통신의 비밀과 자유 및 온라인상 표현의 자유 보호의 쟁점과 개선방안[1)]

사단법인 오픈넷
김가연, 손지원

제1절 통신의 비밀과 자유의 보호 현황과 쟁점

1. 통신의 비밀과 자유의 의의와 최근 침해 양상

(1) 통신의 비밀과 자유의 헌법적 의미

정보통신기술의 발전은 시공을 초월한 자유로운 의견과 정보의 공유를 가능하게 해 개인의 사생활 영역을 확장할 뿐 아니라 민주적 참여를 촉진하고 인권의 보장에 기여하고 있다. 그러나 동시에 통신감시기술의 고도화에 따라 국가뿐만 아니라 기업이나 사인에 의한 감시가 광범위하게 이루어져 통신의 비밀을 침해하고 집회·결사의 자유, 표현의 자유 등 다른 기본권을 위협하며 시민사회의 활발한 기능을 제약한다. 그리고 우편물 검열이나 유선전화의 감청 같은 전통적 통신매체에 대한 감시를 넘어 휴대전화 감청 및 위치추적, 인터넷 패킷감청, 이메일 및 카카오톡에 대한 압수수색 등 새로운 통신매체에 대한 감시의 문제가 대두되고 있다.

우리나라 헌법은 제18조에서 "모든 국민은 통신의 비밀을 침해받지 아니한다."고 하여 통신의 비밀 보호를 그 핵심내용으로 하는 통신의 자유를 기본권으로 보장하고 있다. 통신의 자유를 기본권으로서 보장하는 것은 사적 영역에 속하는 개인간의 의사소통을 사생활의 일부로서 보장하겠다는 취지에서 비롯된 것이라 할 것이다.[2)] 이에 따라 통신의 비밀 보호란 개인이 그 의사나 정보를 통신수단에 의해 전달하는 경우 본인의 의사에 반해 그 내용, 당사자 등을 공개당하지 아니할 자유를 말한다. 그리고 본인의 동의 없이 통신수단을 개봉, 도청, 열람하는 행위 등은 금지되고, 적극적으로 통신사실의 존재, 통신내용, 통신방법, 통신당사자 등을 알고자 하는 행위가 허용되지 않을 뿐만 아니라, 통신사무에 종사하는 자가 직무상 적법하게 지득한 것이라도 이러한 통신내용 등을 누설하여서는 아니 된다.[3)]

우리 헌법상 제16조의 주거의 자유와 제17조의 사생활의 비밀과 자유가 '고립된 존재'로서의 개인의 사적 영역을 보호하는 것이라면, 제18조의 통신의 비밀 보호는 '타인과의 관계'를 전제로 하는 개인의 사적 영역을 보호하려는 취지로 볼 수 있다.[4)] 개인과 개인 간의 관계를 전

---

1) **본 보고서는 아주대학교 산학협력단이 수행하고 오픈넷이 참여한 2019년도 국가인권위원회의 정보인권 보고서 개정 발간 연구용역보고서의 일부분임.**

2) 헌재 2001. 3. 21. 2000헌바25.

3) 이진구·김일환, "통신비밀의 보호범위와 한계에 관한 비교법적 연구",「미국헌법연구」제27권 제1호, 2016, 219-220면.

4) 황성기, "현행 통신비밀 보호법제의 헌법적 문제점",「언론법학」제14권 제1호, 2015, 9면.

제로 하는 통신은 다른 사생활의 영역과 비교해 볼 때 국가에 의한 침해의 가능성이 매우 큰 영역이라 할 수 있다. 왜냐하면 오늘날 개인과 개인 간의 사적인 의사소통은 공간적인 거리로 인해 우편이나 전기통신을 통하여 이루어지는 경우가 많은데, 이러한 우편이나 전기통신의 운영이 전통적으로 국가독점에서 출발하였기 때문이다. 사생활의 비밀과 자유에 포섭될 수 있는 사적 영역에 속하는 통신의 자유를 헌법이 별개의 조항을 통해서 기본권으로 보호하고 있는 이유는, 이와 같이 국가에 의한 침해의 가능성이 여타의 사적 영역보다 크기 때문이라고 할 수 있다.[5] 통신의 자유는 물론 사인간에 있어서도 보장되어야 한다.

(2) 통신의 비밀의 보호대상

헌법 제18조상의 '통신의 비밀'의 보호대상이 될 수 있는 것은 통신내용 이외에도 통신의 구성요소가 될 수 있는 통신의 당사자에 관한 사항(당사자의 이름, 주소, 전화번호, 인터넷서비스의 아이디 등), 착발신지, 통신일시, 통신횟수, 통신방법 등도 포함된다고 보는 것이 일반적이다. 왜냐하면 이들 사항을 통해서도 특정한 통신의 '내용'을 '추정'할 수 있는 가능성이 있기 때문이다.[6] 따라서 「통신비밀보호법」이 규정하고 있는 '통신사실확인자료'[7]와 「전기통신사업법」이 규정하고 있는 '통신자료'[8]도 원칙적으로 통신의 비밀의 보호대상이 된다.
한편 통신비밀의 보호대상이 되는 영역 중 가장 핵심이 되는 것은 통신내용이라고 할 수 있다. 따라서 이로부터 '통신내용'과 '통신내용 이외의 사항'(이하'메타데이터'라 한다)에 관해서 각각의 보호 정도를 달리할 수 있는 가능성은 존재한다. 결국 이 문제는 통신내용과 메타데이터에 관한 통제수단이나 절차의 이원화가 가능한지, 그리고 가능하다고 하더라도 각각의 고유

---

5) 헌재 2001. 3. 21. 2000헌바25.
6) 김일환, "통신비밀의 헌법상 보호와 관련 법제도에 관한 고찰", 「형사정책」 제16권 제1호, 2004, 34면.
7) 「통신비밀보호법」 제2조(정의)
11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
가. 가입자의 전기통신일시
나. 전기통신개시·종료시간
다. 발·착신 통신번호 등 상대방의 가입자번호
라. 사용도수
마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료
바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료
사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료
8) 「전기통신사업법」 제83조(통신비밀의 보호) ③ 전기통신사업자는 법원, 검사 또는 수사관서의 장(군수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사(「조세범 처벌법」 제10조 제1항·제3항·제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청하면 그 요청에 따를 수 있다.
1. 이용자의 성명
2. 이용자의 주민등록번호
3. 이용자의 주소
4. 이용자의 전화번호
5. 이용자의 아이디(컴퓨터시스템이나 통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호를 말한다)
6. 이용자의 가입일 또는 해지일

한 헌법합치적인 통제수단이나 절차는 어떠한 것들이 존재할 수 있는지, 더 나아가서 공통된 통제수단이나 절차로는 어떠한 것들이 존재하는지의 문제로 발전하게 된다.[9)]
그런데 여기서 주의할 점은 '통신의 비밀'에 해당하는 영역들인 통신내용과 메타데이터가 모두 사후적으로는 '개인정보'가 된다는 점이다.[10)] 현행「통신비밀보호법」제12조가 통신제한조치로 취득한 자료의 사용제한을 규정하고 있는 것도 이러한 맥락에 서 있는 것으로 이해된다. 그리고 통신의 비밀에 해당하는 것들이 결국 개인정보가 된다는 점은 통신비밀보호법제의 설계와 운영에 있어서 당사자의 개인정보자기결정권이 그 한계로서 작용할 수 있다는 것을 의미한다.[11)]

(3) 최근 침해 양상

1) 국가의 감시능력 진화

빅데이터, 인공지능, 생체인식과 같은 감시 기술의 발전은 정보수사기관의 통신 감시 능력을 강화시켜 새로운 통신의 자유 침해 문제를 야기하고 있다. 지난 2013년 에드워드 스노든(Edward Snowden)의 폭로로 드러난 미국 국가안보국(National Security Agency, NSA)의 인터넷 대량감시(mass-surveillance) 사건이 대표적인 사례이다. 스노든에 의해 밝혀진 바에 따르면, NSA는 프리즘(PRISM)이라는 프로그램을 통해 이메일과 검색엔진, 인터넷 전화, 그리고 기타 미국인들이 지난 몇 년간 사용해온 전자 통신 내역을 감시해오고 있었다. 또한 AOL, 애플, 페이스북, 구글, 마이크로소프트, 스카이프, 팔톡(PalTalk), 야후, 유튜브 등 가장 유명한 웹서비스 업체들 다수가 프리즘 프로그램에 협력했다고 한다.[12)]
우리나라에서는 2014년 카카오톡 사찰 사태가 국가의 통신 감시 현황에 대한 국민적 관심을 불러일으키는 계기가 되었다. 2014년 9월 당시 노동당 정진우 부대표는 종로경찰서로부터 '전기통신에 대한 압수·수색·검증 집행사실 통지'를 받았는데, 2014년 5월 1일부터 6월 10일까지 '카카오톡 메시지 내용, 대화 상대방 아이디 및 전화번호, 대화일시, 수발신 내역 일체, 그림 및 사진 파일' 전체를 압수수색하였다는 내용이었다.[13)] 비록 기술상의 문제로 제공된 건 단 하루치의 대화였지만, 정진우 부대표와 같은 대화방에 있었던 2천 명 이상의 대화 상대방의 개인정보가 함께 제공된 것으로 드러나 큰 사회적 충격을 주었다. 이후 많은 이용자들이 텔레그램 등 외국산 메신저로 이른바 '사이버 망명'에 올랐다. 그리고 2015년에는 국가정보원이 스파이웨어를 통해 민간인을 사찰해왔다는 의혹이 제기되었다. 2015. 7. 6. 이탈리아의 스파이웨어 개발업체 '해킹팀'의 내부 자료가 유출되었는데, 이 자료를 통해 국가정보원이 해킹팀의 스파이웨어 RCS를 구매했음이 밝혀졌다. 이에 대해 국내 정보인권 단체들은 통신기기의 RCS 감염 여부를 확인할 수 있는 "오픈백신" 프로그램을 만들어 배포한 바 있다.[14)]

---

9) 황성기, 앞의 논문, 13면.
10) 예컨대 구치소장이 청구인과 배우자의 접견을 녹음한 행위 및 구치소장이 검사의 요청에 따라 청구인과 배우자의 접견녹음파일을 제공한 행위가 위헌인지 여부가 문제된 사건에서, 헌법재판소는 접견녹음파일은 '개인정보'에 해당하므로, 접견녹음파일을 제공한 행위는 정보주체인 청구인의 동의 없이 관계기관에 제공한 것으로 청구인의 개인정보자기결정권을 제한하는 것으로 보았다. 헌재 2012. 12. 27. 2010헌마153, 접견 녹음파일 송부 요청 취소.
11) 황성기, 앞의 논문, 13면.
12) 이광석 외,『4차 산업혁명 시대에서 정보인권 보호를 위한 실태조사』, 국가인권위원회 연구보고서, 사단법인 참세상, 2018, 84면.
13) https://act.jinbo.net/wp/8239/ (2019.10.11. 최종접속)

2) 기업의 노동감시 증가

노동에 대한 데이터화는 디지털 모바일 시대에 양산되고 있는 새로운 노동 과정에 '적합한' 관리·감시 양식으로 떠오르고 있다. 업무용 앱이나 배달 앱은 특정한 공간 안팎을 가릴 것 없이 개별 노동자에 직접 관통하는 방식으로 노동자 주체의 종·추적(tracking and tracing)을 가능하게 할 뿐만 아니라, 더 중요한 점은 그것이 실시간으로 가능하다는 사실이다. 앱으로 추출된 데이터를 통해 개별 노동자의 이동 동선, 결재-성과 보고 등의 업무의 전 과정을 실시간으로 맵핑(지도화)하는 게 가능하다. 심지어 노동자의 품행까지 통제할 수 있다. 일일이 관찰하지 않고도 작업장 안팎에서 노동자의 행동 하나하나까지 데이터화할 수 있는 일종의 데이터감시(dataveillance)다.[15]

특히 대기업 등에서 광범위하게 사용되는 모바일단말관리(Mobile Device Management, MDM) 앱은 원격으로 스마트폰, 태블릿 PC 등의 환경과 보안 설정, 특정 데이터 삭제 등을 할 수 있는 일종의 모바일 관리 체계인데, 회사가 제공하는 MDM 앱을 설치한 경우 통신기기의 위치를 파악해 사내 인트라넷 접근 권한을 제공한다거나, 회사 내에서 카메라·녹음기 같은 일부 기능을 정지시키는 등 원거리에서 통신기기를 제어하는 방식으로 기능한다. 통화·문자 내역이나 이메일 송수신 내역을 수집하는 경우도 있다. 이러한 MDM 앱은 노동자의 사생활 및 통신의 비밀 침해 문제를 야기한다.

3) 사회적 약자에 대한 감시 문제 대두

아동과 청소년, 여성, 성소수자 등 사회적 약자에 대한 감시 문제도 부각되고 있다. 유엔 총회는 2016. 12. 채택한 '디지털 시대의 프라이버시권 결의안'[16]에서 디지털 시대의 프라이버시권의 침해가 여성, 아동 및 소외 계층에게 특히 영향을 미친다는 점을 강조했다. 한국에서는 2014년부터 청소년의 스마트폰 중독을 억제하고 유해정보로부터 보호한다는 취지로 스마트폰 관리앱의 설치를 강제하는 「전기통신사업법」 제32조의7, 일명 청소년스마트폰감시법이 시행되었는데, 이러한 관리앱은 유해정보 차단 외에도 접속 웹사이트 조회, 스마트폰 사용 시간 모니터링, 위치 추적 등의 감시 기능을 갖추고 있어 이동통신사나 부모에 의한 청소년의 스마트폰 감시를 용이하게 한다.

2. 국제 동향 및 기준

(1) UN

통신의 비밀과 자유를 포괄하는 프라이버시권은 「세계인권선언」 제12조와 「시민적·정치적 권리에 관한 국제규약」(International Covenant on Civil and Political Rights, 이하 '자유권규약(ICCPR)'또는 'B규약'이라 한다) 제17조에서 보장하는 중요한 인권임에도 불구하고, 유엔

14) https://opennet.or.kr/9543 (2019.10.11. 최종접속)
15) 이광석 외, 앞의 연구보고서, 91-92면.
16) 유엔 총회 71차 결의, A/RES/71/199.

인권 시스템에서 상대적으로 간과되어 왔다. 하지만 2013년 에드워드 스노든(Edward Joseph Snowden) 의 폭로를 계기로 고도화된 통신기술에 의한 대량감시 문제에 대해 국제적으로 많은 논의가 이루어지면서 유엔의 태도도 변화하여 디지털 시대에서의 프라이버시권 보호를 위한 각국의 조치를 지속적으로 촉구하고 있다.

전술한 바와 같이 유엔 총회(UN General Assembly)는 2013. 12.에 '디지털 시대의 프라이버시권 결의(The right to privacy in the digital age resolution)'[17]를 채택한 바 있는데, 여기서 불법적이거나 자의적인 통신의 감시와 도청이 프라이버시권과 표현의 자유를 침해하고 민주사회의 원리를 위협함을 강조하고, 국경을 초월한 감시와 도청이 대규모로 이루어지는 경우 인권의 보장과 향유에 미치는 부정적인 영향에 대해 깊은 우려를 표명하였다. 최근 2018. 12.에 채택한 결의[18]에서는 디지털 통신의 비밀을 확보하고 보호하기 위한 암호화, 가명화, 익명화 등의 기술적 해결책이 인권, 특히 프라이버시권, 표현의 자유, 집회 및 시위의 자유를 포함한 인권의 향유에 중요함을 강조하면서 국가는 해킹의 형태를 포함한 불법적이거나 임의적인 감시 기술을 사용해서는 안 된다고 선언했다. 그리고 각국이 디지털 통신 정보를 망라하는 정보보호법제를 도입·시행할 것을 촉구했다.

2015. 7. 유엔 인권이사회(UN Human Rights Council)가 프라이버시권 특별보고관으로 임명한 조셉 카나타치(Joseph Cannataci)는 2019. 7. 15.부터 26.까지 한국을 방문해서 가진 기자회견을 통해 한국의 경우 통신수단에 대한 비내용적 정보(메타데이터)에 대한 열람요청 건수가 다른 대부분의 민주주의 국가보다 훨씬 많다고 하면서 이에 대한 사법적 감독체계가 필요하다고 지적한 바 있다.

프라이버시권 특별보고관이 신설되기 전인 2014년 8월 임명된 표현의 자유 특별보고관 데이비드 케이(David Kaye)는 표현의 자유뿐만 아니라 통신의 비밀 보호에도 중요한 보고서를 두 차례 제출한 바 있다. 그 첫 번째는 2015년 5월 제출한 '디지털 통신에 있어서의 암호화와 익명성(encryption and anonymity in digital communications)'에 관한 보고서[19]이다. 이 보고서에서 특별보고관은 디지털 시대에 안전한 소통을 위해 암호화와 익명성이 어떤 역할을 하는지, 그것이 표현의 자유 및 프라이버시와 어떠한 관계가 있는지, 암호화와 익명성을 제약하는 현실의 문제는 무엇인지를 검토하고, "암호화와 익명성은 디지털 시대 표현의 자유권 행사를 위해 필요한 프라이버시와 보안을 제공한다"고 결론을 내리고 각 국가가 암호화와 익명성을 증진하고 제한하지 않을 것을 권고하고 있다. 특히 각 국가는 모바일 이용자에 대한 SIM 카드 등록을 요구하지 말아야 한다고 권고하고 있어 2014년 도입된 한국의 휴대폰 본인확인제에 시사하는 바가 크다.

다른 보고서는 2016년 5월 제출한 디지털 시대의 기업의 책임에 관한 보고서[20]이다. 이 보고서에서 특별보고관은 네트워크와 플랫폼에 전송되거나 저장되는 디지털 통신과 데이터가 국가나 사인에 의한 감시에 점점 더 많이 노출되고 있음을 지적하면서, 이러한 감시가 온라인 보안과 정보접근성을 저해할 수 있고, 일반 시민들이 추적이 두려워 자기 검열을 하게 만들어 온라인 표현에 위축효과를 가져올 수 있음을 우려했다. 그리고 결론으로 정부에 대해서는 디지털 통신내용을 삭제하거나 이용자 정보에 접속할 수 있는 요구, 요청, 조치가 정당한 제정법률에 기반해야 하며, 독립적인 외부기관의 감독을 받아야 하고, 자유권규약 19조 3항에 명

17) 유엔 총회 68차 결의, A/RES/68/167.
18) 유엔 총회 73차 결의, A/RES/73/179.
19) 유엔 인권이사회 29차 결의, A/HRC/29/32.
20) 유엔 인권이사회 32차 결의, A/HRC/32/38.

시된 목적들을 달성하기 위해 사용되는 수단으로서 필수성과 비례성을 입증할 수 있어야 한다고 권고하고, 민간 기업에 대해서는 감시 기술의 이양 등 대정부 사업이 인권에 미치는 영향 등을 검토하는 투명한 인권영향평가 절차를 개발하고 실행할 것을 권고했다.

한편 유엔 총회는 2013년 결의에서 유엔 인권최고대표(UN High Commissioner for Human Rights)에게 디지털 시대의 프라이버시권에 관한 보고서의 작성을 요청한 바 있다. 이 보고서는 2014. 9. 인권이사회에, 2014. 12. 총회에 각각 제출되었다. 인권최고대표는'디지털 시대의 프라이버시권 보고서(The right to privacy in the digital age)'[21]에서 디지털 시대의 통신기술은 정부, 기업, 개인이 감시, 도청, 개인정보 수집을 실행할 수 있는 능력 또한 향상시켰다고 우려하였다. 국가는 그 어느 때보다 동시적이고 침투적이며 정밀하고 광범위한 감시를 수행할 수 있는 더 큰 능력을 보유하게 되었으며, 세계적으로 정치적·경제적·사회적 생활이 점점 더 의존하고 있는 기술 플랫폼은 대량 감시에 취약할 뿐 아니라, 이를 실제로 용이하게 하고 있다고 하였다. 또한 이러한 대량 감시와 디지털 통신 도청, 개인정보 수집은 프라이버시권뿐만 아니라, 표현의 자유, 알권리, 집회·결사의 자유, 가정에 대한 권리 등 다른 인권에 영향을 미친다고 강조했다. 인권최고대표는 긴급한 조치로서, 각국은 법, 정책, 관행이 국제인권법을 완벽하게 준수하는지 검토하고 또한 자국 시민과 다른 나라 시민들 간에 차별적인 취급[감시]을 근절하기 위해 행동할 것을 권고했다. 그리고 2018년 3월 보고서[22]에서는 디지털 시대의 프라이버시권에 대한 기업의 의무를 중점적으로 다루었다. 인권최고대표는 국가 감시와 통신 도청에 관하여 대량 감시가 국제법상 허용되지 않음을 강조하고, 국가가 종종 이용자의 개인정보의 수집과 제공을 기업에 의지하고 정보통신서비스 제공자의 막대한 정보에 대해 접근을 요구하며 통신정보 보관을 강제하는 것을 비판하면서 이러한 조치는 시민들이 익명으로 통신할 능력을 제한하고 필요성과 비례성의 원칙을 위반한다고 하였다. 또한 해외 기업의 서버에 보관된 개인정보에 국가의 접근을 용이하게 하기 위한 법적 제도는 절차적 안전장치를 약화시키거나 우회하도록 만들 수 있고 항소나 구제 방법에 대한 개인의 접근에 부정적 영향을 미칠 수 있다고 우려했다. 결론에서는 국가 감시에 대한 독립적 승인 및 감독 장치를 강화하고 통신사 등 기업에 포괄적이고 무차별적인 통신정보 보관 요건을 부과하는 법을 재고할 것을 권고하고 기업에는 프라이버시권과 인권을 존중하고 통신과 개인정보에 대한 높은 수준의 보안과 기밀 유지를 권고했다.

2015. 11. 유엔 자유권규약위원회(UN Human Rights Committee, 이하 '위원회'라 한다)는 대한민국 제4차 국가보고서에 대한 최종견해에서 한국의 통신자료 제공, 기지국 수사, 국가정보원 감청에 대하여 우려를 표명하였다. 더불어 한국의 통신 감시를 개선하기 위해 정부에게 관련 법률을 개정할 것과, 특히 국가정보원의 통신수사를 제대로 감독할 것을 주문하였다. 위원회는 한국 정부에 대한 권고문 중 "사적 통신에 대한 사찰, 감시 및 감청(Monitoring, surveillance and interception of private communication)" 분야에서 "42. 위원회는 전기통신사업법 제83조제3항에 따라 수사기관이 수사목적을 이유로 영장 없이 전기통신사업자에게 이용자 정보를 요구한다는 것에 대해 우려한다. 집회 참가자들을 특정하기 위한 소위 '기지국 수사'의 집행 및 이에 대한 불충분한 규제, 그리고 폭넓은 감청의 이용, 특히 국정원에 의한 감청과 이에 대한 불충분한 규제에 대해서도 우려한다"고 밝히고, 연이어 "43. 대한민국 정부는 국가 안보를 위한 감시를 포함해 모든 감시가 규약에 부합하도록 보장하기 위해 필요한 법 개정을 하여야 한다. 특히 이용자 정보는 영장이 있을 때만 제공해야 하고, 국정원의

---

21) 유엔 인권이사회 27차 결의, A/HRC/27/37.

22) 유엔 인권이사회 39차 결의, A/HRC/39/29.

통신수사를 감독할 수 있는 기제를 도입해야 하며 기지국 수사가 자의적으로 이루어지지 않도록 보호수단을 강화해야 한다"고 권고하였다.[23]

(2) EU

「유럽인권협약」[24] 제8조 제1항은 "모든 사람은 그의 사생활, 가정생활, 주거 및 통신을 존중받을 권리를 가진다"고 규정하고 있고, 제10조 제1항은 "모든 사람은 표현의 자유에 대한 권리를 가진다. 이 권리는 의견을 가질 자유와 공공당국의 간섭을 받지 않고 국경에 관계없이 정보 및 사상을 주고받는 자유를 포함한다"고 규정하고 있다. 여기서 양 조항의 보호영역은 대단히 넓게 해석되는데, 제8조 제1항은 통신의 기밀성을 보장하고 개인정보 자기결정권을 보호한다면, 제10조 제1항은 통신의 자유를 광범위하게 보호하고 있다. 그리고 EU의 헌법을 구성하는 「EU 기본권 헌장」[25] 제7조(사생활존중권)과 제8조(개인정보 보호)도 주요한 인권 규범이다.

1997. 12. EU는 1995년 개인정보보호지침에 대해 통신 분야에서의 개인정보 보호에 관한 특별법적 지위를 가지는 지침(이하 '1997년 지침'이라 한다)[26]을 입법하였다. 이후 동 지침은 2002년에 전자통신 분야의 프라이버시 및 개인정보 보호를 다루는 프라이버시 및 전자통신에 관한 지침, 이른바 'E-Privacy 지침'[27]으로 대체되었다. E-Privacy 지침은 전자통신 영역의 개인정보 관련 용어 정의, 트래픽 정보의 파기, 익명화 조치(Using anonymous or pseudonymous data), 쿠키 사용 제한 등을 규정하여, EU 회원국 국민들의 프라이버시권, 기본권과 자유를 보호할 뿐 아니라 전자통신 서비스와 개인정보가 EU 공동체 내에서 자유롭게 이동할 수 있도록 보장하는 것 등을 주요 내용으로 하고 있다. 제5조(통신의 비밀)에서는 원칙적으로 이용자의 동의 없는 통신 및 관련 트래픽 정보의 청취, 도청, 저장 또는 다른 종류의 감청이나 감시를 원칙적으로 금지하고 있다. 그리고 2016. 5. 24. 정보보호일반규정(GDPR)의 발효에 따라 2017. 1. 유럽집행위원회는 E-Privacy 지침을 대체할 'E-Privacy 규정'[28] 초안을 채택하였다. GDPR이 기본권 헌장 제8조를 주로 규율하는 데 비해, E-Privacy 규정은 기본권 헌장 제7조를 EU 법체계에 통합하는 데 그 목적이 있다. E-Privacy 규정은 GDPR에 대한 특별규정으로서 GDPR에 우선하여 적용된다.[29]

한편 「2006년 통신정보보관지침」[30]의 발효 이후 그 국내법 이행을 둘러싸고 10여 년간 치열

---

23) UN Human Rights Committee. Concluding observations on the fourth periodic report of the Republic of Korea. Adopted by the Committee at its 115th session (19 October-6 November 2015).

24) European Convention on Human Rights (ECHR).

25) CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION.

26) Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

27) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

28) Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

29) E-Privacy 규정은 본래 2018. 5. 25. GDPR과 함께 시행될 예정이었으나 2019. 10. 현재까지 시행 예정일이 정해지지 않았다.

30) Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

한 논쟁이 이루어졌다. 위 지침은 통신사업자 또는 정보통신서비스제공자에게 자신의 통신서비스를 제공하는 과정에서 생성되거나 처리되는 통신정보를 최소 6개월에서 최대 2년까지 보관할 의무를 부과했다(제3조 및 제6조). 통신사업자가 보관해야 할 통신정보는 통신의 발신지 또는 목적, 통신의 일시·기간·형식, 통신기기, 통신기기의 위치 등을 특정할 수 있는 정보를 말한다((제5조 제1항).

이에 대해 오스트리아에서는 「통신정보보관지침」을 이행하는 국내법의 관련 규정들에 대하여 헌법소원이 제기되었으며, 오스트리아 헌법재판소는 유럽사법재판소에 「통신정보보관지침」이 「EU 기본권 헌장」 제7조(사생활존중권)와 제8조(개인정보 보호) 그리고 제11조(의사표현 및 정보의 자유)와 일치하는지 선결을 요청하였다.[31] 이에 따라 2014. 4. 유럽사법재판소는 위 지침은 「유럽인권협약」 및 「EU 기본권 헌장」의 사생활존중권과 개인정보보호권을 침해하여 무효라고 판결하였다.[32] 「통신정보보관지침」의 목적은 정당하고 수단도 적합하나, 정보의 보관과 접근에 관한 절차적·실체적 요건들이 비례성을 충족하지 못한다는 것이었다. 중대범죄의 정의나 보관 기간의 정의가 광범위한 점도 비판받았다. 이에 따라 오스트리아와 벨기에 헌법재판소도 「통신정보보관지침」의 이행을 위한 국내법이 헌법에 위반된다고 결정했다.[33] 유럽사법재판소는 이 사건 이후로도 스웨덴, 영국의 통신정보 보관 관련 법률에 대한 결정에서 통신정보의 의무적 보관이 「EU 기본권 헌장」을 침해한다는 취지를 계속 확인하였다.

2015년에는 개인정보 보호 적정성 평가기준에 관한 미국과 EU 간의 「세이프하버 협정(Safe Harbor Agreement)」이 무효화되었다. 동 협정에 따라서 미국은 EU 시민들의 개인정보의 역외 이전을 위해 유럽에서 시행되고 있는 정도의 적정한 개인정보 보호 수준을 준수해야 할 의무를 부담하고 있었고 EU 집행위원회는 2000. 7. 26. 적정성 판단에 의한 승인 결정을 내렸다.[34] 그 이후 이 결정은 유럽연합에서 활동하는 수많은 미국기업의 상거래에 대한 기초를 형성했는데, 스노든(Edward Joseph Snowden) 의 폭로를 기점으로 상황이 근본적으로 변화되었다. 즉 페이스북이나 애플 등의 미국의 1T 기업들이 저장한 EU 시민들의 개인정보가 미 정보당국의 감시에 노출될 수 있다는 우려가 제기되면서, EU 집행위원회는 협정의 문제점을 수정해야 한다는 비판에 직면했다.[35] 2013년 오스트리아 페이스북 사용자인 막스 슈렘스(Maximilian Schrems)는 페이스북 아일랜드가 개인정보를 미국으로 이전하지 못하도록 조치해줄 것을 요청하는 진정을 아일랜드 개인정보보호청장에게 제기하였다. 2014. 7. 아일랜드 고등법원은 이 사건이 유럽연합(EU) 집행위원회와 미국 상무부가 2000년에 체결한 개인신상정보 전송에 관한 「세이프하버 협정」의 적정성과 관련이 있다고 보고 유럽사법재판소에 그에 대한 판단을 구했는데, 유럽사법재판소는 2015. 10. 6. 본 세이프하버협정을 무효화하는 결정을 내렸다.[36] 그러나 얼마 후인 2016. 2. EU 집행위원회는 미국 정부와 「EU-미국 프라이버시 보호(EU-US Privacy Shield)」라는 새로운 명칭의 협정을 체결하였다.

---

on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

31) 민영성·박희영. "통신정보보관제도의 정당성: 유럽사법재판소 및 오스트리아 헌법재판소 판결의 관점에서", 「법학논문집」 제40집 제1호, 2016, 457면.

32) CJEU, Judgement of 8.4.2014, Case C 293-12 and C-594/12.

33) 민영성·박희영, "유럽사법재판소의 통신정보보관지침의 무효 판결과 그 시사점", 「법학연구」 56(4), 2015, 54면.

34) 2000/520/EC.

35) 이상학, "국가감시와 기본권보호", 「유럽헌법연구」 20, 2016, 230면.

36) Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner.

또한 유럽인권재판소도 정보기관의 감시로부터 정보인권을 보호하기 위한 규범을 강화하는 데 일조하였다. 즉 2018. 9. 13. 유럽인권재판소는 2000년 영국 수사권한 규제법의 대량감시 프로그램이 인권을 침해한다고 판단하였다.[37] 이러한 판단에 따르면 안전조치나 민주적인 감독장치가 없는 대량 감청은 「유럽인권조약」 제8조를 위반하며, 송·수신자의 인적 정보, 통신일시, 위치를 비롯한 통신 메타데이터의 무제한적인 수집은 동 조약 제8조 및 제10조를 위반하는 것이다. 유럽 시민단체들은 이번 판결이 메타데이터의 대량 수집과 감시의 침해 사실이 인정되었다는 점에서 환영하였다. 메타데이터는 누군가의 생활에 대해 많은 사실을 아주 잘 드러내고 사생활에 대한 권리를 침해할 수 있다는 점에서 메타데이터에 대한 대량 감시가 통신내용에 대한 감시보다 덜 침해적인 것이 아니기 때문이다.[38]

(3) 각국의 법제 동향

1) 독일

독일은 통신감시에 대하여 「형사소송법(StPO : Strafprozeßordung)」과 「서신, 우편 및 전기통신 비밀제한에 관한 법률(Gesetz zur Beschränkung des Brief, Post und Fernmeldegeheimnisses)」(이하 '통신비밀제한법'이라 한다)에서 규정하고 있다. 형사소송법은 통신감청과 우리나라의 통신사실확인자료와 유사한 개념인 통신정보((Verkehrsdaten)에 대하여 근거규정을 두고 있으며, 통신비밀제한법은 국가안보기관의 통신감청에 대한 근거 법률로서 제정되어 운용되고 있다. 통신감청은 형사소송법과 통신비밀제한법에 열거된 특정 범죄에 대한 범죄혐의가 있고, 사실관계의 조사나 피의자의 소재수사가 다른 방법으로는 아주 곤란하거나 불가능한 경우에만 허용되고 있다. 한편, 통신정보의 개념과 수집은 형사소송법 제100g조에 근거를 두고 있으며 통신자료의 개념은 「전기통신법(Telekommunikationsgesetz - TKG, 1996)」 제3조 제3호에 근거한다. 전기통신법은 통신자료(Bestandsdaten)를 통신정보서비스에 대한 계약관계의 성립, 실질적인 형성, 변경, 해지와 관련된 계약당사자에 대한 일체의 정보라고 정의하고 있다.

단순한 통신자료의 제공과 관련해서는 법률개정을 통하여 통신사업자에 대하여 직접적인 의무를 부여함과 동시에 제공자료의 범위와 절차를 명확히 하고 있다는 점은 주목할 필요가 있다. 2012. 1. 24. 연방헌법재판소의 법률개정 촉구결정[39]에 대하여 연방정부는 2012. 10. 24. 개정법률안을 발의하였으나, 그 위헌성이 문제되어 연방의회에서 이를 바탕으로 수정된 법률안을 의결하기에 이르렀다.[40] 동 법률안에 따라 전기통신법 제113조가 개정되었으며, 형사소송법에 제100j조가 새로이 추가되었다. 이는 전기통신사업자의 통신자료 제공의무를 명시하여 통신자료제공의 근거와 절차를 보다 명확히 하였을 뿐만 아니라, 대상이 되는 통신자료의 성격에 따라 그 보호의 정도를 단계화함으로써 일종의 개인정보인 통신자료의 이용과 보호를 조화하고자하는 취지를 잘 반영하고 있다고 평가할 수 있다.[41]

독일은 2006년 통신정보보관지침에 따라 2007년 통신정보저장 의무를 부과하는 법률을 제정

---

37) CASE OF BIG BROTHER WATCH AND OTHERS v. THE UNITED KINGDOM (Applications nos. 58170/13, 62322/14 and 24960/15).
38) 이광석 외, 앞의 연구보고서, 151면.
39) BVerfG, 1 BvR 1299/05.
40) Drucksache 17/12034.
41) 이진구·김일환, 앞의 논문, 225면.

했으나, 동법은 2010년 독일 연방헌법재판소의 위헌판결을 받았다.[42] 또한 2014년 유럽사법재판소는 통신정보보관지침을 무효화시켰다, 따라서 동 지침에 따를 필요가 없음에도 불구하고, 독일은 2015. 12.「통신정보에 대한 저장의무와 최장저장기간의 도입에 관한 법률」(이하 '통신정보저장법'이라 한다)[43]을 제정했다. 본 법률은 형사소송법과 전기통신법의 개정내용을 담고 있는데, 독일 연방헌법재판소와 유럽사법재판소가 지적한 문제점을 보완하여 통신정보 저장 제도를 개선하고자 했다. 통신정보의 저장의무는 전기통신법 제113a조 내지 제113g조에 새로 규정되었다.[44] 그러나 통신정보저장법이 2014년 유럽사법재판소 판결에 합치하지 않는다는 비판이 지속적으로 제기되었고, 2019. 9. 독일 연방행정법원은 통신정보저장법이 E-privacy 지침에 합치하는지 여부를 유럽사법재판소의 판단에 맡기기로 결정했다.[45]

2015. 12. 28. 개정된 형사소송법 제100g조는 수사기관의 통신정보 수집 시 전기통신법 제113b조에 의하여 의무적으로 보관되어 있는 통신정보에 대해서는 더욱 엄격한 요건을 적용하여, 통신정보 수집이 허용되는 대상범죄를 감청 대상범죄보다 더욱 한정하고 있으며, 보충성 요건으로 "사실관계의 조사 또는 피의자의 소재지 조사가 다른 방법으로는 현저히 곤란하거나 불가능하다고 예상"되는 경우를 규정하고 있다. 또한 통신정보 수집 대상자도 엄격히 제한하고 있다.

독일은 9.11. 테러 이후 국제테러리즘에 대처하기 위해 2002. 1. 9.「국제테러대책법(Gesetz zur Bekämpfung des internationalen Terrorismus)」을 제정·실시하고, 이후 2007. 1. 5.「테러대책법보충법(Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetz)」을 제정하여 극단주의 결사에 대한 규제를 강화하였다. 2008년에는「연방범죄수사청을 통한 국제테러 위험 방어를 위한 법률(Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt)」을 제정하였는데, 이 법은 연방범죄수사청법 개정을 통해 동 기구에 대해 광범위한 직무와 권한을 부여함으로써 다양한 형태의 국제테러 위험의 방지를 도모하고 있다.[46] 독일에서는 형사소송절차 및 행형단계에서 테러범죄 혐의자의 권리를 제한하는 특례규정들을 두고 있는데, 테러혐의자의 추적을 용이하게 하기 위해 통신감청과 우편검열, 함정수사, 전산망 검색권을 인정하고 있다.[47]

2) 프랑스

프랑스는 통신감청에 관한 법적 근거를 1991년에 마련하였고, 범죄수사를 목적으로 하는 사법감청과 국가안보와 조직범죄의 대처수단으로서 행정감청으로 구분하고 있으며, 법제가 마련된 이후에도 사법감청 권한의 확대와 행정감청의 수단과 절차 등이 입법과정 속에서 보완되어 왔다. 특히 2015년 발생한 샤를리 엡도(Charlie Hebdo) 테러를 시작으로 유대인 상점 테러, 2016년 니스 테러와 같은 잔혹한 범죄로 인해 무고한 시민이 테러단체로부터 목숨을 잃는 사건이 발생하면서, 범죄조직의 범죄모의를 사전에 인지할 수 있는 통신제한에 관한 입법적 장

---

42) BVerfGE, Urteil 2.3.2010 -1 BvR 256/08.
43) Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten n vom 10. Dezember 2015 (BGBl. I S. 2218).
44) 정애령, "독일 통신데이터저장제도(Vorratsdatenspeicherung)의 비판적 고찰-유럽연합지침과 독일의 통신데이터저장제도 재도입 법률을 중심으로-",「공법연구」제45집 제3호, 2017, 135면.
45) 독일 연방행정법원 보도자료 https://www.bverwg.de/pm/2019/66 (2019.11.1. 최종접속)
46) 제성호, "독일의 테러방지법과 테러대응기구",「법학논문집」제41집 제1호, 2017, 72-73면.
47) 제성호, 앞의 논문, 75면.

치를 강화하였다.[48)]

「전기·전자통신의 비밀에 관한 법률(Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances emises par la voie des communications electroniques)」에서 감청에 대한 사안을 일괄적으로 규정하고 있는데, 제1장에서 '수사목적의 감청', 제2장에서 '국가안보 목적의 감청'을 각각 규율한다.[49)] 프랑스의 경우 기본적으로 영장주의라는 개념자체가 없으며, 다만 범죄수사, 소추를 목적으로 하는 통신자료보관 및 제공 요청은 사법기관을 통해서 하도록 함으로써 영장주의와 유사한 사법적 통제를 하고 있다.

프랑스에서는 「우편 및 전기통신법(Code des postes et des communications electroniques)」에 따라 통신사실확인자료와 통신자료를 통합적으로 규제하고 있는 것으로 보인다. 우선 수사목적의 통신사실확인자료 및 통신자료 제공에 대해 우편 및 전기통신법전의 L(법)제34조의 1에서는 사법기관이 범죄수사·소추의 목적으로 전기통신사업자에 이를 요청할 수 있고, 전기통신사업자는 위 요청에 응하기 위해 해당 자료를 최장 1년간 보관할 수 있는 것으로 규정하고 있다. 전기통신사가 보관할 수 있는 자료의 범위에 대해 2006년 통신정보보관지침을 수용하여, 우편 및 전기통신법전의 R(규칙) 제10조의 13의 제정을 통해 아래와 같이 구체적으로 열거하고 있다. 우편 및 전기통신법전 L(법) 제34조의 1을 적용함에 있어, 전기통신사업자는 범죄수사·소추 목적을 위해 1) 사용자의 신원을 확인할 수 있는 정보, 2) 사용된 통신단말기와 관련된 정보, 3) 통화 시간, 기간 등, 4) 요청된 부과서비스와 관련된 정보, 5) 통신목적지와 관련된 정보를 보관할 수 있다. 한편, 수사 목적 외 테러예방 등 국가안전을 목적으로, 경찰 및 군 경찰요원은 L제34조의 1에 규정을 준용하여, 전기통신사업자에게 처리 및 보관 정보에 대한 제공요청을 할 수 있다. 하지만 경찰요원이 관련자료 제공 요청을 전기통신사업자에게 바로 하는 것이 아니라 반드시 내무부 산하에 임명된 위원의 결정을 거쳐서 요청하여야 한다.[50)]

2015년 11월 130여 명의 사망자가 발생한 파리 연쇄테러가 발생한 직후 프랑스 정부는 국가비상사태를 선포하고 테러와의 전쟁을 시작했다. 입법적 조치로는 2016. 6. 3.「조직범죄, 테러리즘, 그 자금조달 대응강화 및 형사절차의 합리화 및 보장의 개선에 관한 법률」[51)]이 제정되었다. 동 법은 새로운 통신기술의 발전에 따라, 검사와 예심판사에게 새로운 수사 수단을 사용할 수 있는 권한을 부여했다. 즉 검사와 예심판사는 전자통신 접속 자료를 감청하기 위한 기술 장치를 사용할 수 있고, 컴퓨터 자료를 획득할 수 있는 권한을 가지게 되었다.[52)] 이로써 현행범 수사 또는 예심수사 절차에서 수사대상자의 정보시스템에 보관된 음성의 재생, 영상정보의 취득, 정보데이터 및 전자메일의 취득이 가능하게 되었다.[53)]

---

48) 여은태, "프랑스의 통신제한 법제와 그 시사점",「법학논총」제35집 제1호, 2018, 55면.

49) 한동훈,『프랑스의 통신비밀보호법제-감청기간 및 연장을 중심으로-』, 한국법제연구원, 2010.

50) 이성기, "「통신사업자의 통신사실확인자료 및 통신자료 제공의 요건과 절차」에 관한 비교법적 연구 : 미국, 영국, 독일, 프랑스, 일본의 제도 비교를 중심으로",「법과 정책연구」, 제14집 제1호, 2014, 55면.

51) Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale, J.O. n°0129 du 4 juin 2016

52) 김문귀, "프랑스의 대테러법제에 관한 연구 - 2016년 대테러강화법 및 그 시사점",「한국프랑스학논집」96, 2016, 203면.

53) 정용기, "최근 프랑스의 테러대응 법령의 변동과 시사점에 관한 연구",「한국테러학회보」제9권 제3호, 2016, 124-125면.

3) 미국

현재 미국에서 통신감청에 대해 주로 규율하는 법은 1968년 제정된「범죄단속 및 가두안전종합법(the Omnibus Crime Control and Safe Streets Act of 1968)」과 1986년 제정된「전자통신프라이버시법(Electronic Communication Privacy Act of 1986, ECPA)」이다. 범죄단속 및 가두안전종합법은 제3편에서「연방감청법(the Federal Wiretap Act, 18 U.S.C. §§2510-2522)」을 규정하여 형사절차에서 국가기관의 전화감청행위에 대한 기준을 마련했다. ECPA에 포함된「펜트랩법(the Pen Registers and Trap and Trace Devices chapter of Title 18, 18 U.S.C. §§ 3121-3127)」은 감청금지대상으로 전화통화뿐만 아니라 인터넷을 통한 컴퓨터 데이터 전송을 포함하였고, 새로운 규율대상으로 이동추적장치(mobile tracking devices), 통화번호 등 기록장치(pen register) 및 발신자 추적장치(trap and trace device)가 입법화되었다. 한편 연방감청법 하에서의 감청(intercept)은 모든 대화가 수신단계에서 동시에 진행되는 것을 말한다. 따라서 수사기관이 저장된 대화내용에 접근해서 그 대화내용을 복사하는 것은 이 법에 의한 감청이 아니며「저장통신법(Stored Communication Act, 18 U.S.C. §2701-12)」이 적용된다.

미국의 경우 감청영장을 받기 위해서는 수사기관은 일반적인 영장 발부 요건보다 더욱 엄격한 요건을 충족해야만 한다. 그리고 통신자료와 통신사실확인자료는 명확히 구분되지 않는다. 저장통신법상 사용자 정보(Subscriber Information)가 통신자료에 대응하는데 이의 제공과 관련하여 당사자가 동의가 없는 이상 법원 또는 대배심(Grand Jury)의 명령장이 필요하며 예외적으로 텔레마케팅 사기 수사와 관련한 경우 수사기관의 공문서로 통신자료의 제공이 가능하다.[54] 따라서 미국의 경우 수사기관이 통신사업자로부터 통신자료를 제공받기 위해서는 우리나라와 달리 법원의 영장 또는 허가가 필요하다고 보아야 한다.[55]

한편, 미국의 통신제한제도는 수사목적을 위한 경우와 안보목적을 위한 경우로 나뉘어 구축되어 있으며, 수사목적의 통신제한조치는 연방법원이 안보목적의 통신제한조치는 법무부가 주관하고 있다. 수사목적 이외에 안보목적을 위해서는「해외정보감시법(Foreign Intelligence Surveillance Act 1978, FISA)」을 두고 있다. FISA는 국가안보를 저해하는 외국세력 및 그 구성원, 연계된 미국인 및 미국기관 및 단체에 대한 통신감청을 규율하기 위해 제정되었다.

미국의 테러리즘 대응에 가장 포괄적이고 광범위한 영향을 미친 법은 2001년 제정된「애국법(USA PATRIOT Act)」[56]이다. 애국법은 해외정보감시법,「종합테러방지법(Antiterrorism and Effective Death Penalty Act of 1996)」, 전자통신프라이버시법 등을 강화한 법으로, 국제테러리즘 및 정보활동과 관련한 통상의 수사절차에 대한 요건을 완화하고 수사기관의 권한을 강화했다. 그러나 국가안보국(NSA)를 포함한 행정부에 전례가 없는 강력한 권한을 부여함으로써 그 권한남용과 위헌가능성에 대한 우려가 문제되었고, 스노든의 폭로로 인해 그러한 우려는 현실로 밝혀졌다. 이를 수정하기 위해 NSA를 포함한 정보기관의 무차별적인 정보수집 행위를 금지하는「자유법(USA FREEDOM Act)」[57]이 도입되었는데, 동법은 2015. 5. 13. 미 하원을 압도적인 표차로 통과하고 동년 6월 2일 발효되었다. 동 법은 업무기록물 요청, 전자

54) 19 U.S.C.A. 2703(c)(1):18 U.S.C.A. 2703(c)(2).
55) 이성기, 앞의 논문, 4-5면.
56) Uniting and Strengthening America by Providing Appropriate Tools to Restrict, Intercept and Obstruct Terrorism Act of 2001.
57) Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015.

감시, 펜트렙 장치 사용, 외국정보, 테러리즘 대응 및 기타 범죄관련 정보수집과 수사절차에 관한 연방 정부의 권한 수정을 목적으로 해외정보감시법을 개정한 법이다.
최근, 미국에서는 휴대전화에 대한 압수·수색과 관련하여 Riley 판결이, 과거의 휴대전화 (기지국) 위치정보를 제공받기 위해서는 수색영장을 받아야 한다는 Carpenter 판결[58]이 선고되는 등, 프라이버시에 민감한 휴대전화에 대한 수사를 통제하는 연방대법원의 경향이 나타나고 있다. 프라이버시 민감정보를 가지고 있는 휴대전화의 특수한 성격과 법에서 예상하지 못했던 발전하는 수사기법에 대한 대응하기 위한 것으로 보인다.[59]

4) 캐나다

2014년 6월 캐나다 대법원은 경찰이 아동포르노 수사를 위해 특정 IP주소의 망이용계약자의 신원정보를 망사업자로부터 영장 없이 취득한 것이 위헌이라는 결정을 내렸다.[60] 특히 망사업자의 이용약관에 "범죄수사를 위해 경찰과 협조할 수 있으며 이에 따라 이용자 신원정보를 제공할 수 있다"라는 조항이 있었음에도 불구하고, 대법원은 위 조항은 경찰의 "적법한 권한행사(lawful authority)"에 응할 수 있다는 의미일 뿐이기 때문에 이용자는 자신의 신원정보에 대한 프라이버시권을 포기한 것은 아니라고 판시하였다. 대법원은 "인터넷 이용의 맥락에서 익명성으로서의 프라이버시를 이해하는 것이 중요하다"면서 이용자신원정보는 이용자가 인터넷에서 익명성의 기대를 갖고 행한 모든 활동에의 "연결고리(link)" 역할을 한다며 경찰이 이용자신원정보를 취득할 때는 이용자의 모든 사적인 인터넷활동에 대한 프라이버시를 제한하는 것이며 이는 사법기관의 명령에 의해서만 행해질 수 있다고 판시하였다.[61]

(4) 시민사회

2013. 9. 20. 스위스 제네바에서 전자개척자재단(EFF), 액세스 나우(Access Now), 아티클 19(Article 19), 프라이버시 인터내셔널(Privacy International), 휴먼라이츠워치(Human Rights Watch), 국경없는기자회를 포함한 세계의 260여개 정보인권단체들은 국가에 의한 감청, 통신사실정보 취득, 이용자정보 취득 등에 대해 국제인권법이 요구하는 "필요성과 비례성의 원칙" 또는 "13개의 원칙"을 발표하였다.[62] 한국에서는 (사)오픈넷, 진보네트워크센터, 소비자시민모임이 참여했다. 이 원칙은 제24차 UN인권이사회 부속행사에서 당시 UN 인권최고대표(UN High Commissioner for Human Rights) 나비 필레이(Navi Pillay)와 UN 표현의 자유 특별보고관(UN Special Rapporteur on Freedom of Expression and Opinion) 프랭크 라 뤼(Frank La Rue)에게 전달되었다.
필요성과 비례성의 원칙은 첫째, 통신서비스이용자 신원정보를 국가기관이 취득하는 것도 역시 통신감시의 일환으로 인정되어 영장주의 원칙을 적용할 것, 둘째, 국외의 통신에 대한 감시에 대해서도 똑같은 원칙을 적용할 것, 셋째, 통신서비스 이용에 대해 국가가 "실명제"를

58) United States v. Carpenter, 819 F. 3d 880 (2016).
59) 이흔재, "미국의 휴대전화에 대한 통신감청 및 위치정보 확인수사의 법제 및 최근 판례에 대한 비교법적 연구", 「법학논총」 31(3), 2019, 214면.
60) R. v. Spencer, 2014 SCC 43.
61) 판결 원문 및 국문 번역본은 https://opennet.or.kr/6743 참조.
62) https://necessaryandproportionate.org/principles (2019.10.11. 최종접속).
국문번역본은 https://opennet.or.kr/4123 참조.

강제해서는 안될 것, 넷째, 통신감시의 대상이 된 사람에게는 최소한 감시가 완료되기 전까지는 정보취득에 대해 통보할 것을 요구하고 있다.
그리고 2016년 1월에는 세계 171개 시민사회단체, 기업, 개인들이 세계 각 국의 지도자들에게 강력한 암호화를 지지할 것과 디지털 보안을 약화시킬 수 있는 법, 정책, 명령 등을 거부할 것을 촉구하는 서신을 발송했다.[63] 여기서 국제 시민사회는 모든 정부가 통신과 시스템의 무결성을 강화함으로써 이용자의 안전과 보안을 지원해야 하며 암호화 및 기타 보안 통신 도구 및 기술에 대한 접근을 제한하거나 그것을 저해하는 법, 정책, 혹은 기업과의 비밀 협약을 포함한 여타 명령이나 관행들을 거부할 것을 촉구했다. 그리고 이용자들은 정부가 정당한 절차와 인권에 대한 존중 없이, 콘텐츠, 통신 기록, 혹은 암호화 키에 강제로 접근할 것이라는 두려움 없이, 가능한한 가장 강력한 암호화를 이용할 수 있는 선택권을 가져야 하며, 기업들은 그러한 암호화를 제공할 수 있는 선택권을 가져야 할 것을 천명했다.

3. 국내 법·제도 현황

(1) 관련 법제 현황

우리나라에서 국가에 의한 통신비밀의 침해에 관한 통제절차와 방법을 규정하고 있는 대표적인 법률로는 「통신비밀보호법」과 「전기통신사업법」이 존재한다. 여기서 통신비밀보호법은 전기통신의 감청에 관한 일반적인 사항을 규율하고 있는 법률이고, 전기통신사업법은 전기통신사업자의 사업방식에 대한 규율을 목적으로 하는 법률이다. 또한 「형사소송법」 그리고 「국민보호와 공공안전을 위한 테러방지법」(이하 '테러방지법'이라 한다)을 들 수 있다.

1) 통신비밀보호법상 통신제한조치(감청) 제도

「통신비밀보호법」상 '통신'은 "우편물 및 전기통신"을 말한다(동법 제2조 제1호). '전기통신'은 "전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것"을 의미한다(동법 제2조 제3호). 그리고 '감청'이라 함은 "전기통신에 대하여 당사자의 동의없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것"을 말한다(통신비밀보호법 제2조 제7호).
「통신비밀보호법」에서 전기통신의 감청은 우편물의 검열을 포함하여 '통신제한조치'라는 개념으로 포섭되어 있고, 수사기관 등에 의한 통신제한조치에 대해서는 통신비밀보호법이 제5조(범죄수사를 위한 통신제한조치의 허가요건), 제6조(범죄수사를 위한 통신제한조치의 허가절차), 제7조(국가안보를 위한 통신제한조치), 제8조(긴급통신제한조치), 제9조(통신제한조치의 집행), 제9조의2(통신제한조치의 집행에 관한 통지), 제9조의3(압수·수색·검증의 집행에 관한 통지), 제15조(국회의 통제) 등에서 규정하고 있다. 이에 의하면 통신의 내용에 해당하는 음성통화내용, 이메일 등을 대상으로 하는'통신제한조치'의 경우 그 대상이 내란죄, 폭발물에

63) https://www.SecureTheInternet.org (2019.11.1. 최종접속),
국문번역본은 https://act.jinbo.net/wp/9197/ 참조.

관한 죄 등 중범죄로 한정되어 있고, 수사기관 등이 통신비밀보호법이 정한 요건 및 절차에 따라 법원의 허가를 받아야 실시할 수 있어서 통신사실확인자료 제공보다 더욱 엄격한 제약 하에서 이루어진다.

과학기술정보통신부(구 미래창조과학부, 이하 '과기정통부'라 한다)의 "통신자료 및 통신사실확인자료 제공 등 현황"에 의하면 전화번호(계정)수를 기준으로 전체 통신제한조치의 약 98.8%가 국가정보원에 의해 이루어지고 있다. 대부분 국가 안보와 관련한 수사를 위하여 이용되고 있는 것으로 보인다.

[표 1] 2013년 - 2018년 기관별 통신제한조치 협조 현황[64)]

구분		2013년	2014년	2015년	2016년	2017년	2018년
검찰	전화번호수	1	7	-	-	-	-
	문서수	1	4	-	-	-	-
경찰	전화번호수	96	301	88	53	83	42
	문서수	71	193	40	32	42	25
국정원	전화번호수	5,927	6,363	6,214	6,630	6,692	6,718
	문서수	512	371	294	279	177	236
군수사기관등*	전화번호수	8	7	-	-	-	-
	문서수	8	5	-	-	-	-
합계	전화번호수	6,032	6,678	6,302	6,683	6,775	6,760
	문서수	592	573	334	311	219	261

* 군 수사기관 등 : 국군기무사령부, 국방부 등

2) 통신비밀보호법상 통신사실확인자료 제공 제도

'통신사실확인자료'란 통신내용 외에 전기통신사실에 관한 자료를 의미하는 것으로서, 여기에는 가입자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자 번호, 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 추적자료가 포함된다(통신비밀보호법 제2조 제11호).

수사기관 등에 의한 통신사실확인자료의 제공 절차 등에 관한 세부적인 사항은 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차), 제13조의2(법원에의 통신사실확인자료제공), 제13조의3(범죄수사를 위한 통신사실 확인자료제공의 통지), 제13조의4(국가안보를 위한 통신사실 확인자료제공의 절차 등), 제13조의5(비밀준수의무 및 자료의 사용 제한) 등에서 규정하고 있다. 이에 따르면 검사 또는 사법경찰관은 필요한 경우 법원의 허가를 받아 전기통신사업자에게 통신사실확인자료 제공을 요청할 수 있다.

과기정통부의"통신자료 및 통신사실확인자료 제공 등 현황"에 의하면, 통신사실확인자료 제공의 문서수는 증가 추세이나, 전화번호(계정)수는 2013년 16,114,668건, 2014년 10,228,492건에서 2015년 5,484,945건, 2016년 1,585,654건, 2017년 1,052,897건으로 감소하는 추세에 있으며, 2018년도에는 555,091건으로 대폭 감소하였다. 통신사실확인자료 제공은 2017년 상반기 이후 급격하게 감소하여 다시 증가하지 않고 꾸준히 줄어들고 있는 추세이다. 더불어

64) 출처: 과기정통부(구 미래창조과학부) 보도자료.

2018년 6월 통신비밀보호법 제2조와 제13조를 근거로 통신사실확인자료를 무작위로 제공받는 기지국 수사와 실시간 위치추적 수사에 대해 헌법재판소가 위헌이라 판단함으로써 앞으로도 이전의 높은 수치로 되돌아갈 가능성은 낮아 보인다.

[표 2] 2013년 - 2018년 기관별 통신사실확인자료 제공 현황[65]

구분		2013년	2014년	2015년	2016년	2017년	2018년
검찰	전화번호수	514,698	203,040	168,396	163,795	157,340	155,900
	문서수	55,722	62,382	64,154	59,527	62,616	61,595
경찰	전화번호수	15,444,131	10,069,167	5,304,994	1,415,145	885,238	391,859
	문서수	200,624	191,261	223,290	241,039	234,922	220,612
국정원	전화번호수	5,115	2,095	2,789	1,210	3,398	1,830
	문서수	1,428	846	981	424	701	715
기타기관*	전화번호수	150,724	14,190	8,766	5,504	6,921	5,502
	문서수	8,085	4,695	2,517	2,331	3,018	2,692
합계	전화번호수	16,114,668	10,288,492	5,484,945	1,585,654	1,052,897	555,091
	문서수	265,859	259,184	300,942	303,321	301,257	285,614

* 기타기관 : 군 수사기관, 사법경찰권이 부여된 행정부처(관세청, 법무부, 고용노동부, 식품의약품안전처 등)

3) 전기통신사업법상 통신자료 제공 제도

「전기통신사업법」 제83조는 '통신비밀의 보호'라는 제목 하에, 전기통신사업자의 통신비밀 침해 및 누설행위를 금지하면서도, 수사기관 등이 수사 목적 등을 위하여 전기통신사업자에게 일정한 이용자 관련 정보 제공을 요청할 수 있는 제도를 두고 있는데, 그것이 바로 '통신자료 제공제도'이다.

'통신자료'란 "이용자의 성명, 이용자의 주민등록번호, 이용자의 주소, 이용자의 전화번호, 아이디(컴퓨터시스템이나 통신망의 정당한 이용자를 식별하기 위한 이용자 식별부호를 말함), 이용자의 가입일 또는 해지일"을 말하고(전기통신사업법 제83조 제3항 제1호 내지 제6호), 수사기관 등에 의한 통신자료 요청절차 등에 관한 세부적인 사항은 전기통신사업법 제83조 제3항부터 제9항에서 규정하고 있다. 이에 따르면 검사, 수사관서, 정보수사기관은 전기통신사업자에게 법원의 영장 없이 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 통신자료제공을 요청할 수 있다.

과기정통부의 "통신자료 및 통신사실확인자료 제공 등 현황"에 의하면 통신자료제공은 법원의 허가 없이 수사기관의 요청만으로 쉽게 이루어지기 때문에 대량으로 요청 및 제공되고 있고 있는 것으로 보이며, 연간 전체 인구수의 17.3%에 해당하는 8백 9십 만 개 이상의 계정 정보가 조치되고 있는 것은 심각한 문제이다.

[표 3] 2013년 - 2018년 기관별 통신자료 제공 현황[66]

구분		2013년	2014년	2015년	2016년	2017년	2018년
검찰	전화번호수	2,858,991	4,267,625	2,736,238	2,208,469	1,934,319	2,110,476
	문서수	188,438	213,991	202,991	195,763	192,039	194,818
경찰	전화번호수	6,230,617	8,371,613	7,520,195	5,833,312	4,176,093	3,826,000
	문서수	694,395	723,282	854,312	856,756	739,029	721,726

65) 출처: 과기정통부(구 미래창조과학부) 보도자료

국정원	전화번호수	113,305	114,764	122,719	47,433	23,867	29,522
	문서수	4,432	4,382	4,152	3,009	2,672	2,698
기타기관*	전화번호수	371,746	213,454	197,927	183,290	170,706	175,109
	문서수	57,662	59,358	63,419	54,086	56,011	55,239
합계	전화번호수	9,574,659	12,967,456	10,577,079	8,272,504	6,304,985	6,141,107
	문서수	944,927	1,001,013	1,124,874	1,109,614	989,751	974,481

* 기타기관 : 군 수사기관, 사법경찰권이 부여된 행정부처(관세청, 법무부, 고용노동부, 식품의약품안전처 등)

이에 대해 헌법소원과 다수의 민사소송이 제기된 바 있는데, 2012년 헌법재판소는 통신자료 취득행위는 임의수사에 해당하여 공권력의 행사가 아니고, 통신자료제공 요청에 응할 것인지 여부는 전기통신사업자의 재량에 맡겨져 있어 기본권 침해의 직접성이 인정되지 않는다고 결정하였다.[67] 한편, 2016년 3월 대법원은 통신자료를 제공한 기업은 손해배상 책임이 없다고 판결하였다.[68] 하지만 이후에도 통신자료 제공에 대한 민사소송과 행정소송이 이어지고 있고, 시민사회는 헌법소원(2016헌마388)도 재차 청구한 상황이다. 2016. 11. 28. 국가인권위원회는 현재 심리중인 통신자료 제공 제도 헌법소원(2016헌마388)에 대해 “통신자료 제공 제도는 개인정보 수집 목적과 대상자 범위가 지나치게 넓고, 사전 또는 사후에 사법적 통제가 이루어지지 않으며, 정보주체가 자신의 개인정보 제공 사실을 인지할 수 있는 통지 절차가 마련되지 않아 개인정보자기결정권을 침해할 소지가 있다”는 의견을 헌법재판소에 제출한 바 있다.[69] 그리고 통신자료 제공 제도를 개선하기 위해 사법적 통제 장치 마련 등을 골자로 하는 전기통신사업법개정안과 통신비밀보호법개정안이 제19대 국회에 이어 제20대 국회에도 다수 발의되어 있다.

4) 형사소송법상 디지털 증거 압수·수색

구 「형사소송법」(2011. 7. 18. 법률 제10864호로 개정되기 전)은 압수의 대상으로 제106조에서 “증거물 또는 몰수할 것으로 사료하는 물건”을, 제107조에서 “우체물 또는 전신에 관한 것으로서 체신관서 기타가 소지 또는 보관하는 물건”을 규정하고 있었고, 디지털 정보에 대한 압수수색의 경우 엄밀하게 그 압수의 대상이 ‘물건’인 저장매체가 아니라 그에 저장된 ‘정보’이므로, 유체물이 아닌 정보가 「형사소송법」상 압수수색의 대상이 될 수 있는지 여부에 관하여 견해의 대립이 있었다. 그 후 2011. 7. 18.자로 「형사소송법」이 개정되어 현행 「형사소송법」 제106조 제3항은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와 비슷한 정보저장매체인 경우에 정보의 범위를 정하여 출력, 복제하는 방법이 원칙적인 압수 방식이라고 명시적으로 규정함으로써 디지털 정보에 대한 압수가 가능하다는 점을 명문화하였고, 같은 조 제4항에서는 법원이 제3항에 따른 ‘정보’를 제공받은 경우의 통지의무에 관하여 규정하였다.
인터넷을 기반으로 이루어지는 디지털 통신의 형태는 다양한데 이로부터 파생되는 디지털 정보의 취득이 형사소송법상 일반적인 압수수색 규정에 따라 행해지는 것은 문제이다. 컴퓨터 하드디스크에 저장되어 있는 디지털 정보의 경우 물건을 압수수색하는 것과 달리 기술적으로 범죄혐의와 유관한 정보만 따로 추출하는 것이 쉽지 않다 보니 그동안 포괄적인 압수 방법을

66) 출처: 과기정통부(구 미래창조과학부) 보도자료
67) 헌재 2012. 8. 23. 2010헌마439.
68) 대법원 2016. 3. 10. 선고 2012다105482 판결.
69) 인권위, 2016. 11. 28. 통신자료 제공 제도 헌재 의견 제출.

취해 왔다. 이로 인해 방대한 디지털 증거의 수집이 가능했고 범죄혐의와 무관한 정보주체의 사생활 침해, 통신비밀 침해가 현저히 크다는 지적이 많았다. 일례로, 전교조시국선언, 세월호 참사 교사선언 고발 사건에서 수사기관이 압수수색을 통해 수집한 정보를 토대로 새로운 수사로 확대한 사례가 논란이 되었다.

2019. 10. 2. “카카오톡 사찰” 논란을 불러일으킨 정진우 전 노동당 부대표 사건에 대해 서울중앙지방법원은 정씨 등 24명이 국가와 카카오를 상대로 낸 손해배상 청구 소송에서 5년만에 판결을 내리면서 국가를 상대로 한 정씨의 일부 승소만 인정하였을 뿐 나머지 청구를 모두 기각하였다(2014가단5351343). 경찰은 2014년 세월호 참사 책임자 처벌을 요구하는 집회를 주도한 혐의로 정씨를 수사했다. 경찰은 법원에 정씨의 휴대전화 카카오톡 메시지 내용과 대화상대방의 아이디와 전화번호 등에 대해 압수수색 영장을 신청했고, 경찰은 발부된 영장을 팩스로 카카오에 전송했다. 이에 카카오는 정씨의 대화상대 전화번호 목록과 대화 일시·내용·사진 등을 이메일로 경찰에 제출했고, 검찰은 이를 근거로 정씨를 일반교통방해죄 등으로 기소했다. 정씨는 이와 같은 수사과정에서 경찰이 자신과 같은 단톡방에 있었을 뿐 메시지를 주고받지는 않은 이들의 전화번호 등에 대해서까지 압수했다며 지난 2014. 12. 국가 등을 상대로 300만 원의 배상을 요구하는 소송을 냈다. 오민석 부장판사는 “당시 압수수색 영장의 내용과 목적 등에 비춰보면 정씨가 가입한 대화방의 경우 '대화 상대방'에는 정씨와 이야기를 주고받기 위해 가입한 제삼자가 모두 포함된다고 보아야 하고, 그 대화방에서 정씨가 대화를 건넨 적이 있는 상대만으로 그 범위가 제한된다고 볼 수 없다”고 밝혔다. 이어 “정씨가 가입한 대화방에 들어와 있지만 전혀 대화한 사실이 없는 제3자나 그 대화방에서 정씨를 제외한 제3자들만이 대화를 나눈 경우의 제3자들이라 하더라도, 그 제3자들은 모두 정씨와 이야기를 주고받기 위한 상대방으로서 대화방에 들어와 있다고 보아야 하므로, 영장에 기재된 '대화 상대방'에 포함되고, 그러한 제3자의 전화번호 등은 영장에 기재된 '압수할 물건'에 속한다고 보아야 한다”고 설명했다. 오 부장판사는 다만 경찰이 영장을 집행하면서 영장 원본을 카카오에 제시하지 않고 팩스로 송부한 것은 위법하다고 판단하면서도, 영장을 팩스로 전송한 것은 1990년 후반부터 업무의 효율성을 높이기 위해 이어져온 실무관행에 따른 것인 점 등을 고려해 손해배상액을 100만 원으로 정했다. 아울러 오 부장판사는 정씨와 함께 소송을 제기한 나머지 23명에 대해서는 “영장의 집행으로 메시지 내용이나 전화번호 등 정보가 압수됐다고 볼 증거가 없다”며 국가 또는 카카오의 배상책임을 인정하지 않았다.

위 판결에 대해 참여연대 사법감시센터는 “이런 태도는 인터넷 이용자이자 정보주체인 시민들의 정보인권을 소홀하게 취급하는 것이다. 일상생활의 더 많은 부분이 통신 매체에 의존할수록 국가기관 또는 막강한 권력을 가진 제3자가 우리의 통신내용을 보겠다고 요구하는 일이 늘어날 것이다. 그리고 통신내용은 과거보다 더 많이, 더 손쉽게 제3자에 공개될 수 있다. 누가 이것을 견제할 수 있을까. 자신의 통신내용이 충분히 보호받지 못한다고 생각하는 순간 집회·시위의 자유를 비롯하여 행동의 자유, 나아가 국가에 불복종할 수 있는 국민의 권리조차 위축될 것이다. 항소심에서는 부디 법원이 올바르게 판단하여 1심의 판결을 바로잡기 바란다”는 판결 비평을 발표했다.[70]

또한 「통신비밀보호법」 제9조의3은 실시간 전기통신과 “송·수신이 완료된 전기통신”를 구분하고, 실시간 전기통신의 경우는 통신제한조치(감청), 송·수신이 완료된 전기통신에 대해서는 형사소송법상 압수·수색·검증에 의할 것을 예정하고 있다. 대법원도 “통신비밀보호법 제2조 제3호 및 제7호에 의하면 같은 법상 ‘감청’은 전자적 방식에 의하여 모든 종류의 음향·문언·부호

70) https://www.peoplepower21.org/Judiciary/1664107 (2019. 11. 15. 최종접속)

또는 영상을 송신하거나 수신하는 전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다. 그런데 해당 규정의 문언이 송신하거나 수신하는 전기통신 행위를 감청의 대상으로 규정하고 있을 뿐, 송·수신이 완료되어 보관 중인 전기통신 내용은 대상으로 규정하지 않은 점, 일반적으로 감청은 다른 사람의 대화나 통신 내용을 몰래 엿듣는 행위를 의미하는 점 등을 고려하여 보면, 통신비밀보호법상 '감청'이란 대상이 되는 전기통신의 송·수신과 동시에 이루어지는 경우만을 의미하고, 이미 수신이 완료된 전기통신의 내용을 지득하는 등의 행위는 포함되지 않는다"고 하여 같은 입장이다.[71]

이러한 입장에서 2016. 10. 13. 대법원은 「국가보안법」위반 혐의로 기소된 '자주 통일과 민주주의를 위한 코리아연대' 공동대표 이아무개씨 등 3명에게 징역 2년에 자격정지 3년을 선고한 원심을 확정하면서, 통신제한조치(감청) 집행을 위탁받은 카카오가 3~7일마다 정기적으로 서버에 저장된 대화내용을 추출해 수사기관에 제공한 것은 위법하다고 판단했다. 대법원은 "전기통신의 감청은 전자장치 등을 사용해 실시간으로 카톡에서 송수신하는 문언을 청취하여 지득하는 방식 외에 다른 방식으로 집행해서는 안 된다"며 "카카오의 집행은 동시성 또는 현재성 요건을 충족하지 못해 통신비밀보호법이 정한 감청이라고 볼 수 없으므로 이 사건 통신제한조치허가서에 기재된 방식을 따르지 않은 것으로서 위법하다"고 밝혔다. 다만 대법원은 위법하게 수집된 카톡 대화를 증거로 인정하지 않아도 다른 증거로 이씨 등의 유죄는 인정된다고 판단했다.[72]

하지만 이러한 분류는 고도의 지능정보사회에 맞지 않는 아날로그 입법이다. 고전적 의미의 감청은 통신이 끝나면 '휘발'되어 그 통신의 내용이 세상 어디에도 존재할 수 없는 경우를 상정한다. 과거 유선전화나 무전기 정도를 생각하면 이해가 쉬울 것이다. 즉 그 '실시간'을 놓치면 더 이상 '지득 또는 채록'할 수 없기 때문에 종래의 감청은 당연히 실시간으로 진행되어졌고, 따라서 굳이 '실시간'이라는 요건을 법문에다 명시할 필요도 없었다. 이것이 바로 현행 「통신비밀보호법」이 상정하고 있는 '아날로그' 마인드이다. 그러나 요즘의 디지털 통신은 저절로 휘발되지 않으며, '비휘발' 또는'저장' 옵션이 선택되는 한 디지털 통신의 내용은 마치 결재를 위한 서류마냥 차곡차곡 쌓여 통신이 끝나면 한 권의 책처럼 추려져 수사기관에 전달된다. 그 결과 서버로 날아오는 통신데이터를 서버입구의 '앞'에서 수집하면 감청, 서버입구의 '뒤'에서 수집하면 압수·수색이 된다. 다시 말해 디지털 통신에 있어서는 감청과 압수·수색의 기술적 본질은 같다. 둘 다 복사(copy)일 뿐이다.[73]

5) 「국민보호와 공공안전을 위한 테러방지법」(일명 테러방지법)

2016. 3. 2. 19대 국회에서 통과되기 훨씬 전인 2001년부터 국회 매 회기마다 테러방지 관련 법안이 제출되어 오다가, 2015. 11.월 파리 이슬람무장단체의 테러공격을 계기로 박근혜 정부가 테러방지법안 통과를 압박하였다. 이에 대해 테러 위협을 빙자한 '국민감시법', '국정원 강화법'이라고 반대하는 다수의 국민, 시민사회의 강력한 반대가 있었음에도 불구하고, 결국 「국민보호와 공공안전을 위한 테러방지법」(일명 테러방지법)이 제정되었다.

테러방지법의 주요 내용은 국가정보원이 주도하는 '대테러센터'를 설립하고, '대테러센터'로

---

71) 대법원 2012. 10. 25. 선고 2012도4644 판결.
72) 대법원 2016. 10. 13. 선고 2016도8137 판결.
73) 오길영, "현행 통신비밀보호법의 문제점과 개선방향", 「언론과법」 14(1), 2015, 34면.

하여금 테러정보의 수집 외에 대테러활동 기획·지도 및 조정하며, 관계기관에 테러사건 대책본부를 설치하여 국가정보원의 지도를 받도록 하고 관계기관대책회의를 운영하고 특수부대나 군병력의 출동을 요청할 수 있도록 하는 것이었다.
그러나 실질적 내용은 포괄적인 테러라는 개념을 도입해 국가정보원에 국민의 금융정보, 통신기록까지 마음대로 볼 수 있도록 과도하고 포괄적인 권한을 부여하여 국민감시를 무제한 허용하는 것이라는 게 시민사회의 비판이다. 국가정보원은 자의적 판단으로 '테러위험인물'을 지정할 수 있고, 테러위험인물에 대한 출입국·금융거래 및 통신 이용정보, 노조·정당의 가입, 정치적 견해, 건강, 성생활 등 민간정보를 포함한 개인정보와 위치정보 등 무차별 수집이 가능하다. 또한 테러위험인물에 대한 조사 및 추적권한이 부여되고, 감청사유의 확대로 인해 영장 없이 36시간 감청할 수 있는 범위(긴급통신제한조치)도 확대된다.

6) 전기통신사업법상 휴대폰 본인확인제

2014. 10. 15. 개정된 「전기통신사업법」은 대포폰의 유상 구매와 유통을 금지하고 이를 위반한 경우 형사처벌하는 내용을 신설하였다(제32조의4 제1항, 제95조의2 제2호 및 제3호). 동시에 휴대전화 통신계약을 체결하는 과정에서 본인확인을 거쳐야 함을 명문화하고 그에 필요한 시스템을 한국정보통신진흥협회에 위탁하여 구축하도록 하는 소위 휴대폰 본인확인제 또는 실명제를 도입하였다(제32조의4 제2항 및 제32조의5). 이에 따라 본인확인절차를 거쳐야만 휴대전화 통신계약을 체결할 수 있게 되었다. 이러한 휴대폰 실명제는 익명 통신을 전면적으로 불가능하게 하므로 통신의 비밀과 자유를 제한하는 제도이다.

(2) 헌법재판소 주요 결정례

1) 2018년 기지국 수사 헌법불합치결정

이 사건에서는 2012년 선거 기간 중 금품살포 의혹을 조사하던 수사당국이 특정 시간 해당 지역 기지국을 이용한 659명의 통신사실확인자료를 제공받았다. 같은 해 피해자들은 「통신비밀보호법」 제13조 제1항에 대한 헌법소원심판을 청구했고 2018. 6. 28. 헌법재판소는 위 조항에 대해 과잉금지의 원칙에 반하여 개인정보자기결정권과 통신의 자유를 침해한다는 이유로 헌법불합치결정을 내렸다.[74]
헌법재판소는 "이동전화의 이용과 관련하여 필연적으로 발생하는 통신사실확인자료는 비록 비내용적 정보이지만 여러 정보의 결합과 분석을 통해 정보주체에 관한 정보를 유추해낼 수 있는 민감한 정보인 점, 수사기관의 통신사실확인자료 제공요청에 대해 법원의 허가를 거치도록 규정하고 있으나 수사의 필요성만을 그 요건으로 하고 있어 제대로 된 통제가 이루어지기 어려운 점, 기지국수사의 허용과 관련하여서는 유괴·납치·성폭력범죄 등 강력범죄나 국가안보를 위협하는 각종 범죄와 같이 피의자나 피해자의 통신사실확인자료가 반드시 필요한 범죄로 그 대상을 한정하는 방안 또는 다른 방법으로는 범죄수사가 어려운 경우(보충성)를 요건으로 추가하는 방안 등을 검토함으로써 수사에 지장을 초래하지 않으면서도 불특정 다수의 기본권을 덜 침해하는 수단이 존재하는 점을 고려할 때, 이 사건 요청조항은 과잉금지원칙에 반하여 청구인의 개인정보자기결정권과 통신의 자유를 침해한다"고 판단했다.

---

74) 헌재 2018. 6. 28. 2012헌마538, 통신비밀보호법 제13조 제1항 위헌확인 등(헌법불합치,잠정적용).

2) 2018년 실시간 위치추적 헌법불합치결정

수사기관이 2013. 12. 9.부터 12. 30.까지 철도공사 민영화에 반대하며 파업을 하던 철도노조 위원장을 비롯 철도노조 조합원 15명과 그들의 가족 21명의 통신사실확인자료 제공을 받았다. 당시 수사기관은 휴대전화와 인터넷 사이트 접속위치를 실시간으로 추적했단 사실이 드러났다. 이에 피해자들은 2014년에「통신비밀보호법」제2조 제11호 바목 등에 대해 헌법소원심판을 청구하였으나, 헌법재판소는 오랜 심리 기간을 거쳐 2018. 6. 28. 마침내 위 조항에 대해 과잉금지의 원칙에 반하여 개인들의 개인정보자기결정권과 통신의 자유를 침해한다며 헌법불합치결정을 내렸다.[75)]

헌법재판소는 "수사기관은 위치정보 추적자료를 통해 특정 시간대 정보주체의 위치 및 이동상황에 대한 정보를 취득할 수 있으므로 위치정보 추적자료는 충분한 보호가 필요한 민감한 정보에 해당되는 점, 그럼에도 이 사건 요청조항은 수사기관의 광범위한 위치정보 추적자료 제공요청을 허용하여 정보주체의 기본권을 과도하게 제한하는 점, 위치정보 추적자료의 제공요청과 관련하여서는 실시간 위치추적 또는 불특정 다수에 대한 위치추적의 경우 보충성 요건을 추가하거나 대상범죄의 경중에 따라 보충성 요건을 차등적으로 적용함으로써 수사에 지장을 초래하지 않으면서도 정보주체의 기본권을 덜 침해하는 수단이 존재하는 점, 수사기관의 위치정보 추적자료 제공요청에 대해 법원의 허가를 거치도록 규정하고 있으나 수사의 필요성만을 그 요건으로 하고 있어 절차적 통제마저도 제대로 이루어지기 어려운 현실인 점 등을 고려할 때, 이 사건 요청조항은 과잉금지원칙에 반하여 청구인들의 개인정보자기결정권과 통신의 자유를 침해한다"고 판단했다.

3) 2018년 인터넷 패킷감청 헌법불합치결정

국가정보원장이 국가보안법위반 범죄수사를 위하여 김모씨의 휴대폰, 인터넷회선 등에 대해 2008년경부터 2015년경까지 법원으로부터 총 35차례의 통신제한조치를 허가받아 집행했는데 그 중 청구인 명의로 가입된 인터넷 회선에 대해 6차례에 걸쳐 인터넷 통신망에서 정보 전송을 위해 쪼개어진 단위인 전기신호 형태의 '패킷'(packet)을 수사기관이 중간에 확보하여 그 내용을 지득하는 이른바 '패킷감청'이 행해졌다. 이에 청구인은 2016년에「통신비밀보호법」제5조 제2항 중 '인터넷회선을 통하여 송·수신하는 전기통신'에 관한 부분에 대해 헌법소원을 제기하였고, 2018. 8. 30. 헌법재판소는 위 조항에 대해 과잉금지 원칙에 반하여 통신의 비밀과 자유 및 사생활의 비밀과 자유를 침해한다는 이유로 헌법불합치결정을 내렸다.[76)]

헌법재판소는 "이 사건 법률조항은 인터넷회선 감청의 특성을 고려하여 그 집행 단계나 집행 이후에 수사기관의 권한 남용을 통제하고 관련 기본권의 침해를 최소화하기 위한 제도적 조치가 제대로 마련되어 있지 않은 상태에서, 범죄수사 목적을 이유로 인터넷회선 감청을 통신제한조치 허가 대상 중 하나로 정하고 있으므로 침해의 최소성 요건을 충족한다고 할 수 없다. 이러한 여건 하에서 인터넷회선의 감청을 허용하는 것은 개인의 통신 및 사생활의 비밀과 자유에 심각한 위협을 초래하게 되므로 이 사건 법률조항으로 인하여 달성하려는 공익과 제한되

---

75) 헌재 2018. 6. 28. 2012헌마191, 통신비밀보호법 제2조 제11호 바목 등 위헌확인(헌법불합치,잠정적용).

76) 헌재 2018. 8. 30. 2016헌마263, 통신제한조치 허가 위헌확인 등(헌법불합치,각하).

는 사익 사이의 법익 균형성도 인정되지 아니한다. 그러므로 이 사건 법률조항은 과잉금지원칙에 위반하는 것으로 청구인의 기본권을 침해한다"라고 판단했다.

4) 2019년 휴대폰 실명제 합헌 결정

2014. 10. 15. 개정된 「전기통신사업법」은 대포폰의 유상 구매와 유통을 금지하고 이를 위반한 경우 형사처벌하는 내용을 신설하고, 동시에 휴대전화 통신계약을 체결하는 과정에서 본인확인을 거쳐야 함을 명문화하고 그에 필요한 시스템을 한국정보통신진흥협회에 위탁하여 구축하도록 하는 소위 휴대폰 본인확인제 또는 실명제를 도입하였다(제32조의4 제2항 및 제32조의5). 시민사회단체 관계자들은 휴대폰 실명제가 익명으로 통신할 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 침해한다고 주장하면서 2017. 11. 1. 위 법률 조항들에 대해 헌법소원심판을 청구하였다. 이에 대해 헌법재판소는 2019. 9. 26. 재판관 7(기각):2(인용)의 의견으로 '휴대전화 가입 본인확인제'에 관한 위 법률 조항들이 개인정보자기결정권과 익명 통신의 자유를 침해하지 않는다는 결정을 선고하였다.[77)]

헌법재판소는 휴대폰 본인확인 조항이 익명 통신의 자유와 개인정보자기결정권을 제한하는 점을 인정하면서도, "타인 또는 허무인의 이름을 사용한 휴대전화인 이른바 대포폰이 보이스피싱 등 범죄단의 범행도구로 이용되는 것을 막고, 개인정보를 도용하여 타인의 명의로 가입한 다음 휴대전화 소액결제나 서비스요금을 그 명의인에게 전가하는 등의 명의도용피해를 막고자 하는 입법목적은 정당하고, 이를 위하여 본인확인절차를 거치게 한 것은 적합한 수단이다. 가입자는 계약 체결 시에 자신의 주민등록번호를 제공해야 하지만 그 중 특히 뒷자리 중 성별을 지칭하는 숫자 외의 6자리는 일회적인 확인 후 폐기되므로 주민등록번호가 이동통신사에 보관되어 계속적으로 이용되는 것이 아니다. 가입자는 대면(오프라인)가입 대신 온라인 가입절차에서 공인인증서로 본인확인하는 방법을 택하여 주민등록번호의 직접 제공을 피할 수도 있다. … 심판대상조항에 의해서는 아직 의사소통이 이루어지지 않은 이동통신서비스 가입단계에서의 본인확인절차를 거치는 것이므로, 이동통신서비스 가입자가 누구인지 식별가능해진다고 하여도 곧바로 그가 누구와 언제, 얼마동안 통화하였는지 등의 정보를 파악할 수 있는 것은 아니다. 따라서 심판대상조항으로 인해 가입자가 개개의 통신내용과 이용 상황에 기한 처벌을 두려워하여 이동통신서비스 이용 여부 자체를 진지하게 고려하게 할 정도라고 할 수 없다. 개인정보자기결정권, 통신의 자유가 제한되는 불이익과 비교했을 때, 명의도용피해를 막고, 차명 휴대전화의 생성을 억제하여 보이스피싱 등 범죄의 범행도구로 악용될 가능성을 방지함으로써 잠재적 범죄 피해 방지 및 통신망 질서 유지라는 더욱 중대한 공익의 달성효과가 인정된다. 따라서 심판대상조항은 청구인들의 개인정보자기결정권 및 통신의 자유를 침해하지 않는다"라고 판단하였다.[78)]

(3) 국가인권위원회 주요 결정례

1) 「전기통신사업법」 통신자료제공제도와 「통신비밀보호법」 통신사실확인자료제공제도 개선권고

77) 헌재 2019. 9. 26. 2017헌마1209, 전기통신사업법 제32조의4 제2항 등 위헌확인.
78) 이에 대한 비판은 (사)오픈넷, "전기통신사업법상 휴대폰 실명제 합헌 결정 유감" 논평 참조, https://opennet.or.kr/16787 (2019. 11. 15. 최종접속)

2014. 4. 9. 국가인권위원회는 ①「전기통신사업법」 제83조 제3항이 규정한 가입자 이름, 주소, 주민등록번호 등 '통신자료'를 '통신사실확인자료'에 포함시키고 법원의 허가장을 받아서 요청하게 할 것, ② 통신사실확인자료를 요청할 때 현재의 영장요건인 '수사상의 필요성'뿐만 아니라 '범죄의 개연성'과 요청 자료의 '사건 관련성'을 추가하는 것으로 강화할 것, ③ 실시간 위치정보를 요청할 때는 ②의 요건뿐만 아니라 다른 방법이 없을 것이라는 보충성을 추가하여 수사과정에서 개인정보보호 정도를 강화하도록 관련법의 개정을 추진할 것을 미래창조과학부장관에게 권고하였다.[79] 주문에 제시된 구체적인 권고 내용은 아래와 같다.

1.「전기통신사업법」 중 제83조 제3항을 삭제하는 내용의 법 개정을 추진할 것
2.「통신비밀보호법」 중 다음의 내용을 반영하는 법 개정을 추진할 것
   가. '가입자정보', '실시간위치정보'의 정의규정을 신설하는 것
   나. 제2조 제11호 중 바.목과 사.목에서 '실시간위치정보'를 제외하는 것
   다. 제13조와 관련하여 검사 또는 사법경찰관이 범죄수사를 목적으로 가입자정보 및 통신사실확인자료(실시간위치정보는 제외한다)의 제공을 요청할 수 있는 요건을 "피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당사건과 관계가 있다고 인정할 수 있는 것"에 한정하는 것
   라. 범죄의 수사를 목적으로 하는 '실시간위치정보'제공의 요청은 위 다.항의 요건 외에 보충성의 요건을 갖춘 경우로 한정하는 것

2) 통신자료 제공 제도 헌재 의견 제출

2016. 11. 28. 국가인권위원회는 「전기통신사업법」에 따른 정보.수사기관의 통신자료 수집은 개인정보자기결정권을 침해할 소지가 있다는 의견을 헌법재판소에 제출하였다. 위 통신자료 제공 제도에 대한 헌법소원(2016헌마388)과 관련하여 인권위는 "통신자료 제공 제도는 개인정보 수집 목적과 대상자 범위가 지나치게 넓고, 사전 또는 사후에 사법적 통제가 이루어지지 않으며, 정보주체가 자신의 개인정보 제공 사실을 인지할 수 있는 통지 절차가 마련되지 않아 개인정보자기결정권을 침해할 소지가 있다"고 판단하였다.[80]

3) 「통신비밀보호법 일부개정법률안」에 대한 의견표명

2019. 7. 22. 국가인권위원회는 정부 발의 「통신비밀보호법 일부개정법률안」에 대해, 통신사실확인자료제공 및 이에 대한 통지, 위치정보 추적자료제공, 기지국 통신사실확인자료제공 등 주요 내용이 헌법재판소 결정 취지, 위원회 결정례 등에 비추어 정보주체 기본권을 충분히 보장하는 방향으로 개정될 수 있도록 국회의장과 법무부장관에게 의견을 표명하였다.[81] 주문에 나타난 구체적인 의견표명의 내용은 다음과 같다.

---

79) 인권위 2014. 4. 9.「전기통신사업법」 통신자료제공제도와「통신비밀보호법」 통신사실확인자료제공제도 개선권고.
80) 인권위, 2016. 11. 28. 통신자료 제공 제도 헌재 의견 제출.
81) 인권위 2019. 7. 22.「통신비밀보호법 일부개정법률안」에 대한 의견표명.

1. 통신제한조치 연장과 관련하여, 위 개정법률안 제6조 제7항에서 통신제한조치의 총연장기간 또는 총연장횟수를 축소 및 제한하는 것이 바람직함.
2. 통신사실확인자료제공과 관련하여, 위 개정법률안 제13조 제1항에 대상범죄 및 대상자 한정, 구체적인 범죄혐의 또는 해당 사건과의 관련성 소명 요구, 보충성 요건 강화 등 자료제공 요건을 강화하는 것이 바람직함.
3. 위치정보 추적자료제공과 관련하여, 위 개정법률안 제13조 제2항에 대상범죄 및 대상자 한정, 구체적인 범죄혐의 또는 해당 사건과의 관련성 소명 요구, 보충성 요건 강화 등 자료제공 요건을 강화하는 것이 바람직함.
4. 기지국 통신사실 확인자료제공과 관련하여, 위 개정법률안 제13조 제3항에 대상범죄 명시, 구체적인 범죄혐의 또는 해당 사건과의 관련성 소명 요구, 보충성 요건 강화 등 자료제공 요건을 강화하는 것이 바람직함.
5. 통신사실확인자료제공 통지와 관련하여, 요청사유 등 통지사항 명문화, 통지의무 위반자에 대한 제재규정 마련, 공소제기 등 수사상 보안유지 필요 사유 소멸 시 통신사실확인자료제공사실에 대한 즉시통지, 통지유예 기간 규정 및 법원 등 객관적·중립적 기관의 허가, 보다 엄격하고 구체적인 유예사유 명시 등 제도를 보완하는 것이 바람직함.

4. 주요 쟁점 사례

(1) 통신자료 제공 남용 사례

1) 통신3사 상대 통신자료 제공현황 공개 및 손해배상 청구소송

2013. 4. 인터넷포털과 달리 수사기관의 요청에 무조건 통신자료를 제공하였음에도 통신자료 제공현황 열람 요청에 응하지 않는 이동통신 3사를 상대로 통신3사 이용자들이 통신자료 제공현황에 대한 열람청구 및 손해배상청구소송을 제기하였다. 1심은 통신자료 제공현황을 공개하라는 판결을 선고하였으나 손해배상 책임은 부정하였다. 항소심은 1심에서 인정하지 않았던 손해배상 책임도 인정하였다. 수사업무에 지장이 발생할 수 있다는 막연한 사정만으로 헌법과 법률이 보장하는 정보주체의 개인정보자기결정권을 제한할 수 없다며, 원고들의 공개청구를 상당기간 거부한 것이 개인정보자기결정권을 침해한 불법행위라고 인정하였다. 통신3사가 이에 불복하고 상고하였으나, 2018년 7월 20일 대법원이 3년 반만에 통신3사의 상고를 기각하여 항소심 판결이 그대로 확정되었다.

2) 2016년 통신자료 무단 수집 500인 헌법소원 및 수사기관 상대 국가배상 청구소송

2016. 3. 테러방지법 제정에 반대하는 국회의원, 노조가입자 등 다수의 국민의 통신자료를 수사기관이 수집해 갔다는 폭로가 이어졌다. 이에 자신의 통신자료를 수집해 갔는지 확인하는 대국민 캠페인을 시민단체에서 벌였다. 자신의 통신자료가 제공된 것이 확인된 국민 500여명이 「전기통신사업법」 제83조 3항에 대해 헌법소원을 제기하여 현재 심리 중에 있다(2016헌마388). 같은 해 6월에는 수십여명의 시민들이 영장 없이 통신자료를 제공받은 국가정보원, 서울지방경찰청 등 수사기관을 상대로 국가배상청구소송을 제기했다. 이는 같은 해 3월 대법원

이 통신자료제공에 대하여 포털을 상대로 내려진 손해배상판결을 파기환송하면서 “전기통신사업자가 수사기관의 통신자료 제공 요청에 따라 통신자료를 제공함에 있어서, 수사기관이 그 제공 요청권한을 남용하는 경우에는 이용자의 인적사항에 관한 정보가 수사기관에 제공됨으로 인하여 해당 이용자의 개인정보와 관련된 기본권 등이 부당하게 침해될 가능성이 있다”고 하면서, “수사기관의 권한 남용에 의해 통신자료가 제공되어 해당 이용자의 개인정보에 관한 기본권 등이 침해”된 경우에는 그 책임을 해당 수사기관에 직접 추궁하는 것이 타당하다고 설시한 바에 따른 것이다.[82)]

(2) 기무사의 세월호참사 유가족 사찰 및 불법감청 사건

2014. 4. 16. 전라남도 진도군 조도면 부근 해상에서 여객선 세월호가 침몰하면서 승객 304명이 사망하거나 실종되었다(이하 ‘세월호참사’라 한다). 세월호참사 희생자들의 유가족들은 세월호참사에 대한 진상규명과 책임자처벌을 요구해왔지만 아직까지 명확한 침몰원인은 밝혀지지 않았고, 관련 책임자 처벌도 이루어지지 않고 있다. 박근혜 전 정부 산하 국가 권력기관은 세월호참사의 진실을 조사하기 위해 설립된 세월호참사 특별조사위원회를 강제해산하는 등 조직적으로 세월호참사의 진상규명 및 책임자 처벌을 방해하였다.
정부에 구성된 민관 합동 조사팀이 밝힌 바에 따르면, 옛 국군기무사령부(이하 ‘기무사’라 한다)는 세월호참사 다음 날인 2014. 4. 17.부터 소속 부대원에게 세월호참사 희생자 유가족들의 동향을 파악하라 지시하였다. 기무사는 유가족들의 생년월일, 휴대전화, 포털 활동, 개인 블로그 주소, 전자우편, 인터넷 물품구매내역, 주민등록증, 통장사진 등을 수집하였고, 현장에 사찰하는 요원들에게 유가족으로 신분을 위장하라는 등 지침을 내리기까지 하였다. 특히 기무사는 진상규명과 책임자 처벌을 요구하는 세월호 유가족들을 ‘종북세력’으로 분류하고, 언론에 허위사실을 유포하는 등의 국가범죄를 자행하였다. 그럼에도 불구하고 국방부 특별수사단이 2018. 11. 발표한 수사결과에 따르면 피의자 중 5명만이 정식 기소되고, 나머지 4명이 기소유예되었다.
민주평화당 천정배 의원이 2019. 4. 8. 기무사가 작성한「세월호 TF」일일보고서를 공개하면서, 박근혜정부 시절 기무사가 일반 시민 다수의 통화를 무작위로 불법감청한 것이 드러났다. 기무사는 2014. 6. 10.부터 2014. 7. 22.까지 서울, 하남, 성남, 용인, 안성 등에서 자체 보유한 기동방탐장비 또는 미래부(현 과기정통부) 산하 전파관리소의 전파감시설비를 이용하여 법원의 허가 없이 민간의 통신내용을 불법적으로 청취, 녹음하였다. 택시, 병원, 놀이터, 영화관 등 민간의 대화 내용이 무차별적으로 도청되었음이 드러났다. 2019. 4. 15. 시민사회단체는 기무사 등 불법감청 관련 대상자를 검찰에 고발하였다.

(3) 전교조 서버 압수·수색 사건

2014년 7월에 경찰이 세월호참사 관련 교사선언과 조퇴투쟁을 주도한 혐의로 전교조 조합원 76명에 대해 수사하면서 서초동에 있는 전교조 서버에 대해 긴급 압수수색을 진행하면서, 사적인 대화내용이 들어있는 이메일과 네이버 밴드까지 압수수색한 사실이 알려졌다. 피의자는 조사 전까지는 이 사실에 대해 전혀 알지 못했다고 하고, 당시 영장에는 ‘홈페이지 서버 자료’와 ‘서버에 보관된 전교조 이메일 계정 내역’만으로 한정되어 있었다고 한다. 그런데도 휴대폰

82) 대법원 2016. 3. 10. 선고 2012다105482 판결.

까지 압수하여 문제가 되었다.

(4) 국가정보원의 이탈리아 해킹팀 RCS 프로그램 구입 및 실행 사건

2015년 7월 이탈리아 해킹팀의 사이트가 해킹되어 고객 명단이 위키리크스(WikiLeaks)에 공개됨으로써 우리나라 국가정보원이 이탈리아의 '해킹팀'이라는 업체로부터 컴퓨터와 스마트폰에 스파이웨어를 침투시켜 그 컴퓨터와 스마트폰을 감시하는 RCS(Remote Control System)를 2012년부터 구매하고 이용해 왔다는 사실이 알려졌다. 당시 국가정보원은 대북정보수집용이라고 해명했지만 이 해킹감청프로그램을 이용해 민간인들과 정치인 등의 컴퓨터와 스마트폰 등을 불법감청했을 것이란 의심이 팽배하였다.
실제로 해킹팀에 의해 유출된 자료에 따르면, 국가정보원이 카카오톡이나 갤럭시 3 국내 모델을 해킹하려 했고 안랩의 'V3 모바일 2.0'과 같은 국내용 백신을 회피하기 위한 방법을 강구했으며, 서울대 공대 동창회 명부', '미디어오늘' 기자를 사칭한 천안함 보도 관련 문의 워드파일에 악성코드를 심고자 했다고 한다. 또한 네이버 맛집 소개 블로그, 벚꽃축제를 다룬 블로그, 삼성 업데이트 사이트를 미끼로 내건 주소에 '악성 코드를 심어 달라'고 요구하기도 했다고 한다. 이는 국가정보원이 해킹프로그램을 통해 국민들의 컴퓨터와 스마트폰을 엿보고 프라이버시를 침해한 것이다. 또한 해킹을 금지하는 정보통신망법, 허가 받지 아니하는 도청을 금하는 「통신비밀보호법」을 위배함과 동시에 「국가정보원법」 제11조의 직권남용 금지 등의 규정을 위배한 것이다.
2017년 6월 출범한 국가정보원 개혁발전위원회(이하 '개혁위'라 한다)는 이명박·박근혜 정부 당시 국가정보원 관련 '15개 의혹 사건'을 선정해 조사했는데, 그 중 '해킹프로그램 RCS 통한 민간인 사찰 사건'도 포함되었다. 개혁위는 같은 해 10월 발표한 보도자료에서 "국정원은 2012년 이탈리아의 해킹 프로그램 'RCS'를 구매해 테러·국제범죄 등과 연계된 총 213명의 컴퓨터와 휴대전화의 자료를 수집했다"고 밝혔다. 그러나 "RCS 대상자에 내국인 4명이 포함돼 있어 조사한 결과, 해외 거주 북한 연계 혐의(2명), 해외 체류 테러 연계 혐의(1명), 국내 거주 국제범죄 연계 혐의(1명)로 사찰 목적의 내국인은 없었다"며 "해외 교포 3명을 대상으로 RCS를 사용한 것도 북한 연계 혐의를 수집하기 위해서였다"고 했다. 논란 속에 스스로 목숨을 끊은 국가정보원 담당자 임모 과장에 대해서도 일각에선 타살 의혹을 제기했다. 그러나 개혁위는 "RCS 도입·운용 실무자로서 억울함과 조직에 누를 끼쳤다는 책임감을 느끼던 중 심적 중압감으로 극단적인 선택을 한 것"이라고 했다.
그리고 2015년 당시 진보네트워크센터, 민주노총, 민변, 참여연대 등의 시민단체와 국민고발인 2,786명은 국가정보원을 「통신비밀보호법」 및 정보통신망법 위반으로 검찰에 고발했는데, 4년 뒤인 2019. 7. 23. 검찰은 "국정원이 RCS를 이용해 총 213명을 대상으로 211건의 점거 및 정보를 수집한 점에 대해 정보통신망법위반(악성프로그램 전달, 정보통신망 침입, 타인의 정보 또는 침해, 개인정보 수집)을 인정하고, 통화내용을 수집한 19건에 대해서도 통비법위반(감청)을 인정하면서도, RCS 활용은 모두 기술개발부서장(국장급)의 승인 하에 진행되었을 뿐, 국정원장과 2, 3차장이 등이 RCS 도입 및 사용에 관여했다고 볼 증거가 없다"며 이들에 대해 무혐의 처분을 내렸다.

(5) 사인간 감시 사례

1) 기업의 노동감시 문제

업무용 앱은 많은 기업들에서 활용되고 있는 업무 관리 시스템이다. 업무 혁신을 앞세워 스마트오피스, 모바일오피스 등 업무 환경을 재편하려했던 21세기 초반부터 등장했다. 업무용 앱 도입 바람은 증권사, 보험사 등의 금융권을 비롯해 주요 대기업은 물론 한국정보사회진흥원, 중앙선거관리위원회, 한국인터넷진흥원, 에너지관리공단, 도시철도공사, 국민건강보험공단, 한국관광공사 등 공공기관까지 거셌다. 최근 업무용 앱은 삼성그룹 제조계열사는 물론이고 LG그룹, SK그룹, 포스코 등 대기업 다수에서 광범위하게 활용 중이다. 이외에도 KB국민카드는 직원들에게 업무용 앱 설치를 요구했고, 피죤의 경우 노동조합 활동을 하는 직원들에게 실시간으로 영업 사원의 위치를 파악할 수 있는 앱 설치를 지시했다. 포스코 역시 광양제철소에 출근하는 하청 노동자들에게 통화내역 열람이 가능한 앱을 설치하라고 요구했다.

업무용 앱이 문제로 부각됐던 사례는 2014년 KT가 업무용 앱 설치를 지시했고, 이에 직원 이모씨가 개인정보 침해 우려를 들어 앱 설치를 거부하면서 촉발된 사건이다. KT는 무선 통신의 품질을 측정하는 안드로이드 기반 앱을 만들고 설치 방법 등에 대한 교육을 실시한 뒤 업무지원단 소속 직원 283명 중 일부에게 개인 스마트폰에 이 앱을 설치하라고 지시했다. 해당 앱은 위치 정보는 물론 개인 스마트폰의 카메라, 연락처, 개인정보(달력 일정), 저장소, 문자메시지, 계정 정보 등 12개 항목에 접근 권한을 가지고 있었다. 업무지원부 경기지원팀에 근무하던 이씨는 앱 설치 대상에 포함되자 개인정보 침해가 우려된다는 이유로 앱 설치를 거부하고 업무수행을 위한 사업용 단말기를 따로 지급해 주거나 다른 부서 배정을 요청했다. 그러나 KT는 인사위원회를 열어 이씨가 '성실 의무'와 '조직 내 질서존중의 의무'를 위반했다며 정직 1개월의 징계를 내리고 정직 기간이 끝나자 이 씨를 타 부서로 전보발령 냈다. 이에 이씨는 KT의 업무지시가 개인정보 보호법을 위반한 것으로, 앱 설치 거부를 징계사유로 삼을 수 없다며 소송을 제기했고 재판부는 이 씨의 손을 들어줬다. 재판부는 "원고가 이 사건 앱의 설치를 거절해 업무수행을 하지 못했다는 것만으로 성실의무를 위반했다고 볼 수 없다"며 "달리 피고 회사의 업무지시 필요성이 원고의 개인정보 자기결정권에 대한 제한의 불이익보다 더 크다고 볼 수 없다"고 판시했다. 이 사건은 항소심에서도 같은 판결을 받아 직원 이 씨가 승소했다.[83]

노동자 폭행 등 갑질 논란을 일으킨 웹하드 업체 위디스크(회장 양진호)는 해킹앱을 개발해 직원들의 통화 기록, 메시지, 연락처 등 수 만건을 실시간으로 들여다보며 도·감청했다는 언론 보도가 나왔다. 2018년 11월 언론 보도에 따르면, 이 업체 회장은 2011년 말쯤부터 '하이톡'이라는 사내 메신저 개발을 추진했다. 이 과정에서 회장은 직원들이 휴대폰에 '하이톡'을 깔면 자동으로 도청 프로그램 '아이지기'가 몰래 설치되도록 해킹 소스를 끼워 넣었다. 본래 '아이지기'는 자녀 안전을 확인하기 위한 프로그램으로 고안됐다. 휴대폰에 있는 전방, 후방 카메라를 원격으로 촬영해서 주변을 살피거나 실시간 위치추적을 하는 기능 등이 포함돼 사실상 '실시간 감시'를 할 수 있는 장치다. 2012년경부터 직원들을 도청하기 시작해 통화·문자 메시지·주소록·통화 녹음 파일 등 피해 규모가 약10만 건에 이르는 것으로 파악됐다.[84]

2) 청소년스마트폰감시법과 감시앱

---

83) 서울고등법원 2018. 6. 26. 선고 2017나2024180 판결.
84) 이상 이광석 외, 앞의 연구보고서 참조.

2015. 4. 16.부터 시행된「전기통신사업법」제32조의7은 이통사가 청소년과 전기통신서비스 제공에 관한 계약을 체결하는 경우 청소년유해매체물 및 음란정보에 대한 차단수단을 제공하여야 한다고 하고 있으며, 동법 시행령 제37조의8는 이통사가 계약 체결 시 차단수단의 종류와 내용 등을 고지하고 차단수단을 설치하도록 강제하고 있고, 계약 체결 후에는 차단수단이 삭제되거나 차단수단이 15일 이상 작동하지 아니할 경우 법정대리인에게 통지하도록 하고 있다(이하 '청소년스마트폰감시법'이라 한다). 차단수단이라 함은 스마트폰 애플리케이션을 말하는데, 현재 시중에 나와 있는 차단앱 중 다수는 유해정보 차단을 넘어 스마트폰 사용 모니터링, 위치 추적 등 청소년의 사생활을 과도하게 침해하고 개인정보를 수집하는 기능들을 갖추고 있는 사실상 감시앱이다.

이런 감시앱은 보안이 취약한 경우가 많아 해커들의 표적이 되며, 청소년을 개인정보 유출, 해킹 등의 보안 위험에 노출시키는 것도 문제이다. 2015년에는 정부가 개발·보급해온 "스마트보안관"이 무려 26건의 보안 취약점을 갖고 있음이 시티즌랩의 보고서에 의해 밝혀져 큰 파장을 불러일으켰다.[85] 보고서가 공개된 직후 스마트보안관은 폐기되었지만, 현재는 "사이버안심존"으로 이름만 바꿔 제공되고 있다. 또한 3대 이통사인 KT와 LGU+가 무상으로 제공하고 있는 차단수단도 보안에 매우 취약한 것으로 밝혀졌다.[86]

2016년 8월, 사단법인 오픈넷은 청소년과 청소년 자녀를 둔 부모를 대리하여 청소년스마트폰 감시법에 대해 헌법소원을 청구했다. 청소년스마트폰감시법은 이통사가 청소년의 스마트폰에 차단수단을 의무적으로 설치하고 청소년이 어떤 정보를 검색하고 접근하는지를 상시 감시하게 하여 스마트폰을 사용하는 청소년의 사생활의 비밀과 자유를 침해하고, 청소년과 법정대리인의 개인정보를 수집, 보관, 이용하기 때문에 개인정보자기결정권도 침해한다.

제2절 통신의 비밀과 자유 증진을 위한 개선방안

1. 통신비밀보호법 개정

(1) 통신제한조치(감청) 제도 개선

1) 영장주의의 실질화

통신제한조치에 대한 영장주의 실질화를 위해서는 감청의 목적과 대상 등의 구체적인 명시와 함께 법원의 사후적 통제절차의 마련이 필요하다. 특히 감청의 대상은 사후통지를 받기 전까지는 감청이 이루어지고 있다는 사실을 전혀 모르는 경우가 대부분이며, 범죄수사 목적 감청의 기간은 2개월, 국가안보 목적 감청의 기간은 4개월인데다가 법상으로는 연장횟수에 제한도 없어 그 침해가 장기간 계속될 수 있으며, 감청의 대상뿐만 아니라 그와 통신을 행한 모든 사람에게 통신의 비밀 침해가 발생하고, 수사기관 등이 감청의 목적과 관련 없는 통신정보까지도 지득할 수 있어 침해가 광범위하다는 점에서 기본권에 대한 제한이 매우 큰 공권력 작용이기 때문에 더욱 엄격한 통제가 필요하다.

「통신비밀보호법」은 제5조에서 규정한 범죄의 수사를 위하여 필요한 경우에 감청을 허가할 수

85) https://opennet.or.kr/14032 (2019.11.1. 최종접속)
86) https://opennet.or.kr/14231 (2019.11.1. 최종접속)

있도록 규정하면서 감청을 허가할 수 있는 대상범죄의 범위를 광범위하게 규정하고 있어 제한이 필요하다. 심지어 국가안보를 위한 감청의 경우에는 대상이 되는 범죄가 특정되어 있지 않고, 목적 또한 불명확하고 광범위하므로 목적과 대상을 구체적으로 명시할 필요가 있다. 그리고 대상범죄의 요건에서 "계획" 및 "피내사자"를 삭제하고 보충성 요건을 "범인의 체포 또는 증거의 수집이 불가능하거나 현저히 곤란한 경우"등으로 강화할 것이 요구된다.[87]
그리고 현행 「통신비밀보호법」상의 구조에 따르면, 법원은 통신제한조치 허가서(영장) 발부 이외에는 어떠한 통제 권한이나 수단도 갖고 있지 않다. 영장주의의 실질화라는 측면에서 본다면 법원이 허가 단계에서뿐만 아니라 그 이후의 집행 과정 그리고 종료 후에도 관여할 수 있는 수단이나 절차를 마련하는 것이 필요하다.

2) 총연장기간 또는 연장횟수 제한

통신제한조치 기간은 헌법상 무죄추정의 원칙과 통신의 비밀 보호에 비추어 인정되는 불감청 수사원칙의 예외로 설정된 기간으로, 이 기간을 연장하는 것은 예외에 대한 특례를 인정하는 것이므로 최소한도에 그쳐야 한다. 헌법재판소는 감청 당시에 개인이 감청 사실을 알 수 없기 때문에 방어권을 행사하기 어려운 상황이라는 점에서 영장을 통해 압수·수색의 사실을 고지받고 시행되는 압수·수색의 경우보다 오히려 그 기본권의 제한의 정도가 크며, 이 기간을 연장하는 것은 예외에 대하여 다시금 특례를 설정하여 주는 것이 되므로 최소한에 그쳐야 한다고 밝히면서 「통신비밀보호법」 제6조 제7항 단서 부분에 대해 헌법불합치 결정을 내린 바 있다.[88]
이에 대해 2019년 3월 정부가 제출한 「통신비밀보호법 일부개정법률안」(이하 '정부 개정안')은 제6조 제8항에서 통신제한조치를 연장하는 경우 총 연장기간은 1년을 초과할 수 없고, 내란·외환의 죄 등 범죄에 대하여는 3년을 초과할 수 없도록 규정함으로써 감청 연장기간에 대해 최소한의 한계를 설정하라는 헌법재판소 결정의 취지를 반영하고자 하였다. 그러나 감청 연장의 기간을 원칙적 1년, 예외적 3년으로 규정한 것은 근거가 불명확할 뿐만 아니라 과도하여 헌법재판소 결정의 취지에 어긋날 소지가 있다. 따라서 총연장기간을 보다 짧은 기간으로 정하고 연장의 횟수도 제한하는 등 보다 엄격한 방향으로 개선할 필요가 있다.

3) 사후통지 제도 개선

헌법 제12조에 규정된 적법절차원칙은 비단 형사절차뿐만 아니라 모든 국가작용 전반에 적용되며, 적법절차원칙에서 도출되는 중요한 절차적 요청으로, 당사자에게 적절한 고지를 행할 것, 당사자에게 의견 및 자료 제출의 기회를 부여할 것 등을 들 수 있다.[89] 통신제한조치에 관한 수사기관의 권한남용을 방지하고 정보주체의 기본권을 보호하기 위해서는, 적법절차원칙에 따라 정보주체에게 적절한 고지와 실질적인 의견진술의 기회가 부여되어야 한다. 그런데 현행 「통신비밀보호법」은 감청의 대상자에 대한 사후통지만 규정하고 있고 사전통지는 규정하고 있지 않아, 정보주체로서는 그 사실을 통보받기 전까지는 자신이 어떤 절차와 내용으로 감

87) 이호중, "통신비밀보호법 개선 대안", 「통신비밀보호법의 개선 쟁점과 방향」 토론회 자료집, 2019, 28면.
88) 헌재 2010. 12. 28. 2009헌가30, 통신비밀보호법 제6조 제7항 단서 위헌제청.
89) 헌재 2003. 7. 24. 2001헌가25; 헌재 2015. 9. 24. 2012헌바302 등 참조.

청당했는지 알 수 없는 구조이다. 게다가 사후통지의 경우에도 감청의 집행 종료일이 아닌 감청을 집행한 사건에 관한 처분을 한 날을 기준으로 통지를 하고 있어 문제이다. 또한 수사기관이 통지를 하는 경우에도 그 사유에 대해서는 통지하지 아니할 수 있도록 함으로써 정보주체는 수사기관으로부터 사후통지를 받더라도 자신이 어떠한 사유로 감청당했는지 전혀 짐작할 수도 없다. 그 결과 정보주체로서는 감청과 관련된 수사기관의 권한남용에 대해 적절한 대응을 할 수 없으며, 이는 적법절차원칙에 위배된다.

헌법재판소도 "현행법상 감청의 집행 통지는 해당 사건에 관하여 검사가 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지 결정을 제외한다)을 한 때를 기준으로 하여, 집행 사유를 제외하고 집행 사실과 집행기관 및 그 시간만을 통지하게 되어 있어(법 제9조의2), 집행 통지를 받더라도 무슨 사유로 감청을 당했는지 알 수가 없고, 수사가 장기화되거나 기소중지 처리되는 경우에는 감청이 집행된 사실조차 알 수 있는 길이 없는바, 이러한 통지 제도는 객관적이고 사후적인 통제 수단의 부재와 결합하여 인터넷회선 감청으로 인한 개인의 통신 및 사생활의 비밀과 자유의 침해 정도를 가늠하기조차 어렵게 한다"고 하였다.[90]

심지어 통지유예 제도를 두고 있는데, 유예 기간을 한정하고 있지 않고 관할 지방검찰청 검사장 등 수사기관의 승인으로 유예를 할 수 있어 사실상 무기한 통지유예가 이루어질 수 있다. 이 또한 적법절차 원칙 위반이며, 정보주체의 기본권 보호와 방어권 보장 측면에서 바람직하지 않다.

사후통지 기간을 '집행 종료한 날로부터 30일 이내' 또는 보다 단기간으로 정할 필요가 있다. 통지유예에 대해서도 적정한 통지유예 기간을 정하고, 이를 초과할 경우 법원의 허가를 받게 하며, 통지유예 결정 자체도 법원의 허가를 받도록 함으로써 남용의 가능성을 최소화하는 개선이 필요하다.

(2) 통신사실확인자료 제공 제도 개선

1) 영장주의의 실질화

과거에는 통신내용과 통신사실확인자료는 통신내용 이외의 사항인 메타데이터로서 그 보호의 정도가 다르다고 보았다. 「통신비밀보호법」 역시 통신제한조치에 대해서는 대상범죄를 제한하는 등 요건을 엄격하게 규정한 반면, 통신사실확인자료 제공에 대해서는 대상범죄 제한 없이 "수사 또는 형의 집행을 위한 필요한 경우"라는 수사의 필요성만을 요구하는 등 완화된 요건으로 규율하였다.

그러나 빅데이터 분석기법 도입 등 정보통신 환경 변화로 통신내용과 메타데이터 간 보호가치의 차이가 사라지고 있는 상황에서 통신사실확인자료의 수집이 통신내용의 수집보다 기본권 침해 정도가 적다고 보기 어렵다. 헌법재판소도 통신사실확인자료가 비내용적 정보기이기는 하나, 여러 정보의 결합과 분석을 통해 정보주체에 관한 다양한 정보를 유추해내는 것이 가능하므로 통신내용과 거의 같은 역할을 할 수 있고, 강력한 보호가 필요한 민감한 정보로 통신내용과 더불어 통신의 자유를 구성하는 본질적 요소에 해당하며, 통신사실확인자료 제공 시 엄격한 요건 하에 예외적으로 허용해야 한다고 판단한 바 있다.[91]

따라서 통신사실확인자료 제공에 있어도 통신제한조치에 준하는 엄격한 요건이 요구된다. 「통

90) 헌재 2010. 12. 28. 2009헌가30, 통신비밀보호법 제6조 제7항 단서 위헌제청.
91) 헌재 2018. 6. 28. 2012헌마538, 통신비밀보호법 제13조 제1항 위헌확인 등.

신비밀보호법」 제5조 제1호에서 감청 대상범죄를 한정하고 있는 것처럼 통신사실확인자료 제공 대상범죄를 한정하고, 구체적인 범죄혐의 또는 해당사건과의 관련성을 소명하도록 할 필요가 있다. 나아가 가령 사실관계의 조사 등이 다른 방법으로는 현저히 곤란하거나 불가능한 경우 등에 한하여 이를 활용할 수 있도록 하는 등 보충성의 요건을 강화해야 할 것이다. 또한 통신사실확인자료 제공 대상자 범위에 제한이 없어 통신사실확인자료 대상범위가 피의자·피내사자뿐만 아니라 관련자까지 무한히 확대될 우려가 있으므로, 피의자, 계정소유자 등으로 대상을 한정함으로써 증인, 참고인, 피해자 등으로 대상범위가 과도하게 확대되는 것을 제한할 필요가 있다.

특히 수사기관의 실시간 위치정보 추적자료 제공 요청과 관련해 헌법재판소는 "① 수사기관이 전기통신사업자로부터 실시간 위치정보 추적자료를 제공받는 경우 또는 불특정 다수에 대한 위치정보 추적자료를 제공받는 경우에는 수사의 필요성뿐만 아니라 보충성이 있을 때, 즉 다른 방법으로는 범죄 실행을 저지하거나 범인의 발견·확보 또는 증거의 수집·보전이 어려운 경우에 한하여, 수사기관이 위치정보 추적자료의 제공을 요청할 수 있게 하는 방법, ② 통신비밀보호법 제5조 제1항에 규정된 통신제한조치가 가능한 범죄 이외의 범죄와 관련해서는 수사의 필요성뿐만 아니라 보충성이 있는 경우에 한하여 수사기관이 위치정보 추적자료의 제공을 요청할 수 있도록 하는 방법 등"이 개선입법으로 고려될 수 있다고 판시하였다.[92)]

기지국 수사의 경우에는 피의자를 특정하지 않고 특정 기지국에 접속한 모든 사람의 통신사실확인자료를 일괄해서 받는 것이므로, 대상 범죄를 중범죄로 제한하고 기지국 수사를 불가피하게 허용할 수밖에 없는 실질적인 요건을 구체화할 필요가 있다. 헌법재판소는 "기지국 수사의 허용과 관련하여서는, ① 유괴, 납치, 성폭력범죄 등 강력범죄나 국가안보를 위협하는 각종 범죄와 같이 피해자나 피의자의 통신사실 확인자료가 반드시 필요한 범죄로 그 대상을 한정하는 방안, ② 위 중요 범죄와 더불어 통신을 수단으로 하는 범죄 일반을 포함시키는 방안, ③ 위 요건에 더하여 다른 방법으로는 범죄수사가 어려운 경우(보충성)를 요건으로 추가하거나, 또는 위 중요 범죄 이외의 경우에만 보충성을 요건으로 추가하는 방안, ④ 1건의 허가서로 불특정 다수인에 대한 통신사실 확인자료 제공요청을 못하도록 하는 방안 등을 독립적 또는 중첩적으로 검토함으로써, 수사에 지장을 초래하지 않으면서도 불특정 다수의 기본권을 덜 침해하는 수단이 존재한다"고 하였다.[93)]

한편 통신제한조치 제도와 같이 통신사실확인자료 제공 제도는 법원의 사후적 통제절차에 대한 어떠한 규정도 갖고 있지 않다는 문제점을 갖고 있다. 즉 현행 「통신비밀보호법」상의 구조에 따르면, 법원은 통신사실확인자료 허가서 발부 이외에는 어떠한 통제권한이나 수단도 갖고 있지 않다. 따라서 영장주의의 실질화라는 측면에서 본다면 법원이 통신사실확인자료 제공 요청의 허가 단계에서뿐만 아니라 그 이후의 집행과정 그리고 종료 후에도 관여할 수 있는 수단이나 절차를 마련하는 것이 필요하다.

2) 사후통지 제도 개선

현행 「통신비밀보호법」은 통신제한조치와 마찬가지로 통신사실확인자료 대상자에 대한 사후통지만 규정하고 있고 사전통지는 규정하고 있지 않다. 게다가 사후통지의 경우에도 통신사실확인자료가 제공된 날이 아닌 통신사실확인자료를 제공한 사건에 관한 처분을 한 날을 기준으로

92) 헌재 2018. 6. 28. 2012헌마191 등, 통신비밀보호법 제2조 제11호 바목 등 위헌확인 등.
93) 헌재 2018. 6. 28. 2012헌마538, 통신비밀보호법 제13조 제1항 위헌확인 등.

통지를 하고 있어 문제이다. 또한 수사기관이 통지를 하는 경우에도 그 사유에 대해서는 통지하지 아니할 수 있도록 함으로써 정보주체는 수사기관으로부터 사후통지를 받더라도 자신이 어떠한 사유로 통신사실확인자료 제공을 당했는지 짐작할 수도 없다.
헌법재판소는 2018. 6. 28. 선고 2012헌마191 결정에서"사전에 정보주체인 피의자 등에게 이를 통지하는 것은 수사의 밀행성 확보를 위하여 허용될 수 없다 하더라도, 수사기관이 전기통신사업자로부터 위치정보 추적자료를 제공받은 다음에는 수사에 지장이 되지 아니하는 한 그 제공사실 등을 정보주체인 피의자 등에게 통지해야 한다"고 판시하였다. 따라서 사후통지 기간을 '제공 받은 날로부터 30일 이내' 또는 보다 단기간으로 정해 최대한 빨리 통지를 하도록 제도를 개선해야 할 것이다. 그리고 통신사실확인자료 제공 통지 내용에는 요청사유 영장에 기재된 죄명 및 적용법조 등을 포함하는 것이 바람직하다.
또한 통지유예 제도를 두고 있는데, 유예 기간을 한정하고 있지 않고 관할 지방검찰청 검사장 등 수사기관의 승인으로 유예를 할 수 있어 사실상 무기한 통지유예가 이루어질 수 있다. 이는 적법절차 원칙 위반이며, 정보주체의 기본권 보호와 방어권 보장 측면에서 바람직하지 않다. 통지유예에 대해서 적정한 통지유예 기간을 정하고 이를 초과할 경우 법원의 허가를 받게 하고, 통지유예 결정도 법원의 허가를 받도록 하여 남용의 가능성을 최소화하는 개선이 필요하다. 그리고 통신제한조치와 달리 통지의무 위반에 대해 아무런 제재를 하고 있지 않아 통지제도의 실효성을 위한 제재 규정 신설이 필요하다.

3) 통신사실확인자료 보관 의무 폐지

2014년 유럽사법재판소는 「통신정보보관지침」에 대해 무효 판결을 내렸다. 그런데 우리나라에서는 「통신비밀보호법」 제15조의2 전기통신사업자의 협조 의무 조항 및 시행령을 통해 통신사실확인자료의 일정기간 보관을 의무화하고 있다. 이에 따라 범죄혐의와 상관없이, 전기통신사업자의 서비스 제공 목적과 무관하게 모든 사용자의 통신사실확인자료가 단지 수사의 필요성 때문에 보관되고 있는데, 이는 개인정보 보호원칙에 벗어날 뿐만 아니라 무죄추정의 원칙에도 어긋나는 것이다. 단지 수사의 편의를 위해서 통신사실확인자료의 일정기간 보관을 의무화하는 제도는 폐지될 필요가 있다.

2. 통신자료 제공 제도 개선

통신자료 제공에 대해서는 영장주의를 적용하고 적법절차 원칙에 따르는 개선이 필요하다. 특히 통신자료에는 주민등록번호가 포함되는데, 오늘날 주민등록번호는 단순히 식별 및 인증기능에 그치지 않고 다른 개인정보에 접근하기 위한 핵심 연결자 역할을 하고 있으므로 주민등록번호의 제공은 매우 엄격하게 규제되어야 할 것이다. 또한 법체계상 통신자료 요청제도로 인한 기본권 제한의 본질은 '이용자의 통신의 비밀'이므로 이를 제한하는 내용은 「전기통신사업법」이 아닌 「통신비밀보호법」에서 규율해야 한다. 전술한 바와 같이 국가인권위원회도 2014년의 의견표명에서 「전기통신사업법」 제83조 제3항을 삭제할 것을 권고한 바 있다.
먼저 통신자료 요청제도의 대상인 통신자료도 엄연히 통신의 비밀의 보호대상이 된다는 점에서, 통신자료 제공 제도만을 영장주의의 예외로 설정해야 할 이유가 존재하지 않는다. 따라서 통신자료 제공 제도에 대해서도 통신의 비밀 보호라는 기본권 강화의 관점에서 영장주의가 적

용되도록 법제도를 개선하는 것이 필요하다. 그리고 통신자료는 이용자의 개인정보이며, 개인정보를 대상으로 한 조사、수집、보관、처리、이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다. 따라서 통신자료 요청 및 제공이 통신자료의 주체인 이용자의 의사와 상관없이 이루어지고 있다는 것은 이용자의 개인정보자기결정권을 형해화시킬 수 있다. 다만 통신자료에 적용되는 영장주의의 '수준'을 어떻게 설정할 것인가의 문제가 있을 수 있는데, 기본권의 제한이라는 점에서 최소한 형사소송법상의 압수·수색에 적용되는 영장주의는 반드시 적용되어야 할 것이다.

그리고 헌법상 적법절차의 원칙은 형사절차뿐만 아니라 모든 국가작용 전반에 적용되는 것으로, 이로부터 당사자에 대한 적절한 고지, 의견 및 자료제출 기회 부여와 같은 중요한 절차적 요청이 도출된다. 통지 제도는 국가기관의 강제처분에 관하여 당사자에게 적절한 고지를 행함으로써 정보주체의 기본권 보호와 방어권 보장에 기여한다. 그런데 통신자료 제공 제도는 통신자료 요청 및 제공이 이용자의 의사와 상관없이 이루어지고 있고, 이용자가 전기통신사업자에 의한 통신자료 제공을 저지하기 위해 그 과정에 사전 개입할 수 있는 절차가 전혀 없으며, 사후적으로도 통지를 받지 못하고 있다는 점에서 적법절차 원칙에 전혀 부합하지 못하고 있어 개선이 필요하다.

3. 디지털 증거 압수·수색 제도 개선

「형사소송법」상 디지털 증거의 압수·수색에 대해서는 최근 판례가 중요한 방향을 제시해준다. 대법원은 2015. 7. 16. 자 2011모1839 전원합의체 결정에서 기존의 전자정보 압수수색의 원칙을 확인하고, "수사기관 사무실 등으로 반출된 저장매체 또는 복제본에서 혐의사실 관련성에 대한 구분 없이 임의로 저장된 전자정보를 문서로 출력하거나 파일로 복제하는 행위는 원칙적으로 영장주의 원칙에 반하는 위법한 압수가 된다"고 하면서, "저장매체에 대한 압수·수색 과정에서 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란한 예외적인 사정이 인정되어 전자정보가 담긴 저장매체 또는 하드카피나 이미징 등 형태(이하 '복제본'이라 한다)를 수사기관 사무실 등으로 옮겨 복제·탐색·출력하는 경우에도, 그와 같은 일련의 과정에서 형사소송법 제219조, 제121조에서 규정하는 피압수·수색 당사자(이하 '피압수자'라 한다)나 변호인에게 참여의 기회를 보장하고 혐의사실과 무관한 전자정보의 임의적인 복제 등을 막기 위한 적절한 조치를 취하는 등 영장주의 원칙과 적법절차를 준수하여야 한다"고 밝혔다. 한편"전자정보에 대한 압수·수색이 종료되기 전에 혐의사실과 관련된 전자정보를 적법하게 탐색하는 과정에서 별도의 범죄혐의와 관련된 전자정보를 우연히 발견한 경우라면, 수사기관으로서는 더 이상의 추가 탐색을 중단하고 법원으로부터 별도의 범죄혐의에 대한 압수·수색영장을 발부받은 경우에 한하여 그러한 정보에 대하여도 적법하게 압수·수색을 할 수 있다고 할 것"이라고 하였다.

대법원의 이러한 판시를 법제화하기 위해서 「형사소송법」에 디지털 증거의 압수·수색에 관한 조항을 별도로 신설하는 방안을 고려해볼 수 있다. 그리고 추가적으로 압수된 디지털 증거에 대한 환부 및 폐기 의무, 방법, 절차 등 마련하고, 디지털 압수・수색에 대한 수사기관의 사후통지의무 제도를 도입하고, 임의제출이나 압수수색 영장의 발부 없이 또는 별건 영장에 의하여 수집된 경우에는 절차적 위법이 명백할 경우 증거능력에 제한을 두거나 디지털 증거 압수・수색 영장 실질심사 제도의 도입을 검토해 볼 필요가 있다.

또한「통신비밀보호법」제9조의3에 규정된 전기통신에 대한 압수·수색·검증의 집행에 관한 통지도 통신제한조치 및 통신사실확인자료 제공에 관한 통지와 동일한 문제점을 가지고 있으므로, 통지의 시기 및 통지의 내용 등을 개선해야 한다.

4. 정보수사기관 개혁

국정원과 경찰, 기무사(현 군사안보지원사령부) 등 정보수사기관들이 지난 정권에서 국내 정치 개입, 민간인 사찰 등 불법 활동을 벌여온 사실이 밝혀지고 그 수장들이 구속되고 사법처리되는 일이 반복되고 있다. 이에 시민사회단체들은 정보수사기관에 대한 개혁의 목소리를 높이고 있다. 2017년 9월 참여연대, 민들레-국가폭력피해자와 함께하는 사람들, 민주사회를 위한 변호사모임, 민주주의법학연구회, 진보네트워크센터, 천주교인권위원회, 한국진보연대 등 시민사회단체들과 함께 구성한 <국정원감시네트워크>는 정책의견서를 발표하고 국정원 개혁방안을 제시했다. 그리고 2019년 9월에는 인권·시민사회단체들이 정보경찰폐지인권시민사회단체네트워크('정보경찰폐지넷')를 발족하고 정보경찰 폐지를 위해 활동해 나갈 것을 밝혔다. 정보경찰폐지넷은 정보경찰이 저지른 불법행위, 경찰의 정보수집 활동에 대한 법과 제도의 근거부족, 정보경찰의 인권침해 및 정보왜곡 등을 상세히 지적하고 한 목소리로 정보경찰 폐지를 촉구하고 있다.

이에 따르면 국정원 개혁을 위해서는「국정원법」제3조 제1항 제1호에 명시된 국정원의 정보수집 권한 부분을 개정하여 국정원의 국내정보 수집 권한을 폐지하고, 국정원의 범죄 수사권을 다른 일반 수사기관으로 이관해야 한다. 군사안보지원사령부의 권한에 대해서도 같은 수준의 개혁이 필요하다. 경찰 개혁을 위해서는 정보경찰의 폐지와 정보국 축소, 유관부처의 업무 이관 등이 논의되고 있다. 또한 정보수사기관에 대한 감독과 통제 강화 방안을 마련해야 한다.

그리고 국정원에 국민사찰 권한을 지나치게 광범위하고 포괄적으로 제공하고 있는 테러방지법의 폐지 또는 전면적인 개정이 필요하다. 테러방지법 제2조 정의 규정에서 "테러위험인물"은 대단히 포괄적으로 규정되어 있고, "대테러조사"는 단순한 비구속적 행정조사의 수준을 넘어서는 거의 강제적·구속적인 행정조사의 수준에 들어가는 것을 의미하여 헌법상 영장주의에 위반되며, 제9조(테러위험인물에 대한 정보 수집 등)는 국정원에 매우 광범위한 정보 수집 권한을 부여하고 있어 심각한 인권침해가 우려된다.

5. 사인간 감시 문제

신기술을 매개한 노동 감시를 체계적으로 통제할 수 있는 법제 마련이 필요하다. 한편으로, 작업장 내 혹은 플랫폼 노동 등 불완전 노동 환경에서 발생하는 지능화된 노동감시를 규제하기 위한 법제와 이에 대한 감독 시스템이 마련될 필요도 있다. 그리고 사인간 통신 감시를 강제하는 청소년스마트폰감시법과 같은 제도는 폐지되어야 한다.

제3절 온라인에서의 표현의 자유 보호 현황과 쟁점

1. 온라인에서의 표현의 자유의 의의와 제한

(1) 일반적인 표현의 자유의 의의와 제한 원리

민주주의 국가에서 '표현의 자유'가 갖는 의미는 특히 중요하다. 표현의 자유는 자유로운 인격발현의 수단임과 동시에 합리적이고 건설적인 의사형성 및 진리발견의 수단이며, 민주주의 국가의 존립과 발전에 필수불가결한 기본권으로, 다른 기본권에 비하여 고양된 보호를 받는다. 물론 표현의 자유도 다른 기본권과 마찬가지로 헌법 제37조 제2항에 따라 '국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우'에 제한될 수 있으며, 특히 헌법 제21조 제4항의 "언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니 된다."는 규정에 따라 제한될 수도 있다. 그러나 표현의 자유의 중요성 및 표현행위로 인한 해악은 물리적 행위로 인한 것과 달리 비가시적이라는 특성 때문에, 표현의 자유를 제한하는 제도는 '명확성 원칙'이나 '명백하고 현존하는 위험의 원칙'과 같이 더욱 엄격한 요건을 충족할 것이 요구된다.

법률은 되도록 명확한 용어로 규정하여야 한다는 명확성의 원칙은 민주주의·법치주의 원리의 표현으로서 모든 기본권제한입법에 요구되는 것이나, 표현의 자유를 규제하는 입법에 있어서는 더욱 중요한 의미를 지닌다. 현대 민주사회에서 표현의 자유가 국민주권주의 이념의 실현에 불가결한 것인 점에 비추어 볼 때, 불명확한 규범에 의한 표현의 자유의 규제는 헌법상 보호받는 표현에 대한 위축효과를 수반하고, 그로 인해 다양한 의견, 견해, 사상의 표출을 가능케 하여 이러한 표현들이 상호 검증을 거치도록 한다는 표현의 자유의 본래의 기능을 상실케 한다. 즉, 무엇이 금지되는 표현인지가 불명확한 경우에, 자신이 행하고자 하는 표현이 규제의 대상이 아니라는 확신이 없는 기본권주체는 대체로 규제를 받을 것을 우려해서 표현행위를 스스로 억제하게 될 가능성이 높은 것이다. 그렇기 때문에 표현의 자유를 규제하는 법률은 규제되는 표현의 개념을 세밀하고 명확하게 규정할 것이 헌법적으로 요구된다.[94)]

또한 표현행위로 인한 해악의 결과란 추상적이기 때문에 판단자의 자의에 따라 제한 여부가 남용될 수 있다. 따라서 표현 행위가 장래에 있어 국가나 사회에 단지 해로운 결과를 가져올 수 있다는 추상적 해악의 발생 가능성만을 이유로 제한해서는 안 되고, 법률에 의하여 금지된 해악을 초래할 명백하고도 현실적인 위험성이 입증된 경우에 한정되어야 한다는 것이 바로 명백하고도 현존하는 위험의 원칙이다.

---

94) 헌재 2010. 12. 28. 2008헌바157 등 참조.

(2) 온라인상 표현의 자유의 제한 유형

오늘날 대부분의 소통행위와 표현행위는 온라인에서 이루어지고 있다. 공간이 옮겨졌을 뿐, 온라인에서의 표현의 자유 역시 오프라인과 마찬가지로 중요한 기본권으로 보장되어야 하며, 엄격한 제한 원리가 적용되어야 함이 원칙이다. 그러나 한편, 인터넷은 기존의 물리적 형태의 매체와 현격히 다른 특성을 가진 매체임에는 틀림없다.

헌법재판소는 「공직선거법」상 인터넷 선거운동 금지 조항 위헌확인 사건[95]에서 다음과 같이 판시한바 있다. "이러한 논란은, 인터넷이라는 매체가 이 사건 법률조항이 최초로 도입될 당시에는 전혀 예상하지 못했던 새로운 매체일 뿐만 아니라, 이 사건 금지조항에서 예시하고 있는 기존 오프라인 시대의 의사전달 매체들과는 뚜렷이 대비되는 특성을 지니고 있기 때문이다. (…) 이 사건 금지조항에서 예시하고 있는 광고, 인사장, 벽보, 사진, 문서·도화, 인쇄물이나 녹음·녹화테이프는 모두 그 작성 내지 제작·배포에 상당한 비용과 노력이 소요되고, 이를 이용한 정보의 전달 및 수용도 일방적·수동적으로 이루어지므로, 후보자(또는 후보자가 되고자 하는 자)나 그와 직접 관련된 자 이외의 일반유권자가 위와 같은 매체를 이용하여 정치적 의사표현을 하거나 선거운동을 하는 경우를 상정하기가 쉽지 않고, 이를 제한 없이 허용할 경우 후보자간 경제력 차이에 따른 폐해가 발생할 위험성이 높으며, 전달매체에 자체적인 정보 교정의 가능성도 없다고 할 수 있다. (…) 그 반면, 인터넷은 개방성, 상호작용성, 탈중앙통제성, 접근의 용이성, 다양성 등을 기본으로 하는 사상의 자유시장에 가장 근접한 매체이다. 즉, 인터넷은 저렴한 비용으로 누구나 손쉽게 접근이 가능하고 가장 참여적인 매체로서, 표현의 쌍방향성이 보장되고, 정보의 제공을 통한 의사표현 뿐 아니라 정보의 수령, 취득에 있어서도 좀 더 능동적이고 의도적인 행동이 필요하다는 특성을 지니므로, 일반유권자도 인터넷 상에서 정치적 의사표현이나 선거운동을 하고자 할 개연성이 높고, 경제력 차이에 따른 선거의 공정성 훼손이라는 폐해가 나타날 가능성이 현저히 낮으며, 매체 자체에서 잘못된 정보에 대한 반론과 토론, 교정이 이루어질 수 있고, 국가의 개입이 없이 커뮤니케이션과 정보의 다양성이 확보될 수 있다는 점에서 확연히 대비된다. (…) 그리고 이러한 특성으로 인하여, 인터넷은 국민주권의 실현 및 민주주의의 강화에 유용한 수단인 동시에 '기회의 균형성, 투명성, 저비용성의 제고'라는 선거운동 규제의 목적 달성에도 기여할 수 있는 매체로 평가받고 있다고 할 수 있다."[96]

한편, 일명 '불온통신'을 규제한 「전기통신사업법」에 대한 위헌확인 사건[97]에서는 "불온통신 규제의 주된 대상이 되는 매체의 하나는 인터넷이다. 인터넷은 공중파방송과 달리 '가장 참여적인 시장', '표현촉진적인 매체'이다. 공중파방송은 전파자원의 희소성, 방송의 침투성, 정보수용자측의 통제능력의 결여와 같은 특성을 가지고 있어서 그 공적 책임과 공익성이 강조되어, 인쇄매체에서는 볼 수 없는 강한 규제조치가 정당화되기도 한다. 그러나 인터넷은 위와 같은 방송의 특성이 없으며, 오히려 진입장벽이 낮고, 표현의 쌍방향성이 보장되며, 그 이용에 적극적이고 계획적인 행동이 필요하다는 특성을 지닌다. 오늘날가장거대하고, 주요한 표현매체의 하나로 자리를 굳힌 인터넷상의 표현에 대하여 질서위주의 사고만으로 규제하려고 할 경우 표현의 자유의 발전에 큰 장애를 초래할 수 있다. 표현매체에 관한 기술의 발달은 표현의

---

95) 헌재 2011. 12. 29. 2007헌마1001 등, 공직선거법 제93조 제1항 등 위헌확인(한정위헌).
96) 헌재 2011. 12. 29. 2007헌마1001 등, 판례집 23-2하, 739, 754-755.
97) 헌재 2002. 6. 27. 99헌마480, 전기통신사업법 제53조 등 위헌확인(위헌,각하).

자유의 장을 넓히고 질적 변화를 야기하고 있으므로 계속 변화하는 이 분야에서 규제의 수단 또한 헌법의 틀 내에서 다채롭고 새롭게 강구되어야 할 것이다"고 판시하였다.[98]
이렇듯 표현의 자유의 발전에 있어 인터넷의 의미를 높이 평가한 결정례도 있지만, 보통 인터넷의 매체적 특수성은 온라인상 표현물 규제의 정당화 논거로 사용되는 경우가 더욱 많다. 예컨대 "인터넷 등 정보통신망에서의 정보의 빠른 전파력과 광범위한 파급효로 인하여 사람의 명예는 과거와 비교할 수 없을 정도로 심각하게 훼손되고, 그 피해의 회복 또한 쉽지 않게 된다."[99], "인터넷 등 정보통신망이 갖는 익명성과 비대면성, 빠른 전파가능성으로 말미암아 표현에 대한 반론과 토론을 통한 자정작용이 사실상 무의미한 경우도 적지 않고, 신상털기 등 타인의 인격 파괴에 대한 최소한의 감정적·이성적 배려마저도 상실한 채 개인에 대한 정보가 무차별적으로 살포될 가능성이 있으며, 이로 인하여 한 개인의 인격을 형해화시키고 회복불능의 상황으로 몰아갈 위험 또한 존재한다.",[100] "전기통신회선을 통해 유통되는 정보, 특히 인터넷을 통해 유통되는 정보는 종전의 고전적인 통신수단과는 비교할 수 없을 정도의 복제성, 확장성, 신속성을 가지고 유통되기 때문에 불법정보에 대하여 신속하게 적절한 조치를 취하지 않으면 그로 인해 발생할 수 있는 개인적 피해와 사회적 혼란 등을 사후적으로 회복하기란 사실상 불가능에 가깝다."[101] 등의 헌법재판소의 판시가 그러하다.
이러한 인터넷 매체의 특수성으로 인하여 유포자에 대한 형사처벌을 넘어 인터넷상 정보의 '유통' 자체를 예방, 차단하는 방식의 규제가 많이 도입되어 있다. 이러한 온라인상 표현물 규제는 크게 ① 국가기관이 주체가 되어 온라인상 표현물을 심의하고 삭제·차단 명령을 내리는 방식, ② 정보통신서비스제공자(인터넷상의 정보매개자, Online Service Provider)에 대한 정보 관리 책임 부과, ③ 온라인 실명제 등으로 나타난다.

2. 국제 동향 및 기준[102]

(1) UN 자유권규약위원회 표현의 자유에 대한 일반논평 34호

UN 자유권규약위원회 표현의 자유에 대한 일반논평 34호(General comment No. 34)[103]는 UN의 「시민적·정치적 권리에 관한 국제규약」(International Covenant on Civil and Political Rights, 이하 '자유권규약(ICCPR)'라 한다)의 이행여부를 감시하고 집행하는 유엔 자유권규약위원회(The UN Human Rights Committee, 이하 '위원회'라 한다)가 동 규약 19조(표현의 자유)에 관하여 발표한 일반논평이다. 일반논평이란 국제인권조약의 조문을 유권해석한 것을 말한다. 일반논평 34호는 표현의 자유가 인권의 증진과 보호에 필수적인 투명성과 책임성의 원리를 실현하는데 필수적임을 밝히고 있다. 주요 내용은 다음과 같다.
공적인 사안에 대하여 미디어가 검열이나 제한 없이 자유롭게 공적인 견해를 표명할 수 있어

98) 헌재 2002. 6. 27. 99헌마480, 판례집 14-1, 616, 632.
99) 헌재 2016. 2. 25. 2013헌바105 등, 판례집 28-1상, 26, 34.
100) 헌재 2016. 2. 25. 2013헌바105 등, 판례집 28-1상, 26, 35.
101) 헌재 2012. 2. 23. 2011헌가13, 판례집 24-1상, 25, 39.
102) 이하 박경신·손지원, 『디지털인권 보장을 위한 법제도 개선 및 정책방안』, 국민정책연구원, 2017. 3. 참조.
251) UN Human Rights Committee, "International Covenant on Civil and Political Rights, General comment No. 34" (CCPR/C/GC/34), 12 September 2011.

야 한다(13항). 표현의 자유의 제한은 타인의 권리 존중이나, 국가안보, 공공질서를 이유로 한 표현의 자유를 제한하는 경우에도 권리 그 자체의 행사에 위협이 되게 해서는 안 된다고 하며, 그 원칙과 예외가 서로 뒤바뀌는 방향으로 운영되어서는 안 되며, 반드시 그 제한이 공익의 목적을 달성하는데 필수적이며 비례하여 행사되었는지 엄격하게 심사해야 한다는 헌법상의 일반원칙을 재확인하고 있다(21항). 또한 표현의 자유를 제한하는 법률이 있다고 하더라도 그 제한에 있어서 법률에 절대적인 재량을 부여하는 것은 아니며 법률에서 제한될 수 있는 표현의 영역을 상세하게 규정해야 하며(25항), 제한의 내용적인 요건으로 특정화, 개별화된 직접적, 즉각적인 위협의 수준에 이르러야 그 표현의 자유를 제한할 수 있다고 명시하고 있다(35항). 또한 공공의 인물이 단순히 모욕을 받고 있다는 사실만으로 처벌이 정당화 되지 아니하며, 공공의 인물은 비판과 정치적인 반대의 당연한 대상이 되기에 명예훼손을 이유로 한 형사처벌이 이루어져서는 안 된다는 원칙 또한 확인하고 있다(38항). 그리고 해악 없이 과실로 행한 허위의 진술, 공익성을 근거로 한 진술에 대해서는 명예훼손처벌의 방어요건이 되어야 한다는 원칙적인 점 또한 확인하고 있다. 무엇보다도 국가가 명예훼손의 비범죄화를 고려하여야 함을 명시하고 있다(47항).

(2) UN 표현의 자유 특별보고관 라 뤼의 한국보고서

자유권규약(ICCPR)을 반영하는 또 하나의 중요한 문헌은 유엔 인권이사회(UN Human Rights Council)가 임명하고 유엔 총회에 보고하는 표현의 자유 특별보고관의 보고서(Report of Special Rapporteur on Freedom of Expression)이다. 2010년 5월 유엔 특별보고관 프랑크 라 뤼(Frank La Rue)는 의사·표현의 자유에 대한 권리의 증진과 보호에 관한 실태 조사를 위해 대한민국을 공식 방문하였고, 이에 대한 보고서[104](이하 '라 뤼 한국보고서')를 발표하였다. 이 보고서는 대한민국의 정치적, 역사적 배경을 대략적으로 기술하고 의사·표현의 자유권에 대한 국제법 기준과 국내법 기반을 전반적으로 설명하고 있다. 본 보고서에는 명예훼손은 허위일 경우에 성립한다는 점[105], 명예훼손 형사처벌 폐지 권고[106], 인터넷 임시조치제도 및 방송통신심의위원회에 의한 통신심의제도 폐지를 권고하는 내용[107][108] 등이 있다.

---

104) Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mission to the Republic of Korea"(A/HRC/17/27/Add.2), UN Human Rights Council, 21 March 2011.

105) Frank La Rue, op. cit. : "27. The Special Rapporteur reiterates that for a statement to be considered defamatory, it must be false, must injure another person''s reputation, and made with malicious intent to cause injury to another individual''s reputation."

106) Frank La Rue, op. cit. : "89. The Government should, in line with the global trend, remove defamation as a criminal offence from the Criminal Act, given the existing prohibition of defamation in the Civil Act."

107) Frank La Rue, op. cit. : "92. The Special Rapporteur is concerned about the vague condition and scope of liability of intermediaries as prescribed in article 44-2(6) of the Network Act, which may lead to excessive regulation of online content. The Special Rapporteur recommends that the Government repeal all provisions relating to intermediary liability."

108) Frank La Rue, op. cit. : "93. The Special Rapporteur is also concerned that there are insufficient safeguards to ensure that the KCSC does not operate as a de facto post-publication censorship body to delete information critical of the Government on the grounds of violating the Network Act. In accordance with the decision adopted by the NHRCK on 30 September 2010, the Special Rapporteur recommends the current functions of the KCSC be transferred to an independent body which is free from any political,

(3) 유럽평의회의 인터넷에서 커뮤니케이션의 자유를 위한 7원칙

유럽평의회(Council of Europe)의 각료위원회(Committee of Minister)는 2003년 5월 28일 위 「유럽인권협약」 제10조에 근거해서 「인터넷에서의 커뮤니케이션의 자유에 관한 선언(Declaration on Freedom of Communication on the Internet)」[109]을 제정하여 회원국들이 준수해야 할 7개 원칙을 선언하였다. 그 내용은 다음과 같다.

- 제1원칙 (인터넷에서의 내용규제) : 회원국들은 인터넷에서의 정보내용(content)에 대하여 다른 정보전달수단에 적용되는 것 이상의 제한을 가하여서는 아니 된다.
- 제2원칙 (자율규제 혹은 상호적 규제) : 회원국들은 인터넷에서 유통되는 정보내용에 관하여 자율규제(self-regulation) 혹은 상호적 규제(co-regulation)를 촉진하여야 한다.
- 제3원칙 (사전국가통제의 부재) : 공권력은, 포괄적인 차단조치나 여과조치를 통하여, 일반대중이 국경을 불문하고 인터넷에서의 정보 및 기타의 커뮤니케이션에 접근하는 것을 막아서는 아니 된다. 이 원칙은 청소년을 보호하기 위하여 특히 학교나 도서관과 같이 그들에게 접근이 허용되는 장소에서 여과장치를 설치하는 것을 막는 것은 아니다.

  「유럽인권협약」 제10조 제2항의 안전조건이 존중된다는 전제 위에서, 만일 권한 있는 국가기관이 인터넷 정보내용의 불법성(illegality)에 대하여 잠정적이거나 종국적인 결정을 내린다면, 명백하게 신원을 확인할 수 있는 인터넷 정보내용을 삭제하거나 또는 그 대안으로 그것에의 접근을 차단할 수 있는 조치를 취할 수 있다.
- 제4원칙 (정보사회에서 개인의 참여를 억제하는 장애의 제거) : 회원국들은 모든 사람이 감당할 수 있는 적정한 가격으로 차별 없이 인터넷 커뮤니케이션 및 정보서비스에 접근하는 것을 촉진하고 장려하여야 한다. 더 나아가, 일반대중이 예컨대 개인 웹사이트를 설치·운영함으로써 적극적으로 참여하는 것에 대하여 어떤 형태의 허가제도 허용되지 않으며 또는 그와 유사한 효과를 가지는 요건을 설정해서도 아니 된다.
- 제5원칙 (인터넷을 통한 서비스 제공의 자유) : 인터넷을 통한 서비스의 제공에 대하여는 사용된 전송수단을 유일한 이유로 하는 특별인가제가 적용되어서는 아니 된다. 회원국들은 이용자 및 사회집단들의 여러 요구(needs)에 부응하는 인터넷을 통한 서비스가 다양하게 제공될 수 있도록 촉진하는 조치들을 강구하여야 한다. 서비스제공자들은 국가적 및 국제적 통신네트워크에의 차별 없는 접근을 보장하는 규제체계 속에서 서비스를 운영할 수 있도록 허용되어져야 한다.
- 제6원칙 (인터넷 정보내용에 대한 서비스제공자의 책임 제한) : 회원국들은 서비스제공자들에게 그들이 액세스를 제공하거나 전송 또는 저장하는 인터넷 정보내용에 대하여 전반적인 모니터를 할 의무를 지워서는 아니 되며, 불법적인 행위(illegal activity)를 가리키는 사실이나 상황을 적극적으로 찾아내는 의무를 부과해서도 아니 된다.

  회원국들은 서비스제공자들이 국내법이 규정하는 바에 따라 정보를 전달하거나 인터넷에의 접근을 제공하는 데에 그들의 기능이 한정되어 있는 때에는 인터넷에서의 정보내용(content)에 대해 책임을 지지 않는다는 점을 보증하여야 한다.

---

commercial, or other unwarranted influences with adequate safeguards against abuse, including judicial review."

109) https://wcd.coe.int/ViewDoc.jsp?id=37031 (2019.11.13. 최종접속)

서비스제공자들의 기능이 그보다 더 넓고 그리고 그들이 다른 당사자에게서 나온 정보 내용을 저장하고 있는 경우에, 만일 서비스제공자들이 문제의 정보나 서비스가 국내법이 규정하는 바에 따라 불법이라는 점을 인식한 시점으로부터, 또는 손배배상청구가 있는 상황에서 문제의 행위나 정보의 불법성을 드러내는 사실이나 정황을 인식한 시점으로부터, 신속하게 그 정보나 서비스를 삭제하거나 차단하는 조치를 취하지 않은 경우, 회원국들은 그들에게 공동책임을 지울 수 있다.

위의 항이 규정하는 바의 서비스제공자의 의무를 국내법에서 구체화함에 있어서, 우선적으로 그 정보를 유통시킨 사람들의 표현의 자유(freedom of expression)를, 나아가 이용자들이 그 정보에 응답하는 권리(the corresponding right of users to the information)를 존중하기 위한 세심한 주의가 기울여져야 한다.

모든 경우에, 위에서 언급한 책임의 제한은, 법위반상태를 가능한 한 종료시키거나 예방하기 위하여 서비스제공자들을 대상으로 한 법원의 강제명령(injunctions)이 발하여질 수 있다는 점에 대해서는 영향을 미치지 아니한다.

- 제7원칙 (익명성) : 온라인감시(online surveillance)를 받지 않는다는 보장을 확실히 하기 위하여 그리고 정보와 사상의 자유로운 유통을 강화하기 위하여, 회원국들은 자신들의 신원(identity)을 공개하지 않으려는 인터넷 이용자들의 의사를 존중하여야 한다. 이 원칙은 회원국들이 국내법, 유럽인권협약, 기타 사법과 경찰 분야의 국제협정에 따라 범죄행위에 책임이 있는 자들을 추적하기 위하여 조치를 취하고 협력하는 것을 막는 것은 아니다.

(4) UN 표현의 자유 특별보고관 데이비드 케이의 기업 책임에 대한 보고서

UN 표현의 자유 특별보고관 데이비드 케이(David Kaye)가 제32차 유엔 인권이사회를 맞아 발표한 디지털시대 표현의 자유와 민간기업에 대한 보고서[110]이다. 지구적인 플랫폼을 보유한 민간기업들이 국가의 검열과 감시를 대행하면서 이용자들의 표현의 자유에 미치는 영향력을 비판적으로 고찰하면서, 정부, 기업, 국제기구가 견지해야 할 일반적인 원칙에 대해서 권고하고 있다. 여기서 다음의 내용이 특히 주목을 끌고 있다.

> "85. 정부는 표현의 자유를 행사할 수 있도록 인권을 보호하고 존중할 기본적인 책임을 진다. 정보통신기술과 관련해서 이는 정부가 민간기업에 대하여 법률, 정책, 법외적 수단 등으로 표현의 자유에 대한 필수적이거나 비례적이지 않은 간섭을 행하는 조치를 요구하거나 압력을 가해서는 안 된다는 의미이다. 디지털 통신내용을 삭제하거나 이용자 정보에 접근할 수 있는 요구, 요청, 조치들은 정당한 제정 법률에 기반해야 하며, 독립적인 외부기관의 감독을 받아야 하고, 자유권규약 19조 3항에 명시된 목적들을 달성하기 위해 사용되는 수단으로서 필수성과 비례성을 입증할 수 있어야 한다. 특히 민간기업 규제와 관련해서 정부의 법률과 정책들은 투명하게 채택되고 실행되어야 한다."

110) UN Human Rights Council, "Report of the Special Rapporteur on the promotion andprotection of the right to freedom of opinion and expression" (A/HRC/32/38), 11 May 2016.

(5) 정보매개자 책임에 관한 마닐라 원칙

마닐라원칙[111]은 세계 각국의 정보인권단체들이 만든 정보매개자책임에 대한 국제 원칙이다. 인터넷상 모든 소통은 인터넷사업자, SNS, 검색엔진 등 다양한 정보매개자를 통해 이루어지기 때문에, 정보매개자들의 콘텐츠 정책은 표현의 자유, 프라이버시 등 이용자의 권익에 지대한 영향을 미치고, 정보매개자들의 법적 책임에 대한 규제와 정책은 그 어느 때보다 중요하다. 마닐라원칙은 바로 이 정보매개자들이 이용자 권리의 침해자가 아닌 수호자로서 기능하는 온라인 환경을 만들기 위해 전세계의 인권활동가 및 시민단체들이 UN인권기구들의 권고문, EU전자상거래지침, UNESCO보고서 등 다양한 국제문헌들을 연구하고 검토하여 국가와 정보매개자들이 준수해야 할 정보매개자책임에 대한 국제법적 원칙을 고안해 낸 결과물이다.
마닐라원칙은 인터넷상 정보 규제 시 지켜야 할 원칙을 정립함으로써 이용자의 표현의 자유, 결사의 자유, 프라이버시권 등을 보호하고자 하며, 크게 다음 6 가지의 대원칙 및 33개의 세부원칙으로 이루어져 있다.

1. 정보매개자들은 제3자의 정보에 대한 책임으로부터 법적으로 보호받아야 한다.
2. 정보 차단은 사법기관의 명령 없이 의무화되어서는 안 된다.
3. 정보 차단 요청은 명백하고, 분명하고, 적법절차를 따라야 한다.
4. 정보 차단 요청 및 실무 및 관련법은 필요성과 비례성의 원칙을 준수해야 한다.
5. 정보 차단 법, 정책 및 실무는 적법절차의 원칙을 지켜야 한다.
6. 정보 차단 법, 정책 및 실무는 투명성과 책임성을 포함해야 한다.

이러한 마닐라원칙은 국내의 정보매개자책임 제도, 즉 정보통신망법상의 임시조치제도, 저작권법상의 OSP전송차단 제도, 전기통신사업법상 모니터링제도 등에 대해 시사하는 바가 크다. 특히 대원칙 1의 세부원칙들은 모니터링 의무나 불법이 아닌 정보에 대한 차단책임을 다루고 있으며, 사법기관의 명령 없이 정보 차단을 해서는 안 된다는 대원칙 2는 방송통신심의위원회, 한국저작권위원회 등 법원의 개입 없는 행정기관의 차단 요청을 허용하는 한국의 법제에 시사하는 바가 크다.

(6) FOC의 인터넷의 자유와 인권 보호에 관한 정책 및 관행 수립을 위한 탈린 의정서

온라인자유연합(Freedom Online Coalition, FOC)은 2011년부터 인터넷의 자유를 지지하기 위해 설립된 정부간 기구로, 현재 30개 나라가 회원국으로 가입되어 있다. 아시아에서는 일본과 몽고 두 나라만 가입하였고, 우리나라는 아직 가입되어 있지 않다. FOC는 2014년 인터넷의 자유와 인권을 보호에 관한 정책 및 관행 수립을 위한 탈린(Tallinn) 의정서[112]를 채택하였다. 그 주요 내용을 살펴보면 다음과 같다.

---

111) A GLOBAL CIVIL SOCIETY INITIATIVE, “Manila Principles on Intermediary Liability”, March 24, 2015.
112) Freedom Online Coalition, “Recommendations for Freedom Online”, Adopted in Tallinn, Estonia on April 28, 2014.

- 기본적으로 온라인에서도 오프라인에서 갖는 권리와 같은 권리를 갖는다.
  - 각국 정부는 자유형 부과, 검열, 해킹, 과도한 감시, 차단 등의 방법을 통한 온라인에서의 표현의 자유를 제한하는 각종 억압적 조치를 중단하여야 한다.
  - 인터넷이 행정의 투명성과 정부의 정보공개 (열린 정부) 관행을 진보시킬 수 있는 강력한 도구라는 점을 상기하고, 인터넷이 그러한 장이 될 수 있도록 만들어야 한다.

3. 국내 법·제도 현황

온라인상 표현의 자유와 관련된 국내의 관련 법·제도는 매우 다양하나, 그 중 가장 큰 영향력을 발휘하며 쟁점이 되고 있는 법·제도를 중점적으로 검토하고, 최근 새롭게 대두되고 있는 논의를 분석한다.

(1) 방송통신심의위원회 통신심의제도

1) 제도 개요 및 현황[113]

정부가 인터넷상 '정보'(contents, 즉, 정보통신망상에서 문자, 음성, 영상 등으로 표현된 모든 종류의 자료 또는 지식)의 유통을 차단하는 방식은 다양하다. 그러나 그 중 대한민국에서 가장 광범위하고 보편적으로 이루어지고 있는 형태는 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조 및 동법 시행령 제8조[114]에 따른 방송통신심의위원회의 통신심의 제도이다.
방송통신심의위원회는 통신심의를 거쳐 시정요구 결정을 내릴 수 있는데, '시정요구'란 방송통신심의위원회가 불법정보 및 청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보를 선별하여, 정보통신서비스 제공자(포털, KT 등 망사업자, 호스팅업체) 또는 게시판 관리·운영자에게 해당 정보의 삭제 또는 접속차단 등을 요구하는 것이다. 문언은 '요구'이나, 행정기관이 발하는 처분[115]으로서 준수율(이행율)이 약 98%에 달하여 사실상 강제력을 가진 규제이다.

---

113) 이하 '한국인터넷투명성보고서 2019', 고려대학교 법학전문대학원 공익법률상담소, 2019. 9. 참조.

114) 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조(심의위원회의 직무)
4. 전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 대통령령이 정하는 정보의 심의 및 시정요구

「방송통신위원회의 설치 및 운영에 관한 법률 시행령」 제8조(심의위원회의 심의대상 정보 등) ① 법 제21조제4호에서 "대통령령이 정하는 정보"란 정보통신망을 통하여 유통되는 정보 중 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의7에 따른 불법정보 및 청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보를 말한다.
② 법 제21조제4호에 따른 시정요구의 종류는 다음 각 호와 같다.
1. 해당 정보의 삭제 또는 접속차단
2. 이용자에 대한 이용정지 또는 이용해지
3. 청소년유해정보의 표시의무 이행 또는 표시방법 변경 등과 그 밖에 필요하다고 인정하는 사항
③ 정보통신서비스제공자 또는 게시판 관리·운영자는 제1항 및 제2항에 따른 시정요구를 받은 경우에는 그 조치결과를 위원회에 지체 없이 통보하여야 한다.

115) 방송통신심의위원회는 위원회의 성격을 민간독립기구라고 주장하나, 여러 행정소송 판결에서 '방송통신심의위원회는 대통령이 위촉하는 9인으로 구성되고 위원들은 국가공무원법상 결격사유가 없어야 하고 그 신분이 보장되며, 국가로부터 운영에 필요한 경비를 지급받을 수 있고 그 규칙이 제정·개정·폐지될 경우 관보에 게재·공표되는 등의 사정에 비추어 행정청에 해당하고, 인터넷 포털사이트 등에 대한 방송통신심의위원회의 게시물의 삭제 등의 시정요구는 단순히 비권력적 사실행위인 행정지도에 불과한 것이 아니라 의무의 부담을 명하거나 기타 법률상 효과를 발생하게 하는 것으로서 항고소송의

방송통신심의위원회는 “정보통신망법 제44조의7에 따른 불법정보”와 “청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보”에 대하여 시정요구를 할 수 있다. 여기서 “정보통신망법 제44조의7에 따른 불법정보”란, 음란물, 명예훼손, 협박·스토킹, 기술적 훼손, 영리목적 표시의무 미이행의 청소년유해매체물, 사행행위, 국가기밀 누설, 국가보안법 위반, 그 밖의 범죄 목적 정보를 말한다. 그리고 “청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보”란 그 의미가 명확하지 않아 시정요구 대상 범위에 대하여 논의의 여지가 있으나, 방송통신심의위원회는 현재 「정보통신에 관한 심의규정」(방송통신심의위원회 규칙 제38호)에 따라, ‘불법정보’에 이르지 않은 정보라도 심의규정상 ‘유해정보’에 해당한다고 판단되면, 삭제·차단 등의 시정요구를 내려 유통을 전면적으로 차단하고 있다.

2018년을 기준으로 할 때 총 252,166건의 정보가 심의되었고, 그 중 238,246건 (94.5%)에 대해 시정요구가 이루어졌다. 2018년 시정요구 가운데 ‘접속차단’은 187,980건 (78.9%), ‘삭제’는 41,000건 (17.2%), ‘이용해지 등’ 9,041건(3.7%), ‘기타(청소년유해표시관련)’는 225건 (0.1%)의 비중을 차지하였다.

한편, 2019. 2. 방송통신위원회가 웹사이트 차단 방식으로 SNI 필드 차단 방식을 도입하여 https 접속 방식의 해외 불법 사이트에 대한 접속차단을 시행한 것에 대하여 큰 사회적 논란이 일었다. 접속차단 제도 자체는 오래된 제도이나, 기술적으로 차단이 불가능했던 다수의 해외 서버 이용 사이트에 대한 차단 조치가 집행되어 실제로 접속이 불가능해지자, 이를 체감하기 시작한 국민들이 웹사이트 차단은 국가의 과도한 검열과 통신 활동에 대한 감시라며 불만을 표출했다. https 차단 정책에 반대하는 청와대 국민청원은 27만명을 넘어섰고, 헌법소원도 제기되었다.[116] 방송통신위원회는 사회적으로 문제가 심각한 디지털 성폭력물, 불법촬영물을 유통하는 음란 사이트나, 도박, 저작권 침해 등 불법 사이트를 차단하기 위하여 불가피한 조치라고 해명했다.

2) 문제 사례[117]

(가) 추상적인 심의규정을 이용한 정치 심의가 의심되는 사례

「정보통신에 관한 심의규정」은 ‘사회적 혼란을 현저히 야기할 우려가 있는 내용’(제8조 제3호 카목)을 심의 대상으로 규정하고 있다. 시사 이슈들에 대하여 정부가 발표한 사실과 다른 내용의 의혹을 제기하는 다수의 인터넷 게시글들이 본 심의규정을 이유로 삭제되는 경우가 있다. 2015년에는 세월호 및 사고 구조 지연에 국정원이 개입되어 있다는 내용의 게시글(2015년 제33차 통신심의소위원회), 연천 포격이나 목함 지뢰 폭발 사건 등은 북한의 도발이 아니며 단순 사고거나 국정원 등이 조작한 것이라는 의혹을 제기하는 내용의 게시글들(2015년 제61차, 제62차, 제63차, 제64차 통신심의소위원회)이 심의되어 문제가 되었고, 2016년에는 경찰청의 신고로 고고도 미사일방어체계인 사드(THAAD)의 유해성을 언급하며 대한민국 내 사드 배치를 반대하는 내용의 게시글들을 삭제 의결(2016년 제53차, 제54차, 제56차, 제58차 통신심의소위원회)하여 논란이 되었다.

또한 심의규정 제8조 제2호 바목 ‘과도한 욕설 등 저속한 언어 등을 사용하여 혐오감 또는 불

대상이 되는 행정처분에 해당’한다고 판시하였다(서울행정법원 2010. 2. 11. 2009구합3592 등).

116) 서울경제, 2019. 8. 12.자 “불법 사이트 차단조치 위헌심판 받는다” 기사.

117) 이하 ‘한국인터넷투명성보고서’ 2015~2019 참조.

쾌감을 주는 내용'을 이유로 대통령이나 고위공직자에 대한 비판적 표현물을 시정요구한 사례도 있다. 2011년에는 알파벳과 숫자를 사용하여 당시 현직 대통령이었던 이명박에 대한 욕설을 추정하게 하는 트위터 계정명 '2mb18noma'를 사용하였다는 이유로 계정 전체를 접속 차단한 사례가 발견되었다(2011년 제16차 통신심의소위원회원회). 2014년에는 리조트 붕괴 사고, 세월호 참사 국면에서 박근혜 전 대통령 및 정부, 여당을 향해 욕설을 사용하며 비판한 글을 삭제한 사례(2014년 제16차 통신심의소위원회, 2014년 제36차 통신심의소위원회)가 있었다.

(나) 신중한 심의 없이 웹사이트 전체를 불법정보로 보아 차단한 사례
2014년 방통심의위는 '포쉐어드'라는 파일 공유 웹사이트를 저작권 위반 정보로 보아 차단하였으나(2014. 10. 16. 제19차 전체회의), 법원에서 포쉐어드 내 일부 불법물이 유통되고 있다고 하더라도 사이트 운영 자체가 저작권법 위반 행위를 방조하고 있는 것으로는 볼 수 없고, 포쉐어드 사이트 전체를 차단한 것은 비례원칙을 위반하여 재량권을 일탈, 남용한 위법한 처분'이라는 판결을 받았다.[118] 2015년에는 웹툰 사이트 '레진코믹스'를 '음란' 사이트로 차단하였다가 이용자들의 항의를 받고 철회한 사례(2015년 제22차 통신소위)도 있었다. 2016년에는 영국인 기자가 운영하는 북한의 IT 기술 정보 전문 웹사이트 '노스코리아테크' 를 '국가보안법 위반 정보로 접속차단하였다(2016년 제22차, 제33차 통신심의소위원회). 노스코리아테크는 북한 IT 정보에 있어 세계적으로 독보적 전문성을 인정받고 있는 매체로 우리나라 언론사뿐 아니라 월스트리트저널, 로이터, BBC 등 유명 외신에도 다수 인용되고 있는 매체였다. 결국 이 역시 법원에서 위법한 처분이라는 판결을 받았다.[119]

3) 국제 동향

UN 표현의 자유 특별보고관, 유럽안보협력기구(OSCE) 대표, 미주기구(Organization of American States, OAS) 표현의 자유 특별보고관과 공동으로 "표현의 자유는 다른 소통의 매체에 적용되듯이 인터넷에도 적용된다"고 선언한 바 있다.[120] 인터넷상 표현물이라고 보호가치가 적다거나 행정기관의 심의, 추상적 기준으로 무분별하게 이루어지는 삭제와 차단이 정당화될 수는 없다는 것이다.
UN 표현의 자유 특별보고관 프랑크 라 뤼(Frank La Rue)는 보고서에서 "방송통신심의위원회가 정부나 유력한 기업들을 비판하는 내용의 정보를 정보통신망법 위반이라는 이유로 삭제하는 사실상의 사후 검열기구로 기능하지 않도록 보장할 수 있는 안전장치는 미흡하다. (…) 표현의 자유를 제한하는 모든 법은 자유권규약 제19조 제3항에 명시된 적법한 목적을 달성하

118) 서울행정법원 2016. 1. 28. 선고 2015구합3461 판결.
119) 서울고등법원 2017.10.18. 선고 2017누49388.
120) ''challenge to freedom of expression in the new century: joint statement by the United Nations Special Rapporteur on freedom of opinion and expression, the OSCE Representative on freedom of the media and the OAS Special Rapporteur on freedom of expression'', 20 November 2001, attached to ""Civil and Political Rights, including Question of Freedom of Expression: Report of the Speical Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mr. Abid Hussain, submitted in accordance with Commission resolution 2001/47"", UN Doc. E/CN.4/2002/75, 30 January 2002, Annex V.

기 위해 명확하고 누구에게나 접근 가능하여야 하며, 어떠한 정치적 또는 상업적 혹은 기타 부당한 영향력으로부터도 독립적인 기구에 의해 자의적이거나 편파적이지 않으며 적절한 남용 방지 장치를 갖춘 방식으로 운용되어야 함을 강조하는 바이다."[121]라고 권고했다.
또한 UN 표현의 자유 특별보고관 데이비드 케이(David Kaye)도 2019. 7. 한국 정부에 'SNI 필터링을 이용한 웹사이트 차단 정책'에 대해 우려를 표명하며, 국제인권법 기준에 부합하는 표현의 자유 제한 조치를 시행할 것을 촉구했다. 이 문서에서는 한국의 웹사이트 차단 정책 및 새로운 SNI 필터링 정책이 자유권규약(ICCPR) 제19조를 비롯한 국제인권법과 기준에 위배되고 있는 점을 구체적으로 기술하고 있다.[122] '불법 사이트'의 광범위한 분류와 통신심의의 근거 규정인 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조가 표현의 자유 제한에 관한 자유권규약 제19조(3)의 명확성과 정확성 수준을 충족하지 못하고 있음을 지적하며, 이는 규제기관의 일방적인 집행 권한과 맞물려 정부가 대중의 정보접근권을 부당하고 불균형적으로 제한할 수 있는 여지를 폭넓게 부여한다고 우려하였다. 또한 삭제 또는 차단 결정에 대한 독립적인 외부의 검토와 감독의 결여는 정부기관의 검증 없는 재량권 행사를 강화시키고, 적법절차 원칙에 대한 우려를 가중시킨다고도 하였다. 나아가 대한민국 정부는 사법기관이 아닌 정부기관이 적법한 표현의 결정자가 되는 규제 모델을 거부해야 한다고 강조하고 있다. 한편, SNI 필터링이 통신의 실제 내용을 읽는 것은 아니라 할지라도, 이 기술은 개인들의 온라인 트래픽과 활동을 실시간으로 파악하고 변조(필터링)할 수 있는 범위를 새로운 영역으로 확장하는 것이라고 밝혔다. 케이 특보는 "각국 정부는 표현의 자유 보장에 필수적인 온라인 프라이버시 증진을 위해 HTTPS와 같은 암호화 기술의 사용을 장려하여 왔다"고 말하며, "SNI 필드를 감시하는 것은 암호화로 보장되는 프라이버시 보호를 우회하고, 이로써 표현의 자유를 부당하게 위축시킨다. 검열 목적으로 취약점을 탐색하는 이러한 관행은 이해관계자들 간의 자발적인 기술적 협력과 정보 교환을 요하는 보안 거버넌스 분야에 대한 대중의 신뢰를 약화시킨다"고도 하였다.

(2) 선관위 선거법 위반 정보 삭제 명령 제도

1) 제도 개요 및 현황

「공직선거법」상 선거관리위원회는 선거법을 위반하는 인터넷 게시물에 대하여 정보통신서비스 제공자에게 삭제 등의 조치를 요청할 수 있다. 해당 요청을 받은 정보통신서비스제공자는 지체없이 이에 응해야 하며, 이행하지 않을 경우 과태료 혹은 형사처벌의 대상이 된다(동법 제82조의4[123]).

---

121) Frank La Rue, op. cit. : "48. The Special Rapporteur welcomes the NHRCK opinion and underscores that any law that restricts the right to freedom of expression to serve a legitimate aim as set out in article 19, paragraph 3, of the Covenant must be clear and accessible to everyone, and applied by a body which is independent of any political, commercial, or other unwarranted influence in a manner that is neither arbitrary nor discriminatory, and with adequate safeguards against abuse. "

122) https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24687 (2019. 11. 13. 최종접속)

123) 「공직선거법」 제82조의4(정보통신망을 이용한 선거운동) ③ 각급선거관리위원회(읍·면·동선거관리위원회를 제외한다) 또는 후보자는 이 법의 규정에 위반되는 정보가 인터넷 홈페이지 또는 그 게시판·대화방 등에 게시되거나, 정보통신망을 통하여 전송되는 사실을 발견한 때에는 당해 정보가 게시된

이 제도로 삭제되는 게시물은 선거마다 급격히 증가하고 있는 것으로도 밝혀졌다. 제20대 총선에서는 약 17,000건, 2017년 19대 대선에서는 약 40,000여건에 이르는 방대한 양의 국민의 온라인상 표현물이 본 제도로 삭제되고 있다.[124]

2) 문제 사례[125]

(가) 여론조사 결과를 단순 인용해도 삭제한 사례

「공직선거법」 제108조 제6항은 "누구든지 선거에 관한 여론조사의 결과를 공표 또는 보도하는 때에는 선거여론조사기준으로 정한 사항을 함께 공표 또는 보도하여야 하며…"라고 정하고 있다. 이는 여론조사 결과가 왜곡되는 것을 막기 위하여, 주로 공정하게 보도할 의무가 있는 영향력 있는 언론사 등의 매체에 대하여 요구되는 제한 규정이다. 그러나 선거관리위원회는 일반 유권자들이 개인 블로그나 웹사이트 게시판에 단순히 여론조사 결과를 공유하는 것에도 본조를 엄격히 적용하고 있다. 이 조항 위반을 이유로 삭제된 1,871건 중 1,840여건이 여론조사 결과를 단순 인용한 사례였다. 언론기사에 보도된 여론조사 결과를 그대로 스크랩하거나 TV 뉴스 화면을 캡쳐하여 게시한 경우도 삭제 대상이 되었으며, 구체적인 수치를 적지 않고 여론의 동향을 언급만해도 삭제되었다.

(나) 시민들이 참여하는 온라인 설문조사도 삭제한 사례

「공직선거법」 제108조 제5항은 여론조사 실시의 경우 일정한 조건을 갖추도록 규정하고 있는데, 이는 '객관적인 여론조사'를 가장해 특정 후보와 정당의 당선을 위해 사실상 선거운동을 하는 것을 막기 위한 것이다. 그러나 본조를 이유로 삭제된 사례를 보면 '문재인의 역할은 무엇인가?', '박영선, 정청래 중에 누가 더 더불어민주당에 필요한가?' 등 특정 후보에 대한 지지도 조사라기보다 설문을 통해 의견을 개진하고 직접 참여하는 사례가 대다수였다.

(다) 후보자에 대한 비판, 풍자도 '비방'으로 삭제한 사례

후보자에 대한 비판글에 일부 욕설이나 비하적 표현이 섞여있다는 이유로 '비방'으로 해석하여 삭제한 사례도 다수 있었다. 문대성 후보의 경우, 논문 표절로 박사학위가 취소된 것을 비

인터넷 홈페이지를 관리·운영하는 자에게 해당 정보의 삭제를 요청하거나, 전송되는 정보를 취급하는 인터넷 홈페이지의 관리·운영자 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호의 규정에 의한 정보통신서비스제공자(이하 "정보통신서비스제공자"라 한다)에게 그 취급의 거부·정지·제한을 요청할 수 있다. 이 경우 인터넷 홈페이지 관리·운영자 또는 정보통신서비스 제공자가 후보자의 요청에 따르지 아니하는 때에는 해당 후보자는 관할 선거구선거관리위원회에 서면으로 그 사실을 통보할 수 있으며, 관할 선거구선거관리위원회는 후보자가 삭제요청 또는 취급의 거부·정지·제한을 요청한 정보가 이 법의 규정에 위반된다고 인정되는 때에는 해당 인터넷 홈페이지 관리·운영자 또는 정보통신서비스 제공자에게 삭제요청 또는 취급의 거부·정지·제한을 요청할 수 있다.

④ 제3항에 따라 선거관리위원회로부터 요청을 받은 인터넷 홈페이지 관리·운영자 또는 정보통신서비스 제공자는 지체없이 이에 따라야 한다.

⑤ 제3항에 따라 선거관리위원회로부터 요청을 받은 인터넷 홈페이지 관리·운영자 또는 정보통신서비스 제공자는 그 요청을 받은 날부터, 해당 정보를 게시하거나 전송한 자는 당해 정보가 삭제되거나 그 취급이 거부·정지 또는 제한된 날부터 3일 이내에 그 요청을 한 선거관리위원회에 이의신청을 할 수 있다.

124) 행정안전위원회, 공직선거법 일부개정법률안 검토보고서(2018. 2.), 한국인터넷투명성보고서 2017, 2018 참조.

125) 참여연대이슈리포트, '선관위의 인터넷 게시물 삭제 내역 조사보고서' (2016. 10. 4.), 제20대 총선 분석자료 참조.

판하는 게시물도 비방으로 보아 삭제되었고, 인천 윤상현 후보의 병역 문제와 이혼 등을 적시한 글들은 500여건 넘게 삭제되었다. 유승민 후보의 얼굴을 '내시'에 합성한 풍자 이미지도 비방으로 보아 삭제되었다.

(라) 의혹 제기글 삭제 및 일부 허위임을 이유로 하여 게시물 전체를 삭제한 사례
나경원 후보 자녀의 대학입학 전형에 대한 의혹을 제기한 글 다수가 허위사실공표로 삭제되었다. 또한 안철수 후보를 비판하는 내용의 유튜브 동영상이 다수 삭제되었으며, 이 중에는 동영상 링크 주소만 적시한 게시물도 있었다. 그 밖에 후보자의 당선 횟수를 단순히 잘못 표기한 것도 삭제되었다.

(마) 선관위의 개표 과정에 대한 의혹 제기를 '선거의 자유방해'로 삭제한 사례
'선거의 자유방해죄' 조항은 위력, 위계, 사술 등 기타 부정한 방법으로 선거의 자유를 방해한 자를 처벌하는 조항이다. 선관위는 투개표 과정에 대한 문제제기와 선관위를 비판하는 내용의 글들이 본조를 이유로 삭제하였다.

(3) 정보통신망법 임시조치 제도

1) 제도 개요 및 현황

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 제44조의2 제2항 및 제4항에서 정보통신망을 통하여 일반에게 공개된 정보로 말미암아 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자가 삭제요청을 하면 정보통신서비스 제공자는 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 30일 이내에서 해당 정보에 대한 접근을 임시적으로 차단하는 조치를 하도록 규정하고 있다.[126)]
헌법재판소는 이 제도에 대해 "글이나 사진, 동영상 등의 다양한 방법으로 정보통신망에 게재되는 사생활이나 명예에 관한 정보에 대해서는 반론과 토론을 통한 자정작용이 사실상 무의미한 경우가 적지 않고, 빠른 전파가능성으로 말미암아 사후적인 손해배상이나 형사처벌로는 회복하기 힘들 정도의 인격 파괴가 이루어질 수도 있어, 정보의 공개 그 자체를 잠정적으로 차단하는 것 외에 반박내용의 게재, 링크 또는 퍼나르기 금지, 검색기능 차단 등의 방법으로는 이 사건 법률조항의 입법목적을 효과적으로 달성할 수 없다. (…) 타인의 명예나 권리를 표현의 자유가 갖는 구체적 한계로까지 규정하여 보호하고 있는 헌법 제21조 제4항의 취지 등에 비추어 볼 때, 사생활 침해, 명예훼손 등 타인의 권리를 침해할 만한 정보가 무분별하게 유통됨으로써 타인의 인격적 법익 기타 권리에 대한 침해가 돌이킬 수 없는 상황에 이르게 될 가

126) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2008. 6. 13. 법률 제9119호로 개정된 것) 제44조의2 (정보의 삭제요청 등) ① 생략
② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제 등을 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 공시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.
③ 생략
④ 정보통신서비스 제공자는 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.

능성을 미연에 차단하려는 공익은 매우 절실한 반면, 이 사건 법률조항으로 말미암아 침해되는 정보게재자의 사익은 그리 크지 않"다는 이유로 합헌으로 결정하였다.[127] 그러나 "권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우"까지 임시조치를 의무화하는 것은 표현의 자유와 알 권리를 심각하게 침해한다는 이유로 다시 헌법소원이 제기되었다(2016헌마275).

위 법률 조항에 따른 임시조치로 연간 약 450,000건, 일일 평균 1,250건이 넘는 인터넷 게시글이 차단되고 있는 것으로 알려지고 있다.[128] 또한 이러한 임시조치는 공인에 의하여 요청되는 경우가 대부분이며, 결과적으로 대체로 공인에 한정된 피해주장자의 권리보호 수단으로 활용되고 있음이 속속 밝혀지고 있다.[129] 인터넷상 여론을 통제하여야 할 필요성이 가장 크며 이러한 활동이 가능한 인적, 재정적 자원을 가진 공인이나 기업들이, 임시조치 제도가 간단한 방법으로 인터넷 글들을 지울 수 있는 제도라는 맹점을 이용하여 자신들에 대한 온라인상의 비판글들을 무차별적, 대량적으로 조치하고 있는 경우가 많다.

2) 문제 사례

(가) 병원 및 대기업 등의 소비자불만글에 대한 임시조치 남발 사례

소비자불만글은 소비자의 합리적 선택을 돕고 알 권리를 보장하며, 상품과 서비스를 판매하는 기업에 대한 견제, 감시를 통해 그들이 경쟁하도록 하여 사업자들로 하여금 더 나은 서비스와 상품을 제공하도록 하는 원동력이 되는, 공익에 기여하는 바가 매우 큰 표현물이다. 그러나 우리나라의 임시조치 제도로 인하여 사업자들은 인터넷상의 본인들에 대한 비판적 후기, 소비자불만글을 쉽게 없애고 있다.

특히, 환자들의 평가에 민감한 병원들이 임시조치 제도를 남용하고 있는 사례가 자주 드러나고 있다. 성형부작용이나 의료사고, 위생 관리 문제, 수술 후유증, 불필요한 수술 권유 등과 관련한 사례가 현실세계에서 줄을 잇고 있고, 사회적 파장을 몰고 오는 사례가 빈번함에도, 인터넷에서는 병원 이용에 대한 부정적 후기나 의료사고와 관련한 정보를 찾아보기가 힘들다. 이의 이유에 대하여, 병원들이 직접, 혹은 홍보대행사 등을 통해 지속적으로 인터넷상 이용후기를 모니터링하고 부정적 이용후기에 대해서는 임시조치(게시중단)을 요청하고 있기 때문이라는 보도도 있었다.[130] 대표적으로, 2014년 말 불거진 '수술실 생일파티' 성형외과의 임시조치 남용 사례가 있다. 강남의 한 성형외과에서 환자가 누워 있는 수술대를 배경으로 간호조무사가 내민 케이크를 의사가 받는 사진이 SNS를 통해 확산되며 수술실 위생, 안전과 의료윤리 논란이 일었던 사건이 있었다. 해당 병원은 즉시 공식 사과했고, 이미 신문과 방송 뉴스로 널리 보도되며 사회적으로 많은 시사점을 던진 사건이지만, 해당 성형외과는 한편 이 사건을 언급한 인터넷글들을 명예훼손을 이유로 임시조치 신고하여 인터넷에서 족족 차단되고 있음이 밝혀졌다.[131] 한편, 라섹 수술 부작용으로 난시가 생겼음에도 모른척하는 병원의 태도에 분노하여 인터넷에 글을 쓰고 해당 병원을 다룬 기사에 비판 댓글을 달았는데 병원이 전문업체를

---

127) 헌재 2012. 5. 31. 2010헌마88, 판례집 24-1하, 578, 578-579.
128) 국민의당 신용현 의원실 국정감사 자료 (출처 : 방송통신위원회)
129) 이재진, 이정기 "인터넷 포털의 '임시차단' 조치에 관한 탐색적 연구",「한국언론학보」제56권 제3호, 2012, 51-84면.
130) KBS, 2014. 8. 29.자 소비자리포트, "성형부작용, 후기도 못올리나?"
131) 한겨레, 2015. 4. 13.자 "'수술실 생일파티 사진' 누가 인터넷에서 가렸나" 기사.
한국일보, 2015. 1. 14.자 "'수술실 생일파티' 고발기사 퍼 와도 삭제 대상?" 기사.

고용하여 임시조치 신고를 하여 해당 글들이 삭제당하였다는 사례[132], 한 정형외과 병원에서 허리 수술을 받은 뒤 부정적 후기를 올렸다가 임시조치 당한 사례[133] 등이 밝혀졌다.
한편, 온라인상 평판을 감시할 필요가 높고 이를 할 수 있는 경제적 자원이 있는 대기업이 임시조치 제도를 이용하여 비판적 여론을 차단하는 경우도 많다.[134] 온라인 마케팅 업체들이 '온라인 평판 관리'라는 명목으로 기업으로부터 대리권을 수여받아 인터넷상의 비판적인 글들을 찾아 대량으로 임시조치 신청을 대행하는 서비스가 횡행하고 있다는 보도도 있었다.[135] 한 블로거가 대기업 남양유업의 제품 과장광고 의혹 및 대리점에 대한 갑질 행태를 비판한 언론기사를 전재, 링크하며 비판한 글들이 임시조치된 사례[136]가 있었고, 이 임시조치는 남양유업으로부터 대리권을 받았다고 주장하는 온라인 마케팅 업체의 신고로 이루어졌음이 민사소송 과정에서 밝혀졌다. 기타 이랜드 노동조합원이 블로그에 노동조합의 투쟁 관련 기사를 스크랩하여 제시하고, 이에 대해 노동조합을 지지하는 짧은 의견을 덧붙인 것에 대해 이랜드 월드가 명예훼손 신고로 임시조치된 사례, 한솔교육 학습지 교사노조의 투쟁과 관련한 게시물 역시 한솔 교육측의 요청에 의해 임시조치된 사례, 지난 해 계약한 보험료와 올해 보험료 견적을 비교하며 삼성화재 보험료가 큰 폭으로 상승했다는 내용의 게시글에 대해서 삼성화재측에서 명예훼손을 이유로 임시조치했던 사례[137], 인터넷 예매 사이트 '티켓무비'가 다른 예매 사이트와 비교하여 상대적으로 불편하다고 기술한 것에 대해 '티켓무비' 측이 명예훼손으로 신고하여 임시조치된 사례, 조선, 중앙, 동아 등 신문의 미국산 쇠고기 협상과 촛불시위에 대한 보도에 대하여 항의하는 일부 시민들이 이들 신문의 광고주 목록을 인터넷에 게재하고 불매운동을 전개한 다수의 게시물들에 대하여 신문사 및 광고주의 요청으로 임시조치되었던 사례 등이 있다.

(나) 정치인, 공적 인물의 비판적 여론 통제를 위하여 임시조치 제도를 이용 한 사례
한편, 정치인이나 공적 인물이 그들에 대한 비판적 여론을 통제하기 위하여 임시조치 제도를 남용한 사례도 많다.
서울광장의 집회를 전면 금지하겠다고 밝힌 당시 서울시장 오세훈을 비판한 블로그 글에 대하여 서울시가 임시조치를 요청하여 임시조치 되었던 사례, 전 국회의원 주성영이 다음 아고라 경제토론 게시판에 주성영의 싸이월드 주소링크와 함께 "주성영 퇴진, 만취한 채 민폐 끼치는 주성영의 싸이월드입니다. 방명록에 글 남기고 왔어요"라는 내용의 글에 대하여 명예훼손 신고로 임시조치되었던 사례, 한 경찰간부가 시위대와 충돌한 상황에서 시위대를 향해 거칠게 진압봉을 휘두르는 장면이 포착되어 일명 '사무라이 조'라는 별명이 붙으며 화제가 된 해당 경찰간부를 비판한 블로그 포스팅 및 해당 인물에 대한 공개질의서를 포함한 다음 아고라 게시판의 게시물이 임시조치되었던 사례, "지배구조 이해하면 뉴스가 보인다… 중앙일보의 삼성, 국민일보의 조용기, 세계일보의 통일교 - 주인을 물지 못하는 개, 주식회사 언론의 태생적 한계" 라는 제목으로 언론사의 지배구조를 분석·비판한 미디어오늘의 신문기사를 스크랩한 블로그 포스팅에 대하여 대형 교회의 유명 목사가 명예훼손을 이유로 신고하여 임시조치한 사

132) 서울신문, 2017. 3. 2.자 "비방도, 비판도 없애드려요… '댓글 흥신소'의 명암" 기사.
133) 헤럴드경제, 2017. 12. 27.자 "좋은 후기는 마케팅, 나쁜 후기는 고소감? 병원들의 아전인수" 기사.
134) 이하의 사례의 대부분은 이재진·이정기, "인터넷 포털의 '임시차단' 조치에 관한 탐색적 연구", 「한국언론학보」 제56권 제3호 2012, 51-84면에 수록된 것을 참조함.
135) 서울신문, 2017. 3. 2.자 "비방도, 비판도 없애드려요… '댓글 흥신소'의 명암" 기사.
136) http://blog.naver.com/fiftyfifty/220663079270 (2019. 11. 13. 최종접속)
137) http://censored.kr/?p=1241 (2019. 11. 13. 최종접속)

례,[138] 2009년 당시 김문수 경기지사가 “만약 우리 대한민국이 일제 식민지가 안 됐다면… 전쟁이 일어나지 않았다면, 과연 오늘의 대한민국이 있었을까?”라고 발언한 것에 대해, 다음(Daum)아고라-이슈청원 사이트에 김 지사의 발언을 그대로 게재하고 “망국적인 발언을 규탄한다”며 사퇴를 요구하는 게시판이 임시조치 되었던 사례, “국민을 믿지 못하는 정부… 아무도 믿지 않는 정부…”라는 제목으로 노무현 대통령 서거에 따른 추모제와 이에 대한 정부 규제, 집시법에 의한 촛불집회의 과잉규제 등에 대한 의견을 신문자료 등을 활용해 게시한 글에 대하여 서울지방경찰청장이 신고하여 임시조치되었던 사례, 인터넷 포털 3사에 서울대 법인화 반대 패러디 동영상 ‘총장실 프리덤’에 대하여 서울대학교가 해당 동영상이 담긴 다수의 게시물 주소(URL)에 대하여 삭제를 요청하여 임시조치되었던 사례, 국회의원 출마를 앞둔 박기준 전 검사가 본인이 과거 연루되어 조사받았던 스폰서 검사 사건을 다룬 정치 블로거의 블로그 글에 대하여 임시조치를 요청하여 임시조치되었던 사례,[139] 세월호 실소유주로 지목된 고 유병언이 언급된 글들을 유족이 신고하여 임시조치한 사례[140]가 밝혀졌다.
대형 교회나 소속 목사의 대리단체가 이들을 비판하는 게시물의 삭제를 무차별적으로 요청한 사례도 발견되었다.[141] 교회 세습으로 논란이 일고 있는 명성교회의 김삼환 목사가 세월호 사건에 대하여 “하나님이 대한민국 국민에게 기회를 주기 위해 세월호를 침몰시켜…꽃다운 아이들을 희생시키며 국민에게 기회를 주는 것“이라고 발언했다가 ‘세월호 망언 목사’로 불리며 물의를 빚었던 사건과 명성교회 세습을 비판하는 글들을 임시조치 신고하여 차단한 사례[142], ‘사랑의 교회’ 고(故) 옥한음 목사의 아들인 옥성호 집사가 낸 ‘갑각류의 크리스천-블랙편’이라는 책에 대한 서평을 하면서, 위 책이 담고 있는 내용을 소개하고, 한국사회에서 기독교가 비판받는 이유가 무엇인지, 진정한 의미의 크리스천은 무엇인지에 대하여 의견을 밝힌 내용에 대하여 사랑의 교회 담임목사 오정현의 대리단체의 신고로 임시조치된 사례[143], 이명박 전 대통령이 소망교회의 김지철 목사에게 위로전화를 했다는 소망교회 관계자의 공개된 발언 및 이를 언급한 기사내용을 토대로, 이명박 당시 대통령이 전화통화를 이용해 정치적 활동을 하는 점에 대한 비판적 의견을 개진한 내용의 게시글이 소망교회의 대리단체를 표방하는 단체의 신고로 임시조치된 사례[144] 등이 밝혀졌다.

3) 국제 동향

외국의 입법례들 중 임시조치와 같이 차단조치가 사실상 의무화되는 경우는 찾아보기 어렵다. 대부분 정보통신서비제공자에게 불법게시물 신고가 들어왔을 때 즉시 삭제하면 법적 면책을 주는 방식으로 동기를 부여한다. 즉, 정보통신서비스제공자는 불법게시물 신고가 들어오더라도 삭제, 차단할 ‘의무’는 갖지 않기 때문에 고유의 판단에 따라 불법 여부가 불확실한 정보에

---

138) http://censored.kr/?p=1255 (2019. 11. 13. 최종접속)
139) 시사IN, 2016. 1. 11.자 “어디 한 번 써봐 삭제하면 그만이야” 기사.
140) http://blog.naver.com/PostView.nhn?blogId=fishes1272&logNo=221165112836 (2019. 11. 13. 최종접속)
141) 한겨레, 2011. 8. 9.자 “대형교회3곳, 포털에 비판글 삭제 요청” 기사.
142) http://blog.naver.com/PostView.nhn?blogId=cciieer&logNo=220980588657 (2019. 11. 13. 최종접속)
http://blog.naver.com/PostView.nhn?blogId=esedae&logNo=220859004134 (2019. 11. 13. 최종접속)
143) http://lmpeter.tistory.com/2128 (2019. 11. 13. 최종접속)
144) http://lmpeter.tistory.com/1374 (2019. 11. 13. 최종접속)

대하여는 자신의 책임 하에 게시물을 유지할 수가 있다. 미국의 저작권법 DMCA 제512조의 '노티스앤테이크다운'(Notice-and-Takedown) 제도는 이마저도 삭제편향이 발생할 수 있다며 침해를 최소화하기 위하여 저작권 침해 정보로 판단되는 정보라도 게시자의 재게시요청이 들어올 경우에는 이를 복원해야만 법적 면책을 받을 수 있도록 하고 있다.[145)]
2010. 5. '라 뤼 한국보고서'에서는 한국의 임시조치 제도가 그 추상성으로 말미암아 과도한 인터넷 게시물 규제로 이어질 수 있으므로 이를 폐지할 것을 촉구하고 있다.[146)] 나아가 정보매개자의 책임 시스템은 서비스제공자의 의무가 아닌 선택으로 규정되어야 하고, 복원권이 보장되는 선에서 정당화될 수 있다고 하였다.[147)]

---

145) 사단법인 오픈넷, "인터넷임시조치제도 개선의 5대 원칙" (https://opennet.or.kr/14421)

146) Frank La Rue, op. cit. : "92. The Special Rapporteur is concerned about the vague condition and scope of liability of intermediaries as prescribed in article 44-2(6) of the Network Act, which may lead to excessive regulation of online content. The Special Rapporteur recommends that the Government repeal all provisions relating to intermediary liability"

147) (b) Regulation of online content by intermediaries

38. The Network Act provides that when information which intrudes upon a person' privacy, defames an individual, or otherwise violates another person' rights is disseminated via the Internet, the "ictim of such a violation may request the provider of information and communications services who handled the information to delete the information or publish a rebuttable statement"8 Upon receiving such a request, the provider of information communication services, or intermediaries, must delete or block access to the information for up to 30 days, then notify the applicant and the publisher of information immediately of the measures taken, and post a public message to inform the users that it has taken the necessary measures
39. If it is difficult to judge whether a particular information "iolates any right or is anticipated that there will probably be a dispute between interested parties" article 44-2(4) of the Network Act stipulates that information and communications services providers, such as blog service providers and web portals with user-generated content, may temporarily block access to the information for up to 30 days, irrespective of whether there has been a request for any measures to be taken.
40. Additionally, article 44-3 stipulates that the service provider may, if it finds that information circulated through its network and managed by it intrudes upon someone' privacy, defames someone, or violates someone' rights, "ake temporary measures at its discretion" Further, article 44-2(6) provides that "f [a provider of information communications services] takes necessary measures [to delete or block access to information], it may have its liability for damages caused by such information mitigated or discharged"
41. The Special Rapporteur is concerned that the Network Act relegates the responsibility for controlling information on the Internet to intermediaries or private companies, rather than to an independent body that is capable of assessing whether a particular post or information violates existing laws on privacy and defamation, and other relevant laws. Moreover, the excessive authority given to intermediaries to regulate online content is a matter of concern, particularly due to the fact that the scope of their liability as prescribed in article 44-2(6) is vague. Hence, although article 44-2(5) of the Network Act stipulates that "very provider of information and communications services shall clearly state the details, procedure, and other matters concerning necessary measures in its standardized agreement in advance" there is a concern that intermediaries will be more inclined to err on the side of safety by deleting or blocking access to information to avoid liability.
42. Furthermore, even if the original publisher contests the decision taken by online service providers to delete or block access to the information that he or she has disseminated online, the Network Act does not set out any requirements for the service providers to

(4) 선거기간 인터넷 실명제

1) 제도 개요

「공직선거법」 제82조의6은 선거기간 중 인터넷신문 및 포털 사이트가 게시판, 댓글 등의 서비스를 제공하는 경우에는 해당 이용자의 실명확인조치를 하도록 의무화하는 일명 선거기간 인터넷 실명제를 규정하고 있다.[148]

2) 국내 동향

'인터넷 실명제'는 정보통신서비스 제공자에게 게시판 이용자로 하여금 인터넷상 정보를 게시할 때 본인임을 확인하는 절차를 거치도록 의무화하는 제도를 의미한다. 헌법재판소는 2012년에 상시적 인터넷 게시판 실명제(본인확인제)에 대해서는 과잉금지원칙을 위반하여 익명 표현의 자유와 개인정보자기결정권을 침해한다는 이유에서 위헌결정을 내린 바 있지만,[149] 2015년에는 인터넷언론사가 선거운동기간 중 당해 홈페이지의 게시판 등에 정당·후보자에 대한 지지·반대의 정보를 게시할 수 있도록 하는 경우 실명확인조치를 의무화한 위 선거기간 인터넷 실명제 조항에 대하여 헌법재판소는 합헌 취지의 결정을 내렸다.[150]

---

take any follow-up action. Instead, it is left to the discretion of intermediaries to establish their own procedures in their service terms and conditions. Hence, there are no guarantees in place to ensure that the right to freedom of expression is protected from arbitrary and excessive limitation, including the possibility of abuse by political figures to censor criticism. While individuals may seek recourse through the judiciary after a decision has been taken by online service providers, it can be lengthy and financially burdensome, and creates a chilling effect on the right to freedom of expression.

148) 「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 동영상 등의 정보(이하 이 조에서 "정보등"이라 한다)를 게시할 수 있도록 하는 경우에는 행정안전부장관 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.

② 정당이나 후보자는 자신의 명의로 개설·운영하는 인터넷홈페이지의 게시판·대화방 등에 정당·후보자에 대한 지지·반대의 정보등을 게시할 수 있도록 하는 경우에는 제1항의 규정에 따른 기술적 조치를 할 수 있다.

③ 행정안전부장관 및 신용정보업자는 제1항 및 제2항의 규정에 따라 제공한 실명인증자료를 실명인증을 받은 자 및 인터넷홈페이지별로 관리하여야 하며, 중앙선거관리위원회가 그 실명인증자료의 제출을 요구하는 경우에는 지체 없이 이에 따라야 한다.

④ 인터넷언론사는 제1항의 규정에 따라 실명인증을 받은 자가 정보등을 게시한 경우 당해 인터넷홈페이지의 게시판·대화방 등에 "실명인증" 표시가 나타나도록 하는 기술적 조치를 하여야 한다.

⑤ 인터넷언론사는 당해 인터넷홈페이지의 게시판·대화방 등에서 정보등을 게시하고자 하는 자에게 주민등록번호를 기재할 것을 요구하여서는 아니 된다.

⑥ 인터넷언론사는 당해 인터넷홈페이지의 게시판·대화방 등에 "실명인증"의 표시가 없는 정당이나 후보자에 대한 지지·반대의 정보등이 게시된 경우에는 지체 없이 이를 삭제하여야 한다.

⑦ 인터넷언론사는 정당·후보자 및 각급선거관리위원회가 제6항의 규정에 따른 정보등을 삭제하도록 요구한 경우에는 지체 없이 이에 따라야 한다.

149) 헌재 2012. 8. 23. 2010헌마47, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 제1항 제2호 등 위헌확인(위헌).

150) 헌재 2015. 7. 30. 2012헌마734 등, 공직선거법 제82조의6 제1항 등 위헌확인 등(기각).

위 결정요지에서 헌법재판소는 “선거운동기간 중 인터넷언론사 게시판 등을 통한 흑색선전이나 허위사실이 유포될 경우 언론사의 공신력과 지명도에 기초하여 광범위하고 신속한 정보의 왜곡이 일어날 수 있으므로, 실명확인조항은 이러한 인터넷언론사를 통한 정보의 특성과 우리나라 선거문화의 현실 등을 고려하여 입법된 것으로 선거의 공정성 확보를 위한 것이다. 실명확인조항은 실명확인이 필요한 기간을 ‘선거운동기간 중’으로 한정하고, 그 대상을 ‘인터넷언론사 홈페이지의 게시판·대화방’ 등에 ‘정당·후보자에 대한 지지·반대의 정보’를 게시하는 경우로 제한하고 있는 점, 인터넷이용자는 실명확인을 받고 정보를 게시할 것인지 여부를 선택할 수 있고 실명확인에 별다른 시간과 비용이 소요되는 것이 아닌 점, 실명확인 후에도 게시자의 개인정보가 노출되지 않고 다만 ‘실명인증’ 표시만이 나타나는 점 등을 고려하면, 이 사건 법률조항이 과잉금지원칙에 위배되어 게시판 이용자의 정치적 익명표현의 자유, 개인정보자기결정권 및 인터넷언론사의 언론의 자유를 침해한다고 볼 수 없다.”고 판시하였다.[151]

3) 국제 동향

인터넷상의 불법·유해정보의 규제에 관한 외국의 입법례들을 보더라도, 미국이나 영국의 경우 인터넷상의 유해 정보에 대한 규제를 원칙적으로 업계의 자율에 맡기고 있고, 독일 등 유럽의 많은 국가들 역시 민간 주도의 자율규제를 기초로 하여 인터넷서비스 제공자의 책임제한이나 면책요건을 정하는 방식으로 관계 법령을 수립하고 있으며, 일본의 경우에도 불법·유해정보가 게시되는 때에 민관이 협조하여 사후적으로 대처하도록 규율하고 있는 등 대부분의 주요 국가들은 본인확인제와 같은 적극적인 게시판 이용규제를 시행하고 있지 않다.
미국의 경우, 1960년에 연방대법원은 Talley v. California 사건에서 전단배포자의 신원확인을 강제하는 것은 익명표현의 자유(right to anonymous speech)를 침해하는 것이라고 판단하였고, 1995년에 Mclntyre v. Ohio Elections Comm'n 사건에서 선거 유인물을 발행하는 사람이나 선거본부의 이름과 주소가 명기되지 않은 경우에 그 유인물의 배포를 금지시킨 오하이오주 법률을 내용규제에 해당하여 수정헌법의 핵심을 이루는 정치적 언론에 대한 제한이라고 하여 위헌선언한 바 있다.[152]
전술한 ‘라 뤼 한국보고서’에서도 선거기간 인터넷 실명제 조항에 대한 개정 권고 의견이 포함되어 있다. 그는 공직선거법상 선거기간 인터넷 실명제 조항을 언급하고[153], 나아가 “인터넷 실명제가 익명성을 기반으로 하는 표현의 자유에 영향을 미칠 것을 우려한다. 게다가 정부에 비판적인 사람들이 자신의 견해를 밝힘으로써 받게 되는 형사상 제재 위협으로 인하여 의견 표명을 꺼리는 경향을 보일 것이다. 이러한 점에서 특별보고관은 2004년 2월 대한민국 국가위원회가 채택한 결정에 주목하는 바이며, 그 권고는 실명제가 ‘명백한 사전검열이자, 익명성에 바탕한 인터넷상의 표현의 자유를 제한하고, 표현의 자유를 침해한다”고 하였다. 이어서 “인터넷을 통해 자행되는 범죄와 그러한 범죄자의 신원을 밝혀야 할 정부의 책임과 관련하여 제기되는 우려가 합당한 측면도 있으나, 특별보고관은 대한민국 정부가 신원 확인을 위한 다른 수단을 고려하고 그러한 수단도 신원 확인 대상자가 이미 범죄를 저질렀거나 저지르려고

151) 헌재 2015. 7. 30. 2012헌마734 등, 판례집 27-2상, 308, 309-309.
152) 홍진수, 인터넷실명제법 제정을 위한 공청회 자료집, 2006. 8. p.21.
153) Frank La Rue, op. cit. : “56. 나아가, 앞서 실명인증제와 관련해 언급했듯이, 개인이 정당이나 후보자에 대한 지지 또는 반대를 표시하는 글을 게재하는 경우, 모든 “인터넷 언론사”는 해당 개인의 실명을 확인하여야 할 의무가 있으며, 이를 위반하는 경우에는 천만 원 이하의 벌금이 부과될 수 있다.“

한다는 상당한 근거나 합리적인 의심이 있는 경우에 한하여 사용할 것을 권고한다."고 밝혔다.[154]

(5) 사실적시 명예훼손죄, 모욕죄

1) 제도 개요 및 현황

온라인에만 특수하게 적용되는 규제는 아니지만, 대부분의 표현 행위가 온라인으로 이루어지는 오늘날 온라인상 표현의 자유를 심각하게 제약하는 일반법으로 '사실적시 명예훼손죄'와 '모욕죄'가 있다. 우리나라 명예훼손 법제는 적시한 사실이 '진실'이더라도 명예훼손으로 형사처벌하는 '사실적시 명예훼손죄'(형법 제307조)[155]가 있고 인터넷상 유포 시에는 가중처벌(정보통신망법 제70조)하고 있다.[156] 또한 '모욕죄'(형법 제311조)는 공연히 사람을 모욕하는 행위를 금지하고 있다. 모욕죄는 구체적인 사실의 적시가 없더라도 '추상적 판단'이나 '경멸적 감정'을 표현하여 타인의 사회적 평가를 저하시킨 경우를 처벌 대상으로 삼고 있다.
2015년을 기준으로 보면, 명예훼손 고소 및 고발 건수는 약 2만 5천 건이고, 모욕죄 고소 건수는 약 3만 7천 건에 이른다. 2007년부터 9년 사이에 일반 명예훼손은 1.5배, 사이버 명예훼손은 2.6배, 모욕은 8.7배로 증가한 수치이다. 모욕죄의 경우 1일 평균 100건 이상의 고소가 접수된 것으로 볼 수 있다.[157]

---

154) Frank La Rue, op. cit. : "52. The Special Rapporteur is concerned about the impact of such identification systems to the right to freedom of expression, which is rooted in anonymity. Additionally, individuals may be less inclined to express their opinions, particularly those that are critical of the Government, given the threat of criminal sanctions for doing so. In this regard, he notes the decision adopted by the NHRCK in February 2004, which stated that the realname identification "learly qualifies as pre-censorship, restricts freedom of Internet-based expression rooted in anonymity, and contravenes freedom of expression" While there are legitimate concerns regarding crimes perpetrated via the Internet and the responsibility of the Government to identify such persons, the Special Rapporteur recommends that the Government consider other means to identify a person and only if there is probable cause or reasonable doubt that the person to be identified has committed or is about to commit a crime."
"94. Given that the real-name registration system restricts the exercise of the right to freedom of Internet-based expression rooted in anonymity, the Special Rapporteur recommends that the Government consider other means to identify a person and only if there is probable cause or reasonable doubt that the person to be identified has committed or is about to commit a crime."

155)「형법」 제307조(명예훼손) ① 공연히 사실을 적시하여 사람의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만 원 이하의 벌금에 처한다.
② 공연히 허위의 사실을 적시하여 사람의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만 원 이하의 벌금에 처한다.
제309조(출판물 등에 의한 명예훼손) ①사람을 비방할 목적으로 신문, 잡지 또는 라디오 기타 출판물에 의하여 제307조제1항의 죄를 범한 자는 3년 이하의 징역이나 금고 또는 700만 원 이하의 벌금에 처한다.
제310조(위법성의 조각) 제307조 제1항의 행위가 진실한 사실로서 오로지 공공의 이익에 관한 때에는 처벌하지 아니한다.

156)「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제70조(벌칙) ① 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 3년 이하의 징역이나 금고 또는 2천만 원 이하의 벌금에 처한다.

157) 금태섭 의원실 보도자료, '하루에 100건 이상 '모욕죄' 고소, 고발
http://www.gsgold.kr/bbs/board.php?bo_table=gs_board3&wr_id=23 (2019. 11. 13. 최종접속)

2) 국내 동향

사실적시 명예훼손죄의 위헌성 논란은 오래 전부터 제기되었으나, 2018년부터 미투운동과 맞물려 더욱 부각되기 시작했다. 공개적이고 상습적인 성폭력 행위나 증거·증인이 충분하여 진실로 쉽게 증명될 수 있는 성폭력 사실을 폭로한 경우에도, 성폭력 가해자가 폭로자를 명예훼손으로 고소하여 협박·위축시키는 2차 가해를 더욱 손쉽게 해주는 요인으로 지적된 것이다. 성폭력 가해자가 일부분은 사실이고 일부분은 허위라며 만연히 상대 여성을 명예훼손으로 고소하면, 어떤 조항이든 범죄 성립 가능성을 부정할 수 없는 수사기관으로서도 이러한 고소만으로도 수사를 개시할 수밖에 없기 때문에, 미투 폭로 여성들이 이러한 2차 피해를 겪고 있다는 제보가 속출했다. 성폭력 가해자들은 최종적으로 고발자들이 명예훼손으로 처벌받는 것을 목표로 한다기보다 본인들에 대한 폭로를 초기에 진화하는 수단으로 명예훼손 고소를 남발하는 경우가 많다.[158] 이는 미투 외에도 기업의 비리, 상사의 갑질, 권력자의 부정행위 등을 내부고발하고 공론화시키는 과정에서 다수가 겪고 있는 폐해다.

2018년 4월, 법률가 330인은 사실적시 명예훼손죄 폐지를 촉구하는 법률가 선언문을 발표하였다. 여기에서 진실을 말하는 것은 표현의 자유로 보호되어야 함에도, 진실한 사실에 기반하지 않은 개인의 '허명'을 보호하기 위해 진실을 말한 사람을 형사처벌의 대상이 될 수 있도록 하는 것은 위헌적이고, 이러한 형사처벌의 위험이 수많은 부조리에 대한 고발을 위축시켜 사회 진보의 기회를 박탈하는 심각한 사회적 해악을 가지고 있음을 지적하며, 정치권이 본 법을 조속히 폐지할 것을 촉구하였다.[159] 그리고 한국형사정책연구원에서도 2018년 10월 사실적시 명예훼손죄를 폐지하는 것이 바람직하다는 내용의 보고서가 발간된 바 있다.[160]

한편, 타인에 대한 부정적인 감정이나 의견을 표현하는 것을 범죄화하여 더욱 광범위하고 포괄적인 표현들이 처벌 대상이 될 수 있는 모욕죄를 공인들이 이용하는 사례도 자주 발견되고 있다. 2019년 제1야당의 원내대표인 나경원 의원이 자신과 관련된 기사에 '나베', '매국노', '국X' 등의 단어를 사용하며 악성 댓글을 게시한 170개의 아이디를 모욕 혐의로 고소하였음이 밝혀져 모욕죄의 문제점이 다시 수면 위로 떠올랐다.[161]

3) 국제 동향

세계적으로 명예훼손죄의 형사범죄화 자체를 폐지해가는 추세이고, 적어도 진실사실을 말한 경우에는 처벌하지 않는 것이 국제법의 원칙이다. 유엔 자유권규약위원회는 우리나라가 1990년 비준한 자유권규약(ICCPR) 중 표현의 자유 부분에 대하여 사실이 진실한 경우에는 최소한 형사처벌 대상이 되어서는 안 된다는 취지의 유권해석을 내린바 있다.[162] 미국, 독일, 프랑스 등 대부분의 선진국들도 사실적시 명예훼손죄를 두고 있지 않으며, 2015년 유엔 자유권규약

158) 손지원, "미두운동의 걸림돌, 사실적시 명예훼손죄를 둘러싼 쟁점과 개선 방안",「언론중재」2018년 여름호 참조.
159) https://opennet.or.kr/14691 (2019. 11. 13. 최종접속)
160) 윤해성·김재현,『사실적시 명예훼손죄의 비범죄화 논의와 대안에 관한 연구』, 한국형사정책연구원, 2018. 10.
161) https://opennet.or.kr/16427 (2019. 11. 13. 최종접속)
162) Geveral Comment 34, para. 47 : "All such laws, in particular penal defamation laws, should include such defences as the defence of truth..."

위원회[163]와 2011년 유엔 표현의 자유 특별보고관[164] 역시 대한민국 정부에 사실적시 명예훼손죄의 폐지를 권고한 바 있다. 국제인권단체 휴먼라이츠워치의 연례인권보고서 한국편에서는 진실을 말해도 명예훼손죄로 처벌할 수 있는 현행 형법 규정 폐지 여부가 현 정부의 인권 수준을 보여주는 척도가 될 것이라고 말했으며, 2018년에는 국제인권기구인 아티클 19(Article19)이 대한민국에 사실적시 명예훼손죄를 비롯한 형사 명예훼손죄의 폐지를 촉구하는 성명을 발표했다.[165]

모욕죄와 관련하여서는 UN 인권위원회가 자유권 규약 해석에 대한 일반논평에서 사실적 주장이 아닌 단순한 견해나 감정 표현에 대하여 형사처벌이 이루어져서는 안 됨을 선언한 바 있고,[166] UN 표현의 자유 특별보고관 역시 한국 정부에 이를 지적한 바 있다.[167]

4. 주요 쟁점 사례

(1) 혐오표현 규제

1) 논의의 대두 및 국내 동향

---

163) 2015년 유엔 자유권 규약 위원회 권고 Human Rights Committee, “Concluding observations on the fourth periodic report of the Republic of Korea”, Adopted by the Committee at its 115th session (19 October-6 November 2015).

“Criminal defamation laws

46. The Committee is concerned about the increasing use of criminal defamation laws to prosecute persons who criticize government action and obstruct business interests, and of the harsh sentences, including lengthy prison sentences, attached to such legal provisions. It further notes with concern that even a statement which is true may be criminally prosecuted, except if this statement was made for the purpose of public interest alone (art. 19).

47. The State party should consider decriminalizing defamation, given the existing prohibition in the Civil Act and should in any case restrict the application of criminal law to the most serious of cases, bearing in mind that imprisonment is never an appropriate penalty It should ensure that the defence of truth is not subjected to any further requirements. It should also promote a culture of tolerance regarding criticism, which is essential for a functioning democracy.”

164) 2011년 유엔 표현의 자유 특별보고관 권고

Frank La Rue (2011), “Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Mission to the Republic of Korea”(A/HRC/17/27/Add.2), UN Human Rights Council, 21 March 2011

“27. The Special Rapporteur reiterates that for a statement to be considered defamatory, it must be false, must injure another person''s reputation, and made with malicious intent to cause injury to another individual''s reputation.

89. The Government should, in line with the global trend, remove defamation as a criminal offence from the Criminal Act, given the existing prohibition of defamation in the Civil Act.”

165) https://opennet.or.kr/15205 (2019. 11. 13. 최종접속)

166) General Comment 34, para. 47 : “[P]enal defamation laws. . . should not be applied with regard to those forms of expressions that are not, of their nature, subject to verification.”

167) 라 뤼 한국보고서, para 27 : “With regard to opinions, it should be clear that only patently unreasonable views may qualify as defamatory”

2013년을 전후하여 온라인 커뮤니티 사이트 '일간베스트'의 활동이 활발해지면서 혐오표현의 문제가 특히 주목받기 시작하였다. 이 커뮤니티에서 민주화운동, 여성, 외국인, 호남 지역 폄하글이나 비방 용어들이 다수 확산되었기 때문이다. 2016년에 '강남역 살인사건'이라는 여성 혐오범죄가 발생하자 혐오표현 규제를 비롯하여 혐오문화에 엄정하게 대응하여야 한다는 움직임이 일었다. 한편 여성 혐오에 대하여 미러링 방식으로 대응하는 온라인 커뮤니티 사이트 '워마드' 역시 주목을 받게 되고 성 대결 구도가 심화되면서 사회 전반의 혐오문화에 대한 우려도 생겨났다. 2018년에는 예멘 난민 550명이 제주도로 입국하여 난민 신청을 하면서 난민과 무슬림에 대한 혐오문화도 부각되기 시작했다. 2019년에는 영향력 있는 공인들이 역사적 사건을 왜곡하는 발언이 문제시되어 5.18 민주화 운동 희생자나 일본군 위안부 피해자 등 역사적 사건의 피해자에 대한 모욕을 혐오표현의 관점에서 규제해야 한다는 논의가 일었다. 한편 사회의 구성원의 출신과 개성이 다양해지고 이를 존중해야 한다는 인식도 확산됨과 동시에, 이에 대한 반작용으로 이주민이나 성소수자를 대상으로 한 혐오표현도 공론장에 적극적으로 등장하기 시작하였다.

혐오표현 규제가 현안인 만큼 이와 관련한 여러 법안들이 발의되어 있고, 앞으로도 꾸준히 발의될 것으로 보인다. 대표적으로 박선숙 의원 대표발의의 「전기통신사업법 일부개정법률안」은 "대통령령으로 정하는 혐오·차별·비하 표현"을 내용으로 하는 정보에 대하여 부가통신사업자에게 ① 차단수단을 제공할 의무 부과하는 한편, ② 이러한 정보가 유통되지 아니하도록 모니터링하고, 발견 시 지체 없이 삭제 및 유통방지에 필요한 조치를 할 의무를 부과하는 것을 주요 내용으로 하고 있다. 다만, 혐오표현 관련 법안들은 대부분 그 대상 집단 설정과 표현으로 인한 해악의 결과를 구체화하지 못하고 있는 것으로 보인다. 2019년 4월에는 여야 3당이 일명 '5·18 민주화운동 왜곡 처벌법'을 공동 발의하였는데, 이는 역사 부정, 역사 왜곡과 연결하여 역사적 사건의 희생자들에 대한 혐오표현을 규제하고자 하는 법안이라 할 수 있다. 해당 법안은 5·18 민주화 운동을 "1979년12월 12일과 1980년 5월 18일을 전후하여 발생한 헌정질서 파괴 범죄와 부당한 공권력 행사에 대항하여 시민들이 전개한 민주화운동"으로 정의하고, 출판물 또는 정보통신망의 이용 등의 방법으로 이를 부인, 비방, 왜곡, 날조 또는 허위사실을 유포한 자를 7년 이하의 징역 또는 7천만 원 이하의 벌금에 처하게 하는 내용을 담고 있다.

한편, 현행 법령 중 혐오표현 금지로 해석될 수 있는 법으로, 「장애인차별금지 및 권리구제 등에 관한 법률」 제32조 제3항은 "누구든지 장애를 이유로 학교, 시설, 직장, 지역사회 등에서 장애인 또는 장애인 관련자에게 집단따돌림을 가하거나 모욕감을 주거나 비하를 유발하는 언어적 표현이나 행동을 하여서는 아니 된다"라고 규정하고 있다.

2) 국제적 기구 또는 단체의 동향[168]

UN 자유권규약 제20조 제2항은 "차별, 적의 또는 폭력의 선동이 될 민족적, 인종적 또는 종교적 증오의 고취는 법률에 의하여 금지된다"고 하여 증오(혐오)의 고취를 금지하는 법률의 도입을 당사국의 의무로서 부과하고 있다. 동 조항이 금지하는 행위의 구성요건은 첫째, 차별로부터 보호되어야 할 소수자집단에 대해 증오를 고취하는 행위여야 하며, 둘째, 그 증오의 고취는 선동적 요소를 갖추어야 한다. 셋째, 차별, 적의 또는 폭력이라는 해악을 야기할 위험성이 있어야 한다.[169] 유럽평의회는 1997년 '혐오표현에 관한 권고'[170]를 채택하여, 정부,

168) 이하 홍성수 외, 『혐오표현 실태조사 및 규제방안 연구』, 국가인권위원회 연구보고서, 2016; 국회 입법조사처, "혐오표현 규제의 국제적 동향과 입법과제" 현안보고서 제306호, 2017. 6. 12. 등 참고.

공권력, 공공기관 및 관료들이 혐오표현을 하지 않을 책임을 특별히 강조하였고, 혐오표현에 대응하기 위해 형법뿐 아니라 민법, 행정법 등으로 이뤄진 종합적인 법제를 수립할 것, 형사적 제재수단으로서 사회봉사명령을 도입할 것 등을 회원국에 요구함으로써, 혐오표현에 대한 종합적인 대응을 독려하였다.

유럽인권재판소(유럽인권위원회)는 유럽인권협약 당사국에서 행해진 혐오표현 규제가 표현의 자유 침해인지 아니면 정당한 제한에 해당하는지에 대한 다수의 사건을 다루어 왔다. 유럽인권재판소는 표현의 자유에 대한 제약이 정당한 것으로 인정될 수 있는지를 유럽인권협약 제10조 제2항에 의거해 세 단계로 심사한다. 첫째, 그 개입은 법률에 근거해야 할 뿐 아니라, 해당 법률은 '명확한 용어로 규정되어, 시민들이 자신의 행위를 규제할 수 있어야' 한다.[171] 둘째, 타인의 명예나 권리의 보호 등 동 조항에서 인정한 정당한 목적을 추구해야 한다. 셋째, 정당한 목적을 추구하는 데 있어 민주사회에서 필요한 것이어야 한다. 유럽인권재판소에 따르면, 여기서 '필요'하다는 것은 그 제약에 '중대한 사회적 필요'가 있어야 한다는 것으로서, 이를 판단하기 위해서는 표현의 내용, 맥락과 함께, 그 개입이 정당한 목적의 추구를 위한 적정한 수단인지, 그 개입으로 인해 제한되는 표현의 자유에 비해 보호되는 권리 혹은 공익이 더 큰지를 심사한다.[172]

국제인권단체 아티클19은 혐오표현에 관해 심층적인 연구와 논의를 주도하여 표현의 자유와 평등을 조화롭게 옹호, 증진할 수 있는 혐오표현 대응 기준과 다양한 방안에 대한 논의 결과물을 발간해 왔다. 그 중 2015년 '혐오표현 해설'[173]에서는 국가가 금지해야 할 의무가 있는 해악이 중대한 '혐오표현'과 그렇지 않은 표현(심히 불쾌한 표현, 종교모독, 역사부정 등)에 대한 구분 기준을 제시하고 있다. 전자에 해당하는 혐오표현은 '집단살해(제노사이드)에 대한 직접적이고 공개적인 선동'이나 '차별, 적대, 폭력의 선동이 되는 차별적인 혐오의 고취'가 있다. 제노사이드 협약 제3조(c)에 따르면 국가는 집단살해 행위를 비롯한"직접적이고 공개적인 집단 살해 선동"을 형사상 범죄로 취급해 이를 금지하고 처벌해야 한다고 명시하고 있다. 이러한 의무는 국제형사재판소 규정 및 유엔의 임시 국제형사재판소들 규정에서도 반복해서 언급하고 있다. 이러한 표현이 가지는 위험성과 제재 필요성에 대해서는 별다른 논의의 여지가 없다. 중요한 것은 자유권규약 제20조 제2항에서 규정한 '차별, 적대, 폭력의 선동이 되는 차별적인 혐오의 고취'이다. 기준의 추상성으로 말미암은 표현의 자유 침해 우려 때문에 많은 국가에서 적용을 유보하고 있다. 아티클19의 본 문서에서는 이에 대한 구체적 기준을 제시하고 있다. 화자의 의도가 차별적인 혐오를 고취하고자 하는 구체적 의도로써, 차별, 적의, 폭력에 대해 청중이 선동당할 가능성을 인지하고 의도한 것이어야 할 것, 그리고 혐오 고취의 결과로 청중이 실제로 선동되어 금지 행위에 가담할 가능성이 높은 임박한 위험이 있어야 한다는 '심각성 요건'을 제시하고 있다. 이 심각성 요건을 판단함에 있어서는 1. 표현 맥락 (표현이 전달된 정치, 경제, 사회적인 맥락, 2. 화자 (지위, 영향력, 청중과의 관계), 3. 의도 정도 (우발성

---

169) UN Special Rapporteur on Freedom of Expression, Frank La Rue, Report on Hate Speech and Incitement to Hatred, 7 September 2012, 1/67/357, para. 43.
170) Council of Europe Committee of Ministers, Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "Hate Speech", 30 October 1997.
171) The Sunday Times v. United Kingdom, Application no. 6538/74, ECHR, 26 April 1979, para. 49.
172) Zana v. Turkey, Application no. 18954/91, ECHR, 25 November 1997, para. 51.
173) Article 19, 'Hate Speech' Explained : A Toolkit, 2015
서울대학교 인권센터, 'Aricle 19, 혐오표현 해설' (국문번역본)

이거나 경솔한 표현이었는지, 계획적이고 반복적인지 등), 4. 표현 내용 (표현의 직·간접성), 5. 표현의 정도 및 규모, 6. 잠재적인 해악의 가능성과 그 임박성 등을 고려해야 한다고 한다. 한편, 이러한 혐오표현에 대한 제재는 주로 민법과 행정법에서 다루어져야 하며, 형사처벌은 가장 심각한 사건에 한해 최후의 수단으로 활용해야 한다는 입장이다.

3) 주요 국가의 동향[174]

해외 각국의 혐오표현 규제 관련 입법례를 살펴보면 다음과 같다.[175]
영국은 「1986년 공공질서법(Public Order Act 1986)」 제3장에서 '인종적 증오'라는 제목으로 인종적 증오선동 금지를 규정하고 있다.[176] '인종적 적대감'이란 "피부색, 인종, 국적(시민권 포함) 또는 민족적 혹은 국가적 출신에 의해 정의되는 사람의 집단에 대한 적대감"을 말하며, 이러한 인종적 적대감을 고무하기 위한 의도를 가지거나, 인종적 적대감이 유발될 우려가 있는 위협적, 매도적 혹은 모욕적인 말이나 행동을 사용하거나 위협적, 욕설적, 모욕적인 글을 공개하는 것을 규제하고 있다.
독일은 형법 제130조 대중선동죄[177]에서 일정한 국적, 인종, 종교 또는 출신민족으로 이루어진 특정 집단이나 일부 인구집단 또는 거기에 속한 개인에 대하여 그에 속한다는 이유로 증오 또는 폭력적이거나 자의적인 조치를 선동하거나, 모욕하거나 악의적으로 경멸 또는 중상함으로써 인간의 존엄을 침해하는 경우를 처벌 대상으로 삼고 있다. 또한 일명 '홀로코스트 부정죄'로 불리는 조항에서는 국제형법전 제6조 제1항에서 명시하고 있는 나치에 의해 이루어진 행위나 나치의 전단적 폭력을 공연히 혹은 집회로 승인, 부인, 찬미, 경시하는 경우 등을 처벌

---

174) 이하 홍성수 외, 『혐오표현 실태조사 및 규제방안 연구』, 국가인권위원회 연구보고서, 2016; 국회 입법조사처, "혐오표현 규제의 국제적 동향과 입법과제" 현안보고서 제306호, 2017. 6. 12. 등 참고
175) 이승현, "혐오표현과 표현의 자유", 한국인터넷거버넌스 포럼 발표문(2018. 7. 5.) 참조.
176) 영국 「공공질서법(Public Order Act 1986)」
제17조 ('인종적 적대감(racial hatred)'의 의미) 이 장에서 '인종적 적대감'이란 피부색, 인종, 국적(시민권 포함) 또는 민족적 혹은 국가적 출신에 의해 정의되는 사람의 집단에 대한 적대감이다.
제18조(말이나 행동의 사용 또는 글의 공개) (1) 위협적, 매도적 혹은 모욕적인 말이나 행동을 사용하거나, 위협적, 욕설적, 모욕적인 글을 공개하는 자는 다음의 경우 유죄이다
(a) 인종적 적대감을 고무하기 위한 의도를 가지거나
(b) 모든 상황상 인종적 적대감이 유발될 우려가 있는 경우
177) 독일 형법 제130조 대중선동죄
① 공공의 평화를 어지럽히는 적정한 방법으로 1. 일정한 국적, 인종, 종교 또는 출신민족으로 이루어진 특정 집단이나 일부의 인구집단 또는 거기에 속한 개인에 대하여 그에 속한다는 이유로 증오 또는 폭력적이거나 자의적인 조치를 선동하는 경우, 또는 2. 전술한 집단이나 일부의 인구집단 또는 개인을 그에 속한다는 이유로 모욕하거나 악의적으로 경멸 또는 중상함으로써 인간의 존엄을 침해하는 경우에는 3월 내지 5년의 자유형에 처한다.
② 1. 전술한 특정 집단, 인구집단 또는 개인에 대하여 그에 속한다는 이유로 그들에 대한 폭력적이거나 자의적인 조치를 선동하는 경우 또는 모욕하거나 악의적으로 경멸 또는 중상함으로써 인간의 존엄을 침해하는 경우로 이를 글(제11조 제3항)을 통하여 (a) 배포, (b) 공공에 공개, 게시, 표명 기타 접근가능하게 하거나 (c) 18세 이하에게 제공, 공급 또는 접근가능하게 하거나 (d) (a)에서 (c) 까지의 의미로 사용하거나 타인에게 사용하게 할 목적으로 이들을 수입·수출하기 위해 생산, 입수, 공급, 저장, 제공, 발표, 추천, 수행한 경우, 2. 라디오, 미디어, 통신서비스를 통해 1에 제시한 내용의 것을 배포한 자는 3년 이하의 자유형이나 벌금에 처한다.
③ 공공의 평화를 혼란하게 한 방법으로서, 국제형법전 제6조 제1항에서 명시하고 있는 국가사회주의에 의해 이루어진 행위를 공연히 혹은 집회로 이를 용인하거나, 부인하거나 경시하는 자는 5년 미만의 자유형 또는 벌금에 처한다.
④ 국가사회주의의 전단적 폭력을 승인하거나, 찬미하거나, 정당화함으로써 피해자의 존엄을 해치는 방법으로, 공연히 혹은 집회로 공공의 평화를 혼란하게 한 자는 3년 이하의 자유형이나 벌금에 처한다.

하고 있다.

프랑스는 언론법[178]과 형법[179]에서 민족, 국가, 인종, 종교, 성, 성적 지향, 장애를 이유로 개인 또는 집단에 대한 차별, 적대감, 폭력을 선동하거나, 그 개인이나 집단을 명예훼손, 모욕을 한 경우를 처벌하고 있다.

캐나다는 형법 'Hate Propaganda'의 장[180]에서 피부색, 인종, 종교, 민족적 출신 또는 성적

---

178) 프랑스 언론법 제24조

⑤ 제23조에 규정된 수단에 의해서, 민족, 국가, 인종 또는 종교에 속하는지 유무를 이유로 개인 또는 집단에 대한 차별, 적대감, 폭력을 선동하는 자는 45,000유로의 벌금이나 1년의 구금, 또는 양자의 어느 하나에 처한다.

⑥ 전술한 수단에 의해서, 성, 성적 지향 또는 정체성, 장애를 이유로 적대감, 폭력을 선동하거나 그들에 대해 형법 제225-2조와 제432-7조에 규정한 차별을 선동하는 자에 대해서도 동일하다.

프랑스 언론법 제32조

① 제23조에 규정된 수단에 의해서 개인의 명예를 훼손한 자는 12,000유로의 벌금에 처한다.

② 동일한 수단에 의해서, 민족, 국가, 인종 또는 종교에 속하는지 유무를 이유로 개인 또는 집단에 대해 명예를 훼손한 자는 1년의 구금과 45,000유로의 벌금, 혹은 양자의 어느 하나에 처한다.

③ 성, 성적 지향 또는 정체성, 장애를 이유로 개인 또는 집단에 대해 명예를 훼손한 자에 대해서도 전항과 동일한 형에 처한다.

프랑스 언론법 제33조

③ 전항에 규정된 조건하에, 민족, 국가, 인종, 종교에 속한 유무를 이유로 하여 개인 또는 집단에 대해 모욕이 행해진 때에는 6월의 구금과 22,500유로 벌금에 처한다.

④ 성, 성적 지향 또는 정체성, 장애를 이유로 행해진 모욕에 대해서도 전항과 동일한 형에 처한다.

179) 프랑스 형법 제3절(비공연한 인종주의적 혹은 차별적 명예훼손 및 모욕)

R624-3

① 공연하지 아니한 상황에서 출신을 이유로 또는 사실 여부에 관계없이 특정 민족, 국민, 인종 또는 종교에의 소속 여부를 이유로 하여 사람 또는 사람의 집단에 대하여 명예를 훼손하는 자는 제4급 위경죄에 대한 벌금에 처한다.

② 성, 성적지향, 장애를 이유로 한 사람 또는 집단에 대하여 행하는 비공연한 명예훼손행위에 대해서도 동일한 형에 처한다.

R624-4

① 공연하지 아니한 상황에서 출신을 이유로 또는 사실 여부에 관계없이 특정 민족, 국민, 인종 또는 종교에의 소속 여부를 이유로
하여 사람 또는 사람의 집단을 모욕하는 자는 제4급 위경죄에 대한 벌금에 처한다.

② 성, 성적지향, 장애를 이유로 한 사람 또는 집단에 대하여 행하는 비공연한 모욕행위에 대해서도 동일한 형에 처한다.

R625-7

① 공연하지 아니한 상황에서 출신을 이유로 또는 사실 여부에 관계없이 특정 민족, 국가, 인종 또는 종교에의 소속을 이유로 하여 사람 또는 사람의 집단에 대한 차별, 적대감 또는 폭행을 비공연하게 선동하는 행위는 제5급 위경죄에 대한 벌금에 처한다.

② 성, 성적지향 또는 장애를 이유로 한 사람 또는 집단에 대하여 증오 또는 폭행을 비공연하게 선동하거나 제225-2조와 제432-7조에 규정한 차별을 비공연하게 선동하는 행위도 동일한 형에 처한다.

180) 캐나다「형법(Criminal Code)」

제318조(제노사이드 옹호(Advocating genocide))

(4) 이 조에서 '식별 가능한 집단'이란 모든 공공부문에서 피부색, 인종, 종교, 민족적 출신 또는 성적지향에 의해 구별되는 것을 의미한다.

제319조(공공에서의 적대감의 선동(Public incitement of hatred))

(1) 공공장소에서 표현의 전달에 의해 식별 가능한 집단에 대한 적대감을 선동한 자는, 그 선동이 치안방해를 일으킬 우려가 있는 경우,

(a) 기소 가능한 범죄로서 유죄이며 2년 이하의 징역에 처하거나,

(b) 약식판결에 기해 처벌 가능한 죄로서 유죄이다.

(2) (고의에 의한 적대감의 증진) 사적인 대화를 제외하고, 표현의 전달에 의해 식별 가능한 집단에 대한 적대감을 고의로 증진하는 자는,

(a) 기소 가능한 범죄로서 유죄이며 2년 이하의 징역에 처하거나,

(b) 약식판결에 기해 처벌 가능한 죄로서 유죄이다.

지향에 의해 구별되는 '식별 가능한 집단'에 대한 적대감을 선동하여 치안 방해를 일으킬 우려가 있는 경우, 적대감을 고의로 증진한 경우 등을 처벌하고 있다.
일본은 2016년의 「해외 지역 출신자에 대한 부당한 차별적 언동 해소를 위한 대책 추진에 관한 법률(本邦外出身者に対する不当な差別的言動の解消に向けた取組の推進に関する法律)」[181] 에서 '해이 지역 출신자에 대한 부당한 차별적 언동'을 "해외 지역 출신자에 대해 차별적 의식을 조장 또는 유발할 목적으로 공공연하게 그 생명, 신체, 자유, 명예 혹은 재산에 위해를 가하고자 함을 고지하거나 그들을 지역사회로부터 배제할 것을 선동하는 부당한 차별적 언동"으로 정의하고, 이러한 차별적 언동이 없는 사회 실현을 위하여 국가 및 지방자치단체가 적절한 시책을 강구할 책무를 규정하고 있다.[182]

(2) 허위정보 규제[183]

1) 논의의 대두 및 국내 동향

최근 정치권에서 '가짜뉴스'[184]를 사회악으로 지목하고 엄정한 대응에 나서며 허위정보에 대한 강력 규제론이 대두되고 있다. 허위정보의 유포는 역사적으로 늘 존재하여 왔으며 새로운 경향이 아니다. 그러나 현대로 올수록 기술의 발달로 합성과 같은 조작이 용이해지고, 또 인터넷을 이용하여 누구나 쉽게 정보의 생산자 역할, 즉 '미디어' 기능을 할 수 있게 되었으며, 소셜 네트워크 서비스 등을 통한 전파력 때문에 정보의 영향력이 커지자 허위정보에 대한 우려도 함께 커졌기 때문에 허위정보에 대한 규제론이 탄력을 받고 있는 것으로 보인다. 한편 정치적으로는 사회의 양극화가 심화되면서 의제 선점과 정보 전쟁이 격화되고 있는 점도 그 배경이 되고 있다고 분석할 수 있을 것이다.
개인의 인격권을 침해하는 결과로 이어지는 허위정보 유포의 경우는 형법 및 정보통신망법상의 허위사실 적시 명예훼손죄 및 공직선거법상의 허위사실공표죄 등으로 규율된다. 결국 현재 도입이 논의되는 허위정보 규제는 특정 개인에 대한 것이 아닌, '사회통합을 저해'하거나, '사회질서를 혼란'하게 하거나, '공익을 해할 우려'가 있는, 공적 사안에 대한 허위정보에 대한 규제다. 헌법재판소는 2010년 '공익을 해할 목적'으로 허위의 통신을 한 자를 처벌하는 일명 '허위사실유포죄' 조항에 대하여 헌법상의 명확성 원칙 위배 등을 이유로 위헌 결정을 한 바 있다.[185]

---

(3) 누구도 이하의 각 항에 해당하는 경우 제2항의 죄에 해당하지 않는다.
(a) 전달되는 표현이 진실인 것을 증명한 때
(b) 선의로 종교적 주제 혹은 경전상 믿음에 기한 의견을 표현하거나 논의를 통해 규명하려고 시도한 때
(c) 표현이, 그에 대한 논의가 공공의 이익을 위한 것으로 공공의 관심사에 관련된 주제에 관한 것이었을 경우 또는 피고인이 그 진술을 진실이라고 믿을 합리적 근거가 있는 경우 또는
(d) 캐나다의 식별 가능한 집단에 대한 적대감의 감점을 발생시키거나 발생시키는 경향이 있는 문제를 제거하기 위하여, 선의로 이를 지적하려는 의도를 가진 경우

181) 平成 28年 法律 제68号, 시행일 : 平成 28년(2016년) 6월 3일.
182) https://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=428AC1000000068 (2019.11.15. 최종접속)
183) 손지원, "가짜뉴스 규제법의 헌법적 분석 및 해외 동향", 「언론중재」 2018년 겨울호(Vol. 149) 참조
184) '가짜뉴스', '허위조작정보' 등 여러 용어가 있으나, 보통 이들 정보에 대한 규제론은 허위의 내용을 담고 있는 표현물에 대한 규제를 통칭하므로, 이하에서는 '허위정보'로 통칭하기로 한다.
185) 헌재 2010. 12. 28. 2008헌바157 등, 전기통신기본법 제47조 제1항 위헌소원.

2018년 말 기준, 국회에는 허위정보 규제와 관련하여 22개의 법안이 계류되어 있는 것으로 알려졌다. 그 중 대표적인 법안은 더불어민주당 박광온 의원이 대표발의한 「가짜정보 유통방지에 관한 법률안」과 자유한국당 김성태 의원이 대표발의한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」이다. 「가짜정보 유통방지에 관한 법률안」은 가짜정보를 "정부기관 등(언론중재위원회, 법원, 선거관리위원회 등)에서 명백하게 그 내용이 사실이 아니라고 판단한 정보"로 규정하고, 방송통신위원회가 가짜정보의 내용을 공고하도록 하며, 가짜정보 등 타인의 권리를 침해하는 정보를 생산한 자는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처할 수 있고, 정보통신서비스 제공자에게 가짜정보에 대한 모니터링 및 차단 의무를 지우는 것을 골자로 하고 있다. 김성태 의원의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」은 "정치적 또는 경제적 이익을 위하여 고의로 거짓 또는 왜곡된 사실을 언론보도로 오인하게 하는 내용의 정보"를 정보통신망법 제44조의7의 불법정보에 추가하여 유통을 금지할 수 있도록 하고, 이를 유통한 자에 대해서는 7년 이하의 징역 또는 7천만원 이하의 벌금에 처할 수 있도록 하며, 역시 정보통신서비스 제공자에게 모니터링, 임시조치, 차단 의무를 부과하고 있다. 다른 허위정보 관련 법안들도 이들과 크게 다르지 않다. 전체적으로 규제 대상 정보를 "정치적 또는 경제적 이익을 위한", "거짓의 사실 또는 왜곡된 사실"이라고 정의하고 있으며, 일부는 "언론보도로 오인하게 하는 내용의 정보" 등으로 한정하고 있다. 허위정보에 대한 제재, 조치들도 대체로 유사하게 규정되어 있다.

2) 국제 기준 및 동향

허위정보 규제 찬성론 측에서는 독일의 「네트워크 집행법」(NetsDG)을 허위정보 규제법이라고 인용하고 있다. 이 법안은 독일법상 '불법'정보에 대하여 사법부의 판단 전에도 소셜네트워크 서비스 제공자가 신고를 받아 삭제·차단할 의무를 부과하는 것을 골자로 하고 있다. 그러나 독일법도 정보 내용의 '허위성'만을 이유로 '불법'정보로 분류하는 규정은 없다. 독일 언론에서 문제삼는 허위정보는 주로 독일 형법 제130조 '대중선동죄'[186]에 해당하는 정보, 즉, '특정 집단에 대한 차별·폭력을 선동하는' 정보를 의미한다. 따라서 독일의 「네트워크집행법」은 이러한 특정 집단에 대한 차별·폭력을 선동하는 허위정보에 대한 문제의식을 기반으로 이를 보다 적극적으로 규제하기 위해 만들어진 법안이라 할 수 있고, 이는 허위정보에 대한 규제가 아니라 '혐오표현'에 대한 규제라고 보아야 한다. 나아가 사업자에게 일반적인 모니터링 의무를 부과하고 있지는 않고, '신고'가 되어 사업자가 구체적으로 인지한 특정 정보가 불법으로 판단되는 경우에야 비로소 삭제할 의무를 부과하고 있다. 이마저도 표현의 자유를 침해하는 위헌적인 법률이라는 비판과 논란이 끊이지 않고 있다.[187]

말레이시아 의회는 2018. 8. 가짜뉴스를 유포하거나 작성한 자를 처벌할 수 있도록 한 '가짜뉴스 처벌법'을 폐지했다. 본 법안이 언론을 탄압하고 정권에 대한 비판을 가로막는 수단으로 악용된다는 점을 고려한 것이다.[188]

2018. 11. 프랑스 하원이 통과시킨 것으로 알려진 '정보조작대처법'(Les propositions de loi

186) 독일형법 제130조 '대중선동죄'는 '공공의 평온을 어지럽히는 방식으로, 국적, 인종, 종교, 그 민족적 출신에 따라 특정되는 집단에 대하여… 증오를 불러일으키거나 이에 대한 폭력적 또는 자의적 조치를 유발하는 자'를 처벌하는 내용이다. 국회입법조사처, 「현안보고서」 제306호, "혐오표현 규제의 국제적 동향과 입법과제"(2017. 6. 12.), 19-21면 참조

187) 언론중재위원회, 해외언론법제연구보고서 제1권 제1호, 2018. 8. pp. 68-69 참조.

188) 국민일보, 2018. 8. 18.자 "결국 폐지된 세계 최초의 '가짜뉴스 처벌법'" 기사.

contre la manipulation de l'information)은 선거기간동안 투표의 진정성에 영향을 미칠 수 있는 허위정보가 고의로, 그리고 대량으로 유포된 경우, 판사가 명령으로 이를 중지시킬 수 있다는 내용을 담고 있다. 선거에 있어 유권자의 의사형성이 왜곡되지 않도록 한다는 목적의 범위 내에서, 사법부의 판단으로 허위정보의 유포를 중지시키도록 하고 있는 것인데, 이 역시 표현의 자유를 침해한다는 비판이 이어지고 있다.[189]

2018. 1. EU 집행위원회는 HLEG(the High Level Expert Group)라는 전문가 자문기구를 발족하고, 가짜뉴스와 온라인 허위정보에 대한 정책 및 대응 방안을 자문했다. 이에 따라 HLEG가 발행한 보고서[190]에서는 어떤 형식으로든 공적·사적 '검열'의 방식은 지양되어야 하며, 단기적 대응보다 장기적 대응을 모색해야 한다고 강조하고 있다. 대신 ① 온라인 뉴스의 투명성을 향상, ② 미디어 리터러시 함양, ③ 이용자와 언론이 허위정보에 제동을 걸 수 있는 장치 마련, ④ 뉴스 미디어 생태계의 다양성과 지속성 보장, ⑤ 허위정보의 영향력과 조치에 대한 지속적 연구 장려를 주요 대응책으로 제시하고 있다.

한편 2017. 3. 3. 표현의 자유에 관한 유엔 인권 특별보고관은 가짜뉴스 대응에 관한 공동 성명에서 정부의 가짜뉴스 규제는 표현의 자유를 침해할 위험이 높음을 지적하며, 정부의 역할은 보다 다양하고 신뢰할 수 있는 정보들이 더욱 자유로이 유통될 수 있는 환경을 조성하는 것임을 강조하였다.[191]

제4절 온라인 표현의 자유 증진을 위한 개선방안

1. 방송통신심의위원회의 통신심의 제도의 폐지 혹은 개정

국가기관, 정부에 의한 온라인 표현물 규제는 지양되어야 한다는 것이 국제인권기준이자 다수 전문가들의 의견이다. 현재 방송통신심의위원회의 통신심의 제도는 행정기관인 방송통신심의위원회가 수행한다는 데에 가장 문제가 있다. 헌법적으로 표현물에 대한 행정검열이 금지되는 가장 근본적인 이유는 사법부가 아닌 국가기관에 의한 심의는 정치적 영향력에서 자유로울 수 없기 때문이다. 즉, 행정기관은 태생적으로 국가권력의 영향력 하에 있고, 행정기관의 표현물 심의는 정부에 비판적인 합법적인 표현물들을 억제하고 여론을 통제하기 위해 남용될 위험이 높기 때문에 헌법적으로 금지되는 것이다. 특히 방송통신심의위원회 위원은 대통령이 위촉하고 3인은 국회의장이, 3인은 국회의 소관 상임위원회에서 추천한 자를 위촉하게 되어 있는데, 이는 사실상 정부, 여당 추천의 위원이 3분의 2를 차지하여 의사결정권을 쥐는 구조를 가지고 있다. 이 때문에 정치 심의가 행해질 위험이 높고, 이러한 우려는 전술한 바와 같이 실제 문

189) 슬로우뉴스, 2018. 11. 21자 "프랑스 '정보조작대처법', 결국 통과되다" 기사.

190) "A multi-dimensional approach to disinformation - Report of the independent High level Group on fake news and online disinformation" (European Commission, March 2018) https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation (2019. 11. 13. 최종접속)

191) JOINT DECLARATION ON FREEDOM OF EXPRESSION AND "FAKE NEWS", DISINFORMATION AND PROPAGANDA https://www.law-democracy.org/live/wp-content/uploads/2017/03/mandates.decl_.2017.fake-news.pdf (2019. 11. 13. 최종접속)

제 사례에서도 드러난 바다.
정보의 '불법' 여부와 이를 기준으로 국민의 기본권을 제한할 것인지 여부는 종국적으로 사법부의 판단에 따라 결정되어야 하는 부분이다. 법률 전문가들로 구성되지 않은 위원회가 고도의 법률적 판단이 필요한 '음란', '명예훼손', '국가보안법 위반' 여부 등을 판단하는 것은 그 자체로 큰 오류가능성, 즉 합법적인 표현물의 유통을 금지시킴으로써 표현의 자유와 알 권리를 침해할 위험이 높게 존재한다.
나아가 현 제도는 국가기관이 '유해정보'를 그 심의 대상에 포함시키고 있어 그 위헌성을 가중시킨다. 헌법재판소도 판시한 바와 같이, 국가가 유해성에 대한 막연한 의심이나 유해의 가능성만으로 표현물의 내용을 광범위하게 규제하는 것은 표현의 자유와 조화되기 어렵다. 다원성과 가치상대주의를 이념적 기초로 하는 민주주의 사회에서 상대적이고 가변적인 개념을 잣대로 표현의 허용 여부를 국가가 재단하게 되면 언론과 사상의 자유시장이 왜곡되고, 정치적, 이데올로기적으로 악용될 우려가 있다. 민주주의에서 어떤 표현이나 정보의 가치 유무, 해악성 유무를 국가가 1차적으로 재단하여서는 아니 되고 시민사회의 자기교정기능, 사상과 의견의 경쟁메커니즘에 맡겨야 한다[192]. 따라서 현재와 같이 방송통신심의위원회가 정보의 '유해성'이라는 막연한 기준으로 정보의 전면적인 삭제, 차단을 결정하는 것은 위헌의 소지가 크다.
이러한 문제와 위헌성을 극복하고 국제기준에 부합하도록 하기 위해서는, UN 표현의 자유 특별보고관과 2010년 국가인권위원회의 권고대로 방송통신심의위원회 통신심의 권한을 폐지하고 정보통신 서비스 제공자 및 시민사회 대표 등이 함께 구성하는 민간자율심의기구로 이양하여야 한다.
방송통신심의위원회의 통신심의 기능을 그대로 두고 제도 단계적인 제도 개선을 꾀할 경우에는, 적어도 '건전한 통신윤리의 함양을 위하여 필요한 경우'나 '유해정보'와 같은 추상적이고 불명확한 심의 기준은 개정되어야 한다. 유해정보에 대한 심의는 '청소년유해정보'로 구분하여 세밀화, 구체화하고, 이러한 청소년유해정보에 대해서는 전면적인 삭제, 차단의 시정요구가 아니라 청소년유해정보 표시의무나 접근제한 조치만을 시정요구 할 수 있도록 명확히 구분하여야 한다.
불법정보 심의 역시, 근본적으로는 현재 지나치게 포괄적이고 광범위한 심의 대상 정보를 축소시켜 행정력을 집중시키고 신중한 심의를 도모하는 것이 바람직하다. 행정기관이 선제적으로 개입하여 차단하여야 하는 정보는 국민의 신체, 재산에 명백하고 급박한 위해를 가할 위험이 있는 불법정보만을 그 대상으로 한정하여야 하는 것이 바람직하다. 이러한 정보의 심의와 함께 수사기관과의 공조를 통해 운영자, 유포자를 형사처벌하여 근원적 해결을 모색하는 것이 더 실효성도 있다. 예를 들면 현재 정보통신망법 제44조의7 제1항에서 방송통신위원회, 방송통신심의위원회가 규제할 수 있는 불법정보로 규정되어 있는 '음란' 정보는 아동청소년 이용 음란물이나 성폭력처벌특례법상 디지털 성폭력물로 한정하고, '명예훼손', '국가보안법 위반', '기타 범죄 조장 정보' 등 해악이 중대·명백하지 않거나 고도의 법률적 판단이 필요한 정보는 삭제하는 것이다. 이러한 불법정보에 대해서는 사법기관의 판단에 따른 조치를 도모하는 것이 바람직하고, 법원 명령, 가처분 결정 등이 신속하게 내려질 수 있는 제도의 보완을 통해 이루어지도록 하는 방향을 검토해야 한다.

2. 임시조치 제도의 개정

---

192) 헌법재판소 2002. 6. 27. 결정, 99헌마480.

임시조치는 위 문제 사례에서 보았듯이 상당수가 기업의 소비자불만글 억제를 위하여, 혹은 공인에 대한 의혹제기를 억제를 위하여 이루어지고 있는 것으로 보인다. 공인에 대한 정당한 비판이나 소비자로서 할 수 있는 기업의 제품이나 서비스에 대한 평가까지도 그 위법성과 무관하게 임시조치 당함으로서 표현의 자유와 알 권리에 대한 심각한 침해를 일으키고 있다.
현행 임시조치 제도의 구조는 사실상 신고를 받은 모든 권리침해 정보에 대하여 인터넷 서비스 제공자(정보매개자)에게 차단 의무를 부과하고 있기 때문에 더욱 과검열을 조장하며 표현의 자유와 알 권리를 균형적으로 보호하지 못하고 있는 측면이 있다. 정보매개자책임 규제가 국제기준에 부합하려면 기본적으로 '세이프 하버(safe harbor)' 방식을 채택하여 정보매개자가 특정 불법정보의 존재를 알지 못하였거나 미국의 저작권법(DMCA) 제512조의 노티스앤테이크다운(Notice and Takedown)과 같은 제도를 시행하는 한 제3자가 제공한 정보에 대하여 책임을 지지 않는다는 책임면제조항을 규정하는 선이어야 한다. 즉, ① 서비스 제공자는 피해주장자의 요청이 있을 때 그 게시물을 차단하면 그 게시물 유통에 대한 책임을 면제받고, ② 게시자가 복원을 요청하는 경우 복원하면 차단 조치에 대해서도 면책을 받으며, ③ 재게시 이후의 분쟁에 대해서는 당사자간의 소송으로 다투도록 하는 것이다. 즉, 서비스제공자가 각 게시물의 합법성을 일일이 판단하지 않고 게시자와 피해주장자의 요청을 그대로 따라 줌으로써 게시자와 피해주장자 양측으로부터 면책을 받도록 하는 것이다. 이러한 조치는 의무사항이 아니라 기본적으로 정보의 유통 여부를 서비스 제공자의 판단에 맡기되, 조치를 시행했을 경우에는 면책하도록 함으로써 판단에 대한 부담을 경감하는 것이다. 이 경우 권리침해의 불법성이 명백한 정보에 대한 신속한 조치를 하고자 하는 입법목적도 달성할 수 있을 뿐 아니라, 게시자들의 신속한 복원권을 보장하고 서비스 제공자의 유연한 판단도 가능케 함으로써 표현의 자유와 알 권리도 보다 균형적으로 보장할 수 있게 된다. 이러한 국제 기준에 따른 구조를 고려하면, 현행 임시조치는 제도는 의무조항이 되어서는 안 되며, 게시자의 이의제기시의 복원권이 보장되어야 한다. 현재의 본조 제2항의 "삭제, 차단하여야 한다"는 의무부과형 문구를 "~할 경우 책임이 면제된다"는 면책형으로 개정할 필요가 있다.
가장 큰 임시조치 제도의 문제로 지적되는 점은 기업과 공인에 의한 남용 가능성과 게시자의 복원권이 제대로 보장되어 있지 않다는 것이다. 기업이나 공인에 의한 남용 가능성을 최소화하기 위하여는 신고자 적격에 제한을 두거나, 사안을 '사생활 침해' 등으로 한정, 축소하는 방향을 고려해볼 수 있다. 또한 본조 제4항에서 '권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 정보'까지 모두 임시조치 대상 정보로 포섭시킴으로써, 기업이나 공인과 관련한 공익성이 높은 정보들까지 포괄적으로 삭제, 차단의 대상이 되고 있는바, 이 제4항은 반드시 삭제될 필요가 있다. 한편 게시자의 이의제기시에는 임시조치를 즉시 해제하고 이에 대해 신고자가 다시 다투고자 하는 경우 분쟁해결절차가 진행되도록 하여 표현의 자유를 보다 증진하는 방향으로 개정할 필요가 있다.

3. 공직선거법상의 실명제와 선거관리위원회 삭제명령제도 폐지

익명이나 가명으로 이루어지는 표현은 외부의 명시적·묵시적 압력에 굴복하지 아니하고 자신의 생각과 사상을 자유롭게 표출하고 전파하여 국가권력이나 사회의 다수의견에 대한 비판을 가능하게 하며, 이를 통해 정치적·사회적 약자의 의사 역시 국가의 정책결정에 반영될 가능성을 열어 준다는 점에서 표현의 자유의 내용에서 빼놓을 수 없다. 인터넷 공간에서 이루어지는 익명표현은 인터넷이 가지는 정보전달의 신속성 및 상호성과 결합하여 현실 공간에서의 경

제력이나 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 보호될 필요가 있다.[193] 한편, 정치적 표현에는 정치적 보복이나 차별의 위험이 따르기 때문에 다른 표현보다 익명표현의 자유는 더욱 강하게 보호받아야 한다. 즉, 정치적 보복이나 차별의 두려움 없이 자신의 생각과 사상을 자유롭게 표출하고 전파하여 권력에 대한 의혹제기와 비판을 가능하게 할 수 있으려면 익명이나 가명으로 하는 표현은 더욱 자유롭게 허용되어야 하는 것이다. 투표나 선거와 같은 대의민주주의의 가장 기본적인 의사표현은 익명성의 보장을 핵심으로 하고 있다. 위 공직선거법 조항에 대한 헌법재판소 결정의 반대의견에서는, '헌법이 비밀선거 원칙을 규정한 취지에 비추어 보면, 투표 시뿐만 아니라 투표 전에 이루어지는 정치적 의사표현에 있어서도 의사표현자의 신원에 대한 비밀이 보장될 필요가 있다. 정치적 외압 가능성은 투표 행위에 대해서만 존재하는 것이 아니며, 선거와 관련한 여론 형성을 일정한 방향으로 왜곡하거나 유도하기 위해 나타날 수도 있기 때문이다. 따라서 선거운동에 있어서 정치적 익명표현의 자유는 비밀선거 원칙을 규정한 헌법정신에 비추어도 그 보호 필요성이 인정된다.'고 설시하였다.

그런데 실명제는 게시판 이용자의 표현의 자유를 사전에 제한하여 의사표현 자체를 위축시킴으로써 자유로운 여론의 형성을 방해한다. 즉, 실명제는 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 제한이라는 것이 헌법재판소의 기본적 의견이다.[194]

나아가 인터넷 실명제의 위헌 이유 중 하나는 실명제(본인확인제) 시행 이후에 명예훼손, 모욕, 비방의 정보의 게시가 표현의 자유의 사전 제한을 정당화할 정도로 의미 있게 감소하였다는 증거를 찾아볼 수 없다는 것이었다. 또한 공직선거법 조항에 대한 헌법재판소 결정의 반대의견에서도, '선거운동기간 중에 인터넷 게시판 등에서 이루어지는 실명확인제가 흑색선전을 막기 위한 실효성 있는 수단이라고 볼 수 있는지도 의문'이라고 하며, '선거후보자에 대한 흑색선전은 단순한 후보자 비판의 문제가 아니라 치밀한 사전계획에 입각하여 조직적으로 이루어지는 것이 일반적이므로, 인터넷 실명제로 막기 어려운 불법행위이다. 공정한 선거를 해치는 악의적 의사표현은 선거를 둘러싼 정치적·사회적 상황의 여러 조건들이 변수로 작용하여 나타나는 것이지, 익명표현을 허용함에 따라 발생하는 문제라고 볼 수 없다. 정당한 익명표현과 유해한 익명표현을 구분하는 명확한 사회적 합의를 도출하기 어려운 상황에서, 책임 있는 의견이 개진되거나 위법한 표현행위가 감소될 것이라는 추상적 가능성만으로 유해한 익명표현뿐만 아니라 유익한 익명표현까지 사전적·포괄적으로 규제하는 것은 정치적 의사표현을 위축시켜 선거의 공정이라는 입법목적 달성에 오히려 장애가 된다.'고 설시한 바 있다. 또한 인터넷을 이용한 선거범죄에 대하여는 명예훼손죄나 후보자비방죄 등 여러 사후 제재수단이 이미 마련되어 있어 예방적 효과도 확보하고 있다. 수사편의 및 선거관리의 효율성이라는 기술적 편리성에만 치우쳐 사전적·예방적 규제를 통하여 익명표현 자체를 제한하는 것은 국민을 잠재적 범죄자로 취급하는 것으로 침해의 최소성 원칙에도 위반된다.

---

193) 헌재 2012. 8. 23. 2010헌마47.
194) 위 헌법재판소 결정.

선거운동기간이 정치적 표현의 자유를 행사함에 있어 가장 긴요한 시기라고 볼 수 있는 점과 표현의 자유 보장이 민주주의의 근간이 되는 중요한 헌법적 가치라는 점을 고려할 때, 익명표현의 자유를 제한하는 데 따르는 불이익이 선거의 공정성 유지라는 공익보다 훨씬 크다고 할 수 있어 법익균형성에도 위반되는 것으로 볼 수 있다. 이러한 헌법과 국제법상의 인권 보호 정신에 따라, 표현의 자유와 알권리, 개인정보자기결정권을 침해하는 공직선거법상의 인터넷 실명제는 폐지되는 것이 바람직한 방향일 것으로 보인다.

선거관리위원회의 선거법 위반 정보 삭제명령 제도 역시, 이와 같은 선거기간 중 국민의 정치적 표현의 자유 보장의 중요성에 비추어 재검토해야 한다. 민주주의를 가장 직접적으로 실현하는 수단인 선거기간에는 정당 및 후보자에 대한 의혹제기와 검증, 의견 교환이 어느 때보다 더 자유롭고 활발하게 이루어져야 하는 시기다. 이러한 시기에 단순한 가치판단이나 의견표현, 후보자들에 대한 자질 검증을 위한 다양한 비판 및 의혹을 제기하는 표현물들에 대하여 사법기관의 선거법 위반 여부 판단이 내려지기도 전에 선거관리위원회의 판단만으로 일방적으로 삭제할 수 있도록 하는 것은 유권자의 정치적 표현의 자유와 알 권리를 침해할 위험이 크다. 위에서 설명한 선거기간 동안 허위정보의 유통을 중지시키는 프랑스의 '정보조작대처법'에서도 적어도 규제기관이 아니라 '판사', '사법부'의 판단에 따른 조치를 규정하고 있고, 이 역시도 많은 비판이 이어지고 있음을 고려할 필요가 있다.

20대 총선 분석 결과를 보면, 선거관리위원회가 선거법을 다소 과도하게 적용하여 후보자에 대한 의혹제기, 부정적 평가, 이용자간의 단순한 선호도 투표에 대해서도 삭제 명령을 내린 사례가 다수 발견되었다. 또한 특정 지역에서 특정 후보에 대한 게시물이 집중적으로 삭제된 것을 볼 때, 선거관리위원회는 후보자가 삭제 요청한 게시물들에 대해서 충분한 법적 판단 없이 대부분 수용하여 삭제 명령을 내리고 있는 것으로 보인다.[195] 이는 공직선거법 자체가 선거기간 표현의 자유를 지나치게 제한할 수 있는 조항이 많아 후보자에 대한 비판적 게시물이라면 대부분 선거법 위반의 정보로 판단될 수 있기 때문이기도 하다. 공직선거법 전반에 대한 검토와 더불어, 선거관리위원회에 이러한 광범위한 단속 권한을 부여한 공직선거법 제82조의4에 대한 폐지나 개정이 필요하다.

4. 사실적시 명예훼손죄와 모욕죄의 폐지

사실적시 명예훼손죄는 타인의 사회적 평가를 저하시킬만한 발언이라면 '진실', '허위'를 불문하고 일단 모두 형사범죄를 구성할 수 있게 함으로써, 그 형벌조항의 존재 자체로 인하여 표현의 자유에 대한 엄청난 위축효과를 발생시킨다. 적시된 사실이 허위이든 진실이든, 명예훼손죄의 구성요건에는 일단 모두 해당되기 때문에, 명예훼손 고소를 하는 사람은 자신에 대해 적시된 사실이 '허위'임을 구체적으로 입증할 필요가 없으며, 피고소인은 자신이 공표한 사실이 '진실'임을 증명하여도 피의자 신분을 당장 벗어날 수 없다. 진실한 사실을 고발한 사람들이 이처럼 명예훼손으로 역고소를 당하고 형사범죄의 피의자, 수사 대상이 되어 또 다른 피해와 고통을 겪게 되고, 사람들은 이와 같은 위험을 부담스러워하여 진실한 사실을 말하는 것을 스스로 억제하게 된다.

'공공의 이익을 위한 적시'의 경우 위법성을 조각하는 조항이 있다고 하더라도 이는 수사단계에서는 적극적으로 검토되지 않고 보통 기소/불기소 혹은 유죄/무죄 판단에 이르러서야 진지

195) 참여연대이슈리포트, '선관위의 인터넷 게시물 삭제 내역 조사보고서' (2016. 10. 4.)

하게 고려된다. 사후에 위 요건들에 대한 판단이 제대로 이루어져 불기소 결정이나 무죄 판결이 내려진다고 하더라도, 처벌가능성을 사전에 실질적으로 제한할 수 있는 장치가 없기 때문에 명예훼손죄에 대한 고소의 남발은 제한될 수 없고, 고발자가 상대방으로부터 고소를 당하여 형사범죄의 피의자가 되어 수사를 받는 위험으로부터 보호할 수 없다. 즉, 사실적시 명예훼손죄를 형사범죄로 구성하는 조항이 있는 한, 위의 사전적인 폐해를 방지하기 어렵다.

또한 '공익 목적'이라는 위법성 조각사유가 무용한 것은 그 개념의 불명확성, 추상성 때문이기도 하다. '공공의 이익을 위하여'라는 요건 개념은 판단자의 주관에 따라 달라질 수 있는 불명확하고 추상적인 개념으로써, 죄의 성부를 가늠할 수 있는 척도가 되지 못한다. 정보통신망법상의 사이버 명예훼손죄의 구성요건인 '비방의 목적' 여부 판단에 있어서도 결국 공익 목적의 유무를 기준으로 판단하고 있는데, 이 추상성으로 말미암아 한 가지 사례에 관해서도 재판부에 따라 다른 결론이 나오는 경우도 많다. 12년 전 미투 운동과 유사한 사안에서, 대법원은 '학내 성폭력 사건의 철저한 진상조사와 처벌 그리고 학내 성폭력 근절을 위한 대책마련을 촉구하기 위한 목적으로 공익의 이익을 위하여 한 것으로 봄이 상당하고, 달리 비방의 목적이 있다고 단정할 수는 없다'고 판시[196]하였으나, 이 사건의 원심 재판부는 '성폭력과 같은 범죄사실의 공표에 있어서 충분한 증거나 조사없이 가해자의 실명을 공개하며 공표하는 것은 공익 목적보다 비방 목적이 더 크다'고 하며, 대구 여성의 전화에 유죄를 선고했었다. 이들 사례는 죄의 성부를 가르는 '공익 목적', '비방 목적'이라는 개념이 법에 정통한 법관들조차 그 판단의 중점에 따라 각자 달리 해석될 수 있는 불명확한 개념임을 보여주는 사례이다.[197]

사실적시 명예훼손죄로 인하여 유독물질이 나온 식품, 화학제품, 비위생적 식당, 의료사고가 난 병원 등에 대한 보도는 유권기관의 판단이 나오기 전까지는 일단 익명보도를 하는 것이 원칙적인 모습이 되었고, 국민들은 해당 업체의 실명을 몰라 두려움에 떨어야 한다. 뿐만 아니라 같은 업종에 종사하는 선량한 업체나 사람들이 억울하게 피해를 보거나 의심을 받아야 한다.[198] 진실을 적시함으로 인하여 침해받는 '명예'는 처음부터 그 사람이 가질 자격이 없는 명예, 즉 '허명'으로 볼 수 있는데, 이를 보호하기 위하여 폭로자, 제3자, 국민의 권리와 법익들을 희생시키는 사실적시 명예훼손죄는 법익 균형성에도 위배하고 있다고 볼 수 있다.

결론적으로 사실적시 명예훼손죄는 헌법상 비례의 원칙에 위반하여 표현의 자유와 형사처벌에 잇따르는 국민의 제 기본권을 침해할 위헌의 소지가 높은 조항이며, 위에서 검토한 국제기준과 권고에 따라 폐지를 고려하여야 한다. 과거 성이력과 같이 타인의 프라이버시를 침해하는 사실을 적시하는 것을 제재하기 위해 본 죄를 유지해야 한다는 반론이 있다. 그러나 이와 같은 개인의 프라이버시 침해 역시 기본적으로는 민사상 불법행위 손해배상 영역에서 해결되어야 하는 문제이며, 국가형벌권의 행사가 1차적으로 개입하여야 하는 영역으로 보기 어렵다. 그럼에도 불구하고 국민 법감정 등을 고려하여 이에 대한 형사처벌 조항이 유지될 필요가 있다면, '명예'를 보호법익으로 하는 것이 아닌 헌법 제17조상의 '사생활의 비밀과 자유'를 보호법익으로 하여, 이를 침해하는 사실을 적시한 경우에 처벌하는 조항을 신설하는 것을 고려할 수 있을 것이다.

모욕죄의 경우, 구체적인 사실의 적시가 없더라도 '사람의 사회적 평가를 저하시킬 만한 추상적인 판단이나 경멸적 감정'을 표현하는 것을 형사처벌하고 있다. 그러나 이러한 '모욕'은 형

196) 대법원 2005.4.29, 선고 2003도2137 판결.

197) 손지원, "사실적시 명예훼손죄의 제도 개선 방향", (2018. 12. 11. 방송통신위원회, 국회 이철희 의원실, 한국법제연구원, 한국형사정책연구원 공동주최 '사이버 명예훼손 제도 개선 토론회'의 토론문)

198) 박경신, "진실적시에 의한 명예훼손 처벌제도의 위헌성",「세계헌법연구」제16권 제4호, 2010, 1-29면.

사범죄의 구성요건임에도 추상적이고 불명확하여 판단자의 주관에 따라 크게 달라질 수 있는 개념이며, 일반인, 심지어 판사조차도 어떤 표현이 모욕적인지 아닌지를 명확히 판단하기 어렵다. 몇 개의 모욕죄 판례들을 보더라도 타인에 대한 부정적인 의사표시에 대해 모욕죄를 인정하는 분명한 기준이나 일관성을 찾기 어렵다. 또한 구체적인 사실의 왜곡이 아닌 개인의 감정 표현만으로는, 표현 대상이 된 타인의 사회적, 외부적 평가에 구체적인 위해를 끼치기 어렵다. 이렇듯 명백, 현존하는 위험이 있다고 볼 수 없는 일상적이고 경미한 행위를 형사처벌 대상으로 삼고 있는 모욕죄는 헌법상 죄형법정주의, 명확성 원칙, 헌법상의 비례의 원칙에도 위배할 소지가 높고, 국제기준에도 어긋나는 조항으로써 폐지를 검토할 필요가 있다.

5. 혐오표현에 대한 대응

혐오표현 규제에 대한 국제인권조약과 유럽을 중심으로 한 각국의 규제입법이 존재하지만, 혐오표현의 구체적인 정의에 대해서 이를 명시하는 경우는 드물고 국제사회의 보편적 합의가 있다고도 보기 어렵다. 해외의 학계에서도 마찬가지이다. 이는 '혐오(hate)' 혹은 '적대적' 표현이 가지는 의미의 복잡성, 기존의 표현내용규제의 대상이 된 표현행위들과의 차별성 여부, 혐오표현의 문제점을 인식하는 각 국가 및 사회의 역사적 배경과 경험의 다양성으로 인해 그 개념정의가 쉽지 않기 때문이다.[199] 우리나라에서도 혐오표현에 대한 규제 필요성에 대해서는 대체로 공감대가 형성되어 있으나, 그 기준과 범위에 대해서는 논의가 분분하다.

'혐오표현'의 개념은 필연적으로 불명확성과 추상성을 내포할 수밖에 없는데, 이것이 바로 규제의 한계이자 규제 도입시 가장 숙려하여야 할 부분이다. '규제가 필요한 혐오표현'이 어디까지인지를 명확히 한계짓지 않고 규제를 도입하여 자칫 집단에게 모욕감을 주는 모든 유해하고 불쾌한 차별·비하적 표현을 규제하게 되면, 표현의 자유를 지나치게 침해하는 결과가 발생하거나 사회 구성원의 반발심을 촉발하여 오히려 사회의 분열로 이어질 위험도 있다.

우선 혐오표현 중 중대한 해악을 불러일으키는 혐오표현, 즉 규제가 필요한 혐오표현은 무엇인가에 대한 심도 있는 고찰이 필요하다. '집단이 느끼는 모욕감'이나 '사회분열'과 같은 해악은 혐오표현을 규제할만한 명백하고 현존하는 위험으로 보기 어렵다. 혐오표현의 해악은 사회 전체에 대해 표적집단(혐오표현의 대상 집단)에 대한 차별과 적의를 확산시킬 뿐만 아니라, 표적집단 구성원 개인에게 불안과 공포를 상기시키는 방식으로 개인의 존엄성을 침해하고, 이로써 공론장에서 표적집단 구성원의 표현행위와 영향력을 위축시켜, 사회의 표적집단에 대한 배제와 차별의 공고화로 이어진다는 데에 있다.[200]

이러한 혐오표현의 해악과 규제 이유에 비추어 볼 때, 규제 대상 혐오표현을 정의함에 있어서 우선 표적집단은 사회적 소수자 집단이 되어야 할 것이다. 혐오표현으로 인해 실제 사회에서 그 집단에 속한다는 이유만으로 배제, 차별, 폭력의 대상이 될 수 있고, 이에 대하여 구체적인 불안, 공포, 위축을 경험할 위험이 높은 집단이 그 대상이 되어야 한다. 혐오표현 정의 규정은 흔히 "국가, 인종, 민족, 종교, 성별, 성적 지향, 장애를 이유로"의 문구를 사용하고 있다. 이러한 분류 및 한정도 필요하지만, 이 문구만을 기준으로 할 경우 위에서 설시한 바와 같이 규제가 필요한 범위를 넘어 지나치게 광범위한 표현물, 즉, 사회에서 주류적 지위를 차지하거나 차별, 배제, 공포, 위축의 위험이 거의 없는 국가, 인종, 종교, 성별 집단 등에 대한 표현마저

199) 이승현, "혐오표현 규제에 대한 헌법적 이해",「공법연구」제44집 제4호, 한국공법학회, 2016. 6.
200) 이승현, 앞의 논문 참조.

규제 대상이 될 수 있다는 문제가 생길 수 있다. 물론 '사회적 소수자'라는 기준도 상대적인 개념으로써 불명확성을 안고 있어 이를 어떻게 법문언에 녹여낼지에 대한 심층적 연구가 필요할 것이다.
또한, 표현의 정도에 있어서도, 단순한 '차별·비하'나 '모욕감, 불쾌감'을 불러일으키는 표현이 아니라, 표적집단 구성원에게 불안, 공포, 위축을 불러일으키고, 실제 사회에서 실제적인 배제, 차별, 폭력으로 이어질 위험이 있는 표현을 규제 대상으로 설정하여야 한다. 최소한 '차별, 적의 또는 폭력을 선동하는' 내용이어야 하며, 이는 앞서 설시한 UN 자유권규약과 이에 대한 특별보고관의 해석에서도 제시된 기준이다. 보다 구체적으로는 국제인권단체 아티클19이 제시하고 있는 심각성 요건, "화자가 청중들로 하여금 차별, 적의, 폭력을 일으키도록 하고자 하는 구체적인 선동의 의도가 있었을 것", 그리고 "그 결과로 청중이 실제로 선동되어 금지 행위에 가담할 높은 임박한 위험이 있을 것"을 기준으로 고려할 수 있을 것이다.
한편, 역사부정과 연결된 혐오표현 역시, 그 혐오표현으로 인하여 유사한 사건이 재발할 위험, 혹은 역사적 사건의 피해자에 대한 사회의 실제적인 배제, 차별, 폭력으로 이어질 위험이 현재에도 지속되고 있는지를 심층적으로 분석, 연구한 뒤 규제 도입을 논해야 할 것이다.
규제의 수준과 관련하여서는, 실제적인 배제, 차별, 폭력 행위를 실행한 것이 아닌, 이를 발생시킬 수 있는 '가능성', '위험'을 내포한 표현을 하였다는 이유로 형사처벌을 규정하는 것은 지양되어야 한다. 국가 형벌권의 행사는 해악이 중대하고 명백한 행위에 한해서 최후의 수단으로 고려되는 것이다. 또한 위에서도 설시한 바와 같이 혐오표현 규제는 필연적으로 불명확성과 추상성을 내포하고 있기 때문에 형벌규정이 가져야 할 죄형법정주의가 요구하는 명확성의 정도를 충족시키기란 거의 불가능하기 때문이기도 하다.
혐오표현이 가지는 해악, 즉 소수자에 대한 사회의 실제적 배제, 차별, 폭력을 방지하기 위하여는, 혐오'표현'에 대한 규제보다는 이러한 실제적 배제, 차별, 폭력 행위의 금지를 국가가 천명하는 것이 더욱 효과적이며 중요하다. 포괄적 차별금지법의 제정 등을 통하여 이러한 행위들과 혐오범죄의 가중처벌을 법적으로 명시할 필요가 있다. 또한 표현은 의식의 발로일 뿐이므로, 표현 규제는 근본적으로 효용성에 있어 많은 한계를 가질 수밖에 없다. 따라서 무엇보다 언론, 시민, 소수자의 대항 표현이 활발하게 작동할 수 있는 환경을 지원하고, 차별적 인식 철폐 및 미디어 리터러시 교육의 강화를 꾀하는 진흥적 정책을 마련하는 것이 중요하다. 규제 대상 혐오표현의 명확하고 합리적인 기준 설정을 위하여 사회적 합의를 이끌어가는 것부터 이러한 혐오문화 대응 정책 마련까지 국가인권위원회와 같은 인권 전문 독립기구의 역할이 중요할 것이다.

6. 허위정보에 대한 대응

개인에 대한 허위사실 유포의 경우 우리나라는 이미 엄격한 명예훼손 법제와 공직선거법상 후보자에 대한 허위사실공표죄 등으로 규율되고 있다. 향후 딥페이크 기술 등을 이용한 개인의 인격권 침해 정보 문제 역시 이러한 현행 법제로 충분히 규율이 가능하다. 소수자 집단에 대한 허위정보를 제시하면서 차별, 폭력을 선동하는 정보도 규제 필요성이 있을 수 있으나, 이는 허위정보 규제가 아닌 혐오표현 규제의 맥락에서 논의될 문제이다. 결국 현재 일반적으로 논의되고 있는 허위정보 규제는 개인이나 집단에 대한 공격이 아니라, '사회질서를 혼란'하게 하거나 '공익을 해하는', 공적 사안에 대한 허위정보에 대한 규제다. 그러나 내용의 '허위성'만을 이유로 표현물을 규제하는 것은 법적 정당성이 없을뿐더러, 정치적으로 남용될 위험이 높

기 때문에 지양되어야 한다.
어떠한 표현 내에서 증명할 수 있는 '사실'과 '의견'을 구분하기도 어려울 뿐만 아니라, 맥락과 해석에 따라 의미가 달라질 수도 있다. 또한 어떠한 사실이 '허위'인지 '진실'인지에 대한 판단은 시간의 흐름에 따라 달라질 수 있다. 대게 일정한 사실의 주장자가 당시까지 해당 사실의 '존재'를 증명하지 못하면 '허위'로 분류되는 경우가 많은데, 사실의 존재는 증명하기 어렵거나 증거를 가진 측에 의하여 조작·은폐되어 끝내 증명하지 못하는 경우도 많다. 따라서 어떠한 사실이 진실인지 허위인지를 종국적으로 판가름하는 작업은 매우 어려운 일이기에 내용의 '허위성'만을 이유로 표현행위를 함부로 규제해서는 안 된다. 헌법재판소 역시 전기통신기본법 위헌소원에서 "허위사실이라는 것은 언제나 명백한 관념은 아니다. 어떠한 표현에서 '의견'과 '사실'을 구별해내는 것은 매우 어렵고, 객관적인 '진실'과 '거짓'을 구별하는 것 역시 어려우며, 현재는 거짓인 것으로 인식되지만 시간이 지난 후에 그 판단이 뒤바뀌는 경우도 있을 수 있다. 이에 따라 '허위사실의 표현'임을 판단하는 과정에는 여러 가지 난제가 뒤따른다"는 보충의견을 낸바 있다.
판단의 실질적 곤란함과 동시에 과연 누가 '판단자'가 될 것인가 역시 중요한 쟁점이다. 우리나라에서 논의되는 허위정보 규제는 대체로 국가 주도의 공적, 강제적 규제다. 국가권력이 '허위'와 '진실'을 구분하여 이를 기준으로 표현의 허용 여부를 결정하거나 허위 표현자를 색출하여 처벌하겠다는 내용이며, 이는 곧 헌법이 가장 경계하고자 한 국가의 표현물 '검열'과 다름없다. 역사적으로도 국가권력의 표현물 검열은 반정부적 여론을 차단하고 억압하는 수단으로 남용될 수 있기 때문에 민주국가에서는 금기시된다. 이와 같은 이유로 국제적으로도 허위정보 규제의 방식으로 국가 검열의 방식은 지양되어야 한다는 논의가 주류를 이루고 있다.
효용성 측면에서도, 무궁무진한 양과 질의 정보가 유통되는 인터넷의 특성상 일일이 정보의 가치를 따져 유통을 금지시키는 방식의 규제는 근본적인 한계를 가진다. 따라서 허위정보에 대하여 규제 만능주의로 접근하기보다는, 더욱 다양한 정보가 유통되어 경쟁할 수 있는 환경, 시민이 신뢰성 있는 정보를 더욱 많이 접할 수 있는 환경을 조성하고, 미디어 리터러시 교육의 강화와 팩트체크 시스템의 활성화 등의 방안을 강구하여야 할 것이다.

<끝>