2012-03

이슈리포트 〈액트온〉

◇ 인터넷과 표현의 자유
/ 장여경 ····· 1

◇ 프라이버시 보호 정책 방향
/ 오병일·장여경 ····· 38

진보네트워크센터

서울시 서대문구 충정로3가 227-1 우리타워 3층
전화 02)774-4551, 이메일 della@jinbo.net
홈페이지 http://act.jinbo.net

발행인_ 진보네트워크센터 (대표 이종회)
배포처_ 진보넷 회원님들
발행일_ 2012년 4월 15일

인터넷 표현의 자유*

장여경
(진보네트워크센터)

I. 문제 제기

한국 인터넷 이용률은 2010년 기준으로 77.8%이며 가구당 인터넷 보급률은 81.6%에 달한다.[1] 일반 시민의 미디어 접근이 쉽지 않은 언론 출판 환경 속에서, 인터넷은 한국의 일반 시민에게 필수적인 표현 매체이다. 그러나 한국에서 인터넷 표현의 자유에 대한 침해 논란이 계속됐으며 이는 특히 이명박 정부가 들어선 후 크게 더욱 두드러졌다. 인터넷 표현의 자유 규제에서 무엇보다 심각한 문제는 직접 유통을 규제하거나 게시자를 형사 처벌하는 문제가 무엇보다 심각한 것이다. 정부의 정치적 입장이나 정책과 다른 견해를 표명한 인터넷 게시물을 행정심의로써 삭제하고 '허위의 통신' 등의 죄목으로 형사 처벌한다는 비판이 제기되어 왔다. 또한, 인터넷

---

* 이 글은 2012년 제19대 총선을 앞두고 1월 29일 발간된 『미디어 생태계 민주화를 위한 2012 정책보고서』(미디어커뮤니케이션네트워크 편저)에 게재된 원고를 수정하여 4월 21일 발간되는 『표현의 자유를 위한 정책 제안』(표현의자유를위한연대 편저)에 게재한 원고이다.

1) "인터넷 이용률", 나라지표, 〈http://www.index.go.kr〉; "가구 인터넷 보급률 및 컴퓨터 보유율", 좌동.

실명제와 이를 기초로 한 이용자 정보 제공이 공권력을 비판하고자 하는 이들을 위축시킴으로써 간접적으로 표현의 자유를 침해한다는 지적도 끊이지 않고 있다.

Ⅱ. 국제인권기준

1. 국제인권규범

가. 국제규약과 그 해설

인터넷 표현의 자유도 그 근거가 되는 국제인권규범은 시민적, 정치적 권리에 관한 국제규약 제19조이다. 특히 제19조 제2항은 "스스로 선택하는 기타의 방법"이라고 하여 표현의 자유의 수단을 제한하지 않음으로써 인터넷 표현의 자유 근거로 작용한다고 볼 수 있다.

> 시민적 정치적 권리에 관한 국제규약 제19조
>
> 1. 모든 사람은 간섭받지 아니하고 의견을 가질 권리를 가진다.
> 2. 모든 사람은 표현의 자유에 대한 권리를 가진다. 이 권리는 구두, 서면 또는 인쇄, 예술의 형태 또는 스스로 선택하는 기타의 방법을 통하여 국경에 관계없이 모든 종류의 정보와 사상을 추구하고 접수하며 전달하는 자유를 포함한다.
> 3. 이 조 제2항에 규정된 권리의 행사에는 특별한 의무와 책임이 따른다. 따라서 그러한 권리의 행사는 일정한 제한을 받을 수 있다. 다만, 그 제한은 법률에 의하여 규정되고 또한 다음 사항을 위하여 필요한 경우에만 한정된다.
>   (a) 타인의 권리 또는 신용의 존중
>   (b) 국가안보 또는 공공질서 또는 공중보건 또는 도덕의 보호

자유권위원회(Human Rights Committee)는 2011년 7월 제102차 회기에서 채택하여 9월 12일에 배포한 '일반논평 34호'[2]에서 규약 제19조가

2) Human Rights Committee, General Comment No. 34. Article 19: Freedoms of

인터넷에도 적용되는 지점을 상세히 밝혔다. 즉, “제2항에서는 모든 형태의 표현과 그 전파 수단을 보호한다 … 여기에는 모든 형태의 시청각 방식과 전자적 혹은 인터넷 기반 표현 방식이 포함된다(12문단).”는 것이고, “당사국은 인터넷과 이동식 기반의 전자정보보급 시스템과 같은 정보와 통신기술의 발달이 전 세계의 의사소통 관행을 엄청나게 변화시켰음을 고려하여야 한다. 이제는 사상과 의견을 교환하기 위해 전통적 대중매체의 중개에 의존할 필요가 없는 전 지구적 네트워크가 있다. 당사국은 이러한 새로운 매체를 육성하고 개인들이 거기에 접근할 수 있도록 필요한 모든 조치를 취해야 한다(15문단).”며 인터넷이 표현의 자유에서 갖는 중요성을 환기하였다. 또한 “당사국은 대중매체를 규제하는 입법적, 행정적 체제가 제3항과 일관되도록 해야 한다. 규제 제도는 신문 및 방송부문과 인터넷 간의 차이를 고려하고, 동시에 다양한 매체가 어떻게 수렴하는지 그 방식에도 주의하여 마련되어야 한다(39문단).…(하략)”면서 “인터넷 서비스 공급자나 검색엔진과 같이 통신을 지원하는 체계를 포함하여, 웹사이트, 블로그, 기타 인터넷 기반, 전자적, 혹은 기타 유사 정보보급체계의 운영에 대한 규제는 제3항에 부합하는 경우에만 허용될 수 있다. 허용되는 규제는 일반적으로 특정 내용에 한정된다. 어떤 사이트나 체계의 운영을 포괄적으로 금지하는 것은 제3항에 부합하지 않는다. 정부에 대해, 또는 정부가 채택한 정치사회체제에 대해 비판적일 수 있다는 이유만으로 어떤 사이트나 정보배급체계가 자료를 발간하지 못하게 금하는 것 역시 제3항에 부합하지 않는다(43문단).”고 그 한계를 상세히 규정하였다.

나. 유엔 표현의 자유 특별보고관의 연례보고

2011년 6월 제17차 유엔 인권이사회에서 프랭크 라 뤼 의사표현의 자유에 관한 유엔 특별보고관은 연례보고서[3]를 인터넷 표현의 자유에 할당하

---

opinion and expression, CCPR/C/GC/34, 2011.7.21, 〈http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf〉

3) Frank La Rue, Report of the Special Rapporteur on the promotion and protection

였다. 이 보고서에서 특별보고관은 전 세계에 걸친 인터넷 표현의 자유에 대한 위협 요인을 지목하였다. 콘텐츠에 대한 자의적인 차단이나 필터링, 정당한 표현의 불법화, 인터넷 사업자와 같은 중개인에 법적 책임 부과, 지적재산권 침해라는 이유로 인한 이용 해지, 사이버 공격, 부실한 프라이버시 보호 등이 핵심적인 문제이다.[4)]

먼저, 정당한 표현을 제재하기 위하여 형사법을 자의적으로 사용하는 것은 '위축 효과'를 야기할 뿐 아니라 구금 등 당사자에 대한 인권 침해로 이어진다는 점에서 경계의 대상이다. 선거시기, 사회적 격동기 등 주요한 정치적 순간에 이용자들이 정보에 접근하거나 전달하는 것을 기술적으로 방해하는 일이 세계 각국에서 곧잘 발생하는 것은 우연이 아니다. 특별보고관은 기술적인 방식으로 이루어지는 인터넷 차단이나 필터링이 투명하고도 엄격한 조건에서만 제한적으로 이루어져야 한다고 권고하였다.[5)]

또 명예훼손이나 국가안보 보호라는 이유로, 사실은 정부나 권력자들의 마음에 들지 않는 콘텐츠를 검열하는 일이 많이 발생하는 상황이 우려스럽다. 특히 특별보고관은 명예훼손을 범죄화해서는 안 되며 평화적인 의견 제시가 국가안보라는 이유로 제약되어서는 안 된다고 여러 차례 강조하였다. 정부정책에 관한 토론이나 정치 논쟁, 선거 캠페인, 소수 종교나 사상에 대한 의견에 대해서는 어떠한 이유로도 제한을 두어서는 안 된다.[6)]

최근에는 인터넷 사업자와 같은 중개인의 역할이 커지면서 그에 대한 통제를 통해 국가와 사적 권력의 입맛대로 인터넷 콘텐츠가 검열되는 상황도 발생하고 있다. 특별보고관은 중개인이 콘텐츠에 개입할 때에는 인권을 존중하기 위하여 지켜야 할 것이 있다고 지적하였다. 인터넷 콘텐츠에 대한 조치는 사법부의 개입 후에 이루어지는 것이 원칙이고, 조치에 대해 이용

---

of the right to freedom of opinion and expression, A/HRC/17/27, 2011.5.16, 〈http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf〉.

4) Frank La Rue, 위의 보고서, IV.

5) Frank La Rue, 위의 보고서, IV. A. 및 VI. A. 70-71.

6) Frank La Rue, 위의 보고서, IV. B. 및 VI. A. 72-73.

자에게 투명하게 알리는 한편, 조치를 취하기 전에 이용자에게 사전고지를 해야 하며, 사후 이의제기 절차를 보장해야 한다는 것이다.[7)]

눈에 띄는 대목은 지적재산권 침해와 표현의 자유 문제를 결부시킨 것이다. 특별보고관은 이용자들이 지적재산권법을 위반했을 때 인터넷 접속을 차단하는 제도들에 대해 경악했다. 최근 지적재산권 강화추세와 더불어 삼진아웃제, 즉 세 번 위반했을 때 인터넷 이용을 해지하는 법안을 도입한 몇몇 나라들이 있다는 것이다. 특별보고관은 지적재산권 관련 법으로 인터넷 이용자들의 이용권을 박탈하는 제도를 폐지하거나 수정할 것을 권고하였다.[8)]

특별보고관은 인권기구나 반체제 인사들이 DDos 공격의 목표가 되는 현상도 걱정스럽게 보았다. 또한, 페이스북과 같은 소셜네트워크를 이용하여 인권운동가나 반체제 인사들을 사찰하는 것 또한 문제로 보았다.[9)] 무엇보다 익명 토론을 제약하는 것은 인터넷 이용자의 프라이버시권을 침해하고 인터넷상에서 정보와 생각의 자유로운 흐름을 방해한다는 점에서 비판의 대상이다.[10)]

다. 미국 연방대법원 판결

미국 연방대법원은 1997년 6월 26일 Reno v. ACLU 판결[11)]에서 연방통신품위법(the Communications Decency Act: 일명 CDA)의 '저속한 표현의 전송'(indecency transmission)에 관한 조항과 '명백히 거슬리는 표현의 전시'(patently offensive display)에 관한 조항은 그 규제범위가 광범위하여 수정헌법 제1조를 침해한다는 이유로 위헌결정을 내렸다. 이 판결은 인터넷 표현의 자유를 천명한 효시로서 국제적으로 널리 알려졌다. 특히

---

7) Frank La Rue, 위의 보고서, VI. A. 74-77, 특히 76.
8) Frank La Rue, 위의 보고서, IV. D. 49 및 VI. A. 78-79.
9) Frank La Rue, 위의 보고서, IV. E. 및 VI. A. 80-81.
10) Frank La Rue, 위의 보고서, IV. F. 및 VI. 82-84.
11) 521 U.S. 844, 117 S.Ct. 2329.

이 판결에서는 방송매체에 대한 규제근거들, 즉, 방송에 대한 광범위한 정부규제의 역사, 주파수의 희소성, 방송의 침투적 성격[12] 등은 '사이버공간'(cyberspace)에서는 존재하지 않는다는 점을 지적하였다.

그뿐만 아니라 McIntyre v. Ohio 판결[13]은 표현을 하고자 하는 자에게 자신의 신원을 밝힐 것을 요구하는 것은 표현의 자유를 위축시킨다며 익명표현의 자유를 확립하였다.

2. 국제기구의 한국에 대한 권고

2011년 6월 제17차 유엔 인권이사회에서 프랭크 라 뤼 의사표현의 자유에 관한 유엔 특별보고관은 한국보고서를 발표하면서 인터넷 표현의 자유에 특별한 관심을 할애하였다.[14] 특별보고관은 네티즌 '미네르바'에 대한 구속기소, 언론소비자주권국민캠페인 카페 운영자에 대한 구속기소, 최병성 목사의 쓰레기시멘트 게시물에 대한 삭제 사례들을 구체적으로 들며 대한민국 인터넷 표현의 자유 실태가 걱정스러운 수준이라고 판단하였다. 먼저, 특별보고관은 어떤 표현이 '허위'라는 이유로 처벌받는 데 반대하며 2010년 헌법재판소의 '허위의 통신' 위헌 결정을 환영하였다(35, 90). 또한, 특별보고관은 방송통신위원회와 방송통신심의위원회(이하 '방통심의위')는 물론이고 포털 등 온라인 사업자를 통해 이루어지는 온라인 콘텐츠 규제에 깊은 우려를 드러내었다. 특별보고관은 방송통신위원회와 방통심의위가 인터넷 콘텐츠를 규제할 수 있도록 한 법률상 '불법정보'의 유형이

---

12) 방송의 침투적 성격(uniquely pervasive presence)이란 방송 특히 텔레비전이 가족구성원 모두가 접근 가능하고 매우 친숙하기 때문에 우리가 숨 쉬는 공기처럼 가족생활 깊숙이 그리고 빠짐없이 들어와 있다는 의미인데, 바로 이러한 성격 때문에 정부에 의한 방송 규제가 필요하다는 논거로 사용된다.

13) 514 U.S. 334(1995).

14) Frank La Rue, Mission to the Republic of Korea, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 2011.3.21, A/HRC/17/27/Add.2, 〈http://www2.ohchr.org/english/bodies/hrcouncil/17session/reports.htm〉. 이하 유엔 표현의 자유 특별보고관의 언급은 모두 이 보고서 참고.

모호하고, 방통심의위가 정부에 비판적인 정보를 삭제하는 사실상의 사후 검열 기구로서 기능하는 측면이 있다고 지적하였다(45, 47). 따라서 방통심의위의 권한과 기능을 독립적 자율규제기구로 이양할 것을 권고한 국가인권위원회의 결정을 환영하며, 특별보고관 역시 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 '정보통신망법'이라 함)을 명확하게 개정하고 방통심의위의 기능을 어떠한 정치적, 상업적 및 기타 부당한 영향력으로부터도 자유로운 독립 기구에 이관할 것을 권고하였다(47, 48, 93). 더불어 특별보고관은 포털 등 온라인 사업자들이 임시조치 제도를 남용하지 않도록 관련 법률을 손볼 것을 권고하였고(92), 인터넷 실명제 대신 다른 신원확인수단을 모색할 것 역시 권고하였다(94).

프랑크 라 뤼 유엔 표현의 자유 특별보고관 한국보고서
(A/HRC/17/27/Add.2, 2011.3.21.)

90. 특별보고관은, 전기기본통신법 제47조 제1항이 위헌이라고 결정하여 동 조항의 효력을 정지시킨 2010년 12월 28일 헌법재판소의 결정을 환영한다.
91. 그러나 특별보고관은 정보통신망법 제44조의7에 열거된 '불법정보'의 유형이 광범위하고 모호하여 의사 표현의 자유 행사에 위축 효과를 야기할 수 있다는 점에 대하여 여전히 우려를 가지고 있다. 따라서, 특별보고관은 대한민국 정부가 동 조항을 포함한 정보통신망법의 관련 조항들이 법적 명확성 원칙에 부합되도록 하고 자유권규약 제19조 제3항에 열거된 사유를 보호하기 위해 필요한 것으로 정당화 될 수 있는 조치를 취할 것을 권고한다.
92. 특별보고관은 정보통신망법 제44조의2 제6항에 기술된 중계업체의 책임 요건 및 범위가 모호하여 결과적으로 온라인 콘텐츠에 대한 과도한 규제를 초래할 수 있음을 우려한다. 특별보고관은 대한민국정부에게 중계업체의 법적 책임과 관련된 모든 조항을 삭제하도록 권고한다.
93. 또한, 특별보고관은 방송통신심의위원회가 정부에 비판적인 정보를 정보통신망법 위반이라는 이유로 삭제하는 사실상 사후 검열 기구로서 기능하지 않도록 하는 안전장치가 미흡하다는 점에 우려를 표한다. 2010년 9월 30일 국가인권위원회가 채택한 결정에 의거하여, 특별보고관은 대한민국정부에게 방송통신심의위원회의 현 기능을, 사법적 심사를 포함하여 남용을 방지할 수 있는 적절한 안전장치를 갖추고 있으며 어떠한 정치적, 상업적 및 기타 부당한 영향

력으로부터도 자유로운 독립 기구에게 이양할 것을 권고한다.
94. 실명제가 익명성을 기반으로 하는 인터넷상 표현의 자유 행사를 제한하고 있음을 고려하여, 특별보고관은 대한민국 정부에게 다른 신원 확인 수단을 검토하고 그러한 수단도 신원 확인 대상자가 범죄를 저질렀거나 저지르려고 한다는 상당한 근거나 합리적인 의심이 있는 경우에 한하여 사용하도록 권고한다.

Ⅲ. 인권상황평가: 실태와 문제점

1. 헌법재판소와 국가인권위원회의 견해

2002년 헌법재판소는 전기통신사업법 제53조, 즉 '불온통신의 단속' 조항에 관한 위헌확인 사건에서 인터넷에 대하여 공중파방송과 달리 "가장 참여적인 시장", "표현촉진적인 매체"라고 규정하였다.[15] 공중파방송은 전파자원의 희소성, 방송의 침투성, 정보수용자 측의 통제능력의 결여와 같은 특성이 있어서 그 공적 책임과 공익성이 강조되기 때문에 인쇄매체에서 볼 수 없는 강한 규제조치가 정당화되기도 하지만, 인터넷은 방송의 특성이 없으며, 진입장벽이 낮고, 표현의 쌍방향성이 보장되며, 그 이용에 적극적이고 계획적인 행동이 필요하다는 특성을 지닌다는 것이다. 더불어 헌재는 "오늘날 가장 거대하고, 주요한 표현매체의 하나로 자리를 굳힌 인터넷상의 표현에 대하여 질서 위주의 사고만으로 규제하려고 할 경우 표현의 자유 발전에 큰 장애를 초래할 수 있다. 표현매체에 관한 기술의 발달은 표현의 자유의 장을 넓히고 질적 변화를 야기하고 있으므로 계속 변화하는 이 분야에서 규제의 수단 또한 헌법의 틀 내에서 다채롭고 새롭게 강구되어야 할 것이다."고 지적하였다.

국가인권위원회는 '불온통신의 단속' 조항에 관한 위헌결정 이후 이를 대체하여 '불법정보의 유통금지 등'에 대한 조항[16]을 도입하려는 전기통신

15) 헌재 2002.6.27. 선고, 99헌마480, 전기통신사업법 제53조 등 위헌확인. 이하 헌법재판소의 '불온통신의 단속' 위헌 결정에 대한 언급은 모두 이 결정 참고.

사업법 개정법안에 대하여 “일률적으로 행정명령이라는 공적규제로 통제하려고 하는 것은 행정규제의 최소화 원칙에 상치되며, 국민의 표현의 자유, 알권리 등을 현저히 침해할 가능성이 있으므로 바람직하지 않다”고 밝히며 “국가 행정에 의한 통제보다는 정보통신사업자의 자율적인 규제의 방향으로 가는 것이 바람직할 것”이라고 의견표명을 했다. 또한, 전기통신사업법 개정안에서 명확성 원칙에 반하는 규정 내용을 삭제하거나 변경할 것을 권고하기도 했다.[17] 국가인권위원회는 이러한 문제의식을 이어받아 2010년 방송통신위원장에게 “현행 방송통신심의위원회에 부여하고 있는 불법정보 등에 대한 심의권 및 시정요구권을 정보통신 서비스 제공자 및 게시물 관리 사업자 대표들과 시민사회 대표들이 함께 구성하는 민간자율심의기구에 이양하는 내용으로 관련 규정을 개정할 것”을 권고하였다.[18]

그 밖에도 국가인권위원회는 인터넷 표현의 자유에 대하여 여러 차례에 걸쳐 의견을 표명하였다. 먼저 인터넷 실명제에 대하여 국가인권위원회는 2004년 「공직선거 및 선거부정방지법」에 인터넷언론사의 선거게시판 등에 인터넷 실명제를 도입하려는 법안이 “명백한 사전검열에 해당하며 익명성에서 기인하는 인터넷상의 표현의 자유와 여론형성의 권리를 제한하여, 세계인권선언 제19조와 헌법 제21조의 표현의 자유에 반하고 헌법 제17조의 개인의 자기정보 관리 통제권을 침해할 우려가 있다”며 반대하는 의견을 표명하였다.[19] 또한, 2008년 이명박 정부 들어 인터넷 실명제의 대상 범위를 확대하려는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 전부개정안」을 정부가 발의하자, 국가인권위원회는 헌법이 보장하고 있는 표현의 자유 및 직업수행의 자유를 침해할 수 있으므로 이처럼 개정하는

16) 현재 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7에 해당한다.

17) 국가인권위원회, “의견서: 전기통신사업법 개정안과 관련하여”, 2002.8.12.

18) 국가인권위원회, “정보통신심의제도에 대한 개선권고”, 2010.9.30. 결정. 이하 방통심의위의 인터넷 행정심의 제도에 대한 국가인권위원회의 언급은 모두 이 결정 참고.

19) 국가인권위원회 제1소위원회, “‘정치관계법’개정에 대한 국가인권위원회의 의견”, 2004.2.16.

것은 바람직하지 않다는 의견을 국회의장에게 전달하였다.[20] 또 국가인권위원회는 사이버모욕죄 신설을 내용으로 한 「형법 일부개정법률안」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」이 국회에 발의된 데 대하여 사이버모욕죄를 반의사불벌죄로 규정한 것에 반대하고 기존의 모욕죄와 같이 친고죄로 규정할 것을 권고하였다.[21] 2009년 국가인권위원회는 당시 헌법재판소에 계류 중이었던 「전기통신기본법」 제47조 1항, 일명 '허위의 통신' 조항에 관하여 형벌규정이 갖추어야 할 명확성을 갖추고 있지 못하여 표현의 자유를 침해할 우려가 크다는 의견을 헌법재판소에 제출하였다.[22]

한편 '공익을 해할 목적으로 전기통신설비로 허위 통신을 한 사람'을 처벌하도록 규정한 이 조항에 대하여 헌법재판소도 2010년 위헌이라는 결정을 내렸다.[23] 헌법재판소는 어떤 표현행위가 공익에 해당하는 것인지 아닌지에 관한 판단은 법 전문가라도 객관적으로 확정될 수 없다고 보았고, 현재의 다원적이고 가치 상대적인 사회구조하에서 구체적으로 어떤 행위상황이 문제 되었을 때 문제가 되는 공익은 하나로 수렴되지 않는다고 지적하였다.

이상과 같은 기준에 의하면 인터넷 표현의 자유란 다음과 같이 요약할 수 있다. 인터넷 매체는 방송 등 다른 매체에서보다 수용자의 적극성과 참여를 촉진하는 특성이 있다는 점에서 그 표현의 자유를 더 두텁게 보호해야 한다. 국가기관이 인터넷 표현의 자유를 규제할 때는 명확한 법률 규정에 따라 최소한으로 규제해야 한다. 특히 헌법재판소가 국가 권력의 인터넷 규제로 인한 '위축 효과'를 우려하였다는 사실은 시사하는 바가 크다.

---

20) 국가인권위원회, "「정보통신망 이용촉진 및 정보보호 등에 관한 법률 전부개정안」 제115조(게시판 이용자의 본인 확인) 제1항 제2호에 대한 의견", 2009.12.2.

21) 국가인권위원회, "「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안(나경원 의원 대표발의)」에 대한 의견표명", 2009.2.5. 결정; "「형법 일부개정법률안(장윤석 의원 대표발의)」에 대한 의견표명", 2009.2.27. 결정.

22) 국가인권위원회, "「전기통신기본법」 제47조 제1항에 관한 의견", 2009.6.8.

23) 헌재 2010.12.28. 2008헌바157, 2009헌바88(병합) 결정.

헌법재판소는 '불온통신의 단속'에 대한 위헌 결정에서 "표현의 자유를 위축시키지 않게 명확하면서도, 진정한 불온통신을 효과적으로 규제할 수 있도록 입법한다는 것은 쉬운 일이 아닐 것이다. 그러나 규제대상이 다양·다기하다 하더라도, 개별화·유형화를 통한 명확성의 추구를 포기하여서는 안되고, 부득이한 경우 국가는 표현규제의 과잉보다는 오히려 규제의 부족을 선택하여야 할 것이다. 해악이 명백히 검증된 것이 아닌 표현을 규제하는 것은 득보다 실이 크다고 보는 것이 표현의 자유의 본질이기 때문이다"라고 설시하였다.[24]

2. 규제 현황과 문제점

현재 우리나라 인터넷 표현의 자유 규제는 크게 직접 규제와 간접 규제로 나누어볼 수 있다. 직접 규제는 다시 행정심의와 임시조치 등 유통을 규제하는 것과 직접 형사 처벌하는 것으로 나눌 수 있다.

가. 유통규제

현재 제도적으로 규정되어 있는 유통규제는 방통심의위의 행정심의, 사생활 침해에 대한 온라인 사업자들의 임시조치, 저작권 침해에 대한 온라인 사업자들의 임시조치를 들 수 있다.

1) 방송통신심의위원회의 행정심의

인터넷에 대한 유통 규제는 일차적으로 행정심의를 통해 이루어진다. 인터넷 행정심의는 상용 인터넷접속서비스가 시작되었던 1995년 법정기구로 발족한 (구)정보통신윤리위원회[25]로부터 현재까지 지속해왔다. 특히

24) 헌재 2002.6.27. 선고, 99헌마480.

25) "정보통신윤리위원회는 1992년 7월 국무총리 주재로 열린 '새질서, 새생활 실천

2008년 이명박 정부 들어서부터는 「방송통신위원회의 설치 및 운영에 관한 법률」(이하 '방송통신위원회법')에 의하여 방통심의위가 설립되어 인터넷 등 통신 분야 심의를 담당하고 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7(불법정보의 유통금지 등) 조항은 음란·명예훼손·위협·서비스방해·청소년유해매체물·사행행위·국가기밀·국가보안법·범죄 교사 및 방조 등 인터넷 불법정보에 대하여 방통심의위와 방송통신위원회를 통한 행정심의 제도를 규정하고 있다. 방통심의위는 개인이나 포털, 방송통신위원회 및 각급 공공기관으로부터 심의를 요청받거나 자체적인 모니터링을 통해 인지한 불법정보를 심의한 후 시정요구 결정을 하고 이를 정보통신서비스 제공자 또는 게시판 관리·운영자에게 권고한다. 정보통신서비스 제공자 또는 게시판 관리·운영자가 이를 이행하지 않을 때 대통령 직속기구인 방송통신위원회는 그 정보의 성격에 따라 해당 정보의 취급을 거부·정지 또는 제한하도록 명할 수 있다(동법 제44조의7 제2항과 제3항). 이 명령에 따르지 않으면 2년 이하의 징역 또는 1천만 원 이하의 벌금에 처해진다(동법 제73조 제5호).

한편, 불법정보는 아니지만 전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 시행령이 정하는 정보에 대하여 방통심의위는 심의 및 시정요구를 할 수 있다(방송통신위원회법 제21조 제4호). 또한, 대통령령에는 위 불법정보 및 청소년에게 유해한 정보 등 '심의가 필요하다고 인정되는 정보'를 방통심의위가 심의 및 시정 요구할 수 있도록 다시 규정하고 있다(동법시행령 제8조). 이 규정에 따른 시정요구는 그 이행을 강제하기 위한 제재 규정이 있지는 않다.

결국, 실질적인 심의의 전체적 구조는 다음과 같다.

실무대책협의회'에서 그 구성이 협의되어 같은 해 10월, 전기통신사업법 제53조 및 동 시행령 제19조에 의거 민간자율기구로서 구성되었다. 1995년 1월에는 위원회의 역할 강화 필요성이 대두되어 전기통신사업법을 개정, 같은 해 4월에 법정 기구로 새롭게 출범하였다." 사이버인터넷역사박물관, "정보통신윤리위원회 발족", 〈http://i-museum.kisa.or.kr/sub01/article_read.do?pageIndex=1&aSeq=2910&cate2=11〉, 검색일: 2011. 10. 31.

〈표 1〉 방통심의위 심의 구조[26]

근거조항	시행령 내용	세부심의사항	제재방법(세부내용)
설치법 제21조 제4호	(1) 정보통신망법 제44조의7	음란	시정요구: (1) 해당 정보의 삭제 또는 접속차단 (2) 이용자에 대한 이용정지 또는 이용해지
		명예훼손	
		스토킹	
		네트워크교란	
		'영리성' 청소년유해물	
		사행행위	
		국가기밀	
		국가보안법	
		범죄교사 및 방조	
	(2) 청소년유해매체물	청소년유해매체물	상기(1)+(2)+표시의무
	(3) 기타 "심의가 필요하다고 인정되는 정보"		

또한, 방통심의위는 자체적인 「정보통신에 관한 심의규정」[27]에 의해 정보의 불법성, 유해성 등을 심의한 후 정보통신서비스 제공자 또는 게시판 관리·운영자에게 삭제, 이용해지, 접속차단, 표시의무 이행, 표시방법 변경 등의 시정요구를 한다(방송통신위원회법 시행령 제8조 제2항 내지 제4항). 2008년 5월 16일 설립 이후 2010년 12월 31일까지 인터넷게시물에 대한 심의 건수는 총 99,693건으로 매월 약 3,115건이고 이 중 방통심의위에 의해 시정요구가 의결된 건수는 매월 약 2,304건이다.[28] 구체적인 심의 현황은 아래 표와 같다.

---

26) 출처: 박경신, "방송통신심의위원회의 인터넷내용심의의 위헌성", 한양대학교 법학논총 제27집 제2호, 2010, 65-99쪽.

27) 이 규정은 (구)정보통신윤리위원회의 '정보통신윤리심의규정'을 그대로 이어받아 별다른 개편 없이 사용해 왔다.
〈http://www.kocsc.or.kr/02_infoCenter/info_Law_View.php?ko_board=info_Law&ba_id=1881&page=1〉, 검색일: 2011. 10. 21.

28) 방송통신심의위원회, 『제1기 방송통신심의위원회 백서: 2008.2-2011.4』, 2011; 방송통신심의위원회 정보공개 종합. 이하 인용된 통계의 출처는 모두 같음.

〈표 2〉 방통심의위 심의 현황(2008년~2010년)

* 건수

구분	심의	시정요구 (심의 대비 비율)	이행 (시정요구 대비 비율)
2008	29,589	15,004 (50.7%)	14,997 (100%)
2009	24,346	17,636 (72.4%)	17,634 (100%)
2010	45,758	41,103 (89.8%)	40,662 (98.9%)
계	99,693	73,743 (74.0%)	73,293 (99.4%)

위에서 볼 수 있듯이 방통심의위에 의해 심의의 대상이 된 게시물들은 거의 삭제 등 조치의 대상이 되고 있으며 시정요구를 받은 게시물 대부분이 인터넷망으로부터 완전히 제거되고 있다. 사실상 100%의 이행률은, 방통심의위의 시정요구가 수용자에 대하여 실질적 위력을 발휘하고 있음을 나타낸다. 따라서 사상의 자유시장에서 상호비판을 통해 인터넷 게시물의 유해성을 걸러내기보다 방통심의위의 시정요구를 통해 인터넷 게시물을 퇴출하고 표현게시물의 유통 여부를 정부기관의 판단으로 통제함으로써 인터넷상의 표현에 대하여 질서 위주의 사고만으로 규제하고 있다는 비판이 지속해서 제기되어 왔다.

하지만 방통심의위의 시정요구 성격을 두고 논란이 계속되었다. 방통심의위는 자신들은 행정청이 아니며 삭제 등 시정요구는 강제성이 없는 권고라고 주장해 왔고, 형식상 '권고'이기 때문에 이 시정요구의 법률적 지위가 '비권력적 행정지도'라는 분석도 있었다[29].

그러나 그 위원들은 국가공무원법상 결격사유가 없어야 하고 그 신분이 보장되며 위원 중 위원장과 부위원장을 포함한 3인은 상임으로 임명되고 형법 등의 벌칙 적용에서 공무원으로 간주되는 한편, 국가가 기관의 운영 등에 필요한 경비를 지급할 수 있고 기관의 규칙이 제정·개정·폐지될 경우

29) 지성우, "현행 통신심의제도의 법적 문제점에 대한 고찰", 『정보인권의 법적 보장과 그 구체화 공동학술세미나』, 국가인권위원회, 2010.12.23. 참고.

관보에 게재·공표된다는 점에서 방통심의위는 방송통신위원회와 마찬가지로 합의제 행정청에 해당하고 그 시정요구는 행정처분에 해당한다고 보는 것이 타당하다는 것이 법원의 판단이다.[30] 헌법재판소 또한 방통심의위를 공권력 행사의 주체인 국가행정기관이라 인정할 수 있고, 그 시정요구에 대해서는 ▲정보통신서비스제공자 등에게 조치결과 통지의무를 부과하고 있고, ▲정보통신서비스제공자 등이 이에 따르지 않는 경우 방송통신위원회의 해당 정보의 취급거부·정지 또는 제한명령이라는 법적 조치가 예정되어 있으며, ▲행정기관인 방통심의위가 표현의 자유를 제한하게 되는 결과를 발생을 의도하거나 또는 적어도 예상하였다 할 것이므로, 단순한 행정지도로서의 한계를 넘어 규제적·구속적 성격을 갖는 것으로서 헌법소원 또는 항고소송의 대상이 되는 공권력의 행사라고 보는 것이 타당하다고 판단하였다.[31]

방통심의위의 시정요구가 일종의 행정처분에 해당한다고 할 때 게시자 등에 대한 사전고지와 청문 절차가 규정되어 있지 않은 점은 큰 결함이다. 이러한 이유로 2010년 9월 국가인권위원회는 방통심의위가 게시자들의 표현의 자유를 제약하면서 직접 통지를 하지 아니하고 사전적으로 의견 제출할 기회를 보장하지 않는 것은 헌법 제12조의 적법절차원칙을 위반할 소지가 매우 크다고 판단하였다.[32]

무엇보다 행정부가 자의적으로 게시물의 불법성을 판단하고 게시물의 삭제 등 인터넷망으로부터의 제거를 사실상 강제하는 것은 표현의 자유 침해이다.[33] 먼저, 행정기관은 사법부와 달리 정치권력으로부터 독립성이 보장되어 있지 않아 그 판단이 자의적이거나 정치권력을 비호하는 용도로 동원될 가능성이 있고 사법심사의 가능성이 존재하는 한 행정기관의 판단 또는 처분은 잠정적일 수밖에 없다. 국가인권위원회는 이러한 상황에서 인터

30) 서울행정법원 2010.2.11. 선고 2009구합35924 판결.

31) 헌재 2012.2.23, 2011헌가13 결정.

32) 국가인권위원회, "정보통신심의제도에 대한 개선 권고", 2010.9.30자, 〈http://www.humanrights.go.kr/02_sub/body02_v.jsp?id=2671&page=14〉.

33) 박경신, 앞의 글, 82쪽.

넷 심의제도가 사후심의라고 할지라도 행정기관이 자의적으로 행사할 수 있는 재량의 폭이 한정되어 위축 효과가 방지될 정도로 심의대상과 심의기준이 명백하지 않은 한, 방송통신위원회의 심의 및 시정요구는 표현의 자유에 대한 중대한 침해에 해당하고 그 결과 현행 헌법이 검열제도를 금지하는 취지에 부합되지 않을 소지가 있다고 보았다.

특히 국가보안법 위반과 관련한 심의는 법원의 심사 전에 정보·수사기관인 경찰과 국가정보원의 요청에 따라 방송통신위원회와 방통심의위의 심의가 이루어지며, 그 인용과 이행률이 100%에 달하는 문제는 심각하다.[34] 극소수 이행을 하지 않는 운영자에게는 방송통신위원회의 '취급 거부 · 정지 또는 제한'의 명령이 떨어진다. 지난 2003년부터 2011년 4월에 이르기까지 이루어진 방송통신위원회의 '취급 거부·정지 또는 제한'의 명령에 따라 처분된 3,716건의 게시물은, 모두 정보통신망법 제44조의7 제1항 8호, 즉 국가보안법 위반에 대한 것이었다.[35] 최근에도 한국대학생총학생회연합 사이트가 이 명령에 따라 폐쇄되었고 같은 방식으로 인권운동사랑방, 노동전선 등 인권노동운동단체에도 게시물 삭제 명령이 내려졌다[36].

그 밖에도 기관별 심의 신청 및 결과 현황 통계(2010년 1월 1일~12월 31일)에서 전체적으로 경찰 등 중앙행정기관 및 공공기관의 비율이 압도적이며 그 시정요구와 이행 비율도 상당히 높다는 사실을 볼 수 있다.

즉, 방통심의위는 공공기관 요청을 사실상 그대로 수용함으로써 본 심의제도를 통해 공공기관의 요청을 검증한다는 제도의 취지를 제대로 살리지 못하고 있으며, 중앙행정기관을 비롯한 공공기관이 이 제도를 국민의 비판을 통제하기 위한 수단으로 남용할 여지가 있다. 실제로 여러 사례에서 방통심의위 행정심의가 표현의 자유를 침해한다는 지적이 계속되어 왔다.

---

34) 2008년 발족 후부터 2010년 7월까지. 최문순 의원 보도자료 2010.10.19.

35) 방송통신위원회 2011.5.25. 정보공개에 의함

36) 2011.11. 이들 명령에 대한 행정소송이 각기 제기되었다.

〈표 3〉 방통심의위에 대한 기관별 심의 신청 및 결과 현황(2010년)

구분	심의	시정요구 (심의 대비 비율)	이행 (시정요구 대비 비율)
경찰 등 중앙행정기관	13,086	12,772 (97.6%)	12,127 (94.9%)
한국마사회등 기타 공공기관	8,472	8,425 (99.4%)	8,385 (99.5%)
온라인서비스제공자	599	25 (0.4%)	25 (100%)
일반인	10,693	8,333 (77.9%)	8,195 (98.3%)
합계	32,850	29,555 (89.9%)	28,732 (97.2%)

2008년 7월, 방통심의위는 소비자들이 작성한 불매운동 게시물이 '위법적인 2차 보이콧'이라며 '삭제'를 결정하였고 이에 대한 헌법소원이 제기되었다(2008헌마500). 문제의 게시물들은, 조선·중앙·동아 등 3개 지배적 신문사의 촛불시위 왜곡보도에 항의하고 불매운동을 하기 위하여 일반 시민이 해당 신문사에 광고를 게재한 기업들의 명단과 공개된 전화번호를 목록화한 것들이었다. 방통심의위의 이와 같은 조치는 헌법상 표현의 자유와 소비자의 권리를 침해하는 위헌적인 공권력 행사라는 비판이 제기되었다.[37] 2009년 4월, 방통심의위는 환경운동가가 '발암성 폐 쓰레기 시멘트'를 비판한 게시물에 대하여 시멘트회사의 명예를 훼손하였다며 '삭제' 결정을 하였다. 2010년 2월, 서울행정법원은 이 게시물 삭제를 취소하라고 판결하였지만, 방통심의위가 항소하였고 서울고등법원은 관련 법률에 대하여 위헌법률심판제청을 결정하였다. (2011헌가13).

하지만 이와 같은 문제 제기에 대하여 헌법재판소는 방통심의위의 직무에 관한 법률들이 명확성 원칙, 포괄위임입법금지 원칙, 법률유보원칙, 과잉금지원칙에 위배되지 않는다고 함으로써,[38] 표현의 자유에서 명확성의

37) 황성기, "신문사 광고주 관련 정보에 대한 방송통신심의위원회의 위법 결정의 헌법적 문제점", 공법학연구 제10권 제2호, 2009. 참고.

38) 헌재 2012.2.23, 2008헌마500; 헌재 2012.2.23, 2011헌가13.

원칙이나 과잉금지의 원칙을 아예 포기하는 결과를 초래했다는 비판을 받고 있다.

그 밖에도 방통심의위는 2010년 8월 19일, 국외 사이트인 트위터의 계정 '@우리민족끼리'의 개인 페이지 URL(http://twitter.com/uriminzok)을 국가보안법 위반으로 접속차단 시정요구를 하기도 하였다.

무엇보다 방통심의위가 대통령과 정부, 정치인을 비판하는 게시물에 대하여 명예훼손 등 불법이라며 삭제하는 것은 공공적인 비판을 크게 위축시켜 왔다. 방통심의위는 2008년 5월 28일, 다음 카페 '이명박 탄핵을 위한 범국민운동본부'에 올라온 게시글을 심의해 '언어 순화와 과장된 표현의 자제 권고'를 내렸다. "이명박 아주 지능형입니다"라는 글에서 이 대통령의 영문 이니셜 MB를 컴퓨터 메모리용량에 빗대 '머리용량 2MB', '간사한 사람' 등으로 표현한 것이 인격을 폄하한다는 것이었다. 2011년 5월에는 대통령에 대한 욕설을 연상시킨다는 이유로 한 트위터 이용자 개인 페이지 URL(http://twitter.com/2MB18nomA)이 차단되었다.

2009년 1월에는 김문수 경기도 지사의 발언이 식민지적이라며 비판하고 사퇴를 요구하는 게시물에 대하여, 2009년 7월에는 오세훈 서울시장이 재향군인회에 금품을 지급한 것을 비판한 게시물에 대하여 각각 명예훼손이라며 '삭제' 결정을 내렸다. 경찰 역시 방통심의위에 대통령이나 경찰을 비판하는 게시물에 대해 적극적으로 삭제를 요구해 왔다. 2008년 7월에는 경찰이 방통심의위에 대통령과 정부를 비판한 게시물 199건을 삭제할 것을 요청했다는 사실이 알려져 물의를 빚기도 하였는데, 방통심의위는 이중 일부에 대한 '삭제'를 결정하였다. 2009년 6월에는 노동절 집회 참가 시민을 향해 장봉을 휘두른 경찰의 모습을 담은 보도사진과 이름을 게재한 게시물에 대하여 '초상권' 침해라며 '삭제' 결정을 하였다. 천안함 침몰 사건이나 연평도 포격 사건에 대하여서도 정부와 다른 견해를 표방한 게시물들을 삭제 처리하였고 대통령에 대한 욕설 게시물이나 인터넷 게시물도 다수 삭제 혹은 접속 차단해 왔다.

이러한 사례를 검토한 유엔 표현의 자유 특별보고관은 방통심의위가 △기관의 독립성을 충분히 보장할 수 없고 △온라인 정보를 규제하는 데 있

어 중개업체들에 상당한 권한을 발휘할 수 있고 △정보통신망법상 '불법정보'의 유형이 명확하지 않고 광범위하며 △방통심의위가 명예훼손이라는 구실로 공익 정보에 대한 차단이나 삭제 권고를 하지 않도록 보장하는 데 필요한 투명성, 책임성, 정밀성이 미흡하고 △정부나 유력한 기업들을 비판하는 내용의 정보를 삭제하는 사실상의 사후 검열기구로 기능하지 않도록 보장할 수 있는 안전장치는 미흡하다는 점에 우려를 표하였다.

2) 명예훼손 및 사생활 침해에 대한 임시조치

행정심의와 달리 임시조치는 포털 등 온라인 사업자에 의해 이루어진다. 현행 정보통신망법 제44조의2, 일명 '임시조치' 조항에 의하면 어떤 정보에 의해 사생활 침해나 명예훼손을 당했다고 주장하는 사람이 그 정보의 삭제 등을 요청하면 온라인 사업자가 해당 정보를 삭제할 수 있다.

즉, 정보통신망법 제44조의2 제1항, 제2항, 그리고 제4항은 타인이 특정 게시물에 의해 권리가 침해되었다고 주장하면서 그 게시물의 삭제를 요청하기만 하면 정보통신서비스제공자는 반드시 이를 삭제하거나 "권리침해에 관한 판단이 어렵거나, 분쟁이 예상되는 경우에는" 최소한 임시조치를 하도록 하고 있다. 여기서 임시조치란 "해당 정보에 대한 접근을 임시로 차단하는 조치"를 말하며 "임시조치의 기간은 최대 30일 이내로 한다."고 되어 있다. 이 법의 목적은 타인의 권리를 침해하는 인터넷상의 게시물들을 신속하게 차단하려는 것에 있다.

그런데 동조 제6항[39]은 온라인 사업자들이 임시조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다고 규정하였을 뿐, 게시자가 재게시를 요구하는 경우 해당 게시물의 처리를 어떻게 할 것인지에 대해 명확한 규정이 있지 않다[40]. 이 때문에 온라인 사업자들이 임시조치를 취하지 않

39) ⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

40) 저작권 위반 게시물에 대한 유사한 조치의 경우 법률로 재게시 규정을 두고 있다.

을 때 예상되는 손해배상 책임[41]을 감수하지 않기 위하여 임시조치 요청에 광범위하게 응하게 되었다. 하지만 재게시 절차가 보장되고 있지 않기 때문에 부당하게 임시조치되었다 하더라도 게시자가 권리를 회복하기가 쉽지 않으며, 설령 30일이 지나 복구된다 하더라도 그 글의 효력은 게시가 금지되는 동안 끝났을 수밖에 없다.

위 조항들의 총체적 효과는 게시물이 그 합법성과는 무관하게 누군가 불법이라고 주장만 하면 억제될 수 있다는 것이며 그렇다면 정보통신망을 통하여 타인에게 피해를 주는 게시물을 규제한다는 입법목적에 비추어 헌법상 과잉금지의 원칙을 명백히 위반하는 것이다[42]. 가장 큰 문제는 이 제도가 정부나 정치인이 자신에 대한 비판을 신속하게 삭제하는 목적으로 사용되고 있다는 점이다.

2007년 11월 14일, 오세훈 서울시장이 서울 광장에서 집회를 전면 불허하겠다고 밝힌 것을 비판한 블로그 게시물이 서울시의 요구로 임시조치되었다[43]. 2008년 5월과 7월에는 경찰청장의 동생을 비판한 인터넷 게시물들이 경찰의 요구로 임시조치되었다. 이 게시물들은 어청수 경찰청장의 동생이 투자한 호텔의 불법 성매매 의혹에 대해 대전문화방송이 보도한 영상을 포함하고 있었고, 경찰청은 구글 유튜브 등 14곳의 인터넷 사이트에 대해 대량으로 게시물 삭제를 요청하였지만, 원출처인 방송국에 대해서는 어

「저작권법」 제103조(복제 · 전송의 중단) ③제2항의 규정에 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.

41) 게시물 삭제 요청에 응하지 않았다는 이유로 운영자가 손해배상을 해 주어야 하는 경우가 많아지고 있다. 2009년 4월 16일, 대법원은 피해자의 게시물 삭제 요구에 응하지 않은 NHN과 다음커뮤니케이션, 야후코리아 등 3개 포털에 대해 제기된 손해배상 청구소송에서, 피해자에 3천만 원을 지급하도록 한 원심을 확정했다. 대법원 4009.4.16. 선고, 2008다53812 손해배상(기) 등.

42) 박경신, “인터넷 임시조치제도의 위헌성 : 남이 싫어하는 말은 30일 후에 하라”, 중앙법학 제11집 제3호, 2009년 10월, 7쪽.

43) 임시조치 사례들은 대부분 오병일, “표현의 자유 침해하는 한국의 인터넷 규제 정책”, 국회 미디어발전국민위원회 공술문(2009.5.15.) 참조.

떠한 대응도 하지 않았다[44]. 2008년 10월, 한나라당 주성영 의원을 '만취한 채 폐 끼친다'고 지적하고 그의 미니홈피를 링크한 석 줄짜리 게시물이 해당 의원의 신고에 따라 임시 조치되었다. 2009년 4월에는 철거민들이 경찰 진압 과정에서 화재로 숨진 용산 참사에 대하여 여당 의원들의 발언 내용을 링크하고 이들을 '인두겁을 쓴 이들'이라고 비판한 게시물이 한나라당 장제원 의원의 신고로 임시 조치되었다. 또 2009년 4월 고 장자연 씨 관련 조선일보 방상훈 사장의 성 접대 의혹을 거론한 게시물들이 해당 신문사의 신고로 임시 조치되었다. 후에 법원이 관련 의혹을 제기한 민주당 이종걸 의원의 게시물이 명예훼손 손해배상 대상이 해당하지 않는다고 판결하였지만[45], 같은 의혹을 다룬 일반 이용자들의 글 수백 건이 임시 조치된 뒤였다. 2009년 5월, 경찰은 노동절 집회에 참석한 비무장 시민에게 경찰간부가 진압봉을 휘두른 폭력 행위를 비판한 게시물들에 대해서도 임시조치를 요구하였다. 삭제된 게시물들은 언론에 보도된 사진에 기반을 둔 것이었으며, 삭제된 게시물 중에는 한 블로거가 해당 경찰간부에게 정중하게 쓴 공개 질의서도 포함되어 있었다. 경찰은 이 게시물들에 대한 임시조치와 별도로 방통심의위의 심의를 요청하여 6월 삭제 결정이 내려지기도 하였다.

이러한 임시조치 제도는 노동조합이나 소비자의 기업 비판 게시물을 삭제하는 데에도 남용되고 있다. 2007년 8월 이랜드-뉴코아 노동조합 관련 게시물들이 사측인 '이랜드월드' 측의 요청으로 대량 임시조치되었다. 심지어 소비자 가격을 비교한 게시물이나[46] 자사의 상품에 대해 부정적인 평가를 한 게시물에 대해서도 기업이 임시조치를 요구하여 삭제된 사례가 보고되었다.

---

44) "사이버수사대는 경찰청장 해결사?", 주간경향 2008.8.5.

45) 2011년 11월 30일 서울중앙지법은 조선일보가 "허위보도로 명예가 훼손당했다"며 MBC와 신경민 당시 뉴스데스크 앵커, 보도본부장을 상대로 낸 16억원의 손해배상 청구소송에서 원고 패소 판결했다. 또 이종걸, 이정희 의원을 상대로 낸 10억원의 손해배상 청구소송에서도 원고 패소 판결했다. "조선일보·방상훈, '장자연 소송' 졌다", 미디어오늘 2011.11.30.

46) "포털, 블로그 글 동의없이 마구 삭제", 한겨레 2007.8.30.

유엔 표현의 자유 특별보고관은 임시조치 제도에 대하여 △사생활 침해나 명예훼손 여부에 대한 심사는 중개인, 즉 민간업체가 아니라 '독립적 기구'에 의해 이루어져야 하고 △중개인의 책임의 범위가 모호하게 규정된 법령으로 말미암아 중개인에 온라인 콘텐츠를 규제할 수 있는 과도한 권한을 줬고 △중개인들이 책임을 회피할 목적으로 정보를 삭제하거나 접근을 차단함으로써 과오를 범하는 결과를 유도할 수 있다고 지적하였다. 특별보고관은 더불어 임시조치를 당한 게시자가 이의를 제기한다 하더라도, 서비스 제공자의 후속조치가 모호하다는 점도 지적하고 있다. 비판을 검열하려는 정치인에 의해 남용될 가능성을 포함하여 자의적이고 과도한 제한으로부터 표현의 자유에 관한 권리를 보호할 수 있는 보장책은 전무한 상태라는 점 또한 우려하였다. 특별보고관은 결론적으로 중개인의 법적 책임을 규정한 법률 조항을 삭제할 것을 권고하였다.

그러나 정부는 운영자가 임시조치를 이행하지 않으면 과태료를 부과하는 내용으로 오히려 임시조치를 강화하는 정보통신망법 개정안(의안번호: 182396)을 국회에 제출했다.

3) 저작권 침해에 대한 임시조치와 삼진아웃 제도

지난 2009년 6월, 한 네티즌이 손담비의 '미쳤어' 음악에 맞춰 율동을 하는 5세 딸의 동영상을 자신의 블로그에 올렸다가, 한국음악저작권협회의 저작권 침해 주장에 의해 삭제되었다. 해당 블로거는 이에 대해 소송을 제기했고, 다행히 1심 및 항소심 법원은 이를 공정이용으로 인정했다. 그러나 대다수의 게시글은 권리자 단체의 '묻지마 삭제' 요구에 아무런 항변의 권리도 없이 삭제되고 있다. 디지털 환경에서 불법복제로 인한 저작권 침해만이 조명되고 있지만, 이용자들의 정당한 표현이나 커뮤니케이션 행위가 규제당하는 일이 비일비재하다. 예컨대, 지난 2005년에는 KBS의 인기 드라마 '불멸의 이순신'의 팬 카페에 올려진 동영상이나 사진에 대해 KBS가 삭제 요구를 한 바 있으며, 같은 방식으로 방송프로그램 캡처 화면이 포함된 블로그 포스팅이 사라지고 있다. 이는 인터넷상에서 이루어지는

이용자들의 UCC, 인터넷 방송, 블로그 포스팅, 카페를 통한 소통 행위가 단지 타인의 저작물을 포함한다는 이유로 저작권 침해로 규정되고 있기 때문이다.

「저작권법」은 배타적 권리를 강화하는 방향으로 끊임없이 개정되고 있다. 2006년 저작권법 전문개정을 통해 P2P, 웹하드 등 특수한 유형의 온라인서비스제공자에 필터링 등 기술적 조치를 의무화하였고, 2009년에는 소위 '저작권 삼진아웃제'를 내용으로 한 개정안이 통과되었다. 저작권 삼진아웃제는 저작권을 침해하였다는 경고를 3회 이상 받은 이용자 및 게시판에 대해 문화체육관광부 장관이 저작권위원회의 심의를 거쳐 최대 6개월 동안 이용자 계정 및 게시판의 운영을 정지할 수 있도록 하고 있다. 이는 방통심의위의 내용심의 및 방송통신위원회의 삭제명령과 유사한 구조로서, 사법적인 판단 없이 정부가 기본권을 제한한다는 점에서 마찬가지로 위헌적이다.

유엔 표현의 자유 특별보고관은 지적재산권을 명분으로 한 인터넷 차단, 특히 저작권 삼진아웃제가 표현의 자유에 미치는 영향에 대하여 각별히 언급하고 있다. 특별보고관은 "인터넷 통신 차단 여부의 통제가 중앙집권화"되고, 지적재산권 위반으로 "인터넷 접속을 차단한다는 제안들"에 대해 심각한 우려를 표하였다.

2011년 5월 한EU FTA가 국회에서 비준됨으로써 그 이행을 위해 「저작권법」 역시 개정되었다. 이에 따라 한국의 저작권 보호기간도 저작자 사후 70년으로 연장되었고, 접근 통제적인 기술적 보호조치도 「저작권법」에 포함하였으며, 저작권 규제를 보다 강력하게 집행할 수 있게 되었다. 또한, 2011년 11월 22일, 국회에서 날치기 통과된 한미 FTA가 발효되면 저작권은 더욱 강화된다. '일시적 복제'를 저작권법상 복제로 인정하여 인터넷 이용을 위축시킬 우려가 있으며, 법정손해배상제도 등 집행 조치가 한층 더 강화된다.

저작권법상 저작재산권의 제한, 즉 공정이용(fair use) 영역은 축소되고 있다. 지난 2010년 2월 19일, 문광부가 발의한 저작권법 개정안(의안번호: 189180)은 '저작권을 침해한 복제물임을 알면서 복제하는 경우' 사적 복제

를 인정하지 않는 내용을 포함하고 있다. 이는 소위 개인적인 '다운로드'를 불법화하겠다는 것인데, 그동안 인정됐던 '저작물의 사적 복제'를 위축시킬 것으로 우려된다. 개인적 영역에서 이루어지는 사적 복제를 어떻게 규제할 것인지, 그 실효성에 대한 비판이 제기되고 있으며, 이 조항의 효과적인 집행을 위해서는 개인의 인터넷 이용을 모니터링할 수밖에 없어 프라이버시 침해로 이어질 수 있다.

나. 형사처벌

음란, 명예훼손, 국가보안법이나 선거법 위반 등 표현물의 불법성을 이유로 형사처벌할 때 인터넷 표현물 역시 예외가 되지 않는다. 이들 법률의 표현의 자유 제한에 대해서는 별론으로 하고, 이 절에서는 인터넷 표현물을 형사처벌하는 데 고유하게 적용되어 온 두 개 법률의 현황과 문제점을 살펴보고자 한다. 먼저 「전기통신기본법」 제47조 1항, 일명 '허위의 통신' 조항은 1961년 12월 30일 제정된 후 사실상 사문화되어 있다가 이명박 정부 들어와 네티즌들을 구속 혹은 기소하는 데 사용되기 시작했다. 또한, 정보통신망법상 사이버 명예훼손 조항으로 기소되는 네티즌들이 최근 매우 증가했다는 사실도 주목해볼 필요가 있다.

1) 허위의 통신

2008년 5월 촛불시위 당시 소위 '광우병 괴담'을 엄단하겠다는 검경의 발표와 관련하여 1명의 청소년 네티즌이 '허위의 통신' 조항으로 불구속기소된 이래로,[47] 촛불시위 과정에서 사망설 등을 배포한 네티즌들이 이 조항에 의해 구속 및 형사기소되고 일부 유죄 판결을 받기도 하였다. 2009년

47) 이 청소년은 친구에게 "학생시위 – 5월17일 전국 모든 중고등학교 학생들 단체 휴교 시위, 문자 돌려주세요"라는 내용의 문자메시지를 보냈다가 허위의 통신 조항에 의해 기소됐다. 2010년 9월 9일 대법원에서 무죄가 확정되었다.

1월에는 정부의 경제 정책을 비판해 온 필명 '미네르바'라는 이용자가 '허위의 통신' 혐의로 구속 및 기소된 사건이 국내외에서 많은 관심을 받았다. 2010년 천안함, 연평도 사건 당시에 이 죄목에 의한 형사 소추가 다수 발생하였는데[48], 이들의 혐의 다수는 휴대전화나 인터넷 메신저를 이용하여 지인들에게 '예비군 소집' 등의 내용으로 장난 문자를 보내거나 정부의 발표 내용과 다른 내용의 통신을 한 것이 공익을 해할 목적의 허위사실 유포라는 것이었다.

천안함 사건에서 수사당국은 수사를 넘어서서 '허위사실유포'를 규제한다는 명목으로 여론을 통제했다. 경찰은 천안함 관련 게시물에 대해 방송통신심의위원회 등 관계기관에 심의·삭제를 요청하고 수사 처리하라는 엄단 방침을 내리는 한편 포털사이트에 천안함 관련 모니터링 강화 및 삭제를 요구하고 핫라인 구축을 주문했다는 사실이 밝혀졌다.[49]

이러한 상황에서 2010년 12월 28일 헌법재판소는 전기통신기본법 제47조 제1항 '허위의 통신' 조항이 위헌이라고 결정하였다. 결정의 주된 이유는 '공익' 개념이 불명확하다는 것이었다(2008헌바157). 이로 인하여 해당 조항에 의한 형사처벌 예정자는 구제되었으나, 법무부는 "헌법재판소의 위헌 결정으로 처벌규정의 공백이 발생하게 된 것에 대해 안타깝게 생각한다.…전쟁·테러 등 국가적·사회적 위험성이 큰 허위사실 유포 사범에 관한 처벌규정 신설을 신속히 추진하겠다"고 발표하는 등 대체 입법 방침을 밝혔다.[50]

여당 등 국회 또한 곧바로 대체 입법에 나섰다. 예컨대 "국가안전보장에 중대한 위험을 초래", "자유민주적 기본질서의 파괴와 사회혼란을 유도",

---

48) 2010년 12월 29일 대검찰청에 따르면 전기통신기본법 47조 1항을 근거로 입건된 천안함 · 연평도 사건 관련 허위사실 유포자는 총 47명에 달한다. 천안함 사건 입건자는 총 14명으로, 이중 5명 불구속기소, 7명 약식기소, 2명 기소유예처분을 받았고, 연평도 사건 입건자는 33명으로, 이중 29명 불구속 기소, 2명 기소유예, 2명 수사진행 중인 상태였다. "천안함·연평도 유언비어 47명 '위헌 수혜'", 뉴시스 2010.12.29.

49) 국회의원 최문순 보도자료 2010.6.25.

50) 법무부 보도자료 2010.12.28.

“공공복리의 현저한 저해”에 해당하는 표현물을 처벌하도록 하거나(의안번호: 1810562), “국가안전보장이나 사회ㆍ경제적 질서 또는 공공기관의 정상적인 업무수행을 해할 목적으로”라는 표현으로 명확성을 보완하려 하였고(의안번호: 1810595), “국가 안전보장의 위해”, “불법집회 및 불법시위의 참여유도를 통한 사회적 혼란 초래”, “증권시장, 외환시장 등에 관한 거짓 정보의 유통을 통한 경제적 혼란 유도”, “법집행에 대한 신뢰를 훼손하여 국민의 불안 조성”, “특정 종교나 정치단체의 비방” 등의 표현으로 처벌대상을 더욱 구체화하기도 하였다(의안번호: 1810936). “전기통신설비에 의하여 공공연히 허위의 사실을 주장하여 국가위기를 초래하는 폭력적 선동이 유발되거나 국민 경제상 막대한 피해를 야기한” 표현에 대하여 형사처벌하도록 한 법안도 발의되었다(의안번호: 1810978).

혹은 다른 법률을 이용하여 여전히 ‘허위의 통신’을 처벌하려는 시도가 계속됐다. 2011년 3월 경찰은 일본 원전 사고로 유출된 방사능 물질이 한반도에 상륙한다는 일명 ‘방사능 괴담’에 대하여 정보통신망법이나 경범죄처벌법을 통하여 공포심이나 불안감을 유발하는 통신을 처벌하겠다고 발표하였고,[51] 11월에는 검찰이 FTA에 반대하는 ‘허위사실 유포’를 하는 자에 대해 ‘원칙적으로 구속수사’하겠다고 밝혀[52] 논란이 일었다.

그러나 ‘허위의 통신’ 조항에 대한 의견서에서 국가인권위원회가 밝혔듯이, 허위사실유포에 대한 대처는 반박으로 가능하지만, 형사처벌로 모든 유형의 허위사실 유포행위를 일반적으로 금지하는 것이므로 합리적이지 않다. 국제사회는 허위표현금지규정에 따른 형사처벌 범위가 불명확하고 광범위하므로 표현의 자유를 침해할 우려가 크다는 지적을 지속해서 제기해 왔으며, 실제로 대부분 자유민주국가에는 이러한 허위표현금지규정이 존재하지 않거나 폐지되었다.

---

51) “일본 방사능물질 한국 상륙 루머관련, 수사착수”, 서울경찰청 보도자료(2011.3.16).

52) “한미FTA 비준 반대 불법집단행동 대비『공안대책협의회』개최”, 대검찰청 보도자료(2011.11.7).

2) 사이버 명예훼손

정보통신망법상 명예훼손으로 인한 형사 기소 사례가 계속 늘고 있다.[53]

〈표 4〉 정보통신망법 위반(명예훼손) 사건처리 현황

연도	기소	구속
2006년	701	16
2007년	844	10
2008년	841	6
2009년	1,033	6
2010년	1,065	0

일명 '사이버 명예훼손'이라 지칭되는 이 규정은 반의사불벌죄로서 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 다른 사람의 명예를 훼손한 자는 사실을 드러낸 경우 3년 이하의 징역이나 금고 또는 2천만 원 이하의 벌금에 처하고, 거짓의 사실을 드러낸 경우 7년 이하의 징역, 10년 이하의 자격정지 또는 5천만 원 이하의 벌금에 처하도록 하였다(동법 제70조). 이는 공연히 사실을 적시하여 사람의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만 원 이하의 벌금에 처하도록 하고, 공연히 허위의 사실을 적시하여 사람의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만 원 이하의 벌금에 처하도록 한 형법 제307호의 규정에 비하여 사이버상의 명예훼손을 가중처벌하는 것이다.

그런데 사이버 명예훼손에 공인과 공공기관이 명예훼손의 피해자로 나서는 사례가 늘고 있다. 2010년 3월 문화부는 피겨스케이트 스타 김연아 선수가 문화부 장관의 포옹을 피하는 듯한 영상을 배포하였다는 이유로 인터넷 이용자 8명을 명예훼손으로 형사고소 하였다가 취하하였다. 공인에

53) 대검찰청 2011.5.25. 정보공개에 의함.

대한 인터넷 비판 글에 대하여 명예훼손을 이유로 한 형사고소가 계속된다면, 후에 법원이 무죄 판결을 하더라도, 공공 비판에 대한 위축을 야기할 수 있다는 우려를 낳고 있다.

법원은 사이버 명예훼손에 있어서 △ 당해 명예훼손적 표현으로 인한 피해자가 공무원 내지 공적 인물과 같은 공인인지 아니면 사인에 불과한지 여부, △ 그 표현이 객관적으로 국민이 알아야 할 공공성·사회성을 갖춘 공적 관심 사안에 관한 것으로 사회의 여론형성 내지 공개토론에 기여하는 것인지 아니면 순수한 사적인 영역에 속하는 것인지 여부, △ 피해자가 그와 같은 명예훼손적 표현의 위험을 자초한 것인지 여부, △ 그 표현으로 훼손되는 명예의 성격과 그 침해의 정도를 고려하여 판단하여야 할 것이고, 특히 공인의 공적 활동과 밀접한 관련이 있는 사안에 관하여 진실을 공표한 경우에는 원칙적으로 공공의 이익에 관한 것이라는 증명이 있는 것으로 보아야 할 것이며, 행위자의 주요한 동기 내지 목적이 공공의 이익을 위한 것인 이상 부수적으로 다른 개인적인 목적이나 동기가 내포되어 있더라도 공공의 이익에 관한 것으로 봄이 상당하다고 보고 있다(2005도3112; 2009도14890 등).

유엔은 여기서 더 나아가 명예훼손에 대한 형사처벌 조항 폐지를 권고하였다. 유엔 표현의 자유 특별보고관은 명예훼손이 여전히 형사상 범죄로 남아 있는 것은 본질적으로 가혹한 조치이며 표현의 자유에 관한 권리를 부당하게 위축시키는 효과를 야기한다고 지적하면서 대한민국 정부에 형사상 명예훼손죄를 삭제할 것을 권고하였다. 특별보고관은 특히 공무원, 공공기관 및 기타 유력 인사들에 대한 비판을 포함하여 비판적 의견을 수용하는 문화를 조성할 것을 대한민국 정부에게 촉구하며, 이러한 문화는 민주주의의 필수 요소라고 꼬집었다.

다. 이용자정보 제공

이용자정보 제공은 표현물을 직접 규제하지는 않지만 간접적으로 이용

자를 위축시키는 효과(chiiling effect)가 있다.

1) 인터넷 실명제

2004년부터 각 국민에게 출생 시 부여되는 주민등록번호를 토대로 '의무적 인터넷 실명제'가 도입되었다. 인터넷 실명제는 익명 표현의 자유를 침해하고 국민의 정치참여를 위축시키며, 각 인터넷 사이트로 하여금 민감한 개인정보인 주민등록번호의 수집과 오남용을 부추긴다는 점에서 비판을 받고 있다.

2004년 개정된 「공직선거법」에 따르면 선거운동 기간 중 모든 인터넷언론 게시판은 실명확인이 된 이용자에 한하여 글쓰기를 허용해야 하고, 관련된 기술적 조치를 취하지 않으면 1천만 원 이하의 과태료 처분을 받는다(동법 제82조의6 및 제261조). 2006년 5월 지방선거에서 실명제 시스템을 거부한 '민중의 소리'가 과태료 처분을 받았으며, 2007년 12월 대통령선거에서 실명제 시스템을 거부한 '참세상'이 1천만 원의 과태료 처분을 받았다. 2007년 12월은 대통령선거 시기이기도 하였지만 '차별금지법안'을 둘러싼 논란이 커질 때였다. 성별, 연령, 인종, 피부색 등 13개 영역에 대한 차별을 금지했던 본래 법안이 입법 과정에서 병력, 출신국가, 성적지향, 학력, 가족형태, 언어, 범죄경력 등 7개 영역을 삭제한 것을 두고 논쟁이 벌어졌다. 하지만 성소수자 등 이 법안의 이해당사자들은 인터넷언론 게시판에서 벌어지는 논쟁에 참여할 수 없었다. 자신의 정체성이 실명으로 노출될 수 있기 때문이었다. 또한, 대통령 후보자들의 입시 정책에 대해 공개적으로 평가할 계획이었던 한 청소년 단체의 활동이 실명제 때문에 크게 위축되었다. 이 단체는 자신들의 활동에 호응하는 청소년들이 실명 인증을 하고 인터넷에 글을 쓰는 과정에서 주민등록번호상 나이가 노출되어 불이익을 받을 것을 우려하였다. 현행 「공직선거법」은 청소년의 선거운동을 금지하고 있기 때문이다. 그러나 2010년 2월 헌법재판소는 「공직선거법」상 인터넷 실명제가 표현의 자유 침해가 아니며 합헌이라고 결정하였다.[54] 헌법재판소 결정의 취지는 인터넷이용자가 스스로 판단에 따라 실명확인 절

차를 거치거나 거치지 않고 자신의 글을 게시할 수 있으므로 사전검열금지의 원칙에 위배된다고도 할 수 없다는 것이었다.

〈표 5〉「공직선거법」상 인터넷 실명제 적용 인터넷 언론사 현황[55]

구분	실명제 실시	실명제 회피 (게시판 잠정폐쇄)	실명제 거부 (과태료 부과)
18대 국회의원선거 (2008.4.)	834	452	0
17대 대통령선거 (2007.12.)	880	259	1
제4회 지방선거 (2006.5.)	483	172	1

2007년 개정된 정보통신망법에 따르면, 일일 방문자 수 10만 명 이상의 포털, 언론, UCC 사이트들은 상시적으로 본인확인이 된 이용자에 한하여 글쓰기를 허용해야 하고, 관련된 기술적 조치를 취하지 않을 경우 3천만 원 이하의 과태료 처분을 받는다(동법 제44조의5 및 제76조 제1항 제6호)[56]. 이명박 정부 들어 실명제의 대상 확대를 둘러싸고 논란이 더욱 불거졌다. 2009년 2월 대상사이트가 37개에서 구글 코리아를 포함한 153개로 확대되었으며, 다시 2010년 2월 167개를 거쳐 2011년 3월 146개 웹사이트에 적용되었다. 적용대상 사업자 선정 과정에서 페이스북, 트위터, 미투데이 등 SNS(소셜네트워크서비스)는 사적 커뮤니케이션 영역이라는 이유로 제외되었고, 이 때문에 국내사업자 역차별 논란이 불거지기도 하였다. 대상을 더욱 확대하기 위한 정부의 개정 법률안(의안번호: 1802396)이 국회에 발의되었다.

인터넷 실명제에 대한 문제 제기는 끊이지 않고 계속됐다. 2010년 1월

54) 2010.2.25. 2008헌마324, 2009헌바31(병합).

55) 출처: 중앙선거관리위원회 각 선거 총람 종합

56) 이 법에서는 '제한적 본인확인제'(제44조의5)라는 표현을 쓰고 있으나, 이 제도가 인터넷 실명제와 본질적인 측면에서 같다는 점에서 본 글에서는 크게 구분하지 않았다.

과 4월 정보통신망법상 인터넷 실명제에 대한 헌법소원이 제기되었다[57]. 2009년 4월 구글 코리아는 한국 정부가 요구한 본인확인제를 적용하지 않겠다고 발표한 후 '한국' 설정 이용자의 글쓰기를 중단하였고, 한국 정부는 구글의 서버가 국외에 있으니 실명제 의무가 적용되지 않는다고 태도를 바꿨다. 한국 인터넷 이용자들 가운데에서는 실명 인증을 하는 국내 사이트에서 구글 등 국외 사이트로 이메일 계정이나 블로그를 옮기는 '사이버 망명'이 늘고 있다.

한편, 2009년 개정된 「인터넷 주소자원에 관한 법률」에 따르면, 인터넷 도메인을 사용하려는 자가 실명이 아닐 경우 인터넷주소관리기관은 그 도메인이름을 말소해야 하고, 관련된 조치를 취하지 않으면 1천만 원 이하의 과태료 처분을 받는다(동법 제11조 및 제27조). 2011년 개정된 「게임산업진흥에 관한 법률」에 따르면, 게임물 관련 사업자에는 게임물 이용자의 회원가입 시 실명·연령 확인 및 본인 인증을 비롯하여 게임물 이용자의 게임 과몰입과 중독을 예방하기 위한 조치를 취해야 하며, 이러한 조치에 대한 문화체육관광부 장관의 자료 제출 또는 보고 요청에 따르지 않을 경우 2년 이하의 징역 또는 2천만 원 이하의 벌금, 1천만 원 이하의 과태료에 처해진다(동법 제45조, 동법 제48조).

유엔 표현의 자유 특별보고관은 인터넷 실명제에 대하여 △익명성을 기반으로 하는 표현의 자유에 영향을 미치고 △정부에 비판적인 사람들이 자신의 견해를 밝힘으로써 받게 되는 형사상 제재를 두려워하여 의견 표명을 꺼리는 경향을 보일 것이라는 데 우려를 표하고 대한민국 정부에 다른 신분 확인 수단을 검토하고 그러한 수단도 신분 확인 대상자가 범죄를 저질렀거나 저지르려고 한다는 상당한 근거나 합리적인 의심이 있는 때에만 사용하도록 권고하였다. 특별보고관이 언급한 '다른 수단', 즉 범죄자를 식별하여 신원을 추적하는 절차는 이미 통신비밀보호법 등 국내의 타법에 잘

57) 헌법재판소 2010헌마47, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 제1항 제2호 등 위헌확인(심리중); 헌법재판소 2010헌마252 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 제1항 제2호 등 위헌확인(심리중)

규정이 되어 있으므로 이 관점에서는 인터넷 실명제가 궁극적으로 폐지되어야 마땅하다.

2011년 7월 SK커뮤니케이션즈에서 운영하는 네이트와 싸이월드 이용자 3천5백만 건의 개인정보가 유출된 사건을 기하여, 인터넷서비스제공자의 개인정보 유출 위험성을 증대시키는 주요 원인으로 인터넷 실명제가 비판을 받고 있다. 국회 입법조사처는 "주요 국외국가들과 비교하면 우리나라 포털 사이트의 개인정보 유출 위험성은 더욱 크다고 할 수 있는데, 그 핵심적인 빌미를 제공해 주고 있는 것이 바로 인터넷 실명제 의무화 조항"이라고 꼬집으며 인터넷 실명제 관련 규정들을 재고하여 식별번호 자체의 수집을 자제하는 방향으로 법과 제도를 개선하도록 권고하여 눈길을 끌었다.[58]

2) 통신자료와 통신사실확인자료 제공 및 감청

인터넷 실명제 의무화 등 때문에 온라인 사업자들은 이용자의 개인정보를 상시로 보관하고 수사기관의 요청에 협조해 왔다. 수사기관이 이용자의 개인정보를 요청하는 과정에서 법원의 허가는 불필요하거나 형식적인 데 그치고 있다. 이 때문에 뚜렷한 범죄 혐의가 없는 이용자의 개인정보들이 손쉽게 수사기관에 제공됐으며, 상시적인 인터넷 사찰 의혹이 불거지고 있다. 수사기관이 인터넷을 사찰하고 있다는 인식은 일반 시민으로 하여금 권력에 비판적인 게시물을 쓸 때 중대한 위축 효과를 낳는다.

「전기통신사업법」에 따르면 수사기관이나 정보기관이 전기통신사업자에게 이용자의 성명, 주민등록번호, 주소, 전화번호 등 통신자료를 요청할 때 서면에 의하도록 하였다. 그러나 서면 요청에는 범죄사실의 입증이나 법원의 영장이 불필요하며, 긴급할 때는 서면을 사후에 제출해도 된다(동법 제83조). 이 문제에 대하여 위헌논란이 있었고,[59] 헌법소원이 제기되어

58) 국회 입법조사처, "이슈와 논점: 네이트 해킹사고와 포털의 개인정보보호", 2011.8.9.

59) 오기두, "수사상 전자통신자료의 취득에 관한 헌법적 문제", 헌법논총 15집, 2004.12, 347~410쪽,

현재 심리 중이다(2010헌마439). 수사기관과 정보기관의 통신자료 요청은 해마다 급증하는 추세에 있으며 2010년 인터넷에 대한 통신자료 요청은 132,337건에 달했다.[60]

이메일 등 송·수신이 완료된 전기통신에 대한 압수·수색·검증이 남발되는 것도 문제이다. 「형사소송법」상 절차에 의해 이루어지는 이메일 압수·수색·검증은 법원의 영장을 통해 이루어진다. 그러나 대상 기간이 한정되지 않아 장기간의 이메일이 제공되기 일쑤인 데다가, 제3자인 통신사업자를 통해 간접적으로 강제 수사가 이루어지므로 일반 형사소송절차에서처럼 사전통지나 참여권을 보장받고 있지 못하다.[61] 2010년 천안함 사건 당시 경찰은 '허위의 통신' 혐의로 조사받는 네티즌들에 대하여 2009년 1월부터 압수된 이메일을 소급하여 검토하고 사상검증과 다름없는 추궁을 하여 논란을 빚었다.[62]

한편, 「통신비밀보호법」은 수사기관이나 정보기관이 온라인 사업자에게 글쓴이의 IP주소와 인터넷 로그기록 등 통신사실 확인자료를 요청할 때 법원의 허가를 받도록 하였으며 사업자의 협조 의무를 규정하였다(동법 제13조 등). 그러나 법원에 허가를 받을 때 범죄사실을 입증할 필요가 없으며, 긴급할 때는 법원의 허가를 사후에 받아도 된다. 수사기관과 정보기관의 통신사실 확인자료 요청은 해마다 급증하는 추세에 있으며 2010년 인터넷에 대한 통신사실확인자료 요청은 49,091건에 달했다.[63]

「통신비밀보호법」은 수사기관이나 정보기관이 온라인 사업자에게 인터넷 메일이나 비공개 글 등 통신비밀에 해당하는 내용에 대한 감청을 요청할 때 법원의 허가를 받도록 엄격히 규정하였다(동법 제5조 등). 그러나 실제로 법원에 영장을 받을 때는 그다지 엄격하게 심사되지 않기 때문에 법원의 기각률은 3%대에 그칠 뿐이다.[64] 긴급할 때는 사후에 영장을 받아도

60) 방송통신위원회, "'10년 하반기 감청 및 통신사실확인자료 제공 현황", 2011.5.4.
61) 박경신, "이메일압수수색의 제문제와 관련법률개정안들에 대한 평가", 『법학연구』(인하대학교) 제13집 제2호, 2010.8.
62) "전기통신법 47조 1항 '인권 감전사'", 위클리경향 제899호, 2010.11.9.
63) 방송통신위원회, 앞의 자료.

되며 36시간 이내 감청을 끝내면 영장이 불필요하다. 이 때문에 수사기관과 정보기관의 인터넷 감청은 해마다 급증하는 추세에 있다. 2010년 인터넷에 대한 감청은 723건이었다.[65] 대부분의 감청은 국내 일반범죄수사의 권한이 없는 국가정보원에 의해 시행되고 있기 때문에 더욱 문제가 심각하다. 2010년에는 정부 감청 통계 건수의 97%(전화번호 기준)가 국가정보원에 의해 시행되었다.[66] 특히 국가정보원은 개별 이메일이나 게시글이 아니라 인터넷 회선 전체에 대한 패킷 감청(Internet Deep Packet Inspection)을 해온 것으로 밝혀져 큰 사회적 충격을 주었다. 패킷 감청에 대해서는 헌법소원이 제기되어 현재 심사 중이다.[67] 한편 2009년 KT가 자사의 인터넷 회선망에서 DPI 기술을 사용하여 이용자의 통신 내용을 감청한 후 이를 토대로 한 맞춤광고 사업을 시작하여 DPI 기술의 상업적 사용에 대한 논란을 불러왔다.[68] 2011년에는 KT와 SKT 등 무선통신망을 점유하고 있는 이동통신사업자가 DPI 기술을 이용하여 자신의 이동통신망에서 타사의 경쟁서비스를 차별해 왔음이 알려져 통신비밀 침해와 망중립성 논란이 불거졌다.[69]

---

64) 2010년 등 국정감사 자료에 의함

65) 방송통신위원회, 앞의 자료.

66) 진보네트워크센터·경제정의실천시민연합, “경실련과 진보넷, mVoIP 제한 및 DPI 사용 SKT와 KT 고발”, 보도자료(2011.11.23).

67) 헌법재판소 2011헌마165, 통신제한조치허가위헌확인 등(심리 중).

68) 오마이뉴스, 2009.9.3. “KT '쿡 스마트웹'은 당신이 한 일을 알고 있다?”.

69) 진보네트워크센터 · 경제정의실천시민연합, “경실련과 진보넷, mVoIP 제한 및 DPI 사용 SKT와 KT 고발”, 보도자료(2011.11.23).

IV. 개선방향: 정책 과제

헌법재판소는 '불온통신의 단속' 위헌 결정에서 "온라인 매체상의 정보의 신속한 유통을 고려한다면 표현물 삭제와 같은 일정한 규제조치의 필요성 자체를 부인하기는 어렵다고 하더라도, 내용 그 자체로 불법성이 뚜렷하고, 사회적 유해성이 명백한 표현물 – 예컨대, 아동 포르노, 국가기밀 누설, 명예훼손, 저작권 침해 같은 경우가 여기에 해당할 것이다 – 이 아닌 한, 청소년보호를 위한 유통관리 차원의 제약을 가하는 것은 별론으로 하고, 함부로 내용을 이유로 표현물을 규제하거나 억압하여서는 안 된다. 유해성에 대한 막연한 의심이나 유해의 가능성만으로 표현물의 내용을 광범위하게 규제하는 것은 표현의 자유와 조화될 수 없다."고 판시한 바 있다. 이러한 기준에서는 현재 방통심의위의 행정심의가 갖는 위헌성을 누구도 부인하기 어렵다. 표현의 자유를 보장하는 인터넷 심의제도의 개선방향은 다음과 같이 제시될 수 있다.

1. 행정심의 폐지

정보의 불법성을 판단하고 처분하는 주체는 행정기관이 아니라 법원이어야 한다. 따라서 행정기관이 불법정보를 심의하여 삭제 또는 차단하는 행정심의 제도를 폐지하고, 그 근거가 되는 불법정보에 관한 규정(정보통신망법 제44조의7) 역시 폐지해야 한다. 행정기관에 의한 청소년유해매체물 지정 제도는 물론 기타 유해 정보에 대한 행정심의 역시 폐지되어야 한다.[70] 결국, 방통심의위의 행정심의 제도를 모두 폐지해야 한다는 것이다.

한편 사생활이나 저작권과 같이 특정인의 권리를 침해하는 정보는 그에 대한 신속한 위법 판단을 내리기 위해 법원의 전자가처분 신청제도를 활성화해야 한다.

---

70) 2011년 청소년유해매체물 심의에 대한 논란이 불거졌던 가요, 게임 심의는 민간자율심의로 전환중이지만 여전히 청소년보호위원회의 강제 규제 권한이 남아있어 이중규제 논란이 되고 있다.

2. 임시조치제도의 보완

인터넷 서비스를 운영하는 사업자들이 방조책임 등을 피하기 위하여 이용자 표현의 자유를 과도하게 규제하여 '사적 검열'에 이르지 않도록, 현재의 정보통신망법 제44조의2 상의 면책을 필요적 면책으로 전환해야 한다. 단, 현재 피해를 주장하는 자의 요청만으로 최소한 30일간 표현물이 억제되는 현 상황을 타개하기 위해 게시자가 복원을 요청할 경우 사업자가 이를 준수하는 경우에만 위의 면책이 부여되도록 하여야 한다.

3. 자율규제의 촉진과 공공적 운용

청소년유해매체물 대신 이용자의 선택권을 보장하기 위하여 표현물의 유해성 정도를 기술하는 자율적인 내용등급제를 도입한다. 다만 여성의 상품화 등 시장의 선정성을 공공적으로 규제하기 위하여 자율등급 제도의 운용 과정에 이용자의 참여를 보장하는 등 공공적 운용 방안이 모색되어야 한다.

국외에서는 민간 핫라인과 심의기구가 활발하게 활동하면서 아동 포르노 등 불법정보가 발견되면 사법기관 및 인터넷 사업자에 신고하는 역할을 수행하고 있다. 우리나라에서도 교사, 학부모, 아동보호단체 등 다양한 민간 핫라인이 자율적으로 활동하도록 제도적으로 촉진해야 한다.

다만 포털 사업자 등 주요 인터넷 서비스 운영 사업자들의 심의기구가 발휘할 영향력이 압도적일 것인 만큼 이 기구가 사적으로 부당한 검열을 하지 않도록 심의의 대상과 절차를 약관에 명시적으로 규정하고 심의 과정의 공정성과 공개성을 보장하는 한편 이용자의 참여를 보장해야 한다.

4. 저작물의 공정이용 보장

공적 지원을 받은 저작물에 대한 자유로운 이용 허용, 사적 복제 허용, 장애인 접근권 향상을 위한 저작권 제한 확대, 이용자들의 비영리적 표현 및 커뮤니케이션 보장 등 저작권으로 저작물에 대한 접근 및 이용자의 표현의 자유가 제한되지 않도록 공정이용 영역을 확대하는 저작권법 개정이

이루어져야 한다. 또한, '특수한 유형의 온라인서비스제공자'에 대한 필터링 의무화나 저작권 삼진아웃제 등 과도한 규제는 폐지되어야 한다.

5. 명예훼손과 허위를 이유로 한 형사처벌 폐지

사이버 명예훼손에 대한 형사처벌은 폐지되어야 한다. 특히 민사상 명예훼손 책임에 있어서도 국가·지방자치단체는 원고가 될 수 없으며, 진실한 사실의 표현에 대해서는 명예훼손의 책임을 물어서는 안 된다. 공무원의 소속기관이나 직무에 관한 표현에 대해서도 역시 표현자가 허위라는 사실을 알면서도 악의적으로 명예를 훼손한 경우가 아닌 한 손해배상의 책임을 물을 수 없다. 또한, 어떤 통신 내용이 '허위'라는 이유로 형사처벌해서는 안 된다.

6. 인터넷 실명제 폐지

공직선거법은 물론 정보통신망법, 「인터넷 주소자원에 관한 법률」, 「게임산업진흥에 관한 법률」 등 법률상 의무를 부과한 인터넷 실명제는 인터넷 이용자의 익명 표현의 자유와 개인정보에 대한 자기결정권을 침해하기 때문에 폐지되어야 한다.

7. 이용자정보 제공과 감청에 대한 법원의 통제 강화, 패킷 감청 중단

정보수사기관이 인터넷 이용자의 통신자료를 취득할 때는 법원의 심사가 예외 없이 적용되어야 한다. 통신사실확인자료를 취득할 때는 그 심사기준 및 연장절차 등이 더욱 엄격하게 법원에 의해 심사되어야 한다. 감청에 대해서는 법원의 심사가 지금보다 훨씬 더 엄격해져야 하며 특히 프라이버시침해의 광범위성 때문에 필연적으로 영장주의를 위배하게 되는 인터넷 패킷 감청은 어떠한 경우에도 허용되어서는 아니된다.

프라이버시 보호 정책 방향*

오병일 · 장여경
(진보네트워크센터)

1. 문제 제기

2011년 7월 SK커뮤니케이션즈가 운영하는 네이트와 싸이월드에서 3,500만 건의 개인정보가 유출되었다. 이는 지난 2008년 발생한 옥션의 1,800만 건 개인정보 유출 사고 이후 최고 기록을 경신한 것으로서, 옥션 사고 이후로도 2008년 (구)하나로텔레콤 600만 명, 2011년 현대캐피탈 42만 건, 넥슨 1,320만 명 등 정보통신 분야에서 대규모 개인정보 유출 사고가 계속되어 왔다.

다른 한편으로 최근에는 스마트폰을 통한 위치정보 수집의 문제가 또 다른 관심을 끌었다. 2011년 4월 아이폰의 위치정보 수집관련 국내외 언론 보도가 이루어지자, 방송통신위원회는 애플과 구글의 미국 본사 위치정보 시스템에 대한 현장점검을 거쳐, 2011년 8월 애플 및 구글의 위치정보보호 법규 위반행위에 대해 시정요구 및 과태료를 부과하였다[1].

---

* 이 글은 2012년 제19대 총선을 앞두고 1월 29일 발간된 『미디어 생태계 민주화를 위한 2012 정책보고서』(미디어커뮤니케이션네트워크 편저)에 게재된 원고이다.

1) 방송통신위원회, “방통위, 애플 및 구글의 위치정보보호 법규 위반행위에 대해

또한 통신 기록과 내용이 관련 법률과 이용자의 의사에 의해 장기간 저장되기 시작하면서, 이를 이용한 통신 수사가 크게 증가해 왔다. 특히 2008년 이명박 정부의 등장 이후 수사기관이 전국교직원노동조합, YTN 노동조합 등에 대해 장기간의 이메일을 압수수색하는 일이 발생하였고, 2009년 6월에는 검찰이 PD수첩을 수사하는 과정에서 작가의 7년치 이메일을 압수수색하고 그 사적인 내용을 언론에 공표하는 일마저 발생하였다. 통신수사의 남발과 오남용에 대한 비판이 커지는 가운데 2009년 8월에는 국가정보원이 인터넷 회선을 통째로 감청하는 '패킷 감청'(DPI : Deep Packet Inspection) 기술을 사용해 왔음이 드러나 큰 사회적 충격을 주었다. 비슷한 시기에 KT에서는 같은 기술을 사용하여 이용자의 통신 내용 분석을 토대로 한 맞춤광고 사업을 시작하여 논란을 불러 왔다[2]. 2011년에는 KT와 SKT가 DPI 기술을 이용하여 mVoIP 서비스를 차별해 왔음이 알려져 통신 비밀과 망중립성 침해 논란이 불거졌다(진보네트워크센터 등, 2011).

이처럼 정보통신 분야에서는 개인정보의 온라인 유출, 위치정보 추적, 감청에 이르기까지 다양한 형태의 프라이버시 침해가 발생하고 있다. 문제의 원인은 침해의 주요 주체인 국가와 기업의 개인정보 수집과 처리 동기에서 찾아볼 수 있다. 먼저 국가는 주지하다시피 근대에 들어서 납세, 국방, 복지, 수사 등의 목적으로 국민의 개인정보를 수집 및 이용해 왔으며, 이때 국민의 프라이버시에 대한 국가의 제한은 법원이 발부한 영장 등에 의해 통제되어야 한다는 것이 근대 헌법의 정신이다. 그러나 최근 신자유주의적 경찰국가화 경향이 강화되는 가운데 경찰권 발동은 '구체적 위험'이 존재하는 경우에 한하여 정당화된다는 고전적인 제한법리가 위협받고 있으며 광범위한 치안 정보의 수집이 용인되고 있다. 이러한 상황에서 통신서비스의 발달과 이용이 늘면서 정보수사기관의 정보 수집 능력이 크게 확대된 반면, 이에 대한 적절한 감독과 견제는 부족한 상황이다.

시정요구 및 과태료 부과", 보도자료(2011. 8. 3).

2) 오마이뉴스, 2009. 9. 3. "KT '쿡 스마트웹'은 당신이 한 일을 알고 있다?".

기업에 의한 개인정보 침해는 주로 개인정보의 상업적 가치에서 유래한다. 해킹에 의한 유출 사고(네이트, 옥션, 넥슨 사례)는 개인정보의 취득을 통해 얻을 수 있는 경제적 이득이 뚜렷해지면서 그 시도가 끊이지 않고 있다. 타인의 개인정보를 도용하여 게임 아이템을 거래하거나 개인정보를 현금화하는 것이 가능하기 때문이다[3]. 다른 한편으로 통신기업 스스로의 상업적 동기로 개인정보를 침해하는 경우도 늘고 있다(하나로텔레콤, 애플, 구글, KT, SKT 사례 등). 불특정다수를 대상으로 한 대중 마케팅의 한계를 넘어 개인별 특성에 맞춘 마케팅 기법이 발달하면서 그에 따른 개인정보의 수집과 이를 활용한 DBMS(Database Management System) 기술 역시 발전하였고 개인정보의 상업적인 활용성이 크게 증가하였다. 이를테면 현재 고객이 있는 위치를 파악한 후 그 주변에 고객의 취향에 맞는 상품을 배치하고 그 구입을 유도하는 식이다. 이 때문에 고객의 신상정보로부터 행태 정보는 물론, 소셜네트워크 서비스(SNS)를 통해 공개되는 정보에 이르기까지 대용량 데이터(big data)를 마구 수집하여 프로파일링하고 데이터 마이닝하는 사업이 크게 발달하고 있다(베이커, 2010; 프레이저, 2011). 특히 최근 널리 사용되고 있는 스마트폰 등 모바일 통신기기는 그 이용자와 밀착되어, 당해 정보주체에 대한 다양하고 민감한 정보를 수집하고 유출할 수 있다(심우민, 2011b).

한국의 경우 정보통신망에서의 개인정보 보호 관련 법률의 제정이 비교적 일찍 이루어지는 등[4] 개인정보 침해 문제에 대하여 입법적으로 통제하려 노력해온 편이지만 근본적인 문제 해결은 요원하다. 주민등록번호로 인한 국가적인 식별 시스템이 의무적으로 시행되고 있고 그 번호가 민관에 의해 널리 사용되면서 식별 정보의 수집이 일반화되었기 때문에 그 이용과 침해 정도가 매우 크다. 유비쿼터스 환경 속에서 주민등록번호가 일단 노

3) 매경이코노미, 제1636호(2011. 12. 21), “해커의 세계…전 국민 신상정보 2번 이상 털렸다”.

4) 「(구)정보통신망 이용촉진 등에 관한 법률」에 개인정보 보호제도에 대한 사항이 대폭 규정되면서 법명이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 현재와 같이 변경된 것이 2001년의 일이다.

출되면 온라인 행적(trail)은 물론 때로는 오프라인에서도 명의도용과 행적 추적이 손쉬울 뿐 아니라 유출된 주민등록번호의 변경이 제도적으로 허용되지 않기 때문에 그 피해가 평생에 걸쳐 계속 발생한다. 특히 의무적 인터넷 실명제를 도입함으로써 인터넷서비스제공자들이 개인정보를 광범위하게 수집하도록 강제한 법제도가 최근 개인정보 오남용과 유출의 주요 원인으로 지목되고 있다(심우민, 2011a).

정보통신 환경에서 불거진 개인정보 보호 문제는 방송통신융합 환경 속에서 미디어 영역 전반으로 확대되고 있다. 방송 통신 융합 기술의 발달은 방송국에서 일방적으로 송출하여 보내주는 영상물을 시청하는 것 뿐 아니라 방송 중간에 시청자의 직접적인 의견을 반영할 수 있도록 사용자가 직접 통신 기술을 이용하여 입력하거나, 개인이 제작한 데이터를 이용하여 방송을 할 수 있게 하였다. 이러한 기술의 발달로 개인정보 침해의 위협이 증가하였다(김진형·황준, 2008). 예컨대 IPTV 환경 내 개인정보 침해 요인은 단계별로 다음과 같이 다양하다.

이 장에서는 정보통신망의 개인정보, 위치정보, 그리고 통신 정보의 수집과 유통 문제를 중점적으로 분석해 보고자 한다.

2. 이론적 배경

사회적으로 큰 관심을 끌었던 교육행정정보시스템(NEIS)에 대한 2003년 국가인권위원회의 결정에서 볼 수 있었듯이, 「헌법」 제17조 '사생활의 비밀과 자유'의 불가침의 내용으로 자기정보접근권, 자기정보정정청구권, 자기정보사용중지청구권을 포함한 정보관리통제권, 즉 개인정보에 대한 자기결정권이 인정되고 있다[5].

헌법재판소는 2005년 개인정보 자기결정권에 대하여 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개

5) 국가인권위원회, 교육행정정보시스템(NEIS) 관련 권고(2003. 5. 17).

〈표 1〉 IPTV 환경내 개인정보 침해 요인

단계별				수집·저장·관리 정보	침해요인
가입단계				개인 식별 정보, 연락처 정보, 결재 정보 등	- 인식이 부족한 내부직원에 의한 개인정보 유출 및 변경 - 외부인의 불법적 접근(해킹)에 의한 개인정보 유출
사용단계	플랫폼			고객 가입정보, 시스템 로그정보, 서비스이용정보, 과금정보, 상품주문내역 정보, 주요성향 정보, 단말정보, 리모콘 조작정보 등	- 수집된 정보들로 IP망을 통한 타겟 마케팅이 가능 - 시스템 로그 정보를 활용한 평소 TV 시청 시간 파악 - 리모콘 조작 정보를 리턴 서버에 저장 - 수집된 정보를 가공하여 새로운 정보를 생성하거나 제3자에게 제공
	네트워크	기본적으로 IP망을 사용	데이터 서비스	쿠키에 저장된 정보	- 쿠키에 의한 개인정보 수집 - 해킹, 악성코드 등에 의한 불법적 개인정보 수집
			통신 서비스	통화내역 및 내용, 주이용 서비스	- 도청 및 메시지 위·변조 - 서비스 거부 - 불법 스팸
			방송 서비스	개인의 초상권, 주요선호 콘텐츠	- 무분별하게 타인의 동의 없이 사생활을 촬영·방송하여 초상권을 침해 - 멀티캐스팅으로 인한 신분위장, 부당한 재전송, 부인, 트래픽 관찰 등으로 인한 기술적 침해 . 정상적인 서비스 수신 방해 . 사용자의 의도와 무관한 콘텐츠 방송
			망 구분 (폐쇄망 / 공개망)	랑데뷰 포인트를 지나는 모든 패킷	- 통신 서비스의 도청 - 주 사용 서비스의 정보를 수집하여 제3자에게 제공가능 - 원하는 패킷을 네트워크 관리자가 임의로 제한함으로써 사용자의 프라이버시 침해
	단말			인증서등의 개인정보, 리모콘 조작 정보	- 인증서 등 개인정보·리모콘 조작 정보가 STB에 저장
해지 단계				STB 상의 저장 정보, 가입신청서상의 정보, 해지 신청서상의 정보	- 서비스 종료 후 개인정보 미파기 - 개인정보 파기에 대한 확인의 어려움 - STB 상에 존재하는 개인정보의 복구 가능성 - 번들상품의 해지시 특정 한 가지 상품에 대한 해지의 어려움 - 가입에 비해 복잡하고 까다로운 해지

* 출처: 권현오(2007)

와 이용에 관하여 스스로 결정할 권리를 말한다."고 설시한 바 있다[6].

헌법재판소는 "[컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서] 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다"고 경고하며, "이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치"라고 지적하였다. 즉, 개인정보자기결정권은 개인에게 자신에 관한 정보의 공개와 이용에 대하여 원칙적으로 스스로 결정할 권한을 보장하고 있으며, 현대적인 정보처리기술의 조건 아래서는 국가 등 공권력에 의한 개인정보의 무제한적 수집, 저장, 이용 및 교부에 대하여 개인을 보호할 것이 요구된다는 것이다.

개인정보의 무단 수집과 이용을 방관하는 것은, 그 정보에 기초한 사람의 분류, 낙인, 차별을 고착화시키는 결과를 낳을 수도 있다. 개인정보 데이터베이스에 실현되어 있는 한 개인의 정보가 그에 대한 행정서비스와 고객서비스의 수준을 결정하기 때문이다. 정보사회에서는 개인의 사회적 정체성이 디지털화된 개인정보에 의해 좌우될 위험성이 상존하고 있다. 일례로, 잘못된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동에 미치는 위험성은 지대할 뿐만 아니라, 나아가 개인의 인격 자체에도 치명적인 위해를 가할 수 있다(이인호, 2001). 더 나아가 개인정보를 축적 · 처리하는 공 · 사의 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이 된다. 그리하여 이들 개인정보를 토대로

6) 헌재 2005. 5. 26. 선고, 99헌마513, 2004헌마190(병합).

일정 부류의 사람들을 사회적으로 낙인을 찍는 일(예컨대, 신용불량자나 취업기피인물명단의 작성 · 유통)이 얼마든지 가능해지게 되고, 그 결과 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다(성낙인 외, 2008).

개인정보자기결정권은 단순히 타인에 의한 개인정보의 취급을 억제하는 이외에도 개인이 자신에 관한 정보의 유통을 적극적으로 형성하고 조절한다는 측면에서 이해될 수 있다(성낙인 외, 2008). 여기서 개인정보자기결정권의 적극적 측면은 대단히 중요하다. 오늘날 대부분의 개인정보가 자신도 모르게 처리되는 현실 속에서 정보주체가 이 유통 과정에 개입하기 위해서는 적극적인 권리를 완전히 인정받을 수 있어야 하기 때문이다. 컴퓨터나 전산망 등을 통한 개인사생활감시와 개인정보침해는 언제, 어디서 무엇이 얼마만큼 침해되고 있는지를 전혀 또는 거의 모르고 있다가 침해되었다는 사실을 알게 되면 그 구제가 사실상 거의 불가능하다는 특징을 갖고 있다(김일환, 2005). 개인정보 수집과 처리를 위한 정보시스템은 갈수록 막대한 자원이 투입되는 거대 기술 구조물이기 때문에, 도입 이후 개인정보 자기결정권이 침해되는 상황이 발생한다 하더라도 정보주체가 이를 중단시키기가 어렵다. 따라서 개인정보 수집 단계에서부터 그 목적을 명확히 한정하고, 개인정보의 처리 방법 및 종류에 있어서 목적 내 필요 최소한의 개인정보를 수집하고 이용하도록 한정하며, 목적 외 이용을 제한할 수 있는 법적·기술적 조치가 준비되어 있어야 하는 것이다

이와 같은 개인정보에 대한 정보주체의 권리는 국제 규범 및 입법에 있어서 원칙으로 인정받아 왔다. 개인정보보호에 대한 최초의 국제규범인 1980년 OECD 「개인정보보호가이드라인」[7] 뿐 아니라 1990년 UN의 「전산처리된 개인정보파일의 규제에 관한 지침」[8] 및 1995년 EU 「개인정보보호에 관한 유럽의회와 각료회의 지침」[9]에서도 확인되고 있다.

---

7) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

8) Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990.

우리나라의 경우에도 정보주체의 권리는 「공공기관의 개인정보 보호에 관한 법률」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'), 「신용정보의 이용 및 보호에 관한 법률」, 「위치정보의 보호 및 이용 등에 관한 법률」 등 관련 법률에 원칙으로 포함되어 왔다.

특히 2011년 9월 30일부터는 「개인정보보호법」이 제정 시행되고 있다. 본래 공공부문은 「공공기관의 개인정보 보호에 관한 법률」, 정보통신 부문은 정보통신망법 등 영역별 법률에 의해 나누어 규율되어 왔으나, 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화할 필요성이 제기됨에 따라 개인정보보호법이 제정된 것이다. 이 법의 제정은 1997년 통합전자주민카드 반대 운동과 2003년 교육행정정보시스템 반대 운동 등 개인정보 보호와 관련한 사회적 논란이 불거질 때마다 인권시민단체가 요구해 왔던 바였다. 방송통신 영역에서는 개인정보보호법보다는 정보통신망법 등 개별법이 우선적으로 적용되겠지만, 이 법의 제정으로 인하여 비로소 개인정보 유출사고가 발생할 경우 그 사실을 고객에게 통지하도록 의무화되고(제34조), 개인정보 단체 소송이 도입된 한편(제7장), 독립적인 개인정보 보호위원회가 설립되는 등(제7조) 개인정보 보호 및 구제의 체계에 있어 큰 변화를 맞았다. 민간 영역의 CCTV 영상을 제3자가 수집하거나 이용하는 것을 원칙적으로 제한하면서 이를 방송영상 등에 사용하는 것이 법률적으로 규율되기 시작했다는 점도 중대한 변화이다.

3. 현황과 문제점

(1) 정보통신망

지난 2011년 9월 30일 개인정보보호법이 시행에 들어가면서 각종 기관

9) Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 95/46/EC.

이나 중소기업에서 혼란을 겪고 있다고 한다.[10] 반면, 인터넷 및 통신산업 부문은 일찌기 「정보통신망법」의 규율 하에, 타 영역에 비해 개인정보 보호를 위한 법적 체계나 정보보안 시스템을 갖춰온 영역이다. 그럼에도 옥션, 하나로텔레콤, 네이트와 싸이월드, 넥슨 등 정보통신 기업에서의 개인정보 유출 사고가 계속적으로 발생하였다. 그것도 유출 건수가 수 천만 건에 이르는 대형사고 들이다. 이와 같이 대규모 개인정보 유출사고가 반복되는 이유는 무엇일까?

우선, 주요 정보통신 기업이 보유하고 있는 개인정보는 우선 양 자체가 방대하다. 2009년 2월 현재 네이버의 가입자 수는 3,300만 명, 다음의 가입자 수는 3,500만 명[11]으로 주요 포털업체는 대한민국 국민 대다수의 개인정보를 보유하고 있다. KT, SKT, LGU+ 등 통신 3사 역시 마찬가지다.

둘째, 과도한 개인정보 수집을 들 수 있다. 정보사회에서 해킹이나 내부자 공모에 의한 개인정보 유출은 어찌보면 필연적으로 발생할 수밖에 없다. 100% 완벽한 보안이란 있을 수 없기 때문이다. 그렇기 때문에 불필요한 정보를 수집하지 않는 것이 중요하다. 개인정보를 보유하지 않는 것보다 완벽한 보안은 없다. OECD 「개인정보보호가이드라인」과 UN의 「전산처리된 개인정보파일의 규제에 관한 지침」에서 모두 공통적으로 내세우고 있는 제1원칙이 '수집제한의 원칙'인 것도 이 때문이다.(오병일, 2011) 해외 포털과 달리 국내 포털은 주민등록번호를 수집하고 있으며, 성별이나 직업을 필수정보로 요구하는 곳도 있다. 통신사들 역시 주민등록번호를 필수정보로 수집하고 있으며, 통신사의 웹사이트 가입을 위해 고객명, 생년월일, 로그인 ID, 비밀번호, 비밀번호 질문과 답변, 자택 전화번호, 자택주소, 휴대전화번호, 이메일 주소, 직업, 결혼여부, 주민등록번호, 닉네임, 학력, 추천인 ID를 모두필수정보로 수집하고 있는 곳도 있다.(진보네트워크센터, 2009) 이러한 상황을 방송통신위원회가 몰랐던 것은 아닌데, 옥션에서의 개인정보 유출사고 이후 발표한 대책 문서에서 방통위는 '주민등

10) 디지털타임즈, 2011.10.3, "[사설] 개인정보보호법 혼란 최소화해야"
11) 아시아경제. 2009.2.27. "新네이트 출범…포털 2위 노린다."

록번호 등 서비스 제공과 무관한 개인정보를 과다 수집하는 관행으로 개인정보 침해의 중요 원인이 됨'이라고 지적한 바 있다. '야후, MSN, 아마존 닷컴 등 외국 주요사이트는 성명, 이메일, 생년월일 등 기본정보만 수집'하는데 반해, '국내 사이트의 73% 이상이 주민등록번호를 수집('06)'하고 있다고 분석하고 있다.[12)]

셋째, 주요 통신기업들은 취급위탁이나 제3자 제공을 통해 개인정보를 방대하게 공유하고 있다. 이는 특히 통신업체에서 심각하다. 이들은은 '개인정보 취급방침'을 통해 개인정보를 제공받는 제3자(업체) 및 위탁업체를 공개하고 있다. 제3자 제공의 경우 제공받는 자, 제공목적, 제공정보의 종류 등을 구분하여 공개하고 있으며, 위탁처리의 경우 수탁자 및 위탁업무 내용을 공개하고 있다. 통신업체들이 요금결제, 이용료 정산, 본인 인증, 제휴 서비스, 콘텐츠 서비스 등의 목적으로 개인정보를 제공하는 타 업체의 수는 수백 개에 이른다. 또한, 수많은 대리점 혹은 판매점을 운영하고 있기 때문에, 업무위탁을 통해 개인정보를 제공하는 업체 수는 대리점 등을 포함하여 무려 1000~2000개에 달한다. 이와 같이 무수히 많은 제3자에게 개인정보를 제공하는 과정에서 개인정보가 수집 목적 외로 활용되거나 유출될 가능성도 높아지게 된다.(진보네트워크센터, 2009)

넷째, 통신업체들이 개인정보를 동의없이 취급위탁하거나, 해지자 개인정보를 파기하지 않는 등 개인정보의 관리를 부실하게 해왔다. 지난 2008년 4월, 서울지방경찰청이 '하나로텔레콤의 600만 명의 고객 개인정보 유출 사건'을 발표한 이후, 방송통신위원회는 초고속인터넷업체, 포털, 이동통신사 등에 대한 개인정보 관리실태 점검[13)]에 들어갔으며, 대부분의 업체들이 방송통신위원회의 제재를 받았다.(진보네트워크센터, 2009)

---

12) 방송통신위원회, 2008.4.24. "인터넷상 개인정보 침해방지 대책"

13) 방송통신위원회는 2008년 5월부터 SK브로드밴드(舊하나로텔레콤)에 대한 조사를 시작으로, 6월에는 KT, LG파워콤 등 2개 초고속인터넷사업자, 9월에는 4개 복수종합유선방송사업자 및 4개 포털사업자, 10월부터는 3개 이동전화사업자 등 총 14개사에 대해서 연속적으로 개인정보 관리실태를 점검하였다(방송통신위원회. 2008.12.30. "방통위, 3개 이동전화사업자의 개인정보 유용행위에 대해 과태료 부과.").

〈표 2〉 개인정보 유용행위 등에 대한 방송통신위원회 시정조치 현황

업체명	시정조치 내용	시정조치 이유
하나로 텔레콤	'08.7.1~8.9일까지 (40일간) 신규가입자 모집정지	개인정보 유용
KT	'08.8.30~9.28 (30일간) 신규가입자 모집정지	개인정보 유용
LG 파워콤	'08.8.30~9.28 (30일간) 신규가입자 모집정지	개인정보 유용
SKT	과태료 5,000만 원	고객정보를 동의 없이 또는 고지 없이 취급 위탁한 행위, 해지자 개인정보를 파기하지 않은 행위 등
KTF	과태료 3,000만 원	고객정보를 동의 없이 취급 위탁한 행위, 동의철회 고객에 대해 필요한 조치를 하지 않은 행위 등
LGT	과태료 5,000만 원	고객정보를 동의 없이 또는 고지 없이 취급 위탁한 행위, 해지자 개인정보를 파기하지 않은 행위 등
티브로드 한빛방송	과태료 3,000만 원	초고속인터넷 가입자 정보를 동의 없이 또는 고지 없이 취급 위탁한 행위 및 기술적 · 관리적 조치미비
CJ 헬로비젼	과태료 1,000만 원	개인정보 전송 시 암호화 조치 미흡 등 기술적 · 관리적 조치미비
씨엔엠	과태료 3,000만 원	초고속인터넷 가입자 정보를 동의 없이 또는 고지 없이 취급 위탁한 행위 및 기술적 · 관리적 조치미비
큐릭스	과태료 3,000만 원	초고속인터넷 가입자 정보를 고지 없이 취급 위탁한 행위, 해지자 개인정보를 파기하지 않은 행위 및 기술적 · 관리적 조치미비
NHN	과태료 3,000만 원	해지자 개인정보 미파기, 법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적 · 관리적 조치미비
다음커뮤니케이션	과태료 3,000만 원	포털가입자 정보를 동의 없이 취급 위탁한 행위, 법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적 · 관리적 조치 미비
SK커뮤니케이션스	과태료 2,000만 원	법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적 · 관리적 조치미비
야후 코리아	과태료 2,000만 원	법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적 · 관리적 조치미비

*자료: 방송통신위원회 보도자료에서 취합.

대다수 통신업체들이 주민등록번호를 수집하고 있는 문제는 특히 심각하다. 주민등록번호는 모든 대한민국 국민들에게 부여되는 고유한 식별번호로서, 서로 다른 개인정보를 연동할 수 있는 열쇠가 되기 때문이다. 또한, 그 자체로 생년월일, 성별, 출생지 등 개인정보를 포함하고 있을 뿐만 아니라, 주민등록번호의 변경이 사실상 불가능해 한번 유출될 경우 그 피해를 회복하기 힘들다.

문제는 정부가 주민등록번호 수집의 문제를 이미 인식하고 있었으면서도[14] 그동안 이 문제를 방치·조장해왔다는 점이다. 기업들이 주민등록번호를 보관하는 대표적인 근거는 '인터넷 실명제'이다. 인터넷 실명제는 「정보통신망법」 제44조의5(게시판 이용자의 본인 확인)에 따른 것인데, 시행령 제29조(본인확인조치) 3호는 '게시판에 정보를 게시한 때부터 게시판에서 정보의 게시가 종료된 후 6개월이 경과하는 날까지 본인확인정보를 보관할 것'이라고 규정하고 있다. 네이트-싸이월드 개인정보 유출사고 이후, 수많은 언론과 전문가, 심지어 국회 입법조사처[15]에서도 '인터넷 실명제'를 유출사고의 주범으로 지목했다. 그러나 방통위는 인터넷 실명제가 개인정보 유출과 무관하다고 주장하는데, 인터넷 실명제는 "정보통신서비스제공자들은 신용평가정보사 등 전자서명법에 따른 공인인증기관 등으로부터 본인인증을 받은 후, 본인 확인정보(본인인증 결과값)만을 보관하도록 되어 있으므로, 본인확인제가 주민번호 등 개인정보 수집을 의무화하는 것은 아니"라는 것이다.[16] 이미 2008년 옥션 사태때부터 관련된 문제제기가 있었음에도 지금에서야 이렇게 변명하는 것은 비겁한 태도라고 하지 않을 수 없는데, 최소한 방통위는 기업들을 제대로 계도하지 않은 책임을 져야 한다.

---

14) 앞서 언급한 방송통신위원회의 보도자료 "인터넷상 개인정보 침해방지 대책"(2008.4.24)에서 '주민등록번호 등 서비스 제공과 무관한 개인정보를 과다 수집하는 관행으로 개인정보 침해의 중요 원인이 됨'이라고 지적하고 있다.

15) 심우민, 2011a

16) 방송통신위원회, 2011.8.3, "[해명자료] 전자신문 보도(8.3) 관련 방송통신위원회 입장"

어쨌든 방통위의 해석이 나옴에 따라, 이제 기업들도 주민등록번호를 보관하지 않겠다는 선언을 하고 나섰다. 개인정보가 유출된 SK커뮤니케이션즈뿐만 아니라, 네이버와 다음(daum)도 2012년 말까지 더 이상 주민등록번호를 수집하지 않고, 이미 수집된 주민등록번호도 폐기하겠다고 밝힌 것이다.[17] 그러나 이름-주민등록번호 대조방식의 본인확인 방식이 유지되는 한, 여전히 명의도용의 위험성은 남는다. 타인의 개인정보를 훔치려는 이유는 그것이 가치가 있기 때문이다. 인터넷 실명제는 여전히 명의도용을 위해 주민등록번호를 필요로 하며, 이는 주민등록번호의 유출과 암거래를 부추기는 요인이 된다.

주민등록번호 유출로 인한 추가적인 피해를 막기 위해서는 지금이라도 민간에서의 주민등록번호 수집을 금지해야 한다. 이름-주민등록번호 대조방식의 본인확인 방식을 포함하여, 단지 '저장(보관)'만 하지 않는 것이 아니라 주민등록번호의 입력 자체를 요구하지 않아야 한다. 이러한 문제제기가 이미 오래전에 제기되었고, 정부 역시 2008년 대책에서 '전자상거래 등 법적 권리 관계가 발생하는 경우에 한해 주민번호를 수집토록 하고, 일반적 포털 등은 수집을 제한하는 방안 추진'한다고 하였으나, 실제로 주민등록번호의 수집을 제한하는 법제화는 추진되지 않았다. 고작 일정 규모 이상의 사업자에 대해 주민등록번호 외의 회원가입 방법을 의무적으로 제공하도록 하였을 뿐이다.[18]

인터넷 실명제 외에 기업들의 주민등록번호 수집을 부추기는 또 하나의

---

17) 엄밀하게 얘기하면 '수집'하지 않는 것이 아니라, '보관'하지 않는 것이다. 기사에 따르면, 여전히 이름-주민등록번호 대조 방식의 본인확인 방식은 유지하는 것으로 보인다. 다만, 이를 보관하지 않겠다는 것이다. (이데일리, 2011.12.20, "대형포털, 수집한 주민등록번호 폐기한다")

18) 제23조의2(주민등록번호 외의 회원가입 방법) ① 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 통하여 회원으로 가입할 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다. ② 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다.

요인은 전자상거래와 관련된 기록 보유를 의무화한 「전자상거래 등에서의 소비자보호에 관한 법률」이다. 이 법률 제6조[19] 1항은 거래에 관한 기록을 일정 기간 보존하도록 의무화하고 있는데, 2항에서 소비자가 동의를 철회하는 경우에도 보존할 수 있도록 하면서 관련 개인정보를 '성명·주소·주민등록번호 등 거래의 주체를 식별할 수 있는 정보'로 규정하고 있다. 시행령 6조에서는 거래기록에 따라 6개월, 3년, 5년의 보존기간을 규정하고 있다.(오병일, 2011) 여기서 주민등록번호를 삭제한 개정안이 2011년 12월 현재 국회에 계류 중이다.[20]

통신사들도 초고속인터넷이나 핸드폰 가입시 주민등록번호를 받고 있는데, 이는 아무런 법적 근거도 없다. 2011년 9월 30일 시행된 「개인정보보호법」에서는 제24조[21]에서 주민등록번호 등 고유식별번호의 수집 등 처

---

19) 제6조(거래기록의 보존 등) ① 사업자는 전자상거래 및 통신판매에서의 표시·광고, 계약내용 및 그 이행 등 거래에 관한 기록을 상당한 기간 보존하여야 한다. 이 경우 소비자가 쉽게 거래기록을 열람·보존할 수 있는 방법을 제공하여야 한다.
②제1항의 규정에 의하여 사업자가 보존하여야 할 거래의 기록 및 그와 관련된 개인정보(성명·주소·주민등록번호 등 거래의 주체를 식별할 수 있는 정보에 한한다)는 소비자가 개인정보의 이용에 관한 동의를 철회하는 경우에도 정보통신망이용촉진및정보보호등에관한법률 제30조제3항의 규정에 불구하고 이를 보존할 수 있다.
③제1항의 규정에 의하여 사업자가 보존하는 거래기록의 대상·범위·기간 및 소비자에게 제공하는 열람·보존의 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

20) 1807288, 2009.12.31, 정부발의. 상임위 대안 마련으로 폐기.

21) 제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.
1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
② 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.
③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

리를 제한하고 있다. 물론 동의를 받으면 수집할 수 있지만, 제24조 1항에서 '다른 개인정보의 처리에 대한 동의와 별도로 동의를 받'도록 하고 있다. 한편 같은 법 제16조는 '목적에 필요한 최소한의 정보'만을 수집하도록 하고 있으며, 필요최소한의 정보 외의 정보 수집에 동의하지 않는다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하지 못하도록 하고 있다. 따라서 이제 통신사들이 가입자들의 주민등록번호를 수집하는 것은 법적 근거가 없어 보인다.

주민등록번호의 유출 문제가 불거지면서, 정부와 기업은 본인확인 방식을 이름-주민등록번호 대조방식에서 아이핀(I-PIN)으로 전환하려고 하고 있다. 물론 지금도 아이핀 인증이 이용되고는 있지만, 불편하기 때문에 이용률이 그다지 높지는 않은 상황이다.[22] 그러나 아이핀은 대안이 될 수 없으며, 오히려 개인정보 유출에 따른 위험이 더 클 수 있다.

우선, 불필요한 인증 요구의 문제는 여전히 남는다. 인터넷 실명제의 근본적인 문제는 서비스 이용에 필수적이지 않음에도 불구하고, 본인 인증을 요구한다는 점이다. 그 방식이 이름-주민등록번호 확인 방식이든, 아이핀 방식이든, 공인인증서 방식이든 이 문제는 여전히 남는다. 해외 대다수의 사이트와 같이 인증 자체를 하지 않으면 된다.

둘째, 아이핀 역시 주민등록번호에 기반한 시스템이다. 따라서 주민등록번호 수집 및 도용의 문제를 여전히 가지고 있다. 아이핀을 개설할 때 자신의 이름과 주민등록번호를 입력하고, 휴대폰, 신용카드, 공인인증서, 대면확인 등의 본인 확인 과정을 거친다.[23] 그러나 2차 확인 방법 역시 주민등록번호에 기반을 두고 있다. 이미 지난 2010년 6월, 무기명 선불카드, 대리

---

④ 행정안전부장관은 제2항에 따른 방법의 제공을 지원하기 위하여 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련할 수 있다.
[시행일 : 2012.3.30] 제24조제2항

22) 이데일리, 2011.8.1. "인터넷 여전히 주민번호..아이핀 360만 불과"

23) 이와 같이 추가적인 본인 확인 과정을 거친다는 사실 자체가 이름-주민등록번호 대조 방식이 본인 확인 수단이 될 수 없다는 것을 입증한다. 더구나 국민 대다수의 주민등록번호가 이미 유출되었고, 오프라인에서도 쉽게 타인의 주민등록번호에 접근할 수 있는 상황에서는 말이다.

인증제도, 대포폰 인증 등 아이핀 발급 체계의 허점을 이용해 아이핀을 불법 발급받은 사례가 적발되기도 했다.[24] 이후 방통위는 선불카드나 대리인 증제도를 통한 본인확인 방법을 제외하였지만, 여전히 대포폰을 통한 아이핀 발급 등 명의 도용의 위험은 남아있다.

셋째, 100% 완벽한 보안이란 없다고 했을 때, 인증기관에서 보유하고 있는 개인정보 역시 유출되지 않으리라는 보장은 없다. 불필요한 인증은 6대 인증기관[25]에 의한 불필요한 개인정보 수집으로 이어지는데, 이들 인증기관에서 보유하고 있는 개인정보가 유출될 경우의 파급력은 일반 업체들의 그것보다 훨씬 클 것이다. 이들 인증기관은 개인의 인터넷 사이트 가입내역까지 보관하고 있으니 말이다. 지난 2008년 한 조사에서 아이핀 정보 노출이 심각하다는 사실이 밝혀지기도 했다.[26]

넷째, 아이핀은 이용자들이게 불편을 야기한다. 특히 노인과 같이 기술에 익숙하지 않은 이용자에게는 더욱 복잡하게 느껴질 것이다. 이름-주민등록번호 확인 방식의 인증이 유출 및 명의 도용 위협에도 불구하고 여전히 주된 인증 방식으로 이용되는 것은 그나마 간편하기 때문이다. 자신 명의로 핸드폰이나 신용카드를 개설하지 않은 사람(예를 들어, 부부같은 경우 한 사람 명의로 핸드폰 가입이나 신용카드를 사용하는 경우도 있고, 노인들은 자식 명의로 가입하는 경우도 많다.)은 그나마 아이핀에 가입하기도 힘들다. (오병일, 2011)

한편, 「정보통신망법」 제30조[27] 2항 2호는 정보주체가 열람을 요구할

---

24) 연합뉴스, 2010.6.6. “아이핀 불법발급 유통 적발”

25) 2011년 8월 현재 서울신용평가정보, 코리아크레딧뷰로, 한국신용정보, 한국신용평가정보, 한국정보인증, 공공아이핀센터 등 6개 기관이 아이핀을 발급하고 있다.

26) 보안뉴스, 2008.10.1. “한심한 아이핀·G-PIN...개인정보 노출 심각!!”

27) 제30조(이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.

② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.

1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보

경우, '이용자의 개인정보를 이용하거나 제3자에게 제공한 현황'을 제공하도록 하고 있다. 그러나 현실적으로 정보통신 기업들은 정보주체의 열람권을 제대로 보장하지 않는 것으로 나타났다. 특히 개인정보를 수사기관에 제공한 내역에 대해서는 제공을 거부하는 업체들이 많았으며, 제공가능한지에 대한 법 해석도 모호했다. 또한, 일부 통신업체의 경우, 개인정보취급방침에서 개인정보의 이용 · 제공내역에 대한 열람권을 명시하고 있지 않았다. 업체들은 개인정보취급방침에 취급위탁업체 및 제휴업체의 목록을 공개하고 있기는 하지만, 이것만으로는 실제로 내 개인정보가 어떤 업체에 제공되었는지 파악하기 힘들다. 그러나 홈페이지를통해 제3자에게 제공한 내역을 열람할 수 있도록 한 사업자들은 없었으며, 제3자 제공내역의 열람을 요구한 경우에도 단지 개인정보취급방침을 확인하라고 답변한 업체들이 많았다. 기업들이 수집한 개인정보가 취급위탁이나 제3자 제공을 통해 기업 간에 공유되는 경향이 높아가는 현실에서 정보주체가 자기정보가 제3자에게 제공된 내역을 열람할 권리는 중요해지지 않을 수 없다. (진보네트워크센터, 2009)

(2) 위치정보

개인의 위치정보는 특히 민감한 정보다. 위치정보는 개인의 일상 활동을 감시하거나 추적할 수 있는 수단이 될 수 있기 때문이다.[28] 정보통신기술의 발전은 사물이나 사람의 위치를 파악할 수 있는 능력의 향상을 가져왔다. 특히 스마트폰의 대중화에 따라 위치정보에 기반한 앱 및 서비스들도 다양화되고 있다. 아직은 초보적인 수준이지만, 모바일 앱과 서비스의 수준이 고도화될수록 편리함의 이면에 감춰진 감시와 통제의 위험성도 커질

2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

28) 대표적인 것이 삼성SDI 전현직 노동자들에 대해 불법복제된 휴대전화를 통해 몇 개월 동안 위치추적을 통한 감시가 이루어진 사례이다. 한겨레신문. 2004.7.14. "'위치추적' 삼성SDI 고소."

수 있다.

개인의 위치정보는 「위치정보의 보호 및 이용 등에 관한 법률」(이하 「위치정보법」)에 의해 규제된다. 정보통신망에서의 개인정보의 보호 및 이용을 규율하는 「정보통신망법」이 있음에도 불구하고, 지난 2005년 1월 27일 제정된 「위치정보법」[29]은 위치정보의 특별한 보호를 명분으로 하고 있지만, 사실 위치정보 기반 산업의 육성 및 규제를 위한 법안이다. 그러나 「위치정보법」이 개인의 위치정보를 제대로 보호할 수 있는지, 또는 위치정보 기반 서비스에 적합한 규제체제를 갖추고 있는지에 대해서는 여전히 논란이 많다.

지난 2011년 4월, 애플사가 일부 아이폰 이용자의 동의 철회에도 불구하고 위치정보를 수집해왔다는 의혹이 제기되었다. 방송통신위원회는 애플과 구글의 미국 본사 위치정보시스템에 대한 현장점검을 거쳐, 2011년 8월 애플 및 구글의 위치정보보호 법규 위반행위에 대해 시정요구 및 과태료를 부과하였다. 방통위 조사결과에 따르면, "2010. 6. 22.~2011. 5. 4.(약 10개월) 기간 동안 일부 아이폰의 경우 이용자가 위치서비스를 '끔'으로 설정했을 때에도 아이폰 주변의 기지국 및 WiFi AP 위치값을 서버로 전송하였고, 애플서버는 해당 Wi-Fi AP 및 기지국의 위경도 값을 아이폰으로 전송하는 등 위치정보 수집행위를 한 것으로 나타났다."[30] 이에 대해 '소유자의 동의를 얻지 아니하고 이동성 있는 물건의 위치정보를 수집·이용·제공하는 행위를 금지하고 있는' 「위치정보법」 제15조 1항[31]을 위반

29) 법률 제7372호, 2005. 1.27, 제정. 2005. 7.28 시행

30) 방송통신위원회, "방통위, 애플 및 구글의 위치정보보호 법규 위반행위에 대해 시정요구 및 과태료 부과", 보도자료(2011. 8. 3).

31) 제15조(위치정보의 수집 등의 금지) ①누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집 · 이용 또는 제공하여서는 아니된다. 다만, 제29조의 규정에 의한 긴급구조기관의 긴급구조 또는 경보발송 요청이 있거나 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

한 것으로 판단하여 과태료 300만원을 부과한 것이다. 또한, 애플과 구글이 위치정보를 이용자의 휴대단말기 내의 위치정보 캐쉬에 암호화하지 않고 저장한 행위에 대해서는 동법 시행령 제20조 제2항 제2호의 위치정보 시스템에의 권한 없는 접근을 차단하기 위한 암호화 조치의무 위반이라고 판단하여 시정요구를 하였다.

이에 대해 서로 다른 방향에서 비판이 제기되고 있다. 그 하나는 방통위는 애플사가 「위치정보법」을 위반했다고 의결했지만, 수집된 정보는 '개인위치정보'는 아니라고 판단했는데, 이는 잘못이라는 것이다. 「위치정보법」은 제2조 제1호에서 위치정보를 "이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 전기통신기본법 제2조제2호 및 제3호의 규정에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것"이라 정의하고 있으며, 2호에서는 개인위치정보를 "특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)"로 규정하고 있다. 그런데 개인이 항시 휴대할 것으로 예상되는 휴대전화의 특성상, 애플사가 수집한 위치정보는 개인식별가능성을 가질 수 있으므로 '개인위치정보'로 보아야 한다는 것이다. (이민영, 2011) 그러나 방통위는 애플사가 수집한 위치정보는 '개인을 식별할 수 없는 형태'로 서버에 저장되어 있었기 때문에 '개인위치정보'는 아니라고 보았다는 것이다.[32]

또 다른 측면에서의 비판은 현행 「위치정보법」에서 '소유자의 동의를 얻지 아니하고 이동성 있는 물건의 위치정보를 수집할 수 없다'고 규정하여, '개인에 대한' 정보가 아닌 정보마저도 소유자의 동의를 얻도록 요구하는 것은 세계적으로 유례가 없는 과도한 규제라는 것이다.[33] 위의 두 비판

32) 연합뉴스, 2011.8.3, "석제범 방통위 국장 '애플·구글 위법' 문답".
http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=001&aid=0005195417

33) 헤럴드경제, 2011.8.23, "〈헤럴드 포럼〉 위치정보보호법 애플적용, 문제 있다", 박경신 교수 컬럼.

은 서로 배치되는 것은 아니다. 후자의 비판대로 개인식별성이 없는 물건의 위치정보에 대해서도 이를 수집하기 위해서는 소유자의 허락을 얻도록 하는 것은 과도할 수 있다. 그러나 「위치정보법」에서 '이동성이 있는 물건'의 위치정보를 규정하고 있는 것은, 스마트폰이나 교통카드처럼 통상 개인의 위치정보는 그 개인이 소지하고 있는 물건을 통해 파악되기 때문이다. 즉, 그 자체로는 개인정보가 아닐지라도 다른 개인정보와 결합함으로써 '개인위치정보'가 될 수 있다. 이에 따라 '다른 정보와 쉽게 결합할 가능성'을 어떻게 판단할 것인가가 쟁점이 될 수 있으며, 현재로서는 그 구체적인 기준이 확립되었다고 보기는 어렵다.(이진규, 2011) 지난 2011년 5월, 구글코리아와 다음커뮤니케이션이 모바일 광고플랫폼을 통해 개인이 식별되는 위치정보를 동의없이 수집했다는 의혹을 받고 경찰의 압수수색을 당한 바 있다.[34] 결국 2011년 12월 14일, 경찰은 구글과 다음이 수집한 정보는 위도·경도 등 GPS 위성정보일 뿐, 개인위치정보는 아니라고 결론을 내리고 무혐의 처리했는데[35], 이 사건 역시 위치정보의 개인식별성과 관련된 문제라고 할 수 있다.

위치정보 규제대상의 모호함도 문제로 지적된다. 「위치정보법」은 제2조에서 '위치정보사업'을 "위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 것"으로, '위치기반서비스사업'은 "위치정보를 이용한 서비스를 제공하는 것을 사업으로 영위하는 것"이라 규정하고 있다. 위치정보사업자는 방통위의 허가를 받아야 하고, 위치기반서비스사업자는 방통위에 신고를 해야 한다. 그런데, 위의 모바일 광고 플랫폼의 사례처럼, 모바일 광고 플랫폼을 사용하는 앱에서 위치정보를 수집할 때, 위치정보의 수집 주체가 이용자인지, 모바일 광고 플랫폼인지, 앱인지 등의 경계가 모호할 수 있다는 것이다.(정혜승, 2011) 또한, 현재의 규제체제는 위치정보사업자에 대해서 더욱 강력한 규제를 하고 있지만, 프라

---

http://biz.heraldm.com/common/Detail.jsp?newsMLId=20110823000137

34) 연합뉴스, 2011.5.3, "위치정보 수집 혐의 구글 · 다음 압수수색".

35) 아이뉴스24, 2011.12.14, "위치기반 모바일광고 활성화 "아직은 먼 얘기""

이버시 침해의 위험성에 비추어볼 때 위치정보사업자와 위치기반서비스사업자의 규제 형평성의 문제도 제기되고 있다.(이민영, 2011) 더불어 현행 「위치정보법」은 위치정보를 수집하기는 하지만 위치기반서비스사업자에게 위치정보를 제공하지 않는 기관이나 업체는 규제 대상에서 제외되는 점도 문제로 제기된다. 이에 따라 교통카드를 통해 수집된 위치정보나 승용차요일제 규제를 위해 수집된 위치정보 등은 「위치정보법」의 적용을 받지 않는데, 이 법이 민감한 개인정보로서 위치정보의 보호를 보다 강화하기 위한 것이라면 위치기반서비스에 제공되지 않는다고 해서 규제 대상에서 제외될 이유는 없어 보인다.(진보네트워크센터, 2009)

다양한 위치정보 앱이나 서비스가 도입되면서 사회적 약자에 대한 감시로 악용될 가능성도 우려된다. 「위치정보법」 제19조제3항은 위치기반서비스제공자가 개인위치정보를 제3자에게 제공하는 서비스를 할 경우,[36] 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하도록 하고 있다.[37] 그러나 비록 정보주체의 동의가 있었다고 하더라도, 사회 관계에서 약자인 자녀, 노인, 장애인, 노동자 등이 현실적으로 이에 대한 동의를 거부하기 힘든 상황이라는 점을 고려하면, 이러한 위치기반 서비스가 약자에 대한 감시로 기능할 가능성을 배제하기 힘들다.(진보네트워크센터, 2009) 사회적 약자에 대한 감시뿐만 아니라, 시민 상호간의 감시문화를 확산할 우려도 있다. 상호 위치정보 확인에 동의한 부부나 연인의 현재위치를 상대방에게 실시간으로 알려주는 '오빠 믿지'와 같은 앱이 대표적이다.[38] 이러한 앱이 상호 동등한 관계 속에서 이용되는 것도 문제일 수 있지만, 불평등한 관계 속에서 악용될 가능성도 배제할 수 없다.

수사기관 등 국가기관에 의한 국민 통제의 목적으로 이용될 수 있다는 우려도 제기된다. 「위치정보법」 제29조는 긴급구조를 위해 소방서 등 긴급구조기관이 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있도

---

36) 예를 들어, 아동이나 치매노인 등에 대한 신변보호서비스, 친구찾기 서비스, 차량관제 서비스 등이 모두 이에 해당한다.

37) 이는 주로 이동통신 서비스에 기반한 서비스를 염두에 둔 조항으로 보인다.

38) 지디넷코리아, 2011.8.13, "너의 위치 정보를 허하라…악마의 앱 '봇물'"

록 하고 있다. 그런데, 유괴 등 범죄의 수사를 위해서 이에 경찰관서를 포함시켜야 한다는 요구가 제정 당시부터 존재했다. 그러나 수사기관에 의한 악용의 우려 때문에 제외되었는데, 지난 2008년 11월 28일 정부가 발의하여 2011년 12월 현재 국회에 계류되어 있는 「정보통신망법」 개정안[39]은 「위치정보법」 전부를 이 법에 통합하면서 경찰관서에서도 위치정보사업자로부터 개인위치정보를 요청할 수 있도록 허용하고 있다. 그러나 정보수사기관은 이미 통신비밀보호법을 악용하여 실시간 위치추적을 해온 것으로 드러나[40] 남용의 우려는 가시지 않고 있다.

개인위치정보의 활용이 증가하면서, 정보주체의 권리를 보장해야할 필요성도 커지고 있다. 「위치정보법」제29조는 긴급구조 목적으로 개인위치정보를 이용할 경우에도 제공 사실을 정보주체에게 즉시 통보하도록 하고 있으나, 이러한 규정은 사실상 지켜지지 않는 것으로 드러났다.[41] 또한, 위치정보에 대한 정보주체의 열람권도 제대로 보장되지 않고 있다. (진보네트워크센터, 2009)

최근 한 조사에 따르면, 이용자들 역시 위치기반 앱의 개인정보 수집에 대해 불안감을 갖고 있는 것으로 나타났다.[42] 설문조사 결과 전체 이용자의 57.3%가 '위치기반 어플리케이션의 개인정보 수집에 대해 불안감을 갖고 있다'고 답했다고 한다. 스마트폰 등 위치정보를 파악할 수 있는 기술과 장비의 도입은 증가할 것이고, 개인의 위치를 갈수록 정밀하게 추적할 수 있을 것이다. 다양한 위치기반 앱과 서비스가 편리함, 정보제공, 보안 등을 무기로 우리 삶에 도입될 것이다. 물론 위치정보를 이용한 새로운 서비스들이 우리에게 가치와 정보를 제공할 수도 있다. 그러나 개인위치정보가 프라이버시에 미치는 영향은 치명적일 수 있다. 개인위치정보가 어디엔가 기록으로 쌓일수록 정보수사기관에 이용될 가능성도 높아지게 될 것이다.

---

39) 의안번호 제1802396호

40) 자세한 내용은 본 글의 '통신비밀' 부분 참조.

41) 미디어오늘, 2011.10.6, "개인 위치정보 4천만건 몰래 추적당했다"

42) 디지털타임즈, 2011.12.18, "'위치정보 앱' 왜 불안한가 했더니?"

모든 위치정보가 개인식별성을 가지는 것도 아니며, 개인정보와 결합될 위험성도 다르다. 무엇을 위치정보로 볼 것인가 역시 맥락에 따라 달라질 수 있다. 따라서 위치정보를 이용한 서비스의 발전을 저해하지 않으면서도, 개인위치정보를 실효성있게 보호하기 위해서는 좀 더 섬세한 법제도가 마련될 필요가 있다.

(3) 통신비밀

헌법 제18조는 "모든 국민은 통신의 비밀을 침해받지 아니한다."고 규정하고 있다. 통신의 비밀은 개인이 그 의사나 정보를 우편물이나 전기통신 등의 수단에 의하여 전달 또는 교환하는 경우에 그 내용 등이 본인의 의사에 반하여 공개되지 아니할 권리를 말하며 통신의 자유라고도 한다. 국가안보 및 범죄수사 등 공공의 안전을 위한 감청은 허용될 수 있으나 최후적 수단으로 사용되어야 하며, 그 내용과 절차에 엄격한 사전 · 사후 통제장치를 마련해 국민의 통신의 자유와 사생활의 비밀과 자유에 대한 제한을 최소화하는 것이 바람직하다.

통신의 자유는 오늘날과 같이 전자우편 또는 인터넷의 활용이 일상화되고 있는 상황에서 통신행위와 표현행위를 포괄하는 양면성을 가진 자유이다. 통신기술의 발달은 개인간 의사전달 수단을 다양화함으로써 통신 자유를 확장하는데 기여했지만, 그에 못지않게 아니 그 이상으로 개인의 통신비밀을 광범위하게 침해할 수 있는 수단을 제공하고 있다. 오늘날 한 개인에게 통신 활동이 차지하는 비중을 감안할 때 통신 감청에 의한 개인 통신정보의 노출은 한 개인의 인격 전반의 노출은 물론 그에 따른 왜곡까지 우려된다는 점에서 더 심각한 문제를 야기한다. 신체 자유 제한은 외형적으로 드러나지만 통신 감청은 대상자가 의식할 수 없다는 점에서 더 심각한 인권 침해를 초래한다.

따라서 통신 비밀은 국가권력에 의한 제한을 최소화하고 통신사업자 등 사인에 의한 침해를 엄격히 통제함으로써 보호되어야 한다. 현행 「통신비밀보호법」에서는 동법에 의한 우편물의 검열 또는 전기통신의 감청이 범

죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다는 점을 명시하고 있다(동법 제3조의 제2항). 또한, 사이버공간에서 표현행위는 일반적인 언론 자유보다 더 강하게 보장되어야 하므로 익명성의 보장과 접속에 있어서 추적당하지 않을 권리가 강하게 보장되어야 한다(오동석, 2007).

국가안보 및 범죄수사 등의 목적으로 통신의 비밀을 제한하는 것과 관련한 현행 법률은 크게 「전기통신사업법」, 「통신비밀보호법」, 「형사소송법」으로 볼 수 있다.

〈표 3〉 통신 관련 자료 제공의 절차 현황

제공 대상	적용법률	제공 절차
이용자 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입/해지일자 [통신자료]	전기통신 사업법 제54조	요청사유, 해당이용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 요청 ※ 긴급한 사유가 있는 때에는 사후제출
가입자 전기통신일시, 전기통신개시 · 종료시간, 상대방 가입자번호, 사용도수, 인터넷 로그기록자료, 발신기지국의 위치추적자료, 정보통신기기 접속지 위치추적자료 [통신사실 확인자료]	통신비밀 보호법 제13조부터 제13조의5	요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(군사법원 포함) 또는 지원의 허가를 받아 요청 ※ 긴급한 사유가 있는 때에는 사후제출 ※ 정보기관의 경우 별도 규정
발송 · 수취하거나 송 · 수신하는 특정한 우편물이나 전기통신 또는 대상자가 일정한 기간에 걸쳐 발송 · 수취하거나 송 · 수신하는 우편물이나 전기통신 [통신제한조치]	통신비밀 보호법 제5조부터 제9조의2	통신제한조치의 종류 · 그 목적 · 대상 · 범위 · 기간 · 집행장소 · 방법 및 당해 통신제한조치가 허가요건을 충족하는 사유등의 청구이유를 기재한 서면 청구서와 청구이유에 대한 소명자료를 첨부하여 법원의 허가서를 발부받아 요청 ※ 긴급한 사유가 있는 때에는 36시간 이내 사후제출 ※ 정보기관의 경우 별도 규정
송 · 수신이 완료된 전기통신에 대한 압수 · 수색 · 검증	형사소송법 제215조	피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간 등을 기재하고 재판장 또는 수명법관이 서명날인한 압수 · 수색영장을 발부받아 요청

먼저 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입 또는 해지일자 등 통신 이용자의 인적사항에 대한 자료는 「전기통신사업법」 제54조에 의해 이루어진다. 이 법에 따르면 일반수사기관이나 정보수사기관이 통신사업자에게 이용자의 성명 등에 대한 통신자료를 요청할 때 서면에 의하도록 하였다. 이 조항은 1991년 8월 「공중전기통신사업법」이 「전기통신사업법」으로 개정되면서 제54조에 '통신비밀의 보호'에 대한 규정을 신설하고 제3항에 "전기통신사업자 또는 … 전기통신사업의 일부를 수탁하여 취급하는 자는 수사상 필요에 의하여 관계기관으로부터 전기통신업무에 관한 서류의 열람이나 제출을 서면으로 요구받은 때에는 이에 응할 수 있다"고 규정한 것으로부터 유래했다. 그러나 수사기관이 '전기통신업무에 관한 서류의 열람이나 제출'을 요구할 수 있는 법률적 요건과 절차의 모호함에 대한 비판이 계속되었다.[43] 그로 인하여 2000년 1월 전기통신사업자에 대하여 전기통신업무에 관한 서류의 제출 등을 요구할 수 있는 자를 검사 및 수사관서의 장등으로 제한하고, 그 제공되는 서류의 범위를 한정하는 등 절차를 강화하는 개정이 이루어져 오늘에 이른다.

하지만 현행 법률에 따르면 통신자료에 대한 수사기관의 서면 요청에 있어 범죄사실의 입증이나 법원의 영장이 불필요하며, 긴급한 사유가 있는 때에는 서면을 사후에 제출해도 된다. 그 긴급한 사유가 무엇인지에 대해서는 법률에 규정을 두고 있지 않다. 이로 인하여 통신자료의 제공에 있어 남용의 가능성이 크므로 적절한 제한이 필요하다는 지적이 일고 있다. 이

43) "통신비밀의 보호를 정한 54조의 예만 해도 사업자에 대해 … 통화내용의 유출통로를 크게 넓힘으로써, 기본권 제한의 과잉금지 원칙을 스스로 거스르고 있다." 문화일보, 1999. 9. 4, "〈사설〉전화걸기 무서운 세상"; "통신업체에서는 수사기관들이 문서를 제출하지 않고 전화로 가입자정보를 요구해도 바로 알려주는 것이 관행으로 돼 있다." 경향신문, 1999. 9. 14, "보호막 뚫린 私生活 - '통신가입자 정보제공' 문제점"; "여야는 전기통신사업법에서 대표적인 '독소조항'으로 지적받고 있는 통화정보제공 관련부분의 개정을 추진키로 했다. 이 조항은 그동안 수사기관이 통화상대방의 전화번호, 통화시간, 특정 전화번호의 주소지 등 통화정보를 무차별적으로 제공받을 수 있어 법 남용의 소지가 많다는 지적을 받아왔다." 동아일보, 1999. 10. 21, "여야, 전기통신사업법 개정 통화정보제공 제한".

문제에 대하여 헌법소원이 제기되어 현재 심리 중이며[44]. 국회에도 통신자료의 제공에 있어 법원의 허가를 받도록 하는 내용의 법안들이 발의되었다[45].

수사기관과 정보기관의 통신자료 요청은 해마다 급증하는 추세에 있으며 2007년 특히 인터넷 분야에서 급격히 증가하였다. 이는 2007년 7월 37개 주요 인터넷 사이트에 국가적인 실명제가 의무화되면서 이에 대한 수사기관의 요청이 증가한 데 따른 것으로 추정된다. 다음, 야후 코리아, 디씨인사이드 등은 의무적 실명제 도입 후부터 이용자의 실명 정보를 수집하기 시작했기 때문이다.

〈표 4〉 통신자료 제공 통계

* 단위 : 문서수

통신수단 / 년	유선전화	이동전화/무선호출	PC통신/인터넷	합계
2005	56,614	244,999	41,158	342,771
2006	48,462	204,080	71,024	323,566
2007	57,375	275,342	93,691	426,408
2008	58,374	296,914	119,280	474,568
2009	59,913	358,375	143,179	561,467
2010	61,418	397,294	132,337	591,049

* 출처 : (구)정보통신부 / 방송통신위원회

44) 헌법재판소 2010헌마439, 전기통신사업법제54조 제3항 위헌확인 등(심리중)

45) 2009년 5월 22일 이정현 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1804925호)」에서는 「전기통신사업법」에 규정된 가입자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입 또는 해지일자 등을 가입자정보로 정의하여 「통신비밀보호법」의 규정에 포함하고, 검사 또는 사법경찰관이 수사 또는 형의 집행을 위하여 필요한 경우 법원의 허가를 받아 전기통신사업자에게 가입자정보의 제공을 요청할 수 있도록 하여 통신자료의 제공과 관련한 절차 규정을 강화하였다. 2010년 3월 2일 이정희 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1807787호)」에서는 「전기통신사업법」 에 따른 '통신자료'를 이 법의 적용을 받도록 하여 '통신사실 확인자료'와 같이 엄격한 절차에 따라 제공받을 수 있도록 하였다.

한편, 통신 이용자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료 등 통신사실 확인자료는 「통신비밀보호법」에 의해 제공된다. 「통신비밀보호법」은 일반수사기관이나 정보기관이 통신사업자에게 통신사실 확인자료를 요청할 때 법원의 허가를 받도록 하였으며 사업자에 협조 의무를 규정하였다. 본래 「통신비밀보호법」이 제정되었을 당시에는 통신사실 확인자료 제공에 대한 아무런 조항이 없어 「전기통신사업법」에 의해 제공되어 오다가, 2001년 12월 「통신비밀보호법」이 개정되면서 "검사 또는 사법경찰관이 … 통신사실 확인자료제공을 요청하는 경우에는 미리 서면 또는 이에 상당하는 방법으로 관할지방검찰청 검사장(검찰관 또는 군사법경찰관이 통신사실 확인자료 제공을 요청하는 경우에는 관할 보통검찰부장을 말한다)의 승인을 얻어야 한다"고 관련 규정을 두게 되었다. 2003년부터 국정원과 국군기무사령부가 일간지 기자의 통화내역을 조회하는 등 통신사실 확인자료 제공의 오남용 문제가 사회적으로 불거지면서,[46] 2005년 5월 개정에서 일반수사기관과 정보기관이 통신사실 확인자료 제공을 요청할 경우 "요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다) 또는 지원의 허가를 받"도록 절차가 강화되었다.

또한 정부는 2005년 통신비밀보호법 시행령을 개정하여 통화내역이나

---

46) 한겨레신문, 2003. 10. 7, "[사설] 기자 '통화' 조회는 반언론적 발상"; 한겨레신문, 2003. 10. 8, "통화 멋대로 조회…"영장도입을""; 국민일보, 2004. 1. 30, "[사설] 정부가 아직도 이 수준인가"; 경향신문, 2004. 1. 30, "국정원, 靑요구로 기자 통화내역 조회"; 한국일보, 2004. 2. 18, "한국일보 기자 통화내역도 조회"; 국민일보, 2004. 2. 18, "기무사령부도 기자 통화내역 조회했다"; 한국일보, 2004. 2. 19, "'통화내역 조회' 가입자 33명중 1명꼴"; 서울신문, 2004. 2. 19, "[사설] 통화조회 남발 이대로 안된다" 등 참조.

로그기록 등 통신사실 확인자료의 보관을 의무화하였다. 그 기간은 매체별로 차등을 두어 시내·시외 유선전화 관련 자료는 6개월, 이동전화 관련 자료는 12개월, 인터넷 관련 자료는 3개월을 규정하였다. 이 시행령 개정은 모법에 관련 근거가 없으며(포괄적 위임), 모든 통신 이용자를 잠재적 범죄자로 간주한다는 점에서 그 위헌성을 지적받고 있다.

〈표 5〉 통신사실 확인자료 제공 통계

* 단위 : 문서수

통신수단 / 년	유선전화	이동전화/무선호출	PC통신/인터넷	합계
2005	21,636	118,940	54,793	195,369
2006	21,948	87,114	41,681	150,743
2007	31,337	110,738	41,584	183,659
2008	37,912	128,166	46,667	212,745
2009	43,426	147,577	57,549	248,552
2010	42,836	146,922	49,091	238,849

* 출처 : (구)정보통신부 / 방송통신위원회

다른 한편으로 통신사실 확인자료 제공의 요건과 절차가 엄격하지 않아 오남용되고 있다는 비판이 일고 있다. 현행 법률에 따르면 수사기관이 '수사 또는 형의 집행을 위하여 필요한 경우'만으로 통신사실 확인자료의 제공을 요청할 수 있도록 하여 범죄사실을 입증할 필요가 없다. 긴급한 사유가 있는 때는 법원의 허가를 사후에 받도록 하였고, 긴급한 사유가 무엇인지에 대해서는 법률에 규정을 두고 있지 않다. 이와 관련하여 통신사실 확인자료의 제공 요건과 절차를 강화한 법안들이 발의되었다[47].

47) 2009년 5월 22일 변재일 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1803789호)」에서는 범죄수사를 위한 통신사실 확인자료 요청의 경우 예외 없이 법원의 허가를 먼저 얻은 후 하도록 절차를 강화하였다. 또한 현행 법률이 정보기관의 경우 '국가안전보장에 대한 위해를 방지하기 위하여 정보수집이 필요한 경우' 전기통신사업자에게 통신사실 확인자료 제공을 요청할 수 있도록 규정된 데 대하여(동법 제13조의4) 변재일 의원의 개정안에서는 현행 감청의 허가 요건과 동일하게 '국가안전보장에 대하여 상당한

수사기관과 정보기관의 통신사실 확인자료 요청은 해마다 급증하는 추세에 있으며 특히 불거진 문제는 2010년 그 실태가 처음 알려진 '기지국 수사'이다. 2010년 4월 2일 방송통신위원회의 발표에 따르면[48] 형사소송법상 '압수수색영장'을 발부받는 방식으로 제공되던 기지국 단위 통신사실 확인자료 제공이 2009년 하반기부터 통신비밀보호법 상 '통신사실확인허가서'로 대체되었다. 이와 같이 특정 시간대 특정 기지국에서 발신된 모든 전화번호를 압수수색이나 통신사실 확인자료로 제공받는 수사 방식을 '기지국 수사'라고 지칭한다. 기지국 수사 1회에 통상 12,000건의 전화번호가 제공되며, 제공 요청은 계속 증가하여 2010 전체적으로는 38,706,986건의 전화번호가 제공되었다[49]. 기지국 수사의 문제점은 일차적으로 법률에 규정된 통지 의무(동법 제13조의3)를 경찰이 이행하지 않는다는 것이다. 통지 의무를 이행하지 않으면 피해자가 피해 사실을 인지하기 어려우며 그 권리 구제 또한 불가능하다. 2010년 4월 임시국회에서 야당 의원들이 기지국 수사가 위법이라고 규정하고 자료제출을 거부하는 법원, 경찰, 방통위를 규탄하고 현장검증을 주장하였으나, 기지국수사의 정확한 규모와 피해당사자는 지금껏 확인되지 않고 있다. 이와 관련하여 기지국 수사를 금지하거나 통지 의무를 이행하지 않으면 처벌하는 내용의 법안들이 발의되었다[50].

위험이 현존하거나 예상되어 그 위해를 방지하기 위한 경우'로 그 요건을 강화하였다. 이정희 의원의 개정안에서는 "수사 또는 형의 집행을 위하여 필요한 경우"라는 요건을 "수사(피의자가 죄를 범하였다고 의심할만한 상당한 이유가 있는 경우에 한한다) 또는 형의 집행을 위하여 필요한 경우"로 강화하였다. 또한 "요청사유, 해당 가입자와의 연관성"을 기록한 서면으로 법원의 허가를 요청하도록 한 절차를 "해당 피의자의 범죄혐의에 대한 소명자료, 해당 통신자료제공이 수사 또는 형의 집행을 위하여 필요하다는 점에 대한 소명자료"로 강화하였다.

48) 방송통신위원회, "′ 09년 하반기 통신사실확인자료 제공 등 협조 현황", 보도자료(2010. 4. 2).

49) 방송통신위원회, "′ 10년 하반기 감청 및 통신사실확인자료 제공 현황", 보도자료(2011. 5. 4).

50) 2010년 4월 20일 전병헌·변재일 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1808219호)」에서는 통신사실 확인자료 요청 시 해당 가입자의 인적사항을 반드시 기입하도록 하여 불특정 다수에 대한 통신사실

다른 한편으로 실시간 위치추적의 문제도 논란이 되어 왔다. 현재 정보수사기관은 실시간 위치추적 자료를 통신사실 확인자료로서 제공받고 있으며, 법원의 허가서가 발급되면 허가서에 적힌 사용기한 동안 통화가 발생하지 않더라도 매 10분 또는 30분 간격으로 기지국의 위치정보를 담당 수사관의 휴대전화 SMS로 발송받고 있었다[51]. 국정감사 자료에 따르면 통신사실 확인자료를 이용하여 휴대전화 실시간 위치추적을 한 건수는 2009년 상반기에만 일평균 53건에 달하며, 동기 이통사 통신사실 확인자료 제공 건수 중 13%에 해당한다[52]. 또한 정보통신망에서의 실시간 위치추적이 남용된다는 지적도 있어왔다[53]. 이러한 '전자미행'은 통신비밀보호법이 통신사실 확인자료에 대한 규정을 신설하였던 2001년 당시 접수시점 이전의 과거 자료에 한정되는 의미로 보고 입법 심사가 이루어졌다는 점에서[54] 입법취지에 어긋나며, 과거의 자료를 전제하고 완화된 요건 하에서 장래의 정보를 제공하는 것이 위헌이라는 주장이 제기되고 있다.

가장 민감하고 논란이 많이 되는 것은 전화 통화, 이메일 등 공개되지 않은 통신의 내용에 대하여 통신제한조치, 즉 감청을 실시하는 경우이다. 소위 '초원복집' 사건[55] 등 많은 논란을 거쳐 1993년 제정된 「통신비밀보

확인자료 요청을 못하도록 하였고, 2010년 9월 13일 변재일 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1809324호)」에서는 통신사실 확인자료제공 통지의무를 위반할 경우 벌칙조항을 두었다.

51) 한겨레, 2009. 1. 14, "경찰 '묻지마 감청'…사후통보 시늉만".

52) 변재일, 2009, "09년 상반기 휴대전화 위치추적 허가 일평균 53건", 보도자료(2009. 10. 22).

53) 경향신문, 2011. 12. 3, "유명 게임회사들, 수사기관 '전자미행'에 협조하고 있다?".

54) 과학기술정보통신위원회 수석전문위원, 通信秘密保護法中改正法律案에대한 意見提示의件 : 檢討報告書(2001. 2), 6면.

55) 1992년 12월 제14대 대통령 선거를 앞두고 당시 법무장관 등 정부 주요기관장들이 부산의 한 음식점에 모여, 여당 후보를 당선시키기 위해 지역감정을 부추기고 야당 후보를 비방하는 내용을 유포시켜야 한다고 논의하는 대화 내용이 야당 후보 측의 도청에 의해 언론에 공개됐다. 여당 후보였던 김영삼 씨가 이 사건을 둘러싼 논란 속에 대통령으로 당선되었고, 집권 초기부터 도청을 방지하기 위한 법률 제정이 정부와 국회에서 논의되기 시작하였다.

호법」은 제정 당시부터 법률적 근거 없이 시행되던 정보수사기관의 도청을 제도적으로 통제하는 데 초점을 두고 이들이 감청을 요청할 때 법원의 허가서를 받도록 규정하였다. 이때 통신 감청은 헌법상의 기본권을 중대하게 제한하는 것이므로 법률에 규정된 대상 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가될 수 있다(동법 제5조). 또한 법률에서는 검사와 사법경찰관이 법원에 대하여 감청의 허가를 구하는 절차에 대하여 상당히 엄격하게 규정하였다(동법 제6조).

그럼에도 불구하고 국정원의 감청 비율이 높다는 사실이 논란을 빚어 왔다. 아이디/전화번호수별로 기관별 제공 현황을 보았을 때 국정원의 제공 비율은 무려 97~98%에 달한다.

〈표 6〉 기관별 통신제한조치 통계

* 단위 : 전화번호/아이디건수

기관 / 년	검찰	경찰	국정원	군수사기관	합계	국정원비율
2005	100	241	8,082	112	8,535	94.7%
2006	43	131	8,440	51	8,665	97.4%
2007	41	95	8,628	39	8,803	98.0%
2008	24	94	8,867	19	9,004	98.5%
2009	9	163	9,278	47	9,497	97.7%
2010	4	227	8,391	48	8,670	96.8%

* 출처 : (구)정보통신부 / 방송통신위원회

이 통계는 (구)정보통신부와 방송통신위원회가 통신비밀보호법에 의해 사업자로부터 제출받은 자료에 의해 구성된 것으로서, 정보수사기관이 보유하고 있는 감청 장비를 이용하여 직접 감청하는 경우는 포함하지 않은 것이다. 이러한 한계에도 불구하고 국정원의 감청 비율이 지나치게 높다는 사실은 현행 법률에 명시된 보충성의 원칙이 충분히 지켜지고 있는지에 대해 의구심을 갖게 한다. 일반 범죄수사와 관련이 없는 정보기관이 광범위

한 감청을 실시하는 것은 정치적인 반대자들을 감시하고 억압하는 불법적인 목적으로 사용될 수 있다는 점에서 매우 심각한 문제이다. 2005년 (구) 안전기획부와 국정원의 불법 도청 실태가 폭로된 일명 '안기부 X파일' 사건 이후로도 현재까지 「통신비밀보호법」의 관련 조항들은 개선된 바가 없기에 불법 감청 문제는 또다시 불거질 수 있는 소지가 잠복해 있다.

현재 모든 감청이 법원의 영장 하에 적법하게 이루어지고 있다 하더라도 법원이 그 기능을 다하지 못하고 있다는 우려가 제기되고도 있다[56]. 더불어, 현행 법률이 법원의 영장 발부 후에는 사후 감독에 대한 규정을 전혀 명시하지 않고 감청 집행과 그 자료에 대한 사항을 감청을 집행하는 정보기관의 재량에 전적으로 맡기고 있는 실태도 문제이다. 감청 집행 시 법원 등에서 입회를 하여 실제 감청이 발부된 영장대로 집행되도록 감독하고 감청 결과는 봉인하여 법원에서 관리하고 필요시 당사자 등이 청구하여 열람할 수 있도록 보장하는 방안이 강구될 필요가 있다[57]. 현행 「통신비밀보호법」에 영장주의의 예외가 존재한다는 사실도 계속하여 문제로 지적되어 왔다. 먼저 정보기관이 외국인을 감청할 때는 법원의 허가가 아닌 대통령 승인만으로 가능하도록 규정하였다(동법 제7조 제1항). 또한 "국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 … 규정에 의한 절차를 거칠 수 없는 긴급한 사유가 있는 때"에는 법원의 허가 없이 감청을 할 수 있다(동법 제8조 제1항). 이러한 규정들은 영장주의를 우회할 수 있는 방법을 제공함으로써 편법적이거나 불법적인 통신 감청으로 이어질 수 있다는 우려를 낳고 있다.

---

56) 조국통일범민족연합 사건 당시 감청 영장이 2개월씩 무려 14차례 연장되어 총 28개월간 감청이 이루어진 사례도 있었다. 이러한 관행은 2010. 12. 28. 헌법재판소의 위헌 결정 이후에서야 중단되었다. 헌재 2010.12.28 결정, 2009헌가30.

57) 일본, 대만, 독일 등에서 이러한 제도를 운영하고 있다. 이정희 의원의 개정안에는 이와 같은 내용의 제도 개선안이 포함되었다.

〈표 6〉 통신수단별 통신제한조치(감청) 통계

* 단위 : 문서수

통신수단 / 년	유선전화	이동전화/무선호출	PC통신/인터넷	합계
2005	621	1	355	977
2006	577	0	456	1,033
2007	503	0	646	1,149
2008	506	0	646	1,152
2009	574	0	942	1,516
2010	358	0	723	1,081

* 출처 : (구)정보통신부 / 방송통신위원회

2005년 안기부 X파일 사건에서 불법 휴대전화 도청 문제가 불거지자 국정원은 휴대전화 도청 장비를 폐기하였다고 발표하였고[58], 그후 현재까지 공식적인 통계상으로는 휴대전화 감청이 이루어지고 있지 않다. 이 사건 이후로 국정원은 휴대전화 감청이 불가능하여 범죄수사에 제약이 많다는 이유에서 통신비밀보호법 개정을 추진하여 왔다[59]. 이 법안은 전기통신사업자에게 감청 장비를 구비할 의무를 신설하여 이를 위반할 경우 10억원 이하의 이행강제금을 부과하고, 통신사실 확인자료 보관 의무를 신설하는 한편 그 제공 대상에 GPS 위치정보를 추가하여 논란을 빚었다. 국가인권위원회는 "사실상 감청 자체가 예외적 허용이 아니라 상시적으로 행해질 수 있는 것이라는 인식을 조성하면서 개인 사생활 및 프라이버시를 크게 위축시킬 수 있"다고 지적하며 이 법안을 반대하였다[60].

---

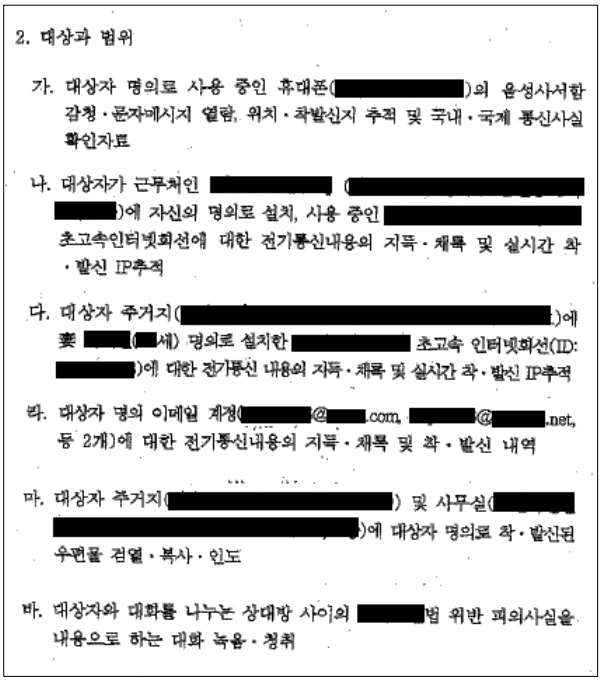
58) 국정원 발표에 따르면, 2001년 12월 통신비밀보호법이 개정되어 감청설비 신고 등 절차가 강화되고 16대 대통령 선거를 앞두고 불법 도청 논란이 커지자 안기부가 2002년 3월 불법 도청팀을 해체하고 CAS는 물론 R2 등 도청 장비들을 전량 폐기하였다고 한다.

59) 통신비밀보호법 일부개정법률안(대안), 2007. 6. 26(의안번호: 176928)와 통신비밀보호법 일부개정법률안(이한성 의원 대표발의), 2008. 10. 30(의안번호: 1801650) 참고.

60) 국가인권위원회, "「통신비밀보호법 일부개정법률안(이한성 의원 대표발의)」에 대한 의견표명"(2009.2.27).

인터넷 감청은 증가하는 추세 속에 있으며 최근에는 특히 '패킷 감청' 논란이 커지고 있다. 남북공동선언실천연대 사건에 대한 재판과정에서 국정원이 패킷 감청을 실시한 사실이 드러나자, 2009년 8월 31일 인권단체들이 이를 비판하는 기자회견을 개최함으로써 패킷 감청 문제가 처음 알려졌다[61]. 같은 해 국정감사에서는 국정원이 보유한 패킷 감청 장비가 31대라는 사실이 알려졌다[62].

〈그림 1〉 감청 허가서 (일부 예시)



2. 대상과 범위

가. 대상자 명의로 사용 중인 휴대폰([redacted])의 음성사서함 감청·문자메시지 열람, 위치·착발신지 추적 및 국내·국제 통신사실 확인자료

나. 대상자가 근무처인 [redacted] ([redacted])에 자신의 명의로 설치, 사용 중인 [redacted] 초고속인터넷회선에 대한 전기통신내용의 지득·채록 및 실시간 착·발신 IP추적

다. 대상자 주거지([redacted])에 妻 [redacted](□세) 명의로 설치한 [redacted] 초고속 인터넷회선(ID: [redacted])에 대한 전기통신 내용의 지득·채록 및 실시간 착·발신 IP추적

라. 대상자 명의 이메일 계정([redacted]@[redacted].com, [redacted]@[redacted].net, 등 2개)에 대한 전기통신내용의 지득·채록 및 착·발신 내역

마. 대상자 주거지([redacted]) 및 사무실([redacted])에 대상자 명의로 착·발신된 우편물 검열·복사·인도

바. 대상자와 대화를 나누는 상대방 사이의 [redacted]법 위반 피의사실을 내용으로 하는 대화 녹음·청취

61) 아이뉴스24, 2009. 8. 31, "국정원 인터넷회선 패킷 감청 의혹제기"; 오마이뉴스, 2009. 8. 31, "국정원, 인터넷 사용내역도 엿봤다"; 한겨레신문, 2009. 8. 31, "국정원, 우리집 인터넷 통째로 엿봤다"; 서울신문, 2009. 9. 1, "국정원, 인터넷회선 통째 감청 의혹" 등.

62) 국민일보, 2009. 11. 16, "인터넷 사용 내용 실시간 수집 가능… 국정원 '패킷 감청' 설비 확충 안팎".

법원은 허가서 한 장으로 우편물 검열과, 유선전화·휴대전화·인터넷 메일에 대한 감청은 물론 인터넷 회선 전체와 대화에 대한 감청까지 한번에 모두 실시하는 저인망식 감청을 허용해 왔다(〈그림 1〉). 그중 패킷 감청(〈그림 1〉의 '나'항과 '다'항)은 피의자의 주거지와 직장에서 사용하는 인터넷 회선 전체에 대한 감청을 허가한 것으로서, 패킷 감청을 이용하면 대상자가 인터넷을 통해 접속한 사이트 주소와 접속시간, 대상자가 입력하는 검색어, 전송하거나 수신한 게시물이나 파일의 내용을 모두 볼 수 있다. 이메일과 메신저의 발송 및 수신내역과 그 내용 등 통신내용 일체도 마찬가지로 볼 수 있다. 이는 피의자에 대하여는 포괄영장을, 피의자와 동일회선을 사용하는 사람들, 피의자와 통신한 제3자에게 대하여는 일반영장의 성격을 갖게 된다는 측면에서 영장주의에 위배되고 과잉금지원칙에 위배되어 위헌이라는 비판을 받고 있다. 패킷 감청은 그 범위가 너무 광범위하여 대상자와 대상 통신내용을 특정할 수 없다는 점에서 우리 「통신비밀보호법」이 허용하는 감청의 범위를 벗어난 위법한 감청이라는 것이다. 더구나 수사에 필요한 자료는 해당 패킷이 목적지에 도달한 후 기존의 이메일 전달(forwarding) 방식의 감청이나 압수·수색으로도 충분히 입수 가능하므로 패킷 감청이 굳이 인정될 필요가 없다. 결론적으로 통신 감청이 최소한으로, 보충적으로 이루어져야 한다는 「통신비밀보호법」의 제정 취지대로라면 현재와 같은 형태의 인터넷 회선 감청은 중지되어야 할 필요가 있다. 패킷 감청에 대해서는 헌법소원이 제기되어 현재 심사 중이다[63]. 헌법소원에 대한 국정원의 답변에서 지메일 등 외국계 이메일을 감청한다는 사실이 알려지기도 하였다[64].

실시간 통신이 아닌 송수신이 완료된 이메일 등은 통신비밀보호법의 보호대상이 아니기 때문에[65] 형사소송법상 압수수색의 방식으로 제공되고

63) 헌법재판소 2011헌마165, 통신제한조치허가위헌확인 등(심리중).

64) 한겨레, 2011. 9. 16, "구글 지메일도 국정원이 감청".

65) 대판 2003. 8. 22, 2003도3344; 박영선,
"압수수색·통신감청·통신사실확인자료제공 등 올 상반기에만 33만 7천여건",
보도자료(2008. 10. 10) 참고.

있다. 그러나 그 제공 요건이 지나치게 완화되어 있어 장기간에 걸쳐 제공되는 등 오남용되는 문제가 지적되어 왔으며 일반 압수수색과 달리 당사자 참여권을 보장하지 않는 것 또한 문제로 지적되어 왔다. 이에 제공 요건을 강화하는 내용의 법안이 발의되었다[66].

통신감청 및 통신자료의 제공은 일차적으로 국가기관이 범죄수사 등 공익을 위하여 국민의 기본권을 제한하는 것이지만, 통신사업자는 감청의 중요한 행위자이다. (구)한국통신 등 주요 기간통신사업자는 군사독재정권 시절부터 국가 감청의 주요한 협조자로 활동해 왔다. 이 과정에서 설령 국가기관이 불법적인 도청을 행한다 하더라도 통신사업자가 이를 거부하거나 고발하지 못해 왔다. 안기부 X파일 사건에서 (구)한국통신이 안기부의 요구에 따라 R2와 같은 불법 도청 장비를 자신들의 설비에 설치하거나 불법 회선을 제공한 사실 외에도, 일상적으로 수사기관의 불법 도청 요구에 협조한 사실이 드러났다. 2000년 5월 12일 감사원 발표에서는 법원의 감청 영장 등을 확인하지 않거나 수사기관에 비밀번호나 복제용 인식부호를 넘겨주는 등 통신사업자들의 불법적인 협조 사례가 다수 발견되었다[67].

최근에는 기간통신사업자가 맞춤광고, 경쟁서비스 차별 등 자사의 이해관계를 위하여 패킷 감청 기술인 DPI를 실시하여 논란을 빚고 있다. 이미 2008년 미국과 영국에서 기간통신사업자가 맞춤광고를 이유로 DPI 장비를 설치한 바 있고, 2009년 한국에서는 KT가 DPI를 이용한 맞춤광고 서비스로 '쿡스마트웹'의 서비스를 시작하여 논란을 빚었다[68]. 최근에는 이동통신 사업자가 mVoIP 서비스를 차별하려는 목적으로 DPI를 사용하는 사례가 전 세계에서 보고되고 있는데, 한국에서는 2011년 KT와 SKT가 다음커뮤니케이션즈의 마이피플을 차별하는 과정에서 DPI를 사용하는 문제

66) 이정희 의원의 개정안에는 "피의자가 죄를 범하였다고 의심할만한 상당한 이유가 있고 송·수신이 완료된 전기통신에 대한 압수·수색·검증이 범죄수사에 필요하며 해당 압수·수색·검증으로 범죄의 혐의를 확인할 수 있다고 볼만한 상당한 개연성이 있는 경우에 한하여" 이메일 등 송수신이 완료된 전기통신에 대하여 압수수색할 수 있도록 규정하였다.

67) 2000년 5월 12일 감사원은 "통신제한조치 운용실태 감사결과"를 발표하였다.

68) 시범 서비스 이후 중단된 것으로 알려져 있다.

가 쟁점으로 불거졌다[69]. 즉 이동통신사들이 통신이용자가 무선패킷으로 주고받는 문자 등 통신내용을 DPI 기술로 감청하여 경쟁사의 음성문자를 차단했다는 의혹이 제기된 것이다. 이러한 상황은 통신 감청의 문제와 동시에 망중립성에 대한 고민거리를 우리 사회에 던지고 있다.

4. 결론과 제언

현대 정보 사회에서 개인정보의 수집과 처리가 많아지면서 프라이버시 침해 논란이 불거지자 개인정보 자기결정권을 보장하는 내용으로 보호 입법이 이루어져 왔다. 그러나 정보주체의 의사와 상관없이 개인정보가 국가적·상업적 목적을 위하여 활용될 가능성은 높아지고만 있으며, 특히 정보통신망에서는 정보주체가 인식하지 못하는 사이에 개인정보가 처리되거나 과다한 통신 감청과 자료 제공이 이루어져 왔다. 최근 모바일 환경 하에서는 위치정보의 제공이 문제시되면서 정보주체의 통제권이 무력해져 간다는 비판이 제기되고 있다. 따라서 정보를 수집·활용하는 주체들에 대한 실효성 있는 규제방안의 모색과 더불어, 헌법상 기본권으로서의 자기정보통제권 보장을 위한 노력이 계속되어야 한다(심우민, 2011b).

정보통신망에서의 개인정보 유출 사고 위험을 줄이기 위해서는 우선 개인정보의 수집 자체가 최소화되어야 한다. 특히 민간에서의 주민등록번호 수집은 제한할 필요가 있다. 민간영역에서는 주민등록번호 수집을 원칙적으로 금지해야 하며, 인터넷 실명제, 전자상거래 소비자보호법 등 주민등록번호 수집을 요구하는 법제도 개선될 필요가 있다. 둘째, 인터넷 실명제는 폐기되어야 한다. 비단 주민등록번호 수집 및 명의도용 문제가 아니더라도 인터넷 실명제는 그동안 많은 비판을 받아왔다. 악플을 규제하겠다는 인터넷 실명제 도입의 명분은 효과를 거두고 있는지는 여전히 의문인 반면, 이용자의 표현을 통제하고 추적하기 위한 수단으로는 효과적으로 활용

69) 2011년 11월 23일 진보네트워크센터와 경제정의실천시민연합이 이 문제에 대하여 공정거래위원회, 국가인권위원회, 방송통신위원회에 신고 또는 진정을 제기하였다.

되어 왔다. 2009년 유튜브의 인터넷 실명제 도입 거부 이후에는 자국 기업에 대한 역차별이라는 인터넷 기업들의 성토도 쏟아졌다. 정부는 주민등록번호 대신 아이핀을 쓰는 방향으로 유도하고 있지만, 아이핀 역시 불필요한 인증을 요구한다는 점에서, 그리고 이용자의 인터넷 가입기록 유출 등 더 큰 피해를 야기할 수 있다는 점에서 대안이 될 수 없다. 셋째, 이미 유출된 주민등록번호의 피해 확산을 방지하기 위해서는 새로운 주민등록번호로의 재발급이 허용되어야 한다. 또한, 장기적으로는 현행 주민등록번호 제도를 개편할 필요가 있다.[70] 넷째, 정보주체의 자기정보통제권이 실질적으로 보장되어야 한다. 특히, 위탁 및 제휴 등을 통해 개인정보가 타 기업과 광범위하게 공유되는 현실에서, 자기정보통제권의 보장을 위해서는 제3자 제공 내역에 대해서도 쉽게 열람할 수 있도록 해야 한다.

스마트폰의 확산으로 다양한 위치정보 앱 및 서비스가 등장함에 따라, 개인에 대한 추적·감시의 위험도 높아지고 있다. 그러나 현행 「위치정보법」은 변화하는 현실을 제대로 반영하지 못하고 있는 실정이다. 익명의 위치정보 활용은 보장하되, 정보주체의 식별가능성이 있는 위치정보의 경우에는 엄격한 보호가 필요하다. 위치정보의 활용이 사회적 약자에 대한 감시에 이용되지 않도록 정보주체의 통제권이 보장되어야 한다. 언제든지 위치정보 수집에 대한 동의를 철회할 수 있어야 하며, 본인의 위치정보가 제3자에게 제공되었을 경우 통지받을 수 있도록 실효성있는 조치가 필요하다. 아직 많은 사람들이 위치정보의 프라이버시 침해에 대해 우려를 갖고 있는만큼, 개인위치정보의 실효성있는 보호가 오히려 위치기반 서비스 발전의 기반이 될 수 있다.

정보수사기관이 통신자료, 통신사실확인자료, 통신감청, 이메일에 대한 압수수색을 집행할 때는 오남용되지 않도록 그 요건과 절차를 보다 강화할 필요가 있으며 법원의 실질적인 통제 기능이 보장되어야 한다. 구체적으로 보면 다음과 같다. 첫째, 현재 법원의 허가 없이 제공되는 가입자 정보, 즉

70) 현행 주민등록번호 제도는 전 국민에게 강제발급된다는 점, 번호 자체에 생년월일 등 개인정보를 포함하고 있다는 점, 원칙적으로 재발급을 허용하지 않고 있다는 점 등의 문제가 지적되고 있다.

통신자료에 대하여 통신비밀보호법의 적용을 받도록 하고 '통신사실확인자료'와 같은 법원의 허가 절차에 따라 제공받도록 해야 한다. 둘째, 통신사실확인자료를 제공받을 때는 해당 피의자의 범죄혐의에 대한 소명자료, 해당 통신자료제공이 수사 또는 형의 집행을 위하여 필요하다는 점에 대한 소명자료를 첨부하여 법원의 허가를 받도록 절차를 강화한다. 셋째, 통신사실확인자료 중 위치정보추적자료의 경우 장래의 정보를 제공할 때 통신제한조치에 준하는 엄격한 절차에 따라 제공받도록 해야 한다. 넷째, 범죄수사를 위한 통신제한조치의 허가요건을 보다 강화하여, 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 현저히 어려운 사실이 소명되며, 해당 통신제한조치로 범죄의 혐의를 확인할 수 있다고 볼만한 상당한 개연성이 있는 경우에 한하여 허가하도록 하여 보충성의 요건을 충족하도록 하고, '국가보안법에 규정된 범죄' 전체를 대상으로 하는 등 폭넓은 현행 대상범죄의 범위를 축소하여야 한다. 또한 통신제한조치의 허가를 청구할 때는 피의자의 성명, 피의사실의 요지, 죄명, 적용법조, 통신제한조치의 대상이 된 통신수단, 통신제한조치의 종류·그 목적·대상·범위·집행장소·방법·기간 및 그 기간이 경과하면 통신제한조치를 하지 못하며 허가서를 반환하여야 한다는 취지, 그 밖에 대법원규칙으로 정하는 사항을 상세히 기재하도록 하여 피의자가 특정되지 않는 감청 등의 오남용을 방지하여야 한다. 통신제한조치의 기간 또한 2개월에서 10일로 단하고 연장을 금지해야 한다. 국가안보를 위한 통신제한조치 역시 국가의 존립에 현실적이고 상당한 위협을 가할 것으로 예상되는 경우에 한하여 시행하도록 요건을 강화한다. 다섯째, 대통령의 승인을 얻어야 하는 통신제한조치와 긴급통신제한조치를 삭제하여 무영장주의를 일소한다.

여섯째, 통신제한조치를 집행하거나 통신자료를 제공받은 경우에 처분여부와 관계없이 통신제한조치를 종료한 날부터 30일 이내에 통지하도록 하여 통지 누락의 소지를 없애야 한다. 일곱째, 송 · 수신이 완료된 전기통신의 압수 · 수색 · 검증에 대한 근거규정을 신설하고 통신제한조치에 준하도록 그 절차를 강화한다. 여덟째, 특히 감청 집행 시 법원 등에서 입회를

하여 실제 감청이 발부된 영장대로 집행되도록 감독하고 감청 결과는 봉인하여 법원에서 관리하고 필요시 당사자 등이 청구하여 열람할 수 있도록 보장하는 방안이 강구될 필요가 있다. 아홉째, 패킷 감청 등 인권침해적인 기법의 사용은 국가기관과 통신사업자 모두에게서 중단되어야 한다.

〈참고문헌/자료/사이트 등〉

권현오, 2007, “IPTV의 프라이버시 침해요인 분석 및 보호방안 연구”, 한국정보보호진흥원.

김일환, 2005, “個人識別番號(住民登錄番號)의 違憲性與否에 관한 考察”, 국가인권위원회 주최 토론회 「주민등록번호제도 이대로 좋은가?」(2005. 4. 6).

김진형·황준, 2008, “방송 통신 융합 환경에서의 개인정보보호를 위한 보안 기법에 관한 연구”, 한국인터넷정보학회 2009 제20차 정기총회 및 추계학술발표대회(2009. 10), 51-54면.

베이커, 스티븐, 2010, 『뉴머러티 : 데이터로 세상을 지배하는 사람들』, 이창희 역, 세종서적.

성낙인 · 이인호 · 김수용 · 권건보 · 김삼용 · 이지은 · 김주영 · 손형섭 · 박진우 · 김송옥, 2008, “개인정보보호법제에 관한 입법평가”, 현안분석 2008-45, 한국법제연구원.

심우민, 2011a, “네이트 해킹사고와 포털의 개인정보보호”, 「이슈와 논점」 제282호, 국회 입법조사처(2011. 8. 9).

심우민, 2011b, “스마트폰을 통한 개인정보 무단수집의 문제점과 대책”, 「이슈와 논점」, 국회 입법조사처(2011. 12. 16).

오병일, 2011, “개인정보 유출 피해 최소화를 위한 법제도적 대안 – 인터넷 실명제와 주민등록번호를 중심으로”, 3500만명 개인정보 유출 사태의 원인 및 대책 마련을 위한 토론회 발표문 (2011.8.16)

오동석, 2007, “통신비밀보호법 개정안에 대한 반대의견”, 국회 문병호 의원 등 주최 토론회 「통신비밀보호법의 올바른 개정을 위한 토론회」(2007. 6. 5).

이민영, 2011, “애플社의 아이폰 위치정보 수집과 정보인권”, 〈기업의 개인정보 수집과 보호〉 토론회 발제문, 국가인권위원회 (2011.8.31)

이인호, 2001, “개인정보자기결정권의 한계와 제한에 관한 연구”, 「개인정보연구」 01-01, 한국정보보호진흥원.

이진규, 2011, “개인정보와 위치정보의 정의, 그리고 최근 정보유출사건과 관련된 고려사항”, 〈기업의 개인정보 수집과 보호〉 토론회, 국가인권위원회 (2011.8.31)

정혜승, 2011, “개인정보 보호를 위한 기업의 노력과 근원적 고민”, 〈기업의 개인정보 수집과 보호〉 토론회 토론문, 국가인권위원회 (2011.8.31)

진보네트워크센터, 2009, “개인정보 수집·유통 실태조사”, 국가인권위원회 연구용역

진보네트워크센터·경제정의실천시민연합, 2011, “경실련과 진보넷, mVoIP 제한 및 DPI 사용 SKT와 KT 고발”, 보도자료(2011. 11. 23).

프레이저, 엘리, 2011, 『생각 조종자들 : 당신의 의사결정을 설계하는 위험한 집단』, 이현숙,이정태 공역, 알키.