

sienia skargi do organu nadzorczego. Można więc wnosić, że dopiero na tym etapie taka możliwość występuje.

Opłata za rozpatrzenie skargi

Stosownie do treści art. 57 ust. 3 RODO organ nadzorczy wypełnia zadania na rzecz osoby, której dane dotyczą, bezpłatnie. Jedyny wyjątek od tej zasady przewiduje się w ust. 4 w tym przepisie, zgodnie z którym, gdy żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swą powtarzalność, organ nadzorczy może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. W wypadku spełnienia chociaż jednej z tych przesłanek alternatywnym działaniem organu jest odmowa podjęcia żądanych w skardze działań. Jeżeli jednak organ nadzorczy skorzysta z możliwości nałożenia opłaty lub odmowy podjęcia działań, przepis art. 57 ust. 4 zd. 2 RODO zobowiązuje go do wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne.

Z powyższych przepisów wynika kilka istotnych wniosków, ponieważ szczególnym zadaniem organu nadzorczego wobec podmiotu danych jest rozpatrywanie skarg od niego otrzymanych. Zasadą pozostaje, że taki skarżący nie ponosi opłat z tytułu rozpatrzenia przez organ jego skargi, w tym wydania aktu administracyjnego kończącego postępowanie (jeżeli taki akt został wydany). Niedopuszczalne pozostaje więc wymaganie od skarżącego uiszczenia opłaty skarbowej lub innej opłaty w kwocie zryczałtowanej. W mojej ocenie ogólne rozporządzenie nie dopuszcza możliwości ustanowienia takich opłat przez prawodawcę krajowego z powodów podanych poniżej.

Dwiema wyjątkowymi sytuacjami, w przypadku których jest możliwe nałożenie przez organ opłaty, jest złożenie skargi „oczywiście nieuzasadnionej" lub „nadmiernej, w szczególności ze względu na swą powtarzalność", co stanowi powielenie przesłanek przewidzianych w art. 12 ust. 5 RODO dla administratora rozpatrującego żądanie podmiotu danych[17]. Sama wysokość opłaty powinna być przez organ ustalona „w rozsądnej wysokości wynikającej z kosztów administracyjnych", a zatem musi być ona adekwatna do rzeczywiście poniesionych kosztów i nie może stanowić nadmiernego utrudnienia w realizacji uprawnienia.

Z tak skonstruowanego rozwiązania wynika kilka istotnych wniosków. Nawet w przypadku spełnienia prawem określonej przesłanki nałożenie opłaty pozostawiono uznaniu organu nadzorczego. Sam sposób sformułowania przesłanek świadczy, że ich zaistnienie powinno być ustalone *a casu ad casum* przez organ nadzorczy, przy czym może on przyjąć stałe kryteria pomocnicze pomagające w tym ustalaniu. Dodatkowo organ musi wykazać zaistnienie przesłanki określone w art. 57 ust. 4 RODO, co wymaga sporządzenia uzasadnienia. Usprawiedliwiony wydaje się zatem pogląd, że mamy do czynienia ze szczególnym rodzajem rozstrzygnięcia organu nadzorczego, i to zarówno w przypadku nałożenia opłaty, jak i odmowy podjęcia działań. Również sama wysokość opłaty powinna zostać ustalona indywidualnie w zależności od okoliczności faktycznych i z uwzględnieniem przesłanek wskazanych w ogólnym rozporządzeniu. Takie „elastyczne" ustalanie wysokości opłaty występuje już w prawie krajowym w ustawie z 6.9.2001 r. o dostępie do informacji publicznej[18], w której opłatę nakłada się, gdy podmiot zobowiązany „ma ponieść dodatkowe koszty związane ze wskazanym we wniosku sposobem udostępnienia lub koniecznością przekształcenia informacji w formę wskazaną we wniosku", a wysokość ustalonej opłaty musi odpowiadać tym kosztom.

Przebieg postępowania organu nadzorczego

Pomimo lakoniczności przepisów proceduralnych w ogólnym rozporządzaniu na gruncie tego aktu można wyróżnić kilka etapów procesowych:

1) wszczęcie postępowania,
2) postępowanie wyjaśniające,
3) zakończenie postępowania,
4) sądowa kontrola organu nadzorczego, tj. jego aktów lub czynności, bezczynności lub przewlekłego prowadzenia postępowania.

Postępowanie wszczynane jest wyłącznie na wniosek (skargę) osoby, której dane dotyczą. W ogólnym rozporządzeniu nie określono wymogów w stosunku do samej skargi, w szczególności jej formy i treści. W art. 57 ust. 3 RODO nakłada się na organ nadzorczy szczególny obowiązek ułatwienia składania skarg („organ nadzorczy ułatwia wnoszenie skarg (…) za pomocą takich środków, jak gotowy formularz skargi, który można również wypełnić elektronicznie, co nie wyklucza innych sposobów komunikacji")[19]. Obowiązkiem organu nadzorczego jest umieszczenie w sieci elektronicznego formularza pomocniczego, który osoba, której dane dotyczą, będzie mogła elektronicznie wypełnić i za jego pomocą skutecznie online złożyć skargę do organu nadzorczego. Wzór takiego formularza może zostać określony w krajowych przepisach uzupełniających ogólne rozporządzenie, a gdyby to nie nastąpiło, musi to uczynić sam organ nadzorczy. Jednak zastosowanie elektronicznego formularza nie może wykluczać innych niż elektroniczne sposobów składania skarg do

[17] W polskiej wersji językowej ogólnego rozporządzenia w art. 12 ust. 5 RODO znajduje się przesłanka żądania „ewidentnie nieuzasadnionego", natomiast w art. 57 ust. 4 RODO „oczywiście nieuzasadnionego". Powodem różnicy jest jednak wyłącznie różnica w tłumaczeniu przymiotnika „*manifestly*", który występuje w obu tych przepisach.

[18] T.j. Dz.U. z 2016 r. poz. 1764 ze zm.

[19] Na ten temat także motyw 141 zd. 5 RODO.

organu nadzorczego, w szczególności nie może być podstawą do odmowy rozpatrzenia skargi z przyczyn formalnych.

Przepisy rozporządzenia ogólnego nie wymają szczególnej formy wszczęcia postępowania. Dopuszczalne będzie zatem przyjęcie, że datą wszczęcia postępowania będzie dzień doręczenia skargi organowi nadzorczemu (zob. art. 61 § 3 KPA).

W prowadzonym postępowaniu organ nadzorczy dla potrzeb ustalenia stanu faktycznego jest uprawniony do korzystania ze środków dowodowych, o których mowa w art. 58 ust.1 lit. a–b i e–f RODO. W motywie 141 RODO wskazuje się, że w zakresie dowodowym organ powinien się kierować zasadą proporcjonalności („Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie").

Z przepisów rozporządzenia ogólnego wynika także obowiązkowy dla organu termin zakończenia postępowania. Sądowa skarga na bezczynność organu nadzorczego jest bowiem dopuszczalna dopiero po trzech miesiącach od dnia wniesienia skargi, gdy organ w tym terminie nie rozpatrzył skargi lub nie poinformował skarżącego o postępach lub efektach rozpatrywania skargi (art. 78 ust. 2 RODO). Z rozwiązania tego wynika, że podstawowym terminem dla organu nadzorczego jest termin trzymiesięczny, w którym musi on rozpatrzyć sprawę (np. wydać rozstrzygnięcie załatwiające skargę) lub zawiadomić skarżącego o przedłużeniu postępowania wraz z informacją o postępach i efektach postępowania. Z motywu 141 RODO wynika, że postępowanie może być przedłużone, jeżeli dana sprawa wymaga dalszych czynności wyjaśniających lub koordynacji działań z innym, krajowym organem nadzorczym.

Ogólne rozporządzenie przewiduje również sądową kontrolę aktów lub czynności organu nadzorczego, jak również jego bezczynności, uruchamianą w wyniku wniesienia środka sądowego przez skarżącego. W art. 78 ust. 1 RODO przyznaje się skarżącemu prawo do sądowego zaskarżania wiążącej decyzji organu nadzorczego. W motywie 141 RODO wyjaśnia się, że w szczególności dotyczy to sytuacji odrzucenia lub oddalenia skargi w części lub w całości. Odrębne prawo do środka sądowego przysługuje, gdy organ nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą, w określonym terminie „o postępach lub efektach rozpatrywania skargi" (art. 78 ust. 2 RODO). Dotyczy to zwłaszcza przypadku, gdy organ nadzorczy nie podejmuje działania, choć jest to niezbędne do ochrony praw osoby, której dane dotyczą (skarżącego) – motyw 141 RODO. Środek ten można zakwalifikować jako skargę na bezczynność organu nadzorczego, ale nie ma też uzasadnienia, aby ograniczać podmiotowi danych również prawo do skargi sądowej na przewlekłe prowadzenie postępowania przez organ nadzorczy.

Podsumowanie

Powyższe wskazuje, że przepisy ogólnego rozporządzenia nie ukształtowały w sposób wystarczający procedury rozpatrywania skarg, a jedynie wprowadziły pewne rozwiązania w tym względzie. Konsekwencją tego jest, że to prawodawca krajowy musi kompleksowo uregulować procedurę w tym przedmiocie oraz określić prawne formy działania organu nadzorczego, oczywiście uwzględniając nieliczne regulacje w tym względzie zawarte w ogólnym rozporządzeniu.

Słowa kluczowe: skarga, organ nadzorczy, prawo do ochrony danych, podmiot danych.

Complaint to watchdog and its examination according to the general regulation on data protection. Proceeding in regard to complaint of a person of whom the data concern

From the point of view of a person of whom the data concern (subject of data), the core of law regulation on personal data protection amounts to granting them the right to protect their personal data. This person realizes their eligibility against the administrator of the data, and when it fails, they have a right to file a complaint to an independent administrative authority of personal data protection (watchdog). The job of this authority is to look into this complaint so that in case of ascertainment of violation of law on data protection it can lead to following the law by administrative means. In the article the author presents regulation in this matter included in the regulation of the European Parliament and the Council 2016/679 of 27.4.2016 in the matter of legal person protection in regard to processing of personal data and in the matter of free movement of such data and overruling the directive 95/46/EC (general regulation on data protection) comparing it to past solutions effective until 25.5.2018, which can be found in the directive 95/46/EC of the European Parliament and the Council of 24.10.1995 in the matter of legal person protection in regard to processing of personal data and its free movement and realizing the directive of Polish law of 29.8.1997 on personal data protection.

Keywords: complaint, watchdog, right to data protection, subject of data.

Zasada czasowego ograniczenia przechowywania danych osobowych na gruncie RODO

r.pr. *Michał Bienias*[1]

Celem niniejszego opracowania jest przedstawienie zasady czasowego ograniczenia przechowywania danych osobowych z RODO oraz zaproponowanie okresów retencji danych w odniesieniu do różnych celów przetwarzania danych osobowych, ze szczególnym uwzględnieniem działalności ubezpieczeniowej.

Uwagi wstępne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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[2] nakłada na administratorów danych obowiązek dochowania zasady ograniczenia przechowywania danych (zasady czasowości). „Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą" (art. 5 ust. 1 lit. e RODO). Zasada ta została uregulowana także w innych przepisach RODO, gdyż w myśl zasady domyślnej ochrony danych administrator powinien wdrożyć „odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne do osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych" (art. 25 ust. 2 RODO).

Zasada czasowego ograniczenia przechowywania danych osobowych

Na sposób realizacji zasady ograniczenia przetwarzania wskazują motywy preambuły RODO. Należy przy tym pamiętać, że chociaż preambuła nie może sama w sobie stanowić odrębnej normy prawnej, to motyw preambuły RODO może wskazywać wykładnię danego przepisu prawa[3]. Zgodnie z motywem Nr 39 preambuły „dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu".

Motyw Nr 39 preambuły RODO wprost mówi o konieczności ustalenia okresów retencji danych (stworzenia odpowiedniej polityki retencyjnej) lub dokonywania okresowego przeglądu danych pod względem ich niezbędności do osiągnięcia celu, dla którego są przetwarzane. Nie jest przy tym możliwe ani zalecane przyjmowanie jednolitej – dla wszystkich kategorii danych osobowych – polityki retencyjnej. Ustalenie jednego okresu retencji dla wszystkich danych klienta (np. trzy lata) stanowiłoby naruszenie zasady ograniczenia przechowywania, a w niektórych przypadkach prowadziłoby do pozbawienia administratora możliwości obrony przed roszczeniami byłych klientów (np. przy umowach, gdzie okres przedawnienia roszczeń jest dłuższy). Okres retencji należy bowiem ustalać w stosunku do każdego wyodrębnionego celu przetwarzania. Cele przetwarzania determinują bowiem okres, w jakim dane mogą być przechowywane, a także dopuszczalny zakres danych przetwarzanych w danym okresie. Zakres przetwarzanych danych powinien przy tym ulec ograniczeniu do tych danych, których przetwarzanie po ustaniu danego stosunku

[1] Autor jest starszym prawnikiem w Kancelarii Prawnej Traple Konarski Podrecki i Wspólnicy. Autor pracuje przy licznych projektach wdrożeniowych RODO dla branży internetowej, reklamowej, ubezpieczeniowej oraz FMCG.

[2] Dz.Urz. UE L Nr 119, s. 1; dalej jako: RODO lub rozporządzenie ogólne.

[3] Zob. orzeczenie TS z 13.7.1989 r., Casa Fleischhandels-GmbH v. Bundesanstalt für landwirtschaftliche Marktordnung, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61988CJ0215 (dostęp z 14.2.2018 r.).

(np. wygaśnięciu umowy) jest konieczne z uwagi na ochronę uzasadnionego interesu administratora danych, np. ochronę przed roszczeniami cywilnoprawnymi, czy też z uwagi na przepisy prawa (np. przepisy o rachunkowości – przechowywanie dokumentacji księgowej). W rezultacie w razie przetwarzania danych osobowych zebranych na podstawie art. 6 ust. 1 lit b RODO: „przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą", dane osobowe będą przechowywane w następujących okresach:

– przez okres trwania umowy, a następnie
– przez okres wynikający z przedawnienia potencjalnych roszczeń (np. trzy lata, jeżeli dane osobowe dotyczą innych przedsiębiorców z którymi zostały podpisane umowy w związku z prowadzeniem działalności gospodarczej – art. 118 KC) oraz
– przez okres wynikający z innych przepisów szczególnych, np. dane wynikające z dowodów księgowych (przykładowo pięć lat liczone od początku roku następującego po roku obrotowym, w którym operacje, transakcje odnoszące się do umowy zostały zakończone, spłacone, rozliczone – art. 74 ust. 2 pkt 4 ustawy z 29.9.1994 r. o rachunkowości[4]).

Zarówno na podstawie RODO, jak i obecnie obowiązującej ustawy z 29.8.1997 r. o ochronie danych osobowych[5] czasowym wyznacznikiem jest osiągnięcie zamierzonego celu przetwarzania. Później nie muszą być one wprawdzie „z urzędu" usunięte, natomiast powinny być co najmniej poddane anonimizacji, pozbawione cech identyfikujących. Nie wystarcza w żadnej mierze jedynie utrudnienie identyfikacji. W rezultacie zachowane informacje powinny wówczas utracić walor danych osobowych w rozumieniu ustawy[6].

Tworzenie polityki retencyjnej na gruncie RODO

Motyw Nr 39 preambuły RODO wprost mówi o konieczności ustalenia okresów retencji danych (stworzenia odpowiedniej polityki retencyjnej) lub dokonywania okresowego przeglądu danych pod względem ich niezbędności do osiągnięcia celu, dla którego są przetwarzane. Obowiązek usunięcia danych osobowych należy uzależnić od nastąpienia określonego zdarzenia (które jest powiązane z określonym celem przetwarzania danych):

– od cofnięcia zgody przez osobę, której dane dotyczą – jeżeli podstawą prawną przetwarzania jest art. 6 ust. 1 lit. a RODO – w przypadku przetwarzania danych w celach marketingowych na podstawie zgody;
– od wyrażenia sprzeciwu przez osobę, której dane dotyczą – jeżeli podstawą prawną przetwarzania jest art. 6 ust. 1 lit. f RODO – przetwarzanie danych jest niezbędne w celu realizacji uzasadnionego interesu administratora (w celu prowadzenia marketingu bezpośredniego);
– od przedawnienia roszczeń – jeżeli dane były uprzednio przetwarzane w celu realizacji umowy;
– od upływu terminów określonych w przepisach szczególnych.

Po upływie najdłuższego z okresów pozwalających na przechowywanie danych ubezpieczyciel powinien dane klientów nieodwracalnie usunąć ze wszystkich swoich nośników danych (co może być realizowane przez fizyczne niszczenie nośników danych) lub zanonimizować je w sposób, który nieodwracalnie uniemożliwi ustalenie tożsamości tych osób, z wyłączeniem tych danych, które ubezpieczyciel powinien posiadać z uwagi na inne przepisy prawa (np. przepisy o rachunkowości).

Co więcej, przy ustalaniu okresu retencji danych przetwarzanych po zakończeniu umowy na wpływ biegu okresu przedawnienia roszczeń ma zawieszenie i przerwanie biegu przedawnienia. Bieg ulega przerwaniu przez każdą czynność przed sądem lub innym organem powołanym do rozpoznawania spraw lub egzekwowania roszczeń danego rodzaju albo przed sądem polubownym, przedsięwziętą bezpośrednio w celu dochodzenia lub ustalenia albo zaspokojenia lub zabezpieczenia roszczenia lub przez wszczęcie mediacji. W razie przerwania przedawnienia w ww. wypadkach przedawnienie nie biegnie na nowo, dopóki postępowanie to nie zostanie zakończone (art. 123 § 1 pkt 1 KC w zw. z art. 124 § 2 KC). Dodatkowo roszczenie stwierdzone prawomocnym orzeczeniem sądu lub innego organu powołanego do rozpoznawania spraw danego rodzaju albo orzeczeniem sądu polubownego, jak również roszczenie stwierdzone ugodą zawartą przed sądem albo przed sądem polubownym albo ugodą zawartą przed mediatorem i zatwierdzoną przez sąd przedawnia się z upływem 10 lat, chociażby termin przedawnienia roszczeń tego rodzaju był krótszy. Termin należy liczyć od uprawomocnienia się orzeczenia.

Powyższe zasady, a także wiele innych zasad wynikających z charakteru działalności administratora (w zależności czy jest to działalność reklamowa, czy bankowa lub ubezpieczeniowa, czy też e-commerce) powinny zostać opisane w polityce retencyjnej administratora danych.

[4] T.j. Dz.U. z 2016 r. poz. 1047 ze zm.; dalej jako: RachU.

[5] T.j. Dz.U. z 2016 r. poz. 922 ze zm.

[6] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych. Komentarz, wyd. VI, komentarz do art. 26, Lex/el. 2018.

Okresy retencji danych w działalności ubezpieczeniowej

Należy zwrócić uwagę na trudności związane z ustaleniem okresu retencji danych osobowych zebranych w celu wykonania umowy. Na przykład w branży ubezpieczeniowej po zakończeniu umowy ubezpieczenia dane osobowe mogą być przetwarzane w celu dochodzenia roszczeń wynikających z umowy lub w celu obrony przed roszczeniami klienta wynikającymi z umowy przez okres trzech lat (zgodnie z art. 819 KC). Istnieją jednak argumenty przemawiające za tym, aby okres retencji danych wynosił dziesięć lat, a nie trzy lata. W praktyce działalności ubezpieczeniowej mają miejsce przypadki roszczeń klientów z tytułu występowania w umowach klauzul abuzywnych, dlatego dłuższy okres przechowywania danych osobowych można uzasadnić niezbędnością przetwarzania danych osobowych do obrony przed takimi roszczeniami (art. 6 ust. 1 lit f RODO). Przykładowo SO w Warszawie[7] uznał, że roszczenie powódki nie wynikało z umowy ubezpieczenia ze względu na istnienie klauzuli abuzywnej w tej umowie (sporne postanowienie umowne nie łączyło strony, więc roszczenie dochodzone pozwem nie wynikało z umowy ubezpieczenia, wobec czego nie miał zastosowania okres przedawnienia właściwy dla roszczeń z umowy ubezpieczenia): „W pierwszej kolejności należy wskazać, iż roszczenie powódki nie jest roszczeniem z umowy ubezpieczenia. Skutkiem bowiem uznania określonego postanowienia umowy za klauzulę niedozwoloną, jest to że nie wiąże ono powoda-konsumenta. W związku zatem z przesądzeniem jak wyżej wskazano, iż postanowienia umowy w zakresie obciążania powódki nieracjonalną opłatą manipulacyjną z tytułu wcześniejszego rozwiązania umowy, brak jest jakiejkolwiek podstawy do spełnienia na rzecz pozwanego świadczenia. W sytuacji zatem gdy żądana przez powódkę kwota ma swą podstawę w roszczeniu z tytułu bezpodstawnego wzbogacenia, nie zaś świadczenia okresowego, to roszczenie o zapłatę przedmiotowej kwoty żądanej przez powoda podlega ogólnemu 10-letniemu terminowi przedawnienia (art. 118 KC). Termin ten zatem należy zacząć liczyć od dnia rozwiązania umowy, tj. 6.8.2009 r., zaś roszczenia z tego tytułu przedawniłyby się po 6.8.2019 r., pozew tymczasem został wniesiony 15.9.2016 r. przed upływem takowego terminu". W przypadku gdyby zakład ubezpieczeń przyjął trzyletni termin przedawnienia roszczeń, w razie wniesienia przez byłego klienta będącego konsumentem powyższego powództwa zakład ten byłby pozbawiony możliwości obrony przed takim roszczeniem (w związku z usunięciem wszystkich danych dotyczących tego klienta zakład ubezpieczeń nie miałby nawet wiedzy, czy ta osoba kiedykolwiek była jego klientem).

Podobne wątpliwości występują w ubezpieczeniach majątkowych. Roszczenia z tytułu odpowiedzialności cywilnej przedawniają się w takim terminie, jaki przewidziany jest dla roszczenia odszkodowawczego przysługującego poszkodowanemu wobec sprawcy szkody (ubezpieczonego, ubezpieczającego). Jednakże, w odniesieniu do szkód na osobie: „przedawnienie nie może skończyć się wcześniej niż z upływem lat trzech od dnia, w którym poszkodowany dowiedział się o szkodzie i o osobie obowiązanej do jej naprawienia" (art. 442^1 § 3 KC). Powyższy przepis stwarza liczne trudności, gdyż zakład ubezpieczeń nie wie, kiedy poszkodowany dowiedział się o szkodzie i osobie obowiązanej do jej naprawienia (kiedy dla poszkodowanego upłynął okres przedawnienia roszczeń), a więc nie wie, kiedy usunąć dane osobowe zapisane na polisie. Z drugiej strony, mając na uwadze przepisy RODO, nie jest zalecane przechowywanie danych osobowych bez ustalenia momentu końcowego ich przechowania. W związku z tym zalecane jest ustalenie dla tych danych tego samego okresu przechowywania danych jak dla innych roszczeń z tytułu odpowiedzialności cywilnej (np. 20 lat – jeżeli w danym ubezpieczeniu mogą wystąpić szkody, które wynikają ze zbrodni lub występku).

Problem przetwarzania danych osobowych „w nieskończoność"

Zasada ograniczenia czasowego przetwarzania danych osobowych ma na celu zabezpieczyć osobę, której dane dotyczą, przed przetwarzaniem jej danych osobowych przez niczym nieograniczony okres, tj. „w nieskończoność", a właściwie do śmierci osoby fizycznej. Po śmierci osoby fizycznej dane osób zmarłych mogą być przetwarzane bez ograniczenia czasowego (nie ma potrzeby wdrażania polityki retencyjnej w tym zakresie) ze względu na fakt, że RODO nie stosuje się do osób zmarłych (zgodnie z motywem Nr 27 preambuły RODO).

Punktem granicznym przy przechowywaniu danych osobowych jest osiągnięcie przez administratora danych zakładanego w chwili zbierania danych celu, w jakim pozyskał i przetwarzał dane osobowe. W szczególności problem ten będzie występował w sytuacji, gdy umowa została zakończona, wszelkie terminy przedawnienia roszczeń wynikających z umowy upłynęły, a określone świadczenie nigdy nie zostało wypłacone (tzw. zobowiązanie naturalne lub niezupełne), gdyż wierzyciel nigdy nie zgłosił się po świadczenie do dłużnika. Budzi wątpliwości fakt, czy w takiej sytuacji, po zakończeniu umowy i upływie terminów przedawnienia, administrator ma wciąż przechowywać dane osobowe wierzyciela na wypadek, gdyby kiedyś zgłosił się jeszcze po swoje świadczenie (podczas gdy może to nigdy nie nastąpić, a dłużnik nie ma obowiązku spełnienia świadczenia).

[7] Zob. wyrok SO w Warszawie z 7.3.2017 r., III C 1217/16, niepubl.

Należy dodać, że zgodnie z art. 120 KC bieg przedawnienia rozpoczyna się od dnia, w którym roszczenie stało się wymagalne, a jeżeli wymagalność roszczenia zależy od podjęcia określonej czynności przez uprawnionego, początek biegu przedawnienia następuje z dniem, w którym roszczenie stałoby się wymagalne, gdyby uprawniony podjął czynność w najwcześniej możliwym terminie. W wielu przypadkach dla rozpoczęcia biegu przedawnienia nie jest zatem istotne to, czy czynność uprawnionego została podjęta i czy uprawniony w ogóle był świadom tego, że przysługuje mu roszczenie i powinien podjąć jakąś czynność w celu jego zrealizowania[8]. Należy natomiast ustalić, kiedy najwcześniej uprawniony mógł tę czynność podjąć oraz kiedy roszczenie stałoby się wymagalne, gdyby uprawniony wówczas tę czynność podjął[9]. Oznacza to, że mogą istnieć roszczenia, o których wierzyciele nie wiedzą (i które się przedawniły).

Przyjęcie, że administrator danych może przechowywać dane osobowe podmiotu danych (wierzyciela) aż do czasu jego zgłoszenia po upływie terminu przedawnienia roszczenia wierzyciela oraz innych roszczeń wynikających z umowy, może stanowić naruszenie zasady czasowego ograniczenia przechowywania danych osobowych. Przechowywanie danych osobowych wierzyciela przedawnionego roszczenia nie stanowi uzasadnionego interesu administratora (dane nie są niezbędne do ustalenia, dochodzenia lub obrony roszczeń), a co najwyżej uzasadniony interes osoby, której dane dotyczą (wierzyciela) – co nie jest przesłanką przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f RODO. Uzasadniony interes będący przesłanką przetwarzania danych może być także interesem strony trzeciej, przy czym zgodnie z art. 4 pkt 10 RODO stroną trzecią nie jest osoba, której dane dotyczą.

Powyższy problem wystąpi w działalności ubezpieczeniowej, w sytuacji gdy umowa została zakończona, lecz osoba uprawniona nigdy nie zgłosiła się po świadczenie. W wielu przypadkach ubezpieczyciele przechowują dane takiej osoby „wiecznie", na wypadek gdyby uprawniony się zgłosił (mimo że ubezpieczyciel nie ma już obowiązku wypłaty świadczenia). Osoba uprawniona może nawet nie wiedzieć, że przysługuje jej świadczenie.

Inne obowiązki z RODO związane z przetwarzaniem danych osobowych

Z zasadą ograniczenia przetwarzania danych osobowych związane są także inne obowiązki wynikające z RODO, tj.:

- spełnienie obowiązku informacyjnego: administrator danych ma obowiązek podania okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – kryteria ustalania tego okresu (art. 13 ust. 2 lit. a RODO oraz art. 14 ust. 2 lit. b RODO);
- osoba, której dane dotyczą, jest uprawniona do uzyskania dostępu do danych osobowych oraz następujących informacji: w miarę możliwości planowanego okresu przechowywania danych osobowych, a gdy nie jest to możliwe – kryteria ustalania tego okresu (art. 15 ust. 1 lit. d RODO);
- w rejestrze czynności przetwarzania umieszcza się, jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych (art. 30 ust. 1 lit. f RODO);
- właściwy organ nadzorczy zatwierdza wiążące reguły korporacyjne, w których określone zostaje zastosowanie ogólnych zasad ochrony danych – w szczególności ograniczenia celu, minimalizacji danych, ograniczonych okresów przechowywania, jakości danych (art. 47 ust. 2 lit. d RODO).

Podsumowanie

W związku z powyższymi uwagami do czasowego ograniczenia przetwarzania danych osobowych administrator przy wdrażaniu polityki retencyjnej powinien wziąć pod uwagę następujące zasady:

- nie jest dopuszczalne przechowywanie pełnego zakresu danych przez najdłuższy możliwy w danym stanie faktycznym okres (np. gdyby w odniesieniu do danego klienta najdłuższy był okres wynikający z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, zbędne może być przechowywanie w rejestrze transakcji pełnej dokumentacji medycznej klienta);
- w razie przechowywania danych osobowych zebranych w celu wykonania umowy, po upływie okresów przedawnienia, jeżeli nie upłynął okres wynikający z innych przepisów (np. przepisów rachunkowych), dopuszczalne jest przechowywanie na podstawie tych przepisów tylko tych danych, które stanowią dowody księgowe;
- odpowiednie wyodrębnienie w systemach informatycznych danych przetwarzanych w konkretnym celu (lub przechowywanie ich w innych systemach np. księgowych);
- liczenie okresu retencji danych osobowych dla każdej umowy (dla każdego celu przetwarzania) odrębnie. W sytuacji gdy klient korzysta z dwóch różnych usług (zawarł dwie umowy) oraz jeżeli okres retencji danych z pierwszej umowy (dla której przetwarzany jest szerszy zakres danych) upłynął wcześniej, niezbędne jest usunięcie wszystkich tych danych, które nie są wykorzystywane na

[8] Zob. wyrok SN z 24.4.2003 r., I CKN 316/01, OSNC 2004, Nr 7–8, poz. 117.

[9] *E. Gniewek, P. Machnikowski* (red.), Kodeks cywilny. Komentarz. Wyd. 7, komentarz do art. 120 KC, Legalis/el. 2018.

potrzeby drugiej umowy (danych, które nie są niezbędne dla drugiej usługi);
- odpowiednie oznaczanie danych klienta w systemie w zależności od wystąpienia zdarzeń wpływających na okres biegu przedawnienia roszczeń;
- odpowiednie przeszkolenie pracowników;
- dokonywanie regularnej oceny zawartości swoich systemów informatycznych pod kątem usuwania zbędnych danych.

Słowa kluczowe: dane osobowe, retencja danych osobowych, zasada czasowości, zasada ograniczenia przechowywania danych osobowych, RODO, ubezpieczenia, polityka retencyjna, retencja danych osobowych w zakładach ubezpieczeń.

Limitation principle regarding personal data retention based on GDPR

The aim of the present study is to show limitation principles regarding personal data retention from GDPR and proposing terms of retention of data regarding different purposes of processing personal data while allowing for insurance companies.

Keywords: personal data, retention of personal data, limitation principle, limitation principle regarding personal data, GDPR, insurance, retention policy, retention of personal data in insurance companies.

Nowe formy szczególne czynności prawnych w Kodeksie cywilnym – dokumentowa oraz elektroniczna – a obowiązywanie rozporządzenia eIDAS

Justyna Adamczyk[1]

W niniejszym opracowaniu autorka opisuje zmiany w polskim porządku prawnym, które są następstwem przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[2]. Autorka omawia nowelizację Kodeksu cywilnego ze szczególnym uwzględnieniem formy dokumentowej oraz elektronicznej. Porusza kwestię definicji dokumentu oraz wskazuje, czym jest informacja oraz nośnik, a także odwołuje się do prawa unijnego. Nawiązuje również do wybranych zagadnień regulowanych przez rozporządzenie eIDAS, np. usług zaufania czy eID. Opisuje wpływ rozporządzenia eIDAS na polską infrastrukturę techniczną. W podsumowaniu ocenia nowe przepisy i przedstawia swe wnioski oraz postulaty.

Uwagi wstępne

Przepisami ustawy z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw[3] wprowadzono do obrotu prawnego kolejne typy czynności prawnej – formę dokumentową oraz formę elektroniczną. Przepisy wspomnianej ustawy weszły w życie 8.9.2016 r. Według uzasadnienia projektu tej nowelizacji uregulowanie nowej formy (dokumentowej) ma służyć ułatwieniu zawarcia czynności prawnych (np. umowy), jak również pełnić rolę dowodu zgodnie z normami Kodeksu postępowania cywilnego[4]. Odnosząc się do formy elektronicznej, projekt wskazał na potrzebę jednoznacznego wyróżnienia oddzielnej formy szczególnej, lecz równocześnie równoważnej formie pisemne[5].

Co więcej, nowelizacja z 10.2.2015 r. jest kolejnym krokiem na drodze do informatyzacji procedury cywilnej. Według uzasadnienia projektu tej ustawy zarówno możliwości techniczne polskiego sądownictwa, jak i wiedza prawników w zakresie nowych technologii zostały wzięte pod uwagę. Taki zabieg ma zagwarantować, że wprowadzona regulacja nie będzie wyłącznie martwą literą, niewykorzystywaną w praktyce z racji niedostosowania do aktualnych uwarunkowań[6].

Forma dokumentowa

Zmiany art. 73, 74 oraz 76 KC są następstwem uregulowania w ustawie kolejnej formy czynności prawnych – formy dokumentowej. W sytuacji gdy forma dokumentowa zostanie zastrzeżona dla danej czynności prawnej, następstwa jej niezachowania stanowią analogię do następstw niezachowania formy pisemnej. Na podstawie art. 73 § 1 KC (w brzmieniu po nowelizacji) rygor nieważności przedmiotowej formy musi jednoznacznie być wskazany przez ustawę, by móc traktować ją jako formę *ad solemnitatem*. Gdy rygor nieważności nie zostanie wskazany przez ustawę, należy uznać, że przedmiotowa forma została zastrzeżona *ad probationem* (art. 74 § 1 KC)[7]. Przepis ten nie znajduje zastosowania, kiedy forma dokumentowa została zastrzeżona *ad eventum*. Zgodnie z art. 74 § 2 KC niedochowanie formy dokumentowej *ad probationem* nie skutkuje ograniczeniami dowodowymi w trzech przypadkach: zgoda obu stron, na żądanie konsumenta w sytuacji sporu, dojście do skutku czynności prawnej uprawdopodobniono w dokumencie. Zgodnie z art. 74 § 3 KC w przypadku niedochowania formy dokumentowej zastrzeżonej wyłącznie dla czynności prawnej jednej ze stron druga strona może żądać dopuszczenia dowodów – ze świadków bądź przesłuchania stron – by potwierdzić dojście do skutku danej czynności prawnej[8].

Stosownie do treści art. 74 § 4 KC następstwa niedochowania właściwej formy czynności prawnej w przypadku przedsiębiorców unormowano odmiennie[9]. Gdy dana forma nie zostanie zachowana i nie poczyniono zastrzeżenia co do rygoru nieważności, nie przyniesie to żadnych konsekwencji w odniesieniu do ważności samej czynności prawnej, jak

[1] Prawnik specjalizujący się w prawie cywilnym, postępowaniu cywilnym, prawie prywatnym międzynarodowym oraz prawie międzynarodowym publicznym.

[2] Dz.Urz. UE L Nr 257, s. 73; dalej jako: Rozporządzenie eIDAS.

[3] Dz.U. poz. 1311; dalej jako: nowelizacja z 10.7.2015 r.

[4] Uzasadnienie projektu ustawy z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, https://legislacja.rcl.gov.pl/docs//2/177283/177315/177316/dokument109786.pdf (dostęp z 26.11.2016 r.), s. 4; dalej jako: uzasadnienie projektu nowelizacji z 10.7.2015 r.

[5] *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny (wyciąg), [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Komentarz, Warszawa 2016, s. 92.

[6] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 1.

[7] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 1.

[8] *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny…, s. 66–67.

[9] *Ibidem*, s. 55.

również nie nałoży ograniczeń dowodowych. Ustawodawca poprzez nowelizację art. 74 § 4 KC chciał rozwiać wszelkie wątpliwości odnośnie do zmiany rygoru dowodowego na rygor nieważności. Niezachowanie formy dokumentowej bez rygoru *ad solemnitatem* nie wpływa ani na sankcje dowodowe, ani na ważność samej czynności prawnej dokonanej między przedsiębiorcami[10].

Strony danej umowy, poza zastrzeżeniem w niej formy dokumentowej, powinny ustalić następstwa jej niedochowania. Nieistnienie tego uzgodnienia w postanowieniach umowy skutkuje tym, że przedmiotowa forma (w niejasnych sytuacjach) jest postrzegana jako zastrzeżona *ad probationem* (art. 76 KC)[11].

Według aktualnego (znowelizowanego) brzmienia art. 77 § 2 KC rozwiązanie umowy (z uzyskaną uprzednio zgodą obu stron), odstąpienie, jak też jej wypowiedzenie dokonywane są w formie dokumentowej. Ustawa bądź umowa może przewidywać w takim wypadku inne rozwiązanie. Wcześniej czynności te należało stwierdzić pismem. Warto wskazać, jak SN określił w swoim orzecznictwie interpretację wskazanego sformułowania – „stwierdzić pismem". Zgodnie z wyrokiem SN z 6.11.2002 r.[12] wymóg stwierdzenia pismem zostaje spełniony, gdy oświadczenie woli wyrazi się tak, że jest ono powiązane z pismem, czyli przykładowo paragonem. Opisane rozwiązanie spełnia również warunki właściwe formie dokumentowej. Nowelizacja art. 77 § 2 KC pozwala podmiotom dokonać wybraną następczą czynność prawną przy pomocy nośnika informacji różnego od pisma[13].

Nowe brzmienie art. 77^1 § 2 KC odnosi się do obrotu profesjonalnego i sytuacji, gdy umowa dochodzi do skutku z wyłączeniem przedmiotowej formy. W takim wypadku jeden z przedsiębiorców musi bez zbędnej zwłoki potwierdzić treści tej umowy przy użyciu dokumentu adresowanego do drugiego przedsiębiorcy, co daje skutek w postaci obowiązywania umowy o treści ustalonej takim dokumentem. Konieczne jest, aby dokument potwierdzający przewidywał takie zmiany bądź uzupełnienia umowy, które nie wpływają znacznie na jej treść. Dodać należy, że niezwłoczny sprzeciw drugiego przedsiębiorcy dokonany w dokumencie niweczy cały zabieg. Wzorem dla wspomnianego przepisu jest przepis przewidujący zbliżone w swej treści konsekwencje związane z formą pisemną i jej zachowaniem przy zawieraniu umów. Rola wskazanych norm polega na tym samym – pozytywny wpływ na obrót profesjonalny[14].

Zgodnie z art. 77^2 KC zachowanie formy dokumentowej wymaga oświadczenia woli, które złożone jako dokument pozwala wskazać autora tego oświadczenia woli[15]. W kwestii tej mogą pojawić się pewne trudności, ponieważ strony mogą poddawać w wątpliwość, kto jest twórcą np. wiadomości SMS[16]. Przepis ten zatem wskazuje dwie przesłanki, które trzeba spełnić równocześnie[17].

Na podstawie nowelizacji z 10.7.2015 r. można zauważyć, że prawodawca zdecydował się na zastosowanie ustawowej formy dokumentowej do dwóch sytuacji. Pierwsza z nich odnosi się do ww. art. 77 § 2 KC, natomiast druga dotyczy art. 720 § 2 KC. Zgodnie z powołanym przepisem forma dokumentowa zastrzeżona *ad probationem* musi zostać zachowana wyłącznie w przypadku zawierania umowy pożyczki o wartości powyżej 1000 zł. Korzystanie z formy dokumentowej w przypadku pozostałych czynności prawnych jest uzależnione od woli stron danej czynności prawnej. Gdy umowa pożyczki dotyczy wartości poniżej 1000 zł, nie stosuje się rygorów *ad probationem*. Udowodnienie dojścia do skutku tej umowy będzie możliwe za pomocą każdego istniejącego środka dowodowego (włączając zeznania świadków oraz przesłuchanie stron)[18].

1. Forma tekstowa

Wzorcem dla wprowadzenia formy dokumentowej została forma tekstowa, zaczerpnięta z niemieckiego porządku prawnego. Formę tekstową należy zastrzec, wtedy gdy dojście do skutku czynności nie wymaga ani formy pisemnej, ani elektronicznej. Dostateczne są znaki pisemne, które pomogą ustalić autora oświadczenia woli (np. wiadomość mailowa). Forma tekstowa została usytuowana w niemieckim porządku prawnym między dwoma innymi formami – pisemną oraz ustną[19]. Wprowadzone przez polskiego ustawodawcę regulacje pokazują, że forma dokumentowa jest rozumiana szerzej niż forma tekstowa[20].

Pierwsze regulacje (prawa niemieckiego) odnoszące się do ww. formy stawiały warunek, by autor oświadczenia woli własnoręcznie podpisał się albo należało umieścić wzmiankę identyfikującą autora oświadczenia woli. Nawiązując do metody przechowywania oświadczenia woli złożonego z zachowaniem formy tekstowej, nie wymagano tutaj uwzględniania potrzeby jego niezwłocznego odtworzenia, bez posługiwania się przy tym środkami pomocniczymi[21].

2. Dokument

Pojęcie „dokumentu" należy do elementarnych pojęć prawa cywilnego, a jego zastosowanie jest tak szerokie, że

[10] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 2.
[11] *J. Gołaczyński, D. Szostek* (red.), Kodeks cywilny…, s. 67.
[12] I CKN 1158/00, Legalis.
[13] *M. Gutowski* (red.), Kodeks cywilny. Komentarz, t. 1, Warszawa 2016, s. 541.
[14] *Ibidem*, s. 530–538.
[15] *E. Gniewek*, *P. Machnikowski* (red.), Kodeks cywilny. Komentarz, wyd. 7, Legalis/el. 2016.
[16] M. Gutowski (red.), Kodeks…, s. 540.
[17] *E. Gniewek*, *P. Machnikowski* (red.), Kodeks…
[18] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 5; *M. Gutowski* (red.), Kodeks…, s. 541–542.
[19] *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny…, s. 64–65.
[20] Uzasadnienie projektu nowelizacji z 10.7.21015 r., s. 4.
[21] *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny…, s. 64–65.

opisuje dokumenty różnego typu, jak też spełniające odmienne funkcje. Legalna definicja tego terminu zatem pełni funkcję porządkującą oraz doprowadziła do zerwania z jego tradycyjną interpretacją, nawiązującą jedynie do pisemnej postaci. Zaproponowana przez ustawodawcę definicja dokumentu (art. 77^3 KC) odwołuje się do oświadczenia woli (czyli informacji, z którą można zapoznać się). Ma to podstawę w pochodzeniu wyrazu dokument od łacińskich słów: *do* (łac. dać, udzielać)[22] oraz *mens* (łac. myśl)[23]. Dokument tworzą dwa elementy występujące jednocześnie – informacja, którą można odtworzyć, i nośnik. Głównym atrybutem dokumentu pozostaje informacja – zawartość mieszcząca w sobie różnorodne oświadczenia. Zawartość tę należy właściwie utrwalić. Taka definicja nie traktuje podpisu jako konstytutywnego elementu dokumentu.

Z punktu widzenia metody przygotowania dokumentu definicja daje dowolność co do ujawnienia jego zawartości (np. poprzez dźwięk), jak również utrwalenia za pomocą wybranego nośnika (np. papier) i urządzenia (np. telefon komórkowy). Technologiczna neutralność omawianej definicji zostaje ograniczona poprzez pełnienie roli dowodu przez dokument. Utrwalić informację należy przy użyciu środka, który pozwoli ją zachować oraz odtworzyć w późniejszym czasie[24]. Definicja dokumentu nie określa typu nośnika. Dokument, który ma postać elektroniczną, zawiera informację zapisaną w pliku, czyli jest to jej nośnik. Wspomniany nośnik jest czymś innym niż informatyczny nośnik danych (miejsce, na którym został zapisany dokument)[25].

Słowo dokument pojawia się również w innych przepisach Kodeksu cywilnego, np. w art. 78 KC. Analizując wskazane przepisy, można dojść do wniosku, że pojęciu dokument nadano różne znaczenia. Niejednolita treść wskazanego terminu utrudnia jego interpretowanie. Szeroka i dosłowna interpretacja omawianego terminu nie jest zgodna z wykładnią systemową. Lepszym rozwiązaniem wydaje się wąska interpretacja terminu dokument (art. 77^3 KC) . Domniemuje się, że ustawodawca miał na myśli nośniki informacji niespełniające kryteriów właściwych dla innych form czynności prawnych (dokument *sensu stricto*)[26].

Wprowadzone nowelizacją szerokie ujęcie dokumentu wiąże się z postępem technologicznym. Zyskujące na popularności korzystanie z elektronicznych instrumentów wymiany informacji musiało zostać uregulowane przez ustawodawcę. Stronom zawierającym umowy należało zagwarantować, w sytuacji wystąpienia na drogę sądową, możność udowodnienia dojścia umowy do skutku oraz jej treści. Obecnie dokument może mieć zupełnie inną postać niż tradycyjnie przygotowany przy użyciu znaków graficznych. Za przykład może posłużyć protokół elektroniczny, który mieści w sobie różnorodne elementy, m.in. zapis graficzny oraz foniczny. Nowelizacja bez wątpienia przyczyni się do uproszczenia spraw sądowych, głównie dzięki wprowadzeniu definicji legalnej dokumentu. Pomoże również rozwiązać trudności związane z dokumentami obejmującymi treść różną od liter alfabetu. Istota wprowadzanych norm sprowadza się do wskazania elementarnych atrybutów dokumentu. Należy pamiętać, że z uwagi na szczególne okoliczności dokument będzie sporządzany w konkretnej postaci. Za dostateczne należy uznać wskazanie autora oświadczenia woli. Uregulowanie nowej formy doprowadziło do wytworzenia legalnej podstawy dla formy występującej wcześniej w obrocie (np. wiadomość SMS)[27].

Według definicji legalnej dokumentu powinno się dokonać klasyfikacji dokumentów na te, które zawierają tekst, i pozostałe dokumenty. Biorąc pod uwagę definicję legalną dokumentu, można stwierdzić, że dokument prywatny zawierający podpis daje wyłącznie możliwość odnalezienia autora oświadczenia, chociaż może zostać to ustalone za pomocą odmiennej metody[28].

3. Nośnik

Obowiązująca obecnie konstrukcja prawna formy dokumentowej daje duże pole w kwestii wyboru nośników informacji. Stawia ona jednak warunek, aby wybrany nośnik po zapisaniu na nim określonej informacji umożliwił jej odczytanie po jakimś czasie. Czynność prawną można zatem przedstawić graficznie, dźwiękowo oraz za pomocą obrazów. Utrwalenia można dokonać, wykorzystując takie nośniki, jak m.in.: kartka papieru, pendrive, płyta DVD, dysk twardy, Blu-ray[29].

Do zapisania dokumentu można wykorzystać informatyczny nośnik danych bądź można wykorzystać kilka takich nośników, a każdy z nich posiada wyłącznie fragment dokumentu. By móc odtworzyć taki dokument, należy posłużyć się właściwym programem, który importuje dane ze wszystkich informatycznych nośników danych. Wspomniane warunki towarzyszą interoperacyjności (ang. *interoperability*)[30], w przypadku której należy posłużyć się właściwym systemem teleinformatycznym, by móc odczytać zapisane w kilku lokalizacjach dane. Gdy do zbadania dokumentu zostaje powołany biegły (informatyk), w pewnych przypadkach obowiązkowe będzie zbadanie kilku informatycznych nośników danych. Rozumienie dokumentu w przedstawiony sposób przystaje do współczesnych metod utrwalania danych[31].

[22] *J. Sondel*, Słownik łacińsko-polski, Kraków 2009, s. 305.
[23] *Ibidem*, s. 618.
[24] Por. *D. Szostek*, Nowe ujęcie dokumentu w prawie prywatnym, PME 2011, Nr 2, s. 13–14.
[25] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 3.
[26] *E. Gniewek, P. Machnikowski* (red.), Kodeks…
[27] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 4 i 6.
[28] *Ibidem*, s. 7–8.
[29] *J. Gołaczyński, D. Szostek* (red.), Kodeks cywilny…, s. 74–75.
[30] Zob. *G. Szpor,* Administracyjnoprawne problemy informatyzacji, [w:] *J. Supernat* (red.), Między tradycją a przyszłością w nauce prawa administracyjnego, Wrocław 2009, s. 722 i n.
[31] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 3.

4. Informacja

W definicji dokumentu pojawia się również termin informacja, który jest tłumaczony przez różne dziedziny[32]. Trafna wydaje się (zdaniem autora niniejszego artykułu) interdyscyplinarna definicja informacji przyjęta przez *G. Szpor*. Zdaniem tej autorki informacja to dobro (niematerialne) przenaszalne, które zmniejsza niepewność oraz można utrwalić je za pomocą nośnika fizycznego, jak również przekazywać[33]. Taka koncepcja pasuje do przypisanej dokumentowi funkcji dowodowej – minimalizowania niepewności[34].

Forma elektroniczna

W art. 78[1] KC wyróżniono kolejną formę czynności prawnych – formę elektroniczną[35]. Na wstępie warto zwrócić uwagę na fakt, że przed nowelizacją przedstawiciele doktryny prezentowali różne stanowiska co do istnienia formy elektronicznej jako odrębnej formy czynności prawnych[36].

Formę tę zachowuje się, gdy oświadczenie woli zostaje złożone w postaci elektronicznej. Powinno się opatrzyć je również bezpiecznym podpisem elektronicznym, który jest weryfikowany za pośrednictwem ważnego kwalifikowanego certyfikatu (art. 78[1] § 1 KC). Należy zauważyć, że forma elektroniczna jest traktowana w zasadzie na równi z tradycyjną formą pisemną (zgodnie z obecnym brzmieniem art. 78[1] § 2 KC). Zrównanie to może spotkać się z pewnymi odstępstwami przewidzianymi w ustawie lub pochodzącymi od stron czynności prawnych[37].

Do tej pory stanowisko doktryny dotyczące wyróżnienia nowej formy nie było jednorodne. Za zmianami opowiadali się m.in.: *Z. Radwański*[38], *D. Szostek*[39] i *M. Świerczyński*[40]. Autorzy argumentowali swe stanowisko różnicami w funkcjach spełnianych przez podpis zwykły (własnoręczny) i elektroniczny. Inną koncepcję przyjął w tym zakresie *W. Kocot*[41], który wskazywał, że dokument elektroniczny powinien zostać uregulowany w sposób zbliżony do formy pisemnej w zakresie skutków dochowania formy. Spór w doktrynie obejmował także art. 79 KC, który normuje składanie oświadczenia przez osoby, które nie są w stanie pisać, ale potrafią czytać. Po nowelizacji Kodeksu cywilnego i wyróżnieniu nowej formy (elektronicznej) wspomniany przepis ma zastosowanie jedynie w przypadku jednej formy – pisemnej[42].

Z uwagi na wyróżnienie nowej formy ustawodawca dokonał również zmian w brzmieniu art. 73 oraz 74 KC. Gdy forma elektroniczna została zastrzeżona ustawowo, jej niezachowanie skutkuje nieważnością, kiedy rygor nieważności został wskazany w ustawie (art. 73 § 1 KC). Gdy forma elektroniczna zastrzeżona bez rygoru nieważności nie zostanie zachowana, w sytuacji sporu dochodzi do ograniczeń dowodowych. Jednakże regulacja ta nie ma zastosowania w przypadku zastrzeżenia formy wyłącznie *ad eventum* (art. 74 § 1 KC). W art. 74 § 3 uregulowano natomiast sytuację zastrzeżenia formy elektronicznej i jej niedochowania dla oświadczenia woli złożonego przez jedną stronę czynności prawnej[43].

Wprowadzona nowelizacja uchyliła art. 78 § 2 KC odnoszący się do e-podpisu[44]. Wskazane zmiany wiążą się z obowiązywaniem nowego unijnego rozporządzenia – rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[45].

Rozporządzenie eIDAS

Państwa członkowskie mają obowiązek przestrzegać przepisów przedmiotowego rozporządzenia eIDAS (ang. *Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*) od 1.7.2016 r. Akt ten zastąpił dyrektywę Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram z zakresie podpisów elektronicznych[46]. Projekt rozporządzenia eIDAS został przyjęty 3.4.2014 r. Należy wspomnieć, że rozporządzenie stosuje się bezpośrednio w porządkach prawnych państw członkowskich. Wprowadza ono także jednolite przepisy dla wszystkich państw UE[47].

[32] Zob. np. *P. Fajgielski*, Informacja w administracji publicznej – prawne aspekty gromadzenia, udostępniania i ochrony, Wrocław 2007, s. 13 i n.; *J. Janowski*, Technologia informacyjna dla prawników i administratywistów, Warszawa 2009, s. 71 i n.; *W. Wiewiórowski*, *G. Wierczyńki*, Informatyka prawnicza, wyd. 2, Warszawa 2008, s. 29 i n.

[33] *G. Szpor*, Informacja w zagospodarowaniu przestrzennym. Zagadnienia administracyjnoprawne, Katowice 1998, s. 25–26.

[34] *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny…, s. 81.

[35] *Ibidem*, s. 92.

[36] Zob. *J. Gołaczyński*, Umowy elektronicznie w obrocie gospodarczym, Warszawa 2005, s. 78–86. Autor ten opowiedział się za koncepcją wskazującą na istnienie formy elektronicznej jako oddzielnej formy czynności prawnych od momentu wejścia w życie nowelizacji z 10.7.2015 r. Z tego powodu autor sformułował temat swojej pracy jak na wstępie. Por. *P. Podrecki*, Prawo internetu, wyd. 2, Warszawa 2007, s. 98.

[37] Uzasadnienie projektu nowelizacji z 10.7.2015 r., s. 5.

[38] Zob. *Z. Radwański* (red.), System prawa prywatnego, t. II, Warszawa 2002, s. 165–166.

[39] Zob. *D. Szostek*, Czynność prawna a środki komunikacji elektronicznej, Kraków 2004, s. 215 i n.

[40] Zob. *M. Świerczyński*, Podpis elektroniczny w praktyce handlowej, dodatek do MoP 2002, Nr 24, s. 9.

[41] Por. *W. Kocot*, Elektroniczna forma oświadczenia woli, PPH 2001, Nr 3, s. 3.

[42] *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny…, s. 92–93.

[43] Por. *J. Gołaczyński, D. Szostek* (red.), Kodeks cywilny…, s. 95.

[44] *J. Gołaczyński, D. Szostek* (red.), Kodeks cywilny…, s. 92. Por. *J. Kaspryszyn*, Podpis elektroniczny osoby niemogącej pisać, [w:] *J. Gołaczyński* (red.), Prawo umów elektronicznych, Kraków 2006, s. 30–36.

[45] Dz.Urz. UE L Nr 257, s. 73; dalej jako: rozporządzenie eIDAS.

[46] Dz.Urz. UE L Nr 13, s. 12.

[47] *A. Kujaszewska*, eIDAS, een.org.pl/index.php/prawo-578/blind_style/1/page/4/articles/eidas.html (dostęp z 27.11.2016 r.).

Wprowadzona regulacja ujednolica stanowisko dotyczące usług zaufania, które gwarantują pewność transakcji transgranicznych. Rozporządzenie eIDAS unormowało również tak zwane mechanizmy umożliwiające identyfikację elektroniczną (skrót z ang. *eID*)[48], które dokładnie sprawdzają personalia osób korzystających z usług w sieci. Wprowadza nowe usługi zaufania, ochrony stron www, doręczenia oraz pieczęci elektroniczne, jak też odnoszące się do nich usługi konserwacji oraz walidacji[49].

1. Motywy przyjęcia nowego rozporządzenia

Przedmiotowe rozporządzenie ma wpłynąć pozytywnie na poziom ufności co do zawieranych transakcji elektronicznych. Przyczyni się to do poprawy efektywności publicznych oraz prywatnych usług online, w tym usług transgranicznych. Wpłynie również pozytywnie zarówno na tak zwany e-biznes, jak i transakcje handlowe dokonywane online. Bardzo często obywatele mają problem z posługiwaniem się własną tożsamością elektroniczną, by móc uwierzytelnić się na obszarze pozostałych państw członkowskich. Powodem takiego stanu rzeczy jest nieobecność systemu wzajemnej uznawalności mechanizmów identyfikacji elektronicznej. Uniemożliwia to prawidłowe funkcjonowanie rynku wewnętrznego. Uznawane na zasadzie wzajemności środki służące identyfikacji elektronicznej powinny wpłynąć korzystnie na wewnątrzrynkowy obrót. Należy również zagwarantować pewny system elektronicznej identyfikacji oraz autoryzacji, który posłuży korzystaniu z transgranicznych usług elektronicznych. Zapewni to każdemu obywatelowi (państwa należącego do UE) możliwość wykonania urzędowych obowiązków w innym państwie członkowskim UE za pośrednictwem usługi elektronicznej[50].

By móc osiągnąć cele przyświecające wprowadzeniu nowego rozporządzenia, sformułowano wymogi dla wzajemnego uznawania środków służących identyfikacji, a także określono legalne granice funkcjonowania następujących instrumentów elektronicznych: podpisów, pieczęci, znaczników czasu, jak również dokumentów elektronicznych. Wymienić należy jeszcze w tym miejscu usługi związane z doręczeniami elektronicznymi oraz służące autoryzacji witryn internetowych. Przepisy rozporządzenia eIDAS normują także odpowiedzialność za wyrządzenie szkody oraz mechanizmy współdziałania członków UE, które służą wykonaniu założeń przedmiotowego rozporządzenia. Rozporządzenie eIDAS w swych postanowieniach odnosi się do zagadnienia podpisu elektronicznego poprzez wdrożenie zasady mówiącej o stwarzaniu korzystnych warunków technicznych dla obsługi różnych formatów zaawansowanych podpisów elektronicznych. Rozporządzenie to traktuje także o ustanowieniu specjalnego znaku dla oznaczenia kwalifikowanych usług zaufania publicznego. Ułatwi to dostawcom wspomnianych usług ich oznaczenie. Przygotowaniem znaku zajmie się Komisja. Ponadto, w nawiązaniu do usług zaufania, należy wskazać, że rozporządzenie eIDAS przewiduje: konsekwencje związane z posługiwaniem się usługami zaufania, kryteria, jakie mają spełnić dostawcy omawianych usług, nadzór, jak również normy o odpowiedzialności za spowodowanie szkód (będących następstwem nierespektowania jego regulacji)[51].

2. Zmiany w polskim ustawodawstwie i dostosowanie infrastruktury technicznej

Wejście w życie nowego rozporządzenia jest związane z obowiązkiem dokonania zmian w polskim ustawodawstwie. Ustawa z 5.9.2016 r. o usługach zaufania oraz identyfikacji elektronicznej[52] uchylająca dotychczas obowiązujące przepisy o podpisie elektronicznym, czyli ustawę z 18.9.2001 r. o podpisie elektronicznym[53], weszła w życie 7.10.2016 r. Ponadto nowa ustawa reguluje zarówno właściwą terminologię, jak i zagadnienia, które państwa członkowskie samodzielnie mogą unormować[54].

Poza zmianami w przepisach należy także przystosować systemy informatyczne. Bliższa analiza jest niezbędna w zakresie zagadnienia uznawania trzech instrumentów unijnych: kwalifikowanego znacznika czasu, pieczęci elektronicznej oraz podpisu elektronicznego. Zarówno przedsiębiorcy, jak i organy administracji publicznej winni są podjąć działania na rzecz dostosowania własnych programów obsługujących podpisy elektroniczne do aktów wykonujących rozporządzenie eIDAS oraz do najnowszych standardów. Co w takim razie dzieje się w sytuacji, gdy dany podmiot nie może we własnym zakresie przystosować swych aplikacji do audytu podpisów oraz pieczęci elektronicznych? Rozwiązanie jest proste – należy zwrócić się do dostawcy usług zaufania.

3. Usługi publiczne a rozporządzenie eIDAS

Rozporządzenie eIDAS przyczynia się również do progresu usług z sektora publicznego. Postanowienia odnoszące się do podpisów elektronicznych nakładają również na państwa zobowiązania w przedmiocie regulacji systemów weryfikujących podpisy zaawansowane pochodzące z pozostałych państw. Zmiany mają co najmniej uwzględniać formaty wy-

[48] Zob. e-Identification, https://ec.europa.eu/digital-single-market/en/e-identification (dostęp z 16.12.2016 r.).

[49] Obowiązek stosowania Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 – od 1.7.2016 r., https://mc.gov.pl/aktualnosci/obowiazek-stosowania-rozporzadzenia-parlamentu-europejskiego-i-rady-ue-nr-9102014-od-1 (dostęp z 27.11.2016 r.).

[50] *A. Kujaszewska*, eIDAS…

[51] *Ibidem.*

[52] Dz.U. poz. 1579.

[53] T.j. Dz.U. z 2013 r., poz. 262, nieobow.

[54] Obowiązek stosowania...

mienione w decyzji wykonawczej Komisji (UE) 2015/1506 z 8.9.2015 r. ustanawiającej specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego, zgodnie z art. 27 ust. 5 i art. 37 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym[55]. Kwalifikowane podpisy elektroniczne są uznawane na zasadzie wzajemności w poszczególnych państwach członkowskich usług. Urzędy przystosowują własne aplikacje akceptujące podpisy elektroniczne, tak by uwzględniały one listy TSL (ang. *Trusted Services Status List*)[56].

Forma dokumentowa a rozporządzenie eIDAS

Przy omawianiu wzajemnej relacji między formą dokumentową a rozporządzeniem eIDAS szczególna uwaga zostanie zwrócona na pojęcie dokumentu. Definicja dokumentu obowiązująca obecnie na mocy art. 77^3 KC jako uniwersalna i technologicznie neutralna obejmuje dokumenty sporządzone w tradycyjnej oraz elektronicznej postaci[57]. Polski prawodawca jasno odróżnia od siebie pojęcie formy czynności prawnych oraz dokumentu. Forma nie stanowi komponentu dokumentu, lecz wpływa na złożone oświadczenie woli. Definicja dokumentu europejskiego prawodawcy nie cechuje się uniwersalnością. Rozporządzenie eIDAS określa pojęcie dokumentu elektronicznego (art. 3 pkt 35) jako zachowaną w postaci elektronicznej treść, odnoszącą się m.in. do tekstu czy zapisu wizualnego. Rozporządzenie stosowane jest bezpośrednio, więc od 1.7.2016 r. dokumenty powinny być klasyfikowane na te, które posiadają tekst, oraz pozostałe[58].

Forma elektroniczna a rozporządzenie eIDAS

Poza wskazanym w niniejszej pracy art. 78^1 KC istnieją inne normy traktujące o kryteriach zachowania formy elektronicznej. Rozporządzenie eIDAS, jako akt unijny, stosowane jest bezpośrednio przed przepisami krajowymi. Według preambuły (pkt 21) przedmiotowego rozporządzenia zagadnienia obejmujące dojście umowy do skutku, jak również jej ważność bądź tyczące się pozostałych obowiązków prawnych powinny się znaleźć poza jego zasięgiem, wtedy kiedy ustawodawstwo wewnętrzne lub prawo UE uregulowało już kwestię formy. Rozporządzenie eIDAS nie powinno również wpływać na prawo wewnętrzne regulujące formę właściwą rejestrom publicznym, ze szczególnym uwzględnieniem rejestrów handlowych oraz dotyczących gruntów[59].

Wnioskować zatem należy, że przedmiotowe rozporządzenie będzie mieć wpływ na przepisy dotyczące warunków zachowania nowej formy czynności prawnych, ale jedynie pośredni, co wiąże się również z art. 25 ust. 2 rozporządzenia eIDAS[60]. Zrównanie formy elektronicznej oraz pisemnej (na mocy art. 78^1 KC) jest także powiązane z obowiązującym rozporządzeniem eIDAS (art. 25). Według art. 25 rozporządzenia eIDAS podpis elektroniczny wywołuje skutki prawne oraz może być dowodem (podczas procesu sądowego) bez względu na jego postać oraz niespełnianie przez niego kryteriów właściwych kwalifikowanym podpisom elektronicznym. Na mocy ust. 2 tego przepisu doszło do zrównania skutków prawnych kwalifikowanego podpisu elektronicznego oraz podpisu własnoręcznego. Co ważne, regulacje rozporządzenia eIDAS i przepisy nowelizujące Kodeks cywilny nie są ze sobą w żaden sposób sprzeczne. Należy dodać, że niewprowadzenie art. 78^1 KC przy uwzględnieniu obowiązywania art. 25 rozporządzenia eIDAS skutkowałoby traktowaniem uchylonego obecnie art. 78 § 2 KC w kategoriach kolejnego rozwiązania służącego zachowaniu formy pisemnej, w konsekwencji czego wyróżnienie kolejnej formy (elektronicznej) stałoby się zbędnym zabiegiem[61].

Podsumowanie

Przepisy nowelizacji z 10.7.2015 r. obowiązują w polskim porządku od dość niedawna, więc nie jest prostą rzeczą dokonać oceny ich efektywności. Można jednak przedstawić wnioski i postulaty *de lege ferenda*, które pojawiły się po analizie ww. zagadnień.

W pierwszej kolejności zostaną omówione regulacje dotyczące formy dokumentowej. Zaczynając od uzasadnienia wprowadzenia nowej formy czynności prawnej, warto podkreślić, że zostało ono przedstawiono w dość ogólny sposób. Wprowadzanie zmian do części ogólnej Kodeksu cywilnego jest poważnym zabiegiem, który powinien być podyktowany istotnymi motywami mającymi przynieść wiele korzyści.

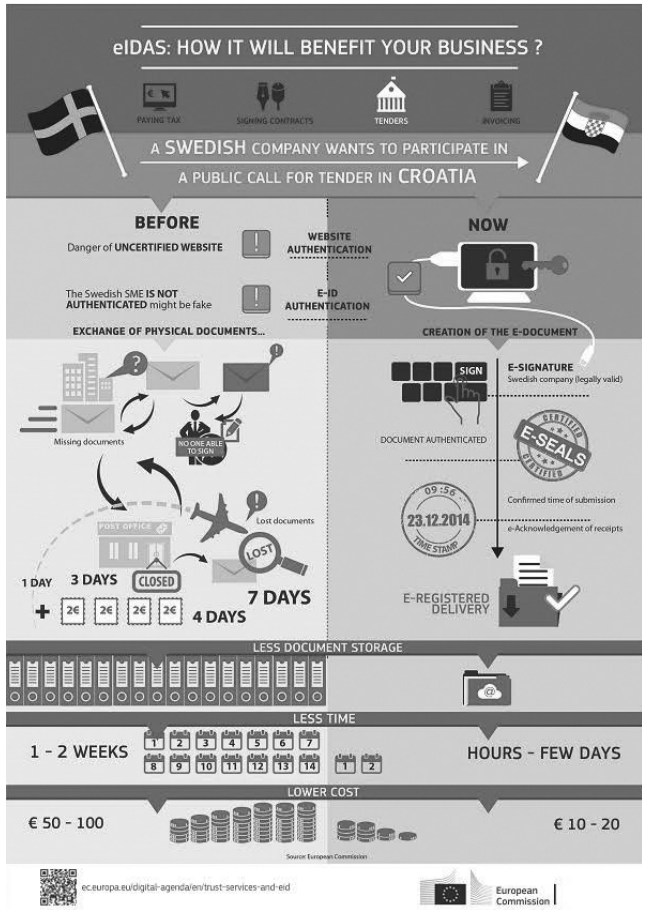
W uzasadnieniu do projektu nowelizacji z 10.7.2015 r. wskazywano na usprawnienie obrotu oraz określenie legalnego zasięgu dla formy już wykorzystywanej. Z uwagi na obowiązujący art. 60 KC należałoby się zastanowić nad tym, czy nowelizacja w zakresie formy dokumentowej była konieczna. Mówiąc o formie dokumentowej (i jej ocenie), nie

[55] Dz.Urz. UE L Nr 235, s. 37.
[56] Obowiązek stosowania..., (dostęp z 28.11.2016 r.).
[57] Por. *W. Kocot*, Wpływ Internetu na prawo umów, Warszawa 2004, s. 334–338; *J. Gołaczyński* (red.), Umowy elektroniczne w obrocie gospodarczym, Warszawa 2005, s. 86–89.
[58] *J. Gołaczyński, D. Szostek* (red.), Kodeks cywilny…, s. 87.
[59] *Ibidem*, s. 93.
[60] Zob. EU trust mark, https://ec.europa.eu/digital-single-market/en/eu-trust-mark (dostęp z 16.12.2016 r.).
[61] *J. Gołaczyńs*ki, *D. Szostek* (red.), Kodeks cywilny…, s. 94.

można pominąć tak doniosłej zmiany w przepisach, jaką było wprowadzenie art. 77^3 KC, czyli nowej definicji dokumentu. Po raz kolejny należy przywołać uzasadnienie do projektu nowelizacji z 10.7.2015 r., w którym nowej definicji przypisuje się funkcję porządkową oraz wskazuje się na jasne zerwanie z tradycyjną interpretacją terminu. Trudno oprzeć się wrażeniu, że występuje tutaj pewna sprzeczność. Porządkowanie nie polega wszak na kreowaniu nowej definicji, lecz na pewnych zabiegach prawnych mniejszej wagi, które pomagają rozwiać wątpliwości przy wykładni pojęcia. Ustawodawca chciał także wskazać konstytutywne cechy wszystkich dokumentów, lecz równocześnie zwrócił uwagę na pojawienie się sytuacji, kiedy możliwe będzie indywidualne ustalenie treści pojęcia dokument. Nasuwa się wniosek, że nowa definicja dokumentu nie jest uniwersalna[62]. Właściwe wydaje się wprowadzenie kolejnych zmian w przepisach, gdyż nowelizacja nie została w należyty sposób przygotowana, co może przełożyć się na nieosiągnięcie zamierzonych celów.

Nowelizacja w odniesieniu do formy elektronicznej może zostać uznana za pozytywną zmianę, gdyż zakończyła spór co do traktowania tej formy jako oddzielnej czy jako rodzaju formy pisemnej. Zrównanie formy pisemnej (zwykłej) oraz elektronicznej także wpłynie korzystnie na obrót prawny. Podmioty zawierające czynność prawną mogą wybrać jedną z form, wtedy kiedy forma pisemna (zwykła) została ustawowo zastrzeżona oraz w sytuacji normowanej art. 76 KC, czyli w sytuacji wymagającej zachowania jedynie formy elektronicznej[63]. Pamiętać jednak należy, że zrównanie form, według treści art. 78^1 § 2 KC, może zostać wyłączone ustawowo bądź poprzez czynność prawną[64]. Choć uzasadnienie do projektu nowelizacji z 10.7.2015 r. nie zawiera zbyt szczegółowych przyczyn wprowadzenia tej formy, to została ona uregulowana w bardziej przemyślany sposób niż forma dokumentowa. W efekcie nowelizacja będzie efektywną regulacją, a nie jedynie martwym przepisem.

Zaprezentowana obok grafika obrazuje korzyści wynikające z obowiązywania rozporządzenia eIDAS.



Rys. 1. Zalety wprowadzenia rozporządzenia eIDAS

Źródło: https://ec.europa.eu/digital-single-market/news/eidas-infographic (dostęp z 16.12.2016 r.).

[62] Por. *M. Gutowski* (red.), Kodeks…, s. 542–543 i 548. Poglądy doktryny pojawiające się we wskazanej pozycji co do ww. zagadnień należy uznać za słuszne.

[63] *E. Gniewek*, *P. Machnikowski* (red.), Kodeks…

[64] Por. *J. Gołaczyński*, *D. Szostek* (red.), Kodeks cywilny…, s. 93; *E. Gniewek, P. Machnikowski* (red.), Kodeks…

Słowa kluczowe: nowelizacja, czynność prawna, forma dokumentowa, forma elektroniczna, dokument, informacja, nośnik, rozporządzenie eIDAS.

New particular forms of legal acts in Civil Code – documental and electronic – and eIDAS regulation being in force

In this article the author describes modifications in Polish law system which are the result of passing the regulation of the European Parliament and the Council 910/2014/2014 of 23.7.2014 in the matter of electronic identification and trust service in relation to electronic transactions on the domestic market and overruling the directive 1999/93/CE. The author presents the amendment of Civil Code, particularly documental and electronic form. She presents issue of document's definition and indicates

what is the information and carrier, moreover appeals to EU law. She also refers to selected issues from eIDAS Regulation, e.g. trust services or eID. Next, she describes the impact of eIDAS Regulation on Polish technical infrastructure. In conclusion, she evaluates new regulations and introduces her deductions and postulates.

Keywords: amendment, legal act, documental form, electronic form, document, information, carrier, eIDAS regulation.

Trolling prawnoautorski (*copyright trolling*) a nadużycie prawa podmiotowego

Anna Skibińska[1]

Gwałtowny rozwój technologiczny oraz legislacja obejmująca coraz to nowe dziedziny życia społecznego sprawiają, że zmianom podlega również specyfika ochrony prawnoautorskiej w Polsce. Stosunkowo nowym zjawiskiem jest m.in. trolling prawnoautorski (w świecie anglojęzycznym znany jako: *copyright trolling* lub *IP trolling*). W niniejszej pracy przedstawiona zostanie jego definicja oraz wyróżniki pozwalające na zakwalifikowanie danego zachowania jako prawnoautorskiego trollingu. Autorka omawia także wewnętrzną typologię tego pojęcia związaną z jego zakresem podmiotowym i przedmiotowym oraz związki prawnoautorskiego trollingu z instytucją nadużycia prawa podmiotowego uregulowaną w art. 5 KC. W podsumowaniu przedstawiono najistotniejsze skutki opisywanego zjawiska oraz postulaty *de lege ferenda* dotyczące kształtu ochrony prawnoautorskiej w polskim ustawodawstwie.

Uwagi wstępne

Trolling prawnoautorski nie został jak dotąd[2] zdefiniowany w żadnym akcie prawnym obowiązującym w Polsce. Dorobek literatury również jest w tym przedmiocie niewielki[3]. Po raz pierwszy sporo uwagi poświęcono temu zjawisku w 2014 r., opisując w mediach sprawę warszawskiej adwokat. Jej kancelaria prawna wysyłała liczne przedsądowe wezwania do zapłaty, zarzucając w nich naruszenie majątkowych praw autorskich poprzez ściąganie oraz rozpowszechnianie za pomocą sieci *peer to peer* popularnych filmów[4]. Co istotne, do pism tych nie dołączano pełnomocnictw, sugerowano, że adresat jest podejrzanym w toczącym się postępowaniu karnym (które w istocie było umorzone bądź znajdowało się w fazie *in rem*) oraz nie wskazywano ani sposobu ustalenia danych osobowych adresata, ani uzasadnienia dla proponowanej kwoty ugodowej. Rzekomy pokrzywdzony nie oświadczał też, jakich roszczeń się zrzeka, co z uwagi na wymóg zgody prokuratora (w postępowaniu przygotowawczym) lub sądu (na etapie postępowania sądowego) dla umorzenia postępowania karnego stawia pod znakiem zapytania skuteczność owej umowy[5]. Trzeba także podkreślić, iż agresywny ton tego typu pism oraz kategoryczne sformułowania nie licowały zwykle z rzeczywistym stanem sprawy, tudzież wagą potencjalnego naruszenia. W rezultacie Okręgowa Rada Adwokacka w Warszawie wszczęła przeciwko adwokat postępowanie dyscyplinarne, ale podobne działania podejmowały w Polsce w ostatnich latach także inne kancelarie.

Trolling prawnoautorski w Polsce – definicja i wyróżnik zjawiska

W nawiązaniu do opisanej wyżej strategii prawnoautorskiego trollingu należy wskazać, że zgodnie z art. 17 ustawy z 4.7.1994 r. o prawie autorskim i prawach pokrewnych[6]: „Jeżeli ustawa nie stanowi inaczej, twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu". Odpowiedzialność cywilną za naruszenie tego przepisu opisano w art. 79 PrAutU. Oprócz roszczenia o zaniechanie naruszania lub usunięcie skutków naruszenia można żądać też naprawienia szkody w oparciu o art. 415 KC i n. lub zapłaty dwukrotności wynagrodzenia, które w chwili jego dochodzenia byłoby należne tytułem udzielenia przez uprawnionego zgody na korzystanie z utworu. *Onus probandi* wykazania szkody oraz związku przyczynowego między szkodą a czynem zabronionym, zgodnie z art. 6 KC, spoczywa na podmiocie dochodzącym przed sądem swoich roszczeń.

Szczególnie istotna w powiązaniu z *copyright trollingiem* jest jednak odpowiedzialność karna uregulowana w art. 116 PrAutU, bowiem to ona przyczynia się do nasilenia omawianego zjawiska w Polsce. Potencjalnych naruszycieli autorskich praw majątkowych identyfikuje się zwykle w wyniku wszczęcia, instrumentalnie tu traktowanego, postępowania karnego oraz połączenia adresu IP z konkretną osobą. W trakcie postępowania organy ścigania ustalają abonenta łącza, czyli osobę kryjącą się za danym adresem IP. Później rzekomi pokrzywdzeni uzyskują dostęp do akt sprawy, a po zdobyciu potrzebnych danych osobowych, nie czekając zazwyczaj na

[1] Autorka jest studentką Kolegium Międzyobszarowych Studiów Indywidualnych na Uniwersytecie Wrocławskim. Jako kierunek wiodący realizuje prawo na Wydziale Prawa Administracji i Ekonomii, a w 2017 r. ukończyła studia I stopnia na Wydziale Filologicznym na kierunku dziennikarstwo i komunikacja społeczna (specjalność: *creative writing*).

[2] Stan na dzień 1.12.2017 r.

[3] Pierwszą definicję sformułowały w liście otwartym do Prezesa NRA organizacje stowarzyszone w projekcie *Copyright Trolling Stop*, następnie powoływała się na nią m.in. *E. Laskowska* – por. *taż*, Konstrukcja ochrony prawnoautorskiej na tle procesu europeizacji prawa prywatnego, Warszawa 2016, s. 327–328 i http://di.com.pl/files/List_otwarty_do_NRA.pdf, s. 1 (dostęp z 24.11.201 r.).

[4] Między innymi: „Czarny Czwartek. Janek Wiśniewski padł" i „Last minute".

[5] Wątek ten zostanie omówiony w dalszej części artykułu.

[6] T.j. Dz.U. 2017 r. poz. 880 ze zm.; dalej jako: PrAutU.

ustalenia organów ścigania, wysyłają wezwania do zapłaty. Tymczasem wypada zaznaczyć, że ludzie obawiają się pism od prawników i często płacą dla „świętego spokoju”[7].

Chcąc zdefiniować występujący współcześnie trolling prawnoautorski, warto wskazać najpierw na kilka cech, jakie immanentnie się z nim wiążą. Zwykle zjawisko to charakteryzuje działanie podmiotów profesjonalnych (kancelarii prawnych)[8] sprofilowanych na masowe zawieranie ugód w związku z rzekomym naruszaniem autorskich praw majątkowych przez adresatów wysyłanych wezwań do zapłaty. W literaturze *copyright trolling* określa się jako swoisty „model biznesowy”, którego celem jest skłonienie zastraszonej osoby do zawarcia ugody, jego opłacalność zapewnia zaś duża skala[9]. Oprócz tego znamiennymi elementami rozważanego zjawiska są agresywne oportunistyczne działania, związane z pragnieniem wywołania u odbiorcy pisma wstydu lub strachu przed ewentualnym dochodzeniem roszczeń w sądzie[10]. Tymczasem, nawet w przypadku niezawarcia sugerowanej umowy, prawnoautorski troll rzadko wszczyna postępowania sądowe.

Między zwykłym dochodzeniem roszczeń a *copyright trollingiem* istnieją trzy podstawowe różnice. Otóż są to: skala ilościowa (masowość rozsyłanych wezwań do zapłaty), skala jakościowa (nikłość dowodów pozwalających na przypisanie naruszenia prawa konkretnemu podmiotowi) oraz zasadnicza dysproporcja w dostępie do profesjonalnej pomocy prawnej, dzieląca strony[11]. Proceder ten bywa też nazywany „monetyzacją naruszeń”, gdyż spieniężanie naruszeń przynosi (w opinii prawnoautorskich trolli) wyższe dochody aniżeli sprzedawanie praw autorskich na rynku[12].

Mając na uwadze przedstawione wyżej właściwości prawnoautorskiego trollingu, należy zdefiniować go jako: sprzeczne z zasadami etyki (natarczywe, agresywne), a przy tym przesadne, masowe oraz nastawione przede wszystkim na szybkie uzyskanie korzyści majątkowych, czynności wykonywane przez podmioty uprawnione lub rzekomo uprawnione do dochodzenia roszczeń z tytułu naruszenia autorskich praw majątkowych.

Wewnętrzna typologia trollingu: trolling *sensu stricto* oraz *sensu largo*, trolling pośredni lub bezpośredni – podmioty trollingu prawnoautorskiego

Przechodząc do omówienia podmiotów zaangażowanych w ten proceder, nawiążę do artykułu, który ukazał się w 2016 r. Zaproponowano tam ciekawy podział trollingu prawnoautorskiego na pośredni – wówczas *copyright trolling* występować może jedynie ze względu na sposób egzekwowania roszczeń (gdy podmiot uprawniony dochodzi owych roszczeń od naruszyciela autorskich praw majątkowych) oraz bezpośredni (gdy roszczeń dochodzi nieuprawniony – zarówno od naruszyciela, jak i od osoby, która nie złamała prawa, bądź też uprawniony, ale tylko od osoby, która nie dopuściła się żadnego naruszenia)[13]. Po zaakceptowaniu doniosłości przedstawionego wyżej podziału warto jednak przyjąć odmienną terminologię, która odnosiłaby się także do profesjonalnego (tj. wykonywanego z pomocą prawników w oparciu o stosowne pełnomocnictwa) bądź nieprofesjonalnego, osobistego dochodzenia autorskich praw majątkowych przez, liczących tutaj na łatwy zarobek, nieuprawnionych lub uprawnionych, w tym twórców[14]. Jako trolling *sensu stricto* sklasyfikować można więc trolling pośredni z przywołanego artykułu, w zbiorczym pojęciu trollingu *sensu largo* umieścilibyśmy zaś także trolling bezpośredni w znaczeniu zaprezentowanym w omawianym artykule. Oba rodzaje tak skategoryzowanego trollingu dzieliłyby się natomiast na trolling bezpośredni (dochodzony osobiście przez uprawnionego lub nieuprawnionego) oraz pośredni (gdzie działają podmioty wyspecjalizowane w tych zagadnieniach). Dzięki takiej typologii zwiększyłaby się sposobność kompleksowego opisania rozważanego zjawiska oraz przejrzystość przeprowadzanych klasyfikacji.

Przedmiot trollingu prawnoautorskiego – definicja utworu oraz kwestia jego rozpowszechniania w sieci *peer to peer*

Zgodnie z definicją legalną zawartą w art. 1 ust. 1 PrAutU utworem nazywamy: „każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek

[7] Por. *K. Kulesza*, Czym jest „copyright trolling”?, http://www.biznes-firma.pl/czym-jest-copyright-trolling/27199 (dostęp z 24.11.2017 r.).

[8] Wyjątkiem były czynności podejmowane osobiście przez fotograf *Judytę P.*

[9] *I. Drożdż*, *K. Sączek*, Dozwolony użytek osobisty w Internecie a problem torrentów, Internetowy Przegląd Prawniczy TBSP UJ 2016, Nr 4, s. 68.

[10] Wiąże się to często z żądaniem zapłaty od osób, które pobierały oraz udostępniały pliki z pornografią, a fakt ten (jako wstydliwy) pragną za wszelką cenę ukryć.

[11] *M. Maj*, Copyright trolling – raport, https://prawokultury.pl/media/entry/attach/MMaj-CopyrightTrolling-raport.pdf, s. 2 (dostęp z 24.11.2017 r.).

[12] Tak *M. Sag*, Copyright trolling. An Empirical Study, https://www.law.berkeley.edu/files/Matthew_Sag_Copyright_Trolls_March212014.pdf (dostęp z 24.11.2017 r.); podaję za: *ibidem*, s. 3.

[13] *O. Wrzeszcz*, Trolling prawnoautorski (copyright trolling), Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej 2016, Nr 4, s. 49.

[14] Taka sytuacja należy, co prawda, do rzadkości, niemniej przy kompleksowym opisie tego zjawiska nie można o niej zapominać; por. *T. Staśkiewicz*, Uważaj na copyright trolling! Polska fotografka wykorzystuje naiwność szkół i fundacji. Przez to ma ogromne „honoraria”, http://innpoland.pl/129133,uwazaj-na-copyright-trolling-polska-fotografka-wykorzystuje-naiwnosci-szkol-i-fundacji-przez-to-ma-ogromne-honoraria (dostęp z 24.11.2017 r.).

postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia". Biorąc pod uwagę specyfikę naruszeń praw autorskich w sieciach P2P[15], na których oparte są popularne platformy torrentowe[16] oraz których najczęściej dotyczą działania prawnoautorskich trolli, zaznaczyć należy, że pliki w modelu klient–klient rozprzestrzeniane są w wersji sfragmentaryzowanej. Komputer każdego użytkownika spełnia tutaj jednocześnie rolę klienta oraz serwera. Pliki są porcjowane i dopiero pobranie wszystkich elementów (swoistych „porcji pliku") pozwala na zdekodowanie całego utworu[17]. Nasuwa się więc pytanie, czy zgodnie z przytoczoną definicją, takie fragmenty plików można traktować jak utwory w świetle ustawy o prawie autorskim i prawach pokrewnych? Jako sporna jawi się kwestia posiadania przez nie cech „twórczości i indywidualności", skoro mamy do czynienia z „ułamkiem pliku" (pojedynczo bezużytecznym, zyskującym wartość dopiero po połączeniu z pozostałymi częściami). W orzecznictwie nie udało się dotąd ustalić minimalnego poziomu twórczej indywidualności, jaka znamionować powinna dzieło bądź jego fragment, aby mogły one zostać objęte ustawową ochroną[18]. Ze względu na postęp technologiczny oraz tendencję do miniaturyzowania różnorodnych nośników informacji, trzeba jednak przyjąć, że: „w przypadku ściągnięcia i udostępnienia pliku w sieci P2P, pobrany fragment nie powinien być postrzegany jako część składowa utworu, ale traktowany jako fragment charakteryzujący się takimi samymi cechami jak całość utworu, który został jedynie zmodyfikowany parametrami technicznymi, wynikającymi ze sposobu funkcjonowania programu klienckiego i na które użytkownik sieci nie miał wpływu"[19].

Przechodząc natomiast do pojęcia „rozpowszechniania", należy wskazać, iż termin ten nie został zdefiniowany w ustawie o prawie autorskim i prawach pokrewnych. W art. 6 ust. 1 pkt 3 PrAutU znajdziemy jedynie wyjaśnienie „utworu rozpowszechnionego", ale jest ono na tyle ogólne, że nie wydaje się przydatne do stworzenia definicji „rozpowszechniania". Właściwsze jest nawiązanie do art. 5 PrAutU, gdzie w pkt 3 *in fine* czytamy o innych sposobach rozpowszechniania, polegających na: „publicznym udostępnieniu utworu w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i w czasie przez siebie wybranym".

Kolejne wątpliwości budzi moment, od którego w sieciach P2P zaczyna się rozpowszechnianie. Rozróżnić wypada: zgłoszenie adresu IP jako gotowego do udostępnienia pliku, moment udostępnienia pierwszego fragmentu oraz udostępnienie całości utworu[20]. Tutaj także, w odniesieniu do wysoko rozwiniętej technologii oraz szybkości internetowej komunikacji, najtrafniejsza jest szeroka definicja „rozpowszechniania", które rozpoczynałoby się już od stworzenia potencjalnej możliwości skorzystania z utworu online, co potwierdza wykładnia art. 3 dyrektywy Parlamentu i Rady 2001/29/WE z 22.5.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym[21].

Trolling prawnoautorski *sensu stricto* a nadużycie prawa podmiotowego

Istotne jest to, że w obecnym stanie prawnym brakuje konkretnego przepisu, który sankcjonowałby *copyright trolling* jako naruszenie obowiązującego w Polsce prawa. W doktrynie przyjmuje się jednak, że istnieją możliwości skutecznej ochrony przed *copyright trollingiem* w postępowaniu sądowym. Wielu prawników uważa, że w stosunku do roszczeń opartych na naruszeniu praw autorskich można zastosować art. 5 KC[22].

Sądy w Polsce od lat uznawały za prymarny interes twórcy i początkowo nie dostrzegały znamion prawnoautorskiego trollingu, zupełnie ignorując fakt coraz częstszego występowania tego zjawiska oraz jego negatywne konsekwencje[23]. Tendencja ta zmieniała się stopniowo, począwszy od 2014 r., wraz z upowszechnianiem wśród opinii publicznej informacji na temat omawianego procederu oraz jego zauważalną intensyfikacją. Przykładowo w wyroku z 11.3.2015 r. SO w Kaliszu wyraźnie zaznaczył, że „powódka świadomie wykorzystuje brak jednoznacznej i wyraźnej informacji o swoim autorstwie utworów fotograficznych zmieszczonych w Internecie, które nie są dostatecznie zabezpieczone technicznie przed rozpowszechnianiem bez wiedzy i zgody, co można oceniać w kategorii nadużycia prawa podmiotowego z art. 5 KC"[24].

Niezwykle istotne orzeczenie, w którym SO w Lublinie jednoznacznie zakwalifikował *copyright trolling* jako nadużycie autorskich praw majątkowych, wydane zostało 31.7.2017 r. Czytamy tam, iż „zakres ochrony przyznany uprawnionemu w konkretnym stanie faktycznym może być wyznaczony także przez klauzulę generalną nadużycia prawa podmiotowe-

[15] Dalej również jako sieci *peer to peer* (termin wprowadzony przez IBM w 1984 r.), technologia bezpośredniego udostępniania zasobów; por. *J. Chwalba*, Korzystanie z programów *peer-to-peer* a dozwolony użytek prywatny w prawie autorskim, Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej 2008, Nr 2 (102), s. 19.

[16] Jest to system komunikacji w Internecie, oparty na równorzędności stron i braku stałej struktury. Por. *I. Drożdż*, *K. Sączek*, Dozwolony…, s. 59.

[17] *Ibidem*, s. 58.

[18] Por. wyrok SN z 22.6.2010 r., IV CSK 359/09, OSNC 2011, Nr 2, poz. 16.

[19] Tak *O. Wrzeszcz*, Trolling prawnoautorski…, s. 51.

[20] *Z. Okoń*, [w:] *P. Podrecki* (red.), Prawo Internetu, Warszawa 2007, s. 399–400.

[21] Dz.Urz. UE L Nr 167, s. 10; dalej jako: dyrektywa 2001/29/WE.

[22] Tak *A. Oryl*, IP trolling: można się przed nim bronić, Rzeczpospolita z 28.4.2016 r., s. C7; autor jest radcą prawnym Deloitte Legal.

[23] Por. Odpowiedź na interpelację nr 30707 w sprawie instrumentalnego wykorzystania przepisów prawa w procederze tzw. copyright trollingu, http://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=7556DD07 (dostęp z 24.11.2017 r.).

[24] Zob. wyrok SO w Kaliszu z 11.3.2015 r., I C 1813/14, http://orzeczenia.kalisz.so.gov.pl/content/$N/152505000000503_I_C_001813_2014_Uz_2015-03-11_002 (dostęp z 24.11.2017 r.).

go. (…) W ocenie sądu ma rację pozwana, podnosząc, że [w – przyp. *A.S.*] okolicznościach sprawy działania powoda można określić mianem *copyright trollingu* i uznać, że powodowi bardziej zależało na czerpaniu korzyści finansowych z mniej lub bardziej świadomych naruszeń licencji do przedmiotowego utworu, niż na ograniczaniu takiej możliwości i ewentualnych strat z tego tytułu. W tej sytuacji w niniejszej sprawie zarzut nadużycia autorskich praw majątkowych może być skutecznie postawiony powodowi, gdyż domaga się nadmiernych korzyści ekonomicznych od pozwanej"[25].

Przedstawione stanowiska SO dobitnie przemawiają za możliwością uznania działań prawnoautorskich trolli *sensu stricto* za nadużycie prawa podmiotowego. Instytucja ta, uregulowana w art. 5 KC, ma bowiem zastosowanie do wszystkich działów prawa cywilnego, a ustanowiono ją w celu zapewnienia aksjologicznej i funkcjonalnej zgodności systemu prawnego ze stosunkami prawnymi[26]. Jako klauzula generalna pozwala na uelastycznienie ustawowej regulacji oraz przeciwdziałanie zachowaniom, które, choć pozornie nie naruszają przepisów, to jednak są sprzeczne ze społeczno-gospodarczym przeznaczeniem prawa lub z zasadami współżycia społecznego. Co istotne, w doktrynie przeważa stanowisko zgodne z tzw. wewnętrzną teorią nadużycia prawa podmiotowego, wedle której (stosownie do literalnego brzmienia art. 5 zd. 2 KC) tego typu zachowania nie można zakwalifikować jako wykonywania prawa, natomiast działanie wbrew regułom nie mieści się w granicach prawa podmiotowego[27].

Aby jednak trolling prawnoautorski *sensu stricto* uznać za nadużycie prawa podmiotowego, trzeba wpierw przypomnieć rozumienie pojęć: społeczno-gospodarcze przeznaczenie prawa oraz zasady współżycia społecznego. Pierwsza wymieniona klauzula interpretowana jest co do zasady ściśle poprzez wzgląd na funkcje określonego prawa w społeczeństwie oraz wartości ekonomiczne (jest ona wszak odstępstwem od reguły pewności prawa i może ograniczać autonomię danego podmiotu tylko wyjątkowo – kiedy jego postępowanie koliduje z prawami podmiotowymi innej osoby). W piśmiennictwie wskazuje się, że społeczno-gospodarcze przeznaczenie prawa wynika z jego treści oraz charakteru, dla określenia którego pomocne są również postanowienia Konstytucji RP[28]. Zasady współżycia społecznego tłumaczy się natomiast jako: „szczególne reguły postępowania w życiu społecznym, utożsamiane z normami moralnymi, odnoszącymi się do stosunków międzyludzkich"[29], podstawowe zasady etycznego i uczciwego postępowania[30].

Klauzula generalna z art. 5 KC służy także realizacji sprawiedliwości w znaczeniu materialnoprawnym, tj. wartości wskazanej w art. 45 ust. 1 Konstytucji RP. Obejmuje ona zachowania faktyczne oraz czynności prawne (również proceduralne), dokonywane na podstawie kompetencji zawartych w prawie podmiotowym. Dodatkowo, zgodnie z tzw. zasadą „czystych rąk", której wyraz odnajdujemy zarówno w doktrynie, jak i w judykaturze – nie zostanie uwzględniony zarzut nadużycia prawa podniesiony przez osobę, która sama nie przestrzega zasad współżycia społecznego, gdyż stanowiłoby to opaczne rozumienie klauzuli generalnej z art. 5 KC[31]. Zasadę tę wiąże się z paremią: *nemo audiatur propriam turpitudinem allegans*[32]. Jednakże w omawianej sytuacji *copyright trollingu sensu stricto* nie będziemy mieć do czynienia z niegodziwością ofiary trolla. Wszakże ten, kogo zidentyfikowano przy pomocy adresu IP, często działał nieświadomie oraz nie miał na celu uzyskania korzyści majątkowej. Dlatego nie można zarzucić takiej osobie zachowania sprzecznego z zasadami współżycia społecznego, które wedle tzw. zasady „czystych rąk" pozbawiałoby rzeczony podmiot możliwości podniesienia zarzutu z art. 5 KC.

Wydaje się więc, że w przypadku masowego rozsyłania wezwań do zapłaty, które ponadto znamionują: zastraszający ton, agresywna stylistyka oraz groźby obejmujące wszczęcie postępowania karnego w razie niepodpisania ugody, czynności te uznać możemy za spełniające dyspozycję z art. 5 KC. Niemniej każdą z sytuacji, jaką zakwalifikowalibyśmy do *copyright trollingu*, rozpatrywać musimy w sposób indywidualny, dogłębnie analizując wszelkie okoliczności sprawy. Konstrukcja ta znajduje bowiem zastosowanie jedynie do przypadków szczególnych i nietypowych, kiedy nie istnieje inna możliwość obrony, a uwzględnienie powództwa prowadziłoby do sytuacji nieakceptowanej ze względów aksjologicznych i teleologicznych[33].

Reasumując, dopiero wtedy gdy po rozważeniu zarówno stanu faktycznego, jak i sposobu dochodzenia roszczeń przez stronę uznamy, iż doszło do obalenia domniemania, zgodnie z którym uprawniony czyni ze swego prawa użytek zgodny z przeznaczeniem i zasadami współżycia społecznego, mamy podstawy, aby odmówić danemu podmiotowi ochrony prawnej. Za każdym razem tego typu kwalifikacja należy jednak do dyskrecjonalnej oceny sądu, a zatem błędem byłoby bezrefleksyjne postawienie znaku równości między *copyright trollingiem sensu stricto* a klauzulą generalną nad-

[25] Zob. wyrok SO w Lublinie z 31.7.2017 r., I C 758/16, http://orzeczenia.lublin.so.gov.pl/content/$N/153005000000503_I_C_000758_2016_Uz_2017-07-31_001 (dostęp z 24.11.2017 r.).

[26] Por. wyrok TK z 17.10.2000 r., SK 5/99, OTK ZU 2000, Nr 7, poz. 254.

[27] *Z. Radwański*, *A. Olejniczak*, Prawo cywilne – część ogólna, Warszawa 2013, s. 106; odmienne stanowisko zajmuje w tej kwestii m.in. *M. Pyziak-Szafnicka*.

[28] Tak *T. Justyński*, Nadużycie prawa w polskim prawie cywilnym, Kraków 2000, s. 113.

[29] *Z. Radwański*, *A. Olejniczak*, Prawo cywilne…, s. 286.

[30] Por. wyrok SN z 28.11.2001 r., IV CKN 1756/00, Legalis.

[31] Por. *T. Justyński*, Nadużycie…, s. 149, oraz orzeczenie SN z 22.2.1967 r., III CR 383/66, BSN 1967, Nr 4–5, poz. 66.

[32] Łac. „Nie będzie wysłuchany, kto powołuje się na własną niegodziwość".

[33] Por. wyrok SA w Łodzi z 23.3.2014 r., I ACa 1208/13, www.orzeczenia.ms.gov.pl.

użycia prawa podmiotowego. Sądy powinny zawsze chronić zasadę praworządności oraz pewności obrotu, a jednocześnie bezwzględnie zapobiegać stanom, do których odnosi się słynna paremia: *summum ius – summa iniuria*[34].

Status materialnoprawnej ugody zawieranej przez podmioty prawnoautorskiego trollingu –miarkowanie odszkodowania, wady oświadczenia woli oraz bezpodstawne wzbogacenie

Zamierzonym skutkiem rozsyłania przez prawnoautorskich trolli agresywnych pism jest przede wszystkim zawarcie z potencjalnym naruszycielem autorskich praw majątkowych materialnoprawnej ugody[35] oraz otrzymanie żądanej kwoty. Warto zaznaczyć, że wysokość owej kwoty, w świetle ugruntowanego orzecznictwa, powinna odpowiadać szkodzie lub stosownemu wynagrodzeniu, jakie podmiot autorskich praw majątkowych otrzymałby, gdyby osoba, która naruszyła jego prawa, zawarła z nim uprzednio umowę o korzystanie z utworu w zakresie dokonanego naruszenia (wyliczenie to opiera się na obiektywnych kryteriach w postaci: średniej wartości rynkowej naruszonego prawa, sumie opłat licencyjnych lub honorariów autorskich)[36]. W razie wątpliwości nie jest wykluczone skorzystanie z opinii biegłego, ale zarówno roszczenie o naprawienie szkody z art. 79 ust. 1 pkt 3 lit. a, jak i roszczenie o zapłatę wielokrotności stosownego wynagrodzenia z art. 79 ust. 1 pkt 3 lit. b PrAutU przysługuje jedynie wtedy, gdy doszło do wyrządzenia szkody[37]. Ciężar jej wykazania spoczywa na dochodzącym roszczenia, a w rozważanych ofertach ugodowych brakuje jakichkolwiek informacji, które wskazywałyby wyznaczniki żądanej kwoty.

Dobrą ilustracją dla zobrazowania często nieuzasadnionych, wygórowanych roszczeń prawnoautorskich trolli jest wypowiedź dyrektora pewnej instytucji kultury, wobec którego rozmaite żądania kierowała fotograf *Judyta P.*: „Pierwsze wezwanie do zapłaty wpłynęło do nas już w 2013 r. i opiewało na kwotę prawie 20 tys. zł. Kolejne wezwanie do zapłaty to już ponad 100 tys. zł. Następne na kwotę nieco niższą, a teraz Pani *J.P.* proponuje ugodę na kwotę 45 tys. [zł – przyp. *A.S.*]"[38]. Bazując na danych przedstawionych we wspomnianym raporcie[39], zauważymy, iż kwoty proponowane w ugodach kształtują się od 470 do 13 000 zł, jednak żaden z podmiotów nie podaje w pismach podstaw ich wyliczenia. Z uwagi zatem na budzący wątpliwości i nierzadko krytykowany[40] penalno-represyjny charakter roszczenia o zapłatę sumy pieniężnej (uregulowany w art. 79 ust. 1 pkt 3 lit. b PrAutU) oraz orzeczenie TK z 23.6.2015 r., w efekcie którego przepis ten utracił moc w zakresie, w jakim uprawniony mógłby dochodzić trzykrotności stosownego wynagrodzenia w przypadku zawinionego naruszenia autorskich praw majątkowych, opisane żądania wydają się nieuzasadnione i niewspółmierne. Zdaniem Trybunału wprowadzanie do roszczenia odszkodowawczego elementów ryczałtowości nie może prowadzić do całkowitego zagubienia proporcji pomiędzy wielkością poniesionej szkody a tymże odszkodowaniem[41]. Analogicznie kwota wskazywana w ugodzie nie może zbliżać się do (znanej m.in. z orzecznictwa sądów amerykańskich) koncepcji kary cywilnej, a tego typu przesadne roszczenie prawnoautorskiego trolla, ze względu na czytelną sprzeczność z zasadą sprawiedliwości społecznej wyrażoną w art. 2 Konstytucji RP, nie zasługuje zaś na uwzględnienie.

Jako umowa wzajemna i tzw. ustalająca[42] ugoda przekształca dotychczasowy stosunek prawny w wyniku obustronnych ustępstw, wywierając wpływ na treść i wykonanie zobowiązań. Ugoda nie ma jednak samoistnej mocy prawotwórczej, co oznacza, iż nie stanowi nowego tytułu prawnego dla wyrażonych w niej praw i obowiązków[43]. Jako czynność konsensualna nie wymaga (o ile strony w jej treści nie zawrą odmiennych postanowień lub nie wynika to z jej przedmiotu) szczególnej formy. Podobnie jak w pozostałych umowach jej granice wyznacza art. 58 KC[44]. Zastosowanie może mieć tu także instytucja wyzysku z art. 388 KC oraz wady oświadczenia woli z zastrzeżeniem odrębności dotyczących błędu uregulowanych w art. 918 KC[45].

Na gruncie przytoczonej wyżej regulacji wątpliwości budzi status ugody zawieranej między potencjalnym naruszycielem a prawnoautorskim trollem. W przypadku trollingu *sensu stricto* zbadać należy zwłaszcza swobodę kształtowania przez obie strony stosunku prawnego oraz wpływania na treść ugody. Kluczowa jest świadomość, iż ugoda cywilnoprawna nie obejmuje ścigania przestępstwa w oparciu o art. 122 w zw.

[34] Łac. „Szczyt prawa (to) szczyt bezprawia"; zbyt ściśle, formalnie wymierzona sprawiedliwość staje się krańcową niesprawiedliwością.

[35] Instytucję tę szczegółowo regulują przede wszystkim art. 917 i 918 KC.

[36] Por. wyrok SA we Wrocławiu z 23.3.2008 r., I ACa 456/08, OSAW 2008, Nr 4, poz. 112; wyrok SN z 13.12.2007 r., I CSK 321/07, Legalis, oraz pkt 26 preambuły dyrektywy 2001/29/WE.

[37] Rozumianej szeroko, zgodnie z art. 361 § 2 KC; por. *J. Barta*, *R. Markiewicz*, Prawo autorskie i prawa pokrewne, Warszawa 2011, s. 111.

[38] Przytaczam za: *M. Maj*, Copyright trolling…, s. 30.

[39] *Ibidem*, s. 35.

[40] Por. *P. Bogdalski*, Środki ochrony autorskich praw majątkowych oraz ich dochodzenie w świetle prawa polskiego, Kraków 2003, s. 123.

[41] Zob. wyrok TK z 23.6. 2016 r., SK 32/14, OTK ZU, poz. 932.

[42] *Z. Radwański, J. Panowicz-Lipska*, Zobowiązania – część szczegółowa, Warszawa 2012, s. 397.

[43] Choć zaznaczyć trzeba, że opinie o szerszym zakresie ugody wypowiadali m.in. *A. Szpunar* oraz *M. Pyziak-Szafnicka*.

[44] Nieważna jest ugoda sprzeczna z ustawą, mająca na celu obejście ustawy lub sprzeczna z zasadami współżycia społecznego.

[45] „Doniosłość ma tylko błąd co do stanu faktycznego, który, zgodnie z treścią ugody, obie strony uważały za niewątpliwy, a spór albo niepewność nie byłyby powstały, gdyby w chwili zawarcia ugody strony wiedziały o prawdziwym stanie rzeczy"; por. *Z. Radwański*, *J. Panowicz-Lipska*, Zobowiązania – część szczegółowa, Warszawa 2012, s. 399.

z art. 116 PrAutU, a wiedzy takiej bywa często pozbawiona typowa ofiara trollingu. Oprócz tego, jeżeli uznamy, że doszło do nadużycia prawa (spełnione zostały przesłanki z art. 5 KC), zastosowanie może znaleźć również art. 415 KC. Wskazana regulacja odpowiedzialności odszkodowawczej opiera się na zasadzie winy (z której aspektem przedmiotowym wiąże się pojęcie bezprawności). Zważywszy na przeważającą w literaturze tzw. normatywną koncepcję winy[46], naganność zachowania wynika bezpośrednio z samej istoty nadużycia prawa podmiotowego. Rozpatrując więc dalsze postępowanie stron (po zawarciu rzeczonej ugody oraz zapłacie wymaganej kwoty), istnienie szkody oraz związku przyczynowo-skutkowego wskazanego w art. 361–363 KC wydaje się bezsporne, a przy tym spójne z dominującą teorią adekwatnego związku przyczynowego.

Jeśli zaś chodzi o wady oświadczenia woli, to w przypadku trollingu *sensu stricto*, z uwagi na regulację szczególną z art. 918 KC, możemy rozważać przede wszystkim groźbę opisaną w art. 87 KC. Aby możliwe było uchylenie się od skutków złożonego oświadczenia woli, groźba ta powinna być bezprawna i poważna. Groźbę tłumaczy się zwykle jako: „zapowiedź wyrządzenia komuś zła, jeżeli nie dokona on żądanej czynności prawnej"[47], a jej powagę łączy się z niebagatelnym, zobiektywizowanym niebezpieczeństwem dla osobistych lub majątkowych dóbr osoby składającej oświadczenie woli lub jakiejkolwiek innej osoby. Bezprawność jest tu rozumiana szeroko – jako sprzeczność z porządkiem prawnym oraz sprzeczność z zasadami współżycia społecznego. Dodatkowo dzieli się ją na bezprawność środka oraz bezprawność celu[48].

Podsumowując, jeśli w piśmie otrzymanym od prawnoautorskiego trolla odnajdujemy groźbę wszczęcia postępowania sądowego, niewątpliwie mamy do czynienia z groźbą bezprawną oraz co do zasady poważną, spełniającą przesłanki z art. 87 KC[49]. Ofiara trolla ma zatem prawo pisemnie uchylić się od skutków prawnych złożonego oświadczenia woli. Czynnikiem decydującym o „powadze groźby" będzie jednocześnie: realność (rzeczywiste niebezpieczeństwo) oraz rozmiar zła, jakie grozi adresatowi pisma wysłanego przez rzeczonego trolla. Oceniając zatem sankcję w postaci wszczęcia postępowania karnego (jaka wynika z treści omawianych wezwań do zapłaty) w połączeniu z trollingiem *sensu stricto* (czyli dochodzeniem roszczeń przez podmiot uprawniony w stosunku do naruszyciela autorskich praw majątkowych), wskazane wyżej groźby będą spełniać obie przesłanki – bezprawności oraz powagi niebezpieczeństwa.

W oparciu o tożsame kryteria zbadać trzeba status materialnoprawnej ugody, gdy mamy do czynienia z trollingiem *sensu largo* (z uprzednim wyłączeniem z tej zbiorczej kategorii omówionego wyżej trollingu *sensu stricto*). Wówczas, z uwagi na brak naruszenia prawa autorskiego przez ofiarę trolla lub brak stosownego uprawnienia podmiotu dochodzącego roszczenia, groźba towarzysząca składaniu oświadczenia woli nie ma charakteru realnego. Wydaje się natomiast, że w oparciu o art. 58 § 1 KC zawarcie ugody między wymienionymi wyżej podmiotami byłoby bezwzględnie nieważne z uwagi na brak jakiegokolwiek stosunku prawnego łączącego te osoby oraz kauzalny i zobowiązujący charakter ugody[50], ponieważ uznanie nie stanowi nowej podstawy roszczenia[51]. Sprzeciwiałoby się to wszakże aksjologii, zgodnie z którą racjonalny prawodawca chroni wszelkie przesunięcia majątkowe, czego przejawem jest m.in. instytucja bezpodstawnego wzbogacenia. Zbędna jest więc analiza ewentualnych wad oświadczenia woli towarzyszących zawieraniu ugody w trzech przypadkach trollingu *sensu largo* (tj. z wyłączeniem trollingu *sensu stricto*), gdyż sankcje bezwzględnej nieważności czynności prawnej są najdalej idące oraz pochłaniają wszelkie sankcje, jakie mogłyby wynikać z uznania, iż podczas zawierania ugody wystąpiła wada oświadczenia woli.

Przechodząc zatem do sygnalizowanego uprzednio zagadnienia bezpodstawnego wzbogacenia, wypada przypomnieć, iż „ogólną regułą prawa cywilnego jest, że każde przejście wartości majątkowych z jednej osoby na drugą musi być prawnie uzasadnione"[52]. Do uzyskania zwrotu bezpodstawnie utraconej wartości konieczne jest zatem łączne wystąpienie czterech przesłanek uregulowanych w art. 405 KC, tj.: wzbogacenia jednego podmiotu, zubożenia drugiego podmiotu, związku między wzbogaceniem a zubożeniem i bezpodstawności wzbogacenia. Rozpatrując ugodę zawartą między prawnoautorskim trollem a jego ofiarą, bezsporny pozostaje fakt spełnienia pierwszych trzech przywołanych przesłanek. Ofiara po zawarciu ugody płaci żądaną kwotę, w efekcie czego następuje jej zubożenie oraz wzbogacenie nadawcy wysłanego uprzednio wezwania. W sytuacji *copyright trollingu sensu stricto* oraz bezpodstawności nienależnego świadczenia możemy się powołać na wymienione w art. 410 KC odpadnięcie podstawy prawnej (*conditio causa finita*) – na skutek uchylenia się od skutków prawnych wadliwego oświadczenia woli złożonego pod wpływem groźby. W pozostałych trzech przypadkach trollingu *sensu largo* (czyli gdy zachodzi bezwzględna nieważność owej ugody) mamy zaś do czynienia z *conditio sine causa*.

[46] Zgodnie z którą wina stanowi ujemną ocenę zachowania podmiotu, polegającą na podjęciu niewłaściwej decyzji w danej sytuacji, gdy pomimo możności zachowania się inaczej, dany podmiot zachował się bezprawnie – por. *Z. Radwański*, *A. Olejniczak*, Zobowiązania – część ogólna, Warszawa 2010, s. 198.

[47] *Z. Radwański*, *A. Olejniczak*, Prawo cywilne…, Warszawa 2013, s. 277.

[48] Por. wyrok SN z 19.3.2002 r., I CKN 1134/99, OSNC 2003, Nr 3, poz. 36.

[49] Por. orzeczenie SN z 4.2.1957 r., III CR 834/55, NP 1957, Nr 7–8, s. 187.

[50] Por. *D. Dulęba*, Ugoda w polskim prawie cywilnym, Warszawa 2012, s. 65 – autor podkreśla, że kauzą ugody jest zawsze *causa obligandi vel acquirendi*, ponieważ strony czynią sobie wzajemnie ustępstwa.

[51] Tak *ibidem*, s. 153; odmiennie m.in. *A. Szpunar*, Z problematyki ugody w polskim prawie cywilnym, PS 1995, Nr 9, s. 12, i *Z. Masłowski*, Uznanie, ugoda, odnowienie, zwolnienie z długu, poręczenie, Katowice 1996, s. 51.

[52] *Z. Radwański*, *A. Olejniczak*, Zobowiązania – część ogólna, Warszawa 2010, s. 286.

Podsumowanie

W związku z tym, że immanentną cechą rodzimego prawnoautorskiego trollingu jest instrumentalne traktowanie postępowania karnego jako sposobu na uzyskanie (na podstawie adresów IP) danych osobowych podmiotów rzekomo naruszających prawo, można zaproponować zmianę art. 116 PrAutU. Korzystne byłoby ograniczenie odpowiedzialności karnej za naruszenie majątkowych praw autorskich do sytuacji, gdy jest to działanie świadome, tzn. kiedy sprawca działa w zamiarze bezpośrednim. Nie naruszyłoby to zasadniczych interesów podmiotu autorskich praw majątkowych (któremu wciąż przysługiwałyby roszczenia cywilne), a tego typu zmiana mogłaby w znacznym stopniu zniwelować zjawisko *copyright trollingu* i przyczynić się do odciążenia organów ścigania. Nadto nie byłoby to sprzeczne z wytycznymi dyrektywy 2001/29/WE[53] ani z Porozumieniem w sprawie handlowych aspektów praw własności intelektualnej z 1994 r.

Jeszcze dalej idącą koncepcję całkowitej dekryminalizacji rozpowszechniania utworu bez zgody twórcy, które to rozpowszechnianie nie miało na celu uzyskania korzyści majątkowej, zgłosiła w 2014 r. grupa posłów w formie projektu ustawy zmieniającej ustawę o prawie autorskim i prawach pokrewnych[54]. W uzasadnieniu wskazywano, że: „Przestępstwo przewidziane w art. 116 ust. 1 ustawy dokonywane jest bez korzyści majątkowej, najczęściej w sposób nieświadomy i nie ma na celu świadomego pokrzywdzenia uprawnionego z praw autorskich. Wobec powyższego kryminalizacja takich zachowań stoi w sprzeczności z zasadniczymi wartościami, które prawo karne winne jest realizować"[55]. Projekt ten nie został jednak rozpatrzony podczas VII kadencji Sejmu. Kilka miesięcy później z podobną propozycją wystąpił poseł *P. Wipler* w interpelacji z 5.2.2015 r.[56]. Argumentował on, iż: „Mamy (…) do czynienia nie tylko z sytuacją, w której prawo karne jest instrumentalnie wykorzystywane do dochodzenia roszczeń cywilnych, ale również z przerzucaniem kosztów związanych z dochodzeniem tych roszczeń wprost na polskiego podatnika, nie mówiąc już o zaangażowaniu instytucji państwa w działania mające cechy działalności zarobkowej pod płaszczykiem ochrony praw autorskich"[57]. Niestety w odpowiedzi z 3.3.2015 r., Minister Sprawiedliwości nie zakwalifikował opisywanego procederu jako działań sprzecznych z prawem ani choćby nadużycia prawa[58]. W tym kontekście należy zatem przypomnieć, jak poważny problem stanowi *copyright trolling*. Istnieją wręcz wyspecjalizowane kancelarie, które czerpią korzyści z ludzkiej niewiedzy oraz nieprzystosowania prawa autorskiego w Polsce do „ery cyfrowej"[59].

W konkluzji wypada podkreślić, że brak akceptacji dla naruszania autorskich praw majątkowych oraz dążenie do zwalczania jego przejawów w żadnym razie nie mogą być agresywne ani sprzeczne z zasadami współżycia społecznego. Prawnoautorska ochrona nie ma charakteru absolutnego, dlatego musi ona równolegle uwzględniać prawa i interesy osób trzecich[60]. Dodatkowo warto zauważyć, iż *copyright trolling* w dłuższej perspektywie może szkodzić nie tylko pierwotnym ofiarom tego zjawiska, lecz również samym prawom autorskim, których dochodzenie (na skutek skojarzeń z nieetycznym postępowaniem prawnoautorskich trolli) będzie budzić coraz więcej wątpliwości. Jak dotąd nie udało się także dowieść, że masowe wysyłanie propozycji ugodowych skutkuje faktycznym zmniejszeniem skali naruszeń autorskich praw majątkowych. Jeśli zatem jako przyczyny *copyright trollingu* podaje się przede wszystkim niską świadomość prawną Polaków oraz złożoność i niejasność regulacji dotyczącej prawa autorskiego[61], wskazane byłoby zaangażowanie większych środków finansowych oraz czasu na edukację obywateli, stanowcze określenie stanowiska w tej sprawie przez władze państwowe (zwłaszcza Ministra Sprawiedliwości), a także przeprowadzenie w ustawodawstwie postulowanych zmian. To wszystko pozwoliłoby na lepsze przystosowanie obowiązującego prawa autorskiego do warunków cyfrowej rzeczywistości.

[53] Por. pkt 10, 58 preambuły oraz art. 8 dyrektywy 2001/29/WE.

[54] *J. Kralka*, PiS z ciekawym pomysłem na dekryminalizację piractwa i okiełznanie copyright trollingu, http://techlaw.pl/pis-z-ciekawym-pomyslem-na-dekryminalizacje-piractwa-okielznanie-copyright-trollingu/ (dostęp z 24.11.2017 r.).

[55] Projekt Ustawy o zmianie ustawy o prawach autorskich i prawach pokrewnych zgłoszony 18.9.2014 r., https://sip.lex.pl/#/act-project/102024383/1/zm-ustawa-o-prawie-autorskim-i-prawach-pokrewnych?keyword=trolling&cm=SREST (dostęp z 24.11.2017 r.).

[56] Interpelacja nr 30707 do ministra sprawiedliwości w sprawie instrumentalnego wykorzystania przepisów prawa w procederze tzw. copyright trollingu, http://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=799E0E76 (dostęp z 24.11.2017 r.).

[57] Orzeczenie SN z 7.5.2008 r., III KK 234/07, http://www.lex.pl/akt/-/akt/iii-kk-234-07 (dostęp z 24.11.2017 r.).

[58] Odpowiedź na interpelację nr 30707 w sprawie instrumentalnego wykorzystania przepisów prawa w procederze tzw. copyright trollingu, http://www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=7556DD07 (dostęp z 24.11.2017 r.).

[59] Por. *T. Staśkiewicz*, Uważaj na copyright trolling…

[60] Tak *E. Laskowska*, Konstrukcja..., s. 327.

[61] Por. Opinia wyrażona przez *J. Lipszyca*, prezesa Fundacji Nowoczesna Polska: „Naruszanie praw autorskich w celach niekomercyjnych ma charakter absolutnie masowy i wynika ze złej konstrukcji prawa. (…) potrzebne są zmiany systemowe (…), które umożliwiłyby obywatelowi legalne korzystanie z dóbr kultury podczas komunikacji z innymi" – za: *K. Borowska*, Trolling: Jak prawnicy zastawiają sieci na internautów, http://www.rp.pl/artykul/1139177-Trolling--Jak-prawnicy-zastawiaja-sieci-na-internautow.html (dostęp z 24.11.2017 r.).

Słowa kluczowe: trolling prawnoautorski, nadużycie prawa podmiotowego, autorskie prawa majątkowe, sieci *peer to peer*, ugoda materialnoprawna.

Copyright trolling and abuse of subjective rights

Rapid technological development and legislation covering more and more areas of social life make changes to the specificity of copyright protection in Poland. A relatively new phenomenon is, among others, copyright law trolling (in the English-speaking world known as: copyright trolling or IP trolling). In this paper, its definition and distinguishing features will be provided to qualify a given behavior as copyright trolling. The author of the article also discusses the internal typology of this concept related to its subjective and objective scope and the relationship between copyright and trolling with the institution of abuse of subjective right regulated in art. 5 of the Civil Code. The summary presents the most important effects of the described phenomenon and de lege ferenda postulates regarding the shape of copyright protection in Polish legislation.

Keywords: copyright trolling, abuse of legal right, copyright, peer to peer networks, material settlement agreement.

Ponowne wykorzystywanie informacji sektora publicznego a ochrona danych osobowych według ogólnego rozporządzenia o ochronie danych oraz dyrektywy 2003/98/WE – wybrane zagadnienia

Dominik Sybilski[1]

Informacje sektora publicznego (ISP), które są przekazywane każdemu zainteresowanemu do ponownego wykorzystywania, mogą zawierać dane osobowe. Problem kolizji prawa do wykorzystywania informacji z podstawowym prawem do prywatności i ochroną danych osobowych jest niezwykle aktualny. Ustawa z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznego[2] weszła w życie 16.6.2016 r. Obecnie trwają prace nad reformą prawa krajowego, która ma na celu wykonanie przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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[3], które zacznie obowiązywać od 25.5.2018 r. W przypadku ponownego wykorzystywania ISP, gdy zagrożona jest ochrona prywatności i ochrona danych osobowych, konieczne jest stosowanie zrównoważonego podejścia. Dotyczy to zarówno prawodawcy na etapie projektowania aktów prawnych, jak i dysponentów danych udostępniających ISP do ponownego wykorzystywania. Pomocne w tym zakresie mogą być wytyczne Grupy Roboczej art. 29 zawarte w opinii 06/2013 w sprawie otwartych danych i ponownego wykorzystywania ISP.

W niniejszym opracowaniu omówiono wybrane zagadnienia dotyczące realizacji prawa do ponownego wykorzystywania informacji sektora publicznego w kontekście konieczności zapewnienia ochrony danych osobowych według dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[4] oraz rozporządzenia ogólnego. W szczególności analizie poddano zalecenia Grupy Roboczej art. 29 zawarte w Opinii 06/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[5] dla nowego porządku prawnego obowiązującego po 25.5.2018 r. Artykuł stanowi wprowadzenie do omawianej problematyki.

Uwagi wstępne

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego wdrożyła do polskiego porządku prawnego dyrektywę 2013/37/UE Parlamentu Europejskiego i Rady z 26.6.2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego[6]. Implementacja dyrektywy zbiegła się z zakończeniem prac nad unijną reformą ochrony danych osobowych, tj. przyjęciem rozporządzenia ogólnego. Od 25.5.2018 r. rozporządzenie będzie obowiązywało we wszystkich państwach UE. Obecnie trwają prace nad reformą prawa krajowego, która ma na celu wykonanie przepisów rozporządzenia.

Informacje sektora publicznego, które są przekazywane każdemu zainteresowanemu do ponownego wykorzystywania, mogą zawierać dane osobowe. Problem kolizji prawa do wykorzystywania informacji, zakotwiczonego w konstytucyjnej zasadzie jawności oraz wolności rozpowszechniania informacji z podstawowym prawem do prywatności i ochroną danych osobowych, jest zatem niezwykle aktualny.

Ponowne wykorzystywanie informacji sektora publicznego

Instytucja ponownego wykorzystywania została po raz pierwszy wprowadzona do polskiego porządku prawnego ustawą z 16.9.2011 r. o zmianie ustawy o dostępie do informacji publicznej i niektórych innych ustaw[7], która stanowiła implementację dyrektywy 2003/98/WE. Nowelizacja ta wprowadziła do ustawy z 6.9.2001 r. o dostępie do informacji publicznej[8] rozdział 2a pt. Ponowne wykorzystywanie informacji publicznej.

W wyniku przeprowadzonego przeglądu wykonania dyrektywy 2003/98/WE podjęto decyzję o jej nowelizacji. Przy-

[1] Asystent w Zakładzie Prawa Administracyjnego Instytutu Nauk Prawnych PAN. Autor specjalizuje się w prawie dostępu do informacji i ponownego jej wykorzystywania.

[2] Dz.U. poz. 352; dalej jako: WykInfPubU.

[3] Dz.Urz. UE L Nr 119, s. 1; dalej jako: ogólne rozporządzenie lub RODO.

[4] Dz.Urz. UE L Nr 345, s. 90; dalej jako: dyrektywa 2003/98/WE.

[5] Grupa robocza art. 29 (Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych ustanowiona na mocy art. 29 dyrektywy 95/46/WE) w związku z wejściem w życia RODO zostanie zastąpiona przez Europejską Radę Ochrony Danych.

[6] Dz.Urz. UE L Nr 175, s. 1; dalej jako: dyrektywa 2013/37/UE.

[7] Dz.U. Nr 204, poz. 1195.

[8] T.j. Dz.U. z 2016 r. poz. 1764 ze zm.; dalej jako: DostInfPubU.

jęta w 2013 r. dyrektywa 2013/37/UE zmieniająca dyrektywę 2003/98/WE stanowiła wykonanie celów, o których mowa w Komunikacie z 12.12.2011 Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. Otwarte dane – siła napędowa innowacji, wzrostu gospodarczego oraz przejrzystego zarządzania[9]. Celem inicjatywy Komisji było zwiększenie wykorzystania potencjału ISP dla wzrostu konkurencyjności i innowacyjności gospodarki europejskiej. Podstawową zmianą dyrektywy 2003/98/WE było rozszerzenie zakresu podmiotowego ponownego wykorzystywania o biblioteki, muzea i archiwa. Treści będące w posiadaniu tych podmiotów na gruncie dyrektywy 2003/98/WE podlegały wyłączeniu z ponownego wykorzystywania. Inną istotną zmianą było wprowadzenie ogólnej zasady, zgodnie z którą wszystkie dokumenty udostępniane przez organy sektora publicznego mogą być ponownie wykorzystane do dowolnych celów komercyjnych lub niekomercyjnych.

Dyrektywa 2013/37/UE została implementowana przepisami ustawy o ponownym wykorzystywaniu informacji sektora publicznego, które obowiązują od 16.6.2016 r. Ustawodawca zaproponował nowy sposób wdrożenia zmienianej dyrektywy w polskim systemie prawnym, który miał zapewnić, że rozwiązania dotyczące ponownego wykorzystywania będą bardziej przejrzyste i łatwiejsze w stosowaniu[10]. Zakładał on wyodrębnienie przepisów o ponownym wykorzystywaniu z ustawy o dostępie do informacji publicznej oraz uregulowanie zasad i procedury ponownego wykorzystywania w nowej ustawie. Takie rozwiązanie miało w sposób precyzyjniejszy i bardziej zrozumiały dla adresatów norm prawnych rozróżnić instytucje dostępu do informacji oraz ponownego wykorzystywania.

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego określa zasady i tryb udostępniania i przekazywania ISP w celu ponownego wykorzystywania, podmioty zobowiązane, które udostępniają lub przekazują te informacje[11], warunki ponownego wykorzystywania oraz zasady ustalania opłat. Co istotne, przepisy o ponownym wykorzystywaniu opierają się na systemach dostępu do informacji obowiązujących w państwach członkowskich[12], dlatego też – zgodnie z art. 7 ust. 1 WykInfPubU – przepisy tej ustawy nie naruszają prawa dostępu do informacji publicznej ani wolności jej rozpowszechniania, ani przepisów innych ustaw określających zasady, warunki i tryb dostępu do informacji będących ISP.

Dla omawianej tematyki kluczowe znaczenie ma wyjaśnienie pojęć ISP oraz ponownego wykorzystywania.

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego wprowadziła do polskiego porządku prawnego nowe pojęcie informacji sektora publicznego (ISP). Przed wejściem w życie tej ustawy zakres przedmiotowy ponownego wykorzystywania wyznaczało pojęcie informacji publicznej. Obecnie zakres ten wyznacza ISP[13]. Zgodnie z art. 2 ust. 1 WykInfPubU jest nią każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotów zobowiązanych. Zakres pojęcia ISP jest zatem szerszy od pojęcia informacji publicznej (IP) i odpowiada wprost definicji dokumentu, o którym mowa w art. 2 pkt 3 dyrektywy 2003/98/WE. Przyjęcie takiego rozwiązania uzasadnione było przede wszystkim poszerzeniem zakresu podmiotowego dyrektywy 2003/98/WE o biblioteki, archiwa i muzea. Zasoby będące w posiadaniu tych instytucji, mieszczące się w pojęciu dokumentu, o którym mowa w dyrektywie, wykraczają poza zakres pojęcia IP[14]. Oparcie zakresu przedmiotowego ponownego wykorzystywania o ISP – w porównaniu z porządkiem prawnym regulowanym przepisami ustawy o dostępie do informacji publicznej – zwiększa zatem ryzyko udostępnienia w trybie WykInfPubU informacji zawierających dane osobowe[15].

Zawarta w art. 1 ust. 3 WykInfPubU definicja ponownego wykorzystywania odpowiada art. 2 pkt 4 dyrektywy 2003/98/WE. Przez ponowne wykorzystywanie należy rozumieć wykorzystywanie przez osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej ISP w celach komercyjnych lub niekomercyjnych innych niż pierwotny publiczny cel, dla którego informacja została wytworzona. Przy czym ponownym wykorzystywaniem nie jest udostępnianie lub przekazanie ISP przez podmiot wykonujący zadania publiczne innemu podmiotowi wykonującemu zadania publiczne wyłącznie w celu realizacji takich zadań.

W ocenie skutków wniosku zmiany dyrektywy 2003/98/WE wskazuje się, że ponowne wykorzystywanie ISP oznacza wszelkie twórcze wykorzystywanie danych, np. przez zwiększenie wartości danych, łączenie danych z różnych źródeł w celu wytworzenia pożądanego rezultatu, rozwijanie aplikacji, dokonywane zarówno w celach komercyjnych, jak

[9] KOM(2011) 882.

[10] Uzasadnienie do rządowego projektu ustawy o ponownym wykorzystywaniu informacji sektora publicznego, Druk Nr 141, http://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=141(dostęp z 1.10.2016 r.).

[11] W art. 5 WykInfPubU rozróżniono dwa tryby udzielenia ISP do ponownego wykorzystywania. Udostępnienie ISP odnosi się do bezwnioskowego udzielenia ISP poprzez systemy teleinformatyczne lub inny sposób (w szczególności BIP i centralne repozytorium), z kolei przekazanie ISP obejmuje wyłącznie udzielenie ISP na wniosek. W artykule użyto obydwu sformułowań wymiennie bez rozróżnienia na sposób udzielenia ISP.

[12] Art. 1 ust. 3 dyrektywy 2003/98/WE.

[13] Zob. szerzej: *G. Sibiga*, „Informacja publiczna" oraz „informacja sektora publicznego" – różnice pomiędzy pojęciami wyznaczającymi zakres stosowania ustaw informacyjnych, Informacja w Administracji Publicznej 2016, Nr 4, s. 39–42.

[14] Uzasadnienie do rządowego projektu ustawy o ponownym wykorzystywaniu informacji sektora publicznego, Druk Nr 141.

[15] Por. *A. Piskorz-Ryń* (red.), Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, Wrocław 2017, s. 93.

i niekomercyjnych. Instytucja ponownego wykorzystywania koncentruje się na wykorzystaniu gospodarczej wartości ISP, gdzie służy ona jako materiał wyjściowy dla rozwoju nowych produktów i usług. Podczas gdy podmioty publiczne są twórcami i dostawcami oryginalnego materiału, sektor prywatny odgrywa istotną rolę jako uczestnik i pośrednik procesu przetwarzania informacji pomiędzy ich źródłem (podmiot publiczny) a końcowym użytkownikiem[16].

Dane osobowe w dyrektywie 2003/98/WE i jej zmianie

Prawo do ponownego wykorzystywania podlega licznym ograniczeniom. Jedną z przesłanek ograniczających ponowne wykorzystywanie ISP na gruncie ww. dyrektyw jest konieczność zapewnienia ochrony danych osobowych.

Zgodnie z art. 1 ust. 4 dyrektywy 2003/98/WE akt ten w żaden sposób nie wpływa na poziom ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych zgodnie z przepisami Unii i prawa krajowego, w szczególności nie zmienia zobowiązań i praw określonych w dyrektywie 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[17]. Przepis ten oznacza, że przepisy o ponownym wykorzystywaniu powinny być stosowane w pełnej zgodności z regułami odnoszącymi się do ochrony danych osobowych zgodnie z dyrektywą 95/46/WE i przepisami państw członkowskich, czyli na gruncie prawa polskiego ustawy z 29.8.2997 r. o ochronie danych osobowych[18].

Co istotne, dyrektywa 2013/37/UE dodała w art. 1 w ust. 4 lit. cc. W przepisie tym wymieniono trzy rodzaje dokumentów, w odniesieniu do których przepisy dyrektywy 2003/98/WE nie mają zastosowania, a tym samym nie podlegają ponownemu wykorzystywaniu. Są to:

- dokumenty wyłączone z dostępu na podstawie systemów dostępu z powodu ochrony danych osobowych;
- dokumenty, do których dostęp jest ograniczony na podstawie systemów dostępu z powodu ochrony danych osobowych;
- części dokumentów dostępne na podstawie tych systemów, które to części zawierają dane osobowe, których ponowne wykorzystywanie zostało określone w przepisach jako niezgodne z prawem dotyczącym ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

Uzupełnieniem regulacji jest motyw 11 preambuły, który stanowi, że zgodnie z dyrektywą 95/46/WE państwa członkowskie powinny określić warunki, pod którymi przetwarzanie danych osobowych jest zgodne z prawem. Ponadto wyeksponowano zasadę związania celem przetwarzania danych osobowych, odwołując się do postanowienia dyrektywy 95/46/WE przewidującego, że nie można dalej przetwarzać danych osobowych po to, by gromadzić je w sposób sprzeczny z określonymi, jednoznacznymi i uzasadnionymi celami, dla których te dane były gromadzone.

Implementując dyrektywę 2003/37/WE zarówno w jej pierwotnym, jak i w zmienionym brzmieniu, krajowy ustawodawca nie zdecydował o wprowadzeniu przesłanki ograniczającej prawo do ponownego wykorzystywania ze względu na ochronę danych osobowych. Za próbę określenia relacji pomiędzy prawem do ponownego wykorzystywania a ochroną danych osobowych nie sposób uznać art. 7 ust. 2 WykInfPubU, zgodnie z którym przepisy tej ustawy nie naruszają przepisów ustawy o ochronie danych osobowych[19].

Wątpliwości w zakresie relacji obu regulacji nie eliminuje również art. 6 ust. 2 WykInfPubU, zgodnie z którym prawo do ponownego wykorzystywania podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Przepis ten powtarza normę zawartą w art. 5 ust. 2 DostInfPubU ograniczającą dostęp do informacji publicznej.

Ponowne wykorzystywanie w przepisach rozporządzenia

Przepisy RODO określają – w art. 86 – relację prawa ochrony danych osobowych z prawem dostępu do dokumentów. Dane osobowe[20] zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa

[16] Impact Assessment Accompanying The Document Proposal For A Directive Of The European Parliament And The Council amending European Parliament and Council Directive 2003/98/EC on the re-use of public sector information SEC (2011) 1552 final, s. 10.

[17] Dz.Urz. WE L Nr 281, s. 31.

[18] T.j. Dz.U. z 2016 r. poz. 922 ze zm.; dalej jako: OchronaDanychU.

[19] *G. Sibiga*, Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia, Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016, Warszawa 2016, s. 20. Zob. również: *A. Piskorz-Ryń* (red.), Ustawa…, s. 196–215.

[20] W myśl art. 4 RODO dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). 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.

członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych. Przepis ten należy interpretować łącznie z motywem 154 preambuły, który stanowi, że publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny. Organ publiczny (podmiot publiczny) powinien móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane przepisami prawa Unii lub prawa państwa członkowskiego, któremu organ (lub podmiot) ten podlega.

Artykuł 86 RODO należy zaliczyć do tej kategorii przepisów ogólnego rozporządzenia, które – zdaniem *G. Sibigi* – powinny być obligatoryjnie przyjęte w prawie krajowym[21]. Wprawdzie nie służy on bezpośrednio wdrożeniu postanowień rozporządzenia, ale zachowaniu równowagi między prawem ochrony danych osobowych oraz prawem do informacji, które może być w różnorodny sposób ujęte w prawie krajowym[22]. Szersza analiza kwestii wyważania prawa do ochrony danych osobowych i publicznego dostępu do dokumentów, który na gruncie prawa krajowego jest uregulowany przepisami ustawy o dostępie do informacji publicznej, wykracza poza ramy niniejszego opracowania. Niemniej kwestia ta będzie wywoływała konsekwencje dla ponownego wykorzystywania ISP, bo – jak wskazano powyżej – przepisy dyrektywy 2003/37/WE opierają się na systemach dostępu (do dokumentów) istniejących w państwach członkowskich.

Dla omawianej tematyki istotne jest, że – w myśl motywu 154 – przepisy krajowe powinny godzić ponowne wykorzystywanie ISP z prawem do ochrony danych osobowych i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie rozporządzenia. Rozporządzenie nie daje jednak żadnych nowych wytycznych, jak zrealizować ten cel. Motyw 154 powtarza bowiem przywołane wyżej postanowienia dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE (art. 1 ust. 4 lit. cc).

Ponowne wykorzystywanie ISP zawierających dane osobowe

Wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, niezależnie od tego, czy są dostępne publicznie, stanowią dane osobowe. Zgodnie z definicją przytoczoną wcześniej ponowne wykorzystywanie ISP stanowiących dane osobowe będzie ich przetwarzaniem w rozumieniu przepisów o ochronie danych osobowych, np. przez gromadzenie danych i dokonywanie na nich dalszych operacji[23]. W związku z tym ponowne wykorzystywanie tych danych nadal podlega właściwym przepisom o ochronie danych osobowych i może następować wyłącznie z poszanowaniem zasad wynikających z tych przepisów, w tym zasady proporcjonalności, minimalizacji danych oraz zasady celowości[24].

Zarówno podmioty zobowiązane będące dysponentem danych, jak i „każdy zainteresowany", który pozyska dane jako ISP w trybie ich ponownego wykorzystywania, przetwarzając dane osobowe, od 25.5.2018 r. będą musiały respektować zasady ich przetwarzania określone w przepisach RODO[25]. Ich szczegółowa analiza wykracza poza ramy artykułu, trzeba jednak zaznaczyć, że rozporządzenie poszerzyło uprawnienia osób, których dane są poddane przetwarzaniu, np. w zakresie uprawnień informacyjnych wynikających z zasady przejrzystości.

Wnioski, jakie płyną z analizy przytoczonych aktów prawa UE oraz ustawy o ponownym wykorzystywaniu informacji sektora publicznego, mogą być następujące. Po pierwsze, prawo do ponownego wykorzystywania nie jest stosowane automatycznie i nie ma charakteru nadrzędnego wobec właściwych przepisów o ochronie danych. Po drugie, przepisy te jednocześnie nie wprowadzają bezwzględnego zakazu przekazywania ISP zawierających dane osobowe do ponownego wykorzystywania. Przepisy o ochronie danych osobowych oraz o ponownym wykorzystywaniu pozostają równorzędne. Ich współstosowanie może rodzić dla praktyki pewne trudności[26].

Zasadne będzie odwołanie się do rekomendacji Grupy Roboczej art. 29 zawartych w Opinii 06/2013[27]. Opinia ta została wydana już na gruncie dyrektywy 2013/37/UE, natomiast przed przyjęciem rozporządzenia. Analiza przepisów RODO pozwala wyprowadzić wniosek, że zalecenia zawarte w Opinii 06/2013 co do zasady pozostają aktualne i do czasu wydania nowych w tym obszarze rekomendacji przez Europejską Radę Ochrony Danych mogą być pomocniczo stosowane. Warto w tym miejscu zauważyć, że Wytyczne w sprawie zalecanych licencji standardowych, zbiorów da-

[21] *G. Sibiga*, Dopuszczalny zakres…, s. 19.

[22] *Ibidem*.

[23] Zgodnie z art. 4 pkt 2 RODO „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

[24] Opinia 06/2013, s. 31.

[25] Podstawowe zasady przetwarzania danych osobowych zostały enumeratywnie wymienione w art. 5 RODO. Są to: zasada zgodności z prawem, rzetelności i przejrzystości; zasada ograniczenia celu przetwarzania danych; zasada minimalizacji danych; zasada prawidłowości danych; zasada ograniczenia przechowania danych; zasada; integralności i poufności danych; zasada rozliczalności.

[26] O koncepcji współstosowania przepisów ustawy o ponownym wykorzystywaniu informacji sektora publicznego i ustawy o ochronie danych osobowych zob. *M. Sakowska-Baryła*, Ograniczenia prawa do ponownego wykorzystywania ISP, [w:] *E. Badura*, *M. Błachucki*, *X. Konarski*, *M. Maciejewski*, *H. Niestrój*, *A. Piskorz-Ryń*, *M. Sakowska-Baryła*, *G. Sibiga*, *K. Ślaska*, Ponowne wykorzystywanie informacji sektora publicznego, Ministerstwo Cyfryzacji 2016.

[27] Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowiona na mocy art. 29 dyrektywy 95/46/WE w związku z wejściem w życia ogólnego rozporządzenia o ochronie danych zostanie zastąpiona przez Europejską Radę Ochrony Danych.

nych i opłat za ponowne wykorzystanie dokumentów[28], wydane przez Komisję Europejską w celu wsparcia państw członkowskich w wykonaniu przepisów dyrektywy 2013/37/UE, zalecają stosowanie Opinii 06/2013 w zakresie ponownego wykorzystania danych osobowych.

W opinii tej wskazano, że przy stosowaniu dyrektywy 2003/98/WE i przepisów o ochronie danych do ponownego wykorzystywania danych osobowych podmiot zobowiązany może podjąć jedną z trzech różnych decyzji. Po pierwsze, może zdecydować o nieudostępnieniu danych osobowych do ponownego wykorzystania. Po drugie, może zdecydować o przekształceniu danych osobowych do formy zanonimizowanej (najczęściej w formie zbiorczych danych statystycznych) i udostępnieniu do ponownego wykorzystania tylko takich zanonimizowanych danych. Po trzecie, może podjąć decyzję o udostępnieniu danych osobowych do ponownego wykorzystania (w razie potrzeby podlegającą szczególnym warunkom i odpowiednim zabezpieczeniom).

Podejmując decyzję, podmiot zobowiązany musi w szczególności uwzględnić – wymienione wcześniej – wynikające z art. 1 ust. 2 lit. cc dyrektywy 2003/98/WE, jak również z motywu 154 zd. 7 RODO trzy okoliczności, z których wszystkie są wyłączone z zakresu stosowania ponownego wykorzystywania.

Grupa Robocza art. 29 rekomenduje, aby państwa członkowskie na poziomie przepisów krajowych jasno wskazały, które dane są udostępniane publicznie, do jakich celów oraz w jakim stopniu i na jakich warunkach ponowne wykorzystywanie jest dozwolone. Brak szczegółowych przepisów nie oznacza jednak, że dostępne publicznie dane osobowe mogą być zawsze ponownie wykorzystywane[29].

W praktyce problematyczna może się okazać realizacja podstawowej dla ochrony danych zasady celowości. Zasada ta wymaga, by dane osobowe, które zgromadzono do konkretnego celu, nie zostały następnie wykorzystane do innego celu niezgodnego z celem pierwotnym[30]. Podmiot, który pozyska ISP zawierające dane osobowe – niezależnie, czy od dysponenta danych, czy ze źródeł publicznie dostępnych – zgodnie z definicją ponownego wykorzystywania będzie je wykorzystywać, czyli przetwarzać, w innych celach niż te, dla których zostały przez podmiot zobowiązany wytworzone. Dyrektywa 2003/98/WE nie wyklucza możliwości, by nałożone w tym względzie warunki dopuszczały przetwarzanie wyłącznie w określonych celach. Dyrektywa ta jednocześnie stanowi, że warunki nie mogą ograniczać niepotrzebnie możliwości ponownego wykorzystywania. Należy wskazać, że postanowienia RODO dotyczące badania zgodności innego celu przetwarzania danych z celem, w którym dane osobowe zostały pierwotnie zebrane (art. 6 ust. 4), co do zasady opierają się na rekomendacjach Grupy Roboczej art. 29 zawartych w Opinii Nr 3/2013 z 2.4.2013 r. w sprawie zasady celowości, a następnie powtórzonych w opinii 06/2013. Analizując, czy dalsze przetwarzanie danych osobowych jest niezgodne z celami, dla których dane te zostały zgromadzone, zdaniem Grupy Roboczej art. 29 należy w szczególności uwzględnić: a) związek między celami, dla których zgromadzono dane osobowe, a celami dalszego przetwarzania; b) kontekst, w jakim gromadzono określone dane osobowe, oraz uzasadnione oczekiwania osób, których dane dotyczą, co do ich dalszego wykorzystania[31]; c) charakter danych osobowych oraz wpływ dalszego przetwarzania tych danych na osoby, których dane dotyczą; d) zabezpieczenia wprowadzone przez administratora w celu zapewnienia uczciwego przetwarzania danych oraz zapobieżenia niepożądanym skutkom dla osób, których dane dotyczą[32].

Aktualne pozostaje przedstawione w Opinii 06/2013 zalecenie, by w przypadku, gdy ISP zawierają dane osobowe i dozwolone jest ich ponowne wykorzystywanie, ponowni użytkownicy znali zasady przetwarzania takich danych od początku. Można tego dokonać poprzez zawarcie odpowiedniego postanowienia w licencji (warunkach ponownego wykorzystywania), przez co ochrona danych osobowych staje się zobowiązaniem umownym[33]. Licencje powinny określać granice wykorzystywania danych, w tym zapewnienie zgodności z celem, dla których zostały pierwotnie zebrane. Oznacza to, że w warunkach licencji należy określić pierwotny cel opublikowania danych oraz operacje, które byłyby z nim zgodne[34].

Grupa Robocza art. 29 zaleca, aby klauzula o ochronie danych była uwzględniania również w sytuacjach, gdy do ponownego wykorzystania udostępnione zostaną zanonimizowane zestawy danych uzyskanych z danych osobowych. Warunki ponownego wykorzystywania danych zanonimizowanych powinny zakazywać ponownej identyfikacji osób fizycznych i ponownego wykorzystania danych osobowych do celów, które mogą mieć wpływ na osoby, których dane dotyczą[35].

Rozporządzenie realizuje koncepcję podejścia do ochrony danych osobowych opartą na ryzyku[36]. Uwzględniając różne potencjalne czynniki ryzyka dla ochrony danych, a w szczególności fakt, że po publicznym udostępnieniu ISP zawierających dane osobowe sprawowanie skutecznej kontroli nad tymi danymi będzie znacznie utrudnione, istotne jest przestrzeganie zasad dotyczących ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej[37]. Rozwiązania te po raz pierwszy do polskiego porządku prawnego wprowadza art. 25 RODO.

[28] Dz.Urz. UE C Nr 240, s. 1.

[29] *Ibidem*, s. 10–11.

[30] *Ibidem*, s. 23.

[31] Art. 6 ust. 4 lit. b RODO stanowi o wzięciu pod uwagę kontekstu, w którym zebrano dane osobowe, w szczególności relacji między osobami, których dane dotyczą, a administratorem.

[32] Opinia 06/2013, s. 23.

[33] Na gruncie ustawy o ponownym wykorzystywaniu informacji sektora publicznego postanowienie to mogłoby stanowić element warunków ponownego wykorzystywania przedstawianych w ofercie, o której mowa w art. 23 ust. 1 pkt 3. W ustawie tej wprost nie przewidziano możliwości licencjonowania ISP, natomiast ISP można udostępnić, określając warunki ponownego wykorzystywania.

[34] *P. Drobek*, Ryzyka dla ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego, [w:] *G. Szpor* (red. nauk.), Jawność i jej ograniczenia, *A. Piskorz-Ryń* (red. tomu), T. V, Dostęp i wykorzystywanie, Warszawa 2015, s. 260.

[35] Opinia 06/2013, s. 32.

[36] *P. Drobek*, Ryzyka…, s. 241 i n.

[37] Opinia 06/2013, s. 32.

Ponadto według Grupy Roboczej art. 29 podmiot zobowiązany powinien przeprowadzić ocenę skutków w zakresie ochrony danych, zanim udostępni ISP zawierające dane osobowe do ponownego wykorzystania. W ocenie powinno się wskazać m.in. podstawę prawną ujawnienia danych (i ewentualną podstawę prawną ich ponownego wykorzystania), przeanalizować zasady w zakresie celowości, proporcjonalności oraz minimalizacji danych, a także uwzględnić konieczność specjalnej ochrony danych wrażliwych. W trakcie przeprowadzania tej oceny należy starannie uwzględnić możliwy wpływ na osoby, których dane dotyczą[38]. O ocenie skutków planowanych operacji przetwarzania dla ochrony danych osobowych stanowi art. 35 RODO.

Należałoby również postulować, aby w procesie tworzenia prawa przeprowadzano ocenę skutków planowanej regulacji dla prywatności i ochrony danych osobowych, która uwzględniałaby wpływ przewidywanych w projektach rozwiązań technologicznych na gwarancje autonomii informacyjnej jednostki, np. w ramach przeprowadzanej przez projektodawcę ocenie skutków regulacji[39].

Ocena skutków w zakresie ochrony danych powinna również zostać przeprowadzona w sytuacjach, gdy do ponownego wykorzystywania będą udostępniane zanonimizowane zestawy danych uzyskane z danych osobowych. W takim wypadku zasadnicze znaczenie ma ocena ryzyka ponownej identyfikacji oraz dobra praktyka w zakresie przeprowadzania testów na ponowną identyfikację. Wyniki oceny mogłyby pomóc podmiotowi zobowiązanemu w określeniu odpowiednich zabezpieczeń minimalizujących ryzyko, w tym m.in. środków technicznych, prawnych i organizacyjnych, takich jak odpowiednie warunki licencji (warunki ponownego wykorzystywania), środki techniczne uniemożliwiające masowe pobieranie danych czy zastosowanie odpowiedniej techniki anonimizacji[40]. Wyniki oceny mogą również prowadzić do podjęcia decyzji o rezygnacji udostępniania ISP zawierających dane osobowe do ponownego wykorzystania[41].

Podsumowanie

W przypadku ponownego wykorzystywania ISP, gdy zagrożona jest ochrona prywatności i ochrona danych osobowych, konieczne jest stosowanie zrównoważonego podejścia. Dotyczy to zarówno prawodawcy na etapie projektowania aktów prawnych, jak i dysponentów danych udostępniających ISP do ponownego wykorzystywania. Z jednej strony przepisy w zakresie ochrony danych osobowych nie powinny stanowić przeszkody w rozwoju rynku ponownego wykorzystywania. Z drugiej strony niezbędne jest poszanowanie prawa do ochrony danych osobowych i prawa do prywatności. Dlatego ważna jest realizacja przez administrację rządową we współpracy z Generalnym Inspektorem Danych Osobowych i interesariuszami postulatu Grupy Roboczej art. 29 dotyczącego ustanowienia i wspierania sieci wiedzy lub centrów doskonałości, a tym samym umożliwienie wymiany dobrych praktyk w zakresie anonimizacji i otwartych danych[42].

[38] *Ibidem*, s. 8.
[39] *P. Drobek*, Ryzyka…, s. 240.
[40] Przeglądu technik anonimizacji dokonała Grupa Robocza art. 29 w Opinii Nr 5/2014 z 10.4.2014 r. w sprawie technik anonimizacji.
[41] *Ibidem*.
[42] Przykładem dobrej praktyk może być sieć anonimizacyjna Zjednoczonego Królestwa (UK Anonymisation Network, UKAN), powołana jako konsorcjum Uniwersytetu w Manchesterze, Uniwersytetu w Southampton, Biura Statystyk Krajowych i Open Data Institute.

Słowa kluczowe: sektor publiczny, dane osobowe, RODO, informacje sektora publicznego, informacja publiczna.

Re-use of public sector information and personal data protection according to the General Data Protection Regulation and the directive 2003/98/EC – selected aspects

Public sector information, which is given to anyone who is interested, may contain personal data. The problem of collision of law to re-use information with right to privacy and data protection is extremely topical. The law of 25.2.2016 on re-use of public sector information took effect on 16.6.2016. Currently, work is conducted in regard to reforming state law which aims to implement provisions of General Data Protection Regulation which will be in force since 25.5.2018. In case of re-use of public sector information, when privacy and personal data protection are in a risk it is necessary to use balanced approach. It regards both the lawmaker on the stage of drafting legal acts, and holders of data who share public sector information in order to re-use it. Guidelines of the Article 29 Working Party might be helpful in this matter, which are included in the Opinion 06/2013. In the present article there is a discussion on selected aspects regarding implementation of the right to re-use of public sector information in the context of necessity to provide personal data protection Special analysis was devoted to recommendation of the Article 29 Working Party for the new legal order effective after 25.5.2018.

Keywords: public sector, personal data, GDPR, information of public sector, public information.

Ogólne rozporządzenie o ochronie danych osobowych (RODO) a prawo polskie – wybrane zagadnienia

Piotr Wróbel[1]

W niniejszym opracowaniu autor analizuje wpływ zbliżającej się europejskiej reformy ochrony danych osobowych na wybrane aspekty polskiego systemu prawnego. Autor podkreśla wybór szczególnej formy regulacji, jaką jest ogólne rozporządzenie, jako aktu bezpośrednio skutecznego i stosowalnego we wszystkich państwach członkowskich UE. Badany jest dopuszczalny zakres działalności legislacyjnej polskiego ustawodawcy w kontekście projektowanej ustawy o ochronie danych osobowych w nowym brzmieniu. Przyznane w niej roszczenia cywilnoprawne zostają następnie skonfrontowane z ich odpowiednikami w ugruntowanych już regulacjach polskiego Kodeksu cywilnego. Autor podejmuje próbę oceny skutków wynikających z podobieństw i różnic roszczeń przyznanych osobom fizycznym wskazanymi regulacjami.

Uwagi wstępne

Unijny ustawodawca, podejmując decyzję w sprawie ujednolicenia systemów ochrony danych osobowych w państwach członkowskich, stanął przed potrzebą wyboru środka legislacyjnego, który podoła realizacji założeń planowanej reformy. Obowiązująca od dwóch dekad 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[2] reprezentująca model harmonizacji minimalnej, tj. ustanawiającej pewien minimalny standard ochrony regulowanej w niej praw, została zastąpiona nie przez dyrektywę zakładającą tzw. harmonizację maksymalną, lecz przez zupełnie odmienny rodzaj aktu prawnego, jakim jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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[3]. Fakt ten już sam w sobie podkreśla założenia i cele reformy, która zmieni podejście do ochrony danych osobowych zarówno w sektorze prywatnym, jak i publicznym. Jednolitość przepisów na terenie całej UE z całą pewnością odmieni postrzeganie problemu bezpieczeństwa danych osób fizycznych, przetwarzanych na coraz większą skalę i za pomocą coraz to nowszych narzędzi. Jednak, mimo wyboru tak bezpośredniego środka ingerencji w systemy prawa państw członkowskich, RODO pozostaje aktem bardzo specyficznym, przewidującym szerokie kompetencje legislacyjne państw do doprecyzowywania pewnych poruszanych w nim zagadnień. W konsekwencji faktyczna pełna harmonizacja prawa wszystkich krajów UE w zakresie ochrony danych osobowych zostaje postawiona pod znakiem zapytania.

Jedną z kwestii budzących wątpliwości, która pojawia się przy analizowaniu wyżej wymienionych zagadnień, jest dopuszczalny zakres działalności legislacyjnej państw członkowskich w zakresie krajowych systemów ochrony danych, który w założeniu powinien zostać zdominowany przez europejski akt prawny, jakim jest RODO. Wyzwanie, przed jakim staje w chwili obecnej polski ustawodawca, polega nie tylko na potrzebie dostosowania przepisów, które do tej pory samodzielnie regulowały omawianą gałąź prawa, lecz także (a może przede wszystkim) na dostosowaniu przepisów sektorowych, które z jednej strony muszą być zgodne z nowymi założeniami, a z drugiej – muszą zostać uaktualnione pod kątem zmian w samej strukturze polskich aktów prawnych obejmujących ochronę danych osobowych.

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. Jednym z nowych elementów w tym zakresie jest pojawienie się roszczenia odszkodowawczego, przysługującego osobie fizycznej względem podmiotu odpowiedzialnego za niezgodne z przepisami procesowanie jej danych.

Rozporządzenie ogólne jako specyficzny akt prawa unijnego

We wstępnych rozważaniach należy przeanalizować, dlaczego, po przeszło dwudziestu latach obowiązywania dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r., europejski ustawodawca postanowił zmienić model regulacji systemu ochrony danych osobowych w UE poprzez zastosowania innego rodzaju aktu prawnego, jakim jest RODO, które zastąpi starą regulację. Dotychczas obowiązujący akt prawa wspólnotowego już ze swej natury w odmienny sposób kształtował materię, której miał doty-

[1] Student Wydziału Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] Dz.Urz. UE L Nr 281; dalej jako: dyrektywa 95/46/WE.

[3] Dz.Urz. UE L Nr 119, s. 1; dalej jako: ogólne rozporządzenie lub RODO.

czyć. Posłużono się dyrektywą jako aktem skierowanym do państw członkowskich, które te powinny implementować do swojego porządku prawnego w taki sposób, aby osiągnąć rezultat przewidziany przez dyrektywę, zachowując jednakże swobodę w zakresie wyboru formy i środków stosowanych w celu osiągnięcia tego stanu[4]. Założenia zastosowanego środka legislacyjnego przewidywały formę tzw. minimalnej harmonizacji, tj. przyjęto pewien minimalny standard, do którego realizacji miały dążyć państwa członkowskie, jednocześnie pozostawiono im możliwość podnoszenia poziomu ochrony w krajowym procesie implementacji[5].

Rozporządzenie jest z kolei środkiem legislacyjnym o zupełnie innym założeniu w kwestii zakresu obowiązywania. Ma zasięg ogólny oraz wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich[6]. W miejsce aktu wiążącego jedynie państwa członkowskie, i to co do rezultatu procesu implementacji, pojawia się akt, który będzie bezpośrednio stosowany i skuteczny nie tylko względem państw członkowskich i w odniesieniu do ich organów, ale będzie również zachowywać ten charakter w stosunkach horyzontalnych, czyli tych, które zaistnieją pomiędzy podmiotami praw i obowiązków opisanych w RODO[7].

Zmiana stosowanego środka legislacyjnego wynika z potrzeby rzeczywistego ujednolicenia zakresu ochrony danych osobowych, ponieważ dotychczasowa regulacja doprowadziła do sytuacji, w której przepisy poszczególnych państw członkowskich nadmiernie się zróżnicowały, co utrudniało zarówno funkcjonowanie organizacjom (w szczególności międzynarodowym), jak i realizację praw osób, których dane dotyczą[8]. Jednocześnie przestarzałe już przepisy nie uwzględniały skali, na jaką obecnie przetwarzane są dane osób fizycznych[9]. Obecnie powszechność przetwarzania danych i transgraniczny charakter tych procesów wymagają ustanowienia jednolitych zasad, na jakich mają się one odbywać, zarówno w celu ochrony osób, których dane są przetwarzane, jak i podmiotów, które te operacje prowadzą. Dyrektywa 95/46/WE nie doprowadziła do ujednolicenia regulacji w poszczególnych państwach członkowskich, tym samym uniemożliwiając realizację koncepcji wewnętrznego rynku, w szczególności wewnętrznego jednolitego rynku cyfrowego[10]. Jak wskazuje już art. 1 RODO, celem regulacji jest nie tylko zagwarantowanie ochrony podmiotom danych, lecz jednocześnie (i równorzędnie) swoboda przepływu tego rodzaju danych w Unii. Takie dwojakie określenie celów rozporządzenia podkreślają także motywy Nr 3 i 4 tego aktu. Powstające pytanie, czy cele te nie są sobie przeciwstawne, dychotomiczne i czy osiągnięcie jednocześnie obu jest w ogóle możliwe, zasługuje bezsprzecznie na odrębne opracowanie[11].

Rozporządzenie ogólne wpłynie nie tylko na akty prawne stanowione na poziomie unijnym, lecz także na te należące do porządków krajowych państw członkowskich. Forma rozporządzenia gwarantuje jego bezpośrednie obowiązywanie i stosowanie, z uwzględnieniem zasady pierwszeństwa prawa unijnego oraz zasady zgodnej wykładni prawa krajowego. Obowiązujący od maja 2018 r. akt bezsprzecznie wpłynie więc w szerokim zakresie na krajowe systemy ochrony danych osobowych, powstałe jeszcze na gruncie dyrektywy 95/46/WE, a tym samym często mocno się od siebie różniące.

W przypadku Polski jasne jest już w chwili pisania niniejszego opracowania, że obecnie obowiązująca ustawa z 29.8.2997 r. o ochronie danych osobowych[12] zostanie w całości uchylona co do jej aktualnego brzmienia, a nowy projekt, mimo pozostawienia oryginalnej nazwy aktu, regulować będzie inny zakres przedmiotowy, niż miało to miejsce dotychczas. Polskie Ministerstwo Cyfryzacji poddało konsultacjom społecznym projekty nowej ustawy o ochronie danych osobowych z 12.9.2017 r.[13] oraz ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych z 12.9.2017 r.[14], które powinny trafić pod obrady Sejmu w marcu 2018 r.

Ponieważ RODO w większości przypadków reguluje już kwestie, których dotyczyła stara UODO, jej nowa wersja skupia się na zagadnieniach, które unijny prawodawca pozostawił do doprecyzowania i uregulowania we własnym zakresie państwom członkowskim. *D. Lubasz* wskazuje, że tzw. klauzule kompetencyjne występują w RODO w kilkudziesięciu przypadkach, zezwalając legislatorom krajowym na podjęcie działań w szerokim zakresie, o ile ich wynik będzie pozostawać w zgodzie z duchem europejskiej regulacji i jej postanowieniami. Z uwagi na mnogość punktów, w których państwa członkowskie zostały upoważnione do aktywności prawodawczej, autor ten nazywa RODO wręcz hybrydą rozporządzenia i dyrektywy[15].

Należy wyraźnie podkreślić, że z uwagi na formę rozporządzenia prawo do stanowienia przez państwa członkowskie

[4] Art. 288 Traktatu o Funkcjonowaniu Unii Europejskiej z 26.10.2012 r. (Dz.Urz. UE C Nr 326, s. 47); dalej jako: TFUE.

[5] *A. Kunkiel-Kryńska*, Metody harmonizacji prawa konsumenckiego w Unii Europejskiej i ich wpływ na procesy implementacyjne w państwach członkowskich, Rozdział III, Lex/el. 2013.

[6] Art. 288 TFUE.

[7] *W. Wiewiórowski*, Nowe ramy ochrony danych osobowych w Unii Europejskiej, Dodatek specjalny do MoP 2012, Nr 7, s. 3.

[8] *M. Zadrożny*, [w:] *A. Dmochowska*, *M. Zadrożny* (red.), Unijna reforma ochrony danych osobowych – analiza zmian, Rozdział I, Warszawa 2016, s. 1.

[9] *Ibidem*.

[10] *D. Lubasz*, [w:] *E. Bielak-Jomaa*, *D. Lubasz*, RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Art. 1, Lex/el. 2017.

[11] Zob. *A. Grzelak*, [w:] *M. Kawecki*, *T. Osiej* (red.), Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia, Rozdział II, Legalis/el. 2017.

[12] T.j. Dz.U. z 2016 r. poz. 922 ze zm.

[13] Zob. https://www.gov.pl/documents/31305/0/Ustawa+o+ochronie+danych+osobowych+-+projekt+ (dostęp z 27.11.2017 r.); dalej jako: OchronaDanychU.

[14] Zob. https://www.gov.pl/documents/31305/0/Ustawa+Przepisy+wprowadzające+ustawę+o+ochronie+danych+osobowych+-+13.09.2017+%281%29.pdf/93d48166-2e06-cd02-ff22-ef3c446eadd8 (dostęp z 27.11.2017 r.).

[15] *D. Lubasz*, [w:] *E. Bielak-Jomaa*, *D. Lubasz*, RODO. Ogólne…

może być realizowane w zakresie ochrony danych osobowych jedynie w przypadkach wyraźnie wskazanych przez samo RODO. Zasadniczo uważa się za niedopuszczalne, aby ustawodawcy państw członkowskich w jakikolwiek sposób wprowadzali rozporządzenia do porządku krajowego, gdyż mogłoby to doprowadzić do pozbawienia rozporządzeń waloru źródeł prawa unijnego. Nie jest także dozwolone, aby państwa członkowskiego dokonywały wiążącej wykładni rozporządzenia[16]. Wyjątkiem są wspomniane właśnie klauzule kompetencyjne.

Nowa ustawa o ochronie danych osobowych

W świetle wyżej przedstawionych zagadnień uzasadniona wydaje się analiza projektu nowej ustawy o ochronie danych osobowych pod kątem dopuszczalności jej zakresu przedmiotowego ze spektrum wyjątków, na których doprecyzowanie pozwala państwom członkowskim RODO. Opracowanie takiego zagadnienia nie jest jednakże możliwe w krótkiej formie niniejszego artykułu, przede wszystkim z uwagi na mnogość klauzul kompetencyjnych zawartych w RODO. Dlatego elementem zbioru tych wyjątków, który pragnę poddać analizie, są kwestie odpowiedzialności cywilnej podmiotów przetwarzających dane osób fizycznych.

Wskazane zagadnienie zostało uregulowane w rozdziale 8 projektu nowej UODO. W art. 78 ust. 1 tego aktu wskazuje się, że każda osoba, której prawa przysługujące na mocy przepisów o ochronie danych osobowych zostały naruszone, może żądać zaniechania tego działania, a także ażeby ten, kto dopuścił się naruszenia, dopełnił czynności potrzebnych do usunięcia jego skutków. Następny ustęp stanowi natomiast, że roszczenie z art. 78 ust. 1 nie wyłącza możliwości wystąpienia z innymi roszczeniami z tytułu naruszenia przepisów o ochronie danych osobowych. Przytoczone przepisy bez wątpienia odwołują się do regulacji art. 79 oraz 82 RODO. Ten pierwszy gwarantuje prawo do skutecznego środka ochrony prawnej przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu, drugi z kolei zawiera liczne regulacje wskazujące m.in. na odpowiedzialność wszystkich podmiotów procesujących dane, obowiązek naprawienia szkody, zasadę odpowiedzialności, solidarny charakter odpowiedzialności czy też prawo do regresu.

Pojawia się pytanie, dlaczego polski projekt przyznaje podmiotom danych roszczenie z art. 78 ust. 1 nowej UODO, skoro przepisy RODO wprost wskazują na odpowiedzialność przetwarzających dane względem osób fizycznych, których dane dotyczą. Odpowiedź wiąże się ze sporami interpretacyjnymi, które toczą się wokół roszczenia z art. 82 RODO. Mianowicie, mimo że 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"[17]. Uzasadnienie projektu ustawy[18] wskazuje, że założeniem prawodawcy była realizacja normy kompetencyjnej ustanowionej w art. 79 ust. 1 RODO, tj. przyznanie skutecznego środka ochrony prawnej podmiotowi danych. Autorzy projektu przyjmują, że art. 82 RODO ogranicza przyznane odszkodowanie do charakteru majątkowego roszczenia, pozbawiając podmiot danych prawa żądania np. usunięcia skutków naruszenia przepisów o ochronie danych osobowych. Przepis ten ma więc spełniać rolę uzupełniającą względem roszczenia z rozporządzenia, poszerzając jego zakres o żądania o charakterze niemajątkowym[19].

W tym miejscu należy zastanowić się nad prawidłowością takiego rozwiązania. Z jednej strony autorzy w art. 78 ust. 2 jasno wskazują, że stosowanie tego przepisu nie może naruszać ani zaprzeczać skuteczności normy z art. 82 RODO, sami jednak wprost stwierdzają, że dążą do rozszerzenia przyznanej przez RODO ochrony. Stanowisko takie może budzić wątpliwości, ponieważ rozporządzenie ogólne ze swej natury wyznacza pewien standard ochrony, który co do zasady nie powinien być ani uszczuplany, ani rozwijany, chyba że akt unijny wprost na to zezwala. Przepis ten ewidentnie ma służyć uniknięciu niejasności w interpretowaniu natury roszczenia z art. 82 RODO. *D. Lubasz* nie widzi jednak problemu we wskazanym uregulowaniu art. 78 nowej UODO, wskazując, że art. 79 RODO faktycznie tworzy zobowiązanie państwa do wprowadzenia odpowiednich rozwiązań we własnych systemach prawnych, tak aby podmioty danych miały zapewnioną pełną ochronę. W analizowanym kontekście realizacja tego celu może się odbyć zarówno poprzez wprowadzenie w prawie krajowym nowych rozwiązań prawnych, jak i dostosowanie dotychczas obowiązujących do potrzeb takiego postępowania. Podobnie *M. Gumularz* stwierdza, że art. 79 ust. 1 RODO nie wyklucza wprowadzenia na płaszczyźnie prawa materialnego innych (niż roszczenie odszkodowawcze z art. 82 RODO) podstaw dochodzenia roszczeń wywodzonych z naruszenia ogólnego rozporządzenia[20].

[16] *T. Jaroszyński*, Rozporządzenie Unii Europejskiej jako składnik systemu prawa obowiązującego w Polsce, Lex/el. 2011.

[17] *D. Lubasz*, [w:] *E. Bielak-Jomaa*, *D. Lubasz*, RODO. Ogólne…

[18] Zob. https://www.gov.pl/documents/31305/0/Uzasadnienie+do+ustawy+o+ochronie+danych+osobowych+-+13.09.2017.odt/455148c6-64be-1fa5-34b0-729ce5ce7540 (dostęp z 27.11.2017 r.).

[19] Zob. Uzasadnienie do projektu, s. 38.

[20] *M. Gumularz*, Wpływ regulacji odpowiedzialności odszkodowawczej w ogólnym rozporządzeniu o ochronie danych osobowych na systemy prawa prywatnego państw członkowskich, Europejski Przegląd Sądowy 2017, Nr 5, s. 32.

Kolejny przepis, tj. art. 78 ust. 3 projektu nowej UODO, również rodzi wątpliwości, czy przyjęty zakres regulacji nie wykracza poza przyznane mu dozwolone ramy. Mianowicie przepis ten stanowi, że w zakresie nieuregulowanym RODO oraz niniejszą ustawą dochodzenie roszczeń, o których mowa w art. 78 ust. 1, następuje na zasadach określonych przepisami Kodeksu cywilnego. Zastanawia jednakże fakt, na jakiej podstawie przyjęto, że wskazana polska regulacja, jako element krajowego porządku prawnego, będzie właściwa do uzupełniającego stosowania w kwestiach nierozstrzygniętych przez RODO. Takie doprecyzowywanie rozporządzenia byłoby możliwe jedynie w przypadku, gdy ten europejski akt sam by na to zezwalał. Uzasadnienie projektu ustawy milczy w tej kwestii. Co prawda, autorzy projektu ustawy słusznie zauważają, że przepisy RODO nie są kompletne w zakresie dochodzenia roszczeń odszkodowawczych z art. 82, nie uwzględniając chociażby takich zagadnień, jak możliwość stosowania przepisów: wyłączających winę lub bezprawność, o podżeganiu, pomocnictwie i skorzystaniu ze szkody czy też art. 429 KC dotyczącego odpowiedzialności powierzającego przetwarzanie danych innemu podmiotowi[21]. W uzasadnieniu brakuje jednakże źródła kompetencji do wprowadzenia regulacji z art. 78 ust. 3 projektu nowej UODO, co należy poddać krytyce. Rozporządzenie ogólne nie wskazuje wprost na zastosowanie prawa krajowego w kwestiach odpowiedzialności cywilnej tam, gdzie sama regulacja rozporządzenia nie wystarcza do rozstrzygnięcia konkretnej kwestii. Wręcz przeciwnie. Motywy, jak chociażby Nr 146, wskazują, jak należy interpretować niektóre pojęcia z art. 82, w tym przypadku odpowiednio pojęcie szkody w świetle orzecznictwa TS, z kolei motyw Nr 75 zawiera otwarty katalog rodzajów szkód majątkowych i niemajątkowych. Motywy udzielają jednakże jedynie pewnych wskazówek, nie rozwiewając wszelkich wątpliwości i nie dopowiadając w pełni tego, co nie zostało uwzględnione w rozporządzeniu. Z tego względu należy przyjąć, że w celu skutecznego stosowania rozporządzenia i zapewnienia praw podmiotom przetwarzanych danych niezbędne będzie pomocnicze stosowanie prawa krajowego. Tak też argumentuje poparcie tego stanowiska *M. Gumularz*, wskazując, że nie sposób traktować art. 82 RODO jako samodzielnego i wyczerpującego reżimu odpowiedzialności odszkodowawczej i z tego względu należy umiejscowić go w reżimie odpowiedzialności deliktowej krajowego porządku prawnego[22]. W tym miejscu należy zauważyć, że polskie przepisy stosowane w sprawach o naruszenie przepisów o ochronie danych osobowych będą musiały być stosowane i interpretowane w taki sposób, by nie naruszały ani nie wypaczały RODO, bo jedynie w takiej sytuacji można przyjąć dopuszczalność ich uzupełniającego stosowania. W praktyce polska doktryna prawa cywilnego, jak również same regulacje raczej nie będą stanowiły problemów pod kątem dopuszczalności ich stosowania w kontekście RODO, w szczególności tam, gdzie art. 82 pozostawia kwestie zupełnie nieuregulowane. Przykładowo rozumienie pojęcia szkody zarówno w polskiej nauce prawa, jak i w orzecznictwie TS jest bardzo zbliżone, wręcz pokrywające się[23]. Wyjątek stanowią zagadnienia, które po części określa art. 82 RODO, nie czyniąc tego jednak w sposób zupełny, jak np. w przypadku zastosowania art. 429 KC, który mógłby mieć znaczenie w sytuacji powierzenia danych przez administratora innemu podmiotowi, która to z kolei sytuacja jest regulowana w RODO, jednakże nie w zakresie poruszanym przez polską ustawę.

Przyjęcie dopuszczalności uzupełniającego stosowania prawa krajowego nie wpływa jednak na rozwikłanie jeszcze jednej zasadniczej kwestii, a mianowicie problematyki wskazania prawa właściwego w przypadku deliktu z zakresu ochrony danych osobowych o charakterze transgranicznym. Jak wskazuje *M. Świerczyński*, przepisy RODO milczą w tym zakresie. Choć art. 82 ust. 6 RODO wskazuje na właściwość sądu do rozstrzygania spraw dotyczących niezgodnego z prawem przetwarzania danych osobowych, przepis ten milczy w kwestii wyboru właściwego prawa materialnego. *M. Świerczyński* wskazuje, że przepisy rozporządzenia Rzym II[24], zawierające normy kolizyjne dotyczące czynów niedozwolonych, wprost wyłączają jego zastosowanie do zobowiązań pozaumownych wynikających z naruszenia prawa do prywatności i innych dóbr osobistych[25]. Rozporządzenie ogólne nie zawiera więc rozstrzygnięcia tej kwestii i tym samym po raz kolejny trzeba będzie sięgnąć do prawa krajowego. Polska ustawa z 4.2.2011 r. – Prawo prywatne międzynarodowe[26] zawiera co prawda w art. 16 odrębną regulację poświęconą prawu właściwemu do dochodzenia roszczeń z naruszenia dóbr osobistych, jednakże nie można uznać tego przepisu za odpowiedź na analizowany problem, ponieważ dana osobowa sama w sobie nie jest zawsze dobrem osobistym (choć może nim być, o czym niżej).

Przedmiot roszczeń cywilnoprawnych z tytułu naruszenia dóbr osobistych a naruszenia przepisów o ochronie danych osobowych

Jak zaznaczono powyżej, dana osobowa nie jest co do zasady kategorią dobra osobistego w samej swej istocie. Roz-

[21] *M. Gumularz*, Wpływ regulacji…, s. 35.

[22] *Ibidem*, s. 32.

[23] *D. Klimas*, *P. Wróbel*, Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia (w druku).

[24] Rozporządzenie (WE) Nr 864/2007 Parlamentu Europejskiego i Rady z 11.7.2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Dz.Urz. UE L Nr 199, s. 40).

[25] *M. Świerczyński*, [w:] *M. Kawecki, T. Osiej* (red.), Ogólne rozporządzenie…, rozdział IV.

[26] T.j. Dz.U. z 2015 r. poz. 1792.

porządzenie 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 KC jako dobra osobiste osoby fizycznej[27]. 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. 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 także odszkodowania za wyrządzenie szkody majątkowej. Są to więc dwa oddzielne i niezależne reżimy odpowiedzialności deliktowej[28].

Powyższe stwierdzenie staje się jednak mniej oczywiste, jeżeli analizować oba reżimy odpowiedzialności z uwzględnieniem projektowanej ustawy o ochronie danych osobowych w jej obecnym kształcie. O ile w dalszym ciągu przedmiot naruszenia w obu reżimach odpowiedzialności może być formalnie odrębny, choć w praktyce identyczny, o tyle rodzaje dochodzonych roszczeń nie są już odmienne. W art. 78 ust. 1 projektu nowej UODO wprowadza się bowiem regulację odpowiadającą art. 24 ust. 1 KC i pokrywającą się z nią w najważniejszym aspekcie. Chodzi mianowicie o prawo do żądania zaprzestania naruszeń oraz do podjęcia czynności potrzebnych do usunięcia jego skutków. Chociaż w dalszym ciągu regulacja z Kodeksu cywilnego ma szerszy zakres zastosowania, ponieważ dotyczy także sytuacji zagrożenia naruszeniem, a nie jedynie sytuacji *post factum*, jak jest to w nowej UODO, oraz zawiera także roszczenia zadośćuczynienia pieniężnego bądź też zapłaty określonej sumy na wskazany cel społeczny, to jednak co do zasady spełnia jedną zasadniczą funkcję – uzupełnia RODO o roszczenia o charakterze niemajątkowym.

W świetle powyższych unormowań należy skonstatować, że doprowadzono do sytuacji, w której dwie regulacje, dotyczące tylko formalnie odrębnych zagadnień, przyznają niemal identycznie roszczenia, są więc niemal tożsame zakresowo i potencjalnie można uznać je za konkurencyjne. Wiążą się z tym faktem dość oczywiste problemy. Mianowicie już w chwili obecnej 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. Skoro regulacja dotycząca ochrony dóbr osobistych w Kodeksie cywilnym jest już dobrze znana, powszechnie stosowana i przede wszystkim kompletna, to czy racjonalne będzie w ogóle dochodzenie swoich praw na podstawie nowych regulacji z zakresu ochrony danych osobowych? Przecież obie regulacje zapewniają niemal identyczne roszczenia. Należy więc zastanowić się, czy przepisy nowej UODO i RODO w zakresie odpowiedzialności cywilnej mogą okazać się w praktyce rzadko stosowanymi mechanizmami dochodzenia praw podmiotów przetwarzanych danych. Co prawda dochodzenie praw na podstawie art. 24 KC 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. Dla kontrastu idealnym przykładem mniejszej pewności prawa w przypadku przepisów o ochronie danych osobowych jest kwestia orzekania o odpowiedzialności za szkodę na gruncie RODO w kontekście błędnego tłumaczenia polskiej wersji tego aktu, wskutek czego odpowiedzialność na zasadzie ryzyka z angielskiej wersji językowej została zastąpiona węższą odpowiedzialnością na zasadzie winy[29].

W związku z powyższymi uwagami, chociaż sama decyzja o odrębnym, bezpośrednim uregulowaniu odpowiedzialności cywilnej za nieprawidłowości w przetwarzaniu danych osobowych w założeniu była dobrym rozwiązaniem, ze względu na niekompletność nowych regulacji wprowadza ona zbędny chaos w polskim systemie prawa. Jak wskazuje *D. Lubasz*, „istotne znaczenie z punktu widzenia osób, których dane dotyczą, ma fakt oderwania podstawy potencjalnych roszczeń od naruszenia dóbr osobistych, w tym zwłaszcza prawa do prywatności, i oparcia ich na naruszeniu praw zagwarantowanych przepisami (…) rozporządzenia"[30], jednakże w praktyce przepisy te mogą być po prostu ze względów praktycznych niepowoływane przez podmioty dochodzące swoich praw.

[27] *D. Klimas*, *P. Wróbel*, Cywilnoprawna… (w druku).
[28] *Ibidem*.
[29] Zob. *D. Klimas*, *P. Wróbel*, Cywilnoprawna… (w druku).
[30] *D. Lubasz*, [w:] *E. Bielak-Jomaa*, *D. Lubasz*, RODO. Ogólne…

Zakres zastosowania art. 24 KC a art. 78 ust. 1 projektu nowej UODO

Aby udzielić odpowiedzi na pytanie o celowość stosowania nowych przepisów o ochronie danych osobowych w kontekście alternatywnej możliwości skorzystania z ochrony wynikającej z Kodeksu cywilnego, należy poddać analizie faktyczny zakres zastosowania obu rodzajów roszczeń.

Projekt nowej UODO, określając przedmiot ochrony, wskazuje na prawa, które są chronione mocą przepisów o ochronie danych osobowych, a które zostały naruszone. Regulacja ta wskazuje więc przede wszystkim na prawa wynikające z samego RODO, ale akt ten nie będzie jedynym obowiązującym w tym zakresie, dlatego na gruncie prawa europejskiego istotna może się okazać chociażby tzw. dyrektywa policyjna[31]. Polska regulacja wskazuje natomiast na ochronę dóbr osobistych, ujętych w otwartym katalogu, którego przykładowe elementy wymienia art. 23 KC. Jak wskazano powyżej, przedmiot ochrony obu kategorii może być, a w praktyce często będzie, tożsamy. Szczególny problem interpretacyjny tworzy jednakże jedno z dóbr osobistych ukształtowanych przez doktrynę oraz orzecznictwo, a mianowicie prywatność. Jak wskazuje *M. Krzysztofek*, wynika to z faktu, że dane osobowe są elementem, czy też aspektem, prawa do prywatności[32]. Pojawia się więc pytanie, czy należy uznać dane osobowe za odrębne dobro osobiste, skoro stanowią one element innego dobra osobistego w postaci prawa do prywatności? Wydaje się, że uproszczenie takie byłoby zbyt daleko idące, a co więcej, powodowałoby dalsze trudności praktyczne w interpretacji przepisów dotyczących obu tych kategorii, jeszcze bardziej pogłębiając wspomniany już problem mieszania dwóch reżimów odpowiedzialności. W doktrynie za wyodrębnieniem danych od dóbr osobistych opowiada się także *P. Sobolewski*, stwierdzając, że „dane osobowe nie są odrębnym od prywatności dobrem osobistym. Restrykcyjne przepisy dotyczące przetwarzania danych osobowych stanowią wyraz ochrony prawa do prywatności za pomocą środków administracyjnoprawnych, natomiast ochrona prywatności jako dobra osobistego jest zapewniana przy wykorzystaniu instrumentów cywilnoprawnych”[33]. Tak więc roszczenia cywilnoprawne z Kodeksu cywilnego mają za zadanie zapewnić bezpośrednią ochronę prywatności jako dobra osobistego, natomiast ochrona danych osobowych jest jedynie środkiem do osiągnięcia celu w postaci ochrony szeroko rozumianej prywatności, jednakże na zupełnie odmiennej płaszczyźnie prawa. Roszczenia przyznane przez projekt nowej UODO i RODO co prawda modyfikują charakter przepisów o ochronie danych osobowych poprzez uwzględnienie w nich roszczeń cywilnoprawnych, jednakże nie należy zapominać, że wskazane akty prawne co do zasady są regulacjami administracyjnoprawnymi, zawierającymi jedynie elementy prawa prywatnego. Ze względu na powyższe wydaje się uzasadnione przyjęcie, że tożsamość przedmiotu obu roszczeń może zachodzić dopiero na najniższym poziomie, tzn. przedmiotu konkretnej danej osobowej i dobra osobistego.

Sama odrębność danych osobowych i dóbr osobistych nie wyklucza jeszcze, że naruszenie tych pierwszych będzie implikować naruszenie także prywatności jako dobra osobistego. Możliwość zaistnienia takiego schematu dopuszczają autorzy projektu nowej UODO[34], wskazując na częste powiązanie naruszenia ochrony danych osobowych z naruszeniem prywatności. Twórcy regulacji są jednak jednocześnie świadomi, że specyficzne rozumienie prywatności jako intymnej, indywidualnej sfery życia człowieka może prowadzić do wąskiego interpretowania jej zakresu, tym samym ograniczając możliwość powiązania obu naruszeń. Posługując się przykładem, można zadać pytanie, czy niespełnienie obowiązku aktualizacji danych na wniosek osoby fizycznej, której te dotyczą, pozyskanych np. w celu zrealizowania wcześniej zawartej umowy, będzie automatycznie naruszeniem prawa do prywatności? Wydaje się, że koncepcje naruszeń w tym przypadku nie pokrywają się.

Przedstawione dotychczas kwestie prowadzą do konkluzji, że postawiona wcześniej teza o potencjalnej nieprzydatności roszczeń z art. 78 projektu nowej UODO może się okazać, przynajmniej częściowo, nietrafna. Wydaje się, że w typowych sprawach z pogranicza danych osobowych i dóbr osobistych, dotyczących np. bezprawnego posłużenia się wizerunkiem, danymi kontaktowymi czy też związanych z pozyskiwaniem informacji o osobach fizycznych, przydatniejsze w dochodzeniu swoich praw mogą się okazać roszczenia wynikające z art. 24 KC jako dobrze już znane w polskiej praktyce i zakorzenione w rodzimym porządku prawnym. Kiedy jednak przedmiotem roszczenia będą żądania o charakterze raczej technicznym, organizacyjnym, powiązanym w sposób szczególny z danymi osobowymi i prawem osoby fizycznej do sprawowania nad nimi kontroli, przepisy nowej UODO powinny znaleźć swoje zastosowanie. Analiza zakresów przedmiotowych regulacji obu polskich ustaw jasno wykazuje, że zakresy roszczeń, choć czasem bardzo zbliżone, jednak nie są identyczne, a oczywiste jest, że sama tożsamość

[31] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową rady 2008/977/WSISW 27.4.2016 r. (Dz.Urz. UE L Nr 119, s. 89).

[32] *M. Krzysztofek*, Ochrona danych osobowych w Unii Europejskiej, Warszawa 2014, s. 39.

[33] *P. Sobolewski*, [w:] *K. Osajda* (red.), Kodeks Cywilny. Komentarz, rozdział art. 23, Beck Online Komentarze, Legalis/el. 2017.

[34] Zob. Uzasadnienie do projektu, s. 37.

możliwych żądań (np. zaniechania naruszeń) nie rekompensuje tych rozbieżności.

Ostatnim, wartym poruszenia zagadnieniem jest kwestia zbiegu roszczeń z Kodeksu cywilnego, RODO oraz nowej UODO. Zgodnie z art. 24 ust. 3 KC przepisy tego artykułu nie uchybiają uprawnieniom przewidzianym w innych przepisach. Konsekwencją tak sformułowanej regulacji jest fakt, że rozważania nad wyborem roszczenia wskazane we wcześniejszych akapitach nie muszą mieć większego znaczenia, ponieważ możliwe będzie stosowanie obu ich rodzajów jednocześnie. Inną kwestią jest ocena racjonalności i praktycznego wymiaru takiego rozwiązania. Dochodzenie roszczeń niemajątkowych na podstawie przepisów Kodeksu cywilnego, jak również projektu nowej UODO nie wyłącza zastosowania przepisów dotyczących roszczeń majątkowych na gruncie RODO. Poza wskazanym już art. 24 ust. 3 KC podobną regulację zawiera art. 78 ust. 2 nowej UODO, bezspornie odwołujący się do art. 82 RODO, który stanowi źródło roszczeń cywilnych wynikających z europejskiej regulacji.

Podsumowanie

Z powyższych rozważań wydaje się jasno wynikać, że szybko nadchodząca reforma systemu ochrony danych osobowych pod wieloma względami stanowi szerokie pole do prowadzenia dyskusji i badań naukowych. Skoro już sama teoretyczna analiza zagadnień, takich jak dopuszczalność uzupełniającego stosowania prawa krajowego, przyjęcie jego funkcji doprecyzowującej czy też rozróżnienie dóbr osobistych i danych osobowych, stanowi w wielu punktach niemały problem interpretacyjny, nietrudno sobie wyobrazić, w jakim stopniu kłopotliwe może się okazać stosowanie nowych przepisów w praktyce. Należy podkreślić, że rozwiązania przyjęte w projektach polskich ustaw towarzyszących RODO pozostają na chwilę obecną jedynie propozycjami, które mogą ulegać jeszcze niejednokrotnym zmianom. Jak jednak wskazuje *P. Litwiński*, sytuacja, w której opracowywane projekty nie weszłyby w życie do maja przyszłego roku, nie dostosowując tym samym ustaw sektorowych do wymogów reformy, miałaby katastrofalne skutki dla polskiej gospodarki[35]. Rozporządzenie ogólne pozostaje więc poważnym wyzwaniem zarówno dla teoretyków prawa, praktyków, jak i samego krajowego ustawodawcy.

[35] *P. Litwiński*, [w:] *S. Cydzik*, Dane osobowe: nic nie zatrzyma unijnych zmian, RP.pl 2017, http://www.rp.pl/Dane-osobowe/310309863-Dane-osobowe-nic-nie-zatrzyma-unijnych-zmian.html (dostęp z 6.12.2017 r.).

Słowa kluczowe: RODO, dane osobowe, dobra osobiste, Kodeks cywilny, UODO, roszczenia, odpowiedzialność.

General regulation on personal data protection (GDPR) and Polish law – selected aspects

In this paper the author analyses the impact of the upcoming European personal data protection reform on selected aspects of Polish legal system. The author emphasizes the choice of specific form of regulation, which is the general regulation, as the act directly effective and applicable in all member states of EU. Subsequently, admissible scope of legislative agenda of the Polish legislator is studied in the context of changes planned in the Polish personal data protection act. Civil claims granted by said act are confronted with their counterparts in already well-established regulations of Polish Civil Code. Finally, the author attempts to evaluate consequences that arise from similarities and differences of claims granted to legal persons by both regulations.

Keywords: GDPR, personal data, personal rights, Civil Code, data protection act, claims, liability.

WYMOGI EDYTORSKIE:

- język publikacji: polski, angielski, niemiecki, rosyjski;
- edytor tekstu Word (format .doc lub .docx);
- styl czcionki: Times New Roman;
- wielkość czcionki: tekst główny – 12 pkt, przypis – 10 pkt;
- interlinia: 1,5 wiersza (w przypadku przypisów – 1 wiersz);
- objętość artykułu: do 30 000 tys. znaków ze spacjami;
- marginesy: standardowe – wszystkie 2,5 cm;
- przypisy dolne: odsyłaczami przypisów powinny być cyfry arabskie; odsyłacz należy umieścić bezpośrednio po fragmencie, do którego odnosi się przypis (przed kropką kończącą zdanie);
- należy dołączyć słowa kluczowe w języku polskim i angielskim;
- tytuł powinien być napisany czcionką Times New Roman 14 pkt (czcionka pogrubiona);
- tekst powinien składać się z następujących części: lid (streszczenie ok. 1500 znaków ze spacjami), uwagi wstępne, rozwinięcie (z podziałem na zatytułowane części), podsumowanie;
- do artykułu należy załączyć także lid (streszczenie) w języku angielskim (ok. 1500 znaków ze spacjami);
- śródtytuły nie powinny być numerowane, lecz pogrubione;
- należy dołączyć notę biograficzną (ok. 800 znaków ze spacjami);
- prosimy o wskazanie afiliacji.

Powoływane w przypisach pozycje bibliograficzne prosimy pisać według wzoru:

Inicjał. Nazwisko, Tytuł, ew. numer wydania, tom, część itp., miejsce i rok wydania, a następnie cytowane strony skrótem „s.", np.: *J. Kowalski*, Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku kolejnego powołania się **bezpośrednio** na cytowaną pozycję:

Ibidem, s. 15–16.

Powołanie kolejny raz, gdy cytujemy tylko jedną pozycję danego autora:

J. Kowalski, *op. cit*., s. 29–20.

Kolejne powołanie, gdy cytuje się kilka pozycji danego autora, zawiera pierwsze wyrazy tytułu, np.:

J. Kowalski, Jak pisać..., s. 28–29.

W przypadku **prac pod redakcją**, jeśli powoływana publikacja stanowi część całości:

P. Igrek, Cytowanie, [w:] *J. Kowalski* (red.), Jak pisać przypisy?, t. 2, Warszawa 2006, s. 12–13.

W przypadku publikacji w czasopismach tytuł czasopisma zastępuje nazwę wydawnictwa, po nim następuje rok (rocznik), przecinek, następnie numer (nr) w ramach rocznika ewentualnie także numer od początku wydawania pisma i numer strony:

J. Kowalski, Jak pisać przypisy?, Wiadomości Tekściarskie 2006, Nr 28 (236), s. 7.

Kilka kwestii specjalistycznych:

1. Oczekiwane oznaczenie ustawy wygląda następująco: Dz.U. z 2006 r. Nr 28, poz. 456.
2. Publikator prosimy podawać jedynie przy pierwszym przywołaniu aktu prawnego. Wówczas nazwę aktu i datę (miesiąc słownie) podajemy w tekście głównym (np. ustawa z 13.4.2003 r. o zasadach pisania artykułów), w przypisie zaś publikator (np. t.j. Dz.U. z 2006 r. Nr 28, poz. 456).
3. Zapisując artykuł, ustęp, punkt aktu prawnego, skrótów nie oddzielamy przecinkami, tak więc: art. 28 ust. 59 pkt (bez kropki!) 36, a nie: art. 28, ust. 59, pkt. 36.
4. W przypadku orzeczeń sądowych prosimy o zastosowanie następujących oznaczeń: Wyrok SN z 11.5.2011 r., I CA 123/11, OSNCP 2011, Nr 8, poz. 34. Nazwę orzeczenia i jego datę prosimy podać w tekście głównym (np. wyrok SN z 11.5.2011 r.), natomiast w przypisie publikator (I CA 123/11, OSNCP 2011, Nr 8, poz. 34).

Harmonogram publikacji:

Nr 1 – teksty do końca stycznia, druk luty/marzec
Nr 2 – teksty do końca kwietnia, druk maj/czerwiec
Nr 3 – teksty do końca lipca, druk sierpień/wrzesień
Nr 4 – teksty do końca października, druk listopad/grudzień

Osoba do kontaktu: dr *Aleksandra Klich*, e-mail: pme@beck.pl

EDITORIAL REQUIREMENTS:

- language of publication: Polish, English, German, Russian;
- text editor MS Word (.doc or .docx);
- font style: Times New Roman;
- font size: main text – 12 pts, footnote – 10 pts;
- line spacing: 1.5 line (for footnotes – 1 row);
- volume of the article: up to 30,000 characters with spaces;
- margins: standard – all 2.5 cm;
- footnotes: cross-referenced footnotes should be Arabic numerals; reference should be placed immediately after the passage to which the footnote regards (before the full stop ending a sentence);
- article must be attached with key words in Polish and English;
- the title should be written in Times New Roman 14 pts (bold);
- text should consist of following parts: lead (summary, around 1500 characters with spaces), initial comments, amplification (with a division into parts with titles), summation;
- article should also be attached with a lead (summary) in English (around 1500 characters with spaces);
- intertitles should not be numbered, but bold;
- article must be attached with a biographical note (approx. 800 characters including spaces);
- please indicate affiliation.

The referenced sources should adhere to the following style:

Initial(s). Last name, Title, edition number if applicable, volume, part, etc., place and year of publication, followed by the page(s) referred to with the 'p. (pp.)' abbreviation, e.g.: *J. Kowalski*, How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For subsequent reference made **directly** to the cited item:

Ibidem, p. 15–16.

Further reference, when several positions by a given author are being cited, include the first words of the title, e.g.:

J. Kowalski, How to..., p. 28–29.

For edited volumes, when the publication referenced forms a part of the whole:

P. Igrek, Citing, [in:] *J. Kowalski* (ed.), How to do references?, Vol. 2, Warszawa 2006, p. 12–13.

For publications in periodicals, the title of the periodical replaces the name of the publisher, followed by the year, comma, then the number (No.) within the year, possibly the consecutive number and page numbers:

J. Kowalski, How to do references?, Editorial news 2006, No. 28 (236) p. 7.

A few technical issues:

a. Expected indication of a legal act goes as follows: Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April on the rules of writing articles), and the publishing body shall be given in the footnote (e.g. Journal of Laws of 2006, No. 28, item 456).
b. When writing article, paragraph, point of a legal act, abbreviations should not be separated by commas, that is: art. 28 par. 59 point (no full stop!) 36, not: art. 28, par. 59, pt. 36).
c. For court judgements, please use the following indications: Judgement of the Supreme Court of 11.5.2011, I CA 123/11, OSNCP 2011, No. 8, item 34. Mind that the appelative of the judgement and its date should be indicated in the main text (e.g. Judgement of the Supreme Court of 11.5.2011), and the publishing body in the footnote (I CA 123/11, OSNCP 2011, No. 8, item 34).

Publication schedule (deadlines):

No. 1 – submitting manuscripts – end of January (print – February/March)
No. 2 – submitting manuscripts – end of April (print – May/June)
No. 3 – submitting manuscripts – end of July (print – August/September)
No. 4 – submitting manuscripts – end of October (print – November/December)

Contact Person: *Aleksandra Klich* PhD, e-mail: pme@beck.pl