현안분석 2001-5

디지털경제법제②

# 미국의 인터넷 법제에 대한 고찰

李 大 熙

한국법제연구원

# 미국의 인터넷 법제에 대한 고찰

A Study on the Internet-related Legislations in the US

研究者 : 李大熙(배재대학교 법학부 교수)
Dae-Hee Lee

2001.10

한국법제연구원

# 목 차

# 제 1 장 서 론

전세계적인 인터넷 검색프로그램이 광범위하게 사용되기 전에는 인터넷으로 인한 법률상의 쟁점은 중요한 것이 아니었다. 또한 인터넷상으로 상거래가 많이 행해지지 않았던 경우에는 TV나 출판물 등 주류의 매체에 비하여 손해의 가능성은 크지 않았다. 그러나 인터넷상으로 영업활동이나 광고를 하거나 기타의 행위가 증가하게 되자 사정은 크게 변하였다. 인터넷의 급속한 발전·확대는 생활의 일부분을 차지할 뿐만 아니라 전자상거래(electronic commerce), 정보거래(trade in information), 프라이버시(privacy), 명예훼손(defamation), 표현의 자유(freedom of speech), 음란성(obscenity), 실시허락(licensing), 온라인상의 광고, 온라인에 의한 도박, 과세, 관할권(jurisdiction), 온라인상의 범죄행위, 스팸메일, 컨텐츠 규제 등 여러 분야의 법적인 문제점을 야기하고 있다. 또한 지적재산권 분야와 관련하여 상표, 저작권, 특허, 영업비밀, 데이터베이스(data base), 퍼블리시티권(right of publicity), 그리고 트레이드 드레스(trade dress) 등 기존의 지적재산권을 디지털환경에 적용되는 것과 관련하여 많은 문제점이 발생하고 있다.

이 글은 인터넷과 관련된 미국에서의 입법을 전반적으로 고찰하고자 한다. 그렇다면 과연 고찰의 범위를 어떻게 설정할 것인가가 문제된다. 이에 대해서는 클린턴 행정부의 "A Framework for Global Electronic Commerce"[1]가 제시하고 있는 내용이 도움이 될 것으로 보인다. 이 보고서는 인터넷과 관련된 입법에 관한 전반적인 구조를 밝히고 있는데, 정부의 간섭을 최소화하고 민간에 의한 주도를 강조하고 있으며, 인터넷과 관련된 입법에 관한 쟁점을 크게 금융에 관한 쟁점, 법적인 쟁점, 시장접근에 대한 쟁점으로 구분하고 있다. 금융에 관한 쟁점으로는 관세 및 조세와 전자지불방법, 법적인 쟁점으로서는 전세계적인 전자상거래를 위한 규범(청약, 승낙, 사기방지법, 관할권, 법의 선택), 지적재산권의 보호, 프

1) William J. Clinton & Albert Gore, Jr., A Framework for Global Electronic Commerce(1997).

라이버시, 보안·암호이며, 시장접근에 관한 쟁점은 콘텐츠(contents)의 규제, 통신의 하부구조 및 정보기술, 기술적인 표준 등이다. 인터넷과 관련된 개별적인 입법활동분야는 조세, 저작권, 디지털 서명을 비롯한 전자상거래, 프라이버시, 스팸 메일, 포르노, 도박 등을 들 수 있다. 따라서 이 글은 인터넷과 관련된 미국의 법제를 크게 전자상거래, 지적재산권, 기타의 법제로 나누어서 고찰하고자 한다. 사실상 인터넷 법제와 관련하여 가장 많은 부분을 차지하고 있으며 가장 많은 쟁점이 발생하고 있는 분야가 지적재산권 및 전자상거래 분야일 것이다. 기타의 법제에 관한 부분에서는 컨텐츠 규제, 조세, 스팸 메일, 인터넷 도박, 암호 등을 중심으로 하여 미국의 인터넷 법제를 고찰하고자 한다. 다만 인터넷에 관한 미국의 법은 여전히 형성되고 있는 단계에 있으므로, 이 글은 비록 법으로 성립하지 못하였으나 과거에 법안이 되었었던 것과 2001년도 회기에 제출되어 있는 법안을 간단하게 고찰하고자 한다. 또한 인터넷관련 법제로서는 주에 의한 법제를 들 수 있는데 이러한 법제는 통일적이지 않으며 연방법보다 그 영향이 상대적으로 미약하므로, 이 글은 관련되는 한도에서 제한적으로만 주법을 고찰하고자 한다.

# 제 2 장 전자상거래

## 제 1 절 통일컴퓨터정보거래법(UCITA)

### 1. 정보거래의 규율필요성

정보산업과 정보에 기초한 상거래는 국가경제에서 중요한 지위를 차지해 가고 있다. 그런데 이러한 산업의 거래대상과 계약구조는 전통적인 상품의 거래의 그것과는 완전히 다르다. 곧 정보거래(information transactions)는 디지털 정보에 대한 '실시허락(licensing)'을 포함하는 거래이며, 배포에 관한 배타적인 권리를 포함하고 있는 지적재산권이 관여하며, 디지털 기술이 일정한 역할을 한다. 정보거래의 주된 특징은 거래에 의하여 이전되고 획득되는 가치가 CD나 폴로피 디스켓과 같은 유형의 재산이 아니라 유형의 매개체로부터 분리될 수 있는 정보나 권리라는 것과 정보에 대한 거래가 조건적이라는 것을 특징으로 한다. 곧 정보를 담고 있는 유형의 매개체가 아니라 그 속에 담겨져 있는 무체물인 정보가 거래의 주된 목적이며, 이러한 정보는 일반적인 지적재산과 마찬가지로 복제가 무제한적으로 가능하다. 또한 이러한 정보를 거래하는 계약이 가지는 문제점은 그 기본적인 계약유형이 매매(sale)나 리스(lease)가 아닌 실시허락이라는 데 있다. 실시허락은 한 당사자(실시허락자)가 계약에 의하여 자신의 재산이나 자신이 통제하고 있는 정보를 다른 당사자(실시권자)가 사용할 수 있도록 허락하는 것이다. 곧 실시허락은, 정보를 포함시키고 있는 유형의 매개체에 대한 소유권을 이전시키는 것과 관계없이, 정보에 대한 권리를 이전시키기 위한 것으로서 그 정보의 이용에 대하여 조건이나 제한을 과하는 계약이다. 따라서 실시허락에는 물품의 매매나 리스에 바탕을 둔 기존의 법체제가 적용될 수 없고 새로운 법체제를 필요로 하고 있다. 따라서 디지털정보거래는 정보 자체의 판매가 아니라 정보의 사용허락에 초점이 맞추어져 있고, 정보를 담고 있는 유형의 매개체 자체의 이전은 거래의 부수적인 것에 불과하다. 그러므로 디지털정보의 거래에 대한 규율은 이같은 거래의 특성을 반영하는 것이어야 하

고, 디지털정보거래의 기초가 되는 계약의 성립, 계약상의 권리와 의무, 보증, 이행 및 구제수단 등을 그 내용으로 해야 할 것이다.

컴퓨터정보거래에 관한 통일법(Uniform Computer Information Transactions Act, 이하 UCITA)의 제정이 추진될 당시 미국은 통일상법전(UCC)에 의하여 매매(Art.2) 및 리스(Art.2A)에 관한 입법만을 가지고 있었다. 따라서 컴퓨터정보 또는 디지털정보의 거래를 규율하기 위한 입법은 필연적인 것이었다.

## 2. 성립과정

컴퓨터정보를 거래하기 위한 입법은 미국 통일상법전 Art.2B로 추진되었다. 정보거래의 진정한 목적은 디스켓이나 CD와 같은 유형의 매개체가 아니라 이에 포함되어 있는 무체물인 정보임에도 불구하고, 미국 법원들은 동산매매(sale of goods)에 관한 UCC Art.2를 종종 적용해 왔다. 따라서 컴퓨터 소프트웨어에 대한 분쟁을 해결할 필요성이 있어 NCCUSL에 의하여 Art.2B에 대한 프로젝트가 시작되었다. Art.2B는 디지털정보거래를 세계 최초로 규율하고자 한 입법으로서, 1991년 매사추세츠 변호사협회의 위원회의 제안에 의하여 시작되었으며 1992년 NCCUSL(National Conference of Commissioners on Uniform State Law)은 이를 위하여 기초위원회를 구성하였다. 정보거래를 규율하기 위하여 통일적인 법체제를 구축하려는 Art.2B도 다른 분야의 상사법의 法令化와 마찬가지로 컴퓨터정보거래에 관한 상업적인 관행을 반영하고 이 분야의 판례법을 법령화하고자 하는 것이었다.

Art.2B는 1994년 초안이 기초된 후 1995년 '무체물의 실시허락'에 대하여 Art.2B 기초위원회가 새로이 선임되었으며, 1996년 2월 첫 초안을 발간한 이래 10여 차례 이상의 초안이 기초되었다. 또한 Art.2B의 제정도 NCCUSL뿐만 아니라 미국법률가협회(American Law Institute, ALI) 양자에 의하여 추진되었다. 그러나 초안을 발간하는 과정에서 시간이 지남에 따라 무체적인 정보에 대한 거래는 유체물품에 대한 거래와 상당히 다르고 물품에 대한 거래를 강조하고 있는 Art.2와 Art.2A(리

스, lease)에 포함시키기에 적절하지 않다는 것이 명백해지게 되었다. 따라서 컴퓨터정보거래를 법령화하는 프로젝트를 UCC로부터 분리하여 통일법으로 입법하는 것이 고려되었고, 마침내 1999년 4월 8일 ALI와 NCCUSL은 이를 UCC로부터 분리하기로 결정하였다. 그리고 NCCUSL은 더 이상 ALI와 협력을 하지 않고 독자적으로 이를 추진하기로 하였다. 그리고 컴퓨터정보거래를 규율하는 법을 Uniform Computer Information Transactions Act(UCITA)로 명명하였으며, 1999년 7월의 NCCUSL의 연례회의에서 이를 채택되었다.

### 3. UCITA의 구성

UCITA는 제1장의 총론을 비롯한 9개의 장(Part)으로 구성되어 있다. 제1장 총론(Sec.101~114)은 UCITA의 적용범위, 합의에 의하여 당사자를 구속할 수 있는 것에 대한 제한, 표준계약 및 shrink wrap license 사용의 제한, 전자상거래의 인정, 법과 법정지의 선택 등 총칙적인 규정을 두고 있다.

제2장(Sec.201~210)은 계약의 성립과 계약의 조건에 관한 것으로서, 전자적인 환경에서의 계약체결 및 계약조건의 결정 등에 관하여 규정하고 있다. 제3장(Sec.301~309)은 계약의 해석에 관한 것으로서, 계약문언의 중시에 관한 규칙(parole evidence rule), 계약조건의 수정, 당사자의 의사가 명확하지 않은 경우의 해석 등에 관하여 규정하고 있다. 제4장(Sec.401~409)은 보증에 관한 규정으로서 컴퓨터정보거래에 적합한 것으로서 일반적으로 인정된 보증에 관하여 규정하고 있다. 제5장(Sec.501~511)은 계약상의 권리와 의무의 이전에 관한 규정으로서, 소유권 및 실시계약하에서의 권리 및 의무의 이전에 관하여 규정하고 있다. 제6장(Sec.601~618)은 이행에 관한 규정으로서, 이행에 관한 전통적인 규칙을 컴퓨터정보거래의 측면에서 적합하게 규정하고 있다. 제7장(Sec.701~710)은 계약의 위반에 관한 규정으로서, 컴퓨터정보가 유형의 매개체에 고정된 경우의 계약위반에 관하여 UCC 제2장의 규칙을 옮겨다 놓았으며, 포기나 예견된 계약위반 등에 관한 판례법 및 UCC

제2장의 규칙을 규정하고 있다. 제8장(801~816)은 구제수단에 관한 것으로서, UCC 제2장에 기초하고 있으나 컴퓨터정보거래에서 적절하도록 UCC 제2장의 규칙을 다소 변경시켜 놓고 있다. 제9장(901~904)은 기타의 규정이다.

### 4. UCITA의 적용범위

UCITA가 대상으로 하는 것은 디지털정보를 비롯한 기타의 정보이다. UCITA의 전신인 Art.2B는 컴퓨터 소프트웨어나 멀티미디어 등의 창조와 배포, 컴퓨터 데이터, 인터넷, 그리고 온라인상으로 정보를 배포하는 거래 등에 초점을 맞추는 것이다. 따라서 인쇄, 영화, 방송, 음향저작물(sound recording, 실연자의 저작물) 등과 같이 정보산업에 대한 거래에는 적용되지 않는다. 1998년 8월 1일의 Art.2B의 초안은 (1) 실시계약과 소프트웨어 계약, 그리고 (2) 소프트웨어 계약에 관계되는 소프트웨어를 지원·유지·수정하기 위한 합의에 적용된다고 규정하였다[103(a)]. 그러나 1999년 2월 1일의 초안[이하 Art 2B 초안]과 UCITA 최종초안은 "컴퓨터정보 거래(computer information transactions)"에 적용된다고 규정하였다.[2B-103(a), UCITA 103(a)].

#### (1) 컴퓨터정보거래

Art.2B의 초안은 컴퓨터정보를 소프트웨어를 포함하는 전자정보(electronic information)로서, 컴퓨터에 의하여 직접 처리·이용될 수 있거나 획득될 수 있는 형태의 전자정보를 의미한다고 규정하였었다[102-1(8)]. UCITA에 의하면 컴퓨터정보는 '컴퓨터에 의하여 획득되거나 컴퓨터에 의하여 접속할 수 있거나 컴퓨터에 이용될 수 있는 전자적인(electronic) 형태의 정보'에 초점을 맞춘 것으로서 정보의 복제물[copy, 곧 정보를 포함하는 디스켓 등]과 정보를 포함한다고 규정되어 있다[Sec. 102(10)]. '전자적인'이라는 것은 디지털(digital)이나 이와 유사한 기능을 가진 형태의 정보를 포함한다고 하여 아날로그나 기타 미래의 컴퓨터 기술을 포함하는 형태의 정보를 의미한다고 규정함으로써, 디지털기

술에 한정함으로써 UCITA를 현재의 기술에 한정되어 적용될 가능성을 배제하고 있다. 컴퓨터정보는 그것이 컴퓨터로 들어갈 수 있다고 하여 컴퓨터정보가 되는 것은 아니며 컴퓨터에서 직접 처리될 수 있는 형태의 전자적인 정보에 한정된다. 또한 컴퓨터정보는 인쇄된 정보(printed information)나 정보가 포함되어 있지만 컴퓨터에서 직접 이용될 수 없는 비디지털형태(nondigital form)는 포함하지 않는다고 하고 있다. 그리고 컴퓨터정보 거래는 서적과 같은 인쇄물의 형태로 된 정보를 배포하거나 이를 배포하기 위하여 창조하기로 하는 계약을 포함하지 않으며, 인쇄물의 형태로 배포할 목적으로 정보를 창조하기로 하는 계약의 경우 그 정보가 전자적인 형태로 전달될지라도 그러한 계약에는 적용되지 않는다.

UCITA는 '컴퓨터정보 거래(computer information transactions)'에 대하여 컴퓨터정보나 컴퓨터정보권(computer informational rights)을 제작, 수정, 이전 또는 실시허락하기 위한 합의나 합의를 이행하는 것으로 정의하고 있다[102(11)]. 거래에 대한 통신을 컴퓨터정보의 형식에 의할 것이라고 당사자들이 합의한다고 해서 컴퓨터정보거래가 되지 않는다. 이것은 거래의 대상이 컴퓨터정보인 경우에 한정한다는 것이며, 당사자가 거래를 하기 위하여 컴퓨터정보를 사용한다고 해서 컴퓨터정보가 되는 것은 아니라는 것을 의미한다. 그리고 컴퓨터정보거래는 컴퓨터프로그램의 이전이나 소프트웨어를 개발하기 위한 계약을 포함한다.

요컨대 UCITA는 소프트웨어나 컴퓨터 데이터베이스와 같은 컴퓨터정보를 개발하기 위한 계약에 적용되며, 영화, 음향저작물, 방송프로그램 등에는 적용되지 않는다[Comment 2 to Sec.103]. 그리고 UCITA가 적용되는 것은 컴퓨터프로그램을 배포, 사용허락하는 것을 포함하는 계약에 적용되며, 거래가 컴퓨터프로그램의 복제물의 사용허락이거나 판매이거나에 관계없이 적용된다. 복제물의 사용허락과 판매는 서로 아무런 차이가 없기 때문이다. UCITA는 컴퓨터시스템에 대한 접속이나 컴퓨터시스템의 정보를 포함하는 계약에 적용된다. UCITA는 디지털방식의 멀티미디어 저작물의 개발 및 배포를 위한 계약에 적용된다. 그리고 UCITA는 컴퓨터정보의 데이터를 처리하거나 분석하기 위한 계약에 적용된다.

(2) 혼합거래

제103조 (b)항은 혼합된 거래(mixed transactions), 곧 컴퓨터정보와 컴퓨터정보권이 포함되는 거래이지만 그것이 거래의 주된 대상이 아닌 경우에는 컴퓨터정보와 컴퓨터정보권에 속하는 계약에 관한 쟁점을 포함하는 거래의 부분에 적용된다고 규정하고 있다. 곧 어떠한 거래가 컴퓨터정보와 물품(goods)을 포함하는 경우에는 컴퓨터정보, 컴퓨터정보에 대한 정보권, 그리고 컴퓨터정보를 개발하거나 수정하는 것을 포함하는 거래의 부분에 적용된다고 규정하고 있다. 그러나 컴퓨터프로그램의 복제물(copy)이 상품에 포함되거나 상품의 일부로서 판매·대여되는 경우에는 그 상품이 컴퓨터이거나 컴퓨터 주변기기인 경우 또는 그 상품의 매수인 등에게 그 프로그램에 대한 접근이나 사용을 허용하는 것이 그 상품을 거래하는 주된 목적인 경우에 UCITA가 적용된다.

(3) UCITA가 적용되지 않는 경우

UCITA 제103조 (c)항은 UCITA와 UCC 제9장이 충돌하는 한도에서는 제9장이 적용된다고 규정하고 있다. 제103조 (d)항은 UCITA의 적용이 배제되는 것으로서, (ⅰ) 금융서비스에 관한 계약, (ⅱ) 방송프로그램, 영화, 음향저작물, 음악저작물 및 음반 제조, 획득, 이용, 배포, 수정 등에 관한 계약, (ⅲ) 법정허락(강제적인 것이므로 계약과 상관없는 것), (ⅳ) 고용계약, (ⅴ) 컴퓨터정보를 자발적으로 사용하는 경우, (ⅵ) 대상이 통일상법전 제3장부터 제8장까지의 범위에 해당하는 경우 등을 열거하고 있다.

(4) 당사자들의 선택에 의한 적용배제

UCITA는 디지털정보거래에 계약 자유의 원칙이 지배하는 것을 인정하고 있다. 따라서 UCITA는 당사자가 UCITA가 적용될 것을 합의하거나 UCITA의 전부 또는 일부가 적용되지 않을 것을 합의할 수 있도록 하고 있다[104]. 그러나 당사자의 이같은 합의는 일정한 제한이 따른다.

첫째 UCITA가 적용된다고 당사자가 합의하더라도 당사자의 합의에

의하여 변경시킬 수 없거나 그 법이나 절차가 특정한 방법에 의하여서만 변경될 수 있는 법칙이나 절차가 적용되는 것이 배제되지는 않는다.

둘째, UCITA가 적용되지 않는다는 당사자의 합의는 전자적인 착오(electronic error)의 경우 소비자를 보호하기 위한 규정인 제214조와 전자적인 자구행위(electronic self-help)에 관한 규정인 제816조의 규정을 배제할 수 없다.

셋째, 대량시장계약의 경우 UCITA가 적용되지 않는다는 당사자의 합의는 UCITA의 합리성에 관한 원칙(doctrine of unconscionability), 기본적인 공공질서 또는 선의의 의무(obligation of good faith)에 관한 규정을 배제할 수 없다.

넷째, 대량시장계약의 경우, UCITA가 적용되는 정도를 변경시키는 조건은 눈에 띄는 명확한(conspicuous) 것이어야 한다.

## 5. Mass Market Licensing

### (1) 대량실시계약의 의의

대량실시계약(Mass Market License)은 대량시장거래(mass-market transaction)에서 사용되는 표준적인 형태의 계약을 의미한다[UCITA 102(44)]. 대량시장거래는 소매시장으로서 일반인들에게 유사한 조건에 따라 정보가 미리 포장된 형태로 이용될 수 있다. 이러한 시장의 주된 참여자는 소비자이며, 대부분의 거래가 상대적으로 적은 양을 대상으로 하며, 계약조건에 대하여 협상이 이루어지지 않으며, 재판매를 하는 자와의 거래가 아닌 최종 이용자와의 거래를 그 특징으로 한다. 이것은 실시권자(구매자)와 실시허락자(판매자)간에 계약조건을 일일이 협상하여 계약을 체결하는 경우의 높은 거래비용이 수반되는 것에 기인한다.

대량실시계약에서 쟁점이 되는 것은 이와 같이 당사자간에 계약조건에 대한 협상이 없이 체결된 계약의 조건이 계약의 내용으로 되어 구속력이 있겠느냐이다.

(2) Shrink Wrap License의 의의

1980년대에 들어오면서 컴퓨터가 광범위하게 이용되고 이에 따라 소프트웨어에 대한 수요가 증가함으로써 소프트웨어는 대규모적으로[곧 대량시장(mass market)에 의하여] 배포되기에 이르렀다. 따라서 소프트웨어의 복제물을 밀접하게 통제하거나 서비스를 제공하는 것이 적절하지 않게 되었다. 또한 협상을 하기 위한 거래비용에 비하여 실시허락을 하고자 하는 소프트웨어의 비용이 상대적으로 낮기 때문에 소프트웨어에 대한 실시허락을 개별적으로 협상하는 것이 비현실적인 것이 되었다. 따라서 소프트웨어 생산업자들은 실시허락을 위한 표준적인 계약을 점차 이용하고자 하였고, 결국 비닐로 포장된 소프트웨어 패키지에 표준적인 실시계약의 조건을 포함시키기에 이르렀는데, 'shrinkwrap license'라 불리는 것이 바로 이것이다. 이외에도 소프트웨어 생산업자들이 소프트웨어의 사용에 대한 책임이나 소프트웨어의 이용을 제한하거나 역분석(reverse engineering)을 금지하기 위하여, 또는 소프트웨어가 다시 이전되는 경우에 추가적인 수입을 얻기 위하여 shrinkwrap license를 이용하였다. 이와 같이 (ⅰ) 소프트웨어를 배포하는 데 사용되는 대량실시계약에서 (ⅱ) 계약의 조건을 소프트웨어의 포장지 자체 또는 포장지 내부에 인쇄되도록 하고, (ⅲ) 소비자는 이를 검토할 기회를 가지며 (ⅳ) 계약의 조건에 동의하는 것을 원하지 않는 소비자는 이를 반환할 수 있으며, (ⅴ) 계약조건에 대한 통지 및 계약의 조건에 소비자가 동의할 것을 요구하는 것이 포장의 외부에 나타나 있는 형태의 대량실시계약의 방법을 shrinkwrap license라고 한다.[2)]

Shrinkwrap license의 경우 소비자들은 소프트웨어를 구입하여 패키지를 열어볼 때까지 실시허락에 관한 조건을 알 수 없게 된다. 여기에서 한발 더 나아가 소프트웨어 생산업자들은 소프트웨어 자체에 실시허락에 관한 조건을 포함시키기 시작하였다. 이 경우 소프트웨어를 컴퓨터에 설

2) Daniel B. Ravicher, Facilitating Collaborative Software Development: The Enforceability of Mass-Market Public Software Licenses, 5 VA. J. L. & TECH. 11. 39-40 (2000).

치하기 전에 실시허락에 관한 조건이 화면상에 나타나며, 소비자가 이러한 조건에 동의한다면 마우스로 눌러서(click) 동의를 표시하도록 하여 소프트웨어 설치착업을 계속 진행시키게 한다. 'clickwrap license'(또는 click-here license)라 불리는 이러한 형태의 실시허락도 이에 대한 동의가 이루어지기 전에 소프트웨어의 매매라는 상거래가 이루어 질 것이 요구된다. 또한 인터넷(internet)의 이용이 보편화되면서 웹(world wide web)을 통하여 프로그램을 컴퓨터의 하드 드라이브에 다운로드(download) 받아서 이용할 수 있는 허락을 받을 수 있는데, 이것은 web-wrap license라고 불린다.

(3) Mass-Market License의 유효성

1) ProCD, Inc. v. Zeidenberg

대량실시계약 또는 shrink-wrap license가 유효한지 여부에 관한 대표적인 판례는 ProCD, Inc. v. Zeidenberg 케이스[3]이다. ProCD 케이스가 나오기 전에는 어느 법원도 Mass-Market License가 유효하다고 판결하지 않았으나, ProCD 케이스는 shrink-wrap license에 의한 표준적인 형태의 계약은 유효하다고 판결하였다. ProCD 케이스에서 원고는 많은 비용을 투자하여 1000만명을 수록하는 전화번호부를 제작하였고 이를 CD의 형태로 판매하였다. CD에는 방대한 정보를 효과적으로 이용할 수 있도록 하기 위한 탐색 소프트웨어가 내장되어 있었는데, 물론 이 소프트웨어는 저작권에 의하여 보호되는 것이었다. 그런데 CD를 포장하고 있는 상자에 의하면 소프트웨어가 동봉되어 있는 실시허락에 열거된 제한에 따른다고 언급되어 있었다. 실시허락은 CD에 내장되어 있었을 뿐만 아니라, 사용설명서에도 인쇄되어 있었으며, 소프트웨어가 운용될 때마다 화면에 나타났다. 이 실시허락에 의하면, 최종이용자(CD의 구매자)는 탐색 소프트웨어와 전화목록의 전부 또는 일부를 네트워크상의 다른 이용자가 이용하게 하거나 각각 다른 이용자가 시간을 달리 하여(time-shared) 이용하게 해서는 안되며, 목록에 접근하기 위하

3) 908 F. Supp. 640 (W.D. Wis.), rev'd, 86 F.3d 1447 (7th Cir. 1996).

여 사용되는 컴퓨터 이외의 컴퓨터에 목록의 전부 또는 일부를 이전시켜서는 안된다고 명시하고 있었다.

전원일치의 연방대법원 판결인 Feist 케이스에 의하면 전화목록은 저작권에 의하여 보호되는 것이 아니며 일반인의 공유영역에 속하는 것이다. 이에 기초하여 피고는 원고 CD의 모든 목록을 복제한 다음 피고의 탐색 소프트웨어를 결합시킨 다음 인터넷상의 웹 페이지에 모든 목록을 탐색할 수 있도록 함으로써 원고와 경쟁하였다. Feist 케이스로 인하여 전화목록을 복제한 것에 대한 저작권침해를 주장할 수 없었기 때문에 원고는 계약위반과 부당이용(misappropriation)을 주장하였다.

이러한 사실관계는 먼저 제작자가 일방적으로 정한 shrinkwrap license가 계약법상 구속력있는 합의가 될 수 있는가의 문제, 곧 위스콘신주가 채택한 UCC, 곧 주법의 해석에 관한 쟁점과 관계된다. 만약 구속력이 있다면, 계약이 저작권법의 측면에서 규율할 수 있는가의 문제로서 연방법 우선적용의 원리와 관련되는 연방법상의 쟁점이 발생한다. 이러한 쟁점에 대하여 제1심의 Crabb 판사는 모두 부정적으로 판단하여, 계약에 의한 권리주장은 저작권법 제301조에 의하여 그 적용이 배척된다고 하였다. 만약 이와 달리 판시한다면 저작권법이 달성하고자 하는 미세한 균형을 변경할 것이고, 특히 사실상 Feist 케이스에 위반하는 데도 불구하고 위반하지 않는 결과가 발생할 것이라는 것이다. 이에 대하여 제7연방 항소법원의 Easterbrook 판사는 계약상의 쟁점 두 가지 모두에 대하여 제1심 법원의 판결을 파기하였다.

2) UCITA

**가) 일반원칙 : 동의에 의한 채택**

UCITA 제208조는 당사자가 동의하는 경우에 표준적인 형태를 비롯한 기록의 조건을 계약의 조건으로 채택할 수 있다고 규정하고 있다[208(a)]. 이행 또는 사용이 시작된 후에도 기록의 조건이 당사자에 의하여 채택될 수 있다고 함으로써[208(b)] Mass-Market License에 대하여 규정하고 있다. 이 경우 합의의 전부 또는 일부가 후의 기록에 나타

날 것을 당사자가 알만한 이유를 가지고 있고 이행이나 사용이 시작되기 전에 그 기록을 검토할 기회가 없었어야 한다.

UCITA는 표준적인 형식의 기록으로 되어 있는 대량실시계약의 조건이 당사자간의 계약의 조건이 되기 위해서는 이행의 초기 또는 이행 중에 당사자가 실시계약에 동의할 것을 요구하고 있다[209(a)]. 동의를 할 수 있기 위해서는 동의를 하기 전에 기록을 검토할 기회를 가졌어야 한다. 만약 당사자가 이행하기 시작한 이후에 기록의 조건이 제기된 경우에는, 당사자가 이에 동의하고 그러한 조건이 제안될 것이라는 것을 알만한 이유가 있는 경우에만 유효하다[Comment 2 to Sec. 209].

**나) 예 외**

이러한 원칙에 대하여 UCITA는 두 가지 예외를 규정하고 있는데, 그 첫째가 불합리적이며 공공질서에 반하는 경우이다. 곧 당사자들이 기록의 조건을 수용하였을지라도 비합리적이거나 공공질서에 반하는 조건은 무효일 수 있다[209(a)(1)]. 특이하거나 숨겨져 있거나 일방적인 조건을 예로 들 수 있다.

둘째, 당사자들이 합의된 조건과 일치하지 않는 경우이다. 곧 대량 실시계약의 조건이 당사자가 명시적으로 합의한 조건과 일치하지 않는 경우, 대량 실시계약의 조건은 계약의 조건이 되지 않는다[209(a)(2)]. 이것은 당사자간에 이루어진 흥정을 대량 실시계약하에서의 조건에 의하여 변경시키지 못하도록 한 것이다.

**다) 반환권**

UCITA는 실시권자(곧 컴퓨터정보제품의 구입자)가 처음으로 실시계약에 동의를 할 때까지 조건이 알려지지 않은 경우 그 제품을 반환할 수 있는 권리(return right)를 부여하고 있다[211(2)]. 이것은 실시권자에게 실시계약의 조건을 검토하고 이를 수용하거나 거절할 기회를 보장해 주기 위한 것이다. 이것은 최종적인 이용자가 실시계약을 거부하고 정보를 이용할 수 있다는 것을 의미하는 것이 아니라, 처음으로 합의를 할 때 최종적인 소비자가 실시계약을 검토하고 이를 거부하였더라면 있었을

지위에 상응하는 지위로 돌아갈 수 있는 권리를 의미한다. 이 권리는 실시권자가 실시계약에 동의를 하는 경우에는 적용되지 않으며, 또한 동의하였던 합의를 당사자들이 취소할 수 있게 하는 수단이 아니다[Comment 4 to Sec. 209].

반환을 하는 당사자는 컴퓨터정보를 반환하거나 제거하도록 하는 실시허락자의 지시에 따라 야기된 합리적인 비용을 상환받을 수 있다[209(b)(1)]. 또한 컴퓨터정보를 실시권자가 설치한 이후에 반환하는 경우에는 설치하기 이전으로 복구하기 위하여 필요한 합리적이며 예견가능한 비용을 보상받을 수 있다[209(B)(2)].

## 제 2 절 통일전자거래법(UETA)

### 1. 입법의 필요성 및 UETA의 목적

통일전자거래법(Uniform Electronic Transactions Act, 이하 UETA)는 전자기록(electronic records)과 전자서명(electronic signature)을 일반적인 서면(document)과 수기에 의한 서명과 법적으로 동등한 것으로 취급하기 위한 것으로서, 이들이 법적 효력을 가지도록 통일적인 표준을 제공하는 것을 목적으로 하는 입법이다. 어떠한 계약이나 합의가 서면 및 서명에 의할 것을 법적으로 요구하는 것은 미국에서 기망방지법(statute of fraud)이나 서류에 의한 거래기록을 요구하는 기록보관법(record retention statute)에 기인한다. 이러한 법적 요건은 전자상거래에 대한 장애가 될 것이며, 따라서 UETA는 정보의 전자적인 기록을 인정함으로써 이러한 장애를 제거하였다.

UETA의 목적은 전자기록이나 서명을 유효화함으로써 전자상거래에 대한 장애를 제거하고자 하는 것이지, 계약에 관한 일반적인 사항을 규율하는 계약법이 아니다. 따라서 UETA에 의하여 미국 계약법의 실체적인 규범이 영향을 받는 것이 아니다. 또한 UETA는 일반적인 서명에 관한 법도 아니며, 서명에 관한 한 각주의 디지털서명법 및 연방의 전자서명법에 의하여 규율되며, UETA는 다만 이러한 법을 보완하는 역할을 할뿐이다.

### 2. 개념의 정의

UETA는 제2조에서 UETA에 사용되고 있는 용어에 대하여 정의하고 있는데, 주요한 용어로서는 자동화된 거래(automated transaction), 전자적인(electronic), 전자대리인(electronic agent), 전자기록(electronic record), 전자서명(electronic signature), 정보, 기록(record), 보안절차(security procedure) 등이다.

UETA는 '전자적인(electronic)'에 대하여 전기, 디지털, 자석, 무선, 광학, 전자기 또는 기타 이와 유사한 기능을 가진 기술과 관련된다고 정의하고 있다. 전자기록은 전자적인 수단에 의하여 창조·발생·송부·통신·수령·저장된 기록으로 정의되고 있으며, 전자서명은 어떠한 기록에 부착되어 있거나 논리적으로 연관되어 있고 그 기록에 서명할 의도가 있는 자가 실행하거나 채택한 음향·상징(symbol)·과정으로 정의되고 있다. 또한 기록은 유형의 매개체에 기재되어 있는 정보 또는 전자적 기타 매체에 저장되고 인식할 수 있는 형태로 검색할 수 있는 정보라고 정의되고 있다. 거래(transaction)에 대하여 UETA는 영업·상업·정부의 업무를 수행하는 것과 관계되는 2인 이상간에 행하여지는 행위 또는 일련의 행위라고 정의하고 있다.

### 3. 적용범위

UETA는 거래와 관련되는 전자기록과 전자서명에 적용된다는 원칙을 규정하고[3(a)], 적용되지 않는 사유를 열거하고 있다. 예컨대 유언이나 유언변경 또는 신탁에 대해서는 적용되지 않으며, 통일상법전의 일부(Sec.1-107, 1-206, 제2장, 제2A장을 제외한 UCC), 컴퓨터정보거래법(UCITA) 기타 법률이라고 규정하고 있다. 우선 UETA는 기본적으로 거래에 적용되는 것으로서, 모든 서면 및 서명에 적용되는 것이 아니라 거래와 관련되는 전자기록 및 서명에만 적용된다. 통일상법전의 일부가 적용에서 배제된 것은 UCC의 각 해당조항들이 이미 전자적인 거래를 반영하였다는 것을 인정한 것이다.

### 4. 전자기록과 서명의 인정 및 전자계약

UETA는 기본적으로 그 매체나 수단에 따라 기록, 서명, 계약에 영향을 미치지 않도록 하는 입장을 취하고 있다. 이에 따라 UETA는 기록이나 서명이 전자적인 형태로 되어 있다는 것만을 이유로 하여 그 법적 효력이나 집행력이 부인되어서는 안된다고 규정하고 있다[7(a)]. 또한 계약의 체결에 있어서 전자기록이 사용되었다고 해서 계약의 법적 효과나 집행력이 부인되어서는 안된다고 규정하고 있다[7(b)]. 기록이 서면으로 행하여질 것이 법에 의하여 요구되는 경우 전자기록에 의하여 이 요건은 충족되며, 서명이 법에 의하여 요구되는 경우 역시 전자서명에 의하여 이 요건은 충족된다[7(c)(d)].

제7조는 UETA의 기본적인 전제를 규정하는 것으로서, 기록이나 서명 또는 계약이 창조, 제시, 유지되는 매체가 그 법적 의미에 아무런 영향을 주지 못하도록 하고 있다.

### 5. 전자기록 및 전자서명의 귀속 및 효과

UETA는 전자기록이나 전자서명이 어떠한 사람의 행위인 경우에는 그 사람에게 귀속된다고 규정하여[9(a)] 발생된 효력의 귀속주체를 명시하고 있다. 어떠한 사람의 행위가 있었는지 여부는 전자기록이나 전자서명이 귀속될 자를 결정하기 위하여 사용되는 어떠한 보안절차에 의하여서도 입증될 수 있다[9(a)]. 이것은 귀속(attribution)에 관하여 존재하는 규칙을 변경하는 것이 아니며, 귀속에 관하여 존재하고 있는 규칙이 전자적인 환경에서도 적용될 수 있다는 것을 확인하는 것이다. 예컨대 전자우편에 의하여 주문을 하는 경우 특정인이나 그의 피고용자가 그 특정인의 성명을 주문의 일부로서 타이프치거나, 상품을 주문하도록 프로그램된 특정인의 컴퓨터가 주문의 일부로서 그 특정인의 성명 기타 그 특정인을 나타내는 정보를 포함하는 주문을 하는 경우, 전자기록과 전자서명은 그 특정인에게 귀속된다.[4] 어떠한 기록을 특정인에게 귀속시키는

4) Comment to Art. 9.

주된 방법은 서명이지만 서명에 한정되지는 않으며, 팩시밀리에 나타나 있는 정보(인쇄된 종이에 나타나 있는 정보)도 정보에 의하여 귀속을 결정할 수 있다.

일단 기록이나 서명의 특정인에게 귀속되는 것이 정해진 경우, 그 특정인에게 귀속된 전자기록이나 전자서명의 효과는 기록을 행하거나 전자서명을 하는 당시의 상황에 따라 결정하도록 되어 있다[9(b)].

### 6. 전자기록의 변경이나 오류

거래당사자간에 전송되는 과정에서 전자기록이 변경되거나 오류가 발생한 경우에 전자기록의 효력이 어떻게 될 것인가가 문제된다. 우선 당사자들이 변경이나 오류를 검색하기 위한 보안절차를 사용할 것을 합의하였는데 한 당사자는 이러한 절차를 준수하였으나 다른 당사자는 준수하지 않은 경우, 준수하지 않은 당사자도 절차를 준수하였더라면 변경이나 오류를 찾아낼 수 있었다면 준수한 당사자는 변경되거나 오류가 있는 전자기록의 효력을 부인할 수 있다[10(1)].

자동화된 거래에 있어서 어느 개인이 전자대리인과 거래를 하는 과정에서 오류를 범한 경우 UETA는 일정한 요건하에 그 개인이 오류로 인한 전자기록의 효력을 부인할 수 있도록 하고 있다. 첫째, 전자대리인이 오류를 방지하거나 정정할 기회를 제공하지 않았어야 한다. 둘째, 그 개인이 오류를 인지하게 된 때에 그 개인이 (ⅰ) 상대방에게 오류를 즉시 통지하고 상대방이 수령한 전자기록에 의하여 그 개인이 구속될 것을 의도하지 않아야 하며, (ⅱ) 그 개인이 오류가 있는 전자기록으로 인하여 상대방으로부터 받은 대가(consideration)를, 상대방의 합리적인 지시에 의하여, 반환하거나 제거하여야 하며, (ⅲ) 상대방으로부터 받은 대가로부터 이익이나 가치를 사용·수령하지 않았어야 한다[10(2)].

위의 두 가지에 해당하지 않는 경우의 변경이나 오류는 다른 법이 정한 바에 의하여 결정된다[10(3)]. 제10조 2항과 3항은 당사자들이 합의에 의하여 배제할 수 없는 강행규정이다.

### 7. 전자기록의 보관

법에 의하여 기록이 보관될 것이 요구되는 경우, 그 기록에 있는 정보의 전자적인 기록이 보관되면 된다. 다만 이 전자적인 기록은 전자적인 기록으로 처음으로 작성된 후 기록에 나타나 있는 정보를 정확히 반영하여야 하며 후에 참조하기 위하여 접속될 수 있는 것이어야 한다[12(a)]. 어떠한 기록이 원본 그대로 제출되거나 보관될 것이 요구되는 경우에도 마찬가지이다[12(d)].

### 8. 증거로서의 채택

기록이나 서명이 전자적인 형태로 되어 있더라도 증거로서 배제될 수 없다([13].

### 9. 자동화된 거래

'자동화된 거래(automated transaction)'는, 전체 또는 부분적으로, 전자적인 수단이나 전자적인 기록에 의하여 행하여지는 거래로서, 한 당사자 또는 양 당사자의 행위나 기록이 계약의 체결 및 이행과 거래상의 의무의 이행에 있어서 사람에 의하여 검토되지 않는 거래를 의미한다[2(2)]. 이러한 자동화된 거래에 있어서 계약은 당사자들의 전자대리인의 상호행위에 의하여 체결될 수 있으며 어느 개인이 전자대리인의 행위나 이에 따른 계약조건이나 합의를 알지 못하거나 검토하지 않더라도 마찬가지라고 함으로써[14(1)], 전자대리인에 의한 자동화된 거래를 인정하고 있다. 또한 계약은 사람과 전자대리인간의 상호행위에 의하여 체결될 수 있다[14(2)]. 따라서 이 규정은 인간의 의사(intent)가 결여됨으로써 계약이 체결될 수 없다는 것을 완전히 배제하고 있다. 곧 거래에 기계가 관여하는 경우에 있어서 필요한 의사는 프로그램을 만드는 것과 기계를 이용하는 것에서 생긴다는 것을 인정하였다.

전자대리인(electronic agent)은, 사람이 검토하거나 사람에 의한 행위가 없이, 전체 또는 부분적으로 전자기록이나 이행을 독립적으로 시작

하거나 이에 대처하기 위하여 사용되는 컴퓨터 프로그램이나 전자적 수단 또는 기타의 수단을 의미한다[2(6)]. 전자대리인은 컴퓨터프로그램이나 기타 자동화된 수단과 같은 기계로서, 이를 사용하는 사람의 도구이다. 도구는 독립적인 의지가 없기 때문에 이 도구를 사용하는 자는 이를 사용함으로써 발생하는 결과에 대하여 책임을 지는 것이 일반적이다. 전자대리인은, 프로그램의 파라미터(parameter)의 한도에서, 일단 어느 당사자에 의하여 착동되었다면, 그 당사자가 다시 관여하지 않더라도 다른 당사자 또는 전자대리인과 상호작용할 수 있다.[5]

## 제 3 절 연방전자서명법

### 1. 전자서명법의 의의

미국의 클린턴 대통령은 2000년 6월 30일 전자서명법(Electronic Signatures in Global and National Commerce Act, 이하 연방 전자서명법 또는 E-Sign Act)[6]에 서명함으로써 연방서명법은 2000년 10월 1일에 발효하게 되었다. E-Sign Act는 전자상거래에 있어서 획기적인 입법으로서, 이 법이 추구하는 근본적인 목적은 거래에 관련되는 서명, 계약, 기록이 전자적인 형태로 되어 있다고 해서 그 법적 효력 및 집행이 부인되는 것이 아니라는 원칙을 확립하는 것이다. 전자서명법이 제정되기 전 각 주들은 주 내에서 이러한 효과를 가지는 입법을 해 왔으나, 이러한 입법을 한 주는 과반수를 넘지 못하였고 제정된 입법도 상당히 달랐다. 미국에서 디지털서명의 집행력과 진정성(authenticity)에 관한 쟁점은 연방법이 아니라 대부분 주에 의하여 규율되었다. 주 중에서도 유타주는 공개키 기반구조(public key infrastructure)에 기초한 디지털서명법을 처음으로 입법하였으며, 유타주의 디지털서명법은 미국변호사협회(ABA)의 디지털서명에 관한 가이드라인(Digital Signature Guidelines) 모범으로 하였다. 2001년 현재 미국에서는 약 41개주에서 디지털서명에 관한 법을 가지고 있거나 주의회에 의한 입법작업중에 있

5) Comment to Art. 2 of UETA.
6) 15 U.S.C. § §7001-

다. 주들에 의한 디지털서명의 규율이 통일되지 않음으로써 전자상거래에 대한 대처가 지연되고 디지털서명에 관한 법이 통일되지 않는 위험이 있게 되었다. 곧 각 주간의 상이한 입법으로 인하여 야기되는 주간의 효율적인 온라인 거래에 대한 장애를 제거하고 여러 주가 입법을 하지 않음으로써 야기되는 불확실을 제거하기 위한 수단으로서 전자서명법은 전국적으로 통일적인 표준을 규정한 것이었다. 그러나 전자서명법은 각 주의 입법이 연방법의 표준에 합치한다면 각 주가 주 자체의 입법을 하는 것을 허용하였다.

### 2. 유타주의 디지털서명법

미국 주 중에서의 최초의 디지털서명법인 유타주의 디지털서명법은 ABA의 디지털서명 가이드라인[7]에 기초한 것이다. 이 법의 주목적은 전자상거래를 진작시키기 위한 것인데, ABA의 가이드라인을 기초하였던 위원회의 몇몇 위원들은 가이드라인이 완성되기 전에 유타주를 위하여 디지털서명을 위한 샘플법령을 기초하였고, 이에 따라 유타주 디티털서명법(Utah Digital Signature Act)[8]이 제정되었다. 유타주의 입법 후 여러 주들이 유타주의 법과 유사한 입법을 하였으며, 유타주의 입법은 한국의 전자서명법을 비롯한 외국의 입법에도 많은 영향을 주었다.

유타주의 디지털서명법에 의하면, 두 가지의 요건을 충족하다면, 종이에 서명된 것과 같이 디지털서명은 유효하고 집행력이 있다. 첫 요건은 메시지가 디지털서명을 포함하고 있어야 한다는 것이며 둘째로는, 디지털서명은 인증서에 기재된 공개키에 의하여 입증되어야 한다는 것이다. 유타주의 법을 충족하는 디지털서명은 자서(自書)에 의한 서명을 요구하는 유타주의 법을 충족한다고 함으로써, 자서에 의한 서명을 요구하는 유타주의 법령을 수정할 필요성을 제거시켜 주었다. 또한 주 자체가 주된 인증기관(CA)이 될 뿐만 아니라 유타주의 상무부를 통하여 인증기관을 허가하도록 규정하고 있다.

---

7) ABA, Information Security Committee, Electronic Commerce Division, Digital Signature Guidelines 1996 A.B.A. Sec. Sci. & Tech. 13.

8) Utah Digital Signature Act, Utah Code Ann. §46-3-101.

### 3. E-Sign Act의 제정배경 : UETA와의 관계

미국에서 E-Sign Act가 제정되기 전 많은 주 및 연방법들은 자서에 의한 서명 및 서류에 의한 기록을 요구하는 규정들을 가지고 있었다. 여러 주들이 전자서명 및 전자기록에 부분적인 효력을 부여하였으나 어떠한 경우에 전자서명이나 기록이 유효하고 집행력이 있는가에 대한 법이 통일되지 않았다. 이러한 법통일의 필요성을 인식하여 1997년 NCCUSL은 모든 주가 공통적으로 채택할 수 있도록 전자서명 및 기록을 사용하는 것에 관한 통일적인 기준을 규정하는 모범법을 제정하고자 하였다. 이에 따라 UETA가 탄생하게 되었고 NCCUSL은 1999년 7월 UETA 최종초안을 승인하였다.

UETA는 다른 종류의 통일법[예컨대 통일상법전(UCC)]과 마찬가지로 각주의 의회가 이를 채택하여야 채택한 주의 법으로 성립한다. 사실상 UETA는 E-Sign Act가 기초하는 토대를 마련하였으며, E-Sign Act와 마찬가지로 전자서명 및 기록이 서면과 서명을 요구하는 법적 요건을 충족한다고 규정하고 있다(UETA 제7조). 또한 UETA는 전자적인 환경에서 당사자간의 합의, 정보의 교환, 정보의 보관, 의무의 이행 등의 목적을 달성하고자 하였으며, 전자적인 기록을 사용하려는 당사자에 대하여 확실성과 법적 보호를 제공하고자 하였다. 뿐만 아니라 규범을 충족하기 위하여 특별한 방법이나 기술을 특정하는 것을 거부함으로써, 기술중립성(technology neutrality)의 개념을 포함하고 있다.

E-Sign Act가 제정될 당시 약 18개의 주가 UETA를 채택하고 있었다. 그러나 과거의 경험으로 미루어볼 때, NCCUSL의 통일법을 모든 주가 채택하는 데에는 약 4년 내지 7년의 기간이 소요되었다. 따라서 미국의 연방의회는 전자상거래 및 인터넷에 대해서는 보다 더 빠른 조치가 필요하다고 여기게 되었다. 뿐만 아니라 인터넷은 국경을 전제로 하는 매개체가 아니므로, 이에 대한 규율이 비효율적인 것이 된다면 미국 각 주의 법이 통일되지 않을 우려가 있었다.

E-Sign Act의 제정을 서두르게 했던 또 다른 사유는, 캘리포니아 주에 의한 UETA의 입법과 같이, 몇몇 주가 NCCUSL이 기초한 통일법의

법안과 상당히 다르게 입법한다는 사실이었다. 캘리포니아 주는 UETA의 적용으로부터 상당한 수의 소비자거래 및 금융거래를 제외하였다. 따라서 연방 의회는 이러한 방식의 UETA 입법으로 인하여 주들에 의한 UETA의 채택에 의하여 법의 통일을 달성하는 것은 매우 어렵고 따라서 상당 분야의 상거래가 UETA에 의하여 혜택을 받을 수 없을 것이라고 판단하게 되었다.[9]

E-Sign Act는 UETA와 마찬가지로 이미 존재하는 주법 및 연방법을 대신하는 것이 아니라 이러한 기존의 법에 추가하여 전자서명 및 전자서류에 법집행력과 법적 효력을 부여하고 있다. E-Sign Act는 UETA의 주요 특징 및 기본적인 정책목표를 채택하고 있다. 곧 E-Sign Act는, UETA와 마찬가지로, 첫째, 기록이나 서명은 그것이 전자적인 형태로 되어 있다는 것만을 이유로 하여 법적 효력과 집행력이 부인되어서는 안 된다는 것, 둘째, 법에 의하여 기록이 서면에 의할 것으로 요구되는 경우, 전자기록이 이러한 요건을 충족한다는 것, 셋째, 법에 의하여 서명이 요구되는 경우, 전자서명이 이 요건을 충족한다는 것 등 세 가지의 일반적인 규칙에 기초하고 있다.

### 4. E-Sign Act의 주요내용

#### (1) 일반원리

전자서명법은 전통적인 법적 요건인 서면(writing) 또는 서명(signature)이 전자적인 환경에서 야기되는 법적 불확실성을 제거하고자 하는 것이었다. 곧 계약이 서명되거나 서류는 서면이어야 한다는 법적 요건은 전자적으로 서명된 계약이나 전자적인 서류에 의하여 충족될 수 있도록 하는 것이다. 곧 전자매체(electronic medium)에 대해서도 종이로 된 매체와 동일한 법적 효과를 부여하고 동일하게 이행될 수 있도록 하는 것이다.[10] 이에 따라 전자서명법 제101(a)는 (1) 서명, 계약 또는 거래에

9) Jeremiah S. Buckley & Margo H.K. Tank, The Electronic Signatures in Global and National Commerce Act—An Overview, 20 ANN. REV. BANKING L. 221, 222-225 (2001).

10) Statement by Representative Bliley, 146 Cong.Rec. H4352 (June 14, 2000).

관한 기타의 기록은, 전자적인 형태로 되어 있다고 해서, 그 법적 효과, 유효성, 이행가능성이 부인되어서는 안되며, (2) 거래에 관한 계약은, 계약을 체결하는 데 있어서 전자서명이나 기타 전자기록이 사용되었다고 해서, 그 법적 효과, 유효성, 이행가능성이 부인되어서는 안된다고 규정하고 있다. 이 규정의 내용은 UCITA 107(a)의 내용과 동일한 것이다.

전자서명법은 '전자적인(electronic)'에 대하여 전기, 디지털, 마그네틱, 무선, 광학적, 전자기 기타 이와 유사한 기능을 가진 기술과 관련되는 수단이라고 정의하고 있다. '전자기록(electronic record)'은 전자적인 수단에 의하여 생성, 송신, 통신, 수령, 저장되는 계약 또는 기타 서류, '전자서명'은 계약이나 기타 기록에 첨부되거나 논리적으로 연관되며 기록에 대하여 서명하려는 자가 실행하거나 채택하는 전자적인 음향, 상징, 과정으로 정의하고 있다(제106조). 전자서명법은 UETA와 마찬가지로 특별한 전자서명을 특정하지 않고 있으며, 당사자가 이를 선택할 수 있도록 하고 있다. 따라서 전자서명은 일정한 과정에 의하여 단순히 클릭하는 것(예컨대 "I Agree"라고 되어 있는 부분을 클릭하는 것), 사람의 동공, 지문, 음성 등을 이용한 생물학적인 방법에 따라 확인하는 것(biometric identification), 수기된 서명을 디지털화하는 것 기타 이들을 결합한 것이 될 수 있다.[11]

(2) 적용범위

첫째, E-Sign Act는 서면이나 서명을 요구하는 법에 아무런 영향을 미치지 않는다[§ 101(b)(1)].

둘째, E-Sign Act는 소비자보호법에 의한 실체적인 보호에 아무런 영향을 미치지 않으며, 법령 등에 의하여 소비자에게 제공되거나 이용될 것으로 요구되는 서류의 내용 및 공시시기에 대하여 아무런 영향을 미치지 않는다[§ 101(c)(2)(A)].

셋째, E-Sign Act는 특정한 거래 및 통신에 대하여 전자서명법이 적용되는 문제점을 해결하기 위하여 전자서명법은 적용의 예외를 규정하고 있다. 곧 103(a)는 전자서명법 제101조가 규정하고 있는 원리와 요건이

11) Buckley & Tank, at 225.

적용되지 않는 것으로서, 유언·유언변경, 신탁·입양·이혼·기타 가족법 관련사항, 1-107·1-206·매매 및 리스에 관한 2편 및 2A편을 제외한 통일상법전 등이 규율하는 한도에서 계약이나 기타의 기록에 적용되지 않는다고 규정하고 있다. 또한 103(b)는 법원의 명령·통지 또는 공식적인 법원서류, 공공서비스의 취소나 종료 등의 통지에 대해서도 적용되지 않는다고 규정하고 있다.

(3) 소비자보호

전자서명법에 있어서 가장 논란이 되었던 쟁점은 소비자보호에 관한 것이었다. 캘리포니아 주는 UETA를 주법으로 입법하는 데 있어서 상당수의 소비자거래를 UETA로부터 제외시켰는데, E-Sign Act를 제정하는 데 있어서도 광범위한 제외를 규정하여야 한다는 주장이 제기되었으나, 이같은 주장은 배척되었다. 소비자 옹호자들의 주된 근심사항은 소비자들이 전자적인 통신을 통하여 계약조건에 의하여 구속당한다는 것을 알지 못할 수 있으며 온라인상의 법률관계에 대한 통제를 의식하지 못한다는 것이었다. 예컨대 소비자들은 온라인상으로 계약을 체결하도록 유인될 수 있으나, 기술적인 발전이나 변화로 인하여 계약조건의 변경을 통지받을 수 없다는 것이다. 이와 마찬가지로 컴퓨터 시스템의 변경이나 전자우편의 변경으로 인하여 소비자들은 중요한 통지사항을 역시 수령하지 못할 수도 있다는 것이었다. 이러한 문제점을 해결하기 위하여 전자서명법은 소비자들이 온라인상 체결한 계약의 조건을 통지받고 인식하며 적절하게 통제할 수 있도록 하기 위한 특별한 규정들을 포함하고 있다.

소비자들은 E-Sign Act에 의하여 특별한 보호를 받는다. 거래에 관한 정보가 소비자에게 서면에 의하여 제공되어야 하거나 소비자가 이용할 수 있도록 법령 등에 의하여 요구되는 경우, 이러한 정보를 제공 또는 이용가능하게 하기 위하여 전자적인 기록을 사용하는 것이 법의 요건을 충족한 것으로 되기 위해서는 일정한 요건을 충족하여야 한다. 곧 (i) 소비자가 그러한 전자적인 기록의 사용에 적극적으로 동의하고 그러한 동의를 철회하지 않았어야 하며, (ii) ①소비자가 서류를 서면 또는 전자

적인 형태로 제공받거나 이용할 수 있다는 권리를 가지며 동의를 철회할 수 있는 권리를 알리고, ②소비자의 동의는 의무를 야기시키는 특정 거래에만 적용되는지 아니면 정해진 유형의 기록에도 적용되는지 여부를 소비자에게 알리고, ③소비자가 동의를 철회하기 위하여 사용하여야 하는 절차를 설명하고, ④소비자가 동의를 한 이후에 어떻게 전자적인 서류의 복제본을 획득하는지 소비자에게 알리는 등의 명확하고 눈에 띄는(conspicuous) 서면이 소비자가 동의하기 전에 제공되어야 한다[101(c)(2)].

또한 소비자가 동의의 대상이 된 정보를 제공하기 위하여 사용되었던 전자적인 방식으로 정보에 접속할 수 있다는 것을 합리적으로 증명할 수 있는 방식으로, 소비자가 전자적으로 동의하거나 자신의 동의를 전자적으로 확인하여야 한다[101(c)(1)(C)(ⅰ)]. 곧 소비자는 전자적인 기록에 접속하고 이를 보유하기 위하여 필요로 하는 하드웨어나 소프트웨어의 요건에 대한 언급(statement)을 제공받아야 한다. 또한 소비자가 동의한 후 전자기록에 접속하기 위하여 필요로 하는 하드웨어나 소프트웨어의 요건에 변화가 발생하여 소비자가 그 이후의 전자기록에 접속하거나 이를 보유할 수 없는 중대한 위험이 야기되는 경우, 동의를 철회할 수 있는 기회를 제공하는 하드웨어 또는 소프트웨어의 개정된 요건에 대한 언급을 제공받아야 한다[101(c)(1)(D)(ⅱ)].

소비자의 동의에 관한 요건은 정보를 전자적으로 제공하는 것에 대한 법적 효과를 보장하는 것이다. 그러나 이 규정을 준수하지 않았다고 해서 계약의 법적 효과, 유효성, 이행가능성에 영향을 주지 않는다[101(c)(3)]. 이 경우에는 일반적인 계약에 관한 실체법이 적용된다. 소비자가 서명을 하기 전에 온라인상으로 계약의 조건을 볼 수 있었던 경우, 비록 소비자가 전자적인 형태의 정보에 접속할 수 있다는 것이 합리적으로 나타낼 수 있는 방법으로 동의하지 않았더라도, 이행가능한 계약이 존재하게 된다.

(4) 정부와의 거래

전자서명법을 제정하면서 제기되었던 쟁점 중의 하나는 정부의 업무에 영향을 주는 행위가 전자서명법상의 거래(transaction)에 해당될 수 있

다는 것이었다. 이에 따라 전자서명법은 정부와 관련되는 특정한 행위를 전자서명법이 규정하고 있는 거래의 개념으로부터 제외하였다. 따라서 주로 정부의 목적을 위한 개인당사자의 행위와 정부의 행위는 전자서명법상의 거래가 되지 않는다.

(5) 기록의 보존

전자서명법은 법령에 의하여 계약이나 거래와 관계되는 서류가 보존될 것이 요구되는 경우, 계약에 관한 정보의 전자적인 기록이나 기타 기록을 보존하면 되는데, 이러한 기록은 두 가지 요건을 충족하여야 한다[101(d)]. 곧 첫째, 전자기록 등은 계약이나 기타 기록에 규정된 정보를 정확하게 반영하여야 하며, 둘째, 법령에 의하여 이에 접속할 권리가 있는 모든 사람이 접속할 수 있어야 한다.

(6) 전자대리인의 인정

전자서명법은 UCITA와 마찬가지로 전자대리인(electronic agent)을 인정하고 있다. 곧 계약이나 기타 기록은, 그 성립, 작성 또는 인도가 하나 이상의 전자대리인의 행위를 포함하고 있다고 해서, 법적 효력, 유효성, 이행가능성이 부인되어서는 안된다고 규정하고 있다[101(g)]. 다만 전자대리인의 사용이 인정되기 위해서는 전자대리인의 행위가 이에 구속될 자에게 법적으로 귀속될 수 있어야 한다. '전자대리인(electronic agent)'은 컴퓨터 프로그램이나 전자적 또는 기타 자동화된 수단을 지칭하는 것으로서 어떠한 행위나 반응을 하는 시점에 개인이 이를 검토하거나 행위를 하지 않고서 독립적으로 행위를 야기하거나 전자적인 기록에 반응하는 수단이라고 정의하고 있다[]106.

(7) 연방정부 및 주정부에 대한 적용 배제

전자서명법 제104조는 연방정부 및 주정부기관이 일정한 경우에는 서명이나 기록이 계속하여 서면으로 행하여질 것을 요구할 수 있도록 융통성을 부여하고 있다. 곧 연방정부 및 주정부기관은 종이로 된 서류나 기

록의 작성을 요구하는 등 서류의 작성을 위한 표준이나 방식을 규정할 수 있으며, 101(c)가 규정하고 있는 소비자의 동의를 요구하는 요건을 면제할 수 있다.

(8) 연방법의 우선적용 및 UETA

전자서명법의 매우 중요한 내용 중의 하나는 주법과의 관계에 관한 것이다. 전자서명법은 주간의 통상 및 외국과의 통상에서 또는 이러한 통상에 영향을 주는 거래에 적용된다. 그런데 전자서명법은, 각 주들이 1999년 7월에 승인된 UETA를 각 주가 채택한다면, 각 주들은 전자서명법을 수정 또는 제한하거나 이를 대신할 수 있다고 규정하고 있다. UETA는 전자서명법과 유사하게 기능을 하지만 몇 가지 점에서 차이가 있다. 이에 따라 전자서명법은 전자서명법이 통일적으로 적용되는 것을 손상하는 UETA의 두 가지 규정을 무효화하고 있다. 첫째, UETA 제3(b)(4)는 각 주들이 특정한 주의 법을 UETA의 적용으로부터 제외하는 것을 허용하고 있다. 이 규정을 이용하여 주의 법을 제외시킨 대표적인 주가 캘리포니아 주인데, 캘리포니아 주는 약 65개의 소비자보호관련 법률을 UETA의 적용으로부터 제외시키고 있다.[12] 요컨대 UETA가 주로 하여금 일정한 법을 UETA가 적용되는 것으로부터 제외시키고 전자서명법은 1999년의 UETA를 채택한 주에게 전자서명법을 제외시킬 수 있도록 하고 있는데, 양 법의 이러한 조항에 의하여 1999년의 UETA를 채택한 국가는 결국 전자서명법과 달리 규정할 수 있게 되어 전자서명법이 통일적으로 적용되는 것이 손상된다. 따라서 전자서명법은 UETA 3(b)(4)에 따라 주가 정해놓은 예외는, 그러한 예외가 전자서명법과 일치하지 않는 한도에서, 전자서명법이 우선적으로 적용된다고 규정하고 있다.

둘째, UETA 8(b)(2)는 주가 기록을 전달하는 방법을 특정할 수 있도록 허용하고 있다. 전자서명법은, 주가 이 규정에 따라 비전자적인 전달방법을 부과함으로써 전자적인 기록의 유효성에 관한 일반적인 원칙을 회피하는 것을 허용하지 않음으로써, UETA 8(b)(2)를 무효화하고 있다.

12) Cal. Civil Code §1633.3(b) (West 2000).

# 제 3 장 지적재산권

## 제 1 절 서 론

인터넷과 관련하여 야기되는 법적 쟁점 중에서 가장 많은 쟁점이 발생되는 분야는 지적재산권 분야이다. 따라서 현재 인터넷관련 법제에서 가장 많은 입법이 행하여진 분야도 지적재산권 분야임을 부정할 수 없다. 인터넷과 관련하여 상표, 저작권, 특허, 영업비밀, 데이터베이스(data base), 퍼블리시티권(right of publicity), 트레이드 드레스(trade dress) 등 디지털환경에 적용되는 것과 관련하여 많은 문제점이 발생하고 있다. 우선 저작권과 관련하여 인터넷을 통하여 전송되는 저작물의 중간적이거나(interim) 최종적인(final) 복제물(copies)은 저작권법상의 복제물에 해당하는가의 여부, 인터넷상에서의 검색(browsing)에 의한 복제권, 전시권, 공연권 침해여부, 이용자의 컴퓨터에서 서비스제공자의 컴퓨터 기타 여러 컴퓨터에 정보를 올리는 경우(uploading)와 저작물을 다운로드(download) 받는 경우의 복제권의 침해여부, 전자우편의 송수신에 의한 복제권의 침해여부, 디지털방식에 의한 전송이 공연권이나 전시권을 침해하는지 여부, WIPO 저작권 조약의 통신권(rights of communication, 제8조)에 관한 쟁점, 저작물이 디지털화화는 경우의 2차적 저작물에 관한 쟁점 등 저작권의 배타적인 권리에 관한 쟁점이 발생한다. 인터넷상에서 저작자의 권리범위의 설정은 독점적인 권리부여에 의한 창작의 인센티브뿐만 아니라 인터넷상에서 저작물을 이용할 수 있는 일반인의 이익과 인터넷의 발달에 영향을 줄 수 있는 문제이므로, 양자를 매우 정교하게 균형시켜야 하는 정책적인 쟁점까지도 발생한다. 또한 저작권과 관련된 쟁점에는 인터넷 서비스제공자(internet service provider, ISP), BBS(bulletin board service) 운영자, 웹사이트(web site) 운영자 등의 저작권법상의 책임, 이미 출판된 간행물을 다시 전자 데이터베이스로서 복제한 경우의 전자출판권(electronic publishing right)에 관한 쟁점, 현재 진행되고 있는 경기의 점수나 기록과 같이 시간과

밀접한 관계가 있는 정보(time-sensitive or hot-news information)의 저작권에 의한 보호의 문제, 온라인상에서의 공정이용(fair use)의 문제, 링크와 프레이밍에 의한 저작권 침해문제, 케싱(caching)에 의한 저작권 침해문제 등의 쟁점이 발생한다.

인터넷에서 특허법과 관련된 것으로서는 신규성을 판단하는 데 있어서 웹사이트나 기타 인터넷상에 게시된 자료 또는 정보가 발명을 기재하고 있는 경우 특허요건으로서의 신규성이 상실되느냐 여부와 통신, 암호화(cryptography), 전자우편, 전자지급(electronic bill paying), 전자자료교환(electronic data interchange, EDI), 그래픽 사용자환경(graphic user interface, GUI) 등과 관련된 기술이 특허의 대상이 되는가 등을 들 수 있다.

사이버공간에서의 상표법상의 쟁점은 크게 세 가지로 분류할 수 있다.

첫째, 도메인네임과 상표간의 문제로서 상표법상의 문제로서 가장 혼한 형태라고 할 수 있다. 예컨대, 도메인네임이 상표인가, 타인의 상표를 도메인네임으로 이용한 경우 상표의 침해가 되는가, 타인이 자신의 상표나 상호를 도메인네임으로 등록하였다면 어떻게 대처하여야 할 것인가 등의 쟁점이다.

둘째, 인터넷, 특히 웹의 기술인 링크, 프레이밍, 메타텍 등은 저작권과도 관련되지만 상표의 이용과 밀접한 관계가 있으며 상표법상의 문제점을 일으키고 있다.

셋째, 예컨대 인터넷상에 자료를 올리거나(uploading) 자료를 받는(downloading) 등 인터넷상에서의 행위와 관련하여 상표법상의 분쟁이 발생한다.

넷째, 도메인네임 체계(domain name system)에 관한 쟁점이다. 도메인네임 체계는 인터넷주소를 IP 주소로 번역하기 위하여 사용되는, 분산되어 존재하는 정보의 데이터베이스로서, 이용자가 인터넷을 탐험할 수 있도록 하기 위한 것이다.

저작권 및 특허 그리고 상표 이외에도 인터넷과 관련하여 영업비밀과 관계된 쟁점, 예컨대 영업비밀이 인터넷에 올라가 있는 경우 비밀성

(secrecy)을 상실하는지에 관한 쟁점이나 영업비밀이 인터넷에 연결된 네트웨크상에 전송되어 있거나 기타 외부의 서비스공급업가 전송시키고 있는 경우나 해커(hacker)가 암호코드를 해독하는 경우와 같이 영업비밀의 보호에 관한 쟁점이 발생한다. 그리고 온라인상으로 데이터베이스의 중요성은 커지고 있는데, 편집저작물의 개별적인 정보를 보호받기 위한 방안, 예컨대 영업비밀로 유지하거나 계약에 의하여 보호하는 것과 관련된 쟁점이 발생한다. 유명인의 이름이나 이미지를 승낙을 받지 않고 이용하는 것으로부터 보호하는 권리도 ISP나 웹사이트 운영자에 의하여 침해될 수 있으므로, 퍼블리시티권에 관한 문제점이 발생한다. 현재 미국에서는 웹사이트나 사용자환경(user interface)을 트레이드 드레스로서 보호하려는 시도가 많이 행해지고 있는데, 컴퓨터 프로그램의 비어문적인 요소(nonliteral aspects)에 대한 저작권에 의한 보호범위를 제한하는 미국의 판례들을 고려한다면, 트레이드 드레스(trade dress)에 의하여 사용자환경 등을 보호할 중요성은 커진다.

지적재산권에 대한 여러 쟁점에 대해서는 현재 많은 판례가 집적되고 있는 상황이며, 이러한 쟁점에 관한 대표적인 입법은 저작권에 관한 1998년의 Digital Millennium Copyright Act(DMCA)와 1999년의 Anticybersquatting Consumer Protection Act(ACPA)이다.

## 제 2 절 DMCA

### 1. 서 론

컴퓨터기술과 통신기술의 급격한 발전에 기인하는 디지털 형태의 저작물은 지적재산권, 특히 저작권의 전체적인 윤곽을 변화시키고 있다. 디지털기술은 컴퓨터의 발전과 이에 의한 컴퓨터 네트워크, 곧 인터넷과 결합함으로써 더욱 더 각광을 받게 된다. 인터넷은 디지털 환경이다. 디지털기술의 향상과 전자 네트워크 또는 기타 통신기술의 급격한 발전에 의하여 저작물이 복제·배포·공연·수정되는 것을 매우 용이하게 하며 그 속도도 급속도로 증가시키고 있다. 모뎀 등에 의하여 인터넷에 접속할

수 있는 자는 누구든지, 그리고 전세계 어느 곳으로든지 이미지, 텍스트, 사운드 등을 배포할 수 있다. 예컨대 디지털화된 저작물의 복제물을 수백만명에게 순식간에 용이하게 전송시킬 수 있으며, 원거리에 있는 컴퓨터나 네트워크에 복제물을 올림으로써 역시 수많은 사람들이 저작물이 공연되는 것을 시청할 수 있으며, 원거리에 있는 컴퓨터나 네트워크로부터 복제물을 간단하게 다운로드받을 수 있게 된다.

요컨대 디지털기술과 통신기술이 결합함으로써 저작물의 유포가 상대적으로 간단하고 신속하게 이루어지며, 어느 누구든지 일반인들에게 저작물을 보급하고 공표할 수 있으며, 인터넷상으로 전송되는 복제물의 질적인 면이 원저작물과 사실상 구별될 수 없을 정도로 동일하며, 인터넷상으로 공표하는 것에 대해서는 거의 비용이 소요되지 않으며, 이용자들도 인터넷상으로 용이하고 저렴하게 저작권이 있는 자료를 획득할 수 있다. 따라서 디지털 저작물과 인터넷으로 인하여 저작물의 복제권, 배포권, 전시권, 공연권 등이 매우 용이하게 침해될 수 있고, 따라서 저작권자가 복제물의 판매에 초점을 맞추기보다는 디지털형태로 된 저작물이 있는 컴퓨터시스템에 접속하는 것을 통제하고자 하는 것은 여기에 기인하는 것이다.

Digital Millennium Copyright Act of 1998(DMCA)은 이러한 디지털환경에 의하여 야기되는 저작권법상의 쟁점을 처음으로 해결하기 위한 것이다. DMCA는 크게 다섯 부분으로 이루어져 있는데, Title Ⅰ은 WIPO 저작권협약(WIPO Copyright Treaty)과 실연음반조약(WIPO Performances and Phonogram Treaty)을 이행하기 위한 것이며, Title Ⅱ는 온라인서비스 제공업자(Online Service Provider, OSP)의 책임제한에 관한 것이며, Title Ⅲ는 MAI Systems Corp. v. Peak Computer, Inc. 케이스에 대한 반응으로서 컴퓨터의 수리와 관련하여 저작권의 침해를 면제하는 입법이며, Title Ⅳ는 도서관을 위한 일시적인 녹음, 원거리교육 등에 관한 것이며, Title Ⅴ는 선체디자인의 보호에 관한 것이다.

## 2. 기술조치

### (1) 기술적인 조치의 의의 및 보호

디지털환경하에서 저작권자는 디지털형태로 된 저작물을 보호하기 위하여 광범위한 기술적인 조치(technical measures)를 취하게 마련이다. 기술적인 조치는 저작물의 복제물이 저작권자의 허락없이 복제, 전송, 배포되는 것을 방지할 수 있다. 기술적인 조치의 예로서는 암호화, SCMS (serial copy management systems), 디지털 워터마크(digital watermark),[13] 디지털 서명(digital signature), 비밀번호(password), 비밀번호가 정확한 것인지 확인하기 위한 프로그램 등을 들 수 있다. 기술적인 조치는 저작권의 침해를 방지하는 데 기여할 수 있으나, 기술적인 조치만으로서는 저작권이 충분히 보호될 수 없다. 우선 다른 종류의 기술을 사용함으로써 저작권을 보호하기 위한 기술적인 조치를 우회하여(bypass) 저작권을 침해할 수 있기 때문이다. 그러므로 저작물을 보호하는 기술적인 조치를 우회하거나 무력화시키는 기술을 불법화함으로써 기술적인 조치를 보호할 필요성이 있게 된다. 그러므로 기술적인 조치의 보호에 관한 발상은 ①디지털 형태의 내용물(디지털 저작물 또는 디지털 콘텐츠)을 보호하기 위하여 암호화와 같은 기술이 사용되면, ②이 기술을 해제하여 저작권을 침해하는 것이 필연적으로 수반되고, ③따라서 침해를 가능토록 하는 이러한 기술을 규제할 필요성이 있다는 것에 시작된다. 곧 기술적인 조치의 보호는 끊임없이 그리고 신속하게 행하여지는 기술적인 진보들간에 법이 개입하여 저작권을 보호하고자 하는 것이다.

정보화사회에 있어서 가장 중요한 상품은 디지털 콘텐츠(digital contents, 곧 저작물)와 이러한 디지털 콘텐츠에 접속하고 이를 전송시키는 기술 두 가지를 들 수 있다. 이러한 기술과 콘텐츠는 상호 의존관계에 있다. 곧 기술이 존재하지 않는다면 콘텐츠는 신속하게 전송될 수 없으며, 좋은 품질의 콘텐츠가 존재하지 않는다면 기술에 대한 수요도 감소할 것이다. 온라인상의 산업이 증가하면서 기술과 콘텐츠는 전자상거래

13) 암호화, SCMS, 디지털 워터마크에 대해서는 CMI에 관한 제9절 참조.

시장의 성공을 좌우할 수 있는 주요한 요소로 떠올랐다. 그러나 기술과 콘텐츠간에는 인터넷상에서의 규범을 제정하는 데 있어서 긴장관계가 형성되기도 한다. 제1절 제3관에서 논한 바와 같이 디지털 기술에 의하여 디지털 정보는 쉽게 복제되고 수정될 수 있고, 따라서 저작권에 의한 보호의 효과를 감소시킨다. 그러므로 자신의 저작물을 보호하기 위하여 저작권법에 의존하는 정보 제공업자(content provider, CP)는 디지털 기술의 진보에 대하여 점점 더 염려를 할 수밖에 없다. 이에 반하여 기술을 개발하는 회사들은 콘텐츠에 저렴하고 신속하게 접근하고 이를 전송하는 기술제품을 새로이 개발하고자 한다.

콘텐츠 제공자가 미국의 할리우드(미국의 영화산업)로 대표된다면 기술을 개발하는 회사들은 실리콘밸리로 대표된다. 이와 같이 서로 상반되는 이해관계를 가진 양자가 싸움을 벌이는 분야 중의 하나가 바로 기술적인 조치의 보호이다. 할리우드측(할리우드 및 저작권자)은 ①저작권을 보호하기 위하여 저작권자가 사용하는 기술조치를 좌절시키는 행위 및 ②저작권자의 기술조치의 좌절을 용이하게 하는 다른 기술을 강력하게 금지시킬 것을 주장한다. 이에 반하여 실리콘밸리측(기술개발자, 저작물 이용자, ISP)은 광범위한 금지를 반대하면서, 역분석(reverse engineering), 컴퓨터의 안전성 검사, 암호화 연구 등을 위한 저작물의 합법적인 이용에 대한 악영향을 끼칠 것이라고 주장한다. 따라서 기술적인 보호조치에 대한 입법은 저작권자와 기술개발자 또는 저작권자와 저작물의 이용자간의 한판 대결의 장이 될 수밖에 없다. 따라서 이러한 입법을 하는 데 있어서는 양자의 이해관계가 정교하게 균형이 이루어지도록 해야 한다. 미국의 DMCA에 있어서는 저작권자 측이 승리한 것으로 평가되고 있는데, DMCA가 전자상거래를 위한 "예측가능한, 최소한도의, 일관된, 간결한" 법적 환경요소가 될 수 없다는 비판[14]이 행하여지는 것도 바로 이같은 사실에 기인하는 것이다.

1996년의 WIPO 외교회의에서 처음으로 국제무대에 등장한 것으로서는 저작권 관리정보와 기술적인 조치(technical measure)의 보호였

14) Pamela Samuelson, Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised, 14 BERKELEY TECH. L. J. 519, 524 (1999).

다. 저작권을 보호하기 위한 기술조치를 좌절시키는 기술이나 서비스를 규제하기 위한 국제적인 규범을 세우는 것이 WIPO 외교회의에서의 미국의 중요한 디지털 의제였다. 기술조치에 관한 논의는 주로 미국의 영화산업으로부터 나온 것이라고 할 수 있다. 미국의 영화산업은 기술적인 조치에 관한 입법을 하는 데 실패하였으나, 클린턴 행정부의 NII(National Information Infrastructure)에 의하여 입법화시킬 수 있는 기회를 가지게 되었다. 콘텐츠 소유자들도 디지털 콘텐츠의 보호문제를 해결하기 위하여 기술조치를 좌절시키는 기술(circumvention technology)의 강력한 규제를 찬성하게 되었다.

각 국가간의 최종적인 타협에 의하여 성립한 WIPO 저작권협약 제11조는 "체약당사국들은 본 조약과 베른협약에 따라 저작자가 권리를 행사하는 것과 관련하여 저작자가 사용하는 효과적인 기술조치와, 저작물에 관하여 저작자가 허락하지 않거나 법이 허용하지 않는 행위를 제한하는 효과적인 기술조치를 좌절시키는 것에 대하여 적절한 법적 보호와 효과적인 법적 구제수단을 제공하여야 한다"고 규정하고 있다. 미국은 DMCA에 의하여 WIPO 저작권협약의 기술조치에 관한 사항을 이행하고자 하였다.

(2) DMCA의 주요 규칙

DMCA에 의하여 새로이 규정된 미국 저작권법 제1201조는 기술조치에 관하여 기본적으로 세 가지로 규정하고 있다. 곧 (ⅰ) 저작물에 대한 접근을 방지하기 위한 기술조치를 좌절시키는 '행위'가 금지되며[1201(a)(1)(A)], (ⅱ) '접근을 통제하는 기술조치'를 좌절시키는 기술 등이 금지되며[1201(a)(2)], (ⅲ) '저작권자의 권리를 보호하는 기술조치'를 좌절시키는 기술 등이 금지된다[1201(b)(1)]. 이러한 규정은 기본적으로 ① 저작물에 대한 '접근을 통제'하는 기술조치에 관한 것[1201(a)(1)(A)과 ②'저작권을 보호'하는 기술조치에 관한 것[1201(a)(2), 1201(b)(1)]으로 구분되며, 다른 한편으로는 ①기술조치를 좌절시키는 '행위'의 금지에 관한 것[1201(a)(1)(A), 1201(a)(2)]과 ②기술조치를 좌절시키는 '기술'의 금지에 관한 것으로 구분된다.

미국 저작권법 제1201조의 기본구조

| 기 본 규 정 (X) | 거 래 의 금 지 (Y) |
|---|---|
| A: 접근을 통제하는 기술조치를 좌절시키는 행위의 금지(1201(a)(1)) | A′: 접근을 통제하는 기술조치를 좌절시키기 위한 기술 등의 거래금지(1201(a)(2)) |
| B: | B′: 추가적인 위반: 저작권을 보호하기 위한 기술조치를 좌절시키기 위한 기술 등의 거래금지(1201(b)) |

위의 도표에서 볼 수 있는 바와 같이 X는 기본적인 위반을 나타내는 것이고 Y는 이러한 기본적인 위반을 보충하기 위하여 X의 위반을 도와주는 자들에 대한 것이다. 그런데 저작물에 대한 접근을 통제하는 기술조치를 좌절시키는 행위를 금지하는 기본규정(A)과 이를 보충하는 거래의 금지규정(A′)이 있으나, 저작권을 보호하기 위한 기술조치를 좌절시키는 경우에는 거래의 금지에 관한 보충적인 규정(B′)만이 존재하고 이에 대한 기본규정(B)은 존재하지 않는다. 이것은 무엇을 의미하는가? B는 전통적인 저작권법의 영역에 해당하는 것으로서 이를 새로이 금지시킬 필요성이 존재하지 않는다. 그러나 A는 저작권법상 존재하지 않았던 것으로서 좌절시키는 행위는 불법이 아니었고, 따라서 이를 금지하는 기본규정(A)이 필요하게 되고 행위에 대한 이러한 금지를 보충하는 규정(A′)이 필요하게 된다.[15]

이와 같이 행위 및 기술의 거래를 금지시키는 것은 재산권의 보호 및 이에 대한 제한사유와 밀접한 관련이 있다. 우선 미국 저작권법 1201조는 타인의 성에 침입하기 위하여, 곧 타인의 저작물에 허락을 받지 않고 접근하기 위하여 기술적인 보호조치를 좌절시키는 것 자체를 허용하지 않고 있다. 이러한 금지에 대하여 1201조는 여러 예외를 허용하고 있다. 일단 성내에 적법하게 들어온 경우, 곧 저작물을 적법하게 획득한 경우,

15) Report of the Senate Comm. on the Judiciary, S. Rep. No.105-190, at 12 (1998)

저작물을 공정이용하는 것과 같이 적법한 행위에 따라 보호조치를 좌절시킬 수 있다.

1) 접근을 방지하기 위한 기술조치를 좌절시키는 '행위'의 금지

DMCA는 저작물에 접근하는 것을 통제하는 기술조치를 좌절시키는 행위를 금지하고 있다[1201(a)(1)(A)]. 이 규정은 주거에 침입하여 절도하는 것과 같이 저작물의 복제물을 획득하기 위하여 기술조치에 의하여 잠겨진 방에 전자적으로 침입하는 것과 마찬가지이다. 따라서 저작물 자체에 대한 접근을 봉쇄하는 것으로서 사실상 저작권의 침해는 아니다. 이로써 저작물을 공정하게 또는 사적으로 이용할 수도 없으며 일반인에 공유영역에 있는 저작물도 이용할 수 없게 된다.

접근통제에 관한 기술조치의 좌절금지에 관한 조항은 DMCA 이후 2년 후, 곧 2000년 10월 28일에 발효하기로 규정되어 있다[1201(a)(1)(A)]. 또한 이 조항은 일정한 유형의 저작물에 대해서는 그 적용을 제외시키고 있다[1201(a)(1)(B)]. 곧 이러한 유형의 저작물 이용자가, 접근통제에 관한 기술조치의 좌절을 금지시킴으로써, 침해가 되지 않는 저작물을 이용할 수 없게 되는 경우에는 그 저작물에 대해서는 좌절금지에 관한 조항이 적용되지 않는다. 이것은 좌절금지에 관한 조항에 의하여 저작권자에게 새로운 권리가 부여되는만큼 저작권자 및 저작물 이용자에게 상당한 영향을 주고, 저작물의 정당한 이용이 제한되지 않도록 하기 위한 것이다.

DMCA는 어떠한 저작물이 좌절금지에 관한 예외에 해당하는가에 관하여 규정하고 있지 않은데, 이에 대하여 DMCA는 DMCA 발효후 2년 동안 Librarian of Congress가 Register of Copyrights의 권고에 따라 이에 따른 결정을 하도록 하고 있다[1201(a)(1)(C)]. 이에 따라 2000년 10월 27일 저작권을 담당하는 의회도서관(Library of Congress)은 예외와 관련되는 규칙[16]을 발표하였고, 이 규칙에 의하여 예외에 해당하는 저작물로서 (i) 여과 소프트웨어 응용프로그램(filtering

16) Library of Congress, Copyright Office, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201, 65 Fed. Reg. No.209 (Oct. 27, 2000).

software applications)에 의하여 봉쇄된 웹사이트의 목록으로 구성된 편집물과 (ii) 오작동·손상·폐기 등에 의하여 접근을 허용하지 못하는 접근통제 메커니즘에 의하여 보호되는 어문저작물(컴퓨터프로그램 및 데이터베이스 포함)이 지정되었다.

2) 기술조치를 좌절시키는 '기술 등'의 금지

**가) 접근을 통제하는 기술조치**

DMCA는 접근을 통제하는 기술적인 조치를 좌절시키기 위하여 사용되는 기술이나 제품, 또는 서비스를 제작하거나 이용가능하게 하는 것을 금지시키고 있다[17 U.S.C.§1201(a)(2)]. 곧 [1](i) "저작물에 대한 접근을 효과적으로 통제하기 위한 기술조치"를 좌절시킬 목적으로 '주로(primarily)' 디자인 또는 생산되거나, (ii) 기술조치를 좌절시키는 것 이외에는 상업적으로 제한적인 목적이나 유용성을 가지거나, (iii) 기술조치를 좌절시키기 위한 이용을 알고 있는 자에 의하여 또는 이러한 자와 협력하는 타인에 의하여 상업화된, [2] 기술, 제품, 서비스, 도구, 구성요소(component), 또는 그 부품을 [3] 생산, 수입, 일반인에게 제공, 공급, 기타 거래하는 것은 금지된다[17 U.S.C.§1201(a)(2)].

기술조치를 좌절시키는 기술 등의 거래를 금지시키는 이 규정과 1201(b)(1) 규정은 침해를 목적으로 하거나 침해 이외에는 상업적인 중요성이 제한되어 있는 기술이나 도구 등을 금지함으로써, 저작권자를 보호하는 동시에 여러 가지의 목적이 있는 합법적인 도구 등은 계속 생산·판매되도록 하기 위한 것이다. 따라서 상업적으로 중요한 것으로서 침해가 되지 않는 소비자용 전자제품, 통신 또는 컴퓨터 제품 등은 금지되지 않는다.

**나) 저작권자의 권리를 보호하는 기술조치**

(a)(2)와 마찬가지로 (i) "저작권자의 권리를 효과적으로 보호하기 위한 기술조치"를 좌절시키기 위한 목적으로 '주로' 디자인되거나 ..., (ii) 기술조치를 좌절시키는 것 이외에 ..., (iii) 기술조치를 좌절시키기 위한 이용을 ...상업화된, 기술 ... 등을 생산 ... 기타 거래하는 것은 금지된다[17 U.S.C.§1201(b)(1)].

(3) 기술조치 및 좌절의 개념

DMCA는 접근을 통제하는 기술조치와 저작권자의 권리를 보호하는 기술조치에 대하여 기술조치 및 기술조치의 좌절(circumvention)의 개념을 각각 달리 규정하고 있다. 우선 저작물에 대한 접근을 통제하는 기술조치와 관련하여 '접근을 통제하는 기술조치'는 저작물에 접근하기 위하여 저작권자의 허락을 얻어 정보나 과정 또는 처리(treatment)를 적용시키도록 하는 것으로 정의하고 있다. '기술적인 조치를 좌절시킨다는 것'은, 저작권자의 허락없이, 암호화된 저작물을 해독하거나, 기타 기술적인 조치를 회피, 우회(bypass), 제거, 무력화(deactivating) 또는 손상시키는 것으로 정의되고 있다[1201(a)(2)].

저작권자의 권리를 보호하는 기술조치와 관련하여, '기술조치'는 저작권자의 권리행사를 방지하고 억제하고 기타 제한하는 것이며, '기술적인 조치를 좌절시킨다는 것'은 기술조치를 회피, 우회, 제거, 무력화, 기타 손상시키는 것으로 정의하고 있다[1201(b)(2)(A)(B)].

(4) 기술조치를 좌절시키는 행위의 금지에 대한 예외규정

DMCA의 원래의 초안은 '법을 집행하거나 첩보 목적'으로 기술적인 보호조치를 좌절시키는 것을 허용하였다. 그러나 정보산업 관련 기업이나 단체들은 이에 의하여 많은 합법적인 행위들도 불법화될 것이라고 주장하였다. 암호를 위한 연구나 컴퓨터의 안전성 시험은 디지털 경제가 추구하는 목표를 수행하는 데 있어서 중요한 역할을 한다. 그러나 DMCA의 원래의 초안에 의하면 이같은 암호연구나 컴퓨터 안전성 시험은 불법이 된다. 이에 따라 미국 의회는 기술적인 보호조치를 좌절시키기 위한 합법적인 이유가 많이 있다는 것을 인식하였고, DMCA 법률안은 '기술조치를 좌절시키는 행위(act of circumvention)'에 관한 여러 예외를 규정하기에 이르렀다. 이러한 예외조항에 따라 DMCA는 더욱 더 복잡하게 되었으나 디지털경제가 성장하는 데 있어서는 좌절을 금지시키는 조항이 가지는 폐해는 줄어들게 되었다.

1) 공정이용의 원리

제1201조는 저작권법상의 권리, 구제수단, 권리의 제한, 공정이용을 포함한 방어수단에 영향을 미치지 않는다[1201(c)(1)]. 접근 및 복제라는 행위와 관련하여, 1201조는 접근을 방지하기 위한 기술조치를 좌절시키는 것은 금지시키지만, 복제를 방지하기 위한 기술조치에 대해서는 그렇지 않다. 이것은 일반인들이 저작물을 계속 공정이용할 수 있다는 것을 보장하기 위한 것이다. 곧 저작물의 복제는 일정한 경우 공정이용이 될 수 있으므로 복제를 방지하기 위한 기술조치를 좌절시키는 행위는 금지시키지 않는 것이다. 그러나 접근을 방지하기 위한 기술조치를 좌절시키는 행위는 금지되므로, 공정이용의 원리는 저작물에 허락없이 접근하는 행위에 대해서는 방어수단이 되지 않는다. 예컨대 저작권자가 저작물의 복제물에 기술적인 보호조치를 취하였는데 이 복제물을 정당하게 획득한 경우, 이 기술조치를 좌절시키는 것에 대해서는 공정이용의 원리가 적용될 수 있게 된다.

2) 비영리 도서관, 기록보존소, 교육기관에 대한 예외

공정이용의 원리가 여전히 적용되더라도 도서관이나 비영리 그룹들은 기술조치에 관한 규정으로 인하여 일반인의 정보에 대한 접근이 영향받을 것을 염려하였다. 이에 따라 비영리 도서관, 기록보존소, 교육기관 등에 대해서는 상업적으로 이용되는 저작물에 접근하는 예외가 허용되었다[1201(d)]. 이 예외는 그 저작물을 구입할 것인지를 선의로 결정하기 위한 경우에만 저작물에 접근할 수 있으며 다른 수단에 의하여서는 저작물을 획득할 수 없는 경우에 한정된다.

3) 컴퓨터 및 소프트웨어 산업에 대한 예외

DMCA 입법초기에 컴퓨터 및 소프트웨어 산업은 기술조치의 규정에 대한 예외를 규정하기 위하여 의회를 설득하는 데 실패하였다. 상·하원 각 위원회가 법안을 심리하기 시작하여서야 컴퓨터 및 소프트웨어 산업이 염려하던 것에 관심을 기울이기 시작하였다. 이에 따라 세 가지 예외

가 규정되기에 이르렀다. 첫째, 소프트웨어 개발업자가 컴퓨터 프로그램 간에 호환성을 획득하기 위하여 기술조치를 좌절시키는 예외가 허용되었다[역분석, 1201(f)]. 둘째, 전자제품 등의 제조업자가 제품의 디자인을 기술적인 조치에 부합하도록 할 의무가 없다[1201(c)(3)]. 셋째, 기술, 제품, 서비스, 도구, 구성요소 등과 관련하여 제1201조에 의하여 기여책임 내지 대위책임을 확대하거나 축소되지 않는다[1201(c)(2)]. 넷째, 컴퓨터나 컴퓨터 시스템의 안전성 시험(security test)은 접근금지에 대한 규정의 위반이 되지 않는다.

4) 하원 상무위원회에 의한 예외

DMCA를 입법하는 데 있어서 하원 상무위원회가 관여하였고, 이에 의하여 새로운 예외조항이 추가되었다. 이러한 예외는 디지털 경제관련 기업 및 도서관, 교육기관 및 기타 비영리 그룹이 제기한 염려에 대한 것이었다. 우선 암호화연구에 대한 예외가 인정되었으며[1201(g)], 소비자와 관련된 두 개의 예외, 곧 청소년 보호에 관한 예외[1201(h)] 및 프라이버시를 보호하기 위한 예외[1201(i)]가 규정되었다. 이러한 예외조항들은 디지털경제 관련기업들의 염려를 완화시키기 위한 것이었지만, 그 범위가 너무 협소하다고 비판받고 있다. 따라서 현재 규정된 것 이외의 합법적인 목적을 위하여 좌절시키는 것도 허용되고 더 광범위한 예외를 인정하기 위하여 법을 개정할 필요가 있다는 주장이 제기되고 있다.[17]

### 3. 온라인서비스 제공자의 책임

(1) 온라인서비스 제공자의 의의

인터넷 서비스제공업자(Internet Service Provider, ISP)는 모뎀(modem)에 의하여 인터넷과 연결된 컴퓨터 또는 컴퓨터 네트워크에 접속시켜주는 자, 곧 인터넷에 접속시켜주는 자를 의미한다. 인터넷에 대

17) Pamela Samuelson, *Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need To Be Revised*, 14 BERKELEY TECH. L. J. 519, 537-38 (1999).

한 직접적인 접속은 많은 비용이 소요된다. 따라서 직접 접속은 정부, 대규모업체, 대학 등에 한정되며, 개인이나 소규모업체는 ISP를 이용하게 된다. ISP는 접속에 대하여 요금을 부과하는 상업업체이지만 무료 또는 저렴한 가격으로 인터넷에 접속하도록 하는 비영리기관도 있다. ISP는 콘텐츠 제공자 및 온라인 서비스제공업자와 구별된다. 콘텐츠 제공자(Content Provider, CP)는 인터넷상에서 콘텐츠를 송신하고 타인이 이용할 수 있도록 하는 자로서, 콘텐츠 제공자는 전자우편, 뉴스그룹, 대화방 등을 이용함으로써 인터넷에 접속할 수 있는 자라면 누구든지 CP가 될 수 있다. 또한 CP는 자신의 서버를 운영할 필요도 없으며 타인의 서버 공간을 빌리거나 온라인 서비스(online service)를 이용하여 홈페이지를 만듦으로써 CP가 될 수 있다. 그러나 저작권법과 관련하여 논의되는 CP는 주로 자신의 서버를 운영하면서 콘텐츠를 타인이 검색하여 이용할 수 있도록 하기 위하여 콘텐츠를 인터넷에서 이용가능하게 하는 자, 특히 인터넷상에서 상업적으로 콘텐츠를 판매하는 자를 의미한다. 온라인 제공업자(Online Service Provider, OSP)는 인터넷에 대한 접속 및 전자우편, 대화방, 검색엔진, 콘텐트 등의 온라인 서비스를 가입자(subscriber, 이용자)에게 제공하는 자이다. OSP는 자신의 네트워크상에서 자신의 콘텐츠를 제공할 뿐만 아니라 인터넷상의 더 많은 자원(resoruces)으로 연결시켜주기도 한다. 따라서 OSP는 ISP 및 CP보다 넓은 개념으로서, OSP는 동시에 OSP 및 CP가 되는 것이 일반적이다.

(2) OSP 책임의 문제점

OSP는 일정한 콘텐츠(contents)를 제작하여 가입자가 이를 이용될 수 있게 하거나 제3의 서버에 접근할 수 있는 도구로서 역할을 한다. 일반적으로는 양자의 기능을 모두 행하는 것이 원칙이다. 또한 이러한 기능과 관계없이 OSP는 통신시설의 네트워크를 만들어 운영하거나, 네트워크가 운영될 수 있는 소프트웨어를 작동시키거나, 가입자에게 인터넷에 접근을 시켜주는 등 체계상의 기능(system function)을 수행하고 있다. 이러한 역할이나 기능과 관련하여 OSP가 저작권법상 어떠한 책임을 질 것인지 쟁점이 되고 있다.

우선 저작권과 관련된 OSP의 책임을 논하기 위해서는 OSP를 통하여 온라인 서비스를 이용하는 자(subscriber)의 행위를 논하여야 한다. OSP의 가입자들은 OSP가 제공하는 서비스에 의하여 인터넷에 접속할 뿐만 아니라 전자우편, 대화방, 홈페이지나 BBS를 운영할 수 있다. 인터넷환경 또는 디지털환경하에서는 이들 OSP 가입자들, 곧 인터넷 이용자들에 의하여 저작권은 매우 용이하게 침해된다. 이들 가입자들은 저작권법을 알지 못하거나 자신의 저작권 침해가 밝혀지지 않을 것이라고 생각하여 저작권을 의도적으로 침해하기도 한다. 예컨대 저작권으로 보호되는 타인의 자료를 BBS나 대화방에 올리거나, 자신의 홈페이지에 올려놓거나, 전자우편에 의하여 송신하는 경우, 이들이 저작권을 직접 침해한다는 데에는 이론(異論)이 있을 수 없다. 또한 인터넷상에서 저작물을 다운로드받는 것도 저작권의 침해가 되는 것은 당연하다. 미국음반협회(RIAA)가 인터넷상에서 무료 MP3 파일을 배포하는 웹사이트 운영자에게 배포를 금지하라고 개별적으로 통지하거나 직접 소송을 제기하는 등 저작권자들은 이들 가입자들로부터 저작권 침해를 방지하기 위한 노력을 한다. 그러나 저작권을 침해하는 자(저작물을 인터넷에 올리는 자)의 신원은 보통 익명이며, 저작물을 받아봄으로써 저작권을 다시 침해하는 자의 숫자도 무수히 많고 전세계 각지에 소재하게 된다. 침해자의 신원이 밝혀지더라도 손해배상을 받기 위한 비용이 손해배상액보다 더 많이 소요되므로 저작권자가 직접침해자에 대하여 법적 대응을 하는 것은 비현실적이다. 요컨대 저작권자가 직접 침해자에 대하여 대응하는 것이 불가능하거나, 가능하더라도 현실적이지 못하다. 저작권자들은 인터넷상에서 침해를 방지하고 침해가 발생하는 경우에는 배상을 받기를 원한다. 저작권자들의 이러한 목적을 달성할 수 있는 방안으로 논의되는 것이 온라인 서비스를 제공함으로써 가입자의 직접적인 침해를 가능토록 한 OSP이다.

OSP의 저작권법상의 책임을 정하는 문제는 인터넷의 계속적인 발전을 위하여 해결되어야 하는 핵심적인 요소 중의 하나이다. OSP의 저작권법상의 책임은 OSP, 가입자, 기타 콘텐츠 제공자의 관여 또는 책임에 따라 결정되는 복잡한 문제이다. 또한 OSP의 책임을 정하는 것은 전자적

인 전송을 감시해야 하는 실무상·기술상의 어려움도 포함하는 문제이다. 저작권의 침해와 관련하여 OSP가 저작권이 있는 저작물을 직접 인터넷에 올려놓는 경우 OSP가 저작권 침해에 대하여 책임을 진다는 것은 아무런 문제가 되지 않는다. 그러나 OSP의 가입자가 저작물을 인터넷에 올려놓는 경우 가입자의 행위에 대하여 OSP가 책임을 질 것인가에 대해서는 문제점이 발생할 수밖에 없다.

OSP가 가입자의 저작권 침해에 기하여 책임을 부담하여야 하는가에 대해서는 저작권자와 OSP간에 상당한 논란이 되고 있다. 저작권자들은 온라인상의 저작권 침해에 대하여 OSP에게 책임을 강력하게 부과하는 것을 희망한다. 첫째, 공정이용이나 기타 저작권에 대한 제한이 적용되지 않는 경우 저작권자들은 인터넷에서 저작물의 배포를 금지시키고 저작물의 이용에 대한 합리적인 이익을 얻어야 한다는 것이다. 저작권자들은 저작물이 인터넷상에서 적절하게 보호되지 않고 저작물에 대하여 통제할 수 없다면 새로운 저작물을 창작할 동기를 가지지 않게 되어 저작물은 감소될 것이므로, 결국 일반인에게 지식을 전달하는 것이 방해될 것이라고 주장한다.

둘째, 저작권자들은 OSP가 OSP의 네트워크에서 저작권의 침해를 통제할 수 있다고 주장한다. 곧 OSP는 저작권 침해를 통제하기 위하여 서면으로 된 OSP의 방침(policy)이나 가이드라인을 이용할 수 있고, 이러한 방침 등을 설명하는 경고를 할 수 있으며, 하드웨어나 소프트웨어를 이용하여 저작권을 침해하는 자료가 올려졌는지를 결정할 수 있으며, OSP의 시스템에서 발생하는 저작권 침해행위를 가장 잘 통지받을 수 있으며, 저작권 침해행위를 신속하게 중지시킬 수 있는 지위에 있다는 것이다.

마지막으로, 저작권자들은 OSP가 책임을 부담하더라도 온라인상 이용될 수 있는 정보에 대하여 부정적인 영향을 주지 않는다고 주장하였다. 엄청나게 증가하고 있는 인터넷 이용자의 숫자를 고려하면 OSP도 인터넷 성장의 수혜자이고 따라서 가입자의 침해행위에 대하여 책임을 부담하여야 한다고 주장한다.

OSP는 저작권법상의 책임과 관련하여 가입자의 침해행위로 인하여 책임을 부담하지 않거나 부담하더라도 제한적이어야 한다고 주장한다.

곧 침해가 의도적이고 반복되는 경우 또는 침해행위를 실제로 알고 있었고 그러한 행위를 중지시킬 수 있는 능력과 권한을 가지는 경우에만 책임을 부담하여야 한다고 주장한다. 이의 근거로서 첫째, OSP가 인지 또는 통제하지 못하는 저작권 침해자료들에 대하여 무제한적인 책임을 부담한다면 온라인에 의한 서비스산업은 와해되고 따라서 인터넷의 성장은 마비된다고 주장한다. 따라서 저작권의 침해를 실제로 알고 있었고 저작권을 침해하는 자료를 제거할 수 있었으나 제거하지 않은 경우에만 책임을 부담하여야 한다고 주장한다. 또한 OSP에게 엄격책임을 부과하는 것은 OSP의 시스템을 통과하는 정보의 내용을 OSP가 감시할 수 있는 동기를 제공하지만, 이것은 프라이버시와 OSP가 제공하는 서비스에 대한 접근을 손상시킨다고 주장한다. 그리고 OSP의 시스템에서 수많은 전송이 이루어지는데 이를 OSP가 감시한다는 것은 비현실적이며, 저작권을 침해하는 자료를 파악해내는 것이 항상 가능한 것은 아니라고 주장한다.

둘째, OSP는 디지털 전송을 위한 '단순한 도구(mere conduit)', 곧 수동적인 전달자에 불과한 것이고 이것은 전화회사와 유사하다는 것이다. 따라서 전화회사가 저작권침해에 대하여 책임을 부담하지 않듯이 OSP도 저작권 침해책임으로부터 면제되어야 한다고 주장한다. 또한 저작권 침해에 대하여 OSP에게 엄격책임을 부담시키면 영업을 하기가 어렵게 되며 따라서 인터넷에서 이용될 수 있는 정보가 감소할 것이라고 주장한다.

마지막으로 OSP는 자신들의 시스템에서 행하여지는 대부분의 행위를 알지 못하거나 통제하지 못하는 경우에 그러한 행위에 책임을 지우는 것은 불공정하다고 주장한다. 이들은 저작권을 침해하는 팩스가 전화선으로 송신되는 경우에 전화회사가 엄격하게 책임을 지지 않는다는 것을 지적하며, OSP에게 책임을 지운다면 이것은 고속도로의 소유자에게 고속도로에서 발생하는 범죄행위에 대하여 책임을 지우는 것과 같다고 주장한다. 따라서 OSP가 침해행위를 알고 있으며 이를 제지시킬 수 있는 능력이 있는 경우에만 저작권에 대한 책임을 져야한다고 주장한다. 또한 OSP의 시스템을 통과하는 수많은 송신을 감독할 수 없으며 어느 가입자가 침해

하였는지 그리고 침해가 어느 곳에서 행하여졌는지를 알아내는 것을 불가능하므로 OSP에게 책임을 지우는 것은 실현불가능한 것이라고 한다.

(3) DMCA의 기본구도

미국 저작권법에서 OSP의 책임을 규정한 조항은 제512조인데, 이 조항은 1998년의 DMCA에 의하여 추가된 것이다. 제512조는 기본적으로 OSP가 OSP의 정의 규정에 해당하고 저작권자가 저작물을 보호하기 위한 일정한 법적 요건을 충족하는 한도에서 OSP의 책임을 면제해 주고 있다. 따라서 DMCA는 디지털 네트워크 환경에서 OSP와 저작권자가 협력하여 저작권 침해를 탐지하여 이에 대하여 대처하도록 하는 동기를 제공하려는 것이다. OSP의 입장에서 본다면 OSP가 자신의 시스템에서 행하여지는 저작권의 침해를 방지하고 침해과일을 제거할 동기를 제공한다. 이 규정은 OSP의 네트워크에 올려져 있는 자료에 대한 OSP의 직접, 기여, 대위책임과 관련하여 통신산업과 콘텐츠 제공산업간의 타협을 반영하는 것이다.

제512조는 OSP의 침해책임이 면제되는 네 가지 경우(safe harbour)를 규정하고 있다[512 (a), (b), (c), (d)]. OSP는 이 규정에 의하여 1차적으로 침해에 대한 방어를 할 수 있으며, 이에 해당하지 않는 경우 공정이용 등과 같은 일반적인 저작권법상의 방어수단을 이용할 수 있다. 또한 네 가지 면제조항에 해당하지 않는 경우에도 OSP가 침해책임을 지기 위해서는 저작권법상의 침해요건을 갖추어야 한다. OSP가 네 가지 중의 면제조항에 해당하면 직접, 기여, 대위침해에 기인한 금전적인 손해배상책임을 지지 않으며, 원칙적으로 금지명령도 제한된다[512(j)]. OSP가 이러한 보호를 받기 위해서는 OSP의 정의에 해당하여야 하며[512(k)] 보호를 받기 위한 요건에 해당하여야 한다[512(i)].

(4) 책임이 면제되는 경우

OSP의 책임이 면제되는 경우는 (ⅰ) 네트워크상에서의 수동적인 디지털통신, (ⅱ) 네트워크상에서의 임시적이며 중간과정의 저장, (ⅲ) 이용자

에 의한 자료의 저장 및 (iv) 정보검색의 제공에 대한 면제 등이다. 면제되는 책임의 내용은 저작권 침해에 대하여 ①'손해배상책임, 소송비용, 변호사비용, 기타의 형태의 금전적인 지급'의 면제와, ②원칙적으로 '금지명령(injunction) 등 기타 공평법상의 구제수단(equitable relief)'의 면제이다.

1) 네트워크상에서의 수동적인 디지털통신[512(a)]

(i) OSP의 시스템이나 네트워크(법문상으로는 OSP에 의하여 통제·운영되거나 OSP를 위하여 통제·운영되는 시스템이나 네트워크)를 통하여 자료를 전송(transmitting), 전송연결(routing), 연결시켜 주거나, (ii) 이러한 전송, 전송연결, 연결 과정에서 자료를 즉각적이며 일시적으로(immediate and transient) 저장하는 것에 대해서는 책임이 면제된다.

이러한 책임이 면제되기 위해서는 ①자료의 전송이 OSP 이외의 자에 의하여 시작되거나 지시에 의하여야 시작되어야 하며, ②전송·전송연결·연결·저장 등이 OSP가 선택하지 않고서 자동적이며 기계적인 과정에 의하여 행하여져야 하며, ③타인의 요청에 의하여 자동적으로 응답하는 것을 제외하고는, OSP가 자료의 수령자를 선택하지 않아야 하며, ④즉각적이며 일시적으로 저장하는 과정 중에 OSP가 자료의 복제물(copy)이 자료의 수령자로 기대되는 자(anticipated recipient) 이외의 자가 접근할 수 있는 방법으로 OSP의 네트워크나 시스템에 계속 남아있어서는 안되고, 자료의 수령자로 기대되는 자에 대해서도 전송 등을 위하여 합리적으로 필요한 이상의 기간동안 계속 남아있어서는 안되며, ⑤자료의 내용이 변경되지 않고 시스템이나 네트워크를 통하여 전송되어야 한다. 이러한 전제요건의 골자는 전화회사와 같이 OSP가 자료의 내용이나 수령자의 신원에 대한 통제를 하지 않는 역할만 할 것을 요구하는 것이다.

2) 네트워크상에서의 임시적이며 중간과정의 저장[512(b)]

**가) 캐싱의 의의 및 유형**

캐싱(caching)은 자주 이용되는 디지털정보(digital information)를 인터넷이라는 네트워크상의 여러 전송지점에 캐쉬(cache)라 불리는 저

장공간에 일시적으로 저장함으로써 후에 이를 다시 이용하고자 하는 경우 그 정보의 원래의 출처로 다시 갈 필요성이 없도록 하는 기술을 일컫는다. 일반적으로 캐싱은 어느 웹사이트를 후에 다시 방문하는 경우에 이용하기 위하여 그 웹사이트의 자료를 복제하여 일시적으로 저장하는 것을 의미한다. 곧 웹 페이지나 사이트를 보고자하는 이용자에게 전송하기 위하여 컴퓨터가 이를 전자적으로 저장하는 일종의 인터넷 기술이다. 캐싱은 또한 원거리에 있는 웹사이트 전부 또는 어떠한 자료의 전체적인 부분을 복제하는 관행을 일컫기도 하는 데, 이같은 형태의 캐싱은 있는 그대로의 복사 또는 반사를 의미하는 'mirroring'이라고도 불린다.

캐싱의 목적은 어떠한 데이터에 대한 반복적인 접속의 속도를 빠르게 하는 동시에 데이터의 반복적인 다운로드로 인하여 발생하는 네트워크의 혼잡을 감소시키기 위한 것이다. 예컨대 대륙간의 케이블을 사용하기 위한 비용이 高價이고 많은 수요에 따른 병목현상으로 인한 지연으로 인하여 정보가 어느 국가의 서버에 일시적으로 저장된다. 예컨대 미국출처의 자료를 찾는 경우 그 자료는 태평양의 케이블을 통하여 국내의 서버로 전송되면, 국내의 서버는 후에 이 자료를 다시 검색하는 것에 대비하기 위하여 이를 일시적으로 저장한다. 따라서 국내 이용자가 후에 다시 이 자료를 검색하는 경우 한국의 국내 서버가 원래의 미국의 서버에 자료를 요청하지 않고 국내 서버의 캐시(cache)로부터 자료를 직접 전송하는 것이다. 이와 같이 캐싱에 의하여 정보가 전송되는 거리를 단축시키게 되며 이에 따라 병목현상으로 인한 지연을 방지할 수 있다. 캐시 서버(cache server)는 저장된 정보를 일시적으로, 예컨대 몇초, 몇일, 몇주일 또는 그 이상의 기간이 경과하면 저장한 정보를 제거하게 된다. 요컨대 캐싱은 인터넷의 핵심적인 가치, 곧 저렴하고 신속한 정보의 검색을 향상시키게 된다.

캐싱은 국제적 또는 국내적 캐싱으로 구별되기도 하지만, 저작권법상으로 문제점을 야기하는 것은 이용자의 컴퓨터에 의한 캐싱(client caching 또는 local caching)과 네트워크 서버에 의한 캐싱(proxy caching)이다. 전자는 정보를 이용자의 컴퓨터에 일시적으로 저장하는 것이다. 예컨대 이용자가 어떠한 웹사이트에 접속하고자 하는 경우 이용자의

검색프로그램(MS Explorer나 Netscape의 Navigator 등의 Web browser)은 이용자 컴퓨터의 메모리에 이용자가 요청한 '웹사이트의 복제물'이 포함되어 있는지 여부를 결정하기 위하여 이용자의 컴퓨터를 즉시 자동적으로 검색한다. 만약 그 복제물이 포함되어 있다면 검색프로그램은 그 복제물을 화면에 나타나게 해 준다. 만약 포함되어 있지 않다면 검색프로그램은 요청된 웹사이트를 인터넷으로부터 검색하여 즉시 그 복제물을 이용자 컴퓨터의 RAM에 일시적으로 저장한다.

네트워크 서버에 의한 캐싱은 ISP의 시스템과 같이 이용자에게 인터넷에 접속할 수 있도록 하는 네트워크 서버(network server, proxy server라고도 함)가 자신의 네트워크에 웹사이트의 복제물을 일시적으로 저장하는 것이다. 이용자의 컴퓨터에 의한 캐싱과 같이 이용자가 웹사이트를 요청하면, 네트워크 서버는 자신의 네트워크가 요청된 웹사이트의 복제물을 포함하고 있는지 여부를 체크한다. 포함되어 있다면 인터넷을 통하여 요청된 사이트에 접속하는 것이 아니라 자신의 시스템에 일시적으로 저장되어 있는 웹사이트의 복제물을 나타나게 해 준다. 예컨대 국내의 CP가 自社의 서버에 어느 신문사의 홈페이지를 일시적으로 저장하는 경우, 후에 다른 이용자가 이 신문을 검색하고자 한다면 신문사의 홈페이지가 아닌 CP의 서버로부터 홈페이지를 보게 되는 것이다. 포함되어 있지 않다면 인터넷을 통하여 요청된 웹사이트에 접속한 후 자신의 네트워크에 그 웹사이트의 복제물을 일시적으로 저장하며, 후에 이 웹사이트가 다시 요청된 경우 이 복제물을 나타나게 해 준다.

### 나) DMCA에 의한 면제의 요건

DMCA의 규정은 이용자가 자료에 신속하게 접근할 수 있도록 하기 위하여 시스템을 운용하는 서버(system server)가 웹사이트 자료의 복제물을 이용할 수 있게 하는 관행인 시스템 캐싱(system caching)에 관한 것이다. 또한 이 규정은 이용자간에 전달된 메시지를 일시적으로 저장하는 것과 웹사이트나 뉴스그룹(newsgroup)에 저작물을 올리는 것과 이로부터 다운로드받는 것까지도 포함하는 것으로 여겨지는 것으로서, 그 면제의 범위가 비교적 광범위하다.

이러한 면제에 해당하기 위하여 서비스 제공자는 ①자신의 시스템이나 네트워크에 저장되어 있는 자료를 수정해서는 안되며, ②일반적으로 채택된 산업계의 데이터 통신규약에 따라 자료를 타인에게 이용하도록 하는 자가 특정한 경우에는 자료를 다시 올리거나 기타 최신화하는 것에 관한 규칙을 준수하여야 하며, ③자료를 온라인상 이용하도록 한 자가 자료를 다시 회수하는 기술의 능력에 개입하여서는 안되며, ④자료를 제공하는 자가 그 자료에 대하여 접속의 조건으로서 사용료나 비밀번호 등을 부과한 경우, 그러한 조건을 충족한 자에게만 접속을 허용할 수 있어야 하며, ⑤OSP의 가입자가 저작권자의 허락없이 자료를 온라인상 이용가능하게 한 경우, 저작권 침해에 대한 통지를 받는 즉시 저작권을 침해하는 것으로 주장된 자료를 신속하게 제거하거나 이에 대한 접속을 불가능하게 하여야 한다. 다만 이 규정이 적용되기 위해서는 (ⅰ) 저작권을 침해한 것으로 주장된 자료가 원래의 사이트로부터 제거 또는 이에 대한 접속이 불가능하게 되었거나, 법원이 제거 또는 접속불능을 명하였고, (ⅱ) 통지를 하는 당사자가 '자료가 제거되었거나 접속이 불가능하게 되었거나, 법원이 자료의 제거 또는 접속불능을 명하였다'는 사실을 통지의 내용에 포함시켜야 한다.

### 다) 침해의 통지

저작권자에 의한 침해통지가 유효하기 위해서는, 통지가 서비스 제공자의 지정된 대리인에게 서명된 서면에 의하여야 하며, 저작물을 표시하여야 하며, 저작권을 침해한 것으로 주장된 자료(곧 OSP의 시스템에 있는 저작권 침해자료)를 표시하여야 하며, 침해를 주장하는 당사자를 OSP가 접촉할 수 있는 정보를 제공하여야 하며, 침해를 주장하는 당사자가 OSP의 시스템에서 이용되고 있는 저작물이 저작권자나 그의 대리인으로부터 허락을 받지 않고 사용되고 있거나 기타 법에 의하여 허용되지 않는다는 것을 선의로 믿고 있다고 언급하여야 하며, 통지된 정보가 정확하며 통지하는 당사자는 저작권자를 위하여 행위할 권한이 있다는 것을 언급하여야 한다[512(b)(2)(E), 512(c)(3)].

3) 이용자의 지시에 의한 자료의 저장[512(c)]

이 규정은 OSP의 시스템이나 네트워크에 이용자의 웹사이트가 저작권을 침해하는 자료를 담고 있는 경우, 서비스 제공자가 이를 알고 있지 않다면 책임을 면제시켜 주는 규정이다. 곧 OSP의 네트워크에 있는 자료를 이용자의 지시에 의하여 저장하는 것에 대하여 책임이 면제된다.

이러한 면제규정이 적용되기 위해서는 첫째, ①OSP의 시스템이나 네트워크에 있는 자료나 자료를 사용하는 행위가 저작권을 침해한다는 것을 실제로 알고 있어서는 안되거나, ②실제로 알고 있지 않은 경우에는 침해행위를 명확하게 나타내는 사실이나 상황을 알고 있어서는 안되거나, ③① 및 ②에 해당하는 것을 알게 되는 즉시, 신속하게 자료를 제거하거나 그 자료에 대한 접속을 불가능하게 하여야 한다. 둘째, OSP가 침해행위를 통제할 수 있는 권리와 능력을 가지는 경우, 침해행위에 직접 기인하는 금전적인 이익을 받아서는 안된다. 셋째, 저작권자에 의한 침해통지를 받으면 침해자료를 제거 또는 접속불능토록 하기 위하여 즉시 대처하여야 한다[512(c)(1)]. 통지가 유효하기 위한 요건은 위의 캐싱에서와 같다.

4) 정보검색의 제공에 대한 면제[512(d)]

이 규정은 서비스 제공자가 '정보발견도구(information location tool)'를 사용하여 저작물을 침해하는 자료나 침해하는 행위를 포함하고 있는 온라인상의 위치로 이용자를 전송시키거나 연결시키는 것에 대한 책임을 면제하는 것이다. 정보발견도구에는 목록(directory), 색인(index), 포인터(pointer) 또는 하이퍼텍스트 링크(hypertext link) 등이 포함되므로[512(d)], 링크뿐만 아니라 검색엔진(search engines), 목록나열(directory listings) 등도 포함된다. 책임이 면제되기 위해서는 침해에 대한 인지, 침해자료의 즉시 제거, 금전적인 이익 등 제512조 (c)항과 동일하며[512(d)(1)(2)], 침해에 대한 통지도 마찬가지이다[512(d)(3)].

(5) OSP의 정의

DMCA는 제512조 (a)항의 네트워크상에서의 수동적인 디지털통신에 있어서의 OSP에 대하여 "이용자가 지정한 지점간에, 송신 또는 수신되는 자료의 내용을 수정하지 않고서, 이용자가 선택하는 자료를 송신하고(transmission), 송신을 연결하며(routing), 디지털 온라인상으로 자료를 전달하는 등의 서비스를 제공하는 실체"라고 정의하고 있다[512(k)(1)(B)]. 제512조 (a)항 이외에서 언급되는 OSP는 "온라인상의 서비스나 네트워크 서비스를 제공하거나 이러한 서비스를 위한 시설을 운영하는 자이며, (a)항에서의 OSP를 포함한다"고 정의하고 있다[512(k)(1)(B)].

(6) OSP의 책임면제 자격

DMCA는 OSP가 저작권 침해를 방지 내지 경감시키기 위한 동기를 제공하기 위하여 제512조에 의하여 책임이 면제되기 위한 자격요건을 규정하고 있다. 곧 제512조에 의하여 책임이 면제되기 위하여 OSP는, 첫째 반복적으로 저작권을 침해하는 가입자에 대한 서비스를 종료시킨다는 OSP의 방침(policy)을 채택하고 합리적으로 시행하며 가입자에게 통지하여야 한다. 둘째, OSP는 저작권자의 표준적인 기술조치(standard technical measures)를 수용하고 이를 방해하여서는 안된다[512(ⅰ)(1)]. 표준적인 기술조치는 제10절 및 제11절에서 논의한 저작권관리정보 및 기술조치와 대략 일치하는 것으로서, 저작권자가 저작물을 표시하고 보호하기 위하여 사용되는 기술조치이다. 이러한 기술조치는 저작권자 및 OSP의 전반적인 합의에 따라 개발되고, 누구든지 합리적이며 비차별적인 조건으로 이용할 수 있으며, OSP에게 상당한 비용을 부담하거나 OSP의 시스템이나 네트워크에 상당한 부담을 과해서는 안된다[512(ⅰ)(2)].

(7) 자료의 제거 또는 접속불능에 대한 OSP의 책임

저작권의 침해주장이나 침해행위를 명확하게 나타내는 사실 또는 상황에 기초하여 OSP가 시스템상에서 선의로 자료를 제거하거나 접속을 불가

능하게 한 경우, 후에 저작권을 침해하지 않았다고 판명된 경우에도, OSP는 아무런 책임을 지지 않는다. 이와 같이 책임을 지지 않기 위하여 서비스 제공자는 ①저작권을 침해한 것으로 주장된 자료의 소유자에게 즉시 통지하기 위한 합리적 조치를 취하였어야 하며, ②자료의 소유자로부터 반대의 통지를 받은 경우, 저작권 침해를 통지한 자에게 이 반대의 통지를 전달하고 제거된 자료를 다시 올려놓거나 불가능하게 된 접속을 가능하게 한다고 통지하여야 하며, ③자료의 소유자로부터 반대의 통지를 받은 후 일정기간 이내에 제거된 자료를 다시 올리거나 불가능하게 된 접속을 다시 가능하게 하여야 한다. 반대의 통지를 받은 원래의 침해 통지자가 침해행위를 금지시키기 위한 소송이 제기되었다는 것을 서비스 제공자의 지정대리인에게 다시 통지한 경우, 서비스 제공자는 침해한 것으로 주장된 자료를 복구시키거나 접속을 가능하게 할 필요는 없다 [512(g)(2)(C)].

### 4. 저작권 관리정보

#### (1) 저작권 관리정보에 의한 저작물의 보호

저작권 관리정보(Copyright Management Information, 이하 CMI)는 디지털 형태의 저작물에 부착된 것으로서 저작자, 저작물 및 저작물의 사용조건 등에 관한 정보를 의미한다. 인터넷상에서 저작권이 쉽게 침해될 수 있게 된 것은 컴퓨터기술과 통신기술 등의 기술의 발전에 기인한다. 따라서 저작권의 침해에 대응하는 방안도 역시 기술에 귀결될 수밖에 없는데, 이러한 기술로서는 디지털 워터마킹과 암호화를 들 수 있다. 디지털 워터마킹이 디지털 매체 자체에 대한 통제하고 한다면 암호화는 디지털화된 내용(디지털 콘텐츠, digital contents)에 접근하는 것 자체를 통제하는 것이다.

##### 1) 디지털 워터마킹

디지털 워터마킹(digital watermarking, 또는 digital fingerprinting, steganography)[18]은 디지털화된 정보를 압축·암호화과일을 만

드는 것으로서 파일에 포함되어 있는 정보를 파일로부터 분리할 수 없도록 하는 과학의 한 분야이다. 디지털방식에 의한다는 점에서 디지털 워터마크(digital watermark)는 그동안 전통적으로 사용되어 왔던 워터마크와 구별되는데, 워터마크의 대표적인 예는 빛에 비추는 경우에만 나타나도록 하는 지폐에 사용되는 워터마크이다. 디지털 워터마크가 인식될 수 있다면 화상이나 음악의 질을 떨어뜨리고 저작권 침해자에 의하여 제거될 수도 있다. 따라서 제 역할을 하기 위하여 디지털화된 화상이나 음악을 청취할 때 디지털 워터마크는 인식되지 않아야 한다.[19] 디지털 워터마크는 'header information'과 달리 컴퓨터 이미지 그 자체에 저작권 관리정보를 입력시키는 것이다. 이러한 정보는 이미지를 구성하는 부분(pixel, 하나의 바이트)들의 명도를 변경시킴으로써 컴퓨터 이미지 내에서 만들어지는 것으로서 눈에 띄지 않는 디자인이다. 디지털 워터마크는 복제, 편집, 스캐닝, 조작, 파일압축, 파일 포맷방식간의 변환 등 서류가 여러 차례에 걸쳐 변환되더라도 인식될 수 있어야 한다. 다만 전통적인 워터마크와 달리 디지털 워터마크는 소프트웨어를 사용하는 경우에만 인식될 수 있다. 디지털 워터마크가 저작권의 보호와 관련하여 중요한 의미를 지니는 것은 눈에 보이지 않는 여러 가지의 정보, 곧 저작자의 이름이나 전자우편의 주소 또는 저작물을 이용하기 위하여 접촉하기 위한 정보 등을 포함할 수 있다는 점이다.

디지털 워터마크는 저작물의 도난 자체를 방지할 수는 없으나 인터넷상에서 저작물을 보호하는 것과 관련하여 여러 가지의 중요한 역할을 수행할 수 있다. 첫째, 디지털 워터마크는 인터넷, 디지털 위성, 디지털 케이블 등으로 전송되는 정지화상, 동화상, 음성 등의 파일이 해적행위의

18) Steganograhpy는 글씨 위에 무엇을 덮었다는 의미의 희랍어에 기원하는 데, 비밀적인 내용을 숨겨서 메시지를 전달하기 위한 것이었다. 예컨대 나무 위에 글씨를 쓰고 그 위에 왁스를 발라서 메시지를 전달하는 것, 사람의 턱에 메시지를 문신을 새긴 후 수염을 길러서 메시지를 전달하는 것, 사람의 눈에 보이지 않는 잉크를 사용하여 메시지를 전달하는 것 등이 모두 steganography에 해당한다.

19) 과거에는 보호되는 이미지를 추적하기 위하여 컴퓨터 이미지 파일의 위에 저작권 소유정보를 포함하는 일련의 코드인 'header information'이라는 것이 사용되었다. 그러나 컴퓨터 이미지 파일에서 이것을 찾아내는 것은 쉬우며 파일로부터 쉽게 제거할 수 있었으므로, 저작권의 침해를 추적하기에 충분한 것이 아니었다.

대상이 되는 것을 억제할 수 있다. 왜냐하면 이러한 워터마크를 제거하게 되면 저작물의 화질이나 음질이 떨어지게 되고, 따라서 화질이나 음질의 열등한 복제물을 해적행위에 의하여 획득할 동기는 그만큼 감소하기 때문이다.[20]

둘째, 디지털 워터마크는 저작권자가 인터넷에 올려진 불법 복제물의 출처를 추적할 수 있도록 하여 침해자의 책임을 물을 수 있도록 한다. 디지털 워터마크가 저작물의 이용이 적법한 지 여부는 알려주지 않지만 특별한 검색프로그램을 이용하여 저작권을 침해한다고 믿어지는 웹사이트를 찾아낼 수 있다.

셋째, 디지털 워터마크는 불법 복제물이 만들어지는 것을 억제하여 저작권자가 인터넷에 아무런 두려움없이 자신의 저작물을 올려놓을 수 있도록 한다. 왜냐하면 디지털 워터마크가 있는 저작물의 복제물은 원본과 쉽게 구별될 수 있기 때문이다.

예컨대 Digimarc社의 PictureMarc라는 디지털 워터마크는 컴퓨터 이미지를 편집하는 소프트웨어에 의하여 인식되며 저작권의 소유와 실시허락에 관한 정보를 나타나게 해 준다. Digimarc사의 디지털 정보는 컴퓨터 이미지를 제거하거나 조작함으로써 편집할 수 없으며, MarcSpider라는 검색프로그램에 의하여 디지털 워터마크가 표시된 저작물이 인터넷상에서 어디에 위치하고 있는지를 저작권자에게 제공하는 서비스를 제공하고 있다. 따라서 이를 이용하는 저작권자는 인터넷상에서 디지털방식으로 저작권 관리정보가 들어가 있는 이미지를 허락을 받지 않고 사용하는 것을 찾아낼 수 있다.

2) 암호화

디지털 워터마크 이외에 저작권을 보호하기 위하여 사용되는 것은 암호화(encryption)이다. 암호화는 어떠한 방식이나 알고리즘(algorithm)에 따라 읽을 수 있는 정보(메시지, plaintext라고 함)를 이해할 수 없는

20) MP3에서 논한 바와 같이 음악 CD는 MP3 파일로 만들어지거나(ripping) 복제될 수 있다. 이것은 현재의 대부분의 CD가 디지털 방식에 의한 해적행위의 위협이 없었을 때 개발·생산된 것에 기인한다.

정보(ciphertext라고 함)로 변환시키는 과정, 또는 디지털 형태로 저장된 데이터를 알고리듬(algorithm)을 사용하여 이해할 수 없는 코드로 변환시키는 방법으로 정의되고 있다. 이 메시지를 받은 자가 이를 다시 읽을 수 있는 정보로 번역하기 위해서는 암호해독(decryption)이 필요하다. 이같은 암호법(cryptography)[21] 사용되는 주된 목적은 데이터의 무결성(integrity), 진정성(authentication), 부인방지(nonrepudition), 비밀유지 등을 보장하는 것이다. 가장 흔히 이용되는 암호화방법 중의 하나는 PGP(Pretty Good Privacy)인데, 이것은 텍스트를 암호화하기 위하여 RSA(Rivast-Shamir-Adleman)의 공개/비밀 알고리듬(public/private algorithm)을 사용한다. RSA는 쌍으로 된 암호화/암호해독 열쇠(encryption/decryption keys)를 사용하는 데, 하나의 열쇠로 암호화된 서류는 다른 열쇠로 해독할 수 있게 된다.

저작자는 암호기술을 이용하여 자신의 저작물을 보호하고자 해 왔다. 암호화기술을 이용하여 디지털 저작물에 대한 접근 및 사용을 통제하는 기술이 디지털 봉투(digital envelope) 또는 디지털 상자(digital box)라는 기술이다. 디지털 상자는 자물쇠에 의하여 잠겨진 상자로서, 박스의 내용물(예컨대 음악저작물)에 접근하기 위하여 이용자는 이용료를 지급하여야 한다. 그 이외의 과정은 암호해독과 동일하다.

암호화는 전자 데이터를 보호하기 위한 해결책으로 여겨져 왔다. 그러나 일단 해커(hacker)가 열쇠를 깨뜨려서 서류를 해독하고 나면, 그가 열쇠 및 암호해독 소프트웨어나 암호해독된 서류를 수많은 사람에게 송부할 수 있으므로, 완전한 해결책은 될 수 없다. 또한 저작권자와 저작물의 이용자간의 관계에서 고려하면, 저작권의 존속기간이 만료하였음에도 불구하고 저작물에 접속할 수 없다는 문제점이 발생한다. 앞서 언급한 바와 같이 암호화에 의한 저작물의 보호는 저작물 자체에 대한 접근을 통제하는 것이기 때문이다. 같은 논리선상에서 저작물의 이용이 공정이용

21) 암호법은 전자통신과정에서 비밀을 확보하고자 하는 응용수학의 한 분야이며, 메시지를 감추는 과정이 암호화(encryption)이다. 암호화 알고리즘(cryptographic algorithm)은 데이터를 이해할 수 없는 형태로 전송하기 위하여 사용되는 수학함수 또는 등식이다.

이나 사적이용이 될 수도 있으며, 저작물이 일반인의 공유영역(public domain)에 들어갔음에도 저작물에 접근조차 할 수 없다는 문제점이 제기되고 있다.

1996년의 WIPO 저작권조약은 각 체약국이 (ⅰ) 저작권자의 허락없이 전자적인 권리관리정보를 제거 또는 변경하거나, (ⅱ) 권리관리정보가 제거 또는 변경되었다는 것을 알고서 저작물이나 저작물의 복제물을 배포, 수입, 일반인에게 방송하거나 전달하는 것에 대하여 (행위자가 이러한 행위에 의하여 WIPO 저작권조약이나 베른협약이 보호하는 권리의 침해를 유도하거나 가능·용이하게 하거나 은닉할 것이라는 것을 알아야 함) 적절하고 효과적인 보호를 하도록 하고 있다(제12조). WIPO 실연·음반조약도 이와 동일하게 규정하고 있다(제19조).

(2) 저작권 관리정보의 정의

WIPO 저작권조약 제12조는 '권리관리정보(rights management information)'라는 표현을 쓰고 있는데, '저작물, 저작물의 저작자, 저작물에 대한 저작권자 또는 저작물의 이용에 대한 조건에 관한 정보와 그러한 정보를 나타내는 숫자나 코드로서, 이러한 정보가 저작물의 복제에 부착되거나 저작물을 일반인에게 전달하는 과정에서 나타나는 경우'라고 정의하고 있다(제12조 제2항).

미국의 DMCA는 CMI에 대하여 상세히 정의하고 있는데, 저작물의 복제물이나 음반 또는 저작물의 공연이나 전시와 관련하여 전달되는 저작물, 저작자, 저작권자, 실연자, 저작물의 사용의 조건, 이러한 정보를 표시하는 숫자나 상징 또는 이러한 정보에 대한 연결 등의 정보를 의미하며, 여기에는 디지털형태로 된 정보도 하지만 저작물의 사용자를 개인적으로 나타내는 정보는 포함되지 않는다[미국 저작권법 제1202조 (c)]. 이러한 정보는 (ⅰ) 저작물을 표시하는 제목 기타의 정보(저작권의 통지를 청하는 정보 포함), (ⅱ) 저작물의 저작자의 이름 및 이에 대한 기타의 정보, (ⅲ) 저작물에 대한 저작권자의 이름 및 저작권자를 표시하는 기타의 정보, (ⅳ) 시청각 저작물(audiovisual works)을 제외한 저작물에

실연을 고정시킨 실연자의 이름 및 이에 대한 기타의 정보, (v) 시청각 저작물의 경우, 시청각 저작물에 관련된 작가, 실연자 또는 감독 등의 이름 및 이에 대한 기타의 정보, (vi) 저작물 사용의 조건, (vii) 이러한 정보를 표시하는 숫자나 상징 또는 이러한 정보에 대한 연결, (viii) 저작권국이 규정에 의하여 정할 수 있는 기타의 정보 등이다[제1202조 (c)].

(3) 저작권 관리정보에 대한 DMCA의 규율

DMCA에 의하여 개정된 미국 저작권법은 크게 두 가지로 저작권 관리정보(CMI)를 규율하고 있다. 첫째, 허위(false)의 CMI에 관한 것으로서, 저작권침해를 유도하거나 가능·용이하게 하거나 은닉하기 위하여 허위의 CMI를 제공, 배포 또는 수입하는 것은 금지된다[제1202조 (a)항]. 둘째, CMI의 제거 또는 변경으로서, 저작권자의 승낙이나 법에 의하지 않고서는, (i) CMI를 의도적으로 제거 또는 변경하거나, (ii) 제거 또는 변경되었다는 것을 알면서 CMI를 배포 또는 수입하거나, (iii) 제거 또는 변경되었다는 것을 알거나 저작권침해를 유도하거나 가능·용이하게 하거나 은닉할 것이라는 것을 알면서(또는 알만한 합리적인 이유가 있다면) 저작물이나 저작물의 복제물 또는 음반을 배포, 수입 또는 공연하는 것은 금지된다[제1202조 (b)항].

## 제 3 절 ACPA

### 1. 도메인네임의 무단점유 및 ACPA

도메인네임은 선접수 선등록에 따라서(on a first-come, first-served basis) 등록되므로, 상표권자의 상표를 타인이 먼저 등록할 수 있다. 도메인네임을 등록함에 있어서는 상표에서와 같은 심사절차가 없으며, 선점되어 있지 않다면 단 2-3분 이내에 등록이 이루어질 수 있다. 상표권자가 아닌 자에 의한 등록문제는 사이버공간의 해적행위자(cyberpirate)라고 알려진 사람들이 상표권자에게 판매하기 위하여 도메인네임을 등록함으로써 악화된다. 이같은 해적행위자들에게는 상거래를 위하여 도메인

네임을 사용하려는 의도가 전혀 없으며, 이들은 상표와 관련되는 도메인네임을 상표권자에게 되돌려주려는 조건으로 금전을 강요하려고 한다. 또한 미국의 NSI의 예에서 볼 수 있는 바와 같이 상표와 도메인네임이 관련된 분쟁은 도메인네임의 등록기관까지도 분쟁에 휘말려들게 한다.

인터넷상에서 도메인네임이 상표법과 관련하여 발생하는 분쟁의 유형은 등록의 목적에 따라 다음과 같이 구분할 수 있다. 물론 이러한 도메인네임에 관한 분쟁의 유형은 명확하게 구별되는 것은 아니며 혼용되어 있을 수도 있다. 첫째, 도메인네임의 무단점유(cybersquatting)로서 도메인네임을 상표권자에게 판매하기 위한 목적으로 상표권자보다 먼저 등록하는 것인데, 이와 같이 등록하는 자를 무단점유자라고 한다. 둘째, 상표권자가 도메인네임을 이용한 웹사이트를 만들지 못하도록 하거나 경쟁자를 괴롭히기 위하여 도메인네임을 등록하는 경우이다. 셋째, 타인의 상표를 도메인네임을 등록하여 그 상표권자와 경쟁을 하거나 경쟁을 하지 않는 등 상업적인 목적으로 사용하는 경우이다. 판결결과에만 의한다면 chanel.co.kr 사건이 전자에 해당하고 viagra.ac.kr 사건이 후자에 해당한다. 넷째, 타인의 잘 알려진 상표와 약간 다른 2단계 도메인을 등록하는 경우이다. 이것은 인터넷 이용자가 도메인네임을 잘못 타이프하는 경우를 이용하기 위한 것으로서, 타인의 유명한 상호나 상표에 기생(parasite)하기 위한 것이다. 다섯째, 제1차 도메인이 각각 다른 경우에 동일한 제2차 도메인을 등록하는 것이다. 예컨대 NSI가 할당하는 .com, .net, .org 등의 제1차 도메인(gTLD)과 각 국가가 할당하는 국가별 제1차 도메인(ccTLD) 하에서 동일한 제2차 도메인을 등록하는 경우이다. 후술하는 Avery Dennison Corp. v. Sumpton 케이스[22]가 여기에 해당한다.

여섯째, 예컨대 Dell 컴퓨터의 부품을 판매하기 위하여 dellspareparts.com에서와 같이 타인의 상표나 상호를 도메인네임의 일부로 사용하는 경우이다. 마지막으로 billclinton.com, hillary.com, billandclinton.com에서 볼 수 있는 것과 같이 타인의 이름을 도메인네임으로 등록하는 것이다.

---

22) 189 F.3d 868 (9th Cir. 1999).

이러한 유형 중에서 도메인네임을 가장 남용하는 형태는 도메인네임의 무단점유라 할 수 있다. 도메인네임의 무단점유 또는 사이버공간에서의 해적행위(cyberpiracy)에 대해서 미국의 下院은 상표가 가지는 굿윌(good will)로부터 이익을 얻기 위한 악의를 가지고 상표와 동일하거나 혼동을 야기할 정도로 상표에 유사한 도메인네임을 등록, 거래, 사용하는 것이라고 하였다.[23] 이같은 해적행위는 도메인네임을 상거래에서 사용하려는 의사가 없이 상표와 동일하거나 유사한 도메인네임을 등록하여 이익을 취하려는 것이다. 이러한 행위는 소비자의 신뢰를 저하시키고 소비자가 인터넷을 이용하는 것을 방해할 뿐만 아니라, 상표의 가치를 파괴하는 것이다. 사이버공간에서의 해적행위는 여러 가지 방법으로 상표권자에게 손해를 가할 수 있다. 곧 해적행위로 인하여 소비자는 상표권자의 웹사이트를 찾지 못하게 되므로 영업상의 손실을 야기시킨다. 해적행위자가 타인의 상표와 동일하거나 유사한 도메인네임을 등록하여 이를 이용하는 경우에는 상표권자의 상표가 가지는 판매력을 약화시킨다. 해적행위자가 도메인네임을 포르노 사이트를 운영하는 데 이용하는 경우에는 상표를 손상시킬 수 있다. 마지막으로 상표권자는 상표가 부당하게 이용되는 것을 방지하기 위하여 끊임없이 감시하고 상표권을 집행하여야 하므로 간접적으로 손해를 보게 된다.[24] 미국에서 무단점유방지법(Anty-cybersquatting Consumer Protection Act, 이하 ACPA)[25]가 제정된 이유는 바로 여기에 기인하는 것이다.

1999년 11월 29일 클린턴 대통령은 ACPA를 통과시킴으로써 제9연방항소법원의 판시내용, 곧 Panavision International L.P. v. Toeppen 케이스[26]의 내용을 법령화하였다. 이 법은 무단점유에 의하여 야기되는 상표법상의 여러 위반에 대한 연방법상의 구제수단을 제공하기 위하여 연방 상표법을 개정하는 것, 곧 제43(d)[15 U.S.C. §1125(d)]를 추가하는 것이었다.

23) Trademark Cyberpiracy Prevention Act, H.R. No.106-412 (Oct. 25, 1999).
24) Trademark Cyberpiracy Prevention Act, H.R. No.106-412 (Oct. 25, 1999).
25) Pub. L. No.106-113, 1113 Stat. 1537 (1999) (codified as amended at 15 U.S.C. §1125(d) (1999).
26) 945 F. Supp. 1296 (C.D. Cal. 1996), aff'd (9th Cir. 1998).

## 2. FTDA에 의한 무단점유의 규율

### (1) 연방법에 의한 상표희석법의 도입

ACPA가 1999에 통과되기 이전에 도메인네임의 무단점유를 규율할 수 있는 입법으로서 1995년 Federal Trademark Dilution Act(Federal Trademark Dilution Act, 이하 FTDA)가 있었다. 이 법은 상표의 희석에 관한 입법인데, 상표를 희석으로부터 보호하는 것은 주법에 의하여 보호되어 왔으나, 1995년 Federal Trademark Dilution Act(이하 FTDA)에 의하여 연방법에 의하여 인정되기에 이르렀다. 연방 상표법은 저명한 상표(famous mark)의 소유자(senior user)는 그 상표가 저명해진 이후에 타인(junior user)이 상거래에서 상표나 상호를 상업적으로 사용하여 그 상표의 식별력을 희석시킨 경우에 금지명령 기타 구제수단을 구할 수 있다고 규정하고 있다.

### (2) FTDA의 저명성에 관한 판단

희석에 관한 규정은 원고의 상표가 저명하고, 원고의 상표가 저명해진 이후에 피고에 의한 사용이 시작되어야 희석에 의한 소인이 인정된다고 규정하고 있다. 미국 연방법은 상표가 저명한가를 판단하는 데 있어서 법원이 고려할 만한 여덟 가지의 기준을 규정하고 있다. 즉 (1) 상표의 본질적인 식별력이나 획득된 식별력의 정도, (2) 상표가 사용된 상품이나 서비스와 관련한 상표의 사용의 기간과 정도, (3) 상표의 광고와 알림(publicity)의 기간과 정도, (4) 상표가 사용된 거래지역의 지리적인 정도, (5) 상표가 사용된 상품이나 서비스를 위한 거래경로(channel of trade), (6) 거래지역이나 거래경로에서 상표소유자와 금지명령을 구하려는 자가 사용한 상표의 인지(recognition)의 정도, (7) 제3자가 사용한 동일하거나 유사한 상표의 사용의 성질과 정도, (8) 상표가 주등록부(Principal Register)에 등록되었는지 여부 등이다.

(3) FTDA에 의한 구제수단

반희석법은 희석된 저명한 상표의 소유자가 전국적인 금지명령에 의하여 구제될 수 있도록 규정하고 있다. 다만 희석에 의한 침해자가 고의로(willfully) 저명 상표 소유자의 명성이나 굿 윌을 이용하려 한 경우에는, 금지명령뿐만 아니라 전통적인 상표침해에 대한 구제수단인 (a) 피고가 얻은 이익(profit), (b) 원고가 입은 손해에 대한 배상(damage), (c) 소송비용까지도 원고는 청구할 수 있도록 하고 있다.

(4) FTDA에 의한 예외

연방법의 희석에 관한 규정은 여러 형태의 예외를 규정하고 있다. 이러한 예외로서는 공정이용(fair use)을 위한 것으로서 비교를 하는 상업광고(comparative commercial advertising)를 하거나 저명한 상표소유자의 경쟁자가 그 저명한 상표소유자의 상품이나 서비스의 동일성을 나타내는 것을 증진하는 경우이다. 또 다른 예외로는 다른 공정이용에서와 같이 상표를 비상업적인 목적으로 사용하는 경우와 뉴스 형태의 모든 보고나 모든 논평(commentary)이 포함된다.[27]

3. ACPA의 내용

(1) 訴因의 제공

연방 상표법 제43(d)(1)은 악의에 의한 무단점유에 대한 訴因(cause of action)을 제공하는 것이다. ACPA는 상표와 관련된 굿윌로부터 이익을 얻을 목적으로 식별력있는 상표를 악의 및 남용적인 방법으로 도메인네임으로 등록하는 것을 금지하고자 하는 것이다. 도메인네임의 무단점유가 되기 위해서는 (ⅰ) 상표로부터 이익을 얻으려는 악의(bad faith intent)가 있어야 하며, (ⅱ) 도메인네임을 등록, 거래 또는 사용하여야 한다. 또한 무단점유로부터 보호받을 수 있는 상표는 식별력있는 상표

27) 미국 연방상표법 § 43 (c) (4), 15 U.S.C. § 1125 (c) (4).

(distinctive mark) 및 저명상표(famous mark)이어야 한다. ACPA의 규율대상이 되는 것은 식별력있는 상표의 경우에는 이와 동일하거나 혼동을 야기할 정도로 유사하여야(confusingly similar) 한다. 또한 저명상표의 경우에는 이와 동일하거나, 혼동을 야기할 정도로 유사하거나, 저명상표를 희석하는 것이어야 한다[§43(d)(1)(A)]. 따라서 ACPA에 의하여 보호되기 위해서는 상표가 식별력이 있거나 저명하여야 한다.

(2) 악 의

1) 악의 요건

ACPA는 제소를 하기 위한 요건으로서 악의를 요구하고 있는데, 악의를 요구하는 것은 무단점유에 기한 책임을 묻기 위한 핵심적인 요소이다. ACPA는 악의를 판단하기 위한 9가지의 요소를 규정하고 있다. 곧 (ⅰ) 도메인네임에 대한 등록자의 상표권 및 기타 지적재산권, (ⅱ) 도메인네임이 등록자의 이름이나 기타 등록자를 나타내기 위하여 흔히 사용되는 이름으로 구성된 정도, (ⅲ) 상품이나 서비스를 성실하게 제공하는 것과 관련하여 등록자가 도메인네임을 과거에 사용하였다는 것, (ⅳ) 도메인네임하의 사이트에서 등록자가 상표를 비상업적으로 성실하게 사용하였다는 것 또는 정당하게 사용하였다는 것, (ⅴ) 사이트의 출처, 후원, 연관관계 또는 승인에 관하여 혼동가능성을 야기함으로써, 상업적인 이익을 얻거나 상표를 손상 또는 경멸하기 위하여, 상표권자의 온라인상의 고객을 도메인네임에 의하여 접근할 수 있는 사이트로 끌어들임으로써 상표가 가지는 굿윌을 손상하는 것, (ⅵ) 상품이나 서비스를 제공하기 위한 성실한 의도로 도메인네임을 사용하지 않았거나 사용하려는 의도없이 금전적인 이익을 얻기 위하여 상표권자 또는 제3자에게 도메인네임을 이전, 판매 기타 양도하려 의도하였거나, 그러한 행태를 나타내는 과거의 행위, (ⅶ) 도메인네임을 등록하는 데 있어서 오해를 불러일으키는 허위의 접촉정보(contact information)를 제공하였다는 것, 등록자가 정확한 접촉정보를 의도적으로 유지시키지 않았다는 것, 또는 그러한 행태를 나타내는 과거의 행위, (ⅷ) 타인의 식별력이 있거나 저명한 상표와

동일 또는 혼동을 야기할 정도로 유사하다는 것을 알면서 여러 개의 도메인네임을 등록 또는 획득하였다는 것, (ix) 도메인네임에 포함된 상표가 제43(c)(1)의 의미에서 식별력이 있는지 여부 또는 저명한지 여부의 정도 등이다[1125(d)(1)(B)(ⅰ)].

이같은 요소들은 과거에 도메인네임의 무단점유자들이 도메인네임을 판매하기 위하여 취하였던 행위들을 반영하는 것이다. 또한 이러한 요소들은 제한적인 것이 아니라 열거적인 것이고, 따라서 법원은 악의를 결정하는 데 있어서 그 외의 다른 요소를 고려할 수도 있다.

2) 악의의 결여에 관한 요소

악의에 관한 요소는 두 가지 유형, 곧 판사가 악의를 나타내는 증거라고 고려할 수 있는 요소와 악의가 결여되어 있다는 것을 보여주는 요소로 나눌 수 있다. 악의가 결여되어 있다는 요소로서 법원은 도메인네임에 대한 등록자의 상표권 및 기타 지적재산권을 고려할 수 있는데[§ 43(d)(1)(B)(ⅰ)(Ⅰ)], 이것은 무단점유자가 상표를 사용할 권리를 가질 수도 있다는 것을 인정한 것이다. 또한 도메인네임이 등록자의 이름이나 기타 등록자를 나타내기 위하여 흔히 사용되는 이름으로 구성된 정도를 고려할 수도 있다[§43(d)(1)(B)(ⅰ)(Ⅱ)]. 따라서 판사는 어떠한 개인이 자신의 이름을 도메인네임으로 사용할 뿐인 경우, 이를 악의가 결여된 증거하고 할 수 있다. 상품이나 서비스를 성실하게 제공하는 것과 관련하여 등록자가 도메인네임을 과거에 사용하였다는 것[§43(d)(1)(B)(ⅰ)(Ⅲ)]과 도메인네임하의 사이트에서 등록자가 상표를 비상업적으로 성실하게 사용하였다는 것 또는 정당하게 사용하였다는 것[§43(d)(1)(B)(ⅰ)(Ⅳ)]도 악의가 결여되었다는 요소가 된다.

3) 악의를 나타내는 요소

가) 유사한 도메인네임의 등록

제43조 (d)에서 악의를 나타내는 요소들은 과거에 무단점유자들의 행태의 예를 입법화한 것이다. 예컨대 ACPA는 타인의 도메인네임과 유사한

도메인네임을 등록하는 것을 무단점유의 한 형태로 인정하였다[§43(d)(1)(B)(ⅰ)(Ⅴ)]. 이같은 무단점유에 있어서는 타인이 사용하는 도메인네임의 철자를 잘못 타이프한 도메인네임을 등록하는 것이다. 이것은 소비자들이 의도하였던 도메인네임의 웹사이트(곧 상표권자의 웹사이트)가 아니라 우연히 실수에 의하여 그 도메인네임과 유사한 도메인네임의 웹사이트에 접속하게 하려는 목적으로 도메인네임을 등록하는 것이다. 이 경우 무단점유자는 소비자들이 상표권자가 제공하는 상품이나 서비스와 유사하거나 심지어 상표권자의 상품을 판매한다. ACPA는 바로 이러한 형태의 무단점유를 해결한 것이다.

나) 도메인네임의 판매행위

도메인네임을 판매하려는 것[§43(d)(1)(B)(ⅰ)(Ⅵ)]과 여러 개의 도메인네임을 등록하는 것[§43(d)(1)(B)(ⅰ)(Ⅷ)]은 전형적인 형태의 무단점유를 나타내는 행태들이다. 이러한 요소들은 Pananvision Int'l, LP v. Toeppen 케이스에 적용될 수 있는 것들이다. 곧 법원은 도메인네임을 사용하려는 의도없이 금전적인 이익을 위하여 상표권자 또는 제3자에게 도메인네임을 이전, 판매 기타 양도하려 했다는 것을 고려할 수 있다. 뿐만 아니라 등록자가 도메인네임을 판매하려 했다는 과거의 행위까지도 고려할 수 있다. 이것은 도메인네임을 실제로 사용하지 않고 판매하려는 행위를 인정함으로써, 진정한 무단점유자와 무단점유의 의도없이 도메인네임을 등록한 자(innocent user)를 구별하기 위한 것이다.

다) 다수 도메인네임의 등록행위

또한 법원은 타인의 식별력이 있거나 저명한 상표(famous mark)와 동일 또는 혼동을 야기할 정도로 유사하다는 것을 알면서 여러 개의 도메인네임을 등록 또는 획득하였다는 요소를 고려할 수 있다[§43(d)(1)(B)(ⅰ)(Ⅷ)]. 이것은, 무단점유가 되기 위해서는 도메인네임이 타인의 상표와 동일하거나 혼동을 야기할 정도로 유사하다는 것을 등록자가 알고 있었어야 할 것을 요구함으로써, 역시 무단점유의 의도없이 도메인네임을 등록한 자를 보호하기 위한 것이다. 또한 상표는 '도메인네임의 등록시에' 저명하여야 한다.

저명한 상표에 대하여 ACPA 매우 광범위하게 보호하는 선택을 했다고 할 수 있다. 곧 상표와 동일하거나 혼동을 야기할 정도로 유사하게 상표를 이용하는 경우에 상표는 보호받는다. 저명한 상표에 대한 무단점유를 입증하기 위하여서는 상표와 동일하거나 혼동을 야기할 정도로 유사하거나 상표를 희석시킨다는 것을 입증하여야 한다. 이것은 상표희석법[Federal Trademark Dilution Act, §43조 (c), 15 U.S.C. §1125(c)]과 유사하게 무단점유로부터 저명한 상표를 보호하는 것인데, 제43조 (c)항과 달리 상표의 저명성을 판단하기 위한 요소를 정의하지 않고 있다. 따라서 저명한 상표는 좀 더 관대한 판단기준에 따라 보호를 받을 수 있게 되는 것이다.

라) 허위 접촉정보의 제공행위

법원은 도메인네임을 등록하는 데 있어서 허위의 접촉정보를 제공하는 것 등을 고려할 수 있다[§43(d)(1)(B)(ⅰ)(Ⅵ)]. 이것은 무단점유자들이 자신의 신원을 은닉하고자 한 사실을 인정한 것이다.

4) 악의가 부정되는 경우

ACPA는 악의의 인정에 대한 방어를 규정하고 있다. 곧 등록자가 도메인네임을 정당하게 사용하거나 도메인네임을 사용할 권리가 있다고 믿었거나 믿을만한 합리적인 근거가 있다고 법원이 결정한 경우에는 악의가 존재하지 않는다[§43(d)(1)(B)(ⅱ)]. 이것은 악의를 인정하는 여러 요소가 있는 경우에도 도메인네임을 합법적으로 사용할 수 있는 등록자를 보호하기 위한 것이다. 따라서 정당한 사용에 기한 방어(fair use defense)는 매우 중요한 의미를 가진다.

(3) 구제수단

ACPA는 도메인네임의 무단점유에 관한 규정을 위반한 것에 대한 訴因을 제공하고 있다. 위반에 대한 구제수단으로서 ACPA는 금지명령(injunction)과 법정손해배상이나 실제의 손해배상을 선택토록 하고 있다. 이에 따라 상표권자가 무단점유를 금지시키기 위하여 상표침해나 상표희

석에 따라서 소송을 제기할 필요가 없다. ACPA는 무단점유로 인한 피해자에게 법적인 구제수단을 제공하기 위한 것이므로, 미국 의회는 도메인네임의 무단점유에 있어서 ACPA의 규정이 상표침해에 의한 소송보다 용이하게 적용될 것을 의도한 것이다.

1) 금지명령

금지명령과 관련하여 법원은 도메인네임의 무단점유에 관한 규정의 위반을 방지하기 위하여 법원이 적절하다고 여길 수 있는 금지명령을 상표권자에게 부여할 수 있다[§34, 15 U.S.C. §1116(a)].

2) 손해배상

ACPA는 침해에 대하여 실제의 손해(actual damages)를 배상할 것을 규정하고 있다[§35, 15 U.S.C. §1117(a)]. 이에 의하여 피고가 얻은 이익, 원고의 손해 및 법원의 비용을 배상받을 수 있다. 손해배상을 산정함에 있어서 법원은 원고가 입은 실제적인 손해액의 3배에 해당하는 손해배상(treble damages)을 허용할 수 있으며, 특별한 경우에는 승소한 당사자에게 변호사비용(attorney)을 허용할 수 있다.

도메인네임의 무단점유에 대하여 구제수단에 대하여 ACPA가 추가시킨 주된 구제수단은 위에서의 실제의 손해 대신에 법정손해(statutory damages)를 원고가 선택할 수 있다는 것이다[§35(d), 15 U.S.C. §1117(d)]. 원고가 법정손해를 선택할 수 있는 시기는 법원의 최종적인 판단이 행하여지기 이전의 어느 시점에서나 가능하다. 법정손해액은 1천 달러에서 10만달러 이하이다. 그동안 도메인네임의 무단점유에 있어서 원고가 입은 손해를 입증하는 것은 매우 어려웠다는 것을 고려하면, 상표권자는 이 규정에 의하여 무단점유자로부터 배상을 구하는 것이 더 용이해지게 되었다.

3) 도메인네임의 압수·취소·이전

도메인네임을 등록, 거래, 사용하는 것에 관한 소송에서, 법원은 도메인네임을 압수, 취소 또는 상표권자에게 이전시킬 것을 명할 수 있다[§

34(d)(1)(C), 15 U.S.C. § 1116(d)(1)(C)]. ACPA가 제정되기 이전에 등록된 것에 대해서도 이같은 구제수단이 허용된다.

(4) 대물관할

ACPA의 가장 중요한 것 중의 하나는 도메인네임 그 자체에 대하여 대물관할권에 기한 소송제기를 허용하였다는 것이다. 미국 연방상표법상의 희석에 관한 규정은 상표를 희석시키는 것에 대하여 대물관할권(in rem jurisdiction)을 인정하지 않고 있다. 따라서 도메인네임 등록기관에 허위의 정보를 제공하는 무단점유자를 제소하는 것이 불가능한 경우가 많았다. 곧 무단점유에 책임있는 당사자를 찾아내는 것이 어려웠으며 이에 따라 대인관할권(in personam jurisdiction)에 기하여 소송을 제기하기가 어려웠다. 이같은 문제점을 해결하기 위하여 ACPA는 일정한 경우에 대물관할권을 인정하고 있다[§ 1125(d)(2)]. 그러나 과거에는 법원이 관할권을 행사하여 도메인네임의 등록을 취소할 수 없었던 것을 고려한다면, 대물관할권이 인정됨으로써 상표권자는 상당히 중요한 무기를 획득한 것이 된다.

상표권자는 도메인네임 등록자를 찾아내기 위하여 적절한 노력(due diligence)를 하였거나 등록자에 대하여 대인관할권을 행사할 수 없는 경우에 도메인네임 등록기관에 대하여 대물관할권을 행사할 수 있다. 상표권자가 대물관할권에 기한 소송을 제기하는 경우, 도메인네임이 등록된 상표 소유자의 권리를 침해하거나 제43조 (a)항, (b)항 또는 (c)항에 규정된 권리를 침해하여야 한다. 그리고 법원이 (ⅰ) 민사소송에서 피고이어야 했던 자에 대한 대인관할권을 획득할 수 없거나, (ⅱ) 적절히 노력했음에도 불구하고 민사소송에서 피고이어야 했던 자를 발견할 수 없었어야 한다. 적절한 노력이라는 것은 도메인네임 등록기관에 등록자가 제공한 우편주소 및 전자우편주소에 도메인네임의 무단점유에 관한 규정을 위반했다는 것과 이에 따라 제소하겠다는 의도를 통지하는 것과 소송이 제기된 후 법원이 명하는 바에 따라 소송의 통지를 공표하는 것이다[1125(d)(2)(A)].

대물관할권에 기한 소송을 제기할 수 있는 제1심 연방법원은 (ⅰ) 도메인네임 등록기관이 위치한 곳, 또는 (ⅱ) 도메인네임의 처분과 이용에 관한 통제 및 권한을 확보하기에 충분한 서류가 예치될 수 있는 곳이다[§43(d)(2)(C)]. 그러므로 상표권자는, 소송이 제기되기 전 또는 이후에 도메인네임 등록기관이 법원에 필요한 서류를 예치할 것에 동의한 경우에는, 어느 곳의 제1심 연방법원에서라도 대물관할권에 기한 소송을 제기할 수 있다는 것을 의미한다.

대물관할권을 인정함으로써 상표권자에게 생기는 주된 장점은 도메인네임 등록자가 이제 상표권자로부터 숨어 있을 수 없다는 것과 소송제기의 통지와 서류송달절차가 극히 간단하다는 것이다. 또한 등록기관이 원고의 소장을 서면으로 통지받은 즉시 법원의 명령에 의한 경우 이외에는 도메인네임을 이전, 중지 기타 수정해서는 안되며, 도메인네임의 처분과 이용에 관한 통제 및 권한을 확보하기에 충분한 서류를 법원에 신속하게 예치하여야 한다[§43(d)(2)(D)(ⅰ)].

대물관할권에 기한 소송의 단점은 대물관할권에 기한 구제수단은 법원이 도메인네임을 몰수(forfeit) 또는 취소하는 명령을 하거나 도메인네임을 상표권자에게 이전시키는 명령을 하는 경우에 한정된다는 것이다[§43(d)(2)(D)(ⅰ)]. 따라서 손해배상이나 변호사비용이 인정되지 않는다. 그러나 상표권자가 대물관할권에 기하여서만 소송을 제기하여야 하는 것은 아니며, 대물관할권 이외에 대인관할권에 기한 소송의 제기도 허용된다[§43(d)(2)(4)]. 또한 상표권자는 ACPA가 인정하는 구제수단 이외에 다른 민사소송이나 기타 허용될 수 있는 구제수단을 얻을 수도 있다[§43(d)(2)(3)].

(5) 도메인네임 등록기관의 의무 및 책임제한

대물관할에 따라서 연방 제1심 법원에 제소된 소의 訴狀에 대하여 서면에 의하여 통지를 받은 도메인네임 등록기관은 ACPA에 따라서 일정한 의무를 부담한다. 곧 등록기관은 도메인네임의 등록 및 도메인네임의 사용에 관한 법원의 통제 및 권한을 정하는 데 충분한 서류를 예치하여

야 한다. 또한 소송계류 중에, 법원의 명령에 의하지 않고서는, 도메인네임을 이전, 중지 기타 수정해서는 안된다[1125(d)(2)(D)(ⅰ)].

대물관할에 기한 상표권자의 소송제기와 이에 따른 법원의 처분과 관련하여 도메인네임 등록기관은 금지명령 및 금전적인 손해배상에 대하여 책임을 지지 않는다. 다만 책임을 지는 경우는 악의 또는 고의적인 무시(reckless disregard)인 경우에 한하며, 여기에는 법원의 명령을 의도적으로 따르지 않는 경우가 포함된다[§ 43(d)(2)(D)(ⅱ)].

# 제 4 장 기타 분야의 법령

## 제 1 절 스팸 메일

### 1. 스팸메일의 의의

전자우편(email)에 의한 광고는 전통적인 광고와 달리 비용이 매우 저렴하고 신속한 것을 특징으로 하므로, 수령자가 희망하지 않는 전자 메시지를 전세계상의 수많은 전자우편 이용자에게 송부한다. 이와 같이 온라인에 의한 직접적인 광고를 스팸메일(spam mail, 또는 junk email, bulk email, unsolicited · unwanted email)이라고 한다. 스팸메일에 대하여 인터넷서비스 제공자 및 개인들은 스팸메일을 보내는 자들의 블랙리스트를 작성하거나, 스팸메일의 명백한 출처가 되는 도메인네임을 걸러 내거나, 스팸메일의 배포를 방지하는 소프트웨어를 개발하는 등의 반응을 해왔다. 이에 대항하여 스팸메일을 보내는 자들은 이러한 소프트웨어에 의하여 자신들의 메시지가 봉쇄되는 것을 방지하기 위하여 자신의 도메인네임이나 주소를 은닉하고자 하였다. 이에 따라 미국에서는 많은 소송이 제기되고 있는 상태이며, 여러 주에서는 이러한 스팸메일을 규제하는 법을 제정하고 있고 연방법 차원에서도 여러 법안이 제안되었다.

### 2. 연방법 차원의 법안

#### (1) Inbox Privacy Act of 1999

연방법 차원에서 미국에서는 스팸메일에 관한 많은 법안이 제안되었다. 우선 1999년 Murkowski 상원의원이 제안한 Inbox Privacy Act of 1999[28]는 희망하지 않은 전자우편의 전송을 규제하고자 한 것이었다. 이 법안은 인터넷서비스 제공자와 그 고객이 원하지 않는 전자우편을 희망하는지 여부를 선택할 수 있도록 하였으며, "전자 우편의 수령자가 전자우편의 전송을 원하지 않는 요청을 한 경우에는 전자우편을 송부할 수

28) S.759, 106th Cong. (1999).

없다"고 규정하였다[2(a)(2)]. 또한 인터넷서비스 제공자가 법위반을 인지한 후 1년 이내에 손해배상을 청구하기 위하여 소송을 제기할 수 있도록 하였다. 그리고 미국의 연방거래위원회(FTC)가 "인터넷상에서 또는 인터넷에 의하여 판매와 서비스와 관련된 기망적인 행위와 관행을 정의하고 금지하기 위한 규칙을 제정"할 권한을 부여하고 있다. 뿐만 아니라 FTC가 법의 위반을 조사할 수 있는 권한도 부여하였으나, 이 법안은 연방의회를 통과하지는 못하였다.

(2) Unsolicited Electronic Mail Act of 2001

스팸메일과 관련된 최근의 법안은 Unsolicited Electronic Mail Act of 2001[29]이다. 이 법안은 원하지 않는 전자우편으로부터 개인, 가족, 인터넷서비스 제공자를 보호하기 위한 것으로서, 기망적인 전송정보를 포함하는 것으로서 원하지 않는 상업적인 전자우편을 발송한 것에 대하여 형사적인 처벌을 규정하고 있다(제4조). 또한 원하지 않는 상업적 전자우편의 수령자가 전자우편을 추가적으로 수령하고 싶지 않다는 것을 거부할 수 있도록 송신자의 주소를 포함하도록 송신자에게 의무지우고 있다[5(a)(3)]. 인터넷서비스 제공자가 원하지 않는 상업적 전자우편의 송부 또는 수령을 선의로 봉쇄하기 위한 조치를 취한 경우 연방법 및 주법 등에 의한 책임을지지 않는다고 규정함으로써[5(c)(1)], 인터넷서비스 제공자가 스팸메일을 봉쇄할 수 있는 광범위한 재량을 부여하고 있다.

이 법안은 법의 집행과 관련하여 FTC에게 광범위한 재량권을 부여하고 있다. 법의 위반이 발생하였다고 FTC가 믿는다면, FTC는 위반자에게 통지를 하고 위반자가 추가적으로 위반하는 것을 중지할 것을 요구하여야 한다[6(a)(1)-(2)]. 이러한 통지에 의하여 위반이 제지되지 않는다면 FTC는 위반자에 대하여 complaint를 보낼 수 있으며, 심리후에 통지의 요건을 위반하였다면 통지의 조건을 이행하도록 하는 명령을 발할 수 있다[6(a)(4)(B)]. 연방법원은 검찰총장의 청구에 의하여 FTC에 의한 통지의 이행을 명하는 명령을 발할 수 있다.

29) H.R.95.IH, 107th Cong. (2001).

희망하지 않는 상업적인 전자우편에 대해서는 사인(私人)이 소송을 제기할 수 있도록 하고 있다. 곧 전자우편의 수령자나 인터넷서비스 제공자는 주 및 연방법원에 (i) 위반을 중지시키기 위한 소송과 (ii) 위반으로 인한 손해배상을 받기 위한 소송을 제기할 수 있다[6(b)(1)]. 스팸메일로 인한 손해배상청구와 관련하여 수신자 또는 인터넷 서비스 업체에게 실제의 재산상의 손실액 또는 위반 건 수당 500달러를 청구할 수 있도록 하고 한 건당 총액 50,000달러를 넘지 못하도록 하고 있다. 그러나 만약 위반자가 반복적이거나 의도적으로 위반하였다면 손해가 3배까지도 배상될 수 있다[6(b)(2)].

이 법안은 주법이 이 법안과 일치하지 않는 한도에서 연방법이 우선적용된다고 규정하고 있다[7(b)]. 그러나 원하지 않는 상업적인 전자우편과 관련하여 주법에 의한 침해이론(tresspass) 및 계약법에 의한 민사적인 구제수단에 대해서는 연방법이 우선적용되는 것이 아니라고 함으로써, 이 법안의 연방법 우선적용의 원리(doctrine of preemption)의 적용은 불완전한 것이라고 할 수 있다.

### (3) CAN SPAM ACT of 2001

CAN SPAM ACT of 2001[30]은 상원에서 제안된 법안으로서, 상업적인 전자우편의 내용이 중대하게 또는 의도적으로 허위이거나 오해를 불러일으키는 메시지를 포함하고 있다는 것을 알면서 원하지 않는 상업적인 전자우편을 의도적으로 송부하는 자에게 형사적인 처벌을 가할 것을 규정하고 있다[4(a)]. 또한 허위이거나 오해를 불러일으키는 메시지나 기망적인 메시지의 송신을 불법화하고 있으며, Unsolicited Commercial Electronic Mail Act of 2001과 유사하게 원하지 않는 전자우편의 송신자가 자신의 주소를 포함시키도록 하고 있으며, 수신자가 우편을 수신한 이후 추가적인 수신을 거부하였는 데도 송신을 하는 것을 불법화하고 있다[5(a)]. 인터넷서비스 제공자와 관련하여 인터넷서비스 제공자가 일정 유형의 전자우편의 송신을 거부하는 등의 행위가 유효인지 아니면 무효인지에 대하여 이 법안이 아무런 영향을 미치지 못하도록 하고 있다.

30) S.630, 107th Cong. (2001).

이 법안은 법의 집행에 관하여 비교적 상세하게 규정하고 있다. 우선 법의 집행을 FTC에게 맡기고 있으며, 연방예금보험법(Federal Deposit Insurance Act) 등에 의하여서도 집행될 수 있으며, 주의 검찰총장이 금지명령 및 손해배상을 위하여 민사소송을 제기할 수 있도록 하고 있으며, 인터넷서비스 제공자도 금지명령 및 손해배상을 위하여 소송을 제기할 수 있도록 규정하고 있다[제6조].

### 3. 주법에 의한 스팸메일의 규율

미국의 많은 주들이 스팸메일을 규제하기 위하여 새로이 법을 제정하거나 기존의 법을 정교하게 하고 있다. 스팸메일에 관한 입법을 처음으로 제정한 주는 1997년에 제정한 네바다 주이다. 2001년 현재 약 18개의 주가 스팸메일에 관한 입법을 하고 있는 상태이며, 몇몇 주들이 입법안이 제안된 상태에 있다. 대부분의 주법들은 송부자를 허위로 나타내는 것에 대한 제재를 가하는 내용을 가지고 있으나, 주법의 내용은 차이점을 많이 가지고 있는 상태이다.

## 제 2 절 Internet Tax Freedom Act

### 1. ITFA의 의의 및 제정과정

1998년 10월 21일 클린턴 대통령이 서명한 Internet Tax Freedom Act(ITFA)[31]는 주·지역정부와 산업계간의 타협의 산물로서 2년여에 걸친 초당파적인 노력의 결과로서 제정된 것이다. ITFA의 주된 내용은 인터넷 접속과 인터넷 상거래에 주·지역정부가 1998년 10월 1일부터 2001년 10월 21일까지 3년간 조세를 과하는 것을 유예하는 것(moratorium), 인터넷의 초창기 형성·발전시기에 주 및 지역정부의 조세에 의하여 방해받지 않도록 하기 위한 국가적인 정책목표를 반영하는 것이었다. 만약 이 입법이 제정되지 않았더라면 3만개 이상의 주·지역정부에 의하여 전자상거래는 과세되었을 것이고 각기 다른 주·지역정

31) Pub. L. No.105-277, §§1100 et seq., 112 Stat. 2681, 2681-719 (1998).

부에 의하여 중복적으로 과세될 위험이 있었다. ITFA의 주된 목적은 능률적이고 공정한 조세정책의 개발, 곧 주요한 국제적인 상거래의 경로로서 인터넷의 발전에 부당한 방해를 하지 않고 주 및 지역정부의 수입원을 조정해주는 시스템의 개발이었다.

ITFA는 1997년 3월의 미국 연방하원의원인 Christopher Cox와 상원의원인 Ron Wyden이 법안을 제출하는 데에서 직접적으로 비롯되었다. 이 법안은 인터넷상에서의 조세를 전국적으로 유예시키는 법안이었고, 1998년에 양 법안에 대해서는 상원과 하원에서 많은 지지가 있게 되었고 National Governors' Association 등 많은 지지를 확대하게 되었다.

전자상거래에 관한 클린턴 행정부의 정책도 ITFA의 제정에 상당한 기여를 하였다. 클린턴 행정부는 1997년 7월의 "A Framework for Global Electronic Commerce"라는 보고서에서 전자상거래에 대한 접근방식에 관한 지도원리를 천명하였다. 이러한 지도원리에 해당하는 것으로는 민간분야의 주도적인 역할, 전자상거래에 대한 정부의 부당한 간섭의 배제, 전자상거래에 대한 정부의 최소한의 관여, 세계적인 견지에서의 전자상거래의 발달 및 전자상거래에 대한 조세의 중립성이었다. 이 보고서는 "미국은 전자상거래에 대하여 조세가 과하여져서는 안된다고 믿고 있으며, 인터넷상 행하여지는 상거래에 대한 조세는 이미 확립되어 있는 국제적인 조세의 원칙과 일치하여야 하며, 과세의 관할 및 2중과세를 회피하여야 하며, 실행하기에 간단하고 이해하기 편리하여야 한다"고 밝혔다. 또한 인터넷에서의 판매에 대한 조세가 추구하여야 할 원리로서, 첫째, 조세가 상거래를 왜곡하거나 방해하지 않아야 한다고 밝혔다. 곧 조세제도가 상거래의 유형에 따라 차별하거나 거래의 성격이나 위치를 변경시킬 동기를 발생시켜서는 안된다는 것이다. 둘째, 조세제도는 간단하고 투명하여야 한다고 밝혔다. 셋째, 조세제도는 미국 및 국제사회가 오늘날 사용하고 있는 조세제도와 조화하여야 한다고 밝혔다. 이 보고서는 주 및 지방정부가 전자상거래에 과세하는 방향으로 움직임으로써 전자상거래의 발전을 저해할 수 있다는 것을 염려하였고, 전자상거래에 관한 조세에 대하여 각 주 및 지역정부들이 통일적이고 간단한 접근방법을 취하기 위하여 협조할 것을 지지하였다. 1997년 7월에 발표된 이 보고서

는 전자상거래에 대하여 연방정부가 취하여야 할 접근방법을 설정하는 데 도움을 주었다. ITFA는 바로 그 첫 단계 중의 하나라고 할 수 있다.

## 2. ITFA의 주요내용

### (1) 과세의 유예

ITFA는 세 가지 유형의 조세에 대하여 과세를 유예하였다.[32] 첫 번째의 유예는, 1998년 10월 1일 이전에 조세를 부과하고 집행하지 않은 경우에 한하여, 인터넷에 접속하는 것에 대한 과세를 제한하는 것이었다. 따라서 AOL(American Online)를 비롯한 인터넷서비스 제공자가 인터넷에 접속시켜주는 대가로 고객에게 부과하는 월가입비에 대하여 주가 과세하는 것이 금지된다. 또한 이 규정은 교환되는 데이터의 양에 따라 과세하는 'bit 조세(bit tax)'를 금지시켰다.

둘째, 동일한 과세대상에 대하여 여러 기관이 과세하는 것(multiple tax)이 금지된다. 이러한 과세를 금지하는 것은 전자상거래에 대하여 여러 주가 과세하는 것을 방지하기 위한 것이다.

셋째, ITFA가 제한하는 세 번째 조세는 차별적인 조세(discriminatory tax)이다. 차별적인 조세는 유사한 과세를 하는 다른 그룹이나 행위 또는 재산을 평가하지 않고서 특정 그룹, 행위, 재산에 대하여 과세를 하는 것이다. ITFA는 전자상거래를 전통적인 상행위보다 호의적이지 않게 대우하는 것을 금지시키고 있다. 또한 ITFA는 주 외부에 존재하는 서버(server) 및 인터넷서비스 제공자에 대하여 과세의 기초가 되는 일정한 연관관계(nexus)를 주가 만들지 못하도록 제한하였다. 또한 주 외부의 컴퓨터서버를 이용한 원거리의 판매자에 대한 과세와 관련하여, ITFA는, 그 원거리의 판매자가 주와 연관관계가 있는지, 따라서 거래에 대하여 조세를 납부할 의무가 있는지를 결정하는 데 있어서 원거리 판매자의 컴퓨터서버에 구매자가 접속할 수 있는 유일한 능력만이 요소로서 주가 고려하였다면, 원거리의 판매자가 인터넷상에서 행한 판매에 대하여 그 주가 과세하는 것을 금지시켰다.

32) § 1101(a)(1)-(2), 112 Stat. at 2681-719.

이미 존재하고 있는 조세에 대한 예외규정(grandfather clause)을 제외하고는, 전자상거래에 대한 과세의 유예는 개별적인 주들이 모든 전자상거래 관련 행위에 대하여 과세하는 능력을 상당히 제한한 것이었다.

과세의 유예는 소급효를 가지고 있지 않으므로, ITFA가 시행되기 이전에 이미 발생한 조세 및 이러한 조세와 관련된 분쟁에 아무런 영향을 주지 않는다. 이것은 당시 주정부의 조세에 대한 소송에 휘말려 있는 인터넷서비스 제공자가 ITFA에 따른 조세의 면제를 주장하는 것을 방지하기 위한 것이었다.

(2) 예 외

전자상거래에 대하여 이미 존재하였던 주·지역정부의 과세는 ITFA에 의한 과세금지로부터 면제되었다. 곧 1998년 10월 1일 이전에 일반적으로 부과되고 사실상 집행되고 있었던 조세에 대하여 ITFA는 과세의 금지에 대한 예외를 허용하고 있다[§1101(a)(1)]. ITFA가 제정될 당시 약 12개의 주가 전자상거래에 대하여 과세를 하고 있었다. 만약 12개의 주에서 전자상거래에 대한 과세가 금지될 경우 주들이 상실하게 될 조세수입은 매년 5천만 달러라는 통계와 5억달러라는 통계가 있다. 또한 인터넷상으로 주문되거나 인도되는 상품에 대하여 판매세(sales tax)를 부과하는 것을 허용하고 있다. 이러한 판매세는 통신판매 등 인터넷상의 판매에 상응하는 판매에 대하여 비차별적으로 과세되어야 한다. 차별적인 과세의 금지는 인터넷과 관련된 특정행위(예컨대 웹호스팅, 인터넷 검색행위, ISP에 대한 조세 등)에 대하여 각 주가 과세하는 것을 금지시키는 것이다.

ITFA는 주·지역정부에 의한 조세에 대해서만 적용되며, 연방정부에 의한 조세에는 적용되지 않는다. 그러나 이 법은 조세가 유예되는 기간동안 연방정부에 의한 조세가 부과되는 것을 금지하는 선언을 포함하고 있다.

(3) 권고위원회의 구성

ITFA는 전자상거래에 대한 조세를 연구하고 연구결과를 의회에 보고하도록 하기 위하여 19명의 위원으로 구성된 권고위원회(Advisory Com-

mission)를 구성하도록 하고 있다. 이 위원회는 의회와 연방·주·지역 정부가 임명한 대표와 전자상거래 산업계의 대표로 구성된다. 이 위원회는 인터넷을 이용한 거래와 인터넷에 대한 접속 및 기타 이에 상응하는 주내·주간·국제적인 판매행위에 대한 연방·주·지역·국제적인 과세 및 관세에 대하여 연구를 할 의무를 부담한다[1102(g)(1)]. 이 위원회의 주요 목적은 인터넷접속서비스, 온라인서비스, 인터넷을 이용한 통신 및 거래 등이 다른 유형의 판매에 상응하는 기술중립적인 방식으로 대우될 것을 보장하는 주모범법안을 검토하는 것이었다.

(4) 국제적인 측면에서의 비과세정책의 천명

ITFA는 조세로부터의 인터넷의 보호가 국제적으로 확대되어야 한다는 미국 의회의 정책목표를 규정하는 조항을 포함하고 있다. 끝 이 조항은 미국의 대통령이 인터넷에 외국의 관세, 무역장벽, 기타 장애가 없도록 하기 위하여 외국과 협의할 것을 지시하고 있다[1203]. 또한 ITFA는 미국의 대통령이 세계무역기구(WTO) 등과 같은 기구에 의하여 외국과 양자간·지역적·다자간 조약을 모색할 것을 주문하고 있다. 이러한 조항을 통하여 ITFA는 미국에서 금지되고 있는 동일한 유형으로부터 인터넷상에서의 활동을 보호하고, 전자상거래의 발전을 촉진하고자 하였다.

### 3. ITFA 이후

2001년 상반기 현재 미국의 의회에서는 인터넷상에서의 조세와 관련하여 약 12개의 법안이 제출되어 있는 상태이다. 이러한 법안이 올해의 회기(제106차)에 모두 통과될 것은 아니지만, ITFA가 규정하고 있는 과세의 유예를 연장하는 법안이 제출되어 있는 것에 주목할 필요가 있다. Internet Tax Elimination Act(H.R. 3252), Internet Nondiscrimination Act(H.R. 3709), Extension of the ITFA Moratorium Through 2001(S. 2225) 등이 그것이다. 이러한 법안들은 인터넷상에서 판매되는 상품이나 서비스에 대한 주 및 지역정부의 과세를 전면적으로 금지하거나, ITFA의 과세유예를 영구적인 것으로 하거나, 현재의 과세유예를 5년간 더 연장하는 것 등을 내용으로 하고 있다.

# 제 3 절 프라이버시

## 1. 서 론

인터넷 분야에서 프라이버시(privacy)는 상당히 많은 관심을 끌고 있다. 인터넷상에서 공개될 수 있는 개인적인 데이터로서 이용자가 제공한 데이터(성명, 전자우편의 주소, 사회보장번호, 신용카드번호 등), 이용자가 웹사이트를 방문한 기록에 관한 정보(검색한 웹사이트, 구매한 내용, 검색한 광고 등), 쿠키(cookies, 이용자가 최근에 방문한 웹사이트에 기초하여 이용자가 선호하는 웹사이트의 기록) 등을 들 수 있다. 개인에 관한 이같은 여러 자료가 타인에 의하여 수집되어 인터넷상 공표됨으로써 개인의 프라이버시가 침해될 가능성이 매우 높아졌다. 이에 따라 미국에서는 정부에 의한 규제, 연방입법안의 제출, 주법에 의한 규제 등 다양한 해결책이 논의되고 있는 상황이다.

## 2. 연방정부에 의한 규제

미국의 연방거래위원회(FTC)는 인터넷상에서의 프라이버시 및 불공정하고 기만적인 관행이어서 연방거래위원회법 5(a)를 위반한 것에 관하여 규율할 권한을 적극적으로 주장해왔다. 1998년 FTC는 소비자의 프라이버시를 보호하기 위하여 필요한 네 가지 요소로서, (ⅰ) 온라인상 소비자의 개인적인 정보가 어떻게 사용되는지에 관한 소비자에 대한 통지, (ⅱ) 소비자의 개인적인 정보가 사용될 것인지 여부와 어떻게 사용될 것인지에 대한 소비자의 선택, (ⅲ) 개인적인 정보에 대한 보안, (ⅳ) 정확성을 기하기 위한 소비자의 개인적인 정보에 대한 접근 등을 발표하였다. 이외에도 FTC는 온라인상 개인적인 정보의 수집, 개인적인 정보의 공개 및 판매, 개별적인 이용자 정보의 이용 등에 대하여 사적인 소송을 제기하였다.

## 3. 연방법 및 주법에 의한 제소

최근 몇 년 동안에 인터넷 회사가 데이터를 수집하는 관행에 대하여 여러 소송이 제기되었다. 이러한 소송들은 전자적인 통신 또는 통신시스

템에 대한 접근 및 공개를 규율하는 연방법에 기초하는 것이었다. 이와 관련된 연방법으로서는 (i) 통신의 어느 당사자로부터 동의를 얻지 않고서 사적인 통신내용을 듣거나 관측하는 것을 불법화시키는 Electronic Communications Privacy Act of 1986 (ECPA), Title I, 18 U.S.C. §2510 이하 (Wiretap Act), (ii) 전자적으로 저장된 통신의 내용을 공개하는 것, 곧 전자통신서비스가 정부에 제공할 수 있는 정보를 엄격히 제한하고 있는 ECPA Title II, 18 U.S.C. §2701 이하 (Stored Information Act), (iii) 제3자의 컴퓨터에 있는 데이터에 허락을 받지 않고 접근하는 것을 불법화하는 Computer Fraud and Abuse Act [18 U.S.C. §1030) 등이 있다.

인터넷상에서의 프라이버시에 대한 침해는 주법상으로 규율될 수 있는데, 그 근거는 판례법상의 프라이버시의 침해 및 불공정한 영업관행(unfair business practices)이다.

### 4. Children's Online Privacy Protection Act(COPPA)[33]

1998년 10월 21일 제정되어 2000년 4월 21일부터 발효한 COPPA는 13세 미만의 어린이로부터 정보를 온라인상 수집하고 이용하는 것을 규제하기 위한 법이다. 이 법은 13세 미만을 겨냥한 웹사이트의 운영자로 하여금 (i) 정보에 관한 웹사이트의 관행을 부모에게 통지하고, (ii) 어린이로부터 개인적인 정보를 수집, 이용, 공개하는 것에 관하여 사전에 부모의 동의를 받으며, (iii) 요청이 있는 경우, 어린이로부터 수집된 개인적인 정보를 부모가 검토할 수 있도록 하며, (iv) 요청이 있는 경우, 이미 수집된 개인적인 정보를 다시 사용하거나 그 어린이로부터 다시 개인적인 정보를 수집하는 것을 부모가 방지할 수 있어야 하며, (v) 게임, 상품제공, 기타 행위에 어린이가 온라인상 참여하기 위하여 개인적인 정보를 수집하는 것을 그러한 행위를 위하여 합리적으로 필요한 정보에 제한시키며, (vi) 개인정보의 비밀성, 보안, 무결성(integrity)을 보호하기 위한 합리적인 절차를 마련하고 유지할 것을 요구하고 있다.

33) 15 U.S.C. §§6501-6505.

이 법은 그 위반에 대하여 개인에 의한 민사소송을 명확하게 규정하고 있지 않으며, FTC 및 주검찰총장에 의하여 집행될 수 있다. 1999년 10월 20일 FTC는 COPPA를 집행하기 위한 규칙[34]을 발표하였는데, 2000년 4월 21일에 발효한 이 규칙은 일반적으로 어린이를 겨냥한 상업적 웹사이트 및 13세 미만의 어린이에 의하여 사용되고 있다고 사실상 인지하고 있는 상업적 웹사이트로 하여금 어린이로부터 온라인상 정보를 수집하기 이전에 입증될 수 있는 부모의 동의를 얻도록 하는 것이다.

(1) 적 용

이 규칙에 의하면, 웹사이트의 운영자는 웹사이트 방문자로부터 또는 방문자에 관하여 개인적인 정보를 수집하거나 유지하는 모든 상업적 웹사이트 또는 온라인서비스로 정의되며, 여기에는 웹사이트나 온라인 서비스를 통하여 상품이나 서비스를 판매하는 자 또는 실체(entity)가 포함된다고 광범위하게 정의하고 있다.

(2) 어린이를 겨냥하는 것

COPPA가 적용되는 어린이를 겨냥한(directed to children) 것인데, FTC는 이를 고려하기 위한 요소로서, 대상, 시각 또는 청각적인 내용, 모델의 나이, 웹사이트에서 사용되는 언어, 웹사이트에 나타나 있는 광고 및 판매촉진책, 만화영화의 등장인물의 사용 또는 어린이를 위주로 하는 행위 및 동기, 웹사이트가 의도하는 방문자 및 방문자의 사실상의 구성 등이다.

(3) 통지와 동의

부모의 동의는 입증될 수 있는(verifiable) 것이어야 하는 데, 이러한 부모의 동의는 웹사이트가 어린이로부터 정보를 수집하기 이전에 부모가 웹사이트에 의한 정보수집의 관행을 통지받았고 어린이의 개인정보를 수집, 이용, 공개하는 것에 동의하도록 하기 위한 모든 합리적인 노력을 의

34) 16 C.F.R. Part 312.

미한다. FTC는 전화나 팩스에 의하여 동의를 받는 것을 인정하였으나, 전자우편만으로는 부모의 동의가 있었다고 입증될 수 있는 것이 아니다.

(4) 위반 및 효과

FTC 규칙에 의하면 COPPA 및 실행규칙을 위반한 것에 대하여 FTC가 소송을 제기하고 민사적인 처벌을 가할 수 있도록 하고 있다.

(5) 예외규정

COPPA는 온라인산업이 자율적인 가이드라인(self-regulatory guidelines)을 FTC에 제출하는 것을 허용하고 있는데, 이러한 가이드라인을 FTC가 승인하고 이를 준수하는 경우, COPPA의 집행으로부터 면제될 수 있다. 현재까지 FTC가 승인한 것으로는 Children's Advertising Review Unit (CARU) of the Council of Better Business Bureau 및 ESRB Privacy Online이다.

5. 기타의 규정

(1) 금융정보

FTC는 2000년 5월 Gramm-Leach-Bliley Act[35]의 요구에 따라 프라이버시에 관한 규칙[36]을 발간하였다. 이 규칙은 2000년 11월 13일 발효하였으며, 2001년 7월까지 이를 완전히 준수할 것이 요구되었다. Gramm-Leach-Bliley Act는 금융기관이 비공개적인 개인정보(non-public personal information)를 공개하는 것과 관계되는 입법이다. 여기에서의 금융기관은 비은행금융기관을 포함하여 광범위하게 정의되고 있는데, 고객의 기록과 정보의 비밀 및 보안을 확보하여야 한다. 이러한 금융기관은 비공개적인 개인정보를 관련기관 등에 공개하는 것에 관한 금융기관의 정책방침 및 관행을 고객에게 공개하여야 한다. 또한 이러한

35) 15 U.S.C. §§6801-6809.
36) 16 CFR 313.1 이하.

정보를 금융기관과 관련되지 않는 제3자에게 공개하기 이전에 이를 고객에게 통지하여야 하며 고객이 통지를 원하지 않는 것을 선택할 수 있어야 한다. 이 법을 집행하고 이 법에 따라 규칙을 제정할 수 있는 정부기관은 연방증권거래위원회(SEC), 연방준비국(Federal Reserve Board), 재무부, FTC 등이다.

(2) 환자의 의료기록

2000년 12월 20일 당시의 클린턴 미국 대통령과 보건후생부장관은 개인적인 건강기록의 프라이버시를 보호하기 위한 기준을 처음으로 제정하였다. 이 규칙[37]은 즉시 발효하였으나 이를 완전히 이행하는 것은 2003년 2월 21일까지이다.

(3) Cable Communications Policy Act

온라인상의 프라이버시를 위한 것은 아니었으나 온라인에 의한 서비스를 제공하는 경우에 적용될 수 있는 프라이버시 입법으로서는 Cable Act [47 U.S.C.§551]이다. 케이블 모뎀의 사용이 증가함에 따라 케이블 TV 서비스를 제공하였던 회사들이 인터넷서비스 제공업자가 될 수 있다. 이 경우 47 U.S.C.§551은 케이블 TV 가입자를 보호하는 데 케이블 모뎀이용자를 보호하는 것으로 해석될 수 있다. 이 규정은 케이블 운영자가, 사전에 서면 또는 전자적인 동의를 받지 않는 경우에는, 가입자에 관한 개인적인 정보를 수집하기 위하여 케이블 시스템을 사용하는 것을 금지하고 있다[555(b)(1)]. 또한 사전에 서면 또는 전자적인 동의를 받지 않는 경우에는, 가입자에 관한 개인적인 정보를 공개하는 것을 금지하고 가입자나 케이블 운영자 이외의 자가 그러한 정보에 허락을 얻지 않고 접속하는 것을 방지하기 위하여 필요한 조치를 취하도록 하고 있다[555(c)(1)]. 이 규정은 몇 가지 예외를 규정하고 있는데, 예컨대 케이블 서비스나 기타 케이블 운영자가 가입자에게 제공하는 서비스와 관련된 합법적인 업무를 행하거나 법원의 명령에 의하여 필요한 경우를 들

37) 45 C.F.R. Parts 160 & 164.

수 있다[555(c)(2)]. 이 규정은 이 규정을 위반함으로써 케이블 운영자의 행위에 의하여 손해를 입은 자가 소를 제기할 수 있는 권리를 부여하고 있다[555(f)(1)].

(4) 기 타

인터넷상의 프라이버시를 규율할 수 있는 기타의 법으로서는 Video Privacy Protection Act[18 U.S.C. § 2710], Right to Financial Privacy Act[12 U.S.C. § 3410 이하], Fair Credit Reporting Act [15 U.S.C. § 601 이하], Privacy Act of 1974[5 U.S.C. § 552a] 등을 들 수 있다. 이같은 법들은 온라인상의 프라이버시를 보호하는 것이 아니었으나, 온라인상의 영업이 확대됨에 따라 적용될 수 있는 법이다.

### 6. 프라이버시를 보호하기 위한 법안

2001년 중순 현재 (107th Congress) 인터넷상에서 개인정보를 수집, 이용, 판매하는 것을 규율하기 위한 여러 법안이 제출되어 있는 상태이다. 이러한 법안의 대표적인 예는 Bankruptcy Reform Act of 2001 (S. 420), Online Privacy Protection Act of 2001 (H.R. 89), Consumer Online Privacy Disclosure Act (H.R. 347), Consumer Internet Privacy Enhancement Act (H.R. 237), Social Security On-line Privacy Protection Act (H.R. 91) 등이다.

## 제 4 절 컨텐츠 규제

### 1. 서 론

1997년 7월 미국정부는 "A Framework for Global Electronic Commerce"라는 이름의 보고서에 의하여 인터넷에 대한 자국의 정책방침을 밝혔다. 이 보고서는 컨텐츠의 규제와 관련하여 "미국정부는 세계적으로 정보가 가장 광범위하게 흘러가는 것을 지지한다.... 전통적인 방송매체와는 달리, 인터넷은 불쾌하고 부적절하다고 여겨지는 컨텐츠로부터

이용자 자신과 어린이들을 방어할 수 있는 더 많은 기회를 제공한다... 그렇다면 이 같은 불쾌하고 부적절한 컨텐츠를 효과적으로 걸러내는 기술이 이용될 수 있는 한도에서, 라디오 및 텔레비전에 전통적으로 적용되었던 컨텐츠 규제는 인터넷에 적용될 필요성이 없다. 사실상 불필요한 규제는 인터넷의 성장과 다양성을 억제할 수도 있을 것이다"라고 하면서 인터넷에 대한 '방임정책(hands-off policy)'을 천명하였다.[38]

미국의 상무성도 "미국정부는 정부가 규제하지 않는, 시장이 주도하는 인터넷의 발전을 지지한다. 이것은 정부가 인터넷을 규율하기 위하여 규범을 제정하는 것을 회피하여야 하는 것을 의미한다. 가능한 한, 인터넷 행위에 대한 규범은 정부의 규제가 아닌 민간의 총체적인 행위에 의하여 규정되어야 한다. 이러한 규범의 목적은 소비자가 프라이버시를 보호하고, 컨텐츠를 통제하며, 부적절한 상거래 행위로부터 자신을 보호할 수 있는 것이어야 한다. 경쟁 및 소비자의 선택(consumer choice)이 인터넷 상거래의 지도원리가 되어야 한다"라고 하면서 역시 방임적인 정책방침을 밝혔다.[39] 미국정부는 위의 보고서에서 산업계가 경쟁적으로 등급제(rating system)를 실시하거나 일정한 컨텐츠를 여과하는 기술이나 나이를 증명토록 하는 시스템과 같은 사용하기가 용이한 기술적인 해결책의 개발을 지지한다고 하였다.[40]

인터넷상에서의 미국의 컨텐츠 규율을 전반적으로 보면, 어린이를 보호하는 규범을 제외한다면 대체로 미국정부는 인터넷을 규율하고 있지 않은 것으로 보인다. 현재 인터넷을 관리하는 부서가 없으며 미국 정부가 방임적인 정책방침을 취하고 있기 때문에, 의회가 장래에 입법하겠다는 일종의 위협에 의하여 산업계가 자발적으로 규제하는 것을 유도하고 있는 상태이다. 인터넷의 컨텐츠 규율에 대한 미국의 방임적인 방침은 불필요하고 과도한 규율이 인터넷의 발전을 저해할 수 있다는 것에도 근거하고 있으나, 자칫하여 광범위하게 규율한 경우에는 미국 헌법상의 표현의 자유에 관한 규정을 위반하는 것에도 기인하고 있다. 과거에 컨텐

38) A Framework for Global Electronic Commerce, at 3.
39) Department of Commerce, THE EMERGING DIGITAL ECONOMY, app. II, at A2-1.
40) A Framework for Global Electronic Commerce, at 3.

츠를 규율하는 입법에 대하여 위헌이라는 주장이 행하여지고 실제로 위헌판결이 난 것을 보면 이를 알 수 있다. 따라서 현재 컨텐츠에 대하여 규제할 수 없으므로 미국 정부는 인터넷의 규제라는 쟁점에 대하여 산업계에 의한 입법제안을 기다리고 있는 상태라고 할 수 있다.

### 2. Protection of Children from Sexual Predators Act

자유방임적인 정책방침에도 불구하고, 미국의 의회는 인터넷 산업계가 표준을 채택하는 것을 기다리지 못하고 1998년 회기에 여러 인터넷과 관련된 입법을 하였다. 대부분의 새로운 입법은 어린이를 보호하는 것에 초점이 맞추어져 있으며, 포르노나 음란물에 관한 기존의 입법도 인터넷에 적용될 수 있으나, 새로운 입법은 인터넷에서의 행위를 규제하기에 더 적합한 것이었다. 예컨대 Protection of Children from Sexual Predators Act[41]는 성적 가해자로부터 어린이를 보호하는 당시의 법을 인터넷상에서 적합하게 적용될 수 있도록 하고 법을 강화한 것이다. 또한 이 법은 어린이의 보호에 대하여 ISP에게 일정한 요건 및 책임을 가하였는데, 이 법은 ISP의 서버를 통하여 발생하는 어린이 포르노와 같이 어린이를 이용하는 것을 ISP가 보고토록 하였으며, 음란한 자료를 16세 이하라고 알려진 개인에게 이를 알면서 전송하는 것을 금지시키고 있다. 물론 ISP가 이용자들의 컨텐츠를 감시할 것은 요구되지 않으며, 이 법을 준수하려는 선의로 행위를 한다면 ISP는 민사책임으로부터 보호된다.

### 3. COPA

#### (1) CDA

인터넷상에서는 상당히 많은 정보가 이용될 수 있으나, 그 성격상 음란물을 비롯한 성적인 정보가 넘치는 것도 부정할 수 없는 사실이다. 미국의 법원들은 인터넷에 대하여 음란성(obscenity)에 관한 법을 인터넷

41) Pub. L. No.105-314, 112 Stat. 2974.

에 적용하기 시작하였으나, 미국의 의회는 인터넷이 광범위하게 이용될 수 있음으로써 청소년들에게 해로운 자료에 접근할 기회가 제공되었다는 것을 인식하여 Communications Decency Act of 1996(CDA)[42]을 제정하였다. Telecommunications Act of 1996[43]의 조항을 규정하는 이 입법의 의도는 인터넷상에서 포르노그라피와 유해한 자료의 흐름을 정지시키는 것이었으며, 어린이가 접근할 수 있는 음란하거나 명백하게 불쾌한 자료를 인터넷상에 이용할 수 있도록 하는 것을 중범죄(felony)로 규정하였다.[44]

(2) COPA의 제정

이 법이 제정된 후 즉시 미국의 시민단체인 ACLU(American Civil Liberties Union)는 이 조항의 집행을 방지하기 위하여 소송을 제기하였고, 1996년 2월 15일 연방 제1심법원은 이 조항의 집행을 정지시켰고, 1996년 6월 11일 헌법상의 표현의 자유에 기초하여 이러한 예비금지명령을 설명하는 판결을 하게 되었다.[45] 1997년 6월 26일 미국 연방대법원은 위의 조항이 위헌이라고 하여 하급법원의 판결을 인정하였다.

음란한 자료에 관한 CDA의 규정이 위헌이라고 판시되자 미국 의회는 Child Online Protection Act(COPA)[46]를 제정하게 되었다. 이 법안에 대하여 미국 법무부의 Acting Assistant Attorney General이 헌법상의 문제가 있다고 경고하였으나, 클린턴 대통령은 1998년 10월 21일 이 법안에 서명하였다. COPA는 웹을 통하여 자료를 배포하는 업체로 하여금 해로운 자료에 대한 접근을 성인에게 제한할 것을 요구하고 있다[47 U.S.C. §231 (a)]. COPA에 의하여 Communications Act of 1934를 개정하는 기초로서 의회는 (i) 어린이의 감독, 보호, 양육은

42) Pub. L. No.105-277, div. C. tit. XIV, 112 Stat. 2681 (47 U.S.C. §231 (Supp. V. 1999)).
43) 47 U.S.C. §§151-641 (Supp. II 1996).
44) 47 U.S.C. §223 (a), (d).
45) ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996).
46) 17 U.S.C. §231.

부모의 책임이지만, 인터넷이 광범위하게 이용됨으로써 부모의 감독이나 통제가 좌절될 수 있으며, (ii) 해로운 자료를 청소년에게서 봉쇄함으로써 청소년의 육체적 및 심리적 복리를 보호하는 것은 정부의 이익[47]이 되며, (iii) 온라인산업이 어린이에게 해로운 자료에 접근하는 것을 부모와 교육자가 억제하는 것을 도울 수 있는 진보적인 방법을 개발하였으나, 온라인산업은 웹상에서 해로운 자료에 접근하는 청소년 문제에 대하여 전국가적인 해결책을 제공한 것이 아니었으며, (iv) 정부의 이익을 충족하기 위하여 가장 효과적이며 가장 제한적이지 않은 방법은 해로운 자료를 그 출처단계에서 배포하는 것을 금지하여 그 출처자에게 정당한 방어수단을 제공하는 것이며, (v) 인터넷상에서의 해로운 자료에 어린이가 노출되는 것으로부터 보호하기 위한 방법을 계속 모색할 필요가 있다는 것을 지적하였다.

이에 기초하여 미국 의회는 47 U.S.C. §231을 통과시켰는데, 이 조항에 의하여 상업적 웹운영자는 청소년에게 해롭다고 여겨지는 자료에 대한 접근을 제한할 것이 요구된다. COPA의 Title I 은 웹 페이지 발간자에게 자료를 평가하고 해로운 자료가 청소년에게 도달하지 않도록 제한하기 위한 수단을 강구할 것을 요구하고 있다. COPA의 TitleⅡ는 부모의 동의없이 어린이로부터 개인적 정보를 수집하는 것을 프라이버시의 침해로 규정하고 있다.

(3) 위반에 대한 구제수단

"청소년에게 유해한(harmful to minors)" 이라는 기준을 위반하는 자료를, 청소년에게 유해하다는 것을 인지하고서(knowingly) 올려놓는 자는 COPA를 위반하는 것이고 형사적인 책임(5만 달러까지의 벌금형 및 최대 6개월까지의 징역)을 부담한다. COPA를 의도적으로 위반한 경우(intentional violation) 그 책임은 가중된다. 위반자는 이러한 형사적인 책임 이외에 민사적인 책임(각 위반에 대하여 5만 달러)을 질 수도 있다.

47) 정부의 이익(compelling government interest)이라는 개념은 연방정부가 입법을 위한 정당한 기초가 되는 것임.

(4) 정의규정

COPA에 따라 기소될 수 있는 웹 페이지는 상업적인 목적 또는 청소년에게 유해한 통신을 이용하게 하는 영업에 종사하는 페이지에 한정된다. "상업적인 목적(commercial purpose)" 또는 "영업에 종사한다(engaged in the business)"는 규정은 웹에 자료를 올리거나 올리기 위하여 자료를 요청하는 자 또는 정규적인 영업으로서 이러한 행위에 시간이나 주의 또는 노동을 전적으로 투자하는 자이다. 인터넷 연결서비스를 제공하는 것만으로는 상업적인 목적을 위한 웹의 사용이 되지 않으며, 인터넷서비스 제공자와 검색엔진의 웹페이지는 상업적인 목적으로부터 제외된다.

COPA가 보호하고자 하는 "청소년(minors)"은 17세 이하의 자로 정의되며, "청소년에게 해로운"이라는 기준은 외설적이거나(obscene) 다음의 세 가지 요건을 갖추는 모든 종류의 통신, 그림, 이미지, 그래픽이미지 파일, 글, 녹음, 서면 기타 자료로 정의된다. 세 가지 요건으로서는, (ⅰ) 평균인이, 현대사회의 기준을 적용하여, 문제된 자료를 전체적으로 그리고 청소년에 관하여 고려하여 음란한 것에 호소하거나 이를 선동하는 것이라고 여기는 경우, (ⅱ) 자료가 명확하게 불유쾌한 방식으로 주법에 특별하게 정의된 성적인 행위를 설명하거나 묘사하는지 여부, (ⅲ) 전체적으로 보았을 때 자료가 청소년에 대하여 진지한 문학적, 예술적, 정치적, 과학적 가치가 있는지 여부이다.

(5) 위원회의 구성

COPA는 청소년이 해로운 인터넷 자료에 접근하는 것을 감소시킬 수 있는 방법을 연구하기 위한 목적으로 온라인상의 어린이의 보호에 관한 위원회(Commission on Online Child Protection)를 설치하도록 하고 있다. 이 위원회의 목적은 청소년이 해로운 자료에 접근하는 감소시키는데 도움이 되는 기술적 방법 및 기타 방법을 연구하는 것이다. 이 위원회가 찾아내는 방법은 이러한 조치를 취하였는데 COPA에 따라 제

소된 자에 대한 방어수단이 될 수 있다. 또한 위원회의조사사항은 어린이를 해로운 자료로부터 보호하기 위한 입법적인 권고의 기초가 된다. 이 위원회는 온라인산업에 종사하거나 인터넷상에서의 자료의 여과에 관한 토론에 연관된 18명의 위원으로 구성된다. 이 위원회는 2000년 11월 30일까지 의회에 보고서를 제출하기로 규정되어 있다.

(6) COPA의 발효 이후

COPA에 대하여 미국 대통령이 서명한 바로 다음날인 1998년 10월 22일 ACLU를 비롯한 여러 원고들은 COPA가 위헌이라고 소송을 제기하였다. 1999년 2월 연방 제1심법원 판사는 COPA가 헌법상의 표현의 자유(First Amendment)를 위반하였다는 실질적 가능성이 있다고 판시하고 금지명령을 내리게 되었다.[48] 그리고 1998년 11월 19일 연방 제1심법원은 원고의 임시금지명령의 신청을 허용하였다. 이러한 금지명령은 제3연방 항소법원(3rd Circuit Court)에 의하여 승인되었다.[49] 법원은 COPA에 의하여 자발적인 검열(self-censorship)이 행하여지는 결과가 초래되고 따라서 어른을 위하여 보호되는 표현에 부담을 가하는 것이 입증될 수 있다고 판시하였다. 곧 신용카드를 요구하거나 기타 어른임을 입증토록 하는 화면을 요구함으로써 (헌법상) 보호되고 있는 통신에 종사하는 웹사이트 운영자의 의욕을 경제적으로 저하시킬 것이라고 하였다. 정부는 청소년을 보호하기 위한 이익(기본권을 제한을 정당화하기 위한 근거로서의 compelling interest)을 가지고 있지만, COPA는 기본권인 표현을 자유를 제한하기 위하여 미국법원에서 사용되어 왔던 기준으로서(특수한 목적에 적합하게) 협소하게 규정되었다거나 가장 제한적인지 않은(least restrictive) 수단을 이용한 것이 아니라는 것이다. 이것은 청소년들이 신용카드를 합법적으로 소유할 수 있다거나, 청소년들이 외국의 웹사이트를 통하여 COPA가 제한하고자 하였던 자료에 접근할 수 있다거나, http 이외의 컴퓨터 규약(protocol)이 사용되거나(유

48) ACLU v. Reno, 31 F. Supp. 473 (E.D. Pa. 1999) (Reno II).
49) ACLU v. Reno, 217 F.3d 162 (3rd Cir. 2000).

해한 자료를) 봉쇄하거나 여과시키는 소프트웨어가 이용될 수 있다는 것에 의하여 예시될 수 있다는 것이다.

### 4. 기 타

위에서 논의한 입법 이외에도 인터넷상의 컨텐츠를 규율하기 위하여 여러 법안이 제출되어 있는 상황인데, 예컨대 Family Friendly Access Act of 1997 및 Internet Freedom and Child Protection Act of 1997은 ISP로 하여금 유해한 컨텐츠를 걸러내도록 하기 위한 소프트웨어를 소비자들에게 제공토록 요구하고자 한다. 또한 Communications Privacy and Consumer Empowerment Act는 ISP가 부모들에게 일정한 권한을 주도록 요구할 것이며, E-Rate Policy and Child Protection Act는 각급 학교 및 도서관이 어린이에게 적절하지 못한 자료에 어린이들이 접근하는 것에 관한 방침을 세우도록 할 것이다. Safe Schools Internet Act of 1998은 인터넷 서비스를 위하여 연방정부로부터 자금을 지원받는 공공의 학교 및 도서관이 적절하지 못한 컨텐츠를 봉쇄하는 소프트웨어를 설치하도록 요구할 것이다.

## 제5절 암 호

암호와 관련하여서는 정보산업에 종사하는 업체가 강력한 암호프로그램을 가질 필요성과 법을 집행하는 측이 디지털 송신에 대한 접속을 할 필요성이 있는 보안상의 이유간에 딜레마가 생긴다. 또한 암호에 관하여 세계 최고수준의 기술을 가진 미국은 암호의 수출을 규제하고자 함에 반하여 암호업체는 이를 수출하려는 이해관계가 대립되어 왔다. 1999년 9월 클린턴 행정부는 암호화된 일정한 메시지를 읽기 위하여 필요한 수단을 법집행기관에게 제공하는 동시에 암호기술의 수출에 관한 통제를 완화시키는 보안 및 프라이버시에 관한 새로운 정책을 발표하였고, 이에 의하여 제안된 법안이 Cyberspace Electronic Security Act(CESA)이다. 이 법안은 64비티의 암호제품이나 소프트웨어를, 특정국가(북한, 이라크 등)를 제외하고 수출하는 것을 허용하는 법안이었다. 또한 CESA

는 암호와 관련된 사이버범죄를 법집행기관이 조사하는 것을 강화시켰다. 따라서 CESA는 법을 집행하기 위한 수단을 제공함으로써 암호의 수출허용을 약화시켰다. 암호에 관하여 좀더 균형적인 법안으로 제안된 것은 Security and Freedom Encryption Act(SAFE)이다. 이 법안은 정부보다는 암호와 관련된 산업에 더 호의적인 법안이었다.

## 제 6 절 인터넷 도박

### 1. 인터넷 도박을 금지하는 미국의 법률

미국은 인터넷 도박에 대하여 금지하는 엄격한 정책을 채택하고 있다. 미국의 법무부는 인터넷상에서의 도박은 최소한 네 개의 연방법에 의하여 불법이라고 주장하고 있다. 이러한 연방법으로서는 Interstate Transportation of Wagering Paraphernalia Act, Professional and Amateur Sports Protection Act, Interstate and Foreign Travel or Transportation in Aid of Racketeering Enterprises Act 등을 들 수 있다.

### 2. Wire Act

인터넷 게임을 금지하는 가장 중요한 입법은 Wire Act인데, Wire Act는 게임 영업을 하고자 하는 자가 전신(wire) 시설을 사용하는 것을 금지하고 있다(18 U.S.C. § 1084). 따라서 Wire Act는 인터넷 카지노를 금지할 가능성이 있는 입법이라고 할 수 있다. 곧 Wire Act에 의하여 어떠한 게임을 위하여 인터넷을 이용하는 것이 금지될 수 있다. 이에 해당하는 규정은 "도박업무에 종사하는 자가 도박에 건 돈이나 물건 또는 이러한 것을 스포츠경기 등에 돈을 거는 것을 도와주는 정보를 전송하기 위하여 전신통신시설을 이용하는 경우 누구든지 이 법에 의하여 벌금 또는 2년 이하의 징역에 처한다"고 하고 있다[18 U.S.C. § 1084]. 따라서 금지되는 행위는 도박업에 종사하는 자가 도박을 용이하게 하기 위하여 전신통신시설을 사용하는 것이다. 이러한 전신통신시설은 출발점과 이러한

전송의 수신점간에 전신, 케이블 기타 이와 유사한 연결에 의하여 서면, 그림, 소리를 전송하기 위하여 사용되는 시스템이라고 정의되고 있다.

이 법과 관련하여 생기는 쟁점은 이 법이 스포츠 등에 대하여 도박하는 것에 한정됨으로써 인터넷 카지노에 적용되느냐 여부이다. 또한 전신시설이라는 정의가 인터넷상의 모든 통신을 포함할 정도로 광범위한가의 쟁점이 발생한다. 이러한 논란에도 불구하고 미국의 법무부 및 여러 주의 검찰총장들은 Wire Act가 모든 유형의 인터넷 게임에 광범위하게 적용된다는 입장을 공식적으로 취하고 있다. Wire Act와 관련하여 발생하는 두 번째 입장은 전신통신시설이라는 정의가 인터넷상의 모든 통신을 포함할 정도로 광범위한가의 문제이다.

Wire Act에 대한 다양한 견해에도 불구하고 미국의 법무부와 여러 주 정부의 검찰총장의 공식적인 입장은 Wire Act가 모든 유형의 인터넷 게임에 광범위하게 적용된다는 것이다.

### 3. Internet Gambling Prohibition Act(IPGA)

IPGA는 1995년에 처음 제안되었고 1999년 11월에 상원에서 만장일치로 통과되었으나 하원에서 통과하지 못한 실패한 법안이다. 이 법안이 다시 통과되어 법이 될 수 있는지 여부는 현재의 부시대통령 행정부에 의하여 결정될 사안이지만, 인터넷상에서의 도박과 관련하여 의미가 있는 법안이라고 할 수 있다. 이 법안은 도박업에 종사하는 자가 도박에 돈이나 물건을 걸거나 이를 수령 또는 송부하기 위하여 인터넷을 이용하는 것을 불법화하였다. 또한 이 법안은 위반에 대하여 벌금이나 징역과 같은 형사적인 제재를 가하고 있으며, 규제기관이 위반자가 다시 위반할 수 없도록 하기 위하여 영구적인 금지명령을 내릴 수 있도록 하였으며, 인터넷서비스 제공자가 도박을 하는 웹사이트를 개설하는 것을 금지시킬 수 있는 금지명령을 구할 수 있도록 하였다. IGPA는 여러 예외를 규정하고 있는데, 예외로서 주의 복권, 경마나 개의 경주, 인디안 게임 등이 규정되었다.

### 4. 2001년도 회기의 법안

2001년도 회기의 인터넷 도박관련 법안으로서는 Internet Gambling Payments Prohibition Act (HR 2579 IH) 및 Unlawful Internet Gambling Funding Prohibition Act (HR 556 IH)이다. 전자의 법안은 타인이 인터넷 도박에 참여하는 것과 관련하여 그 참여자에게 주어진 신용, 전자자금이체, 수표 등을 수령하는 것을 불법화하고 있다. 이 법을 집행하는 것에 대해서는 연방 및 주정부가 법원에 금지명령을 청구할 수 있도록 하고 있으며, 이 법안의 위반에 대해서는 형사적인 제재를 가할 수 있도록 하고 있다. 후자의 법안은 전자의 법안과 유사한 것으로서 도박업에 종사하는 자가 불법적인 인터넷도박에 참여하는 자와 관련하여 그 자로부터 신용, 전자가즘이체, 수표 등을 수령하는 것을 불법화하고 있다. 위반에 대한 제재수단도 전자의 법안과 거의 동일하다.