

## **Internet i prawo**

*Ryszard Tadeusiewicz*

---

---

Po długim okresie swobodnego rozwoju Internetu, kiedy brak jakichkolwiek uregulowań prawnych traktowany był jako podstawowy warunek osiągnięcia celów formułowanych przez Sieciową Społeczność, nadszedł czas na to, by zastanowić się nad sposobem skodyfikowania prawnego działań i zachowań Internautów. Sprawa nie jest prosta, gdyż globalny zasięg Internetu stwarza problemy legislacyjne nieznane wcześniej teoretykom i praktykom prawa. Jest jednak konieczna do rozwiązania, jeśli mają się dalej rozwijać fundamenty przyszłego Społeczeństwa Informacyjnego, takie jak na przykład sieciowa działalność gospodarcza. Żywiłowa komercjalizacja Internetu, jaka zachodzi w ostatnich miesiącach, pozostaje bowiem w jaskrawej sprzeczności z faktem braku istnienia jakiegokolwiek uregulowania prawnego nawet najbardziej podstawowych kwestii – między innymi tego, prawo jakiego kraju powinno być brane pod uwagę podczas realizacji działań handlowych w Sieci. Internet swobodnie przekracza wszelkie granice – polityczne, geograficzne, obyczajowe, kulturowe, religijne itd., a jednocześnie wymagamy, by gwarantował ekonomiczne bezpieczeństwo. Jest to antynomia, którą pokonać mogą tylko nowe rozwiązania prawne. Do pełnej i skutecznej kodyfikacji prawnej różnych działań w Internecie dojdzie na pewno dopiero za jakiś czas, gdyż obecnie piętrzą się w tym obszarze niezliczone trudności – na przykład przeszkodą dla wielu działań jest wciąż żywe przywiązanie większości Internautów do tradycyjnych wartości z okresu całkowitej swobody działań sieciowych. Jednak jak najszybciej trzeba wykonać pierwszy krok w zakresie prawnego porządkowania działań w Cyberprzestrzeni, gdyż potrzeby szybko narastają, a zagrożenie ze strony sieciowej anarchii, w jaką bardzo łatwo może się przerodzić internetowa wolność – są już teraz bardzo poważne. Tym pierwszym poważnym krokiem w dziele wprowadzania porządku prawnego w Internecie może i powinna być Ustawa o Podpisie Elektronicznym, zatem zagadnieniom tego właśnie uregulowania prawnego poświęcono w pracy wyjątkowo dużo miejsca.

---

---

### **Wprowadzenie**

Mówiąc i odmieniając przez przypadki nazwę „Społeczeństwa Informacyjnego” albo „Społeczności Internetu” mamy świadomość, że droga do tego nowego świata nie będzie prosta ani nie będzie oczywista. W trakcie konferencji, w której materia-

łach publikuję tę notatkę, podejmiemy i rozwiniemy wiele wątków, pokazujących jakie rafy trzeba będzie przebyć, zanim burzliwy nurt przemian ponownie rozleje się w spokojną, spławną rzekę cywilizacyjnego porządku. Jeśli jednak Internet oraz inne techniki informacyjne mają stać się „stosem pacierzowym” nowego modelu społeczeństwa, to trzeba koniecznie wprowadzić do nich zespół regulacji prawnych, stanowiącą bezpieczny punkt odniesienia dla przyszłych pokoleń. Trzeba jednak zdecydowanie stwierdzić, że na drodze do tego stanu docelowego jest jeszcze bardzo wiele przeszkód.

### **Prawo Internetu z perspektywy historycznej**

Dopóki Internet był wyłączną domeną uczonych, a potem także relatywnie nielicznych amatorów sieciowej komunikacji, dopóki był całkowicie (programowo!) oderwany od jakiegokolwiek działalności komercyjnej – był on obszarem, w którym prawo nie było potrzebne. Mało tego, w tym pionierskim okresie rozwoju Internetu brak jakiegokolwiek władzy, która by nim zarządzała, a zwłaszcza brak jakiegokolwiek formalnej regulacji normatywnie określającej kierunki jego rozwoju – był nawet traktowany jako swoisty manifest ideowy i stanowił jeden z zasadniczych dogmatów funkcjonowania międzynarodowej społeczności Internautów. Właśnie brak jakichkolwiek zasad prawnych (poza pewnym organizacyjnym nadzorem nad dystrybucją adresów i nazw domen) miał stymulować spontaniczny, nie ograniczony żadnymi formalnymi barierami, rozwój sieci. I rzeczywiście stymulował – bez tej wolności rozwój teleinformatyki z pewnością nie przebiegałby ani tak szybko, ani tak skutecznie, jak to można było obserwować na początku lat dziewięćdziesiątych. Nie oznaczało to bynajmniej, że w tych pionierskich czasach rozwoju Sieci było wszystko wolno! Gdy czyjeś zachowania godziły w swobody innych, na przykład gdy ktoś nagminnie produkował tzw. *spamy* – społeczność Internetu potrafiła skutecznie dokonać „samosądu” na niesfornym Internaucie – na przykład blokując mu skrzynkę lawiną automatycznie generowanych listów.

Funkcjonowała także i rozwijała się swoista „net-etykieta”, która wytworzyła nawet własny kod komunikatów i ich znaczeń – by przypomnieć tylko powszechnie używane do dzisiaj „emtikony”, na przykład uśmieški :- ) albo sekwencje znaków wyrażające smutek :-(. Powstało i nadal powstaje bardzo wiele innych ozdobników sieciowych komunikatów, które w istocie stanowią dosyć desperacką próbę przewyciężenia ograniczenia, jakie tekstowa forma prezentacji wszelkich przekazów stawia przed osobami chcącymi w Sieci wyrazić coś więcej, niż samą tylko „gołą” wiadomość, a zwłaszcza chcącymi przekazać przy okazji internetowego kontaktu z innymi ludźmi jakieś własne emocje. Jednak w pionierskim okresie funkcjonowania Internetu generalnie żadnych spisanych praw nie było, a w strukturach tej nowej Ziemi Obiecanej funkcjonowały w istocie zasady Dzikiego Zachodu, powodujące że nawet ewidentni sieciowi przestępcy (*hackerzy*, a także ich gorsza odmiana, tak zwani *crackerzy*) cieszyli się specyficzną sławą, podobnie jak legendarni rewolwerowcy *Far Westu*.

Sytuacja się zmieniła, gdy w Sieci pojawiła się działalność komercyjna. Gdy mowa o pieniądzach – kończą się żarty, znika wyrozumiałość dla ludzkich słabostek

albo poszanowanie dla czyjejś odmienności. W sprawach biznesowych przesyłana informacja musi być pewna, bezpieczna, nienaruszalna, niezaprzeczalna<sup>1</sup>. Przy załatwianiu interesów handlowych poprzez Internet pojawia się ponownie problem granic państw, które dzieli społeczność międzynarodową nie tylko w sensie politycznym, ale znacznie dotkliwiej – także w sensie gospodarczym.

### **Potrzeba prawa gospodarczego funkcjonującego w Sieci**

Rozwińmy odrobinę ten wątek, gdyż wydaje się ważny. Internet jest zwykle opisywany jako sieć komunikacyjna, która może swobodnie przekraczać granice państw, ustrojów i kontynentów. Jednak może to być konsekwentnie utrzymywane i kultywowane tylko wtedy, gdy Sieć służy wyłącznie *wymianie poglądów*. Gdy zaczyna służyć *wymianie towarów*, granice ponownie pojawiają się – tym razem jako bariery celne. Co prawda świat zmierza obecnie w kierunku globalizacji<sup>2</sup>, gospodarka wielu krajów staje się coraz bardziej otwarta, w blasku fleszy i w huku korków od szampana padają kolejne bariery – ale wciąż istnieją i jeszcze długo będą istnieć na świecie oddzielne systemy podatkowe, zróżnicowane strefy celne, rozmaite kordony sanitarne, a także inne bariery, które można ignorować w cyberprzestrzeni w ramach wymiany informacji, ale nie wtedy, gdy mowa jest o elektronicznym handlu. Internet może przyspieszyć usuwanie tych barier, co – jeśli nastąpi – będzie jedną z bezspornych zasług cywilizacyjnych globalnego usieciowienia! Na razie jednak bariery te **istnieją** – i nie można ich ignorować. Jeśli jednak bariery te mają poprawnie funkcjonować i nie mają być bardziej dolegliwe, niż absolutnie muszą – to ich działanie musi regulować (także wewnątrz Sieci) precyzyjnie spisane prawo. Zobaczmy, jak to jest obecnie.

### **Prawo Internetu w Unii Europejskiej**

Unia Europejska w sprawach legislacyjnych dotyczących Internetu, a w szczególności handlu elektronicznego najchętniej posługuje się dyrektywami<sup>3</sup>. Umożliwia to wskazywanie najważniejszych celów i wzywanie do ich realizacji, bez wymuszania na krajach członkowskich konkretnych metod ich osiągnięcia. Pozwala również na elastyczne dostosowywanie dróg rozwoju do specyfiki konkretnego państwa i jego rynku.

<sup>1</sup> Niezaprzeczalność informacji polega na tym, że nadawca komunikatu nie może się wyprzeć tego, że go wysłał, a więc musi ponieść wszelkie jego konsekwencje, nawet jeśli są dla niego bardzo niekorzystne. W handlu jest to bardzo ważne w kontekście nienaruszalności umowy handlowej także wtedy, gdy jej dotrzymanie przynosi ewidentną szkodę jednej z umawiających się stron.

<sup>2</sup> W dużej mierze zresztą właśnie za sprawą Internetu.

<sup>3</sup> Dyrektywy są najczęściej wydawane w celu harmonizacji prawa w państwach członkowskich Unii. Mają one charakter wiążący, ale nie normatywny, tzn. nie zawierają norm prawnych a wskazują jedynie zadania, które dane państwo ma zrealizować. Dobór środków do tego koniecznych jest wewnętrzną sprawą państwa–adresata. Kraj taki zobowiązuje się do wydania w określonym terminie przepisów wewnętrznych regulujących daną kwestię. Kontrola realizacji dyrektyw należy do Komisji Europejskiej, a w razie nieprawidłowości do Trybunału Sprawiedliwości.

Zgodnie z tą zasadą również główny dokument Unii traktujący o Internecie i o handlu elektronicznym jest wydany w postaci dyrektywy. *Dyrektywa o Handlu Elektronicznym*<sup>4</sup> [10] – bo o niej mowa – zapewnić ma, że organizacja prowadząca działalność opartą na infrastrukturze elektronicznej będzie mogła czerpać korzyści z unijnych priorytetów wolnego przepływu towarów i usług oraz ze swobody ustanawiania działalności gospodarczej. Najbardziej ogólnym założeniem jest uznanie prowadzonej zawodowo aktywności on-line za legalną w ramach Unii Europejskiej, jeśli tylko jest ona zgodna z prawem macierzystego kraju. Dyrektywa o e-commerce definiuje również sposoby identyfikacji lokalizacji firmy internetowej, precyzuje które dane muszą obowiązkowo być ujawniane przez prowadzących działalność, zawiera zasady zawierania umów w postaci elektronicznej oraz granice odpowiedzialności stron kontraktów, jak również sposoby rozstrzygnięcia sporów powstałych w wyniku działalności związanej z e-commerce.

Ogółem, dokument ten wymaga od państw członkowskich zapewnienia w ich systemach prawnych instrumentów pozwalających na zawieranie kontraktów w postaci elektronicznej. Jedynym wyjątkiem jest pozostawienie członkom Unii Europejskiej swobody decyzji w sprawie umów związanych z:

- obrotem nieruchomościami lub modyfikacją praw majątkowych co do nieruchomości,
- sukcesją praw i problemami będącymi w gestii kodeksu rodzinnego lub spadkowego,
- zaangażowaniem sądów lub innych organów publicznych,
- koniecznością zapewnienia szczególnego zabezpieczenia przez osoby nie związane bezpośrednio z samym kontraktem (np. naoczne opinie ekspertów).

Dyrektywa obejmuje swoim działaniem wszystkie rodzaje handlu elektronicznego, w szczególności kontakty firma–firma (B2B) i firma–klient (B2C). Przykładowymi formami działalności pozostającymi w obszarze zainteresowania Dyrektywy są internetowe wydania gazet, bazy danych dostępne on-line, internetowe usługi specjalistów (prawników, lekarzy, pośredników itp.), tzw. usługi *video on demand*<sup>5</sup> czy też marketing bezpośredni z użyciem Internetu. Założenia Dyrektywy nie odnoszą się natomiast w żaden sposób do działalności prowadzonej przez firmy, których siedziba mieści się w krajach nie będących członkami Unii Europejskiej.

### **Wybór właściwego prawa krajowego dla rozstrzygnięcia spraw w Internecie**

Jednym z najważniejszych problemów dotyczących Internetu jest odpowiedź na pytanie, prawo którego kraju jest w mocy, jeśli trzeba rozstrzygnąć ewentualne niejasności. Dopóki sprawa dotyczy działalności o małym zasięgu, na przykład małej firmy,

<sup>4</sup> Poniżej nazywana Dyrektywą.

<sup>5</sup> Czyli możliwość zamówienia określonego programu telewizyjnego (filmu, relacji sportowej) o danej godzinie dla konkretnego abonenta za pośrednictwem specjalnego łącza.

oferującej usługi czy prowadzącej sprzedaż wyłącznie na rynku lokalnym, kwestia ta nie ma znaczenia. Podobna sytuacja ma miejsce w przypadku przedsiębiorstw założonych na terenie Unii i prowadzących międzynarodową działalność internetową, lecz na niewielką skalę (np. wysyłka towarów zamówionych pocztą elektroniczną). Dyrektywa rozstrzyga po prostu, że firma tego typu jest podmiotem prawa tego kraju, w którym ma siedzibę. Dopóki więc takie przedsiębiorstwo działa w zgodzie z lokalnym ustawodawstwem, ma pełną swobodę prowadzenia interesów na terenie Unii.

Istnieją także przypadki wyjątkowe. Pewne obszary działań muszą być traktowane na odmiennych zasadach, niezależnie od skali przedsięwzięcia – między innymi ze względu na obostrzenia nałożone przez inne dyrektywy. Przykładowo, niekiedy wymagane jest zastosowanie prawa tej strony umowy, która jest odbiorcą, może się też zdarzyć, że skorzystanie z prawodawstwa oferenta jest niemożliwe ze względu na niewystarczające instrumenty legislacyjne lub niedostateczną ochronę konsumenta – wtedy zastosowanie znajduje kodeks kraju odbiorcy.

Dla przedsiębiorstw działających na większą skalę i w pełni spełniających wymogi kwalifikujące je do kategorii e-commerce tak proste rozwiązania mogą okazać się niewystarczające, gdyż zasady dotyczące zawierania kontraktów i ich ważności zwykle różnią się w poszczególnych krajach. Na przykład ta sama prezentacja produktu w jednym państwie może być wiążącą ofertą w świetle kodeksu handlowego, w innym nie. Dlatego konieczne było wprowadzenie dodatkowych instrumentów, uściślających zasady aplikacji prawa.

W przypadku umów pomiędzy firmami (B2B e-commerce) generalnie przyjmuje się, że stosowane jest prawo kraju wyraźnie wskazanego przez strony w treści kontraktu. Firmy obdarzone są więc swego rodzaju autonomią tak, by opierając się na swojej wiedzy i dotychczasowych doświadczeniach mogły uzgodnić rozwiązania dla siebie najkorzystniejsze. Obie strony kontraktu mają tutaj taki sam wpływ na przyjęty model i tylko od wyniku negocjacji zależą końcowe uzgodnienia. W praktyce najczęściej zdarza się, że dostawcy dążą do budowania wszystkich umów zawieranych poprzez internetową stronę WWW – lub inne platformy elektroniczne – z zastosowaniem ich rodzimego prawa, by móc potem korzystać ze swego rodzaju znajomego schematu, jeżeli konieczne byłoby rozstrzygnięcie kwestii spornych. Tak więc, jeżeli strony wyraźnie nie uzgodniły inaczej to – w oparciu o międzynarodowe prawo prywatne – umowa w zdecydowanej większości przypadków będzie związana z prawem kraju oferenta. Do wskazania prawa wystarczy zatem poinformowanie swoich potencjalnych klientów o szczegółach dotyczących firmy, profilu jej działalności, kraju jej rejestracji i siedziby, zarządzie itd. – tak, aby nie pozostawiać wątpliwości co do „narodowości” i charakteru przedsiębiorstwa.

Jeśli jednak mimo wszystko byłyby wątpliwości co do określenia siedziby firmy prowadzącej e-commerce, ustala się ją na podstawie orzeczeń Trybunału Sprawiedliwości. Według nich, macierzystym krajem dla takiej organizacji niekoniecznie jest ten, w którym umieszczono węzeł technologiczny lub fizycznie ulokowano serwer WWW. Częściej wskazywane jest państwo, gdzie przedsiębiorstwo zostało prawnie za-

rejestrowane. Jeżeli natomiast firma ma międzynarodowe przedstawicielstwa, za jej siedzibę i kraj macierzysty przyjmuje się to państwo, w którym firma ma swoją centralę.

Aby kontrakt zawarty on-line był wiążący, przed złożeniem zamówienia konieczne jest dopełnienie następujących warunków:

- wymiana informacji na temat technicznych kroków koniecznych do uprawomocnienia się umowy,
- wskazanie języków, które mogą służyć do jej uzgodnienia,
- zapewnienie technicznych środków do wychwytywania i ewentualnej korekty błędów, które mogą wystąpić podczas komunikacji, jak i tych wynikających z ludzkiej pomyłki,
- uzgodnienie czy kontrakt zostanie zapisany do późniejszego wglądu oraz ustalenie sposobów dotarcia do niego.

Dodatkowo, oferent jest zobowiązany do umożliwienia potencjalnym zainteresowanym zapoznania się z ogólnymi założeniami i treścią warunków umowy w taki sposób, aby mogli oni sporządzić ich kopię dla własnego użytku. Praktyka pokazała, że dobrym zwyczajem jest umieszczanie powyższych informacji (jak również wskazania prawa będącego w mocy) w takim miejscu, które kupujący musi odwiedzić, jeśli kontrakt ma być zawarty (np. na stronie WWW, zapoznanie się z którą potwierdzane jest wcisnięciem specjalnego klawisza).

Nieco inaczej wygląda sprawa umów pomiędzy firmami internetowymi a odbiorcami indywidualnymi (B2C). Tutaj również Dyrektywa pozostawia decyzję co do wyboru właściwego prawa stronom kontraktu, z tym jednak zastrzeżeniem, że wybór ten „...nie może w żaden sposób skutkować pozbawieniem konsumenta ochrony, jaką zapewniałoby mu prawo jego własnego kraju” [7].

Przepisy zapewniające dodatkową ochronę konsumentowi odróżniają ten rodzaj umów od wcześniej wspomnianych kontraktów pomiędzy firmami, gdzie strony pozostawały w równowadze względem siebie. Ochrona ta nie może być zniesiona lub zmniejszona dodatkowymi zapisami w umowie, które to, jeśli wystąpią, nie mają mocy prawnej.

Zgodnie z prawem Unii, sprzedający usługę lub dobro zobowiązany jest do zapewnienia odbiorcy między innymi:

- dostępu do danych o swojej tożsamości oraz siedzibie,
- charakterystyki oferowanego towaru czy usługi, wraz z opisem kosztów dodatkowych, łącznie z wyszczególnieniem użytych środków telekomunikacyjnych,
- informacji o sposobie i kosztach dostarczenia towaru jak również informacji o warunkach zwrotu towaru (terminy, koszty, warunki, prawa) i wycofania się z transakcji,
- informacji o długości okresu, w którym oferta pozostaje ważna [12].

Dodatkowo, konsument musi otrzymać pisemne potwierdzenie tego, że umowa została podpisana i jest w trakcie realizacji. Oznacza to także, że odbiorca zna warunki, na jakich może złożyć reklamację (adres, osoby odpowiedzialne, prawa), za-

znajomił się z ewentualnymi usługami dodatkowymi (takimi jak serwis pogwarancyjny, infolinia itp.) i wie, na jakich zasadach może wycofać się z kontraktu. Wszystkie te wymagania mają na celu zapewnienie ochrony słabszej stronie, jaką jest osoba fizyczna, czyli konsument. Pozostałe wymogi są podobne jak w przypadku kontraktów B2B, z tym zastrzeżeniem, że domyślnym prawem, według którego rozstrzygane są sporne kwestie jest prawo tego kraju, w którym żyje odbiorca. Oznacza to, że jeśli w umowie nie zostało wyraźnie zaznaczone inaczej, dostawca musi być przygotowany na rozstrzyganie swoich spraw w ramach piętnastu różnych kodeksów państw stowarzyszonych w Unii, skąd mogą pochodzić jego klienci.

### **Prawo Internetu w Polsce**

Wymiana handlowa przy użyciu środków elektronicznych – w szczególności Internetu – ma w Polsce stosunkowo krótką historię. Jednak dynamika wzrostu i coraz większa rola, jaką e-commerce zaczyna odgrywać w gospodarce narodowej sprawiają, że nieodzowne staje się wprowadzenie przejrzystych reguł jego funkcjonowania.

Szczególnie ważne na tym polu jest dążenie do ujednoczenia otoczenia gospodarczego i prawnego w kontekście międzynarodowym. Po pierwsze, niezmiernie istotna jest harmonizacja polskich przepisów z regulacjami już obowiązującymi lub wprowadzanymi w Unii Europejskiej, po drugie – Polska ma szansę na uniknięcie konkretnych błędów naszych poprzedników i na skorzystanie z ich doświadczeń. Poza Unią należy także pamiętać o współpracy z organizacjami międzynarodowymi wykraczającymi poza granice Europy, takimi jak Organizacja Współpracy Gospodarczej i Rozwoju (OECD) czy Światowa Organizacja Handlu (WTO), które również umożliwiają wymianę doświadczeń oraz poszukują kierunków rozwoju dla rozwiązań prawnych wspierających e-biznes.

Istotnym jest, aby nie przeoczyć najistotniejszego momentu, kluczowego dla przyszłości handlu elektronicznego w Polsce, jakim jest stworzenie odpowiedniej bazy prawnej **zanim** żywiłowy rozwój elektronicznego handlu postawi nas wszystkich w sytuacji faktów dokonanych. Taka przezorna, wyprzedzająca działalność jest potrzebna szczególnie teraz, gdy mamy do czynienia z coraz większym zainteresowaniem e-biznesem zarówno ze strony firm inwestujących swoje środki w przedsięwzięcia internetowe jak i publicznymi dyskusjami na ten temat. Warto również wykorzystać przychylne zainteresowanie mass mediów poświęcających coraz więcej uwagi tej branży.

Świadomość zalet Internetu rośnie wśród Polaków. Mogą o tym świadczyć różne zjawiska zachodzące w naszej rzeczywistości. Jednym z nich jest wspomagana przez państwo popularyzacja dostępu do Sieci w szkołach. Innym ważnym symptomem jest zachowanie się kursów spółek giełdowych związanych z branżą IT<sup>6</sup>, które to, po okresie powszechnej fascynacji, w ciągu ostatniego roku zostały przez inwestorów poddane bardziej krytycznej wycenie, a teraz zmierzają do ustalenia swojej rzeczywistej wartości – ani nie nadmiernie wygórowanej, ani nie nadmiernie zaniżonej.

<sup>6</sup> Skrót od *Information Technology*, często używany dla określenia firm związanych z sektorem informatycznym i telekomunikacyjnym.

Powszechna znajomość wśród Polaków (przynajmniej posiadających wykształcenie wyższe albo średnie) takich pojęć, jak Internet czy e-commerce, pozwala wierzyć, że przy odpowiednim postępowaniu mamy szansę na rozwinięcie tej nowej i silnej gałęzi handlowej – nawet w skali Europy. Do osiągnięcia celu konieczne jest jednak między innymi przygotowanie odpowiednich ram działania, które zapewnią uczestnikom rynku elektronicznego jasność reguł i zasad postępowania. Dlatego sprawą priorytetową dla polskich władz powinno być dokończenie prac związanych z dostosowaniem polskiego prawa do nowej rzeczywistości, a także jego harmonizacja z przepisami krajów Unii Europejskiej, w przeddzień naszego do niej wstąpienia.

W rozdziale tym przedstawione zostało **obecne** otoczenie prawne handlu elektronicznego w Polsce. Szczególną wagę przyłożono do problemu ustanowienia w naszym kraju instytucji podpisu elektronicznego. Wynika to z fundamentalnej roli, jaką odgrywają cyfrowe metody potwierdzania autentyczności dla rozwoju e-commerce. Omówiono także najważniejsze obszary styku prawa i gospodarki elektronicznej, wskazując na stopień zaawansowania aktualnych prac i na wymagania jakie nadal jeszcze stoją przed polskim ustawodawcą.

Pomimo dość pesymistycznych nastrojów panujących w środowisku specjalistów z dziedziny e-commerce dziedzina ta jest niejako „skazana na sukces”, gdyż taki jest trend rozwoju gospodarki światowej. Sukces taki nastąpi, mimo braku odpowiedniej popularyzacji działań władz polskich w środkach masowego przekazu (co pomogłoby nie tylko w uświadomieniu społeczeństwu zmian w prawodawstwie, ale także reklamowałyby samą ideę handlu elektronicznego). Szczególnie dobrze rokuje w tej sprawie fakt, że mimo wspomnianych wyżej zaniedbań edukacyjnych i propagandowych – tak naprawdę w sprawie stworzenia ram legislacyjnych dla e-gospodarki zostało już zrobione w Polsce stosunkowo dużo. Najbardziej istotne z wprowadzonych modyfikacji to:

- Ustawa dotycząca prawa bankowego [20], zmieniająca wymogi konieczne dla uznania oświadczeń woli. Dzięki jej zapisom wszelkie oświadczenia woli składane w związku z dokonywaniem czynności bankowych mogą być wyrażane za pomocą elektronicznych nośników informacji. Ustawa ta dopuszcza również możliwość sporządzania dokumentów związanych z czynnościami bankowymi za pomocą elektronicznych nośników informacji<sup>7</sup>.
- Nowy przepis kodeksu karnego [15], który sankcjonuje uznanie za dokument każdego przedmiotu lub zapisu na komputerowym nośniku informacji, z którym związane jest określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa lub okoliczności mającej znaczenie prawne<sup>8</sup>.
- Nowy artykuł prawa działalności gospodarczej [21], wprowadzający obowiązek podawania przez przedsiębiorcę w ofercie sprzedaży za pośrednictwem m.in.

<sup>7</sup> Artykuł 7.

<sup>8</sup> Artykuł 115 § 14.

sieci informatycznych, co najmniej danych dotyczących osobowości prawnej przedsiębiorcy, numeru, pod którym jest on wpisany do rejestru przedsiębiorców oraz siedziby i adresu przedsiębiorcy<sup>9</sup>.

- Ustawa o ochronie praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny [35], zawierającą między innymi regulacje dotyczące umów zawieranych na odległość, a więc w szczególności umów zawieranych drogą elektroniczną.

Warto jednocześnie nadmienić o zmianach w prawie ubezpieczeniowym, które umożliwiają zawieranie umów ubezpieczenia na odległość, najczęściej metodami elektronicznymi. Bardzo istotne było także wprowadzenie regulacji odnoszących się do zagadnień gospodarki elektronicznej w przygotowywanych przez Komisję Papierów Wartościowych i Giełd projektach kształtujących działanie funduszy inwestycyjnych i regulujących publiczny obrót papierami wartościowymi.

Nowo wprowadzane przepisy w ustawie o funduszach inwestycyjnych mają służyć usankcjonowaniu obsługi zleceń nabycia i odkupienia jednostek uczestnictwa za pomocą elektronicznych nośników informacji. Ta sama idea przyświecała także twórcom zmian w *Prawie o publicznym obrocie papierami wartościowymi*. Tu również chodzi o możliwość składania zamówień on-line, za pomocą metod elektronicznych. Proponowane rozwiązania mają w zamierzeniu dostosować funkcjonowanie rynku papierów wartościowych do wymagań i możliwości nowoczesnych technik przekazywania informacji, a w przyszłości uczynić z nich podstawowe narzędzie komunikacji.

Ważnym wydarzeniem było także zniesienie koncesji na usługi telekomunikacyjne – w tym na świadczenie usług dostępu do Internetu – i zastąpienie ich zezwoleniami [9], co było jednym z koniecznych do podjęcia kroków, jeśli Polska ma dążyć do dostosowania swojego prawa do przepisów Unii Europejskiej. Zniesienie regulacji na szczeblu ministerialnym jest jednym z elementów demonopolizacji rynku, ma również na celu uproszczenie warunków rozpoczęcia działalności telekomunikacyjnej, tak dla operatorów jak i dla dostawców usług korzystających z obcej infrastruktury. Działanie takie zgodne jest z dyrektywami UE i służyć ma przyspieszeniu rozwoju rynku elektronicznego.

### **Zagadnienie szczegółowe: podpis elektroniczny**

Omówione wyżej (w ogromnym skrócie) zagadnienia związane z regulacjami prawnymi w Internecie miały charakter dyskusji dosyć ogólnej. Dla konkretyzacji przeprowadzonych rozważań warto włączyć jeszcze jeden wątek szczegółowy, a mianowicie kwestię prawnego statusu tak zwanego podpisu elektronicznego. Zadaniem tego podpisu jest:

- potwierdzenie, że uczestnicy transakcji są rzeczywiście osobami, za które się podają (innymi słowy identyfikacja stron),

<sup>9</sup> Artykuł 12.

- uzyskanie pewności, że przekaz nie został w żaden sposób zmodyfikowany w trakcie transakcji,
- certyfikacja będąca uwierzytelnieniem oświadczeń składanych drogą cyfrową.

Elektroniczny podpis może przybierać różne formy. Niemniej jednak dla celów systematycznych wyróżnimy tutaj dwa rodzaje podpisów:

- tradycyjny podpis przechowywany w formie elektronicznej,
- podpis cyfrowy, przechowywany w formie ciągu bitów dołączanych bezpośrednio do dokumentu elektronicznego.

Z uwagi na fakt, iż pierwsza z form podpisu wydaje się być bliższą potocznemu rozumieniu tegoż pojęcia, zostanie ona omówiona w pierwszej kolejności. Omawiana forma podpisu elektronicznego nie nadaje się, jak zostanie pokazane niżej, do uwiarygodniania dokonywanych elektronicznie transakcji. Nie jest ona jednak całkowicie bezużyteczna. Znakomita większość banków polskich zмага się z problemem identyfikacji klienta przy jego obsłudze. I w takich właśnie przypadkach stosowane są systemy, których podstawą działania jest podpis klienta przechowywany w formie elektronicznej.

Jak taki system działa? Otóż w momencie zakładania przez klienta rachunku (na przykład oszczędnościowo-rozliczeniowego, lokaty terminowej itp.), składany jest przez niego wzorzec podpisu ręcznego, który następnie przenoszony jest do formy cyfrowej (poprzez zeskanowanie). Taki wzorzec podpisu (w postaci elektronicznego obrazu) wykorzystany może być następnie na różne sposoby, np.:

1. Może znaleźć swoje miejsce w systemie ladowym. Wtedy pracownik banku obsługując klienta może porównać podpis złożony przez niego na czeku, asygnacie lub innym dokumencie wymagającym uwierzytelniającego podpisu z wzorem, który znajduje się w systemie komputerowym. Dzięki takiemu rozwiązaniu można wykrywać podstawowe oszustwa, gdy złodziej próbuje posługiwać się np.: skradzionymi czekami z nieudolnie podrobionym podpisem właściciela.
2. Znacznie obszerniejszą gamę zastosowań podpis w postaci cyfrowego obrazu znaleźć może w bankowym back-office. Istnieją bowiem systemy do automatycznego sprawdzania, w celu weryfikacji, podpisów umieszczonych na dokumentach transakcyjnych. Formularze te (m. in. czeki, asygnaty) przesyłane są siecią komputerową wprost z transakcyjnych systemów płatniczych, gdzie zostały wcześniej zeskanowane. Podpisy zawarte na tych dokumentach są wyodrębniane, a następnie porównywane z ich wersjami znajdującymi się w bazach danych. Porównywanie odbywa się najczęściej na bazie sieci neuronowych.

Należy wspomnieć, iż decydującym dla procesu porównawczego dwóch podpisów jest nie sam obraz podpisu lecz jego deskrypcja opisana wieloma charakterystykami. Niejako „przy okazji” można w ten sposób zautomatyzować odczytywanie z dokumentów innych danych, takich jak pełnomocnictwa, limity ilościowe. Dodatkowym atutem takiego rozwiązania jest bardzo duża szybkość procesu, pozwalająca na przetwarzanie ogromnej liczby dokumentów.

Znacznie szersze zastosowanie ma podpis cyfrowy, który jest wprowadzany do elektronicznych dokumentów w sposób całkowicie odmienny od ich podpisywania odręcznego, co jednak nie przeszkadza, że jest on w sensie prawnym odpowiednikiem tradycyjnego podpisu, jaki składany jest na różnego rodzaju dokumentach. Charakter podpisu zachowany jest poprzez jego podstawowe właściwości, które wyrazić można w następujących postulatach:

- a) podpis powinien gwarantować, iż dokument (oświadczenie woli), który jest nim opatrzony, pochodzi od określonej osoby;
- b) treść dokumentu opatrzona takim podpisem, ani też sam podpis, nie zostały sfałszowane, zmienione lub też podrobione;
- c) w związku z powyższym: jedynie osoba X podpisująca taki dokument może utworzyć podpis osoby X, czyli wnioskując powtórnie – podrobienie podpisu powinno być niewykonalne;
- d) ponadto powinno dać się jednoznacznie stwierdzić, iż podpis został złożony pod danym dokumentem, a co za tym idzie: kopiowanie podpisu z jednego dokumentu na drugi powinno być niewykonalne.

Przytoczone powyżej postulaty zostały w znakomitej części spełnione poprzez szereg rozwiązań zaimplementowanych już dzisiaj w wiele systemów przesyłania dokumentów elektronicznych czy też poczty elektronicznej. Faktyczna realizacja owych propozycji przedstawia się pokrótce w następujący sposób. Podpis cyfrowy, który nazywany jest inaczej podpisem elektronicznym, to ciąg bitów zależny od podpisywanej wiadomości. Podpis ten jest tworzony przez osobę, która podpisuje dokument. Najważniejsze jest stwierdzenie faktu, że podpis cyfrowy jest wypadkową treści podpisywanej wiadomości oraz osoby podpisującej. Algorytmy podpisu elektronicznego oparte są zawsze na konkretnym, wybranym szyfrze, który to szyfr stanowi najczęściej podstawę utworzenia systemu kryptograficznego z kluczem jawnym. W systemie tym z każdym użytkownikiem związana jest para kluczy, z których jeden służy do podpisywania wiadomości, a drugi do weryfikacji podpisu. Klucz służący do podpisywania wiadomości jest zawsze tajny, powinien więc być znany tylko danej osobie. Z kolei klucz służący do weryfikacji podpisu jest publicznie dostępny.

Podpisem wiadomości jest przekształcony kryptograficznie przy pomocy klucza tajnego (prywatnego) ściśle zdefiniowany skrót tejże wiadomości. Natomiast odbiorca takiej wiadomości dokonuje weryfikacji podpisu przekształcając go za pomocą klucza publicznego. Całość powyższego rozwiązania zasadza się na idei tzw. algorytmów asymetrycznych. Aby wnieść dodatkowe zabezpieczenia, wprowadzono do omawianych systemów podpisu elektronicznego również algorytmy symetryczne, które stanowią uzupełnienie przedstawionego powyżej systemu kluczy prywatnego i publicznego.

Regulacje Unii Europejskiej<sup>10</sup> zrównują podpis elektroniczny z podpisem odręcznym, przynajmniej jeśli chodzi o powodowanie skutków prawnych. Sytuacja taka

<sup>10</sup> *Dyrektywa w sprawie podpisu elektronicznego, 99/93/EC.*

jest możliwa nie tylko ze względu na gwarancje bezpieczeństwa i poufności oferowane przez technologie cyfrowe, lecz przede wszystkim z powodu stuprocentowej pewności identyfikacji autora. Tę pewność uzyskuje się obecnie najczęściej poprzez wprowadzenie **certyfikatów** czyli elektronicznych zaświadczeń, za pomocą których dane służące do weryfikacji podpisu elektronicznego są przypisane do konkretnej osoby. Wydawanie certyfikatów jest zadaniem specjalnie wskazanych przez Ustawę instytucji wydających certyfikaty. Od wiarygodności tych instytucji w decydującym stopniu zależy sprawność działania całego systemu podpisów elektronicznych.

Państwa członkowskie UE zostały zobligowane do wprowadzenia takich regulacji do prawa wewnętrznego, aby umowy zawarte elektronicznie były uznawane za wiążące, a tym samym w żaden sposób nie dyskryminowane w stosunku do tradycyjnych form kontraktów. Oznacza to w praktyce, że podpis elektroniczny ma być dopuszczany w postępowaniach sądowych jako pełnoprawny dowód. Do wydania podobnych regulacji zobowiązane zostały także kraje kandydujące do Unii, w tym także Polska. W związku z tym w ciągu roku 2001 w Sejmie Rzeczypospolitej trwały prace nad dwoma projektami ustaw o podpisie elektronicznym. Projekt poselski przesłany został do rozpatrzenia 7 grudnia 2000 roku, zaś projekt rządowy 22 lutego 2001 roku. Prawo to zostało ostatecznie sformułowane w postaci *Ustawy o podpisie elektronicznym* z dnia 18 września 2001 (Dziennik Ustaw 2001, nr 130 poz. 1450). Niestety zarówno oba projekty, jak i finalny tekst ustawy nie były konsultowane ze środowiskiem informatyków (naukowców i praktyków). Nie jest więc zaskoczeniem, że rozwiązania polskiego prawa o podpisie elektronicznym budzą wiele wątpliwości. W szczególności niektóre szczegółowe regulacje prawne mogą być rozpatrywane jako silnie nadmiarowe w stosunku do aktualnego stanu praktyki stosowania podpisów elektronicznych w Polsce. Na ustawy tego typu, jak omawiana wyżej należy jednak patrzeć w perspektywie kilkunastoletniego okresu ich potencjalnego funkcjonowania, dlatego generalnie można wyrazić satysfakcję z faktu, że ustawa o podpisie elektronicznym wreszcie w Polsce powstała i ze dzięki temu podpis elektroniczny zaistniał jako dobrze zdefiniowane pojęcie funkcjonujące i obowiązujące w polskim porządku prawnym. Oczywiście różne szczegóły zarówno procesu składania i uwierzytelniania elektronicznego podpisu, jak i procedury certyfikacji, będą musiały być (zapewne) w przyszłości dopracowane i udoskonalone (być może nawet w trybie nowelizacji Ustawy) – ale korzyść, jaką jest fakt istnienia odpowiedniej bazy dla tych wszystkich udoskonaleń – jest bezdyskusyjna.

## **Problem prawa karnego w Internecie**

Problem konieczności opracowania i wdrożenia norm prawnych w Internecie nie dotyczy wyłącznie dyskutowanej wyżej sfery e-biznesu. W świecie deklarującym rozwój gospodarki opartej na wiedzy, nawet zwykła wymiana informacji też przestała być tak całkiem bezproblemowa. Jakie informacje, gdzie i komu wolno przekazać?

Dostęp do jakich serwerów musi być strzeżony? Czym grozi nielegalne skopiowanie, albo co gorsza zniszczenie informacji?

Te i temu podobne problemy muszą być ściśle uregulowane, między innymi po to, by potencjalnie możliwym sporom – nadać pewne ramy i punkt odniesienia. Zatem nawet przy braku jawnej działalności gospodarczej w Internecie (która to działalność ciągle jeszcze budzi kontrowersje wśród zwolenników tradycyjnego „czystego Internetu”) prawo musi wkraczać do Sieci także i w obszarze jej czysto **informacyjnych** funkcji, pozostawiając okres radosnego rozwoju Internetu, pozbawionego wszelkich ograniczeń i barier jako nieodwołalnie przeszły już do historii.

Nie możemy od tego uciec, choćbyśmy bardzo chcieli, więc dla naszego własnego dobra musimy się zgodzić z tym, że zakres penetracji prawa w Sieci będzie się znacząco poszerzał i pogłębiał. Proces ten nieuchronnie ulegnie także znaczącemu przyspieszeniu, wraz ze wzrostem wartości informacji i wiedzy jako głównego czynnika wzrostu gospodarczego. Trudno jest dzisiaj powiedzieć, jak to przyszłe prawo sieciowe będzie wyglądało. Z całą pewnością będzie inne od obecnie obowiązującego, gdyż obecne przepisy prawne, regulujące funkcjonowanie informacyjnej funkcji Internetu (i innych środków masowego przekazu), nie do końca są jeszcze dopracowane. Tak się dzieje zarówno w Polsce jak i w prawie międzynarodowym, a powodem jest nowa i niezbyt dobrze poznana od strony prawnej natura sieciowych relacji i sieciowych współzależności podmiotów prawa – czyli zarówno ludzi, jak i instytucji. Przykładowo jako typową „niedoróbkę prawną” warto wskazać fakt, że obecnie gros ustaw mających związek z Internetem i z mediami, chroni głównie nadawcę informacji, natomiast odbiorca jest w gruncie rzeczy bezbronny.

Policzmy na przykład, jak wiele uregulowań dotyczy obecnie ochrony praw autorskich, natomiast zauważmy także, iż do tej pory w prawie bardzo mało miejsca przewiduje się na określenie odpowiedzialności prawnej autorów. Tymczasem dla ochrony odbiorców informacji należało by stworzyć prawo, pozwalające na skuteczne ściganie instytucji produkujących programy, których zawodne działanie naraża miliony użytkowników na stresy, a czasem także na utratę wyników ich pracy. Trzeba coś zrobić w sprawie prawnej odpowiedzialności twórców i dystrybutorów wirusów.

Nie można też wiecznie przechodzić do porządku dziennego nad zniszczeniami, których przyczyną są hackerzy. Nie można też bez końca tolerować osób odpowiedzialnych za zamieszczanie w Internecie (i w innych mediach) informacji nieprawdziwych lub niezgodnych z obowiązującym prawem<sup>11</sup>. Dla wszystkich tych zagadnień trzeba koniecznie znaleźć odpowiednie rozwiązania na gruncie prawa Sieci – prawa powszechnie obowiązującego i powszechnie aprobowanego.

Jeśli mowa o odpowiedzialności karnej za czyny popełniane w Internecie, to powraca kwestia identyfikacji i weryfikacji tożsamości podmiotu działającego w Internecie. Polskie prawo skupia się w tym zakresie praktycznie wyłącznie na podpisie

<sup>11</sup> Skoro obecnie informacja staje się pieniądzem – to ścigajmy fałszerzy tych nowych pieniędzy!

cyfrowym, podczas gdy współczesna technika oferuje znacznie więcej możliwości identyfikacji. Elektroniczna weryfikacja tożsamości osoby może się równie dobrze odbywać z wykorzystaniem na przykład szeregu cech biometrycznych: przy użyciu odcisków palców, obrazu tęczówki oka, kształtu twarzy lub dłoni, próbek głosu i praktycznie nieograniczonej gamy innych rozwiązań, gdzie wykorzystanie elektronicznego przekazu danych jest jak najbardziej możliwe, a identyfikacja (przy odpowiednim poziomie technicznym użytych rozwiązań) może być uznana za pewną i niezawodną. Już dziś niektóre banki, domy maklerskie i inne instytucje finansowe oferują możliwość składania zleceń przez telefon. Specjalne techniki cyfrowej weryfikacji głosu mówcy umożliwiają jednoznaczne skojarzenie konkretnej osoby z jej głosem, co uwiarytelnia dany przekaz.

Ze względu na bardzo szybki rozwój technologii istotne jest więc, by sformułowania ewentualnej ustawy karnej, penalizującej czyny popełniane w Internecie w rozumieniu przepisów prawa karnego, nie były zbyt szczegółowe i nie nakładały niepotrzebnych ograniczeń technicznych. Takie właśnie ujęcie spotkać można w odpowiednich dyrektywach Unii Europejskiej, gdzie pojęcia identyfikacji osoby działającej w sieci nie ogranicza się jedynie do podpisu cyfrowego.

### Uwagi końcowe

W całym artykule usiłowano dowieść, że **prawo** (gospodarcze, cywilne, ale także karne) jest w Internecie naprawdę coraz bardziej potrzebne. Prawa takiego brak. Wydaje się, że przynajmniej częściowo wiąże się to z faktem, że Internet powstał i rozwinął się w USA, a więc obecny stan prawny w Sieci jest wynikiem anglosaskiego podejścia do teorii prawa i społeczeństwa. Podejście to, znane w Polsce raczej powierzchownie, bo głównie z sensacyjnych filmów, których akcja toczy się na sali sądowej, opiera się na doktrynie moralnej, zakładającej (w bardzo dużym uproszczeniu), że to dobro jest regułą, a zło wyjątkiem – a nie odwrotnie. Zgodnie z tą doktryną trzeba najpierw zabezpieczyć to pierwsze (czyli ochraniać dobro w jego różnych postaciach), zanim weźmie się za to drugie (to znaczy zanim zacznie się ścigać i karać zło). Jest to w sumie bardzo piękna teoria, ale jak wiele pięknych teorii – często niezbyt dobrze sprawdzająca się w konfrontacji z faktami.

Dlatego prawo w Internecie jest potrzebne, a skoro jest potrzebne – to należy je stworzyć, wdrożyć i egzekwować. Inaczej Sieć stanie się śmietnikiem, którego używanie będzie nie do przyjęcia dla zwykłych, uczciwych ludzi, natomiast którego nadużywanie będzie domeną różnego kalibru przestępców i wykolejeńców. Nie możemy do tego dopuścić!

### Bibliografia

- [1] *Amazon Sales Rise 40 Percent to \$960 Million*. Reuters 2001, [http://www.emarketer.com/estatnews/enews/reuters/01\\_08\\_2001.rwntz-story-bcnetamazonoutlookdc.html](http://www.emarketer.com/estatnews/enews/reuters/01_08_2001.rwntz-story-bcnetamazonoutlookdc.html)

- 
- [2] *An Information Society for All – Progress Report*. Sprawozdanie ze specjalnego spotkania Komisji Europejskiej, European Communities 23 III 2000, [http://europa.eu.int/comm/information\\_society/eeurope/index\\_en.htm](http://europa.eu.int/comm/information_society/eeurope/index_en.htm)
- [3] Bloom B.S. 1999: *Internet Availability of Prescription Pharmaceuticals to the Public*. „Annals of Internal Medicine”
- [4] *Brussels and Lugano Conventions*. <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/brux-idx.htm>
- [5] *Definition of E-commerce*. Na podstawie „Internet Business”. Interest Verlag, Augsburg 1997, <http://www.servicemachine.org/start/Definition/Definition.htm#2>
- [6] *Digital Economy 2000*. Office of Policy Development, U.S. Department of Commerce, <http://www.esa.doc.gov/de2k2.htm>
- [7] *Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. 95/46/EC, 24 X 1995
- [8] *Distance Selling Directive*. Dyrektywa Parlamentu Europejskiego 97/7
- [9] *Dyrektywa o liberalizacji rynku usług i infrastruktury telekomunikacyjnej*. 90/388/EEC, 1 I 1998
- [10] *Dyrektywa o niektórych aspektach prawnych w handlu elektronicznym*. 2000/31/EC, 8 VI 2000
- [11] Gildeggen R. III 1999: *International Sales Contracts*. Pforzheim
- [12] Henkel J., Drugs B.: *Online*. U.S. Food and Drug Administration, [http://www.fda.gov/fdac/features/2000/1\\_online.html](http://www.fda.gov/fdac/features/2000/1_online.html)
- [13] Immerwahr A., Nobile A. I 2001: *Understanding E-commerce*. Blueprints Online, <http://www.publicrelations.villanova.edu/blueprints/html/November/E-commerce1.htm>
- [14] *Kodeks celny*. Dz.U. Nr 23, poz. 117, 9 I 1977
- [15] *Kodeks karny*. Dz.U. Nr 88, poz. 553, 6 VI 1997
- [16] *Kodeks postępowania cywilnego*. Dz.U. Nr 43, poz. 296, 1965 z późniejszymi poprawkami
- [17] *Legal Issues of Electronic Commerce – A Practical Guide for SMEs*. Electronic Commerce Legal Issues Platform 3 V 2001, <http://europa.eu.int/ISPO/legal/en/lab/991216/brochure.doc>
- [18] Niewiarowski C. XII 2000: *Europejskie e-podatki*. „PC World Computer”
- [19] Pickett J.P. 2000: *The American Heritage Dictionary*. Houghton Mifflin Company, Boston
- [20] *Prawo bankowe*. Dz.U. Nr 140, poz. 939, 29 VIII 1997
- [21] *Prawo działalności gospodarczej*. Dz.U. Nr 101, poz. 1178, 19 XI 1999
- [22] *Projekt ustawy o ochronie baz danych*. Wersja II, 8 V 2001, [http://www.piit.org.pl/cgi-bin/komunikaty/list\\_pr.cgi?act=note&type=0&id=224](http://www.piit.org.pl/cgi-bin/komunikaty/list_pr.cgi?act=note&type=0&id=224)
- [23] *Proposal for a Regulation on Administrative Co-Operation in the Field of Indirect Taxation (VAT)*. Commission of the European Communities, Bruksela 7 VI 2000
- [24] *Recommendation for the protection of privacy on the Internet*. R/99/5, 23 II 1999
- [25] *Regulation on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters*. Regulacja 44/2001, 22 XII 2000

- [26] Schulze C., Baumgartner J. 2001: *Don't Panic! Do E-commerce. A Beginner's Guide to European Law Affecting E-commerce*. European Commission's Electronic Commerce Team
- [27] Soo-Jung Smith, *E-business*. PricewaterhouseCoopers 2001, <http://www.pwcglobal.com/Extweb/service.nsf/docid/D4BF5BF044E1B8A785256988000DB583>
- [28] *Sprawozdanie Międzyresortowego Zespołu do spraw handlu metodami elektronicznymi*. Ministerstwo Gospodarki 11 VII 2000
- [29] *State of the Internet 2000*. United States Internet Council & ITTA Inc., <http://usic.wslogic.com/intro.html>
- [30] *The Electronic Commerce Directive*. 2000/31/EC, 8 VI 2000
- [31] *The Electronic Signature Directive*. 1999/93/EC, 13 XII 1999
- [32] *The UNCITRAL Model Law on Electronic Commerce*. United Nations Commission on International Trade Law, <http://www.un.or.at/uncitral>
- [33] *Top 25 Web Properties of March 2001*. Nielsen//NetRatings Inc., [http://cyberatlas.internet.com/big\\_picture/traffic\\_patterns/article/0,,5931\\_741721,00.html](http://cyberatlas.internet.com/big_picture/traffic_patterns/article/0,,5931_741721,00.html)
- [34] *Ustawa o ochronie danych osobowych*. Dz.U. Nr 133, poz. 883, 29 X 1997
- [35] *Ustawa o ochronie praw konsumentów oraz o odpowiedzialności za szkodę wyrządzoną przez produkt niebezpieczny*. Dz.U. Nr 22, poz. 271, 2 III 2000
- [36] *Ustawa o Inspekcji Handlowej*. Dz.U. Nr 4, poz. 25, 15 XII 2000
- [37] *Ustawa o prawie autorskim i prawach pokrewnych*. Dz.U. Nr 24, poz. 83, 4 II 1994 oraz Dz.U. Nr 43, poz. 170
- [38] *WIPO Copyright Treaty*. World Intellectual Property Organization, Genewa 23 XII 1996, <http://www.wipo.org/eng/diplconf/distrib/94dc.htm>
- [39] *Wytyczne na rzecz ochrony konsumentów w kontekście handlu elektronicznego*. Rada OECD, XI