2012 국정감사 정책자료집

국회 행정안전위원회

행정부문 개인정보 보호의 현황과 과제

2012. 10

국회의원 진 선 미
(민주통합당)

목 차

※ 본 연구는
진선미 의원실과 이은우 변호사(민주당 추천 개인정보 보호위원회 위원), 이호중 교수(서강대학교 법학전문대학원), 장여경·정민경 활동가(진보네트워크센터)가 공동으로 수행하였음

Ⅰ. 서론

「개인정보 보호법」 시행('11.9.30) 이후로도 1년 동안 전 국민의 절반 이상의 개인정보가 유출된 것으로 나타났다.[1] 행정안전부가 제출한 '개인정보 유출신고 접수현황'에 따르면, 개인정보 보호법이 시행된 작년 10월부터 올해 8월까지 7개 회사에서 총 2,659만 명의 각종 개인정보가 해킹이나 직원부주의로 유출되었다. 이는 우리나라 총인구(2010년말 4,941만명)의 절반이 넘는 55.4%에 해당한다.

개인정보 유출사고가 끊이지 않으면서 이로 인한 개인정보침해 신고도 크게 늘어났다. 개인정보침해센터 신고처리 현황에 따르면, '07년도에 847건의 개인정보 침해신고가 있었으나 '11년에는 그 3배가 넘는 2,556건의 신고가 접수되었다. 신고된 내용 중 각 12.1%는 사실 조사 불가로, 2.5%는 법 위반 사항 없음으로 처리되었으며 수사기관 이첩도 0.8%에 불과하여 개인정보 침해에 대한 국민의 법 감정과 그 실제 운용 사이에 큰 괴리가 있음을 보여 준다.

<표 Ⅰ-1> 최근 5년간 개인정보침해센터 신고 처리현황

처 리 내 역	2007년	2008년	2009년	2010년	2011년	'12.7월	합계(%)
고 충 해 결	289	445	1,495	1,162	2,107	449	5,947 (63.9)
분 쟁 조 정	90	172	145	191	126	71	795 (8.5)
수사 기관 이첩	18	25	16	5	13	0	77 (0.8)
행정 기관 이첩	31	37	41	10	20	62	201 (2.2)
법위반 사항 없음	53	62	10	47	54	2	228 (2.5)
사실 조사 불가	155	175	329	247	156	69	1,131 (12.1)
피해구제 신청 철회	211	72	103	126	80	40	632 (6.8)
처 리 중	-	-	-	-	-	300	300 (3.2)
합 계	847	988	2,139	1,788	2,556	993	9,311

1) 2012년 국회 행정안전위원회 국정감사 진선미 의원 보도자료(2012.9.17).

공공기관과 민간업체가 보유한 개인정보의 대량 유출사고를 막기 위해 개인정보 보호법이 제정되고 대통령 소속의 개인정보 보호위원회도 출범한지 1년이 흘렀지만, 전혀 달라진 것이 없다.

많은 공공·민간기업들이 여전히 회원가입시 주민번호와 전화번호 등 개인정보 입력을 요구하고 있고, 홈페이지 회원을 탈퇴해도 개인정보를 삭제·파기하지 않고 그대로 남겨 두거나, 개인정보 보유기간을 경과해도 파기시키지 않는다.[2] 수집된 개인정보는 자신도 모르게 이용되고 있다. 행정안전부가 진선미 의원에게 제출한 '최근 4년간('09~'12.8) 개인정보 초과보유로 행정처분을 받은 현황'에 따르면, 총 20개 민간·공공기관이 개인정보 삭제의무를 위반했거나 보유기간을 초과보유하다 행정안전부의 기획조사에 적발되어 과태료나 개선권고 처분을 받은 것으로 나타났다.

특히 공공기관의 실태가 민간 못지 않게 심각한 것으로 드러났다. M기관은 2011년에 20개 파일의 474백만 건의 개인정보를 보유기간을 초과 보유하다 적발되었고, Q기관도 지역가입자 부과내역 등 보유기간이 경과된 12개 파일 166백만여건의 개인정보를 초과보유하다 적발됐다. 최근 5년간 공공기관에서 개인정보 보호법 위반을 이유로 징계받은 건수도 상당하다.[3]

<표 Ⅰ-2> 최근 5년간 개인정보 보호법 위반 공직자 징계현황

(단위 :명)

구분	국가행정기관	교육기관	자치단체	기타공공기관	계
계	39	149	47	154	389
'06년	4	0	7	11	4
'07년	0	45	2	8	45
'08년	13	61	22	89	74
'09년	17	26	15	23	43
'10년	5	17	1	23	22

구분	징계처분 인원						
	소계	파면	해임	정직	감봉	견책	경고등
계	389	6	6	15	21	29	312
'06년	0					12	10
'07년	1			1		1	53
'08년	17	1	1	4	11	7	161
'09년	18	2	5	5	6	8	55
'10년	12	3		5	4	1	33

2) 2012년 국회 행정안전위원회 국정감사 진선미 의원 보도자료(2012.10.04).
3) 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료.

이렇게 적발된 기관이나 사람은 빙산의 일각일 수 있다. 국민들은 특정한 목적 하에서 자신의 개인정보가 기관에 제공되더라도 그 목적에 따른 처리가 끝나면 안전하게 파기될 것으로 기대하고 있는 바, 개인정보처리자가 정보주체의 의사와 무관하게 개인정보를 계속 보유하고 활용하는 것은 개인정보에 대한 자기결정권을 침해하는 행위이다.

헌법재판소는 2005년 개인정보 자기결정권에 대하여 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다."고 설시한 바 있다.[4] 헌법재판소는 "[컴퓨터를 통한 개인정보의 데이터베이스화가 진행되면서] 오늘날 현대사회는 개인의 인적 사항이나 생활상의 각종 정보가 정보주체의 의사와는 전혀 무관하게 타인의 수중에서 무한대로 집적되고 이용 또는 공개될 수 있는 새로운 정보환경에 처하게 되었고, 개인정보의 수집·처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대되어 국가가 개인의 일상사를 낱낱이 파악할 수 있게 되었다"고 경고하며, "이와 같은 사회적 상황 하에서 개인정보자기결정권을 헌법상 기본권으로 승인하는 것은 현대의 정보통신기술의 발달에 내재된 위험성으로부터 개인정보를 보호함으로써 궁극적으로는 개인의 결정의 자유를 보호하고, 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 필요한 최소한의 헌법적 보장장치"라고 지적하였다. 즉, 개인정보자기결정권은 개인에게 자신에 관한 정보의 공개와 이용에 대하여 원칙적으로 스스로 결정할 권한을 보장하고 있으며, 현대적인 정보처리기술의 조건 아래서는 국가 등 공권력에 의한 개인정보의 무제한적 수집, 저장, 이용 및 교부에 대하여 개인을 보호할 것이 요구된다는 것이다.

개인정보의 무단 수집과 이용을 방관하는 것은, 그 정보에 기초한 사람의 분류, 낙인, 차별을 고착화시키는 결과를 낳을 수도 있다. 개인정보 데이터베이스에 실현되어 있는 한 개인의 정보가 그에 대한 행정서비스와 고객서비스의 수준을 결정하기 때문이다. 정보사회에서는 개인의 사회적 정체성이 디지털화된 개인정보에 의해 좌우될 위험성이 상존하고 있다. 일례로, 잘못된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동에 미치는 위험성은 지대할 뿐만 아니라, 나아가 개인의 인격 자체에도 치명적인 위해를 가할 수 있다.[5] 더 나아가 개인정보를 축적·처리하는 공·사의 기관은 개인에

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

대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이 된다. 그리하여 이들 개인정보를 토대로 일정 부류의 사람들을 사회적으로 낙인을 찍는 일(예컨대, 신용불량자나 취업기피인물명단의 작성·유통)이 얼마든지 가능해지게 되고, 그 결과 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다.[6)]

개인정보자기결정권은 단순히 타인에 의한 개인정보의 취급을 억제하는 이외에도 개인이 자신에 관한 정보의 유통을 적극적으로 형성하고 조절한다는 측면에서 이해될 수 있다. 여기서 개인정보자기결정권의 적극적 측면은 대단히 중요하다. 오늘날 대부분의 개인정보가 자신도 모르게 처리되는 현실 속에서 정보주체가 이 유통 과정에 개입하기 위해서는 적극적인 권리를 완전히 인정받을 수 있어야 하기 때문이다. 컴퓨터나 전산망 등을 통한 개인사생활감시와 개인정보침해는 언제, 어디서 무엇이 얼마만큼 침해되고 있는지를 전혀 또는 거의 모르고 있다가 침해되었다는 사실을 알게 되면 그 구제가 사실상 거의 불가능하다는 특징을 갖고 있다. 특히 컴퓨터에 의한 자동정보처리는 공간적으로 떨어져 있는 다른 정보에 순식간에 접근할 수 있게 하였으며, 그 결과 정보가 원래 저장되었던 목적과는 다른 목적으로 이용될 위험성 및 자동 정보결합 가능성이 높다.[7)] 개인정보 수집과 처리를 위한 정보시스템은 갈수록 막대한 자원이 투입되는 거대 기술 구조물이기 때문에, 도입 이후 개인정보자기결정권이 침해되는 상황이 발생한다 하더라도 정보주체가 이를 중단시키기가 어렵다. 따라서 개인정보 수집 단계에서부터 그 목적을 명확히 한정하고, 개인정보의 처리 방법 및 종류에 있어서 목적 내 필요 최소한의 개인정보를 수집하고 이용하도록 한정하며, 목적 외 이용을 제한할 수 있는 법적·기술적 조치가 준비되어 있어야 하는 것이다.

이와 같은 개인정보에 대한 정보주체의 권리는 국제 규범 및 입법에 있어서 원칙으로 인정받아 왔다. 개인정보 보호에 대한 최초의 국제규범인 1980년 OECD 「개인정보 보호 가이드라인」[8)] 뿐 아니라 1990년 UN의 「전산처리된 개인정보파일의 규제에 관한 지침」[9)] 및 1995년 EU 「개인정보 보호에 관한

5) 이인호, 2001, “개인정보자기결정권의 한계와 제한에 관한 연구”, 「개인정보연구」 01-01, 한국정보보호진흥원.
6) 성낙인·이인호·김수용·권건보·김삼용·이지은·김주영·손형섭·박진우·김송옥, 2008, “개인정보 보호법제에 관한 입법평가”, 현안분석 2008-45, 한국법제연구원.
7) 장진숙, “행정정보 공동이용과 정보인권 : 자기정보관리통제권을 중심으로”, 인권복지연구 제6호, 2010.
8) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.
9) Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990.

유럽의회와 각료회의 지침」[10]에서도 확인되고 있다.

우리나라의 경우에도 정보주체의 권리는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, (구)「공공기관의 개인정보 보호에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」, 「위치정보의 보호 및 이용 등에 관한 법률」 등 관련 법률에 원칙으로 포함되어 왔다. 특히 2011년 9월 30일부터는 개인정보 보호법이 제정 시행되고 있다. 본래 공공부문은 (구)「공공기관의 개인정보 보호에 관한 법률」, 정보통신 부문은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 영역별 법률에 의해 나누어 규율되어 왔으나, 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화할 필요성이 제기됨에 따라 개인정보 보호법이 제정된 것이다. 이 법의 제정은 1997년 통합전자주민카드 반대 운동과 2003년 교육행정정보시스템 반대 운동 등 개인정보 보호와 관련한 사회적 논란이 불거질 때마다 인권시민단체가 요구해 왔던 바였다.

우리나라에서 개인정보를 가장 많이 보유한 자는 아마 정부일 것이다.[11] 그러나 우리는 주로 정보의 이용 및 공유 때문에 발생하는 개인정보의 침해 문제보다는 정보의 이용이나 공유의 긍정적인 측면에 보다 관심을 기울여왔다. 컴퓨터 및 전산망 시스템의 구축으로 행정서비스가 보다 신속하고 효율적으로 수행될 수 있다는 사실은 부인할 수 없으나, 행정의 효율이란 명목 아래 국민들의 개인정보에 대한 권리가 과도하게 제한되는 일은 없어야 할 것이다. 특히 행정정보로 활용되는 개인정보를 공공기관에서 관리하는 경우, 개인정보의 질이 확보되지 못하면 의사결정의 오류가 발생하고 컴퓨터나 전산망 등을 통한 정보처리는 과거보다 그 오남용 소지가 커지는 등 정보주체의 기본권을 중대하게 제약할 수 있다. 이에 최근 변화를 맞고 있는 법제도적 환경 속에서 행정부문 개인정보 보호의 현황을 살펴보고, 그 개인정보 이용이 개인정보자기결정권과 조화를 이루는 방안을 모색해 보고자 한다.

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

11) 장교식·조정은, “행정정보통신망 이용에 따른 개인정보침해에 관한 고찰”, 토지공법연구 제51집 2010년 11월.

Ⅱ. 경찰 작용과 개인정보 보호

1. 치안정보 일반

가. 문제 제기

2011년 초 경찰의 범죄정보관리시스템(CIMS : Crime Information Management System)에 의한 개인정보의 수집·저장이 정보의 자기결정권에 대한 불법적 침해라는 문제를 제기하면서 국가배상을 구하는 소가 제기되었다. CIMS는 경찰의 사건관리, 범죄통계 및 지도분석, 수법영상정보, 전자결재, 업무관리, 여죄추적 기능 등이 하나로 통합된 종합적인 정보시스템으로 2004년에 도입되었으며, 2010.5.1. 「형사사법절차 전자화 촉진법」이 시행됨에 따라 현재는 동법이 규정한 형사사법정보시스템(KICS : Korea Integrated Criminal System)으로 대체되어 운영되고 있다.

2011.8.12. 제1심 판결문[1]은 개인정보자기결정권은 헌법 제37조 제2항에 의한 법률유보의 원칙에 의하여 제한이 가능하며, 「공공기관의 개인정보보호에 관한 법률」 제5조는 공공기관이 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있도록 허용하고 있고, 경찰법 제3조 및 경찰관직무집행법 제2조는 '범죄의 예방·진압 및 수사', '치안정보의 수집'을 경찰의 임무로 규정하고 있다는 점에서 법률유보의 원칙에 위반한 것이 아니라고 판시하였다. 또한 2010.5.1. 「형사사법절차 전자화 촉진법」이 시행된 이후에는 동법 제5조가 법적 근거가 된다고 하였다. 또한 「공공기관의 개인정보보호에 관한 법률」 제11조, 제23조 및 「형사사법절차 전자화 촉진법」 제14조, 제15조의 의하여 개인정보의 수집과 이용은 필요한 최소한도의 범위에서 할 수

1) 2011.8.12. 서울중앙지방법원 2010가단315870.

있다는 점에서 과잉금지원칙에 위배되는 것도 아니라고 한다.

CIMS 사례에서 보듯이, 현재 경찰의 개인정보 수집은 경찰법 제3조, 「경찰관직무집행법」(이하 '경직법') 제2조 그리고 「개인정보 보호법」 제15조(종래에는 「공공기관의 개인정보보호에 관한 법률」 제5조)에 의하여 포괄적으로 승인되고 있는 상황이다. 이러한 법상황은 개인정보자기결정권을 지닌 개인의 입장에서 어떠한 개인정보가 어떻게 수집되고 관리되는지를 전혀 알 수 없고 개인정보의 수집 및 처리에 대한 통제권도 전혀 확보될 수 없다는 점에서 심각한 기본권침해를 용인하는 결과에 이르게 된다.

우리나라의 개인정보 보호법제가 전반적으로 미흡한 상태에서 특히나 경찰의 정보수집활동에 대해서는 아무런 법치주의적 통제가 작동하지 못하는 상황이다.

나. 경찰의 개인정보 수집 및 처리 양태

1) 경찰의 개인정보 수집

경찰의 정보활동은 경찰이 경찰활동의 목적을 위하여 특정한 자연인에 관한 개인정보를 수집하고 처리하는 모든 활동을 말한다. 계속 사용을 목적으로 한 모든 의식적인 개인정보의 인지와 수록이 수집에 해당하고, 개인정보의 저장 및 전산화, 그리고 타 기관에의 정보제공은 개인정보의 처리에 해당한다.

경찰관직무집행법 제2조는 "치안정보의 수집·작성 및 배포"를, 경찰법 제3조는 "치안정보의 수집"을 경찰의 직무로 규정하고 있으나 '치안정보'란 치안목적으로 수집, 처리되는 모든 정보를 의미하기 때문에 그 범위를 한정짓기는 매우 어렵다. 경찰의 정보활동을 크게 나누면 범죄수사를 위한 정보활동과 위험예방 업무를 위한 정보활동으로 구분할 수 있다.

• 수사 관련 정보수집 - 피의자통계원표, 범죄수법원지, 수배요구서 등 지명수배 관련 정보수집, 범죄경력관리를 위한 수사자료표, 유치인 명부, 피의자신문조서 등 수사서류 등등

• 정보부서의 정보수집활동 - 「경찰청과그소속기관등직제」와 「경찰청과그소속기관등직제시행규칙」에 규정된 정보부서는 경찰의 '위험예방' 업무을 위한 정보수집을 담당하고 있다. 경찰청 정보국의 구성과 임무는 아래 표와 같다.

<표 Ⅱ-1> 경찰청 정보국의 구성과 임무

관련규정	담당부서	담당업무
「경찰청과그 소속기관등직제」 제14조	정보과장 | 기획정보심의관	1. 치안정보업무에 관한 기획·지도 및 조정 2. 정치·경제·노동·사회·학원·종교·문화 등 제분야에 관한 치안정보의 수집·종합·분석·작성 및 배포 3. 정책정보의 수집·종합·분석·작성 및 배포 4. 집회·시위등 집단사태의 관리에 관한 지도 및 조정 5. 신원조사 및 기록관리
「경찰청과그 소속기관등직제시행규칙」 제11조	정보1과	1. 정보경찰업무에 관한 기획·지도 및 조정 2. 신원조사 및 기록관리 3. 기타 국내 다른 과의 주관에 속하지 아니하는 사항
	정보2과	1. 삭제 <2004.12.31> 2. 치안정보업무에 관한 기획·지도 및 조정 3. 정책정보의 수집·종합·분석·작성·배포 및 조정 4. 삭제 <2004.12.31>
	정보3과	1. 정치·경제·노동분야에 관련되는 치안정보의 수집·종합·분석·작성 및 배포 2. 정치·경제·노동분야에 관련되는 집회·시위 등 집단사태의 관리에 관한 지도 및 조정
	정보4과	1. 학원·종교·사회·문화분야에 관련되는 치안정보의 수집·종합·분석·작성 및 배포 2. 학원·종교·사회·문화분야에 관련되는 집회·시위 등 집단사태의 관리에 관한 지도 및 조정

2) 일반 시민들에 관한 개인정보의 수집과 처리

가) 주민등록정보의 DB화

모든 국민은 만 17세가 되면 주민등록법 제7조에 따라 주민등록증발급신청서를 작성해야 한다. 이 신청서에는 성명, 주소, 본적, 직업, 세대주, 혈액형 등 개인 신상에 관한 기본적인 정보가 기재되어 있으며, 사진과 열손가락 지문이 첨부된다. 신청서 원본은 일괄하여 경찰청으로 송부되어 경찰청이 보관하고 있으며, 경찰청은 이 정보들을 전산입력하여 DB화함으로써 신원확인 등의 목적에 활용하고 있다.

나) 운전면허 응시정보의 수집과 관리

자동차운전면허를 취득하기 위하여 작성하는 응시원서에는 성명, 주소, 보유면허, 장애인여부, 색맹여부, 신체검사결과, 병력 등 기본정보를 기재해야 하고 사진을 첨부해야 한다.[2] 이러한 정보들은 경찰청 소속 운전면허시험관리단에서 전산입력하여 DB화하고 있다.

다) CCTV

경찰은 방범용, 교통법규위반단속용 등의 목적으로 다수의 CCTV를 설치하여 운영하고 있다. 교통법규위반을 단속하는 CCTV는 과속이나 신호위반 등 교통법규 위반차량을 단속하기 위한 것으로 운전자의 얼굴을 인식할 수 있다. 방범용 CCTV는 골목길 등 공공도로에 범죄예방을 목적으로 설치된 것을 말한다. 사람을 대상으로 하여 녹화하며 그 영상정보의 DB는 옷색깔 등의 검색조건에 의하여 검색이 가능할 정도로 발전되어 있다. 그 외에도 수배차량감시용 CCTV, 교통흐름조사용 CCTV 등도 운영하고 있다.

법적 근거는 다음과 같다.

개인정보 보호법
제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

3) 범죄관련 개인정보의 수집과 관리

가) 수사자료표

수사자료표는 일선 수사기관이 피의자의 성명, 주소, 주민등록번호, 본적, 입건내역, 특기사항, 사건번호 등을 기재하고 피의자의 지문을 채취한 것으로 경찰청에 송부하여 경찰청이 일괄 관리한다.[3] 이 수사자료표는 검찰에서 전송해

2) 도로교통법 시행규칙 제57조
3) 형의 실효에 관한 법률 제2조 제4호.

주는 형처분결과와 연계되어 전과자료를 구성하게 된다. 수사자료표 상의 자료는 처분결과의 경중에 따라 범죄경력자료와 수사경력자료로 구분된다.[4)]

통상 일선 경찰관서에서는 사건을 검찰에 송치할 때 범죄경력조회·수사경력조회서를 첨부하는 것이 일반적이다.

나) 범죄수법 원지 등에 의한 정보수집

다) CIMS와 KICS

일선 경찰관서는 고소인, 진정인, 피의자, 피진정인 등의 성명, 주민등록번호 등 인적사항, 범죄사실, 피의자신문조서·진술조서 등 각종 조서, 수사보고, 의견서, 송치서 등 범죄사건과 관련한 개인정보와 각종 수사 관련 내용들을 CIMS에 입력하고 있으며, 이는 실시간으로 경찰청으로 송부되어 관리되고 있다.

<표 Ⅱ-2> CIMS·KICS 수집 및 보관 개인정보 현황(구축 후 연도별)

구 분		2004	2005	2006	2007	2008	2009	2010	2011	2012. 8. 31. 현재
계		4,713,341	4,552,584	4,041,362	4,255,325	4,967,563	5,171,183	4,855,317	5,093,051	3,430,034
피의자	입건	2,670,324	2,411,564	2,167,389	2,272,224	2,613,894	2,607,754	2,192,315	2,085,418	1,321,891
	불입건	121,632	132,498	93,544	98,004	134,036	175,621	277,773	323,712	215,388
피해자		1,847,360	1,899,621	1,651,164	1,617,032	1,858,181	1,971,646	1,842,464	1,972,974	1,401,919
참고인		74,025	108,901	129,265	268,065	361,452	416,162	542,765	710,947	490,836

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료
* 불입건 피의자란 내사종결된 피진정인, 피내사자를 의미함.

4) 형의 실효에 관한 법률 제2조
5. "범죄경력자료"란 수사자료표 중 다음 각 목에 해당하는 사항에 관한 자료를 말한다.
가. 벌금 이상의 형의 선고, 면제 및 선고유예
나. 보호감호, 치료감호, 보호관찰
다. 선고유예의 실효
라. 집행유예의 취소
마. 벌금 이상의 형과 함께 부과된 몰수, 추징(追徵), 사회봉사명령, 수강명령(受講命令) 등의 선고 또는 처분
6. "수사경력자료"란 수사자료표 중 벌금 미만의 형의 선고 및 검사의 불기소처분에 관한 자료 등 범죄경력자료를 제외한 나머지 자료를 말한다.

이 시스템을 이용하여 신원종합검색, One-Call 검색, 전자지도를 이용한 범죄분석, 각종 영상정보 등을 검색이 이루어진다.

• 신원종합검색 - 경찰청의 시스템실에서 주민조회가 가능한 단말기를 통해 주민정보(성명, 주민번호, 주소, 본적, 전입일, 세대주, 수배여부 등), 유치인정보(입건관서, 죄명, 영장발부일자, 체포일시, 입감일시, 입감근거, 출감일시, 출감근거 등), 수용자정보(죄명, 공범, 재소일, 재소기관, 입소사유, 출소일, 출소기관, 출소사유 등), 변사자정보, 182사람찾기정보를 조회할 수 있다.

• One-Call 검색 - 피의자, 피해자, 참고인과 관련된 주민정보(성명, 주민번호, 주소, 본적, 전입일, 세대주, 수배여부 등), 십지지문, 수배정보, 운전면허정보, 차적정보, 유치인정보, 수법자료 등을 종합적으로 검색할 수 있다.

• 수사종합검색시스템(CRIFISS) - 수사종합검색시스템(CRIFISS)은 범죄정보관리시스템과 연계되어 수법원지를 기반으로 한 데이터베이스의 검색을 지원하며, 범죄수법, 신체특징, 성명 등을 조회할 수 있으며, 수법원지에 첨부된 사진과 필적을 데이터베이스화하고 있기에 목격자, CCTV 등 자료에 의하여 범인의 얼굴을 확인한 경우나 협박편지 등을 통해 필적을 확인한 경우에는 조회를 통하여 범인을 찾을 수 있다. 또한 범죄정보관리시스템과 연계되어 있기에 십지지문, 수용자정보, 수배정보 등 광범위한 개인정보를 찾을 수 있다.

다. 문제점

1) 개인정보에 대한 자기결정권과 법률유보의 원칙

오늘날 헌법적 기본권으로 승인되고 있는 개인의 자기정보통제권은 타인이 자신에 관한 정보를 수집하고 보유·처리·사용하는데 대하여 각 개인이 정보주체로서 통제권 내지 지배권을 가지고 있음을 의미한다. 주민등록법상 지문날인제도에 대한 위헌확인 사건[5] 등에서 헌법재판소는 '개인정보자기결정권'을 헌법상의 독자적인 기본권으로 인정하였다. 헌재에 의하면, 개인정보자기결정권이란 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보

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

의 공개와 이용에 관하여 스스로 결정할 권리"이다. 그리고 개인정보자기결정권의 보호대상이 되는 '개인정보'는 "개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보"를 말하고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다고 한다.

헌법재판소도 분명히 지적하고 있듯이, 개인정보자기결정권은 각 개인에게 자신에 관한 정보의 공개와 이용에 대하여 원칙적으로 스스로 결정할 권한을 보장하는 것이기 때문에 "개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다."

2) 두가지 문제지대

첫째, 경찰의 개인정보 수집·처리 등은 개인정보자기결정권에 대한 제한에 해당하므로, 헌법 제37조 제2항의 법률유보원칙에 따라 법률적 근거를 갖추고 있는가 하는 점이다.

둘째는 경찰의 개인정보 수집 및 처리에 대하여 향후 보다 명확한 법률적 근거가 갖추어진다는 전제에서, 그렇다면 경찰활동의 일환으로 개인정보의 수집과 처리는 어떤 조건 하에서 정당화될 수 있으며 그 범위와 한계는 어디까지인가 하는 점이다. 이는 신자유주의 하에서 '위험예방'을 근거로 하여 경찰권이 계속해서 확장되어야 가는 경향을 비판적으로 제어한다는 문제의식 속에서 논의되어야 한다.

라. 독일 경찰법상 정보수집 및 처리

1) 독일 경찰법의 변화

독일 연방헌법재판소가 인구조사법의 인구조사에 대해 개인정보자기결정권을 침해하는 것이라는 위헌결정[6]을 한 후, 독일에서는 국가의 정보수집 및 처리에 관하여 상세한 법규정을 두고 있으며, 경찰의 정보수집에 대해서도 마찬가지이

6) BVerfGE 65, 1 (1983.12.15.)

다. 독일의 경우 각 주마다 독자적인 경찰법을 갖고 있는데, '통일경찰법모범초안에 대한 개정초안(VE MEPolG : Vorentwurf zur Änderung des Musterentwurf eines einheitlichen Polizeigesetzes des Bundes und der Länder)'이 그 입법지침 내지 모델로서의 역할을 하고 있다.

독일 연방헌법재판소의 인구조사결정이 있기 전까지 독일 각 주의 경찰법은 경찰직무에 관한 일반적인 조항만을 두고 있었을 뿐, 경찰의 직무활동으로서 정보수집에 관하여 구체적인 수권규정을 두고 있지 않았다. 현재 우리나라 경직법 제2조 내지 경찰법 제3조와 유사한 상황이었다. 그러나 독일 연방헌법재판소의 인구조사결정에 따르면, 경찰법상의 일반조항만으로는 경찰의 개인정보수집 및 처리의 법적 근거가 충분히 정립된 것으로 볼 수 없다는 점이 분명해졌다. 그리하여 '통일경찰법모범초안에 대한 개정초안'은 경찰의 정보수집 및 처리에 관한 명문의 수권규정을 추가하였으며, 이에 따라 독일의 모든 주의 경찰법은 정보수집 및 처리에 관한 수권규정을 두고 있다.

'통일경찰법모범초안에 대한 개정초안'의 내용을 중심으로 경찰의 정보수집과 처리에 관해 개략적으로 살펴보면 다음과 같다.

2) 경찰 직무규정의 확대와 정보수집권한

사실 독일의 '통일경찰법 개정초안'은 경찰이 기존에 행해왔던 정보수집활동의 기본권침해성을 비판적으로 성찰하고 경찰의 개인정보수집활동을 필요최소한도의 범위로 한정하고자 하는 문제의식을 담고 있는 것은 아니다. '통일경찰법 개정초안'은 그 당시까지 경찰이 행한 정보수집활동의 필요성을 전제로 하여 법률유보의 원칙에 따라 그 법적 근거를 명확히 해야 한다는 목표에 주안점을 두고 있다.

독일의 '통일경찰법 개정초안'은 종래 경찰직무를 규정한 모범초안 제1조 제1항("경찰은 공공의 안전이나 질서에 대한 위험을 방지할 임무를 지닌다.")에 제2문을 다음과 같이 추가하였다 : "경찰은 이러한 임무의 범위 내에서 또한 범죄행위의 소추를 위하여 대비하고 범죄를 예방하며(예방적 범죄투쟁) 장래의 위험을 방지할 수 있도록 준비해야 한다(위험방지를 위한 준비)."[7] 더 나아가

7) §1 I VEMEPolG: Die Polizei hat die Aufgabe, Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren. Sie hat im Rahmen dieser Aufgabe auch für die Verfolgung von Straftaten vorzusorgen und Straftaten zu verhüten (vorbeugende Bekämpfung von Straftaten) sowie Vorbereitungen zu treffen, um künftige Gefahren abwehren zu können (Vorbereitung auf die

서 ‘통일경찰법 개정초안’ 제1a조는 위와 같은 예방적 경찰활동에 대해서는 보충성원칙이 적용되지 않는다고 규정하였다.[8)]

경찰의 직무범위에 관하여 예방적 경찰활동 규정을 추가한 것은 경찰의 정보활동이 ‘구체적 위험’의 전단계에서 주로 행해진다는 점을 고려하여 경찰의 직무범위를 확장한 것이다. 개인정보의 수집과 처리에 관한 수권규범이 경찰법에 명확하게 규정되어야 한다는 것이 연방 헌법재판소의 인구조사 결정의 취지라면, ‘통일경찰법 개정초안’은 경찰의 정보활동에 관한 구체적인 수권규정을 도입하는 것에 조응하여 경찰의 그러한 정보활동을 정당화하는 직무규범의 개정을 함께 추진했던 것이다.

3) 구체적인 규율

가) 경찰의 개인정보 수집 및 처리

1986년의 ‘개정초안’은 주경찰법상 개인정보의 수집과 처리에 관한 권한을 가능한 한 통일적으로 규율하기 위하여 비교적 상세한 수권규범을 규정하고 있다. ‘개정초안’은 제8조의 일반수권조항에 연이어 경찰의 개인정보수집 및 경찰감시(polizeiliche Beobachtung)에 관한 4개의 조문을 추가하였다(제8a조 내지 제8d조). 그리고 제10조의 감식(erkennungsdienstliche Maßnahmen)에 관한 규정 뒤에 개인정보의 저장·변경·이용 및 제공 등에 관한 8개의 조문을 두고 있다.

(1) 경찰의 정보수집

○ 경찰의 일반적인 정보수집

• ‘개정초안’ 제8a조 제1항에 의하면, 경찰은 ‘위험을 방지하기 위하여 혹은 사적 권리의 보호[9)] 내지 다른 기관의 집행을 원조하는 임무를 수행하기 위

Gefahrenabwehr).

8) §1a VEMEPolG: Die Polizei wird außer in den Fällen des §1 Abs. 1 Satz 2 nur tätig, soweit die Abwehr der Gefahr durch andere Behörde nicht oder nicht rechtzeitig möglich erscheint. (경찰은 제1조 제1항 제2문의 경우를 제외하고는 위험의 방지가 다른 행정관청에 의하여 불가능하거나 적시에 가능하지 않은 경우에 한하여 직무를 수행한다.)

9) 독일의 경찰법상 사적 권리의 보호는 경찰의 통상적인 임무는 아니다. ‘법원의 보호를 적시에 받을 수 없고, 경찰의 도움 없이는 권리의 실현이 좌절되거나 현저히 어려워지는 경우’에 한하여 경찰의 임무범위에 포섭될 뿐이다. 개정초안 제1조 (2) 참조.

하여 필요한 범위에서' 위험책임자, 일정한 요건을 충족하는 비책임자, 그리고 위험에 처한 자라든가 실종자, 부상자, 증인, 신고인에 관한 개인정보를 수집할 수 있다.

• 또한 경찰은 '예방적 범죄투쟁을 위하여 필요한 경우에는' 장래에 범죄를 저지를 것으로 의심되는 자, 그와 접촉하거나 동반하는 자, 범죄피해를 당할 것으로 우려되는 자, 증인 등에 관한 개인정보를 수집할 수 있다(동조 제2항). 이 경우 예방적 범죄투쟁을 위한 정보수집의 필요성은 '사실적 근거'에 입각하여 경험칙에 의하여 판단되어야 한다.

• 이처럼 '예방적 범죄투쟁'을 위한 정보수집은 구체적인 위험의 방지를 요건으로 하지 않으며, 범죄행위의 구체적인 위험이 발생하기 전단계에서 경찰의 정보수집을 합법적으로 승인해 주는 근거규범의 역할을 하고 있다.

• 그 외 개정초안은 경찰이 '위험방지의 준비를 위하여 필요한 경우'에 일정한 자에 관한 인적 정보를 수집할 수 있다고 규정하고 있다(동조 제3항).

○ 공개된 행사나 집회, 모임에서의 정보수집

• '개정초안' 제8b조는 공개된 행사나 모임, 집회에서의 정보수집에 관한 규정을 특별히 마련하고 있다. 독일 집회법(Versammlungsgesetz) 상의 집회·시위에 대해서는 집회법 제12a조 및 제19a조에 경찰의 채증(촬영 및 녹음)에 대한 구체적인 근거규정을 두고 있으며, '통일경찰법 개정초안' 제8b조는 집회법의 적용을 받지 않는 공개된 행사나 모임에서 경찰의 정보수집을 가능케 하는 규정이 된다.

○ 특별한 수단의 사용

• '개정초안' 제8c조는 특별한 정보수집수단으로 경찰이 현저한 위험의 방지나 예방적 범죄투쟁을 위하여 장기간의 관찰, 기술적 수단의 은밀한 설치, 신분위장경찰관의 투입, 비경찰정보원의 활용 등을 통해 개인정보를 수집할 수 있음을 규정하고 있다. 기술적 수단의 은밀한 설치란 비디오카메라 또는 녹음장치 등을 은폐된 방식으로 설치하여 관계인들이 모르게 사진이나 동영상을 촬영하거나 녹음하는 것을 말한다.

• 이러한 특별한 수단의 사용은 기본권침해의 강도가 상대적으로 크기 때문에 주경찰법은 대개 특별히 엄격한 요건 하에서만 허용되도록 규정하고 있다. 대체로 '법에 규정된 중대한 범죄의 예방 또는 중대한 위험의 방지를 위하

여 필요한 경우'에 한하여 허용된다. 주의 경찰법을 보면, 생명, 신체 또는 자유에 대한 직접적 위험을 방지하기 위하여 필요한 경우에 한정되고 있다고 하며, 일반적인 범죄예방의 목적으로는 특별한 수단의 사용이 허용되지 않는다고 한다.[10)]

(2) 정보의 처리

○ 정보의 저장

• '통일경찰법 개정초안' 제10a조는 경찰의 직무수행을 위하여 필요한 경우에 개인정보의 저장 등 처리에 관하여 일반조항 형식의 수권규정을 마련하고 있다. 이러한 규정을 근거로 경찰은 그 임무수행에 필요한 경우 개인관련정보를 문서 또는 데이터로 저장하고 수정하거나 이용할 수 있다.

• 경찰은 또한 경찰작용에 대한 선례관리 및 기한이 정해진 기록보관의 목적으로 개인관련정보를 저장할 수 있고 전적으로 이 목적으로만 이들 정보를 저장할 수 있으며 그 한도에서 제10a조는 적용이 배제될 수 있다(제10b조).

○ 정보의 제공

• 정보제공과 관련하여 개정초안은 제10c조에서 경찰이 저장하고 있는 정보에 접근하려는 다른 기관 혹은 사인의 성격에 따라서 그 허용요건을 달리하여 규정할 것을 제안하고 있다. 예컨대 임무의 유사성에 따라 위험방지임무를 담당하고 있는 기관에 대한 정보의 제공은 다른 임무를 수행하는 기관이나 사인에 대한 정보제공보다 상대적으로 완화된 요건 하에서 허용된다.

• 개정초안 제10d조는 정보의 제공 및 이용을 위한 온라인연결의 허용요건에 대하여 별도로 규정하고 있다. 경찰 이외의 기관에 의한 검색을 금지하고 있다.

○ 정보의 대조와 검색

• 개정초안 제10e조는 개인정보를 그 종류에 따라 요건을 구별하여 경찰보유데이터 또는 수배자료와 대조(Abgleich)할 수 있음을 규정하고 있다.

• 제10f조에서는 정보대조의 특수형태로서 경찰이 위험방지 목적으로 다른

10) 김연태, "치안정보의 효율적인 관리방안에 대한 연구 – 경찰의 정보관리에 대한 입법적 개선방안을 중심으로", 치안연구소 정책보고서, 2000, 51면.

자료현황과의 대조를 위하여 공공기관 또는 사기관의 데이터 중 특정한 인적 집단에 대한 개인관련정보의 제공을 요구할 수 있음을 규정하고 있다. 특정인을 확인하기 위한 비교검색(Rasterfahndung)은 중대범죄에 한하여 구체적인 위험을 근거로 하여서만 허용되도록 엄격하게 한정하고 있다.

(3) 정보의 정정, 삭제와 차단

○ 독일의 연방정보보호법뿐만 아니라 주경찰법은 개인정보에 대하여 정보주체의 정정청구권을 규정하고 있으며, 차단 및 삭제의 요건을 규정하여 그 요건에 합치하는 경우 차단 및 삭제청구권을 인정하고 있다.[11]

마. 경찰의 개인정보 수집 및 처리의 법률적 근거

1) 법상황

현재 광범위하고 다양하게 이루어지고 있는 경찰의 정보활동은 개별적인 경우에 따라 법률상의 근거를 갖추고 있는 경우도 있지만, 대개는 그렇지 않다. 우선 경찰의 자체적인 정보수집 및 이용에 대해서 살펴보면, 수사자료표의 작성 및 이용은 형실효법 제5조 제1항에 근거를 두고 있는 반면에, 범죄수법원지에 의한 개인정보의 수집, 우범자관찰보호에 의한 정보수집, 그리고 CIMS나 KICS에 의한 정보처리, 정보과를 중심으로 한 사찰정보의 수집 등에 관해서는 구체적인 실정법상의 근거를 발견할 수 없다. 뿐만 아니라 정보의 저장과 이용에 관해서는 사실상 아무런 규정도, 통제장치도 존재하지 않는다.

이러한 상황에서 경찰의 정보수집활동이 「경찰법」 제3조 및 경직법 제2조에서 규정한 경찰직무를 수행하는 활동의 일환이라는 점을 근거로 하여 당연히 허용되는 것이라는 주장이 우리 사회에 팽배해 있다. 즉, “공공의 안녕과 질서유지”라는 경찰직무상의 목적을 위하여 필요한 범위에서 경찰의 정보수집은 특별한 수권규정이 없어도 당연히 인정된다는 것이다. 이 때 경찰의 정보활동은 다른 경찰작용과 마찬가지로 경직법에 규정된 ‘경찰비례의 원칙’에 의하여 규율된다고 한다.

11) 독일 연방정보보호법 제6조, 제20조 참조.

경찰관직무집행법 제2조(직무의 범위) 경찰관은 다음 각호의 직무를 행한다.
1. 범죄의 예방·진압 및 수사
2. 경비·요인경호 및 대간첩작전수행
3. 치안정보의 수집·작성 및 배포
4. 교통의 단속과 위해의 방지
5. 기타 공공의 안녕과 질서유지

경찰법 제3조(국가경찰의 임무) 국가경찰은 국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압 및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 임무로 한다.

2) 경찰법 제3조와 경직법 제2조가 법률적 근거가 될 수 있는가?

경직법 제2조와 경찰법 제3조는 경찰의 직무활동의 범위를 정한 직무규범이다. 경찰법은 경찰조직법의 성격이 강한 반면에, 경찰의 직무활동에 관한 일반법적 기능을 수행하는 것은 경직법이다. 경직법 제2조는 경찰관의 일반적인 직무집행의 범위를 규정하면서 “치안정보의 수집·작성 및 배포”를 경찰직무의 하나로 규정하고 있다. 그렇지만 경직법에는 경찰의 정보활동에 관련하여 개인정보의 수집요건이라든가 수집범위, 정보의 보관이나 처리 등에 관한 구체적인 규정은 전혀 없다.

일부에서는 경찰법 제3조와 경직법 제2조가 경찰의 정보활동의 실정법적 근거가 된다고 주장한다. 그 근거에 관해서는 “경찰의 정보활동은 국민과의 관계에서 국민의 자유와 권리를 침해하는 구체적인 조치를 수반하지 않으므로 조치권한에 관한 구체적 수권은 필요하지 않다”고 설명하기도 하고, “정보경찰활동이 경찰의 목적 즉 ‘국민의 생명과 신체 및 재산을 보호하고 공공의 안녕과 질서의 유지’를 달성하기 위한 범위 내에서 이루어지는 한” 특별한 수권이 필요없다고 설명하기도 한다.

그러나 지극히 추상적이고 일반적인 직무규범의 성격을 지니는 경찰법 제3조나 경직법 제2조는 경찰의 광범위한 정보수집 및 처리를 근거지우는 ‘수권규범’이라고 볼 수 없다.

우선 경찰의 정보활동이 국민의 자유와 권리를 침해하는 조치를 수반하지 않는다는 주장은 개인정보자기결정권의 기본권적 성격과 법치주의적 의미를 몰각한 설명이다. 종래 침해성이 없다고 보았던 경찰의 개인관련정보에 대한 활동

들은 이제 더 이상 단지 임무규범만을 근거로 정당화될 수 없고 별도의 수권규정을 필요로 한다고 보아야 한다. 범죄관련 정보를 수집하는 활동뿐만 아니라 정보과의 사찰업무인 “정치·경제·노동·사회·학원·종교·문화 등 제 분야에 관한 치안정보의 수집·종합·분석·작성 및 배포”(「경찰청과그소속기관등직제」 제14조 제3항 제2호) 등 경찰의 광범위한 정보수집활동은 필연적으로 개인과 관련된 정보를 포함할 수밖에 없다. 개인정보자기결정권은 개별 정보주체들이 자신에 관한 정보를 타인이 수집하고 이용하는 것을 통제할 권리를 의미하므로, 경찰이 개인정보를 수집하는 행위는 그 자체로 항상 기본권침해적 속성을 지니게 마련이다.[12] 따라서 법률유보의 원칙상 경찰의 정보수집 및 처리에 대해서는 구체적인 수권규정이 반드시 필요하다.

이 때 직무규범과 수권규범을 구별하는 것이 중요하다. 경찰의 임무가 공공의 안녕질서의 유지 내지 위험방지에 있다는 것과 그러한 경찰권 발동으로 인해 개인의 권리침해가 수반되는 경우에 침해의 권한이 인정되는가의 문제는 분명하게 구별되어야 한다. 위험방지임무를 위하여 개인의 권리를 침해하는 것은 위험방지임무의 수행에 있어서 법치국가적 한계의 문제로 취급되어야 한다. 개인의 권리에 대한 침해는 특별한 요건을 갖춘 경우에 한하여 허용되어야 함은 법치국가원칙의 당연한 요청이다. 직무규범과 수권규범의 분리는 법치행정의 원칙에서 요구되는 것이다. 따라서 경찰의 직무에 관한 규정인 경직법 제2조가 기본권침해적 성격을 지니는 경찰의 정보활동을 근거지우는 수권규범이 될 수는 없다고 보아야 한다. 독일의 개정초안 및 주경찰법이 모두 경찰의 직무규정 외에 경찰의 정보수집 및 처리에 관하여 상세한 규정을 둔 이유는 바로 임무규범과 수권규범의 분리라는 법치주의적 요청에 근거한 때문이다.

문제는 경직법 제2조를 직무규범의 성격과 동시에 권리침해적 경찰작용을 근거지우는 개괄적 수권조항으로 이해하는 식의 해석론이다.

경직법 제3조 이하의 규정은 법익침해적 경찰권 행사를 근거지우는 개별적 수권조항이라면, 경직법 제2조는 그러한 개별적 수권규정이 없지만 경찰권발동이 필요한 경우에 일반적으로 적용되는 ‘개괄적 수권규범’이라는 것이다. 이와 같은 해석은 지문날인정보의 이용에 관한 헌법재판소의 결정, CIMS에 관한 법원의 판결 등에서 광범위하게 엿볼 수 있다.

그러나 경직법 제2조가 개괄적 수권조항인가에 대해서는 비판적으로 검토해

12) 우리 헌법재판소도 주민등록법상 지문정보의 날인 및 이용에 관한 결정에서 이 점을 분명히 지적하였다 : “개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.” 판례집 682면.

볼 필요가 있다.

독일의 경우 1931년 프로이센경찰법 제14조 제1항에서 “경찰행정청은 공공의 안녕 또는 질서를 위협하는 위험으로부터 공중 또는 개인을 보호하기 위하여 실정법의 범위 안에서 의무에 적합한 재량에 따라 필요한 조치를 취하지 않으면 안 된다.”는 식의 개괄적 수권규정을 둔 적이 있다. 이 규정과 경직법 제2조를 비교해 보면, 경직법 제2조는 위와 같은 식의 수권규범의 규정방식을 취하고 있지 않다. 경직법 제2조는 단순한 직무규정일 뿐이며, 이를 개괄적 수권규정이라고 해석할 수 없는 것이다.

더욱 중요한 것은 오늘날 법치국가원칙에 비추어 볼 때, 독일 프로이센 경찰법 규정과 같은 식의 개괄적 수권규정은 허용될 수 없다는 점이다. 개괄적 수권규정은 경찰권 발동의 요건과 허용범위에 관한 구체적인 내용을 지시해 주지 못하기 때문에 경찰권 발동에 관한 법치주의적 통제를 담보할 수 없다. 더구나 독일 연방헌법재판소는 인구조사결정에서 정보자기결정권을 침해하는 국가에 의한 개인관련정보의 수집 및 처리가 그 ‘범위에 특유한’ 개별적 수권규범에 근거하여 이루어져야 한다는 점을 분명히 하였다. 경찰은 개인관련정보의 수집 및 처리와 같이 개인의 정보결정권을 침해하는 경찰조치들을 단지 일반수권조항만을 근거로 허용될 수는 없다.

3) 개인정보 보호법은 근거규정이 될 수 있는가

2011.9.30. 시행된 「개인정보 보호법」 제15조는 다음과 같이 규정하고 있다.

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우

※ (구)「공공기관의 개인정보보호에 관한 법률」제5조 (개인정보파일의 보유범위) 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다.

종래 경찰의 개인정보수집 및 처리에 관해서는 경직법 제2조 외에도 「공공기관의 개인정보보호에 관한 법률」 제5조가 근거규정으로 자주 원용되고 있었다. 이제는 개인정보 보호법 제15조가 경찰의 정보수집 및 처리의 근거규정으로 원용될 것이다.

(구)「공공기관의 개인정보보호에 관한 법률」 제5조에 대해서는, 그 규정은 개별 법률에 개인정보의 수집 및 처리에 관한 근거규정이 있음을 전제로 해서 개인정보파일을 보유할 수 있도록 한 근거규정에 불과하며, 이 규정을 근거로 해서 경찰 등 공공기관의 개인정보 수집 및 처리가 포괄적으로 근거지워질 수는 없다는 비판이 제기된 바 있다. 이는 전자화촉진법 제5조에 대해서도 마찬가지이다.

이러한 비판은 2011.9.30. 시행된 개인정보 보호법 제15조에 대해서도 동일하게 타당하다. 물론 개인정보 보호법 제15조는 “공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우”에 개인정보를 수집, 처리할 수 있다고 규정하고 있어 (구)「공공기관의 개인정보보호에 관한 법률」 제5조와는 다소의 차이가 있다. 개인정보파일의 보유로 규정했던 구법에 비하여, 개인정보 보호법 제15조는 개인정보의 수집과 처리 일반에 대해 규정하고 있다. 그러나 이 규정이 경찰의 개인정보 수집 및 처리를 통째로 근거지우는 규정으로 볼 수는 없다. 첫째, “공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우”라는 규정 자체가 매우 추상적이고 모호하여 경찰의 정보활동이 어떤 요건 하에서 그리고 어느 범위에서 허용되는지를 도저히 가늠할 수 없게 되어 있으며, 둘째, 무엇보다도 개인정보의 수집 및 처리는 단순히 공공기관의 업무수행을 위한 ‘부대업무’가 아니라 기본권침해적 공권력작용이기 때문에 그 자체가 독자적인 법적 근거를 지니는 권력작용으로 통제되어야 한다는 법치주의적 요청을 완전히 무시하는 규정이기 때문이다.

4) 소결

경찰법 제3조, 경직법 제2조, 개인정보 보호법 제15조는 경찰의 정보활동에 관한 법적 근거가 될 수 없다.

개인정보자기결정권을 침해하는 경찰작용에 대해서는 구체적이고 개별적인 수권규정이 상세하게 마련되어야 한다.

바. 경찰의 정보수집 및 처리에 관한 통제방안

1) 경찰의 직무범위와 정보수집의 목적 및 요건

가) 목적구속의 원칙

개인정보 보호를 위한 중요한 원칙으로 목적구속의 원칙이 있다. 그 근거는 국가의 정보수집 및 처리에 있어서 권력분립의 원칙이 적용되어야 한다는 점으로부터 도출된다.[13] 목적구속의 원칙은 개인정보의 수집 및 처리는 법률에 의하여 특정된 목적범위 내에서만 허용된다는 원칙이다. 개인정보 보호법 제3조 제1항은 “개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.”고 규정하여 목적구속의 원칙을 반영하고 있다.

여기에서 목적은 일반 시민들이 자신의 개인정보가 왜 수집되어야 하는지 그 필요성을 분명하게 알 수 있을 정도로 특정되어야 한다. 한편, 목적구속의 원칙 및 그것이 요구하는 목적의 특정성은 그 기관의 정보수집이 그 목적 달성에 적합한 것인지 여부 그리고 필요최소한의 조치인지 여부를 판단하는 출발점이 된다는 점에 매우 중요하다.

개인정보를 수집하는 목적이 불명확하거나 특정되지 않은 경우 혹은 지나치게 추상적인 경우에는 목적구속의 원칙에 반한다.[14] 앞서 언급한 바와 같이 경직법 제2조는 경찰의 정보수집 및 처리를 근거지우는 수권규정이라고 보기 어렵지만, 이를 개괄적 수권규정이라고 이해하더라도 그 규정의 추상성과 불명확성으로 인하여 목적구속의 원칙에 반한다는 점에는 의문의 여지가 없어 보인다. 경직법 제2조의 규정만으로는 경찰의 정보수집이 어떠한 목적에서 어떠한 정보를 수집할 필요성이 있는 것인지 도저히 가늠할 수 없기 때문이다.

특히 경찰이 정보원을 활용하여 은밀하게 정보를 수집하거나 동영상촬영 등의 기술적 수단에 의하여 정보를 수집하는 경우에는 목적구속의 원칙이 보다 강조되어야 한다. 그 경우에는 개인정보자기결정권에 대한 침해가 크기 때문에 비례성원칙에 비추어 다른 정보수집보다 더욱 엄격한 목적과 요건이 필요하다.

---

13) Riegel, Datenschutz bei den Sicherheitsbehörden, 2.Aufl., S.139.

14) 김성태, “개인관련정보에 대한 경찰작용 - 독일 주경찰법에서의 규율 -”, 경찰법연구 창간호, 2003, 103면.

나) 목적구속의 원칙의 형해화 위험

법률유보의 원칙, 그리고 목적구속의 원칙에 충실하게 경찰의 정보수집 및 처리에 관하여 실정법에 - 예를 들어, 경직법에 - 자세한 수권규정을 둔다고 할 때, 정작 중요한 것은 경찰의 직무활동의 범위를 어디까지 허용해야 하는가의 문제이다. 현행 경직법 제2조에 근거하여 경찰은 범죄사건의 수사 외에 공공의 안전과 질서유지를 위하여 경찰권을 발동할 수 있으며 경찰직무를 수행하는 과정에서 당연히 정보수집활동이 행해진다. 결국 경찰의 직무범위를 어떻게 설정하는가에 따라 경찰의 정보활동의 허용범위도 달라질 수 있다.

일반적으로 경찰의 직무는 범죄사건의 수사(소위 진압임무)와 위험방지의 예방임무로 크게 나뉘는데, 위험방지를 위한 경찰의 직무범위는 경직법 제2조 제1호 내지 제5호에 규정되어 있다. 경직법 제2조 자체가 권리침해적인 경찰권발동의 직접적인 근거규정이라고 볼 수는 없다 하더라도, 경찰의 위험방지업무의 범위를 어떻게 설정하느냐에 따라 경찰의 개인정보 수집의 허용범위가 달라지게 된다는 점에서 경찰의 직무와 권한의 범위를 정하는 문제는 매우 중요하다.

독일의 1986년 개정초안이 경찰의 개인정보 수집 및 처리에 관한 구체적인 권한규정을 둠과 동시에 경찰의 직무범위를 규정한 제1조의 변경을 포함하고 있음을 주목할 필요가 있다. 앞서 지적한 바와 같이, 경찰의 직무를 정한 규정은 개인정보자기결정권을 침해하는 경찰의 정보활동을 정당화하는 수권규범이 아니기 때문에 경찰의 정보수집과 처리에 관한 수권규정을 구체화하기 위하여 경찰직무규범을 변경할 이유는 없다. 그럼에도 불구하고 독일의 개정초안 그리고 대부분의 주경찰법이 종래의 경찰직무규정을 변경한 이유는 경찰의 정보활동이 주로 “구체적 위험의 방지” 전단계에서 이루어지는 경찰작용이라는 점 때문이다.

독일의 개정초안은 종래 경찰직무를 규정한 모범초안 제1조 제1항(“경찰은 공공의 안전이나 질서에 대한 위험을 방지할 임무를 지닌다.”)에 제2문을 추가하여, 경찰의 직무범위에 관하여 “예방적 범죄투쟁”, “위험방지를 위한 준비”와 같은 개념을 사용하고 있다. 이러한 개념은 경찰의 정보수집활동과 밀접한 관련이 있다. 비록 개정초안이 경찰의 정보활동을 그 자체로 경찰의 임무로 규정하지는 않고 있지만, 경찰의 정보수집은 대개 위험방지를 위한 개입조치 이전단계에서 이루어지는 것임을 고려하면 위와 같은 경찰직무규정의 변경은 종래부터 경찰이 해왔던 정보수집활동을 거의 그대로 정당화하는 실정법적·이론적 출발점으로 기능하는 셈이다. 경찰의 직무로서 “예방적 범죄투쟁”이라든가 “위

험방지를 위한 준비"는 "구체적 위험"의 이전단계에서, 즉 '위험의 방지'가 아니라 '위험 발생의 방지'를 목적으로 하는 경찰작용이며 그 핵심을 이루는 것이 바로 경찰의 정보수집활동이기 때문이다.

다) 경찰의 정보수집 및 처리의 허용기준으로서 "구체적 위험의 원칙"

결국 관건은 경찰권 발동의 요건으로서 '위험' 개념에 있다. 경직법은 "위해"라는 개념을 주로 사용한다. 현행 경직법 제2조는 경찰관 직무범위에 관하여 '교통의 단속과 위해의 방지'를 규정하고 있으며, 보호조치를 규정한 제4조 제1항,[15] 위험발생의 방지에 관한 제5조 제1항,[16] 범죄의 예방과 제지를 규정한 제6조 제1항,[17] 타인의 토지나 건물 등에 대한 경찰관의 출입을 규정한 제7조 제1항 및 제2항[18] 등에서 경찰권 행사의 요건 속에 '위해'라는 개념이 등장한다.

위해는 통상 '위험'과 '장해'를 포괄하는 개념으로 이해되고 있다.[19] 여기에서 '위험'이란 현재의 상황을 그대로 방치할 경우 법익에 대한 손상이 발생할 충분한 개연성이 있는 것을 의미하고, '장해'란 법익에 대한 손상 내지 손해가 이미

15) 경직법 제4조(보호조치등) ①경찰관은 수상한 거동 기타 주위의 사정을 합리적으로 판단하여 다음 각 호의 1에 해당함이 명백하며 응급의 구호를 요한다고 믿을 만한 상당한 이유가 있는 자를 발견한 때에는 보건의료기관 또는 공공구호기관에 긴급구호를 요청하거나 경찰관서에 보호하는 등 적당한 조치를 할 수 있다. <개정 1988.12.31>
1. 정신착란 또는 술취한 상태로 인하여 자기 또는 타인의 생명·신체와 재산에 위해를 미칠 우려가 있는 자와 자살을 기도하는 자

16) 경직법 제5조 (위험발생의 방지) ①경찰관은 인명 또는 신체에 위해를 미치거나 재산에 중대한 손해를 끼칠 우려가 있는 천재, 사변, 공작물의 손괴, 교통사고, 위험물의 폭발, 광견·분마류등의 출현, 극단한 혼잡 기타 위험한 사태가 있을 때에는 다음의 조치를 할 수 있다.
1. 그 장소에 집합한 자, 사물의 관리자 기타 관계인에게 필요한 경고를 발하는 것
2. 특히 긴급을 요할 때에는 위해를 받을 우려가 있는 자를 필요한 한도 내에서 억류하거나 피난시키는 것
3. 그 장소에 있는 자, 사물의 관리자 기타 관계인에게 위해방지상 필요하다고 인정되는 조치를 하게 하거나 스스로 그 조치를 하는 것

17) 경직법 제6조 (범죄의 예방과 제지) ①경찰관은 범죄행위가 목전에 행하여지려고 하고 있다고 인정될 때에는 이를 예방하기 위하여 관계인에게 필요한 경고를 발하고, 그 행위로 인하여 인명·신체에 위해를 미치거나 재산에 중대한 손해를 끼칠 우려가 있어 긴급을 요하는 경우에는 그 행위를 제지할 수 있다.

18) 경직법 제7조(위험방지를 위한 출입) ①경찰관은 제5조제1항·제2항 및 제6조제1항에 규정한 위험한 사태가 발생하여 인명·신체 또는 재산에 대한 위해가 절박한 때에 그 위해를 방지하거나 피해자를 구조하기 위하여 부득이 하다고 인정할 때에는 합리적으로 판단하여 필요한 한도 내에서 타인의 토지·건물 또는 선차 내에 출입할 수 있다.
②흥행장·여관·음식점·역 기타 다수인이 출입하는 장소의 관리자 또는 이에 준하는 관계인은 그 영업 또는 공개시간 내에 경찰관이 범죄의 예방 또는 인명·신체와 재산에 대한 위해예방을 목적으로 그 장소에 출입할 것을 요구한 때에는 정당한 이유없이 이를 거절할 수 없다.

19) 문병효, "경찰관직무집행법 개정안에 대한 비판적 고찰", 고려법학 제58호, 2010, 80면 ; 김성태, "예방적 경찰작용에서의 추상적 위험·구체적 위험", 행정법연구 제9호, 2003, 256면.

발생한 경우를 의미한다.[20] 엄밀하게 말하여 '위해'는 '위험' 개념과는 구별되는 것이지만, 결국 경찰권 발동의 초점은 '위험방지'를 위한 예방적 경찰활동을 어느 범위까지 허용할 것인가의 문제에 있다.

오늘날 경찰국가화 경향이 강화되는 가운데 '구체적 위험'이 존재하는 경우에 한하여 경찰권 발동이 정당화된다는 고전적인 제한법리가 위협받고 있는 상황이다.

행정법학계에서는 경찰권발동의 근거가 되는 위험 개념에 대해 구체적 위험과 추상적 위험으로 구별하여 논의하는 경향이 있다.[21] 여기에서 구체적 위험이란 법익에 대한 손상이 개연성의 정도로 현실적으로 예견되는 경우를 말하며, 추상적 위험이란 현실적인 위험에 대한 예측 및 개연성의 요소를 필요로 하지 않고 단지 '관념적으로 형성된 일반적인 사정에 근거한 위험'을 의미할 뿐이라는 점에서 차이가 있다. 일반론으로 말하면, 위험방지를 위한 경찰의 예방적 작용은 원칙적으로 구체적인 위험의 방지를 요건으로 해서 정당화된다고 한다.[22] 실제 경직법상 경찰의 권리침해적 작용의 개별적 수권규정이라 할 수 있는 '보호조치'(제4조), '위험발생의 방지'(제5조), '범죄의 예방과 제지'(제6조) 등은 경찰권 행사의 근거가 되는 요건을 설정함에 있어 구체적이고 현실적인 법익침해의 위험을 상정하고 있다. 이처럼 경찰의 예방적 활동이 시민의 권리를 침해하는 속성을 지닌 경우에 '구체적 위험'을 요건으로 해야 한다는 점은 과잉금지원칙 내지 경찰비례의 원칙에 의하여 요구되는 것이다.

그러나 독일 경찰법에서 자주 등장하는 개념인 "예방적 범죄투쟁"이라든가 "위험방지를 위한 준비"는 구체적 위험의 전단계에서 즉 '추상적 위험'만을 근거로 하여 경찰권 발동을 정당화한다. 그 핵심에는 경찰의 정보수집활동이 있다. 독일 작센주 헌법재판소는 1996년 정보수집에 관한 작센주 경찰법의 규정과 관련하여 개인정보자기결정권에 대한 침해는 구체적인 위험에 구속되지 않는다고 결정했다.[23] 경찰의 개인정보수집에 대해서는 법치국가적 한계가 적용되어야 하지만, 경찰권 발동의 요건은 위험 개념이 추상화되면 그 위험 개념은 더 이상 법치국가적 통제기능을 수행하기에는 무력한 개념이 된다. 추상적 위

20) 경직법은 위험 개념과 위해 개념을 모두 사용하고 있는데, 그 구별이 상당히 혼란스럽고 양 개념을 명확하게 구별하여 사용하는 것은 아닌 것 같다.

21) 독일의 위험 개념에 관한 논의에 대해서는, 김성태, 앞의 글, 251면 이하 ; 이호용/김종세, "경찰권 발동의 근거로서 '위험' 개념과 양태", 한국공안행정학회보 제19호, 2005, 426-427면 참조.

22) 김성태, 앞의 글, 268면. 이러한 해석은 일반수권조항에 의하는 경우건 개별적 수권조항에 의하는 경우건 동일하다고 한다.

23) SächsVerfG, Urt. v. 14. 5. 1996, JZ 1996, S.957ff..

험은 사실상 경찰의 경험과 직관에 의하여 쉽게 인정될 수 있기 때문이다. 예를 들어, 과거에 폭력시위의 전과가 있는 사람에 대한 정보수집은 그러한 '추상적 위험'에 근거하여 쉽게 정당화될 수 있게 된다.

구체적 위험 요건이 형해화되는 상황에서도, 독일연방헌법재판소의 2006년 4월 4일 소위 'Rastefahndung'과 관련한 결정은 주목할 만하다.[24] 'Rastefahndung'은 우월한 법익에 대한 구체적인 위험이 있을 때만 헌법상 기본권과 합치할 수 있다는 것이다. 독일연방헌법재판소는 노르트라인-베스트팔렌 주 경찰법(NWPolG, 1990년) 제31조에 규정된 경찰의 예방적인 'Rastefahndung'에 대하여 연방과 주의 존속이나 안전 또는 생명, 신체, 자유와 같은 우월한 법익에 대한 구체적인 위험이 존재할 때만 정보의 자기결정에 대한 기본권(기본법 제1조 1항과 결합한 제2조 1항)과 합치할 수 있다고 결정하였다. 나아가 2001년 9월 11일 이래 테러공격과 관련하여 널리 존재하는 것과 같은 일반적인 위험상황 혹은 외교정책적인 긴장상태는 'Rasterfahndung'을 명하기에 충분하지 않으며 오히려 구체적인 위험, 즉 테러공격을 준비하거나 실행하기 위한 구체적 위험이 도출될 만한 사실의 존재가 필요함을 명확히 하였다.

경찰의 권력적 작용이, 특히 경찰의 정보활동이 추상적 위험에 근거하여 정당화될 수 있는가는 경찰행정법의 영역에서 매우 어려운 문제에 속하는데, 분명한 것은 추상적 위험에 근거한 경찰권 발동은 경찰비례의 원칙에 비추어 원칙적으로 정당성을 갖기 어려우며 단지 그로 인한 권리침해가 지극히 경미한 경우에 한하여 극히 예외적으로만 정당화될 수 있다는 점이다.[25] 구체적 위험을 요건으로 하지 않고 단지 경찰의 경험과 추상적인 판단에 의존한 추상적 위험 개념을 경찰권 행사의 요건으로 삼게 되면 실질적으로는 경찰의 자의적이고 정치적인 판단이 경찰권 행사에 개입하는 것을 차단할 방법이 없기 때문에 이는 결국 경찰권의 자의적인 행사와 그로 인한 시민의 권리침해를 용인하는 결과가 되어 매우 위험한 것이기도 하다.

그러므로, 경찰의 정보수집활동을 규제하기 위한 법치국가적 요건으로 "구체적 위험의 요건"은 강조되어야 한다.

24) BverfG, Beschuß vom 4.4.2006 ß 1BvR 518-02.
25) 이 점은, 김성태, 앞의 글, 271면.

라) 개선제안

경찰의 개인정보 수집 및 처리에 관해서는 경직법에 그 요건과 수집허용범위 등에 대해 구체적이고 상세한 규정을 두어야 한다.

소위 예방적 범죄투쟁 등 '추상적 위험'을 근거로 한 개인정보수집은 금지해야 하며, 개인정보의 수집은 '공공의 안전에 대한 구체적인 위험'을 근거로 하여서만 허용되도록 규정해야 한다.

수집목적 외의 사용금지에 대해 명확한 규정을 두어야 한다. 예를 들어, 증인이나 참고인, 피해자에 관한 정보는 '위험야기자'에 대한 정보검색에 동원하지 못하도록 해야 한다.

근본적으로 수집목적에 관해서는 구체적인 통제에 한계가 있음을 분명히 인식할 필요가 있다. 경찰의 정보수집에 대한 시민적 통제는 결국 정보접근 및 정정·삭제청구권 등을 통해 실효성을 확보하는 방향으로 나아가야 한다.

2) 경찰의 정보수집에 대한 규제의 방향

가) 직접성, 공개성 원칙

국가기관의 개인정보 수집은 정보주체인 당사자로부터 직접적으로 그리고 공개적으로 이루어져야 한다. 직접성 원칙과 공개성 원칙은 정보주체인 개인이 자신에 관한 정보의 제공과 이용에 대하여 스스로 결정할 수 있다는 개인정보 자기결정권을 실현하기 위한 핵심적인 원칙이다. 정보주체로부터 직접 공개적으로 정보가 수집되어야 정보주체는 자신에 관한 어떠한 정보가 어떻게 수집되고 처리되는지를 알 수 있기 때문이다.

독일의 '개정초안' 및 주경찰법은 정보수집의 직접성 및 공개성원칙을 규정하고 있다. 다만, 직접성 및 공개성 원칙은 경찰의 모든 정보수집활동에 예외없이 적용될 수 있는 것은 아니다. 독일의 개정초안은 '당사자로부터 직접 정보를 수집하는 것이 불가능하거나 지나치게 높은 비용을 요하는 경우 혹은 직접적인 정보수집이 경찰의 직무수행을 현저히 어렵게 하거나 위협하는 경우'에는 경찰은 다른 기관이나 제3자로부터 또는 비밀리에 정보를 수집할 수 있다는 예외규정을 두고 있다.[26]

그런데 우리의 개인정보 보호법은 정보수집의 직접성원칙이나 공개성원칙을 규정하고 있지 않다.

---

26) §8a (4) VEMEPolG.

개선제안은 다음과 같다. 첫째, 개인정보 보호법에는 정보수집의 직접성 및 공개성원칙을 규정하고, 이에 대한 예외는 개별법률에 특별히 규정한 경우에만 허용되도록 규정한다. 둘째, 경직법에는 경찰의 개인정보수집에 관하여 규정할 때 직접성원칙 및 공개성원칙을 규정하고, 이에 대한 예외가 필요한 경우에는 “필요한 최소한도의 범위에서 엄격한 예외규정을 마련”해야 한다.

나) 민감정보의 수집금지

개선제안으로는, 민감정보의 수집금지에 관해 경직법에 명문규정을 두어야 한다.

다) 공개된 행사나 모임, 집회에서의 정보수집에 대한 제한

개선제안으로는, 공개된 행사나 모임, 집회 등에 관한 경찰의 정보수집은 그 주최자나 참석자 중 공공의 안전에 관한 위험을 야기할 위험성이 구체적으로 존재하는 경우에 한하여 예외적으로만 허용된다는 식의 제한규정을 도입해야 한다.

3) 정보의 저장 및 이용에 대한 통제

정보의 저장과 이용은 원칙적으로 애초에 정보를 수집한 목적을 위해서만 허용되어야 한다.[27] 목적구속의 원칙은 정보수집뿐만 아니라 수집된 정보의 저장과 이용에 대해서도 동일하게 적용되는 원리이기 때문이다. 이와 같이 정보의 저장과 이용 단계에서 목적구속의 원칙이 제대로 기능하기 위한 전제조건은 일차적으로 정보수집의 목적이 상세하게 구체화되어야 한다는 점이다. 경찰은 범죄수사, 범죄예방 및 위험방지를 위하여 개인정보를 수집하고 또 저장, 이용할 수 있지만, 그와 같은 경찰직무의 영역 안에서도 정보수집의 목적과 수집정보의 범위는 최대한 구체적으로 규정되어야 한다.

목적구속의 원칙 그리고 필요성의 원칙으로부터 경찰이 수집한 정보의 저장 및 이용에 관하여 다음의 몇가지 세부적인 규율원칙들을 추출할 수 있다.

첫째, 경찰의 위험방지임무에 근거하여 위험야기자에 관하여 수집한 정보는 해당정보의 보유가 필요한 한도에서 제한되어야 한다. 즉, 정보수집의 근거가 된 위험이 해소된 경우에는 즉시 해당정보를 폐기하도록 규정해야 한다.

27) 김연태, 앞의 책, 114면.

둘째, 경찰이 범죄수사의 과정에서 수집한 개인정보는 원칙적으로 수사목적 이외의 목적으로 저장되거나 이용되어서는 안 된다는 점도 중요하다.[28] 예를 들어, 참고인이나 증인의 지위에서 어떤 사람에 대한 정보가 수집된 경우 해당 범죄사건의 수사를 위하여 그 정보를 저장하고 이용할 수 있지만, 그 개인정보가 소위 '예방적 범죄투쟁'을 위한 정보로 광범위하게 저장되거나 이용되어서는 안 된다.

4) 정보의 온라인 통합시스템에 대한 통제

경찰의 온라인 통합시스템이 문제가 되는 경우는 다음과 같다.

- 행정전산망 통합
- 정보화촉진법에 의한 KICS 운영

독일의 경우 경찰이 수집한 정보에 대하여 경찰기관 상호간 혹은 다른 공공기관과의 무제한적 접근 및 검색이 가능한 식의 온라인 통합시스템에 대해서는 엄격한 요건 하에 통제하는 근거규정을 두고 있다.

실태 및 개선방안에 대해서는 좀 더 연구가 필요하다.

5) 타 기관이 수집·보유한 정보의 검색에 대한 통제

가) 문제상황

오늘날 공공기관이건 사기관이건 간에 컴퓨터 등 정보처리장치에 의하여 다량의 개인정보가 수집되고 관리되고 있다. 각 기관은 기관의 목적에 따라 필요한 범위에서 개인의 신상정보나 비밀에 속하는 정보를 수집하고 사용할 수 있게 된다. 한편 수사기관에서는 수사의 목적상 범인을 발견하거나 범죄사실을 규명하고 증거를 수집하기 위하여 불특정 다수의 개인정보를 수집하고 분석하는 것이 유용할 수도 있다. 그와 같은 개인정보의 검색은 수사목적 외에도 '위험예방'이라는 경찰권 발동의 차원에서도 얼마든지 행해질 수 있다.

28) 다만, 범죄통계를 위한 정보이용은 예외로 할 수 있을 것이다. 이에 대해서는 §10a (6) VEMEPolG 참조.

- 9·11 테러 이후 이슬람인 거주자에 대한 정보검색
- 소위 '발바리사건'에 대하여 경찰이 병무청에 사실조회를 요청한 것 등

하지만, 경찰의 광범위한 정보검색에 관한 규범적 통제는 현재 매우 미약한 수준이다. 개인정보 보호법은 범죄의 수사에 필요한 경우 개인정보의 목적외 사용을 광범위하게 허용하고 있기 때문이다(제18조 제2항). 이에 따르면, 경찰은 행정전산망에 저장된 개인정보는 물론이고, 다른 행정기관이나 사기관이 저장하고 있는 개인정보를 사실상 아무런 제약없이 이용할 수 있다.

더구나 오늘날처럼 개인정보가 대량으로 수집·관리되는 상황에서는 경찰이 위험예방 내지 수사상의 필요에 의하여 개인정보를 검색하는 것이 가져오는 기본권침해의 강도는 매우 크다. 수사기관이 통제대상자(피의자나 위험야지가)를 특정하지 못한 상황에서 신장이나 혈액형, 지문 등 피의자를 식별할 수 있는 특정정보만을 가지고 있는 경우에 다른 기관이 보유한 다량의 개인정보를 검색해 봄으로써 수사기관이 확보한 증거정보에 합치하는 정보를 추려내고 이를 통해 경찰통제의 대상이 되는 개인을 식별해 내는 식의 정보이용이 문제가 된다.

근거규정은 다음과 같다.

- 개인정보 보호법 제18조 제2항
- 형사소송법 제199조 제1항 사실조회요청

형사소송법 상 수사기관(검찰과 경찰)은 다른 기관(공기관인가 사기관인가를 불문한다)에 대하여 수사에 필요한 사실을 조회할 수 있다. 형사소송법 제199조 제2항은 "수사에 관하여는 공무소 기타 공사단체에 조회하여 필요한 사항의 보고를 요구할 수 있다"고 규정하고 있다. 사실조회에 특별한 요건이 규정되어 있지 않으며, 조회내용에 대해서도 특별한 제한이 없어 반드시 개인정보에 제한되는 것은 아니다. 사실조회의 전형적인 예로는, 피의자에 대한 전과조회나 신원조회 등이 여기에 해당한다. 형사소송법학계에서는 일반적으로 조회요구를 받은 상대방은 보고의무가 있다고 보고 있지만, 정보제공을 사실상 강제할 방법이 없기 때문에 상대방이 수사기관의 정보제공요청에 응해야 할 의무는 없다.

개인정보 보호법 제18조 제2항에 따르면, "범죄의 수사와 공소제기 및 유지에 필요한 경우"(제7호)에는 개인정보처리자는 자신이 수집·저장한 개인정보를

다른 기관에 제공할 수 있다. 다만, “정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때”에는 개인정보를 다른 기관에 제공할 수 없다.

나) 수사방법으로서 개인정보수집행위의 의미와 한계

형사소송법 제199조 제2항에 의한 ‘사실조회’가 임의수사인가 강제수사인가는 논란이 되고 있다. 강제수사에 해당한다면 법률에 명확한 근거가 있어야 하며 원칙적으로 영장주의에 의해서만 허용된다. 강제수사인가 임의수사인가 여부는 오늘날 실질적 법익침해 내지 기본권침해여부를 기준으로 판단한다는 것이 일반적인 견해이다.[29] 형소법 제199조 제2항의 사실조회에 대해서는 종래 조회요청을 받은 기관이 보고의무를 지지 않는다는 점에서 임의수사의 한 방법으로 취급되어 왔다. 이러한 전통적인 견해는 상대방에게 정보제공을 강제할 수 있는가 여부에만 초점을 두는 것으로, 수사기관의 정보제공의 요청과 이에 응한 정보의 제공 과정에서 정보주체인 개인의 기본권이 침해된다는 사실이 무시된다는 문제를 안고 있다. 일반적인 의미에서 자기정보통제권이란 개인이 자신의 프라이버시에 해당하는 정보에 관하여 그 공개여부 및 이용에 대하여 통제할 수 있는 권리를 말한다. 그러므로 컴퓨터 등을 통하여 개인정보를 대량으로 수집·저장하고 있는 어떠한 기관이 수사기관의 정보제공요청에 응하여 설사 자발적으로 정보를 제공한 경우에도 이로 인해 정보주체인 개인의 자기정보통제권이 침해되는 사태가 발생하게 된다. 전형적인 예를 들자면, 수사기관의 요청에 응하여 통신사가 개인의 통신기록에 관한 정보를 제공하는 경우라든가, 금융기관이 계좌입출금내역을 제공하는 것 등을 들 수 있다. 이처럼 외관상 ‘협조’라는 미명 하에 자발적인 정보제공으로 보이는 경우에도, 그러한 정보제공요청 및 정보제공행위는 제공되는 정보가 헌법적 보호를 받는 개인정보라면 정보주체인 개인의 자기정보통제권을 침해하는 것으로 보아야 한다.

그러므로 ‘사실조회’에 의하여 수사기관이 개인정보를 취득하는 수사방법은 임의수사가 아니라 강제수사에 해당한다고 보는 것이 맞다. 헌법적 기본권의 침해문제가 도사리고 있다면 위와 같은 정보제공요청과 정보제공행위는 형사소송법 제199조 제2항의 ‘사실조회’ 규정에 의하여 정당화될 수는 없다.[30] 수사기관이 타 기관을 통해 개인정보를 취득하는 행위는 개인의 정보적 자기결정권을 침해하는 속성을 지니고 있기 때문에, - 강제수사의 하나로서 - 헌법 상 법

29) 배종대/이상돈, 형사소송법, 202면 ; 신양균, 형사소송법, 114면 ; 이재상, 형사소송법, 199면 등.
30) 같은 취지로는 신양균, 형사소송법, 131면 참조.

률유보의 원칙에 따라 법률에 명확한 근거가 있어야 할 뿐만 아니라 “필요최소한도의 제한”이라는 비례성원칙에 합치하는 범위에서만 정당화될 수 있다.

현행 형사소송법은 위와 같은 개인정보의 취득에 대하여 강제수사의 하나로 특별히 그 요건이나 절차 등을 규정하고 있지 않다. 현재로서는 위와 같은 정보제공행위를 규율할 수 있는 법적 근거는 개인정보 보호법 제18조 제2항이 있을 뿐이다.

입법론적으로 볼 때에는, 수사기관(또는 법원)이 다른 기관(공사불문)이 수집하여 저장하고 있는 개인정보를 조회하거나 검색하여 필요한 정보를 추출할 필요가 있는 경우에는 법률에 엄격한 요건과 절차를 규정하여 제한된 범위에서만 허용하도록 해야 한다. 정보제공요청이 특정 개인의 신상정보가 아니라 불특정 다수의 개인정보의 검색을 요하는 것이라면 압수수색영장에 준하는 법관의 영장(정보검색 및 정보수집영장)을 발부받도록 규정해야 한다.[31]

다) 개선제안

“수사”를 위하여 개인정보의 조회와 검색이 필요한 경우에 대비하여 형사소송법에 이를 위한 별도의 규정을 마련하여 허용요건을 명확하고 엄격하게 규정하고 절차상으로는 법원의 영장(정보검색영장)을 발부받아 개인정보의 조회와 검색이 가능하도록 규정해야 한다.

경찰이 “위험방지” 업무를 위하여 다른 기관이 보유한 개인정보에 대한 검색을 하는 것은 테러나 마약범죄, 조직범죄 등 매우 중대한 범죄에 한하여 그러한 범죄의 현실적인 위험이 존재하는 경우에 한하여, 그리고 달리 위험야기자를 특정할 방법이 없다는 보충성원칙 하에서 예외적으로만 허용하도록 규정을 마련해야 한다.

2. 통신 정보

가. 통신자료

통신자료 제공요청은「전기통신사업법」제83조에 의거하여 수사기관이 통신사업자에게 수사관서장의 요청서를 제시하고 수사 대상자의 인적사항을 요청하

31) 이에 관해서는 독일 형사소송법 제98조의 a b 참조.

는 제도이다. 검찰·경찰 정보수사기관은 검사, 4급이상 공무원, 총경 등이 결재한 제공요청서를 사업자에게 제시하여 이용자 성명, 주민등록번호, 주소, 전화번호, 가입 및 해지일자, ID를 제공요청할 수 있다.[32] 그러나 통신자료 제공요청은 법원의 허가서 없이도 수사기관이 손쉽게 개인정보를 얻을 수 있어 남용되고 있다는 비판이 제기되고 있다.

<표 Ⅱ-3> 통신자료 제공 현황 (문서별)

	검찰	경찰	국정원	기타기관	합계
2005	63,692	244,132	6,399	28,548	342,771
2006	63,408	221,311	6,313	32,534	323,566
2007	72,764	305,281	7,623	40,740	426,408
2008	91,611	331,977	8,384	42,596	474,568
2009	87,932	412,884	10,478	50,173	561,467
2010	99,534	431,062	10,686	49,767	591,049
2011	115,834	473,109	10,077	52,165	651,185

* 출처: 방송통신위원회 통계 재구성

<표 Ⅱ-4> 통신자료 제공 현황 (전화번호/ID 건수별)

	검찰	경찰	국정원	기타기관	합계
2005	881,954	2,103,661	58,976	145,320	3,189,911
2006	947,369	2,069,948	43,184	151,808	3,212,309
2007	873,423	3,257,258	49,995	143,730	4,324,406
2008	1,061,553	3,770,259	55,090	268,949	5,155,851
2009	984,611	5,351,080	72,089	471,964	6,879,744
2010	1,323,176	5,419,365	76,018	326,233	7,144,792
2011	1,295,968	3,958,055	102,979	491,989	5,848,991

* 출처: 방송통신위원회 통계 재구성

32)「전기통신사업법」제83조 ③ 전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사(「조세범 처벌법」 제10조제1항·제3항·제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출(이하 “통신자료제공”이라 한다)을 요청하면 그 요청에 따를 수 있다. 1. 이용자의 성명 2. 이용자의 주민등록번호 3. 이용자의 주소 4. 이용자의 전화번호 5. 이용자의 아이디(컴퓨터시스템이나 통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호를 말한다) 6. 이용자의 가입일 또는 해지일

방송통신위원회가 연2회 발표하는 통신자료 제공 현황에 따르면 2011년 경찰이 요청한 통신자료요청 문서건수는 47만 3109건에 달하여 이는 전체건수 대비 72.6%에 해당한다. 수사기관이 제공받은 전화번호 수 역시 꾸준히 증가하였는데, 2010년에는 경찰이 제공받은 전화번호는 541만 9365건(75.8%)에 달한다.

방송통신위원회가 발표한 통계에 따르면 기타기관의 통신자료 제공이 증가하고 있는데, 기타기관에는 국방부 및 국군기무사령부, 관세청, 법무부, 노동부, 식약청 등 사법경찰권이 부여된 행정부처를 포함하고 있다. 이처럼 통신자료는 광범위하게 제공되고 있으며 전기통신사업법에 규정되지 않은 제3자의 제공 요청이 통제되지 않고 있다. 이러한 점을 이용하여 범죄 수사 목적 외로 광범위한 사이버 사찰에 남용될 위험이 있다.

최근에는 경찰이 전기통신사업자를 경유하지 않고 직접 인권단체 자유게시판에 대한 통신자료 제공요청을 하였고, 심지어 통신비밀보호법이 정하고 있는 '통신사실확인자료'에 해당하는 접속IP를 요구하여 물의를 빚었다. 전기통신사업자는 전기통신사업법 제 83조 제6항에 의거하여 대통령령으로 정하는 방법에 따라 통신자료 제공을 한 현황 등을 연 2회 방송통신위원회에 보고하도록 하고 있다.[33] 그러나 수사기관이 전기통신사업자를 경유하지 않고 직접 통신자료를 취득하게 되면 방송통신위원회의 통계에도 포함되지 않게 된다. 통신사업자가 아닌 단체나 개인에게 행해지는 통신자료 제공요청은 그 남용을 방지하고자 하는 전기통신사업법의 입법취지를 교묘하게 회피하는 것이다.

나. 통신사실확인자료

통신사실확인자료요청은 통신비밀보호법 제13조에 따라 수사기관이 법원의 허가를 받아 전기통신사업자에게 수사 대상자의 통신사실확인자료를 요청하는 제도이다. 검찰, 경찰, 국정원 등 수사기관이 법원의 허가를 받아 자료제공을 요청한 경우 제공할 수 있다. 다만, 법원허가를 받기 어려운 긴급 상황 시에는 요청서만으로 통신사실확인자료를 제공하고, 제공 후 법원허가서를 제출 받을 수 있다.[34] 제공요청사항으로 상대방 전화번호, 통화일시 및 시간 등 통화사실

33) 「전기통신사업법」 제83조 ⑥ 전기통신사업자는 대통령령으로 정하는 방법에 따라 통신자료제공을 한 현황 등을 연 2회 방송통신위원회에 보고하여야하며, 방송통신위원회는 전기통신사업자가 보고한 내용의 사실 여부 및 제5항에 따른 관련 자료의 관리 상태를 점검할 수 있다.

34) 통신비밀보호법 제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차 <개정 2005.5.26>) ① 검사

과 인터넷 로그기록 접속지자료(IP Address)및 발신기지국 위치추적자료 등이 있다.[35]

<표 Ⅱ-5> 통신사실확인자료 제공 현황 (문서별)

	검찰	경찰	국정원	기타기관	합계
2005	29,631	149,802	4,982	10,954	195,369
2006	25,004	116,052	832	8,855	150,743
2007	28,301	143,316	922	11,120	183,659
2008	42,597	156,796	1,274	12,078	212,745
2009	42,059	193,790	1,719	10,984	248,552
2010	44,940	186,396	1,688	5,845	238,869
2011	45,471	183,110	1,264	5,871	235,716

* 출처: 방송통신위원회 통계 재구성

방송통신위원회가 발표한 통계에 따르면 통신사실확인자료제공이 증가하다가 법원허가를 요하는 절차규정이 개정 적용된 2006년경 경찰과 국정원의 제공요청이 감소한 것을 볼 수 있다. 2009년부터 경찰이 제공받은 전화번호, 아이디 건수가 크게 증가한 것을 볼 수 있는데 이는 종전에 통계에 잡히지 않던 형사소송법상 '압수수색영장'에 의한 기지국 단위의 압수수색이 통신비밀보호법상 '통신사실확인허가서'로 대체됨에 따라 기지국 수사 통계가 2009년부터 편입되었기 때문이다.

또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다. ②제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다. <개정 2005.5.26> ③제2항 단서의 규정에 의하여 긴급한 사유로 통신사실확인자료를 제공받았으나 지방법원 또는 지원의 허가를 받지 못한 경우에는 지체 없이 제공받은 통신사실확인자료를 폐기하여야 한다. <개정 2005.5.26>

35) 통신비밀보호법 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2001.12.29, 2004.1.29, 2005.1.27> 11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다. 가. 가입자의 전기통신일시 나. 전기통신개시·종료시간 다. 발·착신 통신번호 등 상대방의 가입자번호 라. 사용도수 마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료 바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료 사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

<표 Ⅱ-6> 통신사실확인자료 제공 현황 (전화번호/ID 건수별)

	검찰	경찰	국정원	기타기관	합계
2005	127,070	623,162	35,467	31,086	816,785
2006	124,089	429,539	12,499	39,399	605,526
2007	91,708	660,830	10,480	28,216	791,234
2008	113,636	305,570	4,048	23,646	446,900
2009	110,400	14,597,080	5,973	1,369,504	16,082,957
2010	133,802	39,229,941	6,373	21,104	39,391,220
2011	166,452	36,736,650	4,789	396,991	37,304,882

* 출처: 방송통신위원회 통계 재구성

경찰이 제공받은 통신사실확인자료 문서건수는 2011년 18만 3110건(77.6%)이고 전화번호 수는 3673만 6650건(98.4%)에 달한다. 수사기관이 '수사 또는 형의 집행을 위하여 필요한 경우'만으로 통신사실 확인자료의 제공을 요청할 수 있고 통신사실확인자료 허가서는 기간제한, 범위제한 등의 구체적인 요건이 규정되어 있지 않아 무분별한 남용이 우려되는 상황이다. 경찰의 통신사실확인자료 기각률은 2007년 3%였던 것이 2012년 7월에는 12.2%에 달한다. 기각률이 급격히 늘어나는 것은 제공 요청을 남발하고 있다는 사실의 방증이다.

<표 Ⅱ-7> 경찰의 통신사실확인자료 허가현황 (문서건수)

구분	신청	허가	기각 (기각률)
2007년	57,184	55,484	1,700 (3.0%)
2008년	60,077	58,123	1,954 (3.3%)
2009년	67,397	65,091	2,306 (3.4%)
2010년	67,829	63,191	4,638 (6.8%)
2011년	67,334	60,337	6,997 (10.4%)
'12년 7월말	32,295	28,355	3,940 (12.2%)

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

또한, 긴급한 사유가 있는 때는 법원의 허가를 사후에 받도록 하였고, 긴급한 사유가 무엇인지에 대해서는 법률에 규정을 두고 있지 않다. 이로 인하여 긴급 규정이 오·남용 될 소지가 크다. 긴급 통신사실확인자료의 기각률도 증가하는 추세이며 2012년 7월 기준 기각률은 12.5%에 달한다.

<표 Ⅱ-8> 경찰의 긴급 통신사실확인자료 허가현황 (문서건수)

구분	신청	허가	기각 (기각률)
2007년	3,889	3,766	123 (3.16%)
2008년	3,819	3,645	174 (4.55%)
2009년	3,682	3,540	142 (3.85%)
2010년	2,644	2,458	186 (7.03%)
2011년	2,045	1,832	213 (10.4%)
’12년 7월말	1,293	1,131	162 (12.5%)

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

죄종별 현황을 보면 기타, 절도, 사기, 폭력 등, 강도, 살인, 강간, 횡령배임 순이며 기타범죄가 40%대로 제일 많이 비율을 차지하고 있다.

<표 Ⅱ-9> 경찰의 통신사실확인자료 제공 죄종별 현황 (집행건수)

구 분	계	살인	강도	강간 등	절도	폭력 등	사기	횡령 배임	기타
2007년	55,105	1,565	2,770	761	13,418	5,084	9,792	272	21,443
2008년	57,826	1,436	2,835	981	13,703	5,566	8,794	302	24,209
2009년	64,666	1,685	3,739	1,069	18,243	5,055	9,865	370	24,640
2010년	63,877	837	2,732	1,605	17,614	4,766	10,189	591	25,543
2011년	62,006	906	2,531	1,725	15,957	4,578	10,721	653	24,935
’12. 7월	26,879	354	867	700	6,090	2,146	4,919	239	11,564

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

다. 기지국수사

방송통신위원회는 수사기관이 용의자를 특정할 수 없는 연쇄범죄가 발생하거나, 동일 사건단서가 여러 지역에서 시차를 두고 발견될 경우, 사건발생지역 기지국에서 발신된 전화번호를 추적하여 수사를 전개하는 수사기법이 ‘기지국수사’라고 밝히고 있다. 기지국수사는 특정 시간대 특정 기지국에서 발신된 모든 전화번호를 대상으로 하므로, 허가서 1개에 통산 1만개 내외의 전화번호 수가 방송통신위원회 통계로 집계된다. 법원은 종전에 기지국수사 필요시 형사소송법상 압수수색영장을 발부하던 것을 통신비밀보호법상 통신사실확인허가서로도

발부함에 따라 2010. 4. 2. 방송통신위원회의 「09년 하반기 통신사실확인자료 제공 등 협조현황」 통계에 반영되어 기지국 수사의 존재가 처음 알려졌다. 그러나 경찰은 기지국수사와 관련된 통계를 밝히지 않고 있어 방송통신위원회가 연2회 발표하는 통계만 있을 뿐 기지국수사를 어떤 범죄에 많이 쓰이는지 등 정확한 실태 파악은 어려운 상황이다.[36]

<표 Ⅱ-10> 통신사실확인자료 중 기지국 수사 자료 제공 현황

구분	2009하반기	2010상반기	2010하반기	2011상반기	2011하반기
요청 문서건수	1,257	1,846	2,150	2,473	2,143
요청 전화번호 수	15,440,864	21,306,989	17,399,997	20,567,569	16,232,806

* 출처: 방송통신위원회 통계

<표 Ⅱ-11> 통신사실확인자료 중 기지국 수사 비율

구분	전체 요청 문서건수	기지국수사 문서건수	전체 요청 전화번호 수	기지국수사 전화번호 수	기지국수사 문서건수 비율	기지국수사 전화번호수 비율
2009하반기	122,181	1,257	15,778,887	15,440,864	1.02%	97.85%
2010상반기	117,941	1,846	21,598,413	21,306,989	1.56%	98.65%
2010하반기	120,928	2,150	17,792,807	17,399,997	1.77%	97.79%
2011상반기	124,658	2,473	20,842,056	20,567,569	1.98%	98.68%
2011하반기	111,058	2,143	16,462,826	16,232,806	1.92%	98.60%

* 출처: 방송통신위원회 통계 재구성

통신사실확인자료 전체 요청 문서건수 중 기지국 수사 문서건수는 1~2%내로 낮은 비율을 차지하고 있는 반면, 전화번호 수를 보면 기지국수사 전화번호 제공이 평균 98%로 압도적으로 높은 비율을 차지하고 있다. 이는 기지국수사가 허가서 1건 당 과도하게 많은 수의 전화번호를 제공받고 있음을 의미한다.

기지국 수사는 실제로 범죄가 발생하지도 않았는데도 단지 범죄가 발생하였

36) 2010년 인권단체에서 서울중부,중랑,종암,종로,은평,용산,영등포,양천,수서,송파,성북,성동,서초,서부,서대문,방배,마포,동작,동대문,도봉,노원,남대문,금천,구로,광진,관악,강서,강북,강동,강남,혜화경찰서 이하 31곳을 대상으로 기지국 수사방식의 실태 및 통계를 정보공개 청구하였지만 자료가 존재하지 않는다는 등의 이유로 비공개하였다.

다고 의심이 되는 장소라는 이유로 해당 장소를 관할하는 기지국을 이용한 모든 사람들의 착·발신 시간, 통화 시간, 수·발신 번호, 즉 사실상 발신인과 수신인의 성명, 발신지, 수신과 발신의 연원일, 통신의 횟수와 시간과 형태 등 통신에 관한 정보들을 무차별적으로 수집하여 범죄의 혐의가 없는 사람들의 통신비밀과 위치정보를 수사기관이 보유함으로써 통신비밀의 자유, 사생활의 비밀과 자유, 개인정보자기결정권을 침해한다는 비판이 제기되고 있다.

라. 통신감청

통신감청은 통신비밀보호법 제5조, 제6조, 제7조, 제8조에 따라 수사기관이 수사 대상자의 통신내용을 확인하는 제도로, 법원의 허가서를 통신사업자에게 제시하고 감청집행에 관한 협조를 요청하는 제도이다. 일반감청은 검찰, 경찰, 국정원 등 수사기관이 법원의 허가서를 받아 협조를 요청한 경우에 한해 감청 협조를 할 수 있고, 긴급감청은 검사 지휘서 또는 국정원장 승인서로 우선 감청 협조하되, 36시간 내 법원의 허가서를 제출 받아야 한다. 확인사항으로는 통화내용, 전자우편, 비공개모임 게시 내용 등이 있다.

<표 II-12> 통신감청 현황 (문서별)

	검찰	경찰	국정원	군수사기관등	합계
2005	52	197	639	89	977
2006	35	99	870	29	1,033
2007	24	81	1,010	34	1,149
2008	18	75	1,043	16	1,152
2009	9	145	1,320	42	1,516
2010	2	186	856	37	1,081
2011	3	181	481	42	707

* 출처: 방송통신위원회 통계

<표 Ⅱ-13> 통신감청 현황 (통신수단별)

	유선전화	이동전화	무선호출	PC통신·인터넷	합계
2005	621	1	0	355	977
2006	577	0	0	456	1,033
2007	503	0	0	646	1,149
2008	506	0	0	646	1,152
2009	574	0	0	942	1,516
2010	358	0	0	723	1,081
2011	261	0	0	446	707

* 출처: 방송통신위원회 통계

<표 Ⅱ-14> 통신감청 현황 (전화번호/아이디건수별)

	검찰	경찰	국정원	군수사기관등	합계
2005	100	241	8,082	112	8,535
2006	43	131	8,440	51	8,665
2007	41	95	8,628	39	8,803
2008	24	94	8,867	19	9,004
2009	9	163	9,278	47	9,497
2010	4	227	8,391	48	8,670
2011	3	263	6,840	61	7,167

* 출처: 방송통신위원회 통계

전체 감청건수와 인터넷 감청 비율이 급증하고 있으며 인터넷 패킷감청기술이 알려진 2009년에는 인터넷접속, 이메일, 비공개모임의 게시내용 등을 감청할 수 있는 인터넷감청이 942건으로 사상 최고치에 달했다. 전체적으로 국정원 비율이 압도적으로 높으나, 2010년부터 경찰 비율이 증가하기 시작하였다.

전기통신사업자를 거치는 간접감청의 경우 방송통신위원회의 통계에 잡히지만, 정보수사기관의 직접감청의 실태는 사실상 알려져 있지 않다. 2009년 국정감사 결과 국가정보원이 인터넷 패킷감청장비 31대를 보유하고 패킷감청을 실시하고 있다는 사실이 밝혀졌다.

<표 Ⅱ-15> 경찰청 감청기기 사용현황(직접감청)

구분	'07년	'08년	'09년	'10년 6월말
보유 감청기기 사용회수	24	6	12	0

* 출처: 2010년 국회 행정안전위원회 국정감사 최규식 의원 답변자료

감청 기관 중 일반범죄수사를 담당하지 않는 국가정보원의 감청 비율이 압도적으로 높다는 사실이 기형적이지만, 경찰 감청 역시 그 죄종별 현황을 보면 국가보안법의 비중이 높다는 사실을 알 수 있다.

<표 Ⅱ-16> 경찰청 및 경찰청 보안국 감청 죄종별 현황 (집행건수)

구 분	계	살인	강도	강간	감금 협박	약취 유인	마약	국가 보안	기타
2007년	30	17	4	·	3	2	·	14	4
2008년	15	10	1	·	2	1	·	18	1
2009년	14	9	3	·	·	2	·	24	·
2010년	7	2	1	2	·	1	·	28	1
2011년	4	2	·	·	·	·	·	30	2
'12. 7월	7	3	·	·	4	·	·	13	·

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

이처럼 감청은 국가보안법 수사를 위하여 오남용되는 경향이 있으며 그만큼 법원심사가 엄격하지 않다는 방증이다. 범죄수사를 위한 감청의 허가요건에 개연성 요건을 추가하고 허가서 기재 사항을 확대할 필요 있다. 감청의 1회 실시기간 역시 단축할 필요가 있으며, 대상자 식별이 사실상 불가능한 인터넷패킷 감청은 중단되어야 한다. 무엇보다 감청 집행 중 입회나 감독이 이루어지고 있지 않다는 사실은 감청에 대한 통제가 사실상 전무하다는 말이나 다름이 없으며, 감청 자료 보관에 대한 규정이 없어 당사자 열람권과 변호권이 제한되고 있다. 감청이 집행기관의 처분과 발췌에 의존하는 것은 큰 문제인 만큼, 입회인 제도, 봉인 후 법원 보관, 당사자 열람권 등을 보완할 필요가 있다. 또한 국가안보를 위한 통신제한조치의 요건과 절차를 강화할 필요가 있으며 긴급통신제한조치는 삭제하여야 한다.

마. 송·수신이 완료된 전기통신의 압수·수색·검증

형사소송법상 일반 압수·수색·검증 규정에 의하여 수사기관은 비공개모임게시내용, 전자우편 등 통신내용을 제공받고 있다. 2008년 최문순 의원에 따르면 비공개모임게시내용, 전자우편 등 압수수색 영장에 의한 통신내용 제공현황이 2008년 상반기에 눈에 띄게 폭증했던 바 있다. 미국산 광우병 쇠고기 수입에 반대하는 촛불시위가 크게 일었던 해에 특히, 다음(Daum)의 경우에는 여타 통신사업자에 비해 전자우편에 대한 아이디 감청이 50배 이상 월등히 많았고, 경찰 아이디감청이 324% 증가하여 오남용 우려를 낳았다.

<표 Ⅱ-17> 송수신이 완료된 전기통신 제공 현황 (문서건수/아이디수)

구 분		내용	검찰	경찰	국정원	군수사기관	계
다음	2006 (상)	비공개모임게시내용	-	4/22	1/1	1/5	6/28
		전자우편	25/118	132/328	26/54	13/27	196/527
	2007 (상)	비공개모임게시내용	1/1	6/24	-	-	7/25
		전자우편	32/140	165/4473	35/57	17/35	249/4705
	2008 (상)	비공개모임게시내용	1/1	27/133	20/39	4/19	52/192
		전자우편	64/589	269/29833	62/115	35/43	445/30607
네이버	2006 (상)	비공개모임게시내용	-	2/80	-	-	2/80
		전자우편	20/31	46/76	7/8	2/2	75/117
	2007 (상)	비공개모임게시내용	-	2/2715	-	-	2/2715
		전자우편	20/58	96/152	22/24	13/18	151/252
	2008 (상)	비공개모임게시내용	-	11/882	1/1	2/4	14/887
		전자우편	48/120	163/404	38/48	34/36	273/608
야후	2006 (상)	비공개모임게시내용	-	-	-	-	-
		전자우편	8/10	14/19	2/3	3/3	27/35
	2007 (상)	비공개모임게시내용	-	-	-	-	-
		전자우편	11/19	13/15	4/4	2/2	30/40
	2008 (상)	비공개모임게시내용	-	-	-	-	-
		전자우편	26/42	46/66	8/9	7/7	87/124

* 출처: 2008년 국회 문화체육관광방송통신위원회 국정감사 최문순 의원 자료

범죄 사실 입증과 무관한 장기간의 이메일이 압수수색 검증됨에 따라 때로 사상검증의 수단으로 악용되고 있는 것은 큰 문제이다. 송·수신이 완료된 전기통신의 압수·수색·검증을 통신비밀로서 보호하고 통계를 공개해야 할 필요가 있다. 2010년 9월 8일 국가인권위원회는 「형사소송법 일부개정법률안」,「통신비밀보호법 일부개정법률안」 중 전자우편의 압수 수색 및 통신제한조치 관련 규정에 대하여 다음과 같은 의견을 표명하였다.

① 송수신이 완료된 저자우편에 대한 압수수색 등의 강제처분의 요건 및 절차 등에 관하여 명시적인 법률규정을 두어야 한다.
② 송수신이 완료된 전자우편에 대한 압수수색의 대상을 특정하여야 한다.
③ 수사대상자에 대하여 전자우편의 압수 수색 사실이 통지되어야 한다.
④ 수사대상자 및 그 변호인이 전자우편을 압수 수색하는 집행절차에 참여하여야 한다.
⑤ 개정법률안은 수사상 불필요한 정보의 환부 및 삭제에 대해 충분히 언급하고 있지 않으나 기본적으로 수사 목적 달성에 필요하지 않은 전자우편은 환부되거나 삭제되어야 하는 것이 타당하다.

이메일 등 송수신이 완료된 전기통신에 대한 압수·수색·검증에 대한 통지 제도가 신설된 '09. 5. 28. 통신비밀보호법 개정조항 발효에 따라 그 실태가 다음과 같이 집계되고 있다.

<표 Ⅱ-18> 송수신이 완료된 전기통신에 대한 압수·수색·검증 집행건수

구분	2009. 5. 28 ~ 12. 31	2010년	2011년	2012년 7월말
집행건수	873	652	358	80

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료
* 이메일 뿐 아니라 기지국 통화내역 등 모든 전기통신에 대한 압수·수색·검증 집행 건을 포함.

바. GPS 위치정보

기지국, GPS 등 위치정보는 모바일 시대에 개인의 행적을 파악할 수 있는

민감한 개인정보로서, 수사기관의 수집 뿐 아니라 사기업의 광범위한 수집 문제가 전 세계적으로 불거지고 있다. 휴대전화 기지국의 실시간 위치추적의 경우, 통화가 발생하지 않더라도 매 10분 또는 30분 간격으로 자동으로 단말기 위치를 확인하여 그 위치정보를 담당 수사관의 휴대폰 SMS로 발송하는 방법으로 물의를 빚어 왔으며[37], 장기간에 걸친 위치추적 사례도 발생하고 있다. 이에 '희망버스' 기획단에 대한 휴대전화 기지국의 실시간 위치추적 사건의 경우에는 영장주의 위반 등의 이유로 헌법소원이 제기되었다.

휴대전화 GPS 위치정보 제공은 그간 「위치정보의 보호 및 이용 등에 관한 법률」 제 29조[38]에 의거하여 소방방재청과 해양경찰청이 '긴급구조 목적으로' 통신회사로부터 제공받아 왔으며 경찰은 소방방재청과 업무협약에 의하여 소방방재청으로부터 자료를 제공받아 왔다.

최근 수원 여성 살인사건 이후 경찰은 위치정보법을 개정하여 별도의 영장 없이 위치정보를 경찰관서에도 제공할 수 있도록 하였으며 이 법은 2012년 11월 15일부터 시행될 예정이다. 그러나 실시간 GPS 위치정보는 사생활 침해 소지가 매우 크기 때문에, 이를 수사기관에 제공하는 것은 현행 통신사실확인자료 제공보다 엄격한 요건이 필요하다는 지적이 일고 있다. 2012년 1월 23일 미국 연방대법원은 GPS 장치를 이용하여 차량 이동을 실시간으로 감시하여 피의자를 검거한 사건에서, GPS 실시간 위치추적을 '수색'이라고 판단하고 해당 시점과 지역에 대한 수색을 허용하는 일반영장이 없는 이상 이 같은 위치추적 수사는 위법하다는 취지의 판결을 선고한 바 있다(U.S. v. Jones).

3. 금융 정보

금융 정보는 통신 정보 제공의 경우보다 그 제공 요건이 엄격하다. 금융거래 내역의 경우 「금융실명거래 및 비밀보장에 관한 법률」 제4조 제1항 제1호에

37) "경찰 '문지마 감청'…사후통보 시늉만", 한겨레, 2009.1.14.

38)「위치정보의 보호 및 이용 등에 관한 법률」제29조(긴급구조를 위한 개인위치정보의 이용) ① 「재난 및 안전관리 기본법」 제3조제7항의 규정에 따른 긴급구조기관(이하 "긴급구조기관"이라 한다)은 급박한 위험으로부터 생명·신체를 보호하기 위하여 개인위치정보주체, 개인위치정보주체의 배우자, 2촌 이내의 친족 또는 「민법」 제928조의 규정에 따른 후견인(이하 "배우자등"이라 한다)의 긴급구조요청이 있는 경우 긴급구조 상황 여부를 판단하여 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있다. 이 경우 배우자등은 긴급구조 외의 목적으로 긴급구조요청을 하여서는 아니된다. <개정 2006.9.27> ④위치정보사업자는 제1항의 규정에 의하여 개인위치정보를 긴급구조기관에게 제공하는 경우 개인위치정보의 제공사실을 당해 개인위치정보주체에게 즉시 통보하여야 한다.

따라 법원의 제출명령 또는 법관이 발부한 영장에 의한 거래정보 등을 제공할 수 있다.

금융실명거래 및 비밀보장에 관한 법률
제4조(금융거래의 비밀보장) ① 금융기관에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 “거래정보 등”이라 한다)를 타인에게 제공하거나 누설하여서는 아니되며, 누구든지 금융기관에 종사하는 자에게 거래정보 등의 제공을 요구하여서는 아니된다. 다만, 다음 각 호의 1에 해당하는 경우로서 그 사용목적에 필요한 최소한의 범위안에서 거래정보 등을 제공하거나 그 제공을 요구하는 경우에는 그러하지 아니하다.
1. 법원의 제출명령 또는 법관이 발부한 영장에 의한 거래정보등의 제공

신용카드 거래내역 역시 「신용정보의 이용 및 보호에 관한 법률」 제32조 제4항 제5호에 따라 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우에 제공 할 수 있다.

신용정보의 이용 및 보호에 관한 법률
제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 대출, 보증에 관한 정보 등 대통령령으로 정하는 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 개인으로부터 다음 각 호의 어느 하나에 해당하는 방식으로 미리 동의를 받아야 한다.
④ 신용정보회사등이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제3항까지를 적용하지 아니한다.
5. 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우

그러나 2011년 7월 ‘2차 희망버스’ 관련 경찰이 아무런 범죄혐의 없이 단순 참가비를 납부한 30명의 시민의 인적사항을 무차별적으로 조회하여 인권침해 논란이 빚어졌다.[39]

4. DNA 정보

수사기관은「디엔에이신원확인정보의 이용 및 보호에 관한 법률」에 의거하여 DNA 정보를 수집 및 이용하고 있다. 검사 또는 사법경찰관은 법령에 열거된 11종의 죄를 범하여 구속된 피의자의 경우 치료감호대상자로부터 DNA감식

39) “‘희망버스’참가자 무차별 금융조회 논란”, 오마이뉴스, 2012.1.28.

시료를 채취 받을 수 있다. 동의하지 않는 경우 검사의 청구로 법원에서 발부한 영장에 의하여 채취할 수 있다. 채취된 DNA감식시료는 감식 후 DNA신원확인정보 형태로 데이터베이스에 수록하여 경찰총장이 관리하고 시료는 폐기한다. 검사 또는 법원에서 혐의없음, 무죄 등의 처분이나 판결 등이 있는 경우에는 삭제하지만 치료감호하는 경우는 제외된다.

또한 검사 또는 사법경찰관은 범죄현장이나 피해자, 용의자의 신체와 물건 등에서 DNA감식시료를 채취할 수 있지만, 데이터베이스 수록은 그 신원이 밝혀지지 않은 것에 한정하여 이루어진다.

디엔에이신원확인정보의 이용 및 보호에 관한 법률

제6조(구속피의자등으로부터의 디엔에이감식시료 채취) 검사 또는 사법경찰관(군사법경찰관을 포함한다. 이하 같다)은 제5조제1항 각 호의 어느 하나에 해당하는 죄 또는 이와 경합된 죄를 범하여 구속된 피의자 또는 「치료감호법」에 따라 보호구속된 치료감호대상자(이하 “구속피의자등”이라 한다)로부터 디엔에이감식시료를 채취할 수 있다. 다만, 제5조에 따라 디엔에이감식시료를 채취하여 디엔에이신원확인정보가 이미 수록되어 있는 경우는 제외한다.

제7조(범죄현장등으로부터의 디엔에이감식시료 채취) ① 검사 또는 사법경찰관은 다음 각 호의 어느 하나에 해당하는 것(이하 “범죄현장등”이라 한다)에서 디엔에이감식시료를 채취할 수 있다.

1. 범죄현장에서 발견된 것
2. 범죄의 피해자 신체의 내·외부에서 발견된 것
3. 범죄의 피해자가 피해 당시 착용하거나 소지하고 있던 물건에서 발견된 것
4. 범죄의 실행과 관련된 사람의 신체나 물건의 내·외부 또는 범죄의 실행과 관련한 장소에서 발견된 것

② 제1항에 따라 채취한 디엔에이감식시료에서 얻은 디엔에이신원확인정보는 그 신원이 밝혀지지 아니한 것에 한정하여 데이터베이스에 수록할 수 있다.

제8조(디엔에이감식시료채취영장) ① 검사는 관할 지방법원 판사(군판사를 포함한다. 이하 같다)에게 청구하여 발부받은 영장에 의하여 제5조 또는 제6조에 따른 디엔에이감식시료의 채취대상자로부터 디엔에이감식시료를 채취할 수 있다.

② 사법경찰관은 검사에게 신청하여 검사의 청구로 관할 지방법원판사가 발부한 영장에 의하여 제6조에 따른 디엔에이감식시료의 채취대상자로부터 디엔에이감식시료를 채취할 수 있다.

③ 제1항과 제2항의 채취대상자가 동의하는 경우에는 영장 없이 디엔에이감식시료를 채취할 수 있다. 이 경우 미리 채취대상자에게 채취를 거부할 수 있음을 고지하고 서면으로 동의를 받아야 한다.

④ 제1항 및 제2항에 따라 디엔에이감식시료를 채취하기 위한 영장(이하 “디엔에이감식시료채취영장”이라 한다)을 청구할 때에는 채취대상자의 성명, 주소, 청구이유, 채취할 시료의 종류 및 방법, 채취할 장소 등을 기재한 청구서를 제출하여야 하며, 청구이유에 대한 소명자료를 첨부하여야 한다.

⑤ 디엔에이감식시료채취영장에는 대상자의 성명, 주소, 채취할 시료의 종류 및 방법, 채

취할 장소, 유효기간과 그 기간을 경과하면 집행에 착수하지 못하며 영장을 반환하여야 한다는 취지를 적고 지방법원판사가 서명날인하여야 한다.
⑥ 디엔에이감식시료채취영장은 검사의 지휘에 의하여 사법경찰관리가 집행한다. 다만, 수용기관에 수용되어 있는 사람에 대한 디엔에이감식시료채취영장은 검사의 지휘에 의하여 수용기관 소속 공무원이 행할 수 있다.

<표 Ⅱ-19> 법률 시행 이후 현재까지 경찰의 DNA 정보 채취 현황
(2010. 7. 26 법 시행 이후부터 2012. 8. 31기준 통계)

구분	계	구속피의자(제6조)	범죄현장 증거물(제7조)
채취현황	58,596건	23,818명	34,778건

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

그러나 디엔에이법 제6조 채취 건수의 죄명별 사유를 구분하여 보면, 이 법의 제정 취지로 알려졌던 성폭력 관련 범죄의 비율보다, 폭력행위 등 다른 범죄의 비중이 훨씬 높다. 2009년 용산 참사와 쌍용자동차 노동조합 옥쇄 파업에 참여하였던 철거민과 노동자에 이 법 시행에 따른 DNA 채취가 요구되어 이에 대한 헌법소원이 제기된 상태이다.

<표 Ⅱ-20> 법 제6조에 따른 채취 죄명별 채취 건수 및 비율

구분	방화 실화	살인	약취 유인	강간 추행	절도	강도	폭력 행위	특가법	성폭력	마약	아동청소년성보호법	계
제6조 채취	478	1,717	62	1,619	4,111	2,994	3,278	3,475	2,917	2,221	946	23,818

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료 재구성

형이 확정되지 않은 구속피의자의 DNA도 채취하고 있다는 것은 근본적인 문제이며, 그 재범 가능성을 DNA 보관으로 억제할 수 있다고 보기 어려운 광범위한 범죄를 채취 대상으로 하고 있는 것 역시 문제이다.

특히 법률에 명확한 내용이 규정되어 있지 않은 수사 중인 사건 용의자 DNA 채취의 경우, 무려 1100명에 이르는 집단채취가 이루어지는 등[40], 동의를 명분으로 한 사실상의 강제 채취가 이루어지고 있다는 비판이 높다.

40) "경찰 1100여명 유전자 마구잡이 채취", 한겨레, 2011.1.28.

궁극적으로 DNA 채취와 데이터베이스 제도 자체의 인권 침해성을 최소화해야한다. 우선, DNA 데이터베이스를 폐지하거나, 유지하더라도 너무 광범위한 채취 대상범죄를 성폭력범죄 등 DNA 채취와 직접 관련이 있고 재범가능성이 있는 범죄로 최소화하고, 형이 확정되지 않은 구속피의자나 소년범을 제외해야 하며, 채취 여부의 궁극적인 판단은 법원이 해당 사건에 대한 판결 당시 부가처분으로 이루어질 필요가 있다. 이와 별도로 각 수사과정에서 DNA 채취와 활용에 대하여 상세하게 규정한 법률을 제정하여 강제 채취를 최소화하고 간접채취를 통한 오염 우려도 불식시킬 필요가 있다

5. 의료 정보

병원이 보유한 개인정보는 「의료법」에 의하여 형사소송이나 민사소송을 위하여 제공될 수 있다.

의료법
제21조(기록 열람 등) ① 의료인이나 의료기관 종사자는 환자가 아닌 다른 사람에게 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다. 〈개정 2009.1.30〉
② 제1항에도 불구하고 의료인이나 의료기관 종사자는 다음 각 호의 어느 하나에 해당하면 그 기록을 열람하게 하거나 그 사본을 교부하는 등 그 내용을 확인할 수 있게 하여야 한다. 다만, 의사·치과의사 또는 한의사가 환자의 진료를 위하여 불가피하다고 인정한 경우에는 그러하지 아니하다. 〈개정 2009.1.30, 2010.1.18〉
6.「형사소송법」 제106조, 제215조 또는 제218조에 따른 경우
7.「민사소송법」 제347조에 따라 문서제출을 명한 경우

그러나 형사소송이나 민사소송의 경우가 아니더라도 모든 의료정보는 건강보험심사평가원이나 건강보험공단을 통해 광범위한 목적으로 제공될 수 있다. 이 기관들을 규율한다고 볼 수 있는 개인정보 보호법은 '범죄의 수사와 공소의 제기 및 유지에 필요한 경우'나 '법률에서 정하는 소관 업무'를 수행해야 하는 공공기관의 경우, 수집된 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하도록 한 규정에 대한 예외를 인정하고 있다. 결국 의료 정보는 영장이나 그에 준하는 심사 없이도 경찰에 제공될 수 있는 것이다.

2009년 국가인권위원회 조사 의하면, 한 대학병원의 경우 수사협조 목적으로 경찰서에 제공되는 의료정보(성명, 주민등록번호, 병명, 치료내용, 치료결과 등)

가 연간 120건~150건 정도나 된다고 밝혀졌다[41]. 또한, 법원의 신체감정 의뢰에 대한 회신 건수도 2007년 363건, 2008년 504건, 2009년 327건에 달했다.

범죄수사 목적으로 경찰에 제공되는 경우가 적지 않지만 모두 영장에 의하고 있는지 확실치 않으며 막연한 치안정보 수집의 일환으로 제공될 가능성도 배제할 수 없다. 무엇보다 민감한 의료정보의 제공에 대하여 당사자에게 그 사실이 제대로 통보되지 않을 가능성이 크다는 점에서 제도적 보완이 필요하다.

41) 오병일·장여경·김지성·이은우·김철, 「개인정보 수집·유통 실태조사」, 국가인권위원회 용역보고서, 2009.

Ⅲ. 행정 작용과 개인정보 보호

1. 행정정보공동이용시스템

가. 문제 제기

행정정보 공동이용은 대표적인 전자정부 서비스이다.[1] 정부는 행정정보 공동이용센터(http://pr.share.go.kr) 구축을 통해 민원인이 제출해야 하는 구비서류를 대폭 감축함으로써 구비서류 발급을 위한 기관방문을 최소화하는 등 행정기관간에 정보공유를 지속적으로 추진 중이다. 주민등록등(초)본, 건축물대장, 납세증명서, 사업자등록증명 등 발급빈도가 높은 120종의 행정정보에 대해서는 구비서류를 제출할 필요없이 관련 기관이 공유하여 업무를 처리하도록 하고 있고, 행정정보 공동이용 대상정보 및 서비스가 확대됨에 따라 1일 이용률이 매년 지속적으로 증가하여 행정정보 공동이용을 통해 절감한 사회적 비용이 1조 4,000억 원에 이른다고 보도되고 있다. 행정정보를 공유하는 대상기관도 일부 행정기관에서 시작하여 2011년 현재는 모든 행정기관과 공공기관·은행 등 438개 기관으로 확대되어 운영 중이다.

그런데 행정정보의 공동이용으로 인해서 행정서비스가 신속하고 효율적으로 수행될 수 있는 반면, 개인정보의 침해가능성은 증가하게 되었다.[2] 국민들 또한 개인정보 공동이용의 효용성에도 불구하고 공공기관이 개인정보 DB를 구축하거나 그것을 다른 기관과 공유하는 것, 그리고 행정정보의 공동이용에 대해 전반적으로 부정적인 입장을 가지고 있다.[3] 특히 정부를 포함한 수많은 공공기

1) 행정안전부·방송통신위원회·지식경제부, 『2012 국가정보화백서』, 2012.
2) 장교식·조정은, "행정정보통신망 이용에 따른 개인정보침해에 관한 고찰", 토지공법연구 제51집 2010년 11월.
3) 성낙인·이인호·김수용·권건보·김삼용·이지은·김주영·손형섭·박진우·김송옥, 2008, "개인정보 보호법제에 관한 입법평가", 현안분석 2008-45, 한국법제연구원.

관들이 내부적으로 연결되어 사용되는 행정정보 공동이용의 특성상, 정보주체가 행정정보에 포함된 자신의 개인정보가 언제 어떤 식으로 사용되었는지에 대해서 파악하기 어려워 그 침해가 다른 경우보다 훨씬 심각할 것이라고 예상된다. 무엇보다 행정정보 공동이용의 법적 근거로 간주되는 「전자정부법」상 '공동이용'은 사실상 개인정보 공동이용에 관한 것인데 법은 '공동이용' 원칙을 천명하고 있어 개인정보 보호에 관한 법률상 규율을 형식화하는 측면이 있다.

따라서 행정정보통신망을 통한 정보공동이용으로 인한 개인정보의 침해 가능성과 현황에 대하여 면밀히 살펴보고 향후 관련 법제도가 나아가야 할 방향을 제시할 필요가 있다.

나. 행정정보 공동이용이란

현행 「전자정부법」은 제2조 제6호에서 행정정보란 "행정기관등이 직무상 작성하거나 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호, 문자, 음성, 음향, 영상 등으로 표현된 것"을 말한다고 규정하고 있다. '행정정보 공동이용'이라 함은 이러한 행정정보를 소관 직무과정의 일환으로 기관내부문 및 기관외부문 또는 기관과 개인 사이에 공동으로 함께 사용하는 것을 말한다고 할 수 있다.[4] 1998년 3월 28일에 제정되었다가 2001년 6월 30일 폐지된 「행정정보 공동이용에 관한 규정」에서는 '행정정보 공동이용'에 대하여 '행정기관이 보유·관리하고 있는 행정정보를 다른 행정기관이 정보통신망에 의하거나 디스켓·테이프 기타 이와 유사한 매체에 의하여 제공받아 이용하는 것'으로 정의한 바 있다. 한편 '행정정보공동이용시스템'이란, 「전자정부법」 제37조 및 같은 법 시행령 제42조에 따른 행정정보공동이용센터가 행정정보보유기관이 유지·관리하는 행정정보 데이터베이스 및 전자적 체계와 이용기관이 관리하는 전자적 체계를 연계하여 행정정보를 공동이용하기 위하여 구축·운영하는 시스템을 말한다(행정정보 공동이용 지침, 행정안전부예규 제492호, 제4호).

2001년 7월 1일 시행된 「전자정부구현을위한행정업무등의전자화촉진에관한법률」은 제2장에서 전자정부의 구현 및 운영 원칙으로 국민편익중심·업무혁신선행·전자적 처리·행정정보공개·행정기관 확인·행정정보 공동이용·개인정보보호·소프트웨어 중복개발방지·기술개발 및 운영 외주 등의 원칙을 명시적으로 규정

4) 이민영, "행정정보 공동이용의 추진 방향과 법적 과제", 정보통신정책 제 18 권 5호 통권 389호 (2006-3-16).

하였다. 특히 법 11조에서는 “행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다”고 하는 ‘행정정보공동이용의 원칙’을 천명하였다.

정보시스템을 통한 행정정보의 공동이용의 긍정적인 측면으로는 정보전달의 신속성·정확성 확보, 지리적·시간적 한계의 극복, 종이문서 사용 절약 등의 경제적 효과가 발생한다는 점을 꼽을 수 있다. 반면, 정보의 공동이용이 활발해질수록 개인정보가 침해될 가능성이 높아지며, 개인정보가 침해되었을 시에도 침해 여부를 쉽게 알 수 없을 뿐만 아니라 침해의 범위도 파악하기 힘들다. 또한 어떤 과정에서 정보가 침해되었는지 파악하기 어렵기 때문에 그 침해에 대한 책임 소재를 확정하는 것도 쉽지 않다.

다. 행정정보 공동이용의 연혁

범정부 차원의 행정정보 공동이용은 2002년 11월 행정정보공유서비스를 통해 주민등록등(초)본, 등기부등본 등 17종의 대장 및 공부를 공유하는 것에서 시작되었다. 정부는 행정정보 공동이용의 효율적 추진을 위해 2005년 10월 18일 국무총리와 민간위원장을 공동위원장으로 하는 행정정보공유추진위원회를 대통령 자문기구로 출범시키고, 위원회 운영을 지원하는 사무조직으로 같은 해 11월 행정정보공유추진단을 설치하였으며, 같은 해 12월 「행정정보 공유 종합계획」이 마련되었다.[5)]

행정정보공유추진단은 2008년 10월까지 3차에 걸쳐 행정정보 공동이용 확대 구축사업을 추진하였으며, 2008년 12월에는 행정정보 공동이용의 활성화와 서비스 확대를 위한 수요자 맞춤형 행정정보 공동이용체계 BPR/ISP를 실시하며 1세대를 마무리하였다.

2세대로 들어서는 2009년부터는 행정정보 공동이용 중기 전략계획을 수립하여, 행정기관의 보유정보 이외에 공공기관의 보유정보까지 확대하고 이용기관도 행정·공공·금융·교육·위임위탁기관까지 지속적인 확대를 진행하고 있다. 2009년 12월까지는 필수 정보 항목만을 추출·조합한 맞춤형 조회서비스 등을 제공할 수 있는 기반을 마련하는 수요자 맞춤형 행정정보 공동이용체계 기반구

5) 행정안전부 외, 앞의 책, 2012; 김태진·정윤수·기정훈·김종태, “행정정보 공동이용 장애요인에 대한 연구”, <한국지역정보화학회지> 제14권 제2호(2011. 6) : 85~103.

축 1단계 사업을 추진하였다. 2010년에는 2단계 사업으로 맞춤형 조회서비스, 전자민원서류관리서비스 등을 확대 구축하였으며, 2011년에는 3단계 사업으로 공동이용 대상정보·이용기관 확대, 정보조회서비스(원스크린 포함), 전자민원서류관리서비스, 실시간 맞춤정보 유통서비스 등의 확대를 추진 완료하였다. 2012년은 중기전략계획실행이 완성되는 해로 행정정보 공동이용체계 기능 고도화 사업을 추진 중에 있다.

이와 같은 행정정보 공동이용을 범주화하면 다음의 표와 같다.

<표 Ⅲ-1> 행정정보 공동이용의 세대별 비교

구분	1세대			2세대		
	1차 ('05.12 ~'06.8)	2차 ('06.9 ~'07.3)	3차 ('07.12 ~'08.10)	1차 ('09.8 ~'09.12)	2차 ('10.4 ~'10.11)	3차 ('11.3~)
정보확대 (누적)	34종	42종	71종	82종	92종	120종
기관확대 (누적)	·전행정기관 ·공공(5)	·전행정기관 ·공공(43) ·금융(2)	·전행정기관 ·공공(50) ·금융(16)	·전행정기관 ·민간(75)	·전행정기관 ·민간(103)	·전행정기관 ·(기관확대 업무이관)
추가 서비스				·원스크린 (5개사무) ·전자민원 서류관리 시스템시범	·원스크린 (405개사무) ·전자민원 서류관리 시스템확대 ·정보유통허브 기반환경구축	·원스크린 (430개사무) ·전자민원 서류관리 시스템시범 ·정보유통허브 체계구축 ·스마트공동이용서비스
세대비교	·단순 대장 및 공부중심의 공유서비스 ·행정·공공·금융 중심의 제한적 서비스 ·전체 공부항목 제공 ·민원·일반사무의 제한적 공동이용			·행정정보의 속성중심 맞춤서비스 ·금융·교육·위임위탁등 민간확대 ·수요자 필수 정보 선별제공 ·범국가적 민원포탈 공동이용 연계		

* 출처: 김태진 외(2011); 행정정보 공동이용센터(http://pr.share.go.kr)

라. 행정정보 공동이용의 현황

2012년 현재 공동이용 대상 행정정보는 27개 기관에서 120종을 보유하고 있다. 구체적인 보유기관별 구비서류는 다음 <표 Ⅲ-2>와 같다.

<표 Ⅲ-2> 정보조회 정보(구비서류 정보) 현황

정보보유기관	행정정보(구비서류명)	개인정보 유형	
27개	120종	52종	
경찰청(2)	운전경력증명서	○	주민, 운전면허
	자동차운전면허증	○	주민, 운전면허
고용노동부(1)	국가기술자격취득사항확인서		
공무원연금공단(1)	공무원연금내역서	○	주민
관세청(2)	수입신고필증		
	수출신고필증		
국가보훈처(4)	교육지원대상자증명서		
	국가유공자(유족)확인원	○	주민
	대학수업료면제대상자증명서		
	취업지원대상자증명서		
국민건강보험공단(5)	건강보험료납부확인서		
	건강보험자격득실확인서		
	건강보험증		
	사업장건강보험료납부확인서		
	차상위본인부담경감대상자증명서	○	주민
국민연금공단(3)	국민연금가입자가입증명	○	주민
	사업장국민연금보험료월별납부증명		
	연금산정가입내역확인서		
국세청(6)	(국세)납세증명서	○	주민
	납세사실증명		
	사업자등록증명		
	소득금액증명		
	폐업사실증명	○	주민
	휴업사실증명	○	주민
국토해양부(29)	개별공시지가확인서		
	개별주택가격확인서		
	건설기계검사증	○	주민
	건설기계등록원부	○	주민
	건설기계등록증	○	주민
	건설기계사업등록증		
	건설업등록증		
	건축물대장		

국토해양부(계속)	건축물사용승인서	○	주민
	건축사업무신고필증		
	건축허가서	○	주민
	공동주택가격확인서		
	부동산등기용등록번호증명서		
	선박검사증서		
	선박국적증서(상선)		
	선박원부	○	주민
	이륜자동차사용신고필증	○	주민
	임대사업자등록증	○	주민
	임시운행허가증		
	임야대장		
	임야도		
	자동차등록원부	○	주민
	자동차등록증	○	주민
	자동차말소등록사실증명서	○	주민
	주택건설사업사용검사필증		
	지적도		
	토지거래계약허가증		
	토지대장		
	토지이용계획확인서		
근로복지공단(3)	고용보험료완납증명원	○	주민
	산재보험급여지급확인원	○	주민
	산재보험료완납증명원	○	주민
농림수산식품부(5)	선박국적증서(어선)		
	선적증서		
	어선등록필증		
	어업면허증	○	주민
	축산업등록증		
대법원(3)	건물등기사항증명서		
	법인등기사항증명서		
	토지등기사항증명서		
법무부(4)	국내거소신고사실증명		
	외국인등록사실증명	○	외국인
	외국인의부동산등기등록증명서		
	출입국에관한사실증명	○	여권
병무청(1)	병적증명서	○	주민
보건복지부(11)	국민기초생활수급자증명서	○	주민
	보육시설인가증		
	약사면허증	○	주민
	영양사면허증	○	주민
	요양보호사자격증		
	의료기관개설신고증명서		
	의료기사면허증(안경사,방사선사)	○	주민
	의료면허증		

보건복지부(계속)	장애인연금(경증)장애수당장애아동수당수급자 확인서	○	주민
	장애인증명서	○	주민
	전문의자격증		
사립학교교직원연금공단(1)	연금법적용대상교직원확인서	○	주민
소방방재청(1)	안전시설등완비증명서		
여성가족부(1)	한부모가족증명서	○	주민
외교통상부(2)	여권	○	여권
	해외이주신고확인서	○	주민
중소기업청(3)	메인비즈확인서		
	벤처기업확인서		
	이노비즈확인서		
지식경제부(7)	공장등록증명서	○	주민
	석유판매업등록증		
	소프트웨어사업자신고확인서		
	전기공사기술자경력수첩		
	전기공사업등록관리대장		
	전기공사업등록증		
	전기안전점검확인서		
특허청(4)	디자인등록원부		
	상표등록원부		
	실용신안등록원부	○	주민
	특허등록원부	○	주민
평생교육진흥원(1)	학점은행제학위증명(전문학사,학사)		
한국가스안전공사(1)	액화석유가스 사용시설 완성검사증명서(발급 확인서)		
한국산업단지공단(2)	공장신설승인서	○	주민
	산업단지입주계약(계약변경)신청(확인)서	○	주민
해양경찰청(4)	선박출항·입항신고사실확인서(개별)	○	주민
	선박출항·입항신고사실확인서(총괄)	○	주민
	선원승선신고사실확인서	○	주민
	폐기물위탁·처리신고증명서	○	주민
행정안전부(7)	국외이주신고증명서	○	주민
	상훈수여증명서	○	주민
	인감증명서		
	주민등록표 등·초본	○	주민
	지방세 세목별 과세(납세)증명서(자동차세)	○	주민
	지방세 세목별 과세(납세)증명서(재산세)	○	주민
	지방세납세증명서	○	주민
환경부(6)	사업장폐기물배출자신고증명서		
	폐기물(중간/최종/종합)처리업허가증		
	폐기물수집운반업허가증		
	폐기물처리시설설치승인서		
	폐기물처리시설설치신고증명서		
	폐수배출시설설치(허가증/신고증명서)		

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

한편, 정보조회 이용기관 현황은 다음 표와 같다.

<표 Ⅲ-3> 정보조회 이용기관 현황

중앙행정기관	
53개	대통령실, 감사원, 국가정보원, 방송통신위원회, 민주평화통일자문회의, 국가인권위원회, 국무총리실, 법제처, 국가보훈처, 특임장관실, 공정거래위원회, 금융위원회, 국민권익위원회, 기획재정부, 교육과학기술부, 외교통상부, 통일부, 법무부, 국방부, 행정안전부, 문화체육관광부, 농림수산식품부, 지식경제부, 보건복지부, 환경부, 고용노동부, 여성가족부, 국토해양부, 국세청, 관세청, 조달청, 통계청, 대검찰청, 병무청, 방위사업청, 경찰청, 소방방재청, 문화재청, 농촌진흥청, 산림청, 중소기업청, 특허청, 식품의약품안전청, 기상청, 해양경찰청, 행정중심복합도시건설청, 육군본부, 진실화해를위한과거사정리위원회, 대일항쟁기강제동원피해조사및국외강제동원희생자등지원위원회, 국회, 대법원, 헌법재판소, 중앙선거관리위원회
지방자치단체	
260개	시·도(16개), 시·군·구(228개), 시·도 교육청(16개)
공 공 기 관	
100개	• (공사·공단) 기술신용보증기금, 농수산물유통공사, 대한법률구조공단, 대한주택보증주식회사, 대한지적공사, 사립학교교직원연금공단, 한국예탁결제원, 한국법무보호복지공단, 한국공항공사, 한국농어촌공사, 한국산업인력공단, 한국무역보험공사, 한국자산관리공사, 한국장애인고용공단, 한국전기안전공사, 한국토지주택공사, 교통안전공단, 공무원연금공단, 국민건강보험공단, 국민연금공단, 근로복지공단, 신용보증기금, 중소기업진흥공단, 한국전력공사, 한국환경자원공사, 한국주택금융공사, 부산광역시시설관리공단, 한국철도시설공단, 평생교육진흥원, 한국산업단지공단, 서울특별시SH공사, 한국수자원공사, 한국가스안전공사, 대구도시공사, 대전도시공사, 전북개발공사, 서울특별시시설관리공단, 대구광역시시설관리공단, 강동구도시관리공단, 강서구시설관리공단, 경기도시공사, 광주도시공사, 대전시설관리공단, 마포구시설관리공단, 부산도시공사, 부산교통공사, 부산항만공사, 송파구시설관리공단, 울산도시공사, 금융감독원, 대덕연구개발특구지원본부, 서울도시철도공사, 서울메트로, 주택관리공단, 중소기업중앙회, 한국장학재단, 한국지역난방공사, 새마을금고, 강원도개발공사, 한국석유관리원, 강남구도시관리공단, 건강보험심사평가원, 관악구시설관리공단, 국립공원관리공단, 광진구시설관리공단, 국립암센터, 도로교통공단, 동작구도시시설관리공단, 서대문구도시관리공단, 성동구도시관리공단, 속초시시설관리공단, 수원시시설관리공단, 예금보험공사, 종로구시설관리공단, 중구시설관리공단, 창원시시설관리공단, 청주시시설관리공단, 한국기업데이터, 한국승강기안전관리원, 한국저작권위원회 • (협회) 한국전기공사협회, 한국정보통신공사협회, 대한상공회의소, 한국산업기술진흥협회 • (재단) 16개 시·도 신용보증재단
금 융 기 관	
18개	우리은행, 중소기업은행, 신한은행, 하나은행, 한국외환은행, 국민은행, SC제일은행, 한국씨티은행, 농업협동조합중앙회, 수산업협동조합중앙회, 대구은행, 부산은행, 광주은행, 제주은행, 전북은행, 경남은행, 서울보증보험, 홍콩상하이은행
교 육 기 관	
7개	숭실대, 서울대, 안동대, 전북대, 군산대, 목포해양대, 경상대학교

* 출처: 행정정보 공동이용센터(http://pr.share.go.kr)

이용기관별 공동이용 실적은 다음과 같다.

<표 Ⅲ-4> 이용기관별 공동이용 현황

(단위 : 천건)

구 분	이 용 실 적				
	계	2009	2010	2011	2012.8 현재
계(438개)	160,630	41,975	42,933	45,261	30,460
행정기관(313개)	147,585	38,615	39,782	41,390	27,797
·중앙행정기관(52개)	46,121	11,900	11,866	14,105	8,250
·지방자치단체(261개)	101,464	26,715	27,916	27,285	19,547
공공기관(100개)	9,864	2,031	2,422	3,117	2,295
금융기관(18개)	3,179	1,329	729	754	367
교육기관(7개)	2	-	-	1	1

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

이를 다시 조회목적별로 분류하면 다음과 같다. 민원인이 행정기관, 공공기관 등에 대하여 처분 또는 일정한 서비스의 제공 등 특정한 행위를 요구하는 사항에 관한 민원 사무에 의한 공동이용은 지난 4년간 27.5%(44,150,000건)인 반면, 민원사무 외에 행정기관과 공공기관이 해당 법령에 따라 처리하는 일반사무에 의한 공동이용은 같은 기간 72.5%(116,475,000건)에 달했다.

<표 Ⅲ-5> 조회목적별 공동이용 현황

(단위 : 천건)

구 분	이 용 실 적				
	계	2009	2010	2011	2012
계	160,630	41,975	42,933	45,261	30,460
민원사무	44,155	11,721	10,688	12,104	9,642
일반사무	116,475	30,254	32,245	33,157	20,818

마. 행정정보 공동이용의 법적 근거

2006년 11월 국회에 제출된 「행정정보 공동이용법(안)」이 2008년 제17대 국회의 임기 만료로 자동 폐기됨에 따라, 정부는 이 법안의 핵심내용이 포함된 「전자정부법」 개정안을 마련하여 2008년 11월 국회에 다시 제출하고 2010년 2월에는 전부 개정하였다. 「전자정부법」은 여러 차례 개정을 거쳤지만, 행정정보를 수집·보유하고 있는 행정정보보유기관의 장으로 하여금 행정기관등과 행정정보를 공동으로 이용하게 할 수 있다는 내용을 계속 유지하여 왔다. 또한 2007년 7월 4일 개정시행 이후로 「은행법」 제8조 제1항에 따라 은행업의 인가를 받은 자 및 대통령령으로 정하는 법인·단체 또는 기관에게도 행정정보를 공동이용할 수 있도록 하였다.

2010년 전부 개정에서는 행정정보 공동이용대상과 방법 및 절차를 보다 구체적으로 규정하고, 정보주체로부터 행정정보 공동이용에 대한 사전동의를 받도록 하며, 정보주체의 열람청구권을 규정하는 한편, 개인정보침해에 따른 벌칙규정을 강화하였다. 특히 공동이용하려는 행정정보가 「공공기관의 개인정보보호에 관한 법률」 제5조에 따른 개인정보파일인 경우에는 같은 법 제20조제1항에 따른 공공기관개인정보보호심의위원회의 심의를 거쳐 제2항에 따른 공동이용 승인을 하도록 하고, 다만 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하도록 하였다(법 제39조 제4항). 이 조항은 2011년 9월 30일 「개인정보 보호법」이 제정발효된 후 「개인정보 보호법」 제7조에 따른 개인정보 보호위원회의 심의·의결을 거쳐 제2항에 따른 공동이용 승인을 하도록 개정되었다.

이와는 별도로 2008년 11월 행정정보 공동이용에 관한 세부절차를 정한 '행정정보 공동이용 지침'을 제정하였고, 2010년 5월에는 「전자정부법」 및 동법 시행령과 그동안 지침을 운영하면서 제기된 불편사항·건의사항을 반영하여 전부 개정하였다. 「개인정보 보호법」이 제정발효된 후 2012년 3월 8일 법률사항을 반영한 개정으로 오늘에 이르고 있다.

한편, 행정정보 공동이용을 실질적으로 뒷받침하기 위해서는 구비서류 제출을 면제하는 내용의 개별법령 개정이 필요하여 2006년 84개와 2007년 29개의 대통령령을 각각 일괄 개정하였다. 2008년에는 추가된 행정정보에 관한 사항과 등기부등본 등 이른바 공시성 정보에 대하여 사전 동의를 면제하는 내용으로 39개의 대통령령을 일괄개정하였다. 이와 동시에 각 소관 부처별로 총리

령 및 부령 개정 작업을 독려하여 2006년과 2007년 각각 293개와 91개를 개정하도록 하였고, 2008년에도 농림수산식품부 등 11개 부처의 16개 부령(총리령)을 개정하도록 하였다. 공동이용을 통하여 확인할 수 있는 구비서류를 국민에게 요구하지 않도록 행정정보 공동이용 일반법인 「전자정부법」이 개정·시행(2010.5.5)됨에 따라 일선 담당자의 업무처리 근거가 되는 「경제교육지원법 시행령」 등 관련 112건의 시행령에 이를 반영하여 공동이용 의무화의 개별 근거 마련 완결을 추진하였다. 일괄개정안은 법제처심사를 거쳐 10월 20일 차관회의와 10월 26일 국무회의를 통과하여 11월 2일자로 시행되었다. 2010년에는 일괄개정으로 총 264건의 시행령이 개정 완료되었다.

전자정부법 [시행 2012.9.2] [법률 제11461호, 2012.6.1, 타법개정]
제4장 행정정보의 공동이용

제36조(행정정보의 효율적 관리 및 이용) ① 행정기관등의 장은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관등과 공동으로 이용하여야 하며, 다른 행정기관등으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 같은 내용의 정보를 따로 수집하여서는 아니 된다.
② 행정정보를 수집·보유하고 있는 행정기관등(이하 “행정정보보유기관”이라 한다)의 장은 다른 행정기관등과 「은행법」 제8조제1항에 따라 은행업의 인가를 받은 은행 및 대통령령으로 정하는 법인·단체 또는 기관으로 하여금 행정정보보유기관의 행정정보를 공동으로 이용하게 할 수 있다.
③ 행정안전부장관은 행정기관등의 행정정보 목록을 조사·작성하여 각 행정기관등에 배포하고, 행정기관등이 공동이용을 필요로 하는 행정정보에 대한 수요조사를 할 수 있다.
④ 중앙사무관장기관의 장은 행정정보의 생성·가공·이용·제공·보존·폐기 등 행정정보의 효율적 관리를 위하여 관련 법령 및 제도의 개선을 추진하여야 한다.
⑤ 행정안전부장관은 다른 중앙사무관장기관의 장과 협의하여 행정정보의 공동이용에 대한 기준과 절차 등에 관한 지침을 마련하여 고시할 수 있다.

제38조(공동이용 행정정보) ① 제36조 및 제37조에 따라 공동이용센터를 통하여 공동으로 이용할 수 있는 행정정보는 다음 각 호와 같다.
1. 민원사항 등의 처리를 위하여 필요한 행정정보
2. 통계정보, 문헌정보, 정책정보 등 행정업무의 수행에 참고가 되는 행정정보
3. 행정기관등이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피하게 필요하다고 인정하는 행정정보
② 국가의 안전보장과 관련된 행정정보, 법령에 따라 비밀로 지정된 행정정보 또는 이에 준하는 행정정보는 공동이용 대상정보에서 제외할 수 있다.
③ 행정정보보유기관은 공동으로 이용되는 행정정보가 최신 정보가 되도록 하고 정확성을 유지하도록 관리하여야 한다.
④ 행정정보의 공동이용은 특정한 이용목적에 따라 필요한 범위에서 이루어져야 한다.

⑤ 제1항에 따른 행정정보의 범위에서 대상정보의 종류, 범위 및 유형 등은 대통령령으로 정한다.

제42조(정보주체의 사전동의) ① 이용기관이 공동이용센터를 통하여 개인정보가 포함된 행정정보를 공동이용할 때에는 「개인정보 보호법」 제2조제3호의 정보주체(이하 “정보주체”라 한다)가 다음 각 호의 사항을 알 수 있도록 정보주체의 사전동의를 받아야 한다. 이 경우 「개인정보 보호법」 제18조제2항제1호 및 제19조제1호는 적용하지 아니한다.
1. 공동이용의 목적
2. 공동이용 대상 행정정보 및 이용범위
3. 공동이용 대상 이용기관의 명칭
② 제1항에도 불구하고 이용기관이 다음 각 호의 어느 하나에 해당하는 경우로서 정보주체의 사전동의를 받을 수 없거나 동의를 받는 것이 부적절하다고 인정되면 이용기관은 그 행정정보를 공동이용한 후 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령으로 정하는 바에 따라 제1항 각 호의 사항을 정보주체가 알 수 있도록 하여야 한다. 다만, 제3호에 해당하여 이용기관이 범죄수사를 위하여 행정정보를 공동이용한 경우에는 그 사건에 관하여 공소를 제기한 날 또는 입건이나 공소제기를 하지 아니하는 처분(기소중지 결정은 제외한다)을 한 날 이후에 알 수 있도록 하여야 한다.
1. 정보주체의 생명 또는 신체를 보호하기 위하여 긴급하게 공동이용할 필요가 있는 경우
2. 법령에 따라 정보주체에게 의무를 부과하거나 권리·이익을 취소·철회하는 업무를 수행하기 위하여 공동이용이 불가피한 경우
3. 법령을 위반한 정보주체에 대한 조사 또는 처벌 등 제재와 관련된 업무를 수행하기 위하여 공동이용이 불가피한 경우
4. 그 밖에 법령에서 정하는 업무를 수행함에 있어서 정보주체의 사전동의를 받는 것이 그 업무 또는 정보의 성질에 비추어 현저히 부적합하다고 인정되는 경우로서 대통령령으로 정하는 경우
③ 행정안전부장관은 제2항에 따라 정보주체의 사전동의 없이 공동이용할 수 있는 업무와 행정정보의 구체적인 범위를 대통령령으로 정하는 바에 따라 공개하여야 한다.

제43조(정보주체의 열람청구권) ① 정보주체는 공동이용센터를 통하여 공동이용한 행정정보 중 본인에 관한 행정정보에 대하여 다음 각 호의 사항에 대한 열람을 행정안전부장관 또는 해당 이용기관의 장에게 신청할 수 있다.
1. 이용기관
2. 공동이용의 목적
3. 공동이용한 행정정보의 종류
4. 공동이용한 시기
5. 해당 행정정보를 공동이용할 수 있는 법적 근거
② 행정안전부장관 및 이용기관의 장은 제1항에 따른 정보주체의 신청을 받았을 때에는 정당한 사유가 없으면 신청한 날부터 10일 이내에 그 정보주체에게 제1항 각 호의 사항을 통보하여야 한다. 이 경우 10일 이내에 통보할 수 없는 정당한 사유가 있을 때에는 그 사유가 소멸하였을 때에 지체 없이 통보하여야 한다.
③ 제2항의 경우에 이용기관이 범죄수사를 위하여 행정정보를 공동이용한 경우에는 그 사건에 관하여 공소를 제기한 날 또는 입건이나 공소제기를 하지 아니하는 처분(기소중지

결정은 제외한다)을 한 날부터 30일 이내에 그 정보주체에게 통보하여야 한다.
④ 정보주체는 이용기관이 제2항에 따른 통보를 하지 아니하면 이용기관이 공동이용한 행정정보 중 본인에 관한 제1항 각 호의 사항에 대한 열람을 행정안전부장관에게 직접 신청할 수 있다.
⑤ 제1항부터 제4항까지의 규정에 따른 열람 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
⑥ 행정안전부장관은 대통령령으로 정하는 바에 따라 공동이용센터를 통하여 공동이용한 행정정보의 명칭, 공동이용 횟수 등의 기록을 유지·관리하고 공개하여야 한다.

바. 문제점

오늘날과 같은 정보사회에서는 여러 가지 유형의 개인정보침해가 발생하고 있지만, 그 중에서도 정부기관의 전산망 연결로 법적 통제없이 공무원에 의해 개인정보가 검색, 처리 또는 유출되어 개인의 사생활이 침해되는 일이 빈번하게 발생하고 있다[6].

2008년 행정안전부에서 조사한 공공부문의 사이버 침해사고를 살펴보면 5년간 12배 이상이 증가하였으며, 2년간 발생한 공공기관 홈페이지의 개인정보노출건수도 2624개 기관에서 18만 2666건이 발생하였다. 이러한 개인정보침해 사고의 주요 원인으로는 취약한 보안시스템과 관리자의 부주의 등으로 인한 운영상 문제가 지적되었다. 그 중 행정정보 공동이용과 관련한 침해사례는 개인정보의 유출과 관련하여 데이터베이스의 사적사용, 외부기관 자료의 임의제공, 공공기관의 직원이 동료직원 가구사항 조회, 민원제보자의 노출 등의 형태로 공공기관의 개인정보가 침해되는 경우가 있었다.

2008년 감사원은 '행정정보 공유 및 관리실태'에 대한 감사[7]'에서 행정정보 공동이용시스템을 이용하여 담당공무원이 개인정보를 사적으로 무단 열람하고, 외부로 유출하는 문제를 완전히 차단하긴 어렵다고 보고 있다.[8] 담당공무원에 의한 정보유출은 행정정보공동이용시스템이 구축되면서 출현한 문제는 아니지만, 자신이 근무하는 기관의 개인정보 데이터베이스만 볼 수 있었던 기존시스템과는 달리 행정정보 공동이용시스템을 이용하게 되면 다른 기관이 보유하고 있는 개인정보에까지 접근이 가능하게 되므로, 정보유출의 파괴력이 훨씬 커지

6) 장교식 외, 앞의 글, 2010.
7) 감사원은 각 기관에서 개인정보가 포함된 행정정보를 다른 기관에 제공하면서 정보유출 방지를 위한 조치를 제대로 하고 있는지, 그리고 개인정보의 실시간 열람기능을 제공하는 행정정보공동이용시스템의 정보보안기능이 적정한지 등을 중점적으로 감사하였다.
8) 감사원, "감사결과 처분요구서: 행정정보 공유 및 관리실태". 2008.5.

게 되었다고 할 수 있다. 특히 감사원은 행정정보 공동이용 정보의 오·남용 방지체계를 신뢰할 수 없었다고 지적하였다. 행정정보의 오·남용 등을 파악하기 위해서 필요한 정보열람기록이 자동으로 기록되지 않고 정보열람자로 하여금 수동으로 입력하게 하여, 부주의로 잘못 입력하거나 의도적으로 조작할 수 있었다. 실제 행정정보 공동이용 관련 정보 오·남용 실태를 확인하기 위해 2007년 4월부터 같은 해 9월 사이에 서울특별시 ○○구청 등 20개 시·군·구에서 민원사무처리를 위해 위 공동이용시스템을 이용하여 행정정보를 열람한 명세와 시·군·구 행정정보시스템에 기록된 민원사무처리 명세를 비교한 결과 민원사무를 위해 공동이용(열람)한 행정정보 41,332건 중 25,916건(63%)은 민원사무처리부에 기록되지 않아 실제 민원사무를 위해 정보를 열람한 것인지 확인할 수 없게 되어 있었다. 하지만 행정안전부 행정정보공유추진단은 정보열람기록이 정확히 기록되도록 행정정보 공동이용시스템의 정보 오·남용 방지체계를 개선하는 방안을 마련하지 않았고, 2006년, 2007년 행정정보 공동이용기관 실태점검에서도 정보이용자의 민원 또는 행정업무처리 명세와 정보이용 명세를 비교하는 등 개인정보의 오·남용 여부에 대한 점검은 하지 않았다. 결국 행정정보 공동이용시스템은 행정정보 오·남용을 완전하게 방지할 수 없어 주민등록정보 등 개인정보의 유출 소지가 있다는 것이다.

2010년 행정정보 공동이용 과정에서의 부적정이용 유형 사례별로 살펴보면, ① 이용기관에서 등록된 PC에서만 공동이용할 수 있도록 조치하지 않고 장소를 옮겨서 공동이용 ② 공동이용시 사무를 정확히 확인하여 이용하지 않고 타 부서 사무를 승인받아 이용 ③ 업무담당자가 행정정보를 공동이용하면서 업무연관성이 적은 사무에 대한 접권 권한을 신청하여 승인 받아 이용 ④ 특정업무에 해당하는 공동이용 사무가 있는데 다른 공동이용 사무에 포함된 사무를 이용하는 경우 ⑤ 읍면에서 접수 및 처리하는 '쌀소득등보전직불제' 업무는 처리기관이 시도·시군으로 되어있어 토지 등기부등본 열람시 시·군·구 사무를 승인받아 사용한 사례 등이 있었다[9].

또한 2012년 개인정보 보호위원회에서 공공기관 개인정보보호 이행실태를 설문조사한 바에 따르면, 정보주체의 동의가 필요한 개인정보를 수집·이용하는 경우로써 실제로 동의를 받고 있는 경우는 79.7%였으며, 16.2%는 일부만, 4.1%는 받지 않고 있는 것으로 나타났다[10]. 우리나라에서 이처럼 개인정보침

9) 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료
10) 진선미, 앞의 답변자료

해가 발생할 수 있는 가장 큰 원인 중 하나는 바로 '주민등록번호'의 남용이다. 주민등록번호만 알면 서로 다른 개인정보 데이터베이스의 정보도 통합할 수 있게 되고, 이러한 데이터베이스가 많을수록 침해의 가능성도 높아진다. 이 설문조사에서도 별도 동의를 받아야 하는 주민등록번호 등 고유식별정보에 대하여, 59.3%가 별도 동의절차를 제대로 이행하고 있으며, 20.7%는 일부에 한하여 동의를 받고 있고 20%는 동의를 받고 있지 않은 것으로 나타났다.

따라서 개인정보에 해당하는 행정정보의 공동이용이 이루어질 때에는 동일기관이 아닌 다른 행정기관에게 개인정보의 제공이나 수신과 관련되는 법적 근거의 유무를 확인해야 마땅하다. 모든 국가기관은 그들이 지니고 있는 정보만으로 업무의 처리가 부족할 경우, 기관 상호간에 원조해야만 하지만 이러한 공유는 꼭 필요한 경우에 최소한으로 행해져야 한다.

그러나 「전자정부법」은 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 안된다고 규정하면서도 그 개인정보의 수집의 범위나 공유·보유·관리에 대한 구체적인 규정은 없어 개인정보에 대한 침해의 문제가 발생할 가능성을 내포하고 있다. 정보의 주체로부터 직접 수집하기보다는 다른 파일이나 타 조직이 구축해 놓은 개인정보를 활용하는 것을 특징으로 하기 때문에 이러한 동의를 얻기가 어려울 뿐만 아니라 형식화될 위험이 상존한다.[11]

무엇보다 행정정보 공동이용의 목적은 본래 이용제한이 아니라 이용의 활성화에 있기 때문에 원칙적으로 개인정보를 목적에 따라 이용하도록 한 목적 구체성 및 이용 제한의 원칙과 상반된다. 행정정보 공동이용 시스템의 구축으로 개인정보의 이용률이 높아지면 그만큼 남용의 위험성도 커지기 때문에 이용제한의 필요성도 커진다. 또한 공동이용을 전제로 하지 않고 수집된 개인정보의 경우 목적 외로 공유될 때 관련업무의 특성에 맞게 정리·분류·관리된 상태와 괴리가 발생할 수밖에 없다. 비맥락적 의사결정과 도식적 정보처리의 문제가 발생할 수 있는 것이다. 개인정보가 부정확하고 질이 낮은 경우에는 의사결정 과정에서 오류가 기하급수적으로 반복되는 폭포화 현상이 발생할 우려도 있다.

한편 개인정보자료의 안정성 확보 미비로 오남용과 유출사고에 취약함을 드러낼 수도 있다. 그러나 정보관리체계가 기본적으로 복잡한 구조를 가지고 있기 때문에 정보주체는 결정이 이루어진 뒤에야 비로소 부당한 처리가 있었음을 알게 되거나 또는 알지 못하고 지나갈 수 있다. 공동이용에서 개인은 통제 대

11) 김소미, "행정정보 공동이용과 개인정보보호", 충북대학교 법학석사학위논문, 2011.

상 조직을 식별하는 것이 용이하지 않으므로 개인정보의 오류에 대하여 수정·정정·삭제권의 행사가 어렵다. 실제로 행정정보공동이용 실태 점검 결과 보고('10.7.1~10.31)[12]에 따르면, 「행정정보공동이용지침」에 공동이용관리자 직급을 부서장급으로 지정·운영하도록 하였으나, 일부 이용기관에서는 부서장의 결재 공문없이 시스템에서만 접근권한을 부여하거나, 필요 절차의 이행 여부를 확인하지 않고 분임공동이용관리자를 통해 접근권한을 승인한 사례가 있었다. 또한 부서내 인사이동이나 업무분장 변경 등 접근권한 반납 사유가 발생하였음에도 일부 기관에서 접근권한 반납이 즉시 이루어지지 않고 있었다.

현행 「전자정부법」은 공공기관 뿐만 아니라 금융기관에도 행정정보 공동이용의 권한을 주고 있으며, 대통령령으로 정하는 법인·단체 또는 기관도 행정정보를 공동이용할 수 있도록 하였다(「전자정부법」 제36조 제2항). 이러한 민간기관의 정보공동이용은 정보의 유출 및 오·남용의 위험성이 특히 크기 때문에 더욱 신중하게 이루어져야 한다. 실제로 과거 행정정보공유추진위원회의 회의 내용을 살펴 보면, 대법원이나 법무부가 개인정보를 공공·금융기관에까지 확대하는 것은 곤란하다는 의견을 밝힌 바 있으나 공동이용 기관 확대 기조에는 변화가 없었다.[13]

반면 이러한 상황을 감독하려는 취지에서, 신청기관이 공동이용하려는 행정정보가 개인정보파일인 경우에는 개인정보 보호위원회(구 공공기관개인정보보호심의위원회)의 심의 및 의결을 거쳐 공동이용 승인을 하여야 하고, 다만 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하도록 한 법률 조항(「전자정부법」 제39조 제4항)의 운용은 유명무실한 형국이다. (구)공공기관개인정보보호심의위원회의 경우 8년간 고작 10번의 회의로 유명무실한 활동으로 지탄을 받아 왔으며[14], 그나마 2008년 이명박 정부 들어선 이후로는 폐지 방침으로 심의가 제대로 이루어지지 못했다[15]. 2011년 9월 30일 「개인정보보호법」의 제정 발효로 설치된 개인정보 보호위원회는 2012년 1월에 들어서야 위원 인선이 마무리되어 활동을 시작하였으나, 발족 후 2012년 10월 현재까지 행정정보 공동이용과 관련한 심의 및 의결은 1건도 처리하지 않았다. 2010년 해당 조항이 신설된 이후로도 행정정보 공동이용은 꾸준히 확대되어

12) 진선미, 앞의 답변자료
13) 오병일·장여경·김지성·이은우·김철, 「개인정보 수집·유통 실태조사」, 국가인권위원회 용역보고서, 2009.
14) "공공기관 개인정보보호심의위 '유명무실'", 연합뉴스, 2008.9.8.
15) "'무늬만 위원회' 273개 폐지키로 ‥ 국무회의 의결", 한국경제, 2008.5.27.

왔던 바, 해당 기간 동안 개인정보 공동이용이 전혀 이루어지지 않았다는 말이 아니라면 해당 조항은 사실상 제 기능을 못해왔다는 결론에 이르지 않을 수 없는 것이다.

다른 한편, 「전자정부법」제42조에서는 개인정보가 포함된 행정정보를 공동이용할 때는 정보주체의 동의를 받아야 한다고 규정하고 있다. 하지만 이러한 정도의 내용으로는 사실상 어느 정도가 현저하게 인권을 침해하는 것인지, 언제 자신의 정보를 수집하는지 전혀 알 수가 없는 일반 추상적인 규정이라 할 수 있다. 역시 유명무실한 조항이라 볼 수 있는 것이다. 실제로 행정정보공동이용 실태 점검 결과 보고('09.11.3~20)에 따르면, 사전동의서 징구시 △사전동의 양식이나 내용이 다소 부적절하여 수정이 필요(대상정보별로 사전동의를 받지 않고 사무에 대해 포괄적으로 사전동의를 받거나, 1건의 동의서에 향후 사정이 변경되어도 변경전 동의서에 동의한 것으로 간주 하는 등 사전 동의의 범위를 지나치게 넓게 정하고 있음) △사전동의란에는 동의 확인을 받지 않고 공란으로 비워 놓고 서식 하단에만 정보주체의 서명을 받음 △해당 업무와 사전동의한 업무명이 불일치하는 등의 부적절한 사례가 나타났다[16].

이에 전문가들은 행정정보 공동이용 제도 하에서 개인정보가 공동이용되는 실태에 있어서 다음과 같은 개선이 이루어져야 한다고 고언한다[17].

첫째, 개인정보와 관련된 행정정보 공동이용은 기본권을 제한하고 있기 때문에 반드시 구체적인 법률조항에 의거해야 한다. 즉, 공동이용의 목적과 대상정보, 개인정보의 수집범위, 수집 방법, 이용범위 등이 법률에 명확하게 규정되어야 하는 것이다.

둘째, 법률은 개인정보에 해당하지 않는 행정정보와 개인정보에 해당하는 개인정보를 구분하여 규정하고 개인정보에 해당하는 행정정보를 공동이용함에 있어서는 공동이용의 요건이나 절차, 범위 등이 보다 엄격하게 규정되어야 한다. 또한 개인정보를 공동이용하기 위해서는 개인정보의 사용계획을 사전에 충분히 수립하고, 목적구속의 원칙에 반하지 않는 범위 안에서 구체화하여 명확하게 규정하여야 한다.

셋째, 공동이용되는 개인정보의 오류로 인하여 정보주체에게 피해가 발생하지 않도록 개인정보의 최신성과 정확성을 확보하여 개인 정보의 질을 향상시키고, 합리적인 방안을 강구하여 유통되는 개인정보의 유효기간을 설정할 필요가

16) 진선미, 앞의 답변자료
17) 장진숙, “행정정보 공동이용과 정보인권 : 자기정보관리통제권을 중심으로”, 인권복지연구 제6호, 2010.

있다. 사용이 종료된 개인정보는 정보주체에게 통보와 아울러 즉각 폐기하여야 한다. 그리고 개인정보의 포괄적 노출과 유출 등의 부작용을 최소화하기 위하여 수집·보관의 책임주체가 명확하게 규정되어 책임소재를 분명히 할 수 있어야 한다.

넷째, 정보주체에 대하여 단순한 열람권을 넘어서, 어떤 목적으로 자신에 관한 정보를 제공하였는지, 또 누구에게 어떻게 전달하였는지에 관한 설명을 들을 권리가 인정되어야 한다.

무엇보다 전문가들은 개인정보 공동이용의 실태를 개선하기 위해서 평가 및 감독기관의 역할을 실질화할 것을 주문해 왔다. 행정정보 공동이용 사무를 주무하는 행정정보공유추진위원회의 경우, 과거 회의록을 살펴보면 행정정보의 공유를 확대하는데 주된 업무의 초점이 맞춰져 있을 뿐 행정정보 공동이용에 따르는 개인정보 보호의 문제에는 별로 신경을 쓰지 않는 모습을 보여 왔다[18]. 이에 많은 전문가들이 개인정보 영향평가 제도의 신설과 개인정보 보호위원회의 설치 및 그 역할에 기대를 걸어 왔다. 다행히 「개인정보 보호법」은, 공공기관이 구축·운용 또는 변경하려는 개인정보파일이 5만명 이상의 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일이거나 다른 개인정보파일과 연계할 경우 50만명 이상의 개인정보파일인 경우, 혹은 100만명 이상의 정보주체에 관한 개인정보파일인 경우 등에는 개인정보 영향평가를 받도록 하였다(법 제33조 및 동법 시행령 제35조 내지 제38조). 그러나 개인정보 영향평가는 아직 그 사례 건수도 적을 뿐더러[19] 제도가 정착하기까지 적지 않은 시일이 소요될 것으로 보인다.

<표 Ⅲ-6> 개인정보 사전영향평가 실시 현황

('11.9월 법 시행이후 '12.7월까지)

기관명	평가 대상시스템명	평가기간	비고
경찰청	교통경찰업무관리시스템	'12.1~2월	
국방부	국방동원정보체계(예비군 관리 업무)	'12.5~7월	
충청북도	홈페이지, 지적행정시스템, 긴급구조시스템	'12.5~7월	
경기도	추정분담금 정보시스템	'12.5~7월	

18) 오병일 외, 앞의 보고서, 2009.
19) 진선미, 앞의 답변자료

또한 상술하였다시피 개인정보 보호위원회가 심의 및 의결 활동을 시작한 지 1년이 되어간다. 그러나 발족후 2012년 10월 현재까지 개인정보 보호위원회가 제3자에 대한 공공기관의 개인정보 제공 관련 심의 및 의결을 수행한 현황은 겨우 2건으로, 매우 부실하다. 개인정보 보호위원회의 심의 및 의결을 요하는 해당 기간 제3자에 대한 공공기관의 개인정보 제공 건수가 정말 이에 머물러 있다는 것인지 의아스럽지 않을 수 없다[20].

<표 III-7> 개인정보 보호위원회 개인정보 제공 관련 의결 현황

일자	개인정보 보유기관	개인정보 종류	개인정보 요청기관	요청 사유	심의·의결 결과	사유
'12.5. 29	병무청	성명, 생년월일, 입영·전역일자, 입영부대, 입영결과 등	각 대학	대학의 휴·복학 업무수행	기각 (불승인)	개인정보 보호법 제18조제2항 제5호에서 규정하고 있는 개인정보 제3자 제공 가능사유에 해당되지 않음
'12.4. 30	경기도내 11개 시·군	CCTV 영상정보	경기도 소방재난 본부	화재예방 등 소방목적으로 활용	기각 (불승인)	

따라서 이러한 신설 제도가 행정정보 공동이용을 충분히 평가 및 감독하기까지는 많은 법제도상의 보완이 필요하다.

사. 정책 제언

무엇보다 개인정보를 공동이용하고자 하는 목적이 법률에 보다 구체화될 필요가 있다. 「전자정부법」에서는 공동이용센터를 통하여 공동으로 이용할 수 있는 행정정보는 ① 민원사항의 처리를 위하여 필요한 행정정보 ② 통계정보, 문헌정보, 정책정보 등 행정업무의 수행에 참고가 되는 행정정보 ③ 행정기관 등이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피하게 필요하다고 인정하는 행정정보를 들고 있다(법 제38조). 그러나 원론적으로는 전자정부의 추진으로 공동이용대상이 되는 개인정보는, 개인의 주거변동에 대한 확인과 국세의 납부·병역의 이행을 위한 전자적 고지 및 업무수행의 선상에 놓이게 하여

20) 진선미, 앞의 답변자료

행정서비스의 법률적합성을 담보하는 것이 요구된다 하겠다[21]. 이보다 완화된 기준을 생각해 보더라도 현재의 막연한 규정보다 구체적인 목적과 그에 부합하는 요건이 부여될 필요성이 있다. 즉, 개인정보의 공동이용을 하지 않을 경우의 잠재적인 위협이나 결과를 명확히 하고, 공동이용하고자 하는 개인정보와 처음 수집한 목적과의 연계성을 확인하고, 공동이용 방법 이외의 대안적인 방법은 없는지에 대한 분석이 있어야 할 것이다[22].

또한 행정정보 공동이용이란 원칙적으로 본래의 수집 목적에 반하여 제3자 기관에 제공한다는 점에서 목적구속의 원칙에 예외적인 상황임을 인식할 필요가 있다. 개인정보자기결정권에 포함되는 목적구속의 원칙이란 개인정보를 수집하는 목적은 특정되어야 하고 그 후의 이용은 이 특정된 수집목적과 일치되어야 한다는 것이다. 이 원칙은 개인정보 수집기관 이외에 제3자에 대한 제공을 통제하기 위한 것이다. 제3자 제공의 경우에도 수집제한의 원칙이 적용되기 때문에 제공목적이 정당성, 제공범위의 필요최소성, 제공방식의 합리성, 정보주체의 인식명확성이 요구된다. 그러나 개인정보를 이용하는 조직들은 이에 대하여 추상적이고 포괄적인 목적을 제시하여 이용의 제한을 피하려고 하는데 이를 방지하기 위하여 조직의 개인정보 수집을 조직의 목적과 관련하여 최소한의 범위에 한하도록 하는 방안이 요구된다. 특히 정부나 조직을 하나의 단위로 생각하여 정보를 공유하려 해서는 안 되며, 업무를 그보다 구체화된 기능별로 분리하여 개인정보의 이용을 해당 기능에 한하여만 이용할 수 있도록 해야 할 것이다.

한편 공동이용체계는 필요한 개인정보를 개인으로부터 직접 수집하기보다는 제3자로부터 수집하는 간접수집방법을 주로 사용하게 된다. 이 경우 법률의 규정에 의하거나 개인의 동의가 전제되어야 한다. 그러나 전 국민을 대상으로 하는 데이터베이스를 활용하고자 하는 경우에 개인의 동의를 얻는다는 것은 거의 불가능하다고 할 수 있다. 이러한 상황에서 동의의 한 방법으로 행정기관이 개인정보를 수집하도록 하는 신고서에 구체적인 공동이용의 내용을 명시하여 개인들이 인지하고 이에 동의를 구하는 방법이 활용될 수 있다.

더불어 개인정보 이용체계에는 수집목적 외 사용증가로 비맥락적인 의사결정의 가능성이 증가한다는 사실에도 주목하는 대책이 필요하다. 컴퓨터 매칭, 컴퓨터 프로파일링 및 신원조회 등과 같은 단순한 결과만 갖고 의사결정을 하는

21) 이민영, 앞의 글, 2006.
22) 김소미, 앞의 글, 2011.

것을 제한하는 메커니즘이 필요한 것이다. 특히 공공기관이 관리하는 개인 정보의 정확성이 결여되어 있고 그 질이 문제시되는 경우에는 공동이용에 의하여 공공기관의 서비스 제공 여부를 결정하거나 규제의 대상으로 선정하는 것은 매우 신중할 필요가 있다. 따라서 공동이용을 통하여 결정을 하는 경우에는 관련 당사자에게 소명의 기회를 제공하는 절차적 제도가 마련되어야 할 것이다. 또한 정확성과 최신성 등 개인정보의 질과 개인정보의 안전성을 확보해야 한다.

그리고 개인정보 유출의 대부분은 비인간적 요인보다는 인간적 요인에 의하여 더욱 많이 발생하고, 외부인보다는 내부인에 의하여 안전성이 위협되는 경우가 많다는 사실을 인지할 필요가 있다. 최근의 보안 이슈는 주로 비인간적인 것과 외부자의 차단에만 관심을 기울이고 있으나 행정관리 차원에서 인적·관리적인 보안활동이 강화될 필요가 있다.

정보주체에 대한 공개 및 참여의 권리는 언제든지 보장되어야 하며, 「개인정보 보호법」에도 불구하고 행정정보 공동이용과 관련하여 문제되는 개인정보 보호에 관한 사항은 「전자정부법」 내에 행정정보 공동이용의 원칙과 함께 정렬하는 것이 바람직할 것이다. 개인정보 영향평가 제도와 개인정보 보호위원회의 역할 제대로 하여야 함은 물론이다.

여기서 주민등록번호에 대한 문제를 짚고 넘어가야 할 필요성이 있다. 행정정보 공동이용이 개인정보에 대해서도 손쉽게 확대되어 온 데에는 주민등록번호가 민관의 모든 데이터베이스의 식별도구로 사용되고 있기 때문이다. 따라서 궁극적으로 개인정보 공동이용의 범위를 목적 내로 제한하기 위해서는 주민등록번호 역시 주민서비스를 위한 본래의 역할로 제한하고 다른 민관의 데이터베이스는 각자 자기 목적별 식별부호를 마련하는 것이 필요하다. 원칙적으로 주민등록번호는 효율적 대민행정(對民行政)을 유지하는 수단에 불과해야 하는 만큼 민간분야에서 무분별하게 사용되어져서는 아니 되며 특별한 보호가 취해져야 한다[23].

23) 이민영, 앞의 글, 2006.

2. CCTV

가. 문제 제기

국가인권위원회는 2004년 10월 구금시설의 CCTV에 대한 진정사건에서 CCTV가 인권에 미치는 영향에 관하여 다음과 같이 지적하였다. CCTV는 재생 및 무제한 복사가 가능하고, 타인에게 제공하거나 유출할 수 있으며, 특정부위를 정밀하게 촬영할 수 있고 촬영된 내용을 편집할 수 있다. 또한, 24시간 연속으로 대상자의 모든 행동이 감시되고 동태적인 삶의 흐름이 정보의 형태로 녹화됨으로써 개인의 사생활이 과도하게 침해될 우려가 높고, CCTV가 설치된 사실 자체가 주는 '위축효과'로 인해 일반적인 행동의 자유도 현저하게 제한되며, 녹화된 개인정보의 유출등 악용사례가 발생할 가능성도 배제할 수 없다.[24)]

이 가운데 공공기관이 CCTV 등 무인단속장비를 공공장소에 설치·운영하는 것은 그 설치지역과 운영방법 등에 따라 개인의 초상 그 자체뿐만 아니라 특정시간에 어디서 어떤 모습으로 누구와 함께 있었는지 등에 관한 개인정보를 취득하는 것이며, 설치·작동 방법에 따라서는 개인의 사생활 영역내의 모습을 녹화·저장하는 것도 가능하다. 따라서, CCTV 등 무인단속장비의 설치·운영은 촬영되는 사람들에 대하여 초상권과 개인정보자기결정권(헌법 제10조), 사생활, 가정, 주거의 자유와 이를 법으로 보호받을 수 있는 권리(헌법 제17조, 시민적 및정치적권리에관한국제규약 제17조294)를 제한하고 침해할 수 있다.[25)] 특히 범죄예방을 목적으로 24시간 CCTV로 거리를 촬영할 경우 국민을 잠재적 범죄자로 취급하는 것이 될 뿐만 아니라, 개인의 일상에 관한 정보를 무차별적으로 수집하는 것이 된다.[26)]

일반 시민들이 CCTV에 대해 가지고 있는 인식은 양면성을 가지고 있다. 일면적으로는 CCTV가 설치된 것을 보면 안심된다는 생각으로 범죄예방을 위해 사생활에 대한 권리를 유보할 수 있다는 인식이 존재한다. 하지만 국가인권위원회에 CCTV에 대한 진정 및 상담 등이 꾸준하게 제기되는 현황을 보면, CCTV로 인한 권리 침해를 우려하는 시각도 상당하다고 볼 수 있다.

---

24) 국가인권위원회, "구금시설 수용거실 내 CCTV 설치·운영 등 인권침해", 03진인971, 03진인833, 03진인5806(병합) 결정, 2004.10.

25) 국가인권위원회, "공공기관의 CCTV 등 무인단속장비의 설치·운영 관련 정책 권고", 2004.4.19.

26) 권건보, "지방자치단체의 CCTV 설치·운영과 프라이버시", (사)유럽헌법학회 및 국가인권위원회 공동학술발표회 <유럽인권협약과 기본권>, 2009.5.29.

<표 Ⅲ-8> CCTV 관련 국가인권위 진정·상담·민원 현황

(2009년 8월 말 현재)

구분	진정사건	상담	민원	안내	합계
2009	209	386	63	17	675
2010	326	520	265	21	1,132
2011	167	510	224	14	915
2012.8	124	445	195	11	775
합계	826 (23.6%)	1,861 (53.2)	747 (21.4)	63 (1.8)	3,497 (100)

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

나. 법적 근거

2002년 12월 서울시 강남구청이 강남경찰서와 협의하여 강남구 논현1동 일대에 범죄예방을 위한 CCTV 5대를 시범설치한 이후 공공기관의 CCTV가 급격히 증가하였다. 특히 이 시점 이후로 각 지방자치단체의 방범용 CCTV의 운영이 경찰관서로 위탁관리되는 경우가 늘면서 본격적인 'CCTV 방범시대'의 막이 올랐다.

그러나 2007년 11월까지 CCTV에 대한 어떠한 법률적 규제도 존재하지 않았다. CCTV 등 무인단속장비를 설치·운영하여 범죄 수사 등에 활용하는 것이 국회가 제정한 법률이 아니라 지방자치단체나 경찰서장의 재량에 의하고 있었던 것이다. 이에 CCTV 설치·운영에 필요한 사항 및 개인의 화상정보 보호를 위한 사항을 법률에 규정하여 국민의 권리를 보호할 필요가 있다는 문제제기가 이어졌다.

국가인권위원회는 2004년 4월 국회의장과 행정자치부 장관에게, 지방자치단체, 경찰청 등에서 설치·운영하고 있는 범죄예방 및 범죄수사를 위한 CCTV 등 무인단속장비의 설치·운영에 관한 법적 기준을 마련할 것을 권고하였다.[27] 또한 같은 이유로 CCTV에 대한 규정을 포함한 2개 법률이 발의되어 국회에서 논의되었다.[28]

27) 국가인권위원회, 앞의 결정, 2004.4.19.

28) 「공공기관의 개인정보보호에 관한 법률중 개정법률안(김재경의원 대표발의안, 의안번호 제171070호)」, 「공공기관의 폐쇄회로 텔레비전 설치 및 개인의 화상정보 보호에 관한 법률안(김충환의원 대표

마침내 2007년 11월 처음으로 (구)「공공기관의 개인정보보호에 관한 법률」(이하 '공공기관개인정보 보호법')에 CCTV에 대한 규정이 삽입됨으로써 공공기관 CCTV 설치·운영에 관한 법률적 규율이 시작되었다.[29] 이 법률이 시행되기 전까지는 2007년 5월 시점으로 11만여 대에 달하는 것으로 산출되었던 공공기관 CCTV를 통해 수집되는 개인정보의 보호가 제대로 이루어지지 않았다. 이 사실은 법 시행 직후에 실시된 정부의 자체 조사 결과에서도 잘 드러난다. 많은 공공기관 CCTV가 설치사실을 공지하지 않은 채 운영되고 있었고, 개인정보 제공에 대해 대장을 작성하지 않았으며, 「통신비밀보호법」에서 금지하고 있는 음성녹음기능을 사용하고 있는 경우도 있었다.[30]

2011년 9월 30일 개인정보 보호법이 제정발효하면서부터는, 공공기관 뿐 아니라 민간영역까지 아울러 CCTV 등 영상정보처리기기의 설치·운영에 관한 법률적 규율이 시작되었다. 이 법은 (구)공공기관개인정보 보호법이 '범죄예방 및 교통단속 등 공익을 위하여 필요한 경우'라는 요건(동법 제4조의2 제1항)으로 폭넓게 규율해 왔던 것에 비해서 공공기관의 CCTV의 설치와 운영을 5가지 목적 내로 제한했다는 점에서 개선된 측면이 있다.

개인정보 보호법
제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.
1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우
② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.
③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령

발의안, 의안번호 제171287호)」.

29) 이 법률의 적용을 받는 공공기관은 국가행정기관, 지방자치단체, 「초·중등교육법」 및 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교, 「공공기관의 운영에 관한 법률」 제4조제1항의 공공기관, 특별법에 의하여 설립된 특수법인, 「지방공기업법」에 따른 지방공사 및 지방공단을 의미한다(동법 제2조제1호 및 동시행령 제2조).

30) 당시 조사결과는 14개 공공기관 12,778대의 CCTV를 대상으로 이루어졌을 뿐이지만, "안내판 설치 64%, 음성 녹음 1.3%" 등 많은 문제점을 드러내었다. 행정안전부 개인정보보호팀, "공공기관 CCTV 관리실태 현장조사 결과", 2008.2. 참조.

으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.
④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.
⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.
⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.
⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다.
⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

다만 이 조항은 공원·도로·지하철, 상가 내부, 주차장 등 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 ‘공개된 장소’에 설치된 CCTV에만 적용되기 때문에, 비공개 장소에 설치된 CCTV의 경우에는 이 조항이 아니라 개인정보 보호법 제15조의 적용을 받는다. 즉, 특정인에 한하여 출입할 수 있는 사무실 등 비공개된 장소에 CCTV를 설치하고자 하는 경우에는 촬영 범위에 포함된 모든 정보주체의 동의를 받고, 안내판 설치나 보호조치 등은 공개된 장소에 설치된 영상정보처리기기 규정을 준용하는 것이 권장되고 있다.[31)]

그밖에 행정안전부는 「공공기관 영상정보처리기기 설치·운영 가이드라인」(2012.3)을 공표하고, 개인정보 보호법 시행령 등에서 보다 구체적으로 규정한 CCTV 운영단계별 지침을 8가지 원칙으로 제시하고 있다.

• 영상정보처리기기 설치·운영 제한 및 필요 최소한 촬영 금지 - 법 제25조 제1항과 제2항에 열거된 목적으로만 제한

• 영상정보처리기기 임의조작·녹음 금지

• 설치시 의견수렴 및 안내판 설치를 통한 설치 사실 공지 - 공공기관의 경우 △「행정절차법」에 따른 행정예고의 실시 또는 의견 청취(공청회 등) △ 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사. 안내판에는 △설치 목적 및 장소 △촬영 범위 및 시간 △관리책임자의 성명(직책) 및 연락처 △(영상정보처리기기 설치·

31) 행정안전부, 「공공기관 영상정보처리기기 설치·운영 가이드라인」, 2012.3, 2면.

F운영을 위탁한 경우) 위탁받는 자의 명칭 및 연락처 등을 기재

• 영상정보처리기기 운영·관리 방침 수립·공개 및 책임자 지정 - 운영·관리 방침에는 △영상정보처리기기의 설치 근거 및 설치 목적 △영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위 △관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람 △영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법 △영상정보 확인 방법 및 장소 △정보주체의 영상정보 열람 등 요구에 대한 조치 △영상정보 보호를 위한 기술적·관리적 및 물리적 조치 △그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항을 포함

• 영상정보의 목적외 이용·제공 제한 및 보관·파기 철저

• 영상정보처리기기의 설치·운영 위탁 시 관리·감독 철저 - 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 △위탁하는 사무의 목적 및 범위 △재위탁 제한에 관한 사항 △영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 △영상정보의 관리 현황 점검에 관한 사항 △위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항이 포함된 문서로 하여야 함

• 정보주체의 자기영상정보 열람권 보장 - 다만, 정보주체의 개인영상정보 열람 등 요구가 △범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우 △특정 정보주체의 영상정보만을 삭제하는 것이 기술적으로 현저히 곤란한 경우 △타인의 사생활권이 침해될 우려가 큰 경우 △기타 열람등의 요청을 거절할 만한 정당한 공익적 사유가 존재하는 경우에 해당하는 경우 요구를 거부할 수 있음

• 개인영상정보의 안전성 확보 조치 및 자체 점검 현황 등록 - 표준개인정보보호지침의 준수 여부에 대한 자체점검을 실시하여 그 결과를 행정안전부 장관에게 통보하고, 개인정보보호종합지원시스템(http://intra.privacy,go.kr)에 등록하는 한편, 홈페이지 등에 공개. 그밖에 공공기관은 위 각 운영사항에 대하여 표준개인정보보호지침에 따른 대장 등에 기록·관리

개인정보 보호법 외에 공공부문 CCTV 설치와 관련한 규정을 두고 있는 특별한 법률은 다음과 같다.

<표 Ⅲ-9> 공공부문 CCTV 설치에 대해 규정하고 있는 법률

법률	CCTV 관련 규정
형의 집행 및 수용자의 처우에 관한 법률 시행규칙	제162조(영상정보처리기기 설치) ① 영상정보처리기기 카메라는 교정시설의 주벽(周壁)·감시대·울타리·운동장·거실·작업장·접견실·전화실·조사실·진료실·복도·통용문(通用門), 그 밖에 법 제94조제1항에 따라 전자장비를 이용하여 계호하여야 할 필요가 있는 장소에 설치한다. ② 영상정보처리기기 모니터는 중앙통제실·관구실 그 밖에 교도관이 계호하기에 적정한 장소에 설치한다. ③ 거실에 영상정보처리기기 카메라를 설치하는 경우에는 용변을 보는 하반신의 모습이 촬영되지 아니하도록 카메라의 각도를 한정하거나 화장실 차폐시설을 설치하여야 한다.
군에서의 형의 집행 및 군수용자의 처우에 관한 법률 시행규칙	제115조(영상정보처리기기 설치) ① 영상정보처리기기 카메라는 군교정시설의 주벽(周壁)·감시대·울타리·운동장·거실·작업장·접견실·전화실·조사실·진료실·복도·통용문 그 밖에 법 제81조제1항에 따라 전자장비를 이용하여 계호하여야 할 필요가 있는 장소에 설치한다. ② 영상정보처리기기 모니터는 중앙통제실·관구실 그 밖에 군교도관이 계호하기에 적정한 장소(이하 “중앙통제실등”이라 한다)에 설치한다. ③ 거실에 영상정보처리기기 카메라를 설치하는 경우에는 용변을 보는 하반신의 모습이 촬영되지 아니하도록 카메라의 각도를 한정하거나 화장실 가림막시설을 설치하여야 한다.
외국인 보호규칙	제37조(안전대책) ② 소장은 예산의 범위에서 제1항에 따라 안전대책에 필요한 시설을 설치하여야 하며 영상정보 처리기기 등의 장비를 설치할 수 있다.
아동복지법	제32조(아동보호구역에서의 폐쇄회로 텔레비전 설치 등) ① 국가와 지방자치단체는 유괴 등 범죄의 위험으로부터 아동을 보호하기 위하여 필요하다고 인정하는 경우에는 다음 각 호의 어느 하나에 해당되는 시설의 주변구역을 아동보호구역으로 지정하여 폐쇄회로 텔레비전을 설치하거나 그 밖의 필요한 조치를 할 수 있다. 1. 「도시공원 및 녹지 등에 관한 법률」 제15조에 따른 도시공원 2. 「영유아보육법」 제10조에 따른 어린이집 3. 「초·중등교육법」 제38조 따른 초등학교 및 같은 법 제55조에 따른 특수학교 4. 「유아교육법」 제2조에 따른 유치원 ② 제1항에 따른 아동보호구역의 지정 기준 및 절차 등에 필요한 사항은 대통령령으로 정한다. ③ 이 법에서 정한 것 외에 폐쇄회로 텔레비전의 설치 등에 관한 사항은 「개인정보 보호법」에 따른다.
학교폭력예방 및 대책에 관한 법률	제20조의6(영상정보처리기기의 통합 관제) ① 국가 및 지방자치단체는 학교폭력 예방 업무를 효과적으로 수행하기 위하여 교육감과 협의하여 학교 내외에 설치된 영상정보처리기기(「개인정보 보호법」 제2조제7호에 따른 영상정보처리기기를 말한다. 이하 이 조에서 같다)를 통합하여 관제할 수 있다. 이 경우 국가 및 지방자치단체는 통합 관제 목적에 필요한 범위에서 최소한의 개인정보만을 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다. ② 제1항에 따라 영상정보처리기기를 통합 관제하려는 국가 및 지방자치단체는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

학교폭력예방 및 대책에 관한 법률(계속)	③ 제1항에 따라 학교 내외에 설치된 영상정보처리기기가 통합 관제되는 경우 해당 학교의 영상정보처리기기운영자는 「개인정보 보호법」 제25조제4항에 따른 조치를 통하여 그 사실을 정보주체에게 알려야 한다. ④ 통합 관제에 관하여 이 법에서 규정한 것을 제외하고는 「개인정보 보호법」을 적용한다. ⑤ 그 밖에 영상정보처리기기의 통합 관제에 필요한 사항은 대통령령으로 정한다.
지하공공보도시설의 결정·구조 및 설치기준에 관한 규칙	제12조(부대시설의 종류 및 설치기준) 지하공공보도시설에 설치하여야 하는 부대시설의 종류 및 설치기준은 다음과 같다. 2. 중앙방재실은 다음 각 목의 기준에 적합하게 설치할 것 다. 민방위기관·소방기관·경찰기관·가스사업자 및 지하역 방재기관(지하역과 접속되는 경우에 한한다) 등 관계 기관과 유무선 교신이 가능한 설비와 자체 감시카메라(CCTV) 설비를 갖출 것
보행안전 및 편의증진에 관한 법률	제24조(보행자 안전을 위한 영상정보처리기기 등의 설치) ① 특별시장·광역시장·특별자치시장·특별자치도지사·시장·군수 또는 자치구의 구청장은 범죄로부터 보행자를 안전하게 보호하기 위하여 필요하다고 인정하는 경우에는 보행자길에 영상정보처리기기나 보안등을 설치할 수 있다. ② 누구든지 제1항에 따라 설치된 영상정보처리기기나 보안등을 파손하여서는 아니 된다. ③ 제1항에 따른 영상정보처리기기 설치의 대상구역, 시설기준 등 필요한 사항은 행정안전부와 국토해양부의 공동부령으로 정한다. ④ 이 법에서 정하는 사항 외에 영상정보처리기기의 설치·운영, 안전조치 등은 「개인정보 보호법」에 따른다.
주차장법 시행규칙	제6조(노외주차장의 구조·설비기준) ① 법 제6조제1항에 따른 노외주차장의 구조·설비기준은 다음 각 호와 같다. 11. 주차대수 30대를 초과하는 규모의 자주식주차장으로서 지하식 또는 건축물식 노외주차장에는 관리사무소에서 주차장 내부 전체를 볼 수 있는 폐쇄회로 텔레비전 및 녹화장치를 포함하는 방범설비를 설치·관리하여야 하되, 다음 각 목의 사항을 준수하여야 한다. 가. 방범설비는 주차장의 바닥면으로부터 170센티미터의 높이에 있는 사물을 알아볼 수 있도록 설치하여야 한다. 나. 폐쇄회로 텔레비전과 녹화장치의 모니터 수가 같아야 한다. 다. 선명한 화질이 유지될 수 있도록 관리하여야 한다. 라. 촬영된 자료는 컴퓨터보안시스템을 설치하여 1개월 이상 보관하여야 한다.
자전거 이용시설의 구조·시설 기준에 관한 규칙	제16조(자전거 주차장의 설치) 「자전거 이용 활성화에 관한 법률」 제11조에 따라 설치하는 자전거 주차장은 다음 각 호의 기준에 맞게 설치하여야 한다. 2. 폐쇄회로 텔레비전 등 자전거 도난 예방 및 사후조치를 위한 시설을 설치하기 편리할 것
도로교통법 시행령	제87조 (권한의 위임에 따른 주차단속의 특례 등) ②특별시장·광역시장이 제1항에 따라 주차위반사실을 직접 적발·단속한 때에는 행정안전부령이 정하는 과태료부과대상차표지(제13조제1항에 따른 과태료 또는 범칙금 부과 및 견인대상차 표지를 포함한다. 이하 같다)를 붙인 후 그 표지가 붙은 해당 차를 촬영한 사진·비디오테이프나 그 밖의 영상기록매체(이하 “사진증거”라 한다) 또는 무인단속장비에 의하여 해당 차를 촬영한 사진증거 등의 증거자료와 위반장소·위반내용 및 차량번호 등을 기재한 서류를 갖추어 위반장소를 관할하는 구청장 또는 군수에게 통보하여야 한다.

자연공원법 시행령	제47조(국립공원 등에서의 과태료처분) ① 공단의 이사장이나 시·도지사는 그 소속 직원이나 공무원이 국립공원 또는 도립공원 안에서 법 제86조에 따라 과태료가 부과될 위반행위를 적발한 때에는 그 위반행위가 발생한 장소를 관할하는 군수에게 그 인적사항 및 사진·비디오테이프나 그 밖의 영상기록매체 또는 무인단속장비에 의하여 촬영한 사진 등의 자료와 위반장소·위반내용 등을 기재한 서류를 갖추어 이를 통보하여야 한다.
용산공원 조성 특별법 시행령	제27조(과태료의 부과·징수) ① 관리센터의 이사장이나 그 소속 직원이 용산공원 안에서 법 제63조에 따른 과태료 부과대상인 위반행위를 적발한 경우에는 위반행위자의 인적 사항 및 사진, 비디오테이프나 그 밖의 영상기록매체 또는 무인단속장비로 촬영한 사진 등의 자료와 위반장소, 위반내용 등을 적은 서류를 갖추어 국토해양부장관에게 통보하여야 한다.
민간인 통제선 이북지역의 산지관리에 관한 특별법 시행령	제14조(보전산지에서의 행위제한에 관한 특례) ⑤ 법 제21조제1항제9호에서 “대통령령으로 정하는 시설”이란 다음 각 호의 어느 하나에 해당하는 시설을 말한다. 1. 산불의 예방 및 진화 등을 위한 간이 무선통신시설, 간이 저수조(貯水槽), 방화선, 무인감시카메라
산림보호법 시행규칙	제5조(산림보호구역에서의 사업허가·신고 등) ② 법 제9조제2항제1호에서 “농림수산식품부령으로 정하는 산림보호시설”이란 산불예방 안내간판, 산림보호 안내간판, 산불감시초소, 산림보호 관리사(管理舍), 소화전, 무인감시카메라 시설물, 무인안내방송 시설물, 차량차단기 등을 말한다.

다. 공공기관 CCTV 현황

2011년 12월 기준으로 공공기관 CCTV는 365,337대로 집계된다. 행정안전부는 민간 CCTV의 규모를 332만대로 추산하고 있어 공공부문과 민간부문을 아울러 전체적으로는 총 368만 5천대의 CCTV가 설치·운영되고 있는 것으로 파악되고 있다. 공공기관 CCTV는 매년 큰 폭으로 증가해 오다가 개인정보 보호법이 제정발효한 2011년 그 증가세가 다소 둔화되었다.

<표 Ⅲ-10> 공공기관 CCTV 연도별 설치 현황

연도	대수	전년대비 증가율
2007년	99,957	-
2008년	157,197	157%
2009년	241,415	154%
2010년	309,227	128%
2011년	365,337	118%

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료 재구성

공공기관 CCTV의 목적별 설치 현황을 살펴보면, 시설안전 및 화재예방을 목적으로 설치된 경우가 207,782대(56.9%)로 가장 많았고, 범죄 예방을 목적으로 설치된 경우는 142,375대(39.0%)에 달했다.

<표 Ⅲ-10> 2011년 공공기관 CCTV 유형별·목적별 설치 현황

(단위 : 대)

기관유형			CCTV 설치대수	목적별 분류			
				범죄 예방	시설안전 및 화재예방	교통 단속	교통정보 수집·분석 및 제공
총계			365,337	142,375	207,782	11,648	3,532
국가행정기관	소계		97,174	26,340	65,619	4,499	716
	국가행정	본부	3,108	200	2,885	22	1
		소속기관	66,390	20,878	40,550	4,433	529
		공사/공단	27,676	5,262	22,184	44	186
자치단체	소계		132,036	51,331	71,900	6,328	2,477
	시도	본부	6,072	1,398	3,980	368	326
		소속기관	2,842	145	2,493	54	150
		공사/공단	27,207	3,944	22,868	159	236
	시군구	본부	85,585	44,292	34,163	5,425	1,705
		소속기관	3,043	1,059	1,676	248	60
		공사/공단	7,287	493	6,720	74	0
교육기관	소계		135,505	64,387	69,970	809	339
	교육청	본부	366	53	304	9	0
		소속기관	507	98	408	1	0
	각급학교	본교	126,478	60,620	64,772	769	317
		소속기관	3,853	2,498	1,330	18	7
	기타	기타	4,301	1,118	3,156	12	15

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료

라. 문제점

행정안전부는 영상정보처리기기를 설치·운영하려는 공공기관은 개인의 사생활이 침해되지 않도록 영상정보처리기기를 '최소한으로' 설치·운영하여야 한다는 원칙을 밝히고 있다.[32)]

그러나 공공기관 CCTV의 설치 과정에서 최소 설치 및 운영의 원칙은 관철되고 있지 않은 것으로 보인다. 행정안전부의 「2010년도 공공기관 개인정보 관리 실태점검 결과」에 따르면 (구)공공기관개인정보 보호법에서부터 규정된 의견수렴 절차를 이행한 기관은 53%(15개 기관 중 8개)에 지나지 않았으며, 안내판 설치 규정을 이행하지 않은 기관이 17%에 달했다. CCTV 설치·운영 지침을 수립한 기관도 66%에 불과한 것으로 나타나 법률에 따른 공공기관 CCTV의 설치 규제가 입법 목적에 비추어 매우 미흡한 현황이었다.

2009년 서울시 자치구를 대상으로 방범용 CCTV의 설치 및 운영 과정을 조사한 결과, 주민 의견수렴과정은 대개가 홈페이지 등을 통한 행정예고 등의 방법으로 안내하거나 형식적인 설문조사를 하는 데 그친 것으로 드러났다.[33] 주민들 입장에서는 문서로 된 고지나 동의 절차 없이 CCTV 설치 사실을 사전에 인지하는 것도 쉽지 않으며 반대 의견을 제시할 기회는 사실상 봉쇄되어 있는 셈이다.[34] 동의서나 공청회와 같이 비교적 적극적인 의견수렴 과정을 거친 것으로 평가되는 자치구조차도, CCTV 설치·운영에 대한 지침에서 규정하고 있는 △설치·운영되는 CCTV 카메라 대수·위치·성능 및 촬영범위 △정보주체의 권리행사 및 불복수단에 관한 내용·절차 및 방법 △CCTV 촬영시간, 화상정보의 보유기간, 화상정보의 보관·관리·삭제의 방법, 화상정보의 보관 장소 △녹화된 화상정보를 제3자에게 제공하거나 열람·재생토록 할 수 있는 사유와 그 절차 및 방법 등 구체적 사항에 대한 고지가 누락된 채 단순 찬반을 묻는 데 그쳤다. 이러한 형식으로는 정보주체가 CCTV 설치로 인해 자신들에게 미치는 영향을 정확히 인식하고 동의권을 행사하기에 부족할 수 밖에 없다.[35] 이는 일차적으로 법률이나 관련 가이드라인 어디에서도 CCTV 설치에 대한 주민들의 의사를 실질적으로 반영할 수 있는 의견수렴의 요건을 명확히 규정하지 않은데 따른

32) 행정안전부, 앞의 가이드라인, 2012.3.

33) 오병일 외, 앞의 보고서, 2009.

34) 관련하여, “지자체들은 CCTV 설치를 추진하면서 공청회나 여론수렴 등을 통해 주민동의를 먼저 구한 뒤 예산을 집행하는 것이 아니라, 자체적으로 설치장소를 선정한 뒤 주민의견 수렴 및 현장조사를 한다는 방침을 세워 놓고 있는 등 관련규정과 절차를 무시하고 있다”는 지적이 있다. “CCTV 맹신, 사생활은 없다?”, 부산일보, 2009.3.9.

35) “우리나라 공공장소 CCTV 설치를 해당지역주민의 80% 이상이 찬성하고 있다는 사실을 들며 CCTV 설치의 정당성을 이야기하는 입장이 있다. 그러나, 이것은 제대로 된 주민의견으로 볼 수 없는 면도 있다. CCTV 설치에 대한 주민의견을 물으려면, CCTV 설치의 좋은 점과 함께 통행인의 프라이버시권 침해를 위시한 여러 가지 CCTV 설치의 나쁜 점에 대한 대국민 계도도 있어야 한다. 그것이 없이 범죄감소 등 CCTV 설치의 좋은 점만을 집중적으로 홍보한 뒤 실시한 주민의견조사의 결과는 제대로 된 주민의견으로 보기 힘든 점이 있다.” 임지봉, “CCTV 개인영상정보 보호를 위한 개별 입법의 필요성 및 당위성”, 한국정보보호진흥원 개인정보보호기획팀 편, 「신규IT 서비스의 프라이버시 이슈리포트」. 2007.6.

문제로 볼 수 있다.[36]

이 점과 관련하여, 국가인권위원회는 CCTV 등 무인단속장비를 설치할 때 그로 인해 영향을 받는 이들에게 사전에 그 설치목적, 장소, 기기의 성능, 관리책임자(기관) 등의 내용에 대하여 충분히 고지하여야 하고, 동의를 구해야 하는 경우에는 동의의 절차, 대상 등에 대해 법률로 규정해야 한다고 하였다.[37] 국회에서도 공공기관 CCTV 관련 법률을 논의하면서 적극적인 주민 의견수렴 절차를 검토하였던 바 있다. 2005년 4월 행정자치위원회에서 검토된 「공공기관의 폐쇄회로 텔레비전 설치 및 개인의 화상정보 보호에 관한 법률안(김충환의원 대표발의안, 의안번호 제171287호)」에서는 CCTV를 설치하고자 하는 때 수집의 '법적 근거', '목적', '이용 범위' 및 '정보주체의 권리' 등에 관하여 '문서' 등을 통하여 미리 정보주체가 그 내용을 쉽게 확인 할 수 있도록 필요한 조치를 하고 정보주체의 '동의'를 얻을 수 있도록 하였다. 그러나 이 안은 CCTV 정보의 수집 대상이 불특정 다수인이기 때문에 정보주체에게 미리 동의를 얻거나 인식할 수 있게 하는 것이 방법상 어렵다는 이유로 반영되지 않았다.[38]

더불어, 공공기관이 설치한 CCTV에 대해서 추후 주민들의 동의 계속 여부나 CCTV의 설치 및 운영 목적에 따른 효과를 평가하는 절차가 전혀 보장되어 있지 않다는 사실은, 주민들의 개인정보자기결정권의 보장 측면에서 뿐 아니라 막대한 예산이 투여된 정책의 효과가 구체적으로 검증되고 있지 않다는 점에서 큰 문제로 보인다.[39] 또한 자동정보처리장치를 통해 CCTV 영상을 판독하고 이용하는 것에 대해서도 한정하는 규정이 없다. 최근 여러 CCTV 관제센터에 영상을 자동으로 판독하는 시스템이 도입되고 있는데,[40] 자동정보처리장치를

36) 관련하여, CCTV의 설치에 있어서 요구되는 전제조건에 대하여 '범죄예방 및 공익을 위하여 필요한 경우'라는 예시적 사항을 드는 것은 공공기관이 설치하는 CCTV가 지니는 관할로 인하여 한정적인 열거에 따른 제한적인 설정이 태생적으로 억제되어 있고 '행정절차법 소정의 공청회'를 절차적 필수사항으로 규정하고 있는 것은 행정처분이나 입법예고에 있어서 의견청취방식이 아니라 행정예고에 관한 공청회를 규정하고 있는 조항이 되어야 할 것으로 본다는 의견이 있다. 이민영, "공공기관의 개인정보보호에 관한 법적 쟁점", 「정보통신정책」 19권 10호 통권 417호(2007.6.1) 참조.

37) 국가인권위원회, 앞의 결정, 2004.4.19.

38) 행정자치위원회 수석전문위원. 2005.4. 公共機關의個人情報保護에관한法律中改正法律案【정부제출·공성진의원 대표발의·김재경의원 대표발의】, 공공기관의 폐쇄회로 텔레비전 설치 및 개인의 화상정보 보호에 관한 법률안【김충환의원 대표발의】검토보고서.

39) 관련하여, 미국 워싱턴 D.C. 「공공장소와 안전에 관한 조례」에서 경찰서장은 해당지역 주민들의 의견을 고려하여 CCTV를 통한 감시지속 여부를 결정해야 하며, 자신의 결정의 내용과 근거를 그들에게 공지·제시하여야 한다. 그리고 반년에 1회씩 주민회의에서 CCTV 감시의 최신현황을 보고하여야 하고, 매년 CCTV 감시체계 및 그 사용과 관련한 보고서를 제출하여야 한다. 법원의 허가를 받아 행한 감시의 경우 및 현안사건의 수사를 목적으로 행해진 경우에는 예외가 인정된다. 권건보, 앞의 글, 2009.

이용하는 것은 모니터 요원이 육안으로 영상정보를 판독하는 경우에 비하여 기본권 침해 정도가 높기 때문에 별도의 규정을 두는 것이 바람직하다.[41]

특히 영상정보의 목적외 이용·제공 제한에 관한 운영 실태는 매우 심각한 실정이다. 국가인권위원회는, CCTV 녹화기록이 개인의 초상 및 언제 어느 곳에 누구와 함께 있었는가에 관한 개인의 행적을 담고 있으며, 그 녹화기록물은 보유목적 외에 다른 행정목적이나 범죄 목적으로 사용될 가능성이 있으므로, 당사자의 동의나 적법한 근거에 따라서만 제3자에게 제공할 수 있도록 해야 한다고 지적하였다.[42] 그러나 최근 공중파방송 등 영상보도매체에서 CCTV 자료 활용이 크게 늘면서 보도의 선정성이 문제되고 있을 뿐 아니라 때로는 정보주체의 권리를 침해하고 있어 영상정보의 목적외 제3자 제공에 대한 엄밀한 규율이 시급한 실정이다.[43]

개인정보 보호법에 따르면 원칙적으로 수집 목적을 넘어서 개인영상정보를 이용하거나 제3자에게 제공할 수 없다. 다만 공공기관의 경우 △정보주체의 별도의 동의를 얻은 경우 △다른 법률에 특별한 규정이 있는 경우 △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 △통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우 △개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우 △조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 △범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우 △법원의 재판업무 수행을 위하여 필요한 경우 △형(刑) 및 감호, 보호처분의 집행을 위하여 필

40) 최근 CCTV의 자동판독시스템은 정상적인 모션과 그렇지 않은 모션을 구별하는 수준에까지 이르고 있다. “CCTV, 당신을 보고 있다”. SBS 뉴스추적, 2009.9.24, http://news.sbs.co.kr/section_news/news_read.jsp?news_id=N1000647258.

41) 관련하여 독일 연방개인정보 보호법상 개인들의 영상을 확대하고 추출해내거나 생체인식기술을 이용하여 그 주체를 인식하거나 사진을 비교하거나 프로필을 만들어 내기 위하여 자동화된 데이터베이스를 사용하는 경우에는 개인의 보호가치가 있는 이익들에 중대한 영향을 미치기 때문에, 그러한 자동화된 데이터베이스의 사용은 예외적으로만 허용된다고 해석되고 있다고 한다. 정태호, “CCTV 감시에 대한 개인정보 보호법의 규율에 대한 헌법적 평가”, 「헌법학연구」 제14권 제1호(2008.3) 참조.

42) 국가인권위원회, 앞의 결정, 2004.4.19.

43) 진보네트워크센터, “CCTV 화면 방송활용 신중해야”, 2010.12.29; 장여경, “MBC 어린이집 보도, 또 다른 폭력이다”, 미디어오늘, 2011.10.25.

요한 경우 예외를 인정하고 있다. 개인영상정보를 수집 목적 외로 이용하거나 제3자에게 제공하는 경우에는 표준개인정보보호지침 별지 서식 제3호 개인영상정보 관리대장을 활용하여 △개인영상정보 파일의 명칭 △이용하거나 제공받은 공공기관의 명칭 △이용 또는 제공의 목적 △법령상 이용 또는 제공근거가 있는 경우 그 근거 △이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간 △이용 또는 제공의 형태에 대한 사항을 기록하고 관리하여야 한다.[44]

그럼에도 불구하고 최근 수집 목적을 넘어서 개인영상정보를 이용하거나 제3자에게 제공하는 경우가 폭발적으로 증가하였다. 행정안전부가 2012년 국회 행정안전위원회 국정감사에서 진선미 의원에 제출한 “09년부터 서울시 CCTV 영상정보 제공현황”에 따르면, 영상정보 제공이 ’09년 2,101건에서 ’11년에는 1만 2,657건으로 6배 증가했고, 올해 8월까지 1만3,333건이나 제공됐다. 영상정보가 제공된 이후에 미반납·미파기된 건수도 총 제공건수의 2.6%인 811건이었다. 제공기관별로는 총 34,515건 중에 ‘경찰’에게 제공된 것이 99.5%인 3만 4,353건으로 절대 다수를 차지했고, ‘일반개인’에게 제공된 것이 0.4%인 126건, 기타 ‘법원·검찰’이나 ‘소방서’ 등에 제공됐다. 경찰은 각종 범죄수사 목적으로 CCTV 영상정보를 제공받거나 열람하고 있었고, 일반개인은 주로 지갑 등 분실물을 확인하기 위해 영상정보를 열람 혹은 제공받고 있었다.

<표 Ⅲ-11> 서울시 CCTV 영상정보 제공 현황

(단위: 건, %)

구분	제공형태			제공기관						제공후 미반납·미파기 건수
	제공	열람	합계	경찰	법원 검찰	소방서	일반 개인	기타	합계	
2009	1,856	245	2,101	1,996	-	-	32	1	2,029	16
2010	5,814	685	6499	6,473	1	-	22	3	6,499	34
2011	11,141	1,516	12,657	12,615	1	3	32	9	12,660	38
2012.8	11,873	1,460	13,333	13,269	4	1	40	14	13,327	723
합계 (%)	30,684 (88.7)	3,906 (11.3)	34,590 (100)	34,353 (99.5)	6 (0.0)	4 (0.0)	126 (0.4)	27 (0.1)	34,515 (100)	811 (2.6)

* 자료: 행정안전부·서울시

* 주: 서울시 본청, 자치구, 사업소 포함

44) 행정안전부, 앞의 가이드라인, 2012.3.

그런데 경찰은 CCTV정보 제공요청 절차, 수사에 활용, 활용후 파기·반납 등 사후조치에 대한 세부 매뉴얼도 마련하고 있지 않고 그 처분을 영상정보를 제공받은 수사관들에게 맡겨 놓고 있는 상태다. 성범죄 등 민감성 영상정보의 유출 우려가 큰 상황인 것이다. 2009년 조사에서도 자치구로부터 방범용 CCTV의 운영을 수탁받은 경찰관서가 이를 운영하는 실태는 위탁기관인 자치구가 파악하고 있는 바와 다른 것으로 드러나 충격을 준 바 있다.[45] 대개의 자치구는 방범용 CCTV 영상 기록에 대하여 「공공기관 CCTV 관리 가이드라인」에 명시된 30일 이후 자동삭제한다고 답변하였으나 서울 경찰관서 31개 가운데 15개 관서는 “필요한 경우 운용감독관이나 운용책임관의 건의로 경찰서장의 승인받아 관련사건 종결시까지 보존기간을 연장하여 특별관리”한다고 밝혀 CCTV 영상 기록 원본의 삭제와 별도로 사본을 보유하고 있었다.[46]

주무부처인 행정안전부가 CCTV 영상정보가 누가 어떻게 열람·제공되는지 그 현황도 파악하고 있지 않다는 사실은 더욱 심각한 문제이다. 영상정보를 제공받은 자가 어떻게 활용하고 파기하고 있는지에 대한 관리실태조사는 더더욱 없었다. 경찰은 수사를 위해 공공기관뿐만 아니라 다양한 민간주체들로부터 영상정보를 제공받고 있다는 점에서 개인정보보호 사각지대를 해소하기 위한 제도개선이 필요하다.[47]

한편 최근 「학교폭력예방 및 대책에 관한 법률」 등에서 통합 관제에 대한 사항을 규정하는 등, 통합 관제가 확대되는 추세이다. 기관간 또는 자치단체간에 인력과 장비를 공유함으로써 적은 자원으로 효과적인 방범을 수행할 수 있는 역할분담 및 협력체계를 강구하자는 것이다. 행정안전부도 이러한 추세를 반영하여 2009년 9월에 「공공기관 CCTV 관리 가이드라인」을 갱신하면서 ‘CCTV 통합 관리’에 대한 규정을 신설하였던 바 있다. 여기서 ‘CCTV 통합 관리’란 기관내 또는 기관간에 용도별·지역별 CCTV를 물리적·관리적으로 통합하여 모니터링 등을 수행하는 것을 말한다. 그러나 기관내 CCTV를 통합 관리하는 것은 방범용, 쓰레기 투기방지, 시설물 관리, 주차관리, 교통정보 수집 등 고유의 목적으로 설치된 CCTV를 다목적으로 사용하겠다는 것으로서, 개인정

45) 오병일 외, 앞의 보고서, 2009.

46) 일본의 경우 공권력이 설치한 범죄예방 목적의 TV 카메라는 녹화하지 않는 것이 원칙이다. 즉 녹화되지 않는 것을 전제로 하여 ① 실제로 범죄가 실행중이거나 실행직후인 경우로서 ② 증거보전의 필요성과 긴급성이 있고, ③ 그 촬영이 일반적으로 허용되는 한도를 넘지 않는 상당한 방법으로 이루어진다는 조건하에서 CCTV 설치가 허용될 수 있지만, 녹화되는 경우는 범죄예방을 목적으로 한다고 하더라도 CCTV 설치가 허용되지 않는다는 판결이 주목을 받고 있다. 권건보, 앞의 글, 2009.

47) 2012년 국회 행정안전위원회 국정감사 진선미 의원 보도자료(2012.10.8).

보 수집장치를 목적 외의 용도로 활용할 수 없도록 한 개인정보 보호 원칙과 현행 법률에 반하는 것이다.[48] 기관간 CCTV를 통합관리하는 것은 지역 주민 등 이해관계인으로부터 의견수렴 및 동의를 받고 설치된 CCTV의 이용 범위를 넘어선 것으로서 정보주체의 권리를 형해화할 위험이 있다. 개정되기 전의 「공공기관 CCTV 관리 가이드라인」에서도 CCTV를 여러 목적으로 사용하고자 하는 경우 사전의견수렴시 사용 목적을 나열하여 의견수렴을 하고 안내판 등 설치사실 공지시 다목적용 CCTV임을 공지하도록 하며 다목적용 CCTV를 설치·운영할 경우 행정안전부와 사전협의를 하도록 하는 등 다목적 CCTV를 일반 CCTV보다 한층 엄격하게 규제해 왔었다. 이러한 점에서 최근 행정편의적인 수요에 초점을 두어 CCTV 통합 관리가 무비판적으로 확대되는 추세는 상당히 우려스럽다 할 것이다.

개인정보 보호법의 제정발효 이후 행정안전부는 「공공기관 영상정보처리기기 설치·운영 가이드라인」(2012.3)을 발표하면서 '통합관리를 위한 목적사항 추가시' ①목적 변경에 따른 관계 전문가 및 이해관계인의 의견 수렴 ②안내판에 추가된 설치 목적 및 통합관리에 관한 내용을 기재하는 절차를 거치도록 하였다. 그러나 행정안전부가 사실상 안내판 문구 변경을 통해 법률을 편법적으로 운용하고 통합 관제를 광범위하게 허용하는 방침을 갖고 있다는 사실은 매우 유감이다. 개인정보 보호법이 그 시행 이후로도 CCTV 규율을 위한 제 역할을 못하고 있다는 비판을 받고 있는 한 가지 이유가 여기에 있다.

마. 정책 제언

공공기관 CCTV를 통한 개인정보의 수집은 필요최소한으로 이루어져야 한다. 이는 개인정보 보호법에서 천명한 원칙에 명시된바 대로이다.

> 제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

CCTV는 매우 광범위한 규모로 다양한 개인정보를 수집하는 개인정보 자동

48) 이와 관련하여, 미국 워싱턴시의 CCTV 통합운용계획에 대해 시민단체들은 감시카메라를 한곳에 모아 놓고 관리하는 것은 아무라도 감시할 수 있는 무서운 영화 같은 시나리오에 한 발짝 다가가는 일이라며 거세게 반대하고 있다. "워싱턴 CCTV 통합운용 논란", 문화일보, 2008.4.11.

수집장치이기 때문에 필요최소한으로 설치하도록 설치 시점부터 사전적으로 규제하는 것이 중요하다. 그러나 현행 법률상 공공기관의 CCTV 설치가 매우 폭넓게 인정되고 있으며, 의견수렴은 형식적으로 이루어지고 있다.

CCTV가 엄격하게 설치 목적 내로 운영되도록 하려면, 설치 후 규제도 중요하지만 CCTV를 필요최소한으로 설치하도록 사전적으로 규제하는 것이 무엇보다 중요하다. 현행 법률이 CCTV 설치 자체를 금지하는 규정이나 그 기준을 정하지 않은 것은 불충분한 입법이라는 비판을 피할 수 없다. 자칫하면 법적 규제가 CCTV의 설치를 사실상 추인하는 근거로만 사용될 수 있기 때문이다.

(구)정보통신부의 「CCTV 개인영상정보보호 가이드라인」에서는 CCTV를 설치할 때 "정보주체의 초상권, 사생활의 비밀과 자유 등의 침해할 위험이 없는지를 사전에 분석·검토하여 이를 최소화할 수 있는 수단을 강구하여야 한다"고 하였으며, "특정인을 감시할 목적으로" CCTV를 설치해서는 안된다고 명시하였다(동가이드라인 제4조).[49] 국가인권위원회는 CCTV 등 무인단속장비의 설치와 운영이 법률에 근거를 두더라도 그 내용이 명확하고 상세하지 않으면 이 역시 국민의 기본권에 대한 과잉 제한이 되므로, 범죄예방과 범죄수사의 효율성을 높이기 위한 원칙적이고 일반적인 조처들이 검토되고 강구된 후 그러한 조처들로도 범죄예방과 수사라는 목적을 효율적으로 달성할 수 없는 "필요한 경우에 한하여" 동원되는 보충적 수단임을 명확히 해야 한다고 지적한 바 있다.[50]

따라서 법률상 CCTV 설치 목적을 명확히 한정하고, 주민 등 이해관계인에게 CCTV의 설치에 대한 동의 여부를 물을 때는 정보주체가 동의권을 충분히 행사할 수 있도록 상세한 정보제공과 함께 공청회 등 적극적인 의견수렴 형식을 갖추는 것이 바람직하다.

나아가 국가인권위원회가 지적한 바와 같이, "급증하고 있는 영상정보처리기기 설치 경향과 아울러 공공·민간부문의 영상정보처리기기 통합관리 시 예상되는 업무과중을 고려하여 영상정보처리기기에 대한 사후적 관리 외에 등록제 등과 같은 사전적·예방적 관리 규정을 신설"하는 것을 검토해 봄직하다.[51]

---

49) 캐나다 비디오감시가이드라인(Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities)에서는 CCTV가 "현존하는 실질적 문제에 대응하기 위해서만 설치되어야" 하며, "프라이버시 침해를 대체할만한 수단이 없을 때에만 예외적으로 시행되어야" 하고, "시행 이전에 프라이버시에 대한 영향평가가 이루어져야" 한다고 명시하고 있다. 정보통신부, 「CCTV 개인영상정보보호 가이드라인」, 2007.11.

50) 국가인권위원회, 앞의 결정, 2004.4.19.

51) 국가인권위원회, "「개인정보 보호법 제정 법률안(정부입법발의)」 중 영상정보처리기기 관련 규정에 대

더불어 개인정보 보호법에서 '개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우' 공공기관 간의 목적 외 영상정보 제공에 대하여 폭넓은 예외를 인정하고 있는 부분에 대해서는 관련 규정의 보완이 시급해 보인다.[52] 특히 개인정보 보호법이나 관련 가이드라인에서 CCTV가 표현의 자유에 대한 제한이나 차별적 목적으로 이용하는 것을 금지하는 아무런 규정을 두고 있지 않다. CCTV를 집회의 자유를 비롯한 헌법이 보장한 기본권을 행사하는 사람들을 위축시키기 위해 사용하거나 감시시스템 운영자가 선입견을 가지고 사회의 주변집단을 주된 감시대상으로 선정하는 등 차별적인 감시조치가 행해질 위험도 있다. 그러므로 감시시스템을 그와 같이 오남용하는 것을 금지하는 명문의 규정을 두는 것이 바람직하다.[53]

또한 목적외 이용의 가능성을 줄이기 위하여 파기 규정을 명확히 하고 일정한 수준에서 정보주체에 대한 통지 제도를 모색할 필요가 있다. 과거 국회에서 공공기관 CCTV 관련 법률이 논의될 당시에는 CCTV 정보 제공에 대한 통지 제도를 검토했던 바 있다. 앞서 김충환의원 대표발의안에서는 "공공기관의 장은 명백히 수집 목적과 관계없이 수집일 이후 30일이 경과한 화상정보를 즉시 파기하여야 한다. 다만, 당해 화상정보를 수사나 재판자료로 제공하는 경우는 그러하지 아니하다"고 하여 CCTV 처리정보의 파기를 강력하게 의무화하였을 뿐더러, "화상정보를 수사나 재판자료로 제공하는 경우 그 사실을 당해 개인에게 알려 주어야 한다"라는 규정을 덧붙여 자신의 개인정보 처리 사실에 대한 정보주체의 알 권리를 보장하였다.

한 의견표명", 2009.12.3.

52) 관련하여 정태호(앞의 글, 2008)는 독일의 연방개인정보보호법의 경우 국가 및 공공의 안전에 대한 위험을 방지하기 위하여 필요하거나 범죄행위의 소추를 위하여 필요한 경우에만 목적외 사용을 허용함으로써 목적구속의 원칙을 엄격하게 관철하고 있고, 워싱턴 D.C. CCTV 자치령에서는 영상의 모니터링을 범죄의 탐지와 감시, 범죄나 범죄혐의의 증거 확보, 교통관리를 위해서만 할 수 있도록 하고, 그 정보를 기타의 목적으로 사용하는 것을 허용하지 않고 있다고 지적하였다.

53) 이와 관련하여 정태호(앞의 글, 2008)는 감시공간에서 집회가 개최되는 동안에는 CCTV 가동을 중단함으로써 집회참여자가 심리적 압박감 없이 자유롭게 집회에 참가할 수 있도록 해야 한다고 주장하였다. 폭력행위 가담자 색출을 위한 비디오촬영은 폭력집회의 구체적인 위험이 존재하는 경우에 예외적으로 정당화될 수 있다는 것이다. 미국 워싱턴 D.C. 콜럼비아 특별구 경찰의 CCTV 사용에 관한 자치령에서는 수정헌법 제1조의 표현의 자유의 보호를 받는 전단 배부 등에 초점을 맞추어 감시하는 것을 금지하고 있으며, 인종, 종족, 성별, 성적 취향, 장애, 여타의 차별기준에 근거한 차별적 감시도 금지하고 있다고 한다.

IV. 개인정보 보호위원회의 역할

가. 개인정보의 활용의 확장과 그에 대한 규제의 필요성

1) 개인정보의 활용의 확장과 그로 인한 문제

가) 개인정보의 역할 변화

최근 소셜네트워크서비스(SNS)나, 스마트폰, 태블릿 컴퓨터 등이 새로운 정보의 생산, 유통 및 소비의 유형으로 등장하면서 개인정보의 활용범위가 크게 넓어졌다. 개인정보는 갈수록 시장 서비스에서 매우 독특하고 중요한 역할을 담당하고 있으며, 개인정보를 통하거나 매개로 한 고착효과(lock in effect)가 발생하고 있다. 이 과정에서 개인정보가 정보를 축적한 기업의 기득권으로 작용하면서 독점이 강화되고 경쟁을 저해하는 효과를 보이고 있다. 구글, 페이스북, 카카오톡, 애플 등 선도기업들이 개인정보를 매개로 독점을 강화하는 현상이 대표적이다. 기업들이 수집하는 개인정보(예를 들어 페이스북의 친구목록이나, 친구들의 평가, 언급 등과 같은 정보)가 단순한 개인의 정보를 넘어서서 사회적 관계망에 대한 정보 또는 사회적 관계망 그 자체라는 점에 주목할 필요가 있다.

나) 개인정보의 수집, 활용과 관련한 문제들

사회적 관계망이 일부 기업에 의해 집중되면서, 사회적 관계망은 급속도로 상업화되고 있다. 상업화는 필연적으로 '공론의 장'인 사회적 관계망의 공공성을 훼손시킨다. 이러한 양상은 개인정보 보호의 문제를 사생활 보호 뿐만 아니라 공정경쟁, 민주주의, 사회적 관계망의 공공성 보장, 다원주의의 보장 등의 다양한 관점에서 보아야 한다는 것을 보여준다.

구글의 개인정보 통합의 문제나 애플의 아이폰에 의한 위치정보나 개인정보

의 수집, 페이스북의 개인정보 정책의 변경 등을 둘러싼 논란에서 드러났듯이, 그러한 정책의 변경이 미치는 영향은 단순한 사생활 보호의 문제를 넘어선다. 이는 정보통신 서비스에서의 독점의 강화, 사회적 네트워크의 독점화, 그로 인한 사회적 네트워크의 공공성의 훼손, 다양성의 훼손 등의 문제와도 관련이 되는 것이다.

2) 개인정보 보호 관련 감독기관의 필요성과 역할

가) 개인정보 보호 관련 감독기관의 필요성

개인정보 보호 관련 감독기관은 공정경쟁의 보장이나, 민주주의의 보장, 사회적 관계망의 공공성 보장, 다원주의의 보장 등을 주요한 과제로 삼고, 이를 보장하기 위한 역할도 적극적으로 수행해야 한다.

개인정보의 처리나 그로 인한 침해가 대규모로 신속하게 이루어지기 때문에 권리구제도 신속해야 하고, 구제절차는 간편하게 활용될 수 있어야 한다. 개인정보의 축적과 활용은 짧은 시간 내에 선점효과를 가져오기 때문에, 신속한 시정을 하지 않을 경우 선점에 의한 부정적인 효과가 고착되고, 결과를 시정하기 어려워지기 때문이다.

개인정보 보호 관련 감독기관은 이런 점을 종합적으로 고려해서 설계되어야 한다.

나) 개인정보 보호 관련 감독기관의 역할

세계 여러나라 개인정보 보호 관련 감독기관은 정책 기능과 시장 및 공공부문의 감독기능, 위법시정 및 권리구제 기능, 그 외에 교육, 홍보, 연구 등의 기능과 개인정보처리와 관련한 등록과 같은 행정기능을 갖고 있다.

‘정책 기능’은 직접 정책 형성을 하는 것에서부터 단순한 권고에 그치는 것까지 다양한 스펙트럼이 존재한다. 정책의 조율을 하는 기능, 총괄적으로 정책을 결정하는 기능, 정책에 대한 의견을 제시하는 기능, 실제로 행정입법을 제정하는 기능, 직접 행정입법을 제정하지는 않고 의견을 제시하여 제정을 하도록 하는 기능 등을 들 수 있다.

‘권리구제 기능’은 그 대상 분야에 따라, 민간 분야의 개인정보 보호에 대한 권리구제를 하는 기능과, 공공분야의 개인정보 보호에 대한 권리구제를 하는 기능이 있다. 그 방식과 효과도 사법절차를 준용하는 유형과, 옴부즈만형으로

나뉜다. 결정의 효력에서도 법적인 구속력이 부여되는 유형과 권고의 효력만 부여하는 유형이 있다.

3) 분야별로 분산된 개인정보보호 감독기관이 바람직한지, 종합적인 개인정보보호 감독기관이 바람직한지?

가) 종합적인 개인정보보호 감독기관이 바람직함

개인정보보호 감독기관이 각 분야별로 분산되어 존재할 경우에는 각 분야별 특수성에 맞는 규제가 가능할 수 있다는 장점을 기대해 볼 수 있으나, 반면 각 분야별 특수성에 매몰되어 개인정보 보호나 부당한 개인정보의 이용을 막지 못하게 될 가능성도 있다.

개인정보보호 감독기관은 전문적이고 기술적인 내용에 대해서까지 이해가 필요하고, 수많은 침해에 대한 신속한 권리구제를 수행할 수 있는 조직과 역량을 갖춰야 한다. 이런 요구들을 충족하기 위해서는 각 영역별로 분산된 개인정보보호 감독기관보다는 종합적인 개인정보보호 감독기관이 더 적절하고, 바람직하다.

나) 해외의 사례

다음 표에서 보다시피 외국의 개인정보 보호 감독 및 감독기관은 대부분 종합적인 개인정보보호 관련 감독기관으로 설립되어 운영되고 있다. 캐나다, 오스트레일리아, 뉴질랜드, 유럽의 각국은 이러한 종합적인 개인정보보호 관련 규제 및 감독기관을 두고, 그곳에서 집중하여 개인정보 보호 기구로서의 역할을 수행한다.

개인정보보호 감독기관들은 각종 개인정보 침해사건 접수, 당사자에 대한 자료제출 요구, 의견청취, 현장조사 등의 사실조사, 사실조사에 의한 법규 위반여부의 심사, 화해 권고와 분쟁조정, 시정조치 명령, 이행명령, 불이행시의 법원에의 소제기나 형사고발, 소송지원, 프라이버시 침해여부에 대한 직권 실태조사와 감독, 개인정보 보호 원칙 및 법규의 준수여부 감독, 이행명령의 부과, 이행명령 불이행시나 법규 위반 확인시 고발, 개인정보 보호 실행규칙 제정, 개인정보 보호와 관련한 정책의 제시, 의견의 제시, 법안에 대한 의견제시, 개인정보보호와 관련한 연구, 교육, 홍보, 국제협력 활동 등과 같은 다양한 역할을 고루 담당하고 있다.

<표 IV-1> 2012년 상반기 캐나다 개인정보보호 감독관의 활동 내용

일자	활동
2012. 6. 14	중소기업의 클라우드 서비스 이용에 대한 안내
2012. 6. 5	청소년 프라이버시를 위협하는 새로운 기술에 대한 보고서
2012. 6. 4	민간부문 프라이버시 문제에 대한 연례 보고서
2012. 5. 4	전자적으로 보관되는 개인정보의 보호에 있어 캐나다 기업의 부족한 점에 대한 여론조사
2012. 5. 2	프라이버시 증진을 위한 연구와 활동에 5십만 달러 포상
2012. 4. 17	민간 부문의 효과적인 프라이버시 관리에 대해 개관
2012. 4. 5	연구 심포지엄 개최
2012. 4. 4	페이스북 프라이버시 정책에 대한 조사 결과 발표
2012. 4. 2	국경간 개인정보 교환 등 보안 시행 계획에 있어 연방정부에 개인정보 보호법 준수를 요구
2012. 3. 28	제4차 전국 청소년 동영상 컨테스트 우승자 발표
2012. 3. 28	수사기관의 처분에 대한 조사
2012. 3. 27	외부 자문위원 위촉
2012. 3. 8	구글 프라이버시 정책에 대한 답변
2012. 3. 1	청소년이 이용하는 소셜네트워크사이트들의 개인정보 보호법 위반
2012. 1. 24	청소년 인터넷 이용자들의 프라이버시 보호를 위한 새로운 도구 발표
2012. 1. 5	2012년 연간 계획 발표
2012. 1. 4	민간 부문 프라이버시 보호를 위한 양해각서 체결

* 출처: http://www.priv.gc.ca/

나. 개인정보 보호법 제정과 제정과정의 개인정보보호 감독기관의 역할과 권한 왜곡

1) 개인정보 보호법에 의해 도입된 개인정보 보호위원회의 권한, 위상, 역할

가) 개인정보 보호를 위한 가장 중요한 변화는 개인정보 보호위원회

「개인정보 보호법」의 시행으로 인한 가장 큰 변화는 새롭게 발족한 개인정보 보호위원회를 들 수 있다. 해외 각국의 경험에서도 개인정보 보호위원회는 개인정보 보호의 핵심적 역할을 수행하고 있다.

나) 개인정보 보호위원회의 독립성 보장

개인정보 보호에 관한 국제적인 기준들은 개인정보보호 감독기관의 독립성을 강조하고 있다. 1990년 「UN 컴퓨터화된 개인 정보파일의 규율에 관한 지침」에서는 “모든 국가들은 열거된 원칙들의 준수를 감시할 독립된 기관을 설치”하도록 하고 있으며, 「개인정보 보호에 관한 유럽의회와 각료회의 지침(95/46/EC)」에서는 제28조(감독기관)에서 “당해 기관은 위임받은 임무를 완전히 독립적으로 수행한다”고 하고 있다. 「UN 컴퓨터화된 개인 정보파일의 규율에 관한 지침」 및 2001년 유럽이사회(Council of Europe)가 채택한 「감독기구와 국경 간 정보이동과 관련한 개인정보의 자동처리에 관한 개인 보호협약의 추가의정서」에서는 개인정보보호 감독기관에게 필요한 권한 및 독립성을 위한 요건을 규정하고 있다. 개인정보보호 감독기관의 권한으로는 △정보제출 요구를 포함한 조사권(investigation) △개인정보수집자에게 수정, 삭제, 폐기를 명령할 수 있는 권한, 개인정보의 유통금지 명령권, 국회나 기관에 대한 의견제시권, 공표권, 분쟁조정 권한, 침해신고의 접수 등 개입권 △법적 절차를 개시할 권한 혹은 사법기관에 소추할 권한 등을 포함하고 있다. 또한, 개인정보보호 감독기관은 이러한 권한을 완전히 독립적으로 수행해야 하는데, 이에는 감독기관의 구성, 위원의 임명방법, 임기와 해촉 조건, 충분한 자원의 배분, 외부 명령없이 결정을 채택할 수 있는지의 여부 등이 관련이 된다.

국제적인 기준에 비추어 보았을 때, 한국의 개인정보 보호위원회는 독립성을 보장받고 있지 못하며, 충분한 권한도 가지고 있지 못한 상황이다.

다) 개인정보 보호위원회의 권한과 역할의 왜곡

한국 개인정보 보호법의 문제는 대부분의 감독기능이 행정안전부에 있다는 것이다. 개인정보 보호위원회는 공공부문에 대한 시정권고권만 있을 뿐이다. 인터넷, 금융 등 분야별로 개인정보보호 감독기관이 별도로 존재하여 개인정보 보호위원회의 권한은 미비할 뿐 아니라, 독립성이 약화되어 있다. 또한 개인정보 보호위원회에는 행정입법권도 없고 조사권도 제한되어 있으며, 권리구제 권한도 제한되어 있다. 현재 개인정보 권리구제는 행정안전부장관 산하조직인 개인정보분쟁조정위원회가 별도로 담당하고 있는 상황이다.

2) 우리나라의 개인정보 보호법의 제정과정에서 독립감독위원회인 개인정보 보호위원회의 역할에 대한 논의의 변화와 논의의 왜곡

가) 7개의 법안

최초의 개인정보 보호법안은 2004년 11월 22일 제17대 국회에서 민주노동당의 노회찬 의원 등 22인이 인권시민사회단체들과의 논의 끝에 발의한 「개인정보보호기본법안」(의안번호: 170938)이다. 노회찬 의원안 외에 「개인정보보호법안」(정성호의원등 11인, 의안번호: 171323), 「개인정보 보호법안」(이은영의원 외 145인, 의안번호: 172219),[1] 「개인정보 보호법안」(이혜훈의원등 13인, 의안번호: 172953) 등 17대 국회 동안 총 4개의 개인정보 보호법안이 제안되었다. 여당 변재일 의원 등의 주도로 통합안을 마련하기 위한 논의가 막후에서 이루어졌으나 끝내 합의가 이루어지지 못한 채 이 법안들은 17대 국회 임기만료와 더불어 폐기되었다.

제18대 국회 들어서는 3개의 개인정보 보호법안이 제안되었다. 17대 국회에서 개인정보 보호법안을 발의한 바 있는 이혜훈 의원의 「개인정보 보호법안」(이혜훈의원등 15인, 의안번호: 1800570)이 발의된 데 이어, 역시 17대 국회에서 통합안 논의를 주도하였던 변재일 의원의 「개인정보 보호법안」(변재일의원등 13인, 의안번호: 1801598)이 발의되었다. 한편 이명박 정부 들어서 (구)행정자치부가 행정안전부로 재편되면서 전자정부 및 개인정보 관련 업무가 이관되었고, 행정안정부는 2008년 11월 28일 「개인정보 보호법안」을 발의하였다. 국회 검토과정에서는 정부안을 중심으로 논의가 이루어졌으나 행정안전부 중심의 개인정보 보호 추진체계에 대한 인권시민사회단체들의 문제제기가 일부 받아들여져, 일부 내용이 수정된 대안이 2011년 3월 11일 국회 본회의를 통과, 지금의 개인정보 보호법 시행에 이르게 되었다.

나) 개인정보 보호위원회 역할에 대한 합의

17대 국회에서는 모든 개인정보 보호법안이 개인정보 보호위원회를 독립적인 감독기관으로 두는 것으로 하여, 개인정보 보호위원회의 역할과 위상에 대해서 큰 이견이 없었다.

17대 국회에 제출된 이은영 의원 등 145명의 「개인정보 보호법안」은 개인정보 보호위원회의 기능과 역할에 대해서 다음과 같은 규정을 두고 있었으며, 다른 법률안들도 대체로 이은영 의원안과 유사한 수준의 기능과 역할을 부여하고 있었다.

1) 이은영 의원안은 본래 「개인정보보호기본법안」(의안번호: 171334)으로 발의되었으나 국가인권위원회를 개인정보보호 감독기관으로 한 것에 대한 논란 끝에 원안 철회 후 재발의되었다.

• 국가에게 개인정보보호 시책의 강구와 제도 및 사회적 관행의 개선을 위한 책무를 규정하고, 개인정보 보호위원회가 개인정보에 관한 시책을 관장하도록 함(안 제18조 및 제19조).

• 개인정보 보호위원회는 국무총리 소속하에 설치함(안 제24조)

• 개인정보 보호위원회는 개인정보 침해사건에 관하여 자료제출, 현황조회 및 방문조사를 할 수 있도록 함으로써 실질적·효과적인 구제기능을 수행할 수 있도록 함(안 제37조 및 38조)

• 개인정보 침해사건에 대하여 필요한 경우 시정명령 등을 발할 수 있도록 하여 신속한 피해구제 및 구제의 실효성을 보장함(안 제40조)

• 개인정보에 관한 분쟁 조정업무를 신속하고 공정하게 처리하기 위하여 개인정보 보호위원회에 개인정보분쟁조정위원회를 둠(제43조).

• 개인정보 보호위원회는 정책기능, 권리구제기능에 대하여 종합적인 기능을 담당함

다) 18대 국회의 개인정보 보호법안과 정부안의 개인정보보호 감독기관

18대 국회 개원 후 이혜훈 의원안과 변재일 의원안의 두 개의 개인정보 보호법안이 제출되었으나 행정안전부가 정부안을 내면서 갑자기 개인정보 보호위원회의 위상과 역할이 개인정보 보호법안의 가장 핵심적인 쟁점으로 떠오르게 되었다.

정부안에서는 개인정보 보호와 관련한 모든 업무를 행정안전부가 수행하는 것으로 하고, 개인정보 보호위원회는 행정안전부의 심의기구로 전락시켰다. 정부안은 개인정보 보호위원회를 설치하는데(안 제9조 및 제10조), 그 기능으로 개인정보 보호 기본계획, 법령 및 제도 개선 등 개인정보에 관한 주요 사항을 심의하는 것으로 국한하였고, 개인정보 보호와 감독의 권한을 모두 행정안전부가 수행하는 것으로 하였다. 이러한 정부안에 대해서 야당과 시민사회단체는 강력히 반발하였다.

결국 국회에서 여야간의 논의를 통해 개인정보 보호위원회는 대통령 직속의 독립성을 갖는 조직으로서, 개인정보 보호에 관한 법률, 정책, 제도에 대한 의견제시를 하고, 공공부문의 개인정보 침해에 대한 시정조치권을 갖는 독립적인 감독기관으로 하기로 합의가 이루어졌다.

그러나 이렇게 해서 탄생하게 된 현재의 개인정보 보호위원회는 개인정보 보

호 업무를 종합적 포괄적으로 수행하지 못하고, 독립성도 제대로 보장되지 못하는 조직으로 전락한 상황이다. 공공부문에 대해서만 개인정보 침해행위를 조사하고, 위법한 것에 대해서 시정을 권고할 수 있는 권한을 가질 뿐, 민간부분에 대한 개인정보 침해행위에 대한 조사나 권리구제 기능을 가지고 있지 못하기 때문이다. 이는 대부분의 국가에서 개인정보보호 감독기관이 민간 분야에서 옴부즈만형 권리구제 기구의 역할을 하고 있는 것과 대조적이다. 개인정보 보호위원회는 행정입법권도 갖지 못하고 있다. 개인정보 침해에 대한 분쟁조정기능도 개인정보 보호위원회에서 수행하지 않고, 행정안전부장관이 임명하는 개인정보분쟁조정위원회를 따로 두고 있다. 개인정보침해에 대한 신고를 받아 조사를 하고 조치를 하는 조직도 인터넷진흥원 산하 개인정보침해신고센터로서 별도로 두고 있다. 결국 개인정보 보호 기능이 여러 곳에 분산되는 형태로 입법화되어 있다.

다. 입법개선 과제 - 분야별 감독권한의 분산으로 인한 문제를 해결하기 위해 개인정보 보호위원회에 민간, 공공부문의 통합적인 감독권을 부여

1) 우리나라의 개인정보 보호 관련 감독 및 감독기관의 현황

가) 분야별로 개인정보 보호 관련 감독 및 감독기관이 존재함

우리나라의 개인정보 보호 관련 감독 및 감독기관은 각 분야별로 산재하여 존재한다. 따라서 분야별 감독기관은 독립성이 보장되지 못하거나, 독립성이 약화되어 있다.

공공부문에서 개인정보 보호 관련 감독 업무를 수행하거나, 수행할 수 있는 권한을 가지고 있는 기관으로는 국가인권위원회, 개인정보보호심의위원회(폐지)와 행정안전부, 국민고충처리위원회 등이 있다.

민간부문에서는 공정거래위원회, 개인정보분쟁조정위원회, 인터넷진흥원(구 한국정보보호진흥원), 방송통신위원회(과거에는 정보통신부와 통신위원회도 그 역할을 담당했었다), 금융감독위원회, 금융분쟁조정위원회, 전자거래분쟁조정위원회, 소비자원, 소비자분쟁조정위원회 등이 분쟁조정이나 감독 및 감독기관으로 역할하고 있다.

나) 국가인권위원회

국가인권위원회는 「국가인권위원회법」에 따라서 인권에 관한 법령(입법과정 중에 있는 법령안을 포함한다)·제도·정책·관행의 조사와 연구 및 그 개선이 필요한 사항에 관한 권고 또는 의견의 표명을 할 수 있고, 인권침해행위에 대한 조사와 구제를 할 수 있다. 그에 따라 공공기관의 행위로 인하여 개인정보 침해를 가져오는 경우 시정권고할 수 있고, 법령이나 제도, 정책, 관행에 대한 의견을 제시, 권고할 수 있다.

국가인권위원회는 인권과 관련한 부문에서 독립성을 유지하면서 의견을 제시해 오고 있으나, 개인정보 보호의 다양한 부문에서 적극적인 역할을 하는 것을 기대하기는 어렵다.

다) 방송통신위원회

방송통신위원회는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법')에 의하여 정보통신망에서 서비스를 제공하는 자와 정보통신망법이 준용되는 사업자에 대한 규제를 담당해 왔다.

방송통신위원회는 조사권, 시정조치권, 서비스 중단, 과태료부과권 등 강력한 권한을 가지고 있으며, 각종 개인정보 보호와 관련된 고시의 제정 등의 행정입법권을 가지고 있다. 또한 개인정보 누출 등의 통지제도에 따라서 개인정보 누출이 있을 경우 정보통신서비스제공자로부터 신고를 받고, 약관의 신고에 따른 변경 권고권, 본인확인기관의 지정, 정보보호 사전점검과 보호조치 권고, 집적정보통신시설 사업자에 대한 서비스 중단 요구, 안전진단 수행기관 지정, 정보보호 관리체계 인증기관 지정 등, 개인정보 보호 관리체계, 정보보호 관리등급의 부여, 정보통신망 침해사고 대응, 침해사고 신고 접수, 통신과금서비스제공자의 등록과 등록취소권, 과태료 부과권 등 매우 광범위한 권한을 부여받고 있다.

그런데 방송통신위원회는 그 동안 정보통신산업의 발전이라는 정책의 추진에 밀려서, 개인정보 보호에 대해서는 소극적이라는 비판을 받아 왔다. 방송통신위원회의 개인정보 보호 관련 예산도 2008년에 출범 당시 52억원에서 2011년에는 27억원으로 삭감하는 등 개인정보 보호에 관한 정책의 추진에 매우 미흡했다. 방송통신위원회가 출범한 2008년 이후 최근까지 개인정보 보호와 관련한 수많은 사건과 새로운 이슈들이 제기되었음에도 불구하고, 방송통신위원회는 매우 미온적인 대응을 해 왔다는 비판을 받고 있다. 애플이 아이폰 이용자들로

부터 10개월여 동안 동의 없이 무단으로 위치정보를 수집했음에도 300만원의 과징금 부과에 그치고, 구글의 와이파이 정보 무단수집에 대한 미온적으로 대응했으며, 페이스북의 개인정보 방침에 대해서도 시정 권고에 그쳤다. 특히 최근 구글의 개인정보의 통합에 대한 미온적으로 조치하고, 개인정보유출에 대한 미온적으로 조치한 데 대해서는 여러 비판이 제기되어 왔다[2].

라) 행정안전부와 각 부처

행정안전부나 그 밖의 각 부처도 산하기관에 대하여 시정조치를 할 수 있다. 그러나 각 부처로 나뉘어져 있을 때는 독립성이 약화되고, 전문성에도 문제가 있을 수 밖에 없다.

마) 금융위원회

금융위원회도 금융기관의 개인정보 보호 조치에 대한 조사나 시정조치, 고시의 제정 등을 할 수 있다. 그러나 금융위원회는 금융산업의 발전을 위한 진흥역할을 주되게 수행하는 기구로서 개인정보 보호에 대한 감독기능을 수행하는 데 태생적인 한계가 있다.

바) 공정거래위원회

공정거래위원회는 개인정보 약관에 대한 「약관 규제에 관한 법률」의 위반여부를 조사하고, 시정명령을 내릴 수 있다. 이에 따라서 공정거래위원회는 온라인사업자들의 개인정보 관련 이용약관의 불공정한 조항들에 대한 시정조치를 하기도 하였다. 공정거래위원회와 개인정보 보호위원회는 협력적 관계를 가지는 것이 바람직하다.

사) 개인정보분쟁조정위원회와 개인정보침해신고센터

권리구제 기관으로서는 개인정보분쟁조정위원회와 개인정보침해신고센터가

2) 2012년 3월 구글의 개인정보 통합관리 문제가 전세계적으로 논란을 빚고 있던 가운데, 방송통신위원회 권고가 각 2월과 4월에 발표되었으며 구글이 전세계 최초로 수용했다고 자화자찬하였다. 그러나 사실상 개인정보취급방침 수정 정도로 구글의 개인정보통합방침을 추인했을 뿐이라는 비판도 일었다("구글 개인정보통합미봉책… 방통위 나홀로 만족?", 한국일보, 2012.4.6 등 참조). 개인정보 보호위원회는 방통위의 결정과 다른 내용의 결정(6.11)을 내렸으나 방송통신위원회는 수용방침이 없다고 밝혔다("방통위가 면죄부 준 '구글'의 개인정보방침, 개인정보보호위 '정면비판'", 미디어스, 2012.6.11 등 참조). 이런 가운데 EU는 구글에 통합관리 정책을 4개월 내 수정할 것을 경고하여 파문이 일고 있다("EU, 구글 '개인정보 정책' 에 철퇴", 아이뉴스24 2012.10.17).

분쟁조정과 침해에 대한 신고를 받아 조사를 하는 기관으로 운영되고 있다. 그러나 분쟁조정과 침해가 분야별로 나뉘어 있고, 직권조사를 할 수 있는 기관과 분리되어 있으며, 시정조치를 할 수 있는 기관과도 분리되어 있어서 실효성이 크게 떨어진다.

2) 개인정보 보호위원회의 감독권한의 범위와 문제점

가) 현행 개인정보 보호법의 개인정보 보호위원회의 감독권한의 범위

앞서 살펴 보았듯이, 현행 개인정보 보호법의 개인정보 보호위원회의 감독권한은 공공부문에 대한 시정조치권만 있을 뿐, 민간부문에 대한 시정조치권과 감독권이 없다. 현재 민간부문에 대한 시정조치권이나 조사권은 행정안전부, 방송통신위원회, 각 부처, 금융위원회에 있다.

구글, 포털, 통신사, 금융기관 등 국내외 민간기관의 개인정보 침해행위가 문제되는 사안에 대하여 개인정보 보호위원회의 감독권한이 심각하게 제한되고 있는 것이다.

나) 현행 개인정보 보호법의 문제점

현행 개인정보 보호법은 각 감독기관의 역량을 분산시키고 효율성을 저해하고 있다는 점에서 큰 문제를 가지고 있다. 개인정보 보호에 관한 업무를 분야별로 여러 기관에서 나누어서 수행하는 경우, 역량 분산으로 효율성이 떨어질 뿐더러, 신속하게 변화, 발전해 나가는 해당 분야의 수요에 대한 적응력을 갖추기 어려울 수 밖에 없다. 개인정보 감독기관이 시의적절하게 적절한 대응을 하지 못하면 시장 감독에 실패할 가능성이 높다.

또한 각 개인정보 감독기관의 독립성이 약화되면서 감독보다는 진흥에 초점을 둘 가능성이 있다. 방송통신위원회나 금융위원회의 경우 방송통신산업이나 금융산업의 발전, 진흥에 초점을 맞춘 정책 추진이 우선될 가능성이 농후한 것이다. 실제로 그 동안 추진되어 온 정책은 산업발전이 우선하여, 개인정보 보호는 뒷전이었다는 비판이 제기되어 왔다.

국제적인 추세는 통합적인 감독기관을 두고 이 기구가 민간, 공공부문을 아우르는 감독권을 행사하도록 하는 것이다. 통합적인 개인정보보호 감독기관은 강력한 권한으로 독립성 또한 강화되어 있다. 이와 달리 분야별로 분산된 감독기관은 감독기관의 권한을 약화시키게 되며, 이는 독립성 약화와 직결된다.

3) 개선방안

가) 개인정보 보호위원회에 민간, 공공영역의 시정조치권과 감독권 부여

개인정보 보호위원회가 민간과 공공을 모두 아우르는 감독기관으로서 모든 분야에서 조사권과 시정조치권을 가져야 한다. 개인정보 보호위원회가 민간과 공공을 아우르는 개인정보 보호에 관한 감독기관으로 기능을 수행할 수 있도록 개인정보 보호법이 개정될 필요가 있다.

나) 현재의 분산된 개인정보 감독기능을 개인정보 보호위원회로 집중

현재 민간부문 개인정보 보호에 대한 감독권을 보유하고 있는 방송통신위원회, 금융위원회의 경우, 당해 기구가 해당 분야의 진흥업무를 동시에 담당함으로 인해서 개인정보 보호에 관한 감독기능을 독립적으로 수행하는 데 문제가 있으므로, 개인정보 보호에 관한 감독기능은 개인정보 보호위원회로 집중하는 것이 바람직하다. 정보통신사업자, 금융 및 신용정보사업자에 대한 개인정보 보호관련 감독기능을 개인정보 보호위원회가 수행할 수 있도록 정보통신망법 개정, 「신용정보의 이용 및 보호에 관한 법률」, 「금융실명거래 및 비밀보장에 관한 법률」 등도 개정될 필요가 있다.

라. 입법개선 과제 – 개인정보 보호위원회에 개인정보에 관한 통합적인 권리구제권한을 부여하여 권리침해 신고의 처리, 권리구제 및 분쟁조정 신청을 처리하게 함

1) 현재의 개인정보 권리구제 기능

가) 개인정보 권리구제 기능

공공부문의 경우는 개인정보 보호에 대한 감독권이 개인정보 보호위원회, 각 중앙행정기관, 국가인권위원회 등에 분산되어 있다. 민간부문의 경우는 개인정보 보호에 대한 감독권이 행정안전부, 각 중앙행정기관, 방송통신위원회, 금융위원회 등에 분산되어 있다. 더구나 민간부문의 경우 개인의 권리구제 신청권에 대한 절차적 권리보장 규정이 없어서 권리보장이 미흡하다.

나) 개인정보분쟁조정위원회

개인정보분쟁조정위원회는 개인정보 보호위원회와 별도로 행정안전부장관이 임명하는 위원으로 구성되는 조직이다. 조정신청된 사건의 조사를 위해서 분쟁조정위원회 사무국을 두고, 한국인터넷진흥원에서 업무를 보조하고 있다. 양 당사자가 조정안에 동의해야만 조정이 성립한다.

개인정보분쟁조정위원회의 조치는 행정각부 및 감독기관의 시정조치와 별개로서, 분쟁조정이 결렬될 경우 개인정보분쟁조정위원회는 아무런 조치도 취할 수 없다는 점이 한계로 지적된다.

다) 개인정보침해신고센터

개인정보침해신고센터는 위 기구들과 별도로 구성되어 있다. 개인정보침해신고센터 웹사이트 구축 운영도 별도로 이루어지는 등, 포괄적인 개인정보 침해 구제가 이루어지지 않고 있다.

2) 현재의 개인정보 권리구제 제도의 문제점

가) 개인정보 보호위원회의 권리구제 기능의 약화

개인정보 보호법 위반에 대한 개인정보보호 감독기관의 권리구제 기능은 신속한 권리보호를 가능하게 해 주는 효과적인 기능이다. 실제로 전 세계 각국의 통합적인 개인정보보호 감독기관들은 신속한 권리구제라는 옴부즈만 기구로서의 역할을 가장 중요한 역할의 하나로 수행하고 있다. 그런데 우리나라의 개인정보 보호법은 그와 같은 권리구제를 공공부문과 민간부문으로 나누고, 민간부문의 경우는 행정안전부, 각 중앙부처, 방송통신위원회 등으로 분산하여 처리하고 있다. 따라서 전문성도 약화되고, 신속, 정확한 업무처리를 기대하기 어렵다. 해당 분야가 공공부문인지, 민간부문인지 판단하기 어려운 영역도 많다.

나) 개인정보분쟁조정위원회도 분산되어 비효율적

한편, 현행 개인정보 보호법은 행정안전부장관이 임명하거나 위촉하는 20명 이내의 위원으로 구성되는 개인정보분쟁조정위원회를 별도로 구성하여, 이를 통해서 개인정보 분쟁조정을 하도록 하고 있는데, 이것 역시 역량을 분산시키는 바람직하지 못한 조직구성이다.

다) 원스탑 권리구제에 걸림돌

개인정보 보호위원회는 개인정보 침해와 관련한 포괄적인 권리구제기능을 수행할 수 있어야 한다. 개인정보 보호위원회에 개인정보 침해 신고를 하면, 시정조치와 개인정보분쟁조정이 원스탑으로 처리될 수 있어야 한다는 뜻이다.

그러나 현재는 개인정보 보호위원회와 개인정보분쟁조정위원회가 별도의 조직으로 존재함으로 인해 원스탑 처리가 불가능하다. 개인정보 보호위원회로서는 분쟁조정 기능이 없으므로 권리구제 기능이 약화된 상태이다. 피해자인 국민의 입장에서도 권리구제 기관의 분립은 권리구제를 효율적으로 받는 데 방해가 된다.

개인정보분쟁조정위원회로서도 현재는 개인정보보호 감독기관인 개인정보 보호위원회와 분리되어 전문성이 약화되어 있다. 개인정보침해신고센터 역할의 분립도 원스탑 서비스에 반한다.

3) 개선방안

개인정보 침해에 대한 신속하고, 전문적인 권리구제가 이루어지도록 하기 위해서는 모든 역량을 한 곳으로 집중시키는 것이 좋다. 개인정보 보호위원회는 공공부문과 민간부문의 구별 없이 개인정보 침해와 관련된 권리구제 기능을 수행하도록 하고, 개인정보분쟁조정위원회도 개인정보 보호위원회에 두는 것이 바람직하다.

아울러 개인정보 보호위원회는 권리구제 기능을 효율적으로 수행하기 위한 체계 정비를 할 필요가 있다. 사건의 접수, 사건의 조사, 결정의 공개 등에 대한 기준을 마련하고, 전문적인 조사역량도 강화해야 한다. 개인정보 보호위원회에서 통합 운영할 경우 전문인력의 공동 활용이 가능하고, 전문성을 축적할 수 있다는 장점이 있다.

마. 입법개선 과제 – 개인정보 보호위원회에 행정입법권을 부여하고, 개인정보 보호 기본계획 작성 의결권 부여하여 정책형성 기능을 강화함

1) 개인정보 보호위원회의 정책형성기능

개인정보 보호위원회가 가지고 있는 정책형성 기능은 개인정보 보호 기본계획과 시행계획의 의결기능을 들 수 있다. 또한 연차보고를 통한 평가기능을 가지고 있으며, 개인정보 보호에 관한 사안과 법률, 정책, 제도에 대한 의견제시권 또한 가지고 있다.

2) 국가와 지방자치단체의 개인정보 보호 정책의 추진을 위한 개인정보 보호 기본계획 및 시행계획의 의결과 연차보고를 통한 평가기능의 강화

가) 현재의 상황

국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 하는 의무를 가지고 있다(개인정보 보호법 제5조 제1항). 개인정보 보호법에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 하는 책무 또한 가지고 있다(동조 제2항). 국가와 지방자치단체는 이런 책무를 수행하기 위하여 개인정보 보호에 관한 다년계획인 3년 단위의 개인정보 보호 기본계획을 수립해서 집행하고 매년 기본계획에 따라서 시행계획을 수립해서 집행해야 한다.

개인정보 보호위원회는 이 과정에서 개인정보 보호 기본계획과 시행계획을 의결하고, 연차보고서를 작성하는 것을 통해서 개인정보 보호 시책의 방향설정과 계획의 확정, 평가 기능을 수행한다. 이를 통해 개인정보 보호위원회는 중앙행정기관의 개인정보 보호법에 따른 책무의 이행을 총괄적으로 구상하고, 의결하여 추진해 나가는 적극적인 역할을 담당하고 있다. 이와 같은 정책형성 기능은 시정조치 권고를 통한 위법한 상태의 시정기능(법 제64조 제4항)과는 달리 적극적인 정책형성 기능이다. 현재는 행정안전부가 개인정보 보호 기본계획을 작성하고, 개인정보 보호위원회가 이를 심의, 의결하도록 하고 있다.

한편 개인정보 보호위원회의 연차보고서는 계획에 대한 평가의 역할을 한다. 현재는 각부처에서 작성하는 자료를 바탕으로 연차보고서를 작성하고 있다.

나) 개선방안

행정안전부에서 개인정보 보호 기본계획을 작성하고, 개인정보 보호위원회가 심의, 의결하는 경우 심의 의결권이 사실상 제한될 수 밖에 없다. 적극적인 정책형성 기능을 고려한다면 개인정보 보호 기본계획을 개인정보 보호위원회에서 직접 작성하도록 법률을 개정하는 것이 바람직하다.

연차보고서도 각 부처에서 작성하는 것보다는 개인정보 보호위원회가 직접 작성하는 것으로 하는 것이 바람직하다.

3) 개인정보 보호에 관한 정책, 제도, 법률, 사안에 대한 의견제시권

가) 현재의 상황

개인정보 보호위원회는 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항, 그 밖의 개인정보 보호에 관한 사항에 대한 의견제시권을 가지고 있다. 안건의 상정은 대통령, 개인정보 보호위원회의 위원장 또는 위원 2명 이상이 제안할 수 있다.

개인정보 보호위원회의 의견제시권은 그 대상이 개인정보호와 관련된 것이면 제한이 없다. 현행 법령에 대한 의견, 개선할 사항에 대한 의견, 현재 입법과정에 있는 제안된 법률이나 행정입법에 대한 의견, 조례에 대한 의견은 물론이고, 제도에 대한 의견, 법령에 근거하지 않는 구체적 행위에 대한 의견제시도 가능하다.

의견제시의 방법은 직접 민간영역의 사업자나 개인에 대하여 의견을 제시할 수도 있을 것이고, 해당 민간영역의 사업자나 개인에 대한 시정조치권을 갖는 소관부처에 대한 의견제시의 방법을 통할 수도 있을 것이다. 의견제시는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회의 개인정보 보호법 위반에 관한 것일 경우에는 시정권고의 효력이 있고, 이때 해당 기관은 특별한 사유가 없으면 이를 존중하여야 할 것이다.

나) 개선방안

개인정보 보호와 관련된 법령의 제정이나 개정시 의무적으로 개인정보 보호위원회에 통지하고, 의견을 들어야 한다는 규정을 두는 것이 바람직하다. 현재는 이와 같은 의무규정이 없어서 각 부처나 국회에서 법령의 제정이나 개정시 개인정보 보호위원회에 사전 의견조회를 거의 하지 않는다.

4) 처리결과 공표에 대한 의결과 개인정보영향평가에 대한 의견제시권

가) 현재의 상황

현재 개인정보 보호위원회는 처리결과의 공표에 대한 의결을 할 권한과, 개인정보영향평가에 대하여 의견을 제시할 권한을 가지고 있다.

<표 Ⅳ-2> 개인정보 보호위원회 회의현황

년도	회의 차수	개최일자	안 건 명	회의결과
2011	1	12. 12.	개인정보 보호위원회 운영규칙 제정(안)	수정의결
2012	1	1. 9.	'12년도~'14년도 개인정보보호 기본계획	상정·심의
	2	1. 30.	'12년도~'14년도 개인정보보호 기본계획	수정의결
			개인정보 보호법 관련 법령해석 요청 건	원안의결
	3	2. 20.	전문위원회 구성방안	수정의결
	4	3. 6.	주민번호 수집·이용 최소화 종합대책	상정·심의
			'12년도~'13년도 개인정보보호 시행계획 심의방안	원안의결
			조사·분석 전문위원회 위원 인선(안)	원안의결
	5	3. 19.	주민번호 수집·이용 최소화 종합대책	심의계속
	6	4. 9.	주민번호 수집·이용 최소화 종합대책	수정의결
	7	4. 30.	법령정비위원회 구성에 관한 건	원안의결
			'12년도~'13년도 개인정보보호 시행계획	원안의결
	8	5. 14.	시·군 CCTV 영상정보 연계를 위한 심의	기각
	9	5. 29.	병무청 병역관련 개인정보 제공을 위한 심의	기각
	10	6. 11.	구글의 개인정보 취급방침 개선의견	원안의결
	11	6. 25.	한국장학재단 학자금대출 회수를 위한 개인정보 제공 관련 심의	상정·심의
	12	7. 9.	개인정보 유출통지 의무위반 개인정보처리자들에 대한 조치권고	상정·심의
	13	7. 23.	2012. 개인정보보호 연차보고서 심의요청 건	조건부의결
			개인정보 유출통지 의무위반 개인정보처리자들에 대한 조치권고	심의계속

* 출처: 2012년 국회 행정안전위원회 국정감사 진선미 의원 답변자료.

나) 개선방안

현재의 법률상으로는 개인정보영향평가와 관련하여 법률안이 제출되어 있는 경우에도 영향평가를 해야 할지, 시행령안이 제출되어 있는 경우에도 영향평가를 해야 할지가 명확하지 않다.

법률안이나 시행령안이 제출되어 있는 경우에도 영향평가를 해야 하는 것으로 법률의 규정을 명확히 하는 것이 바람직하다.

5) 행정입법권의 부여

가) 현재의 상황

현재 개인정보 보호와 관련한 고시, 지침 등 행정입법의 기능은 행정안전부, 재정경제부, 방송통신위원회, 금융위원회 등이 가지고 있다. 예를 들어 행정안전부 장관은 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있고, 각 중앙행정기관의 장은 표준 개인정보 보호지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다. 그리고 행정안전부장관은 개인정보 처리방침의 작성지침을 작성하여 준수를 권고할 수도 있다.

반면 개인정보 보호위원회는 직접 행정입법을 할 수 있는 기능은 가지고 있지 못하다. 다만, 조례나 법령에 대하여 의견제시를 통해서 간접적으로 권고를 할 수 있을 뿐이다.

나) 개선방안

외국의 경우는 대부분 행정입법의 권한들을 개인정보보호 감독기관이 가지고 있다. 해당 분야의 전문성, 신속한 대응의 필요성을 고려한다면 우리나라의 경우도 이러한 고시나 지침 등의 제정권을 개인정보 보호위원회에 부여하는 것이 바람직하다.

바. 입법개선 과제 – 개인정보 보호위원회의 인사, 예산상의 독립성을 보장하도록 개인정보 보호법의 개정

1) 개인정보 보호위원회의 구성

개인정보 보호위원회는 대통령 소속으로 ‘그 권한에 속하는 업무를 독립하여 수행한다’고 법률에서 그 독립성을 보장하고 있다(제7조 제1항). 독립성이 보장되려면 무엇보다도 개인정보 보호위원회의 예산과 인사의 독립성이 이루어져야 한다. 현재 개인정보 보호위원회는 위원장 1명, 상임위원 1명을 포함한 15명 이내의 위원으로 구성되는데, 개인정보 보호위원회 위원의 인사상 독립성 보장 규정은 없다.

현재 개인정보 보호위원회의 직원에 대한 인사권은 행정안전부장관에게 있다. 다만 「개인정보 보호위원회 소속공무원 임용권 위임에 관한 규정」에서, 행정안전부장관은 개인정보 보호위원회 소속 공무원 임용권 중 4급(과장급을 포함한다) 및 5급 공무원의 전보권, 6급 이하 공무원 임용권, 기능직 공무원 임용권을 개인정보 보호위원회 상임위원에게 위임하고 있다. 인사권을 개인정보 보호위원회 위원장에게 위임하지 않고, 공무원인 개인정보 보호위원회 상임위원에게 위임한 것은 적절하지 못하다. 이는 위원회를 위원장이 대표한다는 원칙에도 어긋나는 것이며, 위원회의 독립성을 해치는 것이다.

2) 문제점과 개선방안

가) 위원장의 상임화와 상임위원의 확대로 독립적, 전문적 업무수행

현재 상임위원은 1명에 불과하고, 위원장이 비상임이므로 독립적인 업무수행이 현저히 곤란하다. 위원장을 상임화하고, 상임위원을 확대하여 독립적, 전문적 업무수행을 뒷받침할 필요가 있다.

나) 위원의 신분보장 규정 마련

개인정보 보호위원회 위원의 신분보장 규정을 두고 있지 않다. 이것도 독립성 보장에 미흡한 부분이다.

예를 들어 국가인권위원회법은 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다는 규정을 두고 있고, 개인정보분쟁조정위원에 대해서도 이와 같은 규정 두고 있다. 개인정보 보호위원회 위원의 신분보장 규정을 입법화할 필요가 있다.

다) 타부처 파견 및 복귀가 아닌 개인정보 보호위원회 독자 인사권 보장

위원회에는 사무를 지원하기 위하여 사무국을 두는데, 현재 사무국장과 사무국 직원의 인사권을 위원장이 행사하지 못하여, 타부처로부터 파견을 받고 있다.

예를 들어 국가인권위원회는 “소속 직원 중 5급 이상 공무원 또는 고위공무원단에 속하는 일반직공무원은 위원장의 제청으로 대통령이 임명하며, 6급 이하 공무원은 위원장이 임명한다”고 하여 인사권을 법률상 보장하고 있고, 대통령실장, 감사원장, 방송통신위원회위원장, 국가과학기술위원회위원장, 원자력안전위원회위원장, 국무총리실장, 공정거래위원회위원장, 금융위원회위원장, 국민권익위원회위원장도 공무원임용령에 의하여 인사권을 갖는데, 개인정보 보호위원회는 인사권이 보장되어 있지 않다.

인사의 독립성은 개인정보 보호위원회의 직무의 독립성과도 관련이 있고, 전문성을 강화하기 위해서도 필요하다. 인사권이 있어야 장기간에 걸쳐서 전문인력이 양성될 수 있을 것이다.

현재 사무처 직원들이 파견부서로 복귀하는 경우 업무의 지속성, 전문성을 보장받기 어렵다. 입법적으로 사무처 직원에 대한 인사권을 개인정보 보호위원회 위원장이 행사하도록 법률로 규정할 필요가 있다.

라) 개인정보 보호위원회에 예산편성권 등 예산상의 독립성 보장

현재 개인정보 보호위원회는 독자적인 예산편성권도 보장되고 있지 않다.

예를 들어 국가인권위원회는 예산편성의 독립성이 법률상 보장되고 있고, 방송통신위원회도 법률상 예산편성의 독립성이 보장되고 있는데, 개인정보 보호위원회는 그렇지 못하다.

현재 개인정보 보호위원회의 예산 편성은 행정안전부장관이 하고 있다. 법령을 개정하여 예산편성권을 개인정보 보호위원회에 부여하는 것이 바람직하다.

V. 결론

국민들로 하여금 안심하고 전자정부에 접근하게 하기 위해서는 정보주체의 개인정보가 안전하게 처리된다는 신뢰를 갖게 하는 것이 중요하다. 그런 점에서 행정부문에서 전자적으로 활용되는 개인정보의 경우 그 처리를 최소화하는 원론적 접근이 하다.[1)]

정보주체로서는 자신의 정보를 누가, 어떤 목적으로 얼마만큼 처리·이용·전달하는지 파악하기가 곤란하고, 나아가 개인정보의 흐름을 자율적으로 통제한다는 것은 불가능할 수밖에 없는 실정이며, 또한 개인은 전자적으로 이루어지는 정보의 전달을 정부가 스스로 개인에게 일일이 문자나 통신을 통하여 어떠한 이유로 어느 기관에 전달하였다고 알려주지 않는 이상 알 수도 없기 때문이다.

또한 행정기관이 보유하고 있는 개인정보가 당초의 목적과 달리 이용될 경우 조사 당시의 기준이나 배경 등을 충분히 인식할 수 없는 상태에서 자칫 개인에 관한 잘못된 인식과 평가에 기초한 행정작용이 이루어질 수 있고, 이는 때에 따라서 인격적 가치의 훼손 등과 같은 막대한 피해를 초래할 수도 있다.[2)]

이러한 관점에서 볼 때 행정부문에서 개인정보 이용의 활성화로 행정의 효율성과 편의성, 국민의 편익증대를 도모하는 것도 중요하지만 그와 동시에 개인정보의 공동이용에 일정한 제한을 가함으로써 자기정보관리통제의 침해라는 부작용을 최소화할 수 있는 방안을 함께 강구할 필요가 있다.

특히 경찰 작용 과정에서 널리 이루어지고 있는 치안정보의 수집에 대하여 보다 구체적인 입법적 통제가 이루어질 필요가 있으며, 범죄수사 과정에서 관행적으로 제공되어 온 통신 정보나 DNA 정보 등에 대해서는 법원의 통제가 이루어질 필요가 있다.

또한 행정 작용 과정에서 널리 확산되어 온 행정정보 공동이용이 정보주체의

1) 이민영, “행정정보 공동이용의 추진 방향과 법적 과제”, 정보통신정책 제 18 권 5호 통권 389호 (2006-3-16).

2) 장진숙, “행정정보 공동이용과 정보인권 : 자기정보관리통제권을 중심으로”, 인권복지연구 제6호, 2010.

권리 실현 문제를 형식적으로 다루며 관련 기관에 의한 감독이 충분치 이루어지고 있지 못한 현실은 매우 유감이다. 많은 국민의 사생활과 관련이 있는 CCTV 또한 그 설치와 운영에 있어서 오남용이 없도록 보다 구체적인 입법적 통제가 이루어질 필요가 있다.

한편 개인정보 보호법이 오랜 열망 끝에 제정되어 2011년 9월 30일부터 시행됨에 따라 이 법이 많은 역할을 할 것으로 기대받아 왔다. 그러나 개인정보 보호법의 규율은 아직 미약하여 국민들에게 체감되지 못하고 있으며, 그 이유 중 하나가 바로 개인정보 보호위원회의 규정에 많은 제약이 있다. 국민의 개인정보 자기결정권이 온전히 실현되기 위해서는 개인정보 보호법의 입법과제들이 하루빨리 실현될 필요가 있다.