

**Jarosław Sozański**

**UNIJNE REGULACJE PRAW  
CZŁOWIEKA  
W CYBERPRZESTRZENI  
A KORZYŚCI, ZAGROŻENIA  
I POSTULATY**



## Wstęp

Regulacje prawne zjawisk życia społecznego są z natury konserwatywne, stąd pojawiają się z opóźnieniem i tylko w sytuacjach koniecznych. Cyberprzestrzeń z kolei jest fenomenem dynamicznym i żywołowym, rozwijającym się w wyniku zbiorowej i wielowątkowej praktyki. Cyberprzestrzeń uznawana jest za obszar wolności, stąd przeciwko ochronie praw podmiotowych w świecie wirtualnym (pomimo takiej potrzeby i konieczności) występuje silna opozycja. Dlatego cyberprzestrzeń w prawie krajowym, międzynarodowym i unijnym długo będzie egzystować pomiędzy dwoma tendencjami - regulacją i deregulacją. Przepisy prawne są nieliczne, a pojawiają się tylko w koniecznym i niekwestionowanym zakresie. Dlatego poniższy artykuł ma charakter prezentacji wybiórczej oscylującej głównie wokół praw podmiotowych.

Cyberprzestrzeń, mimo intensywnego dotąd wykorzystania przez struktury Unii Europejskiej, uznawana jest nadal w UE za ważny kierunek rozwoju, o czym świadczyć może m.in. funkcjonująca od kilku lat domena z rozszerzeniem .eu, która jest dostępna dla 490 milionów Europejczyków w 27 krajach. Struktury unijne bardziej efektywnie od innych organizacji i ugrupowań międzynarodowych korzystają z sieci, udostępniając je szeroko obywatelom i mieszkańcom UE. Wszystko to świadczy o potencjalnej randze i zakresie problemu. Z cyberprzestrzeni korzystają wszystkie w zasadzie instytucje i struktury UE i WE (rozwijając sieci ogólnodostępne oraz zamknięte i specjalistyczne), z szerokim dopuszczeniem indywidualnych odbiorców. Wszystko to jest regulowane stosunkowo nielicznymi przepisami. Jednak zważywszy, że prawo wspólnotowe (*acquis communautaire*) stanowi hierarchicznie zorganizowany system normatywny, należy wstępnie zakładać, że regulacje prawne dotyczące cyberprzestrzeni staną się jego częścią, a więc podsystemem. Wspólny interes wymaga, żeby były one znane użytkownikom sieci (przybliżeniu czego służyć powinien niniejszy, sygnalny artykuł), a także żeby podjęto działania służące eliminowaniu cyberprzestępczości<sup>1</sup>. Zdaję sobie sprawę, że omówienie wszystkich zagadnień z powyższego zakresu wymagałoby ram obszernej monografii. Dlatego w niniejszym opracowaniu ograniczę się do omówienia trzech istotnych problemów: systemu ochrony prawnej UE, elementarnej ochrony w sferze rozwiązań technicznych i programowych oraz pozasądowej ochrony praw z wykorzystaniem sieci, by w ramach tych obszarów wskazać na zagrożenia i postulować remedia.

1) Ważniejsze zagrożenia - zob. szerzej: A. Adamski, *Przestępczość w cyberprzestrzeni*, TNOIK, Toruń 2001; J.W. Wójcik, *Oszustwa finansowe. Zagadnienia kryminologiczne*, Warszawa 2008; W. Fijałkowski, *Internet – przestępcza gałąź gospodarki*, Prokurator 1/2007. Por. też Opinia PE 2007/2088(INI), AD/689981PL.

Podjęte zagadnienia, zarówno teoretyczne, jak i praktyczne, będą przedmiotem poniższych rozważań, których struktura obejmuje:

1. Cyberprzestrzeń a system ochrony prawnej Unii Europejskiej,
2. Prawa osobiste i wizerunek,
3. Unijne regulacje dotyczące sankcji karnych i warunkowego dostępu,
4. Ochronie sieci, topografię, programy, algorytmy w UE,
5. Własność intelektualną w Internecie,
6. Pozasądową ochronę praw człowieka a sieci net,
7. Efektywność i kontakty; uwagi końcowe.

## 1. Cyberprzestrzeń a system ochrony prawnej Unii Europejskiej

Za cyberprzestrzeń przyjęło się zwykle uważać wirtualną przestrzeń społeczną<sup>2</sup>, a ściślej wielopłaszczyznowy obszar kontaktów niebezpośrednich. Jednak nie każdy korzystający z tej przestrzeni podmiot uważa się za cybernautę (internautę). Dlatego cyberprzestrzeń powinna być uważana także za środek służący uzyskiwaniu celów, a więc narzędzie i metodę kontaktów, a szerzej działań społecznych. Mimo wielkich korzyści, jakie niosą oba te aspekty cyberprzestrzeni, każda obecność w niej może być wykorzystana wbrew woli lub przeciwko interesom użytkownika, często też *ex post*. Co więcej cyberprzestrzeń jest również obszarem gromadzenia i wyzyskiwania informacji (często osobistych i indywidualnych) także bez zgody, wiedzy i wbrew interesom zainteresowanych podmiotów. A więc z jednej strony cyberprzestrzeń stanowi poszerzenie praw człowieka i jego wolności, a z drugiej strony niesie ważne dla nich zagrożenia zarówno wynikające (popelniane delikty), jak i niewynikające (naruszenie *privacy*, brak kontroli nad przetwarzanymi wirtualnie informacjami osobistymi, niemożność ich usuwania)<sup>3</sup>. A regulacje prawne są tu zbyt skąpe, mało efektywne oraz (gł. ze względu na dynamiczny rozwój metod korzystania z cyberprzestrzeni) przestarzałe. Dla przykładu wiele osób chciałoby usunąć informacje w Internecie, pojawiające się pod ich imieniem i nazwiskiem, ale: kontakt z operatorem sieci jest bardzo utrudniony, złożony wniosek w tej sprawie nie musi być zrealizowany, a jeśli nawet zostanie, to w sieciach będą krążyć zwielokrotnione kopie usuniętych plików. Oczywiście sytuacja taka stanowi naruszenie naszych powszechnie uzna-

2) Cyberprzestrzeń - pojęcie początkowo używane w powieściach ojca cyberpunku Williama Gibsona na określenie rzeczywistości wirtualnych, w których znajdowali się jego bohaterowie. Obecnie określa się nim przede wszystkim przestrzeń Internetu oraz innych mediów cyfrowych (np. telefonia komórkowa). Jest to właściwie przestrzeń informatyczna, a nie cybernetyczna. Jest ona określana jako nowego typu przestrzeń społeczna.

3) Nieco inaczej rzecz ujmują A. Adamski i W. Fijałkowski, którzy koncentrują się na przestępstwach kryminalnych, z natury mniej licznych oraz łatwiej penalizowanych.

nych praw, a także standardów odnoszących się do danych osobistych, stąd nie powinniśmy tego aprobować. Tym bardziej że jest to sprzeczne ze standardami unijnymi (w tym art. 8 Karty Praw Podstawowych oraz regulacja państw członkowskich UE, w tym Polski). Innym przykładem nagminnego łamania prawa przez dostarczycieli usług mailowych jest takie konfigurowanie programów obsługi poczty (np. sieć Aster), żeby zabronione prawem polskim SPAMy jednak docierały do użytkowników wbrew ich woli. Nie wspominając już o przestępstwach pospolitych oraz istniejących w omawianej sferze zagrożeniach dla praw dzieci i praw autorskich. Dlatego też istotna jest tutaj znajomość podstawowych standardów normatywnych.

W takiej sytuacji unijne regulacje prawne zasługują na szczególną uwagę. Warto pamiętać, że prawo unijne (a właściwie wspólnotowe - *acquis communautaire*) jest odmienne od krajowego i międzynarodowego. Stanowi ono autonomiczny system prawny o charakterze hierarchicznym, nadrzędny nad porządkami krajowymi państw członkowskich. Prawo wspólnotowe jest otwarte zarazem na normatywny wpływ prawa międzynarodowego, a zwłaszcza regulacji Rady Europy<sup>4</sup>. Z naszego punktu widzenia, najistotniejsze znaczenie, obok postanowień traktatów założycielskich (TWE, TUE) i Karty Praw Podstawowych, mają odpowiednie władze, struktury organizacyjne i agencja bezpieczeństwa<sup>5</sup>, normy ustanawiające dobrą administrację oraz regulacje specjalistyczne (ochrona programów i rozwiązań technicznych, netykieta, ochrona praw autorskich i wizerunku), sieci w służbie praw, normy unijne a prawa człowieka w cyberprzestrzeni (prawo do cyberprzestrzeni a zagrożenie praw), prawa osób narażonych na dyskryminację. Przy tym warto pamiętać, że zakres ochrony praw człowieka<sup>6</sup> w Unii jest znacznie szerszy<sup>7</sup> niż

4) Odnosi się to bezpośrednio do wszystkich regulacji ze sfery praw człowieka, a pośrednio do *Konwencji Rady Europy o cyberprzestępczości, otwartej do podpisu 23.11.2001 roku w Budapeszcie*, która została zalecona przez władze UE.

5) Wymienić tu zwł. należy: Agencję Praw Podstawowych Unii Europejskiej - rozporządzenie Rady (WE) nr 168/2007 z 15.02.2007 r. (Dz.U. L 53/2, 2007), korzystającą z Europejskiego Centrum Monitorowania Rasizmu i Ksenofobii - rozporządzenie Rady (WE) nr 1035/97 z 2.06.1997 r. (Dz.U. L 151, 1997), a także Europejską Sieć i Agencję Bezpieczeństwa Informatycznego - rozporządzenie Rady (WE) PE i Rady nr 460/2004 z 10.03.2004 r. (OJ L 2004, 77/1), decyzja ramowa Rady nr 2005/222/JHA z 24.02.2005 r. (OJ L 2006, 64/1) oraz Program Bezpieczny Internet Plus 2005-2008 przyjęty decyzją PE i Rady nr 854/2005/WE 11.05.2005 (OJ L 2005, 141/1).

6) Prawa człowieka są pojęciem nieostrym i trudnym do zdefiniowania. Najczęściej (i najtrafniej) uważa się za nie zespół praw i wolności posiadających ochronę prawną. Por. W. Czapliński, A. Wyzomska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Wyd. C. H. Beck, Warszawa 2004, Nb.382.

7) Szerszy jest też (kwantytatywny) zakres praw, co musi wpływać na mniej efektywną ochronę. Ważne tu jest powiązanie z EKPC. Pojawiają się w tym systemie najwcześniej prawa nowe, jak np. do środowiska, do informacji, do dobrej administracji.

w systemach krajowych i międzynarodowych, co wynika z charakteru porządku prawnego (receptje unormowań z innych systemów oraz interpretowanie regulacji prawnych w kontekście całego *acquis*).

## Pojęcie systemu ochrony prawnej UE

Aktualny porządek prawny Wspólnot i UE (*acquis communautaire*) zapewnia osobom fizycznym i prawnym (w tym firmom) dostęp do szerokiego wachlarza instrumentów ochrony ich praw (*praw podmiotowych*). Można stwierdzić, że zespół tych środków to największy w dotychczasowych porządkach prawnych zakres instrumentów tego typu, a obejmuje on oprócz regulacji służących interesom ogólnym, środki sądowe i liczne instrumenty ochrony pozasądowej. Problematyka ta jest w Polsce mało znana i rzadko wykorzystywana w indywidualnej praktyce. Dotychczasową słabością tak zarysowanego systemu ochrony UE była słaba harmonizacja i koordynacja poszczególnych jego elementów, co wpływało negatywnie także na efektywność wspomnianych instrumentów oraz rodziło obserwowane zwł. ostatnio tendencje (*vide* orzecznictwo ETS) do usuwania takich mankamentów. Traktat Lizboński stanowić tu może wielką zmianę jakościową, zapewniającą jedność systemu... Należy wskazać, że - obok ochrony praw podmiotowych - system prawny (który powinien być spójny, niesprzeczny i efektywny) ma za zadanie również, jeśli nie przede wszystkim, ochronić interesy ogólne, w tym zwłaszcza Unii i państw członkowskich, obejmując swym zakresem m.in. zapobieganie i zwalczanie przestępczości. Istotniejszym z zadań jest tu budowa wspólnej przestrzeni bezpieczeństwa i sprawiedliwości UE. Niezwykle ważny jest tu zakres ochrony praw, czyli odpowiedź na pytanie, jakie kwestie i struktury wchodzą do systemu ochrony prawnej UE<sup>8</sup>.

W praktyce państw członkowskich UE system ochrony prawnej obej-

8) J. Bodio, G. Borkowski, T. Demendecki *Ustrój organów ochrony prawnej, część szczegółowa*, Zakamycze 2005; I. Malinowska, *System organów ochrony prawnej w państwach Unii Europejskiej* [w:] *Polska - Unia Europejska*, (red.) K. A. Wojtaszczyka, Warszawa 2003; I. Malinowska, *Zróżnicowanie modeli ochrony prawnej w państwach Unii Europejskiej*, „Przegląd Europejski” 2(5)2002, s. 41-69. Bodio i Borkowski, obok systemu sądowego jako organów ochrony prawnej wymieniają zakresy takie jak: ochrona interesu publicznego, prokuratura, istota prokuratury, ewolucja prokuratury w Polsce, struktura, zadania, działanie prokuratury, ochrona finansów państwa, najwyższa izba kontroli, historia kontroli państwowej w Polsce, struktura i organizacja NIK, zadania i obowiązki NIK, ochrona praw obywatelskich, rzecznik praw obywatelskich, system ochrony praw obywatelskich, modele instytucji rzecznika w systemie organów ochrony prawnej, zadania i zasady działania rpo, ochrona pluralizmu środków przekazu i prawa do informacji, krajowa rada radiofonii i telewizji, zadania KRRiTV, status prawny członków KRRiTV, korporacyjne podmioty pomocy i obsługi prawnej, istota organów pomocy i obsługi prawnej, status prawny i zadania adwokatury, radców prawnych, notariatu i komorników sądowych, ochrona prawna w prawie Unii Europejskiej.

muje wszystkie instytucje wymiaru sprawiedliwości, a także te (spoza niego) które służą ochronie praw jednostek. Prawo wspólnotowe włącza je do systemu ochrony prawnej UE, uzupełniając o odnośne instytucje i struktury Unii i Wspólnot. System ten funkcjonuje na podstawie norm wspólnotowego dorobku prawnego (*acquis*). W sferze ochrony prawnej istotne znaczenie protekcyjne a także potencjalnie deliktowe tworzy cyberprzestrzeń. Normy odnoszące się do niej należy ujmować w kontekście całego *acquis*.

## Zarys pojęć rządu prawa i system ochrony prawnej w UE

Podstawowe znaczenie dla efektywności krajowych porządków prawnych państw UE mają ich systemy *organizacji wymiaru sprawiedliwości* obejmujące całokształt instytucji i struktur służących zapewnieniu poszanowania prawa w danym państwie<sup>9</sup>. W związku z pierwszeństwem i nadrzędnością prawa wspólnotowego (*acquis communautaire*) oraz jego bezpośrednim stosowaniem w porządkach krajowych, a także – z funkcjonowaniem sądów krajowych jako sądów wspólnotowych, powstawać muszą w takiej sytuacji dwa istotne pytania: a) Czy w chwili obecnej istnieje jednolity system ochrony prawnej Unii Europejskiej<sup>10</sup> lub powstanie on w bliskiej perspektywie? b) Czy (w przypadku odpowiedzi twierdzącej) krajowe systemy ochrony prawnej (w tym organizacje wymiaru sprawiedliwości) staną się częścią takiego systemu?

Jednak filarowa struktura Unii, w sytuacji kiedy współpraca w obszarach II i III filarów pozostaje ograniczona do metody międzyrządowej (a więc tylko do zakresu wspólnej zgody państw), sprawia że współpraca powyższa miała dotąd stosunkowo wąski, a często i wybiórczy charakter.

Postawione wyżej pytania są tym bardziej istotne i aktualne, że 13 grudnia ub.r. przyjęto Traktat Lizboński, który ma stworzyć (w momencie wejścia w życie, tj. 1.01.2009) jednolitą osobowość prawną Unii. Daje przesłanki ku takiej afirmacji takim tendencjom, tym bardziej że sferę współpracy policyjnej i sądowej (obecny III filar) Traktat umieszcza w TFUE (zastępującego obecny TWE), czyli w zakresie regulowanym ponadnarodowo (w przeciwieństwie do obszaru) obecnego II filara pozostawianego w TUE, a więc w zakresie regulacji międzyrządowej. Oznacza to powstawanie zintegrowanego i jednolitego systemu ochrony prawnej UE oraz jednoczesne przejście z porządku *acquis communautaire* do prawa unijnego (*acquis dell'Union*). Stwierdzenie to ma kapitalne znaczenie

9) Por. C. Mik, *Wymiar sprawiedliwości w Unii Europejskiej*, TNOiK, Toruń 2001, s. 27 i n.

10) Całokształt tego zagadnienia nie był w zasadzie podejmowany dotąd w piśmiennictwie polskim i zagranicznym (omawiano poszczególne elementy systemu fragmentarycznie, głównie albo współpracę trzeciofilarową albo prawa podmiotowe), a zagadnienie to ma niezwykle ważne znaczenie zarówno praktyczne, jak i teoretyczne.

nie tylko dla naszego bezpieczeństwa, ale również dla ochrony interesów i praw zarówno osób fizycznych i prawnych, jak i państw członkowskich. Kwestia odnosi się także do wszystkich ogniw polskiego wymiaru sprawiedliwości, a nie tylko sądów (w mniejszym zakresie prokuratur), które już od 1.05.2004 r. starają się sprostać wyzwaniom stawianym przez normy *acquis communautaire* (m.in. prowadząc odpowiednią akcję szkoleniową). Problem wiąże się także z rozwojem współpracy w ramach III filaru oraz w *Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości* UE. Ale unormowania te określając realizację praw podmiotowych osób fizycznych i prawnych, definiują zarazem efektywność  *rządów prawa* w Unii i państwach członkowskich, a także ochrony interesów organów państwa i samych państw oraz Unii i jej instytucji. Można przy tym mieć wątpliwość, czy – zwłaszcza w państwach nowych - umiemy (indywidualnie i zespołowo) korzystać z tak zarysowanego zakresu instrumentów pozostających już do naszej dyspozycji<sup>11</sup>. Dlatego zagadnienie to powinno zasługiwać na szczególną uwagę.

Traktat Lizboński wprowadza do TFUE w pięciu kolejnych rozdziałach tytułu IV *Przestrzeń wolności, bezpieczeństwa i sprawiedliwości* nowe regulacje (art. 61-69) stosowane bezpośrednio w państwach członkowskich, ustanawiając pojęcie *bezpieczeństwa wewnętrznego UE*. Normy tego tytułu zobowiązują parlamenty państw członkowskich do zapewnienia zgodności prawa wewnętrznego z tymi założeniami, a wszystkie ich władze – do zapewnienia efektywności regulacji unijnych w państwach UE. Wprowadzona zostaje współpraca operacyjna w sferze bezpieczeństwa, a także Stały Komitet koordynujący współpracę operacyjną w tym obszarze. Przepisy kolejnych rozdziałów regulują: kontrolę graniczną, azyl i migrację, współpracę sądową w sprawach cywilnych oraz karnych (rozdz. 3 i 4), a także współpracę policyjną. Ustanawiają ponadto Prokuraturę Europejską „w oparciu o Eurojust”, kompetentną do ścigania przestępstw przeciw interesom finansowym Unii oraz do wnoszenia spraw przed sądy krajowe... Takie ujęcie całości zagadnienia pozwala na uzyskanie jednolitości regulacyjnej i systemowej (tu - z uwzględnieniem praw jednostek), w sposób ponadnarodowy i bezpośrednio skuteczny w państwach członkowskich.

Ujednoczeniu uległy też prawa podmiotowe. Artykuł 6 TUE wprowadza zasady wolności i prawa określone przez Kartę Praw Podstawowych, jako zasady podstawowe Unii, a samą Kartę załączoną do Traktatu - jako jego integralną część. Unia (po 1.01.2009) przystępuje do Europejskiej konwencji praw człowieka (EKPC), a ponadto uznaje standardy EKPC jako ogólne zasady prawa UE. Normy powyższe są poszerzone przez za-

---

11) Por. P. Wawrzyk, *Polityka Unii Europejskiej w obszarze spraw wewnętrznych i wymiaru sprawiedliwości*, WAIp Warszawa 2007, s. 39 i n.



*sady demokratyczne* (tytuł II, eksponujący ideę społeczeństwa obywatelskiego) oraz część II TFUE *niedyskryminacja i obywatelstwo*. Poza uprawnieniami wynikającymi z tych norm, cały szereg praw ekonomicznych i społecznych może być podstawą roszczeń sądowych i pozasądowych wysuwanych wobec organów krajowych. Natomiast zasady udziału jednostek w dochodzeniu ich roszczeń przed ETS nie uległy zmianie.

Uwzględniając powyższe kwestie, można stwierdzić, że po wejściu w życie Traktatu Lizbońskiego, dzięki uporządkowaniu regulacji i ich ponadnarodowemu charakterowi, powstanie jednolity system ochrony prawnej UE (*de facto* zostanie rozwinięty i uporządkowany), co przyczyni się nie tylko do ochrony interesów Unii i państw członkowskich (w tym poprawy bezpieczeństwa), ale także do poszerzenia ochrony praw jednostek. Zapewnienie jego efektywności będzie jednak wymagało wielkiego wysiłku implementacyjnego instytucji krajowych.

## 2. Prawa osobiste i wizerunek

W Internecie bardzo często naruszane są standardy w sferze ochrony praw osobistych, w tym wizerunku.

### Naruszanie praw osobistych w Internecie

W Internecie oraz innych sieciach mogą podlegać – i często podlegają – naruszeniu wszystkie prawa, które wchodzą w sferze komunikacji elektronicznej. Chodzi tu zwłaszcza o **ochronę danych osobowych, o prawa osobiste, a zwł. prawo do godności i do wizerunku** (w tym – do *firmy* oraz ochrony adresów i stron internetowych), ochronę prywatności (i rodziny), prawa zawodowe, społeczne i kulturalne, a także o zakaz naruszania innych praw powodujących szkody, w tym uszczerbek majątkowy (prawa ekonomiczne, przemysłowe, autorskie itp.). Ochrona pierwszej grupy prawa (praw osobistych) uległa - wskutek żywiołowej praktyki użytkowników Internetu – pewnemu zawężeniu. Stało się praktycznie niekaralne powielanie opublikowanych informacji, nawet jeśli kolidują one z dobrami osobistymi, choć takie ujęcie nie jest jednoznaczne. Powielanie informacji szkodzących wizerunkowi jednostki musi podlegać penalizacji. Podobnie należy traktować nawet nieumyślne wyrządzenie szkody. Natomiast korzystanie z czyichś dóbr i praw musi być (i jest) karane, acz instrumenty ochrony nie są tu zbyt silne.

Naruszeniem praw osobistych jest też przesyłanie niezamówionych informacji i ofert handlowych (SPAM), co narusza ustawę z 18.7.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 ze zm.) oraz jest czynem nieuczciwej konkurencji w rozumieniu ustawy z 16.4.1993 r.

o zwalczaniu nieuczciwej konkurencji (tekst jedn. Dz.U. 2003, nr 153 poz. 1503). Zadośćuczynieniem przez firmę, która naruszyła te ustawy było zwykle umieszczenie w ogólnopolskim wydaniu dziennika oświadczenia o stosowaniu praktyk naruszających zbiorowe interesy konsumentów<sup>12</sup>.

Dawniej (przed 2002 r.) niektórzy operatorzy, w tym *Wirtualna Polska*, powszechnie stosowali tę praktykę. Nazwa *spam* została zapożyczona z „Latającego cyrku Monthly Python’a” na określenie prób „wciskania” klientowi czegoś czego on nie zamawiał. Spam narusza nie tylko zakres naszej wolności osobistej, w tym handlowej, ale także szereg innych praw osobistych, dlatego jest sprzeczny z prawem międzynarodowym, w tym z prawem wspólnotowym i ustanowionym w systemie Rady Europy. Przesyłaniu *spamu* towarzyszy zwykle naruszanie zasady poufności korespondencji oraz przekazywanie danych adresowych (to ostatnie zwykle bez wiedzy i zgody właściciela). Jak wykazuje to K. Kowalczyk-Bańczyk praktyka ta stanowi naruszenie norm Europejskiej Konwencji o Ochronie praw Człowieka oraz przepisów wielu aktów WE (art. 286 TWE, dyrektyw: 95/46/WE i 200/31, rozporządzenia 45/2001<sup>13</sup>, dyrektywy 2002/58/WE)<sup>14</sup>.

## **Prawo do wizerunku i ochrony danych osobowych**

Prawo ochrony wizerunku jest jednym z praw obywatela, o których mowa w rozdziale II Konstytucji Rzeczypospolitej Polskiej. Ochrona wizerunku wynika z art. 30 i 47 Konstytucji RP, które zapewniają ochronę polegającą na nakazie poszanowania praw innych skierowanym do wszystkich. Ograniczenia w korzystaniu z konstytucyjnych wolności i praw obywatelskich dopuszczalne są tylko w przypadkach ustanowionych w ustawie. Również przepisy Kodeksu cywilnego zawierają regulację dotyczącą ochrony wizerunku człowieka (art. 23) oraz uprawnienia związane z jego ochroną (art. 24). Takie usytuowanie prawa do ochrony wizerunku nakazuje szczególnie uważne i ostrożne podejście do kwestii publikacji w prasie i w Internecie (w sieciach) wizerunków osób. Wizerunek osoby podlega szczególnej ochronie i nie może być dowolnie publikowany, chyba że istnieje ustawowe ograniczenie prawa ochrony wizerunku albo zgoda na publikację takiego wizerunku osoby, której to prawo przysługuje, a nadto istnieją szczególne przesłanki określone w prawie. Prawo prasowe (ustawa z dnia 26 stycznia 1984 r., Dz. U. nr 5, póź. 24 z późn. zm.) reguluje kwestię dopuszczalności publikacji wizerunku osoby, przeciwko której toczy się

12) Niezależnie od powyższej regulacji niektóre firmy dostarczające Internet wycinają z programów operacyjnych poczty możliwość indywidualnego eliminowania SPAM (tak czynił dotychczas ASTER).

13) OJ L 2001 nr 6.

14) K. Kowalczyk-Bańczyk, *Ochrona przed spamem w przepisach wspólnoty Europejskiej*, „Prawo i Podatki w Unii Europejskiej”, nr 1/2006, s. 2-7.

postępowanie przygotowawcze lub sądowe. Art. 13 ust. 2 ustanowił zezwolenie publikacji wizerunku osoby za jej zgodą, a art. 13 ust. 3 - bez zgody tej osoby albo nawet wbrew jej woli, ze względu na ważny interes społeczny na podstawie decyzji właściwego prokuratora lub sądu. Kodeks cywilny oraz inne przepisy chronią również wizerunek osób prawnych oraz podmiotów gospodarczych (nadając wizerunkowi obok wartości moralnej, walor ekonomiczny), do których należy stosować podobne zasady.

Prawo wspólnotowe zapewnia obu typom wizerunku szerszą niż w prawie krajowym ochronę prawną. Ochrona ta odnosi się również do wszelkich publikacji w Internecie, gdzie w zasadzie nie powinny również pojawiać się żadne informacje powstające w sposób sprzeczny z wymienionymi postanowieniami oraz z normami chroniącymi dane osobowe.

### **3. Unijne regulacje dotyczące sankcji karnych i warunkowego dostępu**

#### **Dyrektywa w sprawie sankcji karnych**

Problem ujednoczenia sankcji karnych w państwach członkowskich za naruszenie norm wspólnotowej ochrony własności intelektualnej był rozważany od kilku lat m.in. w trakcie przyjmowania Dyrektywy PE i Rady 2004/48/WE z 29.04.2004 r. w sprawie wzmocnienia praw własności intelektualnej<sup>15</sup>. Różnice kar w systemach krajowych utrudniają skuteczną walkę przeciw podrabianiu i piractwu, których rozprzestrzenianiu sprzyja powszechne korzystanie z Internetu. Wprowadzenie skutecznych kar wymaga też art. 61 porozumienia TRIPs. Dyrektywa zakłada karanie za umyślne przestępstwa podrabiania i piractwa (sprawstwo, współudział, usiłowanie, nakłanianie). Jako sankcje przewiduje się konfiskatę, przepadek i niszczenie nielegalnych towarów oraz kary więzienia, sankcje finansowe i przepadek mienia, a także stały lub czasowy zakaz prowadzenia działalności handlowej (gospodarczej), zakaz korzystania z dotacji publicznych, nadzór sądowy i postępowanie likwidacyjne oraz publikowanie orzeczeń. Przygotowywany równoległe akt wykonawczy w postaci Decyzji ramowej Rady przewiduje m.in. minimalną karę więzienia 4 lata oraz grzywnę 100 do 300 tys. euro. Oba akty prawne powinny być przyjęte w 2007 roku, a państwa członkowskie będą miały 18 miesięcy na ich transpozycję do systemów wewnętrznych.

15) OJ L 2004, 157, 45.

## Usługi o warunkowym dostępie

W 2000 r. Wspólnota Europejska wprowadziła w życie postanowienia Traktatu Światowej Organizacji Własności Intelektualnej (WIPO)<sup>16</sup> o wykonaniach artystycznych i fonogramach<sup>17</sup>. Traktat ten (WPPT) pierwotnie został przyjęty w Genewie w 1996 r., a był otwarty do podpisu dla państw i Wspólnoty Europejskiej (która podpisała Traktat) do 31.12.1997 r. Obecnie jego postanowienia, jako część prawa wspólnotowego, obowiązują ponadnarodowo państwa członkowskie. Zważywszy, że treść tych przepisów musi uwzględniać normy i zasady *acquis* (przez co nabierają one szerszego i zmienionego nieco znaczenia), powstać może więc ciekawa sytuacja, kiedy państwo, które przystąpiło do WPPT popadnie w konflikt między bezpośrednim stosowaniem norm traktatu, a stosowaniem odpowiednich norm wynikających z *acquis*<sup>18</sup>, co odnosi się do usług o warunkowym dostępie.

Odrębnej regulacji w prawie wspólnotowym poddano usługi polegające na warunkowym dostępie do korzystania z nich, takie jak płatna telewizja i radio, usługi audio i wideo, usługi *on-line*, które przekazywane są drogą elektroniczną. Są one płatne w formie subskrypcji albo płatności doraźnej (tzw. *pay-per-view*) oraz przekazywane jedynie na skonkretyzowane żądanie indywidualnego odbiorcy. Prawo wspólnotowe gwarantuje tu swobodę świadczenia tego rodzaju usług na obszarze całej Wspólnoty, czyli na terytorium każdego państwa członkowskiego, zakazując władzom krajowym wprowadzania ograniczeń w tym zakresie. Nie obejmuje to jednak działań służących zwalczaniu faktów naruszania praw legalnych nadawców, polegających głównie na umożliwianiu nieuprawnionego dostępu do ich usług. Państwa zostały także zobowiązane do skutecznego przeciwdziałania produkcji, importowi oraz udostępnianiu lub instalacji w jakiegokolwiek formie urządzeń pozwalających na bezprawne korzystanie z takich usług. Powinny zarazem umożliwić poszkodowanym świadczeniodawcom dochodzenie reparacji szkody oraz występowania o zajęcie takich urządzeń<sup>19</sup>. Podstawowym aktem prawnym jest tu Dyrektywa Rady nr 98/84/WE dotycząca prawnej ochrony usług o warunkowym dostępie.

16) Konwencja o ustanowieniu WIPO została sporządzona w Sztokholmie 14.07.1967 r. Polska jest jej stroną od 1975 r. – ratyfikacja Dz.U. 1975 nr 9 poz. 50 (oświadczenia rządowe – poz. 49 – 51).

17) Decyzja o przystąpieniu i umowa - OJ L 89 2000, s. 15-23.

18) Traktat nie narusza zobowiązań z Międzynarodowej Konwencji o ochronie artystów wykonawców, producentów fonogramów oraz organizacji nadawczych, sporządzonej w Rzymie w dniu 26 października 1961 r. (zwaną „Konwencją rzymską”). Ochrona WPPT nie ma żadnego wpływu na ochronę praw autorskich do utworów literackich i artystycznych, żadne postanowienie nie może być interpretowane jako naruszające taką ochronę (art. 1).

19) Dyrektywa Rady nr 98/84/WE dotycząca prawnej ochrony usług o warunkowym dostępie (OJ L 1998, 320,54).

## 4. Ochrona sieci, topografii, programów, algorytmów w UE

### Informacje ogólne

Wspólnotowe regulacje ochrony praw osobistych (w tym własności intelektualnej) obejmują również korzystanie z Internetu, a także sprzętu elektronicznego i oprogramowania. Wszystkie prawa materialne i niematerialne, chronione w *acquis communautaire*, chronione są również w sferze komunikacji elektronicznej, w tym w sieciach informatycznych, a także w Internecie. Szczególne znaczenie ma tu nie tylko ochrona praw majątkowych (w tym –własności intelektualnej), ale i praw osobistych, w tym prawa do wizerunku oraz poszanowania zasad grzeczności, często utożsamianych z netykieta<sup>20</sup>. Z tym wiążą się również kwestie bezpieczeństwa, co do których przyjęto standardy prawne i organizacyjne. Należy tu wskazać na Europejską Sieć i Agencję Bezpieczeństwa Informacyjnego (ENISA)<sup>21</sup> oraz Program Bezpieczny Internet Plus 2005-2008. Groźnym przestępstwem jest *phishing*, czyli *oszukańcze pozyskanie poufnej informacji osobistej*, takiej jak hasło czy numer karty kredytowej, w celu uzyskiwania korzyści majątkowych.

### Ochrona topografii, programów i baz danych

Ochrona praw w sferze topografii półprzewodników (obwodów scalonych), programów komputerowych i algorytmów informatycznych, jeśli chodzi o zakres i specyfikę ochrony, nosi w sobie i pewne cechy typowe dla praw intelektualnych (programy komputerowe) oraz dla własności przemysłowej (topografia układów). Ochronę topografii reguluje głównie dyrektywa Rady nr 87/54/EWG z 16.12.1986 roku w sprawie ochrony prawnej topografii wyrobów półprzewodnikowych. Z kolei dyrektywa Rady nr 91/250/EWG z 14.05.1991 r. wprowadza ochronę prawną programów komputerowych. Zbliżoną sferę regulują też dyrektywy: nr 96/91/WE o ochronie baz danych, z 13.13.1999 r. o podpisie elektronicznym oraz z 8.06.2000 r. o handlu elektronicznym. Rosnące znaczenie ma też ochrona znaków towarowych oraz domen i nazw w Internecie<sup>22</sup>, problem który doczekał się już znaczącej liczby orzecznictwa TS. Pojęcie topografii komputerowych

20) Obejmuje ona nie tylko zasady grzeczności (w tym zakaz używania słów wulgarnych i obraźliwych), a także zakaz niedozwolonej reklamy handlowej (w tym spamu), która narusza ustawę z 18.7.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. Nr 144, poz. 1204 ze zm.).

21) Główne regulacje to: Rozporządzenie (WE) PE i Rada nr 460/2004 z 10.03.2004 r. (OJ L 2004, 77/1) oraz decyzja ramowa Rady nr 2005/222/JHA z 24.02.2005 r. (OJ L 2006, 64/1).

22) M. Kondrat, *Znaki towarowe w Internecie*, Dom Wyd. ABC, Warszawa 2001, s. 121-142.

obejmuje przestrzenne projektowanie rozmieszczania elementów elektronicznych i sposobu ich łączenia w ramach układu scalonego, stając się niezbędnym dla funkcjonowania urządzeń i uzyskiwania ich pożądanych rozmiarów. Jest to dziedzina o stosunkowo krótkiej tradycji i nie zawsze klasyfikowana w ramach prawa patentowego. Ale niewątpliwie jej przedmiot spełnia niezbędne przesłanki uzasadniające konieczność ochrony, gdyż topografia może podlegać reprodukcji i być wykorzystana w obrocie. Ochrona obejmuje więc stworzone indywidualne topografie stanowiące konsekwencję wkładu intelektualnego autora i nienależące do powszechnego dorobku przemysłu półprzewodników. Przyznawana jest na podstawie rejestracji przez odpowiednie władze państw członkowskich. Jej okres wynosi 10 lat od końca roku kalendarzowego, w którym (licząc od pierwszego ze zdarzeń): złożono stosowny wniosek w tym względzie albo nastąpiło zastosowanie, nie wcześniej niż 2 lata wstecz od pierwszego komercyjnego wykorzystania. Dłuższa rozbieżność tych zdarzeń powoduje bowiem utratę prawa do ochrony. Przysługuje ona przede wszystkim twórcom będącym osobami przynależnymi do z jednego z państw członkowskich, o ile przepisy krajowe nie regulują odrębnie praw do topografii wytworzonych przez twórcę w ramach stosunku pracy. Podlegają jej także osoby fizyczne i prawne, które posiadają stosowne upoważnienie uprawnionego, a które po raz pierwszy w sposób komercyjny wykorzystaly topografię niezastosowaną jeszcze nigdzie wcześniej. Korzystają one z praw zbywalnych i wyłącznych. Licencja obejmuje zgodę komercyjnego wykorzystania, z zakazem kopiowania, a także obrotu samą topografią i półprzewodnikami wykonanymi z jej zastosowaniem. Wyjątkiem natomiast są przypadki kopiowania dla celów analizy oraz naukowo-dydaktycznych, dotyczących topografii, jej koncepcji, techniki oraz zasad działania wykorzystanych przy jej przygotowaniu. Pierwotnie nie przewidywano udzielenia ochrony na podstawie uprzedniej rejestracji dokonanej w krajach nieczłonkowskich, pozostawiając to uznaniu poszczególnych państw, rezygnując z wzajemności oraz wspólnej ogólnoświatowej ochrony, ponieważ eliminowało to kraje będące potęgami w tym zakresie, co nie zabezpieczało odpowiednio interesów producentów wspólnotowych. Dlatego kolejne decyzje Rady rozszerzyły ochronę dyrektywy na pochodzące z państw WTO.

Należy zwrócić uwagę, że prawo wspólnotowe pośrednio reguluje także obowiązywanie licencji patentowych, licencji technologii i know-how, modeli funkcjonujących jako uzupełniające wzory użytkowe, topografie półprzewodników, certyfikaty roślin hodowlanych oraz certyfikaty dodatkowej ochrony, jaka może być udzielona w niektórych przypadkach. Uregulowanie to zostało przygotowane na potrzeby prawa konkurencji w rozporządzeniu 240/96, ale zawiera wiele cennych przepisów dotyczą-

cych samej konstrukcji tego rodzaju licencji. Warto zwrócić uwagę przede wszystkim na legalną definicję umowy know-how. Obejmuje ona prawo do przekazania za wynagrodzeniem z zachowaniem poufnego charakteru oraz upoważnienia do wykorzystywania objętej tajemnicą metody, sposobu lub innowacji o charakterze techniczno-produkcyjnym, którą można i jako istotną z punktu widzenia procesu wytwórczego albo proza ta stanowi pewien całościowy zbiór informacji, które mogą nawet posiadać powszechny charakter i dopiero w całości tworzą nową jakość umożliwiającą komercyjne wykorzystanie. Ze względu na brak jej ogólnej dostępności przedstawia ona określoną wartość, może znajdować się w obrocie i dlatego musi być chroniona nieuprawnionym ujawnianiem oraz używaniem<sup>23</sup>.

## Algorytmy informatyczne w Unii Europejskiej

W końcu 2004 r. po raz kolejny rozpatrywano projekt dyrektywy WE ustanawiającej prawa wyłączne na algorytmy (pojedyncze rozwiązania i elementy programów, np. sposób generowania kolorów<sup>24</sup> lub automatycznej transmisji komunikatów itp.) programów elektronicznych. Pierwszemu projektowi aktu nie nadano dalszego biegu z powodu sprzeciwu Polski (nasz kraj na Radzie UE w końcu grudnia ub.r. poprosił o odłożenie jego rozpatrywania). Powrócono do tego projektu na początku 2005 roku, podczas prezydencji Luksemburga (który naciskał na podjęcie projektu)<sup>25</sup>. Polska chciała zaproponować na posiedzeniu Rady (ale jedynie w przypadku powstania „wątpliwości”) decyzję o powrocie tego projektu do pierwszego czytania, na co konieczna byłaby zgoda wszystkich pozostałych krajów... Ostatecznie sprawa skończyła się odłożeniem regulacji tego zagadnienia *ad calendas grecas*. Specyfika problemu polega na tym, że przyjęcie takiej dyrektywy byłoby bardzo korzystne dla dużych koncernów (np. Microsoft) oraz szkodliwe dla małych firm, a ponadto – prowadziłoby do ograniczenia praw prywatnych użytkowników Internetu oraz całkowitego wyeliminowa-

23) Stosownie do przepisów Rozporządzenia 240/96 umowa licencyjna w zakresie własności przemysłowej ma charakter odpłatny o z góry określonych zasadach.

24) W USA, gdzie unormowano rejestrację algorytmów, zgłoszono tysiące patentów. Zarejestrowano m.in. (znane powszechnie, proste) generowanie kolorów, a właściciel patentu „ściga” teraz setki tysięcy firm i osób, które mają komputery, żądając odszkodowania oraz opłat.

25) Po sprzeciwie rządu polskiego internauci całej Europy zaczęli ślać listy z podziękowaniami i składać rządowi polskiemu gratulacje (założono stronę internetową *Thank You Poland*, na której w ciągu kilku tygodni znalazło się 25 tys. e-maili). Jednakże pojawiła się pogłoska, że negatywne stanowisko naszego rządu wynikało z pomyłki, gdyż wcześniej Polska wyraziła już w strukturach Rady pozytywną opinię w sprawie projektu tego aktu. Po ponownym podjęciu tego projektu jest problem, czy rząd polski będzie mógł teraz (po poprzedniej zgodzie) głosować przeciw projektowi. Zaczęto więc poszukiwać proceduralnych sposobów zablokowania (np. sprawdzanie, czy istnieje wymagana większość) projektu, który nadal jest na liście A. Por. K. Niklewicz, *Patenty wracają*, „Gazeta Wyborcza”, 21.01.2005, s. 30.

nia z rynku darmowych programów, w tym Linuksa (wykorzystywanego w pracach wiele ośrodków naukowych). Takie rozwiązanie mogło więc okazać się bardzo dotkliwym dla młodzieży i społeczności akademickiej. Przy okazji okazało się, że istnieją pewne luki w prawie patentowym w sferze własności przemysłowej (wystarczy np., że został zgłoszony projekt rozwiązania czy programu, które nie muszą działać, czyli być operatywne), pozwalające na „zarezerwowanie” prawa do przyszłych, nieistniejących jeszcze rozwiązań i programów na rzecz jakiejś firmy.

## Własność intelektualna w Internecie

W prawie wspólnotowym istnieją nieliczne regulacje przedmiotowe. Odnoszą się one m.in. do ochrony danych, dostępu do nich oraz do sposobów komunikacji między instytucjami WE i państwami członkowskimi (regulacje wewnętrzne). Ogólną zasadą *acquis* jest zakaz naruszania praw chronionych innych podmiotów. Głównie spraw naruszeń tego typu dotyczyło orzecznictwo Trybunału Sprawiedliwości WE związane z omawianą problematyką. Funkcjonowanie poszczególnych sieci oraz ich administracja podlega porządkom (systemom prawa) krajowym<sup>26</sup>. Znaki towarowe oraz innych kategorii własności przemysłowej i intelektualnej w Internecie mogą występować w różnych aspektach funkcjonowania sieci. Ich obecność i ochrona może dotyczyć zamieszczania danych i informacji w Internecie oraz handlu i wymiany. We wszystkich tych przypadkach stosuje się *mutatis mutandis* adekwatne do chronionego dobra znane przepisy. Inną nieco kwestią są domeny i ich rejestracja.

## Prawo znaków towarowych w Internecie

Należy podkreślić, że funkcjonowanie poszczególnych sieci krajowych oraz ich administracja podlega porządkom (systemom prawa) krajowym poszczególnych państw. Znaki towarowe oraz inne kategorie własności przemysłowej i intelektualnej w Internecie mogą występować w różnych aspektach funkcjonowania sieci. Ich obecność i ochrona może dotyczyć zamieszczania danych i informacji w Internecie oraz handlu i wymiany, a także tworzenia adresów i stron internetowych. We wszystkich tych przypadkach stosuje się *mutatis mutandis* adekwatne do chronionego dobra przepisy chroniące prawa posiadacza znaku, wzoru lub nazwy, a także prawa autorskie. Inną nieco kwestią są domeny i ich rejestracja. W większości państw domeny (strony internetowe) są rejestrowane na zasadzie pierw-

26) Innym zagadnieniem jest zdominowanie administracji globalnej Internetu przez USA, co może być (i bywa) wykorzystywane jako narzędzie dominacji w różnych sferach. Stąd na uwagę zasługują próby utworzenia sieci niezależnych, a także budowy własnych zbiorów domen. Wspólnoty uruchomiły w 2005 r. tu zbiór domen z rozszerzeniem .ue.



szeństwa, a głównym kryterium rejestracji jest brak identycznej nazwy (domeny). W związku z tym zdarzają się przypadki zgłaszania do rejestracji jako domeny marek i nazw firm. Prowadzi to do sytuacji blokowania ich właścicielom możliwości posiadania adresu i strony z własną nazwą. Z kolei zarejestrowanie strony o zbliżonej nazwie do uznanej firmy powoduje tzw. przekierowania komunikacji internetowych. Oczywiście praktyki te są niedozwolone, ale dla ochrony przed nimi (i obrony własnych praw) trzeba zwracać się do sądu lub arbitrażu. Dopiero prawomocne orzeczenia stanowią podstawę do usunięcia takich nadużyć. Możliwe jest też orzecznictwo polubowne znane i stosowane w sferze konkurencji.

### **Zawłaszczanie domen, czyli cybersquatting i tipesquatting**

Ostatnio zmorą właścicieli praw do nazw znanych firm oraz znaków towarowych są zjawiska zwane z języka angielskiego *cybersquatting* i *tipesquatting*. Pierwszy przestępczy proceder polegał na zarejestrowaniu na określonym rynku domeny internetowej (adresu) z nazwą znanej firmy lub znaku towarowego, najlepiej wchodzącego na rynek, celem wymuszenia wykupienia go za wysoką cenę przez posiadacza praw, „najlepiej” wchodzącego na dany rynek. Za „sprytnie” zarejestrowaną nazwę uzyskiwano w Polsce nawet ponad 100 tys. zł. Tak było w przypadku startu do przetargu na telefonię komórkową firmy Hutchison, a wcześniej Netii, Microsofta, Orange itp. Drugi proceder polegał na zmianie litery (albo ich ilości czy wielkości) w sposób pozwalający na ich wyszukanie razem z nazwą oryginalną. Pomimo że są to przestępstwa, to można je ścigać po wygraniu sprawy sądowej. A tu należy udowodnić, że rejestrujący działał celowo na szkodę firmy lub chciał wymusić wykupienie domeny, co czasami jest trudne<sup>27</sup>. W przypadku przegranej sprawy *intruz* musi oddać domenę i często zapłacić odszkodowanie. Ale sprawy ciągną się długo, stąd wiele firm odkupuje domeny z własną nazwą. W Polsce nie ma jeszcze penalizującego ten proceder aktu prawnego, ale ze względu na członkostwo w UE można jednak odwołać się do Komisji Europejskiej. W USA za podobne naruszenie grozi kara 100 tys. USD. Przykładem spraw naruszających prawo była domena Microsoft R. Rudeckiego z Łodzi, który sprzedawał zioła, zakończona wyrokiem Sądu Okręgowego. Z kolei Centrum Handlowe Janki, po dwóch latach sądowych przepychanek, kupiło własną domenę od intruza. Czasami podobne uzyskanie domeny może nie być przestępstwem, np. spółka Migut Media przejmując firmę za długi, odziedziczyła domenę Orange (wartą jak się okazało 200 tys. euro), którą to nazwę przyjął jako firmową France Telecom, inwestor strategicz-

27) Dla przykładu właściciele domen z nazwami: trzy, 3, three mogą tłumaczyć się, że to ich ulubione liczby.

ny TP SA. Ostatnio hitem są rejestracje domen Benedykt XVI, a tu nie wiadomo, kto miałby sprawców ścigać: Watykan, lokalny episkopat czy sam papież<sup>28</sup>.

## Pozasądowa ochrona praw człowieka a sieci .net

Unia Europejska i Wspólnoty Europejskie w sferze funkcjonowania swych struktur intensywnie i efektywnie wykorzystują cyberprzestrzeń. Kontakty poprzez sieci NET, w tym Internet, są szeroko wykorzystywane w dostępie do informacji publicznej, formułowaniu petycji i skarg oraz w kontaktach z urzędami, nie wspominając już o chronionych sieciach wyspecjalizowanych o charakterze ekonomicznym, Frontexu oraz współpracy policyjnej i sądowej. Sieci te służą też ochronie praw jednostek, w tym ekonomicznych i konsumenckich (o czym niżej), ochronie określonej jako pozasądowa.

W prawie wspólnotowym (unijnym) chronione są prawa osób fizycznych i prawnych (jednostek) zarówno w sposób sądowy (przed ETS oraz sądami krajowymi działającymi jako wspólnotowe) na podstawie przewidzianych prawem WE roszczeń, jak też w sposób pozasądowy. Skarga osoby fizycznej lub prawnej do ETS może dotyczyć tylko naruszeń dokonanych przez instytucje i organy WE. Z kolei ochrona pozasądowa<sup>29</sup> przysługuje w szerszym zakresie (bo nawet tam, gdzie nie ma podstaw do roszczeń) i obejmuje: prawo petycji do Parlamentu Europejskiego, prawo skargi do Ombudsmána (ERPO) oraz prawo wnoszenia pytań i skarg do Komisji oraz innych instytucji WE<sup>30</sup>. Tak zarysowaną, klasyczną ochronę pozasądową uzupełniono w latach 90. prawem zwracania się z pytaniami do instytucji oraz dostępu do dokumentów publicznych, prawem skarg do Komisji w związku z naruszeniem prawa wspólnotowego (zwł. w zakresie: zmowy kartelowej, pomocy publicznej, subsydiów i *dumpingu*), a także prawem do informacji i skarg wobec krajowych władz państw WE. Do tego typu ochrony należy zaliczyć także środki służące ochronie konsumenta<sup>31</sup>, a także ochronie zdrowia i ochronie środowiska. Środki pozasądowe są łatwiej dostępne, tańsze, prostsze i bardziej efektywne. Ponad-

28) P. Rożyński, *Domeneę sprzedam*, „Gazeta Wyborcza”, 7.05.2005, s. 37.

29) Czasem na ochronę pozasądową używa się nazw: alternatywne rozstrzyganie sporów, skargi pozasądowe, koncyliacyjne rozwiązywanie problemów itp. Wydaje się to niezbyt trafne, gdyż pojęcia wymienione w dalszej kolejności są węższe. Skrótowe oznaczenie sieci pochodzi od ich nazw angielskich.

30) Por. A. Łazowski, *Ochrona praw jednostek w prawie Wspólnot Europejskich. Pozasądowe mechanizmy ochrony praw przed instytucjami i organami WE*, Wyd. Zakamycze, Kraków 2002, s. 25.

31) Por. Z. Brodecki (red.), *Konkurencja*, Wyd. LexisNexis, Warszawa 2004, s. 19 i n. oraz E. Łętowska (red.), *Nieuczciwe klauzule w prawie umów konsumenckich*, Wyd. C. H. Beck, Warszawa 2004, s. VII i n.

to nie wykluczają (np. w razie niepowodzenia) skorzystania ze środków sądowych. Pod koniec lat 90. ubiegłego stulecia dla potrzeb niektórych form ochrony pozasądowej wprowadzono sieci informatyczne.

## **Powstawanie sieci służących ochronie praw konsumenckich**

W latach 1997-2001<sup>32</sup> w Unii Europejskiej zapoczątkowano prace nad tworzeniem elektronicznej sieci komunikacji służącej pozasądowemu rozstrzygnięciu sporów, a tym samym – jeszcze łatwiejszej w stosowaniu i skuteczniejszej ochronie praw jednostek (czyli osób fizycznych i prawnych), głównie ekonomicznych, bez konieczności angażowania organów wymiaru sprawiedliwości. Kolejno, na mocy odpowiednich decyzji oraz aktów prawnych władz UE i WE, powstawały sieci: Solvit (obejmująca zagadnienia rynku wewnętrznego), ECC (centra konsumenckie) i EEJ (europejska sieć pozasądowa, obie uległy później połączeniu), a następnie FIN-Net (sieć ws. finansowych) i ADR/ODR (alternatywne rozstrzygnięcie sporów). Sieci te stały się w pełni efektywne w latach 2002-2005 i od tego czasu są internetowo dostępne dla wszystkich podmiotów na obszarze Unii. Cechą wspólną wszystkich tych sieci jest to, że dla każdej z nich utworzono centra krajowe, dzięki czemu łatwiejsze jest (przy znajomości specyfiki i realiów krajowych) rozstrzygnięcie sporów. Wspólne są też dla nich (dostosowane do danej skargi) formularze, z możliwością ochrony danych, nieodpłatność oraz szybkość rozstrzygnięcia sporów (w czasie krótszym niż 10 tygodni). Chodzi przy tym o skłonienie podmiotu naruszającego prawo do (zaprzestania i) naprawienia naruszeń. Wykorzystywane są tu dwa mechanizmy: kontaktu konsumenta z biznesem (C2B) oraz kontaktu konsumenta i biznesu z administracją krajową (C2A, B2A)<sup>33</sup>. Sieci FIN-Net i Solvit mają specyfikę typowo transgraniczną, chociaż we wszystkich sieciach istnieje możliwość i praktyka rozstrzygnięcia sporów na styku różnych państw UE. Pretensje w ramach tych systemów wysuwane są zwykle w kwestii naruszania standardów (praktyki i prawa) *acquis* przez jedno z państw członkowskich, choć możliwe są też podobne pretensje do instytucji oraz organów UE i WE.

32) Z pewnych wyjątkiem dla *Euroguichet* istniejących od 1992 r.

33) Skróty według nazw angielskich, *vide* niżej.

## Sieć SOLVIT

Sieć SOLVIT została stworzona dla pomocy obywatelom i przedsiębiorstwom (firmom) w przypadku pojawienia się problemów związanych z niewłaściwym stosowaniem norm WE dotyczących rynku wewnętrznego przez administrację publiczną innego (niż przynależność podmiotu) państwa UE. Bazuje ona na krajowych centrach tworzonych począwszy od 1997 r. w państwach Unii. Pierwsze takie centra powstały w krajach skandynawskich i nordyckich, a następne we Francji, RFN i Włoszech. Udzielały one pomocy konsumentom krajowym, przeważnie na obszarach o zasięgu lokalnym<sup>34</sup>. Ideę scalenia tych ośrodków wysunięto w komunikacie dla KES i KR opublikowanym w 2000 roku Komisja zaproponowała:

- stworzenie do czerwca 2002 roku łatwiej w obsłudze unijnej bazy danych (sieci Solvit), która – poprzez przejrzystość - stymulowałaby państwa UE do wzajemnej presji (*peer pressure*) na rzecz respektowania odnośnych norm WE,
- wskazanie centrom koordynacyjnym jasnych zasad zarządzania siecią Solvit,
- przekazywanie „mediatorom europejskim” informacji służących harmonizowaniu interwencji krajowych,
- podejmowanie działań prewencyjnych celem eliminowania niewłaściwych sytuacji.

Następnie Komisja wydała rekomendację (zalecenie) z 7.12.2001 roku w sprawie zasad używania sieci Solvit dla rozwiązywania problemów w obszarze wspólnego rynku<sup>35</sup>.

Rynek wewnętrzny jest sferą, w której jednostki mogą swobodnie realizować swoje aspiracje, a duch przedsiębiorczości jest premiowany. Odnośne normy WE (które jeśli są respektowane) zapewniają wielkie korzyści, które jednak stają się nierealne przy niewłaściwym stosowaniu standardów *acquis*. Występujące przypadki błędów i niezrozumienia są często typowe, stąd mogą być łatwo eliminowane. Dlatego ważne tu jest zastosowanie szybkiego i skutecznego remedium, w tym rozwiązywania problemów i sporów, zapobiegania też nadużyciu prawa. Głównym zadaniem Komisji Europejskiej jest więc zagwarantowanie, by porządek *acquis* był w pełni respektowany przez państwa członkowskie, a zarazem, żeby pojawiające się na tym tle spory były jak najszybciej rozstrzygane (co poprawi pewność obrotu i zaufanie w sektorze prywatnym)<sup>36</sup>. W związ-

34) Podawane za: SEC(2001)924, [http://www.cc.cec/di/e-commission/docs/sec\\_2001\\_0924\\_en.pdf](http://www.cc.cec/di/e-commission/docs/sec_2001_0924_en.pdf) [dostęp: 2.07.2008] oraz Communication “Towards the e-Commission - EUROPA 2nd Generation” COM (2003).

35) Opublikowane w Dz.Urz. L nr 331, 15/12/2001, str. 0079 – 0082. Jest to zasadnicza podstawa prawna systemu.

36) Cfr. [http://europa.eu.int/comm/internal\\_market/en/finances/consumer/adr.htm](http://europa.eu.int/comm/internal_market/en/finances/consumer/adr.htm), [dostęp: 12.10.2011].

ku z tym, że procedury sądowe trwają często po kilka lat, konieczne jest efektywne i sprawne pozasądowe rozstrzygnięcie sporów, często nazywane alternatywnym – ADR). Przy czym, we współczesnym społeczeństwie informatycznym wskazane jest wykorzystywanie nowoczesnych metod porozumiewania się – sieci internetowych, co wymaga tworzenia służb rozwiązywania sporów *on line* (ODR)<sup>37</sup>. Sieć FIN-Net natomiast pozwala niezadowolonym konsumentom szybko rozwiązywać problemy związane z transgranicznym zakupem produktu finansowego. Innych przykładów dostarczała europejska sieć pozasądowa (EEJ), europejska sieć „okienek” dla konsumentów Euroguichet oraz systemy informacji Europa Direct i Euro Info<sup>38</sup>. Instrumenty powyższe bazują głównie na modelu relacji między konsumentem a przedsiębiorcą (*consumer-to-business* - C2B), podczas gdy sieć Solvit rozwiązuje problemy na styku konsumenta z administracją (*consumer-to-administration, business-to-administration* - C2A, B2A). Równoległe z wymienioną wyżej nową strategią wysunięto w 2001 r. inicjatywę stworzenia *E-Komisji*, w ramach której miano zapewnić łatwy dostęp obywatelom i przedsiębiorstwom do wszystkich służb Komisji Europejskiej udzielających informacji, konsultacji, porad oraz rozwiązujących problemy (z zamiarem wypracowania jednolitej strategii)<sup>39</sup>, o której pozytywną opinię wyraził KES i KR<sup>40</sup>. Inicjatywę poparła następnie Rada UE i Parlament Europejski. Po implementacji wskazanych przez Komisję działań (wraz z odnośnym budżetem – ok. 1,3 mln E), system Solvit osiągnął pełną sprawność w 2003 roku<sup>41</sup>. Instrumenty prawne Solvitu oparto na art. 95 TWE.

Usługi świadczone przez Solvit są bezpłatne. System prowadzi sprawy związane ze skargami złożonymi przez obywateli lub przedsiębiorstwa, osobiście lub też przez pośredników działających w ich imieniu. W tym ostatnim wypadku, jeśli pośrednicy nakładają na swoich klientów opłaty za świadczone usługi, Solvit może wymagać informowania klientów o bezpłatnym korzystaniu z usług sieci i może się z nimi bezpośrednio skontaktować. Ponadto jeżeli pośrednik jest doradcą prawnym, Solvit może wymagać

37) Por. <http://econfidence.jrc.it>. Komisja Europejska (w latach 2003-2005) opublikowała najpierw komunikat w sprawie ODR, a następnie zieloną księgę dot. ADR w sektorze prywatnym.

38) [http://europa.eu.int/europedirect/it/index\\_it.html](http://europa.eu.int/europedirect/it/index_it.html) oraz <http://europa.eu.int/comm/enterprise/networks/eic/eic.html>.

39) Por. SEC(2001)924. Opracowano i udostępniono wykaz potrzebnych w tym względzie adresów internetowych. Cfr.: [http://www.europa.eu.int/comm/dgs/press\\_communication/pdf/e2g\\_en.pdf](http://www.europa.eu.int/comm/dgs/press_communication/pdf/e2g_en.pdf) oraz [http://www.cc.cec/di/e-commission/docs/sec\\_2001\\_0924\\_en.pdf](http://www.cc.cec/di/e-commission/docs/sec_2001_0924_en.pdf), [dostęp: 12.10.2011].

40) CES 702/2001, 30-31.05.2001 oraz CDR 200/2001 Rev. 2, 14/15.11.2001.

41) Do października 2002 r. została stworzona interaktywna baza danych *on-line* (kompatybilna z innymi systemami), której e-mail: [Solvit@ec.europa.eu](mailto:Solvit@ec.europa.eu). Udostępniono państwo członkowskim.

przedkładania skarg wraz z analizą prawną i pełnym opisem znaczących faktów. Sieć może odmówić prowadzenia spraw, w przypadku których te kryteria nie zostały spełnione. Należy przy tym podkreślić, że Solvit:

- nie jest siecią informacyjną lub udzielającą porad prawnych,
- nie rozpatruje sporów pomiędzy przedsiębiorstwami, między przedsiębiorstwem a konsumentem ani skarg przeciwko instytucjom UE,
- zajmuje się wyłącznie problemami wynikającymi z niewłaściwego stosowania prawa UE przez władze publiczne w państwach członkowskich UE.<sup>42</sup>

SOLVIT zajmuje się w zasadzie każdym problemem o charakterze transgranicznym, między przedsiębiorstwem lub obywatelem z jednej, a organem krajowej administracji publicznej z drugiej strony, który dotyczy ewentualnego niewłaściwego stosowania prawa UE. Dotychczas Solvit zajmował się przede wszystkim problemami rynku wspólnego.

Przed podaniem danych osobowych wypełnia się kwestionariusz dotyczący ochrony prywatności (*privacy*). Następnie wypełnia się formularz zgłoszeniowy skargi *on-line*. Zgłoszenie sprawy do Solvit nie wpływa na bieg terminów wynikających z prawa krajowego, których należy przestrzegać dla zagwarantowania możliwości skorzystania z przysługujących praw (należy złożyć w terminie odwołanie od ew. decyzji, aby nie stracić do tego prawa)<sup>43</sup>. Oprócz załatwiania sporów (spraw) indywidualnych w krajowych centrach Solvit, Komisja Europejska prowadzi skrzynkę pocztową (adresową) systemu, gdzie można uzyskać praktycznie wszystkie potrzebne informacje<sup>44</sup>. W przypadku zainteresowania systematycznym otrzymywaniem nowych informacji o Solvit, należy zarejestrować się na „liście” poczty elektronicznej (*e-mailing list*)<sup>45</sup>. Nowe wiadomości będą zawierać też instrukcje, jak można wyrejestrować się z listy. Dostęp do listy jest ograniczony tylko dla służb Komisji Europejskiej odpowiedzialnych za Solvit.

Po wypełnieniu kwestionariusza prowadzące Centrum SOLVIT<sup>46</sup> potwierdza w terminie jednego tygodnia, czy zajmie się daną sprawą. Zależy to głównie od tego, czy uzna, że dana sprawa jest uzasadniona oraz jakie jest prawdopodobieństwo jej praktycznego rozwiązania. W niektórych sprawach

42) [http://europa.eu.int/comm/internal\\_market/en/update/citizen/](http://europa.eu.int/comm/internal_market/en/update/citizen/) oraz <http://citizens.eu.int/>, [dostęp: 12.10.2011].

43) <http://europa.eu.int/comm/enterprise/networks/eic/eic.html>, [dostęp: 12.10.2011].

44) Adres: SOLVIT Team Leader, Internal Market and Services Directorate General, Unit B.3, European Commission, B – 1049 Bruxelles/ Brussel, Belgium. Zgłoszone pytanie i związane z nim dane są przechowywane tak długo, jak jest to niezbędne dla udzielenia odpowiedzi i, w zależności od istoty problemu, dłużej na wypadek gdyby zaistniała potrzeba monitorowania danej kwestii niezależnie od natychmiastowej odpowiedzi.

45) E-mail: [Solvit@ec.europa.eu](mailto:Solvit@ec.europa.eu).

46) Wszystkie dane dotyczące systemu można uzyskać w Komisji - [Solvit@ec.europa.eu](mailto:Solvit@ec.europa.eu). W Polsce Centrum Solvit funkcjonuje w ramach Ministerstwa Gospodarki (a także MPIPS) i dostępny jest pod adresem: [solvit.mg.gov.pl](http://solvit.mg.gov.pl).

nie tylko jego zastosowanie, ale również sam przepis może stanowić problem. Jeżeli rozwiązanie danego problemu wymaga uchylecia określonego przepisu, taka sprawa może trwać wiele miesięcy lub nawet dłużej i może wymagać formalnych działań prawnych. W takim przypadku Solvit niewiele może pomóc, chociaż państwo członkowskie, które zgodziło się zmienić kwestionowany przepis, może również odstąpić od jego stosowania.

Obywatel lub przedsiębiorca zgłaszający swój problem do Solvitu, podaje szczegóły dotyczące danej sprawy, a w szczególności dane kontaktowe osoby lub organizacji zgłaszającej problem, a także dodatkowe dokumenty sprawy, które zostaną włączone do bazy danych. Chodzi tu o dane niezbędne dla podjęcia próby efektywnego rozwiązania problemu. W większości przypadków uzyskanie pozytywnego wyniku bez szczegółowych informacji, włączając w to dane osobowe, będzie niezmiernie trudne, niemniej jednak system Solvit umożliwi przyjmowanie spraw, w których wszystkie dane szczegółowe klienta nie są udostępniane prowadzącemu Centrum SOLVIT, odpowiedzialnemu za rozwiązanie problemu. W takich przypadkach tylko zgłaszające Centrum SOLVIT ma dostęp do danych umożliwiających identyfikację klienta.

Od lipca 2002 r. Solvit oferuje szybkie i praktyczne rozwiązania dla osób prywatnych i przedsiębiorców, którzy podczas pobytu, pracy lub studiów na obszarze UE mieli kłopoty z korzystaniem z praw przysługujących im na mocy przepisów unijnych. Swoją ośrodek Solvitu posiada każde państwo w UE (a także kraje EOG - Norwegia, Islandia i Liechtenstein). Ośrodki te są częścią krajowej służby publicznej, a ich zadaniem jest udzielanie bezpłatnej pomocy wszystkim jednostkom (rezydentom) UE. Solvit uporał się do końca 2007 r., bez wkraczania na drogę sądową, z 1 800 problemami, z których większość rozwiązano w ciągu mniej niż dziesięciu tygodni. Ponad dwie trzecie spośród spraw, które trafiają do Solvitu, dotyczyło przeciętnych obywateli, którzy mają problem z ubezpieczeniem społecznym, dostępem do rynku pracy (w tym zawodów regulowanych), podatkami lub doprowadzeniem do uznania swoich kwalifikacji zawodowych. W pozostałych przypadkach do Solvitu zwracają się przedsiębiorcy, którzy napotykają na trudności: podatkowe, z dostępem swoich produktów lub usług do danego rynku albo z założeniem działalności poza swoim krajem ojczystym<sup>47</sup>. Komisja przygotowuje roczne raporty z funkcjonowania sieci<sup>48</sup>.

---

47) Przykładem rozwiązanej sprawy była kwestia zakupu przez Włocha samochodu z USA za pośrednictwem holenderskiego importera, który zarejestrował samochód w Niemczech. Lokalnemu włoskiemu urzędowi rejestracji pojazdów nie wystarczyły dokumenty, jakie się zazwyczaj przedstawia przy rejestracji samochodu i zażądał dodatkowych zaświadczeń. Kiedy włoski ośrodek Solvitu poprosił o interwencję włoskie ministerstwo transportu, urząd rejestracyjny wydał wreszcie odpowiedni dokument – rozwiązanie sprawy zajęło niecałe trzy tygodnie.

48) Np. *Development and Performance of the Solvit network in 2007*, European Commission, Brussels 2008.

## Połączone sieci ECC-EEJ

Geneza Europejskich Centrów Konsumenckich - European Centres Network (ECC-net) Sieć Europejskich Centrów Konsumenckich (ECK), powszechnie nazywana *Euroguichets*<sup>49</sup>, w państwach należących do UE istnieje od 1992 r. Jednostki te prowadziły kampanię informacyjną, doradczą oraz promocyjną w sferze spraw konsumenckich<sup>50</sup>. ECC-net miał na celu przełamywanie oporów konsumentów wobec aktywnego uczestniczenia w rynku WE. W dobie swobodnego przepływu towarów, osób, usług i finansów wspólny rynek stwarza możliwości, które coraz częściej są wykorzystywane przez obywateli Europy, zwł. w zakresie:

- zakupu towarów i wymiany usług w ramach odbywanych podróży,
- zakupu towarów lub zamawiania usług u przedstawicieli handlowych odbywających podróże biznesowe po krajach UE,
- zamawiania i zakupu towarów w innych krajach europejskich za pomocą nowoczesnych technik sprzedaży na odległość, zwłaszcza drogą elektroniczną,
- obrotu pieniędzmi między krajami w celu zapłaty za towar lub inwestycję.

Ponadto jednolity rynek wymaga usystematyzowania obecnych krajowych porządków prawnych w celu harmonizacji prawa i sprawnej ochrony konsumenta niezależnie od państwa pobytu w ramach UE.

Działania sieci ECK pozwalają na identyfikowanie nowych problemów prawnych, dając zarazem pełniejszy obraz przeszkód już istniejących. Misją sieci Europejskich Centrów Konsumenckich jest dostarczenie konsumentom kompleksowej obsługi - od informacji o ich prawach, po pomoc w uwzględnianiu ich skarg i rozwiązywaniu sporów. Sieć ECK pomaga konsumentom korzystać z możliwości, jakie stwarza jednolity rynek europejski, bez zagrożenia dla ich interesów ekonomicznych i zawodowych. Jej zadania to m.in.:

- informowanie konsumentów o możliwościach Rynku oraz pomoc w rozwiązywaniu problemów/skarg;
- pomoc w korzystaniu z pozasądowych procedur rozstrzygania sporów o zasięgu pan-europejskim;
- pomoc w łatwym i świadomym korzystaniu z tych procedur w kontekście ponadgranicznym;
- współpraca wewnątrz sieci, a także z innymi europejskimi sieciami, takimi jak: FIN-NET (Financial Network), SOLVIT oraz EEJ (European Judicial network in civil and commercial matters);

49) [www.europa.eu.int/comm.consumers/redress/compl/euroguichet/index\\_en.htm](http://www.europa.eu.int/comm.consumers/redress/compl/euroguichet/index_en.htm)

50) Konsumentów w UE reprezentuje; European Consumer Consultative Group (the Consumers' Committee).



- dostarczanie informacji na temat krajowego i unijnego prawodawstwa oraz orzecznictwa;
- dostarczanie analiz porównawczych w zakresie cen, legislacji i innych kwestii istotnych dla konsumentów;
- dostarczanie Komisji Europejskiej informacji na temat problemów konsumenckich w UE.

Sieć ECK działa na terenie Unii Europejskiej, Norwegii i Islandii, łącznie w 27 państwach.<sup>51</sup>

W Polsce ECK zostało powołane do życia w styczniu 2005 r. na mocy porozumienia Komisji Europejskiej z Urzędem Ochrony Konkurencji i Konsumentów (UOKiK). Projekt finansowany był ze środków Unii i UOKiK. ECK w Warszawie jest członkiem unijnej sieci ECK<sup>52</sup>.

### *Europejska Sieć pozasądowa - European Extra Judicial Network (EEJ-net)*<sup>53</sup>

W państwach Unii oraz w Norwegii i Islandii od 2001 r. rozwinęła się sieć EEJ-net, której zadaniem jest pomaganie i doradzanie konsumentom w realizacji ich praw w rozstrzygnięciu sporów o charakterze transgranicznym (*cross-border cases*)<sup>54</sup>. Ośrodki te funkcjonowały jako sieć, co pozwalało na efektywną wymianę informacji i skuteczne działanie. Początkowo był to roczny projekt pilotażowy, który został przedłużony do 2003 r. Sieć współpracuje z *Financial Network* (FIN-Net) i systemem *Solvit*. Działalność EEJ-net polegała na informowaniu konsumentów o istnieniu ADR (*Alternative Dispute Resolution Mechanisms, out-of-court-settlement of consumer disputes*), a także na pomocy przy wypełnianiu formularzy skargi, gromadzeniu wymaganych dokumentów, wskazywaniu ew. właściwości sądów

51) Informacje o innych inicjatywach Komisji na rzecz dostępu konsumentów do wymiaru sprawiedliwości w kontekście transgranicznym: [http://ec.europa.eu/consumers/redress/index\\_en.htm](http://ec.europa.eu/consumers/redress/index_en.htm), jak również można uzyskać od:

- izb rozrachunkowych działających w ramach europejskiej sieci pozasądowej (EEJ-net),
- lokalnego lub krajowego stowarzyszenia lub agencji konsumenckiej,
- Europejskich Centrów Konsumenta (ECK, dawniej Euroguichets),
- Europejskich Centrów Informacyjnych,
- punktów kontaktowych rynku wewnętrznego dla obywateli i przedsiębiorstw.

52) Europejskie Centrum Konsumenckie w Polsce jest grupą ekspercką, w której skład wchodzi: Aleksandra Olczak - Dyrektor Centrum [Aleksandra.Olczak@konsument.gov.pl](mailto:Aleksandra.Olczak@konsument.gov.pl); Elżbieta Seredyńska - Prawnik/Ekspert ds. Informacji i Skarg Konsumentek; [Elzbieta.Seredynska@konsument.gov.pl](mailto:Elzbieta.Seredynska@konsument.gov.pl); Piotr Stańczak - Prawnik/Koordynator Pozasądowych Metod Rozpatrywania Sporów (ADR); [Piotr.Stanczak@konsument.gov.pl](mailto:Piotr.Stanczak@konsument.gov.pl); Maciej Szulski Sekretarz; [sekretariat@konsument.gov.pl](mailto:sekretariat@konsument.gov.pl)

53) [www.eejnet.org](http://www.eejnet.org), [dostęp: 12.10.2011].

54) Podstawa prawna: Council Resolution of 25.05.2000 on a Community-wide network of national bodies for the extra-judicial settlement of consumer disputes [OJ C 155 of 06.06.2000].

oraz znalezieniu podstawy prawnej, następnie monitorowaniu przebiegu sporu. Były to tzw. *Clearing House*, czyli centra informacji i dokumentacji.

Na początku 2005 r. nastąpiło połączenie obu wyżej opisanych sieci, tj. ECC-net z EEJ-net<sup>55</sup>. Zadania i projekty prowadzone w ramach poszczególnych sieci zostały skoordynowane i powierzone zjednoczonej sieci Europejskich Centrów Konsumenckich. Udostępniają one informacje oraz zapewniają wsparcie w sprawach ponadgranicznych, w tym z Europejskiej Sieci Pozasądowej (EEJ-Net), która pomagała konsumentom rozwiązywać sprawy sporne poprzez pozasądowe rozstrzygnięcie sporów z wykorzystaniem mediacji i arbitrażu. Aktualnie, ośrodki EEC-Net współdziałają często z Biurami Porad Obywatelskich (Citizens Advice Bureaux), nawet w ramach jednego centrum.

Alternatywne rozstrzygnięcie sporów (Alternative dispute resolution -ADR) a sieci ODR

Alternatywne rozstrzygnięcie sporów (ADR) obejmuje procedury i techniki pozasądowe, głównie negocjacje, concyliację, mediację (w tym *kolaboratywną*<sup>56</sup>) oraz arbitraż. ADR zyskały w ostatnich kilkunastu latach powszechną akceptację zarówno jednostek walczących o ochronę praw, jak i prawników. Często jest także uciekanie się do ADR przed wstąpieniem na drogę sądową. Są to procedury mniej kosztowne, szybsze i bardziej efektywne, a zarazem umożliwiające stronom na kontrolę rozwoju sporu. W tej sferze można wyróżnić techniki i procedury o następującym charakterze:

1. W negocjacjach adwersarze uczestniczą dobrowolnie, układają się bezpośrednio. Jednakże nie wyklucza to pomocy ze strony rzecznika (*ombudsperson*), ‘przyjaciela sprawiedliwości’, ‘Helping People Themselves’<sup>57</sup> lub osoby pouczającej strony co do zasad postępowania;

2. W mediacji występuje strona trzecia – mediator, ułatwiający rozwiązanie sprawy i mogący występować z „propozycjami pośrednika”, lecz nienarzucający rozstrzygnięcia sprawy. W niektórych krajach (np. w Wielkiej Brytanii) synonimem ADR jest mediacja;

3. W mediacji kolaboratywnej (*collaborative law*) każda ze stron ma adwokata lub radcę. Strony ustalają porozumienie z pomocą *attorneys* oraz wspólnie zaakceptowanych ekspertów, którzy jednak nie narzucają rozwiązania. Ta procedura jest bardzo popularna w systemie anglosaskim, w biznesie i sprawach rodzinnych;

55) Podstawa prawna: General framework of Community action [COM(2003) 44 – niepublikowana.

56) Popularne w USA i Kanadzie techniki *Collaborative Law* są tak definiowane: “The Collaborative Law Process is problem solving with collaborative lawyers where parties try to understand each other. The parties are responsible for information gathering and solutions”. Obejmuje ona dwa główne działy: rodzinny i zawodowy.

57) Zob.: *Helping People Help Themselves*, in: “Negotiation Journal” July 1990, s. 239-248.

4. W arbitrażu, udział w którym jest dobrowolny, występuje strona trzecia (arbiter, prywatny sędzia lub komisja), która narzuca rozstrzygnięcie według określonych zasad (np. „Scott Avery Clause”). Udział w arbitrażu może wynikać też z uprzedniego porozumienia, popularnego zwłaszcza w sprawach konsumenckich. Zwykle, choć nie zawsze, strony mogą odwołać się od takiego orzeczenia do sądu;

5. Inne techniki i procedury ADR (ze względu na brak tradycji polskiej, pozostawiamy nazwy angielskie): a) *Case evaluation* jest to procedura kiedy strony przedstawiają sprawę osobie oceniającej (ewaluatorowi), która wskazuje stronom na silne i słabe strony ich stanowiska oraz wskazuje, jak spór można bezstronnie rozstrzygnąć, b) *Early neutral evaluation* jest to procedura oceniająca po wniesieniu sprawy do sądu – ekspert oceniający przedstawia ewaluację sprawy i możliwość lub sugestię rozstrzygnięcia, c) *Family group conference* jest formą prezentowania propozycji członków rodziny związanych z daną sprawą (dot. zwł. przypadków złego traktowania), służącą ustaleniu planu rozwiązania problemu, d) *Neutral fact-finding* to procedura z udziałem strony trzeciej, wybranej przez strony i sąd, celem ustalenia faktów lub wyjaśnienia kwestii fachowych, e) *Ombuds* to osoby, które uzyskały taki tytuł (status), pracując zwykle w ramach firmy lub instytucji publicznej (uniwersytet, szpital, organ administracji), a rozstrzygają skargi w sposób niezależny (pracowników i klientów)<sup>58</sup>.

Alternatywne sposoby rozwiązywania sporów są też często nazywane *odpowiednimi* (*appropriate*), a oznacza to zawsze rozstrzygnięcie sporów bez udziału sądu<sup>59</sup>. W ramach Unii są one regulowane Rozporządzeniem WE nr 874/2004. Tradycyjnie formy ADR wymagały zawsze kontaktów osobistych lub pocztowych. Coraz częstsze jest jednak korzystanie z tych metod *on-line*, co nosi nazwę ODR (*online dispute resolution*)<sup>60</sup>. ODR jest najczęściej prowadzone przez organy rządowe. Jednak może obejmować kwestie międzynarodowe lub globalne, jak w przypadku zasad i reguł postępowania UDRP (od *Uniform Domain-Name Dispute-Resolution Policy*, w Internecie skróty z nazwą dziedziny, której dotyczy spór)<sup>61</sup>. ODR jest popularny

58) Szerzej: <http://www.abanet.org/dispute/draftbrochure.pdf>, [dostęp: 23.10.2011].

59) Techniki ADR zob. *Open courseware*: [http://ocw.mit.edu/NR/rdonlyres/Sloan-School-of-Management/15-667Spring2001/4D52CAC7-78CE-453D-9918-6E6EE2146864/0/lec11\\_notes\\_on\\_options.pdf](http://ocw.mit.edu/NR/rdonlyres/Sloan-School-of-Management/15-667Spring2001/4D52CAC7-78CE-453D-9918-6E6EE2146864/0/lec11_notes_on_options.pdf), [dostęp: 23.10.2011].

60) Nazywane często *cyber mediator website* zwł. w sferze e-commerce. Zob. *Online dispute resolution – what means a consumer*, by Lee a. Begrave, [www.folk.uoi.no](http://www.folk.uoi.no).

61) UDRP jest podany regułom i zasadom ICANN. Wg strony [www.udrp.org](http://www.udrp.org): “Uniform Domain Name Dispute Resolution Policy) was adopted in late 1999 by ICANN (the private authority responsible for the administration of certain Internet technical parameters) to offer an alternative to litigation in local courts to settle complaints by trademark owners about cybersquatting. The UDRP created its own definition of “bad faith registration and use” of domain names, and identified some situations that would be considered defenses to a trademark complaint (rights and legitimate interests). UDRP proceedings are binding on all domain name holders in .com, .org, .net, .info and .biz as

w USA i wielu innych krajach, w systemie ONZ oraz w Unii, gdzie utworzono kilka sieci, w tym jedną z udziałem państw członkowskich<sup>62</sup>.

## System FIN-Net

Ramy systemu i sieci FIN-NET mają umożliwić konsumentom kontakt z pozasądowym organem rozjemczym w jego kraju rodzimym, nawet jeśli skarga konsumenta dotyczy zagranicznej firmy finansowej. Najbliższe centrum FIN-Net pomoże konsumentowi w znalezieniu odpowiedniej instytucji rozjemczej i zapewni mu niezbędne informacje o systemie i stosowanej w nim procedury rozjemczej. Struktura, charakter oraz kompetencja powyższych rozwiązań różnią się w poszczególnych krajach. Nawet rozwiązania funkcjonujące w jednym państwie mogą mieć inne formy w różnych branżach. Konsument powinien znać cechy danego mechanizmu, zanim podejmie decyzję o złożeniu skargi za jego pośrednictwem. Cechy te obejmują ważne zagadnienia, takie jak: terminy składania skarg, charakter decyzji podejmowanych przez instytucję (wiążące/niewiążące), ograniczenia dotyczące zasądzanych odszkodowań itd. Konsument powinien również wiedzieć, w jaki sposób ma przesłać skargę (tzn. listem, faksem czy pocztą elektroniczną) oraz których języków może używać. Procedury rozjemcze mają zwykle różną formę w poszczególnych krajach. Najbardziej typowym modelem dla sektora usług finansowych jest tzw. instytucja rzecznika praw obywatelskich. Istnieją również inne modele, np. rozjemcze rady konsumenckie (zajmujące się wyłącznie usługami finansowymi lub bardziej ogólnymi sprawami), konsumenckie rady arbitrażowe oraz systemy rozjemcze prowadzone przez organy nadzoru<sup>63</sup>. Członkowie centrum FIN-Net w kraju rodzimym udzielają informacji o zagranicznych instytucjach rozjemczych w języku narodowym.

Po zebraniu wszelkich niezbędnych informacji o wybranej instytucji rozjemczej oraz po podjęciu decyzji o skierowaniu do niej sprawy, skargę można złożyć u członka FIN-Net w swoim rodzimym kraju. Jeśli członek centrum FIN-NET z tego kraju nie może się zająć sprawą, przekazuje ją do odpowiedniej instytucji w kraju usługodawcy. W niektórych przypadkach znacznie skuteczniejszy jest bezpośredni kontakt z daną instytucją

well as [ccTLDs] and can result in the cancellation or transfer of the domain registration to the trademark owner. UDRP cases are decided by individual Panelists who serve one of four resolution service Providers.”

62) Linki unijne: <http://www.eurofound.europa.eu/eiro/thematicfeature15.htm>, [dostęp: 12.10.2011]. Szerzej teoria: L. Edwards, C. Wilson, (2007) *Redress and alternative dispute resolution in EU cross-border e-commerce transactions*. “International Review of Law, Computers & Technology”, 21, (3), s. 315-333. Por też strony EIRO.

63) Dane w sprawie FIN-NET można uzyskać na stronie: [http://ec.europa.eu/internal\\_market/finservices-retail/finnet/index\\_en.htm](http://ec.europa.eu/internal_market/finservices-retail/finnet/index_en.htm), [dostęp: 23.10.2011]. Strona zawiera szczegółowe informacje o poszczególnych instytucjach.

– w takiej sytuacji członek centrum FIN-NET poinformuje o tym konsumenta. Jeśli chodzi o język skargi, instytucje FIN-NET dążą do zapewnienia, aby skargi można było składać przynajmniej w języku, w którym zawarta została umowa finansowa lub w języku, w którym konsument na ogół kontaktuje się ze swoją instytucją finansową. W wielu instytucjach dostępne są również inne języki. Instytucje członkowskie FIN-NET zajmują się skargami transgranicznymi z taką samą skutecznością i starannością jak w przypadku skarg krajowych. Jeżeli instytucja potrzebuje dodatkowych informacji lub dokumentacji od konsumenta, skontaktuje się z nim bezpośrednio. Jeżeli konieczne są bardziej ogólne informacje, tzn. o ramach legislacyjnych zapewniających ochronę konsumentów w danym kraju, instytucja współpracuje bezpośrednio z członkiem FIN-NET w tym kraju. Konsument korzysta ze współpracy również w razie wysłania skargi bezpośrednio do adekwatnej instytucji.

Należy zwrócić uwagę, że procedury FIN-NET są jedynie alternatywami dla odszkodowań zasądzanych w sądach i że decyzje lub zalecenia organów pozasądowych nie są egzekwowane w taki sam sposób jak orzeczenia sądowe. W większości przypadków instytucje finansowe stosują się do zaleceń organu rozjemczego, nawet jeśli nie są one wiążące. Jeśli instytucje finansowe nie zastosują się do zaleceń, konsument może wejść na drogę sądową. Można poprosić członków FIN-NET o udzielenie szczegółowych informacji co do zastosowanych przy rozstrzygnięciu sporu decyzji.

Jednym z podstawowych celów sieci FIN-NET jest poprawa jakości rozstrzygania sporów w pozasądowych instytucjach rozjemczych na całym Europejskim Obszarze Gospodarczym. Członkowie FIN-NET są związani protokołem ustaleń, który oprócz proceduralnych ram współpracy transgranicznej określa podstawowe zasady pozasądowego rozwiązywania sporów. Protokół ustaleń obejmuje również deklarację intencji organów w sprawie stosowania norm jakościowych określonych w zaleceniu Komisji 98/257/WE (z 1998 r.) w sprawie zasad odnoszących się do organów odpowiedzialnych za pozasądowe rozwiązywanie sporów konsumenckich.

Rządy państw UE zostały poproszone o zgłaszanie Komisji Europejskiej funkcjonujących na ich terenie pozasądowych organów rozjemczych, które spełniają odnośne zalecenia KE. Sieć FIN-Net obejmuje wyłącznie instytucje zostały zgłoszone przez konkretne państwa UE.

## 7. Efektywność i kontakty; uwagi końcowe

Uwzględniając powyższe, można stwierdzić, że dynamicznie rozwijające się w ostatnich latach sieci net tworzone celem ochrony praw konsumenckich gł. ekonomicznych oraz dla alternatywnego rozwiązywania sporów służą umocnieniu i rozszerzeniu klasycznych pozasądowej ochrony praw podmiotowych. Chodzi tu o ochronę wszystkich praw podmiotowych związanych z rynkiem (wspólnym i wewnętrznym) WE; zarówno praw ekonomicznych, praw konsumenta, jak i ochronę konkurencji, a tym samym o poprawę jednolitości i efektywności norm *acquis communautaire*. Powyższe mechanizmy są łatwiej dostępne, tańsze (w zasadzie bezpłatne) i szybsze od instytucjonalnych (w tym sądowych) metod dochodzenia roszczeń. Transgraniczny charakter funkcjonowania tych sieci przyczynia się zarazem do rozwoju *rządów prawa* oraz integracji europejskiej<sup>64</sup>. Warto podkreślić, że w przeciwieństwie do ochrony sądowej (wniesienie roszczenia zwykle kosztuje, a jego rozstrzygnięcie trwa średnio 2-3 lata) skorzystanie z formy rozstrzygania sporów proponowanej przez wymienione sieci jest bezpłatne i prowadzi do rezultatów zwykle w ciągu 2-3 tygodni. Taki termin jest też przewidziany dla odpowiedzi instytucji i urzędów UE i WE na skargi obywateli i mieszkańców obszaru UE. Tę formę ochrony praw jednostek należy uznać za najprostszą, najłatwiej dostępną i najbardziej efektywną. W powyższym omówieniu celowo pominięto wykorzystanie sieci w następujących sferach: system informacji publicznej Unii (BIP), Obywatelstwo Unii, petycje i skargi, formularze kontaktowe ze strukturami UE, fundusze strukturalne i SIMIC, przepływy finansowe w UE, systemy Frontex oraz współpracy policyjnej i sądowej, a także innych sieci specjalnych i baz danych, a ponadto – elektronicznego przekazywania i potwierdzania dokumentów. Ich omówienie wymagałoby bowiem opracowania monograficznego.

64) Dostęp do sieci internetowej oraz dodatkowe informacje można uzyskać pod adresami: [http://europa.eu.int/comm/internal\\_market/en/update/citizen](http://europa.eu.int/comm/internal_market/en/update/citizen), [dostęp 23.10.2011].  
<http://europa.eu.int/comm/enterprise/networks/eic/eic.html>, [dostęp 23.10.2011].  
[http://europa.eu.int/comm/consumers/policy/euroguichets/index\\_en.html](http://europa.eu.int/comm/consumers/policy/euroguichets/index_en.html), [dostęp 23.10.2011].  
[http://europa.eu.int/europedirect/it/about\\_it.html](http://europa.eu.int/europedirect/it/about_it.html), [dostęp 23.10.2011].  
[http://europa.eu.int/europedirect/it/index\\_it.html](http://europa.eu.int/europedirect/it/index_it.html), [dostęp 23.10.2011].  
[http://europa.eu.int/comm/internal\\_market/en/finances/consumer/adr.htm](http://europa.eu.int/comm/internal_market/en/finances/consumer/adr.htm), [dostęp 23.10.2011].  
[http://europa.eu.int/comm/consumers/policy/developments/acce\\_just/acce\\_just06\\_it.pdf](http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just06_it.pdf), [dostęp 23.10.2011].  
<http://econfidence.jrc.it>; [http://ec.europa.eu/internal\\_market/finances-retail/finnet/index\\_en.htm](http://ec.europa.eu/internal_market/finances-retail/finnet/index_en.htm), [dostęp 23.10.2011].

## Zakończenie

Wychodząc ze wspomnianych wyżej unormowań UE, należy stwierdzić, że zarówno w aspekcie faktycznym, jak i prawnym cyberprzestrzeń staje się podsystemem prawno-organizacyjnym UE *in statu nascendi*. Wiele jego standardów i instrumentów służy ochronie praw jednostek. Są także elementy podsystemu służące ochronie instytucji i struktur UE/WE oraz interesów ekonomicznych Unii. Sieci net, w tym Internet rozwijają się niezwykle dynamicznie, a regulacje prawne nie nadążają za tym procesem. W związku z masowym dostępem do sieci oraz uznawaniem ich za obszar nieskrępowanej wolności rozpowszechnienie ilościowe i rodzajowe popełnianych tam deliktów jest duże i mające znaczą dynamikę (nie wspominając już o celowo organizowanym procederze przestępczym<sup>65</sup>). Natomiast stosowane zabezpieczenia są szybko dezaktualizowane przez rozwój techniki i hackerów. Istnieją znaczne trudności ze ściganiem sprawców powyższych deliktów. Natomiast w sferze praw człowieka administratorzy sieci są mało wrażliwi na ochronę praw osobistych. Ich odpowiedzialność w interesie całej społeczności (w tym organów wymiaru sprawiedliwości) musi ulec zwiększeniu. Należy wprowadzić efektywne normy ograniczające nadużywanie wolności przez internautów, ze szkodą dla praw osobistych. Omawiany podsystem powinien być włączony do systemu ochrony prawnej UE. Jednakże spore trudności z przyjmowaniem odnośnych aktów prawnych<sup>66</sup> nie mogą nas nastrajać zbyt optymistycznie.

W powyższym omówieniu celowo pominięto wykorzystanie sieci w następujących sferach: system informacji publicznej Unii (BIP), Obywatelstwo Unii, petycje i skargi, formularze kontaktowe ze strukturami UE, fundusze strukturalne i SIMIC, przepływy finansowe w UE, systemy Frontex oraz współpracy policyjnej i sądowej, a także innych sieci specjalnych i baz danych, a ponadto – elektronicznego przekazywania i potwierdzania dokumentów. Ich omówienie wymagałoby bowiem opracowania monograficznego.

---

65) Por. J.W. Wójcik, *dz.cyt.* oraz W. Fijałkowski, *dz.cyt.*

66) Zob. np.: cytowane wcześniej problemy z regulacją algorytmów, kłopoty z wyegzekwowaniem kar wobec Microsoftu oraz Opinia PE 2007/2088(INI), AD/689981PL.

## Bibliografia

### Druki zwarte:

- Adamski A., *Przestępczość w cyberprzestrzeni*, TNOiK, Toruń 2001.
- Bodio J., Borkowski G., Demendecki T., *Ustrój organów ochrony prawnej, część szczegółowa*, Wyd. Zakamycze, Kraków 2005.
- Brodecki Z. (red.), *Konkurencja*, Wyd. LexisNexis, Warszawa 2004.
- Czapliński W., Wyrozumska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Wyd. C. H. Beck, Warszawa 2004.
- Kondrat M., *Znaki towarowe w Internecie*, Dom Wyd. ABC, Warszawa 2001.
- Łazowski A., *Ochrona praw jednostek w prawie Wspólnot Europejskich. Pozasądowe mechanizmy ochrony praw przed instytucjami i organami WE*, Wyd. Zakamycze, Kraków 2002.
- Łętowska E. (red.), *Nieuczciwe klauzule w prawie umów konsumenckich*, Wyd. C. H. Beck, Warszawa 2004.
- Mik C., *Wymiar sprawiedliwości w Unii Europejskiej*, TNOiK, Toruń 2001.
- Wawrzyk P., *Polityka Unii Europejskiej w obszarze spraw wewnętrznych i wymiaru sprawiedliwości*, WAIp Warszawa 2007.
- Wójcik J.W., *Oszustwa finansowe. Zagadnienia kryminologiczne*, Warszawa 2008.
- Malinowska I., *System organów ochrony prawnej w państwach Unii Europejskiej* [w:] Wojtaszczyka K. A. (red.), *Polska - Unia Europejska*, Warszawa 2003.

### Czasopisma:

- Fijałkowski W., *Internet – przestępcza gałąź gospodarki*, Prokurator 1/2007.
- Edwards L., Wilson C., (2007) *Redress and alternative dispute resolution in EU cross-border e-commerce transactions*. "International Review of Law, Computers & Technology", 21, (3).
- Helping People Help Themselves*, in: "Negotiation Journal" July 1990.
- Kowalczyk-Bańczyk K., *Ochrona przed spamem w przepisach wspólnoty Europejskiej*, „Prawo i Malinowska I., *Zróźnicowanie modeli ochrony prawnej w państwach Unii Europejskiej*, „Przegląd Europejski” 2(5)2002.
- Podatki w Unii Europejskiej*” nr 1/2006.
- Niklewicz K., *Patenty wracają*, „Gazeta Wyborcza”, 21.01.2005.
- Rożyński P., *Domemę sprzedam*, „Gazeta Wyborcza”, 7.05.2005.



## **Netografia:**

[http://europa.eu.int/comm/internal\\_market/en/update/citizen](http://europa.eu.int/comm/internal_market/en/update/citizen); <http://europa.eu.int/comm/enterprise/networks/eic/eic.html>

[http://europa.eu.int/comm/consumers/policy/euroguichets/index\\_en.html](http://europa.eu.int/comm/consumers/policy/euroguichets/index_en.html)

[http://europa.eu.int/europedirect/it/about\\_it.html](http://europa.eu.int/europedirect/it/about_it.html)

[http://europa.eu.int/europedirect/it/index\\_it.html](http://europa.eu.int/europedirect/it/index_it.html)

[http://europa.eu.int/comm/internal\\_market/en/finances/consumer/adr.htm](http://europa.eu.int/comm/internal_market/en/finances/consumer/adr.htm)

[http://europa.eu.int/comm/consumers/policy/developments/acce\\_just/acce\\_just06\\_it.pdf](http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just06_it.pdf)

<http://econfidence.jrc.it>

[http://ec.europa.eu/internal\\_market/finservices-retail/finnet/index\\_en.htm](http://ec.europa.eu/internal_market/finservices-retail/finnet/index_en.htm)

[http://ec.europa.eu/internal\\_market/finservices-retail/finnet/index\\_en.htm](http://ec.europa.eu/internal_market/finservices-retail/finnet/index_en.htm)

<http://www.abanet.org/dispute/draftbrochure.pdf>

[http://ocw.mit.edu/NR/rdonlyres/Sloan-School-of-Management/15-667Spring2001/4D52CAC7-78CE-453D-9918-6E6EE2146864/0/lec11\\_notes\\_on\\_options.pdf](http://ocw.mit.edu/NR/rdonlyres/Sloan-School-of-Management/15-667Spring2001/4D52CAC7-78CE-453D-9918-6E6EE2146864/0/lec11_notes_on_options.pdf)

<http://www.eurofound.europa.eu/eiro/thematicfeature15.htm>

[www.eejnet.org](http://www.eejnet.org)

[http://europa.eu.int/comm/internal\\_market/en/update/citizen/](http://europa.eu.int/comm/internal_market/en/update/citizen/)  
oraz <http://citizens.eu.int/>

<http://europa.eu.int/comm/enterprise/networks/eic/eic.html>

[http://europa.eu.int/comm/internal\\_market/en/finances/consumer/adr.htm](http://europa.eu.int/comm/internal_market/en/finances/consumer/adr.htm)  
oraz [http://www.cc.cec/di/e-commission/docs/sec\\_2001\\_0924\\_en.pdf](http://www.cc.cec/di/e-commission/docs/sec_2001_0924_en.pdf),