

UNIWERSYTET ADAMA MICKIEWICZA w POZNANIU
WYDZIAŁ PRAWA i ADMINISTRACJI

Piotr Szyndzielorz

ELEKTRONICZNA FORMA CZYNNOŚCI PRAWNYCH

Praca napisana w
Katedrze Prawa Cywilnego,
Handlowego i Ubezpieczeniowego
pod kierunkiem
Prof. dra hab. Adama Olejniczaka

Poznań 2001



SPIS TREŚCI

WYKAZ SKRÓTÓW	4
SŁOWNIK	6
Rozdział I. WSTĘP	8
1. Uzasadnienie wyboru tematu.	8
2. Forma oświadczenia woli a współczesne środki komunikacji na odległość.	10
3. Społeczne, prawne i ekonomiczne konsekwencje stosowania formy elektronicznej.	11
 Rozdział II. TRADYCYJNA CYWILISTYKA O FORMIE OŚWIADCZENIA WOLI	14
1. Oświadczenie woli.	14
1.1. Chwila złożenia oświadczenia woli.	16
1.2. Wady oświadczenia woli.	18
2. Forma oświadczenia woli.	21
2.1. Swoboda formy.	22
2.2. Formy szczególne.	22
2.3. Niedochowanie formy.	25
3. Dokument i podpis.	26
3.1. Prawne znaczenie podpisu.	26
3.2. Sposób złożenia podpisu.	28
 Rozdział III. ELEKTRONICZNA FORMA OŚWIADCZENIA WOLI	30
1. Materiałнопrawne znaczenie informacji elektronicznej – „elektroniczne oświadczenie woli”....	31
1.1. Doręczenie.	37
1.2. Błąd.	41
1.3. Odwołanie elektronicznego oświadczenia woli.	49
2. Forma elektroniczna – cechy konstytutywne, wizje i problemy prawne.	50
3. Zarys problematyki zawarcia umowy.	53
 Rozdział IV. ELEKTRONICZNY NOŚNIK OŚWIADCZENIA WOLI	55
1. Ustawa modelowa o wiadomości elektronicznej.	55

2. Dokument elektroniczny w Polsce de lege lata.	60
3. Semantyczna analiza „pisemności” dokumentu elektronicznego.	64
4. Nośnik oświadczenia woli.	68
ROZDZIAŁ V. PODPIS ELEKTRONICZNY	73
1. Kryptografia i podpis elektroniczny – aspekty techniczne.	73
2. Podpis elektroniczny – ewolucja i zakres pojęcia.	80
3. Funkcje podpisu elektronicznego.	90
4. System certyfikacji, odpowiedzialność wystawcy certyfikatów.	94
Rozdział VI. CZYNNOŚCI PROCESOWE DOKONYWANE W DRODZE ELEKTRONICZNEJ	104
2. Wnoszenie pism drogą elektroniczną.	104
2. Moc dowodowa dokumentu elektronicznego.	108
Rozdział VII. ZAKOŃCZENIE	113
BIBLIOGRAFIA	116



WYKAZ SKRÓTÓW

1. Źródła prawa:

KC.....	ustawa z dnia 23.04.1964r. – Kodeks cywilny (Dz.U. z 1964r. Nr 16, poz. 93 ze zm.)
KK.....	ustawa z dnia 06.06.1997r. – Kodeks karny (Dz.U. z 1997 Nr 88 poz. 553 ze zm.)
KPA.....	ustawa z dnia 14.06.1960r. – Kodeks postępowania administracyjnego (Dz.U. z 1980r. Nr 9, poz.26 ze zm.)
KPC.....	ustawa z dnia 17.11.1964r. - Kodeks postępowania cywilnego (Dz.U. z 1964r. Nr 43, poz. 296 ze zm.)
KSH.....	ustawa z dnia 15.09.2000r. - Kodeks spółek handlowych (Dz.U. z 2000r. Nr 94, poz. 1037)
PrBank.....	ustawa z dnia 29.08.1997r. – Prawo bankowe (Dz.U. z 1997 Nr 140, poz. 939)
<i>Obce:</i>	
BGB.....	Gesetz vom 18.08. 1896 – Bürgerliches Gesetzbuch
IuKDG.....	Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste vom 13.07.1997 (BT - Drs. 13-7943 vom 11.06.1997)
RL.....	Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signatur vom 13.05.1998
SigG.....	Gesetz zur diditalen Signatur vom 22.07.1997 (BGBI. I S. 1870, 1872)
SigV.....	Verordnung zur digitalen Signatur vom 08.10.1997
ZPO.....	Gesetz vom 30. Januar 1877 – Zivilprozessordnung, 12. September 1950 (RGBI. 1877 S. 83; BGBI. I 1950 S. 455), zuletzt geändert durch Art. 1 des Gesetzes zur Änderung des Gesetzes zur Neuordnung des Berufsrechts der Rechtsanwälte und der Patentanwälte vom 17. Dezember 1999 (BGBI. I S. 2448)
<i>Projekty:</i>	
UoP – P.....	Poselski projekt ustawy o podpisie elektronicznym z dnia 21.12.2000r.

UoP – Rz..... Rządowy projekt ustawy o podpisie elektronicznym z dnia 06.02.2001r.

2. Organy orzekające:

NSA	Naczelnego Sądu Administracyjnego
SA.....	Sąd Apelacyjny
SN.....	Sąd Najwyższy
BGH.....	Bundesgerichtshof

3. Czasopisma:

CuR.....	Computer und Recht
DNotZ	Deutsche Notar-Zeitschrift
Dz.U.....	Dziennik Ustaw
GP.....	Gazeta Prawna
MMR.....	Multimedia und Recht
MoP.....	Monitor Prawniczy
NJW.....	Neue Juristische Wochenschrift
OSN.....	Orzecznictwo Sądu Najwyższego Izby Cywilnej
PiP.....	Państwo i Prawo
PPH.....	Przegląd Prawa Handlowego
RP.....	Rzeczpospolita
TuW.....	Tekommunikation und Wirtschaft
ZUM.....	Zeitschrift für Urheber – und Medienrecht

4. Inne skróty:

BIM.....	Bundesinnenministeriums (BMI)
BNK.....	Bundesnotarkammer
BzU.....	Begründung zur Unterschriftenverordnung vom 12. 08.1995
EDI.....	Electronic Data Interchange
KUA.....	Krajowy Urząd Akredytacji
PKI.....	Public Key Infrastructure

SŁOWNIK

Hash value – skrót wiadomości – ciąg numeryczny będący skrótem treści wiadomości, o takiej właściwości, że zmiana treści wiadomości spowoduje automatycznie zmianę wartości hash. Funkcja skrótu (algorytm hash) musi działać w sposób praktycznie wykluczający sytuację, w której dwie różne wiadomości mają jednakową wartość hash. W literaturze mówi się również o „cyfrowym odcisku palca” (tak Steffen Raßmann: Elektronische Unterschrift im Zahlungsverkehr, CuR nr 1/1998).

Interfejs (angielskie *interface*) - układy i urządzenia sprzętowe oraz oprogramowanie służące do wymiany informacji między składowymi systemu komputerowego. Element pośredniczący w komunikacji. Interfejsy występują między elementami sprzętu (interfejs sprzętowy), np. karta interfejsu sieciowego, między programami (procesami), np. komunikacja za pośrednictwem plików lub wymiany komunikatów, oraz między ludźmi a komputerami (np. interfejs graficzny). W zależności od zastosowanych środków technicznych wyróżnia się interfejsy znakowe, graficzne, głosowe, dotykowe i mieszane. (Zdzisław Płoski: Słownik Encykopedyczny – Informatyka, 1999)

Interfejs użytkownika (angielskie *user interface, front end*) - całość oprogramowania wraz z odpowiednimi urządzeniami, służąca do wymiany informacji między człowiekiem a komputerem. (Zdzisław Płoski: Słownik Encykopedyczny – Informatyka, 1999)

Mailbox – skrzynka pocztowa - skojarzony z użytkownikiem bufor, przeznaczony do przechowywania listów przesyłanych pocztą elektroniczną. Skrzynka pocztowa jest obsługiwana przez program pocztowy. (Zdzisław Płoski: Słownik Encykopedyczny – Informatyka, 1999)

PKI – *Infrastruktura klucza publicznego* – architektura, organizacja, techniki, zasady oraz procedury, które wspólnie wspomagają implementację i działanie kryptograficznych systemów klucza publicznego, opartych na certyfikatach. PKI składa się z powiązanych ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych (...). (<http://www.centrum.pl/>)

Poczta elektroniczna (e-mail) - jeden z najważniejszych sposobów komunikacji poprzez sieć Internet. Polega na przekazywaniu listów elektronicznych, czyli wiadomości tekstowych, dodatkowo opatrzonych adresem e-mail odbiorcy, nadawcy, a także dodatkowymi informacjami. Oprócz tekstu, listy mogą także zawierać pliki dowolnych formatów (obrazy, dźwięki, pliki danych i inne) przesyłane jako załączniki. Nazwa E-mail (niekiedy zapisywana jako email) oznacza także pojedynczą wiadomość poczty elektronicznej. Do wysyłania i odbierania poczty elektronicznej używa się specjalnych programów pocztowych. (<http://wiem.onet.pl/wiem/>)

Provider – *usługodawca* - firma lub osoba fizyczna dostarczająca usługi, np. firma telekomunikacyjna umożliwiająca łączność między komputerami za pomocą sieci telefonicznej. (Zdzisław Płoski: Słownik Encyklopedyczny – Informatyka, 1999)

Serwer - komputer lub program umożliwiający dostęp do pewnej usługi innym programom bądź komputerom zwanym klientami.

Do typowych przykładów należą: serwery plików umożliwiające dostęp innym komputerom w sieci do jakiegoś dysku, serwery usług internetowych - komputery podłączone do sieci Internet (...). (<http://wiem.onet.pl/wiem/>)

1. UZASADNIENIE WYBORU TEMATU.

Czy można by obecnie zasadnie mówić o problemach narastających wokół tradycyjnych instytucji prawnych gdyby nie lawinowy rozwój Internetu? Pewnie tak, być może nie w tak szerokim kontekście, ale niewątpliwie tak. Internet jest faktem naszych czasów, który musimy zaakceptować z wszystkimi jego konsekwencjami. Dla jednych jawi się on jako źródło niespotykanych dotychczas możliwości, inni podchodzą do niego pełni obaw i niepokoju. Prawda, jak to zwykle bywa, leży pośrodku. Faktem niezaprzeczalnym jest, że Internet jest sprawcą chaosu terminologicznego i to nie tylko w obszarze instytucji prawnych. Nie należy jednak zbytnio demonizować zjawiska, aczkolwiek sieć globalna wykazuje ekspansję, jaką nie mogą pochwalić się żadne inne media¹. Poza tym ma charakter globalny. Wytworzzone przez różne czynniki sprawcze podziały na państwa, rasy, grupy zawodowe, etniczne, płeć, etc., nie wytrzymują konfrontacji z cyberprzestrzenią. Jedynym ograniczeniem jest technologia, która wymaga zaangażowania niezbędnego kapitału. W rezultacie w miejsce dawnego, politycznego podziału na Wschód i Zachód, coraz bardziej kontrastowy staje się podział równoleżnikowy na bogatą Północ i biedne Południe. Budowanie „globalnej wioski” tylko sprzyja pogłębianiu tej asymilacji.

Można spotkać stanowiska bardzo optymistyczne, pokładające głęboką wiarę w zdolności przystosowawcze systemu prawa. Opierają się one na przekonaniu, że skoro prawo przez wieki potrafiło ustosunkować się do społeczno-gospodarczych przeobrażeń, to również obecny stan rzeczy nie stanowi wyjątku. Całkiem prawdopodobne, trzeba jednak pamiętać, że nigdy przedtem informacja sama przez siebie nie była najbardziej pożądanym zasobem produkcyjnym. Można się zdziwić o jak błahe (pozornie) informacje czasami chodzi. Zupełnie niewykluczone, że niedługo np. problem zakupów zniknie w ogóle z naszego codziennego życia. Założyć można, że np. nasza lodówka podłączona do globalnej sieci „sama rozpozna” zapotrzebowanie, złoży zamówienie, być może wyszuka

¹ Z danych OBOP-u wynika, że dostęp do Internetu na już 16% Polaków tj. około 4,9 mln, „Chip” 6/2000 str.38

najkorzystniejszą (według zdefiniowanych przez nas kryteriów, a więc niekoniecznie najtańszą) ofertę. Pozostanie problem logistyki. Internet stwarza takie możliwości, a ich praktyczną realizację systemy EDI recypowane do obrotu komercyjnego. Trudno sobie w chwili obecnej wyobrazić, że tajemnice naszej lodówki mogą stanowić przedmiot pożądanej informacji, pokonującą łącza światowej sieci. Problem błały, a jednak. Co więcej, prawo będzie musiało ustosunkować się do niego i do wielu innych, wydawałoby się bardziej trywialnych problemów.

Jest to oczywiście przykład bardzo skrajny i będący przedmiotem odległej przyszłości, pokazuje jednak, że przyszłość, w tym również przyszły kształt prawa bardziej niż dotychczas kreować będą finalni użytkownicy. Nigdy bowiem społeczeństwo, ekonomia i prawo nie były połączone tak ciasną więzią.

Nowe zjawiska rodzą nowe problemy, wymuszają potrzebę dokonania nowych, jednoznacznych ustaleń. Polska refleksja prawnia i polskie prawo nie są szczególnie opóźnione w obszarze zagadnień szeroko rozumianego prawa komputerowego¹. Nie napawa jednak szczególnym optymizmem przyjęcie jako punktu odniesienia dorobku chociażby doktryny i judykatury niemieckiej. Na niemieckim rynku wydawniczym praktycznie od roku 1985 ukazują się specjalistyczne czasopisma, publikacje, etc. poświęcone wyłącznie prawnym aspektom obrotu elektronicznego², podczas gdy na polskim rynku wydawniczym istnieje w tym zakresie zupełna luka.

Obrót elektroniczny rodzi wiele pytań, które można jedynie zasygnalizować, lecz *de lege lata* nie sposób na nie jednoznacznie odpowiedzieć. Rodzi również szereg postulatów *de lege ferenda*, które obecnie oscylują głównie wokół problemów bezpieczeństwa i pewności obrotu.

¹ „*Prawo informatyczne (prawo komputerowe) zajmuje się prawnymi skutkami stosowania komputerów i elektronicznego przetwarzania danych. Ponieważ nie zostało ono wyodrębnione, przedmiot tego prawa wchodzi w skład szczególnych dyscyplin prawniczych (...)*” Krzysztof Knoppek: Wydruk komputerowy jako dowód w procesie cywilnym, PiP 2/93 str. 54 i nast.

² Dla przykładu wskazać można JurPC Internet-Zeitschrift für Rechtsinformatik, publikowany również w wersji internetowej <http://www.jurpc.de/>, Computer und Recht, Multimedia und Recht, etc.

2. FORMA OŚWIADCZENIA WOLI A WSPÓŁCZESNE ŚRODKI KOMUNIKACJI NA ODLEGŁOŚĆ.

Przepisy regulujące zagadnienia formy czynności prawnych powstały w zupełnie innej epoce. Czy jednak przestały być one adekwatne do współczesnych realiów? W pewnym zakresie oczywiście tak np. w zakresie wymogu własnoręcznego podpisu, ale postulat zmian nie jest bezwzględny. Jak okaże się w dalszych rozważaniach wiele problemów, lepiej lub nieco gorzej, można rozwiązywać na bazie tego, co mamy. Nie mają więc racji rzecznicy radykalnych zmian. Nie tyle prawo wymaga głębskiej przemiany, co przede wszystkim nasza świadomość. Potrzeba pewnego dystansu do nowego, a to wymaga czasu.

Rzeczywiście obrót elektroniczny powoduje problemy w chwili obecnej nierozerwialne, np. miejsce zawarcia umowy *online*. W takich przypadkach konieczna będzie legislacyjna interwencja tudzież zajęcie jednoznacznego stanowiska, powstanie zwyczaju.

Komputer jest pierwszym narzędziem pozwalającym na połączenie w sobie funkcji wielu różnych urządzeń. Stwarza to obiektywne trudności, bo obala ugruntowaną zasadę *verba volant scripta manent*. Dokument utrwalony na elektronicznym nośniku informatycznym może zmieniać postać z pisemnej na dźwiękową, wizualną, etc. Możemy mieć trudności ze zniszczeniem takiego dokumentu, nigdy bowiem nie wiadomo czy gdzieś w sieci nie pozostała jego kopia. Komputer stwarza ogromne możliwości, byłby w stanie obsłużyć cały obecny obrót papierowy. W praktyce nie stanowi on jednak jeszcze dobrej dla papieru alternatywy. Zresztą nie trzeba od razu zakładać, że dominacja jednego podłożu oznacza unicestwienie drugiego, mogą one koegzystować. Wydaje się jednak, że przyszłość doprowadzi do całkowitej eliminacji papieru jako nośnika treści dokumentu (np. w RFN Książki Usług Medycznych od dawna funkcjonują w formie karty procesorowej).

Dotychczasowy rozwój usług informatycznych nie rodzi konieczności radykalnych zmian. Główne problemy prawne, jakie niosą za sobą współczesne środki komunikacyjne dotyczą zagadnień ściśle praktycznych. „*Czy i o ile stan obecny może i powinien rzutować na sposób wykładni przepisów o formie o tym*

*zadecyduje judykatura i orzecznictwo*¹. Na razie konieczna jest ich ścisła interpretacja, są to bowiem przepisy *iuris cogentis*.

Pojęcie „formy elektronicznej” zaczyna wprowadzać stopniowy chaos terminologiczny, wdzierając się również w obszar form szczególnych. Co prawda koncentracja legislacyjna skupia się zasadniczo na formie pisemnej, nie można wykluczyć, że z czasem, kiedy obrót elektroniczny osiągnie odpowiedni poziom sprawności, bezpieczeństwa i stworzone zostanie odpowiednie otoczenie prawne, mówienie o formach szczególnych w ogóle straci na znaczeniu. Wystarczy jedna forma – forma np. elektroniczna – która będzie formą na tyle bezpieczną (pewną), tanią i dla dokonującego czynności odformalizowaną (prostota tylko zewnętrzna tzn. formalizm niewidoczny z poziomu użytkownika), że będzie ją można stosować dla wszelkich przejawów życia prawnego. Ewolucja może pójść w tym kierunku, że w obrębie samej formy elektronicznej wystąpią różne jej warianty, hierarchicznie uporządkowane, które będą dawały różny poziom bezpieczeństwa uzależniony np. do ceny takiej usługi (również narzucone obligatoryjnie). Są to wszystko spekulacje, ale nie pozbawione odrobin rzeczywistości. Już dziś np. w Stanach Zjednoczonych mówi się o wystawcy certyfikatów - *cybernotariusz*².

3. SPOŁECZNE, PRAWNE I EKONOMICZNE KONSEKWENCJE STOSOWANIA FORMY ELEKTRONICZNEJ.

Konsekwencje są w zasadzie obosieczne. Z jednej strony stosowanie elektronicznych środków przekazu danych implikuje pewne społeczne, prawne i ekonomiczne następstwa, z drugiej to właśnie postawy społeczne i potrzeby obrotu gospodarczego dyktują nowe trendy telekomunikacyjne, a te wymuszają odpowiednie instrumentarium jurydyczne.

Dziś nie ma wątpliwości, że najbardziej poszukiwanym obecnie towarem jest informacja, a zatem również możliwość jej szybkiego zagospodarowania. W tym zakresie podstawowe znaczenie odgrywa telekomunikacja. Osiągnąć więc trzeba konstatację następującą: pomiędzy prawem a systemami łączności zachodzi

¹ Stanisław Dmowski, Stanisław Rudnicki: Komentarz do kodeksu cywilnego, Warszawa 1999 str. 239

² Jerzy Jacyszyn: Elektroniczne czynności prawne, PPH 7/1999 str. 29 i nast.

swoista symbioza. Wytwarzanie, gromadzenie, przetwarzanie i transmisja danych w drodze elektronicznej wpływa i będzie wpływać w przyszłości na kształt pokaźnej części prawa, nie tylko cywilnego. O ile pierwotnie problemy koncentrowały się wyłącznie na płaszczyźnie dowodowej, obecnie jest to już całe spektrum zagadnień: forma czynności prawnych, zdolność, prawo dostępu do informacji, etc.

Zasadniczo prawidłowość jest taka, że wszelkie innowacje biorą swój początek w obrocie gospodarczym, a więc tam gdzie pożądana jest najbardziej efektywna alokacja posiadanych zasobów. Za tym podążają przemiany społeczne, stopniowe nabywanie nowych nawyków, kształtowanie pewnych mechanizmów zachowań, które z czasem urastają do rangi zwyczajów. Dopiero na samym końcu pojawia się, jeżeli jest to oczywiście konieczne, reakcja prawa.

Poszczególne konsekwencje formy elektronicznej mogą pozostawać bez jakiegokolwiek wzajemnego związku, czasami jednak splatają się w jeden zbiorczy problem. Do takiej sytuacji prowadzi chociażby dokonywanie zakupów *online*. Zasadniczym powodem wprowadzenie takiej formy były racje ekonomiczne. Już sama forma sprzedaży rodzi problemy prawne i to nie tylko tak „blahe” jak pytanie: kto jest oferentem? Co bowiem powinien powiedzieć prawnik o umowie „sprzedaży”, która dochodzi do skutku w drodze aukcji pomiędzy internautami¹? A jak zakwalifikować pirackie „podróbki” oficjalnych witryn, czy znajdują tu zastosowanie przepisy o osobie czynnej w lokalu przedsiębiorstwa (art. 97 KC)? Są to wszystko prawne aspekty powszechnie zawieranej, w zwykłych sprawach życia codziennego umowy, na które prawo i prawnicy zmuszeni są poszukiwać odpowiedzi.

Pozostaje jeszcze aspekt społeczny. Poniższe wykresy wskazują, że potencjalne zainteresowanie zakupami *online* jest relatywnie duże i, co ważniejsze, z tendencją wzrostu. Jednakże o wiele mniejsze jest już zaufanie społeczne, o czym świadczy chociażby preferowana forma płatności.

¹ Np. <http://www.allegro.pl/>

Rozdział II**TRADYCYJNA CYWILISTYKA O FORMIE
OŚWIADCZENIA WOLI****1. OŚWIADCZENIE WOLI.**

Polski ustawodawca zawał w KC legalną definicję oświadczenia woli:

Art. 60. Z zastrzeżeniem wyjątków w ustawie przewidzianych, wola osoby dokonywającej czynności prawnej może być wyrażona przez każde zachowanie się tej osoby, które ujawnia jej wolę w sposób dostateczny (oświadczenie woli).

Oświadczeniem woli jest, więc przejaw woli, który wyraża w sposób dostateczny zamiar wywołania skutku prawnego w postaci ustanowienia, zmiany lub zniesienia stosunku prawnego.

Jedno lub kilka oświadczeń woli składa się na czynność prawną – jest to element konieczny, ale zarazem wystarczający każdej czynności prawnej i jedynie dla czynności prawnych charakterystyczny.

Samo oświadczenie woli nie jest tożsame z pojęciem czynności prawnej, niejednokrotnie, bowiem, np. w przypadku umowy mamy przynajmniej dwa, zgodne oświadczenia woli. W każdym razie w skład czynności prawnej, która opisuje całość zdarzenia prawnego (działania) musi wchodzić co najmniej jedno oświadczenie woli.

Czynność prawa zawsze wywołuje określony skutek prawy, zależny od woli dokonującego tej czynności człowieka. Tutaj, inaczej jak przy czynach, zarówno samo zachowanie jak i jego prawne konsekwencje objęte są zarówno wiedzą jak i wolą człowieka mającego zdolność do dokonania czynności danego rodzaju. Zgodnie z nurtem obiektywizującym to reguły znaczeniowe ukształtowane zwłaszcza w kulturze danego społeczeństwa winny decydować, czy dane zachowanie należy klasyfikować jako czynność prawną¹.

¹ Zbigniew Radwański: Prawo cywilne-część ogólna, Warszawa 1997 str.183 i nast.

Przepisem o charakterze *lex generalis* w zakresie oświadczenia woli jest art. 60 KC. Regulację o charakterze *lex specialis* zawiera art. 7 PrBank.

Wzmiankowany art. 60 KC materializuje zasadę dowolności sposobu uzewnętrznienia woli, ustalając, że można tego dokonać przy pomocy dowolnych znaków. Stąd też możemy przeprowadzić dychotomiczny podział oświadczeń woli na **językowe i pozajęzykowe** (mimika, gest, czyn). Każde należy analizować stosownie do okoliczności konkretnego przypadku¹. Pozajęzykowe oświadczenia woli określane są mianem oświadczeń składanych w sposób konkludentny. Termin „konkludentne oświadczenia woli” odnosi się tylko do samej formy oświadczenia, nie dotyczy natomiast treści czynności prawnej. Treść bowiem, albo jest niewątpliwa, albo może budzić wątpliwości, a wówczas stosować należy dyrektywę interpretacyjną z art. 65 KC. Należy jednak pamiętać, że w każdym przypadku chodzi o oświadczenie woli, które ma być treścią czynności prawnej, a więc oświadczenie, które ma wywołać określone skutki prawne. Zrozumiałe jest również, iż dowolność ta nie znajdzie zastosowania, gdy ustawa lub umowa przewidyuje będzie w zakresie formy dalej idące wymagania².

Dochodzimy więc do refleksji następującej: na gruncie aktualnej polskiej legislatywy nie można prawnie skutecznie drogą elektroniczną dokonać czynności prawnej, dla której zastrzeżona została forma szczególna, a to z uwagi na to, że nie możemy uczynić zadość warunkom zachowania pisemności z art. 78 KC tzn.:

- treść oświadczenia woli utrwalona w postaci dokumentu
- własnoręczny podpis

Wyjątek od tej zasady wprowadza nowatorski art. 7 PrBank:

Art. 7. 1. Oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażone za pomocą elektronicznych nośników informacji. Związane z czynnościami bankowymi dokumenty mogą być sporządzane za pomocą elektronicznych nośników informacji, jeżeli dokumenty te zostaną w sposób należyty utrwalone i zabezpieczone.

¹ Zbigniew Radwański *op.cit.* str. 197

² Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 198 i nast.

2. Jeżeli ustawa zastrzega dla czynności prawnej formę pisemną, uznaje się, że czynność dokonana w formie, o której mowa w ust. 1, spełnia wymagania formy pisemnej.

Przepis ten stanowi jednak wyjątek od zasady wyrażonej w art. 60 KC, wyjątków zaś nie wolno interpretować rozszerzająco.

Z art. 7 pkt 1 wynika, że znajdzie on zastosowanie wyłącznie do oświadczeń woli składanych w związku z dokonywaniem czynności bankowych (w literaturze poddaje się jednak wątpliwość czy ustawodawca miał na myśli wyłącznie czynności wymienione w art. 5 PrBank). Spełnienie kumulatywnych warunków, z pkt 2 (należyte zabezpieczenie i utrwalenie dokumentów sporządzonych za pomocą elektronicznych nośników informacji), uruchamia domniemanie pisemności.

Powyższy przepis będzie przedmiotem mojej późniejszej analizy.

1.1. Chwila złożenia oświadczenia woli.

Art. 61. Oświadczenie woli, które ma być złożone innej osobie, jest złożone z chwilą, gdy doszło do niej w taki sposób, że mogła zapoznać się z jego treścią. Odwołanie takiego oświadczenia jest skuteczne, jeżeli doszło jednocześnie z tym oświadczeniem lub wcześniej.

Jak wynika z wyżej cytowanego art. 61 KC polski ustawodawca przyjął w zakresie złożenia oświadczenia woli **teorię doręczenia**¹. Oznacza to, że momentem złożenia oświadczenia woli jest chwila, w której adresat miał **obiektywną możliwość** zapoznania się z jego treścią. Chodzi tu o pewną sytuację potencjalną, tj. kiedy w normalnym toku czynności adresat może zapoznać się z treścią oświadczenia, nie ma natomiast potrzeby, by faktycznie zapoznał się z jego treścią, podobnie jak nie mają znaczenia przeszkody subiektywne.

¹ „Uzasadnione jest jedynie rozwiązywanie pośrednie, łączące dojście oświadczenia do adresata z możliwością zapoznania się z treścią tego oświadczenia. Takie rozwiązywanie przyjęto w art. 61 zd. 1 KC. Jest ono aktualne do przypadków składania oświadczeń woli tak między obecnymi, jak i między nieobecnymi”; Stefan Grzybowski: System prawa cywilnego – część ogólna, Wrocław-Warszawa-Kraków-Gdańsk 1974 str. 545

Art. 61 KC znajduje zastosowanie zarówno do oświadczeń składanych między obecnymi, jak i nieobecnymi, mimo że literalna analiza zd. 1 sugerować może, że chodzi wyłącznie o oświadczenie między nieobecnymi. Termin „inna osoba” obejmuje adresata zarówno konkretnie oznaczonego, jak i nie oznaczonego konkretnie.

Poza teorią doręczenia wymienia się w doktrynie:

- 1) „**teorię uzewnętrznienia woli**, według której o chwili złożenia oświadczenia rozstrzyga chwila dokonania przejawu woli, a więc np. napisania listu do adresata
- 2) **teorię wysłania**, według której rozstrzyga chwila wysłania pisma, telegramu itd., a więc np. chwila wrzucenia do skrzynki pocztowej lub nadania telegramu
- 3) **teorię zapoznania się**, według której rozstrzyga chwila faktycznego zapoznania się adresata z treścią oświadczenia woli, np. przez przeczytanie listu”¹.

W literaturze porusza się również problem kwalifikacji jako oświadczeń woli w materialnoprawnym znaczeniu, oświadczeń zawartych w pismach procesowych. Samo oświadczenie (z uwagi na formalne wymagania pisma procesowego) realizuje, co prawda wymagania formy pisemnej (także *ad solemnitatem*), wątpliwości dotyczą jednak materialnoprawnych konsekwencji doręczenia pisma procesowego. Zdaniem prof. A. Szpunara sytuację taką zakwalifikować należy jako dwie zbiegające się czynności: procesową i prawnomaterialną². Teoria doręczenia nie jest jedyną akceptowaną przez polskiego ustawodawcę. Procedury m.in. KPC obok teorii doręczenia wprowadzają również (subsydiarnie) teorię wysłania³. Wniesienie pisma procesowego, zawierającego nawet oświadczenie w materialnoprawnym znaczeniu, nie może być jednak utożsamiane z doręczeniem z art. 61 KC. Są to dwie autonomiczne czynności.

Argumentem przemawiającym na rzecz teorii doręczenia jest zwłaszcza ochrona interesu oświadczającego oraz bezpieczeństwa obrotu.

¹ Stefan Grzybowski *op.cit.*

² Adam Szpunar, „Przegląd Notarialny” 6/98 str. 100 i nast.

³ Np. art.165 §2 KPC „*Oddanie pisma procesowego w polski urządzie pocztowym jest równoznaczne z wniesieniem go do sądu*”.

Wprowadza, więc ustawodawca domniemanie prawne:

- **podstawą** domniemania jest dotarcie oświadczenia woli do adresata, w taki sposób, że może on zapoznać się z jego treścią
- **wnioskiem** – przyjęcie, że adresat faktycznie z treścią oświadczenia się zapoznał

Z drugiej strony, aby doręczenie oświadczenia innej osobie było skuteczne musi temu towarzyszyć taki właśnie ukierunkowany **zamiar** po stronie oświadczającego. Nie powstanie więc skutek doręczenia, jeżeli oświadczający nie miał zamiaru, aby jego oświadczenie dotarło do adresata.

Zgodnie z poglądem utrwalonym w doktrynie i orzecznictwie pocztowy dowód nadania, wydruk kontrolny faksu, etc., jest dowodem *prima facie*¹. Oznacza to, iż oświadczający może powoływać się skutecznie na powyższe dowody, ale dowód taki adresat może obalić wykazując, że co prawda wiadomość została wysłana, ale z uwagi np. na zakłócenia, niestabilność połączenia (rozładowania atmosferyczne, burza słoneczna – zakłócenia połączeń radiowych i satelitarnych), etc., nie dotarła ona w ogóle, ewentualnie dotarła w zniekształconej postaci. Mocniejszym dowodem jest pocztowy dowód doręczenia przy doręczeniach sądowych, który według orzecznictwa SN traktowany jest jako dokument urzędowy w rozumieniu art. 244 KPC² (można tu snuć pewne rozważania dotyczące przyszłości, w niektórych państwach planuje się, w innych zaś jest faktem doręczanie pism, również wniosków i pozów z wykorzystaniem łączystek telekomunikacyjnych. Możliwość taką przewiduje również polski ustawodawca w art. 63 KPA, art. 125 § 2 KPC).

Na dzień dzisiejszy nie można natomiast przeprowadzić skutecznego dowodu na doręczenie poczty elektronicznej. Powód tylko częściowo leży po stronie barier technicznych, istotnym problemem są również warunki funkcjonowania podmiotów świadczących usługi internetowe (telekomunikacyjne), którym obecnie nie sposób przypisać charakteru instytucji zaufania publicznego³.

¹ Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 200

² Tak postanowienie SN z dnia 30.04.1998, III CZ 51/98, OSNC 189/11/1998

³ Uzyskanie przez wystawcę certyfikatów akredytacji stanowi potwierdzenie, że jest on instytucją zaufania publicznego (art. 31 ust. 2 UoP-P)

1.2. Wady oświadczenia woli.

Przepisy prawne określające wady oświadczeń woli ustalają okoliczności, których zaistnienie nie jest bez znaczenia dla skuteczności czynności prawnej: definitelywnie przesądza o jej nieskuteczności (nieważność bezwzględna), ewentualnie stwarza możliwość podważenia czynności prawnej (nieważność względna).

W prawie polskim rozróżnić możemy następujące wady oświadczeń woli:

- brak świadomości lub swobody działania (art. 82 KC)
- pozorność (art. 83 KC)
- błęd
- groźba
- wyzysk (art. 388 KC)¹

W sposób szczególny omówić należy problematykę błędu, z uwagi na jego znaczenie dla obrotu elektronicznego.

Błąd jest wadą oświadczenia woli powodującą względną nieważność czynności prawnej. Sama czynność jest, więc skuteczna (nie znajdzie zastosowania art. 58 KC), zachodzi jedynie możliwość jej wzruszenia. Wzruszenie wadliwego oświadczenia woli jest prawem podmiotowym kształtującym, gdzie możliwość skorzystania z niego obwarzanowa została rocznym terminem zawitym. Po upływie roku od wykrycia błędu prawo do wzruszenia wadliwej czynności wygasza (art. 88 §2 KC)². Charakterystyczną cechą nieważności względnej jest pozostawienie uprawnionej osobie swobody decyzji w przedmiocie unieważnienia czynności prawnej. Podważenie wadliwej czynności prawnej następuje przez złożenie pisemnego oświadczenia woli właściwej osobie. Nie wymaga się, aby uchylenie nastąpiło na drodze sądowej (chyba, że chodzi o wyzysk). Konsekwencją uchylenia się od skutków prawnych oświadczenia woli jest nieważność czynności prawnej z mocą wsteczną. Zniweczeniu ulegają wszystkie skutki prawne nieważnej czynności³.

¹ W doktrynie nie ma jednak zgody co do tego czy jest on wadą oświadczenia woli

² Tak wyrok SA w Warszawie z dnia 9.02.1999, I ACa 1105/98, „Prokuratura i Prawo” – dodatek 35/2/2000; tak również wyrok SA w Lublinie z dnia 29.06.1999, I ACa 192/99

³ Tak wyrok SA w Poznaniu z dnia 23.11.1995, I ACr 483/95, „Wokanda” 45/8/1996

Kodeks cywilny nie zawiera klasycznej definicji błędu, wskazując jedynie przesłanki niezbędne dla prawnej doniosłości błędu. Można jednak powiedzieć, że:

„*Błędem jest niezgodne z rzeczywistością wyobrażenie o czynności, przy czym niezgodność może dotyczyć zarówno faktów jak i prawa*”¹.

Art. 84 KC wskazuje dwie kumulatywne przesłanki prawnej doniosłości błędu:

- błąd musi dotyczyć treści czynności prawnej (art. 84 zd. 1)
- błąd musi być istotny (art. 84 §2)

Błąd prawnie doniosły musi dotyczyć jakiegokolwiek elementu treści czynności prawnej może więc to być błąd co do osoby (*error in persona*), przedmiotu świadczenia (*error in corpore* zarówno *in substantia* jak i *in qualitate*), niekoniecznie obejmować musi *essentialia negotii* czynności prawnej. Brak porozumienia (*dissensus*), czy błędne określenie znanego sobie stanu rzeczy (*falsa demonstratio*) nie stanowią błędu w rozumieniu KC². Drugą cechą konieczną błędu doniosłego jest jego istotny charakter. Wskazuje się, iż wymagane jest, dla prawnej doniosłości błędu, aby błąd był subiektywnie i obiektywnie istotny. Oznacza to, że „można powołać się tylko na błąd uzasadniający przypuszczenie, że gdyby składający oświadczenie woli nie działał pod wpływem błędu (błąd subiektywnie istotny) i oceniał sprawę rozsądnie (błąd obiektywnie istotny), nie złożyłby oświadczenia woli tej treści”³.

Błędy oświadczeń woli podzielić można na:

- błędy *sensu stricto*
- pomyłki

Błąd sensu stricto to fałszywe wyobrażenie o właściwościach przedmiotu transakcji (strony mogą w umowie wyjaśniać cele, zadania, właściwości przedmiotu transakcji, jeżeli tego nie zrobią to przyjąć należy, że strona chciała

¹ Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 277

² Stefan Grzybowski *op.cit.* str. 580

³ Art. 84 § 2 KC

używać rzecz zgodnie z jej przeznaczeniem), natomiast niezgodność między wolą oświadczającego a treścią oświadczenia to **pomyłka**¹.

Nie jest natomiast, co do zasady, prawnie doniosły błęd w pobudce (jest zaliczany do błędów nie dotyczących treści czynności prawnej), jednakże orzecznictwo wskazuje, że jeżeli do treści czynności prawnej włączona została określona motywacja, to wówczas błąd w pobudce urasta do rangi błędu prawnie doniosłego, mimo że sam prawnie doniosły nie jest².

Błąd może dotyczyć zarówno okoliczności faktycznych jak i prawnych. Jeżeli błąd dotyczy okoliczności prawnych, a ponadto jest błędem co do treści i błędem istotnym można na tej podstawie uchylić się od skutków wadliwego oświadczenia woli³.

2. FORMA OŚWIADCZENIA WOLI

„Zawarte w art. 73-81 KC przepisy dotyczące formy oświadczeń woli, jak również wspólny tytuł tych przepisów mówią, z niewielkimi wyjątkami, nie o „formie oświadczeń woli”, lecz o „formie czynności prawnych”. Problematyka formy nie dotyczy jednak całego stanu faktycznego czynności prawnej, lecz jedynie tego jej elementu, którym jest oświadczenie woli. Należy zatem mówić raczej o formie oświadczenia woli niż o formie czynności prawnej”⁴.

¹ Niemiecki BGB w §155 wyróżnia jako kwalifikowaną postać błędu **nieporozumienie**, według polskiego orzecznictwa nie ma podstaw do zastosowania na gruncie naszego prawa.

² Tak np. wyrok SN z dnia 10.09.1997, I PKN 251/97, OSNAPIUS 389/13/1998, z uzasadnienia: „(...) podstępne wprowadzenie w błąd zachodzi wówczas, gdy podejmowane jest świadomie i umyślnie działanie w celu skłonienia określonej osoby do złożenia danego oświadczenia woli (...) uchylenie się od skutków prawnych takiego oświadczenia woli (...) jest ułatwione w stosunku do zasad ogólnych (...) ustawaodawca skoncentrował się przede wszystkim na sposobie wywołania błędu, nie kładąc nacisku na jego rodzaj i charakter(...) wystarcza aby błąd dotyczył okoliczności spoza treści oświadczenia woli, w tym między innymi strefy motywacyjnej, stanowiącej przyczynę złożenia danego oświadczenia (...)”

³ Tak wyrok SN z dnia 24.01.1974, II CR 761/73, OSP 238/11/1975

⁴ Stefan Grzybowski op.cit. str. 559

2.1. Swoboda formy

„Forma” to różne przejawy uzewnętrznienia woli, czyli sposoby złożenia oświadczenia woli. Polskie prawo stoi na gruncie zasady dowolności formy oświadczenia woli. Oznacza to, że co do zasady, dla skuteczności dokonanej czynności prawnej, prawnie obojętny jest sposób uzewnętrznienia woli. Istotne jest tylko, aby zachowanie oświadczającego było obiektywnie zrozumiałe. Ustawodawca nie wymaga, aby oświadczenie było wyraźne. Wystarczy, aby w kontekście towarzyszących jego złożeniu okoliczności możliwe było przypisanie mu zamiaru wywołania konkretnego skutku.

Dział III księgi I KC nosi co prawda tytuł „Forma czynności prawnych”, jednak zdaniem doktryny bardziej trafne jest sformułowanie: „Forma oświadczenia woli”. Pomiędzy pojęciami „czynność prawa” i „oświadczenie woli” nie sposób również postawić znaku równości. Oświadczenie woli jest jedynym koniecznym, jednakże nie zawsze wystarczającym elementem składowym czynności prawnej (innymi elementami koniecznymi mogą być np. przeniesienie posiadania, wpis do księgi wieczystej, etc).

Rekapitulując możemy powiedzieć, że wyrażona w art. 60 KC zasada znajdzie zastosowanie i pozwoli na skuteczne dokonanie czynności prawnej w tych wszystkich przypadkach, kiedy ani umowa, ani ustanawa nie stanowią inaczej.

Czynności prawnej dokonanej przez fakty konkludentne (której treść nie jest jednoznaczna) nie można przypisać treści, która nie wynika z samego oświadczenia, ustawy, zasad współżycia społecznego ani z ustalonych zwyczajów (art. 56 i 65 KC)¹.

2.2. Formy szczególne

Od zasady dowolności formy istnieją wyjątki. Mogą one być rezultatem umowy stron, jak i nakazu ustawodawcy. W takim przypadku mówimy o formach szczególnych. Wszelkie formy oświadczenia woli, które zostały zastrzeżone przez

¹ Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 198

strony lub ustawę stanowią w gruncie rzeczy formę szczególną, jako wyjątek od zasady.

Motywy wprowadzania form szczególnych są różne. W doktrynie wskazuje się m.in. na chęć zwiększenia bezpieczeństwa obrotu, wyeliminowania niebezpieczeństwa zbyt pochopnie podejmowanych decyzji, może wreszcie forma szczególna umożliwiać reglamentację obrotu (np. konieczność ujawnienia czynności w księdze wieczystej). Czasami wprowadzenie formy szczególnej podyktowane jest interesem samych stron (np. forma zastrzeżona *ad probationem*).

Przepisy o formie czynności prawnej mają charakter *iuris cogens*, co oznacza, że w danym przypadku stronom nie wolno złożyć oświadczenia w innej formie niż zastrzeżona forma szczególna. Niedochowanie formy nie zawsze jednak pociągać musi nieważność samej czynności prawnej. „Los” takiej czynności uzależniony jest od sankcji zastrzeżonej na wypadek niedochowania formy.

Polskiemu prawu znane są cztery formy szczególne:

- Forma pisemna zwykła
- Forma z podpisem urzędowo poświadczonym
- Forma z datą pewną
- Forma aktu notarialnego

Katalog tych form jest zamknięty (*zasada numerus clausus*) i hierarchicznie uporządkowany, tzn. forma zostanie zachowana również wówczas, gdy zastosujemy formę wyżej ulokowaną w hierarchii niż forma zastrzeżona (chyba, że zastrzeżono formę aktu notarialnego).

Dla nas, na potrzeby „obrotu elektronicznego”, znaczenie praktyczne posiada głównie forma pisemna zwykła.

Do zachowania formy pisemnej wystarcza spełnienie dwóch przesłanek z art. 78 zd. 1 KC¹:

- nastąpić musi utrwalenie oświadczenia woli
- oświadczenie musi być własnoręcznie podpisane

¹ *Art. 78. Do zachowania pisemnej formy czynności prawnej wystarcza złożenie własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli. Do zawarcia umowy wystarcza wymiana dokumentów, z których każdy obejmuje treść oświadczenia woli jednej ze stron i jest przez nią podpisany.*

KC nic nie mówi o materiale, na którym oświadczenie woli ma zostać utrwalone. Najczęściej, w tradycyjnym obrocie, będzie to papier.

O ile nie ma wątpliwości jak należy rozumieć słowo „własnoręcznie” (tu ewentualne problemy dotyczą jedynie różnych form zastępczych podpisu), o tyle słowo „podpis” i elementy jego treści budzą spore kontrowersje. Pytania dotyczą m.in. tego, czy podpis musi być czytelny, czy może być oparty na pseudonimie, jakie znaczenie ma sygnowanie dokumentu parafą, etc. Nie wdając się w zbędne polemiki trzeba powiedzieć, że treść podpisu, jego czytelność, etc., uzależnione są w dużej mierze od rodzaju oświadczenia, pod którym podpis składamy¹.

Z art. 78 zd. 2 wynika, że do zawarcia umowy nie jest konieczne złożenie podpisu na egzemplarzu dokumentu zawierającego oświadczenie strony będące przez nią podpisane. Do zawarcia umowy wystarcza wymiana tak podpisanych dokumentów.

Zdaniem doktryny zastrzeżona przez ustawę forma pisemna oświadczenia woli nie może być zastąpiona żadną inną poza aktem notarialnym² (np. wg SN wystawienie przez osobę trzecią weksla własnego i wręczenie go wierzycielowi nie czyni zadość wymaganiom formy pisemnej z art. 522 KC)³.

Szczególna regulacja zawarta została w art. 79 i 80 KC. Przepisy te dotyczą podmiotów, które ze względu na pewne cechy subiektywne, nie są w stanie spełnić przesłanek z art. 73 KC. Wprowadza, więc ustawodawca zastępczą formę podpisu. Oświadczenie złożone bez zachowania przesłanek z art. 79 lub 80 KC uważa się za złożone ustnie.

¹ Np.:

1. Uchwała 7 sędziów SN z dnia 30.12.1993, III CZP 146/93, OSNC 1994/5/94

„Podpis wystawcy weksla musi obejmować co najmniej nazwisko. Prawo wekslowe nie wymaga dla ważności weksla, aby podpis był czytelny. Podpis nieczytelny powinien jednak być złożony w formie zwykle używanej przez wystawę”.

2. Uchwała SN z dnia 09.05.1995, III CZP 56/95, OSNC 1995/9/127

„Osoba sporządzająca testament własnoręczny, która w jego treści wymienia swoje imię i nazwisko przed rozrządzeniem majątkiem, nie dopełnia tym samym obowiązku podpisania testamentu w rozumieniu art. 949 § 1 k.c.”

3. Uchwała 7 sędziów SN z dnia 28.04.1973, III CZP 78/72, OSNC 1973/12/207

„Ważny jest testament własnoręczny (art.949 k.c.) zawarty w liście spadkodawcy skierowanym do spadkobiercy, podpisany w sposób określający jedynie stosunek rodzinny spadkodawcy do spadkobiercy, jeżeli okoliczności nie nasuwają wątpliwości co do powagi i zamiaru takiego rozrządzenia”.

² Stanisław Dmowski, Stanisław Rudnicki *op.cit.* 241

³ Uchwała SN z dnia 17.10 1979, III CZP 68/479, OSNCP 67/4/80

2.3. Niedochowanie formy

Problem skutków niezachowania formy nie istnieje w granicach dowolności formy. Uaktualnia się on w momencie zastrzeżenia formy szczególnej. Na podstawie art. 73 i innych przepisów KC wyróżnić możemy trzy sankcje związane z niedochowaniem formy:

1. *ad probationem*
2. *ad solemnitatem*
3. *ad eventum*

Sankcją najdalej idącą jest sankcja nieważności. Niezachowanie formy szczególnej zastrzeżonej pod rygorem nieważności pociąga za sobą nieważność oświadczenia woli (oraz samej czynności prawnej, której oświadczenie jest niezbędnym składnikiem). Czasami jednak ustawodawca stwarza możliwość konwalidacji nieważnej czynności przez spełnienie świadczenia (np. art. 890 §1 KC). Nieważność czynności nie daje również podstaw do traktowania jej jako czynności niebyłej (*nihil actum*). Może ona, bowiem indukować konieczność zwrotu wzajemnych świadczeń, przyznawać *ius retentionis*, etc¹.

Niezachowanie formy czynności zastrzeżonej pod rygorem ograniczeń dowodowych nie pociąga za sobą nieważności czynności prawnej. Oświadczenie woli złożone w innej, niż zastrzeżona, formie jest ważne i skuteczne. Jednak w razie ewentualnego sporu niedopuszczalne jest powołanie się na dowód z zeznań świadków lub/i przesłuchania stron chyba, że zajdzie jedna z przesłanek z art. 74 §2 KC lub art. 246 KPC.

W razie niedochowania formy zastrzeżonej pod rygorem *ad eventum* (dla wywołania określonych skutków prawnych), czynność jest w zasadzie ważna, wywołuje jednak inne skutki prawne niż zamierzały wywołać strony, względnie niektórych skutków nie wywołuje.

Jeżeli źródło obowiązku złożenia oświadczenia woli w formie szczególnej tkwi w ustawie, trzeba ustalić czy chodzi o formę pisemną zwykłą, czy o inną formę szczególną. Niedochowanie formy pisemnej zwykłej pociąga za sobą sankcję

¹ Stanisław Dmowski, Stanisław Rudnicki *ibidem*

ad probationem, brak innej formy szczególnej sankcji *ad solemnitatem*. Ustawa może jednak wprowadzić inną zasadę.

Jeżeli obowiązek zachowania formy szczególnej wynika z samej umowy stron (bez względu na to, o jaką formę chodzi) zawsze zastrzeżona jest ona pod rygorem nieważności. Gdyby jednak strony zastosowały formę pisemną zwykłą, bez określenia konsekwencji jej niedochowania, przyjmujemy, w razie wątpliwości, że zastrzeżono wyłącznie rygor ograniczeń dowodowych¹.

3. DOKUMENT I PODPIS

3.1. Prawne znaczenie podpisu

„Podpis stanowi jeden z najpowszechniejszych elementów codziennego życia prawnego, a mimo to brak jest jego ustawowej definicji (...). Wykładnia semantyczna wyrazu „podpis” prowadzi jednak do wniosku, że pojęcie to obejmuje tylko napisany znak ręczny (...). Podpis jest graficznym znakiem służącym do identyfikacji danej osoby na dokumencie i poniekąd symbolizuje tę osobę (...). Podpis stanowi na ogół afirmację tego dokumentu (...).²

Złożenie własnoręcznego podpisu na dokumencie obejmującym treść oświadczenia woli stanowi *coditio sine qua non* formy pisemnej. Termin „podpis” nie został zdefiniowany przez ustawodawcę. Ustawa wymaga jedynie, by był to podpis własnoręczny. Podpis, mimo że przesłanka taka nie została *expressis verbis* zawarta w ustawie, powinien być również, co do zasady, oryginalny. Tylko bowiem oryginał może być przedmiotem ekspertyzy grafologicznej, mającej stwierdzić autentyczność podpisu. Moc dowodowa podpisu tkwi nie tylko w jego treści. Zwraca się również uwagę na jego grafikę i topografię. Wszystkie te elementy łącznie mają gwarantować niepowtarzalność podpisu, a więc zapewnić

¹ Art. 76. Jeżeli strony zastrzegły w umowie, że określona czynność prawną między nimi powinna być dokonana w szczególnej formie, czynność ta dochodzi do skutku tylko przy zachowaniu zastrzeżonej formy. Jednakże gdy strony zastrzegły dokonanie czynności w formie pisemnej, nie określając skutków niezachowania tej formy, poczytuje się w razie wątpliwości, że była ona zastrzeżona wyłącznie dla celów dowodowych.

² Filip Rosengarten: Podpis i jego znaczenie w prawie cywilnym, „Palestra” 1/1973 str. 10 i nast.

identyfikację składającej go osoby. Własnoręczność podpisu nie jest zasadą bezwzględnie obowiązującą. Ustawodawca wprowadza wyjątki: w art. 921¹⁰ §2 KC i art. 328 §2 KSH, sankcjonując mechaniczne odtworzenie podpisu. Podpis odbity sposobem mechanicznym jest jedną z postaci tzw. zastępczej formy podpisu.

W literaturze zwraca się uwagę na następujące cechy składowe pojęcia „podpis”:

- „jest to językowy znak graficzny – podobnie jak treść oświadczenia woli utrwalony w dokumencie
- składający oświadczenie woli stawia ten znak własnoręcznie, co pozwala przez badania grafologiczne stwierdzić od kogo on pochodzi
- wskazuje on w zasadzie imię i nazwisko składającego oświadczenie woli, aczkolwiek w okolicznościach, gdy jego identyfikacji można dokonać w inny sposób, wystarczy podpisanie się samym tylko nazwiskiem i to nawet w skróconej postaci
- podpis umieszcza się pod tekstem oświadczenia woli (...)”¹

Restrykcyjna regulacja przyjęta w KC w zakresie formy czynności prawnych nie jest jedynym możliwym rozwiążaniem. W zakresie tym inną koncepcję przyjęli np. ustawodawca szwajcarski i austriacki. Mechaniczne odtworzenie podpisu jest wystarczające do zachowania formy pisemnej w tych przypadkach, w których takie zachowanie jest zwyczajowo przyjęte. Jeszcze inaczej ustawodawstwo niemieckie, gdzie wymaga się złożenia własnoręcznego podpisu pod treścią jednostronnego oświadczenia woli².

Korzyści, jakie daje złożenie własnoręcznego podpisu pod oświadczeniem woli zazwyczaj oceniane są w kontekście realizowanych przezeń funkcji. W doktrynie najczęściej zwraca się uwagę na cztery funkcje podpisu własnoręcznego:

- odróżnia ostateczne oświadczenie woli od jego projektów (funkcja gwarancyjna)
- identyfikuje osobę składającą oświadczenie woli (funkcja identyfikująca)
- pozwala stwierdzić, że oświadczenie pochodzi rzeczywiście od osoby podpisanej na dokumencie (funkcja dowodowa)
- chroni oświadczającego przed pochopnym złożeniem oświadczenia (funkcja ostrzegawcza)

¹ Zbigniew Radwański *op.cit.* str.200

² Anna Jędrzejewska: Pisemna forma oświadczenia woli a „automatyzacja” obrotu prawnego, PiP 1/93str. 69

Trzeba jednak zwrócić uwagę, że w obrocie masowym podpis własnoręczny traci stopniowo swoją doniosłość i towarzyszące jego złożeniu przeżycie emocjonalne. Dlatego zwraca się w literaturze uwagę, że nie chroni on obecnie, w sposób dostateczny, przed zbyt pochopnym składaniem oświadczeń woli.

3.2. Sposób złożenia podpisu

Podpis powinien być złożony pod treścią oświadczenia woli. Treść znajdująca się poniżej podpisu nie jest objęta oświadczeniem składającego podpis. W przypadku dokumentów bardziej sformalizowanych, np. weksle, właściwym miejscem na złożenie podpisu jest dolny, prawy róg. Podpis złożony w innym miejscu pociąga za sobą nieważność weksla.

Podpis powinien mieć charakter trwałego. Zasadniczo wymaganie to podyktowane jest względami dowodowymi, ale brak trwałości w kontekście formalizmu wekslowego (np. wypełnienie i podpisanie weksla ołówkiem) powoduje nieważność weksla.

Istotne trudności dotyczą natomiast treści podpisu. Z uwagi na brak legalnej definicji podpisu zachodzi potrzeba ustalania treści tego pojęcia na podstawie wykładni językowej, funkcji jakie realizuje, kontekstu, w jakim używa go ustawodawca¹.

Przepisy poświęcone formie czynności prawnych mają charakter *ius cogens*. Stąd też wymagają ścisłej wykładni, dotyczy to również używanych przez nie terminów, w tym „podpisu własnoręcznego”. Co prawda cytowane wyżej poglądy SN wprowadzają daleko idącą liberalizację wymagań dla podpisu testatora w testamencie holograficznym², wydaje się jednak, że brak podstaw do zastosowania tego kierunku poza art. 949 §1 KC. Tak zliberalizowany pogląd prezentuje SN także w sprawie miejsca umieszczenia podpisu na testamencie. W razie umieszczenia podpisu w innym miejscu niż bezpośrednio pod testamentem, testament jest ważny tylko wówczas, gdy związek podpisu z treścią rozrządzenia jest oczywisty³.

¹ Zbigniew Radwański *op.cit.* str. 199

² Na gruncie wykładni funkcjonalnej priorytet przyznaje się woli testator (*favor testamenti*), *ibidem* OSNC 1973/12/207

³ Uchwała 7 sędziów SN z dnia 05.06.1992, III CZP 41/92, OSNC 1992/9/147

Pomijając wyżej przedstawioną linię orzecznictwa SN przyjmuje się, że podpis powinien być zasadniczo oparty na nazwisku, można więc skutecznie podpisać się samym tylko nazwiskiem. Doktryna i judykatura nie są też zgodne, co do tego, czy podpis winien być czytelny. Zdaniem SN nie ma wymagania, aby podpis był czytelny w sytuacji, kiedy taki „nieczytelny” podpis identyfikuje składającą go osobę¹. Wydaje się, że rozstrzygnięcie zależy od tego, „na czym” ten podpis złożono. Podpis składany na dokumencie sformalizowanym, jakim jest np. weksel, powinien być czytelny i obejmować zarówno imię jak i nazwisko. Nie jest to wszakże wymóg bezwzględny. Jak była o tym mowa, w sytuacji, kiedy identyfikacji autora można dokonać w inny sposób, np. na dokumencie przyłożono pieczęć imienną, można podpisać się nawet skróconym nazwiskiem.

Zdaniem SN podpis własnoręczny złożyć może tylko osoba umiejąca i mogąca pisać. Podpis jest więc językowym znakiem graficznym, stanowiącym wytwór pisania, utrwalony wraz z oświadczeniem w dokumencie². Nie jest więc podpisem tuszowy odcisk palca, który przy zachowaniu warunków z art. 79 KC rodzi skutki prawne przewidziane dla podpisu. Chodzi tu o formy zastępcke, które mimo, iż nie posiadają cech podpisu, w pewnych warunkach są tak samo jak podpis własnoręczny doniosłe³. Podpisem nie jest także, a tylko kopią podpisu, podpis odbity sposobem mechanicznym, podpis widoczny na dokumencie przesłanym faksem, etc.

Nie ma również waloru podpisu parafa. Dokumentu sygnowanego parafą nie traktuje się jako definitivego oświadczenia woli, a jedynie jako jego projekt.

W orzeczeniu z 17.04.1967 SN wyraził pogląd, że nie ma podstaw, aby podpis w ujęciu prawa procesowego rozumieć inaczej niż podpis w rozumieniu prawa materialnego⁴. Takie stanowisko jest źródłem ograniczeń dowodowych oraz uniemożliwia wnoszenie pism drogą połączeń telekomunikacyjnych. O ile można znaleźć funkcjonale argumenty przemawiające na rzecz ograniczeń dowodowych, o tyle brak argumentów, dla których odmawia się skuteczności procesowej pismom z mechanicznie odtworzonym podpisem.

¹ Uchwała 7 sędziów SN z dnia 30.12.1993, III CZP 146/93, OSNC 1994/5/94

² Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 259

³ Podobnie art. 80, art. 92¹⁰ §2 KC, art. 339 KSH

⁴ Postanowienie SN z dnia 17.04.1967, II PZ 22/67, (niepublikowane)

Rozdział III**ELEKTRONICZNA FORMA
OŚWIADCZENIA WOLI**

Współczesne przepisy poświęcone formie czynności prawnych powstały w epoce, kiedy zasadniczym nośnikiem wszelkich informacji, w tym także oświadczeń woli był papier. „Obrót papierowy” wraz ze swoimi zaletami i wadami, zdominował codzienne życie wielu pokoleń, prowadząc do wykreowania charakterystycznych dla niego typów zachowań, które funkcjonowały i nadal funkcjonują, czy to w postaci powszechnie przyjętego zwyczaju, czy *expressis verbis* wyznaczonych norm postępowania.

Współcześnie z uwagi na możliwość czy wręcz obiektywną potrzebę elektronicznego przetwarzania i przesyłania danych wiele spośród tradycyjnych, ugruntowanych instytucji wyraźnie odstaje od rzeczywistości i wymaga rewizji ze strony ustawodawcy. Nie jest to wszakże postulat generalny. Brak legislacyjnej interwencji staje się stopniowo nie tylko hamulcem rozwoju gospodarczego, ale uniemożliwia wręcz sprawne funkcjonowanie nowoczesnego państwa.

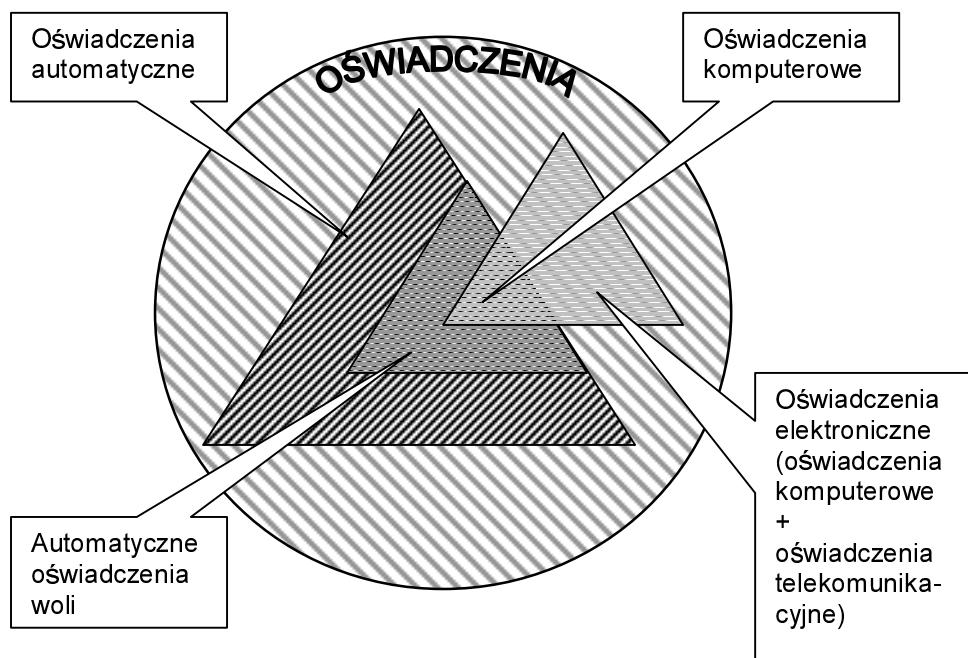
Pytania nurtujące prawników dotyczą nie tylko treści konkretnych przepisów, dotyczą przede wszystkim koncepcji globalnego unormowania obrotu elektronicznego, charakteru prawnego poszczególnych instytucji, recypowania tradycyjnych instytucji o zupełnie nowej treści, burzącej niejako dotychczasowe pryncypia.

Można również poddać w wątpliwość dotychczasowe uporczywe poszukiwania uzasadnienia przesłanek formy pisemnej, dla danych zapisanych na elektronicznym nośniku danych. Chwilowo jest to rozwiązanie w zupełności wystarczające. Nie można jednak wykluczyć, że w przyszłości celowe będzie ukształtowanie od podstaw formy elektronicznej jako formy *sui generis*.

1. MATERIALNOPRAWNE ZNACZENIE INFORMACJI ELEKTRONICZNEJ - „ELEKTRONICZNE OŚWIADCZENIE WOLI”.

Wytwarzanie i wysyłanie oświadczeń przez komputery wykreowało nowe, istotne dla życia prawnego zjawiska, które nie doczekały się jeszcze jednolitej nomenklatury. Część doktryny, dla określenia tak powstałego oświadczenia, używa pojęcia „oświadczenie automatyczne”, inni „automatyczne oświadczenie woli”, jeszcze inni „oświadczenie elektroniczne”. Dla części jedynym właściwym pojęciem jest „oświadczenie komputerowe”. Ta bogata różnorodność pojęć nie jest pozbawiona podstaw, wydaje się jednak, że mają one raczej drugoplanowe znaczenie. Złożenie oświadczenia w obrocie elektronicznym może przebiegać w różnie skonfigurowanych okolicznościach, stąd tak szerokie spektrum ujęć, o czym niżej. Pojęcia te nie są również tożsame.

Wzajemne relacje poszczególnych pojęć można graficznie przedstawić na diagramie:



W literaturze niemieckiej sugeruje się, że pojęciem najbardziej miarodajnym jest pojęcie „oświadczenie komputerowe”. Z terminologicznego punktu widzenia nie jest bowiem obojętne czy oświadczenie jest automatycznie wytwarzane i wysyłane, czy też pochodzi ono od człowieka wprost, a komputer służy wyłącznie do jego transmisji.

Komputerowe oświadczenie to oświadczenie, gdzie komputer, w oparciu o odpowiednie oprogramowanie, automatycznie wytwarza i, co do zasady, w drodze elektronicznej wysyła oświadczenie adresatowi¹.

Cechą charakterystyczną tego oświadczenia jest brak aktywnego udziału człowieka w jego wytworzeniu i wysłaniu. Tymczasem samemu oświadczeniu woli, w dotychczasowym znaczeniu, przypada jedynie funkcja informacyjna (pozwala określić treść przeżyć wewnętrznych człowieka). Decydujące znaczenie dla jego złożenia ma wewnętrzna wola człowieka². W oświadczeniu komputerowym wola ta jest trudno dostrzegalna. Trzeba przyjąć założenie, że taki zamiar człowieka istniał od samego początku.

De lege lata termin „elektroniczne oświadczenie woli” nie posiada żadnej treści merytorycznej. Używany przez doktrynę jest wyłącznie kategorią umowną (terminem roboczym), która może uzyskać prawną doniosłość w przyszłości.

Do niedawna jedynym aktem, który wiązał materialnoprawne konsekwencje z zastosowaniem formy elektronicznej była Ustawa modelowa³. Art. 5 tej ustawy stanowi, iż:

„*Nie można odmówić jakiejkolwiek informacji jej ważności i skuteczności tylko dlatego, że została sporządzona bądź istnieje w postaci elektronicznej*”.

Konsekwencją tego przepisu jest to, że kontrahenci, którzy we wzajemnych stosunkach posługują się informacją elektroniczną nie mogą odmówić jej ważności i skuteczności tylko dlatego, że utrwalona została na elektronicznym nośniku danych. Sam fakt zakodowania i utrwalenia informacji na innym nośniku danych niż papier (najczęściej), nie może być podstawą uznania tej informacji za bezskuteczną lub nie istniejącą w stosunkach pomiędzy tymi stronami.

¹ Josef Mehrings: Vertragsabschluß im Internet, MMR 1/1998 str. 30 i nast.

² Zbigniew Radwański: Teoria umów, Poznań 1977 str. 37

³ Modelowa ustawa UNCITRAL dotycząca zagadnień prawnych związanych z Elektronicznym Przekazem Danych (EDI) i pokrewnych środków komunikacyjnych – przyjęta na 28 oraz 29 sesji Komisji Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego (UNCITRAL) w dniach 2-26 maja 1995r.

W literaturze niemieckiej, proponuje się dychotomiczny podział elektronicznych oświadczeń woli na:

- oświadczenia samodzielnie formułowane przez oświadczającego (również z pomocą EDV) i przesyłane za pośrednictwem połączeń telekomunikacyjnych (**oświadczenia telekomunikacyjne**)
- oświadczenia wytwarzane i przesyłane automatycznie przez urządzenia EDV oświadczającego (**oświadczenia komputerowe**).¹

Oświadczenia telekomunikacyjne są oświadczeniami człowieka, przesyłanymi z wykorzystaniem połączeń telekomunikacyjnych. Doktryna nie ma wątpliwości, że tak ukształtowana wola (*Willensbildung*) jako, że pochodzi od człowieka stanowi oświadczenie woli (*Willenserklärung*).

Pytania rodzi dopiero sytuacja druga – system EDV (*elektronische Datenverarbeitung*) automatycznie wytwarza i wysyła oświadczenie.

Stosunkowo szybko zauważono, że następuje tu rozbicie procesu intelektualnego, na co najmniej dwa podstawowe elementy oświadczenia woli tj. **wolę** oświadczającego i jej **uzewnetrznienie** (*Willensäußerung*), zazwyczaj bowiem ów poślizg czasowy nie występuje. Składanie oświadczenia komputerowego w standardowym trybie ma przebieg następujący:

- osoba X składa oświadczenie woli
- osoba Y (względnie sam X) opracowuje program komputerowy
- komputer wysyła oświadczenie do komputer odbiorcy, z tym, że wysłanie następuje automatycznie, a zatem:
 - oświadczający nie musi mieć świadomości co do faktu wytworzenia i przesłania oświadczenia
 - niejednokrotnie oświadczający nie będzie znał treści wytworzzonego oświadczenia

¹ Tak np. Sven-Erik Heun: Die elektronische Willenserklärung, CuR 10/1994 str. 595 i nast. „Erklärungen, die vom Erklärenden (auch unter Zuhilfenahme von EDV) selbst formuliert und im Wege der Telekommunikation übermittelt werden (**TK-Erklärung**).“

Erklärungen, die von der EDV des Erklärenden automatisiert erstellt und übermittelt werden (**Computererklärung**).“ Można również spotkać określenie *Datenfernübertragung DFÜ* - tak np. Josef Mehrings *ibidem*

W efekcie odnieść można wrażenie, iż to sam komputer podejmuje autonomiczną decyzję o uzewnętrznieniu, wcześniej zkomunikowanego mu przez człowieka oświadczenia. Po stronie komputera nie występuje jednak dowolność zachowań. Komputer „postępuje” zgodnie z wcześniej zadanym mu przez programistę algorytmem, w związku z czym jego zachowania winny być przewidywalne i logiczne.

Brak obecnie argumentów, by mówić o „komputerowym oświadczeniu” w kontekście „oświadczenia woli” (pomijając zupełnie – również istotny, ale oczywisty – aspekt podmiotowości prawnej). Zresztą nawet takowych się nie poszukuje. Zupełnie wystarczające jest (przynajmniej obecnie) przyjęcie założenia, że osoba korzystająca z komputera chce lub musi traktować „oświadczenie komputerowe” jako swoje oświadczenie woli¹. Można, więc wstępnie podzielić pogląd J. Barta i R. Markiewicza, zgodnie z którym komputer porównuje się do *quasi posłańca*². To z kolei pozwala na skorzystanie z dyspozycji art. 85 KC (jak dalej się jednak okaże, brak w tym podejściu pewnej subtelności). Również w literaturze niemieckiej podkreśla się fakt, iż każdorazowe „oświadczenia komputera” są wyłącznie uzewnętrznieniem woli człowieka, z okolicznością zaś, że oświadczający w ogóle korzysta z komputera należy wysnuć zamiar wywołania określonych skutków.

Cały problem koncentruje się więc na urządzeniu technicznym, które stwarza możliwość rozłożenia w czasie powzięcia woli i jej uzewnętrznienia. Nie jest to jednak problem jedyny. Drugi, może nawet istotniejszy, polega na tym, że rola komputera nie ogranicza się do wysyłania wcześniej przygotowanych przez człowieka oświadczeń w ich pierwotnej postaci. Czasami bywa tak, że oświadczenie przybiera postać szablonu i albo komputer wybiera odpowiednie składniki i komponuje oświadczenie o nowej treści, albo sam adresat wybiera alternatywne opcje. W obu przypadkach dochodzi do złożenia oświadczenia o treści niekoniecznie przewidywanej przez oświadczającego (zazwyczaj jednak liczba kombinacji jest zamknięta, a zatem treść oświadczenia jest przewidywalna). Pojawia się pytanie, czy wyznaczone przez przepisy prawne granice pojęcia „oświadczenie woli” nie są zbyt ciasne dla oświadczenia komputerowego?

¹ Tak Josef Mehrings *op.cit.*

² Janusz Barta, Ryszard Markiewicz: Internet a prawo, Kraków 1999 str. 51

Czy takie „oświadczenie” może być w ogóle traktowane jako oświadczenie woli, albo czy będzie ono oświadczeniem woli w każdym przypadku?¹

Początkowe wątpliwości w tym zakresie miały naturę dwuaspektową:

- chodziło o znalezienie podstawy przypisania zautomatyzowanego oświadczenia osobie, która posługuje się komputerem (nie sposób, bowiem przypisać oświadczenia komputerowi, który dokonuje uzewnętrznienia oświadczenia), chodziło więc o granice tej przypisywalności
- chodziło o rozszczepienie w czasie całego procesu składania oświadczenia tj. powięcia zamiaru i jego uzewnętrznienia

W literaturze niemieckiej zwrócono uwagę, iż przy tradycyjnych (pisemnych) czynnościach dla uznania jakiegoś oświadczenia za oświadczenie woli decydujące znaczenie ma to, czy z punktu widzenia odbiorcy było to poważne oświadczenie.

Przyjęto więc tok rozumowania następujący:

Kto korzysta z EDV (*Erklärungen Urheber* – dosłownie inicjator oświadczenia) dla formułowania i wysyłania oświadczeń woli ma **zamiar**, by inni traktowali tę wiadomość jako jego oświadczenie woli. Sam oświadczający powinien mieć również świadomość, iż czynności zautomatyzowane wiążą się dla niego z ryzykiem złożenia oświadczenia woli o treści, której nie mógł do końca przewidzieć (z przyczyn obiektywnych, a więc powinien liczyć się ze złożeniem oświadczenia o dowolnej treści).

Zaakceptowano więc w doktrynie niemieckiej stanowisko, zgodnie z którym: „*zautomatyzowane oświadczenia woli są na ogół prawdziwymi oświadczeniami woli tego, kto posługuje się komputerem, gdyż stanowią wynik logicznych, a nie dowolnych operacji, a ten, kto posługuje się komputerem chce tego rodzaju oświadczeń używać w obrocie jako własnych oświadczeń woli. Taki tok rozumowania odpowiada poglądowi, że o możliwości przypisania komuś oświadczenia woli decyduje tylko to, czy mógł przypuszczać, że jego zachowanie może być dla innych wyrazem oświadczenia woli **jakiejkolwiek treści***”².

¹ Anna Jędrzejewska: Oświadczenia woli składane za pomocą komputera, PiP 3/1992 str. 68 i nast.

² Anna Jędrzejewska *op.cit.*

Z uwagi na zgodę oświadczającego na jakkolwiek treść oświadczenia woli przyrównano oświadczenie zautomatyzowane do **oświadczenia blankietowego**. Blankietowe oświadczenie woli polega na tym, że oświadczający składa podpis *in blanco*, natomiast treść oświadczenia względnie tylko częściowe jej uzupełnienie jest zadaniem osoby w tym celu przez oświadczającego wyznaczonej („umocowanej”). Osoba ta w zasadzie, poza wyjątkowym przypadkiem, nie jest osobą trzecią, a raczej traktowana jest jako jeden podmiot razem z samym oświadczającym. Kreując treść oświadczenia blankietowego związana jest ona zaleceniami oświadczającego.

Ciekawa jest sytuacja prawa „umocowanego”, dlatego że nie jest on ani pełnomocnikiem, ponieważ:

- pełnomocnik działa w imieniu i na rzecz mocodawcy (art. 95 §2 i art. 96 KC)
- osoba ta składa oświadczenie działając pod podpisem „mocodawcy”, dlatego adresat nie musi dochodzić czy istnieją granice „umocowania”

Nie jest on również posłańcem, ponieważ posłaniec sam niczego nie oświadcza a tylko przekazuje (art. 85 KC), tu zaś treść oświadczenia w całości lub w części pochodzi od „umocowanego”. Adresat oświadczenia nie musi nawet wiedzieć, że osoba, która uzewnętrzna wolę nie jest osobą podpisana pod treścią oświadczenia. Jest to konsekwencja posługiwania się blankietowym oświadczeniem woli – akceptacja dowolnej treści oświadczenia¹.

Nasuwa się jednak pytanie następujące, co zrobić w sytuacji, kiedy treść oświadczenia nie odpowiada zaleceniom mocodawcy? Problem ten zostanie omówiony w punkcie poświęconym wadom oświadczeń woli, w tym miejscu wypada jedynie nadmienić, że w zasadzie przyjmuje się, iż dla prawnej doniosłości oświadczenia woli nie ma znaczenia, czy zostało ono wypełnione zgodnie z zaleceniami oświadczającego, czy nie. Stanowisko to znajduje oparcie w założeniu, iż posługiwanie się blankietowym oświadczeniem woli obliguje do uwzględnienia ryzyka wypełnienia oświadczenia niezgodnie z wolą oświadczającego.

¹ Tak samo niemiecka doktryna w odniesieniu do EDV: „Für den Empfänger macht es dabei keinen Unterschied und wird überdies auch nicht erkennbar sein, ob die konkrete Erklärung vom Erklärenden selbst oder von dessen EDV-Anlage erstellt und übermittelt wurde.” - Sven-Erik Heun *op.cit.*

Rekapitulując: aby w obszarze obrotu elektronicznego mówić w sposób prawnie doniosły o oświadczeniu woli, jako ścisłe ukierunkowanym przejście woli człowieka, wystarczające jest, jeżeli oświadczenie złożone przez komputer opierało się na ludzkiej woli (wewnętrznej). Nawet w sytuacji, kiedy oświadczenie jest wytworzane i transmitowane automatycznie, komputer nie może więcej jak tylko realizować program, którego aksjomaty zdefiniował przecież człowiek.

1.1. Doręczenie

Specyfika „obrotu elektronicznego” wymaga pewnej modyfikacji spojrzenia na zagadnienia oświadczenia woli i formy czynności prawnych.

De lege lata nie ma norm szczególnych uwzględniających odmienności obrotu elektronicznego. Zachodzi więc konieczność stosowania wykładni rozszerzającej, w granicach dozwolonej liberalizacji przepisów prawa.

Ponieważ polski ustawodawca hołduje zasadzie doręczenia, naturalną konsekwencją jest pytanie, w którym momencie, mając za podstawę art. 61 KC, uznać można, iż doszło do doręczenia wiadomości elektronicznej.

Zdaniem J. Barta i R. Markiewicza wskazać należy dwa stanowiska:

- 1) do złożenia oświadczenia dochodzi wówczas, gdy dane **przeszły** przez interfejs adresata nawet jeżeli nie zostały one zapisane
- 2) oświadczenie zostało złożone, gdy dane zostały **zapisane** u adresata¹

Autorzy wskazują, że na gruncie polskiego prawa raczej opowiedzieć należy się za drugim stanowiskiem, zgodnie bowiem z teorią doręczenia wiadomość ma dotrzeć do adresata i to w sposób umożliwiający mu zapoznanie się z jej treścią, przeto: „*Miarodajna jest możliwość zapoznania się w normalnym toku czynności, bez szczególnych, nadzwyczajnych nakładów i bez szczególnego wysiłku*”². Pytaniem zupełnie innej natury jest czy faktycznie w obrocie elektronicznym teoria doręczenia realizuje swoją funkcję, czy też celowe byłoby przyjęcie innej teorii np. wysłania, czy zapoznania.

¹ Janusz Barta, Ryszard Markiewicz *op.cit.*

² Sven-Erik Heun *op.cit.*, tak samo również Janusz Barta, Ryszard Markiewicz *ibidem*

Z lektury opracowań niemieckich wynika, iż tamtejsza doktryna uzależnia w pewnym zakresie, moment doręczenia elektronicznego oświadczenia woli od rozstrzygnięcia czy oświadczenie złożono w stosunkach między obecnymi czy nie obecnymi – ten ostatni problem oczywiście wykracza poza ramy niniejszego opracowania, zaznaczmy jedynie, że w większości przypadków będzie to komunikacja pomiędzy nieobecnymi. W takim przypadku rzeczywiście decyduje sama możliwość zapoznania się z treścią wiadomości. Tu również wyróżnia się dwie sytuacje doręczenia elektronicznego oświadczenia woli:

- 1) kiedy Nadawca wysyła swoje oświadczenie bezpośrednio Odbiorcy
- 2) kiedy sam Nadawca lub osoba trzecia, świadcząca określone usługi telekomunikacyjne, utrzymuje oświadczenie w gotowości zapoznania się na żądanie Odbiorcy

W pierwszym przypadku momentem doręczenia jest przejście danych przez interfejs Odbiorcy, który stanowi notabene początek jego strefy władztwa (ustawa modelowa posługuje się określeniem „*system informatyczny*”). Oznacza to, że zakres odpowiedzialności wynikającej z ryzyka przekazu w przypadku Nadawcy i Odbiorcy kończy się np. na gniazdce linii telefonicznej, do którego podłączony jest komputer, faks, czy inne urządzenie¹.

Przyjmuje się, że w obrocie profesjonalnym obiektywna możliwość zapoznania się² z wiadomością elektroniczną powstaje, kiedy wiadomość ta dociera do Odbiorcy w zwykłym czasie pracy chyba, że Odbiorca korzysta z EDI, w takim przypadku zawężenie czasu do „czasu pracy” nie obowiązuje (dotyczy to również obrotu komercyjnego).

W drugim przypadku, nie decyduje moment przejścia danych przez interfejs Odbiorcy. O doręczeniu należy mówić już w momencie, kiedy Odbiorca za zgodą Nadawcy³ lub innej osoby (np. provider) uzyskał dostęp, obiektywnie rzecz biorąc do wiadomości (np. list na mailboxie). W literaturze niemieckiej wskazuje się, że „normalny tok czynności” wymaga sprawdzania mailboxu co najmniej raz w ciągu dnia, a w obrocie profesjonalnym co najmniej dwa razy dziennie tj. na początku i

¹ Tak np. Sven-Erik Heun *op.cit.*

² W prawie niemieckim używa się zwrotu „przyjęcie wiadomości” (*Kenntnisnahme*)

³ Jest to ukierunkowany zamiar złożenia oświadczenia woli, stworzenie obiektywnych warunków do zapoznania się z jego treścią

końcu dnia roboczego (moim zdaniem wszelkie próby sztywnego określenia częstotliwości monitorowania poczty każdorazowo prowadzą do wykreowania pewnej fikcji). Wskazane wyżej momenty, jako najbardziej miarodajne dla doręczenia, nie znajdują zastosowania przy korzystaniu z systemu całodobowego dostępu (24 – Stunden – Services)¹. W takim przypadku oświadczenie przesypane w drodze elektronicznej uważa się za skutecznie doręczone, jeżeli tylko powstaje możliwość jego przetwarzania². Posługiwanie się oświadczeniem komputerowym pociąga za sobą rezygnację z tradycyjnych komponentów teorii doręczenia, wprowadza nową jakość w obszar pojęcia „(...) mogła zapoznać się z jego treścią (...)” (*Möglichkeit der Kenntnisnahme*).

Inna sytuacja w porównaniu z prawem polskim występuje w odniesieniu do oświadczeń składanych między obecnymi, tu bowiem prawo niemieckie przewiduje teorię zapoznania się (*Vernehmungstheorie*).

Polska doktryna skłania się w kierunku tezy, że ten, kto korzysta z elektronicznych środków porozumiewania się na odległość ponosi ryzyko doręczenia wiadomości³. Nie sposób bowiem wykluczyć obarczenia transmisji błędami, które mogą być przyczyną zniekształcenia treści oświadczenia. Ponadto samo oświadczenie i tak może być pozbawione doniosłości prawnej gdyby nie odpowiadało wymaganiom formalnym.

Nieco inną optykę prezentuje orzecznictwo niemieckiego BGH⁴. W większości przypadków wnoszenie faksem pism procesowych odbywa się na ryzyko sądu.

Stosując rozszerzającą wykładnię przepisów o doręczeniu zastępczym (art. 138 i 139 KPC) możemy pokusić się o uwagi następujące. Wymaganiami określonym w art. 61 KC odpowiada doręczenie listu domownikowi adresata, pozostawienie listu lub awiza w skrzynce na listy, etc. Synonimem skrzynki na listy w obrocie elektronicznym jest mailbox na serwerze housta. Klarowność zjawiska przesyłania nam może „normalny tok czynności”, trudny do syntetycznego zdefiniowania z uwagi na niedookreśloność typowych dla obrotu elektronicznego zwyczajów. Wydaje się jednak, że nie ma on aż tak doniosłego znaczenia. Z chwilą bowiem dojścia wiadomości na serwer housta, jest ona dla nas, obiektywnie rzecz ujmując,

¹ Tak m.in. Josef Mehrings *op.cit.*

² Josef Mehrings *op.cit.*

³ Tak Janusz Barta, Ryszard Markiewicz *op.cit.* str. 54

⁴ Stanisław Rudnicki: Współczesne problemy formy czynności prawnych w świetle judykatury niemieckiej, MoP 7/97 str. 272 i nast.

dostępna. Przeszkody techniczne, uniemożliwiające odczytanie wiadomości, mają charakter subiektywny. Poza tym istnieje obecnie wiele możliwości „ściągnięcia” wiadomości elektronicznej. Powoływanie się więc przez adresata, np. na uszkodzenie komputera, nie stanowi należytego usprawiedliwienia zaniedbania z jego strony (braku należytej staranności).

Pojawia się również w obrocie elektronicznym instytucja *quasi awiza*. Z reguły przy profesjonalnych (płatnych) kontach poczty elektronicznej jedną z usług dodatkowych jest serwis SMS. Dostawca poczty informuje o otrzymaniu poczty krótką wiadomością tekstoną wysyłaną na telefon komórkowy lub pager.

Wiadomość w swej treści obejmuje:

- adres zwrotny np. <sklep@post.pl>
- temat wiadomości (jeżeli wiadomość w ogóle ma temat) np. <potwierdzenie przelewu>
- datę i czas dotarcia poczty na serwer houstona
- numer identyfikacyjny nadawcy wiadomości np. <119999> (pełni funkcję podobną do numeru telefonu)

Mając na względzie, że polskie prawo nie określa elementów koniecznych awiza, taką wiadomość można by potraktować jako *quasi awizo*¹. Jedyne wątpliwości, jakie się tu nasuwają polegają na tym, że w obrocie tradycyjnym to nadawca wypełnia stosowny formularz. W przypadku wyżej omówionej wiadomości tekstonej warunek ten zachodzi wyłącznie w odniesieniu do dwóch pierwszych elementów, które zostają automatycznie pobrane z oryginału wiadomości i umieszczone w treści wiadomości tekstonej (bez wiedzy nadawcy).

Obrót elektroniczny sprawia, że w zasadzie w każdej chwili, o każdej porze dnia i nocy musimy liczyć się z możliwością otrzymania poczty elektronicznej (zupełnie inaczej, jak przesyłki konwencjonalne). Dlatego też przyjmuje się, że właściciel skrzynki poczty elektronicznej ma obowiązek regularnego monitorowania jej zawartości w godzinach pracy. Tak rygorystyczny obowiązek nie dotyczy kontrahenta.

¹ Rozporządzenie Ministra Łączności w sprawie warunków korzystania z usług pocztowych o charakterze powszechnym z dnia 15.03.96r. Dz.U. 96/40/173

„§ 12. 1. Nadawca wypełnia przeznaczone dla niego części formularza lub blankietu, stosowanego przez podmiot przy świadczeniu usługi poczтовej o charakterze powszechnym. Podmiot może odmówić wykonania usługi, jeżeli formularz został wypełniony niekompletnie, nieczytelnie, ze skreśleniami, śladami wycierań oraz zmian”.

1.2. Błąd

W literaturze niemieckiej funkcjonuje powiedzenie „*Irren ist menschlich*” (błędy są ludzkie)¹. Czy komputer może więc popełnić błąd? Jeżeli mówiąc „błąd” mamy na myśli wadę oświadczenia woli w rozumieniu art. 84 KC i nast. (niezgodność między obiektywną rzeczywistością a jej odbiciem w świadomości człowieka)², to tak rozumianego błędu nie sposób przypisać maszynie. Błąd jest elementem statutu personalnego osoby fizycznej, jego powstanie poprzedzone zostaje powięciem fałszywego wyobrażenia o rzeczywistości. Niezbędna zatem do popełnienia błędu jest umiejętność myślenia, postrzegania i oceniania rzeczywistości. Komputer natomiast nie myśli, jest urządzeniem technicznym realizującym określone, z góry założone operacje matematyczne. Mówienie o błędzie sensu stricto w obszarze oświadczeń komputerowych jest pewnym skrótem myślowym, chodzi bowiem głównie o konsekwencje błędnych dyspozycji człowieka przetworzonych przez maszynę.

Dodatkowe przesłanki prawnej doniosłości błędu formułuje ustawodawca dla odpłatnych oświadczeń woli składanych innym podmiotom. Jest to o tyle ważne, że najczęściej oświadczenia składane w obrocie elektronicznym zaliczane są do oświadczeń składanych innej osobie i chodzi o czynności odpłatne³.

Możliwość powołania się na błąd powstaje wówczas, gdy błąd (ponadto, że musi być błędem istotnym i co do treści) został wywołany przez adresata (nawet bez jego winy), adresat o błędzie wiedział lub z łatwością mógł się dowiedzieć (art. 84 § 1 KC). Wywarzenie interesu obu stron przemawia za udzieleniem silniejszej ochrony kontrahentowi niż samemu oświadczającemu chyba, że kontrahent sam przyczynił się do powstania błędu.

W niemieckim systemie prawnym doktrynalną ocenę oświadczenia komputerowego oparto na konstrukcji oświadczenia blankietowego, tak również spojrzeć należy za problem błędu i jego konsekwencje.

Przede wszystkim pojawia się pytanie, co dzieje się w momencie wytworzenia oświadczenia komputerowego niezgodnie z założeniami oświadczającego, jak

¹ Josef Mehrings *op.cit.*

² Zbigniew Radwański *op.cit.* str. 225

³ Ze zd. 2 § 1 art. 84 wynika jednak, że w przypadku czynności prawnej nieodpłatnej nie ma potrzeby dowodzić, że osoba, której oświadczenie woli zostało złożone, wywołała błąd - tak wyrok SA w Poznaniu z dnia 18.06.1991, I ACr 151/91, OSA 21/4/1991

bowiem wynika z istoty oświadczenia blankietowego adresat nie musi wiedzieć, że oświadczenie nie pochodzi wprost od oświadczającego. Co do zasady obowiązuje wówczas reguła następująca: dla prawnej doniosłości oświadczenia woli nie ma znaczenia czy zostało ono wytworzzone zgodnie z założeniami oświadczającego, czy nie. Wyraźna jest więc tu ochrona interesów adresata tego oświadczenia, należy bowiem przyjąć, że ten, kto posługuje się takim oświadczeniem musi również uwzględnić ryzyko wytworzenia go niezgodnie z jego wolą, wadliwego działania infrastruktury technicznej.

Obrót zautomatyzowany, zwłaszcza EDI, jest obrotem profesjonalnym, nie ulega, więc wątpliwości, że czynności tu dokonywane mają charakter odpłatny, samo zaś oświadczenie należy do oświadczeń składanych innej osobie. Znajdzie więc zastosowanie art. 84 KC.

W oświadczeniu blankietowym błędem istotnym, na który może powołać się oświadczający będzie tylko błąd „umocowanego”, a to dlatego, iż na tę właśnie osobę scedowana została kompetencja do wypełnienia w całości lub w części treści oświadczenia. Oświadczający z góry akceptuje jego treść, która jednakże winna zawierać się w granicach jego zaleceń. Dla oświadczenia komputerowego oznaczałoby to powołanie się na błąd komputera, co w rzeczywistości oznacza błąd popełniony przez człowieka, głównie przy wprowadzaniu danych. Ewentualnie taki stan faktyczny zakwalifikować można jako błąd systemowy, o czym niżej. W przypadku przekroczenia zaleceń oświadczający może powołać się na swój błąd co do treści oświadczenia, może również powołać się na podstęp osoby „umocowanej”. W takim przypadku, biorąc pod uwagę interes oświadczającego, „umocowanego” należy potraktować jako osobę trzecią. W ramach oświadczenia komputerowego jednoznacznie wykluczyć należy możliwość powołania się na błąd w wyżej omawianym przypadku. Komputer, który wytwarza oświadczenie woli nie myśli, nawet więc, gdy finalnie wytworzone oświadczenie woli wykracza poza wprowadzone przez człowieka aksjomaty, skuteczność dokonywanej czynności prawnej mieści się w ramach ryzyka oświadczającego. Ryzyka związanego z wyborem takiej formy komunikacji. Trzeba jednak wskazać okoliczność szczególną tzn. kiedy powyższy stan faktyczny jest rezultatem ingerencji osoby trzeciej (przy zachowaniu warunków z art. 86 § 2 KC) lub samego kontrahenta w cudzy system informatyczny. Wydaje się, że w takim przypadku

zachodzi podstawa powołania się na podstęp. Dla czynności prawnej, której częścią składową jest blankietowe oświadczenie woli oznacza to dwie sytuacje:

- 1) podstęp strony (adresata oświadczenia), wówczas oświadczający może powołać się na błąd personelu obsługującego system informatyczny, czy błąd samego komputera. Z uwagi na to, że komputer błędu popełnić nie może, właściwe jest powołanie się oświadczającego na swój błąd w pobudce¹. Osoba trzecia podstępnie zmieniła założenia programu, w oparciu o który działa system informatyczny oświadczającego, z zamiarem uzyskania oświadczenia o korzystnej dla siebie treści.
- 2) podstęp personelu obsługującego system informatyczny oświadczającego lub osoby trzeciej (przy spełnieniu przesłanki z art. 86 §2 KC)², w takiej sytuacji personel na zewnątrz danej czynności prawnej traktowany będzie jako osoba trzecia³.

Po stronie osoby, która nie złożyła oświadczenia woli, a podana została przez osobę trzecią jako składająca oświadczenie, nie powstają skutki prawne, chyba że osoba trzecia działała np. w charakterze jej przedstawiciela. Czynność prawna dochodzi natomiast do skutku z osobą faktycznie składającą oświadczenie woli. Adresat takiego oświadczenia może wzruszyć wadliwą czynność powołując się na błąd co do osoby (art. 84 KC). Jeżeli jednak do transmisji takiego oświadczenia wykorzystano medium elektroniczne, możemy mieć trudności w ustaleniu tożsamości rzeczywistego autora oświadczenia woli. Nawet, jeżeli uda nam się zlokalizować miejsce skąd takie oświadczenie wysłano lub komputer, którego użyto do jego wysłania, nie przesądza to jeszcze o tym, kto jest autorem takiego oświadczenia (np. gdy wykorzystano komputer w bibliotece publicznej).

W odróżnieniu od KC, BGB normuje powyższą sytuację *expressis verbis*. Zgodnie z § 122 BGB, w razie nieważności oświadczenia woli z powodów określonych w § 118 (oświadczenie nie było poważnym oświadczeniem - *nicht ernstlich gemeint*)⁴ lub, jeżeli oświadczenie jest wzruszalne na podstawie §§ 119 i 120 oświadczający

¹ W art. 86 „(...) ustawodawca skoncentrował się przede wszystkim na sposobie wywołania błędu (...)” cytowane już orzeczenie SN I PKN 251/97

² Por. wyrok SA w Katowicach z dnia 19.10.1995, I ACr 514/95

³ Anna Jędrzejewska *ibidem*

⁴ „Eine nicht ernstlich gemeinte Willenserklärung, die in der Erwartung abgegeben wird, der Mangel der Ernstlichkeit werde nicht verkannt werden, ist nichtig”.

ma obowiązek naprawić szkodę, jaką poniosły osoby¹ działające w zaufaniu do tego oświadczenia. Nie jest to jednak odpowiedzialność totalna. Niemiecki ustawodawca wprowadza bowiem ograniczenie i wyłączenie odpowiedzialności:

- odpowiedzialność z § 122 Abs. 1 *in principio* ograniczona jest wyłącznie do interesu, jaki miał poszkodowany w ważności oświadczenia (§ 122 Abs. 1 *in fine*)
- obowiązek naprawienia szkody nie powstaje w przypadku, gdy poszkodowany wiedział/powinien był wiedzieć, przy zachowaniu należyej staranności, że oświadczenie jest nieważne lub, że istnieje podstawa do uchylenia się od jego skutków (§ 122 Abs. 2)

Formułuje się w literaturze niemieckiej postulat, aby adresat takiego oświadczenia mógł żądać przynajmniej wyrównania swej szkody związanej z zaufaniem (*Vertrauensschaden*) lub, aby „oświadczający”, dla uniknięcia zawarcia umowy, musiał je zakwestionować². Jest to szkoda w zakresie tzw. ujemnego interesu umownego (*culpa in contrahendo*), np. koszty zawarcia umowy. Sięga ona do granic szkody w ramach dodatniego interesu umownego (*Erfüllungsinteresse*), tj. szkody będącej następstwem niewykonania zawartej umowy³. Zajście okoliczności określonych w § 122 Abs. 2 wyłącza powyższą ochronę. W takim przypadku czynienie użytku z prawa podmiotowego stanowi jego nadużycie (wg niektórych nie stanowi wykonywania prawa w ogóle)⁴. Stąd też przyznaje się „oświadczającemu” *exceptio doli generalis*⁵.

W literaturze niemieckiej spotkać można różne klasyfikacje błędów charakterystycznych dla obrotu elektronicznego. Najczęściej zwraca się uwagę na cztery ich rodzaje:

- 1) błąd obsługi (*Eingabefehler*)
- 2) błąd połączenia (*Übermittlungsfehler*)
- 3) błąd co do danych (*Datenfehler*)
- 4) błąd systemowy (*Software-, und Herdwarefehler*)⁶

¹ Adresat oświadczenia, a jeżeli oświadczenie nie ma adresata – osoby trzecie.

² Janusz Barta, Ryszard Markiewicz *op.cit.* str. 53

³ Tak Othmar Jauering (red.): *Bürgerliches Gesetzbuch*, München 1979 str. 59

⁴ Tak np. Stefan Grzybowski *op.cit.* str. 255

⁵ Por. orzeczenie BGH NJW 69, 1380

⁶ Josef Mehrings *op.cit.*, podobnie również Sven-Erik Heun *op.cit.*

Na gruncie powyższej kwalifikacji rodzi się pytanie o zakres zaskarżalności elektronicznych oświadczeń woli.

Ad. 1

Obejmuje omyłki maszynowe oświadczającego powstałe w rezultacie błędów pisarskich lub wadliwej obsługi komputera. Jest to sytuacja, kiedy komputer wykorzystywany jest zasadniczo jako maszyna do pisania. Okoliczność, że utrwalone w komputerze oświadczenie woli może być przesyłane w drodze elektronicznej nie pozbawia oświadczającego możliwości powołania się na błąd (art. 84 KC)¹. Przez analogię do § 119 Abs. 1 S. 2 BGB błąd taki kwalifikowany jest jako wada wpływająca bezpośrednio na treść oświadczenia.

Ad. 2

Błędy połączenia obejmują zdarzenia powstające w sieci telekomunikacyjnej, prowadzą one do zmiany lub zniekształcenia treści przesłanego oświadczenia. Oświadczający (*Abseder*) może, w oparciu o powyższe okoliczności, wzruszyć oświadczenie powołując się na art. 85 KC tj. zniekształcenie oświadczenia woli przez osobę użytkową do jego przesłania (posłaniec). Jest to w zasadzie stanowisko doktryny niemieckiej powstałe na gruncie interpretacji § 120 BGB². Daje się ono jednak bez trudu przełożyć na polski grunt, bowiem oba przepisy wprowadzają zasadniczo symetryczne rozwiązania. Jedyna różnica polega na użyciu w § 120 BGB, obok słowa „osoba”, słowa „*Anstalt*”, które oznacza „zakład”, „instytucję”³. Zdaniem niemieckiej doktryny „*Anstalt*” w rozumieniu § 120 BGB obejmuje zmiany techniczne, które rozciągają zakres zastosowania § 120 na prywatnych użytkowników sieci (np. zakłócenia na serwerze dostępowym do Internetu)⁴.

¹ Konkluzja taka powstała na gruncie § 119 Abs. 1 S. 2 BGB, nie różni się on jednak od art. 84 KC.

„§ 119. (1) Wer bei der Abgabe einer Willenserklärung über deren Inhalt im Irrtume war oder eine Erklärung dieses Inhalts überhaupt nicht abgeben wollte, kann die Erklärung anfechten, wenn anzunehmen ist, daß er sie bei Kenntnis der Sachlage und bei verständiger Würdigung des Falles nicht abgegeben haben würde. (2) Als Irrtum über den Inhalt der Erklärung gilt auch der Irrtum über solche Eigenschaften der Person oder der Sache, die im Verkehr als wesentlich angesehen werden.“

² „§ 120. Eine Willenserklärung, welche durch die zur Übermittlung verwendete Person der Anstalt unrichtig übermittelt worden ist, kann unter der gleichen Voraussetzung angefochten werden wie nach § 119 eine irrtümlich abgegebene Willenserklärung.“

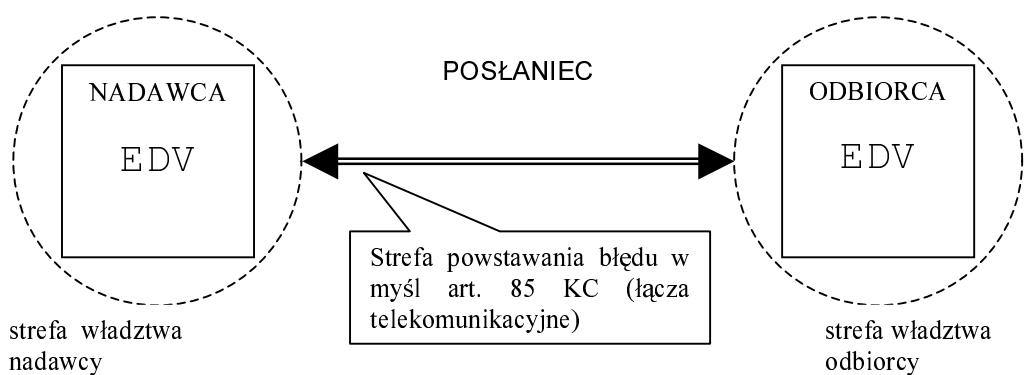
³ Wacław Skubicki: Słownik terminów prawnych i ekonomicznych, Warszawa 1997r.

⁴ Tak Josef Mehrings *op.cit.*, tak też Fritzsche, Malzer, DNotZ 3/95

Wydaje się jednak, że już pojęcie „osoba” jest wystarczająco szerokie, by objąć nim wszelkie przypadki zakłóceń.

Możliwość powołania się na błąd połączenia zachodzi zarówno w obrębie zautomatyzowanym jak i komercyjnym.

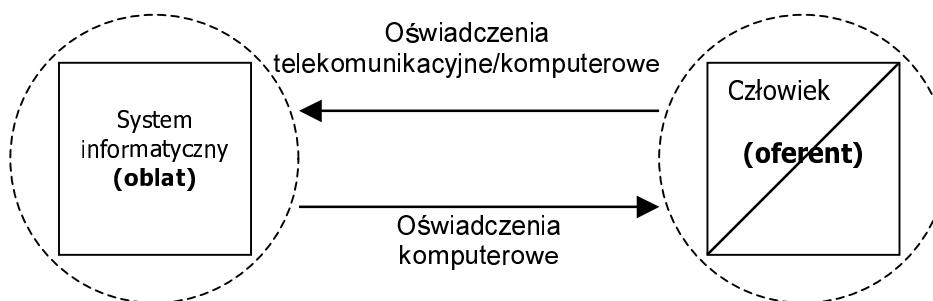
W charakterze posłańca wystąpić może np. operator telefonii stacjonarnej, natomiast nie uzyskuje takiej kwalifikacji system informatyczny (np. EDV) Nadawcy (oświadczającego). Taka kwalifikacja jest konsekwencją zakresu normowania §120 BGB, który obejmuje tzw. błąd przekazu (*Übermittlungsfehler*). Obejmuje on wady oświadczenia powstałe po wyjściu oświadczenia poza strefę władztwa Nadawcy, co widać na poniższym schemacie, a więc w gruncie rzeczy wady powstałe na łączach telekomunikacyjnych (§119 Abs. 1, 2. w związku z §120).



Z drugiej strony zainicjowanie procesu wysyłania oświadczenia, a nawet sterowanie tym procesem odbywa się w systemie informatycznym Nadawcy, który bez wątpienia objęty jest sferą jego władztwa. Nie przesądza to jednak o każdorazowym skutecznym doręczeniu wiadomości elektronicznej, gdyż to uzależnione jest od jakości połączenia telekomunikacyjnego, na które Nadawca zasadniczo nie ma wpływu. Nawet gdyby przyjąć, że Nadawca posiada własne łącza telekomunikacyjne dominuje w literaturze niemieckiej pogląd, że nie mają one charakteru posłańca, lecz rozciagnięciu na owe łącza ulega strefa władztwa Nadawcy. Za takim stanowiskiem podążają określone konsekwencje. Nadawca nie może skorzystać z art. 85 KC.

Ad. 3

Błędne dane (np. nieaktualne ceny na stronie internetowego sklepu) sprawiają, że wytworzone przez komputer oświadczenie nie odpowiada wewnętrznej woli osoby korzystającej z takiego oświadczenia. Oświadczenie komputerowe będzie w takim przypadku złożone skutecznie, ale w pewnych okolicznościach wzruszalne. Obrazowo sytuację przedstawić można na diagramie.



Generalnie sama możliwość wzruszenia oświadczenia komputerowego nie budzi prawniczych sprzeciwów, warunkiem jest wystąpienie prawnie doniosłego błędu. Oferta oparta na błędzie obrachunkowym nie może być wzruszona dlatego, że jest to błąd w pobudce¹, a nie błąd co do treści czynności prawnej. W literaturze spotkać można określenie błędu przewidywania czy wnioskowania, które należą do sfery motywacyjnej podejmowanej czynności prawnej. Tworzą pobudkę, pod wpływem której złożone zostało oświadczenie woli, uznane następnie za błąd oświadczającego, gdy nie osiągnął zamierzonego celu². W sytuacji jednak, gdy taka wadliwa kalkulacja była elementem sprawczym czynności prawnej (została włączona do treści czynności prawnej jako określona motywacja) wtedy błąd w pobudce jest prawnie doniosły.

Przypadek błędu co do danych można zilustrować przykładem: „X” zaciąga w banku kredyt *online*, przy czym w systemie informatycznym banku nie zaktualizowano danych (np. stóp procentowych). Mamy dwie możliwe sytuacje:

- a) nowe stopy procentowe są korzystniejsze dla klienta
- b) nowe stopy procentowe są korzystniejsze dla banku

¹ Tak np. SA w Katowicach z dnia 17.08.1994, I ACz 312/94, „Wokanda” 8/95 „(...) Błąd w prognozowaniu rozpoczętej działalności jest błędem co do pobudki a nie błędem co do treści czynności prawnej i tym samym przepis art. 84 KC nie może tu mieć zastosowania (...)”

² Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 271

ad a)

Zainteresowanym wzruszeniem oświadczenia woli będzie niewątpliwie klient banku. W niemieckiej literaturze odmawia mu się jednak ochrony prawnej w takim przypadku dlatego, że pomiędzy wolą oświadczającego, a treścią oświadczenia nie ma rozbieżności. Klient banku nie wiedział o zmianie wysokości stóp. Nie sposób również drugiej stronie zarzucić podstępu. Komputer, z którym umowa została zawarta, nie myśli, nie mógał, więc wiedzieć o zmianach. Działa prawidłowo, w oparciu o sobie znane wytyczne.

Taki stanowisko będzie do zaakceptowania wyłącznie wówczas, kiedy bank nie zwlekał zbyt długo z aktualizacją danych. Trudno natomiast precyzyjnie stwierdzić ile ten czas może wynosić. Bank powinien zaktualizować dane niezwłocznie. Zwłoka banku uzasadnia powołanie się na podstęp.

ad b)

W tym przypadku to bank zainteresowany będzie wzruszeniem oświadczenia. Widoczne jest tu wyraźne rozbicie na wolę oświadczającego i treść oświadczenia (pomyłka). Za pandektystyczną nauką prawa wyróżnia się:

- wewnętrzny akt woli człowieka, ukierunkowany na wywołanie skutków prawnych
- jego zewnętrzny wyraz – oświadczenie woli

Decydujące znaczenie ma jednak wola wewnętrzna, oświadczenie woli pełni jedyni funkcję informacyjną¹.

Bank w zasadzie mógłby wzruszyć swoje oświadczenie, ale w relativnie krótkim czasie. Opieszałość wyklucza taką możliwość (*mora trahit periculum*). Ewentualnie bank mógłby powołać się na podstęp personelu lub dochodzić roszczeń w ramach stosunku wewnętrznego.

Ad. 4

Błędy systemowe odnoszą się teoretycznie zarówno do błędów sprzętowych (*Hardwarefehler*) oraz programowych (*Systemfehler*). Praktycznie jednak z uwagi na ogólną niezawodność współczesnych komputerów błędy systemowe

¹ Zbigniew Radwański: Teoria umów, Poznań 1977 str. 37

odnoszą się głównie do błędów wywołanych wadliwym funkcjonowaniem oprogramowania.

Zdaniem niemieckiej doktryny błąd systemowy nie jest błędem prawnie doniosłym, nie może więc być podstawą wzruszenia oświadczenia woli¹. Błędy te bowiem pojawiają się już w momencie kształtowania woli przez komputer, na gruncie uprzednio wprowadzonych przez człowieka danych. Ostateczna więc treść oświadczenia powinna być jednoznaczna².

Błędy systemowe przyrównuje się w literaturze niemieckiej do błędu w pobudce. Jest to sytuacja analogiczna jak motyw, który skłonił człowieka do złożenia oświadczenia woli o określonej treści³.

Podsumowując: nadawca wiadomości elektronicznej (zasadniczo będzie to oferent) nie może w rozważanym wyżej przypadku wzruszyć wadliwego oświadczenia woli powołując się na błąd. Nieprawdziwe dane (uwaga ta dotyczy również błędów systemowych) stanowią komponenty, na bazie których winno powstać poprawne tj. zgodne z wewnętrzną wolą oświadczenie woli. Nie są to jednak błędy doniosłe.

Z uwagi zaś na okoliczność, że EDV nie może być traktowany jako posłaniec oświadczający nie może również powołać się na art. 85 KC.

1.3. Odwołanie elektronicznego oświadczenia woli

Problem reguluje art. 61 zd. 2 KC⁴. Jeżeli odwołanie oświadczenia doszło jednocześnie z samym oświadczeniem lub wcześniej jest skuteczne. W pierwszym z omawianych przypadków (oświadczenie komputerowe) możliwość odwołania jest całkowicie wyłączona. W drugim przypadku (oświadczenie telekomunikacyjne) istnieje możliwość skutecznego odwołania oświadczenia do

¹ Tak np. Josef Mehrings *op.cit.*

² Dieter Medicus: Allgemeine Teil des Bürgerlichen Rechts, 1994 str. 256

³ Khun: Rechtshandlungen mittels EDV und Telekommunikation, 1991 str. 151

⁴ Sugestia na bazie analogii do § 130 Abs. 1 S. 2 BGB: „§ 130. (1) Eine Willenserklärung, die einem anderen gegenüber abzugeben ist, wird, wenn sie in dessen Abwesenheit abgegeben wird, in dem Zeitpunkte wirksam, in welchem sie ihm zugeht. Sie wird nicht wirksam, wenn dem anderen vorher oder gleichzeitig ein Widerruf zugeht.“

momentu przewidywanego pobrania wiadomości tzn. pobrania wiadomości w normalnym toku czynności. Przesłanie np. do mailboxu odwołania oświadczenia jest skuteczne niezależnie od kolejności odczytania oświadczeń. Możliwość występującą w drugim przypadku należy jednak również rozważyć potencjalnie¹. Z uwagi na szybkość komunikacji elektronicznej oraz szybkość czy wręcz natychmiastowość przetwarzania poszczególnych zamówień moment złożenia i przyjęcia oferty następuje praktycznie równocześnie. Obiektywnie, nie sposób więc odwołać oświadczenia w oparciu o wyżej wskazaną podstawę. Taką możliwość stwarza konsumentom Dyrektywa Parlamentu Europejskiego z 17.02.1997².

2. FORMA ELEKTRONICZNA - CECHY KONSTITUTYWNE, WIZJE I PROBLEMY PRAWNE.

De lege lata elektroniczna forma czynności prawnych nie doczekała się w Polsce norm o charakterze *lex generalis*. Jedynym, istniejącym w polskim prawie przepisem, który zaledwie podejmuje wyzwanie usankcjonowania formy elektronicznej jest art. 7 PrBank.

Problemem jest rozstrzygnięcie kwestii czy formę elektroniczną uregulować należy w oparciu o ustawy szczegółowe (tak, aby spełniała ona wymagania formy pisemnej zwykłej), czy też, zamieścić ją w kodeksie cywilnym (nawet jako formę *sui generis*), co wymagać będzie jego kompleksowej nowelizacji. Z dwojga rozwiązań bardziej pożądanym wydaje się drugie podejście (takie próby podejmuje się np. w Niemczech).

Art. 7 PrBank budzi spore wątpliwości interpretacyjne (np. czy zakres zastosowania tego przepisu obejmuje wyłącznie czynności bankowe w rozumieniu art. 5 PrBank), które ze względu na ramy niniejszego opracowania w większości pominiemy. Ustawodawca określa przesłanki, które stanowią *conditio sine qua non* spełnienia przez wiadomość elektroniczną wymagań formy pisemnej.

¹ Tak Sven-E. Heun *op.cit.*, tak też Rutke: Rechtsfragen des Electronic Banking, TuW Köln 1988 str. 145

² Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 17.02.1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz. Szerzej na ten temat - Martin Schippan: Electronic Commerce – wie fit ist das sekundäre Gemeinschaftsrecht, ZUM nr. 11-1997, o tym również Janusz Barta, Ryszard Markiewicz: Prawo sieci informatycznych, RP 26.03.1997, http://www.rp.pl/Pl-iso/gazeta/wydanie_970325/

Dokumenty mogą być sporządzane za pomocą elektronicznych nośników informacji, jeżeli zostaną one w należyty sposób utrwalone i zabezpieczone. Jednocześnie ustawodawca nie wyjaśnia, co należy przez owo „*należyte utrwalenie i zabezpieczenie*” rozumieć. Zdaniem W. Kocota niedookreśloność terminologiczna stanowi swoisty walor art. 7, uodparnia bowiem ustawę na zmiany technologiczne, do których zachowuje ona neutralny stosunek¹. Innego zdania jest G. Wiaderek – opierając się na aksjomacie, że banki związane są tajemnicą bankową oraz występują w obrocie jako instytucje zaufania publicznego – wskazuje, że brak precyzji uniemożliwia efektywną weryfikację i nadzór uprawnionych organów². Stwierdza również, że pewną ułomnością art. 7 jest brak wyraźnego wskazania na podpis, jako konieczny warunek skuteczności elektronicznej formy czynności bankowych.

W zakresie pierwszego problemu zgodzić się można, że zbyt duży margines swobody interpretacyjnej jest niepożądany, stąd też trafny postulat autora o legislacyjną interwencję. Może to być jednak, z przyczyn obiektywnych, niemożliwe. Regulacja zbyt kazuistyczna wymagać będzie ustawicznych nowelizacji (problem leży po stronie przyjętych priorytetów: stałości prawa, czy reglamentacji obrotu, co nie oznacza, że nie można ich obu efektywnie pogodzić)³. Nie można natomiast braku podpisu traktować w kategoriach uchybienia ustawodawcy. Złożenie własnoręcznego podpisu jest czynnością konwencjonalną, z reguły, o brzemiennych konsekwencjach prawnych. Ta doniosłość prawa podpisu własnoręcznego wynika z funkcji, jakie taki podpis tradycyjnie w sobie inkorporuje. Nie ma, więc żadnych przeszkód, aby wyciągnąć owe funkcje przed nawias terminu „podpis” i „wtłoczyć” je jako konieczne przesłanki elektronicznej formy oświadczenia woli. W praktyce (wyłącznie ze wzglądów pragmatycznych) spina się owe funkcje nową kategorią – „podpisem elektronicznym” – który, poza realizowanymi funkcjami, nie wykazuje żadnego związku z podpisem tradycyjnym (własnoręcznym).

¹ Wojciech Kocot: Zawarcie umowy w drodze elektronicznej wymiany informacji, PPH 4/98 str. 6 i nast.

² Grzegorz Wiaderek: Internetowe czynności bankowe a forma pisemna czynności prawnych, Internet 2000, Lublin 2000 str. 141 i nast.

³ Warto wspomnieć, że bardzo podobnym w swej treści do art. 7 PrBank jest art. 6 EDI „*Jeżeli przepis prawa wymaga, aby informacja była potwierdzona lub okazana na piśmie, albo określa skutki braku zachowania jej na piśmie, informacja elektroniczna spełnia wymogi pisemności pod warunkiem, że jest dostępna i możliwa do odtworzenia.*” - również nie określono pojęć „dostępna i możliwa do odtworzenia”.

Teoretycznie może dojść do terminologicznego zachwiania w obrębie obu przesłanek z art. 78 KC. Obrót elektroniczny w swej istocie nie różni się od obrotu tradycyjnego, różnice tkwią wyłącznie w przypadłościach (np. podpis elektroniczny nie posiada tak naturalnej cech podpisu własnoręcznego, jaką jest jego topografia).

Problem elektronicznej formy czynności prawnych o wiele wcześniej pojawił się w niemieckim systemie prawnym. Uchwalenie ustawy o usługach informatycznych i telekomunikacyjnych¹ zaktualizowało potrzebę rewizji przepisów BGB i ZPO (zwłaszcza § 126 BGB)².

Pierwszą propozycją były założenia do rozporządzenia o podpisie opracowane przez Niemiecką Federalną Izbę Notarialną³. Zaproponowano wprowadzenie do BGB § 126a, sankcjonującego tzw. „formę elektroniczną”⁴. Treścią „formy elektronicznej” byłby normatywny zapis: „Jeżeli ustawowo zastrzeżona forma miałaby być zastąpiona formą elektroniczną, oświadczający musi tekst oświadczenia podpisać swoim nazwiskiem a cały dokument elektroniczny – sygnaturą digitalną w rozumieniu SigG.”⁵

Dodatkowo notariusz musi niezależnie i bezstronnie poinformować posiadacza klucza o wynikających stąd ograniczeniach i ryzyku, a fakt ten miał zostać stwierdzony w akcie notarialnym.

Kolejny projekt, datowany na 31 styczeń 1997r. przewidywał wprowadzenie „formy tekstuowej”, o następującej treści: „Jeżeli ustawa zastrzega formę tekstuową, oświadczenie woli musi zostać przekazane adresatowi w sposób zapewniający czytelność treści i pewną identyfikację nadawcy. Odbiorca musi mieć możliwość odczytania wiadomości w każdym czasie.”⁶

¹ Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG) vom 13. Juni 1997, dostępny również pod adresem: http://www.iid.de/rahmen/iukdg_bt.html#a0

² Zobacz też Jerzy Jacyszyn *op.cit.* str. 29 i nast.

³ Begründung zur Unterschriftenverordnung vom 12. August 1995 – Vorschlag der Bundesnotarkammer; dostępny również pod adresem: <http://www.fitug.de/>

⁴ W brzmieniu pierwotnym: „Ist durch Gesetz die elektronische Form vorgeschrieben, so muß der Aussteller der Erklärung dem Text seinen Namen hinzusetzen und beides elektronisch unterzeichnen (elektronische Unterschrift). Die elektronische Unterschrift muß in einem als sicher anerkannten Verfahren erklärungsabhängig und unterzeichnerabhängig hergestellt werden. Erklärung und Unterschrift müssen dauerhaft und lesbar wiedergegeben werden können. Die elektronische Unterschrift muß auf eine notarielle Urkunde verweisen, in der Aussteller die Identität der Person bestätigt hat, der verwendete Unterschriftsschlüssel zugeordnet ist, und die Stelle nennen, bei der Unterschriftsschlüssel überprüft werden kann.“

⁵ Entwurf des BMI, Fassung vom 19.05.1999 – <http://www.jurpc.de/aufsatze/20000188.htm>

„(I) Ist durch Gesetz Textform vorgeschrieben, so muß die Willenserklärung einem anderen gegenüber so abgegeben werden, daß sie in Schriftzeichen lesbar und die Person des Erklärenden erkennbar ist. Die

Forma ta miała znaleźć zastosowanie: w prawie o stowarzyszeniach, dzierżawie, najmie, stosunku pracy, rejestrze gruntów, ochronie konsumentów, spółkach i ubezpieczeniach.¹ „Forma tekstowa” spotkała się jednak z krytyką środowisk prawniczych, które ostatecznie (głównie BNK) opowiedziały się za wcześniejszym rozwiązaniem, tj. formą elektroniczną.

3. Zarys problematyki zawarcia umowy.

Specyfika obrotu elektronicznego, zwłaszcza Internet rodzi kolejne nurtujące prawników pytania. Pytaniem w tym zakresie zasadniczym nie jest pytanie czy umowa zawierana jest w trybie oferty, bo najczęściej jest. Prawidłowo postawione pytanie brzmi: kto jest oferentem a kto oblatem?

Wystawienie towaru, a w zasadzie jego obrazu, np. w sklepie internetowym, nie jest ofertą w rozumieniu art. 66 § 1 KC, lecz jedynie zaproszeniem do składania ofert (*invitatio ad offerendum*).

W obrocie elektronicznym zredukowaniu ulega czas, jaki upływa pomiędzy złożeniem a przyjęciem oferty, w efekcie, z przyczyn obiektywnych, trudno skorzystać z dyspozycji art. 66 § 2 KC². Pytaniem zupełnie innej natury jest czy Internet jest środkiem bezpośredniego porozumiewania się na odległość. Odpowiedź wykracza poza ramy niniejszego opracowania, poza tym nie sposób udzielić jednoznacznej odpowiedzi. Rozstrzygnięcie zależy bowiem od każdorazowej konfiguracji sytuacji komunikacyjnej.

W obrocie w pełni automatycznym i całodobowym (24 – *Stunden – Services*), oferent oczekiwany może praktycznie natychmiastowej odpowiedzi oblata (jeżeli taką możliwość przewidziano, biorąc np. pod uwagę bezpieczeństwo obrotu).

Przyjęcie oferty w systemie elektronicznym następuje w bardzo krótkim czasie, zredukowanym praktycznie do kontroli dopuszczalności (zdolności) do zawarcia

telekommunikative Übermittlung wahrt die Form, wenn die Erklärung beim Empfänger jederzeit durch Umwandlung in Schriftzeichen lesbar gemacht werden kann. (2) Bei einem Vertrag ist der Form des Absatzes 1 auch genügt, wenn Angebot und Annahme jeweils getrennt erklärt werden. (3) Die Textform wird durch schriftliche Form oder notarielle Beurkundung sichergestellt.“

¹ Jerzy Jacyszyn *op.cit.*

² Per analogiam do § 147 Abs. 1 S. 2 BGB: „§ 147. (1) Der einem Anwesenden gemachte Antrag kann nur sofort angenommen werden. Dies gilt auch von einem mittels Fernsprechers von Person zu Person gemachten Antrage. (2) Der einem Abwesenden gemachte Antrag kann nur bis zu dem Zeitpunkt angenommen werden, in welchem der Antragende den Eingang der Antwort unter regelmäßigen Umständen erwarten darf.“

umowy. Nie chodzi tu oczywiście o zdolność w aspekcie prawnym (art. 11-22 KC), lecz wyłącznie formalną np. wypełnienie wszystkich niezbędnych pozycji w formularzu zamówienia (w praktyce ten etap dla oferenta może być zupełnie niezauważalny). W obrocie tradycyjnym umowa pomiędzy nieobecnymi dochodzi do skutku, jeżeli oferent mógł, obiektywnie biorąc, zapoznać się z oświadczenie oblata o przyjęciu oferty. W obrocie elektronicznym możliwość taka powstaje, kiedy wiadomość znajdzie się w systemie informatycznym oferenta (dosłownie strefa władztwa - *Machtbereich*). Systemem informatycznym może być np. EDV oświadczającego w takim przypadku dla powstania możliwości zapoznania się wystarcza, że dane przeszły przez interfejs użytkownika. Oświadczenie można jednak przesłać (i to jest sytuacja zasadnicza) osobie trzeciej (np. provider), która przechowuje oświadczenie na żądanie osoby uprawnionej. Dane są więc przechowywane (*zwischengelagert*) np. na mailboxie. Dane są zapisywane na komputerze tej osoby trzeciej tak, że są one możliwe do odbioru (*abrufbar sind*)¹.

Rekapitulując: oświadczenia komputerowe dają się w zasadzie włożyć w normy prawne powstałe w czasie, kiedy obrót elektroniczny był mocno zaawansowaną fantastyką. Znajdują tutaj również zastosowanie, zasadniczo bez konieczności retuszu, postanowienia KC o wadach oświadczenia woli, w szczególności o błędach. Głębszy sens traci podział oświadczeń, na oświadczenie między obecnymi i nieobecnymi. Nie można go jednak ignorować, chodzi wyłącznie o to, że w praktyce czas, o którym mowa w art. 66 § 2 *in fine* KC ulega skróceniu do ram czasowych z art. 66 § 2 *in principio* KC.

Nie można również skutecznie odwołać oświadczenia komputerowego (na podstawie art. 61 z. 2 KC; § 130 Abs. 1 S. 2 BGB) z przyczyn obiektywnych – brak praktycznie widocznego rozbicia w czasie: złożenia oferty i oświadczenia o jej przyjęciu.

Obrót elektroniczny wykazuje co prawda w Polsce ogromną dynamikę, nie jest jednak tak dojrzały jak np. w Niemczech. Mimo ogromnych zmian i innowacji niemiecka doktryna dochodzi do konkluzji następującej: chociaż zmiany są głębokie nie ma zasadniczo potrzeby zmian samego BGB, co najwyżej w zakresie formy czynności prawnych, a tu zwłaszcza podpisu”².

¹ Josef Mehrings *op.cit.*

² Josef Mehrings *op. cit.*

1. USTAWA MODELOWA O WIADOMOŚCI ELEKTRONICZNEJ.

„Krajowy i międzynarodowy obrót handlowy tradycyjnie charakteryzował się tym, że był prowadzony i rejestrowany za pomocą szeroko stosowanej formy pisemnej. Pisemny zapis zawartych transakcji pozwalał nie tylko lepiej określić intencje kontrahentów, lecz również w dostateczny sposób zabezpieczał i chronił ich interesy (...). Obecnie tradycja składania oświadczeń na piśmie ustępuje miejsca nowoczesnym metodom komunikacyjnym i wymianie informacji za pomocą mediów elektronicznych (...)”¹.

Elektroniczna wymiana danych² pozwala na zredukowanie do minimum udziału człowieka w procesie wytwarzania i transmisji dokumentów, które to procesy wykonywane są automatycznie przez komputer i odpowiednie oprogramowanie. Praktycznie eliminuje to konieczność przechowywania danych w postaci papierowej. Komputer rzadziej aniżeli człowiek popełnia błędy, jeżeli jednak popełni błąd, zatacza on w stosunkowo krótkim czasie szerokie kręgi³. Jednakże to obrót papierowy jest bardziej podatny na ryzyko wystąpienia błędu. Wielokrotne przetwarzanie jednych danych potęguje to ryzyko. EDI niweluje taką możliwość na kilka sposobów:

- dane elektroniczne zazwyczaj wprowadzane są z bazy danych, gdzie zostały już zweryfikowane (najwięcej błędów powstaje bowiem na etapie wprowadzania danych)
- dokumenty elektroniczne przesyłane są precyzyjnie bez względu na ich rozmiar

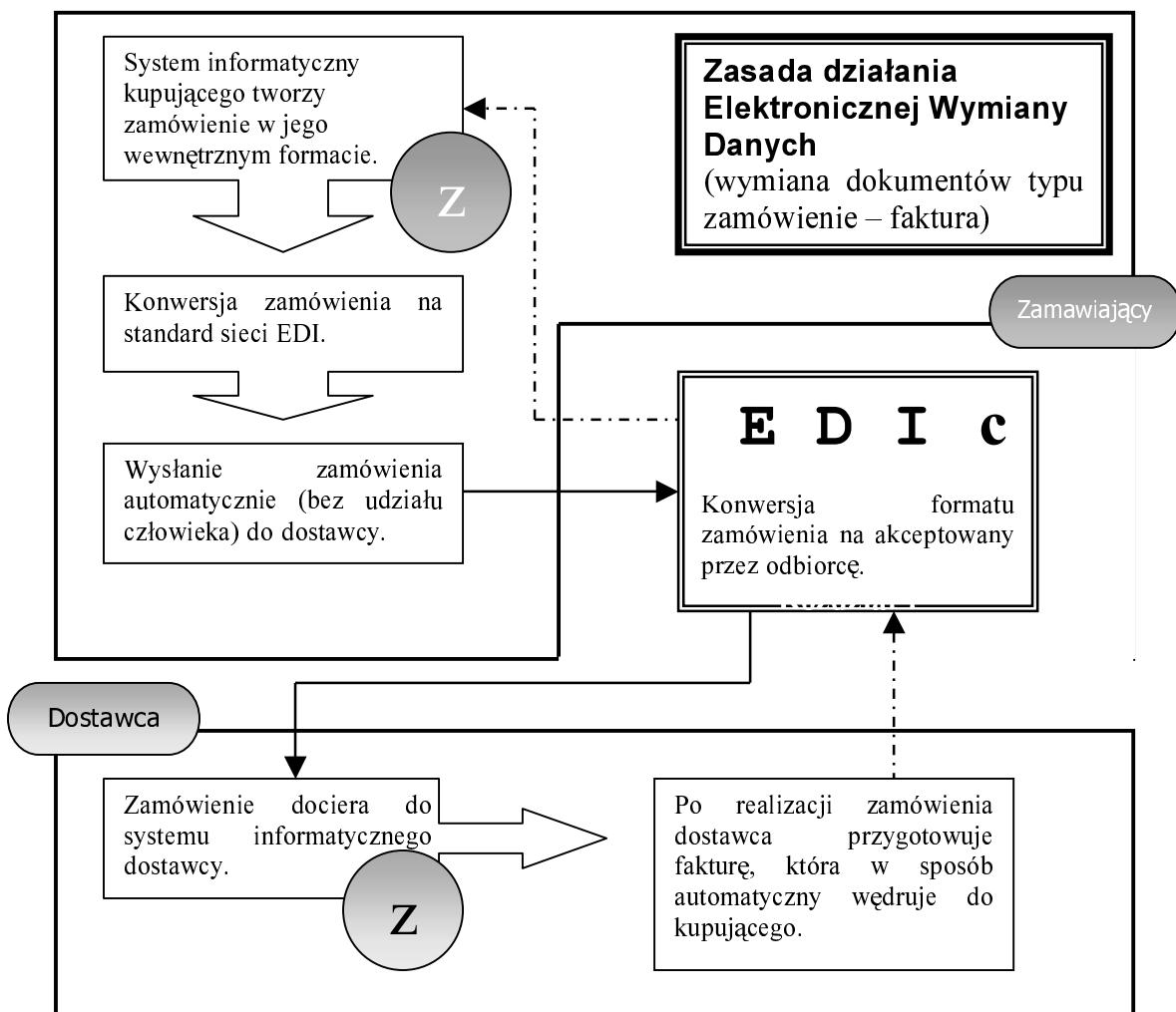
¹ Wojciech Kocot *op. cit.*

² EDI – z ang. Electronic Data Interchange; EDV – z niem. Elektronische Datenverarbeitung – rozumie się przez to transfer informacji elektronicznej z komputera do komputera przy zastosowaniu standardowej struktury tworzenia takiej informacji.

³ Anna Jędrzejewska *op.cit.*

- nawet, jeżeli dokument elektroniczny przetwarza wielu różnych uczestników, z których każdy dodaje dane do istniejącego dokumentu i tak nie ma możliwości zmiany poprzednio wprowadzonej informacji¹

Przesyłanie danych (dokumentów elektronicznych) za pośrednictwem systemu EDI ma przebieg następujący:



Systemy EDI bywają również potocznie nazywane biznesem bez papieru². Zastosowanie systemu ma pewne niekwestionowane zalety (wadą jest przede wszystkim duży koszt). Stwarza on całodobowy dostęp do kontrahenta, w ciągu całego tygodnia, umożliwia dotarcie do osób, z którym nie można było nawiązać kontaktów handlowych z wykorzystaniem konwencjonalnych środków łączności,

¹ Szczegółowe informacje dotyczące działania systemów EDI znaleźć można na stronie <http://www.edi.pl/>

² Szerzej Zbigniew Zwierzchowski: Czek i bank w nowym wcieleniu, RP 30.07.1998; artykuł jest również dostępny pod adresem: <http://arch4.rp.pl/autor-info.html?autorID=1501>

eliminuje bariery językowe, gdyż korzysta się ze standardowych komunikatów elektronicznych.

Pragmatyczne walory EDI rodzą trudne do rozwiązymania problemy prawne, kierunek ich rozwiązania wytyczyć próbuje ustawa modelowa. Ustawa modelowa Jednolitego Prawa Elektronicznego Przesyłania Danych nie ma charakteru imperatywnego. Stanowi jedynie wzorzec, w oparciu o który państwa członkowskie ONZ mogą wprowadzić do swojego prawa wewnętrznego jednolite unormowania dotyczące m.in.:

- standaryzacji przesyłania i wymiany danych za pomocą mediów elektronicznych
- określenia charakteru prawnego umów zawieranych w drodze elektronicznej
- nadania skuteczności prawnej kontraktom zawieranym w drodze elektronicznej wymiany informacji (EDI)¹

Podstawowym pojęciem w obrębie ustawy jest „informacja (wiadomość) elektroniczna”². Jest to informacja, wytworzona, przechowywana i przesyłana za pomocą elektronicznych, optycznych bądź analogicznych środków przekazu, włączając w to także elektroniczny przekaz danych (EDI), pocztę elektroniczną, telegram, teleks i telefaks (art. 2 pkt a.). „Informacja elektroniczna” wyznacza przedmiotowy zakres ustawy.

Z ustawy wynika zasadnicza teza, że sama okoliczność utrwalenia pewnej treści na komputerowym nośniku danych nie może być przyczyną uznania wiadomości za nieważną lub nieistniejącą. Odnosi się to zarówno do organów państwowych (art. 5) oraz samych stron, posługujących się w stosunkach wzajemnych wiadomością elektroniczną (art. 6). *De lege lata* zasada ta znajdzie zastosowanie dla czynności prawnych, dla których nie zastrzeżono żadnej formy (art. 60 KC), ewentualnie zastrzeżono formę *ad probationem*³ (art. 74 KC). Jeżeli dla

¹ Tak Wojciech Kocot *op.cit.*

² Janusz Barta, Ryszard Markiewicz: Transakcje, które biegają po łączach, RP 10.04.1998, artykuł jest również dostępny pod adresem: http://wydanie_980404/prawo/prawo_a_4.html

³ Patrz również wyrok SN z dnia 17.12.1966, I CR 447/66, OSNC 1967/9/153; z uzasadnienia:

„Brak formy pisemnej umowy licencyjnej przewidzianej w art. 19 ustawy z dnia 18 VII 1950 r. (Dz. U. Nr 36, poz. 331) powoduje nieważność tej umowy jako licencyjnej i w konsekwencji nie jest dopuszczalny dowód ze świadków na fakt zawarcia tej umowy (art. 246 k.p.c.). Jednakże brak formy pisemnej wymienionej umowy ma tylko ten skutek, że nie stanowi ona umowy licencyjnej (...) Nieważność ta nie daje jednak podstawy do uznania zawartej umowy za niebyłą (...) Niemniej jednak, jeżeli umowa taka nie jest sprzeczna z ustawą lub z

zachowania formy pisemnej niezbędne jest utrwalenie oświadczenia na piśmie i jego podpisanie, informacja elektroniczna spełnia te wymagania pod pewnymi warunkami. Informacja elektroniczna spełnia wymóg pisemności, gdy jest dostępna i możliwa do odtworzenia (art. 6). Pojawia się tu wzruszalne domniemanie pisemności informacji elektronicznej. Dostępność oznaczać powinna możliwość zapoznania się przez adresata wiadomości elektronicznej z jej treścią w normalnym toku czynności i w każdym czasie. Wiadomość elektroniczna jest dla adresata, obiektywnie ujmując, dostępna, jeżeli znajduje się ona w jego systemie informatycznym (art. 15). Ustawa modelowa nie definiuje jednak pojęcia „dostępność”. Podobnie brak jest definicji „możliwości odtworzenia”. Wydaje się, że należy przez to rozumieć możliwość odczytania wiadomości przez system EDI adresata (a nie człowieka), stąd też wiadomość taka musi być przede wszystkim utrwalona w sposób adekwatny do okoliczności (treść nie musi zostać wyrażona pismem alfabetycznym). Należ również założyć, że zasadniczo ryzyko z powyższego wynikające obciążać będzie dostawcę EDI.

Jeżeli przepis prawa wymaga złożenia podpisu albo określa skutki braku złożenia podpisu, informacja elektroniczna spełnia wymóg złożenia podpisu, jeżeli:

- istnieje skuteczna metoda identyfikacji inicjatora takiej informacji i autoryzacji przez inicjatora zawartych w niej danych, oraz
- metoda ta jest niezawodna i w pełni służy celowi, dla którego wiadomość elektroniczna została wytworzona i zakomunikowana, w świetle towarzyszących okoliczności, a w szczególności umowy między inicjatorem a adresatem (art. 7)

Określenie „istnieje skuteczna metoda” jest na tyle ogólne, że bez problemu mieścią się w nim już funkcjonujące i wdrażane PKI. Co więcej, objąć ono może również inne rozwiązania, obecnie jeszcze nieznane.

Wiadomość elektroniczna powinna być traktowana jako równorzędny z innymi środkiem dowodowym pod warunkiem, że w szczególności: sposób jej wytworzenia, przechowywania i przesyłania, sposób, w jaki zabezpieczono jej integralność oraz oznaczono jej inicjatora zapewnia autentyczność danych w niej zawartych

zasadami współżycia społecznego, wiążę ona strony i skutki jej - jak każdej umowy nienazwanej - powinny być oceniane na podstawie przepisów prawa cywilnego.”

(art. 9 ust. 2). Wiadomość elektroniczna, która spełnia te warunki może stanowić środek dowodowy w każdym postępowaniu przed sądem lub innym organem upoważnionym do rozpoznania sprawy danego rodzaju.

Odróżnienie oryginału dokumentu tradycyjnego od jego kopii nie nastręcza zasadniczo trudności. Dla danych zapisanych na elektronicznym nośniku problem jest istotny z dwóch powodów. Po pierwsze praktyczne trudno stwierdzić, co jest oryginałem wiadomości, a co kopią, po drugie pojawia się pytanie czy dla tego nośnika w ogóle mówienie o kopii na sens. Kopia zazwyczaj posiada te same cechy, co oryginał, zaciera się różnica między pojęciem kopii i oryginału. Art. 8 EDI stawia dwie przesłanki zachowania oryginalności przez wiadomość elektroniczną:

- istnieje dostatecznie obiektywna pewność, że treść informacji pozostaje autentyczna od chwili jej wytworzenia w ostatecznej bądź innej formie elektronicznej
- informację można odtworzyć i ujawnić osobie uprawnionej do jej odczytania

Atrybut oryginalności powiązany został więc wyłącznie z treścią informacji, a nie z nośnikiem, a zatem jedno konkretne oświadczenie woli może teoretycznie funkcjonować w kilku egzemplarzach i każdy z nich będzie oryginalny i autentyczny (dla dokumentów tradycyjnych jest to nieosiągalne, chyba że oświadczenie faktycznie sporządzono w kilku jednobrzmiących egzemplarzach, z których każde jest oryginalne).

Kiedy więc możemy mówić o kopii dokumentu elektronicznego? Zdaniem doktryny niemieckiej kopią dokumentu cyfrowego są dane reprezentowane fizycznie w innej postaci niż oryginał, a dostęp do treści nie wymaga zaangażowania środków technicznych¹. Według tego stanowiska kopią dokumentu cyfrowego będzie np. wydruk.

Jeżeli przepis prawa wymaga trwałego zachowania dokumentu wiadomość elektroniczna ma charakter trwałej, jeżeli kumulatywnie spełnia poniższe warunki:

- jej treść jest w każdej chwili możliwa do odtworzenia i odczytania
- jest utrwalona w tej samej postaci, w jakiej była wytworzona

¹ Stefan Abel: Urkundenbeweis durch digitale Dokumente, MMR 12/98, str. 664 i nast.

- jest utrwalona w sposób umożliwiający ustalenie jej pochodzenia oraz daty przesłania lub doręczenia

Pewne obawy wiążą się również z trwałością elektronicznego nośnika danych (pośrednio więc i samej wiadomości). W przypadku papieru nawet częściowe jego uszkodzenie nie niweczy jeszcze zupełnie treści dokumentu, a w przypadku np. papierów wartościowych inkorporowanego w nim prawa (generalizując musi on zawierać co najmniej minimum treści, aby określić treść inkorporowanego w nim prawa. Oczywiście nie zawsze wystawca/emitent będzie honorował uszkodzone dokumenty). Uszkodzenie elektronicznego nośnika danych z reguły niweczy całą treść zapisanego na nim dokumentu (zapis ma bowiem zupełnie inny charakter niż zapis na kartce papieru). Odzyskanie informacji z takiego nośnika jest albo bardzo trudne, albo wręcz niemożliwe. Obawy można również skierować w zupełnie odwrotnym kierunku tzn. jak skutecznie zniszczyć dokument zapisany na elektronicznym nośniku danych. Wbrew powszechnie panującemu przekonaniu nie jest to proste. „Zwykłe” skasowanie jest niewystarczające, bowiem z reguły dane takie można odzyskać. Poza tym przy obrocie gospodarczym, który „odbywa się” *online* samo pojęcie nośnika danych nieco się rozmywa i w gruncie rzeczy nigdy nie mamy pewności czy posiadany przez nas egzemplarz umowy jest jedyny. Zawsze mógł pozostać „ślad” na komputerze kontrahenta.

2. DOKUMENT ELEKTRONICZNY W POLSCE DE LEGE LATA.

Cechą charakterystyczną dokumentu elektronicznego jest przede wszystkim jego duża wrażliwość na błędy popełniane w chwili jego wytwarzania (wprowadzania danych). Dotyczy to błędów merytorycznych, ale głównie omyłek pisarskich. Specyficzne techniki przetwarzania dokumentów elektronicznych dają możliwość ich wykrywania i łatwego usuwania czy prostowania. Niewątpliwie łatwiej natomiast zapoznać się z informacją zawartą na papierze, aktualizacja danych, ich poprawianie, etc. łatwiej przeprowadzić na dokumencie elektronicznym¹.

¹ Szerzej patrz Andrzej M. Wilk: Państwo w dobie Społeczeństwa Informatycznego – perspektywa strategicznych przemian, Internet 2000, Lublin 2000 str. 185 i nast.

Poza KK polski ustawodawca nie wprowadza do systemu legalnej definicji dokumentu. Z punktu widzenia prawa karnego:

„Dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne” (art. 115 § 14 KK).

Podobnie, dla prawa rzeczowego dokument jest rzeczą, nie ma znaczenia treść intelektualna inkorporowana na określonym podłożu.

Doktrynalne definicje dokumentu podkreślają, że dokumentem jest myśl ludzka, czyli treść intelektualna, wyrażona w sposób graficzny na odpowiednim podłożu.

Aby „dokument” był dokumentem zawierać musi następujące elementy:

- wyraźnie oznaczony być musi autor dokumentu
- treść – myśl autora intelektualnego dokumentu
- myśl musi być wyrażona graficznie (grafika może być dowolna)
- myśl utrwalona musi być na odpowiednim podłożu (w odniesieniu do niektórych typów dokumentów w sposób trwały np. weksel)
- dokument musi być podpisany

Podstawowym nośnikiem treści dokumentu był i nadal pozostaje papier. Jest to konsekwencją ugruntowanej tradycji, w pewnym zakresie również nawyku kreowania dokumentów na tym właśnie podłożu. Obecność dokumentu elektronicznego w naszym życiu prawnym nie jest szczególnie duża, a może trafniej należałoby powiedzieć jest niezauważalna. To również pewna cech swoista, czasami po prostu nie mamy świadomości istnienia dokumentu. Brak kartki papieru, człowieka, który dokonuje zespół czynności finalnie ukierunkowanych na wytworzenie dokumentu. Dokument elektroniczny terminologicznie nie mieści się w obecnej nomenklaturze.

Zaproponować można dychotomyczny podział źródeł prawa, w obszarze zagadnienia dokumentu elektronicznego:

- a) normatywne
- b) pozanormatywne (np. regulaminy bankowe)

ad. a)

Żaden polski akt normatywny *de lege lata* nie posługuje się wprost pojęciem „dokument elektroniczny”, co akurat niczego nie dowodzi, skoro nie definiuje się również pojęcia „dokument”. Samo pojęcie „dokument elektroniczny” zostało co prawda użyte w UoP-P (art. 5 ust. 3), głębsza analiza całości dowodzi jednak, że zostało ono zastosowane nieco na wyrost, bez głębszej refleksji nad konsekwencjami. Można natomiast wskazać przykłady aktów normatywnych, gdzie wyłącznie pośrednio wskazuje się na „coś”, co mogłoby być dokumentem elektronicznym: art. 7 PrBank, art. 125 § 2 KPC czy art. 63 PKA. Użyte w przepisach tych określenia będą przedmiotem mojej późniejszej analizy.

Również ustawy niemieckie nie operują pojęciem „dokumenty elektroniczne” mimo, że sam zwrot powszechnie występuje w literaturze (ściśle, mówi się o „dokumencie cyfrowym”).

Pojęcie „dokument elektroniczny” jest więc pojęciem doktrynalnym i w pewnej mierze skrótem myślowym. Oznacza oświadczenie zapisane na elektronicznym nośniku danych, którego odczytanie wymaga pośrednictwa cyfrowych urządzeń technicznych¹.

ad. b)

W aktach pozanormatywnych, instytucji posiadających własne implementacje PKI często używa się zwrotu „dokument elektroniczny”, „przesyłanie danych elektronicznych”, „elektroniczny wniosek”, etc. (np. na stronach internetowych ZUS służących do teletransmisji danych z programu „Płatnik”)². Pojęcia te nie są jednak definiowane. Należy więc przyjąć, że chodzi tu po prostu o dane (wnioski, etc.) zapisane i/lub przesyłane elektronicznie. Jedyną specyfiką „dokumentu elektronicznego” w tym ujęciu, jest sposób transmisji. Nie wykluczone, że takie podejście jest koncepcją słuszną (wydaje mi się, że jest to jednak zbyt płytkie ujęcie zwłaszcza w kontekście mocy dowodowej).

Dokument elektroniczny utrwalony na elektronicznym nośniku danych jest dokumentem elektronicznym *sensu stricto*. Dokument elektroniczny *sensu largo*

¹ Tak Stefan Abel *op.cit.*

² <http://www.dokumenty.gdansk.zus.pl/Upload.htm>

odejmować będzie także dokumenty zdematerializowane (głównie na papierze) zwane wydrukami komputerowymi lub wydrukami zawartości pamięci¹.

Kwestia uznawania mocy procesowej i materialnoprawnej skuteczności wydruków komputerowych raczej nie budzi sprzeciwów i prawniczych oporów².

Postać wydruku przybierają zarówno dokumenty tak prozaiczne jak np. rachunki telefoniczne, taką postać mają również wypisy z prowadzonych w systemie informatycznym rejestrów sądowych np. księgi wieczyste³. W tym pierwszym przypadku coraz częściej zdarz się otrzymywanie wydruku nie podpisanego (w Niemczech wykształciła się w tym zakresie praktyka polegająca na umieszczaniu adnotacji „wystawiony automatycznie”). Czy jednak na pewno brak na takim dokumencie podpisu? Nie ma najmniejszych wątpliwości, że nie sposób mówić tu o podpisie w rozumieniu art. 78 KC. Wszystko więc zależy od tego, jaką treść zaimplementujemy w pojęcie „podpis” i jaką treść powinien sam podpis zawierać. Brak legalnej definicji podpisu sprzyja niewątpliwie spekulacjom. Nie ma chyba wątpliwości, że wyrażenie „Fakturę wystawił: Kierownik Działu Bilingu” nie czyni zadość wymogowi złożenia podpisu z ugruntowanego, jurydycznego punktu widzenia. Zdaniem większości doktryny nie podpisany wydruk komputerowy nie ma znaczenia w obrocie prawnym jako dokument. Stanowisko to rozciąga się również na moc dowodową wydruku⁴. Oponenci dopuszczają możliwość wprowadzenia substytutu podpisu w postaci np. identyfikatora pracownika⁵.

W nowych realiach najbardziej trafne wydaje się stanowisko pośrednie. Rozstrzygnięcie uzależnić należy głównie od charakteru samego wydruku, od skutków prawnych, które ma on wywołać w obrocie. Jeżeli przedmiotem wydruku jest np. wypis z rejestru publicznego to rzeczą zrozumiałą jest i jednocześnie niezbędna dla ważności samego wypisu, opatrzenie dokumentu pieczęcią, i podpisem pracownika upoważnionego do jego wystawienia. Wypis taki zasadniczo

¹ Dla niektórych wydruk komputerowy nie różni się zasadniczo od zwykłego pisma maszynowego, w Niemczech wydruk traktuje się jako kopię dokumentu elektronicznego.

² Patrz szerzej Krzysztof Knoppek: Wydruk komputerowy jako dowód w procesie cywilnym, PiP 2/1993 str.54 i nast.

³ W systemie informatycznym prowadzić można również księgi rozrachunkowe i księgi podatkowe, z tym, że ich treść jest normatywnie uregulowana – Dz.U. 91/10/35 i 91/125/559

⁴ Andrzej Murzynowski: Wydruk z komputera jako dokument w postępowaniu przed organami państwowymi i społecznymi, Warszawa 1978 str. 89

⁵ Tadeusz Ereciński: Z problematyki dowodu z dokumentu w sądowym postępowaniu cywilnym, Warszawa 1985 str. 84

stanowi dowód określonego faktu, może on uczestniczyć w dalszym obrocie, inne osoby działać będą w zaufaniu do tego dokumentu.

Zupełnie inaczej traktować należy dokumenty wystawiane masowo i automatycznie (np. rachunki telefoniczne, mandaty, wezwania do zapłaty, etc.). Konieczność złożenia własnoręcznego podpisu jest kontra ekonomiczna i zupełnie niepotrzebna. Sama podstawa świadczenia z reguły nie budzi wątpliwości (ewentualnie przy deliktach, np. mandat za przekroczenie szybkości, nie ma charakteru stanowczego, mamy prawo wniesienia odwołania), a identyfikacja wierzyciela może odbywać się poprzez inne dane niż własnoręczny podpis (problemy te powinien rozstrzygać każdorazowo regulamin świadczenia określonych usług).

Aby „dokument elektroniczny” był dokumentem musi zostać zaprezentowany w postaci nadającej się do bezpośredniego odczytania (nie tyle jest dokumentem, co spełnia wymagania stawiane dokumentom w tradycyjnym ujęciu, inną sprawą jest, słuszność takiego podejścia)¹. W nauce prawa przyjmuje się, że dokument zapisany na elektronicznym nośniku danych jest zakodowany, a sąd nie ma obowiązku dekodowania tak zakodowanych treści.

W moim przekonaniu zbyteczne jest tworzenie nowych pojęć, a już na pewno nie należy nowych zjawisk definiować przez wyliczenie, które i tak nie ma żadnej mocy poznawczej. Konstruowanie definicji kazuistycznych i ciasnych w dłuższym okresie czasu doprowadzić może do zupełnego braku wyczucia istoty problemu. Wydaje mi się, że obecnie zupełnie wystarczające byłoby uelastycznienie poglądów w szczególności, co do „własnoręczności”, „podpisu” i języka dokumentu – o czym niżej.

3. SEMANTYCZNA ANALIZA „PISEMNOŚCI” DOKUMENTU ELEKTRONICZNEGO

Dokument elektroniczny oznacza dokument (pismo), którego treść utrwalona została na elektronicznym nośniku danych. Dla zachowania formy pisemnej

¹ Pewną zmianę w odniesieniu do pism procesowych wnoszonych na elektronicznych nośnikach informatycznych wprowadza art. 125 § 4 KPC

niezbędne jest, aby treść oświadczenia woli została utrwalona w dokumencie, a ten został własnoręcznie podpisany (art. 78 KC).

Powszechnie przyjmuje się, że dokument nie musi być sporządzony przez strony osobiści, ale musi być sporządzony na piśmie, dzięki czemu nabiera on wymiaru dowodu¹. Nie ma natomiast znaczenia czy pismo jest maszynowe czy ręczne². Żeby „dokument” był dokumentem poza podpisem (problem własnoręczności podpisu rozwiązują ustawy o podpisie elektronicznym) musi być on sporządzony na piśmie. Problem tego czy dokument zapisany na elektronicznym nośniku danych jest, czy nie jest sporządzony na piśmie nie ma, w zasadzie, istotnej doniosłości praktycznej. Ustawodawcy bowiem przypisują takiemu dokumentowi skuteczność prawną, na gruncie prawa materialnego imperatywnie, w sferze procesowej postulując konieczność uwzględnienia jego mocy dowodowej na równi z dokumentem tradycyjnym.

Warto jednak zbadać, czy założenie ustawodawcy znajduje uzasadnienie w rzeczywistości.

Dokument ma być utrwalony na piśmie, co oznacza wyraźny przekaz za pomocą pisma³. Jaki więc element przesądza o tym, że jeden dokument jest, a inny nie jest utrwalony na piśmie? Kluczem jest treść pojęcia „pismo”. Pismo jest systemem znaków graficznych odpowiadających określonym dźwiękom lub pojęciom⁴ (...) służącym do przenoszenia (transpozycji) mówionej formy języka na formą piszącą zastępowania i przekazywania języka mówionego przez język pisany⁵. Definiensem jest „system znaków graficznych”, mówiąc ściślej znaków językowych. Zamykając więc wnioskowanie dla sporządzenia dokumentu na piśmie nie ma znaczenia podłożę, na którym dokument utrwalono, przesądza utrwalenie treści za pomocą językowych znaków graficznych.

Dochodzimy w ten sposób do pewnych trudności. W literaturze wymaga się, aby pismo było konkretnie pismem alfabetycznym, a treść dokumentu nadawała się do bezpośredniego odczytania. Wymóg taki stawia się w stosunku do dokumentów z punktu widzenia ich mocy dowodowej. Dla materialnoprawnej skuteczności oświadczenia woli nie ma wymogu użycia znaków słownych

¹ Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 256

² Z wyjątkiem testamentu holograficznego (art. 949 KC)

³ Bogusław Dunaj (red.): Słownik współczesnego języka polskiego, Warszawa 1996 str. 751

⁴ Słownik współczesnego języka polskiego str. 348

⁵ Andrzej Z. Makowiecki (red.): Literatura i nauka o języku, Warszawa 1995 str. 590

(mówionych/pisanych). W rzeczywistości „wypowiedź” najczęściej przybiera postać takich znaków, ale niekoniecznie. Art. 60 mówi bowiem o każdym zachowaniu. Zdaniem prof. Zbigniewa Radwańskiego pojęcie „każdego znaku” obejmuje:

- materialny substrat znaku, czyli sporządzony przez kogoś dostrzegalny układ rzeczy lub zjawisk
- reguły znaczeniowe, które z materiałnymi substratami znaków wiążą określone myśli¹

W orzeczeniu amerykańskiego sądu² czytamy, że program komputerowy można uznać za wypowiedź, której swobodę gwarantuje pierwsza poprawka do konstytucji. Zdaniem sądu program komputerowy można uznać za wypowiedź, bowiem jest napisany w określonym języku – języku komputerowym. Z uzasadnienia: „*sąd nie widzi żadnej istotnej różnicy między językiem komputerowym (...) a językiem niemieckim czy francuskim (...). Podobnie jak intonacja muzyczna czy sposób zapisu równań matematycznych język komputerowy jest po prostu językiem i służy przekazywaniu informacji komputerom lub tym osobom, które go rozumieją (...).*”

W istocie potoczne znaczenie pojęcia „język” jest bardzo szerokie, oznacza sztucznie skonstruowany kod, oparty na przekazywaniu określonej, zwykle związanej z daną dziedziną wiedzy, informacji za pomocą symboli. Stąd możemy mówić o języku logiki, komputerów, programowania, etc.³.

Z powyższej definicji wynika, że również język mówiony jest swoistym kodem np. język polski może być nie zrozumiały dla Anglika mimo, że w języku polskim i w angielskim mamy ten sam nośnik informacji tj. drgania powietrza. Sąd amerykański w wyżej cytowanym orzeczeniu pominał drobną subtelność, pomiędzy językiem programowania, a językiem komputera brak tożsamości.

Język komputera (*Rechnersprache*) to język służący do kodowania rozkazów komputera, zaś język programowania (*Programierugssprache*) to język służący do formułowania programów⁴. Komputer nie zna języka programowania, bo ten jest każdorazowo zależny od formatu zapisu, a format zapisu jest charakterystyczny

¹ Zbigniew Radwański: Teoria umów, Poznań 1977 str. 44

² Dariusz Cwiklek: Poemat w Pascalu, publikacja dostępna na stronie: <http://www.odeon.pl/>

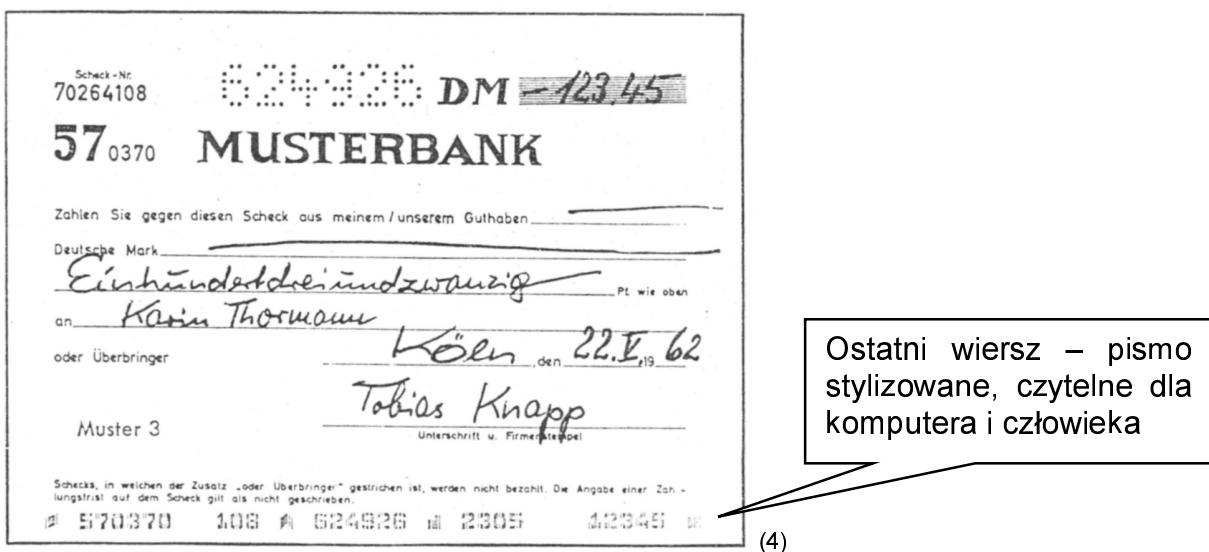
³ Słownik współczesnego języka polskiego str. 348

⁴ Peter Müller (red.): Leksykon informatyki, Warszawa 1977 str. 123

dla danego typu informacji¹. Język programowania, aby stał się zrozumiały dla komputera musi zostać przetłumaczony na język komputera, a o tym decyduje format zapisu. Postacią charakterystyczną dla języka komputera najczęściej jest postać dwumetryczna².

Czy należy zatem podzielić stanowisko tej części doktryny, dla której dokumentem w rozumieniu prawa procesowego jest również wydruk zawartości pamięci, czyli wydruk źródłowy? Jego treść wyrażona jest wówczas w pewnych symbolach kodu technicznego lub innych znakach umownych używanych w operacjach komputerowych³. Moim zdaniem tak, jeśli chodzi o wydruk. Wyeksponowanie na papierze zawartości elektronicznego nośnika danych nie jest bardziej zakodowane niż tekst napisany np. ideogramem, a może nawet jest bardziej jednoznaczny (zupełnie inną kwestią jest, że finalnie możemy otrzymać dokument np. w języku obcym).

Istnieją pewne kompromisowe techniki zapisywania danych elektronicznych np. pismo magnetyczne (stylizowane) czytelne równocześnie dla człowieka i komputera. Dochodzi tu do pewnego paradoksu, bo niewątpliwie mamy tekst zapisany pismem alfabetycznym, ale w postaci np. ciągu cyfr, z których nic bezpośrednio nie wynika (tak, jak np. nr PESEL). Mimo, że tekst jest bezpośrednio dostępny, jest w istocie zakodowany i jego odczytanie wymaga pośrednictwa urządzeń technicznych.



¹ Elżbieta Sobol (red.): Słownik wyrazów obcych, Warszawa 1995 str. 355

² Leksykon informatyki str. 123

³ Tak np. A. Murzynowski *op.cit.*

⁴ Przykład pochodzi z Leksykonu informatyki *ibidem*

O wiele trudniej uzasadnić pisemność dokumentu zapisanego na elektronicznym noźniku danych. O ile można w tym przypadku mówić o znaku językowym, trudno mówić o znaku graficznym. Należałoby w zasadzie w drodze wykładni rozszerzającej definicją pisma objąć translację danych, tzn. transpozycję języka pisanej/mówionej na język komputerowy. Dane utrwalone na elektronicznym noźniku danych, podobnie jak pismo ludzkie, reprezentowane są przez określone, jednoznaczne, znaki umowne jak impulsy, cechy magnetyczne czy optyczne. Mają one określone znaczenie w danym języku – języku komputerowym.

Uzasadnienie semantyczne jakiegoś zjawiska nie posiada kluczowego znaczenia dla życia prawnego. Prawo wymaga przede wszystkim, aby obiekt realizował pewne przypisane mu funkcje, posiadał pewne cechy, w oparciu o które uzyskał on konkretne znaczenie prawne np. moc dowodową. Dokument elektroniczny poza przypadkowością zbiegu nazwy z dokumentem tradycyjnym i tym samym obszarem zastosowania bardziej różni się od stricte dokumentu niż jest do niego podobny. Stąd uzasadnione są obawy, jakie rodzi jego ewentualne stosowanie w procesie na równi z dokumentem tradycyjnym.

4. NOŚNIK OŚWIADCZENIA WOLI.

Podłoże, na którym dotychczas utrwalano treść oświadczeń posiada tę charakterystyczną cechę, że umożliwia w prosty sposób transpozycję języka mówionego na język pisany tj. wyrażony za pomocą językowych znaków graficznych. Zastosowanie papieru do archiwizowania dokumentów ma szereg walorów głównie w obszarze zachowania jego integralności i autentyczności. Słabą stroną jest mała bezwładność informacji zawartej na kartce papieru, co jest rezultatem fizycznego istnienia podłożu, na którym myśl została utrwalona.

Obecnie brak raczej wątpliwości, co materialnoprawnego znaczenia informacji zapisanej na elektronicznym noźniku danych, o wiele gorzej jest z mocą dowodową takich „dokumentów”.

Polski ustawodawca nie zaskakuje jednolitością terminologiczną, a tym bardziej precyzją sformułowań. Art. 7 PrBank mówi o „*elektronicznych noźnikach informacji*”, UoP-P o „*noźniku elektronicznym*”, instrukcja kancelaryjna dla organów samorządowych województwa o „*elektronicznym noźniku*

informatycznym”, definiowanym przez wyliczenie, jakkolwiek trudno dopatrzyć się tu wspólnego kryterium klasyfikacji¹. Zupełnie inaczej prawo i doktryna niemiecka, posługuje się jednoznacznym pojęciem „nośnika danych” (*Datenträger*), ewentualnie z przymiotnikiem „cyfrowy” (co jest pojęciem węższym od „elektroniczny”). Już samo uporanie się z problemami terminologicznymi rodzić może wiele trudności.

Jest pewną cechą charakterystyczną dla języka polskiego piętnowanie nowych zjawisk przymiotnikiem „elektroniczny”, „informatyczny”, „informacyjny”, etc. Pojęcia te nie są równoznaczne, a poza tym wydaje mi się, iż zupełnie wystarczające jest korzystanie z pojęcia „nośnik danych” (ewentualnie z przymiotnikiem „elektroniczny”). Co prawda tak szerokie ujęcie obejmuje każde podłoże zdącone do przyjęcia informacji, jednakże z uwagi, że do tej pory był to głównie papier, używanie określenia „nośnik danych” sugeruje (sam przez siebie), że chodzi o inne niż papierowe podłoże. Trzeba również zauważać, że niecelowe jest swobodne posługiwanie się pojęciami „nośnik danych” i „nośnik informacji”, nie są to bowiem synonimy.

Nośnik informacji (*Informationsträger*) to znak umowny lub nieumowny² (...), któremu przypisane jest pewne brzmienie, wtórnie znak graficzny, punkt magnetyczny, impuls, etc.³. Natomiast **nośniakiem danych** jest każdy materiał, na którym mogą być zapisane i przechowywane dane, a w razie potrzeby odtwarzane w niezmienionej postaci.

Z powyższych definicji wynika, że to, co nas tak naprawdę interesuje to nie nośnik informacji, lecz nośnik danych, to, co niemiecka doktryna trafnie nazywa „*Datenträger*”. Dochodzimy więc do pewnej subtelności. Otóż, art. 7 PrBank nie mówi w zasadzie o „podłożu”, na którym ma zostać utrwalona pewna treść, lecz o samym sposobie naniesienia danych na określone podłoże (jakiekolwiek). Wniosek taki wynika z językowej wykładni art. 7 „(...) **za** pomocą elektronicznych nośników informacji (...)”, a nie „**na** elektronicznych nośnikach informatycznych”. Zupełnie inaczej art. 5 ust. 1 UoP-P, gdzie wyraźnie jest mowa o „*zapisie na*”.

¹ Załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 1998 r. Dz. U. 1073(R)/160/1998; **art. 3 pkt 24** „nośnik informatyczny - dyskietkę, taśmę magnetyczną lub inny nośnik, na którym zapisano w formie elektronicznej treść dokumentu, pisma itp.,”

² Literatura i nauka o języku str. 857

³ Leksykon informatyki str. 253

A zatem w pierwszym przypadku wskazuje się na nośnik informacji, w drugim na nośnik danych.

Trudno rozstrzygnąć, czy te rozbieżności są rezultatem przypadku, czy wręcz przeciwnie zamierzeniem zupełnie przemyślanym. Z dwojga, przyjmując drugie założenie, właściwsze wydaje się podejście pierwsze. Art. 7 sugeruje bowiem, że chodzi o dane zapisane w języku komputerowym, co nie wynika z art. 5 UoP-P. W rezultacie uwolniono pojęcie „dokumentu elektronicznego” od relatywizacji do jakiegokolwiek nośnika danych.

Natomiast całkowitą pomyłką jest definicja „*elektronicznego nośnika informatycznego*”. Z definiendum wynika bowiem, że chodzi o nośnik danych, definiens zaś nasuwać może skojarzenia z nośnikiem informacji. Wydaje się, że chodziło o bardzo precyzyjne i wąskie określenie nośnika (elektroniczny i informatyczny zarazem), w rezultacie pojawia się jednak mnóstwo wątpliwości.

W zasadzie każdy nośnik danych jest dla tych danych pamięcią (wszystkie rodzaje środków zapamiętujących, które zachowują informacje przez dowolnie długie okres czasu i w razie potrzeby mogą informacje te udostępniać w niezmienionej postaci).

W praktyce jednak wyróżnia się pamięci (nośniki danych *sensu largo*):

- jednorazowego zapisu (*nicht überschreibbaren Datenträger*)
- wielokrotnego zapisu (*überschreibbaren Datenträger*)

oraz nośniki danych (nośniki danych *sensu stricto*):

- dziurkowane
- dokumenty ze znakami kreskowymi
- dokumenty czytelne dla człowieka

Podział nośników danych na jednorazowego i wielorazowego zapisu ma znaczenie szczególnie doniosłe dla zachowania integralności dokumentu zisanego na elektronicznym nośniku danych.

Jeżeli dokument utrwalony został na jednej kartce papieru, nie ma trudności z zachowaniem jego integralności. Wystarczy, co do zasady, złożenie podpisu pod treścią dokumentu. Jeżeli treść oświadczenia nie mieści się na jednym arkuszu stosuje się inne zabiegi techniczne mające na celu zachowanie autonomiczności wszystkich części dokumentu np. zszycie i ponumerowanie arkuszy, zachowanie ciągłości tekstu przez przenoszenie zdań na stronę następną, w przypadku aktów

notarialnych parafowanie każdego arkusza osobno¹, etc. Jeżeli w treści dokumentu znajduje się odesłanie do innego dokumentu, powinien on być z reguły fizycznie połączony z tym dokumentem lub wskazany jako załącznik, stanowiący integralną część zasadniczego dokumentu².

Dokument zapisany na elektronicznym nośniku danych ma zupełnie inny charakter. Fizyczny podział dokumentu np. na strony nie istnieje, ma on wyłącznie na celu zilustrowanie wydruku dokumentu i w pewnym zakresie ułatwić poruszanie się po samym dokumencie. Elektroniczny nośnik danych ma o wiele większą pojemność od pojedynczej kartki papieru, w rezultacie przechowywać może dokumenty składające się z wielu arkuszy, czy też wiele, różnych, dokumentów. Z uwagi na specyfikę zapisu pojawiają się obawy o zachowanie tożsamości dokumentu. Zachowaniu integralności służyć ma przede wszystkim stosowanie podpisu cyfrowego. W rzeczywistości podpis cyfrowy nie gwarantuje, że nie będzie można zmienić treści dokumentu, a jedynie, że zmiana taka nie będzie niezauważalna.

Problem integralności dokumentu elektronicznego nie zachodzi, jeżeli dokument utrwalony został na nośniku jednorazowego zapisu. Integralność tkwi, więc w pewnej cesze charakterystycznej samego nośnika a nie dokumentu. Dla dokumentu tradycyjnego integralność była rezultatem pewnej symbiozy pomiędzy podłożem a własnoręcznym podpisem. W obrocie elektronicznym oba te aspekty funkcjonować mogą niezależnie. Dokument podpisany cyfrowo zachowuje swoją integralność niezależnie od nośnika, na którym go zapisano. Dokument nie podpisany cyfrowo, ale utrwalony na nośniku jednorazowego zapisu, np. CD-R, pośrednio gwarantuje swoją integralność. Obiektywnie bowiem nie można niczego na tym nośniku zmienić. Dokument może jednak zostać skopiowany np. na dysk twardy komputera, tak zapisane dane nie gwarantują już autonomiczności.

Dokument zapisany na elektronicznym nośniku danych nie tylko zajmuje mniej miejsca, łatwiej uaktualniać jego treść, czy doręczyć go adresatowi³. Ma on jednak szereg cech, które utrudniają jego stosowanie w kontekście dokumentu tradycyjnego. Jego odczytanie wymaga zaangażowania urządzeń technicznych, co prawda można go transportować, np. jako faks, ale wówczas nie sposób go

¹ Art. 93 ustawy „Prawo o notariacie” Dz. U. 153/22/1991; „Jeżeli akt notarialny jest sporządzony na dwóch lub więcej arkuszach, to arkusze te powinny być ponumerowane, parafowane i połączone”

² Stanisław Dmowski, Stanisław Rudnicki *op.cit.* str. 256

³ Andrzej M. Wilk *op.cit.*

podpisać cyfrowo. Faks nie jest również traktowany jako dowód w rozumieniu KPC. Bardzo poważnym problemem jest określenie, co jest kopią, a co oryginałem dokumentu zapisanego na elektronicznym nośniku danych. Jest to problem o wiele bardziej doniosły niż dla dokumentów papierowych.

1. KRYPTOGRAFIA I PODPIS ELEKTRONICZNY - ASPEKTY TECHNICZNE.

„**Kryptologia** jest dziedziną wiedzy obejmującą zagadnienia związane z ukrywaniem wiadomości (danych) przed podmiotami nieupoważnionymi przy pomocy ich przekształcenia (**szyfrowania**) do postaci wiadomości „niezrozumiałych” i ich odtwarzaniem (**deszyfrowaniem**) przez podmioty upoważnione (**kryptografia**) lub nieupoważnione (**kryptoanaliza**)”.¹

Do niedawna, ze względów militarnych oraz potrzeb bezpieczeństwa publicznego i prawnego, programy kryptograficzne objęte były zakazem eksportu. W efekcie wersje eksportowe znanych programów komunikacyjnych pozbawiano pewnych komponentów w stosunku do ich narodowych odpowiedników. Obecnie z uwagi na zjawisko globalizacji obrotu, elektronicznego przetwarzania wszelkich danych i związane z tym potrzeby jak i niebezpieczeństwa, co raz częściej nowoczesna kryptografia angażowana jest dla potrzeb cywilnych, a programy zapewniające bezpieczną komunikację znaleźć można w komercyjnych aplikacjach.

Dzięki nowoczesnym metodom kryptografii możliwe jest:

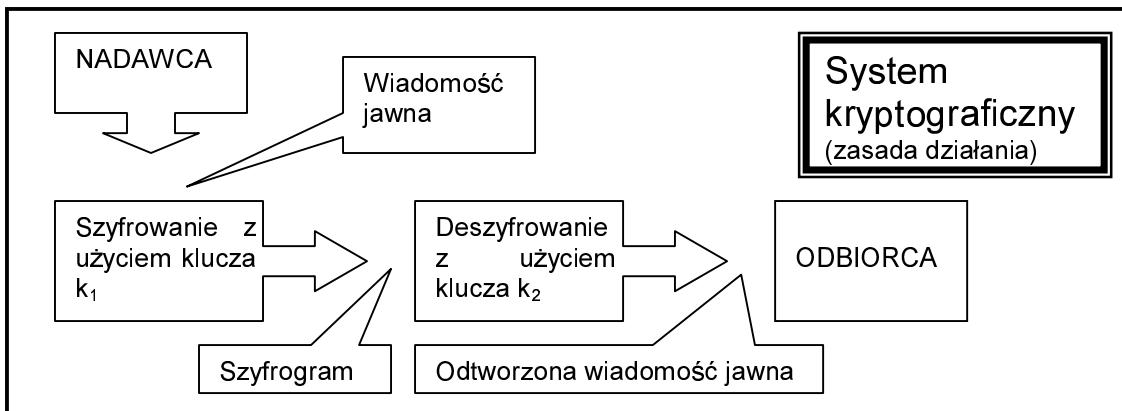
- bezpieczne szyfrowanie wiadomości
- jednoznaczne zidentyfikowanie nadawcy wiadomości
- zapewnienie integralności wiadomości

Wiadomość, którą poddajemy szyfrowaniu nosi nazwę **wiadomości jawnnej**. Po zaszyfrowaniu przybiera postać tzw. **szyfrogramu** tj. wiadomości zaszyfrowanej. Proces szyfrowania i deszyfrowania uzależniony jest od odpowiednich przekształceń matematycznych, które nazywamy **algorytmem kryptograficznym**.

¹ Cytowane materiały pochodzą ze strony: <http://www.centrum.pl/pl/index.html>

Zazwyczaj sama formuła algorytmu jest powszechnie znana, a o jego skuteczności decyduje dodatkowy parametr przekształcenia (klucz), znany jedynie podmiotom upoważnionym.

System, w którym dokonuje się szyfrowania i deszyfrowania wiadomości nosi nazwę **systemu kryptograficznego** – zasadę jego działania przedstawia schemat.



Upraszczając dokonać można dychotomicznego podziału metod kryptograficznych na:

- 1) metody symetryczne
- 2) metody asymetryczne

W praktyce raczej nie stosuje się żadnej z tych metod w czystej postaci, lecz w celu poprawy bezpieczeństwa, łączy się elementy każdej z nich.

W kriptografii technologicznie bardzo zaawansowanej dodaje się elementy stanowiące biologiczne cechy indywidualizujące człowieka (np. linie papilarne), a metody wykorzystujące takie dane nazywamy **metodami biometrycznymi**.

Ad. 1

Kriptografia oparta na metodzie **kluczy symetrycznych** (Private Key) nie jest rozwiązaniem nowym, znana była od wielu wieków i do połowy lat siedemdziesiątych minionego stulecia była w zasadzie metodą jedyną. Zakłada ona, że istnieje jeden tajny klucz, który służy zarówno do szyfrowania jak i

rozszyfrowania wiadomości, jest więc on wspólny dla nadawcy i odbiorcy. Zaletą tej metody jest niewątpliwie jej szybkość i odporność na „łamanie”, z drugiej strony ma ona pewne mankamenty, zwłaszcza konieczność przekazania odbiorcy kopii klucza prywatnego. Jest więc ona efektywna dopóty klucz pozostaje tajny, poza tym nigdy nie daje pewności, że wiadomość faktycznie pochodzi od konkretnej osoby (weryfikacja opiera się w gruncie rzeczy na założeniu, że klucz znają tylko nadawca i odbiorca, a więc podmioty upoważnione). Posiada ona również pewne ograniczenie koncepcyjne – skoro bowiem mamy jeden tajny klucz stosować ją można w stosunkach relatywnie wąskiej grupy podmiotów, najlepiej w stosunkach bilateralnych (w innym przypadku wypatrzona zostaje sama jej idea).

W metodzie symetrycznej zazwyczaj zastosowanie znajduje algorytm **DES** (Data Encryption Standard).

Ad. 2

Metoda asymetryczna oparta jest na matematycznej zależności, zgodnie z którą, o ile relatywnie łatwo jest obliczyć iloczyn dwóch liczb pierwszych (nawet dużych), o tyle nie sposób w drodze matematycznej analizy znanego iloczynu dwóch nieznanych liczb pierwszych szybko rozłożyć na czynniki.

Metoda kluczy niesymetrycznych zakłada istnienie pary kluczy komplementarnych – klucza prywatnego i publicznego. Każda wiadomość zaszyfrowana przy pomocy klucza prywatnego może zostać rozszыfrowana tylko przy pomocy odpowiadającego mu klucza publicznego – proces ten jest **przemienny** tzn. można go przeprowadzić w drugą stronę, nie jest natomiast procesem **symetrycznym** tzn. klucza użytego do zaszyfrowania informacji nie można użyć do jej rozszycowania (metoda ta opiera się na algorytmie **RSA** (Rivest, Shamir, Adleman) opracowanym w Massachusetts Institute of Technology).

Newralgicznymi momentami metody asymetrycznej, od których uzależniona jest jej późniejsza efektywność, są:

- **generowanie liczby**, z której wydzielone zostaną klucze. Jest to pierwszy etap powstawania kluczy i od jego prawidłowego przebiegu zależy ich niepowtarzalność. Każdy z kluczy realizuje inną funkcję jednak oba tworzą niepowtarzalną całość.

- **przechowywanie kluczy**, w metodzie symetrycznej pojawiała się problem zaufania do kontrahenta, co ostatecznie owocowało koniecznością posiadania wielu kluczy. W metodzie asymetrycznej problem dotyczy tylko bezpiecznego przechowywania klucza prywatnego, nie sposób bowiem odtworzyć go z klucza publicznego (mówiąc zupełnie teoretycznie możliwość taka istnieje, ale jest to tzw. problem trudny obliczeniowo).
- **matematyczna weryfikacja podpisu elektronicznego**, jest to słaba strona tej metody – bardzo czasochłonna.

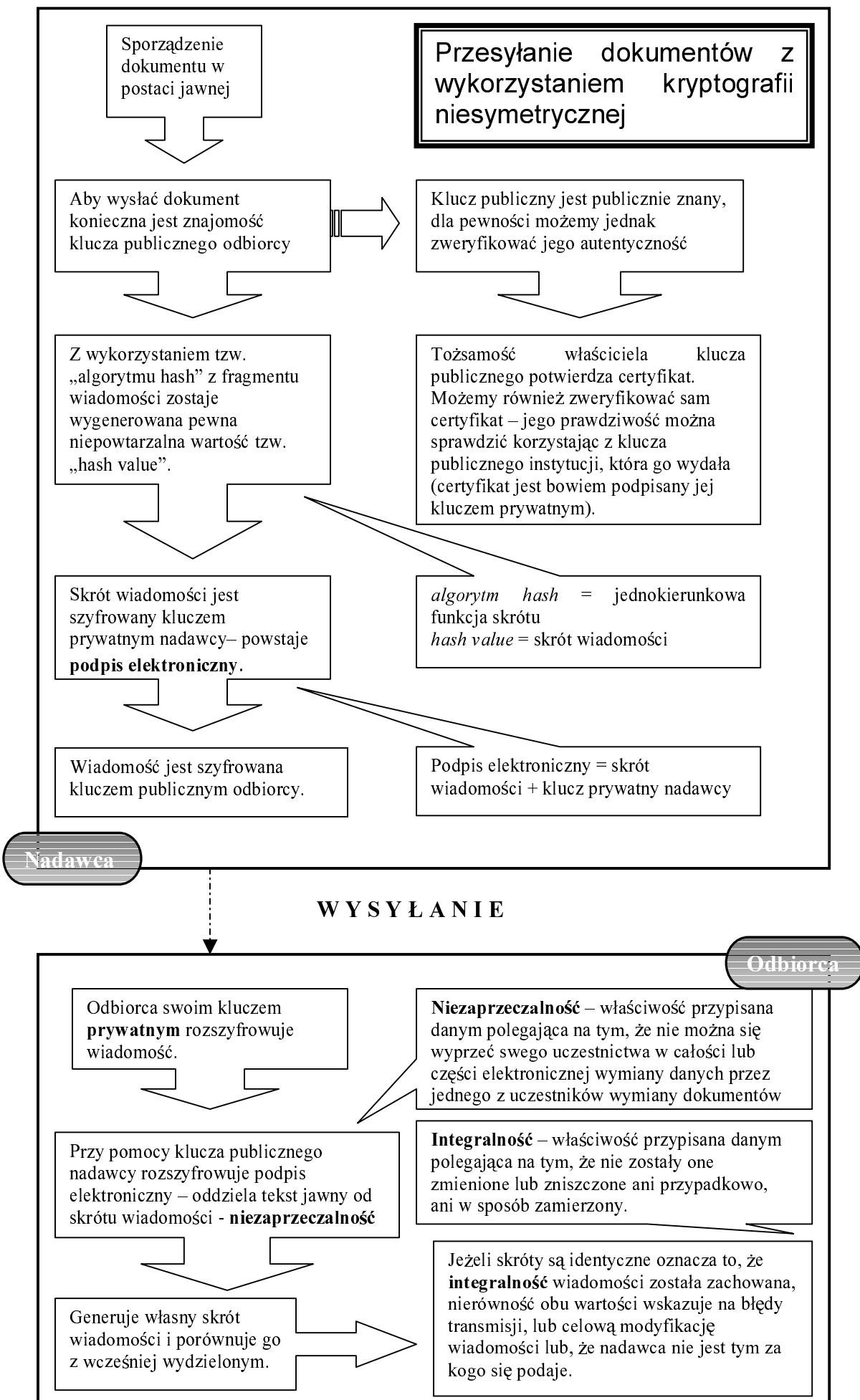
Klucz prywatny jest tajny, klucz publiczny jest jawnym i potencjalnie dla każdego dostępny¹. Z jawności klucza publicznego nie wynikają jednak żadne niebezpieczeństwa. Jeżeli bowiem nadawca zaszyfruje wiadomość kluczem publicznym adresata, to jedyną osobą, która może ją odczytać jest sam adresat, gdyż tylko on zna klucz prywatny niezbędny do rozszyfrowania tak zakodowanej wiadomości, użycie klucza publicznego do rozszyfrowania wiadomości będzie bezskuteczne. W zależności od kolejności zastosowania kluczy można zapewnić albo **poufność** albo **autentyczność** wiadomości. Aby osiągnąć oba te cele równocześnie konieczne jest zastosowanie dwóch par kluczy tj. nadawcy i odbiorcy (patrz schemat).

Powszechna dostępność do klucza publicznego nie rodzi również niebezpieczeństw podszycia się (tzw. maskarada) pod użytkownika komplementarnego klucza prywatnego, ponieważ klucz publiczny realizuje wyłącznie jeden z dwóch celów:

- zaszyfrowania wiadomości do użytkownika klucza prywatnego (poufność)
- odszyfrowania wiadomości zaszyfrowanej kluczem prywatnym (autentyczność)

Nie można również przy pomocy klucza publicznego rozszyfrować żadnej wiadomości przeznaczonej dla właściciela klucza.

¹ klucz ten jest **publicznie znany**, co niekoniecznie oznaczać musi, że jest **ogólnie dostępny**, może być bowiem dostępny jedynie dla pewnej grupy podmiotów.



W tej metodzie w ogóle nie występuje problem bezpiecznego przekazania klucza prywatnego adresatowi, co jest niekwestionowaną zaletą. Metoda ta jest jednak bardzo skomplikowana i w efekcie mało wydajna. Ideę funkcjonowania metody asymetrycznej ilustruje zamieszczony powyżej schemat.

Istnieje możliwość łączenia powyższych metod. W przypadku komunikacji *online*, do zestawienia połączenia wykorzystuje się metodę niesymetryczną, gdzie przesyła się tzw. **klucz sesyjny** (jednorazowy dla danej sesji). Następnie wykorzystuje się go do szyfrowania dalszej transmisji, już z zastosowaniem metody symetrycznej. Dzięki takiej kombinacji rozwiązano zarówno problem szybkości transmisji, jak i bezpiecznego przekazania klucza.

Skuteczność każdej metody kryptograficznej relatywizowana jest nie tylko długością zastosowanego klucza ale również bezpiecznym jego przechowywaniem. Rozwiązaniem obecnie już nieco archaicznym jest umieszczanie klucza względnie jego fragmentu na dyskietce (tak np. polskie wdrożenia IKP dla ZUS), jednak obecnie standartem raczej jest przechowywanie klucza na chipkarcie (w takim przypadku komputer musi posiadać odpowiedni interfejs – przykłady prezentuje poniższe zdjęcie). Dodatkowo sama karta zabezpieczona jest przed niepożądanym użyciem przez osobę trzecią numerem PIN lub hasłem. Skorzystanie z takiej karty, a w zasadzie klucza, wymaga zestawienia dwóch elementów: „wiedzy” i „posiadania”.

Idea podpisu elektronicznego wiąże się w swojej najbardziej rozpowszechnionej postaci z wykorzystaniem tzw.

jednokierunkowej funkcji skrótu¹.

Funkcja skrótu spełnia rolę podobną do odcisku palca i umożliwia powiązanie wiadomości o dowolnej długości z charakterystyczną dla tej wiadomości liczbą – **skrótem wiadomości**.



¹ jednokierunkowość funkcji skrótu polega na tym, że o ile łatwo powinno dać się obliczyć skrót wiadomości o tyle problemem trudnym obliczeniowo powinna być operacja odwrotna. Jednokierunkowość oznacza również, że problemem trudnym obliczeniowo powinno być wyznaczenie dwóch wiadomości o jednakowej wartości funkcji skrótu tj. skrótu wiadomości.

Mimo, że obecnie funkcjonują już praktyczne wdrożenia IKP (Infrastruktury Klucza Publicznego) nie są one rozwiązaniami ujednoliconymi które regułowała by międzynarodowa norma (różnice dotyczą również regulacji prawnej, zwłaszcza w Polsce, gdzie z jednej strony brak ustawy o podpisie cyfrowym z drugiej powstają wdrożenia IKP z reguły na wewnętrzny użytku różnych instytucji, co destabilizuje to spójność systemu prawa). Droga ku unifikacji jest jeszcze bardzo daleka, społeczność międzynarodowa nie pozostaje jednak bierna przykładem są prace Komisji Narodów Zjednoczonych ds. Międzynarodowego Prawa Handlowego (UNCITRAL)¹ nad modelowym prawem o podpisie elektronicznym. Powstają również kompletne systemy sygnatury digitalnej np. PGP (Pretty Good Privacy).

W ostatecznym rozrachunku sygnatura digitalna oferuje jednak większe bezpieczeństwo i pewność obrotu aniżeli czynił to podpis własnoręczny. Dotyczy to zwłaszcza:

- ochrony integralności dokumentu przed późniejszymi zmianami
- potwierdzona zostaje tożsamość nadawcy (pośrednio, ale w sposób wystarczający)
- powstaje niezaprzeczalny związek między dokumentem a podpisem
- proces zweryfikowania podpisu jest całkowicie zautomatyzowany (taka koncepcja podpisu w powiązaniu z systemem certyfikacji daje pewność tożsamości nadawcy na poziomie zbliżonym do ekspertyzy grafologicznej)

Zaangażowanie nowoczesnej techniki dla potrzeb obrotu prawnego rodzi dodatkowe pytania i niebezpieczeństwa. Wiele obaw dotyczy m.in. krótkiej żywotności współczesnych systemów operacyjnych, chodzi bowiem o to czy za lat np. dziesięć archiwizowane będą dokumenty powstałe obecnie, czy obecnie skuteczne metody kryptograficzne będą efektywnie chronić dowody z przeszłości (aż trudno sobie wyobrazić chaos jaki wywołać mogły by fikcyjne reprodukcje testamentów, rachunków, wpisów w księgach wieczystych, etc.), jak długa jest żywotność elektronicznych nośników informacji, etc. Innymi słowy pojawia się

¹ <http://www.un.or.at/uncitral/mainindx.htm>

pytanie, czy przewidzieliśmy wszystkie konsekwencje wdrożenia tak zaawansowanej technologii, która zmienia nasz świat i cywilizację, czy nie czekają nas w przyszłości niespodzianki przy których problem roku 2000 był nie wartym rozgłosu epizodem. Błędy mogą okazać się nieodwracalne.

2. PODPIS ELEKTRONICZNY - EWOLUCJA I ZAKRES POJĘCIA

Jednym z bodajże najistotniejszych problemów powstających w zakresie zagadnienia formy elektronicznej jest podpis, ściślej podpis cyfrowy¹ otwierający bramy legalnego obrotu, wywołujący zamierzone konsekwencje prawne. Już na gruncie rozważań powyższych zauważać można, że w zasadzie niewiele łączy podpis elektroniczny z podpisem w tradycyjnym ujęciu. Trzeba wyraźnie zaznaczyć, że legalizacja podpisu elektronicznego nie zmierza wcale do przypisania mu atrybutów podpisu własnoręcznego². Z przyczyn obiektywnych podpis elektroniczny nigdy nie będzie w stanie ich zrealizować, chodzi tylko o przypisanie mu prawnej doniosłości podpisu własnoręcznego. Aby było to możliwe podpis elektroniczny musi realizować przynajmniej te same funkcje, co podpis własnoręczny i w zbliżonym do niego zakresie. W rzeczywistości zakres realizowanych przez ten pierwszy funkcji jest o wiele szerszy (co niekoniecznie oznacza, że lepszy). To jednak nie wszystko, bardzo istotny element, z reguły jednakże w literaturze pomijany, dotyczy przeżyć psychicznych podmiotu prawa uwiklanego w stosunek prawnego. Nie ulega bowiem wątpliwości, że o ile składaniu podpisu własnoręcznego towarzyszy przeżycie emocjonalne, o tyle podpis elektroniczny jest pod tym względem jego niedoskonałym substytutem. Aczkolwiek spotkać można w literaturze, trafne skądinąd, stanowisko zgodnie, z którym we współczesnym obrocie masowym także podpis własnoręczny nie chroni w sposób wystarczający przed pochopnym podejmowaniem decyzji. Nie można więc

¹Patrz szerzej Krzysztof Stefanowicz: Podpis elektroniczny, „Biznes Polska”, 25.01.2001 <http://www.biznespolska.pl/>

²Rządowy projekt ustawy o podpisie elektronicznym z 21.12.2000 w art. 1 stanowi: „Ustawa tworzy warunki prawne do stosowania w obrocie prawnym podpisu elektronicznego jako równorzędnego podpisowi własnoręcznemu”

wykluczyć, że z czasem to właśnie podpis cyfrowy będzie bardziej efektywnie realizował swoje funkcje, przy czym, jeżeli oczywiście do tego dojdzie, będzie to raczej rezultatem np. odpowiednio zaprojektowanego interfejsu użytkownika, niż jego psychicznego przeżycia. Wynika to z posługiwania się w obrocie środkiem technicznym, który stanowi swego rodzaju komunikacyjny bufor. Równocześnie zastosowanie urządzeń technicznych bardzo przyśpiesza i upraszcza obrót, co z kolei decyduje o pochopnym, a często nieświadomym podejmowaniu decyzji i towarzyszącym im konsekwencjom. Wskazane wyżej okoliczności mają rzecz jasna odniesienie wyłącznie od obrotu komercyjnego. W elektronicznym obrocie profesjonalnym z reguły po obu stronach stosunku występują podmioty mające status osoby prawnej, a tu o wiele słabsze jest poczucie własnej tożsamości. To samo dotyczy podpisu. Osoba prawa działa bowiem przez swoje organy, których personalna obsada może ulegać zmianie.

Podpis elektroniczny posiada wszakże wiele cech jednoznacznie pozytywnych. Na przykład, jak wynika z treści art. 79 i 80 KC podmiot prawa posiadający pełną zdolność do czynności prawnych może być w pewnym zakresie upośledzony. Ze względu na pewne jego cechy personalne ustawodawca nakłada na niego dalej idące wymagania w zakresie formy, niż na inne osoby, które owych personalnych cech nie posiadają. Forma elektroniczna i sygnatura digitalna mogą skutecznie znieść te ograniczenia, ponieważ multimedialne możliwości współczesnych komputerów pozwalają np. na dźwiękowe prezentowanie zapisanych w dokumencie treści, zaś procedura złożenia elektronicznego podpisu może nie wymagać umiejętności pisania.

Pierwsze regulacje prawne poświęcone elektronicznemu podpisowi powstały w Stanach Zjednoczonych (pierwszym takim aktem na świecie był *Utah Digital Signature Act* przyjęty w 1995r¹). Na kontynencie najszybciej na zmieniającą się rzeczywistość zareagowali Niemcy, tam też przyjęte rozwiązania stanowić będą bazę do dalszych rozważań.

Jest rzeczą oczywistą, że podpis elektroniczny w żadnym razie nie może być prostym graficznym przedstawieniem obrazu podpisu własnoręcznego, byłby bowiem zbyt łatwy do podrobienia – w rezultacie nieefektywny.

¹ Został on dość szybko zmieniony, wskazano, że wdrożenie podpisów cyfrowych wymaga przede wszystkim wyjaśnienia podstawowych pojęć: „podpis cyfrowy”, „organ certyfikacyjny”, „certyfikat”. Ich brak dość szybko doprowadzić może do chaosu terminologiczno – prawnego. Szerzej: Jerzy Jacyszyn *op.cit.*

Art. 3 (Gesetz zur Digitalen Signatur – Signaturgesetz – SigG) ustawy o usługach informacyjnych i telekomunikacyjnych z 13 czerwca 1997 poświęcono zagadnieniom związanym z podpisem elektronicznym¹. Celem ustawodawcy było zrealizowanie dwóch funkcji:

- 1) wprowadzenia regulacji dotyczącej elektronicznego składania oświadczeń woli i zawierania na ich podstawie umów.
- 2) spełnienie postulatów zmierzających w tym kierunku, aby w przypadku procesu sądowego także posługując się dokumentem elektronicznym z elektronicznym podpisem możliwe było uzyskanie tych samych korzyści dowodowych, jakie daje dokument pisemny².

Niemiecka ustanowia reguluje wyłącznie problematykę podpisu elektronicznego *sensu stricto* tj. pomijając zupełnie aspekty kryptograficzne³, co zgodne jest w zasadzie ze stanowiskiem Komisji Europejskiej – wprowadza ścisłe rozróżnienie pomiędzy podpisem cyfrowym tj. usługą, która zapewnia autentyczność i integralność danych, a kodowaniem tj. usługą, która zapewnia poufność danych⁴.

Wbrew ogólnie panującej opinii pojęcia „podpis cyfrowy” i podpis elektroniczny nie są równoznaczne. Pojęcie „podpis elektroniczny” jest pojęciem szerszym (podpis cyfrowy jest jednym z możliwych podpisów elektronicznych).

Na tę subtelną różnicę zwraca uwagę Dyrektywa o podpisie elektronicznym Komisji Unii Europejskiej (Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen (RL) vom 13.5.1998).

Postanowienia dyrektywy koncentrują się w zasadzie na podpisie cyfrowym, w wyjaśnieniach wskazuje się jednak, że Komisja rozszerza ich zakres na podpis elektroniczny⁵. Dyrektywa wyjaśnia, że podpis elektroniczny to cyfrowa sygnatura zawarta w danych do danych, dodana lub logicznie z nimi powiązana, użyty przez

¹ Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienstes-Gesetz - IuKDG)

² Janusz Barta, Ryszard Markiewicz *ibidem*

³ Te i inne problemy reguluje Verordnung zur digitalen Signatur (Signaturverordnung – SigV) z 8.10.1997r.

⁴ Ensuring Security and Trust in Electronic Communication: towards a European Framework for Digital Signatures and Encryption z 8.10.1997r.

⁵ Więcej Alexander Roßnagel: Elektronische Signaturen in Europa, MMR 12/98 str. 331

podpisującego (sygnatariusza) dla wskazania, że podpisujący potwierdza zawartość tych danych (Art.2 Abs.1 RL). Podpis elektroniczny spełniać powinien następujące wymagania:

- jest jednoznacznie powiązany z podpisującym
- identyfikuje podpisującego
- jest postawiony za pomocą takich środków, że podpisujący może mieć nad nim osobistą kontrolę
- jest powiązany z danymi w taki sposób, aby stwierdzić, że dane nie zostały zmienione

Dyrektyna nie wyjaśnia natomiast gdzie tkwi różnica pomiędzy jednym a drugim podpisem. Zdaniem niemieckiej doktryny podpis elektroniczny nie jest ograniczony wyłącznie do metody kryptograficznej (*Verschlüsselungsverfahren*) opartej na jawnym kluczu publicznym (ściślej – parze kluczy komplementarnych). „Podpis elektroniczny” otwiera więc bramy rozwoju i stosowania innych metod kryptograficznych.

Niemiecki SigG posługuje się pojęciem „podpis cyfrowy” (*digitalen Signatur*): **Podpis cyfrowy jest pieczęcią na danych postawioną za pomocą klucza prywatnego przez inicjatora informacji elektronicznej** (§2 Abs. 1). Pieczęć ta powinna być weryfikowalna za pomocą powiązanego z kluczem prywatnym klucza publicznego, do którego dołączono certyfikat wystawiony przez zaufaną osobę trzecią (licencjonowany wystawca certyfikatów). Tak złożony podpis zapewniać powinien autentyczność wiadomości i jej niezaprzeczalność¹. Wystawcą certyfikatu może być osoba fizyczna (*natürlichen Person*) lub prawa (*juristische Person*), która uzyskała licencję na wykonywanie czynności certyfikacyjnych. Również polski projekt ustawy o podpisie elektronicznym (UoP – P) zawiera jego legalną definicję (art. 4).

¹ „Eine digitale Signatur im Sinne dieses Gesetzes ist ein mit einem privaten Signaturschlüssel erzeugtes Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen öffentlichen Schlüssels, der mit einem Signaturschlüssel-Zertifikat einer Zertifizierungsstelle oder der Behörde nach § 3 versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt“.

Definicja zbudowana jest z trzech części:

- ust. 1** – zawiera definicję sensu stricto:

„*Podpisem elektronicznym są dane elektroniczne dołączone do innych danych elektronicznych lub logicznie z nimi powiązane w celu potwierdzenia tożsamości podpisującego*” (definiensem są dane elektroniczne)

- ust. 2** – wprowadza kwalifikowaną kategorię podpisu elektronicznego „**bezpieczny podpis elektroniczny**”

„*Bezpieczny podpis elektroniczny to taki, który spełnia następujące warunki:*

- 1)** *jest jednoznacznie związany z podpisującym,*
 - 2) umożliwia określenie tożsamości podpisującego,**
 - 3) jest tworzony przy użyciu urządzeń i informacji, nad którymi podmiot podpisujący posiada całkowitą i wyłączną kontrolę, oraz**
 - 4) jest powiązany z danymi, do których został dodany w taki sposób, że każda późniejsza zmiana tych danych jest możliwa do stwierdzenia,**
 - 5) jest oparty o kwalifikowany certyfikat, został wytworzony za pomocą bezpiecznych urządzeń i spełnia inne wymogi w zakresie zabezpieczeń określonych w ustawie i przepisach wydanych na jej podstawie.”**
- ust. 3** – traktuje o warunkach technicznych składania bezpiecznego podpisu¹.

„*Bezpieczny podpis elektroniczny powinien być składany za pomocą bezpiecznych urządzeń zapewniających co najmniej, aby:*

- 1) dane kreujące podpis elektroniczny i służące do jego składania:**
 - a) *były niepowtarzalne,*
 - b) *została zagwarantowana ich poufność ,*
 - c) *nie mogły być pozyskane przez osoby niepowołane,*
 - d) *były maksymalnie zabezpieczone przy zastosowaniu dostępnych technologii przed fałszerstwem,*
 - e) *były zabezpieczone przez uprawnionego do składania podpisu przed użyciem ze strony osób trzecich,*
- 2) nie zmieniały danych, które mają być opatrzone podpisem,**
- 3) dane, które mają być podpisane zostały przedstawione podpisującemu, przed procesem składania podpisu.”**

¹ Pierwotnie chodziło o każdy podpis, a nie tylko jego postać kwalifikowaną

Bardzo precyzyjną (od strony technicznej) definicję podpisu zawiera przyjęty przez Radę Ministrów 6.02.2001 projekt ustawy o podpisie elektronicznym (UoP-Rz). „*Podpisem elektronicznym są dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację osoby fizycznej składającej podpis, oraz spełniają następujące wymogi (...)*”. W istocie podpis elektroniczny, jego „treść” bezpośrednio uzależniona jest „treści” dokumentu, na którym został on „złożony”. Oświadczenie woli utrwalone na nośniku elektronicznym spełnia wymagania formy pisemnej pod warunkiem, że treść tego oświadczenia potwierdzona została bezpiecznym podpisem (art. 5 ust. 1 UoP – P). Nie wyjaśniono jednak czy chodzi o zachowanie każdej formy pisemnej czy wyłącznie formy pisemnej zwykłej. Precyzyjnie i bardzo szeroko normuje skutki prawne podpisu elektronicznego UoP-Rz. Jeżeli na dokumencie elektronicznym został postawiony podpis elektroniczny weryfikowalny na podstawie kwalifikowanego certyfikatu, ma on takie same znaczenie w obrocie prawnym jak dokument sygnowany własnoręcznym podpisem. Co więcej tak sporządzony dokument czyni również zadość wymaganiom formy pisemnej zastrzeżonej *ad solemnitatem* (art. 5 ust. 2). W zakresie nie uregulowanym przez UoP-Rz stosuje się odpowiednio przepisy regulujące skutki prawne podpisu własnoręcznego.

Podpis elektroniczny wykracza więc poza tradycyjne funkcje podpisu o integralność sygnowanego nim tekstu. Poza tym nie jest on znakiem graficznym (ciągiem znaków), lecz ciągiem bitów pośrednio identyfikujących daną osobę. Podpis własnoręczny zawiera w charakterze pisma ścisłe określone cech podpisującego¹. W znaczeniu powszechnie używanym podpis to napisany lub uwierzytelniony znak ręczny (odcisk palca)².

Złożenie podpisu elektronicznego opiera się również o pewien schemat postępowania, cykl uporządkowanych, następujących po sobie czynności. Jest czynnością konwencjonalną³. Nie każde złożenie podpisu własnoręcznego będzie czynnością prawną. Skutki wymagają oceny pod kątem kontekstu, okoliczności,

¹ Filip Rosengarten *op.cit.*

² Postanowienie SN z dnia 17.04.1967, II PZ 22/67, (niepublikowane)

³ Złożenie podpisu jest prostszą czynnością konwencjonalną, której na mocy pewnych wyraźnie ustanowionych lub zwyczajowo ukształtowanych reguł prawnych nadaje się nowy sens społeczny, Sławomira Wronkowska, Zygmunt Ziembicki: Zarys teorii prawa, Poznań 1997

które towarzyszą złożeniu podpisu. Własnoręczne złożony autograf jest podpisem w ścisłym znaczeniu. Nie wywołuje on jednak żadnych skutków prawnych, bo jego złożeniu nie towarzyszyła odpowiednio ukierunkowana wola podpisującego (podobnie złożenie podpisu „dla próby”). Zupełnie inaczej podpis elektroniczny. Zazwyczaj w procedurze jego złożenia, poza samym podpisującym, uczestniczą i inne podmioty (np. wystawca certyfikatów), które ponoszą określona odpowiedzialność związaną z samym faktem złożenia takiego podpisu i jego późniejszymi następstwami. Przyjąć więc należy, że każdorazowe złożenie podpisu elektronicznego (bez względu na zamiar podpisującego) wywołuje skutki prawne. Prawnie obojętna jest motywacja podpisującego. Tak więc doniosłe będzie złożenie podpisu dla żartu, próby, etc. Za takim rozwiązaniem przemawiają również względy funkcjonalne, wymaga tego specyfika czynności dokonywanych w środowisku wirtualnym. Przyjęcie takiego domniemania niezbędne jest dla działania w zaufaniu do tak dokonanych czynności. Oczywiście otwarta pozostaje droga do późniejszego wzruszenia czynności prawnej, np. z uwagi na wady oświadczenia.

Pomiędzy podpisem elektronicznym a jego posiadaczem nie występuje w zasadzie żadna więź emocjonalna. Nie sposób mieć osobistego stosunku do „czegoś”, czego w zasadzie nie widać, co stanowi losowo nam przyporządkowany ciąg liczb.

Nie ma w zasadzie przeszkód, aby osoba trzecia posłużyła się cudzym podpisem elektronicznym za, lub bez zgody jego posiadacza. W obu przypadkach dochodzi do nieautoryzowanego użycia podpisu¹(w niektórych systemach prawnych rygorystyczne wymagania w zakresie składania własnoręcznego podpisu prowadzą do pewnego paradoksu. Np. w Niemczech wyznacza się specjalnego podpisującego, który upoważniony jest do składania podpisu w imieniu oświadczającego, nawet jego nazwiskiem. Odbicie podpisu sposobem mechanicznym nie czyni zadość wymaganiom ustawy)².

Złożenie podpisu własnoręcznego wymaga posiadania pewnych manualnych predyspozycji, które z pewnymi wyjątkami (art. 79 – 80 KC) posiadają wyłącznie osoby fizyczne. Tylko osoba fizyczna umie i może złożyć własnoręczny podpis.

¹ Czy jednak dochodzi tu do fałszerstwa podpisu? Czy penalizuje **art. 270. § 1.** „*Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, (...)*”

² Patrz szerzej Anna Jędrzejewska: Pisemna forma oświadczenia woli a „automatyzacja” obrotu prawnego, PiP 1/93 str. 69

Osoba prawa z uwagi na swoją naturę nie ma i nigdy mieć nie będzie predyspozycji do złożenia podpisu (z wyjątkiem autoryzacji dokumentów w systemach EDI). Osoba prawa działa przez swoje organy w sposób przewidziany w ustawie i opartym na niej statucie (art. 38 KC). Organy osoby prawnej muszą zatem być personalnie obsadzone, tylko bowiem człowiek jako istota rozumna działać może w obrocie cywilnoprawnym¹.

Człowiek może występować jako organ osoby prawnej, jeżeli:

- struktura organizacyjna danej osoby prawnej przewiduje dany organ i konstytuuje jego kompetencje
- personalna obsada tego organu nastąpiła zgodnie ze strukturą organizacyjną danej osoby prawnej
- osoba powołana na to stanowisko rzeczywiście działa w tym charakterze dla osoby prawnej².

Działania organu osoby prawnej traktowane są jak działania samej tej osoby, chyba że dana osoba podszywa się pod organ osoby prawnej. W takim przypadku jej czynności nie wywołują żadnych skutków prawnych (z wyjątkiem ochronny dobrej wiary kontrahenta takiego *quasi* organu. Pozorne działanie rodzi obowiązek naprawienia szkody)³.

Rozważyć należy czy osoba prawa może być posiadaczem własnego podpisu elektronicznego (który będzie niezmienny, niezależnie od personalnej obsady jej organów). Kwestia ta nie została jednoznacznie uregulowana. Art. 3 pkt 9 UoP-P zawiera legalną definicję „podpisującego”, jest to **osoba fizyczna**, której przyporządkowane są dane służące do sporządzenia podpisu oraz odpowiednie dane służące do kontroli podpisu i która składa elektroniczny podpis albo we własnym imieniu, albo w imieniu osoby trzeciej, lub podmiot certyfikujący, stosujący certyfikaty w celu świadczenia usług certyfikacyjnych. Art. 6 projektu

¹ Jedyną osobą prawną nie mającą organów jest Skarb Państwa:

„W obowiązującym porządku prawnym Skarb Państwa jest osobą prawną o szczególnych cechach. Odróżnia się od innych osób prawnych w szczególności tym, że pozbawiony jest siedziby oraz organów w rozumieniu art. 38 k.c. Skarb Państwa ma natomiast swoją wewnętrzną strukturę organizacyjną, która w obrocie cywilnoprawnym, a także w odniesieniu do czynności procesowych pojawia się pod postacią tzw. *stationes fisci*. Skarb Państwa bowiem to jedynie zbiorcze określenie przypisywane różnego rodzaju jednostkom państwowym, wyodrębnionym co prawda organizacyjnie, ale nie mającym podmiotowości cywilnoprawnej”. Postanowienie SN z dnia 28.03.1995, SN I CRN 24/95, OSNC 1995/7-8/117

² Zbigniew Radwański: Prawo cywilne - część ogólna, Warszawa 1997 str. 162 i nast.

³ Podobnie § 122 BGB

mówiąc o „podmiocie” podpisującym¹, gdzie pojęcie „podmiot” zgodnie z art. 3 pkt 8 oznacza osobę fizyczną, osobę prawną, albo jednostkę organizacyjną nie posiadającą osobowości prawnej. Pojawia się więc wątpliwość czy w art. 6 chodzi o „podmiot” czy „podpisującego” w rozumieniu art. 3? Wydaje mi się, że należy zastosować szersze pojęcie. Pośrednio uzasadniał to art. 9 ust. 1 pkt 2 projektu z 5.12.2000r. gdzie wskazywano na „nazwę” posiadacza certyfikatu (w wersji z 21.12.2000r. w art. 9 pozostawiono jedynie elementy certyfikatu kwalifikowanego, gdzie wskazuje się na imię i nazwisko podpisującego). Posiadanie certyfikatu nie jest oczywiście tożsame w żadnej mierze z posiadaniami klucza podpisu (sam klucz przypisać można osobie fizycznej jako organowi osoby prawnej, certyfikat – osobie prawnej). Dodatkowo sięgnąć należy do art. 7 ust. 1 „(...) z *podmiotem składającym podpis elektroniczny (...)*”.

Rozstrzygnięcia problemu nie ułatwia rozwiązywanie przyjęte przez niemieckiego ustawodawcę. SigG definiuje certyfikat jako cyfrowe zaświadczenie o przyznanie publicznego klucza (*öffentlichen Schlüssels*) podpisu osobie fizycznej (§ 2 Abs. 1). Wśród elementów treści wskazuje się m.in. na: nazwisko lub pseudonim posiadacza klucza (*Signatursschlüssel – Inhabers*; § 7 Abs. 1/1 SigG).

Na gruncie powyższych rozważań pokusić można się o refleksję następującą. Osoba prawa może posiadać swój własny podpis elektroniczny, który będzie jej wyłącznie przypisany tak jak np. REGON. Powyższe wątpliwości odnoszą się natomiast do drugiego elementu podpisu elektronicznego (złożenie podpisu wymaga, jak była o tym mowa łączności woli i posiadania) tj. woli, czyli dokonania czynności konwencjonalnej złożenia podpisu. Specyfika osoby prawnej uniemożliwia dokonywanie jakichkolwiek czynności manualnych, niezbędnych również dla złożenia podpisu elektronicznego. Rekapitulując podpisującym może być wyłącznie osoba fizyczna, która może złożyć podpis w imieniu osoby trzeciej (z tym, że organ nie działa w imieniu osoby prawnej, bo nie ma on w ogóle własnej autonomii). Ma to również znaczenie dla odpowiedzialności wewnątrz samej osoby prawnej (nie ma znaczenia dla odpowiedzialności zewnętrznej). Spada więc na podpisującego po części ryzyko nieautoryzowanego posłużenia się kluczem podpisu.

¹ „*Podmiot podpisujący może stosować podpis elektroniczny(...)*”

Jednoznacznie rozstrzygnięto natomiast problem w UoP-Rz. Przyjmuje się generalne założenie, że podpis elektroniczny złożyć może wyłącznie osoba fizyczna (weryfikacja podpisu wskazuje również wyłącznie określoną osobę fizyczną). Podpis elektroniczny musi jednak umożliwić stwierdzenie, w jakim charakterze działała osoba fizyczna. Wśród wymienionych możliwości projekt expressis verbis wymienia „*(...)w charakterze członka organu lub organu określonej osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej (...)*”.

Podpis elektroniczny nie redukuje udziału osoby fizycznej w procedurze jego złożenia, z tym, że jej rola ogranicza się wyłącznie do odblokowania np. chipkarty, na której zakodowano klucz prywatny osoby prawnej (np. wzór linii papilarnych pana X działającego w charakterze organu osoby prawnej, ale ten sam wzór może być również zakodowany na jego prywatnej chipkarcie, będą to jednak podpisy dwóch różnych podmiotów prawa – elementem wspólnym będzie np. topografia kciuka pana X, która jednak nie jest elementem podpisu, a elementem zabezpieczenia przed jego nieautoryzowanym użyciem).

Mimo braku legalnej definicji podpisu własnoręcznego powszechnie przyjmuje się, jest on językowym znakiem graficznym. Ustawowe definicje podpisu elektronicznego mogą mu nadać określone skutki prawne, nie zmienią jednak faktu, że nie jest on podpisem w powyższym znaczeniu. Trudno się oczywiście nie zgodzić, że jest to kwestia ścisłe terminologiczna. W istocie jednak podpis elektroniczny jest pewnym tworem matematycznym, tak ukształtowanym, aby był w stanie zrealizować funkcje tradycyjnie przypisywane podpisowi własnoręcznemu. Nie było więc w zasadzie potrzeby tworzenia nowej kategorii pojęciowej. Z powodzeniem bowiem wystarczyłoby wyeksponowanie w regulacji ustawowej samych funkcji podpisu własnoręcznego i uzależnienie od ich realizacji ważności, i skuteczności dokumentu elektronicznego – wydaje się, iż przeważyły względy pragmatyczne. Złośliwi twierdzą, iż pojęcie – „podpis elektroniczny” – jest owocem kompromisu, dla prawników bowiem cokolwiek mówi rzeczownik „podpis”, informatycy zaś jakiekolwiek skojarzenia łączą z przymiotnikiem „elektroniczny”.

3. FUNKCJE PODPISU ELEKTRONICZNEGO

Celem podpisu elektronicznego jest m.in. potwierdzenie tożsamości podmiotu podpisującego. Podpis elektroniczny nie stwarza możliwości ustalenia tożsamości wprost. Jeżeli proces weryfikacji podpisu elektronicznego daje pozytywny rezultat, tzn. skrót wiadomości wydzielony i wygenerowany są identyczne oznacza to tylko, i wyłącznie, że do złożenia podpisu elektronicznego posłużyono się kluczem prywatnym będącym komplementarną częścią użytego przez nas klucza publicznego. Weryfikacja podpisu elektronicznego pozwala więc na jednoznaczne stwierdzenie, że:

- podpis elektroniczny został utrwalony z użyciem klucza prywatnego odpowiadającego kluczowi publicznemu
- dane zapisane na nośniku nie uległy zmianie ani żadnej inne modyfikacji po złożeniu podpisu elektronicznego¹

Aby podpis elektroniczny był prawnie doniosły musi realizować te same, co podpis własnoręczny funkcje. Nadto podpis elektroniczny chroni dokument przed jego przerobieniem (a zasadzie nie tyle chroni, co sygnalizuje ingerencję w treść dokumentu)². Ma więc uniemożliwić niezauważalną modyfikację treści dokumentu. Jeszcze na etapie prac nad ustawą Niemiecka Izba Notarialna (*Bundesnotarkammer*)³ zaproponowała założenia do rozporządzenia o podpisie⁴. Wydaje się, że dosyć na wyróst określono funkcje nowej instytucji. W projekcie wskazano, iż aby podpis był uznawalny, musi:

- 1) chronić dokument przed podrobieniem i przerobieniem
- 2) realizować ta same funkcje, co podpis własnoręczny tj.:
 - a) gwarantującą (*Echtheitsfunktion*)
 - b) świadczącą (*Abschlußfunktion*)
 - c) ostrzegającą (*Warnfunktion*)
 - d) identyfikującą (*Identitäsfunktion*)

¹ Uzasadnienie wstępniego projektu rządowego ustawy o podpisie elektronicznym <http://www.vagla.eu.org/>

² „(...) versehen ist, den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt”
SigG § 2 Abs. 1

³ Materiały dotyczące m.in. podpisu elektronicznego znaleźć można na stronie: <http://www.dnoti.de/>

⁴ Begründung zur Unterschriftverordnung - Stand: 12 August 1995

W rzeczywistości jednak żaden z obecnie funkcjonujących systemów podpisów cyfrowych (np. PGP) nie jest w stanie zrealizować wszystkich tych funkcji w stu procentach.

Z uwagi na specyfikę obrotu elektronicznego powyższe funkcje wypełniono różną od podpisu własnoręcznego treścią. I tak:

ad. a)

Funkcja gwarantująca powinna stanowić dowód, że osoba, która podpisała dokument elektroniczny złożyła oświadczenie o treści w nim zawartej – domniemanie prawdziwości (podobnie jak dokument prywatny). Funkcja gwarantująca rozciąga się również na wspomnianą wyżej ingerencję w treść dokumentu. Mówiąc o tym *expressis verbis* art. 4 ust. 2 pkt 4 UoP-P „*jest powiązany z danymi, do których został dodany w taki sposób, że każda późniejsza zmiana tych danych jest możliwa do stwierdzenia*”¹.

Zrealizowanie funkcji gwarantującej w praktyce jest jednym z poważniejszych problemów PKI, wymaga bowiem utrzymania w tajemnicy prywatnego klucza podpisu. Należy więc podjąć czynności, które zabezpieczą nośnik, na którym ten klucz zapisano. W innym razie bezpieczeństwo obrotu stanowi iluzoryczny postulat.

Składanie oświadczeń woli z wykorzystaniem mediów elektronicznych nie wymaga podejmowania wielu czynności pomocniczych (np. wyjście do sklepu), które finalnie prowadziły do dokonania czynności prawnej. Oczywiście bezpośrednio nie były one prawnie relevantne, dawały jednak czas, który mógł inaczej ukształtować ostateczną wolę oświadczającego. Obrót elektroniczny jest obrotem bardzo dynamicznym, stąd też skutki prawne bardzo szybko emanują na różne przejawy życia prawnego.

Ustawodawcy zalecają więc stosowanie środków kontroli dostępu (*Zugangskontrolle*) do klucza podpisu, którego nie sposób przechowywać wyłącznie w pamięci człowieka. Najprostszym sposobem jest zabezpieczenie nośnika numerem PIN (*Personenidentitätsnummer*). Numer taki nie odgrywa w obrocie żadnej roli, poza autoryzowaniem dostępu do nośnika. W szczególności

¹ Tak również §1 Abs. 1 SigG „*Zweck des Gesetzes ist es, Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können*“.

nie można mu przypisać funkcji, jaką tradycyjnie łączy się z nazwiskiem (BzU). Lepsze rezultaty tzn. ścisłejsze powiązanie podpisu z konkretną osobą uzyskuje się dzięki metodom biometrycznym (linie papilarne, wzór siatkówki, próbka głosu, etc.).

Posłużenie się przez osobę trzecią cudzym kluczem podpisu za zgodą tej osoby należy potraktować jako analogię do złożenia podpisu *in blanco* (tak niemieccy notariusze w Begründung zur Unterschriftverordnung). Jest to dosyć swoiste stanowisko zważywszy na dotychczasową penalizację takiego zachowania (podpis jest bowiem dobrem osobistym, które korzysta z ochrony prawnej niezależnie od woli i wiedzy jego posiadacza).

ad. b)

Funkcja świadcząca potwierdza, że dokument nie jest projektem, lecz wyrazem ostatecznego oświadczenia woli. W odróżnieniu od dokumentu sygnowanego podpisem własnoręcznym w dokumencie elektronicznym praktycznie niemożliwa jest niezauważalna zamiana jednego z arkuszy takiego dokumentu (trudno tu w ogóle mówić o stronach jako taki, bo dokument elektroniczny stanowi jedną, spójną całość). Ważne jest, aby urządzenia stosowane do prezentacji danych zapisanych na nośniku elektronicznym umożliwiały podpisującemu zapoznanie się z ich treścią. Art. 21 ust. 10 UoP-P obowiązkiem tym obciąża wystawcę certyfikatów. Jeżeli strony nie korzystają z certyfikacji (wg art. 6 ust. 3 UoP-P nie ma takiego obowiązku) same ponoszą ryzyko nieczytelności treści dokumentu¹. Przypadek braku certyfikacji dotyczyć będzie albo obrotu profesjonalnego i zautomatyzowanego (EDI), albo innych stosunków bilateralnych lub w ramach zamkniętego systemu użytkowników. Wszelkie więc mogące pojawić się problemy winna zasadniczo regulować umowa zawarta pomiędzy stronami.

¹Adam Szpunar: glosa do uchwały SN z dnia 31 maja 1994 r., III CZP 75/94, OSP 33/2/1995 - t.1, „*Nie ma błędu, gdy ktoś podpisuje dokument, nie znając jego treści. Osoba taka nie myli się, ponieważ świadomie zaakceptowała postanowienia zawarte w dokumencie. Podobnie należy ocenić sytuację, gdy podpisujący wyciągnął niewłaściwe wnioski na temat treści dokumentu i podjął niesłuszna decyzję.*”

ad. c)

Funkcja ostrzegawcza ma sygnalizować, że składane jest oświadczenie woli, a więc chronić przed dostatecznie nieprzymyślanym dokonaniem czynności prawnej. Osoba korzystająca z podpisu elektronicznego musi mieć świadomość ryzyka związanego z obrotem elektronicznym. Paradoks obrotu elektronicznego nie wiąże się z elementem ryzyka (choć to jest również istotne), polega na tym, że prostota dokonywania czynności prawnych, mająca być jego zasadniczym walorem, stanowi jego główną wadę. Powszechnie ugruntowane jest przekonanie o anonimowości, jaką oferują media elektroniczne i związane z tym poczucie bezkarności. Jest to przekonanie naiwne. Funkcja ostrzegawcza oznacza również, że na gruncie aktualnej wiedzy podpis elektroniczny oraz procedura jego składania zapewniają adekwatny do tej wiedzy poziom bezpieczeństwa.

Kluczowe znaczenie w zakresie funkcji ostrzegawczej ma, aby moment złożenia podpisu był dla podpisującego wyraźnie widoczny (art. 21 ust. 11 UoP-P).

ad. d)

Rola funkcji identyfikującej sprowadza się do zweryfikowania tożsamości autora dokumentu elektronicznego. Ustalenie tożsamości dokonującego czynności prawnej obok zachowania integralności dokumentu stanowi zasadnicze zadania podpisu elektronicznego. Nie dziwi więc, że w ramach BzU sugerowano bardzo daleko idące środki ostrożności. Zaświadczenie notarialne miało jednoznacznie określać, komu został przyporządkowany konkretny klucz publiczny wraz z certyfikatem. Ostatecznie SigG nakłada na wystawcę certyfikatów obowiązek niezaprzeczalnej identyfikacji osoby wnoszącej o udzielenie certyfikatu (§ 5 Abs.1). Wystawca certyfikatów ma ponadto obowiązek stworzyć warunki do powszechniej (tj. ogólnodostępnej) i każdorazowej identyfikacji podpisującego za pośrednictwem łączny telekomunikacyjnych (§ 5 Abs. 5 SigG). Tożsamość podmiotu wystawca certyfikatów potwierdza przez udzielenie mu certyfikatu oraz klucza publicznego (*öffentlichen Signaturschlüssels*), służącego do jego identyfikacji. Aby cały system weryfikacji podpisującego działał efektywnie konieczne jest stosowanie środków ochrony danych zawartych w certyfikatach przed ich podrobieniem i przerobieniem, co stanowi duże wyzwania dla świadczących te usługi. Dane te są bowiem powszechnie dostępne. Konieczne

jest również sprawdzenie czy dane zgłaszcane do certyfikatu są zgodne z rzeczywistością. Oba te obowiązki obciążają finalnie wystawcę certyfikatów (§ 5 Abs. 4 SigG).

Rozwiązania bardzo zbliżone zawiera UoP-P w art. 23, art. 21 ust. 9 oraz art. 7. Szczególnie ważny jest art. 21 ust. 9, który uniemożliwia efektywne skorzystanie z klucza podpisu bez uprzedniego, skutecznego ustalenia tożsamości jego posiadacza. „Skutecznie” według BzU oznacza w formie aktu notarialnego. Podnieść mogą się głosy, że jest to niczym nieuzasadniony formalizm. Zgodzić można się, co do formalizmu, ale czy jest on nieuzasadniony? Moim zdaniem nie (przynajmniej w odniesieniu do osób fizycznych).

UoP-P rozstrzyga powyższy problem terminologiczny. Art. 27 uzależnia rozstrzygnięcie od charakteru prawnego oferenta:

- jeżeli oferent jest osobą fizyczną – na podstawie dowodu tożsamości
- jeżeli oferent jest osobą prawną – na podstawie wypisu z rejestru
- jeżeli oferent jest jednostką organizacyjną nie posiadającą osobowości prawnej – na podstawie innych określonych prawem dokumentów dotyczących powołania jednostki

Rekapitulując pojawia się refleksja następująca. Podpis elektroniczny wnosi do obrotu prawnego zupełnie nową jakość. Wbrew panującym nastrojom lęku zapewnia wyższy stopień bezpieczeństwa i nie wątpliwie jago wdrożenie pobudzi znacznie życie prawne. Nie same tu jednak superlatywy. Pozorna prostota i faktyczne bezpieczeństwo wymaga zbudowania prawnego i technicznego zaplecza, bez którego obejść może się zupełnie podpis tradycyjny. Wydaje się, mimo wszystko, że jednak warto (skończą się np. spory interpretacyjne o podpis pod testamentem, ale to kwestia nie tak znowu bliskiej przyszłości).

4. SYSTEM CERTYFIKACJI, ODPOWIEDZIALNOŚĆ WYSTAWCY CERTYFIKATÓW

Dotychczasowe rozważania zarysowują zaledwie prawne i techniczne konotacje podpisu elektronicznego, w wystarczający wszakże dla uchwycenia istoty problemu sposób. Jak była już o tym mowa, identyfikacja kontrahenta odbywa się

za pomocą jego klucza publicznego, ustalenie tożsamości w oparciu o wystawiony certyfikat. W rzeczywistości nie interesuje nas weryfikacja samego podpisu elektronicznego (tj. procesu polegającego na rozszyfrowaniu wiadomości do postaci jawniej, oddzieleniu tekstu jawnego od skrótu wiadomości oraz wygenerowaniu własnego skrótu w celu ich porównania), nie ma ona dla nas wartości poznawczej. Chodzi wyłącznie o zweryfikowanie autentyczności klucza publicznego (proces weryfikacji podpisu elektronicznego może mieć prawidłowy przebieg, jeżeli przeprowadzimy go w oparciu o sfabrykowany klucz publiczny, m.in. takie sytuacje ma wyeliminować certyfikat).

Można również zweryfikować sam certyfikat, czyli w zasadzie klucz publiczny wystawcy certyfikatów. Dotyczy to jednak wyłącznie akredytowanych (licencjonowanych) wystawców certyfikatów (*Zertifizierungsstelle*), tj. takich, którzy otrzymali akredytację kompetentnego organu¹. Zadania tego organu obejmują w szczególności:

- udzielenie wystawcy publicznej gwarancji jakości świadczonych przez nich usług
- certyfikacja własnych kluczy publicznych wystawców certyfikatów (niezależnie od posiadania akredytacji)

Posiadanie certyfikatu nie jest jednakże *conditio sine qua non* ważności podpisu elektronicznego (art. 5 ust. 2 UoP-P). Ważność podpisu bez certyfikatu uzależniona jest od:

- zgody kontrahenta podpisującego lub
- umowy stron (art. 6 ust. 3 UoP-P)

Przyjęte rozwiązanie pozostawia rozstrzygnięcie w sferze autonomii woli stron. Trzeba jednak zauważyć, że zakres zastosowania ograniczony jest raczej do systemów wewnętrznych (np. EDI), stosunków bilateralnych czy zamkniętej grupy podmiotów. W kontaktach „przypadkowych” (np. zawieranie pojedynczej umowy za pośrednictwem Internetu) założyć należy brak zaufania do podpisu bez certyfikatu.

¹ Według UoP-P funkcję taką ma pełnić Krajowy Urząd Akredytacji art. 3 pkt. 17, w Niemczech jest to Bundesamt für Sicherheit in der Informationstechnik

Inną zupełnie sprawą jest brak akredytacji. Art. 16 ust. 2 zezwala na świadczenie usług certyfikacyjnych bez posiadania zezwolenia i/lub akredytacji. Brak akredytacji wiąże się jednak z pewnymi istotnymi ograniczeniami:

- w relacjach z jednostkami sektora publicznego posługiwać się można wyłącznie certyfikatem kwalifikowanym, który wystawić może wyłącznie akredytowany wystawca certyfikatów (art. 5 ust. 4 UoP-P)
- uzyskanie akredytacji przez wystawcę certyfikatów stanowi potwierdzenie, że jest on instytucją zaufania publicznego (art. 31 ust. 2 UoP-P)

Dla uzyskania certyfikatu kwalifikowanego konieczne jest posiadanie odpowiedniego zabezpieczenia finansowego (art. 19 UoP-P).

Niemiecki SigG wymaga, aby wystawca certyfikatów posiadał licencję oraz niezbędną wiedzę specjalistyczną. Wymóg ten jest spełniony również wówczas, gdy wiedzę tę posiadają osoby zatrudnione przez wystawcę (§ 4 SigG). Działalność certyfikacyjną prowadzić mogą zarówno osoby fizyczne jak i prawne (§ 2 Abs. 2 SigG).

Pojęcie certyfikatu.

„Certyfikat jest elektronicznym odpowiednikiem dowodu tożsamości. Umożliwia on zarówno zidentyfikowanie użytkownika Internetu, ale również użytkownik Internetu, który łączy się z serwerem posiadającym swój własny certyfikat, ma pewność, że połączył się z właściwą instytucją, a nie z kimś, kto się pod nią podszywa¹.“

Definicje certyfikatu zawarte w ustawach o podpisie elektronicznym nie wykazują jednolitości. SigG określa certyfikat (*Signaturschlüssel-Zertifikat*) jako cyfrowe zaświadczenie przyporządkowania publicznego klucza podpisu osobie fizycznej (§2 Abs. 3 SigG).

Bardziej ogólną (wydaje się więc, że trafniejszą) definicję zawiera art. 3 pkt 14 UoP-P. Certyfikatem jest elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do określonej osoby składającej podpis elektroniczny i potwierdzają tożsamość tej osoby. Trafnie w miejsce pojęcia „klucz publiczny” wprowadzono pojęcie „dane

¹ <http://www.fortisbank.com.pl/services/PlanetPL.html>

służące do (...)", które jest pojęciem szerszym. Dodatkowo pojęcie to jest elastyczne w stosunku do innych metod kryptograficznych tzn. nieopartych na parze kluczy komplementarnych. Pozostaje więc ono w zgodzie z zakresem pojęcia podpis elektroniczny (nie niweczy konsekwencji jego zastosowania, oba są dostatecznie szerokie dla innych metod kryptograficznych).

Najczęściej przyjmuje się, że certyfikat w swojej treści zawierać powinien co najmniej¹:

- nazwę lub identyfikator organu wydającego
- identyfikator subskrybenta²
- klucz publiczny subskrybenta
- numer seryjny certyfikatu
- podpis organu wydającego

Spośród ogółu certyfikatów UoP-P wyodrębnia certyfikaty kwalifikowane (podobnie jak RL).

Ze względu na ciągłe udoskonalanie PKI certyfikaty wydawane są wyłącznie na czas oznaczony. Maksymalny okres ważności certyfikatu wynieść ma trzy lata (art. 8 ust. 2). Nieco inaczej aspekt ważności certyfikatu rozwiązał ustawodawca niemiecki. SigV uzależnia ważność certyfikatu od dwóch determinantów:

- kryterium zasadniczym, podobnie jak w polskim projekcie, jest czas. Wynosi on maksymalnie pięć lat i jest to relatywnie długi okres (jeżeli wziąć pod uwagę dynamikę rozwoju informatyki)
- warunkiem dodatkowym jest, aby w tym czasie zachowały swoją skuteczność, przyjęte w chwili wystawienia certyfikatu za wystarczające, algorytm i jego parametry

Innymi słowy certyfikat ważny jest dopóty stosowany algorytm jest adekwatny do aktualnego stanu wiedzy, czyli gwarantuje zachowanie założonego poziomu bezpieczeństwa obrotu, nie dłużej jednak jak pięć lat od jego wystawienia.

Uczestnicy obrotu korzystają ze swobody wyboru wystawcy certyfikatów (art. 8 ust. 1 UoP-P).

¹ Patrz także art. 9 UoP-P; §7 SigG; Art. 2 RL

² Subskrybent – osoba będąca podmiotem wydanego certyfikatu, która jest inicjatorem wiadomości oraz podpisuje ją (...) <http://www.centrum.pl/>

Zadania i obowiązki wystawcy certyfikatów, charakter prawny umowy oświadczenie usług certyfikacyjnych.

Podpis elektroniczny nie posiada treści, tak jak podpis odręczny. Oba podpisy są skuteczne (tzn. realizują stawiane im zadania) wyłącznie w powiązaniu z charakterystycznymi dla nich nośnikami. Rozważając zupełnie teoretycznie podpis elektroniczny można „wyeksponować” na papierze, podobnie podpis własnoręczny może być postawiony na elektronicznym nośniku informatycznym. Czynności takie pozbawione są wszakże skutku, jaki zazwyczaj zrealizować ma prawnie doniosły podpis. Nie możemy powiedzieć, że mamy tu podpis w znaczeniu prawnym.

Mimo tego, że podpis elektroniczny jest przypisany konkretnej osobie i związek ten możliwa zweryfikować, jest on wyłącznie owocem przypadku. Brak naturalnej więzi sprawia, że podpis elektroniczny bez systemu certyfikacji nie będzie należycie realizował przypisanych mu funkcji. Nie dotyczy to przypadku, kiedy posługiwanie się podpisem elektronicznym wynika z umowy stron. Weryfikacja uczestników obrotu odbywa się w oparciu o tę właśnie umowę.

Podpis elektroniczny nie istnieje fizycznie, nie można więc poddać go ekspertyzie grafologicznej (w tradycyjnym znaczeniu). Tym bardziej widoczna jest potrzeba stworzenia sprawnego systemu certyfikacji.

Art. 6 RL reguluje zagadnienia odpowiedzialności wystawcy certyfikatów wobec usługobiorców. Odpowiedzialność ta rozciąga się m.in. na:

- dokładność wszystkich informacji zawartych w certyfikacie kwalifikowanym jak data wystawienia, chyba że świadczący usługę postanowił inaczej w certyfikacie
- zgodność z wszystkimi wymogami RL o wydaniu certyfikatu kwalifikowanego
- zapewnie, że posiadający certyfikat dysponuje, w czasie wystawienia certyfikatu, odpowiednim narzędziem do tworzenia podpisu

Również polski projekt ustawy (UoP-P) wiele miejsca poświęca problematyce odpowiedzialności wystawcy certyfikatów. Świadczenie usług certyfikacyjnych odbywa się na podstawie umowy cywilnoprawnej „*określającej w szczególności cenę usługi*” (art. 17 ust. 2). Projekt nie wskazuje wyraźnie na żaden z typów normatywnych umów uregulowanych w KC. Jedynym wyraźnie wskazanym

elementem przedmiotowo istotnym tej umowy jest jej odpłatność. Wydaje się, że najważniejsze będzie przyjęcie, że jest to umowa nienazwana, do której znajdą zastosowanie przepisy KC o zleceniu (art. 734-751 KC). Normatywna konstrukcja umowy zlecenia nie zakłada, co prawda odpłatności jako *essentialia negotii* tej umowy (art. 743 § 1 KC), zlecenie może być jednak odpłatne (art. 735 § 1 KC).

Wystawca certyfikatów pośredniczy przy dokonywaniu czynności prawnych w drodze elektronicznej, głównie w zakresie weryfikacji klucza podpisu. Ma to jednak decydujące znaczenie dla skuteczności czynności prawnej.

Przepisy KC o zleceniu, w zależności od przedmiotu świadczonych przez wystawcę certyfikatów usług, znajdą zastosowanie wprost lub odpowiednio (art. 750 KC – usługi polegające na czynności faktycznej). Wystawca certyfikatów świadczy usługi w zakresie wydawania, zawieszania i unieważnienia certyfikatów (art. 18 ust. 1 UoP-P). Certyfikat jest „*elektronicznym zaświadczeniem*” (art. 3 pkt 14 UoP-P), w związku z czym, jego wystawienie nie jest czynnością prawną, lecz materialnotechniczną, ponieważ „(...) zaświadczenie nie rozstrzyga żadnej kwestii, lecz jest (...) stwierdzeniem pewnych znanych faktów lub stanu prawnego. Zaświadczenie zatem nie tworzy, nie uchyla i nie zmienia istniejących stosunków prawnych (...)”¹. Podobnie czynnościami faktycznymi są usługi polegające na udostępnianiu produktów i procedur składania podpisu elektronicznego, etc. (art. 18 ust. 2 UoP-P).

Działanie przyjmującego zlecenie może polegać na dokonaniu czynności w imieniu dającego zlecenie (a więc z takim skutkiem, że odpowiednie prawa i obowiązki nabywa bezpośrednio dający zlecenie tj. usługobiorca w rozumieniu art.3 pkt 13 UoP-P). Taka czynność polegać może na złożeniu podpisu elektronicznego wyłącznie na wyraźną i jednoznaczna dyspozycję podpisującego lub działającego na jego rzecz operatora (art. 21 ust. 11 UoP-P)². Wystawca certyfikatów działa więc jako pełnomocnik usługobiorcy. Art. 734 § 2 KC eliminuje konieczność odrębnego ustanowienia pełnomocnictwa. „Połączenie zlecenia z pełnomocnictwem stwarza taką sytuację prawną, że przyjmujący zlecenie jest nie

¹ Tak wyrok NSA z dnia 28.06.1983, I SA 268/83, ONSA 47/1/1983

² Dosłownie przepis ten stanowi, że środki techniczne mają to umożliwiać, inne definicje wskazują, że chodzi tu o obdarzoną zaufaniem instytucję lub urządzenie pod kontrolą tej instytucji. Ostatecznie wszystko zależy od przyjętej procedury składania podpisu, możliwe, że z technicznego punktu widzenia podpis składać będzie operator, a posiadacz podpisu przy pomocy np. chipkarty dokonuje jedynie każdorzędnego umocowania operatora do dokonania tej czynności. Skutki prawne dotyczą bezpośrednio samego podpisującego.

tylko upoważniony, ale także zobowiązany do działania w imieniu dającego zlecenie”¹. Nie jest natomiast możliwa sytuacja, aby w tym konkretnym przypadku wystawca certyfikatów działał w imieniu własnym, lecz na rachunek dającego zlecenie (art. 740 KC). Jest on bowiem podmiotem (ewentualnie instytucją zaufania publicznego) zajmującym się wyłącznie wystawianiem certyfikatów i świadczeniem innych związań z tym usług (głównie weryfikacją klucza publicznego). Jego rola jest wyłącznie pasywna, warunkowana ewentualnymi dyspozycjami usługobiorcy. Nie ma ani podstaw, ani możliwości podejmowania jakichkolwiek czynności bez uprzedniej wiedzy i wyraźnej zgody podpisującego.

Prawa i obowiązki stron.

Podstawowym obowiązkiem wystawcy certyfikatów jest wykonanie zobowiązania z umowy o świadczenie usług certyfikacyjnych czyli wystawienie certyfikatu, tudzież świadczenie innych usług (wymienionych w art. 18 ust. 1 UoP-P). W razie niewykonania lub nienależytego wykonania zobowiązania wystawca ponosi odpowiedzialność kontraktową (art. 471 KC) za szkodę wynikłą nawet z winy nieumyślnej. Należ tu również uwzględnić możliwość powstania szkody w ramach tzw. ujemnego interesu umownego (*culpa in contrahendo*). Jest to szkoda wynikła z niedojścia umowy do skutku np. wadliwy przebieg procesu weryfikacji, skądinąd właściwego kontrahenta, z przyczyn obciążających wystawcę. Szkoda w granicach ujemnego interesu umownego obejmuje to, co strona by miała, gdyby nie podjęła działań zmierzających do zawarcia umowy. Nie ma wątpliwości, że obejmuje ona oba składniki szkody tj. *damnum emergens* i *lucrum cessans* (w zakresie tego drugiego składnika niektórzy dopatrują się zbyt daleko idących konsekwencji, wskazując na możliwość niezawarcia jakieś innej umowy, należy brać pod uwagę wyłącznie konsekwencje wynikające z już zawartych umów)². Przyczyną wadliwej weryfikacji, a w rezultacie powstania szkody, mogą być błędy zawarte w samym certyfikacie. Zasadniczo wystawca nie ponosi odpowiedzialności cywilnej za szkodę spowodowaną błędami informacyjnymi zawartymi w certyfikacie, jeżeli takie nieprawdziwe dane podane zostały przez usługobiorcę. Zasada ta nie znajduje zastosowania, jeżeli wystawca o tych

¹ Zbigniew Radwański, Janina Panowicz-Lipska „Zobowiązania – część szczegółowa” Warszawa 1996 str.101

² Tak Zbigniew Radwański: Zobowiązania – część ogólna, Warszawa 1997 str. 88

błędach wiedział lub z łatwością mógł je zauważyc (art. 26 ust. 2 UoP-P). Wystawca certyfikatów nie ponosi również odpowiedzialności cywilnej za szkody spowodowane użyciem certyfikatu z naruszeniem jego przeznaczenia, oraz za szkody powstałe przy transakcjach, których wartość przekraczała limit określony w certyfikacie (art. 26 ust. 3 i 4 UoP-P). Poza powyższymi wyłączeniami odpowiedzialności wystawca certyfikatów ponosi odpowiedzialność cywilną za szkody wyrządzone w związku z:

- brakiem zgodności informacji zawartych w certyfikacie z danymi podanymi w ofercie na jego wydanie w czasie wydania certyfikatu,
- brakiem zgodności z niniejszą ustaw wydanego certyfikatu oraz procedur jego tworzenia i wydawania,
- nienależytym sprawdzeniem, czy podmiot wskazany w wydanym certyfikacie posiada w czasie wydania tego certyfikatu klucz prywatny odpowiadający kluczowi publicznemu zawartemu w wydanym certyfikacie,
- brakami lub uchybieniami w procesie generowania we własnym zakresie kluczy kryptograficznych przeznaczonych dla usługobiorców.

Umowa zlecenia oparta jest na zaufaniu do osoby przyjmującej zlecenie. W szczególności, z punktu widzenia potencjalnego kontrahenta, chodzi o usługi związane z potwierdzeniem tożsamości podpisującego. Wystawca może zawiesić wydany przez siebie certyfikat (art. 12 ust. 2 UoP-P). W takim przypadku spoczywa na nim obowiązek zawiadomienia podpisującego o przyczynach zawieszenia. Ponosi on odpowiedzialność odszkodowawczą za szkodę wyrządzoną przez swoje niedbalstwo (uchybienie temu obowiązkowi). Podpisujący (usługobiorca) ze swojej strony ma jednak obowiązek udzielenia niezwłocznej odpowiedzi na powiadomienie wystawcy. Milczenie podpisującego stwarza po stronie wystawcy certyfikatów możliwość unieważnienia certyfikatu¹. Podpisujący traci również roszczenie wobec wystawcy z tytułu ewentualnie poniesionej szkody (ryzyko szkody przechodzi na podpisującego).

¹ „(2) Certyfikat unieważniony nie może być już stosowany do stwierdzenia tożsamości podpisującego. (3) Unieważnienie certyfikatów z moc wstępna, a także przywracanie ważności unieważnionemu certyfikatowi jest niedopuszczalne”. (art. 10 UoP-P)

Podstawowym obowiązkiem usługobiorcy jest:

- złożyć ofertę zawierającą kompletne i prawdziwe dane oraz podpis oferenta
- wnieść ustaloną opłatę

Wprowadzenie do treści certyfikatu informacji o umocowaniu do reprezentowania osoby trzeciej wymaga przedstawienia pisemnej zgody tej osoby, co musi zostać potwierdzone przez wystawcę certyfikatów.

Obok zagadnienia wygaśnięcia/rozwiązania umowy wskazać trzeba kwestię ustania samego certyfikatu. UoP-P przewiduje trzy możliwości:

- a) wygaśnięcie
- b) zawieszenie
- c) unieważnienie

ad a)

Certyfikat wygasa z mocy prawa:

- po upływie czasu, na jaki został wystawiony
- po zaprzestaniu przez wystawcę certyfikatów świadczenia usług certyfikacyjnych
- certyfikat wydany na podstawie nieprawdziwych danych podanych w ofercie jest bezwzględnie nieważny (skutek *ex tunc* – zniweczone zostają wszystkie skutki prawne czynności gdzie taki certyfikat stosowano)¹.

W dwóch pierwszych przypadkach skutki wygaśnięcia certyfikatu działają wyłącznie na przyszłość (*ex nunc*), od uprawomocnienia się postanowienia sądu o dokonaniu wpisu do KRS.

ad b)

Wystawca certyfikatu może zawiesić certyfikat na okres nie dłuższy niż 72 godziny w celu zbadania czy istnieją podstawy do unieważnienia certyfikatu (art. 12 UoP-).

¹ Czynność taka będzie bezwzględnie nieważna tj. od samego początku i *ex lege*. Czynność taka, jako czynność prawną, nie wywołuje żadnych skutków prawnych. Wydaje się również, że wykluczona będzie również możliwość konwalidacji lub konwersji

ad c)

Wystawca unieważnia certyfikat na żądanie:

- posiadacza certyfikatu
- osoby trzeciej, której dane zawiera certyfikat
- KUA, gdy nie spełnia on wymagań określonych w ustawie
- po ustaniu osobowości prawnej posiadacza certyfikatu (na podstawie odpisu aktu zgonu – gdy posiadacz był osobą fizyczną lub prawomocnego postanowienia sądu o wykreśleniu z rejestru – gdy posiadacz był osobą prawną)

Wykreślenie działa *ex nunc* od opublikowania w publicznie dostępnym rejestrze certyfikatów (art. 10 ust. 4 i 5 UoP-P).

Rozdział VI

CZYNNOŚCI PROCESOWE DOKONYWANE W DRODZE ELEKTRONICZNEJ

1. Wnoszenie pism procesowych drogą elektroniczną.

Zagadnienia formy elektronicznej i elektronicznego obrotu prawnego pozostają aktualne również na płaszczyźnie procesowej. Nowoczesne środki techniczne nie tylko stwarzają możliwości składania oświadczeń woli w postaci elektronicznej informacji, pozwalając także na ich przetwarzanie i przesyłanie bez pośrednictwa papieru.

Art. 63 KPA¹ dopuszcza wnoszenie podań za pośrednictwem poczty elektronicznej:

Art. 63. § 1. Podania (żądania, wyjaśnienia, odwołania, zażalenia) mogą być wnoszone pisemnie, telegraficznie lub za pomocą dalekopisu, telefaksu, poczty elektronicznej a także ustnie do protokołu.

Problemem newralgicznym pozostaje oczywiście własnoręczny podpis. Minimalne wymagania co do treści podania zawiera art. 63 §2, są to:

- wskazanie osoby, od której podanie pochodzi
- jej adres
- żądanie
- czynić zadość innym wymaganiom ustalonym w przepisach szczególnych

Ustawodawca nie wylicza podpisu wnioskodawcy *expressis verbis*, wymóg ten nie budzi jednak wątpliwości². Brak podpisu równoznaczny jest z brakiem formalnym. Wymagania treści podania nie idą, więc tak daleko jak w stosunku do pism w postępowaniu kontrydyktoryjnym (cywilnym). Jest to efektem odformalizowania samego postępowania administracyjnego.

¹ W brzmieniu ustalonym przez art. 2 ustawy z dnia 29 grudnia 1998 r. o zmianie niektórych ustaw w związku z wdrożeniem reformy ustrojowej państwa (Dz. U. 1998 r. Nr 162 poz. 1126).

² Zbigniew Janowicz: Kodeks postępowania administracyjnego – komentarz, Warszawa 1999 str. 197

Ustawodawca sankcjonuje prawnie elektroniczny transfer informacji, nie wyjaśniając jak uczynić zadość wymaganiom formalnym. Wypada zauważać, że dokument wnoszony za pośrednictwem poczty elektronicznej nie jest dokumentem w ujęciu tradycyjnym. Specyficzny jest nośnik treści (o ile w ogóle jest) i specyfika ta rozciąga się również na podpis. Teoretycznie podanie można sygnować podpisem tradycyjnym, a w zasadzie jego graficzną reprodukcją (pobraną np. za pomocą skanera), odpada jednak *ratio legis* takiego rozwiązania. Taka reprodukcja nie realizuje funkcji podpisu własnoręcznego. Rozwiązaniem optymalnym byłoby posłużenie się podpisem cyfrowym, jest to jednak ciągle postulat *de lege ferenda* (pomijając aplikacje o ograniczonym zakresie zastosowania np. Płatnik ZUS).

De lege lata wydaje się, że powyższy przypadek można by zakwalifikować jako wniesienie warunkowe z reżimem podania wniesionego ustnie do protokołu. Po podpisaniu protokołu podanie uzyskałoby moc wsteczną od chwili wniesienia. Taka koncepcja wypacza jednak idei elektronicznego transferu informacji¹.

Podobne uregulowanie wprowadził ustawodawca nowelą do KPC².

Art. 125 § 2 Jeżeli przepis szczególny tak stanowi, pisma procesowe wnoszą się na urzędowych formularzach lub na elektronicznych nośnikach informatycznych.³

Zauważać należy subtelną, ale zasadniczą różnicę pomiędzy regulacją art. 63 KPA a art. 125 §2 KPC. Ten pierwszy wyraźnie mówi o wnoszeniu pism pocztą elektroniczną, w drugim przypadku chodzi o pisma wnoszone na elektronicznych nośnikach informatycznych. Według §1 pkt 24 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 1998 r. w sprawie instrukcji kancelaryjnej dla organów samorządu województwa⁴ **nośnik informatyczny** to:

¹ Postulaty *de lege ferenda* zostały uwzględnione w obu projektach ustaw o podpisie elektronicznym. UoP-P rozszerza domniemanie autentyczności z art. 245 KPC na dokumenty elektroniczne podpisane bezpiecznym podpisem elektronicznym (art. 5 ust. 3). Analogiczny przepis zawiera UoP-Rz (art. 5 ust.4). Zajęto wyraźne stanowisko w kwestii wnoszenia pism w drodze elektronicznej – wyraźnie dopuszczając taką możliwość (art. 5 ust. 4 UoP-P odnosi się wyłącznie do art. 63 KPA, ust. 5).

² W oznaczeniu ustalonym przez art. 1 ustawy z dnia 24 maja 2000 r. o zmianie ustawy - Kodeks postępowania cywilnego, ustawy o zastawie rejestrów i rejestrze zastawów, ustawy o kosztach sądowych w sprawach cywilnych oraz ustawy o komornikach sądowych i egzekucji (Dz. U. 2000 r. Nr 48 poz. 554).

³ Nie ma natomiast rozporządzenia o którym mowa w art. 125 § 4. Minister Sprawiedliwości określi, w drodze rozporządzenia, szczegółowe zasady i termin wprowadzenia techniki informatycznej, warunki, jakim powinny odpowiadać elektroniczne nośniki informatyczne, na których pisma procesowe mają być wnoszone, tryb odtwarzania danych na nich zawartych oraz sposób ich przechowywania i zabezpieczania, uwzględniając stan wyposażenia sądów w odpowiednie środki techniczne i poziom rozwoju technik informatycznych.

⁴ Art. 3 pkt 24 Instrukcji kancelaryjnej dla organów samorządu województwa, Dz.U. 1073/160/1998 (R)

dyskietka, taśma magnetyczna lub inny nośnik, na którym zapisano w formie elektronicznej treść dokumentu, pisma itp.

Dokument utrwalony jest na nośniku pamięci masowej tj. fizycznie istniejącej jako rzecz w rozumieniu prawa rzecznego. Wydaje się jednak, że nie przekroczymy granic interpretacji, jeżeli w drodze wykładni rozszerzającej (*a simili*)¹ założymy, że zakres zastosowania art. 125 §2 KPC obejmuje wnoszenie pism procesowych *online*.

Art. 126 §1 pkt4 KPC wprowadza jako *conditio sine qua non* pisma procesowego podpis strony albo jej przedstawiciela ustawowego lub pełnomocnika. Pytaniem zasadniczym jest czy podpis ten musi być własnoręczny? Postanowienie SN z 17.04.1967r. stanowi, że:

„Nie ma żadnych uzasadnionych powodów, aby podpis w rozumieniu przepisów procesowych rozumieć inaczej niż podpis w rozumieniu prawa cywilnego materialnego”

Odtworzony mechanicznie na piśmie procesowym wzór podpisu nie czyni zadość wymogowi, przewidzianemu w art. 126 § 1 pkt 4 KPC”².

Pisma procesowe wnoszone na elektronicznym nośniku informatycznym z przyczyn obiektywnych nie mogą zostać sygnowane podpisem w rozumieniu prawa cywilnego materialnego.

Znacznie bardziej elastyczne stanowisko prezentuje linia orzecznicza niemieckiego Trybunału Federalnego (*Bundesgerichtshof BGH*)³. BGH wychodząc od konstytucyjnej zasady prawa obywateli do sądu dopuszcza możliwość wnoszenia pism procesowych za pośrednictwem faksu. Prawo takie występuje również w tych przypadkach gdzie ZPO podobnie jak KPC wprowadza obowiązek złożenia podpisu pod pismem procesowym, np. § 130 Abs. 1 ZPO⁴. Warunkiem skuteczności takiego wniesienia jest, aby oryginał dokumentu, którego kopia za pośrednictwem faksu trafia do sądu, nie budził wątpliwości co do swojej **treści** oraz **woli** autora wywołania określonych skutków prawnych. W taki sposób wnosić można wszystkie pisma oraz środki odwoławcze z wyjątkiem pism procesowych przygotowawczych. Zasada ta nie dotyczy pism procesowych, dla których przepisy szczególnie wymagają własnoręcznego podpisu dla ważności pisma.

KPC konieczność złożenia podpisu własnoręcznego (tj. oryginalnego i autentycznego) rozciąga na wszystkie pisma procesowe. Inaczej ZPO, gdzie

¹ Analogia legis stosujemy wówczas, gdy sens językowy przepisu jest niejasny, S. Wronkowska, Z. Ziembicki *op.cit.* str. 168

² Postanowienie SN II PZ 22/67 *op.cit.*

³ Patrz szerzej Stanisław Rudnicki: Współczesne problemy formy czynności prawnych w świetle judykatury niemieckiej, MoP 7/1997 str. 272 i nast.

⁴ „Die vorbereitenden Schriftsätze sollen enthalten: (...) in Anwaltsprozessen die Unterschrift des Anwalts, in anderen Prozessen die Unterschrift der Partei selbst oder desjenigen, der für sie als Bevollmächtigter oder als Geschäftsführer ohne Auftrag handelt.“

wymóg ten obejmuje jedynie przypadki *expressis verbis* wskazane. W pozostałych przypadkach wystarczająca jest kopia podpisu na wydruku faksu (ale tylko wówczas, gdy oryginał w ogóle istnieje). Momentem wniesienia pisma jest zakończenie wydruku kompletnego dokumentu przez faks odbiorcy (sądu). Ryzyko ewentualnych zakłóceń transmisji, niemożności zakończenia wydruku z przyczyn zawinionych przez odbiorcę, etc., najczęściej obciąża odbiorcę.

W ramach art. 126 § 1 pkt 4 KPC należy przede wszystkim odejść od tak wąskiego znaczenia pojęcia „podpis”. Wymóg własnoręczności podpisu zredukowany powinien zostać do niezbędnego minimum, do taksatwnie wskazanych przypadków. A *contrario* uznać należy za wystarczające dla zrealizowania funkcji podpisu, sygnowanie dokumentu kopią podpisu, lub jego substytutem (podpisem elektronicznym). Nie eliminuje to oczywiście samego problemu podpisania pisma utrwalonego na elektronicznym nośniku informatycznym. Poza możliwością skorzystania z podpisu elektronicznego spotkać można rozwiązanie alternatywne¹. Wskazuje się, że do pisma utrwalonego na nośniku informatycznym dołączyć należy podpisane własnoręcznie przez podawcę oświadczenie. Mam jednak wątpliwości o zachowanie *ratio legis* tego rozwiązania w takim przypadku. Wyjaśnij przypadek wnoszenia pism *online* oraz stosowania podpisu elektronicznego, wnoszenie pism w postaci elektronicznej połączonych z pisemnym oświadczeniem traci jakiekolwiek uzasadnienie. Nie przemawiają za tym ani względy pragmatyczne, ani tym bardziej bezpieczeństwo i pewność obrotu. Jednym, ale zupełnie ważkim argumentem za, jest trwałość i koszt nośnika.

Art. 130¹ § 2 KPC dotyczy zwrotu pisma nie wniesionego na elektronicznym nośniku informatycznym (wówczas, gdy było to wymagane) albo na nośniku nie odpowiadającym przypisanym mu warunkom², lub nie mogącego otrzymać biegu z powodu innych braków formalnych. Wobec braku w/w rozporządzenia trudno powiedzieć, czy sąd ma obowiązek dokonać zwrotu z wykorzystaniem takich samych środków technicznych, którymi posłużyono się do wniesienia pisma. Ustawodawca w ogólne nie zajmuje w tym zakresie stanowiska. Moim zdaniem na tak postawione pytanie należy udzielić odpowiedzi negatywnej. Za takim rozstrzygnięciem przemawia chociażby treść art. 130¹ § 4 KPC:

„W terminie tygodniowym od dnia doręczenia zarządzenia o zwrocie pozwu powód może wnieść go ponownie. Jeżeli pozew nie jest dotknietý brakami, wywołuje skutek od daty pierwotnego wniesienia. Skutek taki nie następuje w razie kolejnego zwrotu pozwu”.

¹ Więcej patrz Arkadiusz Bieliński: Potwierdzenie na ekranie, RP 06.06.2000

² Określonym przez Ministra Sprawiedliwości w rozporządzeniu wydanym na podstawie art. 125 § 4 KPC

Chodzi głównie o problem doręczenia zarządzenia w kontekście zachowania terminu do ponownego wniesienia pozwu (nie przysługuje natomiast prawo do wniesienia zażalenia na zarządzenie o zwrocie pozwu przewidziane w art. 394 § 1 pkt 1 KPC).

Stanowisko takie uzasadnić należy głównie nienajlepszą jakością polskiej infrastruktury telekomunikacyjnej. W rezultacie priorytet przyznać należy prawu do sądu. Prawo to byłoby zagrożone, jeżeli przyjąć by doręczenia *online*. Łatwo bowiem dojść by mogło do uchybienia bardzo krótkiego (tygodniowego) terminu. Zupełnie odmiennie należy rozważyć przypadek, kiedy strona jest reprezentowana przez zawodowego pełnomocnika. Należy przyjąć domniemanie, że działający profesjonalnie pełnomocnik wyposażony jest w zaplecze techniczne umożliwiające mu skutecną i pewną komunikację elektroniczną. Tu można by ewentualnie pokusić się o dopuszczalność takiego doręczenia.

Natomiast żadnych sprzeciwów nie budzi sama idea wnoszenia pism na elektronicznych nośnikach informatycznych. Sąd bowiem jest instytucją, która powinna stwarzać takie możliwości, z zastosowaniem nowoczesnej techniki, nawet w całodobowym wymiarze. Samo rozwiązanie zwiększy niewątpliwie i w perspektywie również uproszczy dostęp obywateli do organów wymiaru sprawiedliwości.

Uregulowanie jest jeszcze dosyć mało wyraziste i wymaga dużego wkładu legislacyjnego, a także zaangażowania doktryny i judykatury. Mimo pojawiających się wątpliwości i niebezpieczeństw wskazany kierunek jest niewątpliwie słuszny.

2. MOC DOWODOWA DOKUMENTU ELEKTRONICZNEGO¹.

Systemy elektronicznego przetwarzania i przesyłania danych coraz częściej znajdują zastosowanie dla wymiany informacji w obrocie handlowym. Dane dotychczas utrwalane na papierze są, w celu ich archiwizacji digitalizowane. Korzyści wynikające ze stosowania mediów elektronicznych są powszechnie znane:

- szybkość wytwarzania i obiegu dokumentów
- oszczędność miejsca, dane w postaci cyfrowej zajmują mniej miejsca, łatwiej też zorientować się w zawartości takiego archiwum
- niższe koszty, etc.

¹ Bardzo głęboką analizę problemu, wykraczającą jednak poza ramy niniejszego opracowania zawiera artykuł Thomasa Deutscha: Die Beweiskraft elektronischer Dokumente, JurPC Web-Dok. 188/2000 <http://www.jurpc.de/ausatz/20000.188.htm> - fn0

Praktyczne korzyści, jakie oferują media elektroniczne podmiotom nimi się posługującym nie rekompensują, przynajmniej na razie, trudności, jakie pojawiają się w związku z tym na płaszczyźnie dowodowej.

Na doktrynalną definicję dokumentu cyfrowego trafić można w literaturze niemieckiej. Dokumentem cyfrowym są takie oświadczenia, które zostały utrwalone, przy pomocy cyfrowej maszyny matematycznej (komputera), na możliwych do odczytu elektronicznych nośnikach danych¹.

KPC nie zawiera definicji legalnej dokumentu. Art. 244 i 245 wskazują jedynie wymagania co do jego treści i dokonują, z punktu widzenia mocy dowodowej, dychotomicznego podziału dokumentów na urzędowe i prywatne. Obie kategorie korzystają z domniemania autentyczności², co oznacza, że dokument został wystawiony przez osobę, która go podpisała. Dokument urzędowy korzysta nadto z domniemania prawdziwości. Stanowi on dowód tego, co zostało w nim urzędowo zaświadczenie. W przypadku dokumentów prywatnych domniemanie obejmuje wyłącznie fakt, że osoba, która go podpisała, złożyła oświadczenie o takiej właśnie treści³. Nie rozciąga się ono na zgodność tego oświadczenia z rzeczywistym stanem rzeczy⁴.

Nie budzi zasadniczo prawniczych sprzeciwów wykorzystanie jako środka dowodowego wydruku komputerowego. Przez wydruk komputerowy należy rozumieć dokument, który stanowi graficzne przedstawienie danych utrwalonych na elektronicznym nośniku informatycznym. Wydruk stanowi więc kopię danych przechowywanych w postaci elektronicznej. „(...) do wydruków z komputera odpowiednie zastosowanie mają przepisy o dokumentach, w szczególności art. 244 KPC dotyczący dokumentów urzędowych (...)”⁵. Wydruk komputerowy musi być wyrażony na piśmie, ściślej pismem alfabetycznym (literami i cyframi)⁶. Zaprezentowanie dokumentu w postaci źródłowej (np. edycja binarna, etc.) nie ma charakteru pisma⁷. Dla mocy dowodowej dokumentu konieczne jest również, co do zasady, jego podpisanie⁸. Anonim nie stanowi bowiem i nie może stanowić

¹ Stefan Abel *op. cit.* – formułuje pytanie, czy reguły dowodowe przyjęte dla dokumentów papierowych znajdują tu również zastosowanie?

² Patrz także art. 5 ust. 3 UoP-P: „Postanowienia kodeksu postępowania cywilnego regulujące domniemanie autentyczności treści podpisanej dokumentu prywatnego, odnoszą się także do dokumentów elektronicznych opatrzonych bezpiecznym podpisem elektronicznym.”

³ „Dokument prywatny nie korzysta z domniemania prawdziwości zawartych w nim oświadczeń, każda zaś osoba mająca w tym interes prawy może twierdzić i dowodzić, że treść złożonych oświadczeń nie odpowiada stanowi rzeczywistemu.” Postanowienie SN z dnia 15.04.1982 III CRN 65/82 niepublikowane

⁴ Jerzy Jodłowski, Zbigniew Resich, Jerzy Lapierre, Teresa Misiuk-Jodłowska: Postępowania cywilne, Warszawa 1997 str. 336

⁵ Kazimierz Piasecki (red.): Kodeks postępowania cywilnego z komentarzem, Warszawa 1989

⁶ Tak Krzysztof Knoppek *ibidem*

⁷ Pogląd nie jest jednolity, patrz rozdział V pkt 3

⁸ „Niepoświadczona podpisem strony kserokopia nie jest dokumentem (...)” uchwała SN z dnia 29.03.1994, IIICZP 37/94, OSNCP 1994/11/206, z uzasadnienia „(...) kpc nie zna pojęcia kserokopii (podobnie jak

żadnego dowodu w sprawie rozpoznawanej przez organy wymiaru sprawiedliwości¹. Z drugiej strony złożenie podpisu *in blanco* nie ma charakteru złożenia „podpisu pod dokumentem” w rozumieniu art. 78 KC, chyba że jest to np. weksel *in blanco*².

Zagadnienie mocy dowodowej dokumentu elektronicznego nie doczekało się w Polsce głębszej analizy. Celowe wydaje się więc sięgnięcie do dorobku niemieckiej doktryny, inną natomiast kwestią jest czy są to poglądy dla nas właściwe.

Główny problem dotyczy definicji dokumentu w znaczeniu procesowym. Zdaniem doktryny § 415 ZPO należy rozumieć w ten sposób, że dokumentem jest pisemne ucieśnienie myśli ludzkiej³. Reprodukcje oryginału w postaci zapisów dźwiękowych⁴, wideo i innych nie stanowią dokumentu w powyższym znaczeniu. Dokumentem nie są również dane przesyłane za pośrednictwem EDV z uwagi na brak bezpośredniego dostępu do ich treści. Odtworzenie dokumentu wymaga zastosowania środków technicznych. Identyczne zresztą stanowisko zajmuje doktryna polska: „*Za dokument nie można uznać pism zaszyfrowanych lub zakodowanych, a sąd nie ma żadnego obowiązku dekodowania takich tekstów lub łamania zastosowanych w nich szyfrów*⁵.“ Tymczasem każda dana zapisana na elektronicznym nośniku informatycznym jest zakodowana sama przez siebie, jest zapisana w formacie zapisu charakterystycznym dla tej danej. Dominujące stanowisko przyjmuje, że dokumentu cyfrowego nie da się podciągnąć wprost pod środek dowodowy w znaczeniu procesowym.

Z procesowego punktu widzenia dokument tradycyjny ma do zrealizowania dwie funkcje:

- obiegowość
- zapewnia niezmienność treści złożonego oświadczenia (*verba volant scripta manent*)

wydruku komputerowego), jako pojęciem przeciwnym pojęciu oryginału posługuje się pojęciem odpisu. Skoro jednak tak odpis, jak kserokopia stanowią odwzorowanie oryginału (...) to istnieje podstawa do objęcia pojęciem podpisu także kserkopii (...).” – dopuszczalność rozciągnięcia tego stanowiska SN na wydruk komputerowy nie budzi wątpliwości.

¹ Wyrok SN z dnia 09.12.1980, II URN 171/80, OSP 1981/7/126 „*Anonim jest z istoty swej zjawiskiem niemoralnym, nie akceptowanym przez społeczeństwo i jako taki nie może być nigdy i w żadnym kontekście brany pod uwagę przez sąd*”.

² Stanisław Dmowski, Stanisław Rudnicki *op. cit.* Str. 256

³ Schreiber: Die Urkunde im Zivilprozeß, 1982r. str. 32

⁴ Art. 308 § 1 i 2 KPC do dowodu z taśmy stosuje się odpowiednio przepisy o dowodzie z oględzin oraz o dowodzie z dokumentów; patrz również wyrok SN z dnia 10.01.1975, II CR 752/74, (niepublikowane).

⁵ Krzysztof Knoppek *op.cit.*

Pojawia się więc pytanie, czy „niepisemny” oznacza automatycznie „nieobiegowy” i „nieautentyczny”¹?

Według niemieckiej doktryny obiegowość dokumentu oznacza możliwość przyjęcia do wiadomości w każdym czasie myśli inkorporowanej w jego treści. Z tych powodów nie mają mocy dowodowej dokumentu zapisy dźwięku czy obrazu². Niektórzy prawnicy zdają się nie dostrzegać zasadniczej różnicy pomiędzy zapisem na elektronicznym nośniku danych, a zapisem dźwięku czy obrazu. Bardzo mocno eksponuje się również konieczność zaangażowania środków technicznych w proces odczytania treści takiego dokumentu. Nie można obecnie przytoczyć prawnych argumentów na rzecz odmiennego stanowiska. W literaturze niemieckiej wskazuje się jednak zdroworozsądkowo, że „uciążliwość” w postaci środków technicznych mocno się zdewaluowała, komputer bowiem stał się standardowym wyposażeniem biura (w tym sądów) tak jak np. „(...) lampa czy okulary do czytania (...)”³. Takiego argumentu nie można traktować poważnie w dyskursie o mocy dowodowej dokumentu elektronicznego (pomijając zupełnie okoliczność, że bardziej odnosi się on do niemieckiej, niż polskiej rzeczywistości). Sugeruje on wyłącznie potrzebę rewizji przestarzałego stanowiska.

Nie sposób również dostrzec istotnej różnicy pomiędzy dokumentem elektronicznym, a dokumentem, co prawda pisemnym, lecz sporządzonym w języku obcym lub pismem Braille'a. Zwłaszcza w tym drugim przypadku zachodzi konieczność uprzedniego przetłumaczenia tekstu, który nie jest dostępny wprost, ani zapisany pismem alfabetycznym.

Powszechnie wśród atutów dokumentu papierowego wskazuje się, że jego treść może tkwić w martwym punkcie i pozostawać niezmienną praktycznie tak długo jak długo istnieje sam nośnik. Wszelkie zmiany w treści dokumentu są zazwyczaj od razu widoczne.

Dla rozstrzygnięcia o mocy dowodowej dokumentu elektronicznego pozostaje jeszcze kwestia podpisu na dokumencie. Jak była już o tym mowa, termin „podpis” rozumieć należy tak samo, jak na gruncie prawa materialnego. Podpis musi więc być własnoręczny, kopia nie czyni zadość wymogowi własnoręczności (nie realizuje funkcji podpisu). Nie będzie zatem dokumentem w powyższym znaczeniu wydruk faksu, który nie zawiera oryginału podpisu (mimo, że podpis ten jest autentyczny).

¹ Stefan Abel *op.cit.*

² Możemy spotkać się z określeniami np. „audiodokumentu” – tak np. Brunon Hołyst: Kryminalistyka, Warszawa 1996 str. 508 „Dla odróżnienia w sensie merytorycznym i formalnym dokumentu klasycznego wprowadzono termin „audiodokument”, którym może być taśma magnetofonowa (...”).

³ Stefan Abel *op.cit.*

Niemiecka optyka własnoręczności podpisu nie jest jednoznaczna. Judykatura i część doktryny stoi na stanowisku, że bezwzględnie niezbędne jest złożenie własnoręcznego podpisu¹, inni są zdania, że wystarczy chociażby podpisanie dokumentu na maszynie (w odniesieniu do dokumentu prywatnego §§ 416, 440 Abs. 2 ZPO)². Brak sztywnego stanowiska, że podpisowi w procesowym ujęciu nadać należy materialnoprawne znaczenie³. Przyjmuje się więc, nieco *contra legem*, że dokument cyfrowy (*digitale Dokument*) z certyfikatem licencjonowanego wystawcy (*anerkannten Zertifizierungsstelle*) oraz dokumenty cyfrowe utrwalone na elektronicznych nośnikach danych jednokrotnego zapisu (*nicht überschreibbare Datenträger*), należy na gruncie powyższych wątpliwości traktować jako podpisany dokument. Z procesowego punktu widzenia są one równorzędne dokumentom tradycyjnym⁴. Taka konstatacja stanowi oczywiście wyłącznie pogląd i postulat części doktryny.

W rzeczywistości, tzn. patrząc obiektywnie, nie da się „dokumentu cyfrowego” podciągnąć do końca pod kryteria stawiane przez KPC czy ZPO. Stąd postulat *de lege ferenda* wprowadzenia zupełnie nowych przepisów normujących dowód z dokumentu elektronicznego, względnie rozszerzenie zakresu zastosowania przepisów dotychczasowych. Akty Komisji UE zobowiązują państwa członkowskie do usankcjonowania równorzędnej z dokumentem tradycyjnym mocy dowodowej dokumentu cyfrowego, podписанego cyfrowo⁵.

¹ Tak orzeczenie BGH NJW 1774/1992 (patrz również orzeczenia, w których telekopia pisma ma moc oryginału, np. BGH IVa ZB 7/89, NJW 1990, z tym że chodzi tu wyłącznie o skutek wniesienia pisma faksem, a nie moc dowodową dokumentu).

² Tak Baumbach, Lauterbach, Albers, Hartman, ZPO, 1998

³ „§ 126. (1) Ist durch Gesetz schriftliche Form vorgeschrieben, so muß die Urkunde von dem Aussteller eigenhändig durch Namensunterschrift oder mittels notariell beglaubigten Handzeichens unterzeichnet werden.“

⁴ Stefan Abel *op.cit.*

⁵ Art. 5 Abs. 2/b Mitteilung der Kommission vom 16.4.1997, KOM (97), 157 „(...) daß digitale Dokumente in Gerichtsverfahren in gleicher Weise wie handschriftliche Unterschriften zugelassen sind (...).“

Rozdział VII**ZAKOŃCZENIE**

Zamierzeniem moim nie było udzielenie odpowiedzi na podstawowe pytania prawne, które towarzyszą elektronicznemu przekazowi danych. Nie najważniejsze są również trudności, jaki temu towarzyszą. Bardziej celowa, od przebudowy systemu prawnego, wydaje się bowiem głęboka refleksja nad nadchodzącymi zmianami. Wydaje mi się, że kluczem do rozwiązania większości problemów jest przede wszystkim należyte zrozumienie i zaakceptowanie specyfiki elektronicznego obrotu, jego masowego i globalnego charakteru. Wydaje się być wyłącznie kwestią czasu przełamanie uprzedzeń i obaw związanych z zastosowaniem mediów elektronicznych w codziennym życiu prawnym. Niebanalną rolę społeczną mają do spełnienia w tym zakresie inicjatywy legislacyjne oraz edukacja społeczeństwa, realizowana przez instytucje publiczne¹.

Podsumowując powyższe rozważania wskazać należy, iż:

- 1) Rzeczą najistotniejszą jest ujednolicenieję pojęć w obrębie obrotu elektronicznego. Brak zrozumiałych, a przede wszystkim jednoznacznie sformułowanych definicji stanowi główną siłę sprawczą wielu dylematów prawnych. Niejednokrotnie stawiane przez prawników pytania odnoszą się do zakresu zastosowania definicji już istniejących. Chodzi więc o akceptowalne granice swobody interpretacyjnej.
- 2) W zakresie absolutnie niezbędnym konieczna jest również interwencja ustawodawcy. Interwencja ponad niezbędnego minimum nie tylko jest niepożądana, ale wręcz szkodliwa. Nie sposób bowiem wprowadzać dualizmu rozstrzygnięć w obrębie tożsamykh instytucji prawnych, np. odrębnych przepisów dla wad oświadczeń woli składanych z wykorzystaniem elektronicznego medium transmisji danych. Wydaje się, że istniejące w tym zakresie instrumentarium prawne jest wystarczające. Konieczne jest jedynie jego wzbogacenie o specyficzne dla

¹ Niedostatek wiedzy próbuje eliminować m.in. wrocławska ELba CSB S.A., która stworzyła wirtualny home banking <http://homeb.elbacsb.com.pl-bankwirtualny/>. Można tu przeciwiczyć „na sucho” tzn. bezangażowania prawdziwych pieniędzy działanie różnych funkcji oprogramowania związanych z obsługą rachunków przez Internet. Więcej na ten temat: Zbigniew Zwierzchowski, *ibidem*

społeczności internetowej zwyczaje i praktyki oraz linię orzecznictwa. Obszarami, gdzie interwencja ustawodawcy jest niezbędna, są zwłaszcza ustawowe przesłanki formy pisemnej. Do tej pory udało się jedynie rozwiązać problem doniosłości prawnej podpisu, co jest w gruncie rzeczy problemem najprostszym. Na horyzoncie jawi się już problem zupełnie inny tj. wzajemnego stosunku pomiędzy „formą elektroniczną” (jeżeli taka w ogóle powstanie) a katalogiem form szczególnych. Problem dotyczy ich wzajemnej egzystencji tudzież wyeliminowania tych ostatnich przez formę elektroniczną. Przyjęcie drugiego scenariusza otworzyć może problem wewnętrznego podziału formy elektronicznej.

- 3) Obszarem wielu pytań i wątpliwości jest moc dowodowa dokumentów istniejących tylko w postaci elektronicznego zapisu.
- 4) Konieczne jest wypracowanie zwyczajów lub zajęcie wspólnego stanowiska, co do większości zagadnień z zakresu treści czynności prawnych¹.
- 5) Masowy i globalny obrót elektroniczny wymaga zastosowania rozwiązań ujednoliconych i standardowych, jednakowych dla wszystkich uczestników tego obrotu.

Celem moim nie było znalezienie odpowiedzi na możliwe do postawienia pytania. Chodziło mi wyłącznie o zaprezentowanie poglądów doktryny i judykatury na pytania już postawione, wskazanie w jaki sposób można radzić sobie w nowych warunkach, mając do dyspozycji określony surowiec prawny. Chciałem zasygnalizować aktualne trendy i zmiany, jakich spodziewać się możemy w przyszłości.

Najlepiej sytuację, w której się obecnie znajdujemy oddają słowa ks. prof. Andrzeja Dzięgały wypowiedziane na zakończenie konferencji naukowej zorganizowanej na Katolickim Uniwersytecie Lubelskim w grudniu 1998 roku:

¹ Przykładem takich zwyczajów mogą być wytyczne OECD dotyczące ochrony klientów korzystających z handlu elektronicznego, mają one stanowić również wzór „najlepszych praktyk” handlowej działalności *online*.

Szerzej Wojciech Łegowski, Computerworld, 13.12.1999,
<http://wwwcomputeworld.pl/wiadomości/archiwum/1/6/1653.asp>

„(...) Zjawisko globalizacji postępuje (...) od wielu dziesiątek lat. Stąd moje przekonanie, że ani prawnicy, ani systemy prawne wcale się dzisiaj nie spóźniają. Wprost przeciwnie, jeżeli ktokolwiek, to właśnie prawnicy, stosując obowiązujące aktualnie normy prawne, potrafią udzielić możliwie najbardziej konkretnych odpowiedzi na najbardziej ogólnie pytania (...)¹”.

¹ Cytat pochodzi z książki: Internet – problemy prawne, Lublin 1999



BIBLIOGRAFIA

- 1) S. Abel: Urkundenbeweis durch digitale Dokumente, „Multimedia und Recht“ nr 12/98
- 2) J. Barta, R. Markiewicz: Prawo sieci informatycznych, „Rzeczpospolita“ 26.03.1997
- 3) J. Barta, R. Markiewicz: Transakcje, które biegają po łączach, „Rzeczpospolita“ 10.04.1998
- 4) J. Barta, R. Markiewicz: Internet a prawo, Kraków 1999
- 5) A. Bieliński: Potwierdzenie na ekranie, „Rzeczpospolita“ 06.06.2000
- 6) D. Cwiklek: Poemat w Pascalu, <http://www.odeon.pl/>
- 7) W. Czachórski (red.): System prawa cywilnego – część ogólna tom1, Wrocław-Warszawa-Kraków-Gdańsk 1974
- 8) T. Deutsch: Die Beweiskraft elektronischer Dokumente, „JurPC“ <http://www.jurpc.de/ausatz/20000.188.htm> - fn0
- 9) S. Dwowski, S. Rudnicki: Komentarz do kodeksu cywilnego, Warszawa 1999
- 10) B. Dunaj (red.): Słownik współczesnego języka polskiego, Warszawa 1996
- 11) T. Erciński: Z problematyki dowodu z dokumentu w sądowym postępowaniu cywilnym, Warszawa 1985
- 12) S. E. Heun: Die elektronische Willenserklärung, „Computer und Recht“ nr. 10/1994
- 13) B. Hołyś: Kryminalistyka, Warszawa 1996
- 14) J. Jacyszyn: Elektroniczne czynności prawne, „Przegląd Prawa Handlowego“ nr 7/1999
- 15) Z. Janowicz: Kodeks postępowania administracyjnego – komentarz, Warszawa 1999
- 16) O. Jauering (red.): Bürgerliches Gesetzbuch, München 1979
- 17) A. Jędrzejewska: Oświadczenie woli składane za pomocą komputera, „Państwo i Prawo“ nr 3/1992
- 18) A. Jędrzejewska: Pisemna forma oświadczenia woli a „automatyzacja“ obrotu prawnego: „Państwo i prawo“ nr 1/93

- 19) J. Jodłowski, Z. Resich, J. Lapierre, T. Misiuk-Jodłowska: Postępowania cywilne, Warszawa 1997
- 20) D. Kraszewski: raport „eHandel w Polsce”
<http://www.arthurandersen.com.pl/>
- 21) Khun: Rechtshandlungen mittels EDV und Telekommunikation, 1991
- 22) K. Knoppek: Wydruk komputerowy jako dowód w procesie cywilnym, „Państwo i Prawo” nr 2/1993
- 23) W. Kocot: Zawarcie umowy w drodze elektronicznej wymiany informacji, „Przegląd Prawa Handlowego” nr 4/98
- 24) A. Z. Makowiecki (red.): Literatura i nauka o języku, Warszawa 1995
- 25) D. Medicus: Allgemeine Teil des Bürgerliches Rechts, 1994
- 26) J. Mehrings: Vertragsabschluß im Internet, „Multimedia und Recht“ nr. 1/1998
- 27) P. Müller (red.): Leksykon informatyki, Warszawa 1977
- 28) K. Piasecki (red.): Kodeks postępowania cywilnego z komentarzem, Warszawa 1989
- 29) Z. Radwański: Prawo cywilne-część ogólna, Warszawa 1997
- 30) Z. Radwański: Teoria umów, Poznań 1977
- 31) Z. Radwański, J. Panowicz-Lipska: Zobowiązania – część szczegółowa, Warszawa 1996
- 32) S. Rassmann: Elektronische Unterschrift im Zahlungsverkehr, „Computer und Recht“ nr 1/1998
- 33) F. Rosengarten: Podpis i jego znaczenie w prawie cywilnym, „Palestra” nr 1/1973
- 34) A. Roßnagel: Elektronische Signaturen in Europa, „Multimedia und Recht“ nr 12/98
- 35) S. Rudnicki: Współczesne problemy formy czynności prawnych w świetle judykatury niemieckiej, „Monitor Prawniczy” nr 7/1997
- 36) W. Skubicki: Słownik terminologii prawniczej i ekonomicznej niemiecko – polski, Warszawa 1997
- 37) E. Sobol (red.): Słownik wyrazów obcych, Warszawa 1995
- 38) K. Stefanowicz: Podpis elektroniczny, „Biznes Polska” 25.01.2001,
<http://www.biznespolska.pl/>

-
- 39) A. Szpunar: Glosa do uchwały SN z dnia 31 maja 1994, III CZP 75/94, OSP 1995/2/33 - t.1
- 40) A. Szpunar: „Przegląd Notarialny” nr 6/98
- 41) G. Wiaderek: Internetowe czynności bankowe a forma pisemna czynności prawnych, „Internet 2000”, Lublin 2000
- 42) A. M. Wilk: Państwo w dobie Społeczeństwa Informatycznego – perspektywa strategicznych przemian, „Internet 2000”, Lublin 2000
- 43) S. Wronkowska, Z. Ziembicki: Zarys teorii prawa, Poznań 1997
- 44) Z. Zwierzchowski: Czek i bank w nowym wcieleniu, „Rzeczpospolita” 30.07.1998
- 45) Z. Żuławski: Podpis cyfrowy zalegalizowany, „Gazeta prawną” 14.03.2000
http://www.gp.infor.pl/grupa/gp_aktualności/aktualności/informatyka/podpis.html
- 46) Uzasadnienie wstępniego projektu rządowego ustawy o podpisie elektronicznym <http://www.vagla.eu.org/>
- 47) I i II Badanie Polskich Użytkowników Sieci Internet, Katedra Marketingu Akademii Ekonomicznej w Krakowie 1999/2000 <http://badanie.ae.krakow.pl/>
- 48) <http://www.centrum.pl/pl/index.html>
- 49) <http://www.edi.pl/>
- 50) <http://www.fortisbank.com.pl/services/PlanetPL.html>
- 51) <http://wiem.onet.pl/wiem/>
- 52) <http://www.un.or.at/uncitral/mainindx.htm>

Orzecznictwo:

- 1) Uchwała 7 sędziów SN z dnia 28.04.1973, III CZP 78/72, OSNC 1973/12/207
- 2) Uchwała SN z dnia 17.10 1979, III CZP 68/479, OSNCP 67/4/80
- 3) Uchwała 7 sędziów SN z dnia 05.06.1992, III CZP 41/92, OSNC 1992/9/147
- 4) Uchwała 7 sędziów SN z dnia 30.12.1993, III CZP 146/93, OSNC 1994/5/94
- 5) Uchwała SN z dnia 29.03.1994, IIICZP 37/94, OSNCP 1994/11/206
- 6) Uchwała SN z dnia 09.05.1995, III CZP 56/95, OSNC 1995/9/127
- 7) Wyrok SN z dnia 17.12.1966, I CR 447/66, OSNC 1967/9/153

-
- 8) Wyrok SN z dnia 24.01.1974, II CR 761/73, OSP 238/11/1975
 - 9) Wyrok SN z dnia 09.12.1980, II URN 171/80, OSP 1981/7/126
 - 10) Wyrok SN z dnia 10.09.1997, I PKN 251/97, OSNAPiUS 389/13/1998
 - 11) Postanowienie SN z dnia 17.04.1967, II PZ 22/67, (niepublikowane)
 - 12) Postanowienie SN z dnia 28.03.1995, SN I CRN 24/95, OSNC 1995/7-8/117
 - 13) Wyrok NSA z dnia 28.06.1983, I SA 268/83, ONSA 47/1/1983
 - 14) Wyrok SA w Poznaniu z dnia 18.06.1991, I ACr 151/91, OSA 21/4/1991
 - 15) Wyrok SA w Katowicach z dnia 17.08.1994, I ACr 312/94, „Wokanda” 8/95
 - 16) Wyrok SA w Katowicach z dnia 19.10.1995, I ACr 514/95
 - 17) Wyrok SA w Poznaniu z dnia 23.11.1995, I ACr 483/95, „Wokanda” 45/8/1996
 - 18) Wyrok SA w Lublinie z dnia 29.06.1999, I ACa 192/99
 - 19) Wyrok SA w Warszawie z dnia 9.02.1999, I ACa 1105/98, „Prokuratura i Prawo” – dodatek 35/2/2000