PME
3/2017

PRAWO Mediów Elektronicznych

www.ksiegarnia.beck.pl

ISSN 2082-100X 03
9 772082 100176

Cena 65 zł (w tym 5% VAT)

C·H·BECK

PME

3/2017

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 trzeci numer kwartalnika naukowego Prawo Mediów Elektronicznych. Podobnie jak poprzednie wydania i ten numer jest poświęcony zagadnieniom wpływu nowoczesnych technologii na prawo. W szczególności na uwagę zasługują dwa artykuły: *Katarzyny Syskiej* – Prawo dostępu do danych w kontekście prawa przenoszalności – porównanie celu regulacji, zakresu i przesłanek stosowania oraz *Pauliny Leji* – Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych. W tym numerze znajdą Państwo również drugą część artykułu dr *Aleksandry Budniak-Rogali* o przeprowadzeniu dowodu za pomocą środków porozumiewania się na odległość na podstawie art. 235 § 2 KPC po nowelizacji z 10.7.2015 r.

Ciekawe poglądy odnoszące się do instytucji prawa do bycia zapomnianym odnaleźć można w artykule *Marcina Rojszczaka*, a krótki rys prawnoporównawczy o możliwości składania pism procesowych w postępowaniu cywilnym elektronicznie – w artykule *Anny Materli*.

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*

Prawo dostępu do danych a prawo przenoszalności – porównanie celu regulacji, zakresu i przesłanek stosowania

adw. *Katarzyna Syska*[1]

Celem niniejszego artykułu jest ustalenie różnic między prawem dostępu do danych osobowych a prawem do przenoszenia danych osobowych na gruncie 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[2]. W pierwszej kolejności przedstawiony będzie cel regulacji prawa dostępu do danych oraz prawa przenoszalności danych. W dalszej części zawarta jest analiza porównawcza dotycząca przesłanek stosowania każdego z praw, ograniczeń ich stosowania, zakresu danych przekazywanych na podstawie każdego z praw, formatu przekazywania danych, a także zakresu obowiązków administratora w przypadku zgłoszenia żądania skorzystania z prawa dostępu lub prawa do przenoszenia danych. Ponadto w tekście wskazuje się na praktyczne problemy, które mogą się pojawić przy odpowiadaniu na żądania osób, których dane dotyczą, co do skorzystania z tych praw.

Uwagi wstępne

Prawo dostępu do danych osobowych jest podstawowym prawem związanym z przetwarzaniem danych. Pozwala ono osobom, których dane dotyczą, kontrolować wykorzystywanie ich danych osobowych[3]. Jego celem jest więc zapewnienie transparentności (przejrzystości) przetwarzania danych osobowych. Prawo dostępu nie jest regulacją nową – przewiduje je również 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[4] oraz ustawa z 29.8.1997 r. o ochronie danych osobowych[5], a także inne akty prawne dotyczące ochrony danych osobowych[6].

W ogólnym rozporządzeniu prawu dostępu do danych osobowych poświęcony jest art. 15. Przepis ten jest bardziej szczegółowy niż odpowiadający mu art. 12 lit. a dyrektywy 95/46/WE. Dla przykładu, art. 15 ust. 3 RODO reguluje kwestię ewentualnych opłat za otrzymanie kopii swoich danych, a także możliwość żądania i uzyskania kopii danych drogą elektroniczną. Celem Komisji Europejskiej było wzmocnienie prawa dostępu do danych osobowych, a także harmonizacja szczegółowych warunków korzystania z tego prawa[7].

Natomiast prawo do przenoszenia danych jest uprawnieniem nowym, które pojawiło się dopiero w ogólnym rozporządzeniu. Zgodnie z art. 20 ust. 1 i 2 RODO prawo do przenoszenia danych składa się z trzech elementów: (1) prawo osoby, której dane dotyczą, do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych jej dotyczących, które dostarczyła administratorowi, (2) prawo przesłania tych danych osobowych innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, oraz (3) prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Właśnie to ostatnie uprawnienie – do żądania bezpośredniego przesłania danych innemu administratorowi – stanowi *novum* w prawie ochrony danych osobowych[8].

Komisja Europejska zaproponowała wprowadzenie prawa do przenoszenia danych do porządku prawnego UE jako odpowiedź na trudności w wycofaniu (odebraniu) danych od jednego usługodawcy i przeniesienia ich do innego usługodawcy do dalszego przetwarzania. Komisja uznała, że przy częstym korzystaniu z konkretnej usługi świadczonej online ilość zgromadzonych przez usługodawcę danych osobowych staje się przeszkodą dla zmiany dostawcy usług, nawet jeżeli dostępne są usługi lepsze, tańsze lub lepiej chroniące prywatność. Ponowne ręczne wprowadzanie danych do innej usługi może wymagać zbyt dużego wysiłku. Prowadzi to z kolei do uzależnienia od konkretnego usługodawcy. W opinii Komisji

[1] Autorka jest adwokatem współpracującym z kancelarią prawną Traple Konarski Podrecki i Wspólnicy.

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

[3] *J. Barta, P. Fajgielski, R. Markiewicz*, Ochrona danych osobowych. Komentarz, Warszawa 2015, wyd. 6, Lex/el., komentarz do art. 32.

[4] Dz.Urz. L Nr 281, s. 31–50; dalej jako: dyrektywa 95/46/WE.

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

[6] Na przykład Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28.1.1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25).

[7] Dokument roboczy służb Komisji – ocena skutków w zakresie wniosku Komisji z 25.1.2012 r. dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), SEC(2012)0072 final (ang. *Commission Staff working paper – impact assessment*), s. 34.

[8] *W. Wiewiórowski*, Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych, Europejski Przegląd Sądowy 2017, Nr 5, s. 25.

przenoszalność danych jest niezbędna w celu zapewnienia skutecznej konkurencji, co widać na przykładzie innych branż, np. możliwości przenoszenia numerów telefonów[9].

Niektórzy autorzy twierdzą, że prawo do przenoszenia danych zostało wprowadzone z myślą o internetowych sieciach społecznościowych, co wynika z faktu, że znajduje ono zastosowanie tylko w przypadku, gdy podstawą przetwarzania danych jest zgoda lub umowa[10] (o czym będzie mowa w kolejnej części artykułu). Poza sieciami społecznościowymi jako przykład zastosowania prawa do przenoszenia danych podaje się platformę handlu elektronicznego eBay. Na platformie tej istnieje system oceny sprzedawców. Renoma sprzedawców i pozytywne opinie wyrażane o nich przez kupujących mają olbrzymie znaczenie dla sprzedawców. Umożliwienie przenoszalności profili sprzedawców (wraz z opiniami o nich) znacząco ułatwiłoby im rozpoczęcie swojej działalności na innych platformach handlowych, gdyż nie musieliby budować swojej renomy od zera[11].

Prawo do przenoszenia danych – jako dające większą kontrolę nad własnymi danymi i umożliwiające wybór usługodawcy – stanowi też wyraz autonomii informacyjnej jednostki[12]. Przyznanie większej kontroli nad swoimi danymi osobom, których dane dotyczą, wskazane jest jako cel regulacji także w wytycznych Grupy Roboczej Artykułu 29[13] dotyczących prawa do przenoszenia danych[14], a także w motywie 68 RODO.

Analiza porównawcza

W tej części artykułu prawo dostępu i prawo do przenoszenia danych zostaną porównywane pod kątem przesłanek stosowania, ograniczenia stosowania, zakresu przekazywanych danych, formatu przekazywania danych, a także zakresu obowiązków administratora.

1. Przesłanki stosowania

Przesłanki stosowania analizowanych praw można podzielić na kryteria o charakterze prawnym oraz faktycznym.

Przy przesłankach natury prawnej należy odnieść się do prawnych podstaw przetwarzania danych osobowych. Prawo dostępu do danych osobowych stosuje się bez względu na podstawę przetwarzania danych – art. 15 RODO nie zawiera w tym zakresie żadnych ograniczeń. Natomiast zgodnie z art. 20 ust. 1 lit. a RODO prawo przenoszalności znajduje zastosowanie tylko w przypadkach, gdy podstawą przetwarzania danych jest zgoda (art. 6 ust. 1 lit. a lub art. 9 ust. 1 lit. a RODO) lub umowa (art. 6 ust. 1 lit. b RODO).

Należy zwrócić uwagę, że w przypadku gdy przetwarzanie danych ma kilka podstaw prawnych – np. w pewnym zakresie odbywa się w związku z realizacją obowiązku prawnego, częściowo na podstawie umowy, a częściowo na podstawie uzasadnionego interesu – prawo do przenoszenia danych można stosować tylko w odniesieniu do tych danych, które są przetwarzane na podstawie umowy. Dla przykładu, instytucja finansowa przetwarzająca dane klienta m.in. w celu wykrywania prania brudnych pieniędzy – co odbywa się w ramach wykonania obowiązków prawnych – nie ma obowiązku umożliwiania przenoszenia danych klienta w tym zakresie, mimo że z klientem łączy ją umowa, która również stanowi podstawę przetwarzania danych[15].

Jeśli chodzi o przesłanki natury faktycznej, aby móc korzystać z prawa do przenoszenia danych, przetwarzanie musi odbywać się w sposób zautomatyzowany (art. 20 ust. 1 lit. b RODO). Natomiast sposób przetwarzania danych nie ma znaczenia w przypadku zamiaru skorzystania z prawa dostępu – ma ono zastosowanie zarówno w przypadku przetwarzania w formie papierowej, jak i przy użyciu systemu informatycznego.

Z powyższego wynika, że co do zasady żądania dostępu do danych mogą być składane w każdym przypadku przetwarzania danych, natomiast żądania przenoszenia danych – w wybranych przypadkach.

2. Ograniczenia stosowania

Zarówno w przypadku prawa do przenoszenia danych, jak i prawa uzyskania kopii danych w ramach prawa dostępu przewidziano takie samo ograniczenie stosowania tych praw. Mianowicie korzystanie z nich nie może niekorzystnie wpływać na prawa i wolności innych – co wynika z art. 15 ust. 4 oraz art. 20 ust. 4 RODO. W grę wchodzić mogą różne rodzaje praw osób trzecich, np. prawo do prywatności i ochrony danych osobowych innych osób, ochrona tajemnicy handlowej lub innych praw własności intelektualnej. Dla przykładu, profil osoby w sieci społecznościowej zawiera też dane innych osób, takie jak lista znajomych czy zdjęcia innych osób. Dokumentacja medyczna zawiera dane lekarzy, którzy zajmowali się danym pacjentem. Z kolei dane, takie jak

[9] Dokument roboczy służb Komisji – ocena skutków..., s. 28; w kontekście prawa konkurencji szerzej: *I. Graef*, *J. Verschakelen*, *P. Valcke*, Putting the right to data portability into a competition law perspective, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2416537 (dostęp z 30.11.2017 r.).

[10] *P. de Hert*, *V. Papakonstantinou*, The new General Data Protection Regulation: Still a sound system for the protection of individuals?, Computer Law & Security Review 2016, Nr 32, s. 190.

[11] *B. Van der Auwermeulen*, How to attribute the right to data portability in Europe: A comparative analysis, Computer Law & Security Review 2017, Nr 33, s. 70.

[12] *G. Zanfir*, The right to Data Portability in the context of the EU data protection reform, International Data Privacy Law 2012, t. 2, Nr 3, s. 152.

[13] Organ doradczy UE w zakresie ochrony danych osobowych; dalej jako: Grupa Robocza.

[14] Wytyczne Grupy Roboczej Artykułu 29 z 5.4.2017 r. dotyczące prawa do przenoszenia danych (ang. *Guidelines on the right to data portability*), Nr dokumentu WP 242 rew.01, http://giodo.gov.pl/pl/1520296/10055 (dostęp z 30.11.2017 r.).

[15] Wytyczne Grupy Roboczej dotyczące prawa do przenoszenia danych…, s. 9.

ocena zdolności kredytowej, preferencji zakupowych, stylu życia, potencjalnego rozwoju kariery, są wynikiem analizy przeprowadzonej w oparciu o narzędzia będące przedmiotem tajemnicy przedsiębiorstwa lub prawa autorskiego[16].

Należy jednak podkreślić, że zgodnie z motywem 63 RODO ochrona praw i wolności osób trzecich nie powinna „skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji". W kontekście prawa dostępu do danych Grupa Robocza wyraziła opinię, że rzadkie będą sytuacje, w których prawa i wolności innych osób byłyby nadrzędne wobec prawa dostępu do danych, a administratorzy nie powinni odmawiać osobom, których dane dotyczą, dostępu do ich danych osobowych, powołując się na przesłankę niekorzystnego wpływu na prawa i wolności innych[17].

W praktyce odpowiedź na pytanie, czy żądanie dostępu do danych lub żądanie przeniesienia danych może niekorzystnie wpływać na prawa i wolności innych osób, będzie wymagała każdorazowej oceny w oparciu o okoliczności konkretnego przypadku[18].

Choć przesłanka niekorzystnego wpływu na prawa i wolności innych brzmi tak samo w przypadku prawa dostępu i prawa do przenoszenia danych, wydaje się, że przy ocenie potencjalnego niekorzystnego wpływu należy brać pod uwagę charakter żądania. O ile żądanie przekazania kopii danych z profilu w sieci społecznościowej w ramach prawa dostępu wydaje się dopuszczalne (szczególnie biorąc pod uwagę, że dane osób trzecich są najprawdopodobniej znane żądającemu[19]), o tyle żądanie przeniesienia tych danych do innego usługodawcy budzi wątpliwości. Nie ma bowiem pewności, czy osoby trzecie, których dane są zawarte w profilu osoby składającej żądanie, wyraziłyby zgodę na przetwarzanie ich danych osobowych przez innego usługodawcę lub chęć zawarcia z nim umowy[20].

Wytyczne Grupy Roboczej dotyczące prawa do przenoszenia danych nie do końca rozwiewają powyższe wątpliwości. Jeśli chodzi o potencjalny negatywny wpływ na prawo do prywatności innej osoby, Grupa Robocza stwierdziła, że można o nim mówić, jeżeli przesłanie danych do innego administratora (nowego usługodawcy) uniemożliwia osobom trzecim korzystanie z ich praw związanych z przetwarzaniem danych osobowych. Rekomendowane jest też wdrożenie narzędzi umożliwiających osobom żądającym przekazania lub przeniesienia danych wybór danych, które chciałyby otrzymać lub przenieść do innego usługodawcy, a także wyłączenie spod żądania – gdzie to właściwe – danych innych osób[21]. Takie samo rozwiązanie mogłoby być zastosowane w stosunku do kopii danych otrzymywanej w ramach prawa dostępu do danych.

Ponadto, zgodnie z art. 20 ust. 3 RODO, prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Takie ograniczenie nie występuje w odniesieniu do prawa dostępu do danych.

Dodatkowe ograniczenia stosowania prawa dostępu i prawa przenoszalności mogą być nałożone na mocy prawa unijnego lub prawa państwa członkowskiego w oparciu o art. 23 RODO. Jednakże takie ewentualne ograniczenia – jako niewynikające bezpośrednio z ogólnego rozporządzenia – pozostają poza zakresem niniejszego artykułu.

Podsumowując, prawo dostępu i prawo przenoszalności mają taką samą przesłankę ograniczającą ich stosowanie w postaci niekorzystnego wpływu na prawa i wolności osób trzecich. Jednakże stosowanie tego kryterium ograniczającego może być różne w odniesieniu do każdego z praw, szczególnie w przypadku składania żądania przesłania danych bezpośrednio innemu administratorowi w ramach prawa przenoszalności. Wydaje się bowiem, że żądanie przesłania danych innemu usługodawcy może częściej powodować niekorzystny wpływ na prawa innych osób niż żądanie dostępu do danych. Ponadto w przypadku prawa przenoszalności przewidziano dodatkową przesłankę ograniczającą, tj. brak stosowania tego prawa przy przetwarzaniu niezbędnym do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, która nie występuje w odniesieniu do prawa dostępu do danych.

3. Zakres przekazywanych danych

W przypadku otrzymania żądania dostępu do danych administrator przekazuje osobie, której dane dotyczą, informacje o przetwarzaniu jej danych osobowych wskazane w art. 15 ust. 1 RODO, a także kopię tych danych. Wśród informacji o przetwarzaniu danych znajduje się m.in. cel przetwarzania danych, zakres przetwarzanych danych, informacje o odbiorcach danych, informacje o prawach przysługujących osobie, której dane dotyczą.

---

[16] Szerzej zob. *G. Malgieri*, Trade Secrets v Personal Data: a possible solution for balancing rights, International Data Privacy Law 2016, t. 6, Nr 2, s. 102.

[17] Wytyczne Grupy Roboczej Artykułu 29 z 3.10.2017 r. dotyczące zautomatyzowanego podejmowania decyzji i profilowania zgodnie z rozporządzeniem 2016/679 (ang. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*), Nr dokumentu WP 251, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47963 (dostęp z 30.11.2017 r.), s. 24.

[18] *E. Parry*, Subject Access and Data Portability, [w:] *R. Jay* (red.), Guide to the General Data Protection Regulation, Londyn 2017, s. 251.

[19] Jednym z kryteriów, które należy wziąć pod uwagę, jest to, czy dane osoby trzeciej są znane osobie żądającej dostępu do danych – zgodnie z Kodeksem postępowania dotyczącym żądań dostępu do danych (ang. *Subject access code of practice*) przygotowanym przez Komisarza ds. Informacji (ang. *Information Commissioner*, brytyjski organ nadzorczy do spraw ochrony danych osobowych), s. 39.

W Kodeksie znajdują się praktyczne wskazówki dotyczące odpowiadania na żądania dostępu do danych w sytuacji, gdy dane te zawierają też dane osobowe osoby innej niż żądający, https://ico.org.uk/media/for-organisations/documents/2014223/subject-access-code-of-practice.pdf (dostęp z 30.11.2017 r.).

[20] *B. Van der Auwermeulen*, How to attribute…, s. 60.

Jeśli chodzi o kopię danych przekazywanych w ramach prawa dostępu, art. 15 RODO nie przewiduje ograniczeń dotyczących zakresu tych danych. Co do zasady obowiązkiem administratora jest więc ujawnienie wszystkich danych o osobie, która składa żądanie dostępu, w tym danych zebranych przez administratora nie od osoby, której dane dotyczą. Ograniczenia w tym zakresie mogą jednak wynikać z opisanego wyżej niekorzystnego wpływu na prawa i wolności innych osób.

Natomiast prawo otrzymania danych w ramach prawa do przenoszenia danych, zgodnie z art. 20 ust. 1 RODO, jest ograniczone tylko do takich danych osobowych, które dotyczą osoby składającej żądanie i jednocześnie zostały przez nią dostarczone administratorowi. Takie ujęcie zakresu danych podlegających przenoszeniu może wynikać z genezy prawa do przenoszenia danych jako prawa mającego zastosowanie szczególnie w odniesieniu do sieci społecznościowych[22].

Należy w tym kontekście odnieść się do definicji „danych dostarczonych administratorowi" przedstawionej przez Grupę Roboczą w wytycznych dotyczących przenoszalności. Zgodnie z wytycznymi można dokonać podziału danych na trzy kategorie:

1) dane świadomie i aktywnie przekazywane przez osobę, której dane dotyczą (np. adres pocztowy);
2) dane wynikające z obserwacji działalności osoby, której dane dotyczą (np. dane surowe o zużyciu energii zbieranie przez inteligentne liczniki, dane o lokalizacji), oraz
3) dane wywiedzione lub wynikowe, wynikające z przeprowadzonej przez administratora analizy danych surowych lub profilowania (np. profil użytkownika, ocena zdolności kredytowej)[23].

W opinii Grupy Roboczej należy przyjąć szeroką definicję danych dostarczonych przez osobę, której dane dotyczą. Rzecznicy ochrony danych postulują, że w pojęciu tym powinny mieścić się dwie pierwsze z przedstawionych powyżej kategorii danych osobowych, tj. dane świadomie i aktywnie przekazywane przez osobę, której dane dotyczą, jak również dane zaobserwowane o tej osobie[24]. Takie podejście spotkało się z krytyką ze strony przedstawicieli przedsiębiorców[25], a także zgłoszeniem wątpliwości przez Komisję Europejską[26].

W ramach przygotowań do rozpoczęcia stosowania ogólnego rozporządzenia administratorzy podlegający obowiązkowi udostępniania danych w ramach prawa przenoszalności będą więc musieli określić zakres danych podlegających przenoszeniu i przygotować pod tym kątem swoje systemy informatyczne.

Podsumowując, zakres danych przekazywanych w ramach kopii danych na podstawie prawa dostępu jest szerszy niż w przypadku prawa do przenoszenia danych. Przenoszeniu nie podlegają bowiem dane wywnioskowane o osobie, której dane dotyczą, na podstawie danych przez nią dostarczonych lub o niej zaobserwowanych. Natomiast w ramach kopii danych uzyskiwanej na podstawie prawa dostępu do danych powinny się co do zasady znaleźć także dane wywnioskowane o osobie składającej żądanie dostępu (np. jej profil marketingowy oraz dane wykorzystane w celu przypisania jej do danego profilu lub do utworzenia profilu[27]).

4. Format przekazywania danych

W przypadku prawa dostępu do danych ogólne rozporządzenie nie przewiduje żadnego szczególnego formatu przekazywania danych. Jedynym wymogiem jest to, aby dane były czytelne dla osoby składającej żądanie. Dane mogą być przekazywane zarówno w formie papierowej, jak i elektronicznej, przy czym – zgodnie z art. 15 ust. 3 RODO – jeżeli żądanie otrzymania kopii danych jest składane drogą elektroniczną, zasadą jest udzielanie odpowiedzi powszechnie stosowaną drogą elektroniczną. W motywie 63 RODO administratorzy są też zachęcani do udostępnienia osobom, których dane dotyczą, systemu, który zapewniłby bezpośredni dostęp do ich danych osobowych. Nie ma jednak wymogów co do szczególnego elektronicznego formatu danych.

Natomiast w przypadku prawa do przenoszenia danych art. 20 ust. 1 RODO wprost wskazuje, że dane mają być udostępniane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Dodatkowe wyjaśnienia są zawarte w motywie 68 RODO, zgodnie z którym format powinien być interoperacyjny, przy czym nie nakłada to na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania. Grupa Robocza wskazała w wytycznych, że formaty przekazywania danych mogą różnić się w zależności od sektora, ale „zawsze należy wybierać je tak, aby osiągnąć cel bycia interpretowalnym [przez system informatyczny – dop. aut.] i zapewnić osobie, której dane dotyczą, duży stopień przenoszenia danych"[28]. Nie może to być format, z którego korzystanie wymagałoby zakupienia kosztownych licencji[29].

Należy zatem stwierdzić, że prawo dostępu różni się istotnie od prawa do przenoszenia danych w zakresie formatu przekazywania danych.

[21] Wytyczne Grupy Roboczej dotyczące prawa do przenoszenia danych…, s. 12–13.
[22] *E. Parry*, Subject Access…, s. 239.
[23] Wytyczne Grupy Roboczej dotyczące prawa do przenoszenia danych…, s. 10–11.
[24] *Ibidem*, s. 10.
[25] *W. Wiewiórowski*, Prawo do przenoszenia…, s. 29.
[26] *D. Meyer*, European Commission, experts uneasy over WP29 data portability interpretation, https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation/ (dostęp z 30.11.2017 r.).
[27] Wytyczne Grupy Roboczej dotyczące zautomatyzowanego podejmowania decyzji i profilowania…, s. 24.
[28] Wytyczne Grupy Roboczej dotyczące prawa do przenoszenia danych…, s. 19.
[29] *Ibidem*, s. 19.

5. Zakres obowiązków administratora

Na podstawie art. 15 RODO obowiązkiem administratora jest przekazanie osobie, której dane dotyczą, informacji, o których mowa w ust. 1 tego przepisu (m.in. o celu przetwarzania, zakresie danych, odbiorcach danych), a także kopii danych tej osoby. W związku z tym administrator powinien także dokonać oceny, czy przekazanie danych może niekorzystnie wpłynąć na prawa i wolności innych. Administrator powinien być przygotowany na to, aby w miesięcznym terminie wyznaczonym przez art. 12 ust. 3 RODO odpowiedzieć na żądanie dostępu do danych, w tym także drogą elektroniczną.

Natomiast w przypadku prawa do przenoszenia danych obowiązkiem administratora przekazującego (pierwotnego) dane jest udostępnienie osobie, której dane dotyczą, danych przez nią dostarczonych administratorowi w szczególnym formacie elektronicznym. Ponadto, przy uwzględnieniu technicznych możliwości, administrator pierwotny powinien – na żądanie osoby, której dane dotyczą – przekazać dane tej osoby bezpośrednio innemu administratorowi (otrzymującemu) wskazanemu przez tę osobę. Obowiązek taki nie występuje w przypadku prawa dostępu do danych. W związku z prawem przenoszalności na pierwotnym administratorze ciąży obowiązek przygotowania odpowiednich narzędzi, w tym przygotowania swoich systemów informatycznych, do przekazywania danych osobie składającej żądanie lub bezpośrednio wskazanemu przez nią wtórnemu administratorowi[30]. Ponadto administrator przekazujący dane powinien określić zakres przenoszonych danych, jako że spod prawa do przenoszenia wyłączone są dane wywnioskowane o konkretnej osobie[31]. Podobnie jak w przypadku prawa dostępu, administrator przekazujący powinien dokonać oceny, czy przeniesienie danych nie będzie niekorzystnie wpływać na prawa i wolności innych.

Należy też odnieść się pokrótce do obowiązków administratora otrzymującego dane w wyniku żądania przeniesienia danych. Zgodnie z wytycznymi Grupy Roboczej administrator otrzymujący powinien zapewnić, aby przekazane mu dane były adekwatne i nienadmierne w stosunku do celu nowego przetwarzania danych. Ponadto nowy administrator jest odpowiedzialny za zapewnienie zgodności z innymi zasadami przetwarzania danych określonymi w art. 5 RODO, np. z zasadą legalności i ograniczenia celu[32]. Administrator otrzymujący musi więc m.in. określić cel przetwarzania danych oraz podstawę prawną przetwarzania danych. W praktyce może to rodzić wiele trudności, ponieważ administrator przyjmujący nie ma możliwości uprzedniego sprawdzenia, czyje i jakie dane otrzyma[33]. W doktrynie podnosi się zatem, że administrator otrzymujący powinien mieć możliwość wyboru co do tego, które z otrzymanych danych przyjąć do przetwarzania, a które usunąć[34]. Innym obowiązkiem, który administrator otrzymujący powinien spełnić niedługo po otrzymaniu danych, jest obowiązek informacyjny.

Z powyższych rozważań wynika, że zakres obowiązków administratora w przypadku otrzymania żądania dostępu do danych jest dużo węższy niż w przypadku żądania przeniesienia danych. Administrator odpowiadający na żądanie dostępu jest zobowiązany jedynie do przekazania osobie, której dane dotyczą, określonych informacji dotyczących przetwarzania oraz kopii danych tej osoby. Natomiast w ramach prawa do przenoszenia danych administrator musi określić zakres przekazywanych danych, przekazać dane w szczególnym formacie lub nawet przekazać je bezpośrednio innemu administratorowi danych. Ponadto istotne obowiązki są nałożone na administratora otrzymującego dane w wyniku żądania przeniesienia danych, chociażby zapewnienie legalności przetwarzania danych.

Podsumowanie

Mimo że prawo do przenoszenia danych osobowych bywa określane jako rozszerzenie prawa dostępu do danych, między tymi uprawnieniami zachodzą istotne różnice. Po pierwsze, różne są przesłanki stosowania tych praw – prawo dostępu obowiązuje bez względu na podstawę prawną przetwarzania danych i sposób ich przetwarzania, natomiast z prawa do przenoszenia danych można korzystać tylko, jeżeli przetwarzanie odbywa się w sposób zautomatyzowany oraz jeżeli podstawą prawną przetwarzania danych jest zgoda lub umowa.

Po drugie, zakres danych przekazywanych w kopii danych w ramach prawa dostępu jest szerszy niż w przypadku prawa do przenoszenia danych. Przenoszeniu nie podlegają bowiem dane wywnioskowane o osobie, której dane dotyczą, a jedynie dane aktywnie dostarczone przez tę osobę lub o niej zaobserwowane. Natomiast w ramach kopii danych uzyskiwanej na podstawie prawa dostępu do danych powinny się co do zasady znaleźć wszystkie dane przetwarzane o osobie składającej żądanie, w tym dane uzyskane niebezpośrednio od tej osoby lub dane wywnioskowane o niej.

Kolejną różnicą jest format przekazywania danych. W przypadku prawa do przenoszenia danych musi to być ustrukturyzowany, powszechnie używany format nadający się do odczytu maszynowego, natomiast format nie ma znaczenia przy odpowiadaniu na żądanie dostępu do danych,

[30] *W. Wiewiórowski*, Prawo do przenoszenia…, s. 27.

[31] *M. Czerniawski*, Obowiązki administratora danych wynikające z prawa do przenoszenia danych, MoP 2017, Nr 20 (dodatek), s. 31.

[32] Wytyczne Grupy Roboczej dotyczące prawa do przenoszenia danych…, s. 7.

[33] *M. Czerniawski*, Obowiązki administratora…, s. 32.

[34] *W. Wiewiórowski*, Prawo do przenoszenia…, s. 28.

o ile przekazane informacje są czytelne dla osoby, której dane dotyczą.

Ponadto zakres obowiązków administratora w przypadku otrzymania żądania dostępu do danych jest węższy niż w przypadku żądania przeniesienia danych. Głównym obowiązkiem administratora odpowiadającego na żądanie dostępu jest przekazanie osobie, której dane dotyczą, określonych informacji dotyczących przetwarzania oraz kopii danych tej osoby. Natomiast w przypadku prawa do przenoszenia danych administrator przenoszący jest zobowiązany do określenia zakresu przekazywanych danych, przekazania danych w szczególnym formacie lub nawet do przekazania ich bezpośrednio innemu administratorowi danych. To właśnie ten drugi obowiązek – przesłanie danych bezpośrednio innemu administratorowi – stanowi najistotniejszą różnicę między prawem dostępu a prawem do przenoszenia danych. W ramach prawa dostępu istnieje bowiem jedynie wymóg przekazania danych osobie, której dane dotyczą. Natomiast w związku z przenoszeniem danych istotne obowiązki ciążą także na administratorze otrzymującym dane, w tym zapewnienie zgodności z zasadami przetwarzania danych.

Z kolei jeśli chodzi o podobieństwa między prawem dostępu a prawem przenoszalności, należy wskazać taką samą przesłankę ograniczającą ich stosowanie w postaci niekorzystnego wpływu na prawa i wolności osób trzecich. W praktyce może jednak okazać się, że to kryterium ograniczające będzie różnie stosowanie w odniesieniu do każdego z praw, szczególnie jeżeli żądaniem zgłaszanym w ramach prawa do przenoszenia danych jest bezpośrednie przesłanie danych innemu administratorowi.

Jak się wydaje, przy stosowaniu prawa do przenoszenia danych mogą pojawiać się różne trudności i wątpliwości. Administratorzy będą musieli ustalić zakres danych podlegających przenoszeniu przy uwzględnieniu podstawy prawnej przetwarzania danych (co może być szczególnie skomplikowane w sytuacji, gdy przetwarzanie odbywa się w oparciu o kilka podstaw) oraz tego, które dane należy uznać za dostarczone przez osobę składającą żądanie – gdzie należy odnieść się do wytycznych Grupy Roboczej. Ponadto konieczne będzie określenie formatu przekazywania danych. Warto też zastanowić się nad kryteriami ustalania, kiedy może zachodzić niekorzystny wpływ na prawa i wolności osób trzecich, oraz czy w związku z tym korzystanie z prawa do przenoszenia danych powinno być ograniczone. Wątpliwości będą też dotyczyły administratorów otrzymujących dane i będą oni musieli rozwiązać problemy związane z określeniem podstawy prawnej przetwarzania, celu przetwarzania lub też z minimalizacją danych.

Słowa kluczowe: dane osobowe, ochrona danych osobowych, ogólne rozporządzenie o ochronie danych, prawo dostępu, prawo do przenoszenia danych.

Right to data access and right of portability – comparing aim of regulation, scope and premises of applying

The aim of the present article is to determine the differences between the right to personal data access and the right of personal data portability based on the Regulation 2016/679 of 27 April 2016 of the European Parliament and the Council of the European Union on the protection of legal persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation). Firstly, the author presents the aim of the regulation of the right to data access and the right of data portability. Next, there is a comparative analysis regarding premises of applying each of these rights, limitation of applying them, scope of transferred data based on each right, form of transferring data, and also obligations of an administrator in case of making a request to use the right to data access or the right to data portability. Moreover, the article points to practical problems which may occur while replying to requests of people whose data concern using the abovementioned rights.

Key words: personal data, protection of personal data, general data protection regulation, right to access, right to transfer data.

Ochrona danych osobowych a Internet rzeczy, profilowanie i repersonalizacja danych

Paulina Leja[1]

Celem niniejszego opracowania jest opis Internetu rzeczy oraz repersonalizacji danych, a także skutków i zagrożeń, jakie ze sobą niosą w kontekście ochrony danych osobowych. Autorka odnosi przedstawiane kwestie do regulacji zawartych 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].

Uwagi wstępne

Internet to ogólnoświatowy system połączeń między komputerami. Obecnie, jak podaje największy portal społecznościowy Facebook, 3,2 mld ludzi ma dostęp do Internetu i każdego roku zwiększa się on o 200–300 tys. osób[3]. Jednocześnie Internet odnosi się nie tylko do przestrzeni adresów IP przydzielonych serwerom i hostom, lecz także staje się instrumentem pozwalającym gromadzić dane o swoich użytkownikach.

Takie zjawisko wymusza pytanie o granice i środki ochrony danych osobowych, które stają się przedmiotem coraz bardziej szczegółowych regulacji, również ustawodawcy unijnego. Pogodzić on musi konieczność ochrony podstawowych praw i wolności osób fizycznych[4] w związku z czynnościami przetwarzania danych oraz interesy podmiotów, które te dane gromadzą.

Najważniejszym aktem prawa unijnego dotyczącym poruszanego zagadnienia jest RODO. Rozporządzenie to weszło w życie 25.5.2016 r., lecz jego bezpośrednie stosowanie, we wszystkich państwach członkowskich, rozpocznie się od 25.5.2018 r.

Rozporządzenie 2016/679

W preambule RODO znaleźć możemy zapis: „Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych”[5]. Tym samym należy wywnioskować, że ustawodawca unijny świadomy jest postępującego rozwoju technologicznego, który niesie ze sobą zjawiska z zakresu zarządzania danymi osobowymi, często uregulowanymi prawnie w niewielkim stopniu, lub w ogóle. Wprowadzając pewne mechanizmy ochrony oraz normy celowościowe, ustawodawca stara się wyjść im naprzeciw. Odnosząc się do wybranych zjawisk występujących na skalę globalną, chciałabym przeprowadzić analizę zakresu ochrony, którą przyznaje europejska reforma o ochronie danych osobowych.

Zakresem zastosowania RODO jest przetwarzanie[6] danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz przetwarzanie danych w sposób inny niż zautomatyzowany, o ile stanowią lub mają stanowić część zbioru danych[7]. Tytułem wyjaśnienia, termin „dane osobowe” – zgodnie z definicją zawartą w art. 4 RODO – oznacza informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. „Możliwość” zidentyfikowania opiera się na identyfikacji bezpośredniej lub pośredniej. Dane te mogą być wyrażone w dowolny sposób[8]. Aby dane osobowe można było uznać za zbiór, konieczne jest ich uporządkowanie według określonych kryteriów[9]. Kluczowe jest posiadania przez zbiór odpowiedniej struktury, co nie oznacza jednak uporządkowania poszczególnych elementów, ale jedynie ich dostępność[10].

[1] Autorka jest studentką prawa na Wydziale Prawa Administracji i Ekonomii Uniwersytetu Wrocławskiego.

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

[3] Zob. http://www.computerworld.pl/news/404591/Dostep-do-Internetu-ma-juz-3-2-mld-mieszkancow-Ziemi.html (dostęp z 30.3.2017 r.).

[4] Zob. art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (Dz.Urz. UE z C 2016 r. Nr 202, s. 1); art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE C z 2012 r. Nr 326, s. 1).

[5] Zob. motyw 6 preambuły RODO.

[6] Więcej o przetwarzaniu zob. *P. Carey*, Data Protection, Oxford 2004, s. 20.

[7] *D. Wociór*, [w:] *D. Wociór* (red.), Ochrona danych osobowych i informacji niejawnych z uwzględnieniem rozporządzenia unijnego, Warszawa 2016, s. 5.

[8] *J. Barta*, *P. Fajgielski*, *R. Markiewicz*, Ochrona danych osobowych. Komentarz, Warszawa 2004, s. 391.

[9] *P. Kowalik*, [w:] *D. Wociór* (red.), Ochrona danych osobowych…, s. 45–46.

[10] *P. Fajgielski*, Ochrona danych osobowych w telekomunikacji – aspekty prawne, Lublin 2003, s. 47.

W RODO zawarto również normę traktującą o tym, że „osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi". Regulacja ta wraz z art. 6 – dającym legitymację legalności przetwarzania – stanowić będzie kanwę poniższych rozważań dotyczących wybranych zjawisk internetowych. Artykuł 6 RODO zawiera enumeratywną listę, z której podmiot musi spełniać co najmniej jeden wymóg, aby działania w zakresie przetwarzania danych osobowych były legalne. Mowa tu o:

1) zgodzie podmiotu na przetwarzanie danych osobowych;
2) niezbędności przetwarzania w celu wykonania umowy lub podjęcia działań przed zawarciem umowy, na żądanie osoby, której dane dotyczą;
3) niezbędności do wykonania obowiązków ciążących na administratorze danych;
4) niezbędności do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5) niezbędności do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
6) niezbędności do celów prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z tym że zastrzeżone są wyjątki, tj. występowanie interesów lub podstawowych praw i wolności osoby, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów, które chce realizować administrator lub osoba trzecia, w szczególności kiedy dane dotyczą dziecka. Prawnie realizowane interesy muszą mieć podstawy w prawie unijnym lub prawie państwa członkowskiego, któremu podlega administrator.

W kontekście tych przesłanek oraz norm celowościowych zawartych w preambule RODO, chciałabym ocenić legalność oraz wskazać potencjalne zagrożenia, które powstały w obecnym stanie prawnym, w związku z wybranymi zjawiskami mającymi miejsce w Internecie, a w szczególności: Internetem przedmiotów i repersonalizacją danych.

Internet przedmiotów

Internet przedmiotów nazywany jest również Internetem rzeczy. W periodyku Forbes ukazał się artykuł[11], w którym *P. Prajsnar* – ekspert ds. analityki Big Data – wskazuje, że „wbrew pozorom Internet rzeczy wcale nie jest Internetem »rzeczy«, lecz danych. Gdyby nie dane, które stanowią paliwo IoT[12], byłby on tylko fabryką elektrośmieci". W najprostszym ujęciu Internet przedmiotów to zespół rozwiązań umożliwiający osobom i przedmiotom łączenie się poprzez sieć z innymi dowolnymi ludźmi lub przedmiotami, niezależnie od czasu czy miejsca[13]. W nieco szerszym ujęciu należy dodać, że chodzi o globalną infrastrukturę, w której rzeczy otrzymują jednostkowe identyfikatory, dzięki którym możliwe jest przesyłanie i identyfikacja danych, takich jak np. czas, lokalizacja, ruch, wilgoć, tętno, które pozwalają na współpracę z innymi systemami. Internet of Things wykorzystuje technologie, takie jak chmura[14], czyli dzięki mocom obliczeniowym serwerów[15] przetwarzane są dane z przedmiotów zaprojektowanych w celu bycia podłączonym do Internetu, lub chip RFID[16] (ang. *Radio-frequency identification*), który umożliwia przesyłanie danych za pomocą fal radiowych.

Przykłady zastosowania Internetu przedmiotów można dostrzec chociażby w transporcie (np. w możliwości śledzenia lotów[17]), logistyce (np. dzięki viatrack[18]) czy zarządzaniu infrastrukturą miejską[19]. Śledzenie aktywności pracowników czy przedmiotów w przemyśle jest jedną z wielu możliwości IoT, które zamiast na skalę masową, w ramach decyzji pracodawcy coraz częściej znajduje zastosowanie w indywidualnych przypadkach.

Użytkownicy smartfonów mają już możliwość pobrania na swój telefon aplikacji, które zbierają wiele szczegółów o naszej osobie. Przykładowo jedną grupę stanowią aplikacje dotyczące naszego zdrowia, a drugą – aplikację do zarządzania naszym domem, czyli służące automatyce domowej (tzw. *smart home*).

Urządzenia z zakresu ochrony zdrowia[20] (*quantifiedself*) wykorzystują możliwości smartfonów lub działają, jeżeli umocuje się je na ubraniu lub na ciele. Zaliczają się do nich wszelkiego rodzaju analizatory ciała (tzw. *Body trackers*), które mogą mierzyć jakość snu (np. *SleepBetter Runtastic*), liczbę kroków (np. *Fitbit*), analizować bieg (np. *runtastic Bieganie i Fitness),* temperaturę (*Body Temperature*). Kolejnym krokiem w rozwoju urządzeń z zakresu zdrowia jest mierzenie tętna (*HeartRate Monitor*) czy ilości składników mineralnych w ciele (*Vitastiq*)[21]. Rozwija się bowiem rynek osobistych czujników, który pozwala z jednej strony

[11] Zob. http://www.forbes.pl/czym-jest-internet-rzeczy-,artykuly,195983,1,1.html (dostęp z 30.3.2017 r.).

[12] IoT (ang. *Internet of Things*) – Internet rzeczy.

[13] *O. Vermesan*, *P. Friess*, Internet of Things Strategic Research Roadmap, Bruksela 2011, s. 12.

[14] *R. Surowiec*, Dane osobowe w chmurach, Rzeczpospolita 2011, Nr 168, s. 23, dostępne również: http://www.rp.pl/artykul/690616-Dane-osobowe--w-chmurach.html (dostęp z 27.3.2017 r.).

[15] *G. Santucci*, Towards Connectobjectome: The age when the totality of all objects become conneted, [w:] *I.G. Smith* (red.), Internet of Things, Halifax 2012, s. 7–11.

[16] *S. Spikermann*, The RFID PIA – developed by industry agreed by regulators, [w:] *D. Wright, P. De Hert* (red.), Privacy Impact Assesment, Berlin––Heidelberg–Nowy Jork 2012, s. 1–22.

[17] Zob. np. https://www.esky.pl/radar; http://lotradar.pl/ (dostęp z 30.3.2017 r.).

[18] Zob. np. http://www.viatrack.pl/index.php/zastosowania/duze-floty.html (dostęp z 30.3.2017 r.).

[19] Zob. aplikację: impk, http://pasazer.mpk.wroc.pl/jak-jezdzimy/mapa--pozycji-pojazdow (dostęp z 30.3.2017 r.).

[20] Więcej o aplikacjach w zakresie ochrony zdrowia: *E.M. Kwiatkowska,* Internet rzeczy. Czy będą nas leczyć komputery?, Internetowy Kwartalnik Antymonopolowy i Regulacyjny 2016, Nr 5, s. 25–27.

[21] *E. Mucha*, Technologie biometryczne, Przegląd Pololicyjny 2015, Nr 2, s. 190–203.

coraz dogłębniej poznać swoje ciało, jego funkcje i odruchy, a z drugiej strony kreuje coraz bardziej wrażliwe dane[22]. Część tych aplikacji niejako „przemyca" zgodę na publikowanie tych danych na portalach społecznościowych lub wymaga do ściągnięcia aplikacji dostępu do dokładnej lokalizacji urządzenia[23]. Natomiast wejście w posiadanie informacji o lokalizacji urządzenia w połączeniu ze zbieranymi danymi pozwala na niemal bezbłędną identyfikację użytkownika. Wydaje się, że regulacja unijna, mimo postulatów o szczególną ochronę danych wrażliwych, nie wdrożyła rozwiązań gwarantujących szczególną ochronę. Pozostawienie tego w gestii państw członkowskich umożliwia natomiast występowanie zjawiska *race to the bottom*[24], które jest niekorzystne dla użytkowników.

Urządzenia z zakresu „*smart home*" pozwalają, aby użytkownik „kontrolował wszystkie urządzenia w domu, od oświetlenia, przez rolety, po wentylację i ogrzewanie. Masz możliwość sterowania z każdego miejsca w budynku i poza nim"[25]– jak reklamuje się jeden z producentów rozwiązań z tego zakresu. Jednocześnie podaje on na swojej stronie bardzo przekonujące dane: 12% mniej zużycia wody rocznie, 24% mniej zużycia energii rocznie. Jednak fakt posiadania tych danych wiąże się z niczym innym jak ze zbieraniem i przetwarzaniem danych o użytkownikach swoich rozwiązań.

Rozważania dotyczące ryzyka dla ochrony prywatności i ochrony danych osobowych rozpocząć należy od kwestii legalności tych zjawisk. Użytkownik, który pobiera aplikację bądź synchronizuje dany czujnik ze swoim smartfonem, najczęściej spełnia chociażby jedną przesłankę, która legalizuje przetwarzanie danych przez twórców aplikacji. Z jednej strony warunkiem koniecznym do pobrania aplikacji jest wyrażenie zgody, a z drugiej strony w pewną wątpliwość poddać można, czy zgoda ta jest świadoma – czy pozwala użytkownikowi pozyskać wiedzę, na czyją rzecz udziela podmiotowej zgody i w jakim celu oraz jakie konkretnie dane będą przetwarzane[26]. Ponadto zgoda[27], jak podkreślają przepisy RODO, powinna być dobrowolna, konkretna, świadoma i jednoznaczna, co w przypadku pobierania aplikacji jest raczej stanem postulatywnym, odbiegającym od rzeczywistości.

Nieco dalej idącym, acz znacznie bardziej spektakularnym zagrożeniem, które nasuwa się przy rozważaniu tych zjawisk, zwłaszcza w przypadku rozwiązań z zakresu „smart home" – jest tzw. atak hakerski. Odzwierciedlenie tych lęków zostało zobrazowane już w popkulturze – np. w drugim sezonie serialu pt. Mr. Robot grupa hakerów, włamując się do systemu i ustawiając ekstremalne parametry w zakresie temperatury oraz aktywując wszelkie urządzenia elektryczne, wypędziła mieszkankę z jej własnego domu[28]. Potencjalne ryzyko związane z gromadzeniem i przetwarzania takich danych ma zatem o wiele dalej idące konsekwencje niż brak kontroli.

W. Wiewiórowski[29] wskazuje, że jako potencjalne ryzyka z tymi zjawiskami możemy uznać:

1) tworzenie i ujawnianie wzorców zachowań użytkowników[30];
2) oceny zachowania użytkownika, tworzenie wzorca normalności oraz stały nadzór mieszczenia się w normach[31];
3) wyciąganie negatywnych konsekwencji ze względu na odbieganie od normy, np. jeżeli zwiększamy stopniowo jasność w swoim domu – oznaczać to może, że psuje nam się wzrok, a taką informację można udostępnić potencjalnym reklamodawcom lub ubezpieczycielowi;
4) brak możliwości udzielania świadomej i dobrowolnej zgody na przesyłanie danych osobowych (wiele osób utożsamia wprowadzenie urządzeń w tryb offline z brakiem przesyłania danych. Wiele urządzeń zapewnia rejestrowanie i przechowywanie danych, które zostają przekazane administratorowi w momencie włączenia do sieci);
5) brak kontroli nad generowanymi danymi – związane głównie z wbudowanymi mikrofonami, chipami, czujnikami, które funkcjonują w sposób niezrozumiały dla użytkowników;
6) automatyczne podejmowanie decyzji przez urządzenia otrzymujące dane od nas;
7) długoterminowe przechowywanie danych;
8) repersonalizacja danych (omówiona poniżej).

Powołując się ponownie na wnioski *W. Wiewiórowskiego*, nie da się nie zgodzić, że kwestie bezpieczeństwa urządzenia oraz komunikacji pomiędzy urządzeniami są w konflikcie z interesami producentów, twórców aplikacji, sponsorów urządzeń lub aplikacji. Dane osobowe pozwalające na tworzenie wzorców, badanie nawyków i zachowań czy na reperso-

[22] *K. Krassowski*, Identyfikacja biometryczna – nasz przyjaciel czy wróg?, Studia Prawnoustrojowe, t. 23, 2014, s. 189–201.

[23] *R. Surowiec*, Dane osobowe…

[24] Zjawisko *race to the bottom* wyjaśnione zostało w piśmie *The Economist* http://www.economist.com/blogs/freeexchange/2013/11/labour-standards, jak również na blogu The Broker, http://www.thebrokeronline.eu/Blogs/Inclusive-Economy-Europe/The-race-to-the-bottom-explained (dostęp z 10.6.2017 r.).

[25] Hasło reklamowe: https://ampio.com.pl/ (dostęp z 30.3.2017 r.).

[26] *A. Dmochowska*, Unijna reforma przepisów ochrony danych osobowych – analiza zmian, Warszawa 2016, s. 19.

[27] Szerzej zob. *J. Kosuniak*, Odwoływalność zgody na przetwarzanie danych – doświadczenia przedsiębiorcy telekomunikacyjnego, [w:] *A. Mednis* (red.), Prywatność a ekonomia. Ochrona danych osobowych w obrocie prawnym, Warszawa 2013, s. 73–79.

[28] Zob. https://qz.com/733269/mr-robot-played-to-our-worst-technology-fears-with-a-mini-horror-movie-about-a-hacked-smart-home/ (dostęp z 30.3.2017 r.).

[29] *W.R. Wiewiórowski*, Ochrona danych osobowych w świecie Internetu przedmiotów, Dodatek do MoP 2014, Nr 9, s. 9.

[30] O tym, jak przejść od profilu cyfrowego do opisu osoby, pisze: *A. Roosendaal*, Digital Personae and Digital Profile as Representations of Individuals, [w:] *M. Bezzi, P. Duquenoy, S. Fischer-Huebner, M. Hansen*, *G. Zhang* (red.), Privacy and Identity Management for Life, Berlin–Heidelberg–Nowy Jork 2010, s. 227–223.

[31] *A. Welsh*, The Identity Theft Protection Guide, Nowy Jork 2004, s. 236–258.

nalizację stają się coraz cenniejszym towarem pozwalającym na wpływanie na zachowanie mas, a tym samym na zyski. W RODO ustanowiono wysokie standardy dotyczące zgody na przetwarzanie danych osobowych. Istotny jest także fakt, że przetwarzanie danych osobowych musi korespondować z wyrażoną zgodą również w aspekcie celowościowym[32]. Niemniej wydawać by się mogło, że system weryfikacji faktycznej korelacji między przetwarzaniem a celem producentów jest utrudniony ze względu na generalność tej normy. Wiele zagrożeń wiążących się ze zbieraniem danych pokazuje, jak daleko idące mogą być konsekwencje dostępu do danych użytkowników – mogą one dotyczyć płaszczyzny zarówno społecznej, jak i finansowej. Użytkownicy w pierwszej kolejności mogą być kategoryzowani jako atrakcyjni konsumenci, a w dalszej wiązać się to może z umożliwieniem dostępu do określonych dóbr, tworząc nową kategorię dóbr luksusowych w oparciu o schematy zachowań. Może to wykreować nowy wymiar kapitalizmu oraz konsumpcji opartej na ograniczeniach zamiast na dostępie. Tymczasem RODO wydaje się nie poruszać tych kwestii, ustanawiając jedynie normy umożliwiające dążenie do stanu postulatywnego, jakim jest ochrona jednostek. Przy ogromie potencjału korzyści ekonomicznych takie regulacje mogą okazać się niewystarczające.

Repersonalizacja danych

Repersonalizacja danych łączy się ściśle z tematem Internetu przedmiotów. Polega ona bowiem na tworzeniu z pozoru anonimowych zbiorów danych osobowych, które jednak przy stałym nadzorze nad osobą mogą prowadzić do tworzenia profili umożliwiających jej identyfikację[33]. Oznacza to, że dane, które zostały zebrane w czasie korzystania z Internetu rzeczy, mogą być przetwarzane w ogromnych zbiorach, a następnie odszyfrowane i przyporządkowane jednostkom.

Punkt 30 preambuły RODO zawiera zapis: „osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawieniem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i identyfikowania tych osób".

Istnieją dwa podstawowe podejścia do tworzenia profili użytkowników, a mianowicie:

– profile predykcyjne[34] – tworzy się w drodze wnioskowania na podstawie obserwacji indywidualnego i zbiorowego zachowania użytkowników w czasie, w szczególności przez monitorowanie odwiedzanych stron oraz reklam, które użytkownik wyświetla lub na które klika. Bazując na tych informacjach próbuje się przewidzieć zachowanie takiej osoby;
– profile jawne – zestawy informacji dotyczące osób zebrane z różnych źródeł. Tworzy się na podstawie danych osobowych przekazywanych w ramach usługi sieciowej przez same osoby, których dane dotyczą, np. podczas rejestracji. Wspomniane metody można łączyć. Ponadto profile predykcyjne mogą stać się jawne później – kiedy osoba, której dotyczą dane, utworzy dane logowania dla danej strony internetowej[35].

Mimo że dane takie najczęściej są poddawane procesowi anonimizacji, wskazać należy potencjalne skutki repersonalizowania danych. *Y.-A. de Montjoye* wraz z grupą naukowców z MIT-u (*A. „Sandy" Pentland, L. Radaelli* i *V.K. Singh*)[36] przez trzy miesiące przyglądali się takim anonimizowanym danym dotyczącym kart kredytowych 1,1 mln osób z nieujawnionego kraju. W danych nie było ani nazwisk posiadaczy kart, ani informacji o kontach bankowych, z którymi karty są powiązane. Naukowcy chcieli sprawdzić, co można powiedzieć o ludziach na podstawie takich właśnie informacji. Okazało się, że całkiem sporo. Uczonym wystarczyły cztery różne fragmenty informacji, by zidentyfikować 90% posiadaczy kart płatniczych. Wykazano, że znajomość ceny produktu zwiększa ryzyko reidentyfikacji o 22%[37]. Wystarczyło połączyć dane z serwisów społecznościowych, na których użytkownicy oznaczali swoją obecność w restauracji lub chwalili się nowym ubraniem, z sumami transakcji z pobliskich miejsc, aby ustalić, kto jest posiadaczem karty płatniczej[38]. W innym eksperymencie *Y.-A. de Montjoye* wraz z *C. Hidalgo*, *V. Blondelem* i *M. Verleysenem* użyli 15-miesięcznych danych z 1,5 mln osób, aby pokazać, że cztery punkty – przybliżone miejsca i godziny – wystarczą do identyfikacji 95% osób fizycznych w bazie danych dotyczących mobilności. Opracowali formułę służącą do oszacowania niepowtarzalności

[32] Jak również legalności, celowości, adekwatności, czasowości, integralności i poufności danych. Szerzej zob. *A. Dmochowska*, Unijna reforma…, s. 11–17.

[33] *W.R. Wiewiórski*, Ochrona danych osobowych…, s. 10.

[34] Zob. http://www.computerworld.pl/news/395648/VII-Forum-Bezpieczenstwa-i-Audytu-IT-GIODO-o-analizie-predykcyjnej-i-profilowaniu.html (dostęp z 30.3.2017 r.).

[35] Zob. Opinia Grupy art. 29 Nr 2/2010 w sprawie internetowej reklamy behawioralnej przyjęta 22.6.2010 r., pkt 2.3., s. 8, https://piu.org.pl/public/upload/ibrowser/seminaria/Jakosc%20Danych%20IX/GIODO_W-Wiewiorowski_ZASADA_CELIOWOSCI_DATA_MINING.pdf, slajd 16 (dostęp z 30.3.2017 r.). O procesie zbierania danych o osobach fizycznych również: *K. Markowski,* Prywatność czy rzetelność obrotu gospodarczego?, [w:] *A. Mednis* (red.), Prywatność a ekonomia. Ochrona danych osobowych w obrocie prawnym, Warszawa 2013, s. 41–46.

[36] Zob. http://demontjoye.com/projects.html – strona *Y.-A. de Montjoye*; project: Unique in the Shopping Mall: Reidentifying credit card data (dostęp z 30.3.2017 r.).

[37] Zob. https://www.media.mit.edu/projects/on-the-reidentifiability-of-credit-card-metadata/overview/ (dostęp z 30.3.2017 r.).

[38] Zob. http://kopalniawiedzy.pl/dane-osobowe-karta-platnicza-anonimowosc,21822 (dostęp z 30.3.2017 r.).

śladów mobilności człowieka i wskazali, że nawet wtedy gdy dane są niskiej jakości, nie zapewniają one anonimowości[39].

Inni badacze – z University of Birmigham – dowiedli, że dzięki danym GPS zebranym w New Hampshire i taksówkach San Francisco są w stanie rozpoznać niemal 100% posiadaczy smartfonów[40].

W opinii 5/2014 w sprawie technik anonimizacji przyjętej przez Grupę Roboczą 10.4.2014 r. wskazuje się, że „wymagane jest zachowanie szczególnej ostrożności w postępowaniu ze zanonimizowanymi informacjami, zwłaszcza w każdym przypadku, gdy takie informacje wykorzystuje się (często w połączeniu z innymi danymi) do celów podejmowania decyzji". Jednocześnie w rozdziale pt. Analiza techniczna, niezawodność technologii i typowe błędy wskazuje się następujące zagrożenia:

„1) wyodrębnienie, które oznacza możliwość wydzielenia niektórych lub wszystkich zapisów identyfikujących określoną osobę fizyczną w zbiorze danych;
2) możliwość tworzenia powiązań, czyli zdolność do powiązania co najmniej dwóch zapisów dotyczących jednej osoby lub grupy osób, których dane dotyczą (w tej samej bazie danych lub w dwóch różnych bazach danych). Jeżeli atakujący może ustalić (np. w drodze analizy korelacji), że dwa zapisy przypisane są tej samej grupie osób fizycznych, ale nie może wyodrębnić poszczególnych osób w tej grupie, dana technika zapewnia ochronę przed wyodrębnieniem, ale nie przed możliwością tworzenia powiązań;
3) wnioskowanie, czyli możliwość wydedukowania ze znacznym prawdopodobieństwem wartości danego atrybutu z wartości zbioru innych atrybutów".

Grupa Robocza, podobnie jak *W. Wiewiórowski* w przypadku zagrożeń wynikających z Internetu rzeczy, wskazuje wiele konsekwencji wynikających ze zjawiska repersonalizacji. Identyfikacja osoby w grupie stanowi podstawę do określenia wzorców jej zachowania. Wskazuje również, że wdrażanie systemów zabezpieczeń, które chronią jedynie częściowo rekordy znajdujące się w bazach danych, doprowadzić może do dogłębnej analizy śladów pozostawianych przez użytkowników sieci[41].

Rozporządzenie 2016/679 nie reguluje *stricto* repersonalizacji danych. Natomiast w motywie 26 preambuły znaleźć można zapis: „zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować".

Zapis ten daje podstawę do stosowania zasad legalizacji danych, które mają być anonimizowane, a później repersonalizowane. Norma ta zwraca uwagę na konieczność wzięcia pod uwagę zarówno postępu technologicznego, jaki nastąpił do momentu identyfikowania, jak i dostępną technikę[42]. Skutkiem tego regulacja ta buduje standardy i zakres ochrony niezależne od wiedzy prawodawcy, przenosząc ciężar potencjalnego dowodu w zakresie wiedzy na osoby depersonalizujące dane. Z drugiej strony, ze względu na dynamikę zmian oraz fakt, że informacje o sposobach depersonalizacji nie są powszechne, nieostrość regulacji zaciera granice ochrony.

Warto również wskazać, że repersonalizacja danych niesie ze sobą wiele różnych zagrożeń, niezależnie czy dane zostaną zdeanimizowane czy też nie. Obserwując pewne wzorce zachowań ludzkich, przedsiębiorcy mogą wykorzystywać nawyki ludzi, np. w sposobie odbierania treści ze stron internetowych, aby uniemożliwić lub znacznie utrudnić użytkownikom Internetu zapoznawanie się z konkretnymi treściami, poprzez odpowiednie rozmieszczenie informacji. Tworzenie wzorców zachowań pewnych grup społecznych może także doprowadzić do ograniczania możliwości wyboru osób fizycznych w ramach ich decyzji konsumenckich wyłącznie do ich dotychczasowych decyzji. Użytkownicy mogą być klasyfikowani, w zależności od swoich wyborów, przyporządkowani do konkretnych grup opartych na zbiorowych trendach i zamykani w świecie definiowanym, przez wybory z konkretnego, badanego odcinka czasu. Odpowiedzią na

[39] The privacy bounds of human mobility, http://demontjoye.com/projects.html (dostęp z 30.3.2017 r.).

[40] Zob. https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-015-0049-x oraz http://dl.acm.org/citation.cfm?doid=2426656.2426666 (dostęp z 30.3.2017 r.).

[41] Tzw. *browse fingerprints* czyli odciski palców w sieci, polegająca na anonimowym identyfikowaniu przeglądarki internetowej z dokładnością do 94%, szeroko można poczytać na technicznych stronach internetowych, np. https://github.com/Valve/fingerprintjs (dostęp z 18.11.2017 r.).

[42] Obecnie powstały już programy służące do depersonalizacji danych, dedykowane dla programów obsługujących migrację danych, np. http://ssisctc.codeplex.com/, dla programu SSIS (dostęp z 2.6.2017 r.).

anomalię użytkownika może być natomiast deanonimizacja danych, a następnie automatyczna korekta prezentowanych jednostce treści, dla danej jednostki, w oparciu o jej konkretne, zdeanimizowane już zachowania.

Rozporządzenie 2016/679 a Internet rzeczy i repersonalizacja danych

Powyżej opisane zostały potencjalne skutki oraz zagrożenia związane z operacjami na danych osobowych, które obiegają od klasycznego rozumienia ich przetwarzania. Rozporządzenie 2016/679 w motywie 39 i 4 preambuły przewiduje, że wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne oraz że przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Faktem jednak jest, że zjawisko Internetu rzeczy i repersonalizacji danych nie zostało bezpośrednio uregulowane w RODO, stąd ustalenie granic legalności nasuwać może pewne problemy. Jak słusznie wskazuje *D. Lubasz*, RODO celowo nie definiuje nawet samego przetwarzania danych w sposób częściowo lub całkowicie zautomatyzowanych, ze względu na wprowadzenie neutralności technologicznej[43]. Właśnie gwałtowny postęp technologiczny wymusił wprowadzenie wielu klauzul generalnych, które pozwalają znaleźć punkty odniesienia do legalnych aspektów omawianych zjawisk, które interpretować trzeba z uwzględnieniem celów ustawodawcy. Same zapisy jednak nie dają jasnych odpowiedzi, jakie zabezpieczenia należy wprowadzić, żeby chronić jednostki, które nieświadomie mogą stać się podmiotem operacji na danych[44].

Ochrona osób możliwa jest przy konkretnym określeniu zagrożeń. Rozporządzenie 2016/679 odnosi się do ryzyka naruszenia praw lub wolności osób. W motywach od 75 do 81 preambuły możemy znaleźć szereg zapisów dotyczących tego zakresu. Ustawodawca unijny wskazuje, że naruszenie takie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych. Za kluczowy w związku z przetwarzaniem danych osobowych wskazać należy motyw 75 preambuły, który zawiera katalog otwarty zagrożeń. Zawiera on w szczególności skutki, kiedy „przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych". Warto również dodać, że RODO wprowadza również definicję legalną naruszenia ochrony danych osobowych, którą należy rozumieć jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych[45].

Stworzenie tego katalogu oraz definicji konieczne było w celu nałożenia na osoby odpowiedzialne za przetwarzanie danych obowiązku oceny skutków oraz minimalizowania ryzyka. Jako kluczowe należy wskazać wdrożenie odpowiednich środków technicznych i organizacyjnych, RODO jednak przewiduje wiele innych wymogów[16] koniecznych do zastosowania w celu przetwarzania danych osobowych oraz w przypadku naruszeń[47]. Odpowiedzialność za przetwarzanie zgodne z prawem, rzetelne i przejrzyste dla osoby, której dane dotyczą[48], możliwe jest przy pełnym zrozumieniu mechanizmów funkcjonowania przetwarzania danych dla osób, których dane dotyczą. Potwierdza to ustawodawca, który wskazuje, że w motywie 60 preambuły zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba,

[43] *E. Bielak-Jomaa, D. Lubasz* (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2017, *passim*.

[44] Konsumenci często nie zdają sobie sprawy z potencjalnych zagrożeń związanych z przetwarzaniem danych osobowych. Powstał już sklep, w których płacić można danymi osobowymi: https://www.engadget.com/2017/09/07/data-dollar-store-london-ben-eine/czy https://www.lonelyplanet.com/news/2017/08/31/pay-personal-data-london-street-art-pop/(dostęp z 19.11.2017 r.). Zjawisku przyjrzał się już *P. Hustinx* w opinii z 26.3.2014 r., https://edps.europa.eu/sites/edp/files/publication/14-07-14_ph_for_ev_online_en.pdf (dostęp z 19.11.2017 r.). O tworzeniu waluty z danych osobowych zob. np.: https://www.kaspersky.com/about/press-releases/2017_data-dollar-the-new-currency-based-on-the-value-of-personal-data (dostęp z 19.11.2017 r.).

[45] Definicja legalna „naruszenia danych osobowych" znajduje się w art. 4 pkt 12 RODO.

[46] Szerzej *D. Lubacz*, Europejska reforma ochrony danych osobowych – nowe obowiązki administratorów w ogólnym rozporządzeniu o ochronie danych, [w:] *E. Bielak-Jomaa*, *D. Lubasz* (red.), Polska i europejska reforma ochrony danych osobowych, Warszawa 2016, s. 63–85.

[47] Regulacja zawarta jest w art. 34–36 RODO.

[48] Zasady dotyczące przetwarzania danych osobowych znajdują się w art. 5 RODO – szerzej np. *B. Kaczmarek-Templin,* Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia, [w:] *E. Bielak-Jomaa, D. Lubasz* (red.), Polska i europejska reforma…, s. 102–126.

której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Tym samym ustawodawca stwarza podstawy do uświadomienia jednostek o operacjach, które przeprowadza się na ich danych. Motyw 60 preambuły RODO stanowi, że każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Analiza tego zapisu wraz z regulacją z motywu 59 preambuły stanowiącym, że należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania i, gdy ma to zastosowanie, bezpłatnego uzyskiwania w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu, daje obraz ram, jakie ustawodawca przewidział na ochronę jednostek[49]. Tak sformułowane normy dotyczące częstotliwości oraz łatwości dostępu i sprostowania, usunięcia czy sprzeciwu dotyczących danych osobowych, a także konieczność wprowadzenia procedur wydawać się mogą wystarczające w przypadku aspektów ujętych w RODO (np. przetwarzania danych w celach marketingowych). Natomiast w przypadku zbierania danych podczas korzystania z Internetu rzeczy oraz repersonalizacji danych, których skutkiem może być stworzenie dokładnych profili dotyczących niemalże każdego aspektu życia jednostki, można postulować o nieco dalej idące, bardziej szczególne zapisy. O wiele łatwiej w przypadku tych zjawisk o naruszenie ochrony danych osobowych, a wykorzystanie danych zgromadzonych w ten sposób może być o wiele korzystniejsze finansowo[50].

Postulat *delege ferenda* dla ustawodawcy unijnego

Ewolucja technologiczna, w tym rozwój Internetu wiąże się z licznymi wyzwaniami oraz konfliktami równorzędnych dóbr. Gromadzenie danych oraz przetwarzanie ich na szeroką skalę przez przedsiębiorców doprowadzić może do pewnych zmian w zakresie stosunków społeczno-gospodarczych, które wpłyną bezpośrednio na każdą jednostkę. Zgoda ustawodawcy na pewne zachowania przedsiębiorców oraz innych podmiotów czerpiących z przetwarzania danych osobowych korzyści finansowe wiąże się w pewnym stopniu z erozją praw człowieka, praw jednostek. Warto jednak wprowadzać rozwiązania, które stanowią kompromis pomiędzy interesami zarówno osób fizycznych, jak i przedsiębiorców. Wydawać by się mogło, że pewnym rozwiązaniem pozwalającym z jednej strony na rozwój działalności gospodarczej, a z drugiej na ochronę jednostek jest wprowadzenie pewnej formy kontroli społecznej sprawowanej wyłącznie przez zainteresowane osoby. Pełen dostęp w postaci *real time*[51] podglądu do przekazywanych konkretnym przedsiębiorcom informacji oraz sposób przetwarzania danych (np. przekazywanie je podmiotom trzecim) wraz z możliwością usunięcia części z nich może stanowić odpowiedź na pewien zakres przedstawionych problemów. Z jednej strony pozwoliłoby to zbudować świadomość społeczną oraz osób fizycznych o tym, że dane są gromadzone, a zgoda wcześniej wyrażona wiązałaby się z o wiele dalej idącą wiedzą o samym przetwarzaniu danych niż tą, która idzie za np. zaznaczeniem wymaganego okienka zgody w formularzach internetowych czy przy instalowaniu aplikacji. Z drugiej strony jednostki będą miały faktyczny wpływ na zakres informacji, na podstawie których będą otrzymywać spersonalizowane komunikaty lub oferty, co może stanowić dla użytkowników atrakcyjne rozwiązanie. Sami przedsiębiorcy zaś będą mogli budować swoje oferty oraz dostosowywać się do zachowań konsumentów przy ich faktycznej, a nie jedynie domniemanej zgodzie. Pozwoliłoby to również włączyć do tworzenia profili, na podstawie zbieranych informacji „czynnik ludzki" w postaci samych zainteresowanych, którzy mogliby, w oparciu o dostęp w poszczególnych aplikacjach, wpływać na informacje o nich gromadzone, a z drugiej strony strzec swojej prywatności. Wprowadzenie wymogu udostępnienia danych użytkownika nie stanowi też postulatu obciążającego finansowo przedsiębiorców w nadmiernym stopniu.

Podsumowanie

Niewątpliwie problematyka ochrony danych osobowych jest zagadnieniem niezwykle złożonym. Rozwiązania wprowadzone przez RODO pozwalają w pewnym stopniu pogodzić ochronę praw człowieka wraz z interesami osób czerpiących korzyści finansowe z operacji związanych z danymi osobowymi. Ze względu na rozwój technologiczny brak jest często dostatecznego zbadania zjawisk mających miejsce w Internecie oraz ich konsekwencji, a niezdefiniowanie problemu utrudnia postawienie prawnych norm oraz granic dopuszczalnego zachowania. Nie można nie zgodzić się, że

[49] Szerzej zob. *J. Kosuniak*, Odwoływalność zgody…, s. 73–79; *P. Litwiński*, Korporacyjne systemy raportowania nadużyć (whistle blowing hotlines) a ochrona danych osobowych, [w:] *A. Mednis* (red.), Prywatność a ekonomia. Ochrona danych osobowych w obrocie prawnym, Warszawa 2013, s. 113–127.

[50] O handlu danymi osobowymi np.: http://www.telegraph.co.uk/technology/news/12012191/How-much-is-your-personal-data-worth.html, (dostęp z 19.11.2017 r.); http://cyberprzestepczosc.info/handel-danymi-osobowymi/ (dostęp z 19.11.2017 r.)

[51] *Real time* [ang.] – system czasu rzeczywistego. System, w których odpowiedzi na zapytania urządzeń technicznych zależne są od chwili wypracowanego wyniku. Do istoty systemu należy równoległość w czasie zmian w środowisku oraz obliczeń realizowanych na podstawie stanu środowiska. Środowiskiem w powyższym kontekście nazywana jest baza danych lub jej część, zawierająca gromadzone dane użytkowników.

kwestie dotyczące Internetu rzeczy oraz repersonalizacji danych nie zostały wyczerpane przez ustawodawcę unijnego. Te dwa zjawiska posiadają potencjał usprawnienia funkcjonowania jednostek we współczesnym świecie, jednak niosą ze sobą zagrożenia, które mogą doprowadzić w dalszej perspektywie nawet do zmian społeczno-gospodarczych. Konieczne wydaje się obserwowanie tych zjawisk oraz reagowanie, zarówno legislacyjnie, jak i w dużej mierze dzięki orzecznictwu i doktrynie, które będą rozwijać generalne normy i normy celowościowe zawarte w RODO.

Słowa kluczowe: Internet rzeczy, IoT, repersonalizacja danych, RODO, rozporządzenie o ochronie danych osobowych, rozporządzenie 2016/679, ogólne rozporządzenie o ochronie danych, nowe technologie, aplikacje, deanonimizacja, anonimizacja danych, personalizacja danych.

Personal data protection and the Internet of Things, profiling and re-personalization of data

The aim of the article is describing the Internet of Things and re-personalization of data with effects and threats which they may cause in the context of protection of the data. The author of the article compares them to the regulation included in the Regulation 2016/679 of 27 April 2016 of the European Parliament and the Council of the European Union on the protection of legal persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC (General Data Protection Regulation).

Key words: Internet of Things, IoT, re-personalization of data, Regulation (EU) 2016/679, General Data Protection Regulation, new technologies, application, anonymization of data, de-anonymization, personalization of data.

Przeprowadzenie dowodu za pomocą środków porozumiewania się na odległość na zasadzie art. 235 § 2 KPC a realizacja zasady bezpośredniości – uwagi w kontekście nowelizacji KPC z 10.7.2015 r. – część 2

dr *Aleksandra Budniak-Rogala*[1]

Niniejszy artykuł stanowi próbę przedstawienia kompleksowej wykładni regulacji z art. 235 KPC w kontekście realizacji zasady bezpośredniości ze szczególnym uwzględnieniem zmian wprowadzonych ustawą z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw[2], która weszła w życie 8.9.2016 r. Opracowanie zostało podzielone na dwie części. Na wstępie części pierwszej przedstawione zostały założenia związane z realizacją zasady bezpośredniości w postępowaniu cywilnym statuowanej w oparciu o regulację z art. 235 § 1 *in principio* KPC. Następnie omówiona została dopuszczalność przeprowadzenia dowodu przez sędziego wyznaczonego lub sąd wezwany na zasadzie art. 235 § 1 KPC jako wyjątek od przedmiotowej zasady. Na dalszym etapie rozważań odniesiono się do wymogów związanych z przeprowadzeniem dowodu przy użyciu środków porozumiewania się na odległość w myśl art. 235 § 2 KPC – w brzmieniu zarówno przed wejściem w życie przepisów powołanej nowelizacji, jak i po nim. Warto przy tym podkreślić, że na jej mocy ustawodawca skreślił zdanie 2 z art. 235 § 2 KPC, zgodnie z którym sąd orzekający przeprowadzał dowód w obecności sądu wezwanego lub referendarza sądowego w tym sądzie. Zdaniem autorki dokonaną zmianę należy ocenić pozytywnie – podobnie jak samą instytucję dowodu na odległość. W poniżej przedstawionej części drugiej artykułu zostały z kolei opisane relacje pomiędzy dopuszczalnością przeprowadzenia dowodu przez sędziego wyznaczonego lub sąd wezwany (art. 235 § 1 KPC) a możliwością przeprowadzenia dowodu na odległość (art. 235 § 2 KPC) oraz pomiędzy przeprowadzeniem dowodu poza siedzibą sądu (art. 235 § 2 KPC) a regulacją wprowadzającą rozprawę odmiejscowioną (art. 151 § 2 KPC). Omówiona została też delegacja ustawowa z art. 235 § 3 KPC. Przeprowadzone rozważania doprowadziły ostatecznie do wniosku, iż zastosowanie konstrukcji dowodu na odległość prowadzi do wzmocnienia realizacji zasady bezpośredniości w postępowaniu cywilnym.

Relacja pomiędzy regulacją dopuszczającą przeprowadzenie dowodu przez sędziego wyznaczonego lub sąd wezwany (art. 235 § 1 KPC) a przepisem statuującym możliwość przeprowadzenia dowodu przy użyciu środków porozumiewania się na odległość (art. 235 § 2 KPC)

W nawiązaniu do wcześniejszych rozważań problematyczna wydaje się relacja pomiędzy regulacją z art. 235 § 1 KPC, dopuszczającą przeprowadzenie dowodu przez sędziego wyznaczonego lub sąd wezwany, a art. 235 § 2 KPC statuującym możliwość przeprowadzenia dowodu przy użyciu środków porozumiewania się na odległość.

Jak podkreśla w tym kontekście zasadnie *A. Klich*, w znowelizowanym brzmieniu art. 235 § 1 i 2 KPC należy dostrzec wyraźne oddzielenie przez ustawodawcę aspektów konstrukcyjnych wykorzystywania środków komunikowania się na odległość (art. 235 § 2 KPC) od rozwiązań dotyczących sądu wezwanego – sędziego wyznaczonego (art. 235 § 1 KPC). W przypadku przeprowadzenia dowodu na odległość sąd, w którym będzie miał obowiązek stawić się świadek czy też strona postępowania (ewentualnie biegły sądowy) w celu złożenia zeznań (przedstawienia opinii ustnej) za pośrednictwem urządzeń rejestrujących dźwięk albo obraz i dźwięk, umożliwiających przeprowadzenie tele- lub wideokonferencji, będzie zobowiązany jedynie do asysty techniczno-organizacyjnej. W takiej sytuacji nie będzie zatem konieczne angażowanie sądu (sędziego) czy też referendarza sądowego, gdyż wystarczająca będzie obecność urzędnika sądowego, który zadba o stronę techniczną i umożliwienie złożenia tych zeznań bez przeszkód natury organizacyjnej i porządkowej[3].

Warto mieć przy tym na względzie, że dowód na odległość wykazuje liczne zalety w porównaniu z instytucjami sądu wezwanego (sędziego wyznaczonego).

[1] Autorka jest adiunktem w Zakładzie Postępowania Cywilnego na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego oraz adwokatem (ORA Wrocław).

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

[3] *A Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Komentarz, Warszawa 2016, kom. do art. 235 KPC, Nb 11–12, s. 187–189.

Po pierwsze, wypada odnotować, że w sytuacji korzystania z pomocy sądowej nie jest realizowana zasada bezpośredniości[4], gdy tymczasem przeprowadzenie dowodu za pomocą środków porozumiewania się na odległość prowadzi do wzmocnienia realizacji przedmiotowej reguły[5]. Jak podkreśla *A. Kościółek*, „bezpośrednia styczność sądu orzekającego z osobą przesłuchiwaną pozwala bowiem na kompleksowy odbiór otrzymywanych informacji, oparty na współpracy wszystkich przeznaczonych do postrzegania zmysłów – w tym w szczególności zmysłu widzenia. Poza werbalnie dostarczonymi przez osobę przesłuchiwaną informacjami istotne znaczenie mają bowiem również informacje na temat różnych aspektów zachowania, reakcji i sposobu wypowiadania. Przeprowadzenie przesłuchania przy pomocy sądu wezwanego prowadzi natomiast do percepcji otrzymywanych informacji opartej jedynie na przygotowanym przez sąd wezwany przekazie treści przeprowadzonej czynności dowodowej"[6].

Po drugie, istnieje niewątpliwe niebezpieczeństwo, że dowód przeprowadzony w drodze pomocy sądowej nie będzie zawierał wszystkich istotnych elementów[7]. Sąd wezwany i sędzia wyznaczony są bowiem związani zleceniem przeprowadzenia dowodu. Mają zatem do dyspozycji jedynie wyraźnie określone w zleceniu czynności oraz wyczerpująco oznaczone fakty i okoliczności podlegające stwierdzeniu. Organy pomocy sądowej mogą wprawdzie uzupełnić postanowienie sądu orzekającego przez przesłuchanie nowych świadków, ale wyłącznie na wniosek strony oraz tylko w odniesieniu do faktów wskazanych w tym postanowieniu (*vide* art. 240 § 2 KPC). Przesłuchanie na odległość pozwala natomiast na szybką reakcję i właściwe dostosowywanie na bieżąco pytań zadawanych przesłuchiwanemu[8].

Po trzecie, nie sposób pominąć faktu, że z oczywistych względów posługiwanie się przez sąd orzekający przy przeprowadzeniu dowodu sądem wezwanym prowadzi w wielu wypadkach do znacznego przedłużania postępowania[9].

Po czwarte, warto podkreślić, że przeprowadzenie dowodu na odległość skutkuje znaczną redukcją kosztów[10]. Chodzi tutaj przede wszystkim o koszty związane z przesłuchaniem świadków i stron czy też ewentualnie biegłych (w tym w szczególności koszty dojazdu do sądu i utracone zarobki). Samo przeprowadzenie dowodu na odległość może natomiast następować przy użyciu urządzeń służących do generowania protokołu elektronicznego. Mając z kolei na uwadze zakres wdrożenia w przedmiotowym zakresie, wypada stwierdzić, iż na obecnym etapie podjęcie czynności dowodowych na odległość nie będzie zasadniczo pociągało za sobą dodatkowych kosztów związanych z przygotowaniem infrastruktury technicznej.

W konsekwencji, mając na względzie prymat zasady bezpośredniości w postępowaniu cywilnym, uwzględniając równocześnie redakcję art. 235 § 1 i 2 KPC oraz biorąc pod uwagę obecne uwarunkowania techniczne i organizacyjne, należy opowiedzieć się za wykorzystywaniem przez sąd orzekający przede wszystkim możliwości przeprowadzania dowodów na odległość, a tylko w przypadku gdy nie jest to możliwe – zlecanie ich przeprowadzenia sądowi wezwanemu lub sędziemu wyznaczonemu[11]. Inaczej ujmując, na gruncie analizowanej regulacji wypadałoby przyjąć zasadę, zgodnie z którą stosowanie instytucji pomocy sądowej powinno mieć charakter wyjątkowy, uzasadniony szczególnymi okolicznościami, uniemożliwiającymi wykorzystanie środków komunikowania się na odległość[12]. Jak podkreśla słusznie *K. Markiewicz*, docelowo powinno się praktycznie wyeliminować przeprowadzenie dowodu w drodze pomocy prawnej przez sąd wezwany[13].

Reasumując, w sytuacji gdy świadek lub strona postępowania (czy też biegły) przebywają poza okręgiem sądowym, za podstawową formę złożenia przez nich zeznań (przedstawienia opinii ustnej) należałoby uznać ich (jej) odebranie przy użyciu urządzeń technicznych umożliwiających dokonanie tej czynności na odległość[14]. W takim przypadku szczególnie relewantne pozostaje zapewnienie zarówno stronom, jak i sądowi orzekającemu możliwości zadawania pytań w toku składania zeznań lub ustnej opinii – zwłaszcza w odniesieniu do dowodów o podstawowym znaczeniu dla rozstrzygnięcia sprawy, jakimi są częstokroć właśnie wymienione środ-

[4] *J. Gołaczyński*, Doręczenia, protokół i przesłuchanie elektroniczne w postępowaniu cywilnym – postulaty *de lege ferenda*, PME, dodatek do MoP 2006, Nr 16, s. 58; *J. Gołaczyński*, *M. Leśniak*, *B. Pabin*, Doręczenia, protokół i przesłuchanie elektroniczne w postępowaniu cywilnym – postulaty *de lege ferenda*, E-Biuletyn CBKE 2006, Nr 3, www.cbke.prawo.uni.wroc.pl (dostęp z 19.7. 2016 r.).

[5] Więcej na ten temat zob. w toku dalszych rozważań.

[6] Tak: *A. Kościółek*, Elektroniczne czynności procesowe w sądowym postępowaniu cywilnym, Warszawa 2012, s. 312. Por. też *A. Kościółek*, Informatyzacja czynności dowodowych w postępowaniu cywilnym, AUwr Nº 3137, PPiA LXXXII, Wrocław 2010, s. 261. Zob. także *M. Muliński*, *M. Krakowiak*, Przesłuchanie świadka w postępowaniu cywilnym za pomocą środków nowoczesnej techniki – postulat *de lege ferenda*, PS 2005, Nr 3, s. 72.

[7] *J. Gołaczyński*, Doręczenia, protokół i przesłuchanie…, s. 58; *J. Gołaczyński*, *M. Leśniak*, *B. Pabin*, Doręczenia, protokół…

[8] Por. *M. Muliński*, *M. Krakowiak*, Przesłuchanie świadka…, s. 72; *A. Kościółek*, Informatyzacja czynności…, s. 260–261; *A. Kościółek*, Elektroniczne czynności…, s. 312.

[9] *J. Gołaczyński*, Doręczenia, protokół i przesłuchanie…, s. 58; *J. Gołaczyński*, *M. Leśniak*, *B. Pabin*, Doręczenia, protokół…

[10] *J. Gołaczyński*, Doręczenia, protokół…, s. 58; *J. Gołaczyński*, *M. Leśniak*, *B. Pabin*, Doręczenia, protokół…; *D. Sielicki*, Zastosowanie Internetu w zakresie działania organów władzy sądowniczej, E-Biuletyn CBKE 2006, Nr 1, www.cbke.prawo.uni.wroc.pl (dostęp z 25.7.2016 r.).

[11] *J. Misztal-Konecka*, [w:] *K. Piasecki* (red.), Kodeks postępowania cywilnego. T. I. Komentarz do art. 1–366, Legalis/el. 2016, kom. do art. 235 KPC, Nb 31.

[12] *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 12, s. 188–189.

[13] *K. Markiewicz*, Informatyzacja postępowania cywilnego – *de lege lata* i *de lege ferenda*, [w:] *K. Markiewicz*, *A. Torbus* (red.), Postępowanie rozpoznawcze w przyszłym Kodeksie postępowania cywilnego, Warszawa 2014, s. 427–428.

[14] *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 12, s. 188–189.

ki dowodowe o charakterze osobowym. W istocie bowiem czynności dowodowe na odległość pozwalają na zachowanie przez sąd orzekający możliwości osobistej oceny materiału dowodowego, prowadzą do ograniczenia kosztów postępowania i jego przyspieszenia[15]. Przedmiotowych wymogów nie spełnia natomiast z pewnością instytucja sądu wezwanego i sędziego wyznaczonego. W konsekwencji słusznie podnosi *Ł. Goździaszek*, że wprowadzenie do procedury cywilnej dowodu na odległość należy ocenić jednoznacznie pozytywnie – przedmiotowa instytucja stanowi bowiem wreszcie rzeczywistą alternatywę wobec korzystania z pomocy sądowej realizowanej przez sąd wezwany[16].

Przeprowadzenie dowodu poza siedzibą sądu (art. 235 § 2 KPC) a rozprawa odmiejscowiona (art. 151 § 2 KPC)

W celu uzupełnienia prowadzonych rozważań wypada odnieść się do relacji pomiędzy przepisem statuującym możliwość przeprowadzenia dowodu na odległość (art. 235 § 2 KPC) a regulacją wprowadzającą rozprawę odmiejscowioną (nowy art. 151 § 2 KPC).

W oparciu o dotychczasowe brzmienie art. 151 KPC posiedzenia sądowe odbywają się w budynku sądowym, a poza nim tylko wówczas, gdy czynności sądowe muszą być wykonywane w innym miejscu albo gdy odbycie posiedzenia poza budynkiem sądowym ułatwia przeprowadzenie sprawy lub przyczynia się znacznie do zaoszczędzenia kosztów[17]. Przepis ten uległ zmianie 8.9.2016 r. na mocy art. 2 pkt 20 nowelizacji KPC z 10.7.2015 r. poprzez wprowadzenie § 2. Zgodnie z jego treścią przewodniczący może zarządzić przeprowadzenie posiedzenia jawnego przy użyciu urządzeń technicznych umożliwiających jego przeprowadzenie na odległość. W takim przypadku uczestnicy postępowania mogą brać udział w posiedzeniu sądowym, przebywając w budynku innego sądu, i dokonywać tam czynności procesowych, a przebieg czynności procesowych transmituje się z sali sądowej sądu prowadzącego postępowanie do miejsca pobytu uczestników postępowania oraz z miejsca pobytu uczestników postępowania do sali sądowej sądu prowadzącego postępowanie.

W kontekście analizowanej problematyki wypada przede wszystkim zauważyć, że art. 151 § 2 KPC nawiązuje wprost do art. 235 § 2 KPC[18]. Z treści pierwszego z powołanych przepisów wynika możliwość przeprowadzenia posiedzenia jawnego za pomocą środków porozumiewania się na odległość, drugi statuuje natomiast dopuszczalność przeprowadzenia postępowania dowodowego poza siedzibą sądu orzekającego. Nie ulega kwestii, że nieodłączny i najistotniejszy element rozprawy stanowi zwykle postępowanie dowodowe. Zakres zastosowania art. 151 § 2 KPC zawiera więc niejako konstrukcyjnie w swej treści zakres zastosowania art. 235 § 2 KPC. Nie sposób jednak nie zauważyć, że wzajemna relacja analizowanych regulacji jest specyficzna. Podejmując bowiem decyzję o przeprowadzeniu rozprawy za pomocą środków porozumiewania się na odległość, organ sądowy musi brać pod uwagę możliwość przeprowadzenia w jej ramach również postępowania dowodowego. Decyzja w przedmiocie dopuszczenia dowodu na odległość nie wywiera natomiast bezpośredniego wpływu na sposób przeprowadzenia pozostałych czynności w toku rozprawy – innych niż wskazane czynności dowodowe.

Delegacja ustawowa zawarta w treści art. 235 § 3 KPC

Omawiając kwestie sposobów przeprowadzania dowodów w postępowaniu cywilnym, należy się również odnieść do regulacji z art. 235 § 3 KPC. Wspomniany przepis zawiera w swej treści delegację ustawową. Na jej podstawie 24.2.2010 r. Minister Sprawiedliwości wydał rozporządzenie w sprawie urządzeń i środków technicznych umożliwiających przeprowadzenie dowodu na odległość w postępowaniu cywilnym[19]. Określa ono rodzaje urządzeń i środków technicznych umożliwiających przeprowadzenie dowodu na odległość, korzystanie z tych urządzeń oraz sposób przechowywania, odtwarzania i kopiowania zapisów dokonanych podczas przeprowadzania dowodu na odległość (§ 1 DowOdlegR)[20].

Zgodnie z regulacjami powołanego rozporządzenia przeprowadzanie dowodu na odległość następuje przy zastosowaniu urządzeń technicznych analogowych lub cyfrowych umożliwiających przekaz telekomunikacyjny w rozumieniu art. 2 pkt 27a ustawy z 16.7.2004 r. – Prawo telekomunikacyjne[21], a w szczególności urządzeń umożliwiających dwukierunkową łączność w czasie rzeczywistym, pozwalających

[15] Tak: *J. Misztal-Konecka*, [w:] *K. Piasecki* (red.), Kodeks postępowania…, kom. do art. 235 KPC, Nb 31. Podobnie: *A. Zalesińska*, Wpływ informatyzacji na założenia konstrukcyjne procesu cywilnego, Warszawa 2016, s. 228–229.

[16] *Ł. Goździaszek*, Zasada bezpośredniości i pisemności postępowania dowodowego w świetle nowelizacji Kodeksu postępowania cywilnego z 5 grudnia 2008 r., PME 2010, Nr 2, s. 26 i n.

[17] W doktrynie podkreśla się, że art. 151 KPC ma fundamentalne znaczenie dla określenia miejsca podejmowania czynności dowodowych w toku postępowania w sprawach cywilnych. W treści tego przepisu ustawodawca reguluje bowiem miejsce podejmowania czynności przez sąd lub uczestników postępowania wobec sądu, jeżeli są one dokonywane na posiedzeniach sądowych. Por. *S. Cieślak*, Formalizm postępowania cywilnego, Warszawa 2008, s. 256 i n., oraz *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 3, s. 181.

[18] Tak też: *A. Zalesińska*, Wpływ informatyzacji…, s. 232.

[19] Dz.U. Nr 34, poz. 185; dalej jako: DowOdlegR.

[20] Tak: *E. Rudkowska-Ząbczyk*, [w:] *E. Marszałkowska-Krześ* (red.), Kodeks postępowania cywilnego. Komentarz, Legalis/el. 2016, kom. do art. 235 KPC, Nb 21. Więcej na ten temat zob. *J. Misztal-Konecka*, [w:] *K. Piasecki* (red.), Kodeks postępowania…, kom. do art. 235 KPC, Nb 34–40.

[21] T.j. Dz.U. z 2016 r. poz. 1489 ze zm.; dalej jako: PrTelU.

na przesył dźwięku lub obrazu i dźwięku pomiędzy uczestnikami czynności procesowej. Dowód na odległość może być przeprowadzony z wykorzystaniem sieci telekomunikacyjnej w rozumieniu art. 2 pkt 35 PrTelU, a w szczególności z wykorzystaniem sieci telekomunikacyjnej eksploatowanej przez sąd. Należy mieć przy tym na względzie, że wymienione urządzenia powinny gwarantować integralność przekazu telekomunikacyjnego. Jeśli natomiast przedmiotowy przekaz wymaga poufności, należy zastosować środki lub rozwiązania techniczne zapewniające dostęp do zrozumiałej formy zabezpieczonego przekazu tylko osobom uprawnionym (§ 2 DowOdlegR). Dodatkowo rozporządzenie wskazuje na zasady prowadzenia wykazów oraz korzystania z wymienionych urządzeń, łącznie z zasadami prowadzenia specjalnych harmonogramów ich dostępności (por. § 3 i 4 DowOdlegR). Z przeprowadzeniem dowodu na odległość łączy się także konieczność utrwalenia przebiegu tej czynności oraz przechowywania, odtwarzania i kopiowania sporządzonych zapisów. Powołane rozporządzenie określa zatem również minimalne wymogi w przedmiotowym zakresie (*vide* § 5–9 DowOdlegR)[22].

Dopuszczalność przeprowadzenia dowodu za pomocą środków porozumiewania się na odległość a zasada bezpośredniości – podsumowanie

Postęp techniczny stanowi niewątpliwie istotne podwaliny procesu informatyzacji postępowania cywilnego. W analizowanym aspekcie jego pierwsze relewantne refleksy widoczne były z momentem wprowadzenia do procedury cywilnej rozwiązań technologicznych umożliwiających generowanie protokołu elektronicznego. Omawiane nowelizacje przepisów postępowania cywilnego stawiają natomiast kolejne kroki w kierunku unowocześnienia prawa procesowego cywilnego, wprowadzając możliwość przeprowadzania posiedzeń jawnych i dowodów za pomocą środków porozumiewania się na odległość. Nie ulega przy tym w zasadzie wątpliwości, iż realizacja wymienionych konstrukcji będzie dopuszczalna w oparciu o infrastrukturę techniczną wykorzystywaną do sporządzania elektronicznego zapisu posiedzenia sądowego[23].

W analizowanym kontekście w konkluzji wypada odnieść się do kwestii realizacji zasady bezpośredniości na gruncie dopuszczalności przeprowadzenia dowodu na odległość. W doktrynie wskazuje się, że przeprowadzanie środków dowodowych z wykorzystaniem instrumentów komunikowania się na odległość należy postrzegać jako przejaw zasady bezpośredniości, a nie wyjątek od niej[24].

Jak już wcześniej wspomniano, omawiana reguła opiera się na założeniu, że tylko bezpośrednie i osobiste zetknięcie się sądu orzekającego ze stronami, świadkami, biegłymi oraz dowodami rzeczowymi zapewnia możliwość poczynienia odpowiednich spostrzeżeń, relewantnych z punktu widzenia oceny wiarygodności oraz mocy dowodów[25]. Zdaniem *A. Kościółek* w nawiązaniu do analizowanej problematyki przedmiotową zasadę należy rozpatrywać na dwóch płaszczyznach: w odniesieniu do miejsca przeprowadzenia dowodu i w nawiązaniu do sposobu jego przeprowadzenia. Jeśli chodzi o pierwszy z wymienionych aspektów, to w sytuacji, gdy postępowanie dowodowe jest przeprowadzane tradycyjną metodą, zarówno w przypadku przeprowadzania czynności dowodowych w siedzibie sądu orzekającego, jak i poza nią, organ prowadzący postępowanie oraz źródło dowodu znajdują się w bezpośredniej odległości (np. na tej samej sali sądowej, w tym samym miejscu poza budynkiem sądu). Natomiast w sytuacji, gdy postępowanie dowodowe jest przeprowadzane przy wykorzystaniu urządzeń technicznych umożliwiających dokonanie takich czynności na odległość, dochodzi do rozdzielenia miejsca przeprowadzenia dowodu między siedzibę sądu, w której znajduje się przeprowadzający ten dowód skład orzekający, a siedzibę sądu, w której znajduje się źródło dowodu. Odnosząc się z kolei do drugiego w wymienionych komponentów zasady bezpośredniości, wypada odnotować, że – identycznie jak w przypadku standardowej procedury przeprowadzania dowodów – samo przeprowadzenie dowodu na odległość należy niezmiennie do sądu prowadzącego dane postępowanie.

Mając na uwadze powyższe, *A. Kościółek* zasadnie proponuje, by na nowo zdefiniować kategorię bezpośredniości w postępowaniu dowodowym. „Pojęcie to nadal należy wiązać z wymogiem przeprowadzenia czynności bezpośrednio przez sąd orzekający. Wymóg ten jest nadal tożsamy z bezpośrednim kontaktem między sądem orzekającym a źródłem dowodu. Jednak w kontekście nowoczesnych rozwiązań technologicznych wspomniany kontakt bezpośredni nie jest już uzależniony od fizycznej bliskości kontaktujących się pod-

[22] Por. *T. Demendecki*, [w:] *A. Jakubecki* (red.), Komentarz aktualizowany do Kodeksu postępowania cywilnego, Lex/el. 2016, kom. do art. 235 KPC; *A. Zalesińska*, Wpływ informatyzacji…, s. 229–230. Zob. też: *A. Kościółek*, Elektroniczne czynności…, s. 304 i n.; *K. Gajda-Roszczynialska*, [w:] *Ł. Błaszczak*, *K. Markiewicz* (red.), Dowody i postępowanie dowodowe w sprawach cywilnych, Warszawa 2015, s. 355–356.

[23] W tym kontekście por. też *A. Klich*, Możliwości wykorzystania protokołu elektronicznego i środków komunikacji na odległość na potrzeby postępowania dowodowego w sprawach cywilnych, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Teoria i praktyka, Warszawa 2016, s. 89, oraz *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186–187.

[24] Tak: *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186–187. Podobnie: *A. Kościółek*, Elektroniczne czynności…, s. 300–303; *K. Gajda-Roszczynialska*, [w:] *Ł. Błaszczak*, *K. Markiewicz* (red.), Dowody…, s. 354; *A. Zalesińska*, Wpływ informatyzacji…, s. 97.

[25] Zob. *A. Kościółek*, Elektroniczne czynności…, s. 302. Por. też doktrynę i orzecznictwo powołane w odniesieniu do wcześniejszych rozważań w przedmiotowym zakresie.

miotów, lecz wynika również z rozwiązań zapewniających zachowanie bieżącego kontaktu, niezależnie od odległości. Dlatego też charakterystyczna dla przeprowadzanych tradycyjnie czynności dowodowych jedność miejsca pobytu sądu orzekającego oraz źródła dowodu nie ma znaczenia dla zachowania założeń zasady bezpośredniości w przypadku czynności przeprowadzanych na odległość. Czynności dowodowe na odległość, realizujące zasadę bezpośredniości, należy uznać za elektroniczną alternatywę dla tradycyjnie bezpośrednich czynności dowodowych"[26]. W takiej sytuacji sąd orzekający zapoznaje się bowiem bezpośrednio z materiałem dowodowym[27], oddziałuje w trybie rzeczywistym na przebieg postępowania dowodowego i może na bieżąco dokonywać weryfikacji i oceny materiału dowodowego – identycznie jak w przypadku, w którym postępowanie dowodowe odbywa się w budynku sądu prowadzącego postępowanie[28]. Według *A. Klich* w razie przeprowadzenia dowodu na odległość osobisty kontakt sądu ze środkiem dowodowym jest umożliwiony przez rzeczywisty przekaz zapewniony przez sprzęt do nagrywania dźwięku lub obrazu i dźwięku. Mamy wówczas do czynienia z tzw. właściwością odmiejscowioną sądu orzekającego[29]. Jak podkreśla w tym kontekście z kolei *A. Zalesińska*, „w trakcie takiego przesłuchania następuje poznawanie postaw drugiej strony oraz wzajemna wymiana informacji. Ten mechanizm sprzężenia zwrotnego daje przesłuchującemu szansę uzgodnienia podstawowych pojęć i treści przekazywanych (w przypadku biegłych) oraz zadawanie kontrolnych i uzupełniających pytań (w przypadku świadków)"[30]. Analizowana forma przeprowadzenia postępowania dowodowego daje zatem sądowi możliwość bezpośredniego poczynienia własnych spostrzeżeń, które stają się niezwykle istotne na etapie oceny wiarygodności i znaczenia poszczególnych środków dowodowych[31].

Konstatując, wypada więc stwierdzić, że czynności dowodowe na odległość pozwalają na zachowanie przez organ prowadzący postępowanie osobistej, a tym samym pełnej i kompleksowej oceny materiału dowodowego. Nadają one zatem nową jakość zasadzie bezpośredniości[32]. W doktrynie podkreśla się, że przedmiotowa reguła została przeorientowana pod wpływem informatyzacji postępowania cywilnego, co polega na tworzeniu nowych – alternatywnych – jej form[33]. Należy mieć przy tym na względzie, iż możliwości alternatywnej realizacji zasady bezpośredniości ewoluowały wraz z wdrażaniem nowoczesnych technologii i ich wykorzystaniem przez wymiar sprawiedliwości[34]. Dynamiczny rozwój w przedmiotowym zakresie stanowi bowiem alternatywę dla dotychczasowych rozwiązań legislacyjnych i umożliwia pełną realizację analizowanej reguły[35].

Ostatecznie wydaje się, że upowszechnienie się w praktyce sądowej czynności dowodowych na odległość powinno wpływać na wzmocnienie zasady bezpośredniości[36]. Wykorzystanie takich form sprzyja bowiem z pewnością w dużo większym stopniu rzetelności postępowania niż przeprowadzenie dowodów w drodze pomocy sądowej[37]. Należy mieć na względzie, że każde powtórzenie wiadomości – w tym przekazanie sądowi orzekającemu informacji dotyczących czynności dowodowej przeprowadzonej przez sąd wezwany lub sędziego wyznaczonego – grozi jej zniekształceniem[38]. Dodatkowo warto podkreślić, że w przypadku skorzystania z instytucji pomocy sądowej sąd orzekający bazuje na materiale dowodowym poddanym uprzednio subiektywnej ocenie sądu wezwanego. Z oczywistych względów przedmiotowe zjawisko jest w swej istocie wysoce niepożądane[39]. Omawiany sposób przeprowadzania postępowania dowodowego z osobowych źródeł dowodowych generuje ponadto niewątpliwie oszczędności zarówno po stronie wymiaru sprawiedliwości, jak i osób przesłuchiwanych, które dzięki jego użyciu zostają zwolnione z obowiązku osobistego stawiennictwa w budynku sądu wzywającego. Wystarczające okazuje się bowiem udanie się do sądu wezwanego znajdującego się w bliskiej odległości od ich miejsca zamieszkania[40]. W konsekwencji skutkuje to

[26] Tak: *A. Kościółek*, Elektroniczne czynności…, s. 302–303. W tym kontekście por. też: *S. Cieślak*, Forma czynności w procesie cywilnym – stan obecny i perspektywy rozwoju, [w:] *K. Markiewicz, A. Torbus* (red.), Postępowanie rozpoznawcze w przyszłym Kodeksie postępowania cywilnego, Warszawa 2014, s. 158; *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 94; *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186.

[27] Por. *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186–187.

[28] W nieco innym ujęciu zob. także *Ł. Goździaszek*, Zasada bezpośredniości…, s. 29, oraz *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 94.

[29] Więcej zob. *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 94.

[30] Tak: *A. Zalesińska*, Wpływ informatyzacji…, s. 97; Podobnie: *A.Zalesińska,* Przesłuchanie na odległość w Polsce – postulaty *de lege lata* i *de lege ferenda* na tle konstrukcji prawnych przyjętych w innych krajach, E-Biuletyn CBKE 2007, Nr 2, www.cbke.prawo.uni.wroc.pl (dostęp z 19.7. 2016 r.).

[31] Tak: *A. Zalesińska*, Wpływ informatyzacji…, s. 228–229. Por. też *J. Turek*, Czynności dowodowe sądu w procesie cywilnym, Warszawa 2011, s. 84 i n.

[32] Tak: *A. Kościółek*, Elektroniczne czynności…, s. 303. Por. także: *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 94.

[33] *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186.

[34] Por. *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186–187.

[35] Tak: *A. Zalesińska*, Wpływ informatyzacji…, s. 97.

[36] *A. Zalesińska*, Przesłuchanie…; *A. Zalesińska*, Wpływ informatyzacji…, s. 228; *Ł. Goździaszek*, Zasada bezpośredniości…, s. 28, 29; *A. Kościółek*, Informatyzacja czynności…, s. 255; *A. Kościółek*, Elektroniczne czynności…, s. 303–304; *K. Markiewicz*, Informatyzacja …, [w:] *K. Markiewicz, A. Torbus* (red.), Postępowanie…, s. 406.

[37] Tak: *K. Markiewicz*, Informatyzacja…, [w:] *K. Markiewicz, A. Torbus* (red.), Postępowanie…, s. 406. Podobnie: *A. Kościółek*, Elektroniczne czynności…, s. 303–304.

[38] Tak: *A. Zalesińska*, Przesłuchanie…

[39] Por. *A. Zalesińska*, Przesłuchanie…

[40] Tak: *A. Zalesińska*, Wpływ informatyzacji…, s. 229. Por. też: *M. Mulinski*, *M. Krakowiak*, Przesłuchanie świadka…, s. 73; *D. Sielicki*, Zastosowanie Internetu…; *A. Zalesińska*, Przesłuchanie…; *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 90, 93.

przyspieszeniem, a także zwiększeniem sprawności i efektywności postępowania, przeciwdziałając jego przewlekaniu[41]. Co więcej, buduje to również pożądane zaufanie do wymiaru sprawiedliwości[42]. Ostatecznie wydaje się, że użycie analizowanej konstrukcji powinno prowadzić do niwelowania barier powodujących ewentualne wykluczenie prawne osób, które z powodu stanu zdrowia, stopnia niepełnosprawności czy też ze względu na barierę finansową są pozbawione możliwości osobistego stawiennictwa w sądzie, przed którym odbywa się postępowanie dowodowe[43] .

W uzupełnieniu powyższego wypada zgodzić się ze stanowiskiem *A. Klich*, która wskazuje, iż *de lege ferenda* zasadne się wydaje wprowadzenie na grunt prawa procesowego cywilnego konstrukcji analogicznej do aktualnego wniosku strony o rozpoznanie sprawy pod jej nieobecność, której istotą byłaby możliwość udziału strony w posiedzeniu sądu przy użyciu urządzeń rejestrujących dźwięk albo obraz i dźwięk. Ograniczenie w przedmiotowym zakresie mogłaby wprawdzie stanowić sytuacja, w której dany sąd nie zostałby wyposażony w adekwatne urządzenia techniczne, umożliwiające swobodne przeprowadzenie dowodu na odległość. Mając jednak na względzie zaawansowany stopień wdrażania protokołu elektronicznego, a tym samym stopniowe wyposażanie sądów powszechnych w sprzęt umożliwiający rejestrowanie przebiegu posiedzenia za pomocą narzędzi teleinformatycznych, nie wydaje się, jakoby mogło to stanowić istotną barierę w odniesieniu do popularyzacji konstrukcji dopuszczających przeprowadzenie rozprawy odmiejscowionej i dowodu na odległość[44]. Przyjęcie proponowanego rozwiązania mogłoby natomiast zwrócić uwagę organów procesowych na możliwość wykorzystania sprzętu umożliwiającego utrwalenie w formie elektronicznej zapisu przebiegu posiedzenia do przeprowadzenia dowodów na odległość[45], prowadząc w konsekwencji do popularyzacji i upowszechnienia przedmiotowej instytucji[46].

[41] Podobnie *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 90, 93. Por. też *M. Muliński*, *M. Krakowiak*, Przesłuchanie świadka…, s. 73; *D. Sielicki*, Zastosowanie Internetu...; *A. Zalesińska*, Przesłuchanie…

[42] *D. Sielicki*, Zastosowanie Internetu...; *A. Zalesińska*, Przesłuchanie…

[43] Por. *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186. Szerzej zob. *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 89–90.

[44] Por. *A. Klich*, [w:] *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, kom. do art. 235 KPC, Nb 10, s. 186–187.

[45] Tak: *A. Klich*, Możliwości wykorzystania…, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja…, s. 89.

[46] W tym kontekście por. też *D. Sielicki*, Zastosowanie Internetu…, oraz *A. Kościółek*, Informatyzacja czynności…, s. 265–266.

Słowa kluczowe: zasada bezpośredniości, dowód na odległość, pomoc sądowa.

Taking evidence by using means of distance communication under the Article 235 § 2 CCP in relation to the directness principle – remarks in the light of the CCP amendment of 10 July 2015 – part 2

This paper constitutes an attempt to present comprehensive interpretation of the Article 235 of the Polish Code of Civil Procedure (CCP) in the light of the directness principle and by taking into account, in particular, modifications introduced by the Act of 10 July 2015 on Amending the Civil Code, Code of Civil Procedure and certain other acts (Dz.U. [Journal of Laws] item 1311), which entered into force on 8 September 2016. The paper has been divided into two parts. Preliminary remarks of the first part of the paper present the outcomes of the directness principle application in the course of civil proceedings, as stipulated in the Article 235 § 1 CCP in principio. Further, the paper discusses premises for taking evidence by the delegated judge or requested court pursuant to the Article 235 § 1 CCP as an exception to the said principle. Subsequently, the author comments taking evidence by using means of distance communication as provided for in the Article 235 § 2 CCP – both in the wording before and after the provisions of the abovementioned amendment entered into force. It is worth mentioning that by said amendment the Legislator deleted the second sentence of the Article 235 § 2 CCP, by which the adjudicating court was obliged to take this evidence in the presence of requested court or registrar of this court. In the author's opinion this modification should be considered as a positive change. Same positive opinion should be given to the institution of taking evidence remotely. In the second part of the paper the author describes relations between admissibility of taking evidence by delegated judge or requested court (Article 235 § 1 CCP) and taking evidence remotely (Article 235 § 2 CCP) as well as between taking evidence outside the courthouse (Article 235 § 2 CCP) and conducting a remote hearing (Article 151 § 2 CCP). The paper also discusses the statutory delegation of power laid down in the Article 235 § 3 CCP. The performed analysis leads to the conclusion that taking evidence by using means of distance communication actually strengthens the execution of the directness principle in the civil procedure.

Key words: directness principle, remotely taken evidence, judicial assistance.

Funkcjonowanie elektronicznych biur podawczych w wybranych krajach

r.pr. *Anna Materla*[1]

Celem opracowania jest opisanie rozwiązań przyjętych w wybranych państwach europejskich (Niemcy, Włochy i Francja) na potrzeby stworzenia elektronicznego biura podawczego w postępowaniu cywilnym. Mimo że w opisywanych krajach istniały już podstawy prawne dotyczące elektronicznych dokumentów, podpisów elektronicznych oraz ewentualnie korzystania ze środków elektronicznych, sądy nie były przystosowane do odbierania pism wnoszonych drogą elektroniczną, a uczestnicy postępowania cywilnego byli niepewni co do stosowania tego kanału dostępu do wymiaru sprawiedliwości. Dla prawidłowego funkcjonowania elektronicznego biura podawczego niezbędne jest zaprojektowanie i wdrożenie systemu teleinformatycznego, ale systemy istniejące w opisywanych krajach działały regionalnie lub nie były dostępne w każdym sądzie. W celu rozwiązania tego problemu Niemcy, Włochy i Francja zdecydowały się na wprowadzenie zmian w zakresie funkcjonujących w tych państwach systemów informatycznych, służących do wnoszenia pism do sądu, oraz na nałożenie na podmioty profesjonalne obowiązku korzystania z tego systemu. W artykule przedstawiono zmiany w przepisach w zakresie elektronicznej komunikacji z sądami w opisywanych krajach. Ponadto artykuł prezentuje zasady wnoszenia pism do sądu drogą elektroniczną przyjęte w tych państwach, które mogą następnie stanowić wskazówki dla pozostałych ustawodawstw w zakresie tworzenia i implementacji systemów informatycznych obsługujących proces wnoszenia dokumentów elektronicznych do sądów.

Uwagi wstępne

Poza granicami Polski nie stosuje się pojęcia elektronicznego biura podawczego, ale w poszczególnych jurysdykcjach pomysł uruchomienia możliwości składania i doręczania pism drogą elektroniczną istniał od wielu lat. W różnych państwach na świecie odmiennie to regulowano oraz implementowano. Często pomimo prawnej możliwości składania pism drogą elektroniczną brakowało systemu, który byłby powszechnie dostępny i należycie obsługiwałby dokumenty wniesione w ten sposób. W konsekwencji faktyczne wykorzystanie przepisów przewidujących skorzystanie z drogi elektronicznej przy wnoszeniu pism w postępowaniu cywilnym było znikome.

Mając powyższe na uwadze, od kilku lat można zaobserwować zmiany w zakresie przepisów dotyczących elektronicznego składania pism w postępowaniu cywilnym. Coraz więcej państw decyduje się na wprowadzenie systemu informatycznego, który umożliwia składanie i doręczanie dokumentów w postępowaniu cywilnym drogą elektroniczną. Niektóre z krajów postanawiają nałożyć na określone podmioty (przede wszystkim podmioty profesjonalne) obowiązek korzystania z tych systemów.

Wnoszenie pism drogą elektroniczną w Niemczech

W Niemczech nie funkcjonuje pojęcie elektronicznego biura podawczego, raczej korzysta się z wyrażenia „elektroniczny obrót prawny", który jest utożsamiany z bezpieczną i prawnie skuteczną wymianą elektronicznych dokumentów między obywatelami, urzędami i sądami. Niemcy są przykładem państwa, w którym prawna możliwość składania pism procesowych drogą elektroniczną prawnie istnieje już od wielu lat. Niemiecki ustawodawca na podstawie ustawy o dostosowaniu przepisów o formie pisemnej w prawie prywatnym i innych przepisach do nowoczesnego obrotu prawnego z 13.7.2001 r.[2] oraz ustawy o reformie postępowania w zakresie doręczeń z 25.6.2001 r.[3] przyjął regulacje ramowe w celu dopuszczalności zastąpienia formy pisemnej elektroniczną. Przepisy, które zostały przyjęte na podstawie tych ustaw, ustanowiły podstawy prawne zarówno do wnoszenia pism drogą elektroniczną do sądu, jak i dla elektronicznych doręczeń dokonywanych przez sąd. Zmieniono m.in. § 126 ust. 3 niemieckiego kodeksu cywilnego[4] w ten sposób, że ustawowa forma pisemna może zostać zastąpiona formą elektroniczną. W takim przypadku wystawca dokumentu elektronicznego musi opatrzyć go podpisem elektronicznym w rozumieniu niemieckiej ustawy o podpisach elektronicznych[5]. Następnie ustawą o stosowaniu elektronicznych form komunikacji

[1] Autorka jest radcą prawnym i doktorantką w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, działającym na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001, BGBl. I, s. 1542.

[3] Gesetz zur Reform des Verfahrens bei Zustellungen vom 25. Juni 2001, BGBl. I, s. 1206.

[4] Bürgerliches Gesetzbuch, BGBl. I, s. 1190, dalej jako: BGB.

[5] § 126a ust. 1, BGB.

z 22.3.2005 r.[6] znowelizowano m.in. reguły dotyczące wnoszenia pism procesowych oraz dopuszczono możliwość prowadzenia elektronicznych akt.

Na podstawie wyżej wymienionych przepisów ustanowiono również możliwość elektronicznych doręczeń. W poszczególnych procedurach dopuszczono elektroniczne doręczenia dokumentów elektronicznych m.in. urzędom, osobom prawnym, adwokatom, doradcom podatkowym i notariuszom[7]. W przypadku takiego sposobu doręczenia potwierdzenie odbioru jest odsyłane jako elektroniczny dokument, który został opatrzony podpisem elektronicznym.

Przepisy o formie elektronicznej i elektronicznych doręczeniach stanowią podstawę prawną dla funkcjonowania elektronicznej skrzynki sądów i administracji[8], czyli specjalnego oprogramowania, które umożliwia wnoszenie pism i dokumentów drogą elektroniczną. Z tej możliwości mogą obecnie skorzystać zarówno osoby fizyczne, osoby prawne i ich przedstawiciele, jak i adwokaci. Podstawą funkcjonowania EGVP jest § 130a ZPO. Zgodnie z tym przepisem pisma i ich załączniki, opinie, oświadczenia stron lub osób trzecich mogą zostać zapisane jako dokument elektroniczny oraz wniesione do sądu, jeśli taki dokument nadaje się do odtworzenia przez sąd. Takie dokumenty powinny zostać podpisane kwalifikowanym podpisem elektronicznym[9]. EGVP umożliwia identyfikację nadawcy oraz założenie konta w tym systemie, a także komunikację z wieloma sądami, bez potrzeby każdorazowego ponawiania procesu tworzenia konta dla poszczególnych instytucji. Skorzystanie z EGVP nie wiąże się z dodatkowymi kosztami dla użytkownika, ale obecnie nie jest możliwe w każdym sądzie, co znacznie ogranicza możliwość wnoszenia pism w ten sposób[10].

W związku z tym, mimo istnienia w Niemczech od ponad 10 lat podstaw prawnych do wnoszenia pism procesowych drogą elektroniczną, z tej formy komunikacji z sądami korzystano jednak w znikomym zakresie, a forma papierowa jest nadal dominująca[11]. Jako przyczyny niewielkiego zainteresowania tymi systemami wskazuje się brak zaufania do elektronicznej komunikacji oraz wymóg posiadania kwalifikowanego podpisu elektronicznego[12]. Ponadto, jak już wspomniano, korzystanie z EGVP nie jest powszechnie możliwe, ale jedynie w niektórych sądach. Z tych powodów obecnie obserwuje się proces dalszego rozwoju elektronicznego biura podawczego w Niemczech, a mianowicie wprowadzenie obowiązku posługiwania się tą formą komunikacji z sądami przez adwokatów za pośrednictwem specjalnej skrzynki elektronicznej (beA)[13].

W 2013 r. przyjęto ustawę o wspieraniu elektronicznego obrotu prawnego z sądami z 10.10.2013 r.[14] W związku z tym, że ustawa przewiduje rewolucyjne zmiany, jej wejście w życie podzielono na kilka etapów[15]. Celem tej ustawy jest wprowadzenie dla adwokatów oraz innych osób uprawnionych do reprezentacji, a także urzędów obowiązku korzystania z drogi elektronicznej przy porozumiewaniu się z sądem. Oznacza to, że od 1.1.2022 r. droga elektroniczna ma stać się obowiązkową i jedyną drogą komunikacji między adwokatami i innymi podmiotami profesjonalnymi oraz wymiarem sprawiedliwości. Podmioty te nie będą miały możliwości dalszego korzystania z systemu EGVP. Droga elektroniczna stanie się pierwotnym sposobem wnoszenia pism i dokumentów do sądów. Jeżeli przesłanie dokumentu elektronicznie będzie niemożliwe z powodów technicznych, wyjątkowo można wnieść pismo na zasadach ogólnych. Należy jednak, z chwilą skorzystania z drogi zastępczej (czyli pisemnej) lub niezwłocznie po tym, uprawdopodobnić przyczyny, z powodu których przesłanie pisma elektronicznie nie było możliwe[16]. Od zasady wnoszenia pism drogą elektroniczną zostały przewidziane wyjątki, tj. sprawy karne, sprawy egzekucyjne (poza zajęciem wierzytelności do 5000 euro) i sprawy dotyczące zgodności przepisów z konstytucją[17].

Osoby fizyczne niebędące adwokatami nie mają obowiązku korzystania z drogi elektronicznej. Nie mogą skorzystać bezpośrednio z beA, ale pozostają im pozostałe dostępne kanały komunikacji elektronicznej z sądem, tj. obecnie konto „De-Mail"[18] oraz EGVP.

Celem systemu beA jest przede wszystkim zapewnienie prywatności, tj. poufności oraz autentyczności, przy odbieraniu i wysyłaniu dokumentów między adwokatami i sądami. System beA ma pełnić funkcję szczególnego rodzaju skrzynki nadawczo-podawczej, w którą zostanie wyposażony każdy adwokat, ale nie służy do przechowywania maili ani nie zastępuje oprogramowania kancelaryj-

[6] Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz vom 22. März 2005, BGBl. I, s. 837.

[7] Przykładowo § 174 ust. 3 niemieckiego kodeksu postępowania cywilnego, Zivilprozessordnung, BGBl. 2007 I, s. 1781, dalej: ZPO.

[8] Elektronisches Gerichts- und Verwaltungspostfach, dalej jako: EGVP.

[9] *M. Müller*, Die Digitalisierung der Justiz in Deutschland, Hamburg 2015, s. 130 i n.

[10] *A. Kulow*, Elektronische Signatur und das besondere elektronische Anwaltspostfach: FördElRV update 2016, Kommunikation&Recht 2015, Nr 9, s. 540.

[11] Por. uzasadnienie projektu ustawy o wspieraniu elektronicznego obrotu prawnego z sądami (Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten), druk Nr 818/12, ID: 17-50035, źródło: http://dipbt.bundestag.de/extrakt/ba/WP17/500/50035.html (dostęp z 14.2.2017 r.).

[12] *A. Kulow*, Elektronische Signatur…, s. 540.

[13] Besonderes elektronisches Anwaltspostfach (beA), dalej jako: beA.

[14] Gesetz zur Förderung des elektronischen Rechtsverkehrs mit den Gerichten vom 10. Oktober 2013, BGBl. I, s. 3786.

[15] *A. Kulow*, Elektronische Signatur…, s. 537.

[16] Projektowany art. 130d ZPO. Na podstawie art. 1 ust. 4 ustawy o wspieraniu elektronicznego obrotu prawnego z sądami.

[17] *A. Kulow*, Elektronische Signatur…, s. 537.

[18] Jest to środek komunikacji dopuszczony na podstawie ustawy o De-Mail z 28.4.2008 r., BGBl. I, s. 666. Rozwiązanie zostało wprowadzone, aby zapewnić pewny, godny zaufania środek komunikacji w Internecie. Por. *M. Müller*, Die Digitalisierung der Justiz…, s. 100 i n.

nego[19]. Ma on także stanowić środek komunikacji między adwokatami, sądami i urzędami, nie podmiotami trzecimi. Niemiecki ustawodawca zdecydował się na wykorzystanie podpisu elektronicznego jako formy identyfikacji, mimo że w literaturze niemieckiej podkreśla się, że podpis elektroniczny nie cieszy się dużą popularnością[20]. Aby zapewnić odpowiednią identyfikację uczestników systemu beA, każdy adwokat zostanie wyposażony w specjalny numer SAFE-ID. Informacje o adwokatach dopuszczonych do wykonywania zawodu będą przekazywane przez poszczególne izby, za co ponoszą one odpowiedzialność. Zgodnie z założeniami beA przy tworzeniu opisywanego systemu teleinformatycznego będą uczestniczyły zarówno sądy, jak i izby reprezentujące adwokatów. Szczegóły funkcjonowania beA na razie nie są jednak znane, gdyż brakuje w tym zakresie rozporządzenia wykonawczego[21].

Na gruncie znowelizowanego ZPO beA została zakwalifikowana jako „bezpieczny środek przekazywania" do dokumentów elektronicznych w rozumieniu § 130a ust. 4 nr 2 ZPO. Dotychczas posługiwanie się elektronicznymi dokumentami w Niemczech było dopuszczalne, ale uzależnione od tego, czy sąd był przystosowany do przetwarzania takich dokumentów[22]. Nowelizacja wprowadza możliwość posługiwania się elektronicznym dokumentem, jeśli został opatrzony kwalifikowanym podpisem elektronicznym lub został podpisany przez osobę odpowiedzialną oraz wniesiony za pomocą bezpiecznego środka przekazywania[23]. Ustawa przewiduje cztery takie bezpieczne kanały. Są to konto „De-Mail", EGVP, beA oraz inne sposoby przekazu, przyjęte na poziomie Federacji i ustanowione w drodze rozporządzenia. Ustawodawca zostawił więc w tym zakresie furtkę dla ewentualnych przyszłych rozwiązań, które obecnie jeszcze nie funkcjonują. Osoba, która nie jest adwokatem ani podmiotem profesjonalnym i która składa dokument do sądu drogą elektroniczną, może więc wybrać jedną z dostępnych możliwości.

W znowelizowanym niemieckim kodeksie postępowania cywilnego przewidziano również, co dzieje w sytuacji, gdy dokument złożony drogą elektroniczną nie może zostać odtworzony przez sąd. Niezwłocznie powiadamia się o tym nadawcę, wskazując na brak skuteczności wniesienia dokumentu oraz obowiązujące wymagania techniczne. Dokument uznaje się za wniesiony z chwilą pierwotnego wniesienia, jeśli nadawca niezwłocznie dostarczy go do sądu w odpowiedniej formie oraz uprawdopodobni, że wniesiony dokument jest zgodny co do treści z dokumentem pierwotnie złożonym do sądu[24].

Niemiecki ustawodawca, opierając się na doświadczeniach mało popularnego wykorzystywania środków elektronicznych w postępowaniu cywilnym, zdecydował się wprowadzić obowiązek korzystania z drogi elektronicznej dla adwokatów i innych podmiotów profesjonalnych. W tym celu jest tworzony dodatkowy kanał komunikacji między adwokatami i sądem – beA, przygotowywany w porozumieniu z samorządem zawodowym adwokatów w Niemczech. Na aprobatę zasługuje fakt, że w Niemczech propaguje się wykorzystanie środków komunikacji elektronicznej w postępowaniu cywilnym przez wprowadzenie różnych form identyfikacji uczestników postępowania cywilnego, zainteresowanych wnoszeniem pism drogą elektroniczną. Z drugiej strony można mieć wątpliwości, czy jest potrzebne aż tyle różnych kanałów do komunikacji uczestników postępowania z sądami. Weryfikacja tego założenia będzie możliwa jednak dopiero w praktyce.

Wnoszenie pism drogą elektroniczną we Włoszech

Idea informatyzacji postępowania cywilnego we Włoszech funkcjonuje pod nazwą *Processo Civile Telematico*, czyli w tłumaczeniu „proces cywilny online". Nazwa odzwierciedla zakres działań podejmowanych w celu wprowadzenia środków komunikacji elektronicznej do tego postępowania, ponieważ od początków informatyzacji włoskiego postępowania cywilnego starano się implementować rozwiązania dla całego przebiegu procesu[25]. Stosowanie środków komunikacji elektronicznej w procesie cywilnym ma stanowić remedium na problem zbyt długiego rozstrzygania spraw sądowych we Włoszech[26].

Podstawy prawne wprowadzenia rozwiązań elektronicznych były budowane we Włoszech od wielu lat. Mimo iż prawnie dopuszczono stosowanie elektronicznych dokumentów, elektronicznych akt oraz wymianę tych dokumentów drogą elektroniczną, nie korzystano z tych rozwiązań w wystarczającym zakresie. Już w latach 90. wprowadzono we Włoszech obowiązek sporządzania kopii elektronicznego systemu śledzenia i zarządzania sprawami sądowymi. Nie zmieniło to jednak podejścia do sporządzania akt sądowych,

[19] *A. Kulow*, Elektronische Signatur…, s. 540.
[20] *Ibidem*, s. 537.
[21] *Ibidem*.
[22] § 130 a ust. 1 ZPO w obecnym brzmieniu.
[23] § 130 a ust. 3 ZPO po nowelizacji.
[24] § 130 a ust. 6 ZPO po nowelizacji.
[25] Przykładem takiego projektu jest system, który rozwijano we Włoszech w latach 2000–2005 w siedmiu włoskich sądach. Już wtedy system *Processo Civile Telematico* (ang. *Trial On-Line*, dalej jako: TOL) obejmował funkcjonalności digitalizacji i elektronicznego wnoszenia dokumentów w postępowaniu cywilnym, wymianę informacji związanych z postępowaniem, zarządzanie aktami sprawy, elektroniczne powiadomienia i komunikację z sądem, dokonywanie płatności. W praktyce taki system nie zyskał popularności. Ostatecznie jednak system TOL, obecnie działający we Włoszech, dysponuje mniejszą liczbą funkcjonalności. *G. Lupo*, *J. Bailey*, Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples, Laws 2014, s. 358.
[26] *R. Caponi*, The Performance of the Italian Civil Justice System: An Empirical Assessment, The Italian Law Journal 2016, tom 2, Nr 01.

nadal część z nich była drukowana lub prowadzona w postaci papierowej[27]. W tym czasie do włoskiego systemu prawnego wprowadzono również koncepcję elektronicznego dokumentu oraz podpisu elektronicznego[28], co teoretycznie umożliwiło wymianę elektronicznych dokumentów. Nadal brakowało jednak technicznych rozwiązań, które pozwalałyby na faktyczne zastosowanie tych przepisów, a które wprowadzono dopiero później. Przepisy dotyczące stosowania środków komunikacji elektronicznej we Włoszech były jeszcze kilkukrotnie zmieniane, co spowodowało, że regulacje prawne dotyczące składania i doręczania dokumentów drogą elektroniczną są bardzo kompleksowe[29].

We Włoszech, po kilku próbach pilotażowych i regionalnych projektów, zdecydowano się na wprowadzenie powszechnego obowiązku posługiwania się drogą elektroniczną przy wnoszeniu pism do sądów. W literaturze wskazywano, że regionalne rozwiązania, umożliwiające wnoszenie pism procesowych drogą elektroniczną, ale niedostępne w niektórych częściach kraju, stanowią naruszenie prawa dostępu do sądu[30]. Wprowadzenie obowiązku składania pism procesowych elektronicznie następowało jednak stopniowo i uwzględniało poszczególne instancje sądów. W zakresie komunikacji sądów z pełnomocnikami i stronami obowiązek posługiwania się drogą elektroniczną wprowadzono od lutego 2013 r. dla sądów I i II instancji oraz od lutego 2016 r. dla SN. Składanie pism procesowych w nowych sprawach w sądach rejonowych obowiązkowo musi następować elektronicznie od czerwca 2014 r., a w sądach apelacyjnych od stycznia 2015 r.[31] Obecnie droga elektroniczna jest w zasadzie pierwotną formą wnoszenia pism do sądów we Włoszech i dotyczy to zarówno prawników, osób prawnych, jak i fizycznych[32].

Obecnie działający we Włoszech system TOL został zbudowany we współpracy Ministerstwa Sprawiedliwości i samorządów zawodowych adwokatów, działających w tym kraju. Za pośrednictwem systemu TOL jest udostępniany specjalny pulpit służący do przygotowania odpowiednich dokumentów, załączania zeskanowanych dokumentów, w tym potwierdzenia przelewu opłaty. TOL umożliwia także komunikację z sądem i między stronami[33]. Wszystkie dokumenty przesyłane przez ten system muszą zostać opatrzone podpisem elektronicznym[34]. Obecnie pisma oraz inne dokumenty elektroniczne są przesyłane do sądu za pośrednictwem certyfikowanej skrzynki e-mail[35].

Z systemu TOL korzysta we Włoszech ponad milion zewnętrznych użytkowników, w tym 250 000 prawników. W okresie od stycznia 2013 r. do maja 2016 r. odnotowano ponad 20 milionów elektronicznych czynności przeprowadzonych za pośrednictwem tego systemu, w tym każdego miesiąca użytkownicy zewnętrzni dokonują około 700 000 takich czynności[36].

Włochy w ciągu ostatnich 10 lat stały się jednym z wiodących krajów w zakresie informatyzacji postępowania cywilnego. Należy pozytywnie ocenić fakt, że aktualnie funkcjonujący system służący do wnoszenia dokumentów drogą elektroniczną bazuje na doświadczeniach wcześniejszych, regionalnych systemów, istniejących we Włoszech. Wprowadzenie bardzo szerokiego obowiązku posługiwania się komunikacją elektroniczną przy wnoszeniu i doręczaniu pism wydaje się dość drastycznym rozwiązaniem. Dane statystyczne dotyczące liczby prawników korzystających z systemu TOL oraz obsługiwanych czynności wskazują, że takie posunięcie włoskiego ustawodawcy zdecydowanie przyczyniło się do zwiększenia zakresu wykorzystania tego systemu.

Wnoszenie pism drogą elektroniczną we Francji

We Francji od wielu lat jest rozwijany system e-Barreau, który umożliwia wnoszenie oraz wymianę dokumentów elektronicznych między sądami a adwokatami[37]. Podobnie jak w większości krajów najpierw przyjęto regulacje prawne dopuszczające złożenie pism procesowych drogą elektroniczną, a następnie przystąpiono od budowania odpowiedniego systemu informatycznego[38]. Jak się okazało, najtrudniejsze było nie samo wdrożenie systemu informatycznego, ale stworzenie sieci podmiotów odpowiedzialnych za jego utrzymanie oraz zachęcenie użytkowników do korzystania z niego[39].

Zmiany we francuskim systemie prawnym pod kątem stosowania elektronicznej komunikacji wprowadziły ustawy

[27] *D. Carnevali*, *A. Resca*, The civil Trial On-Line (TOL): a true experience of e-justice in Italy, s. 10.

[28] Wspomniane przepisy przyjęto na podstawie dekretu Prezydenta Nr DPR 513/1997.

[29] *D. Carnevali*, *A. Resca*, The civil Trial On-Line…, s. 10–11.

[30] *G. Lupo*, *J. Bailey*, Designing and Implementing e-Justice Systems…, s. 361.

[31] Informacja na stronie włoskiego Ministerstwa Sprawiedliwości, E-justice in Italy: the „On-Line Civil Trial, maj 2016 r., źródło: https://pst.giustizia.it/PST/resources/cms/documents/eJustice_in_Italy_rev_May_2016.pdf (dostęp z 14.2.2017 r.).

[32] Od tej zasady minister sprawiedliwości może przewidzieć wyjątki dla poszczególnych postępowań. Por. art. 16bis ust. 5, Decreto-Legge 18 ottobre 2012, n. 179.

[33] *G. Lupo*, *J. Bailey*, Designing and Implementing e-Justice Systems…, s. 361.

[34] *Ibidem*, s. 359.

[35] *Ibidem*, s. 360.

[36] Informacja na stronie włoskiego Ministerstwa Sprawiedliwości, E-justice in Italy…

[37] System składa się z następujących systemów: RPVA (réseau privé virtuel avocat), zwanego też e-Barreau, funkcjonującego po stronie adwokatów i RPVJ (réseau privé virtuel justice) po stronie sądów; dalej jako: e-Barreau.

[38] *M. Velicogna*, *A. Errera*, *S. Derlange*, e-Justice in France: the e-Barreau experience, Utrecht Law Review, 2011, t. 7, wyd. 1, s. 164.

[39] *Ibidem*, s. 165.

Nr 659/1996[40] oraz 230/2000[41], które dopuściły korzystanie z podpisu elektronicznego, uregulowały skutki podpisywania dokumentów z wykorzystaniem tego podpisu oraz ich moc dowodową[42]. Wzorem dla implementacji e-Barreau był projekt e-Greffe, rozwijany od 2003 r. w sądzie I instancji w Paryżu, który umożliwiał dostęp do informacji o sprawie oraz pobieranie dokumentów elektronicznych (m.in. orzeczeń), a także komunikację z referendarzami za pośrednictwem wiadomości e-mail[43]. Dostęp do tego systemu był ograniczony do niektórych, z założenia prostych, postępowań[44]. Rozwijanie tego systemu nie korespondowało jednak ze zmianami w przepisach procedury cywilnej, więc część czynności wykonywanych za pośrednictwem tego systemu wymagało potwierdzenia w formie papierowej, co duplikowało liczbę wykonywanych czynności[45].

Od 2005 r. rozpoczęto prace nad projektem wspólnego dla całego kraju systemu, który umożliwił nie tylko uzyskiwanie informacji z sądu, lecz także dwustronną komunikację między sądami i profesjonalnymi pełnomocnikami. Nastąpiło to w ten sposób, że Ministerstwo Sprawiedliwości (jako podmiot reprezentujący sądy) oraz Krajowa Rada Adwokacka (*Conseil national des barreaux*) zobowiązały się dostosować istniejące systemy teleinformatyczne, tak aby możliwe było ich połączenie ze sobą, a także zapewnienie odpowiedniego poziomu bezpieczeństwa[46]. Ministerstwo Sprawiedliwości zobowiązało się dostosować istniejący w sądach system zarządzania sprawami. Krajowa Rada Adwokacka miała obowiązek podłączyć ich prywatną sieć do systemu sądowego.

Takie zabiegi wymagały zmian w przepisach postępowania. Do francuskiego kodeksu postępowania cywilnego dodano tytuł XXI „komunikacja drogą elektroniczną", obejmujący artykuły od 748-1 do 748-9[47]. Przepisy te dopuszczają skorzystanie z drogi elektronicznej w postępowaniu cywilnym odnośnie do m.in. przesyłek, doręczeń i powiadomień o dokumentach w postępowaniu cywilnym, pism, opinii, zawiadomień, wezwań, raportów, protokołów[48]. Adresat musi jednak wyraźnie zgodzić się na wykorzystanie środków elektronicznych, chyba że przepisy szczególne nakładają obowiązek korzystania z tego sposobu komunikacji[49]. Sąd otrzymuje elektroniczne poświadczenie odbioru, wysyłane przez odbiorcę, z podaniem daty oraz – w stosownych przypadkach – również godziny[50]. W przypadku skorzystania z komunikacji elektronicznej i przedłożenia do sądu dokumentu tą drogą, jesli składany dokument został sporządzony w oryginale w formie papierowej, sędzia może żądać jego przedstawienia[51]. Wykorzystanie drogi elektronicznej nie pozbawia strony prawa do żądania doręczenia orzeczenia sądowego, opatrzonego klauzulą wykonalności[52].

Francuski ustawodawca zdecydował również uregulować, co robić w sytuacji, gdy skorzystanie z drogi elektronicznej w ostatnim dniu terminu będzie niemożliwe z przyczyn niezależnych. W takim przypadku termin zostaje przedłużony do następnego dnia roboczego[53]. Co do zasady, wyżej opisane przepisy, stanowiące podstawę dla elektronicznej komunikacji, miały obowiązywać od 1.1.2009 r., ale zostały wprowadzone już w 2008 r. Oprócz opisanych regulacji, znajdujących się w CPC, Ministerstwo Sprawiedliwości i Krajowa Rada Adwokacka w związku z implementacją systemu przyjęły również wytyczne, które regulowały szczegółowe zasady wnoszenia pism do sądu drogą elektroniczną. Ponadto na potrzeby sądu kasacyjnego wprowadzono odrębny system informatyczny, z którego korzystanie jest jednak fakultatywne.

Wprowadzenie e-Barreau nie obyło się bez problemów. Niektórzy prawnicy bardzo niechętnie korzystali z tego systemu, w szczególności w związku z naliczanymi za korzystanie z niego opłatami[54]. Ponadto system umożliwiał wymianę dokumentów, ale do 2011 r. nie można było w tym trybie wnosić pism do sądu, ponieważ sądy nie miały możliwości weryfikowania podpisu elektronicznego[55].

We francuskim systemie prawnym można zauważyć tendencję wprowadzania obowiązkowej elektronicznej komunikacji z sądem, z tym że w procedurze cywilnej obowiązek ten został na razie ograniczony do sądów odwoławczych. Wnoszenie pism procesowych do tych sądów musi następować drogą elektroniczną. Jeśli jednak z przyczyn niezależnych skorzystanie z tej drogi będzie niemożliwe, pisma można wnieść w formie papierowej do sekretariatu sądu w liczbie egzemplarzy przeznaczonej dla każdego odbiorcy oraz dodatkowo dwóch odpisach. Komunikacja między pełnomocnikiem a sądem jest co do zasady prowadzona elektronicznie[56]. Od 1.1.2017 r. wprowadzono również obowiązkowe wnoszenie drogą elektroniczną skarg do Rady Państwa (*le Conseil d'Etat*)

[40] Zob. loi n° 96–659 du 26 juillet 1996 de réglementation destélécommunications.

[41] Zob. loi n° 2000–230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique.

[42] *M. Velicogna*, *A. Errera*, *S. Derlange*, e-Justice in France…, s. 169.

[43] *Ibidem*, s. 170.

[44] *Ibidem*, s. 171.

[45] *Ibidem*, s. 172.

[46] Na mocy porozumień zawartych między Ministerstwem Sprawiedliwości i Krajową Radą Adwokacką z 4.5.2005 r., 28.9.2007 r. oraz 10.6.2010 r.

[47] Code de procédure civile, dalej jako: CPC. Zmiany wprowadzono m.in. dekretem Nr 2009-1524 z 9.12.2009 r. (décret n°2009-1524 du 9 décembre 2009, JORF n°0287).

[48] Art. 748-1 CPC.

[49] Art. 748-2 CPC.

[50] Art. 748-3 CPC.

[51] Art. 748-4 CPC.

[52] Art. 748-5 CPC.

[53] Art. 748-7 CPC

[54] *M. Velicogna*, *A. Errera*, *S. Derlange*, e-Justice in France…, s. 175 i 180.

[55] *Ibidem*, s. 178.

[56] Art. 930-1 CPC wprowadzony dekretem Nr 2009-1524 z 9.12.2009 r. dotyczącym postępowania odwoławczego z obowiązkowym zastępstwem w sprawach cywilnych (décret n° 2009–1524 du 9 décembre 2009 relatif à la procédure d'appel avec représentation obligatoire en matière civile).

oraz sądów administracyjnych i odwoławczych sądów administracyjnych[57].

Na uwagę zasługuje fakt, że system e-Barreau jest dalej rozwijany. Producenci systemów informacji prawnej, np. LexisNexis oraz Wolters Kluwer, oferują oprogramowanie wspierające pracę prawników oraz jednocześnie odpowiednio skorelowane z systemem e-Barreau[58]. System ten nie tylko jest dostępny przez stronę internetową, lecz także została udostępniona aplikacja mobilna[59].

System e-Barreau we Francji również czerpie ze wzorców wcześniej istniejącego rozwiązania regionalnego, ale stopniowo są dodawane nowe funkcjonalności. Jednocześnie obowiązek posługiwania się drogą elektroniczną przy wnoszeniu pism i dokumentów do sądów również rozszerza się na nowe postępowania. W przypadku tego systemu także można zauważyć, że został stworzony w ramach ścisłej współpracy z francuskim samorządem adwokatów.

Podsumowanie

W opisywanych państwach podstawy prawne wnoszenia dokumentów drogą elektroniczną istniały już wiele lat, jednak mimo to również w tych krajach raczej niechętnie korzystano z komunikacji elektronicznej w kontaktach z sądami. Spowodowało to w ostatnich latach wprowadzenie zmian w przepisach.

Na podstawie opisanych przykładów państw, w których uregulowano kwestie związane z wnoszeniem pism procesowych drogą elektroniczną, można zaobserwować tendencję do wprowadzania co najmniej częściowego obowiązku posługiwania się tym sposobem komunikacji z sądem. Taki obowiązek jest nakładany na podmioty profesjonalne, tj. przede wszystkim adwokatów. W komunikacji elektronicznej z sądami najczęściej do weryfikacji podmiotów oraz podpisywania dokumentów przewidziano podpis elektroniczny. Eksperymentuje się jednak również z innymi metodami weryfikacji nadawców pism procesowych składanych elektronicznie (np. systemy De-Mail, EGVP w Niemczech).

Wprowadzenie obowiązku korzystania z drogi elektronicznej wymaga jednak odpowiednio rozwiniętego, sprawdzonego oraz funkcjonującego już co najmniej kilka lat systemu teleinformatycznego. Dopiero poprawnie działający system w wersji podstawowej może stanowić bazę do wprowadzania do systemu dodatkowych funkcjonalności (np. rozwijanie aplikacji mobilnej, łączenie systemów służących do składania pism do sądu z programami do zarządzania sprawami/kancelarią). Wydaje się, że warunkiem koniecznym budowy takiego systemu jest ścisła współpraca przy jego tworzeniu przez reprezentantów ze strony sądów oraz odpowiednich zrzeszeń podmiotów profesjonalnych, tak aby jak najbardziej funkcjonalnie połączyć systemy ze sobą.

[57] Art. 3 dekretu Nr 2016-1481 z 2.11.2016 r. dotyczącego stosowania postępowań zdalnych przed Radą Państwa, sądami administracyjnymi i odwoławczymi sądami administracyjnymi (Décret n° 2016-1481 du 2 novembre 2016 relatif à l'utilisation des téléprocédures devant le Conseil d'Etat, les cours administratives d'appel et les tribunaux administratifs, JORF n°0257).

[58] *M. Velicogna*, *A. Errera*, *S. Derlange*, e-Justice in France…, s. 182.

[59] Zob. https://itunes.apple.com/fr/app/e-barreau-mobile/id820-341024?l=fr&ls=1&mt=8 (dostęp z 14.2.2017 r.).

Słowa kluczowe: elektroniczne biuro podawcze, wnoszenie dokumentów drogą elektroniczną do sądu, systemy teleinformatyczne w sądownictwie, informatyzacja postępowania cywilnego, postępowanie cywilne.

Functioning of electronic incoming correspondence logs in chosen European countries

The aim of this paper is to present solutions that have been adopted in chosen European countries (Germany, Italy and France) in order to build an electronic incoming correspondence log in regard to civil proceedings. Despite the fact that basic provisions concerning electronic documents, electronic signatures and alternatively use of electronic means have been already implemented for many years, courts were not adjusted to the requirements of electronic incoming correspondence logs and also participants of the civil proceedings were reluctant to use this option, because they were unsure about this form of e-justice. For a proper functioning of an electronic incoming correspondence log, an IT system has to be designed and implemented, but the existing systems in described countries were only regional systems or could not be used in every court. In order to solve those problems, Germany, Italy and France decided to improve or rebuilt their electronic incoming correspondence logs and at least partly adopt an obligation to the professionals to use this system. This article presents amendments concerning the use of electronic communication with courts in the legal provisions in chosen countries. An outcome of the article may be some possible solutions for other jurisdictions on how to deal with various problems concerning implementation of an electronic incoming correspondence log.

Key words: *electronic incoming correspondence log, electronic filing of documents to the court, IT systems in judiciary, e-justice in civil proceedings, civil proceedings.*

Analiza i praktyczne uwagi w zakresie konstrukcji i stosowania prawa do bycia zapomnianym w UE

Marcin Rojszczak[1]

Regulacje prawne związane z ochroną danych osobowych ewoluują w kierunku umożliwienia jednostkom skutecznej kontroli informacji ich dotyczących publikowanych w sieci Internet. Na świecie w awangardzie zmian w tym zakresie od lat znajduje się UE, w której prawa i wolności osobiste są trwale zagwarantowane w Karcie Praw Podstawowych. Bezkompromisowa ochrona praw jednostki jest wzmacniana zarówno przez prawodawcę unijnego, jak i przez orzeczenia sądów konstytucyjnych państw członkowskich oraz Trybunału Sprawiedliwości UE.
Celem niniejszego opracowania jest przedstawienie najważniejszych zasad prawa do bycia zapomnianym oraz analiza, czy obecny kształt tego prawa, będący następstwem orzeczeń TS, nie wpływa negatywnie na gwarancje związane z innymi prawami podstawowymi, takimi jak prawo do informacji czy swobody wypowiedzi.

Uwagi wstępne[2]

Wraz z rozwojem usług informacyjnych duża część aktywności zawodowej i osobistej jest realizowana z wykorzystaniem Internetu. Każdego roku przybywa nowych e-usług, a istniejące podlegają transformacji i udoskonaleniu. Coraz więcej osób posiada po kilka profili na różnych portalach społecznościowych, za pomocą których prowadzi rozbudowaną korespondencję skierowaną do wszystkich użytkowników Internetu, wzbogaconą licznymi zdjęciami i treściami multimedialnymi z ich życia prywatnego. Zaawansowane algorytmy przetwarzania coraz częściej potrafią skutecznie korelować bardzo rozbudowane zbiory danych – w efekcie pozwalając np. na automatyczne rozpoznawanie produktów, miejsc czy twarzy na publikowanych zdjęciach. Dzięki analizowaniu aktywności użytkowników oraz korelowaniu rozproszonych zbiorów danych możliwe jest także prognozowanie zdarzeń przyszłych.

Niestety, nadal zrozumienie złożoności współczesnych usług informatycznych jest wśród ich użytkowników stosunkowo niewielkie. Udostępnianie dużej ilości danych osobistych nieokreślonej grupie osób, korzystanie z nowych – często dobrze niepoznanych – usług społecznościowych oraz bezrefleksyjne akceptowanie nowych polityk prywatności, wprowadzanych przez usługodawców, prowadzi do stopniowej utraty kontroli nad obiegiem informacji dotyczących sfery prywatności.

Osoby, które zdały sobie sprawę z tej sytuacji i chciałyby odzyskać kontrolę nad informacjami rozpowszechnianymi na ich temat, do niedawna trafiały w legislacyjną próżnię i były zdane na dobrą wolę poszczególnych usługodawców internetowych i regulacji wynikających z – często bardzo rozbudowanych i niejasnych – regulaminów świadczenia usług. Opisana luka wynika z faktu, że istniejące regulacje dotyczące danych osobowych – zarówno na poziomie krajowym (ustawa z 29.8.1997 r. o ochronie danych osobowych[3]), jak i europejskim (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[4]) – zostały opracowane i przyjęte do stosowania w latach dziewięćdziesiątych XX w. – a więc w czasach, gdy znany nam obecnie Internet jeszcze nie istniał.

Przyjęta w 1997 r. Konstytucja RP nie definiuje wprost prawa do ochrony danych osobowych – jest ono wywodzone z ogólnych gwarancji dotyczących prawa do prywatności (art. 47) oraz ochrony informacji o sobie (art. 51). Zgodnie z art. 47 każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Natomiast poszczególne przepisy art. 51 wprowadzają dodatkowe gwarancje związane z gromadzeniem i przetwarzaniem danych osobowych, ale – jak wskazuje się w doktrynie – ich zakres podmiotowy i przedmiotowy jest węższy niż wynikający z art. 47. W takim przypadku prawa jednostek i obowiązki podmiotów przetwarzających powinny być wywodzone bezpośrednio z art. 47 Konstytucji RP[5].

Prywatność obejmuje w szczególności ochronę informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności (zwanej autonomią informacyjną), w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym informacji o swoim życiu[6]. Autonomia informacyjna stanowi zatem istotny element składowy prawa do prywatności i może być zdefiniowana jako prawo do samodzielnego decydowania o ujawnianiu innym

[1] Autor jest absolwentem prawa i informatyki, doktorantem Instytutu Nauk Prawnych PAN.

[2] Stan prawny oraz odnośniki internetowe aktualne na 2.11.2017 r.

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

[4] Dz.Urz. UE L Nr 281, s. 31; dalej jako: dyrektywa 95/46.

[5] Zob. np. rozważania dot. podmiotów uprawnionych i zobowiązanych na tle art. 51 ust. 1 – *M. Wild*, Komentarz do art. 51, Nb 16, [w:] *M. Safjan*, *L. Bosek* (red.), Warszawa Konstytucja RP. Tom I. Komentarz do art. 1–86, Warszawa 2016.

[6] Zob. wyrok TK z 19.5. 1998 r., U 5/97, OTK 1998, Nr 4, poz. 46.

informacji dotyczących swojej osoby oraz prawo do sprawowania kontroli nad tymi informacjami znajdującymi się w posiadaniu innych podmiotów[7]. W szczególności wyrazem korzystania z autonomii informacyjnej może być żądanie usunięcia określonych informacji z przestrzeni publicznej. W takim rozumieniu prawo do usunięcia danych dopełnia uprawnień jednostki dotyczących kontrolowania zakresu informacji dostępnych na jej temat w przestrzeni publicznej[8].

Sąd Najwyższy zajmuje obecnie stanowisko, że przy wykładni krajowych przepisów związanych z ochroną danych osobowych nie można pominąć dyrektywy 95/46, w której już na wstępie podkreślono, że systemy przetwarzania danych są tworzone po to, aby służyły człowiekowi, i muszą one szanować podstawowe prawa i wolności osób fizycznych, a szczególnie prawo do prywatności[9].

Istniejące przepisy nie dość precyzyjnie definiowały prawa jednostki do żądania usunięcia danych przetwarzanych na jej temat, nawet jeżeli te informacje były prawdziwe i nie naruszały innych przepisów.

Sytuacja w ostatnich latach zaczęła się powoli zmieniać na skutek precedensowego wyroku TS w sprawie *Google Spain*[10] oraz uwzględnienia w przyjętym w 2016 r. rozporządzeniu 2016/679[11] przepisów wprowadzających tzw. prawo do bycia zapomnianym (a ściślej: prawo do usunięcia danych). Szczególnie interesujące wydają się prawne konsekwencje związane z wejściem w życie RODO, co nastąpi 25.5.2018 r.

Okoliczności sprawy Google Spain

Aby zrozumieć formalną koncepcję prawa do bycia zapomnianym, należy przybliżyć najważniejsze okoliczności oraz tezy wyroku TS wydanego w sprawie *Google Spain*. Trybunał udzielił odpowiedzi na pytania prejudycjalne dotyczący sporu pomiędzy Google Spain SL i Google Inc. a hiszpańskim Urzędem Ochrony Danych Osobowych (Agencia Española de Protección de Datos, AEPD). Przedmiotem sporu była skarga obywatela Hiszpanii skierowana do AEPD w zakresie nakazania spółce Google zaprzestania przetwarzania informacji na jego temat, które – w jego ocenie – wpływały negatywnie na jego osobę, budując nieprawdziwy i mylny wizerunek wśród użytkowników Internetu. W szczególności po wpisaniu w okno wyszukiwania imienia i nazwiska skarżącego wyszukiwarka przedstawiała linki do artykułów dotyczących licytacji komorniczej majątku skarżącego, która miała miejsce wiele lat wcześniej. Już na tym etapie warto podkreślić kilka faktów, które będą istotne w dalszych rozważaniach nad zakresem i celowością wprowadzania do porządku prawnego prawa do bycia zapomnianym. Po pierwsze, zarówno skarżący, jak i w dalszym etapie postępowania AEPD nie kwestionowali prawdziwości opublikowanych informacji. Ponadto nie podniesiono także zarzutu, że udostępnione informacje były wprowadzone nielegalnie do domeny publicznej lub z naruszeniem praw majątkowych osób trzecich. Co więcej, adresatem żądania był nie tylko właściciel i operator wyszukiwarki internetowej (Google), lecz także wydawca dziennika La Vanguardia, w którym opublikowany został kwestionowany artykuł źródłowy. W odniesieniu do wydawcy La Vanguardia żądano usunięcia kwestionowanych treści, natomiast od Google – przyjęcia środków koniecznych do usunięcia danych osobowych dotyczących skarżącego z jej indeksu oraz uniemożliwienia dostępu do tych danych w przyszłości. Hiszpański organ nadzoru zdecydował się częściowo uwzględnić żądanie skarżącego. Mianowicie zobowiązał Google do usunięcia odniesień do kwestionowanych tekstów w dzienniku La Vanguardia, ale jednocześnie odrzucił żądania adresowane do wydawcy samego dziennika, wskazując, że usunięcie lub modyfikowanie źródłowych ogłoszeń opublikowanych na stronach internetowych nie jest potrzebne, ponieważ informacje te zostały opublikowane w ramach obowiązującego prawa (w rzeczywistości były to urzędowe ogłoszenia o licytacji komorniczej – znane, choć w innej formie, także w Polsce). AEPD uznał zatem, że chociaż sama informacja była opublikowana zgodnie z prawem, to jej dalsze rozpowszechnianie przez Google może naruszać interesy skarżącego. Na skutek odwołania przez Google oraz pytania prejudycjalnego zadanego przez hiszpański sąd sprawa zawisła przed TS.

Aby zrozumieć wywód prawny przedstawiony w uzasadnieniu wyroku Trybunału, a także jego implikacje w postaci prawa do bycia zapomnianym w kształcie wprowadzonym w RODO, omówienia wymaga prawna definicja administratora danych. Zgodnie z legalną definicją przedstawioną w art. 7 pkt 4 OchronaDanychU administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba decydujący o celach i środkach przetwarzania danych osobowych. Podobna definicja funkcjonuje na gruncie nadal obowiązującej dyrektywy 95/46. Zgodnie z art. 2 ust. d przez pojęcie administratora danych należy rozumieć osobę fizyczną lub prawną, organ publiczny, agencję lub inny organ, który samodzielnie lub wspólnie z innymi określa cele i sposoby przetwarzania danych osobowych.

Jedną z osi sporu, którą musiał rozstrzygnąć Trybunał, było ustalenie, czy koncern Google (lub operator innej wyszukiwarki internetowej) może być uznany za administratora

[7] Zob. wyrok SN z 11.2.2015 r., I CSK 868/14, Legalis.

[8] Por. np. argumentację uzasadniającą potrzebę wprowadzenia prawa do bycia zapomnianym w: *M. Fazlioglu*, Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet, International Data Privacy Law 2013, Nr 3, s. 149–150.

[9] Zob. wyrok SN z 15.2.2008 r., I CSK 358/07, OSNC 2009, Nr 4, poz. 63.

[10] Wyrok TS z 13.5.2014 r., *Google Spain SL v. AEPD*, C-131/12, ECLI:EU:C:2014:317.

[11] 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 (Dz.Urz. UE L Nr 119, s. 1); dalej jako: RODO.

danych. Innymi słowy – czy indeksowanie informacji dostępnych w sieci Internet, które niewątpliwie pod kątem *stricte* technicznym jest przetwarzaniem danych, jest także przetwarzaniem na gruncie przepisów o ochronie danych osobowych. W konsekwencji – czy na przedsiębiorcę przetwarzającego w ten sposób dane można nałożyć obowiązki analogiczne do innych administratorów danych. Trybunał Sprawiedliwości w pkt 43 wyroku stwierdził, że prowadzoną przez operatorów wyszukiwarek internetowych działalność, która polega na zlokalizowaniu informacji opublikowanych lub zamieszczonych w Internecie przez osoby trzecie, indeksowaniu ich w sposób automatyczny, czasowym przechowywaniu takich informacji i wreszcie udostępnianiu ich internautom w sposób uporządkowany zgodnie z określonymi preferencjami, w sytuacji gdy informacje takie zawierają dane osobowe, należy uznać za „przetwarzanie danych osobowych", a w konsekwencji operatora tej wyszukiwarki należy uznać za „administratora" odpowiedzialnego za przetwarzanie danych w rozumieniu przepisów prawa. Oczywistą i bezpośrednią konsekwencją takiej decyzji jest możliwość skorzystania przez każdą osobę, której dane są przetwarzane, z prawa do cofnięcia zgody na przetwarzanie danych – a w efekcie doprowadzenia do konieczności korygowania indeksu wyszukiwarki w sposób odzwierciedlający takie żądanie.

Trybunał w swoim wyroku stwierdził ponadto w sposób niebudzący wątpliwości, że żądanie dotyczące usunięcia danych z wyszukiwarki internetowej jest uprawnieniem niezależnym i niezwiązanym z żądaniem usunięcia takich danych z serwisu internetowego, który informacje te oryginalnie opublikował. W efekcie żądanie powinno być zrealizowane także w przypadku, gdy kwestionowane informacje nie zostały uprzednio czy jednocześnie usunięte ze źródłowych stron internetowych, a nawet wtedy gdy ich publikacja na tych stronach jest zgodna z prawem. Jednakże TS w tym zakresie słusznie zauważył, że „biorąc pod uwagę łatwość, z jaką informacje opublikowane na stronie internetowej mogą zostać skopiowane, oraz okoliczność, że podmioty odpowiedzialne za ich publikację nie zawsze podlegają przepisom prawa Unii, cel polegający na skutecznej i pełnej ochronie osób, których dotyczą dane, nie mógłby być zrealizowany bez uprzedniego czy też jednoczesnego uzyskania usunięcia dotyczących ich informacji przez wydawców stron internetowych"[12].

W tym miejscu pojawia się pierwszy oczywisty problem techniczny, który wymyka się normom prawnym. W przypadku tradycyjnych baz danych żądanie usunięcia danych osobowych realizowane jest w sposób bezpośredni – poprzez trwałe skasowanie rekordu bazy danych i powiązanych z nim relacji, które dotyczą osoby występującej z żądaniem. Specyfika wyszukiwarek internetowych jest jednak inna. Baza danych jest tworzona dynamicznie, odzwierciedlając zmiany wprowadzane w indeksowanych stronach. Jakakolwiek ręczna manipulacja w bazie danych związana z usunięciem rekordów jest z definicji tylko tymczasowa, ponieważ po ponownym zindeksowaniu źródłowej strony internetowej zawartość bazy zostanie odtworzona. Prowadzi to do potrzeby nie tyle usunięcia danych z rejestru wyszukiwarki, ile dodania nowego mechanizmu, odpowiedzialnego za „cenzurowanie" informacji wyświetlanych użytkownikom wyszukiwarki. W przypadku wyszukiwarek nie należy więc mówić o faktycznym usunięciu informacji z bazy danych (byłoby to bowiem działanie bezcelowe), a o filtrowaniu wyników wyszukiwania i usuwaniu z nich odniesień do stron zawierających informacje o osobach, które wystąpiły z żądaniem usunięcia danych. To z kolei prowadzi do wielu problemów praktycznych. Na przykład w jaki sposób zrealizować żądanie, jeżeli wnioskującym jest osoba o popularnym (lub chociaż powtarzalnym) imieniu i nazwisku. Czy w takim przypadku operator wyszukiwarki internetowej powinien skasować wpisy dotyczące wszystkich stron, odnoszące się wszystkich osób posiadających to imię i nazwisko? Co w przypadku, gdy wnioskodawca posiada imię i nazwisko identyczne z inną osobą pełniącą funkcje publiczne? Co jeżeli tą osobą jest czynny polityk, kandydujący w zbliżających się wyborach?

Na inny aspekt słusznie wskazują *E. Michałkiewicz* i *E. Milczarek*, zwracając uwagę na możliwość nadużycia prawa do usunięcia danych w kontekście osób skazywanych wcześniej za przestępstwa, zwłaszcza związane z wolnościami seksualnymi i obyczajnością[13]. W efekcie wzmocnienia praw jednostki dojść może do sytuacji, w której rodzice zostaną pozbawieni dostępu do informacji, że w miejscowości, do której chcą się przeprowadzić, mieszka osoba wielokrotnie karana za czyny o charakterze pedofilskim.

W związku z powyższym oczywiste jest, że wniosek związany z usunięciem danych musi być ręcznie analizowany przez operatora wyszukiwarki. Treść serwisów internetowych często nie pozwala na jednoznaczne określenie, czy publikowane materiały dotyczą osoby, która wystąpiła z wnioskiem, a to z kolei może prowadzić do wielu błędów i nadużyć.

Przykładem obszaru wymagającego dalszego doprecyzowania jest możliwość objęcia prawem do bycia zapomnianym danych zgromadzonych w udostępnionych w Internecie rejestrach państwowych, ze szczególnym uwzględnieniem danych historycznych. Problem ten stał się podstawą sprawy, która zawisła przed TS na skutek wniosku o wydanie orzeczenia w trybie prejudycjalnym złożonym przez włoski trybunał kasacyjny. Jak wskazał rzecznik generalny *Y. Bot* w wydanej 8.9.2016 r. opinii, kwestią problematyczną w niniejszej sprawie było, czy organy krajowe prowadzące rejestry spółek po upływie określonego czasu od zakończenia działalności podmiotu i na wniosek zainteresowanej osoby powinny de-

[12] Wyrok *Google Spain SL v. AEPD*, s. 84.

[13] *E. Michałkiewicz*, *E. Milczarek*, Prawo do prywatności w dobie Internetu, PME 2015, Nr 2, s. 59.

cydować o wykreśleniu lub poddaniu anonimizacji jej danych osobowych zawartych w rejestrze albo o ograniczeniu ich jawności poprzez zawężenie kręgu uprawnionych odbiorców informacji[14].

W opinii rzecznika rejestry publiczne, takie jak rejestr spółek, mogą realizować swój podstawowy cel, jakim jest wzmocnienie bezpieczeństwa obrotu gospodarczego, tylko w sytuacji, gdy dostęp do nich jest zagwarantowany dla każdego bez ograniczeń czasowych. Dlatego w takim przypadku możliwość z korzystania z prawa do bycia zapomnianym powinna być ograniczona. W wyroku z 9.3.2017 r. Trybunał co do zasady podzielił stanowisko rzecznika, wskazując na szczególną rolę jawności informacji na temat tożsamości i funkcji osób, upoważnionych do nadzorowania i kontrolowania spółek, bądź ich reprezentowania wobec osób trzecich[15]. Jednocześnie uznał jednak, że w szczególnych sytuacjach nie można wykluczyć, że prawa podmiotu danych do ochrony prywatności powinny przeważyć nad prawami osób trzecich w dostępie do informacji zgromadzonych w jawnym rejestrze publicznym[16]. Przykładem może być upływ wystarczająco długiego okresu od daty likwidacji podmiotu, w którym pełniła funkcję dana osoba. Decyzja związana z możliwością wprowadzenia takich ograniczeń należy do kompetencji państw członkowskich. W ten sposób Trybunał wskazał, że prawodawcy krajowi, uwzględniając specyfikę bezpieczeństwa obrotu gospodarczego, mogą wprowadzić rozwiązania pozwalające na realizację prawa do usunięcia danych także w odniesieniu do informacji zgromadzonych w rejestrach publicznych.

Zasięg terytorialny prawa do bycia zapomnianym

Trybunał Sprawiedliwości w sprawie *Google Spain* rozstrzygnął, w jaki sposób prawo do bycia zapomnianym powinno być stosowane przez operatorów internetowych posiadających siedzibę poza obszarem UE. Wszystkie główne wyszukiwarki internetowe są serwisami o zasięgu globalnym. Chociaż wyniki wyszukiwania są personalizowane dla konkretnego użytkownika, z uwzględnieniem państwa, w którym przebywa, czy języka, jakim się posługuje, to jednak w tle funkcjonuje ten sam mechanizm indeksujący – a więc ta sama, choć bardzo rozbudowana i rozproszona, baza danych. Powstają zatem dwa kolejne problemy. Po pierwsze, jaki powinien być zakres terytorialny stosowania prawa do bycia zapomnianym, a po drugie – czy prawo to powinno dotyczyć także przedsiębiorców posiadających siedzibę poza terytorium UE.

Analiza powyższych zagadnień musi uwzględniać, że zarówno użytkownik przeglądarki (lub innego publicznego serwisu internetowego), jak i osoba, która chce ograniczyć dostęp do informacji na swój temat, mogą być obywatelami różnych państw, niekoniecznie należących do UE. Ponadto niezależnie od swojej narodowości mogą przebywać w państwach trzecich, które mogą mieć odmienne przepisy dotyczące ochrony danych osobowych. Zgodnie z wyrokiem TS operatorzy przeglądarek powinni zapewnić respektowanie prawa do bycia zapomnianym na terenie UE. Oznacza to, że filtrowanie wyników powinno być stosowane w odniesieniu do użytkowników przebywających na terenie Unii, co prowadzi do wniosku, że w zależności od miejsca pobytu, wpisując tę samą frazę w wyszukiwarce internetowej, możliwe jest uzyskanie różnych wyników.

Problem ten został dostrzeżony przez francuski krajowy organ nadzoru (Commission nationale de l'informatique et des libertés – CNIL), który po przeprowadzeniu postępowania wyjaśniającego 21.5.2015 r. wydał decyzję zobowiązującą Google do wprowadzenia mechanizmów globalnego filtrowania wyników wyświetlanych przez wyszukiwarkę. Ponieważ Google nie dostosował się do tej decyzji, 10.3.2016 r. na przedsiębiorcę nałożona została grzywna w wysokości 100 000 euro[17]. CNIL uznał, że jakkolwiek przeglądarka internetowa Google jest rozbudowanym systemem informatycznym, to za generowanie wyników prezentowanych w różnych państwach odpowiada ten sam algorytm. Skuteczne wdrożenie wyroku *Google Spain* wymaga zatem, aby kwestionowane przez jednostki treści nie były udostępniane na wszystkich rynkach, na jakich działa operator, a nie tylko w państwie, w którym wnioskodawca ma miejsce pobytu. CNIL wskazał ponadto, że globalne filtrowanie wyników wyszukiwania nie wpłynie na ograniczenie prawa do informacji, bowiem kwestionowane treści będą dostępne w indeksie wyszukiwarki po wprowadzeniu innych haseł niż imię i nazwisko osoby, która pragnie skorzystać z prawa do bycia zapomnianym. Warto w tym miejscu zaznaczyć, że podtrzymanie decyzji CNIL na drodze sądowej i utrwalenie tego poglądu w orzecznictwie europejskim doprowadziłoby do sytuacji, w której sądy państw członkowskich UE mogłyby kształtować treści prezentowane przez wyszukiwarki internetowe w państwach trzecich[18].

Drugi z zaznaczanych wcześniej problemów – a więc określenie przedsiębiorców internetowych, wobec których można egzekwować prawo do bycia zapomnianym – ma oczywiste znaczenie praktyczne. Według danych z września 2017 r., sześć z 10 największych portali społecznościowych

[14] Opinia Rzecznika Generalnego Y. Bota z 8.9.2016 r., C-398/15, ECLI:EU:C:2016:652, s. 32.

[15] Wyrok TS z 9.3.2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. S. Manni*, C-398/15, ECLI:EU:C:2017:197, s. 32.

[16] *Ibidem*, s. 60.

[17] Decyzja CNIL z 10.3.2016 r., 2016-054, https://goo.gl/sycKpf .

[18] Reuters, Google appeals French order for global 'right to be forgotten', http://www.reuters.com/article/us-google-france-privacy-idUSKCN0YA1D8.

według liczby aktywnych użytkowników jest zarządzanych przez przedsiębiorców mających siedzibę w Stanach Zjednoczonych, natomiast pozostałe cztery przez podmioty zarejestrowane w Chinach[19]. W efekcie – niejako z definicji – analizowane prawo będzie adresowane do usługodawców nieprowadzących podstawowej działalności w UE. Wskazać należy, że zgodnie z dyrektywą 95/46 o jej stosowaniu można mówić, m.in. gdy przetwarzanie danych odbywa się w kontekście prowadzenia przez administratora danych działalności gospodarczej na terytorium państwa członkowskiego (art. 4 ust. 1 pkt a) lub gdy administrator danych nie prowadzi działalności gospodarczej na terytorium Unii, ale do celów przetwarzania danych osobowych wykorzystuje środki, zarówno zautomatyzowane, jak i inne, znajdujące się na terytorium państwa członkowskiego, o ile środki te nie są wykorzystywane wyłącznie do celów tranzytu przez terytorium UE (art. 4 ust. 1 pkt b). Trybunał musiał zatem rozstrzygnąć, czy przedsiębiorca internetowy posiadający siedzibę oraz centra przetwarzania danych poza obszarem UE powinien – a jeżeli tak, to w jakim zakresie – realizować prawo do bycia zapomnianym. Trybunał przeanalizował ten problem i wskazał, że do uznania, że przedsiębiorca prowadzi na terenie państwa członkowskiego UE działalność podlegającą unijnym regulacjom związanym z danymi osobowymi wystarczy, aby ustanowił w danym państwie oddział lub spółkę zależną, których celem jest promocja i sprzedaż powierzchni reklamowych oferowanych za pośrednictwem głównej usługi internetowej, a działalność tego oddziału lub tej spółki była skierowana do osób zamieszkujących to państwo[20].

Z kolei w sprawie *Weltimmo*[21] TS wprowadził elastyczne warunki uznania, że czynności przetwarzania danych odbywają się w kontekście działalności gospodarczej prowadzonej w UE. W ocenie Trybunału przesłanką taką może być np. zredagowanie strony internetowej usługodawcy w języku powszechnie wykorzystywanym w tym państwie członkowskim lub przyjmowanie płatności w walucie danego państwa członkowskiego[22]. Wyrok ten doprowadził do dalszego powiększenia kręgu zagranicznych usługodawców, zobowiązanych do stosowania europejskich przepisów o ochronie danych. Nadal jednak, na gruncie dyrektywy 95/46, czynności przetwarzania realizowane poza UE i przez przedsiębiorcę zagranicznego, które nie były ukierunkowane na obywateli Unii, nie musiały być realizowane zgodnie z unijnymi przepisami.

Naturalną konsekwencją przedstawionej przez Trybunał wykładni przepisów przepisów może być utrudnienie prowadzenia działalności gospodarczej przedsiębiorcom unijnym i zachęcenie, aby rozbudowane usługi internetowe były świadczone spoza obszaru UE. Operator wyszukiwarki internetowej, który zarejestrował podmiot zależny w dowolnym kraju UE, musi podporządkować się europejskim przepisom o ochronie danych. Operator wyszukiwarki internetowej, który prowadzi identyczną działalność w taki sam sposób, ale nie posiada oddziału lub spółki zależnej na terytorium dowolnego państwa UE i nie kieruje wprost swoich usług na rynek państw członkowskich – tych samych przepisów stosować nie musi. Przy czym obaj przedsiębiorcy konkurują ze sobą i kierują swoje usługi do tego samego grona odbiorców, w dużej części obywateli UE.

Sytuacja ta zmieni się wraz z wejściem w życie RODO, w którym w art. 3 doprecyzowano zakres podmiotów zobowiązanych, uwzględniając także przedsiębiorców nieposiadających jednostek organizacyjnych w Unii, jednak przetwarzających dane obywateli UE, oferujących im towary lub usługi, a także monitorujących ich zachowania.

Problemy interpretacyjne

Jakkolwiek wyrok Trybunału dotyczy konkretnej sprawy i okoliczności w niej przedstawionych, jest oczywiste, że z uwagi na swoją doniosłość tezy w nim zawarte stały się podstawą do dyskusji na temat praktycznych implikacji stosowania prawa do bycia zapomnianym. W pierwszej kolejności należy wskazać, że Trybunał swoim orzeczeniem znacząco wzmocnił prawne mechanizmy ochrony prywatności wynikające z art. 7 (poszanowanie życia prywatnego i rodzinnego) oraz art. 8 (ochrona danych osobowych) Karty Praw Podstawowych[23]. Jednocześnie wzbudził jednak liczne obawy dotyczące ograniczenia wolności wypowiedzi i informacji, także zagwarantowanych w Karcie. Internet i informacje przesyłane za jego pośrednictwem stały się jednym z filarów rozwoju społeczeństwa informacyjnego. Serwisy społecznościowe służą nie tylko komunikacji pomiędzy rodziną czy gronem znajomych, ale również mają istotne znaczenie w budowaniu świadomości obywatelskiej – czego przykłady można było zaobserwować w trakcie tzw. arabskiej wiosny czy nieudanego puczu wojskowego w Turcji[24]. W obu przypadkach wiadomości przekazywane za pośrednictwem popularnych sieci społecznościowych były źródłem informacji dla milionów obywateli na temat sytuacji wewnętrznej w ich państwach, w efekcie przyczyniając się do rozwoju protestów społecznych i wpływając na przemiany polityczne. Z kolei popularność przeglądarek internetowych stała się motorem rozwoju dziennikarstwa niezależnego i wpłynęła na powstanie wielu nieznanych wcześniej jego form, takich jak blogi czy kanały *podcast*.

[19] The Statistics Portal, https://goo.gl/WCimA8.
[20] Wyrok *Google Spain SL v. AEPD*, s. 60.
[21] Wyrok TS z 1.10.2015 r., *Weltimmo v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14.
[22] *Ibidem*, s. 29.
[23] Karta Praw Podstawowych Unii Europejskiej z 30.3.2010 r. (Dz.Urz. UE C Nr 83, s. 389); dalej jako: KPP.
[24] The Guardian, Social media may have been blocked during Turkey coup attempt, z 15.7.2016 r., https://goo.gl/ikhqeg.

Należy zauważyć, że mechanizmy, które w wykonaniu wyroku TS zaczęły być implementowane przez wiodących dostawców usług internetowych – służące do kontroli i filtrowania udostępnianych treści – nie różnią się w swoim przeznaczeniu od rozwiązań wykorzystywanych w Chinach. Oczywiście model chiński jest dużo bardziej skuteczny w kontrolowaniu udostępnianych treści, ponieważ państwo jest w stanie skutecznie nadzorować całą sieć transmisji danych[25]. W przypadku UE odpowiedzialność za tę kontrolę została przesunięta na prywatnych przedsiębiorców działających w warunkach wolnorynkowych – jest więc *de facto* formą autocenzury. Celem działania operatorów wyszukiwarek jest ułatwianie, a nie utrudnianie, dostępu do informacji. Jeżeli z powodu ochrony praw podstawowych wprowadzony ma zostać model kontroli treści internetowych – wydaje się rozsądne, aby koszty jego utrzymania były ponoszone przez państwa, a nie prywatnych przedsiębiorców. Jak wskazano w komunikacie opublikowanym przez Google, krajowe instytucje zajmujące się ochroną danych osobowych mogą być lepiej przygotowane do przeprowadzenia oceny, czy dane informacje powinny być usunięte z indeksu wyszukiwarki[26].

Dodatkowo należy wskazać, że kryteria podane przez Trybunał – pozwalające na skuteczne zastosowanie prawa do bycia zapomnianym – są wyjątkowo szerokie. W analizowanym wyroku wskazano możliwość stosowania wyjątków pozwalających na odmowę usunięcia wyników wyszukiwania, jednak ich katalog nie został precyzyjnie zdefiniowany.

W tym miejscu należy przytoczyć pogląd ETPC, wyrażony w wyroku wydanym w sprawie *Węgrzynowski* i *Smolczewski v.* Polska, że nie jest rolą władzy sądowniczej angażowanie się w przepisywanie historii poprzez nakazywanie usunięcia ze sfery publicznej wszelkich śladów publikacji[27]. Na gruncie krajowym tezę tę podzielił SO w Warszawie, rozpatrując sprawę, której podstawą było określenie odpowiedzialności usługodawcy internetowego za szkodę wyrządzoną prezentowaniem odnośników do treści, których nie był twórcą: „Z momentem, gdy użytkownik wprowadzi do okna dialogowego silnika wyszukiwarki zapytanie, wyszukiwarka zidentyfikuje i wyświetli wyniki wyszukiwania na określonych pozycjach zgodnie z własnymi algorytmami, które zostały opracowane w celu identyfikacji trafnych i użytecznych wyników wyszukiwania. Kształtowanie zaś treści linków i opisów (snippetów) z wyników wyszukiwania leży przede wszystkim po stronie podmiotów administrujących stronami internetowymi wyświetlanymi na listach wyników wyszukiwania. Wyniki wyszukiwania oraz snippety nie zawierają zatem jakichkolwiek twierdzeń pochodzących od operatora wyszukiwarki. Treść linków i snippetów powinna być kształtowania przede wszystkim przez administratorów stron, do których odsyłają linki wyświetlane w wynikach wyszukiwania, w przeciwnym wypadku pozwany musiałby być traktowany co najmniej jako cenzor Internetu[28]".

Na uwagę zasługuje przy tym fakt, że sąd w swoim uzasadnieniu uwzględnił treść orzeczenia w sprawie *Google Spain*.

Do innych wniosków – bliższych koncepcji wynikającej z przywołanego orzeczenia TS, doszedł jednak NSA w wyroku z 9.4.2015 r.[29] Wskazał mianowicie, iż za przetwarzanie danych osobowych może być uznane także ich pośrednie udostępnianie (np. poprzez przekierowanie do innej domeny internetowej), nawet jeżeli dany podmiot danymi tymi fizycznie nie dysponuje. Sąd podkreślił, iż nie może podlegać ochronie prawnej działanie podmiotów, które w sposób bezrefleksyjny dokonują świadomego odesłania do stron internetowych, które mogą naruszać chronione prawem polskim dane osobowe. Niewątpliwie, jeżeli przekierowanie takie nie łączy się z fizycznym posiadaniem danych udostępnionych na innej stronie internetowej, należy to uwzględniać w procesie oceny danego podmiotu jako przetwarzającego dane osobowe i nimi administrującego, jednakże brak posiadania danych nie wyłącza *per se* możliwości uznania danego podmiotu za ich administratora. Oczywiście nie jest tak, iż każde przekierowanie czy stworzenie innych warunków do wyszukania danych przez jedną witrynę internetową w zasobach innej będzie od razu mieścić się w ramach instytucji uregulowanych w ustawie o ochronie danych osobowych. Jak jednak wskazał NSA, nie może być zgody na to, by każde przekierowanie, które nie wiąże się z posiadaniem danych chronionych prawem, z założenia traktować jako nienaruszające przepisów ustawy.

Rozważając prawne konsekwencje funkcjonowania prawa do bycia zapomnianym, należy ocenić, w jaki sposób regulacja taka powinna dotyczyć internetowych repozytoriów wiedzy. Internet to nie tylko portale społecznościowe, ale także portale tematyczne czy encyklopedie elektroniczne. Czy prawo do bycia zapomnianym może prowadzić do wstecznej modyfikacji treści opublikowanych w Wikipedii? Jeżeli tak, to nie trudno wyobrazić sobie sytuację, w której to samo hasło będzie zaprezentowane odmiennie w papierowym i elektronicznym wydaniu tej samej encyklopedii[30]. Warto w tym miejscu przypomnieć tezę z przywołanego wcześniej wyroku ETPC: „nie jest rolą władzy sądowniczej angażowanie się w przepisywanie historii poprzez nakazywanie usunięcia ze sfery publicznej wszelkich śladów publikacji".

[25] Problematyka stosowanej w Chinach cenzury treści internetowych znalazła szerokie omówienie w piśmiennictwie – zarówno w zakresie stosowanych procedur i prawodawstwa, jak i ich wpływu na kształtowanie norm społecznych. Zob. np.: *J. Lee, C. Liu*, Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China, Minnesota Journal of Law, Science, and Technology 2012, Nr 1, s. 125–151.

[26] Google. Prywatność i warunki. Najczęstsze pytania, https://www.google.pl/policies/faq/.

[27] Zob. wyrok ETPC z 16.07.2013, *Węgrzynowski* i *Smolczewski v.* Polska, 33846/07, http://hudoc.echr.coe.int/.

[28] Wyrok SO w Warszawie z 12.10.2015 r., I C 1164/13, http://orzeczenia.warszawa.so.gov.pl/.

[29] Wyrok NSA z 9.4.2015, I OSK 2926/13, http://orzeczenia.nsa.gov.pl/.

[30] The Guardian, Wikipedia swears to fight 'censorship' of 'right to be forgotten' ruling, https://goo.gl/1Adu22.

Wydawca Wikipedii udostępnia statystyki na temat haseł encyklopedycznych, które zostały usunięte z wyszukiwarki Google na skutek realizacji prawa do bycia zapomnianym. W przypadku polskiego wydania Wikipedii jest to m.in. hasło poświęcone Parafii św. Wawrzyńca w Kurnie oraz AZS Legion Katowice[31]. To kolejny przykład, w którym zbyt daleko idące zastosowanie prawa do prywatności może prowadzić do nieadekwatnego ograniczenia prawa do informacji i swobody wypowiedzi.

Analiza wyroku *Google Spain* to także dowód, w jaki sposób nowoczesne technologie często wymykają się normom prawnym nie tylko na gruncie legislacji, ale przede wszystkim na etapie sądowym. Punktem wyjścia do dyskusji o przydatności wprowadzenia możliwości filtrowania (cenzorowania) wyników wyszukiwarki (a tym jest realizacja prawa do bycia zapomnianym) powinna być refleksja na temat celowości i skuteczności takiego działania. W zamierzeniu omawiane prawo powinno umożliwić osobom fizycznym usunięcie informacji na ich temat, które zostały opublikowane w Internecie – niezależnie od prawdziwości tych informacji, a także ich aktualności. Sposobem realizacji tego prawa – zgodnie z treścią wyroku – powinno być zgłoszenie żądania do operatorów wyszukiwarek ze wskazaniem listy kwestionowanych odnośników pojawiających po wpisaniu do okna wyszukiwarki frazy odpowiadającej imieniu i nazwisku danej osoby. Jeżeli jednak w oknie wyszukiwania zostanie wpisana inna fraza (niebędąca imieniem i nazwiskiem), wyniki wyszukiwania mogą zostać przedstawione w sposób odpowiadający rzeczywistości, a więc w sposób niefiltrowany, i umożliwić dostęp do stron, do których dostęp był zablokowany przy próbie wyszukiwania imieniem i nazwiskiem[32].

Przeglądarka internetowa nie jest statycznym mechanizmem, w którym pozycja, na której wyświetlana jest dana strona w rankingu, zależy wyłącznie od analizy jej treści. Równie ważne jest zachowanie użytkowników przeglądarki, a w szczególności fakt, jak często wybierają dany odnośnik i jak oceniają treść prezentowaną na stronie docelowej (tzw. indeks odrzuceń)[33]. Innymi słowy – wyszukiwarka wyświetla na górze rankingu te strony, które są chętniej odwiedzane przez użytkowników w odpowiedzi na wyszukiwaną frazę. W efekcie to użytkownicy poprzez swoje zachowania i decyzje kształtują indeks wyszukiwarki i wpływają na to, w jaki sposób wyszukiwarka prezentuje treści. Wprowadzenie sztucznej – manualnej – kontroli do tego procesu jest o tyle nieskuteczne, że użytkownicy, którzy chcą dotrzeć do interesującej ich informacji, zaczną wybierać odnośniki do innych stron, zawierających tę samą informację, i w ten sposób w krótkim czasie przyczynią się do podniesienia rankingu danej strony w indeksie, przywracając w efekcie stan pierwotny, w którym odnośnik kierujący do niepożądanej informacji będzie prezentowany na szczycie listy wyników.

Ponadto warto wskazać, że mechanizmy wyszukiwania już dawno zostały rozwinięte poza granicę treści tekstowych. Wiodące wyszukiwarki od lat indeksują także zdjęcia i potrafią wskazać nie tylko treść związaną z daną frazą, ale także zestaw powiązanych fotografii. Wiele serwisów internetowych oferuje funkcjonalność tworzenia repozytorium zdjęć z opcjonalną możliwością rozpoznawania twarzy. W efekcie użytkownik, będąc zarejestrowanym w takich portalach, jak Flickr czy Picassa, może otrzymywać powiadomienia, gdy inne osoby (w domyśle – znajomi) opublikują zdjęcie, na którym się znajduje. Ten sam mechanizm jest wykorzystywany przez Google w usłudze Gogle – w tym jednak przypadku pozwala na fotografowanie dowolnego przedmiotu i wyszukiwanie w Internecie innych powiązanych zdjęć i informacji. Mechanizmy rozpoznawania twarzy i przeszukiwania zdjęć z pewnością w niedalekiej przyszłości zostaną udostępnione publiczne i pozwolą na przeszukiwanie fotografii w sposób analogiczny do wyszukiwania tekstu.

Interesująca w tym względzie wydaje się analiza spraw sądowych prowadzonych z powództwa *M. Mosleya* przeciwko Google oraz innym wydawcom internetowym. Sprawy dotyczyły zakazu publikacji materiałów wideo i fotograficznych dotyczących aktywności seksualnej *M. Mosleya* – pełniącego wówczas funkcję prezydenta Międzynarodowej Federacji Samochodowej (Fédération Internationale de l'Automobile, FIA) – które oryginalnie zostały opublikowane 30.3.2008 r przez brytyjski tabloid News of the World. *Mosley* w kolejnych latach wygrał proces o ochronę dóbr osobistych wytoczony wydawcy tygodnika, jak również innym serwisom powielającym materiały przedstawione w oryginalnej publikacji. Ponadto *Mosley* zainicjował także sprawy przeciwko Google we Francji, Niemczech oraz Wielkiej Brytanii. *Mosley* zamierzał doprowadzić do stanu, w którym zdjęcia, których legalność została zakwestionowana przez sąd, nie będą indeksowane przez Google i wyświetlane w wynikach wyszukiwania – niezależnie, czy dany odnośnik został przez niego indywidualnie zgłoszony operatorowi przeglądarki. Oczekiwał, że Google wprowadzi mechanizmy autocenzury powodujące trwałe usunięcie kwestionowanych zdjęć z wyników wyszukiwania także tych stron, które zostaną dopiero zindeksowane w przyszłości. Zarówno francuski sąd okręgowy w Paryżu (Tribunal de Grande Instance de Paris)[34], jak i niemiecki regionalny sąd w Hamburgu (Landgericht Hamburg)[35] orzekły o słuszności żądań powoda,

[31] Notices received from search engines, https://goo.gl/HYaa2Z.

[32] *W. Gregory Voss*, The Right to Be Forgotten in the European Union: Enforcement in the Court of Justice and Amendment to the Proposed General Data Protection Regulation, Journal of Internet Law 2014, Nr 1.

[33] Google Analytics – strona produktu, Współczynnik odrzuceń, https://support.google.com/analytics/answer/1009409?hl=pl.

[34] Wyrok Tribunal de Grande Instance de Paris z 6.11.2013 r., RG 11/07970, https://goo.gl/mPspFP.

[35] Wyrok Landgericht Hamburg z 24.1.2014 r., 324 O 264/11, https://goo.gl/SStZx2.

zobowiązując Google do trwałego usunięcia zdjęć z wyszukiwarki. Na szczególnie interesujący zapowiadał się proces wytoczony w Wielkiej Brytanii. Po pierwsze, sąd krajowy miał w tym wypadku wyrokować już po wydaniu orzeczenia *Google Spain*. Po drugie, prawo brytyjskie regulujące obszar ochrony danych osobowych[36] przewiduje nieznane w polskim systemie prawnym uprawnienie jednostki do zgłoszenia żądania zaprzestania przetwarzania danych, jeżeli zostało uprawdopodobnione, że przetwarzanie to doprowadzi do powstania szkody. W analizowanej sprawie *Max Mosley* wystąpił z takim żądaniem, jednak Google odmówiło jego realizacji. Sprawa została skierowana na drogę sądową i w postanowieniu z 15.1.2015 r. sąd oddalił wniosek Google o umorzenie sprawy i skierował ją do dalszego rozpoznania. W sentencji postanowienia sąd uznał żądania powoda jako uprawdopodobnione[37]. Z uwagi jednak na fakt, ze strony zawarły ugodę, sprawa nie była przedmiotem dalszego badania przez sąd. Niewątpliwie jednak w niedalekiej przyszłości sądy krajowe państw UE będą musiały rozstrzygnąć zakres stosowania prawa do bycia zapomnianym w kontekście prewencyjnego filtrowania zdjęć publikowanych w Internecie.

W dyskusji na temat prawa do bycia zapomnianym niepokoi także stałe utożsamianie koncernu Google z informacjami publikowanymi w Internecie. Internet jest siecią informatyczną, wielowarstwową i rozproszoną (zdecentralizowaną). Sieć Internet jest medium transmisyjnym dla bardzo wielu protokołów, a tylko kilka z nich jest wykorzystywanych przez aplikacje webowe (takie jak usługi Google). Stawianie znaku równości pomiędzy Google a Internetem i projektowanie rozwiązań prawnych przeznaczonych dla ochrony prywatności w Internecie – mając na horyzoncie wyłącznie usługi świadczone przez Google – stanowi znaczącą wadę, immamentnie związaną z koncepcją prawa do bycia zapomnianym. Zanim jeszcze powstała spółka Google i przed udostępnieniem jej wiodącej usługi – wyszukiwarki Google Search – istniały zdecentralizowane protokoły komunikacyjne, służące do dystrybucji treści pomiędzy setkami tysięcy użytkowników na całym świecie. Przykładem może być sieć Usenet stanowiąca podstawę dla znanych także w Polsce grup dyskusyjnych. Sieć Usenet jest zdecentralizowana, podobna w swojej architekturze do sieci *Peer-2-Peer*, a więc jakakolwiek wsteczna moderacja (filtrowanie czy usuwanie wcześniej opublikowanych informacji) jest technicznie niemożliwa. Sieć Usenet jest odrębną usługą internetową, działającą z wykorzystaniem protokołu NNTP, a więc niezależnie i w sposób niezwiązany z treściami WWW, z którymi większość użytkowników utożsamia Internet. Do kogo więc osoba, która stała się przedmiotem dyskusji/publikacji w sieci Usenet i która chciałaby skorzystać z prawa do bycia zapomnianym, powinna kierować swoje żądanie? Jest oczywiste, że nie do operatora serwisu Google (nawet jeżeli treści Usenet są także indeksowane przez wyszukiwarkę), ponieważ Usenet jest odrębną, autonomiczną usługą. Żądania nie można skierować także do administratorów serwerów Usenet, ponieważ – jak wskazano powyżej – jest to sieć zdecentralizowana, w które każdy węzeł zawiera tylko kopię danych. Internet to setki różnych protokołów wymiany informacji – WWW, z której korzysta większość usług udostępnianych przez Google, to tylko jeden z nich.

Innym z zastosowań Internetu, w ostatnich latach coraz bardziej rozpowszechnionym w związku z rosnącymi obawami o prywatność, są wirtualne sieci prywatne (VPN). Nie wchodząc w analizę techniczną, VPN pozwala na zestawianie bezpiecznych (szyfrowanych) połączeń pomiędzy dwoma dowolnymi segmentami sieci Internet (konkretnymi komputerami lub całymi sieciami). W praktyce VPN pozwala na realizację usługi tzw. bezpiecznego proxy, a więc połączenia, w którym cały ruch od użytkownika przesyłany jest do zdalnego serwera i dopiero za jego pośrednictwem przesyłany dalej do sieci Internet. Proxy pozwala na ukrycie tożsamości użytkownika, jak również na podłączenie się przez użytkownika do Internetu w dowolnej części sieci. Możliwe jest więc zestawienie takiego połączenia, w którym komputer stojący w Poznaniu będzie widoczny w Internecie, jakby był podłączony do sieci w Niemczech, Stanach Zjednoczonych czy w Australii. Usługi takie są szeroko oferowane komercyjnie, są w pełni legalne i mają wiele zastosowań praktycznych[38]. Zapewniając anonimowość użytkownikom, pozwalają na przeglądanie treści Internetu w częściach świata, gdzie funkcjonująca cenzura normalnie uniemożliwiłaby dotarcie do poszukiwanych treści. Ta sama technologia pozwala – w oczywisty sposób – ominąć mechanizmy cenzury państw niedemokratycznych, jak też reguły filtrowania stosowane na rynku UE w związku z realizacją prawa do bycia zapomnianym. Nie ma żadnego technicznego problemu, aby dowolny użytkownik (czy cała sieć) został przełączony – bez zmiany fizycznej lokalizacji – za pomocą VPN do innego segmentu Internetu i w ten sposób pomijając ograniczenia funkcjonujące w UE. Dlatego realizacja prawa do bycia zapomnianym poprzez odpowiednie filtrowanie wyników wyszukiwania na podstawie lokalizacji komputera użytkownika jest rozwiązaniem o znacznie ograniczonej skuteczności[39].

Ogólne rozporządzenie o ochronie danych osobowych

Trybunał swoim orzeczeniem wzmocnił gwarancje związane z ochroną danych osobowych w UE. Co jednak oczywi-

[36] Por. art. 10 brytyjskiej ustawy z 16.7.1998 o ochronie danych (Data Protection Act 1998), http://www.legislation.gov.uk/ukpga/1998/29/contents.

[37] Postanowienie High Court of Justice of England and Wales z 15.1.2015 r., HQ 14 X 02964, https://goo.gl/1Xk4tu.

[38] Strona internetowa dostawcy jednej z wiodących usług VPN dostępnej globalnie: https://nordvpn.com.

[39] *K. Finley*, In Europe, You'll Need a VPN to See Real Google Search Results, Wired, 3.8.2016, https://goo.gl/FGQRze.

ste, rolą Trybunału nie jest definiowanie prawa materialnego, a jedynie wyrokowanie w zakresie norm już obowiązujących. W przypadku sprawy *Google Spain* wzorcem kontroli była dyrektywa 95/46 – niemal 20-letnia norma prawna, przyjęta w czasach, w którym sieć Internet dopiero powstawała, a pojęcia, takie jak społeczeństwo informacyjne czy serwisy społecznościowe, nie miały dzisiejszego znaczenia. Jeszcze przed wydaniem orzeczenia w sprawie *Google Spain*, KE zainicjowała prace związane z opracowaniem nowej regulacji w obszarze ochrony danych osobowych[40], która po zakończeniu procedury legislacyjnej została przyjęta jako rozporządzenie 2016/679. Chociaż rozporządzenie weszło w życie 4.5.2016 r. (art. 99 ust. 1), to przepisy będą miały zastosowanie od 25.5.2018 r. (art. 99 ust. 2). Do tego czasu będą obowiązywały przepisy obecne, a więc w przypadku prawa do bycia zapomnianym – w kształcie wynikającym z wyroku *Google Spain*.

Podstawową różnicą rozporządzenia w porównaniu z wcześniej obowiązującą dyrektywą jest rodzaj samego aktu prawnego. Zgodnie z art. 288 Traktatu o funkcjonowaniu Unii Europejskiej[41] rozporządzenie ma zasięg ogólny, wiąże w całości i jest bezpośrednio stosowalne. Natomiast dyrektywa wiąże w zakresie osiągnięcia określonych celów, pozostawiając jednak państwom członkowskim swobodę w zakresie wybranej formy i środków stosowania. Rozporządzenie jest więc źródłem praw i obowiązków dla jednostek, a dzięki bezpośredniej stosowalności może być podstawą do dochodzenia praw przed krajowymi organami sądowymi. Przyjęcie formy rozporządzenia w zakresie ochrony danych osobowych oznacza zatem standaryzację mechanizmów ochrony danych osobowych na terenie całej UE i ujednolicenie trybu postępowania we wszystkich państwach członkowskich[42]. Występująca w przypadku dyrektywy 95/46 implementacja prawa UE do porządku krajowego nie będzie już wymagana, a przepisy rozporządzenia będą stosowane wprost. Fakt ten ma kluczowe znaczenie zwłaszcza dla organizacji międzynarodowych, działających w wielu państwach członkowskich Unii. Standaryzacja mechanizmów ochrony danych osobowych to nie tylko wprowadzenie tych samych definicji administratora danych czy przetwarzania danych osobowych, ale również ustandaryzowanie praw i obowiązków osób, których dane są przetwarzane, oraz podmiotów przetwarzających. W obszarze prawa materialnego RODO jest odpowiedzią na potrzebę wprowadzenia regulacji prawnych zmierzających do zagwarantowania wysokiego poziomu ochrony prywatności w dynamicznie rozwijających się technologiach kształtujących nowoczesne społeczeństwo informacyjne, takich jak analityka Big Data, chmura obliczeniowa (ang. *cloud computing*) czy technologia rozszerzonej rzeczywistości (ang. *augmented reality*).

Rozporządzenie wprowadza także do unijnego porządku prawnego prawo do bycia zapomnianym. Chociaż, jak wskazano wcześniej, było ono częścią dorobku prawnego już od orzeczenia TS w sprawie *Google Spain*, dopiero w RODO prawo do bycia zapomnianym (określane jako prawo do usunięcia danych) zostało zdefiniowane w całości, jako oddzielna norma prawna, a nie przez pryzmat pojedynczego kazusu procesowego. Zgodnie z art. 17 ust. 1 RODO w określonych okolicznościach osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki te dane usunąć. Aby uniknąć niejasności i sporów w obszarze terytorialnego zakresu stosowania, w art. 3 ust. 1 doprecyzowano, że rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy samo przetwarzanie odbywa się w Unii. Natomiast zgodnie z art. 3 ust. 2 rozporządzenie stosuje się także do przetwarzania danych osobowych osób przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom lub monitorowaniem ich zachowania.

W efekcie rozporządzenie powinno być stosowane, jeżeli przetwarzane są dane osobowe obywateli Unii – niezależnie od tego, czy administrator danych prowadzi działalność na terenie UE, czy też samo przetwarzanie odbywa się w Unii. Rozporządzenie doprowadzi zatem do usunięcia nierówności w traktowaniu podmiotów mających siedzibę lub oddział w UE względem podmiotów prowadzących działalność spoza Unii, ale kierujących swoje produkty lub usługi do obywateli UE. Jak wcześniej wskazano, w obecnym stanie prawnym – będącym konsekwencją wyroku *Google Spain* – nie wszyscy przedsiębiorcy świadczący e-usługi i przetwarzający dane osobowe mieszkańców UE muszą stosować się do unijnych przepisów o ochronie danych. Wprowadzona w ogólnym rozporządzeniu zmiana prowadzi zatem do ujednolicenia obowiązków usługodawców, jest więc korzystna z punktu widzenia praw konsumentów z obszaru UE. Nałożenie jednakowych obowiązków, niezależnie od miejsca prowadzenia działalności czy wykorzystywanych środków technicznych związanych z przetwarzaniem informacji (przetwarzanie rozproszone, *cloud computing* itp.), prowadzi także do zwiększenia konkurencyjności przedsiębiorców europejskich.

[40] W tym miejscu warto zauważyć, że już pierwszy wniosek KE dotyczący projektu ogólnego rozporządzenia – opublikowany 25.1.2002 r. – uwzględniał w art. 17 wprowadzenie „prawa do bycia zapomnianym", rozumianego jako rozszerzenie znanego na gruncie dyrektywy 95/46 prawa do usunięcia danych.

[41] T.j. Dz.Urz. UE z 2016 r. C Nr 202, s. 47.

[42] Parlament Europejski, Reforming the Data Protection Package, wrzesień 2012, https://goo.gl/oaabmx.

Istotą wyroku *Google Spain* było wskazanie, że podmiot danych ma prawo żądania zaprzestania prezentowania określonych informacji dotyczących jego prywatności. Należy podkreślić, że TS nie wskazał wprost konieczności „usunięcia" zakwestionowanych danych. Powstaje zatem zasadnicze pytanie, czy prawo do bycia zapomnianym (w kształcie wynikającym z orzeczenia *Google Spain*) i prawo do usunięcia danych (art. 17 ogólnego rozporządzenia) w rzeczywistości definiują to samo prawo podmiotu danych. Aspekt ten jest pomijany w trwającej dyskusji na temat przygotowania administratorów do nowych obowiązków prawnych. Uzasadniony wydaje się pogląd, że prawodawca unijny, definiując zakres prawa do usunięcia danych, może nałożyć na administratora *de facto* nowe obowiązki, odmienne od wynikających z orzeczenia *Google Spain*. Dlatego, chociaż zgodnie z terminologią przyjętą w ogólnym rozporządzeniu, w niniejszym artykule terminy prawo do bycia zapomnianym i prawo do usunięcia danych stosowane są zamiennie, to należy wskazać, że w rzeczywistości oba pojęcia *de facto* opisują inne prawo, bowiem wiążą się z odmiennymi obowiązkami po stronie administratorów danych[43].

Prawo do usunięcia danych w kształcie wynikającym z ogólnego rozporządzenia nie powinno być analizowane w oderwaniu od formalnej podstawy przetwarzania. W przyjętej redakcji art. 17 ust. 1 określono enumeratywne przypadki, uzasadniające realizację żądania usunięcia danych. Podmiot danych może wystąpić z żądaniem, w przypadku gdy ustał cel przetwarzania. W efekcie można uznać, że prawo do usunięcia danych może być stosowane wyłącznie w sytuacji, gdy nie istnieje żadna formalna podstawa przetwarzania. W ten sposób prawo to stanowi dopełnienie zasady minimalizacji danych – a więc służy dostarczeniu legalnych środków, które mogą posłużyć do zobowiązania administratora do usunięcia danych, które nie powinny być dalej przez niego przetwarzane.

Jako trafną należy ocenić także regulację wprowadzoną art. 17 ust. 2, zgodnie z którą, jeżeli administrator upublicznił dane osobowe, co do których wpłynęło żądanie ich usunięcia (realizacja prawa do bycia zapomnianym), to – biorąc pod uwagę dostępną technologię i koszt realizacji – jest on zobowiązany podjąć rozsądne działania, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych lub ich replikacje.

Analizowany przepis wprowadza dwa korzystne rozwiązania z punktu widzenia praktycznej realizacji prawa do bycia zapomnianym. Po pierwsze, wprowadza mechanizm współdziałania pomiędzy wydawcami a innymi serwisami internetowymi – w szczególności operatorami wyszukiwarek – w zakresie komunikowania żądania usunięcia określonych danych. Poza zmniejszeniem pracochłonności dla usługodawców, z punktu widzenia podmiotów danych mechanizm ten pozwoli na szybkie i automatyczne usuwanie z indeksu wielu wyszukiwarek treści, co do których wpłynęło żądanie ich usunięcia. Na praktyczne uzasadnienie takiego podejścia wskazywali także operatorzy wyszukiwarek internetowych, np. koncern Microsoft (operator wyszukiwarki Bing), twierdząc, że: „w przypadku utworzenia lub umieszczenia treści na stronach mediów społecznościowych, która ma być zablokowania, usunięta lub pomniejszona w wynikach wyszukiwania – w wyszukiwarce Bing i innych wyszukiwarkach – należy spróbować użyć narzędzi i procesów usuwania treści dostępnych na tych stronach mediów społecznościowych. Te narzędzia i procesy mogą być najskuteczniejszym sposobem usunięcia treści mediów społecznościowych z wyników wyszukiwania"[44].

Warto zauważyć, że podobne rozwiązania techniczne są znane od lat. Polegają na stosowaniu odpowiednich znaczników w kodzie strony internetowej lub pliku *robots.txt* umieszczonym w indeksowanym folderze. Niezależnie od wybranej techniki wydawca treści internetowych ma możliwość wskazania oczekiwanego zachowania algorytmu indeksującego strony internetowe, w szczególności określenia, że dana strona nie ma być indeksowana (znacznik: *noindex*) lub odnośniki na niej zawarte nie mają być dalej przeszukiwane (znacznik: *nofollow*). Problem stosowania plików *robots.txt* był już analizowany przez TSw sprawie *Google Spain*. Przedstawiciele koncernu Google podnosili, że operator wyszukiwarki nie powinien być odpowiedzialny za ręczną modyfikację indeksu, skoro wydawcy stron dysponują narzędziem pozwalającym na wskazanie treści, które mają być indeksowane. Trybunał uznał jednak, że brak wskazania przez wydawców ograniczenia indeksowania danej strony nie zwalnia operatora wyszukiwarki internetowej ze spoczywających na nim obowiązków wynikających z faktu, że także jest podmiotem zobowiązanym do realizowania praw podmiotów danych. W tym zakresie również w RODO podtrzymano ten pogląd, dlatego norma art. 17 ust. 2 nie zwalnia z odpowiedzialności za przestrzeganie treści rozporządzenia usługodawców, którzy nie zostali poinformowani przez wydawcę treści o żądaniu usunięcia danej strony z rejestru.

Finalna redakcja art. 17 ust. 2, nakładając obowiązki na wydawcę treści, uwzględnia przy tym istniejące ograniczenia techniczne oraz koszty ich realizacji. W ten sposób prawodawca unijny próbuje zachować równowagę pomiędzy intere-

[43] Na różne możliwe skutki „zapomnienia" zbioru danych wskazywano już w analizie ENISA opublikowanej w 2012 r., odnoszącej się do treści prawa przedstawionej w pierwszym projekcie ogólnego rozporządzenia. W raporcie Agencji przedstawiono trzy możliwe płaszczyzny interpretacyjne, z czego tylko jedna prowadziła do konieczności fizycznego usunięcia wszystkich kopii danych. Więcej: *P. Druschel*, *M. Backes*, *R. Tirtea*, The right to be forgotten – between expectations and practice, European Network and Information Security Agency 2012, https://goo.gl/Q4KNSL, s. 7.

[44] Zob. http://help.bing.microsoft.com/#apex/18/PL/10013/-1/PL.

sem osób żądających usunięcia swoich danych a oczekiwaniami wydawców treści – związanymi z racjonalizacją kosztów realizacji tych żądań. Warto przypomnieć, że Trybunał w wyroku *Google Spain* podkreślił, że ochrona praw wynikających z KPP jest nadrzędna względem interesu gospodarczego przedsiębiorcy internetowego – co w odniesieniu do badanej sprawy oznaczało konieczność spełnienia żądania usunięcia danych niezależnie od kosztów, które operator musi ponieść w tym celu. W tym kontekście treść przepisu zaproponowana w RODO wydaje się bardziej racjonalna i uwzględniająca oczywisty fakt funkcjonowania przedsiębiorców w określonej przestrzeni biznesowej, w której rachunek ekonomiczny oraz możliwości techniczne są istotnymi elementami uzasadniającymi podejmowane decyzje.

Większe trudności interpretacyjne dotyczące sposobu stosowania prawa do usunięcia danych mogą dotyczyć przedsiębiorców zagranicznych, stosujących przepisy rozporządzenia na podstawie art. 3 ust. 2. W takim przypadku może bowiem dojść do oczywistej kolizji norm unijnych z prawem właściwym dla miejsca przetwarzania danych. W takim przypadku może się okazać, że realizacja prawa do bycia zapomnianym doprowadziłaby do naruszenia norm publicznoprawnych, do stosowania których zobowiązany jest administrator danych. Problem ten może mieć szczególny wymiar w przypadku przedsiębiorców podlegających prawu Stanów Zjednoczonych. Obowiązujące w tamtejszym systemie prawnym normy konstytucyjne, w szczególności Pierwsza Poprawka, stoją na przeszkodzie wprowadzaniu regulacji ustawowych ograniczających „wolność słowa lub prasy”[45]. Prawo do bycia zapomnianym bez wątpienia należy do tego typu środków[46].

Tak określone prawo do bycia zapomnianym budzi także zastrzeżenia natury technicznej. W szczególności wskazuje się na trudności związane z obowiązkiem usunięcia danych w sytuacji gdy znajdują się one także na kopiach zapasowych administratora. Nie jest jasne, czy w takim wypadku administrator powinien także usunąć dane z kopii zapasowych. Odpowiedź twierdząca prowadziłaby do kolejnych trudności, związanych ze spójnością przetwarzanych informacji. Cyfrowe kopie danych można podzielić na dwa rodzaje: kopie zapasowe oraz kopie archiwalne. Kopie zapasowe służą przywróceniu działania środowiska IT w przypadku awarii, a więc odtworzeniu utraconych informacji. Problem może wystąpić w przypadku, gdy po uwzględnieniu żądania usunięcia danych nastąpi awaria systemu informatycznego i odtworzona zostanie kopia zapasowa wykonana przed uwzględnieniem tego żądania. W takiej sytuacji istnieje możliwość, że usunięte wcześniej dane zostaną przywrócone, co doprowadzi do naruszenia obowiązków prawnych przez administratora danych. Chociaż obecnie problemowi temu poświęca się dużo uwagi, jego praktyczne znaczenie jest stosunkowo niewielkie. Należy pamiętać, że możliwość skorzystania z prawa do usunięcia danych jest warunkowana spełnieniem jednej z wymienionych w art. 17 ust. 1 przesłanek. Należy zatem przyjąć, że realizacja żądania przez administratora nie jest związana wyłącznie z technicznym wykonaniem czynności skasowania określonego zestawu w bazie danych, ale jest poprzedzona analizą i weryfikacją wniosku. Proces ten powinien być udokumentowany, a zatem w przypadku awarii administrator nie powinien mieć trudności w identyfikacji zakresu danych objętych żądaniami zgłoszonymi po dacie wykonania odtwarzanej kopii.

Podsumowując rozważania dotyczące treści prawa do bycia zapomnianym w ujęciu wprowadzonym w ogólnym rozporządzeniu, należy zwrócić uwagę na treść art. 85 RODO. We wskazanym przepisie przewidziano możliwość wprowadzenia przez państwa członkowskie uzasadnionych ograniczeń w stosowaniu przepisów rozdziału III rozporządzenia, do których należy w szczególności art. 17, z uwagi na potrzebę wyważenia ochrony danych osobowych z innymi prawami podstawowymi, takimi jak wolność wypowiedzi i prawo do informacji. Cel wprowadzenia omawianego przepisu – a więc uniknięcie nadużycia prawa do bycia zapomnianym w sposób ograniczający prawo do informacji – jest oczywiście czytelny i słuszny. W praktyce jednak jego stosowanie może budzić liczne kontrowersje implementacyjne. Pozostawienie możliwości decydowania o sposobie wyważanie praw do decyzji państwom członkowskim może skutkować przyjęciem odmiennych, potencjalnie niezgodnych, norm krajowych.

Podsumowanie

Koncepcja prawa do bycia zapomnianym (prawa do usunięcia danych) jest stosunkowo nową instytucją prawną, będącą efektem adaptacji prawnych mechanizmów ochrony prywatności w zglobalizowanym świecie informacji elektronicznej. Jej obecny kształt, wynikający z orzeczenia TS w sprawie *Google Spain*, w wielu miejscach pomija złożoność technologii, którą stara się regulować. Zamiast tego wprowadzono regulacje w odniesieniu do jednej kategorii podmiotów działających na rynku e-usług, jakim są operatorzy wyszukiwarek internetowych. W efekcie obywatele UE otrzymali ułomny mechanizm ochrony swoich praw, który w wielu miejscach jest niespójny i nieskuteczny. Dlatego – nie kwestionując doniosłego znaczenia praktycznego analizowanego orzeczenia – nie można w pełni podzielić poglądu, że orzeczenie Trybunału stanowi „skuteczne narzędzie do walki o ochronę i obronę prywatności w zakresie przetwarzania danych osobowych, nawet względem potężnych operatorów

[45] Polskie tłumaczenie Pierwszej Poprawki do Konstytucji USA: http://libr.sejm.gov.pl/tek01/txt/konst/usa.html.

[46] Problem szerzej analizuje: *M. Rustad*, *S. Kulevska*, Reconceptualizing the Right To Be Forgotten to Enable Transatlantic Data Flow, Harvard Journal of Law & Technology 2015, Nr 2, s. 372–373.

[internetowych]"[47]. Jednocześnie przedsiębiorcy internetowi uzyskali kolejny argument, aby prowadzić i rozwijać swoją działalność gospodarczą i – często innowacyjne – usługi poza obszarem UE. Problemy te zostały zauważone przez prawodawcę unijnego, w wyniku czego prawo do bycia zapomnianym zostało uwzględnione w zmodyfikowanym kształcie w ogólnym rozporządzeniu. Niewątpliwie treść normy wskazana w rozporządzeniu pozwala na uniknięcie niektórych z zauważonych wcześniej problemów. Niestety nie rozwiązuje ona problemu zasadniczego, jakim jest wprowadzenie mechanizmu prawnego, który z całą pewnością nie może skutecznie i całościowo rozwiązać problemu braku kontroli osób fizycznych nad publikowanymi na ich temat treściami elektronicznymi, natomiast może zostać wykorzystany do wprowadzenia środków skutecznej cenzury czy nawet autocenzury na obszarze UE. Warto zaznaczyć, że do chwili obecnej sam tylko koncern Google otrzymał ponad 580 tys. wniosków o usunięcie łącznie ponad 1 750 000 odnośników internetowych[48]. Praktyczna ocena użyteczności prawa do bycia zapomnianych w kształcie wprowadzonym w RODO nastąpi oczywiście dopiero po 25.5.2018 r. Do tego czasu przedsiębiorcy internetowi przetwarzający dane osobowe mają czas na dostosowanie się do nowych regulacji.

[48] *M. Wróbel*, Prawo do „bycia zapomnianym" – glosa – C-131/12, MoP 2017, Nr 2, s. 112.

[49] Google, Europejskie żądania dotyczące prywatności: usunięcie wyników wyszukiwania, https://www.google.com/transparencyreport/removals/europeprivacy/?hl=pl.

Słowa kluczowe: prywatność, prawo do bycia zapomnianym, prawo do usunięcia danych, cenzura, RODO.

Analysis and practical comments on construction and implementation of right to be forgotten in the EU

Legal regulations connected with the protection of personal data are evolving in the direction of granting the individuals an effective control of information concerning them, published on the Internet. In the world of forefront of developments in this field for many years is the European Union, in which individual rights and freedoms are permanently enshrined in the Charter of Fundamental Rights. Uncompromising protection of individual rights is encouraged by both the EU legislature, as well as the judgments of the constitutional courts of the Member States and the European Court of Justice.

The purpose of this article is to present the most important principles of the right to be forgotten and to analyze whether the current form of this law, which is a consequence of the ECJ rulings, does not contribute to the weakening of other fundamental rights such as the right to information and freedom of expression.

Keywords: privacy, the right to be forgotten, the right to erasure, censorship, GDPR.

E-mediacja jako pozasądowa metoda rozwiązywania sporów konsumenckich

Wiktoria Kotwicka[1]

Celem niniejszego opracowania jest analiza funkcjonowania e-mediacji (mediacji online) w sprawach konsumenckich w polskim systemie prawnym na tle regulacji unijnych (dyrektywy w sprawie ADR w sporach konsumenckich 2013/11/UE oraz rozporządzenia w sprawie internetowego systemu rozstrzygania sporów konsumenckich nr 524/2013). Autorka omawia koncepcję e-mediacji w sporach konsumenckich, jej aspekty techniczne, a także zasady postępowań e-mediacyjnych prowadzonych przez podmioty wyspecjalizowane w ramach systemu internetowego rozstrzygania sporów konsumenckich utworzonego w rozporządzeniu 524/2013.

Uwagi wstępne

Rozwój alternatywnych metod rozwiązywania sporów, będących odpowiedzią na pojawiające się potrzeby skutecznego i szybkiego radzenia sobie z konfliktem, w naturalny sposób implikuje pojawienie się coraz bardziej różnorodnych form, przede wszystkim tych związanych z digitalizacją społeczeństwa. Tradycyjne metody ADR coraz częściej znajdują zastosowanie w Internecie.

Zmiany zachodzące w rzeczywistości społeczno-gospodarczej prowadzą do wirtualizacji obrotu, która sprawia, że istniejące granice i bariery tracą dotychczasowe znaczenie. Powoduje to zmniejszenie użyteczności tradycyjnych instrumentów ochrony praw, co uwidacznia się szczególnie w przypadku transgranicznych sporów pomiędzy konsumentem a przedsiębiorcą. Nieefektywność tradycyjnej formy rozstrzygania sporów przez sądy państwowe aktualizuje się również w przypadku krajowych sporów konsumenckich, szczególnie tych o niewielkiej wartości.

Pojęcie e-mediacji w kontekście ODR

Przez e-mediację należy rozumieć proces rozwiązywania sporu, w którym osoba trzecia – profesjonalny mediator – przy użyciu technik komunikacji elektronicznej, takich jak np. poczta elektroniczna, czat, telekonferencja czy wideokonferencja, ułatwia stronom znalezienie satysfakcjonujących ich rozwiązań i zawarcie ugody[2]. Główny cel mediacji elektronicznej jest taki sam jak jej tradycyjnej odmiany. W literaturze przedmiotu można odnaleźć również drugie znaczenie pojęcia mediacji online – odnoszące się do istoty miejsca zaistnienia spornego stosunku prawnego, jakim jest Internet. Pojęcie to odnosi się zatem do mediacji, której przedmiot stanowi spór powstały w środowisku online. W niniejszym artykule przyjęto pierwsze z przytoczonych znaczeń, czyli to bazujące na kryterium narzędzi online stosowanych do rozwiązywania zaistniałego konfliktu, niezależnie od miejsca jego powstania.

Mediacja online wpisuje się wyraźnie w trend rozwojowy związany z digitalizacją społeczeństwa jako szybka i wygodna metoda rozwiązywania konfliktu przez strony, szczególnie wówczas gdy znajdują się one w znacznej odległości od siebie, uniemożliwiającej lub utrudniającej odbycie posiedzenia mediacyjnego[3]. Na potrzeby niniejszego artykułu pochylono się nad pojęciem e-mediacji (mediacji online, mediacji elektronicznej), wychodząc od zagadnienia alternatywnych metod rozwiązywania sporów (tzw. ADR – ang. *Alternative Dispute Resolution*), które za pomocą najnowszej technologii zostały przeniesione do Internetu, przyczyniając się do coraz szybszego w ostatnich latach rozwoju ODR (ang. *Online Dispute Resolution*) – elektronicznego ADR. Postępująca informatyzacja w ramach funkcjonowania wymiaru sprawiedliwości oraz poszerzanie zakresu czynności procesowych i sądowych dokonywanych w systemie teleinformatycznym na potrzeby postępowania sądowego sprawiły, że naturalne wydaje się realizowanie tych samych idei w odniesieniu do ADR.

Alternatywne metody rozwiązywania sporów, do których należy przede wszystkim zaliczyć mediację i arbitraż, jako odpowiedź na pojawiające się potrzeby skutecznego i szybkiego radzenia sobie z konfliktem, przeżywają obecnie rozkwit. Postępowania i techniki alternatywnych metod rozwiązywania sporów w sprawach konsumenckich w zależności od sytuacji stanowią w stosunku do klasycznego procesu cywilnego alternatywę wewnętrzną albo zewnętrzną[4]. Wśród szeroko rozumianych alternatyw wewnętrznych, którymi zwykło się

[1] Autorka jest studentką V roku studiów stacjonarnych Prawa na Uniwersytecie Wrocławskim oraz słuchaczką seminarium magisterskiego prof. dr hab. *J. Gołaczyńskiego*.

[2] *M. Grabowski*, E-mediacja jako metoda rozwiązywania sporów w handlu elektronicznym, ADR 2012, Nr 4, s. 43.

[3] *T.P. Antoszek*, Dopuszczalność e-mediacji w polskim systemie prawnym – wybrane aspekty prawne, [w:] *J. Czapska*, *M. Szeląg-Dylewski* (red.), Mediacja w prawie, Kraków 2014, s. 125.

[4] *K. Gajda*, Alternatywne metody rozwiązywania sporów w sprawach konsumenckich, ADR. Arbitraż i Mediacja 2008, Nr 2, s. 22, http://arbitraz.laszczuk.pl/_adr/26/Alternatywne_metody_rozwiazywania_sporow_w_sprawach_konsumenckich_(cz._I).pdf (dostęp z 20.8.2017 r.).

nazywać alternatywy w ramach sądowego postępowania cywilnego[5], należy wskazać na dążenie sądu do zawarcia ugody oraz postępowanie pojednawcze i mediacyjne. Wśród alternatyw zewnętrznych w stosunku do postępowania cywilnego w sprawach konsumenckich, funkcjonujących poza państwowym wymiarem sprawiedliwości, należy przede wszystkim wymienić pozakodeksowe postępowania prowadzone przez podmioty wyspecjalizowane w ramach unijnego systemu internetowego rozstrzygania sporów. Powyższy dualizm stanowi punkt wyjścia do rozważań dotyczących e-mediacji jako elektronicznej wersji mediacji w sprawach konsumenckich w Polsce. Z jednej strony analizie zostaną poddane przepisy kodeksowe o mediacji, z drugiej zaś – pozakodeksowe postępowania w ramach unijnego systemu rozstrzygania sporów konsumenckich, które w swej istocie często przybierają postać mediacji online. Z uwagi na to, że rozważania dotyczące dopuszczalności e-mediacji w Kodeksie postępowania cywilnego nie będą odnosić się wyłącznie do sporów konsumenckich, lecz do ogólnie pojętej e-mediacji cywilistycznej, natomiast charakterystyka postępowań prowadzonych przez podmioty wyspecjalizowane, dostępnych dzięki platformie ODR, dotyczy wyłącznie spraw konsumenckich, temu zagadnieniu poświęcona zostanie większa część niniejszego artykułu.

Zalety wykorzystywania środków elektronicznych w sporach konsumenckich

Mediacja realizuje jedną z głównych funkcji prawa, jaką jest rozwiązywanie konfliktów, przy zachowaniu konsensualnego i niewiążącego charakteru[6]. Jej elektroniczna odmiana pozwala na nowe, wcześniej niedostępne możliwości, tj. jednoczesne uczestnictwo stron postępowania bez utrudnień w postaci osobistego stawiennictwa w konkretnym miejscu i czasie. Istotne znaczenie ma również oszczędność kosztów, wynikająca z braku konieczności uczestnictwa profesjonalnego pełnomocnika czy doręczeń dokumentów. Ponadto mediacje online odbywające się przez elektroniczną platformę pozwalają na rejestrację całego procesu i jego powtórne odtworzenie[7]. Wymienione zalety wydają się przedstawiać szczególny potencjał w przypadku sporów konsumenckich, których swoiste cechy, takie jak: dysproporcja pomiędzy niską wartością przedmiotu sporu a wysokimi kosztami postępowań sądowych, faktyczna nierówność stron w połączeniu z nieefektywnością i przewlekłością postępowań sądowych, powodują, że to właśnie na gruncie konfliktów i sporów konsumenckich następuje szczególny sektorowy rozwój pozasądowych alternatywnych metod rozwiązywania sporów. W związku z powyższym również ODR, a zatem także e-mediacja, stanowić mogą wysoce użyteczny instrument realizacji ochrony konsumentów, która należy do kompetencji krajów członkowskich UE, mając normatywne źródło m.in. w art. 169 ust. 1 i art. 169 ust. 2a TFUE, w art. 2c Traktatu z Lizbony zmieniającego Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisanego w Lizbonie 13.12.2007 r.[8] oraz w art. 38 Karty praw podstawowych Unii Europejskiej[9].

W literaturze zwraca się również uwagę na możliwe wady mediacji prowadzonej online. Na pierwszy rzut oka wysuwa się brak kontaktu bezpośredniego, z jakim mamy do czynienia przy tradycyjnej mediacji[10]. Zdaniem krytyków tej formy wirtualny kontakt nie powinien być traktowany jako substytut bezpośrednich spotkań mediatora ze stronami, gdyż cyberprzestrzeń nie stanowi lustrzanego odbicia świata rzeczywistego[11]. Wskazana cecha w przypadku sporów konsumenckich może być jednak śmiało uznana raczej za zaletę niż wadę. Przełamanie zasady kontaktu bezpośredniego i osobistego udziału stron, czyli stworzenie nieosobistych relacji, sprzyja bowiem prowadzeniu mediacji elektronicznej, szczególnie wtedy gdy chodzi o spory o niewielkim stopniu skomplikowania czy niewielkiej wartości przedmiotu sporu, a tym często właśnie charakteryzują się spory konsumenckie. Kolejna wskazywana wada e-mediacji to eliminowanie dynamiki i przepływu emocji, które są tak charakterystyczne w klasycznym modelu mediacji. Warto jednak zauważyć, że specyfika spraw konsumenckich nie wiąże się w tak wysokim stopniu ze sferą emocji, co oznacza, że czynnik psychologiczny nie odgrywa tu roli nadrzędnej, jak ma to miejsce na przykład w sporach rodzinnych. *M. Grabowski* wskazuje, że e-mediacja jest uboższą wersją w stosunku do mediacji tradycyjnej i dlatego – o ile to możliwe – powinna być zawsze stosowana subsydiarnie[12]. Z tym stanowiskiem nie sposób się w pełni zgodzić. Wymienione zalety mediacji online bynajmniej nie świadczą o tym, że powinna ona być stosowana zawsze subsydiarnie, lecz wydaje się, że może samodzielnie stanowić podstawową formę rozwiązywania sporów konsumenckich. Przykładem uzasadniającym to stanowisko są

[5] *L. Morawski*, Proces sądowy a instytucje alternatywne (na przykładzie sporów cywilnych), PiP 1993, z. 1, s. 21; *tenże*, Główne problemy współczesnej filozofii prawa. Prawo w toku przemian, Warszawa 2003, s. 228; *Ł. Błaszczak*, Mediacja a inne alternatywne formy rozwiązywania sporów (wybrane zagadnienia), ADR 2012, Nr 2, s. 13.

[6] *L. Morawski*, Wstęp do prawoznawstwa, Toruń 2014, s. 21–47.

[7] *K. Mania*, Online Dispute Resolution, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja, teoria, normy, praktyka, Warszawa 2017, s. 369–370.

[8] Dz.Urz. UE C Nr 306, s. 1.

[9] Dz.Urz. UE C Nr 202, s. 389.

[10] *M. Białek*, Mediacja online (cybermediacja), [w:] *A. Torbus* (red.), Mediacja w sprawach gospodarczych. Praktyka–teoria–perspektywy. Ministerstwo Gospodarki, Departament Doskonalenia Regulacji Gospodarczych, Warszawa 2015, s. 328.

[11] *J.W. Goodman*, The pros and cons of Online Dispute Resolution: an assesment of cyber-mediation websites, http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1073&context=dltr (dostęp z 8.8.2017 r.)

[12] *M. Grabowski*, E-mediacja…, s. 49.

spory e-commerce cechujące się nieosobistą relacją, dla których techniki ODR, pozbawione bezpośrednich kontaktów, stają się właściwym narzędziem pozwalającym na skuteczne rozwiązywanie konfliktów[13]. Wobec powyższych spostrzeżeń należy stwierdzić, że mediację online charakteryzuje wiele zalet w kontekście analizowania tej formy ODR jako potencjalnie efektywnego narzędzia do rozwiązywania kategorii sporów określanych mianem sporów konsumenckich.

W krajowym systemie brak jest legalnej definicji sporów konsumenckich, jednak SN w uchwale z 29.2.2000 r.[14], określił je jako „sprawy związane z szerokim zakresem umów, w których osoba nabywająca rzecz lub na rzecz, której wykonywane są usługi, zaspokajające jej własne potrzeby (konsument), dochodzi roszczenia przeciwko kontrahentowi zajmującemu się profesjonalnie handlem, produkcją i usługami, przy czym roszczenia konsumentów mogą wynikać z różnych tytułów prawnych, w szczególności z tytułu niewykonania lub należytego wykonania zobowiązania oraz z tytułu rękojmi za wady rzeczy i gwarancji"[15]. Definicja ta zarysowuje ogólną istotę spraw konsumenckich, których zakresy podmiotowe i przedmiotowe będą się różnić w zależności od rodzaju omawianej mediacji online.

1. E-mediacja jako alternatywa zewnętrzna. Pozasądowe rozwiązywanie sporów konsumenckich w ramach dyrektywy w sprawie ADR w sporach konsumenckich 2013/11/UE oraz rozporządzenia 524/2013

1.1. Uwagi wprowadzające

Ochrona konsumentów należy do kompetencji krajów członkowskich i UE. Jak już zostało wspomniane, obowiązek ten nabiera szczególnego znaczenia w obliczu istnienia europejskiego rynku wewnętrznego, który powinien zapewnić jednolitą ochronę praw konsumentów, czego gwarantem są m.in. systemy ADR i ODR, pozwalające na szybsze i tańsze w stosunku do sądownictwa powszechnego rozwiązywanie zaistniałych sporów. Istotną regulacją w zakresie sporów konsumenckich było zalecenie Komisji Europejskiej 98/257/WE z 30.3.1998 r. co do zasad mających zastosowanie do organów odpowiedzialnych za pozasądowe rozstrzyganie sporów konsumenckich, określające podstawowe zasady dotyczące ich działalności i prowadzonych postępowań. Kolejnym dokumentem było zalecenie Komisji Europejskiej 2001/310/WE z 4.4.2001 r. nowelizujące wcześniejsze ustalenia w zakresie działalności wskazanych organów oraz promujące ADR[16].

Intensyfikacja sporów konsumenckich o charakterze transgranicznym, w tym ich rozwój w Internecie, spowodowały konieczność wprowadzenia nowych konstrukcji usprawniających rozpoznawanie oraz rozwiązywanie tych sporów. W konsekwencji instytucje UE prowadziły intensywne prace zmierzające do stworzenia konstrukcji rozwijającej idee i możliwości ODR na potrzeby krajowych, a także transgranicznych sporów z udziałem konsumentów. Nowy etap rozwoju pozasądowego rozstrzygania sporów konsumenckich rozpoczął się w 2013 r., gdy weszły w życie kluczowe akty unijnego prawa wtórnego, jakimi są: dyrektywa Parlamentu Europejskiego i Rady 2013/11/UE Nr 2013/11/UE z 21.5.2013 r. w sprawie alternatywnych metod rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) Nr 2006/2004 i dyrektywy 2009/22/WE (dyrektywa w sprawie ADR w sporach konsumenckich)[17] oraz rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr 524/2013 z 21.5.2013 r. w sprawie internetowego systemu rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) Nr 2006/2004 i dyrektywy 2009/22/WE (rozporządzenie w sprawie ODR w sporach konsumenckich)[18]. Z oczywistych względów postanowienia dyrektywy znalazły odzwierciedlenie w postanowieniach prawa wewnętrznego poszczególnych państw członkowskich, co w przypadku Polski zakończyło się przyjęciem ustawy z 23.9.2016 r. o pozasądowym rozwiązywaniu sporów konsumenckich, która odnosi się również do sporów o charakterze transgranicznym[19]. Te akty prawa unijnego i prawa wewnętrznego determinują obecny kształt rozwoju ODR w Polsce. Niewątpliwie zatem ważnym etapem w utrwalaniu rozwoju mediacji online było zapewnienie przez ustawodawcę unijnego możliwości wykorzystywania tej metody w rozwiązywaniu sporów w sprawach konsumenckich[20].

1.2. Postępowanie w sprawie pozasądowego rozwiązywania sporów konsumenckich

Wdrożenie do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady 2013/11/UE z 21.5.2013 r. w sprawie alternatywnych metod rozstrzygania sporów konsumenckich oraz zmiany rozporządzenia (WE) Nr 2006/2004

[13] *K. Mania*, Online…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 384.
[14] III CZP 26/99, OSNC 2000, Nr 9, poz. 152.
[15] *Ibidem*.
[16] *K. Mania*, Online…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 383–384.
[17] Dz.Urz. UE L Nr 165, s. 63; dalej jako: dyrektywa 2013/11/UE.
[18] Dz.Urz. UE L Nr L Nr 165, s. 1; dalej jako: rozporządzenie Nr 524/2013.
[19] *K. Flaga-Gieruszyńska*, Przyszłość transgranicznych sporów konsumenckich – wybrane zagadnienia, [w:] *M. Kraska*, *S. Mamrot* (red.) Cyfrowe usługi publiczne w Europie, Poznań 2017, s. 13, https://www.eprawo.net/ (dostęp z 19.8.2017 r.).
[20] *K. Antolak-Szymanski*, *O.M. Piaskowska*, Mediacja w postępowaniu cywilnym. Komentarz, Warszawa 2017, s. 203–204.

i dyrektywy 2009/22/WE (dyrektywa w sprawie ADR w sporach konsumenckich) oznaczało konieczność zapewnienia konsumentom dostępu do prostych, skutecznych, szybkich i tanich sposobów rozstrzygania sporów krajowych i transgranicznych wynikających z umów sprzedaży lub świadczenia usług. Z preambuły powoływanej dyrektywy wynika, że taki dostęp powinien być zapewniony zarówno w przypadku transakcji dokonywanych przez Internet, jak i pozostałych transakcji i ma on szczególne znaczenie, gdy konsumenci dokonują transgranicznych zakupów towarów i usług. Duży nacisk został położony na tworzenie zintegrowanego internetowego systemu rozwiązywania sporów konsumenckich metodami ODR, w tym mediacji online. Niniejsza dyrektywa oraz rozporządzenie 524/2013 stanowią powiązane i wzajemnie uzupełniające się instrumenty prawne, przy czym w art. 5 rozporządzenia przewidziano ustanowienie platformy ODR, która zapewnia konsumentom i przedsiębiorcom jeden punkt dostępu służący do pozasądowego rozstrzygania sporów internetowych przez podmioty ADR w ramach wysokiej jakości postępowań ADR[21].

Jeśli chodzi o podmioty ADR w Polsce, system pozasądowego rozwiązywania sporów konsumenckich – wprowadzony ustawą z 23.9.2016 r. o pozasądowym rozwiązywaniu sporów konsumenckich[22] – opiera się na podejściu mieszanym, co oznacza, że obok siebie działają zarówno podmioty publiczne, jak i niepubliczne. Podmioty te zajmują się rozwiązywaniem sporów typowych dla danego sektora gospodarki, dla którego zostały utworzone. Natomiast jeżeli w jakimś sektorze nie utworzono podmiotu uprawnionego do prowadzenia postępowania w sprawie pozasądowego rozwiązywania sporów konsumenckich, to właściwy dla niego będzie podmiot o charakterze horyzontalnym, tj. Inspekcja Handlowa. Zapewnia to tzw. pełne pokrycie sektorowe – każdy spór konsumencki może być rozwiązany przez właściwy, wyspecjalizowany podmiot. Model ten w dużym stopniu bazuje na już funkcjonujących rozwiązaniach, które sprawdzają się w praktyce, ale jest jednocześnie otwarty na powstawanie nowych podmiotów.

System pozasądowego rozwiązywania sporów konsumenckich obejmuje:

1) niepubliczne sektorowe podmioty utworzone przez przedsiębiorców z danej branży (funkcjonujące obecnie lub nowo powstałe). Przykładem jest Arbiter Bankowy, podmiot utworzony przez Związek Banków Polskich;
2) publiczne sektorowe podmioty utworzone „przy" lub „w" strukturze organów publicznych. Przykładami są: Koordynator do spraw negocjacji działający przy Prezesie Urzędu Regulacji Energetyki, Rzecznik Praw Pasażera Kolei działający przy Prezesie Urzędu Transportu Kolejowego, Prezes Urzędu Komunikacji Elektronicznej, Rzecznik Finansowy;
3) podmiot o charakterze horyzontalnym – Inspekcja Handlowa, która zajmuje się sprawami, dla których nie został utworzony właściwy podmiot sektorowy[23].

Zarówno podmioty publiczne, jak i niepubliczne, aby uzyskać status podmiotu uprawnionego do pozasądowego rozwiązywania sporów konsumenckich, muszą zostać wpisane do rejestru prowadzonego przez Prezesa Urzędu Ochrony Konkurencji i Konsumentów (UOKiK). Podmiot wpisany do rejestru może zostać notyfikowany Komisji Europejskiej jako podmiot uprawniony do prowadzenia postępowań w sprawie pozasądowego rozwiązywania sporów konsumenckich. Co ważne, udział podmiotów publicznych w systemie pozasądowego rozwiązywania sporów konsumenckich jest obowiązkowy[24].

Jeśli idzie o definicję konsumenta, dyrektywa 2013/11/UE rozszerza dotychczasowe rozumienie pojęcia konsumenta przy uwzględnieniu orzecznictwa TS, tym samym pośrednio obejmując przedsiębiorców. Na gruncie omawianej dyrektywy definicja konsumenta obejmuje osoby fizyczne, których działania nie mają związku z ich działalnością handlową, gospodarczą, rzemieślniczą lub wykonywaniem wolnego zawodu. Jeśli jednak umowa została zawarta przez przedsiębiorcę w celu częściowo niemającym takiego związku (umowy o podwójnym celu), a cel związany z działalnością gospodarczą jest na tyle ograniczony, że nie ma charakteru przeważającego w ogólnym kontekście umowy, osobę taką należy również uznać za konsumenta[25].

Dyrektywa nie wprowadziła definicji form ADR w sporach konsumenckich, jednak w pojęciu tym mieści się mediacja, na co wskazuje bezpośrednie odwołanie w motywie 19 preambuły[26]. Choć dyrektywa nie statuuje definicji ADR, jednak w wielu przepisach, w szczególności w art. 2 ust. 1, opisuje formy postępowań ADR jako:

1) narzucanie rozwiązania sporu przez podmiot ADR,
2) proponowanie rozwiązania sporu przez podmiot ADR,
3) doprowadzenie przez podmiot ADR do spotkania stron w celu ułatwienia polubownego rozstrzygnięcia[27].

[21] *M. Białek*, Mediacja…, [w:] *A. Torbus* (red.), Mediacja…, s. 334–335.

[22] Dz.U. poz. 1823; dalej jako: SporKonsU.

[23] Uzasadnienie do ustawy o pozasądowym rozwiązywaniu sporów konsumenckich, Druk sejmowy Nr 630, s. 4.

[24] UOKiK, Polubowne rozwiązywanie sporów konsumenckich od 10.1.2017 r. Pytania i odpowiedzi, Warszawa 2016, s. 6–8, https://www.uokik.gov.pl/download.php?plik=18703 (dostęp z 20.8.2017 r.).

[25] *R. Flejszar*, *K. Gajda-Roszczynialska*, Alternatywne metody rozwiązywania sporów ze szczególnym uwzględnieniem mediacji – postępowanie cywilne, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja, teoria, normy, praktyka, Warszawa 2017, s. 247–248.

[26] *K. Mania*, Online…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 386.

[27] *Ł. Goździaszek*, Internetowy system pozasądowego rozstrzygania sporów konsumenckich w Unii Europejskiej. Komentarz, Warszawa 2017, s. 30.

Jak wskazuje *Ł. Goździaszek*[28], narzucanie rozwiązania sporu jest bliskie pojęciu sądownictwa polubownego, proponowanie rozwiązania oraz doprowadzenie do spotkania stron odpowiadają zaś pojęciu mediacji lub ugodowego załatwienia sprawy.

Polski ustawodawca, implementując dyrektywę 2013/11, w art. 3 SporKonsU wskazał, że postępowaniem w sprawie pozasądowego rozwiązywania sporów konsumenckich jest postępowanie mające na celu rozwiązanie sporu konsumenckiego, prowadzone zgodnie z zasadami określonymi w tej ustawie i polegające na:

1) umożliwieniu zbliżenia stanowisk stron w celu rozwiązania sporu przez jego strony;
2) przedstawieniu stronom propozycji rozwiązania sporu;
3) rozstrzygnięciu sporu i narzuceniu stronom jego rozwiązania[29].

Należy zauważyć, że dwie pierwsze formy postępowania niewątpliwie odpowiadają w swej istocie mediacji. Zgodnie z art. 37 ust. 1 SporKonsU postępowanie w sprawie pozasądowego rozwiązywania sporów konsumenckich prowadzi się w postaci papierowej lub elektronicznej. Powyższy przepis jednoznacznie wskazuje zatem na możliwość prowadzenia przez podmioty ADR postępowania w sprawie pozasądowego rozwiązywania sporów konsumenckich polegającego na umożliwieniu zbliżenia stanowisk stron w celu rozwiązania sporu przez jego strony lub przedstawieniu stronom propozycji rozwiązania sporów, które potocznie nazywane postępowaniami mediacyjnymi, w wersji elektronicznej przybierają postać e-mediacji. Ustawodawca unijny kładzie nacisk przede wszystkim na postępowanie elektroniczne. I tak, zgodnie z dyrektywą ADR, podmiot ADR musi być gotów przyjąć wniosek konsumenta wraz z załącznikami w postaci elektronicznej oraz umożliwić wymianę informacji między stronami za pomocą środków elektronicznych, strony zaś powinny mieć możliwość podawania informacji i przedstawiania dowodów bez potrzeby fizycznej obecności (motyw 42 dyrektywy ADR)[30]. Oznacza to, że wspomniane postępowanie może odbyć się w całości w środowisku online, a istniejące ramy prawne umożliwiają przeprowadzenie mediacji online w pełni drogą elektroniczną. Od regulaminu podmiotu ADR zależeć będzie, czy wymagana jest fizyczna obecność stron postępowania lub ich pełnomocników. Wśród polskich podmiotów dostępnych na platformie ODR większość zastrzega sobie, że w niektórych przypadkach fizyczna obecność stron postępowania lub ich pełnomocników może być wymagana (m.in. poszczególni wojewódzcy inspektorowie Inspekcji Handlowej, Koordynator do spraw negocjacji przy Prezesie Urzędu Regulacji Energetyki, Rzecznik Finansowy), natomiast postępowanie przed takimi podmiotami, jak np. Prezes Urzędu Komunikacji Elektronicznej oraz Stowarzyszenie Praw Pasażerów Przyjazne Latanie, nie wymaga fizycznej obecności stron ani ich pełnomocników.

W związku z potrzebą zapewnienia spójności terminologicznej należy wyjaśnić kwestię ogólnego usytuowania instytucji mediacji w prawie polskim. W ustawach szczegółowych[31] zmienianych ustawą o pozasądowym rozwiązywaniu sporów konsumenckich nastąpiło ujednolicenie terminologiczne, w konsekwencji czego wszystkie publiczne podmioty ADR prowadzą postępowanie w sprawie pozasądowego rozwiązywania sporów konsumenckich. Wcześniej bowiem pojęciami mediacja, postępowanie mediacyjne nazywane były także postępowania ustawowe, do których nie stosowało się przepisów Kodeksu postępowania cywilnego (ustawa o Inspekcji Handlowej, mediacja przed Prezesem UKE)[32]. Poczynione rozróżnienie terminologiczne (mediacja – postępowanie w sprawie pozasądowego rozwiązywania sporów konsumenckich) służy pewnemu uporządkowaniu oraz zapewnieniu zgodności z zasadami techniki prawodawczej, nie wpływa jednak na samą istotę postępowania w sprawie pozasądowego rozwiązywania sporów konsumenckich, które, jeśli jest niewiążące, w wersji elektronicznej przybiera postać e-mediacji.

1.3. Platforma internetowego rozstrzygania sporów konsumenckich

Fundamentalnym celem rozporządzenia 524/2013 było statuowanie platformy ODR, która w praktyce jest systemem teleinformatycznym z interefejsem strony internetowej (https://webgate.ec.europa.eu/odr/main). Platformę ODR należy utożsamiać z portalem dostępowym – serwisem informacyjnym wzbogaconym o funkcjonalność, dzięki której konsumenci mogą kontaktować się z działającym na rynku podmiotem ADR[33]. Platforma ODR służy zatem krajowym podmiotom ADR, które prowadzą postępowanie ADR w oparciu o własne (krajowe) przepisy proceduralne, przy czym przepisy te w znacznej mierze są pochodną zasad postępowania ADR ustanowionych w dyrektywie 2013/11.

Za pośrednictwem platformy konsument ma możliwość złożenia skargi dotyczącej towarów lub usług zakupionych przez Internet oraz może znaleźć niezależną stronę trzecią (podmiot ADR), która zajmie się rozwiązaniem sporu. W odniesieniu do dostępności usług ODR w ramach platformy występują ograniczenia zarówno natury podmiotowej, jak i przedmiotowej. Pierwszym z nich jest domicyl, ponieważ

[28] *Ibidem*.

[29] *Ł. Goździaszek*, Internetowy system…, s. 31.

[30] Uzasadnienie do ustawy o pozasądowym rozwiązywaniu sporów konsumenckich, Druk sejmowy Nr 630, s. 18, http://orka.sejm.gov.pl/Druki8ka.nsf/0/4169A98E5E473726C1257FD9002D8320/%24File/630.pdf (dostęp z 20.8.2017 r.).

[31] Prawo energetyczne, Ustawa o Inspekcji Handlowej, Prawo lotnicze, Ustawa o transporcie kolejowym, Prawo telekomunikacyjne, Ustawa o nadzorze nad rynkiem finansowym, Prawo pocztowe.

[32] Uzasadnienie do ustawy o pozasądowym rozwiązywaniu sporów konsumenckich, Druk sejmowy Nr 630, s. 10.

[33] *Ł. Goździaszek*, Internetowy system…, s. 32.

platforma nie obsługuje: konsumentów mieszkających poza terytorium UE i konsumentów składających skargę dotyczącą sprzedawcy z siedzibą poza UE. Z platformy można korzystać na użytek sporów transgranicznych, jak też wyłącznie krajowych. Drugim ograniczeniem podmiotowym jest wyłączenie stosowania platformy wobec konsumentów składających skargę dotyczącą innych konsumentów, a także przedsiębiorców składających skargę dotyczących innych przedsiębiorców[34]. Ograniczenie przedmiotowe z kolei odnosi się do określonych rodzajów transakcji i usług, ponieważ nie można wykorzystywać platformy do dochodzenia roszczenia powstałego w związku z umowami sprzedaży lub umowami o świadczenie usług zawartymi nieinternetowo. Celem prawodawcy unijnego było zatem wsparcie wyłącznie handlu elektronicznego.

Proces składania skargi odbywa się wyłącznie online. Po wypełnieniu formularza skargi sprzedawca jest informowany o jej treści, by w terminie 10 dni kalendarzowych wybrać podmiot oferujący usługi ADR, na co konsument może wyrazić zgodę w terminie kolejnych 10 dni. Platforma automatycznie przekazuje skargę podmiotowi ADR, z którego skorzystają strony zgodnie z wcześniejszymi uzgodnieniami. Jeśli w ciągu 30 dni kalendarzowych od wniesienia skargi strony nie osiągną porozumienia w sprawie wyboru podmiotu ADR lub gdy wskazany podmiot odmówi rozpatrywania danego sporu, skarga nie jest dalej rozpatrywana. Organ, który podjął się rozwiązania sporu, ma 90 dni na jego rozstrzygnięcie i w tym terminie powinien powiadomić strony o swojej decyzji. Należy pamiętać, że postępowanie toczy się według reguł ustalonych przez wybrany przez strony organ, a natura prawna zakończenia sprawy jest zdeterminowana rodzajem organu, który strony sporu wybrały, ponieważ może on co do zasady stosować metody koncyliacyjne, ale może również wydać rozstrzygnięcie wiążące dla stron, jeżeli wybrały one organ o charakterze arbitrażowym[35]. Wśród polskich organów ADR, które są dostępne na platformie ODR, obecnie większość stosuje metody koncyliacyjne, wobec czego postępowania w sprawie pozasądowego rozwiązywania sporów przyjmują najczęściej postać e-mediacji, której szczegółowe zasady określone są w regulaminach danych podmiotów.

W literaturze przedmiotu często podkreśla się, że specyfika e-mediacji polega na tym, że występuje w niej tzn. czwarta strona[36]. Jest nią oprogramowanie służące do komunikacji i wymiany treści, organizowania informacji, monitorowania korespondencji. Czwarta strona niejako wyręcza mediatora przy czynnościach, które musi on podjąć. Określenie czwarta strona jest przenośnią mającą za zadanie podkreślić silny wpływ urządzeń elektronicznych na przebieg e-mediacji[37]. Platforma ODR odgrywa niewątpliwie rolę czwartej strony w postępowaniach w sprawie pozasądowego rozwiązywania sporów konsumenckich, służy ona przede wszystkim wsparciu ich inicjacji i obsługi informatycznej.

2. E-mediacja jako alternatywa wewnętrzna. Dopuszczalność e-mediacji w KPC

Alternatywami wewnętrznymi nazywa się w literaturze te formy postępowania sądowego, które nie mają charakteru postępowania adjudykacyjnego[38]. Postępowanie mediacyjne stanowi zatem przykład takiej alternatywnej metody rozwiązywania sporów. Stosowanie e-mediacji będzie możliwe we wszystkich sprawach, w których zawarcie ugody jest dopuszczalne. Zgodnie z art. 10 KPC sąd dąży w każdym stanie postępowania do ugodowego załatwienia sprawy, w szczególności poprzez nakłanianie stron do mediacji. Oznacza to, że skorzystanie z mediacji online będzie związane ściśle z pojęciem zdatności ugodowej danej sprawy cywilnej[39]. Jako przykłady sporów, które mogą być rozwiązywane w drodze mediacji online, uznać należy spory z udziałem konsumentów, a zatem zgodnie z art. 22^1 KC z osobami fizycznymi dokonującymi z przedsiębiorcami czynności prawnych niezwiązanych bezpośrednio z ich działalnością gospodarczą lub zawodową. W przeciwieństwie do postępowania w sprawie pozasądowego rozwiązywania sporów dostępnego przez platformę ODR mediacja w wersji elektronicznej w ramach KPC swoim zakresem przedmiotowym objąć może spory pomiędzy konsumentem a przedsiębiorcą wynikające z umów zawartych zarówno internetowo, jak i bez użycia środków komunikacji elektronicznej w Internecie.

W odniesieniu do mediacji, która miałaby być prowadzona przy użyciu środków komunikacji elektronicznej, wydaje się, że rozstrzygnięcia wymagają trzy problemy, które warunkują możliwość prowadzenia e-mediacji na gruncie przepisów Kodeksu postępowania cywilnego[40].

Pierwszą kwestią poddaną pod rozwagę będzie zawarcie umowy o mediację drogą elektroniczną. Zgodnie z art. 183^1 § 2 zd. 1 KPC mediację prowadzi się m.in. na podstawie umowy. Nie ma jednocześnie wskazań, w jakiej formie umowa ta ma być zawarta. Opierając się na poglądzie wyrażonym w doktrynie, umowa o mediację może być zawarta

[34] *K. Flaga-Gieruszyńska*, Przyszłość…, [w:] *M. Kraska*, *S. Mamrot* (red.) Cyfrowe…, s. 15.

[35] *Ibidem*, s. 17.

[36] Pojęcie to wprowadzili *E. Katsh*, *J. Rifkin*, Online Dispute Resolution: resolving Conflicts in Cyberspace, San Francisco 2001, s. 93 i n. [za:] *L. Wing*, *D. Rainey*, Online dispute resolution and the development of theory, s. 41, https://www.mediate.com/pdf/wing_rainey.pdf (dostęp z 10.8.2017 r.).

[37] *M. Grabowski*, E-mediacja…, s. 49.

[38] Zob. *L. Morawski*, Proces…, s. 21; *tenże*, Główne problemy…, s. 228, *Ł. Błaszczak*, Mediacja…, s. 13.

[39] *M. Białek*, Mediacja…, [w:] *A. Torbus* (red.), Mediacja…, s. 333.

[40] *P. Rodziewicz*, Czy istnieje potrzeba wprowadzenia instrumentu prawnego dotyczącego Online Dispute Resolution (ODR) w zakresie rozstrzygania sporów wynikłych z transgranicznych transakcji handlu elektronicznego?, PME 2012, Nr 1, s. 40.

w dowolnej formie, w tym również *per facta concludentia*[41]. W związku z powyższym zawarcie umowy o mediację może nastąpić przy użyciu technik komunikacji elektronicznej, np. poczty elektronicznej. Należy nadmienić, że drugą podstawą do prowadzenia mediacji jest postanowienie sądu kierujące strony do mediacji, jednak obecnie obowiązujące przepisy nie przewidują, aby mogło być one wydane przez sąd w postaci elektronicznej, jest ono bowiem objęte ograniczeniami wynikającymi z zasady oficjalności doręczeń.

Kolejną, a zarazem najistotniejszą kwestią jest odpowiedź na pytanie, czy stosownie do regulacji kodeksowych posiedzenie mediacyjne może odbyć się na odległość przy użyciu internetowych środków komunikacji elektronicznej. Zgodnie z art. 183^{11} KPC mediator niezwłocznie ustala termin i miejsce posiedzenia mediacyjnego. Wyznaczenie posiedzenia mediacyjnego nie jest wymagane, jeśli strony zgodzą się na przeprowadzenie mediacji bez posiedzenia mediacyjnego. Ustawodawca przewidział zatem dwie formy prowadzenia mediacji: na posiedzeniu mediacyjnym i poza nim. Jak trafnie zauważa *K. Mania*[42], brak normatywnej definicji mediacji bez posiedzenia pozwala uznać, że mieści się w nim także mediacja prowadzona drogą online, np. poprzez wideokonferencję. Wprowadzenie możliwości prowadzenia mediacji bez posiedzenia wydaje się stanowić znaczny ukłon w stronę implementacji nowoczesnych form komunikacji w ramach Online Dispute Resolution.

Ostatnie sygnalizowane zagadnienie stanowi kwestia rezultatu mediacji – zawarcie ugody bądź zakończenie procedury bez jej uzyskania. Z powyższym zagadnieniem łączy się obowiązek przygotowania protokołu opisującego przebieg mediacji. Aby odpowiedzieć na pytanie, czy możliwe jest zawarcie ugody na drodze elektronicznej, co implikuje e-mediację, należy przeanalizować brzmienie art. 183^{12} § 2 KPC. Wspomniany przepis zawiera obowiązek stron do podpisania ugody, a także stwierdza, że niemożność podpisania ugody mediator stwierdza w protokole. W związku z ugodą rozróżnić można dwie sytuacje. Pierwsza – gdy ugoda zostaje zawarta przed mediatorem, jednak żadna ze stron nie występuje o jej zatwierdzenie, wówczas ugoda taka wywołuje jedynie skutki ugody pozasądowej, tj. umowy prawa cywilnego[43]. Mając powyższe na uwadze, zawarcie ugody pozasądowej przy użyciu środków komunikacji elektronicznej jest dopuszczalne, ponieważ ugoda taka nie wymaga dla swojej ważności złożenia podpisów (chyba że co innego wynika z przepisów regulujących formę czynności prawnej). Druga sytuacja dotyczy natomiast ugody zawartej w drodze elektronicznej, która, wpisana do protokołu, ma podlegać zatwierdzeniu przez sąd. Dla zatwierdzenia ugody mediacyjnej wymagane jest złożenie podpisów przez strony wraz z protokołem podpisanym przez mediatora, co w praktyce uniemożliwia przeprowadzenie pełnego postępowania mediacyjnego online[44]. Należy jednak zwrócić uwagę na pewną lukę w przepisach, która mogłaby być interpretowana *in favorem* e-mediacji. Artykuł 183^{12} § 2 KPC przewiduje sytuację, w której podpisanie ugody nie jest możliwe. Jak wskazuje się w doktrynie, gdy strony zawarły ugodę bez możliwości złożenia podpisu, wtedy mediator ma obowiązek stwierdzić w protokole tę niemożność, nie ograniczając się tylko do owej informacji, ale wskazując okoliczności wpływające na taki stan[45]. Z pewnością niemożność podpisania ugody obejmuje wszelkie przypadki, w których strona z uwagi na fizyczne ograniczenia nie może złożyć podpisu. W odniesieniu do e-mediacji można zaryzykować stwierdzenie, że takim czynnikiem byłby fizyczny (geograficzny) dystans dzielący strony[46]. Wydaje się, że tak szeroka interpretacja pojęcia niemożności podpisania ugody jest trafna i uzasadniona w kontekście dobrowolności mediacji i postulatu autonomii stron w mediacji oraz odformalizowania ugód[47]. Choć zdawałoby się, że powyższa konstatacja rozwiązuje problem podpisania ugody, powinno się w tym miejscu podkreślić, że decyzja sądu w przedmiocie zatwierdzenia ugody ma charakter uznaniowy. Z praktyki zaś wynika, że sądy najczęściej wzywają strony do podpisania ugody[48], nie dopuszczając możliwości zatwierdzenia niepodpisanej ugody, co niejako przekreśla zawarcie ugody sądowej za pomocą technik komunikacji elektronicznej w mediacji online.

Mimo że istniejące ramy prawne w zakresie mediacji zdają się dopuszczać e-mediację jako jedną z metod ODR, należy zauważyć, że jej pełne przeprowadzenie za pomocą środków komunikacji elektronicznej jest obecnie utrudnione.

Podsumowanie

Zarówno rozwój alternatywnych metod rozwiązywania sporów, jak i tym bardziej *Online Dipsute Resolution*, koresponduje z koncepcją społeczeństwa aktywnego, wyedukowanego konsumenta świadomego swoich praw i przedsiębiorcy skłonnego do ustępstw. Tymczasem w Polsce istotną barierą psychologiczno-społeczną w rozwoju mediacji jest brak chęci korzystania z autonomii woli w rozwiązywaniu sporów cywilnych, w tym konsumenckich, i ciągle silna potrzeba rozstrzygnięcia każdego, nawet najdrobniejszego, sporu na drodze sądowej z udziałem państwowego wymiaru sprawie-

[41] *Ibidem.*

[42] *K. Mania*, Online…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 372.

[43] *P. Telenga*, [w:] *A. Jakubecki* (red.), Kodeks postępowania cywilnego, Komentarz, wyd. 3, Warszawa 2008, s. 280.

[44] *K. Mania*, Online…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 373.

[45] *R. Morek*, Mediacja i arbitraż (art. 183^{1}–183^{15}, 1154–1217 KPC). Komentarz, Warszawa 2006, s. 81.

[46] *T.P. Antoszek*, Dopuszczalność…, [w:] *J. Czapska*, *M. Szeląg-Dylewski* (red.), Mediacja…, s. 134.

[47] *Ibidem*, s. 134.

[48] Zob. *K. Mania*, Online…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 373; *T.P. Antoszek*, Dopuszczalność…, [w:] *J. Czapska*, *M. Szeląg-Dylewski* (red.), Mediacja…, s. 134.

dliwości poprzez uzyskanie władczego rozstrzygnięcia, co jest związane ze swoistym paradoksem, polegającym na tym, że społeczeństwo pomimo niskiego zaufania do sądów oraz długości postępowań sądowych decyduje się na skorzystanie z drogi sądowej[49].

Biorąc pod uwagę specyfikę sporów konsumenckich, można mieć nadzieję, że dzięki pracom legislacyjnym na poziomie krajowym i europejskim zarówno mediacja, jak i jej wersja elektroniczna staną się nie tylko teoretycznie, ale także praktycznie efektywnym narzędziem w rozwiązywaniu tych sporów. Celem niniejszego artykułu było zaprezentowanie koncepcji e-mediacji jako właściwej i dopuszczalnej przez polskiego ustawodawcę metody rozwiązywania sporów konsumenckich, realizującej postulat ochrony praw konsumentów. Postępowanie w sprawie pozasądowego rozwiązywania sporów konsumenckich wprowadzone w dyrektywie 2013/11/UE implementowanej przez Polskę ustawą o pozasądowym rozwiązywaniu sporów konsumenckich**,** które bardzo często przyjmuje postać e-mediacji, z całą pewnością może być użytecznym narzędziem do rozwiązywania sporów zarówno krajowych, jak i transgranicznych powstałych w związku z umowami zawartymi internetowo. Przepisy Kodeksu postępowania cywilnego również dopuszczają prowadzenie e-mediacji, która może okazać się szczególnie przydatna, gdy umowa pomiędzy konsumentem a przedsiębiorcą została zawarta poza Internetem.

Warto ponadto zauważyć, że stanowiące powiązane i wzajemnie uzupełniające się instrumenty prawne – dyrektywa 2013/11/UE dotycząca pozasądowego rozstrzygania sporów konsumenckich wymagająca wprowadzenia daleko posuniętych konkretnych rozwiązań, takich jak: zapewnienie szerokiej dostępności podmiotów i postępowań ADR, prowadzenie wykazów podmiotów ADR, zapewnienie dostępu do postępowania ADR nieodpłatnego lub dostępnego za opłatą o nieznacznej wysokości, oraz rozporządzenie 524/2013 przewidujące ustanowienie platformy ODR – wpływają nie tylko pozytywnie na rozwój e-mediacji w sprawach konsumenckich, lecz także mogą przyczynić się do popularyzacji metod ODR w rozwiązywaniu innych sporów prawnych.

[49] Zob. *R. Flejszar*, *K. Gajda-Roszczynialska*, Alternatywne…, [w:] *K. Płeszka*, *J. Czapska*, *M. Araszkiewicz*, *M. Pękala* (red.), Mediacja…, s. 249.

Słowa kluczowe: mediacja, e-mediacja, ODR, ADR, konsument, spory konsumenckie

E-mediation as an out of court method of consumer disputes

The aim of the present study is the analysis of functioning of e-mediations (online mediations) regarding consumer disputes in the Polish legal system in the context of EU regulations (directive regarding ADR in consumer disputes 2013/11/EU and the regulation regarding online system of consumer disputes resolution no. 524/2013). The author describes the concept of e-mediations regarding consumer disputes, their technical aspects, and also the principle of e-mediations proceedings conducted by specialized entities within the framework of the online system of consumer disputes resolutions created in the regulation 524/2013.

Key words: mediation, e-mediation, Online Dispute Resolution, Alternative Dispute Resolution, consumer, consumer disputes.

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

Beck Akademia
konferencje • szkolenia • e-learning

Szkolenia dla praktyków

KALENDARIUM 2018

styczeń	30 stycznia	Zasady obliczania powierzchni najmu w kamienicach	Adrian Hołub
	31 stycznia	Upadłość konsumencka w praktyce	SSR Cezary Zalewski
luty	1 lutego	Kodeks karny skarbowy – dla praktyków	dr Adam Bartosiewicz
	6 lutego	Nowelizacja Kodeksu postępowania administracyjnego z 1.6.2017 r.	SWSA Tomasz Grossmann
	13 lutego	Nowe orzecznictwo w sprawach inwestycji budowlanych – zagospodarowanie przestrzenne i prawo budowlane	r.pr. dr Tomasz Filipowicz SNSA Alicja Plucińska-Filipowicz
	15 lutego	PODATKI 2018: VAT – fakturowanie i ewidencjonowanie. CIT i PIT – ograniczenia optymalizacji, zmienione limity kosztów	Kalina Figurska, Katarzyna Kozakowska, Rafał Sidorowicz
	20 lutego	Prawo restrukturyzacyjne w praktyce	SSR Cezary Zalewski
	24 lutego–19 maja	Kurs przygotowujący do egzaminu na doradcę podatkowego – IX edycja	Piotr Bujnowicz, Mateusz Latkowski, dr Ireneusz Mirek, Małgorzata Sęk, Patryk Smęda, dr Michał Wilk
	27–28 lutego	Dwudniowe warsztaty: OCHRONA DANYCH OSOBOWYCH – dostosowanie przedsiębiorców do ogólnego rozporządzenia o ochronie danych	mec. Xawery Konarski, adw. dr Grzegorz Sibiga
marzec	5 marca	Udzielanie i wykonywanie zamówień publicznych 2018 – konferencja	Prowadzący konferencję: prof. Ryszard Szostak
	16 marca	Upadłość konsumencka w praktyce	SSO Anna Hrycaj
	22 marca	Zmiany w postępowaniu administracyjnym a prawo nieruchomości	dr Maciej J. Nowak
	27 marca	Czas pracy 2018	mec. Piotr Wojciechowski



Więcej informacji:
www.akademia.beck.pl tel.: **22 311 22 22**

Beck Akademia
konferencje • szkolenia • e-learning

KONFERENCJE I SZKOLENIA

SZKOLENIE 2-DNIOWE

Przygotowanie do wdrożenia ogólnego rozporządzenia o ochronie danych przez przedsiębiorców

Warszawa 27–28 lutego 2018 r.

Prowadzący: adw. Xawery Konarski, adw. dr Grzegorz Sibiga

Udział w szkoleniu pozwoli m.in.:

- usystematyzować wiedzę na temat obowiązków przedsiębiorców określonych w ogólnym rozporządzeniu o ochronie danych,
- poznać możliwy sposób wdrożenia w przedsiębiorstwie nowych przepisów ogólnego rozporządzenia o ochronie danych,
- ustalić harmonogram działań wdrażających nowe przepisy,
- zapoznać się z aktualnym stanem dostosowania prawa polskiego do ogólnego rozporządzenia o ochronie danych oraz z działaniami właściwych organów w celu wykonania przepisów.

SZKOLENIE 1-DNIOWE

Ochrona danych osobowych – Dostosowanie przedsiębiorców do ogólnego rozporządzenia o ochronie danych

Warszawa 4 kwietnia 2018 r.

Prowadzący: adw. Xawery Konarski, adw. dr Grzegorz Sibiga

Celem szkolenia jest omówienie praktycznych aspektów dostosowania działalności przedsiębiorców do nowych przepisów oraz przedstawienie działań dostosowawczych i ich harmonogramu.

DOWIEDZ SIĘ WIĘCEJ!

Wejdź na: **www.AKADEMIA.beck.pl** lub napisz na **akademia@beck.pl**