PÓŁROCZNIK NAUKOWY
PRAWO MEDIÓW ELEKTRONICZNYCH

Redakcja:
Redaktor naczelny – prof. dr hab. Jacek Gołaczyński
Sekretarz redakcji – dr Dariusz Szostek
Redaktor numeru – dr Marek Leśniak

Rada programowa:
dr Marek Świerczyński, UKSW
dr Wojciech Wiewiórowski, UG
dr Grzegorz Sibiga, INP PAN
prof. dr. Andreas Wiebe, University of Göttingen
adwokat Xawery Konarski
dr hab. prof. nadzw. UWr. Włodzimierz Gromski
dr hab. prof. nadzw. UWr. Krzysztof Wójtowicz
prof. dr hab. Ryszard Jaworski, UW
radca prawny Jacek Wilczewski,
Kancelaria Prawna Grynhoff Woźny Wspólnicy
adwokat Artur Kmieciak
sędzia Jacek Czaja

Recenzenci:
dr hab. prof. UKSW Grażyna Szpor
dr hab. prof. nadzw. UMK Andrzej Adamski
dr hab. prof. UOp Piotr Stec,
dr hab. prof. UŚ Jacek Górecki,
dr hab. prof. nadzw. UŁ Sławomir Cieślak
prof. Richard Warner, Ph.D, IIT Chicago-Kent College of Law
dr hab. prof. UJ Ryszard Markiewicz
prof. em. dr. Wolfgang Kilian, University of Hanover
dr hab. prof. UŚ Kazimierz Zgryzek

Korekta językowa:
dr Agnieszka Kulik-Jęsiek

Okładka, skład i łamanie:
Kamil Ligienza

ISSN 2082-100X

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: ebiuletyncbke@prawo.uni.wroc.pl

Produkcja:
VNT Law & Communications Sp. z o.o.
ul. Norblina 84, 40-748 Katowice,
tel.: 32 352 42 00, faks: 32 352 42 01
mob.: 0 602 334 664 , 0 660 530 054
e-mail: vnt@vnt.com.pl, szkolenia@vnt.com.pl
www.vnt.com.pl

WPROWADZENIE

Szanowni Państwo,
Oddajemy Państwu do czytania kolejny numer czasopisma naukowego Prawo Mediów Elektronicznych. Od 2013r. będzie ukazywał się jako półrocznik. Stąd też, co prawda, zmniejszy się ilość publikowanych artykułów, ale zmieni się nieco charakter zamieszczanych tam artykułów. Zachęcimy bowiem do publikacji na łamach naszego czasopisma autorów zagranicznych, bedziemy także zamieszczać w większym stopniu głosy do orzeczeń sądów polskich i europejskich. Stale bedziemy informowali o aktualnych pracach legislacyjnych dotyczących nowych technologii.

Zachęcam zatem do lektury
prof. dr hab. Jacek Gołaczyński

Zasady publikacji:
Redakcja prosi o przysyłanie materiałów do publikacji w biuletynie zarówno w formie elektronicznej: pocztą elektroniczną lub na dyskietkach, jak również w formie wydruku. Tekst powinien być podpisany własnoręcznie przez autora. Tekst powinien być sporządzony w formacie MS Word, z zachowaniem interlinii oraz marginesów szerokości 3 cm. Tekst nie powinien przekraczać 15 stron znormalizowanego formatu A-4. Redakcja zastrzega sobie możliwość dokonywania skrótów, poprawek stylistycznych, językowych interpunkcyjnych. Prosimy autorów o podawania także swoich adresów prywatnych, numerów telefonów, adresów poczty elektronicznej, tytułów naukowych, zajmowanych stanowisk lub pełnionych funkcji, a także adresów właściwych urzędów skarbowych, numerów kont bankowych tych urzędów oraz danych osobowych potrzebnych do deklaracji podatkowej. Artykuły i recenzje niesamodzielnych pracowników naukowych będą poddawane recenzji.

SPIS TREŚCI

SPIS TREŚCI

Gabriela Bar
Charakter prawny komunikatów typu „push notification" **5**
The legal nature of „Push Notification" type messages

Agnieszka Lewestam
Umowa factoringowa jako przykład umowy nienazwanej mieszanej **10**
Factoring agreement as an example of an innominate mixed contract

Mateusz Szkuta
Inkorporacja wzorców umownych w postaci elektronicznej **12**
Incorporation of standard contracts patterns in electronic form

Beata Wójtowicz-Woźniczka
Elektroniczne postępowanie klauzulowe – kolejny etap informatyzacji wymiaru sprawiedliwości **17**
Electronic enforcement warrant – next phase of computerization of Justice

Janusz Zagrobelny
Podpis elektroniczny w postępowaniu karnym – glosa krytyczna do postanowienia SN z dnia 26 marca 2009 r. (sygn. akt I KZP 39/08) **20**
Electronic Signature in criminal proceedings

Dan Jerker B. Svantesson
Private International Law and the Internet – An Australian Perspective and Beyond **23**
Międzynarodowe prawo prywatne a Internet – perspektywy australijskie

Maria Kaczorowska
Konferencja naukowa „Ochrona publicznych baz danych", Warszawa, 6 listopada 2013 r. **31**
Scientific conference „Security of public databases"

ARTYKUŁY

GABRIELA BAR

CHARAKTER PRAWNY KOMUNIKATÓW TYPU „PUSH NOTIFICATION"

Technologie i urządzenia mobilne z każdym rokiem zyskują na popularności, znajdując zastosowanie w działalności dużych i małych przedsiębiorstw z różnych branż, a także służąc jako narzędzie rozrywki. Pierwszy komputer mieszczący się w dłoni, czyli palmtop (ang. *palm* – wewnętrzna strona dłoni, *top* – wierzch) został zaprezentowany podczas pokazów Consumer Electronics Show (CES)[1] w Las Vegas w 1992 r. Wówczas też użyto dla niego nazwy *Personal Digital Assistant* (PDA). Z kolei pierwszy smartfon (ang. *smartphone*) został zaprezentowany przez IMB w 1993 r. na targach COMDEX (ang. *Computer Dealer's Exhibition*)[2].

Obecnie rynek urządzeń i systemów mobilnych jest jednym z najdynamiczniej rozwijających się rynków branży elektronicznej.[3] Smartfony łączą w sobie funkcje telefonu komórkowego i palmtopa, umożliwiając zarówno prowadzenie kalendarza firmy, odbieranie i wysyłanie poczty elektronicznej, korzystanie z przeglądarki, robienie zdjęć, nagrywanie filmów, a także zarządzanie informacjami osobistymi (ang. *Personal Information Management*) i odczytywanie dokumentów w formatach Microsoft Office, PDF, Open Office i Libre Office. W ciągu dwóch ostatnich lat udział smartfonów w rynku wzrósł z 35 do 56 procent[4].

Rosnącą popularnością cieszą się tablety – przenośne komputery o rozmiarach większych niż telefon komórkowy lub palmtop, z dużym dotykowym ekranem, doskonale nadające się do korzystania z programów multimedialnych i gier. W III kwartale 2013 r. na rynek trafiło 47,6 mln tabletów, czyli o 7 procent więcej niż w poprzednim kwartale i o 36,7 procent więcej niż w III kwartale 2012 r.[5]

Wraz z rozwojem tego rodzaju urządzeń pojawiają się nowe aplikacje mobilne – zarówno użytkowe, jak i czysto rozrywkowe. Często aplikacje te stanowią inną wersję rozwiązań wykorzystywanych w komputerach stacjonarnych lub przenośnych.

Usługi poczty elektronicznej, serwisów społecznościowych, e-bankowości, wyszukiwarek, rezerwacji biletów (teatralnych, lotniczych) dostępne są już powszechnie w wersji na smartfony, tablety i palmtopy. Istnieje także duże zapotrzebowanie na mobilne aplikacje dla biznesu, oferowane przez duże korporacje[6], ale także tworzone na zamówienie przez niezależnych deweloperów[7]. Ogromną popularnością wśród graczy cieszą się Google Play i Apple Store, oferujące m.in. tysiące gier na telefony komórkowe.

Rosnąca konkurencja sprawia, że coraz częściej nieodłącznym elementem aplikacji na urządzenia mobilne są tzw. *push notifications*, czyli powiadomienia wysyłane do użytkownika danego urządzenia z serwera usługodawcy, niebędącego dostawcą usług telekomunikacyjnych ani dostawcą usług internetowych. *Push notifications* mogą stanowić rodzaj reklamy lub informacji o promocjach w serwisie usługodawcy, zachęcać do powrotu do korzystania z danej aplikacji (najczęściej gry). Komunikaty tego typu często stanowią reklamę behawioralną, kierowaną do użytkownika konkretnego urządzenia. *Push notifications* mogą także stanowić element danego oprogramowania, służący poprawie jego funkcjonalności, np. w postaci przypomnienia o konieczności jego aktualizacji lub prośby o wypełnienie ankiety oceny produktu.

Omawiane powiadomienia mogą pojawiać się na urządzeniu mobilnym użytkownika, niezależnie od uruchomienia przez niego aplikacji, z której pochodzą. W związku tak dużym ryzykiem naruszania prywatności użytkownika zaawansowane technologicznie urządzenie mobilne, np. smartfony, posiadają zazwyczaj funkcję uzyskiwania zgody użytkownika na otrzymywanie komunikatów typu *push notifications*, użytkownik jest zatem chroniony przed ingerencją „zewnętrznych" aplikacji już z poziomu dostawcy systemu operacyjnego swojego smartfona (Android, Windows Phone).

Ochrona taka nie jest jednak wystarczająca, gdyż zależy od rodzaju urządzenia i jego ustawień. Tymczasem istotna jest odpowiedź na pytanie o dopuszczalność wysyłania z serwera usługodawcy powiadomień typu *push* i o obowiązki po jego stronie w zakresie uzyskania zgody usługobiorcy na otrzymywanie takich komunikatów.

W zależności od rodzaju komunikatu, do oceny dopuszczalności posługiwania się technologią *push notifications* na gruncie polskiego prawa, zastosowanie znajdą przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (usude)[8], w szczególności art.5 – 8 usude oraz art.16 – 22 usude, a w odniesieniu do przekazów o charakterze reklamowym także art.9 i 10 usude. W zakresie ochrony prywatności usługobiorcy odwołać należy się także do ustawy z dnia 29 sierpnia 1997 r. o ochro-

[1] Oficjalna strona internetowa CES: http://www.cesweb.org/, 22.11.2013r.

[2] Oficjalna strona organizatora targów: http://www.interop.com/, 22.11.2013r.

[3] W porównaniu do roku ubiegłego, Android (oprogramowanie na urządzenia mobilne Google'a) osiągnął sprzedaż większą o ponad 63% (204,4 miliona urządzeń), a udział w rynku wzrósł o ponad 6% do 81,3%. System mobilny Microsoftu – Windows Phone - podwoił swój udział na rynku i ma już 4%. Sprzedano także prawie trzykrotnie więcej urządzeń, niż w analogicznym okresie w roku 2012. Więcej: http://www.dobreprogramy.pl/Statystyki-urzadzen-mobilnych-w-Q3-2013-Android-kontynuuje-dominacje-a-Windows-Phone-podwaja-udzial-w-rynku,News,49002.html, 24.11.2013r.

[4] Zob. http://media2.pl/telekomunikacja/106547-Rynek-mobile-2013-Urzadzen-mobilnych-wiecej-niz-ludzi-infografika.html, 24.11.2013r.

[5] Zob. http://tech.wp.pl/kat,130050,title,Swiatowy-rynek-tabletow-w-3Q2013-wedlug-szacunkow-IDC,wid,16135709,wiadomosc.html?ticaid=111b95, 24.11.2013r.

[6] Zob. np. http://www.cisco.com, 24.11.2013r.

[7] App Store Volume Purchasing Program for Business, http://www.apple.com/business/vpp/, 24.11.2013r.

[8] Dz. U. Nr 144, poz. 1204 z późn. zm.

nie danych osobowych (uodo)[9] – w związku z brzmieniem art. 16 ust. 1 usude.

Podmiot posługujący się powiadomieniami typu *push* winien spełniać wymogi stawiane usługodawcy w rozumieniu usude w zakresie obowiązków informacyjnych (zarówno o prowadzonej działalności, jak i zagrożeniach związanych z korzystaniem z usługi oraz funkcji i celu oprogramowania lub danych niebędących składnikiem treści usługi, wprowadzanych przez usługodawcę do systemu teleinformatycznego, którym posługuje się usługobiorca), zgodnie z art. 5 i 6 usude[10], a także w zakresie zapewnienia użytkownikowi poufności i bezpieczeństwa (art. 7 usude).[11] Wprawdzie usude nie daje usługobiorcy możliwości zgłoszenia sprzeciwu wobec użycia oprogramowania niebędącego składnikiem treści usługi, jednakże zgodnie z obowiązującym od 22 marca 2013r. nowym art. 173 Prawa telekomunikacyjnego[12] usługodawca winien uzyskać zgodę użytkownika na zainstalowanie w jego urządzeniu plików *cookies* oraz na zbieranie dzięki nim informacji o aktywności użytkownika. W związku z tym, że „ciasteczka" mogą zawierać rozmaite rodzaje informacji o użytkowniku danej strony WWW lub aplikacji oraz „historii" jego łączności z danym serwerem, zazwyczaj wykorzystywane są do automatycznego rozpoznawania użytkownika, dzięki czemu serwer usługodawcy może wygenerować przeznaczony dla niego komunikat lub reklamę. Umożliwia to tworzenie spersonalizowanych serwisów WWW, obsługi logowania, „koszyków zakupowych" w internetowych sklepach itp. Z tego powodu prawo europejskie dopuszcza stosowanie *cookies*[13]. Zgoda na korzystanie z *cookies* może być wyrażona w sposób niejako dorozumiany - poprzez ustawienia przeglądarki bądź aplikacji, z której użytkownik korzysta. Niemniej w takiej sytuacji usługodawca musi uprzednio poinformować o stosowaniu *cookies* – w sposób jasny i wyczerpujący, aby użytkownik mógł podjąć świadomą decyzję o działaniach, które mogłyby skutkować nieuprawnionym przechowywaniem danych lub dostępem do nich[14].

Oferując usługę elektroniczną, np. możliwość pobrania gry na telefon komórkowy usługodawca obowiązany jest posługiwać się regulaminem świadczenia usług drogą elektroniczną, który określa nie tylko rodzaje i zakres oferowanych usług, ale także m.in. wymagania techniczne niezbędne do współpracy z systemem teleinformatycznym, którym posługuje się usługodawca (art. 8 ust. 3 usude)[15]. Z regulaminu usługodawcy wynikać powinno, czy *push notifications* są komponentem oferowanej usługi i w jaki sposób ingerują w urządzenie użytkownika.

Przyjąć należy, iż instalując dane oprogramowanie użytkownik godzi się na jego komponenty, akceptując regulamin usługodawcy oraz warunki licencji na korzystanie z danego oprogramowania. Dochodzi zatem do zawarcia umowy pomiędzy użytkownikiem i dostawcą aplikacji, zazwyczaj z użyciem wzorca umownego, jakim jest regulamin świadczenia usług drogą elektroniczną (por. art.384 k.c.)[16].

Ocena charakteru prawnego powiadomień wysyłanych użytkownikowi przez zainstalowaną przez niego aplikację winna odbywać się wszakże z uwzględnieniem przepisów dotyczących informacji handlowej (art.9 i 10 usude). *Push notifications* mają w dużej mierze charakter reklamy lub zachęty do skorzystania z usługi elektronicznej. Tego typu zachęty przybierają często formę powiadomienie o prezencie (*gift notification*) w stylu"You've just got a gift!", co zazwyczaj będzie uznane za formę akcji promocyjnej usługodawcy.

Pojęcie „informacji handlowej" zostało zdefiniowane w art.2 pkt 2 usude jako każda informacja przeznaczona bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumienie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi.[17]

Definicja powyższa jest neutralna technologicznie, dotyczy zatem wszystkich komunikatów o charakterze reklamowym udostępnianych drogą elektroniczną, zarówno w postaci wiadomości e-mail, SMS, MMS, informacji przesyłanych przez komunikatory internetowe, serwisy społecznościowe, strony internetowe[18], a także – komunikatów wysyłanych z serwera usługodawcy bezpośrednio na urządzenie użytkownika, jak *push notifications*.

Informacja handlowa musi być wyraźnie wyodrębniona i oznaczona w sposób niebudzący wątpliwości, że jest to informacja handlowa. Oznaczenie informacji jako handlowej może bowiem ochronić usługobiorcę przed niekorzystnymi decyzjami gospodarczymi[19], ponadto zaś pozwala to usługobiorcy na usunięcie takiego komunikatu, jeżeli nie chce on korzystać z oferowanej promocji.

Takie ujęcie znajduje odzwierciedlenie w regulaminach serwisów dla deweloperów aplikacji mobilnych, które wymagają od

[9] Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.

[10] Na ten temat: R. Wójcik, Świadczenie usług drogą elektroniczną, [w:] W. Mendys (red.), Prawne aspekty e-biznesu, Rzeszów 2005, s. 45-51; G. Rączka, Ochrona usługobiorcy usług elektronicznych, Toruń 2007, s. 189 i nast.; P. Litwiński, [w:] P. Podrecki (red.) Prawo Internetu, Warszawa 2004, s. 195.

[11] Na ten temat: X. Konarski, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, Warszawa 2004, s. 100 i nast., P. Litwiński, [w:] P. Podrecki (red.) Prawo…, s. 196.

[12] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.).

[13] Zob. Dyrektywę 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniającą dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów (Dz. Urz. UE L 337/11 z 18.12.2009r.).

[14] Por. przypisy 28 oraz 65 do 67 preambuły dyrektywy 2009/136/WE.

[15] Na ten temat: D. Lubasz, Handel elektroniczny. Bariery prawne, Warszawa 2013, Lexis.pl, Rozdział III, sekcja 3.1.1.5.

[16] Na temat stosunku art. 8 ust. 1 pkt 2 usude do art. 384 § 4 k.c. zob. G. Rączka, Ochrona konsumentów w usługach świadczonych drogą elektroniczną, PPH 2005, nr 7, s. 34; X. Konarski, Komentarz..., s. 104; W. Kocot, Wpływ Internetu na prawo umów, Warszawa 2004, s. 246.

[17] Na temat definicji reklamy, informacji, informacji handlowej zob. np. G. Rączka, Ochrona usługobiorcy usług elektronicznych, Toruń 2007, s. 52-59; S. Stanisławska-Kloc, Świadczenie usług drogą elektroniczną - aspekty konsumenckie, [w:] E. Nowińska, P. Cybula (red.), Europejskie prawo konsumenckie a prawo polskie, Kraków 2005, s. 266; A. Malarewicz, Konsument a reklama. Studium cywilnoprawne, Warszawa 2009, s. 96-100; D.E. Harasimiuk, Zakazy reklamy towarów w prawie europejskim i polskim, Warszawa 2011, s. 38-39.

[18] K. Kowalik-Bańczyk, [w:] J. Gołaczyński (red.), Ustawa o świadczeniu usług drogą elektroniczną, Warszawa 2009, s. 99.

[19] Zob. Raport Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego Pierwszy raport o stosowaniu dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) z 21 listopada 2003 r., COM (2003) 702 final, s. 9.

twórców tych aplikacji, aby przy instalacji danej aplikacji wyświetlała się informacja dla użytkownika, w jaki sposób dana aplikacja używa reklam[20], a także, aby reklamy nie symulowały interfejsu użytkownika, żadnej aplikacji ani powiadomień i ostrzeżeń systemowych. Niedozwolone jest zmuszanie użytkownika do kliknięcia reklamy lub przesłania danych osobowych w celach marketingowych, by mógł on w pełni korzystać z aplikacji. We wszystkich reklamach pełnoekranowych należy umieścić dobrze widoczny i łatwo dostępny element umożliwiający zamknięcie reklamy bez żadnych konsekwencji lub niezamierzonego kliknięcia[21].

Zgodnie z wymogami art.9 ust.2 pkt 1 usude należy przyjąć, iż *push notification* o charakterze reklamowym musi zawierać oznaczenie podmiotu, na którego zlecenie jest rozpowszechniany oraz jego adresy elektroniczne. Oznaczenie podmiotu zlecającego rozpowszechnienie informacji handlowej może nastąpić w sposób bezpośredni poprzez wskazanie, np. imienia i nazwiska, firmy lub nazwy, pod którą prowadzi działalność gospodarczą, bądź w sposób pośredni poprzez zamieszczenie linku do strony internetowej[22]. Wskazanie adresu elektronicznego obejmuje zarówno podanie adresu poczty elektronicznej, jak i adresów stron internetowych. Wymóg powyższy – w odniesieniu do informacji handlowej mającej postać wiadomości e-mail – zostanie spełniony także wówczas, gdy adres elektroniczny nie zostanie wprawdzie dodatkowo podany w treści wiadomości, lecz pojawiać się będzie jako adres odbiorcy podczas odpowiedzi na wiadomość e-mail. Dopuszczalna jest też sytuacja, gdy adres elektroniczny będzie jednocześnie oznaczeniem podmiotu zlecającego rozpowszechnianie informacji handlowej, jeżeli zawiera nazwę przedsiębiorstwa lub imię i nazwisko usługodawcy[23]. Ze względu na nietypową formę informacji handlowej w postaci *push notification* (komunikat, który wyświetla się niejako „jednorazowo", co do którego należy podjąć decyzje o kliknięciu bez możliwości zapisania go i przeczytania w czasie późniejszym), informacje wymagane na podstawie art.9 ust.2 pkt 1 usude muszą pojawić się w jego treści – najczęściej w postaci odesłania (link) do strony internetowej usługodawcy.

Regulacja art.9 ust.2 pkt 2 usude wymaga, aby informacja handlowa zawierała wyraźny opis form działalności promocyjnej, np. obniżki cen, nieodpłatne świadczenia pieniężne lub rzeczowe i inne korzyści związane z promowanym towarem, usługą lub wizerunkiem. W przypadku *push notifications* będą to zazwyczaj: premie oraz prezenty, promocyjne konkursy lub gry. Warunki skorzystania z tego rodzaju promocji, w tym okres obowiązywania, zakres i warunki przystąpienia, muszą być sformułowane w sposób zrozumiały dla odbiorcy i niebudzący wątpliwości[24]. Nie wyklucza to jednak możliwości odesłania usługobiorcy poprzez hiperłącze do szczegółowych warunków promocji opublikowanych na stronie internetowej usługodawcy. W taki sam sposób informacja handlowa może odsyłać do informacji mogących mieć wpływ na określenie zakresu odpowiedzialności stron (art.9 ust.2 pkt 3 usude)[25].

Podkreślenia wymaga, iż mimo zgodności z przepisami art. 9 ust. 1 i 2 usude informacja handlowa może stanowić czyn nieuczciwej konkurencji (art. 9 ust. 3 usude)[26]. Możliwy jest także zbieg roszczeń z obu ustaw: usude oraz ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[27]. Istotne jest zatem, aby usługodawca wysyłający powiadomienia typu *push* na urządzenie użytkownika, działał zgodnie z regulacjami dotyczącymi uczciwej reklamy (w szczególności art.16 ustawy o zwalczaniu nieuczciwej konkurencji)[28].

Regulaminy największych platform dla developerów tworzących aplikacje na telefony komórkowe wprowadzają liczne ograniczenia co do możliwości ingerencji aplikacji w urządzeniu użytkownika bez jego wiedzy i zgody, zwłaszcza jeśli chodzi o przesyłanie komunikatów o charakterze reklamowym. W szczególności zakazane jest, aby aplikacje wyświetlały reklamy w postaci powiadomień systemowych na urządzeniu użytkownika, chyba że powiadomienia te pochodzą z integralnej funkcji zapewnianej przez zainstalowaną aplikację (np. aplikację linii lotniczej, która informuje użytkowników o ofertach specjalnych). Jeśli aplikacja wprowadza zmiany za wiedzą i zgodą użytkownika, to musi on dokładnie wiedzieć, która aplikacja to zrobiła, a także móc łatwo wycofać zmiany bądź całkowicie odinstalować aplikację[29].

Na gruncie usude warunkiem przesłania informacji handlowej do oznaczonej osoby jest jej uprzednie „zamówienie" przez odbiorcę (model *opt-in*)[30]. Niezamawiane informacje handlowe są zakazane na podstawie art. 10 usude[31]. Polskie przepisy nie przewidują wyjątków od tej zasady, dopuszczonych w dyrektywie o prywatności i łączności elektronicznej[32]. Przepis art. 13 ust. 2 tej dyrektywy stanowi, że w wypadku istnienia kontaktów handlowych pomiędzy stronami (np. umowy pomiędzy usługodawcą a zarejestrowanym na portalu gier mobilnych użytkownikiem) usługodawcy wolno przesyłać – bez konieczności uzyskania zgody odbiorcy – informacje handlowe drogą elektroniczną pod warunkiem zapewnienia odbiorcy możliwości wyrażenia sprzeciwu[33]. Takiej alternatywy nie daje usude.

Zgoda na przesyłanie *push notifications* o charakterze reklamowym nie może być zgodą domniemaną (art.4 usude) i winna obejmować wyraźnie upoważnienie usługodawcy do przesyłania informacji handlowej. Może być udzielona w dowolnej formie, w tym poprzez zaznaczenie odpowiednich pól wyboru w formularzu na stronie internetowej usługodawcy lub poprzez podanie numeru telefonu odbiorcy komunikatów[34].

[20] www.developer.android.com, 22.11.2013r.

[21] Zob. http://play.google.com/about/developer-content-policy.html, 24.11.2013r.

[22] M. Namysłowska, [w:] D. Lubasz (red.), M. Namysłowska (red.), Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw, Warszawa 2011, Lexis.pl 2013 - komentarz do art. 9 usude.

[23] Ibidem.

[24] A. Frań, Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Lex 2002, komentarz do art. 9 usude.

[25] M. Namysłowska, [w:] D. Lubasz (red.), M. Namysłowska (red.), Świadczenie usług…, Lexis.pl 2013 - komentarz do art. 9 usude.

[26] K. Kowalik-Bańczyk, [w:] J. Gołaczyński (red.), Ustawa o świadczeniu..., s. 107.

[27] Dz. U. Nr 47, poz. 211 z późn. zm.

[28] Więcej na ten temat: M. Namysłowska, [w:] D. Lubasz (red.), M. Namysłowska (red.), Świadczenie usług…, Lexis.pl 2013 - komentarz do art. 9 usude.

[29] Por. Warunki usługi Google Play, https://play.google.com/intl/pl_pl/about/play-terms.html, 22.11.2013r.

[30] Model opt-out wymaga bowiem aktywności odbiorcy w postaci wyrażenia sprzeciwu wobec otrzymywania informacji handlowych i nie zapobiega otrzymywaniu pierwszej niezamówionej informacji handlowej. Na ten temat: D. Kasprzycki, Spam, czyli niezamawiana komercyjna poczta elektroniczna. Zagadnienia cywilnoprawne, Kraków 2005, s. 61-69.

[31] Więcej na ten temat: D. Kasprzycki, Spam…, s. 176 i 177.

[32] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (Dz. U. UE z 31 lipca 2002 r., L 201/37).

[33] X. Konarski, Komentarz…, s. 116.

[34] Por. P. Litwiński, [w:] P. Podrecki (red.), Prawo…, s. 188.

Istotną kwestią pojawiającą się z związku z korzystaniem przez usługodawców z technologii *push notifications* są zasady ochrony prywatności, w tym - danych dotyczących usługobiorcy, w szczególności takich jak: imię i nazwisko, adres zamieszkania, adresy elektroniczne, numer telefonu, adres IP, dostawca usług internetowych, system operacyjny, rodzaj wykorzystywanej przeglądarki, częstotliwość korzystania z aplikacji, rodzaj odwiedzanych stron internetowych i częstotliwość tych odwiedzin oraz tzw. *clickstream*[35].

Zagadnienia te są szczególnie ważne w kontekście zbierania o użytkowniku urządzenia mobilnego informacji mających służyć przygotowaniu i skierowaniu do niego spersonalizowanych komunikatów reklamowych (reklama behawioralna, profilowanie).

Profilowanie zdefiniować można jako zbieranie i zestawianie informacji na temat określonej osoby, a następnie traktowanie tej osoby na podstawie utworzonego profilu. Specyfika sieci komputerowych pozwala na stosunkowo łatwe pozyskiwanie i zestawianie informacji o tej samej osobie, co jest szczególnie użyteczne z punktu widzenia prowadzenia działalności reklamowej w Sieci[36].

Kwestię korzystania z danych usługobiorcy, zarówno podanych przez niego, jak i zebranych poprzez obserwację jego aktywności w Sieci, w trakcie korzystania, a także po zakończeniu korzystania z usługi regulują art.18 i 19 usude. Przepisy te zostawiają usługodawcom wąski margines swobody wykorzystania informacji o użytkowniku bez jego zgody.

Do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, bez zgody usługobiorcy, mogą być zestawiane wyłącznie dane eksploatacyjne, pod warunkiem usunięcia wszelkich oznaczeń identyfikujących usługobiorcę, zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca (anonimizacja danych).

Danymi eksploatacyjnymi są, zgodnie z art.18 ust.5 usude, dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną:

- oznaczenia identyfikujące usługobiorcę nadane mu przez usługodawcę[37];
- oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca, np. numer telefonu, numer IMEI *(ang. International Mobile Equipment Identity)* używany przez sieci GSM do identyfikacji urządzenia mobilnego, adres karty sieciowej MAC (ang. Medium Access Control) oraz adres IP identyfikujący dany system teleinformatyczny;
- informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną, tj. dane o połączeniach pomiędzy urządzeniami komputerowymi, ich adresy IP, daty i czas trwania połączenia, rodzaj połączeń;
- informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną, np. adresy przeglądanych stron internetowych, zapisy wysyłanych wiadomościach SMS i wiadomości poczty elektronicznej, informacje o korzystaniu z usług dostarczane przez pliki *cookies*.

Należy zauważyć, że dane eksploatacyjne, nie będąc danymi osobowymi, mogą uzyskać charakter „osobowy", na skutek ich powiązania z konkretną osobą fizyczną. Takie powiązanie wystąpi, gdy tożsamość osoby fizycznej można określić bezpośrednio lub pośrednio. Poprzez identyfikację należy przy tym rozumieć możliwość fizycznego wskazania danej osoby[38]. Na skutek takiego powiązania powstaną profile użytkowników, które można określić jako identyfikowane, służące zazwyczaj kierowaniu do konkretnego odbiorcy spersonalizowanych komunikatów, zachęcających do skorzystania z usługi lub powrotu do korzystania z aplikacji. Takie profile mogą być tworzone wyłącznie za zgodą usługobiorcy. Powstają one bowiem poprzez zestawianie m.in. informacji pozwalających na ustalenie tożsamości osoby, do której się odnoszą lub informacji na temat systemu teleinformatycznego, z którego osoba ta korzysta.

Wobec regulacji art.19 ust.4 usude w związku z art.18 ust.4 i 5 usude bez zgody usługobiorcy mogą powstawać wyłącznie tzw. profile nieidentyfikowalne, na podstawie których nie można ustalić, kogo konkretnie one dotyczą. Należy przy tym podkreślić, że zabroniona jest nie tylko identyfikacja konkretnego usługobiorcy (strony umowy zawieranej za pomocą środków komunikacji elektronicznej), ale także systemu teleinformatycznego, z którego usługobiorca korzysta. Oznacza to konieczność usunięcia przy tworzeniu profili nieidentyfikowanych, zarówno danych takich jak: imię, nazwisko, PESEL, adres zamieszkania, adres elektroniczny, ale także login, adres IP, numer karty sieciowej i numer telefonu[39].

W odniesieniu do danych w sieciach komputerowych sporne jest, czy charakter „osobowy" mają dane pozwalające namierzyć, odnaleźć i kontaktować się z użytkownikiem, co miałoby znaczenie dla kwalifikacji informacji takich jak: adres e-mail, numer telefonu komórkowego i adres IP[40]. Najwięcej kontrowersji budzi adres IP, który może, ale nie musi zaliczać się do danych osobowych. W sytuacji, gdy jest on na stałe lub na dłuższy okres czasu przypisany do konkretnego urządzenia, które przypisane jest z kolei konkretnemu użytkownikowi, należy uznać, że stanowi on daną osobową. Niemniej adres IP będzie uznawany za dane osobowe jedynie wówczas, gdy podmiot przetwarzający adres IP ma jednocześnie dostęp do danych łączących adres IP z innymi danymi identyfikującymi osobę. Do czasu, gdy podmiot nie uzyska pewności, że sam nie jest w stanie łączyć adresu IP z innymi danymi identyfikującymi osobę, powinien zabezpieczać adres IP tak jakby był on daną osobową[41].

[35] Por. regulamin Apple'a na stronie internetowej: http://www.apple.com/privacy/, 21.11.2013r., który pozwala na gromadzenie tego rodzaju danych, a następnie wykorzystywanie ich do analizy trendów na rynku usług elektronicznych, zachowania użytkownika i jego preferencji oraz tworzenia reklam behawioralnych.

[36] P. Litwiński, [w:] P. Podrecki (red.), Prawo…, s. 230.

[37] Do oznaczeń identyfikujących usługobiorcę należy zaliczyć oznaczenia przydzielane przez usługodawcę, np. numery identyfikacyjne. Nie jest takim oznaczeniem login usługobiorcy, który jest przez niego samego wybrany w celu zarejestrowania się w danym serwisie. Zob. K. Klafkowska-Waśniowla [w:] D. Lubasz – komentarz do art. 18 usude

[38] P. Barta, P. Litwiński, Ustawa o ochronie…, s. 93. Zob. także art. art. 6 ust. 2 uodo, zgodnie z którym 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: fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

[39] K. Klafkowska – Waśniowska, [w:] D. Lubasz (red.), M. Namysłowska (red.), Świadczenie usług…, Lexis.pl 2013 - komentarz do art. 19 usude.

[40] Zob. P. Barta, P. Litwiński, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2009 s. 94-95.

[41] Stanowisko GIODO w sprawie Czy adres IP komputera należy do danych osobowych?, http://www.giodo.gov.pl/319/id_art/2258, 22.11.2013r. Por. także opinię Grupy Roboczej ds. Ochrony Danych, powołanej przez Parlament Europejski i Radę Europejską, która uznała

W związku z treścią art. 19 ust. 5 usude zakazane jest także zestawianie danych osobowych usługobiorcy z przybranym przez niego pseudonimem, który również w określonych warunkach może pozwolić na identyfikację danego użytkownika[42].

W świetle powyższego należałoby uznać, że spersonalizowane komunikaty typu *push* wykorzystujące profilowanie wymagają zgody użytkownika urządzenia mobilnego na ich otrzymywanie. Nie ulega bowiem wątpliwości, iż komunikaty tego rodzaju mają sens w zasadzie tylko wówczas, gdy nawiązują do aktywności użytkownika w Sieci i do jego preferencji. Z kolei wysłanie *push notification* wymaga zestawienia danych o owej aktywności i preferencjach z danymi, które można uznać za dane osobowe użytkownika, w szczególności numerem telefonu lub adresem elektronicznym, ewentualnie adresem IP. Zgoda użytkownika winna być udzielona usługodawcy, nie zaś poprzez ustawienia danego urządzenia mobilnego, gdyż to usługodawca jest podmiotem odpowiedzialnym za przetwarzanie danych usługobiorcy i tworzenie profile użytkownika[43].

Skoro zgoda usługobiorcy wymagana do:

– przesyłania informacji handlowych (art.10 ust.2 usude),
– przetwarzania danych osobowych usługobiorcy – do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców, także po zakończeniu świadczenia usługi drogą elektroniczną (art.18 ust.4 i art.19 ust.2 pkt 2 usude),
– nieusuwania oznaczeń identyfikujących usługobiorcę w ramach przetwarzania danych (art.19 ust.4 u.ś.u.d.e.), musi być zgodą wyraźną, a nie domniemaną lub dorozumianą z oświadczenia woli o innej treści (art. 4 ust. 1 usude), dla jej uzyskania nie jest wystarczające umożliwienie usługobiorcy rezygnacji z promocji oferowanej w *push notification*[44]. Jeżeli zatem na ekranie urządzenia mobilnego danego użytkownika pojawi się komunikat o treści „You've received a gift!", to wysyłający go usługodawca winien nie tyle umożliwić użytkownikowi rezygnację z odbioru „prezentu" poprzez zaznaczenie odpowiedniej opcji (zazwyczaj *checkbox*), ile zobligować go do zaznaczenia okna wyboru w wypadku, gdy chce z promocji skorzystać. Brak zaznaczenia pola wyboru oznacza nieskorzystanie z „prezentu", co powinno nastąpić bez żadnych dodatkowych konsekwencji i z możliwością zamknięcia okna komunikatu.

Podsumowując, komunikaty typu *push notifications* mają zazwyczaj charakter informacji handlowej, do której zastosowanie winny znaleźć rygorystyczne wymogi z art. 10 usude. Niezależnie od tego każdorazowo możliwość wysłania takiego komunikatu przez usługodawcę uzależniona jest od uprzedniego zgromadzenia informacji o użytkowniku, w tym najczęściej nie tylko danych eksploatacyjnych, ale także danych osobowych (w przypadku urządzeń mobilnych niezbędną daną do przekazania powiadomienia będzie numer telefonu, ewentualnie numer IMEI, adres MAC lub adres IP). Usługodawca zatem będzie zobowiązany przestrzegać także zasad ochrony danych osobowych w związku ze świadczeniem usług drogą elektroniczną (Rozdział 4 usude).

Abstract

Gabriela Bar in the dissertation "The legal nature of 'Push Notification' type messages," addresses the issues of the development of markets in the electronics industry and the devices functioning there: smartphones, tablets, palmtop computers (PDA). She illustrates in detail the role of application components in mobile devices, so-called push notifications and legal conditions of their practical application in several respects. The first is commercial information, the second - designation of the entity, the next – regulations of the Act on providing services through electronic means (uśude). These types of messages must follow the principle of the protection of personal data in connection with the provision of electronic services.

literalnie adres IP za dane dotyczące osoby możliwej do zidentyfikowania, stwierdzając, że: dostawcy usług internetowych oraz menedżerowie lokalnych sieci mogą, stosując rozsądne środki, zidentyfikować użytkowników Internetu, którym przypisali adresy IP ponieważ systematycznie zapisują w plikach daty, czas trwania oraz dynamiczny adres IP (czyli ulegający zmianie po każdym zalogowaniu) przypisany danej osobie. To samo odnosi się do dostawców usług internetowych, którzy prowadzą rejestr (logbook) na serwerze HTTP Nie ma wątpliwości, że w takich przypadkach można mówić o danych osobowych, w rozumieniu art. 2 Dyrektywy.

[42] K. Klafkowska – Waśniowska, [w:] D. Lubasz (red.), M. Namysłowska (red.), Świadczenie usług…, Lexis.pl 2013 - komentarz do art. 19 usude.

[43] Więcej na temat tworzenia profili użytkownika na potrzeby reklamy behawioralnej: Opinia Grupy Roboczej ds. Ochrony Danych Osobowych nr 2/2010 (wersja polskojęzyczna 00909/10 PL WP 171), http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/2010_en.htm, 23.11.2013r.

[44] Przepis art. 4 usude jest konsekwencją przyjęcia w ustawie o świadczeniu usług drogą elektroniczną obowiązku uzyskania zgody usługobiorcy na przesyłanie informacji handlowych lub przetwarzanie danych, czyli przyjęcia tzw. modelu opt-in. Przeciwstawna koncepcja, tzw. model opt-out zakłada, że usługobiorca musi wyrazić sprzeciw wobec przesyłania informacji handlowych lub przetwarzania niektórych danych osobowych. Tak: M. Namysłowska, [w:] D. Lubasz (red.), M. Namysłowska (red.), Świadczenie usług…, Lexis.pl 2013 - komentarz do art. 4 usude.

AGNIESZKA LEWESTAM

UMOWA FACTORINGOWA JAKO PRZYKŁAD UMOWY NIENAZWANEJ MIESZANEJ

Podstawą normatywną konstruowania umów nienazwanych *(contractus innominatus)* jest zasada swobody umów, uregulowana w art.353[1]KC. Strony zawierające umowę factoringową mogą ułożyć stosunek prawny według swego uznania, jednakże jego treść lub cel nie mogą pozostawać w sprzeczności z właściwością (naturą) stosunku, przepisami prawnymi oraz zasadami współżycia społecznego[1].

Pogląd klasyfikujący factoring jako oryginalną konstrukcję, określaną mianem umowy nienazwanej mieszanej, jest powszechny w polskim piśmiennictwie. Przed rozstrzygnięciem trafności tej klasyfikacji należy jednak podkreślić, iż istnieją spory definicyjne dotyczące samego zagadnienia umowy nienazwanej oraz mieszanej. Zasadnym jest zatem dokładne określenie tych pojęć. Kryterium podziału umów na nienazwane i nazwane jest unormowanie stosunku obligacyjnego przepisami prawa pozytywnego[2].

W. Kurowski powołując się na poglądy m.in. F. Zolla, A. Kleina, A. Ohanowicza, Z. Radwańskiego omówił sposób wyznaczenia granic tego podziału[3].

Spór skupia się na rozbieżnościach odnoszących się do zakresu w jakim umowa powinna zostać zaklasyfikowana w prawie pozytywnym oraz rangi normujących ją przepisów.

Z. Radwański uważa, że przepisy regulujące umowy nazwane nie muszą mieć rangi ustawowej[4]. Mogą to być zatem wszystkie przepisy powszechnie obowiązujące w Polsce takie jak: ustawy, rozporządzenia i ratyfikowane umowy międzynarodowe. Zgodnie ze stanowiskiem W. Czachórskiego essentialia negotii umów nazwanych powinny regulować przepisy normujące określony typ umowy[5].

Źródłem tworzenia nowych, niespotykanych wcześniej stosunków prawnych jest praktyka gospodarcza i społeczna. Coraz częściej pojawia się potrzeba regulacji prawnej kolejnych umów, takich jak umowa factoringowa, która z pewnością szybciej przestałaby być umową nienazwaną, gdyby nie różnice w jej rozumieniu w praktyce transkontynentalnej. Podstawowe znaczenie ma bez wątpienia ustalenie kryteriów wyodrębnienia umów nienazwanych jako dwustronnego stosunku prawnego. Można zatem wyróżnić następujące przesłanki:

- dwustronna czynność prawna będąca ważną umową,
- brak nazwania, chociaż to określenie nie musi nastąpić wprost lecz może wynikać z kontekstu lub opisania,
- brak tożsamości umowy z umową nazwaną lub takiego podobieństwa, które wskazuje na rodzaj umowy nazwanej, albo wyjątek od zasad konkretnej umowy nazwanej,
- określenie stron umowy, jej przedmiotu i treści oraz praw i obowiązków stron,
- pozostawanie w zgodzie z porządkiem prawnym, tzn. w zgodności kreowanego stosunku prawnego (treści, celu) z jego właściwościami, ustawami i zasadami słuszności, dobrymi obyczajami (zasadami współżycia społecznego) .

Praktyka zaczerpnięta z innych systemów prawnych przenika stopniowo na grunt polski, głownie za sprawą licznych firm z kapitałem zagranicznym inwestujących w Polsce, które oczekują przejęcia ich zwyczajów w tworzeniu stosunków obligacyjnych. Gdy dany stosunek prawny, który do tej pory nie istniał, tworzy się poprzez praktykę umawiania się zainteresowanych podmiotów, budują one jego cechy i treść. Po pewnym czasie upowszechniania się tej praktyki, która realizuje pożądany cel gospodarczy, tworzą się ogólne zasady dla tego stosunku prawnego, uznawane przez prawo. Przy szerokim rozumieniu natury stosunku prawnego biorąc pod uwagę ogólne warunki dotyczące umowy nienazwanej, a następnie w jej ramach, można dokonywać modyfikacji prowadzących do wykształcenia różnych postaci danej umowy (np. factoring pełny, niepełny)[6].

Literatura francuska wskazuje trzy cechy umów nienazwanych: subsydiarność, relatywność i przejściowość występowania. Subsydiarność oznacza, że oceniając umowę rozpatruje się ją w kryteriach istniejących już w obrocie ustawowych typów umów. Relatywność umów nienazwanych oznacza konieczność odwołania się przy ich określaniu do definicji oznaczonych typów umów nazwanych. Poszukuje się umów posiadających najbardziej zbliżone cechy do badanej umowy. Przejściowość występowania umów nienazwanych jest związana z przekonaniem, iż powtarzalność określonych relacji prawnych w umowach między stronami i ich standaryzacja powinna doprowadzić do wykształcenia się *essentialia negoti* takiej umowy i chociaż minimalnego uregulowania ustawowego[7].

W doktrynie pojawia się pogląd, iż pojęcie umowy mieszanej również nie jest ujednolicone. B. Gawlik klasyfikuje umowy mieszane jako podklasę umów nienazwanych, gdzie występuje równorzędne połączenie treści co najmniej dwóch umów nazwanych lub nienazwanych. Dla kontrastu, J.Górski nie wymaga takiej równorzędności oraz dopuszcza do zbioru umów mieszа-

[1] Barowicz M., Obrót wierzytelnościami. Aspekty prawne, Warszawa 2009, str.28
[2] Katner P., Przeniesienie wierzytelności w umowie factoringu,s.100
[3] Kurowski W., Faktoring jako kompleks umów, Rejent, 1999r., s.151
[4] Radwański Z., Teoria umów, PWN, Warszawa 1977r., s.209
[5] Czachórski W., Zobowiązania. Zarys wykładu, Warszawa 1983r., s.118
[6] Katner W. [w:] Radwański Z., System prawa prywatnego. Prawo Zobowiązań – umowy nienazwane, tom 9, Warszawa 2010r.
[7] Ibidem.

nych również umowy, które są określonym typem umowy nazwanej, ale zawierają świadczenia dodatkowe charakterystyczne dla umowy innego typu.[8]

Cechą umowy mieszanej jest niejednolitość i złożoność określonego stosunku obligacyjnego. Istotną kwestią jest, aby różnorodne elementy kontraktów miały jednolite znaczenie dla istoty danej umowy. Zdaniem Z. Radwańskiego i J. Panowicz-Lipskiej, umowy mieszane stanowią część umów nienazwanych[9].

W. Czachórski twierdzi natomiast, iż umowa mieszana może być zarówno umową nienazwaną jak i nazwaną i ten pogląd nie budzi wątpliwości.

Rozważając trafność określenia umowy factoringowej jako umowy nienazwanej mieszanej należy nadmienić, iż autorzy podzielający ten pogląd wskazują elementy tej umowy zaczerpnięte z różnych innych typów umów np. pożyczki, sprzedaży, ubezpieczenia, zlecenia.

Warto mieć na uwadze, że zarówno przeniesienie wierzytelności jak i usługi świadczone przez faktora, mają charakter równoważny dla factoringu, dlatego nie dopuszcza się możliwości dokonania jego kwalifikacji prawnej jako jeden ze stosunków zobowiązaniowych.

Z braku innej regulacji, umowę factoringową powinniśmy zakwalifikować jako umowę nienazwaną oraz ze względu na występowanie elementów różnych innych umów mieszaną.

Na gruncie dotychczasowych rozważań pojawia się pytanie, czy i jakie postanowienia prawa powszechnie obowiązującego będą miały zastosowanie do kwestii nieunormowanych przez strony umowy.

Piśmiennictwo wskazuje możliwość zastosowania przepisów dotyczących różnych umów nazwanych, jednakże zakres tego rozwiązania jest w praktyce trudny do określenia[10].

W takich przypadkach jako organ decyzyjny odnośnie wyboru odpowiednich przepisów względem umowy factoringowej, należałoby wskazać sąd lub organ administracyjny-nie strony.

Rozstrzygając problem wyboru przepisów, które powinny być zastosowane w odniesieniu do umów mieszanych, zasadne jest przyjęcie stanowiska, że w przypadku gdy główny rodzaj zobowiązania przeważa, a świadczenia uboczne mają odmienny charakter, właściwe będzie zastosowanie przepisów regulujących umowę nazwaną głównego typu. Jednakże, gdy umowa mieszana łączy w sobie równorzędne elementy różnych rodzajów zobowiązań, w stosunku do każdego ze świadczeń należałoby zastosować właściwe dla niego przepisy[11].

Jedyny akt prawny, w którym pojawia się słowo „faktoring", to Polska Klasyfikacja Działalności[12].

W praktyce treść umowy factoringowej jest ujęta w standardowym wzorze przygotowanym przez firmę factoringową. Najczęściej wykorzystuje się regulaminy lub ogólne wzory umów uzupełnione o indywidualną, kilkustronicową właściwą umowę, zawierającą dane stron oraz indywidualnie negocjowane postanowienia modyfikujące bądź uzupełniające standardowe ogólne warunki umów. Te ostatnie są nierzadko formułowane w sposób faworyzujący firmę factoringową. Wszystkie wzorce umowne podlegają modyfikacji. Inną konsekwencją braku regulacji ustawowej i swobodnego umownego kształtowania treści umowy są rozbieżności między wzorami umów stosowanymi przez poszczególne firmy factoringowe. Szukając dostawcy usług factoringowych, nie powinniśmy zatem kierować się wyłącznie warunkami finansowymi dyskonta faktur, ale też upewnić się, że porównujemy oferty zbliżone merytorycznie.

Nieistnienie ustawowych regulacji odnoszących się do factoringu sprzyja rozwojowi tej usługi. Konkurencja działa jak katalizator skłaniając do poszukiwania skuteczniejszych metod zarządzania ryzykiem. Swoboda na rynku factoringowym oznacza upowszechnianie finansowania na podstawie umowy factoringowej. Przesadnie szczegółowa prawna regulacja usługi factoringu mogłaby spowodować, iż oferta stałaby się dostępna dla węższego grona odbiorców. Brak szczególnych regulacji w polskim ustawodawstwie zwiększa dostępność branży. Taka elastyczność omawianej usługi umożliwia płynne dopasowanie oferty factoringowej zarówno w okresie kryzysu jak również renesansu gospodarczego. Przedsiębiorcy korzystający z usługi factoringowej mają możliwość poprawy płynności finansowej swojej firmy oraz skrócenia cyklu obrotu wierzytelnościami np. poprzez ich windykację. Zyskują także dzięki szerokiej ofercie usług dodatkowych proponowanych przez faktorów.

Abstract

Agnieszka Lewestam in the article "Factoring agreement as an example of an innominate mixed contract" states that the non-existence of statutory regulations relating to factoring favors the development of this service. Also, the flexibility of the service in question allows for smooth adjustment of the factoring offer both in times of economic crisis as well as renaissance. Entrepreneurs using factoring services have the opportunity to improve their company's financial liquidity and reduce debt trading cycle, e.g. through their recovery. They also gain through the wide range of additional services offered by the factors.

[8] Katner P., Przeniesienie wierzytelności w umowie factoringu, Wolters Kluwer, Warszawa 2011r., s. 101

[9] Radwański Z., Panowicz - Lipska J, Zobowiązania – część szczególna, wyd.5, Warszawa 2004,s.10

[10] Kruczalak K., Factoring i jego gospodarcze zastosowanie, PWN 1997r., s.79

[11] System prawa prywatnego. Prawo zobowiązań-część ogólna, pod red. E. Łętowskiej, tom 5,CH Beck,s.452

[12] Rozporządzenie Rady Ministrów z 24 grudnia 2007r. w sprawie Polskiej Klasyfikacji Działalności (Dz.U.Nr 251, poz. 1885)

MATEUSZ SZKUTA

INKORPORACJA WZORCÓW UMOWNYCH W POSTACI ELEKTRONICZNEJ

1. Wstęp

Internet, stworzony pierwotnie jako sieć o przeznaczeniu militarnym, stał się publicznie dostępnym medium wymiany informacji, kreując stosunki nowego rodzaju. Jego rozwój umożliwił szeroko pojętą ponadnarodową wymianę informacji na dotychczas nieznanej płaszczyźnie. Ujawniając jednocześnie zagrożenia nowego typu, wynikające z niekontrolowanego przypływu informacji.

Podjęte działania legislacyjne zdeterminowane były koniecznością dostosowania regulacji do wymogów nakreślonych zdematerializowanym obrotem gospodarczym[1]. Ze względu na fakt, iż technologia cyfrowa i Internet, dają potencjalnie większe możliwości działania w zakresie użytku komercyjnego (B2B), konsumenckiego czy komercyjno-konsumenckiego (B2C) zauważalne jest wprost proporcjonalne zwiększenie możliwości dokonania naruszeń praw podmiotów partycypujących w tego typu obrocie.

Przedmiotem niniejszego opracowania jest analiza skutecznego sposobu inkorporacji wzorca elektronicznego na podstawie art.384 §4 KC. Wybór tematu wiąże się z rozbieżnością poglądów w tej kwestii. Zauważyć też trzeba, że część dotychczasowych poglądów zdezaktualizowała się, w związku z kształtowaniem się nowych sposobów obrotu elektronicznego.

2. Wzorce w postaci elektronicznej

2.1. Wzorzec elektroniczny w rozumieniu art. 384§4 KC

Przepis art.384 §4 KC ustanawia szczególne przesłanki inkorporacji wzorców elektronicznych do określonego typu stosunków. Temu reżimowi podlegają wszelkie podmioty, bez względu na swój status, w umowach wszelkiego typu, które mogą być zawarte przy użyciu takich wzorców. Natomiast szereg przesłanek inkorporacji wzorca określonych w art.384 §1-2 KC nie znajduje zastosowania[2].

Stosowanie art. 384 §4 KC uzależnione jest tylko od faktu posługiwania się przez proponenta zdematerializowanym wzorcem umowy przy spełnieniu szczególnych wymogów „udostępnienia". Umożliwia to postawienie tezy, iż brak jakichkolwiek ograniczeń, zarówno podmiotowych jak i przedmiotowych, dla stosowania normy art.384 §4 KC. Wyjątek stanowią przypadki, gdzie z natury stosunków, wzorce umowne nie mają zastosowania oraz gdy ustawy szczególne nakładają takie wymogi, jak wyrażenie zgody przez konsumenta na posługiwanie się wzorcem[3].

Kwestia inkorporacji wzorców elektronicznych została uregulowana w przepisach kodeksu cywilnego oraz ustawy o świadczeniu usług drogą elektroniczną[4]. W pierwszej kolejności należy więc rozstrzygnąć, które z uregulowań w konkretnym przypadku będą miały zastosowanie. Porównując normy wynikające z przepisów kodeksu cywilnego i ustawy o świadczeniu usług drogą elektroniczną uznać można, iż pomimo ogólnej zasady stosowania kodeksu cywilnego, w szczegółowo wskazanych przypadkach to właśnie tej ustawie należy przyznać pierwszeństwo stosowania, zgodnie z regułą interpretacyjną *lex specialis derogat legi generali*. W przypadku stosunków niepodlegających tej ustawie zastosowanie znajdą uregulowania kodeksowe.

2.2. Wzorzec elektroniczny na podstawie ustawy o świadczeniu usług drogą elektroniczną

Zgodnie z art.2 ust 4) u.ś.u.d.e. przez pojęcie „świadczenie usługi drogą elektroniczną" należy rozumieć: *„wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej, w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*". Przedstawiona definicja, określająca zakres zastosowania ustawy, inaczej niż w ustawodawstwie wspólnotowym, została zredagowana poprzez opisowe przedstawienie sposobu świadczenia usługi elektronicznej, a nie poprzez wyodrębnienie pojęcia „usługi świadczonej drogą elektroniczną"[5]. Należy doprecyzować znaczenie każdej z enumeratywnie wskazanych w przepisie przesłanek, które dla zastosowania przepisów ustawy muszą zaistnieć łącznie.

---

[1] M.in. Ustawa z dnia 14 lutego 2003 roku o zmianie ustawy - Kodeks cywilny oraz niektórych innych ustaw (Dz.U. 2003 Nr 49 Poz 408)

[2] Tak: T. Szczurowski, Udostępnienie wzorca w postaci elektronicznej, PPH 2005, Nr 7, s. 40; W. Popiołek, [w:] K. Pietrzykowski (red.) Komentarz do Kodeksu Cywilnego, t. I, 2009, s. 1081; M. Olczyk [w:] M. Olczyk, M. Pecyna, Komentarz do niektórych przepisów kodeksu cywilnego, zmienionych ustawą z dnia 14 lutego 2003 r. o zmianie ustawy – Kodeks cywilny oraz niektórych innych ustaw (Dz.U. Nr 49 poz. 408), LEX 2012. Odmiennie D. Szostek [w:] J. Barta (red.), R. Markiewicz (red.), Handel elektroniczny. Prawne problemy, Kraków 2005, s. 157;

[3] Por. art. 6 ust. 3 ustawy z dnia 2 marca 2000 r. o ochronie niektórych praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny (Dz.U. 2000 r. Nr 49 Poz 408)

[4] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 nr 144 poz 1204 z późn. zm.)

[5] M. Świerczyński [w] J. Gołaczyński J (red.), Ustawa o świadczeniu usług drogą elektroniczną. Komentarz., Oficyna, 2009. LEX i cyt. tam autorzy

Po pierwsze, wykonywanie usługi winno następować bez jednoczesnej obecności obu stron, co związane jest ze specyfiką usług elektronicznych, których uczestnicy wykorzystują rozwiązania techniczne do przekazu, odbioru czy transmisji danych na żądanie, bez potrzeby swojej jednoczesnej fizycznej obecności. X. Konarski uznał, iż dla rozstrzygnięcia, czy dana usługa stanowi świadczenie na odległość, istotna jest kwestia, czy możliwe jest również zamówienie danej usług bezpośrednio w placówce usługodawcy[6]. Zasygnalizowano również, iż wyróżnić można też sytuacje, w których pomimo fizycznej obecności stron, usługa będzie świadczona na odległość[7].

Po drugie, usługa powinna być świadczona na indywidualne żądanie usługobiorcy. Słusznie wskazuje się, iż: „Element indywidualnego żądania usługobiorcy należy interpretować w ten sposób, że może on zażądać świadczenia usługi (na przykład polegającej na przeglądaniu on-line bazy informacyjnej) z miejsca i w czasie indywidualnie przez niego wybranym"[8]. Wskazać można, iż w rezultacie świadczenia danej usługi elektronicznej na żądanie, stosunek stron nabiera charakteru zindywidualizowanego. Za przykład usług elektronicznych świadczonych na indywidualne żądanie przytacza się: przeglądanie stron internetowych, VOD[9] czy wiadomości SMS[10]. A contrario przyjąć można, iż w przypadku braku możliwości wyboru usługi, czasu jej świadczenia czy braku indywidualnego odbioru danych – świadczenie pozbawione zostanie cech świadczenia elektronicznego w rozumieniu ustawy. Przykładem usług niespełniających takich przesłanek są: transmisje radiowe, teletekstowe, telewizyjne, usługi poczty głosowej, telefaksu czy marketingu telefonicznego[11].

Po trzecie, usługa powinna być świadczona poprzez przekaz danych z wykorzystaniem urządzeń do ich elektronicznego przetwarzania. Taki sposób świadczenia oznacza, iż po obu stronach stosunku, w celu spełniania świadczenia elektronicznego, niezbędne jest wykorzystywanie urządzeń elektronicznych. Zasada ta ściśle związana jest z brakiem jednoczesnej obecności stron, ponieważ w miejsce strony nieobecnej (brak fizycznego kontaktu), wstępuje jej „substytut" – urządzenie elektroniczne, przy użyciu których usługa jest wykonywana.

Po czwarte, usługa powinna być świadczona za pomocą sieci telekomunikacyjnej poprzez nadawanie – odbieranie lub transmitowanie danych. Zgodnie z art.2 ust.3) ustawy – Prawo telekomunikacyjne[12] przez system teleinformatyczny, rozumieć należy: *„zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy (…)"*. Przez co rozumieć należy takie urządzenie telekomunikacyjne, które przeznaczone jest do podłączenia bezpośrednio lub pośrednio do zakończenia sieci, czyli miejsca, w którym abonent otrzymuje dostęp do publicznej sieci telekomunikacyjnej[13]. Zgodnie z powyższym, usługa elektroniczna może wyłącznie polegać na nadawaniu, odbieraniu czy transmitowaniu danych za pośrednictwem sieci telekomunikacyjnej. Pozwala to przyjąć, iż usługami elektronicznymi w rozumieniu u.o.ś.u.d.e. nie mogą być usługi, które posiadają swój „materialny substrat".[14] Innymi słowy, usługi, w wyniku których usługobiorca otrzymuje zmaterializowany przedmiot (a nie dane), nie stanowią usług elektronicznych[15]. M. Świerczyński twierdzi również, iż: *„Samo dostarczanie dóbr (choćby następowało ono w wyniku wykonania zawartej elektronicznie umowy) nie jest objęte pojęciem usługi informacyjnej, podobnie jak nie są tymi usługami wszystkie te czynności, które ze swej natury nie mogą być świadczone na odległość za pomocą środków elektronicznych"*[16].

3. Implementacja uregulowań prawa europejskiego

Regulacja art. 384 §4 KC została wprowadzona nowelą z dnia 14 lutego 2003 roku[17], implementując postanowienia zawarte w dyrektywie o handlu elektronicznym[18]. W art.10 ust.3. dyrektywy wskazano, iż: *„Warunki umów oraz ogólne postanowienia umowy muszą być udostępniane usługobiorcy w sposób umożliwiający ich przechowywanie i odtwarzanie"*. Polski ustawodawca implementował to uregulowanie przyjmując następującą redakcję przepisu: *„Jeżeli jedna ze stron posługuje się wzorcem umowy w postaci elektronicznej, powinna udostępnić go drugiej stronie przed zawarciem umowy w taki sposób, aby mogła ona wzorzec ten przechowywać i odtwarzać w zwykłym toku czynności"*.

W obu przypadkach mowa jest o „udostępnieniu", jako o przesłance koniecznej do związania wzorcem, stanowiącej techniczny sposób inkorporacji wzorca w stosunkach elektronicznych, będącego odpowiednikiem „doręczenia" w rozumieniu przyjętym w odniesieniu do wzorców umownych w ogólności. Pojęcie „udostępnienia" w dyrektywie obwarowane zostało przesłanką „umożliwienia przechowywania i odtwarzania", co powtórzono w art.384 §4 KC. Jednocześnie przepis ten uszczegóławia ten wymóg, poprzez nałożenie obowiązku zapewnienia „przechowywania i odtwarzania wzorca w postaci elektronicznej w zwykłym toku czynności".

Porównując treść dyrektywy oraz przepis art.383 §4 KC można stwierdzić, że pomimo drobnych różnic, europejska regulacja została wprowadzona bez zabiegów doprecyzowujących[19]. W moim mniemaniu, dodanie w art. 384 §4 KC do przesłanki „przechowywania i odtwarzania" wskazania, iż chodzi o zachowanie „zwykłego toku czynności" niczego nie wnosi. Takie „doprecyzowanie" nie określa technicznego sposobu skutecznej inkorporacji wzorca, natomiast - wobec posłużenia się ogólnym określeniem – skutkuje powstaniem przestrzeni do zaistnienia potencjalnych rozbieżności.

---

[6] X. Konarski, Komentarz do ustawy o świadczeniu usług drogą elektroniczną, Warszawa 2004, s. 67, tak też: E. Łętowska, Prawo umów konsumenckich, Warszawa 2002, s. 279

[7] Gołaczyński J. (red.), Kowalik-Bańczyk K., Majchrowska A., Świerczyński M., Ustawa o świadczeniu usług drogą elektroniczną. Komentarz., LEX 2012

[8] X. Konarski, Komentarz..., s. 69,

[9] Video-On-Demand – skrót: "VoD" lub "VOD"; ang. Video on Demand - wideo na żądanie — usługa umożliwiająca odtwarzania materiałów filmowego lub słuchanie nagrań dźwiękowych, w wybranym przez usługobiorcę czasie, późniejszym od czasu emisji.

[10] M. Świerczyński [w] J. Gołaczyński J (red.), Ustawa o świadczeniu... i cyt. tam autorzy

[11] M. Świerczyński [w] J. Gołaczyński J (red.), Ustawa o świadczeniu... i cyt. tam autorzy

[12] Ustawa z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz. U. 2004 Nr 171 Poz 1800 z późn. zm.)

[13] Art. 2 ust. 43 i 53 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne

[14] A. Frań-Adamek, Komentarz do ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.02.144.1204), LEX 2012

[15] Szerzej: D. Kot, Dyrektywa Unii Europejskiej o handlu elektronicznym i jej implikacje dla prawa cywilnego, Kwartalnik Prawa Prywatnego 2001, z. 1, s. 47-49

[16] M. Świerczyński [w] J. Gołaczyński J (red.), Ustawa o świadczeniu... i cyt. tam autorzy

[17] Ustawa z dnia 14 lutego 2003 r. o zmianie ustawy - Kodeks cywilny oraz niektórych innych ustaw (Dz.U. z 2003 nr 49 poz. 408)

[18] Dyrektywa Parlamentu Europejskiego i Rady 2000/31/WE z dnia 8 lipca 2000 roku w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku Urz. UE L 178 z dnia 8 czerwca 2000 roku)

[19] Tak również: T. Szczurkowski, Udostępnienie wzorca.., s. 36

4. Wymogi skutecznej inkorporacji wzorca w postaci elektronicznej na podstawie 384§4 KC

4.1. Sposób udostępnienia wzorca

Pomimo rozbieżności pomiędzy znaczeniami pojęć „doręczenia" i „udostępnienia" przyjmuje się, iż „udostępnienie" stanowi odpowiednik przesłanki „doręczenia" z art.384§1 KC. Zarówno doręczenia jak i udostępnienie ma na celu umożliwienie zapoznania się z treścią wzorca, mającego regulować stosunki między stronami umowy[20].

W doktrynie wskazuje się na potrzebę konkretyzacji (indywidualizacji) wzorca elektronicznego ze względu na jego zdematerializowany charakter, co powiązano z wyodrębnieniem przesłanki, iż udostępnienie wzorca nastąpić ma w sposób umożliwiający jego przechowywanie i odtwarzanie w zwykłym toku czynności[21]. Moim zdaniem wymóg konkretyzacji wzorców umownych poprzez konieczność spełnienia szczególnych wymogów dotyczących zapewnienia dostępu do ich treści, jest niefortunny. Za główny cel „konkretyzacji" obrano przeciwdziałanie zagrożeniom związanym z ulotnym (zdematerializowanym) charakterem wzorca. Rozwiązanie tej kwestii polegać ma na zapewnieniu możliwości posiadania dowodu zawarcia umowy przy użyciu wzorca elektronicznego, poprzez skonstruowanie przesłanki przechowywania i odtwarzania w zwykłym toku czynności[22].

M. Pecyna wskazuje, iż udostępnienie elektronicznego wzorca umownego spełniające wymogi przechowywania i odtwarzania w zwykłym toku czynności, nastąpi poprzez jego przesłanie na adres poczty elektronicznej adherenta. Przyjęcie tej metody pozwoli jednocześnie ustalić strony (wysyłającego – proponenta i odbierającego – adherenta) oraz czas udostępnienia (wysyłki i doręczenia), gwarantując tym samym utrwalenie wzorca, uniemożliwiające niekontrolowaną ingerencję w jego treść, po zawarciu umowy[23].

W rozumieniu tej koncepcji udostępnienie wzorca przybiera postać doręczenia w znaczeniu funkcjonalnym, ze względu na fakt niemożliwości doręczenia wzorca elektronicznego w znaczeniu „fizykalnym" [24]. F. Wejman przez pryzmat ukształtowanej przez siebie teorii funkcjonalnego doręczenia wzorca twierdzi, iż konieczne jest faktyczne posiadanie przez adherenta egzemplarza wzorca elektronicznego, potwierdzającego zawarcie umowy[25]. Tym samym Autor ten neguje możliwość udostępnienia wzorca elektronicznego za pośrednictwem strony www.

Dostrzega się również mniej zdecydowane podejście części doktryny do kwestii udostępnienia wzorca, która uznaje, iż skuteczna inkorporacja wzorca elektronicznego może mieć miejsce w następstwie jego przesłania na adres poczty elektronicznej lub przekazanie go na dyskietce[26]. Cz. Żuławska, odrzucając pogląd o dopuszczalności udostępnienia wzorca na stronie www wskazuje, iż koniecznym jest zagwarantowanie pełnego i swobodnego dostępu do wzorca, co będzie możliwe w przypadku jego faktycznego posiadania[27]. Odmienne stanowisko prezentuje W. Kocot stojący na stanowisku, iż udostępnienie wzorca na stronie internetowej jest wystarczające pod warunkiem zapewnienia możliwości swobodnego jego powielania za pośrednictwem powszechnie dostępnych programów[28].

T. Szczurkowski z kolei zróżnicował sposoby inkorporacji wzorca elektronicznego, odwołując się do kryterium podmiotu – konsument i profesjonalista. Autor stwierdza iż: *„Jeśli umowa jest zawierana z konsumentem (tzw. umowa jednostronnie gospodarcza), to udostępnienie wzorca może być zrealizowane jedynie przez przesłanie go pocztą elektroniczną, jeśli natomiast umowa jest zawierana między przedsiębiorcami (tzw. umowa dwustronnie gospodarcza), to udostępnienie wzorca w postaci elektronicznej może być zrealizowane także przez umieszczenie go na stronie www"*[29]. Przedstawiony punkt widzenia jest próbą interpretacji dostosowanej do różnych rodzajów adherentów – profesjonalistów i konsumentów, jednakże – zgodnie z dyrektywą wykładni językowej *lege non distinguente* – należałoby go odrzucić, ponieważ sam ustawodawca w art.384 §4 KC nie dokonał jakichkolwiek rozróżnień, zarówno podmiotowych jak i przedmiotowych.

Ze względu na nieostrość postanowień art.384 §4 KC część doktryny prezentuje stonowane podejście przedstawiając techniczne sposoby skutecznej inkorporacji wzorców elektronicznych. W. Popiołek wskazuje, iż wystarczającą przesłanką stosowania art.384 §4 KC jest sytuacja, w której adherent będzie miał możliwość utrwalenia wzorca, gwarantującej mu jego przechowywanie oraz powtarzalne odtwarzanie, pod warunkiem jego udostępnienia przy zachowaniu standardowych i ogólnodostępnych metod[30].

4.2. Moment udostępnienia wzorca

Zgodnie z treścią art. 384§4 KC udostępnienie wzorca powinno nastąpić „przed zawarciem umowy", co stanowi powielenie postanowienia normy zawartej w art. 384 §1 KC[31]. Bez względu na formę wzorca umownego, niedopuszczalne jest uznanie obowiązywania wzorca przed jego udostępnieniem czy doręczeniem. Natomiast dokładne umiejscowienie w czasie pojęcia „przed zawarciem" nie tyle nie jest możliwe, co zbyteczne. Za punkt wyjścia należy przyjąć ogólne założenie, że moment skutecznego udostępnienia (doręczenia) wzorca musi zaistnieć wcześniej, niż samo zawarcia stosunku zobowiązaniowego między stronami.

Inną kwestią jest problem okresu podtrzymania dostępności wzorca w celu przechowywania i przetwarzania. W przeciwień-

[20] Tak W. Popiołek [w:] K.Pietrzykowski (red.), Komentarz do..., s. 977; C. Żuławska, [w:] G. Bieniek, H. Ciepła, S. Dmowski, J. Gudowski, K. Kołakowski, M. Sychowicz, T. Wiśniewski, C. Żuławska, Komentarz do Kodeks…, s. 134

[21] M. Bednarek [w:] E. Łętowska (red.) t. 5, System Prawa Prywatnego, Prawo zobowiązań – część ogólna, Warszawa 2006, s. 599, M. Pecyna [w:] M. Olczyk, M. Pecyna, Komentarz do niektórych przepisów kodeksu cywilnego, zmienionych ustawą z dnia 14 lutego 2003 r. o zmianie ustawy - Kodeks cywilny oraz niektórych innych ustaw (Dz.U.03.49.408), LEX 2003; C. Żuławska, [w:] G. Bieniek, H. Ciepła, S. Dmowski, J. Gudowski, K. Kołakowski, M. Sychowicz, T. Wiśniewski, C. Żuławska, Komentarz do Kodeksu…, s. 134 oraz F. Wejman, Wzorce umów na stronach www i w poczcie elektronicznej, TPP 2000, Nr 4, s. 53.

[22] M. Bednarek [w:] E. Łętowska, System…, s. 599; M. Pecyna [w:] M. Olczyk, M. Pecyna, Komentarz do niektórych przepisów kodeksu cywilnego, zmienionych ustawą z dnia 14 lutego 2003 r. o zmianie ustawy - Kodeks cywilny…, LEX 2003; C. Żuławska, [w:] G. Bieniek, H. Ciepła, S. Dmowski, J. Gudowski, K. Kołakowski, M. Sychowicz, T. Wiśniewski, C. Żuławska, Komentarz do Kodeksu…, s. 134 oraz F. Wejman, Wzorce umów …, , s. 53

[23] M. Pecyna [w:] M. Olczyk, M. Pecyna, Komentarz do…, LEX 2003. Podobnie F. Wejman, Wzorce umów na…, s. 54; M. Pecyna, Kontrola wzorców umownych poza obrotem konsumenckim, Zakamycze 2003, s. 98 oraz A. Stosio, Umowy zawierane przez Internet, Warszawa 2002, s. 267;

[24] T. Szczurkowski, Udostępnienie wzorca.., s. 37 i cytowani tam autorzy

[25] F. Wejman, Wzorce umów na…, s. 54

[26] W. Czachórski, A. Brzozowski, M. Safjan, E. Skowrońska-Bocian, Zobowiązania – zarys wykładu, Warszawa 2009, s. 165

[27] C. Żuławska, Komentarz do Kodeksu…, s. 133

[28] W. Kocot, Wpływ Internetu na prawo umów, Warszawa 2004, s. 246

[29] T. Szczurkowski, Udostępnienie wzorca.., s. 37 i cytowani tam autorzy

[30] W. Popiołek [w:] K. Pietrzykowski, Komentarz do…, s. 1081

[31] W. Popiołek [w:] K. Pietrzykowski, Komentarz do…, s. 1081

stwie do doręczenia, które stanowi zdarzenie jednorazowe, redakcja normy art.384 §4 KC wskazuje, iż koniecznym jest zachowanie ciągłości w dostępie do wzorca. W zależności jednak od miejsca przechowywania wzorca, zapewnienie dostępności powinno ulec zróżnicowaniu. Jeżeli wzorzec elektroniczny jest udostępniany adherentowi przez proponenta w sposób ciągły (np. na stronie www) to w moim przekonaniu powinien on pozostać dostępny do odtwarzania, aż do czasu zakończenia stosunku między stronami. Takie założenia wywieść można z konieczności zapewnienia dostępu do wzorca przez okres, w którym znajduje on zastosowanie. Natomiast, jeżeli wzorzec został udostępniony w taki sposób, iż adherent wszedł w jego posiadanie w postaci pliku (np. poprzez jego wysyłkę na adres e-mail) to uważam, iż zwalnia to proponenta z obowiązku stałego podtrzymywania jego dostępności.

4.3. Zapewnienie przechowywania i odtwarzania wzorca w zwykłym toku czynności

Kwalifikowane przesłanki inkorporacji wzorca w formie elektronicznej z art. 384§4 KC określają dolną granicę czynności technicznych niezbędnych do skutecznej inkorporacji. Uznać należy, że inne (dalej idące) wymogi niż zapewnienie przechowywania i odtwarzania w zwykłym toku czynności mają charakter fakultatywny. Uzasadnia to odrzucenie poglądów, które rozszerzają zakres wymogów na przykład o konieczność umożliwienia zmaterializowania wzorca poprzez jego wydruk. W praktyce zwykle zapewnia się taką możliwość, lecz w poglądzie reprezentowanym przez orzecznictwo, który osobiście podzielam, nie jest to konieczne[32].

Ze względu na zastosowanie w przepisie koniunkcji, konieczne jest jednocześnie zapewnienie udostępnienia w taki sposób, aby można było wzorzec przechowywać i odtwarzać z zachowaniem zwykłego toku czynności. Wychodząc od słownikowego znaczenia pojęcia „przechowywanie" rozumieć przez to należy zespół czynności zapewniających uchronienie wzorca elektronicznego przed zepsuciem, zniszczeniem, zaginięciem itp. poprzez umieszczenie w odpowiednich warunkach[33]. Pozwala to twierdzić, że pojęcie to sprowadza się do możliwości zarchiwizowania treści wzorca, czyli umożliwienia jego zapisu[34]. Natomiast pod terminem „odtwarzanie" rozumieć się powinno jego reprodukcję, czyli czynności techniczne skutkujące wizualizacją i dostępem do zawartości[35].

Zastrzeżenie przechowywania i odtwarzania zostało powiązane z przesłanką „zwykłego toku czynności". Przyjmuje się, iż chodzi tu o możliwość przechowywania i odtwarzania w sposób łatwy oraz wprost, czyli bez konieczności posiadania specjalnego sprzętu technicznego czy oprogramowania oraz dokonywania szczególnych czynności[36]. W moim przekonaniu swobodny dostęp do treści wzorca, zapewnia udostępnienie go w powszechnie stosowanych formatach plików (np. *.pdf, *.html, *.doc, *.odt, w tym również umieszczonych w archiwach plików *.zip czy *.rar), które mogą zostać odczytane przy użyciu domyślnie zainstalowanych programów. Natomiast, w przypadku konieczności posiadania dodatkowego oprogramowania, proponent powinien wskazać nazwę programu wraz z miejscem, skąd może on zostać nieodpłatnie pobrany. Można założyć, iż przewodnią myślą przesłanki „zwykłego toku czynności" jest zapewnienie bezproblemowego i niewymagającego trudności zapoznania się z treścią wzorca. Przyjąć należy, że udostępnienie kodowanego pliku bez podania hasła, wymagającego specjalnego oprogramowania czy wymuszającego podjęcia jakichkolwiek innych dodatkowych czynności (np. wysłanie wiadomości SMS, wyrażenie zgody na przetwarzanie danych w celach marketingowych, wpis na listę mailingową czy konieczność uiszczenia należności) powinno skutkować brakiem inkorporacji postanowień wzorca elektronicznego, w związku z niespełnieniem wymogów ustanowionych przepisem 384§4 KC.

Odnosząc się do przechowywania udostępnionego wzorca elektronicznego, stwierdzić można, iż jego położenie może być dowolne, pod warunkiem posiadania dostępu do niego przez adherenta. W obecnym kształcie powszechnego obrotu elektronicznego, wskazać należy, iż standardem nie jest już przechowywanie danych na nośnikach, które fizycznie posiadamy, lecz w chmurze[37]. Zwrócić należy uwagę, iż w takim przypadku użytkownik posiada wyłącznie zdalny dostęp do odtwarzania i przetwarzania wzorca, bez posiadania rzeczywistego dostępu do sprzętu elektronicznego, na którym został zapisany. Zarówno w przypadku poglądu przyjmującego konieczność wysyłki egzemplarza wzorca na adres poczty elektroniczne, jak i w przypadku stanowiska, iż wystarczające jest udostępnienie wzorca na stronie internetowej, na dzień dzisiejszy egzemplarze wzorca nie znajdują się w faktycznym posiadaniu adherenta, ponieważ znajdują się na określonym serwerze, do którego uzyskuje on dostęp.

5. Wnioski

Współczesny obrót gospodarczy nieodwracalnie dematerializuje się, pociągając za sobą konieczność zapewnienia odpowiedniej dynamiki zawiązywania stosunków, właściwej do obecnego poziomu techniki oraz oczekiwań społecznych.

Tezy autorów aprobujących rozumienie pojęcia „udostępnienia" wzorca elektronicznego, jako zespołu czynności sprowadzających się do wysyłki wiadomości elektronicznej z dołączeniem wzorca nie powinny zostać bezkrytycznie akceptowane. Pomimo słusznie podnoszonego zarzutu niemożliwości wyeliminowania niekontrolowanej ingerencji w treść wzorca, udostępnianego w sposób odmienny niż poprzez jego przesyłkę drogą elektroniczną, uważam, że zasadniczy problem tkwi w postawie adherentów, którzy poprzez swoje zaniechanie nie zapoznają się z treścią wzorca. Zawsze istnieje możliwość nie zawarcia umowy, jeżeli adherent nie zaakceptuje warunków kontraktowych. Natomiast, jeżeli adherent nie podejmuje jakiejkolwiek próby zapoznania się z treścią stosunku mającego go łączyć z proponentem, to interpretowanie w takim przypadku przepisów na korzyść adherenta, uważam za podejście niewłaściwe.

W moim przekonaniu, ekspozycja na odpowiedniej stronie www powinna zostać uznana za wystarczający sposobów właściwego udostępnienia wzorca. Pogląd ten oparty jest na treści ustawy o świadczeniu usług drogą elektroniczną. Ustawa opisuje

[32] Wyrok Sądu Apelacyjnego w Warszawie z dnia 12 października 2012 r. w sprawie o sygn. akt I ACa 444/12, LEX 2013

[33] E. Sobol (red.), Mały słownik języka polskiego, PWN 1997, s. 717

[34] Tak również: M. Bednarek [w:] E. Łętowska (red), System…, s. 599

[35] E. Sobol (red.), Mały słownik języka polskiego, PWN 1997, s. 552

[36] M. Bednarek [w:] E. Łętowska (red), System…, s. 600

[37] Chmura obliczeniowa – model przetwarzania danych oparty na użytkowaniu usług dostarczonych przez zewnętrzne podmioty bez konieczności używania własnych zasobów.

przesłanki inkorporacji wzorca wprawdzie w stosunkach innego rodzaju, lecz przewiduje mniej rygorystyczne wymagania, niż regulacja kodeksowa czy propozycje zwolenników wysyłki treści wzorca na adres poczty elektronicznej. Pomimo, iż obrót elektroniczny implikuje szereg trudności, w szczególności w zakresie dowodowym, to podkreślić należy, iż w wyniku ukształtowania się stosunków w zdematerializowanym obrocie można przyjąć, iż ekspozycja na stronie internetowej treści wzorca stała się wiodącym rozwiązaniem technicznym udostępnienia wzorca elektronicznego. Z racji powszechności zastosowania w stosunkach danego rodzaju, można uznać, iż ta forma udostępnienia przybrała już miano zwyczaju.

W związku z ogólnikowym i opisowym brzmieniem przepisu z art.384 §4 KC pojęcie „udostępnienia" powinno być interpretowane, bez wskazywania konkretnych technicznych sposobów jego realizacji. Uzasadnia to fakt, że sam ustawodawca nie dokonał wskazania konkretnego sposobu inkorporacji wzorca elektronicznego a wyłącznie uzależnił to od spełnienia odpowiednich przesłanek. Każdy sposób udostępnienia wzorca będzie zatem wystarczający do skutecznej jego inkorporacji. Warunkiem jednak pozostaje konieczność udostępnienia wzorca przed zawarciem umowy oraz zagwarantowania jego przechowywania i odtwarzania w zwykłym toku czynności. Tym samym udostępnienie treści wzorca za pośrednictwem strony www, poczty e-mail, w formie pliku do pobrania czy i w inny sposób spełniający ustawowe przesłanki, powinno być uznane za wystarczające dla skutecznej inkorporacji wzorca elektronicznego.

Abstract

In turn, Mateusz Szkuta in the paper, "Incorporation of standard contracts patterns in electronic form" examines effective ways of incorporating electronic pattern on the basis of Article 38 § PCC and the Act on providing services through electronic means. The author concludes that comparing the content of the Directive and the provision of Article 383 § PCC can be noted that, despite minor differences, the European regulation was introduced without depreciation. Despite the discrepancy between the meanings of the terms „service" and „sharing" it is assumed that „sharing" is the equivalent of a "service" of Article 38 § PCC. Both the service and the sharing are to enable reading the contents of the pattern, having governed relations between the parties. The theses of the authors affirming understanding of the term „sharing" standard electronic pattern, as a set of actions that come down to sending electronic mailings with the enclosure of the pattern should not be, in the author's opinion, uncritically accepted. In the opinion of the speaker, the exposure on the relevant website should be considered as sufficient way to make the correct pattern available. This view is based on the contents of the Act on providing services through electronic means. The Act describes the conditions for the incorporation of a pattern, but provides less stringent than the regulations of the Code or suggestions of the supporters the idea of sending content.

BEATA WÓJTOWICZ-WOŹNICZKA

ELEKTRONICZNE POSTĘPOWANIE KLAUZULOWE – KOLEJNY ETAP INFORMATYZACJI WYMIARU SPRAWIEDLIWOŚCI

Elektroniczne postępowanie klauzulowe, to kolejny, po elektronicznym postępowaniu upominawczym, etap informatyzacji wymiaru sprawiedliwości w jego aspekcie procesowym.

Głównym założeniem, które legło u podstaw dalszego rozwoju procedury cywilnej, pod względem teleinformatycznym, jest pełna realizacja zasady szybkości postępowania. Przejawia się ona odciążeniem tradycyjnych wydziałów cywilnych od spraw o ograniczonym, względnie minimalnym stopniu skomplikowania merytorycznego, a na tyle licznych, że dezorganizują pracę wydziałów, rozciągając w czasie rozpoznawanie spraw, wymagających przeprowadzenia rozprawy. Nie bez znaczenia pozostaje tutaj także zasada ekonomiki procesowej, która przejawia się poprzez zminimalizowanie kosztów tak dla strony inicjującej postępowanie (koszty: doręczeń, odpisów; dodatkowych wykwalifikowanych kadr itp.), ale przede wszystkim dla sądu, który eliminuje w dużym stopniu podobne, w znaczeniu przedmiotowym, koszty, nie mniej w o wiele wyższej wysokości. Istotnym dla twórców założeń nowego rozwiązania procedowania jest, podobnie jak w przypadku elektronicznego postępowania upominawczego, funkcjonowanie w oparciu o specjalnie do tego przygotowany program informatyczny, z praktycznie całkowitym wyłączeniem obiegu papierowego.

W założeniach ustawodawcy, elektroniczne postępowanie klauzulowe będzie wprowadzane etapowo, poczynając od elektronicznego bankowego tytułu egzekucyjnego, któremu to, między innymi, poświęcona została, pozostająca na etapie legislacyjnym, Ustawa o zmianie ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz.U. nr 16 poz.93 z późn. zm.), ustawy z dnia 17 listopada 1964 r.– Kodeks postępowania cywilnego (Dz.U. nr 43 poz.296 z późn. zm.) oraz niektórych innych ustaw.

Na jej tle można wyróżnić ścisłe, a zarazem bezwarunkowe, zasady, na których opiera się funkcjonowanie elektronicznego postępowania o nadanie klauzuli wykonalności elektronicznemu bankowemu tytułowi egzekucyjnemu:

Składanie pism wyłącznie za pośrednictwem systemu teleinformatycznego (od strony wierzyciela, tj. banku, z wyłączeniem osoby dłużnika, któremu pozostawia się prawo wyboru).

Powyższe wprowadza dodany art.781^2 k.p.c., gdzie w § 1 stanowi się: „wniosek o nadanie klauzuli wykonalności bankowemu tytułowi egzekucyjnemu w postaci elektronicznej składa się wyłącznie za pośrednictwem systemu teleinformatycznego". Tym samym wierzyciel (w tym wypadku wyłącznie bank – wierzyciel jednorodzajowy) ma obowiązek korzystania z systemu teleinformatycznego, co wyklucza tradycyjną formę komunikacji z sądem, tj. złożenie wniosku i pism w formie papierowej. Konsekwencją niezastosowania się do wymogu ustawodawcy jest bezskuteczność złożonego wniosku (pisma), o czym mowa w znowelizowanym art.125 § 2^1 k.p.c., który otrzyma brzmienie: „jeżeli przepis szczególny tak stanowi (w tym przypadku art.781^2 k.p.c.) albo dokonano wyboru sposobu wnoszenia pism w sprawie za pośrednictwem systemu teleinformatycznego, pisma procesowe wnosi się wyłącznie za pośrednictwem tego systemu. Pisma nie wniesione w ten sposób nie wywołują skutków prawnych, jakie ustawa wiąże z wniesieniem pisma do sądu, o czym sąd poucza wnoszącego pismo (…)". Istotnym novum jest tutaj nie zwrot wniosku, czy też pisma, stosownie do brzmienia art.130 § 2 k.p.c., lecz zawiadomienie (zarządzenie) przewodniczącego o bezskuteczności czynności dokonanej w niewłaściwy sposób.

Jak zaznaczono wyżej, wyjątkiem od reguły składania pism wyłącznie za pośrednictwem systemu teleinformatycznego jest sytuacja dłużnika, który ma prawo wyboru: forma papierowa względnie teleinformatyczna, z tym jednak zastrzeżeniem, iż wybór tej ostatniej jest dla niego wiążący i wszystkie pisma dla swej skuteczności winny być wówczas składane w tym systemie. Dłużnik może w każdym czasie zrezygnować z tej formy wnoszenia pism składając, tak jak przy wyborze, stosowne oświadczenie w systemie teleinformatycznym (art.125 § 2^3 k.p.c.). Wybór formy papierowej nie wyłącza działania sądu wyłącznie w systemie teleinformatycznym, jak zakłada to § 3 art.781^2 k.p.c. stanowiąc, iż czynności sądu, referendarza i przewodniczącego są utrwalane wyłącznie w systemie teleinformatycznym, a wytworzone w ich wyniku dane w postaci elektronicznej opatrywane są bezpiecznym podpisem elektronicznym w rozumieniu art.3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.", lecz rodzi konieczność podjęcia czynności technicznych, polegających na przetworzeniu dokumentu papierowego na postać elektroniczną (digitalizacja).

Pisma podpisywane podpisem elektronicznym, weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, w rozumieniu Ustawy o podpisie elektronicznym, albo podpisem elektronicznym, potwierdzonym profilem zaufanym e–PUAP, w rozumieniu Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

Art.126 § 5 k.p.c. otrzyma w związku z tym brzmienie: „Pismo procesowe wniesione za pośrednictwem systemu teleinformatycznego opatruje się bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu lub podpisem elektronicznym, potwierdzonym profilem zaufanym Elektronicznej Platformy Usług Administracji Publicznej".

Do pisma (wniosku) składanego w systemie teleinformatycznym dołącza się elektronicznie poświadczone odpisy pełnomocnictw i dokumentów.

Założenie to jest konsekwencją projektu zmiany art.128 § 2 k.p.c. i 129 § 2 k.p.c., gdzie stanowi się, iż „do pisma procesowego wnoszonego za pośrednictwem systemu teleinformatycznego dołącza się poświadczone elektronicznie odpisy załączników." – art.128 § 2 k.p.c., a „zamiast oryginału dokumentu strona może złożyć odpis dokumentu, jeżeli jego zgodność z oryginałem została poświadczona przez notariusza albo przez występującego w sprawie pełnomocnika strony będącego adwokatem, radcą prawnym, rzecznikiem patentowym lub radcą Prokuratorii Generalnej Skarbu Państwa. Elektroniczne poświadczenie odpisu dokumentu następuje z chwilą wprowadzenia tego dokumentu do systemu teleinformatycznego." – art.129 § 2 k.p.c.

Rozwinięciem powyższego, z punktu widzenia elektronicznego bankowego tytułu egzekucyjnego jest nowelizowany art.97 ust.4 ustawy – Prawo bankowe, gdzie stanowi się, iż „do wniosku o nadanie klauzuli wykonalności bankowemu tytułowi egzekucyjnemu, poza bankowym tytułem egzekucyjnym w postaci elektronicznej, dołącza się odpisy dokumentów poświadczone elektronicznie. Odpis powinien zostać poświadczony przez wnioskodawcę za zgodność z oryginałem.".

Zauważyć przy tym należy, iż w przeciwieństwie do elektronicznego postępowania upominawczego, elektroniczne postępowanie w przedmiocie nadania klauzuli wykonalności elektronicznemu bankowemu tytułowi egzekucyjnemu, dla oceny zasadności wniosku, wymaga przeprowadzenia postępowania dowodowego. Postępowanie to koncentruje się rzecz jasna na dowodzie z dokumentu poświadczonego elektronicznie w postaci czynności bankowej, z którą w bezpośrednim związku pozostaje elektroniczny bankowy tytuł egzekucyjny, oświadczenia o poddaniu się egzekucji, ewentualnie w postaci innych dokumentów, które okażą się konieczne dla zweryfikowania zasadności wniosku o nadanie klauzuli wykonalności bankowemu tytułowi egzekucyjnemu. Wszystkie dokumenty pozwalające ocenić wniosek pod względem merytorycznym wprowadzane są do sytemu jako skan dokumentu poświadczony elektronicznie.

Pismo składane drogą elektroniczną musi był opłacone – brak opłaty rodzi bezskuteczność wniosku.

Problematyce tej ustawodawca poświęca swą uwagę w treści art.130 § 6 i 7 k.p.c. Podobnie jak w przypadku wymogu składania pism w systemie teleinformatycznym, brak opłacenia wniosku skutkować będzie zawiadomieniem w formie zarządzenia przewodniczącego o bezskuteczności wniosku/pisma podlegającego opłacie. To samo dotyczy sytuacji, gdy złożono tzw. „paczkę wniosków", a uiszczona opata nie odpowiada sumie opłat należnych od wszystkich pism.

Wniosek o nadanie klauzuli wykonalności elektronicznemu bankowemu tytułowi egzekucyjnemu może dotyczyć tylko jednego tytułu (art.7812 § 2 k.p.c.).

Oznacza to, iż objęcie jednym wnioskiem kilku elektronicznych bankowych tytułów egzekucyjnych będzie skutkować jego bezskutecznością, o czym przewodniczący w formie zarządzenia zawiadomi wierzyciela.

Elektroniczne rozpoznawanie wniosku – wszystkie czynności sądu, referendarza i przewodniczącego są utrwalane wyłącznie w systemie teleinformatycznym, a wytworzone w ich wyniku dane w postaci elektronicznej opatrywane są bezpiecznym podpisem elektronicznym, w rozumieniu art.3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (art.7812 § 3 k.p.c.), z tym zastrzeżeniem, iż doręczenia dla dłużnika dokonywane są w systemie tradycyjnym do czasu ewentualnego wyboru wnoszenia pism za pośrednictwem systemu teleinformatycznego.

Szeroka kognicja orzecznicza referendarzy sądowych

Ustawodawca w projektowanej zmianie do ustawy – Kodeks postępowania cywilnego rozszerzył w sposób istotny kompetencje referendarzy sądowych stanowiąc w art.781 § 1^1 k.p.c., iż „czynności w sprawach o nadanie klauzuli wykonalności tytułom egzekucyjnym, o których mowa w art.777 § 1, może wykonywać referendarz sądowy" i dotyczy to wszystkich czynności, w tym tych o charakterze wpadkowym jak: umorzenie postępowania wobec cofnięcia wniosku; odrzucenie wniosku; przekazanie sprawy zgodnie z właściwością miejscową itp.

Powyższe niewątpliwie rozszerza się także na zdolność orzeczniczą referendarzy w sprawach o nadanie klauzuli wykonalności na rzecz następcy prawnego oraz na małżonka dłużnika w ogólności, co w obrębie elektronicznych bankowych tytułów egzekucyjnych podlegać będzie rozpoznaniu w ramach elektronicznego postępowania klauzulowego. Podobnie rzecz tyczy dalszych tytułów wykonawczych, gdy tym pierwotnym był elektroniczny bankowy tytuł egzekucyjne opatrzony sądową klauzulą wykonalności.

Jako że wnioski w ramach omawianego postępowania będą rozpoznawane przez referendarzy sądowych, procedura zyskuje na szybkości, albowiem środki zaskarżenia w postaci skarg na orzeczenie referendarza rozpoznawane zostaną przez sędziego danego sądu, będącego przewodniczącym wydziału, co w znacznym stopniu eliminuje zaangażowanie sądów odwoławczych w merytoryczne badanie poprawności orzeczniczej.

Powyższe uwagi dotyczyły aspektów elektronicznego rozpoznawania wniosków o nadanie klauzuli wykonalności elektronicznym, bankowym tytułom egzekucyjnym w ujęciu stricte proceduralnym. Nie mniej istotne, w tej mierze, pozostają zmiany w zakresie regulacji bankowego tytułu egzekucyjnego, zawarte w omawianej nowelizacji, obejmującej zmianę ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U. z 2012 r. poz.1376,1385,1529).

Szczególnie znaczące to wprowadzenie wyłącznie elektronicznej formy bankowego tytułu egzekucyjnego i opatrzenie go bezpiecznym podpisem elektronicznym, w rozumieniu art.3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz.262). Zmianą wobec aktualnego brzmienia art.96 ust.2 Prawa bankowego są: wskazanie w treści e–bte kwoty zadłużenia, do której bank może wystawić bankowy tytuł egzekucyjny, wskazanie sposobu wyrażenia odsetek zmiennych w bte tj., że odsetki zmienne mogą być wyrażone wyłącznie na podstawie stopy referencyjnej ustalanej przez Radę Polityki Pieniężnej i ogłaszanej w Dzienniku Urzędowym Narodowego Banku Polskiego albo stopy procentowej pochodzącej z innego publicznie dostępnego źródła, która może być zweryfikowana przez strony czynności bankowej. Są to zatem

kolejne elementy, obok dotychczas wymaganych, podlegające weryfikacji przy ocenie poprawności wystawienia bankowego tytułu egzekucyjnego. Wyeliminowano natomiast zapis, iż bankowy tytuł egzekucyjny należy opatrzyć pieczęcią banku wystawiającego tytuł oraz podpisami osób uprawnionych do działania w imieniu banku a to wobec wprowadzenia ust.1, a zgodnie z którym bankowe tytuły egzekucyjne, o jakich mowa w ust.1, są wystawiane wyłącznie w systemie teleinformatycznym i opatrywane bezpiecznym podpisem elektronicznym, w rozumieniu art.3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz.262). Co istotne, wydane przez Ministra Sprawiedliwości rozporządzenia wykonawcze określać będą dokładne brzmienie elektronicznego bankowego tytułu egzekucyjnego tak, by wyeliminować brak jednolitości w orzecznictwie. Rzecz tyczy tu w szczególności problemu poprawnego określania roszczeń odsetkowych w taki sposób, by możliwym była ich weryfikacja przez dłużnika oraz aby uzyskany w oparciu o bankowy tytuł egzekucyjny tytuł wykonawczy nadawał się do wykonania.

Formę elektroniczną przewidziano również dla oświadczenia o poddaniu się egzekucji, nie eliminując formy tradycyjnej – pisemnej. Wybór należy do wierzyciela – banku, który dokonuje czynności bankowej z dłużnikiem. Zmianą do obecnego brzmienia art. 97 Prawa bankowego, w zakresie elementów, jakie winno zawierać oświadczenie o poddaniu się egzekucji, jest oznaczenie czynności bankowej, z której wynika zadłużenie.

Na koniec nie sposób nie wspomnieć o kwestiach organizacyjnych, związanych z procedowaniem w ramach elektronicznego postępowania o nadanie klauzuli wykonalności elektronicznemu bankowemu tytułowi egzekucyjnemu.

Czynności te powierzone zostaną specjalnie w tym celu utworzonym wydziałom cywilnym, które powstaną na bazie dotychczasowych, na chwilę obecną etapowo wygaszanych, Ośrodków Migracji Ksiąg Wieczystych. Pozyskana w ten sposób kadra orzecznicza (referendarze sądowi) oraz sekretarska, a nadto zaplecze techniczno – biurowe, eliminuje wydatki Ministerstwa Sprawiedliwości na tworzenie i wyposażanie tego rodzaju jednostek.

W przeciwieństwie do elektronicznego postępowania upominawczego, nie będzie to jeden wydział w skali kraju, lecz projektuje się ich 10, które swą właściwością miejscową obejmować będą obszar danej apelacji, względnie dwóch. Wiąże się z tym konieczność zmiany ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych, która to stworzy podstawy do wskazania przez Ministra Sprawiedliwości tak sądów rejonowych właściwych do rozpoznawania spraw w postępowaniu o nadanie klauzuli wykonalności elektronicznemu bankowemu tytułowi egzekucyjnemu (zmiana art.20 poprzez wprowadzenie pkt 7), jak i wydziałów odwoławczych, rozpoznających ewentualne środki zaskarżenia od orzeczeń wydawanych w ramach postępowania o nadanie klauzuli wykonalności elektronicznym bankowym tytułom egzekucyjnym.

Przewiduje się, iż wyspecjalizowane w elektronicznym postępowaniu klauzulowym wydziały cywilne powstaną w sądach rejonowych, jako kolejny wydział cywilny. Te zaś wyznaczone zostaną przez poszczególne wytypowane sądy okręgowe, obejmując tym samym następujące obszary właściwości:

Sąd Okręgowy	**Wydział Cywilny (właściwy dla elektronicznego postępowania klauzulowego)**	**Obszar właściwości**
Sąd Okręgowy we Wrocławiu	Wrocław	Apelacja Wrocławska
Sąd Okręgowy w Krośnie	Krosno	Apelacja Krakowska
Sąd Okręgowy w Siedlcach	Siedlce	Apelacja Lubelska
Sąd Okręgowy w Słupsku	Słupsk	Apelacja Gdańska
Sąd Okręgowy w Łomży	Łomża	Apelacja Białostocka
Sąd Okręgowy w Zielonej Górze	Zielona Góra	Apelacja Poznańska
Sąd Okręgowy w Elblągu	Elbląg	Apelacja Warszawska i Łódzka
Sąd Okręgowy w Gorzowie Wielkopolskim	Gorzów Wielkopolski	Apelacja Szczecińska
Sąd Okręgowy w Tarnobrzegu	Nisko	Apelacja Rzeszowska
Sąd Okręgowy w Gliwicach	Racibórz	Apelacja Katowicka

Przedstawiona analiza najistotniejszych zagadnień związanych z nowym, bo elektronicznym postępowaniem klauzulowym zawężonym na chwilę obecną do bankowego tytułu egzekucyjnego, co daje podstawy do konstatacji, iż zasadnym byłoby w niedalekiej przyszłości rozszerzenie tego postępowania na inne, jeśli nie wszystkie szczególne rodzaje postępowania klauzulowego, jak choćby na następcę prawnego (art.788 k.p.c.), czy na małżonka dłużnika (art.787 k.p.c.) itd.

Abstract

In turn, Beata Wojtowicz-Wojniczka in the article, "Electronic enforcement warrant – next phase of computerization of Justice" examines the most important issues concerning a new, as it is in electronic form, enforcement warrant, narrowed at the moment the bank enforcement title. It gives the author the basis for a conclusion that it would be reasonable in the near future to extend this procedure to other, if not all of the specific types of conduct granting enforcement clause, such as the successor in interest (Article 788 of PCCP) or to the spouse of the debtor (Article 787 of PCCP), etc. Beata Wojtowicz-Wojniczka explains the procedure for signing the documents with electronic signature verified by a valid qualified certificate, within the meaning of the Act on electronic signature or electronic signature attested by a trusted profile e-PUAP, within the meaning of the Act on the computerization of entities performing public tasks. She also notes that the letter (proposal) submitted in the ICT system is accompanied by electronically certified copies of powers of attorney and documents. She emphasizes that the letter submitted electronically must be paid – the lack of charges raises the futility of the application. An application for a declaration of enforceability electronic banking writ of execution may involve only one title (Article.7812 § 2 PCCP).

JANUSZ ZAGROBELNY

PODPIS ELEKTRONICZNY W POSTĘPOWANIU KARNYM – GLOSA KRYTYCZNA DO POSTANOWIENIA SN Z DNIA 26 MARCA 2009 R. (SYGN. AKT I KZP 39/08)

Informatyzacja postępowań sądowych jest postępującym procesem w polskim ustawodawstwie. Pomimo wprowadzania do polskiego porządku prawnego kolejnych instytucji, mających na celu poszerzenie zastosowania rozwiązań informatycznych w postępowaniach sądowych[1], najtrudniejszą przeszkodą w szerszym stosowaniu narzędzi informatycznych pozostaje bariera psychologiczna. Grupą uczestników postępowań sądowych cechującą się najsilniejszym dystansem do narzędzi informatycznych pozostają wciąż sędziowie[2], w dużej mierze przywiązani do wyuczonej metodologii pracy. Tendencję tą przypisać można najwyraźniej również sędziom Sądu Najwyższego, orzekającym w sprawie będącej przedmiotem niniejszej glosy.

Sąd Najwyższy, w postanowieniu z dnia 26 marca 2009 r. (sygn. akt I KZP 39/08) uznał: *„nie wywołuje skutku procesowego w postaci wniesienia środka odwoławczego oświadczenie procesowe strony przesłane w formie dokumentu elektronicznego, zgodnie z wymogami ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. Nr 130, poz.1450 ze zm.), albowiem zarówno w procedurze wykroczeniowej, jak i w procedurze karnej taka forma czynności procesowej nie jest przewidziana"*.

W opisywanej sprawie Sąd Rejonowy uznał oskarżonego za winnego popełnienia dwóch wykroczeń oraz wymierzył mu karę grzywny. Siódmego dnia po doręczeniu obwinionemu uzasadnienia wyroku, do elektronicznej skrzynki podawczej Sądu Rejonowego wpłynął w formie elektronicznej dokument adresowany do Sądu Okręgowego za pośrednictwem Sądu Rejonowego, zawierający wszelkie cechy apelacji za wyłączeniem własnoręcznego podpisu oraz oznaczenie obwinionego jako jej autora. Z urzędowego poświadczenia przedłożenia wynikało, że dokument przesłany w formie elektronicznej został opatrzony bezpiecznym podpisem elektronicznym, weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, zgodnie z wymogiem ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. Nr 130, poz.1450 ze zm.). Treść tego dokumentu, w formie wydruku komputerowego, została załączona do akt sprawy.

Przewodniczący wydziału stwierdził, że apelacja odpowiada wymogom formalnym, zarządził jej przyjęcie, a następnie akta zostały przesłane do Sądu Okręgowego.

Konsekwentnie, upoważniony sędzia Sądu Okręgowego wydał zarządzenie o wyznaczeniu rozprawy apelacyjnej. Na tej rozprawie, Sąd powziął wątpliwości, co do dopuszczalności wniesienia apelacji w postaci dokumentu elektronicznego oraz postanowił o zadaniu następującego pytania prawnego Sądowi Najwyższemu:

„Czy przesłanie do sądu pisma procesowego – apelacji w formie dokumentu elektronicznego opatrzonego bezpiecznym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu, o jakim mowa w art.3 pkt 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz.U. z 2001 r. Nr 130, poz.1450 ze zm.) czyni zadość, w kontekście brzmienia art.5 ust.2 wskazanej ustawy, wynikającym z art.105 § 1 k.p.s.w. i art.119 § 1 k.p.k. w zw. z art.38 § 1 k.p.s.w. wymogom formalnym apelacji, jako pisma procesowego?"

Sąd Najwyższy, pomimo powołania się na określoną w art.5 ust.2 ustawy o podpisie elektronicznym (u.p.e.) zasadę równoważności podpisu elektronicznego z podpisem własnoręcznym, uznał że przepis ten **nie znajduje** zastosowania w stosunku do postępowań sądowych.

Uzasadnieniem tego twierdzenia miała być norma wynikająca z art.58 ust.2 u.p.e., nakładająca na organy władzy publicznej obowiązek „umożliwienia odbiorcom usług certyfikacyjnych wnoszenia podań i wniosków oraz innych czynności w postaci elektronicznej".

Z oceny Sądu Najwyższego wynika, że postanowienia u.p.e. nie mają charakteru samodzielnego (*„ustawodawca, pomimo treści art.5 ust.2 u.p.e., dopiero w drodze odrębnych aktów prawnych wskazuje zakres stosowania dokumentu elektronicznego"*), a wymagają dopiero „implementacji" w odpowiednich kodeksach. Argumentem przemawiającym za takim stanem rzeczy w ocenie Sądu Najwyższego miało być również stosowanie tak w art.125 k.p.c. jak i w art.63 § 1 k.p.a. wyraźnych dozwoleń na stosowanie podpisu elektronicznego.

Sąd Najwyższy wywiódł również, że brak w k.p.k. odpowiednich przepisów dotyczących wnoszenia pism procesowych przez strony drogą elektroniczną, *„stanowi lukę aksjologiczną, co musi zostać odczytane jako regulacja negatywna"*. Ostatecznie, Sąd Najwyższy skonstatował, że *„elektroniczna forma wymiany dokumentów (art.1 pkt 6 ustawy) nie odnosi się do czynności procesowych w postępowaniu sądowym, albowiem określenie „wymiana informacji", związanych z załatwianiem spraw wiązać należy z czynnościami administracji sądowej, a nie z czynnościami procesowymi, co do których w ustawach procesowych nie operuje się pojęciem „informacji". Przyjąć więc trzeba, że użyte w tej*

[1] Por. ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2001 r., Nr 130 poz. 1450), ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r., Nr 64, poz. 565) jak również art. 125 k.p.c.

[2] R. Cisek, E-Protokół i inne „nowinki" informatyzacji sądownictwa, czyli po co to komu?, Kwartalnik Naukowy Prawo Mediów Elektronicznych 3/2011.

ustawie określenie „sąd" oznacza sąd w znaczeniu organizacyjno-ustrojowym, a nie procesowym."

Nie sposób zgodzić się z tak przedstawionymi racjami Sądu Najwyższego.

Na wstępie warto zauważyć, że rozumowaniem nieuprawnionym jest rozróżnianie administracyjnej roli sądu od jej roli orzeczniczej w braku wyraźnego ustawowego rozróżnienia tych ról przez u.p.e. (*lege non distinguente).* Co więcej, wbrew twierdzeniu Sądu Najwyższego, postępowania sądowe, w swojej istocie, niewątpliwie stanowią formę wymiany informacji – w naukach informatycznych pojęcie „informacja" jest interpretowane jako pojęcie możliwie szerokie. W szczególności wymianą informacji jest przekazywanie treści pism procesowych.

Ponadto, art. 5 ust. 2 u.p.e. nie obejmuje treści mogących sugerować warunkowość swojego zastosowania, bądź ograniczenia swojego zakresu podmiotowego do organów odpowiedzialnych za legislację, jak zdaje się wywodzić Sąd Najwyższy. Co więcej, u.p.e. stanowi ustawę, która implementowała do prawa polskiego postanowienia art. 5 dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, i jako taka, zgodnie z utrwalonym orzecznictwem ETS, podlegała zarówno prounijnej wykładni, jak i obowiązkowi bezpośredniego stosowania dyrektywy w przypadku:

a) braku terminowej jej implementacji,
b) bezwarunkowości normy przewidzianej w dyrektywie,
c) wystarczającej jej precyzyjności.

Normy przewidziane w art. 5 wyżej wspomnianej dyrektywy nakazują Rzeczypospolitej Polskiej zapewnić, by kwalifikowane podpisy elektroniczne *„spełniały wymogi prawne podpisu w odniesieniu do danych w formie elektronicznej w ten sam sposób, co podpis odręczny w odniesieniu do danych znajdujących się na papierze"*. Nie jest to norma o charakterze warunkowym, jej hipoteza i dyspozycja są precyzyjne, a – jako część *acquis communautaire* w chwili wstąpienia Polski do UE – data jej implementacji upłynęła 1 maja 2004 r.

Wobec powyższego, Sąd Najwyższy, nawet w braku stosownych uregulowań ustawowych, powinien był zastosować bezpośrednio dyrektywę, lub co najmniej dokonać prounijnej wykładni przepisów u.p.e. (np. poprzez zastosowanie analogii z art. 78 § 2 k.c.), umożliwiającej pełne wprowadzenie w życie norm wspomnianej dyrektywy.

Nawet przyjąwszy brak wyżej powołanego prawa unijnego, obligującego do zastosowania prounijnej wykładni – rozumowanie SN uznające art. 58 ust. 2 u.p.e. jako wystarczające uzasadnienie dla odmowy zastosowania art. 5 ust. 2 u.p.e., stanowi nietrafną interpretację tego przepisu. Przepis ten nakłada na *„organy władzy publicznej"* obowiązek *„umożliwienia odbiorcom usług certyfikacyjnych wnoszenie podań i wniosków oraz innych czynności w postaci elektronicznej w przypadkach, gdy przepisy prawa wymagają składania ich w określonej formie lub według określonego wzoru."*. Jest to przepis, którego celem było zapewnienie **dostępności** wzorca dokumentu w formie elektronicznej**, w przypadku, gdy taki wzór jest wymagany**. Jak trafnie zauważył Tomasz Kościelny w komentarzu do art. 58 u.p.e.[3], naczelnym przykładem zastosowania art. 58 ust. 2 u.p.e. miało być umożliwienie wnoszenia formularzy PIT drogą elektroniczną.

Przykładem czynności sądowej, dokonywanej według wzorca określonego w rozporządzeniu, jest np. pozew wniesiony w postępowaniu cywilnym uproszczonym, czy oświadczenie o stanie rodzinnym, majątku, dochodach i źródłach utrzymania. Konsekwentnie, sądy na swoich stronach internetowych udostępniają wzorce pism umożliwiające ich wypełnienie, oraz wysłanie ich drogą elektroniczną[4].

W postępowaniu karnym natomiast, pisma procesowe nie mają charakteru ściśle sformalizowanego. Kodeks postępowania karnego określa jedynie ich elementy obligatoryjne (np. art. 119 k.p.k.). Sąd oparł swoje rozumowanie na stwierdzeniu, że ustawodawca, w wykonaniu normy art. 58 ust. 2 u.p.e., nie zmodyfikował odpowiednio art. 428 k.p.k., wymagającego wniesienia dokumentu na piśmie.

W mojej ocenie, rozumowanie to jest zasadniczo nietrafne. Art. 58 u.p.e., mający charakter przepisu nakazującego usuwanie utrudnień w stosowaniu podpisu elektronicznego na równi z własnoręcznym, w drodze wykładni przez SN został zastosowany jako **bariera** stojąca na przeszkodzie zastosowania podpisu elektronicznego – stanowi to całkowite zignorowanie *ratio legis* tego przepisu.

Art. 5 ust. 2 u.p.e. statuuje zasadę akceptacji podpisu elektronicznego. Rzecz jasna, wyjątki od tej zasady winny być wprowadzane w drodze przepisu szczególnego. Niedopuszczalnym natomiast jest twierdzenie, że wyjątek taki może ustanowić **milczenie** ustawodawcy w postaci „luki aksjologicznej".

Wbrew rozumowaniu Sądu, niespełnienie określonego w art. 428 § 1 k.p.k. wymogu pisemności apelacji jest **szanowane** przez zastosowanie art. 8 u.p.e., który jawnie zakazuje *„odmawiania ważności i skuteczności podpisowi elektronicznemu tylko na tej podstawie, że istnieje w postaci elektronicznej"*. Jest to przepis mający charakter typowo antydyskryminacyjny – w tym przypadku – zakazujący dyskryminacji dokumentów podpisanych za pomocą podpisu elektronicznego. Dyskryminacja zaś, może występować w formie dyskryminacji bezpośredniej (tj. bezpośredniego zastosowania określonej cechy jako kryterium w danej sprawie) oraz dyskryminacji pośredniej (tj. zastosowanie pozornie neutralnego kryterium, które wywiera skutek wobec wszystkich lub znacznej części podmiotów charakteryzujących się daną cechą)[5].

Stąd, jakkolwiek istotnie – Sąd Najwyższy nie odmówił ważności podpisowi (tj. nie doszukał się braku wynikającego z art. 119 k.p.k.), to wskazał na brak formy pisemnej określonej w art. 428 k.p.k. Nie ulega wątpliwości, że podpis elektroniczny ze swojej natury nie może występować w dokumentach o charakterze czysto pisemnym. Sąd Najwyższy, stosując pozornie neutralne kryterium różnicujące – w istocie dokonał wykładni niemożliwej do pogodzenia z art. 8 u.p.e.

Podsumowując, stanowisko przyjęte przez Sąd Najwyższy, czyniąc użytek z argumentacji na granicach rozumowania *contra legem*, skutkuje niewątpliwie niepożądanym brakiem możliwości wnoszenia pism procesowych drogą elektroniczną. Wnioskiem z tego orzeczenia zdaje się być potrzeba „implementacji" w k.p.k. przepisów o podpisie elektronicznym. Pozostaje zadać pytanie, jak bardzo precyzyjnym językiem będzie musiał posłużyć się ustawodawca, by judykatura go w pełni zaakceptowała?

[3] T. Kościelny, K. Szaniawski, Komentarz do ustawy o podpisie elektronicznym, Kraków 2003.

[4] Por. http://www.wroclaw.sa.gov.pl/pl/dokumenty/zwolnienie_od_kosztow_sadowych (odczyt z dnia 1 kwietnia 2013 r.).

[5] Por. np. art. 183a § 3-4 k.p.

Abstract

In the study entitled: „Electronic Signature in criminal proceedings..." Janusz Zagrobelny notes that the standpoint adopted by the Supreme Court, making use of the argument on the limitations of contra legem reasoning, undoubtedly results in an undesirable lack of opportunities for submitting pleadings electronically. The conclusion of this judgment seems to be the need to „implement" in the Polish Code of Criminal Procedure regulations governing electronic signatures. It remains, in author's opinion, to pose a question of how precise language will have the legislature to use, to make the judicature to fully accept it? He also notes that despite the introduction of the Polish legal system new institutions, aiming at expanding the ICT use to legal proceedings, the hardest obstacle to the wider use of these tools is a psychological barrier. He refers to the fact that the Supreme Court, despite citing Article 5, section 2 of the Act on Electronic Signatures (upe), relying on the principle of equivalence of electronic signatures with handwritten signature, found that this provision does not apply in relation to court proceedings.

DAN JERKER B. SVANTESSON[1]

PRIVATE INTERNATIONAL LAW AND THE INTERNET – AN AUSTRALIAN PERSPECTIVE AND BEYOND[2]

1. Introduction

With falling airline ticket prices, it has become popular to book round-the-world tickets. Such tickets typically allow the passenger a limit the number of stops on the path around the globe. In a similar manner, while this article in a sense represents a global circumnavigation of the topic of Private International Law and the Internet, it only makes a limited number of 'stops'. In other words, I make no claim of providing an exhaustive treatment of this broad and fascinating topic. Rather, the article seeks to give an indication of some of the most interesting recent developments in this field, while at the same time outlining and discussing the basic, ever-present fundamentals of the topic.

As is indicated in the title, the article is written from an Australian perspective. That should, however, not be seen as a strict delineation of the article's geographical scope. Instead, and to reconnect to the airline analogy above, Australia can be seen as the location from which the journey takes off.

2. Australian Law as the Point of Departure

Australia's main 'claim to fame' in Internet-related law is the High Court of Australia's decision in a dispute between a business man from the state of Victoria, on the one hand, and US publishing giant Dow Jones & Company Inc on the other[3]. The case arose out of the fact that Dow Jones published an article allegedly defamatory of Mr Gutnick. The article was available both in a magazine and online and was mainly read in the US. However, a small number of copies of the magazine were distributed in Victoria, and the website containing the article had a small number of subscribers in Victoria. No exact number of readers could be established for either the web or magazine version of the article, but it was suggested that important Victorian business people had in fact read the article.

Mr Gutnick sought to take legal action in Victoria and under the laws of Victoria. If one allows room for speculations, it may seem reasonable to suspect that, apart from the obvious convenience of litigating 'at home', the potential impact of the free speech provision in the First Amendment of the US Constitution may have constituted a significant incentive to avoid litigation in the US.

In any event, the matter reached the High Court of Australia, and that Court had to decide whether Mr Gutnick could sue in Victoria (the question of jurisdiction) and, if such a law suit could proceed, which country's substantive law should be applied (the choice of law question).

Interestingly, the judges of the High Court took fundamentally different, in fact bi-polar, positions on the topic of the arguable novelty of the Internet as a medium for communication. Kirby J recognised the Internet as a technological revolution and noted: *Intuition suggests that the remarkable features of the Internet (which is still changing and expanding) makes it more than simply another medium of human communication. It is indeed a revolutionary leap in the distribution of information, including about the reputation of individuals*[4].

In sharp contrast to this, Callinan J proclaimed that:
The Internet, which is no more than a means of communication by a set of interconnected computers, was described, not very convincingly, as a communications system entirely different from pre-existing technology[5].

Despite the bi-polarity of these positions, both these judges came to the same conclusion on the matters before the Court.

2.1 Jurisdiction

As far as jurisdiction is concerned, it may be of interest to start with some observations about the differences between countries abiding by the common law system and countries adhering to the civil law system. While the civil law world is diverse indeed, many civil law countries rely on guidance found in the statute that regulates procedural questions in domestic disputes when assessing whether to claim jurisdiction in cross-border cases. Examples of this can be found in eg, the Swedish *Rättegĺngsbalken*[6] and the German *Zivilprozeßordnung*. In contrast, many common law countries have adopted a structure under which it could be said that there are three different bases for a court claiming jurisdiction:

- presence (ie, service upon a party present in the jurisdiction);
- submission (ie, the defendant submitting to the jurisdiction of the court); or
- so-called Order 11 grounds (ie, statutory grounds for serving a party outside the jurisdiction).

[1] Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

[2] This article is based on a presentation titled 'Private International Law and the Internet (An Australian Perspective)' given by the author at University of Wroclaw on 25 June 2013. In part, the article draws, and builds, upon several works published previously by the author, including Dan Svantesson, Private International Law and the Internet (Kluwer Law International, 2nd ed, 2012).

[3] Dow Jones & Company Inc v Gutnick [2002] HCA 56.

[4] Ibid [164].

[5] Ibid [180].

[6] Rättegĺngsbalk [Swedish Code of Judicial Procedure] (Sweden) (1942:740).

While the first two ought to be relatively self-explanatory, the third may require some clarification. The expression 'Order 11 rules' stems from the fact that these rules were originally found in Order 11 of the pre-EEC English Rules of the Supreme Court[7]. Each major court has a set list, based on statute, of grounds upon which it may claim jurisdiction.

The relevant list of jurisdictional grounds, in the *Gutnick* case, was found in the *General Rules of Procedure in Civil Proceedings* 1996 (Vic), and more specifically, the relevant jurisdictional rule was found in Rule 7.01(1) of the Victorian Rules reading as follows:

> (1) Originating process may be served out of Australia without order of the Court where:
> (i) the proceeding is founded on a tort committed within Victoria;
> (j) the proceeding is brought in respect of damage suffered wholly or partly in Victoria and caused by a tortious act or omission wherever occurring.

Thus, Gutnick would be allowed to sue Dow Jones in Victoria if the Court concluded either that the tort of defamation was committed within Victoria or that the damages Gutnick suffered from the defamation were suffered wholly or partly in Victoria.

Under the circumstances, the majority of the High Court of Australia found that Victoria may exercise jurisdiction of Dow Jones, as the tort sued for was committed in Victoria[8] and damages were suffered in Victoria[9].

Having made these observations, it is interesting to pause to consider the similarities and differences between the approach taken by the High Court of Australia and the approach taken by the European Court of Justice (ECJ).

2.1.1 A First Stopover – European Union law and the Gutnick Case

In Europe, as is well known, the question of jurisdiction in a matter such as the *Gutnick* case is regulation by the Brussels I Regulation. Relevantly, Article 2 outlines the main rule and states that: '[s]ubject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State'. To this main rule must be added Article 5(3) relevant for torts: 'A person domiciled in a Member State may, in another Member State, be sued: in matters relating to tort, delict or quasi-delict, in the courts for the place *where the harmful event occurred or may occur*' (emphasis added).

The application of these rules was tested in *Fiona Shevill et al v Presse Alliance SA*[10]. There the ECJ concluded that:

The victim of a libel by a newspaper article distributed in several Contracting States may bring an action for damages against the publisher either before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award damages for all the harm caused by the defamation, or before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised [the so-called mosaic principle][11].

However, in recent years the ECJ has had reasons to develop this further in various contexts. Most importantly, for our purposes, the ECJ had to consider the application of these rules to cross-border Internet defamation cases in the combined cases of *Martinez v MGN Limited* and *X v eDate Advertising*[12].

There, the ECJ concluded that:

> Article 5(3) of the Regulation must be interpreted as meaning that, in the event of an alleged infringement of personality rights *by means of content placed online on an internet website*, the person who considers that his rights have been infringed has the option of bringing an action for liability, in respect of all the damage caused, either *before the courts of the Member State in which the publisher of that content is established* or *before the courts of the Member State in which the centre of his interests is based*. That person may also, instead of an action for liability in respect of all the damage caused, bring his action *before the courts of each Member State in the territory of which content placed online is or has been accessible*. Those courts have jurisdiction only in respect of the damage caused in the territory of the Member State of the court seised[13].

Thus, had the *Gutnick* case been decided under European law – ie, if EU law had global effect – Mr Gutnick could have sued in the US, based on Article 2 of the Brussels Regulation having the court there decide all the worldwide damages caused. And under the *Shevill* reading of Article 5(3), Mr Gutnick could sue in every single country in which he thought his reputation had suffered damage, but only in relation to damage suffered there. However, under the 'centre of interest' rule that emerged from the *eDate/Martinez* case, he could also sue in Victoria in relation to all the worldwide damages caused.

2.1.2 A Second Stopover – the People's Republic of China and the Philippines on Technological Neutrality

Having mentioned the ECJ judgment in the combined cases of *Martinez v MGN Limited* and *X v eDate Advertising*, it would be remiss not to point out a particularly significant aspect of the approach taken by the Court in that case. For years, there has been a remarkably widespread acceptance of an aim for technology neutral law making in relation to Internet technologies. That is, legal rules are to be expressed in technology neutral terms to avoid eg such rules becoming outdated by the rapid pace of technological evolution.

However, as is clear from the above, the approach taken by the ECJ in the *eDate/Martinez* case is distinctly technology-specific – it applies to 'alleged infringement of personality rights *by means of content placed online on an internet website*'.[14]

[7] See P Smart, 'Private International Law' in Smart and Halkyard (eds), Trade and Investment Law in Hong Kong (Butterworths, 1995) 468. In fact, other common law countries also refer to these rules as Order 11 Rules (See, eg, Order 11 of the High Court Civil Procedure Rules of Ghana). Note, however, also that this is by no means universally so amongst the common law states (see, eg, the discussion of Australian law below).

[8] Dow Jones & Company Inc v Gutnick [2002] HCA 56 [48]. See also General Rules of Procedure in Civil Proceedings 1996 (Vic) r 7.01(1)(i).

[9] Ibid. See also General Rules of Procedure in Civil Proceedings 1996 (Vic) r 7.01(1)(j).

[10] Case No. C-68/93 [1995] 2 WLR 499.

[11] Ibid 500.

[12] C-509/09 and C-161/10.

[13] Ibid [52] (emphasis added).

[14] Ibid (emphasis added).

Interestingly, the EU is not alone in having departed (at least in part) from technology neutral law making. On 28 October 2010, the Standing Committee of China's National People's Congress adopted the *Law of the People's Republic of China on the Application of Law for Foreign-Related Civil Relations*. The law went into effect on 1 April 2011. Interestingly, the *Law of the People's Republic of China on the Application of Law for Foreign-Related Civil Relations* contains a technology-specific provision dealing with Internet defamation. Article 46 reads as follows:

Where such personal rights as the right of name, portrait, reputation and privacy are infringed upon via network or by other means, the laws at the habitual residence of the infringed shall apply[15].

Furthermore, on 12 September 2012, the President of the Philippines approved the *Cybercrime Prevention Act of 2012*[16]. This is clearly a technology-specific Act.

In light of these examples, it may be questioned whether we are witnessing a trend bringing the era of technology neutral law making to an end or whether they ought to be seen as isolated examples of departures from technology neutral law making. Only the future will tell.

2.2 Choice of Law

Where a court concludes that it may exercise jurisdiction over a foreign defendant, it also has to decide which country's substantive laws should govern the dispute. Thus, the High Court of Australia also needed to consider whether the laws of Victoria would govern the dispute in the *Gutnick* case as Mr Gutnick was hoping.

In relation to torts, Australia, at the time of the *Gutnick* case, applied the *lex loci delicti* – the law of the place of wrong – to defamation cases[17]. However, it is of course not immediately obvious what the place of wrong is in a case such as the *Gutnick* case.

Relying on traditional principles established in a series of older cases, the Court noted that the place of wrong is the place where the publication takes place, and publication takes place where the defamatory material is made manifest to the receiving third party, in an, to the receiver, comprehendible format.

Thus, in relation to those who read the allegedly defamatory article in Victoria, publication took place in Victoria, which then means that Victoria was the place of wrong in relation to those publications.

In 2005, Australian law as to defamation, including the relevant choice of law rule, was reformed, and the following rule was introduced for situations such as that of the *Gutnick* case:
If there is a multiple publication of matter in more than one Australian jurisdictional area, the substantive law applicable in the Australian jurisdictional area with which the harm occasioned by the publication as a whole has its closest connection must be applied in this jurisdiction to determine each cause of action for defamation based on the publication[18].

Section 11(3) then outlines the following factors that the court may take into account in determining the Australian jurisdictional area with which the harm occasioned by a publication of matter has its closest connection:

(a) the place at the time of publication where the plaintiff was ordinarily resident or, in the case of a corporation that may assert a cause of action for defamation, the place where the corporation had its principal place of business at that time; and
(b) the extent of publication in each relevant Australian jurisdictional area; and
(c) the extent of harm sustained by the plaintiff in each relevant Australian jurisdictional area; and
(d) any other matter that the court considers relevant.

2.3 Declining Jurisdiction

Courts in civil law countries typically have strictly limited discretion as to under what circumstances they may decline to exercise jurisdiction. In contrast, courts in countries following the common law tradition may, in reliance on the doctrine of *forum non conveniens*, decline to exercise jurisdiction by reference to factors such as:

– The connection between the selected forum and the subject matter of the dispute as well as the parties;
– Judicial, practical and economic advantages and disadvantages for the parties;
– The availability of alternative forums; and
– The substantive law to be applied.

While most common law countries places focus on whether there is another 'more appropriate forum', Australia has (so far) stubbornly stuck to its own focal point, that is, whether the Australian court is 'a clearly inappropriate forum'. Thus, an Australian court may decline jurisdiction by reference to the doctrine of *forum non conveniens* where it finds itself to be a 'clearly inappropriate forum' – a test that rarely is met.

In the Gutnick case, Kirby J placed great faith in this doctrine:
It seems to me […] that that [the issue of forum non conveniens] is the place in which the Internet problem is going to be solved in the world. Countries are going to say, 'Of course we've got jurisdiction. The damage happened here or some other - we can serve here but it is much more convenient that this matter be litigated in another place'[19].

However, the Gutnick case itself demonstrates why this line of reasoning was overly optimistic. Mr Gutnick had limited his claim to publications occurring in Victoria (and had undertaken not to sue anywhere else). Thereby, he effectively cut the connection with all other jurisdictions. After all, what court could be seen to have a stronger connection to a matter relating to damages suffered only in Victoria than do the courts of Victoria?

This very tactic also has subsequently been adopted by litigants in other common law jurisdictions. For example, in the 2012 Canadian case of *Breeden v Black*[20] the plaintiff – Lord Black – limited his claim to injury suffered in the jurisdiction he took action and undertook not to bring any libel action in any other jurisdiction[21].

[15] Law of the People's Republic of China on the Application of Law for Foreign-Related Civil Relations of 2011, art 46.
[16] Republic Act No 10175, An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefore and for Other Purposes.
[17] See John Pfeiffer Pty Limited v Rogerson [2000] HCA 36 and Regie National des Usines Renault SA v Zhang [2002] HCA 10.
[18] For Victoria, see Defamation Act 2005 (Vic), s 11(2).
[19] Transcript of High Court hearing of Dow Jones & Company Inc v Gutnick, 28th of May 2002, points 1484 – 1487 .
[20] [2012] SCC 19.
[21] Ibid [33].

2.3.1 A Third Stopover – European Union Law and Australian Law Compared

Here it is again relevant to compare Australian law to that of the European Union. Despite significant differences, such as the fundamental differences as to the discretion of courts to decline jurisdiction, the end results are remarkably similar. In a common law country, a litigant seeking to sue a foreign defendant may be required to limit her/his claim to damages occurring in that jurisdiction or risk having the matter thrown out by reference to the doctrine of *forum non conveniens*.

Similarly, the application of Article 5(3) of the Brussels Regulation (as applied in *Shevill*) means that such a litigant can only receive damages compensating for the event occurring in the jurisdiction where the litigation takes place.

Thus, the net result is the same even though the methods of reaching this result are fundamentally different. Observations such as this are important as they can indicate areas of consensus about what results the law should aim to achieve.

3. A Fourth Stopover – US Law on Recognition and Enforcement

While the *Gutnick* case eventually settled out of court, it is interesting to consider what would have happened had Mr Gutnick been successful in the substantive defamation matter in an Australian court and then sought to enforce an Australian judgment in the US.

The US has a history of refusing to enforce foreign judgments perceived to interfere with the freedom of speech provided in the US through the First Amendment to the US Constitution[22]. However, recent developments have brought increased attention to this practise. On 10 August 2010, the US adopted a federal statute seeking to address what the US perceives as 'libel tourism'[23]. The key feature of the statute is to make mandatory the non-recognition of foreign defamation judgments that are seen as inconsistent with the First Amendment's protection of free speech. With actual enforcement being such a central component in the proper functioning of the private international law machinery – not least in the Internet context – the approach taken by the US is doubtless a step in the direction of under-regulation. The obvious risk is that this initiative prompts the response that other countries implement similar non-recognition legislation as to areas of law when they do not trust how US courts adjudicate matters. In other words, the US initiative may spark a downward spiral effect.

4. A Fifth Stopover – French Law and Geo-Location Technologies

A key problem with Internet content, from the perspective of private international law, is that, once content is placed on the Internet, it may be accessed (virtually) globally. This sort of thinking has had two types of consequence, both of which may be illustrated by reference to the conduct of Australian courts.

The first is showcased in the *Gutnick* case where the majority of the Court stated that:

However broad may be the reach of any particular means of communication, those who make information accessible by a particular method do so knowing of the reach that their information may have. In particular, those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction[24].

This sends a strong message that anyone bold enough to use the Internet to communicate content does so at her own risk globally.

The other consequence is clear from the Supreme Court of New South Wales' approach in *Macquarie Bank Limited & Anor v Berg*[25] where it refused to grant an injunction in relation to allegedly defamatory content and stated that:

An injunction to restrain defamation in NSW s designed to ensure compliance with the laws of NSW, and to protect the rights of plaintiffs, as those rights are defined by the law of NSW. Such an injunction is not designed to superimpose the law of NSW relating to defamation on every other state, territory and country of the world. Yet that would be the effect of an order restraining publication on the Internet. It is not to be assumed that the law of defamation in other countries is coextensive with that of NSW, and indeed, one knows that it is not. It may very well be that according to the law of the Bahamas, Tazhakistan [sic], or Mongolia, the defendant has an unfettered right to publish the material. To make an order interfering with such a right would exceed the proper limits of the use of the injunctive power of this court[26].

In contrast to the approach taken by the High Court in the *Gutnick* case, the Court here views the ubiquitous nature of Internet content as an obstacle.

Neither the Court in the *Gutnick* case, nor the Court in the *Macquarie Bank Limited & Anor v Berg* case, took account of and discussed the technological reality of so-called geo-identification. As noted already in 2000 by the French County Court of Paris, there are so-called geo-location technologies available that make it possible to ascertain the geographical location of Internet users with a rather high degree of accuracy. In the *Yahoo!* case,[27] the Court relied on expert testimonies to conclude that: 'it may be estimated in practice that over 70% of the IP addresses of surfers residing in French territory can be identified as being French'[28].

There are several ways in which an Internet users' geographical location may be ascertained: for example, through Global Positioning System (GPS) signals, mapping of WiFi hotspots and so-called triangulation for those who connect to the Internet using smart devices such as smart phones and tablet computers. Here, however, I will restrict the discussion to geo-location technologies based on matching Internet Protocol (IP) addresses to geographical locations.

[22] K Wimmer, International Liability for Internet Content: Publish Locally, Defend Globally (Covington and Burling, 2003) <www.cov.com/publications/download/oid11035/347.pdf> 18.

[23] See, further, Emily C Barbour, 'The SPEECH Act: The Federal Response to "Libel Tourism"' (Congressional Research Service, 16 September 2010) <http://www.fas.org/sgp/crs/misc/R41417.pdf>.

[24] Dow Jones & Company Inc v Gutnick [2002] HCA 56 [39].

[25] [1999] NSWSC 526.

[26] Ibid [14].

[27] International League Against Racism & Anti-Semitism (LICRA) and the Union of French Jewish Students (UEJF) v Yahoo! Inc County Court of Paris, interim court order of 20th of November 2000.

[28] Ibid. However, it would seem that one of the experts, Ben Laurie, later felt a need to explain his statement: Ben Laurie, An Expert's Apology (21 November 2000) <http://www.apache-ssl.org/apology.html>.

As the access-seeker enters the appropriate Uniform Resource Locator (URL) into his/her browser, or clicks on the appropriate hyperlink, an access-request is sent to the server operating the requested website. As the server receives the access-request, it in turn sends a location request (eg, forwards the access-seeker's IP address) to the provider of the geo-location service. The provider of the geo-location service has gathered information about the IP addresses in use and built up a database of geo-location information. Based on the information in this database, the provider of the geo-location service gives the website server an educated guess as to the access-seeker's location. Armed with this information, the web server can provide the access-seeker with the information deemed suitable (eg, a message along the lines of: 'Sorry. This website is intended for the people of Sweden only'[29] or perhaps an advertisement specifically targeted at people from the access-seeker's particular location).

There are currently several products on the market utilising this type of systems[30]. This technology is not necessarily prohibitively expensive for larger website operators, nor does it appear particularly difficult to operate.

As to the accuracy of such technologies, it is worth noting how, in 2007, the Court in *ACLU v Gonzales*[31] reviewed expert testimony relating to Quova's geo-location technologies and observed the following:

A product that Quova markets can determine, within a 20 to 30 mile radius, the location from which a user is accessing a Web site through a proxy server, satellite connection, or large corporate proxy. The fact that Quova can only narrow down a user's location to a 20 to 30 mile radius results in Quova being unable to determine with 100 percent accuracy which side of a city or state border a user lives on if the user lives close to city or state borders. If a visitor is accessing a Web site through AOL, Quova can only determine whether the person is on the East or West coast of the United States. Quova has been used by Web site operators to direct traffic so that only users in the United States can view products that can only be distributed in the United States and to customize content for users in the United States as opposed to users in a another country. The services Quova offers can cost anywhere from $6,000 to $500,000 a year[32].

Another provider, Digital Element, claims that its product *NetAcuity* is over 99.9% accurate at a country level and over 95% accurate at a city-level, worldwide[33].

This is significant, since geo-location technologies fundamentally challenge the concept that the distribution of Internet content cannot be restricted reference to geographical criteria[34].

5. A Sixth Stopover – Canadian Law and the Path towards Uniformity on One Important Issues

Canada – not least through the internationally well-known 2005 dispute in the *Bangoura* case[35] – has been faced with several interesting cases within the field of private international law and the Internet. The year of 2012 added at least three new cases deserving of international attention[36]. Here I will, however, only focus on one such case, and more specifically on what that case hints at for the future.

In *Éditions Écosociété Inc v Banro Corp*,[37] the defendant (subsequently appellant) Éditions Écosociété Inc had published a book argued to defame the plaintiff (subsequently respondent) Banro Corp. Having noted evidence that the book in question was available for sale in bookshops in Ontario, could be bought on the publisher's website (which was available also in Ontario) and was available in 15 copies in libraries in Ontario, the Court had no hesitation in concluding that the tort had occurred in Ontario.

Having noted how the *lex loci delicti* (the law of the place of wrong) is the applicable choice of law rule for torts in Canada, the Court noted that the alternative of focusing on the place of most substantial harm has gained significant support in the context of the tort of defamation[38]. In that context, the Court discussed the Australian transition from a focus on *lex loci delicti* to focusing on the place of closest connection (as outlined above) in some detail. However, it is of course also possible to see this as a move in the same direction as the ECJ's focus on the 'centre of interest', and if we over the coming years see a widespread adoption of such a focus, we may indeed speak of a paradigm shift in the area of private international law and the Internet.

6. Returning to the Point of Departure – Concluding Remarks

One may rightfully find oneself dizzy after this whirlwind tour of private international law rules around the world. However, it is hoped that the above highlights some of the major developments to date in the field of private international law and the Internet and that it showcases some of the issues scholars in this highly interesting field will have to struggle with over the years to come.

Returning to Australian law, it should be pointed out that attempts are made to substantially reform Australia's private international law. It is encouraging to see that this useful initiative by the Private International Law Section of the Attorney-General's Department is so clearly conscious of, and attentive to, the particular difficulties (and potential solutions) the Internet brings to the table[39].

[29] For example, when using a computer at University of New South Wales (Australia) to access Showtime's website <http://www.sho.com>, I received the following message: 'We at Showtime Online express our apologies; however, these pages are intended for access only from within the United States.'

[30] See, eg, <http://www.quova.com>, <http://www.akamai.com>, <http://www.caida.org/tools/utilities/netg> and <www.digitalenvoy.net>. See also the following geo-location products that can be tested for free online: <http://www.perl-studio.com/iptocountry/index.php>; <http://www.activetarget.com/livedemo.asp>; <http://www.ip2location.com/free.asp>; and <http://www.geobytes.com/IpLocator.htm>.

[31] ACLU v Gonzales, 478 F Supp 2d 775 (ED Pa 2007).

[32] Ibid [182]-[186].

[33] Digital Element, NetAcuity and NetAcuity Edge IP Location Technology <http://www.digitalelement.com/our_technology/our_technology.html>.

[34] See further, Dan Svantesson, 'Time for the Law to Take Internet Geo-Location Technologies Seriously' (2012) 8(3) Journal of Private International Law 473-87 and Marketa Trimble, 'The Future of Cybertravel: Legal Implications of the Evasion of Geolocation' (2012) 22 Fordham Intellectual Property Media and Entertainment Law Journal 567.

[35] Bangoura v Washington Post, (2005) 258 D.L.R. (4th) 341.

[36] Club Resorts Ltd v Van Breda [2012] SCC 17; Breeden v Black [2012] SCC 19; Éditions Écosociété Inc v Banro Corp [2012] SCC 18.

[37] Éditions Écosociété Inc v Banro Corp [2012] SCC 18.

[38] Ibid [56].

[39] See, in particular, pp 15-18 of the relevant Discussion Paper: Reducing Legal Complexity of Cross-Border Transactions and Relationships: Driving Micro-Economic Reform through the Establishment of More Cohesive and Clearer Jurisdictional, Applicable Law and Choice of Court Rules <https://consult.govspace.gov.au/files/2012/11/Discussion-Paper-1-Reducing-legal-complexity-of-cross-border-transactions-and-relationships.doc>.

KONFERENCJE

MARIA KACZOROWSKA

KONFERENCJA NAUKOWA „OCHRONA PUBLICZNYCH BAZ DANYCH", WARSZAWA, 6 LISTOPADA 2013 R.

Konsekwencją postępującego procesu informatyzacji różnych dziedzin funkcjonowania państwa jest coraz większa dostępność danych gromadzonych w formie elektronicznej przez organy publiczne, co z jednej strony przyczynia się do rozwoju obrotu prawnego, z drugiej strony jednak stwarza wiele zagrożeń dla interesów jednostek. W obliczu wyzwań, jakie niesie ze sobą rozwój technologii informatycznych i ustawiczny przyrost zasobu generowanych danych cyfrowych, problematyka dotycząca zadań państwa w sferze bezpieczeństwa informacyjnego w kontekście takich zagadnień jak ponowne wykorzystywanie informacji publicznej czy przetwarzanie danych osobowych w dużych zbiorach danych (*Big Data*) zyskuje aktualnie na znaczeniu. W szeroką debatę nad kierunkami rozwoju regulacji prawnych normujących zasady gromadzenia i udostępniania informacji sektora publicznego wpisują się obrady konferencji naukowej „Ochrona publicznych baz danych" z udziałem przedstawicieli władz publicznych, nauki prawa oraz praktyki, zorganizowanej 6 listopada 2013 r. przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie w ramach projektu Narodowego Centrum Badań i Rozwoju „Model regulacji jawności i jej ograniczeń w demokratycznym państwie prawnym".

Po powitaniu uczestników konferencji przez prof. dr hab. Grażynę Szpor (Uniwersytet Kardynała Stefana Wyszyńskiego) otwarcia obrad dokonał prof. dr hab. Cezary Mik (Uniwersytet Kardynała Stefana Wyszyńskiego), akcentując doniosłość podejmowanej problematyki dla współczesnego państwa, na którym spoczywa obowiązek zapewnienia odpowiedniego poziomu ochrony publicznych zasobów danych.

Program konferencji obejmował trzy sesje.

Tematem pierwszej sesji, moderowanej przez prof. dra hab. Czesława Martysza (Uniwersytet Śląski, Najwyższa Izba Kontroli), była prawna ochrona baz danych w sferze publicznej. W otwierającym sesję referacie zatytułowanym *Autorskoprawna ochrona publicznych baz danych* dr Justyna Kurek (Uniwersytet Kardynała Stefana Wyszyńskiego) omówiła kryteria decydujące o objęciu bazy danych ochroną przewidzianą w ustawie o prawie autorskim i prawach pokrewnych (dalej: upapp)[1], a następnie poddała analizie wybrane publiczne bazy wiedzy pod kątem spełnienia przesłanek ochrony. Referentka wskazała, że w świetle orzecznictwa Sądu Najwyższego dokumenty udostępniane w bazach takich jak Internetowy System Aktów Prawnych czy Centralna Baza Orzeczeń Sądów Administracyjnych, mimo że mają charakter twórczy, jako materiały urzędowe nie mogą być uznane za przedmiot prawa autorskiego, ponieważ podlegają wyłączeniu na mocy art.4 upapp. W ocenie dr J. Kurek regulacja ta może stanowić przeszkodę w dalszym rozwoju tego typu baz danych. Daje to podstawę do zgłoszenia postulatu wprowadzenia legalnej definicji materiału urzędowego, a także zmiany kryteriów przyznania publicznym bazom danych ochrony na gruncie prawa autorskiego. Dr Krzysztof Felchner (Uniwersytet Jagielloński) zaprezentował referat na temat *Ochrona sui generis publicznych baz danych*. Instytucja prawa do tzw. ochrony swego rodzaju, wprowadzona w art.7 ust.1 dyrektywy 96/9/WE w sprawie ochrony prawnej baz danych[2], a w prawie polskim uregulowana ustawą o ochronie baz danych[3], ma charakter niezależny od ochrony przysługującej na mocy prawa autorskiego. Warunkiem przyznania ochrony *sui generis* jest poniesienie istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji zawartości bazy danych. Jak zwrócił uwagę referent, spełnienie tej przesłanki w przypadku publicznych baz danych jest wykluczone ze względu na fakt, że są one finansowane ze środków pochodzących z podatków, co nie może być kwalifikowane jako inwestycja. Wyłączenie spod ochrony *sui generis* może być w tym przypadku zrekompensowane poprzez zastosowanie instytucji ponownego wykorzystania informacji publicznej. Odpłatny charakter udostępnienia informacji publicznej w celu ponownego wykorzystania pozwala bowiem na uznanie go za inwestycję. Zagadnienie ponownego wykorzystania informacji z publicznych baz danych ze szczególnym uwzględnieniem opłat zostało rozwinięte w wystąpieniu dr Agnieszki Piskorz-Ryń (Uniwersytet Kardynała Stefana Wyszyńskiego), która przybliżyła zasady odpłatności za ponowne wykorzystywanie informacji publicznych na gruncie dyrektywy 2003/98/EU w sprawie ponownego wykorzystywania informacji sektora publicznego[4] oraz zmieniającej ją dyrektywy 2013/37/EU[5], a także przedstawiła w ujęciu porównawczym regulacje z tego zakresu obowiązujące w państwach Unii Europejskiej. Z przeprowadzonej przez re-

[1] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2006 r. Nr 90, poz. 631 z późn. zm.).

[2] Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych (Dz. Urz. UE L 77 z 27.3.1996, s. 20-28).

[3] Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (Dz. U. Nr 128, poz. 1402 z późn. zm.).

[4] Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003, s. 90-96).

[5] Dyrektywa Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 175 z 27.6.2013, s. 1-8).

ferentkę analizy wynika, że większość krajowych porządków prawnych przewiduje rozwiązanie odpowiadające zasadom przyjętym w dyrektywie sprzed nowelizacji, a zatem w przypadku pobieranych opłat całkowity dochód z dostarczania i zezwalania na ponowne wykorzystywanie dokumentów nie może przekraczać kosztów zbierania, produkowania, reprodukowania i rozpowszechniania wraz z rozsądnym zyskiem z inwestycji. Inaczej na tym tle przedstawia się regulacja polskiej ustawy o dostępie do informacji publicznej (dalej: udip)[6], na gruncie której przy ustalaniu opłaty uwzględniane są koszty wynikające ze złożonego wniosku, a ponadto brak przesłanki rozsądnego zwrotu z inwestycji. Tematem referatu przygotowanego przez Kingę Kafarską (Urząd Patentowy) było *Zlecanie tworzenia baz danych przez organy publiczne podmiotom prywatnym*. Referentka wymieniła formy udostępniania informacji publicznej dotyczącej działalności Urzędu Patentowego jako centralnego organu administracji publicznej, do których należą bazy danych prowadzone dla poszczególnych przedmiotów ochrony patentowej, a także oficjalne publikatory. Podkreśliła zarazem, że katalog ten nie obejmuje bazy orzeczeń Urzędu. W tej sytuacji powstaje ryzyko związane z potencjalnym niekontrolowanym wykorzystywaniem informacji publicznej przez podmioty komercyjne, które mogą być zainteresowane stworzeniem bazy danych oferującej dostęp do orzecznictwa. Uzasadnia to postulat udostępnienia przez Urząd Patentowy informacji o działalności orzeczniczej po ich wstępnym przetworzeniu (anonimizacji) zgodnie z art.23f udip. W kolejnym wystąpieniu Piotr Drobek (Biuro Generalnego Inspektora Ochrony Danych Osobowych) poruszył zagadnienie ochrony danych osobowych w publicznych bazach danych. W rozważaniach na temat relacji między ochroną danych osobowych a ponownym wykorzystywaniem informacji referent odwołał się m.in. do rekomendacji tzw. Grupy Roboczej Artykułu 29 oraz orzecznictwa Europejskiego Trybunału Sprawiedliwości. P. Drobek zwrócił uwagę, że anonimizacja udostępnianej informacji w praktyce nie daje pełnej gwarancji ochrony danych osobowych ze względu na możliwość jej agregacji z informacjami uzyskanymi z innych źródeł i w efekcie przekształcenia jej z powrotem w informację osobową. W związku z tym, jak zaakcentowano w referacie, należy promować standardy dotyczące anonimizacji i reidentyfikacji danych. Pierwszą sesję konferencji zakończyło wystąpienie dr Magdaleny Durzyńskiej (sędzia cywilista) poświęcone problematyce domeny publicznej. Ze względu na brak definicji legalnej w prawie polskim pojęcie domeny publicznej kształtowane jest przez orzecznictwo. Referentka wskazała, że mimo przyjęcia szerokiego rozumienia domeny publicznej, opartego na zasadzie otwartego dostępu do wiedzy, Sąd Najwyższy uznał za niedopuszczalne zawłaszczanie niektórych nazw czy haseł, mających charakter nabytych i powszechnie używanych dóbr, przez podmioty prywatne. M. Durzyńska nawiązała także do kwestii udostępniania treści orzeczeń w portalach orzeczeń sądów powszechnych, podkreślając, że z jednej strony rozwiązanie to służy ujednoliceniu linii orzeczniczej sądów i zwiększeniu świadomości prawnej obywateli, jednak z drugiej strony może prowadzić do naruszenia prywatności stron, bowiem z uwagi na specyfikę spraw rozpatrywanych w sądach powszechnych anonimizacja danych niejednokrotnie okazuje się niewystarczającym zabezpieczeniem przed identyfikacją podmiotów uczestniczących w postępowaniu.

Referaty wygłoszone w ramach drugiej sesji dotyczyły zagadnień finansowania publicznych baz danych. Rolę moderatora pełnił prof. dr hab. Cezary Kosikowski (Uniwersytet w Białymstoku). W wystąpieniu prof. dra hab. Piotra Zapadki (Uniwersytet Kardynała Stefana Wyszyńskiego) został podjęty temat *Źródła finansowania infrastruktury informacyjnej*. Referent wskazał, że kształtowanie zasad finansowania publicznych baz danych powinno opierać się na przyjęciu jako punktu odniesienia określonych wzorcowych rozwiązań stosowanych w analogicznych systemach finansowania. Nacisk należy położyć również na efektywność i cel finansowania, stanowiące wyznacznik ustalenia zakresu i źródeł pozyskiwania środków na tworzenie infrastruktury informacyjnej państwa. Piotr Waglowski (VaGla.pl) wygłosił referat *Finansowanie publicznych serwisów informacyjnych*, w którym poddał analizie koszty utrzymania i obsługi przykładowych stron internetowych prowadzonych przez organy publiczne, stwierdzając, że nie odpowiadają one wymogom racjonalnego wydatkowania środków publicznych. Ponadto referent krytycznie ocenił formę komunikowania się przedstawicieli instytucji publicznych z obywatelami za pośrednictwem komunikatorów internetowych. Zgodnie z przytoczoną argumentacją udzielane w ten sposób informacje są pozbawione doniosłości prawnej, w przeciwieństwie do informacji udostępnianych w Biuletynie Informacji Publicznej czy na elektronicznej Platformie Usług Administracji Publicznej. Na tej podstawie P. Waglowski wysunął postulat ograniczenia liczby publicznych serwisów informacyjnych i zwiększenia roli Biuletynu Informacji Publicznej. Kolejny referat, który przedstawiła dr inż. Agnieszka Gryszczyńska (Uniwersytet Kardynała Stefana Wyszyńskiego), był poświęcony finansowaniu rejestrów sądowych. Podjęte przez referentkę rozważania dotyczyły przede wszystkim kwestii relacji między wysokością opłat, do których ponoszenia zobowiązane są osoby zainteresowane dokonaniem wpisu lub dostępem do rejestru, a nakładami ponoszonymi przez sąd jako organ prowadzący rejestr. Dr inż. A. Gryszczyńska podkreśliła, że w celu zapewnienia efektywności funkcjonowania rejestrów przy ustalaniu zasad odpłatności za korzystanie z ich zasobów należy przede wszystkim dokonać oceny, które z oferowanych form dostępu faktycznie odpowiadają potrzebom obrotu. Punktem odniesienia w tym zakresie mogą być praktyczne doświadczenia związane z szerokim zainteresowaniem dostępem do elektronicznej przeglądarki ksiąg wieczystych, a także możliwością samodzielnego pobierania odpisów z Krajowego Rejestru Sądowego. Zdaniem referentki takie podejście, zakładające zrównoważenie funkcji fiskalnej i ewidencyjnej rejestrów sądowych, powinno wyznaczać kierunki zmian legislacyjnych w dziedzinie opłat za dostęp do informacji rejestrowych. Krzysztof Mączewski (Geodeta Województwa Mazowieckiego, Urząd Marszałkowski Województwa Mazowieckiego) w referacie na temat *Finansowanie baz danych państwowego zasobu geodezyjnego i kartograficznego* dokonał analizy związku między dochodami, jakie generują serwisy udostępniające informację przestrzenną, a kosztami ich funkcjonowania. Jak wskazał referent, w obecnym stanie prawnym przychody z opłat wnoszonych przez odbiorców nie pokrywają kosztów związanych z prowadzeniem wojewódzkiego zasobu geodezyjnego i kartograficznego. W ocenie K. Mączewskiego konieczne jest jednoznaczne określenie kompetencji organów publicznych w sferze

[6] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.).

finansowania tego typu baz danych. Dr Ewa Perłakowska (Naczelna Dyrekcja Archiwów Państwowych) wystąpiła z referatem *Finansowanie baz danych archiwalnych*, w którym omówiła podstawy prawne działania archiwów, zakres prowadzonej przez nie działalności statutowej i usługowej oraz zasady udostępniania materiałów archiwalnych wynikające z ustawy o narodowym zasobie archiwalnym i archiwach[7]. Referentka zwróciła uwagę na sukcesywne poszerzanie dostępu do zasobów archiwalnych, czego przejawem jest np. wprowadzona niedawno możliwość nieodpłatnego kopiowania materiałów archiwalnych przy użyciu własnego sprzętu. W ostatnim z wystąpień przewidzianych w programie drugiej sesji dr inż. Kajetan Wojsyk (Centrum Systemów Informacyjnych Ochrony Zdrowia) poruszył zagadnienie finansowania systemu informacyjnego ochrony zdrowia. Autor referatu podkreślił, że informacje dotyczące funkcjonowania ochrony zdrowia zgromadzone w licznych odrębnych rejestrach są w wielu przypadkach niepotrzebnie powielane, co skutkuje podwyższeniem kosztów prowadzenia rejestrów. Z tego powodu aktualnie prowadzone są prace mające na celu scalanie rozproszonych rejestrów, a także udostępnienie usług z zakresu administracji elektronicznej w ramach realizowanych projektów P1 (Elektroniczna Platforma Gromadzenia, Analizy i Udostępniania zasobów cyfrowych o Zdarzeniach Medycznych) i P2 (Platforma udostępniania on-line przedsiębiorcom usług i zasobów cyfrowych rejestrów medycznych).

Trzecia sesja konferencji, której obrady moderował prof. dr hab. Bolesław Szafrański (Wojskowa Akademia Techniczna), była poświęcona technicznej ochronie publicznych baz danych. Dr inż. Maciej Kiedrowicz (Wojskowa Akademia Techniczna) wystąpił z referatem zatytułowanym *Dostęp do publicznych zasobów. Big Data czy Big Brother?*. Referent zwrócił w nim uwagę na stale wzrastającą liczbę prowadzonych rejestrów publicznych i wyeksponował zagrożenia, jakie wiążą się z ujawnianiem w nich danych osób fizycznych i prawnych. Szczególne znaczenie w tym kontekście należy przypisać dostępowi do numeru PESEL, którego znajomość umożliwia uzyskanie dalszych danych o konkretnych osobach, wykorzystywanych następnie do ich profilowania. Referat Jacka Kowalskiego (Body of European Regulators for Electronic Communications) *Big Data – wyzwanie dla dostawców usług telekomunikacyjnych* obejmował analizę zasad świadczenia usług międzynarodowego roamingu. Nowa regulacja obowiązków spoczywających w tym zakresie na operatorach i uprawnień przysługujących klientom została zawarta w rozporządzeniu 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii[8]. Kolejny referat został zaprezentowany przez Janusza Dygaszewicza (Główny Urząd Statystyczny), który podjął temat *Big Data w statystyce publicznej*. Referent zwrócił uwagę na problemy definicyjne związane z pojęciem *Big Data*, odnoszącym się do zbiorów danych, które cechuje duża ilość, zmienność i różnorodność danych, a także brak ustrukturyzowania. Wśród źródeł tego typu danych wykorzystywanych w badaniach statystycznych wymienione zostały portale społecznościowe i zapisy sensorów natężenia ruchu. J. Dygaszewicz podkreślił, że dostęp do tej kategorii danych pozwala na obniżenie kosztów prowadzonych badań. Zaznaczył jednocześnie, że istotny problem w tym kontekście stanowi brak regulacji odnoszących się do zabezpieczenia pozyskiwanych informacji (zwłaszcza ze źródeł prywatnych) i zarządzania nimi. Tematem wystąpienia dra inż. Jerzego Stanika (Wojskowa Akademia Techniczna) były *Wybrane aspekty standaryzacji w ochronie publicznych baz danych*. W referacie omówiono wymogi dotyczące zapewnienia odpowiedniego poziomu bezpieczeństwa informacji. Referent szczegółowo odniósł się do procedur związanych z bezpieczeństwem danych osobowych i informacji niejawnych (uregulowanych odpowiednio w ustawie o ochronie danych osobowych[9] i ustawie o ochronie informacji niejawnych[10]), a także danych wrażliwych (nieposiadających regulacji ustawowej). Jak podkreślił referent, znaczącą rolę w zakresie standardów bezpieczeństwa informacji odgrywa międzynarodowa norma ISO/IEC 27001. Ostatni referat, przedstawiony przez Dorotę Chromicką (Uniwersytet Kardynała Stefana Wyszyńskiego), dotyczył anonimizacji danych osobowych i jednostkowych. W swoich rozważaniach referentka wyeksponowała problemy uwidaczniające się w praktyce udostępniania orzeczeń sądów, do których zaliczyła stosowanie niejednolitych zasad anonimizacji, przypadki błędów czy zbyt daleko idącej anonimizacji danych, prowadzącej do ograniczenia przydatności orzeczenia. Na podstawie omówionych przykładów D. Chromicka stwierdziła, że standaryzacja procedur anonimizacji danych okazuje się właściwie niemożliwa, niemniej jednak w jej ocenie zasadne jest podejmowanie działań legislacyjnych w tej dziedzinie.

Podsumowując obrady konferencji, prof. dr hab. G. Szpor podkreśliła wagę podjętych w ramach poszczególnych sesji rozważań, mających na celu diagnozę aktualnych problemów związanych z ochroną baz danych w sferze publicznej. Ponadto przekazana została wszystkim zainteresowanym informacja o planowanej publikacji wygłoszonych referatów w zbiorze pokonferencyjnym.

Abstract

Maria Kaczorowska in the report "Scientific conference 'Security of public databases" emphasizes that the sessions discussed in detail are part of a wide-ranging debate on the directions of the development of regulation, normalization rules for the collection and sharing of public sector information. This conference was attended by representatives of public authorities, science, law, practitioners, researchers of the Cardinal St. Wyszynski University in Warsaw, as part of the National Research and Development Centre entitled "A regulatory model of open rule and its limits in a democratic state of law. „Three thematic sessions of the conference included: the legal protection of databases in the public sphere, the issues of financing public databases, and the technical protection of databases. The papers presented at the conference and discussed briefly in this report, are to be published in a collection of conference papers, which was highlighted by Professor C. Szopr while summarizing the sessions.

[7] Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. z 2011 r. Nr 123, poz. 698 z późn. zm.).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 531/2012 z dnia 13 czerwca 2012 r. w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii (Dz. Urz. UE L 172 z 30.6.2012, s. 10-35).

[9] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).

[10] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228).