PME
1/2018

PRAWO Mediów Elektronicznych

www.ksiegarnia.beck.pl

ISSN 2082-100X

Cena 65 zł (w tym 5% VAT)

C.H.BECK

PME

1/2018

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 pierwszy w 2018 r. numer kwartalnika naukowego Prawo Mediów Elektronicznych. Tradycyjnie został on poświęcony problematyce prawnej związanej z prawem nowych technologii. W bieżącym numerze znajdziecie Państwo m.in.: artykuł dotyczący elektronicznej identyfikacji w Unii Europejskiej autorstwa *A. Burek* oraz Telemedycyna transgraniczna w zakresie prawa właściwego dla odpowiedzialności deliktowej autorstwa *A. Nowak*, a również E-wymiar sprawiedliwości w aspekcie europejskim na przykładzie projektu e-Codex autorstwa *L. Łuczak-Noworolnik*. Zapoznacie się Państwo także ze sprawozdaniem z konferencji naukowej, która odbyła się w Wiedniu w październiku 2017 r. Common Vision Confernece 2017 w relacji *M. Kaczorowskiej*. Na koniec zachęcam do lektury artykułu *K. Klimas* o elektronicznej komunikacji pomiędzy stronami a sądem w sprawie drobnych roszczeń oraz opracowania *P. Siemkowicza* o kradzieży tożsamości w Internecie z perspektywy prawa karnego.

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

Zachęcam do lektury,

prof. dr hab. *Jacek Gołaczyński*

Sprawozdanie: „Common Vision Conference 2017. Tradition meets Innovation", Wiedeń, 5–6.10.2017 r.[1]

dr *Maria Kaczorowska*[2]

Problematyka rejestracji nieruchomości oraz dostępu do informacji o nieruchomościach w kontekście nowych możliwości wynikających z upowszechnienia zaawansowanych technologii informatycznych zajmuje współcześnie ważne miejsce w dyskusji nad kierunkami rozwoju społeczno-gospodarczego w poszczególnych krajach, jak również w skali ogólnoeuropejskiej i w wymiarze globalnym. Do inicjatyw służących propagowaniu szerokiego udostępnienia i wykorzystania zasobów informacji przestrzennych, w tym pochodzących z elektronicznych rejestrów publicznych, w celu zapewnienia bezpieczeństwa obrotu nieruchomościami, racjonalnego planowania przestrzennego, a także realizacji idei zrównoważonego rozwoju zaliczają się wspólne działania podejmowane w ramach porozumienia Common Vision przez europejskie organizacje aktywne w dziedzinie ksiąg wieczystych, katastru, geodezji i kartografii. W efekcie współpracy między Europejskim Serwisem Informacji o Nieruchomościach (European Land Information Service – EULIS), Europejskim Stowarzyszeniem Rejestrów Nieruchomości (European Land Registries Association – ELRA), Organizacją EuroGeographics, Stałym Komitetem ds. Katastru Unii Europejskiej (Permanent Committee on Cadastre in the European Union – PCC) i Europejską Radą Geodetów (Council of European Geodetic Surveyors, Comité de Liaison des Geometres Europeens – CLGE), jak również Grupą Roboczą ds. Zarządzania Nieruchomościami Europejskiej Komisji Gospodarczej ONZ (United Nations Economic Commission for Europe, Working Party on Land Administration – UNECE-WPLA) i Międzynarodową Federacją *Geodetów* (International Federation of Surveyors, *Fédération* Internationale des *Géomètres* – FIG) zorganizowana została w Wiedniu w dniach 5–6 października 2017 r. druga konferencja z cyklu „Common Vision"[3], której temat przewodni brzmiał „Tradition meets Innovation". Głównym jej organizatorem był *Austriacki* Federalny Urząd Geodezji i Metrologii (Bundesamt für Eich- und Vermessungswesen – *BEV*). Obrady konferencji połączono z obchodami 200. rocznicy powstania austriackiego katastru[4]. W konferencji uczestniczyli, poza członkami wymienionych organizacji współpracujących w ramach inicjatywy Common Vision, przedstawiciele krajowych instytucji prowadzących rejestry nieruchomości oraz służb geodezyjno-kartograficznych, a także środowiska naukowego z różnych krajów europejskich, w tym z Polski.

Zagadnienia poruszane w prezentowanych podczas konferencji referatach dotyczyły przede wszystkim roli tradycyjnych instytucji związanych z procesem rejestracji nieruchomości – ksiąg wieczystych i katastru nieruchomości – wobec wyzwań związanych z dokonującą się rewolucją cyfrową, w aspekcie poszukiwania rozwiązań, które odpowiadałyby aktualnym wymogom obrotu gospodarczego oraz oczekiwaniom obywateli w dobie społeczeństwa informacyjnego.

Jak podkreślano w wystąpieniach, podejmowane obecnie działania mające na celu sukcesywną modernizację systemów rejestracji nieruchomości funkcjonujących w poszczególnych państwach powinny być ukierunkowane m.in. na zapewnienie sprawnej wymiany informacji poprzez ściślejsze powiązanie zinformatyzowanych rejestrów – prawnego i fizycznego, czego przykładem może być nowoczesna austriacka baza danych o nieruchomościach, obejmująca na bieżąco aktualizowane i synchronizowane ze sobą systemy ksiąg gruntowych i katastru. Wyeksponowana została również potrzeba rozwijania możliwości wykorzystania technik wizualizacji danych przestrzennych w dziedzinie wielopoziomowego zagospodarowania przestrzeni. Realizacji tych założeń podporządkowana jest koncepcja katastru wielowymiarowego i wielozadaniowego, umożliwiającego rejestrację wyodrębnionych przestrzennie obiektów i związanych z nimi praw o charakterze czasowo-przestrzennym (kataster 3D, 4D). Rozwiązania takie są w praktyce wdrażane np. w Holandii. Przedmiotem rozważań podjętych przez referentów były ponadto postulaty dotyczące kształtowania nowoczesnych systemów informacji przestrzennej, których podstawą są wzajemnie powiązane ze sobą dane pochodzące z wielu źródeł, zarówno publicznych, jak i prywatnych, a tym samym dostosowanych w coraz więk-

[1] Sprawozdanie przygotowane w ramach realizacji projektu badawczego „Informatyzacja ksiąg wieczystych", nr rej. 2015/17/B/HS5/00460, finansowanego ze środków Narodowego Centrum Nauki.

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

[3] Pierwsza konferencja współorganizowana przez partnerów tworzących grupę Common Vision odbyła się pod hasłem „Migration to a Smart World" w Amsterdamie 5–7.6.2016 r. Zob. *M. Kaczorowska*, Przyszłość systemów rejestracji nieruchomości wobec rozwoju inteligentnych technologii. Wybrane problemy prawne na tle wniosków z konferencji „Common Vision Conference 2016. Migration to a Smart World", Amsterdam, 5–7 czerwca 2016 r., Opolskie Studia Administracyjno-Prawne 2017, t. 15, nr 2, s. 301–320.

[4] http://www.kataster200.at/kataster200en/ (dostęp z 28.11.2017 r.).

szym stopniu do potrzeb użytkowników. W procesie tym istotne znaczenie ma zastosowanie efektywnych narzędzi przetwarzania zasobów danych typu *big data*, a także wykorzystanie potencjału Internetu rzeczy. W powyższe tendencje wpisuje się idea katastru 4.0, która zakłada stworzenie samoobsługującego się systemu katastralnego opartego na współdziałaniu różnych kategorii podmiotów dostarczających dane oraz inteligentnych urządzeń. Różnorodne możliwości zastosowania tego typu rozwiązań technologicznych, m.in. w dziedzinie poprawy jakości usług publicznych, transportu czy cyberbezpieczeństwa, zostały omówione w ramach prezentacji wyników projektu badawczego „Cadastre 2035" realizowanego na Uniwersytecie Aalto w Finlandii.

Doniosłą rolę w zwiększaniu dostępności i funkcjonalności elektronicznych rejestrów nieruchomości odgrywają wdrażane innowacyjne e-usługi, sprzyjające uproszczeniu i przyspieszeniu transakcji obrotu nieruchomościami. Znaczące postępy pod tym względem widoczne są np. na Litwie, gdzie m.in. uruchomiono publiczne serwisy elektroniczne umożliwiające notariuszom przekazywanie danych *online* do odpowiednich rejestrów. Nowatorskim rozwiązaniem w dziedzinie rejestracji nieruchomości jest także zastosowanie technologii łańcucha bloków (*blockchain*), która ma przyczyniać się do podniesienia poziomu bezpieczeństwa obrotu. Podczas konferencji założenia dotyczące wykorzystania technologii *blockchain* przedstawiono na przykładzie zreformowanego w 2017 r. ukraińskiego systemu katastralnego.

Wiele uwagi w trakcie obrad konferencji poświęcono realizowanym na poziomie europejskim inicjatywom na rzecz rozwoju transgranicznego obrotu nieruchomościami i integracji krajowych rejestrów nieruchomości, z wykorzystaniem technologii informatycznych. Koncepcja połączenia rejestrów w ramach europejskiego portalu E-Sprawiedliwość – jako centralnego punktu dostępu do informacji na temat wymiaru sprawiedliwości w państwach członkowskich UE i narzędzia współpracy sądowej – została przewidziana w unijnej strategii dotyczącej europejskiego systemu e-sprawiedliwości na lata 2014–2018[5]. Istotny wkład w urzeczywistnienie idei utworzenia sieci elektronicznych rejestrów nieruchomości (*Land Registers Interconnection* – LRI) stanowi projekt EULIS, zakładający umożliwienie użytkownikom z poszczególnych państw bezpośredniego dostępu drogą elektroniczną do informacji z zagranicznych rejestrów nieruchomości. Równolegle prowadzone są prace w ramach projektu „Model Interoperacyjności dla Rejestrów Nieruchomości" (*Interoperability Model for Land Registers* – IMOLA), zainicjowane przez stowarzyszenie ELRA. Podejmowane do tej pory działania mające na celu poszerzenie dostępu do krajowych rejestrów nieruchomości w skali Europy jedynie w ograniczonym zakresie przyniosły spodziewane efekty, o czym świadczy niewielka liczba państw tworzących sieć rejestrów w ramach systemu EULIS. Obrady konferencji były okazją do podsumowania dotychczasowej współpracy EULIS z Komisją Europejską oraz zaprezentowania planów dotyczących dalszej realizacji projektu LRI.

Analizowane podczas konferencji „Common Vision 2017" postępy przemian systemów informacji o nieruchomościach pod wpływem rozwoju technologicznego skłaniają do pogłębionej refleksji nad nowym kształtem rozwiązań prawnych o utrwalonej tradycji w ustawodawstwie poszczególnych państw, z uwzględnieniem z jednej strony szerokich możliwości, z drugiej strony natomiast złożonych problemów związanych z wdrażaniem interaktywnych technologii informatycznych w dziedzinie szeroko rozumianego zarządzania przestrzenią, dotyczących np. ochrony danych osobowych i prywatności.

[5] Wieloletni plan działania na lata 2014–2018 dotyczący europejskiej e-sprawiedliwości (Dz.Urz. UE C Nr 182, s. 2–13).

Elektroniczna komunikacja pomiędzy stronami a sądem w europejskim postępowaniu w sprawie drobnych roszczeń – zagadnienia prawne i uwagi praktyczne

Katarzyna Klimas[1]

Celem niniejszego opracowania jest analiza prawnych i faktycznych możliwości wprowadzenia do modelu europejskiego postępowania w sprawie drobnych roszczeń elektronicznej komunikacji stron z sądem oraz elektronicznych czynności sądowych, w tym oceny zakresu realnego wdrożenia informatycznych mechanizmów w tym postępowaniu. Rozważania w tym zakresie należy rozpocząć od weryfikacji podstaw prawnych istniejących na gruncie przepisów prawa unijnego i krajowego. Ocena doświadczeń związanych z funkcjonowaniem w polskim prawie elektronicznego postępowania upominawczego z kolei stanowi podstawę ekonomicznej analizy zasadności wprowadzania komunikacji elektronicznej w europejskim postępowaniu w sprawie drobnych roszczeń oraz wpływu zasad postępowania cywilnego na urzeczywistnienie założeń projektu e-CODEX PLUS zakładającego wdrożenie komunikacji elektronicznej w europejskim postępowaniu w sprawie drobnych roszczeń oraz europejskim postępowaniu nakazowym.

Uwagi wstępne

Zagadnienie prawnej i faktycznej możliwości wprowadzenia elektronicznej komunikacji w europejskim postępowaniu w sprawie drobnych roszczeń stanowi element szerszego zagadnienia, jakim jest stosowanie w sądownictwie i wymiarze sprawiedliwości rozwiązań informatycznych, usprawniających, a w pewnym zakresie także zastępujących pracę sędziego, referendarza sądowego czy pracowników sądów. Nie ulega wątpliwości, że postępująca cyfryzacja społeczeństwa, rozwój technologiczny, z którego wyników obywatele państw członkowskich UE korzystają każdego dnia, a także wzrastająca świadomość europejskiego społeczeństwa, wpływają pozytywnie na proces informatyzowania sądownictwa, będąc motorem oczekiwanych zmian. Istotny wpływ na przemiany i społeczne oczekiwania względem wdrażania cyfrowych udogodnień w administracji publicznej[2] ma również postępująca globalizacja, której wynikiem jest migracja znacznej grupy obywateli państw członkowskich poza teren swojej ojczyzny, a także poza obszar UE. Nie dziwi zatem fakt, że wzrasta zainteresowanie i liczba użytkowników e-administracji. Kierunek, zgodnie z którym zwiększa się zakres możliwości wykorzystania elektronicznych technik tworzenia, przesyłania, a także gromadzenia danych, jest zauważalny w nowelizacjach Kodeksu postępowania cywilnego. Podstawowym dziś narzędziem uskuteczniającym i usprawniającym proces dochodzenia ochrony prawnej przed sądem jest elektroniczne postępowanie upominawcze regulowane w art. 505^{28}–505^{39} KPC. Statystki jednoznacznie wskazują, że obywatele Polski chętnie i coraz częściej korzystają z właściwości e-sądu w Lublinie[3]. Doświadczenia związane z funkcjonowaniem elektronicznego postępowania upominawczego wskazują co prawda na istotne problemy natury praktycznej, związane ze znacznym obciążeniem e-sądu[4], niemniej za bezsporny sukces elektronicznego postępowania upominawczego należy uznać „stworzenie realnej drogi sądowej do rozpoznawania spraw, które wcześniej nie były wnoszone do sądu"[5]. Stąd też elektroniczne postępowanie upominawcze uznawane jest za wzorzec informatyzacji postępowania cywilnego[6]. Ustawą z 10.7.2015 r. o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw[7] wprowadzono zmianę art. 125 KPC poprzez nowelizację § 2^1, zgodnie z którym jeżeli przepis szczególny tak stanowi albo dokonano wyboru wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego, pisma procesowe w tej sprawie wnosi się wyłącznie za pośrednic-

[1] Doktorantka w Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej Uniwersytetu Wrocławskiego, pracownik Centrum Kompetencji i Informatyzacji Sądownictwa Sądu Apelacyjnego we Wrocławiu, badacz w projekcie eCODEX PLUS.

[2] Zob. *D. Szostek*, Opinia w sprawie rządowego projektu ustawy o zmianie ustawy – Kodeks cywilny, ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (druk sejmowy Nr 2678).

[3] Zob. raport „EPU – elektroniczne postępowanie upominawcze (e-sąd) w latach 2010 – I p. 2017", https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/.

[4] Zob. *A. Brenk*, Elektroniczne postępowanie upominawcze – kilka uwag na temat e-sądu, Krajowa Rada Sądownictwa 2014, Nr 3, s. 13; *A. Kościółek*, Sprzeciw w elektronicznym w postępowaniu upominawczym – uwagi na tle obowiązujących oraz projektowanych rozwiązań legislacyjnych, MoP 2013, Nr 13, s. 681.

[5] *Ł. Goździaszek*, Elektroniczne postępowanie upominawcze, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Teoria i praktyka, Legalis/el./ 2016.

[6] *J. Gołaczyński*, Elektroniczne biuro…, Legalis/el. 2016.

[7] Dz.U. poz. 1311 ze zm.

twem systemu teleinformatycznego. Pisma niewniesione za pośrednictwem systemu teleinformatycznego nie wywołują skutków prawnych, jakie ustawa wiąże z wniesieniem pisma do sądu, o czym sąd poucza wnoszącego pismo. Przepis ten ma stanowić podstawę wdrożenia i wykorzystywania w przyszłości tzw. Elektronicznego Biura Podawczego (RB) będącego systemem obsługującym wszystkie postępowania sądowe[8], co stanowi docelowy kierunek wieloletnich działań ustawodawcy[9].

Do czasu uruchomienia i udostępnienia EBP katalog postępowań cywilnych, które mogą być wszczynane poprzez czynności elektroniczne podmiotu inicjującego sprawę, regulowany jest przepisami proceduralnymi, które wprost nadają uprawnienie do stosowania takiej formy. W tym zakresie obok elektronicznego postępowania upominawczego wskazać można wniosek o wpis do rejestru przedsiębiorców Krajowego Rejestru Sądowego spółki tworzonej na podstawie ustawowego wzorca umowy[10] czy wniosek o wpis zastawu rejestrowego do rejestru zastawów[11]. Jak wskazuje *J. Gołaczyński*, „brak jest jednak możliwości składania pism procesowych w innych postępowaniach cywilnych[12]".

Charakterystyka europejskiego postępowania w sprawie drobnych roszczeń

Analizę obowiązujących ram prawnych, w zakresie formy komunikacji w toku europejskiego postępowania w sprawie drobnych roszczeń, należy rozpocząć od wskazania genezy i charakterystyki tego rodzaju postępowania. Podstawowym aktem prawnym statuującym byt europejskiego postępowania w sprawie drobnych roszczeń, jako jednym z dwóch europejskich postępowań transgranicznych, obok europejskiego postępowania nakazowego[13], jest rozporządzenie (WE) Nr 861/2007 Parlamentu Europejskiego i Rady z 11.7.2007 r. ustanawiającego europejskie postępowanie w sprawie drobnych roszczeń[14].

Postępowanie to stanowi alternatywę dla postępowań przewidzianych w krajowych porządkach prawnych, co oznacza, że zakres stosowania rozporządzenia 861/2007 nie obliguje powoda do obrania drogi europejskiego postępowania w sprawie drobnych roszczeń i nie ogranicza prawa do dochodzenia roszczeń na podstawie innego postępowania, w tym europejskiego postępowania nakazowego[15]. Poczynić należy jednak uwagę, że w związku z treścią art. 2 ust. 2 rozporządzenia 861/2007 zawierającego katalog spraw wyłączonych spod europejskiego postępowania w sprawie drobnych roszczeń postępowanie to nie będzie stanowiło alternatywnej drogi postępowania w każdej sprawie[16]. Przede wszystkim jednak, z uwagi na niski wolumen spraw i ograniczenie wartości przedmiotu sporu do równowartości 5000 euro[17], europejskie postępowanie w sprawie drobnych roszczeń będzie stanowić konkurencyjną drogę dla postępowania uproszczonego (art. 505^1 i n. KPC), jeśli w rozpatrywanej sprawie cywilnej zaistnieje tzw. element transgraniczny[18]. Zgodnie z art. 3 rozporządzenia 861/2007 przez sprawę transgraniczną rozumie się sprawę, w której przynajmniej jedna ze stron ma miejsce zamieszkania lub miejsce zwykłego pobytu w państwie członkowskim innym niż państwo członkowskie sądu lub trybunału rozpatrującego sprawę.

W kontekście rozpatrywania podstaw prawnych i faktycznych dla stosowania elektronicznej komunikacji w europejskim postępowaniu w sprawie drobnych roszczeń podnieść należy, że utrudnione jest dochodzenie roszczeń w sprawach o charakterze transgranicznym w elektronicznym postępowaniu upominawczym z uwagi na elektronicznym postępowaniu upominawczym z uwagi na wymóg wskazania numeru PESEL, zarówno powoda, jak i pozwanego. Równocześnie obowiązujące przepisy regulujące kształt i zasady funkcjonowania EBP nie zapewniają ram prawnych tworzących realną możliwość skorzystania z elektronicznej drogi inicjowania postępowania przez obywateli innych państw członkowskich. W obu wypadkach podstawę stanowi rozporządzenie Ministra Sprawiedliwości z 26.4.2016 r. w sprawie trybu zakładania i udostępniania konta w systemie teleinformatycznym obsługującym postępowanie sądowe[19], zgodnie z którym identyfikacja w systemie opiera się na numerze PESEL, który posiadają obywatele Polski, a także pewien niewielki odsetek obywateli innych państw członkowskich. Powyższa uwaga czyni tematykę niniejszego artykułu szczególnie uzasadnioną oraz aktualną.

---

[8] *A. Zalesińska*, Wpływ informatyzacji na założenia konstrukcyjne procesu cywilnego, Legalis/el. 2016.

[9] Zob. *J. Gołaczyński*, Model informatyzacji postępowania cywilnego w nowym Kodeksie postępowania cywilnego, [w:] *K. Markiewicz*, *A. Torbus* (red.), Postępowanie rozpoznawcze w przyszłym kodeksie postępowania cywilnego, Legalis/el. 2014.

[10] Zob. art. 23^1, 106^1 i 157^1 KSH.

[11] Art. 39 ust. 2a ustawy z 6.12.1996 r. o zastawie rejestrowym i rejestrze zastawów (t.j. Dz. U. z 2017 r. poz. 1278 ze zm.)

[12] *J. Gołaczyński*, Elektroniczne biuro…, Legalis/el. 2016.

[13] Rozporządzenie (WE) Nr 1896/2006 Parlamentu Europejskiego i Rady z 12.12.2006 r. ustanawiające postępowanie w sprawie europejskiego nakazu zapłaty (Dz.Urz. UE L Nr 399, s. 1 ze zm.) oraz art. 505^{15}–505^{20} KPC.

[14] Dz.Urz. UE L Nr 199, s. 1 ze zm.; dalej: rozporządzenie 861/2007.

[15] Oczywiście pod warunkiem podstaw do wszczęcia takiego postępowania.

[16] W zakresie obszernej tematyki zakresu zastosowania rozporządzenia 861/2007 odsyłam do literatury: *A. Harast-Sidowska*, Europejskie postępowanie nakazowe i w sprawie drobnych roszczeń. Komentarz praktyczny. Wzory pism procesowych, Legalis/el. 2015; *K. Weitz*, [w:] *K. Weitz*, *P. Grzegorczyk* (red.), Europejskie prawo procesowe cywilne i kolizyjne, Warszawa 2012, s. 489; *J. Pisuliński*, Europejski nakaz zapłaty, Europejski Przegląd Sądowy 2008, Nr 1, s. 6; *A. Włosińska*, Odmowa uznania zagranicznego orzeczenia sądowego w świetle postanowień Konwencji Lugańskiej, Kraków 2002, s. 141.

[17] Art. 2 ust. 1 rozporządzenia 861/2007.

[18] *K. Flaga-Gieruszyńska*, komentarz do art. 505^{21}, [w:] *K. Flaga-Gieruszyńska*, *A. Zieliński* (red.), Kodeks postępowania cywilnego. Komentarz, Legalis/el. 2017.

[19] Dz.U. poz. 637.

Cechą charakterystyczną europejskiego postępowania w sprawie drobnych roszczeń jest jego sformalizowanie i standaryzacja, które służyć mają uproszczeniu i przyspieszeniu postępowania[20]. Sam ustawodawca europejski w treści motywów rozporządzenia 861/2007 wskazuje na podstawowy cel wprowadzenia europejskiego postępowania w sprawie drobnych roszczeń, stanowiąc, że: „Europejskie postępowanie w sprawie drobnych roszczeń powinno uprościć oraz przyspieszyć przebieg postępowań spornych dotyczących drobnych roszczeń w sprawach transgranicznych, a także zmniejszyć koszty, poprzez udostępnienie fakultatywnego narzędzia uzupełniającego istniejące możliwości przewidziane w prawie poszczególnych państw członkowskich, które to prawo pozostanie nienaruszone. Niniejsze rozporządzenie powinno również ułatwić uznawanie i wykonywanie orzeczenia wydawanego w innym państwie członkowskim w ramach europejskiego postępowania w sprawie drobnych roszczeń".

Realizacja zasady standaryzacji postępowania jest urzeczywistniona wprowadzeniem wymogu wnoszenia pism procesowych oraz pism obejmujących czynności sądowe na formularzach urzędowych stanowiących załączniki do rozporządzenia 861/2007. W przeciwieństwie do unijnych przepisów regulujących europejskie postępowanie nakazowe w rozporządzeniu 861/2007 pominięta została kwestia regulacji szczegółowych elementów pozwu, którego obligatoryjne części[21] wynikają bezpośrednio z zakresu formularza A. Formularz pozwu zawiera wymóg opisu dowodów uzasadniających powództwo, a w stosownych przypadkach wymaga także dołączenia do pozwu wszelkich odpowiednich dokumentów. Powyższe wynika bezpośrednio z treści art. 4 ust. 1 rozporządzenia 861/2007[22], a także z motywu 12 stanowiącego, że do formularza pozwu należy dołączyć w odpowiednich przypadkach wszelkie odpowiednie dokumenty uzupełniające. W doktrynie podkreśla się jednakże, w kontekście postulatu dążenia do obniżenia kosztów postępowania, że wprowadzone przez ustawodawcę unijnego postanowienia nie przesądzają ostatecznie o konieczności dołączania do pozwu dowodów w postaci dokumentów, a co do zasady, poprzestać należy na ich opisaniu[23]. Przy wnioskach dowodowych warto zaznaczyć, że w europejskim postępowaniu w sprawie drobnych roszczeń nie obowiązuje system prekluzji dowodowej, co oznacza, że powód ma możliwość przedstawienia w toku trwającego postępowania także dowodów niewskazanych przez niego w treści pozwu. Stanowi o tym treść motywu 12, w którym postanowiono, że w odpowiednich przypadkach powód ma uprawnienie do złożenia w trakcie postępowania dalszych dowodów. Strony w europejskim postępowaniu w sprawie drobnych roszczeń mają zatem prawo zgłaszać nowe dowody aż do zamknięcia rozprawy[24].

Po wniesieniu pozwu oraz jego pozytywnym badaniu[25] pod względem spełnienia wymogów formalnych, dostateczności przedstawionych przez powoda informacji, należytego wypełnienia formularza A, a także braku podstaw do stwierdzenia, że powództwo jest oczywiście bezzasadne lub niedopuszczalne, sąd doręcza pozwanemu formularz pozwu wraz z załącznikami, a także częściowo wypełnionym przez sąd formularzem C (formularz odpowiedzi na pozew). Pozwany, w terminie 30 dni od dnia doręczenia mu formularza pozwu, składa odpowiedź na pozew, wypełniając część II formularza odpowiedzi C, załączając w odpowiednich przypadkach wszelkie odpowiednie dokumenty uzupełniające i odsyłając je do sądu lub trybunału, zgodnie z zastrzeżeniem art. 5 ust. 3 rozporządzenia 861/2007, pozwany może udzielić odpowiedzi w inny odpowiedni sposób bez wykorzystania formularza odpowiedzi. Oczywiste przy tym pozostaje jednak, że odpowiedź udzielana przez pozwanego z pominięciem wykorzystania odpowiedniego formularza zawierać powinna wszelkie niezbędne składniki: oznaczenie sądu, stron postępowania roszczenia, sygnatury sprawy, okoliczności będące stanowiskiem wobec roszczenia, dowody służące zakwestionowaniu powództwa, podpis, a ewentualnie także wniosek o przeprowadzenie rozprawy, wniosek o zwrot kosztów czy też powództwo wzajemne[26].

Powództwo wzajemne może, ale nie musi, zostać wniesione jednocześnie z odpowiedzią na pozew powoda. Zasadniczo przepisy rozporządzenia 861/2007 nie wskazują terminu do wniesienia powództwa wzajemnego, stąd też aktualne zdaje się pytanie o możliwość zastosowania w tym zakresie art. 2014 § 1 KPC, stanowiącego o tym, że powództwo wzajemne jest dopuszczalne, jeżeli roszczenie wzajemne jest w związku z roszczeniem powoda lub nadaje się do potrącenia, przy czym powództwo wzajemne można wytoczyć bądź w odpowiedzi na pozew, bądź oddzielnie, nie później jednak niż na pierwszej rozprawie, albo w sprzeciwie od wyroku zaocznego. Jak wskazuje *A. Harast-Sidowska*, „w sytuacji, gdy pozwany złożył odpowiedź na pozew (niezależnie od

[20] Zob. *A. Laskowska*, Europejskie postępowanie w sprawie drobnych roszczeń, PPE 2010, Nr 5, s. 11; *S. Cieślik*, Formalizm postępowania cywilnego, Warszawa 2008, s. 213. Zob. też uchwały SN: z 30.5.2001 r., III CZP 19/01, Legalis; z 17.1.2002 r., III CZP 78/01, Legalis.

[21] Obligatoryjnymi elementami pozwu są: dane dotyczące sądu, stron postępowania i ich przedstawicieli, określenie jurysdykcji krajowej, uzasadnienie transgranicznego charakteru postępowania, określenie dochodzonego roszczenia, wskazanie podstaw faktycznych uzasadniających roszczenie, oznaczanie informacji, czy powód zwraca się do sądu o wydanie zaświadczenia dotyczącego orzeczenia, wybór sposobu komunikacji z sądem.

[22] Formularz pozwu zawiera opis dowodów uzasadniających powództwo, a w stosownych przypadkach dołącza się do niego wszelkie odpowiednie dokumenty uzupełniające.

[23] *A. Harast-Sidowska*, Europejskie postępowanie…, Legalis/el. 2015.

[24] Por. art. 217 § 1 KPC – strona może aż do zamknięcia rozprawy przytaczać okoliczności faktyczne i dowody na uzasadnienie swoich wniosków lub dla odparcia wniosków i twierdzeń strony przeciwnej.

[25] Lub też po uzupełnieniu braków w trybie określonych w art. 4 ust. 4 rozporządzenia 861/2007.

[26] *Ł. Goździaszek*, Europejskie postępowanie w sprawie drobnych roszczeń, [w:] *E. Marszałkowska-Krześ* (red.), Postępowanie cywilne, Warszawa 2017, s. 475.

formy) bez wskazania, czy zamierza wnieść pozew wzajemny albo nie dołączył odpowiedniego formularza, pozwany traci prawo jego wniesienia. Jeżeli natomiast pozwany nie wniósł odpowiedzi na pozew i wobec niego zapadł wyrok zaoczny, to powinien mieć możliwość wniesienia powództwa wzajemnego w sprzeciwie od wyroku zaocznego"[27]. Taka wykładnia, wobec okoliczności, że przeprowadzenie rozprawy stanowi wyjątek w europejskim postępowaniu w sprawie drobnych roszczeń, wydaje się najpełniej realizować praktyczne i funkcjonalne założenia tego rodzaju postępowania. W sytuacji skutecznego[28] wniesienia powództwa wzajemnego powód ma 30 dni od momentu doręczenia na udzielenie odpowiedzi (art. 5 ust. 6 rozporządzenia 861/2007).

W myśl art. 5 ust. 1 rozporządzenia 861/2007 europejskie postępowanie w sprawie drobnych roszczeń jest postępowaniem pisemnym, czego naturalną konsekwencją jest zasada, że sąd orzeka w sprawie rozpoznawanej w europejskim postępowaniu w sprawie drobnych roszczeń na posiedzeniu niejawnym[29]. Jednocześnie w ust. 2 wskazanego przepisu, zasada pisemności ulega ograniczeniu stosownie do regulacji, zgodnie z którą „sąd lub trybunał przeprowadza rozprawę tylko wtedy, jeżeli uzna, że wydanie orzeczenia nie jest możliwe na podstawie pisemnych dowodów lub jeżeli wnosi o to strona. Sąd lub trybunał może oddalić taki wniosek, jeżeli uzna, że w okolicznościach danej sprawy rozprawa nie jest konieczna do rzetelnego przeprowadzenia postępowania". Podczas ustalania przez sąd, czy zachodzą podstawy do przeprowadzenia rozprawy niezbędne jest dokonanie oceny całości okoliczności oraz zgłoszonych wniosków dowodowych, a także, jak podnosi się w literaturze, kierowania się przez sąd dyrektywną dążenia do zmniejszenia kosztów postępowania[30]. Sąd nie jest również związany wnioskiem strony, który może zostać oddalony niezaskarżalnym postanowieniem[31].

Zasada pisemności ulega również wzmocnieniu w związku z dopuszczeniem możliwości przesłuchania świadków oraz stron postępowania na piśmie, zgodnie z treścią art. 525^{25} § 1–2 KPC, stanowiących, że świadek składa zeznanie na piśmie, jeżeli sąd tak postanowi. W takim przypadku świadek składa przyrzeczenie przez podpisanie tekstu przyrzeczenia. Przesłuchanie strony następuje na piśmie, jeżeli sąd tak postanowi. Przepisy polskiej ustawy proceduralnej stanowią rozszerzenie i uzupełnienie postanowień zawartych przez prawodawcę europejskiego w art. 9 ust. 2 rozporządzenia 861/2007, w którym postanowił, że sąd może dopuścić przeprowadzenie dowodu z pisemnych zeznań świadków, biegłych lub stron. Dążąc do realizacji założeń i celów europejskiego postępowania w sprawie drobnych roszczeń jako postępowania szybkiego oraz efektywnego, ustawodawca unijny zastrzegł w ust. 4 art. 9 rozporządzenia 861/2007, że sąd może przeprowadzić dowód z opinii biegłych lub z zeznań ustnych tylko wówczas, gdy wydanie orzeczenia nie jest możliwe na podstawie innych dowodów. Tym samym urzeczywistnieniu uległa dyrektywa wyrażona w ust. 1 wskazanego artykułu, zgodnie z którą sąd wybiera najprostsze i najmniej obciążające sposoby przeprowadzenia dowodu. W kontekście uwag i analizy poczynionych w ramach niniejszego opracowania należy jednak podkreślić, że realizując podstawowe założenia rozporządzenia 861/2007, tj. dążenie do przyspieszenia, uproszczenia i minimalizacji kosztów przeprowadzenia postępowania w transgranicznych postępowaniach cywilnych, ustawodawca nie wyeliminował możliwości przeprowadzania postępowania dowodowego, które najpełniej wyraża zasadę kontradyktoryjności odgrywającą istotną rolę w europejskim postępowaniu w sprawie drobnych roszczeń[32]. W tym zakresie europejskie postępowanie w sprawie drobnych roszczeń konstrukcyjnie różni się od drugiego z europejskich postępowań transgranicznych – europejskiego postępowania nakazowego[33].

Docelowo europejskie postępowanie w sprawie drobnych roszczeń kończy się wydaniem przez sąd wyroku. Ustrukturyzowana i sformalizowana procedura rozpoznawania spraw w tym rodzaju europejskiego postępowania transgranicznego nakazuje sądowi wydanie orzeczenia w terminie 30 dni od dnia zamknięcia rozprawy albo od otrzymania wszystkich informacji niezbędnych do wydania orzeczenia (art. 7 ust. 2 rozporządzenia 861/2007)[34].

Podstawy prawne dla elektronicznej komunikacji pomiędzy stronami a sądem w europejskim postępowaniu w sprawie drobnych roszczeń

Elektroniczna dwustronna komunikacja w europejskim postępowaniu w sprawie drobnych roszczeń znajduje podstawy w rozporządzeniu 861/2007. W pierwszej kolejności dla tzw. elektronicznych pism procesowych[35] znaczenie ma

[27] *A. Harast-Sidowska*, Europejskie postępowanie…, Legalis/el. 2015.

[28] Zob. art. 5 ust. 7 rozporządzenia 861/2007.

[29] Stanowi to wyjątek od zasady określonej w art. 148 § 1 KPC – tak: *R. Kulski*, komentarz do art. 505^{23} KPC, [w:] *A. Marciniak* (red.), Kodeks postępowania cywilnego. Tom IV. Komentarz do art. 1096–1217, Warszawa 2016, s. 743.

[30] *A. Harast-Sidowska*, Europejskie postępowanie…, Legalis/el. 2015.

[31] Kwestionowanie odmowy przeprowadzenia rozprawy przez stronę może odbywać się w ramach wniesionej apelacji – tak m.in.: *M. Manowska*, Postępowania odrębne w procesie cywilnym. Warszawa 2010, s. 397.

[32] *A. Harast-Sidowska*, Europejskie postępowanie…, Legalis/el. 2015.

[33] *Ibidem*, s. 31.

[34] W zakresie analizy podstaw dla wydania orzeczenia w europejskim postępowaniu w sprawie drobnych roszczeń zob. m.in.: *A. Arkuszewska*, Zaskarżanie orzeczeń i zarządzeń wydanych w europjeskim postępowaniu w sprawie drobnych roszczeń, EPS 2011, Nr 8, s. 16; *K. Weitz*, [w:] *T. Ereciński*, *J. Gudowski*, *M. Jędrzejewska*, *K. Weitz*, Kodeks postępowania cywilnego Komentarz, Część pierwsza. Postępowanie rozpoznawcze, t. 1, Warszawa 2009, s. 860.

[35] *A. Zalesińska*, Wpływ informatyzacji…, Legalis/el. 2016.

art. 4 ust. 1 rozporządzenia 861/2007, zgodnie z którym powód wszczyna europejskie postępowanie w sprawie drobnych roszczeń, wypełniając formularz pozwu A zawarty w załączniku A i składając go we właściwym sądzie lub trybunale bezpośrednio, za pośrednictwem poczty lub innych środków komunikacji, takich jak faks lub poczta elektroniczna, akceptowanych przez państwo członkowskie, w którym wszczyna postępowanie. Jednocześnie w art. 13 ust. 1 rozporządzenia 861/2007 prawodawca europejski postanowił, że orzeczenia oraz inne dokumenty wydawane przez sąd doręczane będą stronom drogą pocztową lub drogą elektroniczną, w przypadku gdy takie środki są technicznie dostępne i dopuszczalne zgodnie z przepisami procesowymi państwa członkowskiego, w którym prowadzone jest europejskie postępowanie w sprawie drobnych roszczeń, a jeżeli strona, której mają zostać doręczone dokumenty, ma miejsce zamieszkania lub miejsce zwykłego pobytu w innym państwie członkowskim – w przypadku gdy takie środki techniczne są zgodne z przepisami procesowymi tego państwa członkowskiego oraz w przypadku gdy strona, której mają zostać doręczone dokumenty, udzieliła wcześniej wyraźnej zgody na doręczanie jej dokumentów drogą elektroniczną lub w przypadku gdy zgodnie z przepisami procesowymi państwa członkowskiego, w którym strona ta ma miejsce zamieszkania lub miejsce zwykłego pobytu, strona ta ma prawny obowiązek zaakceptowania tej szczególnej metody doręczenia.

W ustawodawstwie europejskim istnieją zatem ramy prawne dla wdrożenia informatycznych rozwiązań w zakresie wnoszenia i doręczania elektronicznych pism procesowych oraz elektronicznych czynności sądowych[36] w europejskim postępowaniu w sprawie drobnych roszczeń. Zaznaczyć jednakże należy, że przepisy prawa unijnego dopuszczające elektroniczną komunikację uzależniają możliwość stosowania elektronicznych pism procesowych, elektronicznych doręczeń oraz innych elektronicznych czynności sądowych, od dostępności i dopuszczalności odpowiednich środków technicznych przez prawo krajowe danego państwa członkowskiego[37].

Polski prawodawca nie przewidział możliwości stosowania technologicznych rozwiązań w zakresie komunikacji pomiędzy sądem a stronami w krajowych przepisach regulujących europejskie postępowania transgraniczne, opierając się jednakże w tym zakresie na przepisach ogólnych. W tym zakresie prawo wyboru sposobu wnoszenia pism procesowych oraz doręczenia w europejskim postępowaniu w sprawie drobnych roszczeń wynika z art. 125 § 21 KPC, zgodnie z którym jeżeli przepis szczególny tak stanowi albo dokonano wyboru wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego, pisma procesowe w tej sprawie wnosi się wyłącznie za pośrednictwem systemu teleinformatycznego. Pisma niewniesione za pośrednictwem systemu teleinformatycznego nie wywołują skutków prawnych, jakie ustawa wiąże z wniesieniem pisma do sądu, o czym sąd poucza wnoszącego pismo.

Z kolei dla elektronicznego doręczenia pism sądowych ustawodawca postanowił w art. 131^1 § 1 KP, że sąd dokonuje doręczeń za pośrednictwem systemu teleinformatycznego (doręczenie elektroniczne), jeżeli adresat wniósł pismo za pośrednictwem systemu teleinformatycznego albo dokonał wyboru wnoszenia pism za pośrednictwem systemu teleinformatycznego. W przypadku doręczenia elektronicznego pismo uznaje się za doręczone w chwili wskazanej w elektronicznym potwierdzeniu odbioru korespondencji. W przypadku braku takiego potwierdzenia doręczenie elektroniczne uznaje się za skuteczne po upływie 14 dni od daty umieszczenia pisma w systemie teleinformatycznym. W świetle powyżej przedstawionych regulacji prawnych podkreślić jednak należy, że przepisy krajowe wskazują precyzyjnie środek komunikacji elektronicznej, który jest dopuszczalny w polskim systemie prawnym – system teleinformatyczny. Artykuł 125 § 2 KPC w brzmieniu nadanym mu ustawą z 24.5.2000 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy o zastawie rejestrowym i rejestrze zastawów, ustawy o kosztach sądowych w sprawach cywilnych oraz ustawy o komornikach sądowych i egzekucji[38] stanowił, że jeżeli przepis szczególny tak stanowi, pisma procesowe wnosi się na urzędowych formularzach lub na elektronicznych nośnikach informatycznych. Przepis ten jednakże nie miał nigdy praktycznego zastosowania i – jak wskazuje *A. Zalesińska* – przekazywanie danych przy wykorzystaniu informatycznych nośników danych wywołałoby skutek odwrotny do zamierzonego, czyli zamiast uprościć postępowanie, prowadziłoby do konieczności dokonywania wielu dodatkowych czynności[39].

Zostały zatem, zarówno na poziomie unijnym, jak i krajowym, wypracowane ramy prawne dla wykorzystania systemu teleinformatycznego przy wnoszeniu pism procesowych, a także do celu realizacji elektronicznych doręczeń w europejskim postępowaniu w sprawie drobnych roszczeń.

[36] *S. Cieślik*, Elektroniczne czynności sądowe – perspektywy rozwoju, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), Informatyzacja postępowania cywilnego. Teoria i praktyka, Legalis/el. 2016.

[37] Zgodnie z art. 13 ust. 2 rozporządzenia 861/2007 cała niewymieniona w ust. 1 komunikacja pisemna między sądem lub trybunałem a stronami lub innymi osobami biorącymi udział w postępowaniu odbywa się z wykorzystaniem środków elektronicznych, za potwierdzeniem odbioru, jeżeli takie środki są technicznie dostępne i dopuszczalne zgodnie z przepisami procesowymi państwa członkowskiego, w którym prowadzone jest europejskie postępowanie w sprawie drobnych roszczeń, pod warunkiem że strona lub osoba wyraziła wcześniej zgodę na takie środki komunikowania się lub, zgodnie z przepisami procesowymi państwa członkowskiego, w którym strona ta lub osoba ma miejsce zamieszkania lub miejsce zwykłego pobytu, ma ona obowiązek zaakceptowania takich środków komunikowania się. Z kolei w art. 4 ust. 2 rozporządzenia 861/2007 ustawodawca unijny postanowił, że państwa członkowskie powiadamiają Komisję o środkach komunikowania, które mogą zaakceptować, a Komisja podaje te informacje do wiadomości publicznej.

[38] Dz.U. Nr 48, poz. 554 ze zm.

[39] *A. Zalesińska*, Wpływ informatyzacji…, Legalis/el. 2016.

Praktyczne aspekty wdrażania elektronicznej komunikacji w europejskim postępowaniu w sprawie drobnych roszczeń

Utworzenie prawnych ram do korzystania przez strony oraz sądy rozpoznające sprawy w europejskim postępowaniu w sprawie drobnych roszczeń z komunikacji elektronicznej, zarówno na poziomie krajowym, jak i europejskim, nie przesądza jednak o faktycznym i ekonomicznym uzasadnieniu do wdrożenia odpowiedniego systemu teleinformatycznego. Samo bowiem wytworzenie podstawy prawnej dla elektronicznej formy pism procesowych oraz czynności sądowych, bez odpowiednich przepisów wykonawczych oraz faktycznej infrastruktury technicznej, czyni uprawnienia stron do elektronicznej komunikacji z sądem nierealnymi do wykorzystania. Uwaga ta pozostaje szczególnie aktualna wobec formalnego ograniczenia w korzystaniu przez osoby nieposiadające numeru PESEL z krajowych systemów teleinformatycznych, o czym wyżej była już mowa.

Wśród zalet stosowania informatycznych rozwiązań w wymiarze sprawiedliwości, do których niewątpliwe należy niski koszt, szybkość oraz prostota w porównaniu do tradycyjnych metod doręczania pism, należy na względzie mieć zasady postępowania cywilnego oraz jego funkcje. Modelowym rozwiązaniem pozostaje w tym zakresie elektroniczne postępowanie upominawcze, które stanowiło milowy krok dla informatyzacji postępowań sądowych. Najistotniejszą cechą elektronicznego postępowania upominawczego jest bowiem wprowadzenie wyłącznej formy elektronicznej dla dokonywania czynności postępowania zarówno dla sądu, jak i powoda, a w pewnym ograniczonym zakresie także pozwanego. Elektroniczne postępowanie upominawcze stanowi jednakże rodzaj postępowania, w którym udział strony pozwanej aktualizuje się dopiero w momencie doręczenia pozwanemu wydanego nakazu zapłaty. W tym zakresie elektroniczne postępowanie upominawcze zbliżone jest do zwykłego postępowania upominawczego, postępowania nakazowego, a także – europejskiego postępowania nakazowego[40]. Postępowania te wykluczają możliwość przeprowadzenia rozprawy, a rozpoznanie sprawy następuje na posiedzeniu niejawnym w składzie jednoosobowym[41]. Pozwany nie bierze zatem udziału w postępowaniu do momentu doręczenia mu nakazu wraz z odpisem pozwu, co stanowi wyjątek od zasady jawności postępowania cywilnego[42]. Pozwany nie może też zapobiec wyznaczeniu sprawy, a jego obrona polega na wniesieniu odpowiednio zarzutów lub sprzeciwu od wydanego już nakazu zapłaty.

Taka konstrukcja postępowania umożliwia w elektronicznym postępowaniu upominawczym przeprowadzenie postępowania w całości elektronicznie[43]. Do momentu wydania nakazu zapłaty bowiem komunikacja odbywa się wyłącznie pomiędzy sądem a stroną inicjującą postępowanie, która korzystając z elektronicznego postępowania upominawczego, jednocześnie wyraziła zgodę i wolę posługiwania się do celu tej komunikacji dedykowanym systemem teleinformatycznym. Pierwszą z czynności podejmowanych przez pozwanego jest natomiast sprzeciw, który stosownie do art. 505^{31} § 2 KPC może zostać wniesiony, albo w formie pisemnej zwykłej albo w formie elektronicznej za pośrednictwem systemu teleinformatycznego.

Rola pozwanego jako strony sporu aktualizuje się znacznie wcześniej, jako że bezpośrednio po wniesieniu pozwu sąd ma obowiązek doręczyć pismo pozwanemu, na które pozwany udziela w terminie 30 dni odpowiedzi. Pozwany może również skierować przeciwko powodowi powództwo wzajemne. Dopuszczalne, choć w charakterze wyjątku, jest również przeprowadzenie rozprawy. Nawet przy założeniu dostępności w europejskim postępowaniu w sprawie drobnych roszczeń przeprowadzenia rozprawy na odległość[44] nie sposób uznać, żeby model postępowania ukształtowany przez prawodawcę europejskiego w rozporządzeniu 861/2007 był zbieżny z założeniami elektronicznego postępowania upominawczego. Przeprowadzenie rozprawy w formie wideokonferencji (tzw. rozprawa odmiejscowiona) zostało dopuszczone na podstawie art. 151 § 2 KPC, jednakże z uwagi na brak praktycznego doświadczenia w wykorzystaniu tego modelu posiedzenia sądowego, a także przy konieczności zapewnienia technicznej infrastruktury w sądzie innego państwa członkowskiego wskazana możliwość nie wydaje się realnym udogodnieniem. U podstaw europejskiego postępowania w sprawie drobnych roszczeń leży zapewnienie pełnej kontradyktoryjności postępowania od momentu zainicjowania postępowania do jego ostatecznego zakończenia oraz przyznanie zbieżnych uprawnień i ekwiwalentnego poziomu aktywności obu stron postępowania. Biorąc pod uwagę również transgraniczny charakter postępowania, w którym udział biorą obywatele różnych państw członkowskich, o różnym poziomie informatyzacji wymiaru sprawiedliwości, dostępności e-usług w administracji publicznej, a przede wszystkim świadomości obywateli, zadanie skutecznego wdrożenia systemu teleinforma-

[40] Zob. *A. Kościółek*, *A. Banaszewska*, Automatyzacja czynności orzekania w europejskim postępowaniu nakazowym, [w:] *B. Śliwczyński*, *L. Łuczak-Noworolnik*, e-Wymiar sprawiedliwości w aspekcie europejskim, Poznań 2016, s. 37–52.

[41] Art. 484^{1} § 1, art. 497^{1} oraz 505^{28} KPC w zw. z art. art. 497^{1} KPC.

[42] *A. Guzińska*, komentarz do art. 484^{1} KPC, [w:] *E. Marszałkowska-Krześ* (red.), Kodeks postępowania cywilnego. Komentarz, Legalis/el. 2017.

[43] Przy czym w razie braku podstaw do wydania nakazu zapłaty postępowanie zostanie zakończone przekazaniem sprawy do właściwości sądu właściwości ogólnej (art. 505^{23} oraz 499 w zw. z art. 505^{28} KPC).

[44] Szerzej: *A. Kościółek*, *A. Zalesińska*, Informatyzacja europejskich postępowań transgranicznych a polskie regulacje procesowe, [w:] *M. Kraska*, *Sz. Mamrot* (red.), Cyfrowe usługi publiczne, Poznań 2017, s. 30–31.

tycznego służącego obsłudze europejskiego postępowania w sprawie drobnych roszczeń stanowi obecnie wyzwanie nieuzasadnione ekonomicznie i praktycznie.

Pomimo istotnych ograniczeń i przeszkód, które w perspektywie dalszego rozwoju europejskiej informatyzacji sądownictwa z pewnością będą minimalizowane lub eliminowane, należy uwzględnić aktualne możliwości usprawnienia przebiegu europejskiego postępowania w sprawie drobnych roszczeń. Postępowanie to, jako jedno z dwóch europejskich postępowań transgranicznych, objęte jest zakresem projektu e-CODEX PLUS[45], którego docelowym założeniem jest stworzenie technicznej i prawnej możliwości wnoszenia oraz odbierania pism w europejskich postępowaniach transgranicznych za pomocą krajowych systemów teleinformatycznych połączonych z portalem eJustice (https://e-justice.europa.eu/home.do?action=home&plang=pl). W związku z okolicznością, że w niedługim czasie w pewnej grupie państw członkowskich zostanie wdrożona możliwość wprowadzania pozwów w europejskim postępowaniu w sprawie drobnych roszczeń w formie elektronicznej, rozważyć należy co najmniej zasadność stworzenia infrastruktury pozwalającej polskim sądom powszechnym, które na mocy przepisów regulujących to postępowanie są sądami właściwymi dla rozpoznania sprawy, odbioru elektronicznego powództwa wniesionego przez obywatela innego państwa członkowskiego.

Podsumowanie

Szczegółowa analiza obowiązujących przepisów unijnych oraz krajowych regulujących europejskie postępowanie w sprawie drobnych roszczeń, jak również dopuszczalność stosowania tzw. elektronicznych pism procesowych oraz dokonywania elektronicznych czynności sądowych, w tym w szczególności elektronicznych doręczeń, w sposób jednoznaczny ujawniła istotne rozbieżności pomiędzy europejskim postępowaniem w sprawie drobnych roszczeń a przyjmowanym za model w zakresie informatycznych rozwiązań – elektronicznym postępowaniem upominawczym. Rozbieżności wskazują nie tyle na niemożliwość cyfryzacji europejskiego postępowania w sprawie drobnych roszczeń, ile uzasadniają rozważenie zakresu tej cyfryzacji w kontekście względów natury praktycznej i ekonomicznej.

Stąd też wnioski przedmiotowego opracowania sprowadzają do uznania, że o ile istniejące ramy prawne stwarzają możliwość wprowadzenia dwustronnej komunikacji elektronicznej w europejskim postępowaniu w sprawie drobnych roszczeń, o tyle realny poziom informatyzacji, interoperacyjności i integralności technicznych rozwiązań wykorzystywanych przez państwa członkowskie UE w sądownictwie, a także różnice w świadomości i zaufaniu obywateli do informatycznych mechanizmów wykorzystywanych w wymiarze sprawiedliwości, nie czynią możliwym wdrożenia obecnie pełnej komunikacji elektronicznej pomiędzy sądem a stronami w toku trwania całego postępowania.

Nie oznacza to jednak, że należy ignorować fakt postępującego rozwoju technologicznego i dążenia Europy do wypracowania komplementarnych rozwiązań w zakresie europejskich postępowaniach transgranicznych. Wręcz przeciwnie, w związku z brakiem technicznych i prawnych przeciwwskazań do umożliwienia powodowi elektronicznego wniesienia powództwa należy podjąć starania, aby na obecnym etapie realizacji wspólnego kierunku wyznaczonego przez państwa członkowskie umożliwić polskim sądom powszechnym właściwym dla rozpoznania spraw w europejskim postępowaniu w sprawie drobnych roszczeń odbiór pozwu wniesionego drogą elektroniczną przez obywateli innych państw członkowskich. Jak wskazuje *S. Cieślik*, doświadczenia informatyzacji wymiaru sprawiedliwości pokazują, że w pierwszej kolejności podejmowana jest próba wprowadzenia elektronicznej formy dla pism inicjujących postępowanie[46]. Sukces i efektywność elektronicznej komunikacji w tym zakresie będzie stanowić w przyszłości fundament stopniowego rozszerzania zakresu informatyzacji europejskiego postępowania w sprawie drobnych roszczeń.

Praca naukowa finansowana ze środków finansowych na naukę w latach 2018-2019 przyznanych na realizację projektu międzynarodowego współfinansowanego.

[45] *Sz. Mamrot*, Elektronizacja postępowań sądowych. Doświadczenia z realizacji projektów e-CODEX oraz e-Sens, [w:] *B. Śliwczyński*, *L. Łuczak-Noworolnik*, e-Wymiar sprawiedliwości w aspekcie europejskim, Poznań 2016, s. 163–174.

[46] *S. Cieślik*, Formalizm…, s. 227.

Słowa kluczowe: europejskie postępowanie w sprawie drobnych roszczeń, elektroniczny nakaz zapłaty, elektroniczna komunikacja, elektroniczne czynności sądowe

Electronic communication between the parties and the court in the European Small Claims Procedure – legal issues and practical remarks

The aim of this study is to analyze the legal and factual possibilities of implementing to the European model of small claims procedure electronic communication of parties with the court and electronic court activities, including the assessment of the scope of implementation of IT automatization, in European Small Claims procedure. Consideration in this respect begins with the verification of the legal basis laying under the provisions of EU and national law. Assessment of experiences related to the functioning of the Polish electronic writ-of-payment proceedings (EPU) provides the basis for an economic analysis of implementing electronic communication in the European Small Claims procedure and the impact of civil procedural rules on the implementation of the e-CODEX PLUS project assuming electronic communication in the European Small Claims Procedure and European Payment Order.

Keywords: European Small Claims Procedure, electronic payment order, electronic communication, electronic court activities.

E-wymiar sprawiedliwości w aspekcie europejskim na przykładzie projektu e-CODEX

r.pr. *Lucyna Łuczak-Noworolnik*[1]

Celem niniejszego opracowania jest przedstawienie projektów wielkoskalowych z grupy *Large Scale Pilots*, które mają upowszechnić wykorzystywanie środków komunikacji elektronicznej w sprawach transgranicznych. Rezultaty projektów z założenia mają usprawnić przedłużające się postępowania sądowe, zniwelować problemy z doręczeniami pocztowymi oraz wyeliminować konieczność osobistego stawiennictwa w sądach. Tym samym analizowane projekty jawią się jako inicjatywy spełniające fundamentalną rolę w budowaniu europejskiego społeczeństwa informacyjnego.

Uwagi wstępne

Bez wątpienia elektronizacja wymiaru sprawiedliwości na przestrzeni ostatnich kilku lat jest jednym z prężniej rozwijających się obszarów. Obok e-administracji oraz e-zdrowia staje się coraz częściej przedmiotem zainteresowania ze strony organów UE, które starają się upowszechnić korzystanie z nowoczesnych środków komunikacji elektronicznej, także w sferze publicznej[2]. Realizacja tak zakreślonego celu jest dokonywana m.in. poprzez dofinansowanie międzynarodowych projektów pilotażowych z grupy tzw. *Large Scale Pilots*. Pilotażowe projekty wielkoskalowe to inicjatywy, których celem jest wdrożenie wypracowanych rozwiązań informatycznych, pozwalających na przeprowadzenia transgranicznych usług cyfrowych w państwach członkowskich UE w wybranych domenach: e-biznes[3], e-sprawiedliwość[4], e-zdrowie[5], e-zamówienia publiczne[6], e-identyfikacja[7].

Aktualny pozostaje pogląd, zgodnie z którym państwa członkowskie powinny podejmować działania w celu umożliwienia prowadzenia europejskich postępowań transgranicznych w formie elektronicznej. Dzięki temu, w sposób naturalny powstaje alternatywa dla postępowania wykorzystującego drukowane formularze. Konstytucyjne prawo do sądu to nie tylko dostęp do wymiaru sprawiedliwości, ale również możliwość korzystania z efektywnych procedur pozwalających na skuteczne egzekwowanie swoich praw. Rządy państw członkowskich borykają się z licznymi utrudnieniami na drodze do usprawnienia wymiaru sprawiedliwości, szczególnie w przypadku sporów o charakterze transgranicznym. Przedłużające się postępowania sądowe, problemy z doręczeniami pocztowymi, konieczność osobistego stawiennictwa w sądach to jedynie przykładowy katalog takich wyzwań. W tym kontekście informatyzacja postępowania cywilnego jawi się jako najskuteczniejszy środek pozwalający na pełne urzeczywistnienie tego postulatu.

Projekty pilotażowe dotyczące rozwijania i badania transgranicznych usług cyfrowych

Akty prawne przyjmowane na szczeblu UE zdradzają tendencję do wprowadzania rozwiązań umożliwiających doręczenia elektroniczne, telekonferencje, wnoszenie pism procesowych do sądu za pośrednictwem systemów teleinformatycznych. Poza tym Komisja Europejska we współpracy z państwami członkowskimi UE, przedsiębiorcami, organami administracji publicznej, środowiskami akademickimi, sektorem prywatnym i społecznościami lokalnymi już od 2008 r. opracowuje projekty pilotażowe mające na celu rozwijanie i badanie sprawnych, transgranicznych usług cyfrowych[8]. Na przestrzeni kilku lat zrealizowano kilka projektów z grupy *Large Scale Pilots*, do których należą:

[1] Asystent w Zakładzie Prawa Medycznego Uniwersytetu Medycznego im. Karola Marcinkowskiego w Poznaniu. Autor publikacji naukowych i popularnonaukowych oraz prelegent konferencji naukowych i branżowych poświęconych tematyce związanej z elektronizacją wymiaru sprawiedliwości, czynnie zaangażowana w prace w ramach międzynarodowych projektów z grupy tzw. Large Scale Pilot, tj. epSOS, e-SENS, e-CODEX, SPOCS oraz openMedicine.

[2] *L. Łuczak-Noworolnik*, E-wymiar sprawiedliwości jako przykład dążenia do informatyzacji działalności instytucji państwowych, (w:) *Z. Rykiel*, *J. Kinal*, *D. Porczyński* (red.), Wirtualne i estetyczne aspekty humanizacji przestrzeni społecznej, Rzeszów 2015, s. 61–71.

[3] SPOCS (Simple Procedures Online for Cross- Border Services), e-SENS (Electronic Simple European Networked Services) https://www.esens.eu (dostęp z 11.3.2018 r.).

[4] e-CODEX e-Justice Communication via Online Data Exchange https://www.e-codex.eu (dostęp z 11.3.2018 r.), e-SENS (Electronic Simple European Networked Services) https://www.esens.eu (dostęp z 11.3.2018 r.).

[5] ePSOS (Smart Open Services for European Patients), http://www.epsos.eu (dostęp z 11.3.2018 r.).

[6] PEPPOL (Pan-European Public Procurement Online), http://www.peppol.eu/about_peppol/about-openpeppol-1 (dostęp z 11.3.2018 r.).

[7] Więcej na temat projektów Large Scale Pilots zob. https://ec.europa.eu/digital-agenda/en/large-scale-pilot-projects (dostęp z 11.3.2018 r.). Szczegółowy opis e-usługi dostępny w dokumencie https://www.esens.eu/sites/default/files/eSENSD514BusinessLifecycleRequirementsFrameworkv1.pdf (dostęp z 11.3.2018 r.).

[8] Komisja Europejska, 2010, EUROPA 2020 – Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, COM(2010) 2020, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:PL:PDF (dostęp z 11.3.2018 r.).

Nazwa projektu	Cel główny projektu	Cele szczegółowe projektu
Projekt STORK 2.0 Secure idenTity acrOss boRders linKed 2.0	Bezpieczna wymiana informacji w zakresie tożsamości elektronicznej	Przyczynia się do urzeczywistnienia jednolitego europejskiego obszaru elektronicznej identyfikacji i uwierzytelniania. Ustala interoperacyjność na poziomie krajowym oraz UE dla dowodów tożsamości elektronicznej zarówno dla osób prawnych, jak i fizycznych
Projekt e-CODEX e-Justice Communication via Online Data Exchange	Przyspieszenie działania wymiaru sprawiedliwości	Poprawia transgraniczny dostęp obywateli i przedsiębiorstw do usług prawnych w Europie oraz interoperacyjność organów wymiaru sprawiedliwości w UE
Projekt epSOS Smart Open Services for European Patients	Poprawa systemu opieki zdrowotnej	Polega na projektowaniu, tworzeniu i ocenie infrastruktury usługowej, która umożliwi transgraniczną interoperacyjność elektronicznych systemów dokumentacji medycznej
Projekt PEPPOL (przeniesiony do organizacji non-profit OpenPEPPOL) Pan-European Public Procurement Online	Poprawa funkcjonowania udzielania zamówień publicznych	Ułatwia europejskim przedsiębiorstwom przeprowadzanie online transakcji z organami publicznymi w Europie przy procedurach udzielania zamówień
Projekt SPOCS Simple Procedures Online for Cross-Border Services	Ułatwienie zakładania i prowadzenia działalności gospodarczej oraz zapewnienie prawidłowego funkcjonowania pojedynczych punktów kontaktowych	Pozwala zakładać online działalność gospodarczą za granicą oraz zapewnia właściwe funkcjonowanie pojedynczych punktów kontaktowych na terytorium UE
Projekt e-SENS Electronic Simple European Networked Services	Poprawa dostępu do transgranicznych usług publicznych na terenie Europy oraz budowa Jednolitego Rynku Cyfrowego na terenie UE oraz krajów zrzeszonych	Wspomaganie procesu wdrożenia europejskich dyrektyw i regulacji w różnych obszarach, tj. e-Sprawiedliwość, e-Zdrowie, elektroniczne zamówienia publiczne, zakładanie działalności gospodarczej online i inne. Umożliwienie wspólnego działania wszystkich państw członkowskich na rzecz elektronicznych usług. Zapewnienie skuteczniejszej i sprawniejszej obsługi stale rosnącej liczby spraw transgranicznych przez instytucje publiczne, w tym sądy. Zapewnienie większego bezpieczeństwa obywatelom w UE. Modernizacja systemów wymiaru e-administracji oraz e-sądownictwa w Europie. Poprawa współpracy i wymiany informacji pomiędzy instytucjami publicznymi w Europie

Projekt Me-CODEX . Maintanance of e-Justice Communication via Online Data Exchange	Utrzymanie rezultatów projektu e-CODEX do czasu ich przejęcia przez wybraną agencję. W projekcie zostaną wypracowane wymagania dla agencji zapewniające długoterminowe utrzymanie dorobku projektu e-CODEX	Zwiększenie się liczby krajów, które korzystają z rozwiązań e-CODEX. Powstanie reguł i wymogów, które zapewnią długoterminowe utrzymanie rozwiązań e-CODEX. Komunikacja elektroniczna wypracowana w ramach projektu: – zmniejszy koszty realizacji transgranicznych spraw sądowych dla obywateli i przedsiębiorców, – umożliwi szybsze uzyskanie rozstrzygnięcia, – zapewni większą transparentność, – usprawni prace wymiaru sprawiedliwości
Projekt e-CODEX PLUS e-Justice Communication via Online Data Exchange PLUS	Podłączenie sądów do por-talu e-Justice[9] w celu umożliwienia elektronicznego odbioru pozwów w ramach europejskiego nakazu zapłaty i postępowania w sprawie drobnych roszczeń	W Polsce planowane jest podłączenie sądów apelacji wrocławskiej

Źródło: Opracowanie własne na podstawie informacji opublikowanych na oficjalnych stronach internetowych projektów[10].

Projekt e-CODEX

Najbardziej interesujący z punktu widzenia analizowanej tematyki był projekt e-CODEX realizowany pod auspicjami Komisji Europejskiej w ramach Programu na rzecz Wspierania Polityki w zakresie Technologii Informacyjnych i Komunikacyjnych (*ICT PSP*) w latach 2010–2016. W projekcie brało udział 30 partnerów – ministerstw, instytucji badawczych, organów standaryzacyjnych oraz stowarzyszeń z 23 państw. Polskę od 2011 r. reprezentował poznański instytut badawczy, tj. Instytut Logistyki i Magazynowania oraz Ministerstwo Sprawiedliwości[11].

Jednym z fundamentalnych założeń projektu e-CODEX było stworzenie rozwiązań pozwalających na zaoszczędzenie czasu i obniżenie kosztów poprzez wprowadzenie bezpiecznych i uproszczonych sposobów realizacji postępowań sądowych na terytorium UE. Podejmowane działania nakierunkowane były także na rzeczywiste wsparcie idei jednolitego rynku europejskiego. Zadaniem projektu e-CODEX było także poprawienie dostępu obywateli i przedsiębiorców do instytucji prawnych oraz usprawnienie komunikacji z organami wymiaru sprawiedliwości drogą elektroniczną. Punktem wyjścia do dalszych działań było zauważalne zjawisko powszechnej rezygnacji przez obywateli UE z dochodzenia swoich roszczeń w sporach z kontrahentami zagranicznymi. Pozwy w sprawach transgranicznych najczęściej nie były składane z powodu nieznajomości zagranicznych regulacji prawnych, konieczności kontaktu z organami wymiaru sprawiedliwości w innym kraju i kosztownych, długotrwałych postępowań sądowych[12]. Uwzględniając powyższe uwarunkowania, projekt e-CODEX miał na celu uproszczenie elektronicznej wymiany informacji w krajach UE w toku postępowań sądowych. W przypadku powstania sporu transgranicznego obywatel poprzez platformę e-CODEX mógł złożyć wymagane dokumenty drogą elektroniczną, nie wychodząc z domu czy też z biura. Wartością dodaną wypracowanego rozwiązania było przygotowanie obszernych objaśnień ułatwiających przejście i poprawne wypełnienie konkretnego formularza. Zalogowany użytkownik uzyskiwał także na bieżąco informacje o otrzymanych dokumentach i rozstrzygnięciach sądowych. W trakcie prac w projekcie postawiono sobie za jeden z celów zacieśnienie współpracy ze środowiskiem prawniczym, tak aby jego przedstawiciele mieli realny wpływ na tworzone narzędzia. Pełnomocnicy

[9] Zob. https://e-justice.europa.eu/home.do?action=home&plang=pl (dostęp z 15.3.2018 r.).

[10] Zob. *L. Łuczak-Noworolnik*, Elektroniczne usługi publiczne w wymiarze europejskim – na wybranych przykładach, (w:) *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), E-obywatel, E-sprawiedliwość, E-usługi, Warszawa 2017, s. 322–332.

[11] Więcej na temat samego projektu na ogólnej stronie internetowej: https://www.e-codex.eu (dostęp z 15.3.2018 r.) oraz na polskiej stronie internetowej prowadzonej przez Instytut Logistyki i Magazynowania: https://www.eprawo.net (dostęp z 15.3.2018 r.).

[12] Szerzej na temat identyfikowanych barier w rozwoju e-justice w Unii Europejskiej *K. Flaga-Gieruszyńska*, Wybrane aspekty efektywności postępowań elektronicznych w sprawach transgranicznych, (w:) *B. Śliwczyński*, *L. Łuczak-Noworolnik* (red.), e-Wymiar sprawiedliwości w aspekcie europejskim, Poznań 2016, s. 8; https://www.eprawo.net/images/KonferencjaNaukowa/eWymiar-sprawiedliwoci.pdf (dostęp z 15.3.2018 r.).

profesjonalni zyskali tym samym nowe rozwiązanie pozwalające na sprawną komunikację z organami wymiaru sprawiedliwości w innych państwach UE[13]. Możliwość realizacji postępowań drogą elektroniczną – stworzona przez projekt e-CODEX – była pozytywnie oceniana przez prawników, którzy jako wartość dodaną wskazywali zapewnienie sprawniejszej realizacji postępowań oraz pewność doręczenia dokumentów do właściwego sądu zagranicznego.

Projekt e-CODEX realizowany był równolegle na szczeblu siedmiu różnych pakietów[14]:

Pakiet prac 1 – Administracja i trwałość projektu,

Pakiet prac 2 – Komunikacja,

Pakiet prac 3 – Pilotaż i testowanie,

Pakiet prac 4 – Elektroniczny podpis oraz elektroniczna tożsamość,

Pakiet prac 5 – Elektroniczna wymiana informacji oraz elektroniczne płatności,

Pakiet prac 6 – Dokumenty i semantyka,

Pakiet prac 7 – Architektura.

Wyniki prac poszczególnych grup zostały przedstawione w postaci obszernych dokumentów, nazwanych deliverable, opublikowanych następnie na stronie internetowej projektu pod adresem: https://www.e-codex.eu/downloads.

Projekt skupiał się w szczególności na wprowadzeniu możliwości skutecznej realizacji wybranych europejskich postępowań sądowych, takich jak:

1) europejskiego postępowania nakazowego uregulowanego w rozporządzeniu (WE) Nr 1896/2006 Parlamentu Europejskiego i Rady z 12.12.2006 r. ustanawiającym postępowanie w sprawie europejskiego nakazu zapłaty[15],
2) europejskiego postępowania w sprawie drobnych roszczeń uregulowanego w rozporządzeniu (WE) Nr 861/2007 Parlamentu Europejskiego i Rady z 11.7.2007 r. ustanawiającego europejskie postępowanie w sprawie drobnych roszczeń[16].

Przywołane akty prawne z uwagi na formę, w której zostały przyjęte (rozporządzenie), są stosowane bezpośrednio we wszystkich państwach członkowskich UE (poza Danią[17]). Ponadto w celu ustandaryzowania przebiegu europejskich postępowań sądowych uregulowanych w ich treści wprowadzono do każdego z wyżej wskazanych rozporządzeń załączniki zawierające formularze wykorzystywane zarówno przez sąd, jak i strony postępowania. Możliwość skorzystania ze standardowych formularzy bez wątpienia wprowadza realną możliwość przeprowadzenia postępowania drogą elektroniczną, pod warunkiem że państwo członkowskie dopuszcza taką formę. Zgodnie bowiem z treścią art. 7 rozporządzenia w sprawie europejskiego postępowania nakazowego: „Pozew wnosi się w formie papierowej lub za pomocą innego środka komunikacji, w tym komunikacji elektronicznej, akceptowanego przez państwo członkowskie wydania i dostępnego sądowi wydania". Analogiczne uregulowanie odnajdujemy w art. 4 ust. 1–2 rozporządzenia w sprawach drobnych roszczeń, w świetle którego: „1. Powód wszczyna europejskie postępowanie w sprawie drobnych roszczeń, wypełniając formularz pozwu A zawarty w załączniku A i składając go we właściwym sądzie lub trybunale bezpośrednio, za pośrednictwem poczty lub innych środków komunikacji, takich jak faks lub poczta elektroniczna, akceptowanych przez państwo członkowskie, w którym wszczyna się postępowanie. Formularz pozwu zawiera opis dowodów uzasadniających powództwo, a w stosownych przypadkach dołącza się do niego wszelkie odpowiednie dokumenty uzupełniające. 2. Państwa członkowskie powiadamiają Komisję o środkach komunikowania, które mogą zaakceptować. Komisja podaje te informacje do wiadomości publicznej".

Ponadto każde z państw członkowskich powiadamia Komisję Europejską o środkach komunikowania, które akceptują, a Komisja podaje te informacje do wiadomości publicznej poprzez Europejki atlas sądowy w sprawach cywilnych. Obecnie Europejski Atlas Sądowy w sprawach cywilnych stanowi jedną z podstron portalu e-Justice[18]: https://e-justice.europa.eu/content_european_payment_order-353-pl.do[19].

[13] Szerzej na ten temat *L. Łuczak-Noworolnik*, *A.F. Żurawski*, Jak skutecznie dochodzić należności od zagranicznych kontrahentów – narzędzia informatyczne usprawniające pracę pełnomocnika profesjonalnego w sporach transgranicznych, Palestra 2016, Nr 6, s. 95–102.

[14] Zob. https://www.eprawo.net/index.php/projekty/o-projekcie/opis-prac (dostęp z 15.3.2018 r.).

[15] Dz.Urz. UE L Nr 399, s. 1–32 ze zm.; dalej jako: rozporządzenie w sprawie europejskiego nakazu zapłaty.

[16] Dz.Urz. UE L Nr 199, s. 1–22 ze zm.; dalej jako: rozporządzenie w sprawie drobnych roszczeń.

[17] Odpowiednio w pkt 32 preambuły rozporządzenia w sprawie europejskiego nakazu zapłaty oraz pkt 38 preambuły rozporządzenia w sprawie drobnych roszczeń Dania nie uczestniczy w przyjęciu wyżej wskazanych rozporządzeń.

[18] Portal e-Justice funkcjonuje od 16.7.2010 r. i powstał w ramach działań podejmowanych przez Instytucje UE w celu wdrażania technologii informacyjno-komunikacyjnej w dziedzinie prawa. Portal zgodnie z zamiarem jego twórców ma w szczególności zwiększyć bezpieczeństwo obrotu prawnego oraz podnieść świadomość prawną podmiotów funkcjonujących na terytorium UE. Portal e-Justice jest dostępny pod adresem: https://e-justice.europa.eu/home.do we wszystkich językach urzędowych UE i dostarcza: informacji m.in. na temat systemów sądowniczych; podstawowych wiadomości na temat danych gromadzonych w rejestrach prowadzonych przez poszczególne państwa członkowskie w UE takich jak np. rejestry handlowe, księgi wieczyste; wskazówek, jak znaleźć prawnika albo mediatora w innym państwie UE. Zob. *M. Błaszczyk*, Portal e-justice – narzędzie usprawniające współpracę w Unii Europejskiej, (w:) *G. Szpor* (red. naukowy), Jawność i jej ograniczenia, *J. Gołaczyński* (red. tomu), Tom VIII. Postępowania sądowe, Warszawa 2015, s. 237 i n.

[19] Europejski Atlas Sądowy to strona internetowa prowadzona przez Komisję Europejską dostarczająca informacji dotyczących współpracy sądowej w sprawach cywilnych. Atlas umożliwia wypełnienie on-line standardowych formularzy sporządzonych do celów niektórych procedur transgranicznych. Pomaga również w określeniu właściwych sądów lub organów. W atlasie zawarte są też informacje o systemach sądowniczych w państwach członkowskich. Wszystkie informacje są dostarczane przez państwa członkowskie. Europejski Atlas Sądowy w sprawach cywilnych był dostępny pod adresem: http://ec.europa.eu/justice_home/judicialatlascivil/ i podobnie do portalu e-Justice był dostępny we wszystkich językach państw członkowskich UE. Szerzej na ten temat w sprawozdaniu Komisji dla Rady, Parlamentu Europejskiego i Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie zastosowania decyzji Rady Nr 2001/470/WE ustanawiającej europejską sieć

Dobór procedur pilotażowych był podyktowany przede wszystkim względami pragmatycznymi, przy uwzględnieniu zauważalnej tendencji wzrostowej liczby toczących się sporów transgranicznych. Głównymi odbiorcami projektu byli obywatele, przedsiębiorcy, a także pełnomocnicy profesjonalni działający w imieniu swoich klientów.

Na podkreślenie zasługuje fakt, iż poza stworzeniem dedykowanej platformy umożliwiającej m.in. elektroniczne składanie pozwu o wydanie europejskiego nakazu zapłaty do Niemiec, Grecji, Malty[20], w toku prac przeprowadzono pogłębione badania aktowe, ankietowe oraz dyseminowano wiedzę na temat europejskich postępowań sądowych. Jedną z form upowszechniania było opracowanie i przeprowadzenie warsztatów dla przedsiębiorców oraz pełnomocników profesjonalnych w kilkunastu różnych miejscach w Polsce, począwszy od Poznania, przez Warszawę, Kraków i Białystok. Badana tematyka była także przedmiotem dyskusji w trakcie ogólnopolskiej konferencji naukowej pod hasłem „e-Wymiar sprawiedliwości w aspekcie europejskim", której wynikiem była monografia wydana pod tym samym tytułem[21].

Wyniki projektu e-CODEX zostały przejęte przez projekt e-SENS, który zakończył się 31.3.2017 r. Projekt e-SENS korzystał w pełni z wyników innych projektów z grupy LSP, stając się ich naturalną kontynuacją, utrzymując przy tym wypracowane rezultaty. Projekt e-SENS opierał się na wynikach wyżej wskazanych projektów i stanowił pomost pomiędzy fazą pilotażową a operacyjną, w trakcie której transgraniczne usługi publiczne są już w pełni dostępne dla obywateli UE. W projekcie brało udział 20 partnerów z następujących państw: Austrii, Czech, Danii, Estonii, Francji, Grecji, Hiszpanii, Holandii, Irlandii, Luksemburga, Niemiec, Norwegii, Polski, Portugalii, Rumunii, Słowacji, Słowenii, Szwecji, Turcji i Włoch. Projekt w dużym stopniu sfinansował Europejski Instytut Norm Telekomunikacyjnych (*ETSI*) i *OpenPEPPOL*[22].

Kolejne projekty

Aktualnie trwają intensywne prace w ramach dwóch kolejnych projektów Me-CODEX oraz e-CODEX PLUS dotyczących tematyki, którą obejmował projekt e-CODEX.

W projekcie Me-CODEX prace są prowadzone w pięciu pakietach[23]:

1) WP1 Zarządzanie i koordynacja projektu – celem pakietu jest zapewnienie sprawnej realizacji projektu od strony finansowej i administracyjnej.
2) WP2 Model zarządzania i utrzymania (Governance) – celem pakietu jest opracowanie mapy drogowej dotyczącej krótko- i długoterminowego utrzymania dorobku projektu e-CODEX. W ramach prac powstaną wytyczne dotyczące przejęcia dorobku projektu e-CODEX przez wskazaną agencję.
3) WP3 Techniczne utrzymanie komponentów e-CODEX – celem pakietu jest aktualizacja, usuwanie błędów, wsparcie dla modułów projektu e-CODEX. WP3 będzie utrzymywał następujące moduły: DOMIBUS Gateway, DOMIBUS Connector, Security Library, Central Testing Platform, DOMIBUS Admin GUI, pMode Generator i powstałe schematy XML dla pilotowanych procedur.
4) WP4 Komunikacja i marketing – celem pakietu jest zwiększenie wiedzy na temat rozwiązań projektu e-CODEX w zakresie elektronicznej komunikacji w transgranicznych sprawach sądowych.
5) WP5 Badania i konsolidacja pilotaży – celem pakietu jest rozszerzenie uruchomionych pilotaży na nowe kraje, a także zidentyfikowanie nowych procedur, które mogłyby wykorzystać stworzone elektroniczne rozwiązania.

W projekcie e-CODEX PLUS prace są prowadzone w ramach ośmiu zadań[24]:

1) Koordynacja projektu,
2) Faza przygotowawcza,
3) Wdrożenie elektronicznej obsługi procesów ENZ i DR w sądzie,
4) Instalacja Gateway/Connector (środowisko testowe),
5) Testy,
6) Przygotowanie środowiska produkcyjnego,
7) Uruchomienie produkcyjne,
8) Analiza wartości dodanej wynikającej z reguł biznesowych.

Celem projektu e-CODEX PLUS (finansowanego z programu CEF *Connecting Europe Facility*) jest podłączenie sądów do portalu e-Justice w celu umożliwienia elektronicznego odbioru pozwów w ramach europejskiego nakazu zapłaty i postępowania w sprawie drobnych roszczeń. W Polsce planowane jest podłączenie sądów apelacji wrocławskiej. Projekt

sądową w sprawach cywilnych i handlowych: http://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52006DC0203&from=PL (dostęp z 13.3.2018 r.). Zob. *I. Miedzińska*, Europejska Sieć Sądowa i Europejski Atlas Sądowy w sprawach cywilnych jako instrumenty współpracy transgranicznej – aspekty instytucjonalne, (w:) *B. Śliwczyński*, *L. Łuczak-Noworolnik* (red.), e-Wymiar sprawiedliwości w aspekcie europejskim, Poznań 2016, s. 80 i nast.; https://www.eprawo.net/images/KonferencjaNaukowa/eWymiar-sprawiedliwoci.pdf (dostęp z 15.3.2018 r.).

[20] Monografia udostepniona na licencji Creatve Commons Uznanie autorstwa 3.0 Polska pod adresem: https://www.eprawo.net/images/KonferencjaNaukowa/eWymiar-sprawiedliwoci.pdf (dostęp z 15.3.2018 r.).

[21] Zob. https://www.eprawo.net/index.php/131-raport-z-badan-ankietowych-projektu-e-codex-pelnomocnicy-profesjonalni-wobec-transgranicznych-postepowan-sadowych (dostęp z 13.3.2018 r.); https://www.eprawo.net/index.php/warsztaty2 (dostęp z 13.3.2018 r.).

[22] *L. Łuczak-Noworolnik*, Elektroniczne usługi publiczne w wymiarze europejskim – na wybranych przykładach, (w:) *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), E-obywatel, E-sprawiedliwość, E-usługi, Warszawa 2017, s. 322–332.

[23] Informacje pochodzą ze strony: https://www.eprawo.net/index.php/projekty-w-trakcie-realizacji/mecodex/opis-prac (dostęp z 15.3.2018 r.).

[24] Informacje pochodzą ze strony: https://www.eprawo.net/index.php/projekty-w-trakcie-realizacji/mecodex/opis-prac (dostęp z 15.3.2018 r.).

realizowany jest od 1.6.2017 r. i zakończy się z 31.5.2019 r. Koordynatorem projektu e-CODEX PLUS, podobnie jak w przypadku projektu e-CODEX i e-SENS, jest Ministerstwo Sprawiedliwości Nadrenii i Westfalii. Partnerami projektu są podmioty z Austrii, Grecji, Holandii, Portugalii oraz Polski. Polskę reprezentuje Instytut Logistyki i Magazynowania oraz Uniwersytet Wrocławski.

Podsumowanie

Znamienne w omawianym obszarze pozostają niezmiennie słowa Koordynatora projektów e-CODEX, e-SENS, e-CODEX PLUS z Ministerstwa Sprawiedliwości Nadrenii Północnej-Westfalii (Niemcy). W jego ocenie: „Usługi cyfrowe w Europie są zróżnicowane, co skutkuje wieloma utrudnieniami w transakcjach transgranicznych. Ponadto odmienne jest także podejście do usług cyfrowych – komunikacji za pośrednictwem poczty e-mail czy formularzy elektronicznych – odrębne są formalności, a w grę wchodzą także aspekty kulturowe, nie wspominając o trudnościach ze zrozumieniem różnych pojęć biznesowych czy dokumentów. Z wszystkimi tymi wyzwaniami trzeba się uporać”[25].

W analizowanym kontekście niebagatelne znaczenie mają projekty informatyczne realizowane na szczeblu UE, które pełnią istotną funkcję w budowie społeczeństwa informacyjnego. Przyczyniają się także do upowszechnienia wiedzy na temat informatyzacji działalności wymiaru sprawiedliwości. Bez wątpienia cyfryzacja transgranicznych usług publicznych wprowadzana poprzez projekty z grypy LSP przynosi wymierne korzyści i oszczędności zarówno pod względem czasu, jak i pieniędzy, tak po stronie organów wymiaru sprawiedliwości, obywateli, przedsiębiorców, jak i pełnomocników profesjonalnych.

[25] Zob. http://cordis.europa.eu/result/rcn/158775_pl.html (dostęp z 15.3.2018 r.).

Słowa kluczowe: e-wymiar sprawiedliwości, *Large Scale Pilots*, elektronizacja wymiaru sprawiedliwości, e-sądownictwo, e-CODEX, e-SENS

E-justice system in the European aspect on the example of project e-CODEX

The aim of the present study is showing multiscale projects from the group of Large Scale Pilots which are to popularize using means of electronic communication in transboundary cases. Premise of the results of the projects is to amend prolonged judicial proceedings, level problems with postal deliveries and eliminate the necessity of personal appearance in court. At the same time, the analyzed projects seem as initiatives fundamentally acting in the development of European informational society.

Keywords: e-justice system, Large Scale Pilots, digitization of justice system, e-judicature, e-CODEX, e-SENS.

Identyfikacja elektroniczna w UE – od dyrektywy do rozporządzenia

Agata Burek[1]

Intensywny rozwój komunikacji elektronicznej przyczynił się do zapoczątkowania zawierania umów elektronicznych, do czego niezbędne są bezpieczne, godne zaufania i skuteczne mechanizmy identyfikacji elektronicznej, tzn. takie, w których przesyłane dane nie są dostępne dla osób niepożądanych, oraz takie, w których bez problemu można zidentyfikować strony umowy, a złożone przez nich oświadczenia woli wywołują odpowiednie skutki prawne. W tym momencie pojawiło się miejsce na stworzenie odpowiednich regulacji prawnych. Pierwsze powstały pod koniec XX w., w tym dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z 13.12.1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych[2]. Po latach okazało się, że dyrektywa ta nie spełniła wystarczająco swoich głównych założeń. Celem niniejszego opracowania jest wskazanie, dlaczego tak się stało, a tym samym wskazanie powodów, dla których UE postawiła na nową regulację: rozporządzenie Parlamentu Europejskiego i Rady Nr 910/2014 z 23.7.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE[3], które jako akt ujednolicenia prawa jest nową nadzieją na rozpowszechnienie transakcji elektronicznych na terytorium UE.

Uwagi wstępne

Prężny rozwój technik komunikacji elektronicznej coraz intensywniej wpływa na kwestie gospodarcze i społeczne współczesnego życia. Internet umożliwił permanentny oraz obojętny terytorialnie kontakt pomiędzy podmiotami na całym świecie. Wraz z postępem nieograniczonej komunikacji odczuwana potrzeba anonimowości użytkowników sieci teleinformatycznych straciła na znaczeniu. Obecnie wzrosła nie tylko potrzeba rozpoznawalności, ale również zabezpieczenia swojej tożsamości, ochrony przed podszyciem się. Co więcej, brak pozytywnego potwierdzenia swojej tożsamości drugiemu podmiotowi rodzi problemy w rozwoju wielu możliwości, jakie daje nam komunikacja elektroniczna. Mowa tutaj o czynnościach życia codziennego, jak zakupy online, zawieranie umów elektronicznych czy rezerwacja biletów, które w naturalny sposób przeszły ze świata pozawirtualnego w rzeczywistość wirtualną. Podobnie wygląda kwestia kontaktu z organami administracji publicznej podczas wyrabiania dowodu osobistego czy zakładania działalności gospodarczej. Każda czynność elektroniczna powinna być odpowiednio zabezpieczona przed udostępnieniem zawartych w jej ramach danych niepożądanym osobom trzecim. Podstawą rozwoju e-usług jest zaufanie przez użytkowników do używanych w jej ramach narzędzi (oprogramowania), a także do tożsamości drugiej strony oraz autentyczności i integralności danych[4]. Bazę transakcji elektronicznych powinny stanowić też łatwe mechanizmy ich obsługi. Uwidoczniła się potrzeba identyfikacji, uwierzytelnienia i autoryzacji swojej tożsamości. Identyfikacja to nic innego jak utożsamienie – przypasowanie danych do podmiotu, np. nicku, do konkretnej osoby. Uwierzytelnianie natomiast ma na celu weryfikację podanej tożsamości i jest jednym z najbardziej kluczowych komponentów bezpiecznych transakcji elektronicznych. W momencie gdy tożsamość użytkownika będzie potwierdzona, następuje autoryzacja, czyli proces polegający na odmówieniu albo przyznaniu dostępu do systemu[5]. Wszystkie wymienione elementy istnieją nie tylko w świecie e-usług. Są tak samo stosowane w transakcjach tradycyjnych[6], np. w banku uwierzytelniamy się za pomocą złożenia podpisu zgodnego ze wzorem albo po uprzednim okazaniu dowodu osobistego. Następnie przechodzimy proces autoryzacji, otrzymując dostęp do danych na naszym koncie. W transakcjach tradycyjnych komponenty te są już tak naturalne, że prawie niewyczuwalne. Dopiero w sytuacji e-usług nabierają one większego znaczenia.

Jednak, co staje się, gdy już otrzymamy taki dostęp? Tutaj rozpoczyna się rola prawa, którego zadaniem jest określenie: skutków stosowania narzędzi elektronicznych, przesłanek, które wyznaczą skuteczność złożenia oświadczenia woli, czy takie oświadczenie będzie miało moc dowodową, a także dokonanie systematyki pojęciowej.

[1] Autorka jest studentką kierunku prawo na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] Dz.Urz. UE L Nr 13, s. 12–20; dalej jako: dyrektywa 1999/93/WE.

[3] Dz.Urz. UE L Nr 257, s. 73–114; dalej jako: rozporządzenie eIDAS.

[4] *J. Muszyński*, Identyfikacja, uwierzytelnianie i autoryzacja, http://www.computerworld.pl/news/Identyfikacja-uwierzytelnianie-i-autoryzacja,299422.html (dostęp z 1.4.2017 r.).

[5] *A. Smoliński*, Sposoby zabezpieczeń systemów IT jako ewolucja konwencjonalnych metod zabezpieczeń, s. 12.

[6] *T. Mielnicki* (red.), Identyfikacja i uwierzytelnienie w usługach elektronicznych, Przewodnik Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013, s. 6.

Od dyrektywy do rozporządzenia

Identyfikacja elektroniczna zaczęła być regulowana pod koniec XX w. Pierwsze akty prawne dotyczyły podpisu cyfrowego i zostały ustanowione w Stanach Zjednoczonych Ameryki. Między innymi była to ustawa o podpisach cyfrowych stanu Utah z 9.3.1995 r.[7]. W ślad za regulacjami amerykańskimi poszedł prawodawca wspólnotowy, który uchwalił dyrektywę 1999/93/WE. Celem podpisu elektronicznego miało być zagwarantowanie zaufania do transakcji elektronicznych i ich rozpowszechnianie.

Wspólnoty Europejskie nie pozostawiły tej materii regulacjom krajowym, ponieważ w rozpowszechnieniu transakcji elektronicznych widziały rozwój rynku wewnętrznego. Dlatego pojawiła się potrzeba standaryzacji prawa dotyczącego identyfikacji elektronicznej. Gdyby regulowały to poszczególne prawa krajowe, skutki stosowania danych e-usług miałyby zasięg tylko w danym państwie. Nie tylko powodowałoby to ograniczenie rozwoju e-handlu na rynku wewnętrznym, ale powstałyby również różnice technologiczne i terminologiczne.

Początkowo zdecydowano, że dyrektywa, która jest instrumentem harmonizacji, będzie wystarczająca. Przypomnijmy, że celem takiej regulacji miało być ustanowienie jasnych ram wspólnotowych dla podpisów elektronicznych, co skutkowałoby wzmocnieniem ogólnej akceptacji nowych technologii[8]. Założeniem prawodawcy wspólnotowego było rozpowszechnienie mechanizmu podpisu cyfrowego na terenie UE oraz swobodny, transgraniczny przepływ produktów i usług, pochodzących z handlu elektronicznego i skuteczność prawna podpisu cyfrowego. Dzięki regulacjom omawianej dyrektywy ułatwiony miał być kontakt obywateli UE z władzami innych państw członkowskich w dziedzinach takich jak: podatki, wymiar sprawiedliwości, zamówienia publiczne, ubezpieczenia społeczne i ochrona zdrowia[9]. Kluczowe było również nadanie podpisowi elektronicznemu mocy dowodowej przed sądami, co miało budzić poczucie bezpieczeństwa, w sytuacji gdy niezbędne będzie domaganie się swoich praw przed organami sprawiedliwości. Reasumując, dyrektywa 1999/93/WE miała na celu rozpowszechnienie stosowania podpisu elektronicznego poprzez zapewnienie bezpieczeństwa i zaufania do transakcji elektronicznych.

Komisja UE została zobowiązana do sporządzenia sprawozdania dla Parlamentu Europejskiego i Rady, sprawdzającego wykonanie dyrektywy 1999/93/WE[10]. Dokument ten powstał 15.3.2006 r. Bazę sprawozdania stanowiło studium sporządzone przez zewnętrznych konsultantów oraz nieformalne konsultacje z zainteresowanymi z 2003 r. Przeprowadzono je w celu zebrania praktycznych uwag. Sprawozdanie miało kompleksowo zbadać problemy, z jakimi boryka się identyfikacja elektroniczna w UE – nie tylko teoretycznie, ale też ze względu na obowiązującą praktykę.

Sprawozdanie potwierdziło, że dyrektywa 1999/93/WE sprostała swojemu zadaniu i zrealizowała większość swoich celów. Akt ten implementowało do krajowego porządku prawnego 25 państw członkowskich, co uznano za systematyzujący status prawny podpisu elektronicznego. Jednakowoż stwierdzono, że podpisy elektroniczne nie spopularyzowały się na terytorium UE w takim stopniu, jak zakładano. Od razu można zauważyć tutaj sprzeczność. Podstawowym celem dyrektywy 1999/93/WE było rozpowszechnienie podpisu elektronicznego. Miał on usprawniać handel na rynku wewnętrznym. Obiektywnie należy uznać, że skoro w omawianym sprawozdaniu stwierdzono, że podpisy cyfrowe, zwłaszcza zaawansowane oraz zaawansowane oparte na kwalifikowanym certyfikacie i złożone za pomocą bezpiecznego urządzenia, nie były stosowane na taką skalę, jak zakładano, to dyrektywa 1999/93/WE nie spełniła swojego zadania. Wśród elementów, które złożyły się na taki rezultat, można wymienić:

– komplikacje techniczne, związane z technologią PKI, w których jest stosowany czynnik zaufania podmiotowi trzeciemu, przy zawieraniu transakcji nieznanych sobie stron;
– brak regulacji wymogów usług weryfikacji podpisu elektronicznego przez podmioty świadczące usługi certyfikacyjne oraz ustaleń dotyczących wzajemnego uznawania się przez podmioty świadczące usługi certyfikacyjne, co doprowadziło do wykreowania odmiennych regulacji prawnych w poszczególnych państwach;
– brak interoperacyjności technicznej na poziomie krajowym i międzynarodowym, skutkujący powstaniem niewspółgrających ze sobą systemów;
– droga i skomplikowana archiwizacja dokumentów opatrzonych podpisem elektronicznym.

Chociaż zaawansowane formy podpisu elektroniczne nie przyjęły się w praktyce na tak dużą skalę, jak oczekiwano, to w wielu państwach członkowskich powstały inne mechanizmy bazujące na podpisie elektronicznym w prostszych formach. Wyszczególnić można dwa przeważające przykłady. Pierwszy to usługi bankowości elektronicznej, w której stosuje się hasła jednorazowe. Przyporządkować je można definicji zwykłego podpisu elektronicznego. Drugim zastosowaniem jest elektroniczny dostęp do administracji publicznej, czyli krajowy system identyfikacji. Często funkcjonują one na podstawie kart identyfikacyjnych, umożliwiających identyfikację, uwierzytelnianie i podpisywanie. Świetnym przykładem jest

[7] *M. Marucha-Jaworska*, Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym, Warszawa 2015, s. 46.

[8] Zob. motyw 4 preambuły dyrektywy 1999/93/WE.

[9] *M. Marucha-Jaworska*, Rozporządzenie eIDAS. Zagadnienia prawne i techniczne, Warszawa 2017, s. 20–21.

[10] Art. 12 dyrektywy 1999/93/WE.

Platforma Usług Administracji Publicznej – ePUAP. Jednak pod regulacją dyrektywy 1999/93/WE krajowe systemy identyfikacji nie były uznawane na terytorium UE poza państwem pochodzenia. Ani bankowość elektroniczna, ani krajowe systemy identyfikacji nie były regulowane prawem wspólnotowym, a zdecydowanie wyparły proponowane przez tę dyrektywę instytucje. Zastanawiające jest, czy popularność krajowych systemów identyfikacji oraz e-bankowości nie unaoczniły słabości dyrektywy 1999/93/WE. Skoro obywatele UE używają identyfikacji elektronicznej, to znaczy, że są nią zainteresowani, ale proponowane przez prawodawcę wspólnotowego mechanizmy nie spełniają oczekiwań użytkowników. To, co ich interesuje, to łatwość dostępu i obsługi oraz niskie koszty użytkowania. Można nawet stwierdzić, że najprostsze mechanizmy (zabezpieczania, szyfrowania) wystarczyły, by użytkownicy e-usług poczuli do nich zaufanie.

Pomimo powstałych problemów Komisja podkreśla pozytywny wpływ dyrektywy 1999/93/WE na rynek wewnętrzny, ponieważ uregulowano status prawny podpisu elektroniczne, w tym podstawowe zasady jego dopuszczalności. Jednak powstałe trudności należy usunąć za pomocą różnych inicjatyw[11]. Dla przykładu w maju 2010 r. sporządzono komunikat Komisji Europejskiej „Europejska Agenda Cyfrowa", gdzie założono cel zbudowania zaufania i zapewnienia bezpieczeństwa w środowisku internetowym za pomocą modernizacji przepisów dotyczących podpisu elektronicznego[12]. Dodatkowo Rada Europejska w paru konkluzjach z 2011 r. podniosła potrzebę transgranicznych transakcji elektronicznych, a także bezpiecznej identyfikacji elektronicznej i uwierzytelniania. W konkluzjach pozostawiono Komisji utworzenie jednolitego rynku cyfrowego. We wszystkich działaniach organów UE, które miały zapoczątkować zmianę dyrektywy 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, kładzie się nacisk na zapewnienie bezpieczeństwa i zaufania do transakcji elektronicznych, co można uzyskać dzięki: zwiększeniu pewności prawa, wprowadzeniu regulacji nadzoru, zapewnieniu wzajemnego uznawania krajowych systemów identyfikacji elektronicznej czy powiększeniu zakresu usług zaufania. Z opisanych inicjatyw organów UE wynika jedno – w ciągu pięciu lat od publikacji sprawozdania Komisji z wykonania dyrektywy 1999/93/WE nie było żadnego rzeczywistego działania mającego na celu zmianę prawa w zakresie identyfikacji elektronicznej. Dopiero w Akcie o Jednolitym Rynku Cyfrowym postawiono na modyfikacje tej dyrektywy[13]. W trakcie swojej prezydencji, tzw. w drugiej połowie 2011 r., Rzeczpospolita Polska rozpoczęła europejską dyskusję prowadzącą do opracowania nowej regulacji w sprawie identyfikacji elektronicznej na rynku wewnętrznym. Tym razem miało być to rozporządzenie. Istotną rolę odegrało Ministerstwo Gospodarki, które zorganizowało konferencję pt. *Boosting trust in the digital single market: the role of e-signature*. Podczas wydarzenia podjęto tezę, że w zakres europejskiego rynku cyfrowego wchodzi wspólny system identyfikacji elektronicznej, który należy stworzyć. Komisja Europejska 4.6.2012 r. opublikowała projekt rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającym dyrektywę 1999/93/WE. Przyczyny powstania nowego aktu przedstawione przez Komisję nie różniły się od poglądu przedstawionego w sprawozdaniu z wykonania tej dyrektywy. Oficjalnie nikt nie uznał, że była to zła regulacja. Stwierdzono natomiast, że nowa regulacja ma rozszerzać dorobek dyrektywy. Ostatecznie rozporządzenie eIDAS zostało uchwalone 23.7.2014 r. W podstawowej części, która stanowi większość jego przepisów, weszło do stosowania 1.7.2016 r. Jedno z uznawanych za jego główne założenie, czyli uznawanie krajowych systemów eID przez państwa członkowskie UE (wzajemne uznawanie), ma być stosowane od 29.9.2018 r.

Dyrektywa to instrument harmonizacji prawa[14]. Jej adresatem są państwa członkowskie, którym pozostawia się swobodę wyboru środków i form, za pomocą których ma zostać osiągnięty cel dyrektywy zgodnie z art. 288 akapit 3 Traktatu o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana)[15]. Państwa członkowskie są jednak zobowiązane do transponowania regulacji dyrektywy do prawa krajowego. Prowadzi to do stworzenia wspólnych podstaw w konkretnej materii, ale jednocześnie powoduje powstanie różnic między regulacjami państw[16]. Porządki prawne państw członkowskich zbliżają się w ten sposób do siebie, ale nie są identyczne, jednolite. Akty prawne państw członkowskich, które implementują dyrektywę mogą, w pewnym zakresie, od siebie odbiegać.

Rozporządzenie, odmiennie od dyrektywy, jest instrumentem ujednolicenia prawa. Do jego głównych cech należy ogólność i abstrakcyjność. Jako akt o ogólnym charakterze skierowany jest do szerokiego kręgu adresatów, w tym: organów UE i państw członkowskich, osób fizycznych czy osób prawnych oraz instytucji. Oznacza to, że konstruuje również prawa i obowiązki skierowane do jednostek[17]. Rozporządzenie, po wejściu w życie, wiąże w całości i – co bardzo ważne – jest bezpośrednio stosowane[18]. Eliminuje się w ten sposób potrzebę transponowania przepisów rozporządzenia do po-

[11] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady, Sprawozdanie z wykonania dyrektywy 1999/93/WE w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, Bruksela 15.3.2006 r.

[12] Europejska agenda cyfrowa: kluczowe inicjatywy, Bruksela 19.5.2010 r., http://europa.eu/rapid/press-release_MEMO-10-200_pl.htm (dostęp z 1.4.2017 r.).

[13] 12 projektów dla jednolitego rynku na 2012 r.: wspólnie na rzecz nowego wzrostu gospodarczego, IP/11/46, Bruksela 13.4.2011 r., http://europa.eu/rapid/press-release_IP-11-469_pl.htm (dostęp z 1.4.2017 r.).

[14] *J. Barcz*, Instytucje i prawo Unii Europejskiej. Podręcznik dla kierunków prawa, zarządzania i administracji, Warszawa 2015, s. 232.

[15] Dz.Urz. UE C Nr 202; dalej jako: TFUE.

[16] *J. Barcz*, Instytucje i prawo…, s. 232–233.

[17] *Ibidem*, s. 230.

[18] Zob. art. 288 akapit 2 TFUE.

rządków krajowych, ponieważ automatycznie stają się ich częścią, a zakres prawny regulowany rozporządzeniem nie może być już stanowiony przez organy państw członkowskich[19]. Tym samym państwa członkowskie nie posiadają kompetencji zmiany przepisów, które są dla nich kłopotliwe. Rozporządzenie jest bardzo skutecznym instrumentem ujednolicenia prawa na terenie UE, ponieważ intensywnie ingeruje w prawa krajowe, ma szeroki zasięg terytorialny i podmiotowy[20].

Powyższe rozważania teoretyczne można przełożyć na omawiane zagadnienie, dyrektywa 1999/93/WE, będąca instrument harmonizacji, spowodowała różnice między regulacjami państw członkowskich w zakresie identyfikacji elektronicznej. Do głównych zalicza się: odmienności terminologiczne, różnice w funkcjonowaniu nadzoru[21] oraz niejednakowe wymogi, które muszą spełnić podmioty świadczące usługi elektroniczne, a także wymogi samego podpisu elektronicznego. Rozporządzenie stawia jednolite warunki uwierzytelniania oraz wymogi dla dostawców usług zaufania. Ujednolicenie standardów stawianych identyfikacji elektronicznej ułatwia wprowadzenie wzajemnego uznawania krajowych systemów identyfikacji elektronicznej przez państwa członkowskie oraz daje duże szanse na rozpowszechnienie się transgranicznych transakcji elektronicznych.

Cele rozporządzenia eIDAS

Warto przyjrzeć się celom, jakie stawia sobie nowa regulacja, mająca zapewnić bezpieczeństwo i zaufanie w kwestii transakcji elektronicznych. Prawodawca unijny stanowi, że rozporządzenie eIDAS ma poszerzać oraz umacniać dorobek uchylonej dyrektywy. Celem nie jest zmienienie całego istniejącego porządku prawnego dotyczącego identyfikacji elektronicznej. Pod rządami dyrektywy nie powstały odpowiednie ramy transgraniczne i międzysektorowe, ułatwiające funkcjonowanie bezpiecznych transakcji elektronicznych, ale nie oznacza że takich ram nie w ogóle nie było[22]. Dopiero późniejsze komplikacje, które dotyczyły praktycznego stosowania zawartych w regulacji mechanizmów, oraz sam charakter dyrektywy spowodowały, że podpis elektroniczny nie rozpowszechnił się jako narzędzie służące do zawierania umów elektronicznych w takim stopniu, jak zakładano. Twierdzi się, że było to spowodowane za małym poczuciem bezpieczeństwa wśród potencjalnych użytkowników usług elektronicznych. W ten sposób wyklarował się naturalny cel nowego rozporządzenia – ulepszenie i ujednolicenie ram prawnych dla podpisów elektronicznych oraz ustanowienie nowych usług, które jednocześnie spełnią warunek bezpieczeństwa i zaufania.

Jednym z najbardziej istotnych celów eIDAS jest wprowadzenie reguł dotyczących korzystania z usług zaufania i identyfikacji elektronicznej na rynku wewnętrznym[23]. Krajowe systemy identyfikacji elektronicznej dotychczas nie były regulowane przez przepisy wspólnotowe. Regulacje takie powstały w poszczególnych państwach członkowskich w ramach krajowej administracji publicznej. Brakowało instytucji, która umożliwiałaby korzystanie z owych systemów w każdym państwie członkowskim[24]. Dlatego eIDAS kładzie duży nacisk na zapewnienie wzajemnego uznawania notyfikowanych systemów identyfikacji elektronicznej na terytorium UE. Takie bariery transgraniczne mają zostać uchylone przynajmniej w zakresie usług publicznych[25]. Obywatel ma w ten sposób zyskać możliwość kontaktowania się z sądami oraz urzędami państw członkowskich za pomocą środka identyfikacji elektronicznej pochodzącego z jego kraju. Zasada wzajemnego uznawania ma dodatkowo objąć poszczególne kwalifikowane usługi zaufania, co spowodować może rozwój dostawców usług zaufania, którzy posiądą możliwość wyjścia ze swoimi usługami poza rynek krajowy[26].

Rozporządzenie eIDAS zakłada neutralność technologiczną, co powinno służyć popularyzowaniu umów elektronicznych na rynku wewnętrznym[27]. Założenie otwartości na rozwój technologiczny wynika z bardzo szybkiego tempa zmian w tej dziedzinie[28]. Gdyby w ciągu najbliższych lat powstały lepsze, łatwiejsze, a przede wszystkim bezpieczniejsze mechanizmy szyfrowania tożsamości, ich wprowadzenie na rynek nie powinno być ograniczone przez prawo. Nowe technologie będą musiały spełniać jedynie wymogi zawarte w Rozporządzeniu eIDAS[29].

Kolejny cel eIDAS to przyznanie mocy dowodowej poszczególnym narzędziom, tj. podpisy elektroniczne. Uchylona dyrektywa dawała im co prawda taką moc, ale Komisja w swoim sprawozdaniu stwierdziła, że nie wyklarowało się orzecznictwo umożliwiające jednoznaczne uznawanie podpisów elektronicznych w praktyce[30]. Dostawcy usług zaufania również wyrażają zdanie, że sądy nie w każdym przypadku dopuszczały takie dowody. Obwinia się w tej kwestii nieścisłości prawne[31]. Teraz wprost istnieją przepisy zabraniające

[19] *J. Barcz*, Instytucje i prawo…, s. 231–232.
[20] *M. Marucha-Jaworska*, Rozporządzenie eIDAS…, s. 33.
[21] *Ibidem*, s. 23.
[22] Motyw 3 preambuły eIDAS.
[23] Forum eIDAS_PL Forum wymiany wiedzy w zakresie Rozporządzenia eIDAS w Polsce, Webinar Forum eIDAS_PL 1 z 26.11.2015 r., https://www.youtube.com/watch?v=BnRr27v9Aqo.
[24] *P. Polański*, Europejskie prawo handlu elektronicznego. Mechanizmy regulacji usług społeczeństwa informacyjnego, Warszawa 2014, s. 337.
[25] Motyw 12 preambuły eIDAS.
[26] Forum eIDAS_PL Forum wymiany wiedzy w zakresie Rozporządzenia eIDAS w Polsce, Webinar Forum eIDAS_PL 1 z 26.11.2015 r., https://www.youtube.com/watch?v=BnRr27v9Aqo.
[27] Motyw 27. preambuły eIDAS.
[28] Motyw 26. preambuły eIDAS.
[29] Motyw 27. preambuły eIDAS.
[30] Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady…, s. 6.
[31] Forum eIDAS_PL Forum wymiany wiedzy w zakresie Rozporządzenia eIDAS w Polsce, Webinar Forum eIDAS_PL 1 z 26.11.2015 r., https://www.youtube.com/watch?v=BnRr27v9Aqo.

odmowy mocy dowodowej podpisom elektronicznym i innym podobnym narzędziom w postępowaniu sądowym na terytorium UE[32].

Rozporządzenie eIDAS pozostawia pewne kwestie do regulacji państwom członkowskim. Te bowiem zostały zobowiązane do wyznaczenia organu nadzoru[33], który będzie sprawowany nad kwalifikowanymi dostawcami usług zaufania. W ramach swoich kompetencji krajowy organ nadzoru sporządza i publikuje tzw. list zaufania, informacje o kwalifikowanych dostawcach usług zaufania w swoim kraju[34]. Sankcje za naruszenie regulacji wprowadzonej przez eIDAS również należy ustalić w ramach swojego państwa[35]. Pomimo że rozporządzenie, jako akt, charakteryzuje się bezpośrednim stosowaniem i co do zasady niemożliwe jest transponowanie regulacji rozporządzeń w postaci ustaw krajowych, to w pewnych przypadkach wymagane jest uchwalenie aktu prawa krajowego, np. w sytuacji wprowadzenia specjalnych instytucji krajowych[36]. Wspomniany wcześniej nadzór usług zaufania jest instytucją potrzebującą takiej regulacji. Każde państwo członkowskie posiada odrębną, swoją strukturę administracji publicznej, dlatego do jego kompetencji należy wybór odpowiedniego podmiotu, który sprawować będzie nadzór usług zaufania.

Podsumowanie

Reasumując, głównym celem eIDAS jest ujednolicenie rynku cyfrowego UE za pomocą ustanowienia szczegółowych przepisów oraz jednolitych standardów uwierzytelniania, w tym możliwości wzajemnego uznawania systemów identyfikacji elektronicznej. Skutkiem nowej regulacji ma być zapewnienie poczucia bezpieczeństwa i zaufania na rynku transakcji elektronicznych wśród ich użytkowników.

Ostateczna ocena celów rozporządzenia eIDAS możliwa jest dopiero po analizie instytucji w nim zawartych, a przede wszystkim po obserwacji funkcjonowania nowych mechanizmów w praktyce. Wtedy możliwe będzie stwierdzenie, czy założone i zamierzone cele zostały spełnione, czy pozostały tylko niezrealizowanymi ideami.

[32] Motyw 22. preambuły eIDAS.
[33] Motyw 30. preambuły eIDAS.
[34] Art. 22 eIDAS.
[35] Art. 16 eIDAS.
[36] *J. Barcz*, Instytucje i prawo…, s. 231.

Słowa kluczowe: identyfikacja elektroniczna, podpis elektroniczny, umowy elektroniczne, dyrektywa, rozporządzenie, transakcje elektroniczne, system identyfikacji elektronicznej, Unia Europejska (UE)

Electronic ID in EU – from directive to regulation

The intensive development of electronic communication has initiated the conclusion of electronic contracts for which secure, trustworthy and effective electronic identification mechanisms are necessary. I.e. those in which the data sent are not available to third parties and those in which the parties to the contract can be identified without difficulty, and their declarations of will bring legal effects. At this point, the need arose to create appropriate legal regulations. The first ones were created at the end of the 20th century, including Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. After many years, it turned out that the Directive, as an act of law harmonization, did not meet its main objectives, and also ceased to fit modern electronic identification solutions. That is why the European Union has set a new regulation: Regulation no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions which, as the act of harmonizing the law, is a new hope for the dissemination of electronic transactions on the territory of the European Union.

Keywords: electronic identification, electronic signature, electronic contracts, directive, regulation, electronic transactions, electronic identification system, European Union.

Zakres skuteczności regulacji art. 190a § 2 KK dla zwalczania działań sprawczych związanych z tzw. kradzieżą tożsamości w sieci Internet

dr *Piotr Siemkowicz*[1]

Celem niniejszego opracowania jest analiza art. 190a § 2 KK, a w szczególności próba odpowiedzi na pytanie, jaka jest w praktyce skuteczność przedmiotowego przepisu dla zwalczania przestępstw, które wiążą się z wcześniejszym przejęciem danych dotyczących tożsamości innej osoby za pośrednictwem sieci Internet, a następnie wykorzystania tych danych dla działań przestępczych. Autor zwraca także uwagę na przykładowe techniki, którymi posługują się przestępcy w celu wyłudzania danych osobowych bądź ich przejęcia, a także sygnalizuje potencjalne zagrożenia istniejące w sieci Internet, a wiążące się z udostępnianiem danych osobowych oraz wizerunku przez użytkowników, w tym zwłaszcza na tzw. portalach społecznościowych. W opracowaniu przedstawiono także analizę nowego zjawiska, którym jest podszywanie się przez sprawców pod tzw. wirtualne postacie funkcjonujące w ramach gier typu MMORPG. Ostatecznie w opracowaniu wskazano na postulowaną konieczność dokonania zmian legislacyjnych w zakresie regulacji czynu z art. 190a § 2 KK, które mogą przyczynić się do poprawy skuteczności tego przepisu w zakresie ścigania sprawców przestępstwa „kradzieży tożsamości".

Uwagi wstępne

Nowe zdobycze technologiczne, w tym zwłaszcza wiążące się z rozwojem sieci Internet i udogodnieniami komunikacji elektronicznej, niosą za sobą także zagrożenia, które faktycznie nie istniały u schyłku XX w. Zagrożenia te, w tym także związane z tzw. kradzieżą tożsamości, stawiają w pierwszej kolejności przed ustawodawcą, a następnie organami ścigania i sądami, nowe wyzwania. Wymaga to z jednej strony stworzenia nowych i skutecznych narzędzi legislacyjnych do zwalczania tego rodzaju przestępczości, z drugiej zaś odpowiedniego przeszkolenia prokuratorów i sędziów pozwalającego na operowanie nie tylko niezbędnym zakresem wiedzy prawniczej, ale w szczególności także technicznej i informatycznej. Dopiero bowiem połączenie warsztatu pracy prawnika z niezbędnym zakresem wiedzy informatycznej pozwala na skuteczne wykrycie, a także ocenę określonych typów działań przestępczych podejmowanych najczęściej za pośrednictwem sieci Internet, a zmierzających między innymi do wejścia w posiadanie danych dotyczących tożsamości innej osoby, a następnie wykorzystania tych danych do celów przestępczych.

Kradzieży tożsamości jako przestępstwo

Wprowadzenie ustawą z 25.2.2011 r. o zmianie ustawy Kodeks karny[2] art. 190 a § 2 KK, dotyczącego tzw. kradzieży tożsamości, który wszedł w życie 6.6.2011 r., bez wątpienia było krokiem w dobrym kierunku. Przed wprowadzeniem do Kodeksu karnego omawianej regulacji wiele zachowań o charakterze przestępczym pozostawało bowiem poza możliwością ich kryminalizacji. Przytoczyć warto w tym miejscu chociażby za *F. Radoniewiczem* opisywany przez niego przypadek założenia przez nieznaną osobę profilu na Facebooku z danymi osobowymi znanego aktora, gdzie sprawca, podszywając się pod niego, korespondował z jego znajomymi z branży artystycznej oraz dokonywał wpisów komentujących aktywność podejmowaną przez innych użytkowników, czym szkodził reputacji oraz dobremu imieniu pokrzywdzonego[3]. Jak przy tym podkreślał wskazany autor, w przedmiotowej sprawie zostało ostatecznie wydane postanowienie z 29.12.2010 r. o odmowie wszczęcia dochodzenia w przedmiocie „zmiany zapisu na informatycznym nośniku danych poprzez utworzenie na portalu społecznościowym profilu pokrzywdzonego bez jego wiedzy i zgody", tj. w zakresie czynu z art. 268 § 2 KK, z uwagi na przyjęcie, że zachowanie sprawcy nie wyczerpywało znamion czynu zabronionego, przy czym faktycznie w aktualnym stanie prawnym (po 6.6.2011 r.) mogłoby to zostać zakwalifikowane jako czyn z art. 190a § 2 KK.

Oczywiste jest przy tym, że przywłaszczenie czyjejś tożsamości przez przestępcę, zwłaszcza w ramach możliwości stwarzanych przez sieć Internet, może stać się dla pokrzywdzonego faktycznym utrapieniem, z uwagi na możliwość wykorzystania takich danych osobowych przez sprawcę w ramach innych czynów karalnych, w tym głównie z art. 212

[1] Autor jest adwokatem, specjalizującym się w sprawach karnych. W zakresie zainteresowań naukowych autor zajmuje się głównie problematyką tzw. przestępstw komputerowych, w tym popełnianych za pośrednictwem sieci Internet.

[2] Dz.U. Nr 72, poz. 381.

[3] *F. Radoniewicz*, Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016, s. 449.

§ 2 oraz z art. 286 § 1 KK. Wszak sprawca, który wszedł w nieuprawnione posiadanie czyichś danych osobowych bądź wizerunku, może, posługując się nimi, założyć „na rachunek" pokrzywdzonego fałszywe konto e-mail (rejestrując się jako pokrzywdzony), a następnie wysyłać z niego pomawiające inne osoby treści bądź też zdjęcia i filmy objęte np. normą art. 202 § 3 i 4b KK – co może spowodować wszczęcie przeciwko tej osobie postępowania karnego oraz konieczność procesowego wykazywania, iż treści te zostały faktycznie rozpowszechnione bez wiedzy pokrzywdzonego. Osoba dysponująca danymi osobowymi innej osoby może dokonywać na jej rachunek zakupów w sieciach sklepów internetowych, a często nawet zawrzeć umowę pożyczki bądź umowę kredytową – podszywając się pod dane pokrzywdzonego, zwłaszcza jeżeli weryfikacja autentyczności pożyczkodawcy lub kredytobiorcy dokonywana przez określoną instytucję finansową nie będzie odpowiednio wnikliwa. Przestępca może ostatecznie po uzyskaniu danych osobowych pokrzywdzonego założyć w oparciu o te dane fałszywy profil na portalu społecznościowym i zamieszczać w jego ramach szkalujące pokrzywdzonego bądź inne osoby informacje, a nawet założyć – podszywając się pod niego – blog internetowy w celu zamieszczenia na nim informacji naruszających np. normę art. 256 § 1 lub art. 257 KK.

Artykuł 190a § 2 KK stanowi w szczególności, iż karze pozbawienia wolności do lat trzech podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej. Z kolei art. 190a § 3 KK przewiduje formę kwalifikowaną przestępstwa „kradzieży tożsamości", zagrożoną karą pozbawienia wolności od roku do lat 10, w sytuacji gdy następstwem czynu określonego także w § 2 jest targnięcie się pokrzywdzonego na własne życie.

Ściganie przestępstwa określonego w § 2 art. 19a KK następuje przy tym na wniosek pokrzywdzonego.

Czyn z art. 190a § 2 KK jest przestępstwem formalnym – bezskutkowym, które jak słusznie zauważa się w doktrynie, zostaje dokonane w chwili, gdy sprawca przystąpił już do „robienia użytku" z danych osobowych lub wizerunku, nawet gdy szkody jeszcze nie wyrządził[4]. Przestępstwo to może zostać popełnione jedynie w zamiarze bezpośrednim kierunkowym, gdzie działanie sprawcy musi zostać podjęte w celu wyrządzenia pokrzywdzonemu konkretnej szkody materialnej lub osobistej. Tym samym do realizacji przedmiotowego przestępstwa w żadnym zakresie nie jest wystarczające działanie podjęte przez sprawcę w zamiarze ewentualnym – a więc aby sprawca jedynie godził się na wyrządzenie swoim działaniem szkody osobie, pod którą się podszywa przy wykorzystaniu jej wizerunku lub danych osobowych[5]. Podobne stanowisko wyraził także SN w wyroku z 27.1.2017 r., wskazując w tezie przedmiotowego orzeczenia, iż „przestępstwo określone w art. 190a § 2 KK może być popełnione wyłącznie w zamiarze bezpośrednim, tak więc dla realizacji jego znamion nie jest wystarczające, aby sprawca jedynie godził się na wyrządzenie swoim działaniem szkody osobie, pod którą się podszywa, wykorzystując jej wizerunek lub dane osobowe"[6].

W przypadku natomiast formy kwalifikowanej skutkiem – z art. 190a § 3 KK, jak zauważa się w doktrynie, przedmiotowy skutek w postaci targnięcia się pokrzywdzonego na własne życie niekoniecznie musi być objęty zamiarem sprawcy, natomiast musi być on obiektywnie przewidywalny, a tym samym sprawca musi co najmniej przewidywać następstwa swojego czynu[7].

Przestępstwo z art. 190a § 2 KK nie będzie możliwe do popełnienia przez zaniechanie, ponieważ użycie w nim znamienia czasownikowego „podszywać się" wymaga od sprawcy podjęcia określonego działania[8]. Stroną przedmiotową przestępstwa z art. 190a § 2 KK jest przy tym podszywanie się pod inną osobę poprzez wykorzystanie jej wizerunku lub innych jej danych osobowych w celu wyrządzenia jej szkody majątkowej lub osobistej.

Pojęcie podszywania się nie jest zdefiniowane w Kodeksie karnym. Należy więc przyjąć, że oznaczać ono będzie każdą formę wykorzystania cudzych danych osobowych lub wizerunku, która będzie stwarzała wrażenie, że użycie tych danych dokonane zostało przez ich faktycznego dysponenta, nie zaś przez osobę fikcyjnie podającą się za pokrzywdzonego. Jak słusznie zauważa przy tym *A. Lach*, zachowanie sprawcy może być bezpośrednio nakierowane na inną osobę – np. przez podanie jej danych osobowych lub też może ono oddziaływać na określone urządzenie informatyczne, weryfikujące dostęp do niego na podstawie podawanych danych[9].

Zauważyć należy, że nie zawsze „podszycie się", a więc naśladowanie danej osoby, będzie mieściło się w gestii zainteresowania prawa karnego. Jak zauważa *K. Sowirka*, samo naśladowanie kogoś, w szczególności poprzez upodobnienie się do niego strojem, wyglądem czy zachowaniem, jednakże bez zamiaru wprowadzenia w błąd innej osoby, nie będzie podlegało penalizacji na podstawie art. 190a § 2 KK[10]. Cytowany autor podaje przy tym przykłady sobowtórów oraz fanów gwiazd, którzy starają się upodobnić lub wręcz wyglądać jak ich idole, a także satyryków, parodystów i komików, którzy w ramach swojej pracy artystycznej wręcz naśladują określone osoby.

[4] *M. Filar*, [w:] *M. Filar* (red.), Kodeks Karny Komentarz, Warszawa 2016, s. 1175.

[5] *M. Królikowski*, *A. Sakowicz*, [w:] *M. Królikowski*, *R. Zawłocki* (red.), Kodeks karny część szczególna, t. I, Warszawa 2017, s. 592.

[6] V KK 347/16, Legalis.

[7] *J. Sobczak*, Wpływ internetu na zjawisko samobójstwa, [w:] *M. Mozgawa* (red.), Samobójstwo, Warszawa 2017, s. 291.

[8] *K. Sowirka*, Przestępstwo „kradzieży tożsamości" w polskim prawie karnym, IUS NOVUM 2013, Nr 1, 2013, s. 70.

[9] *A. Lach*, Kradzież tożsamości, Prokuratura i Prawo 2012, Nr 3, s. 33.

[10] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 67.

W praktyce możliwa jest również sytuacja, gdy sprawca będzie posługiwał się częściowo swoimi danymi osobowymi, częściowo zaś danymi osobowymi innej osoby – a więc np. własnym adresem i telefonem oraz imieniem i nazwiskiem innej osoby. Jak słusznie zauważa się w doktrynie, w przedmiotowej sytuacji to organ procesowy będzie musiał ocenić, czy rodzaj i zakres wykorzystanych danych osobowych pozwala na przyjęcie, iż sprawca faktycznie podszył się pod inną osobę[11].

Przestępstwo z art. 190a § 2 KK zostało przez ustawodawcę umieszczone w rozdziale XXIII Kodeksu karnego – a więc w ramach przestępstw przeciwko wolności. Umieszczenie art. 190a § 2 KK zaraz po przestępstwie stalkingu z art. 190a § 1 KK może sugerować, iż czyn z art. 190a § 2 KK jest także pewną formą przestępstwa stalkingu – co uznać należy za rozwiązanie nietrafne. W szczególności bowiem przestępstwo stalkingu z art. 190a § 1 KK wymaga dla jego realizacji „uporczywości nękania", a więc powtarzających się działań sprawcy w określonym okresie, podczas gdy czyn z art. 190a § 2 KK może być zrealizowany nawet przez jednorazowe podszycie się sprawcy pod inną osobę – poprzez wykorzystanie jej wizerunku lub innych jej danych osobowych, pod warunkiem że działanie to wiąże się z zamiarem sprawcy wyrządzenia tej osobie szkody majątkowej lub osobistej.

W doktrynie wysuwane były także uprzednio – między innymi z uwagi na wskazaną powyżej odmienność czynu z art. 190a § 2 KK od tzw. przestępstwa stalkingu opisanego w art. 190a § 1 KK – postulaty w zakresie umieszczenia czynu typizowanego w art. 190a § 2 KK w innym rozdziale Kodeksu karnego, w tym jako samodzielne (niepowiązane ze stalkingiem) przestępstwo. W szczególności *A. Lach* opowiadał się za umieszczeniem przestępstwa „kradzieży tożsamości" w rozdziale XXVII Kodeksu karnego, zawierającego przestępstwa przeciwko czci i nietykalności cielesnej[12], natomiast *K. Sowirka*, postulując zaliczenie przedmiotowego przestępstwa z art. 190a § 2 KK do przestępstw przeciwko ochronie informacji bądź do przestępstw przeciwko czci i nietykalności cielesnej, także opowiadał się za przeniesieniem przestępstwa opisanego w art. 190a § 2 KK do odrębnego artykułu w kodeksie, bez formalnego związania tego czynu ze stalkingiem[13]. Postulaty obu cytowanych autorów w pełni należy przy tym zaaprobować jako podkreślające odmienność czynu z art. 190a § 2 KK „kradzieży tożsamości" od przestępstwa stalkingu z art. 190a § 1 KK.

Wizerunek jako dobro osobiste

Pojęcie wizerunku osoby zostało uregulowane w ramach art. 23 KC dotyczącego ochrony dóbr osobistych. Przepis ten stanowi zwłaszcza, że dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Dodatkowo art. 81 ust. 1 ustawy z 4.2.1994 r. o prawie autorskim i prawach pokrewnych[14] wskazuje, iż rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie. Zgodnie natomiast z treścią art. 81 ust 2 PrAutU zezwolenia nie wymaga rozpowszechnianie wizerunku:

1) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
2) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Jak podkreśla się także w doktrynie, pojęciu wizerunku osoby nadaje się dwa znaczenia: wąskie – związane z przedmiotem, na którym istnieje fizyczne utrwalenie wyglądu danej osoby, oraz szerokie – a więc w rozumieniu wytworu niematerialnego, który za pomocą środków plastycznych przedstawia rozpoznawalną podobiznę danej osoby, zawierając zarazem istotną wartość identyfikacyjną poszczególnych elementów takich jak kolor oczu, stale noszone okulary, fryzura, makijaż, ubiór, a nawet sposób poruszania się, zachowania czy też gestykulacji, jeśli w oderwaniu lub w łączności z innymi cechami są one dla tej osoby charakterystyczne[15].

Wizerunkiem osoby w rozumieniu art. 190a § 2 KK będzie przy tym – jak się wydaje – jedynie przedstawienie bądź też wyobrażenie określonej osoby fizycznej w postaci graficznej, a więc w postaci zdjęcia, rysunku, karykatury, w tym także we wszelkich formach przetworzonych w systemie elektronicznym. Niezbędnym wymogiem będzie jednak każdorazowo możliwość powiązania takiego wizerunku z określoną osobą fizyczną, pozwalającego na jej identyfikację.

Z uwagi na znamię czasownikowe „wykorzystania przez sprawcę wizerunku" osoby, poza zakresem kryminalizacji art. 190a § 2 KK, pozostaną zatem wszelkie inne formy posługiwania się wizerunkiem innej osoby, nieposiadającym jednak swojego wyznacznika w formie graficznej – a więc np. poprzez jedynie słowne przedstawienie tzw. wizerunku publicznego, politycznego, artystycznego związanego ze sposobem postrzegania określonej osoby przez społeczeństwo jako człowieka, polityka, naukowca itp. Oczywiste jest jednak, że posłużenie się opisem danej osoby w formie niegraficznej (opisem słownym) może skutkować realizacją przez sprawcę

[11] *A. Lach*, Kradzież tożsamości…, s. 34.
[12] *Ibidem*, s. 32.
[13] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 65–66 oraz s. 78.
[14] T.j. Dz.U. z 2017 r. poz. 880 ze zm.; dalej jako: PrAutU.
[15] *J. Barta*, *R Markiewicz*, [w:] *J. Barta, M. Czajkowska-Dąbrowska*, *Z. Ćwiąkalski*, *R. Markiewicz*, *E. Traple*, Prawo autorskie i prawa pokrewne. Komentarz, Kraków 2005, s. 626.

innego czynu karalnego, w szczególności czynu z art. 212 § 1 KK – a więc przestępstwa zniesławienia, jeżeli dodatkowo ze słownym opisem „wizerunku" danej osoby połączone będzie pomówienie jej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności. W sytuacji gdy sprawca przedstawi w sposób pejoratywny, a tym samym zniesławiający słowny opis „wizerunku" danej osoby za pośrednictwem środków masowego komunikowania się, zamieszczając taki opis np. na stronie internetowej lub też w ramach komunikatora społecznościowego, może zrealizować on swoim działaniem dyspozycję art. 212 § 2 KK.

Dane osobowe a tożsamość osoby fizycznej

Pojęcie danych osobowych uregulowane jest w art. 6 ust. 1 ustawy z 29.8.1997 r. o ochronie danych osobowych[16]. Przepis ten stanowi, iż w rozumieniu ustawy za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dodatkowo art. 6 ust. 2 OchrDanychU wskazuje, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Równocześnie art. 6 ust. 3 OchrDanychU stanowi, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.

Tym samym za dane osobowe w rozumieniu ustawy o ochronie danych osobowych należy uznać w szczególności adres zamieszkania, imiona i nazwiska rodziców, numer PESEL i NIP, linie papilarne, wzór siatkówki oka, a także wiele informacji dotyczących danej osoby, takich jak wykształcenie, stan cywilny, wykonywany zawód, pełnione funkcje[17]. Należy zgodzić się także z *A. Lachem*, iż imię i nazwisko danej osoby będą stanowić dane osobowe jedynie wówczas, gdy samodzielnie umożliwią identyfikację danej osoby lub też umożliwią tę identyfikację w powiązaniu z innymi informacjami[18]. Cytowany autor słusznie bowiem zauważa, że w sytuacji gdy sprawca posłuży się popularnym i często występującym imieniem i nazwiskiem (np. *Jan Kowalski*), same te dane nie będą jeszcze pozwalały na identyfikację konkretnej osoby.

Danymi osobowymi w rozumieniu ustawy o ochronie danych osobowych mogą być także adresy e-mail, adresy stron WWW bądź też loginy do określonych portali lub też usług internetowych, w sytuacji gdy samoistnie lub też w połączeniu z innymi informacjami pozwolą na zidentyfikowanie danej osoby, a więc w szczególności gdy w swojej treści zawierają imię i nazwisko użytkownika[19].

Z pojęciem danych osobowych nierozerwalnie jest związane także pojęcie tożsamości osoby ludzkiej. Tożsamość związana jest przy tym z tzw. pojęciem identyczności – oraz oznacza bycie tym samym w znaczeniu ciągłości, a także świadomość siebie oraz własnej odrębności[20]. Na pojęcie tożsamości w jej ujęciu prawnym składają się przy tym dane określające osobę, a więc jej dane osobowe, pseudonimy oraz inne dane, które bądź samodzielnie użyte, bądź też w połączeniu z innymi danymi pozwalają na jej identyfikację[21].

W ramach sieci Internet tożsamość może być przy tym postrzegana jako tożsamość rzeczywista – będąca odzwierciedleniem wszystkich danych danej osoby w świecie realnym, jako tożsamość fikcyjna – tzw. pseudonim lub nick używane w ramach czatów lub grup dyskusyjnych oraz jako tożsamość anonimowa[22]. Jak zauważa przy tym *A. Lach*, każda osoba może dysponować kilkoma tożsamościami, w tym jedną rzeczywistą i kilkoma fikcyjnymi lub anonimowymi, które tworzone są dla różnych obszarów aktywności życiowej[23].

W tym miejscu należy wskazać, że w ramach sieci Internet przetwarzane są oraz gromadzone na określonych serwerach, portalach społecznościowych, portalach sklepów internetowych, stronach WWW, w ogólnie dostępnych bazach danych, a nawet w ramach komunikatorów internetowych, ogromne ilości danych, w tym także bezpośrednio danych osobowych pozwalających na prostą identyfikację osoby, jak też danych dotyczących wizerunku osób fizycznych. Część danych osobowych i wizerunków osoby udostępniana jest dobrowolnie przez użytkowników w ramach powszechnie dostępnych usług Web 2.0 oraz wpisów na portalach społecznościowych takich jak Facebook, Twitter, nk.pl itp. Dane osobowe, takie jak imię i nazwisko właściciela firmy, a także NIP i adres prowadzonej działalności gospodarczej (często tożsamy z miejscem zamieszkania), a także numer telefonu i adres e-mail, zamieszczane są oficjalnie na stronach internetowych administrowanych przez instytucje państwowe lub publiczne, takich jak np. CEIDG. Numer PESEL każdej osoby będącej właścicielem nieruchomości odnaleźć możemy także oficjalnie w ramach ogólnie dostępnej elektronicznej bazy Ksiąg Wieczystych. Faktycznie więc uznać należy, że

[16] T.j. Dz.U. z 2016 r. poz. 922 ze zm.; dalej jako: OchrDanychU.
[17] *A. Lach*, Kradzież tożsamości…, s. 35.
[18] *Ibidem*, s. 35.
[19] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 70.
[20] *A. Lach*, Karnoprawna reakcja na zjawisko kradzieży tożsamości, Warszawa 2015, s. 1–16.
[21] *M. Romańczuk-Grącka*, Prawnokarna ochrona tożsamości elektronicznej w perspektywie przeciwdziałania nielegalnym rynkom finansowym, [w:] *W. Pływaczewski* (red.), Przeciwdziałanie patologiom na rynkach finansowych. Od edukacji ekonomicznej po prawnokarne środki oddziaływania, Warszawa 2015, s. 238.
[22] *A. Lach*, Karnoprawna reakcja…, s. 18.
[23] *Ibidem*, s. 19.

wejście w posiadanie danych osobowych określonej osoby fizycznej za pośrednictwem sieci Internet, w tym nawet za pośrednictwem wyszukiwarek internetowych, nie stanowi żadnego problemu.

Jak słusznie zauważa *T. Trejderowski*[24], w sytuacji znajomości jedynie imienia i nazwiska pokrzywdzonego i ewentualnie nazwy miasta, w którym zamieszkuje, potencjalny sprawca może uzyskać na portalu społecznościowym następujące dane dotyczące tej osoby:

- zobaczyć jej zdjęcia oraz zdjęcia jej rodziny i znajomych;
- poznać wiek, a także przybliżoną datę urodzenia;
- poznać jej znajomych, przyjaciół i kolegów z pracy oraz członków rodziny;
- uzyskać dane dotyczące tej osoby – czym się aktualnie zajmuje, gdzie pracuje lub studiuje;
- poznać przebieg jej edukacji, w tym ukończone szkoły, uczelnie oraz odbyte kursy;
- poznać numer Gadu-Gadu, Skype'a oraz telefonu;
- poznać stan cywilny na podstawie analizy nazwiska, fotografii lub porównując nazwiska znajomych;
- poprzez analizę fotografii i listy znajomych dowiedzieć się, czy dana osoba posiada dzieci, ich liczbę oraz poznać ich płeć i oszacować wiek;
- w przypadku publikacji zdjęć ze ślubu – ustalić, gdzie dana para miała uroczystość weselną;
- poprzez szczegółowe porównanie nazwisk na liście znajomych można ustalić powiązania rodzinne, w tym rodzeństwo, kuzynów, bliższych i dalszych krewnych oraz powinowatych;
- porównując szkoły i uczelnie, w których uczy się dana osoba razem ze swoimi znajomi, poznać jej znajomych z konkretnych szkół i uczelni;
- poprzez analizę podpisów pod fotografiami oraz komentarze do nich i do profilu można poznać wiele szczegółów z życia prywatnego danej osoby, a więc gdzie spędzała wakacje, w jakich klubach się bawi, jak spędza wolny czas, jakie ma hobby itp.;
- poprzez analizę dat i godzin dodawania kolejnych zdjęć lub udzielania odpowiedzi na komentarze, ustalić, w jakich porach dana osoba korzysta z Internetu, a także czy ma do niego dostęp w pracy.

Cytowany autor zwraca również uwagę, że poprzez tzw. mechanizm „like" – a więc zaznaczanie jako „lubię to" określonych wpisów czy też zdjęć np. na Facebooku, potencjalny sprawca może z łatwością ustalić, co dana osoba lubi, jakie są jej zainteresowania i poglądy[25].

Nie może jednak budzić wątpliwości, że w zakresie wskazanym powyżej na ujawnienie swojej tożsamości w sposób bezpośredni lub też co najmniej dorozumiany, a tym samym na wejście w posiadanie danych zamieszczanych na publicznych portalach – zwłaszcza o charakterze społecznościowym, wyraża zgodę sam użytkownik. Tym samym powinien on przynajmniej godzić się z tym, że inne osoby dane te poznają. W przedmiotowym wypadku potencjalny pokrzywdzony wyzbywa się niejako przysługującego mu prawa do prywatności. Poza dyskusją pozostaje ocena takiego zachowania, które bez wątpienia może narazić potencjalnego pokrzywdzonego na daleko idące i negatywne dla niego konsekwencje, także w sferze wiktymologicznej, a więc tzw. podatności na stanie się ofiarą przestępstwa. Nie ulega bowiem wątpliwości, że poza możliwością przejęcia danych osobowych takiej osoby przez potencjalnego sprawcę przestępstwa z art. 190 a § 2 KK, tego rodzaju aktywność w sferze portali społecznościowych narazić może ich użytkownika na inne niebezpieczeństwa, w tym np. na potencjalne dokonanie na jego szkodę przestępstwa z art. 279 § 1 KK, a więc kradzieży z włamaniem do jego mieszkania, w sytuacji gdy zamieści na portalu społecznościowym informację, że we wskazanym okresie przebywać będzie z całą rodziną na zaplanowanym urlopie, poza miejscem swojego zamieszkania.

Oczywistym jest także, że zdobycie przez sprawcę określonej kategorii danych osobowych innej osoby, w tym w szczególności numeru PESEL, imion rodziców i panieńskiego nazwiska matki, może umożliwić sprawcy – o czym wspomniano powyżej, popełnianie innych przestępstw bezpośrednio na szkodę osoby, której dane osobowe uzyskał, lub też na szkodę innych pokrzywdzonych, w tym w szczególności przestępstwa oszustwa z art. 286 § 1 KK, gdzie sprawca, podając się za inną osobę, może uzyskać od określonej instytucji finansowej pożyczkę kredytową lub też np. dokonać zakupów za pośrednictwem sklepu internetowego. Zauważyć także należy, iż w ramach sieci Internet weryfikacja danych osobowych następuje bez osobistego kontaktu pomiędzy osobą podającą określone dane osobowe a osobą dane te weryfikującą[26]. W ramach interakcji pomiędzy użytkownikiem – klientem a podmiotem świadczącym określone usługi w sieci Internet tożsamość danej osoby najczęściej weryfikowana jest także przy użyciu takich danych, jak login i hasło lub też token czy karta dostępu[27]. Także w przypadku dokonywania transakcji kartami płatniczymi za pośrednictwem sieci Internet brak jest możliwości faktycznej weryfikacji tego, czy osoba podająca dane niezbędne do transakcji jest faktycznym właścicielem karty płatniczej, a także czy kartą tą rzeczywiście dysponuje, czy też weszła jedynie w posiadanie numeru tej karty i danych osobowych osoby, na którą kartę wystawiono. Brak jest bowiem w tym wypadku fizycznej obecności karty płatniczej w punkcie akceptanta w chwili dokonywania

[24] *T. Trejderowski*, Kradzież tożsamości. Terroryzm informatyczny, cyberprzestępstwa, internet, telefon, Facebook, Warszawa 2013, s. 148–150.
[25] *Ibidem*, s. 151.
[26] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 65.
[27] *A. Lach*, Kradzież tożsamości…, s. 29–30.

transakcji, a także nie dochodzi do bezpośredniego kontaktu sprzedającego z kupującym[28].

Wykorzystanie cudzego wizerunku i danych osobowych a przestępstwo z art. 190a § 2 KK

Nie można także nie zauważyć, że w ramach portali społecznościowych mogą być często tworzone fałszywe konta – dotyczące faktycznie nieistniejących w rzeczywistości osób, gdzie poprzez zaproszenie potencjalnego pokrzywdzonego do tzw. grona znajomych, a następnie dokonywanie przez niego określonych wpisów, dochodzi do zbierania informacji o tej osobie, w tym także bezpośrednio w zakresie danych osobowych[29].

Czyn z art. 190a § 2 KK, w brzmieniu nadanym mu przez ustawodawcę, pozwala faktycznie na ściganie jedynie tych sprawców, którzy podszywając się pod inną osobę oraz wykorzystując w tym celu jej wizerunek lub inne dane osobowe, działają w celu wyrządzenia jej szkody majątkowej lub osobistej. Oznacza to, iż poza zainteresowaniem art. 190a § 2 KK pozostają wszelkie te działania potencjalnych sprawców, które nie są nakierowane na wyrządzenie szkody majątkowej lub osobistej.

Wobec powyższego samo pozyskiwanie i gromadzenie czyichś danych osobowych za pośrednictwem sieci Internet bądź też wizerunków danej osoby fizycznej, w sytuacji gdy sprawca dopiero w przyszłości zamierza przy ich pomocy podszywać się pod tę osobę w celu wyrządzenia jej szkody majątkowej lub osobistej, nie podlega faktycznie penalizacji w ramach czynu z art. 190a § 2 KK. Działanie takie pozostaje więc bezkarne, a to z uwagi na to, iż ustawodawca przy nowelizacji z 25.2.2011 r. nie włączył do Kodeksu karnego przepisu penalizującego także formę stadialną przestępstwa „kradzieży tożsamości" – a więc przygotowania do czynu z art. 190a § 2 KK[30]. Bez wątpienia natomiast już samo gromadzenie danych osobowych określonej osoby fizycznej lub też ściąganie i zapisywanie np. na twardym dysku komputera ewentualnego przyszłego sprawcy wizerunków takiej osoby, w sytuacji gdy czyni on to w celu popełnienia dopiero w przyszłości czynu zabronionego związanego z wyrządzeniem danej osobie przy użyciu tych danych szkody majątkowej lub osobistej, wypełnia dyspozycję art. 16 § 1 KK – a więc przygotowania do realizacji przestępstwa z art. 190a § 2 KK. *De lege ferenda* należałoby się więc zastanowić, czy przy najbliższej nowelizacji Kodeksu karnego nie byłoby pożądanym zabiegiem legislacyjnym także penalizowanie samego przygotowania do czynu z art. 190a § 2 KK.

Nie można przy tym tracić z pola widzenia, że nie zawsze sprawca zbierający dane osobowe określonej osoby lub osób będzie czynił to w celu wyrządzenia jej bezpośrednio szkody majątkowej lub osobistej, pomimo iż jego działania związane z gromadzeniem tych danych będą faktycznie nastawione na uzyskanie korzyści majątkowej. Dane osobowe stanowią bowiem aktualnie często przedmiot obrotu handlowego, a sprawca może je gromadzić w celu np. odsprzedaży określonemu podmiotowi[31].

Zauważyć przy tym należy, że poza faktyczną penalizacją czynu z art. 190a § 2 KK, z uwagi na brak karalności przygotowania do tego przestępstwa, pozostają także te działania sprawcy, które za pośrednictwem określonych metod socjotechnicznych bezpośrednio zmierzają do uzyskania danych osobowych danej osoby, w sytuacji gdy nie realizują one zarazem znamion czynu z art. 267 § 1 KK. Wskazany przepis stanowi bowiem, że odpowiedzialności karnej za przestępstwo z art. 267 § 1 KK podlega ten, kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Tym samym, jeżeli sprawca uzyska takie dane osobowe pokrzywdzonego, jednakże bez otwierania zamkniętej korespondencji bądź bez podłączenia się w tym celu do sieci telekomunikacyjnej lub też bez przełamania czy też ominięcia elektronicznych, magnetycznych, informatycznych lub innych szczególnych jej zabezpieczeń, nie będzie ponosił w tym zakresie zazwyczaj odpowiedzialności karnej, w szczególności gdy następnie tymi danymi osobowymi nie posłuży się w celu podszywania się pod inną osobę, a zarazem wyrządzenia jej w ten sposób szkody majątkowej lub osobistej.

Poza zainteresowaniem art. 190a § 2 KK pozostaje także posłużenie się przez sprawcę danymi osobowymi lub wizerunkiem osoby zmarłej, co jest związane z brakiem możliwości zidentyfikowania jako osoby fizycznej człowieka po jego śmierci[32]. Jak podkreśla się bowiem w doktrynie, kult i pamięć o osobie zmarłej jest jednym z dóbr osobistych człowieka, które po jego śmierci przysługują rodzinie zmarłego, co daje podstawę w przypadku naruszenia tych dóbr dochodzenia ochrony cywilnoprawnej[33].

Przestępstwo z art. 190a § 2 KK nie może zostać także zrealizowane w sytuacji, gdy sprawca posłuży się fikcyjnymi danymi osobowymi lub fikcyjnym wizerunkiem nieistniejącej osoby. Oczywiście działania takie mogą natomiast nosić znamiona czynu z art. 286 § 1 KK, w sytuacji gdy sprawca

[28] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce, Warszawa 2012, s. 401.

[29] *E. Całus*, Przestępstwo kradzieży tożsamości w Internecie – uwagi na tle art. 190a § 2 KK, [w:] *M. Gdula* (red.), Ochrona prywatności w nowych technologiach, Wrocław 2015, s. 5.

[30] *A. Lach*, Karnoprawna reakcja..., s. 99.

[31] *M. Siwicki*, Kradzież tożsamości – pojęcie i charakterystyka zjawiska, Część I, Edukacja Prawnicza 2009, Nr 11, s. 36.

[32] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 68.

[33] *Ibidem*, s. 68.

wprowadzi w błąd, posługując się takimi fikcyjnymi danymi osobowymi, inną osobę oraz doprowadzi ją do niekorzystnego rozporządzenia swoim mieniem[34].

W literaturze przedmiotu oraz w literaturze informatycznej opisywane są przy tym liczne metody działań sprawców, zmierzające do uzyskania dostępu do danych osobowych określonych osób fizycznych, w tym także do tzw. danych wrażliwych – pozwalających następnie na dokonywanie określonych przestępstw, w tym z art. 190a § 2 KK czy też z art. 286 § 1 KK – a więc przestępstw oszustwa. Poza oczywistymi i prostymi metodami pozyskiwania cudzych danych osobowych, takimi jak przeglądanie wyrzuconych – bez wcześniejszego ich zniszczenia dokumentów, w tym faktur czy też listów przewozowych, jedną z częściej spotykanych metod wyłudzania danych osobowych jest tzw. *phishing*. Działanie to sprowadza się zazwyczaj do wysyłania wiadomości e-mail na pocztę użytkownika spreparowanych w taki sposób, aby stwarzały one wrażenie, iż pochodzą z określonej instytucji, np. banku lub urzędu (ZUS, Urząd Skarbowy itp.)[35]. Wiadomość ta sugeruje także zazwyczaj wystąpienie określonego problemu technicznego, który wymaga zweryfikowania przez użytkownika na wskazanej stronie internetowej danych osobowych, a także loginów i haseł dostępu. Zazwyczaj także, jak zauważa *E. Całus*, wiadomość taka posiada wpisany w jej treść link, o skorzystanie z którego proszony jest użytkownik w celu przekierowania np. na stronę banku, przy czym w przypadku kliknięcia we wskazany link użytkownik przekierowywany jest na fałszywą stronę internetową – do złudzenia przypominającą stronę określonego banku lub instytucji, gdzie pojawia się miejsce do wpisania danych uwierzytelniających, takich jak login, hasło, PIN, bądź też danych uwierzytelniających transakcję w postaci kodów jednorazowych[36].

Jak słusznie podkreśla się przy tym w doktrynie, opisywane powyżej działanie sprawcy mające postać *phisingu*, a polegające na wysyłaniu e-maili pochodzących rzekomo od innej osoby bądź instytucji (banku, podmiotu świadczącego usługi internetowe), z prośbą o podanie danych osobowych przez odbiorcę, nie będzie karalne[37]. W szczególności bowiem obecnie czynności mające na celu uzyskanie takich danych osobowych w celu wyrządzenia później szkody odbiorcy można potraktować jedynie jako formę niekaralnego przygotowania[38].

Aktualnie inną, a zarazem trudniejszą do wykrycia techniką zmierzającą także do przejęcia danych osobowych, w tym loginów i haseł dostępu, jest tzw. *pharming*, stanowiący pewną modyfikację *phisingu*, który polega na przekierowaniu użytkownika z autentycznej strony WWW określonej instytucji na stronę stworzoną przez przestępców[39].

Pharming jest poprzedzony przy tym zazwyczaj wcześniejszym złamaniem przez sprawcę zabezpieczeń określonego serwera DSN, np. banku, oraz zmianą adresów na tym serwerze, co powoduje, że użytkownik po wejściu na prawdziwą stronę WWW jest następnie przekierowywany na inną podszywającą się pod nią stronę stworzoną przez hackera, gdzie dochodzi do przejęcia wpisywanych danych osobowych, a także np. loginów, haseł, numerów kart kredytowych czy też kodów jednorazowych do operacji bankowych[40]. *Pharming* może także przybierać inną formę – sprawca infekuje najpierw komputer ofiary wirusem komputerowym lub innym złośliwym oprogramowaniem, po czym wskazany wirus lub program przekierowuje pokrzywdzonego ze strony autentycznej np. banku lub sklepu internetowego na fałszywą stronę WWW, która wygląda identycznie jak strona, którą pokrzywdzony zamierzał otworzyć[41].

W praktyce dane osobowe mogą być uzyskiwane przez potencjalnych sprawców przestępstwa z art. 190a § 2 KK, także poprzez stosowanie innych metod socjotechnicznych, w tym poprzez zwykły kontakt telefoniczny – po uzyskaniu numeru telefonu potencjalnego pokrzywdzonego np. z bazy CEIDG, gdzie poprzez fałszywe podanie się np. za operatora sieci telefonicznej w celu przedstawienia fikcyjnej oferty rozmówca przeprowadzi rzekomą weryfikację abonenta i poprosi go o podanie danych osobowych takich jak imię, nazwisko, adres zamieszkania, numer PESEL, imiona rodziców bądź panieńskiego nazwiska matki. Przedmiotowe techniki działania sprawców, związane z telefonicznym wyłudzaniem danych osobowych oraz numerów kart płatniczych, często są określane mianem *phone phisingu* bądź też *vishingu*[42].

Zauważyć przy tym należy, że numer PESEL i panieńskie nazwisko matki, jako dane zwyczajowo ujawniane jedynie w niektórych dokumentach, są często podstawą weryfikacji tożsamości danej osoby w kontakcie z autentycznymi operatorami telefonii, dostawcami Internetu czy też w telefonicznych kontaktach z bankami lub instytucjami finansowymi. W przypadku zatem wejścia w posiadanie takich danych osobowych przez potencjalnego sprawcę istnieje obawa, iż może on, wykorzystując wskazane dane ofiary, przejść następnie pomyślnie telefoniczną weryfikację np. w określonym banku, co do którego posiada informację, iż pokrzywdzony posiada tam rachunek bankowy. Oczywiste jest także, że dane dotyczące rachunku bankowego pokrzywdzonego często bez trudu można uzyskać w sieci Internet, np. poprzez analizę strony WWW związanej z działalnością gospodarczą prowadzoną przez pokrzywdzonego.

[34] *K. Chałubińska-Jentkiewicz*, *M. Karpiuk*, Prawo nowych technologii. Wybrane zagadnienia, Warszawa 2015, s. 382.
[35] *M. Romańczuk-Grącka*, Prawnokarna ochrona…s. 246–247.
[36] *E. Całus*, Przestępstwo kradzieży..., s 5–6.
[37] *A. Lach*, Kradzież tożsamości…, s. 37.
[38] *Ibidem*, s. 37.
[39] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce…, s. 402–403.
[40] *M. Ziarek* (analityk, Kaspersky Lab Polska), Phising, pharming i sieci zombie – to czego nie wiesz o swoim komputerze, https://www.securelist.pl/threats/5883,phishing_pharming_i_sieci_zombie_to_czego_nie_wiesz_o_swoim_komputerze.html (dostęp z 11.3.2018 r.).
[41] https://www.avast.com/pl-pl/c-pharming (dostęp z 11.3.2018 r.).
[42] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce…, s. 402.

Kolejnymi metodami socjotechnicznymi opisywanymi przez *E. Całus* jest tzw. oszustwo nagrodowe oraz oszustwo rekrutacyjne[43]. W pierwszym wypadku sprawca informuje potencjalną ofiarę w wiadomości e-mail lub też telefonicznie o określonej wygranej, prosząc zarazem o podanie danych osobowych „niezbędnych do odebrania nagrody", co często wiąże się z ujawnieniem wskazanych danych osobowych przez pokrzywdzonego. W drugim wypadku opisywanym przez cytowaną wyżej autorkę sprawca przesyła do pokrzywdzonego wiadomość e-mail zawierającą informację o fikcyjnej ofercie zatrudnienia. W ramach takiej oferty, jak zauważa autorka, sprawca często zwraca się również o nadesłanie CV oraz skanu dowodu osobistego pokrzywdzonego, przy czym w rzeczywistości rzekoma firma mająca zatrudnić pokrzywdzonego nie istnieje.

Do uzyskania danych osobowych pokrzywdzonego dojść może także poprzez fizyczny kontakt sprawcy z pozostawionymi w biurze ofiary dokumentami, fakturami lub poprzez wgląd do niezabezpieczonego komputera w miejscu pracy – do którego sprawca uzyskuje dostęp z uwagi na zatrudnienie w tym samym miejscu lub z uwagi na wykonywanie tam doraźnych czynności np. serwisanta, pracownika ochrony lub pracownika personelu sprzątającego. Do przejęcia danych osobowych przez potencjalnego sprawcę czynu z art. 190a § 2 KK dojść może także poprzez uzyskanie dostępu do dokumentów poszkodowanego, np. w sytuacji zagubienia przez niego dowodu osobistego.

Zauważyć przy tym należy, że w ramach sieci Internet użytkownicy często przyporządkowują do siebie określone „wirtualne postacie", tworzone na potrzeby np. gier sieciowych (online), gdzie dany użytkownik funkcjonuje jako określona postać graficzna (avatar), z którą często się utożsamia. Gry takie zaliczane są do kategorii gier MMORPG, przy czym użytkownik po uzyskaniu najczęściej darmowego konta na serwerze dostawcy usługi w postaci przedmiotowej gry online – co wymaga zazwyczaj podania podstawowych danych osobowych (imię, nazwisko, data urodzenia, państwo i miasto użytkownika, adres e-mail), uzyskuje login i hasło dostępowe do konta, a zazwyczaj także dodatkowo kod dla odzyskania utraconego konta „Recovery Key". Po uzyskaniu dostępu do konta użytkownik wciela się w określoną postać wirtualną, np. rycerza, trolla, czarnoksiężnika itp., a także jako wskazana postać wirtualna uczestniczy w przedmiotowej grze, do której dostęp posiada faktycznie nieograniczona liczba użytkowników występujących w niej pod postacią innych fikcyjnych, wirtualnych avatarów. Każda postać w miarę czasu trwania gry uzyskuje określone sprawności i atrybuty związane z poziomem gry, na którym się znajduje, a także zdobywa wirtualną walutę, uzyskiwaną za wygrane pojedynki w postaci np. wirtualnych złotych monet lub brylantów. Zarówno za wirtualną walutę uzyskaną w trakcie gry, jak i często za realne płatności dokonywane najczęściej za pośrednictwem karty płatniczej, użytkownik może także nabywać od administratora gry dodatkowe wirtualne przedmioty i artefakty, takie jak np. miecze, topory, tarcze, części zbroi, które w określony sposób wzmacniają jego postać oraz dostarczają jej nowych „mocy". Tym samym po odpowiednio długim okresie uczestniczenia w grze oraz po uzyskaniu lub zakupieniu określonych atrybutów wirtualnej postaci staje się ona faktycznie „niezwyciężona", w tym w szczególności dla nowych użytkowników, dopiero rozpoczynających grę, których wirtualne avatary nie są jeszcze odpowiednio „silne". Przedmiotowa „wirtualna postać" – avatar uzyskuje zatem z biegiem czasu określoną wartość, przekładającą się na wartość pieniężną. Użytkownicy przedmiotowych gier często także odsprzedają następnie określone atrybuty swojego avatara, np. w postaci części uzbrojenia, na aukcjach internetowych innym użytkownikom. W sieci znane jest również zjawisko tzw. *pushingu* sprowadzające się do odsprzedaży przez jednego użytkownika innemu pełnej wirtualnej postaci wraz z kontem, do którego ta postać jest przypisana, bądź też np. przelania określonej ilości wirtualnej waluty na nowo utworzone konto przez użytkownika, co pozwala mu już na wstępie gry nabyć od administratora określoną ilość atrybutów wzmacniających jego avatara. Zauważyć także należy, że zjawisko to jest najczęściej nielegalne, z uwagi na zakaz tego rodzaju działań dokonywanych przez użytkowników, wpisany w treść większości regulaminów administratorów gier gatunku MMORPG.

Zbliżony charakter może mieć również tzw. zjawisko *cheatingu* będącego formą oszustwa w grze typu MMORPG, sprowadzającego się najczęściej do nieuprawnionego (wbrew woli operatora) kopiowania wirtualnych przedmiotów oraz waluty używanej w grze[44].

Także tego typu „wirtualne postacie" stały się od pewnego czasu przedmiotem zainteresowania przestępców, którzy uzyskując różnymi metodami dane do konta innego użytkownika (login, hasło), a często także jego dane osobowe, przejmują kontrolę nad jego kontem i tym samym avatarem. W następstwie tego może dojść bądź do zniszczenia wirtualnej postaci, którą dysponował pokrzywdzony użytkownik, bądź też do przeniesienia jej na inne konto, innego użytkownika lub też odsprzedaży wirtualnej postaci oraz przypisanych do niej atrybutów i wirtualnej waluty zgromadzonych na koncie pokrzywdzonego, za co sprawca uzyskuje wymierne korzyści finansowe od nabywcy. W przypadku przejęcia „wirtualnej postaci" przez sprawcę, który następnie nadal z niej korzysta, dochodzi przy tym faktycznie do pewnej formy „podszycia się" pod poprzedniego użyt-

[43] *E. Całus*, Przestępstwo kradzieży…, s. 5–6.

[44] *K. Gienas*, Prawo autorskie w ramach „wirtualnych światów", CBKE e-BIULETYN 2007, Nr 4, http://www.bibliotekacyfrowa.pl/Content/22502/Prawo_autorskie_w_ramach.pdf (dostęp z 14.3.2018 r.).

kownika, który dotychczas dysponował tą postacią, a więc stanowiła ona jego avatar.

Do przejęcia kont użytkowników gier MMORPG oraz przypisanych do nich wirtualnych postaci dochodzi przy tym najczęściej za pomocą tych samych metod, które wykorzystują sprawcy przestępstwa z art. 190a § 2 KK. Metodą tą może być zatem *phising*, gdzie sprawca w wiadomości e-mail przesłanej do użytkownika podaje się za administratora gry i prosi o weryfikację danych tego użytkownika oraz hasła dostępu i loginu do konta. Sprawca może posłużyć się także dla zdobycia wskazanych danych dostępu do konta użytkownika metodą hackingu, poprzez zainfekowanie komputera użytkownika koniem trojańskim, najczęściej poprzez otworzenie przez takiego użytkownika załącznika w wiadomości e-mail w tym celu do niego przesłanej. Przedmiotowe zagrożenie, związane z infekowaniem koniem trojańskim komputerów użytkowników gier MMORPG w celu wykradania haseł i loginów dostępowych do ich kont, określane jest mianem zagrożenia Win32/PSW.OnLineGames, przy czym po zainstalowaniu przedmiotowego konia trojańskiego na komputerze użytkownika działa on jak typowy keylogger rejestrujący wszystkie znaki, które użytkownik wprowadza podczas logowania się do gry[45].

Opisywane są przy tym przypadki faktycznego przejęcia konta użytkownika gier typu MMORPG w celu uzyskania kontroli nad „wirtualną postacią". W szczególności warto odwołać się do zdarzenia mającego swój finał sądowy, gdy 20-letni mieszkaniec Płocka sprzedał mieszkańcowi Warszawy wirtualną postać rycerza z gry Tibia na aukcji internetowej za kwotę kilkuset złotych, po czym po pewnym czasie postanowił odzyskać swoją wirtualną postać oraz po zdobyciu kodów dostępu ponownie przejął kontrolę nad kontem, do którego przypisany był sprzedany przez niego rycerz, a także usunął go w tym celu z konta nabywcy[46]. Ostatecznie sprawa zakończyła się wyrokiem skazującym, gdzie sprawca dobrowolnie poddał się karze pięciu miesięcy pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres trzech lat próby i karze grzywny, przy czym sąd zobowiązał go dodatkowo do zwrotu wirtualnej postaci pokrzywdzonemu oraz do zwrotu pieniędzy, które uprzednio nabywca zainwestował w wyposażanie wirtualnego rycerza[47].

Również wyrokiem skazującym wydanym w sierpniu 2010 r. przez SR w Sławnie, 20-letni *Patryk S.* oskarżony o to, że „działając w celu wyrządzenia szkody innej osobie (…), po uzyskaniu za pomocą programu szpiegującego dostępu do konta usunął dane informatyczne w postaci wirtualnych przedmiotów" (którymi były faktycznie miecz, zbroja i tarcza w grze Metin2), został skazany na karę roku pozbawiania wolności z warunkowym zawieszeniem wykonania tej kary na okres próby oraz na karę grzywny[48].

Jak się wydaje, przedmiotowe zachowania sprawcze, związane z opisanym powyżej zjawiskiem kradzieży tzw. wirtualnych postaci, w większości wypadków realizować będą znamiona czynu z art. 286 § 1 KK, a więc przestępstwa oszustwa, z uwagi na doprowadzenie pokrzywdzonego do niekorzystnego rozporządzenia mieniem – w sytuacji gdy sprawca zarazem wprowadzi go w błąd np. co do faktycznego zamiaru nabycia lub odsprzedaży postaci wirtualnej, a w niektórych wypadkach także znamiona czynu z art. 267 § 1 KK, gdy sprawca w celu uzyskania kodów dostępu do konta pokrzywdzonego uzyska bez uprawnienia dostęp do tych danych, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenia. Brak jest natomiast obecnie możliwości zakwalifikowania przedmiotowych zachowań sprawczych jako przestępstwa z art. 190a § 2 KK, a to z uwagi na okoliczność, iż przepis ten wymaga „podszycia się pod inną osobę", a więc co do zasady pod osobę fizyczną. Oczywiste jest przy tym, że „wirtualna postać", nawet w sytuacji gdy pokrzywdzony z nią się utożsamia, nie posiada atrybutów osoby fizycznej.

Inna sytuacja zachodziłaby natomiast wówczas, gdyby sprawca w celu przejęcia „wirtualnej postaci" uzyskał np. metodą *phisingu* nie tylko dostęp do loginu i hasła pokrzywdzonego, ale także do jego danych osobowych, udostępnionych uprzednio administratorowi gry, a następnie podawałby się za poprzedniego użytkownika, np. w odpowiedzi na zapytanie administratora gry przesłane do niego wiadomością e-mail. Jak się wydaje, w takiej sytuacji mogłoby dojść do wypełnienia normy art. 190a § 2 KK, w szczególności jeżeli równocześnie przyjmiemy, że osoba, która utraciła w ten sposób swojego avatara i pod którą aktualnie sprawca się podszywa, poniosła z tego tytułu wymierną szkodę majątkową.

W tym miejscu należy zauważyć, że ustawowy zakres ujęcia szkody w ramach art. 190a § 2 KK nie chroni w sposób wystarczający wszystkich osób, którym na skutek działania sprawcy podszywającego się pod inną osobę szkoda taka zostaje wyrządzona. Szkodę zarówno w ujęciu majątkowym, rozumianym jako *damnum emergens* oraz *lucrum cessans*, jak i szkodę osobistą, rozumianą jako szkoda na osobie oraz tzw. krzywda, w ramach czynu z art. 190a § 2 KK można bowiem wywołać wyłącznie w odniesieniu do bezpośredniego pokrzywdzonego tym przestępstwem, a więc osoby fizycznej, pod którą w celu wyrządzenia takiej szkody podszył

[45] *M. Maj*, Kradzież tożsamości w grze… i co dalej, Dziennik Internautów. Internauci z 4.6.2008 r., http://di.com.pl/kradziez-tozsamosci-w-grze-i-co-dalej-21124 (dostęp z 12.3.2018 r.).

[46] Zatrzymano sprawcę kradzieży wirtualnego rycerza w grze Tibia, Dziennik Internautów. Biznes i prawo, 29.7.2011 r., http://di.com.pl/zatrzymano-sprawce-kradziezy-wirtualnego-rycerza-w-grze-tibia-39410 (dostęp z 12.3.2018 r.).

[47] *M. Gajewski*, Do więzienia za wirtualną kradzież. W Polsce!, CHIP z 29.7.2011 r., https://www.chip.pl/2011/07/kradziez-postaci-w-grze-mmo-skonczyla-sie-wyrokiem-sadowym/ (dostęp z 12.3.2018 r.).

[48] *D. Szyller*, *M. Fabiański*, Kradzież w krainie demonów, Rzeczpospolita z 25.8.2012 r., http://www.rp.pl/artykul/925892-Kradziez-w-krainie-demonow.html (dostęp z 12.3.2018 r.).

się sprawca. Jak słusznie podkreśla się natomiast w doktrynie, przestępstwo kradzieży tożsamości z art. 190a § 2 KK może naruszać nie tylko dobra osoby, której dane osobowe są faktycznie przywłaszczone, ale także może naruszać dobra prawne innych osób[49]. W przypadku bowiem podszycia się pod określoną osobę szkoda – w szczególności o charakterze osobistym – może zaistnieć także w dobrach innej osoby. Jako przykład można przedstawić fikcyjną sytuację, gdy sprawca, wykorzystując wizerunek członka danej rodziny, np. ojca, i podszywając się pod ten wizerunek w celu zamieszczenia na portalu społecznościowym wpisu mającego stworzyć wrażenie, iż osoba ta posiada określone, pejoratywne cechy (np. sprzedaje narkotyki), doprowadza do napiętnowania społecznego także pozostałych członków tej rodziny, a nawet czasowego ich wykluczenia społecznego. Bez wątpienia szkoda osobista w opisanej sytuacji, związana z działaniem sprawcy nakierowanym na jedną osobę, może zaistnieć także w odniesieniu do innych osób, pod które faktycznie sprawca się nie podszywał.

Podkreślić także należy, że zgodnie z treścią art. 49 § 1 KPK za pokrzywdzonego uważa się osobę fizyczną lub prawną, której dobro prawne zostało bezpośrednio naruszone lub zagrożone przez przestępstwo. Tym samym już z samej definicji pokrzywdzonego – będącego osobą fizyczną wynika, że także w przypadku innej osoby niż ta, pod którą sprawca bezpośrednio się podszył (w celu wyrządzenia jej szkody majątkowej lub osobistej), jeżeli dochodzi do faktycznego naruszenia lub zagrożenia jej dóbr prawnych wyrządzeniem szkody majątkowej lub osobistej, powinna być ona włączona do kręgu osób pokrzywdzonych czynem z art. 190a § 2 KK. Z uwagi na użycie jednak w dyspozycji art. 190a § 2 KK jednoznacznego sformułowania „kto podszywając się pod inną osobę wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej szkody majątkowej lub osobistej", brak jest możliwości bez stosownej zmiany legislacyjnej zastosowania wykładni rozszerzającej w tym zakresie – zwłaszcza w kontekście bezpośrednio wynikającego z zasady *nullum crimen sine lege* (art. 1 § 1 KK) postulatu *nullum crimen sine lege stricta*, a więc zakazu stosowania niekorzystnej dla sprawcy analogii oraz wykładni rozszerzającej.

Podsumowanie

Jak się wydaje, poprzez użycie w dyspozycji przedmiotowego art. 190a § 2 KK sformułowania „kto podszywając się pod inną osobę wykorzystuje jej wizerunek lub inne jej dane osobowe w celu wyrządzenia jej lub też innej osobie szkody majątkowej lub osobistej" doszłoby do pożądanego z punktu widzenia następstw przedmiotowego przestępstwa rozszerzenia odpowiedzialności sprawcy czynu z art. 190 a § 2 KK, także za ewentualną szkodę (majątkową lub osobistą) wyrządzoną innej osobie niż jedynie ta, pod którą sprawca bezpośrednio się podszył. Co oczywiste, postulat ten ma charakter wyłącznie propozycji *de lege ferenda*.

Tym samym uznać należy, że aktualny brak kryminalizacji przygotowania do przestępstwa z art. 190 a § 2 KK, uznającego w szczególności za takie przygotowanie pozyskiwanie bądź też gromadzenie danych osobowych lub wizerunków danej osoby, w celu wykorzystania ich następnie do podszycia się pod określoną osobę i wyrządzenia jej przez to szkody majątkowej lub osobistej, jak też brak możliwości uznania za pokrzywdzoną czynem z art. 190a § 2 KK także innej osoby niż ta, pod którą sprawca faktycznie się podszywa, stanowią istotne mankamenty przedmiotowej regulacji.

Bez wątpienia wprowadzenie postulowanych w treści niniejszego opracowania zmian legislacyjnych przyczyniłoby się do skuteczniejszego zwalczania przestępstw kradzieży tożsamości, i to już w ich stadium początkowym, gdzie sprawca faktycznie czyni przygotowania do popełnienia przedmiotowego przestępstwa, a także do zwiększenia bezpieczeństwa ofiar tego przestępstwa, rozumianych w szerokim, a nie jak dotychczas jedynie wąskim zakresie.

Oczywiście nie można tracić z pola widzenia także konieczności podejmowania działań w zakresie kryminologicznym, w szczególności poprzez stałe zwiększanie świadomości potencjalnych ofiar przestępstw z art. 190a § 2 KK odnośnie do występujących w ramach sieci Internet zagrożeń będących następstwem bezkrytycznego często udostępniania swoich danych osobowych i wizerunku graficznego np. na portalach społecznościowych. Konieczne wydają się w tym zakresie działania podejmowane na szczeblu rządowym – w szczególności przez Ministerstwo Sprawiedliwości, a sprowadzające się do określonych kampanii medialnych w tym telewizyjnych i prasowych, a także poprzez stosowne publikatory internetowe, które mogą zwiększyć poziom ostrożności i wyczulenia społecznego na tego rodzaju bezprawne działania podejmowane przez przestępców.

Przedmiotowe działania, a tym samym zwiększenie świadomości społecznej w zakresie skutków, które niesie za sobą ewentualne przejęcie tożsamości danej osoby przez przestępcę przyczynić mogą się także do większej wykrywalności przestępstw kradzieży tożsamości, które często obecnie pozostają w sferze tzw. ciemnej liczby przestępstw. W szczególności bowiem, jak zauważa się w doktrynie, często sami pokrzywdzeni przedmiotowymi przestępstwami nie podejmują działań w zakresie zawiadomienia o nich organów ścigania pomimo często dotkliwych szkód z nimi związanych, a to z uwagi na świadomość tych pokrzywdzonych, że do pozyskania ich danych osobowych bądź wizerunku doszło w wyniku ich własnych zaniedbań, w tym niewłaściwego zabezpieczenia danych i dokumentów[50].

[49] *K. Sowirka*, Przestępstwo „kradzieży tożsamości"…, s. 73.
[50] *M. Siwicki*, Kradzież tożsamości – pojęcie i charakterystyka…, s. 32.

Podkreślić należy przy tym, że w literaturze przedmiotu od dawna postulowane są określone działania profilaktyczne, które powinny być objęte w szerokim zakresie także informacjami w ramach kampanii społecznych. W szczególności warto w tym miejscu przytoczyć postulat *M. Kowalczyk-Ludzia* oraz *K. Pruszkiewicz-Słowińskiej* wskazujący na konieczność niszczenia dokumentów zawierających dane identyfikujące przed wyrzuceniem ich do śmieci, przechowywanie ważnych dokumentów w zamkniętych pomieszczeniach, przechowywanie poufnych informacji w plikach i katalogach chronionych hasłami, wzmożonej czujności w zakresie rozpoznawania fałszywych wiadomości e-mail bądź też stron WWW, a także poprzez przeprowadzanie finansowych transakcji online wyłącznie na bezpiecznych stronach[51].

Metody zabezpieczenia się przed określonymi formami działań podejmowanych przez sprawców w sieci Internet, a zmierzających do przejęcia danych osobowych, sprowadzają się przy tym często do tzw. zwykłej przezorności i rozwagi oraz znajomości podstawowych zasad działania określonych instytucji, w tym zwłaszcza banków. W szczególności bowiem banki nigdy nie wysyłają do swoich klientów pytań dotyczących haseł, loginów lub innych danych, a także nie podają w swoich wiadomościach linków do stron transakcyjnych[52].

Tym samym podstawowa zasada ograniczonego zaufania w sieci Internet, sprowadzająca się między innymi do nieotwierania e-maili nieznanego pochodzenia oraz unikania nieznanych stron WWW, na których może występować złośliwe oprogramowanie, może uchronić nas przed możliwością przejęcia naszych danych osobowych bądź innych danych wrażliwych przez przestępców. Zasada ograniczonego zaufania w sieci Internet ma swoje odzwierciedlenie także w potrzebie powstrzymania się przed zamieszczaniem danych osobowych, zdjęć oraz wszelkich innych informacji pozwalających na kradzież naszej tożsamości, na portalach społecznościowych bądź też udostępniania tych danych niesprawdzonym dostawcom usług internetowych.

Wskazane działania profilaktyczne, niezależnie od ochrony prawnokarnej, jaką stwarza art. 190a § 2 KK, mogą skutecznie uchronić nas przed możliwością stania się ofiarą przedmiotowych działań przestępczych.

[51] *M. Kowalczyk-Ludzia*, *K. Pruszkiewicz-Słowińska*, Wybrane zagadnienia dotyczące kradzieży tożsamości na gruncie przepisów prawa karnego i prawa medycznego – studium przypadku, Przegląd Policyjny 2016, Nr 2, s. 87.

[52] *R. Kaszubski*, *Ł. Obzejta*, Karty płatnicze w Polsce…, s. 406.

Słowa kluczowe: kradzież tożsamości, wizerunek, dane osobowe, wirtualna postać, sieć Internet, podszywanie się pod inną osobę

Scope of effective law regulations of art. 190a § 2 of the Penal Code on combating actions concerning the so-called Internet-related identity thief

The subject of the analysis in this paper is the art. 190a § 2 of the Penal Code. Based on this, an attempt has been made to give the answer about effectiveness of regulation against online identity fraud and subsequent criminal acts. The author also takes notice of exemplary methods used by criminals trying to capture or bilk personal data and potential threats of sharing personal information or effigy by Internet users, especially on social networking websites. Moreover this work provides analysis of the new phenomenon which is "online identity impersonation" taking place within games known as MMORPG. Finally, this article points the importance of postulated changes to legislation concerning regulations from the art. 190a § 2 of the Penal Code, which could gain pursuing effectiveness of "identity thief" perpetrators.

Keywords: identity thief, effigy, personal data, online identity, Internet, impersonation.

Telemedycyna transgraniczna – problematyka prawa właściwego dla przypadków odpowiedzialności cywilnej podmiotów medycznych na gruncie prawodawstwa unijnego

Aleksandra Nowak[1]

Coraz większą popularnością na gruncie europejskim cieszą się usługi opieki zdrowotnej świadczone z wykorzystaniem innowacyjnych technologii informacyjno-komunikacyjnych. Tak zwana telemedycyna ma szansę stać się w przyszłości jednym z filarów systemu opieki zdrowotnej – zarówno w wymiarze lokalnym, jak i ogólnoeuropejskim. Na szczególną uwagę w tym kontekście zasługują transgraniczne usługi telemedyczne, które – choć niewątpliwie niosą za sobą liczne korzyści – wobec braku harmonizacji regulacji na szczeblu wspólnotowym stanowią przedmiot istotnych kontrowersji. W niniejszym opracowaniu Autorka poddaje ten problem analizie, a w szczególności ramy normatywne, w jakich telemedycyna funkcjonuje na poziomie prawodawstwa wspólnotowego.

Uwagi wstępne

Ponad 4 miliardy ludzi na całym świecie korzysta dziś z Internetu, przy czym dostęp do globalnej sieci komputerowej w Europie ma blisko 85% ludności. Wyższy odsetek użytkowników Internetu w stosunku do ogółu populacji występuje wyłącznie na terenie Ameryki Północnej, sięgając 95%. Tylko od 2000 r. liczba osób korzystających z sieci zwiększyła się, w skali globalnej, o niemal 1000%[2]. Rewolucja internetowa, poprzez umożliwienie wymiany informacji na niespotykaną dotąd skalę, doprowadziła do powstania nowoczesnego społeczeństwa informatycznego i zredefiniowała rynki światowe, które w przeważającej mierze funkcjonują dziś w cyberprzestrzeni. Globalny rynek cyfrowy nieustannie poszerza się, obejmując coraz to nowe dziedziny życia, a infrastruktura informatyczna wypiera tradycyjne formy aktywności gospodarczej.

Funkcjonowanie współczesnej gospodarki powiązane jest także immanentnie z rozwojem innowacyjnych technologii w zasadniczo wszystkich obszarach działalności. Podobnie większość rewolucyjnych osiągnięć nauk medycznych ostatnich dziesięcioleci zawdzięcza istnienie wykorzystaniu na szeroką skalę owoców współczesnej techniki i informatyki. Analiza tempa rozwoju cywilizacyjnego we wskazanym zakresie pozwala przyjąć, że wchłonięcie usług medycznych przez rynek cyfrowy stanowi naturalne następstwo tego procesu.

Zjawisko telemedycyny

Niektórzy autorzy upatrują genezy telemedycyny w tak odległych momentach historii jak XIV w., kiedy to podczas epidemii dżumy przekazywano informacje o występowaniu przypadków zachorowań przy wykorzystaniu heliografów lub znaków dymnych[3]. Jakkolwiek interesujący, fenomen ten niewiele miał wspólnego z telemedycyną w jej obecnym rozumieniu. Jako pierwsze udokumentowane wykorzystanie nowożytnych osiągnięć technicznych w celu przekazu informacji medycznych wskazać można przesłanie wyników badania wykonanego za pomocą galwanometru strunowego (pierwowzór elektrokardiografu) przy użyciu łącza telefonicznego na początku XX w.[4]. Niewątpliwie jednak proweniencji telemedycyny w jej współczesnym kształcie poszukiwać należy w osiągnięciach Narodowej Agencji Aeronautyki i Przestrzeni Kosmicznej (NASA) na gruncie telekomunikacji i telemetrii, związanych z pierwszymi programami kosmicznymi[5]. To właśnie opracowanie i pionierskie wykorzystanie technologii pozwalającej na monitorowanie podstawowych funkcji życiowych (tętna, temperatury, ciśnienia krwi, częstości oddechów) astronautów z Ziemi powinno się w istocie rzeczy wskazać jako inaugurację procesu kształtowania się nowoczesnej telemedycyny.

Doświadczenia płynące z przypadków sprawowania opieki medycznej nad astronautami znalazły także zastosowanie na mniejszych dystansach. W Stanach Zjednoczonych poten-

[1] Autorka jest studentką V roku studiów stacjonarnych prawa na Wydziale Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.

[2] Dane na 31.12.2017 r. – zob. https://www.internetworldstats.com/stats.htm (dostęp z 21.2.2018 r.).

[3] K.M. Zundel, Telemedicine: history, applications and impact on librarianship, Bulletin of the Medical Library Association 1996, Nr 84, s. 72, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC226126/ (dostęp z 23.2.2018 r.).

[4] *W. Einthoven*, Le télécardiogramme, Archives Internationales de Physiologie 1906, Nr 4, s. 132–164, [za:] WHO, Telemedicine. Opportunities and development in Member States. Report on the 2nd global survey on eHealth 2010, s. 9, http://www.who.int/goe/publications/goe_telemedicine_2010.pdf (dostęp z 23.2.2018 r.).

[5] *R. Bashshur, J. Lovett*, Assessment of telemedicine: results of the initial experience, Aviation, Space, and Environmental Medicine 1997, Nr 48, s. 65–70, [za:] *K.M. Zundel*, Telemedicine..., s. 72.

cjał telemedycyny dostrzeżono w możliwości zapewnienia profesjonalnej opieki medycznej pacjentom znajdującym się na terenach wiejskich. Brak wyspecjalizowanej kadry medycznej na tych obszarach kompensowany był poprzez realizację specjalnych projektów mających na celu promocję i rozwój konsultacji medycznych i diagnozy za pośrednictwem różnorodnych środków komunikacji na odległość[6].

W 1950 r. *J. Gershon-Cohen* opublikował artykuł pt. Teleognoza (*Teleognis*). Wskazywał, że teleognoza to pojęcie stanowiące kombinację trzech terminów: „teleo", „rentgen" i „diagnoza", służące do określenia czynności polegających na przesyłaniu obrazów radiologicznych za pomocą kabli radiowych lub telefonicznych pomiędzy odległymi lokalizacjami geograficznymi w celu ich interpretacji, zapewniających możliwość uzyskania specjalistycznej konsultacji. Pojęcie to posłużyło do opisania działań podejmowanych na przestrzeni dwóch lat w ramach współpracy ośrodków medycznych w West Chester w Pensylwanii i Filadelfii oddalonych od siebie o 28 mil. *J. Gershon-Cohen* wskazywał na użyteczność i ekonomiczną opłacalność podobnych procedur w przypadkach, w których prowincjonalne szpitale nie dysponują odpowiednio wykwalifikowanym personelem[7]. W kolejnych dekadach coraz więcej ośrodków w Stanach Zjednoczonych wdrażało działania realizujące te idee. Stopniowo poszerzał się nie tylko zakres specjalności medycznych wykorzystujących potencjał telemedycyny, ale także wachlarz stosowanych środków porozumiewania się na odległość[8].

Pojęciem telemedycyny (*telemedicine*) zaczęto posługiwać się w Stanach Zjednoczonych już w latach 70. XX w. Termin ten, skonstruowany z połączenia dwóch pojęć: łacińskiego „*medicus*" i greckiego „*tele*", dosłownie oznacza „leczenie na odległość"[9]. Pomimo upowszechnienia się usług medycznych świadczonych za pomocą nowoczesnych technologii informacyjno-komunikacyjnych pojęcie telemedycyny nie doczekało się jednolitej definicji. Zakres analizowanego terminu należy zatem rekonstruować na podstawie innych, zaczerpniętych z dorobku międzynarodowego definicji.

W rozumieniu przyjętym przez Komisję Europejską telemedycyna to „świadczenie usług zdrowotnych z wykorzystaniem TIK [technologii informacyjno-komunikacyjnych – dopisek *A.N.*], w sytuacji, gdy pracownik służby zdrowia i pacjent (lub dwaj pracownicy służby zdrowia) nie znajdują się w tym samym miejscu"[10]. Komisja Europejska wskazuje także, że usługi telemedyczne wiążą się z przesyłem w różnorodnej formie (tekstu, obrazu, dźwięku lub innej) danych medycznych, które są niezbędne do podjęcia działań prewencyjnych, diagnozy, leczenia i monitorowania stanu zdrowia pacjenta[11].

Światowa Organizacja Zdrowia (WHO) definiuje z kolei telemedycynę jako „świadczenie usług opieki zdrowotnej, w której kluczową rolę odgrywa rozłączność miejsca, przez wszystkie osoby wykonujące zawody medyczne, przy wykorzystaniu ICT [technologii informacyjno-komunikacyjnych – dopisek *A.N.*] służących wymianie istotnych informacji w celach diagnostycznych, leczniczych oraz zapobiegania chorobom i urazom, prowadzenia badań i ich oceny, zapewnienia, kontynuacji kształcenia pracowników służby zdrowia, czyli w celu poprawy zdrowia jednostek oraz tworzonych przez nie społeczności[12]". Jednocześnie WHO wskazuje na cztery elementy konstruujące pojęcie telemedycyny:

1) służy ona zapewnieniu wsparcia klinicznego,
2) ma na celu przezwyciężenie barier geograficznych, sprzyjając łączeniu uczestników systemu opieki zdrowotnej, którzy nie znajdują się fizycznie w tej samej lokalizacji,
3) wykorzystuje różnorodne technologie informacyjno-komunikacyjne,
4) zmierza do poprawy wyników zdrowotnych[13].

Według lakonicznej definicji Amerykańskiego Stowarzyszenia Telemedycyny (*American Telemedicine Association*) istotą telemedycyny jest świadczenie usług zdrowotnych i wymiana informacji medycznych przy użyciu komunikacji elektronicznej[14].

Wielość funkcjonujących w praktyce definicji przyczynia się do powstawania wątpliwości natury terminologicznej. Na marginesie rozważań warto zwrócić uwagę, że trudności te pogłębia występowanie w literaturze i obrocie innych określeń takich jak: TEC (*technology enabled care*), telezdrowie, e-Zdrowie, m-Zdrowie itp. Pojęcia te nie są jednak synoni-

[6] *K.M. Zundel*, Telemedicine..., s. 73.

[7] *J. Gershon-Cohen*, *A.G. Cooley*, Teleognosis, Radiology 1950, Nr 55, s. 582–587, [za:] *K.M. Zundel*, Telemedicine..., s. 73.

[8] W latach 70. XX w. w Stanach Zjednoczonych przeprowadzano liczne eksperymenty z zakresu wykorzystania środków porozumiewania się na odległość na potrzeby konsultacji medycznych. Większość z nich zakończyła się sukcesem. Za ilustrację posłużyć może wykorzystanie łączy telefonicznych na potrzeby interpretacji badania echokardiograficznego (zob. *J.P. Finley*, *D.G. Human*, *M.A. Nanton*, *D.L. Roy* i in., Echocardiography by telephone: evaluation of pediatric heart disease at a distance, American Journal of Cardiology 1989, Nr 63, s. 1475–1477), czy też zaadaptowanie telewizji do przeprowadzania konsultacji audiowizualnych (zob. *B.L. Rundy*, *P. Crawford*, *P.K. Jones*, *M.L. Kiley* i in., Telemedicine in critical care: an experiment in health care, Journal of Applied Chemistry and Environment Protection 1977, Nr 6, s. 439–444).

[9] *E.M. Strehle*, *N. Shabde*, 100 years of telemedicine: does this new technology have a place in pediatrics?, Archives of Disease Childhood 2006, Nr 91, s. 956; https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2082971/ (dostęp z 23.2.2018 r.).

[10] Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów w sprawie korzyści telemedycyny dla pacjentów, systemów opieki zdrowotnej i społeczeństwa, KOM(2008)689 wersja ostateczna 2008, http://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1426260639870&uri=CELEX:52008DC0689 (dostęp z 23.2.2018 r.).

[11] *Ibidem*.

[12] WHO, Telemedicine. Opportunities..., s. 9, [tłum. za:] *M. Czarnuch*, *M. Grabowski*, *P. Najbuk*, *Ł. Kołtowski* (red.), Otoczenie regulacyjne telemedycyny w Polsce – stan obecny i nowe otwarcie, Warszawa 2015, s. 9; https://www.dzp.pl/files/shares/Publikacje/Otoczenie_Regulacyjne_Telemedycyny_w_Polsce.pdf.pdf (dostęp z 23.2.2018 r.).

[13] WHO, Telemedicine. Opportunities..., s. 9.

[14] Zob. http://www.americantelemed.org/main/about/about-telemedicine/telemedicine-faqs (dostęp z 23.2.2018 r.).

miczne i nie należy ich utożsamiać mimo częściowej zbieżności zakresów przedmiotowych[15].

Wybrane rodzaje świadczeń telemedycznych

Błyskawiczny rozwój telemedycyny sprawił, że obecnie, wobec mnogości różnorodnych rodzajów świadczeń telemedycznych, trudno o ich jednolitą klasyfikację. Niemniej możliwe jest wskazanie przykładowych kryteriów podziału analizowanych usług.

Mając na względzie kryterium podmiotowe, a więc uwzględniając, w jakim charakterze występują strony uczestniczące w wymianie danych, można wyróżnić takie świadczenia telemedyczne, które są świadczone na rzecz pacjentów, oraz takie, które świadczone są na rzecz innych podmiotów medycznych. Podmiotem świadczącym usługi telemedyczne będzie zawsze osoba profesjonalnie udzielająca świadczeń zdrowotnych. Można zatem stwierdzić, że w tym sensie stosunki mające za przedmiot usługi telemedyczne mogą występować jako jednostronnie lub dwustronnie profesjonalne.

Do przedmiotowych kryteriów podziału należą: sposób przekazywania danych medycznych, rodzaj świadczonych usług oraz specjalizacja medyczna w zakresie, której świadczona jest usługa. Pierwsze ze wskazanych kryteriów przedmiotowych pozwala na wyodrębnienie trzech zasadniczych metod przekazu informacji funkcjonujących na gruncie telemedycyny. Mianowicie dane medyczne mogą być gromadzone w postaci danych cyfrowych (zdjęć, plików wideo lub innych), a następnie przesyłane do dalszej analizy za pomocą zabezpieczonego łącza („*store and forward*"). Usługi telemedyczne mogą być także świadczone w drodze komunikacji w czasie rzeczywistym np. wideokonferencji („*real time*"). Ostatnim sposobem przekazu danych jest tzw. zdalny monitoring („*remote monitoring*") polegający na monitorowaniu na odległość stanu zdrowia pacjentów[16]. Telemonitorowanie, szczególnie pomocne w przypadku osób cierpiących na przewlekłe choroby np. cukrzycę, przewlekłą niewydolność serca czy astmę, może polegać na pozyskiwaniu danych w sposób zautomatyzowany za pomocą urządzeń monitorujących stan zdrowia (np. pompy insulinowe, implantowane kardiowerter-defibrylatory serca) lub gromadzeniu ich przy aktywnym udziale pacjenta (np. gdy samodzielnie wykonuje dzienne pomiary poziomu cukru we krwi i przekazuje dane przy wykorzystaniu sieci Internet)[17].

Przyjmując jako kryterium podziału rodzaj świadczonych usług, możemy wyróżnić m.in. wyżej wspomniany telemonitoring, telerehabilitację, telekonsultacje, telediagnostykę. Ta ostatnia obejmuje swym zakresem takie świadczenia telemedyczne, jak np. teleradiologia, teleendoskopia czy telepatologia[18]. Nie sposób przedstawić zamkniętego katalogu możliwych usług telemedycznych. Takie próby zresztą, wobec nieustannego rozwoju telemedycyny, pozbawione byłyby znaczenia praktycznego. Niektóre z usług elektronicznych w ochronie zdrowia mają relatywnie długą, bo niemal 100-letnią historię (np. teleradiologia), inne wykształciły się niedawno. Dobrą ilustrację w tym zakresie stanowią – wciąż nowatorskie – teleoperacje, których istota polega na przeprowadzaniu zabiegów operacyjnych przy braku jednoczesnej obecności chirurga i pacjenta w tej samej lokalizacji[19], tj. z wykorzystaniem różnorodnych technologii informacyjno-komunikacyjnych lub przy zastosowaniu robotów chirurgicznych. Zdalna chirurgia, czerpiąca w głównej mierze z innowacyjnych osiągnięć robotyki, rozpoczęła intensywny rozwój wraz z końcem XX w. Już w 2001 r. przeprowadzono pierwszą międzykontynentalną teleoperację. Pacjentka przebywająca w Strasburgu została poddana zabiegowi usunięcia pęcherzyka żółciowego przez lekarza znajdującego się w Nowym Yorku. Operacja przeprowadzona zdalnie z wykorzystaniem robota chirurgicznego „Zeus", zakończyła się sukcesem[20]. Choć od tego przełomowego wydarzenia minęło bez mała 17 lat, teleoperacje wciąż nie są wykorzystywane na tak szeroką skalę jak inne usługi telemedyczne. Jest to gałąź telemedycyny, która jak się wydaje, niesie za sobą najwięcej korzyści, ale jednocześnie jest źródłem najliczniejszych zagrożeń. Niemniej, kierunek ewolucji uwarunkowań ekonomicznych, demograficznych, społecznych, a także nieustający rozwój techniczno-informatyczny pozwala przypuszczać, że teleoperacje, jakkolwiek nie zastąpią operacji tradycyjnych (bezpośrednich), będą mogły stać się w przyszłości istotnym elementem systemu opieki zdrowotnej. Powyższe rozważania dowodzą, że technologia telemedyczna wciąż znajduje się w fazie rozwoju, a dziś możemy jedynie spekulować odnośnie do dalszych kierunków jej ewolucji.

Wreszcie, uwzględniając trzecie z przedmiotowych kryteriów, tj. rodzaj specjalizacji medycznej, w zakresie której świadczona jest usługa, możemy wyróżnić telechirurgię, teleradiologię, telepsychiatrię, telepediatrię, telekardiologię i inne. Zasadniczo technologia telemedyczna w różnych jej postaciach przeniknęła już do większości dziedzin medycy-

[15] *M. Czarnuch*, *M. Grabowski*, *P. Najbuk*, *Ł. Kołtowski* (red.), Otoczenie regulacyjne..., s. 9.

[16] *Ibidem*, s. 11.

[17] Komisja Europejska, Komunikat Komisji...

[18] *M. Czarnuch*, *M. Grabowski*, *P. Najbuk*, *Ł. Kołtowski* (red.), Otoczenie regulacyjne..., s. 9.

[19] *H.W.R. Schreuder*, *R.H.M. Verheijen*, Robotic Surgery, International Journal of Obstetrics and Gynaecology 2009, Nr 116, s. 198–213, [za:] *S.M. Saceanu* i in., Telesurgery and Robotic Surgery: Ethical and Legal Aspect, Journal of Community Medicine & Health Education 2015, Nr 5; https://www.omicsonline.org/open-access/telesurgery-and-robotic-surgery-ethical-and-legal-aspect-2376-0214-1000355.pdf (dostęp z 24.2.2018 r.).

[20] *Operation Lindbergh*. A World First in *TeleSurgery*: The Surgical Act Crosses the Atlantic! New York – Strasbourg. Press Conference, Espace Multimedia 2001, https://www.ircad.fr/wp-content/uploads/2014/06/lindbergh_presse_en.pdf (dostęp z 24.2.2018 r.).

ny. Na potrzeby rozważań natury prawnej podział według specjalizacji ma jednak, jak się wydaje, mniejszą doniosłość praktyczną. Określony typ usługi świadczony może być bowiem na gruncie różnych specjalizacji. Wspomniane już telemonitorowanie może być świadczeniem przyjmującym różną formę zarówno w ramach telekardiologii, telepneumologii, jak i telediabetologii.

Jak wynika z powyższych rozważań, intensyfikacja wpływu nowych technologii na medycynę warunkuje ciągłe poszerzanie się katalogu rodzajów usług telemedycznych oraz ich wykorzystywanie w coraz większej liczbie specjalizacji. Na potrzeby regulacji prawnych konstruowanie *a priori* pełnego katalogu świadczeń telemedycznych nie jest ani możliwe, ani tym bardziej zasadne. Próby unormowania materii z pogranicza nauk medycznych i nowych technologii dobitnie ukazują, że prawo nie zawsze nadąża za tempem nauki. Z tych względów konieczne jest tworzenie regulacji prawnych na tyle elastycznych, by były one w stanie dostosować się do ciągłego rozwoju i zmian na gruncie zdobyczy nauki i techniki.

Korzyści rozwiązań telemedycznych

Niewątpliwie do beneficjentów rozwiązań telemedycznych należą zarówno pacjenci, jak i osoby wykonujące zawody medyczne[21].

Wykorzystanie innowacyjnych osiągnięć technologicznych i informatycznych w ochronie zdrowia umożliwia przede wszystkim przełamanie barier geograficznych, zapewniając dostęp do profesjonalnych świadczeń także osobom zamieszkałym na obszarach słabo rozwiniętych, na których dostęp do opieki zdrowotnej jest utrudniony lub brakuje specjalistów. Jednocześnie dla profesjonalistów medycznych oznacza to dostęp do pacjentów w szerszym zakresie i znaczną oszczędność czasu. Efektywne wykorzystanie czasu pracy przekłada się z kolei na zwiększenie produktywności pracowników służby zdrowia, a co za tym idzie – skrócenie kolejek pacjentów oczekujących na uzyskanie świadczeń. Do skrócenia czasu oczekiwania przyczynia się także możliwość przeprowadzenia wstępnej selekcji pacjentów przy wykorzystaniu systemów komunikacji elektronicznej[22].

Wykorzystanie technologii i usług teleinformatycznych skutkuje nie tylko oszczędnością czasu, ale także znacząco ogranicza koszty sprawowania opieki zdrowotnej. Amerykańskie Stowarzyszenie Telemedycyny wskazuje właśnie redukcję kosztów jako jeden z najistotniejszych czynników przemawiających za wdrażaniem rozwiązań telemedycznych w możliwie najszerszym zakresie. Telemedycyna pozwala na ograniczenie liczby hospitalizacji i skrócenie czasu ich trwania, zminimalizowanie dojazdów z i do szpitala, a także optymalizację procesu leczenia pacjentów chorych przewlekle[23].

Telemedycyna niesie za sobą także niewątpliwe korzyści w wymiarze gospodarczym, na co szczególną uwagę zwraca Komisja Europejska. W cytowanym już Komunikacie z 2008 r. wskazano, że wykorzystanie innowacyjnych rozwiązań technologicznych i informatycznych w ochronie zdrowia może wnieść znaczący wkład do gospodarki UE, przemysł europejski bowiem, w tym tysiące małych i średnich przedsiębiorstw, mają znaczny udział w tym sektorze[24].

Usługi telemedyczne w świetle prawa unijnego

Jak wielokrotnie wskazywał w swoich orzeczeniach TS, świadczenia opieki zdrowotnej, w tym telemedyczne, są usługami w rozumieniu art. 57 Traktatu o Funkcjonowaniu Unii Europejskiej[25] i ani ich szczególny charakter, ani sposób organizacji lub finansowania nie powodują ich wyłączenia z zakresu stosowania podstawowej zasady swobody świadczenia usług (art. 56 TFUE)[26]. Swoboda świadczenia usług, jakkolwiek jest jedną z podstawowych wolności konstytuujących rynek wewnętrzny, nie ma charakteru absolutnego. Państwa członkowskie mogą bowiem wprowadzać i utrzymywać ograniczenia w zakresie świadczenia usług, jeśli są one uzasadnione nadrzędnym interesem publicznym (m.in. koniecznością ochrony zdrowia publicznego), są środkiem proporcjonalnym i nie mają charakteru dyskryminującego[27].

Usługi telemedyczne są w rozumieniu prawa unijnego zarówno usługami zdrowotnymi, jak i usługami społeczeństwa informacyjnego[28]. Stąd, rozważając ramy normatywne, w jakich telemedycyna funkcjonuje na poziomie prawodawstwa wspólnotowego, należy uwzględnić regulacje odnoszące się do obydwu rodzajów usług[29].

[21] *T.M. Drake*, *J.E. Ritchie*, The Surgeon Will Skype You Now: Advancements in E-clinic, Annals of Surgery 2016, Nr 263, s. 636; https://journals.lww.com/annalsofsurgery/Fulltext/2016/04000/The_Surgeon_Will _Skype_You_Now___Advancements_in.3.aspx (dostęp z 24.2.2018 r.).

[22] *M. Czarnuch*, *M. Grabowski*, *P. Najbuk*, *Ł. Kołtowski* (red.), Otoczenie regulacyjne..., s. 14.

[23] Zob. http://www.americantelemed.org/main/about/about-telemedicine/telemedicine-benefits (dostęp z 24.2.2018 r.).

[24] Komisja Europejska, Komunikat Komisji...

[25] Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana 2016), Dz.Urz. UE C Nr 202; dalej jako: TFUE.

[26] Zob. wyroki TS z 31.1.1894 r. w połączonych sprawach: 286/82 i 26/83 Luisi i Carbone, Zb. Orz. 1984, 00377; z 10.5.1995 r., C-384/93, w sprawie Alpine Investments, Zb. Orz. 1995, I-01141; z 28.4.1998 r., C-158/96, w sprawie Kohll, Zb. Orz. 1998, I-01931; z 12.7.2001 r., C-368/98, w sprawie Vanbraekel, Zb. Orz. 2001, I-05363; z 16.5.2006 r., C-372/04, w sprawie Watts, Zb. Orz. 2006, I-04325.

[27] *M. Kożuch*, [w:] *A. Zawidzka-Łojek*, *R. Grzeszczak*, *A. Łazowski*, Prawo Unii Europejskiej. Vademecum. Instytucje i porządek prawny. Prawo materialne, Warszawa 2015, s. 558–559.

[28] Komisja Europejska, Komunikat Komisji...

[29] *B. Kelly*, E-Health: Ethical and data privacy challenges in the EU, Informa 2011, s. 27; https://www.cov.com/~/media/files/corporate/publications/2011/04/e-health---ethical-and-data-privacy-challenges-in-the-eu.pdf (dostęp z 24.2.2018 r.).

1. Usługi telemedyczne jako usługi zdrowotne

Na poziomie wspólnotowym brak jest ujednoliconej regulacji w dziedzinie ochrony zdrowia, a działania UE opierają się w tym zakresie na zasadzie pomocniczości. Unia nie podejmuje działań zmierzających do pełnej harmonizacji systemów opieki zdrowotnej państw członkowskich, a jedynie, w ramach swoich kompetencji, wspiera państwa członkowskie w dążeniach wypracowania wspólnych standardów ochrony zdrowia i życia ludzkiego. Zgodnie z brzmieniem ust. 7 art. 168 TFUE: „Działania Unii są prowadzone w poszanowaniu obowiązków państw członkowskich w zakresie określania ich polityki dotyczącej zdrowia, jak również organizacji i świadczenia usług zdrowotnych i opieki medycznej. Obowiązki państw członkowskich obejmują zarządzanie usługami zdrowotnymi i opieką medyczną, jak również podział przeznaczonych na nie zasobów".

Niemniej, w związku ze specyfiką usług medycznych i wzrostem mobilności pacjentów, zrodziła się konieczność ustanowienia jednolitych zasad ułatwiających dostęp do bezpiecznej transgranicznej opieki zdrowotnej. Celem dyrektywy Parlamentu Europejskiego i Rady 2011/24/UE z 9.3.2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej[30] jest w szczególności uwzględnienie dorobku orzeczniczego TS, zwłaszcza w zakresie zasad zwrotu kosztów opieki zdrowotnej świadczonej w państwie członkowskim innym niż państwo zamieszkania osoby korzystającej z opieki[31].

Zgodnie z brzmieniem art. 1 ust. 2 dyrektywy 2011/24/UE jej przepisy znajdują zastosowanie we wszystkich przypadkach „świadczenia opieki zdrowotnej na rzecz pacjentów, niezależnie od tego, jak jest ona zorganizowana, udzielana i finansowana". Objęcie zakresem zastosowania dyrektywy 2011/24/UE wszelkich usług bez względu na sposób ich udzielania (*regardless of how it is* [...] *delivered* [...]) oznacza, że regulacje tam przewidziane należy także odnieść do usług telemedycznych.

2. Usługi telemedyczne jako usługi społeczeństwa informacyjnego

W rozumieniu dyrektywy 2000/31/WE z 8.6.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[32], usługą społeczeństwa informacyjnego jest każda usługa świadczona za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy. Świadczenia telemedyczne będą zatem usługami społeczeństwa informacyjnego, wyłącznie gdy będą wykonywane odpłatnie (bez znaczenia pozostaje kto płaci świadczeniodawcy wynagrodzenie świadczeniobiorca czy osoba trzecia), bez równoczesnej obecności stron, drogą elektroniczną (co oznacza, że usługa jest wysyłana i odbierana w miejscu przeznaczenia za pomocą sprzętu elektronicznego do przetwarzania – włącznie z kompresją cyfrową – oraz przechowywania danych, i która jest całkowicie przesyłana, kierowana i otrzymywana za pomocą kabla, fal radiowych, środków optycznych lub innych środków elektromagnetycznych), na indywidualne żądanie odbiorcy usług (przy czym przyjmuje się, że pacjenci wyrażający zgodę na leczenie i akceptujący jego formy telemedyczne zgłaszają żądanie w sposób dorozumiany)[33].

Przepisy dyrektywy 2000/31/WE nakładają na usługodawców wiele obowiązków informacyjnych. Szczególne powinności w tym zakresie ciążą na podmiotach świadczących usługi w ramach wykonywania zawodów regulowanych. Powyższe oznacza, że osoby świadczące usługi telemedyczne obciążone są nie tylko obowiązkami informacyjnymi o charakterze ogólnym (m.in. w zakresie nazwy usługodawcy, adresu jego siedziby czy adresu poczty elektronicznej), ale także powinny umożliwić łatwy, bezpośredni i stały dostęp usługobiorcom oraz właściwym władzom do określonych informacji szczególnych m.in. tytułu zawodowego, którego używają oraz państwa, w którym został on przyznany, a także, w określonym zakresie, zasad wykonywania zawodu w państwie członkowskim siedziby.

Telemedycyna transgraniczna na gruncie regulacji unijnych

Wydawać mogłoby się, że transgraniczne usługi telemedyczne mają dziś szansę stać się zupełnie nową jakością świadczenia usług medycznych w UE. Jednak pomimo braku istotnych barier technologiczno-infrastrukturalnych rozwój tego obszaru opieki zdrowotnej napotyka niemałe trudności praktyczne. Zasadnicze przeszkody do wdrażania na szeroką skalę usług telemedycyny transgranicznej są związane na gruncie europejskim z problemami natury prawno-organizacyjnej[34]. Regulacje unijne odnoszące się do telemedycyny są nieliczne i rozproszone w różnych aktach prawnych. Istotną

[30] Dz.Urz. UE L Nr 88, s. 45.; dalej jako: dyrektywa 2011/24/UE.

[31] Zob. wyrok TS z 27.10.2011 r., C-255-09, w sprawie Komisja v. Portugalia, Zb. Orz. 2011, I-10547.

[32] Dz.Urz. UE L Nr 178, s. 1; dalej jako: dyrektywa 2000/31/WE.

[33] Komisja Europejska, Commission Staff Working Document on the applicability of the existing EU legal framework to telemedicine services accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions eHealth Action Plan 2012–2020 – innovative healthcare for the 21st century, SWD/2012/0414 wersja ostateczna, http://eur-lex.europa.eu/legal-content/de/ALL/?uri=-CELEX:52012SC0414 (dostęp z 25.2.2018 r.).

[34] *M. Kielar*, *W. Trąbka*, *A. Romaszewski*, Uwarunkowania transgranicznych telekonsultacji medycznych w środowisku chmury obliczeniowej, Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie 2014, Nr 33, s. 82.

rolę odgrywają regulacje wewnętrzne państw członkowskich, choć i te są, w skali kontynentu, szczątkowe.

Telemedycyna niesie za sobą, poza niewątpliwymi korzyściami, także liczne zagrożenia. Stąd, jako jeden z istotnych problemów telemedycyny, wskazać należy problematykę odpowiedzialności podmiotów medycznych za szkody wyrządzone przy wykonywaniu działalności z zakresu opieki zdrowotnej. Wachlarz możliwych scenariuszy jest w tym zakresie niezwykle szeroki, a konieczność dostosowania zasad odpowiedzialności do realiów usług opieki zdrowotnej świadczonych przy pomocy technologii informacyjno-komunikacyjnych może rodzić swoiste trudności. Problematyka odpowiedzialności podmiotów medycznych dodatkowo komplikuje się na gruncie telemedycyny transgranicznej, gdzie równolegle wyłania się konieczność stosowania odpowiednich norm kolizyjnych w celu ustalenia prawa właściwego dla przypadków tej odpowiedzialności.

1. Telemedycyna transgraniczna w świetle dyrektyw unijnych

Jakkolwiek kompetencje w zakresie ustalania zasad kształcenia oraz zasad dostępu do zawodów medycznych należą do państw członkowskich, w celu realizacji swobody przepływu osób i usług powstała konieczność ujednolicenia regulacji dotyczących uznawania wiedzy i kwalifikacji do wykonywania zawodu w sytuacjach, gdy kwalifikacje takie zostały już nabyte w innym państwie członkowskim[35]. Potrzeba ta została zrealizowana na gruncie przepisów dyrektywy 2005/36/WE Parlamentu Europejskiego i Rady z 7.9.2005 r. w sprawie uznawania kwalifikacji zawodowych[36]. Należy jednak podkreślić, że regulacja ta nie znajdzie zastosowania w zakresie transgranicznych usług telemedycznych. Możliwość taką jednoznacznie wyłącza brzmienie art. 5 ust. 2, zgodnie z którym przepisy dyrektywy 2005/36/WE stosuje się wyłącznie w odniesieniu do przypadków przeniesienia się usługodawcy na terytorium innego państwa członkowskiego w celu tymczasowego i okazjonalnego wykonywania zawodu. Tymczasem świadczenie usług telemedycznych odbywa się bez faktycznego przemieszczania się którejkolwiek ze stron umowy.

Osoba będąca świadczeniodawcą usług telemedycznych musi zatem spełniać wyłącznie warunki wykonywania zawodu medycznego określone przez prawo państwa członkowskiego, na którego terytorium fizycznie się znajduje. Przepisy obowiązujące w państwie członkowskim pobytu usługobiorcy nie mogą nakładać na usługodawcę dodatkowych wymogów ani uzależniać możliwości udzielania telemedycznych świadczeń opieki zdrowotnej na rzecz odbiorców przebywających na terytorium tego państwa od uzyskania przez podmiot medyczny dodatkowych licencji czy zezwoleń[37].

W tym kontekście istotne znaczenie ma dyrektywa 2011/24/UE, której art. 4 ust. 1 stanowi, że transgraniczna opieka zdrowotna powinna być świadczona zgodnie z przepisami oraz normami i wytycznymi w zakresie jakości i bezpieczeństwa określonymi przez państwo leczenia. Na potrzeby tej regulacji „państwo członkowskie leczenia" zostało zdefiniowane jako państwo członkowskie, na którego terytorium opieka zdrowotna jest faktycznie świadczona. Szczególne rozwiązanie przyjęto w tym zakresie w odniesieniu do telemedycyny. Na gruncie dyrektywy 2011/24/UE należy bowiem przyjąć, że państwem leczenia w przypadku telemedycyny jest państwo członkowskie, w którym ma siedzibę świadczeniodawca (art. 3 lit. d).

W kontekście usług telemedycznych szczególne znaczenie ma również wyrażona w art. 3 dyrektywy 2000/31/WE zasada państwa pochodzenia, zgodnie z którą świadczenie usług społeczeństwa informacyjnego podlega prawu państwa członkowskiego, na terytorium którego znajduje się siedziba usługodawcy. Jakkolwiek zasady tej nie stosuje się do zobowiązań z umów konsumenckich, wyjątek ten nie dotyczy telemedycyny, która – jak zauważono wyżej – jest usługą opieki zdrowotnej i jako taka wyłączona jest spod zakresu zastosowania przepisów dyrektywy 2011/83/UE[38]. W świetle art. 2 lit. c dyrektywy 2000/31/WE siedzibą usługodawcy jest miejsce, w którym faktycznie prowadzi on działalność gospodarczą przez czas nieokreślony.

Powyższe rozważania prowadzą do wniosku, że prawem właściwym do dokonania oceny w zarówno w zakresie kompetencji zawodowych podmiotu świadczącego usługi telemedyczne, jak i rozstrzygnięcia, czy przy świadczeniu usługi zachowane zostały wszelkie wymagane przez prawo standardy świadczenia opieki zdrowotnej (w zakresie ich jakości, norm bezpieczeństwa i należytej staranności, reguł deontologicznych itp.) jest prawo państwa członkowskiego, z którego terytorium podmiot medyczny prowadzi działalność.

2. Telemedycyna transgraniczna w świetle rozporządzenia Rzym I oraz rozporządzenia Rzym II

Rozważania w zakresie prawa właściwego dla przypadków odpowiedzialności cywilnej podmiotów medycznych powstałych na tle świadczenia usług telemedycznych wymagają pewnej systematyzacji. Po pierwsze, wskazać należy, że przypadki te, w zależności od charakteru stosunków

[35] *M. Kożuch*, [w:] *A. Zawidzka-Łojek*, *R. Grzeszczak*, *A. Łazowski*, Prawo Unii Europejskiej..., s. 540.

[36] Dz.Urz. UE L Nr 255, s. 22; dalej jako: dyrektywa 2005/36/WE.

[37] *V.L. Raposo*, Telemedicine: The legal framework (or the lack of it) in Europe, GMS Health Technology Assessment 2016, Nr 12, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4987488/#R46 (dostęp z 26.2.2018 r.).

[38] Zob. art. 3 ust. 3 lit. b dyrektywy 2011/83/UE w zw. z załącznikiem do dyrektywy 2000/31/WE.

prawnych łączących usługodawcę z pacjentem, objęte być mogą odmiennymi reżimami prawnymi[39]. W tym zakresie wyróżnić można takie sytuacje, w których odpowiedzialność przybierze charakter kontraktowy, i takie, w których odpowiedzialność ta będzie miała charakter pozaumowny (deliktowy). Wśród tych ostatnich wskazać można na przykład sytuacje, w których lekarz występuje jako pracownik zakładu opieki zdrowotnej i nie łączy go z pacjentem żaden stosunek umowny, a podjęcie przez niego leczenia następuje w ramach realizacji działalności zakładu. W przypadku wyrządzenia pacjentowi szkody zakład ponosi odpowiedzialność kontraktową, a lekarz – deliktową.

Po drugie, umowy o świadczenie usług telemedycznych, jak już wspomniano, mogą być umowami dwustronnie bądź jednostronnie profesjonalnymi. Oznacza to, że w zależności od tego, czy odbiorca usług występuje jako profesjonalista (np. inny podmiot medyczny w ramach konsultacji), czy też jako konsument, zastosowanie znajdą odmienne reguły odpowiedzialności.

Uwzględnienie powyższej klasyfikacji prowadzi do wniosku, że dla ustalenia prawa właściwego dla przypadków odpowiedzialności cywilnej podmiotów medycznych świadczących transgraniczne usługi telemedyczne zastosowanie znaleźć mogą różne regulacje kolizyjnoprawne: rozporządzenie Parlamentu Europejskiego i Rady (WE) Nr 593/2008 z 17.6.2008 r. w sprawie prawa właściwego dla zobowiązań umownych (Rzym I)[40] bądź rozporządzenie (WE) Nr 864/2007 Parlamentu Europejskiego i Rady z 11.7.2007 r. dotyczące prawa właściwego dla zobowiązań pozaumownych (Rzym II)[41].

Stosownie do brzmienia art. 1 rozporządzenia Rzym I przepisy tej regulacji stosuje się do zobowiązań umownych w sprawach cywilnych i handlowych powiązanych z prawem różnych państw. Fundamentalną zasadą systemów norm kolizyjnych odnoszących się do zobowiązań umownych realizowaną także przez rozporządzenie Rzym I jest zasada swobody wyboru prawa właściwego (art. 3 ust. 1). Jeśli strony umowy, będące profesjonalistami, nie skorzystały w tym zakresie z przyznanej im autonomii i nie dokonały wyboru, prawo właściwe określone będzie z uwzględnieniem wyliczonych w art. 4 łączników, co w kontekście transgranicznych umów o świadczenie usług telemedycncyh oznacza, że prawem właściwym będzie prawo państwa, w którym usługodawca ma miejsce zwykłego pobytu. Zasada swobody wyboru prawa doznaje pewnych modyfikacji na gruncie umów konsumenckich, tj. zawieranych z profesjonalistami przez osoby fizyczne w celu niezwiązanym z ich działalnością gospodarczą lub zawodową. Wybór taki nie może bowiem prowadzić do pozbawienia konsumenta ochrony przyznanej mu na podstawie przepisów bezwzględnie obowiązujących w państwie, którego prawo byłoby właściwe, gdyby strony nie dokonały wyboru (art. 6 ust. 2). W braku wyboru prawem właściwym będzie z kolei prawo państwa, w którym konsument ma miejsce zwykłego pobytu, pod warunkiem że przedsiębiorca wykonuje swoją działalność gospodarczą lub zawodową w tym państwie, lub w jakikolwiek sposób kieruje taką działalność do tego państwa (art. 6 ust. 1). W kontekście telemedycyny istotny jest sposób interpretacji działalności „kierowanej" do państwa członkowskiego. Usługi telemedyczne ze swej natury najczęściej reklamowane i oferowane są za pośrednictwem Internetu. Stąd należy mieć na uwadze dorobek orzeczniczy TS w zakresie rozumienia pojęcia działalności „kierowanej" do państwa członkowskiego, na terytorium którego konsument ma miejsce zwykłego pobytu za pośrednictwem globalnej sieci. Trybunał przyjął bowiem, że oprócz wszelkich wyraźnych form wyrażenia woli pozyskania konsumentów z tego państwa, należy każdorazowo uwzględnić także oznaki pośrednie (np. wprowadzenie na stronie internetowej opcji pozwalającej konsumentowi na używanie innego języka lub innej waluty)[42]. Rozstrzygnięcie, czy przedsiębiorca kieruje swoją działalność gospodarczą lub zawodową do państwa zwykłego pobytu konsumenta, ma istotne znaczenie praktyczne, jeśli bowiem przedsiębiorca ani nie wykonuje swojej działalności gospodarczej w tym państwie, ani w żaden sposób jej do niego nie kieruje, zastosowanie w zakresie prawa właściwego znajdą reguły ogólne. Oznacza to, że jak wspomniano powyżej, prawem właściwym będzie prawo państwa, w którym podmiot świadczący usługi telemedyczne ma miejsce zwykłego pobytu.

Normy kolizyjne w zakresie prawa właściwego dla zobowiązań pozaumownych zawarte w rozporządzeniu Rzym II stosuje się, zgodnie z brzmieniem art. 1 ust. 1 tego aktu, do zobowiązań pozaumownych w sprawach cywilnych i handlowych, powiązanych z prawami różnych państw. Pojęcie zobowiązania pozaumownego powinno być do celów rozporządzenia Rzym II pojmowane w sposób autonomiczny[43]. Stosownie bowiem do brzmienia art. 2 ust. 1 szkoda obejmuje wszelkie następstwa wynikające z czynu niedozwolonego, bezpodstawnego wzbogacenia, prowadzenia cudzych spraw bez zlecenia lub *culpa in contrahendo*. Na gruncie usług telemedycznych szczególne znaczenie przypisać należy zobowiązaniom obejmującym obowiązek naprawienia szkody powstałej wskutek dopuszczenia się przez osobę wykonującą zawód medyczny czynu niedozwolonego. Prawem właściwym dla przypadków odpowiedzialności deliktowej w myśl art. 4 ust. 1 rozporządzenia Rzym II jest prawo państwa, w którym powstała szkoda, niezależnie od tego, w jakim państwie

[39] *M. Nesterowicz*, Prawo medyczne, Toruń 2016, s. 84.
[40] Dz.Urz. UE L Nr 177, s. 6.
[41] Dz.Urz. UE L Nr 199, s. 40.
[42] Zob. wyrok TS z 7.12.2010 r., w sprawach połączonych C-585/08 i C-144/09, Pammer i Hotel Alpenhof, Zb. Orz. 2010, I-12527.
[43] *J. Gołaczyński*, Prawo prywatne międzynarodowe, Warszawa 2017, s. 267.

było zdarzenie powodujące szkodę, oraz niezależnie od tego, w jakim państwie występują skutki pośrednie tego zdarzenia. Oznacza to, że jeśli strony nie poddały zobowiązania pozaumownego innemu, wybranemu na warunkach określonych w art. 14 prawu, właściwe będzie prawo państwa, w którym przebywał pacjent w chwili doznania szkody, a nie prawo państwa, z terytorium którego świadczona była usługa.

3. Stosunek rozporządzenia Rzym I oraz rozporządzenia Rzym II do dyrektywy 2011/24/UE oraz dyrektywy 2000/31/WE w kontekście odpowiedzialności cywilnej podmiotów medycznych za szkody powstałe w związku ze świadczeniem transgranicznych usług telemedycznych

Reguły kolizyjne rozporządzenia Rzym I i rozporządzenia Rzym II w określonych sytuacjach prowadzą do wniosków *prima facie* sprzecznych z rozwiązaniami regulującymi prawo właściwe dla wykonywania usług telemedycznych, przewidzianymi w dyrektywie 2011/24/UE oraz dyrektywie 2000/31/WE.

Dla ilustracji posłużyć można się sytuacją, w której lekarz przebywający w państwie A, przeprowadzając teleoperację na pacjencie znajdującym się w chwili zabiegu w państwie B, nie dochowuje należytej staranności i dopuszcza się błędu terapeutycznego, w wyniku którego pacjent ponosi szkodę. Lekarza i pacjenta nie łączy stosunek umowny, a operacja jest wykonywana przez lekarza w wykonaniu obowiązków pracowniczych wobec zakładu opieki zdrowotnej. W takim wypadku powstaje pytanie: prawo którego z tych państw będzie właściwe z punktu widzenia odpowiedzialności lekarza? Na gruncie rozporządzenia Rzym II prawem właściwym dla rozstrzygnięcia o odpowiedzialności deliktowej lekarza będzie prawo tego państwa, w którym przebywał pacjent w chwili doznania szkody (państwa B). Tymczasem, zarówno dyrektywa 2011/24/UE, jak i dyrektywa 2000/31/WE nakazują, w zakresie świadczenia usług telemedycznych, stosowanie przepisów obowiązujących w państwie pobytu usługodawcy (państwa A).

Do zbliżonych wniosków prowadzi studium przypadku, w którym pacjent przebywający w państwie C (występujący w roli konsumenta) zawiera z lekarzem prowadzącym jednoosobową działalność gospodarczą (prywatną praktykę lekarską) w państwie D umowę o świadczenie usług z zakresu telekonsultacji. Lekarz oferuje swoje usługi za pośrednictwem reklamy radiowej emitowanej w państwie pobytu pacjenta. W wyniku zaniedbań lekarz dopuszcza się błędu diagnostycznego, w efekcie czego zaleca pacjentowi sposób leczenia nieodpowiedni dla jego schorzenia. W związku z długotrwałym prowadzeniem błędnej terapii stan pacjenta się pogarsza. Należy przyjąć, że o ile strony nie postanowiły inaczej, prawem właściwym dla odpowiedzialności kontraktowej lekarza za błąd medyczny będzie, na gruncie rozporządzenia Rzym I, prawo państwa, w którym konsument ma miejsce zwykłego pobytu, a zatem prawo państwa C. Podobnie jak w poprzednim przypadku, konkluzja ta zdaje się pozostawać w sprzeczności z postanowieniami dyrektywy 2011/24/UE i dyrektywy 2000/31/WE.

Na tym tle rodzi się pytanie, jaki jest wzajemny stosunek analizowanych regulacji. Należy przyjąć, że przepisy wskazanych dyrektyw, w zakresie, w jakim ustanawiają dla świadczeń telemedycznych zasadę państwa pochodzenia, nie wyłączają zastosowania przepisów rozporządzeń Rzym I i Rzym II[44]. Artykuł 4 dyrektywy 2011/24/UE ogranicza się do wyrażenia oczywistej zasady, że usługi opieki zdrowotnej powinny być świadczone zgodnie ze standardami przyjętymi w państwie, na terytorium którego prowadzi działalność podmiot medyczny[45]. Podobnie kształtuje się *ratio legis* art. 3 dyrektywy 2000/31/WE. W odmiennym przypadku podmiot świadczący usługi elektroniczne zmuszony byłby każdorazowo dostosować swoją działalność do regulacji prawnych państwa, na którego terytorium znajduje się odbiorca usługi, co byłoby obowiązkiem w istocie rzeczy niemożliwym do zrealizowania. Przyjęcie zasady państwa pochodzenia znacząco ułatwia usługodawcom funkcjonowanie na rynku usług elektronicznych i stanowi bodziec do większej aktywizacji na rynku wewnętrznym[46].

Powyższa konstatacja oznacza, że prawo właściwe dla odpowiedzialności cywilnej podmiotów świadczących transgraniczne usługi telemedyczne powinno być ustalane na podstawie przepisów rozporządzenia Rzym I (w przypadku odpowiedzialności kontraktowej) lub rozporządzenia Rzym II (w przypadku odpowiedzialności deliktowej). Jakkolwiek wskazane powyżej postanowienia dyrektywy 2011/24/UE i dyrektywy 2000/31/WE nie wpływają bezpośrednio na prawo właściwe, znajdą one zastosowanie dla potrzeb ustalenia czy, w określonych okolicznościach, podmiotowi medycznemu może zostać przypisana odpowiedzialność. Oznacza to, że jeżeli prawem właściwym jest prawo państwa innego niż państwo pobytu usługodawcy, przepisy obowiązujące na terytorium tego ostatniego muszą zostać wzięte pod uwagę przy ustalaniu, czy zachowane zostały wymagane przez to prawo standardy bezpieczeństwa, czy dochowano należytej staranności, czy zrealizowane zostały stosowne obowiązki informacyjne itp.[47].

[44] Komisja Europejska, Commission Staff Working Document..., s. 27.
[45] *Ibidem*.
[46] *C.A. Hernández Sánchez*, The Meaning of the Information Society Services in the E-Commerce Directive, University of Oslo 2005, s. 56, https://www.duo.uio.no/bitstream/handle/10852/20433/MeaningxofxInformationxSocietyxServicesxinxthexE-commercexDirective.pdf?sequence=2 (dostęp z 25.2.2018 r.).
[47] Komisja Europejska, Commission Staff Working Document..., s. 27.

W kontekście usług opieki zdrowotnej regulacje wyznaczające standardy postępowania i przyjęte reguły deontologiczne mają szczególne znaczenie, pozwalają bowiem na zakwalifikowanie określonego postępowania jako sprzecznego z zasadami sztuki medycznej i warunkują możliwość przypisania podmiotowi medycznemu odpowiedzialności za wyrządzoną szkodę. Choć standardy te na gruncie europejskim nie różnią się istotnie od siebie, dostrzec można pewne odrębności. Jakkolwiek większość z nich związana jest z przyjętym w poszczególnych państwach członkowskich systemem wartości (np. problematyka dopuszczalności aborcji, eutanazji), niektóre różnice istnieją w oderwaniu od sfery moralności (np. możliwość anonimowego uzyskania świadczeń opieki zdrowotnej, która dozwolona jest m.in. w Hiszpanii i Portugali, a zakazana m.in. w Finlandii i Włoszech)[48].

Taka postać dualizmu regulacyjnego, choć istotnie upraszcza obrót z punktu widzenia usługodawców, wpływa niekorzystnie na pozycję usługobiorców. Zamęt legislacyjny rodzi ponadto trudności związane z oceną przypadków, w których odpowiedzialność podmiotu medycznego pozostaje w związku ze świadczeniem usług opieki zdrowotnej niedopuszczalnych na gruncie prawa państwa pobytu pacjenta (np. różnorodne formy teleaborcji).

Podsumowanie

Choć telemedycyna niesie za sobą niewątpliwe korzyści i może istotnie poprawić funkcjonowanie systemów opieki zdrowotnej w Europie, w szczególności w kontekście niepokojących prognoz demograficznych starego kontynentu[49], usługi telemedyczne pozostają mało rozpowszechnione, a ich rynek charakteryzuje duże rozproszenie[50]. Ani liczne inicjatywy mające na celu popularyzację usług telemedycznych w państwach członkowskich, ani znaczące zaangażowanie finansowe Unii w rozwój technologii telemedycznej[51] nie doprowadziły do ostatecznego przełamania barier rozwoju tej dziedziny usług medycznych.

Telemedycyna dysponuje już dojrzałymi rozwiązaniami technicznymi, a nieustanna popularyzacja usług elektronicznych sprawia, że w dzisiejszym, zinformatyzowanym społeczeństwie powoli wzrasta też zainteresowanie cyfrowymi usługami medycznymi. Niemniej, wciąż zgoła czym innym jest w powszechnej świadomości zakup towaru konsumpcyjnego za pośrednictwem sieci Internet, a czym innym poddanie się skomplikowanemu zabiegowi medycznemu. Gdy w grę wchodzi ludzkie zdrowie i życie, sceptycyzm jest reakcją naturalną.

Nieufność pacjentów i osób wykonujących zawody medyczne do telemedycyny, w szczególności w wymiarze transgranicznym, pogłębia brak jednolitej regulacji prawnej. Harmonizacja na poziomie unijnym ma w istocie rzeczy charakter szczątkowy, a istniejące przepisy nie są jasne. Problem ten dostrzegalny jest m.in. na gruncie problematyki prawa właściwego dla przypadków odpowiedzialności cywilnej podmiotów medycznych.

W przeciwieństwie do prawnych barier rozwoju telemedycyny występujących w porządkach krajowych państw członkowskich, które mogą być i są systematycznie znoszone[52], bariery te na płaszczyźnie europejskiej są szczególnie trudne do wyeliminowania. Unia Europejska nie dysponuje bowiem instrumentarium odpowiednim do ujednolicenia zasad odpowiedzialności podmiotów medycznych za szkody wyrządzone przy leczeniu. Kompetencje w tym zakresie należą do wyłącznych kompetencji państw członkowskich, co oznacza, że pełna unifikacja tych zasad nie jest możliwa, a każdorazowo zastosowanie będą musiały znaleźć odpowiednie normy kolizyjne.

[48] *V.L. Raposo*, Telemedicine: The legal framework...

[49] Społeczeństwo starego kontynentu starzeje się w szybkim tempie. W latach 2006–2016 mediana wieku w UE wzrosła o 4,3 lat (średnio o 0,3 roku w skali roku), http://ec.europa.eu/eurostat/statistics-explained/index.php/Population_structure_and_ageing/pl (dostęp z 27.2.1018 r.).

[50] Komisja Europejska, Komunikat Komisji...

[51] *V.L. Raposo*, Telemedicine: The legal framework...

[52] Zob. np. Décret n° 2010–1229 du 19 octobre 2010 relatif à la télémédecine. Journal officiel de la République Française 2010; 245:13, https://www.legifrance.gouv.fr/eli/decret/2010/10/19/SASH1011044D/jo/texte (dostęp z 27.2.2018 r.); ustawa z 9.10.2015 r. o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw, Dz.U. poz. 1991 ze zm.

Słowa kluczowe: telemedycyna transgraniczna, Unia Europejska (UE), odpowiedzialność podmiotów medycznych, prawo właściwe

Cross-border telemedicine – law applicable to civil liability regarding medical malpractice under EU legal framework

Health services provided with use of innovative information and telecommunication technology have recently gained popularity in Europe. So-called telemedicine has the potential to become one of the pillars of health care systems – both on the domestic and European level. In this respect, particular attention should be paid to cross-border telemedicine services which – in the absence of European harmonization – are subject of great controversy, notwithstanding their undoubted beneficial effects. This paper provides an overview of the issue, notably in terms of European Union legal framework on telemedicine.

Keywords: cross-border telemedicine, European Union (EU), medical liability, law applicable.

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:

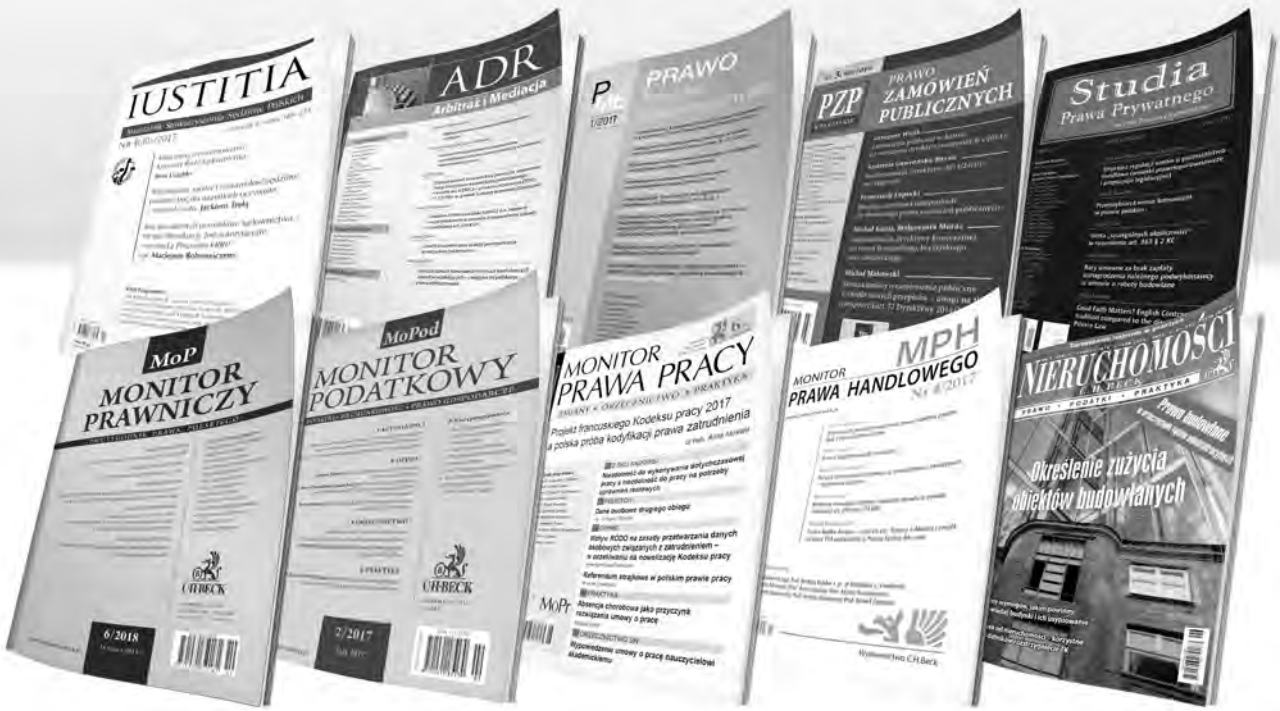
a. Expected indication of a legal act goes as follows: Journal of Laws of 2006, No. 28, item 456. The publishing body should only be provided when referring to the act for the first time. Then the name and date of the act (month – in words) shall be given in the body of the text (e.g. The Act of 13 April 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

Czasopisma
Prenumerata



- **Niezbędne informacje** o bieżących zmianach w prawie
- Przegląd **najistotniejszego orzecznictwa**
- **Obszerne dodatki tematyczne** – praktyczne omówienie problematycznych rozwiązań
- **Dedykowane seminaria** – prowadzone przez wybitnych specjalistów z poszczególnych dziedzin prawa – rabaty dla prenumeratorów

Zamów: tel. 22 311 22 22

C.H.BECK

www.czasopisma.beck.pl