

안녕하십니까? 먼저 여름으로 넘어가는 무더운 날씨에도 불구하고 2014년 정보인권 포럼에 참석해 주신 내빈 여러분께 감사의 말씀을 드립니다.

오늘날 정보통신 기술이 급격히 발달하면서 언제 어디서나 인터넷을 사용하여 필요한 정보를 취득할 수 있는 등 불과 몇 십년 전에는 상상할 수 없었던 일들이 현실이 되어가고 있습니다. 또한 우리나라는 인터넷이 도입된 지 불과 30여년이 지난 이 시점에 전 세계의 정보통신기술과 인터넷 기술을 선도하는 국가로 자리매김해 오고 있습니다.

하지만 급격한 기술의 발전은 세상에 편리함과 유익함만을 안겨주는 것은 아닙니다. 이러한 기술의 발전은 개인의 프라이버시권을 침해할 수도 있으며, 개인정보의 유출로 금전적 손해를 가져오기도 하고, 때에 따라서는 익명성에 의하여 개인에게 큰 상처가 될 수도 있습니다.

또한 다른 한편으로는 정부의 전자주민카드 도입 무산, 교육행정정보시스템 도입 갈등, 형사사법통합정보체계 도입 갈등 등 새로운 사회적 갈등을 발생시키기도 합니다. 이러한 과정 속에서 우리 헌법재판소는 정보주체가 스스로 결정할 수 있는 개인정보자기결정권을 헌법에 명시되지 아니한 독자적 기본권으로서 실시하며 헌법상의 기본권으로 인정하였습니다.

이렇듯 정보통신기술의 발전에 따른 개인정보자기결정권의 인정은 정보통신기술의 사용과 관련한 다양한 분야에서 인권적 접근이 필요하다는 것을 보여준 단적인 예라고 할 수 있습니다.

위원회는 그 동안 통신비밀보호법, 금융지주회사법 및 주민등록번호 제도 개선 등 정보인권 현안에 대하여 권고 및 의견표명, 2012년 정보인권을 주제로 약 50여개 회원국이 참여하는 아셈인권세미나 개최, 국내·외적으로 정보인권에 대한 다양한 논의를 종합한 정보인권보고서 발간 등 정보사회의 인권 기준 마련을 위해 지속적으로 노력해 왔습니다.

이러한 노력과 더불어 오늘 오전 우리 위원회는 한국인터넷기업협회와 MOU체결을 통하여 우리나라 정보통신 기업들의 사회적 책임과 정보인권 향상을 위해 서로 노력하기로 합의 하였습니다.

모두들 아시겠지만, 정보통신 분야에 있어 인터넷 포털 등 인터넷의 사회적 영향력과 중요성은 날로 증대되고 있습니다. 이러한 시점에 한국인터넷기업과의 업무협약은 우리 사회의 정보인권 보장을 위한 사회적 환경이 구축되는데 중요한 출발점이 될 수 있을 거라 생각합니다.

오늘 위원회는 정보통신서비스의 이용에 있어 개인정보자기결정권보장을 위하여 최근 국내·외에서 논의되고 있는 국가의 정보통신기업을 통한 감시, 본인확인과 개인정보 유출에 따른 개인정보자기결정권 보장, EU 사법재판소의 구글에 대한 판결과 잊혀질 권리 등에 관한 논의의 장을 마련하였습니다.

모든 하나 하나의 이슈들이 전 세계적으로 뜨거운 논의가 진행되고 있는 사안인 만큼 정보인권 보호를 위한 정책 마련을 위하여 정부, 기업, 관련 전문가들의 다양한 의견을 듣고자 합니다.

저는 여기 모인 여러분들의 고민과 토론이 개인이 자신의 가치에 걸 맞는 삶을 살아갈 수 있도록 하는 중요한 징검다리가 될 것이라고 믿으며, 이번 포럼을 계기로 많은 전문가들과 국민들이 정보인권과 관련하여 더 많은 관심을 갖게 되기를 바랍니다.

국가인권위원회에 많은 관심을 보여주시고 참석해주신 여러분들께 다시 한번 감사드리며, 오늘 포럼에 참석하신 모든 분들에게 정보인권과 관련한 좋은 기회가 될 수 있기를 기원합니다.

2014년 6월 10일

국가인권위원회 위원장 **현 병 철**

- 일시 : 2014. 6. 10.(화) 14:00 ~ 17:00
- 장소 : 프레지던트 호텔 모팰트홀(31층), 아이비홀(19층)

사회 : 박성훈 (국가인권위원회 인권정책과)

시간		내용 및 발표자
14:00 ~ 14:15		[인사 및 참석자 소개] - 축사 : 현병철 (국가인권위원회 위원장)
제 1 부	14:15 ~ 14:30	[통신자료 제공에 대한 국가인권위원회의 결정과 그 함의] 박성훈 (국가인권위원회 인권정책과) - 시연 : 국가의 통신자료 제공 요청 관련 영상(Google 사례) - 프리젠테이션 : 전기통신사업법 개정에 대한 권고 결정 내용 설명
	14:30 ~ 15:30	[국가기관에 통신자료 제공 현실과 제도개선] - 좌장 : 심상돈 (국가인권위원회 정책교육국장) - 발제 : 오길영 (신경대학교 경찰행정학과 교수) - 토론 : 이창범 (경희대학교 법무대학원 겸임교수) 유주성 (경찰교육원 교수) 권양섭 (군산대학교 법학연구원 교수) 최성진 (한국인터넷기업협회 사무국장)
15:30 ~ 15:50		중간 휴식
제 2 부	15:50 ~ 16:50	[제 1 세션 : 본인확인제의 현황과 정책적 방향] - 좌장 : 이석준 (국가인권위원회 인권정책과장) - 발제 : 김기창 (고려대학교 법학전문대학원 교수) 정민하 ((주)네이버 정책협력실 실장) - 토론 : 심우민 (국회입법조사처 조사관) 박찬욱 (방송통신위원회 개인정보보호윤리과) 박성훈 (국가인권위원회 인권정책과)
		[제 2 세션 : 구글 판결과 잊혀질 권리] - 좌장 : 조형석 (국가인권위원회 법제개선팀장) - 발제 : 이민영 (가톨릭대학교 법학부 교수) - 토론 : 지성우 (성균관대학교 법학전문대학원 교수) 양홍석 (법무법인 이공 변호사) 정혜승 (다음커뮤니케이션 대외협력실장) 구본권 (한겨레신문 사람과디지털연구소 소장)
16:50 ~ 17:00		각 세션 종합토론

제 1 부

■ 국가기관에 통신자료 제공 현실과 제도개선 1

발제 : 오길영 (신경대학교 경찰행정학과 교수) / 3

토론 : 이창범 (경희대학교 법무대학원 겸임교수) / 27

유주성 (경찰교육원 교수) / 31

권양섭 (군산대학교 법학연구원 교수) / 35

최성진 (한국인터넷기업협회 사무국장) / 43

제 2 부

■ 제 1 세션 : 본인확인제의 현황과 정책적 방향 45

발제 : 김기창 (고려대학교 법학전문대학원 교수) / 47

정민하 ((주)네이버 정책협력실 실장) / 53

토론 : 심우민 (국회입법조사처 조사관) / 63

박찬욱 (방송통신위원회 개인정보보호윤리과) / 73

박성훈 (국가인권위원회 인권정책과) / 75

■ 제 2 세션 : 구글 판결과 잊혀질 권리 77

발제 : 이민영 (가톨릭대학교 법학부 교수) / 79

토론 : 지성우 (성균관대학교 법학전문대학원 교수) / 115

양홍석 (법무법인 이공 변호사) / 117

정혜승 (다음커뮤니케이션 대외협력실장) / 123

구본권 (한겨레신문 사람과디지털연구소 소장) / 131

■ 정보인권 포럼_ 정보통신서비스 이용과 개인정보자기결정권 보장을 중심으로

국가기관에 통신자료 제공 현실과 제도개선

발제: 오길영 (신경대학교 경찰행정학과 교수)

토론: 이창범 (경희대학교 법무대학원 겸임교수)

유주성 (경찰교육원 교수)

권양섭 (군산대학교 법학연구원 교수)

최성진 (한국인터넷기업협회 사무국장)

통신데이터 남용의 실태와 그 쟁점



오길영 (신경대학교 교수, 정보통신법)

I. 들어가며

오늘날의 통신은 가히 디지털 일색이다. 편지는 이메일(e-mail)로, 전신은 MMS(Multi-media Message Service)로, 전화는 스마트폰(Smart Phone)으로 전환되어 이미 디지털 통신문화가 인류의 생활 속에 깊숙이 정착되어 있음은 물론, 통신기술에 있어서의 전송방식 또한 무전기 등의 특별한 분야를 제외하고는 이제는 아날로그 방식을 찾아내기가 힘든 상황이 되었다. 결국 지금의 ‘통신’이라는 말은 대체로 ‘디지털 통신’의 ‘준말’이라고도 할 수 있을 것이다. 한편 디지털 통신의 경우 아날로그 통신과는 달리 족적을 남긴다는 특징이 있다. 즉 현재 진행되고 있는 모든 종류의 통신은 모두 각각의 ‘통신데이터’를 남기고 있으며, 음성통신을 비롯한 각종의 디지털 통신들이 양산해내는 이 가공할 만한 양의 데이터를 ‘빅데이터(Big Data)’¹⁾라고 통칭하고 있음은 이미 주지의 사실이다. 따라서 이러한 본격 디지털 통신의 시대에 있어 통신데이터에 대한 규제와 정책의 중요성은 굳이 강조할 필요가 없을 것이다. 고도화된 통신네트워크 시대를 살아가는 현 인류의 ‘삶의 내용과 궤적’이 고스란히 통신데이터로 묻어나기 때문이다.

최근 필자는 통신데이터에 관한 중요한 두 가지의 뉴스를 접하게 되었다. 먼저 지난 5월 19일 ‘2013년 하반기 통신제한 및 통신사실확인자료 제공 현황’이 미래창조과학부에 의해 발표되었다.²⁾ 여기에는 집계된 통신제한조치, 즉 감청 통계와 통신사실확인자료 제공 통계, 그리고 통신자료 제공 통계(편의상 이하에서는 이 세 가지를 통칭하여 ‘통신데이터 제공’이라 칭함)가 각 항목별로 상세히 분석되어 있다. 그 결론만을 간단하게 요약해보자면, 통신제한조치 건수도, 통신사실확인자료의 제공 건수도, 통신자료의 제공 건수도 모두 전년 동기 대비 ‘증가’하였다는 것이 핵심이다. 씁쓸한 뉴스가 아닐 수 없다.

1) 이에 관한 상세는 오길영, “빅데이터 환경과 개인정보의 보호방안”, 일감법학 제27호, 건국대학교 법학연구소, 2014, 157-161쪽.

2) 미래창조과학부, “'13년 하반기 통신제한 및 통신사실확인자료 제공 현황”, 보도자료, 2014.5.20자.

〈표 1〉 2013 하반기 통신데이터 제공 총괄 현황³⁾

구 분		2012년		2013년	
		상반기	하반기	상반기	하반기
통신제한	문서건수	267	180	255	337 (87.2% 증가)
	전화번호수	3,851	2,236	3,540	2,492
	문서1건당 전화번호수	14.4	12.4	13.9	7.4
통신사실확 인자료	문서건수	119,306	120,002	133,789	132,070 (10.1% 증가)
	전화번호수	12,637,507	12,765,110	9,380,125	6,734,543
	문서1건당 전화번호수	105.9	106.4	70.1	51.0
통신자료	문서건수	395,061	425,739	465,304	479,623 (12.7% 증가)
	전화번호수	3,856,357	4,023,231	4,827,616	4,747,043
	문서1건당 전화번호수	9.8	9.5	10.4	9.9

통계의 내용을 간략히 분석을 해보자면, 지난 2년간 통신제한조치 허가서의 경우 1통의 허가서를 통해 대략 12개의 전화번호를 감청한 셈이 된다. 통신사실확인자료의 경우에는 83개, 통신자료의 경우에는 거의 10개에 이른다. 단순히 이 삼자만의 결과를 두고 보아도 통신사실확인자료의 남용에 대한 우려를 떨치기가 힘들다. 특히 지난해에만 대략 26만 5천 건의 제공이 있었으며 이를 위해 1600만 개의 전화 및 인터넷 등의 통신데이터가 제공되었다는 사실은 놀랍다. 또한 이러한 수치가 2500만 개의 통신데이터 제공이 있었던 2012년에 비해 그나마 감소된 것이라는 점은 심지어 공포스럽기까지 하다. 2500만 개라는 수치는 대한민국의 인구수를 5000만 명⁴⁾으로 잡을 때 2년에 한번 씩 전 국민을 풀-스캔 한다는 의미이며, 2년간의 평균치인 2000만 개를 기준으로 생각해보아도 3년이면 모든 대한민국 국민이 한번 이상 국가의 감시를

3) 이 표는 미래창조과학부, 앞의 보도자료, 1-11쪽의 표 내용을 참고하여 필자가 재구성한 것이다; 괄호 안은 전년도 동기 대비 증감률이다.

4) 이는 통계청의 추계인구수를 기준으로 삼았다: <http://kosis.kr/nsportalStats/nsportalStats_0102Body.jsp?menuId=1&NUM=1>, 검색일: 2014.6.3.

받는 셈이 된다. 이 결과는 2014년 4월 현재 이동통신 가입자 수(약 5500만 명)나 스마트폰 가입자 수(약 3800만 명), 그리고 단말기 보급대수(약 5100만 개) 등을 고려한다고 해도 거의 비슷한 결과가 산출된다.⁵⁾ 넉넉히 3년이면, 각자 한번 이상 소위 ‘털리는’ 것이다.

두 번째의 뉴스는 이러한 우리네의 상황과는 정반대인 매우 의미있는 외신이다. 지난 4월 8일 유럽사법재판소(Court of Justice of the European Union)가 2006년 유럽연합이 제정한 바 있는 ‘통신데이터 보관지침(the Data Retention Directive)⁶⁾’을 무효 결정한 것이다.⁷⁾ 동 지침은 통신사업자나 인터넷 사업자 등에게 이용자를 식별할 수 있는 통신데이터를 일정기간 보유하도록 의무화하는 내용을 담고 있다. 즉 우리의 ‘통신데이터 보관 및 제공’을 의무화하고 있는 통신비밀보호법 제15조의2 및 동 시행령 제41조와 유사한 내용의 유럽연합 지침이 무효이라는 것이다. 즉 국가가 데이터 보관을 의무화하여 취득하는 것은, 개인의 프라이버시권과 개인정보자기 결정권에 대한 심각한 침해를 야기한다는 것이다.

이러한 기본권 침해의 정당성에 대해 재판소는, 설사 데이터의 보관이 기본권의 본질에 불리한 영향을 미치는 것이 아니고 해당 규정이 공익적 목적을 충족한다고 할지라도, 그러한 침해가 실제 반드시 필요한 경우로 제한되도록 충분히 보장하고 있지 않다는 점에서 ‘비례의 원칙’의 한계를 초과한 것으로 판단하였다. 구체적으로는 ① 모든 개인의 모든 전자통신 수단과 트래픽 정보를 어떠한 구별이나 제한 또는 예외가 없이 중대범죄와의 전쟁이라는 목표 하에서 다루도록 하고 있다는 점, ② 그러한 침해를 정당화할 만큼 심각한 위법행위에 대해서만 데이터를 접근·사용한다는 것을 보장하는 객관적인 기준을 가지고 있지 않다는 점, ③ 데이터의 보관 기간의 설정이 꼭 필요한 경우로 한정되기 위한 객관적인 기준을 마련하고 있지 않다는 점 등이 주요한 이유이다. 나아가 동 지침이 데이터 오남용 또는 불법적인 사용에 대하여 충분한 보호 장치가 없다는 점과 유럽연합 내에서만 수집·보관되어야 함을 규정하는 내용이 없다는 점

5) 이는 미래창조과학부의 통계를 기준으로 삼았다. <http://www.msip.go.kr/www/brd/m_220/down.do?brd_id=w_g0408&seq=433&data_tp=A&file_seq=1>, 검색일: 2014.6.3.

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

7) Court of Justice of the European Union, “The Court of Justice declares the Data Retention Directive to be invalid”, Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, PRESS RELEASE No 54/14 Luxembourg, 8 April 2014, <<http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>>, 검색일: 2014.6.3.

등도 문제이라고 밝혔다.

같은 시기에 접한 정반대의 뉴스는 참으로 많은 생각을 하게 한다. 이러한 유럽 쪽의 소식을 우리의 상황에 대입해보면, 무차별적인 통신데이터의 수집 및 제공 관행에 대하여 앞으로는 강력한 브레이크가 걸린다는 것인데 필자로서는 참으로 꿈만 같은 일이라고 생각한다. 이러한 고민이 바로 이 글을 쓰게 된 이유이다. 즉 우리나라의 통신데이터 규제현실과 문제점들을 가히 선진적이라 할 수 있는 유럽 쪽의 입장에 비추어 제대로 짚어보기 위함이다.

II. 사항별 쟁점의 검토

통신관련 입법은 적지 않다. ‘전기통신기본법’, ‘군용전기통신법’ 등 안면이 잘 없는 법률로부터 ‘정보통신사업법’, ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’과 같이 인터넷 이슈와 관련하여 감초처럼 등장하는 법률들, 그리고 말도 많고 탈도 많기로 유명한 ‘통신비밀보호법’까지 하여 대략 법률만 20여개에 육박한다. 한편 본고에서는 통신데이터의 규제와 관련하여 주로 3가지의 법규를 살펴보고자 한다. 통신데이터의 내용을 감시하는 소위 ‘패킷감청’의 경우에 적용되는 통신비밀보호법과 통신사실확인자료의 근거규정이 자리하고 있는 통신비밀보호법 시행령 그리고 통신자료의 제공을 규정하고 있는 전기통신사업법이 그것이다. 이하에서는 통신데이터와 관련된 이 3가지의 사항에 대하여 우리의 현실적 문제점을 중심으로 각각 살펴보기로 한다.

1. 통신제한

앞서 살핀 자료에 의하면 지난 2년간 1통의 통신제한조치 허가서(이하 감청영장)로 감청한 전화번호의 수는 대략 12개 남짓이다. 정상적인 사회생활을 하는 성인을 기준으로 생각해 볼 때 12개의 전화번호를 가질 수 없다는 점에서 일단 남용에 대한 우려를 금할 수 없다. 또한 그 감청주체의 대부분이 국정원이라는 점은 다시금 도마에 올려야 할 고질병임을 재차 확인하는 계기가 된다.⁸⁾ 물론 여기서의 전화번호란 비단 유선전화와 이동전화 등의 음성통화용 기기의

8) 감청주체에 있어 국정원의 비율을 살펴보면, 2010년에는 96.8%, 2011년에는 95.4%, 2012년에는 97.4%, 2013년에는 98.3%를 기록하여 모두 95%를 넘는 고공행진을 지속하고 있다. 표2를 통해 확인할 수 있다.

번호만을 의미하지는 않는다.

〈표 2〉 2013 하반기 통신제한조치 현황⁹⁾

구 분		2012년		2013년	
		상반기	하반기	상반기	하반기
통신수단 (단위: 문서건수)	유선전화	124	58	91	100 (72.4% 증가)
	이동전화	-	-	-	-
	인터넷 등	143	122	164	237 (94.3% 증가)
감청주체 (단위: 전화번호 또는 ID 건수)	국정원	3,715	2,213	3,511	2,416 (9.2% 증가)
	기타 ¹⁰⁾	136	23	29	76 (230% 증가)
	국정원 비율	96.5%	98.9%	99.2%	97%

인터넷 등의 데이터 통신도 통신에 해당되므로 ID 등의 디지털 식별자가 포함되며, 이러한 점에서 통신제한조치, 즉 감청은 새로운 문제점을 가지게 된다.

1.1. 이동전화 감청여부의 논란

현재 우리나라 이동통신의 기술은 소위 LTE-A(Long Term Evolution-Advanced)라 불리는 4세대 이동통신, 즉 4G¹¹⁾의 단계에 이르러있다.¹²⁾ 음성통화만이 가능하던 아날로그 방식의

9) 이 표는 미래창조과학부, 앞의 보도자료, 2-3쪽의 표 내용을 참고하여 필자가 재구성한 것이다; 괄호 안은 전년도 동기 대비 증감률이다.

10) 여기서의 기타는 국정원을 제외한 기관들을 말하여, 검찰·경찰·국방부·국군기무사령부·해양경찰청 등을 말한다.

11) 주파수 집성(Carrier Aggregation) 기술을 활용하는 이동통신서비스로 유선인터넷보다 1.5배 기존의 LTE 방식보다 2배 빠른 속도로 서비스가 가능한 기술을 말한다. 우리나라에서는 지난해 6월 SK텔레콤이 가장먼저 서비스를 시작한 바 있다.

12) 4G의 정의에 대해 논란이 있을 수 있다. 우리나라에서 지난 2011년부터 상용서비스가 시작된 바 있는 LTE 방식의 기술은 엄밀히 말하자면 3세대와 4세대의 중간기술(흔히 3.9세대라 칭함)에 해당한다. 왜냐하면 2008년 국제전기통신연합(International Telecommunication Union, ITU)은 4G의 규격으로 저속 이동시 1Gbps, 고속 이동시 100Mbps의 속도로 데이터를 전송할 수 있어야 한다고 정하였으나 LTE나

1G의 시대, 유럽의 GSM(Global System for Mobile communications)방식과 미국의 CDMA(Code Division Multiple Access)방식으로 전 세계가 대분되던 2G의 시대, 이 양자를 계승한 WCDMA(Wideband Code Division Multiple Access, 유럽방식)와 CDMA 2000(Code Division Multiple Access 2000, 미국방식)의 번성기¹³⁾였던 3G시대를 지나 이제는 유선인터넷보다 스마트폰으로 검색하는 것이 더욱 빨라져버린 4G시대에 와있는 것이다. 이렇듯 급속도로 발전해가고 있는 이동통신기술을 두고 법학의 영역에서 굳이 세대를 구분한다는 것이 별의미가 없을지도 모르겠으나, 적어도 1G와 그 이후의 구분은 매우 큰 의미가 있다고 할 수 있다. 1G는 음성통화만이 가능한 아날로그 방식으로서 말 그대로 전화기였다. 그러나 그 이후의 세대에 와서는 디지털 방식으로 전환되면서 음성통화가 디지털화되고 데이터통신은 각 세대별 네트워크의 속도가 지원하는 수준에 부합하는 디지털 콘텐츠의 송수신이 가능해진 것이다. 이에 발맞추어 감청의 방식 또한 아날로그에서 디지털로 전환되어야 했고, 이동통신에 대한 감청의 범주에 종래의 음성통화뿐만이 아니라 새로이 데이터통신도 포함되었기 때문이다. 즉 유선 인터넷에 대한 소위 패킷감청이 이제는 스마트폰에도 적용되어 그 범주가 확장된 것이다.

한편 위의 '표2'에서 살필 수 있는 바와 같이 우리 정부는, 이동통신에 대한 감청을 '·'으로 표시하고 있다. 즉 미래창조과학부의 공식입장은 이동통신의 감청이 전무하다는 것인데, 이는 지난 2005년에 있었던 소위 '안기부 X과일 사건'이후에 국정원이 휴대전화 감청을 하지 않겠다고 선언하고 실제로 그 이후 단 한 번도 휴대전화를 대상으로 한 감청영장을 법원에 청구한 바 없기¹⁴⁾ 때문으로 판단된다. 그러나 미래창조과학부의 입장은 다르다. 즉 이렇듯 국가기관의 의지로 휴대전화 감청을 하지 않고 있는 것이 아니라, "2G에서는 감청이 가능했지만 3G나 4G에서

와이브로(Wireless Broadband Interne, Wibro) 등은 이에 미달하기 때문이다. 이러한 기준으로 ITU에 4G기술로 선정후보로 물망에 오른 것은 LTE를 개선한 LTE-A와 와이브로를 개선한 와이브로-에볼루션(Wibro-Evolution, 즉 와이맥스)이었다. 그후 2010년 ITU는 'LTE, 와이브로, 기타 진화한 3G 망(예를 들어 HSPA+) 등도 4G라고 부를 수 있다'는 보도자료를 내면서 종래의 입장을 번복한바 있다. 따라서 4G의 기준이 흐려졌고 덕분에 우리나라에서도 LTE도 4G이라고 칭할 수 있게 된 것이다. 요컨대 ITU의 규격 원안에 의하면 LTE를 4G라 할 수는 없고 LTE-A부터가 본격적인 4G 기술의 상용이라고 할 것이다.

- 13) 미국식 CDMA 2000은 CDMA 2000 EV-DO, 리비전(Rev.) A/B 등으로, 유럽식 WCDMA는 HSPA(HSDPA/HSUPA), HSPA+ 등으로 발전하며 데이터 전송속도가 향상되어 왔다.
- 14) 이를 정확히 확인할 바는 없으나, 적어도 감청사건에 대해 긴 시간동안 연구를 해오고 있는 필자의 경우 지속적으로 많은 수의 감청영장을 접하고 분석해 왔음에도 불구하고 휴대전화 음성통화에 대한 청구를 발견할 수는 없었다.

는 기술적으로 감청이 안 되어 휴대전화의 감청이 기술적으로 불가능하다”고 밝힌 바¹⁵⁾ 있다. 그러나 이러한 입장에는 쉬이 동의할 수 없다. 이미 국내 언론을 통하여 스마트폰의 도청이 가능함이 공공연히 보도¹⁶⁾된 바 있고 스마트폰 도청업자가 실형을 선고받은 사실이 보도¹⁷⁾되기도 했음은 물론, 심지어 스마트폰의 도청을 쇼프로그램에서 재연해 보이기도 했으며¹⁸⁾ 아예 요즘은 선거를 앞두고 스마트폰 도청방지장치가 판매가 호황이라는 소식¹⁹⁾까지 들려오고 있다. 물론 이러한 도청은 모두 악성코드를 통한 스마트폰의 해킹방식이기도 하다. 따라서 음성통화가 아니라 데이터 통신 쪽에 기반하여 진행되는 감청이기도 하다, 이러한 방식을 통해서도 해당 휴대전화의 음성통화가 그대로 전송되기는 마찬가지이므로 미래창조과학부의 입장은 타당할 수 없다. 그렇다면 음성통화 쪽²⁰⁾을 직접 감청할 수는 없는가? 즉 아날로그 시대의 감청처럼, 남의 전화를 엿듣는 ‘전통적인’ 형태의 감청이 요즘은 불가능한가 하는 물음이다. 물론 가능하다. 이는 주로 외국에서의 보도²¹⁾에서 확인할 수 있는데, 기술적으로는 ‘가상 기지국(Virtual Base Transceiver Station, VBTS)’ 기술을 사용하게 된다. 즉 감청장비를 피감청자의 휴대전화가 송수신하게 되는 기지국인 것처럼 속이고, 원래의 기지국과 피감청 휴대전화 사이에 끼어들어 양자를 오가는 패킷정보를 낚아채는 기술이다. 이는 ‘IMSI-Catcher’라고 통칭되는 원래 2G 시절

15) 미디어오늘, “국정원 감청영장은 무조건 발부된다?”, 2013.11.4.자의 기사내용중 손승현 통신정책기획과장의 답변을 재인용함, <<http://www.mediatoday.co.kr/news/articleView.html?idxno=112807>>, 검색일: 2014.6.3.

16) SBS, “[현장21] ‘월 30만원이면...’ 스마트폰 도청 충격 실태”, 2013.2.19.자, <http://w3.sbs.co.kr/news/newsEndPage.do?news_id=N1001640852>, 검색일: 2014.6.3; YTN, “스마트폰도 도청 무방비!”, 2013.11.5.자, <<http://news.naver.com/main/read.nhn?mode=LPOD&mid=tvh&oid=052&aid=0000484335>>, 검색일: 2014.6.3.

17) 아시아경제, “스마트폰 도청앱 사용, 법원 ‘집유’개고 ‘실형’선고”, 2013.11.6.자, <<http://www.asiae.co.kr/news/view.htm?idxno=2013110614505782871>>, 검색일: 2014.6.3; SBS, “스마트폰 도청 앱 쓰면...이젠 실형 범죄”, 2013.11.6.자, <<http://news.naver.com/main/read.nhn?mode=LPOD&mid=tvh&oid=055&aid=0000265182>>, 검색일: 2014.6.3.

18) XTM, 남자의 기술 4화 “충격! 스마트폰 도청, 도촬 실태!”, <<http://ch.interest.me/xtm/VOD/VODView/201302168157/883249/37330>>, 검색일: 2014.6.3.

19) 한국경제, “스마트폰 도청방지장치, 지방선거 앞두고 인기”, 2014.4.13.자, <<http://www.hankyung.com/news/app/newsvew.php?aid=2014041351851>>, 검색일: 2014.6.3.

20) 현재 국내의 음성통화는 2G·3G·4G가 모두 사용되고 있는 것으로 보인다. 소위 ‘효도폰’으로 아직도 판매가 진행되고 있는 2G폰의 경우에는 2G로 음성통화, 최근 LG U+가 상용한바 있는 VoLTE(Voice over LTE)는 4G로 음성통화를, 그 이외의 경우에는 3G로 음성통화를 수행해 내고 있다.

21) The Wall Street Journal, “How ‘Stingray’ Devices Work”, 2011.9.21자, <<http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/>>, 검색일: 2014.6.3.

의 유럽 쪽 표준인 GSM방식에 기반하여 개발된 기술이기는 하나, 미국으로 건너가서는 이 기술을 채용한 감청장비의 이름인 'Stingray'로 널리 알려지게 되었다. 'Stingray'는 마치 기지국인 양 작동을 하는데 작동반경내의 휴대전화기 소유자가 휴대전화를 사용하고 있지 않을 때에도 매 7초 내지 15초 간격으로 신호를 송신하여 반경 내의 휴대전화들을 '접속 상태'로 강제전환을 시킨다. 이러한 방식으로 감청자는 반경내의 모든 휴대전화 이용자의 송수신상황과 위치정보를 모니터링할 수 있고 일부 기기의 경우에는 음성패킷을 풀어 직접 음성통신을 감청할 수도 있다²²⁾고 알려져 있는데, 음성통화의 감청이 공식적으로 진행되고 있는 미국 내에서는 이 장치에 대해서가 아니라²³⁾ 그 사용에 있어서 '수색영장의 요부'가 법적으로 논란이 된 바²⁴⁾ 있다. 이러한 미국의 사례에 비추어보면, 더 이상 우리나라 이동통신에 대하여 음성통화 감청기술이 없다는 말은 무의미한 것이다. 1G 시절부터 지금까지 우리나라는 지속적으로 미국방식의 이동통신기술표준을 따라왔기 때문에 미국에서 가능한 기술이 우리나라에만 불가능할 수는 없기 때문이다. 요컨대, 데이터통신 기반형인 '감청-앱' 기술을 활용하건 음성통신 기반형인 '가상 기지국' 기술을 활용하건, 아니면 이 둘을 동시에 활용하건 음성통신의 감청은 현재의 기술로 얼마든지 가능하다. 따라서 미래창조과학부의 입장이 타당하지 않음은 자명하고, 이는 오히려 감청영장의 발부가 없이 불법적으로 진행되는 직접감청(즉 도청)의 경우에는 공식적인 자료가 없으므로 이를 통계상 반영할 수가 없다는 항변 정도로 해석되어야 마땅할 것이다.

1.2. 패킷감청의 문제

필자에게 있어 패킷감청의 문제는 참으로 오랫동안 주목해온 문제이다. 2009년 처음 이 문제

22) EFF, "Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About", 2012.10.22.자, <<https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy>>, 검색일: 2014.6.3.

23) 이에 대한 많은 비판은 <<https://www.eff.org/search/site/stingray>>, 검색일: 2014.6.3.에서 참조할 수 있다.

24) The Wall Street Journal, "'Stingray' Phone Tracker Fuels Constitutional Clash", 2011.9.22.자, <<http://online.wsj.com/news/articles/SB10001424053111904194604576583112723197574?mg=reno64-wsj&url=http%3A%2Fonline.wsj.com%2Farticle%2FSB10001424053111904194604576583112723197574.html>>, 검색일: 2014.6.3.; The Wall Street Journal, "Judge Questions Tools That Grab Cellphone Data on Innocent People", 2012.10.22.자, <<http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people/>>, 검색일: 2014.6.3.; 2006년 독일에서도 'IMSI-Catcher'에 대한 논란을 잠재운 독일 연방헌법재판소의 판단이 있었다. 이에 관하여는 후술하기로 한다.

를 지적할 당시에는, 별로 주변인들로부터 큰 반향이 없었던 것이 사실이다. 그 당시만하더라도 아직 휴대전화의 용법은 주로 음성통화이었기 때문에 데이터통신에 대한 감청이 그다지 관심을 끌지 못한 면이 없지 않아 있다. 그러나 데이터통신의 비중이 음성통화를 넘어서고 있는 지금에 와서는 ‘감청’이라는 용어에 대한 대표주자 격으로 등장하는 이슈가 바로 ‘인터넷 회선 감청’, 즉 패킷감청의 문제이다. 기반기술인 DPI(Deep Packet Inspection)²⁵⁾ 또한 그 활용범위가 넓어져서 여러 부문에서 사용되고 있다. ① 네트워크 보안(Network security),²⁶⁾ ② 대역관리(Bandwidth management),²⁷⁾ ③ 소비자 분석(Customer profiling),²⁸⁾ ④ 수사용 감청(Governmental surveillance),²⁹⁾ ⑤ 콘텐츠 규제(Content regulation)나 저작권 제재(Copyright enforcement)³⁰⁾ 등 많은 영역에서 활용되고 있다.³¹⁾ 또한 하나의 기능에 특성화되어 있던 초창기와는 달리, 요즘은 하나의 장비에 다수의 기능³²⁾을 복합적으로 담아내는 장비가 주류를 이루고 있기도 한 상황이기도 하다. 복합기가 경제적이라는 측면도 이유가 되겠으나, 무엇보다 급속도로 발전한 하드웨어의 역량 덕분이 아닌가 한다. 나아가 인터넷접속이 종래의 유선망뿐만 아니라 실시간으로 이동하며 진행되는 무선망접속을 통해서도 진행되고 있기 때문에, 현재 시점에서는 DPI의 기술역량은 가히 가공할 만한 수준일 것이라 추측해 본다.³³⁾

25) OSI 7계층 가운데 하위 4계층까지의 분석을 SPI(Shallow Packet Inspection), 상위 3계층에 대한 분석을 DPI로 파악하고 있음은 패킷감청을 주목하고 있는 이들에게는 일종의 상식이다. 즉 DPI는 운송을 위한 정보가 기록되어 있는 ‘헤더(Header)’부분이 아니라 ‘페이로드(Payload)’, 즉 패킷(Packet)의 콘텐츠(Contents) 부분을 검사하는 것을 말한다.

26) 이에 관한 상세와 그 법적 검토는 오길영, “인터넷 감청과 DPI”, 민주법학 제41호, 2009 참조.

27) 이에 관한 상세와 그 법적 검토는 오길영, “망중립성 논의에서의 DPI와 그 위법성”, 망중립성을 말한다(블로터앤미디어, 2013) 참조.

28) 이에 관한 상세와 그 법적 검토는 오길영, “감청의 상업화와 그 위법성”, 민주법학 제43호, 2010 참조.

29) 이에 관한 상세와 그 법적 검토는 오길영, “국가정보원의 패킷감청론에 대한 비판”, 민주법학 제48호, 2012 참조.

30) 이에 대한 상세는 박희영, “DPI 기술의 운영과 ISP의 형사책임”, Internet and Information Security 제2권 제1호, 2011, 109-111쪽.

31) Milton L. Mueller, “Convergence of control? Deep Packet inspection and future of the Internet”, *Communications & Convergence Review* 제2권 제2호, 2010, 94-95쪽.

32) 예를 들어 DPI는 패턴검사(Pattern matching), 행태분석(Behavioral analysis), 통계분석(Statistical analysis) 등의 기능을 수행한다: Milton L. Mueller, 앞의 글, 95-96쪽.

33) 휴대전화에 대한 음성통화 감청여부는 차치하고, 휴대전화의 데이터통신 부분에만 주목하자면 이에 대한 감청은 진행되고 있는 것으로 보인다. 그간 필자가 많은 감청영장들을 살펴본 경험에 의하면, 음성 사서함이나 문자메세지 및 카카오톡 등에 대한 감청허가를 요청한 사례가 있기 때문이다. 그렇다면 적어도 이러한 통계는 미래창조과학부의 발표자료에 반영되어 있어야 할 것인데, 어찌하여 휴대전화 부문이 ‘(즉 0)으로 기록되어 있는 것인지 알 수 없다. 이를 ‘인터넷 등’의 항목으로 취급하였는지의 여

패킷감청 논란의 핵심은 감청영장이 요구하는 감청의 대상을 특정할 수 없다는 데에 있다. 이는 DPI의 기술적 구조와 IP운영의 원리가 이러한 ‘불특정성’이라는 특성을 필연적으로 양산해 내기 때문에 비롯되며, 결국 감청대상을 미리 특정하여 적시하게 되어있는 우리 헌법상 영장주의의 원리에 부합하지 않아 ‘포괄영장’의 문제로 귀결된다는 것이 필자의 결론이다.³⁴⁾ 이러한 논의를 바탕으로 지난 2011년 시민단체로 구성된 ‘공안기구감시네트워크’가 국가정보원의 패킷감청에 대하여 헌법소원(2011 헌마165)을 청구한 바 있으나, 아직까지 묵묵부답인 상태에 머물러 있다.

한편 기다리고 있는 헌법재판소의 판단에 앞서 대법원에서 패킷감청에 대한 짧은 판단이 있었다.³⁵⁾ 즉 “인터넷 통신망을 통한 송·수신은 통신비밀보호법 제2조 제3호에서 정한 ‘전기통신’에 해당하므로 인터넷 통신망을 통하여 흐르는 전기신호 형태의 패킷(packet)을 중간에 확보하여 그 내용을 지득하는 이른바 ‘패킷 감청’도 같은 법 제5조 제1항에서 정한 요건을 갖추는 경우 다른 특별한 사정이 없는 한 허용된다고 할 것이고, 이는 패킷 감청의 특성상 수사목적과 무관한 통신내용이나 제3자의 통신내용도 감청될 우려가 있다는 것만으로 달리 볼 것이 아니다”라고 실시하여 패킷감청을 통신비밀보호법상의 유효한 감청방법임을 지지한 바 있다. 그러나 이는 너무나 간략하여 패킷감청이 가지고 있는 문제점들을 제대로 검토했다고는 보기 힘들며, 특히 그 문제의 핵심이 광범위한 감청의 범위만이 아니라 아예 감청대상 자체가 특정가능성이 없어 영장주의의 원리에 정면으로 배치된다는 점을 간과하고 있다는 점에서 비판을 해볼 수 있을 것이다.

이러한 법적 논의를 떠나 지금의 현실을 고려해보아도 데이터통신의 비중이 점차 증가하고 있고, 이는 앞서 ‘표2’에서 살필 수 있는 바와 같이 패킷감청의 빈도가 유선통화를 넘어선 결과로 등장한다. 하루빨리 우리 헌법재판소의 올바른 판단이 나오기를 기다려 본다.

2. 통신사실확인자료

앞서 ‘표1’에서 살핀 바와 같이 가장 뜨거운 논란의 무대 위에 서있는 것이 바로 통신사실확인자료이다. 그야말로 천문학적인 감시가 진행되고 있다는 것인데, 2년 평균 2000만 개를 상회

부가 불분명하기 때문이다.

34) 이에 대한 상세는 오길영, 앞의 글(각주 29), 349-358쪽.

35) 대법원 2012.10.11. 선고, 2012도7455 판결.

하는 통신기기가 ‘털렸다’는 사실을 두고 오남용의 가능성을 의심하지 않은 이를 찾기란 그리 쉽지 않을 것이다. 결국 이러한 문제점에 대하여 최근 국가인권위원회가 동 제도에 관한 개선권고를 결정하였음³⁶⁾은 너무나 당연한 일이라 하겠다.

2.1. 입법상의 미비

통신사실확인자료의 남용과 관련하여 가장 빈번히 회자가 되는 것이 절차적인 문제이다. 우리 통신비밀보호법의 경우 제13조 제1항에서 “검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자에게 통신사실 확인자료의 열람이나 제출을 요청할 수 있다”고 규정하면서 동조 제2항에서는 “제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다”라고만 규정하고 있다. 즉 ‘서면’이라는 형식적 요건을 제외하면 영장발부에 대한 실질적 요건이 전혀 명시되어 있지 않은 상태이다. 한편 미국의 경우에는 이에 상응하는 규정이 ECPA(The Electronic Communications and Privacy Act) 제2장(과거의 통신사실확인자료)과 제3장(장래의 통신사실확인자료)에 나누어 규정되어 있는데, 전자는 ‘완화된 영장요건(수사 관련성에 대한 구체적이고 적시가능한 입증 필요함)³⁷⁾이 후자는 ‘가장 완화된 영장요건(수사 관련성에 대한 입증)³⁸⁾이 필요하다.

36) 이에 관한 상세는 <http://www.humanrights.go.kr/04_sub/body02.jsp?m_link_url=04_sub/body02.jsp&m_id1=72&m_id2=75&m_id3=&m_id4=&flag=VIEW&SEQ_ID=609282>, 검색일: 2014.6.3에서 확인할 수 있다.

37) 18 U.S. Code § 2703(d): A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

38) 18 U.S. Code § 3123(a)(1): Upon an application made under section 3122 (a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

〈표 3〉 통신사실확인자료에 대한 미국과 한국 입법의 비교³⁹⁾

구분		미국 ECPA	한국 통신비밀보호법
과거의 통신사실 확인자료	영장발부 요건	관련성을 보여주는 구체적이고 적시가능한 사실의 증명	법원의 허가
	통지의무	없음	공소제기 또는 불기소처분 이후 30일 이내
장래의 통신사실 확인자료	영장발부 요건	취득정보와 현지 진행중인 형사절차와의 관련성의 소명	법원의 허가
	통지의무	없음	공소제기 또는 불기소처분 이후 30일 이내
	취득기간	최대 60일	제한없음

물론 ECPA의 경우 우리 통신비밀보호법에 마련되어 있는 통지의무를 가지고 있지 않다는 차이가 있기는 하나, 영장발부에 대한 그 어떠한 실질적 요건도 마련하고 있지 않고 있는 현재의 규정은 참으로 심각한 입법미비가 아닐 수 없다. 너무나 낮은 문턱으로 인해 실제로 가공할만한 남용이 진행되고 있기 때문이다.

입법의 미비는 여기에서 그치지 않는다. 영장발부의 주체에 있어서도 적지 않은 문제가 있기 때문이다. 앞서 살핀 동법 제13의 범문은 영장발부 요청의 주체로 ‘검사 또는 사법경찰관’을 지정하고 있다. 이는 통신제한의 경우(동법 제6조), ‘사법경찰관’은 검사에게 그 허가를 신청할 수는 있으나 발부주체인 법원에 대한 신청주체는 어디까지나 ‘검사’에 한정하고 있는 입법태도와는 사뭇 다르다. 즉 우리 헌법이 예정하고 있는 영장발부의 절차는 ‘검사’만이 신청가능하고 ‘법관’이 ‘영장’을 발부하도록 되어있는 소위 ‘검사독점적 영장청구제도’⁴⁰⁾(헌법 제12조 제3항)를

39) 이 표는 김재윤, “통신사실 확인자료 및 금융거래정보 청구절차 개선방안 연구”, 치안정책연구소 용역 최종보고서, 2013, 46쪽의 표 내용을 참고하여 필자가 재구성한 것이다.

40) 이 제도의 취지에 대해 헌법재판소는 “제5차 개정헌법이 영장의 발부에 관하여 ‘검찰관의 신청’이라는 요건을 규정한 취지는 검찰의 다른 수사기관에 대한 수사지휘권을 확립시켜 종래 빈번히 야기되었던 검사 아닌 다른 수사기관의 영장신청에서 오는 인권유린의 폐해를 방지하고자 함에 있다고 할 것이고, 따라서 현행 헌법 제12조 제3항 중 ‘검사의 신청’이라는 부분의 취지도 모든 영장의 발부에 검사의 신청이 필요하다는 것이 아니라 수사단계에서 영장의 발부를 신청할 수 있는 자를 검사로 한정하는 것으로 해석함이 타당하다. 즉, 수사단계에서 영장신청을 함에 있어서는 반드시 법률전문가인 검사를 거치도록 함으로써 다른 수사기관의 무분별한 영장 신청을 막아 국민의 기본권을 침해할 가능성을 줄이고자 함에 그 취지가 있는 것이다(헌법재판소 1997.3.27. 선고 96헌바28.31.32 결정)”라고 실시한 바 있다.

취하고 있음에 비추어 본다면 동 조항은 위헌성이 농후한 조항이 될 것이다.⁴¹⁾

그렇다면 영장이 아닌 것인가? 실제로 통신사실확인자료 제공요청 허가청구권의 법적 성질을 영장의 청구로 보지 않는 견해가 있다.⁴²⁾ 이 견해에 의하면 ① 통신사실확인자료의 제공요청이 만약 헌법 제17조에서 규정하고 있는 사생활의 비밀보호의 대상이 되는 ‘개인정보’에 해당한다면 개인정보자기결정권을 침해하는 것으로 검사의 독점적 영장청구권의 대상이 되나, 통신사실확인자료는 비식별정보로서 설사 식별정보와 결합한다고 하여도 특정 개인을 알아볼 수 있는 구체성을 결여하였다는 점에서 개인정보자기결정권의 보호대상에 해당되지 않고,⁴³⁾ ② 2005년 개정 이전의 통신비밀보호법의 규정은 통신사실확인자료에 대하여 법원의 허가가 아닌 ‘검사장의 승인’만을 얻도록 하고 있었는데, 만약 통신사실확인자료 제공의 법적 성질이 헌법상 영장주의가 적용되는 것이라면 동 개정 이전의 규정이 위헌임은 물론 그 당시에 제공된 통신사실확인자료들은 모두 위법수사가 되어 타당하지 않다고 한다.⁴⁴⁾

그러나 이러한 견해에는 동의할 수 없다. 먼저 기본권 침해성이 없으므로 영장주의의 적용을 받지 않는다는 취지인 ①에 대하여는 지난 2010년에 있었던 독일 연방헌법재판소의 위헌결정⁴⁵⁾이 좋은 반론이 될 것이다. 독일 연방헌법재판소는 결정이유에서 ‘전기통신의 비밀을 보장하고 있는 독일 기본법 제10조 제1항은 무형적 정보가 전기통신시설을 이용하여 개별적인 수신자에게 전달되는 것을 공권력이 그 통신의 내용을 인식하는 것으로부터 보호하고자 하는 것을 목적으로 하고 있는 조항인데, 이러한 보호는 공권력이 전기통신의 과정과 내용을 인식하는 것뿐만이 아니라 통신과정의 인식과 관련되는 정보처리 및 데이터처리과정에도 적용되고, 획득된 인식내용을 기반으로 행해지는 사용에도 확대된다’고 실시하면서 ‘모든 통신데이터의 인식내용, 기록 그리고 사용 및 공권력을 통한 모든 통신내용의 평가 또는 그 밖의 사용은 기본권 침해에 해당한다’고 판단한 바 있다.⁴⁶⁾ 즉 개인정보자기결정권의 침해가 아니라 통신비밀보호권의 침

41) 사실 이 부분은 다소 난해한 문제와 얽혀있다. 일반적으로 통신제한조치 허가서(소위 감청영장)에 대한 법적 성격을 일종의 영장으로 파악하고 있으나, 실제 통신비밀보호법상의 어떠한 범문에도 ‘영장’이라는 표현을 사용하고 있지 않기 때문이다. 또한 감청영장의 발부주체가 ‘법관’이 아니라 ‘법원’이라고 표현하고 있다는 점도 이례적이라 할 수 있을 것이다.

42) 김재윤, 앞의 글, 51-56쪽.

43) 김재윤, 앞의 글, 53-54쪽.

44) 김재윤, 앞의 글, 55-56쪽.

45) BVerG 1 BvR 256/08 vom 2. 3. 2010; 이 결정은 앞서 밝힌 바 있는 최근의 유럽사법재판소의 결정과 그 궤를 같이 하는 것이다.

46) 박희영, “통신사실확인자료의 저장과 통신비밀의 침해(上)”, 월간법제 2010년 5월호, 법제처, 2010,

해라는 것이다. 따라서 기본권 침해성이 있으면 감사의 독점적 영장청구권의 대상이라는 ①의 논리에 의하면, 통신사실확인자료 제공요청 허가청구권의 법적 성질은 영장의 청구이어야 한다.

다음으로 ②에 대해서는 입법연혁을 반론으로 제시하고 싶다. 동 견해가 밝힌 바와 같이 ‘검사장의 승인’으로 통신사실확인자료의 제공이 가능했던 것은 2001년 12월 29일 일부개정으로 2002년부터 시행된 ‘법률 제6546호’의 통신비밀보호법 시절이다. 이때에 비로소 통신사실확인자료의 제공절차에 관한 제13조 규정이 신설된 것이다. 그러다 2005년 5월 26일 일부개정 법률인 ‘법률 제7503호’에 와서 드디어 ‘검사장의 승인’이 ‘법원의 허가’로 변경된다. 개정이유⁴⁷⁾에 의하면 이러한 변경은 “엄격한 절차를 마련함으로써 국민의 기본권을 충실히 보장하”기 위함이라고 한다. 그렇다면 동 절차규정이 신설되기 이전의 상황은 어떠한가? 통신사실확인자료의 제공은 전기통신사업법에 의해 근거하고 있었으며, ‘법률 제6546호’의 개정이유⁴⁸⁾에 의하면 “전기통신가입자에 대한 통신자료 제공의 법적 근거와 절차를 전기통신사업법이 아닌 이 법에서 체계적으로 규정하”기 위해 동 규정을 신설했다고 한다. 즉 입법자는 이때에 와서야 비로소 통신사실확인자료가 헌법상의 통신비밀보호권과 관련이 있음을 깨달은 것이다. 결국 그 이전에는 지금의 통신자료와 같은 취급을 받고 있었던 셈이다. ②의 논지에 의하면 결국 통신비밀보호법이 처음으로 제정되던 1994년 이후부터 당해 개정까지는 ‘검사장의 승인’조차 필요가 없는 무방비상태라는 것인데, 이 부분은 어찌 해석할 것인가? 이 또한 위헌적 상태가 아니겠는가? 그런데 제공절차에 관한 제13조 규정이 그 기간 동안은 아예 존재하지도 않는데, 위헌법률심사는 도대체 어떻게 청구할 수 있겠는가? 아니면 당시 전기통신사업법 제54조의 규정을 위헌법률심사의 도마에 올리면 해결되는가? 그러나 안타깝게도 당시의 전기통신사업법 제54조는 ‘이용자의 성명, 주민등록번호, 주소, 가입 또는 해지일자’ 등 ‘통신자료’만을 제공하도록 규정하고 있어서 이 역시 심사가 불가능할 것이다.⁴⁹⁾ 그렇다면 이번에는 합헌인 것인가? 요컨대 ②의 논지는

32-33쪽.

47) <<http://www.law.go.kr/lsInfoP.do?lsiSeq=68717&lsId=&efYd=20050827&chrClsCd=010202&urlMode=lsEfInfoR&viewCls=lsRvsDocInfoR#0000>>, 검색일: 2014.6.3.

48) <<http://www.law.go.kr/lsInfoP.do?lsiSeq=59598&lsId=&efYd=20020330&chrClsCd=010202&urlMode=lsEfInfoR&viewCls=lsRvsDocInfoR#0000>>, 검색일: 2014.6.3.

49) 통신사실확인자료의 개념이 우리 입법사에 처음으로 등장한 것은 ‘법률 제6546호’의 통신비밀보호법 개정시 부터이다. 즉 제공절차 규정이 마련되면서 동시에 탄생한 것이다. 그러나 그 당시의 통신사실확인자료의 정의규정(동법 제2조 제11호)을 살펴보면 현재의 정의규정과는 그 내용이 상이하다는 것을 발견할 수 있다. 즉 컴퓨터통신과 인터넷 환경을 반영하고 있는 현재 규정상의 ‘마문’과 ‘비문’, 그리고 ‘사문’이 없었던 것이다. 이들은 2002년 3월 25일 일부개정 대통령령 ‘대통령령 제17548호’인 통신비밀

법률 제·개정 의의와 위헌법리에 대하여 심대한 오류를 가지고 있으며, 따라서 전혀 타당하지 못하다.

2.2. 소위 ‘기지국 수사’의 문제

기지국 수사의 문제가 말로 현재 이 분야에 있어서 가장 뜨거운 이슈이다. 실제로 제공되는 통신사실확인자료의 대부분이 바로 기지국 정보이기 때문이다. 국가인권위원회의 권고결정문에 의하면, 2009년의 경우 제공된 전체 통신사실확인자료에 있어 기지국 수사용 제공의 비중은 무려 96% 이상이고, 2010년의 경우에는 98.3%, 2011년에는 98.6% 달했던 것으로 확인된다.⁵⁰⁾ 상황이 이러하다 보니, 소위 집회 참가자를 파악하기 위한 ‘썩쓸이’ 또는 ‘저인망식’ 수사라는 불미스러운 수식어가 붙게 된 것이다.⁵¹⁾

기지국 수사의 문제점은 이러한 남용현실에만 있는 것이 아니다. 특정 기지국에서 송수신된 이동통신기기를 추적하여 수사를 전개하는 기지국 수사의 본질은 위치정보의 제공이다. 따라서 이러한 위치정보가 통신사실확인자료의 범주내에 포함될 수 있는가 하는 것이 이 문제의 핵심이다. 즉 기지국과 기기와의 사이에서 진행되는 ‘전자적 교신’이 통신이냐의 문제인 것이다. 물론 사용자가 직접 음성통화나 데이터통신을 실행하는 경우는 당연히 통신에 해당하겠으나, 실제 사용자가 이러한 통신을 하지 않더라도 자동적으로 진행되는 기지국과 기기사이의 교신정보를 이용해 휴대전화의 실시간 위치추적이 진행되고 있다는 점⁵²⁾에서 이러한 논의는 중요한 쟁점이 된다.

이에 대하여 필자는 이미 오래전부터 통신의 개념에 포함할 수 없음을 주장⁵³⁾해 오고 있다. 왜냐하면 법적 의미에서의 통신은 격지자에 대한 의사표시의 전달이므로 그 내용은 ‘의사표시’

보호법 시행령에 ‘제3조의2’로 신설되었다가 그 이후 2005년 1월 27일 일부개정 법률인 ‘법률 제7371호’부터 현재의 정의개념으로 편입되었다.

50) 국가인권위원회, “전기통신사업법 통신자료제공제도와 통신비밀보호법 통신사실확인자료제공제도 개선 권고”, 국가인권위원회, 2014, 9쪽.

51) 진보넷, “갈수록 심각해지는 통신 감청과 통신자료 제공 문제”, 진보네트워크센터 논평, 2014, <<http://act.jinbo.net/drupal/node/8007>>, 검색일: 2014.6.3.

52) 한겨레신문, “경찰이 휴대전화로 실시간 위치추적” 송경동 시인 헌법소원 제기, 2012.2.29.자, <http://www.hani.co.kr/arti/society/society_general/521319.html>, 검색일: 2014.6.3; 실제로는 사용자의 통신여부와 무관하게 10분 간격으로 위치정보가 담당수사관에게 문자메시지로 발송된다고 한다.

53) 이에 관한 상제는 오길영, “통신비밀보호법 개정안 비판”, 민주법학 제34호, 2007 참조.

이어야 하는데, 기지국 위치정보는 어떠한 의사표시도 담고 있지 않은 채로 순수한 ‘전자적 교신’만을 수행할 뿐이기 때문이다. 즉 사용자의 의사표시를 송수신하는 것이 아니라 순수한 기술 정보를 전자적으로 교신하는 것에 불과하므로 이는 통신개념에 포함될 여지가 없다는 것이다. 따라서 기지국 위치정보는 통신비밀보호법상의 통신사실확인자료에도 포함될 수도 없다. 왜냐 하면 통신사실확인자료는 통신이 존재함을 전제로 그 통신에 대한 사실 및 관련사항이어야 하는데, 기지국 위치정보의 경우 개념적으로 통신의 여부와는 무관한 독립된 전자적 신호의 교신이기 때문이다.

한편 이러한 필자의 오랜 주장에 대한 유력한 지지자로 독일 연방헌법재판소가 등장한 바 있다.⁵⁴⁾ 독일 연방재판소는 앞서 살핀바 있는 ‘IMSI-Catcher’ 기술에 대해 위헌여부를 심사⁵⁵⁾하면서 다음과 같이 설시한 바 있다.

‘IMSI-Catcher’를 설치한 경우에는 오로지 기계들 사이에서만 기술적인통신이 이루어진다. 그것은 통신의 내용과 관련된 인간이 창출한 정보의 교환은 없다. 그 데이터의 전송은, 구체적인 통신의 과정 또는 사적인 관련성을 가지는 통신접속의 형성과는 무관하게 발생한다. 데이터의 교환은 오로지 (기계적) 가동준비가 된 것을 확보하기 위해서 필요한 것이고, 개인적 통신에 대하여는 어떠한 관련성도 없다. (이를 통해) 확보된 데이터는 통신의 과정에 관련된 것이 아니라, 통신과정의 기술적인 요건이 되는 휴대전화의 준비상태를 위해 비로소 존재하게 되는 것이다. 통신수단으로 기여하는 기기에서 만들어지는 기술적인 신호는 단순히 기술적인 호환이나 통신의 준비상태를 보증하기 위한 것으로 전혀 통신이 아니다. 이는 통신의 상태와는 달리 통신관련성과 통신의 내용을 추론할 가능성이 없고, 단지 단말기의 위치를 인지함으로써 사람의 소재지를 추론하게 할 뿐이다. 전기통신시설을 통하여 전달되는 데이터는, 실제 생각과 정보의 교환을 위해 이용될 때 비로소 통신의 내용과 통신의 형태로서의 자격이 부여된다. ... 중략 ... 실제의 통신과정 이외에 선행되어 있는 통신의 개시는 동일한 (기본권적) 보호를 받지 못한다.

54) BVerfG, Beschluss vom 22.8.2006 - 2 BvR 1345/03.

55) 본 결정은 ‘IMSI-Catcher’를 기지국 수사용으로 사용하는 것에 대한 심사이며, 이를 감청용 장비로 활용하는 것에 대한 판단이 아니다. 다만 동 법원은 설시에서 ‘IMSI-Catcher’를 통한 감청의 독일 형사소송법 제100i조를 통해서 보호되지 않을 수도 있다고 하여, 위법일 수 있다는 우회적 표명을 한 바는 있다; 이에 대한 상세는 박희영, “IMSI 및 IMEI와 휴대전화의 위치확보의 합헌성 여부”, 월간법제 2009년 11월호, 법제처, 2009 참조.

‘통신이 가능하다고 여기는 것은 아직 통신이 아니다.’⁵⁶⁾

이러한 검토의 결과 독일 연방헌법재판소는 ‘MSI-Catcher’를 통해 수집되는 기지국 위치정보는 통신비밀의 보호영역이 아니라 개인정보자기결정권과 관련이 있다고 판단하였다. 이 장치를 통해 수집되는 휴대전화의 단말기번호와 카드번호는 통신 자체와는 관련이 없다는 것이 결론이기 때문이다. 필자의 논리구성과 큰 차이를 보이지 않는다.

또한 미국의 경우에는 추적용 위치정보, 즉 이동추적장치 및 발신자 추적장치(Trap and Trace Device)에 대해서는 통신사실확인자료와는 아예 별개의 것으로 취급하고 있다. 즉 ECPA는 우리의 통신사실확인자료에 해당하는 내용은 소위 저장통신법(Stored Communications Act, SCA)⁵⁷⁾에서 규정하고 있는 반면 추적용 위치정보에 대해서는 소위 펜트랩법(Pen/Trap provisions)⁵⁸⁾에서 그 장을 달리하여 규정하고 있다.

이러한 점들을 종합해 볼 때 실시간 위치추적용 기지국 정보를 통신사실확인자료의 범주에 포함시키는 것은 그리 타당하지 않다고 판단된다. 통신확인사실자료 제공의 남용이 실로 극한에까지 달해있는 현재의 상황 또한 이러한 논리를 뒷받침한다. 따라서 기지국 위치정보를 별도의 영장발부가 필요한 새로운 부류의 정보로 분류하여 아예 따로 규제하는 입법의 신설이 바람직하다고 생각한다.

3. 통신자료

통신자료 제공의 남용 또한 통신사실확인자료의 상황과 크게 다를 것이 없다. 제공 문서건수는 1위에 랭크되어 있고, 2년 4분기 추이를 보자면 계속 증가되는 추세를 보이고 있기 때문이다. 그러나 통신자료의 경우 그 규제가 통신비밀보호법이 아니라 전기통신사업법이고 따라서 헌법상 통신비밀의 보호대상에 해당하지 않는다는 점이 큰 차이이다. 이는 통신자료 제공의 범위를 규정하고 있는 전기통신사업법 제83조 제3항을 살펴보면도 타당한 해석으로 보인다. 즉 이용자의 ‘성명·주민등록번호·주소·전화번호·아이디·가입일 또는 해지일’ 등의 정보는 이들 자체만을 두고 볼 때 통신과의 관련성을 인정하기는 어렵다. 단지 이용자 개인의 신상정보인 것이다.

56) 이 부분의 인용은 박희영, 앞의 글(각주 54), 76-77쪽의 내용을 필자가 번역의 취지에 맞게 약간 수정한 것이다.

57) 18 U.S. Code Chapter 121 §§ 2701-2712.

58) 18 U.S. Code Chapter 206 §§ 3121-3127.

3.1. 규정의 타당성의 문제

전기통신사업법 제83조 제3항은 법원의 허가를 요건으로 하지 않는다. 법문에 의하면 ‘요청 사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(자료제공요청서)’의 제출만이 유일한 요건(동법 동조 제4항)이다. 또한 수사실무에 있어서도 ‘4급 이상의 공무원 또는 총경 등의 결제만 있으면 되고, 그 이외의 별다른 요건이 없는 것으로 확인된다. 따라서 결국 규정 자체가 지금의 남용을 상정하고 있는 셈이라고도 할 수 있다.

이러한 문제점에 대하여 국가인권위원회는 통신자료를 통신사실확인자료에 포함시키는 방식으로의 개정을 권고하고 있다.⁵⁹⁾ 즉 전기통신사업법 제83조의 제3항을 삭제하고, 통신확인사실 자료의 정의규정인 통신비밀보호법 제2조 제11호에 ‘가입자정보’를 새로이 신설할 것을 권고하고 있기 때문이다. 이는 미국의 입법방식을 따른 것으로 판단된다. ECPA의 경우 우리의 통신자료⁶⁰⁾와 통신사실확인자료⁶¹⁾를 동일한 조문 하에 구분하여 규정하고 있기 때문이다. 그 분류가 우리의 경우와 정확하게 맞아 떨어지는 것은 아니나 대체로 부합하고, 차이점이 있다면 양자에 있어 적용되는 제공시의 허가절차가 상이하다는 점이다. 즉 전자의 경우에는 비교적 요건이 완화되어 있는 소환장(Subpoena)⁶²⁾이 후자의 경우에는 ‘수사 관련성에 대한 구체적이고 명료한 입증이 필요한 법원명령(Court Order)⁶³⁾이 적용된다. 이러한 형태의 입법을 취할 경우에 관련되는 헌법상의 권리, 즉 보호되는 기본권의 내용은 통신비밀보호권이 될 것이다.

한편 통신자료의 내용이 전형적인 개인식별정보(Personally Identifiable Information, PII)이라는 점에서, 이를 통신비밀 보호법제가 아니라 아예 개인정보 보호법제로 편입시키는 것도 또 하나의 방안이 될 수 있다. 물론 이러한 형태의 입법을 취할 경우에도 엄격한 요건의 영장주의에 의해야 함은 당연하다. 이 또한 헌법상의 기본권 보호, 즉 개인정보자기결정권의 보호를 받

59) 국가인권위원회, 앞의 권고결정문, 1쪽.

60) 18 U.S. Code § 2703(c)(2): 성명, 주소, 근거리 또는 장거리 전화통화 내역 또는 통화시간기록, 서비스 기간 및 사용된 서비스의 유형, 전화번호나 매체번호 또는 다른 가입자 번호나 신원 및 유동IP의 주소, 서비스 사용료의 지불수단 등.

61) 18 U.S. Code § 2703(c)(1): 통신의 내용정보를 제외한 고객 또는 가입자에 속하는 기록 및 기타의 정보.

62) 여기서의 소환장은 법원이 재판과정에 발부한 ‘재판소환장(Trial Subpoena)’과, 연방 또는 주의 법률이나 연방 또는 주의 대배심의 승인을 받은 ‘행정소환장(Administrative Subpoena)’을 말한다: 18 U.S. Code § 2703(c)(2) 후단.

63) 18 U.S. Code § 2703(d).

이야 하기 때문이다. 이러한 입법형태의 장점은 현재 우리 판례의 시각과 부합한다는 점이다. 즉 “... 갑 회사가 수사기관에 대해 을의 주민등록번호와 전화번호 등 인적사항 일체를 제공한 행위는(포털업체가 수사기관에 통신자료를 제공한 것은) 을의 개인정보를 충실히 보호하여야 할 의무를 위반하여 을의 개인정보자기결정권 내지 익명표현의 자유를 위법하게 침해함으로써 을로 하여금 그 법익침해와 관련한 손해를 입도록 한 것이므로 ...”라는 항소심⁶⁴⁾의 판단이나, “수사의 밀행성 보장은 수사의 편의를 위한 것인 반면, 통신자료제공 현황의 공개는 헌법상 기본권인 개인정보자기결정권을 실현하는 것이므로 보다 보호가치가 크다”라고 판단하고 있는 하급심⁶⁵⁾의 판단에서 우리는 이러한 입법형태의 가능성을 짐쳐 볼 수 있다.

3.2. 법문 해석의 문제

통신자료에 관하여 가장 유명한 일화는, 통신자료 제공에 관한 전기통신사업법 제54조 제3항(현재의 제83조 제3항)⁶⁶⁾의 규정에 대한 우리 헌법재판소의 문리해석이다.⁶⁷⁾ 인용하면 다음과 같다.

이 사건 통신자료 취득행위는 피청구인이 이 사건 전기통신사업자에게 청구인에 관한 통신자료 취득에 대한 협조를 요청한 데 대하여 이 사건 전기통신사업자가 임의로 이 사건 통신자료를 제공함으로써 이루어진 것이다. 그런데 피청구인과 이 사건 전기통신사업자 사이에는 어떠한 상하관계도 없고, 이 사건 전기통신사업자가 피청구인의 통신자료제공 요청을 거절한다고 하여 어떠한 형태의 사실상 불이익을 받을 것인지도 불분명하며, 수사기관이 압수수색영장을 발부받아 이 사건 통신자료를 취득한다고 하여 이 사건 전기통신사업자의 사업수행에 지장을 초래할 것으로 보이지도 않는다. 또한 이 사건 통신자료 취득행위의 근거가 된 이 사건 법률조항은 “전기통신사업자는 ... 요청받은 때에 이에 응할 수 있다.”라고 규정하고 있어 전기통신사업자에게 이용자에 관한 통신자료를 수사관서의 장의 요청에 응하여 합법적으로 제공할 수 있는 권한을 부여하고 있을 뿐이지 어떠한 의무도 부과하고 있지 않다. 따라서 전기통신사업자

64) 서울고등법원 2012.10.18. 선고, 2011나19012 판결.

65) 서울중앙지법 2014.5.20. 선고, 2013가합517759 판결.

66) 통신자료에 제공에 관한 현재의 ‘제83조 제3항’의 규정은, 2010년 3월 22일 전부개정된 ‘법률 제10166호’ 이전에는 원래 ‘제54조 제3항’이었다. 양자는 대동소이하다. 굳이 차이를 꼽자면, 당시에는 “... 정보수사기관의 장으로부터 ... 다음 각호의 자료의 열람이나 제출을 요청받은 때에 이에 응할 수 있다”였으나 지금은 “... 정보수사기관의 장이 ... 다음 각 호의 자료의 열람이나 제출을 요청하면 그 요청에 따를 수 있다”로 끝을 맺는다. 즉 규정의 내용상으로는 차이가 없다.

67) 헌법재판소 2012.8.23. 선고, 2010헌마439 결정.

는 수사관서의 장의 요청이 있더라도 이에 응하지 아니할 수 있고, 이 경우 아무런 제재도 받지 아니한다. 그러므로 이 사건 통신자료 취득행위는 강제력이 개입되지 아니한 임의수사에 해당하는 것이어서 헌법재판소법 제68조 제1항에 의한 헌법소원의 대상이 되는 공권력의 행사에 해당하지 아니한다고 할 것이므로 이에 대한 심판청구는 부적법하다.

요컨대 법문이 “... 요청받은 때에 이에 응할 수 있다”라고 규정하고 있어, 제공의 여부는 전기통신사업자의 재량이지 의무사항이 아니라는 것이 주요한 요지이다. 그야말로 ‘문리해석’이 아닐 수 없다. 이렇듯 동 법문을 결국 임의수사인 것으로 해석하고 있는 헌법재판소의 입장은, 아마도 종래의 헌법재판소의 입장을 그대로 수용한 결과이라고 판단된다. 우리 헌법재판소는 임의수사와 강제수사의 구별기준에 대하여 실질설을 취하면서, 구체적으로는 ‘수사기관의 물리적 강제력의 행사유무’로 판단하는 입장을 취해 온 바 있다.⁶⁸⁾ 반대로 학계에서는 수사기관이 아니라 ‘상대방의 의사여하’를 기준으로 강제수사의 유무를 판단하는 견해⁶⁹⁾가 다수설이다. 이에 의하면 강제수사란 상대방의 의사에 반하여 실질적으로 그의 법익을 침해하는 처분을 말하여 상대방의 법익침해를 수반하지 않는 수사를 임의수사로 본다.

이러한 이론적 논의를 차치하고 동 결정을 바라본다면, 참으로 답답한 판단이 아닐 수 없다. 즉 수사기관과 통신사간의 권력적 구조를 제대로 고려하지 않았음은 물론, 앞서 살핀 남용의 현실을 도외시한 것이라는 비판을 피하기 힘들어 보인다. 왜냐하면 ‘... 할 수 있다’라는 법문은 사실상 사문화된 것이기 때문이다. 피혐의사실에 대해 사전정보가 전무한 전기통신사업자는 수사기관이 제시한 요청사유의 타당성에 대해 심사할 능력도 여지도 없으며,⁷⁰⁾ 이렇듯 재량판단의 여지가 없는 전기통신사업자의 상황을 요청수사기관 또한 이미 숙지하고 있는 터이므로 이에 대한 거절은 곧 수사기관에 대한 일종의 ‘도전’으로 받아들여지게 되는 것이 피할 수 없는 사실이기 때문이다.

한편 동 결정의 소수의견은 참으로 의미있는 판단을 한 바 있다. 이 사건에서의 통신자료 취득이라는 대물적 처분은, 형식적으로는 통신사업자를 상대로 진행된 것이지만 실제로는 전기통신사업자가 아니라 통신사용자의 기본권이 제한되는 경우로 보아야 한다는 것이다. 또한 전기

68) 헌법재판소, 1997.3.27. 선고, 96헌가11 결정; 헌법재판소, 2004.9.23. 선고, 2002헌가17·18(병합) 결정 등

69) 이재상, 신형사소송법 제2관(박영사, 2009), 213쪽; 진계호, 형사소송법 제2관(형설출판사, 2004), 237쪽; 임동규, 형사소송법 제6관(법문사, 2009), 161쪽; 이영란, 한국형사소송법 개정판(나남출판, 2008), 289쪽 등.

70) 국가인권위원회, 앞의 권고결정문, 6쪽.

통신사업자가 수사기관의 요청을 거절할 가능성이 사실상 희박하고 그렇다고 통신사용자가 나서서 그 제공을 저지할 방도도 없기 때문에 통신사용자의 의사에 상관없이 진행되는 것이며, 따라서 수사기관의 통신자료 취득행위는 우월적 지위에서 일방적으로 진행되는 권력적 사실행위에 해당한다는 것이다. 통신자료의 남용현실을 고려하자면, 그 이론구성의 정합성 정도를 불문하고 이 견해를 지지하지 않을 수가 없다. 많은 후속판례들이 이 결정의 취지를 그대로 인용하고 있는 상황인데다 통신자료의 남용이 그야말로 극에 달해있는 현시점의 고민을 상기해보면, 소수의견이 훨씬 더 설득력 있어 보이는 것은 혼자만의 착각은 아닐 것이다.

Ⅲ. 나오며

생각보다 글이 상당히 길어졌다. 아마도 쟁점도 많고 할 말도 많았기 때문인 것으로 보인다. 본문의 내용이 길었던 만큼, 여기서는 주요내용을 짧게 요약하는 것으로 글의 결론을 대신하기로 한다.

통신제한조치, 즉 감청에 대하여는 먼저 이동전화 감청여부에 대한 우리 정부의 입장을 비판하였다. 즉 미래창조과학부는 현재의 이동통신은 기술적으로 감청이 불가능하다고 밝혔으나, 반증을 통해 이러한 점이 사실이 아님을 밝혔다. 악성코드를 통한 소위 ‘감청-앱’의 활용, 또는 ‘Stingray’라고 불리는 ‘가상기지국 방식’의 감청기술이 현재의 이동통신에 대한 감청을 진행하고 있음을 내·외신의 보도자료를 통해 적시하였다. 즉 우리 정부의 입장을 신뢰할 수 없다는 것이다. 다음으로 패킷감청에 대하여는 패킷감청의 기반기술인 DPI에 대한 심도 있는 검토를 진행하지 않은 채로 단순히 통신비밀보호법상의 정의규정에 패킷감청을 대입하는 피상적인 판단을 내린바 있는 우리 대법원의 입장을 비판하였다. DPI의 기술적 특성상 감청대상을 특정할 수 없으므로 영장주의의 원리에 부합하지 않는다는 것이 주요한 논거이다. 현재로서는 헌법재판소의 올바른 판단을 기대해 보는 수밖에 없다.

통신사실확인자료에 대하여는, 먼저 통신비밀보호법 제13조의 입법상 미비를 지적하였다. 영장발부 주체의 혼돈이 있고 영장발부의 실질적 요건이 결여되어 있다는 것이다. 실질적 요건에 대하여는 이에 상응하는 미국 입법의 내용을 비교법적 검토를 위해 제시하였으며, 영장발부 주체의 혼돈의 의미를 오관하고 있는 학설에 대하여는 ‘독일 연방재판소의 결정내용’과 ‘입법연역

의 검토'를 통해 논리적 반박을 가하였다. 다음으로 가장 뜨거운 이슈인 기지국 수사, 즉 실시간 위치추적에 대하여는 '기지국과 기기사이의 단순한 교신은 통신의 개념에 포함할 수 없다'는 필자의 오랜 주장이 타당함을 입증하려 노력하였다. 즉 사용자의 의사표시를 송수신하는 것이 아니라 순수한 기술정보를 전자적으로 교신하는 것에 불과하므로 이는 통신개념에 포함될 여지가 없다는 것이다. 통신사실확인자료는 통신을 전제로 하므로, 기지국 위치정보는 결국 통신사실확인자료에 포함될 수 없다는 것이 주장의 핵심이다. 이러한 주장의 타당성을 보완하기 위하여 동일한 설시를 펼치고 있는 독일 연방헌법재판소의 판단과 미국의 입법태도를 유력한 근거로 제시해 보았다.

통신자료에 대하여는, 먼저 통신자료의 제공에 대하여 법원의 통제를 염두에 두고 있지 않고 현행 규정의 문제점을 적시하였다. 그 대안에 대하여 미국식 입법형태를 취한 바 있는 국가인권위원회의 입장을 소개하고 이에 더하여 필자의 새로운 견해를 주장하였다. 즉 통신자료를 통신비밀 보호법제가 아니라 개인정보 보호법제로 편입시키는 방법이 바로 그것이다. 그 타당성의 근거로 부합한다고 판단되는 우리 판례의 실시내용을 제시해 보았다. 다음으로 통신자료의 제공을 전기통신사업자의 재량으로 파악하고 이를 임의수사의 형태로 판단한 바 있는 헌법재판소의 입장을 비판하였다. 이 결정을 대하여 종래 헌법재판소의 입장을 따르게 된 결과라는 점에서 이론적으로는 수긍할 수는 있을지 몰라도, 통신자료의 남용이 극에 달해 있는 현실에 있어서는 전혀 타당성을 가질 수 없다는 필자의 평가이다. 그 현실적 타당성은 오히려 소수의견이 더 높다는 것이다.

참고문헌

1. 단행본

- 망중립성이용자포럼, 망중립성을 말하다, 블로터앤미디어, 2013.
 이영란, 한국형사소송법 개정판, 나남출판, 2008.
 이재상, 신형사소송법 제2판, 박영사, 2009.
 임동규, 형사소송법 제6판, 법문사, 2009.
 진계호, 형사소송법 제2판, 형설출판사, 2004.

2. 논문

- 김재윤, “통신사실 확인자료 및 금융거래정보 청구절차 개선방안 연구”, 치안정책연구소 용역 최종보고서, 2013.
 박희영, “통신사실확인자료의 저장과 통신비밀의 침해(上)”, 월간법제 2010년 5월호, 법제처, 2010.
 _____, “IMSI 및 IMEI와 휴대전화의 위치확보의 합헌성 여부”, 월간법제 2009년 11월호, 법제처, 2009.
 _____, “DPI 기술의 운영과 ISP의 형사책임”, Internet and Information Security 제2권 제1호, 2011.
 오길영, “빅데이터 환경과 개인정보의 보호방안”, 일감법학 제27호, 건국대학교 법학연구소, 2014.
 _____, “망중립성 논의에서의 DPI와 그 위법성”, 망중립성을 말하다, 블로터앤미디어, 2013.
 _____, “국가정보원의 패킷감청론에 대한 비판”, 민주법학 제48호, 2012.
 _____, “감청의 상업화와 그 위법성”, 민주법학 제43호, 2010.
 _____, “인터넷 감청과 DPI”, 민주법학 제41호, 2009.

Milton L. Mueller, “Convergence of control? Deep Packet inspection and future of the Internet”, *Communications & Convergence Review*, 제2권 제2호, 2010.

3. 기타

- 국가인권위원회, “전기통신사업법 통신자료제공제도와 통신비밀보호법 통신사실확인자료제공제도 개선권고”, 국가인권위원회, 2014.
 미래창조과학부, “’13년 하반기 통신제한 및 통신사실확인자료 제공 현황”, 보도자료, 2014.5.20.자.
 진보넷, “갈수록 심각해지는 통신 감청과 통신자료 제공 문제”, 진보네트워크센터 논평, 2014.

토론문



이창범 (경희대학교 법무대학원 겸임교수)

국가인권위원회는 수사과정에서 국민의 사생활 및 개인정보보호를 강화하기 위하여 금년 4월 「전기통신사업법」과 「통신비밀보호법」 개정을 미래창조과학부장관에게 권고한 바 있음. 일부 위원들의 소수의견이 첨부되어 있기는 하지만, 위원회의 권고 내용은 아래와 같음

첫째, 「전기통신사업법」 제83조제3항에서 규정하고 있는 ‘통신자료’(가입자 이름, 주소, 주민등록번호 등)를 ‘통신사실확인자료’에 포함시키고 법원의 허가장을 받아서 요청하게 할 것.

둘째, 통신사실확인자료를 요청할 때 현재의 영장요건인 ‘수사상의 필요성’뿐만 아니라 ‘범죄의 개연성’과 요청 자료의 ‘사건 관련성’을 추가하는 것으로 강화할 것.

셋째, 실시간위치정보를 요청할 때는 ‘수사상의 필요성’과 ‘범죄의 개연성’ 그리고 ‘범죄의 개연성’과 함께 다른 방법이 없을 것이라는 ‘보충성’을 추가할 것

발제자도 기본적으로 국가인권위원회의 위 권고를 찬성하는 입장에서 본 발표를 준비하신 것으로 이해됨. 이에 더하여 발제는 다음과 같은 사항을 추가적인 문제점으로 지적하고 있음

첫째, 매년 통신제한조치의 95% 이상이 정보기관인 국가정보원에 의해서 행해지고 있고, 이는 감청에 대한 시민들의 불안을 자극하는 국정원의 고질적 질병이라는 것임

둘째, 정부가 발표한 통신제한조치 통계에서 유선전화와 인터넷에 대한 통계만 있고 이동전화에 대한 통계가 없다는 사실을 지적하며, 통신사를 거치지 않고 국정원에 의해 직접적으로 행해지는 직접 감청 및 도청의 의혹을 제기함

셋째, 통신환경이 음성통화에서 데이터통신으로 전환되고 있는 환경에서 DPI(패킷감청) 기술을 이용한 인터넷 회선 감청의 문제점을 지적하고 있음. 즉 인터넷 회선 감청의 광범위성과 감청 대상 특정의 곤란성을 지적하며 이는 ‘포괄영장’의 문제로 구결되어 감청 대상을 미리 특정하도록 되어 있는 우리 헌법의 영장주의 원칙에 벗어나 위헌성이 높다는 것임

넷째, 통신사실확인자료에 대한 영장 신청주체를 검사 이외에 사법경찰관에게 까지 확대한

한 것은 우리 헌법이 규정하고 있는 영장주의에 대한 예외로 위헌이라 주장임. 즉 헌법상 영장은 검사만이 신청할 수 있다는 ‘검사독점적 영장청구제도’(헌법 제12조 제3항)의 취지에 어긋나 위헌성이 농후하다는 지적임

다섯째, 통신사실확인자료의 96% 이상이 기지국 정보라는 사실을 들어 기지국 수사의 문제점을 지적하고 있음. 즉 기지국 수사는 집회 참가자들을 파악하기 위한 ‘씩쓸이’ 또는 ‘저인망’ 수사라는 지적임

여섯째, 기지국과 기기와의 사이에서 자동적으로 교환되는 ‘전자적 교신 정보’ 특히 기지국 위치정보는 의사표시가 아니므로 통신의 개념에 포함시킬 수 없고, 따라서 기지국 위치정보를 통신사실확인자료에 포함시키는 것은 타당하지 않다고 주장하며 통신사실확인자료에서 제외시켜 별도의 영장발부가 필요한 새로운 부류의 정보로 분류하여 따로 규제가 필요한 입법이 필요하다고 하여 국가인권위원회의 입장을 뒷받침함

마지막으로, 통신자료 요청권을 ‘임의수사’로 보고 있는 헌법재판소의 자세를 강하게 비판함과 동시에, 일명 ‘회피연야’ 사건에 대한 2012년 서울고등법의 판결을 예로 들며, 통신자료는 개인정보에 해당하므로 ‘엄격한 요건의 영장주의’가 필요하다는 입장임

이상의 논의들은 그동안 인권시민단체들이 줄기차게 주장해온 내용과 일치하고, 토론자도 상기 국가인권위원회의 권고와 발제자가 주장하는 제도 개선 필요성에 대하여는 전체적으로 공감하는 바임. 그러나 해결 방안에 대하여는 다소 생각이 다름.

먼저, 토론자는 통신자료 등의 제공 수치가 다시 증가했다는 단순한 통계결과의 외형적 수치 외에 통계 수치의 내용까지 분석할 필요가 있음을 느낌. 주어진 자료가 충분하지 못해 정확한 팩트 파악이 어렵긴 하지만, 방송통신위원회가 발표한 자료를 보면, 첫째, 통신제한조치의 경우 요청 횟수는 증가하였으나 1회당 요청한 전화번호 수는 미세하지만 감소하는 추세이고, 둘째, 통신사실확인자료의 경우도 요청 횟수는 증가하였으나 1회당 요청한 전화번호 수는 현저히 감소하고 있음. 미세하긴 하지만 수사기관들의 자제 노력이 엿보임. 수사기관의 노력이 있다면 그 또한 평가를 해주어야 할 것임

다음으로, 통신자유침해 유형별로 감청주체를 살펴보면, 통신제한조치는 감청주체가 대부분 정보기관인 국가정보원에 의해 주도되고 있으나(96% 이상), 저인망식 수사로 비판을 받고 있는 통신사실확인자료는 검찰, 경찰, 군수사기관 등에 의한 요청이 절대적으로 많음. 특히 경찰에

의한 요청이 98%를 넘음. 법원의 통제가 전혀 없는 통신자료의 경우도 검찰, 경찰, 군수사기관 등에 의한 요청이 절대적으로 많음. 경찰에 의한 요청이 65% 수준을 넘게 유지되어 오고 있으며, 검찰도 30% 대 수준인 반면 국가정보원에 의한 요청은 1% 수준을 유지해 오고 있음.

상기의 통계 분석결과가 의미하는 바가 매우 클 것으로 생각되나 이에 대한 구체적인 원인 분석이 없는 것이 아쉬움으로 남음. 적어도 국가정보원의 수사는 통신사실확인자료와 통신자료에는 크게 의존하고 있지 아니한 것으로 분석됨. 그렇다면 검찰과 경찰이 어떤 수사를 위해서 주로 통신사실확인자료와 통신자료를 요청하고 있는지 그 의미를 분석할 필요가 있음. 따라서 그와 같은 분석의 바탕 위에서 제도개선을 논의하는 것이 보다 설득력이 있을 것임

다음으로 제도 개선으로 들어가 통신자료, 통신사실확인자료, 실시간위치정보에 대한 법원의 통제를 강화해야 한다는 원론적 입장에 대하여는 토론자도 기본적으로 동의함

그러나 형사소송법에 의한 “체포·구속·압수·수색”과 통신비밀보호법에 따른 “열람·제출”, 그리고 전기통신사업법에 따른 “제공”은 각각 그 제도의 배경이 다른 바 이를 동일시 할 수는 없으며 통제의 수준을 달리해야 할 것임. 통신사실확인자료도 그 제출이 강제되고 있는 한 기본권 침해 소지가 있는 것은 당연하고, 자료제출요구도 그것이 사실상 강제되는 경우에는 기본권 침해의 위험이 있다 할 것임. 그러나 이와 같은 기본권 침해 위험이 있다고 해서 이들을 모두 “검사”가 청구한 영장에 의해야 한다는 것은 헌법이 규정한 “체포·구속·압수·수색”의 의미를 확대 해석한 측면이 있음

토론자는 개인적으로 **전화감청, 패킷분석 등 통신제한조치나 실시간 위치추적**은 사실상 “체포·구속·압수·수색”과 그 성질이나 위험성 면에서 동일·유사하므로 엄격한 영장주의에 의해야 할 것이지만, **통신자료의 제공 요청과 통신사실확인자료의 열람·제출 요청**에 대해서는 완화된 영장주의나 영장주의 외의 입법·행정적 통제 방식도 가능해야 한다고 봄.

즉, 토론자는 앞서서도 경찰과 검찰이 통신자료 및 통신사실확인자료를 요청한 수사의 목적 또는 내용에 대한 분석이 선행되어야 한다고 전제한 바 있으나, 그 같은 분석을 토대로 하여 수사의 목적에 따라 차별화된 접근방법이 인정되어야 한다는 것임. 예컨대, 오늘날과 같이 정보인권에 대한 시민들의 인식이 강화된 현실에서, 통신자료 또는 통신사실확인자료의 요청이 단순히 **수사상 편의나 효율성**을 위한 목적으로 이용되거나, 시위참가자 색출, 노동운동 감시, 정치 사찰 등 이른바 **공안 목적**으로 이용되는 것은 더 이상 용납되기 어려울 것임. 이와 같은 목적의

통신자료 등 제공 요청에 대해서는 형사소송법상 일반 영장주의에 따르도록 해야 함

그러나 **흉악범, 연쇄범, 탈세범, 외환사범, 국가안보사범** 등의 수사에 대해서는 완화된 영장주의 내지 영장주의 외의 통제장치가 적용되어야 함. 현행법의 문제점은, 통신제한조치와는 달리, 통신자료 및 통신사실확인자료의 열람 또는 제출 요청은 범죄의 내용에 관계없이 수사 또는 형의 집행을 위하여 필요하면 언제든지 할 수 있도록 광범위한 예외를 인정하고 있다는 것임

따라서 시급성을 요하는 중대범죄에 대하여 제한적으로 완화된 영장주의를 적용하거나 영장주의의 예외를 인정하더라도 그것이 위헌적이라 보지 아니함. 개인정보 보호법과 위치정보법에서도 “정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우”에는 동의 없는 개인정보 수집·이용을 허용하고 있음.

미국의 경우도 통신자료에 대해서는 엄격한 영장주의를 적용하지 않고 ‘소환장’제도를 채택하고 있으며, 통신사실확인자료에 대해서도 완화된 영장주의를 적용하고 있음. 결론적으로 토론자는 통신제한조치, 통신사실확인자료 열람·제출, 통신자료 요청의 위험성을 구분하지 않고 기본권 침해 위험이 크다는 이유로 획일적으로 엄격한 영장주의를 적용하는 것은 바람직스럽지 않다는 생각이며, 오히려 차별화된 접근방법이 시민의 권리보호에 더 유익할 수 있음

또한, DPI를 이용한 인터넷 회선 감청이 헌법상 허용되느냐 아니냐의 논의는 학문적으로는 매우 의미 있는 이슈일 수 있으나, 실무적으로 보다 더 중요한 것은 인터넷 회선 감청의 남용을 막고, 적법한 수준의 감청을 담보하기 위한 논의라고 생각함. 이미 여러 가지 다양한 목적으로 패킷 감청 방법이 광범위하게 이용되고 있는 현실에서, 수사기관에 대해서만 인터넷 회선 감청을 금지하는 것은 현실성이 없어 보임. 이번 발제를 배경으로 해서 이 문제를 양지로 끌어내어 인터넷 회선 감청의 목적, 방법, 범위 등에 대한 보다 심도 있는 논의가 요망됨.

토론문



유주성 (경찰교육원 교수)

전기통신사업법 제83조 제3항에서는 전기통신사업자에게 수사기관이 수사목적으로 정보수집을 위해 요청하면, 이용자의 성명, 주민등록번호, 주소, 전화번호, ID, 이용자의 가입일 또는 해지일 등 6개항 정도의 통신자료를 적극 지원할 수 있도록 규정하고 있다. 이는 헌법 제17조에서 보장된 기본권인 사생활의 자유는 헌법 제37조 제2항에 따라 국가안정보장·질서유지·공공복리를 위하여 필요한 경우 법률로서 제한될 수 있다 것을 근거로 하고 있다고 보인다. 민주주의 사회에서 수사기관의 역할은 범죄를 진압하는 역할을 통해 공공의 안전을 보장함으로써 국민들 각자가 자유와 권리를 향유할 수 있는 기초적인 토대를 제공하는 것이므로, 수사기관이 수사 목적을 신속히, 효율적으로 달성할 수 있는 제도적 장치를 마련해 주는 것은 의미가 있다. 하지만 수사기관의 활동은 기본권 침해 위험성이 항상 존재되어 있으므로 남용되어서는 안 되고, 수사목적이나 필요성에 따라 한정되어야 한다. 그러나 최근 3년간 수사기관에 제공한 통신자료 제공 현황을 분석해보면, 전반적으로 급격한 증가 추세에 있음을 알 수 있다. 이에 대해 최근 인권 위원회에서는 수사기관이 통신자료 요청을 지나치게 남발하고, 전기통신사업자들은 기계적으로 제공하고 있다고 지적하면서, 통신자료 제공절차에 있어 영장주의 적용을 수사기관의 통신자료제공 요청 남용에 대한 예방책으로 권고한바 있다. 그리고 국회에서도 수사기관의 통신자료 요청 남용에 따른 국민의 기본권 침해를 우려하여 영장주의 적용과 이용자에게 고지 의무를 신설하는 것을 골자로 한 전기통신사업법이 개정발의 되기도 하였다. 특히, 2012년 10월에는 NHN의 수사기관에 대한 통신자료 제공에 대해 서울고법에서 손해배상판결을 함으로써, 포털 3사(NHN·다음·네이트) 등 주요 전기통신사업자들이 판결 선고일로부터 수사기관의 통신자료 제공중단 결정을 함으로 일반압수수색영장을 받아서만 통신자료 취득이 가능하도록 수사 실무 환경이 변화되기도 하였다.

하지만 통신자료제공절차를 강제수사화 하여 영장주의를 일괄적으로 적용하려 하는 이러한 움직임에 대해, 실무상 수사의 효율성과 사법통제의 실효성 확보 측면에서 많은 문제점들이 예상된다. 우선 수사 실무상으로 수사기관의 통신자료 요청은 수사를 위한 정보 수집을 위하여

전기통신이용자 중 어떤 인물을 특정 하는데 그 목적이 있다고 할 수 있다. 이미 특정된 인물이 어떠한 통신을 하였는지 사실 확인을 하는 과정에 앞서, 그 인물이 누구인지 특정하여 수사의 단서로 삼을지를 결정하는 과정이다. 따라서 통신자료취득행위는 대부분 수사 초기 단계에서 이루어지고, 최근에는 전기통신을 이용한 범죄뿐만 아니라 일반 범죄에까지 전화번호 등 단서를 이용 용의자를 특정하고, 수사범위를 좁혀나가기 위해서도 활발하게 이용되고 있다. 2012년 기준 검찰, 경찰, 국정원 등 수사기관이 연간 약 팔십만 건(문서건수 기준) 가까이 활용한 통신자료제공 요청에 대해, 법원의 사전 영장 신청절차를 반드시 거쳐야 한다면, 수사의 차질은 자명하다. 대부분의 일반사건을 처리하고 있는 경찰을 기준으로 보면, 법원의 영장을 신청하고 검사의 청구에 따라 법원이 발부한 영장을 받아 전기통신업자에게 통신자료 제공을 요청하여 이를 다시 받는 과정에만 최소 2-3일 이 소요되어, 수사의 지연과 이에 따른 일선의 부담감은 상상을 초월한다. 그나마 현재에도 과도한 사건 처리수와 수사 인력 부족 문제 등으로 수사기간 내 신속한 사건 처리에 어려움을 토로하고 있는 일선 수사관들의 어려움은 더욱 가중될 수밖에 없을 것이다. 또한 대부분 강력사건의 경우에는 수사의 성공요인이 신속한 초기대응에 있다는 점을 감안하면, 이와 같은 수사 지연은 국민의 안전에 큰 위협이 될 수 있다. 예를 들어, 인터넷 포털사이트에서 살해 혹은 테러 협박을 한 용의자에 대한 신속한 신원특정이 불가하여, 효과적인 진압이나 예방활동을 하지 못하게 된다면, 치명적인 결과를 가져올 수밖에 없을 것이다. 더욱이 현재 법원은 압수수색 영장 발부 시 그 요건을 범죄의 혐의를 어느 정도 명백히 할 것을 요구하고 있는데, 피의자 특정도 제대로 하지 못한 상태에서 해당 피의자의 협의를 구체화하는 일은 일선 수사관들에게 지나치게 큰 부담을 지우는 것이라 생각된다.

또 다른 측면으로, 그간 전기통신사업자의 형식적 판단에 따라 수사기관에 제공되어 오던 통신자료에 대해, 영장주의를 전면 도입하는 것은 이제부터 법원이 수사기관의 요청에 대해 구체적이고 내용적인 측면까지 판단하여야 한다는 것을 의미한다. 현재 기준으로 검찰, 경찰 국정원 등이 연간 팔십만 건 이상 되는 통신자료 요청하는 것에 대해, 법원이 과연 실효성 있는 통제를 할 수 있을지 의문이 들 수밖에 없는 대목이다. 이미 수사기관이 '통신사실 확인자료' 등 제3자 보유한 통신정보 제공요청에 대해 허가장(영장) 제도를 실무적으로 운용함에 있어, 사법적 통제 의 실효성이 결여되는 문제점이 있다는 것은 그간 이미 판사 등 사법실무자들을 중심으로 수차례 제기된 바 있다. 특히 이와 관련하여 설민수 판사의 지적은 귀 기울일 만하다: "제3자 보유 정보에 대한 자료제출요구에 대한 영장주의의 확대문제는 법의 규율이 발전함에 따라 어떻게

보면 피할 수 없는 일인지 모를 일이다. 그런데 현재와 같은 영장주의 하에서는 형식적 영장주의가 확대된다고 하여도 이를 억제하는데 별 실효성일 없을 수 있다. 광범위한 영장주의가 적용되는 ISP에 대한 자료제출요구와 그에 따라 발부되는 영장의 실태는 이렇게 형식적인 외형으로 확대된 영장주의가 가진 실효성의 한계를 잘 보여주는 것인지도 모른다.” 영장주의의 확대에 단순히 그 외면적인 형식적 절차만이 아니고 그 실효성을 확보할 수 있는 제도적 개선이 따르지 않는다면, 광범위한 형식적 영장주의의 적용에도 불구하고 실질적인 사법적 통제가 제대로 작용하지 않는 문제가 발생할 수밖에 없다.

법리적으로 살펴보다라도, 통신자료 제공절차를 강제수사화 하는 부분은 임의수사의 한 형태로 ‘사실조회’ 절차를 두고 있는 우리 형사소송법 체계와도 맞지 않는다. 통신자료 제공절차에 있어 영장제도를 전면적으로 도입하기보다는, 수사의 신속성·효율성을 해치지 않으면서도 실효성 있게 통신자료제공 요청남용을 제한할 수 있는 새로운 개념의 통제수단이 ‘개발’되어야 하는 이유이다. 대체적 통제방안으로 우선, 앞서 언급한 고등법원 판결에서처럼, 전기통신사업자에게 강력한 개인정보보호 의무 부담을 지우고 수사기관의 통신자료제공 요청 시 절차적, 내용적 심사를 철저히 하도록 하는 방법이 있다. 하지만 이 경우, 대부분의 전기통신사업자는 민사상 책임에 대한 부담 때문에, 심사권을 포기하게 되고, 이로 인해 전통법상의 자료제공 규정이 사실상 무력화될 수밖에 없게 되므로 바람직하지 않다. 더욱이 사기업에게 엄청난 민사상 책임부담을 떠안은 채 사법기관에 준하는 판단까지 하도록 책임을 지우는 것은 무리라고 생각된다. 전기통신사업자들에게 형식적·절차적 심사 정도만 제대로 하면 되는 수준으로 책임성을 한정하고, 필요하다면 통신사업자와 수사기관이 통신자료 협조 시 준수해야 할 절차, 기준·범위, 등을 정한 ‘통신자료 제공 관련 가이드라인’을 마련하여 전기통신사업자에게 이에 대해서만 심사를 제대로 하도록 하는 방식이 검토되어야 한다.

둘째, 현재에는 이용자가 수사기관 등에 제공한 자신의 개인정보 열람 또는 제공을 요구하고 있으나, 전기통신 사업자가 수사상의 이유로 열람을 거부함에 따라 법률분쟁이 발생하고 있는 점 등을 감안하여, 수사상 지장을 초래 하지 않는 범위에서 통신자료 제공 현황의 열람 및 제공 범위에 관한 검토도 필요하리라 생각된다. 그리고 통신사실제공에 대해 수사 결과 혐의가 없을 시 당사자에게 통보조차 이뤄지지 않는 현행 실무관행은 문제가 있는 것으로 보이므로, 정보통신사업자의 개인정보보호의무의 일종으로 ‘사후통보의무’를 신설할 필요가 있다. 이를 통해 사전에 법원 허가를 받고 중간 또는 사후에 당사자에게 처리 결과를 통보해야 하는, 압수수색이

나 ‘금융거래내역’, ‘통신사실 확인자료’ 조회 등에 건취 형평성에 맞는 최소한의 보완장치가 될 수 있을 것이다. 그리고 수사기관에게도 수사 종료 후 일정기간 내 당사자에게 통신자료가 제공되었다는 사실에 대해 고지 의무를 부과하는 것도 함께 검토되어야 할 것이다.

셋째, 수사기관의 통신자료제공 요청에 대한 사법기관의 통제가 필요하다면, 사전적 통제(영장통제)보다는 사후적 통제방안(목록제출) 신설을 생각해 볼 필요가 있다. 통신제공은 수사초기 단계에서 피의자 특정 등을 위해 신속하게 이루어져 하는 점을 감안하여, 일단 수사기관에게 요청에 대한 1차적 판단을 맡기고, 사후적으로 ‘통신자료제공 요청목록’ 등을 법원에 제출하도록 하여 남용된 부분이 없는지를 일괄적으로 검토하도록 하는 방안이다. 이를 통해 수사기간의 효율성을 해치지 않으면서도, 법원의 사후 통제를 고려하여, 수사 목적성, 필요성 등 판단에 더욱 신중을 기하게 함으로써, 무분별한 통신자료제공은 방지될 수 있으리라 기대된다. 더욱이 법원이 개인정보보호법 제71조 등을 적용하여 필요시 민사·형사·행정상 책임을 해당 수사관에게 물을 수 있을 것이기 때문에, 그 실효성에 있어서도 의문의 여지가 없다.



권양섭 (군산대학교 법학연구소 연구교수)

I. 들어가며

사이버 수사 및 디지털 증거수집과 관련하여 다양한 논의가 이루어지고 있다. 시민단체뿐만 아니라 학계에서도 찬반 논쟁이 뜨거우며, 법원과 국회에서는 서로 다른 판결과 입법안이 연이어 나오고 있다. 이제는 그동안의 논의를 바탕으로 국민의 정보인권보장¹⁾에 부합하는 결과물을 생산할 때이다. 그동안의 통신자료수집에 대한 논의의 핵심은 다음 두 가지로 요약정리 할 수 있다.

첫째, 통신자료제공제도가 남용되고 있다.

둘째, 이를 개선하기 위한 방안이 필요한데 “개인정보보호 및 표현의 자유”와 “수사의 효율성 및 신속성”이라는 두 가치간의 대립을 어떻게 조화시킬 것인가?가 문제의 핵심이다.

정보통신법분야에서 다양한 연구와 활동을 하고 계시는 오길영 교수님의 발제문에 대한 전체적인 취지에는 동의하나 각론분야에 있어서 다소 의견이 다른 점이 있다.

II. 쟁점분야에 대한 검토

1. 통신제한

가. 주요내용

- (1) 통신제한조치가 남용되고 있으며, 미래창조과학부의 입장과는 달리 이동전화도 감청이 가능하다.

1) 정보인권(Information and Communication technology and Human Rights)이란 “정보사회에서 정보의 유통에 대한 개인의 통제권을 의미하는 것으로, 개인의 존엄과 자유를 보장해주는 기본적인 인간의 권리이며, 정보의 자유(정보소통의 권리)와 정보프라이버시권을 포함한 정보유통의 통제에 관한 권리들의 다발이라고 할 수 있다”.(박성훈, “정보인권 소개 및 침해사례 발표”, 국가인권위원회 부산·경남 지역순회 정보인권 교육 및 토론회, 2011, 4쪽.

- (2) 패킷감청은 감청의 범위만이 아니라 아예 감청의 대상 자체가 특정가능성이 없어 영장주치의 원리에 정면으로 배치된다. 따라서 허용되는 수사방법이 아니다.

나. 토론자견해

(1)번 주장에 대한 검토: 유보

- ▶ 지난 12년간(2002~2013) 통신통신제한조치 현황을 분석해 보면 <표-1>과 같다. 2012년에 비해 2013년에는 수치가 증가하였으나, 2010년 이전에 비하면 상당부분 감소하고 있는 것으로 분석된다.
- ▶ 발표자의 의견처럼 이동전화 감청이 기술적으로 불가능한 것은 아니다. 다만, 소위 '감청-앱'을 활용하거나, '가상기지국 방식'으로 가능하다보니 현실적인 어려움이 있을 뿐이다. 이와 같은 현실적인 어려움을 해결하고자 이동통신사업자에게 감청장비 설치를 의무화하는 통신비밀보호법 개정안²⁾이 제출되었다.

<표-1> 12년간 통신수단별 통신제한조치 현황

년도	유선전화	이동전화	인터넷	합계
2002	1,013	169	346	1,528
2003	1,097	216	383	1,696
2004	887	265	461	1,613
2005	621	1	355	977
2006	577	0	456	1,033
2007	503	0	646	1,149
2008	506	0	646	1,152
2009	574	0	942	1,516
2010	358	0	723	1,081
2011	261	0	446	707
2012	182	0	265	447
2013	191	0	401	592

*자료: 미래창조과학부, 방송통신위원회 홈페이지 보도자료

2) 2014.01.03. 서상기의원 대표발의 통신비밀보호법 일부개정법률안(의안번호: 8985).

(2)번 주장에 대한 검토: 반대

- ▷ 패킷감청의 경우 영장의 특정성을 다소 완화하여 해석할 필요성은 있으나, 영장주의를 실현할 수 있는 가능성이 전혀 없는 것은 아니다. 따라서 원칙적으로 가능한 수사방법이다. 다만, 영장주의의 특정성 요건을 갖추지 못하였거나, 이를 실현할 수 없다면 법원이 심사하여 영장을 기각해야 할 것이다.

예) 해당 정보통신기기를 피의자 혼자 사용하는 경우 → 허가요건 충족시 허용, 다수 및 불특정인이 사용하는 경우 → 기각

- ▷ 자세한 사항은 권양섭, “인터넷 패킷감청의 허용가능성에 관한 고찰”, 법학연구 제39집, 한국법학회, 2010.08.25. 참조

2. 통신사실확인자료

가. 주요내용

- (1) 통신비밀보호법 제13조는 ‘서면’이라는 형식적 요건을 제외하면 영장발부에 대한 실질적 요건이 전혀 명시되어 있지 않는 상태이다.
 - (2) 실시간 위치추적용 기지국 정보는 통신사실확인자료의 범주에 포함시키는 것은 타당하지 않다. 기지국 위치정보를 별도의 영장발부가 필요한 새로운 분류의 정보로 분류하고 따로 규제하는 입법의 신설이 타당하다.
- ☞ 구체적인 내용과 절차는 제시되어 있지 않으나, 국가인권위원회의 권고안과 같은 입장으로 판단됨

나. 토론자 견해

(1)번 주장에 대한 검토: 찬성

현행 통신비밀보호법 제13조는 “수사의 필요성”만을 요건으로 하고 있으나, “범죄혐의 개연성”과 “관련성 요건”을 추가할 필요가 있다. 다만 어느 정도의 범죄혐의의 정도가 존재해야 하는지에 대해서는 압수수색영장에서 요구하는 “최초의 혐의 또는 단순한 혐의”로 족하다고 판단된다.

(2)번 주장에 대한 검토: 제한적 찬성

과거의 기지국 위치기록이 아닌 현재의 기지국 위치기록(실시간 위치정보)은 단순한 개인정보의 문제를 넘어 신체의 자유와도 밀접한 관련성이 있다. 따라서 다른 통신사실확인자료와는 달리 취급되어야 한다.

발제자의 주장처럼 실시간 위치추적용 기지국 정보를 통신사실확인자료의 범주에 포함시키는 것은 타당하지 않으며, 국가인권위원회 권고안처럼 ‘실시간 위치정보’에 대한 정의규정을 신설하고, 별도의 수집절차를 규정해야한다.

다만, 국가인권위원회 권고안처럼 보충성의 요건을 적용하기 보다는³⁾ 대인적 강제처분과 유사한 면이 존재함으로써 체포영장에서 요구하는 사유 수준⁴⁾에서 요건을 규정하는 것이 타당하다고 보여진다.

3. 통신자료

가. 주요내용

- (1) 전기통신사업법 제83조 제3항은 통신과 관련성을 인정하기는 어렵다. 단지 이용자 개인의 신상정보이다. 통신비밀 보호법제가 아니라 개인정보 보호법제로 편입시키는 것도 또 하나의 방안이 될 수 있다.
 - (2) 통신자료제공에 대해서도 영장주의 적용한다.
- ☞ 구체적인 입법안은 제시되어 있지 않으나, 국가인권위원회의 권고안과 같은 입장으로 판단됨

3) 국가인권위원회, “전기통신사업법 통신자료제공제도와 통신비밀보호법 통신사실확인자료제공 개선 권고”, 2014, 1쪽, 13쪽; 본 보고서에서는 체포 구속영장의 경우에도 감청영장과 마찬가지로 보충성의 요건을 요구한다고 기술되어 있으나(해당 보고서 표-6 참조), 이에 대해서는 의문이다.

4) 체포영장이 발부되려면 ①피의자가 죄를 범하였다고 의심할 만한 상당한 이유가 있고, 다음으로 ②정당한 이유 없이 수사기관의 출석요구에 응하지 아니하거나 응하지 아니할 우려가 있어야 한다(형사소송법 제200의2 제1항). 또한 형사소송규칙 제96조의2 해석상 ③증거인멸의 우려와 도주우려의 요건도 요구된다고 해석되어지고 있다(신동운, 신형사소송법 제4판, 법문사, 2012, 253쪽).

나. 토론자 견해

(1)번 주장에 대한 검토: 반대

통신자료도 인터넷상에서 게시판에 글을 쓰거나 이메일 등을 발송할 때에는 단순히 'ID나 닉네임'이 아닌 통신과 관련된 정보로 볼 수 있다. 카페나 토론광장 게시판 등에 글을 작성하여 올렸다고 가정하였을 때 작성자의 신상정보는 게시판에 올려진 글과 결합하여 통신의 일부가 될 수 있기 때문이다. 따라서 통신자료도 통신의 비밀이라는 헌법상의 기본권으로써 보호받아야 한다.

(2)번 주장에 대한 검토: 제한적 찬성

“전기통신사업법 제83조 제3항의 통신자료제공은 기간통신업무 사업자보다 부가통신업무 사업자에게서 주로 문제가 제기되고 있다.”

- 사례: 갑은 '집에 강도가 침입 구조바람' 이란 문자메세지를 112로 보냈다. 신고를 접수받은 경찰은 전기통신사업자에게 핸드폰번호에 대한 통신자료와 통신사실확인자료 제공을 요청하였다.
- 사례: 갑은 인터넷 포털 사이트 게시판에 을에 대한 글을 올렸다. 을은 갑의 글이 자신의 명예를 훼손하였다며 갑을 고소하였고, 경찰관은 전기통신사업자에게 해당글을 작성한 자의 인적사항을 요청하였다.

◇ 전기통신사업법 제83조 제3항은 개인정보 보호와 표현의 자유, 전기통신사업자의 영업권을 침해하는 조항임에는 틀림없으나, 찬반 의견이 팽팽하게 대립하고 있는 상황에서 반대 의견을 일부 수용한 절충설을 제안해 보고자 한다. 참고로 2012년 11월 1일 주요포털은 영장에 의하지 않는 통신자료제공 요청을 거부하겠다고 발표하였으나, 2013년 상반기에도 전기통신사업자가 제공하는 통신자료의 수는 감소하지 않고 오히려 증가했다.⁵⁾

본 토론자가 제안하는 방식은 전기통신사업법 제83조 제3항을 삭제하기보다는 개선하는 쪽으로 제도를 운영해 보고, 폐해가 지속적으로 발생한다면 국가인권위원회 권고안처럼 통신사실확인자료로 편입하는 방안을 논의해 보고자는 것이다.

이와 같은 제안은 통신자료제공 제도 폐지를 반대하는 입장에서 제시하는 근거뿐만 아니라,

5) 2013년 상반기 전기통신사업자들이 수사기관에 협조한 통신자료 제공건수는 465,304건으로 전년 동기(395,061건) 대비 17.8% 증가하였다.

법원의 심사와 허가를 받도록 절차를 규정한다하더라도 자칫 이 절차가 형해화 될 우려가 존재할 수 있다는 점, 단순히 이용자 신상정보를 알기 위해서 통신사실확인자료 제공 절차를 거치게 한다면, 통신사실확인자료절차가 주는 무게감이 떨어져 통신사실확인자료에서 보호하고자 하는 다른 정보들의 중요성이 간과될 우려가 있다는 점에서 제기해 보았다. 형해화 우려는 현재의 통신사실확인자료의 현황과 제공요청에 대한 법원의 기각률⁶⁾을 보면 알 수 있다.

◇ 현행 통신자료제공 조항 개선안

- 광범위한 자료제공을 제한하기 위한 방안: 전기통신사업법 제83조 제4항 개정

제83조(통신비밀의 보호) ④제3항에 따른 통신자료제공 요청은 제3항 각호의 자료⁷⁾ 중 하나를 특정하고 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 하여야 한다.

- 인터넷상의 표현의 자유 침해 문제를 해결하기 위한 방안

- 제1안: 전기통신사업법 제83조 제3항 적용범위에서 부가통신역무⁸⁾를 제공하는 사업자는 제외
- 제2안: 「정보통신망 이용촉진 및 정보보호등에 관한 법률」 제2조 제9호⁹⁾에 대한 정보수집은 제외

6) 국가인권위원회, “전기통신사업법 통신자료제공제도와 통신비밀보호법 통신사실확인자료제공 개선 권고”, 2014, 7쪽 참조.

7) 이용자의 성명, 이용자의 주민등록번호, 이용자의 주소, 이용자의 전화번호, 이용자의 아이디, 이용자의 가입일 또는 해지일

8) “기간통신역무”란 전화·인터넷접속 등과 같이 음성·데이터·영상 등을 그 내용이나 형태의 변경 없이 송신 또는 수신하게 하는 전기통신역무 및 음성·데이터·영상 등의 송신 또는 수신이 가능하도록 전기통신회선설비를 임대하는 전기통신역무를 말하며, “부가통신역무”란 기간통신역무 외의 전기통신역무를 말한다.

9) 동법 제2조 제9호 “게시판”이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램이나 기술적 장치를 말한다.

Ⅲ. 결론

신속한 범죄대응과 효율적인 수사를 위해서는 통신자료 제공 제도가 필요한 것은 사실이지만, 인권보장을 위한 법률적 노력을 간과해서는 안 된다. 수사기관에 제공되는 통신자료(통신사 실확인자료 등)에 대한 요건을 현재보다는 엄격하게 개정하여 기본적인 개인정보자기결정권과 표현의 자유를 보장해 줄 필요성이 있다.

국가인권위원회의 권고 결정과 오늘의 포럼이 국민의 정보인권을 보장하는데 기여하길 바란다. 끝.

토론문



최성진 (한국인터넷기업협회 사무국장)

먼저 이번 정보인권포럼이 국내 정보인권 향상에 중요한 계기가 될 것으로 기대하며, 특히 정보수사당국의 통신데이터의 요청에 대하여 의견을 드릴 수 있는 자리를 갖게 되어 매우 기쁘게 생각합니다.

오길영 교수님께서 발제문을 통해 지적하신 바와 같이 정보수사기관 등이 요청하는 통신데이터의 대부분이 개인식별정보로서 중요한 개인정보임에도 불구하고 제공 건수가 점차 증가하고 있는 현실이 매우 우려스럽습니다. 또한 외국과 달리 국내에서는 관련 법령의 미비와 개인의 프라이버시권과 개인정보자기결정권에 대한 부족한 인식으로 인하여 통신데이터가 비교적 쉽게 정보수사기관 등에게 제공되고 있다는 현실인식에 동의합니다.

기업의 입장에서도 그동안 정보수사기관의 제공 요청에 대하여 명확한 기준과 책임소재 문제에 있어 많은 어려움과 혼란을 겪고 있었습니다. 이에 오 교수님께서 이미 좋은 말씀을 하셨기에 간략히 현행 법령의 문제에 대해서만 좀 더 이야기 해보고자 합니다.

우선 영장이나 법원의 통제 없이 통신자료를 요청하고 제공하는 것에 대하여, 현행 「전기통신사업법」 제83조 3항에 따르면, 전기통신사업자는 수사관서의 장이 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 통신자료제공을 요청하면 그 요청에 따를 수 있도록 되어 있습니다. 문구상으로는 임의수사의 성격을 가지고 있으며, 비록 헌법재판소 결정에 따르면 통신자료제공은 전기통신사업자의 재량사항으로 의무사항이 아닌 것으로 보고 있지만, 수사기관의 요청을 받은 사업자의 입장에서는 이를 거부하기가 곤란한 경우가 상당하다고 할 것입니다. 즉 오 교수님께서 말씀하신 바와 같이 정보수사기관의 요청에 대하여 별도의 기준과 심사 능력이 없는 사업자의 입장에서는 실질적으로는 강제수사와 같은 것으로 볼 수 있을 것입니다. 따라서 본 조항은 통신자료 요청 시 법원의 영장을 받을 필요가

없도록 하고 있어 영장주의 및 적법절차 원리를 위반하고 있다고 보입니다.

이에 「전기통신사업법」 제83조 3항은 사업자 재량(임의)으로 이용자정보를 제공하는 것으로 심각한 개인정보 침해가 발생할 우려가 있으므로 영장주의에 따르도록 개정되거나, 통신비밀보호법에 포함시켜 「전기통신사업법」에서는 삭제하는 것이 바람직 해 보이며, 2013년에 변재일 의원이 대표발의한 「전기통신사업법」 일부개정안(의안번호 1904976) 과 같이 요청에 법원의 허가를 받고 해당 서비스 이용자에게 이를 통지하는 내용으로 법 개정이 이루어져야 할 것입니다.

이와 더불어 「통신비밀보호법」 제13조에서는 정보수사기관이 온라인사업자에게 이용자의 IP 주소와 인터넷로그기록 등 통신사실확인자료를 요청할 때 법원의 허가를 받도록 하고 있으며 사업자의 협조 의무를 규정하고 있는데, 법원이 통신사실확인자료의 범위를 로그인 기록뿐만 아니라, 서비스 이용 기록 일체를 로그기록을 이해하고 MAC Address까지 통신사실확인자료에 포함하고 있는 등 지나치게 광범위하게 해석하고 있습니다. 이에 불필요하거나 1건의 허가를 가지고 별건의 수개 통신사실확인자료를 요청하는 경우도 있어, 통신사실확인자료의 정의를 '로그인 기록'으로 명확하게 하고 그 심사기준 및 연장절차 등을 좀 더 엄격하게 규정하도록 개정하는 것도 또한 필요할 것입니다.

더 나아가 실제 정보수사기관의 요청에 대응하여야 하는 업무를 진행할 사업자의 입장에서는 정보수사기관의 요청으로 인한 서비스 이용자와의 분쟁 및 사업역량의 분산을 막기 위하여, 정보수사기관에서는 자료요청 채널을 단일화하고, 단일화하여 사업자에게 자료요청 하도록 하며, 자료요청 시 요청양식과 구체적인 요청 방법도 함께 법제화가 이루어질 필요가 있다고 보입니다.

끝으로 위에 말씀드린 내용이 본 포럼과 이후 여러 관계자 분들의 노력으로 법령에 반영되어 국민의 인권향상과 더불어 국제적 기준에 합당하도록 규제가 개선되었으면 하는 바램입니다.

끝.

■ 정보인권 포럼_ 정보통신서비스 이용과 개인정보자기결정권 보장을 중심으로

제1세션 : 본인확인제의 현황과 정책적 방향

- 발제: 김기창 (고려대학교 법학전문대학원 교수)
정민하 ((주)네이버 정책협력실 실장)
- 토론: 심우민 (국회입법조사처 조사관)
박찬욱 (방송통신위원회 개인정보보호윤리과)
박성훈 (국가인권위원회 인권정책과)

온라인상 본인확인 : 제도와 정책

김기창
(사)오픈넷, 고려대 법학대학원

2014.6.10

Offline ID 와 Online ID

- 카드 형태의 Offline ID
 - '사진 ID' 기반으로 한 '육안' 확인
 - ID카드 위조하거나, 성형수술 하거나
 - 각 서비스 제공자가 대면 확인. 서비스 제공자가 고객 번호 유지, 관리
- Online ID credentials
 - ID + password
 - 개인인증서, 기타 'token', token 최초 부여 단계, 그 후 배타적 귀속 유지 필요
 - 유출 위험, 정보집적 위험
 -

주민등록번호

- Offline ID 체계를 별 생각 없이 Online ID 화 해버린 disaster 사례
- 심지어, 이름 =ID, 주민번호 = passwd 로 오해
- 국내 보안 기술 및 지식 수준의 미개함 노정
- “생년월일”을 만천하에 공개하는 후진성
- 이미 회복 불가능한 수준으로 유출, 노출
- 주민등록번호제에 대한 헌법적 쟁점 (헌법재판소, 2013.2)
- 그대로 두는 것은 국가의 ‘고의’ 또는 ‘중대한 과실’

Universal ID ?

- 모든 서비스를 모조리 관통하는 ID ?
 - 심각한 보안 위험 자초하는 몰상식한 발상
- Customer Number 개념 도입 필요
 - 민원 서비스, 전기, 가스, 보험, 금융, 오락 등 각 서비스 제공자가 자신의 고객 관리용 unique ID 부여하고 관리하는 것이 정상
 - Tax ID: 사업자번호, 현금영수증 발급번호 사용하면 됨 .
 - 소득 공제: 원하는 납세의무자가 관련 거래 주체들에게 자신의 tax ID 등록하면 됨

민원용 Online ID

- 민원용 Online ID 제도
 - 기존 user → 공인인증서를 민원용 Online ID+passwd 로 대체
 - 신규 user → 동사무소에서 대면확인 후 ID+passwd 교부
- 전자서명, 부인방지 환상은 이제 그만
- 전자문서도 문서 (전자서명 없어도 적법한 문서)
- 서비스 성격에 상응하는 보안대책 적용
- 서버측에서 이상징후 탐지해서 부정사용에 대처
 - 구글 2 step 로그인 참조

민간영역의 Online ID

- 주민등록번호 사용 전면 금지 (예외 없이)
 - 지리적 국가적 경계 없는 “인터넷”
- 서비스제공자들은 주민등록번호가 아니라, 자신의 고유한 고객번호 이미 구비하고 있음.
- 신용정보업체 등은 각자가 적절한 방법 고안
 - 신용정보업체 영업 편의 위해 온 국민 희생?
 - 외국 신용정보 업체들의 know how 배울 필요

이미 다양한 고객번호 존재



정통방법상 본인확인기관 지정권

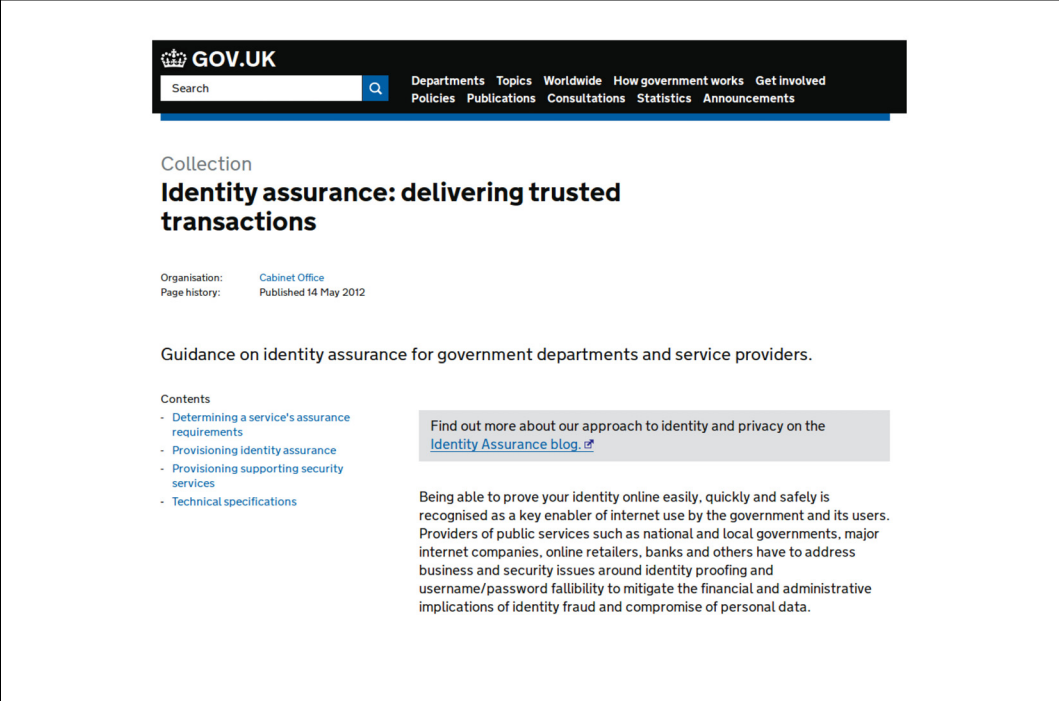
- 44 조의 5 (게시판이용자 본인확인)
 - 공공기관등 (국가기관 , 지방자치단체 , 공기업 · 준정부 기관 , 지방공사 · 지방공단) 이 운영하는 게시판 본인확인 필요
- 이걸 핑계로 본인확인기관 ‘지정권한’ 행사 (23 조의 3)
 - i-PIN 사업자 (서신평 , 한신평 , KCB) 이통 3 사 , 공인 인증업체 등이 본인확인기관 지정받음
- ‘공인’ 본인확인기관의 부조리함 재현

공직선거법, 정보법 등

- 공선법 82 조의 6: 선거운동기간 중 ‘실명확인’
 - 안행부장관의 실명확인
 - 신용정보업자의 실명확인
 - 정통망법상의 ‘본인확인’
- 정보법 시행령 제 17 조 (나이 및 본인확인 방법)
 - 공인인증서
 - I-PIN 등
 - 신용카드 인증
 - 휴대전화 인증

Online Identity Management

- 국제적 사업 가능성이 열린 분야의 사업기회 박탈
- 정부 독점, 정부지정 사업자 독점,
 - ‘국내용’ 온라인 ID 체계
 - 휴대전화 실명제를 전제로 하는 발상
- OAuth 등 활용?
- www.miicard.com www.doublecheckid.com
- 영국 정부 사례
<https://www.gov.uk/government/collections/identity-assurance-enab>
- SAML (Security Assertion Markup Language), OpenID protocol



The screenshot shows the GOV.UK website interface. At the top, there is a search bar and navigation links for Departments, Topics, Worldwide, How government works, Get involved, Policies, Publications, Consultations, Statistics, and Announcements. The main heading is 'Collection Identity assurance: delivering trusted transactions'. Below this, it lists the Organisation as Cabinet Office and the Page history as Published 14 May 2012. A paragraph of text reads: 'Guidance on identity assurance for government departments and service providers.' There is a 'Contents' section with links to 'Determining a service's assurance requirements', 'Provisioning identity assurance', 'Provisioning supporting security services', and 'Technical specifications'. A callout box says 'Find out more about our approach to identity and privacy on the Identity Assurance blog.' Below this, a paragraph explains that being able to prove your identity online easily, quickly and safely is recognised as a key enabler of internet use by the government and its users, and that providers of public services must address business and security issues around identity proofing and username/password fallibility to mitigate the financial and administrative implications of identity fraud and compromise of personal data.

한국 IT 관련 법, 규제 체제의 문제

- 언제나 규제 기득권 창출
 - 지정권한, 감독권한 행사
- 기술 발달, 기술 성장 등에 대한 고려나 원칙은 없음
 - 이권 사업자, 관변 사업자, 과점 사업자만 양산
- '표준'이 뭔지를 모름
 - 이권과 특혜의 카르텔이 표준이라고 오해

이른바 ‘잊혀질 권리’ 적용에 대한 판단과 그 평가*



정민하 ((주)네이버 정책협력실 실장)

1. 들어가며

정보통신망법 제44조의5(게시판 이용자의 본인 확인)를 이유로 온라인 서비스를 이용하는 실제 당사자를 확인하는 ‘본인확인’이라는 것이 가능한 것처럼 당연하게 받아들여졌다. 일명 ‘인터넷 실명제’, ‘게시판 실명제’, 또는 ‘제한적 본인확인제’라고 불렀던 이 제도는 일정한 조건에 해당하는 자가 게시판을 설치·운영하려면 그 이용에 앞서 “신원확인”을 거치도록 의무화 하는 것을 의미하였다.¹⁾ 이 것이 의미하는 바는, 실제 게시판을 이용하는 자가 실제명인가 아닌 가명을 사용하거나 별명을 사용하는 경우라 할지라도 일정조건을 충족하는 사업자의 게시판을 이용하는 경우에는 그 이용에 앞서 반드시 신원의 확인을 거쳐야 한다는 의미이다. 이런 의미에서 이용자 실명을 그대로 사용하는 ‘인터넷 현명제’와 구분될 것이다.²⁾

이와 같은 게시판 실명제는 지난 2012. 8. 23. 헌법재판소에서 위헌결정되어 제445의5제1항 제2호를 삭제함으로써 더 이상 일반 온라인 기업의 게시판에 강제되지는 않지만, 같은 조 같은 항 제1호는 그대로 잔존하여 국가기관, 지방자치단체, [공공기관의 운영에 관한 법률] 제5조제3항에 따른 공기업, 준정부기관 및 [지방공기업법]에 따른 지방공사, 지방공단에는 그대로 남아있다. 즉, 현재의 판결에도 불구하고 현재 결정의 심판 대상에서 제외되었다는 이유로 여전히 유효한 제도로 명맥을 유지하고 있는 것이다.

그러나, 국가기관 등에 적용되는 게시판 실명제 역시 헌법재판소의 위헌결정의 이유의 대부분이 게시판 이용자의 표현의 자유, 개인정보자기결정권의 침해에 초점을 맞추고 있다는 점에서 정보통신서비스 제공자가 운영했던 본인확인제와 그 운영 메커니즘이 동일하다는 관점에서 공공기관 등이 운영하는 본인확인제에 대해서도 당해 위헌결정의 기속력이 미친다고 보아야 한

1) 김송옥 “인터넷실명제에 대한 헌법적 평가와 전망 - 제한적 본인확인제 사건에 관한 판례평석을 겸하여” 공법학연구 제14권 제1호 2면
2) 인터넷 포털 NATE는 실명제가 확대 적용된 2009년부터 뉴스 게시판에서 실명으로 댓글을 달도록 하는 현명제를 유지하기도 하였으나, 현재 판결 이후 2012년 9월에 이를 폐지하였다. 현재는 이용자의 아이디를 노출하고 일부를 마스크(asterisk, *)처리하는 방식으로 변경하여 운영하고 있다.

다는 견해도 있다.³⁾

또한, 공직선거법상에 남아있는 선거관련 인터넷 실명확인제에 대해서도 중앙선거위가 폐지를 추진하기로 밝히기도 하였다.⁴⁾

결론적으로 인터넷 실명제를 유지하기 위해 도입된 ‘본인확인’은 그 설 자리를 더 이상 유지할 수 없음에도 불구하고 청소년보호법상의 섯다운제, 게임산업 진흥에 관한 법률에 따른 제한적 섯다운제, 청소년보호법상의 유해매체물 판매금지 등에서 본인확인을 요구하고 있어 본인확인이 강제되고 있다. 기타, 온라인에서의 상품의 거래 등에서도 정책적으로 본인확인을 강제하고 있는 경우를 자주 확인할 수 있다.

그러나 본인확인은 정말 본인을 확인할 수 있는 제도인 것인가? 본인확인으로 인한 문제는 없는 것인가? 본인확인으로 인한 폐해가 그로 인해 얻을 수 있는 편익보다 더 큰 것을 간과하고 있는 것은 아닌가? “익명성은 도덕적으로 중립적이다(Online anonymous communication is morally neutral.)”라는 명제에도 불구하고, 본인확인을 반드시 강제해야 할 필요는 무엇인가?⁵⁾

2. 본인확인의 문제점

2.1 본인확인은 정말 가능한 것인가?

국가법령정보센터에서 정보통신망 이용촉진 및 정보보호 등에 관한 법률(‘정보통신망법’)의 내용 가운데 ‘화면내 검색’ 기능을 통해 [본인확인]이라는 키워드로 검색을 하면 다음과 같은 관련 조항을 확인할 수 있음

3) 황성기, “인터넷 실명제 위헌결정의 의의 및 전망”, 법률신문, 2012. 9. 13.

4) 중앙선거위 보도자료 “위헌결정에 따른 인터넷 실명확인제 위원회의 논의 결과” Available at http://www.iencd.go.kr/board/board_01.php?mode=view&seq=585&start=0&shTitle=&shKey=&sort=&asc=

5) 미국과학발전협회(AAAS, American Association for the Advancement of Science) “Anonymous communication policies for the internet: results and recommendations of the AAAS conference” 6면 1999. 1. 27

제23조의2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우
2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우
3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우

② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 “대체수단”이라 한다)을 제공하여야 한다.

[전문개정 2012.2.17.]

제23조의3(본인확인기관의 지정 등) ① 방송통신위원회는 다음 각 호의 사항을 심사하여 대체수단의 개발·제공·관리 업무(이하 “본인확인업무”라 한다)를 안전하고 신뢰성 있게 수행할 능력이 있다고 인정되는 자를 본인확인기관으로 지정할 수 있다.

1. 본인확인업무의 안전성 확보를 위한 물리적·기술적·관리적 조치계획
2. 본인확인업무의 수행을 위한 기술적·재정적 능력
3. 본인확인업무 관련 설비규모의 적정성

② 본인확인기관이 본인확인업무의 전부 또는 일부를 휴지하고자 하는 때에는 휴지기간을 정하여 휴지하고자 하는 날의 30일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다. 이 경우 휴지기간은 6개월을 초과할 수 없다.

③ 본인확인기관이 본인확인업무를 폐지하고자 하는 때에는 폐지하고자 하는 날의 60일 전까지 이를 이용자에게 통보하고 방송통신위원회에 신고하여야 한다.

④ 제1항부터 제3항까지의 규정에 따른 심사사항별 세부 심사기준·지정절차 및 휴지·폐지 등에 관하여 필요한 사항은 대통령령으로 정한다.

[본조신설 2011.4.5.]

제23조의4(본인확인업무의 정지 및 지정취소) ① 방송통신위원회는 본인확인기관이 다음 각 호의 어느 하나에 해당하는 때에는 6개월 이내의 기간을 정하여 본인확인업무의 전부 또는 일부의 정지를 명하거나 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 때에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 본인확인기관의 지정을 받은 경우
2. 본인확인업무의 정지명령을 받은 자가 그 명령을 위반하여 업무를 정지하지 아니한 경우
3. 지정받은 날부터 6개월 이내에 본인확인업무를 개시하지 아니하거나 6개월 이상 계속하여 본인확인업무를 휴지한 경우
4. 제23조의3제4항에 따른 지정기준에 적합하지 아니하게 된 경우

② 제1항에 따른 처분의 기준, 절차 및 그 밖에 필요한 사항은 대통령령으로 정한다.

[본조신설 2011.4.5.]

제44조의5(계시판 이용자의 본인 확인) ① 다음 각 호의 어느 하나에 해당하는 자가 계시판을 설치·운영하려면 그 계시판 이용자의 본인 확인을 위한 방법 및 절차의 마련 등 대통령령으로 정하는 필요한 조치(이하 “본인확인조치”라 한다)를 하여야 한다.

1. 국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제5조제3항에 따른 공기업·준정부기관 및 「지방공기업법」에 따른 지방공사·지방공단(이하 “공공기관등”이라 한다)
2. 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 10만명 이상이면서 대통령령으로 정하는 기준에 해당되는 자

② 방송통신위원회는 제1항제2호에 따른 기준에 해당되는 정보통신서비스 제공자가 본인확인조치를 하지 아니하면 본인확인조치를 하도록 명령할 수 있다.

③ 정부는 제1항에 따른 본인 확인을 위하여 안전하고 신뢰할 수 있는 시스템을 개발하기 위한 시책을 마련하여야 한다.

④ 공공기관등 및 정보통신서비스 제공자가 선량한 관리자의 주의로써 제1항에 따른 본인확인조치를 한 경우에는 이용자의 명의를 제3자에 의하여 부정사용됨에 따라 발생한 손해에 대한 배상책임을 줄이거나 면제받을 수 있다.

[전문개정 2008.6.13.]

[단순위헌, 2010헌마47, 2012.8.23., ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’ (2008.6.13. 법률 제9119호로 개정된 것) 제44조의5 제1항 제2호는 헌법에 위반된다.]

제76조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자와 제7호부터 제11호까지의 경우에 해당하는 행위를 하도록 한 자에게는 3천만원 이하의 과태료를 부과한다. <개정 2011.3.29., 2012.2.17., 2013.3.23>

1. 제23조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 자
2. 제23조의2제1항을 위반하여 주민등록번호를 수집·이용하거나 같은 조 제2항에 따른 필요한 조치를 하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

2의2. 제27조의3제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자 및 방송통신위원회에 통지 또는 신고하지 아니한 자

3. 제28조제1항(제67조에 따라 준용되는 경우를 포함한다)에 따른 기술적·관리적 조치를 하지 아니한 자

4. 제29조제1항 본문을 위반하여 개인정보를 파기하지 아니하거나 같은 조 제2항에 따른 조치를 취하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

5. 제30조제3항·제4항 및 제6항(제30조제7항, 제31조제3항 및 제67조에 따라 준용되는 경우를 포함한다)을 위반하여 필요한 조치를 하지 아니한 자

5의2. 제30조의2제1항 본문을 위반하여 개인정보의 이용내역을 통지하지 아니한 자(제67조에 따라 준용되는 경우를 포함한다)

6. 제44조의5제2항에 따른 방송통신위원회의 명령을 이행하지 아니한 자

7. 제50조제1항부터 제3항까지의 규정을 위반하여 영리 목적의 광고성 정보를 전송한 자

8. 제50조제4항 또는 제5항을 위반하여 광고성 정보를 전송할 때 밝혀야 하는 사항을 밝히지 아니하거나 거짓으로 밝힌 자

9. 제50조제7항을 위반하여 비용을 수신자에게 부담하도록 한 자

10. 제50조의5를 위반하여 이용자의 동의를 받지 아니하고 프로그램을 설치한 자

11. 제50조의7제1항을 위반하여 인터넷 홈페이지에 영리목적의 광고성 정보를 게시한 자

12. 제71조부터 제74조까지, 제1호부터 제11호까지 및 제2항의 위반행위를 하여 제64조제4항에 따른 미래창조과학부장관 또는 방송통신위원회의 시정조치 명령을 이행하지 아니한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.

1. 제25조제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보 취급위탁에 관한 사항을 공개하지 아니하거나 알리지 아니한 자

2. 제26조제1항 및 제2항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자에게 개인정보의 이전사실을 알리지 아니한 자

3. 제27조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 관리책임자를 지정하지 아니한 자

4. 제27조의2제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보 취급방침을 공개하지 아니한 자
- ③ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다. <개정 2009.4.22., 2011.4.5., 2012.2.17.>
1. 제20조제2항을 위반하여 전자문서를 보관하지 아니한 자
 2. 제21조를 위반하여 전자문서를 공개한 자
 - 2의2. 제23조의3제1항을 위반하여 본인확인기관의 지정을 받지 아니하고 본인확인업무를 한 자
 - 2의3. 제23조의3제2항에 따른 본인확인업무의 휴지 또는 같은 조 제3항에 따른 본인확인업무의 폐지 사실을 이용자에게 통보하지 아니하거나 방송통신위원회에 신고하지 아니한 자
 - 2의4. 제23조의4제1항에 따른 본인확인업무의 정지 및 지정취소 처분에도 불구하고 본인확인업무를 계속한 자
 - 2의5. 제24조의2제3항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 제공 또는 취급위탁에 대한 동의를 받을 때 개인정보의 수집·이용에 대한 동의와 구분하여 받지 아니하거나 이에 동의하지 아니한 이유로 서비스 제공을 거부한 자
 3. 제42조의3제1항을 위반하여 청소년 보호 책임자를 지정하지 아니한 자
 4. 제43조를 위반하여 정보를 보관하지 아니한 자
 5. 제46조제2항을 위반하여 보험에 가입하지 아니한 자
 6. 제47조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자
 7. 제47조제7항 및 제47조의3제3항을 위반하여 인증받은 내용을 거짓으로 홍보한 자
 8. 삭제 <2012.2.17>
 9. 삭제 <2012.2.17.>
 10. 제47조의4제3항을 위반하여 소프트웨어 사용자에게 알리지 아니한 자
 11. 제48조의2제4항에 따른 시정명령을 이행하지 아니한 자
 - 11의2. 제48조의3제1항을 위반하여 침해사고의 신고를 하지 아니한 자
 12. 제48조의4제4항에 따른 사업장 출입 및 조사를 방해하거나 거부 또는 기피한 자
 13. 제52조제6항을 위반하여 한국인터넷진흥원의 명칭을 사용한 자
 14. 제53조제4항을 위반하여 사업의 휴지·폐지·해산의 신고를 아니한 자
 15. 제56조제1항을 위반하여 약관을 신고하지 아니한 자
 16. 제57조제2항을 위반하여 관리적 조치 또는 기술적 조치를 하지 아니한 자
 17. 제58조제1항을 위반하여 통신과금서비스 이용일시 등을 통신과금서비스이용자에게 고지하지 아니한 자
 18. 제58조제2항을 위반하여 통신과금서비스이용자가 구매·이용 내역을 확인할 수 있는 방법을 제공하지 아니하거나 통신과금서비스이용자의 제공 요청에 응하지 아니한 자
 19. 제58조제3항을 위반하여 통신과금서비스이용자의 요청에 대한 처리 결과를 통신과금서비스이용자에게 알려 주지 아니한 자
 20. 제58조제4항을 위반하여 통신과금서비스에 관한 기록을 보존하지 아니한 자
 21. 제59조제2항을 위반하여 통신과금서비스이용자의 이의신청 및 권리구제를 위한 절차를 마련하지 아니한 자
 22. 제64조제1항에 따른 관계 물품·서류 등을 제출하지 아니하거나 거짓으로 제출한 자
 23. 제64조제2항에 따른 자료의 열람·제출요청에 따르지 아니한 자
 24. 제64조제3항에 따른 출입·검사를 거부·방해 또는 기피한 자

- ④ 제1항부터 제3항까지의 과태료는 대통령령으로 정하는 바에 따라 미래창조과학부장관 또는 방송통신위원회가 부과·징수한다. <개정 2011.3.29., 2013.3.23.>
- ⑤ 제4항에 따른 과태료 처분에 불복하는 자는 그 처분을 고지받은 날부터 30일 이내에 미래창조과학부장관 또는 방송통신위원회에 이의를 제기할 수 있다. <개정 2011.3.29., 2013.3.23.>
- ⑥ 제4항에 따라 과태료 처분을 받은 자가 제5항에 따라 이의를 제기하면 미래창조과학부장관 또는 방송통신위원회는 지체 없이 관할 법원에 그 사실을 통보하여야 하며, 그 통보를 받은 관할 법원은 「비송사건절차법」에 따른 과태료 재판을 한다. <개정 2011.3.29., 2013.3.23.>
- ⑦ 제5항에 따른 기간에 이의를 제기하지 아니하고 과태료를 내지 아니하면 국세 체납처분의 예에 따라 징수한다.
- [전문개정 2008.6.13.]

* 기타 부칙에 본인확인기관 지정 등에 대한 내용이 일부 존재

방송통신위원회는 2012년 8월에 고시 제2012-48호 “본인확인기관 지정 등에 관한 기준”을 공개하기도 하였는데, 제1조(목적)에서는 정보통신망법 제23조의3 및 같은 법 시행령 제9조의3부터 제9조의5까지의 본인확인기관의 지정에 필요한 세부심사기준 및 평가방법과 본인확인업무의 휴지 또는 폐지의 통보 및 신고의 절차 등을 정함을 목적으로 한다.”고 명시하고 있다. 또한 제2조(정의) 제1호에서는 “본인확인기관”이라 함은 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 “대체수단”이라 한다)을 제공하는 자로서 법 제23조의3제1항에 따라 방송통신위원회로부터 본인확인기관의 지정을 받은 자를 말한다고 함

그러나, 이와 같은 모든 내용을 살펴봐도 그 어디에도 “본인확인”이 무엇인지에 대한 명확한 설명을 찾아볼 수는 없다. 고려대학교 김기창 법과대학 교수도 “정통방법은 무엇이 본인확인 조치인지를 구체적으로 정하고 있지 않다.”라고 단언하기도 하였다.⁶⁾

상기 내용에서 사용된 언어의 추론적 조합을 통해 정통방법에서 정의하는 “본인확인”이 무엇인지 재정의 해본다면, “본인확인이란 본인확인기관이 제공하는 ‘대체수단’을 이용하여 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법을 말한다.”고 생각해 볼 수 있다.

그러나, 과연 이러한 방식이 진정하게 본인을 확인할 수 있는 것인지에 대해서는 근본적인 의문이 있다. 위 김기창 교수도 “본인만이 배타적으로 지배하는 정보”를 제시하도록 요구(challenge)하고, 그 요구에 대한 응답(response)을 기초로 본인 여부를 판단하는 방법 외에 온라인 교신에서 본인확인을 할 다른 방법을 현재의 기술 수준에서 상상하거나 실제로 구현하기

6) 김기창, “정통방법상 본인확인제도의 한계와 문제점 - 기술과 법의 갈등” Law&Technology, 제7권 제3호 25면

는 어렵다.”라고 주장하는 것이 비추어 실제 온라인에서의 본인확인이 완벽하게 구현될 수 없음을 인정하고 있다.⁷⁾

방송통신위원회는 지난 2012. 4. 5에 개최된 <주민번호 수집 및 이용 제한 정책 토론회>에서 주민번호 미수집 전환을 위한 안전한 본인확인 수단으로 공인인증서, 휴대폰 인증, 신용카드 인증 등을 제시하였다. 기존 i-PIN까지 포함하면 총 4가지 수단의 안전한 본인확인 수단을 제시한 것이다.⁸⁾ 그러나, 현재 온라인 사업자가 구현하여 사용할 수 있는 방안은 i-PIN, 휴대폰 인증 등이며, 공인인증서의 경우 발급비용 문제로 인해 실제 거의 사용되고 있지 않아 실효성이 없으며 신용카드 인증은 구현 모듈이 개발조차 되지 않아 본인확인 수단으로써의 기능을 하지 못하고 있다.

그런데, 정말 이와 같은 본인확인 수단들이 진정한 ‘본인확인’을 가능하게 하는 것인가? 그렇지 않다고 판단된다. 왜냐하면, 정통방법을 비롯 그 어디에서도 ‘본인확인’이 무엇인지 구체적으로 정의하고 있지 않고 있기 때문이다. 설혹, 주민번호를 사용하지 않는 안전한 본인확인 수단으로 제시된 각 수단들을 살펴봐도 해당 방식들이 실제 이용자 여부를 확인할 수 있는 본인확인 수단으로써의 기능을 충분히 하고 있는지 의문이다.

i-PIN의 경우 발급 이후에는 ID와 비밀번호를 사용하게 되는데, 대부분의 인터넷 이용자들이 여러 사이트에 동일한 ID와 비밀번호를 사용하는 관행에 비추어 생각해보면, ID와 비밀번호가 노출되면 i-PIN도 노출된다고 보아야 할 것이고, 그렇게 된다면 이는 김기창 교수의 정의에 비추어 보아도 ‘본인만이 배타적으로 지배하는 정보’에는 해당할 수 없을 것이다. 또한, 정책적으로 i-PIN의 사용을 확산하기 위해 수많은 캠페인과 노력을 기울였지만, 실제 N포털사에서 i-PIN을 이용하는 경우는 전체 회원의 1%에도 미치지 못하는 현실이다.

휴대전화의 경우도 마찬가지로 부모 등 타인명으로 가입하여 사용하는 경우라던 지, 본인확인 목적으로 타인에게 휴대전화를 잠시 대여해주는 경우에는 본인확인 기능을 충분히 이행하지 못하는 방식인 것이다. 실제 국민 1인당 휴대전화 보급율이 100%를 넘어가는 상황에서 복수의 휴대폰을 가족명의로 개통하여 사용하는 일명 ‘폰테크’의 ‘체리피킹’ 관행이 온라인상에 널리 퍼져있는 것만 보아도 휴대전화를 통한 본인확인이 얼마나 실체없는 허상인지 알 수 있다.

7) 위의 논문 27면

8) 방송통신위원회 “주민번호 수집 및 이용제한 정책 토론회” 2012. 4. 5.

결국 정의되지 않는 본인확인을 ‘수단’만 도입하여 억지로 제도를 유지하고 있는 현행 정보통신망법은 전면적으로 개편되어야 할 것이다.

2.2 정보통신망법상의 본인확인 기관 지정에 따른 타 기관의 본인확인 활용

방통위는 왜 본인확인 기관 지정에 대한 조항을 존치하고 있나? 선거 때문에? 게임 때문에? 청소년보호 때문에? 어느 것이 방송통신위원회가 지켜야 할 가치인가, 타 정부기관의 배려? 정부시책?

정보통신망에 존재하는 본인확인 기관의 지정 조항으로 인하여 타 기관에서 해당 조항을 근거로 본인확인을 당연한 것처럼 활용하고 있다. 대표적으로 청소년보호법 제26조에서 심야시간대(0~6시) 16세 미만 청소년에 대한 인터넷 게임 섯다운제를 규정하고 있고, 같은 법 제16조에서는 청소년유해매체물에 대한 상대방의 나이 및 본인확인 의무를 규정하는 한편 같은 조 제4항에서는 제1항에 따른 상대방의 나이 및 본인 여부의 확인방법에 대해 대통령령에 위임하고 있다.

〈청소년보호법 시행령〉

제17조(나이 및 본인 여부 확인방법) 법 제16조제1항에 따라 청소년유해매체물을 판매등에 제공하는 경우에는 다음 각 호의 어느 하나에 해당하는 수단이나 방법으로 그 상대방의 나이 및 본인 여부를 확인하여야 한다.

1. 대면(對面)을 통한 신분증 확인이나 팩스 또는 우편으로 수신한 신분증 사본 확인
2. 「전자서명법」 제2조제8호에 따른 공인인증서
3. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조의2제2항에 따른 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법
4. 「개인정보 보호법」 제24조제2항에 따라 주민등록번호를 사용하지 아니하고 회원으로 가입할 수 있는 방법
5. 신용카드를 통한 인증
6. 휴대전화를 통한 인증. 이 경우 휴대전화를 통한 문자전송, 음성 자동응답 등의 방법을 추가하여 나이 및 본인 여부를 확인하여야 한다.

또한, 게임산업진흥에 관한 법률 제12조의3에서는 게임과몰입, 중독 예방조치 등을 규정하여 제한적 섯다운제의 근거를 마련하면서 게임물 이용자의 회원가입 시 실명, 연령 확인 및 본인

인증을 의무화 하고 있다.

〈게임산업진흥에 관한 법률〉

제12조의3(게임과몰입·중독 예방조치 등) ① 게임물 관련사업자〔정보통신망 이용촉진 및 정보보호 등에 관한 법률〕 제2조제1항제1호의 정보통신망(이하 “정보통신망”이라 한다)을 통하여 공중이 게임물을 이용할 수 있도록 서비스하는 자에 한한다. 이하 이 조에서 같다는 게임물 이용자의 게임과몰입과 중독을 예방하기 위하여 다음 각 호의 내용을 포함하여 과도한 게임물 이용 방지 조치(이하 “예방조치”라 한다)를 하여야 한다.

1. 게임물 이용자의 회원가입 시 실명·연령 확인 및 본인 인증
 2. 청소년의 회원가입 시 친권자 등 법정대리인의 동의 확보
 3. 청소년 본인 또는 법정대리인의 요청 시 게임물 이용방법, 게임물 이용시간 등 제한
 4. 제공되는 게임물의 특성·등급·유료화정책 등에 관한 기본적인 사항과 게임물 이용시간 및 결제정보 등 게임물 이용내역의 청소년 본인 및 법정대리인에 대한 고지
 5. 과도한 게임물 이용 방지를 위한 주의문구 게시
 6. 게임물 이용화면에 이용시간 경과 내역 표시
 7. 그 밖에 게임물 이용자의 과도한 이용 방지를 위하여 대통령령으로 정하는 사항
- ② 여성가족부장관은 「청소년 보호법」 제26조에 따라 심야시간대의 인터넷게임 제공시간 제한대상 게임물의 범위가 적절한지를 평가할 때 문화체육관광부장관과의 협의를 거쳐야 한다. 〈개정 2011.9.15〉
- ③ 제1항의 예방조치를 위한 게임물의 범위, 방법 및 절차와 제2항의 평가 방법 및 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.
- ④ 문화체육관광부장관은 대통령령으로 정하는 바에 따라 게임물 관련사업자에게 예방조치와 관련한 자료의 제출 및 보고를 요청할 수 있다. 이 경우 요청을 받은 자는 특별한 사유가 없는 한 이에 따라야 한다.
- ⑤ 문화체육관광부장관은 제4항에 따라 게임물 관련사업자로부터 제출 또는 보고받은 내용을 평가한 결과 예방조치가 충분하지 아니하다고 인정하면 해당 게임물 관련사업자에게 시정을 명할 수 있다.
- ⑥ 게임물 관련사업자는 제5항에 따른 시정명령을 받은 때에는 10일 이내에 조치결과를 문화체육관광부장관에게 보고하여야 한다.
- ⑦ 문화체육관광부장관은 제5항에 따라 예방조치를 평가하는 경우 관계 중앙행정기관의 장, 전문가, 청소년, 학부모 관련 단체로부터 의견을 들을 수 있으며, 평가 결과를 공표할 수 있다.

[본조신설 2011.7.21]

위에서 살펴본 바와 같이 본인확인이 무엇을 의미하는지 정보통신망법에서 구체적으로 규정하고 있지 않고 있음에도 불구하고 타 기관에서는 각 기관이 집행의 책임을 담당하고 있는 개별 법규에 본인확인을 당연하게도 의무화 하고 있다. 이미 수많은 언론보도나 학계발표에서 확인되듯이 ‘셋다운제에서의 본인확인이 실제로는 성인 개인정보 도용을 유발한다는 소식은 ‘셋다운제를 실시했더니 심야시간대 40대 게임 이용자의 숫자가 급격하게 증가했다.’는 우스개 소리를 만들어내기도 하였다.

또한 공직선거법 제82조의6에서는 인터넷언론사는 선거운동기간 중 당해 인터넷홈페이지의 게시판, 대화방 등에 정당, 후보자에 대한 지지, 반대의 문자/음성/화상 또는 동영상 등의 정보를 게시할 수 있도록 하는 경우에는 안전행정부장과 SEH는 [신용정보의 이용 및 보호에 관한 법률] 제2조제4호에 따른 신용정보업자가 제공하는 실명인증방법으로 실명을 확인받도록 하는 기술적 조치를 하여야 한다고 규정하면서, 인터넷 언론사가 정보통신망법 제44조의5에 따른 본인확인조치를 한 경우에는 그 실명을 확인받도록 하는 기술적 조치를 한 것으로 본다 고 규정하고 있다. 현재 정보통신망법에 따른 온라인 주민등록번호 수집 및 이용제한제도가 실시되고 있어 실질적으로 본 조항은 ‘실명확인’이 아닌 ‘본인확인’을 강제하는 조항과 다름 없다.

실제 게시판 본인확인제가 위헌판결을 받았음에도 불구하고 정부기관 등에서의 게시판 본인 확인제를 존치하는 한편, 본인확인기관의 지정에 관한 조항들을 유지하고 있는 정보통신망법으로 인하여 타 기관에서 정보통신망법의 해당 조항들을 준용하여 본인확인에 대한 근본적인 고민 없이 이를 강제하고 있는 상황에 다름 없다.

3. 나아가며

실제 본인확인은 그 실체조차 명확하지 않음에도 불구하고 본인확인기관의 지정이라는 정보통신망법상의 규정으로 인해 무분별하게 타 기관에서 본인확인 방식을 강제하고 있다. 인터넷의 특성상 별도의 인증절차를 요구하지 않더라도 본인 추적은 매우 용이하다.⁹⁾

본인확인은 결국 기관의 편의상 신원확인을 의무적으로 거치도록 하여 표현의 자기위축을 강제한 뿐만 아니라, 불필요한 사회적, 경제적 비용을 발생시키고 글로벌 환경에서 대한민국 인터넷을 갈라파고스로 만드는 불필요한 제도일 뿐이다. 단순한 개선이 아니라 전면적 폐지와 새로운 질서의 도입을 고려할 때이다.

9) 김기창, 26면



1. 개관

- 최근 지속적으로 발생하고 있는 개인정보 유출사고와 관련하여 주민등록번호와 같은 개인 식별번호가 문제시 되고 있는 주된 원인은,¹⁾ 주지하다시피 인터넷상에서의 악용이 우려되고 있기 때문임
 - 우리나라의 인터넷 활용은 세계적으로도 유례를 찾아보기 힘든 본인확인 체계를 전제로 하고 있음
 - 이는 네트워크 통신이 발전하면서, 이 영역에서도 오프라인 대면관계에서와 같은 통제를 만들어 내고자 하는 욕망이 법을 통해 매우 노골적인 형태로 발현된 것이라고 할 수 있음(zoning law)
 - 네트워크상 존재하는 정보내의 유용성은 그것이 쉽게 복사·전송될 수 있다는 측면에 있기 때문에, 네트워크 규제를 위한 개인 식별번호의 활용은 그것이 어떤 것이든 항상 유출 및 악용의 위험성을 가질 수밖에 없음

- 따라서 이 토론문에서는 이러한 관점에 입각하여, 현재 정부 등을 중심으로 주민등록번호 대체수단의 일환으로 고려되고 있는 휴대폰 인증, 아이핀, 공인인증서 등의 활용상 문제점을 지적하고자 함

2. 확고한 인터넷상 본인확인 체계

- 우리나라의 인터넷 환경은 이제까지 과도하게 본인확인을 요구해 왔음
 - 일반 표현의 영역에서 인터넷 실명제(제한적 본인확인제)가 세계에서 유일하게 도입된 바

1) 이러한 표현이 주민등록번호에 대한 국가의 사회에 대한 통제수단으로의 활용이라든가 오프라인에서의 악용 문제를 경시할 수 있다는 점을 의미하는 것이 아님

있었으나, 2012년 헌법재판소가 민간영역 온라인 게시판 실명제에 대하여 위헌²⁾으로 결정한 바 있음³⁾

- 이는 주민등록번호의 민간영역에서의 활용을 부추긴 근본적인 원인 중 하나였다고 할 수 있음
 - 전자상거래에 있어서도, 본인확인이 전제된 전자상거래를 사실상 강제해 왔음
 - 이 과정에서 주민등록번호는 물론이고, 보안상 문제점을 가지고 있다고 평가받는 공인인 증서의 사용이 강제되어 왔음
 - 은행권 금융거래에 있어 「금융실명거래 및 비밀보장에 관한 법률」에 근거를 두고 있는 금융실명제에 기반하여 인터넷 금융 거래시 본인확인을 정당화하고 있는 측면도 있음
 - 금융실명제의 운용과 인터넷 금융 거래시 실명확인 문제를 동일시해야 하는 것인지에 대해서는, 입법목적의 실현이라는 측면에 관해서 세부적인 검토가 필요할 것으로 판단됨
- 해외 주요 국가들의 경우 인터넷 활용에 있어 본인확인을 강제하고 있는 경우는 없음
- 민간영역에서 정보통신서비스 제공자들의 자율적인 판단에 따라 본인여부를 확인하는 시도는 있을 수 있겠으나, 국가적 차원에서 본인확인을 법률로써 강제하는 경우는 없음
 - 해외 주요 국가들의 경우 주민등록번호와 같은 전국민 단위의 개인 식별번호가 존재하지 않는다는 점에서 그 원인을 찾을 수도 있을 것임
 - 최근 들어 각광받고 있는 페이스북(Facebook)과 트위터(Twitter)와 같은 대표적인 SNS들의 경우에도 실명확인을 요구하고 있지 않음
 - 전자상거래 영역에 있어서도 일반적인 거래는 주로 신용카드 정보 등을 기반으로 이루어지고 있음
 - 전자상거래에 있어 대표적인 세계적 기업들인 아마존(Amazon), 월마트(Walmart), 이베이(ebay) 등은 모두 회원가입 및 물품 배송을 위해 이름, 이메일 주소, 배송정보 및 결제 정보만을 수집할 뿐 별도로 주민등록번호 등을 통한 '본인 인증절차'를 요구하지 않음

2) 헌재 2012. 8. 23, 2010헌마47, 252(병합)

3) 2014년 5월 2일, 이와 관련한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 일부개정법률안」이 통과되었으나, 헌법재판소의 심의 대상(민간영역 온라인 게시판 실명제; 동법 제44조의5 제1항 제2호)이었던 조문만 개정되어 공공영역 온라인 게시판 실명제에 대해서도 논의가 필요함(동법 제44조의5 제1항 제1호). 이와 더불어 헌법재판소의 결정 취지에서 보자면 「공직선거법」 제82조의6에 대한 검토도 필요함

- 주로 신용카드 등을 통해 거래가 이루어지고 있는 것이 현실이며, 이를 통해 매우 원활한 거래가 이루어지고 있음
- 은행권 금융거래 영역에 있어서는 거래되고 있는 계좌정보가 금융기관에 거래를 개설한 본인인지 여부를 확인하는 절차가 존재하는 것은 사실이지만, 이러한 본인확인의 초점은 실제 존재하는 계좌인지 여부와 거래의사가 있는 것인지 여부를 '실질적으로' 확인하는데 기본적 목적을 두고 있는 것이라고 할 수 있으며(물론 한계는 존재함), 특히 주민등록번호 및 공인인증서를 활용한 획일적인 본인확인 절차(정보 대조)를 '형식적으로' 진행하는 것이 아님
- 해외 주요 국가들의 경우 제도적 차원에서 획일화된 공인인증 체계를 가지고 있지 않으며, 금융기관별로 자체 인증시스템을 갖추고 있는 경우가 대부분임
 - 즉, 금융기관별로 인증수단 및 방식을 다양화하고 있으며, 이러한 방식은 획일화된 공인인증 시스템에 비하여, 사회공학적 또는 구조적 차원의 해킹 등이 용이하지 않음

3. 문제점

- 우리나라 인터넷 환경은 본인확인 체계가 매우 안전하며 실효적이라는 점을 전제로 하고 있는 것이지만, 이러한 관점으로 인하여 인터넷 활용의 위험이 더욱 증대되고 있는 상황임
- 본인확인 체계가 전제된 인터넷 활용은 그 만큼 위험성이 높은 개인정보가 인터넷을 통해 유통 및 이용되고 있다는 점을 의미함
 - 이와 관련해서는, 해외 유수의 인터넷 기업들이 왜 가급적 개인정보 수집의 숫자를 줄이려고 하는지에 대해 진지하게 고려해 볼 필요가 있음
- 실제 인터넷의 본인확인 체계는 현실적으로 다바이스 이용자의 본인 여부를 확인해 주는 것이 불가능함
 - 인터넷을 통한 본인확인은 직접 대면을 전제로 한 것이 아니기 때문에, 아무리 좋은 시스템이 구축된다고 할지라도 오프라인과는 달리, 언제든지 다른 이의 정보를 악용하는 것이 가능함
 - 이러한 측면에서, 제도적으로 사실상 획일화된 공인인증서를 중심으로 하는 전자 및

금융거래 체계는 상당한 편의성(실시간 이체 및 결제 등)을 가짐에도 불구하고, 높은 위험성을 항시 내포하고 있음

- 본인확인을 위한 개인정보의 보유 및 이를 활용한 인증을 민간기업(신용평가사 및 이동통신사)에 위임하고 있어, 개인정보 유출의 위험성이 더욱 증대되고 있음
- 금번 카드사 정보유출 사건을 발생시킨 범인은 KCB(신용평가사/본인확인 기관) 소속 직원으로, 민간기업에 의한 개인정보의 네트워크상 취급이 가지는 위험성을 간접적으로 시사하고 있음
 - 현재 본인확인(i-Pin 발급)을 위한 민간 신용평가사들에는 NICE신용평가정보, 서울신용평가정보, 코리아크레딧뷰(KCB)가 있음
 - 이와 유사하게, 공인인증서의 획일화된 활용이 가지는 보안상 문제점과 관련하여, 공인인증발급기관들이 한국정보인증, 한국전자인증, 한국무역정보통신, 코스콤, 금융결제원 등 민간기관이라는 점도 확인할 필요성이 있음
- 2012년 12월에 이동통신 3사도 본인확인 기관으로 지정된 바 있으나, 이들 또한 민간기업이며 정보유출의 위험성을 부인할 수 없음
- 이상과 같은 신용평가사 및 이동통신사들을 본인확인 기관으로 지정한 이유는 해당 기업들이 업무수행상 이미 인증을 위한 정보들을 보유하고 있기 때문인데, 당해 사업자의 기본 업무를 위한 목적 이외에 우리나라 인터넷에서 빈번히 활용될 수밖에 없는 본인확인 업무를 부가적으로 수행할 수 있게 해 줌으로써 개인정보 유출 위험성을 높인다고 할 수 있으며, 또한 이에 대해서는 유사한 맥락에서 특정 민간 사업자들에게 특혜를 부여하고 있는 것이 아닌지에 대한 주장도 제기됨
 - i-PIN 발급 등의 인증업무를 수행하는 민간 신용평가사들은 '신용조회업무'를 영위한다는 목적으로 신용정보집중기관(한국은행연합회 등) 및 금융기관으로부터 신용정보를 제공받으며(「신용정보의 이용 및 보호에 관한 법률」 제32조), 본인확인기관으로 지정된 신용평가사들은 이러한 정보들을 본인확인에 이용하는 것임
 - 휴대폰을 통한 본인확인은 이동통신 3사(에스케이텔레콤(주), (주)케이티, (주)엘지유플러스)에 의해 수행되고 있는데, 이들은 주민등록번호 대체수단 마련의 일환으로 2012년 12월 28일 방송통신위원회로부터 지정받은 업체들로서, 기존에 법률적으로 의무화되어 있었

던 것은 아니지만(이와 관련하여, 이동통신 3사를 「정보통신망법」상 본인확인기관으로 지정하는 것은 통신사의 정보수집 관행을 정당화시켜주는 기능을 함) 주민등록번호를 비롯한 개인정보를 휴대폰 기기 할부거래 및 요금 결제 등의 다양한 이유로 보유하고 있었으며, 이러한 정보들을 활용하여 이동통신 3사들은 본인확인 서비스를 제공하고 있음

- 금융 및 전자상거래에 있어 가장 보편적이고 확립화된 인터넷 인증수단으로 활용되고 있는 공인인증서의 보안상 문제점에 대해서는 이미 다양하게 제기되고 있는 상황임
 - 실제로 상당수의 금융기관 해킹 사고가 하드디스크 등에 저장된 공인인증서를 탈취하거나, 이용자의 공인인증서 사용시 비밀번호를 탈취(피싱 사이트 등)하는 방식으로 이루어짐
 - 공인인증서를 통해 365일 항시 인증(본인확인)이 가능하며 금융기관별 상호 호환이 원활하다는 장점을 제기하는 의견도 있지만, 실사용자임을 인증하는 절차는 매우 형식적인 것에 불과하여 인증서의 유무 및 비밀번호 일치여부만으로 이루어짐
 - 사실상 공인인증서에 대한 제도적 신뢰를 강하게 부여함으로써, 이와 관련한 사고 대응 대책도 미비하고, 주로 사후적인 대응에 초점이 맞추어져 있다는 한계가 있어, 현재의 공인인증서 정책이 보안에 매우 취약하다는 사실을 보여줌
 - 특히, 이는 금융기관 인증시스템이 공인인증서로 사실상 확립화 되어 있는 상황에서, 비밀번호의 비교만으로 사용자를 인증하는 방식으로부터 필연적으로 발생하는 문제임
- 아이핀, 공인인증서, 휴대폰 등을 통한 인증방식이 주민등록번호를 대체할 수 있는 인증수단으로 제시되고 있지만, 이러한 인증수단들도 최초 발급단계에서는 주민등록번호 활용을 기본전제로 하고 있어 여전히 문제점을 가지고 있음
 - 결국 본인확인 체계의 근본적인 개선이 없다면, 주민등록번호는 향후에도 온라인상에서 상당한 가치를 유지할 것으로 예견됨
 - 물론 양적인 측면에서 주민등록번호의 활용이 감소한다고 볼 수도 있겠지만, 여전히 주민등록번호가 악용될 수 있는 구조라는 점에는 변함이 없음
- 인터넷상 본인확인 체계가 가지는 근원적인 문제 해결 없이, 대체인증 수단의 도입만으로는 현재의 문제 상황을 극복할 수 없으며, 더욱이 개인 식별번호로서의 주민등록번호가 가지고

있었던 위험성을 본질적으로 제거할 수 없을 것임

4. 대안의 모색

- 정부 차원에서의 주민등록번호 대체수단에 관한 논의가 진행되고 있지만, 이는 근본적인 처방이라고 보기는 어려움
- 적실한 대응방안을 모색하기 위해서는, 현재 주민등록번호 등의 활용이 규정되어 있는 법령에는 어떠한 것들이 있는지를 명확히 한 연후에, 후속작업을 진행해야 할 것임
- 주민등록번호 등 식별번호의 활용은 현행 법률상 광범위한 예외가 설정되어 있으며, 그 현황은 다음과 같음

「개인정보 보호법」

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
.....(이하생략).....

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법령에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 안전행정부령으로 정하는 경우

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제23조의2(주민등록번호의 사용 제한) ① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다.

1. 제23조의3에 따라 본인확인기관으로 지정받은 경우

2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우
3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우
- ② 제1항제2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.

- 따라서 인터넷상 전반적인 본인확인체계 개편에 있어, 반드시 전제되어야 하는 작업은 과연 법령상 활용 허용의 예외가 타당한 것인지에 대한 종합적 논의임
- 현재 안전행정부와 방송통신위원회는 주민등록번호를 활용하도록 규정하고 있는 정확한 법령을 파악하고 있지는 못한 것으로 파악됨
 - 현재 법제처 「법령정보센터」를 통 검색해 보면, “주민등록번호”에 대해 규정하고 있는 법령의 수는 총 850개임
 - 이 법령들이 모두 인터넷상 본인확인과 관련된 것이라고 보기는 힘들 것이기 때문에, 이에 대한 정확한 판단이 요구되는 상황임
 - 이 사안과 관련하여, 안전행 정부는 각 부처별로 주민등록번호 활용을 규정하고 있는 법령 현황을 조사하도록 조치한 상태라고 함
 - 방송통신위원회의 경우에는, 한국인터넷진흥원의 ‘주민등록번호 클린센터’를 운영하는 과정에서, 사안별로 문제시되는 법령들을 그때그때 확인하여 업데이트하고 있는 상황이라고 함
 - 방송통신위원회에서 정리한 주민등록번호 활용의 예외를 규정하고 있는 법령들로는 다음과 같은 것들이 있음

〈표 1〉 (정보통신서비스제공자) 주민등록번호 수집허용 법령 요약

근거 법령		내 용	해당 사업자
금융실명거래법	제3조	- 금융회사 는 거래자의 실지명의를 확인할 의무를 가짐 ※ 실지명의 : 주민등록표에 기재된 성명 및 주민등록번호 (외국인의 경우 외국인등록번호 및 여권번호)	은행, 보험회사, 카드회사 등등
신용정보보호법	제34조	- 신용정보회사 는 신용정보 제공·이용자로부터 본인의 동의를 얻은 뒤 주민번호 등 개인정보를 수집할 수 있음	은행, 보험회사, 카드회사
전자상거래소비자보호법	제6조	- 전자상거래 및 통신판매 사업자 는 거래 기록 및 그와 관련한 개인정보를 보존해야만 함	쇼핑몰 등 전자상거래 업자
전자금융거래법	제6조, 제7조, 제16조	- 금융기관 또는 전자금융업자 는 전자금융거래를 위하여 이용자의 신원을 확인하여야만 함 - 금융기관 또는 전자금융업자는 전자금융거래의 상대방에 관한 정보를 보존해야 함 - 5만 원 이상의 전자화폐를 사용하고자 할 경우 실지명의 필요	전자금융업자
조세특례제한법	제126조의 3	- 현금영수증의 발급을 위해 현금영수증 사업자는 주민번호 수집·이용 가능(다만 주민번호가 아닌 다른 방식으로도 가능하므로 선택사항이 되어야 할 것임)	현금영수증 사업자
부가가치세법	제16조	- 재화·용역을 공급받은 자에게 세금계산서를 교부하는 경우, 세금계산서에 공급받은 자의 주소·성명·주민번호 기재 - 사업자 가 관할 세무서에 대손세액공제를 신고하는 경우, 신고서에 재화·용역을 공급받은 자의 주민번호 기재 - 통신판매업자 가 부가가치세 납부 등을 처리하는 납세관리인 (부가통신사업자)를 관할세무서에 신고하는 경우, 납세관리인 선정 신고서에 통신판매업자 주민번호 기재	재화 또는 용역을 공급하는 자 (일반 사업자)
소득세법	제145조	- 기타소득을 지급하는 원천징수의무자는 이를 지급할 때 원천징수영수증을 발급해야 하며, 이 경우 주민번호 기재 - 기타소득 등에 대한 지급명세서를 관할 세무서에 제출시, 기타소득자의 주민등록번호 기재	원천징수의 무자
의료법	시행규칙 제9조, 제12조, 제14조	- 병원은 진단서, 처방전, 진료기록부 등의 기재사항에 주민번호 포함	병원

근거 법령		내 용	해당 사업자
보험업법	시행령 제102조	- 금융위원회와 금융감독원으로부터 업무를 위탁받은 자가 업무의 수행을 위해 고유식별정보 처리 가능	보험협회
자격기본법	제23조, 제34조	- 자격관리자는 자격취득자의 관리 목적 및 자격증 기재사항으로 주민번호 수집·이용 가능	공인자격관리자
관세법	제254조	- 해외구매대행 및 해외배송대행업자는 수입신고서 작성시 수입화주의 주민번호를 기재하여야 하고 수입화주가 구매자가 되는 경우에는 주민번호 수집·이용	해외구매대행업자, 해외배송대행업자
고용보험법	시행령 제41조, 시행규칙 제60조	- 사업주가 근로자에 대하여 직업능력개발 훈련을 실시한 경우 사업주는 직업능력개발 훈련비용의 지원신청을 할 수 있으며, 직업능력개발훈련을 실시하는 자는 직업능력개발훈련을 받는 훈련생에게 훈련수당을 지급할 수 있음 - 해당 신청시 제출하는 법령 서식에 근로자의 주민번호 기재란	사업주 또는 훈련기관
전기통신사업법	제83조	- 수사기관이 전기통신사업법에 의한 통신자료 요청 시 주민등록번호제출	
전자서명법	제15조	- 공인인증서 발급시 발급자의 주민번호 요구	공인인증기관
방송법	시행령 제65조	- 방송사업자에 대해 정보의 공개를 요구하는 자는 방송사업자에게 신청서 제출시 주민번호 기재	방송사업자
벤처기업육성에 관한 특별조치법	제15조, 제15조의4	- 주식교환을 하려는 벤처기업은 주식교환계약서 작성하는데 이에 주주의 주민번호 기재	벤처기업

* 출처: 한국인터넷진흥원 국회제출자료, 2014. 6.

- 주민등록번호 활용에 관한 이상과 같은 광범위한 예외설정은 헌법상 기본권인 개인정보자기 결정권에 대한 침해라고 볼 여지도 있을 것임
- 법률이 아닌 시행령 이하 규정에 의해 설정된 예외의 경우에는 입법권에 의해 설정된 예외가 아닌 경우도 있을 수 있으며, 이 경우에는 과도한 개인정보자기결정권에 대한 제한으로 볼 여지가 있음
- 물론 법률에 근거하여 주민등록번호 등의 수집이 허용된 경우라고 할지라도, 과잉금지 원칙(「헌법」 제37조 제2항)의 위반여부를 검토해볼 필요성이 있음

토론문



박찬욱 (방송통신위원회 개인정보보호윤리과)

토론문



박성훈 (국가인권위원회 인권정책과)

■ 정보인권 포럼_ 정보통신서비스 이용과 개인정보자기결정권 보장을 중심으로

제2세션 : 구글 판결과 잊혀질 권리

발제: 이민영 (가톨릭대학교 법학부 교수)

토론: 지성우 (성균관대학교 법학전문대학원 교수)

양홍석 (법무법인 이공 변호사)

정혜승 (다음커뮤니케이션 대외협력실장)

구본권 (한겨레신문 사람과디지털연구소 소장)

이른바 ‘잊혀질 권리’ 적용에 대한 판단과 그 평가*



이민영 (가톨릭대학교 법학전공 부교수, 법학박사)

I. 논의를 시작하며

Càrregues: 1,2 milions de ptes. Tipus de subhasta: 2,05 milions de ptes.

U.R.E. 08/20 (SANT FELIU DE LLOBREGAT) Tel. 666 56 12

- Meitat indivisa d'un solar al carrer Baix, 55, d'Esparreguera, propietat de DANIEL COCA MAGDALENO. Superfície: 160 m². Sense càrregues. Tipus de subhasta: 3,7 milions de ptes.
- Les dues meitats indivises d'un habitatge al carrer Montseny, 8, propietat de MARIO COSTEJA GONZÁLEZ i ALICIA VARGAS COTS, respectivament. Superfície: 90 m². Càrregues: 8,5 milions de ptes. Tipus de subhasta: 2 milions de ptes. cadascuna de les meitats.
- Meitat indivisa d'un habitatge unifamiliar al carrer Begonia, 8, de la Urb. Mas d'en Gall d'Esparreguera, propietat d'ALFREDO FERNÁNDEZ FERNÁNDEZ. Superfície (total): 317 m². Càrregues: 6,2 milions de ptes. Tipus de subhasta: 2,3 milions de ptes.

U.R.E. 08/23 (VILAFRANCA DEL PENEDES) Tel. 817 19 60

채무초과로 인하여 부동산이 경매되었다는, 이미 15년이 경과된 사실을 내용으로 한 스페인 일간지 『La Vanguardia Ediciones S.L.』의 인쇄본 신문기사(1998. 1.19.자 및 1998. 3. 9.자)가 Google Search Engine 구동 시 정보주체 Mario Costeja González의 이름으로 검색이 되는 문제와 관련하여 최근 분쟁이 있었다. Mario는 스페인 개인정보보호 전담기구인 AEPD(Agencia Española de Protección de Datos)에 대하여 우선 해당 신문사를 상대로 ① 당해 기사를 삭제하거나 자신의 개인정보가 더 이상 현출되지 않도록 수정 또는 검색되지 않도록 하는 조치를 취할 것을 그리고 구글 스페인 또는 구글 본사를 상대로 ② 자신의 개인정보가 검색결과에 드러나지 않도록 하는 것과 아울러 해당 신문사로의 링크도 더 이상 보이지 않게끔 삭제하거나 차단하는 조치를 취할 것이 관철될 수 있도록 청구하였으나 기각되고 말았다. AEPD는 ①에 대하여 노동사회부(MoLSA; Ministry of Labour and Social Affairs)의 명령에 따른 해당 공고의 게재가 경매절차로서의 정당성을 확보하고 있을 뿐 아니라 일반인의 참여를 위한 경매절차의 공정성이 인정된다고 보아 기사 자체는 적법하다고 판단해 그 청구를 기각한 반면, ②와 관련해

* 이 글은 지난 2013년 6월 14일 국회의원회관에서 열린 「잊혀질 권리와 디지털 자유」 세미나 자료집에 수록된 필자의 발제문인 ‘잊혀질 권리 실현을 위한 법제화 방향’의 내용을 수정·보완한 것임을 밝힙니다.

서는 검색엔진 운영자가 개인정보 수집에 대한 책임을 부담해야 함과 더불어 해당 정보 자체를 삭제하지 않으면서도 특정 개인정보에 대한 접근을 차단할 수 있다는 점 등을 이유로 Mario의 주장을 받아들였다. 물론 구글 측은 해당 기사의 내용이 모두 사실이고 법적으로도 문제 없으며 삭제청구는 검열에 해당한다는 점을 논거로 위 AEPD의 결정에 대한 의무이행을 거부하였으나, AEPD 결정 이전에 동일 사안에 대한 구글 측의 제소로 계류 중이던 본안사건과 관련하여 관할법원인 스페인 고등법원(Audiencia Nacional; National High Court of Spain)이 유럽사법재판소(CJEU; Court of Justice of the European Union)에 선결적 판단을 구하면서 이에 대한 CJEU의 심리결과가 지난 5월 13일 있었다.

여기서 알 수 있듯 본인이 과거에 자발적으로 올렸거나 또는 어떤 사건과 관련하여 본인의 의사와 무관하게 유통되고 있던 인터넷상의 기록들로 인해 오랜 시간이 지난 후 예상치 못한 상황에서 피해를 당하거나 곤란한 상황에 처하게 되는 경우가 적지 아니하다(God forgives and forgets but the Web never does!).¹⁾ 이는 곧 ‘잊혀질 권리’²⁾ 도입 논의의 필요성을 짚어볼 수 있는 사례이다.

지난 2010년 6월 EU집행위원회(EC; European Commission)는 유럽연합(EU; European Union)과 미국의 기업들이 단일한 전자상거래시장에서의 신뢰구축에 필요하다는 관점에서 전혀 새로운 기본권으로서 ‘잊혀질 권리’를 제안하였으며, 같은 해 11월 프라이버시 보호대책의 강화를 위해 이미 1995년에 제정된 「Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data(95/46/EC; 이하 ‘유럽연합 준칙’이라 한다).³⁾을 개정해 이용자의 ‘잊혀질 권리’에 관한 규정을 새롭게 도입할 뜻을

1) 구본권 譯, 잊혀질 권리: 디지털 시대의 원형 감옥, 당신은 자유로운가?, 지식의 날개, 2011, 17~18쪽, [原著 : Victor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age, Princeton: NJ, Princeton University Press, 2009].

2) 한글 맞춤법에 따르면 ‘잊혀질 권리’는 표준어가 아니다. ‘잊다’의 피동형은 ‘잊히다’이고 여기에 ‘~권’ 어미를 붙여 조어를 할 때 ‘잊힐 권리’라 바른 표현이다. 그럼에도 국내에 이 용어가 번역되어서 소개 될 당시 현재의 용례로 전해져 통용되고 있기에, 혼란을 줄이려는 의도에서 여기에서도 ‘잊혀질 권리’라는 용어를 사용하기로 한다.

3) 1995년 10월에 채택된 이 지침의 목적은 예컨대, 사업목적으로 다른 기업에 판매하는 것처럼 기업이 자신의 고객이 원하지 않는 방식으로 고객에 대한 정보를 사용하는 것을 금지하는 데 있으므로, 유럽에서 영업하고 있는 모든 기업은 동등한 프라이버시보호를 보장하지 못하는 타국으로의 개인정보 전송을 금지하는 것이 핵심적인 내용이다. 이는 1998년 1월에 채택된 「Directive 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」와 함께 인터넷과 같은 정보통신망상

밝혔다.⁴⁾ 그리하여 2012년 1월 25일 제안된 「Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(이하 ‘유럽연합 규정’이라 한다)」⁵⁾은 ‘정보주체의 잊혀질 권리(the data subject's right to be forgotten and to erasure)’를 명시하고 있는 일반정보보호규정(GDPR; General Data Protection Regulation) 제17조를 통해 유럽연합 준칙 제12조(b)에 따른 개인정보에 대한 삭제요구권을 보다 구체화하고 있다.⁶⁾ 즉, 제3자에

의 프라이버시보호문제를 규율한다; 이민영, 인터넷 개인정보보호에 관한 법제도 연구, 정책연구00-10, 정보통신정책연구원, 2000, 55~57쪽.

- 4) See generally European Commission, *Communication from the Commission to European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions; A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 2010.11. 4.
- 5) 여기에서는 ‘잊혀질 권리’가 새롭게 생성된 기본적 인권으로서 헌법에 열거되지 않은 기본권 지위에 놓이는 것이 아니라 개인정보에 대한 열람·정보제공·처리정지 및 정정·삭제 등의 청구권을 포함하여 정보주체의 권리 단계에서 개인정보자기결정권을 구체화하는 일련의 그 파생적 권리 중 하나임을 재확인할 수 있다.
- 6) General Data Protection Regulation Article 17 (Right to be forgotten and to erasure)
 1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
 - (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
 - (c) the data subject objects to the processing of personal data pursuant to Article 19;
 - (d) the processing of the data does not comply with this Regulation for other reasons.
 2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.
 3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:
 - (a) for exercising the right of freedom of expression in accordance with Article 80;
 - (b) for reasons of public interest in the area of public health in accordance with Article 81;

대하여 정보주체의 개인정보에 대한 링크·복제·복사의 삭제 요구를 통지하도록 개인정보처리자에게 의무를 부과하는 것을 포함하여 ‘잊혀질 권리’의 제반조건에 대하여 규정하고 있으며, 개인정보의 지체 없는 삭제 및 처리정지 요구권⁷⁾과 개인정보를 삭제하는 대신 처리를 제한해

-
- (c) for historical, statistical and scientific research purposes in accordance with Article 83;
 - (d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
 - (e) in the cases referred to in paragraph 4.
4. Instead of erasure, the controller shall restrict processing of personal data where:
 - (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
 - (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;
 - (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;
 - (d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).
 5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.
 6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.
 7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.
 8. Where the erasure is carried out, the controller shall not otherwise process such personal data.
 9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:
 - (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;
 - (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;
 - (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.
 - 7) 다만, ① 표현의 자유의 범리에 따른 표현의 권리를 행사하기 위하여 필요한 경우, ② 공중위생 영역에 있어서 공중의 이익을 위하여 개인정보 보존이 필요한 경우, ③ 역사적·통계적·과학적 연구목적에 위하여 필요한 경우 또는 ④ 개인정보의 보존을 요구하는 법적의무를 준수하기 위하여 필요한 경우에 대하여는 삭제의무를 배제하는 예외를 규정하고 있다.

야 하는 경우를 명시하고 있는 것이다.⁸⁾ 또한 명확하지 못한 ‘접근차단(blocking)’이라는 용어를 피하기 위하여 ‘잊혀질 권리’를 통합하여 개인정보 처리과정에 특정한 경우에 한정되도록 하고 있다.⁹⁾

◎ 개인정보 삭제 및 처리정지 요구권 신설

- 개인정보의 지체 없는 삭제 및 처리정지

- 1) 수집·처리 목적을 달성하여 더 이상 개인정보가 필요하지 아니한 경우
- 2) 정보주체가 개인정보처리에 대한 동의를 철회한 경우
- 3) 동의했던 개인정보의 저장기간이 종료된 경우
- 4) 정보주체가 더 이상 개인정보 처리에 반대한 경우
- 5) 다른 법률에 의해 개정안의 적용이 배제되는 경우
- 6) 그밖에 해당 정보를 처리할 법적 근거가 없어진 경우

- 삭제의무의 예외

- 1) 표현의 자유의 법리에 따른 표현의 권리를 행사하기 위하여 필요한 경우
- 2) 공중위생 영역에 있어서 공중의 이익을 위하여 개인정보 보존이 필요한 경우
- 3) 역사적·통계적·과학적 연구목적을 위하여 필요한 경우
- 4) 개인정보의 보존을 요구하는 법적 의무를 준수하기 위하여 필요한 경우

◎ 삭제에 갈음한 개인정보의 처리 제한

- 개인정보를 삭제하는 대신 처리를 제한해야 하는 경우

- 1) 개인정보의 정확성에 대하여 다툼이 있고 이를 확인하기 위하여 일정한 시간이 필요한 경우
- 2) 수집 목적 달성으로 개인정보가 더 이상 필요로 하지 않게 되었지만 입증을 위하여 필요한 경우
- 3) 개인정보의 처리가 불법이지만, 정보주체가 삭제에 반대하고 대신 이용의 제한을 요구하는 경우

8) ① 개인정보의 정확성에 대하여 다툼이 있고 이를 확인하기 위하여 일정한 시간이 필요한 경우, ② 수집 목적 달성으로 개인정보가 더 이상 필요로 하지 않게 되었지만 입증을 위하여 필요한 경우, ③ 개인정보의 처리가 불법이지만, 정보주체가 삭제에 반대하고 대신 이용의 제한을 요구하는 경우, ④ 정보주체가 다른 자동화된 처리시스템으로 개인정보의 이전을 요구한 경우 등이 이에 해당한다.

9) Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 5/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology "blocking"; European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data(General Data Protection Regulation)*, COM(2012) 11 final, Brussels, 2012, 1.25,[hereinafter COM(2012)], p.9.

- 4) 정보주체가 다른 자동화된 처리시스템으로 개인정보의 이전을 요구한 경우
- 처리가 제한된 개인정보의 이용 : 처리가 제한된 개인정보는 정보주체의 동의가 있거나 타인의 권리보호, 공공의 이익을 위한 목적에 해당하는 경우를 제외하면 입증을 위한 목적으로만 이용되어야 함
 - 처리가 제한된 개인정보의 이용 절차 : 개인정보처리자가 개인정보의 처리 제한을 제거하기 위해서는 미리 그 사실을 정보주체에게 통지

◎ 링크·복제·복사의 중단·삭제 통지의무 신설

- 링크·복제·복사의 중단·삭제 통지 : 개인정보의 삭제 및 처리정지 요구를 받은 개인정보처리자는, 공개에 책임이 있는 경우, 기술적인 수단을 포함한 모든 합리적인 조치를 동원하여 해당 정보를 처리하는 제3자에게 정보주체로부터 링크·복제·복사의 삭제 요구가 있었음을 알리도록 의무화
- 개인정보 공개에 대한 책임의 간주 : 개인정보처리자가 제3자에게 개인정보의 공개(publication)에 대한 권한을 부여한 경우, 개인정보의 공개에 대하여 책임이 있는 것으로 간주
- 의무 불이행자에 대한 제재 : 고의 또는 과실의 귀책사유로 정보주체의 개인정보가 포함된 링크·복제·복사를 삭제하지 아니한 자에게는 감독권한을 부여한 개별 회원국의 Data Protection Agency 혹은 European Data Protection Supervisor 등으로부터 금전적 제재를 받음

당초 2014년부터 시행될 예정이었던 유럽연합 규정은 ① ‘잊혀질 권리’를 명시적으로 도입하고 있는 점¹⁰⁾을 제외하고도 ② 범형식에 있어 준칙(Directive)¹¹⁾이 아닌 법규명령으로서의 규정(Regulation) 형식을 취하고 있는 점,¹²⁾ ③ 단일의 ‘유럽정보보호위원회(European Data

10) 종래 ‘불완전하거나 부정확한 정보’에 대해서만 정정·삭제 요구권을 인정해온 유럽연합 지침 제12조(b)와는 달리 해당 정보의 부정확성 여부를 묻지 아니하고 삭제요구권을 부여하고 있다는 점에서 유럽연합 규정은 인터넷환경에서 저장된 과거정보 등의 유출로 인해 발생하는 침해로부터 자유롭고자 하는 기본권적 권리로 여겨지는 ‘잊혀질 권리’의 도입을 명문화하고 있는 것으로 평가된다. 따라서 유럽연합 규정에 따라 해당 정보를 보존해야 할 법적인 근거가 없는 한 정보주체는 언제든지 자신에 관한 개인정보의 삭제를 요구할 수 있게 되며, 이와 함께 유럽연합 규정은 개인정보 공개에 책임 있는 개인정보처리자는 정보주체의 삭제 요구가 있는 경우 기술적인 수단을 포함한 모든 합리적인 조치를 동원하여 해당 정보를 처리하는 제3자에게 정보주체로부터 링크·복제·복사의 삭제 요구가 있었음을 알리도록 의무화하고 있다.

11) 준칙(directive)이라 함은 원래 행정청이 개별적 처분을 할 수 있는 재량권을 향유하고 있거나 미약한 조건적 제약만 있는 경우에 사전에 정한 권한행사의 기준으로서 법령집행자를 일정방향으로 유도하는 명령과 권고의 중간적 성질의 것을 말한다.

12) 유럽연합 집행부에 해당하는 EC에 의해 제정된 Regulation은 프랑스어로는 règlement 그리고 독일어로는 Verordnung에 해당하는 것으로서, 행정권에 의하여 정립되는 법규로서의 성질을 가지는 일반적 명령, 즉 대국민적 구속력을 갖는 행정입법을 말한다. 따라서 EU 차원뿐만 아니라 회원국 국내법 차원에서도 구속력 있는 일반규칙을 수립하는 법적 행위로 의도된 것이라는 점에서 연방법률과도 비슷한 성

Protection Board)’를 설치하고 있는 점, ④ 위반 시 강력한 제재규정을 두고 있는 점¹³⁾ 등을 특징으로 한다. 그리고 여기에서의 ‘잊혀질 권리’는 현재 생존하고 있는 자에 관한 개인정보의 삭제를 청구할 수 있는지에 대한 논의(개인정보자기결정권의 문제), 사망한 자에 관한 정보를 적극적으로 어떻게 처리할 것인지의 논의(소위 ‘디지털 유산’의 문제),¹⁴⁾ 언론에 게재된 개인에 관한 기사의 삭제를 청구할 수 있는가의 논의(기사 삭제 요구권의 문제)¹⁵⁾ 또는 인터넷 게시판에 게시된 타인의 글에 대한 삭제를 청구할 수 있는가의 논의(게시글 삭제 요구권의 문제) 등을 쟁점으로 하는바, 이들 모두 개인의 혹은 개인에 관한 정보에 대하여 삭제 청구를 허용할 것인가에 대한 문제로 집약될 수 있다.

격을 부여받을 수 있는 법규명령(Regulation)은 국내적 직접효력을 주장할 수 있는 권리를 부여할 수 있다고 하겠다; John Tillotson & Nigel Foster, *Text, Case and Materials on European Union Law*, London: Cavendish Publishing Limited, 2003, p.165.

13) 고의나 과실로 ‘잊혀질 권리’ 실현에 대한 의무를 준수하지 않을 경우 개인에게는 최고 100만 유로(EUR), 개인정보처리자인 기업에게는 연간 전 세계 매출액의 2%까지 제재금이 부과될 수 있다; See COM(2012) Article 79(6).

14) 이에 대하여는 「언론중재 및 피해구제 등에 관한 법률」 제5조의2가 해법을 제시하는 예로 보이지만, 국회 미래창조과학방송통신위원회에는 ‘개인정보의 사후처리’에 관한 제30조의3을 신설하는 것과 ‘디지털유산의 승계 등’에 관한 제44조의11을 신설하는 것을 규정하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부법률개정안이 회부되어 있는 상태이다.

「언론중재 및 피해구제 등에 관한 법률」 제5조의2 (사망자의 인격권 보호) ① 제5조제1항의 타인에는 사망한 사람을 포함한다.

② 사망한 사람의 인격권을 침해하였거나 침해할 우려가 있는 경우에는 이에 따른 구제절차를 유족이 수행한다.

③ 제2항의 유족은 다른 법률에 특별한 규정이 없으면 사망한 사람의 배우자와 직계비속으로 한정되, 배우자와 직계비속이 모두 없는 경우에는 직계존속이, 직계존속도 없는 경우에는 형제자매가 그 유족이 되며, 같은 순위의 유족이 2명 이상 있는 경우에는 각자가 단독으로 청구권을 행사한다.

④ 사망한 사람에 대한 인격권 침해에 대한 동의는 제3항에 따른 같은 순위의 유족 전원이 하여야 한다.

⑤ 다른 법률에 특별한 규정이 없으면 사망 후 30년이 지났을 때에는 제2항에 따른 구제절차를 수행할 수 없다.

「언론중재 및 피해구제 등에 관한 법률」 제5조 (언론등에 의한 피해구제의 원칙) ① 언론, 인터넷뉴스 서비스 및 인터넷 멀티미디어 방송(이하 ‘언론등’이라 한다)은 타인의 생명, 자유, 신체, 건강, 명예, 사생활의 비밀과 자유, 초상(肖像), 성명, 음성, 대화, 저작물 및 사적(私的) 문서, 그 밖의 인격적 가치 등에 관한 권리(이하 ‘인격권’이라 한다)를 침해하여서는 아니 되며, 언론등이 타인의 인격권을 침해한 경우에는 이 법에서 정한 절차에 따라 그 피해를 신속하게 구제하여야 한다.

15) 현행법상 정정보도 등을 청구할 수 있는 기한이 ‘해당 언론보도등이 있음을 안 날부터 3개월 이내, 해당 언론보도등이 있은 후 6개월 이내로 제한되어 있기 때문에 6개월 이전에 게재된 기사로 인한 피해 구제에 대해서는 효과가 없는 실정이다; 「언론중재 및 피해구제 등에 관한 법률」 제14조제1항 등 참조.

II. 법이론적 논의

1. '잊혀질 권리'의 법적 근거

유럽연합이 지난 2010년 11월 4일 발간한 '커뮤니케이션 보고서'에 따르면 '잊혀질 권리'란 '자신의 정보가 더 이상 처리되지 않도록 할 개인의 권리'를 뜻하며, 이러한 권리를 행할 수 있는 요건으로 '정보처리가 개인의 동의에 기반하고 있을 때, 정보주체가 동의를 철회하거나 저장 기간이 만료된 경우'가 제시되어 있다.¹⁶⁾ 정보자기결정권에 있어 접근, 수정, 삭제, 접근차단(blocking)의 권리에 더해 '잊혀질 권리'의 고유한 부분은 '특정기간이 지났을 경우 자동적인 정보의 삭제'가 보장되는 것이라고 정의하는 입장도 같은 맥락이라 할 수 있다.¹⁷⁾

헌법학적 접근에서 '잊혀질 권리'를 이른바 새로운 정보프라이버시로 이해하고, "내면적 정신적 자유의 내용을 포함하는 동시에 자기정보통제권의 양면성을 갖는다는 점에서 종래의 정보기본권의 유형에 포함시키기 어렵다."고 하면서 따라서 "'잊혀질 권리'의 헌법적 근거는 헌법 제10조의 인간의 존엄과 가치의 인격권, 행복추구권 그리고 제17조의 정보프라이버시 권리에서 구할 수 있다."라고 설명하는 견해가 존재한다.¹⁸⁾ 특히 이러한 주장은 '자기정보결정권¹⁹⁾은 정보

16) European Commission, *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee, and the Committee of the Regions; A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 2010, p.8.

17) Maria Giannakaki, *The EU Data Protection Directive Revised: New Challenges and Perspectives*, Athens: Karageorgiou & Associates Publications, 2011, p.8.

18) 정영화, 헌법상 정보 프라이버시로서 '잊혀질 권리', 법학논고 제39집, 경북대학교 법학연구원, 2012, 573쪽에 의하면 '잊혀질 권리'는 정보기술의 발전으로 시간 및 공간의 제약을 벗어나 도처에 개인정보의 데이터를 수집 및 보유하고 있기 때문에 종래 프라이버시 권리의 범위에 따라 충분히 설명하기 어렵다. 정보주체의 동의에 기초하여 정보처리자가 수집, 이용하는 정보 데이터의 삭제를 요구할 경우에 이를 시행하는 범위와 절차에 관하여 정보주체와 정보처리자간의 분쟁대상이 되기 때문이다. 따라서 '잊혀질 권리'는 자기정보결정권에 관련된 문제가 아니라, 자기정보통제권을 어떻게 행사할 것인지에 대한 정보프라이버시 권리에 해당된다. 또한 이는 정보주체의 인격권의 보호범위와 정보처리자의 재산권 등이 충돌하게 된다. 반면에, '잊혀질 권리'가 헌법 제10조와 제17조의 해석에 의하여 인정되는 새로운 기본권일지라도 이미 자유로운 '표현의 내용'에 해당한 경우에 표현의 자유를 새롭게 제한하기 때문에 기본권 간의 충돌을 해결하기 위해서는 새로운 입법 또는 기본권의 확장해석을 모색할 필요성이 제기된다고 한다.

19) 영미법계의 정보프라이버시(information privacy)에 대응하는 관념으로서 대륙법계의 정보자기결정권(*Recht auf informationelle Selbstbestimmung*)이 존재한다. 이는 일정한 범위 내에서 자신에 관한 정

의 개시나 공개에 대한 결정권을 의미하고 자기정보통제권은 정보에 대한 삭제나 폐기 및 오류의 정정을 전제하는 개념'이라는 이원화된 도식에 터 잡고 있으나, 주요국의 헌법적 이해와 궤를 같이하여 개인정보자기결정권이라는 용어으로써 이해하고 있는 헌법재판소의 해석에 따를 때 '잊혀질 권리'가 헌법에 열거되지 아니한, 새롭게 생성되는 기본권인지 여부에 대한 판단이 핵심적이라 할 수 있다. 다시 말해서 이는 개인정보자기결정권이라는 헌법상 기본적 인권에 파생되는 권리로서의 '잊혀질 권리'를 법적 관념으로 포섭하지 않고 별개의 독자적 기본권으로 인정할 수 있는 근거가 확보되어 있는지에 대한 의문이 해소되어야 할 문제이다.²⁰⁾

생각건대, '잊혀질 권리'는 정보주체인 개인 자신과 관련된 개인정보의 삭제와 처리의 제한을 그 주된 내용으로 한다는 점에서 개인정보자기결정권의 하나로 간주되어야 할 것이다.²¹⁾

보를 제공할 것인가를 자유로이 결정할 권한이 인간의 존중과 인격의 자유로운 전개에 해당하여 법적 보호를 필요로 하는 것으로 파악하여 1983년 독일 연방헌법재판소가 결정한 인구조사결정(BVerfGE 65, 1)에서 처음 인정된 개념으로, 자신에 대한 정보가 언제·어떻게·어느 범위까지 타인에게 전달·이용될 수 있는지를 자율적으로 결정할 수 있는 정보프라이버시와 동일한 개념이라 볼 것이다. 다만, 그 용어에 있어서는 학자에 따라 개인정보통제권·개인정보자기결정권·자기정보통제권·자기정보관리통제권 등 다양한 표현을 사용하고 있으나, 그 내용은 크게 다르지 아니하다. 헌법재판소는 "개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉, 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다."라고 실시하고 있다; 헌재 2005.5.26. 2004헌마190, [판례집 17-1], 668, 682~683; 2005. 7.21. 2003헌마282·425(병합), [판례집 17-2] 81, 91~92.

20) 오히려 학계에서는 이른바 정보기본권 체계화의 전개를 역설하면서 ① 정보통신의 안전과 비밀 보장, ② 정보제공권(정보를 제공하지 아니할 권리), ③ 알 권리(정보수령권 및 정보를 수령하지 아니할 권리, 정보수집권, 개별적·일반적 정보공개청구권, 정부·언론에 대한 통제권), ④ 자기정보통제권 혹은 개인정보자기결정권 등으로 분류하는 견해가 제시되어 있으며(김배원, 정보기본권의 독자성과 타당범위에 대한 고찰: 헌법개정과 관련한 체계구성을 중심으로, 헌법학연구 제12권 제4호, 한국헌법학회, 2006, 209~210쪽), 이처럼 개인정보자기결정권의 이원화논리에 대한 엄격한 구분기준은 찾기 어려운 실정이다(권건보, 개인정보보호와 자기정보통제권, 경인문화사, 2005, 91~92쪽). 이러한 이유로 여기서는 일관되게 개인정보에 관한 정보주체의 기본권을 독자적인 기본적 인권으로서의 개인정보자기결정권으로 새기고 '잊혀질 권리'에 대하여 논하고 있는 것이다.

21) Chris Conley, *The Right to Delete*, 2010 AAAI(the Association for the Advancement of Artificial Intelligence) Spring Symposium Series, Palo Alto, California: AAAI Publications, 2010, p.54, available at <<http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158/1482>>.

위에서 살펴본 바와 같이 이러한 개인정보자기결정권의 헌법적 근거와 관련하여서는 크게 헌법 제10조에서 구하는 견해와 헌법 제17조에서 구하는 견해로 나눌 수 있다.²²⁾

전자는 다시 우리 헌법이 사생활의 비밀과 자유를 자유권 조항에서 규정하고 있으므로 사생활의 비밀과 자유는 소극적인 권리라고 이해하면서 정보사회에서 개인의 존엄을 보장하기 위한 정보에 대한 적극적인 자기결정권은 헌법 제10조에서 보장된다고 이해하는 입장과 헌법 제17조는 개인정보자기결정권의 일부 내용을 포섭할 수 있으나 해당 권리의 일반적 근거가 될 수 없다고 보면서 일반적인 개인정보자기결정권의 헌법적 근거는 제10조 제1문 후단의 행복추구권에 그 근거가 있는 일반적 인격권에서 찾아야 한다고 보는 입장으로 나눌 수 있다. 한편, 그에 대해서 후자는 사생활에 관한 권리가 전통적으로 개인이 외부의 간섭을 받지 않고 '혼자 그대로 있을 수 있는 권리(right to be let alone)'를 중심적인 내용으로 하고 있지만 현대 과학기술의 발달과 함께 도래한 정보사회에서는 개인정보의 수집·처리·관리의 대량화·집단화로 인해 개인의 사생활의 비밀과 자유가 침해될 가능성이 현저하게 증대하였으며, 이에 따라 정보주체의 개인정보자기결정권이 중요한 내용으로 추가되었다고 보는 입장이다.²³⁾

하지만 개인정보자기결정권은 특히 컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서 개인정보의 처리와 이용이 시공에 구애됨이 없이 간편하고 신속하게 이루어질 수 있게 되었고, 정보처리의 자동화와 정보파일의 결합을 통하여 여러 기관간의 정보교환이 쉬워짐에 따라 한 기관이 보유하고 있는 개인정보를 모든 기관이 동시에 활용하는 것이 가능하게 되었으며, 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었다. 이렇게 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 된 이와 같은 상황에서 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치로 인식되기 때문에 이를 헌법상 기본권으로 승인하는 것이다.²⁴⁾ 따라서 이는 헌법 제37조제1항이 명시하고 있는 바와 같이 헌법에 열거되지 아니한

22) 그 상세는 이상명, 개인정보자기결정권의 헌법적 근거에 관한 고찰, 공법연구 제36집 제3호, 한국공법학회, 2008, 239쪽 이하 참조.

23) 이에 대한 개관은 함인선, '잊혀질 권리'에 관한 고찰: EU 개인정보보호법안과 우리나라 「개인정보 보호법」의 비교를 중심으로, 인권과 정의 제427호, 대한변호사협회, 2012, 57~58쪽 참조.

국민의 자유와 권리로서 그 원천은 우리 헌법 제10조와 제17조에서 도출된다고 할 수 있다.²⁵⁾ 하지만 이는 개인정보자기결정권의 법적 성격에 관한 것이지 ‘잊혀질 권리’의 그것은 아니다.

‘잊혀질 권리’는 개인정보자기결정권이라는 기본적 인권의 파생적 권리로 이해되며, 다만 그 효력과 범위는 법률의 차원에서 실정법적으로 형성되는 한도에 그칠 수밖에 없을 것이다. 다시 말해서 이른바 ‘잊혀질 권리’란 명칭에서 확인할 수 있듯이 이는 법률 단위에서 상정될 수 있는 실정법적 권리 관념에 해당하는 것이기에 기본적 인권의 반열에서 논의될 수 없다고 할 것이다. 그러므로 ‘잊혀질 권리’의 법률적 근거를 구하고자 할 때 ‘잊혀질 권리’가 ‘개인정보’를 그 대상으로 한다는 점에서 우선 ‘개인정보 보호법’이 그 검토의 대상이 된다고 하겠다. 그렇기 때문에 종래 구(舊) 「공공기관의 개인정보보호에 관한 법률」이나 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등에서 인정해 온 정보주체의 개인정보에 대한 열람 또는 정정요구 등에 관한 권리와 일반법인 「개인정보 보호법」에서 개인정보자기결정권으로부터 파생된 것으로 규율하고 있는 개별적 권리와 동위(同位)의 ‘잊혀질 권리’를 어느 범주까지 제도적으로 보장할 것인지에 관한 문제를 ‘잊혀질 권리’ 자체에 관한 기본권적 개념과 체계적 지위의 문제로 볼 필연성은 없다.²⁶⁾

24) 헌법재판소 2005. 5.26. 99헌마513, 2004헌마190(병합) 결정, 판례집 17-1, 668, 682~683.

25) 다만, 개인정보자기결정권의 헌법적 근거와 관련하여 헌법재판소는 헌법 제10조 제1문 및 제17조에 그 근거를 구하는 것헌법재판소 1995.12.28. 91헌마114; 2005. 7.21. 2003헌마282, 425(병합); 2008.10.30. 2006헌마1401, 1409(병합); 2009. 9.24. 2007헌마1092; 2010.9.30. 2008헌마132 결정 등)과 새로운 독자적 기본권으로 보는 것헌법재판소 2005.5.26. 99헌마513, 2004헌마190(병합); 2009.10.29. 2008헌마257; 2010.5.27. 2008헌마663 등이 혼재하고 있는 양상을 보이고 있다. 특히 후자의 입장과 관련하여 헌법재판소는 다음과 같이 실시하고 있다.

“개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한 두개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다; 헌법재판소 2005.5.26. 99헌마513, 2004헌마190(병합) 결정, 판례집 17-1, 668, 683.

26) 다만, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제30조제3항의 경우 “정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.”고 규정하고 있는 반면, 「개인정보 보호법」 제36조제1항 본문은 “제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다.”라고 규정하고 있다. 또한 구(舊) 「공공기관의 개인정보보호에 관한 법률」의 경우 2007년 5월17

이와 같은 논의는 기본권론적 관점에서도 그러하지만, 「개인정보 보호법」에 규정된 개인정보에 대하여 정보주체가 행사할 수 있는 열람 또는 정정·삭제 및 처리정지 요구에 관한 권리에 있어서 특히 개인정보에 관한 삭제요구권이 ‘잊혀질 권리’와 그 효과적 관점에서도 유사하고 개인정보의 생애주기(life cycle)에 비추어 볼 때 개인정보자기결정권을 실현하는 구체적 권리로서 다각도의 측면에서 논의될 수 있다는 점에서 새롭게 생성된 하나의 기본권에 파생되는 권리라는 설명이 더욱 설득력이 있다.²⁷⁾

이렇게 보면 ‘잊혀질 권리’를 행사할 수 있는 주체는 그 근원인 개인정보자기결정권을 보유하는 기본권주체이어야 한다. ‘잊혀질 권리’는 ‘개인’의 권리인바, 여기서의 개인은 ‘자연인’으로 한정될 수밖에 없다.²⁸⁾ 왜냐하면 ‘잊혀질 권리’는 개인정보자기결정권과 개인의 자유를 위한 것으로 평가되기에 법인을 제외한 자연인에 한정하여야 하기 때문이다.²⁹⁾ 이러한 취지에서 유럽연합 규정은 제1조제2항에서 ‘자연인의 기본적 권리와 자유를 보호하는 것’이 그 목적임을 명확히 하고 있으며,³⁰⁾ 제4조제1항에서는 정보주체의 개념에 대하여 식별된 또는 식별 가능한 자연인으로 명시하고 있는 것이다.³¹⁾

일 당시 일부개정예에 있어 ‘개인정보보호의 원칙’을 제3조의2로 신설하고 같은 조 제4항에서 “공공기관의 장은 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다.”라고 규정하고 있었을 뿐만 아니라, ‘불복청구’와 관련하여 제15조에서 처리정보의 열람·정정·삭제 등의 청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 「행정심판법」으로 정하는 바에 따라 행정심판을 청구하거나 「행정소송법」으로 정하는 바에 따라 행정소송을 제기할 수 있음을 명문으로 규정하고 있었다.

- 27) 후술하는 바와 같이 ‘잊혀질 권리’의 법제화 논의에 촉발점이 된 유럽연합 규정에서도 프랑스의 관련법안과는 다른 내용의 ‘잊혀질 권리’를 정립하고 있다. 이는 ‘잊혀질 권리’가 헌법적으로 확인되는 권리다 발로서의 기본적 인권의 위상이기보다는 실정법 차원에서의 권리 개념으로 이해함이 타당하다는 데 또 다른 논거로 작용한다. 그러므로 현행법에 있어 ‘잊혀질 권리’를 확보하기 위한 논의는 개인정보자기결정권의 이해를 전제로 한 정보주체의 권리실현 방안으로 구체화되어야 하고 여기에는 국내법적 현실에 대한 자각과 반성이 우선되어야 한다.
- 28) ‘잊혀질 권리’를 행사할 수 있는 주체적 요건을 자연인으로 파악할 경우 그 범주가 생존하는 기간 동안에만 해당하는 것인지 여부가 문제된다. 우리의 「개인정보 보호법」의 경우 개인정보를 ‘살아있는 개인에 관한 정보’를 명시하고 있고 이러한 규율은 폐지된 「공공기관의 개인정보보호에 관한 법률」이나 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 경우도 마찬가지이다. 다만, ‘생존하는’ 자연인에 한정할 것인지의 문제를 개인정보자기결정권 자체의 논점으로 여길 이유는 없고 개별법에서 ‘잊혀질 권리’에 관한 보호법익에 상응하게 조율할 수 있겠다.
- 29) Chris Conley, *Supra Note 21*, p.55.
- 30) 유럽연합 규정 제1조제2항 : This Regulation protects the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data.

다만, 그 내용에 있어서 개정안인 유럽연합 규정에 대하여 유럽의회(European Parliament)가 지난 3월 12일 표결한 것은 다음과 같은 기존안 제17조의 규율을 강화하는 반향이었다.

Article 17 (Right to erasure) : European Parliament Vote

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of that data, where one of the following grounds applies:
 - (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
 - (c) the data subject objects to the processing of personal data pursuant to Article 19;
 - (a) a court or regulatory authority based in the Union has ruled as final and absolute that the data concerned must be erased;
 - (d) the data has been unlawfully processed.
- 1a. The application of paragraph 1 shall be dependent upon the ability of the data controller to verify that the person requesting the erasure is the data subject.
2. Where the controller referred to in paragraph 1 has made the personal data public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

Article 17 (Right to be forgotten and to erasure) : Commission Proposal

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:
 - (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
 - (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;
 - (c) the data subject objects to the processing of personal data pursuant to Article 19;

31) 유럽연합 규정 제4조제1항 : ‘data subject’ means an identified natural person or a natural person who can be identified, directly or indirectly...

(d) the processing of the data does not comply with this Regulation for other reasons.

2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

2. ‘잊혀질 권리’ 담론의 재론

가. 개인정보자기결정권과의 관계

일부 학자들에 의하면 유럽에서 ‘잊혀질 권리’라는 새로운 권리를 논의하는 이유는 지금까지 발전해온 정보프라이버시권 또는 개인정보자기결정권으로 다양한 유형의 개인정보를 온전하게 보호하기 어렵다는 주장하고 있다. 이에 따르면,³²⁾ ‘잊혀질 권리’는 정보주체가 개인정보처리자를 상대로 자신의 개인(신상)정보를 삭제하라고 요구할 수 있는 유형과 정보통신서비스 제공자를 상대로 자기관련 (가치적) 개인정보의 삭제를 요청하는 유형으로 나누어볼 수 있다고 한다. 그리고 ‘잊혀질 권리’의 법적 성격에 대하여 전자의 경우에는 개인정보자기결정권이며, 후자의 경우에는 사회적 인격상에 관한 자기결정권이라고 한다.³³⁾ 그리고 ‘잊혀질 권리’의 보호법익이 미치는 대상으로서의 정보는 ① 개인정보자기결정권이 완전히 적용되는 제1유형³⁴⁾과 ② 개인정보자기결정권의 보호영역에 해당되지 않는 제2유형,³⁵⁾ 제3유형³⁶⁾ 및 제4유형³⁷⁾으로 구분된

32) 문재완, 프라이버시 보호를 목적으로 하는 인터넷 규제 의의와 한계: ‘잊혀질 권리’ 논의를 중심으로, 언론과 법 제10권 제2호, 한국언론법학회, 2011, 13~17쪽 참조.

33) 이에 따르면 헌법재판소 2005.5.26. 99헌마513, 2004헌마190(병합) 결정에서 그 내용으로 개인정보자기결정권은 정보주체로 하여금 개인정보의 공개와 이용을 스스로 통제하도록 함으로써 타인에게 형성될 정보주체의 ‘사회적 인격상에 대한 결정권’을 정보주체에게 유보시킨다는 의미를 갖고 있다고 한다. 즉, 개인정보자기결정권의 의미를 풀어보면 개인정보자기결정권의 내용 속에 사회적 인격상에 대한 결정권이 포함되어 있다는 것이다.

34) 개인정보처리자가 개인정보를 취득할 목적으로 정보주체로부터 개인정보를 수집하는 것을 전제로 하여 정보주체로부터 개인정보 수집·보관·이용과 관련하여 동의를 받았는지 여부가 쟁점이 되는 유형 그리고 개인정보를 집적 취득할 목적이 아니었지만 다른 서비스를 하는 과정에 부수적으로 개인정보가 모여 정보프라이버시 침해가 발생하는 유형 등이 이에 속한다고 한다.

다고 한다.

이에 따르면 후자의 경우 직접적인 수집 대상이 아닌 개인의 가치정보이기 때문에 개인정보 자기결정권에서 말하는 개인정보에 해당되는 것으로 보기 어렵다고 한다. 그렇지만 개인정보자기결정권의 개념은 ‘자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리’로서 기본적 인권에 해당하는 것이므로 자기정보에 대한 통제권을 발휘할 수 있는 공개거부나 삭제요청을 그 파생적 권리로 포함하는 관념이며, 이와 유사한 범위에서 검색차단 또는 사정변경사실고지 요구권 역시 이에 수렴가능하다고 볼 수 있다.

결국 ‘잊혀질 권리’의 도입 여부 및 그 범위와 효력은 정보인권으로서 개인정보자기결정권의 확보를 위한 법제도적·법정책적 문제로 귀착되며, 이익형량의 문제나 규범조화적 해석의 문제로 권리상충의 사안을 분쟁의 예방과 해결의 관점에서 풀어야할 중요한 과제이다. 다만, ‘잊혀질 권리’가 개인정보자기결정권의 파생적 권리인 만큼 다른 기본권주체와의 상호관계에 있어서는 개인정보자기결정권과의 기본권충돌 문제로 귀결된다. 기본권의 상충 또는 충돌 (*Grundrechtskollision*)이라 함은 상이한 기본권주체가 상충하는 이해관계로 인하여 서로 충돌하는 각자의 기본권을 주장하거나 행사하기 위해 국가에 대하여 각기 자기의 기본권을 주장하는 경우를 말한다. 이와 같은 기본권충돌의 경우에 법익교량 혹은 이익형량 이론에 따르면 우위에 있는 기본권만을 보호하고 열위에 있는 어느 하나의 기본권은 보호되지 못하는 문제점이 있는바, 이를 극복하기 위하여 제시된 규범조화적 해결원칙은 헌법의 통일성에 입각하여 규범조화의 방법으로 기본권충돌 문제를 해결해야 한다고 본다. 우리나라 대법원과 헌법재판소에서 기본권 충돌에 있어서 법익교량이론 및 규범조화적 해결원칙 등을 모두 사용하고 있는 것으로 보인다.³⁸⁾

35) 예컨대 아무런 사실의 적시 없이 하는 자신 또는 타인의 욕설이나 비난을 자료로 남기는 경우나 예술 작품에 대한 자신 또는 타인의 감상평을 자료로 남기는 경우 등과 같이 구체적인 사실을 제시하지 않고 단순히 어떠한 현상에 대한 판단을 하거나 자신의 생각이나 느낌을 나타내는 것에 대한 정보를 포함하는 자료로서 의견적 가치정보를 포함한 자료의 유형을 말한다고 한다.

36) 예를 들어 자신이 예전에 만난 애인과의 행적에 대한 정보를 포함하는 자료나 사실에 기초한 잘못된 고백 등과 같이 자신 또는 타인이 사실적으로 경험한 사실에 대한 내용전달을 하는 정보로서 이를 포함한 자료가 이른바 사실회상적 가치정보를 포함한 자료의 유형이라고 한다.

37) 가령 지하철에서 예의 없이 행동을 하는 모습이 그대로 영상녹화된 경우나 누군가와 인터넷상의 채팅이나 메시지를 주고받는 내용 자체가 저장된 정보와 같이 어떤 사람의 행동이나 말을 통한 생활적인 모습 자체에 대한 소위 사실자체적 가치정보를 말한다고 한다.

그럼에도 불구하고 개인정보자기결정권의 보장이라는 입법목적의 실현을 위해서는 입법론적 대응방안을 모색할 필요가 있다. 이러한 관점에서는 정보통신기기나 단말기 등과 같은 장치·설비(device)와는 무관하게 접속되는 인터넷환경의 관문 또는 매체장르에 해당하는 포털사이트 혹은 인터넷신문 등을 규율대상으로 하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「언론중재 및 피해구제 등에 관한 법률」 등의 개정을 필요로 한다고 본다.³⁹⁾ 현행법체계에 서는 일반법인 「개인정보 보호법」의 경우 온라인상에서의 정보유통과 관련한 별도의 규정을 요하지는 않는다고 할 것이기 때문이다.

나. 언론부문에서의 ‘잊혀질 권리’

한편, 대부분의 언론사는 ‘잊혀질 권리’의 저널리즘 영역에의 도입에 대해 부정적인 입장을 보이고 있다고 생각된다. 언론보도가 사실을 기반으로 하고 있으며, 진실을 보도하려고 노력하는 것은 언론사의 당연한 책무라는 연유에서 그러할 것이다. 이에 따라 「개인정보 보호법」 제 58조제1항에서는 언론의 취재·보도 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보에 대하여는 삭제요구가 받아들여지지 않는 것으로 적용제외를 규정하고 있다.⁴⁰⁾ 국민의 ‘알 권리’ 충족이라는 공익적 목적에 충실해야하는 것이 언론의 주요책무이기 때문이다.⁴¹⁾ 그렇지

38) 대법원 1988.10.11. 선고 85다카29 판결; 헌법재판소 2004. 8.26. 2000헌마457; 1991. 9.16. 89헌마165 결정 등 참조.

39) 포털사이트는 이용자의 웹페이지 접속 시 최초로 접하는 매개체로서, 일정 정보를 관통하여 고정방문객을 확보하며 문화적·산업적 가치를 재창출하고 있다. 원래 포털(portal)의 사전적 의미는 관문(gateway)을 뜻하나, 인터넷포털은 관문 개념에 종합(synthesis) 개념이 추가된 것이다. 다만, 「언론중재 및 피해구제 등에 관한 법률」 제2조제18호에서 ‘인터넷뉴스서비스’의 개념이 ‘언론의 기사를 인터넷을 통하여 계속적으로 제공하거나 매개하는 전자간행물’로 정의되기 때문에 법령상 적용 제외되는 매체를 고려한다고 해도 「전기통신사업법」에 따른 부가통신사업자인 포털사이트운영자가 인터넷을 통하여 언론 기사를 계속적으로 제공하거나 매개하는 전자간행물은 소위 ‘언론등’에 포함된다.

40) 「개인정보 보호법」 제58조 (적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.

1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안위를 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보

41) 일반적으로는 알 권리의 헌법상 근거로 “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the

만 언론에 의한 정보 제공과 ‘잊혀질 권리’의 도입에 따른 개인정보의 삭제, 즉 정보주체의 권리와 상충은 규범조화적으로 법익교량이 되어야 할 문제이다.⁴²⁾ 그리고 만일 삭제조치가 필요하다고 인정하더라도 기술적·경제적인 부분도 무시할 수 없는 부분이고 이로써 발생하는 비용은 어느 쪽에서 부담해야 하는지도 선결되어야 한다.

언론중재위원회에 따르면 2012년의 경우 뉴스통신·인터넷신문·인터넷뉴스서비스 등 인터넷을 기반으로 하는 매체에 대한 조정청구 비율은 61.8%로, 전년도와 마찬가지로 전체 청구건수의 절반 이상을 차지했다. 2012년 접수·처리된 사건을 매체별로 살펴보면 네이버(naver)가 118건으로 가장 많았으며, 2011년에 117건으로 가장 많은 사건 수를 보였던 다음(Daum)은 98건으로 소폭 감소하였다.⁴³⁾ 매체유형별 청구건수는 인터넷신문 945건(39.4%), 신문 665건(27.7%), 인터넷뉴스서비스 454건(18.9%), 방송 243건(10.0%), 뉴스통신 83건(3.5%), 잡지 11건(0.5%) 순이었다. 2012년에는 전년도에 비해 언론사 닷컴을 포함한 인터넷신문에 대한 청구가 40건이 늘어난 데 반해 포털 등 인터넷뉴스서비스에 대한 청구는 6건이 줄어들었다. 포털에 대한 청구건수가 줄어든 것은 주요 포털사들이 주로 포털에서 검색된 뉴스제목을 클릭하면 포털사 홈페이지가 아닌 기사제공 언론사의 홈페이지로 화면이 전환되는 아웃링크방식으로 뉴스를 게재하

press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”라고 규정하고 있는 연방헌법 증보(The United States Constitution Amendment) 제1조를 들지만, 여기에 국민주권원리를 결부하여 파악하는 견해도 유력하다; Kyrre Eggen, *The Protection of Freedom of Expression in Article 10 in the European Convention of Human Rights*, Oslo: Oslo University Press, 1994, p.63.

미국에서 ‘알 권리’라는 용어는 제2차 세계대전 이후 냉전체제의 구축과정에서 정부의 비밀주의 경향에 대항하는 언론운동에서 주창되었는데, 정보를 입수할 권리와 사전억제 없이 인쇄할 권리 등이 그 핵심 내용으로 거론된다; See James R. Wiggins, *Freedom or Secrecy*, New York, NY: Oxford University Press, 1956, pp.3~4.

- 42) 정보주체의 동의 없이 개인정보를 공개함으로써 침해되는 인격적 법익과 정보주체의 동의 없이 자유롭게 개인정보를 공개하는 표현행위로서 보호받을 수 있는 법적 이익이 하나의 법률관계를 둘러싸고 충돌하는 경우에는 개인이 공적인 존재인지 여부, 개인정보의 공공성 및 공익성, 개인정보 수집의 목적·절차·이용형태의 상당성, 개인정보 이용의 필요성, 개인정보 이용으로 인해 침해되는 이익의 성질 및 내용 등 여러 사정을 종합적으로 고려하여 개인정보에 관한 인격권 보호에 의하여 얻을 수 있는 이익(비공개 이익)과 표현행위에 의하여 얻을 수 있는 이익(공개 이익)을 구체적으로 비교衡量하여 어느 쪽 이익이 더욱 우월한 것으로 평가할 수 있는지에 따라 그 행위의 최종적인 위법성 여부를 판단하여야 한다; 대법원 2011. 9. 2. 선고 2008다42430 전원합의체 판결.
- 43) 방송매체 중에서는 KBS-1·2TV와 KBS지역네트워크를 포함해 한국방송공사가 70건으로 가장 많은 사건 수를 기록했다. 중앙일간지 중에는 2011년에 이어 조선일보가 65건으로 가장 많은 사건 수를 보였다; 교육본부 연구팀 編著, 2012년도 언론조정중재·시정권고 사례집, 언론중재위원회, 2013, 18쪽.

는 방식을 변경하였기 때문인 것으로 해석된다. 포털의 아웃링크기사에 대하여는 기사제공 언론사가 정정보다나 반론보도를 한 경우 대부분 그 내용이 포털에 자동으로 반영되기 때문에 특별히 포털사에 대한 손해배상을 원하는 경우가 아니라면 별도로 정정보다 등을 청구하지 않아도 되기 때문이다. 또한 과란·야후 등 주요 포털사들이 각각 2012년 7월말과 12월말에 사업을 정리하면서 뉴스서비스도 함께 중단한 점도 이유로 들 수 있다.⁴⁴⁾

〈표〉 2012년도 매체 유형별 현황

* () 안의 숫자는 %

(2012. 1. 1.~2012.12.31.)

매체유형 청구건수	신문	방송	잡지	뉴스통신	인터넷 신 문	인터넷뉴스 서비스
2,401	665	243	11	83	945	454
(100)	(27.7)	(10.0)	(0.5)	(3.5)	(39.4)	(18.9)

한편, 2013년의 경우 매체 유형별 청구건수는 인터넷신문 1,130건(46.4%), 일간신문 380건(15.6%), 인터넷뉴스서비스 369건(15.2%), 방송 288건(11.8%), 주간신문 142건(5.9%), 뉴스통신 112건(4.6%), 잡지 10건(0.4%), 기타 2건(0.1%) 순이었는바, 이처럼 인터넷신문을 대상으로 한 조정신청의 증가세가 두드러지고 종이신문에 대한 조정신청이 감소한 것은 독자들의 뉴스 소비 형태가 오프라인에서 온라인으로 옮겨가고 있음을 나타내고 언론보도 피해에 대한 구제도 오프라인 매체의 보도에 비해 인터넷에 기반을 둔 온라인 매체의 보도에서 더욱더 요구된다는 점에서 시사하는 바가 크다고 볼 수 있다.⁴⁵⁾

44) *Ibid.*, p.22.

45) 인터넷신문 외에 인터넷뉴스서비스, 뉴스통신까지 온라인 매체로 포함시켜 본다면 이러한 현상은 더욱 두드러진다. 이들을 모두 합치면 인터넷에 기반을 둔 매체 관련 조정신청 건수는 모두 1,611건으로 전체의 66.2%에 이른다. 이에 반해 인쇄매체에 대한 조정신청 건수는 2012년에 비해 크게 줄어들었다. 일간신문을 상대로 한 조정신청은 2012년 496건에서 380건으로 116건(23.4%)이 감소했으며 주간신문과 잡지를 상대로 조정신청 역시 각각 소폭 감소를 보였다; 교육본부 연구팀 編著, 2013년도 언론조정중재·시정권고 사례집, 언론중재위원회, 2014, 24~25쪽.

이 같은 현상적 추세를 규범적 대응으로 연계한다면 결국 언론기사의 삭제를 요구할 수 있는 ‘잊혀질 권리’의 도입은 언론사의 표현으로 인한 법익과 기사를 삭제할 때 얻을 수 있는 권익 사이의 균형과 조화를 어떻게 이룰 것인가가 관건이다. 다만, 개인정보 처리로 인한 피해의 주장에 대하여는 당사자가 공적 인물일 경우나 기사가 다루는 사안이 공공의 이익과 관련되는 때에는 삭제요청을 받아들이지 않아야 할 것으로 본다. 또한 삭제권 행사에 있어 다툼이 있다면 삭제에 갈음하는 조치로 개인정보 처리를 제한하는 것이 필요하다고 본다.

Ⅲ. 법제도적 고찰

1. 현행법에서의 수용 여부

전술한 유럽연합 규정에 따라 ‘잊혀질 권리’를 도입하는 데 대하여 다음과 같은 비판적인 견해도 존재한다.⁴⁶⁾

첫째, 삭제요청의 진위확인 등에 대한 보완이 필요하다는 의견이다. 개인정보처리자가 정보주체의 삭제요청의 진위 여부를 어떤 방법으로 판단하고 ‘잊혀질 권리’를 어떤 방법으로 실현해야 하는지에 대한 이행방법이 보다 구체화되지 않으면 개인정보처리자에 대한 규제가 적정하지 못하다는 주장이다.

둘째, 제3자에 대한 통지 등이 현실적으로 곤란하다는 점이다. 온라인상에서 개인정보는 순식간에 복사되어 전파되기 때문에 제3자에게 삭제요구를 통지하는 것은 현실적으로 불가능하며 천문학적 비용이 소요된다는 것이다.

셋째, 불법행위 은닉수단으로 악용될 우려가 다분히 있다는 비판도 있다. 불법행위를 숨기기 위한 수단으로 전이된다면 ‘잊혀질 권리’의 입법목적과의 괴리를 야기하여 오히려 범죄에 대한 수사를 방해할 수 있다고 반론을 제기한다.

이와 같은 생각은 개인정보자기결정권과 상충하는 가치로서 개인정보처리권의 규제에 대한 적정성과 아울러 개인정보 활용과의 합리적인 균형을 가능하게 한다는 데서, 법익교량적·규범

46) Conrad Coutinho, *The Right to Be Forgotten?*, Columbia Science and Technology Law Review, 2011, 4, 6., available at <<http://www.stlr.org/2011/04/the-right-to-be-forgotten/>>.

조화적 입법의 형성 및 해석과 적용의 헌법합치적 가치와 정보질서의 철학을 상기해볼 필요가 있다.⁴⁷⁾ 다시 말해서 ‘잊혀질 권리’의 필요성이 갖는 목적의 정당성을 심사척도로서 과잉금지원칙 또는 비례원칙에 의한 정합성 확보가 이루어져야 한다는 것이다. 또한 현행 우리 법제에서 이와 같은 논의를 얼마나 수용하고 있는지 여부를 되짚어보는 일도 선행되어야 한다. 그렇지만 개인정보자기결정권의 개념에 따라 개인정보 수집에 대한 정보주체의 동의와 이에 대한 동의 철회는 개인정보자기결정권의 핵심적인 파생적 권리로 파악된다. 이에 맞서 ‘잊혀질 권리’의 특이성으로 ① 정보를 생성하고 게시하며 유포하는 것에 대한 제한의 문제가 아니라 정보 생성 및 게시 등의 공개 이후 정보상태에 대한 권리라는 점, ② 디지털 메모리의 고유한 특성인 정보에의 접근 용이성, 정보의 지속 가능성, 정보 검색·제공의 포괄성에 기인한 권리침해의 지속성, ③ ‘잊혀질 권리’를 둘러싼 권리주체의 복합적 구조와 이와 같은 상황적·구조적 특이성으로 말미암아 기본권 충돌관계를 전제로 한다는 측면 등에 주목하는 견해도 존재하지만,⁴⁸⁾ 이러한 특이성이 ‘잊혀질 권리’의 전유물인지 여부를 검증하지 않은 이 같은 주장은 개인정보 처리과정에서 볼 때 정보의 생애주기 단계에서 논의한다면 공개 전후의 시점 문제는 본질적인 것이 아니라는 점에서 설득력을 얻지 못한다고 사료된다.

한편, 개인정보를 정보주체로부터 수집하는 경우가 아닌 때, 즉 이미 수집된 개인정보로부터 새롭게 생성되거나 기록·보유·저장되는 개인정보에 대하여는 정보주체로부터의 동의 획득이 불가능하거나 개인정보처리자로 하여금 이를 의무화하는 데 이익형량 또는 법익교량에 의하여 논리구성을 하기 어려우므로 정보주체의 권리보장에 대해서는 개인정보의 수집과는 다른 논의

47) 우리나라의 경우 「대한민국헌법」 제119조는 제1항에서 “대한민국의 경제질서는 개인과 기업의 경제상의 자유와 창의를 존중함을 기본으로 한다.”고 규정하여, 국가가 시장의 자율성을 보장하면서 시장참여자들간의 경쟁을 위한 규칙(game rule)을 확정하고 그 행위준거를 제시하는 한편 그들이 상호신뢰감이나 안정감을 가지고 시장활동(market operation)을 영위할 수 있도록 각종의 표준이나 지침 등을 설정함으로써 그 과정과 결과 모두를 행위자가 책임질 수 있게 하는 것을 기본적인 경제질서로 삼고 있다. 즉, 국가는 규범설정자이자 심판관이며 사후적 교정자 또는 후견자로서 기능함으로써 시장의 자율성을 최대한 보장해 주어야 한다는 것이다. 다만 같은 조 제2항에서는 “국가는 균형 있는 국민경제의 성장 및 안정과 적정한 소득의 분배를 유지하고, 시장의 지배와 경제력의 남용을 방지하며, 경제주체간의 조화를 통한 경제의 민주화를 위하여 경제에 관한 규제와 조정을 할 수 있다.”고 하여, 경제주체간 조화를 통한 경제의 민주화라는 요청에 따라 국가가 시민사회의 경제영역에의 참여를 중심으로 하는 절차적 장치와 그 실천이 적절하고도 유의미한 판단 아래 이루어지도록 하여 그들이 진정한 참여자로 기능할 수 있게 하고 있기도 하다.

48) 조소영, 잊혀질 권리: 정보의 웰다잉(well-dying)을 위한 법리 검토, 공법연구 제41집 제2호, 한국공법학회, 2012, 437~438쪽 참조.

가 필요하다.⁴⁹⁾ 이러한 점 역시 ‘잊혀질 권리’ 도입의 입법방안에 대한 실질적 수요라 할 수 있다. 즉 개인정보처리에 대한 동의·철회가 동의 획득 자체를 전제로 하지 않아 법리적으로 무의미한 경우에도 정보주체의 개인정보자기결정권을 확보하는 방안은 이미 처리된 개인정보에 대하여 삭제·처리정지·검색차단 또는 사정변경사실고지 등의 요구를 할 수 있게 하는 것이 이론적으로 가능하고, 개인정보처리자의 개인정보처리권과의 형평을 고려하여 이와 같은 의무 부과와 행정규제에 관한 법적 근거를 마련할 수 있는 것이다. 결국 동의 획득과 동의 철회 여부는 무관하게 개인정보자기결정권의 보장에 관한 일관된 파생적 권리가 필요하고 이와 같은 범주에서 ‘잊혀질 권리’가 주목받게 되는 것이다. 그렇다면 「개인정보 보호법」은 정보주체의 권리로 이를 어느 정도 규율하고 있는 것으로 해석할 수 있다.⁵⁰⁾

그런데 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 경우 정보통신서비스 제공자를 정보주체의 개인정보에 관한 권리 보장의 규율대상으로 하고 있지만, 「개인정보 보호법」은 일반법적 효력을 가진다. 따라서 정보통신서비스 제공자에 대하여는 법률 제11690호로 2013년 3월23일 일부개정된 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 개인정보자기결정권에 기인하는 파생적 권리의 보장 의무를 보유하고 할 것인바, “정보통신서비스 제공자등(정보통신서비스 제공자와 그로부터 이용자의 개인정보를 제공받은 자)은 정보통신서비스를 대통령령으로 정하는 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.”라고 규정하고 있는 같은 법 제27조제2항이 바로 그것이다. 그리고 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 개인정보 누출 등의 통지⁵¹⁾나 개인정보 이용내역의 통지⁵²⁾는 「개인정

49) 「개인정보 보호법」 제2조제2호는 “처리란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.”라고 규정하고 있지만, 실제로 「개인정보 보호법」에서 규율하고 있는 처리단계는 수집·이용·제공 및 파기에 국한되고 있다. 여하튼 이러한 관점에서 「개인정보 보호법」 소정의 처리 관념에서 볼 때 ‘잊혀질 권리’는 헌법에 열거되지 않은 국민의 자유와 권리로서 개인정보자기결정권이 구체화된 양상이라고 이해하는 것이 논리적인 설명이라고 생각한다.

50) 「개인정보 보호법」 제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

보 보호법」 제4조제1호에 따른 개인정보의 처리에 관한 정보를 제공받을 권리에 해당하여 개인 정보자기결정권에 수렴된다. 다만, 링크·복제·복사의 중단 및 삭제 통지의무는 개인정보 누출 통지의무와 입법취지에 있어 같지는 않지만, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 제29조제2항에서 “정보통신서비스 제공자등은 정보통신서비스를 대통령령으로 정하는 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다.”라고 명문화함으로써 같은 법 시행령 제16조(개인정보의 파기 등)에 따라 통상 3년 동안 이용자가 정보통신서비스를 이용하지 아니하는 경우에는 정보통신서비스 제공자등은 이용자의 개인정보를 해당 기간 경과 후 즉시 파기 하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하도록 하고 기간 만료 30일 전까지 개인정보가 파기되거나 분리되어 저장·관리되는 사실과 기간 만료일 및 해당 개인정보의 항목을 전자우편 등의 방법으로 이용자에게 알리도록 하는 이른바 개인정보 유효기간제 도입을 규정하고 있으므로 이로써 그 취지에 갈음할 수 있을 것이다.

이렇게 본다면 ‘잊혀질 권리’를 도입하는 문제에 대한 성찰보다는 개인정보자기결정권의 보장 범위에 대한 논의를 전개함이 타당할 것이며, 여기에 개인정보에 관한 정보주체의 권리보장 범

-
- 51) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3 (개인정보 누출등의 통지·신고) ① 정보통신서비스 제공자등은 개인정보의 분실·도난·누출(이하 “누출등”이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 모든 사항을 해당 이용자에게 알리고 방송통신위원회에 신고하여야 한다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.
1. 누출등이 된 개인정보 항목
 2. 누출등이 발생한 시점
 3. 이용자가 취할 수 있는 조치
 4. 정보통신서비스 제공자등의 대응 조치
 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
- ② 제1항에 따른 통지 및 신고의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
- ③ 정보통신서비스 제공자등은 개인정보의 누출등에 대한 대책을 마련하고 그 피해를 최소화할 수 있는 조치를 강구하여야 한다.
- 52) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제30조의2 (개인정보 이용내역의 통지) ① 정보통신서비스 제공자등으로서 대통령령으로 정하는 기준에 해당하는 자는 제22조 및 제23조제1항 단서에 따라 수집한 이용자 개인정보의 이용내역(제24조의2에 따른 제공 및 제25조에 따른 개인정보 취급위탁을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니하다.
- ② 제1항에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지 주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다.

위를 확정할 것인가에 관한 헌법합치적 정보질서의 고려가 요구된다고 할 것이다. 그렇지만 정보사회의 역기능적 특징으로 말미암아 그 구체적 규율에 있어서는 입법적 공백이나 흠결이 존재하여 규범적 대응책의 마련이 요구되기도 한다. 예컨대 2013년 4월 현재 국내 초고속인터넷 가입자 수가 1천8백만 명을 넘어섰지만,⁵³⁾ 그 편리함의 이면에는 부작용이 존재하고 있다.⁵⁴⁾ 무엇보다 정보기술의 발달에 따른 정보환경의 변화로 미디어가 팽창함으로써 정보의 생산·분배가 인간의 정보처리능력을 앞지르는 이른바 정보과잉(information overflow)의 현상적 증폭은 관심을 받는 정보만이 선택되어 과도한 분절화를 초래할 뿐 아니라 인터넷 이용자들이 과거 웹상 방치되는 개인정보로 인해 피해를 입는 상황의 발생을 양산하기에 이르렀다.⁵⁵⁾

이와 같은 이유 때문에 ‘잊혀질 권리’ 문제가 대두되었는바, 정보를 둘러싼 전반적인 법현상을 연구대상으로 설정하여 단일 법체계를 탐구하려는 학문적 노력으로 이른바 ‘정보법(Informationsrecht)’ 내지 ‘정보법학(Informationsrechtslehre)’ 차원에서 정보인권을 논하거나 정보를 둘러싼 다양한 법률관계 제반영역을 ‘정보헌법(Informationsverfassungsrecht)’의 틀 속에서 정보인권을 헌법학적으로 구성해내는 시도에 비추어 볼 때,⁵⁶⁾ 여기서는 정보인권을 ‘정보사회에서의 바람직한 정보환경을 조성하고 인간존엄성을 헌법적 정보질서에 부합하게 인식할 때 그 권리의 다발’로 이해하고 그 구체화 측면에서 ‘잊혀질 권리’의 보장에 대한 입법방안의 모색하는 것이 필요하다고 할 것이다.⁵⁷⁾

요컨대, 유럽연합 규정에서의 삭제에 갈음한 개인정보의 처리 제한 또는 링크·복제·복사의 중단 및 삭제 통지의무의 ‘잊혀질 권리’ 보장차원에서의 도입 여부가 관건이 된다. 또한 현행 법제상의 개인정보의 처리에 관한 정보를 제공받을 권리 또는 개인정보의 처리로 인하여 발생한

53) 인터넷통계정보검색시스템(ISIS). (<http://isis.kisa.or.kr>)에서도 이용가능.

54) 인터넷에서의 정보가 불법적이거나 해당 정보의 취급에 인터넷의 특성에 기인하여 특유한 입법조치가 뒤따를 수 있게 되는 것이다; Jessica L. Chilson, *Unmasking John Doe: Setting a Standard for Discovery in Anonymous Internet Defamation Cases*, 95 Va. L. Rev. 389, 2009, pp.389~390.

55) Andrew Chadwick, *Internet Politics: States, Citizens, and New Communication Technologies*, Oxford: Oxford University Press, 2006, p.384.

56) 이미 ‘정보헌법’이라는 용어를 사용해온 독일에서조차 특정한 기본권군을 ‘정보기본권’이라는 하나의 체계로 정립한 단계에는 이르지 않은 것으로 보이며, 아직 독자적인 ‘정보기본권’을 통합적으로 제시하지 못하고 있다고 여겨진다. 다만, 그 법적 성격의 규명을 전제로 ‘기술의 헌법수용성’의 대안으로 ‘헌법의 기술수용성’의 차원에서 기술발전이 생활관계와 기본권에 주는 영향을 고려한 헌법 개정도 신중히 논의해볼 필요가 있다; 김민호·지성우, 정보법의 의의와 과제, 한국정보화진흥원, 2009, 69~70쪽.

57) 같은 맥락에서의 정보인권의 의의에 관한 시론적 탐색은 拙稿, 정보인권의 법적 의의와 좌표, 정보인권의 법적 보장과 그 구체화, 국가인권위원회, 2010, 1~24쪽 참조.

피해를 신속하고 공정한 절차에 따라 구제받을 권리 등의 경우를 생각한다면 법익교량적·규범 조화적 '잊혀질 권리' 보호방안의 논의에 있어서 더욱 신중한 접근이 요구된다고 할 것이다.

2. 개정법률안에 대한 검토

관련된 의원입법이 상정된 상태이므로 이하 함께 논의하기로 한다.⁵⁸⁾

가. 정통망법 개정안 관련

2013년 2월 12일 이노근의원이 대표발의한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안은 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의2⁵⁹⁾

58) 2013년 2월 12일자 보도자료, 「온라인에 노출된 자신이 올린 글 등을 삭제할 수 있도록 하는 '잊혀질 권리'의 법제화 추진(http://www.lng5238.net/board/view.php?db=n3&idx=68&s_no=56&page=1&key=11&index=)」에는 다음과 같이 설명되어 있다.

○ 네이버·다음 등 검색엔진을 통해 인터넷에 무분별하게 노출되고 있는 자신의 글과 사진·동영상 등을 삭제할 수 있도록 법에 명시하는 방안이 추진될 전망이다.

○ 그러나 현재 잊혀질 권리에 대한 법적 근거는 충분치 않다. 현행법상으로 인터넷상의 글·사진을 올리게 되면 「저작권법」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 규정하는바, '저작물'로 간주된다. 하지만 「저작권법」 제103조에서는 글을 올린 사람이 동의하지 않는 저작물에 대해서 복제 및 전송을 중단요구 할 수 있을 뿐 삭제요청에 대한 근거는 없다. 또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조에 따르면, 삭제요청을 할 수 있는 경우를 '사생활 침해나 명예훼손이 있는 경우'만으로 제한하고 있다. 이렇다 보니 단순히 자기가 작성한 글 등이 공개되어 피해를 입게 되는 경우에도 서비스제공자에게 삭제를 요청할 수 있는 권한을 명시한 근거가 실질적으로 없는 셈이다.

○ 이노근 의원의 법안이 통과되면, 온라인상에 게시된 자신의 저작물을 자유롭게 삭제할 수 있도록 하는 근거가 마련될 전망이다. 이 법안의 주요내용인 '개인정보의 자기결정권'은 헌법 제10조에 보장된 일반적 인격권과 헌법 제17조에 보장된 사생활자유에서 근거를 찾고 있다. 일각에서는 헌법 제21조 표현의 자유를 침해하는 것이 아니냐는 우려의 목소리를 내고 있으나, 이 개정안은 명확히 자신이 작성한 저작물만을 삭제요청의 대상으로 한정하고 있으므로 표현의 자유 침해 논란과는 거리가 있다.

○ 이노근 의원은 "정보통신기술이 발달하면서 정보의 용이성은 우리 삶을 편안하게 하고 있지만, 정확하지 않은 정보나 밝혀지기 꺼려하는 개인의 신상까지 무분별하게 전파되어 억울한 사례가 발생하고 있다"며, "자신이 쓴 저작물은 자신이 삭제할 수 있는 최소한의 권한은 보장해줘야 한다"고 말했다.

59) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의2 (정보의 삭제요청 등) ① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 '삭제등'이라 한다)를 요청할 수 있다.

② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치

에 제7항을 신설하는 방안인바, 그 제안이유는 다음과 같다.

정보통신기술의 발달에 따른 정보의 보존과 보급의 용이성은 우리의 삶을 편리하게 개선해주는 반면, 정확하지 않은 정보나 밝혀지기를 꺼려하는 개인의 정보까지 제한없이 전파되도록 하여 불안감을 조성하고 있음. 특히 현행법에 따르면 정보통신망을 통하여 전파되는 정보의 삭제요청은 해당 정보가 사생활 침해나 명예훼손 등 특정인의 권리를 침해한 경우에 한하여 인정함에 따라 개인이 자신과 관련된 내용 또는 과거 자신이 작성한 글 등에 대해서는 삭제요구가 어려울 수 있음. 이에 이용자가 정보통신망을 통하여 공개를 목적으로 작성한 정보에 대한 삭제권한을 명시적으로 인정함으로써 정보의 자기결정권을 강화하려는 것임(안 제44조의2제7항 신설).

현 행	개 정 안
제44조의2(정보의 삭제요청 등) ① ~ ⑥ (생략) <신설>	제44조의2(정보의 삭제요청 등) ① ~ ⑥ (현행과 같음) ⑦ <u>이용자가 자신의 저작물로서 정보통신망을 통하여 일반에게 공개를 목적으로 제공한 정보에 대하여 해당 정보를 취급하는 정보통신서비스 제공자에게 삭제를 요청하는 경우 정보통신서비스 제공자는 지체 없이 대통령령으로 정하는 확인 절차를 거쳐 해당 정보를 삭제하고 즉시 신청인에게 알려야 한다.</u>

이에 대하여 다음과 같은 판단이 가능할 것이다.

등의 필요한 조치를 하고 즉시 신청인 및 정보계재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 게시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다.

- ③ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다.
- 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.
- ⑤ 정보통신서비스 제공자는 필요한 조치에 관한 내용·절차 등을 미리 약관에 구체적으로 밝혀야 한다.
- ⑥ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보에 대하여 제2항에 따른 필요한 조치를 하면 이로 인한 배상책임을 줄이거나 면제받을 수 있다.

첫째, 입법체계상 신설되는 조항의 적절성 여부에 관한 것이다.⁶⁰⁾ 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의2는 타인이 게시하여 권리를 침해하는 위법한 정보의 삭제와 관련되므로 이용자 자신이 게시한 정보의 삭제 요청권을 포함시키는 것은 부적절하다는 지적도 일응 타당한 것으로 보이지만, “정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 ‘삭제등’이라 한다)를 요청할 수 있다.”라고 규정하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의2제1항의 문언상 취지는 이용자 스스로 게시한 타인이 정보를 제공한 문지 아니하고 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 인한 권리침해에 대한 삭제등 요청권의 보장이라 할 것이다. 따라서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44의2가 타인이 게시한 것으로 한정 해석하기 어려우며, 일반 공개 목적의 정보의 제공으로 인하여 권리침해를 입은 이용자(+a)가 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재를 요청할 수 있을 때 정보의 게시주체는 문리해석상 제한될 수 있는 성질의 것은 아니라 할 것이다. 그러므로 개정법률안에서 신설하려는 제7항의 체계정당성은 일단 확인될 수 있다고 본다. 다만, 그 정당성을 인정한다면 오히려 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의2제1항을 “정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 ‘삭제등’이라 한다)를 요청할 수 있다.”라고 개정하는 방안도 고려될 수 있다고 하겠다.

둘째, 개정법률안에서 신설하려는 제7항은 삭제 요청대상을 저작물에 한정하고 있는바, 「저

60) 이는 동일 규범 내에서 또는 상이한 규범간에 -수평적 관계이건 수직적 관계이건- 그 규범의 구조나 내용 또는 규범의 근거가 되는 원칙면에서 상호 배치되거나 모순되어서는 안된다는 하나의 헌법적 요청(*Verfassungspostulat*)인 체계정당성(*Systemgerechtigkeit des Gesetzgebers*)의 원리에 따른 검토라 할 수 있다. 다시 말해서 체계기속성(*Systembindung*) 혹은 체계적합성(*Systemgemäßheit*)의 원칙이라고도 하는 체계정당성의 원칙은 규범 상호간의 구조와 내용 등이 모순됨이 없이 체계와 균형을 유지하도록 입법자를 기속하는 헌법적 원리라 하겠다. 이처럼 규범 상호간의 체계정당성을 요구하는 이유는 입법자의 자의를 금지하여 규범의 명확성, 예측가능성 및 규범에 대한 신뢰와 법적 안정성을 확보하기 위한 것이고 이는 국가공권력에 대한 통제와 이를 통한 국민의 자유와 권리의 보장을 이념으로 하는 법치주의원리로부터 도출되는 것이다; 헌법재판소 2004.11.25., 2002헌바66결정, 판례집 16-2하, 314, 333; Uwe Kischel, *Systembindung des Gesetzgebers und Gleichheitssatz*, AöR 124, 1999, S. 174ff.

작권법』 제2조제1호에 따르면 저작물은 인간의 사상 또는 감정을 표현한 창작물을 말한다. 「저작권법」상 저작물은 ‘문학·학술 또는 예술과 같은 문화의 영역에서 사람의 정신적 노력에 의하여 얻어진 아이디어나 사상 또는 감정의 창작적 표현물’을 가리키므로 그에 대한 저작권은 ‘아이디어 등을 말·문자·음(音)·색(色) 등에 의하여 구체적으로 외부에 표현한 창작적인 표현 형식’만을 보호대상으로 하는 것이어서 ‘표현의 내용이 된 아이디어나 그 기초 이론’ 등은 설사 독창성·신규성이 있는 것이라 하더라도 저작권의 보호대상이 될 수 없을 뿐만 아니라, 표현 형식에 해당하는 부분에 있어서도 다른 저작물과 구분될 정도로 저작자의 개성이 나타나 있지 아니하여 창작성이 인정되지 않는 경우에는 이 역시 저작권의 보호대상이 될 수가 없다.⁶¹⁾ 결국 「저작권법」에 의하여 보호되는 저작물은 문학·학술 또는 예술의 범위에 속하는 창작물이어야 하는바, 여기에서 창작물이라 함은 저자 자신의 작품으로서 남의 것을 베낀 것이 아니라는 것과 최소한도의 창작성이 있다는 것을 의미하고, 따라서 작품의 수준이 높아야 할 필요는 없지만 「저작권법」에 의한 보호를 받을 가치가 있는 정도의 최소한의 창작성은 요구되므로, 단편적인 어구나 계약서의 양식 등과 같이 누가 하더라도 같거나 비슷할 수밖에 없는 성질의 것은 최소한도의 창작성을 인정받기가 쉽지 않다 할 것이다.⁶²⁾ 따라서 사실만을 전달하는 게시글의 경우 창작물에 해당하지 않으므로 비록 개인정보가 포함되어더라도 저작물에 해당되지 않아 삭제 요청의 대상이 될 수 없다는 점과 아울러 오히려 해당 정보가 저작물인지 여부에 대하여 이용자와 정보통신서비스 제공자 모두 판단하기가 어려운 경우가 발생한다는 점으로 인하여 입법목적의 실현을 저해하게 될 것으로 본다.

셋째, 삭제 요청에 대한 요건이나 예외를 인정하지 않음으로 인하여 발생하는 문제가 있을 수 있다. 무제한적인 삭제 요청의 인정은 정보통신서비스 제공자에 대하여 과도한 경제적·기술적 부담을 줄 수 있는바, 예컨대 해당 저작물의 게시자가 회원탈퇴한 것으로 확인되는 경우 이용자가 자신의 저작물을 삭제해달라고 요청한 데 대하여는 그가 게시자인지 확인이 곤란하지만

61) 대법원 1999.10.22. 선고 98도112 판결; 대법원 1999.11.26. 선고 98다46259 판결; 대법원 2009.12.10. 선고 2007도7181 판결 등 참조; ‘사실’이나 ‘역사’에 대한 직접적인 표현형식도 학문 또는 민주주의의 발전을 위하여 저작물이 될 수 없다. ‘사실’이나 ‘역사’의 경우 이미 존재하고 있는 것이므로 이들의 창작을 위하여 ‘배타적 권리’를 부여할 필요가 없기 때문이다.

62) 또한 작품 안에 들어 있는 추상적인 아이디어의 내용이나 과학적인 원리, 역사적인 사실들은 이를 저자가 창작한 것이라 할 수 없으므로, 저작권은 추상적인 아이디어의 내용 그 자체에는 미치지 아니하고 그 내용을 나타내는 상세하고 구체적인 표현에만 미친다; 1997. 11. 25. 선고 97도2227 판결; 대법원 1993. 6. 8. 선고 93다3073, 3080 판결 등 참조.

개정법률안에서 신설하려는 제7항에 근거하여 지속적으로 삭제요청을 할 수 있으며,⁶³⁾ 이 경우 삭제 요청자와 저작물의 게시자가 동일인인지 여부를 현재 기술로 확인이 가능한지도 불분명한 상황에서 정보통신서비스 제공자는 법적 분쟁 가능성의 증가와 민원 비용의 증가를 감수해야 할 것이다. 한편, 표현의 자유 보장 등 예외를 인정하지 않음으로써 공공의 이익 또는 타인의 권리를 침해할 우려가 있다고 하겠다.

나. 저작권법 개정안 관련

2013년 2월 12일 이노근의원이 대표발의한 「저작권법」 일부개정법률안은 현행 「저작권법」에 제103조의4를 신설하는 방안이다.

현 행	개 정 안
〈신 설〉	제103조의4(저작물의 삭제요청) ① 온라인서비스 제공자의 서비스를 이용하여 정보통신망에 자신의 저작물을 게시한 자는 언제든지 해당 온라인서비스제공자에게 게시된 저작물의 삭제를 요청할 수 있다. ② 온라인서비스제공자는 제1항에 따른 해당 저작물의 삭제를 요청받으면 지체 없이 해당 저작물을 삭제하고 즉시 신청인에게 알려야 한다.

그 제안이유는 다음과 같다.

정보통신기술의 발달에 따른 정보의 보존과 보급의 용이성은 우리의 삶을 편리하게 개선해주는 반면, 정확하지 않은 정보나 밝혀지기를 꺼려하는 개인의 사상 등에 관한 정보까지 제한 없이 전파되도록 하여 불안감을 조성하고 있음. 한편, 현행법에서는 온라인서비스제공자의 서비스를 이용한 저작물의 복제·전송에 따라 자신의 권리가 침해될 경우 이에 대한 중단의 요구

63) 삭제 요청자가 회원인 경우 이용자 자신이 제공한 정보인지 확인 가능하지만 비회원이나 탈퇴회원의 경우 확인이 곤란하며, 이용자 본인임을 사칭하여 타인이 정보를 삭제요청하는 경우도 발생 가능하다고 본다.

권한을 명시하고 있는 반면, 권리침해 여부와 관계없이 온라인상에 게시한 자신의 저작물에 대한 자유로운 삭제권한에 대한 언급이 없는 상황임. 이에 온라인서비스제공자의 서비스를 이용하여 정보통신망에 게시한 자신의 저작물에 대한 삭제권한을 명시적으로 규정함으로써 정보의 자기결정권을 강화하려는 것임(안 제103조의4 신설).

이에 대하여 다음과 같은 판단이 가능할 것이다.

첫째, 「저작권법」 제103조가 ‘복제·전송의 중단’과 관련하여 온라인서비스제공자의 의무를 규정하고 있으므로 관련된 제103조의2, 제103조의3과 더불어 이에 대하여 규율하는 것은 체계 정당성의 원칙에 따른 입법체계상 부적합하다고 볼 수 없다.⁶⁴⁾

둘째, 삭제조치의무를 부담하는 주체가 정보통신서비스 제공자에서 온라인서비스제공자로 변경된 것과 확인절차에 대한 하위법령에의 위임이 없는 것을 제외하면 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안과 차이가 없다. 그런데 온라인서비스제공자(Online Service Provider; OSP)⁶⁵⁾를 간단히 정의하면 인터넷이라는 도구를 제공하는 자라 할 수 있으며, ‘다중이 이용하는 통신망에 대한 접속을 매개하고 온라인상에서의 정보의 제공과 제공자료를의 매개에 관련된 각종 기능을 제공하는 업체나 기관·개인 그리고 불특정다수인에게 자료의 송·수신을 가능하게 하는 전자계시판을 운영하는 자’ 혹은 “다수의 컴퓨터가 연결되어 있어 다수의 사람들이 이용할 수 있는 통신망에 대한 접근을 매개하거나 통신망 내에서 또는 다른 통신망과의 사이에서 디지털화된 내용물을 송·수신, 제공, 연결매개 등의 인터넷서비스를 제공하는 실체로 이해된다.⁶⁶⁾ 인터넷서비스사업자를 포괄하는 것은 물론, KT와 같은 기간통신사업자, 구글·다음·네이버 등과 같은 검색서비스제공자, 싸이월드와 같은 부가통신사업자를 비롯하

64) 동일 규범 내에서 또는 상이한 규범간에 그 규범의 구조나 내용 또는 규범의 근거가 되는 원칙면에서 상호 배치되거나 모순되어서는 안된다는 하나의 헌법적 요청(*Verfassungspostulat*)으로서 체계기속성(*Systembindung*) 혹은 체계적합성(*Systemgemäßheit*)의 원칙이라고도 하는 체계정당성(*Systemgerechtigkeit des Gesetzgebers*)의 원칙은 규범 상호간의 구조와 내용 등이 모순됨이 없이 체계와 균형을 유지하도록 입법자를 기속하는 헌법적 원리라고 볼 수 있다; 헌법재판소 2004.11.25., 2002헌바66결정, 판례집 16-2하, 314, 333

65) 「저작권법」 제2조제30호 “온라인서비스제공자”란 다음 각 목의 어느 하나에 해당하는 자를 말한다.
 가. 이용자가 선택한 저작물등을 그 내용의 수정 없이 이용자가 지정한 지점 사이에서 정보통신망(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 정보통신망을 말한다. 이하 같다)을 통하여 전달하기 위하여 송신하거나 경로를 지정하거나 연결을 제공하는 자
 나. 이용자들이 정보통신망에 접속하거나 정보통신망을 통하여 저작물등을 복제·전송할 수 있도록 서비스를 제공하거나 그를 위한 설비를 제공 또는 운영하는 자

66) 정상조, 인터넷과 법률, 현암사, 2000, 68쪽.

여 앞으로 나타날 새로운 유형의 인터넷사업자에게도 적용될 수 있다. 종종 인터넷서비스제공자(Internet Service Provider: ISP) 등으로 불리기도 하는 온라인서비스제공자라는 개념은 서비스의 기능적 측면과 국가의 법제에 따라서 용어가 통일되지 못하는 부분이 있기는 하지만,⁶⁷⁾ 이들 용어의 개념은 대체로 ‘정보통신망을 통하여 저작물 등 정보를 제공 또는 상호유통할 수 있도록 서비스를 제공하는 자’로 정의되고 있다.⁶⁸⁾ 이렇게 볼 때 정보통신서비스 제공자에 대한 규율과 차별성 없이 중복규제되는 것으로 볼 수 있다. 더욱이 이미 살펴본 언론부문에의 적용을 고려할 때 인터넷신문이나 인터넷뉴스서비스 등의 경우 정보통신서비스 제공자에 해당하므로 규율의 일원화가 필요하다고 본다.

다. 개정법안에 대한 대안

주지하는 바와 같이 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조제1항은 “이용자는 사생활침해 또는 명예훼손 등 타인의 권리를 침해하는 정보를 정보통신망에 유통시켜서는 안 된다.”라고 규정하고 있다. ‘정보통신망에서의 권리보호’라는 제명은 권리침해 정보의 유통금지로 이해되는바, 온라인상의 권리침해 정보에 대하여 삭제 또는 반박내용의 게재 요청권을 규정하고 있는 같은 법 제44조의2와의 관련성에서 이 문제를 논의할 필요가 있다고 생각한다. 다른 한편으로는 개정안에서 ‘자신의 저작물’로 한정된 삭제 등 요청대상이 이용자 스스로 작성한 것만을 의미하는지 아니면 자신에 관한 것도 포함되는지 여부에 대하여 해석상 혼란이 가중될 수 있다는 점도 존재한다.

한편, 개정법안에서 신설하는 조항으로 인하여 「대한민국헌법」 제21조제1항이 보장하는 표현의 자유를 침해하는 것이 아니냐는 우려의 목소리에 대하여 명확히 자신이 작성한 저작물만을 삭제요청의 대상으로 한정하고 있으므로 표현의 자유 침해 논란과는 거리가 있다는 입장을 취하고 있지만,⁶⁹⁾ 헌법재판소는 “우리나라는 헌법 제21조에 언론·출판의 자유, 즉 표현의 자유

67) 종래 온라인서비스제공자와 유사한 개념으로 사용되어 온 용례로서는 온라인서비스사업자, 온라인사업자, 온라인정보제공자, 네트워크서비스제공자, 네트워크정보중개자, 인터넷서비스제공자, 인터넷서비스사업자, 인터넷정보제공자, 서비스제공자, 전자게시판운영자, 시스템운영자, 서버관리자, 인터넷접속업자, 통신망사업자, 정보통신망관리자, IP업자, 정보제공자, 정보통신서비스제공자 등이 있다.

68) 문일환, 온라인서비스제공자(OSP)의 법적 의무와 책임, 지식재산연구 제7권 제2호, 한국지식재산학회, 2012, 123쪽.

69) 앞의 보도자료(註 58) 참조.

를 규정하고 있는데, 이 자유는 전통적으로는 사상 또는 의견의 자유로운 표명(발표의 자유)과 그것을 전파할 자유(전달의 자유)를 의미하는 것으로서, 개인이 인간으로서의 존엄과 가치를 유지하고 행복을 추구하며 국민주권을 실현하는데 필수불가결한 것으로 오늘날 민주국가에서 국민이 갖는 가장 중요한 기본권의 하나로 인식되고 있는 것이다. 그런데 사상 또는 의견의 자유로운 표명은 자유로운 의사의 형성을 전제로 하는데, 자유로운 의사의 형성은 충분한 정보에의 접근이 보장됨으로써 비로소 가능한 것이며, 다른 한편으로 자유로운 표명은 자유로운 수용 또는 접수와 불가분의 관계에 있다고 할 것이다. 그러한 의미에서 정보에의 접근·수집·처리의 자유, 즉 ‘알 권리’는 표현의 자유에 당연히 포함되는 것으로 보아야 하는 것이다.”라고 설시하고 있어 특히 공적 인물에 관한 게시글인 경우 그 삭제는 ‘알 권리’와 충돌한다고 볼 것이다.⁷⁰⁾ 이렇게 볼 때 『언론중재 및 피해구제 등에 관한 법률』에서 보장하는 피해구제방안인 정정보도 또는 반론보도 청구에 갈음할 수 있도록 정보삭제 이외에도 반박내용의 게재 요청권을 활용할 수 있도록 전제하고 다만 이용자 스스로 작성한 정보에 대하여는 단서로 제시하는 예외의 경우를 제외하고는 지체 없이 삭제하도록 하는 의무를 정보통신서비스 제공자에 부여하는 방안이 제시될 수 있다고 본다.

70) 헌법재판소 1989. 9. 4, 88헌마22, 판례집 1, 176, 188-190; ‘알 권리’의 법적 성질을 위와 같이 해석한다고 하더라도 헌법 규정만으로 이를 실현할 수 있는가 구체적인 법률의 제정이 없이는 불가능한 것인가에 대하여서는 다시 견해가 갈릴 수 있지만, 본건 서류에 대한 열람·복사 민원의 처리는 법률의 제정이 없더라도 불가능한 것이 아니라 할 것이고, 또 비록 공문서 공개의 원칙보다는 공문서의 관리·통제에 중점을 두고 만들어진 규정이기는 하지만 「정부공문서 규정」 제36조제2항이 미흡하나마 공문서의 공개를 규정하고 있는 터이므로 이 규정을 근거로 해서 국민의 ‘알 권리’를 곧바로 실현시키는 것이 가능하다고 보아야 할 것이다. 이러한 관점에서 청구인의 자기에게 정당한 이해관계가 있는 정부 보유 정보의 개시 요구에 대하여 행정청이 아무런 검토 없이 불응하였다면 이는 청구인이 갖는 헌법 제21조에 규정된 언론 출판의 자유 또는 표현의 자유의 한 내용인 ‘알 권리’를 침해한 것이라 할 수 있으며, 그 이외에도 자유민주주의 국가에서 국민주권을 실현하는 핵심이 되는 기본권이라는 점에서 국민주권의(제1조), 각 개인의 지식의 연마, 인격의 도야에는 가급적 많은 정보에 접할 수 있어야 한다는 의미에서 인간으로서의 존엄과 가치(제10조) 및 인간다운 생활을 할 권리(제34조 제1항)와 관련이 있다 할 것이다.”

IV. 결론에 갈음하여

최근 트위터·페이스북 등 사회관계망 서비스 이용자가 늘어나고 구글이 최근 이들 사이트를 검색 결과에 포함시켜 ‘실시간 검색’ 시대가 되면서 사생활권 침해 우려로 이어지고 있으며,⁷¹⁾ 연동형 정보서비스가 증가하면서 언제 어디서나 개인의 정보와 감성을 타인과 공유할 수 있게 되어 이른바 공적 인물뿐만 아니라 평범한 일반인들도 언제든지 피해를 입게 될 수 있는 상황을 현재의 정보환경에서 발견할 수 있다. 소위 언제 어디서나 ‘잊혀질 수 없는 세상’이 도래한 것이다.⁷²⁾ 이에 따라 본인이 원할 경우 온라인상 모든 개인정보를 삭제할 수 있는 ‘잊혀질 권리’ 관념을 도입해야 한다는 의견이 대두되고 있는 실정이다.⁷³⁾

Google에서 콘텐츠 삭제

이 페이지에서는 관련법에 따라 Google 서비스에서 삭제하고 싶은 콘텐츠를 신고할 수 있는 적합한 페이지로 안내해 드립니다. 정보를 충분히 제공해 주시면 문의 내용을 조사하는 데 도움이 됩니다.

Google 서비스 약관 또는 제품 정책과 관련하여 법적인 문제 이외의 문제가 있다면 다음 페이지를 방문하시기 바랍니다. <http://support.google.com>

해당 콘텐츠가 표시되는 Google 서비스마다 신고서를 각각 제출해 주시기 바랍니다.

어떤 Google 제품과 관련된 요청입니까?

- | | |
|-------------------|----------------------|
| ◦Blogger/Blogspot | ◦Google+ |
| ◦웹 검색 | ◦Google 광고 |
| ◦드라이브 및 문서 | ◦Google Play - Music |
| ◦Google Play - 앱 | ◦Google 쇼핑 |
| ◦이미지 검색 | ◦orkut |
| ◦Picasa | ◦YouTube |
| ◦더 많은 제품 보기 | |

https://support.google.com/legal/contact/lr_eudpa?product=websearch

A recent ruling by the Court of Justice of the European Union found that certain users can ask search engines to remove results for queries that include their name where those results are inadequate, irrelevant

71) 한겨레 2011년 1월 5일자 19면 기사.

72) 강장묵, ‘잊혀질 권리(The right to be forgotten)’, 경희사이버대학교 사이버사회연구소 웹진, 2011. (<http://igcs.khcu.ac.kr/board/view.jsp?m=50026&BRD_O=3766에서도 이용가능)

73) 그 이론적 개관의 상론은 지성우, 소위 ‘잊혀질 권리(right to be forgotten)에 관한 탐색적 연구, 정보법학 제15권 제3호, 한국정보법학회, 2012, 55~85쪽 참조.

or no longer relevant, or excessive in relation to the purposes for which they were processed.

In implementing this decision, we will assess each individual request and attempt to balance the privacy rights of the individual with the public's right to know and distribute information. When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there's a public interest in the information—for example, information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials.

If you have a removal request, please fill out the form below. Please note that this form is an initial effort. We look forward to working closely with data protection authorities and others over the coming months as we refine our approach.

Search removal request under European Data Protection law

You will need a copy of a valid form of photo ID to complete this form. Fields marked with an asterisk * must be completed for your form to be submitted.

We're working to finalize our implementation of removal requests under European data protection law as soon as possible. In the meantime, please fill out the form below and we will notify you when we start processing your request. We appreciate your patience.

이미 프랑스에서는 과거 인터넷 이용자들이 웹상 남겼던 개인정보로 인해 피해를 보는 상황이 빈번히 발생하자 '인터넷 이용자들이 과거 웹상 남겼던 개인정보를 삭제할 수 있는지 여부에 대하여 이른바 '잊혀질 권리(Le droit à l'oubli sur Internet; right to oblivion on the Internet)'의 문제가 제기된 지 오래다.⁷⁴⁾ 자신의 개인정보를 온라인에서 삭제하려고 하는 경우 관련 업계의 자율규제만으로는 당사자인 정보주체의 개인정보보호를 위하여 충분하지 못하므로 법률로써 보장할 필요성이 있다는 주장이 제기된 것이다.⁷⁵⁾ 그리하여 2009년 11월 6일 「디지털시대 사생활권 보장에 관한 법안(Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique)」이 Anne-Marie Escoffier 의원과 Yves Détraigne 의원에 의해

74) '잊혀질 권리'의 근원을 망각권(le droit à l'oubli)에서 구하는 견해로는 *See generally* Jeffrey Rosen, *The Right to be forgotten*, 64 STAN. L. REV. ONLINE 88, 2012, pp.88~92.

75) 가령, 다음과 같은 예를 들 수 있다. 리옹(Lyon)에 있는 어느 고등학교 재학생 자녀를 두고 있었던 A는 1990년 말경 'Libertysurffr'이라는 웹사이트를 통하여 자신의 자녀가 다니는 고등학교의 학생·학부모를 위한 단체 홈페이지를 만들었다. 이 홈페이지에는 학부모들의 성명과 전화번호가 등록되어 있었는데, A는 몇 년간 이 홈페이지를 관리하다가 자신의 자녀가 해당 고등학교를 졸업하자 다른 학부모에게 그 역할을 이양했다. 시간이 한 참 흐른 후, A는 구글이나 야후 같은 사이트를 통해 예전 자신이 관리했던 해당 홈페이지에 등록되어 있던 자신의 이름과 전화번호가 그대로 검색된다는 사실을 발견하고 해당 정보를 삭제하려고 시도하였으나 쉽지 않았다. A는 당시 'Libertysurffr'라는 웹사이트를 통해 해당 홈페이지를 만들었으나, 이 회사는 이후 'Tiscali'라는 회사에 인수되었고 'Tiscali'는 곧 'Alice'라는 회사에 인수되었다. 따라서 A는 해당 정보의 삭제를 위해 많은 사람들과 접촉을 해야 했으며, 해당 정보의 삭제까지 많은 시간이 소요되었다.

하원에 발의되었다. 이는 지난 1978년 6월 제정된 「정보처리촉진 및 자유에 관한 법률(Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés)」의 개정과 함께 새롭게 부각되는 개인정보 보호정책의 쟁점이 인식되어 반영되는 사회안전망의 발달 그리고 기술의 진보에 따라 '디지털 메모리(digital memory)'의 출현과 관련된 위험성이 강조되면서 '잊혀질 권리'의 실현을 위한 조치의 마련에 대하여 명확히 규정하고 있었다.⁷⁶⁾ '디지털 장의사'나 DAS(Digital Aging System)의 도입의 경우 현상적으로 이들 규율을 반영하고 있다.

이른바 '잊혀질 권리'의 개념에 대하여 정보보존(data retention)의 제한 차원에서 '기록의 보유에 관한 법적 규제'라는 포괄적 정의가 취해지기도 하고,⁷⁷⁾ 해당 기록을 보유하고 있는 타인에 의해 통제되기보다는 스스로 자신의 정체성을 통제할 수 있는 개인의 권리라는 측면에서 '기록이 저장되어 있는 영구적인 저장소로부터 특정한 기록을 삭제할 수 있는 권리'로 이해되기도 한다.⁷⁸⁾ 특히 정보프라이버시(information privacy)의 권리로서의 면모에 주목해 '인터넷 이용자들이 웹에 남겨둔 자신의 정보를 통제하고 정보를 지우는 것이 가능한 권리'⁷⁹⁾로 파악하는 견해가 유력하게 제시되고 있으나, '잊혀질 권리'를 프라이버시(privacy)⁸⁰⁾의 새로운 국면으로 바라보면서도 다른 권리와 의 상호충돌 가능성을 염두에 두어 그 불균형성을 지적하는 입장도 존재한다.⁸¹⁾ 어떻게 보면 '잊혀질 권리'가 제도적 문제이기에 앞서 유럽연합과 미국간 역외역무 통제에 관한 정책적·전략적 속성의 것이라는 가정 역시 그 가능성을 완전히 배제할 수 없는 논의의 방점이기도 하다.

살피건대, 인터넷을 통한 온라인 개인정보에 있어 정보주체의 '잊혀질 권리' 보장에 관한 논의는 우리나라의 경우 개인정보자기결정권 보호 차원에서 적정규제의 선을 넘지 않는 수위에서

76) <http://www.senat.fr/dossier-legislatif/ppl09-093.html>

77) Jeremy Warner, *The Right to Oblivion: Data Retention from Canada to Europe in Three Backward Steps*, University of Ottawa Law & Technology Journal Vol.2 Iss.1, 75, 2005, pp.77~78.

78) Chris Conley, *Supra Note 21*, pp.53~58.

79) Franz Werro, *The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash*, in: Aurelia Colombi Ciacchi, Christine Godt, Peter Rott & Leslie Jane Smith, *Liability in the Third Millennium*, Baden-Baden: Nomos Verlag, 2009, pp.285~300.

80) 서구에서 발달해온 프라이버시의 개념은 아직 통설적인 정의에는 이르지 못한 것으로서 다양한 개념징표가 논의되고 있으며, 권리로서 프라이버시는 단순히 소극적인 것이 아니라 개인정보자기결정권이라는 적극적인 접근권과 통제권을 포함하는 것이다; Daniel J. Solove & Marc Rotenberg, *Information Privacy Law*, New York, NY: Aspen Publishers Inc., 2003, p.27; Charles Fried, *Privacy*, 77 Yale L. J. 475, 1968, p.482.

81) Jeffrey Rosen, *The Right to be Forgotten*, 64 Stanford Law Review OnLine 88, 88-92 (2012).

어느 정도 구현되어왔다고 볼 수 있다. 다만, 그 규율내용에 있어서는 현행 법제와 비교해볼 때,⁸²⁾ 유럽연합 규정의 ‘잊혀질 권리’가 그대로 원용되어 반영될 사항은 아니라고 생각한다.

아날로그 시대에는 망각이 일반적이었고 기억이 예외였던 데 반해 디지털 혁명으로 인하여 기억이 일반적이 되었고 망각이 예외가 되어버렸다는 전제 아래,⁸³⁾ 이처럼 디지털화로 인하여 개인에 대한 망각이 기본값이었던 과거가 영원히 사라지지 않고 각인되는 상황은 견고한 원형 감옥으로서 Panopticon을 떠올리게 한다. 반면, 이익형량적·규범조화적 해석에 따르면 논의의 실익은 ‘잊혀질 권리’의 도입에 따른 변화이겠지만 그 근거는 바로 개인정보자기결정권의 보장에 대한 검토와 적정수준의 확보라고 할 것이다. 이와 같은 관점에서 ‘잊혀질 권리’ 도입에 관한 문제 역시 우리 정보환경에 부합하면서 이를 규율하는 우리 법제를 형성하는 것이므로 개인정보자기결정권이라는 헌법상 기본적 인권 보장을 위하여 권리 차원의 적절한 설정을 다른 권리와 충돌을 고려하여 논의할 필요가 있다고 하겠다.

82) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 「개인정보 보호법」 제정 이전에 시행된 것으로 “정보통신망 이용촉진 및 정보보호 등에 관하여는 다른 법률에서 특별히 규정된 경우 외에는 이 법으로 정하는 바에 따른다.”라는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제5조 본문 소정의 ‘다른 법률’은 「개인정보 보호법」을 제외한 정보통신망에서의 정보보호에 관한 개별법을 가리키는 것이고 개인정보법이 개인정보 보호에 관한 일반법임은 제1조, 제3조, 제6조 및 부칙 제4조 등에서 확인할 수 있을 뿐 아니라 특히 「개인정보 보호법」 제6조와 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제5조로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 특별법에 해당함은 입법연혁과 입법취지가 함께 고려되어 도출되는 것이라 본다. 다만, 지난 2014년 3월24일 법률 제12504호로 일 부개정된 「개인정보 보호법」의 경우 ‘다른 법률과의 관계’에 관한 제6조는 “개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.”로 다듬어지게 되었다.

83) 또한 디지털 메모리의 확장으로 인간의 사유작용이 위협해진다고 한다. 망각은 부분적으로 적절성에 기반을 두고 정보를 걸러내는 사유 과정인데, 디지털 메모리에 의해 촉발되는 기억은 인간의 추리 능력을 약화시킬 수 있고, 포괄적인 디지털 메모리는 과거 사건들을 시간 순으로 적절하게 배열하는 인간의 능력을 약화시킬 수 있다는 것이다. ‘완전한 기억’이 결코 축복은 아니라는 것이다. 방대하고 접근 가능한 디지털방식 기술의 장점은 인정하지만 자신이 무심코 한 말이나 글 행동이 타인에 의해 즉 썰처럼 돌아와 지울 수 없는 일을 발생시키기도 한다고 보았기 때문이다. 이에 ‘잊혀질 권리’의 개념 도입이 필요하며, 이를 실현하기 위해 ‘디지털 금욕주의’와 ‘정보만료일 제도’를 도입해야 한다고 주장한다. ‘디지털 금욕주의’는 이용자들이 자발적으로 디지털 기기를 사용하지 않아 정보를 축적하는 행위를 지양하는 것으로 스스로 본인의 정보가 노출되지 않도록 하는 근본적인 방법이라고 할 수 있다. 또한 ‘정보만료일’을 부여하여 정보가 일정 기간이 지나면 유통기한이 만료되게 하는 것이 필요하다고 역설하고 있다; 구본권 譯, 같은 책(註 1), 39쪽 이하 참조.

토론문



지성우 (성균관대학교 법학전문대학원 교수)

토론문



양홍석 (법무법인 이공 변호사)

표현의 자유, 개인정보보호 측면에 본 ECJ판결

양 홍 석 변호사(법무법인 이공)



서울시 서초구 서초동 1544-2 일신빌딩 3층
T +82-2-2038-3620 F +82-2-2038-3621



이번 판결의 긍정적 측면

1 검색엔진 서비스의 특수성을 고려한 Google에 대한 판결

- 이번 판결은 세계적인 검색서비스를 제공하는 Google에 대한 판결
- 검색엔진을 통해 특정 개인에 관한 정보가 집약되고, 체계화될 경우 그 자체로 프라이버시 침해, 사적 감시의 일상화가 가능하다는 점에 관한 우려에 따른 판결
- 특정 개인의 정보 생산보다는 **정보의 확산 측면에 방점**을 둔 판결

2 일반대중의 압도적 관심과 개인의 권리를 형량한 결과에 따른 판결

- 이번 판결의 대상이 된 정보는 판결선고시를 기준으로 보면 16년전 경매정보의 링크를 삭제하라는 것임
- 해당 정보의 링크를 삭제하라는 결론을 도출하는 과정에서 "잊혀질 권리"를 무조건 인정(잊혀질 권리의 절대적 우월성)한 판결은 아님
- **정보주체의 공적생활에서의 역할**(the role played by the data subject in public life), **일반대중의 압도적 관심**(the preponderant interest of the general public)을 이유로 한 형량을 한 결과임

2

이번 판결의 긍정적 측면



3 미국 이외의 지역에 거주하는 사람이 Google에 대해 어떤 행위를 직접 청구할 수 있는 근거를 제시한 판결

- Google 본사가 미국 캘리포니아에 있고, 해당 정보를 어떤 곳에 위치한 서버를 통해 처리하는지 밝혀지지 않은 상황에서 Google에 대해 특정 정보의 삭제, 수정 등을 요구할 때 Google본사를 상대로 해야만 하는 부담이 있었는데, 이를 해결해 준 판결
- 국내에서 Google, Google Korea를 상대로 한 개인정보 보호 관련 소송시에도 중요한 선례가 될 것임

4 '이름' 을 이용한 검색결과에서 링크를 삭제하라고 한 판결

- 스페인고등법원이 곤잘레스의 이름이 포함된 경매정보의 링크 자체가 아니라 **이름을 이용한 검색결과(a list of results displayed following a search made on the basis of his name)**에서 해당 경매정보의 링크를 삭제하라는 것임
- 원본 경매정보가 공고된 신문기사 자체가 존재하는 이상 '이름'이 아닌 다른 검색어로 검색결과로 현출가능함

3

이번 판결의 문제점



1 구체적 영향과정에 관한 실시없이 추상적 기준[시간의 경과, 대중의 압도적 관심]만으로 구체적 사안에 적용하기 어려움

- “잊혀질 권리”가 일반적으로 이용자나 검색엔진 운영자의 권리보다 우선하고, 대중의 압도적 관심을 받는 정보에 대해서는 예외를 인정하였는데 구체적으로 어떤 경우 대중의 압도적 관심을 받는 정보인지에 대해 실시하지 않음
- 시간의 경과에 따라 정확하고 적법했던 정보가 EU 지침에 위반될 수 있다는 개념 자체의 위험성은 별론으로 하더라도, 어느 정도의 시간이 흐르면 “부적당하고, 부적절하거나 더 이상 적절하지 않거나 과도한” 정보가 되는지에 대한 실시 없음
- 기준의 모호함에 사업자에게 법적 위험 회피경향이 더해지면 과소삭제의 폐해보다는 **과다삭제의 위험을 증가**하고, 과다삭제로 인한 **검색엔진의 불안정성이 심화**될 우려가 있음
- ‘이름’을 기초로 한 검색결과에서 정보주체의 선택적 삭제를 허용하는 것은 검색엔진의 검색결과에 대한 신뢰, 중립성을 훼손하는 것인데 이에 대한 고려없이 판단(검색엔진의 사회적 공기로서의 기능에 중대한 장애로 작용할 위험성)

4

이번 판결의 문제점



2 정보접근비용의 증가와 표현의 자유

- 검색결과에서 해당정보가 게시된 웹페이지 링크를 삭제함으로써 인해 해당 정보가 존재하는지 여부를 검색을 통해 손쉽게 확인할 수 없게 됨에 따라 정보접근비용 증가
- 해당정보가 존재하는지 여부를 확인할 수 없게 됨에 따라 해당정보에 관한 표현의 자유(알권리) 등이 제약되는 결과발생
- 특히 ‘이름’을 기초로 한 검색결과에서 링크를 삭제하게 됨에 따라 ‘이름’과 당해정보의 **관련성이 단절되는 효과**
 - 즉, 이 사건과 같이 ‘곤잘레스’에 관한 정보를 검색하고자 하는 경우 해당 경매정보 링크가 삭제되면, 검색하는 사람으로서의 곤잘레스와 관련이 있는 경매정보의 존재 자체를 인지할 수 없게 됨
- **원본 정보가 삭제되지 않더라도, 검색결과에서의 링크 제거만으로 해당 정보의 접근이 차단되는 효과로 인해 표현의 자유(알권리)측면에서 유효한 정보의 활용이 불가능해짐** (특정 정보의 활용을 정보주체가 차단할 수 있고, 이로 인해 적법하게 발행된 정보의 유통이 사실상 불가능해질 우려 있음)

5

이번 판결의 문제점

3 합법·정확한 정보의 유통금지로 인한 표현의 자유(알권리) 제약

- 해당 경매정보는 '곤잘레스'의 이름이 포함되긴 하였으나 신문에 합법적으로 게재된 정보라는 점에서 일반적인 명예훼손, 사생활침해 정보의 삭제와 논평평면을 달리함
- 해당 경매정보는 경매절차가 개시된 사실을 알리는 것으로 시간의 흐름에 따라 부정확해질 수 없는 정보임. 다만, 경매절차 개시 이후의 사정변경에 관한 정보를 포함하지 않는다는 점에서 사정변경에 따른 정보의 업데이트가 없어 부정확해진다고 볼 여지는 있으나 그렇다고 해도 해당 경매정보 자체가 부정확하다고 볼 수는 없음
- 합법·정확한 정보를 합법적으로 유통금지시킬 수 있게 됨에 따라 표현의 자유(알권리)를 제약할 우려 있음
- **대중의 관심이 현실화되지 않은 경우(잠재적 관심), 합법·정확한 정보의 사회적 활용가능성이 봉쇄될 우려가 큼**

6

이번 판결의 문제점

4 기업에 대한 과도한 부담, 사적 검열의 일상화

- 해당정보의 링크를 삭제할 것인지 여부를 검색엔진 운영자의 판단에 맡김
- 정보주체의 주장(삭제요청)이 과연 타당한 것인지에 대해 어떤 기준으로 판단
- 해당정보의 민감성, 해당정보의 공공성에 관한 판단이 검색엔진 운영자의 책임, 업무 경감차원에서 이뤄질 가능성 큼(이로 인해 해당정보의 민감성을 과대평가, 공공성은 과소평가될 우려)
- 검색엔진 운영자가 법적 위험을 회피하기 위한 과다삭제시 이용자의 권리를 보장할 법적 수단이 없음
- 해당 정보의 발행자가 검색엔진 운영자에게 링크를 복원시켜달라는 청구를 할 수 있을지 모호한 상황(해당 정보의 발행자에 대한 통지가 효과적으로 이뤄질 수 있을지 의문)
- **사기업에 의한 정보의 선별적 유통이 일상화되는 상황은 본질적으로 표현의 자유(알권리)에 대한 제한임**

7

합리적 정보유통방안에 관한 제언

1 불법정보의 삭제가 허용되는 상황에서, 합법정보의 합리적 삭제범위 설정을 위한 논의가 필요

- 정보주체의 권리를 침해하는 불법정보(또는 해당 링크)의 삭제는 허용
- 정보주체의 권리를 침해하는 합법정보의 존재를 인정한다면, 그 범위를 어떻게 설정할 것인지가 관건임
- 이번 EC판결과 같이 “일반대중의 압도적 관심”을 구체적 기준으로 활용하기 어려움
- 정보주체의 특성, 해당정보의 특성, 정보유통매체의 특성 등을 종합적으로 고려한 판단 기준 정립이 필요함

2 정보유통여부에 관한 판단을 사법심사로!

- 정보유통에 관한 기준은 권리충돌상황에 대한 사회적 합의의 문제
- 사회적 합의를 발견하고 구현해내는 역할을 사기업에 맡길 수 없음
- 정보유통의 문제에 관한 중립적 판단주체는 현실적으로 법원이 될 수밖에 없음
- 정보의 발행자가 참여가 보장되지 않는 상황에서 표현의 자유 보장은 불가능
- 정보주체, 해당정보의 유통에 관여한 개인이나 기관이 사법심사과정에 함께 참여할 수 있는 절차 마련이 필요함

감 · 사 · 합 · 니 · 다

토론문



정혜승 (다음커뮤니케이션 대외협력실장)

‘잊혀질 권리’에 대한 사회적 논의가 더 필요합니다.

지난 5월 13일 유럽사법재판소(ECJ)가 ‘잊혀질 권리’를 인정한 판결은 전세계적으로 ‘잊혀질 권리’에 대한 논의를 본격 촉발시켰습니다. ECJ는 판결문에서 인터넷 검색업체는 부적절하거나 시효가 지난 검색 결과물에 대해 해당 정보 주체의 요청에 따라 링크를 제거할 책임이 있다고 밝혔습니다. 이른바 ‘디지털 기록’이 평생 사람들을 쫓아다니는 것은 ‘대중으로부터 격리될 권리’, 프라이버시를 침해할 수 있다는 것이 핵심입니다.

누군가의 이름을 검색하면서, 광범위한 정보를 수집하여 프로파일링 하는 것이 기술적으로 가능해진 시대에 자기정보를 지키기 위한 방어권을 인정해준 이 판결의 의미는 작지 않습니다. 국내에서 법이 보호하는 개인정보는 “살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)”고 규정되면서, 흔히 주민등록번호 등을 중심으로 이해되지만, 다양한 정보가 종합 분석될 수 있는 시대의 개인정보 이슈는 그렇게 간단하지 않습니다.

하지만, 제프리 로슨(Jeffrey Rosen)교수는 2012년 스탠포드 법리뷰(Stanford Law Review)에서 잊혀질 권리를 적용할 때 표현의 자유를 침해할 심각한 위험이 있다고 지적했습니다. 설혹 개인에 대한 정보가 사실이라 하더라도, 당사자가 요청한다면 인터넷에서 삭제되는 것이 당연한지 의문을 제기했습니다. 로슨 교수는 해당 개인정보가 언론보도를 위한 것이거나, 예술적인 것이거나 문학적인 것이어서 허용되어야 한다는 것을 사업자 책임으로 돌릴 경우, 사업자들의 검열이 본격화될 것으로 우려했습니다. 인터넷이 더 이상 표현의 자유를 위한 중립적인 플랫폼으로 기능하지 못할 것이라는 주장입니다.

박정신 고려대 법학전문대학원 교수는 6월 9일자 경향 시론에서 다음과 같이 지적했습니다. “.. 명예훼손은 물론 사생활의 침해도 아닌 합법적인 정보를 안내하지 말라고? 이렇게 해석되는

‘잊혀질 권리’는 결국 동료들이 이미 적법하게 알고 있던 자신에 대한 진실을 국가의 힘을 빌려 동료들의 기억으로부터 삭제하겠다는 시도일 뿐이다....

유럽사법재판소 판결에 반대하는 견해를 냈던 검사장(Advocate General)의 말이 명징하다. “과거의 보도에 대해 반론을 제기하는 방식이 아니라 과거의 보도를 새로운 내용으로 교체하는 것은... 역사를 위조하는 것(falsification of history).” 일제시대 때는 친일을 했지만 지금은 마음이 바뀌어 애국하고 있다는 이유로 친일인명사전 색인에서 자신의 이름을 삭제해달라는 것과 다름아니다..”

프라이버시 보호도 중요한 가치이지만, 자칫 ‘잊혀질 권리’가 현실적으로 사실 왜곡을 가져올 수 있다는 우려입니다.

스페인의 곤잘레스 사건 이전에 가장 유명한 사건은 독일에서 벌어진 살인사건을 배경으로 합니다. 볼프강 베를레(Wolfgang Werlé)와 만프레드 라우버(Manfred Lauber)는 1990년 발터 제들마이어(Walter Sedlmayr)라는 배우를 살해한 혐의로 체포되어 1993년 유죄 선고를 받아 15년간 복역했습니다. 이들은 출소 후 위키피디아(Wikipedia)에 이 사건과 관련 기사 삭제를 요구했습니다. 2008년 1월 함부르크 법정은 이들이 이미 죄값을 치렀고, 범죄자에게도 사생활을 보호해야 한다는 이유로 원고 승소 판결을 내렸습니다. 위키피디아 독일어 사이트에서 이들의 이름은 삭제됐습니다. 반면, 위키피디아 영어판에서는 표현의 자유를 규정한 미국 수정헌법 1조를 들어 요구를 거절, 아직까지 관련 글이 남아있습니다.

(http://en.wikipedia.org/wiki/Wolfgang_Werlé_and_Manfred_Lauber) 뿐만 아니라 프라이버시 논쟁과 관련된 대표적 사례로 기술되고 있습니다. 당시 영국의 가디언은 이들의 시도가 정반대의 결과를 가져오는 ‘스트라이샌드 효과’가 나타난 사례로 보도했습니다. (<http://www.theguardian.com/technology/2009/nov/13/wikipedia-sued-privacy-claim>) 온라인에서 열심히 지우고 삭제하려고 노력할수록, 오히려 전세계적으로 유명해지고 널리 알려지는 역효과를 의미합니다. 곤잘레스 역시, 아마 프라이버시 논란에서 가장 유명한 인물이 될 것이 분명합니다. 우리는 여기서 프라이버시 보호와 표현의 자유, 어느 쪽에 무게를 둘 것인지 여부는 국가마다, 각 사회마다 다른 판단을 내릴 수 있다는 점과, 이 문제가 여전히 논쟁적인 현재 진행형 이슈라는 점을 이해해야 합니다.

국내 법은 ‘잊혀질 권리’를 이미 보장하고 있습니다.

‘잊혀질 권리’의 법률적 근거를 구하고자 할 때 ‘개인정보’를 대상으로 한다는 점에서 우선 ‘개인정보보호법’이 검토 대상이 된다는 것이 발제 내용에 포함되어 있습니다. 개인정보 자기결정권의 차원에서 개인정보보호법에서 관련 논의가 필요한 것은 타당한 지적입니다. 다만, 국내 현실에서 ‘잊혀질 권리’는 이미 정보통신망 이용촉진 및 정보보호에 관한 법률을 통해 보호받고 있습니다. 정보통신망법 제44조2(정보의 삭제요청 등)가 규정하는 ‘임시조치’는 전세계에 드문 제도입니다. 미국과 유럽 등 대다수 주요 국가에는 없는 제도입니다.

제1항은 “정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예 훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등”이라 한다)를 요청할 수 있다”고 권리침해 주장자의 권리를 보호합니다. 제2항은 “정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 게시하는 등의 방법으로 이용자가 알 수 있도록 하여야 한다”고 서비스 사업자의 의무를 명시하고 있습니다. 제1항에 따라 요청을 받을 경우, ‘삭제’ 혹은 ‘임시조치’ 둘 중 한가지 조치는 취해야 합니다. 제4항은 “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”며 ‘임시조치’에 대해 설명합니다. 이 법의 핵심은 ‘누구나’ 권리침해 신고를 할 수 있고, 이 경우, 사업자는 어떤 조치든 취해야 합니다. 현재 각 사업자들은 불법성이 명확할 경우, 곧바로 해당 게시물을 ‘삭제’합니다. 다만 명예훼손의 경우, 일개 사업자가 불법성을 판단하기 어렵기 때문에, 즉, ‘권리의 침해 여부를 판단하기 어렵거나 이해당사자 간 다툼이 예상되는 경우’에 해당되기 때문에, 복원 가능한 ‘임시조치’를 합니다. 당사자의 신고만으로 최소한 임시조치, 혹은 삭제 처리가 이뤄지도록 법에서 규정하는 것은 주요 선진국에서는 찾아보기 힘든 제도입니다.

명예훼손 자체가 판단하기 어렵다보니, 대개 권리침해 신고자들은 해당 게시물에 자신의 이름이 포함됐다는 사실만으로 문제를 삼습니다. 임시조치 남용이 사회적 논란이 되면서 한국인

터넷자율정책기구(KISO)는 2009년 공인의 경우, 공공의 알 권리를 보호하는 차원에서 해당 게시글이 명백하게 허위로 소명되지 않는한 처리를 제한하는 정책을 결정했습니다. 그러나 이는 공인에만 해당되는 것으로 이번 사건에서 곤잘레스의 경우, 그냥 민간인일 뿐입니다. 곤잘레스가 만약 국내 포털 사업자에게 같은 요청을 했다면 국내 사업자들은 위 조항에 근거해 ‘임시조치’를 해야만 합니다. 44조2는 타인의 권리를 침해하는 불법 게시물을 규율하기 위한 제도였으나, 사실상 ‘누구나 손만 들면’ 게시글 처리가 가능하도록 해준 제도입니다. 공인을 제외시킨 것은 법적 리스크를 감수한 KISO 회원사들의 선택이었을 뿐입니다.

이같은 맥락에서 국내 사업자들은 검색 제외 요청에 대해서도 법원의 판결 등 명백하게 불법이 소명된 경우, 검색결과에서 노출을 제외합니다. 1차적으로는 해당 원본 게시글이 있는 사이트에 44조의 2에 따라 처리 요청을 하도록 권해드리고 있으나, 원본 사이트가 영세하거나 연락처 자체가 어려운 경우 등에는 검색제외 방식도 가능한 절차가 마련되어 있습니다.

2013년 2월 이노근 의원이 대표발의한 ‘정보통신망법’ 개정안은 제44조2에 제 7항을 신설, “이용자가 자신의 저작물로서 정보통신망을 통하여 일반에게 공개를 목적으로 제공한 정보에 대하여 해당 정보를 취급하는 정보통신서비스 제공자에게 삭제를 요청하는 경우 정보통신서비스 제공자는 지체 없이 대통령령으로 정하는 확인 절차를 거쳐 해당 정보를 삭제하고 즉시 신청인에게 알려야 한다”고 제안했습니다.

현행 법이 사생활 침해 혹은 명예훼손 등 권리를 침해한 경우에 한하여 게시물 처리를 규정함에 따라, 개인이 자신과 관련된 내용 또는 과거 자신이 작성한 글 등에 대해서는 삭제 요구가 어려울 수 있다는 고민을 담은 내용입니다. 타당한 문제 의식에서 출발한 내용이지만, 실제 현실에서는 ‘당사자’가 내용 여부에 상관 없이 문제가 있다고 ‘손만 들면’ 처리해주는 상황입니다. 또 당사자가 쓴 저작물에 대해서는 현행 저작권법에 따라 처리가 가능합니다. 발제자께서 지적하신 바, 창작물이어야 한다는 ‘저작물’의 규정으로 인해 모두 처리 대상이 될 수는 없다는 문제가 있지만, 현실에서는 그렇게 정교하게 판단이 이뤄지지 않는 측면이 있습니다. ‘당사자’의 ‘요청’이 가장 중요한 문제로 대부분 처리됩니다. 덕분에 저작권 침해가 아닌데 무리하게 삭제됐다는 이유로 송사에 휘말려, 결국 사업자가 패소한 사례도 있습니다.

검색 사업자의 책무가 강화되는 것은 다른 부작용을 낳을 수 있습니다.

이번 판결은 ‘잊혀질 권리’에 대해 원본 게시글이 살아있더라도 검색사업자의 책무를 다르게 규정한 점이 더욱 주목됩니다. 검색 엔진의 통상적 데이터 수집, 처리를 개인정보 수집, 처리로 인정함에 따라 검색서비스 사업자에게 ‘정보 관리자’의 책임을 부여하고 있습니다. 원본 게시글이 존재하더라도, 불법 정보가 아니라 합법적인 언론 보도 내용이라고 하더라도, 검색되지 않도록 할 책무가 경우에 따라 발생하는 구조입니다.

그러나 OECD는 그동안 인터넷 업체가 각종 콘텐츠의 중간통로 역할을 하는 과정에서 불법 복제 콘텐츠가 이동하게 되지만, 정부는 이런 '중개 역할'에 대한 법적 책임을 제한해야 한다는 입장을 견지해왔습니다. 정보를 매개하고 중개하는 서비스에 대해 직접 책임을 물을 경우, 정보 유통을 제한하려는 필요성이 발생하며, 이는 사업자의 검열 논란으로 이어지기 때문입니다. 일각에서는 “주요 인터넷 기업은 관련 제도 준비 과정에서 비용 부담이 적지 않아 촉각을 곤두세우고 있다”고 보도하고 있는데, 단순히 비용 문제로만 볼 수 없습니다. 다양한 정보를 수집, 처리하는 과정 자체가 문제가 될 수 있는데, 사업자들로서는 서비스 리스크를 낮추는 방안을 모색할 수 밖에 없습니다. 아무리 합법 정보라도 검색되지 않도록 해달라, 그렇지 않으면 법적 책임을 물겠다고 하면, 정보 유통을 차단하는 편이 쉽고 타당한 결론이 될 수 있습니다.

‘잊혀질 권리’의 범위와 처리 방법 등에 대해 신중한 접근이 필요합니다.

검색서비스 사업자로서 ‘잊혀질 권리’는 어느 수준에서 보호해야 하는지, 적정한 범위가 어디까지인지는 매우 중요한 문제입니다. 일단 공공의 이익을 정의해야 할 필요가 있습니다. ‘잊혀질 권리’보다 ‘공공의 이익’이 우선시 되어야 할 사안은 어디까지 일까요. 현재 KISO는 ‘공인’이라는 기준을 중요하게 보지만, 때로는 평범한 민간인의 경우에도 ‘공공의 알 권리’가 더 가치 있는 경우가 발생합니다. 정치인의 병역비리는 공인이라서 ‘알 권리’에 해당되고 연예인의 경우는 법적으로 공인이 아니라서 상관 없을까요?

또 어느 정도의 시간이 흐르면, 잊혀져도 되는 걸까요. 특정 사건이 발생하고 0년이 흐르면, 노출하지 않는 것이 타당할까요. 1년 전이든, 10년 전이든 상관 없는 문제일까요?

이해가 상충되는 상대방이 있는 사안에 대해서는 ‘잊혀질 권리’가 어디까지 보장될까요? 예컨대 A씨와 B씨가 소송을 벌였고, 기사화됐는데, 몇 년 뒤 A씨가 정보 삭제를 요청할 경우, B씨의 의사와 상관 없이 그냥 삭제를 진행해도 괜찮을까요?

명예훼손, 사생활 침해 등 현행법 상 불법인 정보가 현재 처리되는 절차를 갖추고 있다면, 앞으로는 불법이 아닌 합법 정보도 당사자가 요청하기만 하면 모두 ‘잊혀질 권리’에 포함되는 것일까요?

잊혀질 권리의 물리적 범위는 어디일까요? 문제가 된 사안을 검색 제외 처리했는데, 계속 관련 게시물이 추가로 생성되고 이슈가 된다면 수시로 모니터링 하면서 모두 처리해야 하는 것일까요? 원본, 복사본, 2차 저작물 등 다양한 게시물에 대해 모두 같은 기준으로 처리하면 될까요?

당사자 요청과 상관 없이 해당 이슈는 절대로 잊혀져서는 안될, 기억되어야 할 문제라며 누군가 계속 게시물을 작성하여 새로 올린다면, 그 사람을 처벌할 법적 근거가 있을까요? 곤잘레스씨 사건이 프라이버시와 표현의 자유 논쟁에서 너무 중요한 문제라는 이유로 전세계에서 관련 글을 올리게 된 상황에서, 곤잘레스씨가 또다시 ‘잊혀질 권리’를 주장할 수 있을까요?

더불어, 디지털 시대의 미디어는 어떻게 정의할 수 있을까요. 발제자는 “대부분의 언론사는 ‘잊혀질 권리’의 저널리즘 영역에의 도입에 대해 부정적인 입장을 보이고 있다”고 지적했습니다. 이번 판결도 언론사 원본 기사는 보호했습니다. 그러나 지상파와 라디오, 신문과 잡지로 분류되던 미디어는 이제 누구나 올리는 유튜브 동영상, 블로그 게시글, SNS로 확장되고 있습니다. 언론사 콘텐츠는 ‘잊혀질 권리’에서 벗어나 예외적으로 보호되어야 하는 반면, 이용자들이 만드는 콘텐츠는 언제나 ‘잊혀질 권리’에 따라 삭제되는 현실의 부조리함은 사실 현재 국내에서는 ‘임시 조치’만으로도 논란이 불거진 바 있습니다.

결론

검색서비스는 사람들이 찾고자 하는 정보를 더 정확하게, 더 적합하게 찾아주기 위해 계속 진화합니다. 개인의 프로파일링 정보가 공권력이나 거대 자본에게 악용될 가능성이 우려되는 것이 사실이지만, 기본적으로는 이용자의 편의 등을 위해 온 세상 정보를 찾아주는 것이 검색 서비스의 존재 이유입니다.

국내에서는 다른 나라와 달리, 인터넷 상의 표현이 누군가의 권리를 침해할 가능성을 더 무

겹게 보고, 임시조치를 비롯해 다양한 제도적 장치를 이미 마련해두고 있습니다. 이런 제도 자체가 표현의 자유를 제약한다는 논란이 오히려 더 커지는 실정입니다. 지난해 국정감사에서 공개된 자료에 따르면, 2012년 임시조치된 게시물은 23만 건, 2013년에는 8월까지 이미 22만건에 달했습니다. 임시조치 제도는 우리 사회의 합의에 따라 도입된 제도인 동시에 전세계에 드문 제도라는 점은 여러 가지 고민을 함께 하도록 합니다.

‘잊혀질 권리’에 대해 전세계가 고민에 나선 것은 시대 변화에 따른 새로운 과제입니다. 이용자와 사업자를 비롯해 전문가 그룹에서 더 많은 논의를 통해 표현의 자유와 프라이버시 사이의 적절한 균형을 모색했으면 합니다.

토론문



구본권 (한겨레신문 사람과디지털연구 소장)

토론문은 발제문이 법 이론적 측면에서 다룬 ‘잊혀질 권리’를 좀더 포괄적 관점에서 조명하고자 한다. 디지털 환경에서 잊혀질 권리가 요구되는 배경과 이번 유럽연합 사법재판소의 판결이 인터넷 검색엔진에 끼칠 영향을 중심으로 살펴본다.

1. 인터넷 시대 ‘실질적 모호성’의 회복 시도

지난 5월 13일 유럽연합 사법재판소의 판결은 구체적으로는 검색 링크 제거다. 유럽 역내에서 서비스하고 있는 구글이라는 검색엔진이 이용자들에게 보여주는 검색 결과에서 특정한 사이트로 연결되는 링크의 제거다. 인터넷 역사에 새로운 이정표라는 평가를 받는 데는 이 판결이 유럽연합과 특정 검색엔진만이 아니라, 인터넷 환경 일반에 끼칠 영향의 지대함 때문이다.

해당 정보와 그 정보가 실려 있는 사이트의 존재 자체를 그대로 두고 이를 중개하고 실질적으로 이용가능한 형태로 서비스하는 검색엔진의 검색결과 링크 행위를 ‘삭제’하라고 판결은 곧바로 검색엔진에 대한 강력한 규제가 된다. 검색 사업자를 정보처리 사업자(data controller)로 판단해, 검색엔진이 검색로봇과 알고리즘에 의해 자동적으로 수행해온 ‘색인(indexing)’과 ‘일시 저장(caching)’ ‘순위 배열’ 기능에 대해 정보주체의 수정 및 삭제 요구를 반영하도록 한 조치이기 때문이다.

검색엔진의 인덱싱 기능은 정보가 지닌 시간과 공간의 제약을 뛰어넘어 반영구적으로 보존되고 광범한 범위에서 유통될 수 있도록 해주는 특성으로, 디지털 정보사회의 정보 유통구조를 규정하는 핵심적 요소다. 검색엔진의 인덱싱 기능은 인터넷 사용자들에게 방대한 정보에 접근할 수 있는 한편 알리고 싶지 않거나 부적절한 정보도 손쉽게 노출되는 결과를 가져왔다. 유럽연합의 최고법원이 검색엔진의 인덱싱 기능과 관련한 판결을 내림으로서, 그동안 존재하지 않았던 검색엔진의 기능 제한에 대한 판례와 법적 근거가 생겨났다.

인덱싱은 문서의 색인 기능을 통해 접근성을 높여주는 단순한 편의 제고가 아니라, 문서의 형태와 지위를 규정하는 핵심적 요소라는 논거는 미국에서 판례로 수립됐다. 1989년 미국에서는 동일한 내용이 담겨 있지만 아날로그 형태의 정보와 디지털 형태의 정보를 구별한 판결이 나왔다. 공개되어 있어도 분류되지 않은 정보는 검색가능한 디지털 정보와 근본적으로 구별된다는 논리다. 미국 연방대법원은 ‘실질적 비공개(practical obscurity)’라는 개념을 제시해, 동일한 내용이지만 오프라인의 아날로그 문서와 데이터베이스화된 디지털 문서를 구별했다.¹⁾ 연방대법원은 많은 시간과 노력을 기울여야 찾을 수 있는 법원의 개별적 재판기록과 한 번에 이를 손쉽게 찾을 수 있도록 만든 전산화된 데이터베이스는 구분해야 한다는 판결을 내려, 전산 기록에 대한 언론의 접근권을 불허했다.

미 연방대법원은 이 판결에서 일반인이 접근가능한 공공기관의 정보이지만 분류되지 않은 채 보존되어 있는 방대한 규모의 정보를 ‘실질적 비공개’ 상태의 정보라고 보아, 동일한 정보가 컴퓨터에 의해 분류되고 접근성이 높아진 데이터베이스와 다르게 보았다. 디지털 정보의 핵심적 특성이 인덱싱에서 비롯한다고 보는 관점이다. 인덱싱 기능은 그 효용을 적극 활용한 인터넷 검색엔진을 통해서 증폭되었다.

디지털 형태로 인터넷에 연결되어 있으면 존재하는 것만으로 손쉽게 검색되는 인덱싱은 디지털 이후에 비로소 본격적으로 부각되기 시작했다. 온라인 인덱싱의 편의성이 강조된 것에 비해 예상하지 못한 피해 등 부정적 측면은 사용자의 부주의나 무지로 여겨졌다. 검색엔진의 강력한 인덱싱 기능으로 인한 프라이버시 침해 등 기술이 초래한 부수적 피해에 대한 구제 절차가 확립되지 않은 상태에서 유럽 사법재판소의 판결이 만들어진 것이다.

검색엔진의 인덱싱은 인터넷에 존재하는 거의 대부분의 정보를 접근 가능하게 만들었지만, 접근 가능한(accessible) 모든 정보가 필연적으로 공적인(public) 정보인 것은 아니다.²⁾ 유럽 사

1) U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989). 미국 연방대법원은 이 재판에서 정부의 범죄자 데이터베이스 접근권을 요구한 언론의 요구를 기각했다. 언론 자유를 위한 기자평의회(Reporters Committee for Freedom of the Press)는 정보자유법(FOIA)에 근거해 일반인이 접근가능한 정부의 정보를 모아놓은 정부의 데이터베이스에 대한 접근권을 요구했으나 법원에서 인정받지 못했다. 미 연방수사국(FBI)이 구축한 범죄자 데이터베이스는 각급 법원이 공개한 재판기록으로부터 수집된 것이기 때문에 언론에 공개되어야 한다는 게 언론자유를 위한 기자평의회 논리였다.

2) 미국 미시간주 대법원은 대학 교직원들의 주소와 전화번호는 전화번호부나 웹사이트에 공개돼 있는 정보이지만 정보주체가 다른 사람에게 그 정보를 알려주는 것을 거부할 수 있다고 판결했다. 이 정보는 공개돼 있지만 특정한 맥락에서는 모호성이 유지되어야 하는 정보로, 공적인 정보가 아니라는 판결이다.

법재판소의 판결은 검색엔진을 통해 손쉽게 접근할 수 있는 정보의 속성을 ‘공적 영역(public domain)’의 정보로 보아, 링크 삭제라는 기술적 방법을 통해 해당 정보를 공적 영역에서 분리하고자 하는 판결이라고 이해할 수 있다.

2. 검색서비스 사업자의 책임 범위

유럽 사법재판소는 판결을 통해 구글 검색결과에서 정보주체의 개인정보가 담긴 정보에 연결된 링크 삭제를 판단한 근거를 제시함으로써, 검색엔진 인덱싱의 효력에 대한 판단과 함께 인덱싱 기능 제한의 조건을 명시했다.

정보주체의 삭제 요청에 대한 무조건적 수용이 아니라, 정보주체의 민감한 프라이버시에 관한 것이고, 애초 정보 수집·처리 목적에 비추어 적절성, 관련성, 과도한 처리에 해당하지 않아 함 등을 밝힌 디렉티브95 제6조의 조건이 제시됐다. 이로서 ‘잊혀질 권리’의 적용 대상과 방법이 한결 분명해졌다. 정보주체가 삭제를 요구하는 자신에 관한 모든 정보라는 광범하고 모호한 범위가 아니라, 현재 시점에서 더 이상 ‘공적인 정보로 처리되기에 부적절한 개인에 관한 정보’로 해당 정보주체가 삭제를 요청하는 정보가 대상이다. 또한 과거 신문을 디지털화해서 인터넷 서비스하는 언론사에서 해당 정보를 삭제하는 것이 아니라, 검색결과에서 해당정보를 노출하고 연결하는 링크에 대해 검색사업자가 삭제하도록 한 것이다.

유럽 사법재판소가 판결에서 정보주체의 삭제 요청이 수용될 수 있는 조건으로 디렉티브95 제6조의 요건을 제시했지만, 애초 정보 수집 목적에 비해 적절하지 않고 관련이 없고, 과도한 처리에 해당하고 정확하지 않고 최신 정보로 업데이트되지 않았음에 대한 판단은 해당 정보 삭제 요청을 알고리즘에 의해서 자동적으로 처리할 수 없는 절차임을 말해준다.

판결로 인해, 유럽연합 시민들은 검색엔진에 노출되는 자신에 관한 부적절한 정보에 대해 삭제를 요청할 수 있는 권리를 인정받았고, 검색 서비스 업체에는 과거에 없던 새로운 책무가 부과됐다. 판결 이후 독일 정부와 구글이 밝혔듯이 검색 결과 삭제 요청은 기계나 프로그램에 의해 자동적으로 처리가 아닌, 신청 사안마다 개별적 검토를 통해 처리되어야 한다.³⁾

Michigan Federation of Teachers v. University of Michigan, 481 Mich. 657, 753 N.W.2d 28 (2008).

3) 구글은 오래 전부터 이용자가 웹마스터 도구에 접속해 ‘웹페이지 제거 요청’을 할 수 있도록 허용해오

삭제 요청을 위한 절차와 그에 따른 삭제 여부를 결정하는 구조가 마련되어야 한다. 삭제 요청을 위한 절차는 구글이 2014년 5월 30일 유럽연합 시민들을 위해 만든 페이지처럼 검색업체마다 직접 제작해 운영하는 방식이 있을 수 있다. 또한 정부 산하 조직이나 제3의 독립기구의 형태로 설립해 삭제 요청들을 접수한 뒤 판단해, 검색업체에 통보할 수 있다. 두가지 방법을 절충시켜서, 1차적으로 검색업체에 접수해 처리하고 이의가 있을 경우 이를 처리하는 중재기구 형태의 구조를 만들 수 있다. 인텍싱과 일시저장 등 검색 업체의 서비스 과정에서 발생한 문제에 대한 삭제 요청인 만큼 그에 따른 비용은 우선적으로 검색 업체의 부담이 될 가능성이 크다.⁴⁾

검색 결과 삭제요청 절차보다 중요한 것은 삭제 요청이 적절한지를 판단하는 기준과 구조다.

3. 삭제 요청 정보의 적절성

판결은 디렉티브95 제6조의 요건들을 근거로 제시했지만 수집 목적에 비교해서 현재 시점에서의 적절성, 관련성, 과도하지 않음, 최신성, 정확성이라는 요소들은 구체적으로 기준을 정의하기 어렵고 개별 사안에 따라 고려할 사항이다. 인터넷에 공개되어 있고 접근 가능한 정보이지만 현재 시점에서 더 이상 공적이지 않은 개인에 관한 정보는 어떠한 종류일까를 따져볼 필요가 있다.

소송을 제기한 스페인 변호사 곤잘레스가 문제 삼은 정보는 10여년 전 신문에 실린 부채로 인한 자신의 주택 경매 정보다. 경매의 원인이 된 부채는 청산됐지만 해당 정보는 신문에 실리지 않는다. 특정 시점에서 개인의 신용상태를 알려주는 민감정보로, 법률에 의해서 공표되지만 사정이 달라지거나 일정한 기간이 지나면 더 이상 개인에게 결부돼 사용될 수 없는 성격의 정보다.

전과 기록과 신용정보 기록은 대표적으로 일정 시간이 지나면 효력을 상실하거나 삭제해서 이용되지 않도록 하는 민감정보다. 형 실효 규정에 따르면 형 집행 종료 10년 뒤에는 형이 실

고 있지만, 이는 잊혀질 권리와는 무관한 서비스, 자동화된 시스템에 의해 처리된다. 기본적으로 자신이 만들었거나 관리하는 페이지가 구글 검색결과에 노출되는 점, 구글에 저장된(cached) 페이지에 대해 삭제를 요청하는 기능이다. <https://www.google.com/webmasters/tools/removals?hl=ko&pli=1>

4) 유럽 사법재판소는 판결문(43)에서 구글 검색이 단지 인텍싱된 페이지를 연결시키는 기능만이 아니라, 이를 대가로 광고, 지불 등의 대가를 누리고 있다고 밝혔다.

효되어 전과기록이 삭제된다.⁵⁾ 또한 신용정보 주체에 불리한 정보는 그 사유가 사라지면 5년 안에 삭제하도록 규정되어 있다.⁶⁾ 미국의 공정신용보고법은 7년이 지난 신용보고에서는 개인에 대해 어떠한 불리한 정보도 사용될 수 없도록 규정하고 있다.⁷⁾ 여러 차례 논란을 거치면서 공개 대상과 방법 등이 수정되어온 성범죄자 신상공개도 유사하다. 현재는 10년까지만 특정 사이트(성범죄자 알람이)에서 공개하고 신원 인증 뒤 열람할 수 있도록 접근방법과 기간을 제한하고 있지만, 제도 도입 초기에는 각종 게시판과 관보 등 다양한 경로로 접근이 가능했다.

이처럼 한때 공개된 정보였지만, 현재 시점에서 더 이상 공적이지 않거나 유효하지 않은 정보이자 해당 정보주체에게 민감한 정보인 경우, ‘잊혀질 권리’의 우선적 대상이 될 수 있다. 오프라인에서는 한시적 공개 뒤 폐기 또는 삭제하는 정보가 온라인에서 지속 유통되고 또한 검색 엔진에 의해 인덱싱되고 일시저장되어 반영구적으로 공개되고 있다. 오프라인에서 일정 기간 동안 공적 정보 또는 접근 가능한 정보로 공개되다가 시간이 경과함에 따라, ‘실질적 비공개 (practical obscurity)’ 상태로 되어 접근이 어려운 사실상의 망각된 상태로 된 정보들이 인터넷 검색엔진을 통해 손쉽게 접근되는 현실이 된 것이다.

이번 판결은 더이상 적절하지 않은 개인의 민감정보에 대해 검색결과에서 링크 삭제를 통해 ‘실질적 비공개’ 상태의 정보로 되돌리려는, 인터넷 환경에서 의도적으로 망각을 도입하려는 시도로 볼 수 있다.

한 때 공개된 정보였으나 더 이상 ‘공적’이지 않은 개인에게 민감한 정보에 대한 판단은 나라별 법규와 관행에 따라 크게 다르다. 유럽 국가들과 달리 미국에는 보편적인 형 실효 제도가 없고 주에 따라 경범죄의 경우 전과기록 삭제 청구 재판을 할 수 있다. 미국에서는 재판 이전 혐의범 체포 사진을 찍은 ‘머그샷(mug shot)’도 공개 정보이고, 이를 모아서 인터넷에서 서비스하고 있는 사이트가 있으며 유료로 ‘삭제’ 서비스를 제공하고 있는 사업모델이 있다.⁸⁾

5) 『형 실효에 관한 법률』 제8조. 단『공직선거법』은 선거 입후보자의 금고 이상 전과기록을 선거 공보 등을 통해 유권자들에게 공개하도록 하고 있는데 실효된 형도 공개 대상에 포함시키고 있다.

6) 『신용정보의 이용과 보호에 관한 법률』 제18조(신용정보의 정확성 및 최신성의 유지).

7) Fair Credit Reporting Act : FCRA.

8) 미국 각주의 머그샷 정보를 모아서 서비스하는 www.arrests.org 이 대표적이다. www.RemoveMyMug.com 같은 사이트는 899달러에 머그샷 제거 서비스를 제공하고 있다. NewYork Times 2013.10.5. "Mugged by a Mug Shot Online".

4. 판결 이후의 과제

이번 판결은 정보의 시간적, 공간적 거리를 뛰어넘는 정보 접근 도구로 활용되어온 인터넷의 핵심적 기능에 사회적 통제가 적용된 사례로 의미가 크다. 프라이버시를 침해하는 과거 기록에 대한 인터넷 검색결과를 제한하는, 최초의 ‘잊혀질 권리’ 판결이 유럽연합 이외의 지역에서 어떻게 수용될지도 주요한 문제다.

십수년 전 신문에 실린 채무자 자산매각 공고와 같은 정보는 공개 당시 일정 기간 대중에게 이용되다가 시간이 경과하면서 ‘실질적 비공개’라는 모호성의 영역으로 옮겨졌고, 이후에는 문서보관소의 사료를 찾는 연구자 등이 상당한 시간과 비용을 들여야 접근 가능한 정보였다. 인터넷 검색엔진이 가져온 정보 검색의 편리함은 결과적으로 프라이버시 침해 정보의 검색 노출이라는 부작용도 수반했다. 최초의 ‘잊혀질 권리’ 판결은 이제껏 해결책이 없던 문제에 대한 본격적으로 사회적 통제의 길이 합법적으로 마련되었음을 의미하는 것으로 볼 수 있다.

이번 판결은 인터넷 검색결과로 인한 유사한 부작용 사례에 대한 논의로 확대될 수 있다. 소셜네트워크 상에서 자의로 혹은 제3자에 의해 노출된 사생활 정보, 미성년자 시절에 게재한 각종 콘텐츠, 전과나 신용기록 등 법에 따라 유효기간이 정해진 개인 관련 정보 등을 검색에서 삭제해야 하는지가 대상이다. 프라이버시 및 이들 정보의 공개와 관련한 규정은 국가별 법에 따라 다르기 때문에, 검색엔진 차원에서는 복잡한 문제가 된다. 검색엔진이 인터넷에 존재하는 정보를 월드와이드웹(worldwide web)에 동일하게 노출해온 검색결과에 대해 국가별로 다르게 노출해야 하는 문제가 발생하게 된다.

또한 유럽 사법재판소는 16년 전 신문의 경매정보에 대한 링크 삭제 요청을 타당한 것으로 인정하는 판결을 내렸지만, 해당 정보가 신문사처럼 표현의 자유를 인정받는 언론이 아닌 제3의 사이트에 실린 경우 원 글의 삭제 여부도 논의 대상이다.

국내에서도 논의가 필요한 문제다. 정보통신망법 제44조의2 1항과 4항은 사생활 침해 정보의 삭제 청구와 임시조치(블라인드)를 규정하고 있지만, 유럽의 판결에서 다뤄진 잊혀질 정보와는 다르다. 원래 콘텐츠가 게시된 사이트와 검색엔진에서의 검색결과 노출을 동일한 기준으로 볼 것인지의 문제도 있다. 또한 네이버와 같은 국내 검색엔진은 자신의 서버에 뉴스라이브러리와 같은 과거 신문 콘텐츠를 저장한 채 서비스하고 있어서, 검색 링크 배제가 갖는 효과도 유럽에서 구글의 경우와 다르다.

정보인권 포럼

정보통신서비스 이용과 개인정보자기결정권 보장을 중심으로

| 인 쇄 | 2014년 6월

| 발 행 | 2014년 6월

| 발행인 | **현 병 철** (국가인권위원회 위원장)

| 발행처 | **국가인권위원회 정책교육국 인권정책과**

| 주 소 | (100-842) 서울특별시 중구 무교로 6
금세기B/D (을지로1가 16번지)

| 전 화 | (02) 2125-9835 | F A X | (02) 2125-0919

| Homepage | www.humanrights.go.kr

| 인쇄처 | 도서출판 **한학문화**

| 전 화 | (02) 313-7593 | F A X | (02) 393-3016

발간등록번호 11-1620000-000460-01

사전승인 없이 본 내용의 무단복제를 금함