

인터넷과 표현의 자유 규제 - 익명성 규제와 전파성 규제를 중심으로

Internet and Free Speech Regulation - Focusing on Anonymity Regulation and Expedited Intervention

박경신 고려대학교 법학전문대학원

Kyung Sin Park, Korea University Law School

역사는 승자가 쓴다.

패자는 무엇을 쓰는가?

위의 질문에 대한 답은 한 트위터러에 따르면 대한민국에서는 “트윗(Twit)”이다. 이 말은 한국 네티즌들이 처한 상황을 간명하게 잘 표현하고 있다. 한국의 제도권미디어 즉 방송과 신문이 각각 ‘승자’들에 의해 장악되고 있는 것과 더불어 인터넷 역시 세계에서 유례를 찾아볼 수 없는 어려운 중첩적 규제의 대상이 되면서 ‘패자’들은 그러한 규제의 올가미를 벗어나기 위한 출구로 페이스북과 트위터와 같은 외국서비스로 눈을 돌리고 있다. 이 글에서는 우리나라의 표현의 자유를 제약하는 인터넷규제들을 살펴보고 그러한 규제들의 원인과 해법을 살펴보기로 한다.

우선 이 글에서는 제1장에서 인터넷규제담론의 전제로서 인터넷에서의 소통(이하 “인터넷소통”)의 특성을 살펴보고 이 특성에 대응하여 우리나라에서 전개된 규제의 양상을 살펴본다. 특히 우리나라에서만 전개된 담론의 흐름인 “과잉불법성”론을 해체한다. 제2장에서는 대표적인 인터넷규제담론인 익명성에 대한 대표적인 규제인 본인확인제를 살펴본다. 제3장에서는 또 하나의 인터넷규제담론인 전파성 담론과 이에 대응하는 규제인 방송통신심의위원회의 심의제도의 한 측면인 ‘제3자규제’에 대해 살펴본다.

인터넷의 마지막 특성인 상호성에 부합하는 규제담론을 구성하고 이에 따른 페이스북과 트위터 규제론을 펼쳐보고자 하나 지면관계상 이는 다른 논문으로 미룬다.

I. 규제의 지평

1. 인터넷 소통의 특성과 규제근거

인터넷에서의 소통(“인터넷소통”)의 고유한 특성에 대응하는 것을 목표로 하는 각종 인터넷 규제들이 시행되고 있다. 여기서 우선 인터넷소통의 고유한 특성을 살펴보기로 한다. 물론 논자들에 따라 이 특성들을 다양하게 개념화하지만 여기서는 가장 기초적인 성질들만을 살펴보기로 한다. 예를 들어, 부유(浮游)성, 영구성 등은 아래에서 언급할 전파성과 익명성이 복합적으로 작용한 귀결이다.¹⁾ 또 특성들을 여러 차원으로 나누어볼 수 있겠지만 주로 규제생성과

1) 김용철, 「정보화시대의 사회운동: 온라인 사회운동의 유형과 특징」, 『사이버커뮤니케이션학보』, 통권 제25호 제1호, 2008, 13쪽; 황지연, 「사이버공동체의 정체성과 집합행동」, 『정보와 사회』, 통권 제6호, 2004, 110쪽에서 재인용; 김성태/이영환, 「인터넷을 통한 새로운 의제 설정 모델의 적용」, 『한국언론정보』, 제50권 3호, 2006, 200쪽.

연관된 차원에서 나누어 보겠다.

첫째, 익명성이다. 인터넷의 기반인 TCP-IP체제에서는 물리적인 접속을 연결해주는 매개자와 그 접속으로 생성된 공간 위에서 콘텐츠를 전달하는 즉 우편배달부 역할을 하는 매개자는 항상 분리되어 있다. 이를테면, 브로드밴드업자나 케이블텔레비전 업자가 물리적 접속을 제공하지만, 실제 인터넷을 통한 소통을 할 때는 Naver의 블로그서비스에 블로그의 내용을 위탁하고 구글의 검색서비스에 검색어를 입력하며 Daum커뮤니케이션의 메일서비스에 메일 내용을 위탁한다. 물론 물리적 접속을 얻기 위해서는 배선공사를 위해 자신의 주소를 브로드밴드업자에게 전화 또는 대면소통을 통해 알려줄 수 밖에 없지만, 그 시점 이후에 통신자의 신원이 드러날 수 있는 소통은 원칙적으로 이루어지지 않는다. 결국 브로드밴드업자가 Naver, Daum, 구글에 특정 고정IP에 브로드밴드를 설치한 사람을 통보해주지 않는 한 포털들은 모든 정보를 익명으로 수령하여 처리할 수 밖에 없다. 뿐만 아니라 요즘처럼 거의 모든 브로드밴드가 유동IP기반(물리적 접속지점에 배당되는 주소를 고정시키는 것이 아니라 그때그때 활용가능한 주소를 배당하는 방식)으로 운영되는 상황에서는 인터넷상의 콘텐츠는 그야말로 해당 콘텐츠를 만든 사람과 보는 사람과의 연결이 단절된 상태에서 유통되고 있다고 보아야 한다.

익명성은 규제생성의 강력한 근거가 된다. 사람이 인터넷을 통해서 불법을 저지른 후에 책임을 지울 수 없다는 것은 규제자 입장에서는 용납하기 어려운 것이기 때문이다.

둘째, 전파성이다. 전파성은 동시다발(전파)성, 신속(전파)성 등 여러 측면으로 분류할 수 있겠지만 규제를 추동한다는 측면에서 중요한 것은 인터넷 게시물은 게시되는 순간부터 누구나 TCP-IP의 통일된 규칙만 따른다면 동시에 접근 가능하다는 것이다. TCP-IP체제는 누군가에 의해 조직되고 관리되는 체제가 아니다. 하나의 구심점이 없이 전세계의 모든 단말들이 서로 연결되어 있고 이들 단말들이 서로 간에 정보를 주고 받을 수 있도록 통일된 규칙을 따르고 있는 상태일 뿐이다. 방송이나 전화처럼 정보가 전달되는 방향이나 범위가 정해져 있지 않고 모든 단말들이 규칙만 따른다면 평등하게 대우받기 때문에 모든 게시물은 그 게시물이 게시된 IP주소를 아는 사람에게는 모두 공개되는 것이다. 또 게시물의 IP를 모른다고 하더라도 검색엔진을 통해 해당 게시물을 찾아갈 수 있다. 특히 단말이 모두 평등하기 때문에 모두가 콘텐츠를 생산하기도 하고 모두가 콘텐츠를 소비하게 되는데 이는 전파성을 배가하는 요소이다. 즉 특정 콘텐츠를 본 사람은 그 콘텐츠를 재게시함으로써 더 많은 사람들이 볼 수 있도록 할 수 있어 전파력은 기하급수적으로 늘어나게 된다.

전파성 역시 규제생성의 강력한 근거가 된다. 하나의 불법적인 콘텐츠라고 할지라도 모두가 한꺼번에 볼 수 있고 또 모두가 이를 재게시함으로써 더 많은 사람들이 볼 확률을 높일 수 있는데 이렇게 불법적인 콘텐츠의 빠른 확산은 새로운 규제를 긴절히 요청하게 된다.

셋째, 상호성이다. 인터넷을 통한 소통은 상호적이다. 물론 모든 소통은 궁극적으로는 상호적이다. 의사전달이 이루어지기 위해서는 콘텐츠를 송신한 사람과 콘텐츠를 수신한 사람이 필요하다. 그러나 콘텐츠의 수신은 송신에 비해 항상 수동적인 역할을 하는 재래식 소통방식과 달리 인터넷소통에서는 수신은 매우 적극적인 행위가 된다. 인터넷을 통하지 않는 신문, TV, 라디오를 켜 때 무엇이 나올지 알고 그렇게 하는 경우는 드물다. 보통은 미디어에 접속하면 미디어생산을 주로 하는 자들이 제공하는 것이 '보이고 들리면서' 소통이 이루어진다. 그러나 인터넷소통은 그렇지 않다. 대부분 인터넷미디어에 접속하면 '메인'이라고 부르는 콘텐츠의 집결지가 있고 여기에서 글의 제목을 보고 연결된 하이퍼링크를 누르는 적극적인 방식으로 자신이 소비할 콘텐츠를 선정하게 된다. 이러한 상호성은 SNS에서 더욱 강력해진다. 즉 이용자는

자신이 관리하는 공간만을 접속할 뿐이며 거기에서 보는 것은 자신이 미리 선택한 자들이 생산한 콘텐츠들이다. 즉 ‘보이거나 들리는 것’은 없고 자신이 적극적으로 보고 듣겠다고 작성한 것들만 보고 듣게 된다.

상호성은 규제생성의 강력한 근거가 아니라 도리어 규제를 완화해야 할 단서를 제공한다. 왜냐하면 소통에 대한 규제 대부분은 송신한 사람에게 법적 책임을 부과하는데 인터넷은 수신한 사람의 능동적인 반응이 있을 때만 소통이 완성되기 때문에 소통의 유해성에 대한 책임을 송신자에게 모두 물을 수 없기 때문이다.

2. 규제의 양태

가. 본인확인제 (identity verification regulation)

우리나라의 대표적인 인터넷규제군은 TCP-IP체제가 전제로 하고 있는 익명성을 제한하는 규제들로서 “실명제”, “본인확인제” 등의 이름으로 불리운다.²⁾ 익명성을 제한하려는 목적은 인터넷을 통해 이루어지는 유해한 소통의 당사자들을 추적할 수 있게 되면 그 소통을 차단하거나 위화시킬 수 있다는 논리이다. 우선 인터넷소통을 통해 불법행위를 하려는 자의 경우 자신이 추적되고 법적 책임이 부과될 수 있다면 당연히 그러한 행위로부터 위화될 것이다. 또 미성년자의 경우 자신들이 접근하려는 콘텐츠 자체에 법적 제한이 있고 청소년유해매체물에 접속하는 것은 그 자체로 유해한 소통이 된다. 이때 접속자의 신원 및 연령을 확인할 수 있다면 그러한 미성년자와의 유해한 소통을 차단하거나 제어할 수 있다는 논리이다.

나. 행정심의를 통한 내용규제 (administrative content regulation)

또 하나의 인터넷규제군은 전파성에 초점을 맞춘 규제이다. ‘법원판결이 날 때까지 기다릴 수 없다’는 긴절함을 통념화시키면서 행정기관이 신속하게 개입하여 인터넷 상의 게시물을 삭제 및 차단하는 규제들로서 방송통신심의위원회와 방송통신위원회에 의해 집행된다.³⁾

다. 매개자규제 (intermediary regulation)

마지막으로 익명성과 전파성에 대한 중첩적인 대응은 임시조치제도⁴⁾나 방송통신심의위원회가 정보통신서비스제공자에게 내리는 시정요구제도⁵⁾와 같이 소통의 당사자가 아니라 소통의 매개자를 ‘동원’하는 방식으로 나타났다. 이는 인터넷에서는 소통의 당사자가 본질적으로는 익명으로 남아 있어 소통의 당사자에 대해 규제책을 행사하기가 어렵고 소통의 당사자와 연락이 가능하다고 할지라도 유해한 소통의 전파성이 너무 강하기 때문에 어쩔 수 없이 신원이 이미 확인되어 있는 소통의 매개자들인 포털이나 이동통신사에 대하여 규제책을 행사할 수밖에 없다는 논리이다.

2) 정보통신망이용촉진 및 정보보호에 관한 법 제44조의5, 청소년보호법 제16조, 게임산업진흥에 관한 법률 제12조의3 제1항 제1호, 공직선거법 제82조의6

3) 방송통신위원회 설치법 제21조, 정보통신망이용촉진 및 정보보호에 관한 법 제44조의7

4) 정보통신망이용촉진 및 정보보호에 관한 법 제44조의2

5) 방송통신위원회 설치법 제21조 제4호

3. 우리나라 규제담론의 특성: “과잉불법성”

위에서 언급한 본인확인제, 임시조치제도, 방송통신심의위원회 등의 제도들은 모두 세계적으로 유례가 거의 없는 것들이다. 익명성, 전파성 등은 다른 나라의 인터넷규제담론에서도 똑같은 영향력을 행사하겠지만 특히 우리나라에서 특별히 힘을 얻는 이유는 아마도 필자가 ‘대한민국 예외론’이라고 명명한 사회인식 때문일 것이다. 즉 ‘대한민국 네티즌들은 의사표현에 적극적이어서 훨씬 더 많은 불법정보를 인터넷에 올린다’는 것이다. 실제 2000년대 초반의 보고서들은 대부분 인터넷 전체 정보의 10-15%를 불법정보로 규정하고 있을 것이다.⁶⁾

그러나, 이것은 무엇이 불법인지 마저도 기존 형법 등이 규정한다는 것을 간과한 상황판단이다. 우리나라는 전세계에 흔치 않게 모욕죄와 진실적시명예훼손죄를 활발히 집행하고 있으며 특히 명예훼손 형사처벌의 비율이 다른 나라들에 비해 월등히 높을 뿐 아니라 전세계에서 유일한 위력업무방해죄를 통해 인터넷을 통해 조직되는 집단적 의제설정을 범죄시하는 것이 매우 용이하다. 최근까지는 특정할 수 있는 피해를 발생시키지 않는 경우에도 표현의 내용이 허위라는 이유만으로 처벌하는 허위사실유포죄까지 있었다. 여기서 열거된 모든 죄들은 UN인권위원회, UN인권이사회 산하 표현의자유 특별보고관 등 기타 국제인권기구가 천명한 국제인권기준을 위배한다.⁷⁾ 국제인권기준과 현재 형사처벌 조항들과의 관계는 아래 표에 제시된 바 있다.

표현 전체				
사실적 주장			의견의 표명	
허위 주장		진실주장	행위의 권유	의견의 단순표명
피해특정가 능	피해 특정 불 가			
우리나라의 경우				
형법 307조 2항로 처 벌!	전기통신기 본법 47조1 항로 처벌! (2010.12.2 8. 위헌판 정)	형법307조1항로 처벌!	형법 314조로 처벌!	형법311조로 처 벌!
국제인권기준				
민사책임	처벌없음	처벌없음	처벌없음	처벌없음

6) 김경년, 김재영, “오마이뉴스의 독자의견분석”, 한국방송학보 19-3; 배영 외 3인, “2008년도 본인확인제 효과분석”.

7) 이에 대한 자세한 논의는 박경신, <표현 통신의 자유>, 논형 (2013) 및 박경신의 다음 논문들: “진실적시에 의한 명예훼손 처벌제도의 위헌성”, 『세계헌법연구』 제16권 제4호(2010. 12), 1-29면; “허위 사실유포죄의 위헌성에 대한 비교법적 분석”, 『법학연구(인하대학교)』 제12권 제1호, 1-44면; 공저 김가연, “모욕죄의 보호법익 및 법원의 현행 적용방식에 대한 헌법적 평가”, 『언론과 법』 제10권 제2호(2011. 12), 441-467면; “모욕죄의 위헌성과 친고죄 조항의 폐지에 대한 정책적 고찰”, 『고려법학』 제52권 (2009. 04), 263-299면; 공저 손익찬, “위력에 의한 업무방해죄의 위헌성 - 노동쟁의행위와 소비자보호운동을 중심으로”, 『공익과 인권』 제9호 (2012.1); “명예의 보호와 형사처벌제도의 폐지론과 유지론”, 『서강법학』 (2009.06)제11권 제1호, 357-380면.

이렇게 기존의 형법 등의 체계가 상당히 많은 표현의 범주들을 범죄시해왔기 때문에 우리나라 사람들이 자주 이용하는 포털 등에 불법정보가 많은 것으로 보이는 것이다. 국제인권기준을 적용하자면 기존의 형법 등에 문제가 많이 있다. 단순히 현행 법을 기준으로 불법정보의 비율을 판단하여 우리나라 네티즌들이 특별히 더 공격적이라거나 해로운 언사를 많이 한다고 평가하여 이 평가에 따라 규제를 구성하는 것은 설부르다.

II. 익명성 규제

1. 게시판실명제 위헌결정

우리나라 익명성규제는 2012년도에 규제에 대한 평가의 틀이 확립되는 큰 변화가 있었는데 바로 헌법재판소의 결정이다.⁸⁾ 헌법재판소는 1일 평균 방문자 10만명 이상의 웹사이트 운영자는 그 사이트의 일반적으로 공개된 장소(소위 “게시판”)에 글을 쓰는 모든 사람들로부터 그 사람의 본인확인정보를 수집할 것을 요구하고 있던 정보통신망이용촉진및정보보호에관한법률 제44조의5의 위헌성을 심사하였다. 당시 헌법소원은 본인확인정보를 수집하고 보관해야 하는 의무를 가진 웹사이트 운영자와 본인확인정보를 제출하지 않고는 글을 올릴 수 없는 이용자 입장에서 모두 제기되었는데 현재 결정은 주로 이용자의 입장에 치중하였다.

(1) 우선 헌법재판소는 익명표현의 자유의 중요성에 대해 다음과 같이 판시하였다.

“인터넷공간에서 이루어지는 익명표현은 인터넷이 가지는 정보전달의 신속성 및 상호성과 결합하여 현실 공간에서의 경제력이나 권력에 의한 위계구조를 극복하여 계층, 지위, 나이, 성 등으로부터 자유로운 여론을 형성함으로써 다양한 계층의 국민 의사를 평등하게 반영하여 민주주의가 더욱 발전되게 한다. 따라서 비록 인터넷 공간에서의 익명표현이 부작용을 초래할 우려가 있다 하더라도 그것이 갖는 헌법적 가치에 비추어 강하게 보호되어야 한다. (밀줄 필자 강조)

위에서 “부작용을 초래할 우려가 있더라도”와 같은 표현은 우리나라의 친규제적 사법부에서 많이 보지 못했던 과감한 표현으로서 익명표현의 자유의 정치적 중요성에 대한 강한 긍정이다.

(2) 헌법재판소는 게시판실명제는 글을 쓰려는 사람에게 반드시 사전에 신원을 밝힐 것을 요구하므로 “표현의 자유를 사전에 제한한다”고 지적하며 “표현의 자유는 민주주의 근간이 되는 중요한 헌법적 가치이므로 표현의 자유의 사전 제한을 정당화하기 위해서는 그 제한으로 인하여 달성하려는 공익의 효과가 명백하여야 한다(밀줄 필자 강조)”고 하여 합헌 여부를 엄격하게 심사할 것을 천명하였다.

(3) 헌법재판소는 이렇게 심사기준의 수위를 확립한 후 실명제의 공익의 효과가 명백한지를 살핀다. 실명제가 목표했던 공익은 위에서 말했듯이 불법정보의 위화이다. 그러나 “방송통신위원회가 제시한 자료⁹⁾에 의하더라도 본인확인제 이후에 명예훼손, 모욕, 비방의 정보의 게시가 표현의 자유의 사전제한을 정당화할 정도로 의미있게 감소하였다는 증거는 찾아볼 수 없

8) 헌법재판소 2010 헌마 47 (병합) (2012)

9) 권헌영 외 6인, “인터넷게시판 정책현황 분석 및 실효성 확보방안”, 한국인터넷진흥원 발주 한국전자정부 수탁 연구용역 보고서, 2009. 12., 26쪽.

다.”

뿐만 아니라 헌법재판소는 실명제로 달성하려는 공익이 명백하지 못함을 다음과 같은 놀라운 문단으로 설시한다.

우리 법상의 규제가 규범적으로 현실적으로 적용되지 아니하는 통신망이 존재하고 그에 대한 인터넷 이용자의 자유로운 접근이 가능함에도. . . 본인확인제를 규정함으로써 국내 인터넷 이용자들의 해외사이트로의 도피, 국내 사업자와 해외 사업자 사이의 차별 내지 자의적 법집행의 시비로 인한 집행 곤란의 문제를 발생시키고 있는 바. . . 인터넷은 전세계를 망라하는 거대한 컴퓨터 통신망의 집합체로서 개방성을 그 주요한 특징으로 하므로 외국의 보편적 규제와 동떨어진 우리 법상의 규제는 손쉽게 회피될 수 있고, 그 결과 우리 법상의 규제가 의도하는 공익의 달성은 단지 허울좋은 명분에 그치게 될 수 있음을 간과한 것(밀줄 필자 강조)"

“우리 법상의 규제가 규범적으로 현실적으로 적용되지 아니 하는 통신망”은 바로 외국정보통신서비스 제공자를 말하는 것이다. 즉 국내포털을 아무리 규제해도 똑같은 소통을 해외포털을 통해 할 수 있으니 규제가 현실적으로 무의미하다는 것이다. 법적용이 현실 상 어려운 경우 그 난점을 보상하기 위해 항상 더 강한 규제를 만드려는 것이 보통 규제당국의 습성이고, 우리나라 사법부는 그런 습성에 제재를 거는 과감함을 잘 보여주지 않았는데 이번에는 “현실을 인정하자”는 목소리가 들린다.

위 문단을 짧게 요약하자면 ‘세계성있는 인터넷에 갈라파고스 규제를 적용하려는 것은 부작용만 있을 뿐 성취하는 공익은 없다’는 것이다. “외국의 보편적인 규제와 동떨어진 우리 법상의 규제”는 바로 갈라파고스규제를 풀어 쓴 것이다. 바로 게시판실명제를 중국의 웨이보 등이 채택하기 전까지¹⁰⁾ 전세계에서 유일하게 우리나라만 있는 제도임을 지적한 것이다.

(4) 반면 실명제에 의해 국민에게 끼치는 기본권침해의 정도는 심대하다.

본인확인이라는 방법으로 게시판 이용자의 표현의 자유를 사전에 제한하여 의사표현 자체를 위축시키고 그 결과 헌법으로 보호되는 표현까지도 억제함으로써 민주주의의 근간을 이루는 자유로운 여론 형성을 방해한다.

. . .

이 사건 본인확인제는. . . 표현의 내용을 불문하고 주요 인터넷 사이트의 대부분의 게시판 이용과 관련하여 본인확인을 요구하고 있다. 이는 정보 등을 게시하고자 하는 자가 무엇이 금지되는 표현인지 확신하기 어려운 상태에서 본인의 이름, 주민등록번호 등의 노출에 따른 규제나 처벌 등 불이익을 염려하여 표현 자체를 포기하게 만들 가능성이 높고, 인터넷을 악용하는 소수의 사람들이 존재하고 있다는 이유로 대다수 시민의 정당한 의사표현을 제한하는 것으로서 익명표현의 자유에 대한 과도한 제한이라 할 것이다. . . (밀줄 필자 강조)

(5) 침해당하는 기본권은 표현의 자유 만이 있는 것이 아니라 프라이버시도 있다.

본인확인제는. . . 모든 게시판 이용자의 본인확인정보를 수집하여 장기간 보관하도록

10) <http://journal.kiso.or.kr/?p=501> <2013년11월30일 방문>

함으로써 개인정보가 유출될 위험에 놓이게 하고 다른 목적에 활용될 수 있도록 하며, 수사편의 등에 치우쳐 모든 국민을 잠재적 범죄자와 같이 취급하는 바. . .

본인확인정보 보관의무 부과로 인하여. . . 수사기관 등이 정보통신서비스제공자에게 이용자의 개인정보 제출을 요청(전기통신사업법 제83조 제3항)하는 경우 발생할 수 있는 본인확인정보의 보관목적외 사용 우려에 비추어 보면, 개인정보자기결정권의 제한 역시 중대함을 부인할 수 없다.(밀줄 필자 강조)

2010년 1월 소제기 전후로 지난 5년간 대형개인정보유출사태가 여럿 발생했다.¹¹⁾ 현재도 이 개인정보유출의 위험을 그다지 길지 않은 결정문에서 2회나 언급한 것으로 보아 영향을 받았을 것으로 추측된다.

정리하자면, 게시판실명제 위헌결정의 기본구조는 다음과 같다. (1) 익명표현의 자유는 민주주의를 위해 매우 중요한 기본권이고 (2) 이 기본권에 대한 사전제한은 공익적 효과가 명백해야 하는데 (3) 이 제도는 명의도용의 가능성 및 외국서버를 통한 소통가능성때문에 ‘불법정보 위화’라는 공익적 효과가 명백하지 않고 (4) 소수의 불법정보의 게시자를 적발하기 위해 표현의 내용을 불문하고 모든 국민에게 본인확인 의무를 부과하는 것은 표현의 자유를 과도하게 침해하는 것이며 (5) 본인확인을 위해 개인정보가 보관 및 유통되기 때문에 이용자들의 사생활의 비밀을 침해한다는 것이다.

2. 현행 본인확인제들에 대한 평가

가. 청소년보호법 본인확인제

우리나라는 청소년보호를 목적으로 청소년보호법 하에 술, 담배 등을 청소년유해물로 지정하고 이를 청소년에 판매하는 것을 형사처벌하고 있다.¹²⁾ 이와 함께 청소년유해매체물로 지정

11) 한윤형 발표문, “개인정보보호의 이해 및 안전한 관리 - 개인정보의 의의 및 처리 실태” (2012.11.21.) 정보화진흥원.

2008.2 옥션 1,800만 명 (해킹); 2008.4 하나로 텔레콤 600만 명 (자사 고객 개인정보를 텔레마케팅업체에 제공), 2008.9 GS 칼텍스 1,150만 명 (자회사 직원이 유출); 2010.3 신세계몰 등 25개 업체 2,000만 건 (해킹); 2011.4 현대캐피탈 175만 건 (해킹 및 내부 관리 소홀); 2011.5 리딩투자증권 12,000건 (홈페이지 해킹); 2011.5 세티즌 140만 명 (홈페이지 해킹); 2011.6 대부업체, 저축은행, 채팅사이트 등 1,900만 건 (해커가 여러 사이트의 고객정보 유출 후 인터넷에서 거래); 2011.7 SK컴즈(네이트, 싸이월드) 3,560만 명 (해커가 관리자 ID/비밀번호를 탈취); 2011.8 삼성카드 47만 건 (자사 직원이 유출); 2011.11 넥슨 1,320만 건 (해킹); 2012. 5 EBS 400만 건 (해킹); 2012.7 KT 870만 건 (해킹)

12) **제28조(청소년유해약물등의 판매·대여 등의 금지)** ① 누구든지 청소년을 대상으로 청소년유해약물등을 판매·대여·배포(자동기계장치·무인판매장치·통신장치를 통하여 판매·대여·배포하는 경우를 포함한다)하거나 무상으로 제공하여서는 아니 된다. 다만, 교육·실험 또는 치료를 위한 경우로서 대통령령으로 정하는 경우는 예외로 한다. ② 누구든지 청소년의 의뢰를 받아 청소년유해약물등을 구입하여 청소년에게 제공하여서는 아니 된다. ③ 청소년유해약물등을 판매·대여·배포하고자 하는 자는 그 살대방의 나이를 확인하여야 한다. **제59조(벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다. . . 6. 제28조제1항을 위반하여 청소년에게 제2조제4호가목

된 콘텐츠를 청소년에게 판매하는 것 역시 형사처벌하고 있다.¹³⁾ 청소년유해매체물 지정은 청소년보호위원회 또는 각 분야 심의기관(방송통신위원회, 간행물윤리위원회, 영상물등급위원회 등)이 할 수 있다.

나아가 청소년유해물에 대해서는 “상대방의 나이를 확인”할 의무를 부과하며 청소년유해매체물의 경우 “상대방의 나이 및 본인 여부를 확인”할 의무까지 부과된다. 술, 담배와 같은 청소년유해물의 경우 관련 법에 의해 판매처가 한정되어 있고 이들 판매처는 모두 대면 거래를 전제로 하고 있으므로 구매자의 신원까지 확인하지 않더라도 육안으로 확인되는 얼굴, 신체조건 만으로도 나이를 확인할 수 있으므로 ‘본인 여부’ 확인은 요구되지 않는다.

위의 게시판실명제위헌결정문에 비추어보자면 청소년보호법 본인확인제에 대해서는 다음과 같이 평가해볼 수 있다. 아래의 각 문단은 위의 게시판실명제위헌결정을 소개한 단원의 (1), (2), (3) 등에 대응한다.

첫째, 표현의 자유는 ‘알 권리’를 포함하거나 ‘알 권리’도 표현의 자유와 적어도 똑같은 수위로 보호되어야 한다. 정보에의 접근은 단지 그 정보가 표현의 내용이 되는 사유를 형성하는 근거가 되기 때문이 아니라 타인에게 아무런 해를 끼치지 않는 사적 행위이다. 표현의 자유도 똑같은 이유로 보호되는 만큼¹⁴⁾ ‘알 권리’도 보호되어야 한다. 청소년유해매체물이라고 할지라도 불법이 아니라 단지 청소년에게 보여지는 것이 부적합한 것이므로 성인이 이를 볼 권리는 표현의 자유에 내재된 ‘알 권리’의 일부로서 보호되어야 한다.

둘째, 자신의 신원정보를 19금물 제공자에게 제출하지 않고는 19금물에 접속할 수 없으니 ‘알 권리’를 포함하는 표현의 자유에 대한 사전제한이다. 사전 제한이므로 공익적 효과가 명백해야 한다.

셋째, 청소년들이 명의도용을 통해 접근할 수 있으므로 청소년접근제한 효과는 명백하지 않다. 2013년 초부터 휴대폰인증 즉 이용자가 19금물에 이용하고자 하는 시점에 소지하고 있는 휴대폰번호를 입력하여 인증하는 방식이 되어 명의도용이 어려워지기는 하였으나 국내사업자들의 콘텐츠보다 훨씬 더 유해한 콘텐츠를 외국서버를 통해 자유롭게 접근할 수 있다는 점에서 변함이 없다.

넷째, 규제가 접근제한을 가하려는 대상은 청소년이지만 성인들도 모두 일괄적으로 신원확인정보의 노출을 감수하도록 함으로써 19금물의 이용을 위축시킨다. 청소년을 제한하려고 하면서 “나이를 불문하고” 모든 이용자가 반드시 “명찰”을 달고 성인물을 이용할 것을 강제한다.

다섯째, 본인확인제는 본인확인정보의 저장을 전제로 기능한다. 검증받기 위해 19금물 접속

1) · 2)의 청소년유해약물(술, 담배 - 편집자 주)을 판매 · 대여 · 배포(자동기계장치 · 무인판매장치 · 통신장치를 통하여 판매 · 대여 · 배포한 경우를 포함한다)하거나 영리를 목적으로 무상 제공한 자

13) **제16조(판매 금지 등)** ① 청소년유해매체물로서 대통령령으로 정하는 매체물을 판매 · 대여 · 배포하거나 시청 · 관람 · 이용하도록 제공하려는 자는 그 상대방의 나이 및 본인 여부를 확인하여야 하고, 청소년에게 판매 · 대여 · 배포하거나 시청 · 관람 · 이용하도록 제공하여서는 아니 된다. **제58조(벌칙)** 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다. 1. 영리를 목적으로 제16조제1항을 위반하여 청소년에게 청소년유해매체물을 판매 · 대여 · 배포하거나 시청 · 관람 · 이용하도록 제공한 자

14) 박경신, “국제인권법상 표현의 자유 및 대한민국 법제의 평가”, 홍익법학 제13권 제3호 (2008. 10)

자 명단을 보유하고 있어야 할 것이다. 이 개인정보가 유출될 경우 사생활의 비밀이 노출되는 수많은 피해자가 발생할 수 있다.

위와 같이 청소년보호법 상 본인확인제는 위험판정을 받은 게시판실명제가 가지고 있는 문제들을 모두 노정하고 있다.

뿐만 아니라 청소년보호법 상 본인확인제는 다음과 같은 이유로 게시판실명제 보다 더 위험적이다. 첫째 자유권으로서의 '알 권리'는 표현의 자유에 앞선다. 급부권으로서의 '알 권리' 즉 정보공개청구권은 다양한 이유로 제한될 수 있지만, 자유권으로서의 '알 권리' 즉 합법적으로 공개된 정보에 대해 접근할 권리는 똑같은 정보를 유포할 권리보다 더 강하게 헌법적으로 보호된다. 명예훼손, 사기, 음화배포죄 등 다양한 형법조항들이 표현의 발화를 처벌할 뿐 해당 표현의 수령을 처벌하지는 않는 이유이다. 표현물의 수령을 처벌하는 조항들은 국가보안법의 이적표현물소지죄나 아동청소년성보호에 관한 법률의 아동청소년이용음란물 소지죄 뿐이며 이 경우에도 똑같은 표현물이나 음란물이라 할지라도 배포는 소지에 비해 훨씬 더 엄중하게 처벌된다. 이는 통신에 있어서 수신이 아니라 송신이 적극적인 행위라서 송신자에게 책임을 지우기 때문이다.

마지막으로 개인정보유출시 겪게 되는 프라이버시침해의 위험은 매우 강하다. 19금물의 경우 성적인 표현이 문제가 될터인데 개인이 어떤 성적 팬타지를 가지고 있는가는 사생활의 영역으로서 보호되어야 할 필요가 더욱 강하다.

결론적으로 청소년보호법 본인확인제는 위험일 가능성이 매우 높다.

나. 게임산업진흥법 본인확인제

게임산업진흥법은 온라인게임제공업자에게 모든 이용자에 대해 신원확인을 할 의무를 부과한다.¹⁵⁾ 온라인게임 실명제의 목표는 온라인게임을 하는 사람의 연령을 확인하여 미성년자들이 온라인게임을 하는 것을 부분적으로 제한하기 위함이다. 즉 이용자가 미성년자인 것이 확인되면 섯다운제도 및 법정대리인 동의를 통해 이용권리를 제한한다.¹⁶⁾

15) 게임산업진흥에관한법률 제12조의3(게임과몰입·중독 예방조치 등) ① 게임물 관련사업자[「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 정보통신망(이하 "정보통신망"이라 한다)을 통하여 공중이 게임물을 이용할 수 있도록 서비스하는 자에 한한다. 이하 이 조에서 같다]는 게임물 이용자의 게임과몰입과 중독을 예방하기 위하여 다음 각 호의 내용을 포함하여 과도한 게임물 이용 방지 조치(이하 "예방조치"라 한다)를 하여야 한다. 1. 게임물 이용자의 회원가입 시 실명·연령 확인 및 본인 인증 2. 청소년의 회원가입 시 친권자 등 법정대리인의 동의 확보

청소년보호법 상 본인확인제와는 달리 본인확인을 하지 않더라도 제재가 부과되지는 않는다. 법정대리인의 동의 미확보의 경우에도 사업자에 대한 제재는 없다.

16) 청소년보호법 제24조(인터넷게임 이용자의 친권자등의 동의) ① 「게임산업진흥에 관한 법률」에 따른 게임물 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호에 따른 정보통신망을 통하여 실시간으로 제공되는 게임물(이하 "인터넷게임"이라 한다)의 제공자(「전기통신사업법」 제22조에 따라 부가통신사업자로 신고한 자를 말하며, 같은 조 제1항 후단 및 제4항에 따라 신고한 것으로 보는 경우를 포함한다. 이하 같다)는 회원으로 가입하려는 사람이 16세 미만의 청소년일 경우에는 친권자등의 동의를 받아야 한다.

② 제1항의 친권자등의 동의에 필요한 사항은 「게임산업진흥에 관한 법률」에서 정하는 바에 따른다.

결과적으로는 청소년보호법 상 본인확인제와 비슷한 헌법적 실체를 가지게 된다. 첫째 온라인게임 역시 자기실현의 매개가 되는 합법적인 정보이므로 이 정보에 접근할 권리는 표현의 자유의 일부로서 보장된다. 둘째 온라인게임에 접근하기 위해서는 자신의 신원정보를 제공해야 하므로 정보접근권에 대한 사전제한이므로 그 공익적 효과가 명백해야 한다. 셋째 게임산업진흥법 상의 본인확인제 역시 기존의 본인확인 방식을 이용하기 때문에 그 실효성은 명백하지 않을 것으로 보이면 이는 실제 경험연구에 의해서도 입증된 바 있다.¹⁷⁾ 이를테면 온라인게임을 심야에 하는 학생들의 40%가 명의도용을 하였다고 한다. 넷째 이에 비해 미성년자의 온라인게임이용을 제한하기 위해 성인을 포함한 모든 사람들에게 본인확인을 요구하는 것은 과도한 침해가 되며 이들을 위축시킨다. 다섯째 본인확인 정보의 저장으로 인해 개인정보 유출의 위험이 높아진다.

게임산업진흥법 상의 본인확인제는 청소년보호법 상의 그것보다 더 위헌성이 심하다고 볼 수 있다. 왜냐하면 온라인게임이라고 해서 모두 청소년유해매체물이 아니기 때문에 온라인게임접근제한은 청소년보호라는 공익적 효과와의 인과관계가 없기 때문이다. 물론, 청소년보호법이 스스로 ‘인터넷게임’의 경우 16세 이하의 청소년은 친권자의 동의 하에서만 이용할 수 있도록 규정하고 있기는 하나 이러한 규정이 있다고 해서 온라인게임을 청소년유해매체물로 정의한 것이라고 볼 수는 없다. 청소년유해매체물과 청소년유해물은 친권자의 동의가 있다고 하더라도 청소년이 이용할 것이 허용되지 않기 때문이다.¹⁸⁾

더욱이 청소년의 접근을 완전히 제한하는 것이 아니라 단지 법정대리인의 동의를 얻도록 요구하거나 이용시간을 제한하는 정도의 효과를 위해 모든 온라인게임이용자에게 본인확인을 요구하는 것은 법익의 비례성 측면에서 부정적으로 평가될 수 밖에 없다.

다. 공직선거법 상의 본인확인제

공직선거법은 선거운동기간에 한하여 ‘정당·후보자에 대한 지지·반대’ 글을 쓸 때는 반드시 본인확인을 거치도록 의무화하고 있다.¹⁹⁾ 글을 쓰려면 본인확인을 해야 한다는 점에서 이미

친권자의 동의를 얻지 않더라도 사업자에 대한 제재는 없다. 친권자의 동의 요건 자체가 위헌성이 있다는 주장에 대해서는 황성기, “인터넷게임 이용을 위한 청소년의 회원가입시 부모의 필요적 사전동의제도의 헌법적 문제점”, 「공법학연구」 제12권 제1호, 한국비교공법학회, 2011. 2. 28.

17) 현군택외 3인, <청소년 인터넷게임 건전이용제도(강제적 셧다운) 실태조사 보고서>, 2012년 여성가족부 용역. 이 보고서에 따르면 600명을 조사한 결과 셧다운제 시행 이후 심야시간 게임이용 빈도수에 의미있는 변화는 없었으며 심야시간이용경험이 있는 학생은 9%(54명)였으며, 이 54명의 학생 중 ‘부모님의 게임이용동의하에 부모아이디로 접속함’이라고 응답한 학생은 59%수준이었고, 다른 40%의 학생들은 ‘허락없이 부모님 아이디를 개설하여 게임에 접속함’(27.8%), ‘가족외 타인 주민등록번호를 이용하여 게임에 접속함’(13%)이라고 답했음.

참고로 셧다운제가 게임이용시간을 의미있게 줄이지 못한다는 통계학적으로 세밀한 연구결과는 박문수, 고대영, 박정수, <게임시장의 규제가 산업생태계 발전에 미치는 영향과 시사점>, 산업연구원 (2013.12)

18) 친권자의 동의 하에 청소년 접근이 허용되는 것은 청소년보호법 제29조가 정하는 청소년유해업소 뿐이다.

19) 공직선거법 제82조의6(인터넷언론사 게시판·대화방 등의 실명확인) ① 인터넷언론사는 선거운동기간 중 당해 인터넷홈페이지의 게시판·대화방 등에 정당·후보자에 대한 지지·반대의 문자·음성·화상 또는

위헌판정을 받은 게시판실명제와 같지만 적용범위('정당·후보자에 대한 지지·반대')와 적용기간(2주 혹은 3주 동안의 공식선거운동기간)은 더 좁지만, 다른 한편으로는 게시판실명제가 하루 방문자 10만명 이상인 게시판에만 적용되었던 것에 비하여 적용범위가 더 넓은 면도 있다.

게시판실명제 위헌결정의 기본구조는 공직선거법 상 본인확인제에 대해서도 똑같이 적용될 수 있다. (1) 선거에 관한 익명표현의 자유는 민주주의의 형성에 매우 중요하며²⁰⁾ (특히 선거에서 중요한 진실의 발견을 위해서는 사상의 자유시장이 왕성하게 작동해야 하므로) (2) 그러한 기본권에 대한 사전제한으로서 공익적 효과가 명백해야 함에도 불구하고 (3) 명의도용의 가능성 및 외국서버를 통한 소통가능성때문에 불법정보 위화의 공익적 효과가 명백하지 않고 (4) 소수의 불법정보의 게시자를 적발하기 위해 모든 국민에게 본인확인 의무를 부과하는 것은 표현의 자유를 과도하게 침해하는 것이며 (5) 본인확인을 위해 보관 및 유통되는 개인정보가 이용자들의 사생활의 비밀을 침해한다는 것이다.

특히 2012년 12월 헌법재판소가 인터넷 상의 선거운동 및 정치적 표현에 대한 공직선거법 상의 규제를 위헌결정함으로써²¹⁾ 인터넷에 올라올 것으로 예상되는 선거법상 '불법정보'의 양을 대폭 줄여버렸다. 과거에 헌법재판소가 공직선거법상 실명제에 대해 합헌 결정²²⁾을 여러차례 내렸을 때의 불법정보는 두 가지 유형이었다. 하나는 사전선거운동금지 또는 선거전180일간 후보지지반대 금지 등의 기간제한위반형이고 다른 하나는 표현의 내용 자체가 허위이거나 비방인 불법내용형이었는데, 전자가 후자보다 압도적으로 많았다. 예를 들어 18대 국회의원선거에서 인터넷상 선거법위반행위에 대해 중앙선거관리위원회는 총 10,623건을 적발했는데 비방·흑색선전 5.6%(600건), 사전선거운동 89.2%(9,475건), 기타 5.2%(548건)이었다.²³⁾ 그렇다면 2012년12월 위헌결정 전에는 모든 후보지지반대글 또는 선거운동용 글이 기간제한을 위반하면 공직선거법 제93조와 제254조에 의거하여 불법이 될 우려가 있었고 이에 따라 많은 양의 불법정보를 위화해야 할 공익이 본인확인제도를 상대적으로 정당화할 수 있었다. 그러나, 2012년12월 위헌결정 후에는 이제 전체 선거법 상 불법정보의 5-10% 만을 차지하는 허위사실공표, 후보자비방글들만이 불법이 되므로 이런 소수의 글을 잡기 위해서 유권자다수에게 족쇄를 씌우는 것은 위헌 가능성이 더욱 높아지게 되었다.

더욱이 공직선거법 상 본인확인제는 태생적으로 과도할 수 밖에 없는데 왜냐하면 어느 글이 "정당 및 후보에 대한 반대 지지" 글이 될지 포털이 미리 예측을 할 수 없기 때문에 결국 선거운동기간에는 모든 글의 게시자들에 대해서 본인확인을 할 수 밖에 없게 된다. 결국 선거법 하나 때문에 선거와 무관한 모든 인터넷을 통한 소통에서 익명성이 추방되는 결과가 나올 수 밖에 없게 되는데 법익의 균형성 측면에서 심각한 문제가 아닐 수 없다.

동영상 등의 정보(이하 이 조에서 "정보등"이라 한다)를 게시할 수 있도록 하는 경우에는 안전행정부 장관 또는 「신용정보의 이용 및 보호에 관한 법률」 제2조제4호에 따른 신용정보업자(이하 이 조에서 "신용정보업자"라 한다)가 제공하는 실명인증방법으로 실명을 확인받도록 하는 기술적 조치를 하여야 한다. 다만, 인터넷언론사가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의5에 따른 본인확인조치를 한 경우에는 그 실명을 확인받도록 하는 기술적 조치를 한 것으로 본다. <개정 2008.2.29, 2010.1.25, 2013.3.23>

20) 사실 익명표현의 자유가 헌법상 보장되는 기본권임을 처음 확인한 것은 헌법재판소였다. 헌법재판소 2010.02.25. 선고 2009헌바31 등. 현재는 익명표현의 자유는 보장되지만 선거의 공정성을 위해 선거운동기간이라는 짧은 기간 동안에만 이를 제한하는 것은 합헌이라고 판시하였다.

21) 헌법재판소 2011.12.29. 2007헌마1001 공직선거법 제93조 제1항 등 위헌확인

22) 헌법재판소 2010.02.25. 선고 2009헌바31 등

23) 제 18대 국회의원선거총람.

라. 공통적인 문제

위에서 평가한 청소년보호법, 게임산업진흥법 및 공직선거법 상 본인확인제들은 규제자가 원치 않았던 범위로 익명성제한을 확산시킨다. 예를 들어 성인물 접속자가 과연 성인인지 확인하려는 시도는 접속자를 위축시키고 결국 접속자가 그러한 신원확인이 불필요한 대체콘텐츠를 찾도록 유도한다. 방문자를 다른 사이트로 빼앗기고 싶지 않은 운영자는 최대한 현저하지 않게 본인확인을 해야 할 필요를 느끼며 가장 현저하지 않게 본인확인을 할 수 있는 시점은 바로 보통 최초 계정 개설 시점이다. 해당 운영자의 서비스를 전혀 이용하지 않던 사람이 계정개설을 결정할 시점에는 해당 서비스 내에 반드시 필요한 요소가 있기 마련이며 이러한 필요를 느끼고 있는 이용자에게는 신원확인은 그다지 높은 장애물로 작용하지 않기 때문이다.

이러한 이유로 2012년도의 온라인게시판실명제 위헌결정 이후에도 대부분의 포털들은 자발적으로 계정개설 시점에서 본인확인을 요구하였다. 그런데 이렇게 계정개설시에 본인확인이 이루어지면 규제대상인 19금물, 온라인게임, 선거운동기간 중 후보지지반대글 외에도 다른 콘텐츠의 교환이나 소통도 본인확인이 이루어진 상태에서 이루어지게 된다. 결국은 이용자들은 19금물이나 온라인게임 이용 또는 선거운동기간 중 후보지지반대글 게시가 아닌 다른 포털서비스의 이용도 본인확인 상태에서 해야만 하는 상황이 지속되고 있다. 결론적으로 신원확인을 해야만 온라인 글쓰기를 해야 하는 상황, 2012년 헌법재판소가 위헌이라고 지적했던 상황은 지금도 계속되고 있는 것이다.

3. 익명성 규제에 대한 평가

가. 본인확인제 - 인터넷의 안티테제

위에서 살펴보았듯이 본인확인제의 궁극적인 한계는 명의도용의 가능성과 외국서비스를 통한 우회가능성에서 출발한다.

그런데, 외국서비스를 통한 우회가능성은 인터넷의 본래적인 특성은 아니다. 왜냐하면 인터넷에 대한 물리적 접속을 제공하는 통신사업자들은 국내사업자일 수 밖에 없으며 이들 국내사업자들에게 불법적인 소통 또는 유해한 소통을 제한할 것을 요청하는 방식의 규제가 가능하기 때문이다. 본인확인제의 경우에도 규제자가 원하기만 한다면 국내인들이 이용하는 웹사이트의 경우 외국에 서버를 두고 있더라도 본인확인제를 지키지 않는 경우 통신사업자를 통해 국내유통을 차단하는 방식으로 집행할 수도 있다. 사실 이와 같은 가능성을 원천적으로 차단하기 위해 구글이 유튜브의 Korea페이지의 게시기능을 없애버려 본인확인제 적용을 피했던 것은 유명하다.²⁴⁾ 물론 국내인들은 계속해서 유튜브의 다른 페이지를 통해 게시를 할 수 있었지만 당국은 유튜브 전체를 차단하는 조치를 취하지는 않았다.

그렇다면 본인확인제의 궁극적인 한계는 명의도용의 가능성인데 기실 명의도용의 가능성이란 본인확인제가 대응하려고 했던 익명성의 다른 이름일 뿐이다. 본인확인제는 생태적으로 무산가능성을 내포하고 있다.²⁵⁾ 가장 근원적으로는 기계와 사람 간의 '접속'이 불가능한 상태에

24) 2009년4월당시 유튜브의 결정을 설명한 유튜브 블로그의 공시문 http://youtubekrblog.blogspot.kr/2009/04/blog-post_08.html <2013.12.25. 방문>

25) 김기창은 인터넷 상의 본인확인은 기술적으로 불가능하다고 말한다. 인터넷상으로 할 수 있는 것은 본인의 표지를 소지하고 있는지만 확인할 수 있을 뿐이기 때문이다. 김기창, “인터넷 '실명제'의 기술적, 사업적, 법적 문제점”, <인권과 정의> (2009.7)

서 기계를 통한 통신은 지문인식 또는 홍채인식 등이 보편화되지 않는 한 속명적으로 신원도 용을 가능하게 한다. 실제로 이런 문제 때문에 인터넷 상 본인확인제는 단지 그 이론적 가능성 만 활발하게 논의되거나 이용자나 사업자가 자발적으로 시행하는 형태의 본인확인제 만이 논의되어 왔을 뿐 지금 이 논문의 주제인 강제적 본인확인제가 실제 실시된 경우는 우리나라 외에는 중국의 1개 서비스가 있을 뿐이다.

우리나라의 규제당국이 다른 나라에서 포기한 본인확인제도에 대해 자신감을 갖게 된 것은 주민등록번호의 존재와 밀접한 관계가 있다. 즉 주민등록번호라는 전국민에게 부여되는 고유 식별정보가 있어 이를 기반으로 한 신원확인이 이루어지고 있다. 물론 고유식별정보가 존재한 다는 것 만으로는 신원확인이 불가능하다. “이름 + 출신초등학교 + 졸업년도” 조합도 확률상 으로 보면 훌륭한 고유식별정보이지만 주민등록번호는 주민등록증이라는 상대적으로 간편한 유효성검증수단에 연계되어 있다. 이 때문에 주민등록번호는 학력정보와 달리 기업들이 소비자들과 거래를 하면서 왕성하게 수집하고 보관하고 있다. 그렇다면 인터넷소통의 신원확보 역 시 이 주민등록번호를 이용한다면 기업들이 가진 데이터베이스 조회를 통해 유효성검증을 할 수 있으니 가능하다는 것이 현재 우리나라 익명성 규제의 핵심논리이다.

그러나 이 핵심논리는 타인의 주민등록번호를 이용하여 소통할 위험에 취약하다. 특히 위에서 말했듯이 주민등록번호의 신원확인수단으로서의 가치를 높여주는 것은 기업들이 왕성하게 수집하고 있어서 통신당사자가 입력한 주민등록번호의 유효성검증이 용이하다는 것인데 바로 이러한 왕성한 수집과 보관 때문에 불법적인 유출과 유통이 더욱 가능하고 이는 명의도용 가능성 을 더욱 증폭시킨다. 필자는 이런 현상을 “신뢰성의 패러독스”라고 명명한 바 있다.²⁶⁾

그럼에도 불구하고, 2012년 인터넷실명제 위헌결정이 내려지던 해에 규제당국은 명의도용 가능성 문제를 해결하기 위해 휴대폰인증시스템을 개발하여 대중화하였다. 휴대폰인증시스템 에서는 이용자가 실명, 주민등록번호²⁷⁾ 외에도 휴대폰 번호를 넣어서 본인확인을 한다. 이때 입력된 번호의 휴대폰으로 인증번호가 전송되고 그 인증번호를 이용자가 입력해야 본인확인이 이루어지므로, 실명, 주민등록번호 만을 알고 있다고 해서 명의도용이 이루어지지 않는 다. 결국 위에서 검토한 청소년보호법, 게임산업진흥법, 공직선거법에 따른 본인확인제들은 각각 휴대폰인증시스템을 통해 유지되고 있다.

그러나 이 시스템의 실효성의 전제는 위의 본인확인에서 이용된 휴대폰이 해당 주민등록번호를 가진 사람의 이름으로 발부되었다는 것이다. 그렇지 않으면 타인의 실명, 주민등록번호를 가진 사람은 항상 자신의 휴대폰 번호를 입력하여 명의도용을 완수할 수 있을 것이기 때문이다. 결국 이 시스템은 ‘휴대폰실명제’²⁸⁾라는 또 하나의 위헌적인 제도에 의지해서만 제대로

26) 박경신, “신뢰성의 패러독스, 전자주민증”, 한겨레신문 2010년 10월 28일, <http://www.hani.co.kr/arti/opinion/column/445882.html> <2013.12.25. 방문>

27) 2012년 규제당국은 이와 동시에 위에서 언급했던 대형 주민등록번호 유출사태를 막기 위해 정보통신서비스제공자에 의한 주민등록번호수집을 금지하도록 법을 개정하여서 포털들은 주민등록번호 대신 생년월일 만을 수집하고 있다. 정보통신망 이용촉진 및 정보보호 등에 관한 법률[시행 2012.8.18] [법률 제11322호, 2012.2.17, 일부개정] 제23조의 2

28) 현재 전기통신사업법 제2조(정의)는 ‘전기통신설비’란 전기통신을 하기 위한 기계·기구·선로 또는 그 밖에 전기통신에 필요한 설비를 말하며, ‘전기통신역무’란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말하고 있다고 규정하고 있고, 같은 법 제30조(타인 사용의 제한)는 “누구든지 전기통신사업자가 제공하는 전기통신역무를 이용하여 타인의 통신을 매개하거나 이를 타인의 통신용으로 제공하여서는 아니 된다. 다만, ‘이용자가 제3자에게 반복적이지 아니한 정도로 사용하도록 하는 경우(같은 조 제4호)’ 등의 경우에는 그러지 아니하다.”고 규정하고 있으며, 전기통신사업법 제97조 제7호는 ‘제30조 각 호 외의 부분 본문을 위반하여 전기통신사업자가 제공하

기능할 수 있다.²⁹⁾

‘휴대폰실명제’에 대한 토론은 학계에서 전무한 상태이며 대부분의 사람들이 “대포폰은 범죄자들에게 이용되기 때문에 규제되어야 한다”는 류의 추상적인 이해만을 하고 있는 상태이다. 필자의 입장을 간단히 소개하자면 “익명통신의 자유”는 가장 강력히 보호되어야 하는 기본권 중의 하나라고 생각한다. 첫째 인터넷에의 게시와는 달리 전화통화는 1대1 또는 많아도 수십명 정도를 대상으로 이루어지기 때문에 명예훼손죄, 모욕죄, 선거법규제 등 표현의 자유 규제가 보통 전제로 하는 ‘공연성’이 없다. 둘째, 공갈죄 협박죄처럼 공연성이 요구되지 않는 경우라고 하더라도, 전화통화는 상호간의 동의를 전제로 이루어진다. 서로 모르는 사람 사이에서도 통화를 개시한 후 상대방이 전화를 끊지 않음으로서 암묵적인 동의를 표시한 상태에서 통화의 지속이 가능해진다. 그렇다면 상호 합의하에 이루어지는 대화의 경우 그 대화 자체가 불법적인 피해를 발생시키는 경우는 매우 제한적이라고 보아야 한다. (피싱 등이 익명의 전화 번호로부터 걸려오기는 하지만 피해는 통화의 내용이 발생하는 것은 아니다.) 정리하자면, 인터넷에 수십억명이 볼 수 있는 공연성있는 글을 올릴 익명표현의 자유가 있다면, 전화로 1인의 대상과 동의 하에 대화를 익명으로 할 자유는 훨씬 두텁게 보장되어야 한다.

결론적으로, 이렇게 ‘휴대폰실명제’가 무효가 된다면 본인확인제의 실효성을 제고할 방법은 없어지게 된다.

그럼에도 불구하고 우리는 쉽게 인터넷의 익명성에 대한 두려움을 가지고 있고 ‘익명만 아니라면 인터넷이 더욱 안전한 세상이 될 것’이라는 막연한 기대를 가지고 있다. 위에서 살펴본 대로 인터넷의 성질인 익명성이 기술적으로 제한불가능한 것이라면 인터넷에 대한 디스토피아적인 두려움과 실망을 가지고 살아갈 수 밖에 없다. 아래의 장에서는 익명성에 대한 새로운 고찰을 시도한다.

나. “익명성이 인터넷의 폐해의 원인이라서 이를 제한하기 위해 본인확인제가 필요하다”

는 전기통신역무를 이용하여 타인의 통신을 매개하거나 이를 타인의 통신용으로 제공한 자를 1년 이하의 징역 또는 5천만 원 이하의 벌금에 처한다.’고 규정하고 있다. 이에 대하여 서울북부지방법원 판결(2012 고정3168, 2013.1.23.)에서는 ① 전기통신사업법 제30조의 입법목적은 본래 사설 전화국 운영 등을 금지하는 것으로, 무선통신가입자의 명의대여 제한 또는 휴대전화기 양도 금지를 예정하지 않았고, ② 문언상 휴대전화기 자체를 ‘전기통신사업자가 제공하는 전기통신역무’라고 볼 수 없으므로, 휴대전화기 양도를 ‘전기통신사업자가 제공하는 전기통신역무를 타인의 통신용으로 제공하였다’라고 해석할 수 없다고 하였으나 항소심과 상고심에서 각각 파기되어 유죄가 선고되었다. 서울북부지방법원 제2형사부 판결(2013노188, 2013.5.3.), 대법원 판결 (2013도6062, 2013.10.16.)

29) 현재 2002.05.30, 2001헌바5, 구 전기통신사업법 제74조 등 위헌소원. 이 현재결정에서는 다음과 같은 구법의 조항이 위헌판정을 받았고 그 위헌판정에 대응하여 해당 조항이 현재와 같이 개정되었다. **구 전기통신사업법(2000. 1. 28. 법률 제6230호로 개정되기 전의 것) 제32조의2(타인사용의 제한)** 누구든지 전기통신사업자가 제공하는 전기통신역무를 이용하여 타인의 통신을 매개하거나 타인의 통신용에 제공하여서는 아니된다. 다만, 대통령령이 정하는 경우에는 그러하지 아니하다. **제74조(벌칙)** 제32조의2 본문의 규정에 위반하여 전기통신사업자가 제공하는 전기통신역무를 이용하여 타인의 통신을 매개하거나 타인의 통신용에 제공한 자는 500만원 이하의 벌금에 처한다.

필자는 개정된 조항 역시 위헌성을 치유하지 못하였다고 생각한다.

(1) 익명성에 대한 공포

규제담론의 핵심에 있는, “익명성이 인터넷 폐해의 원인”이라는 주장은 위에서 언급했던 모든 본인확인제의 정당화 근거가 될 수 있다. 익명의 공간이기 때문에 청소년들이 마음대로 성인물을 보거나 밤늦게까지 게임을 할 수 있을 것이며, 익명의 공간이기 때문에 자유롭게 특정 후보에 대한 칭찬이나 욕설을 늘어놓을 수 있을 것이다. 익명성이 없다면 또는 모두 ‘명찰을 달고’ 위의 행동들을 한다면 그러한 유해소통의 빈도 수는 줄어들 것이라는 논리이다.

그러나 우리는 원래 익명 속에서 생활한다. 오프라인 공간도 한정적인 의미에서는 이미 익명의 공간이다. 길거리에 나가면 사람들의 얼굴을 보지만 그 사람이 누구인지 알 길은 없으며 그 사람에게 물어본다고 하여 상대가 알려줄 의무도 없다. 그렇다면 소매치기가 가능한 것은 행위자가 피해자에게 접근해도 이렇게 행위자의 신원을 알 수 없다는 사실을 소매치기들이 이용하기 때문이다. 그렇다고 하여 과연 이와 같은 한정적 익명성을 소매치기의 원인이라고 할 수 있을까. 그것을 원인이라고 한다면 우리는 ‘길거리 보행자들은 모두 명찰을 달도록 강요하는’ 법을 만들어야 할 것이다.

익명성이 ‘인터넷 상의 악행의 원인’이라면 모든 악행의 원인일 것이다. 악행을 행하는 모든 사람은 사후적인 규제나 보복을 피할 강한 동기를 가지고 있고 이는 인간의 본능이다. 모든 악행자들은 자신의 이름을 항상적으로 공개하지 않아도 되는 ‘익명의 환경’을 이용하고 있다고 볼 수 있다. 예를 들어, 모든 보행자들에게 명찰달기를 요구하지 않는 규제적 환경은 보행자들의 익명성을 한정적으로나마 보장한다.

본인확인제가 모든 보행자들에게도 적용되어 익명성이 제거된다면 소매치기, 강도는 줄어들 가능성이 높을 것이다. 그러나 이 논리에는 한계가 없다. 아마도 인터넷 뿐만 아니라 어느 공간에서든 위법을 예방하는 가장 좋은 방법은 우리 자신을 상시 감시체제에 두는 것을 것이다. 본인확인제는 이용자의 사이버 상의 행적에 그 이용자의 신원을 확인할 수 있는 표지를 남기도록 함으로써 감시하는 것이다. 과연 그러한 감시의 부재가 위법행위들의 원인이라고 믿는다면 실제로 그러한 감시가 일상화되는 것이 옳다.

익명성은 인터넷 상의 해악의 발생을 추동한다는 의미에서의 원인이 아니다. 흡연은 모두가 인정하는 해악이며 흡연자 뿐만 아니라 비흡연자에게도 영향을 주며 흡연에 의해 발생하는 공공보건비용을 고려하면 국가경제 전체에도 영향을 주게 된다. 이때 흡연 역시 흡연자는 모두 명찰을 달고 흡연해야 하는 상황과 비교한다면 더욱 많은 사람들이 흡연을 하고 있는 것이다. 그러나 그렇다고 하여 익명성이 과도한 흡연의 ‘원인’이라고 볼 수는 없을 것이다. 결국 익명성을 인터넷 상의 폐해의 ‘원인’이라고 주장하는 것은 근본적인 문제해결에 도움이 되지 않는다.

(2) 해법

정리하자면, 본인확인제는 인터넷소통을 통해 해악이 발생한 후에 이를 규제하려는 국가기관에게 행정편의를 제공할 뿐이다. 그렇다면 그러한 편의를 위해 기본권을 제한해야 하는가, 제한한다면 어느 만큼 제한할 수 있는가는 별도의 문제인 것이다.

보행자실명제가 길거리범죄를 줄여도 보행자실명제가 위험인 것은 보행인들 중에서 범죄자들 숫자는 많지 않은 반면 사생활의 자유를 과도하게 제한하기 때문이다. 익명성의 제거는 부동산소유나 자동차운전처럼 사기, 탈세의 위험이나 타인의 생명에 대한 위험과 같이 특별한

위험이 있을 때만 헌법적으로 허용되고 있을 뿐 보행과 같이 일상적인 활동을 하는 사람에게 까지 적용하는 것은 부당하다.

익명성을 사전적으로 제거하지 않고 범죄퇴치를 할 수 있는 방법은 없지 않다. 바로 범죄가 발생했다고 믿을만한 이유가 있는 경우에 그러한 혐의가 있는 사람을 조사하는 것이다. 소매치기를 예방하기 위해 모든 보행자들에게 명찰을 달기를 요구하기보다, 소매치기처럼 행동하는 사람이 있으면 그 사람에게 가서 신분증을 요구하는 것이다. 실제 오프라인에서의 범죄예방은 이렇게 사후적인 방식으로 이루어지고 있다. 온라인에서도 다를 것이 없다.

청소년보호법의 경우도, 우선 법으로는 청소년에게 청소년유해매체물을 보여주면 처벌한다는 규정을 그대로 두고 사후적으로 그런 행동을 하는 의도적으로 하는 사업자가 있으면 처벌하면 되는 것이다. 또는 청소년에게 온라인게임을 심야에 하도록 해주는 사업자가 있다면 처벌하면 되는 것이다. 그러한 ‘유해한 소통’이 겉으로 드러나지 않는다면 청소년에 대한 탐문수사를 통해 그러한 ‘유해한 소통’을 의도적으로 제공한다고 믿을만한 이유가 있는 사업자들을 골라서 압수수색 등 필요한 수사절차를 거쳐 처벌하며 된다. 사업자들은 자신들의 책임 하에 청소년들에게 청소년유해매체물을 최대한 보여주지 않기 위한 여러 기술적 해법을 고안해낼 것이다. 그 중의 하나가 바로 미국연방대법원³⁰⁾과 우리나라 헌법재판소³¹⁾가 공히 승인한 필터링이다. 즉 사업자들이 청소년유해매체물을 서비스할 때는 국가에서 청소년유해매체물로 지정된 콘텐츠를 인식하는 소프트웨어의 존재를 대대적으로 홍보하여 부모들이 이 소프트웨어를 자신과 자신의 자녀의 단말기에 장착할 수 있도록 하는 것이다.

III. 전파성규제 - 시정요구제도

1. 시정요구제도

여기서는 전파성규제의 예로서 방송통신심의위원회의 시정요구제도를 살펴보고자 한다. 방송통신심의위원회는 행정기구로서 인터넷의 게시물을 심의하여 차단 및 삭제토록 방송통신위원회를 통해 명령하거나 ‘시정요구’할 수 있는 권한을 가지고 있다.³²⁾ 행정기구가 표현물의 합법 또는 불법을 잠정적으로 판단하는 경우 위축효과를 발생시키기 때문에 이러한 행정심의 자체가 금지되어야 한다는 주장³³⁾도 있지만 지면 관계상 여기서는 ‘시정요구’의 절차적 문제만

30) Ashcroft 대 ACLU, 542 U.S. 656 (2004) 이 사건은 미연방대법원은 성인물 열람을 위해서는 신용카드번호를 입력할 것을 의무화한 캘리포니아법에 대해 성인이 합법적인 표현물에 접근할 권리를 침해한다며 위헌판정을 내리며 부모가 필터링소프트웨어를 단말기에 장착하는 것을 대안으로 제시하고 있다.

31) 헌법재판소 2004. 1. 29. 선고 2001헌마894 결정. 이 사건에서 헌법재판소는 필터링기술이 적용될 수 있도록 청소년보호법에 따른 청소년유해매체물 표시를 Platform for Internet Content Selection 일명 PICS와 같은 특정기술표준과 특정메타태그를 통해 하도록 한 정보통신부 고시에 대해 합헌판정을 하였다.

32) 방송통신위원회 설치법 제21조(심의위원회의 직무) 심의위원회의 직무는 다음 각 호와 같다. 1. 「방송법」 제32조에 규정된 사항의 심의

2. 「방송법」 제100조에 따른 제재조치 등에 대한 심의·의결

3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7에 규정된 사항의 심의

4. 전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 대통령령이 정하는 정보의 심의 및 시정요구

33) 박경신, “방송통신심의위원회의 인터넷내용심의의 위헌성”, 『법학논총(한양대학교)』 제27권제2호 (2010.06)

을 다룬다.

문제는 이를 수행하면서 게시물을 게시한 사람에게 사전이든 사후든 아무런 통지를 하지 않는다는 것이다. 심의가 있을 것을 미리 통지하지 않음은 물론 심의의 결과도 통지를 해주지 않는다. 이 때문에 사후적으로 이의제기를 할 수 있는 절차³⁴⁾가 있다손 치더라도 자신의 게시물이 차단 또는 삭제를 당했는지 자체를 알 수가 없으니 이의제기를 할 수 없다. 오직 심의가 완료된 후에 해당 게시물을 삭제 또는 차단할 것을 정보통신서비스제공자에게 통보하는 것이 통지절차의 전부이다. 정보통신서비스제공자에게 해당 게시자에게 연락할 것을 권고하거나 의무화하고 있지도 않으며 정보통신서비스제공자는 고객관리에 있어서 게시물의 삭제 또는 차단이라는 부정적인 내용의 메시지를 전달하는 악역을 피하고자 하기 때문에 자발적으로 게시자에게 연락을 하는 경우는 없다. 이렇게 되니 심의위원회의 결정이 잘못되었을 경우 이를 시정할 수 있는 기회도 게시자가 우연히 자신의 게시물이 삭제된 것을 알고 제때에 소송을 제기하는 때만 주어진다.

심의회의 자체는 일반대중에게 공개되지만 모든 국민이 매번 회의를 방청할 수는 없고 정작 심의진행사실을 가장 잘 알고 있어야 할 게시자에게는 아무런 통지가 이루어지지 않으니 ‘비밀검열’이라는 비판을 피할 수 없다.

2. 시정요구제도에 대한 평가³⁵⁾

이와 같은 통지의 부재는 인터넷소통의 전파성 및 익명성에 의해 정당화된다. 즉 ‘심의위원회에서 통지를 하려 하여도 기본적으로 게시자는 익명으로 존재하기 때문에 통지가 불가능하다는 것이며, 설령 검색을 통해 게시자를 알아낼 수 있다고 하더라도 게시물의 해악이 신속하게 전파될 것을 생각한다면 게시자에게 사전통지를 한 후에야 심의를 하는 것은 너무 늦다’는 것이다. 결국 이 시정요구제도는 인터넷소통의 전파성 및 익명성에 대응하고자 하는 전형적인 매개자(intermediary)규제의 일종인 것이다.

그러나 헌법 제12조제1항은 “모든 국민은 신체의 자유를 가진다. 누구든지 법률에 의하지 아니하고는 체포·구속·압수·수색 또는 심문을 받지 아니하며, 법률과 적법한 절차에 의하지 아니하고는 처벌·보안처분 또는 강제노역을 받지 아니한다”고 하고 있다. 그런데 그 적용범위는 형사절차에만 한정되어 있지는 않다.

우리 현행 헌법에서는 제12조 제1항의 처벌, 보안처분, 강제노역. . . 과 관련하여 각각 적법절차의 원칙을 규정하고 있지만 이는 그 대상을 한정적으로 열거하고 있는 것이 아니라 그 적용대상을 예시한 것에 불과하다고 해석하는 것이 우리의 통설적 견해이다.³⁶⁾

“적법절차는 비단 신체의 자유(헌법 제12조)에서만이 아니고 모든 기본권보장과 관련이 있는 것이고 법치주의의 구체적 실현원리라고 할 것(헌법재판소1990.11.19. 선고 90헌가48 결정참조)이다.”³⁷⁾

그렇다면 위와 같이 적법절차의 원리는 이번 사건처럼 표현의 자유에도 적용될 수 있는 것

34) 방송통신위원회 설치법시행령 제8조 ⑤ 제2항에 따른 시정요구에 대하여 정보통신서비스제공자, 게시판 관리·운영자 또는 해당 이용자는 그 시정요구를 받은 날부터 15일 이내에 심의위원회에. . . 이의신청을 할 수 있다.

35) 이 장의 내용의 일부는 다음의 문헌에 포함되어 있다. 박경신, “방송통신심의위원회의 인터넷내용심의의 위헌성”, 『법학논총(한양대학교)』 제27권제2호(2010.06)

36) 헌재 1992.12.24. 92헌가8

37) 헌재1992.11.12. 91헌가2 판례집4, 713, 723

이며 일반행정기관에 의한 게시물 삭제에도 적용된다고 할 것이다.

우리 헌법재판소는 헌법 제12조 제3항의 ‘적법한 절차’는 미국에서 발달된 적법절차원리를 도입한 것으로 보고 있다.³⁸⁾ 미국연방대법원은 미국헌법의 적법절차(due process)를 해석하기를 정부가 개인의 생명, 자유 및 재산(life, liberty or property)을 제한할 때는 다음과 같은 절차를 따를 것을 요구하고 있다.³⁹⁾ ① 자유의 제한 및 그 이유에 대한 고지 (an adequate notice) ② 이의제기를 할 수 있는 기회, 예를 들어 청문회 (a hearing) ③ 중립적인 판정자에 의한 판정 (a neutral judge)⁴⁰⁾ 이 세가지 요건을 잘 살펴보면 근대의 민형사재판의 절차와 닮아 있음을 알 수 있다.

안타까운 것은 방송통신위원회 설치법 제25조는 심의위원회가 제재조치를 정하는 때에는 당사자에게 ‘미리’ 의견을 진술한 기회를 주어야 한다고 하고 명시하고 있음에도 불구하고⁴¹⁾ 의견진술기회가 주어지고 있지 않다는 점이다. 심의위원회는 심의가 끝난 후 강제력있는 “제재조치”를 결정하지 않고 정보통신서비스제공자에게 강제력이 없는 “시정요구”만을 결정한다는 이유로 제25조 상의 의무를 이행하지 않고 있다. 그러나, 2012년 서울고등법원은 이 “시정요구”가 실제로는 단순히 권고의 효력을 넘어서서 실질적으로는 게시자에 대하여 “행정처분”의 기능을 하고 있다고 판시한 바 있다.⁴²⁾ 그렇다면 모든 행정처분은 행정절차법에 따라 그 결정 및 집행과정이 규율되는데 행정처분을 정할 때는 반드시 처분의 당사자에게 의견을 제출할 기회를 보장해줄 것을 규정하고 있으므로⁴³⁾ 방송통신심의위원회의 ‘시정요구’ 역시 의견을 제출할 기회를 보장해주어야 한다.

3. 전파성에 대한 평가

전파성에 대한 우리나라 인터넷규제의 대응은 전파성의 또다른 측면을 간과하고 있는 것으로 보인다. 즉 인터넷의 특성인 빠른 전파성과 익명성을 그대로 받아들인다면 이를 ‘역이용’하여 게시자에게 충분히 의견진술기회를 주면서도 심의의 속도를 늦추지 않을 수 있다는 것이다.

첫째 속도의 문제에 있어서 익명게시판에 올라온 글의 경우 게시판에 공개된 댓글을 남기는 방식으로 훌륭한 통지기능을 수행할 수 있다. 요즘 게시판들은 보통 댓글을 남기면 원글 작성자에게 통지를 해주는 기능이 장착되어 있다. 그렇지 않다고 하더라도 방송통신심의위원회의

38) 헌재 1992.12.24, 92헌가8

39) Goldberg v. Kelly, 397 U.S. 254, 267 (1970)

40) 참고로 위에서 judge는 반드시 직업적인 법관을 의미하는 것은 아니고 판정자를 말한다.

41) 방송통신위원회설치법 제25조 제2항 심의위원회는 [제44조의7에 따른 불법정보 유통에 대한 취급의 거부·정지 또는 제한]의 제재조치를 정하려는 때에는 미리 당사자 또는 그 대리인에게 의견을 진술할 기회를 주어야 한다.

42) 2012.5.4. 서울고등법원 제3행정부 2010누9428 (상고포기)

43) 행정절차법 제21조(처분의 사전 통지) ① 행정청은 당사자에게 의무를 부과하거나 권익을 제한하는 처분을 하는 경우에는 미리 다음 각 호의 사항을 당사자들에게 통지하여야 한다.

1. 처분의 제목
2. 당사자의 성명 또는 명칭과 주소
3. 처분하려는 원인이 되는 사실과 처분의 내용 및 법적 근거
4. 제3호에 대하여 의견을 제출할 수 있다는 뜻과 의견을 제출하지 아니하는 경우의 처리방법
5. 의견제출기관의 명칭과 주소
6. 의견제출기한
7. 그 밖에 필요한 사항

명의로 같은 게시판에 또다른 글을 게시하면 이에 대한 네티즌들의 반응이 나올테고 곧 게시자에게 자연스럽게 통지가 도달하게 될 것이다. 익명블로그의 경우 안부게시판에 글을 남길 수도 있다. 즉 전파성의 뼈대를 이루는 다양한 통신방법을 그대로 이용하여 심의사실 및 결과를 게시자에게 알려줄 수 있다.

둘째 게시자의 신원을 반드시 사전에 알아야만 게시자의 의견을 청취할 수 있는 것이 아니다. 게시자는 익명으로 자신의 의견을 개진할 수 있는 것이다. 물론 이 경우 의견진술자가 해당 심의대상 게시물을 실제로 게시한 사람인가 확인해볼 필요가 있고 이에 대해서 의견진술자가 입증책임을 져야 하겠지만, 이는 진술의 내용에 대한 평가와 동시에 이루어질 수 있는 것이니 반드시 사전에 의견진술자와 게시자의 동일성을 확인한 후에 진술의 내용을 접수할 필요는 없는 것이다.

IV. 마치며

우리나라 인터넷규제 담론은 인터넷 소통의 기본적 특성이라고 할 수 있는 익명성, 전파성에 직접적으로 대응하는 것을 기조로 하고 있으며 인터넷 소통의 또 하나의 특성이 상호성을 간과하여왔다. 익명성에 대한 직접적 대응은 청소년보호법, 게임산업진흥법, 공직선거법 본인확인제들의 제정으로 귀결되었고 전파성에 대한 직접적인 대응은 방송통신심의위원회와 같이 ‘법원판결을 기다리지 않고 게시물들을 차단 및 삭제하는 시스템’의 확립으로 이어졌으며, 익명성과 전파성에 대한 중첩적인 고려는 인터넷 소통에 대한 규제는 소통 당사자에게 직접 작용하는 것이 아니라 소통의 매개자들 즉 포털이나 통신사들에게 작용하는 방식 즉 임시조치제 도나 방송통신심의위원회 시정요구제도로 나타났다. 이 글에서는 이들 제도 중에서 본인확인제들과 방송통신심의위원회 시정요구제도를 예로 살펴보았다.

위의 모든 본인확인제들은, 2012년 헌법재판소의 게시판실명제 결정에 비추어 보자면, 온라인의 본인확인절차가 동반할 수 밖에 없는 명의로용 가능성을 고려할 때, 이용자 일부(청소년 또는 불법게시자)에 대한 규제를 위해 사전적으로 모든 이용자에게 사생활의 비밀 침해를 감수키는 것으로서, 표현의 자유 또는 정보접근권에 대한 심대한 침해임이 확인되었다. 특히 본인확인제도는 익명성에 대한 추상적인 두려움과 실명성에 대한 맹목적인 기대에 근거한 것으로서 익명성/실명성에 대한 올바른 이해는 본인확인제도의 타당성 및 필요성에 대한 재검토를 요구한다고 하겠다. 방송통신심의위원회의 시정요구제도 역시 국가가 국민의 권리를 제한하거나 국민에게 의무를 부과할 때는 해당 국민에게 의견을 사전에 들어보아야 한다는 기본원리가 전파성, 익명성에 대한 과도한 두려움에 의해 잠식된 결과물임이 확인되었다. 전파성 및 익명성을 제대로 이해한다면 도리어 이를 통해 신속하게 의견진술기회를 게시자들에게 제공할 수 있기 때문이다. 마지막으로 인터넷의 주요 특성이라고 할 수 있는 상호성은 새로운 규제담론의 출현을 요구하는데 이에 대해서는 지면 관계상 다음으로 미루기로 한다.

<영문초록>

A discourse on this country's internet regulation has focused on the need to respond directly to anonymity and rapid diffusion, two fundamental characteristics of the Internet communications. A response to anonymity resulted in a series of mandatory identity verification regulations, and a response to extreme diffusibility resulted in administrative censorship conducted by the Korean Communication

Standards Commission designed to block or delete material ‘without waiting for a court’s judgment’. Also, a concern with anonymity and diffusibility resulted in regulatory schemes operating not on the speakers themselves but on the intermediaries, such as the “provisional take-down” system incentivizing the intermediaries to block content without determining the legality of the contents or the “corrective requests” issued by KCSC to the intermediaries.

This article conducts constitutional evaluation of the identity verification laws and the KCSC “corrective requests” system, respectively on free speech and due process. Identity verification rules, it finds, are the products of fear against anonymity and reliance on a real-name system, which must be re-conceived itself, and the “corrective system” also is a misguided response to the Internet’s diffusibility, which can be better responded by taking advantage of such efficient communication functions to provide notice to those who posted the material. The article will be the first of a two-article piece, the second of which will deal with how reciprocity, the third main characteristic of the Internet communication, affect and shape the relevant regulatory terrain.

<국문초록>

우리나라 인터넷규제 담론은 인터넷 소통의 기본적 특성이라고 할 수 있는 익명성, 전파성에 직접적으로 대응하는 것을 기조로 하고 있으며 인터넷 소통의 또 하나의 특성이 상호성을 간과하여 왔다. 익명성에 대한 직접적 대응은 일련의 본인확인제들의 제정으로 귀결되었고 전파성에 대한 직접적인 대응은 방송통신심의위원회와 같이 ‘법원판결을 기다리지 않고 게시물들을 차단 및 삭제하는 시스템’의 확립으로 이어졌으며, 익명성과 전파성에 대한 중첩적인 고려는 인터넷 소통에 대한 규제는 소통 당사자에게 직접 작용하는 것이 아니라 소통의 매개자들 즉 포털이나 통신사들에게 작용하는 방식 즉 임시조치제도나 방송통신심의위원회 시정요구제도로 나타났다. 이 글에서는 이들 제도 중에서 본인확인제들과 방송통신심의위원회 시정요구제도를 예로 살펴보고 헌법적인 평가를 해본 결과, 본인확인제도는 익명성에 대한 추상적인 두려움과 실명성에 대한 맹목적인 기대에 근거한 것으로서 익명성/실명성에 대한 올바른 이해는 본인확인제도의 타당성 및 필요성에 대한 재검토를 요구한다고 하겠다. 방송통신심의위원회의 시정요구제도 역시 국가가 국민의 권리를 제한하거나 국민에게 의무를 부과할 때는 해당 국민에게 의견을 사전에 들어보아야 한다는 기본원리가 전파성, 익명성에 대한 과도한 두려움에 의해 잠식된 결과물임이 확인되었다. 전파성 및 익명성을 제대로 이해한다면 도리어 이를 통해 신속하게 의견진술기회를 게시자들에게 제공할 수 있기 때문이다. 마지막으로 인터넷의 주요 특성이라고 할 수 있는 상호성은 새로운 규제담론의 출현을 요구하는데 이에 대해서는 이 논문의 속편으로 미루기로 한다.

<Key Words>

identity verification, Korea Communication Standards Commission, anonymity, diffusibility, mutuality, Internet communication, Youths Protection Act, Game Industry Promotion Act, Public Officials Election Act

<색인어>

본인확인제, 방송통신심의위원회, 익명성, 전파성, 상호성, 인터넷소통, 청소년보호법, 게임산업진흥에 관한 법, 공직선거법

<참고문헌>

김용철, 「정보화시대의 사회운동: 온라인 사회운동의 유형과 특징」, 『사이버커뮤니케이션학보』, 통권 제25호 제1호, 2008

황지연, 「사이버공동체의 정체성과 집합행동」, 『정보와 사회』, 통권 제6호, 2004

김성태/이영환, 「인터넷을 통한 새로운 의제 설정 모델의 적용」, 『한국언론정보』, 제50권 3호, 2006

김경년, 김재영, “오마이뉴스의 독자의견분석”, 한국방송학보 19-3; 배영 외 3인, “2008년도 본인확인제 효과분석”

권현영 외 6인, “인터넷게시판 정책현황 분석 및 실효성 확보방안”, 한국인터넷진흥원 발주 한국전자정부 수탁 연구용역 보고서, 2009. 12

한운형 발표문, “개인정보보호의 이해 및 안전한 관리 - 개인정보의 의의 및 처리 실태” (2012.11.21.) 정보화진흥원

황성기, “인터넷게임 이용을 위한 청소년의 회원가입시 부모의 필요적 사전동의제도의 헌법적 문제점”, 『공법학연구』 제12권 제1호, 한국비교공법학회, 2011. 2. 28

현군택외 3인, <청소년 인터넷게임 건전이용제도(강제적 셧다운) 실태조사 보고서>, 2012년 여성가족부 용역.

박문수, 고대영, 박정수, <게임시장의 규제가 산업생태계 발전에 미치는 영향과 시사점>, 산업연구원 (2013.12)

제 18대 국회의원선거총람

김기창, “인터넷 '실명제'의 기술적, 사업적, 법적 문제점”, <인권과 정의> (2009. 7)

박경신, “방송통신심의위원회의 인터넷내용심의의 위헌성”, 『법학논총(한양대학교)』 제27권제2호(2010.06)

【NTD(Notice and Take Down) 비교: 정보통신망법 & 저작권법】

현행	유승희의원안	방통위안	저작권법
제44조의2(정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등”이라 한다)를 요청할 수 있다.	제44조의2(정보의 삭제요청 등) ① ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- <u>차단</u> ----- ----- <u>차단등</u> ----- -----.	제44조의2(<u>임시조치</u> 등) ① - ----- ----- ----- ----- ----- <u>권리</u> 을 침해받았다고 주장하는 자(이하 “ <u>권리주장자</u> ”라 <u>한다</u>)----- ----- ----- <u>삭제</u> - ----- ----- -----.	103조(복제·전송의 중단) ① 온라인서비스제공자(제102조 제1항 제1호의 경우는 제외한다. 이하 이 조에서 같다)의 서비스를 이용한 저작물등의 복제·전송에 따라 저작권, 그 밖에 이 법에 따라 보호되는 자신의 권리가 침해됨을 주장하는 자(이하 이 조에서 “ <u>권리주장자</u> ”라 한다)는 그 사실을 소명하여 온라인서비스제공자에게 그 저작물등의 복제·전송을 중단시킬 것을 요구할 수 있다.
② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하	② ----- ----- ----- <u>차단</u> ----- ----- <u>차단등의</u> ----- ----- -----. ----- ----- ----- ----- -----	② 정보통신서비스 제공자는 제1항에 따른 정보의 삭제를 요청받으면 지체 없이 그 정보에 대한 접근을 임시적으로 차단하는 조치(이하 “ <u>임시조치</u> ”라 한다)를 하고, 지체 없이 다음 각 호의 사항을 권리주장자 및 정보게재자에게 통지하여야 한다. 다만, 정보	② 온라인서비스제공자는 제1항에 따른 복제·전송의 중단요구를 받은 경우에는 즉시 그 저작물등의 복제·전송을 중단시키고 권리주장자에게 그 사실을 통보하여야 한다. 다만, 제102조 제1항 제3호 및 제4호의 온라인서비스제공자는 그 저작물등의 복제·전송자에

현행	유승희의원안	방통위안	저작권법
는 등의 방법으로 이용자가 알 수 있도록 하여야 한다. ③ <u>정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.</u> ④ <u>정보통신서비스 제공자</u>	----- -----. <삭 제> ④ <u>정보게재자가 제2항의</u>	<u>게재자에게 통지할 수 없는 경우에는 해당 게시판에 게시하여야 한다.</u> 1. <u>임시조치의 사실 및 기간</u> 2. <u>이의제기의 방법 및 절차</u> 3. <u>이의제기 시 직권조정절차에 회부된다는 사실</u> ③ <u>정보통신서비스 제공자는 임시조치를 한 사실을 해당 게시판에 게시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.</u> ④ <u>제2항에 따른 임시조치</u>	게도 이를 통보하여야 한다. ③ 제2항에 따른 통보를 받은 복제·전송자가 자신의 복제·전송이 정당한 권리에 의한 것임을 소명하여 그 복제·전송의 재개를 요구하는 경우 온라인서비스제공자는 재개요구사실 및 재개예정일을 권리주장자에게 지체 없이 통보하고 그 예정일에 복제·전송을 재개시켜야 한다. 다만, 권리주장자가 복제·전송자의 침해행위에 대하여 소를 제기한 사실을 재개예정일 전에 온라인서비스제공자에게 통보한 경우에는 그러하지 아니하다. ④ 온라인서비스제공자는

현행	유승희의원안	방통위안	저작권법
는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 “임시조치”라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다. ⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다.	조치에 대하여 자신이 제한 정보가 정당한 권리에 의한 것임을 소명하여 이의신청을 할 경우 정보통신서비스 제공자는 해당 조치를 30일 이내에 해제하여야 하고 즉시 해제예정일을 신청인 및 정보게재자에게 알려야 한다. ⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다. 다만 신청인이 정보게재자의 침해행위에 대하여 소를 제기한 사실을 해제예정일 전에 정보통신서비스 제공자에게 통보한 경우에는 그러하지 아니하다.	의 기간은 30일로 한다. 다만, 제5항에 따른 정보게재자의 이의제기가 있는 때에는 제44조의14제1항에 따른 직권조정절차가 종료되는 날까지로 한다. ⑤ 정보게재자는 제4항 본문에 따른 임시조치의 기간 내에 임시조치에 대하여 이의를 제기할 수 있다. 이 경우 정보통신서비스 제공자는 다음 각 호의 사항을 권리주장자에게 지체없이 통지하여야 한다. 1. 정보게재자의 이의제기 사실 2. 직권조정절차에 회부된다는 사실 3. 직권조정결정의 절차	제1항 및 제3항의 규정에 따른 복제·전송의 중단 및 그 재개의 요구를 받을 자(이하 이 조에서 “수령인”이라 한다)를 지정하여 자신의 설비 또는 서비스를 이용하는 자들이 쉽게 알 수 있도록 공지하여야 한다. ⑤ 온라인서비스제공자가 제4항에 따른 공지를 하고 제2항과 제3항에 따라 그 저작물등의 복제·전송을 중단시키거나 재개시킨 경우에는 다른 사람에 의한 저작권 그 밖에 이 법에 따라 보호되는 권리의 침해에 대한 온라인서비스제공자의 책임 및 복제·전송자에게 발생하는 손해에 대한 온라인서비스제공자의 책임을 면제한다. 다만, 이항의 규정은 온라인서비스제공자가 다른 사람에 의한 저작물등의 복제·전송

현행	유승희의원안	방통위안	저작권법
⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다. <신 설>	⑥ ----- ----- -----제2항 및 제4항----- -----해당 정보 및 차단 등으로----- ----- -. ⑦ 정보통신서비스 제공자는 제2항 및 제4항의 업무를 처리하기 위한 담당자를 지정하고 연락처 게시 등 필요한 조치에 대한 내용·절차 등을 약관에 구체적으로 밝혀야 한다.	⑥ 제5항 각 호 외의 부분 본문에 따른 정보게재자의 이의제기가 있는 경우에는 제44조의14에 따른 직권조정절차에 회부된 것으로 본다. 이 경우 정보통신서비스 제공자는 대통령령으로 정하는 바에 따라 임시조치와 관련된 자료를 제44조의10에 따른 온라인 명예훼손분쟁조정위원회에 지체 없이 송부하여야 한다. ⑦ 정보통신서비스 제공자는 제5항 각 호 외의 부분 본문에 따른 정보게재자의 이의제기가 없는 경우에는 제4항 본문에 따른 임시조치의 기간이 만료한 후 해당 정보를 즉시 삭제하여	으로 인하여 그 저작권 그 밖에 이 법에 따라 보호되는 권리가 침해된다는 사실을 안 때부터 제1항에 따른 중단을 요구받기 전까지 발생한 책임에는 적용하지 아니한다. ⑥ 정당한 권리 없이 제1항 및 제3항의 규정에 따른 그 저작물등의 복제·전송의 중단이나 재개를 요구하는 자는 그로 인하여 발생하는 손해를 배상하여야 한다. ⑦ 제1항부터 제4항까지의 규정에 따른 소명, 중단, 통보, 복제·전송의 재개, 수령인의 지정 및 공지 등에 관하여 필요한 사항은 대통령령으로 정한다. 이 경우 문화체육관광부장관은 관

현행	유승희의원안	방통위안	저작권법
<신설>	⑧ 정보통신서비스 제공자는 대통령령으로 정하는 바에 따라 제2항의 조치에 관한 보고서를 작성하여 매년 2회 방송통신위원회에 보고하여야 한다.	야 한다. ⑧ 정보통신서비스 제공자는 정보의 삭제 요청, 임시 조치에 관한 내용 및 절차 등을 미리 약관에 구체적으로 밝혀야 한다.	계중앙행정기관의 장과 미리 협의하여야 한다.
<신설>	⑨ 방송통신위원회는 제8항에 따른 보고서를 공개하여야 한다.	⑨ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항 및 제3항에 따른 조치와 제7항에 따라 해당 정보를 삭제한 경우에는 이로 인한 책임을 면제받거나 감경받을 수 있다.	
<신설>		⑩ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하	

현행	유승희의원안	방통위안	저작권법
제44조의3(임의의 <u>임시조치</u>) ① 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 <u>임시조치를 할 수 있다.</u> <u><단서 신설></u> ② 제1항에 따른 임시조치에 관하여는 제44조의2제2항 후단, 제4항 후단 및 제5항을 준용한다.	제44조의3(임의의 <u>차단 등</u>) ① ----- ----- ----- ----- <u>침해함이 명백한 경우에는 임의로 차단 등의 조치를 하거나 제44조의2제4항의 해제요청을 거부할 수 있다. 다만 해당 정보가 타인의 권리를 침해하지 아니함이 명백한 경우에는 제44조의2제2항의 요청을 거부하거나 차단조치된 게시물에 대한 해제조치를 할 수 있다.</u> ② -----차단, 해제요청의 거부, 차단요청의 거부, 해제조치에 관하여는 제44조의2제2항 후단, 제4항부터 제9항까지를 준용한다.	<u>는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.</u> 제44조의3(임의의 <u>임시조치</u>) ① (현행과 같음) ② 정보통신서비스 제공자는 제1항에 따른 임의의 임시조치를 한 경우에는 다음 각 호의 사항을 정보게재자에게 지체 없이 통지하여야 한다. 다만, 정보게재자에게 통지할 수 없는	

현행	유승희의원안	방통위안	저작권법
<신설> 제44조의6(이용자 정보의 제공청구) ① 특정한 이용자에 의한 정보의 게재나 유통으로 사생활 침해 또는 명예훼손 등 권리를 침해하였다고 주장하는 자는 민·형사상의 소를 제기하	③ <u>정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.</u>	경우에는 해당 게시판에 게시하여야 한다. 1. <u>임시조치의 사실 및 기간</u> 2. <u>이의제기의 방법 및 절차</u> 3. <u>이의제기 시 직권조정절차에 회부된다는 사실</u> ③ <u>제1항에 따른 임시조치에 관하여는 제44조의2제3항, 제4항, 제5항 각 호 외의 부분 전단 및 제6항부터 제9항까지의 규정을 준용한다.</u> 제44조의6(이용자 정보의 제공청구) ① ----- ----- ----- ----- ----- -----	

회 행	유승희의원안	방통위안	저작권법
		<u>에 직권으로 해당 정보의 삭제 또는 임시조치의 해제에 관하여 조정을 갈음하는 결정(이하 “직권조정결정”이라 한다)을 하여야 한다. 이 경우 분쟁조정위원회가 정보통신서비스 제공자로부터 임시조치와 관련된 자료를 송부받은 날을 직권조정절차가 개시된 날로 본다.</u> <u>② 직권조정결정서에는 주문(主文)과 결정 이유를 적고 이에 관여한 위원 전원이 기명날인하여야 하며, 그 정본을 지체 없이 당사자에게 송달하여야 한다.</u> <u>③ 제2항에 따라 직권조정결정서를 송달받은 당사자는 송달받은 날부터 15일 이내에 소송을 제기하지 아니하면 직권조정결정의 내용을 수락한 것으로 본다.</u> <u>④ 제3항에 따라 소송이 제기된 경우에 직권조정결정의 효력은 상실된다.</u>	

현행	유승희의원안	방통위안	저작권법
<신 설>		⑤ 분쟁조정위원회는 제4항에 따른 사실을 정보통신서비스 제공자에게 통보하여야 한다. 이 경우 정보통신서비스 제공자는 지체없이 해당 정보에 대한 임시조치를 해제하여야 한다. 제44조의15(조정의 효력) 제44조의13제6항에 따른 조정조서 또는 제44조의14제2항에 따른 직권조정결정서는 다음 각 호의 어느 하나에 해당하는 경우에는 당사자 간에 조정조서 또는 직권조정결정서와 동일한 내용의 합의가 성립된 것으로 본다. 1. 제44조의13제6항에 따른 조정조서를 당사자에게 송달한 경우 2. 제44조의14제3항에 따른 소송의 제기가 없는 경우	

정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안 검 토 의 건

정 부 제 출 안(2014. 12. 29.)

2015. 2.



1. 현행 임시조치제도의 문제점

□ 합법적인 정보 삭제·차단의 의무화

- 누구든 권리침해를 소명하여 삭제 신청을 하면 반드시 삭제 등 “조치를 하고(제44조의2 제1항 및 제2항),” “권리침해 판단이 어렵거나 분쟁이 예상되는 경우”에만 임시조치를 “할 수 있다(제44조의2 제4항)”고 하여 합법적인 정보에 대해 불합리한 삭제 요청이 있더라도 최소한 임시조치는 취해야 하는 것으로 해석될 수 있음.
- 결국 명예 등 타인의 권리를 침해하지 않는 합법적 정보에 대해서도 온라인에 있다는 이유만으로 일시적인 차단·삭제를 의무화하는 것은 헌법 제21조 제4항에 어긋남.

□ 정보게재자의 표현의 자유 침해

- 저작권법과 달리 (1) 정보게재자의 복원권을 보장하고 있지 않고 (2) 부당한 요청에 대한 손해배상 규정이 없어, 임시조치 요청자의 권리남용을 막기 위한 장치가 미흡함.

□ 전기통신사업자에 의한 사적 검열

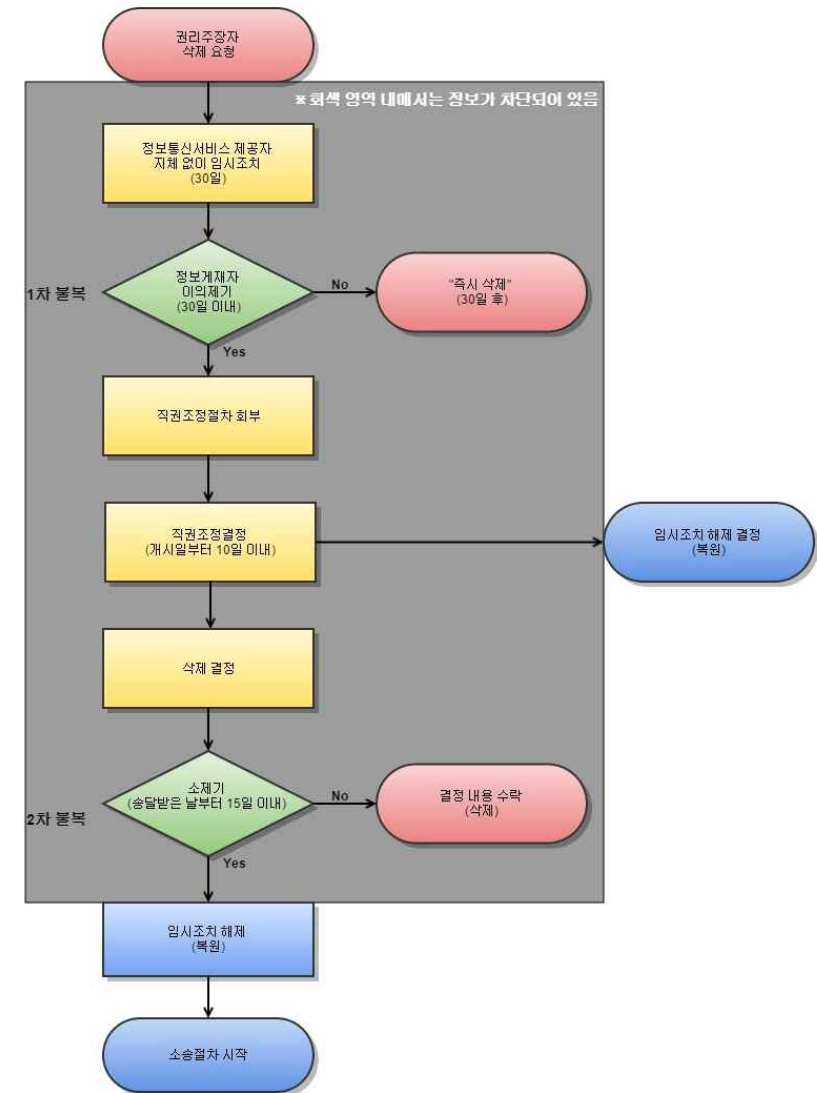
- 제44조의2 제1항은 “권리를 침해한 경우”로 한정되어 있어 위와 같은 삭제 의무는 ‘권리를 침해하는’ 정보에 대해서만 발생하고 임시조치는 임의적인 것으로 해석될 여지도 있으나 이와 같은 불분명함 때문에 상당한 혼란이 존재하고 있음.

- 특히 이렇게 해석되면 사업자에게 정보의 불법성에 대해 실질적 판단의 여지를 남김. 이러한 여지가 있는 경우 리스크 관리에 민감한 대부분의 사업자들에게 합법적인 정보들도 삭제·차단할 동기를 과도하게 부여하게 되어 사실상 사적 검열로 기능하게 됨.

□ 면책조항으로서의 역할 불가능

- 위와 같이 “과잉차단의 동기부여(incitizing into over-censorship)” 문제가 있어, 인터넷사업자 책임조항들은 특정 조치들을 충실히 취하면 불법정보 유통으로 인한 책임을 면하는 면책(safe harbor) 조항으로 구성하는 것이 국제적인 흐름임.
 - 예컨대 미국의 DMCA의 경우 [(1)요청시 차단 - (2) 복원요청시 복원]의 절차만 충실히 지키면 사업자에게 면책이라는 법적혜택을 제공함으로써 차단과 복원의 동기를 같이 부여하여 균형을 잡는 방식임.
 - EU Directive 2000/31/EC의 면책조항과 이를 따른 영국, 독일 등 대부분 EU 국가들의 법제도 일정한 조치를 취하면 면책이 되도록 함으로써 동기를 부여하는 구조임.
- 그런데 현행법은 ‘권리를 침해하는 경우... 요청을 하면... 하여야 한다’고 하여 책임을 부과하는 구조로 되어 있어 세계적 흐름에 역행하고 있음. 별도의 감면규정이 있지만 의무를 부과하는 조항이 선행하기 때문에 면책으로 인한 동기부여가 의미 없어짐.
- 게다가 임의적 감면으로 규정되어 있어 면책 여부가 확실하지 않아 더욱더 삭제·차단을 과도하게 하도록 만듦.

2. 개정안 임시조치 흐름도



3. 오픈넷 검토의견

가. 검토배경

- 방송통신위원회는 정보통신망법 개정안을 2014년 12월 29일 국회에 제출함.
- 박근혜 대통령의 대선공약 중의 하나였던 “인터넷 표현의 자유 증진”의 방법으로서 “인터넷 포털사의 임시조치 남용”을 막기 위해 “정보 게재자의 표현의 자유 보장”을 이루겠다는 취지로 이해됨(공약집 289쪽).
- 일견 정보게재자의 표현의 자유를 보장하는 측면이 있으나 아래와 같이 현행 임시조치제도의 문제점을 대단히 악화시키고 있음. 이는 표현의 자유 보장 공약에 역행하는 개악임.

나. 주요 쟁점

□ 합법정보의 차단 의무화 악화

- 개정안은 합법적 표현물도 누군가 “권리가 침해됨을 주장”하기만 하면 무조건 임시조치할 것을 의무화하고 있음. 현행법이 가지고 있는 문제를 더욱 악화시키는 개정안임.
- 현행법도 해석상 임시조치 의무를 부과한다고 볼 수도 있으나 위에서 설명한 바와 같이 “권리가 침해된 경우”일 것을 요구하여 사업자들이 불합리한 요청을 거부할 여지를 남겨두고 있음.
- 개정안에는 이런 여지가 없어 침해주장자는 요청이 받아들여지지 않으면 합법적인 정보에 대해서도 임시조치 불이행에 대해 사업자를 상대로 손해배상을 청구할 수 있는 반면, 게시자는 합법적인 정보의 차단에 대해 아무 저항도 할 수 없음.

- 이는 불법정보만을 차단하겠다는 정보통신망법의 취지에 어긋나며 언론·출판의 자유는 “타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해”하지 않는 한 보장할 것을 요구하는 헌법 제21조 제4항에도 반함.

□ 2번의 불복 및 소제기를 요건으로 하는 무의미한 복원권

- 정보게재자의 이의제기시 임시조치를 유지하고 직권조정절차로 회부하고, 직권조정결정에 대해 소제기를 해야만 임시조치 해제(복원)가 이루어짐.
- 현행 임시조치에 대한 이의제기율도 매우 낮는데*, 복원을 위해 2번의 불복 그것도 두 번째 불복은 소송을 제기할 것을 요구하는 것은 이의제기를 원천적으로 무산시키는 것과 다를 바 없음.
*국회입법조사처 현안보고서 통계에 의할 때 약 5% 이하로 추정
- 복원이 거의 불가능해 정보게재자의 표현의 자유를 심각하게 침해하는 반면, 권리침해주장자는 소명만으로 정보를 차단시킬 수 있어 보호법익간 지금보다 더욱 큰 불균형이 발생. 이는 게시자의 표현의 자유를 보호하겠다는 대통령 공약사항에 반하는 개정임.
- 저작권법처럼 이의제기시 임시조치를 즉시 해제하고 분쟁해결 절차가 진행되도록 하는 것이 표현의 자유를 증진하고자 하는 법안의 취지에 부합.
- 현행 저작권법 제103조에 의하면 복제·전송자는 소명만으로 재개를 요구할 수 있고 이에 따라 OSP는 복제·전송을 재개시켜야 함. 또한 유승희 의원 대표발의안(의안번호 8685)은 1회 불복만으로 복원을 가능하게 하고 있어 훨씬 바람직함.

- 이렇게 하더라도 게시자들은 이의제기를 자제하는 성향을 보이기 때문에 불합리하게 차단된 일부 정보 외에는 자연스럽게 게시자의 절차적 권리를 침해하지 않으면서 삭제되는 효과를 볼 수 있음

□ 권리남용에 대한 제재 부재

- 저작권법은 ‘정당한 권리 없이’ 차단 또는 재개 요청을 하는 경우 손해배상책임을 지도록 하여 권리남용을 막는 안전장치를 두고 있음.
- ※ 실제로 참여연대는 지난 2009년 가수 손담비의 노래 ‘미쳤어’를 따라 부른 5살 여아의 동영상에 대해 불합리한 차단요청을 한 한국음악 저작권협회에 대해 소송을 제기하여 2010년 10월 고등법원에서 손해배상판결을 얻은 바 있음(피고 항소포기로 확정, 2010나35260)

□ 국제적 흐름에의 역행

- 앞서 언급했듯 현행 저작권법 및 임시조치 제도의 모델이 된 미국 DMCA에 의하면 임시조치 규정은 의무부과조항이 아니라 면책조항으로 기능해야 함. 그래야만 사업자에게 과잉차단의 동기를 부여하는 문제를 해결할 수 있다는 것이 국제적 흐름.
- 즉 사업자가 차단요청-차단-복원요청-복원의 절차를 충실히 거칠 경우 불법정보유통에 대한 책임을 면책해줄 뿐 어떠한 차단 내지 모니터링 의무도 부과하지 않는 시스템이어야 함.
- 현재 현행법과 개정안 모두 특정 조건하에서 사업자가 의무를 부담한다는 내용이지 어떤 조건하에서 사업자가 면책된다는 내용은 없음. 물론 임의적 감면 조항이 있지만 이미 제44조의2 제1항, 제2항이 의무를 부과하고 있기 때문에 책임감면 조항은 의미가 없음.

다. 제안

(1) 불법정보에 대해서만 의무화되도록 변경

- 제1안: 헌법 제21조 제4항의 명령에 맞게 “권리가 침해된 경우”에만 임시조치 의무가 발생하도록 현행법 제44조의2 제1항의 문구를 유지
- 제2안: 개정안에서 임시조치를 “해야 한다”라고 되어 있는 것을 “할 수 있다”라고 수정하여 ‘합법정보의 차단 의무화’ 문제 해결

(2) 복원권의 실질화

- 복원권을 제대로 보장하기 위해서는 2회나 불복을 해야만 임시조치가 해제되어서는 안 되고, 첫 번째 불복(이의제기)시 임시조치가 우선 해제되어야 함(유승희 의원안 참조).
- ※ 두 번째 불복이 소제기를 통해서만 가능한 것도 과도하나 첫 이의제기만으로도 복원이 되어야 하므로 두 번째 불복의 요건에 대한 논의는 생략함

(3) 국제적 흐름과의 조화

- 나아가 국제적 흐름에 부합하기 위해서는 조항의 문구를 개정하여 현재와 같이 “삭제차단하여야 한다”는 의무부과형이 아니라 선진국의 경우와 같이 “~할 경우 책임이 면제된다”는 면책형으로 개편할 필요가 있음. 이는 저작권제도도 마찬가지임.

참 고 문 헌

- 국회입법조사처, 인터넷 분쟁과 임시조치 개선방안 토론회 자료,
2014. 12. 8.
- 김유향·심우민, 「정보통신망법」상 임시조치 규정에 대한 입법영
향분석, 현안보고서 Vol. 205, 국회입법조사처, 2013. 12. 18.
- 이재진·이정기, 인터넷 포털의 ‘임시차단’ 조치에 관한 탐색적 연구,
한국언론학보 56권 3호, 2012년 6월
- 박경신, 인터넷임시조치제도의 위헌성 - “남이 싫어하는 말은 30일
후에 하라”, 중앙법학 11집 3호, 2009년 11월
- 송백현, 정보통신망법상 정보에 대한 임시조치 및 행정규제에 관한
연구, 정보법학 제16권 제1호, 2009

한국의 통신감시 상황과 시민사회의 대응¹

박경신 손지원

(**미게재 논문이므로 인용하시려면 알려주세요.

그동안 게재되면 서지정보 알려드릴게요.)

2011년 한국에서는 7,167개의 전화번호에 대한 감청이 있었고, 약 37,300,000개의 통신 계정(전화번호, 이메일 주소 등)에 대한 통신사실확인²이 있었으며, 약 5,840,000명의 통신자료제공(통신사업자들을 통하여 특정 번호나 아이디의 이용자 신원 정보를 취득하는 것)이 있었다.³ 이것은 단 1년간의 수치이다.

인구수 대비로 따지면, 같은 기간 동안 한국의 감청 건수는 미국(2,732건⁴ 및 외국정보감시법원(Foreign Intelligence Surveillance Court)의 영장에 의한 1,789건⁵을 포함한 총 4,521건)의 약 9.5배이고, 일본(25건)⁶의 약 800배이다. 앞으로 살펴볼 바와 같이, 통신사실확인이나 통신자료제공과 같은 다른 통신 감시 수단의 비교에 있어서도 차이가 크다.

다른 선진국과 마찬가지로, 감청에 있어서는 법원의 승인을 요건으로 하는 법령⁷도 존재하고, 법원의 감청 영장 신청에 대한 기각율은 약 4%⁸로, 미국 법원의 기각율인 0.03%⁹보다 높음에도, 한국의 이러한 막대한 양의 통신감시 문제는 긴 해명을 필요로 한다. 본고는 대한민국에서의 국가의 사적 통신 감시 상황을 명확히 분석하기 위하여 작성되었으며, 또한 이에 대한 시민사회의 대응이 감시 행태에 어떠한 영향을 미쳤는지도 다룰 것이다.

I. 통신사실확인자료 : 한국형 프리즘(PRISM) ?

1. 3천7백만명 이란 숫자가 가능한 이유 : 기지국수사

통신사실확인자료의 취득을 위해서는 미국법과 마찬가지로¹⁰ '수사의 필요성'을 소명하는 신청서와 이에 대한 법원의 승인이 필요하다¹¹. 그러나 1년에 한국 총 인구의 반이 넘는 3천 7백만명의 사람들이 '수사의 필요성이 있는' 사람들이라는 결과가 어떻게 가능할까?

이러한 막대한 수치가 가능한 이유는, 한국 수사기관들이 신원을 알 수 없는 사람들의 모든 통신내역을 일단 대량으로 확보하고 이 데이터를 분석하여 그 중 수사대상을 식별하는, 이른바 '무작위 대량 감시'의 방식을 취하고 있기 때문이다.

'통신사실확인자료(통신내역)'란 미국의 수사용어 중 펜레지스터와 트랩앤트레이스(pen register/trap and trace)정보에 대응될 수 있는데, 송?수신된 특정 전화번호 혹은 IP 주소가 대표적이다.

한국의 수사기관은 특정한 전화번호의 송?수신 통신내역을 요청하는 대신, 특정한 '기지국'의 통신내역을 요청하여 해당 기지국과 교신한 모든 전화번호들을 취득한다. 실제 휴대폰간의 통

화가 이루어질 때가 아닌 슬립모드(Sleep Mode)로 기지국과 교신한 휴대폰 번호까지 모두 취득한다.

이것이 바로 통신사실확인자료 취득의 98.6%를 차지하는 '기지국수사' 방식이다. 수사대상을 구체적으로 특정한 후 그 대상의 통신내역을 확인한 횟수는 235,716번 뿐이다.¹² 나머지는 4,616개의 기지국을 수색하고, 각 기지국에서는 보통 약 7,8천개의 전화번호를 추출하게 되면서¹³ 3천 7백만개의 전화번호라는 어마어마한 결과가 나오게 되는 것이다.

2. 대량 감시의 위헌성

경찰이 이러한 기지국수사를 하는 이유는 무엇일까? 범죄 현장에 있었던 사람들을 심문하는 것이 피의자를 특정하는 유일한 방법인 경우가 있다. 이 경우, 경찰은 일단 해당 지역을 담당하는 기지국을 거친 (대도시 기지국의 경우 시간당 몇 천 건에 해당하는) 모든 휴대폰들의 번호를 취득한다. 그 다음 경찰이 이미 알고 있는 전화번호와 여러 번 통화했거나 현장에서의 통화내역으로 보아 그 근처에 장시간 체류한 것이 확인되거나 또는 범죄와 유관한 다른 기지국과도 교신한 것이 확인되는 등, 범죄와 관련 있는 통신이나 행위를 보인 사람의 전화번호들로 수사대상을 좁힌다.

일부 전문가들은 특정 기지국과의 교신했다는 정보는 그 기지국 근처에 통신자가 있었다는 정보와 등가이므로 기지국 수사를 통해 위치 정보가 취득되는 이상, 그 위치 정보의 정확도가 낮다고 하더라도, 위치정보는 통신의 내용처럼 강하게 보호되어야 할 성질의 것이어서 현재의 '수사의 필요성'과 같이 낮은 허가기준 하에서 이루어져서는 안되며 압수수색 영장 수준의 강화된 허가가 필요하다고 주장하기도 하나¹⁴, 이 논의까지는 깊이 들어가지 않겠다. 우리나라의 통신사실확인자료에 해당하는 펜레지스터/트랩엔트레이스가 낮은 허가기준 하에서 시행되는 이유는 우편물이 도달하기 위해 우편봉투 위에 주소가 쓰여져야 하는 것처럼 통신이 이루어지기 위해 통신사라는 제3자와 공유할 수 밖에 없는 최소한의 정보만을 취득하기 때문이다. 사실 미국연방대법원은 이러한 이유로 아예 법원허가 자체가 필요없다고 하였지만(소위 제3자공리, third party doctrine이다)¹⁵ 미국의회가 대법원이 요구하는 수준보다 기본권을 더 두텁게 보호하겠다는 취지로 낮은 단계의 법원허가를 의무화한 것이다. 우선 기지국도 통신기기이고 휴대폰도 통신기기인 이상 2개의 통신기기 사이의 통신사실을 확인하는 절차는 틀림없이 '통신사실확인'에 포함되는 것은 사실이고 이를 통해 자연스럽게 대강의 위치정보가 도출될 수 있다는 사실만으로도 그 정보를 다른 통신사실확인자료와 다르게 다루기를 요구하면 IP주소나 유선전화번호국번과 같은 전형적인 통신사실확인자료를 통해 대강의 위치를 파악할 수 있는 상황에 대해서도 새로운 논의가 필요하다.

대기상태(sleep mode)의 교신은 '통신'이 아니므로 통신사실확인자료에 포함되지 않고 그러므로 그 기지국 교신정보는 통신사실확인에 의해 취득되어서는 안되고 압수수색영장에 의해 취득되어야 한다는 주장¹⁶도 있지만 이 역시 여기에서 깊이 다루지 않겠다. 위에서 말했듯이 미국의 펜레지스터/트랩엔트레이스 조항이 제3자 공리에 의해 아무런 법원허가 없이 취득될 수 있는 정보를 '통신'과 관련되었다는 이유로 조금이나마 보호하기 위한 것이었다면 '통신'과 관련되지 않은 sleep mode교신기록은 도리어 아무런 법원허가 없이 취득이 가능해야 한다는 논리도 성

립하기 때문이다.

이 글에서 직접 다루고자 하는 문제는, 비록 약한 기준 하에서 통신사실확인자료 취득이 승인될 수 있다고 할지라도, 경찰이 한 사람의 피의자를 확보하기 위해 범죄와 무관한 나머지 대다수의 사람들의 통신내역을 취득하는 것이 승인될 수 있는가이다. 대부분의 수사기법에 대해 우리가 안심하는 이유는 범죄자로 의심되는 몇 사람 외에는 통신사실확인자료 요청을 포함한 수사기법의 대상이 되지 않는다는 믿음 때문이다. 하지만 기지국 수사에서는 범죄와 전혀 무관한 사람들의 통신내역도 취득되고 이에 따라 경찰이 거의 모든 국민을 잠재적 범죄자로 취급하는 결과가 나타난다.. 피의자를 찾겠다는 수사기관의 의도와는 무관하게 수많은 사람들의 통신 행태가 수사기관에 드러나는 이상, 그 많은 사람들에게 대한 '침해'는 피의자 수준으로 일어나고 있는 것이다.

기지국 수사는 특정한 혐의 없이 단지 어느 장소에 있다는 이유만으로 그 장소에 있는 모든 사람들을 수색하는 '저인망 감시'로서 NSA의 무차별대량감시가 UN 인권고등판무관(Higher Commissioner on Human Rights) 및 테러 대응에 있어 기본권 및 인권의 보호 및 진흥에 관한 UN 특별보고관(Special Rapporteur on Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism)¹⁷에 의해 비난받는 것과 같은 이유로 비판되어야 한다. 또 유럽인권재판소에서 위헌으로 판단된 무작위 DNA 정보 수집 및 보관¹⁸ 등과 같은 이유에서 위헌적인 것이라 할 수 있다.

미국시민자유연맹(American Civil Liberties Union)은 2014년 미국 정부가 4시간 반 가량 뉴욕 맨하탄 지역에서 기지국 수사를 신청한 것에 대하여 참고인 보고서를 내면서, 다음과 같은 설득력 있는 논증을 한 바 있다¹⁹.

구체적 용의자가 아닌 다수인을 의도적으로 수사대상으로 삼는 것은, 수정 헌법 제4조와 본질적으로 부합하지 않으며, 역사적으로 오랜 기간 금지되어 온 '일반영장'을 되살리는 것이라는 우려를 낳게 한다. 정부가 대량의 기지국 통신 정보를 취득하도록 허용하는 것은, 곧 수정 헌법 제4조의 제안자들이 그토록 우려하고 비난했던 일반영장의 한 유형을 인정해주는 결과가 될 수 있다. 1965년의 *Stanford v. Texas* 사건(*Stanford v. Texas* 379 U.S. 476, 48182, 1965)을 보자. 항소심 판결에서 실시한 바와 같이 수사기관이 전자적 기록 정보를 조사하기 위한 폭넓은 권한을 요청하는 것은 전자 정보에 대한 모든 영장을 사실상 일반영장으로 만드는 것이고, 이는 곧 수정 헌법 4조를 무의미하게 만드는 심각한 위험을 창출한다. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (en banc) (per curiam); accord *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). 인근 주거지역에서 총기 사건이 신고되었다고 해도, 용의자를 찾기 위하여 여러 블록 반경에 있는 모든 주택들을 동의 없이 수색하는 것은 당연히 허용되지 않는다. 또한 타임스퀘어에서 일어난 절도 사건 때문에 브로드웨이에 있던 모든 사람들의 소지품을 검사하거나 가방을 수색하는 것은 허용되지 않는다. 이러한 저인망식 수색은 전자적 수단을 사용하여 수행되었다고 하여도 마찬가지로 허용될 수 없다. 용의자가, 알 수 없는 이메일 주소를 사용하여 특정일시에 범죄 관련성이 있을 것으로 추정되는 이메일을 보냈다는 정부의 주장만으로, 구글이나 야후 등에게 해당 날짜에 뉴욕시 내에 인터넷망을 통하여 발송된 모든 이메일 목록을 생성하도록 요청하는 권한을 인정할 수는 없는 것이다.

미국시민자유연맹(ACLU)의 이와 같은 주장에 대하여, 치안 판사 James C. Francis V는 다음과 같이 판결하였다²⁰.

나는 정부에게 다음 내용을 포함한 수정된 신청서를 제출하는 것을 요구하는 바이다. (1) 기록이 수집되는 데에 소요되는 기간에 대한 정당한 사유를 더욱 구체적으로 설시할 것, (2) 범죄와 무관한 제3자의 추출된 개인정보에 대한 처리방안을 설명하는 계획을 약속할 것. See *In re S.D. Tex. Application*, 930 F. Supp. 2d at 702 ("이와 같은 데이터를 취득하기 위해서는, 정부는 적어도 이와 같은 민감한 개인정보들의 처리방안을 설명하는 계획을 가지고 있어야 한다."); see also *In the Matters of the Search of Cellular Telephone Towers*, 945 F. Supp 2d 769, 771 (S.D. Tex. 2013) (기지국의 통신 기록에 대한 영장을 발부하나, 수사와 무관한 것으로 확인된 일부 혹은 전부의 원본 및 사본 기록은 기지국 서비스 제공자에게 반환되어야 한다.)

또 다른 치안 판사 Brian Owsley 역시, 범죄 전후 1시간씩 총 2시간의 기지국 수사 신청에 대하여 다음과 같이 판결하였다. ²¹

범죄와 무관한 제3자와 관련된 데이터들에 대해, 정부가 의도한 바가 무엇인지는 논의의 대상이 아니다. 한 건의 범죄 수사에서, 정부는 범죄와 무관한 179명의 성명, 휴대폰번호와 이용자 정보를 받았다.*United States v. Soto*, No. 3:09CR200 (D.Conn. May 18, 2010) (Memorandum in Support of Motion to Suppress). 비록 법원의 승인을 얻은 기지국 수사로 인하여 이와 같은 정보들이 어김없이 정부에 제공되는 결과로 이어진다고 하더라도, 정부가 이와 같은 정보를 얻기 위하여는 적어도 이러한 민감한 개인정보들의 처리방안을 설명하는 계획을 가지고 있어야 한다. 이러한 문제는 심리 절차부터 제기되었음에도, 정부는 지금까지 이에 대한 설명을 하지 않고 있다. 이렇게 정부가 기지국 수사 요청으로 인하여 정보가 공개된 결백한 이용자들의 수정 헌법 제4조상의 사생활의 자유에 관한 권리에 대하여 설명하지 않는 것은 영장청구 기각의 또 다른 이유가 된다.

대량 감시의 함정은, 그것이 범죄에 대한 수사는 될 수 있을지언정, '범죄자'에 대한 수사는 아니라는 것에 있다. 특히 NSA의 대량 감시는 특정 범죄에 대한 용의자를 찾기 위한 것도 아니었고, NSA가 알지도 못하는, 범죄를 저지를 수 있거나 저질렀을 수 있는 사람들을 찾기 위한 것이었다. 이러한 기준에 따르면 모든 사람들은 자연히 잠재적인 감시의 대상이 되는 것이다.

물론, 경찰이 취득한 통신기록이 '누구'의 것인지를 모르는 상황에서는, 이러한 통신기록 상의 프라이버시 보호이익은 그다지 크지 않다는 의견이 있을 수 있다. '누구'의 프라이버시가 침해되고 있는지 알지 못한다면, 프라이버시 침해가 발생하였다고 할 수 없는 게 사실이다. 그러나 뒤에서 논의할 바와 같이 다른 법률에서 행정당국이 이용자의 신원들을 매우 쉽게 파악할 수 있는 권한을 부여하고 있는 이상, 이러한 의견은 충분한 반론이 되지 못한다.

3. 미국과의 비교

2012년 미국의 연방정부 및 주 정부에서는 약 9,000건의 기지국수사가 이루어졌다.²² 2011년 한국에서는 4,616건의 기지국 수사가 있었고, 이는 위 2012년 미국과 비교하였을 때 인구수대비 약 3배 이상 높은 것이다.

하지만 통신사실확인이라는 수사기법의 본연은 기지국수사가 아니다. 본연의 통신사실확인자료 제공 요청은, 특정된 개인들을 대상으로 하며 보통 단일 기기/계정 단위에 송/수신된 통신기록을 확인한다. 전술하였듯이, 2011년 한국의 수사기관은 235,716건(각 건당 약1~3 개의 기기를 조사)의 통신사실확인을 수행하였다.

미국에서는, 한국의 통신사실확인자료에 해당하는 연방 정부기관의 펜 레지스터/기기 추적(pen register/trace and trap device)은 2011년 약 90,000건²³으로 나타나는데, 이는 NSA 및 기타 주 행정기관의 것과 과거의 (혹은 소급 적용되는) 송/수신 기록은 제외된 것이다. 더욱 믿을 만한 수치는 마키(Markey) 상원의원이 2012년, 2013년에 공개한 이동통신사들의 자체 보고서^{24,25}인데, 이를 통해 이동통신사들이 방대한 양의 통신사실확인자료 공개 명령을 받았음을 알 수 있다. 참고로 이 보고서들은 기지국수사 통계를 별도로 구분하고 있어 유용하다. AT&T의 2012년 보고서²⁶에서는, 정부로부터의 297,500건의 통신감시 요청 중 통신 내용에 대한 것과 이용자 신원 정보에 대한 것을 제외하고 총135,300건의 통신사실확인자료 제공 요청이 있었음을 확인할 수 있다. 버라이즌(Verizon)의 2012년 보고서²⁷에 따르면, 정부로부터의 270,000건의 통신감시 요청 중 통신 내용에 대한 것과 이용자 신원 정보에 대한 것을 제외하고 총 110,000건의 통신사실확인자료 제공 요청이 있었다고 한다. 스프린트(Sprint)의 경우 2012년 보고서²⁸상 통신사실확인자료에 해당하는 카테고리들을 합하면 약 148,000건 정도이다. T-Mobile(티모바일)의 보고서²⁹는, 2012년 총 297,350건의 통신 감시 요청이 있었고, 그 중 감청이 3,000건이라는 점만 적시되어 있어, 통신사실확인자료 제공 건수를 정확히 파악할 수 없다. T-Mobile에 대한 통신사실확인을 150,000건으로 가정하고, 이 주요 4사들의 이동통신사업 시장점유율이 90%인 점을 감안할 때(그림 1), 미국 전체의 통신사실확인자료 제공 요청 건수는 대략 500,000 ~ 600,000 건 정도로 추산할 수 있다.

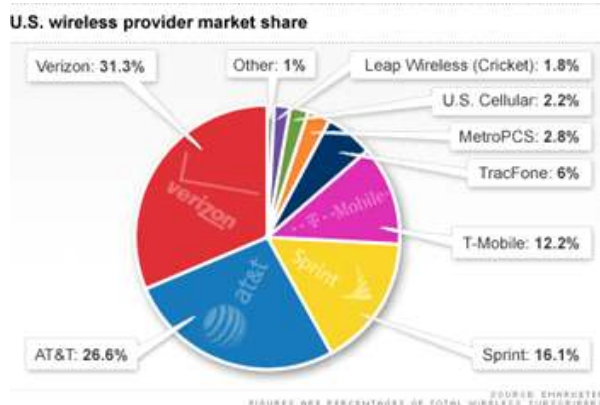


그림 1 . 2012년 미국의 이동통신사업 시장점유율

<http://money.cnn.com/2011/03/23/technology/sprint_verizon/>

요컨대, 2011년 한국의 통신사실확인자료 요청 건수는, 2012년 미국의 이동통신사업자들이 공

개한 수치와 비교하였을 때, 인구수대비로 2배 이상임을 알 수 있다. 이 미국 이동통신사업자들의 보고서는 구글과 같은 인터넷서비스제공자들의 수치를 포함하고 있지 않지만, 이들의 경우, 직접 일일이 내용을 검토하지 않고서는 통신사실과 같은 비내용적 데이터와 내용적 데이터를 구분하는 것은 기술적으로 어렵기 때문에, 통신사실확인자료에 대한 요청 건수는 미미한 편이다³⁰.

II. 통신자료제공

1. 영장 없는 통신자료제공

기지국수사의 합헌성을 주장하는 측의 논거 중 하나는, 통신자들의 통신내역이 그들의 신원이 확인되지 않은 상태에서 취득되기 때문이라는 것이다. 그러나 한국의 통신자료제공(특정 번호나 아이디 이용자의 신원 정보를 요청하여 취득하는 것) 건수는 연간 약 600만건(2011년 수치는 위 참조)인 점에서도 알 수 있듯, 한국은 수사기관이 매우 쉽게 통신자가 누구인지를 파악할 수 있다. 전기통신사업법 제83조 제3항³¹에 따라, 수사기관은 전기통신사업자들에게 팩스나 이메일을 간단히 보내기만 해도 통신자들의 신원을 알 수 있기 때문에, 수사기관은 '무작위 대량 감시는 우리도 누구의 통신내역을 취득하고 있는지 알 수 없기 때문에 프라이버시 침해라고 할 수 없다'고 주장할 수 없는 것이다.

통신자료제공 제도와 같이 정부기관이 이용자의 신원 정보를 제공·취득하는 것은, 사람들이 서로 익명으로 통신할 권리를 침해하기 때문에 그 자체로 프라이버시 침해라 할 수 있다. 인터넷에 무엇이든 게시한 사람은, 그의 신원을 수사기관에게 드러낸 것이고, 이는 곧 그들 스스로 탄압과 보복의 위험에 자신들을 노출시키게 되는 것이다.

현재 한국의 통신자료제공 중 90%는 전화 이용자에 대한 것(남은 10%는 웹사이트 ID 이용자)인데³², 전화 대화는 보통 서로 아는 사람들 사이에서 이루어지기 때문에 전화 대화에 있어 익명 통신의 자유를 논하는 것이 어색할 수 있다. 그러나 대화자들이 서로를 아는 것과, 대화자들의 신원 정보가 수사기관에게 알려진다는 것은 확실히 다른 문제이다. 통신자들은 수사기관이나 다른 제3자에 대하여 익명으로 통신할 권리가 있으며, 즉 이를 위하여는 각자가 통신하고 있는 사람을 제외한 어느 누구에게도 자신의 신원을 드러냄이 없이 통신할 수 있어야 한다.

그러나 한국을 주목해야 하는 이유는 바로 이 지나치게 많은 통신자료제공 건수라 할 수 있다. 미국은 정보통신서비스제공자들에게 발부된 행정명령을 집계하는 정보센터는 없지만, 미국의 주요 사업자들이 발간하기 시작한 '투명성보고서'를 통해 이용자 신원정보 제공요청 현황을 확인할 수 있다. 버라이즌(Verizon)의 투명성보고서는 2013년에, 행정명령에 의한 164,184건을 포함하여 총 320,000건의 이용자 정보 요청이 있었음을 나타내고 있다³³. 수사기관이 이용자 정보를 얻기 위하여 가장 간편한 절차를 이용하였을 것이라고 가정하면, 모든 행정명령이 이용자 정보 취득을 위하여 발부된 것으로 넉넉히 추론할 수 있다. (비록 이 중 몇 건의 요청이 거절되었는지는 알 수 없지만, 한국 기업들의 관행으로 추정컨대 대부분의 요청이 인용되었을 것으로 보인다) 버라이즌의 시장점유율이 대략 30%인 것을 감안하면³⁴, 미국 정부의 이용자 정보

요청의 연간 총수를 대략 500,000건으로 추산할 수 있다. (Verizon(135,000건)과 AT&T(129,300)만이 이용자 신원 정보 건수를 따로 제공하고 있기 때문에, 통신사실확인자료 수치를 계산하였던 것처럼 Markey 상원의원의 2012년 보고서상의 수치를 합산하여 이를 계산하는 것은 무리가 있다. 그러나 이들의 시장점유율을 합하면 대략 60%인 것을 감안하여 추산하면, 2012년에는 미국 전체 약 400,000건의 이용자 정보 제공 요청이 있었던 것으로 볼 수 있다.) 지금까지의 위 수치들은 망 서비스 사업자에 대한 것만 계산한 것이고, 구글과 같은 포털 등 인터넷서비스사업자들도 이용자 신원정보 제공 요청을 받기 때문에 별도의 계산이 필요하다.

구글의 2013년 투명성보고서³⁵에 따르면, 동년도 약 27,000건의 행정명령이 있었고, 이 중 84%가 인용되었다. 구글이 이메일 시장에서 약 20%의 시장점유율³⁶을 가지고 있음을 감안할 때, 미국 정부의 인터넷서비스사업자에 대한 이용자 정보 제공 요청은 연간 약 100,000건으로 추산할 수 있고, 망 사업자들에 대한 것을 합산하면, 총 600,000여건의 이용자 정보 제공 요청이 있는 것으로 볼 수 있다.

결론적으로, 한국의 수사기관이 통신자료제공 제도로써 2011년 영장없이 취득한 이용자 정보는, 2012년 미국의 수치와 비교하였을 때 절대량으로도 10배 이상 많고, 인구수대비로 따지면 60배가 넘는 수준인 것이다.

2. 영장을 필요로 하지 않는 통신자료제공 제도의 위헌성

국제 사정도 그다지 좋지는 않다. 미국법도 우리와 크게 다르지 않을뿐더러, 통신서비스제공자들에게 영장 없이도 이용자의 정보를 제공할 것을 (단순히 허용하는 것을 넘어) 명하고 있거나, 행정명령의 경우 과거의 발신기록도 포함하고 있어³⁷ 오히려 더 열악하다고 평가할 수도 있다. 영국³⁸, 독일³⁹, 프랑스⁴⁰ 역시 이용자 정보 취득에 영장을 요구하지 않고 있다.

그러나 시류는 변하고 있다. Jeffrey Skopek 교수는 관련 논문에서 프라이버시 보호 규범으로서 '익명성에 대한 합리적 기대' 개념을 주창⁴¹하였고, 이는 통신자료제공과 같은 이용자 정보 제공 제도에 잘 적용되는 것이라 생각한다.

'개인 정보'의 기밀성을 유지할 수 있도록 하는 우리 사회의 구조적 기능은, 단순히 그 정보를 숨기는 것에 국한되지 않고 그 정보로써 개인을 식별할 수 있도록 만드는 요소들을 숨기는 것도 포함될 수 있다. 온라인에서 일정 행위가 있었다면, 이와 관련된 요소들은 행위자가 가명을 사용하였는지, 그 가명이 IP 주소와 같은 다른 요소들과 연결되어 있는지, 그리고 그 IP 주소가 행위자의 실명과 연결되어 있는지가 될 것이다.

2014년 4월, 캐나다 대법원은, 행정당국이 이용자 정보에 접근하는 것을 허용하고 있는 정보보호법에 따라 행하여진 경찰의 이용자 정보 취득을 위법이라고 판단하며⁴² 다음과 같이 판시하였다.

인터넷 이용의 맥락에서 특히 중요한 것은 프라이버시를 '익명성'으로 이해하는 것이다. 이용자

의 인터넷 활동과 연결되는 이용자 정보는, 개인의 성명, 주소, 전화번호보다 더욱 고양된 프라이버시 보호법익이 있는 것으로 인식되어야 한다. 이용자(가입자) 정보는, 개인을 식별할 수 있는 특정 정보와 주로 연결되고, 이는 그 정보의 출처, 소유자, 이용자로서 개인의 신원과 관련된 프라이버시 법익에 영향을 끼친다. 일정 수준의 익명성은 인터넷 활동의 특색이며, 모든 사정을 고려하였을 때 익명성은 부당한 압수·수색으로부터 헌법적으로 보호되는 프라이버시권의 근간이다. 이 사건에서, 경찰이 특정 IP 주소의 가입자(이용자) 정보를 요청한 것은, 사실상 특정한 온라인상 행위와 관련있는 특정인물이 누구인지 공개하라는 요청과 다름없다.

이러한 요청은, 이용자가 온라인에서 익명으로 행한 행위들(다른 환경에서도 중요한 프라이버시 법익 문제를 이끌어낼 수 있는 행위들일 것이다)과 용의자를 연결하려는 시도로서, 프라이버시 법익에 있어 익명성의 문제를 불러 일으킨다. 이러한 정보의 공개는, 익명성의 기대를 가지고 내밀하거나 민감한 온라인 활동을 행한 이용자의 신원을 식별할 수 있게 할 것이다. 경찰의 요청은 ISP가 이러한 정보를 자발적으로 공개하여 달라는 것이지만, 결과적으로 수색으로 이어진다.

3. 시민사회의 대응과 최근의 변화

시민사회는 이에 대항하였다. 참여연대 공익법센터⁴³는 위 전기통신사업법 제83조 제3항에 대하여 헌법상 영장주의 원칙 위반을 이유로 헌법소원을 제기하였다. 헌법재판소는 2012년 8월, 해당 조항은 단지 전기통신사업자들에게 해당 정보의 공개를 허용하고 있을 뿐 어떠한 의무를 부과하고 있는 것으로 볼 수 없고, 통신자료제공은 '통신사업자들의 자발적인 행위'로서, 이에 국가의 강제적 공권력 행사가 개입되어 있는 것으로 볼 수 없다는 취지로 이를 기각하였다⁴⁴. 국가후견주의적 성격이 강한 한국의 통치구조에서 행정당국의 포털들에 대한 사실상의 지배력을 생각할 때, 이는 매우 비현실적인 판단이라 할 수 있다. 또 같은 날, 헌법재판소는 참여연대 공익법센터와 진보넷이 제기한 다른 헌법소원에서 주요 웹사이트에 게시하기 위해서는 게시자가 반드시 신원정보를 사이트운영자에게 등록하도록 한 소위 인터넷실명제에 대해 위헌결정을 내려 통신자료제공제도의 물적 토대를 구성하는 신원정보데이터베이스의 생성가능성 자체를 감소시켰다. 또 위헌결정의 이유로도 수사기관에게 이용자의 신원정보를 제공하는 것은 제공 목적외의 사용으로서 개인정보자기결정권 침해에 해당하고 실명제가 이런 침해를 조장한다는 점을 들었는데 통신자료제공제도가 문제가 있음을 지적한 것으로서 사업자 상대 소송의 논리를 제공한 셈이 되었다.

통신자료제공이 '임의적인' 것이어서 국가책임이 없다는 위 결정이 나오자, 참여연대 공익법센터는 즉각 대표적인 문제 사건을 찾아 한국의 가장 큰 포털사인 '네이버'를 상대로 이러한 '자발적인' 공개를 한 것에 대한 손해배상청구를 제기하였다.

이 사건은, 어떤 네티즌이 그의 네이버 블로그에, 당시 문화체육부장관 유인촌이 피겨 스타 김연아의 우승을 축하하기 위한 공식석상에서 김연아를 포옹하기 위해 다가갔으나 김연아가 회피하는 모습이 담긴 유튜브 동영상⁴⁵을 게시하였는데, 보수적인 정치인으로부터 압력을 받은 경찰이 해당 네티즌을 명예훼손 혐의로 수사·소환한 사건이다.⁴⁶

이 사건에서 경찰이 해당 네티즌의 신원정보를 얻고 접촉할 수 있었던 것은, 위 법률 조항에 의하여 네이버로부터 통신자료제공을 받았기 때문이었다. 1심 패소 후, 항소심(서울고등법원)에서는 네이버가 해당 네티즌에게 50만원의 손해를 배상하라는 판결을 받아 승소하였는데, 주요

판시사항은 다음과 같다. 47

피고(포털)는 이용약관에서 정한 바에 따라, 회원의 개인정보를 보호하기 위해 노력하여야 하고, 이용자의 사전 동의 없이는 원칙적으로 이용자의 개인정보를 외부에 공개하지 않아야 할 의무가 있는 점

피고의 '개인정보 취급방침(이용약관)'에는 개인정보를 외부에 공개하지 않는 원칙의 예외로 법령의 규정에 의하거나 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 '요구'가 있는 경우라고 기재되어 있다

(그러나) 이용약관에 구 전기통신사업법을 근거로 수사기관의 '요청'이 있기만 하면 언제나 예외 없이 이용자의 인적사항 일체를 수사기관에 제공한다는 내용이 포함되어 있다고 해석할 수 없을 뿐만 아니라 경찰이 개인정보 제공을 요청하면서 '요청사유 및 가입자와의 연관성'란에 단지 '명예훼손 및 용의자 수사'라고만 기재하고

수사기관의 개인정보 제공 요청에 대해 피고가 사법기관에 준하는 엄격한 심사를 하여야 하는 것은 아니라 할지라도 앞서 본 바와 같이 피고는 전기통신사업자이자 인터넷 종합 정보제공 사업자로서 그 제공 역무의 성격 등으로 인해 상당한 공공성을 갖는다고 보아야 하는 점, 이 사건 카페 등의 커뮤니티 서비스는 익명표현의 자유를 그 본질적 요소로 하는 것이어서 수사기관의 개인정보 제공 요청에 대해 피고는 일반 사인과는 달리 적절한 자기통제 장치를 마련하고 있어야 할 것인 점 등에 비추어 보면, 피고는 적어도 이용자의 개인정보를 실질적으로 보호할 수 있는 역량을 갖추고, 침해되는 법익 상호간의 이익 형량을 통한 위법성의 정도, 사안의 중대성과 긴급성 등을 종합적으로 고려하여 개인정보를 제공할 것인지 여부 및 어느 범위까지 제공할 것인지에 관해 충분히 심사를 하여야 할 의무가 있다.

이 사건은 비록 피고가 즉각적으로 상고하여 지금까지 대법원에 계류 중이지만, 이 판결은 커다란 반향을 불러일으켰다. 전술하였듯이, 포털의 통신자료제공은 전체 통신자료제공의 10% 정도로 연간 약 500,000~600,000 건이었다. 각 건별로 50만원씩의 손해배상책임이 있다고 가정하면, 인터넷 포털사들은 천문학적 액수를 손해배상액으로 지급하여야 할 위기에 직면하게 된다. 즉각적으로, 네이버를 포함한 모든 주요 포털사들과 인터넷 콘텐츠 및 어플리케이션 서비스 제공자들은 다 함께 전기통신사업법 제83조 제3항에 의한 통신자료제공 요청에 더 이상 응하지 않겠다고 발표하였다⁴⁸. 그러나 통신자료제공의 90%를 차지하는 망 사업자들의 움직임에는 이 논문이 출간되는 현재까지도 변화가 없다. 도리어 통신자료제공 여부를 묻는 이용자에게도 답하지 않아 새로운 논란을 불러 일으켰는데 이에 대해서는 아래에 설시한다.

III. 감시 범위의 과잉

관련 법제는 미국과 거의 유사함에도, 인구수대비를 감안하였을 때 한국의 통신자료제공 건수는 미국의 약 60배, 감청은 미국의 9.5배, 통신사실확인인 미국의 최소 2배 이상 많다. 기지국 수사의 숫자도 3배 가량 많았다. 이메일 압수수색의 경우, 한국 혹은 다른 나라에도 정확한 데이터는 찾을 수 없으나⁴⁹, 단순 수치보다는 각 감시 건의 '범위'가 더욱 주요한 문제가 되고 있다.

이메일과 같은 저장된 정보에 대한 압수수색의 경우, 다음과 같은 사례들이 있었다. 검찰은 2007년 7월 치뤄진 서울시 교육감 선거 당시 주경복 교육감 후보의 정치자금법 위반 사건 관련자 100여명을 수사하였는데, 두 달 가량의 선거에 관한 수사를 위하여 관련자들의 7년 치 이메일을 압수하여 확인하였다⁵⁰. 또, PD수첩의 광우병보도에 대한 명예훼손 형사재판을 위하여 제작진들의 7개월치 이메일이 압수수색되었고⁵¹, 이명박 정부 당시 YTN 노조가 친정부 성향의 사장 선임에 반대하며 벌인 파업에 관한 수사에서 노조 간부 20여명의 9개월치의 이메일이 압수된 적도 있었다⁵².

2009년 초 집중적으로 발생한 이러한 사례들은, 한국 인터넷 이용자들이 국내 서비스를 떠나 이메일과 같이 한국의 영장 집행의 효력이 미치지 않는 외국 서비스로 이동하는 '사이버 망명' 현상⁵³을 초래하였다. 사이버 망명은, 유튜브의 한국서비스 창고 업로드 권한을 없애겠다는 2009년 4월 구글의 결정에 따라 가속화되었다. 이 결정은 실명 하에서만 업로드를 허용하는 당시의 국내 인터넷 실명제에 대한 항의의 표현이었으며, 이용자들이 하여금 국내 이메일 서비스는 가입시 이용자들의 실명과 주민등록번호를 제공받고 있어 이용자의 이메일이 추적당하기가 쉽다는 사실을 각성시키는 계기가 되었다⁵⁴.

또한 위 첫 번째 사례에 대하여, 참여연대 공익법센터는 검찰 스스로 영장 범위를 '선거 운동과 관련된 정보'로 한정하였음에도, 7년치의 이메일을 압수수색하여 영장 집행 범위를 유월한 점에 대하여 검찰을 상대로 국가배상소송을 제기하였고, 700만원을 배상하라는 판결을 받아 승소하였다⁵⁵. 법원은 '선거 범죄 혐의와 관련된 이메일을 압수하려면 기간은 선거일로부터 몇 개월 전이거나 길어도 1년을 넘지 않는 날까지로 봐야 한다'고 판단하였다.

감청의 경우, 2010년 진보넷은 검찰이 국가보안법 위반 혐의 수사를 위하여 감청 영장을 14회 연속으로 연장(각 연장 기간은 2개월씩, 총 감청기간 30개월)한 행위와 근거 조항에 대하여 헌법소원을 제기하였다. 국제적으로 전례가 없는 이 사건에서, 헌법재판소는 총 기간과 연장 횟수에 아무런 제한이 없이 감청 영장의 연장을 허용하고 있는 본 조항⁵⁶(이러한 연장에 대한 제한을 규정하고 있지 않은 미국의 ECPA와 유사한 조항⁵⁷)에 대하여 위헌을 선언하였다. 판결 이유는 더욱 놀랍다. '법원이 감청 기간의 연장이 남용되는 것을 통제하는 것은 일정한 한계가 있기 때문에, 남용을 막을 수 있는 최소한의 한계를 설정할 필요가 있다'는 것이었는데, 법원의 통제가 왜 곤란한지에 대하여는 설명하지 않았다. 비록 결과는 고무적이었지만, 이러한 법원의 절망적 고백은 더욱 우려스러운 부분이 아닐 수 없다.

우리는 여기서, 법원이 무력하게 자신들의 권한 행사에 있어 입법자가 지침을 제공해주기를 바라면서, 열악한 통지 제도로 인하여 광범위한 감시 행태에 대한 명확한 문제의식의 부족을 드러내는 한편, 이러한 감시의 대량화·장기화에 대하여 대응하여야 할 책임 역시 통감하고 있음을 알 수 있다.

물론 한 가지 고무적인 면은 압수수색에 있어서는 2011년에 형사소송법이 개정되어 ‘범죄와 관련된 것’에 한해서만 압수와 수색이 이루어지도록 제한규정(106조와 109조)이 만들어졌다. 이에 따라 수사기관이 정보의 내용을 인지한 이후에 범죄와 무관한 것들은 압수(즉 복사)에서는 배제해야 한다. 하지만 수색은 그 자체가 정보의 내용을 인지하는 행위인데 애시당초 정보의 내용을 인지하지 않고는 범죄관련성을 판단하기가 불가능하기 때문에 수색을 처음부터 제한한다는 것이 논리적으로 불가능하다. 프라이버시의 침해는 이미 정보의 내용을 인지하는 시점에서 발생하기 때문에 해법이 필요하다.⁵⁸ 요컨대 수사기관이 정보의 내용을 인지하기 전에 수색의 범위를 줄일 수 있는 방안이 필요하다. 이미 2011년 형소법개정에서 전기통신에 대한 압수수색 영장에는 ‘작성기간’을 한정하도록 한 것이 그런 해법이 될 수도 있겠다. 하지만 해당 작성기간 내에도 범죄와 무관한 정보가 상당히 많이 있을 수 있다. 국내에 소개된 Tamura-Carey⁵⁹ 방식은 단지 정보저장매체의 정보를 수색할 때 수색의 목적이었던 범죄와는 무관하되 다른 범죄와 유관한 정보를 보았을 때 그 정보를 그 새로운 범죄와 이용하기에 필요한 절차만을 규정한 것으로서 ‘압수’단계에만 영향을 줄 수 있다. 또 시민단체들이 말하는 피의자 입회⁶⁰ 역시 수색 자체를 한정할 수는 없다. 수사기관이 아닌 중립적인 제3자가 정보의 내용을 훑어보고 그 중 수사와 관련된 것만을 수사기관에 전달하는 코진스키 방식이 유일하게 그러한 해법이긴 한데 이 또한 여러 문제점이 있어 계속 고민이 필요하다.⁶¹ 사실 이 부분에 있어서는 세계적으로 해법이 나와 있지 않아 도리어 한국의 논의가 도움이 될 수도 있다.

하지만 2014년 10월의 카톡망명사태에서 보여지듯이 수사기관은 ‘압수’를 범죄와 관련된 것으로 한정하는 것에도 상당히 어려움을 겪고 있는 것으로 보인다.⁶² ‘범죄와 관련된 것’만 압수할 수 있도록 정한 형소법 제106조를 위반하여 정보의 압수(복사)가 이루어진 경우에 대해서는 손해배상이 이루어져야 할 것이다.

IV. 이용자에 대한 통지

헌법상 적법절차원칙 하에서는 국가가 사인의 권리를 침해할 때는, 그것이 감시이건 다른 행위이건 간에, 최소한 해당 개인에게 국가가 어떠한 행위를 하고 있는지에 대하여 알려주어야 한다.⁶³ 경찰이 압수영장을 가지고 있다고 해서, 그것이 곧 영장이 은밀하게 집행될 수 있다거나 증거를 훔칠 수 있는 것은 아니다. 수색대상자는 당연히 자신의 영역이 수색 당하고 있다는 사실을 알아야 한다. 한국의 감시 관련 법제는 전반적으로 감시 대상인 이용자에 대한 통지에 관하여 매우 열악하게 규정하고 있다.

1. 감청과 통신사실확인 통지 : 기소 후 30일 ?

한국의 감청과 통신사실확인 규정도 미국법과 같이 수사대상자에 대한 통지를 요구하고 있으나, 공소의 제기 또는 입건을 하지 아니하는 처분을 한 날부터 30일 이내에 통지하도록 규정되어 있다.⁶⁴ (일본의 경우 감청행위의 종료 후 30일 이내에⁶⁵, 미국 역시 감청 행위 종료 후 90일 이내⁶⁶에 대상자에 대하여 통지하여 줄 것을 규정하고 있다.)⁶⁷

예를 들어, 수사가 계속 진행되어 왔고 2년 후에야 기소 여부가 결정되었다면, 수사대상자는 2년 동안 자신에게 어떠한 일이 벌어지고 있었는지 전혀 모른 채 살 수 밖에 없다는 것이다. 2년이 지나 감시 사실이 통지가 된다고 하더라도, 불기소로 결정된 사람들은 이미 오래 전에 벌어졌던 일에 대하여 크게 문제삼고 싶어하지 않을 가능성이 크다. 또한 기소가 결정된 사람들 대부분은 기소된 이후, 보통 검사가 형사재판에서 감청 속기록을 증거로 제시한 때에 비

로소 자신이 감청당했었다는 사실을 알게 된다. 그러나 그 때는 이미 피고인으로서 유?무죄 여부의 다툼에 집중하게 될 것이기 때문에, 사생활 침해는 그다지 중요한 문제가 아니다. 이것이 바로 정의의 집행이 지연되는 것은 정의가 거부되는 것과 같다는 명제를 뒷받침하는 사례일 것이다.

더 문제인 것은, 이러한 통지마저도 법원이 아닌 '검사장'의 결정으로 유예가 될 수 있다는 것⁶⁸인데, 이는 명백한 영장주의의 위반이라 할 수 있다.

더욱이 통지가 기소결정, 불기소결정 등을 조건으로 이루어진다면 아예 기소, 불기소결정 또는 불입건결정 자체가 이루어지지 않은 사람들은 언제 통지를 받게 되는가? 우선 그런 유형의 사람들로 기지국수사에 의해 자신의 통신사실확인자료가 수사기관에 의해 취득된 사람들이 있을 수 있다. 즉 처음부터 수사대상이 아니었는데 자신이 근처에 갔던 기지국에 대해 기지국수사가 진행되면서 통신사실확인을 당한 사람의 경우 아예 통지를 받지 않는 것으로 보인다. 그렇기 때문에 2011년처럼 3천7백만명이나 통신사실확인을 당해도 주변에 이를 통지받은 사람이 없는 것이다. 또 2014년 정청래의원의 발료자료⁶⁹를 보면 기지국수사 대상은 아니지만 개별수사대상이면서도 오랜 시간 수사가 이루어지면서 수사기관들이 통지의무가 있음을 망각하는 경우가 많아 조사기간 동안 34.8% 만이 통지가 되었다고 한다.

2. 이메일 이용자에 대한 통지⁷⁰

이메일에 대한 일반 압수수색에서 통지의 결여 문제는 더욱 극심하다. 현재, 송수신이 완료된 전기통신에 대한 압수수색의 통지는 감청(통신제한조치)의 규정(기소 여부 결정 후 30일 이내)과 유사하게 규정되어 있다.⁷¹

그러나 형사소송법상 일반 압수수색의 절차는 매우 엄격하여, 피의자는 압수수색 영장 집행 '전'에 통지를 받도록 규정⁷²되어 있는데, 이메일 압수수색의 경우에만 이렇게 예외적으로 통지가 지연되는 것은 정당화될 수 없다. 감청의 경우 통지를 사후에 하는 것은 통신의 내용이 보통 저장되지 않아 수사기관이 실시간으로 해당 내용을 청취할 필요가 있다는 면에서 정당화 될 수 있다. 이런 상황에서는 통신 당사자들이 자신들이 감청당하고 있다는 사실을 알게 된다면, 감청수사의 목적 자체를 달성할 수 없기 때문이다. 그러나 이러한 정당화 사유는 이메일과 같이 저장된 통신에 대한 수사에는 적용될 수 없다⁷³⁷⁴. 이에 대한 압수는 노트북에 대한 압수시 현장에서 즉시 영장이 제시되어야 하는 것과 다를 바 없이, 가능한 빨리 이메일 계정의 주인에게 통지되어야 하는 것이다.

그러나 기소 여부 결정 후로 통지가 지연됨에 따라, 피압수자들은 보통 형사재판에서 검사가 증거로서 이메일 내용을 제시할 때에야 비로소 자신의 이메일이 압수되었다는 사실을 알게 되는 경우가 많다. 그러나 법원은 2010년 10월 참여연대 공익법센터가 제기한 관련 소송⁷⁵에서, 이메일 압수수색의 경우, 이를 통지 받은 사람들이 이메일을 삭제하는 등으로 증거를 인멸할 가능성이 있으므로 사전 통지 의무의 예외로서 '긴급한 경우'에 해당한다는 취지로 판시하며, 이러한 통지의 지연 관행을 승인하였다.⁷⁶

이러한 판단은, 기술적으로 확고한 사실, 즉 이메일 계정 내의 이메일들을 삭제하는 것은 단지

해당 계정과 이메일 데이터 사이의 연결을 차단하는 것일 뿐, 이메일 데이터는 서버 하드 디스크의 용량을 초과하지 않는 선에서 무기한 서버에 남아있다는 사실을 간과한 것이다. 또한 법규상 영장집행 전에만 통지를 하면 되므로, 수사기관이 이메일 서비스 제공자들에게 용의자의 이메일 계정 접근을 차단하도록 요청하는 등의 선제적 조치를 취한 후, 적절한 통지와 영장집행을 하도록 할 수 있는데, 이러한 가능한 방법들을 간과한 것이다.

또한 이 판결은 국가인권위원회가 2010년 8월 19일에 발표한 '이메일 압수수색의 경우 특히 사전 통지가 요구되며, 사후 통지는 예외적인 상황하에서만 허용된다'는 내용의 개선안⁷⁷에도 위배된다. 이러한 노력의 결과로, 2011년 7월, 정보저장장치에 대한 압수의 경우 '정보주체'에게 즉시 통지하도록 하는 내용으로 관련법이 개정⁷⁸되었다. 그러나, 본 조항은 장치/기기 그 자체를 대상으로 한 압수수색에만 적용되고 있고, 특정 이메일 계정을 대상으로 한 이메일 압수수색에는 적용되지 않고 있는데, 이는 기술적으로 더 이상 통용되지 않는 구분임에도, 이메일 계정 이용자는 여전히 압수수색의 통지를 받지 못하고 있다⁷⁹.

3. 통신자료제공에 대하여 이용자가 알 권리

통신자료제공의 경우, 헌법재판소가 판단하였듯, 공식적으로는 사업자들이 '자발적으로' 제공하는 것이기 때문에 정부의 통지가 요구되지 않는다. 그렇다면, 자발적으로 이를 제공하는 서비스사업자들은 해당 이용자에게 대하여 통지를 하고 있을까?

정부의 책임하에 이루어지는 감청이나 통신사실확인자료 제공의 경우에는 통지 역시 정부가 스스로 관리, 통제할 필요가 있으므로, 서비스사업자들의 자체적인 통지는 금지되는 것이 당연하다⁸⁰. 하지만 서비스제공자의 '자발적인' 통신자료제공은 국가가 시행하는 것이 아니므로 이러한 고객통지금지규정이 필요하지 않아 고로 존재하지 않는다. 그런데 한국의 서비스제공자들이 이러한 금지 규정이 없음에도 불구하고 자신의 고객들에게 그들의 이용자 정보가 제공되었는지를 알려주지 않고 있다.

포털이 통신자료제공 요청에 따른 것에 대하여 사업자책임을 인정한 2012년 10월 서울고등법원 판결에 대하여, 2011년 기준으로 6백만건 중 90%의 상당하는 통신자료제공을 행한 망사업자들(telecom)은 인터넷회사들과는 전혀 다른 반응을 보였다. 망사업자들은 계속 전기통신사업법상의 통신자료제공에 응할 것이라고 밝혔다. 천문학적 수준의 배상책임을 질 수 있는 위험이 있음에도, 이렇게 자신감을 보이는 이유는 무엇일까? 자신의 정보에 대하여 전기통신사업법상의 통신자료제공이 있었는지를 알려달라는 고객의 문의에 대하여 망사업자는 이를 거절하였다. 이는 사람들이 자신이 피해자인지 알지 못하는 이상, 피해자들은 소송을 제기할 수 없다는 것을 이용한 것이다. 이에 따라 2013년 4월, 참여연대 공익법센터는 망사업자들이 전기통신사업법상 통신자료제공 제도에 의하여 수사기관에 이용자 정보를 제공한 내역을 공개하도록 하는 내용의 소송을 제기하였고⁸¹, 2015년1월에 고등법원에서 승소 판결을 받아 각 통신사들이 통신자료제공 내역을 고객에게 공개하지 않은 행위에 대해 각각 20-30만원의 손해배상이 선고되었다.

지금 논의하고 있는 것은, 더 이상 '통지'라고도 볼 수 없는, '문의에 따른 공개'이다. 사람이

자신의 개인 정보의 보안 상태에 대하여 알 권리는, 일반적인 정보공개 원칙에 따라, 자신의 통장 잔고를 확인할 권리와 다를 바 없이 강하게 보호되어야 하는 권리이다. 주요 포털들은 자신들의 정보가 수사기관에게 제공되었는지를 묻는 고객의 문의에 대하여 이를 공개한 바 있다. 그러나 포털과 망사업자들 어느 누구도 아직 통신자료제공을 고객에게 자발적으로 통지하겠다는 정책을 내놓지는 않고 있다.

사업자로서 이용자의 권리를 보호할 유일한 방법은 이러한 정책을 자체적으로 도입하는 것이며, 법원이 통신자료제공을 자발적인 것으로 보는 이상 이는 매우 중요한 문제라 할 수 있다.

4. 이용자 통지의 중요성

한국의 통신감시의 특수한 양과 범위를 보면, 우리는 판사와 검사들이 감청과 통신사실확인을 신청하고 승인하는 데에 별다른 문제의식을 느끼지 않고 있다고 결론지을 수 있다. 그리고 이러한 사고방식은 영장 없이 통신자료제공 요청을 할 수 있는 행정기관에도 만연해있다. 이러한 사고 방식의 이유 중 하나는, 아마도 사회 전체적으로 감시의 규모와 위험성에 대한 인식이 결여되어 있기 때문일 것이다. 대부분의 감시는 밀행적이기 때문에, 이는 감시의 고유하고 필연적인 문제라 할 수 있다. 일반 대중들이 그들이 감시 당하고 있는지를 알지 못한다면, 당연히 감시의 공포를 표현하거나 전달할 수 없고, 이를 승인하는 판사들 역시 사람들을 감시하에 두는 것이 어떤 의미인지 깨닫지 못하기 때문에 이용자의 프라이버시 법익을 신중히 고려하지 않을 가능성이 높다.

이러한 인식 부족을 해결하기 위한 방법 중 하나는 정부와 사업자 양측 모두 '투명성보고서'를 발간하는 것이고, 또 다른 하나는 이용자에 대한 통지 의무를 강화하는 것이다. 감시 대상자수는 어마어마함에도 열악한 통지 규정으로 인하여 사실상 극소수의 사람만이 이러한 통지를 받고 있다. 예로, 2011년 이루어진 기지국수사로 통신내역이 파악된 3천7백만명의 사람 중 어느 누구도 통지를 받지 못하였다. 통지의 결여는 영장을 발부하는 판사들의 도덕적 해이를 낳는다. 아마도 판사들의 가까운 지인들이나 가족들이 광범위한 압수수색이나 감청을 당하여, 감시 하에 놓여지는 것이 어떤 느낌인지에 대하여 '현실적 깨달음'을 얻기 전까지는, 이에 대한 판사들의 태도는 변하기 힘들 것이다.

V. 결론

한국의 통신감시는 양과 범위, 두 가지 측면에서 모두 우려스럽다. 인구수대비로, 통신자료제공(이용자 신원 정보 취득) 건수는 미국의 약 60배, 감청은 9.5배, 통신사실확인자료(개별 대상에 대한 비내용적 통신내역 정보) 취득은 최소 2배 이상이며, 기지국 수사는 약 3배 정도 많았다. 교육감 선거 관련 수사를 위하여 7년치의 이메일을 압수수색한 사례, 영장을 14차례 연장하여 몇 년간이나 감청을 지속한 사례 등도 있었다. 특히 기지국 수사와 영장없는 통신자료제공은 한국의 광범위한 통신감시 행태를 가능케 한 대표적인 요인으로서, 이들의 합헌성은 엄중히 판단되어야 한다.

그러나, 영장없는 통신자료제공, 무작위 대량감시, 사업자들의 고객문의에 대한 대응, 압수수색의 범위를 한정하는 기법, 인터넷실명제 평가 등에 있어서는 한국의 입법례와 판례들은 미국 등 외국에서의 논의와 상호 긍정적인 영향을 주고 받을 수 있다.

한국의 통신감시 문제를 더욱 특수하게 만드는 것은, 감시 대상자에 대한 통지의 결여 문제, 즉, 통지가 '기소 여부가 결정된 후 30일'까지 지연되어 그 의미를 상실하고 있으며, 통신자료 제공의 경우에는 전혀 통지가 이루어지지 않고 있다는 점이다. 통지의 결여는 수사의 필요성과 대상자의 프라이버시를 어떠한 기준으로 형량하여야 하는가에 대한 공공 담론을 불가능하게 하고, 사법부가 가진 감시를 통제할 수 있는 권능도 약화시킨다. 참여연대 공익법센터, 진보넷, 오픈넷 등 한국의 시민사회는, 이메일 압수수색, 통신자료제공, 감청 연장의 범위를 제한하고, 사람들이 자신의 정보가 수사기관에게 제공되었는지를 알거나 통지받을 권리를 보장하는 내용 등의 입법 운동을 진행하고 있으며, 일부 성과도 있지만 아직 갈 길이 멀다.

1
2 '통신사실확인자료'란 통신 내용이 아닌 통신 상대방의 전화번호, 통신 일시 및 시간 등의 통신내역정보를 의미한다.

3 <http://old.kcc.go.kr/user.do?mode=view&page=P0503>

35108

4 <http://www.uscourts.gov/Statistics/WiretapReports>

요약문 : <http://epic.org/privacy/wiretap/>

5 Issued under Foreign Intelligence Surveillance Act

http://epic.org/privacy/wiretap/stats/fisa_stats.

6 <http://www.asahi.com/articles/ASG263RKWG26UTIL00D>

7 **통신비밀보호법 제5조 (범죄수사를 위한 통신제한조치의 허가요건)**

? 통신제한조치는 다음 각호의 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가할 수 있다. <개정 1997.12.13., 2000.1.12., 2001.12.29., 2007.12.21., 2013.4.5., 2015.1.6.>

http://elaw.klri.re.kr/eng_service/lawPrint.do?hs

8 <http://www.mediatoday.co.kr/news/articleView.html>

9 Tim Cushing, US Courts' Wiretap Report Shows Wiretaps are for Drugs and Warrants are rejected only 0.03% of Times, July 7, 2014

<https://www.techdirt.com/articles/20140703/105021>

[taps-are-drugs-law-enforcement-warrants-rejected-](#)

10 18 U.S. Code 3123 (for prospective transactional data) and 18 U.S. Code 2703 (c), (d) (for stored information on the communications that already have taken place, which include 'retrospective' transactional data). The standards differ, depending on whether prospective (if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation) or retrospective (when the Government offers

specific and articulable facts showing that there are reasonable grounds to believe that the . . . records . . . sought are relevant and material to an ongoing criminal investigation.)

11 통신비밀보호법 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차)

? 검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다.

②제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다.

12 국가인권위원회 결정 '전기통신사업법 통신자료제공제도와 통신비밀보호법

통신사실확인자료제공제도 개선권고', 2014. 4. 9.

13 Id.

14 In the Matter of the Application of the UNITED STATES of America for an ORDER PURSUANT TO 18 U.S.C. 2703(D) Directing Providers to Provide Historical Cell Site Locations Records, **930 F.Supp.2d 698**(S.D. Tex. 2012); The Hon. Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. Pa. J. Const. L. 1, 1723 (2013).

15 Smith v. Maryland, 442 U.S. 735 (1979)

16

17 Office of the UN High Commissioner for Human Rights, A/HRC/27/37 The Right to Privacy in the Digital Age (June 30, 2014): Mass or bulk surveillance programmes may thus be deemed to be arbitrary, even if they serve a legitimate aim and have been adopted on the basis of an accessible legal regime. In other words, it will not be enough that the measures are targeted to find certain needles in a haystack: the proper measure is the impact of the measures on the haystack, relative to the harm threatened; namely, whether the measure is necessary and proportionate.; available at

[http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/](http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Pages/Session27.aspx)

f

Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/69/397, September 23, 2014 : [Mass surveillance] amounts to a systematic interference with the right to respect for the privacy of communications,. . . it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately. Available at <http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/54>

18 *S and Marper v. United Kingdom* (2009) 48 EHRR 50

19 American Civil Liberties Union, Amicus Brief, Government Application for Historical Cell Site Data from Cell Towers in the Vicinity of One Location During 4.5 hours, May 20, 2014, available at

<https://www.aclu.org/sites/default/files/assets/5>

ancis.pdf

20 In the Matter of the APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. §§ 2703(C) and 2703(D) DIRECTING AT & T, SPRINT/NEXTEL, TMOBILE, METRO PCS

④ 제3항에 따른 통신자료제공 요청은 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를

기재한 서면(이하 "자료제공요청서"라 한다)으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있을 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 해소되면 지체 없이 전기통신사업자에게 자료제공요청서를 제출하여야 한다.

⑤ 전기통신사업자는 제3항과 제4항의 절차에 따라 통신자료제공을 한 경우에는 해당 통신자료제공 사실 등 필요한 사항을 기재한 대통령령으로 정하는 대장과 자료제공요청서 등 관련 자료를 갖추어 두어야 한다.

⑥ 전기통신사업자는 대통령령으로 정하는 방법에 따라 통신자료제공을 한 현황 등을 연 2회 미래창조과학부장관에게 보고하여야 하며, 미래창조과학부장관은 전기통신사업자가 보고한 내용의 사실 여부 및 제5항에 따른 관련 자료의 관리 상태를 점검할 수 있다.

⑦ 전기통신사업자는 제3항에 따라 통신자료제공을 요청한 자가 소속된 중앙행정기관의 장에게 제5항에 따른 대장에 기재된 내용을 대통령령으로 정하는 방법에 따라 알려야 한다. 다만, 통신자료제공을 요청한 자가 법원인 경우에는 법원행정처장에게 알려야 한다.

⑧ 전기통신사업자는 이용자의 통신비밀에 관한 업무를 담당하는 전달기구를 설치운영하여야 하며, 그 전달기구의 기능 및 구성 등에 관한 사항은 대통령령으로 정한다.

https://elaw.klri.re.kr/eng_service/lawPrint.do?h

32<http://old.kcc.go.kr/user.do?mode=view&page=P0503>

α=35108

33 <http://transparency.verizon.com/us-data>

34 <http://money.cnn.com/2011/03/23/technology/sprint>

35 <http://www.google.com/transparencyreport/userdata>

36 <http://emailblog.eu/2014/01/27/2013-email-client-1>

37 U.S. Code, Title 18 Section 2703 (c) Records concerning electronic

communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--. [omitted].

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

38 UK Regulation of Investigatory Powers Act 2000, Article 23

39 Federal Electronic Communications Act, Article 113 (1)

40 Code des Postes et Communications électroniques, Article L34-1 through L34-6

41 Jeffrey M. Skopek, Reasonable Expectations of Anonymity, 101 Virginia Law Review ____ (forthcoming May 2015).

42 R. v. Spencer, 2014 SCC 43, June 13, 2014

43 _____

44 2012. 8. 23 2010헌마439

45 <http://www.youtube.com/watch?v=X500D72-MzA>

46 <http://www.koreatimes.co.kr/www/news/nation/2010/>

47 서울고등법원 2012. 10. 18. 선고, 2011나19012 판결 (주심 김상준 판사)

48 http://www.hani.co.kr/arti/economy/economy_genera

49 법원이나 정부기관이 별도의 감시 부분 통계자료를 만들기란 어렵다. 이메일은 수신지에 도달하는 순간, (정보가 아닌 물건에 적용되는) 일반 압수수색 절차의 대상인 고정물이 되기 때문이다.

50 *Hankyoreh Newspaper*, April 23, 2009

http://www.hani.co.kr/arti/society/society_genera

51 *Hankyoreh Newspaper*, 2009.6.19:

http://www.hani.co.kr/arti/society/society_genera

52 *Asia Economy*, 2009.7.1:

<http://www.asiae.co.kr/news/view.htm?idxno=200907>

53 <http://www.hani.co.kr/popups/print.hani?ksn=35155>

54 이메일 서비스는 본인 인증이 필요없는 서비스이나, 국내 포털사들은 보통, 그들이 제공하는 서비스 중 일부라도 본인 인증 요구 대상이면, 수차례 신원 정보를 요청하는 불편과 비용을 최소화하기 위하여 가입 절차부터 모든 신원 정보의 기재를 요하고 있다.

55 서울고등법원 2013. 7. 5. 선고 2012나4678

<http://article.joins.com/news/article/article.asp>

56 통신비밀보호법 제6조(범죄수사를 위한 통신제한조치의 허가절차)

⑦ 통신제한조치의 기간은 2월을 초과하지 못하고, 그 기간중 통신제한조치의 목적이 달성되었을 경우에는 즉시 종료하여야 한다. 다만, 제5조제1항의 허가요건이 존속하는 경우에는 제1항 및 제2항의 절차에 따라 소명자료를 첨부하여 2월의 범위안에서 통신제한조치기간의 연장을 청구할 수 있다. <개정 2001.12.29.>

57 29 U.S. Code 2518 (5)

58 박경신.

59 주국

60 오길영

61 박경신, _____ 오길영,

62 정진우 압수수색 상황에 대한 진보넷 보도자료

63 *Goldberg v. Kelly*, 397 U.S. 254 (1970)

64 통신비밀보호법 제9조의2

65

<https://www.privacyinternational.org/reports/japan/>

<http://www.thefreelibrary.com/Wiretapping+law+use>

66 Electronic Communications Privacy Act, Section 2518. Procedure for interception of wire, oral, or electronic communications

. . .

(8) . . . (d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of. . .

67 미국, 일본, 독일의 통지조항에 대한 자세한 비교에 대해서는 박찬걸, 강동욱, “통신제한조치의 집행에 관한 법정정책적 고찰”, <법과 정책> 제20집 제1호, 제주대학교 법과정책연구소 (2014년 3월), 315-339쪽

68 통신비밀보호법 제9조의2(통신제한조치의 집행에 관한 통지)

④제1항 내지 제3항의 규정에 불구하고 다음 각호의 1에 해당하는 사유가 있는 때에는 그 사유가 해소될 때까지 통지를 유예할 수 있다.

1. 통신제한조치를 통지할 경우 국가의 안전보장공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때

2. 통신제한조치를 통지할 경우 사람의 생명신체에 중대한 위험을 초래할 염려가 현저한 때

⑤검사 또는 사법경찰관은 제4항의 규정에 의하여 통지를 유예하고자 하는 경우에는 소명자료를 첨부하여 미리 관할지방검찰청검사장의 승인을 얻어야 한다. 다만, 검찰관 및 군사법경찰관이 제4항의 규정에 의하여 통지를 유예하고자 하는 경우에는 소명자료를 첨부하여 미리 관할 보통검찰부장의 승인을 얻어야 한다.

69

70 이하의 내용 대부분은 아래 저자의 논문에서 발췌함.

http://m.riss.kr/search/detail/DetailView.do?p_ma
[290fb78355ffe0bdc3ef48d419](http://m.riss.kr/search/detail/DetailView.do?p_ma)

http://ils.inha.ac.kr/board_laborlaw/View.aspx?Mo

31 (PDF)

71 통신비밀보호법 제9조의3

72 형사소송법 https://elaw.klri.re.kr/kor_service/lawPrint.do?h

제121조(영장집행과 당사자의 참여)

검사, 피고인 또는 변호인은 압수수색영장의 집행에 참여할 수 있다.

제122조(영장집행과 참여권자에의 통지)

압수수색영장을 집행함에는 미리 집행의 일시와 장소를 전조에 규정한 자에게 통지하여야 한다. 단, 전조에 규정한 자가 참여하지 아니한다는 의사를 명시한 때 또는 급속을 요하는 때에는 예외로 한다.

제219조(준용규정)

제106조, 제107조, 제109조 내지 제112조, 제114조, 제115조제1항 본문, 제2항, 제118조부터 제132조까지, 제134조, 제135조, 제140조, 제141조, 제333조제2항, 제486조의 규정은 검사 또는 사법경찰관의 본장의 규정에 의한 압수, 수색 또는 검증에 준용한다. 단, 사법경찰관이 제130조,

제132조 및 제134조에 따른 처분을 함에는 검사의 지휘를 받아야 한다. <개정 1980.12.18., 2007.6.1., 2011.7.18.>

73 펜 레지스터 데이터도 마찬가지이나, 이것에 대해서는 다른 기회에 논의하기로 한다. 이 실시간 펜레지스터 데이터와 소급적데이터의 비구별 문제는 다른 국가들에 편재하고 있는 것으로 보인다.

(The same is true for pen register data but we will talk about that in another time since this problem of not distinguishing real-time pen register data and retroactive data seems ubiquitous in other countries.)

74 이메일압수수색에 대해서는 형소법에 따라 곧바로 통지가 이루어져야 한다는 주장에 대해서는 박찬걸 등의 전제서.

75 <http://news.mt.co.kr/mtview.php?no=20101012171123>

76 서울고등법원 2013. 7. 5. 선고, 2012나46780 (대법원 상고 기각)

77 http://www.humanrights.go.kr/03_sub/body02_2.jsp 이 페이지에서 '전자우편'으로 검색시 관련 문서를 찾을 수 있음.

78 형사소송법 제106조 (압수)

① 법원은 필요한 때에는 피고사건과 관계가 있다고 인정할 수 있는 것에 한정하여 증거물 또는 몰수할 것으로 사료하는 물건을 압수할 수 있다. 단, 법률에 다른 규정이 있는 때에는 예외로 한다. <개정 2011.7.18.>

② 법원은 압수할 물건을 지정하여 소유자, 소지자 또는 보관자에게 제출을 명할 수 있다.

③ 법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체(이하 이 항에서 "정보저장매체등"이라 한다)인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체등을 압수할 수 있다. <신설 2011.7.18.>

④ 법원은 제3항에 따라 정보를 제공받은 경우 「개인정보 보호법」 제2조제3호에 따른 정보주체에게 해당 사실을 지체 없이 알려야 한다. <신설 2011.7.18.>

79 <http://m.mediatoday.co.kr/articleView.html?idxno=>

80 통신비밀보호법 제11조 (비밀준수의 의무)

① 통신제한조치의 허가집행통보 및 각종 서류작성 등에 관여한 공무원 또는 그 직에 있었던 자는 직무상 알게 된 통신제한조치에 관한 사항을 외부에 공개하거나 누설하여서는 아니된다.

② 통신제한조치에 관여한 통신기관의 직원 또는 그 직에 있었던 자는 통신제한조치에 관한 사항을 외부에 공개하거나 누설하여서는 아니된다.

③ 제1항 및 제2항에 규정된 자외에 누구든지 이 법의 규정에 의한 통신제한조치로 지득한 내용을 이 법의 규정에 의하여 사용하는 경우외에는 이를 외부에 공개하거나 누설하여서는 아니된다.

④ 법원에서의 통신제한조치의 허가절차허가여부허가내용 등의 비밀유지에 관하여 필요한 사항은 대법원규칙으로 정한다.

[전문개정 2001.12.29.]

81 <http://www.gobalnews.com/news/articleView.html?id> (Korean)