

워크숍 2007 -

입법평가 자료 07-05

# 개인정보보호법제와 CCTV관련 규정 및 문제점, 개선방안

2007. 11. 16.

## 워크숍 일정

- ◆ 주 최 : 한국법제연구원 입법평가연구 TF팀
- ◆ 일 시 : 2007년 11월 16일(금요일) 13:50 ~ 18:00
- ◆ 장 소 : 노보텔 앰배서더 강남 / 보르도AB(지하1층)

### ◆ 구 성

◇ 사 회 : 이광윤 교수(성균관대 법학과)

◇ 주 제 발표

제 1 회의 13:50 ~ 14:40

**【주제】** 우리나라 개인정보보호 법제와 CCTV 관련 규정의 현황·  
문제점 검토 및 평가

발표자: 이민영 교수(가톨릭대학교)

토론자: 권현영 박사(한국정보사회진흥원)

제 2 회의 14:40 ~ 15:30

**【주제】** 미국 개인정보보호법제의 특징과 입법정책적 시사점

발표자: 이창범 박사(한국정보보호진흥원)

토론자: 정찬모 교수(인하대학교)

Coffee Break 15:30 ~ 15:50

제 3 회의 15:50 ~ 16:40

**【주제】** 독일의 개인정보보호법제 및 CCTV 관련법의 문제점과  
개선방안

발표자: 문병효 교수(한경대학교)

토론자: 강문수 박사(한국법제연구원)

제 4 회의 16:40 ~ 17:30

**【주제】** 일본의 개인정보보호법과 CCTV 관련 입법의 동향

발표자: 권건보 교수(명지대학교)

토론자: 채승완 박사(한국정보보호진흥원)

종합토론 및 만찬 18:00 ~

## 목 차

■ 제 1 주제 : 우리나라 개인정보보호 법제와 CCTV 관련규정의 현황·문제점 검토 및 평가(이민영)	
I. 논의를 시작하며 .....	11
II. 실정법체계 분석 .....	14
1. 현행법 관련 .....	14
2. 기본법 관련 .....	18
3. 문제점 검토 .....	27
III. CCTV 규정 진단 .....	38
1. 총괄적 논의 .....	38
2. 개별적 논의 .....	41
IV. 결론에 갈음하여 .....	47
◎ 토 론 문(권헌영) .....	51
■ 제 2 주제 : 미국 개인정보보호법제의 특징과 입법정책적 시사점(이창범)	
1. 개 요 .....	57
2. 개인정보보호법제의 발전 .....	58
가. 헌법과 판례 .....	58
나. 연방 및 주 제정법 .....	60

다. 세이프하버 원칙 .....	62
3. 연방 주요 제정법의 내용 .....	64
가. 프라이버시법 .....	64
나. 금융프라이버시보호 .....	65
다. 통신프라이버시보호 .....	67
라. 교육프라이버시보호 .....	68
마. 아동프라이버시보호 .....	69
바. 비디오대여정보보호 .....	70
사. 영상프라이버시보호 .....	71
4. 연방 개인정보보호기구 .....	72
가. FTC의 설립 및 구성 .....	73
나. FTC의 개인정보보호 활동 .....	74
5. 개인정보 피해구제제도 .....	76
가. 민간분쟁해결제도 .....	77
나. FTC의 개인정보피해구제 절차 및 방법 .....	82
6. 맺음말 : 입법정책점 시사점 .....	86
◎ 토 론 문(정찬모) .....	91
▣ 제3주제: 독일의 개인정보보호법제 및 CCTV관련법의 문제점과 개선방안(문병효)	
I. 서 론 .....	97
II. 독일의 개인정보보호법제 검토 .....	98

1. 헌법적 토대 .....	98
2. 독일연방정보보호법(BDSG) .....	99
3. EU 정보보호지침(EU-DSRL) .....	101
<b>III. 독일개인정보보호법상 CCTV관련규정과 그 내용</b> .....	102
1. 연방정보보호법 제6b조의 신설 .....	102
2. 규정의 목적 .....	103
3. 규정의 연혁 .....	103
4. 다른 규정과의 관계 .....	103
5. 비디오 감시(제1항) .....	104
6. 인식요건 (Kenntlichmachung der Beobachtung) .....	108
7. 정보의 처리 및 이용 .....	108
8. 고지의무(Benachrichtigung) 및 삭제의무(Loesung) .....	110
9. 기 타 .....	111
<b>IV. 문제점 및 개선방안</b> .....	112
1. 개인정보보호에 관한 통합법의 필요성 .....	112
2. 감시목적의 제한 .....	112
3. 엄격한 목적구속 .....	112
4. 고지 및 삭제의무 .....	113
5. 사전통제의 필요성 .....	113
6. 보호가치가 높은 정보에 대한 특별보호 .....	113
7. 관련기관의 책임강화 .....	113
8. 비디오감시시설에 대한 상시감독 및 작동시스템보고 .....	114
9. 정보보호감독관 및 정보보호위원회 등 설치 .....	114
10. 입증책임의 전환 .....	114

11. 정보의 자기결정권보호를 위한 절차법적, 실체법적 구제 ...	115
V. 결 론 .....	115
◎ 토 론 문(강문수) .....	117
▣ 제 4 주 제 : 일본의 개인정보보호법과 CCTV 관련 입법 의 동향(권건보)	
I. 서 설 .....	123
II. 일본 개인정보보호법의 입법 동향 .....	125
1. 통합 개인정보보호법의 제정 이전 .....	125
2. 통합 개인정보보호법의 제정과정 .....	128
III. 개인정보보호법의 체계와 주요 내용 .....	130
1. 전반적인 법의 체계 .....	130
2. 개인정보보호법의 주요 내용 .....	131
3. 행정기관개인정보보호법의 주요 내용 .....	140
4. 개인정보보호에 관한 조례 .....	152
IV. 일본의 CCTV 관련 입법의 동향 .....	155
1. 문제의 상황 .....	155
2. 일본의 감시카메라 관련 입법 동향 .....	156
3. 스기나미 區의 「방법카메라 이용설치기준」 .....	158
◎ 토 론 문(채승완) .....	161

# 제 1 주제

## 우리나라 개인정보보호 법제와 CCTV 관련규정의 현황·문제점 검토 및 평가

발 표 : 이민영 교수(가톨릭대학교 법학부)

토 론 : 권헌영 박사(한국정보사회진흥원)

## 우리나라 개인정보보호 법제와 CCTV 관련규정의 현황·문제점 검토 및 평가

이 민 영  
(가톨릭대학교 법학부 교수)

### I. 논의를 시작하며

흔히들 행정법(行政法)을 헌법(憲法)의 구체화법(具體化法)이라 한다.<sup>1)</sup> 현행 「전자정부법」은 「행정절차법」 소정 행정과정에 대한 절차적 통제에 있어서 전자행정 또는 정보기술과의 연관을 체계화하여 분화한 것으로 볼 수 있고 이에 따라 개인정보보호와 관련해서는 「공공기관의 개인정보보호에 관한 법률」이 제정된 것이라 하겠다. 물론 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 위시하여 민간분야에 적용되는 개인정보보호 관련사항 역시 그 규율의 방식이나 태도에 있어 주무부처나 소관기관의 행정통제(Verwaltungskontrolle)<sup>2)</sup>를 예

1) Vgl. F. Werner, *Verwaltungsrecht als konkretisiertes Verfassungsrecht*, DVBl, Dettendorf: Schmidt Periodicals GmbH, 1959, S.527.

2) 개인정보는 정보주체에 대한 권리보장의 객체가 되는 까닭에 국가전자행정에 관한 규범적 영역이라는 점에서, 행정기관이나 행정담당자가 행정행위를 함에 있어서 지켜야 할 의무인 행정책임(행정책임)을 구현하기 위하여 가해지는 행정권한의 내부적 제어와 외부적 제한을 뜻하는 행정통제가 요청된다. 행정통제의 목적은 행정책임의 이행을 보장하는 데 있으며 행정책임은 행정통제의 확보대상이 되는 것이다(Wolfgang Hoffmann-Riem, *Verwaltungskontrolle; Perspektiven*, in: Eberhard Schmidt-Aßmann & Wolfgang Hoffmann-Riem (Hrsg.), *Verwaltungskontrolle*, Baden-Baden: Nomos Verlag, 2001, S.339f.). 이는 행정책임을 통해 독단적 행정과정을 제한하고, 헌법과 행정법을 실천적으로 해석·적용하며, 행정의 법률적합성에 대한 혼란을 제거할 수 있기 때문이다(Lisa Schultz Bressman, *Beyond Accountability: Arbitrariness and Legitimacy in the Administrative State*, 78 N.Y.U.L. Rev. 461, 2003, p.553).

정하고 있으므로, 법체계 전반의 통일성·일관성 보유가 요청됨은 두 말할 나위 없는 것으로 여겨지기 마련이다.

這間 필자는 개인정보보호법은 중국적으로 정보사회의 균형적 발전에 이바지함을 그 목적으로 하는 개인정보보호에 관한 일반법으로서 보편적인 개인정보 개념을 원용하여야 할 것이고, 다만 사생활 침해의 우려가 큰 개인정보를 민감정보로 규정하고 사상·신념에 관한 정보, 개인의 신체적 특성을 넘어서 가계의 특징을 추출할 수 있는 유전자정보, 개인을 고유하게 식별하기 위하여 부여된 식별자로서 주민등록번호 등을 그 예시로 열거하는 것이 타당할 것이며, 개인정보의 취급에 있어 정보주체가 표명하는 의사표시인 동의에 대하여도 대통령령에서 그 절차와 방식을 규정하도록 위임함으로써 매체별로 구체화된 동의획득방식을 개인정보취급자가 예견할 수 있도록 하여 개인정보의 합리적 이용 및 보호의 균형을 도모하는 방안을 고려해 볼만할 뿐만 아니라, 개인정보보호의 규율대상으로서 공공부문과 민간부문이 적용법리에 있어 상호 구별됨을 반영하기 위하여 공공기관의 개념을 재정립할 것이 요구된다는 관점에서 관련 법규범이 정립되어야 한다는 견해를 피력해 왔다. 이러한 논의는 개인정보라는 보호객체가 법규범뿐 아니라 법현실적으로 인간으로서의 존엄성에 상응하게 처리되어야 할 것임을 확인하면서도, 국가사무나 거래실무에 있어서 활용가치가 상존함을 인식하고 이에 대응해야 할 것이라는 점을 인식한 데 기인한다.

특히 개인정보보호의 규율대상으로서 공공부문과 민간부문이 적용법리에 있어 상호 구별됨을 반영해야 하는 것은 정보자기결정권의 효력이 미치는 범주에 따라 개인정보의 활용이 허용되느냐 아니면 규제되느냐가 달라지기 때문에 귀납적으로 공적 영역과 사적 영역에서의 개인정보보호를 위한 규제법리가 구별되는 논거에 견주어 이론

적 탐색을 완결한 후에야 실질적 정비를 피할 수 있음은 주의를 요한다 할 것이다. 그럼에도 불구하고 개인정보와 관련된 논의는 그 용례에 있어 부정확한 것이지만 그 보호에 기울거나 그 활용에 경도되는 이분법적 검토에 치우쳐왔음이 사실이다. 그리고 보면, 오늘날 우리 사회가 안고 있는 갈등과 분쟁이 다분히 이 분야에 그대로 이식되거나 답습되고 있는 형국임을 부인하기는 어려울 것이라 생각한다. 그 까닭에, 다른 분야와 마찬가지로 개인정보의 합리적 보호와 효율적 이용을 균형 있게 실행해나가려는 관점은 허울 좋은 기계적 절충에 지나지 않다는 비난에서 자유롭지 못할 수 있다. 그리고 그에 대한 반박은 고양된 권리의식에 반감을 가중시키거나 위법한 권리침해에 논거를 안겨줄 수 있는 위험성 역시 상존하고 있다는 점을 배제하기 어려운 실정이다.

결국 국가사무로서 개인정보의 활용이 실질적 법률유보에 따라 이루어져야 할 것임은 자명한 것이나, 개별법에서 그 활용이 규율하는 경우에도 그 위헌성 소지를 배제할 수 있는 헌법이념적 논거를 찾아 내기란 보호되는 가치로서 개인정보에 관한 권리의 존재를 인식한다면 이는 그렇게 쉬운 문제는 아니라 할 것이다. 이러한 점에서, 개인정보보호에 관한 기본적 규율사항을 규정한 입법적 대응(이하에서는 법안 자체의 명칭을 고려하지 않고 단순히 ‘기본법’이라 칭하기로 함)이 여전히 국회에 계류 중인 것은 국가책임에 있어 결단코 간과되어서는 아니 될 방임적 부작위가 존재하는 것으로 판단된다.

이러한 관점에서 개인정보의 보호에 관하여 규정하고 있는 실정법의 규율내용을 정보주체의 권익 보장 측면에서 현황적 재검토를 통하여 그 문제점을 살펴보고, 이에 관한 보완적 논의로서 폐쇄회로 텔레비전(이하 ‘CCTV’라고 함)과 관련된 몇 가지 법적 쟁점들을 살펴보기로 한다.

## II. 실정법체계 분석

### 1. 현행법 관련

#### 가. 일반적 입법현황

컴퓨터로 처리되는 개인정보의 보호에 관하여 우리 법제는 공공부문과 민간부문으로 양분되어 있어, 공적 영역의 『공공기관의 개인정보 보호에 관한 법률(이하 ‘개인정보법’이라 함)』과 사적 영역의 『정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 ‘정보보호법’이라 함)』이 존재한다.

<표 2-1> 개인정보보호 관련 현행법제

구 분	관련법규	규제내용
정부 기록 정보	공공기관의개인정보보호에관한법률	○처리과정상의 정보주체 및 공공기관의 권리의무 규율
	공공기관의정보공개에관한법률	○개인정보의 비공개, 부분공개
	주민등록법	○주민등록 열람 또는 등·초본 교부, 전산정보자료 이용 등
	자동차관리법	○자동차 관리 업무의 전산처리시 사생활 보호
	통계법	○통계작성 과정시 개인 및 단체 법인의 비밀보호
	국정감사및조사에관한법률	○사생활 침해목적의 감사, 조사 제한
	국가공무원법, 특검규제및공정거래에관한법률	○업무상 지득한 비밀의 보호
통신 비밀	통신비밀보호법	○우편물의 검열, 전기통신의 감청 등 통신관련 사생활 보호
	통신제한조치의허가절차및비밀유지에관한규칙	○범죄수사·국가안보를 위한 통신제한조치의 허가절차
	전기통신사업법	○개별이용자에 관한 정보의 공개 및 유용금지 등
	형법 제316조상의 비밀침해죄	○병합 및 전자기록 등 특수매체기록에 대한 기술적 침해
보건 의료 정보	보건의료기본법	○보건의료 관련 사생활의 보호
	의료법, 전염병예방법, 후천성면역결핍증예방법	○업무상 비밀 누설 금지
	생명윤리및안전에관한법률	○유전자정보의 보호 등
소비자 정보	정보통신망이용촉진및정보보호등에관한법률	○정보통신서비스제공자 등에 의한 개인정보 취급 규제
	신용정보의이용및보호에관한법률	○민간부문에 의한 개인신용정보 처리의 규제 ○신용정보주체의 열람 및 정정 청구 등

제 1 주제 우리나라 개인정보보호 법제와 CCTV 관련규정의 현황 · 문제점 검토 및 평가

	금융실명거래및비밀보장에관한법률	○금융거래의 비밀보장
	증권거래법	○정보의 제공, 누설 금지
	위치정보의이용및보호등에관한법률	○위치정보의 수집·제공의 범위, 오·남용 방지
	은행법, 변호사법, 공증인법 등	○업무상 지득한 비밀의 보호

그리고 일반 선언규정을 포함하여 개별분야에 적용되는 업무상 비밀보호 및 정보보호를 규정하고 있는 개별법이 체계성 없이 산재되어 있는 실정이다.<sup>3)</sup> 보호법규에서 전자정부의 이념과 개인정보보호의 가치의 균형점 모색이 필요함에도 불구하고, 부문별로 개인정보보호에 관한 일반법이 사실상 존재하면서도 기능상 법현실에서의 규범력은 굴절되어 있다. 개인정보처리의 위험성이 높고 그만큼 보호의 필요성이 큰 분야에 보다 엄격한 보호체계가 마련되어야 함에도 현행법제는 그러한 체계성이 부족하다는 지적에서 자유로울 수 없는 것이다.

또한 개인정보처리의 위험성의 정도는 공공부문과 민간부문에서 각각 다르며 민간부문 내에서도 처리하는 개인정보의 종류와 성격에 따라 다르게 마련이므로, 보호체계에 대한 종합적인 검토와 보호가치의 재조정을 통한 개인정보 관련법제의 체계적 재정립이 요구된다. 아울러 현행 미온적인 보호체계로는 정보주체의 정보자기결정권을 확립하면서 전자정부시대에 걸맞은 개인정보보호 수준의 수립이 어려울 것으로 전망되고 당해 권익구제기능을 위한 보호기구의 설치 또한 그 독립성을 고려하여야 하며, 프라이버시영향평가제도의 도입 역시 규제 수요에 상응하도록 제도적으로 완비되어야 할 것이다. 이러한 논의로써 법규의 형식적 체계성과 내용적 정당성이 갖추어질 수 있다. 이하에서는 공공부문의 일반법인 개인정보법과 실제로 민간부문의 일반법

3) 그 예로 『정보화촉진기본법』, 『정보통신기반보호법』, 『전자거래기본법』, 『전자서명법』, 『통신비밀보호법』, 『전자상거래 등에서의 소비자보호에 관한 법률』, 『신용정보의 이용 및 보호에 관한 법률』, 『예금자보호법』, 『금융실명거래 및 비밀보장에 관한 법률』, 『주민등록법』, 『호적법』, 『도로교통법』, 『국세기본법』, 『의료법』, 『보건의료기본법』, 『응급의료에 관한 법률』, 『사회보장기본법』 등을 들 수 있다.

으로 기능하고 있는 정보보호법을 중심으로 우리나라의 법제현황을 살펴보기로 한다.

## 나. 부문별 입법현황

### (1) 개인정보법

사적 관계에서 이루어지는 개인정보의 수집과 보관 활용 등은 우선 계약자유의 원칙과 자기책임의 원칙에 의거하여 이루어지는 것으로서 당사자 평등이라는 전제하에서 관계가 형성되므로, 이 과정에서 발생한 문제의 해결을 위하여 제3자의 개입이 처음부터 요구되는 것은 아니다. 물론 정보화가 급속히 진전되는 현대사회에서 개인정보를 수집 및 활용하는 고도화된 기술 및 전략을 가지고 있는 거대기업과 일개 개인으로서의 정보주체를 완전히 당사자 평등이라는 전제하에 놓는 것은 무리가 있지만 원칙을 전제로 할 때 그러하다. 반면에 국가기관이 권력 작용의 일환으로 시행하는 국민의 개인정보 수집행위는 강제성을 띠면서 국가라는 강력한 권력을 지닌 존재와 개인의 불평등한 관계라는 전제하에서 이루어지게 된다. 이러한 불균형을 해소하기 위해 헌법과 법률은 국민에게 각종권리를 보장하고 있지만 그럼에도 불구하고 여전히 국민 개인은 국가가 원하는 개인정보를 언제든지 제공할 수 없는 상황이 형성된다. 이러한 개인정보 취급과 관련된 특성을 고려해 볼 때 공공부문의 개인정보보호에 관한 일반법적 성격을 갖는 개인정보법의 의의는 매우 크다고 볼 수 있다.

개인정보법은 행정전산화에 따른 개인의 사생활보호라는 사회적 요구에 부응하기 위해 1988년부터 입법을 추진하기 시작하여 1995년 1월 8일부터 시행하게 되었다. 이 법은 5개의 장, 25개조, 부칙으로 구성되어 있으며, 공공기관의 컴퓨터에 의하여 처리되는 개인정보를 보호하기 위하여, 각 행정기관이 개인정보처리시스템 내지 개인정보파일을 보유하고자 하는 경우에 그 보유범위 및 내부적 절차를 규율하고,

개인정보파일에 개인별로 수록된 개인정보인 이른바 처리정보를 이용하거나 제3자에게 제공하는 것에 대해 일정한 실체적 및 절차적 제한을 가하며, 정보주체에게는 열람 및 정정청구권을 인정하는 것을 주된 내용으로 하고 있다. 그러나 정부가 행정개혁의 일환으로 추진하고 있는 전자정부사업은 행정정보의 공동이용을 핵심으로 하고 있고, 공동이용 대상 행정정보 중 대부분이 개인정보에 해당된다. 따라서 전자정부사업의 성공은 국민들이 안전하고 신뢰할 수 있도록 제도적·기술적 개인정보보호대책 마련과 불가분의 관계라고 할 수 있다.

## (2) 정보보호법

현행 정보보호법은 정보통신부의 주도 아래 1999년 2월 8일 기존의 「전산망보급확장과 이용촉진에 관한 법률」을 전면개정하여 정보통신망에서의 개인정보보호규정을 새로이 신설했던 「정보통신망 이용촉진 등에 관한 법률」을 2001년 1월 16일 시행 1년만에 다시 전면개정한 것이다. 「정보통신망 이용촉진 등에 관한 법률」은 1990년대 후반 우리나라에서 인터넷 이용이 급속도로 활성화되면서 이용자들의 개인정보 보호에 대한 우려와 이제 막 태동하기 시작한 전자상거래의 활성화를 저해할 것이라는 고려가 작용하고, 또 이미 1995년과 1997년의 유럽연합의 개인정보보호지침에 자극을 받아 제정되었다고 할 수 있다. 당시 인터넷사업자에 의한 개인정보의 수집·이용·처리실태 및 시장에 미치는 과급효과 등에 대한 충분한 조사나 검토 없이, 온라인에서 이루어질 수 있는 모든 개인정보의 수집과 이용을 규율하는 매우 광범위하고 보기에 따라서는 강경한 입법조치였다. 그리하여 그동안 시행 결과 드러난 문제점들을 개선·보완하기 위하여 다시 전면개정의 형식으로 현행 정보보호법을 제정하게 되었는바, 규율대상인 정보통신서비스제공자뿐만 아니라 준용규정에 따라 일부 일반사업자에게도 개인정보보호사항을 강제하고 있다.

## 2. 기본법 관련

### 가. 논의의 전제

지난 2003년 대통령 주재로 열린 국정과제회의에서 정부혁신지방분권위원회가 마련한 전자정부관련법제정비방안에는 “2004년까지 시민사회 의견을 수렴하여 개인정보보호 기본원칙을 천명하고 개인정보영향평가제를 도입하며 개인정보보호기구를 설치하는 것 등을 내용으로 하는 개인정보보호기본법의 제정에 대하여 검토하겠다”는 내용이 담겨 있다.<sup>4)</sup> 이 같은 사항은 사회각계여론이 집합되는 논의과정에서 정책방안이 집결됨으로써 종국적으로 국정과제로 채택되기에 이른 것으로 여겨진다. 교육행정정보시스템(NEIS)의 도입에 있어 제기된 문제점 및 그에 따른 대응방안이 제시될 때에도 결국 총괄적으로 개인정보보호정책을 집행할 행정기구의 설치가 관건이 될 수밖에 없었던 예에서도 볼 수 있듯이, 보호가치 있는 정보주체의 권익보장을 제도화하는데 중추적인 역할을 담당할 존재에 대한 갈망은 사회전반적인 인식의 근저에 녹아들어 있었다.

특히 이에 대하여는 시민사회단체의 노력이 간과되어서는 아니 될 중요한 견인차로 작용해왔음을 지적하지 않을 수 없다. 예컨대 지난 2004년 7월 프라이버시법제정을위한연석회의를 주축으로 하는 시민사회단체가 17대 국회가 주목하여야 할 ‘정보인권 보장을 위한 35대 과제’를 발표한 바 있다. 여기서 공공과 민간 그리고 온라인과 오프라인에 예외 없이 적용될 수 있는 국제적 수준의 개인정보보호기본

---

4) 다만, 2003년에는 개인정보법과 정보보호법을 개정하여, 정보자기결정권을 강화하고 적용범위를 확대할 것이라는 점이 적시되어 있다; 대통령비서실, 청와대 브리핑 제148호, 2003년 10월 2일자, 2~4쪽.

법을 제정하고, 이에 따른 조치를 실질적으로 집행하기 위해 상시적인 사전 감독활동과 신속한 분쟁조정 활동을 일상적으로 수행할 수 있는 독립적인 개인정보보호위원회를 설치해야 한다는 주장이 재차 강조되었다. 그리고 이들은 개인정보보호위원회가 국가인권위원회의 위상에 준하는 독립적인 국가기구의 지위를 가져야 하고, 공공기관과 민간영역을 가리지 않고 사회 전체를 자신의 감독 및 분쟁조정 대상으로 삼아야 하며, 각종 법률제정에 있어 프라이버시보호에 관련된 권고권을 가져야 한다고 주장했다. 이어서 10월에는 프라이버시법제정을위한연석회의가 “개인정보보호위원회는 개인정보 현황에 대한 실태조사, 개인정보침해의 구제, 분쟁의 해결, 개인정보보호 관련 법령의 입안, 개인정보보호 교육 및 홍보, 개인정보를 침해할 수 있는 사업에 대한 사전영향평가 등의 업무를 담당함으로써 사회적 안전망의 역할을 해야 할 것이다. 개인정보보호위원회는 민간영역과 공공영역 모두를 포괄해야하며, 정부의 개인정보 수집 역시 감독해야 하기 때문에 정부로부터의 일정한 독립성이 보장되어야 한다.…”(中略)…신뢰성 있는 정보사회를 구축하기 위해서는 개인정보보호를 위한 사회적 시스템의 마련은 더 이상 늦출 수 없는 과제이다. 이번 정기국회에서 개인정보보호기본법 제정과 민간·공공 영역을 포괄하는 독립적인 개인정보보호위원회의 설립이 반드시 통과되기를 촉구한다!”는 내용의 논평<sup>5)</sup>을 발표하여 기존의 입장을 재확인한 바 있다. 하지만 개인정보보호기구 설립의 정당성이 그 설치방안의 타당성과 무관하지 않으며 이는 개인정보보호에 관한 정책 및 제도에 관한 사항이라는 점에서 입법논리적 검토와 함께 입법정책적 고려가 선행되어야 한다.<sup>6)</sup>

5) <http://networker.jinbo.net/maybbs/view.php?db=ektjtqud&code=policy&n=1085>

6) 개인정보보호기구의 창설에 관한 조직법적·작용법적 논의에 관한 詳細는 拙著, 개인정보법제론, jinhan M&B, 2007, 159~217쪽 참조.

## 나. 법안의 내용

### (1) 노회찬안

정보통신기술 등의 발달로 인하여 그것을 이용한 개인정보의 이동과 유통이 활발해지면서, 개인정보의 수집과 보관 및 활용에 따른 개인정보의 유출, 남용 및 개인정보를 이용한 불법행위들이 늘어나고 있으며, 이로 인하여 사생활이 침해되는 사례가 빈번하게 발생하여 사회문제가 되고 있는 현실이다. 따라서 개인정보보호에 관한 기본원칙을 정하고, 정보주체의 자기정보통제권을 강화하여 권리구제의 방법을 현실화하는 한편, 공공부문과 민간부문의 개인정보보호를 포괄하여 담당하는 독립기구를 설치하는 동시에, 개인정보와 밀접한 관계를 가지는 기술이나 설비의 도입을 효과적으로 관리함으로써 개인 사생활을 보호하려는 목적에서 개인정보보호기본법안을 제안하게 되었다. 그 주요 내용은 다음과 같다.

첫째, 타인의 개인정보를 수집하는 자는 당해 정보주체에게 개인정보의 수집목적 및 이용목적, 보존기간 등을 고지하고, 정보주체의 동의를 얻어야 하도록 하고 있다(안 제5조 제1항 및 제2항).

둘째, 누구든지 사상·신념·과거의 병력 등 개인의 권리·이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 되도록 하고 있으며(안 제6조), 개인정보의 수집목적 또는 제공받은 목적을 달성한 때에는 당해 개인정보를 지체 없이 파기하여야 하도록 하고 있다(안 제8조).

셋째, 개인정보는 수집한 최근의 것으로 갱신해야 하며, 이를 이용하기 전에 그 오류 여부를 확인해야 하도록 하고 있다(안 제9조).

넷째, 정보주체는 개인정보 보유자에 대하여 자신의 개인정보에 대하여 정보주체의 개인정보를 수집한 경위 및 현황 그리고 제3자 제공

내역 등에 관한 사항에 대하여 자료를 요구할 수 있고, 자신의 개인정보에 오류가 있는 경우에는 그 정정을 요구할 수 있으며(안 제11조), 개인정보를 취급하거나 취급하였던 자는 그 개인정보를 취급하는 과정에서 알게 된 개인정보를 누설하여서는 아니 되도록 하고 있다(안 제14조).

다섯째, 만 14세 미만의 아동으로부터 개인정보를 수집하거나 이용 또는 제3자에게 제공하고자 하는 자는 그 법정대리인의 동의를 얻어야 하며(안 제17조), 개인정보 보유자가 영업의 전부 또는 일부를 양도하거나 합병·상속 등으로 그 권리·의무를 이전하는 경우 정보주체에게 영업의 전부 또는 일부의 양도, 합병 또는 상속 등의 사실을 통지하도록 하고 있다(안 제18조).

여섯째, 개인정보 데이터베이스를 보유하고자 하는 자가 공공기관의 개인정보 데이터베이스에 해당하는 경우에는 사전에 개인정보보호위원회에 등록하여야 하며(안 제20조제1항 제1호), 대량의 개인정보나 민감한 개인정보를 처리하려는 개인정보 보유자는 개인정보 데이터베이스가 새로 구축되는 경우 기존 데이터베이스에 새로운 개인정보를 추가함으로써 정보주체에 관한 새로운 정보를 생성할 수 있게 되는 경우 등에 위원회에 개인정보 사전영향평가를 신청하여야 한다(안 제95조).

일곱째, 개인정보보호위원회가 필요하다고 인정한 경우, 정보주체의 동의가 있는 경우 등을 제외하고는 자기가 수집·보관하는 개인정보 데이터베이스를 공공기관이 처리하는 개인정보 데이터베이스와 결합할 수 없도록 하고 있다(안 제23조 제1호 및 제2호).

여덟째, 개인정보의 침해를 이유로 한 손해배상청구의 경우 공통의 이해관계를 가지는 피해자들을 위하여 피해자 중의 1인 또는 수인이 법원의 허가를 받아 대표당사자가 되어 손해배상청구소송을 제기할 수 있도록 하고 있다(안 제29조).

아홉째, 이 법 및 개인정보보호에 관한 다른 법률의 준수여부를 감독하기 위하여 개인정보보호위원회를 설치하도록 하고 있다(안 제60조).

열째, 개인정보보호위원회는 개인정보침해행위가 계속 중에 있다는 상당한 개연성이 있고, 이를 방지할 경우 회복하기 어려운 피해발생의 우려가 있다고 인정할 때에는 그 진정에 대한 결정 이전에 피진정인, 그 소속기관 등의 장에게 개인정보의 수집, 이용의 중단, 기타 필요한 조치를 하도록 권고할 수 있도록 하고 있다(안 제93조).

## (2) 이은영안

이 법안은 정보화가 급속히 진행되는 과정에서 사회 각 분야의 개인정보 침해 사례가 지속적으로 증가하고 있음에도 불구하고 개인정보 보호 관련 법률이 체계적으로 정비되지 못하여 사회적 혼란을 야기하고 있음에 따라, 사회 각계의 의견을 수렴하여 국민적 요구에 부합하는 개인정보보호법을 제정하고자 하는 것이다. 종국적으로 이 법안의 목적은 개인정보의 취급이 정보주체의 참여 속에 공정·투명하게 이루어지도록 하여 개인의 자유로운 인격발현과 정보사회의 지속적 발전에 이바지하고자 함에 있다. 그 주요내용은 다음과 같다.

첫째, 개인의 자유로운 인격발현과 정보사회의 지속적인 발전을 법의 기본이념으로 천명하고 개인정보 취급의 원칙을 제시한 후(안 제2조 제1항 및 제2항), 공공부문과 민간부문을 불문하고 개인정보취급자가 정보주체의 동의, 법률의 규정, 법률행위의 목적달성, 언론·출판 목적 및 정보주체의 생명, 신체 및 재산을 보호하기 위하여 필요한 경우에 제한적으로 개인정보를 수집할 수 있도록 하고 있다(안 제6조).

둘째, 개인의 사생활을 침해할 우려가 있는 개인정보의 수집을 제한하며 차별적인 목적의 개인정보 수집을 금지하고 있다(안 제7조 및 제8조).

셋째, 자동화된 개인정보수집장치(CCTV, 쿠키 및 E-Mail 수집기 등)를 이용하는 경우 일정한 사항을 정보주체에게 알리도록 하여 개인정보의 무단수집을 제한할 수 있는 근거를 마련하고(안 제9조), 정보주체의 열람·정정청구권을 보장하고 개인정보취급자에게 일정한 경우 개인정보를 삭제·과기하거나 접근을 차단하는 조치를 하도록 하고 있다(안 제11조 및 제12조).

넷째, 고유식별자를 정보주체의 동의 없이 당해 식별자의 목적 이외에는 사용할 수 없도록 하고 있다(안 제15조).

다섯째, 일정수준의 개인정보취급자에게 개인정보보호담당자를 지정하도록 하여 개인정보취급자가 자율적으로 규제할 수 있도록 하고 있다(안 제16조).

여섯째, 국가의 개인정보보호 시책 강구와 제도 및 사회적 관행의 개선을 위한 책무를 규정하고 개인정보보호위원회가 개인정보에 관한 시책을 관장하도록 하고 있다(안 제18조 및 제19조).

일곱째, 개인정보보호 업무의 체계적·일관적 집행을 위해 국무총리 소속하에 개인정보보호위원회를 설치하도록 하고 있다(안 제24조).

여덟째, 개인정보보호위원회가 개인정보 침해사건에 관하여 자료제출, 현황조회 및 방문조사를 할 수 있도록 함으로써 실질적·효과적인 구제기능을 수행할 수 있는 근거를 마련하고 있다(안 제37조 및 38조).

아홉째, 개인정보보호위원회가 개인정보 침해사건에 대하여 필요한 경우 시정명령 등을 발할 수 있도록 하여 신속한 피해구제 및 구제의 실효성을 확보하도록 하고 있다(안 제40조).

열째, 개인정보에 관한 분쟁 조정업무를 신속하고 공정하게 처리하기 위하여 개인정보보호위원회에 개인정보분쟁조정위원회를 두도록 하고 있다(안 제43조).

### (3) 이해훈안

정보통신기기의 보급 확대, 전자정부의 추진 등으로 최근 사회 각 분야에서 개인정보의 수집·처리가 급속히 확대되고 있으나 현행 개인정보보호 관련 법률은 특정 분야에 한정되어 있어 사회 전반에 걸쳐 광범위하게 수집·처리되고 있는 다양한 형태의 개인정보를 적절히 보호하지 못하고 있음은 주지의 사실이다. 이로 인해 개인정보보호가 특별히 강조되고 있는 반면 다른 쪽에서는 아무런 제한 없이 개인정보가 수집·사용되고 있는바, 사회 각 분야의 개인정보처리에 대하여 공통적으로 적용될 수 있는 원칙과 기준의 제시가 시급하다는 취지에서 이 법안은 국제적인 흐름에 맞추어 개인정보의 보호와 활용을 조화롭게 이끌어갈 수 있는 종합적인 개인정보보호법을 제정해야 한다는 사회적 요구가 증대되고 있다는 점에서 발의된 것이다. 이로써 이처럼 사회 전체적으로 개인정보의 오·남용으로 인한 피해를 방지하면서 동시에 개인정보의 건전한 활용을 보장할 수 있는 대책 마련이 시급하다는 국민적 공감대가 형성됨에 따라 사회 각계각층의 의견을 수렴하여 이에 부합하는 개인정보보호법을 제정하여, 이를 통해 개인정보의 오·남용과 비밀감시로부터 정보주체의 자유와 권리를 보호하고 동시에 개인정보의 적절한 활용을 보장함으로써 정보사회의 균형적인 발전에 이바지하고자 한다. 그 주요내용은 다음과 같다.

첫째, 개인정보의 보호와 이용을 조화시키기 위하여 개인의 자유 및 권리 보호와 함께 개인정보의 적절한 이용을 이 법의 목적으로 제시하되, 단순히 개인·가족의 이용을 목적으로 개인정보를 처리하는 경우, 정보주체의 급박한 생명·신체·재산상의 위험을 예방하기 위해 개인정보를 처리하는 경우, 통계·연구 등을 목적으로 식별성을 제거하고 개인정보를 처리하는 경우, 언론·출판기관, 종교단체, 정당 등이 고유의 활동을 목적으로 개인정보를 처리하는 경우에는 이 법의 적용

을 제외하고 있다(안 제1조 및 제62조).

둘째, 개인정보처리에 관한 원칙을 개인정보처리 일반에 적용되는 원칙(안 제2장 및 제3장)과 공공부문과 민간부문에 각각 적용되는 특칙으로 구분하여 규정하고 있으며(안 제4장 및 제5장), 개인정보의 처리와 관련하여 정보주체가 향유하는 기본적 권리 및 개인정보처리의 기본원칙을 천명하고 있다(안 제4조 및 제18조).

셋째, 원칙적으로 정보주체의 동의가 있거나 법률의 규정에 의하여 개인정보의 처리가 허용된 경우에만 제한적으로 개인정보를 수집·처리할 수 있도록 하되(안 제6조 제1항), 다만 개인정보처리자의 정당한 이익을 보호하기 위하여 필요한 경우, 공공의 안전과 이익을 위하여 필요한 경우 등에는 동의 없이 개인정보를 수집·처리할 수 있도록 예외사유를 인정하고 있다(안 제29조 제1항).

넷째, 개인정보는 정보주체로부터 직접 수집하는 것을 원칙으로 하고 정보주체 이외로부터 개인정보를 수집하는 경우에는 개인정보의 이용·제공시 그 출처 등을 고지하도록 하고(안 제7조), 고유식별자를 정보주체의 동의 없이 당해 식별자의 고유 목적 이외의 용도로 수집·처리하지 못하도록 하고 있다(안 제10조).

다섯째, 정보주체의 권리를 구체적으로 실현하기 위하여 열람 및 정정 청구권, 이용 및 제공 정지 청구권, 파기·삭제 청구권을 규정하고 있으며(안 제19조 및 제20조), 공공부문의 개인정보처리에 대해서는 원칙적으로 법률유보주의를 채택하고(안 제25조) 개인정보 피해의 사전적 예방기능을 강화하기 위하여 개인정보파일 등록제(안 제26조)와 개인정보사전영향평가제를 도입하고 있다(안 제27조).

여섯째, 영리목적으로 개인정보파일을 구축하여 마케팅 등의 대행사업을 영위하거나 개인정보의 제공사업을 하고자 하는 자는 개인정보위원회에 등록하도록 하고 정보주체가 입은 피해에 대하여 정보를 제

공관은 자와 연대하여 책임을 지도록 하면서(안 제30조), 민간부문의 자율규제활동을 촉진하기 위해 개인정보처리와 관련한 상담·정보제공, 피해구제, 교육·홍보, 정책의 연구·건의 등을 행하는 사업자단체 및 소비자단체를 등록·지원할 수 있게 하고(안 제32조) 개인정보 영향평가의 자율적 실시, 개인정보보호 신뢰마크의 활성화 등을 위해 일정한 시설과 기술을 보유한 자를 지정평가·인증기관으로 지정할 수 있게 하고 이다(안 제52조).

일곱째, 개인정보보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리소속으로 개인정보위원회를 두고, 위원회의 임무가 개인정보의 보호와 이용의 균형적 발전에 있음을 명확히 하기 위하여 명칭을 개인정보위원회로 하며(안 제34조), 개인정보위원회의 주요 기능을 정책연구, 제도개선, 상담 및 피해구제, 교육·홍보, 기술 개발 및 지원 등에 뒀으로써 지원·촉진기능을 강화하고 규제적 기능을 최소화하고 있다(안 제41조).

여덟째, 개인정보위원회가 효율적으로 업무를 수행할 수 있도록 하기 위해 개인정보위원회에게 자료제출요구권, 현황조회권, 방문조사권, 시정권고, 시정명령, 고발 및 징계권고권 등의 권한을 부여하면서(안 제43조 내지 제49조), 개인정보처리자의 자율적 준수를 유도하기 위하여 개인정보위원회가 개인정보침해의 유형·판단기준 및 그 예방조치 등에 관한 지침을 정하여 고시할 수 있게 하고 있다(제50조).

아홉째, 개인정보에 관한 분쟁조정 업무를 신속하고 공정하게 처리하기 위하여 개인정보위원회에 개인정보분쟁조정위원회를 설치할 것을 제안하고 있다(제55조).

열째, 개인을 고유하게 식별하기 위하여 부여·사용되는 신분증표 또는 식별정보의 도용, 사생활 침해를 목적으로 한 은밀한 자동화된 개인정보수집장치의 설치·운영 등을 금지하고 있다(안 제67조).

#### (4) 통합법안

위 세 법안의 내용 가운데 중첩되는 사항을 담아내고 상이한 규정을 조율한다는 원칙에 따라 총 8장, 76조의 이른바 통합법안이 마련되었으나 의안으로 접수되지는 못하였으며, 위 법안들이 국회소관상임위원회 심사를 거친 상태로 계류되어 있다는 점에서 17대 국회 회기 내에 처리될 수 있는 가능성은 희박한 것으로 판단된다. 다만, 위 세 법안 소관이 법제사법위원회로 조율되고 위원장 대안으로 발의되어 본회의 심의를 받을 수 있기 위해서는 그 내용이 통합법안의 내용에 준할 것으로 예상된다.

### 3. 문제점 검토

#### 가. 논의의 전제

여기서는 현행법의 규율체계를 보완하는 기본법의 제정 당위성을 논의하면서, 그 입법목적에 충실할 수 있는 기본법 제정을 위하여 논의되어야 할 사항을 짚어보기로 한다. 개인정보보호를 향한 기본법 제정이 급선무일 수 있겠지만 헌법적 규범가치를 투영하는 정보질서를 현실적 정보환경으로 구축하고 이에 따라 개인정보보호법제를 재정립하며 정보기술산업 발전과 정보주체의 권리보장을 함께 실현하는 것이 보다 근본적이고 중요하다는 관점에서, 이하 거론하기로 한다.

#### 나. 합헌적 정보질서론 : 민간부문의 규제

일정한 연관성은 지니지만 여전히 국가와 구별되는 정보사회 역시 諸社會領域 중 하나이므로, 국가법질서와 상관적 영향을 주고받는다는 데에는 異論이 없을 것으로 본다.<sup>7)</sup> 이는 국가체계와 구별되는 사회구

7) 국가와 사회의 구별논의에 관하여 어떠한 이론적 견해를 채택하느냐에 따라 본질적으로 국가영역에서 정치적 결단이라 할 수 있는 헌법규범과 사회영역에서 형성된 경제현상과의 관계는 다른 국면에 놓이게 된다. 그러나 국가와 사회영역에 관한

조상의 경제영역과 그 논리의 軌를 같이 하며, 明文으로 經濟秩序를 특정하지 않고 있는 헌법의 중립성은 구성원의 속성상 동일선상에 놓여 있는 정보질서에 대한 태도에도 적용될 수 있을 것이라 여겨진다. 대한민국헌법 제119조는 제1항에서 “대한민국의 경제질서는 개인과 기업의 경제상의 자유와 창의를 존중함을 기본으로 한다”고 규정하여, 국가가 시장의 자율성을 보장하면서 시장참여자들간의 경쟁을 위한 규칙(game rule)을 확정하고 그 행위준거를 제시하는 한편 그들이 상호신뢰감이나 안정감을 가지고 시장활동(market operation)을 영위할 수 있도록 각종의 표준이나 지침 등을 설정함으로써 그 과정과 결과 모두를 행위자가 책임질 수 있게 하는 것을 기본적인 경제질서로 삼고 있다. 즉, 국가는 규범설정자이자 심판관이며 사후적 교정자 또는 후견자로서 기능함으로써 시장의 자율성을 최대한 보장해 주어야 한다는 것이다. 다만 동조(同條) 제2항에서는 “국가는 균형 있는 국민경제의 성장 및 안정과 적정한 소득의 분배를 유지하고, 시장의 지배와 경제력의 남용을 방지하며, 경제주체간의 조화를 통한 경제의 민주화를 위하여 경제에 관한 규제와 조정을 할 수 있다”고 하여, 경제주체간의 조화를 통한 경제의 민주화라는 요청에 따라 국가가 시민사회의 경제영역에의 참여를 중심으로 하는 절차적 장치와 그 실천이 적정하고도 유의미한 판단 아래 이루어지도록 하여 그들이 진정한 참여자로 기능할 수 있게 하는 보조자적 지위를 수행할 것을 요구하고 있기도 하다. 헌법상의 경제질서를 시장경제질서로 확정하지 아니한 것<sup>8)</sup>은 입법자

---

현대적 판단은 상호연관성 아래 국가와 사회가 각자의 기능을 수행하여야 하며 사회적 합의(consensus)의 가치규범적 수용이 유기적으로 형성되어야 한다는 점을 강조한다고 볼 수 있다. 즉, 국가와 사회가 헌법과 경제가 지니는 상호관계를 一元論적으로 헌법이 규정하여야 할 국가의 부분영역인 경제라든가 二元論적으로 헌법규범에서 벗어난 독자적 사회영역으로서의 경제부문은 인정할 수 없을 것이라 볼 것이기에 국가로부터 자유로와야 할 경제적 자유의 보장과 함께 규범으로 제시된 이상적 질서에의 존중과 함께 국가규제적 기능의 통제를 함께 조화시켜야 한다는 현실적 측면이 간과되어서는 아니 된다고 할 것이다.

8) 우리 헌법은 특정 경제질서를 직접 명문으로 규정하고 있지 않으므로 憲法制定者가

가 특정한 경제질서에 구애됨 없이 자유롭게 경제정책을 실시할 수 있도록 광범위한 형성재량을 부여하고자 한 데 있고, 이러한 입법형성의 자유는 현존하는 경제질서를 통하여 제한되지 않으므로 헌법은 경제질서상 중립적이라고 할 것이다.<sup>9)</sup> 다만 개인과 기업이 보유하고 향유할 수 있는 경제상 자유와 창의를 존중하는 것이 경제질서의 根幹임을 부인할 수 없다.

이처럼 경제질서에 대하여 중립적인 헌법규범은 정보질서에 대해서도 침묵하고 있는데, 이를 원용하면 정보의 집중화·독점화 및 정보의 불균형·불평등을 극복하기 위한 배분적 정의의 실천을 통해 정보의 민주화를 통한 국민 모두의 인격실현 가능성을 확충한다는 맥락에서 접근되어지는 구조라 할 수 있을 것이다. 물론 그 전체적 기초는 국가의 정보화정책방향이 기업의 정보능력증진을 통해 국가경쟁력을 강화한다는 측면이 엄연히 존재하기 때문에, 정보시장의 투명성·공명성이 보장되도록 규제로서의 시장개입이 보완되는 시스템인 것이다. 위에서 살펴본 바와 같이 규범적으로 개방된 경제질서에서 기업의 자유<sup>10)</sup>는 헌법 제15조에 규정된 직업(선택)의 자유와 헌법 제23조 소정의 재산권 등에서 도출될 수 있는바, 이는 우리 헌법이 상정하고 있는 경제구

---

특정 경제질서를 선택하지 않고 개방시켜 놓고 있다고 하겠다. 헌법규정으로부터 특정 경제질서를 헌법적 질서로 설정하는 것은 헌법적 필요성이나 실효성도 없다고 할 것이므로, 헌법에서 특정 경제질서의 보장을 도출하는 것은 타당하지 않다고 보는 것이 적절하다고 본다; 한수웅, 한국헌법상의 경제질서, 공법학의 현대적 지평, 박영사, 1995, 190쪽.

9) *Vgl.* BVerfGE 4, 7, 18; 14, 19, 23.

10) 헌법 제119조에서 시장자유와 국가개입에 대하여 ‘원칙-예외’의 형식에 따라 규제와 조정을 통해 경제에 개입하는 입법자에게 가증된 소명의무만을 부과하고 있고 헌법상의 사회국가원리나 경제제도론 등의 경우에도 기업의 공적 책임성 원칙에 대한 확인 이상의 구체적인 판단기준을 제시하지 못하고 있는 것은, ‘기업의 자유’의 제한과 한계의 문제는 ‘자유와 책임의 조화’라는 추상적 지침만으로 해결될 수 없고 기업활동규제의 효과와 역기능에 대한 면밀한 검토를 바탕으로 개별적인 기본권해석을 통해 판단될 수 있다; 이덕연, 한국의 경제헌법질서상 기업의 자유, 공법연구 제29집 제1호, 한국공법학회, 2000, 174쪽.

조를 형성하는 기본권이며 산업적 측면에서의 정보활동에 대한 규범적 설정의 기초를 이루고 있기에 정보사회에서의 정보의 활용에 있어서도 헌법적 가치를 제공하는 정보질서를 설명할 수 있게 한다. 따라서 정부규제로서의 시장개입은 자유시장과 정부부문 상호간을 단순히 이분법적으로 분절하는 대립관계를 넘어, 구체적으로 어떤 범위에서 어떤 종류의 규제가 헌법적 가치로서의 정의 관념에 부합하는지를 검토하는 방향에서 접근되어야 할 것이다. 이러한 전제하에서 規制的 矛盾(regulatory paradoxes)을 유형별로 재논의할 필요가 제기되는데, 헌법적 정보질서에 상응하는 정보활용의 자유와 책임의 조화를 구체화하기 위하여는 헌법상의 경제질서와 기업의 자유 그리고 개인정보에 대한 정보주체의 권리 등을 종합적으로 이해하여 우리 헌법이 지향하고 있는 정보질서를 규범적으로 판단해야 할 것이다. 이러한 측면에서 우리 헌법은 원칙적으로 정보의 활용과 유통의 산업적 활성화를 도모하기 위하여 개인과 기업의 정보활동을 장려하고 있으며, 다만 개인정보 보호와의 균형을 위해 예외적으로 정부규제와 시장개입을 허용하고 있는 것으로 새겨야 할 것이다. 정보의 자유를 갖는 개인과 기업 가운데 이를 기업의 자유에 의해 영업활동을 하는 데 있어서는 정보상 자유와 창의를 존중하는 질서가 규범적으로 인정되어야 하고 이를 침해하지 않는 범위 내에서 정보의 민주화라는 요청에 따른 최소한의 정부규제가 정당화되는 것으로 類推解釋할 수 있다고 본다면, 規制合理化의 線上에서 재검토할 필요성이 있다고 할 것이다.

#### 다. 피규율분야의 구별 : 공공부문의 통제

그동안 개인정보보호법규의 체계상 모순을 시정하고자 제기되어 온 기본법의 제정을 주장하는 각계의견은 규제영역으로 공공부문과 민간부문의 통합 혹은 분리에 큰 논란을 지니고 있었다. 그런데 기본법 제정의 논거에 대하여 ①새로운 정보처리기술에 대한 위협성에 대처, ②개

별법간 법체계 및 구성에 있어 함유된 모순 제거, ③기본법 제정을 전제로 독립보호기구 설치의 법제화 등이 논의되어 왔으나, 통합법제 구성상 보호수준이 제고되는 것인지는 짚어보아야 한다.

그리고 다음과 같은 논거로 분리방식을 주장하는 견해가 유력함에 주의를 요한다. 즉 프라이버시<sup>11)</sup>의 연원에 따라 헌법상의 기본적 인 권으로서의 그것과 사법상의 권리로서의 그것이 차이가 있다는 점에서 개인정보보호제도에서도 양자가 구별됨을 강조하고 행정기관에 대해서는 민간사업자보다 엄격한 개인정보보호가 요구된다고 하거나,<sup>12)</sup> 국가가 법률로써 행정기관에 의한 개인정보의 취급에 제한을 마련하는 경우와 국가가 법률로써 사인에 의한 개인정보의 취급에 제한을 마련할 경우와는 문제의 구성은 물론 필요한 조정의 형태가 다르므로 이러한 차이를 무시하는 것은 적절하지 않다는 주장<sup>13)</sup>이 있음은 기본적으로 시장경제의 자율성을 근간으로 하고 있기 때문에 분리 방식의 설득력을 한층 높이고 있다. 또한 공공부문이 보유하는 개인정보의 보호는 헌법 제17조에 의거하여 개인의 존엄을 보장하는 의무를 근거로 하고 있으나 민간부문이 보유하는 개인정보의 보호는

---

11) 프라이버시(privacy)의 語原은 ‘사람의 눈을 피한다’는 뜻으로서의 라틴어인 *privatue* 에서 유래한다. 그 사전적 의미는 “사생활에 대하여 타인의 눈길로부터 떨어져 있는 상태, 은거하는 장소, 타인으로부터 독립하여 私的 秘密이 보장된 분위기, 타인에게 알려지기를 꺼리는 私事, 사적인 친척관계나 친밀한 관계와 같이 은밀한 관계 등을 뜻한다”고 기술되기도 하고(Merriam Webster, *Webster's new international dictionary of the English language unabridged*, Encyclopaedia Britannica, 1966, p.1804.), ‘사회·타인의 호기심 그리고 영향력으로부터 독립된 것으로서 규범적 요소를 포함한 개인적인 영역에 대한 접근의 배타적 통제력’으로 풀이할 수 있다(David L. Sills, *International Encyclopedia of the Social Science*, Vol.12, the MacMillan Press, 1976, p.480). 넓은 의미에서는 권리로서 프라이버시의 개념 범주가 기본권으로서 사생활의 비밀과 자유를 포함하는 의미를 지닌다고 할 수 있지만, 분명 兩者는 중첩되는 영역을 지니고 있으므로 여기서도 이를 混用하기로 한다.

12) Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law : A Study of United States Data Protection*, Charlottesville; Michie Law Publishers, 1996, pp.24~25.

13) 松井茂記, 個人情報保護基本法とプライバシーの權利, *ジュリスト* No.1190, 2000, 41~42面; 田島泰彦, 個人情報保護制度をどう構想するか, *法律時報* 第72卷 第10號, 2000, 4~5面.

개인의 존엄이 기본적 인권으로서 보장되는 것에 대하여는 적어도 헌법의 간접적인 적용을 받는 것이지만 동시에 표현의 자유·알 권리·사적 자치의 원칙 등과의 조정 및 조화가 고려되어야 하므로, 두 부문에서의 개인정보보호에 관한 원리가 상이하게 나타난다고 한다.<sup>14)</sup> 상식적으로 생각해 보아도 공적 영역과 사적 영역에서는 개인정보의 수집목적 및 이용형태 등이 다르다는 것을 알 수 있는데, 통합방식에서는 이러한 특성을 고려하기 어려울 것이라 예상할 수 있는 것이다. 하지만 체계적인 보호법규의 정립을 위해서는 개인정보보호에 관한 기본적인 일반원칙을 수립하고 규제의 필요와 정도에 따라 영역별로 차별적인 내용을 구체화하는 것이 정석이라 할 수 있다. 따라서 공공부문과 민간부문을 동시에 규율하는 기본원칙과 기본내용을 정립하고 개인정보보호의 필요성이 높은 분야 등에 대해서는 개별법으로 규율하며 민간사업자 등의 자율적 해결을 존중하는 입장에서 사적 영역에서는 자율적인 규제를 촉진하고 지원하는 구조를 채택함으로써, 이들을 전체적으로 취합하고 조화하여 운용될 수 있는 최적의 개인정보보호체도를 정립하는 것을 기본방향으로 설정하는 것이 바람직할 것이다. 그리고 통합방식에 따라 개인정보보호에 관한 기본법을 제정한다면 ①통일적이고 체계적인 적용을 가능하게 하는 일반적 대원칙의 수용, ②전문성이 요구되는 경우에만 특별법 또는 개별법을 제정하여 기본법의 원칙은 특별한 경우에만 그 적용의 예외를 인정, ③기본법의 원칙이 보장되고 개별법에 산재되어 있는 예외규정을 최소화함으로써 법적 안정성과 법집행의 실효성 확보 등의 규정을 그 내용으로 포섭하여야 한다. 이러한 접근방식은 중·장기적으로 개인정보보호체계 구성의 근본적 변혁을 가져오는 데 필수적이므로, 무엇보다 충분한 의견수렴과 신중하되 단호한 입법정책적 결단이 요구된다 하겠다.<sup>15)</sup> 그렇

14) 三宅 弘, 個人情報保護法制化の経緯と課題, 法律時報 第72卷 第10號, 2000, 9~10面.  
15) 拙稿, 개인정보보호법제의 개편논의와 개선방안, 정보통신정책 통권 제339호, 정보통신정책연구원, 2004, 37쪽.

다면 현행법 해석에 있어서도 개인정보에 관한 규제방식을 공공부문에 대한 그것과 동일하게 민간부문에 대입하는 정책은 지양되어야 할 것이다. 다만 사적 영역에서의 자유로운 정보유통 및 정보활용의 필요성과 유사하게 전자정부환경에서의 공적 영역의 특수성으로 인해 ‘행정정보의 공동이용’이라는 이념이 구체화되고 있는바, 이는 분명히 개인정보에 영향을 미치는 요인이므로 양자의 관계를 어떻게 조화롭게 설정하는지를 살펴보고 어떠한 점에서 민간부문과는 차이가 있으며 그렇다면 어떠한 논리적 기반을 구축되어야 할지를 여기에서 되짚어 볼 필요가 있다.

이에 대하여 검토해 보자면, 전자정부에서 정보활용의 문제는 공공부문이든 민간부문이든 당위적 전제요건이 되는 것이나 그 논리적 근간이 다른 까닭에 개인정보와 관련한 기본권보장에 있어서도 그 규제의 구별이 요청된다는 결론에 다다르게 된다. 즉, 공적 영역에 있어 개인정보의 활용은 원칙적으로 기본권의 제한을 가져오므로 기본권침해의 소지가 없는 한도 내에서 허용되는 반면, 사적 영역에 있어 개인정보의 활용은 원칙적으로 허용되는 것이지만 영업의 자유 혹은 표현의 자유와 같은 다른 기본권과의 관계에서 이익형량 여하에 따라 상호권익의 조율이 요구되며 이에 따라 예외적인 제한에 대한 규제수준이 가늠될 수 있는 것이다. 따라서 ‘전자정부의 구현이라는 公益<sup>16)</sup>을 위해 불가피하게 개인정보를 활용할 것인가’와 ‘營利目的으로 고객정보서비스라는 영업활동을 하기 위해 개인정보를 활용할 것인가’에 대한 법적 판단은 논리구성상 구별되는 것이고, 이에 대한 통제 역시 다른 척도에 의한 규제법리로 나타나야 하는 것이다.

---

16) 다원적 사회에서 공익개념의 판단은 무척 곤란하기 마련이지만, 행정주체가 행정을 행함에 있어 자의적인 판단에 따라 공익여부를 정해서는 아니 된다. 만약 헌법이나 법률이 공익에 관해 규정하고 있으면 이에 따라야 하고, 규정하는 바가 없다면 구체적 상황에서 제반사정을 고려하여 정해야 한다; 대법원 1990. 4.27. 선고 89누4093 판결.

[그림 2-1] 정보자기결정권의 효력에 따른 개인정보의 활용 여부

	원 칙	논 거	예 외	논 거
공공부문	개인정보활용의 금지	기본권침해	개인정보활용의 허용	기본권제한
민간부문	개인정보활용의 허용	기본권충돌	개인정보활용의 금지	대사인효력

원칙적으로 前者의 경우 공권력에 의한 基本權侵害의 소지가 있는 것이므로 적절한 통제가 요구되는 것이고 다만 정당한 목적의 공익을 위한 개인정보의 활용이 법률유보원칙에 위배되지 않거나 비례원칙의 위반이 없다면, 혹은 기본권의 본질적 내용을 침해하지 않을 때에만 예외적으로 基本權制限이 된다.<sup>17)</sup> 그리고 이를 법률유보의 원칙에 대입하여 행정정보의 공개에 적용한 것이 바로 『공공기관의 정보공개에 관한 법률』이라는 점은 공공영역에 있어서 개인정보침해라는 공권력에 의한 침익적 행정작용을 통제하기 위해 개인정보보호법리가 관철되어야 하고, 다만 공익적 요청이 있는 경우 정당화사유가 충족되어야만 위 법에 따라 제한적으로 개인정보가 공개될 수 있는 구조를 보이고 있다. 그렇지만 後者の 경우 원칙적으로 複數의 기본권주체가 서로 대립되는 상이한 기본권의 적용을 주장하는 基本權衝突의 문제가 되므로 그 구체적 사정을 고려해 조화롭게 法益衡量을 할 것인지가 관건이 되며, 개인정보 관련 권익침해의 경우 예외적으로 정보자기결정권은 제3자적 효력을 갖게 되어 직접 적용될 수 있는 것이다.

17) 물론 헌법이 공익이라는 용어를 직접 사용하고 있는 것은 아니지만, 헌법 제37조 제2항 및 제23조 제2항의 ‘공공복리’, 제23조 제3항의 ‘공공의 필요’, 제77조의 ‘공공의 안녕질서’ 등의 개념은 공익 개념 그 자체를 말하고 있다고 보아도 무방할 것이다. 그리고 현행 헌법상 최고이념은 헌법 제10조상의 ‘인간의 존엄과 가치의 실현’이라는 목표에 있다고 판단되므로, 행정은 궁극적으로 이에 봉사하는 것이어야 하며 이를 이루는 과정에서 예컨대 사회보장·완전고용·물가안정 등과 같은 공익의 구체적 내용이 공간과 시간상 제한된 국가이해를 전제로 영속적으로 구체화될 수 있는 것이다.

이처럼 정보자기결정권이라는 개인의 자유와 정보활용이라는 기업의 자유가 상충된 가치로서 대립하는 민간영역에서는 兩者間 이의형량에 따르는 것이 원칙이며, 다만 예외적으로 정보활용이 부당하게 개인정보를 침해하는 경우 비로소 국가가 개입하게 되어 정보자기결정권의 효력이 관철된다 하겠다. 즉 원칙적으로 금지되는 행위가 아닌 것에 대한 제한원리가 적용되는 것인지 아니면 일반적으로 제한되는 행위에 대하여 정당화사유가 있는 경우 예외적으로 허용할 수 있는 것인지에 관한 구별의 문제인 것이다.

따라서 정보자기결정권의 효력이 미치는 범주에 따라 개인정보의 활용이 허용되느냐 아니면 규제되느냐가 달라지는 것이고 이는 公·私法二元論에 따른 논리필연적 귀결이 아니라 귀납적으로 공·사 영역에서의 개인정보보호를 위한 규제법리가 구별되는 논거를 제시한다. 이에 따르면 그 독립성 여부로 논란이 있는 개인정보보호기구의 설치와 관련하여, 그 소관업무는 공공부문에 대한 개인정보보호사무로서 공권력에 대한 개인정보침해의 통제에 주력하는 개인정보영향평가제가 중점이 되어야 할 것인바, 이로써 정보자기결정권의 내재적 한계와 그 제한에 대한 검토를 수반하여 정책적 판단을 형성해야 할 것이다.

#### 라. 논의의 귀결

요컨대, 전자정부에 있어서는 ①행정상 개인정보보호는 투명한 행정의 전제조건이라는 점, ②행정의 신뢰는 시민의 자발적 참여와 민주주의를 신장한다는 점, ③행정의 투명성과 효율성을 보장하여 시민의 신뢰도를 제고할 수 있다는 점 등에서 개인정보보호는 중요한 변수가 된다. 게다가 전자정부시스템이 가동되어 전자정부서비스가 실시됨으로써 행정의 효율성이 향상되고 민원의 전자적 신청·발급 등으로 국민 편익이 증대되며 전자정부가 정착되어 국가경쟁력이 제고될 것으

로 기대되기도 하지만, 정보인권의 보장이라는 측면에서 개인정보가 얼마나 충분히 보호될 수 있겠느냐 하는 점에서는 오히려 경계심이 증폭된다. 달리 표현하면 인터넷이라는 개방형 네트워크를 경유하여 개인정보가 자유로이 유통되는 시점에서, 자신의 개인정보가 자유의사에 반하여 광범위하게 유출·남용되어 정보자기결정권이 침해되지 않을까 하는 우려가 더욱 높아지게 되는 것이다. 이러한 관점에서 정보주체의 개인정보가 안전하게 처리된다는 신뢰를 갖게 하는 것이야말로 국민들로 하여금 안심하고 전자정부에 접근하게 하는 원동력이 될 것이라는 점을 추론할 수 있으며, 결국 개인정보의 충분한 보호가 전자정부 활성화의 선결조건이 되는 것이다.

따라서 전자정부시스템의 점진적 형성으로 요청되는 개인정보보호 관련법제의 정비 및 기술수준의 향상에 적절히 대응하면서 전자정부 시대에 합당한 보다 개선된 개인정보보호제도의 정착이 시급하다고 하겠다. 또한 정보의 활용 및 정보의 공개 측면에서의 가치를 개인정보보호의 의의와 균형을 이루도록 적정화함이 전자정부실현의 내실에 합치되도록 구성되어야 할 것이다. 이를 위해 사회의 정보화를 위한 정보활용과 정부의 전자화를 위한 정보공개에 대해 개인정보보호가 제한기준으로 설정되도록 최적한계를 조율함으로써, 정보기술의 발전에 중립적이면서도 정부기능의 효율성과 정부활동의 투명성을 제고하는 정보보호수준을 유지하는 데 역점을 두어야 한다. 그 정점에 개인정보에 관한 정보주체의 권리인 정보자기결정권이 존재한다. 그러나 정보자기결정권은 결코 절대적인 보장을 받을 수는 없고, 다른 충돌하는 규범적 가치와 조화를 이루어야 한다. 따라서 정보자기결정권은 알 권리 및 표현의 자유 또는 영업의 자유와 같은 규범가치와 조화를 이루어야 한다. 더욱이 정보자기결정권의 보장 정도는 공공부문과 민간부문이 반드시 동일할 수는 없다고 볼 것이다. 시장에서의 개인정보 수집은 그 기본목적이 시장의 효율성을 높이기 위한 데에 있어 시장

에 참여하는 사람들은 올바른 결정과 판단을 내리기 위해 가능한 한 불확실성을 줄일 필요가 있고 그만큼 개인정보에 대한 요구가 높아지게 된다. 또한 시장에서 이루어지는 소비자에 대한 결정은 공공기관이 시민에 대해 행하는 결정에 비해 그 성격이 권력적이지 않으며 그만큼 영향력이 낮다고 하겠다. 그러므로 민간부문에서 정보자기결정권의 보장 수준은 공공부문에서의 그것에 비해 완화될 필요가 있다.<sup>18)</sup> 다만 그 위험성의 정도에 따라 영역별 또는 부문별로 그 보장 수준을 조절할 필요가 있을 것이다.

그렇다면 개인정보보호를 위한 정보질서가 아니라 바람직한 정보환경을 조성하는 데 최소한의 제한으로서 개인정보보호가 요구되는 것이고, 이를 위해서는 정보활용을 포함한 정보의 자유와 조화로운 개인정보보호 관련 법제도가 형성되어야 한다. 이를 위해서는 민간부문에 있어 개인정보보호에 관한 자율규제를 적정화하고 규제의 법제화로 인한 폐단을 정제하는 것이 필요하다.

생각건대, 이러한 논거로 공공부문에 대한 행정통제와 민간부문에 대한 규제완화에 맞물리게 개인정보와 관련된 정보주체의 권익이 헌법적 정보질서에 상응하게 조율될 수 있도록 법체계의 재정립이 요구된다고 본다면 기본법 제정에 있어서는 적어도 공공부문과 민간부문을 구분하여 규율하고 있는 독일의 연방정보보호법(*Bundesdatenschutzgesetz*)의 규율체계가 확보되어야 할 것으로 판단된다.<sup>19)</sup> 이에 따라 개인정보보호 기구의 권한이 공공부문과 민간부문에 이원적인 조율이 견지되어 기본법의 입법취지에 있어 공공부문의 통제와 민간부문의 규제완화에

18) 同旨 : 이인호, 개인정보자기결정권의 한계와 제한에 관한 연구, 개인정보연구 01-01, 한국정보보호진흥원, 2001, 63쪽; 이 같은 논거에 따라서도 규제영역으로서 공공부문과 민간부문의 구분이 필요하다.

19) 위 법의 규율상세와 그 적용사례에 대하여는 *Vgl. Hans H. Wohlgemuth & Jürgen Gerloff, Datenschutzrecht: Eine Einführung mit praktischen Fällen*, Luchterhand, 2005, 7ff.

대응한 정보자기결정권에 대한 적절한 보장이 헌법적 정보질서에 부합하게 연동될 수 있을 것으로 본다.

### Ⅲ. CCTV 규정 진단

#### 1. 총괄적 논의

##### 가. 입법경위

1989년 2월 들어 국제인권옹호 한국연맹의 법제정 건의를 시작으로 언론과 시민단체 등은 개인정보의 오·남용 사례보도 등 여론조성을 통하여 법제정의 필요성을 촉구하기 시작했는데, 그 결실이 1994년 1월 7일에 제정된 개인정보법이며 그 다음 해 시행되기에 이르렀다. 이후 1999년 1월 29일 법률 제5715호로 개정된 위 법은 일부사항이 보완되었지만, 전자정부구현에서 적절한 대응책의 구비나 새로이 등장한 정보기술 역기능 제거에 부족한 면이 많았기 때문에 그 개정이 요청되었다. 그러던 중 지난 2007년 5월 17일 기존에 논의되었던 CCTV 취급 화상정보와 관련정보주체의 권리를 보장하고 종전에 반영하지 못하였던 사항을 정비하도록 해 법률 제8448호로 일부개정된 위 법이 오는 11월 18일 시행되므로 이에 관한 실질적인 고찰이 필요한 시점이다.

##### 나. 용어정의

이른바 CCTV라 함은 특정 수신자만 서비스하는 것을 목적으로 하는 텔레비전전송시스템을 가리키는 화상통신용어이다. 교육·의료 및 지역 정보서비스 등 산업 분야 전반에 이용되고 있는 CCTV는 송신 측에서 수신 측까지 유선 또는 특수 무선 전송로를 이용하기 때문에 일반 대중은 마음대로 수신할 수 없으며, 산업용 텔레비전 또는 전용

텔레비전이라고도 한다.<sup>20)</sup> 일반적으로 촬영자가 없이 행해지는 映像의 脯燭에 의미를 두어 무인감시카메라로 통용되고 있으며, 이와 같은 기능을 갖는 장치를 無人團束裝備라 부를 수 있고 유럽에서는 이를 CCTV라는 시스템에 주목하기보다는 그 기능적 특질에 초점을 맞추어 비디오감시(video-surveillance)라 부른다.<sup>21)</sup>

전 세계에 설치된 CCTV는 2,600만대이며 미국에만 1,100만대라고 미국 MIT의 공학전문지 Technology Review 2003년 4월호가 보도한 바 있는데, 뉴욕의 미국시민자유연합(ACLU)은 1999년 맨해튼 지역의 CCTV를 2,397대로 집계했지만 9·11 테러 참사를 겪고 난 2003년에는 3배나 증가한 것으로 추산했다.<sup>22)</sup> 한편 15만대의 CCTV가 설치된 영국의 런던에서 시민들은 평균 5분에 한 번씩 하루 300번 정도 CCTV에 노출된다는 보고서도 있다. 우리나라에서도 곳곳에 CCTV가 설치되어 운영되고 있으며, 그 효과에 대하여는 언론에 보도되는 바와 같이 범죄수사의 증거확보에 있어서나 지하철역사에서 발생될 수 있는 안전사고의 예방에 있어서 중요한 역할을 하고 있다는 사실과 함께 사생활침해 논란에 휩싸여 부정적인 측면이 부각되고 있음은 이미 잘 알려진 이야기다. 또한 사회적 감시공포증에 대한 우려를 지적하는 목소리도 귀를 기울여야 할 상황인바,<sup>23)</sup> 누군가 나를 보고 있다는 인식이 사람에게 따라서는 무의식에 침잠되기도 하지만 경우에 따라서는

---

20) 한국정보통신기술협회, 정보통신용어사전, 두산동아, 2001, 1467쪽.

21) 이와 같은 관점에서 여기서도 비디오감시와 CCTV운용을 동의어로 사용하기로 한다.

22) Jay Stanley & Barry Steinhardt, *Bigger Monster Weaker Chains: The Growth of an American Surveillance Society*, Technology and Liberty Program, ACLU, 2003, p.2.

23) 국민일보 2006년 5월 12일자 기사(한국언론재단통합검색<[www.kinds.or.kr](http://www.kinds.or.kr)>); 여기서 상존하는 비디오감시에 대하여 정신질환의 유발이 가능함을 지적하고 있다. 불안장애 또는 공황장애로 이어질 개연성이 있음을 보도하면서도, ‘누군가 날 감시한다’는 생각이 든다고 물론 다 정신질환은 아님은 분명히 하고 있다. 정신과 전문의의 인터뷰를 빌어 감시공포증은 특수한 환경에 적응하기 위한 생체의 가장 기본적인 반응양상이지만, 그 공포증이 일상생활에 까지 악영향을 미친다면 치료의 대상이라는 점을 지적하고 있다.

정신적인 스트레스를 가중시킬 수 있기 때문에 정책적으로는 권리침해의 개연성에 대응하는 법적 구조를 확충하는 것이 필요하다. 사생활침해나 감시공포증을 사전 예방할 수 있기 위해서는 사회적 합의에 따라 일정한 기준을 마련하고 CCTV의 운용이 그 원칙에 부합하도록 하면서 권리침해의 발생에 대한 사후구제절차가 마련되어야 할 것이기 때문이다.

최근의 급격한 범죄증가는 그 대책장구가 어려운 양상을 보이고 있는데, 방범용 CCTV는 이러한 각종 최신 범죄예방 및 통제 기법 가운데 가장 효과적인 도구의 하나로 각광받고 있는 것이 사실이며 CCTV의 전 세계적 확산경향은 이를 반영하고 있다. 하지만 CCTV의 범죄 예방효과에 있어서도 논란이 끊이지 않고 있음 역시 간과할 수 없으며,<sup>24)</sup> 예컨대 ‘풍선효과’를 유발할 뿐이라는 지적은 범죄예방효과에 대한 기대가 과장되었다는 지적을 전면적으로 부정할 수 없는 근거가 될 것으로 보인다.<sup>25)</sup> 이처럼 현상론적으로 CCTV의 운용이 정당한 목적에 의하여 이루어지고 있는 가운데 그 목적이 얼마나 잘 이루어지고 있는지에 대한 분석 역시 의미 있는 일이겠지만, 법해석학적으로는 규범의 공백이 발생하고 있고 이를 보완해야 할 법정정책학적인 요청이 엄연히 존재한다는 점이 간과되어져서는 아니 될 것이다. 다시 말하자면, 사회학적 접근만을 취하여 감시목적과 상관관계를 이루는 비디오

---

24) 가령 2001년도 슈퍼불경기 입장객 10만 명을 스캔한 안면인식시스템은 범죄기록을 지닌 19명의 사람만을 선별하였으나 그 누구도 당국에 의해 추적되는 범죄자는 아니었으며, 플로리다주 탐과의 거리와 버지니아해변에서 범죄용의자식별을 위해 장착되어 사용되었던 안면인식시스템의 경우 단 한 건의 검거실적도 올리지 못했다는 사실은 논란을 가중시켜왔다; CNET News.com, *Technology strains to find menace in the crowd*, 2004. 6. 1.

25) 이러한 예는 국내에서도 찾을 수 있는 바, 국민일보 2004년 10월 12일자 8면 기사는 ‘강남 CCTV 헛돈 썼나?’라는 제목으로 관련사례를 열거하면서 강남구 일대에 CCTV가 설치된 뒤 한때 범행이 줄어들다가 이 같은 사실이 알려진 뒤 범행이 더욱 지능화되면서 최근 범죄가 다시 기승을 부리고 있음을 지적하고 있다. 덧붙여 CCTV 설치 인근지역으로 범죄가 전이되는 이른바 ‘풍선효과’에 대한 우려로 인하여 인근지역 주민 사이에서 불안감이 확산되고 있음을 전하고 있다.

감시의 효과성에 치중할 경우 입법론적 대안을 제시하기는 어려울 수 밖에 없는 것이므로 긴밀한 學際間 研究(interdisciplinary study)를 통하여 원인분석과 결과도출의 견련성을 확보해 나가야 한다. 이와 같은 시점에서 지난 해에는 정보통신부 주최로 CCTV 개인영상정보보호 가이드라인 공청회가 개최되었고 抽象的 行政指導의 산물인 위 가이드라인이 제정되어 시행되고 있다. 한편으로 공공기관의 CCTV 설치·운영에 대하여는 前述한 바와 같이 개인정보법 개정으로 이에 관한 정보주체의 권리보호를 규율하기에 이르렀다.

## 2. 개별적 논의

### 가. 규율범위의 양상

공공부문에 대한 CCTV 관련 논의는 개인정보법의 개정으로 법률유보원칙 위반이라는 위헌요인은 제거된 것으로 볼 수 있다. 하지만 민간부문에 대한 자율규제의 촉진에서 제정된 가이드라인의 경우에는 그 태생적 한계로 인하여 이를 법제화할 필요성이 제기되겠지만, 공공부문에 대한 CCTV 관련 논의는 개인정보법의 개정으로 법률유보원칙 위반이라는 위헌요인은 제거된 것으로 볼 수 있다. 하지만 민간부문에 대한 자율규제의 촉진에서 제정된 가이드라인의 경우에는 그 태생적 한계로 인하여 이를 법제화할 필요성이 제기되지만, 私法上 問題에 적용될 사안이 行政規制的 規律로 정보주체의 권리와 충돌되는 다른 기본권을 제한하는 결과가 양산될 수 있다는 점에서 입법적 고려가 선행되어야 할 것으로 본다.<sup>26)</sup>

26) 금융기관·기업체·공장 등과 같은 민간영역에서 CCTV를 운용하는 경우에는 원칙적으로 私的 自治의 原則이 적용되므로 해당기관이 CCTV를 설치하여 고객 혹은 근로자의 행위를 감시하고 있다는 사실을 고지 받고 이를 이용하는 경우에 그러한 이용조건에 동의한 것으로 볼 수 있을 것이나 그럼에도 불구하고 가령 노동현장에서 사용자의 CCTV 설치·운영에 따른 근로자의 행동감시행위가 필요최소한도를 넘어서서 근로자의 인격권 등 침해를 가져올 경우는 민법상 불법행위책임을 물을

영국 및 독일을 비롯한 유럽 주요국가들은 특히 공공기관에서 운영하는 CCTV의 법률상 근거를 요구하고 있으며,<sup>27)</sup> 이는 곧 법률유보원칙의 실현에 관한 문제와 동일한 사안이라 할 수 있다. CCTV로 인한 안전성으로 인하여 그 감시를 허용할 것인가 아니면 자유를 선택할 것인가 하는 질문에 대답할 수 있기 위해서는 최소한 법률상 규제가 첫 출발이 되어야 하기 때문이다. 따라서 법적 규제의 필요성에 따라 합헌적 근거입법을 명확히 정립하는 것이 요구되어짐에도 불구하고

---

수 있는 것이다. 그러므로 사적 자치의 원칙이 적용되는 민간부문이라 하더라도 CCTV의 운용에 관한 모든 행위가 정당화되는 공간이 아님에 유의해야 한다; 拙稿, 지방자치단체의 CCTV 운용에 관한 공법적 고찰, 인터넷법률 통권 제24호, 법무부, 2004, 113쪽.

27) CCTV의 설치·운영에 관하여는 정보주체의 권리와 운용목적의 공익이 맞서며, 영국에서는 유럽인권협약상의 프라이버시권과 보통법상의 계획허가권한과 같이 법익의 상충성을 보여주고 있다. 하지만 1998년 인권법 제정에 따라 정보인권의 지위는 강화되었고 2004년 현재 4백만 대가 넘는 카메라가 운용 중에 있으므로 이들이 비례원칙에 부합할 수 있는 방도를 찾아야 한다. 그럼에도 불구하고 내무부(Home Office)에서는 CCTV 운용이 인권법과 배치되는 것으로 볼 수 없다고 하였으며, Strasbourg에서 열린 聽聞에서는 비디오감시만으로 인권법 제8조를 위배하는 것으로 볼 수 없다는 해석이 이루어졌다고 한다. 한편 1998년 정보보호법 시행으로 2003년까지 모든 CCTV 시스템은 감독관에 등록하고 정보보호원칙을 준수하도록 요구되어졌으며, 그 구체적 사항은 規範具體化規則으로서 CCTV실행규약(a Code of Practice for CCTV)에 규율된다. 결국 영국은 유럽 프라이버시법을 위배하지 않으면서도 비디오감시에 대하여 공공부문과 민간부문을 차별화해 나름의 규제를 실행하고 있다고 하겠다.

반면에 독일에서는 비디오 감시가 州 警察法の 규율대상이 되어 16개주마다 개별적으로 규제되지만, ①영국과 같이 CCTV 운용의 법적 근거가 없는 유형, ②예외적으로 경찰에 의한 CCTV운용만이 허용되는 유형, ③경찰을 포함하여 공공부문의 전역에 대하여 CCTV 운용 및 畫像의 녹화·저장 등을 허용하는 유형으로 대별할 수 있다. 하지만 개인의 재산권이 公衆에 공개되어 있다면 CCTV의 운용은 허용되지만, 公·私法二元論의 영향을 받는 독일과 같은 대륙법계국가에서는 공공부문에서 운용되는 CCTV와는 법적 성질을 달리 보고 있다. 따라서 사인에 의한 CCTV 운용은 다른 사람의 인격권을 침해하지 아니하는 범위 내에서 재산권에 근거하여 이루어질 수 있지만, 타인과 법익균형성을 유지하여야 하며, 화상의 확대 또는 녹화는 법원의 허가를 얻어야 한다. 이와는 달리 경찰상의 비디오감시는 헌법상 기본권적 문제를 유발하는바, 현재 독일 각州에서는 법률유보의 원칙을 이행하고 있으며 그 관건은 비례원칙준수 여부라 할 것이다. 결국 CCTV 운용은 증대될 것이지만, 영국과 달리 독일 공공부문에 있어 그 법적 근거가 존재함은 상대적으로 정보보호제도의 강화요인으로 작용한다고 보겠다.

행정규칙에 지나지 않은 가이드라인에 따른 행정지도가 정보주체의 권익보장에 있어서 여전히 불충분한 것이고<sup>28)</sup> 이를 법제화함에 있어서는 기본권조화적 규율이 중핵이 될 것이라 판단된다.

#### 나. 규율내용의 문제

위와 같이 볼 때 실정법 차원에서 논의될 수 있는 것은 개정 개인정보법 소정의 CCTV 규율 내용이라 할 것이다. 이에 한정하여 비판적 고찰을 이어가면 다음과 같다.

첫째, 오는 11월 18일 시행되는 개정 개인정보법 제4조의2는 제1항에서 “공공기관의 장은 범죄예방 및 교통단속 등 공익을 위하여 필요한 경우에 「행정절차법」 제2조 제6호에 따른 공청회 등 대통령령으로 정하는 절차를 거쳐 관련 전문가 및 이해관계인의 의견을 수렴한 후 폐쇄회로 텔레비전을 설치할 수 있다”라고 규정하고 있다. CCTV에 의한 화상정보 수집 역시 개인정보의 수집원칙에 의거하여 개인정보법 소정의 제원칙에 따라 수집되어야 함을 천명함으로써,<sup>29)</sup> 개인정보

28) 현행 가이드라인은 그 형식상 국민과 행정권을 모두 구속하고 재판규범이 되는 성질인 법규성이 인정되지 않는 행정규칙으로 보는 것이 일반적이나, 행정조직 내부관계에서 조직·업무처리절차·활동기준 등에 관하여 규율하는 일반적·추상적 규정으로서 대외적 구속력이 없는 행정규칙인 까닭에 규제적 사항이 규정되어 있을 경우 이는 행정규제기본법 제4조제1항(규제법정주의 : 규제는 법률에 근거하여야 하며, 그 내용은 알기 쉬운 용어로 구체적이고 명확하게 규정되어야 한다)을 위반하게 되는 것이다. 하지만 법규명령과 행정규칙의 구별은 그 형식이 아니라 실질적 기능에 따라 구별되는 것이며 뿐만 아니라 행정규칙이란 강학상의 개념이나, 고유한 형식이 존재하는 것이 아니므로 이를 형식상 분류하는 것은 무의미하다고 하는 실질론이 통설적 지위를 점하고 있으며 그렇다면 행정규제기본법 소정의 ‘법령 등’에 해당하는 ‘고시 등’으로서 행정규칙을 훈령·예규·고시 및 공고로 이해할 때 가이드라인을 법규성이 있는 법규명령으로 이해할 수도 있게 되며, 이 경우 가이드라인은 ‘고시 등’에 속하는 행정규칙 형식의 법규명령으로 해석할 수 있는 여지는 존재한다고 볼 수 있다. 이 경우 가이드라인은 일종의 법률보충규칙 내지 규범구체화규칙으로서 법규성을 보유하는 것으로도 파악할 수 있다고 여겨진다.

29) 개인정보법 제3조의2 (개인정보보호의 원칙) ①공공기관의 장은 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적

법 규율이 CCTV에 의한 화상정보의 수집에 대한 법률근거이므로 이를 위배할 경우에는 개인정보법 소정의 일반적 제재와 불복이 가능하도록 설정하고 있어 헌법위반의 문제를 제거하고 있다. 그렇지만 법 시행령과 연계할 때에는 결국 입법기관이나 사법기관뿐만 아니라 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관, 즉 한국은행·한국산업은행 및 한국수출입은행 농협·수협·축협 중앙회, 새마을금고 등이 적용범위에서 배제될 수밖에 없다는 규율대상에서의 한계가 크다는 점을 지적할 수 있다.

둘째, 위 조항에 따라 의견수렴을 위한 공청회 등으로 민주적 정당성을 확보할 수 있는가 하는 문제는 별론으로 하더라도 ‘범죄예방 및 교통단속 등 공익을 위하여 필요한 경우에 한하여 설치 가능하다’는 설치목적상의 한계요인을 정보주체의 권리와 비교형량하는 절차적 요건에서 실질적 논의가 이루어지기 위해서는 지방자치단체별로 조례를 제정하거나<sup>30)</sup> 요건심사 및 영향평가에 관한 준칙을 제정하여 적절한 규제적용이 이루어지도록 보완할 필요가 있다.

셋째, 같은 조 제2항에서는 “설치된 폐쇄회로 텔레비전은 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추어서는 아니 되며, 녹음기능은 사용할 수 없다”라고 규정하고 있는바, CCTV 설치목적에 부합하지 않게 카메라 조작이 이루어질 경우 위 법 제23조 제3항 소정 구성요건에 해당되어 2년 이하의 징역 또는 700만 원 이하의 벌

---

법하고 정당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 아니 된다.

② 공공기관의 장은 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 한다.

③ 공공기관의 장은 개인정보관리의 책임관계를 명확히 하여야 한다.

④ 공공기관의 장은 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다.

30) 주민의 권리를 제한하는 CCTV 운용의 경우 지방자치법 제22조 단서에 따라 법률유보의 원칙이 적용되지 않으면 법률위반이 된다.

금에 처해지는데, 이 경우 예컨대 교통상황과악용 CCTV 관제센터에서 이루어지는 줌인(zoom-in)에 대하여 CCTV 관리위탁에 따라 ‘부정한 목적으로 제4조의2 제2항을 위반하여’라고 하는 구성요건에 부합되는지는 의문이다. 문리해석상 그 운용주체인 공공기관 소속의 개인정보처리담당자를 수범자로 하고 있다고 볼 수 있기 때문이다. 물론 개인정보법은 제4조의3에서 CCTV 설치 및 관리 위탁에 관하여 규율하며 제9조 제5항을 통하여 위탁기관에 대한 안전성확보에 관하여 규정하고 있지만, 수탁기관인 관제센터에 복무하는 자에 대한 적절한 통제를 보완해야 할 것으로 본다. 또한 개인정보법 제24조는 양벌규정을 두고 있는바, 행위자인 공무원에 대한 벌칙 외에 행정기관에 대한 직접적인 제재는 고려되지 않은 것으로 여겨진다는 점에서는 행정통제 관점에서 일정한 이격이 있다고 할 것이다. 오히려 해당기관의 정부업무평가와 연계하는 제재방안이 실질적일 수도 있을 것으로 사료된다.

넷째, 법 제4조의2는 제3항에서 “공공기관의 장은 폐쇄회로 텔레비전을 설치하는 경우 정보주체가 이를 쉽게 인식할 수 있도록 다음 각 호의 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다”라고 규정하면서 각호로 ①설치목적 및 장소, ②촬영범위 및 시간, ③관리책임자 및 연락처 등을 규율하고 제5항에서 “폐쇄회로 텔레비전의 설치, 안내판 설치 등에 관하여 필요한 사항은 대통령령으로 정한다”라고 위임입법의 수권근거를 명시하고 있다. 이에 따라 ①원거리 촬영 또는 교통흐름조사 등의 목적으로 CCTV를 설치하는 경우로서 권리침해의 위험이 적은 경우 안내판 설치에 갈음해 인터넷 홈페이지에 일정사항을 게재할 수 있게 된다. 따라서 정보주체에 CCTV 운용을 고지토록 하는 입법취지가 몰각되거나 안내판 설치로 오히려 감시적 현황과 심리적 압박이 가중될 수 있는 딜레마에 놓일 수 있음도 부인하기 어려운 실정이다.<sup>31)</sup>

31) CCTV 혹은 그 현존의 고지로 감시상황에의 주관적 인식을 복합적인 관점으로 비

#### 다. 기본법과의 연계

통합법안의 경우에 CCTV의 규율에 한정하지 않고 자동정보처리장치의 제한으로 확장하여 이를 다음과 같이 포섭하고 있다.

통합법안 제18조 (자동정보처리장치를 통한 처리 제한) ①누구든지 자동화된 방법으로 개인정보를 처리하는 장치 또는 기기(이하 ‘자동정보처리장치’라 한다)를 설치·운영하여 개인정보를 처리하거나 다른 사람의 모습, 이동경로, 행동태양 등을 관찰하고자 하는 때에는 대통령령이 정하는 방법에 따라 정보주체가 그 사실을 쉽게 인식할 수 있도록 하여야 한다. 다만, 자동정보처리장치를 설치·운영하는 자가 자신의 생명·신체·재산상의 이익을 보호하기 위하여 필요한 경우로서 대통령령이 정하는 경우에는 그러하지 아니하다. ▶ 위반시 형벌

②개인정보처리자가 제1항에 따라 개인정보를 처리하는 때에는 자동정보처리장치의 수집 및 활용 내역 등을 대통령령이 정하는 바에 따라 기록·관리하여야 한다. ▶ 위반시 질서벌

③자동정보처리장치의 구체적인 범위는 대통령령으로 정한다.

이러한 규율은 CCTV 등 자동정보처리장치의 운용에 있어서 기본적인 규범적 틀을 마련하고 있지만, 중국적으로 시행령 제정에 있어 개인정보보호기구의 사회적 합의 반영이 핵심이라 할 것이다. 생각건대, 규제완화요인의 조율과 행정통제요인의 강제가 조화롭게 규율되어야 한다.

---

디오감시를 바라볼 수 있다. CCTV가 존재한다는 사실이 아니라 그것을 알려주는 신호체계로 인해 감시효과가 강화된다는 것이다. 정보주체에게 CCTV 운용을 고지토록 함이, 명시적인 동의를 얻어 CCTV를 운영하도록 하는 것보다 완화된 규범설정이면서도 정보주체의 권리보호와 정보활용의 규제완화에 있어 타당한 것으로 이해되는 것과 달리, 고지신호 자체가 Foucault의 Panopticon을 떠올리게 하고 있음을 알 수 있다; See Mark Cole, *Signage and Surveillance*, *Surveillance & Society* Vol.2, 2004, pp.430~445.

#### IV. 결론에 같음하여

오늘날 정보화시대라고 일컫는 과도기적 용어를 무색케 할 정도로 급변하는 첨단 과학기술의 발전에 힘입어, 우리는 정보사회<sup>32)33)</sup>의 정점에 자리 잡고 있다. 따라서 공·사 영역을 불문하고 국가 전분야가 정보기술의 직접적인 영향을 받고 있는 현상은 새삼스러운 것이 아니다. 그래서 정보<sup>34)</sup> 그 자체가 가치를 가질뿐더러 또 다른 새로운 가치를 만들어내는 사회, 그래서 정보화<sup>35)</sup> 내지는 컴퓨터화(computerizing)

32) 지금 우리가 살아가고 있는 사회를 가리켜, 지각대상(percept)·기호(sign)·의미(meaning) 등의 세 요소로 나누지만 그 자체가 인간의 행위결과로 나타나는 정보(information)에 그 특성을 둔 情報社會(information society)라고 일컫는다는 것은 周知의 事實이다. 정보사회란 ‘정보를 생산도구로 사용하여 재화나 역무 혹은 정보 및 지식을 생산하고 유통시킴으로써 정보 가치가 사회경제활동의 중심이 되는 사회’로 간략히 설명할 수 있다; See F. Webster, *Theories of the Information Society*, London; Routledge, 1995, pp.15~21.

33) 정보사회라는 용어는 1968년 高山建一이 처음 사용하기 시작했는데, 초기 개념은 전체 고용인구의 절반 이상이 정보를 산출해내는 산업에 종사하거나 그들이 산출해내는 생산량이 전체 GNP의 50% 이상을 차지하는 사회를 가리키는 말이었다고 하나(Yoshihiro, *Changing Value Patterns and their Impact on Economic*, University of Tokyo Press, 1982, p.174), 현재는 ‘정보의 생산·처리 및 활용기술이 사회발전의 원동력이 되고 사회구조를 지배하게 되는 사회’라는 의미로 통용되고 있다. 따라서 정보사회를 주도하는 개념으로 특정가치를 가지는 정보와 이를 보유·활용하는 주체 그리고 수단적 변화요인으로서 정보기술 등이 거론되어진다.

34) 사실적 의미의 정보는 미디어(media)에 의해 송출되고 미디어 자체에 내재하는 정보라 할 수 있는데, 발신자와 수신자를 연결하는 미디어는 입력장치, 송신장치, 전송로, 수신 장치, 출력장치 등 다섯 가지 요소로 이루어진다. 그리고 사전적 의미의 정보는 상식적으로는 어떠한 것에 관한 알림, 판단을 내린다는지 행동을 하기 위하여 필요한 지식이라 할 수 있는 바, 일반적으로 형식, 표상, 신호, 기호, 발언, 전언(message)의 6가지의 정보가 있다. 한편, 법률적 의미의 정보를 규정한 『정보화촉진기본법』 제2조 제1호는 정보를 ‘자연인 또는 법인이 특정목적으로 위하여 광(光) 또는 전자적 방식으로 처리하여 부호·문자·음성·음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식’이라고 개념정의하고 있다.

35) 현행법상으로는 『정보화촉진기본법』이 제2조제2호에서 ‘정보화란 정보를 생산·유통 또는 활용하여 사회 각 분야의 활동을 가능하게 하거나 효율화를 도모하는 것’으로 정의하여 정보처리장치를 활용하여 정보를 처리함으로써 사회활동 전반의 비효율과 낭비를 제거하여 국가전체의 효율화를 도모하는 것으로 정보화를 정의하고 있다.

를 통하여 근본적인 변화를 받고 있는 사회가 바로 정보사회인 것이다. 환원하자면, 정보과학기술의 발전을 단순히 숭배하거나 두려워하는 게 아니라 도대체 우리가 어떠한 정보사회에서 살아야만 하는지를 규범적으로 검토해야만 한다. 그렇다면 법적으로 구성되는 정보질서는 현실적인 사회구조를 반영할 뿐만 아니라, 이들이 추구해야만 하는 ‘지침과 기준’을 제공해야 한다.<sup>36)</sup> 이와 관련되는 주요쟁점 가운데 하나가 바로 정보사회에서 개인정보보호의 문제이다.

정보사회에서 개인정보의 지배는 그 정보주체에게는 인격의 존엄과 자유의 불가결한 조건이 되지만, 동시에 정부나 기업에 의한 개인정보의 지배는 정보주체를 통제할 수 있는 권력의 기초가 된다. 디지털 정보혁명으로 촉발된, 이러한 개인정보의 지배를 둘러싼 자유와 권력의 이항대립은 이미 우리 사회에 두드러진 현상이 되고 있다. 그런데 이러한 대립 속에는 결코 무시할 수 없는 개인정보처리의 이익과 가치가 그 위세를 떨치고 있음을 부인하기 어렵다. 현대의 정부는 단순히 물질적 생산조건의 확보라는 기능을 넘어서서 복지나 사회정책 등 사회적 재생산조건을 보장하기 위한 기능을 담당하게 되었고, 이러한 기능을 효율적으로 수행하기 위해서는 무엇보다 개인정보의 수집과 처리가 불가결한 요소가 되고 있다. 특히 최근에는 정보기술의 활용을 통하여 대국민 고객지향성이라는 이념 하에 작고 효율적인 시민위주의 질 좋은 행정서비스를 제공한다고 하는 전자정부의 개념이 구체화되고 있다. 한편, 시장에 있어서도 기업에 의한 고객의 개인정보처리는 자원배분의 효율성을 극대화할 뿐만 아니라 소비자인 정보주체에게는 거부할 수 없을 정도의 달콤하고 편리한 이익을 안겨준다. 그러나 개인정보처리가 가져다 줄 이익과 가치 못지않게 그 위험성 또한 무시할 수 없을 정도로 커서 이른바 원형감옥(Panopticon), 즉 효과적

---

36) Friedrich Schoch, *Öffentlichrechtliche Rahmenbedingungen einer Informationsordnung*, VVD StRL 57, Walter De Gruyter Inc., 1998, S.213.

이고 효율적인 감시체계의 우려를 양산하고 있다. 이제 고도정보사회로 진입하는 길목에서 이러한 위험성을 최소화하면서 개인정보처리의 사회적 이익을 수용할 수 있는 규범적 척도를 찾아내는 것이 우리 사회의 시급하고도 절실한 과제가 되었다.

그런데 개인정보보호법제의 정비와 관련된 최근의 논의에서 민간부문의 경우에는 공공부문과는 달리 헌법과 사법에 의하여 인정되는 기본권 및 권리의 주체로서 그들의 활동을 위하여 개인정보를 수집·처리할 자유를 원칙적으로 갖고 있다는 특징이 충분히 반영되지 못하고 있다. 따라서 앞으로 민간부문과 관련되는 개인정보보호법제정비는 세심한 판단과 고찰을 필요로 한다.

이러한 측면에서 개인정보보호에 관한 법제정비에 있어서 개인정보를 활용하고 유통하는 산업적 수요를 반영하여 개인정보의 취급에 대한 정보주체의 권리를 설정할 필요성이 요청되며, 권익의 형량이 배제되어 정보주체의 정보자기결정권만을 우월적으로 보장하는 데 급급한 입법은 우리 헌법이 상정하고 있는 정보질서에 배치되기 때문에 시급히 시정되어야 할 것으로 사료된다. 이를 위하여 피규율분야의 구별을 전제로 해 개인정보취급자가 합법적이고 공정한 절차에 따라 정보주체가 인식할 수 있는 상태에서 개인정보를 취급할 수 있도록 입법적 대응에 있어 합리적 조율이 요청되어진다는 원론적 논의로써 이 글의 결론에 갈음하며, 이만 本稿를 맺을까 한다.

## 토 론 문

권 헌 영  
(한국정보사회진흥원 박사)

### □ 총괄의견

- 이민영 교수님의 발제는 개인정보보호법제 일반에 관한 논의와 더불어 CCTV관련 법제논의를 기본적인 틀로 설정하고 있어서 개인정보보호법제의 입법현황과 평가에 중요한 자료가 될 수 있을 것으로 생각합니다.
  - 특히, 국회에 제출되어 있는 각 법률안의 내용분석과 최근 개정된 공공기관의 개인정보보호에 관한 법률상의 CCTV 관련 조문을 상세히 분석하고 있어서 입법평가 세미나에 적합합니다.
- CCTV에 관한 규제의 문제는 실상 정보사회 전반의 일반적 현상으로 사적 부문에서도 심각한 피해를 가져올 수 있습니다. 이에 반하여 공공부문의 입법통제만이 이루어진 것은 입법평가에서 반드시 되짚어 봐야 할 문제라고 생각합니다.

### □ 개인정보법의 입법과정

- 현재 국회에 제출되어 있는 개인정보보호법은 대표적인 것이 3개인데 이는 모두 2003년 참여정부가 출범한 이후의 사회적 반향을 반영한 것입니다.
  - 2003년 5월 교육행정정보시스템(NEIS) 관련 사건이 불거지면서 전자정부 등 공공정보시스템에서의 개인정보관리 문제와 2005

년 이른바 연예인 X파일 사건 등을 거치면서 개인정보에 관한 행정체계를 독립적 보호기구로 개편하고 정보주체의 권한을 강화하는 기본법의 제정논의가 시작되었습니다.

- 이러한 논의는 사회적 관심의 상대적 저하와 더불어 정부조직의 다양한 의견이 조율되는 과정 등을 거치면서 입법화에 한계를 드러냈습니다.
  - 입법평가에 있어서는 이러한 입법이 논리와 사회적 요구에도 불구하고 이루어지지 못한 원인이 무엇인지를 밝히는 작업으로서 법학적 방법론과 정책분석 및 평가의 방법론이 병행되어야 한다고 생각합니다.
  - 즉, 내용적 평가는 법학적 방법론으로, 그리고 과정이나 형식 및 절차 등에 관한 평가는 다른 방법론으로 그 입법과정을 분석평가함으로써 타당성을 검증할 수 있을 것입니다.
  - 개인적 생각으로는, 의원입법으로 추진된 법률안에 대한 실질적 주인을 찾아주지 못한 점이 입법지연의 원인이라고 생각합니다.

#### □ CCTV관련 입법에 관한 기타 의견

- CCTV에 있어서 가장 중요한 것은 CCTV에 의하여 침해를 받는 정보주체입니다. 이 규제의 기본적인 틀은 정보주체의 알권리를 강화하는 것이며, CCTV로부터 획득된 정보의 관리자에 대해 그 책임성과 목적 구속성 및 오남용의 예방이 핵심이 될 것입니다.
  - 이를 위해서는 고지와 주체의 참여절차를 명확히 하고 구체적 참여권리(예를 들어, 열람청구권, 삭제청구권 등)을 인정하는 것입니다. 그렇지만, CCTV에서는 누가 그 청구권자인지를 바로 특정할 수 없는 문제가 있습니다. 이런 때 일부 지역이나 공간, 건물 등의 위치를 지정하여 CCTV의 설치목적과 설치주체 등을

제 1 주제 우리나라 개인정보보호 법제와 CCTV 관련규정의 현황·문제점 검토 및 평가

밝혀주도록 하여 정보주체의 알권리를 최소한 보장하는 노력이 필요합니다.

- o CCTV의 문제가 공법과 사법의 구별 문제에 있어서 다를 바가 없이 사회 전반에 활용되고 있으므로 이에 대한 동일한 규율이 필요할 것으로 생각합니다.

## 제 2 주제

### 미국 개인정보보호법제의 특징과 입법정책적 시사점

발 표 : 이창범 박사(한국정보보호진흥원)

토 론 : 정찬모 교수(인하대학교)

# 미국 개인정보보호법제의 특징과 입법정책적 시사점

이 창 범  
(한국정보보호진흥원 박사)

## 1. 개 요

개인의 자유와 개성을 중시해 온 미국은 일찍부터 프라이버시권의 개념을 인식·발견하고 프라이버시 침해를 보통법상의 불법행위로 보아 손해배상책임을 인정해 온 법적 전통을 가지고 있다. 이처럼 관례법 국가인 미국은 프라이버시권에 대해서 법원에서 보통법상의 권리로 인정해 왔기 때문에, 대륙법계 국가인 프랑스, 독일 등 다른 유럽 국가들과는 달리 포괄적이고 체계적인 개인정보 관련 법체계를 가지고 있지는 않다. 그래서 프라이버시보호 및 개인정보보호를 위해 영역별 접근방식을 택하여 세부적으로 개별입법을 제정·시행하고 있다. 입법체계상으로 포괄적인 개인정보보호법을 가지고 있지 않다는 점 외에도 미국은 개인정보에 대한 접근방법에 있어서도 다른 유럽 국가들과는 달리 경제적·기술적 측면에서 바라보는 경향이 있다. 이는 특히 민간부문에서 두드러지는데, 그 이유는 사적 자치의 원칙을 중시하여 정부의 간섭을 최소화한 자유로운 시장경제질서의 유지를 무엇보다도 중시하는 경제적 관점을 가지고 있기 때문이다. 따라서 민간부문에 대해서는 특별히 규제할 필요성이 인정되는 경우에만 법률을 제정할 뿐, 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하는 것이 정부가 담당할 부분으로 여기고 있다. 흔히 ‘자율규제(Self Regulation)’라고 부르는 이러한 접근방식은 개인정보를

인권의 하나로 인정하여 국가가 적극 관여하여 보호해야 한다고 보는 유럽의 입장과는 다른 태도이다.

이와 같이 미국은 개인정보보호를 위한 저인망식의 포괄적인 기본법 내지 일반법을 가지고 있지도 않으며, 되도록이면 시장경제질서에 직접 개입하는 제재조항을 내용으로 하는 법률을 입법화하지 않으려 하는 것이 일반적이다. 그러나 미국에 개인정보 또는 프라이버시 관련 법률이 전혀 없는 것은 아니다. 오히려 기본법 내지 일반법이 부재한 상황이기 때문에, 사회적 변화나 기술발달에 맞춰 공공·통신·금융·온라인 등 각 영역별로 많은 개인정보 관련 법률을 마련해 두고 있다. 또 최근에는 개인정보와 프라이버시를 보호하기 위한 일반법을 제정해야 한다는 목소리가 점점 높아지고 있다. 이하에서는 이러한 미국의 영역별 개인정보 관련 법률현황에 대해 살펴보고, 민간영역에서 소비자의 개인정보보호 기구로서의 역할을 일부 담당하는 연방거래위원회(FTC : Federal Trade Commission)에 대해서 살펴보도록 하겠다. 특히, 미국에서는 자율규제체계의 특성상, 정부에 의해 설립된 감독기구나 규제기구가 없어 민간 분쟁해결기구에 의한 개인정보피해구제제도가 발달하였다. 따라서 마지막으로 이러한 미국의 민간 소송외적 분쟁해결제도 현황과 그 성과 및 문제점에 대해 살펴보도록 하겠다.

## 2. 개인정보보호법제의 발전

### 가. 헌법과 판례

미국은 헌법상 명시적인 프라이버시권 규정을 가지고 있지는 않다. 그러나 미연방대법원(U.S. Supreme Court)은 사적 통신의 자유가 있음을 확고히 한 *Katz v. United States* 판결에서 제1차, 제3차, 제4차, 제5차 수정헌법을 간접적인 의미에서의 프라이버시권 조항으로 해석할 수 있

다고 밝힌 바 있다. 특히 법원은 제4차 수정헌법(Fourth Amendment)<sup>1)</sup>을 함축적인 의미의 프라이버시권 규정으로 볼 수 있다고 하면서, 개인이 ‘프라이버시에 대한 합리적 기대(reasonable expectation of privacy)’를 가진 영역에 있어서는 정부의 감시나 간섭으로부터 자유로울 권리를 가진다고 하였다.<sup>2)</sup> 이로 인해 미국에서는 헌법상 명시적인 개인의 프라이버시권에 대한 규정은 없지만, 다른 헌법상의 조항들을 통해 개인의 사적 자유가 존중되어야 할 프라이버시권을 가지는 것으로 해석되고 있다.<sup>3)</sup>

한편 미연방대법원은 일반적인 프라이버시권 외 개인정보와 관련한 정보프라이버시권(Right to information privacy)에 대해서는 명확한 언급을 하고 있지 않다.<sup>4)</sup> 다만, 법원은 Roe v. Wade 판결<sup>5)</sup>에서 “프라이버시에 대한 독립적인 권리나 영역은 존재한다. 이는 아이를 낳을 것인지에 대한 결정 또는 낙태를 할 것인지에 대한 결정과 같이 한 개인에게 중요한 영향을 끼치는 문제에 대하여 스스로 결정할 권리를

- 
- 1) 제4차 수정헌법은 “누구든지 불합리한 압수·수색으로부터 자신의 신체·주거·서신·물품을 안전하게 보호할 권리를 침해당하여서는 안 된다. 또한 압수·수색의 대상자, 물품, 장소를 명시한 법원의 결정과 같은 합당한 근거 없이는 영장이 발부되어서는 안 된다”라고 하여, 적정절차 원칙과 개인의 신체의 자유를 규정하고 있다.
  - 2) Katz v. United States, 389 U.S. 347, 351-52(1967). 동 판례에서 18 U.S.C. 1084에 위반하여 전화로 내기정보(wagering information)를 제공한 혐의로 기소된 원고 Katz는 FBI가 자신의 전화내용을 도청하기 위해 공중전화부스 밖에 도청장치를 부착한 것은 공중전화 이용자의 프라이버시권을 침해한 것이라고 주장하였다.
  - 3) 그러나 이러한 헌법상 근거는 기본적으로 국가, 즉 행정부 등 공권력에 대한 개인의 프라이버시 및 사적 자유의 보장을 의미하는 것으로 보아야 한다. 즉, 민간 기업이나 단체의 개인정보 침해행위로부터 개인의 자유를 보장하기 위한 헌법상 근거를 동 조항으로부터 바로 이끌어내기에는 다소 무리가 있다. Fred H. Cate, “The Changing Face of Privacy Protection in the European Union and the United States”, 33 Indiana Law Review 174, 203 (1999).
  - 4) Jonathan P. Cody, “Protecting Privacy Over the Internet : Has the Time Come to Abandon Self-Regulation?”, 48 Catholic University Law Review 1183, 1193 (1999) ; Domingo R. Tan, “Personal Privacy in the Information Age : Comparison of Internet Data Protection Regulations in the United States and the European Union”, 21 Loyola of Los Angeles International & Comparative Law Journal 661, 669 (1999).
  - 5) Roe v. Wade, 410 U.S. 113 (1973).

포함하는 개념이다”라고 하였고, Whalen v. Roe 판결<sup>6)</sup>에서는 “프라이버시 영역은 두 가지 유형의 이익(interest)을 포함한다. 첫 번째는 자신의 사적인 사항들이 공개되는 것을 회피할 수 있는 사적 이익이고, 두 번째는 특정한 중요결정을 내리는데 있어 독립성을 가지고 행할 수 있는 이익이다”라고 하여, 개인이 자신의 개인정보를 다른 간섭으로부터 자유로이 사적으로 관리하고 결정할 권리를 가지고 있음을 밝힌 바 있다.

이와 같이 법원은 개인의 프라이버시 또는 개인정보에 대한 권리를 확인하고 보호하고 있는 경향을 보이고 있고, 이는 보통법 체계를 가진 미국에서 하나의 판례법으로 인정되고 있다.

## 나. 연방 및 주 제정법

미국은 각 영역별로 개인정보 또는 프라이버시와 관련한 많은 법률을 제정하여 시행하고 있다. 이러한 제정법은 헌법이나 판례법에서 보장하는 권리보호를 해당 영역에서 더욱 명확하게 규정하여 원칙을 확고히 할 수 있다는 점에서 의미가 있다. 미국의 대표적인 개인정보관련 입법현황을 살펴보면 아래 [표]와 같다.

[표] 미국의 개인정보관련 법제현황

구분	개인정보 관련법
공공부문	·프라이버시법(Privacy Act, 1974) ·정보공개법(Freedom of Information Act, 1974) ·프라이버시보호법(Privacy Protection Act, 1980) ·컴퓨터에의한정보조합과프라이버시보호에관한법률 (Computer Matching and Privacy Protection Act, 1988) ·전자정부법(E-Government Act, 2002) ·운전자 프라이버시보호법

6) Whalen v. Roe, 429 U.S. 589 (1977). 또한, 법원은 Whalen v. Roe 판결 방론(傍論, dictum)에서 개인을 직접 식별할 수 있는 번호나 식별인자를 컴퓨터 데이터베이스로 수집하는 것은 개인의 자유나 권리를 침해할 위험이 함축되어 있다고 밝히고 있다.

제 2 주제 미국 개인정보보호법제의 특징과 입법정책적 시사점

	(Driver's Privacy Protection Act, 1994)
금융부문	·공정신용평가법(Fair Credit Reporting Act, 1970) ·공정·정확한 신용거래법 (Fair and Accurate Credit Transactions Act of 2003) ·금융프라이버시권에 관한 법률 (Right to Financial Privacy Act, 1978) ·금융현대화법(The Financial Modernization Act of 1999) ·그램리치법(Gramm-Leach-Bliley Act)
통신부문	·케이블통신정책법 (Cable Communications Policy Act, 1984) ·통신프라이버시법(Telecommunications Privacy Act) ·전자통신프라이버시법 (Electronic Communications Privacy Act, 1986) ·전기통신법(Telecommunications Act, 1996)
교육부문	·가족의 교육권 및 프라이버시에 관한 법률 (Family Educational Rights and Privacy Act, 1974)
의료부문	·건강보험책임법(HIPPA) (Health Insurance Portability and Accountability Act)
비디오감시	·비디오프라이버시보호법 (Video Privacy Protection Act, 1988)
근로자정보	·근로자기록보호법 (Employee Polygraph Protection Act, 1988) ·미국장애인법(Americans with Disabilities Act) ·가족 및 질병 휴가법(Family and Medical Leave Act)
아동의 개인정보	·아동온라인프라이버시보호법 (Child Online Privacy Protection Act, 1998)
기타	·컴퓨터사기·남용법 (Computer Fraud and Abuse Act of 1986)

이와 같이 미국은 금융, 의료, 교육, 통신, 비디오감시, 근로자정보 등 각 영역별로 별도의 제정법을 마련하여 개인의 프라이버시 및 개인정보를 보호하고 있다. 연방뿐만 아니라 대다수 주에서도 연방 프라이버시 보호 법제에 유사한 법률을 제정하여 시행하고 있다.

## 다. 세이프하버 원칙

한편 제정법이나 관례법 외에도 미국에서 개인정보보호를 위한 중요한 역할을 하는 것으로 ‘세이프하버 원칙(Safe Harbor Principles)’을 들 수 있다. 1998년 10월 25일부터 발효된 EU지침은 동 규정에서와 같은 적절한 수준의 개인정보보호 체계를 갖추지 못한 제3국으로의 개인정보 국외이전을 엄격히 제한하도록 하였는데, 이와 관련하여 미국은 자국의 항공사, 은행, 여행사 및 다국적 기업(Multinational Corporations)의 피해를 방지하기 위해 동 원칙을 마련하고 유럽연합과의 협상 끝에 2000년 7월 합의하여 시행하고 있다.

세이프하버 원칙은 기본적으로 유럽연합 회원국과의 국제교류와 관련하여 유럽 시민들의 개인정보를 전달받아 처리하는 미국 기업이 EU지침에서 규정한 ‘적정성(adequacy)’을 갖추고 있는지 여부를 판단하기 위한 기준이다. 이처럼 동 원칙은 국제조약의 성격을 가진 것이 아니고 개인정보 취급의 적정성 여부를 판단한다는 특정한 목적을 위해 합의된 사항이기 때문에, 미국에서 법적 효력을 가지고 전면적으로 시행되는 것은 아니다. 따라서 세이프하버 원칙에 참가할 것인지 여부는 전적으로 미국 기업의 자발적 의사에 달려 있다. 그러나 실질적으로 동 원칙에 참가할 경우 유럽위원회(European Commission)가 개인정보취급의 적정성을 확인하여 주는 효과를 가지므로 유럽연합 회원국과 개별적으로 별도 협의와 논의를 하여야 할 필요가 없고, 적정성이 추정되기 때문에 특별한 사안이 없는 한 계속해서 개인정보를 교류할 수 있다. 따라서 현재 미국에서는 이러한 세이프하버 원칙의 장점과 이점으로 인해 다수의 기업체가 참여하고 있다.<sup>7)</sup>

---

7) 2003년 12월 현재 433개의 기업이 세이프하버 원칙에 자발적으로 참여하고 있다. (<http://www.export.gov/safeharbor> 참조)

세이프하버 원칙에 참여하려는 기업은 반드시 동 원칙의 내용을 준수할 것임을 공표하여야 한다. 공표방법은 미국 상무부(Department of Commerce)에 서면확인서(Self certification letters)를 제출하고 자사의 프라이버시정책에 위와 같은 사실을 공개하는 것이다.<sup>8)</sup>

세이프하버 원칙은 고지, 선택, 제공, 접근, 안전성, 정보 무결성, 이행의 총 7개 원칙으로 구성되어 있다. 동 원칙의 세부적인 내용은 아래와 같다.

[표] 세이프하버 7원칙

구분	원칙의 내용
고지(Notice)	개인정보의 수집·이용목적, 용도, 정보를 제공하는 제3자의 유형, 문제 제기 또는 권리행사시 접근방법 등에 대하여 고지
선택(Choice)	개인정보가 제3자에게 제공되는지 여부 및 최초의 수집목적과 양립할 수 없는 다른 목적으로 정보가 사용될 것인지 여부에 대해 옵트 아웃 방식의 선택권을 제공(민감한 정보에 대해서는 옵트 인 방식의 선택권 제공)
제공 (Onward Transfer)	개인정보의 위탁처리 등과 같이 제3자에게 개인정보를 제공할 경우, 당사자에게 고지함은 물론 선택권을 부여하여야 함
접근(Access)	정보주체의 접근권과 정정요구권을 보장
안전성(Security)	개인정보를 손실, 오용, 권한없는 접근, 변경, 파괴로부터 보호하기 위한 합리적 예방조치를 취하여야 함
정보 무결성 (Data Integration)	당초의 수집 및 이용목적에 부합한 개인정보의 이용, 정확성·완전성·최신성의 확보
이행(Enforcement)	원칙의 준수를 담보할 수 있는 구제수단과 분쟁해결절차, 제재수단이 확보되어야 함

8) 미 상무부는 웹사이트(<http://www.export.gov>)를 통해 세이프하버 원칙에 참여하는 기업체들 목록은 물론 기업체가 제출한 서면 자기확인서를 모두 공개하고 있다.

세이프하버 원칙에 참여한 기업은 의무사항 중 하나로, 소비자의 이의제기와 분쟁을 적절히 해결하고 자사의 원칙 준수를 담보할 수 있는 대안적인 분쟁해결제도를 갖추어야 한다. 따라서 이러한 대안적 분쟁해결절차와 방법을 통해 소비자는 사업자의 원칙 불이행으로부터 입은 피해를 구제받을 수 있다. 그러나 민간차원의 자율규제 프로그램을 통해서도 해결되지 않은 경우에는 연방거래위원회와 미국 교통부(Department of Transportation)가 개입하여 위반 사업자에게 보다 강력한 제재를 부과할 수 있다.<sup>9)</sup> 또한 지속적으로 원칙을 위반하는 사업자의 경우에는 상무부의 세이프하버 참여기업 목록에서 삭제될 수도 있다.

### 3. 연방 주요 제정법의 내용

이하에서는 앞서 살펴본 미국의 개인정보 관련입법 중에서 공공부문과 민간부문의 개인정보보호에서 있어 중요한 역할을 하고 있는 몇몇 법률의 주요 내용을 살펴보도록 하겠다.

#### 가. 프라이버시법

먼저, 공공부문의 대표적인 개인정보 관련법령은 「프라이버시법」<sup>10)</sup>이다. 1972년 닉슨 대통령이 민주당 선거대책본부를 도청하려다 발각된 사건과 연루되어 사임하게 된 ‘워터게이트 사건’은 미국 전 사회에 커다란 영향을 끼쳤는데, 프라이버시법도 이러한 워터게이트 사건의 영향으로 제정된 법률이다. 동법은 미연방정부를 비롯한 연방공공기관

---

9) 유럽연합은 연방거래위원회와 교통부를 사업자의 불공정 사기행위를 제재하고, 사업자가 세이프하버 원칙을 이행하지 않아 피해를 입은 소비자의 이의제기를 조사하여 구제할 수 있는 권한이 있는 기관으로 인정하고 있다. (“SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTEMNT OF COMMERCE ON JULY 21, 2000”, <http://www.export.gov/safeharbor> 참조)

10) 5 U.S.C. § 552a.

이 공정한 정보사용의 원칙에 맞추어 개인정보를 처리하고 정보주체의 권리를 보장하도록 규정하고 있다. 세부적인 내용은 1973년의 ‘공정정보관행규약(Code of Fair Information Practices)’<sup>11)</sup>을 바탕으로 하여 제정되었으며, 정보주체의 열람·정정요구권, 필요한 범위 내에서의 정보수집원칙, 어떠한 정보가 수집되었는지에 대한 고지의무, 정보공유의 원칙적 금지 등의 내용을 담고 있다. 그러나 동법은 공공기관이 본래의 수집목적과 양립될 수 있는 ‘일상적인 이용(routine use)’을 위해 해당 개인정보를 공개할 수 있도록 하고 있으며, 특정한 공공기관의 경우 정보 정확성이나 기타 법적 의무로부터 면제되도록 하고 있어 실효성을 가지고 있지 못하다는 비판을 받고 있다.<sup>12)</sup>

## 나. 금융프라이버시보호

금융부문에는『공정신용평가법』<sup>13)</sup>과『금융현대화법』<sup>14)</sup>의 두 가지 대표적인 개인정보 관련 법률이 적용되고 있다. 공정신용평가법은 신용

---

11) 동 규약은 미국 보건교육복지부(Department of Health, Education and Welfare)의 자문단에 의해 처음 만들어진 것으로, 기록보유시스템에서의 개인프라이버시 보호를 위한 기본원칙을 규정하고 있다. 동 규약은 미국의 프라이버시 보호법, 개인정보보호법은 물론 자율규제 접근방식에도 폭넓게 수용되었다. 동 규약에서 제시하고 있는 공정한 개인정보 이용원칙은 다음과 같다. 첫째, 개인정보의 기록보유관행은 비밀로 하여서는 안 된다. 둘째, 개인은 자신에 관한 어떠한 정보가 기록되어 있는지, 어떻게 그러한 정보가 공개되고 있는지를 확인하고 이를 정정할 수 있어야 한다. 셋째, 개인은 자신에 관한 식별정보의 기록을 정정하거나 수정할 수 있어야 한다. 넷째, 개인은 자신에 관한 정보가 본래의 목적과 관련 없는 다른 목적을 위해 공개되거나 제공되는 것을 제한할 수 있어야 한다. 다섯째, 식별가능한 개인정보의 기록을 만들고 유지하며 이용하거나 유포하는 단체는 반드시 그러한 정보의 남용을 방지하기 위한 필요한 주의를 다하여야 하며, 의도된 목적을 위한 정보의 신뢰성을 확보하여야 한다. (Advisory Committee on Automated Personal Data Systems, “Records, Computers and the Rights of Citizens”, Department of Health, Education and Welfare, 1973)

12) EPIC & PI, supra note 138, <http://www.privacyinternational.org/survey/phr2003/countries/unitedstates.htm>

13) 15 U.S.C. § 1681 et seq.

14) 15 U.S.C. §§ 6801, et seq.

평가기관(CRA : Credit Reporting Agency)에 의한 개인정보의 오·남용을 막고 개인정보를 보호하기 위해 1970년 제정된 대표적인 개인신용정보보호법이다. 동법의 핵심 내용은 신용평가기관이 개인신용정보의 비밀성과 정확성을 보호하기 위한 ‘합리적 절차(reasonable procedures)’를 준수할 것을 강제하는 것이다. 동법은 이러한 합리적 절차를 판단하기 위한 기준으로서, 개인의 정보접근권, 개인정보 보안, 개인정보의 과기, 필요한 사항에 대한 고지, 정보주체의 동의, 신용평가기관의 책임성에 관한 내용을 포함하는 공정한 정보관행체계를 규정하고 있는데, 이에 의하면, 신용평가기관은 은행, 신용카드회사, 사용자(회사), 임대업자 등의 사업자가 개인의 신용을 평가하기 위해서만 정보를 사용할 것이라는 합리적인 믿음이 있는 경우가 아닌 한 개인정보를 제공하여서는 안 된다. 한편 2003년 12월 4일 미국의 부시 대통령이 『공정하고 정확한 신용거래에 관한 법률(Fair and Accurate Credit Transactions Act of 2003)』에 서명함으로써, 2004년 1월 1일 만료되는 공정신용평가법의 관련 조항이 무기한 연장되었다. 동 법률은 ID도용을 제재하는 주 정부 법령이 연방정부의 관계 법령 범위에서 제정되도록 함으로써 주마다 법률이 다르게 만들어지는 것을 막고 있다.<sup>15)</sup>

한편 ‘Gramm-Leach-Bliley Act(GLBA)’라고도 불리는 금융현대화법은 금융기관에 의해 보유되는 고객의 금융정보를 보호하기 위해 제정된 법률이다. 따라서 은행, 증권회사, 보험회사와 같은 금융기관 및 대부업 등 모든 대출서비스 제공회사, 중개업, 자금전송 또는 보관업, 금융자문이나 신용컨설팅을 제공하는 회사, 채권추심업 등과 같은 기타 금융상품 또는 서비스를 제공하는 모든 회사에 적용된다. 동법은 세 가지 주요한 내용을 담고 있는데, 금융프라이버시에 관한 원칙, 세이프가드 원칙, 프리텍스팅(pretexting) 규정이 바로 그것이다. 금융프라이버시 원칙은 금융기관에 의한 고객의 개인금융정보의 수집 및 이용을

---

15) 연합뉴스, “부시, 개인 신용보호법률 서명”, 2003. 12. 5일 기사 참조.

규제하는 것으로, 금융기관으로부터 금융정보를 제공받는 기업(금융기관 여부를 불문)에도 적용된다. 따라서 이에 의하면, 금융기관은 소비자에게 회사의 개인금융정보에 대한 정책을 고지할 의무가 있고, 소비자 개인정보를 이해관계가 없는 제3자에게 제공하여 정보를 공유하기 전에 반드시 소비자에게 이 사실을 알리고 반대할 권리를 부여하여야 한다. 셰이프가드 원칙은 모든 금융기관이 소비자의 정보를 보호하기 위한 안전장치를 고안하고 시행하며 유지할 것을 요구하는 것이다. 이 원칙은 소비자로부터 직접 정보를 수집하는 금융기관 뿐 아니라 다른 금융기관으로부터 고객 정보를 받는 신용평가회사 등의 금융기관에도 적용된다. 프리텍스팅 규정은 소비자를 속여서 개인의 금융정보를 취득하는 개인 또는 기업으로부터 소비자를 보호하기 위한 규정이다.<sup>16)</sup>

#### 다. 통신프라이버시보호

통신부문에 적용되는 대표적인 법률로는 「케이블통신정책법」<sup>17)</sup>과 「전자통신프라이버시법」<sup>18)</sup>이 있다. 1984년 미 의회는 케이블TV 기술의 진보, 특히 양방향 케이블 시스템의 개발은 부당한 개인정보의 수집을 불러올 위험에 대비하여 케이블통신정책법을 제정하기에 이르렀다. 동법은 케이블을 통해 서비스를 제공하는 사업자에게 여러 가지 의무를 부과하고 있다. 첫째, 동법은 케이블통신회사에게 적어도 1년에 한 번씩 고객에게 자사의 개인정보 수집 및 보유현황에 대해 고지토록 강제하여, 고객이 사업자의 개인정보 수집 및 이용을 제한할 수 있는 기회를 가질 수 있도록 하고 있다. 케이블통신회사가 고지하여야 할 내용으로는 수집목적, 수집되는 정보의 내용, 개인정보의 공개가 예상되

---

16) “*In Brief : The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*” ; “*Financial Privacy : The Gramm-Leach Bliley Act*” (미연방거래위원회 웹사이트, [www.ftc.gov](http://www.ftc.gov) 참조)

17) 47 U.S.C. § 551.

18) 18 U.S.C. § 2701 et seq.

는 경우, 보유기간, 개인정보 열람요구 절차 등에 관한 사항이다. 또한 동법에 의하면 고객에 관한 정보는 고객의 사전 동의없이 이용되거나 제3자에게 제공될 수 없다. 단, 서비스의 제공에 관한 합법적인 영업 활동과정에서 이루어진 정보의 공개는 예외이다.<sup>19)</sup>

한편 전자통신프라이버시법은 전자기록에 관한 정부의 접근절차 및 방법에 대하여 통제함으로써, 전자기록의 비밀성을 보호하는 규칙을 확립하고 있다. 1986년 제정된 동법은 수색영장이나 수신자의 동의 없이 서신을 개봉하는 것을 금지하는 법률<sup>20)</sup> 및 당사자 동의 없는 전화, 데이터 전송, 라디오 통신의 차단 또는 도청장치의 사용을 금지하는 법률<sup>21)</sup>의 통신프라이버시보호의 내용을 전자메일이나 기타 컴퓨터를 통한 데이터 전송과 같은 새로운 통신분야에 확장시킨다는 의미를 가진다. 특히 동법은 저장된 ‘음성메일(voice mail)’ 및 이메일에 대한 권한없는 접근이나 이용을 금지하고, 이러한 저장된 이메일 등의 내용을 해당 전자통신서비스제공자가 외부에 공개하지 못하도록 금지하고 있다. 이러한 금지규정을 위반한 자는 형사상 제재를 받음은 물론, 고의적이거나 의도적인 위반행위로 인해 피해를 입은 자는 민사소송을 통해 금지명령 등의 피해구제를 청구하거나 금전적 배상을 요구할 수 있다.<sup>22)</sup>

## 라. 교육프라이버시보호

1974년 제정된『가족의교육권및프라이버시에관한법률(FERPA)』<sup>23)</sup>은 ‘버클리 수정법(Buckley Amendment)’으로도 잘 알려져 있는 연방법으로

19) Gerald Spindler/Fritjof Börner(Edit.), supra note 134, p. 748.

20) 39 U.S.C. § 3623.

21) 18 U.S.C. §§ 2510 et seq. ; 47 U.S.C. § 605.

22) Ronald L. Plesser/Sheldon Krantz, “Privacy and Related Issues”, 『Internet and Online Law』(Kent D. Stuckey with Contributing Authors)』, Law Journal Press, 2000, § 5.02, pp. 5-8~9 참조.

23) 20 U.S.C. § 1232g.

서, 학생의 교육정보에 대하여 학부모와 학생의 자기정보결정권을 강화하고 프라이버시의 관점에서 교육정보를 보호하기 위해 제정된 법이다. 동법은 학교 등의 교육기관이 연방기금을 교부받지 못하게 되는 몇 가지 사항을 적시하고 이에 대한 감독권을 교육부에 부과함으로써 학생 및 학부모의 교육정보에 대한 권리를 보장하고 있다. 즉, 연방기금의 교부조건으로 정보처리자인 학교 등의 교육기관이 교육정보를 수집·이용·보유·공개 등 처리하는 과정에 있어 지켜야할 몇 가지 의무를 부과하고 있기 때문에, 연방기금을 계속해서 교부받고자 하는 교육기관은 동법에서 규정하고 있는 의무를 준수하여야 한다. 동법에 의하면, 학생 또는 학부모는 학교 등의 교육기관이 보유하고 있는 자신 또는 아동의 교육정보에 대해 조사·심사하고 이를 통해 잘못된 내용이 있으면 정정을 요청할 수 있으며 나아가 개인식별정보(personally identifiable information)의 공개를 중지토록 요구하는 등의 권리를 행사할 수 있다. 또한 학교 등의 교육기관은 ‘교육기록 내 개인식별정보’를 학생 또는 학부모의 서면 동의없이 공개할 수 없으며, 학교가 유지·관리하고 있는 교육정보에 대해 자격 있는 학생 및 학부모에게 고지하여야 한다.

#### 마. 아동프라이버시보호

『아동온라인프라이버시보호법(COPPA)』<sup>24)</sup>은 13세 미만 아동의 개인 정보를 온라인으로 수집하는 행위를 엄격히 제한하고 있는 법률이다. 동법의 적용을 받는 웹사이트는 13세 이하의 아동과 직접적으로 관련된 서비스를 제공하는 상업적 웹사이트 운영자 뿐 아니라 모든 일반인을 대상으로 한 서비스를 제공하더라도 13세 미만의 아동으로부터 개인정보를 수집하는 모든 웹사이트이다.

24) 15 U.S.C. § 6501 et seq.

동법의 적용을 받는 웹사이트는 반드시 홈페이지에 프라이버시정책을 고지하고 개인정보 수집하는 페이지에 프라이버시 정책이 링크되도록 하여야 한다. 또한 웹사이트의 정보수집정책에 대해 부모에게 고지하고 아동으로부터 개인정보를 수집하기 전 부모의 명확한 동의를 구하여야 한다. 또한 접근권을 보장하여 부모에게 아동의 개인정보가 제3자에게 제공되도록 허락할 것인지 여부를 선택하거나 개인정보를 삭제할 기회를 보장하여야 한다. 또한 인터넷 웹사이트 운영자는 인터넷 게임이나 설문조사 등 기타 활동에 아동이 참여할 때 그러한 활동에 참여하는 데 합리적으로 필요한 수준 이상으로 더 많은 개인정보를 제공하여서는 안 되며, 아동으로부터 수집한 개인정보의 비밀성, 안전성, 무결성을 유지하기 위한 노력을 기울여야 한다.<sup>25)</sup>

#### 바. 비디오대여정보보호

『비디오프라이버시보호법』<sup>26)</sup>은 비디오테이프 판매사업자 또는 대여사업자가 개인정보를 포함한 비디오 대여기록을 고객의 동의 또는 법원의 승인 없이 제3자에게 제공하는 것을 금지함으로써 상업 비디오 테이프 이용자 또는 구매자의 프라이버시권을 보호하고 있다. 동법은 다음과 같은 경우에는 위와 같은 개인정보를 포함한 비디오 대여기록 정보의 공개를 일부 허용하고 있다.

- 당해 비디오를 빌려준 소비자에게 공개하는 경우
- 소비자의 서면동의를 있는 경우
- 연방형사법원 영장 및 관할 주법원 영장, 대배심 영장(grand jury subpoena) 또는 특별한 지침에 따른 법원 명령에 의한 공개의 경우

---

25) FTC, “Children’s Privacy : The Children’s Online Privacy Protection Act”, <http://www.ftc.gov>

26) 18 U.S.C. § 2710.

- 제3자에게 비디오 대여자의 이름과 주소만 공개된다고 할 때, 이에 대해 해당 소비자가 반대할 기회를 가졌던 경우
- 정보의 공개가 채권추심 등과 같이 비디오 대여사업자의 일상적인 영업행위 과정에서 부수적으로 발생하는 것일 경우
- 민사법원의 명령에 의한 경우

동법에 의하면, 비디오 대여사업자가 동법에 위반하였다고 주장하는 소비자는 언제든지 민사소송을 통해 손해배상을 청구할 수 있다. 또한 불법적으로 획득된 비디오 대여기록 정보는 모든 법원 소송에서 증거로 사용될 수 없으며, 이는 일정기간 안에 파기되어야 한다.<sup>27)</sup>

### 사. 영상프라이버시보호

미국은 영국 등에 비해 CCTV를 이용한 감시가 보편화되어 있지 않다. 그러나 최근 들어 미국도 점차 CCTV의 보급이 확대되는 추세이고 수사당국이 CCTV 기술 개발을 지원하기까지 하고 있다. CCTV 기술 개발은 주로 CCTV와 얼굴인식 기술의 결합을 통해 공공장소에서 효과적으로 테러분자 등을 색출해 내기 위한 것이다. 경찰 등 수사기관에서는 CCTV를 범죄 예방 및 수사 목적으로 이용하지만 미야 등 실종자 찾기도 활용되고 있다. 미국에서는 CCTV를 이용한 감시행위를 규제하는 특별한 법령은 없다. 오히려 1990년 메릴랜드 주 대법원이 어린이 성범죄 사건에서 CCTV로 촬영된 어린이의 증언을 증거로 인정하는 것이 계기가 되어 어린이 성범죄 사건에서 CCTV 촬영이 관행화되고 있다.

CCTV를 규제하는 법이 없다고 해서 CCTV를 이용한 감시가 무한정 허용되는 것은 아니다. 앞서서도 언급한 것처럼 법원은 제4차 수정헌

---

27) Marc Rotenberg, "The Privacy Law Sourcebook 2002 - United States Law, International Law, and Recent Developments", Electronic Privacy Information Center, 2002, p. 220.

법(Fourth Amendment)을 함축적인 의미의 프라이버시권 규정으로 해석하고 있으며, 개인이 ‘프라이버시에 대한 합리적 기대(reasonable expectation of privacy)’를 가진 영역에 있어서는 정부의 감시나 간섭으로부터 자유로울 권리를 가진다. 다만, 법원은 일반적으로 사람들이 공공장소(public)에 있는 경우에는 공공장소에 있다는 그 자체가 이미 다른 사람에 의한 관찰을 인정한 것이므로 프라이버시에 대한 합리적인 기대는 없는 것으로 보고 있다.<sup>28)</sup> 그러므로 교통카메라, 방범카메라 등과 같이 공개된 장소에 설치된 카메라에 대해서는 프라이버시권을 주장하기 힘들다. 이에 따라 CCTV에 의해서 촬영된 영상정보의 보관 및 저장에 대해서 논란이 있으나 이에 대해 아직 뚜렷한 원칙은 확립되어 있지 않다.

#### 4. 연방 개인정보보호기구

미국은 개인정보 보호를 위한 연방 차원의 별도의 전담기구를 두고 있지는 않다. 다만, 공공부문과 민간부문에서 각각 예산관리국(OMB : The Office of Management and Budget)과 연방거래위원회(FTC : The Federal Trade Commission)가 개인정보보호기구로서의 역할을 담당하고 있을 뿐이다.

먼저 공공부문에 있어서는 예산관리국<sup>29)</sup>이 『1974년 프라이버시법』에 따라 연방정부의 프라이버시 또는 개인정보보호 정책을 정립하는

---

28) Bickel, Robert D., *Legal Issues Related to Silent Video Surveillance*, Alexandria, VA: Security Industry Association, 1999.([http://securitygateway.com/E/E3\\_4.html](http://securitygateway.com/E/E3_4.html))

29) 예산관리국은 1921년 창설된 예산처(BOB : Bureau of Budget)를 1970년 재정비환기구로서 대통령의 예산집행 및 관리, 기타 정책의 수립 및 시행을 지원한다. 1999년에는 연방정부기관의 프라이버시에 대한 접근태도를 조화시키고자 예산관리국 내 최고 프라이버시 자문역(Chief Counselor for Privacy)이 임명되기도 하였는데, 이는 단순한 자문기능을 하는 제한적인 권한만 가지고 있었다. 그러나 부시 행정부가 들어서면서는 프라이버시 자문역 제도는 폐지되었다. (EPIC & PI, *supra* note 138, <http://www.privacyinternational.org/survey/phr2003/countries/unitedstates.htm>)

역할을 맡고 있다. 그러나 예산관리국은 우리나라의 기획예산처와 같이 예산편성과 운용 등 국가재정운영 전반에 관한 정책을 수립하고 집행하는 역할을 하는 기구인 바, 프라이버시 보호와 관련하여서도 예산관리차원에서만 제한적인 역할을 맡고 있을 뿐이다. 한편 민간부문에 있어서는 연방거래위원회가 아동의 온라인 프라이버시, 소비자신용정보, 공정한 거래관행과 관련하여 개인정보 또는 프라이버시를 보호하는 법률을 집행하고 준수여부를 감독할 권한을 부여받아 행사하고 있다.<sup>30)</sup>

이와 같이 미국에는 포괄적인 개인정보보호기구는 없다. 다만, 민간부문에 있어서는 연방거래위원회가 시장감시 및 소비자보호의 일환으로 소비자 프라이버시보호의 기능을 담당하고 있을 뿐이다.

### 가. FTC의 설립 및 구성

연방거래위원회(FTC)는 1914년에 설립된 기구로서, 자유롭고 공정한 거래의 확보를 위해 활동하는 독립기구이다. FTC는 본래 주로 대통령 또는 의회에 대하여 관련입법에 관한 자문을 행하고 소비자에게 필요한 다양한 정보를 제공하려는 목적에서 설립된 기구이나, 점차 공정한 사업관행의 확보와 실행에 초점을 맞추어 활동하게 되면서 그 권한이 더욱 확대되었다.

FTC는 대통령에 의해 임명되는 5인의 위원으로 구성되며, 동 위원의 임기는 7년이다. FTC의 조직은 총 4개 부서로 나뉜다. 일반자문부서

---

30) 주 차원에서는 개인정보보호 전담기구를 두는 주도 있다. 예컨대, 캘리포니아는 2000년 제정된 ‘California Business and Professions Code sections 350-352’에 의거하여 주 최초로 2001년에 프라이버시 보호청(The Office of Privacy Protection)을 설립하였다. 2008년 1월 1일부터는 법률(Senate Bill 90) 개정으로 기존의 프라이버시보호청(The California Office of Privacy Protection)과 정보보안청(the California State Information Security Office)을 하나로 묶어, 통합 정보보호기구인 ‘캘리포니아 정보보안 및 프라이버시 보호청’(the Office of Information Security and Privacy Protection)이 출범하게 된다. <http://www.privacy.ca.gov/>참조.

(The Office of the General Counsel), 경쟁국(The Bureau of Competition), 경제담당국(The Bureau of Economics), 소비자보호국(The Bureau of Consumer Protection)이 그것이다. 일반자문부서는 위원회에 기관의 관찰과 권한에 대한 정보를 제공하고 자문관은 위원회의 법적 대리인으로 활동한다. 경쟁국은 사업자간 과도한 경쟁을 억제하여 잘못된 업무 관행을 방지토록 하고 있다. 경제담당국은 FTC의 행위가 경제에 미치는 영향을 연구한다. 마지막으로 소비자보호국은 불공정하고 부당한 사업관행으로부터 소비자를 보호하는 역할을 담당하고 있다. 현재 FTC는 약 1,000여명의 직원이 있으며, 이들 중 500명 이상은 변호사이고 20명 정도는 경제학자이다.

#### 나. FTC의 개인정보보호 활동

FTC의 주요 임무는 과도한 제한을 가하지 않은 상태에서 시장기능이 효율적으로 작동되고 적절한 경쟁관계를 유지하도록 함으로써 불공정한 사업관행으로부터 자국의 소비자를 보호하는 것이다. 이는 개인정보와 관련해서도 마찬가지이다. 따라서 FTC는 개인정보 및 프라이버시의 중요성을 사업자와 소비자에게 알리는 역할을 하고 있고, 더 나아가 범위반행위나 불공정한 사업관행에 대해 모니터링을 하거나 조사권을 행사한다. 또한 BBBOnLine이나 TRUSTe와 같은 자율규제 차원의 민간 프라이버시 단체로부터 법률이나 가이드라인을 준수하지 않는 사업자에 대한 보고(referral)를 받아 실질적인 제재조치를 취하기도 한다.

FTC가 잘못된 개인정보 처리관행을 가진 사업자를 제재하고 소비자의 개인정보를 보호하기 위한 근거조항으로 삼고 있는 것은 「연방거래위원회법(Federal Commission Act)」<sup>31)</sup> 제5조이다. 동 조항은 ‘영리활동

---

31) 15 U.S.C. §§ 41~58.

과정에서의 불공정하거나 사기적인 행위 또는 관행(unfair or deceptive acts or practices in or affecting commerce)'을 금지하고 있다. 따라서 만약 웹사이트 운영자가 자사 웹사이트에 고지된 프라이버시 정책을 준수하지 않았거나 적용을 받는 일체의 자율규제 차원의 가이드라인을 이행하지 않은 경우에는 사기적 수단 중 하나인 허위사실의 공언(misrepresentation)에 해당되어 FTC의 제재를 받을 수 있다.<sup>32)</sup> 또한 아동과 관련된 개인정보의 수집 및 이용관행 또는 금융기록이나 의료기록과 같은 민감한 정보의 이용관행이 터무니없이 불공정한 경우에도 FTC는 동법 제5조를 적용하여 범위반행위로 보고 있다.<sup>33)</sup> 이는 FTC가 개인정보보호와 관련하여 「금융현대화법」, 「공정신용평가법」, 「아동온라인프라이버시보호법」 등에 대해 관장하고 있기 때문이다. 금융현대화법에 따라, 위원회는 금융 프라이버시의 중요성을 알리는 규범 및 금융기관에서의 개인정보의 행정적·기술적·물리적 안전조치를 확보하는 규범을 실행하고 있으며, 공정신용보고법 및 아동온라인프라이버시보호법에 따라 소비자를 보호하는 각종 역할을 맡고 있다.

32) 실제로 FTC는 GeoCities社가 운영하는 인터넷 웹사이트(www.geocities.com)가 성인과 아동의 개인정보를 자사가 어떻게 이용하고 있는지에 대해 정확히 고지하지 않았으므로써 허위사실을 공언하여 사기적 방법으로 개인정보를 수집·이용하였으므로 연방거래위원회법 제5조를 위반하였다고 결정한 바 있다. 동 사건에서 FTC는 GeoCities에게 개인정보의 수집 및 이용목적, 정보를 제공받는 제3자, 소비자의 열람권과 정정권의 행사방법, 아동의 개인정보에 대한 부모의 동의권 및 통제권 보장에 관한 사항을 명확하고도 눈에 떨 수 있도록 고지하고, 이전에 부당한 방법으로 수집하여 제3자에게 제공한 개인정보는 명시적 동의를 구하지 못하는 한 삭제할 것을 명령하였다. (GeoCities, Docket No. C-3849, Final Order 1999. 2. 12, <http://www.ftc.gov/os/1999/02/9823015cmp.htm> 참조)

33) FTC는 전화 등을 통해 사기적인 방법으로 고객으로부터 직접 금융정보를 얻은 뒤, 이를 인터넷 웹사이트를 통해 판매한 정보브로커를 피고로 하여 1999년 4월 21일 민사소송을 제기한 바 있다. 동 사건은 2000년 6월 사기적 수법을 통한 금융정보의 수집행위를 더 이상 하지 않고 지금까지의 불법적인 행위로 인해 얻은 이익에 상당하는 200,000달러의 지급정지판결(suspended monetary judgement)을 내리는 것으로 합의되었다.

한편 FTC는 앞서 잠시 언급한 것처럼, 세이프하버 원칙에 참여한 기업이 동 원칙을 준수하지 않고 자율규제 프로그램의 결정도 무시하는 경우 개입하여 제재를 가할 수 있는 권한이 있다. 만약 기업이 세이프하버 원칙에 참여할 경우, 동 원칙을 준수하겠다는 내용을 자사 프라이버시정책에 공표함은 물론 세이프하버 자율규제 프로그램에도 동참하게 되는 것이기 때문에, 기업이 스스로 밝힌 프라이버시정책 또는 프라이버시규약을 준수하지 않은 경우와 마찬가지로 취급되어 연방거래위원회법 제5조에 위반하게 된다. 이 경우 FTC는 법원을 통해 금지명령을 구하거나 위반행위에 대해 1일 최고 12,000달러의 벌금을 구할 수도 있다.

이 외에도 FTC는 스팸메일 규제, 광고성 전화에 대해 소비자의 선택권을 부여하기 위한 광고성 전화거부 등록부(National Do Not Call Registry)의 운영, 신분도용 규제 등의 활동을 펼치고 있으며, 관할 영역에 대해 공정한 거래관행 규칙<sup>34)</sup>을 제정하여 사업자들이 이를 준수토록 하는 역할을 맡고 있다.

## 5. 개인정보 피해구제제도

미국에서 잘못된 관행이나 부주의한 개인정보의 취급 또는 고의적인 개인정보 오·남용으로 인해 피해를 입은 자가 그러한 피해를 구제받기 위한 방법은 크게 세 가지로 볼 수 있다. 가장 대표적인 방법은 역시 소송을 통한 피해구제방법이다. 앞서도 언급하였지만, 미국 판례는 프라이버시 침해를 불법행위로 인정하여 피해자가 입은 경제적·정신적 손해에 대한 배상청구를 인정함은 물론 징벌적 손해배상 청구나 침해행위금지청구도 함께 인정하고 있기 때문에, 소송에 의하

34) FTC는 1998년 의회에 제출한 보고서에서 고지·인식, 선택·동의, 접근·참여, 무결성·안전성, 집행·구제라는 다섯 가지 핵심적인 공정정보관행 원칙을 제시한 바 있다. (FTC, "Privacy Online : A Report to Congress", 1998. 6, pp. 7~11)

는 것이 가장 확실한 피해구제 방법 중 하나가 되고 있다.

그러나 이러한 소송을 통한 피해구제제도 외에도, 미국에서는 민간 분야의 소송외적 분쟁해결제도가 법원의 피해구제 역할을 보조하는 중요한 기능을 맡고 있다. 특히 BBBOnLine의 개인정보분쟁해결제도는 그 대표적인 예라고 할 수 있을 것이다. 또한, 개인정보보호기구 차원에서도 미국 연방거래위원회가 소비자의 프라이버시 보호와 관련하여 피해구제의 역할을 일부 담당하고 있기도 하다. 이하에서는 전형적인 피해구제제도인 소송을 제외한 민간분야의 소송외적 분쟁해결제도와 연방거래위원회의 역할을 살펴보기로 한다.

### 가. 민간분쟁해결제도

다른 사람들과의 다툼이나 분쟁, 특히 송사(訟事)에 휘말리는 것을 꺼리는 우리나라의 풍토와는 달리, 미국 사람들은 분쟁이 발생하였을 경우 적극적으로 자신의 권익을 주장하여 관철시키려는 경향이 강하다. 따라서 미국에서는 자연스럽게 소송제도 뿐 아니라 분쟁을 해결하기 위한 다양한 소송외적 해결제도가 발달해왔다. 또한 소송외적 분쟁해결제도의 발달 배경에는 업계의 자율규제를 장려하고 촉진하는 미국의 접근방식도 빠뜨릴 수 없다. 미국에서는 사업자 단체가 자율적으로 독립·비영리 민간단체를 설립하여 실행규약이나 원칙을 마련하고, 이러한 기준에 맞춰 소비자가 신뢰할 수 있는 사업자에게 신뢰마크(Trustmark)를 부여하는 자율규제가 활성화되어 있다. 이러한 신뢰마크 체계는 당해 마크를 제공하는 곳의 분쟁해결제도를 사업자가 반드시 이용하도록 하기 때문에, 실질적으로 사업자가 실행규약을 준수하고 분쟁해결절차에 적극적으로 참여하며 그 결과에 순응할 수 있도록 하는 실효성을 가지게 된다.<sup>35)</sup>

35) Julia Hörnle, "Online Dispute Resolution in Business to Consumer E-commerce Transactions", Journal of Information Law & Technology, <http://elj.warwick.ac.uk/jilt/02-2/hornle.html>.

이러한 민간단체를 통한 소송외적 분쟁해결제도는 개인정보와 관련한 분쟁의 해결에 있어서도 중요한 역할을 담당하고 있다. 그 중에서도 특히 개인정보보호와 관련한 미국의 민간분쟁해결제도에 대해서 말하자면, BBBOnline을 언급하지 않을 수 없다.<sup>36)</sup> BBBOnline의 소송외적 분쟁해결제도는 기본적으로 온라인상 소비자와 사업자의 신뢰구축과 개인정보보호라는 목적으로 마련된 ‘프라이버시 씰 프로그램(Privacy Seal Program)’<sup>37)</sup>의 일환으로 운영되고 있다. 따라서 동 프로그램에 참여하고 있는 인터넷서비스제공자가 프라이버시 인증마크를 표시할 수 있는 자격을 부여받기 위해서는 BBBOnline의 분쟁해결절차에 참여하여야 할 의무가 있다. 이러한 소송외적 분쟁해결제도는 주로 온라인을 통한 분쟁해결방법(ODR : Online Dispute Resolution)으로 운영되고 있다.

이하에서는 BBBOnline의 이러한 온라인 분쟁해결절차와 방법을 자세하게 살펴볼 수 있을 것이다.<sup>38)</sup> 먼저 BBBOnline의 개인정보분쟁해결 절차도는 아래와 같다.

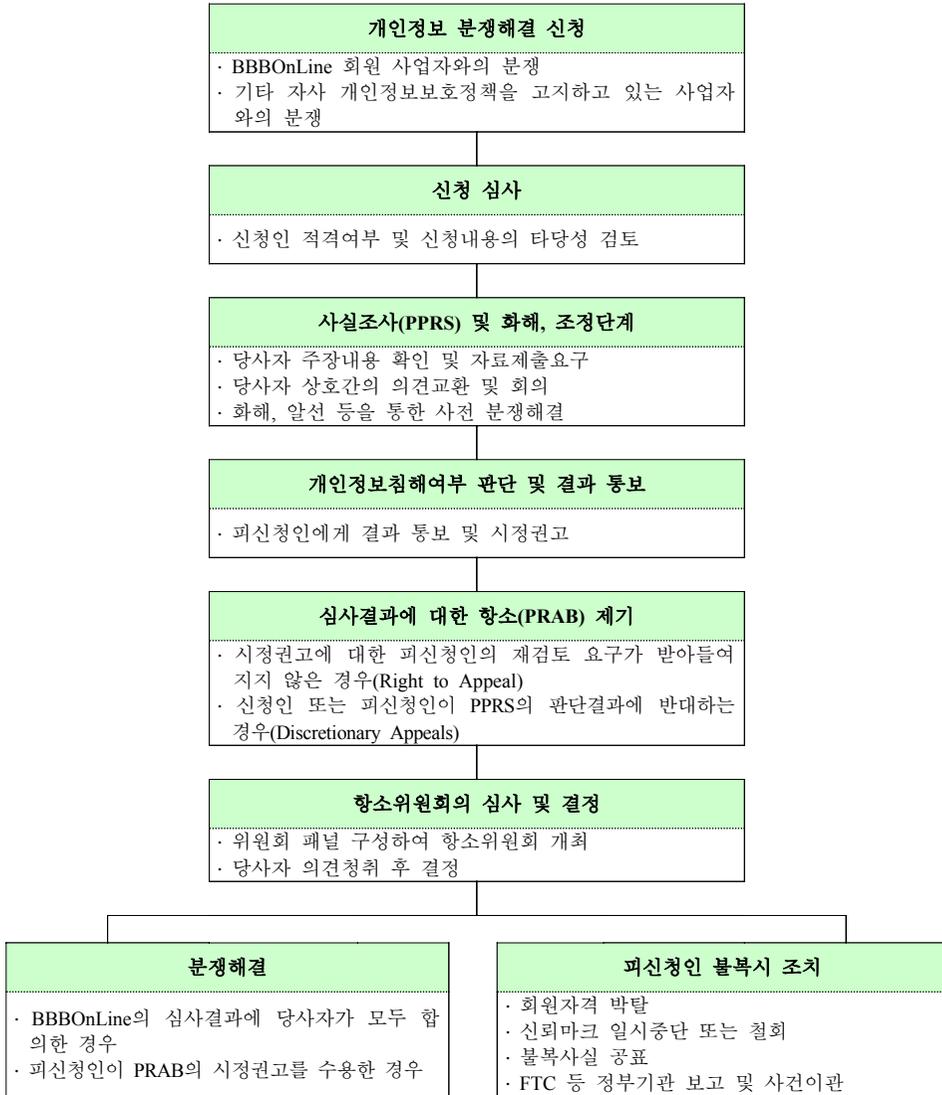
---

36) BBBOnline은 미국의 대표적인 소송외 분쟁해결단체인 ‘The Council of Better Business Bureaus(이하 ‘CBBB’라 한다)’의 분야별 산하조직 중 하나인데, CBBB는 1912년 설립되어 오늘날에 이른 미국의 대표적인 소송외적 분쟁해결단체이다. 현재 전미 지역에 약 250,000여개의 사업자들이 회원으로 가입하고 있는데, CBBB는 각 지역별로 ‘Better Business Bureau(BBB)’를 설립하여 네트워크화함으로써 전국적인 BBB 시스템을 구축하고 있다. (이은선, “온라인을 통한 소송외적 분쟁해결에 관한 고찰”, 개인정보연구, 제2권제1호, 2003. 7, 291~292면 참조) 한편, BBBOnline 외 TRUSTe도 민간단체로서 프라이버시에 대한 신뢰마크를 부여하고 필요할 경우 분쟁조정을 해주는 메커니즘을 갖추고 있으나, 개인정보와 관련한 분쟁의 해결은 BBBOnline의 역할이 더 크다.

37) ‘프라이버시 씰 프로그램’이란 일정한 프라이버시보호 기준을 설정하여 BBB 시스템에 가입한 인터넷 사이트 운영자가 이 기준에 충족할 경우 이를 증명해주는 프라이버시 마크를 표시하여 소비자와 사업자간의 신뢰를 높이는 제도이다. 2003년 12월 현재 626개의 웹사이트에서 프라이버시 마크를 부여받은 상태이다. (BBBOL 웹사이트, <http://www.bbbonline.org/privacy> 참조)

38) BBBOnline의 분쟁해결절차 및 방법은 BBBOnline, “BBBOnline Privacy Program, Dispute Resolution Process Procedures - Privacy Policy Review Service and Privacy Review Appeals Board”, 1999. 2. 11, <http://www.bbbonline.org/privacy/dr.pdf> 참조.

[그림] BBBOOnline의 피해구제 절차도



위와 같이 BBBOOnline의 개인정보분쟁해결 절차는 분쟁해결신청, 사실조사, 심사 및 판단, 항소, 최종결정의 단계로 이어진다. 이를 단계별로 자세히 살펴보면 다음과 같다. 먼저, BBBOOnline의 프라이머시

프로그램 가입회원인 사업자가 BBBOOnLine이 제정한 프라이버시 가이드라인을 위반하여 소비자가 피해를 입었거나, BBBOOnLine의 회원이 아니더라도 개인정보를 수집하여 이용하는 조직 또는 개인이 자신의 개인정보보호정책을 고지하고 있는데 이를 위반하여 정보주체가 피해를 입은 경우, 이들은 BBBOOnLine에 분쟁해결을 신청할 수 있다. BBBOOnLine은 사건 신청을 접수받으면 우선 신청인의 적격여부와 신청내용의 타당성을 검토한다.<sup>39)</sup> 이러한 과정을 거쳐 사실조사가 필요하다고 판단되는 사건은 ‘프라이버시 정책심사(PPRS : Privacy Policy Review Service)’ 단계로 이관된다. 이 단계는 주로 신청인과 피신청인의 주장내용을 확인하고 증거자료를 제출받아 사실관계를 명확히 하는데 초점이 맞춰져 있다. 또한 양 당사자가 서로의 주장과 의견을 확실히 인식할 수 있도록 하여 분쟁이 원만히 해결될 수 있도록 하고 있다. 따라서 일방 당사자가 제출한 답변자료는 다른 당사자에게 제공되어 서로의 의견을 교환하는 과정을 거치며, 필요한 경우 당사자의 합의를 기초로 회의를 개최하기도 한다.

또한 BBBOOnLine은 사실조사가 완료되면 그 결과 및 권고내용을 피신청인에게 제출하여 의견을 듣게 된다. BBBOOnLine은 필요한 경우 피신청인에 시정을 요구하는 내용을 권고할 수 있는데, 이 경우 피신청인은 시정권고의 재검토를 요청할 수 있고 받아들여지지 않을 때는 ‘프라이버시 심사 항소 위원회(PRAB : Privacy Review Appeals Board)’에 항소할 수 있다. 항소 단계는 프라이버시 정책심사 단계에서 이루어진 결정 내용에 반대하는 신청인 또는 피신청인이 모두 신청할 수

---

39) 이에 의하면, ①금전적인 손해배상만을 요구하는 경우, ②사기 또는 기타 법규범의 위반만을 주장하는 경우, ③피신청인이 BBBOOnLine의 회원이 아니면서 다른 적절한 분쟁해결절차를 제공하고 있는 프라이버시 프로그램에 가입하고 있는 경우, ④사전법원조치(previous court action)나 중재, 기타 분쟁해결절차에 의해 이미 분쟁이 해결된 경우, ⑤현재 소송 계류 중인 사건, ⑥다른 분쟁해결방법을 이용하기로 당사자간 사전 합의한 경우에는 신청내용의 적격성이 없는 것으로 판단되어 상담으로 종결된다.

있는데, 여기에는 재량적 항소(Discretionary Appeals)와 항소권(Right to Appeal)의 두 가지 유형이 있다.

[표] BBBOOnLine의 항소 유형

구 분	재량적 항소	항소권
주 체	BBBOOnLine의 프라이버시 프로그램 회원을 대상으로 이의를 제기한 신청인 및 그 피신청인	BBBOOnLine의 프라이버시 프로그램 회원인 피신청인
대 상	프라이버시 정책심사의 결정내용	시정조치가 포함된 프라이버시 정책심사의 결정내용
허용 결정	항소 허용여부를 프라이버시심사 항소 위원회가 결정	항소 허용여부 결정 불필요

BBBOOnLine은 항소가 허용될 경우, 항소위원회의 패널을 구성하여 당사자 의견청취(hearing)를 거친 후 신속하게 결정을 내린다. 그러나 만약 피신청인이 항소위원회의 시정조치 결정에도 불복할 경우, BBBOOnLine은 ①회원자격의 박탈, ②신뢰마크의 일시 중단 또는 철회, ③ 피신청인의 불복사실 공표, ④정부기관에 사건 이관 등과 같은 조치를 취하여 분쟁해결의 실효성을 담보할 수 있다.<sup>40)</sup>

일반적으로 BBBOOnLine에 제기되는 개인정보 관련 사건은 메일링 리스트 또는 마케팅 목적을 위해 구축한 데이터베이스 상에서의 개인정보 삭제요구에 대한 무응답, 개인정보에 대한 접근요청 거절 등 주로 정보주체의 권리행사에 대한 피신청인의 거부나 미조치에 관한 내용이다. 올 9월까지 BBBOOnLine에는 총 1,032건의 사건이 접수되었다. 이 중 단순 상담 및 질의가 516건이었고, 신청 부적격으로 종결된 사건이 485건으로 다수를 차지하고 있다. 그 외는 적격성 여부를 결정

40) BBB/CBBB/BBBOOnLine, “Protecting Consumers in Cross-Border Transactions : a Comprehensive Model for Alternative Dispute Resolution”, CBBB, 2000, p. 12.

중인 사건이 15건, 신청적격성이 인정되어 진행 중인 사건이 8건, 결정전 합의가 이루어진 사건이 8건이다.<sup>41)</sup>

### 나. FTC의 개인정보피해구제 절차 및 방법<sup>42)</sup>

FTC는 앞서 살펴본 것처럼 연방거래위원회법 및 아동온라인프라이버시보호법 등에 의해 사업자가 소비자의 개인정보를 부당하게 취급하는 것을 조사하고 감독하며 제재조치를 취하거나 법원에 소송을 제기하는 역할을 맡고 있다. FTC가 소비자 피해구제를 위해 적극적인 분쟁해결절차를 제공하여 당사자간 합의를 도출하는 것은 아니지만, 이와 같은 과정을 통해 궁극적으로는 개인정보침해로 인해 피해를 입은 소비자를 구제할 수 있는 장치를 마련하고 있다고 볼 수 있다.

FTC는 인터넷 웹사이트 등을 통해 일반 국민으로부터 직접 불공정한 개인정보 취급행위에 대한 이의제기를 접수받으며, 때로 BBBOOnline과 같은 민간 프라이버시단체로부터 법규 위반이나 자율규제 차원의 가이드라인 불이행에 대한 보고를 받기도 한다. 또한 세이프하버 원칙과 관련하여서는 유럽연합 회원국의 개인정보보호기구로부터 사건을 이관받는 경우도 있으며, 필요한 경우 직접 관련 분야에 대해 실태조사를 함으로써 위법사실을 발견하여 문제삼기도 한다.

이렇게 이의제기가 접수되면 FTC는 연방위원회법 제3조에 의거하여 임무수행에 필요한 각종 질의(inquiry)를 행할 수 있고 관련된 정보를 수집할 수 있으며 때때로 관할 영역에 대해 조사(investigate)할 수 있는 권한을 가진다. 특히 FTC의 소비자보호국(Bureau of Consumer Protection)은 개인정보침해 등 소비자보호와 관련된 사건을 조사하기 위해 ‘민사적

41) BBBOOnline 웹사이트(<http://www.bbbonline.org/privacy/dr/2003q3.asp>) 참조.

42) FTC의 소비자 보호를 위한 피해구제절차 및 방법에 대해서는 FTC, “*A Brief Overview of the Federal Trade Commission's Investigative and Law enforcement Authority*”, 2002. 9, <http://www.ftc.gov/ogc/brfovrwv.htm> 참조.

조사요구권(CIDs : civil investigative demands)<sup>43)</sup>을 행사할 수 있다. FTC는 민사적 조사요구권 행사를 통해 사건과 관련된 증거서류를 제출 받고 구두 증언을 얻을 수 있으며, 당사자에게 질문에 대한 서면 응답 또는 보고서를 제출토록 요구할 수 있다.<sup>44)</sup> 그러나 이러한 FTC의 조사 명령이 부당하다고 생각하는 사업자나 기타 조직은 지명위원(designated Commissioner)에게 취소청구(petition to quash)를 제출하여 이의를 제기할 수 있고, 지명위원의 결정에 대해서는 다시 전원위원회에서 이의를 제기할 수 있다.<sup>45)</sup> 그러나 당사자가 취소청구를 하지 않은 채 조사권에 불응한 경우, FTC는 해당 지역의 관할 법원에 이행청구를 할 수 있고 법원은 당사자에게 조사에 응하도록 요구하는 명령을 내릴 수 있다. 법원의 이러한 이행명령(enforcement order)을 따르지 않을 경우에는 법정모독죄로 벌금이 부과될 수 있다.<sup>46)</sup>

이와 같은 과정을 거쳐 사실조사를 마친 결과, 위법행위가 있다고 믿을 만한 근거가 발견된 경우, FTC는 법규 이행을 위한 조치를 취할 수 있다. 여기에는 행정절차상의 이행확보를 위한 조치와 사법절차상의 이행명령의 두 가지가 있다.

먼저 행정절차상의 조치를 살펴보면, FTC는 사업자의 위법사실이 있다고 믿을 만한 근거가 발견되면 바로 행정제재를 내리지 않고 사

43) 1980년 이전에는 소비자보호국도 조사를 위한 영장(subpoena)을 이용하였는데, 연방거래위원회진흥법(FTC Improvements Act of 1980)의 제정에 따라 새롭게 추가된 조항으로 인해 현재는 민사적 조사요구권만을 행사할 수 있게 되었다. 영장조사는 주로 경쟁국(Bureau of Competition)에서 행하는 조사방법이며, 영장을 통한 조사와 민사적 조사요구권(CIDs)에 의한 방법은 조사 범위에서도 다소 차이가 있다.

44) 15 U.S.C. § 57b-1(c)(1).

45) 연방거래위원회 규칙 제2.7조(16 C.F.R. § 2.7).

46) 사실조사 방법으로는 이 외에도 특정 관할영역에 해당되는 사업자나 기타 조직에 대하여 정보수집 등을 위해 질문서를 송부하여 서면답변이나 보고를 받는 방법이 있는데, 이는 매년 정기적으로 또는 특별한 경우 요구할 수 있다(연방거래위원회법 제6(b)조). 이러한 조사방법은 주로 광범위한 실태조사를 하거나 연구를 행하는 데 유용하며, 주로 개별 사건과 관련해서는 민사적 조사요구권이 활용된다.

건을 검토하여, 해당 사업자에게 위법사실과 그에 따른 사업자 부담 조치(charges)를 규정한 문제제기 서류를 제출한다. 사업자가 FTC의 이러한 부담조치를 자발적으로 수용하기로 한 경우, 양 당사자는 위 부담조치를 FTC의 최종명령(final order)으로 보고 위법사실에 대한 모든 소권(訴權)을 포기한다는 내용의 합의를 할 수 있다. 일종의 시정권고를 통한 당사자 합의로써 업계의 자율규제를 중시하는 FTC의 입장을 확인할 수 있는 부분이다. 그러나 사업자가 FTC의 부담조치를 따르지 않을 경우에는 심판절차(trial-type proceeding)를 통해 행정심판관(ALJ : administrative law judge)이 그 당부를 결정한다. 행정심판관은 심문을 통해 사실조사 내용과 범위만 여부에 대한 ‘약식 결정(initial decision)’을 내리고 FTC에 대하여 문제제기를 중단하거나 취소할 것을 명령할 수 있고 또 그 반대일 수도 있다. 행정심판관의 결정은 전원위원회에 회부되어 재심사될 수 있으며 전원위원회는 최종 결정과 명령을 내리게 되는데, 만약 사업자가 전원위원회의 결정에 불복하는 경우에는 관할 항소법원에 이의를 제기할 수 있다. 항소법원이 FTC의 최종결정을 확정하는 경우, 법원은 FTC의 부담조치 이행명령을 내릴 수 있다. 사업자가 항소법원의 결정에도 불복할 때에는 연방 대법원에 소를 제기하여야 한다.

FTC가 내리는 명령은 사업자의 특별한 이의제기가 없어 전원위원회 또는 법원에서 심사중인 경우가 아닌 한, 명령이 내려진 후 60일이 지나면 최종적인 명령으로 결정되어 당사자를 구속하게 된다. 따라서 만약 사업자가 최종명령을 위반할 경우에는 개개 위반행위마다 최고 11,000달러의 민사 범칙금(civil penalty)이 부과될 수 있다. 이러한 과태료의 액수는 FTC가 제기하는 명령 이행청구소송에서 법원이 결정하며, 법원은 또한 ‘강제 금지명령’ 및 적절하다고 판단되는

‘기타 형평에 맞는 추가적인 구제조치명령’을 내릴 수 있다.<sup>47)</sup> 또한 FTC는 명령에 대한 사법심사가 모두 완료된 이후 추가적으로, 관할 지방법원에 행정소송절차에서 문제가 된 사업자의 불법행위로 인해 소비자가 입은 피해의 구제를 위한 민사상 손해배상청구를 할 수 있다.

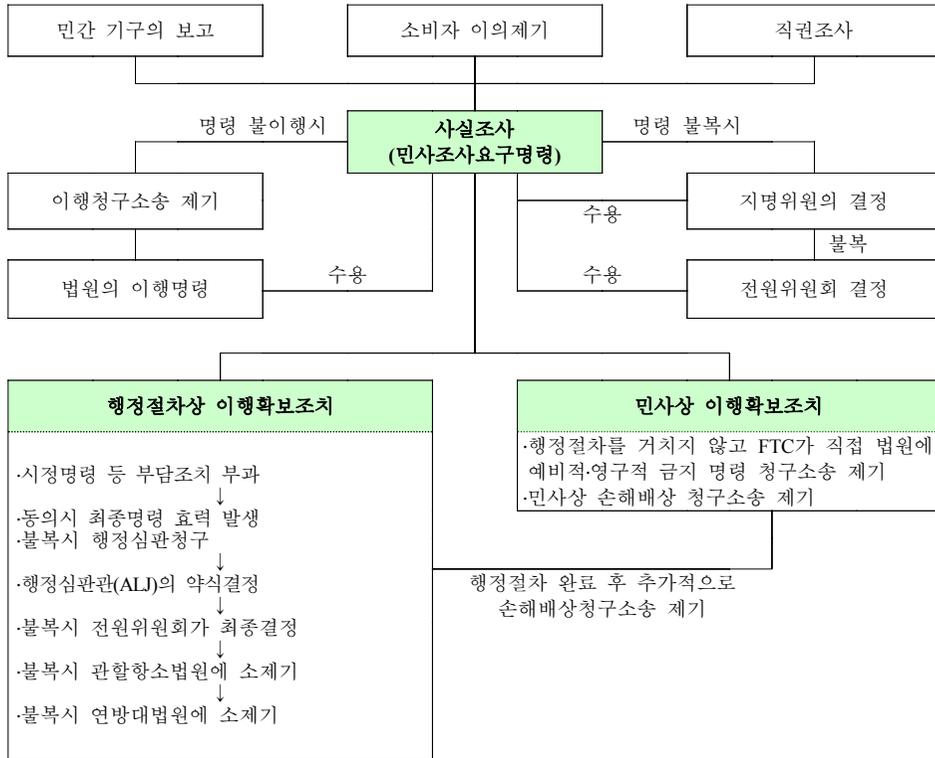
이러한 행정적 피해구제제도는 FTC가 사업자와의 협의를 통해 사전 합의에 이를 수 있는 기회를 줄 수 있고, 또한 사실관계나 법적인 문제가 복잡한 사안은 보다 철저히 조사할 수 있다는 장점이 있다. 그러나 계속해서 항소가 이어지게 되면 신속한 피해구제가 어렵다는 단점 또한 가지고 있다. 이에 최근에 FTC는 이러한 행정절차를 거치지 않고 바로 민사소송을 통해 예비적·영구적 금지명령(preliminary and permanent injunctions) 청구소송을 제기하는 방법도 적극 활용하고 있다. FTC는 사업자가 ‘위법행위를 하였거나 또는 위법행위를 하려고 한다고 믿을 만한 이유’가 있는 경우, FTC의 행정절차를 통해 해당 행위가 불법하다는 최종적인 결론을 내리지 않았다 하더라도 법원에 그 위법성을 주장하여 금지청구를 할 수 있다. 또한 ‘적절한 경우’에는 영구적인 금지청구를 제기할 수도 있다.<sup>48)</sup> 특히, 복잡한 행정절차를 거치지 않고 바로 민사소송을 제기하는 경우 위와 같은 금지청구 뿐 아니라 소비자가 입은 피해에 대한 금전적인 구제조치도 한꺼번에 해결할 수 있다는 점에서 최근 FTC는 소비자보호와 관련된 여러 문제들에 이러한 피해구제절차를 선호하고 있다.

---

47) 연방거래위원회법 제5(1)조.

48) 연방거래위원회법 제13(b)조.

[ 그림 ] FTC의 피해구제 절차도



## 6. 맺음말 : 입법정책적 시사점

세계 각국의 개인정보보호 법제는 크게 유럽식과 미국식으로 나뉘고 있다. 유럽식 모델은 하나의 법률에 의하여 공공부문과 민간부문에 원칙적으로 동일한 개인정보보호 기준과 원칙을 적용하는 반면, 미국식 모델은 공공부문과 민간부문을 분리하여 각기 다른 법률에 의하여 각기 다른 개인정보보호 기준과 방식으로 접근한다. 유럽식 모델의 경우 통상 개인정보보호에 관한 하나의 일반법이 존재하기 때문에 개별

법의 제정은 최소한에 그친다. 또한 독립된 개인정보보호 전담기구가 있어 개인정보보호 일반법은 물론 개별법 내에 산재해 있는 개인정보 보호와 관련된 규정의 집행까지도 통상 전담기구가 책임을 진다. 미국식 모델의 경우 앞에서 살펴본 바와 같이 공공부문에 대해서는 프라이버시 보호에 관한 일반법이라고 할 수 있는 프라이버시법(Privacy Act)과 그 밖의 개별법을 통해서 엄격히 규율하지만, 민간부문에 대해서는 법률을 통한 규제보다 시장의 자율규제에 맡기는 편이다.

유럽식 모델과 미국식 모델은 각기 그들 나라의 고유한 법률문화에 의해서 영향을 받은 것이고 경제·사회적 특징을 반영한 것이기 때문에 장단점을 수평적으로 비교하는 것은 바람직스럽지 못하다. 흔히 미국식 모델을 찬성하는 사람들-주로 사업자 및 사업자들의 이익을 대변하는 사람들-은 미국식 모델이 시장 친화적이면서도 정보자산(개인정보)의 효율적 활용에 기여한다는 점을 강조한다. 또한 문화적으로 프라이버시에 매우 민감한 나라가 개인정보 보호를 위한 법률을 제정하지 않고 사업자들의 자율에 맡기고 있는 것은 그만한 이유가 있다고 주장한다. 그러면서 유럽식 모델은 개인정보를 많이 다루는 공공기관과 개인정보의 취급규모가 작은 중소기업 및 비영리단체를 동일하게 취급함으로써 사회·경제적 효율성을 떨어뜨리고 법 위반자만 양산시켜 법률집행의 실효성을 떨어뜨릴 것이라고 주장한다. 따라서 미국식 모델을 따르던지 유럽식 모델을 따르려면 사회 전 분야가 준수해야 할 최소한의 합의된 원칙만을 규율해야 한다고 주장한다. 반면 유럽식 모델을 찬성하는 사람들-주로 시민운동가 및 그 지지자들-은 미국식 모델은 개인정보를 보호할 수 없는 사각지대가 많은 반면, 유럽식 모델은 사회 전 분야를 대상으로 획일적인 규율방식을 채택하기 때문에 법률의 보호를 못 받는 사각지대가 없고 개인정보 보호에 관한 통일된 원칙을 적용함으로써 법의 실효성이 강화될 것이라고 주장한다.

이러한 분석과 주장들은 나름대로 근거와 설득력을 가지고 있는 것이 사실이지만, 개인정보보호법을 그것만 떼어놓고 보는데서 나오는 일종의 착시현상이라고 할 수 있다. 미국은 개인정보보호법이 없는 것이 아니라 무수한 개별법이 존재하며 이른바 유럽식 입법 모델을 추구하는 시각에서 지적하는 사각지대는 판례법에 의하여 보충되고 있다. 제정법은 없어도 법은 존재한다. 또한, 미국은 개인정보 및 프라이버시 보호 분야에도 징벌배상(punitive damage)제도와 집단소송(class action)제도가 적용되기 때문에 큰 기업이든 작은 회사든 자율규제가 충분히 작동할 수 있는 환경이다. 시장에 맡겨져 있다고 해서 기업들이 마음대로 개인정보를 수집·이용할 수 있는 것이 아니며, ‘결함제조물책임’에서와 같이 언제라도 집단소송을 제기당하거나 징벌배상을 선고받을 수 있기 때문에 더욱 조심하고 불안할 수밖에 없다. 따라서 집단소송이나 징벌배상이 인정되지 않고 있는 우리나라와 같은 환경에서 미국식 입법 모델을 따를 경우 법을 지키는 선량한 기업들만 희생될 수 있고 악질적인 사업자들은 제대로 규제하지 못하는 풍선효과만을 조장할 우려가 있다. 한편, 유럽식 모델의 경우에도 공공부문과 민간부문을 획일적인 원칙으로 규율하거나 모든 민간부분에 획일적인 개인정보보호 원칙을 적용하는 것은 아니다. 구체적인 사항에 따라 원칙의 부분적인 수정·보호 수준을 강화하거나 완화하는 것이 인정되고 있다.

따라서 개인정보보호법은 이미 국제적으로 확인된 원칙을 수용해야 하며, 중소기업 또는 비영리단체 등의 보호를 이유로 미리 개인정보보호법의 전체적인 보호 수준을 낮추어서 기본적인 원칙만 선언하는 ‘기본법’이 되어서는 안 되며, 반대로 의료·금융 정보와 같이 프라이버시 침해 위험이 큰 분야만을 상정해서 국제수준보다 지나치게 엄격한 개인정보보호법이 제정되어서도 안 될 것이다. 국제적인 개인정보

보호 원칙 아래, 구체적인 사정에 따라 지침이나 개별법에 의해서 최소한의 예외를 인정-강화든 완화든-해 줄 수 있는 탄력적인 개인정보 보호법이 되어야 할 것이다.

## 토 론 문

정 찬 모  
(인하대학교 법학과 교수)

### 1. 총 평

- o 사회 및 개인의 안전과 프라이버시 보호의 이익이 충돌하는 중요한 법이론적 이슈이자 구체적인 CCTV 설치, 운용기준이 필요하다는 측면에서 현실적인 사안이다.
- o 전체적인 프로그램 구성과 관련하여 영국은 CCTV를 가장 먼저 광범위하게 사용한 국가로서 영국의 법제 및 논의를 고찰할 필요가 있다. 특히
  - 1998 Data Protection Act이 CCTV에 어떻게 적용되는가
  - Information Commissioner에의 CCTV 시스템 등록의무
  - Durant vs. FSA를 위시한 관련 판례가 주목될 가치가 있다.
- o CCTV 기술발전으로 앵글이 고정된 CCTV 화면을 여러 대 놓고 사람이 감시하는 것은 이미 과거사가 되고 있으며 이미 컴퓨터로 상호 연결된 가변식 앵글의 CCTV로 바뀌고 있다. 컴퓨터와의 연결은 녹화물의 사후 검색뿐만 아니라, 사전에 감시요청정보를 저장하여 이와 일치하는 대상이 화면에 잡히는 경우 CCTV가 이를 추적, 녹화하고 경보를 울리는 시스템을 가능케 한다.

## 2. 이창법박사 발표문에 대한 코멘트

- o 미국 개인정보보호법제의 특징을 포괄적이면서도 이해하기 쉽게 정리하고 있으며 국내관련 법제의 개선에 큰 방향성을 제시하는 논문이다.
- o 다음은 추가검토가 요구되는 사항이다.
  - CCTV로 녹화한 파일에 대하여 정보주체가 열람권 혹은 동의권 철회를 행사한다면 어떻게 되는가? CCTV 관련 문제에 개인정보 보호 법리를 적용하는 것이 곤란한 점이 있음을 보여준다. 프라이버시(사생활보호)의 법리를 원용하는 것이 더 적절해 보인다. 이참에 프라이버시와 개인정보보호의 상호관계에 대한 재고찰의 의의가 있겠다.
  - 발표문은 행정기관(FTC)에 의한 민사벌칙금, 민사상 손해배상 청구 등에 대해 언급하고 있다. 국내법제와의 면밀한 비교검토를 통해 수용여부를 결정할 필요가 있다.
  - 육안에 의한 관찰만 가능하고 녹화는 금지된다는 논의는 기술발전의 현실을 도외시한 느낌이다. 녹화를 전제로 해서 이의 보존과 이용을 규제하는 것이 현실적이다.

## 3. 미국의 CCTV 법제 및 현장실무

- o 헌법과 판례법에 의해 프라이버시에 대한 기대가 구체적 사안에서 인정될 수 있는지에 따라 해결되고 있으나 구체적 입법이 필요하다는 지적이 증가하고 있다.
- o 경찰행정기준이 제정되어 있는 경우도 있다. 예컨대 워싱턴 지역 경찰인 MPDC는 다음과 같은 CCTV 설치, 운영기준을 따르는 것으로

웹에 게시되어 있다.

- 프라이버시 기대가 없는 공개된 장소를 관찰의 대상으로 함
- 특정인을 대상으로 한 자의적, 차별적 관찰은 금지됨.

## 제 3 주제

### 독일의 개인정보보호법제 및 CCTV관련법의 문제점과 개선방안

발 표 : 문병효 교수(한경대학교)

토 론 : 강문수 박사(한국법제연구원)

## 독일의 개인정보보호법제 및 CCTV관련법의 문제점과 개선방안

문 병 효  
(한경대학교 법학부 교수)

### I. 서론

현대사회에서 정보수집 및 처리기술은 날로 발전하고 있는 반면 그에 상응하여 개인정보의 유출 위험성은 날로 커지고 있다. 조지 오웰이 일치감치 예언한 “Big Brother”의 시대가 이미 도래했다는 착각이 들 정도이다. CCTV 등을 통한 비디오감시는 공공기관이나 사기업, 사인의 영역에서 점점 더 행해지고 있다. 비디오감시분야는 날로 성행하고 있고 안전과 관련된 업체는 상대적으로 경기에 의존하지 않는다. 비디오기술은 안전기술로서의 이용에 그치지 않고 오락이나 광고의 목적, 교육, 통신 등등에 투입되고 있다. 가격은 내려가는 반면에 정보기술은 점점 더 발전하고 있기 때문에 그 사용은 날로 늘어나고 있다. 그러나 기술적으로 가능하다고 해서 법적으로 허용될 필요는 없다. 비디오감시는 화상자료가 수집, 녹화되고 처리, 전송되는 사람의 인격권을 침해한다.<sup>1)</sup> 따라서 비디오기술의 투입은 신중해야 한다. 특히 CCTV

1) 개인정보의 개념정립과 관련해서는, 프라이버시 개념으로부터 도출하는 체계에서 벗어나 새로이 개인정보에 관한 권리의 개념을 정보의 경제적 가치를 기준으로 재정립할 필요가 있다는 견해도 있다. 인격권에 국한되었던 종래의 논의가 개인의 인격적 가치에 중점을 두어 헌법학적, 불법행위법적 논의를 하는 반면, 재산권적 논의는 정보의 경제적 가치에 중점을 두고 거래법 법리 속에서 해결책을 찾으려 한다. 이민영, 개인정보법제론, 진한 M&B, 2005, 25쪽 이하 참조. 보호가치 혹은 경제적 가치에 따라 유형별로 분류하고 인격적 속성과의 연관성에 비추어 개인정보를 개별적으로 논의하려는 시도 자체는 의미가 있으나, 경제적 가치, 계약법, 재산권적 측

및 비디오감시는 사적 영역에 대한 위협뿐만 아니라 민주주의시스템에 대한 위협도 문제될 수 있기 때문에 더욱더 신중하게 접근해야 한다.

이하에서는 독일의 개인정보보호법제와 CCTV관련법을 살펴보고 그 문제점과 개선방안에 대해서 논의하고자 한다.

## II. 독일의 개인정보보호법제 검토

### 1. 헌법적 토대

독일에서도 개인정보보호에 대해서는 독일기본법 제1조 제1항과 결부된 제2조 제1항의 일반적 인격권(Personlichkeitsrecht)의 하나로서 접근하는 것이 보통이다. 바로 이러한 인격권보호의 특별한 형태가 1983년 12월 15일 독일연방헌법재판소의 인구조사판결(Volkszaehlungsurteil)<sup>2)</sup>이래의 정보의 자기결정권이다. 이 권리는 초상권을 포함하는 상위개념이다. 정보의 자기결정권은 누가, 무엇을, 언제, 어떠한 사항에 있어 어떤 것을 아는지 스스로 결정하는 개인의 권리로 정의된다. 현대 정보처리의 조건하에서 이 권리는 무제한적인 개인적 정보 수집, 저장, 이용, 전달로부터 보호를 포괄한다. 관련자는 원칙적으로 자신의 개인적 정보를 처리하고 이용하는데 대해 스스로 결정하여야 한다. 이러한 권리의 침해는 법률을 근거로 해서만 허용된다. 이 법률은 충분한 규범명확성을 통해서 어떤 내용적, 절차적 조건하에서 침해가 허용되는지 인식되게 해야 한다.<sup>3)</sup>

개인정보보호는 그러나 이러한 인격권의 차원을 넘어서는 측면도 있음이 지적되고 있다. 연방헌법재판소가 위의 1983년 판결에서 언급

---

면으로 중점이 이동하는 것에 대해서는 의문이 제기될 수도 있을 것임.

2) BVerfGE 65, 1.

3) Weichert, Private Ueberwachung und Datenschutzrecht, Detektiv-Kurier, Heft 04/2001, www.

하고 있듯이 “집회나 시민발의(Buergerinitiative)에의 참여가 행정청에 의해 기록되고 그에 의해 어떤 위험이 발생할 수 있다고 생각하는 사람은 그에 상응하는 기본권(기본법 제8조, 제9조)의 행사를 포기할 것이다. 이것은 개인의 인격발현의 기회에 영향을 미칠 뿐만 아니라 공공복리(Gemeinwohl)에도 영향을 미친다. 왜냐하면 자기결정은 시민의 행위가능성, 참여가능성을 토대로 하는 자유민주주의 공동체의 근본적인 기능조건이기 때문이다.”<sup>4)</sup> “관찰 당한다는 불안함이 조심스런 행동을 초래하고, 시민권적인 자유의 이용을 방해한다. 기술적으로 지속적인 통제 하에 있는 사회는 위헌적이다. 이것은 자유민주주의에 유해하다. 각 개인은 어떤 인적인 정보가 어떤 목적으로 어떤 맥락에서 처리되는지 스스로 결정하고 알아야 한다.” 비디오감시의 실체는 누가 녹화를 하고 이것이 어떻게 이용되는지 인식할 수 없기 때문에 감시기술과 정보의 자기결정권간의 고전적인 갈등영역에 속한다. 연방헌법재판소의 판결에서는 그러나 관련자(Betroffene) 내지는 정보보호자(Datenschuetzer)가 비디오감시의 허용성을 입증해야하는 것이 아니라 그러한 시설의 운영자(Betreiber)가 인간의 권리침해의 불가피성을 입증해야한다는 점이 도출되지는 않는다.<sup>5)</sup>

## 2. 독일연방정보보호법(BDSG)

2001년 5월 18일의 새로운 연방정보보호법은 EU의 정보보호지침(EU-DSRL)에 의해 법률개정이 강제된 측면도 있지만 현대적인 정보보호법의 원칙들, 소위 시스템정보보호의 원칙에 속하는 정보회피(Daten-

---

4) Baemler, Datenschutzrechtliche Grenzen der Videoueberwachung, Beitrag zur Fachkonferenz “Risiken und Grenzen der Videoüberwachung” des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern am 7./8. November 2000 in Schwerin.

5) Weichert, Private Ueberwachung und Datenschutzrecht, Detektiv-Kurier, Heft 04/2001, www.

vermeidung), 정보절감(Datensparsamkeit)의 원칙이나 기술(Technik)에 의한 정보보호의 원칙이나 정보보호감시(Datenschutzaudit)의 원칙들을 이미 포함하고 있다.<sup>6)</sup>

개정된 정보보호법의 주요내용을 살펴보면 다음과 같다.

첫째, 적용영역의 확대

정보처리설비의 투입으로 행해지는 각 인적관련정보의 처리가 파악됨으로써 법률의 객관적인 적용영역이 특히 사경제(Privatwirtschaft)에 대해서 확대되었다.

둘째, 관련자에 대한 투명성확대

새 정보보호법은 정보수집시 책임기관이 관련자에게 책임기관과 정보수집 및 정보처리의 목적을 명명하도록 규정하고 있다. 공공기관에 대해서뿐만 아니라 비공공기관에 대해서도 고지의무가 규정되어 있다(동법 제4조 제3항, 제19a조, 제33조).

셋째, 정보처리제한의 확대

관련자에게는 그와 관련된 정보처리에 대하여 처음으로 이의제기권(Widerspruchsrecht)이 명시적으로 부여되었다(제20조 5항, 제35조 5항). 이것은 그러나 - 책임기관에는 지금까지 알려져 있지 않은 - 구체적인 인적 상황을 근거로 그의 보호이익에 우월성이 주어지는 경우에만 이의를 제기가 가능하다.

넷째, 정보보호통제의 확대

연방정보보호법은 내부의 정보보호관(Datenschutzbeauftragte)에 의한 자기통제(Selbstkontrolle)에 우위를 두고 동법률의 총칙편에 그의 법적지

---

6) Gola/Schomerus, BDSG-Kommentar, Einleitung, Rn. 12.

위 및 임무를 규정하고 있다(제4f조와 제4g조). 특히 위험한 정보처리  
의 경우 소위 사전통제(Vorabkontrolle)와 누구든지 열람이 가능한 절차  
목록의 작성이라는 새로운 과제가 정보보호청에게 주어져 있다.<sup>7)</sup>

### 3. EU 정보보호지침(EU-DSRL)

유럽법에서 유럽인권협약 제8조는 사생활에 대한 권리를 보호하고  
있으며, 개인정보보호는 유럽연합 기본권헌장(Grundrechte-Charta) 제8  
조에 의해서 보호되고 있다. 이러한 일반적인 규정은 1995년의 유럽정  
보보호지침(Europäische Datenschutzrichtlinie)의 발효로 구체화된다. 동  
지침은 25개 유럽연합 회원국을 구속한다. 이것은 광범위한 CCTV시  
스템으로 잘 알려져 있는 영국에도 적용되지만, 영국에서 시행되는 강  
력한 비디오감시체계는 인권협약 및 기본권헌장 제8조 뿐만 아니라  
유럽연합 정보보호지침과도 합치되지 않는다.<sup>8)</sup>

유럽연합정보보호지침은 독일정보보호법의 영향을 받아 기본원칙으  
로 투명성, 목적구속성, 필연성, 참여가능성 등을 규정하고 있다. EU  
지침은 특정내용의 정보, 즉, 건강기록, 성생활, 인종, 민족 출신정보,  
정치, 종교, 철학적 사상 및 신조, 노동조합 소속여부 등을 특별히 보  
호해야한다고 규정하고(보호가치가 높은 정보에 대한 특별보호), 그러  
한 정보의 수집과 이용시 사전에 정보주체에게 알려야 하며 별도의  
동의를 받아야 한다고 규정한다. 이 지침에 따르면 유럽연합 비회원국  
에게 정보를 유통하는 것은 그 나라가 유럽연합국에 상응하는 개인정  
보보호수준이 마련되어 있지 않을 경우 금지되어 있다.<sup>9)</sup>

7) Gola/Schomerus, a.a.O., Einleitung, Rn. 14 ff.

8) Weichert, a.a.O.

9) 로스나겔, 독일의 개인정보보호법, “개인정보 보호제도의 개선을 위한 국제심포지엄”, 2004, 4쪽.

### Ⅲ. 독일개인정보보호법상 CCTV관련규정과 그 내용

#### 1. 연방정보보호법 제6b조의 신설

2003년 개정된 연방정보보호법(BDSG)에서 비디오감시에 관한 규정(제6b조)을 신설하였다.

동법은 비디오 감시가 허용되는 경우를 한정하고, 수집된 정보의 처리 및 이용요건 및 절차에 대하여 규정하고 있다.

비디오 감시는 ①공공기관의 임무수행의 경우, ②주거권의 실현을 위한 경우, ③구체적으로 정해진 목적을 위하여 정당한 이익의 실현(Wahrnehmung berechtigter Interessen)을 위하여 필요하고 관련 당사자의 보호받을만한 이익이 우월하지 않은 경우에 한하여 허용된다(제6b조 제1항).

수집된 정보의 처리와 이용은 그 정보가 달성하려고 하는 목적을 위하여 필요하고 관련 당사자의 보호법익이 우월하지 않을 때만 인정되며(동조 제2항), 다른 목적을 위한 개인정보의 처리와 이용은 국가 및 공공의 안전을 위한 위험방지를 위하여 그리고 범죄수사를 위하여 필요한 경우에 한하여 허용된다(동조 제3항).

비디오 감시를 통하여 수집된 정보가 특정한 개인과 관련될 경우에는 그 처리와 이용에 관하여 이를 당사자에게 고지하여야 하고(동조 제4항), 그 정보가 목적 달성을 위하여 더 이상 필요하지 않을 경우 또는 지속적인 저장이 당사자의 보호법익에 상충될 때에는 지체없이 삭제하여야 한다(동조 제5항).

## 2. 규정의 목적

입법자는 공공이 접근가능한 공간에서의 공공기관에 의하건 비공공기관에 의하건 건비디오감시에 대해서 “정보의 자기결정권”을 존중하여 법률적 토대를 마련하려는 목적으로 동 규정을 마련하였다. 여기서 입법자는 보호가치있는 관찰목적을 배제하지 않으면서 비디오감시시설 운영자의 기본권적 지위도 고려되어야 했다. 이러한 목적하에 비디오감시를 정당화하는 사실관계의 범주가 제한되었고 그로 인해 획득된 정보의 엄격한 목적구속이 규정되었으며 관련자에 대한 투명성이 제고되었다.<sup>10)</sup>

## 3. 규정의 연혁

비디오감시의 제한에 대한 최초의 법안은 1988년 12월 13일 SPD가 연방정보보호법안 제56조 이다. 동 조항에는 수집된 정보가 증거확보에 필요한 경우가 아닌 한 48시간 후에는 삭제되어야 한다고 규정하는 내용 등이 포함되어 있었다. 그 이후 1997년 11월 14일 녹색당이 제14대 의회에서 법안을 제출하였고, 2000년 사민당과 녹색당의 연정에 의해서 제출된 법안이 독일의회에서 2001년 4월 4일 내무위원회의 의결권고를 기초로 구체화되고 강화되었다.<sup>11)</sup>

## 4. 다른 규정과의 관계

독일연방정보보호법 제6b조는 공공기관과 비공공기관에 적용되는데, 공공기관과 관련해서는 연방의 공공기관과 동법 제1조 제2항 제2호의 요건 하에 각 주들의 공공기관이 관련된다. 주의 시설에 대해서는 그

10) Bizer, in: Simitis(Hrsg.), Bundesdatenschutzgesetz, 6. Aufl., §6b, Rn. 4.

11) Bizer, in: Simitis(Hrsg.), Bundesdatenschutzgesetz, 6. Aufl., §6b, Rn. 6 ff.

러나 개정된 주의 정보보호법에 포함된 동종의 규정들이 우선적으로 적용된다. 하지만 전체적으로 이 규정들은 제한적인 효력을 갖는데, 일반 정보보호법은 연방이나 주의 특별한 영역에 대해 규율하는 법이나 집회법(제12a조, 제19a조 *Versammlungsgesetz*), 형사소추기관(제100c조 1항 1a호, *StPO*), 경찰영역에 대해서 보충적이기 때문이다.<sup>12)</sup>

## 5. 비디오 감시(제1항)

### (1) 수범자(Adressat)

독일연방정보보호법 제6b조는 사람과 관련된 정보를 정보처리시설을 투입하여 처리하는 경우, 오로지 개인적이거나 가족의 활동을 위한 경우를 제외하고는, 연방의 공공기관 뿐만 아니라 공공기관이 아닌 경우에 대해서도 적용된다.<sup>13) 14)</sup>

### (2) 오로지 개인적 혹은 가족적인 목적의 배제

제6b조는 비디오감시가 오로지 개인적인 목적을 위해서이거나 가족적인 목적을 위한 경우 적용되지 않는다. 이 경우 비디오감시는 판례에서 전개된 한계 내지는 재산권의 보호를 위해서만 허용된다.<sup>15)</sup> 직업

---

12) Gola/Schomerus, a.a.O., § 6b, Rn. 6.

13) 동 규정은 연방이 아닌 주의 공공기관에 대해서는 적용되지 아니한다. 이에 대해서는 vgl., Bizer, a.a.O., §6b, Rn. 29.

14) 독일연방헌법재판소는 1983년 12월 15일 인구조사판결에서 국가의 정보처리의 적법성 및 이와 관련하여 공적인 영역에서 뿐만 아니라 사적인 영역에서의 정보의 자기결정권에 대한 시민의 보호청구권에 관하여 언급함으로써 정보보호규범의 구체화 및 확대 필요성을 제기하였다. 기본권에 표현된 가치질서는 법의 모든 영역에 작용하기 때문에 인적관련 정보처리에 있어서 입법자는 일반적이고 포괄적인 인격권의 보호를 해야 할 의무가 있다. 이러한 결론하에 입법자는 1990년의 최초의 연방정보보호법개정에서는 주로 경제계로부터의 요구인 공적인 영역에 대한 규정과 사적인 영역에 대한 규정의 분리, 즉 정보보호의 두 영역분리의 요구를 따르는 것을 고려하지 않았던 것이다. vgl. Gola/Schomerus, BDSG-Kommentar, Einleitung, Rn. 6.

15) Bizer, a.a.O., §6b, Rn. 30; BGH, NJW 1955, 1957.

활동이나 영업활동의 범위 내에서 비디오감시가 행해지는 경우는 다시 제6b조의 요건 하에 적용된다. 그러나 이러한 예외의 인정은 비디오감시를 통한 인격권 침해의 위험가능성을 고려하여 엄격히 해석되어야 한다.

### (3) 비디오감시(Videoueberwachung)

동 규정은 시각적-전자적 시설에 의한 관찰(Beobachtung mit optisch-elektronischen Einrichtung)에 대해서 적용된다. 따라서 화상의 형태로 되어 있으면 되고 시간적 간격에 의한건 아니건 그 형태는 문제되지 않는다. 또한 시설도 시각적-전자적 관찰을 가능하게 하는 시설이면 되고 그 크기나 기능, 고정되어 있건 움직일 수 있도록 되어 있건, 줌이 있는지 없는지 하는 것은 문제되지 않는다. 또한 전자적 시설이면 되기 때문에 아날로그 방식이든 디지털 방식이든 문제되지 않는다. 전자적 관찰이라는 구성요건 표지는 그 시설이 스스로 내지 최소한 본질적인 기능이 전기로 조종될 수 있으면 이미 충족된다.<sup>16)</sup> 순수한 관찰은 사실 정보수집이지만 화상이 저장되지 않는 경우로서 이 경우에도 제6b조가 적용된다(Kamera-Monitor-Systeme). 동조는 제1항의 관찰과 제3항의 처리 또는 이용을 구별하고 있기 때문이다.<sup>17)</sup>

### (4) 공공이 접근가능한 공간(Oeffentlich zugangliche Raeume)

공공이 접근가능한 공간에서 관찰되어야 한다. 여기서 공간은 공공이 접근가능한 영역(Bereiche)으로 이해된다.<sup>18)</sup> 지붕이 있는지 사방을 둘러싸고 있는지는 중요하지 않다. 관련된 자가 비디오감시를 피할 수 있는 가능성을 가지고 있다는 점이 기준이 된다. 따라서 건물 밖에서

16) Bizer, a.a.O., §6b, Rn. 35f.

17) Bizer, a.a.O., §6b, Rn. 37; Weichert, Private Ueberwachung und Datenschutzrecht, Detektiv-Kurier, Heft 04/2001, www.

18) Gola/Schomerus, BDSG-Kommentar, § 6b, Rn. 8.

도 이러한 공간은 존재하고 도로나 길, 상점가, 주유소나 기타 외부시설도 경계를 한정함으로써 그 가능성이 제한되는 시설이면 된다.<sup>19)</sup> 공공이 접근가능한 공간은 누구에 의해서도 충족될 수 있는 일반적 표지에 의해 그 접근가능성이 규정된 공간이다. 이러한 의미에서 입장료를 내거나 기타 미리 규정할 수 있고 누구에 의해서도 충족가능한 접근요건이 적용되는 경우에도 접근가능한 공간이라고 할 수 있다(예컨대, 고객카드나 신용카드로만 입장이 허용되는 은행창구, 교통시설, 문화시설). 공중화장실도 이용자가 문을 잠글 수 있지만, 이런 의미에서 접근가능한 공간이다.

반면에 일정한 범주의 사람만이 드나들 수 있는 경우나 회사의 직원들만이 접근할 수 있는 공간은 공공이 접근가능한 공간에 해당되지 않는다. 이러한 이유로 작업장에서의 비디오감시는 이에 해당되지 않는다. 그러나 공공이 접근가능한 공간에서의 노동, 예컨대 상점이나 창구, 교통시설의 경우에는 동조항이 적용된다. <sup>20)</sup>

#### (5) 허용되는 관찰목적

공공이 접근가능한 공간에서의 비디오감시는 공공기관의 임무수행(Nr. 1)이나 주거권의 실현(Nr. 2), 구체적으로 정해진 목적을 위한 정당한 이익의 실현(Nr. 3)을 위해서 필요한 경우, 그리고 관련자의 보호 받을만한 이익이 우월하다는 근거가 존재하지 않을 때에만 허용된다.

제6b조 1항 제1호에 의하면 비디오감시는 공공기관의 임무수행(Aufgabenerfuellung)을 위해서만 허용된다. 정부의 법률초안은 비공공기관의 임무수행에 대해서도 규정했지만<sup>21)</sup> 입법자는 따르지 않았다. 그 결과 비공공기관은 제1호가 아니라 제2호와 제3호를 근거로 해서만 비

---

19) Bizer, a.a.O., §6b, Rn. 41.

20) Bizer, a.a.O., §6b, Rn. 43.

21) BT-Drs. 14/4329, S. 10.

디오감시를 할 수 있도록 되어있다.

제2호의 주거권(Hausrecht) 실현을 위한 비디오감시는 공공기관뿐 아니라 비공공기관에 대해서도 적용된다. 민법상으로 주거권은 독일민법(BGB) 제859조 이하, 제904조, 제1004조 재산권자의 방어청구권에서 도출되지만 그 근거와 한계는 임차권(독일민법 제535조)이나 그 밖의 특별법상의 규정들에서도 도출될 수 있다.<sup>22)</sup> 공적인 영역에서 주거권은 주로 공법적으로 규율되는데, 행정절차법(VwVfG) 제89조 회의진행권이나 법원조직법(GVG) 제175조 내지 제183조의 법정경찰에 관한 권리 등이 그 예가 될 수 있다. 주거권실현을 위한 비디오감시는 예방적 목적뿐만 아니라 억제적(repressive) 목적으로도 사용될 수 있다.

제3호는 구체적으로 정해진 목적을 위한 정당한 이익의 실현(Wahrnehmung berechtigter Interessen)이라는 구성요건표지를 가지고 있다. “정당한 이익의 실현을 위한 감시”라는 표지는 극도로 불필요하게 광범위하여 헌법적으로 문제될 수 있다. 너무 광범위한 개념은 기본권침해를 정당화하기 때문에 헌법합치적으로 좁게 해석되어야 한다는 지적이 있다.<sup>23)</sup> 참고로 정부의 법안에는 “Erfuellung eigener Geschaeftszwecke”이라고 되어 있던 것을 입법자가 더 좁은 허용요건으로 결정한 것이다. 물론 제3호의 정당한 이익의 실현을 위한 비디오감시는 그의 목적이 구체적으로 정해져 있어야만 허용된다. 법률안의 이유에 따르면 그 목적은 비디오감시가 시작되기 전에 구체적으로 확정되어 있어야 한다. 이것은 각 비디오감시조치가 필요했는지에 대한 사후심사를 경감한다. 이것은 비디오감시장치를 운전하기 전에 관찰목적이 문서화되어야 가능할 것이다. 목적을 구체적이고(첫째) 적시에(둘째) 확정했는지에 대한 입증책임은 비디오감시에 대해 책임있는 기관에게 있다. 그에 대한 충분한 입증이 행해지지 않으면, 비디오감시는 그러한 한에서 허용되

22) Bizer, a.a.O., §6b, Rn. 48.

23) Weichert, a.a.O.

지 않는다.<sup>24)</sup>

비디오감시는 제1호 내지 제3호의 목적을 위해 필요한(erforderlich) 경우에만 허용된다. 또한 비디오감시가 필요한 경우라도 관련자의 보호받을만한 이익이 우월하다는 근거가 있으면 허용되지 않는다(이익형량). 이 경우 정보의 자기결정권에 의해 보호되는 비디오감시 대상자의 이익이 그 척도가 된다.<sup>25)</sup>

## 6. 인식요건 (Kenntlichmachung der Beobachtung)

제6b조 제2항에 의하면 비디오관찰의 정황 및 책임기관이 적절한 조치를 통해서 인식될 수 있어야 한다(투명성요건(Transparenz)). 이에 의해 관련자에게 관찰된다는 사실이 인식될 수 있어야 한다. 따라서 몰래카메라는 허용되지 않는다. 비디오감시의 정황은 표지판에 의해 이것이 지적되거나 혹은 카메라가 평균적인 사람에게 의심없이 그 자체로서 인식될 수 있을 때 인식가능한 것으로 본다.<sup>26)</sup> 관련자는 또한 비디오감시에 대해 책임있는 기관에 대해서도 인식할 수 있어야 한다. 여기서 책임기관이라 함은 인적관련 정보를 관찰을 통해서 수집하고 처리하거나 이용하는 기관을 말한다. 책임기관에 관한 정보는 관련자에게 자신의 정보보호권을 누구에게 주장할 수 있는지 알게 해준다. 따라서 책임기관의 동일성, 즉 이름과 주소 등이 기록되어 있어야 한다.<sup>27)</sup>

## 7. 정보의 처리 및 이용

제6b조 제3항은 제1항의 기술적 시설에 의한 관찰로 생성된 인적 관련정보의 처리 또는 이용을 규율하고 있다. 이러한 정보의 처리나

---

24) Bizer, a.a.O., §6b, Rn. 51 ff.

25) Bizer, a.a.O., §6b, Rn. 60.

26) Weichert, a.a.O.

27) Bizer, a.a.O., §6b, Rn. 71 ff.

이용은 그것이 추구하는 목적의 도달을 위해 필요하고 보호받을만한 이익이 우월하다는 어떤 근거가 존재하지 않는 경우에만 허용된다(제 1문, 목적구속 *Zweckbindung*). 목적의 변경은 국가 및 공공의 안녕을 위한 위험방지를 위하거나 범죄수사를 위하여 필요한 경우에만 허용된다(제2문).

제3항 제1문의 규정은 제1항에서 수집된 인적 관련정보의 사용에 대한 특별한 허용요건을 포함하고 있다. 동 규정은 비디오감시에 의해 획득된 정보의 처리나 이용을 제1항에 규정된 원래의 관찰목적(*originaere Beobachtungszweck*)에 엄격히 구속시킴으로써 허용성의 규율과 결합시키고 있다. 목적구속은 정보처리의 전 단계에 대해서 적용된다. 이 규정의 정당성은 시각적-전자적 녹화물의 처리 또는 이용을 통해 나올 수 있는 관련자에 대한 특별한 위험에서 도출된다. 이러한 법률상 허용요건을 넘어서 정보처리, 이용을 하는 경우에는 동법 제4조 제1항과 제4a조 제1항의 요건을 충족하는 동의(*Einwilligung*)가 있는 경우에만 허용된다.<sup>28)</sup>

비디오관찰에 뒤따르는 정보의 처리나 이용은 확정된 목적을 위해 필요하여야 한다. 예컨대 구체적인 위험방지를 위해 정보의 저장이 행해지는 경우, 경찰에게 즉각적인 개입을 위해 필요한 정보를 전달할 수 있기 위하여 단기간의 저장이 필요할 수 있다. 효과적인 위험방지는 보호법익에 대한 손해를 적시에 방지할 수 있기 위해서 경찰의 지체없는 개입을 필요로 한다. 문서화하기 위해 장기간 저장하는 것은 위험방지를 위해서는 필요하지 않지만, 사후 법원에서의 사법절차를 위한 증거확보를 위해서는 필요할 것이다.<sup>29)</sup>

또한 관련자의 보호받을만한 이익이 정보의 처리나 이용보다 우월하다는 어떤 근거가 존재하지 않아야 하는 바, 이러한 이익형량

28) Bizer, a.a.O., §6b, Rn. 74.

29) Bizer, a.a.O., §6b, Rn. 78.

(Abwägung)은 각각의 정보처리단계에 대해 필요하다. 정보의 처리나 이용목적이 관련자의 보호받을만한 이익에 우월해야 한다는 점과 함께 기술적, 조직적 조치들, 예컨대 저장기간이나 삭제조치, 정보회피 내지 정보절감조치(Datensparsamkeit) 등도 고려될 수 있다. 그러한 조치를 통해 정보의 자기결정권에 대한 침해가 최소화 될 수 있다.<sup>30)</sup>

인적 관련 녹화물을 제3자에게 전달하는 것은 통상 관련자의 보호 받을만한 이익이 침해된다. 그러한 전달을 통해 잠재적 수령자의 범주가 확대되고 따라서 수집기관으로부터 멀어짐으로 인해 목적구속이 회피될 위험도 확대되기 때문이다. 이러한 위험증대의 관점에서 인적 관련 녹화물의 전달은 통상 관련자의 보호받을만한 이익을 침해한다. 비디오 감시를 통해 획득된 인적관련 화상을 공적인 미디어에 공표하거나 웹카메라(WebCams)로 녹화된 화상을 인터넷에 배포하는 것은 통상적으로 관련자의 보호받을만한 이익을 침해하게 되므로 허용되지 않는다. 연방정보보호법 제1조 제3항에 의하여 제6b조에 우선하는 예술가의 저작에 관한법률(KunsUrhG) 제22조 제1항 제1문에 따라 그러한 화상은 관련당사자의 동의하에서만 배포되거나 공적으로 관람되는 것이 허용된다.<sup>31)</sup>

## 8. 고지의무(Benachrichtigung) 및 삭제의무(Loesung)

비디오 감시를 통하여 수집된 정보가 특정한 개인과 관련될 경우에는 그 처리와 이용에 관하여 이를 당사자에게 고지하여야 하고(동조 제4항), 그 정보가 목적 달성을 위하여 더 이상 필요하지 않을 경우 또는 지속적인 저장이 당사자의 보호법익에 상충될 때에는 지체 없이 삭제하여야 한다(동조 제5항).

---

30) Bizer, a.a.O., §6b, Rn. 80.

31) Bizer, a.a.O., §6b, Rn. 83 f.

## 9. 기 타

비디오감시는 의문 없이 관련된 당사자의 권리 및 자유에 대한 위협과 결부된다. 따라서 연방정보보호법 제4d조에 의한 사전통제(Vorabkontrolle)가 행해져야 한다. 이것은 비디오 감시시설의 운영자에게 구체적인 필요성에 대한 합리적인 근거제시를 강제한다.<sup>32)</sup>

고의 또는 과실로 비디오에 의해 정보를 수집하거나 계속해서 처리하는 자는 연방정보보호법 제43조 제2항 제1호의 질서위반행위(Ordnungswidrigkeit)를 한 것이다. 허용되지 않는 온라인상의 제공, 예컨대 인터넷을 통한 전송을 행하는 경우 동법 제43조 제2항 제2호가 적용될 수 있다.<sup>33)</sup> 그러한 행위가 요금을 받거나 전파의 의도 또는 해할 목적으로 행해지는 경우 연방정보보호법 제44조에 의한 범죄행위(Straftat)가 된다. 고지의무위반이나 회신의무(Auskunftspflicht)위반의 경우에는 동법 제43조 제1항에 따라 과태료(Bussgeld)가 부과될 수 있다. 또한 투명성요건에 반하는 표식의무(Hinweispflicht)위반의 경우에도 과태료가 부과될 수 있다. 사실 과태료규정은 동법 제33조 제1항에 의한 고지의무만을 규정하고 있지만 동법 제6b조 제4항의 고지의무는 제33조 제1항의 특별규정이기 때문에 고지의무위반은 과태료 부과처분의 대상이 될 수 있다. 그러나 비디오 감시를 하고 있음을 표시해야하는 표식의무위반의 경우에는 그러한 특별한 경우로 간주될 수 없고, 명시적인 규정의 흠결 때문에 질서위반으로 제재될 수 없게 된다.<sup>34)</sup>

---

32) Weichert, a.a.O.

33) Weichert, a.a.O.

34) Weichert, a.a.O.

## IV. 문제점 및 개선방안

### 1. 개인정보보호에 관한 통합법의 필요성

독일은 연방정보보호법에서 개인정보의 보호에 관해서 통일적으로 규정하고 있다. 공공기관이 보유하고 있는 정보뿐만 아니라 비공공기관이 보유하고 있는 정보도 그 대상이 된다. 오늘날에 특히 사경제영역의 비중이 커짐에 따라 그에 의한 개인의 권리침해가 증가하고 있는 바, 이것은 개인정보와 관련해서도 마찬가지이다. 정보보호법의 통일적인 규정을 통해서 현대사회의 그러한 위험성을 예방 또는 제거하는데 효율적으로 대처할 수 있을 것이다.

### 2. 감시목적의 제한

독일연방정보보호법 제6b조의 경우처럼 비디오감시목적의 제한하는 것이 필요하다. 따라서 공공기관의 임무수행이나 주거권의 실현, 구체적으로 정해진 목적을 위한 정당한 이익의 실현을 위한 경우 등으로 비디오감시목적의 제한하고 그 밖에 필요성과 이익형량의 요건을 갖추었을 때 비디오감시를 허용하도록 해야 한다.

### 3. 엄격한 목적구속

비디오감시에 의해 획득된 정보의 처리나 이용을 원래의 관찰목적에 엄격히 구속시키고 다른 목적으로 사용되지 않도록 해야 한다. 목적구속은 정보처리의 전 단계에 대해서 적용된다. 시각적-전자적 녹화물의 처리 또는 이용을 통해 관련자는 특별한 위험에 노출되기 때문이다. 이러한 법률상 허용요건을 넘어서 정보처리, 이용을 하는 경우에는 원칙적으로 허용하지 않되 예외적으로 관련자의 동의가 있는 경우에만 허용되도록 한다.

#### 4. 고지 및 삭제의무

비디오 감시를 통하여 수집된 정보가 특정한 개인과 관련될 경우에는 그 처리와 이용에 관하여 이를 당사자에게 고지하여야 하고, 그 정보가 목적 달성을 위하여 더 이상 필요하지 않을 경우 또는 지속적인 저장에 당사자의 보호법익에 상충될 때에는 지체없이 삭제하여야 한다.

#### 5. 사전통제의 필요성

비디오감시시설의 기술적 수준이나 정도에 따라서 비디오감시는 독일연방정보보호법 제4d조 제5항 제1문의 사전통제(Vorabkontrolle)를 받는다. 사전감시는 개인의 정보수집을 위한 전자카메라의 사용이 관련자의 권리와 자유에 대한 위험을 주는 경우에 행해진다. 감시카메라가 다수 투입되고 중앙에서 통제되는 경우는 특별한 위험성을 내포하고 있기 때문에 사전통제가 요구되는 것이다.<sup>35)</sup>

#### 6. 보호가치가 높은 정보에 대한 특별보호

EU지침은 보호가치가 높은 정보에 대한 특별보호를 규정하고 있는데, 특정내용의 정보, 즉, 건강기록, 성생활, 인종, 민족 출신정보, 정치, 종교, 철학적 사상 및 신조, 노동조합 소속여부 등을 특별히 보호해야한다고 규정하고, 그러한 정보의 수집과 이용시 사전에 정보주체에게 알려야 하며 별도의 동의를 받아야 한다고 규정하고 있는데, 이는 입법시 참조할 만한 것으로 보인다.

#### 7. 관련기관의 책임강화

고의 또는 과실로 비디오에 의해 정보를 수집하거나 계속해서 처리하거나 허용되지 않는 온라인상의 제공, 예컨대 인터넷을 통한 전송을

---

35) Bizer, a.a.O., §6b, Rn. 15.

행하는 경우는 과태료부과처분의 대상이 되도록 하고, 그러한 행위가 요금을 받거나 전파의 의도 또는 해할 목적으로 행해지는 경우 연방정보보호법 제44조의 예처럼 범죄행위로서 처벌되도록 할 필요가 있다. 그 밖에 고지의무위반이나 회신의무위반의 경우, 투명성요건에 반하는 표시의무위반의 경우에도 과태료 등의 부과로 제재가 가해져야 한다.

## 8. 비디오감시시설에 대한 상시감독 및 작동시스템 보고

비디오감시는 개인의 권리와 자유를 침해할 가능성이 높기 때문에 공공기관이나 비공공공간에서의 비디오감시시설에 대해 상시적인 감독이 행해지도록 해야 하고 그 작동시스템에 대해서도 변동상황을 관계기관에 보고하도록 하여야 한다.

## 9. 정보보호감독관 및 정보보호위원회 등 설치

독일의 경우처럼 의회가 정보보호감독관을 임명할 수 있도록 하거나 정보보호위원회를 설치하여 정보보호 임무를 담당하도록 하는 것이 필요하다. 정보보호위원회를 어디에 설치할 것인지는 논란이 될 수 있으나 독립적인 기관으로 설치하고 민간의 전문가나 시민단체 등도 참여할 수 있도록 하여야 한다.

## 10. 입증책임의 전환

비디오감시의 허용성에 대해서는 관찰의 대상이 되는 자나 정보보호관이 입증하게 해서는 안 되고 비디오감시시설의 운영자가 개인의 권리침해불가피성을 입증하도록 하여야 할 것이다.<sup>36)</sup>

---

36) 독일연방헌법재판소의 판결에서는 그러나 관련자(Betroffene) 내지는 정보보호자(Datenschuetzer)가 비디오감시의 허용성을 입증해야하는 것이 아니라 그러한 시설의

## 11. 정보의 자기결정권보호를 위한 절차법적, 실체법적 구제

비디오감시는 필연적으로 개인의 권리와 자유를 제한하고 특히 정보의 자기결정권을 침해할 소지가 크다. 그러기 때문에 반드시 법률유보의 원칙을 지켜서 규정되어야 하며, 비디오감시의 허용목적은 엄격히 제한하고 원래의 목적대로만 정보가 이용되도록 하고 다른 목적을 위해서 사용되지 않도록 규정을 두고 비디오감시시설에 대해서는 사전통제 및 지속적 감독이 이루어지도록 하는 것이 중요하고, 감시자의 사전통제의무나 삭제의무 등이 규정되어야 한다. 또한 자신의 정보에 대해서는 접근이 가능하도록 하여야 하고 정보가 공개되어야 하며, 잘못된 정보 잘못 처리, 이용되는 정보에 대해서는 이의를 제기할 수 있도록 해야 한다. 그 밖에 정보보호관에 대해 정보보호를 요청할 수 있도록 하고 행정소송 등을 통한 사법적 권리구제방법도 확보되어야 한다. 그리고 국가배상이나 손해배상에 의한 구제책도 마련되어야 할 것이다.

## V. 결 론

CCTV 및 비디오감시는 사적 영역에 대한 위협뿐만 아니라 민주주의시스템에 대한 위협도 문제된다. “기술적으로 지속적인 통제 하에 있는 사회는 위헌적이다. 이것은 자유민주주의에 유해하다”는 1983년 독일연방헌법재판소의 진술은 오늘날 우리에게도 충분히 시사적인 내용을 가지고 있다.

물론 그렇다고 해서 비디오감시시설의 일반적 금지까지 요구할 수는 없을 것이다. 다만 비밀스런 관찰기술로서의 비디오감시는 연방헌

---

운영자(Betreiber)가 인간의 권리침해의 불가피성을 입증해야한다는 점이 도출되지 않는다는 Weichert, a.a.O.

법재판소의 주요논지와도 맞지 않다는 점이 지적되어야 한다. 각 개인은 어떤 인적인 정보가 어떤 목적으로 어떤 맥락에서 처리되는지 스스로 결정하고 알아야 한다.

여기서 논리 필연적으로 필요성(Erforderlichkeit)의 문제가 제기될 수 있다. 비디오카메라의 법적 근거나 개별적인 기술의 양태에 앞서 모든 카메라는 그것이 필요한지 심사되어야 하고 이 경우 입증책임의 전환이 발생한다. 비디오를 주문하고 운영, 설치 혹은 찬성하는 자는 그것이 필요하다는 점 및 비디오투입이 필요성원칙의 위반 없이 가능한 것인지를 입증해야 한다.

비디오기술을 투입함에 있어서는 비디오 관찰가능성에 대한 불안, 녹화된 비디오의 사용에 대한 불안이 발생하는 것을 저지할 견제와 균형이 필요하다. 이러한 불안은 연방헌법재판소가 지적하듯이 민주주의의 독(Gift fuer die Demokratie)이기 때문이다.<sup>37)</sup> 이를 위해서는 비디오감시에 대한 법적 근거가 정확하고 이해할 수 있어야 하며, 비디오기술이 원칙적으로 개방되어야 하고 그 기능방식이 투명해야 하며 기능적 통제시스템이 존재해야 한다.<sup>38)</sup>

---

37) Baemler, Datenschutzrechtliche Grenzen der Videoueberwachung, Beitrag zur Fachkonferenz "Risiken und Grenzen der Videoüberwachung" des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern am 7./8. November 2000 in Schwerin.

38) 비디오테크닉에 대한 지속적인 관찰, 비디오카메라에 대한 정기적인 보고와 카메라가 어느 정도의 범위까지 미치는지 시각적으로도 심사할 수 있는 지도로 그려져 있도록 요구하는 견해도 있다. Baemler, a.a.O.

## 토 론 문

강 문 수

(한국법제연구원 부연구위원)

개인정보보호에 관련한 독일의 법제는 크게 『독일연방정보보호법』, 각 주의 『주정보보호법』 그리고 유럽연합의 『개인정보보호에 관한 지침』으로 구성되어 있다. 때문에 쉽게 이를 파악하기는 어려운 형태라 하겠다. 이 가운데 개인정보의 보호에 관한 근간법적인 성격을 가지는 것은 개정 『독일연방정보보호법(BDSG)』이라 하겠다.

이 법률은 1960년대의 소위 “행정자동화”를 위한 정책적 기반조성의 확보라는 기초를 계승하여 중앙정부의주도가 아닌 1970년대의 헤센주와 라인란트 팔츠주가 중심이 되어 중앙정부 차원의 개인정보보호에 관한 규범의 필요성에서 근거하여 1978년에 제정된 바 있다. 입법형식적인 특색으로는, 제정이전의 각 개별 법률에 산재하고 있었던 개인정보에 관한 규정들을 종합하여 체계적으로 구성한 “조합법률”적 성격을 가진다.

이 법률에서 보고하고자 하는 이익은 단순 정보가 아닌 정보를 보유하고 있는 개인이며, 이는 독일 기본법 제1조 제1항과 결부된 제2조 제1항의 일반적 인격권의 하나로 이해되어지고 있다. 독일의 경우에 있어 개인정보보호를 위한 법익의 확정, 요건 등에 관한 주요내용은 1983년 12월 15일 독일연방헌법재판소의 소위 “인구조사판결”을 통하여 법리적인 구체화를 완성한 바 있다. 이 판결문의 주요내용은 무엇보다 정보의 자기결정권에 있다고 하겠다. 정보의 자기결정권이란 발제자의

발표내용과 같이 누가, 무엇을, 언제, 어떠한 사항에 있어 어떤 것을 인지하고 있는지에 대하여 스스로 결정하는 개인의 권리를 말한다. 때문에 이후 개인정보보호에 관한 다양한 법리적 견해와 관련 판례에 있어 정보의 자기결정권은 문제의 출발점이자 곧 해결점이 되었다.

현재 독일에 있어 『독일연방정보보호법』과 관련한 논점은 발제자의 발제문에서는 주1) 에서 간략히 언급하고 있는 바와 같이 개인의 정보를 인격권에 한정하여 논하는 범위를 탈피하여 재산권적 관점으로 영역을 확대하여 재해석하고자 하는 움직임이라 하겠다.

2003년 독일의 개정 『연방정보보호법』은 제6b조를 신설하여 비디오 감시에 관한 내용을 명문화하고 있다. 본 조에서는 비디오 감시가 허용되는 경우를 한정하고, 수집된 정보의 처리 및 이용요건과 절차에 관한 내용을 담고 있다. 이에 있어 문제시되는 것은 사전통제와 감시 목적과 절차의 투명성에 있음이 독일의 다수견해라 할 것이다. 그러나 이와 관련하여 발제자의 발제문에서는 간략한 개조식으로 발제문을 완성하여 다소 아쉬움이 남는다. 때문에 이에 관한 보다 자세한 설명을 부탁하는 바이다.

또한 비디오감시시설에 대한 상시감독 및 작동시스템공지에 관하여서는 법은 일반적인 내용만을 선언하고 있는 수준이라는 점을 고려해 볼 때, 실무에 있어서는 이를 어떻게 운용하고 있는지가 궁금하다. 사실 실무에 있어 이와 같은 상시감독 및 작동시스템의 공지가 과연 가능한지가 의문시 된다.

그리고 발제자는 “연방헌법재판소의 판결에서는 그러나 관련자 내지는 정보보호자가 비디오감시의 허용성을 입증해야하는 것이 아니라, 그러한 시설의 운영자가 인간의 권리침해의 불가피성을 입증해야 한다는 점이 도출되지는 않는다”라고 설명하며 입증책임의 전환을 설명

하고 있으나 그 개념 및 전달에 오해의 소지가 있다고 생각되어지므로 이에 대한 설명이 있어야 할 것으로 생각된다. 이와 관련하여 정보의 자기결정권보호를 위한 절차법적, 실체법적 구제가 필요함을 적시하고는 있으나, 구체성이 결여되어 또한 설명을 구한다.

마지막으로 우리나라의 경우에 있어 공적분야와 사적분야로 구분하여 구성하고 있는 개인정보의 통합화에 관한 발제자의 의견을 청하는 바이다. 사실 독일의 경우에 있어, 법리적으로는 독일연방정보보호법이 공-사적분야 양자를 포괄하는 통합의 형태를 취하고는 있다고 해도 이는 근간법적인 성격을 띠게 되어 각 관련 개별 법률 등에서 이를 구체화 하고 있는 실정으로 생각되어진다. 때문에 발제자가 만약 통합을 주장하신다면 우리 법제에 있어 개인정보에 관한 새로운 기본법을 의도하시는지, 그리고 그러한 입법의 실익은 어디에 있는지 고견을 청한다.

## **제 4 주제**

### **일본의 개인정보보호법과 CCTV 관련 입법의 동향**

발 표 : 권건보 교수(명지대학교)

토 론 : 채승완 박사(한국정보사회진흥원)

## 일본의 개인정보보호법과 CCTV 관련 입법의 동향

권 건 보  
(명지대학교 법학과 교수)

### I. 서 설

(1) 국가의 감시는 항상 국민을 통제하기 위한 억압적 요소로서만 기능해온 것은 아니다. 국가안전의 확보, 범죄의 예방과 진압, 공공복리의 증진 등을 목적으로 하는 현대국가에 있어서 정부가 자신의 기능을 원활하게 수행하기 위해 전 국민을 대상으로 감시를 행하는 것이 필가피한 경우도 있다. 그러한 감시가 국민 개개인에게는 억압적인 것일 수 있겠지만, 전체적으로 볼 때 오히려 그것이 보다 많은 사람의 자유를 보장하는 데 기여할 수 있다.

이러한 감시의 억압적 측면과 보호적 측면은 전혀 별개로서 존재하는 것으로 이해되어서는 곤란하다. 국가에 의한 감시는 행정적 필요를 이유로 정당화되지만, 그렇게 해서 수집된 정보는 언제라도 정치적 지배를 위한 도구로 이용될 수 있기 때문이다. 오늘날 어디서나 국가는 ‘총체적 보호자’로 나타나고 있으며, 바로 이 때문에 국가는 ‘총체적 감시자’가 되고자 한다. 국가는 국민을 보호하기 위해 감시한다고 주장한다. 그러므로 감시의 이데올로기는 곧 보호의 이데올로기이기도 하다.

감시의 정당성을 훼손하지 않는 역감시체계의 구축에 대해서는 자기정보통제권의 적절한 보장으로 설명할 수 있다. 자기정보통제권은

어떠한 상황에서도 혹은 그 어떠한 이유로도 결코 제한할 수 없는 절대적인 의미를 가질 수는 없다. 자기정보통제권도 공동체관련성 내지 공동체구속성을 가지는 한도에서 중대한 공익을 위하여 일정 정도 후퇴되지 않으면 안 되는 것이다. 하지만 자기정보통제권이 역감시체계의 일부로서 실효적으로 작동되기 위해서는 입법적으로 충분한 뒷받침이 이루어져야 한다.

(2) 일본에서는 초기에 개인정보의 보호를 위한 법제화의 움직임은 지방자치단체에 의한 개인정보보호조례의 제정으로 가시화되기 시작하였다. 이후 1988년 12월 16일 「행정기관이 보유하는 전자계산기처리에 따른 개인정보의 보호에 관한 법률」이 공포됨으로써 국가적 단위의 개인정보보호법을 갖추게 되었다. 하지만 민간부문을 규율하는 개인정보보호법이 존재하지 않아 개인정보의 침해에 충분히 대처하기 어렵다는 지적이 많았다. 이에 따라 2003년 5월 30일에 「개인정보의 보호에 관한 법률」이 공포되기에 이르렀고, 이로써 일본에서도 공공부문과 민간부문을 포괄하는 기본법을 두게 되었다. 이러한 일본의 개인정보보호법제의 변화는, 통합기본법의 성격을 가지는 개인정보보호법의 제정 움직임이 가시화되고 있는 국내의 상황과 맞물려, 그 동안 비슷한 입법의 체계를 가지고 있었던 우리나라에 적잖은 영향을 미칠 것으로 예상된다.

(3) 일본에서도 2002년경부터 경시청에 의해 대도시 번화가를 중심으로 방법용 감시카메라를 설치하는 계획이 꾸준히 추진되어 왔다. 최근에는 전국 각지에 「슈퍼 방법등」이라고 하는 이름의 신형 방법카메라가 설치되고 있다. 그리고 전철역이나 초등학교, 상점가, 백화점, 쇼핑몰, 편의점, 맨션 등의 승강기나 주차장 등에서도 사고방지 또는 도난방지 등의 목적으로 감시카메라가 설치되는 사례가 급증하고 있다.

하지만 이러한 가두방범카메라시스템을 규율하기 위한 법률은 아직까지 존재하지 않는다. 감시카메라가 남설되고 있음에도 정작 주민들이나 쇼핑객들로부터는 거의 문제제기가 이루어지지 않고 있는 실정이지만, 일부의 언론이나 변호사, 시민단체 등으로부터 초상권이나 프라이버시권의 침해 가능성을 심각하게 우려하는 목소리가 터져 나오고 있다. 이에 따라 최근 일부 지방자치단체에서는 감시카메라의 적절한 규율을 위한 조례를 제정하여 시행하고 있다.

(3) 그러면 이하에서 최근 일본에서 이루어졌던 개인정보보호입법의 동향을 살펴보고(II), 민간부문과 공공부문의 일반법에 해당하는 개인정보보호법과 행정기관개인정보보호법의 주요내용을 소개하기로 한다(III). 그리고 이어서 CCTV의 설치, 운영에 관한 규제입법의 동향을 아울러 살펴보기로 한다(IV).

## II. 일본 개인정보보호법의 입법 동향

### 1. 통합 개인정보보호법의 제정 이전

(1) 1970년대의 소위 국민총등번호제(國民總背番号制)의 도입을 둘러싼 논란을 계기로 개인정보보호에 대한 국민적 관심은 크게 증대되었다. 이후 1975년 도쿄의 구니타치시(國立市)의 프라이버시보호조례가 제정되었고, 사회당의 「개인정보보호기본법안(요강)」과 「개인정보에 관련된 컴퓨터규제법안」 발표 등이 뒤를 이었다. 그리고 1980년에 채택된 OECD의 ‘프라이버시보호와 개인데이터의 국제유통에 대한 가이드라인에 관한 이사회권고’가 나오자, 이에 대한 중앙정부의 차원에서 대응책이 본격적으로 모색되기 시작하였다. 1981년 1월부터 행정관리청에 프라이버시보호연구회가 설치되었고, 1982년 7월에 ‘개인데이터

처리에 따른 프라이버시 보호대책'이라는 검토결과가 발표되었다.

이러한 상황을 거쳐서 마침내 1988년 4월 28일에 “행정기관이 보유하는 전자계산기 처리에 따른 개인정보의 보호에 관한 법률안”이 일련의 의회에 제출되었다. 이 법안에 대해서는 당초 정부 부처들 사이에 상당한 이견이 노출되었다. 당시 주무 부서인 우정성(郵政省)은 동법의 제정이 수상실의 권한을 강화할 것이라고 우려하였으며, 국민연금과 의료처치에 관한 개인 데이터를 보유하고 있는 후생성(厚生省)도 달갑지 않은 태도를 보였다. 그리고 국가경찰청은 범죄수사에 대한 개인기록의 적용이 제외되어 있었음에도 이 법안의 효과에 대해서 우려를 표명하고 나섰다.<sup>1)</sup> 하지만은 이 법안은 당시의 집권당인 자민당은 물론 야당들로부터 많은 지지를 얻어 의회를 통과하기에 이르렀다. 이어서 1988년 12월 16일에 「행정기관이 보유하는 전자계산기처리에 따른 개인정보의 보호에 관한 법률」로서 공포되었으며(법률 95호), 1989년 10월부터 부분적인 시행을 거쳐 1990년 10월부터 총무청(總務廳)을 주무관청으로 하여 전면 시행에 들어갔다.

하지만 동법은 1999년 12월 8일에 제1차 개정이 있었고(법률 제151호), 동년 동월 22일에 제2차 개정이 있었으며(법률 제160호), 2002년 7월 31일에 제3차 개정이 있었다(법률 제100호). 이 법률에 대해서는 개인정보보호를 위한 감시기능이 총무대신에게 집중되어 있을 뿐 별도의 중립적인 보호감독기관을 설치하지 않고 있다는 점, 개인정보의 수집에 대한 실질적 제한이 결여되어 있어 개인정보보호를 위한 사전적 장치가 미흡하다는 점, 개인정보의 신뢰성과 안전성을 확보하는 제도적 장치가 마련되지 않고 있다는 점, 개인정보의 이용에 대한 제한에 있어서 예외규정이 너무 광범위하다는 점, 데이터관리자인 공공기관의 책임자에 대한 처벌규정이 미비하다는 점 등이 문제점으로 지적

1) 이원부 등, “정보통신망에서의 개인정보 침해사례 분석 및 이용규제방안 연구”, 기술정책연구 98-6, 한국정보보호센터, 1998. 12. 93면 참조.

되었다.)<sup>2)</sup>

(2) 민간부문에 있어서는 개인정보보호에 관한 법규의 적용이 기업 활동에 지장을 줄 수 있다는 인식에 따라, 당초 정부는 민간부문을 규율하는 개인정보보호의 법안을 마련하는 데 소극적인 자세를 보여 왔다. 하지만 1989년에 이르러 통상산업성(通商産業省)이 □□민간부문에 있어서 전자계산기처리와 관련한 개인정보의 보호에 관한 지침□□을 채택한 바 있었다. 이후 정보기술의 발전 및 EU 수준으로 적절하게 개인정보를 보호하지 않는 국가에게로 개인정보의 이동을 금지하는 1995년의 EU지침의 제정 등 국내외의 환경변화로 1997년 3월에 통상산업성은 위 1989년의 지침을 □□민간부문에 있어서 전자계산기처리와 관련한 개인정보의 보호에 관한 가이드라인□□(1997. 3. 4. 통상산업성 고시 제98호)으로 개칭하고 그 내용을 대폭 수정·보완하여 공표하였다. 한편 우정성(郵政省)에서는 ‘정보통신사업에서의 개인데이터 보호지침(1991)’을 공표하기도 하였다.

민간부문에 의한 개인정보의 처리에 있어서 개인정보의 보호는 1997년 3월에 개정된 ‘민간부문에서의 전자계산기 처리에 관련된 개인정보 보호에 관한 가이드라인’에 기초하고 있었다. 일본의 각 사업자단체는 이 통산성의 가이드라인을 참고하여 자체적인 가이드라인을 제정하여 운영해왔다. 1997년 사이버산업연합회의 ‘사이버산업에서의 개인정보보호를 위한 가이드라인’, 1998년 3월 전자상거래실증추진협의회 ‘전자상거래에 있어서의 개인정보보호 가이드라인’ 등이 그것이다.

한편, EU지침에서 규정한 ‘적절한 개인정보보호 수준 확보’의 한 방안으로서 정부는 일본 산업규격인 개인정보보호규격(JIS Q 15001)을 1999년 3월 제정하여 개인정보의 보호에 관한 인식을 제고하기 위해

2) 권건보, “자기정보통제권에 관한 연구-공공부문에서의 개인정보보호를 중심으로”, 서울대학교 박사학위논문, 2004. 2. 180면.

노력하였다. 최근에는 EU 등 국제간 거래환경 조성을 위해 개인정보 보호의 중요성을 부각시키기 위한 다각적인 노력을 기울이고 있다. 그와 아울러 통상산업성 산하의 재단법인 일본정보처리개발협회에서는 1998년 4월 1일부터 ‘개인정보보호지침’을 근거로 하여 개인정보취급 관련 전 사업자를 대상으로 민간부문에서 자율적으로 개인정보보호를 위해 프라이버시마크제도를 시행해오고 있다. 그리고 우정성 산하 일본데이터통신협회에서도 개인정보보호등록센터를 개설하여 개인정보 보호 마크제도를 1998년 4월 30일부터 시행해왔다. 우정성은 통산성과는 달리 대상사업자를 전기통신사업자와 발신정보통지서비스(Number Display Service)의 사업용 이용자로 제한하여 마크를 부여하고 있다.

## 2. 통합 개인정보보호법의 제정과정

공공과 민간의 부문에 있어서의 개인정보보호를 위한 이와 같은 노력과는 별도로, 공공부문과 민간부문에 모두에 적용할 기본법을 제정하기 위한 움직임도 활발하게 전개되어 왔다. 특히 ‘고도정보통신사회 추진본부’ 산하에 설치된 개인정보보호연구회가 1999년 11월에 발표한 중간보고서에서는 i) 전 분야를 포괄하는 기본법을 제정하여 국민 모두에게 적용할 수 있는 원칙을 확립하고, ii) 신용정보·의료정보·전기통신 등 3가지 분야는 개별법을 제정하여 대응하며, iii) 보도·출판·학술·연구분야에 대해서는 원칙의 적용을 제외하는 방안이 검토되었다.<sup>3)</sup>

이후 정부의 정보통신기술(IT) 전략본부에 개인정보보호법법제화전문위원회가 설치되어 2000년 초부터 검토작업에 들어갔다. 이 위원회는 그간의 논의를 토대로 하여 같은 해 6월에 「개인정보보호기본법제

---

3) 박광진 등, “정보통신서비스에서의 개인정보보호에 관한 지침(안) 연구”, 기술정책 연구 99-2, 한국정보보호센터, 1999. 12. 9면.

에 관한 대강안(중간정리)』, 같은 해 10월 11일에 「개인정보보호기본 법제에 관한 대강』을 각각 공표하였다. 그 과정에서 가장 문제가 되었던 것은 표현의 자유의 일환으로서 헌법상 보장되는 취재 및 보도의 자유와의 관계였다. 大綱案의 중간정리에서는 “표현의 자유, 학문의 자유 등에 충분히 유의한다”고만 되어 있어서 표현의 자유를 침해한다는 야당, 언론, 시민단체 등의 강력한 반대에 부딪치게 되었다. 결국 보도기관에 대해서는 사업자의 업무에 관한 규정을 大綱의 적용에서 제외하기로 하였다.

이러한 과정을 거쳐 2001년 3월 27일에 「개인정보보호에 관한 법률안』이 국회에 제출되었고, 이에 대해 같은 해 가을의 임시국회에서 논의를 거듭하였다. 이듬해인 2002년 봄의 통상국회에서는 行政機關個人情報保護法, 獨立行政法人等個人情報保護法, 情報公開·個人情報保護審査會設置法, 整備法의 각 법안도 제출되었고, 이들을 포함한 개인정보보호관련 5법안이 계속 심의되었다. 그러나 이 5법안은 법률로서 성립되지 못하고, 결국 2002년 12월 임시국회가 종료되면서 폐안되고 말았다. 여기에는 부당한 미디어 규제를 초래한다는 언론매체를 중심으로 제기되었던 강한 반대론이 작용하였다.<sup>4)</sup>

이후 여당3당에 의해 그 수정안이 마련되어 2003년 통상국회에서 다시 입법화가 추진되었고, 마침내 2003년 5월 23일에 「개인정보의 보호에 관한 법률』(2003년 법률 제57호), 「행정기관이 보유하는 개인정보의 보호에 관한 법률』(2003년 법률 제58호), 「독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률』(2003년 법률 제59호), 「정보공개·개인정보보호 심사회 설치법』(2003년 법률 제60호), 「행정기관이 보유하는 개인정보의 보호에 관한 법률 등의 시행에 따른 관계법률의

4) 정상호, “일본 개인정보보호법 제정 추진동향”, 한국정보보호진흥원, 『해외정보보호동향』2003. 2. 13면; 황상철, “일본의 개인정보보호를 위한 입법동향 - 개인정보의 보호에 관한 법률안을 중심으로-”, 법제처, 『법제』2003. 1. 67면 등 참조.

정비 등에 관한 법률』(2003년 법률 제61호) 등 이른바 ‘개인정보보호 관련 5법’이 국회에서 성립되어 5월 30일 공포되기에 이르렀다.<sup>5)</sup>

### Ⅲ. 개인정보보호법의 체계와 주요 내용

#### 1. 전반적인 법의 체계

(1) 2003년 5월 23일 개인정보보호 관련 5개 법률의 제정 이후 일본은 공공부문과 민간부문을 포괄하는 기본법의 지위와 민간부문의 일반법의 지위를 가진 「개인정보의 보호에 관한 법률」(이하, ‘개인정보보호법’이라 한다.)을 두게 되었다. 그리고 공공부문을 규율하는 일반법으로 「행정기관이 보유하는 개인정보의 보호에 관한 법률」(이하, ‘행정기관개인정보보호법’이라 한다.)과 「독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률」(이하, ‘독립행정법인등 개인정보보호법’이라 한다.)이 존재한다. 지방자치단체에 있어서는 개인정보보호조례에 의해 규율이 이루어진다. 이러한 개인정보보호법제의 체계를 도표화하면 아래와 같다.<sup>6)</sup>

[ 체계도 ]

	공공부문			민간부문
	국가행정기관	독립행정법인, 특수법인 및 허가법인 등은 행정기관과 비슷하게 취급	지방공공단체	
기본법	[기본이념 등 기본법 부분] 개인정보보호법			
일반법	행정기관개인정보보호법	독립행정법인등개인정보보호법	개인정보보호조례	[개인정보취급사업자의 의무 등 일반법 부분]

5) 이상 園部逸夫, 個人情報保護法の解説, さよせい, 2003, 5-36면; 岡村久道, 新法解説 個人情報保護法入門, 商事法務, 2003, 65-71면 참조.

6) 岡村久道, 新法解説 個人情報保護法入門, 商事法務, 2003, 2면.

	정보공개·개인정보보호심사회설치법, ‘행정기관이 보유하는 개인정보의 보호에 관한 법률 등의 시행에 따른 관계법의 정비등에 관한 법률’		
개 별 법			전기통신사업법, 대금업법, 노동자과건법 등
	유전자기술규제법, 직업안정법 등		

이하에서는 민간부문과 공공부문에 있어서의 일반법적 지위를 가지는 개인정보보호법과 행정기관개인정보보호법을 중심으로 그 주요내용을 고찰하고, 이어서 지방자치단체의 개인정보보호에 관한 조례의 동향에 대해서 살펴본다.

## 2. 개인정보보호법의 주요 내용

동법은 제1장 총칙(제1조 내지 제3조), 제2장 국가와 지방공공단체의 책무(제4조 내지 제6조), 제3장 개인정보보호에 관한 시책 등(제7조 내지 제14조), 제4장 개인정보취급사업자의 의무 등(제15조 내지 제49조), 제5장 잡칙(제50조 내지 제55조), 제6장 벌칙(제56조 내지 제59조)으로 구성되어 있다.

### (1) 총 칙

#### 가. 목적과 기본이념

동법은 “고도정보통신사회의 진전에 수반해 개인정보의 이용이 현저하게 확대됨에 따라 개인정보의 적정한 취급과 관련하여 기본이념 및 정부에 의한 기본방침의 작성 기타의 개인정보보호에 관한 시책의 기본이 되는 사항을 정하여 국가 및 지방공공단체의 책무 등을 분명히 하는 동시에 개인정보를 취급하는 사업자가 준수해야 할 의무 등

을 정함으로써 개인정보의 유용성에 배려하면서 개인의 권리와 이익을 보호함”을 입법의 목적으로 내세우고 있다(제1조). 그리고 基本理念으로서 개인의 인격존중의 이념하에 개인정보를 신중하게 취급하고 그것을 적정하게 취급하도록 도모하여야 함을 밝히고 있다(제3조).

#### 나. 정 의

「개인정보」는 “생존하는 개인에 관한 정보로서 해당 정보에 포함되는 성명, 생년월일 기타의 기술 등에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 조합할 수 있어서 그에 의하여 특정의 개인을 식별할 수 있게 되는 것을 포함)”을 말한다(제2조 제1항).

「개인정보데이터베이스 등」은 “개인정보를 포함한 정보의 집합물”로서 특정의 개인정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것과 그 밖에 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로서 정령으로 정하는 것을 말한다(제2조 제2항).

「개인정보취급사업자」는 “개인정보데이터베이스 등을 사업의 용도로 제공하고 있는 사람”을 말하며, 국가기관이나 지방공공단체, 독립행정법인 등은 이에서 제외된다(제2조 제3항).

#### (2) 국가와 지방공공단체의 책무 등 (제4조 내지 제6조)

- 국가행정기관, 독립행정법인 등이 보유하는 개인정보의 적정한 취급을 확보하기 위한 법제상의 조치 등을 강구할 의무
- 개인정보의 성질 및 이용방법에 따라 특히 적정한 취급의 엄격한 실시를 확보할 필요가 있는 각별한 조치 및 개인정보에 대한 법제상의 조치 등을 강구할 의무

### (3) 개인정보보호에 관한 시책 등

#### 가. 개인정보보호에 관한 기본방침(제7조)

- 시책의 종합적·일체적 추진을 도모하기 위한 기본방침을 국민생활심의회의 의견을 들은 다음 閣議가 결정

#### 나. 국가의 시책(제8조 내지 제10조)

- 지방공공단체 등에 대한 지원, 고충처리에 필요한 조치 등

#### 다. 지방공공단체의 시책(제11조 내지 제13조)

- 지방공공단체가 보유하는 개인정보에 대한 필요한 조치
- 구역내의 사업자 및 주민에 대한 지원, 고충처리의 알선 등 필요한 조치

#### 라. 국가 및 지방공공단체의 협력(제14조)

### (4) 개인정보 취급 사업자의 의무 등

#### 가. 개인정보 취급 사업자의 의무

개인정보보호의 원칙을 대체로 반영하고, 정보주체의 통제권을 강화하였다. 하지만 수집제한의 원칙, 즉 당사자의 동의에 의한 수집이나 필요최소한의 수집 등에 관한 원칙을 명시하지는 않았다. 수집제한의 원칙을 명문화할 경우 개인정보의 활용에 대한 민간업계의 수요를 배려하기 위한 것으로 파악된다.

#### 1) 이용목적의 특정

개인정보를 취급함에 있어서 그 이용 목적을 가능한 한 특정하여야 하며(제15조 제1항), 이용 목적을 변경하는 경우에는 변경전의 이용 목

적과 상당한 연관성이 있다고 합리적으로 인정되는 범위를 초과해서 변경하여서는 안 된다(제15조 제2항).

## 2) 이용목적에 의한 제한

- 미리 동의를 얻지 않고서는 특정된 이용목적의 달성에 필요한 범위를 넘어서 개인정보를 취급해서는 안 된다(제16조 제1항).
- 합병 기타의 사유에 의해 다른 개인정보취급사업자로부터 사업을 승계함에 따라 개인정보를 취득한 경우에는 미리 본인의 동의를 얻지 않고서는 승계 이전의 당해 개인정보의 이용목적의 달성에 필요한 범위를 넘어서 당해 개인정보를 취급하여서는 안 된다(제16조 제2항).
- 다만, ①법령에 근거한 경우, ②사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서 본인의 동의를 얻는 것이 곤란한 경우, ③공중위생의 향상 또는 아동의 건전한 육성의 추진을 위해 특히 필요가 있는 경우로서 본인의 동의를 얻는 것이 곤란한 경우, ④국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서 본인의 동의를 얻음으로써 당해 사무의 수행에 지장을 줄 우려가 있는 경우는 예외로 한다(제16조 제3항).

## 3) 적정한 취득

개인정보취급사업자는 허위 기타 부정한 수단에 의해 개인정보를 취득하여서는 안 된다(제17조).

## 4) 취득시 이용목적의 통지 등

- 개인정보를 취득한 경우에는 미리 그 이용목적의 공표하고 있는 경우를 제외하고는, 신속히 그 이용목적의 본인에게 통지하거나 공표하여야 한다(제18조 제1항).

- 본인과 의 사이에 계약을 체결함에 따라 계약서 기타의 서면에 기재된 당해 본인의 개인정보를 취득하는 경우 기타 본인으로부터 직접 서면에 기재된 당해 본인의 개인정보를 취득하는 경우에는 미리 본인에 대해 그 이용목적 을 명시하여야 한다. 다만 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급히 필요가 있는 경우에는 그러하지 아니하다(제18조 제2항).

5) 데이터 내용의 정확성과 최신성 확보

이용목적의 달성에 필요한 범위 내에서 개인데이터를 정확하고, 최신의 내용으로 유지되도록 노력하여야 한다(제19조).

6) 안전관리조치, 종업원·위탁처의 감독

- 개인데이터의 안전관리를 위해 필요하고 적절한 조치, 종업원·위탁처에 대한 필요하고 적절한 감독(제20조 내지 제22조)

7) 제3자 제공의 제한

- 미리 본인의 동의를 얻지 않고서는 개인데이터를 제3자에게 제공하여서는 안 된다. 다만 ①법령에 근거한 경우, ②사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서 본인의 동의를 얻는 것이 곤란한 때, ③공중위생의 향상 또는 아동의 건전한 육성의 추진을 위해 특히 필요가 있는 경우로서 본인의 동의를 얻는 것이 곤란한 때, ④국가기관 혹은 지방자치단체 또는 그 위탁을 받은 자가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서 본인의 동의를 얻음으로써 당해 사무의 수행에 지장을 줄 우려가 있는 때는 예외로 한다(제23조 제1항).
- 제3자에게 제공되는 개인데이터에 대하여 본인의 요청이 있으면 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지하는 것

으로 하고 있는 경우에는 ①제3자 제공을 이용목적으로 한다는 점, ②제3자에게 제공되는 개인정보의 항목, ③제3자 제공의 수단 또는 방법에 대하여 미리 본인에게 통지하거나 또는 본인이 용이하게 알 수 있는 상태에 두고 있는 때에는 당해 개인정보를 제3자에게 제공할 수 있다(제23조 제2항). 만일 제3자에게 제공되는 개인정보의 항목과 제3자 제공의 수단 또는 방법에 해당하는 사항을 변경하는 경우에는 변경하는 내용에 대해 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다(제23조 제3항).

- 위탁의 경우, 합병 등의 경우, 특정인과의 공동이용의 경우(공동이용하는 취지 기타 일정한 사항의 통지 등을 하고 있는 경우)는 제3자 제공으로 간주하지 않는다(제23조 제4항).

#### 8) 보유개인데이터에 관한 사항의 공표 등

- 보유개인데이터에 관해서 일정한 사항(성명이나 명칭, 이용목적, 개시나 정정 등에 필요한 절차 등)에 대하여 본인이 알 수 있는 상태에 두어야 한다(제24조 제1항).
- 본인으로부터 당해 본인의 식별이 가능한 보유개인데이터의 이용목적의 통지를 요청받은 때에는 원칙적으로 본인에 대하여 지체 없이 그것을 통지하여야 한다(제24조 제2항).

#### 9) 이용목적통지요구, 개시·정정·이용정지 등의 청구

- 이용목적통지요구권 : 정보주체는 개인정보취급사업자에 대하여 본인 식별이 가능한 보유개인데이터의 利用目的을 通知해줄 것을 要求할 수 있고, 사업자는 지체 없이 통지하여야 한다(제24조 제2항 본문).
- 개시청구권 : 정보주체는 개인정보취급사업자에 대하여 본인 식별이 가능한 보유개인데이터의 開示를 請求할 수 있고, 사업자는 정

령으로 정하는 방법에 따라 지체 없이 그에 응하여야 한다. 다만 ①본인 또는 제3자의 생명, 신체, 재산 기타의 권리의익을 해할 우려가 있는 경우, ②당해 개인정보취급사업자의 업무의 적정한 실시 에 현저한 지장을 줄 우려가 있는 경우, ③다른 법령에 위반하는 것이 되는 경우에는 그 전부 또는 일부를 개시하지 않을 수 있다 (제25조 제1항).

- 정정·추가·삭제청구권 : 정보주체는 개인정보취급사업자에 대하여 본인 식별이 가능한 보유개인데이터의 내용이 사실과 다른 경우에는 그 내용의 訂正, 追加 또는 削除를 要求할 수 있고, 이 경우 사업자는 이용목적의 달성에 필요한 범위 내에서 지체 없이 필요한 조사를 행하고 그 결과에 기초해서 변경하여야 한다(제26조 제1항).
- 이용정지·소거청구권 : 정보주체는 개인정보취급사업자가 특정된 이용목적 범위내에서의 취급의무 또는 정당한 방법에 의한 개인정보 수집의무를 위반했다는 이유로 당해 보유개인데이터의 利用停止 또는 消去를 要求할 수 있고, 사업자는 그 청구가 이유 있는 때에는 위반을 시정하기 위하여 필요한 한도 내에서 지체 없이 이용정지 또는 소거를 하여야 한다. 다만 이용정지 또는 소거에 다액의 비용이 드는 경우 등 그것이 곤란한 경우에 정보주체의 권리의익의 보호에 필요한 대상조치를 취한 때에는 그러하지 아니하다(제27조 제1항). 정보주체는 개인정보취급사업자가 정보주체의 사전 동의 없는 제3자 제공 금지의무를 위반했다는 이유로 당해 보유개인데이터의 제3자 제공의 정지를 요구할 수 있고, 사업자는 그 청구가 이유 있는 때에는 제3자 제공을 정지하여야 한다(제27조 제2항 본문).

#### 10) 고충의 처리(제31조)

- 개인정보 취급에 관한 고충의 적절하고 신속한 처리

11) 주무대신의 관여(제32조 내지 제35조)

- 이 절의 규정의 시행에 필요한 한도에 있어서의 보고의 징수, 필요한 조언
- 개인정보취급사업자가 의무규정(노력의무 제외)에 위반해, 개인의 권리의 보호를 위해 필요가 있는 경우에 있어서의 권고, 권고에 따르지 않는 일정한 경우의 명령 등
- 주무대신의 권한의 행사의 제한(표현, 학문, 신교, 정치 활동의 자유)

12) 주무대신(제36조)

- 개인정보취급사업자가 실시하는 사업 등의 소관대신, 규정의 원활한 실시를 위해서 필요가 있을 때는 내각총리대신이 지정

나. 민간단체에 의한 개인정보보호의 추진

1) 단체의 인정(제37조), 대상 사업자(제41조)

- 개인정보취급사업자의 개인정보의 적정한 취급 확보를 목적으로 하고, 고충의 처리 등을 실시하려고 하는 단체의 인정
- 인정단체에 의한 대상사업자(단체의 구성원등)의 이름 또는 명칭의 공표

2) 개인정보보호지침(제43조)

- 인정단체에 의한 개인정보보호지침의 작성·공표

3) 주무대신의 관여(제46조 내지 제48조)

- 이 절의 규정의 시행에 필요한 한도에 있어서의 보고의 수령
- 업무의 실시의 방법의 개선, 개인정보보호지침의 변경 등에 대한 명령

- 인정기준에 적합하지 않게 되었을 경우, 명령에 따르지 않는 경우 등에 있어서의 인정 취소

#### 4) 주무대신(제49조)

- 대상 사업자가 실시하는 사업 등의 소관대신, 규정의 원활한 실시를 위해서 필요가 있을 때는 내각총리대신이 지정

#### 5) 적용제외

- 보도, 저술, 학술연구, 종교활동, 정치활동 등에 제공할 목적으로 개인정보를 취급하는 보도기관, 저술업자, 학술연구기관, 종교단체, 정치단체 등에 대해서는 제4장(제15조 내지 제49조)의 적용을 제외(제50조 제1항)
- 이들 주체는 안전관리, 고충처리 등을 위해서 필요한 조치를 스스로 강구해 그 내용을 공표하도록 노력(제50조 제3항)

#### 6) 벌 칙

- 개인정보 취급 사업자가 주무 대신의 명령에 위반했을 경우 등에 있어서의 벌칙(제56조 내지 제59조)

#### 7) 평 가

이 개인정보보호법은 공공부문 및 민간부문을 모두 규율하는 이 법률은 개인정보보호에 관한 기본법이자, 민간부분에 있어서의 일반법이라고 할 수 있다.<sup>7)</sup> 민간부분에 관한 법제의 미비로 인해 개인정보의 침해에 충분히 대처하지 못한다는 지적에 따라 입법이 이루어진 것인 만큼, 향후 이 입법에 거는 기대가 매우 크다고 할 수 있다.

---

7) 岡村久道, 앞의 책, 2면 [圖表 1] 참조.

하지만 논의의 단계에서 적용배제의 범위가 넓어졌고, 정보통신 관련 업계의 보호육성 논리에 부닥쳐 자율적 규제에 틀을 크게 훼손하지 않으려 애쓴 흔적이 곳곳에서 드러난다. 전반적으로 그러한 방향의 설정은 바람직하다고 하겠으나, 그렇다고 하여 개인정보의 보호를 위한 법률로서의 성격을 잃게 될 정도가 되어서는 곤란할 것이다. 이러한 관점에서 일본에서도 동법이 개인정보의 활용을 위한 법률로 변질되었다는 비판이 벌써부터 제기되고 있다.

앞으로 이 법률의 시행경과를 예의주시하면서, 우리 통합기본법제의 제정과 정비에 참고를 해나가야 할 것이다.

### 3. 행정기관개인정보보호법의 주요 내용

행정기관개인정보보호법은 “행정기관에 대해 개인정보의 이용이 확대되고 있음에 따라 행정기관에 있어서의 개인정보 취급에 관한 기본적인 사항을 정함으로써 행정의 적정과 원활한 운영을 꾀하면서 개인의 권리이익을 보호함”을 입법의 목적으로 제시하고 있다. 그리고 이 법률에 의하여 1988년에 공포되었던 『행정기관이 보유하는 전자계산기 처리에 따른 개인정보의 보호에 관한 법률』이 전면 개정되었다. 하지만 행정기관개인정보보호법은 공포일(2003년 5월 30일)을 기준으로 2년을 넘지 않는 범위내에서 政令으로 정하는 날로부터 시행된다.

#### (1) 구 성

동법은 제1장 총칙(제1조 내지 제2조), 제2장 행정기관에 있어서의 개인정보 취급(제3조 내지 제9조), 제3장 개인정보 파일(제10조 내지 제11조), 제4장 개시·정정 및 이용정지(제12조 내지 제44조), 제5장 잡칙(제45조 내지 제52조), 제6장 벌칙(제53조 내지 제57조)으로 구성되어 있다.

## (2) 적용범위

1) 전자계산기에 의해 처리되는 개인정보에 한하여 적용되던 개정전의 법률과 달리, 동법에서는 手作業 또는 인쇄매체 등에 의하여 작성·처리되는 개인정보도 적용대상이 될 수 있다.

2) 그리고 동법상의 행정기관에는 법률의 규정에 기하여 내각에 설치되는 기관 및 내각 산하에 설치되는 기관, 내각부, 궁내청 및 내각부설치법 제49조 제1항 및 제2항에 규정된 기관, 국가행정조직법 제3조 제2항에 규정된 기관, 내각부설치법 제39조 및 제55조 및 궁내청법 제16조 제2항의 기관 및 내각부설치법 제40조 및 제56조의 특별기관 가운데 政令에서 정한 것, 국가행정조직법 제8조의2의 시설등기관 및 동법 제8조의3의 특별기관으로서 政令에서 정한 것, 회계심사원이 포함된다(제2조 제1항). 따라서 행정기관개인정보보호법은 국가의 행정기관에 대해서만 적용될 뿐이고, 독립행정법인등이나 지방공공단체는 별도의 독립행정법인등 개인정보보호법이나 독자적으로 제정한 개인정보보호에 관한 조례의 적용을 받는다. 따라서 동법은 국가의 행정기관을 적용대상으로 하는 일반법으로서의 지위를 가진다.<sup>8)</sup>

3) 동법상 「개인정보」는 “생존하는 개인에 관한 정보로서 해당 정보에 포함되는 성명, 생년월일 기타의 기술 등에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 조합할 수 있어서 그에 의하여 특정의 개인을 식별할 수 있게 되는 것을 포함)”을 말하고(제2조 제2항), 「보유개인정보」는 “행정기관의 직원이 직무상 작성하거나 취득한 개인정보로서 당해 행정기관의 직원이 조직적으로 이용하는 것으로 당해 행정기관이 보유하고 있는 것”을 말한다(제2조 제3항). 그

---

8) 岡村久道, 앞의 책, 3頁.

리고 「개인정보파일」은 “보유개인정보를 포함한 정보의 집합물”로서 일정한 사무의 목적을 달성하기 위하여 특정의 개인정보를 전자계산기를 이용하여 검색할 수 있거나 그 밖에 일정한 사무의 목적을 달성하기 위하여 성명, 생년월일, 기타의 기술 등에 의하여 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것을 말한다(제2조 제4항). 따라서 자연인으로서 현재 생존하고 있는 개인에 관한 정보만 본법의 보호대상이 되고, 이미 사망한 자나 법인 기타의 단체에 관한 정보는 보호의 대상이 될 수 없다.

4) 한편, 개정전의 법률 제3조에 의하면 統計法 제2조에 규정하는 指定統計를 작성하기 위하여 수집된 개인정보, 동법 제8조 제1항의 규정에 의하여 總務大臣에게 제출된 統計調査에 의하여 수집된 개인정보, 統計報告調整法の 규정에 의하여 총무대신의 승인을 받은 統計報告의 徵集에 의하여 얻은 개인정보는 적용대상에서 제외되었다. 하지만 최근의 개정법에서는 이러한 규정을 두지 않고, 다만 오로지 통계의 작성 또는 학술연구의 목적을 위하여 보유개인정보를 제공할 때에는 본인 또는 제3자의 권리이익을 부당하게 침해할 우려가 있다고 인정되지 않는 한도에서 그 이용목적 이외의 목적을 위하여 보유개인정보를 제공할 수 있도록 하고 있을 뿐이다(제8조 제2항).

한편, 개정법에서는 개시·정정 및 이용정지에 관한 제4장의 규정을 적용대상에서 제외하는 규정을 신설하였다. 제4장의 적용이 배제되는 사항들로 형사사건 혹은 소년보호사건과 관련되는 재판, 검찰관, 검찰사무관 혹은 사법경찰직원이 실시하는 처분, 형벌 혹은 보호처분의 집행, 갹생긴급보호 또는 사면과 관련되는 보유개인정보(당해 재판, 처분 혹은 집행을 받은 사람, 갹생긴급보호의 신청을 한 사람 또는 사면의 진언이 있던 사람과 관련된 것에 한함) 등이 열거되어 있다(제45조 제1항).

### (3) 개인정보 취급의 원칙

#### 1) 보유의 제한 등

행정기관은 법령이 정하는 소관사무를 수행하는 데 필요한 경우에 한하여 개인정보를 보유할 수 있으며, 그 이용의 목적은 가능한 한 특정되어야 한다(제3조 제1항). 이렇게 특정된 이용목적의 달성에 필요한 범위를 초과하여 개인정보를 보유해서는 안 되며(제3조 제2항), 이용 목적을 변경하는 경우에는 변경전의 이용목적과 상당한 관련성을 가진다고 합리적으로 인정되는 범위를 초과하여서는 안 된다(제3조 제3항).

#### 2) 이용목적의 명시

행정기관은 본인으로부터 직접 서면(전자적 기록 포함)에 기록에 기록된 당해 본인의 개인정보를 취득할 때에는 미리 본인에 대해 그 이용 목적을 명시하여야 한다(제4조 본문). 다만 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급하게 필요한 경우, 이용 목적을 본인에게 명시함으로써 본인 또는 제3자의 생명, 신체, 재산 기타의 권리의익을 해칠 우려가 있는 경우, 이용 목적을 본인에게 명시함으로써 국가기관, 독립행정법인등 또는 지압공공단체가 실시하는 사무 또는 사업의 적정한 수행에 지장을 미칠 우려가 있을 경우, 취득상황에 비추어 볼 때 이용 목적이 분명하다고 인정될 경우에는 그러하지 아니하다(제4조 제1호 내지 제4호).

#### 3) 정확성과 안전성의 확보

행정기관의 장은 이용 목적의 달성에 필요한 범위 내에서 보유 개인정보가 과거 또는 현재의 사실과 합치되도록 노력하여야 하고(제5조), 보유 개인정보의 누설, 멸실 또는 피해의 방지 기타 보유 개인정보의 적절한 관리를 위하여 필요한 조치를 강구하여야 한다(제6조 제1항).

#### 4) 이용 및 제공의 제한

개인정보의 취급에 종사하는 행정기관의 직원이나 직원이었던 자 혹은 그 수탁업무에 종사하고 있는 자나 종사하였던 자는 그 업무에 관하여 지득한 개인정보의 내용을 함부로 타인에게 알려주거나 부당한 목적으로 이용하여서는 안 된다(제7조).

그리고 행정기관의 장은 법령에 근거하는 경우를 제외하고 이용목적 이외의 목적을 위해 보유개인정보를 스스로 이용하거나 제공하여서는 안 된다(제8조 제1항). 다만 행정기관의 장이 본인의 동의가 있거나 본인에게 제공할 때, 행정기관이 법령이 정하는 소관사무의 수행에 필요한 한도로 보유개인정보를 내부적으로 이용하는 경우로서 당해 보유개인정보를 이용하는 것에 상당한 이유가 있다고 인정할 때, 다른 행정기관, 독립행정법인등 또는 지방공공단체에 보유개인정보를 제공하는 경우에 있어서 보유개인정보의 제공을 받는 자가 법령이 정하는 사무 또는 업무의 수행에 대하여 상당한 이유가 있다고 인정될 때, 오로지 통계의 작성 또는 학술연구의 목적을 위하여 보유개인정보를 제공할 때, 본인 이외의 사람에게 제공하는 것이 분명하게 본인의 이익이 된다고 인정될 때, 기타 보유 개인정보를 제공하는 것에 대하여 특별한 이유가 있을 때에 해당한다고 인정될 때에는 이용목적 이외의 목적을 위해 보유개인정보를 스스로 이용하거나 제공할 수 있다. 다만 그로 인하여 본인 또는 제3자의 권리의익을 부당하게 침해할 우려가 있다고 인정될 때에는 그러하지 아니하다(제8조 제2항).

그리고 행정기관의 장은 다른 행정기관, 독립행정법인등 또는 지방공공단체에 보유개인정보를 제공하는 경우에 있어서 보유개인정보의 제공을 받는 자가 법령이 정하는 사무 또는 업무의 수행에 대하여 상당한 이유가 있다고 인정하여 제공할 때나 혹은 그 밖에 오로지 통계의 작성 또는 학술연구의 목적을 위하여 보유개인정보를 제공할 때에는

필요하다고 인정할 경우 보유개인정보의 제공을 받는 자에 대하여 제공과 관련되는 개인정보에 대해 그 이용의 목적 또는 방법의 제한 기타 필요한 제한을 붙이거나 혹은 그 누설의 방지 기타 개인정보의 적절한 관리를 위해 필요한 조치를 강구하도록 요구하여야 한다(제9조).

#### 5) 공개의 제한

행정기관개인정보보호법에서는 본인에 대한 열람만을 규정하고, 일반인에 대한 개인정보의 공개는 정보공개법에서 규율하고 있다. 1999년 5월 14일에 제정된 「행정기관이 보유하는 정보의 공개에 관한 법률」은 개인정보가 不開示情報에 해당한다고 하면서도, 공익상의 이유에 의한 재량적 개시를 허용하고 부분개시에 관한 규정을 두어 본인의 사익과 공익 사이의 절충을 도모하고 있다.

#### (4) 보유의 통지와 공표

개인정보처리에 대한 효과적인 감독과 통제를 위하여 책임 있는 기관이 개인정보의 보유현황을 파악할 수 있도록 개인정보의 보유자나 보유기관에게 대해 각종의 의무를 부과하기도 한다. 영국의 신고와 등록제도, 독일의 신고제도, 프랑스의 허가과 신고제도, 일본의 사전통지 등이 여기에 해당된다. 한편, 미국의 공고제도와 같이 국민들이 공공기관의 개인정보 처리개요를 가늠할 수 있도록 일정한 사항을 일반에게 공개하도록 하는 경우가 있다. 이는 개인정보보유상황을 공개함으로써 국민들의 부단한 감시를 받도록 하는 동시에 국민들이 자신에 관한 정보에 대한 접근권의 행사를 용이하게 해주는 측면이 있다. 일본의 공표제도 역시 이러한 취지에서 규정되고 있다. 다만 한편 2003년의 법개정이 있기 이전에는 총무대신으로 하여금 통지받은 개인정보과일을 관보에 공시하도록 하는 규정도 두고 있었으나, 2003년 개정법에서는 이러한 공시제도는 폐지되었다.

## 1) 개인정보파일의 보유 등에 관한 사전통지

행정기관이 개인정보파일을 보유하고자 하는 때에는 당해 행정기관의 장은 미리 일정한 사항(개인정보파일의 명칭, 보유기관의 명칭 및 개인정보파일의 이용에 제공되는 사무를 주관하는 조직의 명칭, 개인정보파일의 이용목적, 기록항목 및 기록범위, 기록정보, 기록정보를 당해 행정기관 이외의 자에게 상시적으로 제공하는 경우 그 제공처 등)을 총무대신에게 通知하여야 한다. 통지한 사항을 변경할 때에도 마찬가지이다(제10조 제1항). 다만, 일정한 개인정보파일<sup>9)</sup>에 대해서는 통지의무의 예외가 인정된다(제6조 제2항). 행정기관의 장은 제1항에 규정하는 사항을 통지한 개인정보파일에 대해 당해 행정기관이 보유를 그만두었을 때 혹은 그 개인정보파일이 본인의 수가 정령으로 정하는 수에 미달하는 경우에 해당하게 되었을 때에는 지체 없이 총무대신에게 그 취지를 통지하여야 한다(제10조 제3항).

## 2) 개인정보파일부의 작성 및 공표

행정기관의 장은 정령으로 정하는 바에 따라 당해 행정기관이 보유하고 있는 개인정보파일에 대해 일정한 사항(개인정보파일의 명칭, 보유기관의 명칭 및 개인정보파일의 이용에 제공되는 사무를 주관하는 조직의 명칭, 개인정보파일의 이용목적, 기록항목 및 기록범위, 기록정보, 기록정보를 당해 행정기관 이외의 자에게 상시적으로 제공하는 경우 그 제공처 등)을 기재한 개인정보파일부를 작성해 公表하여야 한

---

9) 국가안전·외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일, 범죄의 수사, 공소의 제기나 유지를 위하여 작성 또는 취득한 개인정보파일, 행정기관의 직원에 대한 인사·급여 등에 관한 기록, 오로지 시험적인 전자계산기처리의 용도에 제공하기 위한 개인정보파일, 1년 이내에 소거할 목적으로만 작성된 개인정보파일, 업무상 필요한 연락을 위하여 작성된 주소·성명 등, 자기의 직무수행을 위한 보유기관의 내부자료로 작성된 것, 처리정보를 학술연구의 목적으로만 사용되는 것, 기타 정령으로 정하는 것 등.

다(제11조 제1항). 그러나 사전통지의무가 면제되는 개인정보파일, 제1항의 규정에 의한 공표와 관련되는 개인정보파일에 기록되어 있는 기록정보의 전부 또는 일부를 기록한 개인정보파일로서 그 이용목적, 기록항목 및 기록범위가 당해 공표와 관련되는 그 사항의 범위에 속하는 것 등에 대해서는 공표의무가 면제된다(제11조 제2항). 그리고 제1항의 규정에도 불구하고 행정기관의 장은 기록항목의 일부 또는 기록정보 혹은 기록정보를 당해 행정기관 이외의 자에게 상시적으로 제공하는 경우 그 제공처를 개인정보파일부에 기재하거나 혹은 개인정보파일을 개진정보파일부에 게재함으로써 이용목적과 관련되는 사무의 성질상 당해 사무의 적정한 수행에 지장을 미칠 우려가 있다고 인정할 때는 그 기록항목의 일부 혹은 사항을 기재하지 않거나 그 개인정보파일을 개인정보파일부에 게재하지 않을 수 있다(제11조 제3항).

#### (5) 정보주체의 통제권

종래의 공공기관개인정보보호법에서는 개시와 정정에 관한 규정만 두고 있었으나, 2003년의 개정법은 제4장에서 개시, 정정 및 이용정지, 불복신청에 관해 자세한 규정을 두고 있다.

##### 1) 개시청구권

누구든지 본법이 정하는 바에 따라 행정기관의 장에 대해 당해 행정기관이 보유하는 자기를 본인으로 하는 보유개인정보의 開示를 請求할 수 있다(제12조 제1항). 개시청구를 하려면 개시청구서를 행정기관의 장에게 제출해야 하는데(제13조 제1항), 이 경우 개시청구자는 정령으로 정하는 바에 따라 개시청구와 관련되는 보유개인정보가 본인의 것임을 나타내는 서류를 제시하거나 제출하여야 한다(제13조 제2항). 개시청구서에 형식상의 미비가 있다고 인정할 때에는 행정기관의 장은 개시청구자에 대하여 상당한 기간을 정하여 그 보정을 요구할

수 있으며, 이 경우 행정기관의 장은 개시청구자에 대해 보정에 참고가 되는 정보를 제공하도록 노력해야 한다(제13조 제3항).

개시청구가 있으면 행정기관의 장은 不開示情報<sup>10)</sup>에 해당하는 경우가 아닌 한 개시청구자에게 당해 보유개인정보를 개시하여야 한다(제14조).

행정기관의 장은 개시청구와 관련되는 보유개인정보에 불개시정보가 포함되어 있는 경우 불개시정보에 해당하는 부분을 용이하게 구분해 제외할 수가 있을 때에는 개시청구자에게 당해 부분을 제외한 부

---

10) ①개시청구자의 생명, 건강, 생활 또는 재산을 해칠 우려가 있는 정보, ②개시청구자 이외의 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 생년월일 기타의 기술등에 의해 개시청구자 이외의 특정의 개인을 식별할 수가 있는 것 또는 개시청구자 이외의 특정의 개인을 식별할 수는 없지만 개시함으로써 개시청구자 이외의 개인의 권리이익을 해칠 우려가 있는 것(다만, 1.법령의 규정에 의해 또는 관행으로서 개시청구자가 알 수가 있거나 아는 것이 예정되어 있는 정보, 2. 사람의 생명, 건강, 생활 또는 재산을 보호하기 위해 개시하는 것이 필요하다고 인정되는 정보, 3.당해 개인이 공무원등인 경우 당해 정보가 그 직무의 수행과 관련되는 정보일 경우에 있어서 당해 정보 가운데 당해 공무원등의 직 및 당해 직무수행의 내용과 관련되는 부분은 불개시의 대상에서 제외된다), ③법인 기타의 단체에 관한 정보 또는 개시청구자 이외의 사업을 영위하는 개인의 당해 사업에 관한 일정한 정보(1.개시로 인하여 당해 법인등 또는 당해 개인의 권리, 경쟁상의 지위 기타 정당한 이익을 해칠 우려가 있는 것, 2.행정기관의 요청을 받아 개시하지 않을 것을 조건으로 임의로 제공된 것으로서 법인등 또는 개인의 경우 통상적으로 개시하지 않는 것으로 되어 있거나 기타 당해 조건을 교부하는 것이 당해 정보의 성질, 당시의 상황 등에 비추어 합리적이라고 인정되는 것), ④개시로 인하여 국가의 안전이 저해될 우려 또는 타국이나 국제기관과의 신뢰관계가 손상될 우려 또는 타국이나 국제기관과의 교섭상 불이익을 입을 우려가 있다고 행정기관의 장이 인정함에 있어 상당한 이유가 있는 정보, ⑤개시로 인하여 범죄의 예방, 진압 또는 수사, 공소의 유지, 형의 집행 기타 공공의 안전과 질서의 유지에 지장을 미칠 우려가 있다고 행정기관의 장이 인정함에 상당한 이유가 있는 정보, ⑥국가기관, 독립행정법인등 및 지방공공단체의 내부 또는 상호간에 있어서의 심의, 검토 또는 협의에 관한 정보로서 개시로 인하여 솔직한 의견의 교환이나 의사결정의 중립성이 부당하게 훼손될 우려 또는 국민 사이에 혼란을 일으키게 할 우려 또는 특정인에게 부당하게 이익을 주거나 불이익을 미칠 우려가 있는 것, ⑦국가기관, 독립행정기관등 또는 지방공공단체가 실시하는 사무 또는 사업에 관한 정보로서 개시로 인하여 당해 사무 또는 사업의 성질상 당해 사무 또는 사업의 적정한 수행에 지장을 미칠 우려가 있는 것(제14조 제1호 내지 제7호).

분에 대해 개시하여야 한다(제15조 제1항).

한편, 행정기관의 장은 개시청구와 관련되는 보유개인정보에 불개시 정보가 포함되어 있는 경우에도 개인의 권리이익을 보호하기 위하여 특히 필요가 있다고 인정할 때에는 개시청구자에게 당해 보유개인정보를 개시할 수 있다(제16조).

행정기관의 장은 보유개인정보의 전부 또는 일부를 개시할 때 그 취지의 결정을 하여 개시청구자에게 그 취지, 개시하는 보유개인정보의 이용목적 등을 서면에 의해 통지하여야 하고, 그 전부를 개시하지 않을 경우에는 개시하지 않는 취지의 결정을 하여 개시청구자에게 그 취지를 서면에 의해 통지하여야 한다(제18조).

개시청구와 관련되는 보유개인정보에 제3자에 관한 정보가 포함되어 있을 때에는 행정기관의 장은 개시결정 등을 함에 있어서 당해 정보와 관련되는 제3자에게 그 제3자에 관한 정보의 내용 등을 통지하고 의견서를 제출할 기회를 주어야 한다(제23조 제1항). 행정기관의 장은 의견서제출의 기회가 부여된 제3자가 당해 제3자에 관한 정보의 개시에 반대의 의사를 표시한 의견서를 제출하였음에도 개시결정을 할 경우 개시결정일과 개시실시일 사이에 적어도 2주간의 간격을 두어야 하며, 이 경우 행정기관의 장은 개시결정 후 즉시 당해 의견서를 제출한 제3자에게 개시결정을 한 취지 및 그 이유 및 개시실시일을 서면에 의해 통지하여야 한다(제23조 제3항).

## 2) 정정청구권

누구든지 자기를 본인으로 하는 보유개인정보의 내용이 사실이 아니라고 생각할 때에는 본법이 정하는 바에 따라 당해 보유개인정보를 보유하는 행정기관의 장에게 당해 보유개인정보의 訂正(追加 또는 削除를 포함)을 請求할 수 있다. 다만, 이러한 정정청구의 대상이 되는 보유개인정보는 개시결정에 기하여 개시를 받은 것, 사안이송시의 개

시결정에 기하여 개시를 받은 것, 개시결정과 관련되는 것으로서 다른 법령의 규정에 의해 개시를 받은 경우에 한한다(제27조). 정정청구는 정정청구서를 행정기관의 장에게 제출하는 방식으로 해야 하며, 정정청구자는 정정청구와 관련되는 보유개인정보의 본인인 것을 나타내는 서류를 제시하거나 제출하여야 한다(제28조 제1항 및 제2항).

정정청구가 있으면 행정기관의 장은 당해 정정청구에 이유가 있다고 인정할 경우 당해 정정청구와 관련되는 보유개인정보의 이용목적의 달성에 필요한 범위내에서 당해 보유개인정보의 정정을 하여야 한다(제29조).

정정을 할 때에는 그 취지의 결정을 하여 정정청구자에게 그 취지를 서면에 의해 통지하여야 하고, 정정하지 않을 때에는 그 취지의 결정을 하여 역시 그 취지를 서면통지하여야 한다(제30조).

정정결정에 기하여 정정을 하였을 경우 필요가 있다고 인정할 때에는 당해 보유개인정보의 제공처에 대해 지체없이 그 취지를 서면에 의해 통지하여야 한다(제35조).

### 3) 이용정지청구권

누구든지 자기를 본인으로 하는 보유개인정보가 불법적으로 취득하거나 목적외의 보유나 이용에 해당될 때에는 利用停止나 消去를 請求할 수 있고, 목적외의 제공에 해당될 때에는 提供停止를 청구할 수 있다(제36조 제1항). 이러한 청구는 이용정지청구서를 행정기관의 장에게 제출하는 방식으로 이루어져야 한다(제37조 제1항).

이용정지의 청구가 있으면 행정기관의 장은 당해 이용정지청구에 이유가 있다고 인정할 경우 당해 행정기관에 있어서의 개인정보의 적정한 취급을 확보하기 위하여 필요한 한도로 당해 이용정지청구와 관련되는 보유개인정보의 이용정지를 해야 한다(제38조 본문). 다만 당해 보유개인정보의 이용정지로 인하여 당해 보유개인정보의 이용목적

과 관련되는 사무의 성질상 당해 사무의 적정한 수행에 현저한 지장을 초래할 우려가 있다고 인정될 때에는 그러하지 아니하다(제38조 단서).

이용정지를 할 때 행정기관의 장은 그 취지의 결정을 하여 이용정지청구자에게 그 취지를 서면에 의해 통지해야 하고, 이용정지를 하지 않을 때에는 그 취지의 결정을 하여 역시 그 취지를 서면통지하여야 한다(제39조).

#### 4) 불복신청

개시결정등, 정정결정등 또는 이용정지결정등에 대해 行政不服審査法(昭和 37년 법률 제160호)에 따른 불복신청이 있었을 때에는 당해 불복신청에 대한 재결 또는 결정을 해야 할 행정기관의 장은 원칙적으로 情報公開・個人情報保護審査會에 諮問하여야 한다(제42조).

자문을 한 행정기관의 장은 불복신청인 및 참가인, 개시청구자, 정정청구자 또는 이용정지청구자, 당해 불복신청과 관련되는 개시결정등에 대해 반대의견서를 제출한 제3자에 대해 자문을 한 취지를 통지하여야 한다(제43조).

#### (6) 감독기구

행정기관의 장은 행정기관에 있어서 개인정보취급에 관한 고충의 적절하고 신속한 처리에 노력하여야 한다(제48조). 총무대신은 행정기관의 장에 대하여 동법의 시행에 대해 보고를 요구할 수 있고, 그 보고를 정리하여 그 개요를 매년 공표한다(제49조). 그리고 총무대신은 그 밖에 동법의 목적을 달성하기 위해 필요하다고 인정할 경우 행정기관의 장에 대해 행정기관에 있어서의 개인정보취급에 관한 사무의 실시상황에 대해 자료의 제출 및 설명을 요구할 수 있으며(제50조), 개인정보취급에 관련된 의견을 제시할 수 있다(제51조).

## (7) 평 가

과거보다 적용배제의 대상과 범위를 축소함으로써 공공부문에 있어서 개인정보보호법의 규범력을 증대시킨 것은 커다란 진전이라고 본다. 또한 개인정보파일을 보유하고 있는 행정기관이 직접 개인정보파일부를 작성하여 공표하도록 한 것은 데이터주체의 통제력을 실질적으로 뒷받침하는 조치라고 볼 수 있다. 나아가 동법은 개시, 정정 및 이용정지, 불복신청에 관해 아주 자세한 규정을 두고 있으며, 不開示情報(제14조 제2호), 部分開示(제15조), 裁量的 開示(제16조), 제3자에 대한 意見書提出의 기회의 부여(제23조) 등에 있어서 제3자의 권익보호를 기하고 있을 뿐만 아니라 정정청구 이외에도 追加·削除의 청구를 인정하고(제27조), 개인정보가 불법적으로 취득하거나 목적외의 보유나 이용 또는 제공에 대한 본인의 통제권으로서 利用停止나 消去 또는 提供停止의 청구(제36조 제1항)를 허용하고 있다. 이러한 점은 데이터주체의 보호에 큰 진전을 가져올 것으로 기대된다.

하지만 컴퓨터매칭(computer matching) 등을 규율하는 조항을 두고 있지 않아 행정기관간에 온라인으로 결합하여 개인정보를 처리하는 것을 통제하기 어려운 점이 있다. 또한 개인정보보호법의 시행과 감독을 총괄하는 책임기관을 두면서도 개별적 집행과 감독은 각 기관의 장에게 맡기고 있는데, 이러한 내부적 통제시스템으로는 국가행정기관에 의한 개인정보의 침해를 억제하는 데 한계가 있을 것으로 예상된다.

## 4. 개인정보보호에 관한 조례

일본에서 개인정보보호에 관한 적극적 관심과 입법적 노력은 중앙정부보다 지방정부의 차원에서 먼저 나타났다. 1975년에 이미 도쿄도(東京都)의 구니타치시(國立市)에서 「쿠나타치시 전자계산조직 운영에

관한 조례』가 제정되었는데, 이 조례는 제3조에서 “전자계산조직의 이용에 있어 시민의 기본적 인권을 존중하고 시민의 개인적 비밀유지를 꾀하지 않으면 안 된다”고 규정하고, 시행규칙에서 개인정보의 처리에 관한 제한 등을 구체적으로 규정한 바 있다. 이후 컴퓨터에 의한 개인정보처리의 발전에 따라 미야기현(宮城縣)의 센다이시(仙台市), 도쿄도(東京都)의 세다가야꾸(世田谷區), 코오토우쿠(江東區), 메구로쿠(目黒區) 등 점차로 개인정보의 처리를 포함한 전자계산처리에 관한 조례를 제정하는 지방자치단체가 증가하였다.<sup>11)</sup> 1999년 4월 기준으로 전국 3,299개의 지방공공단체(都道府縣과 市區町村 등) 가운데 조례를 제정한 곳은 1,521개 단체로서 전체의 46.1%에 이르며, 規則이나 規程 등에 의하여 개인정보보호대책을 강구하고 있는 865개의 지방공공단체까지 합하면 개인정보보호 관련 자치입법을 마련한 곳은 전체의 72.3%의 수준에 이른다.<sup>12)</sup> 2001년 4월에 이르러서는 전국 3,296개 지방자치공공단체 가운데 60.1%에 해당하는 1,982개의 곳에서 개인정보보호에 관한 조례를 제정하였으며, 규칙이나 규정 등을 제정하고 있는 642개의 단체까지 합할 경우 전체의 79.6%에 달하는 지방공공단체에서 개인정보보호 관련 자치입법을 둔 것으로 파악되었다.<sup>13)</sup>

대체로 이러한 조례들은 단일법을 존중하여 공공부문에 있어서의 전자계산기 처리에 관련된 개인정보를 대상으로 하는 것이지만, 매뉴얼 처리 및 민간 부문까지 조례의 대상 범위에 포함시키는 단체도 증가하고 있다.<sup>14)</sup> 특히 1984년 4월 후쿠오카현(福岡縣)의 카스가시(春日市)에서는 공공부문과 민간부문의 보유정보 및 전산처리와 매뉴얼처리의 정보 모두를 대상으로 하는 개인정보보호조례를 제정한 바 있

11) 김철완/이민영, “인터넷 개인정보보호에 관한 법제도 연구”, 정보통신정책연구원, 『정책연구』00-10, 2000, 79면.

12) <http://www.kantei.go.jp/jp/it/privacy/houseika/dai2/siryou2-2.html> 참조.

13) <http://www.soumu.go.jp/s-news/2001/011023.html> 참조.

14) <http://www.kantei.go.jp/jp/it/privacy/houseika/dai2/siryou2-2.html> 참조.

다.15) 이것은 개인정보보호에 관한 포괄적 입법에 있어서 선구적 모델이라고 평가할 수 있다.

그리고 이러한 조례들 가운데 대다수는 개인정보의 수집·기록·이용·제공 등에 관한 규제 및 자기 정보의 開示, 訂正 등에 관해 규정하고 있으며, 나아가 상당수는 국가 또는 다른 지방자치단체 등과 같은 기관 사이에 온라인으로 결합하여 개인정보를 처리하는 것까지 금지 또는 제한하고 있다.

일본 지방자치단체 가운데 모범적인 사례로 꼽히는 카나가와현(神奈川縣)의 경우 1990년 3월 30일 제정된 개인정보보호조례는 실시기관에 대하여 사상, 신조 및 종교, 인종 및 민족, 범죄경력, 사회적 차별의 원인이 되는 사회적 신분 등 민감한 개인정보의 취급제한(제6조), 수집의 제한(제8조), 이용 및 제공의 제한(제9조), 온라인결합에 의한 제공(제10조), 자기정보개시청구권(제15조), 자기정보정정청구권(제21조) 등에 규정하고, 나아가 민간사업자에 대한 지도와 업무등록, 조사·권고·공표 등에 관해서도 규정하고 있다(제3장). 이 가운데서 특기할만한 것으로 이른바 사업자의 업무등록과 관련하여 縣內에서 개인정보를 취급하는 사업자로 하여금 지사의 등록을 받을 수 있도록 하고(제30조), 이렇게 등록한 사업자는 업무의 등록을 받은 업무와 관계있는 개인정보의 취급에 대해 등록필의 표지를 표시할 수 있도록 규정하고 있다(제32조).16) 개인정보취급업무의 등록상황을 보면 2002년도까지 7,388개 사업자, 13,176개 업무에 이르고 있으며,17) 홍보지를 통한 홍보활동 등으로 민간사업자에 있어서의 개인정보 보호의식이 점차 고조되는 성과를 낳고 있다.

---

15) 堀部政南, 申九賢, 프라이버시와 高度情報化社會, 청림출판, 1995, 126면.

16) 임재홍, “개인정보보호법과 개인정보보호조례”, 『민주법학』9호, 민주주의법학연구회, 1995. 293면 이하; <http://www.delsa.or.kr/main.html> 참조.

17) <http://k-base02.pref.kanagawa.jp:8080/file/O/個人情報保護制度2002.DOC> (表-1) 참조.

## IV. 일본의 CCTV 관련 입법의 동향

### 1. 문제의 상황

전자감시사회에서 개인이 자신의 일거수일투족이 감시되고 있다는 사실을 의식한다든가 혹은 감시될지도 모른다고 걱정하게 될 경우나 자신의 행동에 상당한 제약을 받게 될 수밖에 없을 것이다. Reg Whitaker 도 □□프라이버시의 종말(The End of Privacy)□□이란 책에서 감시카메라의 설치하는 지역주민들의 일상적인 생활은 물론이고 정치적인 반대자나 파업에 참가하는 노조원들의 활동까지 위축시키는 효과를 유발할 수 있음을 지적하고 있다.<sup>18)</sup>

미국 MIT대의 공학전문지 『Technology Review』 2003년 4월호의 보도에 의하면, 전세계에 설치된 감시카메라는 2,600만대이며, 미국에만 1,100만대에 이른다고 한다. 뉴욕의 시민단체 ‘미국시민자유연합(ACLU)’은 1999년 뉴욕 맨해튼 지역의 감시카메라를 2,397대로 집계했지만, 9·11 테러가 발생한 이후 최근까지 3배(7,200대)나 증가한 것으로 추산하였다. 영국에서는 이미 아일랜드공화군(IRA)의 도심테러에 부심하던 1980년대 집중적으로 감시카메라가 설치돼 현재 150만대가 전국 곳곳에 숨어있는 것으로 추정되고 있다. 15만대의 감시카메라가 설치된 런던에서 시민들은 하루 평균 5분에 한번씩, 하루 300번 정도 감시카메라에 노출된다는 보고서도 나와 있다.<sup>19)</sup>

일본에서도 2002년경부터 경시청에 의해 대도시 변화가를 중심으로 방범용 감시카메라를 설치하는 계획이 꾸준히 추진되어 왔다. 최근에는 전국 각지에 『슈퍼 방범등』이라고 하는 이름의 신형 방범카메라가 설치되고 있다. 이는 가로등에 카메라와 긴급통보장치가 함께 설치되

18) 렉 휘테커/이명균·노명현 역, □□개인의 죽음□□, 생각의 나무, 2001, 151면 이하 참조.

19) 국민일보 2004. 5. 10자.

어 비상시 버튼을 누르면 벨이 울림과 동시에 적색등이 점등되고 방범카메라가 작동되는 장치이다. 일본철도 니시니혼(西日本)에서는 월드컵경기장 인근 전철역에 홀리건 소동대비용 감시카메라가 설치된 바 있고, 다수의 초등학교에서도 사건방지를 위해 감시카메라의 도입이 늘어나고 있다. 그리고 전국적으로 상점가에 방범카메라의 설치가 급증하고 있으며, 또한 백화점이나 쇼핑몰 등이나 맨션 등의 승강기나 주차장에서도 도난방지 등의 목적으로 감시카메라를 설치하는 사례가 많아지고 있다. 심지어 세븐일레븐 같은 편의점에서는 가게 전체에 돛형 카메라를 설치하여 온라인으로 민간의 경비회사로 연결되도록 하는 경우까지도 있다.

## 2. 일본의 감시카메라 관련 입법 동향

(1) 이러한 가두방범카메라시스템에 대해서 정작 주민들이나 쇼핑객들로부터는 거의 문제제기가 이루어지지 않고 있는 실정이다. 실제로 여론조사에서도 응답자의 80~90%가 감시카메라의 도입에 찬성을 하고 있는 것으로 나타나고 있다. 이러한 분위기로 인하여 아직까지 일본에서는 감시카메라를 직접 규제하는 법률의 규정은 마련되고 있지 않다.<sup>20)</sup> 하지만 최근 일부 언론이나 변호사, 시민단체 등으로부터 초상권이나 프라이버시권의 침해 가능성을 심각하게 우려하는 목소리가 커지고 있다. 가령 후쿠오카현 변호사회의 인권옹호위원회·감시카메라소위원회, 큐슈 변호사 연합회 혹은 『감시사회를 거부하는 모임』과 같은 시민단체 등이 감시카메라의 법적 문제를 검토하면서 그에 대한 규제를 적극적으로 주장하고 있다.

(2) 판례는 민간이 설치한 방범용 감시카메라에 대해서는 대체로 관대한 입장인 것으로 파악된다. 예를 들자면, 2004년 7월 16일 나고야 지방

---

20) [http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news\\_2004\\_008.htm](http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news_2004_008.htm)

법원은 초상권도 일정한 제한이 가능하고, 특히 편의점과 같은 상점으로서 그 경영자가 어떠한 조치(카메라의 설치나 녹화 등)를 취할 것인지 선택할 수 있는 권리가 인정된다는 취지로 판결한 바 있다.<sup>21)</sup>

한편, 공권력이 설치한 범죄예방 목적의 TV 카메라와 관련하여서는 그것이 녹화되지 않는 경우 ①실제로 범죄가 실행중이거나 실행직후인 경우로서 ②증거보전의 필요성과 긴급성이 있고, ③그 촬영이 일반적으로 허용되는 한도를 넘지 않는 상당한 방법으로 이루어진다는 조건하에서 허용될 수 있지만, 녹화되는 경우는 범죄예방을 목적으로 한다고 하더라도 허용되지 않는다는 판결이 주목을 받고 있다.<sup>22)</sup>

(3) 현재 일본에서는 감시카메라의 설치와 운용에 대해 규제하는 법률은 따로 존재하지 않았지만, 内務省의 規定으로 감시카메라의 설치 운용에 관한 기준을 설정하여 자율적으로 이를 준수하도록 유도해 왔다. 내무성 규정을 보면, 우선 카메라가 있는 장소에 설치자의 연락처나 목적 등을 적은 표지를 세워야 한다. 그리고 목적외의 사용이 금지되며, 데이터의 보존기간은 31일간으로 제한된다. 또한 권한이 없는 사람은 카메라 조작실에 들어갈 수 없다.<sup>23)</sup>

그리고 최근 2004년 2월에는 도쿄의 스기나미구(杉並區)에서는 최초로 『스기나미구 방범카메라의 설치 및 이용에 관한 조례안』이 제출되었고,<sup>24)</sup> 그 해 3월 18일 구의회를 통과하여 같은 해 7월 1일부터 시행되기에 이르렀다.<sup>25)</sup> 이 조례는 스기나미구내의 도로, 공원 기타 규칙으로 정하는 다중이 운집하는 장소에 방범카메라를 설치하려고 하는 경우 카메라 취급자에게 『방범카메라의 설치 및 이용에 관한 기준』을

---

21) [http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news\\_2004\\_008.htm](http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news_2004_008.htm) 참조.

22) 大阪地裁判決, 平成 6年 4月, 니시나리 감시용 TV 카메라 철거 등 청구사건.

23) [http://mizushima-s.pos.to/lecture/2003/030507/030507\\_07.htm](http://mizushima-s.pos.to/lecture/2003/030507/030507_07.htm) 참조.

24) 마이니치신문 2004. 2. 13자.

25) 『NO! 監視』=ニュース 【第 7号】 2004-05-24 참조,

정해 스기나미구장에게 제출할 의무를 부과하고 있다.

아마도 이러한 스기나미구의 조례는 다른 지방자치단체에 대하여 감시카메라 규제에 관한 조례의 제정을 부추기는 기폭제가 될 것으로 예상된다. 그러면 이하에서는 스기나미구의 『방법카메라 이용설치기준』의 주요 내용에 대해 살펴보기로 한다.<sup>26)</sup>

### 3. 스기나미 區의 『방법카메라 이용설치기준』

#### (1) 입법 목적

방법카메라의 적절한 설치 및 이용에 관해 기본적인 원칙과 시책의 기본이 되는 사항을 정함으로써 방법카메라의 유용성에 배려하면서 區民 등의 자유와 권리 이익을 보호하는 것을 목적으로 한다(제1조).

여기서 “감시카메라의 유용성”에 대한 표현을 쓰고 있다는 것에 주목할 필요가 있는데, 이는 감시카메라의 금지를 목적으로 하는 것이 아니라 적절한 규율을 목적으로 한다는 것을 분명히 한 것으로 볼 수 있다.

그리고 ‘구민 등’이라고 한 것은 구내 거주자와 구내의 사업자는 물론이고, 통근자, 통학자, 구내의 단지 통과하는 사람도 포함시키기 위한 의도로 파악된다.

#### (2) 정 의

‘방법카메라’는 범죄예방의 목적(범죄예방을 부수적 목적으로 하는 경우 포함)으로 설치되는 카메라를 의미한다(제2조).

감시카메라의 이용목적은 매우 광범하지만, 여기서 ‘방법카메라’만을 규제의 대상으로 하기로 한 것으로 보인다. 부수적으로 방법의 목

26) [http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news\\_2004\\_007.htm](http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news_2004_007.htm) 참조.

적을 가지는 경우를 포함시킨 것은 방법용 카메라라고 하더라도 고용 계약의 준수 상황 등에 대한 감시가 주된 목적으로 되어 있는 경우도 있으므로 이러한 경우까지도 규제의 대상으로 삼을 수 있도록 하기 위함이다.

### (3) 기본원칙

방법카메라의 설치자 및 이용자는 구민 등이 그 얼굴이나 자태를 함부로 촬영되지 않는 자유를 가지는 것에 유의하여 방법 카메라의 설치, 이용에 신중을 기하고, 화상을 적정하게 취급하도록 노력하여야 한다.

초상권은 누구도 자신의 승낙 없이 함부로 그 얼굴이나 자태를 촬영당하지 않을 자유가 있다는 최고재판소의 판결<sup>27)</sup>로 인정된 것인데, 그러한 초상권을 단순히 관례의 차원이 아니라 조례를 통해 법전화화 이루어졌다고 볼 때 이는 큰 진전으로 평가되고 있다.<sup>28)</sup>

### (4) 방법카메라 설치이용기준의 신고

일정한 요건에 해당하는 경우에는 ‘설치이용기준’을 정해 區長에게 신고하도록 하는 신고제의 구조를 마련하고 있다.

설치의 주체는 ①스기나미구, ②공공기관(국가, 도쿄도의 기관 제외), ③상점회, 반상회 등 ④준공공의 장소와 관계되는 설치자 또는 이용자가 될 수 있다.

여기서 ‘준공공’이라고 한 것은 백화점이나 쇼핑몰 등에 있어서도 판매장의 면적 등에 따라 민간의 감시카메라에 대해서도 규제의 대상으로 삼겠다는 의도를 담고 있다.

27) 最高裁判決, 昭和 44年 12月, 京都府學連事件.

28) [http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news\\_2004\\_007.htm](http://www009.upp.so-net.ne.jp/kansi-no/news/documents/news_2004_007.htm) 참조.

(5) 방법 카메라 취급자등의 의무

- 본인에 대한 화상의 개시
- 고충에 대한 적절·신속한 대응

(6) 실효 확보책

- 취급자 등으로부터의 보고 징수
- 취급자 등에의 시정·중지의 지도 또는 권고
- 사실의 공표

(7) 고충 등의 제기

- 구민 등에 의한 고충 등의 제기
- 구장에 의한 적절·신속한 처리
- 스기나미구 정보공개·개인정보보호 심의회로부터의 의견 청취

(8) 평 가

이러한 스기나미구의 조례는 아무런 법적 근거도 없이 자꾸 늘어만 가는 감시 카메라에 대해 법적 규제의 근거를 제공하는 첫 시도였다 는 점에서 의의가 크다고 할 수 있다. 하지만 후쿠오카 변호사회에서 는 이에 대해 방법카메라의 설치 자체를 금지하는 규정이나 그 기준 을 정하지 않은 불충분한 입법이라는 비판을 가하고 있다. 또한 방법 카메라의 설치이용에 관한 기준에 실효성이 있는 통제장치가 충분히 마련되지 못하고 있다는 지적도 있다. 과연 이러한 법적 규제가 자칫 하면 방법카메라의 설치를 정당화하는 근거가 될 수도 있음을 간과해 서는 안 될 것이다.

## 토 론 문

채 승 완  
(한국정보보호진흥원 박사)

권건보 교수님의 ‘일본의 개인정보보호법과 CCTV 관련 입법동향’은 현재 일본의 개인정보보호법에 관한 체계나 내용을 잘 정리 분석하여 주셨습니다.

그러나 원고에서 몇 가지 확인하였으면 하는 사항이 있습니다. 먼저, 5P의 체계도 부분을 보면 공공부문의 해당 기관에서 보면 ‘독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률’(独立行政法人等の保有する個人情報の保護に関する法律)에 독립행정법인 이외에 특수법인과 허가법인이 포함되는지를 확인해볼 필요가 있습니다. 법률에 따르면 독립행정법인 등에 대한 정의는 기술되어 있지만 특수법인과 허가법인에 대해서는 언급되어 있지 않기 때문입니다.

둘째로, 18P의 도도부현과 시구정촌에 관한 기술로서 원래 지방공공단체 등에는 지자체와 지압독립행정법인 등이 포함되어 있으므로 이를 명확히 분리하여 기술할 필요성이 있습니다. 지자체만을 포함하면 조례제정율은 100%입니다. 기타 지방독립행정법인 등을 포함한다고 하여도 그 수치도 상당한 정도에 이르리라 보여집니다.

셋째로 CCTV 관련해서 일본 동경경시청의 연구결과와 실제로 토네가와댐 관리 사무소에서 운영하고 있는 CCTV관련 동의관련 안내가 있습니다. 이러한 것은 CCTV 관련 일본의 현황을 좀 더 잘 설명하고

있다고 보여줍니다.

특히, CCTV 관련해서 내각부에 질의한 결과 CCTV관련 내용은 개인정보보호법의 개인데이터베이스에 포함되어진다면 개인정보보호법에 의해 규제된다고 합니다. 그러나 세부사항에 있어서는 규제가 미흡한 부분도 있지만 특정 가능하다면 개인정보에 대한 취급과 동등하게 다루어져야 한다고 말하고 있습니다. 따라서 별도의 CCTV 관련 개별법을 제정할 필요가 현재까지는 없다는 입장입니다.

CCTV관련된 이러한 내용은 다소 불투명한 견해라고 보여집니다만 만약 개인정보보호법 안에서 다루어진다면 자세한 가이드라인이 필요하다고 보여지고 만약 개별법에 의해 CCTV관련 내용을 규제한다고 보면 이 역시 기본법에 의해 다루어 지리라 보여집니다. 기본법에 의해 취급된다면 개인정보보호 수준격차 및 개인정보보호 사각지대의 발생을 최소화하여 이로 인한 개인정보 가치의 깎을 줄일 수 있습니다. 이는 결국 CCTV와 관련된 개인정보 제공자와 개인정보 수집자간의 정보의 비대칭성을 최소화한다고 볼 수 있습니다.