

# 사이버공간에서의 익명성과 책임

자유인은 사적 인간이다.(The free man  
is the private man - C. Rossister)

한상희 (건국대학교 법학과)

\* 이 글은 4월 22일 진보네트워킹센터 주최 토론회 <정보 인권과 한국의 정보화>에서 발표되었던 발제문의 일부입니다.

## 1. 자유와 규제

사이버공간에서의 익명성은 자유로운 의사소통을 가능케 함으로써 그것을 해방공간으로 자리잡게 하는 동시에 자신을 드러내지 않을 수 있다는 점을 이용하여 무책임한 발언이나 명예훼손 모욕, 혹은 유언비어 등의 폐해를 드러내기도 한다. 그러다보니 오프라인상에 존재하던 기존의 권력은 이러한 폐해를 이유로 사회질서의 확립을 주장하면서 익명성을 규제하기 위한 장치를 모색하고자 노력한다. 1998년 12월7일 정보통신부가 온라인서비스 이용자들이 건전한 정보를 손쉽게 빠르게 이용할 수 있도록 하기 위해 PC통신과 인터넷 등 온라인서비스를 이용하려면 반드시 실명으로 가입해야 하고, 기존 가입자도 주민등록번호와 성명이 맞지 않으면 강제 해지된다는 것을 골자로 하는 '온라인서비스 이용증진방안'을 마련, 발표한 것(정보통신부, 1998)이나, 2003년 하반기부터 정부부처가 개설한 게시판 등의 경우 인권침해와 명예 훼손 등을 막기 위해" 주민등록번호와 성명으로 실명을 확인받은 자만이 이용할 수 있도록 하는 방침을 정보통신부가 추진하고 있는 것<sup>1)</sup>은 이의 대표적인 예이다. 일종의 통신실명제를 실시할 것을 선언한 것이다. 특히 1998년 안의 경우 정보통신부는, 정보통신서비스에 수요자들이 비실명으로 가입하도록 방임하는 것이 건전치 못한 통신문화를 이끌고, 이용요금의 연체로 인하여 못해 사업자들의 채산성을 악화시키는 주요 원인이라고 판단, 온라인서비스의 가입실명화를 적극 추진해 나갈 계획이라고 한다. 그래서 이를 위해 한국정보통신진흥협회의 신용정보공동관리시스템과 행정자치부의 주민전산망, 한국통신의 전화번호 안내시스템, 신용카드조회업자의 신용정보시스템등을 연결, 기존 가입자는 물론 신규가입자에 대해서도 실명확인을 실시함으로써, 비실명으로 온라인서비스를 이용하는 것을 원천적으로 봉쇄할 계획이라 하면서 이미 98년 12월 1일부터 신용정보시스템과 온라인으로 연결, 주민등록번호와 성명이 맞지 않는 가입자는 신규가입을 사전 차단하고 있다고 발표하였다.<sup>2)</sup>

1) 실제 2003년초 현재 이러한 실명제는 18개 중앙 정부 부처 중 9개 부처에서 실시되고 있는 바, 정보통신부는 그것을 모든 부처로 확대한다는 것이다. 중앙일보 2003.3.28, [http://news.naver.com/news\\_read.php?oldid=200303280000450522012&s=6&e=245](http://news.naver.com/news_read.php?oldid=200303280000450522012&s=6&e=245)

물론 이 시도는 거의 실패로 끝나고 따라서 2003년 새로운 정책시도가 이루어지게 되었지만, 우리나라의 정보통신인구가 2천만이 넘어서면서 인터넷공간이 국민생활의 상당부분을 차지하고 있다는 점을 감안한다면 그 정책지향이 남기고 있는 여운은 결코 적지 않다. 즉, 이 통신실명제의 도입시도가 예상하였던 두 가지의 목적 - 불건전통신문화예방과 정보통신 서비스업자들의 경영정상화 - 중에서 특히 전자의 목적은 여전히 타당할 뿐 아니라, 오히려 그 필요성이 배가되고 있다는 인식이 적지 않기 때문이다. 통신실명제는, 정보통신의 익명성을 이용하여 자신을 드러내지 않는다는 이유만으로 저속 음란한 표현이나 사회질서에 반하는 내용들을 유통시키고 그럼으로써 정보통신질서를 저해하고 나아가 사회적으로 무가치한 정보통신관행들이 나타나게 되는 역기능을 치유할 수 있는 또 하나의 규율방식으로 나름의 유효성이 있다고 생각되고 있는 것이다.

하지만, 그럼에도 불구하고 이러한 주장에 대한 반론은 만만치 않다. 한 네티즌의 논평처럼 익명성을 무기로 자유롭고 도전적인 의견과 비판을 내놓는 통신세력에 대한 통제외도"라든가, 또는 청에 대해 자유롭지 못한 사회에서 유일한 통로이자 탈출구역할을 담당해 온 통신과 인터넷 세계를 여전히 보수적이고 가부장적인 시각에서 정화하겠다는 과욕이 숨어있"다는 음모론적 비난은 대표적이다.<sup>3)</sup> 표현의 자유에 대한 국가 또는 사회윤리와 사회질서를 명분으로 보수적 가치관을 관철시키고자 하는 일련의 권력집단의 공격이라는 관점에서 통신실명제의 역효과를 지적하고 있는 것이다.

이 글에서는 이러한 논란에 즈음하여 통신실명제에 대한 헌법적 평가와 관련한 몇 가지의 헌법문제들을 지적하고 그에 관한 판단의 토대를 제공함에 치중할 것이다.

## 2. 통신실명제, 그리고 통신

### 2.1. 통신실명제의 개념과 의의

#### 2.1.1. 정보통신부의 실명제정책의 의미

우선 통신실명제와 관련한 정보통신부의 두 정책을 비교함으로써 그 제도적 의미를 분석해 보기로 하자. 1998년 정보통신부가 발안하였던 통신실명제는, 전세계적으로 유례가 없는 통일된 일반식별자(identifier)로서의 주민등록번호를 이용하여 가입시점을 기준으로 정보통신 이용자의 신원을 확인하는 방법을 제안하고 있다. 즉, 이에 의하면, 통신실명제는 엄밀히 보아 익명이나 가명의 방법에 대한 개념으로서의 실명제를 채택하기보다는, 통신과정에서 어떠한 방식의 ID를 사용하는가에 관계없이 정보통신서비스를 개시하는 그 순간에 자신의 실제의 신원을 밝히고 이에 의거하여 정보통신서비스를 이용하도록 강제하는 방안을 의미하고 있다<sup>4)</sup>. 반면, 2003년의 실명제정책은 정보통신서비스를 이용할 수 있는 권원이 어떻게 형성되는가에는 관계하지 않고 단지 정부가 개설한 게시판에 글을 올리하고자 하는 자는 반드시

2) 이에 발맞추어 그 당시 개정되었던 주민등록법은 소위 주민등록번호생성기 등을 이용하여 주민등록번호를 위조하는 것을 금지함으로써 통신실명제를 향한 강제장치를 확보하고 있다. 그리고 2003년안의 경우도 전체로서의 정책목표가 이러한 취지와 크게 다르지 않다고 할 수 있다.

3) 청인문화 겨냥한 통신실명제": <http://user.chollian.net/~k21h/a-b48.htm>

4) 엄밀히 본다면 통신실명제의 개념에는 게시하는 표현의 한 내포로서 text속에 표현자의 신원에 관한 사항을 적시하도록 강제하는 것까지 포함되어야 할 것이다. 하지만, 이러한 형태의 실명제는 아직 우리나라에서도 거론된 적이 없는 만큼 일단 그에 관한 논의는 뒤로 미룬다.

사전에 실명확인을 받아야 하도록 강제한다는 것을 주축으로 한다. 정리하자면 전자의 안에서는 정보통신서비스이용자가 정보통신서비스사업자로부터 실명으로 그 이용권한을 부여받을 것을 강제하는 반면, 일단 그렇게 실명의 이용권한을 부여받은 한도내에서는 추후의 통신활동과정에서 자신의 실명을 밝히든 아니든 즉 어떠한 ID나 아바타를 사용하는가는 문제가 되지 않게 된다. 후자의 안은 반대로 정보통신서비스이용자가 어떠한 권원에 의하여 정보통신서비스를 이용하건 관계하지 않고 단지 정부개설의 게시판에 글을 올릴 때에는 반드시 자신의 실명에 대한 공식적 확인을 받을 것을 요구한다. 한마디로 특정한 ID 혹은 아바타를 사용할 것을 강제하는 것이다.

이렇게 분류한다면 두 정책수단은 각각 별개의 모습을 가지고 있고 따라서 별개의 목적을 추구하는 것처럼 보인다. 외관상으로는 1998년의 실명제정책은 IP의 추적가능성을 염두에 둔 것인 반면 2003년의 정책은 의사소통과정에서의 현명성 즉, 의사소통 상대방에 대하여 자신을 드러내는 것을 강제하는 것과 같은 모습을 가지고 있다. 하지만, 그 실질을 살펴보면 양자는 동일한 것을 추구할 뿐이다: 인터넷상의 의사소통과정에서 나타나는 역작용들을 제거하거나 사전에 예방하기 위하여 의사소통당사자들에게 자신의 신원이 확인될 수 있는 가능성'을 의식하게 함으로써 사이버공간을 순화'하겠다는 것이다. 환언하자면, 양자는 모두 실명제를 바탕으로 형성되는 신원추적의 가능성을 전제로 사이버공간상의 의사소통을 사전 억제하거나 사후통제 처벌할 수 있는 여지를 마련하고 이를 통하여 의사소통의 당사자들을 심리적으로 강제하는, 일종의 사회통제 내지는 범죄억지의 정책목표를 바탕으로 하고 있는 것이다.

### 2.1.2. 통신실명제의 기능

통상 실명제는 두 가지의 의사소통적 구조에서 요청된다. 첫째는 의사소통적 관계에 들어가 있는 당사자들이 상호 상대방의 개인적 속성—특히 그의 현실공간(real space)에서의 속성—을 알 수 있거나 또는 그에 관한 정보를 요청하는 상태가 그것이며(콘텐츠로서의 실명), 둘째는 콘텐츠의 밖에서 의사소통의 상대방이나, 이들 의사소통적 관계와 일단 떨어져 있는 제3자—특히 국가와 같은 감시 통제자의 입장에서나, 또는 정보통신서비스사업자와 같은 관리자—의 입장에서 이 의사소통적 관계에 들어가 있는 당사자들의 신원을 (사후적으로) 확정할 수 있는 상태로 만들고자 하는 요청이 그것이다(추적가능성으로서의 실명). 이를 순차적으로 살펴보자.

#### ① 콘텐츠로서의 실명제: 顯名性

실제, 실명제라는 용어는 어떠한 행위자의 행위 그 자체로부터 실체적 의미를 가지기보다는 오히려 그 행위의 상대방, 즉 수신자가 그 행위자의 신원을 확인할 수 있는가의 여부로써 판단되어야 한다. 왜냐하면 실명제가 작동하는 장(field) 그 자체가 일정한 수 이상의 당사자들간의 의사소통을 전제로 하는 것이며, 이 의사소통의 관계 속에서 자신의 개인적 속성(personal attributes)을 의사소통의 내용(contents)으로 담을 것인가 아닌가를 중심으로 당사자 서로의 위상을 정립하게 되는 것이 일반적이기 때문이다. 대체로 사람들이 의사소통적 관계에 들어서게 되는 것은 두 가지의 목적, 즉 정보의 획득과 인간관계의 유지/확산이라는 목적속에서 이루어진다.(황상민, 31-2면) 여기서 전자의 목적에서 요구되는 정보의 신뢰성문제, 그리고 후자의 친밀성요청에서 나타나는 공감대의 형성이라는 문제는 발신자가 아니라

수신자에게 가장 절실한 것으로 등장하며, 이 점에서 발신자의 개인적 속성은 수신자가 의사소통적 관계에 들어서고 나아가 그것을 발전/확산시킴에 있어 중요한 요소를 이루는 것이다.

이렇게 본다면, 실명제의 문제는 수신자가 어떻게 발신자의 인적 속성을 발견하고 확인할 수 있는가의 문제와 직결되지만, 그러나 그럼에도 불구하고 이 때의 실명성이라는 것은 굳이 현실공간의 그것과 반드시 동일할 필요는 없다. 왜냐하면, 실명성의 요청 자체가 신뢰성이나 공감대의 추구라는 목적에서 나오는 것인 만큼, 사이버공간내에서의 특정성만 확보될 수 있다면 얼마든지 그러한 신뢰성이나 공감성은 확보될 수 있기 때문이다. 예컨대, 현실적 ID와는 무관한 가공의 ID로써 뉴스그룹내에서 계속 반복적으로 contents를 게시하여 그 나름의 명성(reputation)을 얻은 경우에서와 같이 신뢰성의 문제는 지속적인 시행착오를 통한 확신(이것은 보기나름으로는 A. Giddens(1991)나 U. Beck(1998)이 말하는 근대적 위험사회에서의 위험기피의 방편이기도 하다)의 문제인 것이며, 따라서 물리적 인식의 여부가 아니라 심리적 평가의 문제이기 때문이다. 특히 후자의 공감대는 더욱 더 의사소통적 관계의 성격에 의존하게 된다.<sup>5)</sup>

## ② 추적가능성으로서의 실명제

둘째의 추적가능성으로서의 실명제의 문제는 문자 그대로 사이버공간의 가상성 자유성과 현실공간의 권력성(넓은 의미에서)의 충돌의 문제이다. 즉, 현실공간에서와 마찬가지로, 어떠한 권력자가 행위자의 의사와 행동을 통제하는 권력적 관계의 문제가 나타난다. 질서유지 또는 사회윤리의 보전 등 어떠한 (공공)목적의 달성을 위한 수단으로서, 기존의 질서에 어긋나는 행위자에 대한 감시와 통제의 장치의 장치를 구축하고 이를 통하여 행위자의 몸(현실적 물리적 공간에 위치하고 있는)에 대한 권력의 행사가능성을 확보하기 위한 담보이자 동시에 수단으로서 실명성을 요청하는 경우가 이에 해당한다.

이 경우의 실명성은 앞서의 현명성과는 다른 구조를 가진다. 전자의 경우에는 상대방의 개인적 속성 자체가 표현의 내용을 이루고 있으며 따라서 누가 말하였나의 문제는 그 표현의 신뢰성이나 공감성의 형성에 중요한 부분이 되고 있는 반면에, 후자의 경우에는 이 표현으로부터 나타나는 책임의 문제는 과연 어떠한 물리적 인격이 감당하여야 할 것인가의 문제로 전이된다. 표현 그 자체의 의미를 결정하는 의미에서의 신원이 아니라, 표현의 결과-책임(accountability와 responsibility)를 귀속시키기 위한 장소로서의 신원이 문제되는 것이다.

이렇게 본다면 실명제는 정확히, 「표현자를 어떻게 추적할 수 있을 것인가」의 문제로 귀착한다. 환언하자면, 아바타의 퍼소나(persona)를 문제삼는 전자의 경우와는 달리, 여기서는 이 아바타를 창조한 현실적 인간의 신원과 그 장소, 시간을 사이버공간에서 나타나는 아바타와 어떻게 연결짓고 나아가 그 현실적 인간을 어떻게 발견할 것인가의 문제가 등장하는 것이다. 예컨대, 갑이라는 현실적 인간이 A라는 아바타를 창조하고, 그것을 통하여 X라는 다른 아바타에게 허위의 사실을 알림으로써 X를 창조한 을이라는 사람에게 현실적인 재산적 손해를 야기시킨 경우(일종의 사이버사기의 경우), 을이나 그의 고소를 접수한 사법경찰의 입장에서는 자신과 의사소통한 A라는 아바타가 아니라 그를 창조한 갑의 신원이 관심대상이 된다. 이 때 을이나 사법경찰관은 A라는 아바타를 통하여-또는 재산상의 이익이 유입된 경

5) 예컨대, 여성들간의 채팅에서는 Tommy라는 id보다는 jane이라는 id가 보다 친숙감을 야기할 수 있을 것이다.

로를 통하여- 값을 추적하고자 노력한다. 그리고 이때의 실명제의 논의는 「A-값」의 관계에 그 추적을 용이하게 할 수 있는 어떠한 다른 연결의 고리를 제도적으로 확보할 것인가 아닌가의 문제로 설정된다.

## 2.2. 익명성의 역작용?: 그 유형

이러한 의문은 우선 사이버공간의 특성 중 가장 주요한 것으로 거론되는 익명성이 야기할 수 있는 역작용부터 논의하면서 풀어보자. Johnson & Miller(1998)에 의하면 일반적으로 익명성이 가지는 폐해로, ①행위자를 특정하기 어려움과 증거수집상의 어려움으로 인한 법집행의 곤란성 ②사회적으로 바람직하지 못한 행위나 유해한 행위를 범하기 쉽게 하는 속성을 가짐, 그리고 ③정보의 근원을 알 수 없어 정보에 대한 신뢰성 감소 등을 들고 이 단점들로 인하여 전반적으로 정보통신공간의 신뢰성이 약화된다고 한다.

이 중, 먼저 법집행(law enforcement)의 곤란성부터 보기로 하자. 익명성은 범죄자의 신원을 직접 드러내지 않도록 하기 때문에 그를 통하여 직접 구체적인 범죄행위를 촉발하는 동인으로 작용한다. A. M. Froomkin(1995)은 익명성의 역작용으로 온라인사기(on-line fraud), 돈 세탁, 조세 제조물책임 저작권 등에 대한 침해의 가능성, 지적재산권에 대한 침해, 그리고 사회윤리의 문제 등의 예를 든다. 여기서 그는 조세나 제조물책임 등과 관련한 범죄는 그리 확률이 높지 않다고 하면서 지적 재산권의 침해가능성이라는 점이 가장 큰 문제라고 언급한다. 특히 소프트웨어의 소스는 언어로 되어 있다는 점에서 그 무엇보다도 사이버범죄에 친숙한 범죄대상이 될 수 있다 할 것이다. 이러한 경우는 일반적으로 현실공간에서 나타나는 범죄행위에서 필요로 하는 익명성과 본질적으로는 다르지 않다. 다만, 이 경우의 익명성이 가지는 역작용은 범죄행위의 태양이나 그 행위자의 신원을 은닉함으로써 누가 어떻게 범죄행위로 나아갔는지의 추적이 용이하지 않다는 것이다. 그러나 이는 범죄를 행하면서 범증(犯證)을 남기지 않으려고 하는 범죄인의 일반적인 심리가 그대로 사이버공간에서 활용될 수 있는 익명화의 용이함을 통하여 나타나는 경우에 지나지 않는다.

문제는, 사이버공간의 경우에는 익명성의 가능성으로 스스로 자신에 관한 정보를 최소화하여 송출할 수 있으며, 이와 함께 자신이 한 행위의 자취나 흔적 자체도 무형적일 뿐 아니라 손쉽게 변환 삭제할 수 있다는 점이다. 증거의 은닉이 현실공간의 그것에 비하여 훨씬 용이한 것이며, 따라서 적발의 가능성도 낮아진다. 또한 현실범죄와는 달리 순간적으로 행위가 이루어지면서 동시에 그 행위과정이 순식간에 지워져 버린다는 점에서 행위자가 자신의 행위를 되돌아보고 반성할 수 있는 중요한 모티프조차도 소멸시키게 된다(백운철 이기욱, 2000).

둘째의 역작용은 정보통신서비스이용자의 개인적 특성에 관한 것-일종의 일반예방적 측면에 관한 것이다. 그것은 익명이라는 은폐성이 범의(犯意)의 형성을 촉진하는 방향으로 작용할 수 있음을 의미한다. 익명성은 전술하였듯이 추적의 가능성을 축소한다. 이에 범죄의 유혹을 받는 사람이 손쉽게 범죄로 나아갈 수 있는 여지를 마련할 수 있다. 통상적으로 범죄에 대한 법규범의 예방적 효과는 적발의 가능성과 제재의 정도에 의하여 통제된다는 점에서 익명성으로 인한 적발가능성의 축소현상은 범죄의 비용을 감소시키고 그 범죄로 인한 기대이익을 상대적으로 증가시킨다는 점에서 범죄를 촉발할 가능성을 야기하게 된다. 그리고 사

이버공간에서는 이러한 익명성의 가능성과 비용이 현실공간에 비하여 현저하게 적다는 점에서 더욱 이 가능성은 확대되게 된다.

부연하자면, 사이버공간은 ①현실공간에서의 대면적 관계와는 다르게, 자신에 관한 정보가 고도로 축소된 채 수신자를 향하여 의사를 표현한다는 점에서 고도의 은닉성을 특징으로 한다. 더불어 자신의 정보를 통제함으로써 자신과 별개의 인격을 창출할 수 있다는 가능성으로 인하여 현실공간에서 유효하게 적용되는 사회규범의 제약을 쉽사리 벗어날 수 있도록 한다. ②자신과 의사소통하게 되는 상대방의 인격 역시 현실적 인격과는 상이하거나 또는 상이한 것으로 인식되는 상황에서는 자신의 행위가 야기하는 결과가 어떠한 현실을 만들어내는지 인식하기 힘들게 된다. 즉, 상대방이나 의사소통공간의 물리적 변화에 대한 인식이 결여되게 됨으로써 결과발생으로 인한 죄의식이나 가책감을 느끼기 힘들게 된다(Rose, p.189) ③그러한 현실적 변화를 겪어야 하는 자 즉, 피해자에 대한 정보 역시 통제됨으로 인하여 범죄자는 피해자를 알지 못하고 따라서 그 피해자의 고통으로부터 느낄 수 있는 죄의식으로부터도 자유로운 상태가 된다. 결국 사이버범죄는 여타 일반적인 사이버 의사소통행위와 마찬가지로 차원에서 손쉽게 저질러지고 손쉽게 잊혀지는 비밀탈적, 일상적 행위로 인식되기 까지 하는 것이다.

앞의 두 역작용이 범죄의 억지에 관한 것이라면, 셋째, 익명성이 가지는 무엇보다도 심각한 역작용은 이상과 같은 개인적 범죄충동 혹은 유발의 문제보다는 오히려 사회문화적 수준에서 나타난다. 즉, 그것은 사이버공간의 문화양태들을 주류의 사회문화로부터 일탈시키거나 혹은 주변적인 것으로 「하락」시키는 효과를 야기한다.<sup>6)</sup> 환언하자면, 익명의 공간을 통하여 사람들은 사회적 규범이나 구속으로부터 해방감을 느끼고 이를 바탕으로 범죄 또는 비행(delinquent behaviour)을 아무런 범죄의식이나 일탈의식 없이 저지르게 되는 가능성을 야기하고 이를 관련된 사이버공간에서 보편적인 것으로 일반화한다는 점이다. 인터넷공간 특히 사이버공간은 의사소통당사자들간의 직접적인 대면관계가 없이 가상의 아바타들을 통해 가상의 피소나들이 접촉하는 방식으로 이루어진다. 이 과정에서 그 의사소통관계에 참여하는 현실인간들은 상대방의 존재에 대한 실재감(實在感)을 상실하거나 상당히 희석시키게 된다. 특히 이들이 상호 익명인 경우에는 탈인격화(deindividuation)<sup>7)</sup>의 상태가 나타나면서, 행위자를 상황의 규범이나 역할 또는 사회적 금기, 제약으로부터 해방"시키는 상황이 이루어진다.(황상민 한규석 편, 33-5) 여기서 당사자들은 보다 손쉽게 사회적 일탈행위로 나아가고자 하는 충동을 느끼게 되고 이러한 과정이 모방이나 공감을 통하여 계속 누적되면서 사이버공간의 금기위반성은 보다 강화된다.<sup>8)</sup>

하지만, 이러한 분석은 과연 법규율의 대상으로서의 사이버공간에 대하여도 그대로 타당할

6) 즉, 주류의 문화공간에서는 감히 공개되지 못하던 담론들이 사이버공간에서는 보다 손쉽고도 공개된 형태로 상호 소통되는 현상이 나타나게 된다. 예컨대, 성행위, 성적 지향, 혐기"나 컬트, 음담패설 등에 관한 사이트나 유흥업소 등에 관한 정보의 범람은 이의 대표적인 예이다.

7) 황상민 한규석(33-5면)은 이를 몰개성화라고 번역하고 있으나, 이 개념은 아바타를 통하여 자신의 현실적 정체성과 분리된 새로운 정체성을 형성한다는 의미로 이용되고 있는 만큼 탈인격화 내지는 탈개체화로 번역하는 것이 바람직하다. 이에 이 글에서는 현실적 정체성으로부터의 이탈이라는 의미를 중심으로 탈인격화라고 번역하기로 한다.

8) 이에 더하여 사이버공간이 가지는 전파성 확산성, 복제 편집의 용이성 무한성, 상대적으로 낮은 이용자 연령층, 그리고 사이버공간에 대한 사회적 감시망의 미구축 등은 이러한 충동을 보다 강화하는 변수로 작용한다.

수 있는 것인지? 혹은 그에 대한 과잉규제 내지는 과소보호의 요인은 제공하고 있지는 않는지 자못 의문스럽지 않을 수 없다. 이는 절을 바꾸어 살펴보기로 하자.

## 2.3. 효율적 법집행 수단으로서의 실명제의 효과

앞에서 언급한 정보통신부의 실명제의 정책논의는 사이버공간에서 일어나는 범죄 또는 어떠한 일탈행위의 당사자를 추적할 수 있는 가능성—혹은 그를 전제로 사전억지효과를 도모할 수 있는 가능성—을 모색함을 염두에 두고 있다 할 것이다. 정보로서의 실명제라는 경우에는 이미 언급한 바처럼, 그것은 신뢰나 공감의 여부에 달려 있는 것이며, 따라서 여기서 별도로 의사소통상대방의 현실적 신원을 확인할 수 있는 어떠한 공적 장치를 특별히 마련해 두어야 할 필요성은 그리 크지 않기 때문이다.<sup>9)</sup> 그러나, 그럼에도 불구하고 개념상으로는 과연 그러한 추적가능성으로서의 실명제는 어떠한 의미를 가질 수 있을 것이냐가 문제로 남는다. 추적가능성이라는 기술적 관점에서만 본다면, 굳이 별도의 제도적 장치가 없다 할지라도 상당한 정도의 네티즌의 신원은 확보할 수 있을 것이기 때문이다. 즉, 실명제의 제도적 존재목표가 사이버공간을 통하여 어떠한 비행을 저지르고 사회적으로 무가치한 결과를 야기하거나 그에 상당하는 위험을 야기한 경우에 그 행위자를 사후적으로 추적하여 적발하고, 일정한 제재로써 그를 통제하고자 하는 것이라고 한다면, 그것은 현실공간에 있어서의 사후제재장치를 가동하는 수준에서 충분히 달성할 수 있기 때문이다.

예컨대, 위의 예와 같은 경우에, 갑은 A라는 아바타를 통하여 행위하였음에도 불구하고 그가 발신한 장소에 관한 정보를 정보통신공간속에 남겨 두게 된다. 발신한 IP주소(및 그것이 존재하는 현실적 공간)와 시간, 그리고 Log File 뿐 아니라, 그가 그러한 발신을 하기 위하여 행하였던 제반의 행동들(책상에 앉아 컴퓨터를 켜고, Log In하고, 타이핑하며 커피를 마시는 등)에 관한 정보들은 그 현실공간에 무수하게 산포되어 있는 것이다. 이는 순수하게 현실공간 속에서 범죄가 이루어졌을 때, 현장조사 등의 방법으로 수사관들이 추적하고자 하는 그 범죄에 관한 정보의 경우와 동일하다.<sup>10)</sup> 물론, PC방 등 IP주소가 특정되지 않거나 특정된다 할지라도 누가 그 IP주소를 이용하여 발신을 하였는지 알기 어려운 경우도 있을 수 있겠지만, 그 또한 일반적 범죄수사의 경우와 다르지 않다. 수사관들은 이러한 경우에 탐문수사등의 방법으로 범죄현장(또는 그 현장이라고 추정되는 장소)를 중심으로 목격자를 찾아 나서거나 유사범죄전력자들에 대한 알리바이를 조사하는 등의 활동을 하면서 추적에 나선다. 분실되었거나 도난당한 신용카드를 부정사용한 경우의 수사활동들은 이의 좋은 예가 된다.

이 점은 위에서 언급한 익명성의 역작용이 나타나는 유형과 연관지으면 더욱 분명해진다. 첫째, 법집행의 실효성과 관련한 문제부터 살펴보자. 실제 범죄자가 익명성을 추구하는 경우

9) 물론 이 경우도 현실적 신원확인 문제를 적극적인 목적에서 고려할 필요성은 존재한다. 이 점은 다시 서술한다.

10) 일례로 지난 2002년 대통령선거결과에 대하여 개표조작설을 퍼트렸던 사건도 IP추적과 더불어 그 행위자의 행태적 습성—한꺼번에 여러 개 사이트의 창을 열어 놓은 채 게시판에 글을 올리고, 울산과 의성에 연고를 가진—을 포착해 냄으로써 경찰이 그를 체포할 수 있었다. 자세한 것은, 오마이뉴스 [http://news.naver.com/news\\_read.php?oldid=20030206000024641086&s=2244&e=2494](http://news.naver.com/news_read.php?oldid=20030206000024641086&s=2244&e=2494) 참조.

는 현실공간에서도 얼마든지 나타난다. 우리나라의 예를 들자면, 다른 입법례에서도 찾아 볼 수 없을 정도로 완벽한 형태의 주민등록제도가 실시되어 있고 거기다가 전대미문의 전국민 지문날인제를 취하고 있음에도 불구하고 범죄를 범하고자 하는 사람들은 이러한 주민등록장치를 회피하고 자신의 익명성이 보장되는 다른 방법이나 수단을 추구하는 한편, 경우에 따라서는 그 다른 사람의 실명을 이용하는 방안을 동원하고자 한다. 마찬가지로, 정보통신의 상황에서도 통신실명제와 관계없이 사람들은 일정한 비행을 함에 있어서는 자신의 신원을 은닉할 수 있는 다양한 방법—예컨대 remailing site<sup>11)</sup>의 이용 등—을 강구하게 되고 이 점에서 실명화의 수단이 완벽하게 효율적이지 않는 한은 여전히 문제는 남게 된다.

둘째 익명성이 범의의 발현가능성이나 그 수행가능성을 촉진한다는 문제점 역시 마찬가지로 일면적이다. 왜냐하면, 범죄의 예방적 효과는 적발의 가능성 및 제재의 정도에 의해서만 통제되는 것이 아니라, 그와 더불어 범규범의 내재화정도 또한 중요한 통제변수로 작용한다는 점이며, 나아가 적발가능성 역시 법집행기관의 능력 뿐 아니라 사회적 감시망의 존재나 사회적 결합성의 정도에 의하여 다시 통제되는 만큼, 익명성이라는 사이버공간의 특성만으로 모든 것을 설명하기에는 한계를 가지기 때문이다. 즉, 익명성의 가능성을 통제하는 정도와 범죄예방적 효과는 일정한 비례적 관계를 가진다고 보다는 오히려 그 외의 독립변수나 매개변수의 영향을 심하게 받는다는 점에서 일응의 한계를 가지는 것이다.

오히려 실명제를 통하여 익명화의 가능성을 축소시키는 효과는 이상과 같은 개인적 수준에서의 범죄적발이나 범죄억지라는 목표보다는 사회문화적 수준에서 사이버공간의 문화양상을 어느 정도 주류의 그것에 근접시키는 하나의 수단으로 활용될 수 있을 것이다. 즉, 실명제의 도입은 상술한 탈인격화의 과정을 둔화시키거나 지체시키는 효과를 가질 수 있다는 것이다. 우선 사이버공간이 대면적 의사소통관계로 이루어지는 것이 아니라는 점에서 이러한 탈인격화의 현상을 완전히 차단하기는 어렵지만, 그럼에도 불구하고 실명제가 도입되면 최소한 자신의 고유정보들을 상대방에게 노출시키게 되는 가능성을 잠재하고 있는 셈이 되고 따라서 그에 상응하는 정도의 탈인격화 방지효과를 거둘 수 있게 된다. 그러나 그럼에도 불구하고 이 또한 한계를 가진다. 마치 현실공간에서도 대중속의 개인은 익명화되고, 그것이 홀리건의 예에서 보듯 집단적 일탈심리를 야기하는 것과 마찬가지로, 사이버공간에서도 아무리 실명화되어 있더라도 그것이 집단적 의사소통속에 존재하는가 아니면 개별적 의사소통관계에 존재하는가에 따라 상이한 결과를 야기할 수 있게 된다.

요컨대, 사이버공간에서의 실명제라는 요청은 그 자체 많은 부분을 처리하는 효율적 장치라기 보다는 가능한 대안 중의 하나에 불과하다. 사정이 이러하다면, 그렇다면 진정 무엇이 통신실명제의 주된 목표가 되어 있는 것인가라는 점은 무엇보다도 먼저 해결되어야 할 의문으로 남게 된다. 그것은 추적에 필요한 비용을 줄이기 위한 것인가? 아니면, 정보통신기술의 특성상 현실공간에서와 같은 수사기법을 사용하여서는 도저히 추적할 수 없는 그 어떠한 특수성이 있는가? 그렇지 않으면 추적가능성을 넘어서는 또다른 목적이 존재하는가? 만일 존

---

11) 예컨대, <http://www.obscura.com/~loki/index.cgi>은 발신자의 추적을 배제하기 위하여 새로운 방식을 채용한 리메일서비스를 제공하고 있다. 가장 대표적인 리메일서비스제공자였던 핀란드의 Helsingius는 1992년 이 서비스를 제공한 후 첫 3개월동안 13,000건을 처리하였고, 나중에는 매일 576개의 뉴스그룹에 대하여 3500통의 메일을 중계하였다고 한다. L. Detweiler, Anonymity on the Internet FAQ, 1993.5.5 at: <http://rtfm.mit.edu/pub/usenet/news.answers/net-anonymity/part1> <2001.9 현재 폐쇄되었음>: A. Branscomb(1995)에서 전재.

재한다면 그 목적은 무엇인가?

### 3. 통신실명제와 헌법: 미국의 경우

#### 3.1. 연방대법원의 입장

##### 3.1.1. 위헌론

통신실명제의 이와 같이 어느 정도 사실상의 한계를 가진다. 그럼에도 불구하고 사이버공간이 가져다 주는 현실적 충격—주류정치 및 문화에 대한 도전으로서의 사이버공간의 해방적 성격—은 이러한 사이버공간에 대한 나름의 제어장치를 구축하여야 할 필요성을 현실정치에 부과하게 된다. 이것이 가장 두드러지게 나타난 경우가 Georgia주의 컴퓨터시스템보호법(Computer System Protection Act, 1996)이다. 이 법은

누구든지 전자메일박스, 홈페이지, 기타 전자적 정보저장뱅크나 전자적 정보에의 접근점을 이용하여 데이터를 구축하거나 유지, 작동 또는 교환하기 위한 목적으로 (……) 컴퓨터네트워크를 통하여 허위의 명의를 담고 있는 데이터를(if such data uses any individual name … to falsely identify the person) 고의로 전송하여서는 아니된다;

고 하고 이어,

누구든지 … 상호명, 등록된 상표명, 로고, 법적 또는 공식적 인명 또는 저작권의 표기를 포함하는 데이터를, 그에 대한 동의를 받았다는 사실 또는 명의사용에 대한 동의나 승인이 없으나 그 명의의 사용을 할 수 있다는 사실을 허위로 진술하거나 또는 그것을 암시하는 방법으로 컴퓨터네트워크를 통하여 고의적으로 전송하여서는 아니된다.

고 규정하고 있다. 이에 대하여 원고인 ACLU 조지아지부는 이 법규정이 내용기반적 규제에 예외 해당하는 것으로, 인터넷을 통하여 익명이나 가명으로 통신함으로써 표현자가 사회적으로 소외당하거나 차별 또는 학대를 받지 않고, 프라이버시를 보호할 수 있는 권리를 침해하고, 나아가 일반적으로 인터넷밖에서 인정되는 것과 같은 방식으로 상호명이나 로고등을 비영리적 교육용 표현이나 뉴스, 논평 등에 링크시킴으로써 이용할 수 있는 권리를 침해한다고 주장하였다. 이에 대하여 피고측은 이 법규정은 사기(fraud)를 예방하고 억지하기 위한 규정이라고 주장하면서, 혹시 규정방식이 모호하거나 광범위하다고 볼 경우 한정해석의 방법에 의하여 그 위헌성이 해소될 수 있을 것이라고 주장하였다.

이에 대하여 연방지방법원은 표현자의 신원(identity)은 저술자가 자유롭게 삽입하거나 제거할 수 있는, 당해 문건 내용상의 다른 요소들과 전혀 다를 바 없는 것”이라고 하는 McIntyre v. Ohio Elections Commission<sup>12)</sup>사건의 판단을 인용하면서 비록 당해 법률은 사

12) 115 S. Ct 1511(1995) 이 사건은 McIntyre부인이 성명을 밝히지 않은 채, 학교운영에 관하여 비판적인 글을 전단으로 만들어 선거기간중에 배포하는 것에 대하여 오하이오주의 조례를 위반하였다는 이유로 \$100의 벌금을 과한 것은 표현의 자유를 침해하는 것이라는 이유로 위헌선언한 것이다. 여기서 연방대법원은 익명성을 선호하는 것은 경제적 또는 공식적 보복에 대한 두려움이나 사회적 따돌림에 대한 염려, 또는 단순히 자신의 프라이버시를 가능한 한 많이 보호하고자 하는 욕구에서부터 나오기도 한다”고 선언하였고, 이러한 인식은 그대로 위의 Miller사건에 반영되고 있다.

기를 억지하고자 하는 점에서 정당하고도 중차대한 주의 이익을 지향하는 것이지만, 그럼에도 불구하고 엄정하게 입법된(narrowly tailored) 것이라고는 할 수 없다는 이유로 그 효력을 정지하는 잠정적 유지결정을 내렸다.<sup>13)</sup>

이 법규정은 표현을 규제하는 법률에 필요한 정도의 세밀성(precision)을 가지고 입안된 것은 아니[다.] 이 법률은 문언상 사회적 따돌림(social ostracism)을 피하고, 차별과 학대를 예방하고 프라이버시를 보호하기 위하여 허위의 명의(identification)를 사용하는 것, 그리고 상호명이나 로고를 비영리적인 교육적 표현이나 뉴스, 논평에 이용하는 것과 같은 [헌법상] 보호되는 표현을 금지하고 있다—이러한 금지는 수정헌법 제1조의 전형적인 문제이다. 따라서 이 법규정이 공중을 속이거나 기망하게 하기 위하여 자신을 의도적으로 허위로 밝히는”자와, 상호명이나 로고를 사용함으로써 유명한 상표를 혼동하게 하거나 모호하게 할 실질적 위험을 야기한 자를 기소하는 데에 합헌적으로 적용될 수 있다 할지라도, 그럼에도 이 법규정은 표현자의 상당한 부분을 위헌적으로 포괄하고 있기 때문에 광범위하다[고 당법원은 판단한다]<sup>14)</sup>

즉, 컴퓨터 네트워크상에서 실명을 사용할 것을 강제하는 위의 법규정은 그 입법목적이 자기범죄의 억지에 있다 할지라도, 범죄적 목적을 가지고 허위명의(즉 가명)를 사용하는 자와 자기보호의 필요에서 허위명의를 사용하거나 인용(citation)의 목적으로 타인의 상호등을 사용하는 자를 구분하지 못하고 따라서 입법목적의 달성에 필요한 최소한도로 규제의 폭을 좁히지 못한, 지나치게 광범위한 규정으로 수정헌법 제1조의 광범위하기 때문에 무효(void for overbreadth)라는 원칙에 어긋난다고 보았다. 뿐만 아니라 법원은 이 법규정에 대하여 형사법규에 일반적으로 요청되는 모호하기 때문에 위헌(void-for-vagueness)의 원칙을 적용하여, 이 법규정은 ①규정대상의 행위의 범위를 충분히 특정하지 않았고, ②자의적 집행의 가능성을 내포하고 있으며, ③원고의 표현의 자유를 침해한다는 이유를 들어 문언상 위헌의 가능성이 있다고 판단하였다. 특히 그 규정상의 모호성의 예로서 법원은 허위의 명의(falsely identify)”, “사용(use)”, “허위의 암시(falsely imply)”, “전자적 정보에의 접근점(point of access to electronic information)” 등의 용어를 들고 있다. 그리고 이러한 모호한 표현들은 피고측의 주장처럼 한정해석할 수 있는 그 어떠한 문법적, 체계적 가능성도 내포하지 않고 있기 때문에 더 이상 합헌적 해석의 여지는 없는 것이라고 보았다.

이 Miller사건의 결정은 그 자체로서 종결되고 더 이상의 상급법원의 판단이 이어지지 않으므로써 통신실명제와 관련하여 미국전역에 걸친 통일된 법리는 일단 잠재된 상태이다. 하지만, 일반적인 추세는 실명제를 법으로써 강제하는 것은 일단 표현의 자유에 대한 제한이며, 따라서 그것을 정당화할 수 있는 국가적 이익과 그 규제방식의 엄격성이라는 요건을 충족하여야 하는 것이라는 점에 대하여는 별다른 이설이 없어 보인다. 문제는 위 Miller 사건이 순수하게 실명제 그 자체의 위헌여부에 관한 판단이 아니라, 일단은 Georgia주법률의 형식적 측면, 즉 그 법규정이 취하고 있는 문언(文言)의 여하에 대하여 내려진 판단이라는 점에서 일도양단적으로 미국의 법제는 어떻다고 이야기하기 힘들게 되었다는 점이다. 환언하자면, 위 결정은 단지 Georgia주법률이 그 규정형식상 광범위할 뿐 아니라, 모호하게 되어 있어

13) 이는 차후 영구적 유지처분으로 변환되었고 주정부가 연방대법원에 상고하는 것을 포기함으로써 종국적으로 그 효력을 상실하게 되었다. 자세한 것은 Wallace(1999) 참조.

14) ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997)

법으로 보호되는 표현과 보호되지 않는 표현의 경계가 잘 못 그어져 있으며, 나아가 어떠한 행위가 법률로써 금지되는지도 명확하게 서술되지 않았다는 점에서 위헌의 가능성을 발견하고 이에 의거하여 그 법의 발효를 정지시켰을 뿐이며, 통신 실명제라는 제도가 만일 광범위하거나 모호하지 않게 잘 재단된(narrowly tailored) 것이라면 과연 그것이 위헌인지 아닌지에 대한 판단은 내려지지 않았다는 것이다.

하지만, 자유주의의 전통에 입각하고 있는 미국연방대법원은 이와 같은 내용규제적 방식의 입법에는 소극적인 경향을 보이고 있다는 점에서 일응 통신실명제에 대하여는 위헌적인 입장에 설 것으로 예상된다. 이미 미국은 헌법의 제정전부터 익명 또는 가명에 의한 팜플렛이 정치 뿐 아니라 사회문화적 이념을 주도하여 왔고<sup>15)</sup> 지금까지도 각종의 언론보도에서 정보원을 초련의 고위층(Teh Sources of Soviet Power)” 또는 “X” 등 익명화된 형식으로 표기하는 관행이 존재함을 감안할 때,<sup>16)</sup> 익명성이 표현의 자유에서 차지하는 비중을 쉽게 방기하기는 어려울 것이다. 실제, 미국연방대법원은 익명의 팜플렛이나 전단, 브로슈어 또는 책자는 인류의 진보에 중요한 역할을 수행하여 왔다”고 단언하기도 하였다.<sup>17)</sup>

### 3.1.2. 합헌론

그러나 그렇다고 해서 연방대법원은 모든 표현영역에서 익명성을 보호하고자 한 것은 아니다. 연방대법원에서는 정치자금의 모금과 관련한 두 사건—Buckley v. Valeo<sup>18)</sup>과 First National Bank of Boston v. Bellotti<sup>19)</sup>—에서 간접적이거나 실명제를 인용하는 취지의 판단을 내리고 있다. 연방선거에서 입후보자에게 기부할 수 있는 금액의 상한을 \$1,000로 한정하고 그 기부자의 명단을 연방선거관리위원회에 제출하도록 한 연방법을 합헌이라고 판단한 전자의 사건에서는 정치적 표현의 한 방식으로서의 선거자금기부행위를 실명으로 할 것을 예정하고 있고, 기업이 특정한 경우를 제외하고는 정치자금기부를 할 수 없도록 한 주법을 위헌이라고 한 후자의 사건에서는, 선거운동을 위한 광고의 출처를 밝히도록 하는 것은 냉각효과 등의 부작용을 야기하지 않는다는 조건하에서는 합헌적일 수도 있다는 취지의 방론을 내어놓기도 하였다. 양자 모두 선거의 과정에서 유권자들이 정확한 정보를 바탕으로 선거이슈를 판단하고 평가할 수 있는 가능성을 확보하고 이를 통하여 자금지배의 원칙을 실천하기 위한 목적에 입각하고 있는 것이다.

California대법원이 공직선거입후보자의 광고전단에 대하여 익명으로 우편배포할 수 없도록 한 주법을 합헌이라고 판단한 것<sup>20)</sup>은 이 두 사건의 판결취지를 그대로 이어받음으로써 가

15) 가장 대표적인 것이 CATO라는 이름으로 팜플렛을 발행하였던 George Clinton이나, Publius라는 가명으로 연방주의紙(The Federalist Papers)를 발행하였던 미국헌법의 아버지들(J. Jay, A. Hamilton, J. Madison) 등이다.

16) J. Wallace, op.cit.

17) Tally v. California, 362 U.S. 60(1960) 이 사건은, 광고용 전단(hadbill)에 그것을 제작하거나 배포하거나 또는 후원하는 자의 성명과 주소를 명기하지 않은 채 전단을 배포하는 것을 금하는 로스엔젤리스시의 조례(The ordinance, 28.06 of the Municipal Code of the City of Los Angeles)를 문언상 무효라고 선언하였다. 여기서 연방대법원은 위의 인용문에 이어, 악명높은 영국의 출판허가법이 미국식민지에까지 적용되게 된 것도 부분적으로는 출판자나 저작자 그리고 배포자의 성명을 노출시키는 것이 정부에 비판적인 작품의 유통을 억제할 것이라는 인식”에 의거한 것이라고 판단하였다.

18) 424 U.S. 1(1976)

19) 435 U.S. 765(1978)

능하였다. California대법원은 Buckley사건에서 연방대법원이 정치적 표현의 자유에 대한 제한은 언제나 일반적 표현의 자유와 동일한 정도의 엄격심사의 대상이 되는 것은 아니며, 정부의 이익과 공개가 강제되는 정보 사이에 중대한 상관관계(relevant correlation)' 또는 실질적인 관계(substantial relation)'가 있으면 된다고 판단한 사실을 중시하고 있다. 그래서 선거법에 있어서는 유권자가 가지는 수정헌법 제1조 및 제4조의 권리에 대하여 합리적이고 비차별적인 제한(reasonable and nondiscriminatory restrictions)'을 가할 뿐이라면 주정부의 규제가 가지는 중요한 이익의 존재만으로도 일반적으로 그 제한을 정당화할 수 있다는 판단을 내린다. 즉, 선거법과 관련하여서는 어느 정도의 이익형량이 가능할 수 있음을 선언한 것이다.

입후보자 등이 선거와 관련한 모든 대량우편(mass mailings)에 대하여 자신을 특정할 것을 요구하는 규정으로 인하여, 그들이 어떠한 우편을 전혀 보내지 않을 것을 선택할 수도 있다. 하지만, 우리가 보기에는 입후보자들이 자기 자신이나 상대방에 대하여 중요한, 진실한 정보를 우송하는 것을 억제하는 경우는 적을 것이다. 왜냐하면, 익명이든 아니든, 입후보자들은 스스로가 당선되기를 원하며, 이러한 욕망이 유권자들에게 자신들의 견해를 알리고, 유권자가 될 가능성이 있는 자들에게 상대방에 대하여 좋지 않은 정보를 제공하도록 만들 것이기 때문이다. 하지만, 입후보자들은 거짓된 우편을 송부하는 것은 억제하게 될 것이다.

California대법원은 이러한 실명표기의 강제가 입후보자들로 하여금 유권자에게 올바른 선거 정보를 전달하는데 기여할 뿐 아니라, 거짓된 정보를 흘리는 폐단을 예방하는 데 도움이 될 것이라고 판단한다. 그러면서 동시에 그 강제장치로 인하여 올바른 정보의 유통에 어떠한 부담을 지우는 일은 없을 것이라 단언한다. 바로 이 때문에, California대법원은 입후보자가 블랙메일을 우송하거나, 자신에 대한 지지도를 조작하여 선거구민들에게 거짓 선전을 함으로써 유권자의 올바른 판단을 흐리게 하는 것을 막고자 하는 주의 이익이 Gristet이 누리는 정치적 표현의 자유를 능가한다고 본 것이다.

### 3.2. 통신실명제: 위헌론과 합헌론

실제 이상과 같은 실명제에 관한 찬반의 양론은 엄밀히 자유주의적 전통과 공화주의적 전통이 교차하는 미국의 정치이념적 흐름과 무관하지 않다. 전자의 전통은 개인의 자유와 권리에 대한 국가적 개입이나 제한을 과감히 배제함으로써 제한정부를 통한 자유공간을 창출하고자 노력하고 있는 반면, 후자의 전통은 자가지배의 원칙을 실천하기 위하여 모든 유권적 시민이 스스로의 판단에 의하여 능동적으로 정치과정에 참여할 수 있는 제반의 환경을 조성할 것을 촉구한다. 이에 의사소통의 과정에 있어서도 전자의 경우에는 표현자의 표현의 자유라는 것이 중시되는 반면, 후자의 경우에는 상호간의 정보의 교환과 그를 통한 토론과 합의의 가능성이 전면에 나선다.

그래서 ACLU나 EFF 등과 같은 자유주의적 진영에 속하는 집단들은 통신실명제에 대하여는 극렬한 언조로 반대하는 입장을 취한다. 그들은 그 실명제는 전통적으로 미국의 정치사

---

20) Gristet v. Fair Political Practices Commission, 884 P.2d 116(1994)

회를 구성하여 왔던 사상의 자유시장을 훼손하는 부당한 국가개입이며, 이를 통하여 자유롭게 자신의 의견을 개진하여 왔던 사람들의 입과 눈을 막는 결과를 야기하게 될 것이라고 본다. 그 중에서도 특히 CATO연구소나 EFF 등과 같이 일종의 캘리포니아 이데올로기<sup>21)</sup>에 입각하고 있는 입장들에서는, 정보통신기술이 가지는 탈권력적 성격 내지는 해방의 능력을 활용함으로써 전자아고라(electronic agora)와 같은, 일종의 제퍼슨식의 민주주의나 전자시장과 같은 보다 완전한 형태의 자유경쟁시장체제를 실현할 수 있다고 보고, 정보통신기술이 사회의 억압적 권력구조를 해체시키고 개인들로 하여금 자신의 문제를 결정할 수 있는 실질적인 힘을 부여하게 되며, 이를 바탕으로 개인적 자유의 신장과 국가권력 및 독점기업권력의 축소가 가능할 것이라고 주장하는 만큼 더욱 이러한 국가적 개입을 허용하는 통신실명제는 위헌적이지 사회적인 악으로 개념화되게 된다.

반면에 공화주의적 입장은 사상의 자유시장론과 달리 공적 문제에 관한 의견의 다양성을 확보하기 위한 국가적 개입의 필요성을 강조한다는 점에 있다. 이러한 초기의 공화주의적 사고들을 가장 정치한 형태로 정리 발전시킨 대표적인 인물인 C. Sunstein(1993, 203)은, 표현의 자유란 시민들로 하여금 공공의 문제에 대한 관심과 정보를 획득하는 수단이자, 이를 바탕으로 시민들이 토론과 합의의 과정을 통하여 민주적 자기지배를 관철하는 중요한 계기를 이룬다고 하면서 따라서 표현의 자유는 심의적 민주주의(deliberative democracy)를 실천하는 토대로서의 의미를 가진다고 주장한다. 그래서 그는 계약자유 원칙에 대한 중요한 공적 통제를 가하였던 뉴딜정책에 비견하여 민주주의의 실천을 위하여 표현의 자유에 대한 공적 규제를 촉구하는, 표현의 자유에 대한 뉴딜이 필요하다고 역설한다.<sup>22)</sup> 즉, 정치자금에 대한 상한선 설정 및 선거입후보자에 대한 무료방송광고시간배정, 반론권의 인정, 공적 내용의 방송에 대한 보조금의 지급이나 그 채널 및 시간의 할당, 교육용 방송프로그램의 개발 및 지원 등 일련의 표현내용을 중심으로 표현행위의 구조를 조정하는 공적 규제장치는 정치적 표현의 다양성을 확보하고 그것을 통하여 시민들이 공적 문제에 대한 심도있고 광범위한 관심을 획득할 수 있도록 하여야 한다고 보는 것이다.(op.cit., 205ff)<sup>23)</sup> 이러한 맥락에서 Sunstein(1996)은 표현, 특히 정치적 표현에 있어서의 실명화는 토론과 합의의 기반이 되는 책임(accountability)의 문제를 담보하는 기본전제라고 주장한다.

### 3.3. 소결

이러한 미국의 논의과정은 일단 세 가지로 압축된다. 첫째, 실명제의 논의는 표현의 자유에

21) 이에 관하여 자세한 것은, R. Barbrook and A. Cameron 참조.

22) 그에 의하면 사상의 자유시장으로 은유되는 관점은 그 시장 자체가 법과 제도에 의하여 결정된다 는 사실을 은폐하는 것이며, 따라서 자유방임주의(laissez-faire)는 그 자체 의도가 의심스러운 허구 (conspicuous fiction)에 지나지 않는다고 한다.

23) 이러한 논의를 뒷받침하기 위하여 C. Sunstein은 New York Times v. Sullivan, 376 U.S. 254(1964)사건에서 언론기관이 현실적 악의(actual malice)를 갖지 않는 한 자유롭게 공적 인물을 비판할 수 있다고 선언한 예와 Red Lion Broadcasting Co. v. F.C.C., 395 U.S. 367(1989)사건에서 공정성의 원칙(fairness doctrine)에 의거하여 반론권을 인정한 예를 들고 있다. O. M. Fiss(1993)의 경우는 기독교적 윤리관에 입각하고 있다는 점에서 약간 다른 출발점을 보이기는 하지만, 역시 이러한 논거에 입각한다. 또한 J. H. Ely(1980, ch.4) 역시 같은 맥락에서 법원은 다수자에 어떠한 실질적 가치를 부과하기 보다는 민주적인 절차적 공정성을 추구하고 또 그 집행을 감시하는 것이 주된 역할이라고 주장한다.

대한 제한의 범주에 해당한다. 즉, 표현자의 신상에 관한 정보를 표현에 즈음하여 공개하는가의 여부는 그 표현의 중요한 내용이며, 따라서 이에 대한 공개의무의 부여는 표현의 자유에 대한 유의미한 제한행위가 된다는 것이다.<sup>24)</sup> 둘째, 이러한 이유로 인하여 실명제에 대하여는 표현의 자유에 대한 일반적인 법리-엄격심사 및 문언상 무효의 법리-가 적용될 수 있다.<sup>25)</sup> 셋째, 인터넷이나 사이버공간에서 이루어지는 의사소통이라 할지라도 이러한 표현의 자유에 관한 법리의 적용에 있어 특별한 대우나 예외가 인정되는 것은 아니다.

문제는 두 번째의 사항 즉, 엄격심사와 문언상 무효의 법리이다. 위에서 언급한 실명제와 관련한 사건들이 모두 범죄의 억지 또는 자기지배의 원리의 실천이라는 중차대한 국가적 이익(compelling interest)을 지향하고 있으며 또 그에 대한 국가측의 입증도 유효하게 존재하고 있다. 하지만, 그럼에도 불구하고 그 입법들이 위헌적인 것으로 판단되거나 그 의심을 받게 되는 것은 그것이 현실적으로 보호되어야 할 여타의 표현영역들-즉, 범죄의 목적 또는 유권 자기방의 목적이 아니라, 따돌림이나 편견 차별의 회피 등 사회적 해악으로부터 자유롭기 위하여 익명을 선택하는 경우-에까지 영향을 미치고 따라서 광범위하니까 무효라는 법리의 적용대상이 되기에 이르기 때문이다. 앞서 제2절에서 실명제가 요청되는 유형중, 후자의 유형에 대한 규제를 위한 법규정이 오히려 전자의 사이버사회의 영역에까지 확장적용되어 건전한 의사소통까지 위축시키는 결과를 야기할 수 있게 되는 경우가 바로 그것이다. 역으로, 만약 이러한 냉각효과 및 과대확장효과(slipping slope effect)를 회피할 수 있는 입법기술이 존재하고 또 그것이 제대로 구현될 수 있다면, 그리고 그에 상응하는 국가적 이익을 입증할 수 있다면, 미국의 현재의 추세로는 얼마든지 실명제의 입법은 합헌판단을 받을 수 있는, 그러한 상황에 존재하고 있다.

이하에서는 이러한 논의<sup>26)</sup>를 중심으로 우리나라에서의 통신실명제의 도입가능성 및 그 실효가능성을 검증해 보기로 한다.

## 4. 우리나라에서의 실명제 현황

### 4.1. 구조: 법제 및 업계관행

우리나라에서 실명제의 논의가 이루어진 것은 그렇게 많지 않다. 입법례로서는 우선 「금융

---

24) 물론 실명제는 동시에 프라이버시에 대한 제한이기도 하지만, 우리나라와는 달리 미국연방대법원의 경우 프라이버시의 권리는 일단 수정헌법 제1조상의 표현의 자유로부터 도출하는 경향이 있으므로 이렇게 본다고 해서 크게 벗어난 것은 아니다.

25) 엄밀히 보아, 자유주의측의 입장과 공화주의측의 입장은 표현의 자유에 대한 제한의 법리에까지 영향을 미친다. 하지만, 이 두 입장이 갈등을 보이는 곳은 내용규제를 전체적으로 악으로 간주할 것인가(자유주의) 아니면 내용규제를 다시 경향규제(tendency regulation)와 좁은 의미의 내용규제로 나누어 전자는 악으로, 후자는 일종의 구조규제 내지는 구조조정의 한 방편으로 볼 것인가(공화주의)에 집중된다. 환언하자면, 실명제는 자유주의의 입장에서는 내용규제로서 일단 위헌의 추정대상이지만, 공화주의의 입장에서는 구조조정의 한 형태로서 California대법원의 판단처럼 일응 중간적 심사에 상당하는 보다 완화된 심사기준이 적용되게 된다.

26) 이는 미국의 논의를 중심으로 한 것이나, 표현의 자유에 관한 한 우리나라의 논의 또한 미국의 그것을 상당부분 받아들이고 있는 실정이므로 크게 정도에 벗어난 결론이 되지는 않는다.

실명거래및비밀보장에관한법률」이 실지명의에 의한 금융거래를 실시”함으로써 경제정의를 실현하고 국민경제의 건전한 발전을 도모함을 목적으로”(제1조) 모든 금융기관에 대하여 거래자의 "실지명의"(여기서 실지명의는 주민등록표상의 명의, 사업자등록증상의 명의 기타 대통령령이 정하는 명의를 말한다. 제2조 제4호)에 의하여 금융거래를 하여야 하도록 규정하고(제3조 제1항) 있다. 또한 「부동산실권리자명의등기에관한법률」은 부동산에 관한 소유권 기타 물권을 실제적 권리관계에 부합하도록 실권리자 명의로 등기하게 함으로써 부동산등기 제도를 악용한 투기 탈세 탈법행위등 반사회적 행위를 방지하고 부동산거래의 정상화와 부동산가격의 안정을 도모하여 국민경제의 건전한 발전에 이바지함을 목적으로”(제1조) 누구든지 부동산에 관한 물권을 명의신탁약정에 의하여 명의수탁자의 명의로 등기하여서는 아니 된다”(제3조 제1항)고 하여 실권리자가 자기의 명의로 등기할 것을 규정하고 있다. 그리고 이들 두 법률 외에는 명문의 규정으로써 일반국민들에게 그 실명을 밝힐 것을 강제하고 있는 경우는 존재하지 않는다. 다만, 소위 「정책실명제」와 관련하여 「사무관리규정」 제34조의2 제1항은 행정기관의 장으로 하여금 주요정책의 결정 또는 집행과 관련하여 주요정책의 결정 및 집행과정에 참여한 관련자의 소속 직급 및 성명과 그 의견”(제1호)을 기록 보존할 것을 명하고 있어 이점에서 일응의 실명제가 담보되고 있을 뿐이다.(이는 선거관리위원회사무 관리규칙 제34조의2도 마찬가지이다.)

하지만, 이러한 몇 안되는 법률에서 실명제를 강제하고 있는 것이 과연 합헌적인가에 관한 논의는 여전히 검증되지 않은 채 남아 있다. 이 부분에 관하여 헌법재판소는 금융실명제 그 자체에 대한 위헌여부의 판단은 하지 않았지만, 「긴급재정명령 등 위헌확인」사건(헌법재판소 전원재판부 1996. 2. 29. 93헌마186)에서 금융실명제를 실시하도록 한 긴급재정명령은 그 긴급성이 인정되어 합헌이라고 판단함으로써 간접적으로 금융실명제의 헌법적 효력을 인정 한 것으로 해석할 여지를 남기고 있다. 그러나 엄밀히 보자면 이 사건에서 금융거래에서의 실명을 강제하는 법률규정이 경제영역에서의 표현의 자유에 해당하는 계약자유 원칙(계약 방식선택의 자유)을 침해하였는지에 대하여 최소한 방론적인 수준에서의 언급은 있었어야 마땅하였다. 왜냐하면, 금융거래를 실명으로 할 것이냐 아니냐의 선택은 경제적 관계에서 자신을 드러낼 것인가 아닌가의 문제이며 그것은 일면에서는 표현의 자유의 문제이자 타면으로는 (경제영역에 있어서의) 사생활의 비밀과 관련한 자기노출의 선택권 문제와 직결되는 것이기 때문이다.

그러나 우리나라에서의 실명제 문제는 엄밀히 이러한 명시적 법규정의 문제라기 보다는 오히려 법체계 전반에서 나타나는 구조적 문제로 이어진다. 현행의 주민등록법은 모든 국민에 대하여 주민등록을 강제하고 있고,<sup>27)</sup> 또 주민등록을 관리하는 기관은 모든 국민에게 고유한 주민등록번호를 부여하도록 하고 있다.<sup>28)</sup> 뿐만 아니라, 주민등록법 제21조 제2항 제3호 및 제4호는 허위의 주민등록번호를 생성하여 자기 또는 다른 사람의 재물이나 재산상의 이익을 위하여 이를 사용한 자”와 허위의 주민등록번호를 생성하는 프로그램을 다른 사람에게 전달하거나 유포한 자”를 3년이하의 징역 또는 1천만원이하의 벌금에 처하도록 하여 2001.

27) 주민등록법 제6조 (대상자) ① 시장 군수 또는 구청장은 30일이상 거주할 목적으로 그 관할구역 안에 주소 또는 거소(이하 "거주지"라 한다)를 가진 자(이하 "주민"이라 한다)를 법의 규정에 의하여 등록하여야 한다.

28) 주민등록법 제7조 (주민등록표등의 작성) ③ 시장 군수 또는 구청장은 주민에 대하여 개인별로 고유한 등록번호(이하 "주민등록번호"라 한다)를 부여하여야 한다. <신설 2001.1.26>

1. 26부터 시행하고 있다.<sup>29)</sup>

이러한 상황에서 법원에서 사용하는 일부 문서를 제외한 거의 대부분의 공문서는 물론, 일반적인 사적 거래에서나 정보통신서비스에의 가입행위 대부분이 이와 같은 주민등록번호와 실명을 제출하도록 요구하고 있는 업계의 관행은 이미 별도의 법규정이 필요 없을 정도로 강력한 통신실명제를 담보하고 있는 것이다. 특히 행정자치부가 제공하고 있는 「주민등록진위확인 자동음성확인 전화서비스」는 주민등록번호와 주민등록증의 발급일자를 입력하면 그의 실명을 알려주는 서비스로서, 정보통신서비스업체로서는 이 세 가지의 정보만 이용자로부터 제공받으면 그가 실명을 사용하는지 아닌지를 곧장 알 수 있는 시스템이 구축되어 있는 실정이다.

이러한 상황에 미루어 본다면, 우리나라에서의 정보통신서비스의 이용실태는 주민등록제도와 ISP업계의 관행이 결합하여 거의 완벽한 형태의 통신실명제가 실시되고 있다고 하여도 과언은 아니다. 즉, 어떠한 통신행위에 관하여 법집행기관이 수사의 의지가 있다면, 최소한 당해 ID와 그 ID를 소지하고 있는 실체인물을 결합시킬 수 있는 추적가능성이 확보되어 있는 셈인 것이다.<sup>30)</sup>

## 4.2. 통신실명제와 정책목표

### 4.2.1. 개요

그러나 그럼에도 불구하고 또 다시 통신실명제가 논의되고 있는 이유는 무엇인가? 한국경제신문은 2001.03.07자에서 '인터넷 실명제 도입논란'이라는 제목의 리포트를 싣고, 최근 '인터넷 실명제'에 대한 강력한 요구가 나타나고 있음을 보도하고 있다. 이에 의하면 '헤티즌이 인터넷 서비스를 이용할 때 반드시 실명확인 절차를 거치도록 하겠다'는 것을 골자로 이를 통하여 인터넷의 '순화' 및 청소년의 탈선방지를 도모할 수 있을 것이라는 전망과, 인터넷의 '자유'이념이 크게 훼손되며 '빅브라더'가 지배하는 통제사회가 될 수 있을 뿐 아니라, 기술적으로도 완전을 기하기가 불가능하다는 소극적 의견을 보도하고 있다.<sup>31)</sup> 여기서 우리의 주목을 요하는 부분은 이러한 통신실명제의 목적이 인터넷의 '순화'와 청소년의 탈선방지에 놓여져 있다는 점이다.

통상적으로 통신실명제의 도입을 추진하는 입장에서는, 그것이 인터넷 내지는 사이버범죄를 예방하거나 그에 관한 법집행의 가능성을 확보한다는 점에 최대의 강조점을 둔다.<sup>32)</sup> 사이버

29) 이미 서울경찰청 사이버수사대는 6일 주민등록번호 생성 프로그램을 인터넷 사이트에 올려 유포 시킨 혐의(주민등록법 위반)로 대학생 安모(23)씨 등 인터넷 사이트 운영자 4명을 입건하였고, 경찰은 관련 사이트 운영자 32명의 신원을 파악, 조사 중이며 이중 미성년자가 19명(59%)이고 형사처벌 대상이 아닌 14세 미만도 7명(22%)이라고 밝혔다. 중앙일보 2001.06.06 (수) 18:40 :<http://news.naver.com/read?command=read&id=2001060600000159012>

30) 이 점은 사이버공간의 해방성을 주창하는 J. Wallace & M. Mangan(1997, 257)의 경우도 마찬가지이다. 그들은 사상의 자유시장에서는 누가 말하였는가 보다는 어떤 내용이 교환되는가가 더 중요한 것이라고 하면서, 현실공간에서와 마찬가지로, 인터넷상에서 어떠한 범죄가 저질러진 경우에는 언제나 흔적을 남기게 되며, 실명제를 도입하지 않더라도 인터넷상의 범죄자의 신원을 확인할 수 있는 것이 일반적이라고 한다.

31) <http://news.naver.com/read?command=read&id=2001030700000529042>

32) 일례로 1999년 형사정책연구원에서 실시한 여론조사에 의하면 통신실명제의 법제화를 찬성하는 비율이 약78%에 이르고 있다고 한다(정진수 외, 2000). 하지만, 이 여론조사는 사이버성폭력과 연

사기나, 크래킹등의 지적 재산권 침해행위, 혐의의 컴퓨터범죄 등에 대하여 실명제를 도입함으로써 범죄로의 충동을 억제하고, 사후적으로도 그 죄증의 확보를 용이하게 한다는 점에 비중을 두는 것이다. 또는 전술한 바와 같이 공화주의적 입장에서는 정치적 토론과 합의를 바탕으로 하는 자금지배의 원칙의 실천을 위하여 모든 정치적 언술에 책임과 신뢰의 토대를 마련하기 위한 방편으로서 실명제의 도입을 주장하기도 한다. 물론 보수적인 성향이 강한 공동체주의의 입장에서는 미덕(virtu)을 실천하는 방법으로서의 실명제라는 주장도 없지는 않다. 하지만, 그럼에도 불구하고 그 어떠한 논의틀 속에도 이렇게 모호한 형태의 목적을 바탕으로 실명제를 도입하겠다는 주장은 나타나지 않는다.

문제는 이러한 입법목적이 과연 표현의 자유에 대한 제한의 사유로서 헌법적으로 유효하게 승인될 수 있는 것인가 라는 점이다. 이하에서는 이를 포함하여 통신실명제의 실시를 정당화한다고 일응 논의되고 있는 범죄억지 내지는 법집행가능성의 확보라는 요청과 인터넷의 순화'와 청소년의 탈선방지라는 요청이 가지는 헌법적 타당성을 검토하고 그에 수반하는 제반의 문제점들을 분석한다.

#### 4.2.2. 법집행가능성의 확보수단으로서의 통신실명제

##### 1) 예방목적의 통신실명제

통신실명제의 도입을 주장하는 입장에서 가장 유효한 입법목적으로 거론하고 있는 것이 법집행가능성의 보장목적이다. 익명의 정보통신행위는 전술한 바와 같이 죄증을 비약할 수 있는 최적상황을 보장하고 있을 뿐 아니라, 정보통신 그 자체가 사이버사기나 지적 재산권침해행위 등 범죄의 수단 또는 객체로서 존재하고 있는 만큼, 이 부분에 대한 국가적 통제는 상당한 당위성을 확보하고 있다.<sup>33)</sup> 이에 미국연방법원에서도 이러한 국가목적은 정보통신행위를 통한 표현의 자유라는 기본적 권리까지도 제한할 수 있는 정당한, 그리고 필수적인 국가이익임을 인정한 바 있다. 위에서 인용한 ACLU v. Miller사건은 이 점에서 대표적인 것이다.

하지만, 이러한 국가목적을 위하여 통신실명제를 도입한다고 할 때, 과연 그것이 표현의 자유를 지배하는 사법심사기준들을 통과할 수 있을 것인지는 별개의 문제이다. 허위의 사실 또는 명예훼손이나 과장된 의견을 인터넷상에 게시하는 경우를 규제대상으로 함으로써 사이버사기를 억지하고자 하는 국가목적은 구체화시키면서 동시에 냉각효과(chilling effects)와 법집행기관의 자의적 권력행사를 방지할 수 있는 잘 차단된 입법이 가능할 수 있겠는가 문제인 것이다. 실제, 이러한 국가목적을 위하여 모든 인터넷게시물에 실명제를 도입한다고 하는 것은 과잉규제금지 즉 광범위하여 무효라는 법리를 벗어나기 힘들며, 그 자체 심각한 내용규제로서 위헌의 소지를 안게 된다.<sup>34)</sup> 특히 1998년 안에서 강조되고 있는 사이버사기는

관하여 실시됨으로써 익명성-범죄성이라는 예단이 응답자에게 제시될 가능성이 농후한 것인 만큼 그 찬반여론의 정확성 및 신뢰성은 의문이다.

33) 정완(2001)은 이러한 취지에서 실명제도입이 사이버범죄에 대한 억제효과를 가진다고 보고 이를 적극 도입할 것을 주장하면서 과도기적으로 타인의 명의 ID 주민등록번호의 사용을 형사법적으로 금지할 것을 주장하고 있다.

34) 예컨대 정부게시판을 명예훼손 유언비어 등으로 오용하는 일부의 네티즌들을 억지하기 위하여 모든 네티즌들에게 실명을 강제한다는 점에서 과잉규제(overbreadth)에 해당하며, 명예훼손 유언비어의 개념과 소위 '견전한' 의사소통과의 구분이 명확하지 않으며 그 판단의 주체도 명시적이지 않다

상대방의 기망을 구성요건적 요소로 하고 있다는 점에서 그 행위의 태양을 특정하는 것이 상당히 곤란한 상태에 있다. 광고행위에서 어떠한 부분까지가 사회적으로 인용가능한 광고이며 어디부터 무가치판단의 대상이 되는 과장광고인지를 구획할 수 있는 별다른 기준도 없는 상황인 것이다. 따라서 이러한 부분을 성급하게 개념화하고자 할 경우 그 법규정의 모호성으로 인한 위헌판단의 소지를 안게 된다. 더구나 위의 Miller사건의 예에서와 같이 교육이나 뉴스전달, 또는 논평의 목적을 위하여 다른 표현을 자신의 표현에 결합시킬 경우 이 때에도 실명을 강제하여야 할 것인지를 판단 또한 모호한 상태로 남게 된다.

뿐만 아니라, 실명제가 가지는 가장 큰 문제점은 그것이 표현의 자유라고 하는 헌법상의 기본권을 실질적으로 제약한다는 점이다. 정보통신부의 2003년 안을 보면 정부개설 게시판에 나타나는 명예훼손, 유언비어 및 저속표현(욕설, 비어 등)을 방지하는 것이 주된 목표로 제시되어 있다. 여기서 명예훼손이나 유언비어와 같은 것은 형사법의 규제대상으로 위에서 언급하였으므로 다시 논의할 필요는 없다. 하지만, 저속표현을 실명제의 방식에 의하여 억지하고자 하는 정책목표는 이 저속표현이 가지는 의사소통상의 기능과 의미를 심히 왜곡하는 것이어서 상당한 헌법적 문제를 야기한다. 즉, 그것을 규제한다는 것은 자신의 의견이나 입장을 논리적으로 풀어낼 수 없거나 그렇게 하고 싶지 않은 시민의 상당부분을 의사표현의 기회로부터 배제하는 결과를 야기한다. 정부정책이나 업무에 대하여 비판의 논리가 아니라 부정적 정서와 감정을 표현하고자 하는 네티즌들이 정부게시판을 통하여 직접 의사소통할 수 있는 기회가 박탈되는 것이다.<sup>35)</sup>

한 마디로 이러한 형태의 실명제는 목적의 정당성에도 불구하고 그 실천을 위한 수단의 선택(수단의 적정성의 요청)에서부터 규제의 최소성의 요청 등이 심각하게 위반될 소지를 적지 않게 내포하게 된다. 특히, 기존의 형법상의 사기죄 등 오프라인에서 적용되는 각종의 형사법규에 의하여 법금(法禁)되고 있는 행위들에 대하여 실명제와 같은 별도의 장치를 마련하는 것은 행위자와 죄증을 추적하는 형사사법기관의 수사상의 편의만을 도모하는 방편적인 것이 되기 쉽고, 이 과정에서 자칫 법규정이 모호하거나 애매한 형태로 규정되어 있음을 이용하여 자의적인 수사나 법집행이 이루어질 가능성이 충분히 존재하게 된다. 더구나 처음부터 기망과 사기의 목적으로 정보통신서비스를 이용하고자 하는 범인의 경우에는 실명제의 존재에도 불구하고 차명이나 허명, 또는 Remailing service 등을 이용하여 법망을 빠져 나가 고자 할 것인 만큼, 이러한 목적을 위한 실명제의 도입은 오히려 처음부터 범의가 없이 단순한 표현 또는 거래행위로 나아가고자 하는 사람들이 본의 아니게 피해를 보는 경우까지도 발생할 수 있게 된다. 그렇다면 이러한 목적을 위한 통신실명제는 거의 대부분이 잘 차단된 입법(narrowly tailored legislation)이라는 심사에 탈락하는, 위헌적인 것이 될 가능성이 농후한 것이다.

## 2) 사후교정수단으로서의 추적가능성

요컨대, 범죄에 대한 일반예방의 수단으로서 통신실명제를 도입하고자 하는 것은 따라서 바

---

는 점에서 모호성(vagueness)의 법리가 적용될 수 있다.

35) 여기서 강조할 것은 저속표현 역시 헌법 제21조상의 보호대상이 되는 표현행위라는 것이다. 물론 청소년보호 등 별도의 필요가 있는 경우에는 어느 정도의 규제대상이 될 수 있을 것이나 그것은 예외적인 상황에서 적용되는 것일 뿐이며, 국가를 상대로 하는 비판과 견제의 기회를 제공하는 정부게시판에는 특별한 경우가 아닌 한 제대로 보호받아야 한다.

람직하지 못하다. 오히려 그것은 사업자의 수준에서 (행정지도의 방식을 통하여) 자율적으로 이루어지도록 하는 것이 바람직할 것이다. 하지만, 이러한 일반론적 논의가 표현자의 실제 명의를 파악하는 것을 모두 부인하는 것은 아니다. 어떠한 범죄가 사이버공간상에서 발생한 경우 사후적으로 그 범죄인을 추적하기 위한 장치가 마련되어야 할 필요가 있기 때문이다. 또한 사이버공간상의 행위로 인하여 어떠한 분쟁이 발생하고 이 분쟁을 처리하기 위하여 분쟁당사자의 현실적 신원을 특정하여야 할 필요성도 엄연히 존재한다. 특히 후자의 경우에는 영장에 의한 강제수사권을 가지고 있는 형사사법기관의 경우와는 달리, 민사상의 가해자의 신원을 확보하기 위한 실효성있는 장치를 어떻게 구축할 것인가는 아주 중차대한 문제로 제기된다.

정보통신서비스를 제공하는 자가 이용자의 현실적 신원을 파악하고 있는 것이 일반적이라는 우리의 정보통신현실에 대하여는 이미 서술하였다. 여기서 문제는 사이버공간에서 피해를 당한 자를 어떻게 보호할 것인가이다. 즉 이 피해자가 이러한 사인(私人)으로서의 정보통신서비스제공자로부터 어떻게 행위자의 현실신원에 관한 자료를 확보할 수 있을 것인가라는 점에 주안점을 두어야 한다. 환언하자면 사이버공간상에서 행위한 자의 인격-아바타-과 그 자의 현실적 인격-현실적 신원을 연결시킬 수 있는 매개자료로서의 접속기록을 어떻게 확보하고 또 활용할 수 있을 것인가라는 점이다. 이를 접속기록보관문제와 접속기록공시문제로 나누어 살펴본다.

첫째, 사이버공간상의 일탈행위를 한 자를 추적함에 있어 IP주소추적방법은 가장 기본적인 것이다. 정보통신서비스제공자의 서버에 기록되어 있는 접속기록에서부터 그 행위자가 서버에 접속하게 된 컴퓨터의 IP주소를 추출하고 이를 바탕으로 그 자의 신원을 탐색하는 방법이 그것이다(이광현, 2001). 통상적으로 서버관리자는 보안등의 이유로 자신의 서버와 접속되는 다른 컴퓨터의 IP주소와 시간 등을 기록하는 log file을 작성하고 이를 보관한다. 하지만, 정보통신사업자가 이용자-아바타를 연결지을 수 있는 log file을 보관하지 않거나 접속속도문제 등을 이유로 기록하지 않고 있는 경우, 또는 서버관리자등이 고의적으로 이 log file을 삭제, 수정하는 경우에는 행위자의 추적 자체가 원천적으로 곤란하게 될 상황에 부딪힐 수 있다. 이에 대하여 이광현(2001)은 두 가지의 방안을 제시하고 있다. 첫째, 정보통신망운영업체(최소한 정보통신사업자)는 그 접속기록을 작성하고 일정기간 이상 보관하여야 할 의무를 규정하는 입법을 추진할 필요성이 있으며,<sup>36)</sup> 둘째, 접속기록을 프린터로 연속출력하거나 편집불가능한 CD-ROM에 저장하는 등, 접속기록을 삭제할 수 없는 매체에 저장하도록 하는 방법을 고려할 수 있다는 것이다. 물론 이러한 입법은 일정한 내용을 기록하고 또 보관하도록 강제한다는 점에서 헌법 제21조(표현의 자유) 및 제15조(영업의 자유)에 대한 제한이기는 하나, 통상적으로 서버의 보안을 위하여 접속기록의 작성 보관은 가장 기초적으로 요청되는 것이며, 그 비용 또한 그렇게 과중하지 않다는 점에서 위헌의 시비는 해소될 수 있을 것으로 보인다.

둘째, 문제는 정보통신서비스제공자가 접속기록을 작성 보관하고 있다 할지라도 그것을 일정한 경우 개시할 것을 강제하는 입법 또는 장치의 가능성이다. 이 부분에서 가장 문제가 되

36) 사이버범죄와 관련하여 이렇게 사후교정적 목적으로 위하여 증거확보의 차원에서 일정기록을 작성, 보관하도록 한 예는 아직 발견되지 않는다. 다만 정보통신망이용촉진및정보보호등에관한법률(개정 20 01. 1.16 법률제6360호) 제43조는 청소년유해매체물을 제공하는 정보제공자에 대하여 당해 정보를 대통령령이 정하는 기간동안 보관할 의무를 부과하고 있다.

는 것은 명예훼손 등과 관련한 민사소송법의 규정이다. 실제 명예훼손의 경우 2001.1.16일 개정된 정보통신망이용촉진및정보보호등에관한법률(2001.7.1 발효)은 제61조에서 정보통신망을 이용하여 타인의 명예를 훼손하는 행위를 별도의 범죄로 규정하고 있어 주로 형사법적 측면에서 다루어지고 있고 이 과정에서 명예훼손의 가해자를 강제수사의 방식에 의해 특정할 수 있다는 점에서 법제상의 문제는 그리 크지 않다. 다만, 모든 명예훼손사건을 형사사건으로 비화시킨다는 점에서는 법과잉의 폐단이 야기된다. 즉, 민사상의 구제조치로서도 충분한 사건을 형사문제로 하면서 범법자를 양산하는 현실을 초래하는 것이다. 하지만, 그렇다고 해서 현재의 민사소송구조를 이용하기에는 상당한 난점이 존재한다.

이에 사인인 피해자의 입장에서 가해자를 특정할 수 있는 방법이 부재한다는 점을 감안, 민사소송절차에 임시의 당사자를 선정하고 그를 피고로 명예훼손에 관한 소송을 일단 제기한 후, 당해 정보통신사업자에 대하여 피고의 신원사항에 대한 정보를 공개할 것을 명령하는 중간판결을 하도록 하는 한편, 그 정보공개에 따라 피고를 특정할 수 있도록 하는 장치가 필요하다.

#### 4.2.3. Virtu'의 구현방식으로서의 실명제

오늘날 우리나라에서 통신실명제를 도입하고자 하는 가장 큰 이유중의 하나가 인터넷의 순화'와 청소년의 탈선방지라는 국가목적이다. 물론 이러한 국가목적, 특히 청소년보호의 부분은 누차에 걸쳐 표현의 자유에 대한 제한목적으로 그 정당성을 인정받아 왔다.<sup>37)</sup> 특히 새로이 등장하는 사이버문화의 주역이 청소년 및 20대의 청년층이라는 점을 감안한다면, 이들을 대상으로 하는 심도깊은 인터넷정책이 시행될 필요성은 충분히 존재한다. 하지만, 그렇다고 해서 이러한 정당한 국가목적이 그대로 통신실명제라는 정책수단과 직결될 수 있음을 의미하는 것은 아니다.

엄밀히 보자면 통신실명제는 청소년보호라는 국가목적을 달성하기 위한 실체적 수단이라기 보다는 오히려 그러한 목적이 손쉽게 달성될 수 있는 일종의 환경적 주변적 변수를 형성하는 것이다. 실명을 사용할 경우 음란과 같은 범죄적 행위로 나아감에 대하여는 억지력을 가지겠지만, 저속이나 사회적 일탈과 같은 하위가치'의 표현행위로 나아가는 것에 대하여는 별다른 억지력을 가지지 못하기 때문이다. 이는 마치 홀리건의 예에서 보듯, 현실공간에서 개개인의 정보가 다 노출될 수 있음에도 불구하고 군중속에 묻혀 있음을 계기로 일탈적 행위로 나아가는 경우와 유사하다. 집단심리에 휘말리는 경우와 같이 주변환경에 따라서 개인의 행동이 달라지는 것은 실명확인가능성의 여부와는 거의 무관하게 이루어진다는 것이다.

이러한 맥락에서 본다면, 통신실명제는 청소년 보호 또는 인터넷의 순화라는 국가목적에 대한 하나의 필요조건 내지는 주변적 매개조건은 될 수 있을지 몰라도 그를 위한 충분조건으로서의 성격은 갖지 못한다. 환언하자면, 필수적인 국가이익과 그 수단과의 관계가 엄격한 인과적 관련성을 갖지 못하는 것이다. 물론 전술한 것처럼 표현의 자유에 대한 규제에 있어서도 경우에 따라서는 중대한 상관관계(relevant correlation)' 또는 실질적인 관계(substantial relation)'가 존재하고 규제의 방법이 합리적이고 비차별적인 제한(reasonable and nondiscriminatory restrictions)'에 해당한다면 합헌이라고 보는 완화된 심사기준이 존재하기는 하지만, 이는 청소년보호나 인터넷의 규제라고 하는 국가목적범주와는 다른 차원에서 논의되는 것이라는 점에서 원용하기 어렵다. 즉, 이러한 완화된 심사기준은 자기지배의

37) 대표적인 것이 CDA사건으로 알려진 ACLU v. Reno, 117 S.Ct. 2329(1997)판결이다.

원칙을 가장 중요한 헌법이념으로 삼고 있는 미국의 경우에 공화주의적 관점에서 정치적 표현의 자유를 수정적으로 이해하는 과정에서 나오는 일종의 변형된 심사기준일 뿐, 그것이 모든 표현영역에 그대로 타당함을 의미하는 것은 아닌 것이다.

또한 설령 이러한 완화된 기준을 적용한다 할지라도 결과는 마찬가지로 된다. 통신실명제는 국가가 정보통신이용자들을 실명의 형태로 감시 감독하는 것을 가능하게 한다. 누구든지 자신의 실명 즉, 자신의 실체 그대로나 또는 익명이나 별명을 사용한다더라도 약간의 추적을 통하여 자신의 실명이 드러날 수 있는 가능성을 인식한 채 정보통신에 임하게 되고 따라서 자신의 모든 정보통신행위 그 자체에 대하여 스스로 책임을 지게되는 구조를 형성하게 된다. 이는 역으로 이러한 책임을 담보로 전국가적인 감시장치가 작동됨을 의미하게 된다. 바로 이 점에서 인터넷의 순화 또는 청소년의 보호라고 하는 일반적인 중국목적에 실명제를 바로 결합시키는 것은 오히려 국가에 의한 사이버공간의 절대적 종속이라는 결과만을 야기하게 될 가능성이 충분히 존재하는 것이다. 부연하자면, 인터넷의 순화 또는 청소년의 보호라는 국가목적은 다시 구체적인 중간목적으로 세분하거나 개별화시키지 않은 채 그냥 그대로 실명제와 결합시키게 되면(중대한 상관관계 또는 실질적인 관계의 부재) 그 자체 국가가 사이버공간을 통제할 수 있는 다양한 권력수단을 마련하게 되는 역기능이 발생할 수 있는 것이다. 이는 문자 그대로 냉각효과와 더불어 확장효과(slipping slope effects)로 상징되는 자의적 제한의 가능성을 열어 놓는다.

여기서 무엇보다도 문제적인 것은 인터넷의 순화, 또는 청소년의 보호라는 국가목적의 추상성이다. 순화'라는 용어의 의미가 가지는 권력성은 차치하고서라도, 그 순화'의 상대방에 놓여 있는 사이버문화의 다양성보장(헌법 제9조)이라는 요청과의 관계 설정은 어떻게 되어야 할 것이며, 나아가 순화'된 사이버공간의 모습은 과연 어떤 것이어야 할 것인지- 법금(法禁)의 대상인 음란표현은 제외한다 할지라도, 저속한 표현이나 일탈적 표현의 개념과 경계는 어떻게 설정될 것인지, 연령이나 지역, 계층, 문화 등의 요소에 따른 가치관의 차이는 어떻게 처리할 것인지 등-, 사이버공간과 현실공간-이야말로 너무도 순화'되어 있지 않다!-의 관계는 어떻게 설정할 것인지 등의 문제가 하나도 해결되지 않은 상태에서 이 순화를 위하여 표현의 자유를 제한한다는 것은 그 자체 과잉의욕'으로서 위험이라 하지 않을 수 없다.

## 5. 결론

1997년 11월 캘리포니아 어빈에서 열린 미국과학발전협회(the American Association for the Advancement of Science)는 「학술의 자유, 책임 그리고 법(Scientific Freedom, Responsibility and Law)」라는 주제로 심포지움을 가지고 그 논의결과를 하나의 권고형식으로 발표하였다. 그 중 인터넷상에서 익명으로 의사소통하는 것과 관련하여서는 다음과 같은 네 가지의 권고안을 제시하였다.(Al Teich, et.als., 1999).

- ① 온라인상에서의 익명의 의사소통은 도덕적으로 중립적인 것이다.
- ② 익명의 의사소통은 강력한 인권으로 간주되어야 한다: 미합중국에서는 그것은 헌법적인 기본권이다.
- ③ 온라인공동체는 익명의 의사소통을 허용할 것인지에 관한 독자적인 정책을 수립할 수 있어야 한다.
- ④ 개인은 자신의 신원이 온라인상에서 공개되는 범위에 관하여 정보를 획득할 수 있

어야 한다.

그들에 의하면 온라인에 있어서의 익명성은 그 자체 악도 아니며 선도 아니라고 한다. 단지, 그것이 어떻게 사용되는가에 따라 악할 수도, 선할 수도 있는 것이며, 따라서 익명성의 해악에만 관심을 가지고 규제하게 되는 경우 익명성의 순기능을 저해할 뿐 아니라, 인터넷 발전 그 자체까지도 심각하게 훼손할 수 있게 된다고 경고하고 있다. 또한 익명성은 그 자체 유엔 인권선언이나 각국의 헌법에서 도출될 수 있는 기본적 권리-인권으로서 이에 대한 제한은 반드시 오프라인에서의 제한과 동일한 수준과 맥락에서 이루어져야 하며, 온라인에 대하여만 특별히 제한하는 것은 바람직하지 않다고 본다. 그리고 익명성의 허용여부에 대한 판단은 국가가 아니라 그 의사소통의 공간을 형성하는 당해 사이버공동체가 하여야 할 것임을 분명히 하고 있다.

이 권고문은 이어 통신실명제에 갈음할 수 있는 대안으로 교육과 홍보, 그리고 정보통신이용자들을 대상으로 하는 윤리강령의 마련 등의 방안을 제시하고 있다. 법으로 강제하는 것은 전술한 바와 같은 헌법문제를 야기함과 동시에 remailer의 존재, 암호화의 문제, 국제간 협력의 문제 등 그 실효력을 결정적으로 떨어뜨릴 장애요소가 적지 않음도 지적하고 있다. 실제, 통신실명제는 엄밀히 보자면 법의 문제라기 보다는 구조의 문제이다. 우리나라의 예를 들자면, 오프라인 공간에서 법으로써 강제하지 않더라도 실명확인 방법으로 주민등록번호와 주민등록증을 사용하는 것이 보편화의 수준을 넘어서서 당연한 상식으로까지 되어 오히려 프라이버시 내지는 개인정보보호라는 역의 논의에까지 이르고 있다.

현대사회가 탈공간화, 탈시간화의 추세를 밟아 가면서 공동체적 생활관계에 와해되고 인간대 인간의 관계가 주로 개별화된 코드의 확인을 우선하는 형태로 변이되면서 실명의 문제는 인간관계의 신뢰성을 확보하는 중요한 발판이 되고 있는 것은 사실이다. 통신실명제가 나름의 의미를 가지는 것도 이 때문이다. 그것은 무엇보다도 검열과 같이 최우선적 기본권으로서의 표현의 자유에 대한 직접적인 공권력행사라는 헌법상의 부담을 지지 않은 채 간접적이고 우회적인 방법으로 건전한 정보유통문화를 조성할 수 있고, 나아가 사회적 일탈행위에 대한 형사법적 규제나 행정적 규제가 가지는 한계-주로 사후적 통제에 그침-를 극복하면서 사전적으로 불건전정보가 통제될 수 있는 유효한 틀을 제공하게 된다는 적극적 평가를 받기도 한다. 개인에 인정되는 사적 자치에 입각한 개인적 자율성의 존중이라는 법이념과 건전한 정보통신문화를 구축함으로써 사회질서를 유지, 강화하여야 할 국가적 의무가 가장 유의미한 방법으로 조화될 수 있기 때문이다. 하지만, 그럼에도 불구하고 그것은 위에서 언급한 헌법문제 외에도, 다음과 같은 점에서 헌법문제를 야기하게 되며, 따라서 그 도입은 극도의 신중함과 엄밀성을 가지고 고려되어야 할 것이다.

첫째, 실정법상의 문제로 공공기관의개인정보보호에관한법률과의 조정여지가 남아 있다. 이 법률에서는, 개인정보를 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호등의 사항에 의하여 당해 개인을 식별할 수 있는 정보”로 규정하고 보충적으로 당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것”도 포함하고 있다.(제2조) 이러한 개인정보를 보유하는 기관의 장은 다른 법률에 의하여 보유기관의 내부에서 이용하거나 보유기관외의 자에게 제공하는 경우를 제외하고는 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니”되며(제10조 제1항), 당해 개인정보화일의 보유목적외의 목적으로 처리정보를 이용하거나 다른 기관에 제공할 수 있”는 예외적인 경우를 아주 한정하여 규정하고 있다.

(동조 제2항) 뿐만 아니라, 금융실명거래및비밀보장에관한법률 제4조(금융거래의 비밀보장)에서는 누구든지 금융거래의 내용에 대한 정보 또는 자료를 타인에게 제공하거나 누설하여서는 아니”됨을 선언하고 있다.

이러한 상황에서 공공기관의개인정보보호에관한법률상의 공공기관에 해당하는 한국정보통신진흥협회나 행정자치부등이 자신이 보유하는 개인정보를 정보통신서비스에의 가입조건으로 공개하는 것은 불가능한 실정이다. 물론 이 경우에 각 부가통신사업자가 약관으로 개인정보의 조회에 대한 동의여부를 묻고 그 동의에 기하여 정보조회를 하며, 만일 그에 거부하는 경우 계약의 체결을 거부하는 방식으로 이 법률의 규제대상에서 벗어날 수도 있을 것이다. 그러나 이 경우에도 아직 미성년자가 대부분을 차지하고 있는 가입희망자가 이 개인정보조회의 의미를 제대로 이해할 것인가(또는 부가통신사업자가 그 의미를 제대로 알려줄 것인가)가 의심스러운 상황에서 단순한 동의의 의사표시만으로 모든 것을 해결하고자 하는 태도는 바람직하지 않다. 특히 위의 안에 의하면 주민등록번호와 성명, 그리고 주소 및 신용에 관한 정보를 이들 데이터뱅크의 연결을 통하여 수집 분석해 내는 것으로 되어 있는 바, 그중에서도 아직까지 개인의 접근이 곤란한 신용정보로써 가입여부를 판단하는 것은 지나친 통제라는 염려를 벗어나기 어렵다.

둘째, 그러나 이 보다 더 심각한 문제는 정보통신에 있어 익명성을 바탕으로 전개되는 자유공간의 창출이라는 그 본질적 특성이 심각하게 저해될 가능성이 있다는 것이다. 가상공간으로서의 정보공간은 현실적인 생활속의 대면적 관계에서 요구되는 것과 같은 성별이나 지위, 사회적 신분, 신체적 정신적 정체를 드러낼 필요가 없다. 오히려 그 사이버공간에서 주어지는 상황에 따라 끝없는 자기분열을 반복하면서 무수한 자아들을 창출 조정하는 것이 보다 일반적이다. 그래서 법외적으로, 특히 사회심리적으로 주어지는 각종의 공식적 비공식적 강제를 의식함이 없이, 자신의 감성과 사고와 판단을 자유롭게 제시할 수 있으며 이를 바탕으로 무한히 자유로운 의사소통공간을 열어간다. 물론 이러한 자유공간이 사회의 신뢰성구축을 바탕으로 하는 사회질서의 안정화에는 부정적인 영향을 미칠 수도 있지만(권기현, 제5장), 이러한 역기능성으로써 언제나 끊임없이 창조되는 자아의 모습을 기초로 새로운 연대의 장을 열어갈 수 있는 기회를 마련하고 있다는 점에서 그 순기능적 측면을 부정할 수는 없다.

하지만, 위의 안은 이 사이버공간의 입구라 할 정보통신서비스에의 가입과정에서 실명을 요구함으로써 언제든지, 그리고 누군가에 의하여 자신의 현실적 정체가 드러날 수도 있다는, 그럼으로써 익명성의 전제 자체가 흔들릴 수도 있다는 사전적 자기통제의 기체에 억압받게 만든다. 청부미를 먹고사는 촌놈들의 좋은세상 만들기<sup>38)</sup>라는 홈 페이지를 만든 공무원들이 익명으로 말할 수 있는 자유’를 이용하여 최근 구조조정에 따른 인원감축이나 열악한 근무조건 등 공무원사회의 불만을 다양하고도 자유롭게 내뿜어내었던 것이, 행정자치부 홈페이지의 대화방 열린 마당’이 실명화되면서 억제되기 시작한 것<sup>39)</sup>은 이의 좋은 예이다.

셋째, 그 실효성이 완벽하지 않아 오히려 정보불평등을 야기할 가능성이 있다. 실명가입을 강제한다는 것이 이 안의 골자이지만, 정보통신서비스에의 가입행위가 대부분이 온라인 상에서 이뤄지기 때문에 주민등록번호와 성명만 알면 실제 가입자가 그 성명의 인격인지와 관계없이 가입절차가 완료되기 때문에 사실상의 실명확인 은 불가능하다는 것이다.<sup>40)</sup> 그러나

38) <http://www.geocities.com/CapitolHill/Parliament/2476/>

39) 문화일보, 1999.6.19. “언로(言路)의 자유를 찾아 사이버 망명을 떠납니다.”

문제는 여기에 그치는 것이 아니라, 이 안이 예정하고 있고 그 적용의 대상이 되는 부가통신사업자를 통하지 않고서도 무수한 정보통신의 기회-각종의 연구망, 교육망등이 대표적이다-가 제공되고 있다는 점에서 더욱 그러하다. 특히 요즘 한창 성업중인 인터넷 카페라든가 PC게임방과 같은 비정규의 시설을 이용할 때에는 굳이 이러한 통신실명확인 절차를 거치지 않고서도 얼마든지 사이버공간에 접근할 수 있고, 따라서 이 안에 예정하고 있는 정보통신의 건전화는 무위로 돌아갈 수가 있는 것이다.

그리고 바로 이 점에 의하여 정보불평등현상이 발생하게 된다. 먼저, 신용불량 또는 실명확인을 거부하는 사람에게는 부가통신사업자가 제공하는 역무에의 접근이 불가능한 반면, 실명확인이 가능한 자와 그것을 허위로 할 수 있는 자는 그러한 역무를 이용할 수 있게 되는 문제가 나타난다. 뿐만 아니라, 더욱 문제로 되는 것은 익명성의 위협을 받는 신랄한 정보통신이용자와 그렇지 않는 '악의의' 정보통신이용자간의 접근능력에 있어서의 차별을 야기할 가능성이 나타난다는 점이다.

넷째, 이 부분에서 이 안이 예정하고 있는 본래의 목적-정보통신의 감시-의 효율성이 저감될 수 있는 여지가 대두된다. 이 안은 실명제를 도입함으로써 정보통신의 흐름을 국가적 감시의 틀내에 편입하고 이로써 정보통신의 건전성을 도모하고자 하는 것이나, '악의의' 정보통신이용자들이 기존의 부가통신사업자의 시설을 이용하기를 포기하고 그외의 정보통신시설에 접근하게 함으로써 오히려 그나마 부가통신사업자에 의하여 이루어지던 정보통신의 통제장치까지도 상실하게 될 우려가 있다는 것이다. 요컨대, 부가통신사업자의 자율규제에 의하여 이루어지던 게시판이나 자료실에 대한 사적 검열장치마저도 제대로 작동되지 않을 가능성이 발생할 우려가 농후하다는 것이다.

결국, 통신실명제는 표현의 자유를 희생하는 위에서 단순히 부가통신사업자의 경영개선만을 도모하는 편향된 효과만 거둘 수 있을 뿐이며, 오히려 극단적으로 보자면, 그것은 사이버공간의 자유로운 의사소통이라는 매력 자체를 약화시키는 역효과만 야기할 수도 있다.

#### 참고문헌

- 권기현(1997), 정보사회의 논리, 나남출판
- 백윤철 이기욱(2000), 사이버공간과 법률에 관한 제문제, 윤명선 외편, 사이버헌법론, 조세통람사 정보통신부 보도자료(1998.12.04) <http://www.mic.go.kr/BroadDir/보도자료/온라인서비스.htm>
- 정완(2001), 주민등록번호 생성프로그램과 ID실명제, "현사정책연구소식 제63호, 2001, 1/2월호
- 정진수외(2000), 신종성폭력-사이버성폭력의 실태와 대책을 중심으로, 한국형사정책연구원
- 황상민, 한규석 편(1999), 사이버공간의 심리-인간적 정보화 사회를 향해서, 박영사
- 이광형(2001), "정보화시대의 새로운 수사기법" in:[http://icic.sppo.go.kr/database\\_case/innerdata-12.htm](http://icic.sppo.go.kr/database_case/innerdata-12.htm)
- Al Teich, M. S. Frankel, R. Kling, and Ya-ching Lee(1999), "Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference," The Information Society, vol.15, No.2.
- Barbrook, R. and A. Cameron, THE CALIFORNIAN IDEOLOGY, in:<http://media.wmin.ac.uk/HRC/ci/calif5.html>
- Beck, Ulrich(1998), 정치의 재발견, 거름
- Branscomb, A.(1995), "Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces," Yale Law Journal, vol.104.

40) 예컨대, <http://mail.datanet.co.kr/tele/9901/end10.html>

- Ely, J. H.(1980), Democracy and Distrust: A Theory of Judicial Review(Cambridge: Harvard University Press)
- Fiss, O. M.(1993), The Irony of Free Speech: Liberalism Devided(New York: Free Press)
- Froomkin, A. M.(1995), "Anonymity and Its Enmities," The Journal of Online Law, 1995. art.4 in:  
<http://www.wm.edu/law.publications.jol/froomkin.html>
- Giddens, Anthony.(1991), 이윤희등 역, 포스트모더니티, 민영사
- Johnson, D. G. and K. Miller(1998), "Anonymity, Pseudonymity, or Inescapable Identity on the Net," Computers and Society, June 1998
- Rose, L.(1995), NetLaw: Your Rights in the Online World(New York: McGraw-Hill)
- Sunstein, C.(1993), The Partial Constitution(Cambridge: Harvard University Press)
- Sunstein, C.(1996), "Constitutional Caution," 1996 University of Chicago Legal Forum
- Wallace, J. D.(1999), "Nameless in Cyberspace Anonymity on the Internet," CATO Institute Briefing Papers, No.54.
- Wallace, J., & M. Mangan(1997), Sex, Laws, and Cyber Space(New York: Henry Holt and Co., Inc)