

현안분석 2008-

입법평가 보고서 08-13

개인정보보호법제에 관한 입법평가

Evaluation of Legislation on the Data Protection Laws

연구자 : 성낙인(서울대학교 법학과 교수)
Sung, Nak-In
이인호(중앙대학교 법학과 교수)
Lee, In-Ho
김수용(부연구위원)
Kim, Su-Yong
권건보(명지대학교 법학과 교수)
Kwon, Geon-Bo
김삼용(중앙대학교 수학과통계학부 교수)
Kim, Sahm
이지은(중앙대학교 경영학과 교수)
Lee, Ji-Eun
김주영(서울대학교 법대 BK21 연구원)
Kim, Ju-Young
손형섭(헌법재판소 헌법연구원)
Son, Hyeung-Seob
박진우(서울대학교 법대 BK21 연구원)
Park, Jin-Woo
김송옥(한국방송통신대학교 강사)
Kim, Song-Ok

2008. 10. 31.

국문 요약

개인정보보호법은 비밀보호법과 달리 개인정보의 안전한 이용을 목표로 한다. 개인정보의 처리(=수집·이용·제공)와 관련해서 정보주체의 자유와 권리를 보호하기 위한 법이다.

지난 2003년 이래 난마와 같이 얽혀 있는 복잡한 개인정보보호법제를 체계적으로 정비하려는 노력이 정부와 시민단체, 그리고 학계에서 꾸준히 그리고 다각도로 이루어져 왔다. 다양한 개인정보보호법들이 공공부문과 민간부문으로 이원화되어 있고 여러 개별입법들이 존재하고 있어 개인정보처리기관이나 정보주체인 일반 국민의 입장에서 관련 법규에 대한 이해도가 낮아 법적 규율의 실효성이 떨어지고 있다. 또 민간부문에서는 일반법이 없어 일부 보호의 공백이 생기는 영역이 있는 등 문제점이 제기되었다. 그리하여 이를 개선하려는 노력의 일환으로 공공과 민간의 모든 개인정보처리를 규율하는 기본법 혹은 일반법을 제정하려는 움직임이 크게 일어났다. 그러나 그 입법개선 방향과 내용에 대해서는 정부, 시민단체, 학계가 각각 입장이 달라 어느 하나의 합의점에 이르지 못하고 있다.

현재 일반법으로서의 개인정보보호법의 제정을 둘러싸고 여러 쟁점에서 첨예한 의견대립이 있다. 가장 기본적인 쟁점은 세 가지로 압축될 수 있는데, 첫째, 현재 여러 영역에서 산발적으로 존재하는 여러 개별입법들을 체계적으로 어떻게 조정할 것인가 하는 입법체계에 관한 문제, 둘째, 이용과 보호의 가치를 합리적이고 균형 있게 조화시키는 개인정보 처리(=수집·이용·제공)의 입법기준이 무엇인가 하는 실체적인 문제(여기에는 개인정보처리의 허용기준, 절차적 요건, 정보주체의 참여권 등이 포함된다), 셋째, 그러한 법적 기준을 어떻게 집행할 것인가 하는 집행체계에 관한 문제, 특히 개인정보감독기구의 조직구성과 권한 및 기능을 어떻게 설정할 것인가 하는 문제를 들 수 있다.

본 입법평가의 기본목적은 이러한 세 가지 쟁점을 중심으로 지난 제17대 국회에서 제출되었던 3건의 개인정보보호법(안)과 현 제18대 국회에 제출되어 있는 개인정보보호법(안), 그리고 행정안전부가 입법예고한 개인정보보호법(안)의 내용을 분석·평가하고 그 대안을 모색해보는 것이다. 이러한 병행입법평가를 통하여 향후 입법자가 법안을 심사하는 과정에서 활용할 수 있는 의미 있는 입법자료를 제공하는 데 궁극적인 목적이 있다.

※ 키워드 : 입법평가, 개인정보보호법, 개인정보, 정보주체, 개인정보의 처리, 개인정보처리자, 개인정보자기결정권, 민감정보, 비밀보호법, 개인정보감독기구

Abstract

Data Protection Laws intend to ensure fair use of personal data, contrary to Confidentiality Laws. The purpose of Data Protection Laws is to protect the rights and freedoms of data subjects, and in particular their right to privacy with regard to the processing(=collection, use, and dissemination) of personal data.

Since 2003, the government, the citizens' group and the academy have constantly made efforts in various directions to reform the complicated system of the data protection laws and regulations. Because various Data Protection Acts are on two separate sector, public and private, and sectoral and particular Acts has been enacted, it's not easy to understand relevant laws and regulations in eyes of data controller or data subject, and it is resulting in the decrease of effectiveness for the law enforcement. As there is no comprehensive or general law in the private sector, the privacy in some areas which are not under the scope of data protection laws may not be protected. Accordingly, as a part of efforts to solve a problem like that, it has been suggested strongly to establish a basic or general Act that governs the collection, use and dissemination of personal data by both the public and private sectors. However, the government, the citizens' group and the academy standing their own ideas respectively have not reached consensus with regard to the orientation and contents of the Act.

Presently, opinions about how the Data Protection Act will be established are sharply opposed in several points. The basic issues of the dispute are as follows; first one is related to the structure of legislation about how sectoral and particular Acts scattered throughout several areas

are arranged; second one is related to substantive questions (including a criteria for lawful processing, procedural requirements of processing, the right of access to the processing data, etc.) about what legal standard is reasonable to harmonize the two values of utilization and protection for the processing(=collection, use, and dissemination) of personal data; last one is related to the enforcement system about how legal standards such like that will be enforced, especially how the structure, power and functions of a Data Protection Authority will be enacted.

This research for evaluation of legislation concerning data protection is to analyze and evaluate the contents of five bills that has been proposed. The five bills are composed of the three bills introduced in the 17th National Assembly, a bill presented in the current(18th) National Assembly and a bill drafted by Ministry of Public Administration and Security. Also, the research is to lay out the alternatives for the bills. The ultimate goal of this evaluation is to provide useful legislative materials for bill examination in the future.

※ Key words : Evaluation of Legislation, data protection laws, personal information or data, data subject, the processing of personal data, data controller, right to self-determination of personal information, sensitive data, confidentiality laws, data protection authority



입법평가서

입법평가서	
1. 입법평가의 대상	<p>개인정보보호법</p> <ul style="list-style-type: none"> ○ 개인정보보호의 입법체계 ○ 개인정보처리의 입법기준 ○ 개인정보보호의 집행체계
2. 입법평가자	<ul style="list-style-type: none"> ○ 연구책임자: 성낙인, 이인호, 김수용 ○ 공동연구자: 권건보, 김삼용, 이지은, 김주영 손형섭, 박진우, 김송옥
3. 입법평가의 필요성	<ul style="list-style-type: none"> ○ 우리나라에서 개인정보처리에 관하여 규율한 최초의 입법은 1980년 12월 18일에 제정·공포된 『형의 실효 등에 관한 법률』(1980. 12. 18. 시행)임. 이 법률은 범죄기록의 작성 및 관리에 관한 사항을 정한 것으로 엄밀히 말하면 개인정보보호법이라기보다는 비밀보호법에 해당함 ○ 개인정보처리(수집·이용·제공)와 관련하여 정보주체의 권리와 이익을 보호하면서 개인정보의 처리를 가능하게 한 본격적인 의미의 개인정보보호법은 1994년 1월 7일에 공포된 『공공기관의 개인정보보호에 관한 법률』(1995. 1. 8. 시행)임. 이 법률은 공공기관에서 보유하고 있는 개인정보데이터베이스의 운영과 관련하여 개인정보의 수집·이용·제공의 허용기준과 그 처리의 절차적 요건 등을 정하고 있음 ○ 민간부문에서 개인정보의 이용과 보호를 조화시키고자 한 개인정보보호법은 1995년 1월 5일에 공포된 『신용정보의 이용 및 보호에 관한 법률』(1995. 7. 6. 시행)임. 이 법률은 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 기하며, 신용정보의 오·남용으로부터 개인의 프라이버시 등을 적절하게 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 제정되었음 ○ 이상의 개인정보보호법 이외에도 현재 개인정보보호와 관련하여 상당히 많은 법률이 산재해 있음 ○ 다양한 개인정보보호법과 비밀보호법이 존재하고 있지만, 일반국민들은 개인정보처리와 관련하여 자신들의 프

입법평가서	
	<p>라이버시가 제대로 보호받고 있지 못하다는 인식이 널리 확산되어 있음. 역으로 강력한 개인정보보호법제로 인하여 사회적으로 필요한 개인정보의 유통이 합법적으로 이루어지지 못한 채 음성적으로 혹은 불법적으로 유통되고 있음. 이처럼 개인정보의 이용과 보호의 문제는 그것을 바라보는 관점에 따라 또는 프라이버시에 대한 인식의 차이에 따라 매우 현격한 차이를 보이고 있음</p> <p>○ 개인정보의 이용과 보호를 어떻게 규율할 것인가는 개인정보처리의 효용성과 위험성을 어떻게 평가하느냐에 달려 있음. 현재 실시되고 있는 많은 개인정보보호법과 비밀보호법은 이러한 평가에 입각하여 마련된 것이지만, 그 내용을 면밀히 분석해 보면 체계성이 결여되어 있거나, 이용과 보호의 균형이 맞지 않는 경우가 많음. 이것은 개인정보처리의 효용성과 위험성에 대하여 정확한 평가에 기초하여 마련되지 않았기 때문임. 이러한 상황 속에서 개인정보의 수집·이용·제공을 규율하고 있는 여러 개인정보보호법과 비밀보호법들을 총체적으로 점검해 볼 필요성이 있음</p>
4. 입법평가의 방법	<p>문헌조사</p> <p>개인정보보호법제의 입법체계와 개인정보의 이용과 보호에 관한 선행연구에 대한 문헌조사를 함</p>
	<p>규범적 분석</p> <p>복잡하게 얽혀 있는 개인정보보호법제들을 분석하여 체계성을 부여하고, 개인정보의 이용과 보호의 합리적인 조화와 균형을 모색함(현행의 개인정보보호법제에 대한 사후적 입법평가를 먼저 실시한 뒤, 행정안전부의 입법예고안 등에 대한 병행적 입법평가를 실시함)</p>
	<p>비교법적 분석</p> <p>선진각국의 개인정보보호법제에 대한 비교법적 고찰을 함. 특히 일본은 2000년에 개인정보보호법이 시행되고 난 이후 시행결과에 대한 평가작업을 지속적으로 진행하고 있음. 따라서 우리나라의 개인정보보호법제에 관한 입법평가에 중요한 참고자료로 활용할 수 있을 것임</p>

입법평가서																										
	실증적 · 경험적 분석	일반인들과 전문가들이 개인정보보호법제의 입법체계와 개인정보의 이용과 보호에 관하여 어떻게 이해하고 있는지를 조사하기 위하여 전국 성인남녀 1000명, 전문가 41명을 대상으로 설문조사를 실시하고 그것을 분석함																								
	비용· 효과 분석	입법평가의 방법으로 비용·효과분석은 유용하지만, 이 평가에서는 의미있게 분석하지 못하였음. 다만 공공기관과 기업에서 이루어지는 개인정보처리 실태를 파악하고 각 부문에서 개인정보처리가 갖는 효용성과 위험성에 대한 평가를 실시하였음. 또한 개인정보처리의 입법기준에 대한 병행적 입법평가를 하는 가운데 법경제학적 차원의 비용·효과분석은 아니지만 행정안전부의 입법예고안의 개별적인 기준들이 사후에 적용될 경우, 어떠한 사회적 파장과 효과가 나타나게 될 것인지에 대한 효과분석을 시도함																								
5. 입법평가의 절차	평가기간	2008. 4. 21.-10. 31.(총 6.4개월)																								
	워크샵 등	<ul style="list-style-type: none"> ○ 공동연구자들간의 의견조율 및 워크샵(총 8회 실시) ○ 최종심: 2008. 10. 13. 																								
	설문조사	일반인 설문조사	<ul style="list-style-type: none"> ○ 조사방법: HRC 마스터 패널을 이용 한 온라인 조사 ○ 조사대상: 전국 성인 남녀 만20세~50세 ○ 표본크기: 1000명 ○ 표본구성 <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th></th> <th>20대</th> <th>30대</th> <th>40대</th> <th>50대</th> <th>계</th> </tr> </thead> <tbody> <tr> <td>남성</td> <td>125</td> <td>145</td> <td>143</td> <td>96</td> <td>509</td> </tr> <tr> <td>여성</td> <td>117</td> <td>140</td> <td>138</td> <td>96</td> <td>491</td> </tr> <tr> <td>계</td> <td>242</td> <td>285</td> <td>281</td> <td>192</td> <td>1000</td> </tr> </tbody> </table> <p>* 표본구성은 2007년 통계청 인구센서스 자료에 근거하여 구성하였음</p>		20대	30대	40대	50대	계	남성	125	145	143	96	509	여성	117	140	138	96	491	계	242	285	281	192
	20대	30대	40대	50대	계																					
남성	125	145	143	96	509																					
여성	117	140	138	96	491																					
계	242	285	281	192	1000																					

입법평가서																							
		<ul style="list-style-type: none"> ○ 표본추출방법: 표본 할당 추출 (Quota Sampling) ○ 조사기간: 2008년 9월 2일~ 2008년 9월 8일 ○ 표본오차: 95% 신뢰수준에서 ± 3.1% 																					
	전문가 설문조사	<ul style="list-style-type: none"> ○ 조사방법: HRC 마스터 패널을 이용한 온라인 조사 ○ 조사대상: 전국 개인정보보호 관련 전문가 ○ 표본크기: 41명 ○ 표본구성 <table border="1"> <tr> <td rowspan="2">성별</td> <td>남</td> <td>36</td> </tr> <tr> <td>여</td> <td>5</td> </tr> <tr> <td rowspan="4">근무기간</td> <td>1년 미만</td> <td>8</td> </tr> <tr> <td>1~5년 미만</td> <td>20</td> </tr> <tr> <td>5~10년 미만</td> <td>7</td> </tr> <tr> <td>10년 이상</td> <td>6</td> </tr> <tr> <td rowspan="3">근무직장</td> <td>기업</td> <td>13</td> </tr> <tr> <td>법학교수</td> <td>16</td> </tr> <tr> <td>법실무</td> <td>12</td> </tr> </table> <ul style="list-style-type: none"> ○ 표본추출방법: 표본 할당 추출 (Quota Sampling) ○ 조사기간: 2008년 9월 9일~ 2008년 9월 18일 	성별	남	36	여	5	근무기간	1년 미만	8	1~5년 미만	20	5~10년 미만	7	10년 이상	6	근무직장	기업	13	법학교수	16	법실무	12
성별	남	36																					
	여	5																					
근무기간	1년 미만	8																					
	1~5년 미만	20																					
	5~10년 미만	7																					
	10년 이상	6																					
근무직장	기업	13																					
	법학교수	16																					
	법실무	12																					
6. 대안 및 한계	대안	<p>개인정보보호의 입법체계</p> <ul style="list-style-type: none"> ○ 대안 1: 분리형 일반법의 제정 ○ 대안 2: 통합형 일반법의 제정 ○ 대안 3: 통합형 기본법의 제정 <p>○ 권고: 법적 보호의 공백(효율성), 법제 정비의 소요비용(비용), 법집행과정의 용이성(적용 적합성), 수범자의 이해가능성(친숙성)</p>																					

입법평가서	
	<p>등을 기준으로 각 대안을 비교분석한 결과 통합형 일반법체계가 가장 유리하였음. 입법정책적으로 공·사 부문의 통합형 입법을 지향하고, 정보통신망법의 개인정보보호 관련 규정을 삭제하며, 부문별로 특칙을 두는 것이 필요함</p>
	<p>개인정보처리의 입법기준</p>
	<p>기본개념의 정의규정에 대한 수정대안, 수집·이용·제공의 허용기준에 대한 수정대안, 수집·이용·제공의 절차적 요건에 대한 수정대안, 공공기관의 개인정보처리기준에 대한 권고 제시(제6편 제2장 참고)</p>
	<p>개인정보보호의 집행체계</p>
	<p>○대안 1: 국가인권위원회의 한 부서로 하는 방안 ○대안 2: 대통령 소속 독립위원회의 설치방안 ○대안 3: 중앙행정기관화의 방안</p> <p>○권고: 개인정보보호의 정책이 실효적인 집행력을 확보하기 위해서는 정부와 분리된 독자적인 기구를 설치하기보다는 정부기구로 존속하게 하는 것이 더 나을 것임. 다만 임기제, 징계와 소추의 엄격한 제한, 정치적 중립성 보장, 의견제시, 조사권, 시정명령 등의 실질적 감독권한 보장 등을 통해 개인정보보호기구의 자율성과 독자성이 확보될 수 있도록 해야 할 것임. 이러한 기능적 독립성을 확보하는 것을 전제로 할 때, 국무총리 직속기구로 개인정보보호위원회를 설치·운영하는 것이 타당할 것임. 그리고 통</p>

입법평가서		
		<p>합감독기구를 중심으로 감독기능을 일원화할 필요가 있음(구체적인 수정안은 제6편 제3장 제2절 참고)</p>
	한계	<ul style="list-style-type: none"> ○ 시간적 한계: 개인정보보호법제에 관한 입법평가팀이 구성되어 개인정보보호법에 대한 문제점 분석, 공동연구자들간의 업무분담, 일반인과 전문가들에 대한 설문조사 및 분석, 입법평가서 작성 등을 하기에는 연구기간(약 6개월)이 너무 짧았음 ○ 비용·효과분석에 대한 한계: 입법평가의 방법으로 비용·효과분석은 유용함. 이 평가에서는 공공기관과 기업에서 이루어지는 개인정보처리 실태를 파악하고 각 부문에서 개인정보처리가 갖는 효용성과 위험성에 대한 평가를 실시하였음. 또한 개인정보처리의 입법기준에 대한 병행적 입법평가를 하는 가운데 법경제학적 차원의 비용·효과분석은 아니지만 행정안전부의 입법예고안의 개별적인 기준들이 사후에 적용될 경우, 어떠한 사회적 파장과 효과가 나타나게 될 것인지에 대한 효과분석을 시도함. 그러나 여러 가지 한계(시간과 비용·효과분석에 대한 전문가의 한계)로 인하여 비용·효과분석을 제대로 실시하지 못했음

색지삽입

목 차

국문요약	3
Abstract	5
제 1 편 개인정보보호법제에 관한 입법평가의 방향설정 ...	41
제 1 장 입법평가의 개요	43
제 1 절 입법평가의 필요성과 목적	43
1. 입법평가의 필요성	43
2. 입법평가의 목적	47
제 2 절 입법평가의 유형과 대상	54
1. 사전적 입법평가와 대상	54
2. 사후적 입법평가와 대상	56
3. 병행적 입법평가와 대상	57
4. 대안의 제시와 권고	60
제 3 절 입법평가의 방법론	60
1. 실증적·경험론적 분석	60
2. 문헌조사 및 분석	65
3. 규범론적 분석	65
4. 비교법적 분석	66
5. 비용·효과 분석	67

제 2 장 개인정보보호법의 존재이유와 특성	69
제 1 절 개인정보보호법 생성의 사회적 배경	69
1. 개인에 관한 정보의 처리를 규율하는 지금까지의 법제와 법리 ...	69
2. 디지털시대의 새로운 문제 상황과 새로운 규율의 필요성	74
제 2 절 개인정보보호법의 목적과 특성	80
1. 개인정보보호법의 입법목적	80
2. 개인정보보호법의 성격과 특징	82
제 3 장 개인정보의 보호와 이용에 관한 기초이론	87
제 1 절 서언 : 입법평가의 필요성	87
제 2 절 선행 연구의 검토	90
1. 구조 차원의 논의	91
2. 행위자 차원의 논의	92
3. 평 가	94
제 3 절 개인정보보호법제의 논의배경	95
1. 사회적 배경	95
2. 이론적 배경	118
제 4 절 소 결	164
제 4 장 개인정보보호에 관한 헌법이론적 분석	167
제 1 절 개인정보보호의 헌법적 의의	167
제 2 절 개인정보보호와 개인정보자기결정권의 보장	168
1. 개인정보자기결정권의 의의	168

2. 개인정보자기결정권의 헌법적 근거	171
3. 개인정보자기결정권의 내용	177
4. 개인정보자기결정권의 제한	183
제 3 절 개인정보자기결정권의 헌법적 한계	186
1. 언론의 자유와의 조화	186
2. 정보공개청구권과의 조화	191
제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가....	203
제 1 장 개인정보처리의 실태 분석: 효용성과 위험성 평가....	205
제 1 절 공공기관 개인정보처리의 효용성과 위험성	205
1. 서 언	205
2. 공공기관의 개인정보처리의 실태	207
3. 효용성 평가	216
4. 위험성 평가	223
5. 소 결	242
제 2 절 기업의 개인정보처리의 효용성과 위험성	244
1. 기업의 개인정보처리의 실태	244
2. 효용성 평가	276
3. 위험성 평가	285
4. 소 결	290
제 2 장 현행 개인정보보호법제의 현황	293
제 1 절 개 관	293
제 2 절 「공공기관의 개인정보 보호에 관한 법률」	295

1. 연 혁	295
2. 현행 법률의 주요 내용	299
제 3 절 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 ...	308
1. 입법의 배경	308
2. 관련 규정의 변천	310
3. 현행법의 주요 내용	315
제 4 절 「신용정보의 이용 및 보호에 관한 법률」	326
1. 연 혁	326
2. 현행법의 주요 내용	329
제 5 절 「위치정보의 보호 및 이용 등에 관한 법률」	335
1. 연 혁	335
2. 현행법상 개인정보보호 관련 내용	338
제 6 절 기타 개별법상의 개인정보보호 관련 규정	343
1. 공공부문의 개인정보보호 관련 조항	343
2. 민간분야의 개인정보보호 관련 조항	351
제 3 장 현행 개인정보보호법제에 관한 개괄적 평가	357
제 1 절 세계적 보호입법모델에 비추어 본 우리 법제의 위상 ...	357
1. 세계적인 보호입법모델의 개관	357
2. 우리의 이원적·영역별·부분적 보호법제	367
제 2 절 현행 개인정보보호법제의 문제점 분석	370
1. 체계부조화의 불균형적인 보호체계	370
2. 예방적 집행기능의 부존재: 처벌 위주의 사후 집행체계	373
3. 독립된 감독기구의 부존재 및 감독기능의 불완전성	374

제 4 장 일본 개인정보보호법제에 대한 사후입법 평가: 경험과 시사점	377
제 1 절 서 언	377
제 2 절 개인정보보호법의 제정 · 시행 · 평가	378
1. 입법의 배경과 제정과정	378
2. 시행 및 추진경과	384
3. 사후 평가와 점검	390
제 3 절 개인정보보호법의 주요 내용 · 체계 · 특징	392
1. 주요 내용	392
2. 입법의 체계	401
3. 기본 특징	403
제 4 절 법률 시행 후 분야별 효과와 과제	406
1. 개인정보보호법의 시작과 새로운 과제	406
2. 의료분야의 과제	408
3. 신용정보 분야의 과제	412
제 5 절 사후입법평가: 시행상황에 대한 점검과 평가	415
1. 2004년 행정기관개인정보보호법의 시행상황점검과 법률의 개정	415
2. 2007년 개인정보보호법의 시행상황점검	417
3. 개인정보보호에 관한 의식조사	433
4. 개인정보보호법의 시행에 대한 평가	449
제 6 절 개인정보보호법 시행 이후의 변화	471
1. 개인정보보호에 관한 시행령의 변경	471
2. 개인정보보호에 관한 기본방침의 변경	472

제 7 절 시사점	478
1. 개인정보보호법의 체계	478
2. 개인정보의 보호수준	479
3. 자율규제 모델	482
4. 과잉반응의 문제	483
5. 공공기관과 사업자의 개인정보 침해	484
제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가....	485
제 1 장 비교법적 고찰	487
제 1 절 미 국	489
1. 개인정보보호법제 현황	489
2. 연방 프라이버시법	491
3. 기타 공공부문에서의 개인정보보호 입법	495
4. 민간부문에서의 개인정보보호	497
5. 자율규제론과 세이프하버원칙	508
6. 전자정부법상 프라이버시영향평가제도	511
7. 입법체계에 대한 평가	513
제 2 절 캐나다	514
1. 개인정보보호법제의 개관	514
2. 프라이버시법의 적용범위와 구성	514
3. 개인정보보호 및 전자문서에 관한 법률	518
4. 기타 개별법	521
5. 프라이버시영향평가	522
6. 입법체계상 특징	526

제 3 절 영 국	527
1. 정보보호법의 제정과 개정	527
2. 정보보호법의 적용범위	529
3. 정보보호법의 구성	530
4. 개인정보보호기구	534
5. 기타 개인정보보호법제	535
6. 입법체계의 평가	537
제 4 절 독 일	537
1. 연방정보보호법의 제정과 개정	537
2. 연방정보보호법(BDSG)의 적용범위	540
3. 연방정보보호법(BDSG)의 구성	541
4. 전기통신서비스정보보호법	544
5. 개인정보보호법의 현대화 방안	546
6. 현행 입법의 체계상 특징	547
제 5 절 프 랑 스	547
1. ‘정보처리·축적 및 자유에 관한 법률’의 제정과 개정	547
2. 정보처리법의 적용범위	550
3. 정보처리법의 주요 규율사항	551
4. 입법체계의 평가	556
제 6 절 이 탈 리 아	557
1. 개 관	557
2. 개인정보보호법제의 현황	557
3. 2003년 개인정보보호법의 구성	558
4. 2003년 개인정보보호법의 주요 내용	563
5. 입법체계상 특징	565

제 7 절 스페인	566
1. 개 관	566
2. 개인정보보호통합법(LOPD)의 구성	567
3. 개인정보보호통합법(LOPD)의 특징과 주요 내용	569
4. 입법체계상 특징	573
제 8 절 일 본	574
1. 개인정보보호법의 제정과 개정	574
2. 개인정보보호법제의 체계	577
제 9 절 외국 입법체계의 종합적 분석	579
1. 개인정보보호법제의 비교	579
2. 입법방식의 분류	582
3. 입법모델별 장단점 분석	584
제 2 장 실증적·경험적 조사결과 분석	587
제 1 절 설문조사의 개요	587
1. 설문조사의 배경	587
2. 일반인 대상 조사의 내용	588
3. 전문가 대상 조사의 내용	591
제 2 절 설문조사의 결과	597
1. 일반인 대상 조사	597
2. 전문가 대상 조사	615
제 3 절 설문조사의 분석	638
1. 수범자의 친숙도	638
2. 입법체계에 대한 숙지의 정도	640

3. 입법체계의 방향성	640
4. 조사결과의 분석	642
제 3 장 우리 개인정보보호법의 입법체계 평가	643
제 1 절 개인정보보호법제의 개관	643
제 2 절 입법체계상의 특징과 문제점	645
1. 입법체계상의 특징	645
2. 입법체계상의 문제점	646
제 3 절 개인정보보호법(안)에 대한 분석	651
1. 법제화 동향	651
2. 각 법안의 소개	653
3. 각 법안의 비교 분석	661
제 4 절 입법체계론의 내용과 평가	672
1. 서 언	672
2. 입법체계의 분석틀	674
3. 입법체계론의 전개	679
4. 입법체계론의 주요 내용	682
5. 입법체계의 평가	688
제 4 편 개인정보처리의 입법기준에 관한 병행적 입법평가....	695
제 1 장 서 언	697
제 2 장 기본용어의 정의규정에 대한 평가와 대안제시	699
제 1 절 개 관	699

제 2 절	개인정보 · 개인기록 · 고유식별정보의 세 가지 개념의 구별필요성	699
제 3 절	“개인정보파일” 개념의 중요 의의와 용어선택의 부적합성	705
제 4 절	“처리”의 개념규정의 적정성	710
제 5 절	개인정보처리자와 정보처리대행자의 개념구분의 필요성	712
	1. 개인정보처리자의 개념규정에 대한 평가와 수정대안	712
	2. 정보처리대행자의 개념설정 및 책임소재규정의 필요성	717
제 6 절	“동의”의 개념규정 신설의 필요성	720
제 3 장	개인정보처리의 입법기준에 대한 평가와 대안제시	723
제 1 절	정보주체의 동의 요건에 대한 비판	723
	1. 개인정보자기결정권에 대한 오해와 이해	723
	2. 개인정보자기결정권에 대한 오해의 경향에 대한 분석과 비판	728
제 2 절	수집 · 이용 · 제공의 허용기준에 관한 외국의 입법사례 분석	751
	1. OECD 가이드라인상의 수집제한의 원칙의 내용	752
	2. 유럽연합 개인정보보호지침상의 허용기준	754
	3. 영국 개인정보보호법상의 허용기준	758
	4. 독일 개인정보보호법상의 허용기준	762
	5. 일본 개인정보보호법상의 허용기준	769
제 3 절	입법예고안의 수집 · 이용 · 제공의 허용기준에 대한 입법평가	776
	1. 종합적 평가	776
	2. 일반개인정보 수집 · 이용의 허용기준의 타당성	777

3. 정보주체의 동의권 인정 조항의 문제점	780
4. 일반개인정보 제공의 과도한 제한과 그 문제의 심각성	781
5. 민감개인정보에 대한 과도한 보호의 문제점	794

제 4 장 수집 · 이용 · 제공의 절차적 요건에 대한
입법평가와 대안제시

제 1 절 4가지 절차적 요건의 개요	801
1. 목적명시 요건	801
2. 품질관리 요건	803
3. 고지 요건	804
4. 보고 요건	805

제 2 절 절차적 요건에 대한 비교법적 분석	806
1. 유럽연합 개인정보보호지침상의 절차적 요건	806
2. 제1항은 다음의 경우에는 적용되지 아니한다.	808
3. 영국 개인정보보호법상의 절차적 요건	809
4. 독일 개인정보보호법상의 절차적 요건	810
5. 일본 개인정보보호법상의 절차적 요건	813

제 3 절 입법예고안의 절차적 요건에 대한 입법평가와 대안제시	818
1. 목적명시 요건에 대한 평가와 수정대안	818
2. 품질관리 요건에 대한 평가와 수정대안	821
3. 고지 요건에 대한 평가와 수정대안	823
4. 보고 요건에 대한 평가	826

제 5 장 공공기관의 개인정보처리기준에 대한 입법평가

제 1 절 개인정보처리의 입법기준에 대한 평가	829
---------------------------------	-----

1. 개인정보처리의 허용기준의 적정성	829
2. 일부 절차적 요건의 흠결	830
3. 민감개인정보 및 고유식별정보의 처리에 대한 과도한 제한	833
제 2 절 개인정보 공동이용의 입법기준에 대한 평가	834
1. 개인정보 공동이용에 대한 현행법의 규율상황	834
2. 개인정보 공동이용의 효용성과 위험성	838
3. 『전자정부법 전부개정법률(안)』에 대한 평가	845
제 5 편 개인정보보호의 집행체계에 관한 병행적 입법평가....	849
제 1 장 개인정보감독기구의 설립방향성	851
제 1 절 서 언	851
제 2 절 독립된 개인정보감독기구의 존재이유	854
제 3 절 개인정보감독기구의 기능과 권한	856
1. 옴부즈맨(ombudsmen)으로서의 민원해결기능	856
2. 감사관(auditor)으로서의 감사기능	857
3. 자문역(consultant)으로서 자문기능	859
4. 교육자(educator)로서의 교육기능	859
5. 정책조언자(policy adviser)로서의 조언기능	861
6. 자율규제의 조정자(negotiator)로서의 유도기능	862
7. 집행자(enforcer)로서의 집행기능	864
제 2 장 개인정보감독기구의 비교법적 고찰	867
제 1 절 비교법적 개관	867
1. 국제규범상의 설립 요구	867

2. 독립된 감독기구 설립의 세계적 추세	870
3. 소 결	872
제 2 절 감독기구에 관한 입법례	873
1. 미 국	873
2. 캐나다	874
3. 영 국	875
4. 독 일	878
5. 프랑스	880
6. 이탈리아	882
7. 스페인	883
8. 일 본	885
제 3 절 개인정보감독기구의 유형별 분석	887
제 3 장 우리의 집행체계에 대한 평가	891
제 1 절 개인정보감독기구의 현황	891
제 2 절 현행 개인정보감독기구의 문제점	894
1. 공공기관개인정보보호심의위원회	894
2. 행정안전부와 방송통신위원회	895
3. 금융위원회와 금융감독원	897
제 3 절 법률안의 감독기구 관련 내용	897
1. (구)이혜훈 법안	897
2. 이은영법안	898
3. 노회찬법안	899
4. 행정안전부 입법예고법안	900
5. (신)이혜훈 법안	900

제 4 절 개인정보보호법(안)의 분석	901
1. 명 칭	901
2. 지 위	901
3. 구 성	902
4. 업 무	903
5. 권 한	905
6. 하위기구	906
7. 평 가	906
제 4 장 감독기구의 설치방안	909
제 1 절 감독기구의 통합 필요성	909
제 2 절 독립적 감독기구의 형태	911
1. 독립성의 의미	911
2. 감독기구의 설치방안	911
3. 검 토	914
제 3 절 감독기구의 기능과 역할	916
1. 감시기능과 조사권한	916
2. 시정권고 및 침해정지명령권	916
3. 피해구제기능과 분쟁조정권한	917
4. 사전적 예방기능	917
5. 종합적인 정책 입안 기능 및 규칙제정권	917
제 4 절 기존의 집행기구와의 관계설정	918
제 6 편 대안의 제시와 권고	921

제 1 장 입법체계에 대한 대안과 권고	923
제 1 절 대안의 제시	923
1. 대안 1: 분리형 일반법 제정 방안	923
2. 대안 2: 통합형 일반법 제정 방안	923
3. 대안 3: 통합형 기본법 제정 방안	924
제 2 절 각 대안의 비교	924
1. 분리형 일반법제정론	924
2. 통합형 일반법제정론	925
3. 통합형 기본법제정론	926
4. 분석의 결론	926
제 3 절 입법정책적 권고	927
1. 공·사 부문 통합형 입법의 지향	927
2. 통합형 일반법의 체계	928
3. 정보통신망법의 개인정보보호 관련 규정의 삭제	929
4. 부문별 특칙의 필요성	931
제 2 장 개인정보처리의 입법기준에 대한 대안과 권고	935
제 1 절 기본개념의 정의규정에 대한 수정대안	935
제 2 절 수집·이용·제공의 허용기준에 대한 수정대안	937
1. 일반개인정보의 수집·이용·제공의 허용기준	937
2. 제3자 제공의 허용기준에 대한 외국 입법례와의 대비	938
3. 민감개인정보의 수집·이용·제공의 허용기준에 대한 외국 입법례와의 대비	944
제 3 절 수집·이용·제공의 절차적 요건에 대한 수정대안	947

1. 목적명시 요건에 대한 수정대안	947
2. 품질관리 요건에 대한 수정대안	948
3. 고지 요건에 대한 수정대안	949
제 4 절 공공기관의 개인정보처리기준에 대한 권고	953
1. 고지 요건의 명시화 필요	953
2. 개인정보 공동이용의 규율에 대한 권고	954
제 3 장 집행체계에 대한 대안과 권고	957
제 1 절 일반적 대안과 권고	957
1. 독립적 개인정보보호기구의 설치	957
2. 개인정보보호기구의 기능	958
3. 개인정보보호기구의 소속	958
4. 감독기능의 일원화	961
제 2 절 구체적 수정안의 제시	961
참 고 문 헌	979
부록 I. 일반인 설문조사지 및 설문조사결과표	1003
I-1. 일반인 설문조사지	1003
I-2. 일반인 설문조사결과표	1017
1. 개인정보보호법제 입법체계에 대한 일반적 인식	1019
2. 개인정보보호 관련 일반적 인식	1025
부록 II. 전문가 설문조사지 및 설문조사결과표	1057
II-1. 전문가 설문조사지	1057

II-2. 전문가 설문조사결과표	1073
부록 III. 일본의 개인정보보호법 관련 자료	1113
III-1. 2004년도 일본 ‘행정기관개인정보보호법’ 시행상황 조사결과보고서	1113
III-2. 일본 ‘개인정보보호설명회참가자의 설문결과보고서 (2008.3) : 소비자 의식-집계결과표-	1149
III-3. 일본 개인정보보호에 관한법률시행령의 일부를 개정하는 정령(2008년정령제166호) 신구대조	1159
III-4. 개인정보보호에 관한 기본방침(2008.4.24)	1160

표 및 그림 목차

【 표 】

[표 1-1-1] 제17대 국회 제출 개인정보보호법(안) 개요	51
[표 1-1-2] 일반인 설문조사의 설계구성요소	61
[표 1-1-3] 일반인 설문조사의 조사내용	62
[표 1-1-4] 일반인 설문조사 응답자 분포	63
[표 1-1-5] 전문가 설문조사의 설계구성요소	64
[표 1-1-6] 전문가 설문조사 응답자 분포	64
[표 1-3-1] 정보사회 감시의 개념지도	146
[표 2-1-1] 공공기관이 보유한 개인정보파일종류의 수	208
[표 2-1-2] 민원사무 1건 당 구비서류 종수 현황(2005년 10월 말 기준)	210
[표 2-1-3] 행정정보공동이용시스템의 단계별 확대구축 사업 현황	212
[표 2-1-4] 연도별 행정정보 공동이용 실적	213
[표 2-1-5] 2008년 9월 확대 66종 구비서류 목록	213
[표 2-1-6] 공공기관 CCTV 설치현황(2007년 6월 기준)	216
[표 2-1-7(a)] 연도별 전자민원 이용현황	219
[표 2-1-7(b)] 행정정보 공동이용에 따른 비용절감 효과	221
[표 2-1-8] 개인정보DB 구축 및 이용의 위험성 및 불쾌감 (일반인 대상)	224
[표 2-1-9] 개인정보DB 구축 및 이용의 위험성 및 불쾌감 (전문가 대상)	225

[표 2-1-10] 개인정보DB 공유의 위험성 및 불쾌감(일반인 대상)	226
[표 2-1-11] 개인정보DB 공유의 위험성 및 불쾌감(전문가 대상)	227
[표 2-1-12] 개인정보처리의 오·남용 가능성(일반인 대상)	228
[표 2-1-13] 개인정보처리의 오·남용 가능성(전문가 대상)	228
[표 2-1-14] 개인정보처리의 오·남용시 위험성(일반인 대상)	229
[표 2-1-15] 개인정보처리의 오·남용시 위험성(전문가 대상)	229
[표 2-1-16] 수집목적 이외 다른 기관에의 제공(일반인 대상)	231
[표 2-1-17] 수집목적 이외 수사기관에의 제공(일반인 대상)	231
[표 2-1-18] 수집목적 이외 다른 기관에의 제공(전문가 대상)	232
[표 2-1-19] 수집목적 이외 수사기관에의 제공(전문가 대상)	232
[표 2-1-20] (정부→정부) 개인정보 공유에 대한 태도	233
[표 2-1-21] (정부→금융기관) 개인정보 공유에 대한 태도	234
[표 2-1-22] 오프라인(이메일 포함) 자료공유 현황	241
[표 2-1-23] 기업의 개인 정보 수집방법	246
[표 2-1-24] 개인들의 홈페이지 회원가입을 통해 기업들이 수집하는 정보현황	249
[표 2-1-25] 자동차 매매 계약 시 제공되는 정보의 공유업체	261
[표 2-1-26] 전자회사에서 수집하는 고객정보	263
[표 2-1-27] LG생활건강의 DB 구성	264
[표 2-1-28] 개인의 기업에 대한 정보 제공목적(2002, 2003, 2006년)	268
[표 2-1-29] 개인의 개인정보 제공에 따른 우려도	270
[표 2-1-30] 세분집단별 응답률과 이익	280

[표 2-1-31] CRM 활동을 통한 고객 순현재가치	283
[표 2-2-1] 개인정보 보호 관련법제 현황	293
[표 2-2-2] 개별 분야별 개인정보보호입법과 주요 내용	294
[표 2-4-1] 일본의 개인정보보호 법률체계	402
[표 2-4-2] 2007년 제정되거나 재검토가 이루어진 가이드라인	418
[표 2-4-3] 개인정보취급사업자에 대한 주무대신에 의한 권한행사의 상황	418
[표 2-4-4] 각 부처별 인정개인정보보호단체의 인정상황	419
[표 2-4-5] 인정개인정보보호단체에 대한 주무대신의 권한행사 상황	420
[표 2-4-6] 기관별 고충상담 수	422
[표 2-4-7] 사업분야별 고충상담 수	423
[표 2-4-8] 상담내용의 내역	423
[표 2-4-9] 상담처리결과의 상황	424
[표 2-4-10] 유출자 수	425
[표 2-4-11] 유출된 정보의 종류	426
[표 2-4-12] 유출형태와 암호화 등의 정보보호조치	427
[표 2-4-13] 유출형태별 보호조치의 비율	428
[표 2-4-14] 【참고】 2006년	428
[표 2-4-15] 【참고】 2006년	429
[표 2-4-16] 유출원 및 유출한 자	429
[표 2-4-17] 【참고】 2006년	430
[표 2-4-18] 유출 후의 개선조치상황	431

[표 2-4-19] 안전관리대책 이외의 개선조치 내역	431
[표 2-4-20] 인정개인정보보호단체의 활동상황	432
[표 2-4-21] 【참고: 2006년의 상황】	433
[표 3-1-1] 기본법의 개별법을 규정한 해외사례	488
[표 3-1-2] 미국의 개인정보관련 법제 현황	490
[표 3-1-3] 민간부문에서의 개인정보보호입법	497
[표 3-1-4] 일본의 개인정보보호 법률체계	578
[표 3-1-5] 미국·캐나다·영국·독일의 개인정보보호법제 비교	579
[표 3-1-6] 프랑스·이탈리아·스페인·일본의 개인정보보호법제 비교	580
[표 3-1-7] 각국의 개인정보보호 법률체계	584
[표 3-2-1] 개인정보보호 관련 법조항 검색 여부	598
[표 3-2-2] 개인정보보호 법조항 검색시 어려움 있었는지 여부	600
[표 3-2-3] 검색시 어려움을 느낀 이유	601
[표 3-2-4] 개인정보보호법 공공부문과 민간부문 별도 적용의 인지 여부	604
[표 3-2-5] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호 대상으로 하고 있다는 사실의 인지 여부	606
[표 3-2-6] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부	608
[표 3-2-7] 개인정보가 제대로 보호되고 있는지에 대한 동의	610
[표 3-2-8] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유	612
[표 3-2-9] 강화된 ‘개인정보보호법’ 제정 필요도	614
[표 3-2-10] 개인정보보호 관련 법조항 검색 여부	616

[표 3-2-11]	개인정보보호 법조항 검색시 어려움 있었는지 여부	618
[표 3-2-12]	검색시 어려움을 느낀 이유	619
[표 3-2-13]	개인정보보호법과 공공부문과 민간부문 별도 적용의 인지 여부	621
[표 3-2-14]	‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호의 대상이 된다는 사실의 인지 여부	623
[표 3-2-15]	민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부	624
[표 3-2-16]	개인정보가 제대로 보호되고 있는지에 대한 동의	626
[표 3-2-17]	강화된 ‘개인정보보호법’ 제정 필요도	629
[표 3-2-18]	개인정보보호법 제정에 대한 인지	630
[표 3-2-19]	통합적 법률 제정에 대한 찬성/반대 의견	632
[표 3-2-20]	통합적 법률 제정의 찬성 이유	633
[표 3-2-21]	통합적 법률 제정시 입법체계	635
[표 3-2-22]	기본법에서 규율해야 할 경우 항목	637
[표 3-3-1]	개인정보보호 관련법제의 현황	643
[표 3-3-2]	개별 분야별 개인정보보호입법과 주요 내용	644
[표 3-3-3]	현행 개인정보보호법제의 체계	645
[표 3-3-4]	입법평가의 기준	689
[표 3-3-5]	각 모델의 비교	693
[표 4-3-1]	수집된 개인정보의 소유권자	732
[표 4-3-2]	수집된 개인정보의 소유권자	734

[표 4-3-3] 개인정보수집 관련 프라이버시 침해 등 문제 발생 등의 정도	735
[표 4-3-4] 개인정보수집 관련 프라이버시 침해 등 문제 발생 등의 정도	736
[표 5-2-1] 유럽평의회 회원국의 감독기구 현황	870
[표 5-2-2] 유럽평의회 비회원국의 감독기구 현황	871
[표 5-2-3] 각국의 개인정보감독기구 현황	887
[표 5-3-1] 공공부문의 개인정보감독기구	893
[표 5-3-2] 민간부문의 개인정보감독기구 현황	894

【그림】

[그림 2-1-1] UN의 전자정부 발전모형	206
[그림 2-1-2] 기관별 구비서류 징구현황(2005년 기준)	210
[그림 2-1-3] 행정정보 공유시스템 구성도	212
[그림 2-1-4] 주소변경 알리미 서비스	218
[그림 2-1-5] 전자민원 G4C 민원신청, 발급, 열람 건수	219
[그림 2-1-6] 행정정보공동이용센터 개념도	222
[그림 2-1-7] (정부→정부) 개인정보 공유에 대한 태도	234
[그림 2-1-8] (정부→금융기관) 개인정보 공유에 대한 태도	235
[그림 2-1-9] 내부통제 개념도	236
[그림 2-1-10] 유통구간 암호화 개요	239
[그림 2-1-11] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유	242

[그림 2-1-12] 회원 가입시 이용약관과 개인정보 활용 동의(Daum) ...	259
[그림 2-1-13] 회원 가입시 이용약관 및 개인정보 활용 동의(Naver) ...	259
[그림 2-1-14] 주민번호 수집 여부	260
[그림 2-1-15] DB 구축 사용률	261
[그림 2-1-16] 현대자동차 매매 계약서	262
[그림 2-1-17] 개인정보 수집 시 기업이 제공하는 권리	265
[그림 2-1-18] 개인정보 수집/위탁 시 이용자 고지 및 약관 명시 내용 ...	266
[그림 2-1-19] 주민번호를 통한 본인확인의 적절성에 대한 인식	267
[그림 2-1-20] 개인정보 제공목적(2006년)	268
[그림 2-1-21] 개인정보 제공 경험이 많은 사이트	269
[그림 2-1-22] 기업이 수집한 고객정보 이용에 대한 태도(일반인)	271
[그림 2-1-23] 기업이 수집한 고객정보 이용에 대한 태도(전문가)	271
[그림 2-1-24] 기업의 개인별 프로필 이용에 대한 태도(일반인)	272
[그림 2-1-25] 기업의 개인별 프로필 이용에 대한 태도(전문가)	273
[그림 2-1-26] 기업이 수집한 나의 연락 정보 판매에 대한 태도 (일반인)	273
[그림 2-1-27] (기업→기업) 개인별 프로필 판매에 대한 태도 (일반인)	274
[그림 2-1-28] 기업이 수집한 나의 연락 정보 판매에 대한 태도 (전문가)	275
[그림 2-1-29] (기업→기업) 개인별 프로필 판매에 대한 태도 (전문가)	276
[그림 2-1-30] 유형별 개인정보/프라이버시 침해 피해 경험	278

[그림 2-1-31] 개인정보유출피해사례	286
[그림 2-1-32] 국가별 IT 투자 대비 정보보호 투자 비율	286
[그림 2-1-33] 사내 정보보호 수준에 대한 우려 원인	287
[그림 2-1-34] 개인정보보호 교육 실시 여부	288
[그림 2-1-35] 개인 정보 제공시 관리수준 확인 여부	289
[그림 2-1-36] 개인정보 제공 시 관리수준 확인하지 않은 이유	289
[그림 2-1-37] 개인정보 보호정책 및 이용약관에서 확인하는 내용	290
[그림 2-2-1] 공공기관 개인정보보호법의 집행체계	307
[그림 2-2-2] 정보통신망법의 집행체계	326
[그림 2-4-1] 공시대상인 개인정보 파일 수 및 보유기관 수의 추이 ...	415
[그림 2-4-2] 성별	436
[그림 2-4-3] 연령	436
[그림 2-4-4] 직업	437
[그림 2-4-5] 관련단체	438
[그림 2-4-6]	439
[그림 2-4-7]	441
[그림 2-4-8]	442
[그림 2-4-9]	443
[그림 2-4-10]	444
[그림 2-4-11]	445
[그림 2-4-12]	446

[그림 2-4-13]	447
[그림 2-4-14]	448
[그림 3-1-1] 프라이버시 영향평가 절차도	526
[그림 3-2-1] 개인정보보호 관련 법조항 검색 여부	597
[그림 3-2-2] 개인정보보호 법조항 검색시 어려움 있었는지 여부 ...	599
[그림 3-2-3] 검색시 어려움을 느낀 이유	599
[그림 3-2-4] 개인정보보호 관련 내용이 포함되어 있을 것 같은 법률 ...	603
[그림 3-2-5] 개인정보보호법 공공부문과 민간부문 별도 적용의 인지 여부	604
[그림 3-2-6] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호대상인 점의 인지 여부	605
[그림 3-2-7] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부	607
[그림 3-2-8] 개인정보가 제대로 보호되고 있는지에 대한 동의	609
[그림 3-2-9] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유 ...	611
[그림 3-2-10] 강화된 ‘개인정보보호법’ 제정 필요도	613
[그림 3-2-11] 개인정보보호 관련 법조항 검색 여부	615
[그림 3-2-12] 개인정보보호 법조항 검색시 어려움 있었는지 여부 ...	617
[그림 3-2-13] 검색시 어려움을 느낀 이유	617
[그림 3-2-14] 개인정보보호 관련 내용이 포함되어 있을 것 같은 법률 ...	620
[그림 3-2-15] 개인정보보호법 공공부문과 민간부문 별도 적용의 인지 여부	621
[그림 3-2-16] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호의 대상이 된다는 사실의 인지 여부 ...	622

[그림 3-2-17] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부	624
[그림 3-2-18] 개인정보가 제대로 보호되고 있는지에 대한 동의	625
[그림 3-2-19] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유	627
[그림 3-2-20] 강화된 ‘개인정보보호법’ 제정 필요성	628
[그림 3-2-21] 개인정보보호법 제정에 대한 인지	630
[그림 3-2-22] 통합적 법률 제정에 대한 찬성/반대 의견	631
[그림 3-2-23] 통합적 법률 제정의 찬성 이유	633
[그림 3-2-24] 통합적 법률 제정시 입법체계	635
[그림 3-2-25] 기본법에서 규율해야 할 경우 항목	636
[그림 3-2-26] 민간부문에 대한 일반법 별도 제정 필요성	638
[그림 4-3-1] 수집된 개인정보의 소유권자	731
[그림 4-3-2] 수집된 개인정보의 소유권자	733
[그림 5-2-1] 독일 연방정보위원회의 조직	879
[그림 5-2-2] 프랑스의 정보자유위원회	881

제 1 편
개인정보보호법제에 관한
입법평가의 방향설정

제 1 장 입법평가의 개요

제 1 절 입법평가의 필요성과 목적

1. 입법평가의 필요성

우리나라에서 개인정보의 처리에 관하여 규율한 최초의 입법은 1980년 12월 18일 제정·공포된 「형의 실효 등에 관한 법률」(1980. 12. 18 시행)이라고 할 수 있다. 이 법률은 범죄기록의 작성 및 관리에 관한 사항을 정한 것으로서, 다른 국가기관이 개인의 범죄기록을 조회할 수 있는 경우를 제한적으로 정하고 그 이상의 제3자 제공을 금지하며, 형의 실효 등 일정한 사유가 있는 때에는 해당 기록을 삭제하도록 하고 있다. 그러나 이 법률은 엄밀히 말하면 개인정보보호법이라기보다는 비밀보호법이라고 할 수 있다.¹⁾

우리나라에서 개인정보의 처리(=수집·이용·제공)와 관련하여 정보주체의 권리와 이익을 보호하면서도 개인정보의 처리를 가능하게 하기 위한 본격적인 의미의 개인정보보호법은 1994년 1월 7일 공포된 「공공기관의 개인정보보호에 관한 법률」(1995. 1. 8. 시행)이 최초이다. 이 법률은 공공기관에서 보유하고 있는 개인정보데이터베이스의 운영과 관련하여 개인정보의 수집·이용·제공의 허용기준과 그 처리의 절차적 요건을 정하고 아울러 정보주체에게는 열람권·정정청구권 등의 참여권을 줌으로써, 한편에서는 개인정보의 적정한 이용을 허용하면서 동시에 다른 한편에서는 안전장치를 마련하여 프라이버시 등 정보주체의 권리나 이익이 함부로 침해되지 않도록 보호하고자 하는 것이다. 이처럼 개인정보의 이용과 보호를 조화시키고자 하는 개인정보보호법

1) 개인정보보호법과 비밀보호법의 개념구별과 차이에 대해서는 아래 제1편 제2장 제2절 참조.

이 민간부문에서 처음으로 입법화된 것은 1995년 1월 5일 공포된 「신용정보의 이용 및 보호에 관한 법률」(1995. 7. 6. 시행)이다. 이 법률은 신용정보업을 건전하게 육성하고 신용정보²⁾의 효율적 이용과 체계적 관리를 기하며 신용정보의 오·남용으로부터 개인의 프라이버시 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 하여 제정되었다.

그리고 온라인상의 개인정보보호를 최초로 법제화한 것은 1999년의 「정보통신망 이용촉진 등에 관한 법률」(2000. 1. 1. 시행)이다. 이 법률은 기존의 「전산망 보급 확장과 이용촉진에 관한 법률」을 개정함으로써 원래 개인정보보호법으로 출발한 것은 아니었다. 그러나 1990년대 후반 우리나라에서 인터넷 이용이 급속도로 증가하면서 이용자들의 개인정보보호에 대한 우려가 고조되기 시작하였고, 이러한 우려가 막 태동하기 시작한 전자상거래의 활성화를 저해할 것이라는 고려가 작용하면서 당시 정보통신부의 주도에 의하여 처음부터 매우 강력한 개인정보보호법으로 출발하였다. 정보통신서비스제공자가 이용자의 개인정보를 처리(=수집·이용·제공)하는 경우에 원칙적으로 정보주체의 동의를 받도록 요구하였던 것이다. 이러한 정책적 기조는 2001년의 개정법에서 더욱 강화되었다. 나아가 2001년의 개정법은 법의 적용대상자를 정보통신서비스제공자 외에도 재화나 용역을 제공하는 자로서 대통령령이 정하는 오프라인 민간사업자(여행업자, 호텔업자, 항공운수사업자, 학원·교습소, 기타 정보통신부령으로 정하는 자)에게까지 확대하였다.

또한, 2004년에는 민간부문에서의 유전정보(유전자검사의 결과로 얻어진 정보)의 이용과 보호를 특별히 규율하기 위한 「생명윤리 및 안

2) “신용정보”란 금융거래등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보로서 대통령령이 정하는 정보를 말한다(법 제2조 제1호). 이들 정보는 신용정보주체의 식별정보, 신용불량정보, 신용거래정보, 신용능력정보, 그리고 공공기록정보로 분류된다.

전에 관한 법률』(2005. 1. 1. 시행)이 제정되었으며, 또한 2005년에는 이동통신기술의 급속한 발달로 물류, 보안, 상거래 등의 영역에서 위치정보를 이용하는 다양한 서비스가 등장함에 따라 위치정보의 유출 및 오·남용으로부터 개인의 프라이버시 등을 보호하고 위치정보의 안전한 이용환경을 조성하기 위하여 「위치정보의 보호 및 이용 등에 관한 법률』(2005. 7. 28. 시행)이 제정되었다.

한편, 이상의 개인정보보호법 외에도 현재 상당히 많은 비밀보호규정들이 여러 법률에 산재해 있다. 「형법」상의 비밀침해죄(제316조)와 업무상비밀누설죄(제317조), 「통신비밀보호법」, 「의료법」, 「국민건강보험법」, 「국세기본법」, 「공직자윤리법」, 「전염병예방법」, 「후천성면역결핍증 예방법」, 「금융실명거래 및 비밀보장에 관한 법률」, 「공증인법」, 「변호사법」등이 그것이다.

이렇게 다양한 개인정보보호법과 비밀보호법들이 존재하고 있지만, 일반 국민들은 개인정보의 처리(=수집·이용·제공)와 관련하여 자신들의 프라이버시가 제대로 보호받고 있지 못하다는 인식이 널리 확산되어 있다. 그러나 역으로 한편에서는 강력한 개인정보보호법제로 인하여 사회적으로 필요한 개인정보의 유통이 합법적으로 이루어지지 못한 채 음성적으로 혹은 불법적으로 유통되는 현실을 우려하는 목소리 또한 적지 않다.

이처럼 개인정보의 이용과 보호의 문제는 그것을 바라보는 관점에 따라서 또는 프라이버시에 대한 인식의 차이에 따라서 매우 현격한 격차를 보이고 있다. 타인이 나에 관한 정보를 수집한다는 것 자체에 민감한 반응을 보이는 사람이 있는가 하면, 그에 대해 전혀 무감감한 사람도 있다. 예컨대, 정부가 주민등록증의 발급시에 지문정보를 수집하는 것에 대하여 심한 거부반응을 보이는 사람이 있는가 하면, 한편으로 그 필요성을 인식하는 사람은 전혀 거부감을 느끼지 않는다. 오히려 후자 중에는 정부의 지문정보 수집에 대해 정부로부터 보호를

받는다고 느끼는 사람도 있다. 아파트 현관에 설치된 CCTV가 우리의 안전을 지켜준다고 믿는 사람에게 그것은 자연스럽게 받아들여지는 반면, 나의 출입시간과 모습이 일일이 기록된다는 것에 대하여 거부 반응을 보이는 사람도 있다.

사실 기록된 개인정보 그 자체는 날카로운 칼과 같이 언제나 양면성을 지니고 있다. 외과 의사가 수술을 위해 사용하는 칼은 사람의 생명을 살리는 칼이 되지만, 강도가 사용하는 칼은 사람을 죽이는 칼이 된다. 기록된 개인정보 또한 누가 어떤 연관에서 이용하느냐에 따라 그 효용이 높을 수도 있고 위험할 수도 있다. 아파트 현관에 설치된 CCTV가 자신의 출입시간과 모습을 일일이 기록하는 것에 대해 거부 반응을 보이는 사람도 그 기록을 토대로 자신이 어느 범죠헌장에 있지 않았다는 알리바이(현장부재증명)의 자료로 유익하게 활용될 수도 있다.

결국 개인정보의 이용과 보호를 어떻게 규율할 것인가는 개인정보 처리(=수집·이용·제공)의 효용성과 위험성을 어떻게 평가하느냐에 달려 있다. 위에서 살핀 많은 개인정보보호법과 비밀보호법들은 이러한 평가에 입각해서 마련되어 있는 것이지만, 그 내용을 면밀히 분석해보면 체계성이 결여되어 있거나 이용과 보호의 균형이 맞지 않는 경우가 많다. 개인정보처리의 효용성과 위험성에 대한 정확한 평가에 기초하여 마련되지 않았기 때문이다. 그리하여 어떤 법률의 규정은 위험성에 대한 과도한 평가로 인해 보호 쪽에 지나치게 치우쳐 있는 반면, 어떤 법률의 규정은 이용의 가치에 경도되어 보호의 수준을 낮게 설정하고 있는 경우도 있다. 또 현재 민간부문의 일반법으로서의 개인정보보호법이 존재하지 않고 있어 많은 영역에서는 보호의 공백이 발생하고 있는가하면, 또 어떤 영역에서는 비밀보호법에 의한 보호로 인해 필요한 이용이 거의 불가능하게 되어 있는 경우도 있다. 또한 개인정보보호법과 비밀보호법이 제대로 구분되지 않은 채 “개인정보”를 마치 “비밀”로 취급하는 잘못된 접근방법을 취하고 있는 법

률이 있으며(대표적으로 정보통신망법), 그러한 법률이 일반 국민들의 규범의식을 오도된 방향으로 이끌고 있는 것으로 판단된다. 나아가 이렇게 잘못된 경향은 대형의 개인정보 누출사고가 터질 때마다 더욱 증폭되어 일반 국민의 의식 속에 자리 잡고 그것이 다시 입법과정에 투영된다.

이러한 상황 속에서 개인정보의 수집·이용·제공을 규율하고 있는 여러 개인정보보호법과 비밀보호법들을 총체적으로 점검해 볼 필요성이 매우 크다. 난마처럼 얽혀 있는 복잡한 관련 법제들을 분석하여 거기에 체계성을 부여하고, 나아가 개인정보의 이용과 보호의 합리적인 조화와 균형을 모색하는 작업은 매우 긴급하고 중요한 입법정책적 과제라고 판단된다.

2. 입법평가의 목적

지난 2003년부터 5~6년에 걸쳐 개인정보보호법제를 새롭게 정비하려는 노력들이 정부와 시민단체, 그리고 학계에서 꾸준히 그리고 다각도로 이루어져 왔다. 다양한 개인정보보호법들이 공공부문과 민간부문으로 이원화되어 있고 여러 개별입법들이 존재하고 있어 개인정보처리기관이나 정보주체인 일반 국민의 입장에서 관련 법규에 대한 이해도가 낮고 법적 규율의 실효성도 떨어지며, 또 민간부문에서는 일반법이 없어 일부 보호의 공백이 생기는 영역이 있는 등 문제점이 제기되었고, 그리하여 이를 개선하려는 노력의 일환으로 공공과 민간의 모든 개인정보처리를 규율하는 기본법 혹은 일반법을 제정하려는 움직임이 크게 일어났다.

그러나 그 입법개선의 방향과 내용에 대해서는 정부, 시민단체, 학계가 각각 입장이 달라 어느 하나의 합의점에 이르지 못하였다. 우선, 입법개선노력에 불을 지핀 것은 정보인권에 관심을 가진 시민단체들

이었다.)³⁾ 일찍부터 이들 시민단체들은 신뢰성 있는 정보사회의 구축을 위해서는 공공과 민간을 아우르는 개인정보보호기본법을 제정하고 양 부문의 개인정보처리를 독립적으로 감독하는 통합된 개인정보감독기구의 설립을 주장하여 왔다.

그러는 가운데 노무현 정부가 출범하고 2003년 10월에 당시 대통령 소속의 정부혁신지방분권위원회(전자정부전문위원회)는 개인정보보호가 전자정부의 성패를 좌우하는 문제일 뿐만 아니라 정보사회의 토대라는 점을 인식하고 공공과 민간을 아우르는 개인정보보호법을 제정한다는 방침을 정하고 대통령의 재가를 받아 이를 국정과제로 채택하였다.

그러나 정부 내에서 합의가 쉽게 이루어지지 못하였다. 당시 공공부문의 개인정보보호법인 「공공기관의 개인정보보호에 관한 법률」을 관장하고 있던 (구)행정자치부는 공공과 민간을 아우르는 일반법의 제정에 소극적이었다. 일반법이 제정되면 (구)행정자치부가 그 일반법의 관장부처가 된다는 보장이 없었고 당시 시민단체가 주장하는 독립된 개인정보감독기구로 개인정보보호업무가 이관될 가능성이 높았다. 당시 전자정부의 추진책임을 맡고 있던 (구)행정자치부로서는 공공부문의 개인정보처리에 관하여 독립된 감독기구의 통제를 받을 수 있다는 것이 커다란 부담으로 작용했던 것으로 판단된다. 이 때문에 (구)행정자치부는 일반법의 제정 대신 「공공기관의 개인정보보호에 관한 법률」을 개정하여 보호를 강화하면서 각 부처의 개인정보처리에 대한 감독 권한을 확대해가고자 하였다. 한편 당시 온라인개인정보보호법인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(제4장)을 관장하고 있던 (구)정보통신부 역시 공공과 민간을 아우르는 일반법 제정에 부정적이었다. 대신에 (구)정보통신부는 정보통신망법을 개정하여 민간부

3) 이 운동은 특히 진보네트워크센터와 함께하는시민행동이 주도하였으며, 그밖에 지문날인반대연대, 문화연대, 민주사회를위한변호사모임, 참여연대, 한국노동네트워크협의회 등이 이에 적극 동참하였다. 그리하여 프라이버시법제정을위한연석회의가 구성되기도 하였다.

문의 일반법을 제정하여 이를 관장하고자 하는 의욕을 나타내었다.⁴⁾

한편, 학자들과 전문가 사이에서는 개인정보보호에 관한 입법체계를 어떻게 정립할 것이냐를 놓고 견해가 대립되었다. 공공부문과 민간부문을 분리하여 별도의 입법체계로 가져가자는 입장(분리입법론)과 공공과 민간을 통합한 입법체계를 새로이 마련하자는 입장(통합입법론)으로 크게 나누어졌다. 통합입법론은 다시 공공과 민간의 개인정보처리를 동일하게 규율하는 통합일반법을 제정하자는 입장(통합일반법제정론)과 기본법을 제정하자는 입장(기본법제정론)으로 나누어졌다. 이들 입법체계에 관한 논의들은 실체법적 문제, 즉 개인정보처리기관에게 어떤 의무를 부과하고 정보주체에게 어떤 권리를 배분할 것인가에 관한 문제뿐만 아니라, 법집행체계, 즉 개인정보감독기구의 구성, 관할범위, 권한 등에 관한 입장의 차이와 관련되어 있다.

이러한 사정 하에서 여러 입장을 각각 반영하는 개인정보보호법(안)들이 국회에 제출되었다. 2004년 후반기에 『공공기관의 개인정보보호에 관한 법률』의 개정안 3건과 민주노동당의 『개인정보보호기본법(안)』(노회찬 의원 대표발의; 이하 “노회찬 법안”)이 국회에 제출되었다. 이 노회찬 법안은 시민단체들의 주장을 반영한 것이었다. 그리고 이어 2005년 2월에는 당시 여당인 열린우리당에서 2건의 『개인정보보호기본법(안)』을 국회에 제출하였다. 당시 정성호 의원이 2005년 2월 1일에 독자적으로 마련한 『개인정보보호법(안)』을 발의하였고, 2005년 2월 2일에는 이은영 의원이 개인정보보호의 기본원칙, 정보주체의 참여권 보장, 국가인권위원회의 개인정보특별위원회를 통한 권리구제 등을 골자로 하는 『개인정보보호기본법(안)』을 발의하였다. 이 이은영 의원이 발의한 법안은 정부혁신지방분권위원회 내 전자정부전문위원회

4) 그리하여 (구)정보통신부는 정보통신망법상의 개인정보보호규정(제4장)을 떼어내어 민간의 모든 개인정보처리를 규율하는 일반법으로서 이른바 『민간부문의 개인정보보호에 관한 법률(안)』을 마련하여 2004년 5월 19일 이를 입법예고하였다(정보통신부공고 제2004-32호).

(전자정부법제정비소위원회)에서 검토해 온 입장들을 정리한 것이었다.

그런데 이들 법안이 제출되고 나서, 개인정보감독기구의 조직구성을 놓고 국가인권위원회 소속의 특별위원회로 하자는 정부여당안과, 독립된 별도의 조직으로 구성해야 한다는 시민단체의 주장이 팽팽히 맞섰다. 그런 와중에 2005년 4월 11일 국가인권위원회가 개인정보감독기구는 별도의 조직으로 구성되어야 한다는 의견을 공식적으로 의결하였다. 그러자 2005년 4월 15일 열린우리당에서 제안된 2건의 기본 법안이 모두 철회되었다. 이후 열린우리당은 2005년 7월 11일 개인정보감독기구를 국무총리 소속 하에 두는 내용의 『개인정보보호법(안)』(이은영의원 대표발의, 찬성자 145인; 이하 “이은영 법안”)을 열린우리당의 당론으로 새로이 제출하였다.

그런데 위 노회찬 법안과 이은영 법안은 그 지난한 노력에도 불구하고 개인정보 “보호의 가치”와 “이용의 가치”를 균형 있게 조정할 결과인지에 대해 의문이 제기되었다. 세계에서 보기 드물 정도로 매우 강력한 보호기준을 설정하고 있으며, 더 나아가 매우 불명확한 행위기준에 의한 형사처벌 및 행정제재 위주로 그 집행을 담보하고 있었다. 이 두 법안은 개인정보의 수집단계에서부터 정보주체의 동의를 사전 또는 사후에 받는 것을 원칙으로 하고 있는데, 그렇게 되면 개인정보의 보호는 충분히 강화되겠지만, 사회적으로 필요한 개인정보의 이용과 유통은 현저히 억제되어 자칫 사회적·경제적 기능이 경색되는 것이 아닌가 하는 우려가 제기되었다. 이런 가운데 2005년 10월 17일 한나라당의 이해훈 의원이 대표발의한 『개인정보보호법(안)』[이하 “(구)이해훈 법안”]이 국회에 제출되었다.

이들 세 법안은 모두 공공과 민간을 아우르는 일반법으로서의 성격을 가지고 있었지만, 개인정보처리(=수집·이용·제공)의 허용기준과 절차적 요건, 정보주체의 참여권, 그리고 감독기구의 조직구성과 권한 등 그 내용면에서는 상당한 차이를 보이고 있었다.

[표 1-1-1] 제17대 국회 제출 개인정보보호법(안) 개요

	이은영 법안	노회찬 법안	(구)이혜훈 법안
적용영역	공공·민간 모두 적용 ※ 단, 현행 공공기관개인정보보호법·정보통신망법 유지	공공·민간 모두 적용 ※ 현행 공공기관개인정보보호법·정보통신망법 폐지	공공·민간 모두 적용 ※ 현행 공공기관개인정보보호법·정보통신망법 폐지
규율대상	업무 목적의 개인정보취급자	개인정보처리자	업무 목적의 개인정보처리자
보호의대상	생존하는 자연인의 개인정보 ※ 개인정보화일 개념 부재 ※ 민감정보 구분 있음	자연인의 개인정보 ※ 사망자의 개인정보 포함 ※ 개인정보화일 개념 존재 ※ 민감정보 구분 있음	생존하는 자연인의 개인정보 ※ 개인정보화일 개념 존재 ※ 민감정보 구분 있음
적용의예외	언론·학술연구·종교 등 적용예외 없음 ※ 단, 언론목적의 수집 허용	언론·학술연구·종교 등 적용예외 없음 ※ 단, 언론목적의 수집 허용	언론·학술연구·종교·정당의 경우 적용 면제
정보처리의법적기준	· 수집 이후 사후 동의 · 민감정보 수집 원칙적 금지 · 동의받은 목적 외 이용 및 제공 원칙적 금지 · 영리목적 판매 명시적 동의 · 언제든지 동의 철회 가능 · 부당차별목적 수집·이용금지 · 위 기준 위반 형사처벌	· 원칙: 수집시 사전 동의 · 좁은 예외 인정 (5가지) · 민감정보 수집 원칙적 금지 · 동의받은 목적 외 이용 및 제공 원칙적 금지 · 언제든지 동의 철회 가능 · 위 기준 위반 형사처벌	· 공공부문: 법률근거 있으면 동의 불필요. 단, 임무수행에 필요한 한도 내 수집·처리 · 민간부문: 처리자의 정당한 권리실현을 위해 필요한 경우 동의 불필요 ※ 단, 개인정보 판매목적 수집시 사전 동의
목적구속원칙	· 엄격하게 인정 · 고유식별자 목적외사용금지	· 엄격하게 인정 · 고유식별자 목적외사용금지	· 엄격하게 인정 · 고유식별자 목적외사용금지
정보정확성	· 정확성 유지의무/정정청구권 · 목적 달성 후 원칙적인 삭제·파기(공공부문 예외) · 위반 시 과태료	· 정확성유지의무/정정요구권 · 목적 달성 후 원칙적 파기 · 위반 시 형사처벌	· 정정·보완·삭제·갱신요구권 · 목적달성 후 원칙적 파기 · 위반 시 과태료

제 1 편 개인정보보호법제에 관한 입법평가의 방향설정

	이은영 법안	노회찬 법안	(구)이혜훈 법안
보안	· 보안 유지 의무	· 보안 유지 의무	· 보안 유지 의무
참여 원칙	· 열람·정정청구권 · 동의철회권 · 무과실 입증책임 부과 · 집단소송제 도입 없음	· 열람·정정요구권 · 동의철회권 · 무과실 입증책임 부과 · 집단소송제 도입	· 열람·정정요구권 · 동의철회권 · 이용·제공정지요구권 · 무과실 입증책임 부과 · 집단소송제 도입 없음
감독 원칙	· 개인정보보호위원회(국무총리 소속) 설치 · 개인정보분쟁조정위원회·침해신고센터 설치 · 개인정보사건영향평가제/개인정보DB등록제 도입 없음	· 개인정보보호위원회(독립기 구) 설치 · 개인정보사건영향평가제 /개인정보DB등록제 도입	· 개인정보위원회(국무총리 소속) 설치 · 개인정보분쟁조정위원회 · 개인정보사건영향평가제 도입(공공 의무, 민간 자율) · 개인정보DB등록제 도입

그런데 국회 내에서 심의를 위해 이들 세 법안이 배정되었던 위원회는 행정자치위원회였다. 불행히도 이들 세 법안을 제출한 의원들은 모두 행정자치위원회 소속이 아니었다. 아무튼 국회 행정자치위원회에서는 이들 법안을 2005년 12월 5일 단 한 차례 상정하여 심의한 이후 더 이상 진척이 없는 상태에서 2008년 5월 29일 임기만료로 폐기되고 말았다. 반면에, 이 기간 동안에 『공공기관의 개인정보보호에 관한 법률』의 개정안이 2007년 5월 17일 공포되었고, 『정보통신망 이용촉진 및 정보보호에 관한 법률』의 개정안은 3차례에 걸쳐 개정되었다. 개별입법은 개정되는 중에도 일반법인 개인정보보호법안들은 국회에서 잠자고 있었던 것이다.

그런데 이러한 사정에 커다란 변화가 일어났다. 2008년 2월 이명박 정부가 출범하면서 정부조직을 개편하는 과정에서 (구)정보통신부가 폐지되고 그 소관업무가 행정안전부와 방송통신위원회로 분산 이관되었으며, 정부조직법상 정보보호 업무가 행정안전부로 일원화되었다. 이에 따라 행정안전부가 개인정보보호 업무를 총괄하게 되면서 이전에 부정적이었던 개인정보보호법(안)의 제정을 적극적으로 추진하기 시작한 것이다.

그리하여 2008년 6월 27일 행정안전부는 제1차 공청회를 개최하여 구상하고 있는 개인정보보호법제정안에 대한 설명을 하였다. 이 제정안은 공공부문과 민간부문 모두에 적용되는 일반법으로서 이 법이 제정되면 현행의 「공공기관의 개인정보보호에 관한 법률」은 폐지하는 것으로 하고 있다. 지난 정부에서 일반법의 제정에 반대하던 행정안전부가 완전히 입장을 바꾼 것이다. 그러나 이 공청회에서의 핵심쟁점은 개인정보감독기구의 독립성 확보에 관한 것이었다.

공청회에서 제시된 법안설명에서는 행정안전부장관이 개인정보보호법의 집행 및 감독책임은 지는 주무부처이고 그 소속 하에 분쟁조정기능만을 주된 업무로 하는 개인정보분쟁조정위원회를 두도록 하고 있었다.⁵⁾ 이에 대해 진보넷 등의 시민단체와 일부 논자들은 법안이 개인정보감독기구의 독립성을 포기한 것이라고 강력하게 비판하였다. 이러한 비판에 직면한 행정안전부는 8월 12일 「개인정보보호법 제정 법률안」을 정식으로 입법예고하고 8월 28일 제2차 공청회를 열었다. 이 입법예고된 법률안에 의하면, 여전히 행정안전부장관이 집행 및 감독책임은 지는 주무부처이고 개인정보분쟁조정위원회가 분쟁조정기능을 수행하되, 몇 가지 사항에 대해 심의기능을 하는 개인정보보호위원회를 신설하여 국무총리 소속 하에 두는 것으로 하고 있다. 이 법안의 개인정보보호위원회를 개인정보감독기구라고 볼 수 있는지, 그리고 법안상의 집행 및 감독체계를 독립된 감독체계라고 볼 수 있는지가 문제되고 있다. 이런 상황에서 2008년 8월 8일 한나라당의 이혜훈 의원이 대표발의한 「개인정보보호법안」[이하 “(신)이혜훈 법안”]이 국회에 제출되었다.

이상의 과정을 살펴보면, 일반법인 개인정보보호법의 제정을 둘러싸고 여러 쟁점에서 첨예한 의견대립이 있음을 알 수 있다. 가장 대표적인 쟁점은 세 가지로 압축될 수 있는데, 첫째, 현재 여러 영역에서

5) 행정안전부, 『「개인정보보호법」 제정을 위한 공청회 자료집』, 2008. 6. 27 참조.

산발적으로 존재하는 여러 개별입법들을 어떤 체계로 조정할 것인가 하는 입법체계에 관한 문제, 둘째, 이용과 보호의 가치를 합리적이고 균형 있게 조화시키는 개인정보 처리(=수집·이용·제공)의 법적 기준이 무엇인가 하는 실체적인 문제(여기에는 개인정보처리의 허용기준, 절차적 요건, 정보주체의 참여권 등이 포함된다), 셋째, 그러한 법적 기준을 어떻게 집행할 것인가 하는 집행체계에 관한 문제, 특히 개인정보감독기구의 조직구성과 권한 및 기능을 어떻게 설정할 것인가 하는 문제를 들 수 있다.

본 입법평가의 기본목적은 이러한 세 가지 쟁점을 중심으로 현 시점에 제출되어 있는 행정안전부의 입법예고안과 (신)이혜훈 법안의 내용을 분석·평가하고 그 대안을 모색해보는 것이다. 이러한 병행입법평가를 통하여 향후 입법자가 법안을 심사하는 과정에서 활용할 수 있는 의미 있는 입법자료를 제공하는 데 궁극적인 목적이 있다.

제 2 절 입법평가의 유형과 대상

1. 사전적 입법평가와 대상

행정안전부의 입법예고안과 (신)이혜훈 법안에 대한 병행입법평가를 하기에 앞서 사전입법평가를 할 필요가 있다. 사전입법평가는 법률입안의 준비단계에서 진행되는 것으로서, 고려되는 규율사안에 대해 과연 그러한 법적 규율이 필요한 것인지, 왜 필요한 것인지, 그 필요성이 생겨나는 사회적 배경이 무엇인지, 규율사안과 관련하여 어떤 이해관계가 어떻게 충돌하고 있는지, 어떤 정책적 가치가 우선해야 할 것인지, 규율사안에 대한 법이론적 기초와 헌법적 법리가 어떻게 전개되는 것인지, 입법목적은 무엇으로 설정할 것인지, 관련된 법률과의 입법체계를 어떻게 설정할 것인지, 그리하여 총체적으로 입법방향을

어떻게 설정하는 것이 타당한지 등을 평가대상으로 한다.⁶⁾

본 연구에서는 이러한 사전입법평가를 위해 우선적으로 개인정보보호법의 존재이유와 특성을 살펴본다(제1편 제2장). 제1편 제2장에서는 개인정보보호법이 생겨나게 된 사회적 배경을 검토하기 위해서 개인정보보호법의 출현 이전까지 개인에 관한 정보의 처리를 규율하는 법제와 법리가 무엇이며, 디지털시대의 출현이라는 새로운 문제 상황에서 왜 개인정보보호법이라는 새로운 규율이 필요하게 되었는지를 분석한다. 나아가, 대체 개인정보보호법이 추구하고자 하는 입법목적이 정확히 무엇이며 기존의 사생활보호법이나 비밀보호법과 어떤 점에서 어떻게 다른지를 분석한다.

이어 제2편 제3장에서는 개인정보의 보호와 이용에 관한 이론적 기초 작업으로서 관련된 선행연구가 어떤 것이 있는지를 구조 차원과 행위자 차원에서 간략히 살펴보고, 개인정보보호법이 논의되게 된 기술적 배경으로서의 정보기술에 관하여 그 특징을 고찰한다. 나아가, 지금까지 법학의 영역에서 프라이버시의 본질을 어떻게 이해하고 있는지를 인격권과 재산권의 관점에서 고찰하고, 이어 사회학의 관점에서 개인정보의 처리와 관련해서 전개되었던 감시사회이론을 살펴본 다음, 마지막으로 프라이버시에 대한 경제학적 분석을 시도해 본다.

제2편 제4장에서는 개인정보보호의 문제를 헌법이론적인 관점에서 검토한다. 개인정보자기결정권 내지 자기정보통제권의 헌법적 근거가 무엇이며 어떤 내용을 담고 있는지 그리고 개인정보보호의 가치와 상충하는 또 다른 헌법적 가치에는 어떤 것이 있는지, 이 양자를 조화시키는 방법이 무엇인지에 관하여 분석한다.

6) 사전적 입법평가는 초안단계, 실행단계, 평가단계로 이루어지고, 초안단계는 다시 체계분석, 문제분석, 목표분석, 예상 가능한 기타의 시나리오 전개로 이루어진다고 한다. 박영도, 『입법학 입문』(한국법제연구원, 2008), 618면 이하 참조. 또한 홍준형, 『법정책의 이론과 실제』(법문사, 2008), 149면 이하 참조.

이상의 분석과 평가를 통해 향후 제정될 개인정보보호법의 기본방향을 설정한다.

2. 사후적 입법평가와 대상

사후적 입법평가는 법률의 제정 이후에 그 법률이 의도하는 목표에 도달하였는지, 어떤 부작용이 나타났는지, 법률이 실용적이고 준수가능한 것으로 입증되었는지, 그리고 개정 또는 폐지의 필요성이 존재하는지 등을 평가대상으로 한다.⁷⁾

위에서 살핀 바와 같이 1995년 이래로 현재 여러 영역에서 개인정보의 이용과 보호를 규율하는 입법들이 있다. 일반법으로 제시된 행정안전부의 입법예고안과 (신)이혜훈 법안에 대한 병행입법평가를 하기에 앞서 이들 선행하는 기존의 개별입법들에서 어떤 부작용과 문제점이 나타나고 있는지를 평가할 필요가 있다. 그럼으로써 그 문제를 극복하기 위한 일반법의 제정이 필요한지를 평가할 수 있게 될 것이다.

이를 위해 우선 제2편 제1장에서는 현재 공공기관과 민간기업에서 개인정보를 처리하는 현황과 실태를 분석하는 가운데 각 부문에서 개인정보처리의 효용성과 위험성을 평가해 본다. 이러한 효용성과 위험성에 대한 평가는 합리적인 개인정보처리의 입법기준과 집행체계를 마련함에 있어서 중요한 입법요소가 된다.

이어 제2편 제2장에서는 현재 시행되고 있는 각 영역의 개별 개인정보보호법들에 대한 내용분석을 시도한다. 각 개별입법의 입법연혁, 적용범위, 개인정보처리의 입법기준, 집행체계 등을 간략히 정리한다. 그 다음 제2편 제3장에서는 이들 개인정보보호법들에 대한 총괄적 평가를 시도한다. 먼저 세계적인 보호입법모델에 비추어 우리의 현행 개인정보보호법제의 위상을 점검해 보기 위하여, 정부 주도의 포괄

7) 박영도, 위의 책, 648면 이하; 홍준형, 위의 책, 149면 이하 참조.

적·일원적 입법모델인 유럽의 접근방식과 자율규제 중시의 이원적·부분별 입법모델을 채택하고 있는 미국의 접근방식을 개관한 다음, 우리의 이원적·영역별·부분적 보호법제가 이들 입법모델과 어떻게 다른지를 살핀다. 그리고 우리의 현행 보호법제가 안고 있는 문제점으로 (i) 불균형적이고 불완전한 보호체계라는 점, (ii) 예방적 집행기능이 부존재하고 처벌 위주의 사후집행체계라는 점, 그리고 (iii) 독립된 통합감독기구가 존재하지 않고, 영역별로 있는 감독기구들도 그 기능이 매우 불완전하고 미흡하다는 점을 분석해낸다.

마지막으로 제2편 제4장에서는 우리보다 앞서 기본법이면서 동시에 민간부문 일반법인 『개인정보의 보호에 관한 법률』을 2003년에 제정하여 시행하고 있는 일본의 시행경험을 분석하고 그로부터 우리의 입법에 참고가 되는 시사점을 도출해낸다. 일본의 이 일반법은 보호수준이 유럽의 개인정보보호법에 비하여 그렇게 높지 않은데도 시행 이후 사회적으로 개인정보처리에 대한 과잉반응의 문제가 드러났다는 점이 특별히 주목된다. 또한 일본이 개인정보의 이용과 보호를 추진해가는 방법과 내용은 우리에게 많은 시사점을 준다.

3. 병행적 입법평가와 대상

병행적 입법평가는 제출된 수개의 법률안 또는 법률안의 일부를 여러 심사기준에 따라 비교·분석하여 어떤 것이 최적의 입법안인지를 평가하는 작업이다. 병행적 입법평가에서는 조문화된 입법안이 전제하고 있는 기본개념과 사용하는 용어들이 규율하고자 하는 사안의 문제 상황을 정확하게 반영하고 있는지, 용어들이 명확하고 이해가능한지, 계획된 규정들이 준수가능하고 일반인에게 수용가능한지, 규정에 흠결과 결함이 없는지, 규정 상호간 또는 다른 법률규정 간에 모순이 없는지, 규율의 법적 기준이 대립하는 이익과 가치를 합리적으로

로 균형 있게 조율하고 있는지, 법적 기준을 집행하기 위한 집행기구나 방법 등의 집행체계가 실현가능하고 효율적인지 등을 평가대상으로 삼는다.⁸⁾

본 입법평가에서는 지금까지 구체적인 법률안의 형태로 국회에 제출되었거나 입법예고된 총 5건의 개인정보보호법안을 병행입법평가의 대상으로 삼는다. 즉 위에서 살핀 바와 같이 지난 제17대 국회에 제출되었다가 임기만료로 자동 폐기되었던 3건의 개인정보보호법안[“이은영 법안”, “노회찬 법안”, 그리고 “(구)이혜훈 법안”]과 2008년 8월 12일 행정안전부가 입법예고한 『개인정보보호법 제정법률안』(이하 “입법예고안”), 그리고 2008년 8월 8일 한나라당의 이혜훈 의원이 대표발의하여 현재 국회 행정안전위원회에 계류되어 있는 (신)이혜훈 법안을 분석한다.

그리고 이들 법안의 병행평가에 있어서는 현재 첨예한 의견대립을 보이고 있고 현안이 되어 있는 세 가지의 커다란 쟁점을 중심으로 평가를 시도한다. (i) 현재 여러 영역에서 산발적으로 존재하는 여러 개별입법들을 어떤 체계로 조정할 것인가 하는 입법체계에 관한 문제, (ii) 이용과 보호의 가치를 합리적이고 균형 있게 조화시키는 개인정보 처리(=수집·이용·제공)의 법적 기준이 무엇인가 하는 실체적인 문제(여기에는 개인정보처리의 허용기준, 절차적 요건, 정보주체의 참여권 등이 포함된다), (iii) 그러한 법적 기준을 어떻게 집행할 것인가 하는 집행체계에 관한 문제, 특히 개인정보감독기구의 조직구성권 및 기능을 어떻게 설정할 것인가 하는 문제가 그것이다.

우선 위 (i)의 입법체계에 대한 평가는 아래 제3편에서 다룬다. 이를 위해 먼저 개인정보보호의 입법체계를 어떤 방향으로 설정해야 할 것인지를 비교법적 관점에서 우선 검토하고(제1장), 입법체계와 관련하여 일반인과 전문가가 어떤 입장과 의견을 가지고 있는지를 알아보

8) 박영도, 위의 책, 634면 이하; 홍준형, 위의 책, 149면 이하 참조.

기 위하여 실시했던 설문조사의 결과를 분석하여 정리한다(제2장). 이어 각 입법안들이 상정하고 있는 입법체계의 내용을 분석하고 그에 대해 종합적인 평가를 내린다(제3장).

다음으로 위 (ii)의 개인정보처리의 입법기준에 대한 병행평가는 아래의 제4편에서 다룬다. 제4편은 행정안전부의 입법예고안을 대상으로 해서 주로 비교법적 분석방법을 사용하여 대표적인 개인정보보호법으로 거론되는 1995년의 유럽연합 개인정보보호지침, 영국과 독일의 개인정보보호법, 그리고 일본의 개인정보보호법과 비교하였다. 우선 입법예고안에서 채택하고 있는 기본개념과 용어에 대한 비교평가를 통해 문제점을 지적하고 그 수정대안을 제시한다(제2장). 다음으로 입법예고안의 수집·이용·제공의 허용기준에 대한 입법평가를 시도하였는데, 그 동안 우리나라에서는 정보주체의 동의 요건을 절대화하는 잘못된 경향이 있어 왔음을 설문조사를 통해 나타난 일반인의 의식과 태도, ‘개인정보침해’라는 언어사용례 분석, 현행의 정보통신망법과 지난 제17대 국회에서 제출되었던 이은영 법안과 노회찬 법안의 분석을 통해 밝힌다. 나아가, 수집·이용·제공의 허용기준을 입법화하고 있는 외국의 입법사례를 면밀하게 분석하고, 이에 기초해서 행정안전부의 입법예고안의 허용기준에 대하여 평가를 내리고 수정대안을 제시한다(제3장). 결론적으로 보면, 입법예고안은 개인정보보호법보다는 비밀보호법에 가까운 접근을 보이고 있어 그 실제의 적용과정에서 상당한 문제가 제기될 것으로 평가된다.

그리고 제4장에서는 개인정보의 처리(=수집·이용·제공)에 있어서 갖추어야 할 절차적 요건을 목적명시 요건, 품질관리 요건, 고지 요건, 그리고 보고 요건의 4가지로 나누어 비교법적 분석과 함께 입법예고안의 절차적 요건들을 분석·평가하고 수정대안을 제시한다(제4장). 이어 제5장에서는 공공기관의 개인정보처리의 입법기준을 별도로 떼어내어 그 타당성 여부를 평가하고, 특히 개인정보 공동이용에 대한 규율을 개인정보보호법 입법예고안이 아닌 「전자정부법 전부개정법

를(안)』에서 별도로 법제화하고 있는 것에 대해 분석·평가한다(제5장).

마지막으로, 위 (iii)의 집행체계에 대한 병행평가는 아래의 제5편에서 검토한다. 먼저 제1장에서는 개인정보감독기구의 설립방향을 설정하기 위하여 왜 독립된 감독기구를 필요로 하는지, 개인정보감독기구의 본래적 기능과 권한이 무엇인지를 분석하고, 이어 제2장에서는 독립된 감독기구의 설립에 관한 세계적인 추세가 어떠한지, 그리고 각국의 감독기구에 관한 비교법적 분석을 시도한다. 그리고 제3장에서는 각 법안들이 감독기구의 위상과 기능을 어떻게 각 설정하고 있는지를 비교 분석한 다음, 제4장에서 개인정보감독기구의 설립방안에 관하여 대안적 결론을 제시한다.

4. 대안의 제시와 권고

이상의 개인정보보호법제에 관한 사전입법평가, 사후입법평가, 그리고 병행입법평가에 입각해서 내려진 최종적인 결과를 수정대안의 형태로 아래 제6편에서 제시한다. 먼저 제1장에서는 입법체계에 대한 대안과 권고사항을 제시하고, 제2장에서는 개인정보처리의 입법기준에 대한 대안과 권고사항을, 마지막으로 제3장에서는 집행체계에 대한 대안과 권고사항을 제시한다.

제 3 절 입법평가의 방법론

개인정보보호법제에 대한 입법평가를 위하여 본 연구는 다음과 같은 여러 분석방법을 동원하였다.

1. 실증적·경험론적 분석

개인정보의 이용과 보호를 어떻게 규율할 것인가는 개인정보처리(=수집·이용·제공)의 효용성과 위험성을 어떻게 평가하느냐에 달려

있는 문제이다. 이러한 평가작업의 기초자료로 활용하기 위해서 일반인 1,000명과 전문가 41명을 대상으로 설문조사를 실시하였다.

일반인 조사는 여론조사기관인 한국리서치(<http://www.hrc.co.kr>)에 의뢰하여 2008년 9월 2일부터 9월 8일에 걸쳐 전국의 성인남녀 1,000명을 대상으로 이루어졌으며, 전문가 조사는 본 연구단의 연구원들이 확보하고 있는 전문가 Pool에서 개별적으로 설문조사에 응하겠다고 허락한 전문가 41명을 대상으로 같은 기간 동안에 이루어졌다. 비교를 위하여 일반인 조사나 전문가 조사나 그 조사내용은 동일하게 구성하였다.

(1) 일반인 조사

[표 1-1-2] 일반인 설문조사의 설계구성요소

조사 방법	HRC 마스터 패널을 이용한 온라인 조사					
조사 대상	전국 성인 남녀 만20세 ~ 50세					
표본 크기	1,000명					
표본 구성 ⁹⁾		20대	30대	40대	50대	계
	남성	125	145	143	96	509
	여성	117	140	138	96	491
	계	242	285	281	192	1000
표본추출방법	표본 할당 추출(Quota Sampling)					
조사 기간	2008년 9월 2일 ~ 2008년 9월 8일					
표본 오차	95% 신뢰 수준에서 $\pm 3.1\%$					

9) 표본 구성은 2007년 통계청 인구센서스 자료에 근거하여 구성하였음.

[표 1-1-3] 일반인 설문조사의 조사내용

구분	내용
개인정보보호법제 입법체계에 대한 일 반적 인식	<p>1)개인정보보호 법조항 검색 관련 -법조항 검색 여부 -검색 시 어려움 느꼈는지 여부 및 그 이유</p> <p>2)개인정보보호 개념 이해 및 인지 -인식상 개인정보보호 내용 포함되었을 것 같은 법률</p>
개인정보보호 관련 일반적 인식	<p>1)개인 정보 보호 현황에 대한 인식 -개인 정보 보호에 대한 신뢰도 -개인 정보 보호가 제대로 보호되고 있지 않다고 생각하는 이유</p> <p>2)정부/기업 개인 정보 DB 구축 및 이용에 대한 태도 -정부/기업 개인 정보 DB 구축 및 이용에 따른 위험성 및 불쾌감 -정부/기업 개인 정보 처리 관련 오/남용 가능성 -정부/기업 개인 정보 처리 관련 오/남용 시 위험성 -정부/기업의 개인 정보 수집 관련 태도</p> <p>3) 온라인상 개인 정보 보호 관련 인식 -인터넷사이트 회원 가입 시 태도 -인터넷게시판실명제 관련 인식 및 태도</p>
인구 사회학적 분석	성 연령 직업 소득 수준 지역 학력

[표 1-1-4] 일반인 설문조사 응답자 분포

Base= 전체		사례수(명)	%
전체		(1,000)	100.0
성별	남성	(509)	50.9
	여성	(491)	49.1
연령	20대	(242)	24.2
	30대	(285)	28.5
	40대	(281)	28.1
	50대	(192)	19.2
학력	고졸이하	(252)	25.2
	대졸	(634)	63.4
	대학원졸	(114)	11.4
직업	화이트	(434)	43.4
	블루	(189)	18.9
	주부	(200)	20.0
	학생	(120)	12.0
	무직/퇴직/기타	(57)	5.7
소득	상(500만원 이상)	(187)	18.7
	중(200만원-499만원 이하)	(640)	64.0
	하(199만원 이하)	(173)	17.3
지역	서울	(221)	22.1
	경기/인천	(285)	28.5
	강원	(29)	2.9
	충청	(98)	9.8
	전라	(99)	9.9
	경상	(268)	26.8

(2) 전문가 조사

[표 1-1-5] 전문가 설문조사의 설계구성요소

조사 방법	본 연구단의 전문가 Pool을 이용한 온라인 조사			
조사 대상	기업종사자, 법학교수, 법실무가			
표본 크기	41명			
표본 구성	기업종사자	법학교수	법실무가	계
	13	16	12	41
표본추출방법	표본 할당 추출(Quota Sampling)			
조사 기간	2008년 9월 2일 ~ 2008년 9월 8일			
표본 오차	95% 신뢰 수준에서 ± 3.1%			

[표 1-1-6] 전문가 설문조사 응답자 분포

Base=전체		사례수(명)	%
전체		41	100.0
성별	남성	36	87.8
	여성	5	12.2
근무기간	1년 미만	8	19.5
	1~5년 미만	20	48.8
	5~10년 미만	7	17.1
	10년 이상	6	14.6
근무직장	기업	13	31.7
	법학교수	16	39.0
	법실무	12	29.3

2. 문헌조사 및 분석

본 입법평가를 위하여 개인정보의 이용과 보호에 관련된 선행연구들에 대한 문헌조사를 실시하였다. 조사결과 국내문헌의 경우 단행본이 38권, 외국번역본 18권이었으며, 각 연구기관이나 정부기관에서 발간한 연구보고서 및 정부보고서가 32권, 그리고 논문자료가 95건에 달하였다. 또한 외국문헌으로서는 영미권의 단행본과 논문이 합쳐서 38건, 독일권이 5건, 그리고 일본 2건을 확인하였다. 이들 선행연구를 담은 문헌들의 내용을 면밀하게 분석·조사하여 그 핵심을 정리하고 본 입법평가의 논점과 관련된 내용을 추출하여 개인정보보호법제에 대한 입법평가의 소중한 참고자료로 활용하였다.

3. 규범론적 분석

본 입법평가는 난마처럼 얽혀 있는 복잡한 개인정보보호 관련 법제들을 분석하여 거기에 체계성을 부여하고, 나아가 개인정보의 이용과 보호의 합리적인 조화와 균형을 모색하고자 하는 작업이다. 때문에 본 입법평가에서는 현행의 여러 개인정보보호법들에 대한 사후입법평가를 실시하였다. 이를 위해 현행의 개인정보보호법제들이 어떤 입법연혁과 과정을 거쳐 제정되었으며, 어떤 규율내용으로 적용되고 있는지를 면밀하게 분석할 필요가 있었다. 그리하여 각 법률 상호간의 관계를 규범적인 관점에서 분석하여 정리해내고, 개인정보의 이용과 보호를 위한 법이론적 기초와 헌법이론적 토대를 분석하였으며, 개인정보처리를 규율하는 규범적 원리를 찾아내어 그것을 본 입법평가에 활용하였다. 또한 행정안전부의 입법예고안에 대한 병행입법평가에 있어서는 법안의 이해가능성을 제고하기 위하여 법적인 기본개념과 용어에 대하여 면밀한 분석을 하고, 그 수정대안들과 그 논거를 적극적으로 제시하였다.

4. 비교법적 분석

본 입법평가에서 주요 방법론으로 채택한 것은 비교법적 분석방법이었다. 이미 선진 각국에서는 일반법으로서의 개인정보보호법이 마련되어 시행되고 있기 때문에 이들의 선행 입법경험과 지식을 충분히 활용할 필요가 있다. OECD 회원국인 우리나라 입장에서 OECD 개인정보보호가이드라인을 입법의 준거로 삼을 필요가 있다. 또한 유럽연합과의 교역을 위해서는 유럽연합의 개인정보보호지침의 보호수준과 균형을 맞추어야 한다. 왜냐하면 유럽연합 개인정보보호지침 제25조는 유럽연합 회원국이 아닌 제3국으로 개인정보가 이전되기 위해서는 그 제3국이 “적당한 수준”(adequate level)의 개인정보보호를 제공하고 있을 것을 요구하고 있기 때문이다.

그리고 개인정보보호를 위한 입법모델은 크게 유럽식과 미국식으로 대별되는데 이러한 세계적인 입법모델에 비추어 우리의 개인정보보호법제의 위상을 파악하는 것은 입법평가에 있어서 매우 중요한 요소가 아닐 수 없다. 그리하여 우리보다 앞서 개인정보보호를 입법화하기 시작한 선진 각국이 개인정보의 이용과 보호의 조화라는 어려운 입법과제를 어떤 입법기준과 어떤 집행방법으로 도모하고 있는지를 이해하는 것은 어쩌면 향후의 입법과정에서 필수적이다.

이를 위하여 본 연구에서는 우선 개인정보처리의 기본원칙들을 담고 있는 국제규범으로서 1980년의 OECD 개인정보보호가이드라인, 1981년 유럽평의회(Council of Europe)의 개인정보보호협약, 1990년 국제연합(UN)의 가이드라인, 1995년 유럽연합(EU)의 개인정보보호지침의 내용을 면밀하게 분석하였다. 그리고 개별 국가의 개인정보보호법으로는 미국의 공공부문 개인정보보호법인 연방프라이버시법을 비롯한 여러 관련 법률들을 조사하였고, 유럽국가로는 주로 영국, 독일, 프랑스

의 개인정보보호법을 분석하였으며, 그리고 일본의 기본법이면서 민간부문 일반법으로 기능하고 있는 『개인정보의 보호에 관한 법률』의 입법기준과 집행체계를 자세하게 분석하였다.

특히 일본 정부는 위 개인정보보호법이 2004년에 시행되고 난 이후 그 시행의 결과를 평가하는 작업을 지속적으로 해 오고 있는데, 그러한 일본의 평가결과는 향후 우리의 입법과정에서 매우 중요한 참고자료로 활용될 수 있을 것으로 보아 별도의 장을 두어 그 경험을 정리하고 시사점을 도출하였다.

5. 비용·효과 분석

본 입법평가에서는 법경제학적 측면에서의 비용·효과 분석은 의미 있게 수행하지 못하였다. 다만, 공공기관과 기업에서 이루어지는 개인정보처리의 실태를 파악하면서, 각 부문에서 개인정보처리가 갖는 효용성과 위험성에 대한 평가를 실시하였다. 이러한 평가요소는 향후의 입법과정에서 합리적인 개인정보처리의 입법기준을 설정하는 데 의미 있는 자료로 활용될 수 있을 것으로 보인다.

또한 개인정보처리의 입법기준에 대한 병행입법평가를 하는 가운데 법경제학적 차원의 비용·효과 분석은 아니지만 행정안전부의 입법예고안의 개별적인 기준들이 사후에 적용되었을 때 어떤 사회적 파장과 효과가 나타나게 될 것인지를 예측하는 효과 분석을 미진하지만 시도해 보았다.

제 2 장 개인정보보호법의 존재이유와 특성

제 1 절 개인정보보호법 생성의 사회적 배경

1. 개인에 관한 정보의 처리를 규율하는 지금까지의 법제와 법리

타인에 관한 정보(개인정보)의 처리(=수집·가공·이용·제공)는 국가사회가 기능하기 위한 필수조건이다. 국가를 비롯한 어떤 조직이든지 그 구성원들에 관하여 신원을 확인하고 관련된 개인정보를 수집·관리하지 않으면 그 조직이 유지될 수 없다.

또한 타인과의 거래에서는 그 타인에 관한 일정한 정보가 자연스럽게 수집되고 처리된다. 그것이 정부와의 거래(세금부과, 범죄수사, 복지혜택지급 등 일체의 상호작용관계)이든 기업과의 거래(서비스이용관계 등)이든 마찬가지이다.

나아가 이러한 거래관계를 떠나서도 사회의 수많은 조직과 개인은 광범위하게 타인의 개인정보에 기초해서 그에 대한 평가를 하고 관련된 결정을 내린다.

이러한 과정에서 개인정보의 처리(=수집·가공·이용·제공)는 필수적일 뿐만 아니라 자연스러운 일이다. 이러한 개인정보의 처리과정에 세계 최초로 법적 관여가 이루어진 것은 1880년에 미국의 Thomas Cooley 판사가 민사상의 손해배상(Tort)에 관한 저서¹⁰⁾에서 “홀로 있을 권리”(the right to be let alone)라는 의미로 프라이버시권이라는 법적 개념을 제시하면서 부터이다.

그로부터 10년 후인 1890년에 Warren과 Brandeis가 이를 보다 상세히 분석한 한 논문¹¹⁾에서 ‘프라이버시권은 진보된 문명세계에서 살고

10) Thomas C. Cooley, *Laws of Torts*(1st ed. 1880), Sec. p. 29.

11) Samuel D. Warren & Louis D. Brandeis, “The Right to Privacy”, 4 Harv. L. Rev. 193,

있는 개인에게 필수적인 것'이라고 주장한 것이 프라이버시권의 역사적 유래이다. 이 프라이버시권의 주장은 당시 인쇄매체인 황색신문들(yellow journalism)의 남용에 대한 법적 대응의 한 형식이었는데, 그 사회적 배경을 보면 이러한 새로운 권리의 주장은 사생활비밀의 가치에 대한 새로운 관념이 사회적으로 형성된 결과였다.

사실 18세기까지의 삶이란 공동체적 삶이었고 따라서 공개적 삶이었기 때문에, 사생활비밀의 가치를 법적으로 보호해야 한다는 관념은 형성되지 못하였다.¹²⁾ 그러나 19세기 후반 미국에서 황색신문들이 유명인의 사생활을 들추어내어 그것을 상업적으로 악용하는 사례가 빈번해짐에 따라 이에 대한 통제장치로서 인정된 것이 프라이버시권(right to privacy)이었다.

미국에서 프라이버시 혹은 프라이버시권이라는 개념은 '타인의 방해를 받지 않고 개인의 사적 영역을 유지하고자 하는 이익 또는 권리'를 통칭하는 개념이다. 그러나 이것은 단일의 이익이 아니고 여러 차원의 이익을 나타내는 개념으로서, 사실 미국에서도 이 개념의 다의성으로 인하여 많은 학자들이 그 개념규정을 시도하여 왔으나 그러한 시도는 충분한 성공을 거두지 못하고 있는 것으로 보인다.¹³⁾ 그러나 적어도 미국의 연방대법원은 정부와의 관계 속에서 인정되는 개인의 헌법상의 프라이버시권이 두 가지 중요한 내용의 보호법익을 가지고 있는 것으로 판시하여 왔다. 그 하나가 "사적인 사항이 공개되는 것을 원치 않는 이익"(interest in avoiding disclosure of personal matters)이며, 또 다른 하나는 "자신의 중요한 문제에 대해 자율적이고 독자적

195 (1890) ; 이에 관한 상세는 서주실, "Warren · Brandeis의 『The Right to Privacy』", □□미국헌법연구□□ 제6호(미국헌법학회, 1995), 45면 이하 참조.

12) M. Ethan Katsh, *The Electronic Media and the Transformation of Law*(New York: Oxford University Press, 1989), p. 190.

13) Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*(Ithaca : Cornell University Press, 1992), p. 25.

으로 결정을 내리고자 하는 이익”(interest in independence in making certain kinds of important decisions)¹⁴⁾이 그것이다.¹⁵⁾

한편, 미국에서 개인에 관한 정보의 처리와 관련하여 사인간의 관계에서 손해배상책임을 지는 불법행위가 인정되는 프라이버시침해는 크게 4가지 유형으로 나누어진다: ① 사적 사실의 공표(public disclosure of private facts)¹⁶⁾ ② 사적 평온의 침해(intrusion upon seclusion)¹⁷⁾ ③ 사회적 인격상의 왜곡(false light)¹⁸⁾ ④ 인격적 징표의 유용(appropri-

14) *Griswold v. Connecticut*, 381 U.S. 479 (1965).

15) *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977). 미연방대법원이 인정하는 이러한 두 가지 보호법익은 우리 헌법상의 “사생활의 비밀과 자유”(제17조)에 의해 직접 보호되고 있다고 할 수 있다. 헌법학자들은 대체로 헌법 제17조를 이렇게 이해하고 있는 것으로 보인다. 예컨대, 성낙인, □□헌법학□□(법문사, 2008), 569-574면(“사생활의 평온을 침해받지 아니하고 사생활의 비밀을 함부로 공개당하지 아니할 권리”, “자유로이 사생활을 형성·영위하는 권리”); 권영성, □□헌법학원론□□(법문사, 2008), 448면(“사생활의 내용을 공개당하지 아니할 권리”, “사생활의 자유로운 형성과 전개를 방해받지 아니할 권리”); 허영, □□한국헌법론□□(박영사, 2007), 380면(“사생활의 내용과 양상이 나의 뜻에 따라 정해지고, ‘나만의 영역’이 나에게만 간직될 수 있는 것을 사생활의 자유와 비밀이라고 말한다.”) 반면에, 우리 헌법 제17조와 같은 규정을 가지고 있지 않은 독일은 기본법 제2조 제1항의 일반적 인격권의 한 내용으로서 보호되고 있다. 그런데 우리 헌법재판소는 사생활자유권을 헌법 제17조에서 근거를 찾지 않고, 독일의 예에 따라 헌법 제10조 행복추구권의 한 내용으로 이해하고 있다.

16) 사적 사실의 공표(public disclosure of private facts)가 위법한 것이 되기 위해서는 두 가지 요건이 충족되어야 하는데, 첫째, “사려분별력이 있는 사람의 입장에서 볼 때 그 공표가 수인하기 어려울 정도로 굉장히 불쾌감을 일으키는 것이어야 하고”(highly offensive to a reasonable person), 나아가 둘째, “그 공표된 사실이 일반 대중의 정당한 관심사항이 아니어야 ”(is not of legitimate concern to the public) 한다. *Restatement (Second) of Torts §652D* (1977).

17) 사적 평온의 침해(intrusion upon seclusion)가 불법행위로 인정되기 위해서는 첫째, “다른 사람이 즐기고 있는 호젓함이나 은둔을 방해하거나 그의 사적인 업무나 일애 허가 없이 개입하여야 하고”(intrudes upon the solitude or seclusion of another or his private affairs or concerns), 나아가 둘째, “그 침입이 사려분별력이 있는 사람의 입장에서 볼 때 수인하기 어려울 정도로 굉장히 불쾌감을 일으키는 것이어야”(is highly offensive to a reasonable person) 한다. *Restatement (Second) of Torts §652B* (1977).

18) 사회적 인격상의 왜곡(false light)이란 다른 사람들의 눈에 어떤 사람을 잘못 보이게 만드는 것을 가리킨다. 이것이 불법행위로 인정되기 위해서는 두 가지 요건이 모두 충족되어야 한다. 첫째, “그 사람을 다른 사람의 눈에 잘못 비치도록 만드는 사항을 공표하여야 하고”(publicly disclose a matter that places a person in a false

tion).¹⁹⁾ 그 밖에 비밀침해(breach of confidentiality)로 인한 불법행위의 성립이 인정되는데, 이는 의사·변호사 등의 전문가가 그의 환자나 의뢰인의 비밀정보(confidential information)를 제3자에게 누설했을 때 인정된다.

우리나라에서도 사생활침해에 대한 손해배상책임이 인정된다. 대법원은 “사생활의 비밀에 관한 사항을 함부로 타인에게 공개당하지 아니할 법적 이익”을 사생활권리로 인정하면서, 다만 은밀한 사생활정보를 공표한 경우라 하더라도 그 정보가 “공공의 이해와 관련되어 공중의 정당한 관심의 대상이 되는 정보”인 때에는 위법성을 인정하지 않고 있다.²⁰⁾ 이처럼 사생활에 관한 은밀한 정보를 대외적으로 ‘공표’(public disclosure)하는 행위는 사생활침해를 구성할 수 있고, 다만 그 공표의 정당한 이익이 있다고 인정될 때에는 그 위법성이 조각된다. 한편, ‘공표’가 아닌 ‘수집’(collection)의 경우에도 아주 제한적으로 사생활침해가 인정될 수 있다. 예컨대, 특정 개인을 추적·감시(tracing & surveillance)하여 그의 일거수일투족에 관한 정보를 수집한다면 그 추적·감시행위는 사생활침해(미국식으로 말하면, 사적 평온의 침해)에 해당되어 민사상의 손해배상책임을 질 수 있을 것이다.²¹⁾ 이 경우

light), 나아가 둘째, “그 공표가 사려분별력이 있는 사람의 입장에서 볼 때 수인하기 어려울 정도로 굉장히 불쾌감을 일으키는 것이어야”(is highly offensive to a reasonable person) 한다. Restatement (Second) of Torts §652E (1977).

19) 인격적 징표의 유용(appropriation)이 불법행위로 인정되기 위해서는 “다른 사람의 이름이나 얼굴을 자신의 이익을 위해서 또는 자신이 이용하기 위해서 유용하여야”(appropriates to his own use or benefit the name or likeness of the plaintiff) 한다. Restatement (Second) of Torts §652C (1977).

20) 대법원 1998. 9. 4. 선고 96다11327 판결.

21) 국군보안사 민간인사찰 사건(대법원 1998. 7. 24 선고 96다42789 판결)에서 대법원은 국군보안사령부가 군과 관련된 첩보 수집, 특정한 군사법원 관할 범죄의 수사 등 법령에 규정된 직무범위를 벗어나 민간인들을 대상으로 평소의 동향을 감시·파악할 목적으로 지속적으로 개인의 집회·결사에 관한 활동이나 사생활에 관한 정보를 미행, 망원 활용, 탐문채집 등의 방법으로 비밀리에 수집·관리한 경우, 이는 헌법에 의하여 보장된 기본권을 침해한 것으로서 불법행위를 구성한다고 판단하였다.

에 법적 규율의 초점은 수집된 개인정보의 보호에 있는 것이 아니라 수집하는 방식, 즉 부당한 추적·감시의 행태로부터 개인의 사적 평온을 보호하고자 하는 데 있다. 그 밖에, 사생활비밀을 보호하기 위한 형사법규정이 있다. 형법 제316조의 비밀침해죄와 제317조의 업무상비밀누설죄가 그것이다. 비밀침해죄는 ‘비밀장치한 문서나 전자기록을 기술적 수단을 이용하여 알아내는 행위’를 처벌하는 것이며, 업무상비밀누설죄는 ‘의사·변호사 등이 그 업무처리 중 지득한 타인의 비밀을 누설하는 행위’를 처벌한다.

이상 지금까지 미국과 우리나라의 일반 민사법과 형사법에서 개인에 관한 정보를 법적으로 규율하는 법리를 보면, 개인에 관한 정보 중에서도 보호의 필요성이 있는 “사생활정보”(private fact)나 “비밀정보”(confidential information)를 부당하게 “공표”(public disclosure)하거나 “누설”(divulge)하는 행위를 민사적 또는 형사적으로 규율하고 있음을 알 수 있다. 특히 형사적 처벌은 일반적인 사생활정보의 공표에 대해 적용되는 것이 아니라, 비밀장치로 봉합되어 있는 것을 부수고 그 안의 정보를 취득하거나(비밀침해죄) 또는 전문가와 의뢰인의 신뢰관계에 기초해서 보호되는 개인의 비밀정보를 그 신뢰관계를 깨고 제3자에게 누설하는 때에 한하여 형사처벌을 가하고 있다.

요컨대, 지금까지 개인에 관한 정보의 보호법제와 법리는 부당한 “공표”(public disclosure)나 “누설 혹은 누출”(divulge)하는 행위에 초점을 맞추어 형성되어 왔다. 일상적인 업무수행을 위하여 타인의 개인 정보를 “수집·이용·가공·제공 혹은 공유”하는 행위에 대해서는 달리 규율하지 않았다. 적어도 1970년대 초까지 그러하였다.

그러나 서독의 Hessen주가 1970년에 데이터보호법(Datenschutzgesetz)을 제정한 이래, 1973년에는 스웨덴에서 세계 최초로 국가 차원에서 개인정보보호법이 제정되었고 뒤 이어 1974년에 미국에서 공공부문 개인정보보호법인 연방프라이버시법(Privacy Act of 1974)이 제정되면

서 개인정보의 처리(=수집·이용·제공)를 새롭게 법적으로 규율하기 시작하였다. 이어서 1977년에 독일이, 1978년에는 프랑스가 프라이버시보호법을 제정하였다.²²⁾ 그리고 국제규범으로서 1980년의 OECD 가이드라인²³⁾, 1980년 유럽평의회 의 개인정보보호협약²⁴⁾, 1990년 국제연합(UN)의 가이드라인²⁵⁾, 1995년 유럽연합(EU)의 개인정보보호지침²⁶⁾ 등이 잇따라 마련되었다. 그렇다면 이렇게 개인정보의 처리(=수집·이용·제공)를 규율하는 새로운 법률인 데이터보호법 내지 개인정보보호법이 생겨나게 된 사회적 배경은 무엇인가?

2. 디지털시대의 새로운 문제 상황과 새로운 규율의 필요성

개인정보보호법의 생성배경은 전적으로 1960년대의 컴퓨터 및 디지털기술이다. 이후 촉발된 디지털혁명은 개인의 사회적 삶의 거의 모든 것을 디지털형태로 기록할 수 있게 되었다. 오늘날 모든 공·사의 기관들은 자신들의 업무수행을 위하여 개인에 대한 수많은 자료들을 디지털화된 형태로 가지고 있다. 인구학적 기본통계, 교육, 재정, 의료, 신용정보, 고용, 납세, 출입국, 치안관련자료, 사회복지, 군복무, 자

22) 이들 법률에 대한 훌륭한 분석서로는, David Flaherty, □□Protecting Privacy in Surveillance Societies□□ (1989)을 들 수 있다. 그밖에 프라이버시보호입법의 세계적 흐름과 동향에 대해서는, David Banisar/Simon Davies, “Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments”, 18 J. Marshall J. Computer & Info. L. 1 (1999) 참조.

23) 『프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인』(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).

24) 『개인정보의 자동처리와 관련한 개인의 보호를 위한 유럽이사회 협약』(Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 September 1980).

25) 『컴퓨터화된 개인정보파일의 규율을 위한 가이드라인』(Guidelines for the Regulation of Computerized Personal Data Files).

26) 『개인정보의 처리 및 자유로운 전송과 관련한 개인의 보호에 관한 지침』(Directive of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data; 95/46/EC).

동차관리, 백화점, 사회단체, 금융 등과 관련한 개인정보는 일부에 지나지 않는다. 사실 사회가 정보화된다는 것은 모든 사회활동이 디지털화된다는 것을 의미한다. 그런데 디지털화된 개인정보는 관리의 측면에서 이전과 비교할 수 없는 효율성을 가지게 된다. 발전된 DBMS(Database Management System)의 활용으로 인해 개인에 대한 정보의 입력, 처리, 검색, 출력이 신속하고 정확하게 이루어질 뿐만 아니라 더 나아가 표준식별번호(universal identification number)에 의한 컴퓨터결합(computer matching)을 통해 분산되어 있는 개인정보들을 용이하고 효율적으로 통합·처리할 수 있게 되었다. 이러한 디지털기술에 의한 개인정보의 처리는 정부와 사회에 결코 무시할 수 없는 효용을 가져다준다. 국가기능의 효율적인 수행은 국민들의 개인정보의 효과적인 처리에 달려 있다. 기업과 사회도 개인정보의 처리를 통해서 자원배분의 효율성을 극대화하게 되며, 정보기술이 개인에게 제공하는 편의와 안락 또한 개인정보의 수집과 공유를 전제로 해서 가능하게 된다.

예컨대, 사회복지행정에 있어서 복지서비스를 받는 개인에 관한 정보를 통합 관리함으로써 정부서비스의 효율성을 제고시킬 뿐만 아니라 복지사기를 방지하여 예산낭비를 줄일 수 있다. 그밖에도 개인정보의 통합관리와 공동이용은 범죄수사, 치안, 세무행정, 교육 등 각 분야에서 능률의 향상을 가져온다. 예컨대, 컴퓨터결합(computer matching)²⁷⁾이나 컴퓨터 프로파일링(computer profiling)²⁸⁾의 기법을 통해 관

27) 컴퓨터결합(computer matching)이란 2개의 다른 기록시스템 속에 동일한 기록이 있는 것을 발견하기 위하여 행하여지는 컴퓨터처리에 의한 데이터비교를 가리킨다. 이것은 통상 정부를 속이고자 하는 자를 찾아내기 위한 목적에서 행하여진다. 예컨대, 미국의 경우 무권리자가 복지혜택을 받는 것을 조사하기 위하여 복지수급자, 식량전표(food stamp)수급자, 국민의료수급자(medicaid)의 기록이 인사위원회의 기록과 결합되며, 보충적 사회보장(SSA) 수급자의 기록은 국세청(IRS)의 기록과 결합되어 있다. 그러나 통합정보관리시스템에 의하여 정보를 공동 활용하게 되면 이러한 컴퓨터연결은 보다 용이하고 간편하게 이루어질 수 있게 되고, 거의 모든 분야에서 다양한 용도로 활용될 수 있다. 박홍운, □□한국의 통합정보관리체계에서 개인정보 프라이버시 보호에 관한 연구□□(서울대 행정학 박사학위논문, 1994), 161면.

28) 컴퓨터 프로파일링(computer profiling)이란 컴퓨터에 의하여 미리 결정된 특성이

런 자료들을 분석함으로써 범죤자나 위험인물 등을 미리 분류하여 사전 예방할 수 있으며 세무관리와 소비관리 등을 통하여 탈세혐의자 등을 쉽게 포착해 낼 수 있다.

또한 개인정보 데이터베이스를 활용한 DB마케팅 활동은 기업의 주된 경쟁력의 원천으로 논의되고 있고, 실제로 고객의 개인정보를 얼마나 확보하느냐가 기업 마케팅전략의 중요 부분을 차지한다. 그리하여 통신서비스업체, 유통업체, 항공사, 금융기관 등은 고객의 평소 이용행태를 분석해 관련 데이터를 자세히 기록해두고 영업에 반영하는 지식기반영업시스템을 도입하고 있는데, 이는 기술적으로 데이터웨어하우징(DW)이라는 시스템에 의하여 운영된다.²⁹⁾ 이 시스템을 통하여 월별, 성별, 연령별 고객과 매장별, 상품별 매출추이를 분석해보면 어느 매장에서 특정한 고객이 특정한 상품을 특정한 기간에 잘 구매한다는 등의 고객성향을 알 수 있고 이를 바탕으로 여러 가지 경영전략이나 효율적인 마케팅활동을 할 수 있게 되는 것이다.³⁰⁾

최근 전자상거래의 발전으로 인해 고객의 개인정보 처리는 더욱 용이하게 되었을 뿐만 아니라 더욱 필요하고도 불가피한 것이 되어 가고 있다. 전자상거래를 통해 수집·분석된 소비자의 개인정보가 기업

나 불법행위의 모형에 특정한 개인이 얼마나 가까운지를 평가하기 위하여 여러 개의 분리된 데이터항목을 상호 연결시키는 것을 말한다. 이것은 통계적으로 비슷하게 나타난 다른 사람의 과거 행태를 기초로 특정한 개인을 판단하는 것인데, 과거의 조사에만 사용되지 않고 예방적인 차원 및 감시활동에 이용될 수 있다.

29) 데이터웨어하우징(Data Warehousing)이란 기업의 각 부문에 흩어진 시스템에서 축적된 각종 자료를 주제별로 통합해 별도의 프로그램을 사용하지 않고도 다양한 각도에서 분석할 수 있는 시스템이라고 정의된다. 예컨대, 고객정보는 여러 개의 운영시스템에 분산되어 있을 수 있는데, 이처럼 여러 곳에 흩어져 있는 고객정보를 “고객”이라는 하나의 주제로 통합하여 구축한 시스템이 데이터웨어하우징이다.

30) 예컨대, 미국의 월마트는 20-30대 기혼 남성고객이 아기 1회용 기저귀를 산 뒤 맥주를 찾는 경향이 있다는 사실을 알아내 기저귀 코너 옆에 맥주매장을 두어 맥주판매량을 한 달 만에 16%나 늘렸으며, 호주 콰타스항공은 주요 고객의 식성을 분석해 기내식 메뉴에 반영해 고정고객 확보에 한몫을 하고 있다. 또한 영국의 바클레이은행은 새로운 금융상품을 개발할 때 가장 적합한 고객을 찾아줌으로써 영업비용을 30% 이상 절약했다고 한다.

들의 마케팅에 활용될 경우, 기업과 소비자 모두에게 유익한 측면이 있기 때문이다. 특히 개인정보가 국경을 초월하여 국제적으로 수집·관리되고 분석될 경우, 국제상거래활동에 크게 기여할 뿐만 아니라 소비자들에게도 폭넓은 선택의 기회를 부여할 수 있다. 다시 말해서, 이제 기업은 극히 적은 비용과 노력으로 세계 각국의 소비자들의 소비행태를 분석할 수 있고 특정 소비자가 현재 어떤 상품에 관심을 갖고 있는지를 정확히 분석해 낼 수 있기 때문에 소비자의 니즈(needs)를 정확히 반영해서 당해 소비자를 공략할 수 있고 소비자로서도 세계 각지로부터 적기에 필요한 상품정보를 받아 볼 수 있게 되는 것이다. 결국 고객의 개인정보의 처리 및 활용은 시장에 있어서 자원배분의 효율성에 기여한다는 긍정적인 측면을 가지고 있다.

그러나 이러한 효용에 못지않게 개인정보처리의 위험성도 동시에 증가하고 있다. 디지털혁명의 기술적 가능성 속에서 이제 개인은 자신의 실존인격 외에 또 하나의 가상인격을 가지게 되는 셈이다. 그런데 기록사회의 위험성은 바로 이러한 가상인격이 실존인격을 규정짓게 된다는 사실에 있다. 다시 말해서, 개인의 사회적 정체성이 디지털화된 개인정보에 의해 좌우될 위험성이 상존하고 있는 것이다. 일례로, 잘못된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동에 미치는 위험성은 지대할 뿐만 아니라, 나아가 개인의 인격 자체에도 치명적인 위해를 가할 수 있다.

그런데 이러한 위험성은 개인정보를 수집·처리·이용하는 각 국면에 따라 다양한 형태로 표출되어 나타난다. 여기서 이 같은 위험성을 체계적으로 인식하고 또 개인정보보호를 위한 정책방안을 수립하기 위하여 다음의 몇 가지 개념을 구분하여 인식할 필요가 있다.³¹⁾

31) 조동기, “정보화사회와 프라이버시”, □□정보화시대의 미디어와 문화□□(한국언론학회·한국사회학회 엮음, 세계사, 1998), 432-436면 참조.

첫째, 개인정보의 정확성(accuracy)의 문제이다. 데이터베이스에 수록된 개인정보가 실제와 다른 경우 그러한 틀린 개인정보에 기초해서 정책결정(정부부문)이나 경영결정(시장부문)이 행하여진다면 그것이 개인의 사회생활에 미치는 파장은 대단히 심각해진다.³²⁾ 그렇기 때문에 개인정보는 정확하게 입력되어야 할뿐만 아니라 잘못된 정보에 대한 수정이 신속하게 이루어져야 하는 것이다. 또한 시간이 경과하여 이미 입력된 자료의 내용이 시의성을 가지지 못하는 경우에도 개인정보의 정확성을 해치게 된다. 그러나 문제는 개인정보의 오류를 발견하는 것이 용이하지 않고, 데이터베이스의 특성상 틀린 자료나 시의성이 없는 자료를 발견했다고 하더라도 그것을 수정하는 것이 쉽지 않다는 점이다.

둘째, 개인정보의 충실성(integrity)의 문제이다. 이는 주로 개인정보를 처리하는 과정에서 발생하는데, 예컨대 컴퓨터연결의 과정에서 적절하지 못한 방식으로 개인자료가 통합되거나 재분류되는 경우 출력된 개인정보는 정보주체를 정확하게 반영하는 충실성을 가지지 못하게 된다. 또한 처리프로그램의 내재적인 문제로 인하여 출력된 개인정보가 체계적으로 왜곡될 수도 있다. 이러한 문제는 하드웨어의 오작동이나 조작자의 실수에 의해 복합적으로 나타날 수도 있다. 이처럼 체계적으로 왜곡된 개인정보에 의하여 실존인격이 규정되는 경우 그 위험성은 더욱 커지게 된다.³³⁾

32) 개인정보의 정확성이 문제된 사례는 빈번히 일어나고 있다. 예컨대, 1996년에 발생한 고교 생활기록부 전산화자료의 입력오류사건을 들 수 있다. 당시 교육부가 입시사정자료용으로 각 대학에 제공한 고교 3학년생 생활기록부 전산화 자료에 수험생의 내신석차, 주민등록번호, 재적학생수 등 일부 내용이 잘못 입력된 것으로 밝혀졌는데, 이러한 오류가 발견된 학교는 전체 1,889개 고교 중 0.4%인 70여개 학교에 달하였다. 이러한 부정확한 개인정보에 의해 개인이 입게 되는 피해는 결코 가벼운 것이 아니다.

33) 예컨대, 미국에서는 컴퓨터연결의 결과 메사추세츠주의 복지수혜자들이 사기행위를 한 것으로 드러나 법정에서 자신들의 무죄를 위해 싸워야 하는 사태가 발생하기도 하였다. 우리나라에서도 외교통상부의 여권발급전산망과 연결된 경찰청의 신원조회전산망이 세밀하지 못한 정보를 제공하여 범죄자와 이름이나 생년월일만 같아도 부적격자로 판정되어 2만여명이 여권발급을 받지 못한 경우가 있고, 또 주민

셋째, 개인정보의 보안성(security)의 문제이다. 이는 개인정보의 관리과정에서 발생하는 문제로서 외부 또는 내부에 의한 불법적인 침입에 의해 개인정보가 누출되는 경우이다. 정보통신망의 확산으로 인해 개인정보의 데이터베이스는 다른 물리적 공간에 존재하지만 상호 연결되어 있기 때문에 외부의 침입에 취약할 수밖에 없게 되었다. 최근 해킹이나 크래킹에 의한 불법적인 침입은 보안기술의 발달에도 불구하고 줄어들지 않고 있다.³⁴⁾ 또한 보안성은 내부자에 의해 의도적으로 침해될 수 있다. 즉 개인정보 데이터베이스에 합법적으로 접근할 수 있는 사람이 개인적인 이득을 취하기 위하여 개인정보를 외부에 유출하는 경우이다.³⁵⁾

넷째, 개인정보의 적합성(adequacy)의 문제를 들 수 있다. 이것은 개인정보의 수집 및 이용과정에서 수집목적의 정당성 및 이차적 이용의 타당성에 관련된 문제이다. 개인정보 데이터베이스는 주로 특정한 목적을 위하여 구축되는데, 그렇게 구축된 개인정보가 본래의 수집목적이나 취지를 벗어나서 사용되는 경우 적합성의 위반문제가 발생한다.

등록번호의 잘못된 처리로 인하여 범죄피의자로 오인되어 수차에 걸쳐 경찰에 연행되어 조사를 받은 사례가 있다.

이러한 사례들은 개인 신상에 관한 자료의 입력과 관리가 완벽하게 이루어지더라도 자료를 처리하는 과정에서 문제가 생길 수 있음을 보여 준다. 때문에 미국에서는 정부 측의 무분별한 컴퓨터연결로부터 개인정보를 보호하기 위하여 1988년에 컴퓨터연결 행위 자체를 규율하는 내용의 □□컴퓨터연결과 프라이버시보호법□□(Computer Matching and Privacy Protection Act)을 제정·시행하고 있다.

34) 해킹(hacking)과 크래킹(cracking)은 접근이 금지된 컴퓨터시스템에 외부인이 무단으로 침입하는 행위를 가리킨다. 해킹은 초창기 해커들이 주창했던 정보공유주의와 정보평등주의라는 가치를 내세우거나 침입 그 자체에 의미를 두는 것이고, 크래킹은 개인적인 이득을 추구하거나 불순한 동기를 가지고 시스템에 침입하는 행위를 말한다.

35) 예컨대, 백화점의 고객명단이 유출되어 범행의 대상선정에 이용된 사례가 있고, 의료보험 관련 자료를 담당자가 유출하여 선거에 이용한 사례, 주민등록기록을 열람하여 가족상황을 파악한 후 독신녀의 주거지를 범죄의 대상으로 정한 사례, 자동차관리전산망을 통하여 외제 고급승용차의 차주를 확인하여 강도의 대상으로 삼은 사례 등 개인정보의 보안성이 침해되어 생겨나는 위험성은 결코 가벼이 넘길 수 없는 문제이다. 최근 들어 개인정보의 불법유출 사례가 급증하고 있는 것으로 나타났다.

이처럼 자료입력의 정확성, 자료처리의 충실성, 자료 관리의 보안성, 자료 이용의 적합성이 확보되지 않는 경우 개인정보의 왜곡이 일어나게 되고, 그에 따르는 위험성은 실존인격에 치명적인 손상을 가하게 될 것이다. 더 나아가 개인정보를 축적·처리하는 공·사의 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이 된다. 그리하여 이들 개인정보를 토대로 일정 부류의 사람들을 사회적으로 낙인을 찍는 일(예컨대, 신용불량자나 취업기피인물명단의 작성·유통)³⁶⁾이 얼마든지 가능해지게 되고, 그 결과 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다. 요컨대, 디지털기술에 따른 개인정보의 처리(=수집·이용·제공)는 효용성과 위험성이라는 두 가지 요소를 모두 가진 칼과 같다. 그러나 칼이 위험성이 있다고 해서 그 사용을 중단시킬 수는 없는 노릇이다. 방법은 오직 하나 ‘안전한 사용’을 유도하는 것이다. 오·남용의 위험성을 차단할 수 있는 안전장치를 마련해 놓고, 정당한 업무수행에 필요한 개인정보의 수집·이용·제공을 목적달성에 맞게 적정한 수준으로 허용하는 것이다. 이러한 안전장치를 법적으로 마련하고자 하는 것이 개인정보보호법이다.

제 2 절 개인정보보호법의 목적과 특성

1. 개인정보보호법의 입법목적

개인정보보호법제의 입법목적은 종래의 사생활비밀보호법제의 그것과는 다르다. 후자의 입법목적은 사생활비밀정보의 공표나 누설로부터 개인의 사적 영역을 온존하게 보존해주고자 함에 있다. 그러나 개인정보보호법제의 입법목적은 ‘개인정보의 안전한 이용’, 즉 ‘잘못된 이용’을 막고자 하는 데 있다.

36) 장영민, “정보통신망발전에 따른 개인정보보호”, □□형사정책연구소□□ 제26호 (한국형사정책연구원, 1996 여름), 9면.

독일의 공공·민간부문을 포괄하는 일반법인 연방의 개인정보보호법(Datenschutzgesetz) 제1조도 개인정보가 저장, 전달, 수정 및 처리되는 과정에서 잘못 이용되지 않도록 함으로써 보호되어야 할 다른 개인의 권리와 이익이 침해되는 것을 막기 위한 것이 이 법의 목적임을 밝히고 있다. 일본의 기본법이면서 민간부문의 일반법인 「개인정보의 보호에 관한 법률」 제1조(목적)도 “이 법률은 고도정보통신사회의 진전에 따라 개인정보의 이용이 현저하게 확대되고 있는 점에 비추어, 개인정보의 적절한 취급과 관련하여 기본이념 및 정부에 의한 기본방침의 작성 기타 개인정보의 보호에 관한 시책의 기본이 되는 사항을 정하고, 국가 및 지방자치단체의 책무 등을 명확히 함과 동시에, 개인정보를 취급하는 사업자가 준수하여야 할 의무 등을 규정함으로써 개인정보의 유용성을 배려하면서도 개인의 권리와 이익을 보호하는 것을 목적으로 한다.”고 규정하고 있다.

또한 세계 각국 개인정보보호법의 입법모델이 되고 있는 1995년의 유럽연합의 개인정보보호지침(95/46/EC)은 제1조(이 지침의 목적)에서 두 가지 입법목적(legislative objectives)을 명시하고 있다: “1. 이 지침에 따라서, 회원국들은 자연인의 기본적인 권리와 자유, 특히 개인정보의 처리와 관련한 프라이버시권(right to privacy with respect to the processing of personal data)을 보호하여야 한다. 2. 회원국들은 위 제1항에 근거해서 주어지는 보호와 관련된 이유를 들어 회원국 사이의 개인정보의 자유로운 유통(the free flow of personal data between Member States)을 제한하거나 금지해서는 아니 된다.” 이는 개인정보의 처리(=수집·이용·제공)를 금지한다는 것이 아니라, 그 처리를 허용하되 그 오·남용을 막음으로써 정보주체의 프라이버시권을 보호해야 하지만, 보호를 이유로 회원국 간의 필요한 개인정보의 유통을 막아서는 안 된다는 것이다.

사실 위 유럽연합의 개인정보보호지침이나 1980년의 OECD 개인정보보호 가이드라인은 세 가지 제정목적(legislative objectives)을 가지고 있었다. 첫째, 개인정

보의 원활한 국제적 유통을 담보하기 위한 것이다. 경제가 세계화되면서 은행이나 보험과 같은 경제의 중요한 부문에서 개인정보의 국제적 유통은 필수적이기 때문이다. 둘째, 1970년대부터 OECD 회원국들은 각각 서로 상이한 개인정보보호법을 국내법으로 제정하기 시작하였다. 이러한 국내법 상호간의 법적 편차는 개인정보의 국제적 유통에 커다란 지장을 줄 수 있었기 때문에 이들 국가 간의 법적 편차를 줄이고 개인정보처리의 기준을 통일시킬 필요가 있었던 것이다. 이 점은 유럽연합의 개인정보보호지침의 제정의도이기도 하다. 셋째, 개인정보의 처리(=수집·이용·제공)에 따르는 개인의 권리나 이익의 침해를 막기 위한 안전장치를 법적으로 확보할 필요가 있었다.

요컨대, 개인정보보호법은 개인정보의 이용 자체를 경원시하거나 불법으로 규정하고자 하는 것이 아니라 ‘안전한 이용’을 도모하고자 하는 데 그 입법목적이 있다.

2. 개인정보보호법의 성격과 특징

개인정보보호법은 비밀보호법이 아니다. 개인정보보호법에서의 “개인정보”는 비밀보호법에서의 “비밀”처럼 그 자체로 보호되어야 할 대상이 아니다. 물론 개인정보보호법에서의 개인정보 안에는 그것이 공표되거나 누설·누출되었을 경우 정보주체의 프라이버시가 침해될 수 있는 민감한 정보도 포함된다. 그러나 개인정보보호법이 기본적으로 규율하고자 하는 행위는 ‘부당한 공표·누설·누출’이 아니라, ‘정당한 업무수행 목적의 수집·이용·제공’이다. 종래의 비밀보호법에서는 이 같은 ‘정당한 업무수행 목적의 수집·이용·제공’을 원칙적으로 규율하지 않는다. 단지, 비밀로 보호되어야 하는 정보를 그 비밀장치를 깨고 취득하는 행위, 즉 비밀장치에 의해 봉합된 것을 부수고 지득하거나(형법상 비밀침해죄), 두 당사자 사이의 통신과정에 몰래 침입하

여 그 내용을 지득하거나(통신비밀보호법상의 범죄), 또는 전문가(의사·변호사 등)로서의 신뢰관계를 깨고 지득한 정보를 공표하거나 누설하는 행위를 규율할 뿐이다. 이 법에서의 규율방식은 규율행위의 ‘원칙적 금지, 예외적 허용’의 방식이다.

그러나 개인정보보호법은 이에 머무르지 않고 ‘정당한 업무수행 목적의 수집·이용·제공’에 대해서까지 규율하는 법이다. 그러나 이 법에서의 규율방식은 ‘원칙적 금지, 예외적 허용’이 아니라, ‘원칙적 허용, 예외적 제한’이다. 만일 개인정보보호법이 규율대상행위를 ‘원칙적 금지, 예외적 허용’의 방식으로 규율한다면 사회 내 개인정보의 필요한 유통은 억제되고 정부와 사회의 정상적인 기능은 거의 마비될 것이다.

요컨대, 개인정보보호법의 규율대상행위는 ‘정당한 업무수행 목적의 수집·이용·제공행위’이고, 그 규율의 방식은 ‘원칙적 허용, 예외적 제한’으로 이루어진다. 다만, 그 원칙적 허용에 대한 안전장치의 일환으로 정보주체에게 그 처리과정에 참여할 수 있는 권리를 주는 것이다. 여기서 반드시 유의할 점은 정보주체가 가지는 ‘정보처리에의 참여권’을 ‘동의권’으로 이해해서는 안 된다는 점이다. 즉, 정보주체의 동의 없는 개인정보처리를 금지하는 것으로 이해해서는 안 된다. 정보주체의 동의는 개인정보처리의 기본적 요건이 아니라 부수적 요건이며, 동의가 있으면 당연히 법적으로 허용되는 수준을 넘어선 처리(=수집·이용·제공)가 가능하게 된다. 세계 어느 나라의 개인정보보호법도 정보주체의 동의를 개인정보처리의 기본적 요건으로 설정하고 있는 경우는 없다는 점에 유의할 필요가 있다.

예컨대, 1980년의 OECD 개인정보보호가이드라인의 “개인 참여의 원칙”(Individual Participation Principle)에 의하면, (i) 정보주체는 자기에 관한 정보를 개인정보처리자가 가지고 있는지 여부를 확인할 권리(소재확인권)를 가지며, (ii) 자기에 관한 정보를 ① 합리적인 기간 내에 ② 과도하지 않은 비용으로 ③ 합리적인 방법에 의해 ④ 알기 쉬운

형태로 전달받을 권리(열람권)를 가진다. (iii) 그리고 소재확인권과 열람권이 거부되는 경우에 개인은 그 이유를 구하고(거부이유를 알 권리) 그 거부에 대하여 다툴 수 있는 권리(이의청구권)가 있으며, (iv) 그 다름에서 이기는 경우에는 해당 정보의 삭제·정정·수정·보완을 요구할 권리(처리정보변경권)를 가진다.³⁷⁾ 또한 유럽연합, 영국, 독일, 일본 등 대부분 국가의 개인정보보호법도 기본적으로 이러한 권리 규정을 두고 있다. 더 나아가, 유럽과 일본은 정보주체의 동의 없는 정보처리를 광범위하게 허용하면서도, 일정한 경우 정보처리에 대한 사후거부권(right to object)을 정보주체에게 부여하고 있다. 또한 유럽은 일정한 형태의 “자동결정에 구속되지 않을 권리”를 정보주체에게 인정하고 있다.

결국 전통적인 비밀보호법이 개인의 사적 영역을 외부의 침입이나 개입으로부터 소극적으로 보존하고자 하는 데에 초점이 맞추어져 있다면, 개인정보보호법은 개인정보의 수집·이용·제공을 원칙적으로 허용하면서 그에 따른 오·남용을 막기 위한 안전장치로서 정보주체에게 정보처리과정에 일정하게 참여할 수 있는 권리(소재확인권, 열람권, 이의청구권, 처리정보변경권, 사후거부권)를 부여하고자 하는 법이

37) PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Individual Participation Principle

13. An individual should have the right:

- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) to have communicated to him, data relating to him

within a reasonable time;

at a charge, if any, that is not excessive;

in a reasonable manner; and

in a form that is readily intelligible to him;

- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

다.³⁸⁾ 즉 종래의 사생활보호법이 “은둔으로서의 사생활보호”(privacy as seclusion)에 그 중심이 있었다면(이른바 “은둔모델”), 개인정보보호법은 “참여로서의 사생활보호”(privacy as participation)라는 접근방법을 취하고 있다(이른바 “참여모델”). 정보주체는 자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 이용되는지를 명확하게 인식하고 그러한 정보처리의 과정에 함께 참여할 수 있어야 한다는 것이다. 이러한 참여로서의 사생활보호 모델은 특히 정부 또는 사기업이 개인정보 처리의 오·남용을 통해 개인을 감시하고 통제하고자 하는 위험을 차단시키는 역감시의 기능을 수행한다.

38) 성낙인, “행정상 개인정보보호”, 『공법연구』 제22집 제3호(한국공법학회, 1994), 288면.

제 3 장 개인정보의 보호와 이용에 관한 기초이론

제 1 절 서언 : 입법평가의 필요성

산업화 이후 급격하게 진행된 기술발전이 초래한 다양한 결과들이 70년대와 80년대에 이르러 공개적으로 노출되게 되자, 이러한 사회의 행위, 특히 기술의 발전이 생태학적 또는 사회적 차원에서 중대한 결과를 가져올 수 있음이 최초로 광범위하게 인식되었고 동시에 만성적인 결과가 초래할 위험성도 인식되었다. 이를 통해 사회적 행위의 결과 및 장래세대에 대한 책임(장래세대의 보호)과 관련된 공개적인 논의가 진행되었다.³⁹⁾

이러한 상황하에서의 오늘날의 입법상황은 지속적인 변화과정상의 결과라기 보다는 사회체계 및 법체계에 있어서 다양한 발전과정이 종합적으로 반영되고 있는 상황으로 파악할 수 있다. 즉, 오늘날 법규범은 더 이상 모든 법률조문의 전체로서 이해하기 보다는 오히려 법규범은 일정한 시간적 및 사회적 맥락에 있어 “의사소통으로 생성된 현실(Kommunikativ generierte Wirklichkeit)”로 이해되고 있다.⁴⁰⁾

39) 이렇게 높아진 결과의식(Folgenbewusstsein)은 변화된 정치적 환경에도 불구하고 오늘날까지 유지되고 있으며, 또한 여러 국가들에서 기술영향평가(Technikfolgenabschätzung: TFA)를 위한 제도 이것은 정치(대개는 의회)에 있어서 결정의 기초를 제공한다는 제안하게 된 계기가 되었다고 한다. 박영도, 『입법평가의 이론과 실제』 (한국법제연구원, 2007), 24~5면.

40) 박영도, 위의 책, 15면. 이러한 법이해로부터 출발할 경우 법규범은 공식적으로 공포된 법조문과 동일시되기보다는 오히려 규범과 사회간의 상호작용의 결과인 일정한 규범적 상태를 의미한다. 오늘날에는 기존의 사회적 상태를 법규범을 통해 보호 내지 수호하는 것이 중요한 것이 아니라, 법이라는 도구를 통해 그러한 상태에 영향을 미치는 것이 중요하다는 의미에서 “법의 동태화(Dynamisierung des Recht)”가 행해지고 있다. 그와 같은 동태화는 최근에 이르러 법규범을 일종의 학습 프로그램(Lernprogramm: 사회적 학습)으로 이해하는 데까지 나아가고 있다.

한편 근대 이후 확립된 국민주권(popular sovereignty, Volkssouveränität)은 공동체의 주인은 그 공동체의 구성원이고, 공동체의 문제와 공동체의 의사는 공동체의 주인인 국민만이 최종적으로 결정하는 것으로, 비록 실제에 있어서 공동체의 의사결정은 공동체의 구성원이 스스로 정하는 경우도 있지만, 국민이 대표자를 선출하여 그로 하여금 결정하게 하고 이의 정당성을 국민에게서 구하기 때문에 주권은 공동체의 의사결정을 정당화하는 원리로 기능하기에, 결국 국민주권은 공동체의 의사결정이 종국적으로 국민에 의하여 정당화된다는 정당화원리로 기능을 한다는 주장⁴¹⁾이 제기될 만큼, 오늘날 국가권력의 정당화는 중요한 문제로 부각되고 있다.

이런 맥락에서 오늘날의 행정 체제는 점차적으로 그것이 지닌 조정 능력과 그를 통한 효과로 정당화되는 경향에 있다고 할 수 있다. 국가는 더 이상 그 자신의 행위가 정치적으로 무리한 것이거나 법적으로 제약된다는 점을 통하여 정당화되고 있으며, 따라서 국가는 사회적·경제적 문제들을 효과적으로 해결하여야 할 책무가 부여되고 있다. 이것은 특히 입법의 경우에 그러하다.

이제 입법은 보다 강력하게 정책형성을 위한 도구로서의 역할을 하게 되는 것이다. 이와 같은 효과지향적 입법은 국가 및 행정 활동에 관계된 규범은 당연히 임무 지향적으로 운영되어야 할 뿐만 아니라, 그 내용은 본질적인 것에 한정되어야 하며, 나아가 법집행과정에서 어떠한 효과를 나타내는지에 대하여도 심사되어야 한다는 것을 의미한다. 이러한 효과지향적 입법은 입법에 있어서 합법성뿐 아니라 효율성을 중요한 기준으로 설정하며, 그것이 입법의 정당성의 중요한 요건이 되고 있다.⁴²⁾

41) 정중섭, 『헌법학원론』(박영사, 2007), 116면.

42) 박영도, 앞의 책, 25~6면. 따라서 효과지향적 입법은 효과지향적 국가를 위한 일반적 요건임과 동시에 효과지향적 행정을 위한 개별적 요건으로 작용하며, “효과지

결국 법규범은 단순히 법률적인 측면뿐만 아니라, 다원주의적 사회라는 현실적 조건과 헌법적 요구 아래에서 그 이념을 여하히 실현할 것인가라는 문제에 관심을 집중하지 않을 수 없게 되었다. 따라서 사회적 법규범은 사회적 갈등을 의도적으로 규율하고 또한 예정된 규제 조치에 있어서는 규율의 목표가 달성될 수 있어야 할 뿐만 아니라, 법치국가적 요구·입법적 요구·행정적 요구·사법적 요구 및 수범자와 관련된 요구 등이 충족되어야 한다.

그리고 규율에 있어서는 실효성의 통제가 가능해야 하고, 개별적 요구와 전체적 이익과의 조정, 부분적으로 상호 모순하는 입법목표간의 충돌조정 등을 효율적·계획적으로 정립하는 노력이 필요하게 되었다. 즉, 법률의 실효성, 효율성을 심사하고 실효적이 아닌 법률은 폐쇄하며 비효율적인 법률은 효율화시키도록 개선될 여지가 인정된다. 그것이 입법평가이며, 바로 여기에 국가는 스스로 행하는 사회통제의 도구인 법률의 영향에 대한 책임을 지게 되며, 그러한 책임을 거두기 위하여 영향에 대한 예측, 평가가 한층 중요하게 되는 것이다.⁴³⁾ 이하에서는 개인정보보호법제에 관한 입법평가를 위한 사전적인 작업으로서 기본적으로 체계성 및 이해가능성 분석을 위주로 논의를 진행한다.⁴⁴⁾ 이를 위해서 우선 개인정보보호에 관련된 법학계의 기존 논의들을 간략히 검토해 보고, 논의의 사회적·이론적 배경들을 살펴본다.

향적 입법 없이는 효과지향적 행정도 없다”라고 말할 정도로 새로운 국가의 행정 모델로서 대두되고 있다. 이러한 효과지향적 입법에 대한 관념은 행정개혁 내지 국가개혁의 일환으로 등장한 이론인 신공공관리론을 입법의 분야에 적용하려는 시도라고 볼 수 있다.

43) 박영도, 앞의 책, 17면.

44) 뒤에 보다 자세히 살펴보겠지만, 법규정의 체계성(Systematik)에 관한 심사는 법규범의 내부적인 구조 및 법적인 논증(Argumentation)의 실제성을 목표로 하며, 또한 이해가능성(Verständlichkeit)의 검토는 용어의 개념적인 명확성과 언어적인 분명함을 높이기 위한 도구라 할 수 있다. 보다 자세한 내용은 박영도, 앞의 책, 107~9면.

제 2 절 선행 연구의 검토

‘정보사회’ 혹은 ‘정보화’로 지칭되는 현대사회에서의 정보의 중요성의 증가에 따르는 제반 사회변화에 대해서 법학 분야에서도 지속적인 관심을 기울여왔다. 개인정보보호법제에 대한 입법평가를 위해서 우선 기존 법학계의 연구결과들을 간략하게나마 정리해 볼 필요가 있다고 할 것인 바, 이는 우리의 입법평가 작업이 기존 연구성과의 직·간접적인 영향 하에서 진행될 가능성이 크기 때문이다. 보다 일반적으로는 모든 ‘이해(Verstehen)’의 과정이 ‘선판단성(Vor-Urteilshaftigkeit)’을 지니고 있기 때문에, 논의의 구체화 과정에서 이러한 선이해(Vorverständnis)의 내용에 대해 합리적으로 그 근거를 밝히도록 함으로써 선이해가 통제할 수 없는 오류원이 되지 않도록 하는 것이 중요하기 때문이기도 하다.⁴⁵⁾ 이러한 맥락에서 이하에서는 개인정보보호와 관련한 우리 법학계의 기존 논의들을 기든스의 ‘구조화 이론(Structuration theory)’⁴⁶⁾에 입각하여 구조 차원의 논의들과 행위자 차원의 논의들로

45) 계획열, 『헌법학(상)』 (박영사, 2005), 74면.

46) 여기에서 언급한 구조화론(structuration theory)은 행위/구조, 개인/사회의 이원론(dualism)에 대한 지속적인 비판의 형식으로 제기된 바 있는 앤서니 기든스(Anthony Giddens)의 이론이다. 일반적으로 사회적 객체(구조)의 제국주의(; 제도이론; 객관주의)와 주체(행위자)의 제국주의(; 행위이론; 주관주의)를 동시에 거부하는 것이 기든스 이론의 출발점이라면, 결정론과 자원론에 내재된 이원론에 대한 대안적 개념이 바로 구조의 이중성(duality of structure)이다. 여기서 구조의 이중성이란 사회구조가 반복적으로 조직하는 실천의 ‘매개’이자 ‘결과’임을 의미한다. 다시 말해 사회체계의 구조적 속성은 행위의 외부에 존재하는 것이 아니라 행위의 생산과 재생산에 지속적으로 연관되어 있는, 오히려 사회적 관행에 의해 실증되고 있는 내적인 것이라 볼 수 있다. 구조화란 바로 이 구조의 이중성으로 인해 시간과 공간을 가로질러 사회적 관계가 구조지어지는 것을 말한다. 기든스의 구조화이론에 대해서는 Anthony Giddens, *Central Problems in Social Theory - Action, Structure and Contradiction in Social Analysis*, 윤병철·박병래 공역, 『사회이론의 주요 쟁점』 (문예출판사, 1991[2003 print]), 74~130면; Anthony Giddens, *The Constitution of Society*, 황명주·정희태·권진현 공역, 『사회구성론』 (자작아카데미, 1998), 43~89면; Kenneth H. Tucker, *Anthony Giddens and Modern Social Theory*, 김용규·박형신 공역, 『앤서니 기든스와 현대사회이론』 (일신사, 1999) 등을 참조.

구분하여 간략하게 살펴본다. 다만, 이하의 선행연구의 검토에서 사용한 구조 차원과 행위 차원의 구분은 상당부분 논의의 전개를 위해서 다소 작위적으로 구분을 시도한 것일 뿐, 오히려 구조화 이론의 핵심이라 할 수 있는 ‘구조의 이중성’으로 대표되는 구조차원과 행위차원의 밀접한 연계성을 지적하는 것으로, 양자의 밀접한 관계에 대한 강조를 대신하고자 한다.

1. 구조 차원의 논의

정보와 관련된 사회의 변화상에 대해 쏠린 관심에 비해서 그 변화상 자체에 대한 본격적인 논의를 전개하고 있는 우리 법학계의 논의는 그다지 많지 않다는 점을 지적하지 않을 수 없다. 일반적으로는 구체적인 문제상황과 관련한 배경적인 논의로 구조차원에 대한 언급이 이루어지고 있다고 할 수 있는데, 이러한 상황에 대해서는 법학계 내부에서도 “... 초미의 관심영역에 머무르면서 과학·기술적인 측면뿐만 아니라 사회·문화적인 측면에서 수많은 논의의 대상이 되고 있는 이 정보화 또는 정보사회라는 것이 무엇을 의미하며, 어떠한 변화를 야기하고 있는가(또는 야기할 것인가)에 대한 명확한 개념정의도 없이 단순히 고도로 일반·추상화된 수준에서 예단하거나 검증되지 않은 가설로부터 일정한 전망을 추론하는 일종의 ‘속빈 강정’과 같은 논의 수준을 벗어나지 못하고 있다는 점”이 지적되고 있기도 하다.⁴⁷⁾

이러한 문제의식을 공유하고 있는 논의들로는 정보환경의 구조변화와 정보법질서의 변화에 대한 논의들이 있으며,⁴⁸⁾ 보다 구체적으로는

47) 한상희, “정보화와 헌법,” 『법학논문집』 제26집 제2호(중앙대학교 법학연구소, 2002. 11), 131면.

48) 정영화, “정보법령에 관한 법이론,” 『세계헌법연구』 제5호(2000.10); 이인호, “디지털시대의 정보법질서와 정보기본권,” 『법학논문집』 제26집 제2호(중앙대학교 법학연구소, 2002.11) 등. 이인호 교수는 “정보는 단순한 데이터나 지식이 아니라 그 자체가 곧 힘(power)인 것이다. 일정한 정보를 누가 받고 누구는 받지 못하게 조정할 수 있을 때 그의 권력은 강화되기 때문이다. ... 개인정보의 지배권을 누가 장악

전자민주주의 및 전자정부와 관련한 논의들과⁴⁹⁾ 개인정보보호제도 및 정보공개제도에 관한 연구들이⁵⁰⁾ 이러한 구조차원의 논의를 형성하고 있다고 할 수 있겠다.

2. 행위자 차원의 논의

개인정보보호와 관련한 행위자 차원의 법학계의 논의는 구조 차원의 논의에 비해 비교적 활발하게 진행되고 있다고 평가할 수 있다.

-
- 하느냐에 따라 종래의 국가권력과 시민사회의 관계는 재조정될 것이며, 동시에 시민사회 내부에서는 새로운 권력관계가 형성될 수도 있다. 이는 자유민주주의체제의 운명을 결정지을 중대한 사안이다. 자유민주체제는 한 마디로 개인의 존엄과 자유의 조건을 확보하는 체제이기 때문이다. 개인정보보호의 문제를 단순히 인격보호의 관점에서만 바라볼 수 없는 이유가 여기에 있다.”(201면)고 하면서, “자유민주주의를 지향하는 현행 헌법상의 정보법질서는 자유로운 정보유통의 이념에 입각하여 정보유통에 대한 통제권을 각기 다른 차원에서 개인에게 부여함으로써 개인의 자유와 민주주의를 확보하고자 하는 기본정책을 표방하고 있다.”(223면)고 적고 있다.
- 49) 이동훈, “전자민주주의를 구현하는 액세스권의 헌법적 함의,” 『성균관법학』 제18권 제1호(2006.6); 김종철, “전자정부와 개인정보보호의 조화,” 『세계헌법연구』 제12권 2호(2006) 등.
- 50) 박종보, “공동정보공개제도와 알 권리의 헌법적 근거,” 『공법연구』 제28집 제1호(1999); 김용섭, “정보공개와 개인정보보호의 충돌과 조화,” 『공법연구』 제29집 제3호(2001.5); 황인호, “개인정보보호제도에서의 규제에 관한 연구: 제도의 재구조화를 위한 입법론을 중심으로,” 『공법연구』 제30집 제4호(2002); 임규철, “유럽연합의 개인정보보호: 제3국으로의 개인정보전송의 경우를 중심으로,” 『아태공법연구』 제11집(2003); 정준현, “개인정보와 국가의 과제,” 『성균관법학』 제15권 2호(2003.10); 김중호, 『국가정보보호법의 필요성과 기본방향』 (경희대학교 출판국, 2004); 이창범, “정보기술 발달과 개인정보 침해에 관한 법적 고찰,” 『공법연구』 제32집 제5호(2004.6); 이강혁, “정보화사회에서의 정보접근의 자유와 개인정보의 보호,” 『외법논집』 제16집(2004.8); 문성제, “온라인상에서의 개인정보보호에 관한 국제동향: 미국의 제도를 중심으로,” 『비교법학연구』 제3집(2004.2); 이민영, 『개인정보법제론』 (진한M&B, 2005); 유일상, “정보공개법상 비공개정보의 범위에 관한 비교법적 연구: 한, 미, 영, 일을 중심으로,” 『헌법학연구』 제11집 제3호(2005.9); 김일환, “개인정보보호기구의 법적 지위와 권한에 관한 헌법적 고찰,” 『공법연구』 제33집 제3호(2005); 강경근, “정보보호의 헌법규범적 접근과 전망,” 『공법학연구』 제6권 제2호(2005); 김일환·김민호, “개인정보보호기구 법제정비의 원칙과 방향에 관한 공법체계적 고찰,” 『토지공법연구』 제36집(2007.5); 이인호, “한국 정보법의 발전동향: 정보공개법과 개인정보보호법을 중심으로,” 『공법연구』 제35집 제4호(2007.6); 백윤철, 이창범, 장교식, 『개인정보보호법』 (한국학술정보(주), 2008) 등.

구체적으로는, 정보자기결정권을 중심으로 한 연구들이 가장 활발하게 진행되고 있으며,⁵¹⁾ 개인정보와 정보 프라이버시와의 관련성에 관한 논의⁵²⁾와 함께 보다 포괄적인 범위의 정보기본권에 관한 논의들도 전개되고 있다.⁵³⁾ 이러한 논의들에 의하면 정보관련 기본권들은 '정보'의 개념이나 분류 또는 주체를 중심으로 '정보기본권'으로서 독자적이고 통합적으로 보장되어야 할 필요성이 있다면서, (개인)정보에 관한 기본권의 헌법적 근거 및 법적 성격, 효력 및 한계에 대한 포괄적인 논의가 전개되고 있다.

한편 특수영역의 개인정보 관련 연구로는 의료정보,⁵⁴⁾ 생체정보,⁵⁵⁾ 교육정보⁵⁶⁾ 등에 관한 논의들도 전개되고 있으며, 사회의 각 부분에서 일어나는 각종의 감시에 관한 논의들,⁵⁷⁾ 특히 최근에는 CCTV에

-
- 51) 김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구,” 『공법연구』 제29집 제3호(2001.5); 임규철, “정보화사회에서의 개인정보자기결정권에 대한 연구: 독일에서의 논의를 중심으로,” 『헌법학연구』 제8집 제3호(2002.10); 김승환, “정보자기결정권,” 『헌법학연구』 제9집 제3호(2003.10); 백운철, “헌법상 자기결정권과 개인정보자기결정권,” 『헌법학연구』 제9집 제3호(2003.10); 권건보, “자기정보통제에 관한 연구: 공공부문에서의 개인정보보호를 중심으로,” 서울대학교 대학원 법학박사 학위논문(2004); 권형준, “자기정보통제권에 관한 고찰,” 『헌법학연구』 제10집 제2호(2004.6) 등.
- 52) 김갑중, 『디지털시대의 정보 프라이버시』 (학영사, 2003); 김동원, “개인정보수집에서 프라이버시와 경쟁가치들의 경합과 균형,” 『정보화정책』 제10권 제4호(2003); 서계원, “정보 프라이버시와 개인정보의 보호,” 『세계헌법연구』 제11권 제1호 (2005).
- 53) 김배원, “정보기본권(상),” 『고시계』 2002년 9월호(2002.8); 김배원, “정보기본권(하),” 『고시계』 2002년 10월호(2002.9); 정영화, “생성되고 있는 정보기본권에 관한 고찰,” 『세계헌법연구』 제7호(2003.5); 이준일, “개인정보에 관한 기본권,” 『고려법학』 제41집(2003); 김배원, “정보기본권의 독자성과 타당범위에 대한 고찰: 헌법개정과 관련한 체계구성을 중심으로,” 『헌법학연구』 제12권 제4호(2006.11).
- 54) 백운철, “우리나라에서 의료정보와 개인정보보호,” 『헌법학연구』 제11집 제1호 (2005.3); 전영주, “의료정보와 개인정보보호,” 『법학연구』 제23집(2006.8).
- 55) 박영철, “생체정보의 보호,” 『헌법학연구』 제10집 제4호(2004.12).
- 56) 이른바 교육행정정보시스템(NEIS)을 둘러싼 논의가 대표적이다. 예를 들어 김일환, “교육행정정보시스템(NEIS)의 법적 정비에 관한 연구,” 『성균관법학』 제17권 제3호(2005. 12) 등.
- 57) 고영삼, “정보지배사회의 전자감시와 개인정보침해,” 부산대학교 사회학박사 학위논문, 1998.2; 이희성, “작업장내에서의 전자메일 및 CCTV의 감시와 근로자의 프라이버시보호,” 『비교사법』 (2003.3); 하경효, “새로운 근로감시기술의 도입에 따른

의한 일상적 감시와 관련한 논의들⁵⁸⁾도 진행되고 있는 바, 이러한 논의들은 전반적으로 조지오웰의 ‘빅 브라더(big brother)’나 푸코의 ‘일망감시장치(관옵티콘, panopticon)’으로 대표되는 감시의 위험성에 대한 상대적 부각과 아울러, 정보 프라이버시 등을 전제한 개인정보의 침해에 대한 방어권적 차원의 논의가 주류를 이루고 있다고 할 수 있을 것이다.

3. 평 가

선행연구의 검토 결과, 특히 개인정보보호에 관련된 논의들이 두드러짐을 확인해 볼 수 있는 바, 이러한 연구들의 전반적인 경향은 정보기술의 발전으로 대표되는 사회의 변화상에 대응하는 법체계의 수립의 중요성을 강조하고 있으며, 정보기술의 발전에 따라 더욱 높아진 개인정보의 침해 가능성 및 감시의 위험성에 대한 강조가 두드러지는 경향을 보인다고 평가할 수 있을 것이다.

그렇지만, 비록 그 결과에 있어서 다양한 스펙트럼을 보이기는 하나, 이러한 논의들이 과연 사회상의 변화 및 그에 대한 분석에 있어 균형 잡힌 시각을 유지하고 있는가에 대한 다소간의 의문을 제기할 수 있는 바, 아래의 진단은 경청할만하다. 단순히 시대가 변화하였기 때문에 그에 상응하여 법도 바뀌어야 한다고 하는 단순논리가 대부분

법적 문제,” 『노동법학』 제18호(2004.6); 권형준·허순철, “직장내 이메일(e-mail) 감청과 프라이버시,” 『헌법학연구』 제10권 제3호(2004.9); 이창범, “사업장내 전자우편 감시제도에 관한 연구,” 『노동정책연구』 제5권 제4호(2005); 김태정, “근로자 사생활의 의미와 보호범위,” 『노동법학』 제22호(2006.6); 김재중, “한국의 전자감시제도 및 그 발전방안,” 『충북대학교 법학연구』 제18권 제1호(2007); 조규범, “전자감시제도에 대한 헌법적 소고,” 『성균관법학』 제19권 제3호(2007.12); 문정민, “성범죄자 전자감시제도에 대한 고찰,” 『법학연구』 제29집(2008.2).

58) 고시면, “공공장소들에서 CCTV를 통한 감시의 위법성 여부’에 관한 독일 칼스루허 행정재판소의 판결,” 『사법행정』 (2005.2); 정태호, “CCTV 감시에 대한 개인정보 보호법의 규율에 대한 헌법적 평가,” 『헌법학연구』 제14권 제1호(2008.3) 등.

을 차지하고 있고, 그것도 주로 정보통신기술의 변화를 그대로 법의 내용으로 충당하고자 일종의 기술결정론적 사고가 정보화에 대한 법학적 분석을 지배하고 있는 것이다.

그러다 보니, 법이 사회변화를 야기하고 유도할 수도 있다는 사고, 또는 헌법 이념적 지향점을 설정하고 이에 의거하여 사회의 변화를 도모하고자 하는 헌법정책적 고려는 아쉽게도 우리 법학계에 그리 쉽게 찾아 볼 수가 없다.⁵⁹⁾

결국, 단순한 기술의 변화의 반영이 아닌 사회변화에 대한 비판적 검토를 바탕으로, 우리 헌법체계상의 이념적 지향점을 함께 고려한 정책적인 고려가 가미된 접근방법이 올바른 개인정보보호의 방향을 제시해 줄 수 있을 것이라 할 수 있을 것이다.

제 3 절 개인정보보호법제의 논의배경

본격적인 개인정보보호의 논의를 진행하기에 앞서 개인정보보호논의를 초래하게 된 사회적 배경에 대한 검토를 먼저 진행한 후, 이론적인 배경을 검토해 본다. 이는 이미 앞서서도 지적한 바 있지만, 단순한 기술결정론적 사고를 지양하기 위한 사전작업으로서의 의미를 가진다고 할 수 있을 것이다.

1. 사회적 배경

이하에서는 먼저 다수의 논의들이 논의의 출발점으로 삼는 정보사회의 실상에 대한 검토를 진행해 보고, 이어서 현대사회의 변화의 주요 동인으로 꼽히는 정보기술의 구체적인 면모를 살펴본다.

59) 한상희, “정보화와 헌법,” 『법학논문집』 제26집 제2호(중앙대학교 법학연구소, 2002. 11), 132면.

(1) 정보사회이론

‘산업사회를 거쳐 정보화사회로 이행되어 가는 오늘날의 사회구조’⁶⁰⁾ 나 ‘오늘날의 지식기반 산업화·정보화사회’⁶¹⁾ 등의 표현은 우리 판례에서도 종종 사용하는 어구로, ‘정보사회’⁶²⁾의 개념에 대한 사회적 수용의 정도를 보여주는 경우라 할 수 있을 것이다.⁶³⁾ 이미 살펴 본 법

60) 헌법재판소 2002. 8. 29. 2001헌마788, 2002헌마173(병합) [헌공 제72호]; 헌법재판소 2005. 12. 22. 2004헌마947 전원재판부 [헌공제111호]

61) 헌법재판소 2003. 9. 25. 2002헌마519 전원재판부 [헌공제85호]

62) 그 명칭과 관련하여 “‘정보(화) 사회’라는 명칭은 과거, 현재 혹은 가까운 장래의 사회형태를 특징짓는 개념으로 사용되는 바, 그 외에도 ‘탈산업화사회’, ‘정보화사회’, ‘고도 정보사회’ 등 다양한 명칭으로 불리기도 한다. 나아가서는 ‘지식산업사회’, ‘하이테크놀로지 사회’, ‘시스템 사회’ 등으로 불리기도 하지만, 그 모두가 변화의 요소에만 초점을 맞추고 있기 때문에 적절한 표현이라 할 수 없으며, ‘정보사회’ 혹은 ‘고도 정보사회’라 칭하는 것이 좋을 것 같다. 왜냐하면, 엄밀히 말해 ‘정보화사회’라는 말에는 ‘지금부터 정보화된다’, 그 때문에 정보통신 기술의 개발이 필요하다는 의미가 포함되어 있기 때문이다. 이것은 1960년대 후반부터 70년대에 걸쳐 통산성에서 사용한 말인 것 같다. 현재 상황에서 생각한다면 이와 같은 말은 이미 과거의 용어라 할 수 있다. 한편, ‘정보사회’에 관해서도 ‘이미 정보화는 상당한 정도로 진행되고 있으므로, 해야 할 일은 정보통신 인프라의 정비’라는 의미가 짙다. (중략) 고도 정보사회라 할 때는 정보통신 인프라가 완전히 정비되는 것이 필요충분조건 … 현재 상황으로는 고도 정보사회의 입구 근처에 와 있다고 볼 수 있기 때문에 오늘날의 사회 형태를 표현할 때 ‘고도 정보사회’ 혹은 ‘정보사회’라고 하는 것이 적절한 것으로 생각된다”는 주장을 기억해 둘 필요가 있는데, 이는 ‘정보사회’, ‘정보화사회’, ‘고도 정보화사회’ 등의 용어들의 구분에 시사점을 제공한다. Kazufumi Orikasa, 高度情報化社會の諸相 - 歴史・學問・人間・哲學・文化, 김재홍, 『고도 정보화사회의 여러 모습: 역사, 학문, 인간, 철학, 문화』 (커뮤니케이션북스, 2004), 24-5면.

63) 그렇지만 의외로 우리 실정법상 ‘정보사회’라는 용어는 그다지 많이 등장하지 않는다. 『전기통신기본법』 제5조에서 ‘전기통신의 원활한 발전과 정보사회의 촉진을 위한 전기통신기본계획’ 이나, 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제3조에서 이용자의 ‘건전한 정보사회 정착을 위한 노력’을 규정하고, 동법 제4조에서 정보통신부장관에게 ‘정보사회의 기반을 위한 시책’의 마련을 촉구하기 위해 사용되는 등 일종의 목적조항으로 사용되는 예가 있다. 그 외에는 『정보화촉진기본법』 제10조에 의해 기존의 ‘한국전산원’의 명칭이 ‘한국정보사회진흥원’으로 교체되면서 사용되기도 했다. 한편, ‘정보사회’ 대신 ‘정보화사회’라는 명칭이 사용된 예로는, 『국가표준기본법』 등이 있다.

학내의 논의들도 대부분 정보사회 담론을 현대사회 인식의 기본전제로 삼고 논의를 시작하고 있다고 평가해도 무방할 것이다. 그럼에도 불구하고, 정보사회가 어떤 사회인가에 대해서는 논자에 따라 다양한 답변을 제시하고 있을 뿐만 아니라, 그 개념 자체를 부정하는 입장도 없지 않아, 간단하게나마 살펴볼 필요성이 있다 하겠다.

1) 정보사회의 의의

정보사회의 의미를 파악해 보기 위해서, 정보사회에 관한 기존의 논의들을 가장 체계적으로 논의하고 있는 웹스터(Frank Webster)의 견해를 중심으로 살펴보도록 하겠다.⁶⁴⁾ 웹스터는 정보사회에 대한 다양한 정의의 시도들을 기술적 정의, 경제적 정의, 직업적 정의, 공간적 정의, 문화적 정의의 다섯 가지로 구분한 바 있다.

먼저 기술적 정의에 의한 ‘정보사회’의 개념은 가장 흔한 정의라 할 수 있다. 일반적으로 눈부신 정보기술상의 혁신을 강조하며, 그 핵심적인 개념으로는 정보처리, 저장 및 전송의 획기적인 발전으로 인하여 사회의 거의 모든 기술에 정보기술(IT)을 활용하게 되었고 컴퓨터 가격의 엄청난 하락과 처리 능력의 놀라운 향상, 그리고 그에 따른 모든 분야에서의 컴퓨터의 응용이 이루어지게 된 사회가 바로 정보사회라는 개념이다. 보다 정교화된 견해로는 통신기술과 컴퓨팅의 수렴과 중첩(imbrication)을 통해 정보의 관리 및 분배의 급격한 향상이 이루어진 사회를 지칭하기도 한다. 보통 미래주의(futurism)로 분류되는 토폴러(A. Toffler), 마틴(James Martin), 벨(Daniel Bell) 등의 논의가 이에 속한다. 이러한 입장의 문제점으로는 우선 측정의 문제 그리고 그와 관련된, ‘정보시대’에 진입하였다고 판단될 수 있는 기술발달의 정도를 결정하는 어려움이, 새로운 유형의 사회에 대한 납득할 만한 정

64) Frank Webster, *Theories of the Information Society*, 조동기 역, 『정보사회이론』(사회비평사, 1997), 28~53면.

의를 위해서 분명히 중심적인 것으로 지적되고, 아울러, 기술혁신의 속도를 어떻게 측정하는가, 한 사회가 ‘산업사회’의 종말을 고하고, ‘정보사회’로 진입하게 되는 시기가 언제인가의 문제가 제기된다.

두 번째로, 정보사회에 대한 경제적 정의는 매클럽(F. Machlup)의 지식경제학적 방법 하에서 통계적 관점에서 접근을 시도하여, 산업분류에 정보기기, 정보서비스 등의 산업군을 추가하고 이 범주들의 국민경제에서의 지위를 비교하여 ‘정보경제 시대의 출현을 측정한다. 포랫(M. Forat)의 정보산업론도 같은 맥락의 연구라 할 수 있다. 문제점으로는 통계 작성상의 관점의 개재, 집합적인 자료의 상이한 경제활동의 동질화 및 진입시기 결정의 문제가 제기된다.

세 번째로, 정보사회에 대한 직업적 정의는 직업의 변화에 초점을 두어, 정보업무와 관련된 직업이 지배적이 될 때 정보사회가 등장한다는 주장이다. 정보업무와 관련된 직업으로는 사무직원, 교사, 법률가, 그리고 연예인 등이 거론된다. 이러한 직업적 규정은 종종 경제적 접근과 결합되게 되므로, 문제점도 상당부분 공유하게 된다. 즉 모든 직업은 상당한 정도로 정보의 처리 및 인지와 관련되기 때문에, 정보관련 직업의 범주화의 문제가 발생하게 될 뿐만 아니라, 정보관련 직종간의 편차에 대해서도 고려하지 못하게 된다.

네 번째의 정보사회에 대한 공간적 정의는 지역을 연결하고 시간과 공간의 조직화에 중대한 영향을 미치고 있는 정보 통신망(network)을 강조하여, 정보의 중요성 증대, 컴퓨터와 통신기술에 의한 하부구조의 확충, 정보의 교역 증가, 국민경제와 지역경제의 통합 등을 정보사회의 지표로 거론한다. 이른바 ‘시공축약(time-space compression)’⁶⁵⁾으로 대표되는 공간적 변화가 바로 정보사회의 특징이라는 것이다. 이러한 입장 역시 통신망의 개념을 어떻게 정의하는가 하는 개념규정의 부정

65) David Harvey, *The Condition of Postmodernity - an Enquiry into the Origins of Cultural Change*(Cambridge, Mass: Blackwell, 1989), p. 284.

확함과 함께 진입시기의 결정 문제가 제기된다.

다섯 번째의 문화적 정의는 엄청나게 증가한 정보로 인해 일상생활의 양식자체가 변화해 버린 사회가 바로 정보사회라는 입장이다. 이러한 주장을 하는 논자들은 이러한 발전을 양적인 개념으로 측정하려는 시도는 거의 하지 않지만, 그 어느 때보다 더 풍부한 기호의 바다 속에 있는 우리들 삶의 ‘분명함(obviousness)’을 강조한다. 아울러, 이러한 주장은 이른바 ‘기호의 죽음’을 이야기 하는데, 지나치게 많은 정보의 존재로 인해서, 보드리아르(Jean Baudrillard)가 지적한 ‘정보가 더 많아질수록 의미는 더 적어지게 된다’는 역설을 접하게 된다고 한다.⁶⁶⁾ 이러한 견해는 우리는 더 많은 상징적 상호작용이 진행되고 있다는 점 외에는 현대사회의 특징을 파악하는 데 실패하고 있는 것으로 보인다.

결국, 정보사회에 대한 개념을 검토하면서 분명해지는 것은 그 개념들이 부정확하거나 불완전하다는 것이다. 이러한 문제를 인식하는 것은 매우 중요한 것으로 ‘정보사회’라는 개념이 현대사회의 특징을 탐구하는 데에는 ‘발견적(heuristic)’ 도구로서의 일정한 가치를 가지고는 있지만, 규정적인 개념으로 받아들여지기에는 너무 부정확하다는 점을 기억할 필요가 있다.⁶⁷⁾

2) 정보사회 이론

비록 정보사회의 개념에 대한 명확한 합의는 존재하지 않지만, 많은 논자들이 정보사회를 둘러싼 논의를 전개하고 있는 것도 엄연한 사실 이기에, 정보사회이론이라는 이론 분야에 대한 논의가 전혀 불가능한 것은 아니다. 이러한 정보사회이론의 시작을 다니엘 벨(Daniel Bell)의 후기산업사회론에서 찾는 이들이 적지 않지만, 벨의 논의에 앞서, 정

66) Frank Webster, 앞의 책, 51면.

67) Frank Webster, 앞의 책, 53면.

보사회에 관한 주장이 제기된 것은 일본의 학자들에 의해서라는 것이 보다 정확하다. 이에 관한 일본학자의 견해를 소개한다.

정보사회론은 많은 서양과학을 도입한 일본에서 처음 탄생한 개념이며, 학문이라고 알려져 있다. 이 정보사회론이 일종의 봄을 일으킨 것은 1960년대 후반의 일이다. 당시 일본의 경제가 고도성장을 맞이한 시기이며 이것이 낙관적이고 화려한 장밋빛 미래 사회론과 결합하여 정보화사회론의 전개에 박차를 가하게 되었다.

그러나 1973년 오일쇼크를 계기로 지금까지의 낙관적인 정보화사회론은 자취를 감추게 되었다. 정보화사회를 실현하기 위해서는 고도 경제 성장의 지속과 활성화가 필수 조건이었던 것이다. 이 같은 정보화사회에 관한 논의는 얼마간 모습을 감추었다가 1980년대에 들면서 다시 활성화되기 시작했다. 이전까지의 정보화사회론을 대신하여 기술적 뒷받침을 받은, 보다 고도의 정보화사회론이 논의되게 되었다. 이 단계에서 정보사회라는 개념은 미국에까지도 영향을 미쳐 나이스비트(Naisbitt, J.)의 ‘메가트렌드(Megatrend)’에서도 언급되는 바와 같이 현대사회를 분석하는 유력한 어프로치로서 주목받기에 이르렀다. 초기의 정보화사회론이 일본에서 탄생했다고는 하지만 그 뿌리를 거슬러 올라가면 미국의 현대사회론의 영향을 많이 받았다고 할 수 있다.⁶⁸⁾

이론적 수준에서의 정보사회에 관한 논의들은 다양하나, 크게 보면 두 가지로 나누어 볼 수 있다. 정보사회를 이전의 자본주의적 산업사회와는 다른 새로운 부류의 사회라는 주장과 자본주의적 산업사회의 연장선 위에서 정보사회를 파악하는 시각의 갈래가 그것이다.⁶⁹⁾

68) Kazufumi Orikasa, 앞의 책, 55~56면. 일본의 1960년대 후반의 정보화사회론은 미국의 지식사회(탈산업사회)론을 일본적으로 전개한 것이라고 할 수 있다. 그러나 중요한 것은 이 지식사회론과 일본의 정보화사회론의 다른 점은 지식사회론에서는 ‘이론적 지식’이 핵심인 반면, 정보화사회에서는 ‘정보’가 핵심이란 점이다.

69) 김원동, “정보사회에 관한 이론적 전망,” 정보사회학회 편, 『정보사회의 이해』 (나남, 1998), 66-67면.

① 정보사회론

정보사회를 자본주의적 산업사회와 구별되는 별개의 사회라고 보는 이론적 차원에는 벨을 중심으로 한 탈산업사회론(post-industrialism), 토플러(Alvin Tofler)의 제3물결 문명론(civilization of the third wave), 포스터(Mark Poster)의 포스트모더니즘(postmodernism), 피오르(Michael Piore)와 세이블(Charles Sabel)의 유연전문화론(flexible specialisation), 그리고 카스텔(Manuel Castells)의 정보적 발전양식론(informational mode of development) 등이 있다.⁷⁰⁾ 여기에 속하는 이론들은 정보사회에 대한 낙관적·비관적 전망의 정도와 연구 초점 등에 따라 좀 더 세분될 수 있음은 물론이다. 하지만 이들 이론은 기본적으로 연속성보다는 ‘변화’를 우선시하고, 변화의 결과로 나타나는 산업사회와 정보사회 간의 ‘단절성’을 강조한다는 점에서 공통점을 지닌다.

② 정보화론

이에 반해, 정보사회와 자본주의적 산업사회 간의 연속성을 강조하는 대표적인 논의로는 쉐러(Herbert Schiller)의 네오맑시즘(neo-Marxism), 아글리에타(Michael Aglietta)의 조절이론(regulation theory), 하비(David Harvey)의 유연적 축적론(flexible accumulation), 그리고 하버마스(Jürgen Habermas)의 공론장(the public sphere) 이론, 기든스(Anthony Giddens)의 근대사회관(역사사회학) 등을 들 수 있다.⁷¹⁾ 이 밖에 정보통신기술의 감시적·통제적 측면을 부각시킴으로써 정보사회의 음지를 집중 조명하고 있는 로빈스(Kebin Robins), 웹스터(Frank Webster), 갠디(Oscar H. Gandy Jr.), 라이언(David Lyon), 등의 정보사회관도 모두 연속론을 주장하는 이론들로 범주화할 수 있다.

70) Frank Webster, 앞의 책.

71) Frank Webster, 앞의 책.

③ 평 가

이처럼 간단하게나마 정보사회에 관한 다양한 논의들을 살펴보았지만, 사실 정보사회에 대한 논의에 있어서는 기존사회와의 연속성 판단여부보다는 오히려 이들 논의에서 거론되는 정보사회의 특성들이 더 많은 의미를 가진다고 할 수 있다. 기본적으로 정보사회론(단절론)이든 정보화론(연속론)이든 현대산업사회에서의 일정한 변화의 양상에 대한 인식에 있어서는 차이가 없기 때문이다. 다만 그들은 단지 현상으로서의 변화양상에 대하여 어떠한 의미를 부여하고 있는가 - 즉, 질적 변화의 모습을 찾는가, 양적 변화로 한정지우는가 - 라는 점에서 다른 평가를 하고 있을 따름이다. 결국 진정한 문제는 이들의 논의에서 지난날과 다른 오늘의 모습을 찾아 그로부터 어떠한 패러다임을 구축하고 현상을 분석, 평가할 것인가이다.⁷²⁾ 결국 현대 사회를 정보사회로 규정짓는 것만으로는 이전 사회와는 다른 사회적 상황에 대한 논의의 출발점으로 충분하다고 하기 어렵기 때문에, 그 실질적인 사회적 상황에 대한 고찰이 수반될 것이 필요하다 하겠다.

3) 정 리

‘정보시대(age of information)’와 관련된 많은 문헌들 가운데는 - 최소한 - 정보가 현대사회에서 특별한 관련성을 가지게 되었다는 점을 제외하면 정보의 주된 특성이나 의미에 대해서는 거의 의견의 일치를 찾아보기가 힘들다. 일반적인 기대와는 달리, 정보사회라는 개념을 현대사회의 분석 도구로 삼고자 하는 시도는 적어도 충분한 의사소통의 장을 열지 못하고 있다고 결론을 지어도 무방할 것이다.⁷³⁾

72) 한상희, 앞의 글, 139면.

73) 다니엘 벨의 탈산업사회론을 중심으로 정보사회이론을 철학적으로 비판하고 있는 견해로는 Mark Poster, *The Mode of Information: Poststructuralism and Social Context*, 김성기 역, 『뉴미디어의 철학』 (민음사, 1994), 48~65면.

이에 대한 대안적인 출발점에서 정보를 접근하는 방법, 즉 현대사회 이론의 목표 가운데 하나는, 흔히 정보사회이론이라 이야기되는 정보에 대한 사회적 영향 접근방법이 절망적으로 단순할 뿐만 아니라 현재 무엇이 일어나고 있고 미래에는 어떤 일들이 발생할 것인지를 이해하고자 하는 사람들을 오도하고 있음을 보여주는 것이다. 또 다른 하나의 목표는, 전문적인 사회과학자들에게는 놀라운 일이 아닐 수도 있지만, 사회이론이 경험적 증거와 결합됨으로써 훨씬 더 풍부하고 따라서 정보영역에서의 최근의 변화를 이해하고 설명하는 데도 궁극적으로 더 실제적이고 유용한 방법임을 보여주는 것이다.

하지만 실정법상 이미 수용되어 있고, 판례에서도 흔히 사용하는 ‘정보사회’ 등의 용어를 전적으로 거부하기란 쉽지 않은 일이다. 결국 ‘정보사회’ 등의 의미를 탐구하는 작업을 계속해 나가되, 현재로서는 이러한 ‘정보사회’ 등의 용어에 현대사회를 지칭하는 수사학적(rhetoric)인 의미 이상을 부여하는 것에는 신중할 필요성이 있다고 하겠다.

(2) 정보기술

모호한 정보사회에 대한 실체를 탐구하고자 하는 시도 보다는 오히려, 현대 사회의 변화의 원동력의 하나로 평가되는 정보기술의 실질적인 모습을 탐구하는 것이 연구의 방향으로서 의미를 가질 수 있다. 이하에서는 특히 입법에 있어서의 수용가능성을 전제로 하여, 정보기술의 의미와 그 핵심적인 사항들에 대하여 간단히 살펴보기로 한다.

1) 정보기술의 의의

기술(technology)이란 자연현상에 대한 과학적 지식을 응용하여 인간이 자연자원을 활용하고 물리적 환경을 관리하기 위한 수단으로 만들어낸 연모와 그 과업을 수행하는 기법과 그리고 그 결과로 창안해 낸 고안물(devices)을 가리키는 것으로, 인간이 새로 발견한 자연(또는 기

타 삶의 환경)의 이치와 그 이론에 기초하여 새로이 생각해 낸 아이디어를 실제생활에 적용하여 구체적인 물리적 소산물로 만들어내는 과정과 결과를 총칭하는 말이다.⁷⁴⁾ 이러한 맥락에서 정보기술이란 정보를 생산, 교환, 이용, 보존하는 기술을 가리킨다고 할 수 있다.

이러한 정보기술은 특히 20세기 중반, 컴퓨터 및 통신 분야의 기술 혁신이 두드러지면서 비롯된 용어이다. 그러나 엄밀히 추정하면 정보기술의 역사는 인간의 커뮤니케이션 행위가 매개체를 통해 이루어지는 시점으로부터 비롯된다. 다만 그러한 매개체 기술이 과학기술에 근거를 두고 발전된 전자 미디어와 각종 통신기술, 그리고 컴퓨터 기술의 상호융합이 급속히 확산되면서 정보기술이라는 포괄적 개념으로 통용되고 있다. 한편, 최근 들어 정보 분야의 기술이 급속히 발전되어 수없이 많은 기술적 전문용어가 범람하고 있다. 특히 통신 및 컴퓨터 분야의 파생기술이 지속적으로 등장하여 용어상의 혼란을 가중시킬 정도에 이른다. 각 전문용어에 대한 이해도 바람직하지만 무엇보다도 중요한 것은 매체마다 획기적인 계기를 맞아 창출된 기술의 의미를 습득하고 시대적 환경에 따른 신기술의 등장을 기술적 진화론에 바탕을 두고 그 사회적 의미를 깨닫는 것이 바람직하다.⁷⁵⁾

2) 정보기술의 요소

현대적 의미의 정보기술의 핵심적인 요소로는 정보의 디지털화와 이렇게 디지털화된 정보를 처리하는 컴퓨터, 그리고 컴퓨터 간의 통신을 통한 정보의 이동을 가능하게 하는 네트워크를 들 수 있다.

74) 김경동, “기술혁신과 사회변동: 정보사회의 생성전개에 대한 이해,” 정보사회학회 편, 『정보사회의 이해』(나남, 1998), 29면. ‘기술’에 대한 보다 깊이 있는 논의는 임흥빈, 『기술문명과 철학』(문예출판사, 1995[1996 print]), 54~90면; Hans Jonas, *Technik, Medizin und Ethik zur Praxis des Prinzips Verantwortung*, 이유태 역, 『기술·의학·윤리: 책임 원칙의 실현』(술, 2005), 17~40면.

75) 전석호, 『정보사회론: 커뮤니케이션 혁명과 뉴미디어』(나남, 2004), 39-40면.

① 디지털·디지털화

디지털(digital)이라는 용어는, 오늘날 매우 다양한 분야에서 사용되고 있는 용어로, 디지털 경제⁷⁶⁾· 디지털 혁명⁷⁷⁾· 디지털 미디어⁷⁸⁾· 디지털 시대⁷⁹⁾ 등 이른바 정보혁명의 핵심으로 거론되는 용어이기는 하지만, 그 의미를 분명하기 제시하기란 그다지 쉽지 않다.

사전적인 의미에 따른다면, 디지털은 ‘분명하게 구분가능한 요소들을 이용하는(방식)’이라고 정의해 볼 수 있을 것이다. 여기에서 굳이 ‘숫자’를 제시하지 않은 이유는, 현재의 디지털의 표현방식이 모두 숫자로 이루어져 있지는 않기 때문이다. 물론 디지털 방식의 가장 대표적인 방식이 숫자를 사용하는 것임은 분명하며, 그 가운데에서도 0과 1만을 사용하는 二進(binary) 체계는 오늘날의 컴퓨터 기술과 직결되는 중요한 의미를 가진다.⁸⁰⁾

결국 현재의 ‘디지털’이란 용어가 사용되는 맥락은 대부분 ‘컴퓨터 기술과 관련된’ 것이라 할 수 있을 것이다. 이러한 디지털의 의미의 확산에 기여한 네그로폰테(Nicholas Negroponte)는 디지털의 이해를 위

76) Lynn Margherio, *The Emerging Digital Economy*(Washington, D.C.: U.S. Department of Commerce, 1998); Erik Brynjolfsson and Brian Kahin, *Understanding the Digital Economy Data, Tools, and Research*(Cambridge, Mass.: MIT Press, 2000); 김범환, 『(인문사회분야 학생을 위한) 정보통신경제론: 디지털 경제론』(청목출판사, 2001); 김민정·김성숙, 『디지털 경제와 소비자』(태일사, 2005); 강대오, “디지털경제하 저작권 문제에 대한 경제적 고찰,” 『한국비블리아 발표논문집』 제5집(2001.11); 김용규, “디지털경제의 특징과 시사점,” 『한양대학교 디지털경제연구』 제6권(2001.12) 등.

77) 경상대학교 사회과학연구소 편, 『디지털 혁명과 자본주의의 전망』(한울아카데미, 2000).

78) 김기태, 『디지털 미디어 시대의 저작권』(이채, 2005).

79) Esther Dyson, *Release 2.0 : A Design for Living in the Digital Age*, 남경태 역, 『인터넷, 디지털 문명이 열린다』(경향신문사, 1997).

80) 디지털이 곧 이진체계를 의미하지 않는다는 사실은 디지털 시계와 아날로그 시계를 구분하는 것으로 쉽게 이해할 수 있을 것이다. 디지털 시계는, 아날로그 시계와는 달리, 분명히 구분되는 숫자들로 시간을 표시함으로 인해 ‘디지털’이라 불릴 뿐 이진체계를 사용하는 것이 아니다.

해서 비트(bits)와 아톰(atom)의 차이를 고려할 것을 권한다.⁸¹⁾ 네그로폰테에 따르면 우리가 ‘原子’로 기억하는 아톰(atom)은 바로 아날로그 세계의 기본단위이고, 비트는 디지털 세계의 기본단위이다. 네그로폰테는 이렇게 언급하고 있다.

비트는 색깔도, 무게도 없다. 그것은 정보의 DNA를 구성하는 가장 작은 원자적 요소이다. 비트는 켜진 상태이거나 꺼진 상태, 참이거나 거짓, 위 아니면 아래, 안 아니면 바깥, 흑이거나 백, 이들 둘 가운데 한 가지 상태로 존재한다. 이해를 하기 쉽게 우리는 비트를 1 혹은 0으로 간주한다. 1의 의미 혹은 0의 의미는 별개의 문제이다.⁸²⁾

이러한 논의를 이어 받은 강남훈은 디지털이란 “정보를 비트의 묶음으로 표현하는 것”이라 정의하며 아울러 비트는 ‘0 아니면 1의 값을 갖는 단위’를 말한다고 한다.⁸³⁾

생각건대 디지털의 개념정의를 위해서는 무엇보다도 아날로그(analog)의 개념과의 대비를 통해 살펴보는 방식을 검토해 볼만하다. 사전에 따르면 ‘어떤 수치를 길이라든가 각도 또는 전류라고 하는 연속된 물리량으로 나타내는 일’⁸⁴⁾로 정의되는 아날로그는 보통 디지털과 대비되는 개념으로 사용되기 때문에, 디지털의 개념요소로는 결국 ‘불연속성’을 강조하는 것이 의미가 있을 것이다.

컴퓨터는 바로 이러한 디지털의 개념 위에 존재한다. 일반적으로 숫자와 계산을 포함한 모든 정보들은 二進數의 형식으로 표현될 수 있고, On이나 Off로 표현될 수도 있으며, 스위치와 같은 전기부품으로도 표현될 수 있다. 다른 부품들과 스위치들을 사용하여 전기장치는 숫자나 다른 모든 형태의 정보들을 표현할 수 있다. 컴퓨터는 이렇게

81) Nicholas Negroponte, *Being Digital*, 백육인 역, 『디지털이다』 (커뮤니케이션북스, 1995[1996 print]), 13면 이하.

82) Nicholas Negroponte, 앞의 책, 15면.

83) 강남훈, 『정보혁명의 정치경제학』 (문화과학사, 2002), 30면.

84) “아날로그,” 국립국어연구원편, 『표준국어대사전』 (두산동아, 1999).

二進化된, 즉 디지털화 된 정보를 처리하게 되는 것이다. 따라서 컴퓨터는 모든 정보를 숫자의 형태로 치환하여 처리하게 되므로, 양과 관련한, 즉 크거나, 일치하거나, 작거나 외의 의미의 측면은 모두 사상한 채, 정보를 처리하게 된다. 따라서 컴퓨터가 보이는 탁월한 검색의 기능은 하드웨어와 소프트웨어의 발전으로 이러한 데이터간의 비교를 빨리 처리할 수 있음에 기인하는 것으로, 숫자적으로 일치하기만 하면, 컴퓨터는 검색의 결과를 산출해 낸다. 따라서 검색결과를 놓고 보았을 때, 전혀 의미의 맥락이 통하지 않는 정보를 산출해 낼 수도 있게 된다.

결국 디지털은 ‘유한한 자릿수의 숫자’의 체계이기 때문에, 일반적으로는 근사값을 갖는 체계라 할 수 있다.⁸⁵⁾ 그렇기 때문에 디지털 정보는 아날로그 정보에 비해서 완전성(perfection)은 다소 떨어질 수도 있기는 하지만 ‘유한한 자릿수의 숫자’로 구성되는 디지털 정보는 아날로그 정보가 가지지 못하는 강력한 장점들을 보유하고 있기도 하다. 그것은 바로 완벽한 복제·재생산(copy; reproduction)의 가능성과 완전한 전송(transmission)의 가능성이다.⁸⁶⁾ 이 두 가지가 바로 디지털이 가지는 가장 중요한 장점이라 할 것이다.⁸⁷⁾ 그 밖에도 한정된 숫

85) 간단한 예를 들어 설명해 보면, 디지털의 세계에서는 1/3의 값을 정확하게 나타낼 수 없고, 소수점 이하의 어느 곳에선가 반올림 등의 처리를 해서 처리하게 된다. 색상의 경우에도 아날로그의 세계인 자연의 세계에는 거의 무한대의 색이 존재하는데 반해서, 현재 컴퓨터의 32비트 색상모드가 ‘사람이 볼 수 있는 색’이라는 의미에서 트루컬러(true color), 혹은 풀컬러(full color)라 불리긴 하지만, 2의 24제곱인 1677만 7216가지의 ‘한정된’ 색을 구현하는 것에 불과하다. 그렇지만 디지털 정보가 언제나 불완전한 정보이기만 한 것은 아니며, 실제의 정보 자체가 한정적인 문자 등의 표시에 있어서는 완전한 정보일 수 있음을 기억할 필요가 있다.

86) 실제로는 복제 작업의 작동상의 오류나 전송상의 오류가 ‘발생할 수’도 있기 때문에, 디지털 정보가 ‘언제나’ 완벽한 복제와 전송이 이루어지는 것은 아니지만, 가능성의 차원에서는 디지털 정보는 완전한 복제와 전송의 가능성을 보유할 뿐만 아니라, 실제로도 대부분 완전한 복제와 전송이 이루어진다.

87) 강남훈 교수는 디지털의 장점으로 ① 정보의 저장크기가 줄어든다. ② 저장·전달을 위해 매체를 가리지 않는다. ③ 압축 암호화가 가능하다. ④ 컴퓨터에 의한 처리가 가능하다는 점을 들고 있다. 강남훈, 앞의 책, 32~33면

자들의 비교로 일치와 불일치를 판단할 수 있기 때문에 검색 등의 조작을 수행할 수 있다는 것도 큰 장점의 하나로 꼽을 수 있을 것이다.

② 정보처리장치: 컴퓨터

주지하듯이 현재의 정보기술의 핵심을 이루고 있는 기술은 역시 컴퓨터 기술이다. 컴퓨터는 사람의 지시를 받아 디지털 정보를 처리할 수 있는 능력을 갖춘 장치라고 할 수 있는데, 오늘날 컴퓨터와 관련된 기술은 사회 전반에 확산되어 다양하게 사용되고 있어, 컴퓨터의 개념을 파악하는 것을 쉽지 않게 만들고 있다.

컴퓨터의 개념을 보다 명확하게 파악하기 위해서는 우선 세부적인 개념을 좀 더 명확히 해둘 필요가 있겠다. ‘데이터를 계산, 보존하고 일정한 프로그램에 따라 이를 처리하는 전자기적 장치’ 류의 정의는 컴퓨터의 자료처리능력에 주안점을 둔 정의로 볼 수 있는데⁸⁸⁾ 이는 ‘컴퓨터 등 정보처리능력을 가진 장치’라는 우리 법제의 규정에도 근접해 있다. 그렇지만 이러한 정의에 의하면 컴퓨터의 개념 안에 너무 많은 전자기기들이 포섭될 우려가 있으며⁸⁹⁾ 이는 통상적인 컴퓨터와 다른 기기들간의 구분과도 일치하지 않는다. 즉 우리는 일반적으로 IC(integrated chip)가 내장되었다는 이유만으로 각종 가전기기들을 컴퓨터라 부르지는 않는다.⁹⁰⁾ 뿐만 아니라, 단순히 수학적인 계산만을 처

88) Peter Knight and James Fitzsimons, *The legal environment of computing*(Sydney Reading, Mass: Addison Wesley Pub. Co., 1990), p. 3에서도 컴퓨터를 ‘정보를 처리하는 장치(a device which processes information)’로 간략히 규정하고 있다.

89) 이론적으로 가장 넓게 컴퓨터를 정의하려면 ‘모든 스위치를 갖는 기계’는 컴퓨터라는 극단적인 형태의 의견이 가능할 수 있다. 모든 스위치는 On/Off로서 1bit의 정보를 처리할 수 있기 때문이다.

90) 주지하다시피, 현재는 상당수의 가전제품에 IC가 사용되고 있는 바, IC를 사용하게 되면, 그 전자제품의 물리적인 구조는 컴퓨터에 상당히 유사해진다. 즉 중앙처리장치에 해당하는 IC에 입/출력기구까지 갖추게 되는 것이다. 전자레인지의 예로 들면, 간단한 버튼조작(입력)으로 입력된 정보는 IC의 프로그램(소프트웨어)에 의해 적절한 시간과 온도로 바뀌어(처리) 그에 맞는 마이크로웨이브를 발생시켜(출력) 요리를 가능케 한다.

리하는 전자계산기(calculator)를 가리켜 컴퓨터라고 하지는 않는다. 뿐만 아니라, 작업선택에 따라 수학적 계산도 가능하고, 수백명의 전화번호와 주소의 입력·보존·검색도 가능하며, 달력 및 스케줄 관리, 시계, 메모기능까지 갖추고 있는 전자수첩 역시 컴퓨터라고 부르지는 않는다. 반면 전자수첩과 비슷한 크기의 ‘PDA(Personal Data(Digital) Assistant)’는 보통 컴퓨터라 부른다. 여기서 우리는 선택의 상황에 놓인다. 위의 정의를 관철함으로써 전자계산기와 워드프로세서도 컴퓨터의 개념에 포함시키거나,⁹¹⁾ 위의 기기들을 배제할 수 있는 ‘種差’를 컴퓨터의 내포에 포함시키는 것이다. 여기서는 후자의 방법으로 컴퓨터 개념의 내포를 증가시키는 쪽을 택한다.

전산학 개론서에도 일반적으로 ‘컴퓨터’는 계산할 수 있는 모든 장치를 말하므로 주판이나 계산기, 소형계산기가 모두 컴퓨터의 형태라고 할 수 있지만 ‘현대적 의미의 컴퓨터’는 데이터와 명령어를 입력하고 저장할 수 있으며 빠른 속도로 이를 처리하여 정확하게 출력을 해낼 수 있는 전자적 데이터 처리 장치라고 정의하여 이러한 것들을 제외시키고 있다. 여기에서는 ‘데이터와 명령어의 입력’이라는 종차를 첨가한 것으로 다른 것들과의 구분을 이끌어내고 있는 셈이다. 사실, 이것이 가장 일반적으로 컴퓨터와 컴퓨터가 아닌 것들을 구분하는 기준으로 생각된다. 즉 고정배선(hard wiring)되어 있어 특정한 임무만 수행하도록 만들어진 기기들과는 달리 컴퓨터는 再프로그램되어 다양한 작업을 수행할 수 있는 ‘汎用性’을 갖게 된다.

아울러 또 다른 컴퓨터의 특징으로 추가할 수 있는 것은 컴퓨터가 사용하는 데이터는 디지털화된 것이라는 것이다. 컴퓨터의 종류로 아

91) 번사이드(J.W.K. Burnside)는 컴퓨터가 여러 가지 형태를 가질 수 있다고 하면서, 자동차 점화기 같은 ‘특수한 형태의 기기들’이나 PC와 같은 형태의 일반적인 컴퓨터(generalized machine)’으로 구분하고, 일반적인 컴퓨터에 대한 논의를 진행한다. J.W.K. Burnside, “The Fundamentals of Computer Technology,” Gordon Hughes(ed.), *Essays on Computer Law*(Melbourne, Australia: Longman Professional, 1990), p. 25.

날로그 컴퓨터와 디지털 컴퓨터를 드는 견해들이 있는데, 이를 추가함으로써 현대적인 의의를 거의 지니지 못하는 아날로그 컴퓨터들을 컴퓨터 개념의 외연에서 제외시킬 수 있게 된다. 결론적으로 컴퓨터란 ‘再프로그램化에 의한 汎用性을 갖는, 디지털화된 자료를 처리하는 電子機器’로 정의할 수 있다.⁹²⁾

이러한 컴퓨터에 의해 막대한 양의 다양한 정보의 신속·정확한 처리가 가능하게 되었다는 점에서 컴퓨터는 현대 사회의 제변화에 있어서 중추적인 역할을 수행하고 있다는 사실은 재론의 여지가 없다.

③ 정보이동체제: 네트워크

네트워크(Network)의 개념은 1530년대부터 사용되어 온 개념으로 본래 ‘그물(net)’과 관련한 작업 혹은 그물 자체를 의미하는 단어였으나, 1650년대 이후 동물이나 식물의 조직을 구성하는 구조를 지칭하는데 사용되기도 하고, 1800년대에는 무형의 상호연관된 사물들의 연쇄 혹은 체제라는 의미가 추가되었으며, 1800년대 말에는 ‘사업망,’ ‘조직망,’ 1900년대에 들어서면서 ‘방송망’의 개념과 1950년대 이후 ‘통신망’의 개념이 추가되어 현재에 이르게 된 바 있다.⁹³⁾ 이러한 다양한 이력을 가지고 있는 네트워크의 개념은 결과적으로 학문분야에 따라 다양하게 사용되고 있다.⁹⁴⁾

정보기술에 있어서의 네트워크는 일반적으로 ‘데이터 통신 시스템에서 단말 장치(전화, 컴퓨터 등), 전송장치, 교환장치, 그리고 이들 사

92) 이러한 컴퓨터의 가장 중요한 속성으로는 ‘보편성(범용성; universality)’에 있고, 두 번째 속성은 ‘속도(speed),’ 세번째 속성은 ‘저장능력(storage capacity),’ 네번째 속성은 ‘신뢰성(reliability),’ 다섯번째 속성은 ‘연계성(connectivity)’을 들 수 있다. 박준식, “정보기술의 발전”, 정보사회학회 편, 『정보사회의 이해』(나남, 1998), 121~122면.

93) OECD의 ‘network’ 항목 참조.

94) 최영은 사회학, 인류학, 정치학, 수학, 생물학, 화학에서의 네트워크의 개념을 소개 하면서 다양한 네트워크의 개념정의들간의 공통점으로 네트워크란 ‘다름 아닌 구성원들간의 관계를 바탕으로 이루어지는 그 어떤 것’을 의미한다고 결론내리고 있다. 최영, 『뉴미디어시대의 네트워크 커뮤니케이션』(커뮤니케이션북스, 1998), 11면.

이를 연결하는 통신 선로로 구성된 연결망' 자체를 의미하고, 네트워킹(Networking)은 '분산된 장소에서 통신 설비를 이용하여 데이터를 처리하는 기법'으로 정의된다. 네트워크와 관련한 핵심적인 사항은 역시, 정보의 '전송'이라는 측면이다. 즉, 네트워크는 곧 정보의 이동과 관련한 개념이라 볼 수 있다.

본 연구에서는 도구와 기능 자체에 주안점을 두어, '컴퓨터 등의 정보기기 간에 정보를 교환할 수 있게 연결되어 있는 상태'를 '네트워크'로, '네트워크상의 정보의 교환활동'을 '네트워킹'으로 정의한다. 즉, '정보기기 간의' 정보교환이므로 하나의 컴퓨터 내부의 통신은 여기에 포함되지 않게 되고, 정보의 형태는 아날로그이건 디지털이건 묻지 않는다. 한편, 이러한 네트워크내의 정보교환과정을 '네트워크 커뮤니케이션(Network Communication)'으로 규정하여 새로운 유형의 커뮤니케이션으로 취급하는 견해도 있는데, 이에 따르면, 이러한 네트워크를 통한 커뮤니케이션, 즉 네트워크 커뮤니케이션을 가능하게 하는 세 가지 필수요소로 편재성, 통신기술, 그리고 지능을 들고 있다.

한편 네트워크와 관련하여 일상적으로 흔하게 사용되는 인터넷(Internet or internet), 인트라넷(Intranet) 등의 개념을 검토해 볼 필요가 있을 것이다. '인터넷'은 'TCP/IP 프로토콜(protocol)을 이용하여 이루어지는 전 세계적인 범위의 공용네트워크'를 의미하는데, 이는 네트워킹이 세계적인 범위로 이루어지는 것을 가리키는 것으로서 기본적으로는 네트워크의 범위와 관련한 명칭이라 할 수 있겠다. 한편, '인트라넷'이라는 개념 역시, 하나의 회사나 학교 등의 기관의 내부에서 이루어지는 네트워크를 가리키는 명칭으로 볼 수 있을 것이다.

네트워킹의 효용은 여러 가지로 살펴볼 수 있겠으나, 가장 기본적인 장점은 역시, 네트워크에 연결되어 있지 않은 컴퓨터의 능력이 그 컴퓨터가 갖고 있는 자원의 한계에 제한되게 되는 반면, 네트워크에 연결되어 있는 컴퓨터는 다른 컴퓨터의 자원들도 이용할 수 있게 된다

는 것으로 표현할 수 있을 것이다. 여기에서 ‘다른’ 컴퓨터의 범위는 구성되어 있는 네트워크의 종류에 따라 한 사무실 내의 컴퓨터들일 수도, 또는 지구 반대편에 있는 컴퓨터일 수도 있다. 뿐만 아니라 네트워크의 구성에 따라 그 이용의 가능성 및 범위도 달라지게 된다. 그렇지만 하나의 컴퓨터의 이용 가능한 자원이 그 컴퓨터의 제한을 벗어나게 됨으로써, 사용자는 보다 많은 결과를 얻어낼 수 있는 상황이 된다는 사실에는 변함이 없다.

이처럼 네트워크라는 개념은 정보기술이전에 이미 존재하던 개념으로 학문분야에 따라 다양하게 사용되고 있기 때문에, 우리 법제에서도 이러한 맥락에서 네트워크의 개념을 정보통신망 이외의 개념으로 사용하고 있음을 확인할 수 있다. 그렇지만, ‘통신망’ 등으로 순화가 가능한⁹⁵⁾ 외래어를 굳이 법제에 사용해야 하는가는 의문이라 할 수 있다. 아울러 ‘정보통신망’과 ‘전기통신망’ 등의 용어가 혼재되어 사용되고 있는 부분도 정리가 필요하다고 할 것인데, 개인적인 의견으로는 굳이 수식어를 붙일 필요 없이 ‘통신망’이라는 용어로 대체하는 것이 가장 간명하고, 활용폭도 넓어지는 장점이 있지 않을까 생각한다.

④ 정 리

지금까지 정보기술의 개략적인 의미와 그 구성요소라 할 수 있는 디지털 및 컴퓨터와 네트워크 등의 개념을 살펴보았다. 이들은 비교적 새롭게 등장한 개념들이고 게다가 외래어들이기 때문에 우리 법체계내에 수용하기가 그다지 수월하지 않은 것이 사실이기에, 더더욱 유의해서 접근할 필요성이 큰 개념들이라 할 것이다. 아울러, 법의 해

95) 국립국어원은 네트워크(network)의 개념으로 ① 『언』 라디오나 텔레비전의 방송에서, 각 방송국을 연결하여 동시에 같은 프로그램을 방송하는 체제 ② 『컴』 랜(LAN)이나 모뎀 따위의 통신 설비를 갖춘 컴퓨터를 이용하여 서로 연결시켜 주는 조직이나 체계로 풀이하면서 전자는 ‘방송망,’ ‘방송 체계,’ ‘통신망’으로, 후자는 ‘통신망’으로 순화할 것을 권하고 있다.

석에 있어서도 논의의 맥락을 잘 살펴 최선의 해석을 얻을 수 있도록 노력해야 할 것이다.

3) 정보기술의 특징

정보기술은 정보의 전송기능을 통해 직접적인 커뮤니케이션의 수단으로 사용될 수 있을 뿐만 아니라, 정보의 처리 및 저장을 통하여 기존의 ‘기록매체’가 수행한 기능을 보다 효율적으로 수행해낼 수 있게 해준다. 일반적으로 커뮤니케이션을 위한 정보의 처리와 관련한 전산 정보기술의 사용은 이렇게 기본적으로는 對人的 기술로서의 성격을 갖게 되지만, 정보의 ‘상품화’의 진전으로 인해 ‘정보상품’을 생산하는 측면에서는 자원 및 생산기술로서 사용됨으로써 대물적 기술로서의 성격도 가지게 된다. 뿐만 아니라 정보기술은 정보상품 이외의 상품 생산에도 생산기술로 투입되어 생산성 향상에 기여할 수도 있다.

이러한 기본적인 성격을 가지는 정보기술은 그 구성요소인 디지털 및 컴퓨터와 네트워크의 특징을 고스란히 보유하게 된다. 즉 디지털의 장점인 완전한 복제가능성과 전송가능성 및 압축·암호화 처리의 가능성을 보유하여 정보의 처리 자체의 신뢰성과 효율성을 증대시킬 수 있으며, 컴퓨터의 장점인 ‘汎用性’에 기반하여 다양한 분야(실질적으로는 거의 모든 분야)에 이용될 수 있게 되며 컴퓨터 기술의 눈부신 발전에 힘입어 뛰어난 저장 및 처리능력을 발휘할 수 있으며, 네트워크의 장점인 연결성(connectability)에 의해서, 분산 및 원격처리가 가능하게 될 뿐만 아니라, 그 광대역화에 따른 전송능력의 확대에 의한 대용량의 자료전송 역시 가능해지고 있다.

이러한 일반적인 특징을 가지는 정보기술은 다른 기술들에 비해서 문제의 해결에 있어서 다양한 해법이 존재할 수 있다는 특성을 가지고, 기술 간의 격차가 상대적으로 크다는 것과 함께 네트워크 효과

(network effect)⁹⁶⁾의 존재로 인해 통신망 건설 등의 사회간접자본의 투자가 크게 요구되는 특성이 있다.⁹⁷⁾

4) 정보기술의 발전

일반적으로 기술의 혁신은 발명과 발견으로 이루어진다. 발명(invention)은 이미 존재하는 요소(elements)와 소재(materials)를 조합하여 새로운 것을 창출하는 혁신의 과정으로서 여기에는 물질적인 것도 있고 사회문화적인 발명도 있다. 한편, 발견(discovery)은 기존의 현실 또는 실재(reality)를 새로운 관점에서 바라보게 되는 혁신의 형태다. 대체로 기술혁신(technological innovation)은 새로운 과학적 이론의 ‘발견’에 힘입어 새로운 연모와 과업수행 방법을 고안해 내는 ‘발명’으로 이루어진다.⁹⁸⁾

96) 네트워크 효과(network effects)는 네트워크 외부성(network externalities)이라고도 불리며 특정 상품에 대한 어떤 사람의 수요가 다른 사람들의 수요에 의해 영향을 받을 때 네트워크 효과가 존재한다고 하는데, 그 상품을 쓰는 사람들이 일종의 네트워크를 형성해 다른 사람의 수요에 영향을 준다는 뜻에서 이런 이름이 붙었다고 한다. 이준구, 『미시경제학』(법문사, 2002), 147면. 한편 전력, 통신, 가스, 상하수도 와 철도 등의 산업은 방대한 규모의 네트워크를 토대로 활동이 펼쳐진다는 점에서 공통적인데, 이들 산업을 총칭하여 네트워크 산업(Network Industries)라고 부르기도 한다. 이승훈, “네트워크 산업의 경쟁정책,” 권오승 편, 『공정거래와 법치』(법문사, 2004), 785면.

97) 마누엘 카스텔(Manuel Castells)은 ‘정보기술 패러다임’의 특징으로 정보가 하나의 원료(raw material) 또는 소재가 되고, 새로운 기술의 영향력이 편재(pervasiveness)하며 네트워크의 논리(networking logic)가 적용되며, 패러다임의 유연성 또는 유통성(flexibility)이 존재하고, 마지막으로 통합성을 보인다는 것을 들고 있다. Manuel Castells, *The Rise of the Network Society*(2nd ed.), 김목한·박행웅·오은주 공역, 『네트워크 사회의 도래』(한울아카데미, 2003 [2005 print]), 106~115면.

98) 김경동, “기술혁신과 사회변동: 정보사회의 생성전개에 대한 이해,” 정보사회학회 편, 『정보사회의 이해』(나남, 1998), 29면. 이러한 기술혁신이 사회변동에 어떻게 작용하는가에 대해서 간단히 살펴보면, 첫째, 기술혁신은 현존하는 기술 자체를 대체하고 변형시켜서 새로운 기술을 창출하는 효과가 있다. 이른바 기술변동의 자가 추진력(self-propelling power)의 반영이라 할 수 있다. 둘째, 기술혁신이 사회변동에 가장 직접적으로 작동하는 영역은 역시 인간의 생산활동 혹은 경제부문이다. 셋째, 생산활동의 변화를 가져오는 기술변동은 일과 직업에도 영향을 미친다. 예를 들면 일의 종류의 다양화, 노동과정의 변질, 직무성격 변화 등을 들 수 있다. 넷째, 산업

정보를 생산, 교환, 이용, 보존하는 기술로서의 정보기술은 컴퓨터의 출현이전에도 분명히 존재하고 있었음에는 異論이 없다. 즉 정보기술의 역사는 인간의 커뮤니케이션 행위가 매개체를 통해 이루어지는 시점으로부터 비롯된다. 그러한 시점은 손짓이나 음향, 좀 더 발전한 형태로는 그림 등을 통한 커뮤니케이션이 이루어지던 선사시대 이전까지 소급하게 될 것이지만, 일반적으로는 역사시대 이후, 즉 언어의 발전 및 문자의 발명이 이루어진 뒤부터 본격적으로 정보기술의 발전이 진행되었다고 볼 수 있을 것이다.⁹⁹⁾

이 시기의 정보기술의 발전에 있어서 가장 획기적인 사건은 역시 인쇄기술의 발명이라 할 수 있다. 과거에는 筆寫에 의해 행해지던 복제를 신속하고 다량으로 가능하게 해 준 인쇄기술은 특히 15세기의 금속인쇄술의 발명으로 획기적인 발전을 가져왔다.¹⁰⁰⁾

구조와 직업활동이 달라짐으로써 인구의 성장과 구성 및 생태적 분포에 변화가 오고 인간의 사회생활의 공간적 조직인 지역공동체의 모습이 달라진다. 다섯째, 기술 변동은 인간의 조직생활의 유형과 특성을 변질시킨다. 여섯째, 사회의 여러 제도들도 변화하고 일곱째, 사회계급구조에도 영향을 미치며, 여덟째, 사회적 상호작용과 사회관계의 성격에도 영향을 주고, 아홉째, 사람들의 인지구조, 상징체계, 세계관, 이데올로기 등이 변화하게 되며, 열번째, 결국 기술은 인간의 가치관과 사회적 가치지향에도 영향을 미친다. 같은 책, 33-35면.

99) 단어문자의 최초의 형태인 상형문자의 출현시기는 기원전 3100년경의 메소포타미아의 수메르문자(Sumerian writing), 기원전 3000년경의 이집트의 신성문자(hieroglyphic writing)의 시기까지 소급되며, 음절문자의 경우는 기원전 2세기 후반(셈족의 서셈족음절문자[West Semitic syllabary]), 음소문자는 기원전 850~800년(그리스의 字母들)까지 소급된다고 한다. “문자,” 한국정신문화연구원 편, 『한국민족문화대백과사전』(한국정신문화연구원, 1991). 한편 언어의 기원에 관한 연구는 16세기에 크게 유행했었다고 하는데 그 결과물 중의 하나는 Jean Jacques Rousseau, *Essai sur l'origine des langues:ou il est parlé de la mélodie et de l'imitation musicale*, 주경복·고봉만 공역, 『언어 기원에 관한 시론』(책세상, 2002). 루소는 당시 가장 일반화되어 있던 神授說을 배제하고 발명과 진화에 초점을 맞추고 있다.

100) 맥루언(Marshall McLuhan)은 알파벳 활자와 인쇄술에 의해 발전된 인간들의 선형적 사고구조가 서구문명의 본질적인 개인주의, 표준화, 획일화, 계량화, 과학주의를 낳았다고 진단하면서, 기존이 시대적 환경을 금속인쇄술을 개발한 구텐베르크(Johannes Gutenberg)의 이름을 따서 ‘구텐베르크 은하계(Gutenberg galaxy)’로 지칭한다. Marshall McLuhan, *The Gutenberg Galaxy: the making of typographic man*, 임상원 역, 『구텐베르크 은하계: 활자 인간의 형성』(커뮤니케이션북스, 2001). 본 장의

이 후의 정보기술상의 획기적인 변화로 꼽히는 것은 對人커뮤니케이션의 획기적인 전환을 가져온 전신(1839년)·전화(1876년)의 발명과 함께, 이른 바 매스미디어(Mass Media)로 불리는 대중매체들의 출현으로 대중신문¹⁰¹⁾, 영화(1895년), 방송(TV는 1939년, 라디오는 1910년) 등의 출현 등을 들 수 있으며, 이들은 시간과 공간에 대한 새로운 차원을 열어 주었으며, 大衆이 사회의 중심적인 존재로 부상시키는 결과를 가져왔다.

이러한 정보기술은 컴퓨터의 출현 이후 새로운 국면을 맞게 되었다고 평가할 수 있을 것이다.¹⁰²⁾ 컴퓨터의 탄생은 어떤 의미에서는 여러 세기 동안의 기술혁신의 절정이라고 할 수 있고, 또 어떤 의미에서는 제2차 세계 대전에서의 기술적인 필요의 결과라고 할 수 있다.¹⁰³⁾

제명은 이러한 맥투언의 논의에서 빌어 온 것이다. 아울러 이러한 발전은 특히 지적재산권법제의 발전에 커다란 영향을 미쳤는데, 인쇄술이 발명되기 이전에는 하나의 저작물을 다량으로 제작하기가 곤란하여 저작물의 복제는 극히 제한적이어서, 그 저작물의 이용이 저작자의 경제적 이익을 크게 침해하지는 않았다. 물론 모작이나, 표절은 여론에 의한 호된 비난이 가해지기는 했으나, 지적재산권법제에 의한 규제는 없었고, 다만 유체재산법(민법)에 의해 지적인 창작품들이 간접적으로 보호될 뿐이었다. 하지만 활판인쇄술을 발명되면서 서적 제작비용이 감소하였고 책의 보급 확대되면서 인쇄부수가 증가하게 되고, 추가제작도 가능해지면서 민법 등에 의한 간접적인 보호만으로는 충분한 보호가 불가능해지는 상황이 도래하게 된 것이다. 송영식·이상정, 『저작권법개설(제3판)』(세창출판사, 2003), 11~12면.

101) 신문의 기원을 무엇으로 인정하는가는 논란이 없지 않다. 신문의 원시적인 형태는 로마시대의 악타 세나투스(Acta Senatus)와 악타 디우르나 포풀리 로마니(Acta Diurna Populi Romani)에 까지 거슬러 올라가기 때문이다. 일반적으로 세계 최초의 일간신문은 독일의 라이프치히에서 1660년에 창간된 ‘라이프치거 자이퉁 Leipziger Zeitung’으로 알려져 있다. 그 뒤 구미를 비롯한 세계 각국에서 질적·양적인 면에서 비약적으로 변모, 발전하여 오늘에 이르고 있다. 최정호·강현두·오택섭, 『매스 미디어와 사회』(나남출판, 1995), 218면.

102) 카스텔(Manuel Castells)은 이러한 국면을 ‘인터넷 은하계(Internet Galaxy)’로 명명한다. Manuel Castells, *The Internet Galaxy: Reflection on the Internet, Business, and Society*, 박행웅 역, 『인터넷 갤러리: 인터넷, 비즈니스, 사회적 성찰』(한울, 2004).

103) Nathan Weinberg, *Computers in Information Society*, 통신개발연구원, 『정보사회와 컴퓨터』(통신개발연구원, 1992), 33면. 컴퓨터 개발과 관련한 역사적인 내용은 이 책의 2장 ‘컴퓨터 略史’의 내용을 참고.

컴퓨터의 발전과 관련된 정보기술의 발전은 특히 20세기 후반 비약적인 발전을 보였는데, 이 시기의 하드웨어적 측면의 정보기술 발전은 크게 극소 전자공학(microelectronics), 컴퓨터(computer), 그리고 정보통신(telecommunication)이라는 세 분야에서 집중적으로 발전되어 온 것을 알 수 있다.¹⁰⁴⁾

(3) 정 리

이미 살펴 본 바와 같이 정보기술은 커뮤니케이션의 수단으로서 기본적으로는 對人的 기술로서의 성격을 갖게 되지만, ‘정보상품’의 생산 측면에서는 자원 및 생산기술로서 대물적 기술로서의 성격도 가지게 될 뿐만 아니라 정보기술은 정보상품 이외의 상품 생산에도 생산기술로 투입되어 생산성 향상에 기여할 수도 있다.

이러한 기본적인 성격을 가지는 정보기술은 그 구성요소인 디지털 및 컴퓨터와 네트워크의 특징을 고스란히 보유하여, 즉 디지털의 장점인 완전한 복제가능성과 전송가능성 및 압축·암호화 처리의 가능성을 보유하여 정보의 처리 자체의 신뢰성과 효율성을 증대시킬 수 있으며, 컴퓨터의 장점인 ‘汎用性’에 기반하여 다양한 분야(실질적으로는 거의 모든 분야)에 이용될 수 있게 되며 컴퓨터 기술의 눈부신 발전에 힘입어 뛰어난 저장 및 처리능력을 발휘할 수 있으며, 네트워크의 장점인 연결성(connectability)에 의해서, 분산 및 원격처리가 가능하게 될 뿐만 아니라, 그 광대역화에 따른 전송능력의 확대에 의한 대용량의 자료전송 역시 가능해지고 있다.

이러한 현대 정보기술의 특징이 오늘날의 각종 사회현상과 관련하여 다양한 긍정적·부정적인 결과를 초래하는 원인으로 거론될 수 있는 바, 정보기술에 대한 정확한 이해가 사회현상에 관련한 논의의 출

104) 보다 자세한 내용은 박준식, “정보기술의 발전”, 정보사회학회 편, 『정보사회의 이해』 (나남, 1998), 109-111면을 참고.

발점이 될 수 있음을 인식할 필요가 있다고 하겠다.

2. 이론적 배경

원래 입법이란 종래에는 일반적·추상적인 법규범으로 정의된 것으로부터도 추론할 수 있는 것처럼 사회의 모든 자 또는 대상에 적용될 수 있는 법규범으로서 파악되고 있으므로, 입법시에는 입법자는 사회사상을 파악하고 있을 필요가 있고 그러한 사회사상에는 다양한 이익이 내재되고 있다. 그렇다면 사회의 이익조정이야말로 입법작용의 본질의 하나로 인정된다면 그러한 이익조정 of 성부가 입법작용의 귀추를 결정하는 것으로서 파악된다.

그러한 사회의 이익조정이라는 작업은 현실로 입안하는 정책, 법률의 영향을 예측하고 그것을 감안하면서 입법자가 입법을 하는 것을 지칭한다. 즉 그러한 영향을 명확히 한 위에 비로소 입법자, 법률의 수범인 등 법률과 관련한 이해관계자는 스스로의 이익을 입법에 반영시키는 단서를 파악할 수 있으며 이익조정이 가능하게 된다.¹⁰⁵⁾ 이러한 맥락에서 개인정보보호논의의 배경이 되는 사회이론에 대한 고찰의 필요성이 인정된다.

그렇지만 모든 사회이론에 대한 고찰을 수행하기란 현실적으로 곤란한 문제이기 때문에, 법의 실효성의 관점을 중시하는 법사회학, 비용과 효용의 관점을 중시하는 법경제학의 기법을 입법에 포섭하여 입법행위의 실시, 효과에 관한 과학적 분석을 행하는 입법평가제도의 특성을¹⁰⁶⁾ 고려하여, 논의의 범위를 법학과 사회학, 그리고 법경제학

105) 박영도, 앞의 책, 31면.

106) 박영도, 앞의 책. 입법평가는 입법에 대한 비평과는 다르며 단순한 통계와도 다르다. 또한 판결에 대한 효과를 연구의 대상으로 할 수도 있으나 입법평가는 그 대상을 입법에 한정한다는 점에 특징이 있다. 또한 입법평가는 시간의 차원을 내포하는 것으로서, 과거와 미래를 동시에 직시한다. 특히, 오늘날 다원적인 사회질서, 점

상의 논의들로 한정하고자 한다.

(1) 법학적 접근

법학 내에서의 개인정보에 관한 기존의 논의들은 기본적으로 기존의 프라이버시(privacy) 논의의 맥락에서 진행되어 온 바, 이러한 논의들은 개인정보의 보호를 인격권의 범주 하에서 프라이버시 보호론의 일환으로 진행해 온 전통적인 입장과, 재산권적인 차원에서 개념화하는 최근의 입장으로 구분해 볼 수 있다. 이하에서는 프라이버시의 개념 및 형성과정과 그 본질과 관련된 논의를 간단히 정리한다.

1) 프라이버시 개관

우리나라 헌법 제17조는 “사생활의 비밀과 자유”로 프라이버시권을 보호하고 있으나 이렇게 명문으로 헌법에 규정한 나라는 아주 드물다고 할 수 있다. 사실 프라이버시 연구의 선진국인 미국에서조차도 프라이버시라는 말은 사람을 오도하는 수사에 불과하고 “프라이버시 권리”에 관한 관례라고 하는 것도 정작 알고 보면 각각 별개의 이익에 관한 관결일 뿐이며 법적 권리로서의 “프라이버시의 권리” 주장은 무익할 뿐 아니라 오히려 유해하기조차 하다는 논의가 끊이지 않는다. 우리나라 헌법은 규정을 두고 있으나 우리나라의 헌법학자들은 비록 규정이 없다고 하더라도 현대헌법이 보장하는 인간의 존엄과 가치, 행복추구권의 한 내용으로 프라이버시권이 당연히 보장되어 있다

증하는 문제의 복잡성 및 탈산업화적 사회로 이행하는 발전경향을 배경으로 할 때 입법은 사회적 과정, 즉 극히 다양한 기관들과 정치적 세력들이 공식적 또는 비공식적 권한을 통해 참여하는 권력분립적 절차로 이해되고 있다. 따라서 입법평가는 다차원적으로 행해진다. 입법평가는 법률에 대한 사전적 평가와 사후적 평가를 지속적으로 교환함으로써, 또한 시간의 흐름에 따른 지속적인 모니터링을 수행함으로써 오류의 반복을 피하고 법률의 질적 개선을 도모하는 것을 가능하게 하는 경험과 지식이 축적되리라는 기대가 깔려 있다.

고 주장한다.

① 프라이버시권의 개념

프라이버시의 개념은 개인의 공적 생활과 대조되는 것으로서 사적이면서 비밀스러운 어떤 사생활을 지칭하는 것이지만 명확히 정의되지 않은 채 일반적으로 사용되어 왔다. 우리에게 어떤 면에서 프라이버시는 개인주의가 정착된 서구적 분위기를 많이 갖고 있는 것으로 생각되기도 한다. 사회적 관계가 상대적으로 강조되어 왔던 우리 문화권에서는 중요한 것으로 간주되지 않았던 것 같다. 더구나 프라이버시라는 용어를 통해서 궁극적으로 획득하려고 하는 것이 일종의 ‘생활의 질’ 혹은 ‘안정’ 등과 같은 매우 심리적이라고 할 수 있는 것이 되고 보니, 이 용어가 담고 있는 의미를 정의하기는 더욱 어려운 것 같다.

비록 프라이버시가 시대적·사회적·문화적으로 통일된 의미를 가지고 있는 것은 아니지만 우리는 서구에서 개념화되어 왔던 내용을 살펴봄으로써 정보사회의 프라이버시권의 개념을 파악할 수 있다. 후에 좀 더 자세히 살펴보겠지만 프라이버시는 쿨리(T. M. Cooley)의 “인간의 신체에 대한 권리는 완전한 불가침의 권리, 즉 혼자 있을 수 있는 권리(the right to be let alone)이다”라는 정의가 워렌·브랜다이즈에 의해 수용된 것으로 우선적으로 개념규정해 볼 수 있을 것이다.

즉, 미국에서 프라이버시라는 개념은 ‘타인의 방해를 받지 않고 개인의 사적인 영역(personal space)을 유지하고자 하는 이익 또는 권리’를 통칭하는 개념으로서, 이것은 단일의 이익이 아니고 여러 차원의 이익을 나타내는 개념이다. 사실 미국에서도 이 개념의 다의성으로 인하여 많은 학자들이 그 개념규정을 시도하여 왔으나 아직 완전한 성공을 거두지 못하고 있는 것으로 보인다.¹⁰⁷⁾

107) Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe*

미연방대법원은 헌법상의 프라이버시권이 두 가지 중요한 내용의 보호법익을 가지고 있는 것으로 판시하고 있다. 그 하나가 “사적인 사항이 공개되는 것을 원치 않는 이익”(interest in avoiding disclosure of personal matters)이며, 또 다른 하나는 “자신의 중요한 문제에 대해 자율적이고 독자적으로 결정을 내리고자 하는 이익”(interest in independence in making certain kinds of important decisions)¹⁰⁸⁾이 그것이다.¹⁰⁹⁾

한편, 1980년대 이후 컴퓨터의 발달에 따라 개인정보가 타인에 의해 전자적 형태로 무한히 축적·처리되기 시작함에 따라 타인의 수중에 있는 개인정보에 대한 정보주체의 통제권을 나타내기 위해 “정보프라이버시”(information or informational privacy)라는 개념을 사용하기 시작하였다.¹¹⁰⁾ 이처럼 미국 내에서의 프라이버시 개념은 매우 다양한 의미를 가지고 있기 때문에, 우리나라에서 프라이버시 개념을 사용할 때 주의를 요한다. 이처럼 다양한 의미를 내포하고 있는 미국의 프라이버시권(right of privacy)이라는 용어에 대한 우리의 번역술어로는

and the United States(Ithaca: Cornell University Press, 1992), p. 25.

108) *Griswold v. Connecticut*, 381 U.S. 479 (1965).

109) *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977). 미연방대법원이 인정하는 이러한 두 가지 보호법익은 우리 헌법상의 “사생활의 비밀과 자유”(제17조)에 의해 직접 보호되고 있다고 할 수 있다. 헌법학자들은 대체로 헌법 제17조를 이렇게 이해하고 있는 것으로 보인다. 예컨대, 성낙인, 『헌법학』 (법문사, 2008), 569-574면(“사생활의 평온을 침해받지 아니하고 사생활의 비밀을 함부로 공개당하지 아니할 권리”, “자유로이 사생활을 형성·영위하는 권리”); 권영성, 『헌법학원론』 (법문사, 2008), 448면(“사생활의 내용을 공개당하지 아니할 권리”, “사생활의 자유로운 형성과 전개를 방해받지 아니할 권리”); 허영, 『한국헌법론』 (박영사, 2007), 380면(“사생활의 내용과 양상이 나의 뜻에 따라 정해지고, ‘나만의 영역’이 나에게만 간직될 수 있는 것을 사생활의 자유와 비밀이라고 말한다.”) 반면에, 우리 헌법 제17조와 같은 규정을 가지고 있지 않은 독일은 기본법 제2조 제1항의 일반적 인격권의 한 내용으로서 보호되고 있다. 그런데 우리 헌법재판소는 사생활자유권을 헌법 제17조에서 근거를 찾지 않고, 독일의 예에 따라 헌법 제10조 행복추구권의 한 내용으로 이해하고 있다.

110) 한편, 미국의 Rosenbaum은 프라이버시 개념의 이 같은 다의성을 세 가지 범주, 즉 공간적 프라이버시(Territorial Privacy), 개인적 프라이버시(Personal Privacy), 그리고 정보프라이버시(Information Privacy)로 나누어 파악하고 있다. 상세는, Joseph I. Rosenbaum, “Privacy on the Internet: Whose Information is it Anyway?”, 38 *Jurimetrics* 565(1998) pp. 566~67 참조.

“사생활권”이라는 표현이 그 다의성을 함께 나타내는 가장 적절한 것으로 판단되지만, 여기에서는 그대로 프라이버시라는 용어를 사용하기로 한다. 요컨대, 서구의 프라이버시(privacy)라는 말은 사생활적 이익을 총칭하는 개념이다. 따라서 가장 넓은 개념이다. 우리 헌법이 상정하고 있는 주거의 자유(제16조), 사생활의 비밀과 자유(제17조), 통신의 비밀(제18조)은 모두 프라이버시의 개념에 포섭된다.

② 프라이버시권의 형성

프라이버시라는 말은 생겨난 지 오래지만 이것이 권리로 인식된 것은 얼마 되지 않았다. 19세기말 미국은 급속히 도시화·산업화되어 생활환경이 급변했다. 자본주의가 그 심각한 모순을 드러내자 당황한 국가권력은 국민의 실질적 평등을 위해 그 통치영역을 확대하기 시작했고 자연히 국민 개개인의 사적 영역은 축소되어 갔다. 정부는 국민의 신상정보를 적극 수집하고 사적 영역을 침식했다. 한편 대중 저널리즘이 창궐하여 선정주의(sensationalism) 보도가 판을 쳤으며 타인의 사생활을 대중의 흥미유발과 자기의 영리를 위한 미끼로 삼아 마구잡이로 침해했다. 19세기말의 미국은 이른바 “황색 저널리즘”이 휩쓸어 기업화한 신문들은 대중의 천박한 호기심을 만족시켜 돈을 벌려고 무책임한 보도로 경쟁을 벌였다. 특히 유명인, 유력자, 연예계 인물, 화제의 인물들을 대상으로 “타당과 분별의 분명한 한계를 벗어나” 그 사생활을 탐색, 폭로함으로써 개인의 프라이버시를 심각하게 침해한 것이다. 또한 전문 조사기관이 생겨나서 민간 기업들까지도 활발한 조사활동을 벌였는데 특히 정부 측 조사기관은 정밀하고도 은밀한 수단방법을 개발하여 개인의 신상이나 사생활 정보를 수집하였다. 19세기 말에는 무정부주의, 공산주의 등 좌익사상이 침투하여 정부나 민간은 이를 조사하느라고 부득이 개인의 프라이버시를 침해했다.¹¹¹⁾

111) 이관기, 『알권리와 프라이버시 - 전통적 대립과 정보사회의 갈등』 (한국교육문화원, 1993), 62~3면.

이러한 여건 아래서 1890년 보스턴(Boston) 시내에 살고 있던 워렌(Samuel D. Warren)씨의 부인은 자기 딸의 결혼을 축하하는 축하연을 자기 저택에서 많은 인사들을 초청하여 아주 정성스럽게 열었다. 그런데 보스턴에서 발간되는 신문들 가운데 특히 『the Saturday Evening Gazette』는 그 신문의 “Blue Blood”라는 칼럼에서 그 날 축하연의 호스테스인 워렌부인에 관하여 그 연회장에서의 아주 사사롭고 당혹스럽게 만드는(highly personal and embarrassing) 처신들을 자세하게 다룬 것을 비롯하여 초청된 인사들의 명단까지 공개하였다고 한다. 이에 워렌은 그 축하연이 조용히 치러지길 바라고 있었으므로 매우 불쾌하였으며, 그의 부인도 아주 당혹스럽게 생각하며 괴로워하였다.¹¹²⁾

워렌은 그의 사회적 지위에 비추어 부인의 축하연에서의 사사로운 행적이 자세히 보도된 데 대해 매우 불쾌하게 생각하면서, 변호사 출신답게 이에 대한 법적 대응을 하려고 전년까지 같은 법률사무소의 동료였던 브랜다이즈(Louis D. Brandeis) 변호사를 찾아가 논의하였고 이 두 젊은 변호사들은 언론에 의해 개인의 사생활이 폭로되어 피해를 입은 사생활의 침해에 대한 법적 구제방법을 검토하였으나, 기존의 법리에 따르면 구제받기 어려운 피해, 즉 정신적 고통을 받는 피해에 대한 구제의 문제였다. 이에 사생활 침해에서 오는 정신적 고통에 대한 구제를 가능하도록 하기 위해 새로운 권리의 필요성을 강조하려고 두 사람이 협력하여 하나의 논문을 작성하였다.¹¹³⁾ 이 논문은 현실적으로 언론에 의해 침해된 사생활의 보호, 사생활의 침해로 인

112) Boston은 미국의 어느 도시보다 개인의 이름이나 사사로운 일들이 신문에 나기를 꺼리는 곳이었다. 그런데 신문은 결혼식과 같은 것이 있는 신나는 행사가 있는 날에는 그 문제가 의례히 크게 다루어졌다. 그러니까 Warren씨의 딸의 결혼 축하연도 당연히 크게 다루게 되었다는 것이다. Warren 부부가 당하는 곤욕(annoyance)에 대해 Prosser는 미국의 신문, 광고업자, 흥행업자들이 그 후 오늘에 이르기까지 값비싸게 지불해 온 곤욕이었다고 한다. William L. Prosser (1960), “Privacy”, *California Law Review*, 48, p. 383.

113) Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy”, 4 *Harv. L. Rev.* 193(1890).

한 정신적 고통이란 침해에 대한 구제를 위하여 기존 법리로는 해결하기 어려운 문제를 적극적으로 새로운 권리 the right to be let alone 을 이론적으로 정립하여 보호하려는 목적에서 쓰여진 점에서 특징적이라 할 수 있다.¹¹⁴⁾ 이를 위하여 워렌·브랜다이즈는 개인의 신체·재산에 대하여 충분한 보장을 한다는 것은 아주 오래된 보통법(Common Law)상의 원칙이라는 것을 대전제로 하고, 시대의 변천에 따라 정치·사회·경제의 제 영역에 있어서 여러 가지 변화가 생기므로 보통법상의 권리보장도 그 성질이나 범위 등을 필연적으로 재규정하지 않을 수 없고, 또한 거기에 상응한 새로운 권리도 인정해야 한다는 견해를 피력하면서, 프라이버시의 권리를 정립하기 위한 구체적인 논리를 전개하면서, 우선 보통법상의 명예훼손과 제정법인 저작권법상의 저작권을 검토하였다.

그들은 먼저 보통법상의 명예훼손에서 다루는 권리침해(wrongs)와 프라이버시 침해의 경우의 침해행위(injury)는 외견상 유사성이 있는 것 같으나, 실제에 있어서는 서로 다르다는 점에서 프라이버시의 보통법상에서의 독자적인 위치를 찾으려고 시도하였는바, 권리를 침해하는 수단의 성격의 측면에서 injury에 대한 법적 구제는 소송의 실질적인 원인을 제공한 ‘단적으로 손상된 감정의 치유’를 의미하는 것 반면, 명예훼손의 법리는 아주 근본적으로 성격이 다른 취지에 입각하고 있고, 그러한 권리침해는 동료 간에 그에 대한 평가가 격하되어서 그가 속한 사회 속의 외부적 관계에서 권리침해로 입은 그 명예에 대한 피해만을 다루는데 그친다는 것을 주장하여, 명예훼손에 관한 보통법상 인정되고 있는 권리침해와 명예훼손과 관련 있는 권리는 ‘그 성질상 정신적이라기보다 오히려 물질적인 것’이어서 명예훼손과 관련 있는 성격의 법리는 그 보장대상을 단지 물질적 재산의 주변에까

114) 서주실, “Warren·Brandeis의 ‘The Right to Privacy,’” 『미국헌법연구』 제6호(1995.7), 48~51면.

지 확장시킬 수 있는데 그치게 된다고 한다. 그래서 그들은 보통법에는 감정에 대한 침해행위에 대해서만 배상해 주는 법리는 전혀 인정되어 있지 않다'고 단언하고 있다. 그래서 사생활에 침해되어 아무리 정신적 고통을 받는다 하더라도 그 침해로 인한 정신적 고통은 손해배상청구가 인정되지 않는 손해에 지나지 않는다는 것이다. 한편 저작권법과 같은 제정법상의 권리는 공刊을 하지 않으면 아무런 가치가 없는 권리인 데 반하여, 보통법상의 상술한 권리는 공간해 버리면 바로 그 권리를 상실하게 된다는 점이 다르다는 점을 밝혔다.

이와 같이 워렌·브랜다이즈는 프라이버시권의 정립을 위하여 명예훼손의 법리, 저작권법상의 권리의 법리와 관련하여 검토하고서, 보통법 위에 본 양자와는 다른 영역의 보호를 인정하고 있다는 데까지 논리를 적용하고 있다. 그러면서 저작권과는 달리 아무런 경제적 이득이 없는 것마저 보통법상 보호를 하고 있다는 데까지 이론을 진전시키고 있으나, 거기에는 역시 재산권과의 관계에서 그 보호대상의 속성을 어느 정도 인정하지 않을 수 없다는 문제에 봉착하게 되어, 그들은 개인이 갖고 있는 것 비록 문학적·예술적·학술적 가치가 없는 것일지라도 의 공간 또는 공표로부터 보호해주려는 그 실체를 구명하기 위하여 영국의 판례를 검토하여, 그들은 특히 '개인의 것'을 불법적으로 공개하여 그에게 정신적 고통을 주는 침해행위와 관련된 사건들을 다루었다.¹¹⁵⁾

그리하여 워렌·브랜다이즈는 '개인의 것'의 불법적 공개에 의한 침해구제가 저작권 등의 재산권의 침해 외에 계약위반, 신탁·신뢰위반 등을 이유로 하여 금지명령이 내려졌다는 것과, 불법침해적인 공개로부터 보호하려는 것은 재산적 이익과는 전혀 관련이 없는 개인·가정

115) 서주실, 위의 글, 56~62면. 이들 사건의 판결은 대체로 기존 법에 다른 재산권의 침해, 명예훼손에 관한 법의 위반, 계약위반 또는 신조의 위반 등을 이유로 침해에 대한 구제가 주어진 사건들이었다.

생활에서 일어나는 일, 즉 사실 그 자체라는 것을 알게 되었고, 그것이 보통법상 새로이 등장시키려는 영역에 대한 기존의 보호였다고 볼 수 있다.

이와 같은 ‘자기의 것’에 대한 공개를 방지할 수 있는 권리는 우선 재산적 가치를 목적으로 하는 권리가 아니라서 점에서 그 성질상 재산권의 일종으로 보기 어렵고, 또한 이 권리로서 보호하려는 것은 지적 재산권이 아니라 가정에서 일어나는 일, 즉 사실 그 자체에 그 기초를 두고 있다는 점에서 보통법상 보호되고 있는 새로운 영역이 부각되고 있다.

그리하여 워렌·브랜다이즈는 종합적인 숙고 끝에 우선 다음과 같이 결론을 내리고 있다. 즉 명예훼손이나 저작권 또는 재산권과 구별되는 보통법상의 보호영역으로서 저작 또는 회화·조형 등을 통하여 생각·감정 그리고 정서 등에 대한 보호는, 그것의 공개방지가 문제되는 한, 개인의 혼자 있게 하는 보다 구체적인 권리(the more general right of the individual to be let alone)의 실현의 하나의 실례에 지나지 않는다는 것이다. 여기서 워렌·브랜다이즈는 쿨리(T. M. Cooley)판사가 1888년 사용한 “the right to be let alone”이라는 표현을 원용하여 보통법상 전술한 보호를 받는 권리에 대해 처음으로 사용하면서, 이 권리라는 것을 폭행 또는 구타를 당하지 않을 권리, 구금되지 않을 권리, 자의적으로 소추되지 않을 권리, 비방을 받지 않을 권리와 같은 것이라고 한다.

이들 여러 권리들은 법상 보장된 다른 권리처럼 본질적으로 소유하고 있다는 성질이 있고, 또한 그것은 재산권의 특징적인 속성이므로 역시 이들 권리도 재산권에 속한다고 말할 수 있을지 모른다. 그러나 이들 권리는 일반적으로 말하는 재산권과는 전혀 그 유사성이 없다고 그들은 분명하게 강조하고 있다. 그러면서 그들은 사적 표현물 또는 개인적 작품을 절도나 도용이 아니라 어떤 형태든 공개되는 것으로부

터 보호하려는 법리는 본질적으로 재산권의 원리가 아니라 그것은 불가침의 인격권의 원리에 입각하고 있다고 한다. 위렌·브랜다이즈는 그들이 사적 표현물을 공개로부터 보호하려는 법리를 불가침의 인격권에서 찾으려고 한 그러한 결론이 정당하다면, 당시의 법은 개인의 프라이버시를 상업주의적인 언론을 비롯한 외부의 침입으로부터 보호 받을 수 있는 권리를 제공한 것으로 생각했다. 여기서 보호받는 대상에는 표현하는 수단이나 형태를 불문하고, 의식적인 노력의 소산이어야 한다는 것도 아니며, 따라서 문학작품이든 아니든 상관없다는 것이다.

그리하여 이른바 문학적·예술적 작품에 대한 출간·복제를 막을 수 있는 권리가 의존하는 기초에는 오로지 인간의 보다 총체적인 면책권, 즉 인간의 인격권의 한 부분으로서의 프라이버시의 권리만이 있다는 것이다. 위렌·브랜다이즈는 이와 같이 개인의 작품이나 표현물의 공개·출간을 본인의 뜻에 반하여 못하도록 보호할 수 있는 근거 내지 권리는 오로지 프라이버시의 권리이며 그것은 보다 총체적인 인격권의 한 부분이라고 규정하고 있다.

그들은 이러한 불법침해적인 공개 내지 공간에 대한 보호가 판례상 재산권을 근거로 하지 않고, 묵시적인 계약위반, 신탁·신뢰의 위반으로 다루어지고 있다는 영국판례도 검토하였다. 영국의 법원에서 계약·신뢰 등의 용어를 사용하고 있는 과정을 보고서, 그들이 판단하기를 그것은 공공의 도덕성, 개인간의 정의, 보편적인 편의 등이 그러한 규칙(rule)의 승인을 요청하게 되고, 또한 그러한 여건하에서의 공개 내지 공간을 받아들일 수 없는 남용으로 판단한 법원의 선언이라고 받아들이고 있다.

그러나 법원이 그러한 선에서 머물러 있다는 것은 어려운 일일 것이라고 봤다. 왜냐하면, 보다 협의적인 법리는 거기서 벗어나는 남용으로 인하여 계약, 신뢰 등을 위반하지 아니하고는 거의 발생하지 않

을 때에만 그 사회의 요청을 충족시켜 줄 수 있기 때문이라 한다. 그렇기 때문에 워렌·브랜다이즈는 보다 더 광의적 기초에 근거를 두어야 한다고 주장한다. 왜냐하면 당대의 침해수법을 보면 가해자가 직접 관계하지 아니하여도 그러한 침해를 할 수 있는 기회가 너무나 많으므로, 법에 의한 침해에 대한 보호는 보다 넓은 기반에 근거를 두지 않으면 안되기 때문이라 한다. 그러니 계약이나 신뢰 등의 협의적인 규칙보다도 보다 넓은 불법행위법상의 규칙에 의존하지 않으면 안된다는 것을 강조하고 있다.

그런 뜻에서 워렌·브랜다이즈는 개개인이 요청하는 보호에 넓은 기반을 제공할 수 있는 것은 오로지 최광의의 재산권뿐이라고 한다. 이러한 재산권에는 모든 소유와 권리, 특권이 포함될 뿐만 아니라 불가침의 인격권까지도 포함될 수 있다는 것이다. 또 그들은 불법침해적인 공개 내지 공간을 금지하는 규칙과 비슷한 것으로서 기업비밀에 관한 법을 검토하고 있다. 여기서도 금지명령은 신뢰의 남용, 계약위반의 법리에 따라 내려지고 있다. 그러니 이 규칙은 제3자가 불법적으로 침해하게 되면 역시 그 근거가 약해진다는 것이다.

이와 같이 불법침해적인 공개문제를 다각도로 검토하고서, 워렌·브랜다이즈는 다음과 같이 종합적으로 결론을 내리고 있다. 즉 앞에서 본 바와 같이 ‘그렇게 보장되는 권리들은, 어떠한 성격의 것일지라도 계약 또는 특별한 신탁으로 생기는 것이 아니라 바로 대세적인 권리라는 것이다. 그리고 이러한 권리들을 보호하기 위하여 적용되어 온 법리는 본질적으로 개인의 재산권 그 말이 확장된 비정상적인 의미로 사용되지 않는 한 이 아니다. 그래서 사적 표현물과 지적·감성적 소산을 보호하는 법리는 바로 프라이버시의 권리를 의미하며 거기에 따른 보호를 사람의 외양, 말하는 것, 행동, 가정적 인간관계 등에까지 미치게 하는 경우에도 이를 정형화하는 새로운 법리를 만들 필요는 전혀 없다’고 한다.

끝으로 워렌·브랜다이즈는 이제 프라이버시의 침해가 법적인 권리 침해로 인정되게 되면, 거기에 따른 구제를 청구하는 요건도 엄연히 존재하게 된다고 하고, 그것은 이미 불법침해적 행위로 말미암아 입게 된 정신적 고통은 배상액의 총액을 산정하는데 가장 본질적인 요소로서 인정받게 될 것이기 때문이라 했다.¹¹⁶⁾

그러나 초기에는 이러한 권리의 규정에 대한 반대 또한 없지 않았다. 예를 들어 가비손(Gavison)은 프라이버시라는 사실상 재산, 명예, 정신적 고통으로부터의 자유라고 하는 각각의 개별적 법으로도 보호될 수 있는 것으로 보았다. 1960년에 프로서(W.L. Prosser)는 프라이버시권의 침해를 사적인 것에 침입, 사적인 것의 공개, 공중의 오해를 받을 수 있는 것의 공표, 그리고 사적인 것을 영리의 목적으로 사용하는 것 등의 네 가지로 분류하여 설명하면서, 이들은 사실상 이미 규정되어 있던 불법행위에 관한 법으로도 다룰 수 있는 것이라고 하였다. 그러나 이러한 지적은 재산침해 등과는 다른 ‘인격적 존엄성’을 다룰 수 없는 한계가 있다.

그러나 이상과 같은 개념은 공통적으로 프라이버시의 대상이 재산권이든 인격권이든 타인으로부터 ‘~를 당하지 않을 권리’라는 의미로 사용되었기 때문에 소극적이고 수동적인 성격으로서 정의된 것이라는 점에서 한계가 있다는 비판을 받는다. 그리고 일생을 대부분 타인과의 관계 속에서 살아가는 현대인들의 권리로서 규정하기에는 불합리하다는 지적도 받게 된다.

이러한 상황에서 1970년대 들어서 프라이버시에 관련된 구체적인 대책들이 각국에서 모색되어 스웨덴이 1973년에 세계 최초로 데이터 보호법을 제정한 뒤, 각국에서 프라이버시에 관련된 입법이 경쟁적으로 형성된다. 미국은 1984년에 프라이버시법을 제정하였고, 프랑스는 1978년에 정보처리·축적 및 자유에 관한 법률을 제정하였다. 1978년

116) 서주실, 위의 글, 69~77면.

에는 영국의 데이터보호위원회인 린도프(Lindop)위원회에서 권고안을 만들었는데, 이는 이후 유럽공동체 국가들이 따라야 할 원칙으로 간주되었다.

이와 같은 법들은 초기의 프라이버시에 관한 권리 규정과 비교할 때 훨씬 더 적극적인 내용을 가지고 있다. 이것은 다음과 같이 시대적 상황이 변화되었기 때문이다. 첫째, 현대사회는 고도로 분화되어 있기 때문에 조직 간에 의존성이 높고 타인과의 접촉이 너무나도 빈번하다. 따라서 ‘혼자 있을 수 있는 권리’라는 것은 사실상 불가능하다. 둘째, 정보기술이 확산됨으로써 개인에 관한 각종 데이터들이 당사자의 의도와 무관하게 생산·유통·이용될 수 있다. 더구나 개인의 재산 정도 등도 전자미디어를 통하여 신속하게 대량 처리될 수 있기 때문에 개인들은 조직이나 국가로부터 자신을 지켜야 한다. 이때 개인은 자신의 ‘개인정보에 대한 부당한 접근을 통제할 것과 자신의 정확한 정보가 자신의 동의하에서 유통될 것을 가능하게 할 권리’를 가질 필요가 있게 되었다.

프라이버시 개념이 초기와 같이 소극적 자기보호에서 나아가 자기정보에 대한 통제권 등에 초점을 맞추는 것에서 알 수 있듯이 프라이버시 개념은 시대적·문화적 상황에 따라 가변적인 속성을 가지고 있는 것이다. 117)

③ 프라이버시권의 보호범위

프라이버시 의 권리는 사생활의 보호를 위하여 중요한 권리이나, 이 권리는 다른 보호법익과 상충될 여지가 없지 않다. 특히 표현의 자유와의 관계에 있어서 더욱 그러하다. 워렌·브랜다이즈는 실제적인 검토에 앞서서 개인의 존엄과 편의가 공공복리 또는 개인간의 정의의 요청에 어느 정도 양보를 해야 되는가를 정확하게 선을 긋는다는 것

117) 고영삼, 『전자감시사회와 프라이버시』 (도서출판 한울, 1998), 26~27면.

은 매우 어려운 과제이지만, 보다 일반적인 원칙은 기존의 명예훼손법과 문학적 예술적 재산권에 관한 법에서 성장해 온 법적 유추를 통해서 도출할 수 있다고 한다. 그리하여 그들은 프라이버시의 권리의 범위 내지 한계로서 여섯 가지를 제시하고 있다. 이를 보면, ① Privacy의 권리는 공적 또는 일반적 이익이 되는 사항에 관한 어떠한 공개도 금지하지 않는다. ② Privacy의 권리는 명예훼손법에 따라 면책특권이 인정된 의사전달이라 할 수 있는 상황에서 행하여진 공개는 비록 그 성질이 사적인 것일지라도 어떠한 사항이든 금지되지 않는다. ③ 구두를 통한 공개로 인하여 생긴 Privacy의 침해에 대하여는 특별한 피해가 없는 한, 법은 아마도 어떠한 구제도 해주지 않을 것이다. ④ Privacy의 권리는 스스로 또는 그의 동의를 얻어 사실을 공개하면 상실된다. ⑤ 공개된 사항의 진실성은 항변의 사유가 될 수 없다. ⑥ 공개한 자에게 악의가 없다는 것은 항변의 사유가 될 수 없다.¹¹⁸⁾

한편 프라이버시는 분석적으로 영역 프라이버시, 신체 프라이버시, 그리고 정보 프라이버시 등 세 가지 차원으로 유형화할 수 있는 것으로 보는 시각도 있다. 영역 프라이버시(territorial privacy)는 개인과 조직의 사적인 영역에 관련된 프라이버시를 말한다. 신체 프라이버시(physical privacy)는 개인의 신체에 대한 타의 침해에 관련된 프라이버시를 말한다. 그리고 마지막으로 정보 프라이버시(information privacy)는 개인의 정보를 스스로 통제할 수 있을 권리와 관련된 것을 말한다. 이러한 시각은 추상적으로 정의되어 온 프라이버시권을 영역, 신체, 그리고 정보 등을 구체적으로 규정하고 있는 데, 이 중 정보 프라이버시와 같은 개념은 앞서 다루었던 개인정보를 가리키는 바, 이러한 정의는 개인정보의 개념이 프라이버시에 포함되는 것으로 보고 있는 시각이다. 미국 IITF(Information Infrastructure Task Force)에서는 개인정보보호방안을 설계하면서 전자시대의 정보 프라이버시의 영역을

118) 서주실, 앞의 글, 79~80면.

연방 정부기록, 통신기록, 그리고 시장에서의 프라이버시 등 네 가지로 분류하고 있다. 이 중 시장에서의 프라이버시는 세금기록, 은행기록, 신용정보 등의 개인금융기록과 비디오 대여기록, 케이블 영화기록 등의 영화기록, 그리고 우편직접판매 등의 것으로 구성되어 있다. IITF의 분류는 미국과 같은 사회적 상황에 맞추어서 잘 설계되어 있는 것으로 보인다.¹¹⁹⁾

④ 프라이버시와 개인정보

일반적으로 개인정보보호의 문제가 프라이버시에 관한 논의의 맥락에서 진행되어 오기는 했지만, 프라이버시와 “개인정보보호”(data protection)는 완전히 동일한 개념은 아니다. 양자는 각각 그 외연을 달리하는 개념으로서 서로 구별되어야 하며, 일반적으로는 개인정보보호는 프라이버시의 한 내용으로 이해될 필요가 있다. 즉 “개인정보보호”는 프라이버시의 한 내용으로서, “타인에 의한 개인정보의 수집·처리와 관련해서” 당해 개인정보의 주체가 가지는 이익을 나타내는 개념이다. 바로 이 이익을 담고 있는 권리를 “개인정보자기결정권” 또는 “자기정보통제권”이라고 한다. 이와는 달리 통신내용을 감청하거나 개인의 사적 비밀을 들추어내어 이를 공표하는 행위는 개인정보보호의 문제와는 구별되는 별개의 프라이버시침해행위이다.

그렇기 때문에 개인정보 일반에 대해 이 같은 사생활비밀보호의 법리가 그대로 타당할 수는 없다. 왜냐하면 사회조직이 유지되고 기능하기 위해서는 개인정보의 유통과 이용이 필수적이기 때문이다. 따라서 개인정보보호법제에 있어서는 개인정보의 “유통”과 “보호”를 적절히 조화하는 선에서 그 보호의 법적 기준이 마련되어야 한다. 개인정보보호법제에 있어서는 정보주체의 동의가 없더라도 개인정보가 “합법적으로” 수집되고 유통될 수 있는 경우가 충분히 인정될 수 있다.

119) 고영삼, 앞의 책, 31면.

사생활비밀의 경우에는 정보주체의 동의 없는 수집과 유통이 원칙적으로 금지되는 것이지만, 개인정보 일반의 경우에는 그렇지 아니다. 개인정보보호법제에 있어서 개인정보 자체를 마치 사생활비밀로 취급하는 태도나 접근방식은 바람직하지 않을 뿐만 아니라 자칫 개인정보 보호를 절대화함으로써 사회 내에 필요한 개인정보의 수집과 유통을 부당하게 막는 우를 범하게 될 것이다. 최근에 개인정보보호법제와 관련한 우리의 규범적 언어생활 속에 만연히 자리를 잡아가고 있는 “개인정보침해”라는 언명은 개인정보보호를 절대시하는 태도를 반영하는 것이면서, 동시에 그러한 태도를 강화하고 있는 것으로 보인다.

그러나 “개인정보” 그 자체가 “침해”되는 것이 아니라, 타자에 의한 개인정보의 수집·이용·제공 등의 처리와 관련해서 당해 정보주체의 사생활적 이익 내지 권리(개인정보자기결정권)가 “침해”되는 것이다. 그리고 이 개인정보자기결정권의 내용은 사회 내 개인정보의 유통의 필요성과 보호의 필요성을 합리적으로 조화시키는 선에서 개인정보보호법에 의하여 구체화되는 것이다.¹²⁰⁾

2) 프라이버시의 본질론

① 인격권론

개인정보의 보호를 헌법 제17조에서 규정하고 있는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”라고 하여 사생활의 비밀

120) 한편 고영삼은 ‘개인정보’와 ‘프라이버시’의 개념의 차이를 설명하면서 “첫째, 프라이버시는 예를 들어 ‘숙녀의 연령,’ ‘부모의 직업’ 등과 같이 사람에 따라 민감한 것일 수도 있고 대수롭지 않게 여길 수도 있는 심리적인 성질의 것이다. 즉 정보주체에 따라 다소 주관적인 성격의 것이기에 개인정보가 가리키는 내용보다 추상적이고 광범하다. 그에 비하여 개인정보는 비교적 객관적이고 명확한 지시대상이 있는 점이 다르다. 둘째, 개인정보의 개념은 프라이버시의 개념보다 사회적 관계의 형성에 있어서 더 심각하게 간주되기도 한다. 예를 들어 정보사회에서는 사회적 관계 속에서 개인정보가 때로는 개인정보의 주체보다도 더 신뢰할 수 있는 것으로 간주되기도 하는데, 이러한 부분은 자아정체성 등에 관련하여 사회학적·철학적으로 심각한 문제를 야기하기도 하는 문제”라고 지적하고 있다. 고영삼, 위의 책, 30~1면.

과 자유의 불가침을 보장하기 위한 것으로 이해하는 견해이다. 즉, 프라이버시를 헌법상의 권리로 보고 개인정보의 성격을 프라이버시의 일종으로 보아 양도할 수 없는 것이라고 한다.¹²¹⁾

헌법 제17조는 외부의 침해로부터 개인의 사적 영역을 보호하고 사생활의 자유로운 형성을 보장하고 있는데, 이러한 사생활에 관한 권리는 전통적으로 개인이 외부의 간섭을 받지 않고 혼자 그대로 있을 수 있는 권리(right to be let alone)를 중심적인 내용으로 하고 있지만, 현대 과학기술의 발달과 함께 도래한 정보화 사회에서는 컴퓨터, 원격사진촬영기기 등을 이용한 개인정보의 수집 처리·관리가 대량·집단화됨에 따라 개인의 사생활의 비밀과 자유가 침해될 가능성이 현저하게 증대하였고, 이에 따라 사생활의 비밀과 자유의 보장이 그 어느 때보다 중요하게 되었고, 개인의 자기정보관리권이 중요한 내용으로 추가되기에 이른 것으로 인정되고 있다.¹²²⁾

이러한 사생활의 비밀·자유에 대한 법적 성격에 대하여는, 우리 헌법은 사생활의 비밀·자유를 자유권 조항에서 규정하고 있고 정보화사회에서 개인의 존엄을 보장하기 위한 정보에 대한 자기결정권은 헌법 제10조에서 보장된다고 볼 것이므로 사생활의 비밀·자유는 소극적인 권리라고 이해하는 견해¹²³⁾가 있는 반면, 사생활의 비밀과 자유는 인간의 존엄과 가치에 기초한 인격권적 성격과, 자유권적 성격 및 이의 보호를 위한 청구권적 성격을 동시에 내포하고 있는 권리로서의 성격을 가진다고 보는 견해¹²⁴⁾가 있다.

121) 김연수, 『개인정보보호: 고도 지식정보 사회의 개인정보와 Cyberlaw』 (사이버출판사, 2001), 41면.

122) 정종섭, 『헌법학원론』 (박영사, 2007), 522~3면.

123) 김철수, 『헌법학개론』 (박영사, 2006), 620면.

124) 권영성, 『헌법학원론』 (법문사, 2005), 446면; 성낙인, 『헌법학』 (법문사, 2008), 570면; 정종섭, 『헌법학원론』 (박영사, 2007), 524면.

② 재산권론¹²⁵⁾

오늘날 개인정보는 개인이 사적 생활을 하는데 필요한 것이라기 보다는 단지 국가나 민간사업자 등이 업무나 영업활동을 수행하기 위하여 그 수행목적에 합치되는 대상자를 선별하기 위해 이용하는 것이 대부분이며, 이 경우 이용되는 개인정보는 정보 전부가 아니라 업무나 사업의 관점에서 다양한 정보군 가운데 필요한 정보를 분석하고 추출하여 재구성한 정보라는 점에 있다. 따라서 선별된 개인정보취급자는 개인정보를 기준으로 특정한 정보나 서비스를 제공하거나 또는 금전을 지급하고 징수하는 것이고, 그러므로 개인정보는 경제적 측면에서 대중을 통제하는 방법으로 활용되고 있는 것이며, 정보주체인 개인은 평등한 서비스를 향유한다는 측면에서 이익을 얻는 것임이 간과되어서는 아니 된다. 그러기에 개인정보의 보호 문제를 프라이버시권의 개념으로부터 도출하는 체계에서 벗어나 새로이 개인정보에 관한 권리의 개념을 재정립할 필요가 대두된다. 그 권리의 객체가 되는 개인정보를 범주화하고 이에 대응하는 권능을 세분화·체계화함으로써 보호와 이용의 조화로운 법률관계를 형성하도록 하는 적극적 의미로 해석될 수 있기 때문에, 우선 국가 또는 민간사업자 등 개인정보관리주체에 대한 부정과 불신의 관념에서 벗어나 정당한 권리·의무의 법률관계로 형성할 수 있도록 하는 것이 중요한 것이다. 결과적으로 보호할 것은 두텁게 보호하고, 이용할 것은 합리적으로 보호할 수 있는 제도적 체계의 확립을 위해서 개인정보에 관한 권리의 재정립이 요구된다 할 것이다.

이러한 시각은 프라이버시에 관한 종래의 논의가 인격권에 국한되었던 한계를 벗어나 재산권적 측면을 도외시하지 않았음에서도 읽을 수 있는 대목이다. 즉 기업의 입장에서 보면 개인정보가 중요한 경영

125) 이만영, 『개인정보법제론』(진한M&B, 2005), 27~30면.

자원으로 등장하고 있지만 소비자 입장에서 보면 개인정보의 주체인 개인의 프라이버시를 심각하게 침해할 수 있다는 점에서 프라이버시 보호에 대한 적절한 대책이 요구되는 바, 경제적 효율성의 관점에서 정책채택의 문제는 어떻게 하면 개인적 측면이나 기업 측면 그리고 사회적 측면에서 보호정책을 유지하는데 드는 비용이 거래비용 감소에 따르는 편익보다 적게 들게 할 수 있느냐에 달려 있다. 이러한 관점에서 제기되는 접근방법 중의 하나는 개인정보에 대해 재산권을 부여하는 것이다. 일반적으로 재산권은 재산을 소유자가 원하는 방식으로 이용하거나 처분할 수 있는 권리, 재산권의 전부 또는 일부를 타인에게 교환을 통해 양도하거나 증여할 수 있는 권리, 재산을 이용해 소득을 전유할 수 있는 권리 등으로 구성된다. 개인정보에 재산권을 부여하게 되면 개인정보를 본인의 명시적 혹은 묵시적 동의 없이 제3자에게 판매하는 것은 불법적인 것이 되며, 승낙이 이루어진 경우에도 판매대금의 지분에 해당하는 권리는 개인에게 귀속될 것이다. 재산권 부여방식은 프라이버시 침해에 대한 적절한 보상청구권을 보장해주며, 적정 수준의 개인정보 유통을 유지시켜 줄 것이다.

일신존속권적 성격의 인격권으로서의 프라이버시가 아니라, 계약자유 원칙에 따른 거래의 대상으로 보면서도 그 활용이 갖는 경제적 효용을 고려하면서 합리적인 개인정보의 유통에 최저기준으로서 권리의 객체를 보호하려는 재산권적 접근은 정책논리의 내재적 결함에도 불구하고 정보환경에 대한 균형감각을 가진 시야를 가져다주는 계기를 마련했다고 평가할 수 있다.

이는 정보자체가 재산적 가치가 있거나 또는 정보의 이용을 통하여 재산적 가치를 획득할 수 있다는 것을 전제로 하여 정보의 귀속관계를 살펴보아 개인정보침해의 경우 사법상 구제수단을 확보할 것을 예정한 법률관계를 물권법적 측면에서 접근하여 기존의 지적재산권과 같은 배타적인 권리를 인정하여야 한다는 전제에서 출발한 것이다.

하지만 개인정보보호를 위하여 거기에 특별법적 보호방안을 마련하여 배타적인 권리로 승격할만한 특성을 지니고 있지 아니하다.

왜냐하면 동산소유자는 자신의 물건을 자유롭게 처분할 수 있는 권능을 가지고 처분할 때 물건을 인도하여 점유를 잃게 되지만, 정보주체는 개인정보를 처분할 수 없을 뿐만 아니라 일응 처분과 같은 법적 효과를 낳는 법률관계를 맺는 것으로 볼 수도 없기 때문이다. 결국 정보주체는 자신의 개인정보를 타인에게 이용케 하는 것과 함께 계속적으로 이용할 수 있으므로 타인의 이용에 따른 일정한 제한을 받지 않으며 이 점에서 개인정보는 물건법상 동산의 물건변동에 관한 법리로써 규율될 수 없는 대상이라 할 것이다.

한편, 기존의 프라이버시 논의가 정보주체인 개인에 관한 인격적 가치에 중점을 두어 헌법학적 혹은 불법행위법적 논의로 제기되어온 반면, 재산권적 논의는 개인정보에 있어서도 그 정보가 경제적 가치를 띠고 있어 거래의 대상이 되고 있다는 거래계의 현실을 간과하지 않고 개인정보를 제공하는 자에 의한 권리보호수단의 확보가 가능하다는 점을 반영하여 거래법 법리 속에서 해결책을 찾아내는 데 의미를 가진다. 이러한 관점을 유지하면서 물건변동법리의 적용이 곤란한 한계성을 극복하여 개인정보에 관한 거래실체를 반영하여 고찰하는 것이 요구되는 바, 이것이 바로 계약법적 접근이라 할 것이다.

온라인상 영업주체가 타인의 개인정보를 정보주체로부터 직접 수집하는 경우를 예로 들자면, 영업주체가 정보주체로부터 개인정보에 대한 물권을 취득하지 못하므로 현실적으로는 개인정보를 이용하는 이용계약(license)을 체결하여 정보주체로부터 얻어진 개인정보를 활용한다. 영업주체는 정보주체의 개인정보를 직접적으로 지배하는 법적 지위를 가지지 못하므로 정보제공자와의 계약내용에 따라 일정한 범위에 한정하여 이용권을 행사할 수 있을 뿐이다. 이 때 수집된 정보는

민법상의 물건과 구별되며, 여기서의 이용권은 물건에 대해 논의되는 소유권과 유사한 속성을 가지고 있지도 않다. 그리고 정보통신서비스 이용계약의 체결에 있어 정보주체의 동의는 이용계약체결에 관한 정보통신서비스제공자의 청약에 대한 승낙의 의사표시라 할 것이며, 개인정보의 수집·이용에 관한 동의의 철회는 정보주체의 일방적인 의사표시로 인한 계약해지로 판단할 수 있는 것이다.¹²⁶⁾ 이렇게 개인정보에 관한 계약법적 논리구성은 정보주체가 개인정보에 관한 자기결정 혹은 자기통제를 통하여 스스로 정보제공 여부를 선택할 수 있도록 한다는 점에서 매우 중요한 논의가치를 가진다.

결국 거래법적 관점에서 개인정보에 접근하게 되면 그것이 개인을 식별하는 신원사항일 뿐만 아니라 재산상태와 인격적인 가치도 함께 가지고 있는 것으로 파악하게 되므로 경제적 가치만을 중시하는 지적재산권의 일반적 성질과 구별되지만, 인간의 신체·자유·명예·초상·정조 등과는 구별되는 것으로 그 보호대상이 순수하게 인격적인 이익만은 아니라는 것을 알 수 있다. 그리고 이러한 개인정보의 법적 성질은 실제로 개인정보가 이용되는 거래계의 현실을 돌아 볼 때, 개인정보의 이용으로 빚어지는 문제가 재산적 불이익과 매우 밀접히 연관되어 있음에서도 읽을 수 있는 것이다.

(2) 사회학적 접근

사회학적 차원에서 개인정보에 관한 논의는 점증하는 정보의 중요성에 발맞추어 지속적으로 증대되어 왔는데, 크게 보아 사회 내에서의 정보의 긍정적인 측면을 강조하는 견해들과 부정적인 측면을 강조하는 견해들로 구분해 볼 수 있다.

126) 배대헌, “정보의 귀속, 유통에 관한 민사법적 접근: On Line상 개인정보의 보호를 중심으로,” 『비교사법』 제8권 제2호(통권 제15권)(2001.12.), 274~6면.

1) 정보와 근대국가: 정보의 긍정적 측면

① 근대국가의 형성과 정보¹²⁷⁾

“우리가 20세기 말에 와서 정보시대로 진입하고 있다고 일반적으로 가정하고 있지만, 근대사회는 그 시작부터 ‘정보사회’였다”¹²⁸⁾라는 주장에서 단적으로 드러나듯, 기든스(Anthony Giddens)는 정보에 대한 중요성의 부각은 아주 깊은 역사적 뿌리를 가지고 있기 때문에 오늘날 정보가 특별한 중요성을 가지고 있는 것은 사실이지만, 기존체제와의 연속선상에서 충분히 파악할 수 있는 것으로 본다.

우선 기든스는 우리가 살고 있는 세계가 과거 어느 때보다 훨씬 더 많이 조직화되고 있다는 것에 주목하는데, 사람들의 일상생활이 체도에 의해 전례를 찾아볼 수 없는 방식으로 계획되고 조정된다는 것은 단순히 개인의 자유가 냉혹하게 감소한다는 것을 암시하는 것만은 아니다. 과거의 환경 속에서는 사람들이 기근, 자연의 불확실성, 여성에 대한 다산의 강요 등과 같은 엄청난 제약을 받았다는 것을 부인할 수 없으며 무엇보다도 일상적인 생계의 유지라는 지루한 압박으로 인하여 사람들은 엄청난 제약을 받았는데, 현대적으로 이러한 제약은, 적어도 일부의 선진사회에서는, 과거만큼 중요한 것이 아니다. 이처럼 오늘날의 생활이 이전에 비해 일상적으로 그리고 체계적으로 관리되고 있다는 전제가, 오늘날 우리가 일종의 감옥 속에 살고 있다는 것을 의미하는 것은 아니며, 오히려 사람들의 자유의 증가는 조직화의 증가와 밀접하게 연관되어 있다고 할 수 있다.

즉 오늘날 생활은 과거 어느 때보다 훨씬 더 질서 있게 조절되고 있는데, 이것은 특히 전통적인 자연의 제약을 극복할 수 있는 현대의

127) 이하의 논의는 기본적으로 Frank Webster, 앞의 책, 99~128면의 논의에 기반하고 있다.

128) Anthony. Giddens, *Social Theory and Modern Sociology*(Cambridge, UK: Polity Press, 1987), p. 27.

능력 때문에 가능하게 되었다. 사람들을 위한 선택의 여지가 증가함에 따라 조직적인 구조가 발달하였고 이러한 조직적 발달이 선택적 여지의 증가에 대한 전제가 되기도 한 것이다. 이러한 조직화가 일반적으로 매우 복잡하다는 것을 강조할 필요가 있다. 한편 이러한 조정을 이루어내는 ‘추상적’인 전문가 체제에 대하여 사람들은 거의 생각하지 않는다거나, 또는 대부분의 경우 사람들이 그 신뢰성에 대하여 믿음을 가지고 있다거나 하는 것은 문제가 되지 않는다. 중요한 사실은 현대 생활이 과거에는 찾아볼 수 없을 정도로 사회적으로 조직화되어 있다는 것이다.

이렇게 생활을 조직화하기 위해서는 사람들과 그들의 활동에 관한 정보가 체계적으로 수집되어야 한다. 사회생활을 조정하려면 사람들에게 대하여 알아야만 하기 때문이다. 간단히 말해서 일상적인 감시는 효과적인 사회적 조직화를 위한 전제조건인 것이다. 사람들을 정찰하는 방식(센서스에서 의료기록, 전화계정, 은행통장, 학생기록 등에 이르기까지)의 확대를 추적하는 것은 어려운 일이 아닌데 그것은 오늘날의 삶의 중요한 특징인 조직화의 증가와 동시에 진행되어 왔다. 조직화와 감시는 삼 쌍둥이(Siamese twins)로서 근대 세계의 발전과 함께 성장하여 왔다고 할 수 있다.

결국 근본적인 의미에서 모든 ‘국가’가 ‘정보사회’에 해당된다고 지적할 수 있다. 왜냐하면 국가권력의 생성은 행정목적 추구를 위하여 규칙적으로 정보를 수집·보관·통제하는 자체 감사의 감시체계를 재생산할 수밖에 없기 때문이다. 그러나 민족국가에서는 고도의 특징적인 행정통합성으로 그 어느 시기보다도 이러한 활동이 최고 절정에 이르게 되었다.¹²⁹⁾ 이러한 추상적인 수준의 논의를 보다 구체화하기 위해 민족국가의 주요 특징을 더욱 면밀하게 검토해 보면, 우선

129) Anthony Giddens, *Nation state and Violence*, 진덕규 역, 『민족국가와 폭력』(삼지원, 1991), 211~2면.

근대세계를 구성하는 민족국가는 상대적으로 새로운 개념이라 할 수 있는 바, 이전 사회와 다른 사회경제적 조직과 정체성을 보유하고 있다고 할 수 있다. 아울러 민족국가의 절대 다수가 전쟁이라는 조건 속에서 형성되었고 튼튼한 방위력을 보유함으로써 존속한다는 점이 지적될 수 있는데, 전쟁과 그에 대한 대비는 민족국가에 대한 근본적인 기여요인이 되었다. 즉 민족국가를 주어진 영토에 대한 주권의 소재로 정의하는 것으로부터 도출되는 것은 정부의 최소한의 책임은 영토의 완전성을 보존하는 것이라는 점으로 전쟁에 대한 대비는 모든 민족국가의 전제조건이며 근대역사에 걸쳐 반복적으로 시험되고 있는 원칙이다. 또한 근대적 전쟁/방위가 사회 전체와 훨씬 더 결정적으로 관련성을 가지게 되었다는 사실도 중요한데, 이는 단순하게는 보다 많은 인구가 근대적 전쟁에 휩싸이게 된다는 것을 의미한다. 이러한 의미에서 국가들 간의 현대적 전쟁은 그 폭력성이 증가되었다고 한다면, 이와 관련된 것으로서, 전쟁이 사회적 영역으로 더 깊숙이 확장되는 다른 하나의 방식이 존재한다. 현대의 전쟁에서는 사회 전체가 전쟁 지원을 위해 동원되기 때문에, 국가의 경제적 힘과 군사적 효율성 사이에는 긍정적인 상관성이 존재한다는 주장이 설득력을 가진다. 결국, 정보, 정보기술, 그리고 국가/군사/산업 연합 간의 연관성을 주목하지 않을 수 없는데 총력전의 시기에는 산업과 방위가 밀접하게 연관되어 있기 때문에, 정보와 정보기술이 전쟁의 발발 및 대비와 특히 밀접한 관계를 가지고 있다는 것을 밝히기는 어렵지 않다. 현대적 전쟁/방위는 최대한으로 신뢰가 있어야 하며 그러한 목적을 위하여 전쟁은 선도적인 기술에 의지해야 한다. 현대적 전쟁/방위는 본질적으로 정보에 관한 것으로, 정보는 현대 전쟁활동의 중심에 있다.

냉전의 종식을 염두에 두면서 방위/전쟁 제도를 운영할 필요성이 사라졌다고 믿는 사람들이 있을 수 있는데, 여전히 “영구적인 정부기능으로서의 첩보활동에 대한 전제조건은 근대 국가체계에 놓여 있다”는

것을 깨닫는 것이 중요하다. 오히려 전 세계에 걸쳐 사건과 활동 군사적 및 민간의 을 일상적으로 그리고 지속적으로 감찰·감시하는 기술이 상호연결된 거대한 체계가 등장하게 되었다. 아울러 감시기계가 외부의 적에 대해서만 작동하는 것은 아니다. 내적인 공격에 대한 민족국가의 취약성을 고려할 때, ‘전복자’를 탐색하려는 강력한 요구가 있게 마련이다. 요컨대, 우리가 목격하는 것은 국경을 보호하려는 민족국가의 의무에서 비롯된 감시체계의 성장을 강요하는 강력한 힘이다. 국경에 의해 분리된 세계에서는 불가피하게 효과적인 방위/전쟁기계의 건설에 대한 내적인 압력이 있을 수밖에 없다. 그리고 국가들이 갈등이나 잠재적 갈등의 상황에 처하기 때문에 ‘효과적’인 것이 무엇인가는 항상 변하기 마련이다. 그러나 변하지 않는 것은 체제 내외부의 실제적 및 잠재적인 적에 대한 최상의 정보를 수집하고 그에 대하여 대응하는 요구이다. 한 수준에서는 이것은 점점 더 정교화되고 있는 ‘스마트’ 무기기술의 설계와 발달에서 나타나고 있다 다른 수준에서는 그것은 엄청나게 복잡한 통신망의 형성을 가져왔다. 나아가서 또 다른 수준에서는, 앞의 두 가지와 교차되기는 하지만, 국가안보에 대한 위협으로 간주되는 모든 것에 대한 감시와 추적을 향한 지속적인 압력이 존재하고 있다.

민족국가의 기초 즉, 전쟁의 와중에서 형성되어 주어진 영토를 지배하려는 모든 통치권력의 우선순위는 기든스가 ‘내적 평화(Internal pacification)’라고 하는 것이었다. 간단히 말해서 외적인 경계를 지키기 위해서는 내적으로 질서와 안정이 이루어져야만 했던 것이다. 의심할 여지없이 초기에는 ‘내적 평화’가 군대의 무력에 의한 강요라는 형태를 띠었지만 장기적인 존속을 추구하는 국가에 대해서는 훨씬 더 많은 것이 요구되었다. 최소한 국가는 그 국민에 대하여 알아야 했는데 그 이유는 특히 외세의 공격에 맞서 싸울 수 있는 인원을 징집해야

할 필요성 때문이었다. 나아가서 민족국가는 그 국민에 대한 지식을 가지고 있어야 세금을 효과적으로 징수할 수 있다. 그리고 이러한 필요는 일정 유형의 센서스가 모든 민족국가의 필수요건이라는 것을 의미하며, 이에 따라 감시는 그 초기부터 우선순위가 되었다. 그 후로 역사적으로 변화가 많았지만, 내부 국민을 감시하는 방식의 확산은 쉽게 확인된다.

② 현대국가의 전개와 정보

오늘날 민족국가에서 살고 있는 사람들은 시민으로서의 권리와 의무를 많이 가지고 있다. 즉 민족국가와 그 구성원 간의 ‘계약’에 따라 시민적 권리와 의무가 출현하게 되었다는 것이다. 감시와 관련되는 주된 고리는 이것들이 어떻게 전달되고 수집되는가와 관계가 있다.

민족국가는 그 보호 아래에서 시민권이 행사되기 때문에 이러한 추가적인 책임을 이행할 수 있는 행정적 수단을 개발해야 한다. 그리고 감시에 대한 특히 강력한 힘은 이러한 근대 사회민주주의 국가의 성장이다.

그 이유는 시민의 권리의 의무에 대한 관리는 국가 성원에 대한 세심한 개체화를 필요로 하기 때문이다. 선거 명부는 전체 인구에 대하여 연령과 주거지를 기록하는 데이터베이스의 개발을 요구한다. 사회적 서비스는 주거조건이나 병력에서부터 부양가족에 대한 정보까지 사람들의 환경에 대한 자세한 기록을 필요로 한다.

국세청은 나라 안의 모든 사람들의 경제적 상황을 자세히 기록하고 있는 엄청난 파일을 만들어낸다. 학교를 다니는 동안에도 성취도, 발달성, 연속성과 변화성 등을 기술하는 기록들이 만들어진다. 빈곤의 최악의 결과를 약화시키려는 프로그램은 불행한 사람들에 대한 많은 정보를 필요로 한다.

즉 “복지 혜택과 서비스의 공여는 대중감시체계의 핵심이다. 그 이유는 바로 이 영역에서 분류, 정보수집 그리고 기록과정이 지속적으로 확대되고 있기 때문이다.”¹³⁰⁾

2) 정보와 감시사회: 정보의 부정적 측면

① 감시사회이론 일반

감시는 정보사회의 형성원리이며 문화적 기반이 되는 가장 특징적인 것이다. 상식적으로 감시는 “단속을 하기 위하여 혹은 나쁜 의도를 지니고 은밀하게 숨어서 관찰한다.”라고 하는 이미지를 가지고 있다. 이 같은 정의에서 물론 ‘단속’이 반드시 나쁜 의미를 가진 것은 아니지만, 우리들은 감시자가 되건 피감시자가 되건 간에 감시에 연루되는 자체에 대하여 좋은 느낌을 가지지는 않는다. 심지어 독재국가에서는 정치적 감시의 이미지도 은연중에 느끼게 되어 이래저래 재미있는 단어인 것은 아니다.

이러한 이미지의 극단적인 예로 오웰(George Orwell)의 『1984년(Nineteen Eighty Four)』에 나오는 빅브라더(Big Brother)를 들 수 있다.¹³¹⁾ 이 책에서 그는 모든 사람의 일거수일투족이 전체주의 권력에 의해 감시당하는 상황을 섬뜩하게 묘사하였다. 빅브라더는 시민들에게 완전한 순종을 요구하며, 그 삶의 모든 측면을 통제한다. 빅브라더는 끊임없이 감시하고 정탐하며, 통일적인 순찰대가 거리의 구석을 서성대고, 헬리콥터가 하늘에 맴돌며, 창문을 들여다 볼 자세를 취하고 있다. 감시의 주요수단은 “telescreen”이라 불리는 장치로서 모든 주택과 아파트의 내부에 설치되어 있다.

그 텔레스크린은 쌍방향의 텔레비전이라 할 수 있는데, 각자가 그것을 관찰할 수 있으나 또한 Big Brother도 그들을 감시할 수 있다.

130) Frank Webster, 앞의 책, 120~1면.

131) George Orwell, *Nineteen Eighty Four*, 김병익 역, 『1984년』 (문예출판사, 1999).

시민들은 그들이 감시되고 있는지, 그 때는 언제인지를 알 길이 전혀 없다. 이러한 빅브라더의 이미지는 이후 많은 논자들에게 감시의 부정적인 측면을 각인시키는 결과를 가져왔다고 해도 지나치지 않을 것이다.

그러나 이러한 행위 자체가, 비록 현대사회의 고유한 것은 아니지만, 언젠가부터 사회적 삶 속에서 하나의 필연적인 삶의 양식으로 되고 있는 것을 부정할 수는 없다. 즉 현대사회에서 사람들의 관심은 예전과 같이 물리적 근접거리에만 제한되지 않는다. 인식의 관점이 전 지구적으로 확장되어 간다. 이런 가운데 예를 들어 조직의 다분화, 이해관심의 다양화, 익명적 대상과의 빈번한 접촉, 중요하지만 일시적인 거래의 보편화, 그리고 “추상체계에 대한 신뢰의 요구” 등이 늘고 있다. 이러한 상황에서 사람들은 사회적 관계의 형성에서 신뢰를 확인할 수 있는 정보의 수집을 요구하게 되는데, 그것은 대상과 대상의 정보에 대한 감시로 연결된다. 그런데 감시는 시민들이 권리를 획득하는 수단이 되기도 하면서 동시에 자율성을 침해받는 경로가 되기도 하기 때문에, 향후 시민사회의 개념화에서 반드시 정치하게 분석되어야 하는 부분이기도 하다.

결국, 감시에 대한 개념을 새롭게 조명할 필요가 있게 되는데 현대사회의 감시를 만약 은밀하게 숨어서 엿보거나 남을 이용하기 위해 비밀리에 활동하는 전통사회의 상식적인 이미지로 생각한다면, 감시를 제대로 이해할 수 없다. 현대의 감시는 그러한 상식적 개념에서의 감시의 이미지를 포함하고 있지만, 공개적인 것도 있고 긍정적인 효과를 수반하는 것도 있다. 피동적이기만 한 것이 아니라, 혜택을 얻기 위한 목적으로 피감시자가 자발적으로 참여하는 경우도 있다. 또 대상을 통제·제약·구속하겠다는 의도가 있기도 하지만, 그보다는 사회관계의 강도를 조절하기 위한 방편으로 의식·무의식적으로 행사되는 것이기도 하다. 때문에 현대의 전자감시를 기능적인 면에서 볼 때,

반드시 은밀하고 부정적인 것으로 간주할 필요는 없다. 단지 감시는 어떤 주체가 “어떤 특정한 의도를 지니고 대중을 관찰·감독하는 것”을 말한다. 이러한 맥락에서의 감시개념을 파악하기 위해 [표 1-3-1]과 같이 감시개념에 대한 지도를 만들 수 있다.

[표 1-3-1] 정보사회 감시의 개념지도

구분		감시의 의도	
		악의적인 것	선의적인 것
감시의 방식	은밀	감시 I	감시 III
	공개	감시 II	감시 IV
감시의 기능		역기능	순기능

[표 1-3-1]에서는 감시를 감시 주체의 의도와 감시의 방식에 따라 네 가지로 구분하였다. 전통적으로 감시는 감시I의 의미(은밀+악의)로만 파악되어 왔다. 그러나 광의의 의미에서는 감시는 위의 네 가지 모두를 포함하는 것이다. 일종의 ‘예의 주시함’과 비슷한 개념으로 간주할 수 있다. 이러한 감시의 여러 가지 유형에 따른 사례를 살펴보면 다음과 같다.

- ① 감시 I (은밀 + 악의): 상식적인 감시의 개념, 뒷조사, 음해, 개인 정보 침해
- ② 감시 II (공개 + 악의): 흑색선전
- ③ 감시 III (은밀 + 선의): 사적배려, 보살핌
- ④ 감시 IV (공개 + 선의): 신용정보조사, 업무감사, 정보공개요구

감시를 이렇게 4차원으로 보는 것은 상식적 이미지를 넘어서 감시를 일종의 ‘사회관계적 속성’으로 보는 것과 맥을 같이 한다. 이러한 관점은 감시란 은밀하게 숨어서 보는 차원보다는 광의의 것임을 뜻한다. 즉 만남의 과정에 수반되는 얼굴표정, 언어, 제스처 등에 개입되

어 있는 말하자면 만남에서 발생하는 약간의 긴장의 징후에 대한 관찰과 상호간의사교환에 있어 예의 주시하는 것을 감시의 근간이라고 본다. 말하자면 관계의 유지나 단절을 결정하기 위하여 혹은 신뢰형성의 가능성을 탐색하기 위하여 상대에 대해 알아보는 것을 감시라고 규정할 수 있다. 이러한 정의는 조직간 관계에서도 동일하게 적용될 수 있을 것이다.

그런데 정보사회는 감시환경에 다음과 같은 변화를 가져왔다. 첫째, 디지털 기술이 감시능력을 엄청나게 확장시켰다. 둘째, 현대국가는 그 존속을 위하여 데이터를 지속적으로 수집하는 등 각종 통계기관을 통하여 정보수집에 상당한 노력을 경주한다. 셋째, 감시의 새로운 대상으로 소비 일상영역이 형성·팽창되고 있다. 이렇게 볼 때, 우리는 감시를 일단 위와 같이 네 가지 차원의 넓은 폭으로 이해한다고 할지라도, 정보사회에서의 감시를 본 연구과제에 맞게 재조정하여 이해할 필요가 있다. 정보 프라이버시와 관련시켜 볼 때, 여기서 사용하고자 하는 감시의 개념은 위의 감시I(은밀 + 악의)과 감시IV(공개 + 선의)의 것이다. 그 이유는 다음과 같다.

- ① 감시 I(은밀 + 악의)은 뒷조사를 하거나 개인정보를 불법적으로 수집·유출하는 등의 것을 말한다. 이것들은 불법적으로 설립된 사설 개인정보조사기관, 비민주적 공안기관 등이 행하는 것과 같으며, 개인정보 침해의 한 방식이 되기 때문에 부정적으로 기능한다.
- ② 감시 II(공개 + 부정)는 갈등관계에 있는 두 당사자 간에 발생할 수 있는 것으로 상대를 저해하기 위한 목적으로 감시하는 행위를 가리킨다. 역시 부정적으로 기능한다. 이 경우는 본 연구와 무관한 부분이다.
- ③ 감시 III(은밀 + 선의)은 배려, 보살핌 등 지극히 사적이고도 애정이 있는 사람들 간의 관계에서 발생하는 방식으로 순기능적 역할을 한다. 이 경우도 본 연구와는 무관하다.

- ④ 감시Ⅳ(공개 + 선의)는 시장에서 개인·법인의 신용정보를 조사하는 것, 업무감사, 국가나 기업에서 복지조장을 위한 공적인 조사, 그리고 공공기관에서 보유한 개인정보를 개인이 요구하여 조회하는 것 등이 해당된다. 2차적 사회 내에서 구성된 계모임 등과 같이 상호부조의 것도 포함된다. 이 방식은 공개적이고도 긍정적인 결과를 초래하기 때문에 개인들이 자발적으로 감시의 대상이 되고자 하기도 한다.

이러한 도식에서 보듯이 정보사회에서 감시를 반드시 은밀·공개 혹은 부정적·긍정적 혹은 강제수집·자발적 제공 등의 일면성으로만 해석하고자 한다면 무리가 따른다. 일종의 양면성을 가지고 있다는 것이다. 즉 정보사회에서 감시는 개인의 행동을 구속하고 제한할 뿐만 아니라 행동을 가능케 하고 권한을 부여하는 것이다. 때문에 감시는 사회통제의 수단인 동시에 시민의 권리를 존중하는 수단이 될 수 있는 것이다.

한편 어떤 경우는 현실적으로 위의 네 가지가 혼재하여 일어나는 감시가 있을 수도 있다. 가령, 위의 은밀·공개, 긍정·부정, 선의·악의, 명확한 의도·불명확한 의도의 여러 차원들이 혼합된 상태로 발생하는 경우도 있을 수 있는 것이다.¹³²⁾

② 감시사회이론의 전개

기든스가 근대 국가의 형성에 있어서 정보의 중요성을 논함에 있어서 기본 전제로 삼았던 사람들이 점점 더 조직화된 생활을 영위해 가고 있다는 주장은 사회과학에서 전혀 새로운 것이 아니다. 그런 주장은 ‘관리사회’에 대한 테오도르 아도르노의 생각, 미셸 푸코의 현대생활의 특징인 ‘감옥망(carcéral networks)’에 대한 기록에서도 분명하게 드러나며, 근대세계의 ‘관료제화’에 대한 막스 베버의 묘사에서도 등

132) 고영삼, 앞의 책, 19~25면.

장하고 있다.¹³³⁾ 그렇지만, 대부분의 논자들이 근대성(modernity)에 대하여 결정적으로 비판적인 견해를 가지고 있다는 것은 잘 알려져 있고 그 중에서도 아도르노의 비판주의는 유명하다. 푸코의 경우, 그가 부인했음에도 불구하고, “차별과 감시가 점점 … 더 구체화되고, 더 복잡하고, 더 효과적이고, 더 결정적으로 되었다”는 결론을 피하기가 어렵다. 그리고 베버의 경우 그가 관료제를 피할 수 없는 것으로 체념하고 받아들였다고 할지라도, 그렇다고 ‘영웅’의 소멸에 대한 그의 침울함이나, ‘완전하고 아름다운 인간성의 시대로부터의 괴리’에 대한 그의 애도, ‘정신을 결여한 전문가와 감정을 결여한 관능주의자’로 가득찬 세계에 대한 그의 니체적 공포, 그리고 합리적 법적 조직체라는 ‘철창(iron cage)’을 동반하는 ‘기계화된 석화(petrification)’에 대한 그의 심한 거부감이 줄어들지는 않았다. 특히 개인정보보호의 문제에 관한 논자들에게는 이러한 견해가 널리 수용되고 있다는 사실을 쉽게 확인할 수 있다. 즉 사람들에 대한 경찰의 정보 수집 배심원들의 심사에서 오용될 수 있거나 심지어는 불법적인 체포를 야기할 수 있는 과 같은 문제를 부각시키고 있는 문헌들이 적지 않다.

두 가지 관련된 쟁점이 특히 절박한 관심사이다. 하나는 기관들이 다른 목적으로 수집된 정보에 접근할 수도 있다는 두려움인데, 예로서 경찰이 고용이나 의료 또는 은행기록에 접근할 수도 있다는 것이다. 다른 하나의 관심사는 보다 일반적인 쟁점으로서 독립된 데이터 베이스를 통합하는 것이다. 대부분의 국가(그리고 매우 많은 다른 종류의) 감시정보가 컴퓨터화됨으로써 과거에는 분리되었던 정보가 통합될 수 있는 가능성이 생겨나게 되었다. 이러한 통합에 대해서 상당한 제약이 부과되고 있지만 그 잠재적 가능성은, 개인의 국민보험번호를 기초로 하여 특정한 개인에 대한 ‘전체적 초상화’를 구성할 수 있는 ‘전자주민카드’에서 분명히 드러난다. 예를 들어 기관이 의료, 교

133) Frank Webster, 앞의 책, 99~101면.

육, 납세, 고용, 은행, 범죄 등의 기록에 접근할 수 있다면 상당히 복잡하고 상세한 개인 정보가 구성될 수 있다는 것은 분명하다. 이러한 과정은 호환성 있는 컴퓨터 통신망을 도입하려는 정부부서의 결정에 의해 촉진될 수 있는데, 이 작업은 1980년대 중반에 시작되어 그 후로 지속적으로 추진되고 있다. 그러한 발달은 효율성과 더 많은 통제를 추구하는 정부 공무원들에게는 분명 매력적인 것이지만, 이미 수행되고 있는 감시를 엄청나게 확장시키게 된다.

③ 푸코의 일망감시장치(panopticon) 논의

이러한 감시의 확장경향에 일망감시장치(panopticon)라는 은유를 가지고 근대성을 이해하는 시도가 자리잡게 된다.¹³⁴⁾ 이 개념은 감옥, 병원, 수용소의 설계에 대한 제레미 벤담(Jeremy Bentham)의 독창적인 생각으로부터 푸코가 따온 것이다. 이러한 논의는 푸코의 □□감시와 처벌□□¹³⁵⁾을 중심으로 전개되었는바, 우리 학계의 적지 않은 논의가 특히 이러한 일망감시장치의 이미지에 기댄 논지의 전개를 수행하고 있기에 좀 더 구체적으로 살펴볼 필요가 있다.

기본적으로 『감시와 처벌』은 형벌제도에 대한 계보학적 기술이라 할 수 있는데, 푸코는 이를 통해 각 시대의 권력이 어떻게 개인을 특정된 방식으로 통제·관리하는지를 살핀다. 그에 따르면 절대군주제 하에서 형벌은 육체에 고통을 주고 그것을 공개함으로써 군주의 절대 권력을 과시하는 화려한 피의 의식이었다.

푸코는 이러한 처벌제도의 변화가 처벌에 대한 개선으로 이해되기 보다는 더 잘 처벌하기 위한 것이며, 육체에 대한 가혹하고 직접적인 처벌이 ‘사법적 감금’으로 그 형태가 바뀐 것으로 본다. 그리하여 푸

134) 벤담의 일망감시장치에 관한 자세한 설명은 홍성욱, “벤담의 파놉티콘(Panopticon)에서 전자 시놉티콘(Synopticon)까지,” 『한국과학사학회지』 제23권 제1호(2001) 참조.

135) Michel Foucault, *Surveiller et punir: nuisance de la prison*, 오생근 역, 『감시와 처벌: 감옥의 역사』 (나남출판, 1994[1996 print]).

코는 18세기 후반에 감옥제도가 만들어지고 그것이 일반화되면서 보다 조직적이고 체계적으로 규율된 사회가 만들어지는 과정에 주목한다. 그는 감옥제도를 규율적 권력이 행사되는 전형적인 예로 보면서 이런 권력이 사회 전체에 침투해서 현대 사회를 규율적 권력이 편재하는 ‘유편적’ 사회로 만들어간다고 본다.

푸코는 이러한 권력의 메커니즘이 인간의 육체에도 작용한다고 본다. 그리고 권력이 육체를 억압하는 것이 아니라 육체를 특정한 목적에 맞도록 만들어내는 점에 주목한다. 즉 권력은 육체를 길들인다. 그는 이것을 육체에 대한 미시권력(micro pouvoir)이라고 부른다. 규율은 육체에 작용하고 그것을 통해 규율은 개인들을 ‘만든다’. 이것은 개인들을 그 작용 대상으로서 뿐만 아니라 수단으로 간주하는 권력의 특수한 기술이다. 이때 개인들은 권력의 매개자일 뿐 그 주체가 아니다. 권력은 개인들을 억누르거나 금지하지 않고 훈련과 배분의 절차에 의해 그렇게 한다.

푸코는 이러한 육체에 대한 권력의 작용을 통해 사회의 다양한 영역들 작업장, 군대, 감옥, 병원, 학교 등에서 규율이 생산, 수행되는 일정한 방식들에 주목한다. 규율은 개인들을 통제하고, 훈련시키며, 조직하는 기술을 통해 작용한다. 이때 개체의 육체는 경제적으로는 노동력을 지닌 대상이며 정치적으로는 복종할 수 있도록 훈련받는다. 이러한 규율은 개체들을 통제가능한 공간에 배치하고, 활동을 통제하고, 훈련시키며, 개체들을 조직하는 기술을 통해 작용한다.

규율장치는 구속하고 억압하며 대량적 방식으로 피라미드적 권력에 복종시키는 것이 아니라, 갖가지 다양한 기술 세부적 규제, 연습, 훈련, 시간 사용, 평가, 시험, 기록 등 들을 사용한다. 그것은 육체의 미세한 부분에 까지 작용해 육체를 길들여서 가능한 효율을 최대화하기 위해 육체의 동작을 통제한다. 규율적 권력은 강제적 탈취 대신에 육체를 훈련시키는 데 주목한다. 이 권력은 사람들의 힘을 감소시키기

위해서 힘을 묶어 두지는 않는다. 그 힘들을 전반적으로 증가시키고 활용할 수 있도록 한다. 이런 권력은 그 대상을 획일적·대량적으로 예측시키는 것이 아니라 분리하고 분석하고 구분하여 체계화한다. 유동적이고 혼란스럽고 무익한 수많은 육체와 대량적 힘을 개별적 요소들의 다양성으로 만들도록 훈련을 시킨다. 규율은 개인들을 제조한다. 규율적 권력은 과도한 힘을 행사하는 방식이 아니라 계획적이고 영구적인 관리방식으로, 미시적인 방식으로 작동한다.¹³⁶⁾ 이러한 전략의 완성을 위한 전략으로 제시된 것이 바로 일망감시장치라 할 수 있다. 다소 길지만 푸코 자신의 설명을 소개하면 다음과 같다.

벤담의 ‘일망(一望) 감시시설(panopticon)’은 이러한 조합의 건축적 형태이다. 그 원리는 잘 알려져 있다. 주위는 원형의 건물이 에워싸여 있고, 그 중심에는 탑이 하나 있다. 탑에는 원형건물의 안쪽으로 향해 있는 여러 개의 큰 창문들이 뚫려있다. 주위의 건물은 독방들로 나뉘어져 있고, 독방 하나하나에는 건물의 앞면에서부터 뒷면까지 내부의 공간을 모두 차지한다. 독방에는 두 개의 창문이 있는데, 하나는 안쪽을 향하여 탑의 창문에 대응하는 위치에 나 있고, 다른 하나는 바깥쪽에 면해 있어서 이를 통하여 빛이 독방을 구석구석 스며들어 갈 수 있다. 따라서 중앙의 탑 속에는 감시인을 한명 배치하고, 각 독방 안에는 광인이나 병자, 죄수, 노동자, 학생 등 누구든지 한 사람씩 감금할 수 있게 되어 있다. 역광선의 효과를 이용하여 주위 건물의 독방 안에 감금된 사람의 윤곽이 정확하게 빛 속에 떠오르는 모습을 탑에서 파악할 수 있는 것이다. 그것은 바로 개체화되고, 항상 밖의 시선에 노출되어 있는 한 사람의 배우가 연기하고 있는 수많은 무대이자 수많은 감방이다. 일망 원형감시의 이 장치는 끊임없이 대상을 바라볼 수 있고, 즉각적으로 판별할 수 있는, 그러한 공간적 단위들을 구획 정리한다. 요컨대 이곳에서는 지하감옥의 원리가 전도되어 있다.

136) 김호기 편, 『현대 비판사회이론의 흐름』 (도서출판 한울, 2001[2002print]), 227~230면.

아니 오히려 지하감옥의 세 가지 기능 감금하고, 빛을 차단하고, 숨겨 두는 중에서 첫 번째 것만 남겨놓고 뒤의 두 가지를 없애버린 형태이다. 충분한 빛과 감시자의 시선이, 결국 보호의 구실을 하던 어둠의 상태보다 훨씬 수월하게 상대를 포착할 수 있다. 가시성의 상태가 바로 함정인 것이다.

이러한 형태는 무엇보다 소극적인 효과이긴 하지만 ... 저 감금시설 속에 밀집해 있으면서 들끓고 소란스러운 대중의 모습을 보지 않게 해 준다. 사람들은 저마다 감시인이 정면으로 바라볼 수 있는 독방 안에 감금된 채 자기 자리를 지키고 있다. 그러나 양쪽의 벽은 그가 동료들과 접촉하는 것을 차단시킨다. 그는 보여지긴 해도 볼 수는 없다. 그는 정보의 대상이 되긴 해도, 정보소통의 주체가 되지는 못한다. 중앙 탑과 마주하도록 방을 배치함으로써 일종의 축을 형성하는 가시성이 강요되는 반면, 원형건물의 분할된 부분들과 완전히 분리된 독방들은 측면에서의 불가시성을 의미하게 된다. 이러한 불가시성은 질서를 보장해 준다. 감금된 자가 죄인인 경우 음모나, 집단 탈옥의 시도, 출감 후의 새로운 범죄 계획 등 상호간의 나쁜 영향의 염려가 없다. 병자라면 전염의 위험이 없고, 광인이라면 상호 폭력을 행사할 위험도 없으며, 어린이일 경우, 남이 한 숙제를 베끼거나 시끄럽게 굴고, 수다를 떨며, 주의를 산만하게 하는 짓을 방지할 수 있는 것이다. 노동자일 경우에도 구타, 절도, 공모의 위험을 막아주고, 작업의 지연이나 불완전한 마감질, 우발적 사고가 발생할 부주의한 일도 일어나지 않게 한다. 밀집한 군중들, 다양한 교환이 이루어지는 장소, 집단적 효과로서 혼합되는 개인들, 이러한 군중형태가 소멸되고 대신 분리된 개인들의 집합이 들어선다. 간수의 입장에서는 군중 대신에 숫자를 헤아릴 수 있고, 통제가 가능한 다수로 바뀌어진 것이고, 죄수의 입장에서는 격리되고 주시되는 고립된 상태로 대체된 것이다. 이로부터 일망감시장치의 주요한 효과가 생겨난다. 감금된 자는 권력의 자

동적인 기능을 보장해주는 가시성의 지속적이고 의식적 상태로 이끌려 들어간다. 감시작용에 중단이 있더라도 그 효과는 계속되도록 하며, 또한 권력의 완성이 그 행사의 현실성을 점차 약화시켜 가도록 한다. 이러한 건축적 장치는 권력이 행사하는 사람과 상관없는 어떤 권력관계를 창출하고 유지하는 기계 장치가 되도록 해 준다. 요컨대 감금된 자가 그 스스로 그 유지자가 되는 어떤 권력적 상황 속으로 편입되는 것이다. 그러기 위해서는, 갇힌 자가 감시자에 의해서 끊임 없이 감시되는 것으로 아주 충분하기도 하지만, 동시에 아주 불충분하기도 하다. 아주 불충분하다는 점은 중요한 점이 죄수가 감시당하고 있다는 것을 자각해야 하는 사실 때문이고, 아주 충분하다는 것은 죄수가 실제로 감시될 필요가 없기 때문이다. 그 때문에 벤덤은 권력이 가시적이고 확인할 수 없는 것이 되어야 한다는 원칙을 내세웠다. 가시적이란, 감금된 자가 자신을 살펴보고 있는 중앙탑의 높은 형체가 항상 눈앞에 어른거린다는 뜻이다. 또한 확인할 수 없다는 것은 감금된 자가 자신이 현재 주시받고 있는지 어떤지를 결코 알아서는 안 되지만, 자신이 항상 주목될 수 있다는 것을 확신하고 있어야 한다는 뜻이다. 벤덤은 감시자가 탑에 있는지 어떤지를 판단할 수 없도록 하기 위해서 또한 감금자들이 독방에서 어떤 사람의 그림자를 인지하거나, 어떤 역광이라도 포착할 수 없도록 다음과 같은 시설을 설계했다. 즉, 감시하는 중앙홀의 창문에 덧문을 씌울 뿐만 아니라, 내부에는 직각으로 구획되는 몇 개의 칸막이벽을 설치하고, 한 구역에서 다른 구역으로 통과하기 위해서는 출입문이 아니라, 지그재그형 통로를 설치하는 것이다. 왜냐하면 아무리 사소한 소리거나, 어렴풋한 불빛이라도, 혹은 조금 열린 문틈에 스며드는 빛이라도 간수의 존재를 드러낼 수 있기 때문이다. ‘일망 감시장치’는 ‘봄 보임’의 결합을 분리시키는 장치이다. 즉, 주위를 둘러싼 원형의 건물 안에서는 아무 것도 보지 못한 채 완전히 보이기만 하고, 중앙부의 탑 속에서는 모

든 것을 볼 수 있지만 결코 보이지는 않는다.

이것은 권력을 자동적인 것이며, 또한 비개성적인 것으로 만들기 때문에 중요한 장치이다. 그 권력의 근원은 어떤 인격 속에 있는 것이 아니라 신체, 표면, 빛, 시선 등의 신중한 구분 속에, 그리고 내적인 메커니즘이 만들어내는 관계 속에, 개개인들이 포착되는 그러한 장치 속에 존재한다. 그것에 의해 군주가 보다 큰 권력을 부여받게 되는 예식이나 의식, 표지 등은 쓸모 없는 것으로 된다. 비대칭과 불균형, 그리고 차이를 보장해 주는 장치가 있을 뿐이다. 따라서 누가 권력을 행사하느냐는 별로 중요하지 않다. 우연히 걸려든 그 누구라도 이 기계장치를 작동시킬 수 있는 것이다. 따라서 그 관리책임자가 부재중이라면 그의 가족이나 측근, 친구, 내방객, 그리고 하인조차도 그 일을 대신할 수 있다. 마찬가지로 이 장치를 움직이는 동기가 무엇이건 상관없다. ... 이러한 익명적이고 일시적인 관찰자가 많으면 많을수록 감금자는 더욱 간파될 위험과 관찰된다는 불안한 의식이 더욱 증가되게 된다. ‘일망 감시장치’는 아주 다양한 욕망으로부터 권력의 동질적인 효과를 만들어내는 경이로운 기계장치이다.

현실적인 예속화는 허구적인 관계로부터 기계적으로 생겨난다. 따라서 죄인에게는 선행을 광인에게는 안정을, 노동자에게는 노동을, 학생에게는 열성을, 병자에게는 처방의 엄수를 강요하기 위해서 폭력적 수단에 의존할 필요는 없다. 벤담은 일망 감시시설이 그렇게 섬세한 것일 수 있다는 사실에 경탄했다. 쇠창살이나 쇠사슬, 그리고 묵직한 자물쇠도 필요 없는 것이다. 단지 구분을 명확히 하고, 출입구를 잘 배치만 하면 되는 것이다. ... 가시성의 영역에 예속되어 있고 또한 그 사실을 알고 있는 자는 스스로 권력의 강제력을 떠맡아서 자발적으로 자기 자신에게 작용시키도록 한다. 그는 권력관계를 내면화하여 일인이역을 하는 셈이다. 그는 스스로 예속화의 원칙이 된다. 바로 이런 사실 때문에 외부의 권력은 물리적인 무게를 경감할 수 있게 되고

점차 무형적인 것으로 된다. 권력이 한계지점에 가까워질수록 그 효과는 더 지속적이고 심원해지며, 단 한 번에 획득되고, 끊임없이 갱신될 수 있다. 즉 모든 물리적인 충돌을 피하고, 늘 앞서서 결정되는 영원한 승리인 것이다.¹³⁷⁾

푸코에 의하면 페스트 등의 질병에 대응하는 감금시설과는 반대로 일방감시시설은 그 기능이 일반화할 수 있는 모델로 당연히 이해되며 그것은 인간의 일상생활과 권력과의 관계를 규정하는 하나의 방식과 같다고 한다. 벤담은 이 시설을 그 자체로 자족적인 특수한 기구로서 제시하고 있는 듯 하고 사람들은 종종 이 시설을 완벽한 감금의 유토피아적 형태로 생각해 왔지만, 푸코는 이 시설이 일종의 몽상적인 건물로 이해되어서는 안 된다고 한다. 즉 그것은 이상적인 형태로 압축된 어떤 권력 메커니즘의 도식이고 저항이나 충돌 등의 모든 장애를 떠나서 행해지는 그 기능이야말로 단순화된 건축적이고 시각적인 체계를 표현될 수 있기에 사실 그것은 모든 특별한 용도로부터 분리시켜 가동할 수 있고, 또한 그렇게 해야 하는 정치기술의 형태라는 것이다. 푸코에 따르면 그 시설의 적용은 다방면에서 이루어질 수 있는 바, 실제적으로는 어떤 기능에서나(교육, 치료, 생산, 징벌 등) 통합될 수 있다.¹³⁸⁾ 뿐만 아니라 이 장치는 구조적으로 민주적인 성격을 지니게 된다. 다시 푸코의 설명을 직접 살펴본다.

더욱이 이 기계의 설비는 그 자체로 폐쇄되어 있더라도 외부의 요소가 항상 개입할 수 있도록 조립된다. 그 누구든지 중앙탑에 와서 감시기능을 수행할 수 있으며, 그렇게 함으로써 그는 감시가 행해지는 방식을 간파할 수 있음을 우리는 알 수 있었다. 실제로 모든 일방감시기구는 그것이 형무소처럼 아무리 조심스럽게 폐쇄된 경우라 할 지라도, 어렵지 않게 임의적인 동시에 끊임없는 감독의 대상이 될 수

137) Michel Foucault, 위의 책, 295~299면.

138) Michel Foucault, 위의 책, 302~4면.

있을 것이다. 더구나 그러한 감독은 지정된 통제자들 뿐만 아니라 일반인의 입장에서조차 행해질 수 있다. 사회의 어떤 구성원이라도 직접 방문해서 학교나 병원, 공장이나 감옥이 어떻게 돌아가고 있는지 자기 눈으로 확인할 권리를 갖는 것이다. 따라서 일망감시장치에 의한 권력의 강화는 폭정의 상태로 변질될 위험이 없다. 규율의 장치는 민주적으로 통제될 수 있다. 왜냐하면, 그 장치는 “세상에서 가장 큰 재판위원회”로 계속 회부될 것이기 때문이다. 한 명의 감시인이 그저 단 한 번의 눈길로 그렇게 많은 서로 다른 개인들을 관찰할 수 있도록 교묘하게 만들어진 이 일망감시장치는 또한 누구라도 찾아와 최소한의 인원으로 된 감시인을 감시할 수도 있게 되어 있다. 눈으로 보는 그러한 장치가 이전에는 사람들을 몰래 감시하는 일종의 암실 같은 것이었지만, 이제는 권력의 행사가 사회 전체에 의해서 통제될 수 있는 투명한 건물로 된 것이다.

일망 감시의 도식은 지워지거나 혹은 그 특징 중 어느 것도 잃지 않은 채, 사회 전체로 확산될 수밖에 없도록 되어 있다. 그것의 임무는 바로 전체화의 기능을 수행하는 일이다. ... 권력을 계속 정비하고, 그것을 한층 더 경제적이고, 효율적으로 만들고자 하는 것은 권력 자체를 위한 것도 아니고, 위기에 처한 사회의 즉각적인 구원을 위한 것도 아니다. 중요한 것은 사회의 여러 역량을 강화시키는 일이다. 생산을 증대시키고 경제를 발전시키며, 교육의 기회를 넓히고 공중도덕의 수준을 높이는 등 말하자면 증가와 다양함을 가져오는 일이다.¹³⁹⁾

요컨대, 이런 장치는 감옥의 체계에 한정되지 않고 일반적인 감시장치로 다양한 대상에 대해 이용될 수 있으며 그것에 어떠한 내용을 담더라도 같은 효과를 얻을 수 있다. 푸코는 일망감시장치가 권력을 자동적인 것으로 만들고, 비인격적인 것으로 만드는 점에 주목한다. 이러한 권력은 비주체적이다. 이 권력의 근원은 특정한 인물에 있는 것

139) Michel Foucault, 위의 책, 305~6면.

이 아니라 일정한 권력효과를 낳는 장치의 보편적 기능에 있다. 여기에서 누가 권력을 행사하는가는 중요하지 않다. 누구라도 이 장치를 작동시킬 수 있다. 그것은 일정한 목표에 따라서 기능하지만 주체와 무관하게 작용한다. 따라서 권력이나 그 효과가 개별적 주체의 선택이나 결정에서 나온다고 볼 필요는 없다. 그리고 이 장치를 작동시키는 의도나 동기도 이런 기능에 영향을 미치지 않는다. 즉 이 장치의 효과는 권력 주체의 의도와 무관하다.

푸코는 이것을 일종의 권력 실험실로 이해한다. 이것은 일정한 개인들에게 실험을 하고 행동을 변화시키며, 개인을 훈육하는 기계로 이용할 수 있다. 노동자에게 각종 기술을 가르치고 교육적인 실험도 할 수 있다. 이 장치는 인간에 관한 다양한 실험을 할 수 있다. 만약 이것을 통제장치로 이용한다면 관리 책임자는 모든 고용인을 감시하여 바라는 효과를 얻을 수 있을 것이다. 여기에서 개인들은 아무것도 숨길 수 없다.

이것은 모든 것이 투명하게 보이는 끔찍한 세계, 어두움의 보호가 사라진 공간, 이성의 명료함만이 어떠한 그늘도 없이 세계를 밝게 비추는 세계이다. 보이지 않고, 알 수 없는 것의 신비가 완전하게 제거된 세계, 탈주술화되고 합리화된 세계와 같다. 이런 점에서 이 장치는 이성적 권력, 모든 것을 투명하게 인식하려고 하는 계몽주의적 이상을 구체화한 것으로 볼 수 있다. 즉 이 장치에서 놀라운 점은 그것이 권력의 테크놀러지가 보여주는 감시의 극단적 형태이기 때문이라기보다는 그것이 ‘이성적’ 장치라는 점이다. 이성의 빛이 구체화하는 이 장치는 이성이 해방의 선구자이면서도 예속과 지배의 훌륭한 수단이 될 수 있음을 보여준다. 모든 것을 ‘이성’의 시선 아래 두려는 이 장치는 다른 이성적 보충물에 의해서 더욱 이성적인 사회를 만들 수 있다. 이러한 일망감시장치의 함의를 살펴보면, 이성이 비판적 능력을 지닌다고 전제할 때, 이 장치는 역설적으로 가장 이성적으로 사회를

관리하고 효율성을 증대시킨다고 할 수 있다. 이것을 도구적 이성이라고 폄하하고 비판적 이성을 강조할 여지는 의외로 크지 않다. 전면 감시장치와 그것을 이용하는 측은 나쁜 의도를 지닌 것도 아니고, 나쁜 목표를 지향하는 것도 아니다. 어떤 더 나은 의도와 보다 훌륭한 목표를 내세워 그 작용을 저지할 것인가? 일단 이 장치가 사회적 기계에서 그 유용성을 인정받는다면 더 적은 효율을 추구하는 것을 ‘인간적’이라고 하면서 이런 ‘비인간적’ 장치를 제거할 수 있을까? 그 ‘밝은’ 눈을 버리고 불투명함, 어둠 속을 헤맬 것인가. 이성의 태양을 본 자는 동굴 속의 그림자 세계를 물리칠 것이다.¹⁴⁰⁾

④ 일망감시장치와 전자감시

이런 일망감시장치가 현대 기술의 도움으로 전자감시사회라는 형태로 나타난다고 보는 견해들이 적지 않다. 이런 관점이 푸코가 다른 일망감시장치와 어떤 점에서 연결되고 어떤 점에서 다른가는 살펴볼 필요가 있을 것이다.

통합된 전자망 형태를 갖춘 현대의 커뮤니케이션과 정보 테크놀러지는 이러한 권력의 동원체계를 변형, 확장시킬 수 있다. 이른바 전자망사회, 전자망도시의 루프 안테나와 회로, 전자망을 염두에 둔다면 사회전체에서 일어나는 행동들을 ‘중앙집중적’이고 은밀하게 조사, 관찰, 감시, 기록할 수 있는 테크놀러지가 구축될 수 있다. 개인들은 (개별적으로) 전산화된 감시자들에게 보이고 인식될 수 있는 존재가 된다. 개인은 전면감시장치에서처럼 ‘감시대상일 뿐 커뮤니케이션의 주체가 아니고’ 그들은 ‘보여질 뿐 볼 수 없다.’

또한 전자망 사회는 개별화되고 영구적인 문서를 이용하는 체계이다. 관찰되고 조사받는 개인에 관한 정보가 계속 기록되고 파일에 저장된다. 개인들은 이런 기술들에 의해 보여지고 알려진다. 전자망은

140) 김호기 편, 『현대 비판사회이론의 흐름』 (도서출판 한울, 2001[2002print]), 242~3, 247면.

원형감옥 같은 건축물의 공간적이고 시간적인 제약을 극복하여, 미세한 거미줄과 같은 전면감시장치의 꿈을 보다 쉽고 더 효과적으로 실현시킬 수 있다. 주체에 대한 일방적이고 전면적인 감시라는 원리는 서류철로 구체화된다. 개인에 관한 꼼꼼한 기록이 담긴 서류철에서 개인들은 전면적인 기록대상으로 바뀐다. 통신망과 그것이 산출하는 데이터베이스는 벽과 창문, 망루나 감시자가 없는 전면감시장치를 이룬다. 개인들은 사회보장카드, 운전면허증, 신용카드, 도서관 출입증 등을 언제나 소지하고 다니면서 지속적으로 사용한다. 모든 거래는 데이터베이스에 기록되고 부호화되고 저장된다. 개인들 스스로가 데이터베이스의 내용을 메운다. 그들은 정보의 원천이자 정보의 기록자이다. 그렇지만 전자망 사회에서 모든 것을 알고 모든 것을 볼 수 있는 유일한 감시자가 있거나 있을 수 있다고 주장할 필요는 없다.

이런 전자감시 사회가 과연 푸코의 전면감시장치의 발전된 형태라고 할 수 있는가? 가장 문제가 되는 점은 이런 논의가 푸코의 전면감시장치의 ‘완벽한’ 감시와 ‘부드러운’ 작용을 받아들이면서도 근대 권력의 주요한 특징인 중심 없는 권력, 주체의 의지로부터 독립된 작용 등을 무시한 채 전통적인 권력관을 그대로 이어받고 있다는 점이다. 전통적 관점을 권력을 그것을 소유한 자가 권력 대상의 의지에 반하여 자기의 강제력을 행사한다고 보면서, 권력을 그것을 지닌 자가 소유한 실체로 보고 그의 의도에 따라 행사되는 힘으로 본다. 이것을 거의 그대로 이어받은 채 현대적 장치를 덧붙인 틀은 현대 사회의 권력작용방식을 어느 정도 보여주지만, 이는 푸코가 논의한 미시권력들의 작용과는 다른 것이다. 즉 이런 전자감시방식은 전통적인 권력자나 권력의 중앙집중체가 단지 새로운 기술로 보다 쉽고 효과적으로 권력을 장악하고 행사한다고 보므로, 종래의 권력관을 조금도 바꾸지 않고서도 얼마든지 그 작용을 설명할 수 있고, 그 모든 작용을 최고

권력자나 권력 중심의 보다 간교하고 은밀한 의도를 실현하는 것으로 볼 수 있다. 결국 이런 지적은 전자감시사회가 푸코의 전면감시장치와 무관하다고 보는 것이 아니라, 그것을 이해하는 방식이 너무 기계적이어서 푸코의 새로운 권력 분석틀 없이도 충분히 설명될 수 있는 점에서 낡은 관점과 새로운 기법의 절충적인 틀에 머물러 있음을 보여주려는 것이다. 결국 푸코의 분석틀은 근대 권력의 성격을 주체 중심의 틀이나 주체가 소유하거나 양도하거나 빼앗기는 어떤 실체가 아니며, 그 작용하는 방식이 금지와 억압에 중점을 둔 부정적인 것이 아니라고 본다. 이러한 푸코의 분석틀에 주목함으로써, 전통적인 관점이 은폐하는 근대 권력의 작용을 설명할 수 있을 것이다.¹⁴¹⁾

(3) 경제학적 접근

경제학에 있어서 정보는 원론적인 중요성을 가진다. 즉 완전경쟁시장의 성립요건 가운데 “시장에 참여하는 모든 경제주체가 완전한 정보를 갖고 있어야 한다”¹⁴²⁾는 요건이 포함되어 있다는 점에서 이러한 측면을 확인할 수 있고, 비대칭적 정보상황에서의 경제주체의 의사결정에 관한 논의에서도 정보의 중요성에 대한 경제학적 인식을 확인할 수 있다. 여기에서는 보다 구체적인 차원에서 기업운영상에 있어서의 정보의 의미와 프라이버시에 대한 법경제학적 분석을 간단히 살펴보기로 한다.

1) 정보의 기업운영상의 의미

기든스는 자본주의적 이윤추구가 담당하는 역할에 주목하면서 “자본주의 기업에서 감시가 관리에 대한 열쇠”라고 지적하고 있다. 한편

141) 김호기 편, 위의 책, 248~50면.

142) 이준구·이창용, 『경제학원론』 (법문사, 2005), 162면.

에드워드 쉘스(Edward Shills)는 사생활 침해자 명단 속에 자본주의 기업을 포함시키면서, 사실 감시의 발달과정에서 근대적 관리의 역할에 주목한 사람은 바로 기업이 사람들의 생활에 대한 주요한 침입자였다고 주장한다. 기본적으로 20세기에 들어와서 나타난 현상이라고 할 수 있는 관리는 본질적으로 정보노동이라는 견해를 입증해 주는 많은 증거가 있다. 이러한 노동은 자본의 회수율을 최대화하는 전략의 수립과 이행 업무를 더 잘 수행하기 위하여 기업의 활동영역을 철저하게 감시하는 것을 주요 목적으로 한다. 여기서 주목해야 할 것은 생산과정에 대한 감시는 초기 대인 감독시대 이래 광범하게 확장되어 왔다는 점이다. 감시에서 이루어진 최근의 혁신으로는 컴퓨터수치제어(CNC), 로봇 그리고 무엇보다 시작시간, 생산율, 출석여부, 질적 관리 등을 자동적으로 개별화시켜 기록할 수 있는 컴퓨터 단말기를 들 수 있다.

근대적 관리는 다른 대부분의 활동의 전제가 되는 생산에 대하여 매우 자세한 감시를 하지만 오늘날의 관리의 대상은 노동과정보다 훨씬 더 포괄적이다. 이것을 이해하는 데 중심적인 것은 기업 자본주의 (corporate capitalism)가 20세기에 세 가지 주요한 방식으로 확장되어 왔다는 점이다. 첫째는 기업이 공간적으로 확장되어 전형적인 선도적 기업은 적어도 전국적으로 그리고 대개는 초국가적으로 확산되어 있다. 둘째, 기업은 적은 수의 더 큰 기업으로 통합된다.

셋째, 흔히 간과되는 것이지만, 기업은 사회의 영역으로 더 깊이 파고들고 있다는 것인데, 이것은 거의 모든 지역에서 쉽게 눈에 떨 수 있는 판매망을 개발하고 예전에는 자신 또는 이웃사람들이 생산하였던 재화와 용역을 구매할 수 있는 것으로 대체시키는 것을 통해 진행된다. 물론 이러한 모든 것에는 나쁜 측면이 있지만, 이러한 감시가 현대 기업에 가지고 있는 실제적인 유용성 역시 언급될 필요가 있다.

즉 소비자의 소비성향, 의류 및 식품에 대한 기호, 선호하는 구매위치 등에 대한 개별적인 정보들은 기업의 판매전략을 매우 향상시켜 줄 수 있는 감시의 유형이다.¹⁴³⁾

2) 프라이버시의 경제적 분석¹⁴⁴⁾

미국의 연방헌법 증보 제4조는 개인, 가정, 문서의 안전에 대한 인간의 권리를 보장하고 있다. 그리고 불합리한 수색들과 압수를 금지하고 포괄적인 영장(즉, 수색 및 압수 대상인 사람과 사물을 특정하지 아니한 영장)발급을 금하고 있다.

가장 좁은 의미로 보면 연방헌법 증보 제4조는 단지 연방관리들이 개인과 재산의 불법 침입을 하지 못하도록 보호하는 것으로 생각될 수 있다(그리고 이 조항은 연방헌법 증보 제14조의 적법절차의 조항을 따라야 하는 주 정부에도 적용될 수 있다고 판결이 이루어진 이후에도 주 정부의 관리에게도 해당된다). 이것은 비록 제한적이지만 매우 중요한 사생활의 보호가 될 수 있다. 만약 경찰이 당신의 집에 와서 수색하면서 당신이 하고 있는 것을 방해한다면 경찰이 당신에 대해 어떠한 정보를 얻지 못하더라도 그것은 사생활 침해라고 할 수 있다. 이는 원하지 않은 전화 판매 권유가 사생활의 침해인 것과 동일한 의미를 가진다. 하지만 경찰이 당신의 전화를 도청한다면 이는 다른 의미의 사생활 침해가 된다. 이로 인하여 당신의 고요함이나 정신 집중이 깨뜨려지지 않아서 전화도청은 사생활의 방해라고 할 수 없지만 은밀함에 대한 사생활 침해가 된다. 거래의 비밀이 없다면 이러한 의미의 사생활 이 보호받을 가치가 있는지에 대한 의문이 없지는 않지만, 전화통화에서 최소한의 은밀함이 보장되어야 한다는 주장이 있는데, 은밀함이 보장되지 않으면 사람들은 의사소통방법을 효율성은

143) Frank Webster, 앞의 책, 124~7면.

144) Richard A. Posner, *Economic Analysis of Law Part 2*, 정기화 역, 『법경제학(하)』 (자유기업원, 2004), 449~51면.

떨어지지만 보다 안전한 수단으로 바뀌게 되어 비용이 발생한다는 것이다. 불법인 의사소통이 이루어지고 있었다면 전화 도청은 손실을 초래하는 것이 아니라 이익을 가져다 줄 수 있다. 그러나 의사소통이 합법적이었다면 손실이 발생하며, 이것은 Katz 소송의 판결에 대한 경제학적 타당성을 제공한다. 판결에 따르면 도청은 압수의 한 형태로 연방헌법 증보 제4조의 적용범위에 있으며 따라서 도청이 비합리적이 라면(이것은 다음에 논의하듯이 비용이 이익을 초과하는 경우이다) 불법이다. 수색과 압수(체포를 포함)로 사회적 비용이 발생한다고 해서 그것을 금지하는 것이 타당하다는 것은 물론 아니다. 사회적 비용이 사회적 이익을 초과하면 경찰이 수색을 하지 못하도록 규제하자는 것이다. 일반적으로는 핸드공식을 이용하여 이 문제를 구성해 볼 수 있다.¹⁴⁵⁾ 수색에 따른 사생활 손실비용(B)이 수색하지 않았을 때, 수색 대상의 유죄를 입증하지 못할 확률(P)에 이로 인한 사회적 비용(L)을 곱한 것보다 적다면 수색(압수)는 합리적이다. P는 두 가지로 구성되어 있다. 하나는 수색으로 경찰에게 가치 있는 어떤 것(아마 소송근거)이 드러날 가능성이며, 다른 하나는 드러난 그 어떤 것이 유죄 입증에 필수 불가결한 것일 가능성이다. 그러므로 수색을 하지 않았더라도 동일한 증거를 얻을 수 있다면 (그리고 더 낮은 B에서 그럴 수 있다면) 수색의 가치는 적을 것이다. 수색으로 인한 침해의 정도가 커서 B가 커질수록, 찾고자 하는 증거의 필수 불가결함(P)이 더 크거나 수사대상 범죄의 중함(L)이 커야 B를 상쇄할 수 있다.

제 4 절 소 결

지금까지 개인정보보호에 관련된 법학계의 기존 논의들을 간략히 검토해 보고, 논의의 이론적 배경들을 살펴본 후, 법제의 적용범위의

145) 핸드 공식은 과실판단을 위해 핸드(Learned Hand)에 의해 정립된 공식으로, 사고확률을 P, 손해를 L, 부담을 B라고 하면 과실인정은 $B < P * L$ 일 때 성립한다.

확정을 위한 기본적인 개념들에 대한 분석을 시도해 보았다. 재차 강조하지만, 입법평가의 지표로서의 체계성 및 이해가능성을 염두에 두는 가운데 이러한 문제의 해결을 위해선 기본적인 개념들이 사용되는 맥락의 분석을 통한 개념의 외연을 확정하는 작업이 수행될 필요성이 크다고 할 것이며, 개인정보의 범위에 대한 면밀한 분석을 통해서, 보호가치 혹은 경제적 가치에 따라 유형별로 분류하고 인격적 속성과의 연관성에 비추어 개인정보를 개별적으로 논의하려는 시도는 전통적 의미에서 제기되어 온 프라이버시와의 관련에만 경도되지 아니하고 경제적 보호가치가 있는 정보의 유통을 규범적으로 정립하려는 노력을 수행해야 할 것이다.

이는 최적의 개인정보보호를 통한 자유로운 정보유통으로 계약자유와 계약정의를 실현하려는 실천적 이념인 것이다. 그리고 이러한 논의는 ‘고객에 관한 개인정보, 즉 고객정보가 기업경영의 핵심적인 수단인 하나로 떠오르고 나아가 그 자체가 기업의 가치를 평가하는 중요한 자산의 하나로 평가되고 있는 디지털 경제시대에 있어서는 개인정보를 효과적으로 보호하는 것 못지않게 기업들이 인터넷 이용자들의 개인정보를 일정한 조건 하에서 자유롭게 수집하고 이를 가공하여 활용할 수 있도록 보장하는 것도 국가전체적인 산업발전이라는 측면에서 어느 정도 필요한 것’이라는 현실적 관점에 대해 개인정보에 관한 구조적 조망을 가능케 하는 법리적 논거를 제시할 뿐만 아니라 적정수준의 개인정보 유통을 유지할 수 있는 정책적 유인으로 작용한다는 점에서 커다란 함의를 발견할 수 있을 것이다.

제 4 장 개인정보보호에 관한 헌법이론적 분석

제 1 절 개인정보보호의 헌법적 의의

(1) 국가나 타인에 의한 감시는 실제로 이루어지지 않는다고 하더라도 그 감시의 가능성을 인식하는 것만으로 개인의 존엄성과 자율성을 크게 위축시킬 수 있다. 그리고 개인이 자신에 관한 정보이지만 그 처리의 상황이나 내용에 대해 전혀 인식하지 못하거나 혹은 실령 짐작하거나 인식한다고 하더라도 그 처리과정에 관여하거나 통제할 가능성이 차단되어 있다면, 개인은 한없는 무기력증과 소외감을 느끼게 될 것이다. 다른 한편으로, 정보사회에서 개인은 자신의 실존인격 외에 사이버스페이스에 또 하나의 가상인격을 가지게 되는데, 가상인격이 실존인격을 규정짓게 될 경우 개인의 사회적 정체성은 디지털화된 개인정보에 의해 좌우될 위험에 처하게 된다. 가령 잘못된 개인정보에 의하여 개인의 사회적 정체성이 왜곡되는 경우 그 개인이 입게 되는 피해는 예측할 수 없을 정도로 그 파장이 크다. 범죄자로 오인되어 체포된다거나 신용거래불량자 명단에 이름이 잘못 기록된다거나 하는 경우 신체의 자유의 침해나 경제생활상의 피해는 말할 것도 없고 고용에 있어서의 차별, 복지수혜의 기회상실, 공동체생활에 있어서 명예의 손상 등 그 피해는 지대한 것이다.¹⁴⁶⁾ 이러한 점에서 오늘날 개인정보의 처리상황은 단순한 명예훼손이나 재산적 피해와 같은 법률상의 이익을 침해를 가져오는 정도에 그치지 아니하고 인격권 내지 프라이버시권, 재산권, 교육권, 사회보장수급권 등과 같은 기본권의 침해로까지 이어진다고 할 수 있다. 따라서 오늘날 개인에 관한 정보의 대량적 수집과 보유 및 용이한 결합을 적절하게 억제함으로써 막강한 정보권력의 남용에 따른 개인의 비인격화 내지 소외화를 막아야 한

146) 성낙인 외, 『개인정보보호를 위한 정책방안 연구』(정보통신부, 1999), 27면 참조.

다는 데 그 어떤 이견도 있을 수 없으며, 그러한 과제는 오늘날 대다수의 국가에서 기본적 인권의 보장이라는 관점에서 파악되고 있다.¹⁴⁷⁾

(2) ‘개인정보보호’라는 용어는 개인정보관리자나 개인정보처리자 등의 입장 내지 개인정보를 둘러싼 법질서를 설계하고 적용·집행하는 측의 관점을 반영한 것이라 할 수 있다. ‘보호’라는 말이 대체로 그러하듯이 개인정보의 ‘보호’에는 다분히 시혜적·후견적 의미가 함축되어 있다고 할 수 있다. 개인정보보호를 ‘하는 쪽’과 ‘받는 쪽’을 생각해보면, 개인정보는 보호를 ‘해주는’ 혹은 ‘해주어야 하는’ 대상이 되고 개인정보보호의 이니셔티브는 개인정보정책에 관여하는 국가기관이나 공공기관 혹은 당해 개인정보를 다루는 민간인 등에게 넘어갈 수밖에 없다. 따라서 당해 정보의 주체는 개인정보보호의 대상이 되고, 경우에 따라서는 자신에 관한 정보에서 파생하는 이익마저 타인의 처분에 따라 좌우되는 것을 수인해야 하는 상황에 처할 수도 있다. 오늘날 자신에 관한 정보를 통제할 수 있는 법적 지위는 우리 헌법상 인격권, 사생활권 등의 기본권으로서 승인되고 있다고 할 수 있다. 그렇다면 개인정보의 보호는 개인정보의 주체의 시각에서 볼 때 자신에 관한 개인정보의 생성, 유통, 소멸에 관여할 수 있는 권리, 즉 ‘개인정보자기결정권’으로서 보장되어야 할 문제라고 해야 한다. 그리고 이것은 개인정보자기결정권이 헌법상 기본권보장의 체계 속에서 논의될 필요가 있음을 의미한다.

제 2 절 개인정보보호와 개인정보자기결정권의 보장

1. 개인정보자기결정권의 의의

(1) 개인정보자기결정권은 “개인이 자신에 관한 정보의 흐름을 파악하여 통제할 수 있는 권리”로 간단히 정의할 수 있다. 이는 자신에 관

147) 권건보, 『개인정보보호와 자기정보통제권』 (경인문화사, 2005), 2-6면 참조.

한 정보의 생성과 유통, 소멸 등에 주도적으로 관여할 법적 지위를 보장하는 것이라고 할 수 있다. 독일 연방헌법재판소는 정보자기결정권을 “원칙적으로 자기의 개인정보의 공개와 이용에 관하여 스스로 결정할 각자의 권한”으로 정의하고 있다.¹⁴⁸⁾ 용어상으로는 차이가 있지만, 개인에 관한 정보에 있어서 정보주체의 자율적 관여권한을 인정하는 기본적인 정신은 동일한 것이라 할 수 있다.

(2) 개인정보자기결정권은 소극적 측면뿐만 아니라 적극적 측면도 아울러 가진다. 개인정보의 수집·추적·보관·제공 등을 거부한다든가 혹은 본인의 의사에 반하거나 잘못된 개인정보의 보유나 처리에 대하여 정정이나 폐기 또는 손해배상을 청구한다든가 하는 것은 개인정보자기결정권의 소극적 측면이라 할 수 있다. 반면에 자신에 관한 정보의 보유상황을 확인하기 위하여 자료의 열람이나 조사를 청구하거나 혹은 원하는 대상에게 그 정보를 스스로 공개하거나 제공한다든가 하는 것은 개인정보자기결정권의 적극적 측면이라 할 수 있다.

개인정보자기결정권은 궁극적으로 개인의 의사소통능력을 보장함을 목적으로 한다. 의사소통은 모든 사회에 있어 본질적인 것이다. 상호간의 의사소통은 민주사회에 있어 필수적인 것이다. 따라서 상호간의 의사소통을 확실히 하기 위하여, 특히 공동체를 한정하는 경제적·사회적·문화적·정치적 생활의 영역에서 개인은 특별한 의사소통권을 가진다. 개별적 의사소통 기본권에는 표현의 자유(제21조), 통신의 비밀(제18조), 청원권(제26조) 등이 있으며, 집단적 의사소통권에는 집회 및 결사의 자유(제21조)가 있다. 하지만 민주적 대화나 기타의 사회적 것으로 중요한 의사소통 및 이익대표의 개입을 통한 사회적 절차의 역동적 규제란 것도 확일적 질서로부터의 회피가 가능할 때에만 생각될 수 있는 것이다. 그러한 종류의 절차는 의사소통의 침해와 정보의 침해를 통하여 영향을 미칠 수 있고 방해를 받을 수 있다. 만약 개인의

148) BVerfGE 65, 1 (Leitsatz 1).

회피적 태도가 항상 기록되고 정보로서 지속적으로 저장되고 이용되며 전달되는지 여부를 확신하지 못하면 은밀하게 자신의 태도를 견지하려고 할 것이다. 가령 집회나 시민발안에 참여하는 것이 혹시 당국에 기록된다는 사실과 그것을 통하여 그에게 위험이 발생할 수 있다는 사실을 생각하게 된다면 개인은 자신의 관련 기본권의 행사를 포기할 것임에 분명하다.¹⁴⁹⁾

“자기와 관련된 정보들 가운데 어떠한 것이 특정한 사회영역에서 알려지는지 충분하고도 확실하게 알 수 없는 사람, 의사소통의 상대방이 무엇을 알고 있는지 충분히 판단할 수 없는 사람은 독자적인 자기결정에 따라 계획하고 결정할 자유를 본질적으로 방해받게 될 것이다. (...) 부당한 정보처리에 의한 자기결정권의 침해는 개개인의 인격발현의 기회는 물론이고 공공복리까지도 저해할 수 있다. 이러한 자기결정은 그 시민들의 행동과 협력 능력에 바탕을 두고 있는 자유민주적 공동체의 기본적인 기능조건이기 때문이다.”¹⁵⁰⁾ 이러한 점에서 오늘날 국가가 자신에 관한 어떤 정보를 조사, 처리해도 되는지를 결정, 통제할 수 있는 권리를 개인에게 부여하는 것은 반드시 필요하다.

그러나 개인정보자기결정권은 단지 개인에게만 자신의 사적인 개인의 복리의 촉진을 보장하여야 하는 것은 아니다. 오히려 그것은 “그 시민의 행위가능성과 협력가능성에 기초하는 자유민주주의적 공동체의 기초적 기능조건”도 된다.¹⁵¹⁾ 개인이 참여하는 의사소통을 스스로 영향을 미칠 기회를 가지는 한도에서는 자신의 사회적 그리고 정치적 환경에도 영향을 미칠 수 있는 것이다. 개인은 자신의 개인적인 자기결정을 단지 그가 그 속에서 움직이는 법질서와 사회질서가 이것을 허용하는 정도에서만 실현할 수 있다. 사회질서가 그의 구성원이 주

149) BVerfG NJW 1984, 422.

150) BVerfGE 65, 1 (43).

151) BVerfGE 65, 45 = NJW 1984, 422.

체로서 거기에 참여한다는 사실을 중요하게 여긴다면, 개인적인 관심사도 공익 안에서 보호되는 의사소통질서는 확정되어야 한다. 이러한 점에서 개인정보자기결정권도 무제한적으로 보장되는 것은 아니다. 개개인은 자신의 정보에 관한 절대적·무제한적 지배를 의미하는 어떤 권리를 가지는 것은 아니다. 오히려 개개인은 사회공동체내에서 발현되고 의사소통에 의존하는 인격인 것이다.¹⁵²⁾

(3) 이러한 개인정보자기결정권은 일반적으로 배제청구권, 열람청구권, 정정·차단·말소·파기청구권 등으로 나타날 수도 있다.¹⁵³⁾ 하지만 개인정보자기결정권이 단순히 타인에 의한 개인정보의 취급을 억제하는 이외에도 개인이 자신에 관한 정보의 유통을 적극적으로 형성하고 조절한다는 측면에서 볼 때, 개인정보자기결정권은 개인정보의 취급과정에 따라 수집에 대한 통제권, 보유에 대한 통제권, 이용에 대한 통제권 등으로 나누어볼 수 있다.¹⁵⁴⁾

2. 개인정보자기결정권의 헌법적 근거

(1) 비교법적 고찰

프라이버시를 헌법상 보장되는 기본권으로서 명문화하고 있는 경우에는 1961년의 터키헌법 제15조, 1971년의 이집트헌법 제57조, 1975년의 포르투갈헌법 제33조 내지 제35조, 1978년의 스페인헌법 제18조 등이 있다.¹⁵⁵⁾ 우리나라도 1980년의 헌법에서 사생활의 비밀과 자유를 기본권의 하나로 규정하였고, 현행헌법에서도 이를 그대로 이어받고 있다. 그런데 단순한 프라이버시의 보호에서 그치지 않고 헌법에 특

152) BVerfGE 65, 1 (43-44).

153) 권영성, 『헌법학원론』(법문사, 2008), 455-456면; 서울고등법원 1996. 8. 20. 선고 95나44148 판결. 하집 96(2)277 등 참조.

154) 권건보, 앞의 책, 116-117면.

155) 권영성, 『신고헌법학원론』(법문사, 1981), 337면 참조.

별히 개인정보의 보호를 위한 규정을 두고 있는 나라도 간간이 눈에 띈다. 포르투갈, 스페인, 네덜란드, 헝가리, 러시아 등이 대표적이라 할 수 있는데, 이들 국가의 헌법 가운데 관련규정의 내용을 살펴보면 다음과 같다.

1975년의 포르투갈헌법은 제33조에서 개인의 인격권, 명예권, 프라이버시권을 보장하면서(제1항), “자신과 가족에 관한 정보를 남용하거나 인간존엄에 반하여 이용하는 것을 효과적으로 방지하기 위하여 법률로써 정한다.”(제2항)고 규정하고 있다. 나아가 제35조에서는 데이터 처리의 이용과 관련하여 “모든 시민은 자신에 관한 데이터뱅크의 내용과 그것이 목적으로 하는 용도에 관하여 설명을 들을 권리를 가진다. 또한 설명된 내용을 정정하고 경신할 것을 요구할 권리가 있다.”(제1항), “통계의 목적으로 식별할 수 없는 데이터를 처리하는 경우를 제외하고는 어떠한 개인의 정치적 신념, 종교적 믿음이나 사생활에 관한 정보도 처리해서는 안 된다.”(제2항), “시민들에게 다목적의 국민 식별번호가 부여되어서는 안 된다.”(제3항)고 규정하고 있다.¹⁵⁶⁾

1978년의 스페인헌법도 제18조에서 개인의 명예권·프라이버시권·인격권(제1항) 및 우편·전보·전화통화의 비밀(제3항)을 보호하는 한편으로, “개인의 명예권과 프라이버시권 및 그러한 권리들의 온전한 행사를 보장하기 위하여 정보의 이용을 법률로써 제한한다.”고 규정하고 있다(제4항).¹⁵⁷⁾

그리고 1983년의 네덜란드헌법은 제10조에서 누구든지 프라이버시권을 가진다고 선언하면서(제1항), 나아가 개인데이터의 기록과 유통(제2항) 및 설명권과 정정권(제3항)에 대해서도 규정하고 있다.¹⁵⁸⁾ 1989년의 헝가리헌법도 제59조에서 “헝가리공화국에서는 누구든지 자신의

156) James Michael, *Privacy and Human Rights*, Hampshire: Dartmouth, 1994, pp. 115-116.

157) *Ibid.*, p. 119; http://www.oefre.unibe.ch/law/icl/sp00000_.html.

158) http://www.oefre.unibe.ch/law/icl/n100000_.html

개인적 데이터를 보호받을 권리를 가진다.”고 규정하고, 제61조에서는 “누구든지 공적 데이터에 접근할 권리와 그것을 전파할 권리를 가진다.”고 규정하고 있다.¹⁵⁹⁾

1993년의 러시아헌법도 제24조에서 본인의 동의 없이 개인의 생활에 관한 정보를 유출하거나 사용, 보관, 수집하는 것을 원칙적으로 금지하면서(제1항), 국민의 권리와 자유에 직접적으로 영향을 미칠 수 있는 자료 등에 대한 접근을 보장하도록 규정하고 있다(제2항).¹⁶⁰⁾

한편, 국제연합(UN)의 시민적·정치적 권리에 관한 규약은 제17조에서 “누구든지 그 사사·가정 또는 통신에 대한 자의적·불법적 간섭이나 그 명예와 신용에 대한 불법적인 침해를 받지 아니한다. 모든 사람은 그와 같은 간섭이나 침해에 대해서 법률의 보호를 받을 권리를 가진다.”고 규정하고 있다.

반면에 개인정보의 보호에 관해서는 커녕 프라이버시에 대한 헌법규정조차 두고 있지 않는 나라들이 오히려 많다. 대표적으로 미국, 독일, 일본 등이 이러한 국가들에 속한다고 할 수 있다. 미국의 경우 연방헌법은 개인의 프라이버시보호에 관한 어떤 일반적 기본권을 규정하고 있지 않으며, 사적 영역의 보호를 위한 개별적 규정도 많지 않다. 그래서 미국에서는 법원의 판례를 통하여 그 흠결을 보완해 왔다. 독일의 기본법에도 프라이버시의 보호에 관한 명문의 규정이 없으나, 학설과 판례는 기본법 제2조 제1항에서 말하는 인격권 속에 프라이버시의 권리가 포함되어 있다고 본다. 일본의 경우도 역시 프라이버시에 관한 명문의 규정이 없지만, 학설과 판례는 헌법 제13조의 생명·자유 및 행복추구권에서 프라이버시권의 근거를 찾을 수 있다고 본다.¹⁶¹⁾

159) James Michael, *op. cit.*, p. 124.

160) http://www.oefre.unibe.ch/law/icl/rs00000_.html

161) 榎原猛, 『プライバシー權の總合的研究』(京都: 法律文化社, 1998), 65-71면 등 참조.

(2) 우리 헌법상의 근거

1) 개인정보자기결정권에 대해서는 그 성격, 구체적 내용, 보장의 정도 등과 관련하여 구구한 의견들이 있을 수 있다. 이것은 일차적으로 우리의 헌법하에서 인격권이나 행복추구권, 사생활의 비밀과 자유, 헌법에 열거되지 아니한 기본권 등이 함께 규정되어 있음으로 인하여 기본권규정의 체계적 이해가 극도로 어렵게 되어 있다는 데서 연유하는 것으로 보인다. 하지만 개인정보자기결정권의 속성상 복합적인 측면이 혼재하고 있다는 점도 이를 우리 헌법의 체계 속에서 자리매김을 한다는 것이 결코 용이하지 않게 하는 이유가 되고 있다. 개인정보자기결정권은 자신에 관한 정보의 흐름을 자율적으로 형성할 수 있도록 한다는 점에서 기본적으로 우리 헌법상 사생활의 자유와 관련된다 하고 하지 않을 수 없다. 물론 개인이 단순한 정보의 객체로 전락하는 것을 방지한다는 점에서는 인격권으로서의 가치도 갖는다고 할 수 있다. 그리고 자신에 관한 정보에 접근하여 자신의 의사를 반영할 수 있다는 점에서 부분적으로 정보보유자에 대한 감시나 통제로서의 의미도 가지는 것도 분명하다. 나아가 개인정보를 유형적·무형적 이익과 교환할 것인지 여부를 자율적으로 결정할 수 있다는 것은 재산권의 한 측면이 될 수도 있는 것이다.

하지만 분명한 것은 이러한 속성과 그 헌법적 근거를 어디에서 도출할 것인가는 별개의 문제라는 점이다. 그리고 우리가 여기서 한 가지 더 유의해야 할 것은 개인정보자기결정권이 문제 삼는 것은 보호받아야 할 개인정보의 내용이 아니라, 그 정보의 수집, 축적, 보관, 전달, 결합 등의 과정에 대하여 정보주체가 어느 정도 관여할 수 있는가 하는 점이다.

2) 사생활의 비밀과 자유는 자신에 관한 정보를 타인에게 알릴지 말지 그리고 자신의 삶의 스타일에 대한 타인의 충고를 받아들일지

말지 원칙적으로 스스로 결정할 수 있는 법적 능력을 전제로 하는 기본권이라 할 수 있다. 이로써 한편으로 외부로부터의 관심이나 간섭으로부터 자유로운 상태를 보장하고, 다른 한편으로는 공동체적 삶에의 편입 내지 참여의 기회를 제공한다. 특히 사생활의 자유는 공권력에 의한 부당한 간섭으로부터 개인의 자유영역을 보호하며, 나아가 공동체 속에서 자유로운 협력과 형성을 위한 전제조건들과 가능성들을 보호한다. 이러한 점에서 자신에 관한 정보를 형성·관리·처분하는 데 관여할 수 있는 개인의 권리는 기본적으로 사생활의 유지와 형성을 자율적으로 결정 내지 통제할 수 있는 사생활의 자유에서 나온다고 할 수 있다.¹⁶²⁾ 하지만 자신의 내밀한 사항을 남이 알게 할지 말지를 결정하는 권리도 개인정보자기결정권에 포함되는 것으로 보아야 하기 때문에 사생활의 비밀을 제쳐두고 사생활의 자유에서만 개인정보자기결정권의 근거를 찾는 것은 옳지 않다고 본다.

비록 자신에 관한 정보가 모두 사적 영역에 속한다고 할 수는 없다 하더라도, 그러한 정보를 어떻게 처분할 것인지를 결정하는 문제는 사생활의 비밀과 자유에 포함되는 내용으로 이해하여야 한다. 가사 개인정보의 침해로 인해 인격적 가치가 훼손된다고 하더라도 혹은 개인정보의 자율적 통제를 통해 자신의 행복감이 고양된다고 하더라도, 그것이 곧 인격권이나 행복추구권에서 개인정보자기결정권의 근거를 구해야 하는 이유가 될 수는 없는 것이다. 한편, 사생활의 유지와 형성에 관한 한 헌법 제17조는 어디까지나 헌법 제10조에 대해 특별법적 지위를 가진다고 보아야 할 것이다. 따라서 개인정보자기결정권의 법적 근거는 헌법 제10조보다 제17조에서 먼저 찾아야 할 것으로 본다.

사생활의 비밀과 자유가 자유권적 기본권이라는 이유로 소극적 권리로서만 이해되는 것은 옳지 않다고 생각한다. 오늘날 공권력의 침

162) 김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 『공법연구』 29집 3호(한국공법학회, 2001), 98면 참조.

해로부터 방어할 수 있는 자유권에 있어서도 침해상태의 배제를 요구하는 소극적 청구권뿐만 아니라, 잠재적 침해요인의 금지 내지 침해의 예방을 위한 조치를 요구하는 적극적 청구권까지도 포함되는 것으로 이해해야 할 경우가 있다.¹⁶³⁾ 특히 개인정보보호와 관련하여서는 자신에 관한 정보에 접근하여 그것이 적절히 그리고 정확히 보유 또는 처리되고 있는지 확인하고, 그 결과 사실과 다른 부분이 있거나 잘못 관리되고 있는 경우 그것을 정정하거나 삭제할 것을 청구할 수 있는 권리가 보장되고 있다. 그런데 이러한 정보주체의 청구권은 개인정보자기결정권의 침해를 제거하거나 그것을 예방하는 차원에서 보장되는 권리라고 할 수 있다. 그것이 청구권의 형태로 행사된다고 하여 반드시 자유권의 본질과 모순되는 것으로 보아야 할 필요는 없다. 오히려 자유권을 실효적으로 보장하기 위한 적극적 방어수단의 하나로 이해하는 것이 자연스러운 것이다.

그리고 통화기록이나 양심, 신앙, 사상, 정치적 견해, 교육정보, 신용정보, 고용정보, 신체장애 등에 관한 정보의 보호는 통신의 자유(제18조), 양심의 자유(제19조), 종교의 자유(제20조), 선거권(제24조), 교육권(제31조), 재산권(제23조), 노동권(제32조, 제33조), 사회보장수급권(제34조) 등의 보장으로 나타날 수도 있다. 또한 언론매체에 대한 액세스권이나 행정기관이 보유하는 개인정보의 열람권은 표현의 자유(제21조)와 알 권리(제1조, 제10조, 제21조 등)의 내용이 될 수 있다. 이러한 점에서 이들 개별적 기본권도 개인정보자기결정권과 일정한 관련을 가질 수 있다. 하지만 사생활보호에 관한 헌법 제17조의 포괄적 성격을 고려한다면, 이들 기본권은 개인정보자기결정권의 근거로서 제한적 의미를 가질 수밖에 없을 것이다. 결론적으로 필자는 개인정보자기결정권의 ‘일반적’ 근거를 헌법 제17조에서 보장하는 사생활

163) 김승환, “정보자기결정권”, 『헌법학연구』 제9권 제3호(한국헌법학회, 2003), 166면; 김일환, 앞의 논문, 98-99면 등 참조.

의 비밀과 자유에서 구하는 것이 옳다고 본다.

3. 개인정보자기결정권의 내용

개인정보자기결정권은 단순히 타인에 의한 개인정보의 취급을 억제하는 이외에도 개인이 자신에 관한 정보의 유통을 적극적으로 형성하고 조절한다는 측면에서 이해될 수 있다. 이러한 점에서 개인정보의 취급과정에 따라 정보주체의 통제권이 작용하는 모습을 포착하는 것은 개인정보자기결정권의 보호영역을 획정하는 데 유용할 수 있다. 그렇다면 개인정보자기결정권은 수집에 대한 통제권, 보유에 대한 통제권, 이용에 대한 통제권 등을 내용으로 한다고 할 수 있다. 물론 개인정보자기결정권은 일반적으로 배제청구권, 열람청구권, 정정·차단·말소·파기청구권 등으로 나타날 수도 있다.¹⁶⁴⁾

그런데 학설 가운데는 개인정보의 수집·분석·처리에 대한 배제청구권은 엄밀한 의미에서의 개인정보자기결정권의 내용이 되기 어렵다고 하는 견해가 있다.¹⁶⁵⁾ 개인정보의 수집·분석·처리 그 자체는 정보주체의 동의 여부에 불구하고 행정기관을 비롯한 공공단체·사기업들에 이르기까지 널리 행하여지고 있는 것이 오늘날의 보편적 관행이며 그 관행은 불가피한 현상으로 인식되고 있다는 점이 그 이유이다. 그러나 타인이 자신에 관한 정보를 수집·분석·처리하는 행위의 배제를 청구할 권리아말로 자기정보관리통제권의 핵심적이고도 기본적인 내용이라고 보아야 할 것이다.¹⁶⁶⁾ 개인정보를 수집할 수 있는 경우를 법률에 명시하고 정보처리자의 통지의무를 실질화한다면 개인정보

164) 권영성, 『헌법학원론』(법문사, 2008), 455-456면; 최대권, 앞의 책, 261-262면; 서울고등법원 1996. 8. 20. 선고 95나44148 판결. 하집96(2)277.

165) 권영성, 위의 책, 428면 각주 1) 참조.

166) 성낙인 외, 『개인정보보호를 위한 정책방안 연구』(정보통신부, 1999), 31면 각주 53번; 김종철, “헌법적 기본권으로서의 개인정보통제권의 채구성을 위한 시론”, 『인터넷법률』 4호(법무부, 2001), 34면 각주 31번.

수집에 대한 통제권은 상당한 정도로 확보될 수 있을 것이다.¹⁶⁷⁾

개인정보자기결정권의 보장을 위해서는 민감한 개인정보의 수집금지, 불법적 방법에 의한 개인정보수집의 금지, 개인의 의사에 반한 처리의 제한, 보유의 방법과 기간의 제한, 접근권의 보장 등이 요청된다. 그러면 이하에서는 개인정보의 처리단계별로 나누어 개인정보자기결정권의 내용을 구체적으로 살펴보기로 한다.

(1) 수집에 대한 통제권

1) 수집동의권

개인정보자기결정권의 핵심적 내용은 무엇보다도 자신에 관한 정보의 유통을 원칙적으로 정보주체의 의사에 따르도록 하는 것이라고 할 수 있다. 따라서 정보주체는 자신에 관한 정보를 자발적으로 타인에게 알리거나 이용할 수 있게 할 수도 있고, 자신이 원할 경우 그 정보에 대한 타인의 접근이나 이용을 막을 수도 있다. 다시 말해 정보주체는 자신에 관한 정보에 대한 처분권을 가지고 있는 것이다. 이러한 정보주체의 권능은 일차적으로 정보수집에 대한 동의권을 통해서 나타난다. 만일 이러한 정보주체의 동의를 얻지 않고서 개인정보를 수집하려면 반드시 법률에 그 근거규정이 있어야 하는데, 법률유보원칙 내지 기본권제한의 일반원칙에 비추어 볼 때 그것은 당연한 요청이라고 하겠다.

2) 설명청구권

정보주체의 동의는 정보주체의 자유로운 결정에 기초한 것이어야 한다. 그러기 위해서는 정보주체가 그 정보의 수집에 따라 발생할 수 있는 여러 문제점들을 충분히 이해할 수 있는 상황이 전제되지 않으

167) 同旨: 최봉철, 앞의 논문, 121면.

면 안 된다. 이러한 점에서 개인정보의 수집에 있어서는 충분한 설명에 기초한 동의(informed consent)가 요구된다고 할 수 있다. 따라서 그 수집에 앞서 수집사실의 고지와 명시적인 수집목적의 제시가 필요하고, 수집된 개인정보의 처리와 이용 등에 대한 구체적인 안내가 있어야 한다. 여기에는 정보처리의 목적, 정보관리자와 정보수집자의 신원, 수집거부에 따른 피해, 향후의 정보처리과정에 있어서 정보주체의 관여권 등에 관한 충분한 고지와 설명이 요구된다.

한편 개인정보는 적법한 절차에 따르되, 원칙적으로 정보주체로부터 직접 수집하여야 한다. 예외적으로 제3자로부터의 수집이 허용되는 경우에도 개인정보를 기록할 때까지 정보주체에게 그 사항을 설명하여야 한다.

3) 민감한 개인정보의 수집금지

사상, 신조 등에 관한 사항은 개인에게 대단히 민감한 개인정보라 할 수 있다. 이러한 개인정보는 수집 그 자체에 의하여 인간 내면의 자유의 본질적 내용을 침해할 가능성이 아주 높다. 따라서 이러한 개인정보들은 그 수집의 단계에서부터 제한할 필요가 있다.

오늘날 많은 입법례에서는 인종, 민족, 정치적 견해, 종교적 신념, 노동조합원자격, 건강상태, 성생활, 형사처벌에 관련된 사항 등을 민감한 개인정보(sensitive personal data)라고 하여 정보주체의 명백한 동의가 없는 한 그 수집을 원칙적으로 금지하고 있다. 그 대표적인 경우로는 영국의 데이터보호법 제2조, 독일의 연방데이터보호법 제3조 제9항 및 13조 제2항, Directive 95/46/EC 제8조 등을 들 수 있다.

한편, 우리의 『공공기관의 개인정보보호에 관한 법률』도 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우를 제외하고는 “사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보”를 수집할 수 없도록 하고 있다(제4조).

(2) 보유에 대한 통제권

공공기관이 보유하는 개인정보는 적법한 절차에 의하여 수집된 것이라 하더라도 그 내용이 사실에 어긋난다든가 과거의 사정에 기초한 것이라든가 또는 수집목적에 충실하지 못한 상태로 보유하고 있다든가 할 경우가 있을 수 있다. 이처럼 자신에 관한 정보가 부정확하거나 불완전한 상태로 타인에 의하여 보유하고 있다는 자체만으로도 정보주체로서는 매우 불쾌하고 불안한 느낌을 가질 수 있다. 더욱이 그것을 기초로 하여 공권력이 행사되거나 외부로 유출되기라도 한다면 정보주체의 정체성에 심각한 위협이 초래될 수도 있다. 이러한 상황에 대처하기 위해서는 정보주체가 자신에 관한 정보를 보유하고 있는 자에 대하여 그 정보의 열람·수정·삭제·차단 등을 요구할 수 있어야 할 것이다. 이러한 요구는 정보주체가 자신에 관한 정보로부터 소외되지 않도록 해주는 최소한의 통제장치라고 할 수 있다. 따라서 이것은 관련 법률에서 어떻게 정하든 정보주체의 권리로서 인정되어야 할 것이다.

1) 열람청구권

정보주체는 자신에 관한 정보를 보유하고 있는 자에 대하여 그 정보의 열람을 청구할 수 있고, 당해 정보의 보유자는 특별한 사유가 없는 한 그 열람을 허용하여야 한다(개인정보보호법 제12조 및 제13조). 이러한 열람청구권은 자신에 관한 정보에 대한 액세스권 내지 자기정보에 대한 알 권리로서 이해될 수 있다.

이 권리를 통해 정보주체는 자신에 관한 정보가 어떤 내용으로 기록·보유되고 있는지, 어떠한 목적을 위해 이용되고 있는지, 그 관리상의 안전상태는 어떤지 등에 대해 확인할 수 있다. 이를 위해 정보주체의 요청이 있는 경우 정보보유자는 그 정보의 내용이나 안전성에

대해 충분한 설명을 해주어야 한다. 이러한 요청이 거부된 경우에는 그 이유를 제시하도록 하고, 나아가 그러한 거부에 대하여 이의를 제기할 수 있는 권리도 보장되어야 할 것이다. 물론 이러한 열람청구권은 가급적 저렴한 비용으로 용이하게 행사될 수 있어야 한다.

2) 정정청구권

정보주체는 자신에 관한 정보에 내용상 부정확하거나 불완전한 부분이 있으면 그 사실을 지적하여 정정할 것을 요구할 수 있다. 이 경우 정보보유자는 정당한 이유가 없는 한 그 부분을 정정하여야 하며, 그 정정사실을 정보주체에게 통지하여야 한다(개인정보보호법 제14조). 만약 정보주체의 정정요구에 이유가 없다고 판단되면 정보보유자는 거부이유와 거부처분에 대한 불복신청의 방법을 통지해야 한다.

이처럼 잘못된 정보를 정정하는 절차는 행정의 현실적응성을 위해서도 필요한 것이지만, 개인정보에 대한 자율적 통제 of 중요성을 감안할 때 정보주체의 권리로서 인식하지 않을 수 없다. 만일 이러한 정정청구권이 보장되지 않는다면 열람청구권은 아무런 의미가 없는 것이 될 수도 있다.

3) 삭제·차단청구권

개인정보의 저장이나 보유가 허용되지 않거나 정보보유자의 직무수행에 더 이상 필요하지 않게 되는 경우에는 정보주체는 정보보유자에 대하여 자신에 관한 정보를 삭제할 것을 청구하거나 그것이 다시는 이용될 수 없도록 차단해줄 것을 청구할 수 있다. 정보주체의 이러한 청구에 이유가 있는 경우에는 정보보유자는 그에 따라야 한다. 하지만 법적으로 혹은 현실적으로 삭제가 불가능하거나 곤란한 사정이 있는 경우에는 정보주체의 삭제청구에도 불구하고 정보보유자는 그 정보를 차단할 수도 있을 것이다. 만일 보유하고 있는 개인정보에 대해

정보주체가 정확성 여부에 관하여 이의를 제기하고 그것이 정확한지 여부를 확인할 수 없는 경우에도 그 정보는 차단되어야 할 것이다.¹⁶⁸⁾

(3) 이용·제공에 대한 통제권

자신에 관한 정보가 적법하게 수집·보유되었다고 하더라도 그것이 당초 정보주체가 동의하거나 법률상 허용되는 범위를 초과하여 이용되거나 무단으로 제3자에게 제공되는 경우 정보주체는 이에 개입하여 자신의 의사를 반영할 기회를 가질 수 있어야 한다. 여기서 정보주체의 의사는 그 활용을 중단하도록 요청하거나 새로운 동의를 얻어서 계속 활용할 수 있도록 하는 형태로 관철될 수 있다.

1) 중단청구권

정보주체는 자신에 관한 정보가 수집 당시 동의한 기간을 경과하여 이용되고 있거나 그 정보가 원래의 목적 이외의 용도로 처리되고 있는 경우 언제든지 그 이용이나 처리의 중단을 청구할 수 있다. 그리고 개인정보의 처리가 자신이나 타인에게 부당하고 실질적인 손해나 고통을 초래하고 있거나 초래할 가능성이 있는 경우에도 정보주체는 정보보유자에 대하여 즉시 혹은 상당한 기간의 경과 후에 그 처리나 이용의 중단을 청구할 수 있다.¹⁶⁹⁾

2) 추가적 동의권

수집 당시에 이루어진 동의는 명시된 목적의 범위 안에서 그리고 그 정보의 보유자나 이용자에 대해서만 효력이 미치기 때문에 원래의 목적을 초과하거나 제3자에게 제공 또는 전달될 경우에는 별도의 동의가 필요하다고 해야 한다. 정보주체는 정보보유자에 대하여 자신에

168) 독일 연방데이터보호법 제20조 제2항 내지 제4항 참조.

169) 영국 데이터보호법 제10조 내지 제11조 참조.

관한 정보를 목적외로 이용하거나 제3자에게 제공 또는 전달하는 데 대한 동의권을 추가로 가진다. 이와 관련하여 정보주체는 정보의 보유자나 이용자로부터 새로운 사정에 대해 미리 통지받을 권리를 가지는 것은 물론이다.

4. 개인정보자기결정권의 제한

(1) 의 의

오늘날 개인은 자신이 의식하든 못하든 사회적 편익과 비용을 누리고 지불하는 공동체의 일원으로서 삶을 영위해가고 있다. 공동체 구성원들 사이의 의사소통에는 필연적으로 타인의 존재를 인정하고 배려하는 자세가 요구된다. 여기에는 무엇보다도 타인에 대한 기본적인 이해가 수반되어야 한다. 비록 자신에 관한 정보라고 하더라도 그 정보를 자신의 지배권에만 가두어두고 타인에게는 그에 대해 한 치의 접근도 허용하지 않는다면 그것은 공동체의 일원이기를 거부하는 자세에 다름 아닐 것이다. 이러한 의미에서 개인정보자기결정권은 어떠한 상황에서도 혹은 그 어떠한 이유로도 결코 제한할 수 없는 절대적인 의미를 가질 수는 없다. 개인정보자기결정권도 공동체관련성 내지 공동체구속성을 가지는 한도에서 중대한 공익을 위하여 일정 정도 후퇴되지 않으면 안 되는 것이다.

우리 헌법 제37조 제2항에 의하면, 국민의 자유와 권리는 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있다. 이는 공동체 외부로부터의 위협에 대처하거나 공동체 내부에서 발생하기 쉬운 혼란을 방지하기 위하여 혹은 공동체의 다른 구성원과의 조화로운 공존을 도모하기 위하여 기본권의 보호범위 가운데 필요한 최소한의 정도를 법률로써 제약할 수 있음을 선언한 것이라 할 수 있다. 이러한 점에서 이 규정은 개인과 공동체 사

이의 긴장관계를 조정하는 의미도 가지는 것이다.

개인정보자기결정권의 제약이 정보주체의 동의에 기초하여 이루어지는 경우는 개인정보자기결정권의 제한이 아니라 정보주체에 의한 그 기본권의 행사에 해당한다고 할 수 있다. 따라서 개인정보자기결정권은 정보주체의 동의를 얻지 아니하거나 그 동의를 초과하여 공권력이 개인정보의 수집, 축적, 보유, 이용, 제공 등의 조치를 취하는 경우로서 이해되어야 할 것이다. 그리고 이러한 개인정보자기결정권의 제한은 공권력에 의한 개인정보자기결정권의 정당한 제약으로서, 기본권제한의 일반원칙을 일탈한 개인정보자기결정권의 침해와 구별된다. 이러한 개인정보자기결정권의 제한은 주로 국방, 경찰, 수사, 재판, 통계, 조세, 복지 등을 위한 공권력의 발동과 관련하여 일어나지만, 정보의 자유, 언론·출판의 자유, 알 권리 등 타인의 기본권과 충돌되는 경우에도 문제될 수 있다.

(2) 제한의 목적

우리 헌법상 개인정보자기결정권은 국가안전보장·질서유지·공공복리를 위해서만 제한될 수 있다. 그 목적에 따라 개인정보자기결정권이 제한되는 구체적인 형태를 살펴보면 다음과 같다.

첫째, 국가안전보장을 위한 제한으로 반국가적 범죄에 대한 수사, 신원조사, 대공·방첩을 위한 사찰 등의 활동을 생각할 수 있다. 이러한 임무를 수행하는 기관으로는 검찰, 경찰, 국가정보원, 군검찰, 헌병, 국군기무사령부 등이 있다.

둘째, 질서유지를 위한 제한으로는 전과조회, 계좌추적, 범죄수사, 성범죄자의 신상공개, 공직자등의 병역사항이나 재산내역의 공개, 공직선거후보자의 전과공개, 주민등록제도 등이 있다.

셋째, 공공복리를 위한 제한으로는 국민건강보험의 시행을 위한 의료정보의 조사, 복지혜택의 부여를 위한 소득 등의 조사, 전염병의 예방

을 위한 질병조사, 사회생활지표의 작성을 위한 통계조사 등이 있다.

(3) 법률에 의한 제한

공권력에 의하여 이루어지는 개인정보의 조사, 저장, 제공, 공개 등은 개인정보자기결정권이라는 기본권의 제한이라 할 수 있으므로, 그 제한에는 반드시 법률의 수권이 있어야 한다. 이는 공권력의 발동에 법률상의 근거를 요구하는 법률유보의 원칙으로서 이해될 수 있으며, 헌법 제37조 제2항이 이를 규정하고 있다. 물론 이 경우의 법률은 국회가 제정한 형식적 의미의 법률로서 그 절차나 내용상 합헌성이 인정되어야 한다. 아무튼 정보조사 기타 정보처리는 관련자가 명시적으로 목적이 구체화된 정보처리에 동의하지 않는 이상 안전보장, 사회질서유지, 공공복리를 위하여 제정한 법률에 근거하여서만 개인정보자기결정권에 대한 제한이 이루어질 수 있다.

그런데 개인정보의 처리를 허용하는 법률이 있다고 하더라도 그것은 법치국가원리에서 도출되는 명확성의 요청을 따라야 한다. 특히 개인정보의 수집·처리와 관련지어 보면 이러한 규범명확성(Normenklarheit)의 원칙은 자신에 관한 정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 해당 개인이 명확하게 인식할 수 있어야만 한다는 것을 뜻한다. 여기서 의도된 데이터처리의 목표는 물론 그 범위의 영역별로 법률에 명확하게 규정되어야 한다.¹⁷⁰⁾ 따라서 조직적이고 절차법적인 예방책들, 관할기관들의 통지의무, 관련자의 포괄적인 설명청구권 등에 관한 법률의 명시적인 언급을 통하여 누가, 언제, 어디에서 어떤 경우에 자기에 관하여 아는지를 관련 시민이 알 수 있도록 보장되어야 한다. 특히 관련자가 법규정으로부터 그의 개인정보가 어떤 구체적인 행정목적들을 위하여 필요한지를 명백히 인식할 수 있어야만 한다. 하지만 입법자가 각 개인의 법률상 의무에 대하여 구체적 목적

170) BVerfGE 65, 1 (44, 46) 참조.

까지 그 법률에서 밝힐 필요는 없고, 일반적으로 그 목적이 당해 법률의 체계 및 입법취지 등에 비추어 그 의미가 분명하여질 수 있다면 그 법률은 이미 충분히 명확하다고 할 수 있다.¹⁷¹⁾

(4) 제한입법

개인정보자기결정권을 제한하는 우리나라의 입법으로는 형사처벌을 위한 증거조사 등에 관한 형사소송법 이외에도 국가정보원법, 통계법, 주민등록법, 국세기본법, 「특정금융거래정보의 보고 및 이용 등에 관한 법률」, 전자정부법¹⁷²⁾, 「행정기관의 정보공개에 관한법률」, 「청소년의 성 보호에 관한 법률」, 공직자윤리법, 「공직자등의 병역사항 신고 및 공개에 관한 법률」, 도로교통법, 국민건강보험법, 의료법, 전염병 예방법, 후천성면역결핍증 예방법 등을 들 수 있다.

제 3 절 개인정보자기결정권의 헌법적 한계

1. 언론의 자유와의 조화

(1) 서 언

언론보도를 위한 취재나 편집에 있어서 기자나 기타의 언론종사자들은 수많은 개인정보를 취급하게 된다. 취재활동에 있어서는 정보원의 신원이나 취재대상의 인적 사항을 파악하는 것이 불가피하다. 그런데 오늘날 언론에 대해서는 대체로 정보에 대한 자유로운 접근과 취득된 정보의 처리에 관한 독자적인 판단을 내용으로 하는 취재의 자유와 편집의 자유가 보장되고 있다. 더욱이 헌법해석상 언론·출판

171) BVerfGE 65, 1 (54) 참조.

172) 종래 「전자정부구현을위한행정업무등의전자화촉진에관한법률」의 명칭을 가지고 있었으나, 2007. 1. 3. 동법이 일부개정(법률 제8171호)되면서 명칭도 지금처럼 「전자정부법」으로 바뀌었다.

의 자유에 대해서는 다른 기본권이나 법익들에 비하여 우월적 지위가 인정되고 있다.

하지만 언론·출판의 자유라고 어떠한 경우에도 제한이 불가능한 절대적 기본권으로 파악되지는 않는다. 심지어 수정헌법 제1조에서 언론·출판의 자유에 대한 제한입법을 금지하는 규정을 두고 있는 미국에서조차 엄격한 조건하에서나마 프라이버시의 침해나 국가안보에 대한 위협 등을 초래하는 경우에는 그 제한이 인정될 수 있다는 점에서는 아무런 이견도 없다.

그런데 언론에 의한 개인정보의 공표와 관련하여서는 언론과 정보주체간의 상충하는 이해의 충돌이 존재할 수 있다. 가령 유명인의 동정에 관한 보도에 있어서 혼혈, 혼인 외 출생, 이혼, 심지어는 AIDS 감염 여부까지도 대중에게 노출된다는가 혹은 범죄관련 보도에 있어서 범인이나 범죄피해자 등의 성명, 나이, 직업, 주소, 전과사실 등이 공개되는 사례가 적지 않다. 물론 이와 같은 공표가 본인의 진정한 승낙에 따라 이루어진 것이라면 문제될 것이 없지만, 만일 그렇지 않다면 세간의 따가운 눈총이나 과도한 관심 또는 자신에 관한 정보의 통제력 상실 등에서 오는 엄청난 정신적·물질적 고통을 그 당사자가 겪게 될 것이라는 점은 불을 보듯 뻔하다. 그러나 다른 한편으로 언론매체는 그 내용이 대중의 중대한 관심사이고 그 보도가 공공의 이익을 위해 이루어진 것이기 때문에 불가피한 것으로 정보주체로서는 감수해야 한다고 주장할 수 있을 것이다.

이와 같은 문제는 종래 언론의 자유와 프라이버시권 사이의 충돌로서 많이 논의되어 왔다. 그런데 사람의 성명, 나이, 직업, 주소 등과 같이 대외적 인식을 예정하고 있는 개인정보까지도 프라이버시로서 보호받을 수 있는 성질의 것이냐에 대해 문제가 제기될 수 있다. 하지만 현대적 정보처리의 능력을 감안할 때 당해 정보의 종류나 성질보다는 정보처리의 위험성에 중점을 두고 이 문제를 바라볼 필요가

있다. 이러한 점에서 언론에 의한 개인정보의 취급이 야기하는 헌법상의 문제는 엄밀하게 이야기한다면 언론의 자유와 개인정보자기결정권 사이의 충돌로서 이해될 수 있을 것이다.

(2) 비교법적 고찰

1) 독일에 있어서 언론매체는 언론·출판의 자유를 가진다는 이유로 연방데이터보호법(Bundesdatenschutzgesetz)의 적용대상에서 특별한 지위를 인정받아 왔다. 즉 1990년의 연방데이터보호법에 의하면 개인 관련데이터를 오로지 저널리즘이나 출판의 목적을 위해서만 처리 또는 이용하는 언론매체에 대해서는 비밀유지의무(제5조), 기술적·조직적 조치(제9조)에 관한 규정만이 적용될 뿐이었다(제41조 제1항). 이와 같은 미디어특권(Medienprivileg)과 관련하여서는 만일 동법을 무제한적으로 적용하게 되면 기본법상 보장되고 있는 언론의 자유의 본질적 내용이 훼손될 수 있으며, 정보자기결정권도 언론의 자유를 촉진하기 위하여 제한될 수 있다는 점이 강조되고 있다.¹⁷³⁾ 다만 일반적으로 언론매체라 하더라도 경영목적이나 영리목적 등 다른 목적을 위하여 개인 관련데이터를 처리 또는 이용할 경우 연방데이터보호법의 전면적 적용을 받게 된다고 보았다.¹⁷⁴⁾ 그러나 다른 한편에서는 개인정보가 축적된 미디어기록 역시 강력한 인격단정의 효과(persönlichkeitsprägende Wirkung)를 낳을 뿐만 아니라 완벽한 인격평가자료(Persönlichkeitsprofile)를 구축할 가능성이 크기 때문에 이러한 미디어특권을 위헌으로 보아야 한다는 견해도 존재한다.¹⁷⁵⁾ 이와 같은 지적을 의식하여 2001년의 연방데이터보호법은 동 조항의 내용을 개정하여 현행의 2003년 개정법에 이르고 있다. 개정된 제41조 제1항에 의하면, 각 주는 오로지 언

173) Rudolf Schomerus/Peter Gola, *Bundesdatenschutzgesetz(BDSG)*, 5. Aufl.(München: C. H. Beck, 1992), S. 473.

174) Hans H. Wohlgemuth, *Datenschutzrecht*, 2. Aufl.(Berlin: Lutherhand, 1993). Rdnr. 43.

175) W. Schmitt Glaeser, *aaO.*, Rdnr. 94 참조.

론·편집 또는 출판의 목적만을 위해서 개인정보를 수집, 처리, 이용하는 언론사에 대해서는 제5조, 제9조, 제38조a에 관한 규정이 적용될 수 있도록 입법하여야 한다. 이러한 내용은 연방데이터보호법의 일부 조항에 한하여 언론에 대한 직접적 적용을 부인하는 것이라 할 수 있지만, 언론사의 완전한 자율적 규제에 맡기지는 않고 각 주의 입법에 의한 규율을 촉구하는 정도에 머물고 있다. 따라서 현행의 연방데이터보호법에서 미디어특권은 1990년 개정법에서보다 훨씬 약화된 수준에서 인정된다고 할 수 있다.

2) 일본에서도 그 동안 언론과 시민단체에서는 개인정보보호법을 전면적으로 적용할 경우 언론의 자유를 위축시키는 결과를 가져올 것이라고 반발해왔다.¹⁷⁶⁾ 언론에 대해서까지 적법하고 적정한 취득과 본인의 적절한 관여 등을 요구할 경우, 정보원으로부터 취재를 거부당하거나 취재내용의 공개를 요구당할 우려가 있고 특히 공인의 의혹추구 등의 취재활동에 있어서 제약이 가해질 위험이 있다는 것이 그 주된 논거였다.¹⁷⁷⁾ 결국 이러한 주장을 받아들여 2003년 5월 30일 법률 제57호로 공포된 바 있는 「개인정보의 보호에 관한 법률」(個人情報の保護に関する法律)에서는 보도기관에 대한 적용제외가 인정되었다. 즉 개인정보를 취급하는 목적의 전부 또는 일부가 방송기관, 신문사, 통신사 기타 보도기관의 보도에 제공하기 위한 것일 때에는 이용목적의 특정, 이용목적에 의한 제한, 적정한 취득, 취득시 이용목적의 통지, 데이터내용의 정확성 확보, 안전관리조치, 제3자제공의 원칙, 보유개인데이터에 관한 사항의 공표, 개시, 정정, 추가, 삭제, 이용정지, 소거 등 개인정보취급사업자의 의무에 관한 제4장의 규정은 적용되지 않는다(제50조 제1항 제1호). 다만 보도기관에 대하여 개인데이터의 안전

176) 황상철, “일본의 개인정보보호를 위한 입법동향-개인정보의보호에관한법률안을 중심으로-”, 『법제』 (법제처, 2003. 1), 67면, 72면 등 참조.

177) 정상호, “일본 개인정보보호법 제정 추진동향”, 『해외정보보호동향』 (한국정보보호진흥원, 2003. 2), 17-18면 참조.

관리를 위해 필요하고 적절한 조치, 개인정보취급에 관한 불평의 처리 기타 개인정보의 적절한 취급을 확보하는 데 필요한 조치를 스스로 강구하고, 당해 조치의 내용을 공표하도록 노력할 의무를 부과하고 있다(제50조 제3항).

3) 영국의 데이터보호법(Data Protection Act)에서는 언론에 의하여 처리된 개인정보에 대하여 데이터주체의 권리와 데이터보호원칙을 제외한 나머지 조항의 적용을 배제하고 있다(제32조). 프랑스의 「정보처리, 정보파일 및 자유에 관한 법률」(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)에서도 인쇄매체나 방송매체에 의해 취급된 개인정보에 대해서는 개인정보의 수집제한에 관한 조항이 적용되지 않을 수 있도록 하고 있다(제33조). 스웨덴의 1998년의 개인정보법(Personal Data Act)은 언론자유법이나 표현의 자유에 관한 기본법에 명시된 언론의 자유 및 표현의 자유에 관한 조항에 위배되지 않는 범위 내에서 적용되도록 하고 있다(제7조).

4) 그러나 이러한 미디어특권을 명시적으로 인정하고 있지 않은 나라에서도 언론에 대하여 모든 개인정보보호의 원칙이 언제나 적용되는 것은 아니다. 가령 명예훼손 등에 관한 법률조항이 존재하거나 판례이론을 통하여 언론매체의 면책이 허용되고 있기 때문이다.

(3) 조화적 해석의 필요성

민주주의 국가에서는 여론의 자유로운 형성과 전달에 의하여 다수 의견을 집약시켜 민주적 정치질서를 생성·유지시켜 나가는 것이므로 표현의 자유, 특히 공익사항에 대한 표현의 자유는 중요한 기본권으로서 최대한 보장되어야 하겠지만, 그로 인하여 개인의 개인정보자기결정권이 과도하게 제한되는 결과가 초래되어서는 안 될 것이다.

언론의 자유와 개인정보자기결정권의 관계에 있어서는 기본적으로 기본권충돌의 해결에 관한 헌법학상의 일반적 논의가 적용될 수 있을

것이다. 따라서 그 기본권들 사이의 충돌은 이익형량의 이론과 규범 조화적 해석론에 의하여 상생의 길을 모색하여야 할 것이다. 또한 프라이버시권과 언론의 자유 사이의 충돌을 해결하기 위한 제시되고 있는 공익의 이론, 공적 인물이론 등도 적용될 여지도 있을 것으로 본다. 물론 여기에는 개인정보의 처리가 초래할 수 있는 현대적 위험에 대한 고려가 필요할 것이다.

그런데 문제는 언론에 의한 개인정보의 취급에 있어서 개인정보자기결정권과 언론의 자유는 서로 우열을 가리기 어려운 기본권이라는 점이다. 양자 모두 정보에 관한 자유로운 처분을 이념으로 하고 있고 공동체생활에 필수적인 의사소통의 자유를 보장함으로써 궁극적으로는 인간으로서의 존엄과 가치를 실현하려는 것을 목적으로 하기 때문이다. 따라서 구체적인 문제의 해결은 양자의 조화적 공존을 가능하게 하는 방안을 모색하되, 그것이 여의치 않을 경우에는 이익형량에 의존할 수밖에 없을 것이다. 여기서 충돌하는 두 보호법익을 어떻게 조정할 것인지는 구체적인 경우에 사회적인 여러 가지 이익을 비교하여 표현의 자유로 얻어지는 이익, 가치와 인격권의 보호에 의하여 달성되는 가치를 형량하여 그 규제의 폭과 방법을 정하여야 한다.¹⁷⁸⁾¹⁷⁹⁾

2. 정보공개청구권과의 조화

(1) 정보공개청구권의 의의

우리 헌법상 정보공개청구권은 행정기관이 보유하고 있는 정보에 대하여 접근하여 열람할 수 있는 기본권을 말한다. 여기서 청구의 대상은 행정기관이 보유하고 있는 정보 일반이며, 그 정보에 법률상 이익을 가지는 자에 제한되지 않고 일반 국민이면 누구나 그 청구의 주

178) 대법원 1998. 7. 14. 선고 96다17257 판결.

179) 권건보, 『개인정보보호와 자기정보통제권』 (경인문화사, 2005), 149면 이하 참조.

체가 될 수 있다. 이러한 정보공개청구권은 행정권이 보유하는 다양한 정보에 대한 국민의 자유로운 접근을 인정하여 국민의 알권리를 보장함으로써 열린 정부에 의한 행정의 공정화·민주화를 실현하는 것을 기본이념으로 한다.¹⁸⁰⁾ 그리고 정보공개는 밀실행정의 관행을 타파하고 그 공평성과 투명성을 높여 부정부패의 방지와 국민의 행정감시기능, 행정운영에 시민의 참여확대, 나아가 공적 자산인 행정정보의 사회환원을 통한 공공성의 증진에 기여하게 된다.¹⁸¹⁾

(2) 양자의 관계

1) 개인정보자기결정권은 자신에 관한 정보의 통제력을 공공기관에 대해서는 물론이고 민간부문에 대해서도 미치게 한다. 이에 비하여 정보공개청구권은 공공기관에 대한 통제와 관련되는 것이므로 주로 공공기관 등이 보유하고 있는 공공부문에 대한 것을 내용으로 한다. 개인정보자기결정권에 있어서 타인이 자기에 관한 정보를 열람하는 것은 예외적인 경우라 할 수 있지만, 정보의 주체가 자신에 관한 정보를 열람할 수 있는 것은 원칙적으로 허용된다. 즉 일반인에 대한 원칙적 비공개를 특징으로 한다고 할 수 있다.¹⁸²⁾ 반면에 정보공개청구권은 주관적 권리구제수단으로서의 성격보다는 객관적 법제도로서의 성격이 강하다.¹⁸³⁾

2) 개인정보자기결정권에 있어서 핵심적 내용으로 인정되고 있는 정보주체의 열람·정정청구권은 개인정보를 보유하고 있는 측에 대한 감시와 통제로서의 의미를 가질 수 있다. 그리고 그 보유자가 행정기

180) 김동희, 『행정법 I』 (박영사, 2001), 374-375면.

181) 이에 관한 자세한 내용은 경건, “정보공개청구제도에 관한 연구-일반 행정법 이론체계와의 관련에서-”, 서울대 박사학위논문, 1998, 24면 이하 참조.

182) 박윤흔, 『행정법강의(상)』 (박영사, 2001), 531면.

183) 김용섭, “정보공개와 개인정보보호의 충돌과 조화”, 『공법연구』 제29집 3호(한국공법학회, 2001. 5), 172면.

관일 경우 행정기관이 보유하는 정보에 대한 공개청구로 파악될 수 있다. 이러한 점에서 개인정보자기결정권은 부분적이기는 하나 정보공개청구권과 중첩될 수 있다. 한편, 개인정보자기결정권은 개인정보의 노출을 억제하는 데만 중점이 있는 것이 아니라 그 흐름을 적극적으로 형성하는 측면도 있다. 따라서 개인이 자신에 관한 정보를 필요에 따라 자의에 의하여 제공하거나 타인에게 알릴 수 있고 타인이 보유하고 있는 자신에 관한 정보의 상태를 파악하여 그것이 그 상태로 계속 보유되거나 활용되어도 좋을 것인지 아니면 새로운 내용으로 변경되어야 할 것인지를 결정할 수 있어야 한다는 것이 간과되어서는 안 된다. 이러한 점에서 정보의 상태와 흐름을 일반인이 자유롭게 확인하고 이용할 수 있는 권리인 정보공개청구권과 더불어 개인정보자기결정권은 의사소통의 활성화와 원활화에 기여하며, 궁극적으로는 시민의 의사소통 능력과 민주사회의 기능축진을 위하여 기능한다고 할 수 있다.

3) 이와 같이 볼 때 개인정보자기결정권과 정보공개청구권은 상호 보완적 관계에 있으면서 별개의 제도로써 조화롭게 각자의 기능을 수행하는 것이라고 하겠다.¹⁸⁴⁾ 그리고 정보 그 자체를 흐름으로 이해하고 정보공개로서의 수집, 이용 및 관리의 관점을 포함한다면 개인정보보호의 문제는 정보의 수집·관리·유통의 전 과정으로 미치게 되어 행정의 투명성을 확보하게 된다는 점에서 양자는 그 조화점을 찾을 수 있을 것이다.

(3) 양자의 우열관계

행정기관이 보유하고 있는 정보 가운데는 개인정보가 포함되어 있는 경우가 적지 않기 때문에 정보공개청구에 따라 모든 정보가 공개

184) 박윤흔, 『최신행정법강의(상)』(박영사, 2001), 531면; 홍준형, 『행정법총론』(한울, 1997), 489면; 김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 『공법연구』 제29집 3호(한국공법학회, 2001), 110면 등 참조.

될 수 있다고 하면 개인정보도 정보주체의 의사와 무관하게 누구에게나 노출될 위험이 있다. 반면에 개인정보가 포함되어 있거나 개인정보라고 하여 정보공개청구를 전혀 허용하지 않을 경우에는 정보공개 청구권의 유명무실화나 적어도 위축효과를 가져오게 된다.

현실적으로 양자가 함께 작용하는 국면을 보면 한 쪽에서는 정보공개청구를 할 경우 다른 쪽에서는 개인정보의 보호를 내세워 공개를 거부하거나 혹은 개인정보보호를 감안하여 공개하지 말아달라고 요구하는 양상으로 전개되는 것이 일반적이다. 사실 정보공개는 정보를 여는 쪽인 데 비하여 개인정보보호는 아무래도 정보를 닫는 쪽에 관심이 있다는 점을 부인하기는 어렵다. 또한 정보를 많이 공개하면 할수록 개인정보보호가 줄어들고 정보의 공개를 적게 하면 할수록 개인정보가 보호되는 결과가 되기 마련이다. 이렇게 정보공개는 정보를 적극적으로 방출하는 것으로 이해하고 개인정보보호는 소극적으로 정보를 감추는 것으로 파악하는 경우 양자는 상호간에 대립과 갈등의 관계에 놓이지 않을 수 없다. 이와 같이 개인정보의 보호를 내용으로 하는 개인정보자기결정권과 정보공개청구권은 상충되는 관계에 있다고 할 수 있다.

양자의 관계에 대해서는 전자가 우월적 지위에 있는 것으로 파악하는 하급심판결이 있는데, 그 판시내용은 다음과 같다.

“사생활의 비밀과 자유의 불가침은 사생활의 내용을 공개당하지 아니할 권리, 자신에 관한 정보를 스스로 관리·통제할 수 있는 권리 등을 내용으로 하는 인격권으로서 오늘날 정보사회가 급속히 진행되면서 그 보호가 절실한 권리이고, 국민의 알 권리 또한 국민의 기본권에 속하나 공공기관의 정보에 대한 공개청구권을 의미하는 한 청구권적·간접적 성격을 가진다고 보여지는 점에서, 위 두 개의 기본권이 경합하여 충돌하는 경우에 구체적 상황을 고려하여 그 보호법익을 형량하되 충돌하는 기본권 모두의 본질적 내용을 훼손하지 아니하

는 범위 내에서 그 효력을 최적정화할 수 있도록 기본권들을 조화시키는 방법으로 제한 가능성이 보다 작은 기본권을 우선시킴이 원칙이라고 할 것인데, 일반적으로 기본권의 보호법익은 생명권, 인격권이 가장 우선한다고 보여지는 점에서 알 권리보다는 개인의 사생활의 비밀과 자유가 더욱 보호해야 할 우선적인 가치라고 할 것이므로 그 범위 내에서는 국민의 알 권리도 제한을 받지 아니할 수 없다고 할 것(이다).”¹⁸⁵⁾

이 판례는 구체적 사건과 관련한 기본권 충돌의 해결문제로서 언론사세무조사결과의 공개여부를 결정하는 데 있어 제반 여러 방법론의 종합을 통하여 문제해결을 도모하면서도 알권리보다 프라이버시권을 우월적인 기본권으로 파악하였다는 점에서 특기할 만하다. 하지만 이 판결은 인간의 존엄성을 모든 기본권이 실현하고자 하는 공통의 가치로 이해하는 헌법체계에 있어서 성급하게 어느 기본권에 일방적 우위를 인정할 수 있을지는 의문이다. 물론 오늘날 거대한 감시체제를 통한 개인정보의 수집과 전산처리에 의한 개인정보의 활용과 악용이 가능한 상황을 감안할 때 사생활보호의 필요성이 알권리의 충족보다 더 강조될 수는 있을 것이다. 하지만 그 우열관계를 일반화시키기보다는 구체적인 상황을 고려하여 개별적으로 검토함으로써 어느 한 쪽이라도 희생을 최소화할 수 있는 방안을 모색하여야 할 것이다.

(4) 개별적 정보공개청구권과 개인정보열람청구권

1) 일반적으로 정보공개청구권은 일반 국민에 의한 정보공개청구이든 이해관계인에 의한 정보공개청구이든 불문하고 모두 알 권리에서도 출되는 헌법직접적 권리로 이해되고 있다.¹⁸⁶⁾ 하지만 최근에 들어

185) 서울고등법원 1995. 8. 24. 선고 94구39262 판결. 하집1995(2)464.

186) 헌법재판소 1989. 9. 4. 88헌마22 결정, 감사의 공소권행사에 관한 헌법소원; 헌법재판소 1991. 5. 13, 90헌마133 결정, 기록등사신청에 대한 헌법소원.

정보공개청구권을 일반적 정보공개청구권과 개별적 정보공개청구권으로 나누어 그 법적 근거와 성격 등을 달리 파악하려는 시도들이 나타나고 있다.¹⁸⁷⁾ 헌법재판소의 소수의견에서도 아래와 같이 정보공개청구권을 이원적으로 고찰하려는 시도가 있었다.

“알 권리”의 내용은 이를 세분하면, (1) “정보를 받을 권리”와 “정보를 구할 권리”로 나누이고, (2) 후자의 정보를 구할 권리는 다시, 국민이 일반적으로 접근할 수 있는 정보원으로부터 정보를 수집하거나 언론기관이 취재활동을 함에 있어서 공권력에 의한 방해 또는 간섭을 받지 않을 권리(자유권적인 정보수집의 자유 또는 권리)와 국가 또는 지방자치단체에 대하여 보유하고 있는 정보의 공개를 요구한 권리(청구권적인 정보공개요구권)로 나누이며, (3) 그 후자의 정보공개청구권은 다시 공권력이 보유하는 모든 정보에 대하여 일반국민 또는 언론기관이 공개를 요구할 권리(일반적 공개청구권)와 공권력이 보유하는 특정의 정보에 대하여 이해관계가 있는 특정 개인이 공개를 요구할 권리(개별적 공개청구권)로 나누인다.¹⁸⁸⁾

또한 대법원도 “국민의 알권리 특히 국가 정보에의 접근의 권리는 우리 헌법상 기본적으로 표현의 자유와 관련하여 인정되는 것으로, 그 권리의 내용에는 자신의 권익보호와 직접 관련이 있는 정보의 공개를 청구할 수 있는 이른바 개별적 정보공개청구권이 포함(된다).”고 하여 같은 태도를 취한 바 있다.¹⁸⁹⁾

2) 여기서 일반적 정보공개청구권이란 주관적인 권리침해 여부와는 상관없이 모든 국민들에게 국가가 갖고 있는 서류나 기록 등에 일반

187) 홍준형, “정보공개청구권과 정보공개법”, 『법과사회』 제6호(법과사회이론학회, 1992), 76면 이하; 경건, 앞의 학위논문, 26-28면, 315면; 박종보, “공공정보공개제도와 알 권리의 헌법적 근거”, 『헌법규범과 헌법현실』 (권영성교수 정년기념논문집)(법문사, 1999), 1014면 이하 등.

188) 헌법재판소 1991. 5. 13, 90헌마133 결정, 기록등사신청에 대한 헌법소원, 최광를 재판관의 소수의견, 판례집 제3권, 258면.

189) 대법원 1999. 9. 21. 선고 98두3426 판결. 공99.11.1.[93], 2237.

적으로 접근할 권리를 말하고, 개별적 공개청구권은 자신에 관한 정보 또는 자기의 권익보호와 직접 관련이 있는 정보에 접근할 권리를 의미한다. 전자는 국가행정의 투명성을 확보함으로써 국민들의 정치적 참여기회를 넓히고 민주주의의 실현을 강화하고자 하는 데에 그 목표가 있기 때문에 해당 개인의 주관적인 권리가 침해되는지와 상관없이 보장된다. 이러한 공익적 성격의 정보공개청구권에 의해 일반 국민들은 국가가 갖고 있는 서류나 기록에 접근할 권리를 가지게 된다. 이에 반하여 후자는 자신의 권리보호를 위하여 인정되는 것이다. 특히 자신에 관한 정보의 공개청구는 공공기관이 보유하고 있는 개인정보의 열람을 요구하는 것으로 개인정보자기결정권으로서의 성격도 가진다.

3) 물론 정보주체에 의한 개인정보의 열람청구는 개인정보보호법에 의해서도 인정되고 있다. 하지만 현행 「공공기관의 개인정보 보호에 관한 법률」의 적용을 받지 아니하는 개인정보가 존재할 뿐만 아니라, 설령 적용범위에 속한다고 하더라도 열람청구는 개인정보화일대장에 기재된 사항에 제한되어 있기 때문에 정보주체로서도 열람을 청구할 수 없는 경우가 적지 않다. 가령 전산처리되지 않는 수기식 파일의 경우에는 아예 개인정보보호법이 적용되지 않는다. 또한 범죄의 수사, 공소의 제기 및 유지 등에 관한 사항을 기록한 개인정보화일에 대해서는 정보주체에 의한 열람청구의 대상이 되지 못한다(제12조 제1항). 왜냐하면 그러한 개인정보화일은 보유의 사전통보의무가 면제되므로(제6조 제2항 제2호), 사전통보를 전제로 하는 개인정보화일대장의 작성이 이루어지지 않게 되기 때문이다(제7조). 이처럼 내용상 개인정보자기결정권에 해당될 수 있지만 개인정보보호제도보다 정보공개청구제도를 이용하는 것이 정보주체에게 유리한 결과가 될 수 있는 경우 혹은 정보주체에게 법률에 대한 구체적 이해를 기대하기 어려운 경우에 개별적 정보공개청구권을 인정할 실익이 있을 것이다. 정보주체에

게 열람청구와 정보공개청구를 선택적 권리행사를 가능하게 하는 것은 정보주체의 권리보호를 강화하는 의미가 된다.

4) 하지만 객관적 공익실현제도로서 기능하는 정보공개법에서 주관적 권리보호를 위한 정보공개까지 규율하려는 것은 법체계간의 부조화를 가져올 수 있다. 이와 관련하여 정보공개제도를 개인정보를 포함하는 행정정보 일반에 대한 공개제도로 파악하여 개인정보공개제도를 일반적 정보공개제도에 편입하여야 한다든가¹⁹⁰⁾ 개인정보자기결정권을 정보공개제도 중에 위치시키는 것이 바람직하다든가¹⁹¹⁾ 하는 주장이 제기되고 있다.

생각건대 정보주체의 열람청구권은 행정기관이 보유하는 정보의 보유와 처리에 대한 감시나 통제의 장치로서 작용될 수 있지만, 무엇보다도 본인의 권익을 보호하기 위한 수단적 성격을 강하게 띠고 있다는 점을 무시할 수 없다. 또한 개인정보자기결정권은 개별적 정보공개청구권뿐만 아니라 개인정보의 수정·삭제청구 등도 포함하는 것이므로 개인정보자기결정권이 그 작용의 국면에 있어서 정보공개청구권보다 훨씬 광범하다고 할 수 있다.

이처럼 양자는 독자적 기능을 수행하는 별개의 권리 혹은 제도라 할 것이므로, 개인정보열람청구를 굳이 일반적 정보공개청구의 일부로서 편입시킨다든가 반드시 정보공개법에서 규정해야 할 내용으로 이해할 필요는 없다고 본다.

오히려 자신에 관한 정보의 공개청구가 이념상으로 개인정보자기결정권에 입각한 것으로 볼 수 있는 만큼, 정보주체의 열람청구권을 실질화함으로써 「공공기관의 개인정보 보호에 관한 법률」이 이를 충분히 규율할 수 있도록 하는 것이 바람직할 것이다.

190) 경건, 앞의 학위논문, 317면.

191) 김효진, “정보공개와 개인정보의 법적 보호”, 『헌법규범과 헌법현실』 (권영성교수 정년기념논문집)(법문사, 1999), 261면.

(5) 정보공개와 한계와 개인정보보호

1) 개인정보의 공개제한의 의미

『행정기관의 정보공개에 관한 법률』은 제3조에서 “공공기관이 보유·관리하는 정보는 이 법이 정하는 바에 따라 공개하여야 한다.”고 하여 정보공개 원칙을 표방하고 있다. 그러면서도 제7조 제1항에서는 비공개대상정보로서 8가지를 열거하고 있다. 그 가운데서 제6호는 “당해 정보에 포함되어 있는 이름·주민등록번호 등에 의하여 특정인을 식별할 수 있는 개인에 관한 정보”를 비공개할 수 있도록 규정하고 있다. 다만, 다목에서 “공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익 또는 개인의 권리구제를 위하여 필요하다고 인정되는 정보”를 비공개의 대상에서 제외하고 있다.

여기서 개인정보보호를 위한 이러한 규정은 개인정보자기결정권의 보장을 위한 것으로 이해할 수 있다. 즉 제7조 제1항 제6호는 개인정보의 제공 내지 공개에 대한 통제권을 보장하는 측면이 있는 것이다. 따라서 이 규정은 개인정보자기결정권이라는 정보주체의 기본권을 고려하여 정보공개청구권을 제한한 것으로 볼 수 있다. 그러나 기본권 충돌의 조화적 해결하기 위하여 다시 제7조 제1항 제6호에 단서를 부가하고 있다.

제6호 본문과 단서를 문언에 충실하게 해석해보면 다음과 같이 이해할 수 있다. 즉, 개인정보라 하더라도 ‘공개하지 않을 수’ 있지만, 공익을 위하여 필요하다고 인정되면 반드시 ‘공개하여야’ 한다. 정보공개청구권보다 개인의 정보통제권을 우선시하면서도, 구체적인 경우 공익에 의한 개인정보자기결정권의 제한을 허용하고 있는 것이다. 언뜻 보면 기본권충돌은 개인정보자기결정권의 우선적 보장의 형태로 입법적 해결을 본 것 같다. 하지만 구체적인 충돌상황의 해결은 공익

적 필요의 인정 여부에 따르도록 함으로써 행정기관과 사법부의 판단에 미루고 있다. 이러한 점에서 입법자는 개인정보자기결정권의 우선이라는 일반적 기준만 제시하고 있다고 할 수 있다. 공개의 공익적 필요가 인정될 수 있는지 여부를 결정함에 있어서는 개인정보보호를 통하여 보호되는 정보주체의 이익과 개인정보의 공개를 통하여 얻을 수 있는 공익을 서로 비교하는 이익형량이 동반될 수밖에 없다. 이러한 이익의 형량은 구체적 사안에 따라 개별적으로 검토되어야 할 것이다. 물론 개별 사안을 법규범에 포섭하는 작업은 구체적인 이익형량에 선행되어야 할 것이다.

2) 이익형량과 기본권의 조화적 보장

그런데 기본권의 충돌상황을 해결함에 있어서 너무 성급하게 이익간의 우열을 가림으로써 일방의 이익만 보호하고 타방의 이익은 희생되는 결과를 초래하여서는 곤란하다. 이익형량에 있어서는 조화적 보호의 가능성을 충분히 모색할 것을 요하는 최적화명령이 적용된다.¹⁹²⁾ 형량의 외곽에서는 실제적 조화의 원칙(Prinzip praktischer Konkordanz)에 따라 양보할 수 없는 가치를 갖는 기본권의 양자 모두 그 작용을 발현하고 한 권리가 다른 권리를 통하여 절대적으로 차단되지 않을 것이 요구되는 것이다. 이러한 내용은 기본권의 최대보장이라는 헌법정신의 반영이라 할 수 있다.

한편 비례의 원칙은 법익의 실제적 조화를 도모하는 데 있어 지속적인 하나의 목적과 하나 또는 복수의 가변적인 수단 사이의 관계문제로서가 아니라 두 개의 법익간의 비교할 수 있는 크기를 설정해 주고 최적화임무(Optimierungsaufgabe)를 적절히 실현될 수 있도록 하는데 기여한다.¹⁹³⁾

192) Konrad Hesse, *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*, 18. Aufl.(Heidelberg: C. F. Müller Juristischer Verlag, 1991), Rdnr. 72.

193) Konrad Hesse, *aaO.*, Rdnr. 72.

이러한 관점에서 볼 때 개인정보자기결정권과 정보공개청구권의 충돌문제를 해결함에 있어서는 무엇보다도 정보주체의 의사를 탐구하려는 노력이 선행되어야 할 것이다. 가령 정보주체가 그 정보공개청구에 대해 하자 없는 찬성의 의사표시를 할 경우에는 더 이상 개인정보자기결정권과의 충돌이 문제되지 않을 것이므로 정보주체와 관련된 정보에 관한 한 공개함이 마땅할 것이다.

다음으로, 비록 정보주체의 동의는 없으나 정보의 공개가 필요하다고 인정되는 경우에도 가능한 한 당해 개인정보의 부분을 빼고서 그 나머지를 공개하는 방식을 택하는 것이 바람직하다. 이와 같은 부분공개법리는 정보공개에 있어서 익명성의 원칙(Grundsatz der Anonymität)이 반영된 것이라 할 수 있다.¹⁹⁴⁾ 익명성의 요청은 타인의 관심과 식별로부터 벗어나서 개인의 내부영역에 홀로 머물고자 하는 인간의 안식욕의 표현이라고 할 수 있는바, 개인식별가능성을 제거할 수 있는 정보에 있어서 개인의 이름이나 기타 개인을 식별할 수 있는 정보를 전부 혹은 부분적으로 익명화(Anonymisierung) 또는 가명화(Pseudonymisierung) 함으로써 개인정보자기결정권은 침해의 가능성이 최소화될 수 있을 것이다.¹⁹⁵⁾ 마지막으로, 만일 이러한 부분적 공개가 불가능하다면 정보공개를 통해 달성하고자 하는 이익과 그 공개로 인한 정보주체의 피해사이의 형량에 따를 수밖에 없을 것이다. 이러한 이익형량의 결과 그 공개를 결정하게 되더라도, 공개에 따른 정보주체의 피해를 최소화하기 위한 절차적 조치가 강구되어야 할 것이다. 가령 당해 정보의 보유기관은 공개청구인의 범위, 공개청구의 목적, 공개결정의 사유, 공개할 정보의 용도 등을 정보주체에게 통지하는 한편, 공개할 정보를 활용할 수 있는 인적·물적 범위를 제한하는 등의 조치가 필요하다.¹⁹⁶⁾

194) 김용섭, 앞의 논문, 191면.

195) Wolfgang Hoffmann-Riem, aaO., S. 535.

196) 권건보, 『개인정보보호와 자기정보통제권』 (경인문화사, 2005), 170면 이하 참조.

제 2 편
현행 개인정보보호법제에
관한 사후적 입법평가

제 1 장 개인정보처리의 실태 분석: 효용성과 위험성 평가

제 1 절 공공기관 개인정보처리의 효용성과 위험성

1. 서 언

현대에 들어와 국가기능은 복지나 사회정책 등 사회적 재생산조건을 보장하기 위한 기능을 담당하는 것으로까지 확대되었다. 이러한 국가적 과제를 합리적이고 효과적으로 수행하기 위해서는 국가에 의한 개인정보의 수집 및 처리가 필수적이라 할 수 있다.

한편, 오늘날 정보통신기술의 발달은 행정기관의 정보 수집 및 관리역량을 획기적으로 향상시킴으로써 행정의 효율성과 공정성을 높이는 데 크게 기여하고 있다.¹⁹⁷⁾

즉, 국가는 당면한 본연의 과제를 수행하기 위하여 국민의 개인정보를 수집하고 처리할 필요성이 높아졌고, 현대의 발달한 정보기술은 보다 쉽고 빠르게 필요한 개인정보를 수집하고 처리할 수 있도록 해주었다.

이러한 맥락에서 정보기술의 활용을 통하여 대국민 고객지향성의 이념 하에 효율적인 행정서비스를 제공한다는 전자정부¹⁹⁸⁾가 탄생한 것이다. 그러나 전자정부는 세계적인 추세이며 우리만의 독특한 무엇은 아니다.

197) 현제 2005. 5. 26. 99헌마513 (지문날인) 사건.

198) “전자정부”라 함은 정보기술을 활용하여 행정기관의 사무를 전자화함으로써 행정기관 상호간 또는 국민에 대한 행정업무를 효율적으로 수행하는 정부를 말한다(『전자정부법』 제2조 제1호).

[그림 2-1-1] UN의 전자정부 발전모형¹⁹⁹⁾



[그림 2-1-1]과 같이 전자정부의 발전모형을 5단계로 구분할 때, 우리나라는 현재 4단계에 도달한 것으로 평가되며, 정부는 향후 전자정부의 핵심요소 중의 하나인 ‘행정정보 공동이용’을 보다 활성화하면 5단계에 접어들 것으로 전망하고 있다.²⁰⁰⁾ 공동이용의 대상인 행정정보는 “행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것”²⁰¹⁾을 말하여, 여기에 개인정보가 포함됨은 물론이다. 즉, 국민의 개인정보가 공공기관 상호간에 공유되는 환경이 조성되었다고 볼 수 있어, 개인정보보호차원에서 이를 다시금 조명해 볼 필요성이 높다.

또한 개인정보처리가 가져다 줄 이익과 가치 못지않게 그 위험성 또한 무시할 수 없을 정도로 커서 이른바 사이버 원형감옥(Cyber-Panopticon)의 우려를 낳고 있다.

사이버 원형감옥에서의 국민은 국가과정에 적극적으로 참여하는 능동적 시민으로서의 국민이 아니라, 국가가 구축하는 개인정보처리시

199) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』(행정정보공유추진위원회, 2007. 12), 24면.

200) 위의 책, 24면.

201) 『전자정부법』 제2조 제4호.

시스템에 의해 국가작용의 내용과 형식이 결정되어지는 소외된 수동적 시민으로서의 국민으로 전락하게 될 것이다.²⁰²⁾

이와 같은 맥락에서 본 절에서는 현재 공공기관의 개인정보처리 현황을 살펴보고, 그것의 효용성과 위험성을 평가해보고자 한다.

2. 공공기관의 개인정보처리의 실태

(1) 개인정보DB의 구축 및 활용

□□공공기관의 개인정보보호에 관한 법률□□²⁰³⁾ 제5조에 따르면, 공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다. 개인정보파일은 공공기관이 구체적인 목적에 따라 수집한 개인정보의 집합물로서 컴퓨터 등에 의하여 처리할 수 있도록 체계적으로 구성한 것이다. 즉, 개인정보파일은 개인정보DB 혹은 개인정보처리시스템이라 할 수 있다.

개인정보파일을 보유하는 기관의 장은 개인정보파일별로 보유 목적·항목 및 열람예정시기 등을 기재한 개인정보파일대장을 작성·비치하여 일반인이 열람할 수 있도록 하여야 하며, 행정안전부장관은 개인정보파일목록을 작성하여 관보 또는 인터넷에 공고하여야 한다. 이에 따라 작성된 2006년 개인정보파일목록집(구 행정자치부 작성)에서 확인할 수 있는 개인정보파일종류의 수는 [표 2-1-1]과 같다. 2006년 6월 기준으로 총 1,144종의 개인정보파일이 존재한다.²⁰⁴⁾

202) 한상희, “국가감시와 민주주의”, 『개인정보의 국가등록·관리제도의 문제점』(프라이버시보호 네트워크 제2차 공동토론회 요지집, 2001. 8. 22), 1-2면.

203) 일부개정 2008.2.29 법률 제8871호.

204) 2000년 8월의 통계, 총 452종, 8,421개의 개인정보화일이 존재한다는 수치와 비교하면 공공기관이 처리하는 개인정보는 2배 이상 늘어났다. 2000년 8월의 통계는 이인호, “공공부문 개인정보보호법제에 대한 분석과 비판”, 『정보법학』 제6권 제1호(한국정보법학회, 2002. 7), 29면.

[표 2-1-1] 공공기관이 보유한 개인정보파일종류의 수²⁰⁵⁾

구분	개인정보파일종류
중앙행정기관 (소속기관 포함)	277종
지방자치단체 (소속기관 포함)	397종
교육청 및 각급학교	67종
정부투자기관 및 기타	403종
합 계	1,144종

다만 [표 2-1-1]은 종류의 수를 말하는 것으로, 실제 개인정보파일의 수는 이것의 몇 배에 달함에 유의해야 한다. 예컨대, 주민등록, 재산세, 지방세, 자동차등록 등의 개인정보파일은 각 지방자치단체마다 보유하는 것이어서 주민등록파일은 한 종류의 개인정보파일이지만 실제 존재하는 주민등록파일은 우리나라 시·군의 수와 같다. 뿐만 아니라 학교생활기록부나 건강기록부 등은 각 학교마다 보유하기 때문에 실제 개인정보파일 수는 초·중·고등학교 수와 같은 것이다. 실제로 강원도 속초시의 경우 2008년 9월 현재 256개의 개인정보파일을 보유하고 있는데,²⁰⁶⁾ 이를 전체 기초자치단체수로 곱하면 기하급수적으로 늘어남을 알 수 있다. 아울러 일정한 유형의 개인정보파일²⁰⁷⁾은 공개

205) □□2006 공공기관의 개인정보화일목록집□□의 내용을 재구성함.

206) 강원도 속초시 홈페이지에서 확인, <<http://www.sokcho.gangwon.kr/home/html/sub6/personinfo01.xls>>.

207) 『공공기관의 개인정보보호에 관한 법률』 제6조 제3항

- “1. 국가의 안전 및 외교상의 비밀 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국 관리에 관한 사항을 기록한 개인정보파일
3. 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한

되지 않아 일반인의 열람대상에서 제외되고 행정안전부 장관의 공고대상에서도 제외되는 것을 감안하면, 실제 작성·활용되는 개인정보파일은 당연히 통계수치보다 많을 것으로 예상된다. 또한 개인정보파일에 담기는 정보는 성명, 주민등록번호, 주소는 기본이고, 파일마다 차이가 있기는 하지만 연락처(전화번호, 휴대전화번호, 이메일주소, 팩스번호), 종교, 학력, 경력, 병역사항, 직장정보(직업, 직급, 근무지 등), 각종 등록번호 또는 면허번호, 각종 변동내역, 진료정보(질병명, 진료내역, 처방전 내용, 접종기록 등), 보호자나 친족에 대한 정보, 결혼여부, 계좌번호, 상담내용, 민원처리내역, 각종 세금 납부내역 등이 포함되어 있다. 하나의 개인정보파일에 최소한 3개 이상의 정보가 보유되는 것을 감안하면 실로 엄청난 양의 개인정보가 처리되고 축적되고 있음을 알 수 있다. 이렇게 형성한 개인정보파일의 일부는 공공기관 상호간, 혹은 공공기관과 금융기관이 공동이용 할 것이 의무화되는 정보로 분류되어 활용되고 있다. 이에 대하여는 항을 바꿔 설명한다.

(2) 개인정보 공동이용 현황

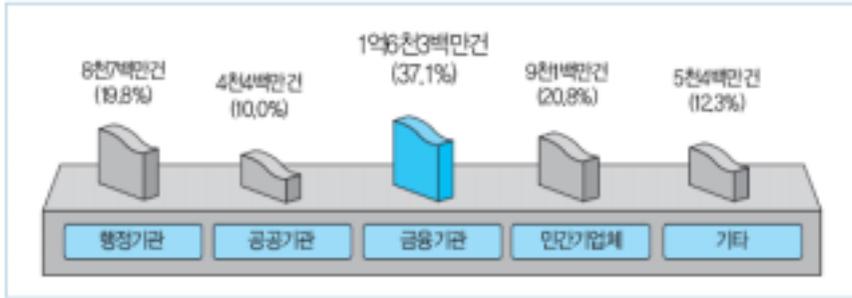
1) 추진배경

[그림 2-1-2] 과 같이 국민들이 각종 민원을 제기하기 위하여 행정기관 등에 제출하는 서류는 2005년에는 4억 4천만여 건에 이르고, 《표 2-1-2》 과 같이 하나의 민원을 해결하기 위하여 여러 종의 구비서류를 제출해야 했다. 이는 곧 국민의 불편과 자원의 낭비²⁰⁸⁾로 연결된다.

사항을 기록한 개인정보파일

4. 삭제 <2007.5.17>
 5. 삭제 <2007.5.17>
 6. 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
 7. 삭제 <2007.5.17>
 8. 그 밖에 이에 준하는 개인정보파일로서 대통령령이 정하는 개인정보파일”
- 208) 이는 무려 1년에 2조 7천억원이라는 사회적 비용을 발생시켰는데, 이는 국민총생산(GDP)의 0.5%에 달하는 금액이다. 행정정보공유추진위원회, 『2007 행정정보 공

[그림 2-1-2] 기관별 구비서류 징구현황(2005년 기준)²⁰⁹⁾



또한, 행정 공무원이 업무처리를 위하여 여러 기관의 정보를 활용하여야 하는 경우, 서면으로 정보보유기관에 협조를 요청하거나 민원인에게 증명서를 첨부하도록 요구하는 방식을 취할 수밖에 없었는데 이러한 방식으로는 업무효율을 높이는 데 한계가 있음은 물론이다. 아울러 기관별로 정보시스템을 구축하여 동일한 정보를 여러 기관에서 중복적으로 수집·관리하는 경우 그만큼 예산과 노력의 낭비가 발생하게 된다.

[표 2-1-2] 민원사무 1건 당 구비서류 종수 현황(2005년 10월 말 기준)

(단위 : 건)²¹⁰⁾

민원사무	1종	2종	3종	4종	5종	6종	7종 이상
4,642 (100%)	1,107 (24%)	937 (20%)	784 (17%)	656 (14%)	374 (8%)	261 (6%)	523 (11%)

동이용 백서』(행정정보공유추진위원회, 2007. 12), 21면.

209) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』(행정정보공유추진위원회, 2007. 12), 21면.

210) 행정정보공유추진위원회, □□2007 행정정보 공동이용 백서□□(행정정보공유추진위원회, 2007. 12), 26면.

이에 따라 업무프로세스를 혁신하여 행정의 능률을 향상하고 민원 서비스를 획기적으로 개선한다는 목적 하에 범정부적인 정보공유체계를 구축할 필요성이 제기되었다. 이를 통하면 민원인이 제출해야할 각종 구비서류를 제출하지 않아도 민원처리부서에서 전자시스템을 통해 확인하여 처리하고, 각종 정책정보 등을 공공기관 상호간에 공동 활용하는 것이 가능하다.

2) 추진현황

① 시스템 구축²¹¹⁾

2000년 1월 구 행정자치부는 행정정보 공동이용 활성화를 위해 행정기관의 시스템을 서로 연계하여 필요한 정보를 다량으로 주고받을 수 있도록 지원하는 행정정보 중계시스템을 개발·운영하고, 2002년 11월에는 민원서비스혁신(G4C)시스템을 구축하여 민원담당 공무원이 민원처리를 위하여 주민등록정보 등 20종의 행정정보를 기관 간 공동이용을 통하여 실시간으로 열람할 수 있도록 하였다.

그리고 2003년 8월부터는 ‘행정정보 공동이용 확대’를 전자정부사업의 핵심과제로 선정·추진하고, [표 2-1-3]과 같이 행정정보 공동이용 기관과 공동이용 대상 정보를 꾸준히 확대하여 왔다. 특히, 2006년 8월 행정정보 공동이용 확대를 안정적으로 지원하기 위해 [그림 2-1-3]과 같이 G4C시스템에서 행정정보 공동이용 기능을 분리하여 행정정보공동이용시스템을 별도로 구축하고 기존에 구축한 행정정보 중계시스템²¹²⁾도 기능을 고도화하는 작업을 수행하였다.

211) 감사원, 『감사결과 처분요구서 -행정정보 공유 및 관리실태-』 (감사원, 2008. 5), 3-4면에서 요약정리 해 놓은 내용을 인용함.

212) 60개 중앙행정기관, 248개 지방자치단체, 20개 공공기관이 연계되어 있다.

[표 2-1-3] 행정정보공용이용시스템의 단계별 확대구축 사업 현황²¹³⁾

단계별	행정정보 공유기반 구축사업 (2005년 12월 ~ 2006년 8월)	범정부 행정정보 공유체계 구축사업 (2006년 9월 ~ 2007년 3월)	행정정보 공동이용 확대 구축사업 (2007년 11월 ~ 2008년 6월)
이용기관	□□모든 행정기관 □□국민연금관리공단, 한국전력공사 등 5 개 공공기관	□□모든 행정기관 □□43개 공공기관 □□우리은행, 기업은행 등 2개 금융기관	□□모든 행정기관 □□61개 공공기관 (예정) □□14개 금융기관 (예정)
공유정보	34종	42종	66종

[그림 2-1-3] 행정정보 공유시스템 구성도



213) 행정정보공유추진위원회, □□2007 행정정보 공동이용 백서□□(행정정보공유추진위원회, 2007. 12), 31면.

② 이용현황

위 행정정보공동이용시스템을 통하여 행정기관 등에서 주민등록등본 등 66종의 구비서류를 열람할 수 있게 되었다([표 2-1-5] 참조). 또한, [표 2-1-4]와 같이 행정정보 공동이용 건수도 2003년의 1,737만 건에서 2007년의 5,103만 건으로 큰 폭으로 증가하였다.

[표 2-1-4] 연도별 행정정보 공동이용 실적 (단위:만 건)

구 분	2003년	2004년	2005년	2006년	2007년
행정정보공동이용시스템	306	499	844	2,368	2,786
행정정보중계시스템	1,431	1,901	1,653	1,885	2,317
계	1,737	2,400	2,497	4,253	5,103

[표 2-1-5] 2008년 9월 확대 66종 구비서류 목록

1	주민등록등(초)본	34	국내거소사실증명
2	토지대장	35	특허등록원부
3	임야대장	36	실용신안원부
4	지방세납세증명서	37	디자인등록원부
5	자동차납세증명서	38	상표등록원부
6	개별공시지가확인서	39	공장등록증
7	건축물대장등본	40	폐기물위탁처리신고필증
8	건축물사용승인서	41	선박원부
9	자동차등록원부	42	상훈수여증명서
10	이륜자동차사용신고필증	43	건설기계등록증
11	건설기계등록원부	44	건설기계검사증
12	호적등본	45	건설기계사업신고증
13	건물등기부등본	46	건설업등록증
14	법인등기부등본	47	건축사업무신고필증
15	토지등기부등본	48	부동산등기용등록번호증명
16	국세납세증명서	49	지적도
17	사업자등록증	50	임야도

18	소득금액증명	51	석유판매업등록증
19	납세사실증명	52	선박검사증서
20	휴업사실증명	53	선박국적증서
21	폐업사실증명	54	(어선)등록필증
22	국가유공자정보(보훈대상)	55	수출입신고필증
23	병적증명서	56	어업면허증
24	출입국사실증명	57	사업장폐기물배출자신고필증
25	외국인등록사실증명	58	폐수배출시설설치신고필증
26	건축허가서	59	외국인부동산등기등록증명
27	국가기술자격증	60	자동차등록증
28	운전면허증	61	개인인감증명
29	취업지원대상자증명	62	법인인감증명
30	국민기초생활수급자증명	63	토지이용계획확인원
31	장애인등록증	64	재산세토지분과세증명서
32	여권정보	65	재산세건물분과세증명서
33	해외이주신고확인서	66	재산세주택분과세증명서

(3) CCTV 설치현황

공공장소의 CCTV는 주로 교통단속이나 범죄예방(방범용)을 위해서 설치되었다.

공중화장실이나 공중목욕탕 등에 CCTV가 설치되어 프라이버시 및 인권침해 논란이 이는 등 사회적 물의를 일으키기도 했지만 어두운 골목길에 파수꾼으로 작용하거나 범인을 잡고 때로는 무고를 입증하는 유용한 도구로 작용하면서 그 설치를 놓고 찬반양론이 팽팽하게 갈리는 것도 사실이다.

그렇지만 CCTV를 통해 개인의 화상정보(개인정보)가 무작위로 수집되며, 이를 악용하면 개인의 일거수일투족을 추적하고 감시하는 수단으로 이용할 수 있기 때문에 범죄예방이나 교통단속 등 구체적 목적달성을 위해 필요한 범위 내에서만 이용할 수 있게끔 제한할 필요는 있다.

또한 그간에는 명확한 법적 근거가 없이 행정목적 달성을 위해 임의적으로 설치·운영되어 왔음도 문제점으로 지적된다.

이에 따라 □□공공기관의 개인정보보호에 관한 법률□□을 개정하여 공공기관의 CCTV에 대한 설치 및 운영에 대한 본격적인 법적 규제의 토대를 마련하였다.

우선 개인정보의 범위를 현행 ‘컴퓨터에 의해 처리되는 정보’에서 ‘컴퓨터 및 CCTV에 의해 처리되는 정보’까지 확대하여 화상정보도 수집부터 이용·제공 및 파기까지 개인정보에 준하는 수준으로 관리될 수 있도록 하였다.

아울러 무분별한 CCTV의 설치를 방지하기 위해 범죄예방·교통단속 등 공익을 위해 꼭 필요한 경우에 한해 공청회 등 대통령령이 정하는 절차를 거쳐 관련 전문가 및 이해관계인의 의견을 수렴한 후 설치하도록 제한하였다.

또한 CCTV의 운영과정에서는 과도한 촬영 등에 의한 개인정보 침해를 방지하기 위해 설치목적의 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추지 못하도록 하고, 녹음기능은 사용하지 못하도록 금지하였다.

부정한 목적으로 이를 위반할 경우에는 2년 이하의 징역 또는 700만원 이하의 벌금에 처하도록 처벌규정을 마련하였다. 한편 공공기관의 장이 CCTV를 설치할 경우에는 정보주체가 이를 쉽게 인식할 수 있도록 설치목적 및 장소, 촬영범위 및 시간, 관리책임자 및 연락처가 담긴 안내판을 설치하도록 하였다.²¹⁴⁾

현재 경찰, 지방자치단체 등에서 범죄예방, 쓰레기투기 단속 등을 위해 전국적으로 약 13만 여대의 CCTV가 설치·운영 중에 있다.

214) 행정자치부, 『희망대한민국 행정자치부 정책백서 (2003~2007)』 (행정자치부, 2008. 2), 350-351면.

[표 2-1-6] 공공기관 CCTV 설치현황(2007년 6월 기준)²¹⁵⁾

구 분		대 수
범죄예방(34.8%)	방법용	45,112
환경개선(1.6%)	쓰레기투기방지	2,117
일반시설관리(34.8%)	시설물관리	41,611
	주차관리	3,451
교통안전(8.6%)	교통정보수집	3,033
	교통단속	8,084
특수시설관리(18%)	재난·산불관리	6,549
	공항·항만관리	831
	기차·지하철안전관리	16,033
기타(2.2%)	기타	2,911
합 계		126,821

3. 효용성 평가

(1) 개인정보처리의 일반적 효용성

컴퓨터로 처리되는 개인정보는 관리 및 이용의 측면에서 이전과 비교할 수 없는 효율성을 가진다. DBMS(Database Management System)의 활용으로 인해 개인에 대한 정보의 처리가 신속하고 효율적으로 이루어질 뿐 아니라, 표준식별번호(universal identification number)에 의한 컴퓨터결합(computer matching)을 통해 분산되어 있는 개인정보들을 용이하고 효율적으로 통합·처리할 수 있다.

215) 위의 책, 350면.

그 효율성이 어느 정도인지는 과거 수기로 신청서를 작성하여 민원을 처리하던 때를 상기하면 쉽게 짐작할 수 있다. 예컨대, 법의 개정으로 인해 복지혜택의 부여기준이 변경되었다고 가정해보자. 담당공무원은 기존에 받아두었던 수많은 수기의 신청서류를 다시 꺼내 하나 하나 들여다보며 적격여부를 판별해내든지, 아니면 일정한 신청기간을 정하여 다시금 수기로 된 신청서를 받아 업무를 처리해야 했다. 개인정보를 비롯한 행정정보의 거의 대부분을 컴퓨터로 처리하게 된 지금은 몇 번의 클릭으로 적격여부를 쉽게 그리고 신속하게 추려낼 수 있다.

이뿐만 아니다. 사회보장혜택의 수급자로 선정되었지만 후에 재산상황이나 가족관계가 변경되어 결격사유가 발생한 경우, 기존에는 민원인이 결격사유를 자진신고하지 않는 한 그러한 상황을 담당공무원이 파악하는 것이 쉽지 않았다.

그렇지만 현재는 행정정보 공동이용을 통해 정기적으로 이를 모니터링하고 수급자선정의 지속여부를 판명하게 된다. 또한 수급신청인의 진술이나 제출한 서류의 진위여부 등도 쉽게 판별해낼 수 있다. 즉, 복지혜택을 부적격자에게 제공함으로써 예산이 낭비되는 것을 막고 이렇게 낭비될 예산을 보다 향상된 복지서비스에 투자할 수 있게 되었다. 이른바 ‘복지사기’의 방지는 물론 효과적인 자원배분에도 기여하는 것이다.

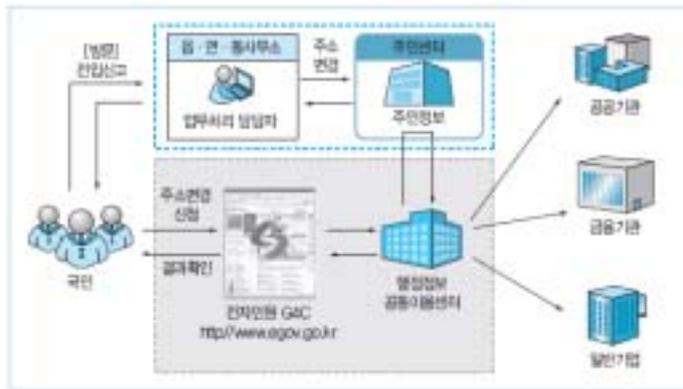
이러한 효율성은 개인정보 공동이용을 통해 여러 행정기관이 각각이 보유한 개인정보를 공유할 수 있음에 따라 보다 구체화되고 극대화된다. 개인정보 공동이용의 효율성은 아래에서 항을 바꿔 설명한다.

(2) 전자민원 G4C의 효율성

G4C(Government for Citizen)는 일명 “통합전자민원창구”라 할 수 있다. 주민이 직접 공공기관에 방문하지 않고도 인터넷상에서 각종 증

명서를 발급받거나 열람해 볼 수도 있고 주민등록증분실신고 등 간단한 민원을 처리할 수도 있다. 아울러 주소변경 알리미 서비스²¹⁶⁾, 주민등록증진위확인서비스, 인감증명발급사실확인의 부가서비스도 제공 받을 수 있다.

[그림 2-1-4] 주소변경 알리미 서비스²¹⁷⁾



또한 기존에는 공공기관의 업무시간 이외에는 민원업무를 처리할 수 없었지만 G4C를 이용하면 365일 24시간, 즉 실시간 이용이 가능하다. 이러한 장점 때문에 전자민원창구를 이용하는 수는 매년 꾸준히 늘고 있는 추세이다. [표 2-1-7(a)]과 [그림 2-1-5]에서 한 눈에 확인할 수 있다.

216) 이사 등으로 거주지 또는 우편물수령지를 변경하고자 할 때, G4C의 이 부가서비스를 이용하면 개별 공공기관(금융기관 포함)에 일일이 통보하지 않아도 된다. 행정정보 공유센터와 연계하여 각 대상기관에 전달되기 때문이다.

217) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』 (행정정보공유추진위원회, 2007. 12), 54면.

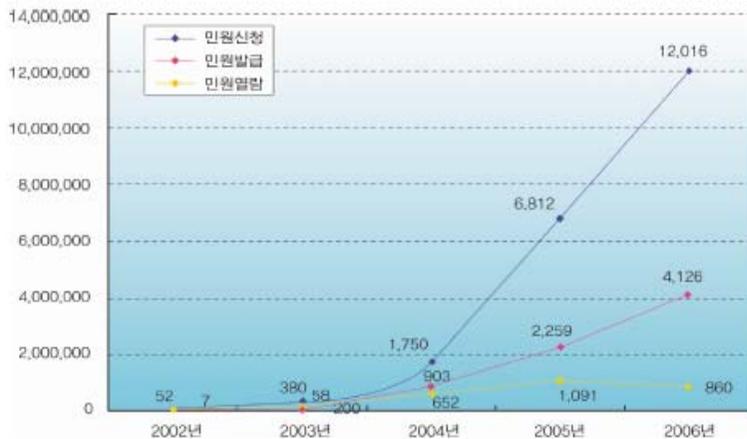
[표 2-1-7(a)] 연도별 전자민원 이용현황²¹⁸⁾

구 분	민원신청		민원발급		민원열람	
	신청건수	평일평균	신청건수	평일평균	신청건수	평일평균
총누계	21,010,647	18,499	7,345,430	8,257	2,810,670	2,353
2006년	12,016,172	46,577	4,126,048	15,428	860,388	3,113
2005년	6,812,076	25,932	2,258,797	8,329	1,091,461	3,860
2004년	1,750,037	6,283	902,759	3,277	652,087	2,300
2003년	380,017	1,353	57,826	786	199,633	702
2002년	52,345	1,103	-	-	7,101	152

* 주민등록증 진위확인 등 부가서비스 : 1,750여만건, 일평균 52,490건

[그림 2-1-5] 전자민원 G4C 민원신청, 발급, 열람 건수

(단위 : 천 건)²¹⁹⁾



218) 행정자치부, 『희망대한민국 행정자치부 정책백서 (2003~2007)』 (행정자치부, 2008. 2), 101면.

219) 위의 책, 101면.

(3) 개인정보 공동이용의 효용성

1) 신속하고 편리한 민원서비스 제공

앞서 살펴본 [그림 2-1-2]와 [표 2-1-2]에 따르면, 민원처리를 위하여 행정기관이나 금융기관은 다수의 증빙서류를 요구하고, 대개 그러한 증빙서류는 다른 기관에서 발급하는 것이 대부분이어서 국민들은 민원 한 건을 처리하기 위해 여러 곳의 행정기관을 방문해야만 했다. 그러나 국가가 보유하고 있는 행정DB를 연계하게 되면, 행정·공공·금융기관이 이 정보를 공동이용함으로써 필요한 구비서류를 민원인으로부터 제출받지 않아도 된다. 국민의 입장에서는 행정기관 방문횟수를 줄여 시간과 비용을 절약함은 물론 보다 신속한 서비스를 제공할 수 있으며, 한 장의 신청서 작성으로 민원을 처리하는 편리함을 맞출 수 있다(e하나로민원서비스).

대출신청 서류준비(5종 이상 서류 필요) : 1 ~ 5일 → 즉시
인·허가 서류준비(2~7종 서류 필요) : 3 ~ 10일 → 즉시

2) 사회적 비용 절감

행정정보 공동이용으로 국민들의 손에 의해 유통되고 있는 구비서류를 줄이게 되면 연간 4억 4천만통의 종이증명서 중 약 67%인 2억 9천만통을 절약할 수 있을 것으로 보인다.²²⁰⁾

행정안전부 정보화전략실은 홈페이지를 통해, 2007년 한 해 동안 행정정보 공동이용으로 8,700만 건의 구비서류를 절감할 수 있었고, 이

220) 행정정보공유추진위원회, 『행정정보 공동이용 백서』 (행정정보공유추진위원회, 2007. 12), 23면.

를 통해 약 5,400억원의 사회적 비용을 절약하는 효과를 얻었다고 밝혔다.²²¹⁾

[표 2-1-7(b)] 행정정보 공동이용에 따른 비용절감 효과²²²⁾

성과유형	성과지표	측정방법	정량적 효과
정부 효율성	민원처리 비용절감	<ul style="list-style-type: none"> · 공동이용건수 x 건당 발급 감축시간 x 시간당 평균임금 - 공동이용건수 : 48,700천 건 - 감축시간 : 0.05시간 - 평균임금 : 8,700원(공무원) 	211.8억원
고객 만족도	방문비용 절감	<ul style="list-style-type: none"> · 공동이용건수 x (처리교통비 + 처리시간 x 시간당 임금) - 공동이용건수 : 48,700천 건 - 처리교통비 : 900원 - 처리시간 : 35분 - 시간당임금 : 8,200원 	2,768억원
	발급비용 절감	<ul style="list-style-type: none"> · 공동이용건수 x 건당 발급비용 - 공동이용건수 : 48,700천 건 - 건당 발급비용 : 100원 적용 	48.7억원

* 공동이용건수는 본사업의 서비스 기간인 2006년 9월부터 2007년 7월까지의 이용건수로 계산하였음

3) 행정업무 혁신

행정정보 공동이용을 통해 대민서비스의 개선뿐만 아니라 업무프로세스의 혁신을 가져올 수 있다는 점에서도 그 효율성을 찾을 수 있다.²²³⁾ 예컨대, 행정기관에서 업무를 처리하기 위해 여러 기관의 정보

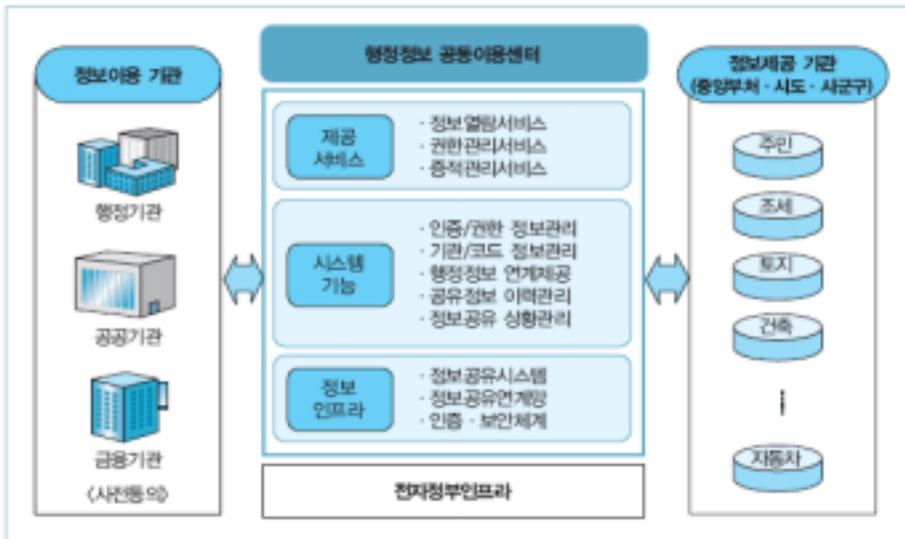
221) 행정안전부 정보화전략실 홈페이지, <http://www.mopas.go.kr/gpms/view/korea/korea_index_vm.jsp?cat= bonbu/elet&menu=elet_08_02_04> 참조.

222) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』 (행정정보공유추진위원회, 2007. 12), 106면.

223) 위의 책, 23-24면.

를 조회하거나 참고해야 하는 경우, 공문을 통해 각 정보보유기관에 협조를 요청하게 되면 공문발송 및 취합의 과정에서 이미 많은 시일이 소요되어 업무효율성이 매우 떨어진다. 범정부적인 행정정보공동이용체계의 구축은 이러한 단점을 극복하여 부처간, 민관간 협업기반의 막힘없는 업무처리를 구현할 수 있다.

[그림 2-1-6] 행정정보공동이용센터 개념도²²⁴⁾



4) 내실 있는 대민서비스 제공

정보공동이용이 활성화되면 일선 창구에서의 증명서 발급업무가 줄어든다. 이에 따라 증명서 발급업무를 담당했던 인력들을 대민서비스 제공업무에 재배치함으로써 한층 더 내실 있는 서비스 제공이 가능해진다.

224) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』 (행정정보공유추진위원회, 2007. 12), 56면.

4. 위험성 평가

(1) 설문조사결과

앞서 밝힌 개인정보처리의 효용성에도 불구하고, 우리 국민은 공공기관이 개인정보DB를 구축하거나 그것을 다른 기관과 공유하는 것, 그리고 행정정보의 공동이용에 대하여 일반적으로 부정적인 입장을 보였다. 설문의 전반적인 결과가 공공기관의 개인정보처리에 대하여 상당한 정도의 불신을 드러냈다. 구체적인 설문조사결과를 살펴보면 아래와 같다.

1) 개인정보DB 구축에 대한 부정적 입장

정부의 각 기관이 개인정보DB를 구축하고 이용하는 것에 대하여 일반인과 전문가 모두 위험하고 불쾌하다는 항목에 높은 지지를 보였다. 주의 깊게 보아야 할 점은 설문내용이 ‘소관업무 수행 외의 목적’으로 DB를 구축이나 이용하는 것의 위험성이나 불쾌감을 묻은 것이 아니라 ‘소관업무의 수행을 위하여’ DB를 구축하거나 이를 이용하는 것이 어떠한지를 물었음에도 위험하고 불쾌하다고 답한 점이다.

사실 이들 기관은 소관업무 수행을 위하여 개인정보DB를 구축하고 이용하는 것이 필수적이다. 그럼에도 불구하고 이렇듯 부정적인 입장을 드러낸 것은 그동안 우리 정부가 이에 관하여 충분한 신뢰를 주지 못한 것이 주요한 이유일 것으로 판단된다. 예컨대 교육행정정보시스템(NEIS) 사태에서도 정보분리의 원칙, 개인정보처리시스템의 공개의 원칙 등 여러 개인정보처리원칙의 위반여부가 문제되었었고 그에 따라 개인정보처리의 오남용 가능성과 위험성이 강하게 지적된 바 있다.²²⁵⁾ 또한 작금의 여러 개인정보유출사건으로 인하여 예민해진 정서

225) 교육행정정보시스템(NEIS)에 대한 헌법적 평가에 관해서는 이인호, “학생의 정

를 반영하는 것이기도 하다.

[설문내용] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 위험하다고 생각하십니까?

[설문내용] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 불쾌하다고 생각하십니까?

① 일반인 조사 결과

일반인을 대상으로 조사한 결과 소관업무 수행을 위하여 개인정보DB를 구축하거나 이용하는 것이 위험하고 불쾌하다는 의견이 75%에 가까웠다. 일반인 대상 조사에게 특이한 점은 ‘잘 모르겠다’는 의견이 위험하지 않다거나 불쾌하지 않다는 의견보다 많은 점이다. 전문가 대상 조사에서는 ‘잘 모르겠다’는 의견이 상대적으로 적었던 것과는 대조된다. 일반국민들은 정부기관이 개인정보DB를 구축하고 이용한다는 것이 어떠한 위험을 가져올 수 있는지 그 의미를 충분히 파악하지 못할 수도 있다.

[표 2-1-8] 개인정보DB 구축 및 이용의 위험성 및 불쾌감(일반인 대상)

(base : 1000명, 단위 %)

	그렇다	그렇지 않다	잘 모르겠다
개인정보DB 구축의 위험성	74.5	5.0	20.5
개인정보DB 구축의 불쾌감	74.8	11.7	13.7

보프라이버시와 교육행정정보시스템(NEIS)”, 『인권과 정의』 제329호(대한변호사협회, 2004. 1) 참조.

② 전문가 조사 결과

일반인 대상 설문조사결과와 비교했을 때, 전문가 그룹은 보다 위험성을 높게 평가하고 불쾌감은 상대적으로 낮게 평가했다. 전체의 85.37%가 위험성이 높다는 의견에, 65.85%가 불쾌하다는 의견에 동조했다.

[표 2-1-9] 개인정보DB 구축 및 이용의 위험성 및 불쾌감(전문가 대상)

(base : 41명, 단위 %)

	그렇다	그렇지 않다	잘모르겠다
개인정보DB 구축의 위험성	85.37	12.20	2.44
개인정보DB 구축의 불쾌감	65.85	26.83	7.32

2) 개인정보DB 공유에 대한 부정적 입장

이미 구축해놓은 개인정보DB를 ‘정당한 업무수행을 위하여’ 다른 기관과 공유하는 것이 위험하거나 불쾌하다고 생각하는지를 묻는 설문에서 일반인과 전문가의 85% 이상이 그렇다고 답하였다. 수치적으로 보면 개인정보DB의 구축과 구축한 기관이 이를 이용하는 것보다 다른 기관과 공유하는 것이 더 위험하고 불쾌하다는 입장을 나타내, DB의 구축 및 이용 보다는 구축한 DB를 공유하는 것에 더욱 민감한 반응을 보이고 있음을 알 수 있다.

또한 정당한 업무수행을 위하여 DB의 공유가 필요하고 경우에 따라서는 필수적일 수도 있는데 이에 대하여 부정적 반응을 보이는 것은 앞서 살펴본 바와 같이 아직까지 우리 정부가 국민의 개인정보를 정당하고 필요한 목적 범위 내에서만 수집·이용·공유한다는 점에 대해 충분한 신뢰를 주지 못했기 때문인 것으로 판단된다.

[설문내용] 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 위험하다고 생각하십니까?

[설문내용] 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 불쾌하다고 생각하십니까?

① 일반인 조사 결과

일반인의 88.4%가 개인정보DB의 공유가 위험하며, 86.9%가 이에 대해 불쾌감을 느끼는 것으로 드러났다. 개인정보DB의 구축 및 이용에 대하여 약 75%가 부정적인 반응을 보였던 것을 감안하면 ‘공유’에 더욱 민감한 것을 알 수 있다.

[표 2-1-10] 개인정보DB 공유의 위험성 및 불쾌감(일반인 대상)

(base : 1000명, 단위 %)

	그렇다	그렇지 않다	잘 모르겠다
개인정보DB 공유의 위험성	88.4	3.8	7.8
개인정보DB 공유의 불쾌감	86.9	5.0	8.1

② 전문가 조사 결과

전문가의 경우 위험성 평가에서는 90% 이상이 위험하다고 응답해 일반인에 비하여 보다 민감한 반응을 보였지만 불쾌감 정도는 근소한 차이로 일반인에 비하여는 낮은 수치를 보였다. 또한 위험하다는 의견비율도 일반인보다 높은 반면, 위험하지 않다는 비율도 일반인보다 높았음도 특이한 점이다.

[표 2-1-11] 개인정보DB 공유의 위험성 및 불쾌감(전문가 대상)

(base : 41명, 단위 %)

	그렇다	그렇지 않다	잘 모르겠다
개인정보DB 공유의 위험성	90.24	7.32	2.44
개인정보DB 공유의 불쾌감	85.37	12.20	2.44

3) 정부의 개인정보처리의 오·남용가능성에 대한 높은 평가

개인정보처리와 관련하여 정부의 오·남용가능성은 일반인과 전문가의 82.9%가 그 가능성이 높다고 평가했다. 그러한 가능성이 없다는 의견은 일반인 1.2%, 전문가 4.88%로 매우 낮은 수치를 보였다. 이러한 오·남용가능성으로 인하여 정당한 소관업무 수행을 위한 DB의 구축 및 이용, 공유에 모두 부정적인 반응을 보인 것으로 판단된다.

[설문내용] 정부의 개인정보처리 관련해서 오·남용 가능성은 얼마나 된다고 생각하십니까?

① 일반인 조사 결과

30%에 가까운 인원이 개인정보처리의 오·남용 가능성이 매우 높으며, 50% 이상이 그 가능성이 높다는 의견을 보였다. ‘가능성이 없다’는 의견이 1%, ‘전혀 가능성 없다’는 의견이 0.2%인 것을 감안하면 매우 높은 수치임을 알 수 있다.

[표 2-1-12] 개인정보처리의 오·남용 가능성(일반인 대상)

(base : 1000명, 단위 %)

	매우 가능성 높다	가능성 높다	보통이다	가능성 없다	전혀 가능성 없다
오남용 가능성	29.2	53.7	15.9	1.0	0.2

② 전문가 조사 결과

전문가 조사에서는 ‘매우 가능성 높다’는 의견이 34.15%, ‘가능성 높다’는 의견이 48.78%로, 일반인을 대상으로 한 설문조사에 비하여 ‘매우 가능성 높다’는 의견이 상대적으로 높았다.

[표 2-1-13] 개인정보처리의 오·남용 가능성(전문가 대상)

(base : 41명, 단위 %)

	매우 가능성 높다	가능성 높다	보통이다	가능성 없다
오남용 가능성	34.15	48.78	12.20	4.88

4) 정부의 개인정보처리의 오·남용시 위험성에 대한 높은 우려

개인정보처리의 오·남용시 위험성이 어느 정도인지를 묻는 설문에서 일반인의 89.4%, 전문가의 92.68%가 위험하다고 응답하였다. 오·남용의 가능성보다 그것이 오·남용되었을 때의 위험성을 높게 평가한 셈이다. 이러한 결과는 오·남용시 위험성이 크기 때문에 그 가능성을 사전에 차단하는 것이 개인정보와 관련하여 정부에 대한 국민의 신뢰도를 높일 수 있다는 방법임을 시사한다.

[설문내용] 정부에서 개인정보처리가 오·남용 되었을 경우 얼마나 위험하다고 생각하십니까?

① 일반인 조사 결과

일반인을 대상으로 한 설문조사결과, ‘매우 위험하다’는 의견은 44.2%, 위험하다는 의견은 45.2%를 보였다. 이에 반해, ‘위험하지 않다’는 의견은 0.8%, ‘전혀 위험하지 않다’는 의견은 0.1%로, 위험하지 않다는 의견은 전체의 1%도 되지 않았다.

[표 2-1-14] 개인정보처리의 오·남용시 위험성(일반인 대상)

(base : 1000명, 단위 %)

	매우 위험하다	위험하다	보통이다	위험하지 않다	전혀 위험하지 않다
오남용시 위험성	44.2	45.2	9.7	0.8	0.1

② 전문가 조사 결과

전문가를 대상으로 한 설문조사결과, ‘매우 위험하다’는 의견은 53.66%로 과반수를 넘어선다. 전문가의 경우 일반인의 경우보다 위험성을 더욱 높게 평가하였다고 볼 수 있다.

[표 2-1-15] 개인정보처리의 오·남용시 위험성(전문가 대상)

(base : 41명, 단위 %)

	매우 위험하다	위험하다	보통이다	위험하지 않다
오남용시 위험성	53.66	39.02	4.88	2.44

5) 수집목적 이외 다른 기관에의 제공에 대한 인식

정부의 각 기관들이 자신의 소관업무의 수행을 위해서 개인정보DB를 구축해서 이를 이용하고 있는데, 그 개인정보를 소관업무 수행목적 이외에 다른 기관에게 제공하는 것을 허용하느냐를 묻는 설문에서 일반인과 전문가 모두 원칙적으로 부정적인 입장을 보였다. 그러나 이 경우에도 수사기관에 제공하는 것은 상대적으로 긍정적인 반응을 보였다는 점이 특이하다.

[설문내용] 정부의 각 기관들은 자신의 소관업무의 수행을 위하여 관련 국민의 개인정보를 수집하여 각각 개인정보DB를 구축하고 이를 관리·이용하고 있습니다. 자신의 소관업무 수행목적 이외에 국민의 개인정보를 다른 기관에게 제공하는 것은 허용되어야 한다고 생각하십니까?

[설문내용] 앞의 질문에서 제공받는 기관이 수사기관이라고 한다면 그 정보제공에 대하여 어떻게 생각하십니까?

① 일반인 조사 결과

정부기관에서 수집한 개인 정보를 다른 정부 기관에 제공하는 행위에 대해서는 53.7%가 절대 허용 안 된다고 응답하고 있으며, 33.4%는 사전 동의가 있으면 허용된다고 답하였다.

그러나 정부기관이 수집한 개인 정보를 수사기관에 제공하는 것에 대하여는 다른 정부기관(53.7%)에 제공하는 것에 비해 낮은 15.8%가 절대 허용이 안 된다고 응답하여, 수사기관에 제공하는 것에 대해서는 보다 수용적인 것으로 나타났다.

[표 2-1-16] 수집목적 이외 다른 기관에의 제공(일반인 대상)

(base : 1000명, 단위 %)

	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부시 더 이상 제공 않는다는 전제 하에 허용	법률에 따른 것이면 허용	다른 기관의 목적이 정당한 업무수행이면 허용
전 체	53.7	33.4	7.4	4.3	1.2

[표 2-1-17] 수집목적 이외 수사기관에의 제공(일반인 대상)

(base : 1000명, 단위 %)

	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부시 더 이상 제공 않는다는 전제 하에 허용	법률에 따른 것이면 허용	공익 목적이기 때문에 자유롭게 허용
전 체	15.8	50.7	12.0	20.5	1.0

② 전문가 조사 결과

정부기관에서 수집한 개인 정보를 다른 정부 기관에 제공하는 행위에 대해서 전문가들은 일반인(53.7%)에 비해 낮은 29.3%가 절대 허용 안 된다고 응답하였고, 사전 동의 있으면 허용된다고 답한 비율이 29.3%로 나타났으며, 법률에 따른 것이면 허용된다고 응답한 비율이 36.6%로 높게 나타났다.

한편, 수사기관에 제공하는 행위에 대해서 전문가들은 일반인(15.8%)과 유사한 17.1%가 절대 허용 안 된다고 응답하였고, 사전 동의 있으면 허용된다고 답한 비율이 26.8%로 나타났으며, 법률에 따른 것이면 허용된다고 응답한 비율이 43.9%로 높게 나타났다.

[표 2-1-18] 수집목적 이외 다른 기관에의 제공(전문가 대상)

(base : 41명, 단위 %)

		사례 수 (명)	절대 허용 안됨	사전 동의 있으면 허용	사후 거부시 더 이상 제공 않는다는 전제 하에 허용	법률에 따른 것이면 허용	다른 기관의 이용목적이 정당한 업무수행이라면 조건 없이 허용
전체		41	29.27	29.27	2.44	36.59	2.44
직업군	기업근로자	13	38.46	30.77	7.69	23.08	0.00
	법학교수	16	18.75	31.25	0.00	50.00	0.00
	법실무가	12	33.33	25.00	0.00	33.33	8.33

[표 2-1-19] 수집목적 이외 수사기관에의 제공(전문가 대상)

(base : 41명, 단위 %)

		사례 수 (명)	절대 허용 안됨	사전 동의 있으면 허용	사후 거부시 더 이상 제공 않는다는 전제 하에 허용	법률에 따른 것이면 허용	공익 목적이기 때문에 자유롭게 허용
전체		41	17.07	26.83	7.32	43.90	4.88
직업군	기업근로자	13	30.77	15.38	15.38	38.46	0.00
	법학교수	16	12.50	31.25	0.000	50.00	6.25
	법실무가	12	8.33	33.33	8.33	41.67	8.33

6) 소관업무의 수행을 위한 다른 기관과의 공유에 대한 인식

정부의 각 기관들이 보유하고 있는 개인정보를 서로 공유함으로써 민원업무의 신속한 처리나 제출 서류의 간소화 등 많은 이점이 있음을 지적하면서, 그러한 개인정보의 공유에 대하여 설문한 결과 일반인과 전문가 모두 그에 대하여 다소 소극적인 반응을 보였다. 편리함의 이면에 있을 수 있는 개인정보처리 오·남용 가능성을 의식했기 때문인 것으로 추측된다.

[설문내용] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인 정보를 각 정부기관들이 자신의 소관업무의 수행을 위하여 공유하는 것에 대하여 어떻게 생각하십니까? (민원업무의 처리가 빠르고 행정 기관에 필요한 서류를 제출하지 않아도 되는 이점이 있는 반면, 개인 정보의 오·남용이 있을 수도 있음)

[설문내용] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 금융기관의 업무수행을 위하여 금융기관들과 공유하는 것이 필요하다고 생각하십니까? (금융기관 이용자는 금융기관에 제출하여야 하는 서류를 줄일 수 있고 금융기관은 이용자가 제출한 정보가 진실한 것인지를 확인할 수 있는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

① 일반인 조사 결과

정부의 각 기관 상호간은 물론 정부와 금융기관의 개인정보 공유에 대하여 전체 설문조사대상자의 60%이상이 바람직하지 않거나 불필요하다는 의견을 보였다.²²⁶⁾

[표 2-1-20] (정부→정부) 개인정보 공유에 대한 태도

(base : 1000명, 단위 %)

	매우 바람직하다	바람직하다	그저 그렇다	바람직하지 않다	전혀 바람직하지 않다
정부→정부	0.1	6.9	30.7	45.4	16.9

226) 특이한 점은 행정정보공유추진위원회가 발간한 2007 행정정보공동이용백서에서의 국민인식조사결과가 본 설문결과와 차이를 보인 것이다. 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』 (행정정보공유추진위원회, 2007. 12), 83면. 백서에서의 국민인식조사결과를 살펴보면 아래와 같다.

행정정보 공동이용 공공기관 및 금융기관 확대에 대한 평가 :

- (1) 공공기관 확대에 대한 의견 - 반드시 필요하다(12.5%), 필요하다(77%), 그저 그렇다(10%), 필요하지 않다(0.5%), 전혀 필요하지 않다(0%)
- (2) 금융기관 확대에 대한 의견 - 반드시 필요하다(10%), 필요하다(57.9%), 그저 그렇다(23.9%), 필요하지 않다(10%), 전혀 필요하지 않다(0%)

[표 2-1-21] (정부→금융기관) 개인정보 공유에 대한 태도

(base : 1000명, 단위 %)

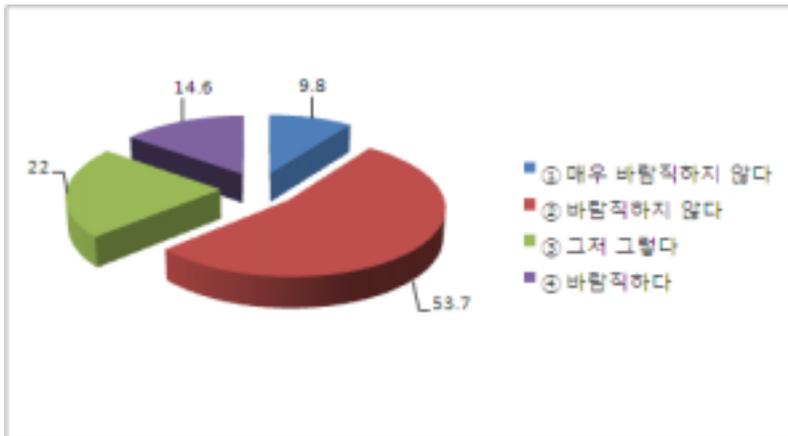
	반드시 필요하다	필요하다	그저 그렇다	필요하지 않다	전혀 필요하지 않다
정부→금융기관	0.6	10.1	26.8	40.8	21.7

② 전문가 조사 결과

전문가를 대상으로 한 설문결과 역시 일반인과 크게 차이를 보이지 않았다. 전체 설문조사대상자의 60%이상이 바람직하지 않거나 불필요하다고 응답했다. 일반인대상 설문결과와의 차이점이라면 정부와 금융기관간의 공유에 대해 보다 민감한 반응을 보인 것이다.

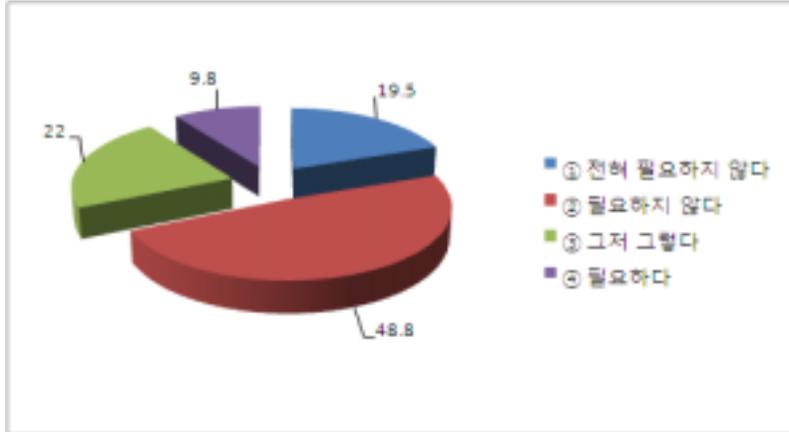
[그림 2-1-7] (정부→정부) 개인정보 공유에 대한 태도

(Base : 41명, 단위 %) 평균(점) 2.41



[그림 2-1-8] (정부→금융기관) 개인정보 공유에 대한 태도

(Base : 41명, 단위 %) 평균(점) 2.22



(2) 개인정보침해의 위험성 증가

1) 담당공무원에 의한 다량의 정보유출 가능성

2008년 9월을 뜨겁게 달궜던 GS칼텍스 개인정보유출²²⁷⁾은 회사 내부자에 의한 것으로 밝혀졌다. 업무담당자에 의한 개인정보유출은 민간부문에서만 일어날 수 있는 것은 아니다.

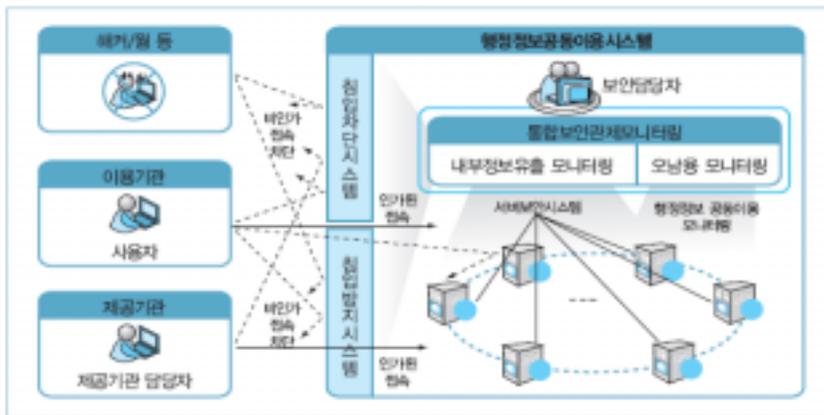
감사원의 감사결과도 지적하고 있듯이 행정정보공유시스템을 이용하여 담당공무원이 타인의 개인정보를 사적으로 무단 열람하는 경우가 발생하고 있다.²²⁸⁾ 담당공무원에 의한 정보유출이 행정정보공유시스템을 이용할 때 비로소 나타나는 문제점은 아니다. 그렇지만 자신

227) 우리나라 전체 성인인구와 맞먹는 1125만 명의 개인정보가 담긴 DVD와 CD가 서울 강남의 유흥가 골목길에서 발견되었다. 그 안에는 이름, 주소, 전화번호, 이메일 주소는 물론, 주민등록번호까지 포함되어 있었다. 범인은 GS칼텍스의 자회사 직원 등 회사 내부 관련자였으며, 그들은 자신의 고객정보 데이터베이스(DB) 접근 권한을 이용해 2008년 7월초부터 한 달 동안 자신의 업무용 컴퓨터에 고객의 개인정보를 다운받았다고 한다.

228) 감사원, 『감사결과 처분요구서 -행정정보 공유 및 관리실태』 (감사원, 2008. 5) 참조.

이 근무하는 기관의 DB만을 볼 수 있었던 기존과는 달리 행정정보공유시스템을 이용하게 되면 타기관이 소장 내지 보유하고 있는 개인정보에까지 접근이 가능하게 된다. 그렇게 되면 한 번의 정보유출로 기존의 몇 배에 달하는 엄청난 피해를 불러올 수도 있다.

[그림 2-1-9] 내부통제 개념도²²⁹⁾



결국 각 기관의 내부통제는 필수적이라 할 수 있다. 내부정보가 유출되지는 않는지, 정보를 오·남용하고 있지는 않는지 모니터링할 수 있는 시스템을 갖추고 있어야 한다. [그림 2-1-9]는 행정정보공유시스템의 내부통제 개념도이다.

이 개념도 상으로는 내부통제가 적절히 이루어질 것으로 보이지만, 감사원의 감사결과는 그렇지 않다. 감사원은 오·남용에 대한 모니터링이나 점검이 적절히 이루어지지 않아 행정정보 오·남용을 완전하게 방지할 수 없어 주민등록정보 등 개인정보의 유출 소지가 있으며 그로 인해 시스템의 안전성과 신뢰도 저하가 예상된다고 하면서 행정안전부장관으로 하여금 이에 대해 개선방안을 강구할 것을 요구하

229) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』(행정정보공유추진위원회, 2007. 12), 128면.

였다.²³⁰⁾ 이하 사례에서는 신문 기사화되었던 몇 개의 사건을 간략하게 정리해보았다.

< 사 례 >

- ▶ ○○시 공무원은 ○○신용정보회사에 근무하는 아내의 부탁으로 동료 직원의 ID를 이용하여 근무시간에 주민등록 등·초본 10만여건을 발급받아 아내에게 전달 <연합뉴스 05.3.8>
- ▶ 전직 경찰관 출신의 개인정보판매상 손○○는 평소 알고 지내는 경찰관에게 개인적으로 필요한 것처럼 주민조회결과를 요청하고, 경찰관 장○○는 2회에 걸쳐 주민조회결과 유출 <연합뉴스 05.3.3>
- ▶ 시 공무원 박○○는 평소 알고 지내던 김○○에게 심부름업자 정○○가 요청한 채무자의 개인정보를 알려주고, 김○○는 심부름업자 정○○에게 일정액을 받고 개인정보를 판매 <노컷뉴스 05.3.10>
- ▶ 졸업앨범 제작업자 및 학교 행정실 직원이 이름, 생일, 가정환경 등이 기록된 아동환경실태조사서 등의 학생정보를 인터넷화상업체 등에 판매 <주요언론 05.2.3>

2) 보안의 문제

2005년에는 전자민원창구인 G4C를 통해 발급받는 문서를 간단한 방법으로 위·변조할 수 있음이 밝혀짐에 따라 서비스의 보안문제가 제기된 바 있다. 결국 서비스제공이 일정기간 중단되고 정부는 행정정보공동이용시스템을 G4C에서 분리하기에 이른다. 최근에도 이와 비슷한 문제가 제기되었다. 2008년 8월 새로 도입된 전자여권에서 단 몇 분 만에 개인정보가 유출될 수 있는 것으로 드러났기 때문이다. 전국 41개 인권단체로 구성된 인권단체연석회의는 2008년 9월 29일 비접촉식(RFID) 리더기를 이용해 전자여권 내의 신상정보를 컴퓨터로 불러들이는 시연을 해보였다.²³¹⁾ 이를 토대로 시민단체는 “한국의 여

230) 감사원, 『감사결과 처분요구서 -행정정보 공유 및 관리실태-』 (감사원, 2008. 5), 46-48면.

231) 프레스시안, “전자여권, 10분이면 감쪽같이 ‘해킹’ - 인권단체, 위·변조 위험 노출된 여권 폐기해야”, (2008. 9. 29.), <<http://www.pressian.com/scripts/section/article.asp?>

권에는 평생 바꿀 수 없는 주민번호 정보가 들어 있는 데다 2년 뒤엔 지문 인식까지 포함될 것으로 예정돼 유출시 훨씬 더 심각한 문제가 된다”며 “이제라도 외교통상부는 이미 발급한 전자여권을 파기해야 한다”고 주장했다.

또한 인터넷상에서 주민등록번호를 사용하지 않고도 행정기관 및 민간 홈페이지에서 본인임을 확인할 수 있는 수단인 공공 I-PIN²³²⁾에 의하여도 개인정보가 유출될 수 있다는 주장이 제기되었다. 공공 I-PIN은 Government Personal Identification Number의 약자로, 인터넷상 개인 식별번호를 의미한다. 행정안전부는 본인정보는 본인확인기관식별정보를 포함한 13자리 난수이며, 본인확인기관 식별정보 이외에 개인정보가 전혀 포함되어있지 않다고 설명해왔다. 그러나 한나라당 이정현 의원(문화체육관광방송통신위원회)이 최근 50개의 사이트를 조사한 결과에 따르면, 행정안전부의 공공 I-PIN(G-PIN)의 경우 20개 사이트에서 ID가 노출됐고, 22개 사이트에서는 본인확인 정보가 드러났다.²³³⁾ 한 번 부여받으면 평생 바꿀 수 없는 주민등록번호와 달리 공공 I-PIN은 유출되었을 경우 언제든지 변경 및 폐기가 가능하기는 하지만, 그것이 개인정보를 보호하며 본인확인을 가능하게 한다는 본래의 기능을 제대로 살리지 못한다면 문제가 있다.

결국 이와 같은 보안의 문제들, 즉 발달하는 기술로 인하여 쉽든 어렵든 시스템에서 개인정보가 유출될 수 있다면, 또는 시스템상의 정보들이 위·변조된다면 큰 혼란이 초래될 것임은 분명하다. 아무리 철저한 보안시스템을 갖추어도 해킹의 위험성은 늘 도사리고 있다.

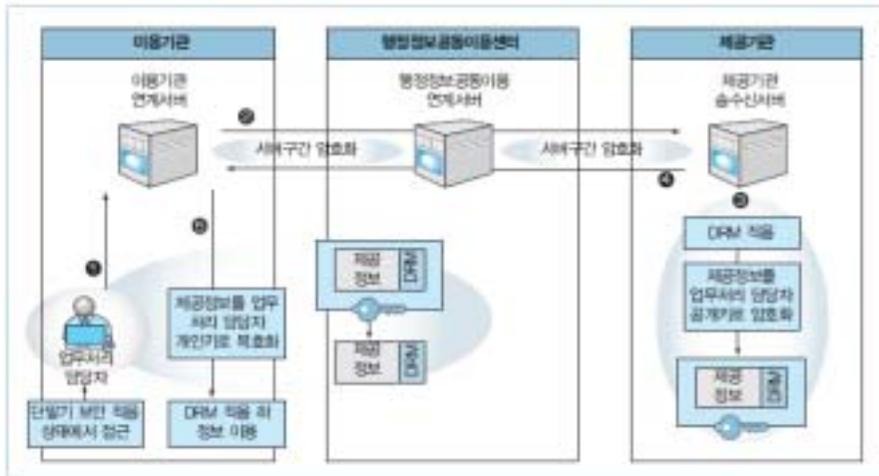
article_num=60080929141547>.

232) <<http://www.g-pin.go.kr/>> 참조.

233) 또한 행정안전부의 공공 I-PIN은 5개의 테스트 아이디 중 노출 빈도가 가장 높았다. 아시아경제, “‘대체 주민번호’ 아이디도 개인정보 유출된다” (2008. 10. 1), <<http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=277&aid=0002036731>>.

이러한 위험성에 대비하여 적절한 법·제도적 안전장치를 갖추는 것이 필요하다. 2005년 G4C의 경우를 상기하면, 행정정보공동이용센터의 경우도 보안체계가 적절한지 여부에 의문을 가질 수 있다. [그림 2-1-10]은 행정정보공동이용센터의 정보유통구간 암호화 개요이다. 행정정보공동이용센터를 통해 유통되는 정보는 모두 암호화하여 유통되고, 이용기관이 직접 제공기관의 DB에 접속하여 정보를 열람하는 것은 아니라는 점을 드러낸다. 이 개념도를 보면 보안수준이 높은 것처럼 보일 수 있다. 그러나 문제는 행정정보공동이용센터 안에는 증적관리시스템이 구축되어있는데, 그 증적관리시스템에 이용기관이 확인한 정보가 축적된다는 데에 있다. 그 정보는 물론 암호화된 상태로 보관되지만 그 시스템 자체가 해킹되어 암호가 풀렸을 경우에는 큰 피해를 불러올 수 있다. 아울러 이는 정보처리의 원칙 중 정보분리의 원칙에도 위반된다.

[그림 2-1-10] 유통구간 암호화 개요²³⁴⁾



234) 행정정보공유추진위원회, 『2007 행정정보 공동이용 백서』 (행정정보공유추진위원회, 2007. 12), 93면.

3) 개인정보보호정책에 있어서 인식 부족

2008년 9월 23일 행정안전부가 원유철 의원(한나라당)에게 제출한 ‘개인정보 보호 관련 인력 및 예산보고서’에 따르면 작년 개인정보보호 관련 업무를 담당할 인원은 8명에 예산은 8억원에 불과했다. 이는 지난해 정보화 관련 전체 예산 4187억원 가운데 0.2%에 해당하는 것으로, 8억원 가운데서도 인건비 등 개인정보보호 사업과 직접적인 관련이 없는 일반수용비가 6억2000만원으로 대부분을 차지했다.

한편 지난해 국가사이버안전센터가 접수·처리한 공공기관 사이버 침해사고는 총 7588건으로 전년도에 4286건에 비해 77% 증가했다. 특히 지난해 지방자치단체에서 발생한 사이버 침해사고는 총 3827건으로 2006년의 1470건에 비해 3배 가까이 늘었고 교육기관도 1464건에서 2148건으로 50% 정도 증가한 것으로 나타났다.²³⁵⁾

최근 신문기사 중 일부이다. 개인정보보호와 관련된 예산이 정보화와 관련된 예산에 0.2%에 불과하다는 사실은 정부가 개인정보보호에 어느 정도의 비중을 두고 정책을 수행하는지를 여실히 보여준다고 하겠다. 특히 공공기관에 의한 개인정보침해 사건이 급격히 증가하고 있음을 감안하면, 우리 정부의 정책은 정보화의 추진에만 급급했을 뿐 그 역기능을 최소화할 수 있는 정책을 적절히 병행하지 못했다고 볼 수 있다. 또한 비밀번호 설정 등 최소한의 안전성 확보조치도 없이 개인정보를 CD 등 매체로 공유하고 있어 개인정보 유출위험이 상존한다는 감사원의 감사결과²³⁶⁾는 개인정보보호 차원에서 인식제고가 필요함을 보여준다. 우리나라 전체 성인인구와 맞먹는 1125만 명의 개인정보가 유출된 GS칼텍스 정보유출 사건이 불러온 사회적 파장²³⁷⁾

235) 디지털 타임스, “공공기관 개인정보보호 예산 턱없어, 작년 8억원 ... 전체 예산의 0.2% 불과” (2008. 9. 24.), <http://www.dt.co.kr/contents.html?article_no=2008092502010351630009>.

236) 감사원, 『감사결과 처분요구서 -행정정보 공유 및 관리실태-』 (감사원, 2008. 5), 44면.

237) 이와 관련하여 정보유출 피해자들이 GS칼텍스를 상대로 손해배상을 청구하는 수십억대 집단소송이 제기됨은 물론, 개인정보보호와 관련한 사회적 관심을 증폭시켰다. 법무부는 개인정보 유출을 막기 위해 범죄신고자나 피해자가 서류를 작성할 때 주민등록번호를 쓰지 않도록 관련법 개정을 추진하고 있어 주목된다. 법률신문, “범죄신고 등 서류 작성 ... ‘주민번호’ 안 쓴다” (2008. 9. 18.), <<http://www.lawtimes>.

으로 미루어 짐작해보면 고의든 아니든 그것으로 인한 정보유출은 심각한 사회문제가 될 것이다. 민간기업의 경우, 거래당사자인 개인이나 회원가입을 한 개인에 관한 정보(기록)이지만 공공기관의 경우 국민 전체가 그 대상이 될 수 있다는 점에 위험성은 배가된다.

[표 2-1-22] 오프라인(이메일 포함) 자료공유 현황(단위: 건)²³⁸⁾

제공 기관	이용기관	자료명	제공 주기	제공 방법	비밀번호 또는 암호	수령 방법	자료건수 (2006년)
구 해양수산부	관세청	선원선박자료	분기	CD	X	등기우편	4,191
구 행정자치부	통일부	주민등록자료	월	USB	X	직원수령	100,000
	구 농림부	토지대장자료	수시	CD	X	직원수령	20,000,000
	국세청	주민등록변경자료	월	CD	X	직원수령	1,386,215
	근로복지공단	거소조회자료	월	디스켓	X	직원수령	40~50
구 건설교통부	소방방재청	건축물대장자료	월	CD	X	직원수령	16,875,431
검찰청	관세청	관세범처분결과	월	공문	X	공문첨부	3,750
	구 국가청렴위원회	공직자부패범죄기소자료	반기	이메일	문서압호	이메일	579
경찰청	병무청	운전면허취득·취소자료	월	공문	문서압호	공문첨부	260,000
	구 국가청렴위원회	공직자직무비리자료	반기	이메일	문서압호	이메일	403
대법원	국세청	사망자호적자료	반기	CD	X	직원수령	254,370
16개 광역시·도	국세청	건설기계등록자료	분기	CD	X	직원수령	333,654
16개 시·도 교육청	병무청	검정고시합격자	분기	디스켓	문서압호	등기우편	10,000

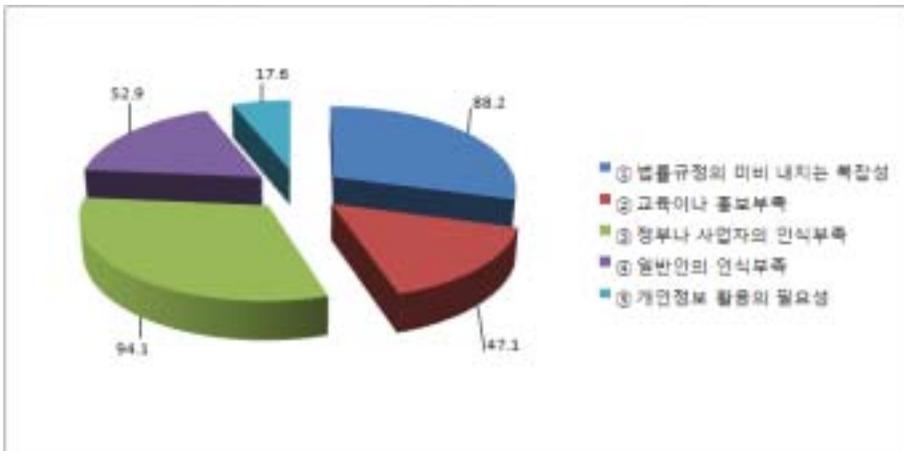
co.kr/LawNews/News/NewsContents.aspx?serial=42343>. 또한 행정안전부 역시 법무부와 같은 정책을 추진하고 있다.

238) 감사원, 『감사결과 처분요구서 - 행정정보 공유 및 관리실태-』 (감사원, 2008. 5), 63면.

[그림 2-1-11]은 개인정보가 제대로 보호되고 있지 않는 이유를 묻는 전문가대상 설문조사 결과이다. [그림 2-1-11]은 i) 법률규정의 미비 내지는 복잡성, ii) 교육이나 홍보부족, iii) 정부나 사업자의 인식부족, iv) 일반인의 인식부족, v) 개인정보 활용의 필요성의 다섯 가지 이유 중 정부나 사업자의 개인정보보호에 대한 인식부족이 현재 개인정보보호에 가장 큰 장애요인이 될 수 있음을 시사한다. 이렇듯 개인정보보호 인식 수준이 낮은 상태에서는 아무리 편리하고 좋은 시스템을 운영한다 할지라도 그에 따른 위험성은 상쇄되지 않을 것이다.

[그림 2-1-11] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유

(Base : 그렇지 않다+ 매우 그렇지 않다 34명, 단위 %, 복수응답)



[설문내용] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이라고 생각하십니까 1순위부터 3순위까지 응답하여 주십시오.

5. 소 결

전자정부의 핵심요체는 바로 효율성이다. 그러나 그러한 효율성은 국민의 신뢰를 담보하지 않고는 의미가 없다.²³⁹⁾ 그 신뢰란 바로 우리

²³⁹⁾ 홍준형, “전자정부와 개인정보보호”, 『정보과학회지』 제22권 제11호 (한국정보과

의 정보가 보호받고 있다는 신뢰를 말한다. 특히 정보통신기술이 비약적으로 발전하여 개인정보가 자유로이 유통되는 환경에서 이러한 신뢰를 확보하지 못한다면 정부는 그 어떠한 정보화 정책도 실패할 수밖에 없다. 11대 전자정부 사업의 핵심을 이루었던 교육행정정보시스템(NEIS) 사태는 이 점을 드러낸 가장 극적인 사례였다. 문제는 그 신뢰를 어떻게 확보하느냐이다. 우선은 정보처리원칙을 확립하고 규범화해야 할 것이다. 아울러 정부가 그러한 정보처리원칙을 지키지 않았을 때 개인이 이에 대등하게 맞설 수 있는 강력한 정보권을 법적으로 보장 또는 개선하는 것이 필수불가결하다.

또한 위에서 살펴본 바와 같이 개인정보DB의 구축, 그리고 그것을 기관상호간에 공유함으로써 민원처리시간이 단축되고 행정서비스가 질적으로 개선되는 반면, 행정정보의 오·남용 및 행정정보의 유출 등으로 개인정보침해가능성이 증가하였다. 따라서 행정정보의 공동이용에 대한 일정한 제한과 한계 설정이 요구되며, 그것이 규범으로 수렴될 것이 요청된다.²⁴⁰⁾

요컨대, 이제 고도정보사회로 진입하는 길목에서 정보화로 인한 위험성을 최소화하면서 개인정보처리의 이익과 가치를 극대화할 수 있는 규범적 척도를 찾아내는 것이 우리 사회의 시급하고도 절실한 과제가 되었다.²⁴¹⁾

이하의 논의는 그 규범적 척도를 찾아내고 그 척도를 바탕으로 현행의 법제를 평가하여 대안을 제시하는 것으로 구성될 것이다.

학회, 2004. 11), 64면.

240) 이민영, “개인정보보호법제의 개편논의와 개선방안”, 『정보통신정책연구』 제16권 제1호(정보통신정책연구원, 2004. 1), 31면.

241) 이인호, “공공부문 개인정보보호법제에 대한 분석과 비판”, 『정보법학』 제6권 제1호(한국정보법학회, 2002. 7), 30면.

제 2 절 기업의 개인정보처리의 효용성과 위험성

1. 기업의 개인정보처리의 실태

개인정보 공급자인 개인들을 대상으로 하여 개인정보를 제공하는 목적이나 정보를 제공함에 있어서 우려하는 사항 및 프라이버시 침해 정도 등에 대한 실태조사는 많이 이루어져 왔으나, 개인정보의 수요자 중 하나인 기업들을 대상으로 한 개인정보 수집과 활용 등에 대한 실태조사는 많이 이루어지지 않고 있는 상황이다.

정보화 사회에서 개인정보는 이미 기업의 주요자산으로 자리 잡은 지 오래다. 고객의 개인정보는 고객 중심형의 마케팅을 전개하는데 가장 기초가 되는 정보이다. 불특정 다수 고객들을 대상으로 제품과 서비스를 판매하는 매스마케팅(mass marketing)에서 나아가 개별 고객에게 특화된 제품과 서비스를 제공하는 1:1 마케팅 및 개별고객과의 관계관리(CRM: customer relationship management)를 수행하기 위해서는 고객에 대한 데이터 수집이 필수적으로 선행되어야 한다. 고객이 제공한 개인정보를 토대로 고객의 다양한 성향을 분석하여야 고객이 원하는 제품의 제공, 다양한 맞춤서비스, 양질의 맞춤 콘텐츠 제공 및 제품 및 서비스의 업데이트가 가능하다. 이러한 이유로 인해 기업들은 고객들의 정보를 수집하고 적절하게 활용하기 위해 많은 노력을 기울이고 있다. 기본 인적사항과 관련된 정보 이외 소비유형, 소득수준, 구매이력, 라이프스타일 등에 대한 고객 정보를 여러 경로를 통하여 수집하고 이렇게 수집한 개인정보를 컴퓨터와 인터넷을 통해 디지털 파일로 만들어 다양한 형태의 마케팅 활동에 활용하고 있다.

우리나라의 경우 미국이나 유럽 등과 같은 선진국에 비하여 고객 데이터를 활용한 정확한 타겟 마케팅이나 고객관계관리 역량이 부족한 편이다. 이는 개인정보의 수집과 업데이트에 많은 비용이 들기 때

문이다. 국내 많은 기업들이 고객정보에 기반을 둔 맞춤형 마케팅과 고객관계관리의 중요성을 인식하고는 있으나 아직까지 고객 데이터를 제대로 수집하고 활용하고 있는 분야는 신용카드사, 은행 등의 금융권과 백화점 등의 유통점, 그리고 이동통신업종 등으로 제한되어 있는 상황이다.²⁴²⁾

(1) 기업의 개인정보 수집 현황

1) 수집 방법 및 수집 내용

기업들은 개인정보를 수집하기 위해 여러 방법들을 활용하고 있다. 상품 구매 시 개인정보 등록을 유도하거나 마케팅 캠페인, 홈페이지 회원 가입 등의 수단을 통해 기업 자체적으로 고객들의 정보를 수집하기도 하지만 자체적인 고객정보의 수집이 어려울 경우 그룹사로부터 제공받거나 타사나 전문명부 업자로부터 개인정보를 구입하기도 한다. 우리나라 기업들을 대상으로 개인정보 수집방법에 대한 실태 조사는 이루어지지 않고 있으나 고객에 대한 정보를 얻고 있는 방법이 일본 기업들과 비슷하다는 가정 하에 일본 기업들의 실태를 살펴 보도록 하겠다. [표 2-1-23]²⁴³⁾을 보면 2005년의 경우 기업이 자체적으로 개인정보를 수집하는 경우 수집방법은 ‘거래 정보로서 축적(59.2%)’, ‘상품구입자 등록(38.0%)’, ‘양케이트(32.1%)’ 등의 순으로 나타났으며 ‘그룹사로부터의 제공(11.8%)’, ‘거래처에서의 위탁(42.3%)’도 높은 비중을 차지하고 있다. 특히 ‘거래처로부터의 위탁’의 비중이 2005년의 경우 2004년의 21.5% 대비 97%가 증가하였다.

242) 한국정보산업연합회(2006, 2007), “CRM Fair 2006, 2007”

243) 경제산업성, 『경제산업분야 사업자의 개인정보보호에 관한 대처 실태조사』 (2007), 13면(채승완, “일본의 개인정보보호체계와 개인정보의 경제적 가치□□, 『한일 경상논집』 (2007), 69면)에서 재인용.

[표 2-1-23] 기업의 개인 정보 수집방법

수집방법	2004년(%)	2005년(%)
거래정보로서 축적	68.1	59.2
이벤트 참가자 등록	25.3	22.5
상품구입자 등록	46.0	38.0
양케이트	24.0	32.1
그룹사로부터 제공	8.1	11.8
캠페인	11.1	15.0
타사로부터 구입	0.7	1.0
거래처에서의 위탁	21.5	42.3
전문 명무업자로부터의 구입	1.6	1.0
홈페이지	18.6	24.8
기타	12.0	11.4

캠페인이나 이벤트 등을 통한 개인정보의 수집은 기업의 입장에서 상당한 비용지출이 수반된다. 따라서 포털이나 온라인 쇼핑몰 등 온라인 기업들 이외 많은 오프라인 기업들도 상대적으로 수집 비용이 저렴한 자사의 홈페이지를 통한 개인정보 수집을 적극적으로 활용하고 있다. [표 2-1-23]에서 나타난 것처럼 홈페이지를 활용하여 개인정보를 수집하는 비율이 2004년의 18.6%에서 2005년에는 24.8%로 증가하였다.

산업 영역별로 국내 대표 기업들의 홈페이지를 통한 고객정보 수집 현황은 [표 2-1-24]에 제시되어 있다.²⁴⁴⁾ 기업마다 약간의 차이는 있으나 개인이 홈페이지에서 회원으로 가입할 때 제공해야 하는 정보는

244) 각사 홈페이지 참고

이름, 로그인ID, 비밀번호, 자택 전화번호, 자택 주소, 휴대전화번호, 이메일, 직업, 결혼여부, 기념일, 법정대리인정보, 주민등록번호, 취미, 보유 차량, 해당기업 서비스 이용기록 등이고 이러한 제공 정보 이외 고객들의 접속 IP 정보를 활용하고 있는 기업들도 있다. 대부분의 기업들은 여러 고객정보를 선택할 수 없는 필수 사항으로 하여 작성하게 하고 있으나, 온라인 포털 및 온라인 쇼핑몰 중 일부 기업은 고객정보를 필수와 선택사항으로 나누어 수집하고 있다. 수집된 정보는 회원관리, 마케팅 및 광고에 활용, 새로운 서비스 제공 및 요금 결제 등에 활용된다고 설명하고 있다.

홈페이지를 통한 개인정보 수집 시 많은 기업들이 고객들에게 개인정보제공여부를 선택할 수 없도록 하고 있다. [표 2-1-24]에서 조사된 대부분의 기업들의 홈페이지에 개인정보제공 동의 선택 여부 항목이 있기는 하지만 개인정보 제공에 동의 선택을 하지 않을 경우 회원으로 가입할 수가 없는 상황이라 이용자들은 사이트의 서비스를 이용하기 위해 어쩔 수 없이 고객정보 이용에 동의하여야 한다. 또한 많은 기업들이 패밀리 사이트 동시 가입을 회원 등록 의무사항으로 명시하고 있다. 삼성전자, LG전자, 삼성생명, KT, LG 텔레콤 등 많은 대기업 사이트가 가입 시 최고 11개 사이트의 동시가입을 요구하고 있다. SC제일은행, 국민은행, 기아자동차, GM대우, KTF멤버스, 다음 등은 자세한 설명 없이 조사라는 명목으로 사용자의 인터넷 사용정보인 쿠키정보, IP 주소, 접속로그 등을 수집하고 있다.²⁴⁵⁾

기업정보 공유의 대상을 불분명하게 명시하거나 포괄적으로 명시하여 이용자의 동의를 받고 있는 기업들도 있다. 삼성생명은 리서치 업체, 이벤트 대행업체 등으로 대상기업을 명확하게 명시하지 않고 있고 SK 엔크린 사이트는 수십 개의 정보공유 및 위탁업체를 명시하고 있다. 개인정보의 제3자 제공 동의 요청시 이용목적에 따른 구분동의

245) 강진규, “기업, 개인정보 수집에만 혈안,” 『디지털 타임스』, 2008.9.21일자.

없이 일괄 동의를 받고 있는 기업들이 대다수이며 광고마케팅에 개인 정보를 이용한다는 내용에 동의를 해야 회원으로 가입할 수 있다. 인터파크, SK 엔크린, KTF 등 몇 개 기업만이 회원가입과 별개로 제 3 자에의 마케팅 활용 동의를 받고 있다.

최근 소비자들의 검색엔진 활용 빈도의 증가 및 소셜네트워크사이트(social network site)의 이용자가 급증함에 따라 이들 사이트의 개인정보보호 수준에 대한 관심 또한 높아지고 있다. 네이버(Naver), 다음(Daum), 네이트(Nate), 엠파스(Empas), 파란(Paran)과 싸이월드(Cyworld) 역시 가입자가 개인정보 수집 및 활용에 대한 거부권을 행사할 수 없도록 페이지가 구성되어 있다. 즉 약관에 대한 내용에 대해 동의를 거부할 경우 회원가입 자체를 할 수가 없다. 또한 동의해야 하는 항목에 부분적인 선택을 할 경우 강제로 동의할 것을 요구하고 있다. 회원으로 가입을 하지 않을 경우 이메일을 사용할 수 없으며 콘텐츠 및 정보 서비스 이용에 제한을 받게 된다. [그림 2-1-12]와 [그림 2-1-13]은 다음과 네이버의 회원가입을 위해 이용약관 동의 및 개인정보동의를 의무사항임을 보여주고 있다.

[표 2-1-24] 개인들의 홈페이지 회원가입을 통해 기업들이 수집하는 정보현황

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
삼성 전자	이름, 로그인, ID, 비밀번호, 자택 전화번호, 자택주소, 휴대폰 전화 번호, 이메일, 직업, 결혼여부, 기 념일, 법정대리인정보, 주민등록 번호, 서비스 이용기록, 접속 IP정 보, 추천인 ID	회원 관리, 마케팅 및 광고에 활용	동의 선택 항목 有	명시되어 있지 않음	삼성홈 페이지 / 영 삼성닷컴 회원가입, 메일수신, 삼성홈 페이지 / 영 삼성닷컴 이용약관 구분 동의	삼 성 전 자 패밀리 사 이트로 회 원 가입 시 삼 성 전 자 계 열 사 (삼 성 전자, 애 니콜, 삼성 컴 퓨 터 등)에 일 괄 ID 및 PASS WO RD로 부여 (선택사항)
LG 전자	* 필수사항 - 이름, 로그인, ID, 비밀번호, 자택 전화번호, 자택주 소, 휴대폰 전화번호, 이메일, 직	요금정산 콘텐츠 제공, 물 품배송 또는 청구서 등 발 송, 구매 및 요금 결제 외,	동의 선택 항목	명시되어 있지 않음	일괄동의 를 하지 않을 경우	LG 전자 패 밀리 사이 트로 회원

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
	업, 결혼여부, 기념일, 법정대리인 정보, 주민등록번호, 서비스 이용 기록, 접속 IP정보, 추천인 ID * 선택사항 - 직장주소, 직장전화번호, 직장 이메일 주소, 실제생년월일, 직업, 결혼예정시기, 주거평수, 이메일수집여부, 회원가입 동기, 취미	회원관리, 마케팅 및 광고에 활용	有		가입 불가	가입시 LG 전자 계열사 (LG 전자, 싸이언, LG웨딩클럽 등)에 일괄 ID 및 PASS WORD로 부여
SK 텔레콤 (tworld.co.kr)	성명, 주민등록번호, 아이디, 패스워드, 이동전화번호, 주소, 연락전화번호, e-mail, 생일, 직업, 취미	* 개인식별정보: 이름, 주민등록번호, ID, 패스워드 - 서비스 이용에 따른 본인 식별 절차에 이용 *결제관련정보: 은행명, 계좌번호, 예금주명, 신용카드종류, 카드번호, 유효기간, 할부기간, 이동전화번호 - 요금 결제에 이용	동의 선택 항목 有	SK C&C, 유엔젤(주)	일괄동의 를 하지 않을 경우 가입 불가	T WORLD, SK 텔레콤 멤버십 사이트, TTL, Ting 동일한 ID 부여

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
KT	이름, 아이디, 패스워드, 별명, 이메일, 주소, 전화번호, 휴대폰 전화번호	서비스 가입, 변경 및 해지, A/S, 서비스 관련 문의를 포함한 이용계약 관련 사항의 처리와 귀사가 직접 또는 타사와의 업무 제휴 등을 통하여 제공하게 되는 신상품의 소개, 이벤트 안내, 고객 유치, 관리 등을 포함한 각종 마케팅 활동 등에 이용	동의 선택 항목 有	* KT의 계열사 - 케이티프리텔(주), 케이티하이텔(주), 케이티네트웍스(주) * 출자회사 - 케이에스콜(주), 코스앤씨(주), 한국콜센터(주), 티엠월드(주), 유엠S&C(주), 한국디지털위성방송(주),(유)가원아이앤비 (주) 텔스타커뮤니케이션	일괄동의 를 하지 않을 경우 가입 불가	
현대 자동차	성명, 주민등록번호, 아이디, 비밀번호, 아이디/비밀번호찾기 문답, 휴대/자택/직장전화, 이메일, 자택/	서비스제공을 위한 계약의 성립 (본인식별 및 본인의사 확인 등),	동의 선택	명시되어 있지 않음	일괄동의 를 하지 않을 경우	

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
	직장주소, 직장명/부서명, 보유차량정보, 취미, 직업, 서비스이용기록, 쿠키	서비스의 이행 (상품배송 및 대금결제 등), 기타 새로운 서비스, 신상품이나 이벤트 정보 안내	항목 有		가입 불가	
기아 자동차	이름, 생년월일, 로그인ID, 비밀번호, 비밀번호 질문과 답변, 자택전화번호, 자택 주소, 휴대전화번호, 이메일, 직업, 회사명, 회사전화번호, 취미, 결혼여부, 기념일, 주민등록번호, 접속 로그, 쿠키, 차량소유여부, 보유차량, 구입희망차종	서비스제공을 위한 계약의 성립 (본인식별 및 본인의사 확인 등)	동의 선택 항목 有	명시되어 있지 않음	일괄동의 를 하지 않을 경우 가입 불가	Q 멤버스 (현대카드, OK캐쉬백, 현대오일뱅크)가입으로 일괄서비스 혜택 제공
인터 파크	* 필수사항 - 희망 ID, 비밀번호, 비밀번호 힌트용 질문과 답변, 성명, 주민등록번호, 주소, 전화번호, 이메일주소, 이메일 수신여부 등 * 선택사항 - 회사주소, 회사전화번호, 생년월일, 결혼여부, 결혼기념일, 직업, 월평균소득, 최종학	이용자의 식별, 계약이행에 대한 연락 및 안내 등의 고지, 고객이 주문 상품 및 경품의 대한 배송, 비밀번호를 잊은 경우의 신속한 처리, 고객의 편의를 위한 맞춤형광고의 제공,	동의 선택 항목 有	(주) 인터파크 로지스틱스, (주) 인터파크 CS, (주)인터파크CS China	제3자 마케팅 활용 동의서 구 분 동의	인터파크 패밀리사이트가입시 (주)인터파크, (주)인터파크 I N T,

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
	력, 자녀 수, 차량정보 등	기념일 행사쿠폰 발송 및 서비스 품질향상을 위한 제휴서비스 제공				(주)인터파크 투어에 동일한 ID 부여
네이버 (NHN)	<p>* 필수사항 - 성명, 주민등록번호, 여권번호(외국인에 한함), 아이디, 비밀번호, 본인확인문답, 이메일 주소, 주민등록번호 발급일자</p> <p>* 선택사항 - 주소, 연락처</p>	서비스 이용에 따른 민원 사항의 처리를 위한 본인 식별, 신용평가기관을 통한 실명확인, 중복가입확인, 연령제한 서비스의 제공, 고객센터의 운영, 부정 이용 방지, 고지사항 전달, 본인 의사확인, 불만처리 등 의사소통 경로의 확보, 새로운 서비스나 신상품, 이벤트 정보 등 최신 정보 안내, 청구서, 경품 등 물품배송 시 정확한 배송지의 확보, 인구통계학적 분석자료(이용자의 연령별, 성별, 지역별 통계분석) 등을 위하여 사용	동의 선택 항목 有	NHN 서비스(주), NHN 게임즈(주)	일괄동의 를 하지 않을 경우 가입 불가	

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
다음	<p>* 필수사항 - 이름, 생년월일, 성별, 로그인ID, 비밀번호, 자택 전화번호, 자택 주소, 휴대전화번호, 법정대리인정보(어린이/학생회원), 서비스 이용기록, 접속 로그, 쿠키, 접속 IP 정보</p> <p>* 선택사항 - 취미, 결혼여부, 주민등록번호, 학력, 신용카드 정보, 은행계좌 정보, 결제기록, 최종학력, 소속, 자녀수, 외국인등록번호</p>	서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산, 회원관리, 마케팅 및 광고에 활용	동의 선택 항목 有	주식회사 MPC, (주)다음서비스	일괄동의 를 하지 않을 경우 가입 불가	회원 가입 시 회원인증을 거쳐야 함 (실명, 휴대폰, 전화번호 인증)
CJ 물	성명, 주민등록번호, 아이디, 비밀번호, 이메일주소, 전화번호, 주소, 은행계좌번호, 신용카드번호	본인 확인 절차 용도, 고지전달, 불만처리나 서비스, 이벤트 정보안내, 유료 정보에 대한 이용 및 상품 구매에 대한 결제	동의 선택 항목 有	명시되어 있지 않음	일괄동의 를 하지 않을 경우 가입 불가	
싸이월드 (SK커뮤니케이션즈)	<p>* 필수사항 - 이름, 주민등록번호, 아이디, 비밀번호, 연락처, 만14세 미만시 법정대리인 정보</p> <p>* 선택사항 - 생년월일, 주소</p>	서비스 제공에 관한 계약 이행 및 서비스 제공에 따른 요금정산, 회원 관리, 마케팅 및 광고에 활용	동의 선택 항목 有	엠피씨, 서비스퀘어	일괄동의 를 하지 않을 경우 가입 불가	

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
아시아 나항공	이름 (한글, 영문), 생년월일 및 주민등록번호, 주소, 전화번호, 전자우편 : 약관의 주요 변경사항, 마일리지 실적, 기타 마케팅 정보 등을 제공하기 위한 정보, 인터넷 아이디와 패스워드, 패스워드 힌트, 국적, 결혼 기념일, 회사명, 직책, 관심분야, 여권번호, 자주가는 나라나 도시 등	서비스제공을 위한 계약의 성립, 서비스의 이행(배송 및 결제 등), 신상품이나 이벤트 정보 안내	동의 선택 항목 有	명시되어 있지 않음	일괄동의 를 하지 않을 경우 가입 불가	아시아나 패밀리 사이트 가입 시 플라이 아시아나, 레디 아시아나, 아시아나 리틀즈, 아시아나 기내 면세점에 동일한 ID 부여(선택 사항)
대한 통운 택배	이름, 로그인ID, 비밀번호, 비밀번호 질문과 답변, 주민등록번호, 자택 전화번호, 자택 주소, 휴대전화번호, 직장전화번호, 이메일 주소	서비스 이용에 따른 민원사항의 처리를 위한 본인확인 절차, 중복가입확인, 고객센터의 운영, 부정이용 방지, 고지사항 전달, 본인 의사확인, 불만처리 등 의사소통 경로의 확보, 서비스 제공	동의 선택 항목 有	명시되어 있지 않음	일괄동의 를 하지 않을 경우 가입 불가	

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
K T F (쇼)	이름, 로그인ID, 비밀번호, 비밀번호 질문과 답변, 주민등록번호, 자택 전화번호, 자택 주소, 휴대전화번호, 직장전화번호, 이메일 주소, 결혼여부, 법정대리인정보, 신용카드정보, 은행계좌, 쿠키 접속 IP정보, 닉네임, 학력, 추천인ID	서비스제공에 관한 계약이행 및 요금정산, 고객관리, 마케팅 및 광고에 활용	동의 선택항 목 有	* KT그룹사 -(주)케이티, KTF M&S, KTH, (주)케이티네트웍스, KT과워텔, *KT그룹과 고객유치, 고객관리 위탁 -(유)가원아이앤비, (주)텔스타커뮤니케이션	K T 그룹사 공동 마케팅 및 제휴사 제공 동의 구분 동의	
SK 엔크린	개인고유정보(성명, 주민등록번호, ID(고유번호), Password(비밀번호), 이메일주소, 주소, 연락처	OK캐쉬백 제휴서비스 제공, 제휴사 또는 가맹점과의 각종 포인트 정산, 공동 마케팅의 수행 및 고객정보 분석을 위해 수집 및 이용	동의 선택항 목 有	* 별도 동의 하에 공개 - OK캐쉬백서비스(주) * 위탁업체 - (주)신세계, (주)	마케팅 위탁업체, 개인정보 3자 제공 은 구분 동의	

제 1 장 개인정보처리의 실태 분석: 효용성과 위험성 평가

기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
				보광훼미리마트, 하이서비스(주), (주)엘비시스템, 이포컴(주), (주)청람커뮤니케이션, SKC&C(주), (주)프라임비즈텔, (주)티엔피네트워크, (주)와이비엘, (주)인플러스, KPB, (주)빌포스트, (주)슈어엠, (주)아레오네트윅, (주)Air-CROSS, OK캐쉬백서비스(주), (주)유비즈토피,		

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

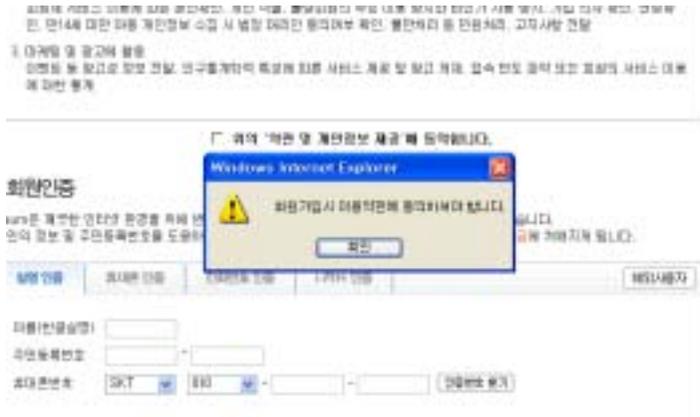
기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
				(주)RTMS		
삼성 카드	<p>* 필수사항 -성명, 웹아이디, 웹패스워드, 자택전화번호, 핸드폰번호, E-mail성명, E-mail수신여부, 자택주소, 본인확인질문, 생일, 결혼여부, 배우자생일</p> <p>* 선택사항 - 직장주소, 직장전화번호, 직업, 차량보유, 연소득, 주거형태, 주이용업소, 부동산보유액, 주거소유형태, 취미</p>	<p>회원관리 등 회원제 서비스 이용에 따른 본인 확인, 개인식별, 불량회원의 부정 이용 방지와 비인가 사용 방지, 가입 의사 확인, 가입 및 가입횟수 제한, 분쟁 조정을 위한 기록보존, 불만처리 등 민원처리, 고지사항 전달 및 확인, 본인의사 확인 및 원활한 의사소통 등</p>	동의 선택 항목 有	명시되어 있지 않음	일괄동의 를 하지 않을 경우 가입 불가	삼성카드 온라인몰 가입시 삼성카드홈페이, 온라인 쇼핑물 서비스, 여행물 서비스, 생활편의 포털사이트 웨딩 서비스 동일한 ID 부여
삼성 생명	<p>* 필수사항 - 주민등록번호, 성명, 회원ID, 비밀번호, 전화번호, e-mail 주소, 자택주소 등 개인식별정보</p> <p>* 선택사항 - 결혼기념일, 취미 등 부가정보, 기타 홈페이지 접속 정보 및 서비스 이용정보, 금융거</p>	<p>회원가입 및 서비스 이용시 본인의 확인, 고지사항 전달, 본인 의사확인, 불만처리 등 원활한 의사소통 경로의 확보, 회원 관심분야에 따른 각종 개인 맞춤</p>	동의 선택 항목 有	* 개인정보취급위탁 - 인피언컨설팅(주), 삼성 SDS, 리서치업체, 이벤트	마케팅 정보제공 구분 동의	주민등록번호 실명인증 필요

제 1 장 개인정보처리의 실태 분석: 효용성과 위험성 평가

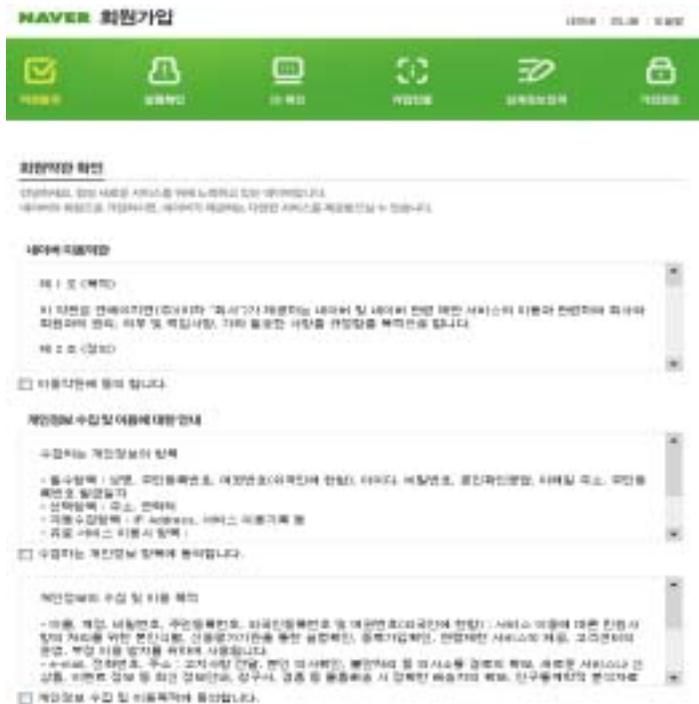
기업명	수집내용	수집목적	동의 선택항 목여부	정보 공유/ 위탁업체	일괄동의 / 구분동의	기타
	래 정보	서비스의 제공		대행업체		

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

[그림 2-1-12] 회원 가입시 이용약관과 개인정보 활용 동의(Daum)

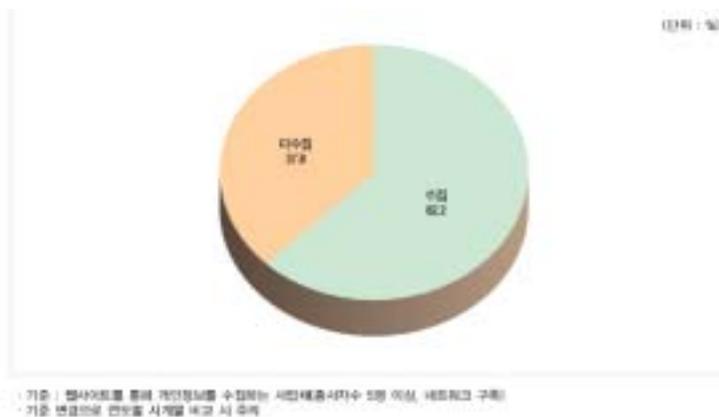


[그림 2-1-13] 회원 가입시 이용약관 및 개인정보 활용 동의(Naver)



[표 2-1-24]에서 조사한 우리나라의 대표적인 대기업들의 경우 비즈니스 분야를 막론하고 개인들의 주민등록번호 정보를 요구하고 있으며 일부 기업의 경우 주민등록번호제공을 선택사항으로 하고 있으나, 회원가입을 위한 사전 본인확인 시 주민등록번호를 입력해야 하므로 사실상 모든 기업들이 개인의 주민등록번호 정보를 수집하고 있다고 볼 수 있다. 한국정보보호진흥원(2007)의 조사에 의하면 웹사이트 상에서 이용자의 본인확인을 위해서 주민번호를 입력하도록 하고 있는 사업체는 62.2%인 것으로 나타났다.²⁴⁶⁾

[그림 2-1-14] 주민번호 수집 여부

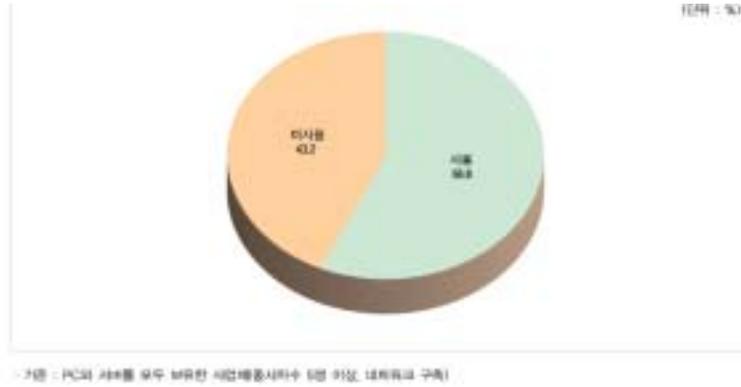


이들 사업체 중 고객의 데이터베이스(DB)를 구축하여 사용하고 있는 비율은 56.8%로 나타났다. 업종별로 살펴보면 금융 및 보험업(73.2%)과 도매업(65.7%)의 DB 사용률이 다른 업종에 비해 상대적으로 높게 나타났다. 규모별로는 종업원 수가 많은 사업체일수록 DB 사용률이 높아지는 것으로 나타났다.²⁴⁷⁾

246) 한국정보보호진흥원, 『2007 정보보호 실태조사, 기업편』 (2007), 131면. 이 조사는 PC와 서버를 모두 보유한 사업체(중사자수 5명 이상, 네트워크 구축)를 대상으로 한 조사임.

247) 한국정보보호진흥원, 『2007 정보보호 실태조사, 기업편』 (2007), 109면.

[그림 2-1-15] DB 구축 사용자



많은 기업들이 웹사이트가 아닌 오프라인 상에서 제품을 구매하는 고객들을 대상으로도 고객정보를 수집하고 있다. 예를 들어 소비자의 자동차 구매 시 작성하게 되는 매매 계약서에 제공되는 개인정보는 이름, 주민등록번호, 사업자 번호, 직업·직장, 주소, 전화번호, 휴대전화 번호, e-메일, 개인거래정보, 거래신용정보, 차량구입정보, 할부금불입정보, 개인신용능력 정보 등이며 개인정보의 제공여부는 개인이 선택할 수 있으나 자신의 정보가 제공되는 업체를 고객들이 선택할 수는 없다. 자동차 구매 시 수집되는 정보는 [표 2-1-25]에서처럼 여러 관련제휴업체와 공유되어지고 있다. 법적으로는 정보제공 후 정보제공 동의를 취소할 수 있으나 실질적으로 취소할 수 있는 방법이 없다는 것이 문제이다. [그림 2-1-16]은 자동차 구매시 작성하게 되는 매매계약서이다.

[표 2-1-25] 자동차 매매 계약 시 제공되는 정보의 공유업체²⁴⁸⁾

구분	공유업체 (제휴관련업체)
현대·기아 자동차	현대캐피탈, 현대카드, 더워런티그룹코리아, GE 캐피탈코리아, 글로비스, 현대백화점, AS 협력업체, 탁송협력업체, 판매대행업체, 보험회사 등
대우자동차	우리디엠에스, 우리캐피탈, 오토114, 서울경매상, 탁송협력업체, 판매대행업체 등

구분	공유업체 (제휴관련업체)
르노삼성자동차	삼성카드, 신한카드, 알씨아이코리아, 탁송협력업체, 판매대행업체
쌍용자동차	제휴관련업체, 탁송협력업체, 판매대행업체 등
재규어·랜드로버	SK네트웍스가 제휴한 주유소, 지역 가맹점 서비스, 이동전화 및 정보통신기기 판매업, 통신서비스업, 스피드메이드, 편의점(OK마트), 디지털사진 인화업(스코피), 패션사업(스마트·타미휠피거·DKNY 등), 와인판매업, 부동산 관련업, 기타 회사가 영위하고 있는 제반 사업

[그림 2-1-16] 현대자동차 매매 계약서(249)



248) 양선희, 한애란, “자동차 살 때 개인정보 줄줄 샌다,” 『중앙일보』, 2008.5.1일자.
 249) 양선희, 한애란, “백화점, 통신회사도 동의서 요구 한번 서명하면 최소화하기 힘들어,” 『중앙일보』, 2008.5.1일자.

삼성전자나 LG전자와 같은 제조업체들은 제품 구매 시 소비자들의 제품등록카드 작성, 프로모션, 서비스, 캠페인 서베이, 콜센터, 판매사원 활용 및 유통업체와의 전략적 제휴를 통해 고객들의 정보를 수집하고 있다. 예를 들어 고객들이 제품등록카드를 작성할 경우 제품 보증기간을 늘여주고 각종 프로모션이나 서베이에 응답하여 고객 정보를 제공할 경우 다양한 인센티브를 제공한다. 제조업의 경우 최종 고객들을 대상으로 하는 직접 판매보다는 유통망을 통해 주로 판매가 이루어지기 때문에 타 업종 대비 고객정보를 수집하기가 어려운 편이다. 전자회사에서 수집하는 고객 정보는 다음과 같다.

[표 2-1-26] 전자회사에서 수집하는 고객정보²⁵⁰⁾

유형	고객정보
기본정보	성명, 주민번호, 성별, 연령, 자택정보, 직업/직장 정보
심리정보	생년월일, 결혼유무, 학력, 취미, 자격증, 소유차종, 주거구분
가족정보	가족 수, 서열, 연령, 가족성명, 가족 주민번호, 가족생년월일, 가족 직업
구매정보	이용점포, 판매점포, 판매상품, 구매액, 구매빈도, 최근 거래정보, 정상판매/세일/특판
신용정보	신용카드 정보, 은행계좌 정보
관측정보	관측행사코드, 매체이용종류, DM발송일/내역, email 발송일/내역, 통신판매 실적
상품정보	상품코드, 상품명, 상품규격, 판매수량
평가정보	누적이용횟수, 고객기여점수, 반응횟수 등

제조업이기는 하나 최종고객들을 상대로 직접 판매를 하는 기업의 경우 상대적으로 고객정보를 수집하기가 용이하다. LG생활건강의 경

250) 전자회사 내부 자료

우 백화점 화장품 브랜드를 대상으로 1998년부터 고객정보를 수집하는 작업을 해왔다. 주요 활용 목적을 고려하여 고객들로부터 필수적으로 확보해야 할 정보를 정의하고, 확보된 정보를 파악한 후 추가로 확보할 정보와 확보방법을 파악하는 등 구체적인 실행방안을 수립한 후 정보를 수집해 오고 있다.²⁵¹⁾

[표 2-1-27] LG생활건강의 DB 구성

활용 목적	필요정보		현정보 현황		확보방법		
	정보유형	상세 Data 항목	기존 확보	신규 확보	판매원	온라인이벤트	구매내역
매장 고객 대응력 제고	인적정보	성명, 주민번호, 주소, 직업					
	피부, 미용정보	피부관심사, 피부타입					
	구매이력 정보	최초구매일, 최종구매일, 구매횟수평균 구매액, 방문 경과기간, 최근 방문매장, 구매상세정보, 선호제품, 재 구매 예상제품					
	고객평가 정보	고객상태, 고객등급					
	캠페인 정보	최근 캠페인정보, 반응정보					
	포인트 정보	적립 포인트, 사용포인트					
	구매 보상 방식 개선	고객선호 정보	고객선호사은품				
	라이프 스타일	취미, 관심분야					

251) 이완수, 허원무, “LG생활건강 백화점 화장품 브랜드 오후의 CRM 전략,” 『한국마케팅저널』 7(1), 2005, 105면.

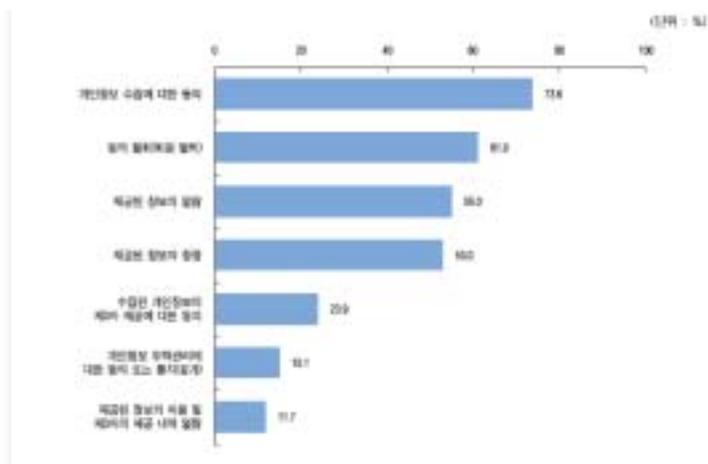
제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

활용 목적	필요정보		현정보 현황		확보방법		
추가 판매 기회 마련	라이프 이벤트	생일, 결혼기념일, 기타					
신규 고객 확보	마케팅	방문계기 (추천, 광고, 캠페인 등)					

2) 개인정보 수집 시 기업의 의무사항 이행 현황

2006년 12월 현재, 웹사이트를 통해 개인정보를 수집 및 관리하고 있는 사업체가 개인정보 수집 시 개인에게 제공하는 권리의 주된 내용은 ‘개인정보 수집에 대한 동의’, (73.6%), ‘동의 철회(회원탈퇴)’(61.0%), ‘제공된 정보의 열람’(55.0%), ‘제공된 정보의 정정’(53.0%) 등의 순인 것으로 나타났다.²⁵²⁾

[그림 2-1-17] 개인정보 수집 시 기업이 제공하는 권리



252) 한국정보보호진흥원, 『2007 정보보호 실태조사, 기업편』 (2007), 42면.

또한 이용자의 개인정보의 수집이나 개인정보의 제 3자 제공 또는 취급을 위탁하는 경우 이용자에게 미리 고지하는 주된 내용은 ‘개인정보의 수집 및 이용 목적’(51.8%), ‘개인정보관리책임자의 성명, 소속부처, 직위, 전화번호 등’(48.4%), ‘수집하고자 하는 개인정보의 항목’(43.0%) 등이다.

이용약관에 명시된 내용은 ‘개인정보의 수집 및 이용 목적(45.9%), ‘개인 정보관리책임자의 성명, 소속부처, 직위, 전화번호 등’(40.5%), ‘수집하고자 하는 개인정보의 항목’ (34.8%) 등의 순으로 나타나 약관 고지 및 명시 내용이 비슷함을 알 수 있다.²⁵³⁾

[그림 2-1-18] 개인정보 수집/위탁 시 이용자 고지 및 약관 명시 내용

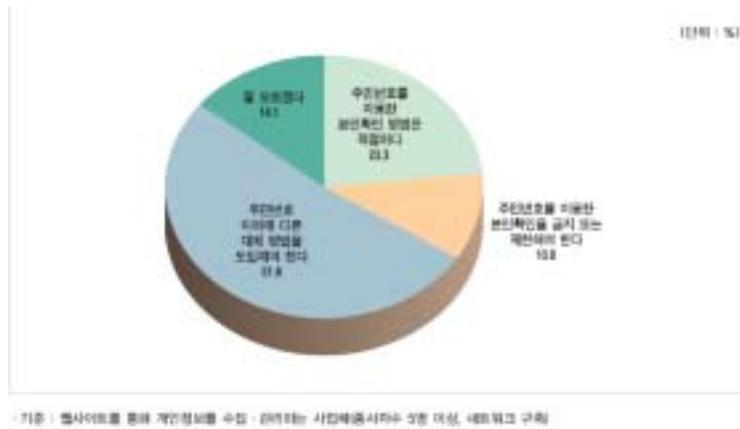


웹사이트 상에서 개인정보를 수집하는 기업들을 대상으로 웹사이트에 회원가입을 신청하는 이용자에 대해 주민번호를 이용하여 본인을 확인하는 것에 대한 의견을 물어본 결과 ‘주민번호 이외에 다른 대체

253) 한국정보보호진흥원, 『2007 정보보호 실태조사, 기업편』 (2007), 43면.

방법을 도입해야 한다’는 응답이 51.8%로 가장 많았으며, ‘주민번호를 이용한 본인 확인을 금지 또는 제한해야 한다’가 10.8%로 나타난 반면 ‘주민번호를 이용한 본인확인 방법이 적절하다’는 응답은 23.3%로 나타나 주민번호의 활용에 대해 부정적인 태도를 가지고 있음을 알 수 있다.²⁵⁴⁾

[그림 2-1-19] 주민번호를 통한 본인확인의 적절성에 대한 인식



(2) 개인들의 정보 제공 현황

개인들은 이메일, 정보 서비스 수신, 콘텐츠 확인을 위해 필수사항인 ‘회원 가입’ 형태로 개인정보를 제공하는 비중이 가장 높으며, 이 비중은 2006년에 67.3%로 2002년(60.7%)과 2003년(62.4%)에 비해 지속적으로 높아지고 있다. ‘상품/서비스 구매’(23.3%)의 목적으로 개인정보를 제공하는 것이 그 다음으로 높게 나타났다.²⁵⁵⁾

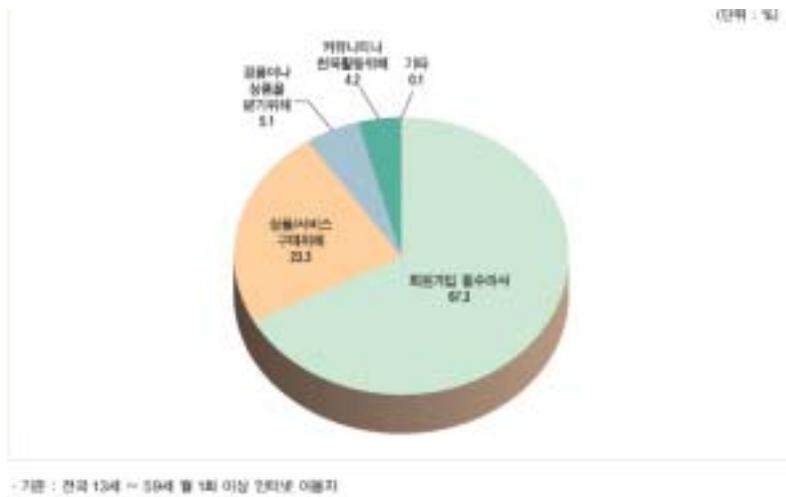
254) 한국정보보호진흥원, 『2007 정보보호 실태조사, 기업편』 (2007), 130면.

255) 한국정보보호진흥원, 『2003 개인 인터넷 이용자의 정보화 역기능 실태조사보고서』 (2003), 65면; 한국정보보호진흥원, 『2007 정보보호 실태조사, 기업편』 (2007), 90면.

[표 2-1-28] 개인의 기업에 대한 정보 제공목적(2002, 2003, 2006년)

구분	2002년 (%)	2003년 (%)	2006년(%)
컨텐츠 및 정보 서비스 이용을 위해 가입 필수	60.7	62.4	67.3
상품/서비스 구매	28.4	27.3	23.3
경품/현금 수령 목적	8.2	8.4	5.1
커뮤니티/친목	2.7	1.9	4.2
기타	0.1	-	0.1
합계	100	100.0	100

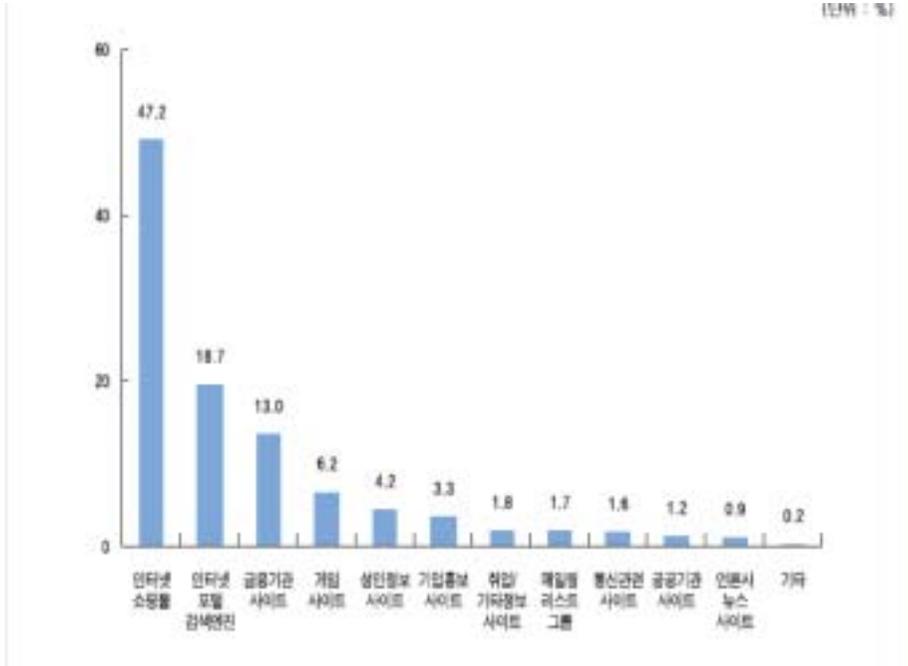
[그림 2-1-20] 개인정보 제공목적(2006년)



웹사이트를 이용하기 위해 개인정보 제공을 요구받았을 때 개인정보를 제공한 사이트를 질문한 결과 응답자의 47.2%가 ‘인터넷 쇼핑몰’로 답하였고 그 다음은 ‘인터넷 포털/검색엔진’(18.7%), ‘금융기관

사이트(13.0%)’의 순으로 나타났다. 이러한 결과는 최근에 전자상거래 시장이 빠르게 성장함에 따라 나타나는 현상으로 볼 수 있다.²⁵⁶⁾

[그림 2-1-21] 개인정보 제공 경험이 많은 사이트



이상의 여러 목적을 수행하기 위해 개인들은 기업에 개인정보를 제공하는 동시에 이에 따른 부작용에 대한 우려도 많이 하고 있다. 가장 높은 비중을 차지하고 있는 우려 유형은 ‘사업자의 관리소홀로 인한 내부자 정보 유출’로 40% 정도이며, ‘본인의 동의 없는 개인정보 수집으로 사생활 노출(23.7%)’ ‘사업자간 고객 정보의 공동이용(15.0%)’의 순으로 나타났다.²⁵⁷⁾

256) 한국정보보호진흥원, 『2007 정보보호 실태조사, 개인편』 (2007), 92면

257) 한국정보보호진흥원, 『2003 개인 인터넷 이용자의 정보화 역기능 실태조사보고서』 (2003), 6면.

[표 2-1-29] 개인의 개인정보 제공에 따른 우려도

우려 유형	2002년	2003년
사업자의 관리소홀로 인한 내부자 유출	37.8	39.1
본인의 동의없는 개인정보 수집으로 사생활 노출	24.3	23.7
사업자간 고객(회원) 정보의 공동이용	13.9	15.0
본인의 ID 및 비밀번호 도용으로 인한 피해	12.7	10.9
공공기관 등에 대한 무분별한 개인정보 제공	11.2	11.4
기타	0.1	-

(3) 개인정보제공에 대한 일반인과 전문가 의견 설문 조사²⁵⁸⁾

기업이 수집한 고객 정보를 자사의 다른 상품이나 서비스를 광고하는 것에 이용하는 것에 대해 일반인의 34.9%가 ‘절대 허용되어서는 안 된다’는 부정적 입장을 보였으며, 54.3%는 ‘사전 동의가 있으면 허용된다’고 응답하였다. 연령별로는 20대(37.2%)가, 직업별로는 블루 계층(38.6%)이 기업의 고객 정보 이용에 대해서 보다 부정적인 태도를 갖고 있는 것으로 나타났다.

한편 전문가들의 경우 기업이 수집한 고객 정보를 자사의 다른 상품이나 서비스를 광고하는 것에 이용하는 것을 7.3%만이 ‘절대 허용해서는 안 된다’는 부정적 입장을 보였으며, 73.2%는 사전 동의가 있으면 허용된다고 응답하여 수집한 고객정보의 이용에 대해 일반인들 보다 훨씬 더 긍정적인 태도를 보이는 것으로 나타났다.

258) 본 연구를 위해 실시된 조사의 결과임.

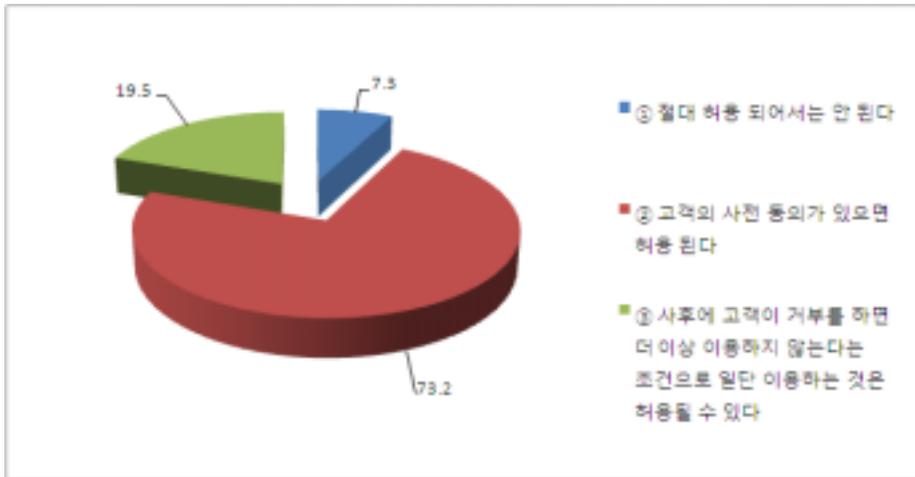
제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

[그림 2-1-22] 기업이 수집한 고객정보 이용에 대한 태도(일반인)



[그림 2-1-23] 기업이 수집한 고객정보 이용에 대한 태도(전문가)

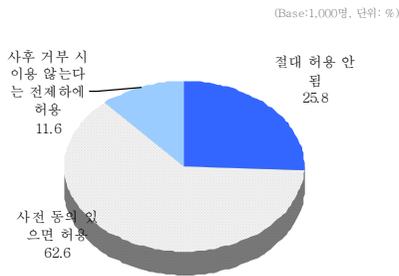
(Base : 41명, 단위 %)



기업이 소비자에게 맞춤형서비스를 제공하기 위하여 소비자의 생활방식, 취미, 소비성향 등을 수집하고 조사·분석하여 개인별 프로파일을

만들어 이용하는 것에 대해서는 ‘사전 동의가 있으면 허용’(62.6%)이 가장 높게 응답되었으며, 그 다음으로 ‘절대 허용 안 됨’(25.8%)의 순으로 나타나 개인정보의 활용이 고객에게 도움이 될 경우 개인정보 활용에 대해 좀 더 긍정적인 태도를 보이고 있다는 것을 알 수 있다. 절대 허용이 안 된다고 응답한 경우는 여성보다 남성이(28.7%), 직업별로는 블루 계층(31.2%) 높은 것으로 나타났다.

[그림 2-1-24] 기업의 개인별 프로파일 이용에 대한 태도(일반인)



전문가들의 경우 기업이 개인별 프로파일을 만들어 이용하는 것에 대해서 ‘사전 동의가 있으면 허용’(80.5%)을 가장 많이 응답하였으며, 그 다음으로는 ‘사후에 고객이 거부하면 이용하지 않는다는 조건으로 일단 이용 허용’(12.2%)의 순으로 나타나 일반인들에 비해 좀 더 긍정적인 태도를 가지고 있는 것으로 나타났다.

[그림 2-1-25] 기업의 개인별 프로파일 이용에 대한 태도(전문가)

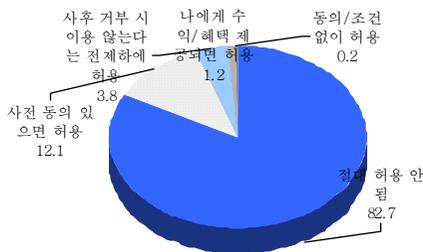
(Base : 41명, 단위 %)



일반인들의 경우 기업이 수집한 이름, 주소, 전화번호, 이메일 주소 등의 연락 정보를 파는 행위에 대해서는 ‘절대 허용 안 됨’이 82.7% 수준으로 나타나 대부분 부정적인 태도를 갖고 있음을 알 수 있다. 특히, 남성보다 여성이(84.5%), 연령별로는 50대가(87.5%), 직업별로는 주부 계층(85.0%)이 보다 부정적 의견을 갖고 있는 것으로 나타났다.

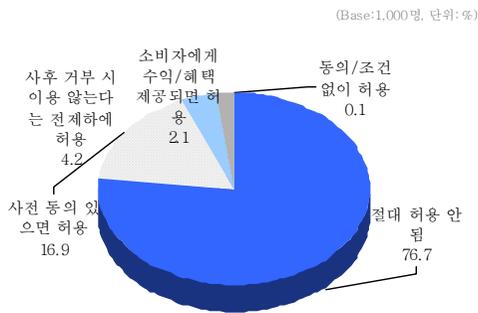
[그림 2-1-26] 기업이 수집한 나의 연락 정보 판매에 대한 태도(일반인)

(Base:1,000명, 단위: %)



기업이 소비자에게 맞춤형서비스를 제공하기 위해 만든 연락처 정보 외의 개인별 프로파일을 다른 기업에게 판매하는 행위에 대해서는 76.7%가 ‘절대 허용 안 됨’으로 응답하고 있으며, ‘사전 동의 있으면 허용’이 16.9% 수준으로 나타나 개인정보를 타 기업에 판매하는 행동에 대해 부정적인 의견을 갖고 있는 것으로 나타났다. 하지만 타 기업에게 개인정보를 판매할 때 구매이력, 라이프스타일 등의 정보보다 개인의 신상정보에 더 민감하게 반응하는 것으로 나타났다.

[그림 2-1-27] (기업→기업) 개인별 프로파일 판매에 대한 태도(일반인)



전문가들의 경우 기업이 수집한 개인의 연락처 정보를 제3자에게 돈을 받고 판매하는 것에 대해 ‘절대 허용 안 됨’이 61%, ‘사전 동의가 있으면 허용’이 31.7%로 나타나 신상정보의 판매에 대해 다소 부정적인 태도를 갖고 있으나 일반인들에 비해서는 좀 더 긍정적인 태도를 보이는 것으로 나타났다.

[그림 2-1-28] 기업이 수집한 나의 연락 정보 판매에 대한 태도
(전문가)

(Base : 41명, 단위 %)



전문가들의 경우 기업이 소비자에게 맞춤서비스를 제공하기 위하여 만든 개인별 프로파일을 다른 기업에게 판매하는 행위에 대해서는 56.1%가 ‘절대 허용 안 된다’로 응답하고 있으며, ‘사전 동의 있으면 허용’이 39% 수준으로 나타나 일반인들에 비해 긍정적인 태도를 가지고 있음을 알 수 있다. 또한 전문가들 역시 개인의 신상정보이외의 구매이력이나 라이프스타일 등의 정보에 대해 덜 민감하게 반응하는 것을 알 수 있다.

[그림 2-1-29] (기업→기업) 개인별 프로파일 판매에 대한 태도 (전문가)

(Base : 41명, 단위 %)



이상의 결과를 종합해보면 일반인뿐만 아니라 법학전문가나 기업에 종사하는 실무자들도 기업이 고객의 정보를 활용하여 광고를 하거나 고객정보를 타 기업에 판매하는 것에 대해 부정적인 태도를 가지고 있음을 알 수 있다. 하지만 고객정보를 타 기업에 판매하는 것에 비해 기업이 고객의 정보를 맞춤형서비스를 위해 마케팅에 활용하는 것에 대해 좀 더 부정적인 태도를 가지고 있는 것으로 나타났다. 또한 일반인들에 비해 전문가들이 고객의 DB활용에 좀 더 우호적임을 알 수 있다.

2. 효용성 평가

기업이 개인정보에 기반을 둔 데이터베이스 마케팅을 수행할 경우 일반적으로 기업측면에서만 큰 혜택이 발생하고 개인들은 프라이버시 침해로 인해 피해만을 입는다고 여기는 분위기가 사회전반에 팽배해

있다. 하지만 기업이 DB 마케팅을 효율적으로 수행할 수 있다면 기업 뿐만 아니라 개인과 사회의 여러 측면에서 효용이 발생할 수 있다.

(1) 개인 측면

1) 맞춤형 정보의 획득

기업이 고객에 대한 정확한 정보를 가지고 있을 경우 소비자는 기업으로부터 맞춤 정보와 서비스를 제공받을 수 있다. 기업이 제품이나 서비스에 대한 정확한 타겟팅을 실시하게 됨에 따라 무분별한 전화나 스팸 메일을 하지 않게 되어 마케팅 비용을 절감할 수 있고, 불필요한 텔레마케팅으로 인한 고객의 피해도 줄일 수 있다. 정확한 타겟 마케팅에 근거한 마케팅 비용의 절감은 영업이익의 상승 및 가격인하 효과를 유발하여 궁극적으로 고객에게 혜택이 돌아갈 수 있다. 또한 고객들은 기업으로부터 유용한 맞춤형 정보만을 제공받기 때문에 정보탐색에 필요한 시간과 비용을 절약할 수 있다는 장점이 있다.²⁵⁹⁾

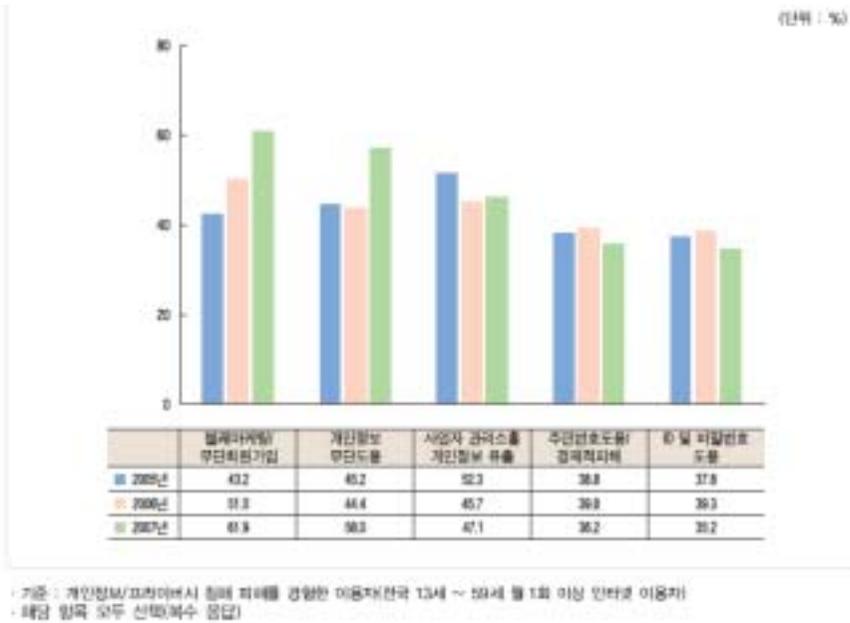
2) 불법적 개인정보의 이용 방지

한국정보보호진흥원(2007)²⁶⁰⁾의 조사에 의하면 개인정보 피해 사례 중 가장 높은 비중을 차지하고 있는 유형이 ‘개인정보의 무단 수집 및 무단회원가입’(61.9%)이며 다음으로는 ‘동의 없이 개인정보를 목적이외의 용도로 사용 및 제 3자 제공’(58.0%)인 것으로 나타났다. 이것은 기업이 합법적으로 고객정보를 수집하고 갱신하는데 드는 비용이 엄청나게 때문에 불법적인 개인정보의 유통이 이루어지고 있다고 것을 의미할 수 있다. 따라서 필요한 개인정보를 수집하는데 드는 비용을 낮춘다면 불법적인 개인정보의 이용이 줄어들 수 있을 것이다.

259) 김병도 외, 『우리나라 데이터베이스마케팅 관련산업의 현황과 발전방향』(서울대학교 경영연구소, 2004), 36면.

260) 한국정보보호진흥원, 『2007 정보보호 실태조사 개인편』(2007), 122면.

[그림 2-1-30] 유형별 개인정보/프라이버시 침해 피해 경험



3) 무분별한 전화, 메일 등의 감소

기업은 고객에 대한 정확한 정보를 가지고 있을 경우 각 상품이나 서비스별로 구매 가능성이 높은 타겟 고객을 선정하고 이들을 대상으로 전화를 걸거나 DM을 발송하여 마케팅활동이나 캠페인을 실시할 수 있다. 따라서 관련성이 낮은 전화나 메일이 현저하게 감소하며 또한 기업측면에서는 마케팅 효율성 제고 효과를 얻을 수 있다.

4) 주소변경으로 인한 불편 및 불이익 감소

만약 합법적인 고객정보의 유통이 가능하다면 고객 데이터베이스를 보유한 기업은 고객정보를 제공하는 업체로부터 일정 비용을 지불하고 정기적으로 자사 고객의 주소를 업데이트 할 수 있다. 이를 통해 고객에게 지속적으로 맞춤형서비스를 제공할 수도 있게 되며 고객들도

이사를 할 때마다 관련업체들에 새 주소지를 알려야 하는 번거로움 없이 편리하게 서비스를 이용할 수 있다.

(2) 기업측면

기업들은 고객정보를 활용하여 마케팅의사결정의 정확도 제고 및 효율성 증대의 효과를 얻을 수 있다.

1) 시장 세분화 / 타겟 마케팅 전략

마케팅 전략의 핵심은 타겟 세분시장의 니즈에 맞는 상품과 서비스를 개발하고 이들에게 제품과 서비스의 차별화된 점을 커뮤니케이션 하는 것이다. 타겟 마케팅의 바탕이 되는 고객 세분화는 잘 구축된 고객 DB 내 풍부한 정보가 있을 때 가능하다.

정확한 표적고객 선정시 수익이 증대되는 경우를 예를 들어 보면 다음과 같다.²⁶¹⁾ 100만 명의 잠재고객명단을 보유한 기업이 DM을 발송할 경우 DM을 받은 고객 중 일부가 제품을 구매하고 제품 판매 시 평균 이익이 \$80, DM 발송비용은 한 장 당 \$0.7이고, 평균 응답률은 1%라고 가정할 때 만약 이 기업이 100만 명 전 고객에게 DM을 발송했다면 이 기업이 해당 DM 발송 이벤트로 얻을 수 있는 이익은 다음과 같다.

$$[\text{총이익} = 100\text{만명(고객수)} * 0.01(\text{응답률}) * 80\$(\text{평균이익}) - 100\text{만명(고객수)} * 0.7\$(\text{DM발송비용}) = 800,000 - 700,000 = 100,000\$]$$

하지만 이 기업이 고객에 대한 데이터를 바탕으로 100 만 명 고객의 예상 응답률을 추정하고 응답률 순으로 이들을 나열한 후, 예상 응답률 기준으로 10만 명씩 10개의 세분집단으로 형성할 경우 10만

261) 김병도 외, 『우리나라 데이터베이스마케팅 관련 산업의 현황과 발전방향』 (서울대학교 경영연구소, 2004).

명으로 구성된 각 세분집단의 실제 응답률과 각 세분집단으로부터 발생하는 이익은 [표 2-1-30]과 같다.

즉 예상이익이 마이너스인 6~10번째 집단 고객을 제외하고 예상이익이 0이상인 1부터 5번째 세분집단의 고객에게만 DM을 발송할 경우 총이익은 \$334,000이 된다. 나머지 50만 고객은 DM 발송비용을 충당할 만큼의 수익을 창출하지 못하는 고객이므로 DM을 발송할 필요가 없다. 이와 같은 타겟팅을 통해 이 기업은 이익을 3배 이상 올릴 수 있었다.

[표 2-1-30] 세분집단별 응답률과 이익²⁶²⁾

십분위	가망고객 수	응답률(%)	이익(\$)	누적이익(\$)
1	100,000	3.00	170,000	170,000
2	100,000	2.00	90,000	260,000
3	100,000	1.40	42,000	302,000
4	100,000	1.15	22,000	324,000
5	100,000	1.00	10,000	334,000
6	100,000	0.60	-22,000	312,000
7	100,000	0.40	-38,000	274,000
8	100,000	0.30	-46,000	228,000
9	100,000	0.10	-62,000	166,000
10	100,000	0.05	-66,000	100,0005

262) Blattberg, R., Kim, Byung-Do and Neslin, S.(2004), *Strategy and Tactics of Database Marketing, Unpublished manuscript*, 김병도 외, 『우리나라 데이터베이스마케팅 관련 산업의 현황과 발전방향』 (서울대학교 경영연구소, 2004), 49면 수정 후 재인용.

사례: 밀러의 핵심고객 발굴²⁶³⁾

2차 세계대전 직후 프리미엄 맥주의 이미지를 부각시켜 고객으로 하여금 ‘상류사회’에 속한다는 인식을 심어 고소득층 소비자에게 성공적으로 어필했으나 20년이 지나는 동안 다른 모든 맥주제품들의 품질 수준이 동일해지자 밀러의 특성이 사라지고 시장점유율도 5위에서 8위로 하락했다. 밀러社를 인수한 필립모리스社는 고객데이터분석을 통해 광고와 판촉 등 맥주회사의 마케팅활동에 가장 민감하게 반응하는 고객층이 ‘블루 컬러’에 속하는 젊은 남성임을 파악해 그들의 라이프스타일을 면밀히 관찰했다. 시장조사 결과를 바탕으로 밀러社는 밀러 하이 라이프(Miller High Life) 발매해 맥주 소비가 가장 많은 블루 컬러 시장을 공략했다. 미국적인 생활방식을 강조한 광고와 블루컬러 계급의 일상생활을 다뤄 일과 후 한 잔 하는 시간을 ‘밀러타임(Miller Time)’이라 명명한 대대적인 캠페인을 통해 밀러 하이 라이프는 2위 브랜드가 됐다.

사례: 체이스 맨하탄 은행²⁶⁴⁾

교차판매는 특히 금융업 분야에서 활발히 이뤄지고 있는데 체이스 맨하탄 은행은 고객에 대한 보다 깊은 이해를 위해 계정별로 작성된 고객파일을 하나로 통합하고 이 과정에서 고객에 대한 인구 통계적 변수와 라이프스타일에 대한 자료를 추가시켰다. 이렇게 구축된 데이터베이스를 이용해 이 은행은 여러 가지 다른 상품의 구매를 권유하는 메일을 발송했다. 그리고 메일 발송 시에도 개인의 특성에 따라 적합한 상품을 권유했으며 여기서 주목할 것은 데이터베이스가 고객 개인별이 아닌 가구별로 구축됨으로써, 고객 개개인의 가치를 보다 더 객관적으로 평가할 수 있는 시스템이 갖춰졌다는 것이다.

2) 우수고객 관리

기업의 수익창출을 위한 분석에 있어서 중요한 이슈 중에 하나가 우수고객을 선별해 내는 문제이다. 기업에 80%의 수익을 가져다주는

263) 세계일류기업의 DBM 성공사례, <http://www.CRMservice.co.kr>

264) 세계일류기업의 DBM 성공사례, <http://www.CRMservice.co.kr>

고객은 전체 고객의 20%의 불과하다는 20:80의 법칙에 근간하여 우수 고객을 선별하기 위해서는 고객의 기업에 대한 수익성 기여도와 같은 우수고객 선별 기준이 마련되어야 한다. 이러한 수익성 분석을 통한 우수고객 산출은 정확하고 풍부한 고객데이터가 축적되었을 때 가능하다. 또한 축적된 고객 데이터는 우수고객들에게 적합한 마케팅 전략을 수립하고 차별화된 서비스를 제공함으로써 이들의 충성도를 제고하는데도 활용되어 질 수 있다.

사례: 시어즈의 고객 로열티 프로그램²⁶⁵⁾

미국의 소매 그룹인 시어즈는 고객들의 타사 카드 사용을 허용하지 않았으나, 타사카드 사용에 대한 요구가 증대하자 이를 수렴하되 자사의 소매점 카드사용액이 감소하지 않도록 하기 위해 시어즈 카드를 토대로 시어즈 우수고객 로열티 프로그램을 도입했다. 시어즈는 고객데이터 분석을 통해 1년 동안 시어즈에서 1천 달러 이상을 소비하고, 적어도 4개 이상의 상이한 제품카테고리에서 구매를 하고, 6회 이상은 방문해 구매하는 고객들을 베스트 고객으로 분류해 이들 고객에게만 보상 프로그램을 실시했다. 이들에게는 시어즈 카드에 붙이는 회원권 스티커를 포함한 가입 축하선물과 일 년 내내 고객이 원하는 시간에 특정 제품을 할인해서 구매할 수 있는 교환권을 제공했다. 또한 점포 내에서 특별한 서비스와 별도의 세일행사, 할부 서비스를 제공해 고객으로 하여금 시어즈의 로열티 고객으로서의 프라이드를 느낄 수 있도록 했다. 이러한 프로그램을 통해 시어즈는 타 신용카드를 받아들인 이후에 오히려 자사카드 매출을 더욱 신장시킬 수 있었다.

3) 기존고객 유지

기업이 고객 베이스를 유지하기 위해서는 신규고객을 끊임없이 획득하는 것도 중요하지만 비용 측면에서 기존고객이 이탈하지 않도록 유지하는 것이 더 바람직하다. 추가의 신규고객 한 명을 확보하는데 기존고객 한 사람을 유지하는 경우보다 5배 이상의 마케팅 비용이 들며

265) 세계일류기업의 DBM 성공사례, <http://www.CRMservice.co.kr>

(Reichheld, 2001) 연간 5%의 고객유지증대는 85%의 이익증대(Reichheld, 1996)효과가 있기 때문이다. 즉 기존고객과의 거래 기간이 증가할수록 월 평균 구매액은 증가하지만 월평균 마케팅 및 운영비용은 감소하는 경향이 있기 때문에, 기존고객의 이탈을 방지하는 것은 기업의 수익성 제고에 결정적 역할을 한다. 또한 오랫동안 거래관계를 유지한 고객은 해당 기업과 브랜드에 대해 충성도가 높고 주변 사람들에게 긍정적인 구전효과를 제공한다. [표 2-1-31]은 기존고객유지의 중요성을 보여주고 있는데, 이 표를 통해 매스마케팅이 아닌 다양한 형태의 CRM 활동을 통해 고객의 순현재가치를 높일 수 있음을 보여주고 있다. 여러 CRM 활동 중에서도 고객유지기간의 증가와 고객 이탈률의 감소가 고객획득 비용의 절감이나 고객 1인당 매출 증가보다 고객가치 증대에 더 중요함을 알 수 있다. 이처럼 기존고객을 효과적으로 관리하여 유지시키기 위해서는, 고객과의 지속적인 양방향 커뮤니케이션을 통해 고객관계관리가 필수적이다. 효과적인 고객관계관리를 위해서는 고객들에 대한 다양한 형태의 정보 축적이 반드시 선행되어야 한다.

[표 2-1-31] CRM 활동을 통한 고객 순현재가치²⁶⁶⁾

고객의 순현재가치에 영향을 미치는 요소	A	B	C	D	E	F
	기존매스마케팅 활동 시	고객 이탈률이 낮아질 때	마케팅 비용을 줄일 때	고객당 매출액을 늘릴 때	고객유지기간이 1년 증가할 때	E+고객 이탈률이 낮아질 때
총 고객 수	500,000	500,000	500,000	500,000	500,000	500,000
연평균 고객 이탈률	24%	20%	24%	24%	24%	18%
고객 1인당 연평균 수입	\$1,200	\$1,200	\$1,200	\$1,440	\$1,440	\$1,440
고객 획득비용	\$500	\$500	\$450	\$450	\$450	\$450
고객 유지기간 (연)	2	2	2	2	3	3

266) Swift, Ronald(2001), ‘The new economic opportunity for business-creating increased profitability through CRM,’ CRM Project, 2. 40면.

고객의 순현재가치에 영향을 미치는 요소	A	B	C	D	E	F
	기존매스마케팅 활동 시	고객 이탈률이 낮아질 때	마케팅 비용을 줄일 때	고객당 매출액을 늘릴 때	고객유지기간이 1년 증가할 때	E+고객 이탈률이 낮아질 때
고객 총 마진	25%	25%	25%	25%	25%	25%
고객 현재가치	\$36,756,364	\$40,727,273	\$51,196,364	\$87,427,636	\$177,583,437	\$223,050,518

사례: 리즈칼튼호텔의 핫라인²⁶⁷⁾

리즈칼튼 호텔은 투숙고객의 특성을 통합데이터베이스 시스템에 축적할 수 있는 ‘고객의 기호 핫라인’ 프로그램을 운영하고 있다. 미국 출장에 나선 고객이 샌프란시스코의 리즈칼튼 호텔에 묵으며 서양식 폭신한 베개가 싫어 프런트에 전화해 약간 딱딱한 베개를 요구할 경우 종업원은 ‘고객의 기호 핫라인’을 통해 고객의 특성을 등록한다. 샌프란시스코에서의 용무를 마치고 다음 목적지인 뉴욕으로 이동해 그 곳 리즈칼튼호텔에 투숙했을 때 고객은 침대 위에 딱딱한 베개가 놓여 있는 것을 발견할 수 있다. 이처럼 리즈칼튼에는 고객이름만 입력하면 고객기호를 알게 해주는 공유 데이터베이스가 있다. 리즈칼튼은 현재 약 50만 명 이상의 고객 프로필을 축적하고 있고 그 중 50% 이상 고객의 기호를 파악하고 있다.

4) 추가 고객정보 획득 및 갱신비용의 절감

아무리 좋은 고객 데이터베이스를 구축하였다고 하여도 각 개인의 신상변화에 대한 정보가 끊임없이 업데이트되어야 한다. Garbage in, Garbage out이라는 말이 있는 것처럼 시스템이 아무리 훌륭하다 할지라도 그 안에 들어있는 정보가 정확하지 않거나 누락된 정보가 많다면 잘못된 정보 유도 가능성이 높아 마케팅을 효율적으로 수행할 수 없다. 따라서 변화하는 고객정보를 고객 데이터베이스에 정기적으로 반영할 수 있는 시스템을 갖추어야 한다. 고객정보를 얻을 수 있는 방법이 다양하고 비용이 낮아진다면 추가고객정보 획득 및 갱신비용이 절감될 수 있을 것이다.

267) 세계일류기업의 DBM 성공사례, <http://www.CRMservice.co.kr>

3. 위험성 평가

이상에서 설명한 것처럼 고객정보를 활용한 기업의 1:1 마케팅 및 고객관계관리는 기업뿐만 아니라 고객들에게 많은 혜택을 제공하지만 개인정보를 제대로 관리하지 않을 경우 여러 위험들이 수반된다. 2008년 2월 옥션의 1,080만 회원 아이디 계좌번호 유출, 4월 하나로텔 레콤의 600만 고객정보 제휴업체에 제공 및 유출, 9월 GS 칼텍스의 1,100만 마일리지 회원 정보 유출 등의 사례를 통해 기업들의 정보 수집 의욕에 비해 기업들의 개인정보보호의식과 관리체계는 상대적으로 미진함을 알 수 있다.

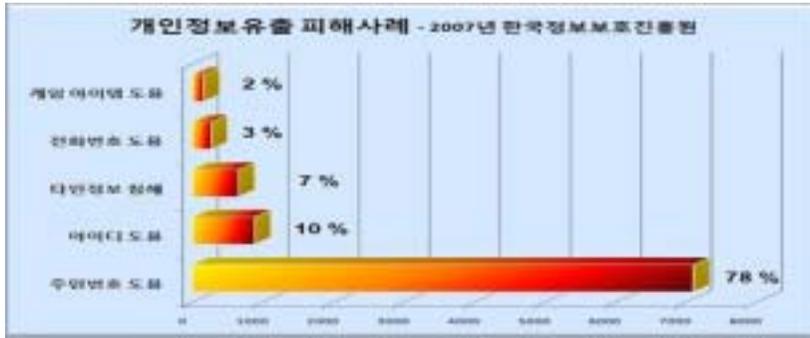
(1) 주민등록번호 활용의 위험

특히 우리나라의 경우 주민등록번호를 활용하여 고객들의 행태를 분석하고 있기 때문에 이용자의 상품 구매 패턴이나 서비스 이용 행태를 익명으로 분석하는 미국 등 선진국의 경우에 비해 개인정보침해의 위험요인이 높다고 볼 수 있다.

이것은 우리나라에서 개인 정보를 활용한 서비스 사업이 일반화되지 못하고 있는 이유 중의 하나가 될 수 있다. 이처럼 우리나라의 경우 개인정보침해의 위험요인이 높기 때문에 개인정보의 보호관리가 더욱 중요함에도 불구하고 기업들의 정보보호 관리 의식 및 노력이 부족한 것으로 나타나고 있다.

2007년 한국정보진흥원의 발표에 따르면 2006년 한해 개인정보 유출 피해는 ‘주민번호 도용’이 7,111건인 78%, ‘아이디 도용’이 10%로 나타나 주민번호 도용문제가 가장 심각한 피해의 유형임을 알 수 있다.

[그림 2-1-31] 개인정보유출피해사례²⁶⁸⁾



(2) 기업의 미진한 정보보호 투자

개인정보유출피해사례가 많이 발생하고 있는 이유 중 하나로 고객의 정보를 활용하고 있는 기업들의 미진한 정보보호 투자를 들 수 있다. 국내 2500개 기업 중 ‘IT투자 대비 정보보호 투자 비율’이 10% 이상인 기업은 0.8%뿐이었다. 또 78%의 기업이 1% 미만을 투자하고 있었으며 60% 이상의 기업들이 정보보호를 위해 아무런 활동을 하지 않는다고 응답하여 미국이나 영국 등에 비해 대부분의 기업이 IT 투자 대비 정보보호 투자비중이 낮은 것으로 나타나고 있다.²⁶⁹⁾

[그림 2-1-32] 국가별 IT 투자 대비 정보보호 투자 비율



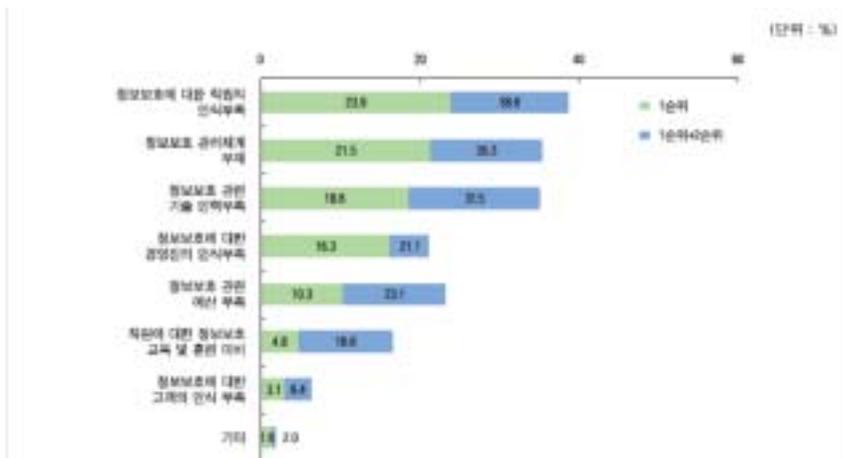
268) 한국정보보호진흥원, 『2007년 하반기 민간기업 정보보호 실태조사』 (2007).

269) 한국정보보호진흥원, 『2007년 하반기 민간기업 정보보호 실태조사』 (2007).

(3) 기업의 정보보호 의식 부족

정보보호투자 비율이 낮은 이유 중 하나로 기업의 정보보호에 대한 인식을 들 수 있다. 사내 정보보호 수준에 대한 자체 평가 점수가 6점 만점에 1~3점인 사업체를 대상으로 정보보호 수준이 낮은 이유를 1순위와 2순위로 물어본 결과 1순위 응답을 기준으로, ‘정보보호에 대한 직원의 인식 부족’(23.9%)이 가장 높게 나타났다. 다음으로 ‘정보보호 관리체계 부재’(21.5%), ‘정보보호 관련 기술 인력 부족’(18.6%), ‘정보보호에 대한 경영진의 인식부족’(16.3%) 순인 것으로 나타났다.²⁷⁰⁾

[그림 2-1-33] 사내 정보보호 수준에 대한 우려 원인



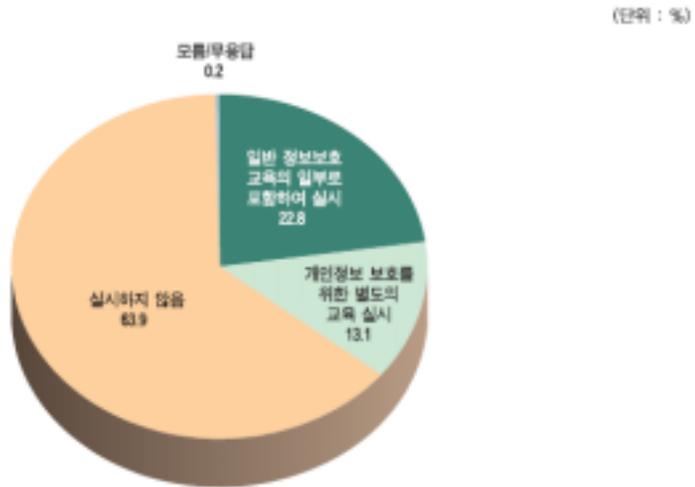
(4) 개업의 개인정보보호교육 미진

웹사이트를 통해 개인정보를 수집·관리하고 있는 사업체 중 개인정보 보호 교육을 실시하지 않고 있는 비중이 63.9%에 이르는 것으로 나타났다

270) 한국정보보호진흥원, 『2007 정보보호 실태조사 기업편』 (2007), 57면.

다. ‘일반 정보보호 교육의 일부로 포함하여 실시’하는 기업이 22.8%, ‘개인정보보호를 위한 별도의 교육을 실시’하는 기업은 13.1%에 불과한 실정으로 개인정보보호 교육실시의 중요성이 간과되고 있음을 알 수 있다.²⁷¹⁾

[그림 2-1-34] 개인정보보호 교육 실시 여부



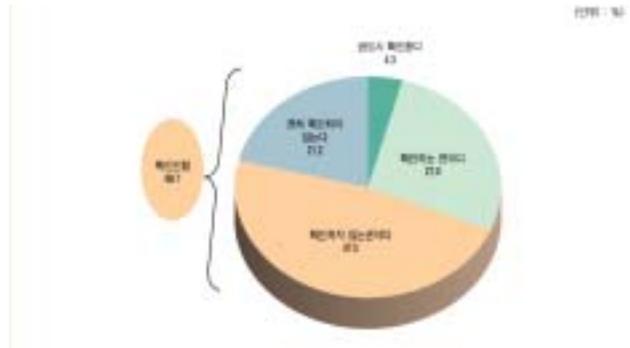
(5) 이용자들의 책임의식 부족

개인 인터넷 이용자들의 개인정보제공에 대한 책임감도 건전한 개인정보의 활용에 중요한 영향을 미치는 요인이다. 웹사이트에 개인정보를 제공할 때 해당사이트의 개인정보 관리수준을 확인하는 정도에 대해 ‘전혀 확인하지 않는다’가 21.2%, ‘확인하지 않는 편이다’가 47.5%로 나타나 68.8%의 개인 인터넷 이용자가 해당사이트의 개인정보 관리 수준을 확인하지 않는 것으로 나타났다.²⁷²⁾

271) 한국정보보호진흥원, 『2007 정보보호 실태조사 기업편』 (2007), 36면.

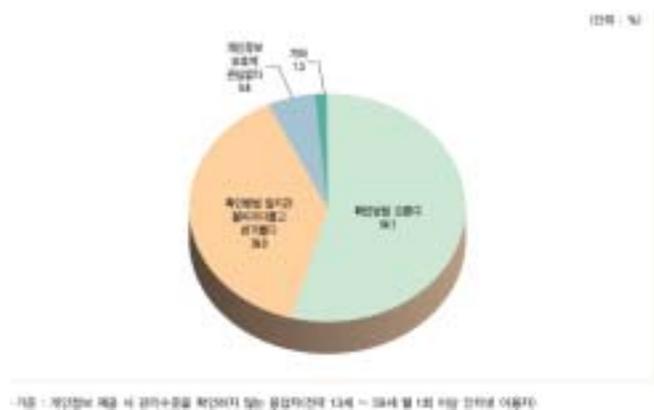
272) 한국정보보호진흥원, 『2007 정보보호 실태조사 개인편』 (2007), 94면.

[그림 2-1-35] 개인 정보 제공시 관리수준 확인 여부



개인정보 제공 시 관리수준을 확인하지 않는 개인 인터넷 이용자들 (n=2,750)의 경우 그 이유로 ‘확인하는 방법을 모른다’(54.1%)를 가장 많이 응답하였으며, ‘확인방법은 알고 있지만 절차가 까다롭고 번거롭다’(39.0%)가 그 다음인 것으로 나타나 관리수준의 확인에 대한 교육이나 정보제공, 확인절차의 사용편이성이 제고되어야 할 것으로 보인다.²⁷³⁾

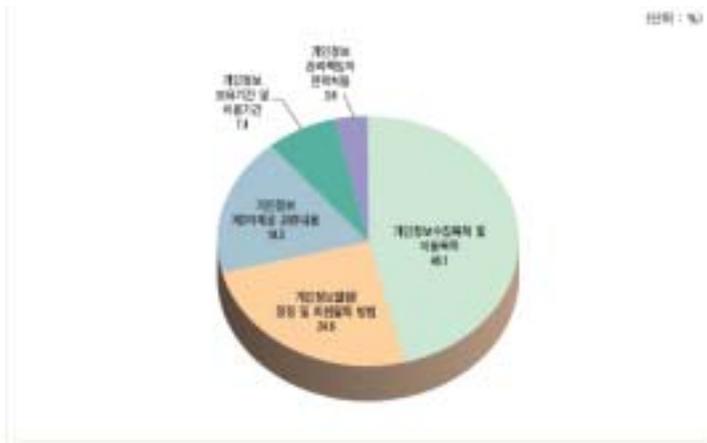
[그림 2-1-36] 개인정보 제공 시 관리수준 확인하지 않은 이유



273) 한국정보보호진흥원, 『2007 정보보호 실태조사 개인편』 (2007), 96면.

개인정보 제공시 관리 수준을 확인할 때 이용약관이나 개인정보보호 정책을 읽어보는 개인 인터넷 이용자들 (965명)이 확인하는 내용의 경우 ‘개인정보 수집목적 및 이용목적(46.1%)’이 가장 많은 것으로 나타났다으며, 다음으로는 ‘개인정보 열람·정정 및 회원 탈퇴 방법(24.6%)’이 높게 나타났다.²⁷⁴⁾

[그림 2-1-37] 개인정보 보호정책 및 이용약관에서 확인하는 내용



이상에서 정부와 기업 및 개인측면에서 개인정보의 활용에 대한 위험성이 존재함을 알 수 있다. 따라서 각 위험요인들 별로 이러한 위험을 줄일 수 있는 다양한 수단들이 강구되어야 할 것이다.

4. 소 결

무한 경쟁시대에 글로벌 기업들을 대상으로 경쟁해야 하는 국내기업들이 고객의 정보를 수집하고 활용하는 것은 경쟁력 강화 및 마케팅 의사결정의 효율화를 위해 필수불가결한 전제조건이다. 일반인들은 기업들의 경우 이윤 추구를 목적으로 개인의 정보를 수집하고 활

274) 한국정보보호진흥원, 『2007 정보보호 실태조사 개인편』 (2007), 100면.

용하기 때문에 기업의 개인정보보호노력이 정부기관의 보호노력에 비해 높아야 한다고 인식하고 있다. 하지만 기업의 개인정보 활용이 개인의 프라이버시 침해를 야기하는 측면의 부작용이 있다는 이유로 고객정보를 활용하여 얻을 수 있는 다양한 순기능적인 측면을 간과하고 기업의 개인정보 활용이 실질적으로 금지되는 것은 바람직하지 않다. 필요한 부분은 법규를 통해 규제하고 이와 더불어 민간기업 스스로가 자율적인 정화 능력을 갖추 수 있도록 조성해 주는 것이 바람직하다.

기업들도 장기적 관점에서의 고객들과의 신뢰 구축이 성공적인 비즈니스 및 궁극적으로 기업의 브랜드 관리에 도움이 된다는 것을 인식하고 단순히 고객의 정보를 수집하고 활용하는데서 나아가 고객정보 수집에 대한 책임감을 가지고 고객 정보 보호를 위해서도 노력해야 한다. 무조건 많은 정보를 수집하기보다는 필요한 목적에 맞게 필요한 정보만을 수집하고 활용하여야 한다. 고객정보 수집 시 고객에게 구체적인 혜택이 돌아갈 수 있게 혜택을 가시화하여 개인정보에 대한 강제 동의를 요구하는 형태가 아닌 원하는 고객을 대상으로 동의하에 정보를 수집하여야 할 것이다. 또한 내부직원의 고의적인 유출과 관리자의 보안조치 소홀이나 실수로 인해 중요한 개인정보들이 노출되고 있으므로²⁷⁵⁾ 개인정보보호를 위한 체계적인 보안 체계를 갖추고 개인정보를 관리하는 보안인력 및 내부 인력에 대한 교육이 이루어져야 한다. 즉 기술적 보호조치, 프라이버시 보호정책, 내부 관리 절차, 직원 교육 등의 기업의 자율적 규제와 협력이 뒷받침 될 때 개인정보보호가 제대로 이루어 질 수 있다.

고객들 역시 자신의 개인정보가 어떻게 이용되는 가에 대해 통제권을 가지고 개인정보의 중요성을 인식하여 정보의 관리를 철저히 해야 한다. 기업과 정부는 고객정보를 불법으로 확보하고 활용하는 업자들에게 현혹되어 개인들이 소중한 정보를 제공하지 않도록 소비자들을

275) 박광진, “개인정보 유출사고의 원인과 정책방향”, 『IT Daily』, 2008. 9. 29일자.

대상으로 한 교육을 실시할 필요가 있다.

결론적으로 정부는 적정 수준에서의 규제를 통해 개인정보보호를 보장하면서도 정보산업의 육성을 위해 고객정보를 활용할 수 있도록 하는 균형적인 접근법을 취하는 것이 바람직할 것으로 보인다. 또한 법 집행을 엄정하게 하여 법 준수 기업과 그렇지 않은 기업을 차별화 하여 관리할 필요가 있다. 특히 우리나라의 경우 주민등록번호에 대한 노출이 개인 프라이버시 침해의 가장 큰 문제이므로 회원 가입 시 공인인증서를 통한 회원인증방법이나 국가에서 통제하는 형태의 인증 방법으로 관리를 하게 하는 것도 고려해 볼 필요가 있다.

제 2 장 현행 개인정보보호법제의 현황

제 1 절 개 관

우리나라의 정보프라이버시 보호를 위한 법제는 아래의 [표 2-2-1]에서 보는 바와 같이 공공부문과 민간부문으로 구분되어 공·사간에 그 법적 근거 및 집행체계를 달리하고 있다. 먼저, 공공부문에 있어서는 전산처리된 개인정보의 보호에 관한 일반법으로 『공공기관의 개인정보 보호에 관한 법률』이 제정되어 있으며, 그 밖에 전자정부법 및 주민등록법, 국세기본법 등의 개별법에서 개인정보보호에 관한 규정들이 산재하고 있다. 한편, 민간부문에 있어서는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』이 정보통신망에서의 개인정보보호에 관한 일반법으로 기능하고 있고, 신용정보에 관해서는 『신용정보의 이용 및 보호에 관한 법률』이, 통신상의 정보보호에 관해서는 통신비밀보호법이 각기 시행되고 있으며, 그 밖에 정보통신기반보호법, 『금융실명거래 및 비밀보장에 관한 법률』 등의 개별법에서도 개인정보에 관한 규정들이 산재하고 있다.

[표 2-2-1] 개인정보 보호 관련법제 현황

적 용 분 야		법 률 명	비 고
공공부문		『공공기관의 개인정보 보호에 관한 법률』	1994년 제정, 1999년 개정
민간 부문	온라인 사업자	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	2001년 전문개정, 2002년 개정
기타분야 (개별법)		『신용정보의 이용 및 보호에 관한 법률』, 『위치정보의 보호 및 이용 등에 관한 법률』, 전자정부법, 주민등록법, 국세기본법, 통신비밀보호법, 보건의료기본법, 『특정범죄신고자등 보호법』, 『금융실명거래 및 비밀보장에 관한 법률』, 형법 등	개별 분야별로 업무상 비밀보호 및 정보보호 규정 산재

개별 분야별로 개인정보보호에 관한 특별규정을 두고 있는 경우로서 대표적인 법률과 관련 규정의 주요 내용을 개략적으로 살펴보면 아래의 [표 2-2-2]와 같다.

[표 2-2-2] 개별 분야별 개인정보보호입법과 주요 내용

대상 정보	관련 법률	규 정 내 용
정부 기록 정보	『공공기관의 개인정보 보호에 관한 법률』	○ 국가, 지방자치단체 등 정부기관 보유의 개인정보 보호
	『공공기관의 정보공개에 관한 법률』	○ 국민의 알 권리 보장을 위한 공공기록의 공개, 열람
	전자정부법	○ 당사자의사에 반하는 개인정보사용의 금지 등
	주민등록법	○ 전국민에 대한 주민등록번호의 부여 등
통신 비밀	통신비밀보호법 등	○ 우편물의 검열, 전기통신의 감청, 통신사실 확인 자료의 제공, 타인간의 대화를 녹음 또는 청취 금지 등 통신관련 사생활의 보호
	『통신제한조치의 허가절차 및 비밀유지에 관한 규칙』	○ 범죄수사나 개인안보를 위한 통신제한조치의 허가절차
	전기통신사업법	○ 개별이용자에 관한 정보의 공개 및 유용금지 등
보건 의료 정보	보건의료기본법	○ 보건의료정보의 누출, 변조 금지
	의료법, 전염병예방법 등	○ 업무상 비밀 누설 금지
	『생명윤리 및 안전에 관한 법률』	○ 유전정보의 보호 등
소비자 정보	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	○ 정보통신망사업자의 개인정보보호
	『위치정보의 보호 및 이용 등에 관한 법률』	○ 위치정보사업자 등의 개인위치정보의 보호
	『신용정보의 이용 및 보호에 관한 법률』	○ 금융기관, 백화점, 할부회사 등의 고객 신용정보 보호
	『금융실명거래 및 비밀보장에 관한 법률』	○ 신용정보주체의 열람 및 정정 청구 등
	증권거래법 등	○ 금융실명거래에 따른 금융기관이용자의 개인정보 이용 등
사생활 일반	형법 제316조(비밀침해죄)	○ 봉합 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록 등 특수매체기록에 대한 기술적 침해

제 2 절 「공공기관의 개인정보 보호에 관한 법률」

1. 연 혁

(1) 1994년 제정법

「공공기관의 개인정보 보호에 관한 법률」은 국가주요업무에 대한 전산화의 확대추진과 전국적 행정전산망의 구축 등으로 개인정보의 무단 사용 또는 무단유출로 인한 개인사생활의 침해 등 각종 부작용이 우려됨에 따라, 공공기관이 컴퓨터에 의하여 개인정보를 취급함에 있어서 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 개인의 권리와 이익을 보호하기 위해 1994년 1월 7일에 제정되었다.

이 법이 적용되는 대상정보는 공공기관이 컴퓨터에 의해 개인정보를 취급함에 있어서 필요한 사항을 정하는 것을 목적으로 하기 때문에, 종래부터 공공기관이 보유하고 있는 종이문서상의 개인정보는 적용이 제외된다. 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에 정하는 바에 의한다고 규정되어 있기 때문에(법 제3조 제1항), 이 법은 공공기관의 컴퓨터로 처리된 개인정보의 보호에 관한 일반법의 지위를 갖고 있다. 제정법은 다음과 같은 내용을 담고 있었다.

- ① 공공기관 정보화일의 보유에 대한 통보
- ② 공공기관이 보유한 정보화일의 관보 공개와 일반인 열람
- ③ 정보주체의 동의가 있는 등의 사항을 제외하고는 개인정보화일의 보유 목적외 용도로 이용금지
- ④ 정보주체의 열람청구, 내용정정청구권
- ⑤ 민간기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 컴퓨터를 사용하여 개인정보를 처리하는 개인 또는 단체에 대

하여는 공공기관의 예에 준하여 개인정보의 보호를 위한 조치를 강구하도록 하였다.

- ⑥ 공공기관의 개인정보처리사무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 말소한 자는 10년 이하의 징역에 처하도록 하며, 개인정보를 누설 또는 권한 없이 처리하거나 개인의 이용에 제공하는 등 부당한 목적으로 사용한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하였다.

(2) 1999년 개정법

법은 1999년 1월 29일 개정을 통해 개인정보를 제공할 수 있는 경우를 본인이 의사표시등을 하지 못하는 경우로서 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 되는 경우로 한정하도록 하여 개인정보의 제공요건을 보다 엄격하게 정하였다(법 제10조 제2항 제5호).

(3) 2007년 개정법

2007년 5월 17일 동법은 폐쇄회로 텔레비전의 설치 및 화상정보보호 등에 관한 법적 근거를 마련하기 위한 개정이 이루어졌다. 이와 동시에 정보주체의 권리를 확대하고 처리정보 보유기관의 안전성 확보조치 의무를 강화하는 방향으로 여러 규정이 개정되거나 신설되었다. 이 때 개정된 법률의 주요내용은 다음과 같다.

첫째, 폐쇄회로 텔레비전의 설치 및 화상정보보호와 관련된 개념을 새롭게 조정하고, 특히 “폐쇄회로 텔레비전”을 정의하는 조항을 신설하였다(제2조 제5의2).

둘째, 개인정보보호의 원칙에 관한 규정을 신설하였다(제3조의2). 이에 따르면 공공기관의 장은 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적법하고 정

당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 아니 된다. 그리고 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 하며, 개인정보관리의 책임관계를 명확히 하여야 한다. 또한 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다.

셋째, 공공기관의 장으로 하여금 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있게 안내하도록 하는 조항도 신설하였다(제4조 제2항).

넷째, 폐쇄회로 텔레비전의 설치, 관리 및 그 위탁에 관한 규정을 신설하였다(제4조의2 및 제4조의3). 범죄예방 및 교통단속 등 공익을 위하여 필요한 경우에 공청회 등 대통령령으로 정하는 절차를 거쳐 관련 전문가 및 이해관계인의 의견을 수렴한 후 폐쇄회로 텔레비전을 설치할 수 있도록 하고, 설치된 폐쇄회로 텔레비전은 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추는 것을 금지시키고, 녹음기능도 사용할 수 없도록 하였다. 또한 폐쇄회로 텔레비전을 설치하는 경우 정보주체가 이를 쉽게 인식할 수 있도록 일정한 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 하도록 하였다. 나아가 일정한 조건하에서 폐쇄회로 텔레비전의 설치 및 관리에 관한 사무를 위탁할 수 있도록 하였다.

다섯째, 보유기관의 장으로 하여금 개인정보보호방침을 정하여 그 내용을 관보 또는 인터넷 홈페이지 등에 게재하여야 하도록 하는 조항을 신설하였다(제7조의2).

여섯째, 공공기관의 장으로 하여금 인터넷상의 본인확인 과정에서 주민등록번호, 성명 등의 개인정보가 변조·유출 또는 도용되지 아니 하도록 안전성 확보에 필요한 조치를 강구하도록 하는 인터넷상의 본

인확인과 관련된 조항을 신설하였다(제9조의2).

일곱째, 보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공할 수 없도록 개정하고(제10조 제1항), 나아가 보유목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한하도록 하는 조항을 신설하였다(제10조 제2항).

여덟째, 개인정보파일의 파기에 관한 규정을 신설하였다(제10조의2). 이에 따르면 보유기관의 장은 개인정보파일의 보유목적 달성 등 당해 개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 그러하지 아니하다. 개인정보파일을 파기한 경우 보유기관의 장은 개인정보파일을 파기한 사실을 관보 또는 인터넷 홈페이지 등에 공고하여야 한다.

아홉째, 본인의 처리정보를 열람한 정보주체는 보유기관의 장에게 문서로 당해 처리정보의 정정 이외에 그 삭제도 청구할 수 있도록 하였다(제14조).

열째, 열람청구 및 정정·삭제청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판을 청구하는 외에도 행정소송을 제기할 수 있도록 하였다(제15조).

열한째, 공공기관의 장이 개인정보를 수집·처리하거나 개인정보파일을 보유함에 있어서 개인정보에 관한 권리 또는 이익의 침해를 받은 자는 행정자치부장관에게 그 침해사실을 신고할 수 있도록 하는 조항을 신설하였다(제18조의2).

열두째, 기존의 개인정보보호심의위원회를 “공공기관개인정보보호심의위원회”로 개칭하고, 그 심의사항을 보다 구체화하였으며, 그 조직

과 운영에 관한 사항을 대통령령에서 규정하도록 하던 것을 동 법률에서 직접 규정하였다(제20조). 이에 따르면 동 위원회는 위원장 1인을 포함한 10인 이내의 위원으로 구성하며, 위원장은 행정자치부차관으로 하고, 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자 중에서 위원장의 추천으로 국무총리가 임명 또는 위촉한다. 그리고 위원의 임기는 2년으로 한다.

열셋째, 공공기관의 장으로 하여금 소관 처리정보의 보호 및 관리를 위하여 개인정보관리책임관을 지정하도록 하는 조항을 신설하였다(제20조의2).

2. 현행 법률의 주요 내용

(1) 적용범위

이 법은 공공기관이 보유하고 있는 개인정보로 컴퓨터로 처리되는 정보를 대상으로 한다(제1조). 따라서 이 법의 적용범위는 “공공기관 등”과 “컴퓨터로 처리되는 개인정보”이다.

1) 공공기관 등

법 제2조 제1호와 대통령령에 의하여 이 법이 적용되는 공공기관 등은 법이 정하는 국가행정기관, 지방자치단체와 대통령령이 정하는 기타기관으로 「초중등교육법」 및 「고등교육법」 기타 다른 법률에 의하여 설치된 각급 학교, 「정부투자기관관리기본법」 제2조의 규정에 의한 정부투자기관, 특별법에 의해 설립된 특수법인, 공무원연금법 제47조 제2호 및 제3호의 규정에 의한 퇴직연금의 지급정지대상기관중 제2호 및 제3호에 해당하지 아니하는 기관을 말한다. 이에 따르면 대부분의 공공기관의 컴퓨터 파일로 처리되는 개인정보가 이 법의 적용을 받게 된다.

2) 보호대상인 개인정보

이 법의 보호를 받는 개인정보는 “생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보를 말한다. 그러나 비록 당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것은 이 법의 보호대상이 되는 개인정보에 포함된다.

이러한 개인정보는 컴퓨터로 처리되는 것에만 한정되어 일반 문서에 의한 개인정보는 이 법의 보호대상 정보에서 제외된다.

3) 개인정보보호의 원칙(제3조의2)

공공기관의 장은 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 아니 된다(제1항). 그리고 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 한다(제2항). 또한 공공기관의 장은 개인정보관리의 책임관계를 명확히 하여야 하며(제3항), 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다(제4항).

(2) 개인정보 관리기관의 의무(공공기관 등)

1) 수집·보유의 제한

공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 안 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 예외가 인정된다(제4조 제1항). 그리고 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리

등에 관하여 문서 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여야 한다. 다만, 제6조 제3항 각 호의 어느 하나에 해당하는 개인정보파일을 보유할 목적으로 개인 정보를 수집하는 경우는 예외로 한다(제4조 제2항).

공공기관은 소관업무를 수행하기 위하여 필요한 범위안에서 개인정보파일을 보유할 수 있다(제5조). 이 때 필요한 범위 내에서 보유한 개인정보파일과 소관업무의 목적과는 필요성원칙과 비례성의 원칙이 충족되어야 한다.²⁷⁶⁾

2) 폐쇄회로 텔레비전의 설치, 관리

공공기관의 장은 범죄예방 및 교통단속 등 공익을 위하여 필요한 경우에 공청회 등 대통령령으로 정하는 절차를 거쳐 관련 전문가 및 이해관계인의 의견을 수렴한 후 폐쇄회로 텔레비전을 설치할 수 있다(제4조의2 제1항). 설치된 폐쇄회로 텔레비전은 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추어서는 아니 되며, 녹음 기능은 사용할 수 없다(제4조의2 제2항). 공공기관의 장은 폐쇄회로 텔레비전을 설치하는 경우 정보주체가 이를 쉽게 인식할 수 있도록 소정의 사항(설치목적 및 장소, 촬영범위 및 시간, 관리책임자 및 연락처)을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다(제4조의2 제3항). 다만 국가안전보장과 관련된 국가중요시설 중 원자력발전소 등 대통령령으로 정하는 시설에 대하여는 안내판 설치 등의 조치를 취하지 않아도 된다(제4조의2 제4항). 폐쇄회로 텔레비전의 설치, 안내판 설치 등에 관하여 필요한 사항은 대통령령으로 정한다(제4조의2 제5항). 그리고 공공기관의 장은 폐쇄회로 텔레비전의 설치 및 관리에 관한 사무를 위탁할 수 있다(제4조의3 제1항).

276) 행정자치부, 공공기관의 개인정보보호제도 이해와 해설, 2003. 3. 25면.

3) 개인정보파일의 보유·변경시 사전협의 및 공고, 개인정보보호방침

공공기관의 장이 개인정보파일을 보유하고자 하는 경우에는 개인정보파일의 명칭, 개인정보파일의 보유목적, 보유기관의 명칭, 개인정보파일에 기록되는 개인 및 항목의 범위, 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭, 개인정보파일의 열람예정시기, 열람이 제한되는 처리정보의 범위 및 그 사유 등의 사항을 행정안전부장관과 협의하여야 하며, 그 가운데 어느 하나에 해당하는 사항을 변경하고자 하는 경우에도 마찬가지이다(제6조 제1항). 행정안전부장관은 협의한 사항을 대통령령이 정하는 바에 따라 연 1회 이상 관보 또는 인터넷 홈페이지 등에 게재하여 공고하여야 한다(제7조). 보유기관의 장은 당해 기관이 보유하고 있는 개인정보파일별로 협의사항을 기재한 대장(개인정보파일대장)을 작성하여 일반인이 열람할 수 있도록 하여야 한다(제8조).

그 밖에도 보유기관의 장은 제6조 제1항의 협의사항, 개인정보관리책임관의 성명·소속 부서·직위 및 전화번호 그 밖의 연락처, 인터넷 홈페이지 접속정보파일 등 인터넷 홈페이지를 통하여 수집되는 개인정보의 보호에 관한 사항 등의 내용이 포함된 개인정보보호방침을 정하여야 하며, 개인정보보호방침을 정한 경우에는 그 내용을 관보 또는 인터넷 홈페이지 등에 게재하여야 한다(제7조의2).

4) 개인정보파일의 안전성 확보 및 인터넷상의 본인확인

공공기관의 장은 개인정보를 처리하거나 개인정보파일을 정보통신망에 의하여 송·수신하는 경우 개인정보가 분실·도난·누출·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 조치를 강구하여야 한다(제9조 제1항). 그리고 개인정보의 처리에 관한 사무를 다른 공공기관 또는 관련 전문기관에 위탁하는 경우에도 마찬가지이다(제9조 제2항).

또한 공공기관의 장은 인터넷상의 본인확인 과정에서 주민등록번호, 성명 등의 개인정보가 변조·유출 또는 도용되지 아니하도록 안전성 확보에 필요한 조치를 강구하여야 한다(제9조의2).

5) 처리정보의 이용 및 제공 제한

보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니 된다(제10조 제1항). 그리고 보유기관의 장은 보유 목적에 따라 처리정보를 이용하게 하거나 제공하는 경우에도 업무수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한하여야 한다(제10조 제2항).

그러나 ① 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, ② 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 공공기관개인정보보호심의위원회의 심의를 거친 경우, ③ 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우, ④ 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우, ⑤ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소부명 등으로 동의를 할 수 없는 경우로서 정보주체 외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우, ⑥ 범죄의 수사나 공소의 제기 및 유지에 필요한 경우, ⑦ 법원의 재판업무 수행을 위하여 필요한 경우에는 해당 개인정보의 파일을 보유목적 이외로 이용하거나 제공할 수 있다(제10조 제3항 본문). 다만, 다음 각 호의 어느 하나에 해당하는 경우에도 정보주체 또는 제3자의 권리와

이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다(제10조 제3항 단서).

6) 개인정보파일의 즉시파기

보유기관의 장은 개인정보파일의 보유목적 달성 등 당해 개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 그러하지 아니하다(제10조의2).

7) 개인정보취급자의 의무

개인정보의 처리를 행하는 공공기관의 직원이나 직원이었던 자 또는 공공기관으로부터 개인정보의 처리업무를 위탁받아 그 업무에 종사하거나 종사하였던 자는 직무상 알게 된 개인정보를 누설 또는 권한없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위항 사용해서는 안 된다(제11조).

(3) 공공기관 외의 개인 또는 단체의 의무

공공기관 외의 개인 또는 단체는 컴퓨터등을 사용하여 개인정보를 처리함에 있어 공공기관의 예에 준하여 개인정보의 보호를 위한 조치를 강구하여야 하며, 관계 중앙행정기관의 장은 개인정보의 보호를 위하여 필요한 때에는 공공기관 외의 개인 또는 단체에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다(제22조). 그러나 이 조항의 집행을 담보할 세부내용이 규정되어 있지 않아 선언적 효력만을 가지고 있다.

(4) 정보주체의 권리

1) 열람청구권 및 정정·삭제청구권

정보주체는 개인정보파일대장에 기재된 범위 안에서 문서로 본인에 관한 처리정보의 열람(문서에 의한 사본의 수령을 포함)을 보유기관의 장에게 청구할 수 있다(제12조). 그리고 본인의 처리정보를 열람한 정보주체는 보유기관의 장에게 문서로 당해 처리정보의 정정 또는 삭제를 청구할 수 있다. 다만, 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있는 경우에는 그 삭제를 청구할 수 없다(제14조).

정보주체의 열람청구권 및 정정·삭제청구권은 공공기관 보유정보의 정확성과 최신성을 확보하고, 잘못된 개인정보를 근거로 한 행정청의 행위로 인해 정보주체가 손해를 보는 것을 예방하는 차원에서 정보주체에게 부여된 권리이다.

2) 불복청구권

정보주체의 열람청구 및 정정·삭제청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판을 청구하거나 행정소송을 제기할 수 있다(제15조).

(5) 개인정보보호기구 : 행정안전부장관, 공공기관개인정보보호심의위원회, 개인정보관리책임관

1) 행정안전부장관

공공기관개인정보보호법의 집행기관은 일차적으로 행정안전부장관이라고 할 수 있다. 현행의 동 법률에 의하면 행정안전부장관은 이 법의 시행을 위하여 필요하다고 인정되는 경우에는 공공기관의 장에 대하여 개인정보의 처리에 관한 자료의 제출을 요구할 수 있으며, 소

속공무원으로 하여금 실태조사를 하게 할 수 있다(제18조 제1항). 공공기관의 장이 개인정보를 수집·처리하거나 개인정보파일을 보유함에 있어서 개인정보에 관한 권리 또는 이익의 침해를 받은 자는 행정안전부장관에게 그 침해사실을 신고할 수 있으며(제18조의2 제1항), 행정안전부장관은 신고된 침해사실을 확인하여 해당 공공기관의 장에게 그 확인결과를 통보할 수 있다(제18조의2 제2항). 확인결과의 통보를 받은 공공기관의 장은 그 처리결과를 지체 없이 행정안전부장관에게 통보하여야 하며, 행정안전부장관은 통보받은 처리결과를 제1항에 따른 신고인에게 통지하여야 한다(제18조의2 제3항). 행정안전부장관은 이 법의 목적을 달성하기 위하여 필요하다고 인정되는 경우에는 공공기관의 장에게 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다(제19조).

2) 공공기관개인정보보호심의위원회

공공부문에서의 개인정보보호에 관한 심의기구로서 공공기관개인정보보호심의위원회가 있다. 현행법상 공공기관의 컴퓨터등에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위하여 국무총리소속하에 공공기관개인정보보호심의위원회를 두고 있다(제20조 제1항). 개인정보보호심의위원회의 업무는 ① 개인정보보호에 관한 정책 및 제도 개선에 관한 사항, ② 처리정보의 이용 및 제공에 대한 공공기관 간의 의견조정에 관한 사항, ③ 개인정보파일의 보유·변경시의 사전협의사항에 관해 행정안전부장관으로부터 심의요청을 받은 사항, ④ 그 밖에 개인정보의 보호에 관하여 대통령령으로 정하는 사항을 심의하는 역할을 한다(제20조 제2항). 위원회는 위원장 1인을 포함한 10인 이내의 위원으로 구성하며(제20조 제3항), 위원회의 위원장은 행정안전부차관으로 하고, 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자 중에서 위원장의 추천으로 국무총리가 임명 또는 위촉한

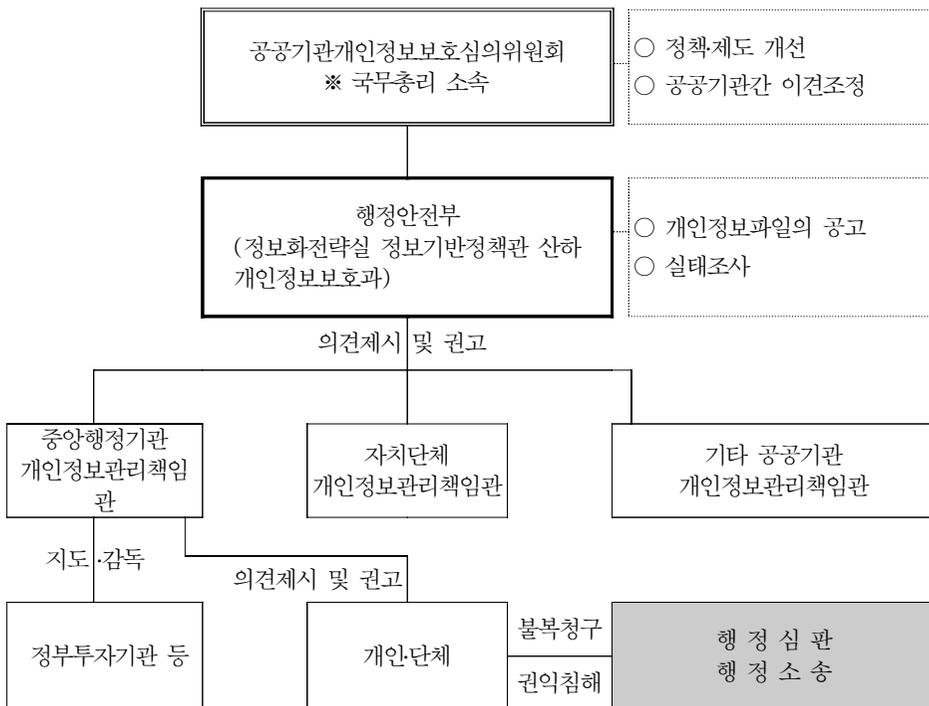
다(제20조 제4항). 위원의 임기는 2년이다(제20조 제5항).

공공기관개인정보보호심의위원회는 중요한 개인정보 정책이나 제도를 심의하는 기능만을 가질 뿐, 의견제시나 시정권고 등은 행정안전부가 담당하고, 피해구제는 행정심판, 행정소송, 국민권익위원회 등이 담당하고 있다. 이러한 점에서 볼 때 공공기관개인정보보호심의위원회의 실질적인 개인정보보호 기능은 미약하다고 평가할 수 있다.

3) 개인정보관리책임관

한편, 공공기관의 장은 소관 처리정보의 보호 및 관리를 위하여 개인정보관리책임관을 지정하여야 한다(제20조의2).

[그림 2-2-1] 공공기관 개인정보보호법의 집행체계



(6) 벌 칙

이 법이 정한 의무를 위반하여 개인정보의 침해를 예방하고 법규 위반자를 처벌하기 위해 벌칙조항을 두고 있다(제23조). 우선 ① 공공기관의 개인정보처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경 또는 삭제한 자는 10년 이하의 징역에 처하고, ② 개인정보취급자가 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적으로 사용한 자는 3년 이하의 징역 또는 1천만 원 이하의 벌금에 처하며, ③ 부정한 목적으로 제4조의2 제2항을 위반하여 폐쇄회로 텔레비전의 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자와 거짓 그 밖의 부정한 방법으로 공공기관으로부터 처리정보를 열람 또는 제공받은 자는 2년 이하의 징역 또는 700만 원 이하의 벌금에 처하도록 하였다(제23조). 그러나 공공기관의 다른 의무들, 즉 ① 수집·보유의 제한, ② 개인정보파일의 사전 통보 및 공고, ③ 개인정보파일의 안전성·정확성·최신성 확보, ④ 처리정보의 이용 및 제공 제한 등에 대하여는 벌칙조항이 없기 때문에 이 법 자체로 이런 행위를 예방하거나 처벌할 수는 없고, 단지 감사기관 감사의 지적사항이 될 수 있을 뿐이다. 따라서 공공기관의 개인정보관리에 대한 통제는 그리 강하지 않다고 볼 수 있다.

제 3 절 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

1. 입법의 배경

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 그 이전의 법률을 대체하는 법률이다. 원래 이 법률은 1985년에 제정된 ‘전산망

보급확장과 이용촉진에 관한 법률’이 그 모태이다. 전산망법은 원래 한국에서의 전산망보급을 위한 입법이었으나 그간 정보통신망의 보급이 일정한 수준에 이룸에 따라 이제 정보통신망보급에 따라 야기되는 개인정보보호를 위한 입법적 조치가 필요하게 되었다.

이에 1998년에는 이 법률을 대체하는 「정보통신망 이용촉진 등에 관한 법률」로 개정되었다. 원래 이 개정 법률에서는 그간 사적 부문에서의 개인정보보호에 관한 입법적 미비를 시정하고자 하는 강력한 의지를 반영하려고 하였으나, 이 법률이 갖는 한계로 인하여 최소한의 개인정보보호를 위한 규정을 마련하는데 그쳤고, 이에 따라 입법명칭에서도 개인정보보호 내지 정보보호에 관한 명시적인 내용을 설정하지 못하였다. 그러나 이 법률의 개정과정에서 개인정보보호의 중요성을 충분히 인정하여 최소한의 입법적 조치를 가한 바 있다.²⁷⁷⁾ 즉 이 법률은 종래의 전산망 보급 확장에서 그 중점이 이제 정보통신망 이용촉진과 개인정보보호로 이행하는 과정상의 법률이라 할 수 있다.

그런데 이 정보통신망법이 시행된 지 채 1년도 안 돼 사적 부문에서의 정보보호에 관한 국민적 요구가 증대되었고, 이에 따라 다시금 ‘정보통신망 이용촉진 등에 관한 법률’의 재개정논의가 2000년 초부터 진행되었다. 이에 그간의 논의를 종합하여 새로이 모습을 드러낸 것이 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이다. 즉 이 법률은 이제 정보통신망 이용촉진에서 오히려 정보통신망 이용에 따라 야기되는 역기능에 대처하기 위하여 개인정보보호와 불법정보로부터의 개인의 보호에 중점을 두고 있다.²⁷⁸⁾ 원래 논의 과정에서 이 법률에서는 개인정보보호에 관한 사항을 중점적으로 다루고 불법정보에

277) 이 때 진행된 연구의 상세는, 성낙인 외, 『개인정보보호를 위한 정책방안 연구』 (정보통신부, 1999) 참조.

278) 개정에 관한 논의의 기본적 의의와 내용은 정보통신부, 『정보통신망이용촉진등에관한법률 개정을 위한 공청회 자료집』, 2000.7.20; 김철완·이민영, 『인터넷 개인정보보호에 관한 법제도 연구』 (정보통신정책연구원, 2000) 참조.

대한 대책으로서의 건전한 정보통신윤리에 관한 사항은 새로운 법률을 제정하는 방향으로 설계되어 있었으나, 개인정보보호와 불법정보문제를 이 법률에서 통합적으로 규제함으로써 인하여 법률의 명칭에 개인정보보호가 아닌 정보보호로 규정하게 되었다.

2. 관련 규정의 변천

(1) 2001년 제정법의 골자

2001년 1월 16일에 제정된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 정보통신서비스이용자의 개인정보를 보호하기 위하여 정보통신서비스제공자에 대한 규제를 강화하고, 타인의 정보통신서비스제공을 위하여 집적된 정보통신시설의 안정적 운영을 위한 제도를 신설하는 것을 주요 골자로 하고 있다. 이 법에서 개인정보보호와 관련된 주된 내용은 다음과 같다.

- ① 정보통신서비스제공자가 개인정보의 수집·처리·관리 등을 타인에게 위탁하는 경우에 그 타인의 개인정보보호위반행위에 대하여 책임을 지도록 하고, 정보통신서비스제공자외의 자가 정보통신망을 이용하여 개인정보를 수집·저장·처리하는 경우에도 이 법에 의한 개인정보보호 관련 의무를 부과하도록 하였다.
- ② 14세 미만의 아동으로부터 개인정보를 수집하는 경우 법정대리인의 동의를 받도록 하고, 법정대리인에게 아동의 개인정보에 대한 열람 및 정정 요구권을 부여하였다(법 제31조).
- ③ 개인정보와 관련된 분쟁을 간편·신속하게 조정하기 위하여 개인정보분쟁조정위원회를 설립하고, 동위원회의 구성·운영 및 조정절차 등에 관한 사항을 정하였다(법 제33조 내지 제40조).
- ④ 타인의 정보통신서비스제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자에게 정보통신시설의 안정적 운영을 위한 보

호조치 등을 마련하도록 하였다(법 제46조).

(2) 2002년의 법률개정

이후 동법은 개인정보 침해행위에 적절히 대응하고, 불법하게 개인정보를 제공받은 자를 처벌함으로써 국민의 사생활을 보호하기 위해 2002년 12월 18일 대폭적인 개정이 단행되었다. 주된 개정내용은 다음과 같다.

- ① 전자우편주소 수집을 거부하는 의사를 명시한 인터넷 홈페이지 등에서 자동으로 전자우편주소를 추출하는 프로그램 등을 이용하여 타인의 전자우편주소를 수집·판매·유통·이용하는 행위를 금지하였다(법 제50조의2 신설).
- ② 개인정보침해 및 불법 스팸메일에 관한 민원을 효과적으로 처리하기 위하여 한국정보보호진흥원에서 민원처리를 위한 자료제출 및 검사에 관한 업무를 처리할 수 있도록 위탁 근거를 마련하였다(법 제56조제3항 신설).
- ③ 개인정보를 수집한 때에 고지한 목적이나 개인정보를 제공받은 목적 범위 외로 개인정보를 불법하게 제3자에게 제공한 자를 처벌하는 외에 그 정을 알고 영리 또는 부정한 목적으로 개인정보를 제공받은 자를 함께 처벌하도록 하였다(법 제62조 제1호 및 제2호).

(3) 2004년의 법률개정

이후 법은 2004년 1월 19일 무단으로 수집되거나 유출 또는 남용될 위험이 있는 이용자의 개인정보를 보호하기 위하여 정보통신서비스제공자의 의무를 강화하고, 다양해지고 있는 인터넷 침해사고에 효과적으로 대응하기 위하여 인터넷에 대한 침해사고 대응체계를 강화하며, 정보통신서비스제공에 관한 사업을 하는 자에 대하여 당해 서비스의 정보보호에 필요한 조치를 하도록 하는 일부개정을 단행했다. 주요

개정내용은 다음과 같다.

① 정보통신서비스제공자는 이용자의 개인정보 수집에 대하여 동의를 얻고자 하는 경우에는, 인터넷 접속정보파일 등 자동으로 개인정보를 수집하는 장치의 설치·운영 및 그 거부에 관한 사항을 고지하거나 이용약관에 명시하도록 하였다(법 제22조 제2항 제5호 신설).

② 정보통신서비스 이용자는 정보통신서비스제공자등에 대하여 자신의 개인정보를 이용하거나 제3자에게 제공한 명세를 요구할 수 있고, 정보통신서비스제공자등은 지체 없이 이에 필요한 조치를 취하도록 하였다(법 제30조 제2항).

③ 인터넷 정보보호를 강화하기 위하여 전국적으로 정보통신망 접속서비스를 제공하는 자 등에 대하여 정보보호지침의 준수를 의무화하고 매년 정보보호 안전진단을 받도록 하였다(법 제45조 제4항 및 제46조의3 신설).

④ 침해사고가 발생하여 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있는 경우에 집적정보통신시설 사업자는 당해 서비스 제공의 전부 또는 일부를 중단하는 긴급조치를 할 수 있도록 하였다(법 제46조의2 신설).

⑤ 정보통신부장관은 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 이를 권고할 수 있도록 하고, 주요정보통신서비스제공자는 정보통신망에 중대한 침해사고가 발생하여 정보통신망 등에 심각한 장애가 발생할 가능성이 높은 경우에는 이용자에게 보호조치를 취하도록 요청할 수 있도록 하였다(법 제47조의2 신설).

⑥ 정당한 권한 없이 또는 허용된 접근권한을 초과하여 부정확한 목적으로 타인의 정보통신망에 침입을 시도한 자도 처벌할 수 있도록 하는 등 벌칙을 강화하였다(법 제63조 제2항 신설).

(4) 2005년의 법률개정

2005년 12월 30일 개정된 법률에서는 피싱 등의 수법을 이용한 금융사기 피해 등을 원천적으로 방지하기 위하여, 정보통신망을 통하여 기망의 방법으로 타인의 정보를 수집하는 행위를 금지하고(법 제49조의2), 이를 위반하였을 때에는 3년 이하의 징역 또는 3천만원 이하의 벌금을 부과하도록 하였다(제63조제1항 제3호 및 제4호).

(5) 2006년의 법률개정

2006년 10월 4일 개정된 법률에서는 종업원 수·정보통신서비스 이용자 수 등이 정보통신부령으로 정하는 기준 이하인 정보통신서비스제공자 등은 개인정보관리책임자를 지정하지 아니할 수 있도록 하고(법 제27조 제1항 단서 신설), 오류를 정정하지 아니하더라도 정정하지 못하는 사유를 이용자에게 통지하는 등 필요한 조치를 취한 경우에는 해당 개인정보를 제공 또는 이용할 수 있도록 하였다(법 제30조 제5항).

(6) 2007년의 법률개정

2007년 1월 26일, 정보통신망을 이용한 신규서비스의 보급 및 이용 확산 등 정보통신환경의 변화에 따라 새롭게 등장하는 개인정보침해 문제에 적극 대처하기 위하여 개인정보의 수집·이용·제공 등에 관한 절차를 강화하는 법률의 개정이 단행되었다. 그 주요 내용은 다음과 같다.

- ① 개인정보의 수집·이용·제공에 대한 고지 및 동의제도 개선·보완 : 개인정보를 수집하는 경우에 고지하고 동의를 얻어야 할 사항을 수집·이용 목적, 수집하는 개인정보의 항목 등 3가지로 명확하게 구분하고, 정보통신서비스제공자가 이용자의 개인정보를

제3자에게 제공할 경우에도 그에 따른 별도의 고지를 하고 동의를 얻도록 함과 아울러 제공받은 자가 개인정보를 이용·제공할 수 있는 범위를 명확하게 규정하였다(법 제22조제1항, 법 제24조의2 신설).

② 개인정보의 취급위탁에 따른 관리·감독 강화 : 정보통신서비스 제공자 등이 제3자로 하여금 이용자의 개인정보를 수집 등 취급할 수 있도록 그 업무를 위탁하는 경우에는 원칙적으로 이용자의 동의를 얻도록 하되, 계약의 이행을 위하여 필요한 경우에는 그 위탁업무의 내용 및 수탁자에 관한 사항을 이용자가 알 수 있도록 개인정보취급방침을 제정하여 인터넷 홈페이지 등에 공개하거나 이용자에게 통지하는 것으로 갈음할 수 있도록 하고, 수탁자가 이용자의 개인정보를 이용할 수 있는 목적을 지정하여 지정된 목적 외로 이용 또는 제공하지 못하도록 수탁자의 책임을 강화하였다(법 제25조).

③ 제한적인 본인확인제도의 도입 : 국가기관, 지방자치단체, 정부투자기관 등 공공기관 등과 정보통신서비스 유형별 일일평균 이용자수 10만 명 이상으로서 대통령령으로 정하는 일정 기준에 해당하는 정보통신서비스제공자가 게시판을 설치·운영하는 경우에는 게시판 이용자에 대한 본인확인을 위하여 필요한 조치를 취하도록 하고, 정보통신서비스제공자가 본인확인을 위하여 필요한 조치를 취하지 않은 경우 정보통신부장관이 시정명령을 하도록 하고 정보통신서비스제공자가 이를 이행하지 않은 경우에는 과태료를 부과하도록 하였다(법 제44조의5 및 제67조제1항제1호 신설).

(7) 2008년의 법률개정

2008년 6월 13일 개정된 동법에서는, 정보통신서비스 제공자가 이용자의 동의를 받지 아니하고 개인정보를 제3자에게 제공하는 사례가

발생함에 따라 정보통신망을 통한 개인정보의 침해행위를 방지하고, 침해행위에 대한 제재의 실효성을 높이기 위하여 개인정보 보호 규정을 위반한 전기통신사업자에게 그 부당이득을 환수하기 위한 과징금을 부과하고, 일부 과태료 부과대상 행위를 형사처벌 대상으로 변경하며, 현재의 과태료 부과금액을 상향 조정하였다(시행일 2008.12.14). 주요 개정내용은 다음과 같다.

- ① 주민등록번호 외의 회원 가입방법 : 정보통신서비스 제공자로서 유형별 일일 평균 이용자 수가 일정 기준에 해당하는 자는 이용자에게 주민등록번호를 사용하지 아니하고도 회원가입을 할 수 있는 방법을 의무적으로 제공하도록 하였다(법 제23조의2 신설).
- ② 개인정보 보호의무 위반행위에 대한 과징금 부과 : 개인정보의 무단 수집·이용·유출, 보호조치 미이행 등 개인정보 보호의무 위반 행위자에게 과징금을 부과하여 그 위법행위로 인한 사업수익의 일부를 환수하도록 하였다(법 제64조의3 신설).
- ③ 과태료 부과대상 행위를 형사처벌 대상으로 상향 조정 : 과태료 부과대상 개인정보 보호의무 위반행위 중 이용자의 동의를 받지 아니하고 개인정보를 수립한 자 등 위법성이 큰 일부 행위자를 형사처벌 대상으로 상향 조정하였다(법 제71조 및 제73조).

3. 현행법의 주요 내용

(1) 적용대상의 범위

이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활 향상과 공공복리의 증진에 이바지함을 목적으로 하고 있다(제1조). 따라서 정보통신서비스 제공자와 정보통신서비스를 이용하는 자의 개인정보가 적용대상이 된다.

1) 정보통신서비스제공자

정보통신서비스제공자라 함은 「전기통신사업법」 제2조 제1항 제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말하는 것으로, 유·무선 전화, 초고속 인터넷서비스제공자와 같은 통신사업자와 인터넷서비스제공자(ISP) 등이 해당된다(제2조 제1항 제3호).

그러나 동법은 제67조에서 정보통신서비스제공자 이외의 자가 개인정보를 수집·저장·처리하는 경우에도 준용하고 있다. 이에 따라 오프라인 사업자로 여행업, 호텔업자, 항공운송업자, 학원, 교습소, 기타 회원제로 개인정보를 수집하여 재화나 용역을 공급하는 사업자 등에도 동법상 개인정보보호 관련 조항이 적용된다. 이렇게 보면 동법의 적용대상을 정보통신서비스제공자에 한정하고 있지는 않다고 할 수 있다.²⁷⁹⁾

2) 보호대상인 개인정보

이 법의 보호대상인 개인정보는 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보를 말한다(제2조 제1항 제6호).

(2) 정보통신서비스제공자의 의무

1) 개인개정보의 수집·이용 동의 등

정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 ① 개인정보의 수집·이용 목적, ② 수집하는 개인정보의 항목, ③ 개인정보의 보유·이용 기간 등을 모두 이용자에게 알리

279) 이창범·윤주연, 『각국의 개인정보피해구제제도 비교연구』 (개인정보분쟁조정위원회, 2003), 54면.

고 동의를 받아야 한다(제22조 제1항). 다만 ① 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우, ② 정보통신서비스 제공에 따른 요금정산을 위해 필요한 경우, ③ 이 법 또는 다른 법률에 특별한 규정이 있는 경우에는 예외가 인정된다(제22조 제2항). 이에 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제1호).

2) 개인정보의 수집 제한 등

정보통신서비스 제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다(제23조 제1항). 이에 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제2호). 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다(제23조 제2항). 이에 위반할 경우 3천만원 이하의 과태료를 부과한다(제76조 제1항 제1호).

한편 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 통하여 회원으로 가입할 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 하며, 이 경우 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다(제23조의2). 이에 위반할 경우 3천만원 이하의 과태료를 부과한다(제76조 제1항 제2호).

3) 개인정보의 이용 제한

정보통신서비스 제공자는 수집한 개인정보를 이용자로부터 동의받은 목적이나 정보통신서비스의 제공에 관한 계약의 이행이나 정보통신서비스 제공에 따른 요금정산 이외의 목적으로 이용하여서는 아니 된다(제24조). 이에 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제3호).

4) 개인정보의 제공 동의 등

① 개인정보의 제공 동의

정보통신서비스 제공자가 이용자의 개인정보를 제3자에게 제공하려면 정보통신서비스 제공에 따른 요금정산을 위해 필요한 경우나 법률에 특별한 규정이 있는 경우를 제외하고는 ㉠ 개인정보를 제공받는 자, ㉡ 개인정보를 제공받는 자의 개인정보 이용 목적, ㉢ 제공하는 개인정보의 항목, ㉣ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 등을 모두 이용자에게 미리 고지하고 동의를 받아야 하며, 고지한 사항이 변경되는 경우에도 마찬가지이다(제24조의2 제1항). 이에 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제3호).

② 제3자 제공 및 목적 외 이용의 금지

정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다(제24조의2 제2항). 이에 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제3호).

③ 개인정보의 취급위탁

정보통신서비스 제공자등이 제3자에게 이용자의 개인정보를 취급할 수 있도록 업무를 위탁하는 경우에는 ㉠ 개인정보 취급위탁을 받는 자, ㉡ 개인정보 취급위탁을 하는 업무의 내용을 이용자에게 알리고 동의를 받아야 한다(제25조 제1항). 다만 정보통신서비스 제공자등은 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 경우로서 전 사항 모두를 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 취급위탁에 따른 고지절차와 동의절차를 거치지 아니할 수 있다(제25조 제2항). 이에 위반할 경우 2천만원 이하의 과태료를 부과한다(제76조 제2항 제1호).

④ 영업의 양수 등에 따른 개인정보의 이전

정보통신 서비스 제공자등이 영업의 전부 또는 일부의 양도·합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 ㉠ 개인정보를 이전하려는 사실, ㉡ 개인정보를 이전받는 자의 성명·주소·전화번호 및 그 밖의 연락처, ㉢ 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법과 절차 등을 인터넷 홈페이지 게시, 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 고지하여야 한다(제26조 제1항). 이에 위반할 경우 2천만원 이하의 과태료를 부과한다(제76조 제2항 제2호).

영업양수자등은 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제공할 수 있는 당초 목적의 범위에서만 개인정보를 이용하거나 제공할 수 있다. 다만, 이용자로부터 별도의 동의를 받은 경우에는 그러하지 아니하다(제26조 제3항). 이에 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제3호).

5) 개인정보관리책임자의 지정 및 개인정보취급방침의 공개

정보통신서비스제공자와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자를 지정하여야 한다(제27조 제1항 본문). 다만, 종업원 수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있으며(제27조 제1항 단서), 이에 따라 개인정보 관리책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보 관리책임자가 된다(제27조 제2항). 또한 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다(제27조의2).

6) 개인정보의 안전한 관리의무

정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 ① 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행, ② 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영, ③ 접속기록의 위조·변조 방지를 위한 조치, ④ 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치, ⑤ 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치, ⑥ 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치 등의 기술적·관리적 조치를 취하여야 한다(제28조 제1항). 만일 ②~⑤의 조치를 취하지 않아 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 자에 대해서는 2년 이하의 징역 또는 1천만원 이하의 벌금에 부과할 수 있으며(제73조 제1호), ①과 ⑥의 조치를 취하지 않을 경우 3천만원 이

하의 과태료를 부과할 수 있다(제76조 제1항 제3호). 아울러 정보통신 서비스 제공자들은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다(제28조 제2항).

그리고 이용자의 개인정보를 취급하고 있거나 취급하였던 자는 직 무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 안 되며, 누구든지 그 개인정보가 누설된 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받아서는 안 된다(제28조의2). 만일 이에 위반 할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제5호 및 제6호).

7) 개인정보의 즉시파기의무

정보통신서비스제공자들은 개인정보의 수집·이용 목적을 달성하거나, 개인정보의 보유 및 이용 기간이 끝나거나 혹은 사업을 폐업하는 경우에는 당해 개인정보를 지체없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다(제29조). 만일 이에 위반하여 파기하지 않을 경우 3천만원 이하의 과태료에 처해진다(제76조 제1항 제4호).

8) 국외이전 개인정보의 보호

정보통신서비스제공자들은 이용자의 개인정보에 관하여 이 법의 규정을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 안 되며(제63조 제1항), 정보통신서비스제공자들은 이용자의 개인정보를 국외로 이전하고자 하는 때에는 이용자의 동의를 얻어야 한다(제63조 제2항).

이용자의 동의를 얻고자 하는 경우에는 미리 ① 이전되는 개인정보 항목, ② 개인정보가 이전되는 국가·이전일시 및 이전방법, ③ 개인정보를 이전받는 자의 성명, ④ 개인정보를 이전받는 자의 개인정보 이용 목적 및 보유·이용 기간 등을 이용자에게 고지하여야 한다(제

63조 제3항). 정보통신서비스제공자등은 제2항의 규정에 의한 동의를 얻어 개인정보를 국외로 이전하는 경우 대통령령이 정하는 바에 따라 보호조치를 취하여야 한다(제63조 제4항).

하지만 국외이전에 대한 동의를 얻지 않거나 소정의 고지를 하지 않고 개인정보를 국외로 이전한다고 하더라도 그에 대한 과태료나 벌칙 등의 제제조항이 없기 때문에 이 조항의 실효성에 대해서는 의문이 제기될 수 있다.

(3) 이용자의 권리

1) 동의권 및 동의철회권

이용자는 정보통신서비스제공자등에 대하여 언제든지 개인정보 제공의 동의를 철회 할 수 있다(제30조 제1항). 정보통신서비스제공자등은 이용자가 제1항의 규정에 의하여 동의를 철회한 경우 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하여야 한다(제30조 제3항). 이에 위반하면 3천만원 이하의 과태료를 부과한다(제76조 제1항 제5호).

2) 열람 및 정정요구권

이용자는 정보통신서비스제공자등에 대하여 본인에 관한 일정한 사항(① 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보, ② 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황, ③ 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황)에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다(제30조 제2항). 정보통신서비스 제공자등은 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다(제30조 제4항). 이에 위반하면 3천만원 이하의 과태료를 부과한다(제76조 제1항 제5호).

정보통신서비스 제공자등은 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그 개인정보를 제공하거나 이용할 수 있다(제30조 제5항). 이에 위반하여 필요한 조치를 하지 아니하고 개인정보를 제공하거나 이용한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다(제71조 제7호).

3) 개인정보침해에 대한 손해배상청구권

이용자는 정보통신서비스제공자등이 이 장의 규정을 위반한 행위로 손해를 입은 경우 그 정보통신서비스제공자등에 대하여 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다(제32조).

(4) 개인정보보호기구

1) 행정안전부 또는 방송통신위원회

과거 개인정보침해에 대한 관리감독은 일차적으로 정보통신부가 담당하였다. 그러나 최근 정부조직법의 개정으로 정보통신부가 해체되고 방송통신위원회가 출범함에 따라 동법의 집행기관에 변화가 발생하였다.

최근 개정된 정보통신망법에 의하면 행정안전부장관 또는 방송통신위원회가 이 법의 위반사항에 대한 조사권과 시정명령권을 갖게 되었다(제64조). 2008년 7월 현재 행정안전부에는 정보화전략실 정보기반정책관 산하에 개인정보보호과를 두고 있으며,²⁸⁰⁾ 방송통신위원회에는

280) 행정안전부 홈페이지 <<http://www.mopas.go.kr>> ‘행정안전부소개’ 참조.

이용자네트워크국 네트워크정책관 산하에 개인정보보호과를 두고 있다.²⁸¹⁾ 따라서 현행법상 정보통신망의 이용에 따른 개인정보의 보호를 감독해야 할 기관은 행정안전부와 방송통신위원회라고 해야 할 것이다.

현행 정보통신망법에 의하면, 행정안전부장관 또는 방송통신위원회는 ① 이 법에 위반되는 사항을 발견하거나 혐의가 있음을 알게 된 경우, ② 이 법의 위반에 대한 신고를 받거나 민원이 접수된 경우, ③ 그 밖에 이용자 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우에는 정보통신서비스 제공자등에게 관계 물품·서류 등을 제출하게 할 수 있으며(제64조 제1항), 정보통신서비스 제공자등이 관계 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원에게 정보통신서비스 제공자등의 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하도록 할 수 있다(제64조 제3항). 그리고 행정안전부장관 또는 방송통신위원회는 이 법을 위반한 정보통신서비스 제공자등에게 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있고, 시정조치의 명령을 받은 정보통신서비스 제공자등에게 시정조치의 명령을 받은 사실을 공표하도록 할 수 있다(제64조 제4항). 이에 따라 필요한 시정조치를 명한 경우에는 시정조치를 명한 사실을 공개할 수 있다(제64조 제5항).

한편 이 법의 개인정보취급에 관한 규정에 위반하여 개인정보를 수집·이용 또는 제3자에게 제공하거나 개인정보 취급위탁을 한 경우, 안전관리조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우 등에는 방송통신위원회로 하여금 해당 전기통신사업자에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있도록 하고 있다(제64조의3 제1항).

281) 방송통신위원회 홈페이지 <<http://www.kcc.go.kr>> ‘위원회소개’ 참조.

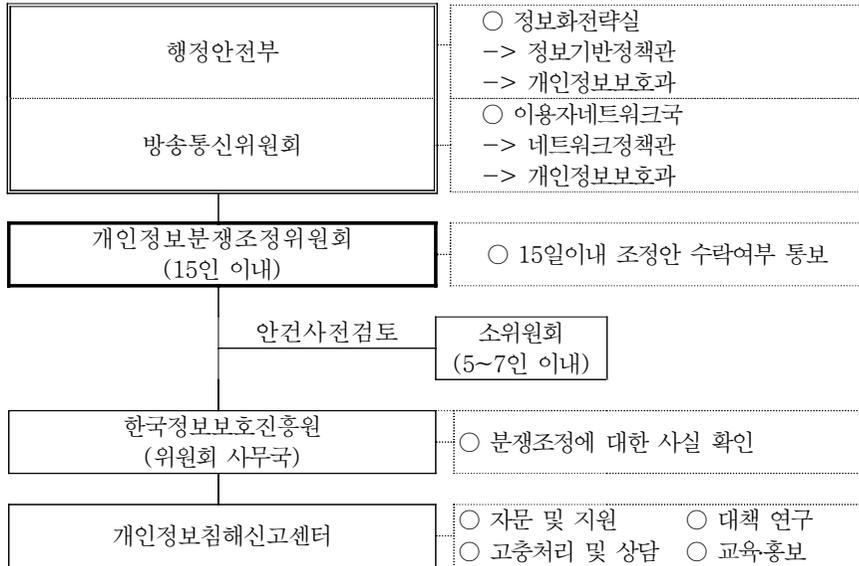
2) 개인정보분쟁조정위원회

이와는 별도로 개인정보침해에 관한 분쟁을 신속·간편·공정하게 조정하기 위하여 개인정보분쟁조정위원회를 두고 있는데, 동 위원회에서는 분쟁조정을 통해 피해를 구제한다(제33조). 동 위원회는 이 법이 정하는 개인정보와 관련된 분쟁이면 온라인, 오프라인을 불문하고 모두 위원회의 조정대상이 된다. 또한 동 위원회는 순수하게 민간영역에서 영리목적으로 서비스를 제공하는 사업자에 의한 개인정보침해 관련 분쟁이 주된 조정대상이며, 국가, 정부단체, 지방자치단체, 학교 등에서 수집·관리하고 있는 개인정보는 위원회의 조정 범위에 포함되지 않는다.

분쟁조정위원회의 구성은 위원장 1인을 포함한 15인 이내의 위원으로 구성되는데, 상임위원은 1인뿐이다. 위원과 위원장은 특정 자격이 있는 자 중에서 행정안전부장관이 임명하고, 임기는 3년으로 연임이 가능하다. 위원의 신분은 자격정지 이상의 형을 선고받거나 심신상의 장애로 업무를 수행할 수 없는 경우가 아니면 그 의사에 반해 면직 또는 해촉되지 아니한다. 한국정보보호진흥원이 동 위원회의 사무국 기능을 하고, 개인정보침해신고센터에서 개인정보침해에 대한 자문과 교육을 실시한다.

분쟁조정위원회는 양 당사자에게 조정안을 제시하는데, 만약 쌍방이 조정안을 받아들이면 분쟁조정을 통한 합의는 민사상 화해계약과 같은 효력을 지닌다. 그러나 조정이 성립되지 않으면, 피해자는 민사소송으로 피해의 구제를 다룰 수 있다. 따라서 분쟁조정위원회의 조정은 어떠한 강제력이나 집행력도 갖지 못하고 실효성을 담보하기 어렵다는 문제가 있다.

[그림 2-2-2] 정보통신망법의 집행체계



제 4 절 『신용정보의 이용 및 보호에 관한 법률』

1. 연 혁

(1) 제 정(1995)

『신용정보의 이용 및 보호에 관한 법률』은 신용조사업무제도의 개선이 행정쇄신과제로 대두됨에 따라 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 기하는 한편, 신용정보의 오남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서를 확립하기 위하여 신용조사법을 폐지하면서 1995년 1월 5일에 제정되었다. 개인정보의 보호와 관련된 법의 주요내용은 다음과 같다.

- ① 신용정보라 함은 금융거래등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보를 말하며 그 구체적인 내용 및 범위는 대통령령으로 정하도록 하였다.
- ② 신용정보업자는 재무부장관의 허가를 받도록 하고 신용정보업자의 업무는 타인의 의뢰를 받아서 신용정보를 조사하고 이를 제공하는 업무, 신용정보를 모집·정리·처리하고 의뢰인의 조회에 따라 제공하는 업무 및 채권추심업무 등으로 정하였다.
- ③ 국가의 안보 및 기밀에 관한 정보, 기업의 경영비밀, 개인의 정치적 사상이나 종교적 신념 기타 신용정보와 무관한 사생활에 관한 정보 등의 모집 및 조사를 제한하였다.
- ④ 재무부장관은 금융기관 등이 보유하고 있는 신용정보를 집중관리·활용하게 하기 위하여 신용정보집중기관을 지정하거나 신용정보집중기관으로 등록하게 하도록 하였다.
- ⑤ 금융기관·백화점·할부판매회사 등 신용정보제공·이용자가 비밀보장의 대상이 되는 금융거래정보·개인질병정보 등을 신용정보사업자들에게 제공하고자 하는 경우에는 당사자인 개인으로부터 사전에 서면에 의한 동의를 얻도록 하였다.
- ⑥ 신용정보주체는 신용정보사업자 등에게 본인의 신용정보에 대한 열람을 청구할 수 있으며 본인의 신용정보가 사실과 다른 경우에는 정정을 청구할 수 있도록 하였다.

(2) 2001년 개정

이후 법은 개인정보의 불법유출행위를 방지하기 위하여 개인의 성명·주소·주민등록번호 등 개인식별 정보의 제공시 해당 개인의 서면동의를 받도록 하는 한편, 신용정보업자등이 개인에게 신용불량자 등록 등 불리한 조치를 취할 때에는 미리 해당 개인에게 통보하도록

하는 내용을 포함하여 2001년 12월 31일에 개정되었다.

(3) 2004년 개정

최근 2004년 1월 29일에 신용정보 수집·조사업무의 효율성을 높이기 위하여 신용정보업자 또는 신용정보 집중기관이 공공기관에 대하여 신용정보의 열람 또는 제공을 요청한 경우 공공기관이 이에 응하도록 하고, 신용정보의 오용·남용을 막고 정보보호를 강화하기 위하여 신용정보주체에게 신용정보업자 등으로부터 신용정보의 제공사실을 통보받을 수 있는 권리를 부여하는 내용의 개정을 단행했다. 개정의 주요 내용은 다음과 같다.

- ① 신용정보제공·이용자가 성명·주소 등 개인을 식별할 수 있는 정보를 신용정보업자 등에게 제공하고자 하는 경우에는 전화 또는 인터넷 홈페이지의 동의란에 행하는 표시에 의하여 본인의 동의를 얻을 수 있도록 하였다(법 제23조제2항 신설).
- ② 신용정보주체는 신용정보업자 등에 대하여 본인에 관한 신용정보를 제공받은 자, 그 이용목적, 제공일자, 제공한 본인정보의 주요내용 등을 통보하도록 요구할 수 있도록 하였다(법 제24조의2 신설).

(4) 2007년 개정

2007년 12월 21일 개정된 법률에서는 정보활용동의서를 받는 방법에 정보제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식을 추가하였다(제23조 제1항). 이는 이용자의 편의 증진과 더불어, 정보통신 산업의 발전과 국제경쟁력을 강화하기 위한 것이었다.

2. 현행법의 주요 내용

(1) 적용 범위

1) 적용대상: 신용정보업자 등

이 법의 적용대상인 신용정보업자등에는 신용정보업자와 신용정보 집중기관, 신용정보제공자, 이용자가 있다. 신용정보업은 신용조회업무, 신용조사업무, 채권추심업무, 신용평가업무 및 그에 부수하는 업무의 전부 또는 일부를 업으로 영위하는 것을 말하는 것으로, 신용정보업자는 신용정보업을 영위할 목적으로 금융감독위원회의 허가를 받은 자를 말한다.

신용정보 집중기관은 신용정보를 집중하여 관리·활용하는 자로서 등록된 자를 말하고, 신용정보제공자와 이용자는 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻어지거나 만들어낸 신용정보를 신용정보업자 또는 신용정보 집중기관에게 제공하거나 신용정보업자 또는 신용정보 집중기관으로부터 신용정보를 지속적으로 제공받아 본인의 영업에 이용하는 자를 말한다.

2) 보호대상: 신용정보

동법에 의해 보호대상이 되는 신용정보는 금융거래 등 상거래에 있어서 거래상대방에 대한 식별, 신용도, 신용거래 능력 등의 판단을 위하여 필요로 하는 정보로서 대통령령이 정하는 정보를 말한다. 이에 따라 ① 개인의 성명·주소주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호)성별국적 및 직업등과 기업 및 법인의 상호, 법인등록번호, 사업자등록번호, 본점 및 영업소의 소재지설립연월일·목적 및 임원에 관한 사항 등 특정 신용정보주체를 식별할 수 있는 정보, ② 금융거래 등 상거래와 관련하여 신용정보주체의 거래내용을 판단

할 수 있는 정보, ③ 신용정보주체의 신용도를 판단할 수 있는 정보, ④ 신용정보주체의 신용거래능력을 판단할 수 있는 정보, ⑤ 금융거래등 상거래에 있어서 신용정보주체의 식별, 신용도, 신용거래능력을 판단할 수 있는 법원의 심판 등에 관한 정보 및 기타 공공기관이 보유한 정보가 법이 보호하고자 하는 대상 정보에 해당한다.

(2) 신용정보업자 등의 의무

1) 신용정보의 모집, 조사의 원칙

신용정보업자등(신용정보업자, 신용정보 집중기관, 신용정보제공, 이용자)은 신용정보를 모집, 조사함에 있어서 이법 또는 정관에서 정한 업무범위 안에서 모집, 조사의 목적을 명확히 하고 그 목적의 달성에 필요한 범위 안에서 합리적이고 공정한 수단에 의하여 한다(제13조).

2) 정보모집과 조사의 제한

신용정보업자 등은 ① 국가의 안보 및 기밀에 관한정보, ② 기업의 경영비밀 또는 독창적인 연구개발정보, ③ 개인의 정치적 사상, 종교적 신념 기타 신용정보와 무관한 사생활에 관한 정보, ④ 불확실한 개인신용정보, ⑤ 다른 법률에 의하여 모집이 금지된 정보, ⑥ 기타 대통령령이 정하는 정보에 대한 정보수집을 할 수 없다(제15조).

만약 신용정보업자 등이 이 규정을 위반하여 해당 정보를 수집한 경우 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 되어 있다(제32조 제2항 제4호).

3) 신용정보의 정확성 및 최신성의 유지

신용정보업자등은 신용정보의 정확성과 최신성이 유지될 수 있도록 신용정보를 적절히 관리하여야 하며, 신용정보주체에 대한 불이익을 초래할 수 있는 오래된 신용정보는 대통령령이 정하는 바에 의하여

기록을 삭제하여야 한다(제18조).

4) 신용정보전산시스템의 안전보호

신용정보업자들은 신용정보전산시스템(공동전산망을 포함)에 대한 제3자의 불법접근 또는 입력된 정보의 변경·훼손·파괴 기타 위험에 대한 기술적·물리적 보안대책을 수립하여야 한다(제19조).

5) 신용정보관리책임의 명확화 및 업무처리기록의 보존

신용정보업자들은 신용정보의 수집·처리 및 이용등에 대하여 금융위원회가 정하는 바에 의하여 내부관리규정을 마련하여야 한다(제20조 제1항). 의뢰인의 주소·성명 또는 정보제공·교환기관의 주소·기관명, 의뢰받은 업무내용 및 의뢰받은 일자, 의뢰받은 업무에 대한 처리내용 또는 제공한 신용정보의 내용 및 일자 등의 사항에 대한 기록을 3년간 보존하여야 한다(제20조 제2항). 기록보존의무를 준수하지 않을 경우 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(제32조 제3항 제4호).

6) 폐업시 보유정보의 처리

신용정보업자 및 신용정보집중기관이 폐업하고자 하는 경우에는 보유정보를 금융위원회가 정하는 바에 의하여 처분·소거 또는 폐기하여야 한다(제21조). 이에 위반할 경우 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(제32조 제3항 제5호).

7) 신용정보활용체제의 공시

신용정보업자와 신용정보 집중기관은 관리정보의 종류, 이용목적, 제공대상 및 신용정보주체의 권리 등에 대하여 대통령령이 정하는 바에 의하여 공시하여야 한다(제22조). 이를 위반한 경우 300만원 이하의 과태료에 처해지게 된다(제35제 제3항 제5호).

8) 개인신용정보의 제공, 활용에 대한 동의

신용정보제공·이용자는 ① 「금융실명거래 및 비밀보장에 관한 법률」 제4조의 규정에 의한 금융거래의 내용에 관한 정보 또는 자료, ② 개인의 질병에 관한 정보, ③ 개인의 성명, 주소, 주민등록번호, 성별, 국적 및 직업 등 개인을 식별할 수 있는 정보, ④ 기타 대통령령이 정하는 개인신용정보 등의 개인에 관한 신용정보를 신용정보업자 등에게 제공하고자 하는 경우에는 대통령령으로 정하는 바에 따라 해당 개인으로부터 서면, 공인전자서명이 있는 전자문서 또는 그 밖에 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식 등 대통령령으로 정하는 방식에 의한 동의를 얻어야 한다(제23조 제1항). 하지만 신용정보제공·이용자가 개인신용정보중 개인의 성명, 주소, 주민등록번호, 성별, 국적 및 직업 등 개인을 식별할 수 있는 정보를 제공하고자 하는 경우에는 전화에 의한 본인의 동의나 인터넷 홈페이지의 동의란에 본인이 행하는 동의표시에 의하여 신용정보업자등에게 제공할 수 있다(제23조 제2항). 동의 없이 해당 정보를 수집한 신용정보제공자와 이용자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하도록 되어 있다(제32조 제2항 제6호).

9) 개인신용정보의 제공, 이용의 제한 및 통보

개인신용정보는 당해 신용정보주체와의 금융거래등 상거래관계(고용관계를 제외)의 설정 및 유지여부 등의 판단목적으로만 제공·이용되어야 한다. 다만, ① 개인이 서면 또는 공인전자서명이 있는 전자문서에 의하여 금융거래등 상거래관계의 설정 및 유지여부 등의 판단목적 외의 다른 목적에의 제공·이용에 동의하거나 개인이 자신의 신용정보를 제공하는 경우, ② 법원의 제출명령 또는 법관이 발부한 영장

에 의하여 제공·이용되는 경우, ②-② 범죄로 인하여 피해자의 생명이나 신체에 심각한 위해가 예상되는 등 긴박한 상황에 있고 제2호의 규정에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공·이용되는 경우, ③ 신용정보업자 및 신용정보집중기관 상호간에 집중관리·활용하기 위하여 제공·이용되는 경우, ④ 조세에 관한 법률의 규정에 의한 질문·조사를 위하여 관할관서의 장이 서면으로 요구하거나 조세에 관한 법률의 규정에 의하여 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공·이용되는 경우, ⑤ 기타 다른 법률의 규정에 의하여 제공·이용되는 경우, ⑥ 채권추심, 인·허가의 목적 등 대통령령이 정하는 목적으로 사용하기 위하여 제공·이용되는 경우에는 그러하지 아니하다(제24조 제1항). 신용정보업자등은 개인신용정보를 제공할 경우에는 금융위원회가 정하는 바에 의하여 의뢰인의 신원 및 이용목적을 확인하여야 한다(제24조 제2항). 이를 어긴 사람은 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다(제32조 제2항 제7호).

(3) 정보주체의 권리

1) 신용정보 제공사실의 통보요구권

신용정보주체는 신용정보업자등이 본인에 관한 신용정보를 제공하는 때에는 대통령령이 정하는 바에 따라 제공받은 자, 그 이용목적, 제공일자, 제공한 본인정보의 주요내용 등을 통보하도록 요구할 수 있다(제24조의2).

2) 신용정보의 열람 및 정정청구 등

신용정보주체는 신용정보업자 등에게 본인의 신분임을 나타내는 증표를 제시하거나 대통령령이 정하는 객관적인 방법에 의하여 본인임을 확인받아 신용정보업자 등이 보유하고 있는 본인정보의 제공 또는

열람을 청구할 수 있으며, 본인정보가 사실과 다른 경우에는 금융위원회가 정하는 바에 의하여 정정을 청구할 수 있다(제25조). 정정청구 시 신용정보기관이 이에 대한 적절한 조치를 하지 않은 경우 300만원 이하의 과태료에 처해지게 된다.

3) 손해배상책임

신용정보업자등과 기타 신용정보의 이용자가 이 법의 규정을 위반하여 신용정보주체에게 피해를 입힌 경우 손해배상책임이 있다(제28조).

(4) 신용정보보호기구

1) 금융위원회

신용정보의 보호기구로서 법이 명시적으로 정한 것은 없다. 그러나 신용정보업의 감독기능을 수행하는 기구인 금융위원회가 이 법에서 규정하고 있는 신용정보보호와 관련된 업무를 수행하는 것으로 나타난다. 금융위원회는 신용정보업자등의 건전한 영업을 위하여 신용정보업자등의 업무를 감독하고 그 업무 또는 재산에 관한 보고 등 필요한 명령을 할 수 있다(제29조 제1항). 그리고 금융위원회는 금융감독원의 검사결과에 따라 신용정보업자등에게 당해 업무의 개선·중지 또는 신용정보의 제공중지 기타 필요한 조치를 명할 수 있다(제29조 제5항). 이에 따라 금융위원회가 개인의 신용정보의 침해를 예방하고 제재조치를 취할 수 있는 감독기관의 역할을 수행한다고 볼 수 있을 것이다.

2) 금융감독원

금융감독원장은 그 소속직원으로 하여금 신용정보업자등의 업무와 재산상황을 검사하게 할 수 있으며(제29조 제2항), 그 검사를 함에 있어서 필요하다고 인정하는 때에는 신용정보업자등에 대하여 자료의

제출, 관계자의 출석 및 의견의 진술을 요구할 수 있다(제29조 제3항). 따라서 금융감독원 또한 개인의 신용정보를 보호하기 위한 감독기구로서 기능한다고 볼 수 있을 것이다.

제 5 절 「위치정보의 보호 및 이용 등에 관한 법률」

1. 연 혁

(1) 2005년 제정법

이동통신기술이 급속하게 발달로 물류, 보안, 상거래 등에 위치정보를 이용하는 다양한 서비스가 등장하면서 개인위치정보가 유출, 남용되는 등 개인의 사생활이 침해될 우려가 날로 증폭되어 가고 있다. 이러한 상황에서 위치정보를 수집하는 사업이나 위치정보기반서비스를 제공하는 사업에 대하여 일정한 제약을 가하고, 위치정보의 수집·제공 등에 관한 절차를 정함으로써 위치정보의 유출로 인한 사생활 침해의 방지를 도모하는 한편, 위치정보와 관련된 기술개발, 표준화 등을 지원하기 위한 법률의 제정이 필요하다는 주장이 제기되었다.

이에 따라 2005년 1월 27일 위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하기 위하여 「위치정보의 보호 및 이용 등에 관한 법률」(일부개정 2008. 2.29 법률 제8867호)이 제정되었다. 개인정보의 보호와 관련된 법의 주요내용은 다음과 같다.

- ① 위치정보 수집 등의 금지 : 누구든지 개인 또는 물건의 소유자의 동의를 받지 아니하고 당해 개인 또는 물건의 위치정보를 수집·이용 또는 제공할 수 없도록 하고, 위반시 3년 이하의 징역 등에 처할 수 있도록 함(법 제15조 및 제41조)

- ② 개인위치정보의 파기 : 위치정보사업자 및 위치기반서비스사업자가 개인위치정보의 수집·이용 및 제공목적을 달성한 때에는 즉시 개인위치정보를 파기하도록 함(법 제23조)
- ③ 의사무능력자 등의 보호를 위한 위치정보 이용 : 8세 미만의 아동, 금치산자, 중증장애인 등으로 의사능력이 없는 자의 친권자, 후견인 및 부양의무자 등이 정신질환자 등의 생명 또는 신체의 보호를 위하여 개인위치정보 수집·이용 또는 제공에 동의하는 경우에는 당해 정신질환자 등의 동의가 있는 것으로 보도록 함으로써 이들의 보호를 위하여 위치정보를 이용할 수 있는 제도적 장치를 마련함(법 제26조)
- ④ 긴급구조를 위한 개인위치정보의 이용 : 공공구조기관은 개인위치정보주체, 그 배우자 또는 직계 존비속의 긴급구조요청이 있는 경우 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있으며, 위치정보사업자는 개인위치정보주체의 동의 없이 위치정보를 수집·제공하도록 함(법 제29조)

(2) 2006년 개정법

긴급구조를 위한 개인위치정보 이용을 요구할 수 있는 자는 개인위치정보주체, 개인위치정보주체의 배우자 또는 직계 존·비속으로만 규정되어 있어서 형제·자매가 긴급구조를 위한 개인위치정보를 이용하지 못하게 되어 있고, 친권자가 없는 미성년자의 경우 자살기도 등의 긴박한 경우에 그 위치추적을 요구할 수 있는 자가 없게 되었다. 이러한 문제를 해소하기 위하여 2006년 9월 27일에 개정된 동법(법률 제8002호)에서는 제29조 제1항을 개정하여 형제·자매도 위치추적을 요구할 수 있도록 개선하고, 친권자가 없는 미성년자의 경우 「민법」 제928조에 따른 후견인이 위치추적을 요청할 수 있도록 하였다.

(3) 2007년 개정법

동법은 2007년 4월 11일, 같은 해 5월 25일, 같은 해 12월 21일에 각각 부분적으로 개정되었다.

먼저 4월과 5월의 개정은 단순히 다른 법률이 개정된 데 따라 변경된 사항을 반영하기 위한 것이었다.

다음으로 12월의 개정 위치정보사업자 또는 위치기반서비스사업자에 대한 규제를 완화하려는 것이었다. 이에 따라 위치정보사업자가 상호 등 경미한 사항을 변경하려는 경우에는 변경허가에 갈음하여 변경신고를 하도록 하고, 위치정보사업자의 변경허가 대상범위를 구체적으로 한정하였다. 또한 위치정보사업을 하려는 자가 위치정보사업의 허가신청시 위치기반서비스사업 신고에 필요한 서류를 첨부하여 그 허가를 받는 경우에는 위치기반서비스사업의 신고를 한 것으로 보도록 하였다.

(4) 2008년 개정법

동법은 2008년 2월 29일에 최종적으로 개정되었는데, 이는 방송통신위원회의 설치 및 운영에 관한 법률의 개정에 따른 일부개정이었다.

하지만 긴급구조기관으로 하여금 태풍, 호우, 화재, 화생방사고 등 재난 또는 재해의 위험지역 안에 위치한 개인위치정보주체에게 생명 또는 신체의 위험을 경보하기 위하여 위치정보사업자에게 경보발송을 요청할 수 있도록 하고, 요청을 받은 위치정보사업자는 위험지역 안에 위치한 개인위치정보주체의 동의가 없음을 이유로 경보발송을 거부하지 못하도록 제29조 제5항에 대한 개정도 함께 이루어졌다.

2. 현행법상 개인정보보호 관련 내용

(1) 용어의 정의

동법상 “개인위치정보”라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다(제2조 제2호).

그리고 “개인위치정보주체”라 함은 개인위치정보에 의하여 식별되는 자를 말한다(제2조 제3호). “위치정보사업”이라 함은 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 것을 말하고(제2조 제6호), “위치기반서비스사업”이라 함은 위치정보를 이용한 서비스를 제공하는 것을 사업으로 영위하는 것을 말한다(제2조 제7호).

(2) 개인위치정보의 보호

1) 개인위치정보의 수집

위치정보사업자가 개인위치정보를 수집하고자 하는 경우에는 미리 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처 등 일정한 사항을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다(제18조 제1항). 개인위치정보주체는 제1항의 규정에 의한 동의를 하는 경우 개인위치정보의 수집의 범위 및 이용약관의 내용 중 일부에 대하여 동의를 유보할 수 있다(제18조 제2항). 위치정보사업자가 개인위치정보를 수집하는 경우에는 수집목적 달성하기 위하여 필요한 최소한의 정보를 수집하여야 한다(제18조 제3항).

2) 개인위치정보의 이용 또는 제공

위치기반서비스사업자가 개인위치정보를 이용하여 서비스를 제공하고자 하는 경우에는 미리 위치기반서비스사업자의 상호, 주소, 전화번호 그 밖의 연락처 등 일정한 사항을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다(제19조 제1항). 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 서비스를 하고자 하는 경우에는 제1항 각호의 내용을 이용약관에 명시한 후 제공받는 자 및 제공목적은 개인위치정보주체에게 고지하고 동의를 얻어야 한다(제19조 제2항).

3) 위치정보사업자의 개인위치정보 제공 등

개인위치정보주체의 동의를 얻은 위치기반서비스사업자는 이용 또는 제공목적은 달성하기 위하여 해당 개인위치정보를 수집한 위치정보사업자에게 해당 개인위치정보의 제공을 요청할 수 있으나, 이 경우 위치정보사업자는 정당한 사유없이 제공을 거절하여서는 아니된다(제20조 제1항).

4) 개인위치정보 등의 이용·제공의 제한 등

위치정보사업자등은 ① 개인위치정보주체의 동의가 있는 경우, ② 위치정보 및 위치기반서비스 등의 제공에 따른 요금정산을 위하여 위치정보 수집·이용·제공사실 확인자료가 필요한 경우, ③ 통계작성, 학술연구 또는 시장조사를 위하여 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우를 제외하고는 개인위치정보 또는 위치정보 수집·이용·제공사실 확인자료를 제18조제1항 및 제19조제1항·제2항에 의하여 이용약관에 명시 또는 고지한 범위를 넘어 이용하거나 제3자에게 제공하여서는 아니된다(제21조).

5) 사업의 양도 등의 통지

위치정보사업자등으로부터 사업의 전부 또는 일부의 양도·합병 또는 상속 등(이하 “양도등”이라 한다)으로 그 권리와 의무를 이전받은 자는 30일 이내에 다음 각호의 사항을 대통령령이 정하는 바에 의하여 개인위치정보주체에게 통지하여야 한다(제22조).

1. 사업의 전부 또는 일부의 양도 등의 사실
2. 위치정보사업자등의 권리와 의무를 승계한 자의 성명, 주소, 전화번호 그 밖의 연락처
3. 그 밖에 개인위치정보 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항

6) 개인위치정보의 파기 등

위치정보사업자등은 개인위치정보의 수집, 이용 또는 제공목적을 달성한 때에는 제16조제2항의 규정에 의하여 기록·보존하여야 하는 위치정보 수집·이용·제공사실 확인자료 외의 개인위치정보는 즉시 파기하여야 한다(제23조).

(3) 개인위치정보주체 등의 권리

1) 개인위치정보주체의 권리 등

개인위치정보주체는 위치정보사업자등에 대하여 언제든지 동의의 전부 또는 일부를 철회할 수 있다(제24조 제1항). 또한 위치정보사업자등에 대하여 언제든지 개인위치정보의 수집, 이용 또는 제공의 일시적인 중지를 요구할 수 있다. 이 경우 위치정보사업자등은 요구를 거절하여서는 아니 되며, 이를 위한 기술적 수단을 갖추어야 한다(제24조 제2항). 그리고 위치정보사업자등에 대하여 본인에 대한 위치정보 수집·이용·제공사실 확인자료, 본인의 개인위치정보가 이 법 또

는 다른 법률의 규정에 의하여 제3자에게 제공된 이유 및 내용 등의 열람 또는 고지를 요구할 수 있고, 당해 자료 등에 오류가 있는 경우에는 그 정정을 요구할 수 있다. 이 경우 위치정보사업자들은 정당한 사유없이 요구를 거절하여서는 아니 된다(제24조 제3항). 위치정보사업자들은 개인위치정보주체가 동의의 전부 또는 일부를 철회한 경우에는 지체없이 수집된 개인위치정보 및 위치정보 수집·이용·제공사실 확인자료(동의를 일부를 철회하는 경우에는 철회하는 부분의 개인위치정보 및 위치정보 이용·제공사실 확인자료에 한한다)를 파기하여야 한다(제24조 제4항).

2) 법정대리인의 권리

위치정보사업자들이 14세 미만의 아동으로부터 개인위치정보를 수집·이용 또는 제공하고자 하는 경우에는 그 법정대리인의 동의를 얻어야 한다(제25조 제1항). 다만 8세 이하의 아동, 금치산자, 정신적 장애를 가진 자로서 중증장애인에 해당하는 자의 경우 그 보호의무자가 8세 이하의 아동 등의 생명 또는 신체의 보호를 위하여 8세 이하의 아동 등의 개인위치정보의 수집·이용 또는 제공에 동의하는 경우에는 본인의 동의가 있는 것으로 본다(제26조 제1항).

3) 손해배상

개인위치정보주체는 위치정보사업자들의 제15조 내지 제26조의 규정을 위반한 행위로 손해를 입은 경우에 그 위치정보사업자들에 대하여 손해배상을 청구할 수 있다. 이 경우 그 위치정보사업자들은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다(제27조).

4) 분쟁의 조정 등

위치정보사업자 또는 위치기반서비스사업자는 위치정보와 관련된 분쟁에 대하여 당사자간 협의가 이루어지지 아니하거나 협의를 할 수

없는 경우에는 방송통신위원회에 재정을 신청할 수 있다(제28조 제1항). 위치정보사업자등과 이용자는 위치정보와 관련된 분쟁에 대하여 당사자간 협의가 이루어지지 아니하거나 협의를 할 수 없는 경우에는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제33조의 규정에 의한 개인정보분쟁조정위원회에 조정을 신청할 수 있다(제28조 제2항).

(4) 긴급구조를 위한 개인위치정보 이용

1) 긴급구조를 위한 개인위치정보의 이용

「재난 및 안전관리 기본법」 제3조제7항의 규정에 따른 긴급구조기관은 급박한 위험으로부터 생명·신체를 보호하기 위하여 개인위치정보주체, 개인위치정보주체의 배우자, 2촌 이내의 친족 또는 후견인의 긴급구조요청이 있는 경우 긴급구조 상황 여부를 판단하여 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있다. 이 경우 배우자등은 긴급구조 외의 목적으로 긴급구조요청을 하여서는 아니 된다(제29조 제1항). 이 경우 개인위치정보주체 또는 배우자등의 긴급구조요청은 공공질서의 유지와 공익증진을 위하여 부여된 대통령령이 정하는 특수번호 전화서비스를 통한 호출에 한한다(제29조 제2항). 긴급구조의 요청을 받은 위치정보사업자는 그 개인위치정보주체의 동의없이 개인위치정보를 수집할 수 있으며, 개인위치정보주체의 동의가 없음을 이유로 긴급구조기관의 요청을 거부하여서는 아니 된다(제29조 제3항). 위치정보사업자는 개인위치정보를 긴급구조기관에게 제공하는 경우 개인위치정보의 제공사실을 당해 개인위치정보주체에게 즉시 통보하여야 한다(제29조 제4항).

긴급구조기관은 태풍, 호우, 화재, 화생방사고 등 재난 또는 재해의 위험지역 안에 위치한 개인위치정보주체에게 생명 또는 신체의 위험을 경보하기 위하여 대통령령이 정하는 바에 의하여 위치정보사업자

에게 정보발송을 요청할 수 있으며, 요청을 받은 위치정보사업자는 위험지역 안에 위치한 개인위치정보주체의 동의가 없음을 이유로 정보발송을 거부하여서는 아니 된다(제29조 제5항).

긴급구조기관과 긴급구조업무에 종사하거나 종사하였던 자는 긴급구조 목적으로 제공받은 개인위치정보를 긴급구조 외의 목적에 사용하여서는 아니된다(제29조 제6항).

2) 개인위치정보의 요청 및 방식

긴급구조기관은 위치정보사업자에게 개인위치정보를 요청할 경우 위치정보시스템을 통한 방식으로 요청하여야 하며, 위치정보사업자는 긴급구조기관으로부터 요청을 받아 개인위치정보를 제공하는 경우 위치정보시스템을 통한 방식으로 제공하여야 한다(제30조 제1항).

제6절 기타 개별법상의 개인정보보호 관련 규정

1. 공공부문의 개인정보보호 관련 조항

(1) 전자정부법

『전자정부법』²⁸²⁾(일부개정 2008.2.29 법률 제8852호)은 행정기관이 보유·관리하는 개인정보는 법령이 정하는 경우를 제외하고는 당사자의 의사에 반하여 사용되어서는 안 된다는 ‘개인정보보호의 원칙’을 규정하고 있다(법 제12조).

민원인으로부터 전자문서를 수신한 행정기관의 장은 그 수신사실을 인터넷 등에 게시하여 전자문서를 송신한 자가 확인할 수 있도록 하여야 하며(시행령 제6조 제2항), 인터넷 등에 수신사실을 게시하는 때에는 접수번호·수신일자·접수등록번호·제목·수신기관 및 담당공

282) 종래 『전자정부구현을위한행정업무등의전자화촉진에관한법률』에서 2007. 1. 3. 법률명칭을 『전자정부법』으로 변경하는 법률의 개정이 있었다(법률 제8171호).

무원의 연락처 등을 명시하되, 전자문서를 송신한 자의 개인정보가 침해되지 아니하도록 하여야 한다(시행령 제6조 제3항).

한편, 행정기관은 민원사항의 처리를 위하여 필요한 행정정보, 통계정보·문헌정보 등 행정업무의 수행에 참고가 되는 행정정보, 「공공기관의 개인정보보호에 관한 법률」 제10조 제2항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보 등을 공동이용하도록 하고 있다(법 제21조 제1항). 동법시행령은 행정기관이 정보파일을 구축하여 보유하거나 이미 통보한 사항을 변경하거나 정보파일을 폐지하고자 하는 경우에는 행정자치부장관 또는 관계 중앙행정기관의 장에게 정보파일의 명칭, 정보파일의 보유목적, 보유기관 및 주관부서, 정보파일의 구성항목, 행정정보의 수집방법 등을 통보하도록 하고 있다(시행령 제21조 제1항). 또한 행정기관의 장은 다른 기관으로부터 제공받은 행정정보에 관하여 이용목적외의 목적으로 이용하는 행위를 금지하고 있다(시행령 제24조 제1호).

행정기관은 행정정보를 서로 공동이용하기 위하여 정보통신망으로 다른 행정정보의 보유기관에 송신하고자 하는 경우에는 특별한 사유가 있는 경우를 제외하고는 개인정보의 보호를 위하여 국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 대통령령이 정하는 방법으로 송신하여야 한다(법 제21조 제3항).

행정자치부장관이 설치하는 행정정보공동이용센터는 「공공기관의 개인정보 보호에 관한 법률」 제7조의 규정에 의한 개인정보파일에 관한 공고내용의 데이터베이스화와 그 안내서비스 제공의 업무를 행한다(시행령 제29조 제2항 제2호).

(2) 국세기본법

「국세기본법」(일부개정 2008.2.29 법률 8860호)은 세무조사의 사전통지(제81조의7 제1항) 및 결과통지(제81조의9), 과세정보의 비밀유지(제81조

의10), 납세자의 정보요구권(제81조의11) 등에 관한 규정을 두고 있다.

먼저, 세무조사의 사전통지와 관련하여 범칙사건에 대한 조사 또는 사전통지의 경우 증거인멸 등으로 조사목적 달성을 수 없다고 인정되는 때를 제외하고, 세무공무원으로 하여금 국세에 관한 조사를 위하여 당해 장부·서류 기타 물건 등을 조사하는 경우에는 조사를 받을 납세자에게 조사개시 10일 전에 조사대상 세목 및 조사사유 등을 통지하도록 하고 있다(제81조의7 제1항).

다음으로, 세무조사의 결과통지와 관련하여 세무공무원이 범칙사건의 조사, 법인세의 결정 또는 경정을 위한 조사 등 대통령령이 정하는 부과처분을 위한 실지조사를 마친 때에는 그 조사결과를 서면으로 납세자에게 통지하도록 하고 있다(제81조의9).

한편, 납세자의 과세정보가 외부에 공개됨으로 인한 납세자의 경제활동에 미치는 피해와 납세자 개인의 공공연한 사생활의 비밀침해를 막기 위하여 다음과 같은 과세정보의 비밀유지에 관한 규정(제81조의10)을 신설하였다. 즉 납세자가 세법이 정한 납세의무를 이행하기 위하여 제출한 자료나 국세의 부과 또는 징수를 목적으로 업무상 취득한 자료 등 과세정보를 납세공무원이 타인에게 제공 또는 누설하거나 목적외의 용도로 사용하는 것은 원칙적으로 금지되며(제81조의10 제1항 본문), 만일 이에 위반하여 과세공무원이 과세정보의 제공을 요구받는 경우에는 이를 거부해야 한다(제81조의10 제3항). 그리고 제1항의 규정에 의하여 과세정보를 알게 된 자가 이를 타인에게 제공 또는 누설하거나 그 목적외의 용도로 사용하는 것도 금지된다(제81조의10 제4항).

마지막으로, 납세자의 권리를 실효적으로 보장하기 위하여 정보요구권을 인정하였다. 이에 따라 세무공무원에게는 납세자가 납세자의 권리의 행사에 필요한 정보를 요구하는 경우 이를 신속하게 제공할 의무가 부과되었다(제81조의11).

(3) 주민등록법

『주민등록법』(일부개정 2008.2.29 법률 8852호)은 시·군의 주민을 등록하게 함으로써 주민의 거주관계를 파악하고 상시로 인구의 동태를 명확히 하여 행정사무의 적정하고 간이한 처리를 도모할 목적으로 1962년에 제정되었다. 동법에서는 개인정보의 보호를 위하여 다음과 같은 규정을 두고 있다.

주민등록의 열람 또는 등·초본의 교부신청자를 원칙적으로 본인 또는 세대원에 제한하고(제29조 제2항), 전산조직 중 무인민원발급기를 이용하는 경우에는 신청자 본인의 주민등록표 등·초본의 교부에 제한하고 있다(제29조 제3항). 그리고 주민등록표에 기록된 주민등록사항에 관한 주민등록전산정보자료를 이용 또는 활용하려는 자는 관계 중앙행정기관의 장의 심사를 거쳐 행정안전부장관의 승인을 받아야 한다(제30조 제1항). 전산자료를 이용·활용하려는 자의 범위는 주민등록표의 열람 또는 등·초본의 교부를 신청할 수 있는 자로 하되, 전산자료의 형태로 제공하는 것이 적합한 경우에 한정한다(제30조 제2항). 전산자료의 제공범위는 주민등록표의 자료로 하되, 특별한 경우에도 주민등록표 등·초본의 자료에 한정한다(제30조 제3항). 행정안전부장관은 전산자료를 제공하는 경우에는 원칙적으로 주민등록전산정보자료 제공심의위원회의 심의를 거쳐야 하며, 자료의 이용·활용 목적을 고려하여 필요 최소한의 자료를 제공하여야 한다(제30조 제4항). 주민등록표에 기록된 주민등록사항에 관한 주민등록전산정보자료를 이용·활용하는 자는 본래의 목적 외의 용도로 이용·활용하여서는 아니 된다(제30조 제5항). 이를 위반한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(제37조 제6호).

또한 주민등록표 보유기관의 장은 주민등록표를 관리할 때에 주민등록표가 멸실, 도난, 유출 또는 손상되지 아니하도록 필요한 안전조

치를 하여야 한다(제31조 제1항). 그리고 주민등록표의 관리자는 이 법의 규정에 따른 보유 또는 이용목적 외의 목적을 위하여 주민등록표를 이용한 전산처리를 해서는 안 되며(제31조 제2항), 주민등록업무에 종사하거나 종사하였던 자 또는 그 밖의 자로서 직무상 주민등록사항을 알게 된 자는 다른 사람에게 누설해서는 안 된다(제31조 제3항). 이에 위반한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(제37조 제7호).

그리고 주민등록번호 부여방법으로 거짓의 주민등록번호를 만들어 자기 또는 다른 사람의 재물이나 재산상의 이익을 위하여 사용한 자, 거짓의 주민등록번호를 만드는 프로그램을 다른 사람에게 전달하거나 유포한 자, 거짓이나 그 밖의 부정한 방법으로 다른 사람의 주민등록표를 열람하거나 그 등본 또는 초본을 교부받은 자 등은 3년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(제37조 제1호, 제4호, 제5호).

(4) 통계법

『통계법』(일부개정 2007.7.23 법률 제8541호)은 통계취급상 초래될 수 있는 개인정보의 침해를 막기 위해 다음과 같은 규정을 두고 있다. 통계작성과정에서 알려진 사항으로서 개인의 비밀에 속하는 사항은 보호되어야 하고(제33조 제1항), 통계의 작성을 위하여 수집된 개인의 비밀에 속하는 자료는 통계작성 외의 목적으로 사용되어서는 아니 된다(제33조 제2항). 또한 통계작성사무종사자등이 직무상 알게 된 사항으로 개인 또는 법인이나 단체의 비밀에 속하는 사항을 누설하거나 권한 없이 타인에게 제공하지 못하도록 하고 있다(제34조).

나아가 동법에서는 개인정보보호 조항의 실효성을 높이기 위해 벌칙조항을 두고 있다. 즉, 통계의 작성을 목적으로 수집되거나 제공을 받은 개인이나 법인 또는 단체 등의 비밀에 속하는 사항을 그 목적 외의 용도로 사용하거나 이를 다른 자에게 제공하거나 속임수나 그

밖의 부정한 방법으로 열람하거나 제공받은 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하고 있다(제39조 제1호 및 제2호).

(5) 자동차관리법

『자동차관리법』(일부개정 2008.6.13 법률 제9109호)에 의하면, 전산정보처리조직에 의하여 처리된 자료를 이용하고자 하는 자는 관계중앙행정기관의 장의 심의를 거쳐 국토해양부장관의 승인을 얻어야 하며(법 제69조 제2항), 승인요청을 받은 국토해양부장관은 자동차관리업무의 효율적인 수행에 지장이 없고 자동차소유자등의 사생활의 비밀과 자유를 침해하지 아니한다고 인정되는 경우에 한하여 이를 승인할 수 있다(법 제69조 제3항).

전산자료 중 자동차소유자의 인적사항 등 개인정보가 포함된 자료를 이용하고자 하는 자는 자료이용의 목적 및 근거, 자료의 범위, 자료의 제공방식·보관기관 및 안전관리대책 등을 기재한 신청서를 관계중앙행정기관의 장에게 제출하여야 한다. 이 경우 신청할 수 있는 전산자료는 필요한 최소한의 범위에 한하여야 하며, 자동차등록원부를 그 공부의 형태대로 복제하거나 전산자료 자체의 제공을 신청할 수 없다(동법 시행령 제14조 제1항). 관계중앙행정기관의 장은 신청내용의 타당성·적합성 및 공익성, 개인의 사생활 침해여부, 자료의 목적외 사용방지 및 안전관리대책 등을 심사한 후 그 심사결과를 신청을 받은 날부터 30일 이내에 신청인에게 통보하여야 한다(동법 시행령 제14조 제2항).

(6) 특정금융거래 정보의 보고 및 이용 등에 관한 법률

『특정금융거래 정보의 보고 및 이용 등에 관한 법률』(일부개정 2008.2.29 법률 제8863호)은 자금세탁의 방지를 위한 업무를 수행함에 있어서 발생할 수 있는 개인정보의 침해를 막기 위하여 다음과 같은

규정을 두고 있다.

금융정보분석원 소속 공무원, 중계기관에 종사하는 자 또는 제7조의 규정에 의하여 제공된 특정금융거래정보와 관련된 특정형사사건의 수사등에 종사하는 자는 그 직무와 관련하여 알게 된 특정금융거래정보 및 제10조의 규정에 의하여 제공받은 정보 또는 자료를 다른 사람에게 제공 또는 누설하거나 그 목적 외의 다른 용도로 사용하여서는 아니되며, 누구든지 금융정보분석원 소속 공무원, 중계기관에 종사하는 자 또는 특정형사사건의 수사등에 종사하는 자에게 특정금융거래정보 및 제10조의 규정에 의하여 제공받은 정보 또는 자료를 제공할 것을 요구하거나 목적 외의 다른 용도로 사용할 것을 요구하여서는 아니된다(제9조 제1항). 만일 이에 위반하여 그 직무상 알게 된 제공받은 정보 또는 자료를 다른 사람에게 제공 또는 누설하거나 그 목적 외의 용도로 사용한 자 또는 특정금융거래정보 및 제공받은 정보 또는 자료를 제공할 것을 요구하거나 목적 외의 다른 용도로 사용할 것을 요구한 자는 5년 이하의 징역 또는 3천만원 이하의 벌금에 처해진다(법 제13조 제2호).

(7) 기타 공직자 직무 관련법

『공직자윤리법』(일부개정 2008.2.29 법률 제8872호)은 공직자윤리위원회 또는 등록기관의 장의 허가를 받지 아니하고 등록의무자의 재산에 관한 등록사항을 열람·복사하거나 이를 하게 하는 것을 금지하고(제10조 제3항), 누구라도 재산등록사항을 이 법에 정한 외의 목적으로 이용하지 못하도록 하고 있다(제13조 후단). 그리고 재산등록업무 종사자의 직무상 지득한 비밀을 누설하지 못하도록 하고(제14조), 금융거래의 내용에 관한 자료를 제공받은 자가 그 자료를 타인에게 제공 또는 누설하거나 그 목적외의 용도로 이를 이용하는 것도 금지하고 있다(제14조의3).

만일 공무원 또는 공직유관단체의 임·직원이 제10조 제3항에 위반하여 허가 없이 등록사항을 열람·복사하거나 이를 하게 한 때와 제14조의 규정에 위반하여 재산등록사항을 다른 사람에게 누설한 때에는 공직자윤리위원회는 해임 또는 징계의결을 요구할 수 있다(제22조 제3호 및 제7호).

또한 제10조 제3항의 규정에 위반하여 허가 없이 재산등록사항을 열람·복사하거나 이를 하게 한 때에는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하고(제27조), 제14조의 규정에 위반하여 재산등록업무에 종사하거나 하였던 자 또는 그 밖의 자로서 직무상 재산등록사항을 알게 된 자가 정당한 사유 없이 공개된 재산등록사항외의 재산등록사항을 누설한 때에는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하며(제28조 제1항), 제14조의3의 규정에 위반하여 금융거래의 내용에 관한 자료를 제공받은 자가 그 자료를 타인에게 제공 또는 누설하거나 그 목적외의 용도로 이를 이용한 때에는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 하고 있다(제28조 제2항).

그 밖에도 「국가공무원법」 제60조는 공무원에 대하여 재직중은 물론 퇴직후에도 직무상 알게 된 비밀을 엄수할 의무를 부과하고, 제78조 제1항 제1호에서 이 규정에 위반할 경우 징계할 수 있도록 하고 있다. 그리고 「지방공무원법」 제52조도 공무원에게 직무상 알게 된 비밀을 엄수할 의무를 부과하고, 제69조 제1항 제1호에서 이에 위반되는 행위를 할 경우 징계할 수 있도록 하고 있다.

그리고 「민원사무 처리에 관한 법률」(일부개정 2008.2.29 법률 제 8852호) 제26조는 행정기관의 장으로 하여금 민원사무의 처리와 관련하여 알게 된 민원사항의 내용과 민원인의 신상정보 등이 누설되어 민원인의 권익이 침해되지 아니하도록 노력하여야 한다고 규정하고 있다. 또한 「독점규제 및 공정거래에 관한 법률」(일부개정 2002.8.26 법률 제06705호) 제62조는 이 법에 의한 직무에 종사하거나 종사하였

던 위원, 공무원 또는 협의회에서 분쟁조정업무를 담당하거나 담당하였던 자는 그 직무상 알게 된 사업자의 비밀을 누설하거나 이 법의 시행을 위한 목적외에 이를 이용하지 못하도록 규정하고 있다. 이에 위반한 자에 대하여 2년 이하의 징역 또는 2백만원 이하의 벌금에 처할 수 있다(동법 제69조 제2항).

2. 민간분야의 개인정보보호 관련 조항

(1) 전기통신사업법

「전기통신사업법」(일부개정 2008.2.29 법률 제8867호)에 의하면, 기간통신사업자는 요금부과, 징수 등을 위하여 이용자의 인적사항에 관한 정보를 다른 전기통신사업자들에게 제공할 수 있다(제34조의4 제1항). 그리고 전기통신사업자가 자신의 역무제공이나 전기통신설비의 제공 또는 상호접속으로 인하여 취득한 개별 이용자에 관한 정보를 본인의 동의나 법률의 규정 없이 공개해서는 안 된다. 또한 기간통신사업자로부터 제공받은 타인의 정보는 제공받은 목적에 한하여 사용해야 하며, 다른 용도에 부당하게 사용하거나 제3자에게 제공해서는 안 된다(제34조의5). 만일 이에 위반하여 정보를 공개·사용하거나 제공한 자는 2년 이하의 징역 또는 1억원 이하의 벌금에 처해질 수 있다.

그리고 누구든지 전기통신사업자가 취급중에 있는 통신의 비밀을 침해하거나 누설해서는 안 된다(제54조 제1항). 이를 위반한 경우 3년 이하의 징역이나 1억 5천만원 이하의 벌금에 처한다(제70조). 또한 전기통신사업에 종사하는 자 또는 종사하였던 자가 그 재직중에 통신에 관하여 알게 된 타인의 비밀을 누설해서도 안 된다(제54조 제2항). 이를 위반한 자는 5년 이하의 징역이나 2억원 미만의 벌금에 처해질 수 있다.

(2) 국민건강보험법

『국민건강보험법』(일부개정 2008.3.28 법률 제9079호)에서는 “공단·심사평가원 및 대행청구단체에 종사하였던 자 또는 종사하고 있는 자는 그 업무상 알게 된 비밀을 누설하여서는 아니된다.”고 규정하고(제86조), 이를 위반한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하고 있다(제94조 제2항 제4호).

(3) 의료법

『의료법』(일부개정 2008.2.29 법률 8852호)에 의하면, 의료인은 본법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 그 의료·조산 또는 간호에 있어서 지득한 타인의 비밀을 누설하거나 발표하지 못한다(제19조). 만일 이에 위반할 경우 고소가 있으면 3년 이하의 징역 또는 1천만원 이하의 벌금에 처할 수 있다(제88조). 나아가 누구든지 정당한 사유 없이 전자처방전에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 안 된다(제18조 제3항). 이는 2002년 3월 30일 개정법에서 양질의 의료서비스에 대한 국민들의 요구가 높아짐에 따라 전자처방전의 발부 및 원격의료서비스의 제공을 허용하기 위하여 의사·치과의사 또는 한의사에게 전자처방전을 교부할 수 있도록 하고 진료기록을 전자문서로 작성·보관할 수 있도록 하면서, 개인정보의 침해를 방지하기 위하여 특별히 신설한 규정이다. 만일 이 규정에 위반하면 5년 이하의 징역이나 2천만원 이하의 벌금에 처해질 수 있다(제87조 제1항 제2호). 한편, 의료인 또는 의료기관 종사자가 이 법 또는 다른 법령에서 특히 규정된 경우를 제외하고는 환자에 관한 기록의 열람·사본교부 등 그 내용확인에 응하는 것을 금지하고 있다(제21조 제1항 본문). 만일 이에 위반한 경우 고소가 있으면 3년 이하의 징역 또는 1천만원 이하의 벌금에 처할 수 있다(제88조). 하지

만 의료인은 같은 환자의 진료에 필요하여 다른 의료기관에서 그 환자에 대한 기록, 임상소견서 및 치료경위서의 열람이나 사본 송부를 요청하거나 환자가 검사 기록, 방사선 필름 등의 사본 교부를 요구하면 이에 응하여야 하며(제21조 제2항), 응급환자를 다른 의료기관으로 이송할 때에는 환자 이송과 함께 초진기록을 보내야 한다(제21조 제3항). 만일 이에 위반한 의료인은 300만원 이하의 벌금에 처해질 수 있다(제90조).

한편 환자, 환자의 배우자, 환자의 직계존비속 또는 배우자의 직계존속(배우자, 직계존비속 및 배우자의 직계존속이 없는 경우에는 환자가 지정하는 대리인)이 환자에 관한 기록의 열람이나 사본 교부 등 그 내용 확인을 요구하는 경우에는 환자의 치료를 위하여 불가피한 경우가 아니면 확인할 수 있게 하여야 한다(제21조 제1항 단서). 만일 이에 위반한 경우 고소가 있으면 3년 이하의 징역 또는 1천만원 이하의 벌금에 처할 수 있다(제88조). 이는 환자의 알 권리를 보장하기 위하여 2000년 1월 12일 개정법(법률 제6157호)에서 추가된 것이다.

(4) 보건의료기본법

『보건의료기본법』(일부개정 2008.3.28 법률 제9034호)에 의하면, 모든 국민은 관계 법령이 정하는 바에 의하여 보건의료인 또는 보건의료기관에 대하여 자신의 보건의료와 관련한 기록 등의 열람이나 사본의 교부를 요청할 수 있다. 다만, 본인이 요청할 수 없는 경우에는 그 배우자·직계존비속 또는 배우자의 직계존속이, 그 배우자·직계존비속 및 배우자의 직계존속이 없거나 질병 기타 요청을 할 수 없는 부득이한 사유가 있는 경우에는 본인이 지정하는 대리인이 기록의 열람 등을 요청할 수 있다(제11조 제2항). 또한 모든 국민은 보건의료인으로부터 자신의 질병에 대한 치료방법, 의학적 연구대상 여부, 장기이식 여부 등에 관하여 충분한 설명을 들은 후 이에 관한 동

의 여부를 결정할 권리를 가진다(제12조). 그리고 모든 국민은 보건 의료와 관련하여 자신의 신체·건강 및 사생활의 비밀을 침해받지 아니한다(제13조).

(5) 응급의료에 관한 법률

『응급의료에 관한 법률』에서도 “응급구조사는 직무상 알게 된 비밀을 누설하거나 공개하는 것이 금지된다”고 규정하고(제40조), 이에 벌칙으로 3년 이하의 징역 또는 1천만원 이하의 벌금을 과할 수 있으나, 다만 이는 친고죄로 되어 있다(제60조 제2항).

(6) 의료기사 등에 관한 법률

『의료기사 등에 관한 법률』에 의하면 의료기사등은 이 법 또는 다른 법령에 특히 규정된 경우를 제외하고는 그 업무상 알게 된 비밀을 누설하여서는 아니 되고(제10조), 그 위반시 3년 이하의 징역 또는 1천만원 이하의 벌금에 처해질 수 있다(제30조).

(7) 전염병예방법

『전염병예방법』도 “보건의료기관·시설 또는 단체 등에서 건강진단 등 전염병 관련업무에 종사하는 자 또는 종사하였던 자는 업무상 알게 된 타인의 비밀을 누설하여서는 아니 된다”고 규정하고 있다(제54조의6). 이를 위반한자에 대해서는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하였다(제55조).

(8) 후천성면역결핍증 예방법

『후천성면역결핍증 예방법』(일부개정 2008.3.21 법률 제8940호)에서는 국가 또는 지방자치단체에서 후천성면역결핍증의 예방·관리와 감

염인의 보호·지원에 관한 사무에 종사하는 자, 감염인의 진단·검안·진료 및 간호에 참여한 자, 감염인에 관한 기록을 유지·관리하는 자가 이 법 또는 이 법에 따른 명령이나 다른 법령으로 정하고 있는 경우 또는 본인의 동의가 있는 경우를 제외하고는 재직 중에는 물론 퇴직 후에도 감염인에 대하여 업무상 알게 된 비밀을 누설하지 못하도록 하고 있다(제7조). 과거 ‘정당한 사유 없이’ 누설하는 것을 금지하였던 것을 최근 2008. 3. 21에 동법을 개정하면서 비밀누설을 훨씬 엄격하게 규제하고 있다. 만일 이에 위반하여 비밀을 누설할 경우 3년 이하의 징역 또는 1,000만원 이하의 벌금에 처해질 수 있다(제26조 제1호).

(9) 금융실명거래 및 비밀보장에 관한 법률

법 제4조는 금융기관에 종사하는 자는 명의자(위탁자 또는 수익자)의 서면상 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(거래정보)를 타인에게 제공하거나 누설하여서는 아니 되고, 누구든지 금융기관에 종사하는 자에게 거래정보 등의 제공을 요구해서는 안 된다. 이를 위반한 자는 5년 이하의 징역 또는 3천만원 이하의 벌금형을 병과할 수 있다(제6조)

(10) 증권거래법

『증권거래법』 제59조는 증권회사의 임원 및 직원은 증권회사를 통하여 유가증권을 매매하거나 매매하고자 하는 자의 서면에 의한 요구나 동의를 받지 아니하고는 타인에게 당해 위탁자의 유가증권의 매매기타의 거래와 그 예탁한 금전 또는 유가증권의 내용에 관한 정보를 제공하거나 누설해서는 안 된다(제1항). 또한 감독기관의 업무상 필요에 의하여 정보를 지득한 자는 그 지득한 정보를 타인에게 제공 또는 누설하거나 그 목적외에 사용해서는 안 된다(제2항)

그러나 법원의 제출명령 또는 법관이 발부한 영장이 있는 경우와 대통령령이 정하는 경우를 제외하고는 누구든지 증권회사의 임원 및 직원에 대하여 정보의 제공을 요구해서는 안 되고, 제공을 요구할 수 있는 때에도 그 질문 또는 조사의 내용은 필요한 범위에 국한해야 한다(제60조).

제59조와 제60조를 위반한 경우에는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처하도록 되어 있다(제208조)

(11) 공증인법

『공증인법』 제5조에 의하면 공증인은 촉탁인의 동의를 얻은 때와 법률에 특별한 규정이 있는 경우를 제외하고는 그 취급한 사건을 누설하지 못하도록 되어있다. 이를 위반한 경우 징계에 회부하도록 되어 있다(제82조)

(12) 법무사법

『법무사법』에 의하면 법무사 또는 법무사이었던 자는 위임인의 동의가 있거나 법률에 특별한 규정이 있는 경우를 제외하고는 정당한 이유 없이 업무상 알게 된 비밀을 누설해서는 안 된다(제27조). 이를 위반한 경우에는 법무사징계위원회에 징계의결을 요구하고 징계처분을 해야 한다(제18조)

(13) 변호사법

『변호사법』(일부개정 2008.3.28 법률 8991호) 제26조에 의하면, 변호사 또는 변호사이었던 자는 그 직무상 알게 된 비밀을 누설하여서는 아니 된다. 다만, 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다. 이를 위반했을 때는 징계사유가 된다(제91조 제2항).

제 3 장 현행 개인정보보호법제에 관한 개괄적 평가

제 1 절 세계적 보호입법모델에 비추어 본 우리 법제의 위상

1. 세계적인 보호입법모델의 개관

세계적으로 개인정보보호를 위한 입법모델은 크게 유럽모델과 미국 모델로 나누어진다.²⁸³⁾ 유럽모델은 “정부 주도의 일원적·포괄적 입법 모델”이며, 최근 세계 각국의 동향은 이 입법모델을 채택하고 있는 추세이다. 이에 비하여 미국모델은 “자율규제 중시의 이원적·부문별 입법 모델”이다. 물론 미국이 민간부문에서 시장중심의 자율규제를 중시하고 있지만, 공공부문에서는 일찍부터 엄격한 공법적 보호체계를 갖추고 있는 점에 유의하여야 한다.²⁸⁴⁾ 우리나라의 현행 개인정보보호법제의 세계적 위상과 좌표를 평가하기 위해서는 간략히 이들 입법모델을 검토할 필요가 있다.

(1) 정부 주도의 일원적·포괄적 입법모델 : 유럽의 접근방식

유럽에 있어서 개인정보보호의 문제는 그 성격상 정치적으로 보호되어야 할 인권의 문제로 취급된다. 즉, 시민은 자신의 개인정보가 공정하게 처리되는 것에 대해 기본적 인권을 가지고 있는 것으로 인정된다.²⁸⁵⁾ 그리하여 이러한 인권을 보장하기 위한 법적 보호수단에 초

283) 개인정보보호모델에 관한 상세는, 이인호, “개인정보보호에 대한 국제적 동향 분석 -3가지 집행모델과 그 통합론을 중심으로-”, 『인터넷법률』 통권 제18호(법무부, 2003) 참조.

284) 미국의 개인정보보호법제에 관한 상세는, 이인호, “미국의 개인정보보호법제에 대한 분석과 시사점”, 『법학논문집』 제29집 제1호(중앙대학교 법학연구소, 2005) 참조.

285) Council of Europe Convention for the Protection of Human Rights and Fundamental

점이 맞추어져 있다. 이 모델 하에서는, 포괄적인 입법을 통해 공공부문이든 민간부문이든 모든 개인정보처리에 관해 총체적이고 전반적인 권리와 의무를 규정한다. 그리고 그 권리와 의무의 집행은 전문적이고 독립된 감독기구를 통해 이루어진다.

현재 유럽연합의 개인정보보호지침을 비롯한 각 회원국의 개인정보보호법은 모든 개인정보의 처리(=수집·이용·제공)의 법적 허용기준과 그 처리에 있어서의 여러 절차적 요건을 상세하게 규정하고 있으며, 나아가 정보주체의 열람·정정·거부권을 인정하고, 그리고 이러한 법적 기준과 요건의 준수를 감독하기 위한 독립된 개인정보감독기구를 마련해 놓고 있다.²⁸⁶⁾ 이에 따라 개인정보처리의 기본원칙들은 모두 법적인 권리와 의무로 전환되어 있다. 사실 유럽연합의 개인정보보호지침(95/46/EC)은 개인정보보호에 관한 각 회원국 간의 국내법원칙의 차이를 제거하고 공통된 법원칙을 마련하기 위한 것이었다. 물론 이들 입법의 구체적인 요건과 그에 대한 해석은 다양할 수 있지만, 그 입법정신의 기저에는 개인정보보호는 국가에 의해서 보장되어야 할 기본적 인권이라는 공통된 입장이 깔려 있다.

이러한 유럽모델의 이념적 배경은 다음과 같이 설명될 수 있다. 뒤에서 살피는 미국의 자유주의 정치전통과는 달리, 유럽은 사회보장의 관점에서 개인정보보호에 접근하고 있다. 미국이 사적 계약에 의한 사회구성 원리를 지향한다면, 유럽의 정치전통은 사회 전체를 통합하

Freedoms 제8조; 1980년 유럽평의회 협약(Convention No. 108); EU 지침(95/46/EC) (제1조 제1항은 지침의 목적이 “자연인의 기본적인 권리와 자유, 특히 개인정보의 처리와 관련한 자연인의 프라이버시권(right to privacy)을 보호”하는데 있음을 선언하고 있음) 등 참조.

286) 유럽연합, 영국, 그리고 독일의 개인정보보호법상의 구체적인 입법기준에 관해서는 아래 제4편 제3장 및 제4장 참조. 그 밖에 유럽 각국의 개인정보보호법의 내용에 대해서는, Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*(Ithaca: Cornell University Press, 1992), pp. 153-192; Fred H. Cate, *Privacy in the Information Age*(1997), pp. 32-48; Douwe Korff, *Data Protection Law in the European Union*(2005) 참조.

여 국가를 창설하는, 그리하여 사회 내 권력을 국가에 포괄적이고 절대적으로 이양하는 이른바 “사회계약”(Social Contract) 이론에 기초하고 있다고 하겠다. 이 정치철학에서는, 개인이 그 속에서 자아발전을 도모하게 되는 사회공동체가 구체적으로 조직되고 형성됨에 있어서 국가는 핵심적인 역할을 수행하는 것으로 간주된다.²⁸⁷⁾ 그리고 시민의 자율은 법적 권리의 뒷받침 하에서 효율적으로 확보될 수 있다고 인식된다.

이러한 정치전통에서, 개인정보보호는 기본적 인권보호의 관점에서 요구되는 정치적 명령이다.²⁸⁸⁾ 시민들은 개인정보보호와 관련해서 민간의 기업보다 정부를 더 신뢰한다.²⁸⁹⁾ 따라서 여기서 개인정보보호의 문제는 공법의 한 영역으로 다루어지게 된다. 즉, 사회보장의 관점에서 국가는 개인정보처리기관과 정보주체 사이의 힘의 균형을 맞추기 위해 직접적인 공법적 규제를 통해 양자 사이에 개입하게 된다. 그리고 그 규제는 모든 부문에 걸쳐 포괄적인 권리와 책임을 설정함으로써 예방적 차원의 보호를 도모하고자 한다.

이런 유럽방식의 일원적·포괄적 입법모델은 지난 30여년의 기간 동안 개인정보처리를 규율하는 기본적인 수단으로 간주되어 왔다.²⁹⁰⁾ 최근 들어서는 종래까지 포괄적 규율모델을 채택하지 않았던 아시아

287) Yves Poullet, “Data Protection Between Property and Liberties: A Civil Law Approach”, in: *Amongst Friends in Computers and Law*(H.W.K. Kaspersen & A. Oskamp eds., 1990), pp. 170-175.

288) 프랑스 개인정보보호법 제1조는 그 첫머리에서 “컴퓨터처리는 시민에게 봉사하여야 한다.”고 선언하고 있다. Law No. 78-17 of Jan 6, 1978, art. 1 <<http://www.cnil.fr/textes/text02.htm>>

289) Herbert J. Spiro, “Privacy in Comparative Perspectives”, in: *Privacy Nomos XIII*(J. Roland Pennock & John W. Chapman eds., 1971), p. 122. 본 입법평가를 위해 수행된 설문조사에 의하면, 우리나라의 시민들도 기업의 개인정보처리가 정부의 개인정보처리보다 더 위험한 것으로 인식하고 있는 것으로 나타났다. 이에 관해서는 아래 제4편 제5장 제1절 참조.

290) Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*(Ashgate, 2003), p. 101.

및 남미의 국가들도 유럽모델의 영향을 받아서 민간부문과 공공부문을 통합적으로 규율하는 일반법으로서의 개인정보보호법을 제정하고 있다. 예컨대, 아르헨티나는 2000년 10월 4일 개인정보보호법(Personal Data Protection Act)을 유럽연합의 개인정보보호법을 모델로 하여 제정하였다.²⁹¹⁾

한편, 캐나다와 호주는 전통적으로 공공부문에서 개인정보보호법을 제정하고 독립된 개인정보감독기구(Privacy Commissioners)에 의해 규율하여 왔던 오랜 경험을 가지고 있다. 그러나 이들은 1990년대 들어 공공부문의 개인정보보호원칙들을 민간부문에 확장시키는 입법정책을 채택하였다. 이들 나라에서는, 민간부문에서의 기존의 자율규제 형태가 미약하다는 점을 인식하였고, 공공부문과 민간부문의 기준들을 일치시켜야 한다는 압력이 있었으며, 유럽연합 개인정보보호지침의 역외 적용에 대한 고려가 그 요인으로 작용하였다.²⁹²⁾

그러나 이러한 유럽모델에 대한 비판이 전혀 없는 것은 아니다. 1999년 9월 13-14일 홍콩에서 열린 제21차 『프라이버시 및 개인정보보호 국제회의』(21st International Conference on Privacy and Personal Data Protection)에서 오스트레일리아의 발제자인 Nigel Waters는 유럽연합의 개인정보보호지침(Directive 95/46/EC)이 세계적인 모델인가, 아니면 국제적인 정보공유에 불필요한 장애물인가 하는 문제제기를 한 바 있다. 여기서 그는 유럽모델에 대한 중요한 비판논거로서 기술 및 조직구조의 변화를 제시하고 있다.²⁹³⁾ 즉, 유럽모델은 사생활침해의 문제에 대한 낡은 대응방식으로서, 최근의 기술 및 조직구조의 변화를 충분히 고려하지 못하고 있다는 것이다. 또한 미국의 Swire와 Litan도 유럽모델은 지나치게 광범위하고(overbreath), 포괄적이며(complexity), 유연성

291) 영문번역본은 <www.privacyinternational.org/countries/argentina/argentine-dpa.html> 참조.

292) Bennett & Raab, *op. cit.*, p. 104.

293) Nigel Waters, "Re-thinking Information Privacy - A Third Way in Data Protection?", 21st International Conference on Privacy and Personal Data Protection(1999. 9. 13), pp. 3-8.

이 결여되어 있다는 점(inflexibility)에서 비판을 가하고 있다.²⁹⁴⁾

또한 유럽모델은 중앙집권적인 감독기구(centralized supervisory authorities)의 실효성에 대해 지나친 신뢰를 두고 있다는 점이 문제점으로 지적된다. 예컨대, Waters는 유럽의 감독기구들의 존재와 역할에 대해 일반 대중의 인지도가 낮고, 개인정보의 남용과 감시를 막는 역할과 기능에 있어 그다지 효율적이지 못하다는 평가를 하고 있다.²⁹⁵⁾ David Flaherty도 유럽과 미국의 보호 법제를 분석한 저서²⁹⁶⁾에서 유럽의 감독기구들이 그 제한적인 업무수행능력으로 인해 개인정보의 남용을 억제하기보다 그것을 정당화시키는데 더 기여하는 것이 아닌가 하는 문제를 중심주제로 다룬 바 있다.

(2) 자율규제 중시의 이원적·부문별 입법모델: 미국의 접근방식

개인정보보호에 관한 미국의 전통적인 입법모델은 공공부문과 민간부문을 분리하여 이원적으로 접근하는 방식이다. 그리하여 공공기관의 개인정보처리에 대해서는 일찍부터 공법적 규율을 통해 인권으로서의 프라이버시를 보호하면서도²⁹⁷⁾, 민간부문의 개인정보처리에 대해

294) Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Data Protection Directive*(1998), p. 50.

295) Nigel Waters, *op. cit.*, pp. 5-6.

296) David H. Flaherty, *Protecting Privacy In Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*(1989).

297) 세계에서 최초로 개인정보보호법이 제정된 것은 1973년에 스웨덴에서였다. 독일, 덴마크, 오스트리아, 프랑스, 노르웨이, 룩셈부르크가 모두 1978년에, 영국이 1984년에, 네덜란드가 1988년에 각각 개인정보보호법을 제정하였다. 미국은 스웨덴보다 1년 늦었지만 세계에서 두 번째로 1974년에 연방차원에서 공공부문을 규율하는 개인정보보호법인『프라이버시법』(Privacy Act of 1974)을 제정하였다. 그리고 이 법은 1988년에 공공기관간의 컴퓨터결합(computer matching)을 규제하기 위해서 제정된 『컴퓨터결합과 프라이버시보호법』(Computer Matching and Privacy Protection Act of 1988)에 의하여 보완되었다. 이 법의 구체적 내용에 대한 소개는, 변재욱, “입법소개: 1988년의 컴퓨터연결 및 프라이버시보호법”, □□미국헌법연구□□ 제1호(미국헌법연구소, 1990), 33-58면; 김일환, □□개인정보보호법제의 정비방안에 관한 연구□□(한국법제연구원, 1997), 120-122면 참조.

서는 기본적으로 시장의 자율규제기능을 중시하고 다만 시장의 실패가 드러난 부문에서 개별입법을 제정하는 접근방식을 취하고 있다. 미국이 공공부문에서 개인정보보호문제를 접근하는 시각은 유럽의 그것과 크게 다르지 않다. 유럽과 다른 것은 민간부문의 개인정보처리에 관한 접근방식이다.

사실 미국은 인터넷 등 컴퓨터기술의 발전을 주도하는 나라로서 정보사회에서 개인정보처리와 관련하여 개인의 프라이버시가 침해될 수 있다는 점을 세계에서 가장 먼저 인식한 나라 중의 하나이다.²⁹⁸⁾ 때문에 공공기관에 의한 무분별한 개인정보처리로부터 시민의 프라이버시를 보호하기 위해서 세계 두 번째로 공법적 규율의 개인정보보호법을 마련했던 것이다. 1974년의 『프라이버시법』은 개인정보를 처리하는 각 공공기관이 준수하여야 할 의무와 정보주체의 권리들을 상세하게 규정하고 있다. 물론 이 법은 유럽처럼 그 의무와 권리의 이행을 감독하는 독립된 감독기구를 별도로 두고 있지는 않지만, 대통령 직속의 관리예산처(OMB)가 그 집행책임을 지고 있고²⁹⁹⁾, 나아가 법원에 의한 효과적인 권리구제절차를 마련해 놓고 있다.

흔히 미국이 개인정보보호와 관련해서 자율규제에 의존한다는 식의 인식은 오해를 불러일으킬 수 있다. 미국이 자율규제를 중시하는 접근방법을 채택하고 있는 것은 민간부문에 국한된 이야기이다.

미국은 민간부문에 있어서는 유럽의 정치적 접근방식과는 달리 시장중심의 경제적 관점을 채택하고 있다. 이 시장중심의 모델에서 정부의 역할은 훨씬 제한적이다. 정부에 의한 직접적인 보호보다는 시

298) Henry H. Perrit Jr., *Law and the Information Superhighway*(Wiley Law Publications, 1996), p. 88.

299) 물론 OMB에 의한 집행체계는 강력하지는 않다. OMB가 감독책임을 맡고 있지만, 전문적인(dedicated) 보호기구는 아니다. 그리고 그의 영향력은 산발적이고 무디게 행사된다. R. Gellman, "Conflict and Overlap in Privacy Regulation: National, International, and Private", in: B. Kahin & C. Nesson (eds.), *Borders in Cyberspace*(MIT Press, 1997).

장의 자율규제(self-regulation)에 더욱 의존한다. 그리하여 산업계의 실무규약(code of practice)과 기업의 개인정보처리관행을 법률보다 선호한다. 이 모델에서 개인정보보호는 정치적으로 보호되어야 할 권리의 문제라기보다 경제적 관계설정의 문제로 취급된다. 그리고 개인정보보호에 관한 논의는 “시민”(citizens)이라기보다 “소비자”(consumers)라는 관점에서 주로 이루어진다.³⁰⁰⁾

이 모델 하에서, 법률은 단지 시장이 실패했다고 인정되는 특정 영역의 구체적 문제를 해결하기 위해서만 개입한다. 그리하여 법률의 직접적인 규율은 좁게 한정된 부분적 보호에만 그친다. 예컨대, 미국의 「비디오프라이버시보호법」(Video Privacy Protection Act)은 비디오 가게에서 고객이 빌린 특정 영화의 제목을 공개하는 것을 금지하고 있을 뿐이고,³⁰¹⁾ 인터넷상에서 스트리밍 비디오(streaming video)를 보는 관람습관에 대해서는 아무런 보호를 하지 않고 있다. 이러한 부분적 보호의 접근모델에 있어서는, 개인정보보호의 기준을 설정하는 1차적 원천은 자율규제이다. 즉 개인정보보호는 의회의 제정법에 의한 법적 권리에 의해서라기보다 주로 산업계의 자율규범 내지 실무규약이나 계약에 의해 이루어진다.

민간부문에서의 이러한 미국모델이 딛고 있는 이념적 배경은 다음과 같다. 미국의 정치체제는 기본적으로 Locke적 자유주의(Lockean Liberalism)의 전통을 가지고 있다. 이 전통에서는 국가권력의 제한에 초점을 맞추는 제한정부(limited government)가 강조되고, 정부가 사적 관계를 규율하는 것에 대해 이념적으로 강한 거부감을 가지고 있다. 로크의 사고에 의하면, 정부의 역할은 재산(property)의 보호에 있으며,

300) 그렇기 때문에 미국의 경우 인터넷에서의 상거래와 관련한 개인정보보호의 문제는 주로 시장의 공정거래질서를 확보하기 위해 설립된 연방거래위원회(FTC)의 소관 사항이며, 기업이 개인정보처리원칙을 위반한 경우 불공정거래행위로 취급되어 규율된다.

301) 18 U.S.C 2710-11 (1994).

정부는 억제되어야 할 힘이다.³⁰²⁾ 개인정보보호와 관련해서도 자유주의적 접근방식은 사적 권리를 선호하며,³⁰³⁾ 정부의 직접적인 개입에 기본적으로 거부반응을 보인다.³⁰⁴⁾

특히 미국은 자유로운 정보유통(free flow of information)을 제1의 원리로 삼는 강한 언론자유 전통을 가지고 있다. 개인정보의 자유로운 유통이 사적 활동과 자율을 촉진시키는 것이기 때문에, 그 만큼 정부규제보다는 사적 계약이야말로 개인정보보호의 일차적인 法源이 되어야 하고, 그러므로 개인은 자기 자신의 권리를 스스로 주장하고 요구하여야 한다.³⁰⁵⁾

이러한 자유주의적 전통은 미국이 개인정보보호의 기본원칙들을 집행함에 있어서 큰 의미를 가진다. 포괄적인 입법이 아닌 부문별 입법을 통한 접근방식은 민간영역에서 이루어지는 개인정보처리에 대해 정부의 개입을 최소화하고자 하는 것이다. 자유주의 정치전통에서는 법률보다 시장이 원칙적으로 개인정보보호의 정도를 결정한다는 점에 대해 기본적인 합의를 이루고 있다. 개인정보는 양도 가능한 상품으로 인식되며, 개인의 자율은 개인정보의 판매에 관한 개인적 결정능력에 달려 있게 된다. 정부의 규제는 자유로운 정보유통의 과정에 인위적으로 개입하는 것이 된다. 이에 따라, 법률은 개인정보가 어느 범위까지 보호되어야 할 것인지에 관한 실체적 내용을 정하는 것이라기

302) John Locke, *The Second Treatise of Government*(1690)(Thomas P. Peardon ed., Liberal Arts Press, 1952), pp. 70-82.

303) 예컨대, David W. Leebron, “The Right to Privacy’s Place in the Intellectual History of Tort Law”, 41 *Case W. Res. L. Rev.* 769, 785-88 (1991) (Brandeis의 프라이버시에 대한 접근방식이 자유주의적 반다수결주의였음을 설명하고 있다).

304) Herbert J. Spiro, “Privacy in Comparative Perspectives”, in: *Privacy Nomos XIII*(J. Roland Pennock & John W. Chapman eds., 1971), pp. 121-128 (미국인들은 자신의 개인정보를 정부보다 사적 기관과 공유하는 것을 더 편하게 느끼는 반면, 유럽인들은 그 반대의 경향을 보이고 있음을 지적하면서, 독일과 미국은 프라이버시에 관해 정반대의 입장에 있는 반면, 영국은 그 중간에 위치한다고 주장하고 있다).

305) Joel R. Reidenberg, “A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace”, 52 *Stan. L. Rev.* 1315, 1342 (May, 2000).

보다 시장의 과정(market process)을 규율하는 것에 초점을 맞추어야 한다. 그 다음에는 시장이 개인정보처리의 기본원칙들을 집행하게 될 것이다. 때문에 미국의 경우 아직 온라인상에서의 개인정보 수집과 이용 및 제3자 제공을 규제하는 입법을 가지고 있지 않다. 다만, 1998년에 이르러서 온라인상에서 아동의 개인정보를 보호하기 위한 법률인 『아동온라인프라이버시보호법』(The Children's Online Privacy Protection Act of 1998)을 제정했을 뿐이다. 그 밖에 민간영역의 각 부문별로 존재하는 입법들도 주로 개인정보의 정확성(accuracy)에 초점을 맞추고 있으며, 정보주체에게 열람 및 정정청구권은 일반적으로 인정되고 있지 않다. 그러나 이러한 미국모델에 대하여 많은 비판이 제기되고 있다. 개인정보보호의 문제를 시장에서 결정하도록 하는 자율규제에 지나치게 의존하는 것은 개인정보보호에 함축되어 있는 비경제적 가치의 문제를 소홀히 다루게 되는 결과로 이어질 가능성이 높다는 것이다.³⁰⁶⁾ 정보적 자기결정권은 중요한 인간의 가치임과 동시에 민주적 정치질서의 핵심요소인데, 이것을 단순히 경제적 시장에 내어 맡기는 것은 이념적으로도 무리라는 것이다. 더 나아가, 개인정보시장에서 개인의 결정권능은 네트워크 효과에 의해 제한될 수 있다. 예컨대, 어떤 한 개인이 자신의 유전정보를 자발적으로 공개하게 되면 그것은 곧 그의 친척의 유전정보를 공개하는 것이 되는 것과 같이, 제3자의 공개로 인해 특정 개인은 자신의 정보에 대한 결정권능을 상실하게 될 수도 있다. 보다 많은 개인정보가 공개되어 유통되고, 추론에 의한 프로파일링(inferential profiling)이 더욱 활발하게 이루어지게 되면, 특정 개인이 시장에서의 선택적 결정에 참여할 수 있는 가능성은 그만큼 축소되게 될 것이다.³⁰⁷⁾

306) Joel R. Reidenberg, "Restoring Americans' Privacy in Electronic Commerce", 14 *Berkeley Tech. L. J.* 771 (1999).

307) Joel R. Reidenberg, Joel R. Reidenberg, "Privacy Protection and the Interdependence of Law, Technology and Self-Regulation", 23rd International Conference on Data Pro-

개인정보를 보호하는 방향으로 시장이 효율적으로 기능하기 위해서는 투명성의 요소는 필수적이다. 그렇지만, 프라이버시 시장은 시장실패의 전형적인 예가 될 수 있다. 기업의 실제 정보처리관행은 일반 대중의 시야에서 대체로 벗어나 있다. 사실, 개인정보처리기관과 정보주체 사이의 관계는 전형적으로 정보불균형(*information asymmetry*)의 상태에 놓여 있다. 즉, 정보처리기관은 자신이 획득하는 개인에 관한 정보의 성격과 범위에 대해서는 알기 어렵게 하면서도, 정작 자신에 관해서는 어떤 정보가 얼마만큼 공개될 것인지를 통제할 수 있는 보다 큰 힘을 가지고 있는 것이다.³⁰⁸⁾ 기업이 개인에 관한 정보를 얼마나 보유하고 있고 어떻게 사용하고 있는지에 관해 당해 정보주체가 아는 것은 대단히 어려운 일이다. 동시에, 기업은 일반 대중의 시야를 벗어나 은밀히 개인정보를 거래함으로써 엄청난 이윤을 얻을 수 있다. 이 경우 피해자는 아무런 구제수단을 갖지 못하며, 정보처리의 기본원칙이 준수되고 있는지를 결정할 어떤 독립된 메커니즘도 존재하지 않는다. 이러한 여건 속에서, 시장은 정보주체에게 공정한 정보처리를 위해 협상할 기회조차도 제공하지 않을 것이고, 또 할 수도 없을 것이다.

물론 이러한 자율규제의 결함을 보완하기 위한 미국의 대응은 시장실패가 분명히 확인되는 영역에서 부분적인 보완입법을 제정하는 것이었다. 그렇지만 이 같은 부분적인 대응은 그 자체 한계를 지니고 있다. 예컨대, 신용을 받을 수 있는 자격여부에 대한 결정과 관련해서 신용정보회사(*credit reporting agencies*)가 과거의 신용정보를 제공하는 것은 규제하고 있지만,³⁰⁹⁾ 순수한 판매목적으로 동일한 정보를 직접 마케팅회사(*direct marketing organizations*)가 제공하는 것은 규제하지 않

tection Commissioners, p. 5.

308) Philip Agre, "Introduction", in: *Technology and Privacy: The New Landscape*(Philip E. Agre & Marc Rotenberg eds., 1997), p. 11.

309) 15 U.S.C. 1681b.

고 있다. 이러한 접근방식은 위험한 정보처리의 많은 영역을 보호하지 않는 상태로 방치하게 된다. 현재 미국은 민간부문을 규율하는 일반적인 개인정보보호법을 제정하지 않고 있는 유일한 선진국이라고 할 수 있다.

2. 우리의 이원적·영역별·부분적 보호법제

2008년 9월 현재 우리나라의 개인정보보호법제는 한 마디로 “이원적·영역별·부분적 보호법제”라고 평가할 수 있다. 이를 분설하면 아래와 같다.

첫째, “이원적”이라 함은 공공부문과 민간부문을 각각 별도의 법률에 의하여 규율하고 있음을 의미한다. 위 본편 제2장에서 살핀 바와 같이, 우선 공공부문의 일반법으로서 공공기관의 개인정보처리를 규율하는 『공공기관의 개인정보보호에 관한 법률』(이하 “공공기관개인정보보호법”)이 1994년에 제정되어 시행되고 있다. 그러나 『주민등록법』, 『호적법』, 『통계법』에서는 각각 주민등록정보, 호적정보, 통계정보의 처리·이용에 관해서 규율하고 있다. 그 밖에 학생정보는 원래 공공기관개인정보보호법의 규율대상이 되나, 2003년 전국단위 교육행정정보시스템(NEIS) 사태³¹⁰를 계기로 2005년 3월에 학생정보의 이용과 보호를 규율하기 위해 교육관계법이 개정되었다.³¹¹ 또한 중앙인사위원회가 관리하는 국가인재데이터베이스의 구축 및 운영을 규율하기 위해 대통령령으로서 『공직후보자에 관한 정보의 수집 및 관리에 관한 규정』이 2005년 9월 30일 제정·공포되었다. 또한 민감한 개인정보(sensitive data)라고 할 수 있는 개인의 범죄기록의 수집·이용·제3

310) 교육행정정보시스템 사태에 관한 헌법적 평가에 관해서는 이인호, “학생의 정보 프라이버시와 교육행정정보시스템(NEIS)”, 『인권과 정의』 통권 제329호(대한변호사협회, 2004. 1) 참조.

311) 교육기본법중개정법률(제7399호)과 초·중등교육법중개정법률(제7398호)이 2005년 3월 24일 공포되었다.

자 제공을 특별히 규율하는 법으로 『형의 실효 등에 관한 법률』³¹²⁾이 있다. 이러한 공공부문의 개인정보보호법은 민간부문에는 적용되지 않고, 민간부문에는 별도의 개별입법들이 존재한다.

둘째, “영역별”이라 함은 민간부문에 있어서 일반법이 없이 몇몇 영역별로 개인정보처리를 규율하는 개별법이 존재함을 의미한다. 예컨대, 온라인, 즉 정보통신망에서의 개인정보의 수집·이용·제공을 규율하는 이른바 ‘온라인개인정보보호법’이 존재한다. 1999년에 전면 개정된 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』(이하 “정보통신망법”)이 그것이다. 그러나 이 법률은 2001년에 다시 개정되면서 정보통신망뿐만 아니라 호텔업 등 오프라인에서의 개인정보의 수집·이용·제공을 함께 규율의 대상으로 삼고 있다. 한편, 위 정보통신망법과는 별도로, 정보통신망에서의 위치정보를 활용함과 동시에 그 보호를 목적으로 『위치정보의 보호 및 이용 등에 관한 법률』(제7372호)이 2005년 1월 27일 제정·공포되었다. 그 밖에 신용정보에 대해서는 『신용정보의 이용 및 보호에 관한 법률』³¹³⁾이 있으며, 유전정보의 이용과 보호를 규율하기 위한 법률로서 『생명윤리 및 안전에 관한 법률』³¹⁴⁾이 있다.

셋째, 우리의 현행 개인정보보호법제를 “부분적”이라고 평가하는 것은 민간부문에서 일반법이 없기 때문에 그로 인해 규율되지 못하고 있는 영역들이 다수 존재함을 의미한다. 그 만큼 보호의 공백이 생겨나고 있다. 예컨대, 일반 기업이 고객과의 거래관계에서 생성되는 고객의 개인정보를 축적·가공하여 이를 자신의 마케팅 목적으로 활용하거나 또는 다른 기업에 제공 내지 판매하는 것에 대하여 그 어떤 법률적 규율도 현재로서는 존재하지 않는다.

312) 이 법률은 1980년에 제정되어 수차례의 개정을 거쳐 2005년 7월 29일에 최종 개정되었다.

313) 이 법률은 1995년 1월 5일 제정·공포된 이후, 수차례 개정되었다.

314) 이 법률은 2004년 1월 29일 제정·공포되었다.

온라인개인정보보호법인 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』상의 개인정보보호는 정보통신서비스제공자와 이용자 사이에서의 서비스이용관계를 전제로 하고 있다. 따라서 동법은 이러한 온라인상의 서비스이용관계에서 이루어지는 개인정보의 수집·이용·제공을 규율하는 법이기 때문에, 그러한 서비스이용관계를 벗어난 영역에서의 수집·이용·제공에 대해서는 원칙적으로 동법이 적용되지 않는다.³¹⁵⁾

따라서 정보통신서비스이용관계를 벗어난 영역에서 개인정보보호는 전적으로 당사자 간의 계약관계에 맡겨져 있다. 한편, 민간의 경우 그렇다고 미국과 같은 기업의 자율규제기능도 제대로 작동되고 있지 않다. 우리의 시장에서는 자율규제의 전통과 관행이 확립되어 있지 않기 때문이다.

요컨대, 우리의 현행 개인정보보호법제는 유럽과 같은 일원적·포괄적 입법모델도 아니고, 그렇다고 미국식의 입법모델이라고 보기도 어렵다. 외양은 미국처럼 공공부문과 민간부문이 나누어져 규율되고 있고 또 민간부문에서도 일부 부문별로 개인정보보호법이 존재하고 있어서 미국식에 유사하나, 보호의 실질 면에서 보면 다음의 두 가지 점에서 미국식의 입법모델과 상당한 차이가 있다. 첫째는, 공공부문의 개인정보보호가 상당히 미약하다는 점이고, 둘째는 민간부문의 경우 보호입법이 없는 영역에서 시장의 자율규제기능이 제대로 작동되고

315) 다만, 동법은 “정보통신서비스제공자 외의 자로서 재화 등을 제공하는 자로서 대통령령으로 정하는 자가 자신이 제공하는 재화 등을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우”에 동법의 개인정보보호규정을 준용하도록 하고 있다(제67조). 그에 따라 대통령령은 “1. 『관광진흥법』 제3조 제1항에 따른 여행업 또는 호텔업을 경영하는 자, 2. 『항공법』 제2조 제26호에 따른 항공운송사업을 경영하는 자, 3. 『학원의 설립·운영 및 과외교습에 관한 법률』 제2조제1호에 따른 학원 또는 같은 조 제2호에 따른 교습소를 설립·운영하는 자, 4. 그 밖에 재화 또는 용역을 제공하면서 회원제 또는 그와 유사한 형태로 개인정보를 수집하는 사업 자로서 관계 중앙행정기관의 장과 협의하여 행정안전부령으로 정하는 자”를 준용 대상으로 정하고 있다(제71조).

있지 않다는 점이다. 그리하여 공공부문에서는 보호입법은 있지만 실질적인 보호가 충분히 이루어지지 않고 있고, 한편으로 민간부문에서는 보호의 공백이 크다. 더 기형적인 것은 온라인에서의 개인정보보호법인 정보통신망법상의 규율내용은 역으로 지나치게 보호 쪽으로 기울어져 있어 합리적인 개인정보의 이용과 유통마저도 억제하는 효과를 내고 있다는 점이다.

제 2 절 현행 개인정보보호법제의 문제점 분석

1. 체계부조화의 불균형적인 보호체계

2008년 9월 현재 우리나라 개인정보보호체계는 종합적으로 “체계부조화의 불균형적인 보호체계”라고 평가할 수 있다. 균형 잡힌 완전한 역감시의 참여모델로 전환시켜야 할 입법정책적 과제를 안고 있다.

보호체계의 불균형성이란 개인정보의 이용과 보호라는 두 가치를 균형 있게 조정하면서 개인정보처리의 위험성이 높고 그만큼 보호필요성이 큰 분야에 보다 엄격한 보호체계가 마련되어야 함에도 우리의 현행 법제는 그러한 체계성이 부족하다는 것을 의미한다. 이러한 불균형성은 다음의 4가지 차원에서 확인된다: (i) 공공부문과 민간부문 사이의 보호수준의 차이에 따른 불균형성, (ii) 민간부문 내에서 개인정보보호법이 존재하는 영역(온라인, 신용정보)과 존재하지 않는 영역(근로자정보, 의료정보, 고객정보 등) 사이의 불균형성, (iii) 온라인개인정보보호법인 정보통신망법상에서 보호와 이용의 가치가 균형 있게 조정되어 있지 못한 불균형성, 그리고 (iv) 민간부문에서 개인정보보호법이 존재하지 않는 영역 중에서도 적절한 보호체계가 전혀 작동하지 않는 영역(고객정보, 근로자정보)과 은둔모델에 의한 지나친 비밀보호체제로 인해 이용의 가치가 거의 무시되어 있는 영역(의료정보)

사이의 불균형성.

먼저, (i) 공공부문과 민간부문 사이의 보호수준의 차이에 따른 불균형성에 대해서 보면, 높은 보호수준이 요구되는 공공부문에서는 보호의 수준이나 집행체계가 매우 미약한 반면, 민간부문에서는 특히 온라인과 신용정보 영역에서 표면상으로는 상당히 높은 보호수준과 형사처벌 및 행정제재를 포함하는 강력한 집행체계를 가지고 있다. 현행 공공기관개인정보보호법은 참여모형을 지향하고는 있으나, 전자정부의 효율성 이념과 가치에 압도되어 충분한 역감시의 참여모형을 구현하지 못하고 있는 것으로 평가된다. 자칫 “개인정보보호법”이 아닌 “개인정보이용법”으로 전락할 우려가 있다. 향후 공공부문에서는 그 보호수준과 집행체계를 더욱 강화하고, 민간부문에서는 보다 명확한 행위기준을 제시하는 방향으로 보호체계의 불균형을 시정하여야 할 것이다.

둘째, (ii) 민간부문 내에서 개인정보보호법이 존재하는 영역(온라인, 신용정보)과 존재하지 않는 영역(근로자정보, 의료정보, 고객정보 등) 사이의 불균형성은 일반법의 부존재로 인한 결과이다. 민간의 경우 개인정보의 보호와 이용의 가치를 균형 있게 규율하는 일반법이 존재하지 않아 개별법의 규율범위에 속하지 못하는 영역들이 다수 존재하여 보호의 공백이 발생하고 있다.

셋째, (iii) 온라인에서의 개인정보보호법인 정보통신망법상의 규율 내용은 역으로 지나치게 보호 쪽으로 기울어져 있어 합리적인 개인정보의 이용과 유통마저도 억제하는 효과를 내고 있다.

넷째, (iv) 민간부문에서 개인정보보호법의 부존재로 인해 적절한 보호체계가 전혀 작동하지 않는 영역(고객정보, 근로자정보)이 있는 반면, 또 다른 영역에서는 개인정보보호법이 아닌 비밀보호법, 즉 은둔모델에 의한 지나친 비밀보호체계로 인해 이용의 가치가 거의 무시

되고 있는 영역(의료정보)이 존재하고 있다.

예컨대, 『보건의료기본법』은 보건의료정보³¹⁶⁾의 이용의 가치를 인정하여 보건의료정보화의 촉진³¹⁷⁾ 보건의료정보의 보급·확대³¹⁸⁾, 그리고 보건의료정보의 표준화 추진³¹⁹⁾을 규정하고 있지만, 정작 『의료법』은 “의료인이나 의료기관 종사자는 이 법이나 다른 법령에 따로 규정된 경우 외에는 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다.”고 규정하고(제21조 제1항), 그 위반에 대해서는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처하도록 하고 있다(제88조).

이에 대한 유일한 예외로서, “같은 환자의 진료에 필요하여 다른 의료기관에서 그 환자에 대한 기록, 임상소견서 및 치료경위서의 열람이나 사본 송부를 요청하”는 경우 의료인은 그에 응하도록 요구하고 있다(제21조 제2항). 이러한 비밀보호체계 하에서는 u-health 비즈니스 모델 등 필요한 의료정보의 유통과 활용은 거의 어렵게 될 것이다. 사회적으로 필요한 의료정보의 유통과 활용을 일정한 요건 하에 허용하되 개인정보처리의 절차적 요건³²⁰⁾ 등 오·남용의 위험성을 차단할 수 있는 안전장치를 마련하는 방식으로 의료정보의 활용과 보호를 함께 추구해나가야 할 것으로 보인다.

316) “보건의료정보”라 함은 보건의료와 관련한 지식 또는 부호·수자·문자·음성·음향 및 영상 등으로 표현된 모든 종류의 자료를 말한다(제3조 제6호).

317) 제54조 (보건의료정보화의 촉진) 국가 및 지방자치단체는 보건의료정보화를 촉진하기 위하여 필요한 시책을 강구하여야 한다.

318) 제56조 (보건의료정보의 보급·확대) 보건복지가족부장관은 보건의료기관, 관련 기관·단체 등이 보유하고 있는 보건의료정보를 널리 보급·확대하기 위하여 필요한 시책을 강구하여야 한다.

319) 제57조 (보건의료정보의 표준화 추진) 보건복지가족부장관은 보건의료정보의 효율적 운영과 호환성 확보 등을 위하여 보건의료정보의 표준화를 위한 시책을 강구하여야 한다.

320) 개인정보처리의 절차적 요건에 관한 상세는 아래 제4편 제4장 참조.

2. 예방적 집행기능의 부존재: 처벌 위주의 사후 집행체계

개인정보보호법제는 개인정보의 이용과 보호라는 상충하는 가치를 미묘하게 조정하는 법제이기 때문에 합법적인 처리(=수집·이용·제공)의 기준이 칼로 두부 자르듯이 선명하게 그어지지 않는다. 복잡한 이익형량의 과정을 거칠 수밖에 없는 영역이 개인정보보호의 영역이다. 개인정보보호법에서는 개인정보처리(=수집·이용·제공)의 허용기준을 정하고 나아가 수집·이용·제공의 과정에서 준수하여야 할 절차적 요건들을 규정한다. 또 정보주체에게는 열람·정정·거부권 등을 주고 이들 권리의 행사를 통해 정보처리의 과정에 참여하게 하여 사전에 개인정보처리의 오·남용을 막음으로써 정보주체의 인격적 이익이나 파생되는 다른 권리와 이익의 침해를 예방하고자 하는 데 그 기본 목적이 있다.

바로 그러하기 때문에 개인정보보호체계에서는 법적 기준을 준수하도록 하는 “예방적 집행”이 무엇보다 중요하다. 예방적 집행이란 개인정보처리의 위험성을 사전적·예방적인 차원에서 막기 위하여 개인정보처리기관이 개인정보보호법의 실체적 규정(수집·이용·제공의 허용기준)과 절차적 규정(목적명시 요건, 품질관리 요건, 고지 요건, 보고 요건)을 제대로 준수하도록 사전에 유도하는 기능이다. 이러한 예방적 집행은 감사(auditing), 자문(consulting), 교육(educating), 그리고 자율규제의 유도(inducing self-regulation)의 방식을 통하여 이루어진다.

그런데 우리의 현행 개인정보보호체계를 보면 이러한 예방적 집행기능이 거의 작동되고 있지 않는 것으로 보인다. 특히 민간부문 온라인개인정보보호법인 정보통신망법은 수집·이용·제공의 법적 기준 위반에 대한 사후처벌 위주로 집행체계가 구축되어 있다. 그것도 법적 기준이 보호의 가치 쪽에 치우쳐 있을 뿐만 아니라 그 기준 자체

가 다소 불명확하고 애매한 상태에서 그러한 법적 기준의 위반 여부를 행정청이 일방적으로 결정하여 행정제재를 가하거나 형사처벌의 대상으로 삼고 있다. 이러한 사후제재 위주의 집행방식은 개인정보보호체계에서는 결코 효과적이지 못한 방식이다. 단발적인 효과는 있을지 모르지만, 지속적이고 실질적인 집행의 효과, 즉 안전한 개인정보의 이용이라는 입법목표는 달성되기 어려울 것이다.

3. 독립된 감독기구의 부존재 및 감독기능의 불완전성

우리의 현행 개인정보보호체계에서 중요한 결함 중의 하나는 독립적인 개인정보감독기구가 존재하지 않는다는 점이다. 독립된 개인정보감독기구의 존재는 ‘안전한 개인정보의 이용’이라는 개인정보보호법의 입법목표를 달성하기 위한 가장 핵심적인 요소이자 안전장치이다. 위에서 언급한 바와 같이 우리의 현행 보호체계에서 “예방적 집행 기능”이 제대로 작동하지 못하고 있는 가장 큰 구조적 이유는 바로 이러한 독립적인 개인정보감독기구가 존재하지 않기 때문이다.

공공부문에서는 행정청인 행정안전부장관이 집행책임을 지고 있고, 민간부문의 온라인부문에서는 이전에는 정보통신부장관이, 그리고 지금은 행정안전부장관과 방송통신위원회가 집행책임과 권한을 가지고 있다. 또 신용정보 부문에서는 금융위원회와 금융감독원장이 집행책임과 권한을 가지고 있다. 그러나 행정안전부장관과 방송통신위원회, 금융위원회와 금융감독원장은 개인정보법의 준수 여부를 감독하는 전문적인 개인정보감독기구가 아니다.

개인정보감독기구의 독립성이 강조되는 이유는 감독을 받는 개인정보처리기관이 바로 정부기관들이기 때문이다. 최근에는 기업과 같은 민간기관도 기업의 운영과 경제활동을 위해 방대한 개인정보데이터베이스를 구축하여 이용하고 있지만, 전통적으로 정부기관들은 소관업

무의 수행을 위하여 국민 개개인의 개인정보를 데이터베이스화하여 처리하고 있다.³²¹⁾ 따라서 개인정보를 처리하는 정부기관들이야말로 개인정보보호법의 규율을 받는, 그리하여 개인정보감독기구로부터 감독을 받는 전형적인 기관들이다. 그리하여 감독을 하는 자와 감독을 받는 자가 기능적으로 분리되어야함은 물론이고, 감독기구가 피감독기관으로부터 독립하여 독자적으로 감독업무를 수행할 수 있어야 한다.

현행 공공부문의 집행체계를 보면 상당히 불완전하고 미흡하다. 개인정보처리시스템(“개인정보파일”)의 보유·변경시의 사전협의, 개인정보파일의 인터넷 및 관보에의 공고, 개인정보파일대장의 작성 및 열람 공개는 그 적용을 받지 않는 예외가 상당히 넓어 시스템공개의 요청이 충분히 실현되지 못하고 있다. 물론 행정안전부장관은 사후적으로 개인정보처리시스템을 보유하는 공공기관에 대하여 자료제출 요구 및 의견을 제시할 수 있지만, 전자정부의 구현을 책임지는 행정자치부장관으로서 그 동안 이러한 감독기능을 충실히 수행해 오지 않았다. 오히려 공공기관 사이의 “개인정보의 공동이용”을 전자정부의 개념요소로 당연시하고 있는 현 상황에서 행정안전부장관이 전자정부의 가치와 상반되는 개인정보보호의 가치를 충실히 실현하는 개인정보감독기구로서 기능할 것을 기대하는 것은 결코 쉽지 않은 일일 것이다.

또한 현행의 공공기관개인정보보호법은 공공기관의 위법한 개인정보처리에 의문을 가진 정보주체나 단체가 제기하는 불만이나 민원에 대하여 범위만 여부를 조사하고 분쟁을 해결하는 별도의 민원해결절차를 마련하고 있지 않다. 단지 정보주체가 행정안전부장관에게 침해사실을 신고하면 행정안전부장관은 그것을 해당 공공기관의 장에게 통보하고, 공공기관의 장은 그 처리결과를 행정안전부장관에게 통보

321) 2006년 전체 공공기관이 보유하고 있는 개인정보데이터베이스(“개인정보파일”)는 총 1144개이다. 이 중 중앙행정기관이 277개, 지방자치단체 397개, 교육기관 67개, 정부투자기관 등이 403개를 보유하고 있다. 행정자치부, 공공기관의 개인정보파일목록집, 2006 참조.

하면 장관은 그것을 신고인에게 통지하고 있을 뿐이다(제18조의2). 한편, 별도의 법률에 의하여 설립된 국가인권위원회가 진정의 처리를 통해 민원해결기능을 어느 정도 담당할 수 있겠으나, 그 또한 여러 한계가 있는 것으로 보인다.

다음으로, 현행 민간부문의 집행체계는 온라인 영역에서 한국정보보호진흥원의 개인정보침해신고센터와 개인정보분쟁조정위원회의 적극적인 보호기능을 제외하면 다른 영역에서는 감독기구가 전혀 존재하지 않거나 있다 하더라도 감독기능이 제대로 이루어지고 있지 않다고 평가할 수 있다. 일반적인 보호법이 없는 관계로 민간부문 전체를 커버하는 감독기구가 존재하지 않는다는 점이 가장 큰 문제점으로 지적된다. 다음으로, 현재 존재하는 다른 기구도 주로 전통적인 행정적 집행권한을 가진 행정청이 주로 사후적 행정권의 발동을 통해 보호법의 위반에 대해 제재를 가하는 형태로 집행기능을 수행하고 있다. 물론 온라인 부문에서 민원처리 및 분쟁조정기능이 이루어지고 있지만, 몇 가지 한계를 가지고 있다. 요컨대, 현재 민간부문 전체를 커버하는 전형적인 개인정보감독기구는 존재하지 않는 상태이고, 따라서 향후 사전적·예방적인 보호기능과 유연하고 융통성 있는 분쟁해결기능을 함께 갖춘 독자적인 감독기구를 마련하는 일이 시급한 과제이다.

제 4 장 일본 개인정보보호법제에 대한 사후입법 평가: 경험과 시사점

제 1 절 서 언

일본의 개인정보보호법제는 유럽과 미국의 법제를 고려하여 제정된 것이다. 일본은 이 법률을 시행한 이후에도 법의 추진사업의 합리적 추진을 위하여 계속적으로 정부 각 성청에서 추진·검토하고 있다. 특히 이 법 시행 3년 후에 시행총괄검토를 하도록 하고 있다. 일본의 이런 검토·추진 사업은 사후입법평가라는 점에서도 시사점을 얻을 수 있다. 사후입법평가의 목적은 ①법률의 목표달성 여부 파악, ②법 규정의 부수적 효과(역효과·반작용)와 그 밖에 발생한 효과의 인식, ③현재 규정의 개정필요성과 개정의 범위 확정을 들 수 있는데³²²⁾ 일본 개인정보보호법제의 사후입법평가는 이 중 현재 규정의 개정필요성 및 개정범위의 논의 보다는, 구체적인 현황과 과제를 검토하여 앞으로 행정부가 추진해야 할 사업을 정비하는 측면이 강하다. 물론 이러한 과정 중 일부 시행령이 개정되기도 하였다.

이하에서는 일본 개인정보보호법의 입법과정과 법의 시행·추진 그리고 사후입법평가의 모습을 간단히 검토한 후(제2절), 일본 개인정보보호법의 특징 및 주요내용을 살펴보고(제3절), 이법 시행 이후 의료·신용정보 분야의 과제를 짚어보고(제4절), 2004년도 행정기관에서의 개인정보보호법 실시상황과 개인정보보호법 제정이후 최근까지 계속 되어온 일본 내각부 국민생활심의회 개인정보보호부회의 사후입법평가 및 추진과제(제5절) 순으로 검토하여 우리나라 개인정보보호법제 입법평가에 있어 적합한 시사점을 도출하도록 한다.

322) Carl Böhrer/Götz Konzendorf(박영도·장병일 譯), 『입법평가 입문- 법률, 법규명령, 행정규칙』 (한국법제연구원, 2007), 293면.

제 2 절 개인정보보호법의 제정 · 시행 · 평가

1. 입법의 배경과 제정과정

(1) 입법의 배경

1) IT사회의 도래

개인정보는 본인과 일정 관계가 있는 자에게 유용할 뿐만 아니라, 본인과 타인 사이에 이러한 개인정보의 이용에 대하여 명시 혹은 묵시적 준칙이 존재하며, 이 준칙을 일탈한 개인정보이용이 발생해도 일정 규모이상으로 심각한 문제가 발생하지 않았다.

그러나 IT기술의 진보와 인터넷의 폭발적 진보는 이러한 사정을 변화시켰다. 개인정보를 데이터화하게 되어 대량의 개인정보를 매우 쉽게 복제하여 타인에게 양도·이전할 수 있게 되었다. 현대사회는 ‘본인’이 알지 못하는 사이에 개인정보가 쉽게 이용될 수 있는 상황을 만들어 냈다.

그 결과, ‘본인’이 예기할 수 없는 개인정보 이용을 촉발하여, 프라이버시 문제에 대해 일반인들의 강한 경계심을 불러일으키게 하였다. 그리고 이러한 경계심이 과도하여 ‘본인’에게나 사회에도 유용한 개인정보가 ‘본인’으로부터 제공되지 않게 되고, 그 이용이 크게 제한되게 되어 풍요로운 정보사회생활의 실현 및 유지가 곤란하게 될 우려³²³⁾도 있게 되었다.

2) 준칙의 필요성

‘본인’이 예기할 수 없는 이용을 방지하고, 개인정보에 관한 ‘본인’의 권리이용을 보호하면서, 개인정보의 원활한 이용을 실현하기 위해

323) 新美育文, “個人情報保護法のもたらす変化”, 『ジュリスト』 No 1253(2003.10), 40頁.

개인정보의 이용에 대하여 명확한 준칙을 설정하는 것이 불가결하게 되었다.

종래와 같이 ‘묵시적 합의’에 맡겨지는 것만으로는 적절히 대응을 할 수 없음이 명백해졌다. 도로교통의 규칙으로 도로교통법이 제정되고 있는 것 같이 개인정보의 이용·유통을 위한 준칙이 법률에서 명확히 규정되어야만 하는 시기가 도래한 것이다.

이러한 시대의 요청에 따라 1980년의 OECD 프라이버시 보호가이드라인과 1995년의 EU 개인정보보호지령이 등장하게 되었다. 일본의 개인정보보호법의 정비도 이러한 배경아래 진행되었다.

유럽은 공공분야와 민간분야를 하나의 법률로 규율하고 있다. 반면 종래 일본은 미국과 기본적으로 동일하게 민간부문에 관해서는 유연한 유도정책과 자주규율을 중심으로 프로젝트를 추진하고, 민간부문을 대상으로 하는 법제화에 관해서는 장래의 검토과제로 하였다. 그러나 그 후 일본에서도 민관(民官)을 불문한 컴퓨터의 이용과 네트워크화가 더욱 급속히 추진되었다. 일본 정부는 내각에 ‘고도정보통신사회추진본부’를 설치하고, 관련부처가 하나가 되어 ‘고도정보통신사회’를 위한 관련시책을 추진하고, 그 중요한 과제의 하나로 전자상거래의 추진을 내세워, 이를 위한 환경정비로서 개인정보보호에 몰두하게 되었다. 그런 한편 개인정보가 IT를 활용하여 대량·고속으로 처리되고, 네트워크를 통하여 유통되어, 고객정보 등의 대량 유출과 개인정보의 부정한 매매 등이 현실 사회문제로 부각되었다.

(2) 입법의 경위

1970년대의 소위 國民總背番号制의 도입을 둘러싼 논란을 계기로 개인정보보호에 대한 국민적 관심이 크게 증대하였다. 이후 1975년도쿄도(東京都)의 구니타치시(國立市)의 프라이버시보호조례가 제정되었고, 사회당의 「개인정보보호기본법안(요강)」과 「개인정보에 관련된

컴퓨터규제법안』 발표 등이 뒤를 이었다. 그리고 1980년에 채택된 OECD의 “프라이버시보호와 개인정보의 국제유통에 대한 가이드라인에 관한 이사회권고”가 나오자, 이에 대한 중앙정부 차원의 대응책이 본격적으로 모색되었다. 1981년 1월부터 행정관리청에 프라이버시보호연구회가 설치되었고, 1982년 7월에 “개인정보처리에 따른 프라이버시 보호대책”이라는 검토결과가 발표되었다.

마침내 1988년 4월 28일에 “행정기관이 보유하는 전자계산기 처리에 따른 개인정보의 보호에 관한 법률안”이 일본의 의회에 제출되었다. 이 법안에 대해서는 당초 정부 부처들 사이에 상당한 이견이 노정되었다. 당시 주무 부서인 郵政省은 동법의 제정이 수상실의 권한을 강화할 것이라고 우려하였고, 국민연금과 의료분야에 관한 개인 정보를 보유하고 있는 厚生省도 달갑지 않은 태도를 보였다. 그리고 국가경찰청은 범죄수사에 대한 개인기록의 적용이 제외되어 있었음에도 이 법안의 효과에 대해서 우려를 표명하고 나섰다.³²⁴⁾ 하지만 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』(行政機關の保有する電子計算器處理に係る個人情報保護に關する法律)이 공포되었으며(법률 95호), 1989년 10월부터 부분적인 시행을 거쳐 1990년 10월부터 총무성을 주무관청으로 하여 전면 시행에 들어갔다.

동법은 1999년 12월 8일에 제1차 개정이 있었고(법률 151호), 동년 동월 22일에 제2차 개정이 있었으며(법률 160호), 2002년 7월 31일에 제3차 개정이 있었다(법률 100호). 이 법률에 대해서는 개인정보보호를 위한 감시기능이 총무대신에게 집중되어 있을 뿐 별도의 중립적인

324) UNCTAD, “Data Protection”, *Trade and Development Report(TDR)*, 1988, p. 25; 이 원부 등, “정보통신망에서의 개인정보 침해사례 분석 및 이용규제방안 연구”, 『기술정책연구』 (한국정보보호센터, 1998. 12), 93면에서 재인용.

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, 정보관리자인 공공기관의 책임자에 대한 처벌규정이 미비하다는 점 등이 문제점으로 지적되었다.³²⁵⁾

일본은 1999년 주민기본대장의 일부를 개정하여 주민기본대장네트 워크시스템³²⁶⁾이 도입되었다.³²⁷⁾ 일본 정부는 주민기본대장법 일부개정법안에 대한 회심회에서 동 시스템데이터는 동법에서 개별 구체적으로 엄격히 용도가 특정되고, 민간에서의 사용은 금지되고 있음을 설명하였다. 다른 한편 동 법안심의를 통하여 민간부문에서는 개인정보보호에 관한 규칙이 확립되지 않은 일본법제에서도 개인정보보호에 대한 전반적인 수준 향상이 필요하다는 인식을 함께 하게 되었다.

당시 자유민주당, 자민당, 공명당·개혁클럽의 정책책임자에 의해 개인정보의 보호에 관한 법률을 제정하려는 정책적 합의가 행해졌고 이에 따라 개인기본대장법의 일부 개정에서 「본 법률의 시행에 따라 정부는 개인정보보호에 만전을 기하기 위하여 신속히 필요한 조치를 강구해야 한다」는 부칙이 전원수정에 의하여 추가되었다.

「필요한 조치」의 구체적인 내용에 관하여 고이즈미 내각총리대신이 「민간부문도 대상으로 하는 개인정보보호에 관한 법정비를 포함한 시

325) UNCTAD, “Japan Adopt Privacy Protection Act,” *Trade and Development Report(TDR)*, 1989, pp. 24-25.

326) 일본정부가 2003년 8월 도입한 일본 관 ‘주민등록번호전산화시스템’을 의미함’.

327) 동 시스템은 어디까지나 지방자치단체(市町村)까지 각각의 컴퓨터처리 되어온 주민기본대장의 데이터를 통일적으로 인터넷화 하여 주민의 신청 등에 따른 부담의 감경 과 행정사무의 간소·효율화를 도모하였다. 동 시스템에서는 국민 일인에게 하나씩 市町村에서 공통으로 하는 고유의 번호(주민표코드)를 사용하고 있다. 그 때문에 일부의 주민 단체와 언론 등은 이 고유번호는 ‘국민총번호제’와 관련되고 국민을 컴퓨터로 관리하게 되는 사회를 지향하는 것이 아니냐하는 강한 경계심을 보이며 반대운동을 전개하였다.

시스템을 신속히 정비하는 교시』에서 제시하였고, 이것은 「개인정보보호의 태도에 관하여 종합적으로 검토한 후, 법제 정비를 포함한 시스템 정비를 원한다』는 취지의 답변이 있었다.

그 후 야당에서는 전술한 정책합의에 근거하여 3당에 의한 프로젝트팀으로, 「야당개인정보기본법시스템검토회』가 설립되는 한편, 정부에서는 閣議決定에 근거하여 고도정보통신사회추진본부 산하에 「개인정보기본법제화전문위원회』(위원장 : 園部逸夫 전 최고재판소판사. 위원장대리 : 小早川光郎 동경대학법학부 교수)를 설치하여 본격적으로 사전적 입법평가를 시작하였다. 동 전문위원회는 넓게 관계 각 방면의 실정 등을 조사하면서, 28회의 회의를 거쳐 동년 10월에 「개인정보보호기본법제에 관한 大綱』을 정리하였고, 정보통신기술(IT) 전략본부(고도정보통신사회추진본부가 2000년 7월에 조직개편 된 것)에 보고하였다.

일본 정부부처 내에는 2000년 1월부터 내각관방에 ‘개인정보보호담당실’이 설치되었고 동 대강에 따른 입법안의 입법 등은 동실을 중심으로 추진되었다. 또한 국가의 행정기관, 독립행정법인 등의 공적 부문이 보유한 개인정보보호에 관하여, 大綱에서는 법령에 근거하여 엄격한 보호관리 아래 두도록 특별한 배려가 필요하다는 관점에서 기본법제와는 별도 법제를 정비해야만 한다고 판단하였다. 그 때문에, 총무성에, 총무대신정무관이 주재하는 「행정기관등개인정보보호법제연구회』(좌장 : 茂串俊元 전직 내각법제국과장. 좌장대리 : 塩野宏 동아대학통신제대학원 교수)가 설립되었다. 동 연구회는 2001년 4월 초 회합으로부터 11회의 회의를 거듭하여, 동년 10월에 「행정기관등보유개인정보보호에관한법제의충실강화에대하여-전자정부의개인정보보호-』를 정비하였다. 동 보고에 따른 법안의 입안 등은, 총무성행정관리국(정보부문)을 중심으로 행해졌다.

(3) 의회의 심의과정

『개인정보보호에관한법률안』은 2001년 3월, 일본 정부로부터 일본 제151회 국회에 제출되었다. 그러나 언론계 등에서 미디어규제를 도입한 것이 아니냐는 강한 우려를 나타냈고, 이러한 이유 등으로 동 국회로부터 동년 가을의 제153회 국회까지 심사가 계속 되었다.³²⁸⁾

2002년 가을의 제155회 국회에서는 여당으로부터 야당에 대하여 수정협제의의가 있었으나 그 협의도 성립되지 않았다. 그러다 여당의 ‘개인정보보호시스템검토회’에서 그간의 논의를 근거로 하여 수정요강을 채택·정리하면서, 여당3당은 심사 중의 개인정보보호 관련5개 법안을 일단 폐지하고, 동 수정요강에 따라 새로운 법안을 다음 국회에 제출하도록 정부에 대하여 요청하였다. 2002년 12월, 개인정보관계법 5개 법안은 중의원에서 심의 만료된 채로 폐지되었다.

이후 2003년 3월 제156회 국회에 ‘여당3당 수정요강’에 따라 개인정보보호관련법5개안³²⁹⁾이 일본 정부로부터 제안되었다. 동 국회에서는, 양원에 각각 『개인정보보호에관한특별위원회』가 설치되어, 관계 5법안에 관해 일괄하여 衆參양원에서 각각 약 40시간의 심사가 진행되었다. 관계5법안은 5월 23일의 참의원 본회의에 있어서 여당에 의해 찬성다수결로 가결되어 성립되고, 동월 30일에 공포되었다. 양원의 특별위원회에서는 각각 附帶決議가 붙여졌다.³³⁰⁾

328) 전술한 것처럼 일본정부는 행정기관, 독립행정법인 등의 보유 개인정보보호의 태도에 대하여 검토를 주었다. 2002년 3월 기본법제에 대한 중요한 개별법제와 위치에 관련하여, 행정기관·독립행정법인 등이 보유하는 개인정보보호에 관한 4개 법안이 제154회 일본 국회에 제출 되었다. 전년에 제출된 개인정보보호법안과 함께 이들 관계5법안은 4월 이후 중의원 본회의에서 취지 설명 및 대표 질문, 동 내각위원회의 심사가 행해졌지만, 야당의 찬동을 얻지 못하였고 20시간에 걸친 심의 후에도 계속 심사가 진행되었다.

329) 따라서 기존의 “행정기관이보유하는전자계산기처리에관한개인정보보호에관한법률”(昭和63年法律95号)이 “행정기관이보유하는개인정보보호에관한법률”(平成15年5月30日法律58号)로 전면 개정되었다.

330) 三上・清水・新田, 『個人情報保護法』(有斐閣, 2003), v.

2. 시행 및 추진경과

동법의 시행과 함께 시행령, 기본방침, 각성청의 가이드라인 그리고 기존에 존재하였던 각 지방의 개인정보보호조례의 재개편이 진행되었다. 그리고 이러한 과정 속에서 개인정보보호에 대한 일반인의 의식이 고양되었다. 또 법에서 시행령, 기본방침, 각 성청 및 업계의 가이드라인 정비작업은 개인정보보호체계가 자율규제의 모습을 갖추는데 원동력이 되었다.

(1) 시행령

일본의 개인정보보호관련5법의 정부 시행령(정령)은 2004년 12월에 제출되어 2005년 4월 1일 ‘개인정보보호법 시행령(정령507호) 및 행정기관개인정보보호법시행령(동548호)’로 시행되었다.

(2) 기본방침

개인정보보호법제의 확립을 위해서는 기본법의 성격을 갖는 개인정보보호법(제1장-제3장) 아래 행정기관·독립행정법인 등 민간사업자, 지방공공단체 등이 일체가 되어 활동해야 하는 것이다. 따라서 개별 법과 시책이 ‘종합적이고 일체적’(법7조)으로 추진되도록, 내각부에 설치된 국민생활심의회 개인정보보호회에서 심의가 진행되었다. 여기서는 ① 기본방침의 방향, ② 국가가 강구해야 하는 조치, ③ 지방공공단체가 강구해야 하는 조치, ④ 개인정보취급사업자가 강구해야 할 조치, 고충의 원활한 처리 등의 기본방침 8항목을 정하게 되었다.³³¹⁾

331) 부록 “개인정보보호법 기본방침” 참고.

(3) 가이드라인의 책정

개인정보보호법 시행 당시인 2005년 18개 분야에 25개 가이드라인이 책정되어 있었는데, 주요 분야의 가이드라인의 내용은 다음과 같다.

1) 경제산업 분야의 가이드라인

2004년 10월 12일에 ‘개인정보의 보호에 관한 법률에 관한 경제산업분야를 대상으로 한 가이드라인’(2004년 후생노동성·경제산업성고시제4호)을 책정하였다. 이것은 종전의 ‘민간부문의 전자계산기처리에 관한 개인정보의 보호에 관한 가이드라인’(평성9년 통상산업성고시제 98호)을 폐지하고 새롭게 경제산업 분야 전반의 가이드라인으로 법규정에 적합하게 개정하였다.

본 가이드라인은 사업의 실태에 따라 개인정보의 적정한 취급의 확보를 위한 사업자 계약을 지원하기 위하여 구체적 지침으로 책정한 것이다. 적용대상 범위는 특정의 업종이 아니고 경제산업성 소관 업무전체(소매업, 서비스업, 제조업, 에너지 관련업 등)가 된다.³³²⁾ 다만, 고용관리에 관한 것, 즉 종업원 등에 관해서는 후생노동성과 공동 관할로 한다.

이 가이드라인의 주된 특징으로는 다음을 들 수 있다. 가. 범위반으로 판단된 ‘하지 않으면 안 된다’는 규정과 위반이 되지 않는 ‘바란다’는 규정을 사용하고 있다. 나. 이와 관련하여 보안(시큐리티)에 대하여 ‘바라는 사항’에 사업자가 사업의 성질, 개인데이터 취급상황 등을 감안하고, 리스크 관리 관점으로부터 선택할 수 있는 대응을 위한 추진 메뉴얼 리스트라는 형태로 열거하고 있다. 다. 시행 후 상황의 유연한 대응, 실무상의 의문에 대하여 신속한 답변을 하며 매년 개선

332) 鳥丸忠彦·太田克良、“經濟産業分野に関する個人情報保護ガイドラインの概要”, 『ジュリスト』 No.1287(2005.4.1), 24頁.

하려는 노력을 하는 취지의 규정을 두고 있다.

이 가이드라인의 대상이 되는 것은 어느 특정 고객의 데이터베이스가 아니라 사업자의 일상 업무 전부에 관한 개인정보의 취급방법이다. 따라서 동법3조에 규정된 기본이념을 실현하기 위하여 각 사업자가 적극적으로 구체적인 대응을 하여야 한다. 그러기 위해서는 다양한 업종에서도 다종다양한 개인정보의 취급에 관한 업계단체의 개별 업종의 개인정보보호의 적절한 취급 방법과 주의할 점에 대한 사례를 수집하여 각 사업자에 정보를 제공하는 것 등의 지원이 매우 중요하다고 한다.³³³⁾

2) 의료 분야의 가이드라인

의료 분야는 금융·신용이 정보통신과 함께 ‘개인정보의 성질과 이용방법에 있어 특히 적절한 취급이 엄격히 확보되어야 할 분야’라고 할 수 있다. 일반 의료에 관하여 2개, 연구에 관하여 4개, 합이 6개의 가이드라인이 책정되어 있다.

2004년 6월에 ‘의료기관등의 개인정보보호에 관한 검토회’³³⁴⁾를 만들어 개인정보보호법 전면실시에 따른 의료기관의 개인정보 적절한 취급을 위한 가이드라인의 책정 및 개별법의 필요성에 관한 검토를 포함한 검토를 하였다. 이러한 검토를 통하여 후생노동성은 12월 24일 ‘의료·개호 관련사업자에게 개인정보의 적절한 취급을 위한 가이드라인’을 정리하였다. 이 가이드라인의 특징은 다음과 같다. 가. 자기정보컨트롤권에 친화적이다. 가이드라인 1에서 동의(특히 제3자 제공의 경우)에 대하여 구체사례를 제시하고 있다. 나. 의료현장의 요청에 배려하여 일정의 유보아래 포괄적동의·묵시에 의한 동의가 인정되고 있다.³³⁵⁾ 다. 가이드라인의 책정은 ‘진료정보의 제공 등에 관한 지침’

333) 鳥丸忠彦・太田克良、前掲論文、24頁.

334) 좌장, 樋口範雄 동경대학교 법학부 교수.

335) 이 점에서 금후과제가 의사, 환자, 제3자에 의해 운용 검토의 장을 설치하는 것

이 존재하고 있는 것을 전제로 한 이것도 그 지침의 유효성과 적절한 운용의 검증이 필요하다. 건강진단 결과, 병력 기타 건강에 관한 개인정보 취급에 유의사항을 알리는 통달(행정지침)이 있다.³³⁶⁾

3) 금융·신용 분야의 가이드라인

금융 분야에 대하여는 금융정보시스템센터(FISC)에 의해 ‘금융기관 등에 관한 개인정보보호보호를 위한 취급지침’(1987.3)이 실무를 지배하고 있었다. ‘신용카드사업에서의 개인신용정보보호·이용에 관한 자주준칙’(2001.3)도 존재하였지만, 개인정보보호법제 제정에 따라 본 준칙도 재정비되었다. 본 가이드라인도 경제산업성 가이드라인의 특칙에 해당한다. 그 내용은 금융가이드라인과 중첩되는 것이 많지만, 제3자 제공에 관하여 개인신용정보기관에 대하여 소비자의 이해를 용이하게 하기 위한 조치를 강구하는 것을 요구하는 점이 특색이다. 또 지불곤란에 빠진 채무자가 개인신용정보기관을 통하여 당해채무자 개인의 지불능력에 관한 정보의 이용을 정지하면 정보교류에 의해 적정한 여신 상황, 다중채무의 방지 문제에 대응할 수 없게 될 우려가 있다³³⁷⁾고 한다. 또 대리인에 의한 개시 등의 요구에 대하여 여신사업자가 본인만 직접 개시하는 것을 인정한다.

그 후 금융분야에서의 개인정보 보호에 대하여 ‘금융심의회금융분과회특별부회’에서 심의를 한 후, ‘금융분야에서 개인정보보호에 관한 가이드라인’ 및 ‘금융분야에 개인정보보호에 관한 가이드라인의 안전관리조치 등에 관한 실무지침’을 공표하였다.

이 바람직하다고 한다(藤原静雄, “個人情報保護に関する制度の整備—その成果と課題”, 『ジュリスト』 No. 1287(2005.4.1), 9頁).

336) 본 ‘진료정보의 제공 등에 관한 지침’에 따르면 死者의 정보에 대해서는 법 및 가이드라인의 대상이 되지 않지만, 본 지침에 대상이 되어 환자·이용자가 사망한 때, 유족에 대한 진료정보·개호기록 제공에 대하여 본 지침에 의하도록 하고 있다. HIV감염증, B형간염 등의 감염증 및 유전정보에 대하여 직업상의 특별한 필요성이 있는 경우를 빼고 취득해서는 안 된다고 하고 있다.

337) 藤原静雄, 前掲論文, 9頁.

그것의 특색으로는 ① 개인생활에 관한 정보가 강제적으로 사업자에게 취득되어 이용된다는 것, ② 경제적 가치가 높고, 누출 등에 의한 부정이익의 우려가 높은 ‘정보의 특성’, ③ 그룹 및 개인신용정보기관 등에 광범위한 정보공유가 행해진다는 ‘정보의 이용방법’, ④ 고객의 자산·부채의 계속적 관리 및 운용에 이용된다는 ‘정보의 이용방법’이라는 점이 특별위원회 심의를 통하여 명확하게 되었다.

개인정보보호법 제36조 제1항 제2호에 정한 주무대신 지정에 따라 금융청 소관 법령에 근거한 사업을 하고 있는 자는 가이드라인의 대상이 된다. 취급 개인정보의 수가 개인정보보호법시행령 제2조에 의해 5000건을 넘지 않는 사업자에게는 본 보호법상의 의무를 지지 않기 때문에 본 가이드라인을 준수할 법적 의무가 없지만, 제3항에 정하는 바와 같이 ‘준수에 힘쓸 것’이 요구된다. 가이드라인 제3조 제1항은 보호법 제15조의 취지에 따라 이용목적에 가능한 특정할 것을 요구하고 있다.

4) 정보통신 분야의 가이드라인

① 개 관

정보통신분야에서는 전기통신사업자에 관한 것, 방송수신자 등에 관한 것이 규정되어 있다. 정보통신분야의 가이드라인은 1991년 9월 제정되어 1998년 개정되었다. 또한 개인정보보호법의 실시와 함께 개정되었다. 전기통신분야의 특색은 형사법에 적용이 가능한 ‘통신 비밀’을 중심으로 한 논의가 있었다. 개인정보보호법의 특색인 개인정보, 개인데이터, 보유개인데이터로 구분하지 않고 ‘개인정보’라는 개념만을 사용하는 것, 제3자 제공에 대하여 개인정보보호보다 엄격히 규정한 것(통신이력, 발신자정보)이 특징이다.

가이드라인은 개인정보보호법의 전면실시 후, 전기통신사업자에 대한 개인정보보호법 적용 기준을 명확히 하는 기능을 하기 때문에 용

어, 정의 등에 대하여 가능한 개인정보보호법과 통일 되어야 한다(제2조 등). 개정 가이드라인에는 전기통신사업자가 취하는 기술적 보호조치에 대하여 알기 쉽게 구체적인 예를 기재하고(제11조), 조직적 보호조치 중 종업자 및 위탁자에 대한 감독 등을 더욱 구체화하는 외에(제12조), 전기통신사업자는 당해 전기통신사업자의 개인정보의 적정한 취급 확보를 위해 필요한 권한 있는 자(개인정보보호관리자)를 두어 개인정보관리에 책임지고 필요한 개인정보보호 취급의 감독 등을 하게 한다(제13조).

② 개정 가이드라인의 주요 특징

첫째, 개인정보보호법 및 전기통신사업법상의 통신비밀과의 관계: 가이드라인은 전기통신사업자에 대하여 개인정보보호법의 적용 기준을 분명히 하는 한편, 통신 정보에 관한 전기통신사업법 제4조 기타 관련 규정에 따라 특히 개인정보의 적정한 취급의 엄격한 실시를 요구하는 전기통신사업자가 개인정보의 취급에 해당하여 준수할 기본적인 사항을 분명히 하는 기능이 있다.

둘째, 일본의 전기통신사업법상 통신비밀 보호 규정도 적용되기 때문에 보다 엄격하게 취급된다. 이를 위하여 가이드라인은 개인정보보호법의 예외 규정에 해당하는 경우에도 통신 비밀에 해당하는 경우에는 통신 당사자의 동의 없는 이용과 제3자 제공은 위법성조각사유인 경우를 제외하고 허락하지 않는 것을 확인하는 규정을 두고 있다(제6조 제4항, 제15조 제6항).

셋째, 대리인에 의한 개인정보의 개시를 요구하고 있다(제19조 제3항).

넷째, 개인정보보호법에는 본인이 개인정보 개시를 요구할 수 있도록 하고(제25, 26, 27조), 이 개시 등을 요구할 때 본인이 원격지에 있거나 병중인 경우 본인의 편리를 위해 대리인에 의해 할 수 있도록 하고 있다(제29조 제3항)

다섯째, 제3자의 제공에 있어서 본인의 동의 없이 개인정보의 제3자 제공금지의 예외로, 본인이 요구할 때는 제공을 정지할 수 있다는 것이 주지되어 있는 경우에 본인의 사전 동의 없이 개인정보를 제3자에게 제공할 수 있다(제23조 제2항). 그러나 전기통신사업자가 가입자의 개인정보를 제3자에 제공하는 경우에는 계약약관에 의해 본인 동의를 얻어 행할 수 있지만, 가이드라인에는 본인에게 사전 동의를 얻어 제공하도록 요구하고 있다.

여섯째, 개인정보 취득·이용의 제한(제4조, 제5조 제3항): 방송분야에서도 정보통신으로서 특정 3분야에 해당한다. 사업자가 취급하는 개인정보의 양이 많고, 가정 등에 침투도가 높고, 시청자 이력 등 개인의 취미에 관한 정보에 관하여 신속한 기술혁신에 따른 서비스의 다양화에 따라 취득된 개인정보보호도 다종대량이다. 이러한 특색으로 개인정보보호법 제3조 적정한 취급의 내용으로 시청이력 등의 관리에 특별한 배려를 요청하고 있다.

일곱째, 개인정보 누출 등이 발생한 경우 대응방안: 개인정보의 누출이 발생한 경우에는 그 개인정보의 본인이 적절히 대응할 수 있기 위하여 전기통신사업자는 사업관계를 본인에게 신속히 통지하도록 요구하고 있다. 또 개인정보 누출, 멸실 및 손상이 발생한 경우에는 제2차 피해 방지, 유사한 사안의 발생회피 등을 위해 가능한 사실관계 등을 공표하면서, 본인의 권리의익의 보호, 제2차 피해 방지, 행정이 신속하고 적절한 대응을 취하도록 사실관계를 행정예 보고할 것을 요구하고 있다(제22조).

3. 사후 평가와 점검

일본은 개인정보보호법 제정 및 전면 시행 후, 내각부 국민생활심의회³³⁸⁾안에 개인정보보호부회를 두었다. 최근 IT 추진에 따른 기업의

338) 내각부 소속의 심의기관.

고객정보 누출과 개인정보 매각 등, 개인정보 취급이 사회문제가 된 사례가 발생하고 있어 국민의 프라이머시에 대한 불안이 높아지고 있다. 이러한 상황에 따라 국민이 안심하고 IT사회의 혜택을 향수할 수 있는 법제도의 보급·정착 등에 힘쓰고 있다.

동법 제7조 제1항의 규정에 근거하여 정책된 ‘개인정보보호에 관한 기본방침’에서 내각부는 동법 시행상황에 대하여 동법 전면 시행 후 3년을 경과하여 검토 하고 그 결과를 기본으로 필요한 조치를 강구하는 것으로 되어 있다. 또 국민생활심의회는 동법의 실시상황을 추행 조사 하도록 하고 있다. 이에 따라 국민생활심의회 개인정보보호부회에서는 2005년 11월에 개인정보보호에 관한 검토를 개시하고, 사업자·민간단체·관련성청으로부터 개인정보보호의 실태에 관하여 청취를 통해 2006년 7월에는 ‘개인정보보호에 관한 중요 검토문제’를 정리·공포하였다. 그 후 내각부에서 국민에 대하여 폭넓게 의견 모집을 하면서 동부회에서 검토과제와 국민의 의견 등을 기본으로 논의하여 일정한 의견을 종합 정리하였다.³³⁹⁾ 또한 개인정보보호부회의 활동으로는 제19차 국민생활심의회 개인정보보호검토부회에서 제21차 국민생활심의회 개인정보검토부회를 개최하여 개인정보보호법 실현을 위한 사업추진, 법제의 검토, 개선, 계몽 등을 해오고 있다.³⁴⁰⁾ 특히 개인정보보호에 대한 ‘과잉반응’과 시행상황 등을 검토하여 개정방안을 제시하고 있다.³⁴¹⁾

2007년 6월 29일 국민생활심의회에서는 ‘개인정보보호에 관한 종합 정리’를 발표하였다. 본 내용은 개인정보보호에 관한 법률 실시 후 현

339) 第21次国民生活審議會個人情報保護部会, □□個人情報保護に関する取りまとめ(意見)□□, (国民生活審議會, 平成19年6月29日).

340) 참고로, 내각생활국의 조직안에 개인정보보호추진실을 두어 관련 업무를 하고 있다.

341) 가장 최근 개최된 제21차 국민생활심의회 개인정보보호부회는 2007년 12월 12일 제1회, 2008년 1월 18일 제2회, 2008년 2월 22일 제3회, 2008년 4월 22일 제4회, 2008년 6월 30일 제5회 회의를 하였다.

황을 파악하고, 관련 과제 및 문제점을 제시하고, 향후 검토대상을 분석하였다. 이 내용은 제5절과 제6절에서 상세하게 검토하도록 한다.

제 3 절 개인정보보호법의 주요 내용 · 체계 · 특징

1. 주요 내용

2003년 5월에 제정된 「개인정보의 보호에 관한 법률」 제3조(기본이념)는 “개인정보는 개인의 인격존중의 이념 아래 신중하게 취급되어야 하며, 그의 적정한 취급을 도모하여야 한다”고 규정하여 민간부문과 공공부문을 총괄하는 개인정보처리의 기본법임을 밝히고 있다. 이 법은 기본법으로 민간부문과 공공부문을 총괄하지만, 공공부문의 경우 「행정기관이 보유하는 개인정보의 보호에 관한 법률」이 별도로 제정되어 일반법으로 기능하고, 민간부문의 경우 위 「개인정보의 보호에 관한 법률」이 일반법의 기능을 담당하고 있다.

(1) 개인정보의 보호에 관한 법률

1) 구 성

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

2) 국가의 책무

이 법 제2장과 제3장은 국가와 지방자치단체의 책무에 대해 규율하고 있다. 우선 국가 및 지방자치단체는 개인정보의 적정한 취급을 위

해 필요한 시책을 책정하고 실시해야 한다(제4조, 제5조). 또한 행정기관이나 독립행정법인 등이 보유하고 있는 개인정보가 그 성질이나 보유목적, 업무내용 등 특성에 따라 적정히 취급될 수 있도록 법제상의 조치를 포함한 모든 필요한 조치를 취해야 한다(제6조).

국가 및 지방자치단체의 개인정보보호에 관한 기본방침으로써 정부는 개인정보보호를 위한 기본방침을 제정하여야 하고, 지방공공단체의 시책을 지원하기 위해 필요한 정보를 제공하고 지침을 마련하여 고시해야 하며, 사업자와 개인과의 사이에서 개인정보 취급과 관련한 문제가 발생한 경우 이를 적절하고 신속하게 해결해 줄 수 있는 고충처리조치를 마련해야 한다고 규정하고 있다(제7조 내지 제9조). 이를 위해 법은 제32조 내지 제36조에서 주무부서의 개인정보 침해에 대한 구제에 관한 사항을 규율하고 있다.

3) 개인정보취급사업자의 의무

- ① 이용목적의 특정, 이용목적에 의한 제한(제15조 및 제16조)
 - 개인정보를 취급함에 있어서 그 이용 목적을 가능한 한 특정할 것
 - 특정된 이용목적의 달성에 필요한 범위를 넘은 개인정보 취급은 원칙적으로 금지
- ② 적정한 취득, 취득시 이용목적의 통지 등(제17조 및 제18조)
 - 허위 기타 부정한 수단에 의한 개인정보의 취득 금지
 - 개인정보를 취득할 때 이용목적의 통지 또는 공표
 - 본인으로부터 직접 개인정보를 취득하는 경우 이용 목적을 명시
- ③ 정보내용의 정확성 확보(제19조)
 - 이용목적의 달성에 필요한 범위내에서 개인정보의 정확성, 최신성을 확보
- ④ 안전관리조치, 종업원·위탁처의 감독(제20조 내지 제22조)
 - 개인정보의 안전관리를 위해 필요하고 적절한 조치, 종업원·위탁처에 대한 필요하고 적절한 감독

⑤ 제3자 제공의 제한(제23조)

- 본인의 동의를 얻지 않은 개인정보의 제3자 제공은 원칙적으로 금지
- 본인의 요구에 따라 제3자 제공을 정지하는 것으로 하고 있어 그 취지 기타 일정한 사항을 통지 등을 하고 있을 때는 제3자 제공이 가능
- 위탁의 경우, 합병 등의 경우, 특정인과의 공동이용의 경우(공동이용하는 취지 기타 일정한 사항의 통지 등을 하고 있는 경우)는 제3자 제공으로 간주하지 않음

⑥ 공표 등, 개시, 정정 등, 이용정지 등(제24조 내지 제27조)

- 보유 개인정보의 이용목적, 개시 등에 필요한 절차 등에 대한 공표 등
- 보유 개인정보의 본인으로부터의 요구에 따라 개시, 정정 등, 이용정지 등

⑦ 불평의 처리(제31조)

- 개인정보 취급에 관한 불평의 적절하고 신속한 처리

⑧ 주무 대신의 관여(제32조 내지 제35조)

- 이 절의 규정의 시행에 필요한 한도에 있어서의 보고의 징수, 필요한 조언
- 개인정보 취급 사업자가 의무규정(노력의무를 제외)에 위반하여 개인의 권리의익 보호를 위해 필요가 있는 경우에 있어서의 권고, 권고에 따르지 않는 일정한 경우의 명령 등
- 주무 대신의 권한의 행사의 제한(표현, 학문, 신교, 정치 활동의 자유)

⑨ 주무 대신(제36조)

- 개인정보취급사업자가 행하는 개인정보의 취급 중 고용관리에 관한 것에 대하여는 후생노동대신(선원의 고용관리에 관한 것에 대하여는 국토교통대신)
- 당해 개인정보취급사업자가 행하는 사업을 관장하는 대신
- 내각총리대신은 규정의 원활한 실시를 위해서 필요가 있을 때는 개인정보취급사업자가 행하는 개인정보의 취급 중 특정의 것에 대하여

여 특정 대신 또는 국가공안위원회를 주무대신으로 지정할 수 있음

4) 민간단체에 의한 개인정보보호의 추진

① 단체의 인정(제37조), 대상 사업자(제41조)

- 개인정보 취급 사업자의 개인정보의 적정한 취급 확보를 목적으로 하고, 불평의 처리 등을 실시하려고 하는 단체의 인정
- 인정 단체에 의한 대상 사업자(단체의 구성원등)의 이름 또는 명칭의 공표

② 개인정보보호지침(제43조)

- 인정 단체에 의한 개인정보보호지침의 작성·공표

③ 주무 대신의 관여(제46조 내지 제48조)

- 이 절의 규정의 시행에 필요한 한도에 있어서의 보고의 수령
- 업무의 실시의 방법의 개선, 개인정보보호지침의 변경 등에 대한 명령
- 인정 기준에 적합하지 않게 되었을 경우, 명령에 따르지 않는 경우 등에 있어서의 인정 취소

5) 적용의 제외

- 보도, 저술, 학술연구, 종교활동, 정치활동 등에 제공할 목적으로 개인정보를 취급하는 보도기관, 저술업자, 학술연구기관, 종교단체, 정치단체 등에 대해서는 제4장의 적용을 제외(제50조 제1항)
- 이들 주체는 안전관리, 고충처리 등을 위해서 필요한 조치를 스스로 강구해 그 내용을 공표하도록 노력(제50조 제3항)

※ 기타 권한 또는 사무의 위임, 시행의 상황의 공표 등에 대해 규정

6) 벌칙

- 개인정보 취급 사업자가 주무 대신의 명령에 위반했을 경우 등에 있어서의 벌칙(제56조 내지 제59조)³⁴²⁾

342) 이상 : 岡村久道, 위의 책, 241-253頁 참조.

(2) 행정기관이 보유하는 개인정보의 보호에 관한 법률: 공공부문 일반법

‘행정기관이 보유하는 개인정보의 보호에 관한 법률’은 행정기관의 행정의 적정하고 원활한 운영을 도모하고 개인의 권리와 이익을 보호함을 목적으로 하는 공공부문의 개인정보보호 일반법이다. 이 법은 행정기관에서의 개인정보취급, 개인정보화일, 본인의 권리와 불복청구 등을 규정하고 있다.

1) 구 성

『行政機關の保有する個人情報の保護に関する法律』(이하, 행정기관개인정보보호법)은 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

전자계산기에 의해 처리되는 개인정보에 한하여 적용되던 개정 전의 법률과 달리 동법에서는 수작업 또는 인쇄매체 등에 의하여 작성·처리되는 개인정보도 적용대상이 될 수 있다. 그리고 동법상의 행정기관에는 법률의 규정에 기하여 내각에 설치되는 기관 및 내각 산하에 설치되는 기관, 內閣府, 宮内廳 및 內閣府設置法 제49조 제1항 및 제2항에 규정된 기관, 國家行政組織法 제3조 제2항에 규정된 기관, 內閣府設置法 제39조 및 제55조 및 宮内廳法 제16조 제2항의 기관 및 內閣府設置法 제40조 및 제56조의 특별기관 가운데 政令에서 정한 것, 國家行政組織法 제8조의2의 시설등기관 및 동법 제8조의3의 특별기관으로서 政令에서 정한 것, 會計審査院이 포함된다(제2조 제1항).

따라서 행정기관개인정보보호법은 국가의 행정기관에 대해서만 적용될 뿐이고, 독립행정법인등이나 지방공공단체는 별도의 『獨立行政法人等の保有する個人情報保護に関する法律』이나 독자적으로 제정한 개인정보보호에 관한 조례의 적용을 받는다. 따라서 동법은 국가의 행정기관을 적용대상으로 하는 일반법으로서의 지위를 가진다.³⁴³⁾

한편 개정 전의 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, 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).

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, 갹생 긴급보호 또는 사면과 관련되는 보유개인정보(당해 재판, 처분 혹은 집행을 받은 사람, 갹생 긴급보호의 신청을 한 사람 또는 사면의 진언이 있던 사람과 관련된 것에 한함) 등이 열거되어 있다(제45조 제1항).³⁴⁴⁾

3) 개인정보 취급의 원칙

- 보유의 제한 등(제3조)
- 이용목적의 명시(제4조)

343) 岡村久道, 위의 책, 3頁.

344) 이상 岡村久道, 위의 책, 254-269頁 참조.

- 정확성과 안전성의 확보(제5조 및 제6조)
- 이용 및 제공의 제한(제7조 내지 제9조)
- 보유의 통지와 공표(제10조 및 제11조)

4) 정보주체의 통제권

- 개시청구권(제12조 내지 제26조)
- 정정청구권(제27조 내지 제35조).
- 이용정지 등 청구권(제36조 내지 제39조)
- 불복신청(제42조 및 제43조)

5) 감독기구

2003년에 개정된 행정기관개인정보보호법에 의하면, 행정기관의 장은 행정기관에 있어서 개인정보취급에 관한 불평의 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).

6) 문제점

일본의 행정기관개인정보보호법에서는 과거와 달리 개시, 정정 및 이용정지, 불복신청에 관해 아주 자세한 규정을 두고 있다. 특히 불개시정보(제14조 제2호), 부분개시(제15조), 재량적 개시(제16조), 제3자에 대한 의견서 제출 기회의 부여(제23조) 등에 있어서 제3자의 권익 보호를 하고 있을 뿐만 아니라 정정청구 이외에도 추가·삭제의 청구

를 인정하고(제27조), 개인정보가 불법적으로 취득하거나 목적외의 보유나 이용 또는 제공에 대한 본인의 통제권으로서 이용정지나 소거 또는 제공정지의 청구(제36조 제1항)를 허용하고 있다는 점에서 정보주체의 보호에 큰 진전을 가져올 것으로 기대된다.

하지만 이 법률에 대해서는 행정정기관의 개인정보보호를 위한 감시기능이 총무대신에게 집중되어 있을 뿐 별도의 독립적인 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, 정보관리자인 공공기관의 책임자에 대한 처벌규정이 미비하다는 점 등이 문제점으로 지적되고 있다.³⁴⁵⁾

(3) 개인정보보호조례

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(國立市電子計算組織運營에 관한條例)’가 제정되었는데, 이 조례는 제3조에서 “전자계산조직의 이용에 있어 시민의 기본적인 권을 존중하고 시민의 개인적 비밀유지를 피하지 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

345) UNCTAD, “Japan Adopt Privacy Protection Act” *Trade and Development Report(TDR)*, 1989, pp. 24-25.

증가하였다.³⁴⁶⁾ 1999년 4월 기준으로 전국 3,299개의 都道府縣과 市區町村 가운데 1,521개 지방공공단체가 조례를 제정하였다. 이는 전체의 46.1%에 해당하며, 規則이나 規程 등에 의하여 개인정보보호대책을 강구하고 있는 865개 지방공공단체를 합할 경우 전체의 72.3%에 달한다.³⁴⁷⁾ 또한 2001년 4월 기준으로 전국 3,296개 단체 가운데 조례를 제정하고 있는 지방공공단체는 1,982개의 지방공공단체가 개인정보보호에 관한 조례를 제정하였다. 이는 전체의 60.1%에 해당되며, 규칙이나 규정 등을 제정하고 있는 642개의 단체까지 합하면 전체의 79.6%에 달하는 규모의 전자계산기 처리에 관련된 개인정보를 대상으로 하는 것이 일반적이지만, 매뉴얼 처리 및 민간 부문까지 조례의 대상 범위에 포함시키는 단체도 증가하고 있다.³⁴⁸⁾ 특히 1984년 4월 후쿠오카현(福岡縣)의 카스가시(春日市)에서는 공공부문과 민간부문의 보유 정보 및 전산처리와 매뉴얼처리의 정보 모두를 대상으로 하는 개인정보보호조례를 제정한 바 있다.³⁴⁹⁾ 이것은 개인정보보호에 관한 포괄적 입법에 있어서 선구적 모델이라고 평가할 수 있다.

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(제6

346) 김철완/이민영, “인터넷 개인정보보호에 관한 법제도 연구”, 『정책연구』, 2000, 79면.

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

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

349) 堀部政南, 申九賢, 『프라이버시와 高度情報化社會』(청림출판, 1995), 126면.

조), 수집의 제한(제8조), 이용 및 제공의 제한(제9조), 온라인결합에 의한 제공(제10조), 자기정보개시청구권(제15조), 자기정보정정청구권(제21조) 등에 규정하고, 나아가 민간사업자에 대해서도 지도와 업무등록, 조사·권고·공표 등에 대해서도 규정하고 있다(제3장). 이 가운데서 특기할 만한 것으로 이른바 사업자의 업무등록과 관련하여 縣内에서 개인정보를 취급하는 사업자로 하여금 지사의 등록을 받을 수 있도록 하고(제30조), 이렇게 등록한 사업자는 업무의 등록을 받은 업무와 관계있는 재인정보의 취급에 대해 등록필의 표지를 표시할 수 있도록 규정하고 있다(제32조).³⁵⁰⁾ 개인정보취급업무의 등록상황을 보면 2002년도까지 7,388개 사업자, 13,176개 업무에 이르고 있으며,³⁵¹⁾ 홍보지를 통한 홍보활동 등으로 민간사업자에 있어서의 개인정보 보호의식이 점차 고조되는 성과를 낳고 있다.

2. 입법의 체계

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 함)을 두게 되었다. 그리고 공공부문을 규율하는 일반법으로 「행정기관이 보유하는 개인정보의 보호에 관한 법률」(이하, ‘공공기관 개인정보보호법’이라 함)과 「독립행정법인등이 보유하는 개인정보의 보호에 관한 법률」(이하, ‘독립행정법인등 개인정보보호법’이라 함)이 존재한다. 지방자치단체에 있어서는 개인정보보호조례에 의해 규율이 이루어진다. 이 밖에 개별분야의 개인정보보호에 대하여서는 기본법에 정하여 두고 있지 않고, 개별법에 산재하여 개인정보를 보호하고

350) 임재홍, “개인정보보호법과 개인정보보호조례”, 『민주법학』 9호(1995), 293면 이하 참조.

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

있다. 이러한 개인정보보호법제의 체계를 도표화하면 다음과 같다.³⁵²⁾

[표 2-4-1] 일본의 개인정보보호 법률체계

구 분	공 공 부 문			민 간 부 문
대상	국가행정기관	독립행정기관, 특수법인, 행정기관에 준 하는 기관	지방 공공단체	민간부문
기본법	‘개인정보의 보호에 관한 법률’ [기본이념 등 기본법 부분] - 개인정보의 적정한 취급에 관한 기본원칙 - 국가, 지방자치단체의 책무 - 민간 개인정보취급사업자의 의무 - 사업자 및 인정개인정보보호단체에 의한 자율적인 피해구제제도			
일반법	‘행정기관이 보유하는 개인정보의 보호에 관 한 법률’ - 일반행정기관 보유 개인정보의 적정한 취급원칙 - 이용목적 내의 정보 보유 - 목적외 이용·제공금지 - 정보주체의 열람, 정정, 이용정지청구권 인정	‘독립행정법인 등이 보유하는 개인정보의 보 호에 관한 법률’ - 일반행정기관 과 동일하게 취급됨	개인정보 보호조례	‘개인정보보호에 관한 법률’에서 규율 [개인정보취급사 업자의 의무 등 일반법 부분]
개별법				전기통신사업법, 대금업법, 노동 자파견법 등
	유전자기술규제법(クローン기술규제법), 직업안정법 등			

2003년 5월 23일 개인정보보호 관련 5개 법률의 제정 이후 일본은 공공부문과 민간부문을 포괄하는 기본법의 지위와 민간부문의 일반법의 지위를 가진 「개인정보의 보호에 관한 법률」을 두게 되었다. 그리고 공공부문을 규율하는 일반법으로 「행정기관이 보유하는 개인정보

352) 岡村久道, 『新法解説 個人情報保護法入門』(商事法務, 2003), 2면 참조.

의 보호에 관한 법률』과 「독립행정법인등이 보유하는 개인정보의 보호에 관한 법률』등이 존재한다. 이 밖에 개별분야의 개인정보보호에 대하여서는 기본법에 정하여 두고 있지 않고, 개별법에 산재하여 개인정보를 보호하고 있다.

이렇게 볼 때 일본의 개인정보보호법제는 통합형 기본법과 부문별 일반법, 그리고 개별법이 병존하는 구조라고 할 수 있고, 이를 굳이 유형화하자면 ‘일원적 기본법주의’에 속하는 것으로 평가할 수 있을 것이다.

3. 기본 특징

기본법이면서 민간부문 일반법인「개인정보의 보호에 관한 법률」의 근간을 형성하고 있는 기본적인 생각과 특색을 간략히 정리하면 다음과 같다.

(1) 첫 번째는 본 법률을 일관하는 기본적인 생각은 개인정보의 유용성과 균형성과 함께 개인의 권리 이익을 보장하는 것이다. 이 점은 제1조에 정한 법률의 목적에서 명확히 하고 있다.

프라이버시를 근원으로 하는 개인의 권리의익의 보호가 중요한 것은 말할 필요도 없지만, 생활중에 스스로의 개인정보를 타인에게 전혀 이용되지 않도록 할 수도 없다. 또, 아무래도 사업 활동을 하는데 고객의 개인정보를 이용해서 여러 가지 상품과 서비스를 제공·개발하고, 종업원의 개인정보를 기본으로 고용관리를 하는 것 등을 빠뜨릴 수는 없다.

(2) 두 번째는 제4장에서 규율하고 있는 「개인정보의 적정한 취급」이란 무엇인가 하는 것이다. 우선 ① 이용목적에 명확히 해 그 범위 내에서 취급하는 것, ② 이용목적과 동떨어진 취급을 하는 경우에는

새롭게 본인의 동의를 얻는다는 것이다. 민간부분은 대등당사자간의 계약을 기본으로 한 사회이므로 개인정보의 취급이 늘 명시적으로 표현되는 것은 아니고 본인과 사업자간의 합의와 신의성실의 원칙이 근본이 된다는 것을 유의할 필요가 있다. 또 ③ 개인정보의 IT처리에 수반한 적절한 안전관리를 도모하는 것도 중요하다. 개인정보를 유연한 관리하에 두면 개인의 권리이익이 침해될 위험이 높아진다. IT의 이용에 적절하게 취급된 정보의 내용, 취급의 방법 등에 대응해서 적절한 수준의 정보안전보장을 확보하는 것이 불가결하다. 개인정보의 IT처리에 있어서도 상응하는 안전보장을 구비한 내부의 체계와 규율을 정비하는 것 등이 요구된다.

(3) 세 번째는 개인정보의 적정한 취급에 관한 ‘준칙’의 준수가 어느 정도로 보장 되는가이다. 본 법률에는 담당자간에 있어서 고충처리, 개시·정정·이용정지 등을 통하여 개인정보의 적정한 취급에 관한 ‘준칙’이 자주적·자율적으로 준수되도록 하는 것을 기본으로 하고 있다. 주무대신으로부터 報告徵收, 조언, 권고, 명령이라고 하는 행정으로부터의 관여도 제도화되어 있지만, 그것들은 필요최소한도의 사후적인 방지로서 행해지는 것이다. 명령을 지키지 않는 사업자에 대한 벌칙은 최종적인 제제수단으로 자리잡고 있다.

본 법은 민간분야에 관해서도 법률의 대상으로 하는 점에서 유럽형이지만, 유연한 유도책과 사후조치 등 사업자의 자동성을 중요시하고 있는 점에서는 미국형의 사고에 가까우며, 일본 사회 실정과 제도적인 기반을 토대로 하여 과도한 규제를 피하면서 기술적인 제도가 정비되었다고 평가되고 있다.

官民 양부분에서 개인정보의 적정한 취급이 확보되도록, 제4장의 민간사업자에 대하여 규제조치뿐만 아니라, 제2장 및 제3장에서 국가와 지방공공단체의 책임, 기본방침의 작성 등을 명확히 하고 있다. 국가

의 행정기관, 독립행정법인 등, 지방공공단체라는 공공부분과 특히 엄격한 개인정보의 취급을 필요로 하는 개인분야에 대하여 각각 그 분야에 어울리는 법적 조치를 강구하도록 하는 구조를 갖고 있는 것이 특징이다.

개인정보취급사업자에 관한 업무를 규정하고 있지만, 유럽 여러 나라의 법률과 같은 사전 등록·신청 등에 의하여 사업자를 행정기관에 의한 강력한 감독 하에 두지 않고, 사업자의 자율적인 취급을 존중하는 구조를 하고 있다. 게다가, 주무대신의 報告徴収, 조언, 권고, 명령의 사후적인 관여를 통하여 사업자의 의무 이행을 확보하도록 하고 있다.

독립된 감독기관을 두지 않고 소관 주무대신이 개인정보취급자에 대하여 보고의 징수, 조언, 권고 또는 명령을 할 수 있다(법 제35조). 개인정보취급사업자가 행한 개인정보의 취급 속에 고용관리에 관한 것에 대하여 후생노동대신 및 당해개인정보취급사업자가 행한 사업의 소관대신(법 제36조)이 본법의 사무를 추진하도록 되어 있다.

주로 「개인정보의 보호에 관한 법률」은 내각부가 소관하고, 「행정기관이 보유하는 개인정보에 관한 법률」, 「독립행정법인 등이 보유하는 개인정보의 보호에 관한 법률」은 총무성관할로 하고 있다.

(4) 본법의 시행에 따라 개인정보취급사업자는 법이 정하는 의무를 위하거나 주무대신의 권고에 관한 조치 명령을 받은 경우, 권고를 거친 명령을 한 경우, 이를 위반한 경우 ‘6개월 이하의 징역 또는 30만엔 이하의 벌금형에 처하게 된다(제56조). 보고 요구를 받은 경우 이를 보고 하지 않거나 허위의 보고를 한 자는 30만엔 이하의 벌금에 처한다(제57조). 또한 개인정보보호법에는 업무위탁처의 감독은 책임을 질 수 있다. 본법이 아니더라도 누출한 개인정보의 누출에 의한 피해가 생긴 경우 누출에 의한 민사손해배상의 책임이 발생할 수 있

다. 기타 간접적 손해로서 개인정보취급사업자는 자신의 신용 저하, 개인정보보호시스템과 데이터 검증 비용이 들게 되며, 쇠도하는 문의 등으로 업무능률저하라는 비용이 들게 될 것이다.³⁵³⁾

제 4 절 법률 시행 후 분야별 효과와 과제

1. 개인정보보호법의 시작과 새로운 과제

『개인정보의 보호에 관한 법률』의 시행으로 개인정보의 적절한 취급을 확보하기 위해 본인관여하에 사후적인 통제를 하게 되었다. 따라서 본인은 종전보다 신중한 자기 개인정보 관리를 요구할 수 있게 되었다. 그러나 본인 권리의익을 보호하고 개인정보 유용성을 활용하기 위해 개인정보보호법이 제정된 것만으로 모든 것이 해결되는 것은 아니다. 오히려 법에 의한 준칙의 도입에 따라 본인에게도 개인정보취급사업자에게도 지금까지와 크게 다른 법 준수를 위한 대응이 필요하게 된다. 본법의 시행 초기부터 분야마다 다음과 같은 과제가 지적되었다.

(1) 개인정보데이터베이스 등 관리 상황의 재점검

개인정보취급사업자에게 그 개인정보데이터베이스 등 관리 상황을 재점검하도록 요구하고 있다. 개인정보보호법은 이용목적에 따르는 제한을 중심으로 개인정보보호에 힘쓰고 있다. 따라서 개인정보데이터베이스를 보관 관리하여 그 이용목적을 색인으로 검색할 수 있는 개인정보취급업자는 개인정보법이 시행 될 때까지 개인정보데이터베이스 시스템을 대폭 다시 검토하지 않으면 안 되었다.

353) <http://www.nec-nexs.com/privacy/explanation/penalty.html>

(2) 개인정보취급사업자의 개인정보 이용형태에 대한 재검토

종래 개인정보취급사업자는 개인정보보호법에서 규율하는 목적 이외의 이용, 제3자 제공을 각별히 신경 쓰지 않고 해 왔다고 할 수 있다. 예를 들어 어떠한 기회에 취득한 고객정보를 가지고 스팸메일을 보내거나 혹은 시장조사를 위하여 그러한 고객정보를 이용하는 것은 목적이외의 이용이지만 당연하게 하고 있었다. 그러나 본법 시행 이후에는 종래와 같이 업자의 편의만을 생각한 취급은 할 수 없게 된 것이다. 또 거래 실무를 보면, 제3자에 제공을 매우 쉽게 하는 경향이 있다. 모회사가 자회사에 혹은 자회사가 모회사에 그 보유 개인정보를 제공하는 것에 대하여 거의 거부감 없이 행해지고 있었다. 그러나 개인정보보호법이 용인하는 제3자 제공은 본인의 동의가 있는 경우를 원칙으로 하고 있다.

예외적으로 본인 동의없이 제3자 제공이 용인될 수 있는 경우도 상당히 엄격하다(제23조). 단순히 모회사 혹은 그룹회사라는 이유로 제3자 제공이 적법한 것으로 되지 않는다. 이런 점에서 개인정보사업자는 개인정보의 이용형태를 재검토 하지 않으면 안 된다.

(3) 고충처리를 위한 상당한 물적·인적 비용의 소요

개인정보취급을 둘러싸고 본인의 고충처리에 적절히 대응 하는 것은 매우 중요하지만 이는 개인정보취급업자에게는 부담스러운 일일 것이다. 종래의 소비자로부터 상품에 관한 고충을 처리하는 이상의 노력을 개인정보 관련 고충 처리에 기울여야 하며 이는 매우 부담스러운 일인 것이다.

2. 의료분야의 과제

(1) 환자정보에 대한 기존의 보호방법

의료분야는 다른 산업분야와는 달리 오래 전부터 관련자의 비밀유지를 법률 규제대상으로 하고 있었다. 즉 의사, 약사, 조산사에게는 일본 형법 제134조에 의해 비밀누설죄가 적용되고, 그 외 각종 의료관계 업종에 대해서도 각각 신분범 중에 이른바 비밀의무에 관한 규정이 설정되고 있다.³⁵⁴⁾ 또 이러한 전문 자격을 갖지 않아도 특정 의료영역에 종사하는 자에 대하여 특별법에 의해 비밀준수의무가 있는 경우³⁵⁵⁾도 있다.

이와 같이 일상진료에서 환자정보의 비밀유지는 개인정보보호법의 성립 이전부터 비교적 엄격한 법규제가 강구되고 있고, 동법 시행에 대하여 특히 비밀준수의무가 있는 것은 아니다. 단 전문 직종만을 대상으로 하는 이러한 비밀준수의무규정이 적용되지 않는 의료기관의 사무직원 등에게 개인정보가 취급될 때, 의료기관에서 본법에 의해 감독 등의 적절한 조치를 할 필요가 있다.

(2) 개인정보보호법의 적용

개인정보보호에 관한 법률이 공포되고, 본법이 실시는 의료분야도 원칙적으로 본법에 적용이 되게 되었다. 일본 정부에 의하면 본법의 적용대상이 되는 사업자는 5000건 이상의 개인정보를 보유하는 자료 예상되지만, 이 기준에 의하면 개업 후 수년이상을 경과한 일반진료

354) 예를 들어 보건의사조산사간호사법제42조의 2), 의료방사선기술법제29조, 임상검사가사, 위생검사가사등에관한법률19조 등.

355) 불임시술 또는 인공임신중절 시행의 사무에 종사하는 자에 대해, 모체보건법27조, 장기알선기관 의사 혹은 직원에 대해 장기의 이식에 관한 법률13조, 정신장애자 지역생활지원센터직원에 대해 정신보건 및 정신장애자복지에 관한 법률50조2의 2.

소는 거의 예외 없이 동법의 적용대상이 된다.³⁵⁶⁾ 또 대체로 의료분야에 동법 적용이 문제될 때 학술 연구 분야에 대하여는 동법 제50조 제1항 제3호에 의해 개인정보보호사업자의 의무에 관한 규정을 적용하지 않지만, 일반 임상분야에 대하여는 이러한 제외규정 중에는 일반 의료기관에 관한 질문이 몇 가지 있다. 즉, 예외적으로 개인데이터를 본인으로부터 동의를 얻지 않고, 미리 특정한 이용목적을 초과하여 이용하거나, 제3자에 제공할 수 있는 경우로 타인의 생명, 신체 또는 자산 보호를 위하여 필요한 경우, 공중위생의 향상 또는 아동의 건강한 육성의 추진을 위하여 특히 필요한 경우 등으로, 각각 본인의 동의를 얻는 것이 어려울 때가 있다(동법 제16조 제3항, 제23조 제1항), 이들 규정에 해당하는 사례는 일반적인 일상의료에서도 있을 수 있다.

(3) 진료기록의 개시 및 정정

본법이 개인정보취급사업자에게 과하고 있는 개인으로부터의 개시·개정청구에 응할 의무를 의료기관에 적용함에 있어서 의료 개인정보의 고유한 문제도 충분히 배려할 필요가 있다. 우선 진료기록 등의 본인에 개시에 대해서는 2000년부터 일본 의사회 ‘진료정보제공에 관한방침’ 및 이에 준하는 각종 방침으로 전국 의료기관에서 실시되고 있으며, 사실상 일본 의료계 표준적인 행동방침이 되고 있다. 따라서 의료분야에 개인정보의 본인에의 개시는 본법에 의해 의료기관이 그 의무를 부담하지만 구체적인 개시의 방법·범위 등에 대하여는 전부 엄격한 적용을 하여 상당한 실적을 쌓고 있는 일본의사회지침을 기준으로 하는 것이 타당하다고 한다.

한편, 개인정보 개시청구에 대하여는 그 내용이 진단병명과 소견 등 의사의 의학적인 판단 사항에 관한 경우에는 이에 따르는 것이 부적절한 경우도 생각할 수 있다. 환자의 성명, 생년월일 등 단순한 오기

356) 石川高明, “医療分野における個人情報保”, 『ジュリスト』 No 1253(2003.10), 60頁.

는 고칠 수 있지만, 진료내용에 관한 기술은 진료카드가 공적인 기록이라는 성격으로 볼 때 신중한 대응이 필요하다.³⁵⁷⁾

(4) 유전자정보를 둘러싼 문제

인간 유전자에 관한 정보는 개인의 병원과 체질, 중대한 유전성병환에 관련된 정보가 포함되어 있기 때문에 그것이 개인을 특정할 수 있는 데이터와 결합된 경우, 취직 과 생명보험에의 가입 등에서의 부당한 차별에 이용될 우려가 있는 센스티브 정보라 할 수 있다. 게다가 이러한 개인의 유전자정보는 소량의 혈액 등의 시료를 채취할 수 있다면 비교적 용이하게 입수·해부할 수 있고 이러한 해석 작업과 연구는 많은 경우 개인정보보호법의 적용이 제외 되는 학술연구기관에서 하고 있는 것이고, 연구에 관한 과학자들은 형법과 특별법상 비밀준수의무를 지지 않는 자라는 것 등을 고려할 때 특별히 대책을 강구해야할 필요가 높다.³⁵⁸⁾

인간게놈지도를 해석하는 계획이 거의 성공함에 따라 현재 세계에는 10만 명 단위 규모로 보다 많은 사람들의 유전자정보를 모아 특정 질환의 치료와 예방에 기여할 계획이 세워져 있다. 이러한 연구는 반드시 사람의 미래에 많은 혜택을 줄 것이지만, 그 과정에 연구에 협력하는 사람들의 프라이버시가 침해되는 등의 피해가 있어서는 안 될 것이다.

일본 의사회는 유전자의학, 의료의 건전한 발전과 환자·被驗者의 인권을 옹호하기 위해 2003년 8월, 의사회 내에 ‘인간 유전자정보 취급에 관한 검토위원회’를 설치하였다.³⁵⁹⁾

357) 石川高明、前掲論文、61頁.

358) 이러한 점에 대하여 의회의 법안 심의 과정에서 제시된 참의원부대결의 중에서 ‘...개인정보의 보호를 위한 개별법을 즉시 검토하여 본법 전면 시행시에는 적어도 일정 구체적인 결론을 얻을 것’으로 하고 있다.

359) 이후 유전자정보 수집, 관리, 이용 등에 대하여 의학계 및 사회일반에 유용한

(5) 환자의 권리

1) 진료카드 개시청구권

진료카드에 대하여 환자에 액세스(접근)권을 보장하기 위하여 개인정보보호법에서 충분하다고 할 수 없다. 개인정보보호법이 제정된 지금도 진료카드개시의무를 지는 것은 ‘개인정보취급사업자’에 해당하는 의료기관에 한정된다. 법 제2조 제3항 본문은 ‘개인정보취급사업자’를 ‘개인정보데이터 등을 사업용으로 제공하는 자’로 정의하지만, 데이터베이스화된 개인정보가 5000건 미만의 경우에는 ‘취급개인정보의 양과 이용방법으로 볼 때 개인 권리이익을 해할 우려가 적다고’(제2조 제3항 제4호)보아 ‘개인정보취급사업자’의 범위로부터 제외하도록 하고 있다.

이렇게 ‘개인정보취급사업자’의 범위를 보면, 모든 의료기관에 대해 진료카드 개시가 법적 의무라고 말할 수 없다. 위의 개인정보데이터 건수를 세는 법을 정확히 알 수는 없지만 어느 정도 이하의 규모의 의료기관은 개인정보취급자의 범위로부터 제외된다. 또 환자 측으로부터 자신이 통원하고 있는 병원이 개인정보취급사업자라는 것을 어떤 방법으로 확인할 수 있는가 하는 문제도 있다.

따라서 모든 의료기관에서 모든 환자에게 진료개시청구권을 보장하기 위해서는 역시 진료카드 개시에 관한 개별입법이 필요하다는 지적³⁶⁰⁾이 있다.

2) 환자가족에 의한 개시청구권

유족에 의한 진료카드 개시청구를 인정할 것인가는 진료카드 등 진료정보의 활용에 관한 검토회 초기부터 계속 논의되어 왔다. 진료카

기준을 제안하였다.

360) 小林洋二, □□個人情報保護法と患者の権利□□, 『ジュリスト』 No 1253(2003.10), 62頁.

드 개시문제는 의료종사자의 저항이 강하고, 1999년에 채택된 일본의 사회의 가이드라인은 유족으로부터 개시청구를 인정하지 않는 입장을 채택하였다. 그러나 그 후 점차 의료사고의 보도 중 의료사고 재발방지를 위하여 의료의 투명성을 확보해야 한다는 목소리가 높아져, 유족에 의한 진료카드개시청구의 필요성이 인식되게 되었다. 이러한 상황 중, 일본 의사회의 가이드라인은 2002년 개정되어 유족에 의한 진료카드개시청구를 인정하도록 하고, 현재 후생노동성이 책정 중인 가이드라인도 같은 입장을 채택하고 있다. 한편, 개인정보보호법이 개인정보취급사업자에게 개시를 의무 하는 것은 어디까지나 본인에 대한 것이고, 유족에 대한 개시는 그 법률 범위 밖에 있다. 이것은 개인정보에 관한 권리가 일반에 상속 대상이 되지 않는다고 생각하고 있는 결과이다.³⁶¹⁾

3. 신용정보 분야의 과제

일본에는 크게 소비자금융, 금융기관, 판매신용 업계마다 세 가지 분야의 개인신용기구가 있다. 본법의 집행 전에는 일본에서 계속 개인신용정보 누출사건이 발생하고 있음에도 불구하고 계약에 의한 통제가 불가능한 외부자 침해행위를 방지 할 수 없었다. 위법행위에 대한 벌칙이 없는 것 등을 지적하며 형벌 적용에 의한 개인신용정보의 부정취득 등 방지와 억지가 필요하였다. 개인정보보호법에는 개인정보의 부정행위에 대하여 직접 벌칙을 적용하는 것이 아니라 간접벌을 규정하고 있다. 부정행위가 발생한 경우에 위반자들에 대하여 형벌 적용 및 위반행위의 시정이 행해지는 제도는 아니다. 또 주무대신 명령의

361) 즉 진료카드 개시문제를 ‘개인정보보호’라는 관점으로 논하는 것은 한계가 있다. 진료카드개시의 문제는, ‘개인정보보호’의 관점을 기본으로 하면서도 의료제도 전체 중에 카르텔이 부과하는 역할, 그 개시에 의한 효과 등에 배려하면서 최종적으로 개별입법에 의해 해결되어야만 하는 것이라고 지적(小林洋二, 前掲論文, 63頁).

대상이 되는 것은 제2조 제3항에 정의된 ‘개인정보취급사업자’이고, 그 외에 제3자는 대상이 되지 않는다. 이러한 본법의 태도에 대하여 개인 신용정보의 누출, 변조, 멸실 등 본인의 이익을 침해하는 행위에 대하여 보호법에는 형사죄의 적용에 의한 행위에 대하여 보호법으로는 형사죄의 적용에 의한 신속한 조치 혹은 그에 의한 미연 방지 효과를 기대하기 힘들다고 비평한다. 개인신용정보에 관하여는 그 특질에 따라 일반 개인정보보다도 엄격한 벌칙이 필요하고, 적용범위도 특별한 법적 조치가 필요하다는 견해도 있다.³⁶²⁾ 개인신용정보에 관해서는 다음의 구체적인 문제에 관하여 계속적인 논의가 있다.

(1) 정보보유자에 의한 정보의 부정제공과 부정사용

개인신용정보에 대하여는 ‘대금업규제등에관한법률’ 제30조 제2항에서 변제능력 조사 이외의 목적으로 사용해서는 안 된다는 취지의 규정이 있다. 이러한 행위는 위반행위이지만 본조 제2항은 훈시규정이 아니라 벌칙규정은 아니다. 개인정보보호법에는 외부자에 부정제공은 제23조(제3자 제공의 제한)에 위반한다고 할 수 있지만, 부정사용과 목적외사용에 관한 벌칙은 없다. 따라서 벌칙이 필요하다고³⁶³⁾ 한다.

(2) 외부자에 의한 절도, 사기, 협박 기타 부정 수단에 의한 정보 취득

1996년 일본에서 정보센터 회원업자가 약1만건의 개인신용정보를 부정하게 입수하여 타인에게 제공한 금전을 얻은 것을 발각한 사건에서 ‘정보’의 절도에 관련한 벌칙이 없어, 결국 공모자들을 사기죄 및 임대업규제법위반으로 고소·고발한 결과, 3인이 임대업규제법 부정등록위반으로 유죄판결을 받은 적이 있다. 정보사회에서 ‘정보’에 관한 벌칙적용에 현행형법에서 대응할 수 없다는 문제가 나타났다. 동

362) 平野征人, “『個人情報情報』にかかわる個別法の必要性”, 『ジュリスト』 No 1253(2003.10), 64頁
363) 平野征人, 前掲論文, 64頁.

법에도 당해 사건에 대한 해결책이 보이지 않으며 개인 신용정보는 악의의 제3자로부터의 위험에 직면하고 있다.

(3) 부정취득된 개인정보의 매매

인터넷 발달에 따라 인터넷에서 개인신용정보를 매매하는 사이트가 횡행하고 있다. 종래의 흥신소와 명부판매 가게(名簿屋)를 포함하여, 부정취득 또는 부정 제공된 정보임을 알고도 정보를 입수하고 타인에게 매매하는 자가 다수 존재하고 있다. 이러한 행위는 개인신용정보 매매의 전문 시장이 기능하고 있는 현실을 보여주는 것이지만, 이것은 부정행위에 의존하는 부정행업이다.

개인정보보호법은 이러한 영업에 대한 처벌을 실효적으로 하고 있지 않다고 비판한다.³⁶⁴⁾

(4) 부정경쟁방지법과의 관계

위에서 언급한 (1) 정보보유자에 의한 정보의 부정제공과 부정사용, (2) 외부자에 의한 절도, 사기, 협박 기타 부정 수단에 의한 정보 취득, (3) 부정취득 혹은 부정 제공된 정보와 알고 있는 정보의 입수와 그 이용·제공의 세 가지 유형 부정행위에 대하여 벌칙규정을 둘 필요성이 지적되고 있다. 그러나 일본 국회에서는 부정경쟁방지법의 일부를 개정하는 법률에서 영업비밀의 형사적 보호를 위해 처벌규정이 설정되어 지적한 개인신용정보에 대한 처벌을 담보할 수 있다고 한다.³⁶⁵⁾

364) 平野征人、前掲論文、65頁.

365) 그러나 개인신용정보는 영업비밀 요건은 ①비밀관리성, ②유용성, ③비공지성 중 비밀관리성에 대하여 정보센터 회원간에 공유된 정보이고, 오히려 정보교환을 하는 것 자체가 유용한 목적인 것, 또 본법은 전제로서 부정경쟁의 목적이 있는 경우에 부정경쟁에 의한 영업상의 이익침해. 혹은 경합 타 회사를 이용할 목적의 정보를 부정취득, 부정사용, 수정개시 하는 행위에 대하여 적용될 것으로 생각되어, 개인신용정보에는 적용될 수 없다고 한다(平野征人、前掲論文、66頁).

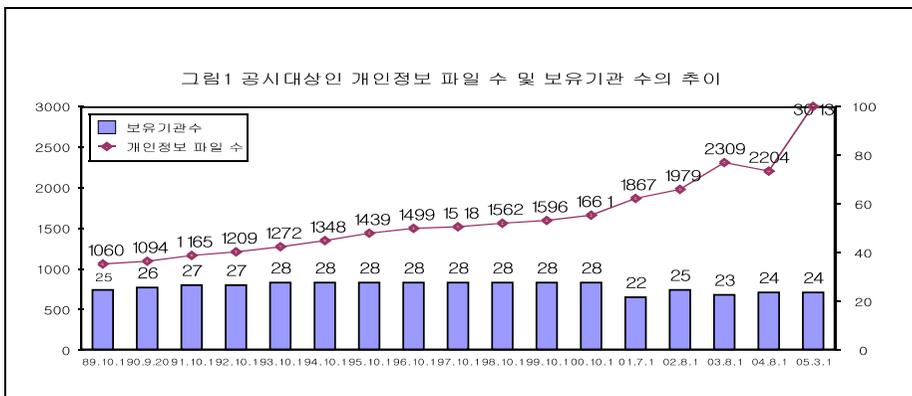
제 5 절 사후입법평가: 시행상황에 대한 점검과 평가

1. 2004년 행정기관개인정보보호법의 시행상황점검과 법률의 개정

일본은 「행정기관이 보유하는 전자계산기 처리에 관한 개인정보의 보호에 관한 법률」(1988년 법률 제95호)의 시행현황에 대한 조사가 2004년 전후로 계속 시행되었다. 이는 동 법의 시행상황을 정확하게 파악하여, 일본 국민들에게 널리 명확하게 하는 것이 조사의 목적이었다. 당시 2005년 3월 1일 기준으로 일본 총무성에서 통지하고 관보에 게재된 개인정보 파일(공시대상개인정보파일)은 24개 행정기관에서 총 3,013 개의 파일이었다.

개인정보 파일의 보유목적 이외의 목적을 위해 처리정보를 이용·제공하는 것은 법률의 규정에 근거한 이용·제공의 경우를 제외하고 원칙적으로 금지하고 있다. 2004년에 법 제9조 제2항(본인의 동의에 의한 제공 등)에 근거하여, 개인정보 파일의 보유목적 이외의 목적을 위해서 처리정보를 이용·제공하고 있는 것은, 8개 행정기관이 보유하고 있는 31개의 파일이었다.

[그림 2-4-1] 공시대상인 개인정보 파일 수 및 보유기관 수의 추이



처리정보의 공개청구에 관하여는 동법 제13조에 근거해 원칙적으로 공개한다. 2004년에는 3개 행정기관이 보유하는 5개 파일에 관해 785건의 공개청구가 있었고, 일부를 공개하지 않았던 31건(사법시험 2차 시험 파일) 및 처리 중 사안 1건(전기통신소비자상담파일)을 제외하여 공개하고 전부 공개하였다.³⁶⁶⁾

개인정보 파일의 보유목적 이외의 목적을 위해 처리정보를 이용·제공하는 것은 법률의 규정에 근거한 이용·제공하는 경우를 제외하고 원칙적으로 금지하고 있는 것은 우리나라 「공공기관의 개인정보보호에 관한 법률」 제10조의 규정과 유사하다.

「행정기관이 보유하는 전자계산기 처리에 관한 개인정보의 보호에 관한 법률」의 실시상황의 검토 후 이 법률은 「행정기관이 보유하는 개인정보의 보호에 관한 법률」(행정기관개인정보보호법)로 전면 개정되었다. 동법에서는 전자계산기로 처리되는 개인정보만을 대상으로 하고 있었던 구 「행정기관이 보유하는 전자계산기 처리에 관한 개인정보의 보호에 관한 법률」(이하 “구법”이라 함)의 대상을 매뉴얼처리 개인정보도 대상이 되기 때문에 동법 제1조에서 “본 법률은 행정기관에서 개인정보의 이용을 확대하고 있는 것을 고려하여, 행정기관에 있어 개인정보 취급에 관한 기본적 사항을 정하여 행정의 적정과 원활한 운영을 도모하기 위하여, 개인의 권리와익을 보호하는 것을 목적으로 한다”라는 표현으로 변화하였다.³⁶⁷⁾

동법 제2항(정의)에서도 구법보다 대상기관이 확대되었다. 즉, IT활용의 진전 상황에 따라, 개인정보를 보유하는 모든 행정기관을 망라하고 있다.³⁶⁸⁾

그 후 「개인정보의 보호에 관한 법률」은 주로 내각부 소관으로 하고, 「행정기관이 보유하는 개인정보에 관한 법률」과 「독립행정법인

366) 총무성행정관리국, 『2004년도행정기관 개인정보 보호법시행상황 조사결과 보고서』(2004.6), 부록의 조사결과 보고서를 참고.

367) 宇賀克也, 『個人情報保護法の逐条解説』(有斐閣, 2005), 225頁.

368) 기타 구법과 동법과의 비교는 宇賀克也, 전계서, 227면 이하를 참조.

등이 보유하는 개인정보의 보호에 관한 법률』은 주로 총무성 관할로 하고 있다.

2005년 개인정보 개시청구 건수는 행정기관 개시 65,618건, 정정 7건, 이용정지 5건. 독립법인은 개시 5,092건, 정정 6건, 이용정지 4건. 불복건수는 행정기관 개시 79건, 정정 1건, 이용정지 0건, 독립법인의 경우 개시 8건, 정정 3건, 이용정지 2건이 있었다. 개인정보 누출, 멸실, 손상이 발생한 것으로 인정된 사건은 행정기관에서는 약 75%가 오송부, 오교부, 오송신에 의한 것이다. 행정기관 320건. 독립법인 855건이 있었다.

2. 2007년 개인정보보호법의 시행상황점검

일본은 내각부를 중심으로 현행 개인정보보호법의 실시 이후에도 지속적인 시행상황을 분석하였다. 2007년에도 『개인정보의 보호에 관한 법률』(2004년 법률 제57호) 제53조 제1항(법률시행상황의 공표)의 규정에 근거하여 일본 내각총리대신은 관계 행정기관의 장에 대하여 본 법률의 시행 상황에 대한 보고를 요구할 수가 있다. 따라서 동조 제2항의 규정에 근거, 내각총리대신은 매년도 동조 제1항의 보고를 정리하여 그 개요를 공표하고 있다.

가장 최근인 “2007년 개인정보보호에관한법률시행상황의 개요”는 다음과 같다.³⁶⁹⁾

(1) 일반적 시행상황

1) 분야별 가이드라인의 검토상황(법 제8조)

2008년 3월 31일 현재 사업 등을 소관 하는 각 관할 부처별로 23개 분야에 대하여 36개의 가이드라인이 정해져 있다. 그 중 2007년 새로

369) 内閣府, 『平成10年度個人情報保護二関する法律施行状況の概要』(2008. 9).

이 정해진 것이 1개, 재검토가 이루어지고 있는 것이 3개이다.

[표 2-4-2] 2007년 제정되거나 재검토가 이루어진 가이드라인

	대상사업 분야	소관부처	가이드라인의 명칭	제정·재검토 연월일
제정	정보통신 [신서편 信書便]	총무성	신서편(信書便)사업분야에 관한 개인정보보호에 관한 가이드라인(고시)	2008년 3월 25일
재검토	의료 [일반]	후생 노동성	의료정보시스템의 안전관리에 관한 가이드라인(국장을 통한 발송)	2008년 3월 31일
	금융·신용 [금융]	금융청	금융분야에 관한 개인정보보호에 관한 가이드라인(고시)	2008년 2월 26일
	사업전반	경제 산업성	개인정보보호에 관한 법률에 관한 경제산업분야를 대상으로 하는 가이드라인(고시)	2008년 2월 29일

2) 개인정보취급사업자에 대한 주무대신에 의한 권한행사의 상황 (법 제32조~제34조)

2007년에는 각 사업분야 등을 관할하는 주무대신에 대한 개인정보보호법에 근거한 보고가 83건 이루어지는 등 사업자 등에 대한 지도·감독이 실시되었다(2006년에는 권고 4건, 보고 60건).

[표 2-4-3] 개인정보취급사업자에 대한 주무대신에 의한 권한행사의 상황

주무대신	행사한 권한		근거조문	
	보고(요구)	78건		
금융청 장관 ³⁷⁰⁾		78건	제16조 제1항 (이용목적에 의한 제한)	35건
			제19조 (자료내용의 정확성의 확보)	10건
			제20조 (안전관리조치)	66건

주무대신	행사한 권한		근거조문	
			제21조 (종업자의 감독)	18건
			제22조 (위탁처의 감독)	2건
			제23조 제1항 (제3자제공의 제한)	38건
후생노동 대신	보 고	1건	제20조 (안전관리조치)	2건
농림수산 대신	보 고	2건	제20조 (안전관리조치)	2건
			제21조 (종업자의 감독)	2건
경제산업 대신	보 고	2건	제20조 (안전관리조치)	2건
			제21조 (종업자의 감독)	2건
			제22조(위탁처의 감독)	1건
합계 ³⁷¹⁾	보 고	계 83 건	제16조 제1항 (이용목적에 의한 제한)	35건
			제19조 (정보내용의 정확성의 확보)	10건
			제20조 (안전관리조치)	71건
			제21조 (종업자의 감독)	22건
			제22조 (위탁처의 감독)	3건
			제23조 제1항 (제3자 제공의 제한)	38건

3) 인정개인정보보호단체의 인정상황 (법 제37조)

2008년 3월 31일 현재, 개인정보보호법 제37조의 규정에 근거하여 주무대신이 인정한 단체는 35개 단체이다. 그 중 2007년 새로이 인정된 단체는 1개 단체이다.

[표 2-4-4] 각 부처별 인정개인정보보호단체의 인정상황³⁷²⁾

부처명	인정단체 수 ()안은 2007년 새로이 인정된 단체 수
경제산업성	15개
금융청	10개

370) 법 제52조 및 시행령 제12조에 근거하여 내각총리대신이 금융청장관에게 권한을 위임하고 있다.

371) 공동관리 하는 사안에 대해서는 각각 계상하였다.

372) 인정단체수의 합계는 공동관리로 중복되는 것을 제외한 수이다.

부처명	인정단체 수 (안은 2007년 새로이 인정된 단체 수)
후생노동성	8개
총무성	3개
국토교통성	3개 (1개)
합계	35개

4) 인정개인정보보호단체에 대한 주무대신의 권한행사의 상황
(법 제46조~ 제48조)

2007년 각 사업분야 등을 관할하는 주무대신에 대한 개인정보보호법에 근거한 보고가 1건 이루어지는 등 인정개인정보보호단체에 대한 지도·감독이 실시되었다(2005년, 2006년에는 권한행사가 이루어지지 않았다).

[표 2-4-5] 인정개인정보보호단체에 대한 주무대신의 권한행사 상황

주무대신	행사한 권한		근거조문	
금융청장관 ³⁷³⁾	보고	1건	제43조 제2항 (개인정보지침)	1건

5) 국민생활심의회 의 논의와 정부의 협조

『개인정보의 보호에 관한 기본방침』(일부변경 전)에 의하면, ① 내각부는 법의 시행상황에 대하여 전면시행 3년 후 추가검토를 하고 그 결과에 근거하여 필요한 조치를 강구하여야 하며, ② 이에 국민생활심의회는 법의 시행상황을 추가조사(Follow up)하도록 하고 있다. 이러한 과정을 거쳐 국민생활심의회는 사업자, 민간단체, 관계부처 등으로부터 폭 넓은 의견을 청취하고 개인정보보호법의 시행상황의 평가

373) 법 제52조 및 시행령 제12조에 근거하여 내각총리대신이 금융청장관에게 권한을 위임하고 있다.

및 개인정보보호에 관한 검토를 실시하여 왔다. 2007년 6월 29일에는 지금까지의 논의를 바탕으로 『개인정보보호에 관한 종합정리³⁷⁴⁾』를 정부에 제출하였다. 그 뒤 다시 검토가 이루어졌다.

이 심의회 의견을 바탕으로 정부는 개인정보보호관계부처연락회의를 개최하고 앞으로의 개인정보보호시책의 추진에 필요한 조치에 대하여 규정한 『개인정보보호시책의 앞으로의 추진에 대하여³⁷⁵⁾』를 결정하였다.

그 후 심의회 의견 및 상기 회의결정을 바탕으로 개인정보의 보호에 관한 기본방침의 재검토 및 개인정보의 보호에 관한 법률 시행령의 개정에 대한 검토가 이루어졌고, 그 외에도 각 부처에서 정한 개인정보 보호에 관한 가이드라인의 공통화를 위한 절차에 착수하였다.³⁷⁶⁾ 또한 소위 『과잉반응』에 대한 조치로서 개인정보보호제도에 관한 적극적인 광고 및 계몽활동을 전개하였다.³⁷⁷⁾

374) 심의회의 의견서에 의한 필요한 조치의 내용 (개요)

- ① 소위 『과잉반응』에 대한 홍보 및 계몽
- ② 각 부처 가이드라인의 공통화에 대한 필요한 검토
- ③ 사업자의 자주적인 협조의 촉진 (기본방침의 재검토 등)
- ④ 시중 명부의 관리방법의 검토 (기본방침의 재검토 등 또는 정령개정)
- ⑤ 국가의 행정기관에 대한 필요한 행정운영 상의 개선
- ⑥ 방재 등의 지방의 협조에 대하여 각 시책의 담당부처에서 필요한 검토

375) 『개인정보보호시책의 앞으로의 추진에 대하여』(2007년 6월 29일 일본개인정보보호관계부처연락회의결정)의 내용 (개요)

- ① 개인정보상담네트워크의 구축 (상담번호, mail-box의 설치)
- ② 소위 『과잉반응』대응의 우수사례조사, 가이드라인의 재검토 등
- ③ 설명회 및 상담회의 실시, 포스터의 작성 및 배포에 의한 홍보 및 계몽

376) 그 후 2008년의 동향은 다음과 같다.

- ① 개인정보의 보호에 관한 기본방침의 일부변경 (2008년 4월 25일 일본내각회의결정)
- ② 개인정보의 보호에 관한 법률 시행령의 개정 (2008년 5월 1일 공포 및 시행)
- ③ 『개인정보의 보호에 관한 가이드라인의 공통화에 대하여』합의 (2008년 7월 25일, 개인정보보호관계부처연락회의)

377) 예를 들어 내각부에서는 자치회나 민생위원, 자주방해조직관계자 등 개인정보의 활용이나 보호에 관심이 높은 사람들을 대상으로 한 설명회 및 상담회를 지난 해 10월부터 12월에 걸쳐 전국 각 도·도·부·현에서 개최하였고, 이에 약 13,000명이 참가하였다.

(2) 사업자 등의 개인정보의 보호에 관한 협조상황

1) 개인정보에 관한 고충처리 상황(법 제9조, 제13조)

① 전체적 상황

2007년 지방공공단체나 국민생활센터에 의하면 개인정보에 관한 고충상담은 총 12,728건에 달하는데(2006년 총 12,876건) 그 중 소비생활센터가 접수한 것이 약 85%이다.

[표 2-4-6] 기관별 고충상담 수³⁷⁸⁾

기관		2007년		(참고) 2006년	
		수	비율	수	비율
지방공공단체	소비생활센터	10,745	84.4%	10,676	82.9%
	기타	741	5.8%	991	7.7%
국민생활센터		1,242	9.8%	1,209	9.4%
합계		12,728	100%	12,876	100%

② 분야별 상황

고충상담의 대상이 되는 사업분야는 특히 적정한 취급을 확보하여야 할 개별분야(의료, 금융·신용, 정보통신)가 전체의 약 35%를 점하고 있다. 또한 기타의 사업분야에 관한 고충상담은 50%를 점하고 있다.

378) 1. 표 중 『소비생활센터』란 PIO-NET 단말기가 설치된 소비생활센터를 말한다.

2. 표 중 『기타』란 개인정보보호조례소관부처 등을 말한다.

[표 2-4-7] 사업분야별 고충상담 수

사업분야	2007년		(참고) 2006년	
	수	비율	수	비율
특히 정정한 취급을 확보하여야 할 개별분야 ³⁷⁹⁾	4,585	36%	3,490	27.1%
의료	217	1.7%	268	2.1%
금융·신용	1,019	8.0%	1,308	10.2%
정보통신	3,368	26.5%	1,914	14.9%
기타의 사업분야	6,653	52.3%	7,601	59%
불명	1,649	13%	1,972	15.3%
합계 (중복되는 부분을 제한다)	12,728	100%	12,876	100%

③ 상담내용의 상황

상담내용은 부정한 취득에 관한 것이 전체의 약 50%로 가장 많고, 다음으로 유출 및 분실에 관한 것이 약 20%, 목적 외 이용에 관한 것, 동의없는 제공에 관한 것이 각각 20% 정도이다.

[표 2-4-8] 상담내용의 내역

상담내용	2007년		(참고) 2006년	
	수	비율	수	비율
부정한 취득	6,307	49.6%	5,315	41.3%
유출 및 분실	3,250	25.5%	3,038	23.6%
목적 외 이용	2,250	17.7%	2,006	15.6%
동의 없는 제공	2,106	16.5%	1,765	13.7%
개시 등	674	5.3%	876	6.8%
고충 등의 창구대응	345	2.7%	460	3.6%
정보내용의 착오	196	1.5%	245	1.9%

379) 2007년도 분은 각 사업분야에서 중복된 부분을 제하고 집계한 것이다(단순집계는 4,604).

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

상담내용	2007년		(참고) 2006년	
	수	비율	수	비율
opt-out위반	151	1.2%	174	1.4%
위탁처 등의 감독	30	0.2%	65	0.5%
기타	2,033	16%	2,371	18.4%
합계 (중복된 부분을 제외한다)	12,728	100%	12,876	100%

④ 처리결과에의 상황

처리결과는 지도·조언의 경우가 전체 90%에 이르고, 기타 정보제공이 약 10%에 이른다.

[표 2-4-9] 상담처리결과에의 상황³⁸⁰⁾

처리결과에의 종류	2007년		(참고) 2006년	
	수	비율	수	비율
지도·조언	11,041	86.7%	10,789	83.8%
기타 정보제공	1,053	8.3%	1,206	9.4%
타기관소개	311	2.4%	441	3.4%
알선해결	212	1.7%	267	2.1%
알선부조	13	0.1%	17	0.1%
처리불능	41	0.3%	69	0.5%
처리불요	57	0.5%	87	0.7%
불명	0	0%	0	0%
합계	12,728	100%	12,876	100%

380) 1. 표 중 『지도·조언』은 자주교섭에 의한 해결가능성이 있는 상담에 대하여 자주해결의 방법을 조언한 것을 말한다.

2. 표 중 『기타정보제공』은 알선 이외의 처리로 『지도·조언』에 해당하지 않는 것을 말한다.

2) 사업자에 의한 개인정보 유출 사안의 상황

① 전체적 상황

『개인정보의 보호에 관한 기본방침』(2004년 4월 2일 일본내각의회 결정, 2008년 4월 25일 일부변경)에서는 사업자가 개인정보유출사안이 발생한 경우 2차 피해의 방지, 유사사안의 발생회피 등을 위하여 가능한 사업관계 등을 공표하는 것이 중요하다고 한다. 이에 따라 2007년에는 사업자가 공표한 개인정보유출사안³⁸¹⁾은 총 848건이다(2005년에는 1,556건, 2006년에는 893건).

② 유출의 규모와 정보의 종류

(i) 상기 사안에서 개인정보가 유출된 자의 수(이하 「유출자」라고 한다)를 구분하여 보면 500인 이하의 사안이 전체의 약 80%를 차지하여 비교적 소규모인 사안이 많았다.

[표 2-4-10] 유출자 수³⁸²⁾

유출자 수	2007년		(참고) 2006년	
	수	비율	수	비율
500인 이하	667	78.7%	683	76.5%
501인~5,000인	104	12.3%	109	12.2%
5,001인~50,000인	60	7.1%	60	6.7%
50,001인 이상	17	2.0%	36	4.0%
불명	0	0%	5	0.6%
합계	848	100%	893	100%

381) 「유출」은 「멸실」, 「훼손」의 사안을 포함한다. 또한 각 주무대신이 파악하여 내각부에 보고한 사안에 한한다.

382) ()안은 유출 사안 전체(2007년 848건, 2006년 893건)에 대한 비율이다.

(ii) 유출된 개인정보의 종류를 고객정보, 종업원정보, 기타 정보로 분류하여 보면 대부분의 사안이 고객정보를 포함하고 있음을 알 수 있다. 유출된 개인정보의 내용을 이름, 생년월일, 성별, 주소(이하 「기본정보」라고 한다)와 그 이외의 정보(이하「부가적 정보」라 한다)로 나누어 보면 기본정보만 유출된 경우는 전체의 약 15%로 대부분의 경우 전화번호, 계좌번호, 메일주소, 신용카드번호 등 부가적 정보도 함께 유출되고 있다.

[표 2-4-11] 유출된 정보의 종류³⁸³⁾

유출된 정보의 종류	2007년				(참고) 2006년			
	수 (비율)		기본정보만 유출		수 (비율)		기본정보만 유출	
고객정보	822	96.9%	124	14.6%	867	97.1%	72	8.1%
종업원정보	48	5.7%	3	0.4%	53	5.9%	8	0.9%
기타 정보	30	3.5%	2	0.2%	27	3%	5	0.6%
합계 (중복된 부분을 제외)	848	100%	125	14.7%	893	100%	75	8.4%

③ 유출 등의 형태와 암호화 등의 정보보호조치

(i) 유출된 정보를 형태별로 나누어 보면 전자매체가 약 40%, 종이매체가 약 60%이다.

383) 1. () 안은 유출된 사안전체(2007년 848건, 2006년 893건)에 대한 비율이다.

2. 표 중 「기본정보만 유출」은 그 중 기본정보만 유출된 사안을 말한다.

(ii) 유출된 정보를 암호화 등의 정보보호조치의 유무별로 나누어 보면 별도의 조치를 취하지 않은 경우가 전체의 70%에 이른다. 반면 일부에 대하여서만 조치를 취한 것을 포함하여 어떠한 형태로든 조치를 취한 경우는 전체의 약 15%에 그치고 있다.

[표 2-4-12] 유출형태와 암호화 등의 정보보호조치³⁸⁴⁾

유출형태 암호화 등 정보보호조치	전자매체만		종이매체만		전자매체와 종이매체		불명		합계
	수	비율	수	비율	수	비율	수	비율	
전부조치	99	11.7%	0	0%	1	0.1%	3	0.4%	
일부조치	26	3.1%	2	0.2%	5	0.6%			
조치 없음	127	15%	483	57%	4	0.5%			
조치불명	61	7.2%	34	4%	3	0.4%			
합계	313	36.9%	519	61.2%	13	1.5%	3	0.4%	848

(iii) 형태별로 보면 전자매체에 의한 유출에는 정보보호조치가 취해진 것은 (일부조치를 포함한다) 약 40%이고, 정보보호조치가 취해지지 않은 것과 비슷한 정도의 비율이다. 또한 종이매체에 의한 유출 중 90%의 경우가 정보보호조치가 이루어지지 않았다.

384) 1. () 안은 유출된 사안 전체(848건)에 대한 비율이다.

2. 암호화 등의 정보보호조치란 정보의 암호화나 분실한 컴퓨터의 비밀번호에 의한 절차제한 등 정보보호를 위해 취한 조치를 말한다.

3. 『종이매체』에는 구두에 의한 유출을 포함한다(『조치불명』과 구분).

[표 2-4-13] 유출형태별 보호조치의 비율

암호화 등 정보보호조치	유출형태	전자매체만		종이매체만	
		수	비율	수	비율
	전부조치	99	31.6%	0	0%
	일부조치	26	8.3%	2	0.4%
	조치 없음	127	40.6%	483	93.1%
	조치불명	61	19.5%	34	6.6%
	합계	313	100%	519	100%

[표 2-4-14] 【참고】 2006년³⁸⁵⁾

암호화 등 정보보호조치	유출형태	전자매체만		종이매체만		전자매체와 종이매체		불명		합계
		수	비율	수	비율	수	비율	수	비율	
	전부조치	76	8%	1	0.1%	2	0.2%	2	0.2%	945
	일부조치	13	1.4%	3	0.3%	6	0.6%			
	조치 없음	186	19.7%	384	40.6%	1	0.1%			
	조치불명	111	11.7%	156	16.5%	4	0.4%			
	합계	386	40.8%	544	57.6%	13	1.4%	2	0.2%	945

- 385) 1. () 안은 유출된 사안 전체(945건)에 대한 비율이다.
 2. 본 결과는 내각부가 실시한 임의의 추가조사의뢰(2007년 12월)에 근거한 추가조사에서 각 부처가 파악한 범위의 정보에 기한 참고수치이다.
 3. 2부처에 의하여 공통으로 관리된 사안(52건)은 중복하여 계상하였으므로 합계는 『2006년 개인정보의 보호에 관한 법률 시행상황의 개요』의 수와는 일치하지 않는다.
 4. 『종이매체만』에는 구도에 의한 유출을 포함한다(『조치불명』과는 구별).

[표 2-4-15] 【참고】 2006년

암호화 등 정보보호조치	유출형태	전자매체만		종이매체만	
		수	비율	수	비율
전부조치		76	19.7%	1	0.2%
일부조치		13	3.4%	3	0.6%
조치 없음		186	48.2%	384	70.6%
조치불명		111	28.8%	156	28.9%
합계		386	100%	544	100%

④ 유출원과 유출자

(i) 유출원은 「당사자」로부터 직접 유출된 경우가 전체의 80%, 「위탁처」로부터 유출된 경우가 전체의 약 20% 이다.

(ii) 「당사자」 및 「위탁처」 중 실제로 유출에 관여한 자(이하 「유출한 자」라 한다) 는 「종업자」가 전체의 80%를 차지한다.

(iii) 유출원인을 보면 「종업자」가 유출에 관여한 경우 「의도적」인 것이 10건, 「부주의」에 의한 것이 630건으로 대부분의 경우 「의도적」인 경우였다.

[표 2-4-16] 유출원 및 유출한 자³⁸⁶⁾

유출원	종업자				제3자				기타	불명	합계
	의도적	부주의	불명	계	의도적	부주의	불명	계			
사업자	6 (0.7%)	517 (61%)	32 (3.8%)	555 (65.4%)	43 (5.1%)	1 (0.1%)	12 (1.4%)	56 (6.6%)	23 (2.7%)	13 (1.5%)	647 (76.3%)
위탁처	4 (0.5%)	113 (13.3%)	14 (1.7%)	131 (15.4%)	23 (2.7%)	5 (0.6%)	1 (0.1%)	29 (3.4%)	15 (1.8%)	5 (0.6%)	180 (21.2%)

386) () 안은 유출사안 전체(848건)에 대한 비율이다.

제 2 편 현행 개인정보보호법제에 관한 사후적 입법평가

유출한 자 유출원	종업자				제3자				기타	불명	합계
	의도적	부주의	불명	계	의도적	부주의	불명	계			
불명	-	-	-	-	-	-	-	-	-	21 (2.3%)	21 (2.5%)
합계	10 (1.2%)	630 (74.3%)	46 (5.4%)	686 (80.9%)	66 (7.8%)	6 (0.7%)	13 (1.5%)	85 (10%)	38 (4.5%)	39 (4.6%)	848 (100%)

[표 2-4-17] 【참고】 2006년³⁸⁷⁾

유출한 자 유출원	종업자				제3자				기타	불명	합계
	의도적	부주의	불명	계	의도적	부주의	불명	계			
사업자	6 (0.7%)	492 (55.1%)	5 (0.6%)	503 (56.3%)	101 (11.3%)	0 (0%)	1 (0.1%)	102 (11.4%)	4 (0.4%)	7 (0.8%)	616 (69%)
위탁처	37 (4.1%)	164 (18.4%)	1 (0.1%)	202 (22.6%)	50 (5.6%)	3 (0.3%)	2 (0.2%)	55 (6.2%)	5 (0.6%)	4 (0.4%)	266 (29.8%)
불명	-	-	-	-	-	-	-	-	-	11 (1.2%)	11 (1.2%)
합계	43 (4.8%)	656 (73.5%)	6 (0.7%)	705 (78.9%)	151 (7.8%)	3 (0.3%)	3 (0.3%)	157 (17.6%)	9 (1%)	22 (2.4%)	893 (100%)

⑤ 유출 후의 개선조치상황

(i) 유출 후의 개선조치를 보면 대부분의 경우 사업자가 어떤 방식으로든 안전관리대책을 마련하고 있다.

(ii) 안전관리대책의 내역을 보면 전체의 90%의 사업자가 교육 및 연수 실시 등 조직적인 대책을 마련하고 있다.

387) () 안은 유출사안 전체(893건)에 대한 비율이다.

[표 2-4-18] 유출 후의 개선조치상황³⁸⁸⁾

	합계	사업자에 의한 개선조치					개선조치 없음	불명
		안전관리대책			기타의 대응			
		조직적	기술적					
2007년	848 (100%)	847 (99.9%)	809 (95.4%)	789 (93%)	168 (19.8%)	827 (97.5%)	0 (0%)	1 (0.1%)
(참고) 2006년	893 (100%)	887 (99.3%)	830 (92.9%)	805 (90.1%)	140 (15.7%)	774 (86.7%)	0 (0%)	6 (0.7%)

(iii) 안전관리대책 이외의 개선상황의 내역을 보면, 전체의 80%의 사업자가 본인에게 사죄 및 연락을 하였고 40%의 사업자가 경찰에 신고하였으며 30%의 사업자가 전용창구를 설치하였다.

[표 2-4-19] 안전관리대책 이외의 개선조치 내역³⁸⁹⁾

	합계 (중복제외)	본인에게 사죄·연락	전용창구 설치	상품권 등 배부	경찰에 신고	기타
2007년	827 (97.5%)	699 (82.4%)	278 (32.8%)	26 (3.1%)	311 (36.7%)	118 (13.9%)

388) 1. 표 중『조직적』안전관리대책이란 안전관리책임자를 두고 사내규정의 정비, 교육 및 연수의 실시, 조사의 실시 등을 하는 것을 말한다.
『기술적』안전관리대책이란 방화벽(Fire wall)의 구축, 정보유출방지 소프트웨어의 도입, 개인정보의접근상황감독 등을 말한다.
『기타의 대응』의 구체적인 내용은 표 12-2 참조.
2. 『안전관리대책』과 『기타의 대응』은 복수회답.
3. () 안은 유출사안 전체(2007년 848건, 2006년 893건)에 대한 비율이다.
389) () 안은 유출사안 전체(848건)에 대한 비율이다.

⑥ 인정개인정보보호단체에 대한 보고

사업자가 인정개인정보보호단체에 소속되어 있는 경우는 208건으로 전체(848건)의 약 25% 정도이다. 또한 그 중 해당 유출을 소속된 인정개인정보보호단체에 보고한 경우는 141건으로 70%의 사안에서 인정개인정보보호단체에 보고가 이루어졌다.

3) 인정개인정보보호단체의 활동상황

인정개인정보보호단체가 개인정보보호법 제42조 및 제 43조에 근거하여 실시한 활동(고충처리, 대상사업자에 대한 설명요구, 자료요구 및 직접 작성 및 공표한 개인정보보호지침을 준수하게 하기 위한 지도, 권고 기타 조치)의 상황은 다음과 같다.

[표 2-4-20] 인정개인정보보호단체의 활동상황³⁹⁰⁾

소관부서	고충처리	설명요구	자료요구	지도	권고	기타조치
금융청	199	50	1	44	0	4
총무성	290	91	3	2	0	0
후생노동성	8	1	1	1	0	1
경제산업성	323	81	8	3	4	0
국토교통성	33	2	0	0	0	22
합계 (공동관리단체의 중복분을 제외)	542	144	10	48	4	27

390) 『기타조치』란 인정개인정보보호단체가 법 제43조에 근거하여 직접 작성 및 공표한 개인정보보호지침을 대상사업자에게 준수하게 하기 위하여 실시한 조치로서 『지도』 및 『권고』 이외의 것을 말한다.

[표 2-4-21] 【참고: 2006년의 상황】

소관부서	고충 처리	설명 요구	자료 요구	지도	권고	기타 조치
금융청	248	36	0	40	1	0
총무성	275	80	4	0	0	0
후생노동성	4	2	2	4	0	0
경제산업성	320	74	6	0	0	0
국토교통성	45	0	0	0	0	0
합계 (공동관리단체의 중복분을 제외)	577	118	8	44	1	0

(3) 지방공공단체에 의한 개인정보보호에 관한 시행상황

개인정보보호법 제11조에서는 지방공공단체는 그 보유하는 개인정보에 관하여 해당 개인정보의 성질 등을 기초로 그 정보가 적정하게 취급될 수 있도록 필요한 조치를 강구하도록 노력해야 한다고 규정하고 있다. 종래 지방공공단체는 지방공공단체가 보유하는 개인정보의 취급에 대해서 조례 등으로 규율하고 있었다. 2008년 4월 1일 현재 각 지방공공단체의 개인정보의 보호에 관한 조례의 제정상황을 살펴보면 전국 각 도·도·부·현(총 47개 단체) 및 시·도·정·촌(총 1,811개 단체)에서 이를 제정하고 있다.

3. 개인정보보호에 관한 의식조사

2007년 10월부터 12월간에 내각부, 각 도도부현, 국민생활센터 공동 개최 “개인정보보호법에 관한 설명회·상담회”(이하 설명회)를 일본 전역 47개소의 회장에서 실시하였다. 설명회의 각 회장에서는 내각부,

각도도부현의 협력을 얻어, 설명회 참가자를 대상으로 한 설문조사결과를 정리하여 “개인정보에 관한 소비자 의식 조사결과(2008년 3월 24일)”를 발표하였다.

본 내용은 설명회 참가자에 대한 설문조사결과이기 때문에 개인정보보호에 관심이 높은 사람들이 많았고, 개인정보보호법에 대한 국민 일반의 의식이 그만큼 반영되고 있지는 않다고 생각되었지만, 차후 일본의 개인정보보호시책에 참고하기 위하여 정리한 것이었다.³⁹¹⁾

(1) 개 요

국민생활센터는 전국 47도·도·부·현에서 행한 ‘개인정보보호법에 관한 설명회·상담회 참가자 12,812명을 대상으로 개인정보에 관한 설문조사를 실시하여(유효 회수 7,091, 회수율 55.3%), ‘개인정보보호법 설명참가자의 설문조사결과보고서’로 정리하였다.

(2) 조사결과 개요

1) 개인정보보호법에의 기대

- 개인정보의 안전관리책임의 강화를 기대한다 -- 3, 588명(50.6%)
- 누출을 확실히 방지하는 것이 법률로는 불가능하다고 생각한다 -- 2,661명(37.5%)

개인정보의 안전관리를 기대하는 목소리가 높지만, 법의 한계를 느끼고 있다.

2) 개인정보보호법시행 후 어떻게 바뀌었나?

- 사회전체에 개인정보에 관한 취급이 신중하게 되어 불편해 졌다 -- 4,822명(68.2%)

391) 独立行政法人国民生活センター, 『個人情報に関する消費者の意識—個人情報保護法説明会参加者へのアンケート調査結果報告書』, 2008. 3.

사회가 불편해졌다고 평가되었다.

3) 개인정보 취급에 대한 대응

- 인터넷에서 자신의 개인정보를 직접 표명하지 않는 등, 사업자에 정보제공은 필요최소한도에 그치게 된다. -- 4,064명(57.3%)
정보의 제공은 최소한에 그치게 되었다고 평가되었다.
 - 개인정보 취급에 대하여 읽은 적이 있다 -- 4, 292명(60.5%)
 - 개인정보취급에 대하여 빼 놓고 읽었다 -- 901명(12.7%)
- 개인정보 취급에 관한 내용을 읽은 적이 있는 사람이 7할에 이른다.

4) 개인정보 이용의 정지

- 어디서 자신의 개인정보를 입수했는지, 알 수 있도록 하고 싶다 --4,469명(63.0%)
 - 자신이 동의한 것에만 개인정보가 유통되게 하고 싶다. -- 4,460명(62.9%)
- 이용에서 동의확인과 유통경로 파악을 원하는 사람이 다수이다.
- 모르는 사업자로부터 상업전화와 스팸메일을 금지하고 싶다. 4,793명(67.6%)
- 특별히 상업전화에 거부감이 강하다.

5) 개시청구에 대하여

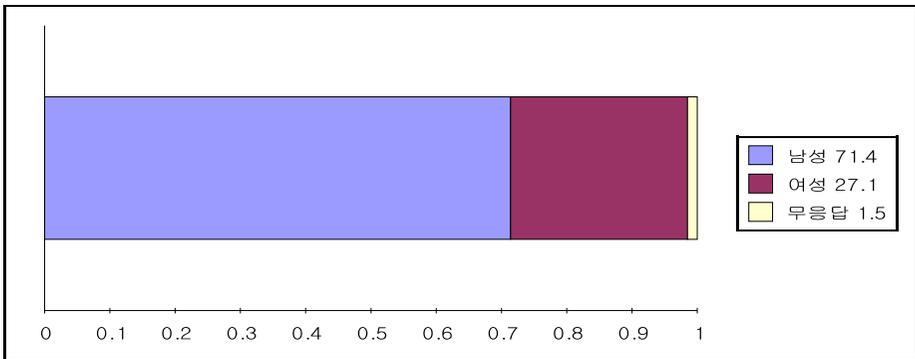
- 개시청구할 필요성이 발생하지 않는다 -- 5,965명(84.1%)
 - 개시청구하고 싶다 생각하지만, 방법을 모른다 -- 803명(11.3%)
- 청구자는 적지만 개시청구하고 싶어도 그 방법을 모르는 사람이 많다.

(3) 설문조사의 속성

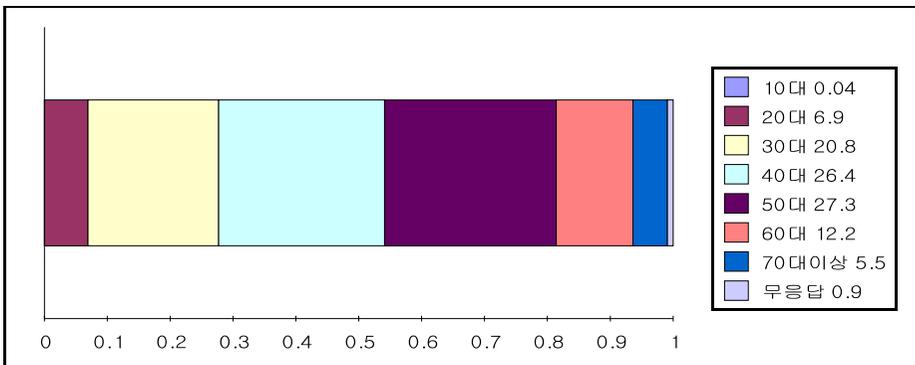
1) 응답자의 성별·연령

응답자의 성별을 보면, 남성은 7,091명 중, 5,062명이고, 전체의 71.4%이다. 여성은 1,924명(27.1%)이며, 불명·무응답은 105명(1.5%)이었다. 또, 연령별 구성을 보면, 50대가 1,933명(27.3%)로 가장 많았고, 다음으로 40대가 1,869명(26.4%)이었다. 40대와 50대가 전체 53.4%를 점유하였다.

[그림 2-4-2] 성별



[그림 2-4-3] 연령

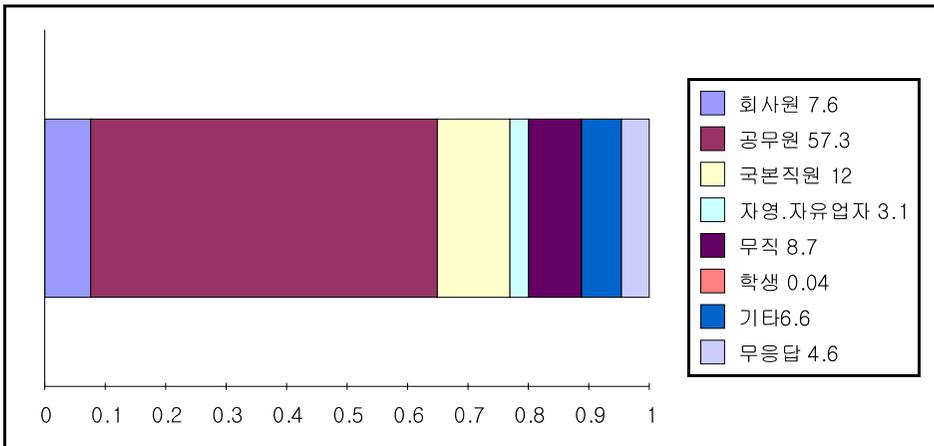


2) 응답자의 직업

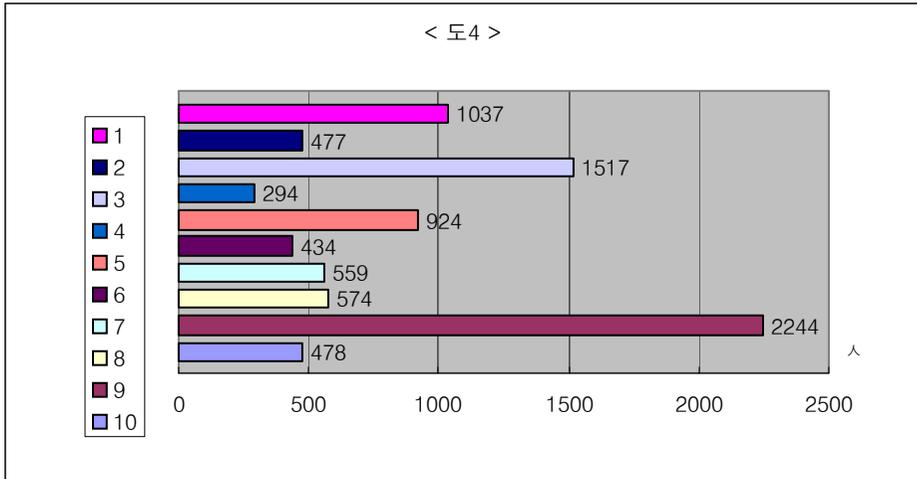
직업별 응답자의 속성을 보면, 공무원이 4,066명(57.3%)이고 반수이상을 점하고 있으며, 다음으로 단체직원 850명(12.0%)이었다. 다음으로 무직 620명(8.7%), 회사원 541(7.6%), 자영·자유업자 219명(3.1%), 학생 3인(0.04%), 기타 469명(6.6%), 무응답 323명(4.6%)이었다.

직업과 함께 관련된 단체 혹은 소속을 ① 자치회, ② 자주방재조직, ③ 학교, ④ PTA단체, ⑤ 민생위원, ⑥ 아동위원, ⑦ 일반, ⑧ 사업자, ⑨ 지방공공단체직원, ⑩ 기타 중에서 복수로 선택하게 하였고, ⑨ 지방공공단체직원(공립 교원 등도 포함)이 2,244명으로 가장 많았다. 다음으로는 ③ 학교 1,517명, ① 자치회 1,037명, ⑤ 민생위원 924명으로 이른바 과잉반응이 현장에서 일어나고 있다고 생각되는 업종의 참가자들이 눈에 띄었다고 한다.

[그림 2-4-4] 직업



[그림 2-4-5] 관련단체



[1.자치회, 2.자주방재조직, 3.학교, 4.PTA단체, 5.민생위원, 6.아동위원, 7.일반, 8.사업자, 9.지방공공단체직원, 10.기타]

(4) 개인정보보호법에 대한 의식

1) 개인정보보호법에 기대하는 것 - 안전관리를 바라는 목소리가 다수

“개인정보보호법에 기대하는 것은 무엇인가?”라는 질문에 대하여 “개인정보 안전관리 책임의 강화를 기대한다”는 응답이 3,588명(50.6%)로 가장 많고, 근소하게 “정보 누출과 악용에 대한 벌칙강화를 요구”하는 응답이 3,580명(50.5%)였다.

개인정보 안전관리와 이를 확보하기 위하여 벌칙강화에 기대하는 목소리가 높다.

또, “모르는 사업자로부터 권유전화와 스팸메일을 제한하거나, 그만 두게 하는 것”은 응답자가 3,561인(50.2%), “자신의 개인정보가 납득할 수 있는 범위 내에서 이용되는 것” 2,916명(41.1%)이고, 자신의 개인정보가 권유전화에 활용되거나 자신이 생각하지 못한 개인정보의 이용

에 대하여 혐오감을 나타내었다.

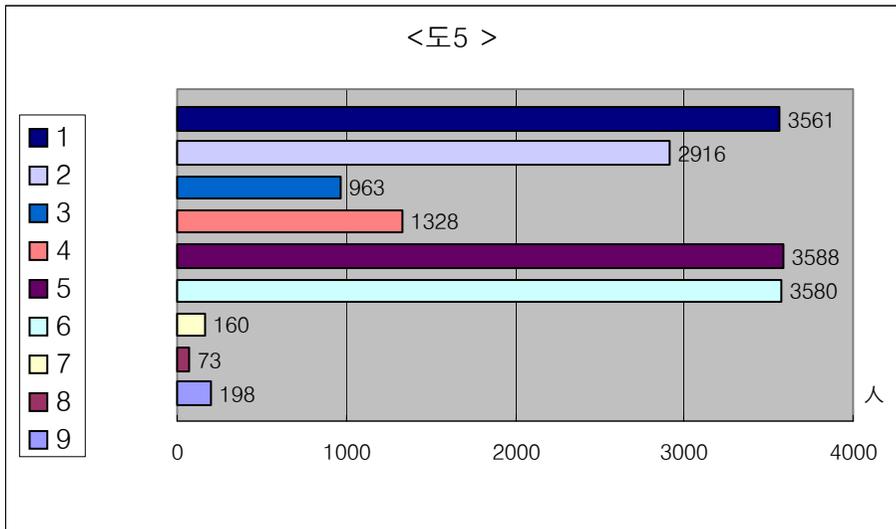
또 “기대하는 것이 없다” 160명(2.3%)으로 소수였고, 개인정보보호법에 무엇인가 기대를 갖고 있는 사람들이 많았다.

참고로 일본 개인정보보호법에서는 제20조에서 안전관리조치에 관하여 규정, 제21조에서 종업자의 감독에 관하여 22조에서 위탁자의 감독에 관하여 규정되어 있다.

<그림 5>

당신이 개인정보보호법에 기대하는 것은 무엇인가? 해당하는 것에 전부 o표시를 하시오.

[그림 2-4-6]



- [1. 모르는 사업자로부터 오는 권유전화와과 스팸메일을 제한하거나 그만두게 할 수 있는 것, 2. 자신의 개인정보가 납득할 수 있는 범위내에서 이용되는 것, 3. 자신 개인정보에 관하여 간이한 절차로 개시청구를 하는 것, 4. 사업자의 종업자에의 감독책임 강화, 5. 사업자가 보유하고 있는 개인정보의 안전관리책임 강화, 6. 정보누출과 악용에 대하여 벌칙강화, 7. 기대하지 하는 것이 없다. 8. 무응답]

안전관리에 대하여 개인정보보호법 20조에서 개인정보취급사업자는 안전관리조치를 강구하도록 정하고 있다. 설문 결과를 보면 “누출을 확실히 막는 것은 불가능하다고 생각한다.”가 2,661명(37.5%)로 가장 많았다.

사업자는 누출이 0%가 되도록 노력하는 것이 당연하지만, 만일 누출이 발생한 경우에 신속히 공표하는 등의 조치를 취하고, 소비자의 불안 해소에 노력해야만 할 것이다.

“누출문제가 발생하고 있기 때문에 법이 역할을 하지 못 한다”는 응답이 2,241명(31.2%)이며, “사업자가 빠른 대응을 하는 등 누출방지에 힘쓰고 있다”라는 평가를 하는 사람은 1,856명(26.2%)로 평가가 나뉘고 있다.

이것은 개인정보보호법 시행에 의해, 사업자측이 적극적으로 누출 사고 등을 공표하게 되고, 개인정보의 누출 사고가 사회에 알려지는 기회가 증가한 것도 요인의 하나로 들어진다.

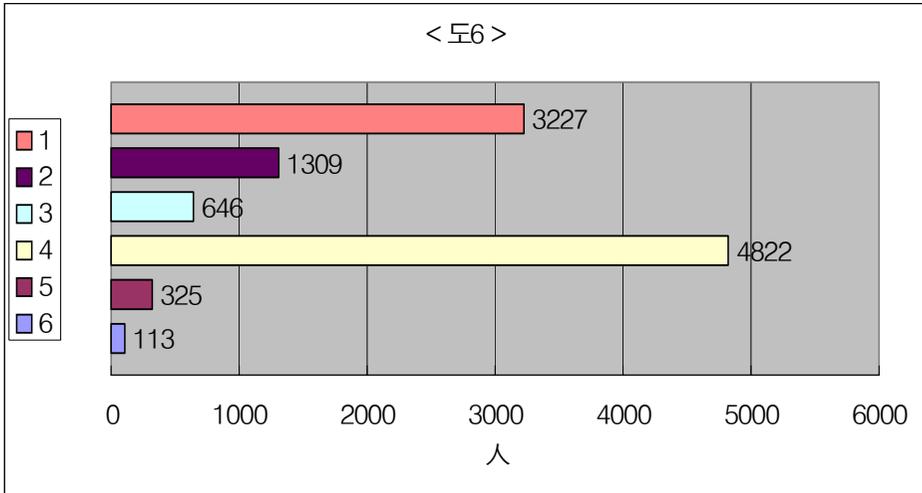
2) 법 시행 후의 변화 - 사회가 불편해졌다

개인정보보호법 시행 후의 변화에 대한 질문으로 “사회전체로 개인정보에 관한 취급이 너무 신중해져서 불편해 졌다”는 응답이 4,822명(68.0%)으로 가장 많았고, 사회전체가 개인정보의 취급에 관하여 신중하게 되었다고 느끼는 사람이 많았다.

한편, “사업자·단체의 개인정보에 관한 취급이 적절하게 되었다” 1,309명(18.5%), “사회전체의 개인정보에 관한 취급이 적절하게 되었다” 646명(9.1%)이고, 개인정보 취급이 적정하게 되었다고 느끼는 사람들은 적었고, 오히려 사회가 불편하게 되었다고 느끼는 사람들이 많은 것으로 나타났다. 또, “특히 변화가 없다”도 회답자의 325명(4.6%)이었다.

개인정보보호법이 시행되어 무엇이 변화하였는가? 해당하는 것에 전부 o표시를 하시오.

[그림 2-4-7]



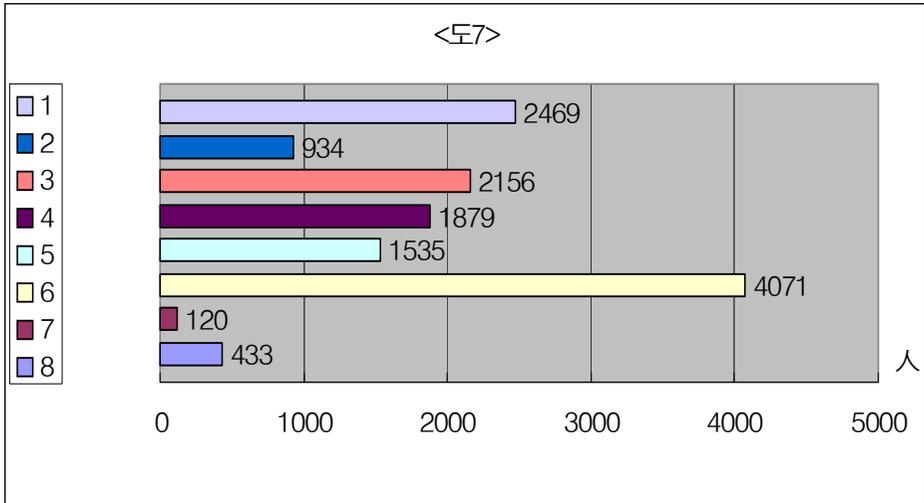
[1. 자기 자신의 개인정보에 관한 취급이 신중해 졌다, 2. 사업자·단체의 개인정보에 관한 취급이 적정하게 되었다, 3. 사회전체의 개인정보에 관한 취급이 적정하게 되었다, 4. 사회단체에서 개인정보에 관한 취급이 너무 신중해져서, 불편하게 되었다, 5. 특별히 변화가 없다고 느낀다, 6. 무응답]

3) 법 시행 후에 곤란한 것 - 무엇이든지 개인정보라고 한다

개인정보법의 시행에 수반하는 곤란한 것은 무엇인가라는 질문에는 “무엇이든 개인정보라고 한다”라는 대답이 4,071명(57.7%)으로 두드러지게 많았고, 다음으로 “명부, 연락망의 작성이 중지 되었다”가 2,469명, “업무, 사업활동이 어려워졌다” 1,879명(26.5%), “사고당시 등 긴급한 경우에도 개인정보 보호를 위해, 개인정보를 알려주지 않게 되었다” 934명 (13.2%, 이 중에는 학교 관계자가 428명으로 비교적 다수를 점하였다)이었다.

개인정보보호법이 시행되어 곤란한 것은 무엇입니까? 해당하는 것에 전부 o표시를 하시오.

[그림 2-4-8]



[1. 명부, 연락망의 작성이 중지되었다, 2. 사진·비디오 등의 촬영이 어렵게 되었다, 3. 일·사업활동의 사무절차가 번잡하게 되었다, 4. 일·사업활동이 어려워졌다, 5. 사고 등 긴급한 경우에도 개인정보보호를 위해, 개인정보를 알려주지 않게 되었다, 6. 무엇이든지 개인정보라고 말해진다, 7. 기타, 8. 무응답]

4) 권유전화와 스팸메일에 대한 의식 - 특별히 권유전화의 거부감이 강하다

권유전화와 스팸메일에 대한 의식의 물음에는 “모르는 사업자로부터 권유전화와 스팸메일은 금지시키고 싶다”4,793명(67.6%), 모르는 사업자로부터 권유전화는 금지시키고 싶지만 스팸메일을 괜찮다” 1,021명(14.4%)로 두 답변을 합치면 80%가 넘는 사람이 자신이 모르는 사업자로부터 권유전화 전화를 금지시키고 싶어 했다.

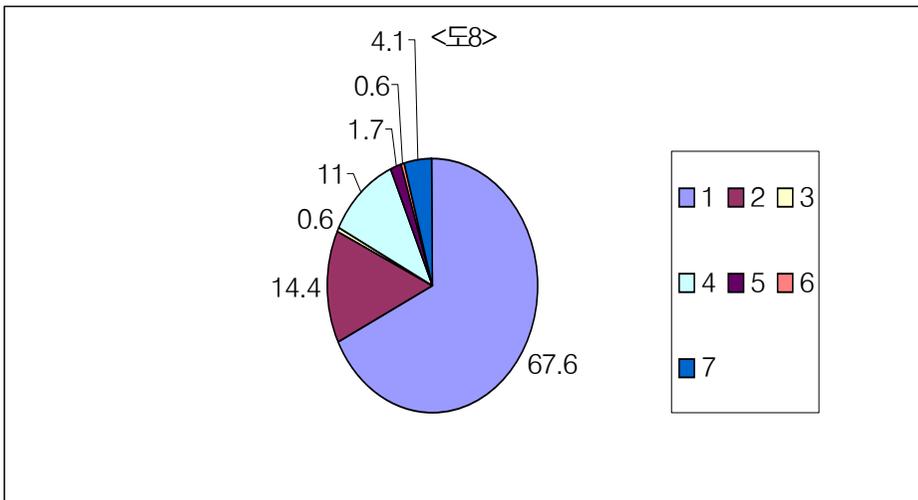
한편, “모르는 사업자로부터 권유전화는 괜찮지만, 스팸메일은 금지시키고 싶다”는 대답은 40명(0.6%)으로 매우 작았고,

전화를 받지 않으면 어떤 내용인지 알 수 없는 권유전화에 대한 거부반응이 스팸메일보다 강하다는 결과가 나타났다.

또, “알지 못하는 사업자로부터 권유전화와 스팸메일이 앞으로 금지할 수 있다면 와도 상관없다” 782명(11.0%)이고, 약1할의 사람들은 거부권이 있다면 권유전화와 스팸메일이 있어도 상관없다고 했다. 그러나 거부권이 없이, 무조건으로 “알지 못하는 사업자로부터 권유전화와 스팸메일이 와도 상관없다”고 한 응답은 122명(1.7%)로 전체에 비해 아주 근소한 숫자였다.

권유전화와 스팸메일에 대해 어떻게 생각하는가? 해당하는 것 한개에 o표시를 하시오.

[그림 2-4-9]



[1. 모르는 사업자로부터 권유전화 전화와 스팸메일은 금지시키고 싶다, 2. 모르는 사업자로부터의 권유전화는 금지시키고 싶지만 스팸메일을 괜찮다, 3. 모르는 사업자로부터 권유전화는 괜찮지만, 스팸메일은 금지시키고 싶다, 4. 모르는 자로부터 권유전화와 스팸메일이 앞으로 거부할 수 있다면, 와도 상관없다, 5. 모르는 사업자로부터 권유전화와 스팸메일이 와도 상관없다, 6. 기타, 7. 무응답]

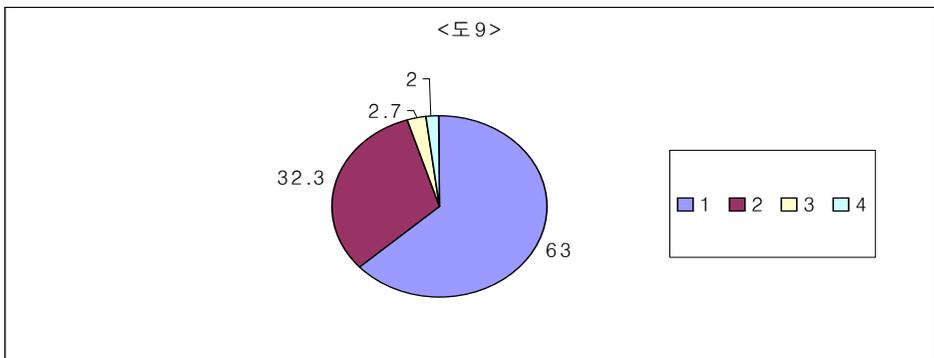
5) 정보의 유통 경로 - 유통경로의 파악을 원하는 목소리가 높다

설문조사의 결과를 보면 “어디에서 자신의 개인정보를 입수하였는가, 알고 싶다”가 4,469명(63.0%), “어디에서 자신의 개인정보를 입수했는가 알고 싶지만, 알기 어렵다고 생각한다”는 회답이 2,288명(32.3%)이며, 약 9할의 사람들이 자신의 개인정보 유통경로를 파악하고 싶어한다. 단, 개인정보보호법으로도 개인정보 유통경로를 파악하는 것은 매우 곤란하다. 개인정보의 유통경로를 파악하기위한 방법으로는 보유개인정보데이터의 개시(동법 25조)가 고려되지만, 개인정보취급사업자가, 보유개인데이터로 당해 개인정보의 유통경로를 기재하지 않으면 개시 대상이 되지 않는다.

사업자 중에는 개인정보 입수처 등을 알려주는 경우도 있다. 고객 등의 의문에 부응하기 위해서는 무엇보다 입수한 개인정보를 이용하는데 있어 사업자는 적극적으로 개인정보의 입수원을 알려줄 것(예를 들어 ...주식회사로부터 제공 입수하였다)이 요구된다.

개인정보보호법에서 사업자 등에 대하여 자신의 개인정보를 어떻게 입수하였는지 묻는 것이 곤란한데, 이에 대하여 어떻게 생각하는가? 해당하는 것에 1개의 o를 표시하십시오.

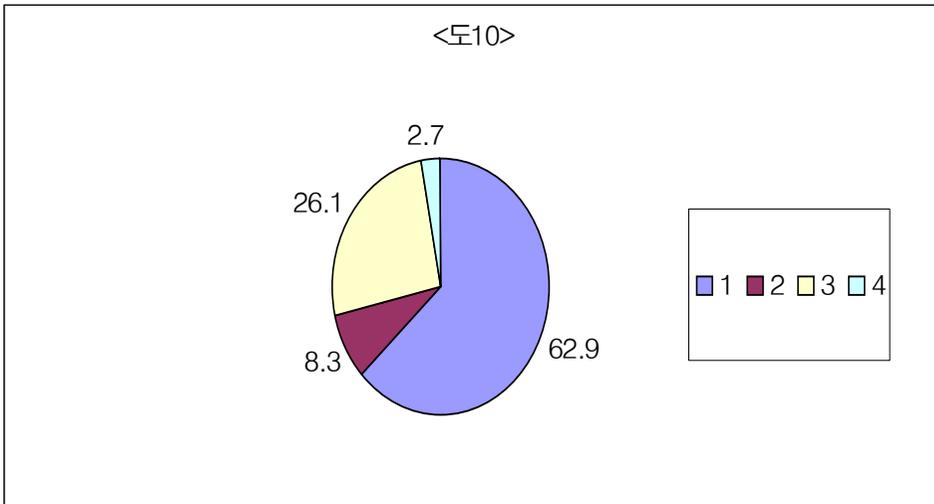
[그림 2-4-10]



[1. 어디서 자신의 개인정보를 입수하였는지 알고 싶다, 2. 어디서 자신의 개인정보를 입수했는지 알고 싶지만 어려울 것으로 생각한다, 3. 특별히 생각한바 없다, 4. 무응답]

자신이 모르는 곳에서 동의 없이 자신의 개인정보가 유통하는 것에 대하여 어떻게 생각하는가? 해당하는 것에 한 개의 o를 표시하시오.

[그림 2-4-11]



[1. 자신이 동의한 곳에만 개인정보가 유통되기를 원한다, 2. 개인정보의 유용성으로 보아 동의 없어도 개인정보의 유통은 특별히 문제되지 않는다, 3. 유통은 상관없지만, 자신의 의사에 의해 이용정지할 수 있도록 하고 싶다, 4. 무응답]

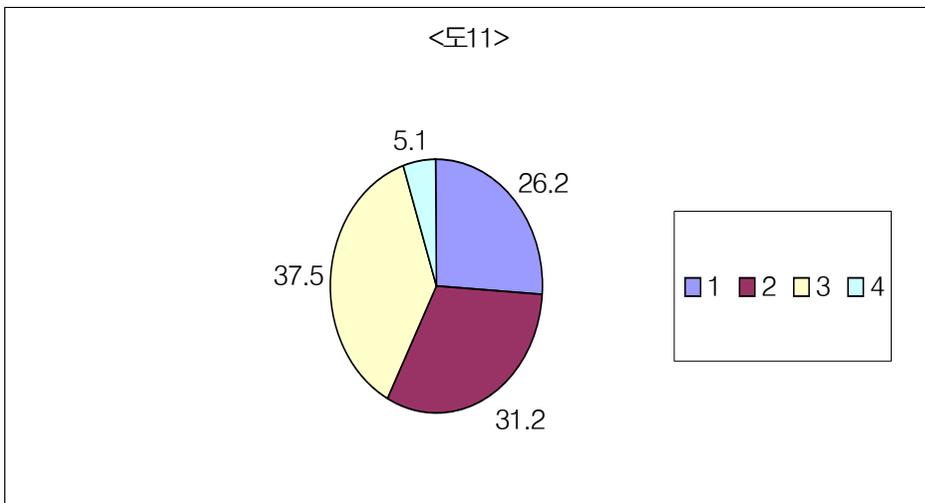
6) 개인정보의 누출 - 법의 한계를 느낀다

개인정보 누출과 개인정보보호법의 역할에 대한 질문으로 “본래, 누출을 확실히 방지하는 것은 법률로는 불가능하다고 생각한다” 2,661명(37.5%)와 법률에 의한 대처의 한계를 느끼고 있는 사람이 매우 많다. “누출문제가 여전히 발생하고 있기 때문에, 효과가 없다”고 느끼고 있는 사람은 2,214명(31.2%)인 반면, “사업자가 빠른 대응 등 누출 방지

에 힘쓰고 있다”고 일정한 평가를 하고 있는 사람이 1,856명(26.2%)로 4분의 1을 넘고 있고, 개인정보보호법과 누출의 문제에 대하여는 다수의견이 갈리고 있다. 이렇게 의견이 갈리고 있는 것은, 개인정보보호법의 시행에 의해, 사업자측이 적극적으로 누출 사고 등을 공표하게 되어, 개인정보의 누출사고가 사회에 알려지는 기회가 늘었다는 것도 한 요인으로 들 수 있다.

개인정보 누출문제에 대하여, 개인정보보호법이 제대로 기능을 하고 있다고 생각하는가? 자신의 생각한 것에 한 개의 o표시를 하시오.

[그림 2-4-12]



[1. 사업자가 재빠른 대응을 하는 등 누출방지에 힘쓰고 있다, 2. 누출문제가 여전히 발생되고 있기 때문에 효과가 없다, 3. 본래 누출을 확실히 방지하는 것이 법률로는 불가능하다고 생각한다, 4. 무응답]

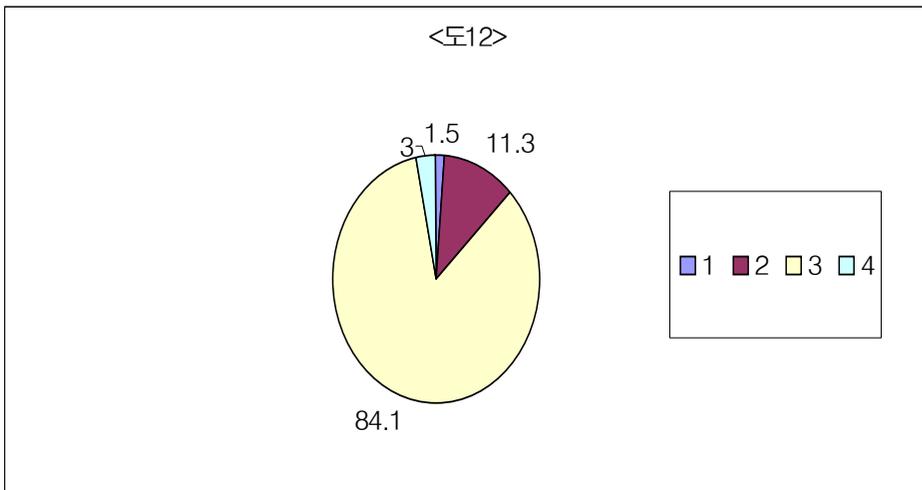
7) 개인정보 개시청구 - 청구하는 사람이 적다

개인정보보호법상은 법25조에 의해, 보유개인데이터라면, 개시청구를 할 수 있다. 여기서 실제로, “개인정보보호법에 근거하여 개시청구

를 한 적이 있는가라는 질문에 “개시청구 할 필요가 없다” 5,965명 (84.1%)로 대다수의 사람들이 실제 개시청구를 할 필요성이 없다고 했다. 그러나 남은 약 16% 중에 “개시청구한 적이 있다”는 회답자는 107명(1.5%)으로 근소하고, 대부분은 “개시청구하고 싶지만 방법을 모른다” 803명(11.3%)이었다. 앞으로는 사업자가 어떠한 개인정보를 보유하고 있는가를 소비자가 파악하기 위하여도 구체적인 개시청구 방법을 주지할 것이 요구된다. 개인정보보호법에 근거 자신의 정보에 대하여 개시청구를 한 적이 있는가?

해당하는 것 1개에 o표시를 하시오.

[그림 2-4-13]



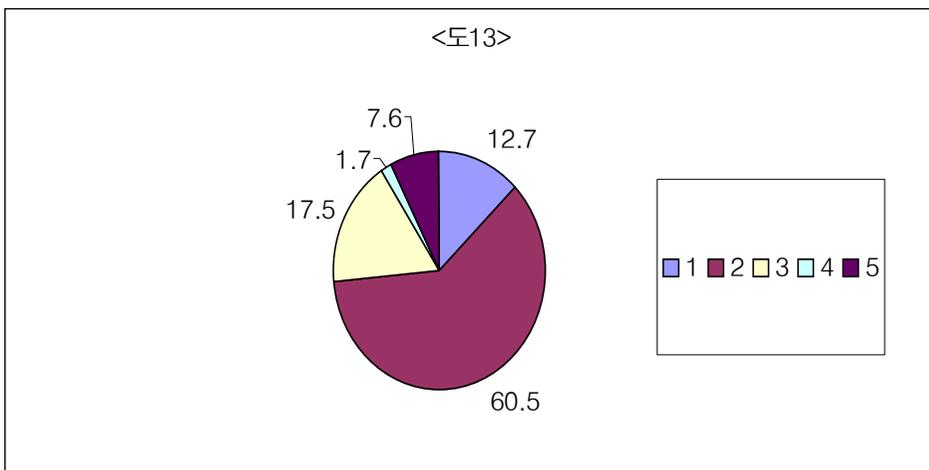
[1. 개시청구한 적이 있다, 2. 개시청구하고 싶지만, 방법을 모른다, 3. 개시청구 할 필요성이 생기지 않는다, 4. 무응답]

8) 개인정보에 관한 기재사항 - 읽은 적이 있는 사람이 7할을 넘어 계약서 등에 기재 되어 있는 “개인정보 취급에 대하여”등을 “빠짐 없이 읽는다”고 하여 개인정보 취급에 관한 의식이 높은 사람이 901

명(12.7%)인 반면, “읽은 적이 없다”가 1,239명(17.5%)이 었다. 또 “그런 항목이 있는 것 자체를 몰랐다”는 121명(1.7%)로 극소수였고, 어떠한 형태라고 파악하고 있는 사람이 다수였다는 결론이었다. 또 “읽은 적이 있다”고 한 응답은 4,292명(60.5%)이고, “빠짐없이 읽는다”와 합쳐 7할을 넘는 사람들이, “개인정보 취급에 대하여”등의 기재를 읽는 것이 있다는 결과였다. 또 “빠짐없이 읽는다”와 “읽은 적이 있다”는 회답자에 내용이 어느 정도 이해할 수 있는가 하는 질문에 “잘 이해한다” 343명, “대체로 이해한다”가 1,229명, “전혀 모르겠다”가 22명이기 때문에 사업자에는 소비자에게 보다 이해하기 쉬운 “개인정보 취급에 대하여”등의 기술에 관한 표현 등에 대해 연구할 것이 요구되고 경우에 따라 정중하게 설명해야 한다.

계약서등에는 “개인정보 취급에 대하여”등이 기재 되어 있는 항목이 있고, 개인정보 이용목적, 제3자제공 등에 대하여 상세히 쓰여 있는 것도 있지만, 읽은 적이 있는가? 해당하는 것에 o표시 하시오.

[그림 2-4-14]



[1. 빠짐없이 읽는다, 2 읽은 적이 있다, 3. 읽은 적이 없다, 4. “개인정보 취급에 대하여”등의 항목이 있는 것 자체를 모른다, 5. 무응답]

4. 개인정보보호법의 시행에 대한 평가

2007년 6월 29일 국민생활심의회에서는 ‘개인정보보호에 관한 종합 정리³⁹²⁾’에서의 개인정보보호법에 대한 평가는 현황, 과제, 향후 검토 과제를 통하여 본법의 시행상황을 검토하고 문제점으로 논의되는 과제를 제시하고, 향후 개인정보보호 사업의 추진 방향을 검토하고 있다. 그 내용은 다음과 같다.

(1) 국민의식과 사업자의 상황평가

앞의 ‘개인정보보호에 관한 여론조사’(2006년 9월 내각부 조사, 이하 ‘여론조사’라 함)에 의하면, 개인정보보호에 관한 의식과 관심이 높아졌음을 느끼는 자가 약 4분의 3, 민간사업자와 행정기관에서 개인정보보호 활동을 하고 있는 것을 느끼는 자가 약 7할이 된다. 또, ‘개인정보의 보호에 관한 사업자의 대응실태조사’(2008년 3월 내각부 조사, 이하 ‘대응실태조사’라 함)에 따르면 개인정보보호에 관한 전 조직적 책임담당부서를 설치하고 있는 사업자와, 프라이버시 폴리시³⁹³⁾ 등을 책정·공표하고 있는 사업자가 각각 5-6할이 되고 있다.

이러한 조사결과에서 보듯이 일본에서는 개인정보보호법이 전면 실시되어 개인정보보호에 관한 국민의식이 높아지고 동시에 사업자의 대응도 진척되고 있다고 하겠다.

한편, 여론조사도 자기가 예기하지 않는 목적으로 개인정보가 이용되고 있는 것이 아닌가? 모르는 사이에 개인정보가 타인에 제공되고 있는 것은 아닌가? 하며 개인정보 취급에 불안감을 느끼는 사람이 각각 7할이나 되어 국민의 개인정보 취급에 대한 불안감은 매우 높다고

392) 第21次国民生活審議会個人情報保護部会, 『個人情報保護に関する取りまとめ(意見)』(国民生活審議会, 平成19年6月29日).

393) 사업자 개인정보보호에 관한 생각과 방침에 관한 선언.

평가 된다.

기본방침에서 사업자는 개인정보의 누출 등의 사안이 발생하는 경우 가능한 사실관계 등을 공표하는 것이 중요하다. 따라서 2005년에는 사업자들이 1,556건의 누출 사안이 발생하였고 여론조사결과에도 영향을 미친 것으로 보인다. 이러한 사안에는 종업자가 관계하고 있는 경우가 많고, 개인정보의 누출방지 등을 위해 지속적으로 종업자의 감독·교육이 필요한 상황이다.

또 대응실태조사에 의하면, 개인정보보호법상 본인의 동의가 없어, 학교와 지역사회와 긴급연락망 등의 명부 작성이 중지되고, 일상생활이 불편하게 되었다고 느끼는 사람이 5할이 되고 있다. 심의회에서 실시한 청취회에서도 지적된 것이지만, 이러한 조사결과와 같이, 동법 등에 대한 오해에 기인하여 필요한 개인정보의 제공까지도 제공하지 않는다거나, 각종명부 작성이 중지되는 등, ‘과잉반응’이라는 상황도 일부 보인다.

(2) 정부 등의 대응상황

개인정보보호법은 국가와 지방자치단체, 인정개인정보보호단체에 대하여, 기본방침에 근거하여 개인정보의 보호를 위한 조치를 강구하도록 요구하고 있다.

일본은 소관성청에서 2007년 5월 31일, 22분야에서 35개 가이드라인을 책정하고, 사업자에 대하여 지도·감독을 하는 외에, 총 34단체를 인정개인정보보호단체로서 인정하고 있다. 또, 내각부 및 각 성청은 사업자 및 국민에 대하여 다양한 매체를 사용하여 개인정보보호제도의 홍보·교육에 힘쓰고 있다. 지방자치단체와 국민생활센터에서는 개인정보에 관한 고충상담을 위한 체제를 정비하고, 2005년에 14,028건의 고충상담을 받고 지도·조언 하는 등, 원활한 고충처리에 힘쓰고 있다.

(3) 과잉반응의 문제

1) 현 황

개인정보보호법 제23조1항에서 개인정보취급사업자는 원칙적으로 사전에 본인의 동의를 얻지 않고 개인데이터를 제3자에게 제공해서는 안 된다고 규정하고 있다.

단, 사회공공의 이익과 타 권리이익의 보호를 우선해야 하는 경우로 ① 법령에 근거한 경우, ② 타인의 생명·신체 또는 재산 보호를 위하여 필요가 있는 경우로 본인의 동의를 얻는 것이 곤란할 때, ③ 공중위생의 향상 또는 아동의 건전한 육성을 위하여 특히 필요가 있는 경우로 본인의 동의를 얻는 것이 곤란할 때, ④ 국가 기관 혹은 지방 공공단체 또는 그 위탁을 받은 자가 법령에 정한 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로 본인의 동의를 얻으면 당해사무의 수행에 지장을 미칠 우려가 있을 때에는 본인의 동의 없이도 제공할 수 있도록 하고 있다.

개인정보보호법제23조제2항에서 개인정보취급사업자는 본인의 요구에 따라 제공을 정지하는 경우 제공된 개인데이터에 대하여 일정 사항을 사전에 본인에게 통지 등을 할 때에 본인으로부터 동의를 얻을 수 없어도 당해 개인데이터를 제3자에 제공할 수 있는 것으로 하고 있다.

총무성은 지방공공단체에 대하여 개인정보보호법 및 행정기관이 보유하는 개인정보의 보호에 관한 법률의 규정 취지에 따라 개인정보보호조례를 미제정한 지자체(시정촌)에게 긴급히 조례제정에 힘쓸 것과 이미 조례를 제정한 단체도 ‘행정기관에관한개인정보보호법’의 내용에 따라 적당한 검토를 하도록 통지하고 있다(2005년 6월 16일 총무성정책총괄관통지).

이른바 ‘과잉반응’의 예로 들고 있는 名簿문제는 다음과 같은 사례가 있다.

① 재해시 要援護者리스트 작성

재해시요원호자리스트 작성에 대해 내각은 2006년 3월 ‘재해시요원호자의 피난지원 가이드라인’을 책정하여 각 지방공공단체에 알리고 있다. 또 2007년 4월 요원호자대책의 구체적인 추진과 방책의 예를 정리하여 지방자치단체에 통지하고 있다.

개인정보에 의해 식별될 특정의 개인정보 수가 5,000을 넘는 자주방재조직은 많지 않기 때문에 직접적으로 개인정보보호법상의 문제는 없다고 생각된다.

② 민생위원·아동위원의 활동을 위한 대상자명부

민생위원·아동위원은, 민생위원법(1947년법률제198호) 및 아동복지법(1946년법률제164호)에서 주민생활 상태를 필요에 따라 적절히 파악하면서 상담에 응하여 조언·원조 등을 하도록 하고 있다.

민생위원·아동위원이 그 활동을 원활히 하기 위하여 후생노동성에서 각 지방공공단체에 대하여 동위원에 개인정보의 제공의 적절한 대응을 요청하고 있다.

또 민생위원·아동위원은 특별직 지방공무원으로서 다양한 생활과제의 해결을 위하여 원조가 필요한 지역주민의 정보를 관계기관 등과 공유하면서 활동한다. 이 때문에 개인정보취급사업자로부터 직무 수행에 필요한 정보제공을 받은 경우 국가 등에 협력하는 필요가 있는 경우에 본인으로부터 동의를 얻지 않고도 제공하는 것이 가능하다고 생각된다.

③ 자치회명부

자치회에 대하여 5000을 초과한 자로 구성된 조직은 적기 때문에, 개인정보보호법의 의무 대상인 ‘개인정보취급사업자’에 해당하는 경우는 많지 않다.

④ 학교의 긴급연락망 등

학교의 긴급연락망과 주소록 등의 작성에 대하여 문부과학성은 ‘학교에서 학생에 관하여 개인정보의 적정한 취급을 확보하기 위하여 사업자가 강구해야만 하는 조치에 관한 지침’(2004년 11월 11일 문부과학성)의 해석을 2006년 2월에 개정하여, 미리 학생들로부터 동의를 얻는 절차를 알리는 방법이 강구되었다.

2) 개선과제

개인정보보호법 등이 전면 실시되고 있고 동법 등에 대하여 오해에 기인하여 필요한 개인정보 제공까지 이용할 수 없게 되어 각종명부의 작성이 주지되는 등, 과잉반응 현상도 일부 보인다고 평한다.

프라이버시 의식이 높아져 공공단체에서 공지·방재의 담당부국과, 민생위원과 자주방재조직등과의 요원호자정보의 공유가 되지 않고, 민생위원 활동을 원활히 할 수 없게 되었다고 지적되었다.

3) 본인의 동의를 얻지 않고 제공할 수 있는 경우의 추가를 둘러싼 논의

① 전반적 사항

이른바 ‘과잉반응’에 대하여 가이드라인에서 적절한 방안을 정한다면 개선가능한 것으로 보이지만 현행법에서 대응할 수 없는 문제가 생기고 있다면 법령상 해결방법도 검토해야만 한다.

전체적으로 볼 때, 이른바 ‘과잉반응’은 가라앉고 있고, 지금 까지 일본전체가 개인정보 취급에 둔감하였기 때문에 이른바 ‘과잉반응’이 생기고 있는 것으로서 우선 현행 개인정보보호법이 정착되어야 한다고 평가 한다.

② 목적의 명확화

이른바 ‘과잉반응’에 대응하기위하여, 개인정보보호법에서 개인정보의 유용성에 배려할 취지를 가능한 한 구체적으로 규정해야 한다.

③ 이익형량제도

본인의 동의를 얻지 않고 개인 데이터를 제공할 수 있는 경우로서 일반적인 이익형량규정을 추가하면 어떤가?

- 일반적인 이익형량규정을 추가하면, 개인정보의 보호와 이용의 균형이 무너진다.
- 일반적인 이익형량규정을 추가하면, 개인정보의 취득원의 개시 의무화 등에 본인의 권리강화도 함께 조치해야만 하는 것이 아닌가?

④ 법령에 근거한 경우

- 본인의 동의를 얻지 않고 개인데이터를 제공할 수 있는 경우로 ‘공적 관행으로 취급 되는 것’을 추가할 수 있는가?
- ‘공적 관행으로 취급 되는 것’이라는 생각은 정부의 설명책임의 문제로 민간사업자의 규율에 추가하는 것은 부적당하다.

⑤ 타인의 생명, 신체 또는 재산의 보호에 필요한 경우

- 본인의 동의를 얻지 않고 개인데이터를 제공할 수 있는 ‘타인의 생명, 신체 또는 재산의 보호를 위하여 필요한 경우’(개인정보보호법제23조 제1항2호)에서 ‘안전’과 ‘생활’을 추가해도 좋은가?

⑥ 국가, 지방자치단체 또는 그 위탁을 받은 자에 협력할 필요가 있는 경우

- 나라 등에 협력할 필요가 있는 경우에 관하여, 공익에 관한 업무로, 소장사무의 수행상 필요한 경우와, 권리이익침해의 우려가 없는 경우에는 본인의 동의를 얻지 않고 개인데이터를 제공할 수 있는 경우로서 명기하면 어떤가?
- 국가 등에 협력할 필요가 있는 경우에, 독립행정법인 등에의 협력을 추가하면 어떨까?
- ‘그 위탁을 받은 자’의 범위가 불명확하다.
- ‘그 위탁을 받은 자’의 범위는 해석과 운영상 명확하면 족하다.

⑦ 조례와의 관계

- 지방공공단체의 조례 중에는 ‘행정기관개인정보보호법’상 보유개인정보를 목적 외 제공할 수 있는 경우로 상당한 규정이 없는 것도 있어 이른바 ‘과잉반응’이 발생하는 측면도 있다. 조례의 재검토도 포함한 지방공공단체의 탄력적인 대응을 추진하기 위하여 개인정보보호법의 근본적인 부분을 재평가 하여야 한다.

4) 향후의 검토방향

일본 정부는 2006년 2월에 ‘개인정보보호관계성청연락회의’에서 국민 및 사업자에 대하여 개인정보보호제도의 주지철저를 도모하면서 개인데이터를 제3자에 제공할 수 있는 경우를 사례에 따라 명확화 하는 등 대응을 한층 강화하려 한다.

① 개인정보보호법의 오해에 의한 개인정보 제공거부

이러한 경우에는 관련성청 합의에 따라, 내각부는 개인정보보호법의 해석과 운용기준을 명료화하고, 관련성청은 분야마다 가이드라인과 그 해석 등의 필요에 따른 재검토 등을 하면서 이를 국민에게 주지시

키도록 하고 계속적으로 이러한 대응을 추진할 필요가 있다.

② 본인의 동의 취득에 의해 작성 가능한 것

개인정보보호법제상 본인의 동의가 있으면 개인정보를 제공할 수 있다. 그러나 프라이버시의식이 높아진 이유로 본인이 게재를 거부하거나 절차의 부담감 등으로부터 다양한 명부를 종래와 같이 작성하는 것이 곤란한 경우가 생긴다.

이러한 상황에 따라 우선 명부의 작성·배포의 절차 등 개인정보보호법의 구체적인 내용에 대하여 홍보 교육을 하는 것이 중요하다.

개인정보보호법 제23조 제1항에서, 사업자는 개인데이터의 제3자제공시에 원칙적으로 사전에 본인의 동의를 얻게 되지만 법령에 근거한 경우와 타인의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우에 본인의 동의를 얻지 않고도 제공할 수 있다. 이 때문에 개인정보의 유용성을 배려하고, 개인의 권리의익을 보호할 수 있다는 규정을 적절히 운용할 것이 요구된다.

이러한 규정에 해당하지 않는 경우에도 동의를 얻지 않고 개인정보를 제공하는 것이 적당한 경우가 있는가에 대하여, 실태를 충분히 지켜보면서 계속 검토할 필요가 있다. 그러나 여론조사로도 안전관리가 불충분하여 개인정보가 누출되고 있는 것은 아닌가? 모르는 사이에 개인정보가 타인에 제공되고 있는 것은 아닌가? 라고 개인정보취급에 대하여 불안을 느끼는 자가 각각 8, 7할에 이르고 있는 점에도 유의가 필요하다.

개인정보보호법 제11조에서 지방공공단체는 그 보유 개인정보의 적정한 취급이 확보되도록 필요한 조치를 강구하고, 현재 모든 도도부현 및 시정촌에서 조례가 제정되어 있다. 지방공공단체에게는 관계기관 등에서 정보공유가 곤란하게 된 경우에도, 행정기관개인정보보호법을 참조하여 조례의 적절한 해석·운용 등과 주민에 대하여 개인정

보호법 취지에 다른 홍보 계몽을 할 필요가 있다.

(4) 보호대상과 의무의 대상

1) 현 황

① 개인정보보호법에서 모든 개인정보를 같이 취급하는 것에 대하여

현행 개인정보보호법 제2조 제1항에서 ‘개인정보’란 생존하는 개인에 관한 정보이고, 특정 개인을 식별할 수 있는 것으로 하고 있다.

개인정보보호법에서 보호의 필요성과 의무의 이행가능성 등의 관점에서 개인정보, 개인데이터 및 보유개인데이터를 구별하고 있다. 외국에도 자동처리 되거나 파일로 관리되는 데이터가 보호의 대상이지만 나라에 따라 약간 차이가 있다. 이를 감안하여 ‘개인정보’의 정의 등에 대하여 국제적인 적합성의 관점에서 정비하는 것이 타당하다고 한다.

② 특별한 조치

‘개인정보의 성질 및 이용방법을 고려하여, 개인의 권리이익이 한층 보호되도록 적절한 취급이 필요한 개인정보’(개인정보보호법제6조)에서 의료, 금융·신용, 정보통신등의 각 분야에서 관련법에 의해 비밀 준수 의무, 규칙과 가이드라인에 의한 엄격한 안전보장조치 등이 규정되어 있다. 특히 개인신용정보에 대하여 2006년 12월 개정·공포된 대금업법에 의해 대금업자에 의한 목적외이용을 벌칙 대상으로 하는 등의 조치가 강구되고 있다.

2) 향후의 검토방향

특히 적절한 취급을 확보해야만 하는 개별분야에서 기존 업법에 의한 준수 의무, 규칙과 가이드라인에 의한 엄격한 안전관리조치 등에 의해 특별 조치가 강구되고 있기 때문에 계속적으로 현행 제도 하에

서 동향을 주시하는 것이 타당하다.

(5) 개인정보취급사업자의 범위

1) 현 황

개인정보보호법 제3조에서 기본이념으로 개인정보는 개인의 인격존중 이념아래 신중히 취급되어야 하며 그 적절한 취급을 도모하지 않으면 안 된다. 이상으로 개인정보데이터 등을 사업용으로 제공하는 자를 ‘개인정보취급사업자’로(개인정보보호법제2조제3항), 이러한 자에 대하여 개인의 권리의익 침해를 미연에 방지하기 위해 법률상의 의무를 과하고 있다.

2) 개선과제

개인정보보호법의 의무대상인가를 묻지 않고 개인의 권리의익 보호의 관점에서 개인정보는 적정하게 취급되어야 하는 것은 당연하다. 타국에서 개인정보 보유량과 상관없이 의무를 과하고 있는 나라가 많기 때문에 모든 사업자에게 의무를 과해야 한다는 지적이 있다.

3) 향후의 검토방향

일본에서 사업자의 부담과 개인의 권리의익 침해 위험성 등을 감안하여 취급 개인정보의 양 및 이용방법에 따라 개인의 권리의익을 해할 우려가 적다는 이유로, 사업자 개인정보 보유량이 5,000을 넘지 않는 자를 개인정보보호법의 의무 대상으로부터 제외하고 있다.

개인정보보호법의 의무 실행가능성에 따라 동법 의무대상의 산정 기준인 개인정보의 보유규모는 현 단계에서 적당한 수준이라고 생각한다.

(6) 사업자 등의 대응

1) 현 황

개인정보보호법 제8조에서 국가는 사업자 등이 개인정보의 적정한 취급 확보를 위한 활동을 지원하기 위하여 정보의 제공, 사업자 등이 강구해야 할 조치의 적절하고 유효한 실시를 도모하기 위한 지침 책정 등의 조치를 취하도록 하고 있다.

2) 개선과제

실태에 따르면 이와 관련한 개인정보보호법의 해석과 탄력적인 운용을 명확히 해야 하는 것은 아니가? 라는 논의가 있다.

주무대신 아래, 각 성청에서 사업 등 분야의 실정에 따라 가이드라인을 책정하고 있고, 가이드라인 등의 규정이 정도 차가 있는 것은 어쩔 수 없는 것인가?

사업분야 마다 가이드라인 등의 규정 중에 공통화 할 수 있는 것도 있지 않은가? 등의 논의가 있다.

3) 향후의 검토방향

이에 대하여 실태에 따라 개인정보보호법의 해석 탄력적인 운용의 명확화에 대하여 어디까지 내각부 및 각 관계성청이 연대하여, 가이드라인과 그 해설의 재검토를 하고 금후에도 현황의 변화에 따른 대책을 추진할 필요가 있다.

주무대신아래 각 성청에서 사업 분야의 실정에 따라, 각각 가이드라인 등을 책정하고 있고, 복수의 가이드라인이 적용되는 사업자가 있는 것을 유의하여 가이드라인의 공동화에 대하여 검토를 해야만 한다. 이때 사업분야의 실정과 가이드라인의 보급·정착의 정도를 고려하여 검토할 필요가 있다.

(7) 사업자의 감독강화

1) 현 황

개인정보보호법은 사업자를 넓게 대상으로 하여 공통 필요최소한의 준칙을 정하면서 각 사업 등 분야 실정에 따라, 사업자에 의해 자율적으로 개인정보보호에 만전을 기하려한다. 따라서 동법에는 실효성을 확보하는 조치로 주무대신에 의해 보고의 징수(제32조), 조언(제33조), 권고 및 명령(제34조)의 권한과 함께 명령위반에 대한 벌칙(제56조)을 규정하고 있다.

2) 개선과제

악질적인 사업자에 대하여 감독을 강화해야 한다는 지적이 있다. 특히, 대규모 또는 악질 개인정보의 누출 사안에서 주무대신에게 한층 엄격한 개인정보보호법상의 권한을 행사해야 한다고 지적되고 있다.

3) 향후의 검토방향

개인정보보호법은 개인정보의 적정한 취급의 실효성을 담보하는 조치로서 주무대신에 권고·명령 등의 감독권한을 부여하고 있고 개인정보의 취급에 의한 개인의 권리이익의 침해에 대하여 경우에 따라 형법 등 관계법령에 의해서도 처벌할 수 있고, 사업자에 대하여 주무대신의 권한을 적정히 행하는 등, 지속적인 개인정보보호법 등 엄격한 적용할 필요가 있다.

악질적인 범죄 사례도 발생하고 있으므로 사업자에 대하여 영비밀의 일환으로 개인데이터를 적절히 관리하는 것과, 취업규칙 등에 의해 종업자의 부정행위 방지를 도모하는 것을 포함하여, 개인데이터의 안전관리를 위하여 필요하고 적절한 조치를 강구하는 것이 계속 요구되며 수사에 지장 없는 범위에서 수사기관과 관계기관이 연대하여 대

응할 것이 요망된다.

종업자에 의해 당해 사업자의 보유 개인정보가 누출하는 것을 막기 위하여 계속 검토할 필요가 있다.

(8) 취득, 이용 및 이용정지·소거

1) 현 황

개인정보보호법에서 개인정보취급사업자에 의한 개인정보의 취득·이용 및 이용정지·소거에 대하여, 제15조, 제16조, 제17조, 제18조제1항, 제18조제2항에 걸쳐 규정하고 있다.

2) 개선과제

개인정보의 취득, 이용에 관하여 개인정보의 취득과 스팸메일 등으로 곤란하게 되는 등 사업 활동에 영향을 주게 됨을 지적하는 한편, 개인정보가 본인이 의도하는 목적 이외에 남용되지 않도록 해야 하는 것 아닌가? 즉, 현행법에서는 목적이용에 관하여 이용정지·소거에 대하여, 현행법에서는 부정하게 취득한 경우 등 법률위반이 있는 경우에 한하고 있지만 이러한 것이 적절한가의 지적이 있다. 일본은 동법 시행 후에도 스팸메일과 권유전화, 광고메일 등이 감소하지 않고 이것이 ‘과잉반응’의 한 요인이 되고 있는 것으로 지적하고 있다. 또 권유전화는 소비자에게 강한 스트레스를 주게 되고 소비자피해로 연결되기 때문에 금지해야만 한다는 의견도 있다. 한편, 사업자에게 본인으로부터 이용정지등을 요구하는 경우, 본인으로부터 요구된 경우는 자주적으로 광고메일의 발송 등의 정지에 따르는 취지를 명확히 하고 있는 사업자도 있다.

3) 향후의 검토방향

스팸메일에 대하여 ‘특정전자메일의송신적정화등에관한법률’(법률제26호), 권유전화에 대하여는 ‘특정상거래에관한법률’(법률제57호)에 의

해 규제하고 있다. 또 상업메일에 대하여 소비자생활센터 등의 고충 상담창구에서 사안에 따른 조언을 하고 있다. 본인이 원하는 개인정보의 이용에 대하여 이러한 관련제도의 활용, 연대가 필요하다.

(9) 적정·안전한 관리

1) 현 황

개인정보보호법 제21조에서 개인정보취급사업자는 종업자에게 개인 데이터를 취급시킬 때 당해개인데이터의 안전관리가 확보되도록 당해 종업자에 대하여 필요하고 적절한 감독을 하지 않으면 안 된다고 규정하고 있다.

2) 개선과제

사업자에 의한 종업자의 감독을 둘러싸고 다음과 같은 지적이 있다.

- ① 특히 고도의 안전관리조치가 요구되는 분야를 중심으로 개인정보보호 때문에 종업자의 부담이 과중한 경우도 있다.
- ② 종업자를 감독하기 위하여 사전에 종업자에게 개인정보보호법등을 교육시킬 필요가 있다.
- ③ 모니터링을 실시할 경우에 노사간 협의를 하는 등 적절한 수단을 행사할 필요가 있다.
- ④ 종업자에게 서약서에서 개인정보호를 명목으로 영업비밀의 보장과 손해배상의 청구 등의 규정을 악용하는 사례가 있어 종업자에게 적절하게 대하고 있는 지도 배려할 필요가 있다.

3) 향후의 검토방향

종업자에 대한 감독은 노동관련 법령에 따라 적정한 것이어야 한다. 또 가이드라인 등에 대하여는 사업자분야의 실정에 따라 ‘고용관리에 관한개인정보의적정취급확보를위하여사업자가강구해야할조치’(2004년7

월1일후생노동성)와 경제산업성 가이드라인 및 고용관리가이드라인에서 중요한 내용으로 모니터링(종업자의 업무 상황을 비디오 등으로 감시하는 것)등의 적정 고려가 필요하다고 한다.

(10) 제3자 제공의 제한

1) 현 황

개인정보보호법 제23조에서 개인정보취급사업자는 법령에 근거한 경우를 제외하고, 미리 본인의 동의를 얻지 않고 개인데이터를 제3자에게 제공하여서는 안 된다고 규정하고 있다.

2) 개선과제

개인데이터의 취급의 위탁과 합병 등 개인데이터공동이용에 대하여 이용목적과 이용자 범위의 한정을 요구하는 의견이 있다.

3) 향후의 검토방향

이러한 의견에 대하여 사업자는 소비자(본인) 사이에 개인데이터 취급의 위탁, 합병 등, 개인데이터 공동이용의 경우에 이용목적과 이용자의 범위를 명확히 하는 등 개인데이터 이용 범위를 적절히 정해야 한다. 또 공동이용에 관한 요건을 완화하도록 요구하는 견해도 있지만 개인데이터 취급의 위탁·합병 등 개인데이터의 공동이용의 경우 이용목적과 이용자의 범위의 명확화는 현행 구조에서도 필요하기 때문에 사업자가 사업내용을 참작하고 적절하게 프라이버시 폴리시 등을 정하는 것으로 대응 할 수 있다고 한다.

(11) 소비자등(본인)과 관계

1) 현 황

개인정보보호법제15조에서 개인정보보호취급사업자는 개인정보를 취급함에 있어 이용목적에 가능한 특정하지 않으면 안 된다고 규정하고 있다.

2) 개선과제

이용목적에 특정 할 때 사업자가 정하고 있는 이용목적 등의 범위가 지나치게 넓은 경우가 있어 개선이 요구된다.

3) 향후의 검토방향

본인에 대하여 개인정보가 어떻게 사업용으로 제공되어 어떠한 목적으로 이용되는 가를 가능한 명확히 해야 한다. 사업자가 사업내용을 고려하고 있는 사업자도 있기 때문에, 개인 권리의익 보호의 관점에서 기본방침의 재검토 등의 조치를 강구할 필요가 있다.

이 때 사업자의 자주적인 조치로서 본인이 이용목적에 선택하도록 하는 것도 생각할 수 있다.

(12) 취득원의 개시에 대하여

1) 현 황

개인정보보호법 제25조에서 개인정보취급사업자는 본인이 본인식별 보유개인데이터의 개시를 요구할 때, 원칙으로 본인에 대하여 지체 없이 당해 보유개인데이터를 개시하지 않으면 안 된다고 한다.

2) 개선과제

- ① 사업자는 소비자 등(본인)에 개인정보 취득원을 명확히 할 것 까지 개인정보보호법이 요구하지 않지만 취득원을 명확히 해야만 한다는 지적이 있다. 어떠한 대응을 생각할 수 있을까?
- ② 사업자가 개인정보 취득원이 명확하지 않기 때문에 소비자(본인)의 불안이 해소되지 않는다는 지적이 있기 때문에 소비자(본인)의 불안을 해소하기 위해서 사업자가 프라이버시 폴리시 등에 개인정보의 주요한 취득원을 포함시키도록 하는 것이 필요하지 않는가?

3) 향후의 검토방향

본인관여 관점에서 개인정보 취득원도 개시 대상이 되어야만 한다는 견해가 있는 한편, 취득원의 정보는 일률적으로 공표할 수 있는 것이 아니고 각각 관리가 필요하게 된 경우 사업운영에 지장을 초래하기 때문에 신중한 검토가 필요하다는 의견이 있다.

외국을 보면 EU국가들은 개인정보취득원에 관하여 개시청구권이 규정되고 있다. 프라이버시 폴리시 등에 取得元, 取得源의 종류와 취득경위라는 개인정보 취득방법을 사전에 가능한 한 구체적으로 명기하고 있는 사업자도 있기 때문에 개인의 권리와익보호의 관점에서 이러한 조치도 참고해야 한다. 이러한 대응을 추진하기 위하여 기본방침의 재검토 등 소요조치를 강구할 필요가 있다.

(13) 인정개인정보보호단체의 기능

1) 현 황

동법에서 고충처리를 시작으로 개인정보의 적정한 취급의 확보를 목적으로 하는 업무를 하는 민간단체에 대한 인정제도를 시행하고 있고, 업무신뢰성을 확보하고 민간단체에 의한 개인정보의 보호를 추진

하기위하여 인정개인정보보호단체를 설정하고 있다.

2) 개선과제

개인정보의 누출이 발생한 경우 당해사업자는 주무관청의 대응에 대하여 설정 개인정보보호단체가 대상 사업자에 지도와 권고를 하는 것도 중요하고 그 기능강화가 요구된다.

3) 향후의 검토방향

인정개인정보단체는 개인정보보호법 제42조 및 43조에 근거하여 대상사업자의 개인정보 취급에 관한 고통 처리, 대상 사업자에 대한 설명·자료요구, 개인정보보호지침을 준수할 위한 필요한 지도, 권고 등을 행하고 있다. 인정개인정보보호단체의 활동상황은 단체마다 다르다고 할 수 있기 때문에 활동이 충분하지 않는 단체는 적극적인 고충처리와 정보제공 등의 조치를 할 것이 요구된다. 또, 사업 분야에 따라서 인정개인정보보호단체의 수가 불충분한 경우도 있기 때문에 그러한 분야를 소관 하는 각 성청에서 인정 촉진에 힘쓸 필요가 있다. 앞으로 국민 및 사업자에 대하여 인정개인정보보호단체의 역할을 더욱 홍보하고 당해 단체가 하는 업무에 대하여 신뢰성을 높이면서 당해단체의 개인정보 누출사안 등에 적극 대응하여 것에 의해 실질적인 기능강화를 도모할 필요가 있다. 이러한 조치에 충실하기 위하여 단체 간 의견교환을 하고 식견을 공유하는 것도 유용하다.

(14) 고충처리의 실제

1) 현 황

개인정보보호 제31조에서 개인정보취급사업자는 고통의 적절하고 신속한 처리에 힘쓰지 않으면 안 된다고 하고 있다. 동법 제42조에서 인정개인정보보호단체는 본인이 대상사업자에 관한 고충 해소를 신청

한 경우 신청인에 필요한 조언을 하고 사정을 조사하며 당해대상사업자에 고충 내용을 통지하여 신속한 해결을 도모하도록 하고 있다.

동법 제13조 지방공공단체는 고충이 적절하고 신속하게 처리되기 위하여 고충 처리 알선 등 필요한 조치를 강구하도록 하도록 하고 있다. 또 동법 제9조에서 국가는 고충의 적절하고 신속한 처리를 도모하기 위하여 필요한 조치를 강구하도록 하고 있다.

2) 개선과제

고충처리는 고충처리를 이후 개선책으로 연결시키기 위해서 상담창구의 네트워크화에 의한 사안의 공유를 촉진해야 한다는 지적이 있다.

3) 향후의 검토방향

개인정보보호에 관하여 고충처리에 대하여 ① 당해 사업자에 직접 신청, ②인정 개인정보보호단체에 신청, ③소비자생활 센터 등 지방공공단체의 창구에 신청, ④국민생활센터에 신청하는 다양한 창구를 인정하고 있다.

소비자 등으로 부터 고충의 원만한 처리에 이바지하도록 인정개인정보보호단체의 인정촉진, 인정개인정보보호단체로부터 대상사업자에 고충상담정보의 제공 등에 의해 인정개인정보보호단체제도의 정착을 도모해야한다.

또 각 기관에서 효과적인 고충처리를 도모하는 한편, 국민생활센터와 소비자생활센터, 인정개인정보보호단체 간에 상담창구에 대응사례를 상호 공유하도록 하는 등 한층 유기적인 연대를 도모하는 것이 필요하다.

(15) 국제적 협력

1) 현 황

개인정보보호의 국제적인 조치로 1980년 OECD 프라이버시보호와 개인데이터의 국제유통에 관한 가이드라인에서 제시한 8원칙이 이후 국제적인 대응과 각국의 대응에 기본이 되고 있다. 일본의 개인정보보호제도도 이 가이드라인에 따른 것이다.

2) 개선과제

개인정보보호에는 세계 공통의 인프라가 필요하기 때문에 개인정보보호에도 국제적 구조와 글로벌한 시야가 필요하다. 일본의 법률에서 국제적 정보의 이전에 관하여 명확히 정하고 있지 않은 것에 대하여 어떻게 생각해야 하는가? 하는 지적이 있다.

3) 향후의 검토방향

OECD는 프라이버시 법집행의 국제적인 과제가 검토되어, APEC는 국경을 초월한 프라이버시 규칙의 구축과 정보공유와 조사·집행의 협력 과제가 검토되고 있는 등, 국제적 대응을 추진하고 있다. OECD, APEC, EU 등에서 추진되고 있는 구조를 따라 국제적 협조를 도모하면서 병행하여 일본 개인정보보호제도에 대해서도 국제적 이해를 구하는 것이 중요하다. 향후 일본에서 일본의 개인정보보호제도와 실태에 더하여 국제적 동향을 함께 고려할 필요가 있다고 한다.

(16) 제3기관의 의의

1) 현 황

동법에서 제4장 개인정보취급사업자의 의무는 사업용으로 제공하는 개인정보가 대상이 되고 있기 때문에 각 사업자 등을 소관 하는 대신

이 주무대신으로서 당해사업의 개인정보의 적절한 취급에 대하여 행정책임과 권한을 갖는 것으로 하고 있다.

2007년 5월 31일 소관 각 성청에서 22분야에 34개 가이드라인이 책정되고 있고, 주무대신 아래 사업자 등에 대한 지도·감독이 실시되고 있다. 2007년 5월 31일을 기준으로 동법 제37조 규정에 근거하여 주무대신이 인정하는 개인정보보호단체로 인정되는 단체는 총 34개 단체이다.

2) 개선과제

외국의 경우 중립적인 제3자기관이 개인정보보호법을 집행하고 있는 예도 많다.

3) 향후의 검토방향

일본에서 개인정보 취급은 민간사업자 사업 활동의 일환으로 당해 사업활동과 불가분한 것이며 업종·실태에 따라 다양한 특성을 갖고 있기 때문에 개인정보의 적절한 취급을 충분히 확보하기 위하여 일체적으로 수행하는 것이 합리적이고 실효적이라 지적 되고 있다. 이러한 이유로 ‘주무대신제’를 유지하고 있는 것은 타당하다고 생각되고, 제3자 기관 설치에 대해서는 국제적 균형을 고려하여 중장기 과제로 검토할 필요가 있다.

(17) 死者의 개인정보 보호

1) 현 황

동법은 死者에 관한 정보의 보호를 위하여 유족 등 제3자의 권리의익을 보호하는 것까지 의도하는 것은 아니다. 따라서 동법에서 ‘개인정보’를 생존하고 있는 개인에 관한 정보에 한정하고 있다. 따라서 死者에 관한 정보에 대하여 동시에 유족 등의 개인정보이기도 한 경우

만 당해 생존하는 개인에 관한 정보로서 보호되고 있다.

2) 개선과제

현행법은 생존하는 개인에 관한 정보만을 보호 대상으로 하고 있는데 재검토 필요는 없는가?

3) 향후의 검토방향

死者에 관한 개인정보의 보호에 대하여 현재 의료·개호분야 가이드라인 및 진료정보지침에서 소요 조치가 강구되고 있기 때문에 그 운용을 주시하는 것이 타당하다.

(18) 행정기관 등 보유 개인정보의 취급

1) 현 황

일본의 행정기관개인정보보호법 제8호 제1항 및 제2항에서, 국가의 행정기관은 ①법령에 근거한 경우, ② 본인의 동의가 있는 때, ③ 보유개인정보를 제공하는 것에 대하여 특별한 이유가 있는 때는 원칙적으로 이용목적 이외의 목적을 위하여 보유개인정보를 스스로 이용하고 또는 제공할 수 있도록 하고 있다.

2) 개선과제

국가의 행정기관에서 종래공표하고 있는 정보를 공표하지 않게 되고, 또 공표하던 고위직원의 정보에 사선이 그어져 있는 등의 문제점이 지적되고 있다. 이런 취급을 어떻게 생각해야 하는가? 정보공개와의 관계정리가 필요하지 않은가? 하는 지적이 있다.

3) 향후의 검토대상

이와 같은 과제에 관하여 국민의 신뢰를 확보하기 위해 필요한 정보를 가능한 제공하면서, 행정기관개인정보보호법의 통일적 운용 등

을 도모하려는 관점에서 ‘국가의 행정기관에 간부공무원의 이력의 공포 현황’(2007년 5월 22일총무성행정관리국장통지)이 정리되었다.

그러나 계속적으로 현행법의 구조아래 행정운영 개선을 위해 필요한 조치를 추진해야 할 것이다.

제 6 절 개인정보보호법 시행 이후의 변화

1. 개인정보보호에 관한 시행령의 변경

전절에서 논의한 일본 개인정보보호법에 대한 사후적 입법평가를 거쳐 개인정보의 보호에 관한 법률시행령의 일부개정(2008년정령제 166호)을 하게 되었다.

제 2 조(개인정보취급사업자로부터 제외되는 자) 법 제2조 제3항 제5호의 정령에서 정한 자는 그 사업용으로 제공하는 개인정보 데이터베이스 등을 구성하는 개인정보에 의해 식별된 특정 개인의 수(당해 개인정보데이터베이스 등의 전부 또는 일부가 타인 작성의 개인정보데이터베이스 등이며, 다음 각 호의 어딘가에 해당하는 것을 편집하거나 가공하지 않고 그 사업의 용도로제공할 때에는, 당해 개인정보 데이터베이스 등의 전부 또는 일부를 구성하는 개인정보에 의해 식별된 특정의 개인 수를 제외)의 합계가 과거 6월 이내의 어느 날도 5천을 넘지 않는 자로 한다.

① 개인정보로서 다음에 기재한 것을 포함하는 것.

가. 성명

나. 주소 또는居所(지도상 또는 전자기계기의 영상면상에 있어 주소 또는居所의 소재 장소를 표시를 포함한 것)

다. 전화번호

- ② 불특정 또는 다수의 자에게 판매할 목적으로 발행되거나 또는 다수 자에 의해 수시로 구입할 수 있는 것 또는 있었던 것

개정 전에는 개인정보로서 성명 또는 주소 혹은 거소(지도상 또는 전자계기의 영상면에 주소 또는 거소의 소재 장소를 나타낸 표시를 포함) 혹은 전화번호만이 포함된 경우로 규정하고 있었기 때문에 손수첩도 개인정보데이터에 해당하였다.

그러나 본 시행령의 개정에 의하여 손수첩은 개인정보데이터에서 제외되고 직원록·자치체직원록·정관요람·사보·변호사회명부 등 판매목적으로 발행되는 명부는 해당되고 동우회회원부·변리사회명부·의사회명부·회원제의 명부는 해당하지 않게 되었다.

2. 개인정보보호에 관한 기본방침의 변경

일본 정부는 개인정보 보호에 관한 법률(2003년법률제57호) 제7조 제1항 규정에 근거하여 “개인정보 보호에 관한 기본방침”을 책정 하는데, 이 기본 방침은 개인정보의 보호에 만전을 기하기 위하여 개인정보 보호에 관한 시책의 추진 기본적인 방향 및 국가가 강구해야 할 조치를 정하면서, 지방공공단체, 개인정보취급사업자 등이 강구해야 할 조치의 방향성을 제시하고, 정부로서 민관의 폭넓은 주체가 이 기본방침에 따라 개인정보 보호를 위한 구체적인 실천에 힘쓰도록 하고 있다.

이 기본방침은 국민생활심의회 개인정보보호심의회를 통하여 연구 검토 되어 2008년 4월 25일 일부 수정되었다.³⁹⁴⁾ 그 수정 내용을 중심으로 일본정부가 2008년 4월 25일에 정한 개인정보 보호에 관한 기본 방침을 정리 한다. 수정한 주요 내용은 다음과 같다.

394) 閣議決定, 『個人情報保護に関する基本方針』(平成20年4月25日 一部変更). 번역 첨부한 부록을 참조.

(1) 개인정보에 관한 시책의 추진에 관한 기본적인 방향

1) 개인정보 과민반응

법의 이념과 제도 구상에서 이른바 “과민반응”에 대처방법을 추가하였다.

우선, 프라이버시 의식 고양과 사회적인 필요성이 있음에도 불구하고, 법의 규정이상으로 개인정보 제공을 꺼리거나, 운용상작성가능한 명부의 작성을 그만두게 되는 것 등 이른바 “과잉반응”이 발생되고 있음을 밝혔다.

국민생활심의회는 “개인정보보호에 관한 총괄의견”(2007년6월29일)에서 법의 구체적인 내용의 광고·계발(啓發)등, 이른바 “과잉반응”대책에 만전을 기하는 것을 요구하고, 정부도 개인정보보호관련성청 관련회의를 추진하여 대책을 결정(“개인정보시책의 앞으로 추진에 대하여”(2007년6월29일 결정)후 이를 시행하고 있다.

일본정부는 개인정보보호법의 정확한 이해를 위하여 사업자 및 국민에 대한 광고·계발(啓發)에 적극적으로 대응하려 한다. 또 각 지방 공공단체에서는 주민에게 주지하기 위하여 적극적인 광고활동에 힘쓸 것이 촉구된다.

또, 이른바 “과잉반응”이 발생한 배경에는 개인정보에 의해 식별된 특정의 개인(이하, 본인이라 함)이 스스로 개인정보의 취급에 불안을 느끼고 있는 것도 하나의 이유로 생각되기 때문에, 법의 적절한 운용 등에 의해, 개인정보의 적절한 취급을 도모해 나갈 필요가 있음을 밝히고 있다.

2) 국제적인 협조

법의 틀 및 기본방침에 근거하여 개인정보보호의 대처를 추진함에 있어, OECD를 시작으로 아시아태평양경제협력(APEC), 구주연합(EU)등

다양한 곳에서 추진되고 있는 국제적인 대응을 따라 프라이버시 보호에 관한 국경을 초월한 집행 협력 등을 추가하여 국제적인 협조를 강조하게 되었다.

(2) 국가가 강구해야 하는 개인정보 보호를 위한 조치에 관한 사항

1) 각 행정기관이 보유하는 개인정보의 보호 추진

국가의 행정기관이 보유하는 개인정보 보호에 대하여는 행정기관개인정보보호법을 적절히 운용하기 위하여, 동법 운용의 통일성, 법적합성을 확보하기 위한 입장에서 총무성은, ‘행정기관이 보유하는 개인정보의 적절한 관리를 위한 조치에 관한 지침(2004년 9월 14일총무성행정관리국장통지)’을 책정하고, 개인정보의 적절한 관리를 철저히 왔고, 계속 각 행정기관 및 국민에 대하여 팜프렛 배포와 설명회 실시 등을 통하여 동법을 주지(周知) 시키며, 시행상황 개요를 공표하는 등 국민에 대하여 정보제공을 하는 제도의 운용의 투명성을 확보하려 한다.

또 각 행정기관은 총무성이 책정한 지침 등을 참고로 하여 그 보유 개인정보의 취급 실정에 따른 개인정보의 적절한 관리 규정을 정비하고 있지만, 계속 ①직원의 교육연수, ②적절한 정부 시큐리티 시스템 정비, ③관리체제와 국민에 대한 상담창구의 정비, ④개인정보의 적절한 관리를 도모하기 위하여 강구한 조치 등에 관한 정보 제공을 추진하려 한다.

또 국가의 행정기관에서 개인정보 제공에 대하여 행정기관개인정보보호법상 필요성이 인정되는 경우에는 개인정보 공표 등은 가능하게 되었다.

2) 분야별 개인정보 보호 추진에 관한 방침

개인정보 보호에 관하여 법의 시행 전에도 사업자 취급 개인정보의 성질과 이용방법 등의 실태에 근거하여 사업자분야별 가이드라인 등

에 근거하여 자주적인 대응을 추진하여 왔으며, 특히 악질적인 사업자의 감독을 위해, 개인정보취급사업자에 대하여 보고의 징수 등의 주무대신의 권한 등에 대하여, 이를 적절히 행사하는 등, 법의 엄격한 적용을 도모하는 내용을 추가 하였다.

3) 광고·계발, 정보제공 등에 관한 방침

개인정보의 보호의 실효성을 위하여, 사업자 및 국민에 대하여 법제도의 주지(周知)를 철저히 하는 것이 매우 중요하다.

이 때문에 내각부 및 각 성청은 계속 사업자 및 국민에 충분한 정보제공이 행해지도록 인터넷 활용, 포스터의 게시, 판플렛의 배포, 설명회의 실시 등 다양한 매체를 사용하여 광고·계발(啓發)에 적극 힘쓰도록 한다. 이때, 개인정보의 취급에 관심 등에 대하여, 세대간, 사업 분야 간에 따라 차이가 있으므로, 매체의 선정 등도 배려하여 매우 세부적인 대응을 하고 ‘개인정보의 유용성을 배려하면서, 개인의 권리이익을 보호하는 것(법제1조)’을 목적으로 하는 법의 구상이 각 주체에 의해 실제 개인정보 취득에서 충분히 반영되도록 한다는 문구를 추가 하였다. 특히, 이른바 ‘과잉반응’에 대한 대처의 일환으로 ‘개인정보보호시책의 금후 추진에 대하여’ 광고·계발(啓發)등을 적극적으로 하도록 하고 있다.

4) 개인정보 보호에 관한 국제적인 구조에의 대응

OECD에는 프라이버시법 집행의 국경을 초월한 과제가 검토되고, APEC은 국경을 초월한 프라이버시 규칙의 구축과 정보공유, 조사·집행의 국경을 초월한 협력 과제가 검토되고 있다. 이러한 OECD, APEC에서의 대응과 EU등에서 추진되고 있는 대응에 따라, 사업자의 자율적인 대처를 존중하는 일본 법제도와와의 적합성에 유의하여 국제적인 협조 관점에서 일본에 필요한 대응을 검토해 나간다. 또 ‘프라이

버시보호법의 집행에 관한 국경을 초월한 협력에 관한 OECD권고'(2007년 6월 12일 채택)에 근거, 내각부는 각 성청과 협력하고, 필요한 대응·조치를 검토한다는 내용을 추가하였다.

(3) 지방공공단체가 강구해야할 개인정보 보호를 위한 조치에 관한 기본적인 사항

지방공공단체도 이른바 '과잉반응'이 일부에서 보임에 따라 지방공공단체에서도 법의 취지에 따라, 조례의 적절한 해석·운용을 첨가하였다.

(4) 독립행정법인등이 강구해야 하는 개인정보 보호를 위한 조치에 관한 기본적인 사항

총무성은 '독립행정법인등이 보유하는 개인정보의 적절한 관리를 위한 조치에 관한 방침'(2004년9월14일총무성행정관리국장통지)을 책정하고, 개인정보의 적절한 관리를 철저히 하고 각 행정기관, 독립행정법인 등 및 국민에 대하여 판플렛의 배포와 설명회의 실시 등을 행한 동법의 주지(周知)를 도모하면서, 시행상황의 개요의 공포 등 국민에 대하여 정보제공을 행한 제도 운용의 투명성을 확보함을 강조하였다.

(5) 지방독립행정법인이 강구해야하는 개인정보 보호를 위한 조치에 관한 기본적인 사항

지방독립법인에 있어 개인정보 보호에 대하여 지방공공단체는 법제11조제2항에서 필요한 조치를 취하도록 요구하고 있다. 이에 따라 각 지방공공단체는 그 설립에 관한 지방독립행정법인의 성격 및 업무내용에 따라 각 단체가 제정하는 개인정보보호조례에 있어 소요(所要)규정을 정비하는 등, 적절한 개인정보 보호조치가 강구되도록 힘쓸 것이 요구된다.

(6) 개인정보취급사업자 등이 강구해야하는 개인정보 보호를 위한 조치의 기본 사항

1) 개인정보취급사업자에 관한 사항

안전관리조치의 정도에 있어, 사업자는 그 취급하는 개인정보의 적절한 보호를 확보되기 위하여 누출, 멸실 또는 손해가 발생한 경우에는 본인이 피해 권리의익의 침해의 크기를 고려하고 사업의 성질 및 개인데이터의 취급상황 등에 기인하는 리스크에 따라 필요하고 적절한 조치를 강구하는 것이 중요하다.

이때에는 개인데이터를 기록한 매체의 성질에 따른 안전관리조치를 강구하는 것이 중요하다. 예를 들어 불특정다수자가 서점에서 수시로 구입가능한 명부에 사업자가 전혀 가공을 하지 않은 것은 개인의 권리의익을 침해할 우려가 적다고 할 수 있기 때문에, 이것을 처분하기 위하여 문서 세절기 등에 의한 처리를 하지 않고 폐기하고, 폐품회수로 제출한 것이라도 사업자의 안전관리조치의 의무위반이 되지 않는 것으로 취급할 수 있다는 내용을 첨가 하였다.

2) 인정개인정보보호단체에 관한 사항

인정개인정보보호단체는 단체마다 그 활동 정도 차이가 보인다는 지적이 있기 때문에, 활동이 충분하지 않는 단체는 적극적으로 고충 처리와 정보제공 등에 힘쓰는 것이 요망된다고 첨언하고 있다.

또 사업 분야에 따라 인정개인정보보호단체의 인정이 충분하지 않는 분야도 있기 때문에, 이러한 분야를 소관 하는 각 성청에서는 더욱 인정 촉진에 힘쓸 것을 강조하였다.

제 7 절 시사점

1. 개인정보보호법의 체계

일본은 2003년 5월 23일 개인정보보호 관련 5개 법률의 제정 이후 공공부문과 민간부문을 포괄하는 기본법의 지위와 민간부문의 일반법 지위를 가진 「개인정보의 보호에 관한 법률」을 두게 되었다. 그리고 공공부문을 규율하는 일반법으로 「행정기관이 보유하는 개인정보의 보호에 관한 법률」과 「독립행정법인등이 보유하는 개인정보의 보호에 관한 법률」 등이 존재한다.

이렇게 볼 때 일본의 개인정보보호법제는 통합형 기본법과 부문별 일반법, 그리고 개별법이 병존하는 구조라고 할 수 있고, 이를 굳이 유형화하자면 ‘일원적 기본법주의’에 속하는 것으로 평가할 수 있을 것이다. 개인정보보호법의 입법에 있어 유럽의 입법은 포괄적인 일반 개인정보보호법을 제정하였고, 미국은 개인정보보호법규를 개별 영역에 만드는 방식 중에 일본은 유럽식의 포괄적이고 공사(公私)에 적용되는 개인정보보호법을 제정하였다. 그러나 일본의 경우 유럽과는 달리 “행정기관이보유하는전자계산기처리에관한개인정보보호에관한법률”이 “행정기관이보유하는개인정보보호에관한법률”로 전면개정 된 상태로 존재 하면서, “개인정보보호법”이 불완전한 일반법적 성격을 가지고 있다.

우리나라도 현재 “공공기관의개인정보보호에관한법률”이 존재하고 있어, 차후 일반법인 “개인정보보호법”이 성립되는 경우 일본식의 법규체제를 따르게 될 것인가? 그렇지 않으면 “공공기관의개인정보보호에관한법률”을 폐지하고 단일 “개인정보보호법”을 입법하는 유럽형 입법 체계를 취할지 검토할 필요가 있다.

2. 개인정보의 보호수준

(1) 입법화 할 때 개인정보의 개념을 어떻게 할 것인지에 대한 많은 논의가 필요할 것이다. 일본에서는 「개인정보」란 제2조 1항에서 「생존하는 개인에 관한 정보로서 당해정보에 포함되는 성명, 생년월일 기타의 기술 등에 의해 특정의 개인을 식별할 수 (다른 정보와 쉽게 조합되어 특정 개인을 식별할 수 있게 되는 것을 포함한다)이다.」라고 한다. 이런 정의는 상당히 넓게, 일반에게 타인에게 알리고 싶지 않은 정보(예를 들어 자산상황·병력 등)뿐만 아니라, 공공연히 알고 있는 것인지 여부를 묻지 않고, 일상생활의 여러 면에서 본인이 사용하는 성명, 주소, 성별 등 특정의 개인이 인식 가능한 것을 모두 「개인정보」라고 규정하고 있다.³⁹⁵⁾

「개인데이터」 및 「보유개인데이터」는 「개인정보」의 한 형태로 개인정보취급사업자가 준수해야만 하는 구체적인 의무(제4조)와 대상을 세밀하게 정하기 위해 정의되었다. 「개인데이터」란 특정의 개인정보를 성명 등으로 검색되도록 컴퓨터를 이용한 데이터 베이스 등에서 체계적으로 정리하고 있는 개개의 개인정보이다(제2조제4항). 이러한 데이터베이스에 포함된 개인정보를 프린트 아웃 하여 취급하는 것도 「개인데이터의 취급」이 된다. 「보유개인데이터」란 「개인데이터」중에 개시, 정정, 이용정지 등의 대상이 되는 것이다.

(2) 본법 시행령의 일부개정(2008년정령제166호)을 통하여 제2조(개인정보취급사업자로부터 제외되는 자) 법제2조제3항 제5호의 정령에서 정한 자는 그 사업용에 제공하는 개인정보데이터베이스를 ①개인

395) 또한, 영상과 음성 등도 특정의 개인이 식별 가능한 상태에 있으면 「개인정보」가 된다. 반면, 익명화되어 특정 개인을 식별할 수 없는 정보는 본 법률의 대상이 아니다. 또 정의상, 死者에 관한 정보에 관하여, 그것이 동시에 생존하는 개인에 관한 정보이기도 한 경우를 제외하고, 본 법률의 대상이 되지 않는다.

정보로서 “가. 성명 나. 주소 또는 거소(지도상 또는 전자기계의 영상면에 있어 주소 또는 거소의 소재 장소를 표시를 포함한 것) 다. 전화번호 ② 불특정 또는 다수의 자에 판매할 것을 목적으로 발행되거나 또는 다수 자에 의해 수시로 구입할 수 있는 것 또는 있었던 것”을 포함하는 것으로 정의하였다.

(3) 이러한 개인정보개념 등의 규정은 일본 개인정보보호법의 보호수준을 특징적으로 보여주고 있다. 이에 관해서는 사후적 입법평가에서도 논의가 있으며, 개인정보보호위원회에서는 ‘개인정보 보호에 관한 기본방침의 일부개정(2008년정령제166호)’을 통하여 기존 개인정보데이터의 범위를 일부 확장(일부 축소: 손으로 쓴 수첩은 제외) 하였다.

기존 시행령에서는 ‘전부 또는 일부가 타인 작성의 개인정보데이터 등에 개인정보로서 성명 또는 주소(혹은 거소) 혹은 전화번호만이 포함된 경우’(시행령2조)라 하고 있다. 따라서 자동차 내비게이션, CD-ROM 전화부, 전자주택지도는 물론 종이 수첩도 이에 해당되었다.

개정에 의한 추가부분은 ‘전부 또는 일부가 타인 작성 개인정보데이터 등으로 불특정 다수자에 판매하는 것을 목적으로 발행하여 불특정 다수자에 의해 수시로 구입될 수 있는 경우’로 하고 있다.³⁹⁶⁾ 따라서 직원록, 자치체직원록, 정관요람, 회사사보, 변호사회명부도 포함되게 된다. 일반 클럽회의 명부, 동우회명부, 세무사회명부, 의사회명부, 약사회명부, 회원제의 명부는 이에 해당하지 않는다.

이는 좀 더 현실적이고 명확한 개인정보, 개인정보데이터베이스 등의 개념이 사후적 입법평가 단계를 통하여 시정된 것이다. 국내 개인정보보호법의 입법평가에서는 개인정보의 개념과 범위에 대한 충분한

396) <개정에 의한 추가 부분>

- 전부 또는 일부가 타인 작성에 관한 개인정보데이터 등으로 불특정 또는 다수자에 판매하는 것을 목적으로 발행되어, 불특정 및 다수자에 의해 수시로 구입될 수 있는 경우
- 예: 직원록, 자치체 직원록, 정부요람, 회사사보, 변호사회명부

고민이 법조문에 반영되어야 할 것이다.

(4) 민감한 기록(sensitive personal data) 특수한 기록

‘민감한 기록에 관하여 1980년 OECD가이드라인’의 해설에 따르면 이는 ‘만인이 공통으로 센스티브라고 간주하는 데이터를 명확히 하는 것은 거의 불가능하다’고 하고 있다.³⁹⁷⁾ 일본에서도 성명, 연령, 성별, 주소 같은 개인정보는 일반인에게 민감하지 않은 정보로 이해하고 있지만 경우에 따라서 심각한 권리의익의 침해를 초래하는 원인이 될 수 있다. 또 가령 센스티브 정보라고 하더라도 이를 이용하는 것이 불가능한 경우가 있고, 이를 취득하는 것이 불가능한 경우도 있을 수 있다. 이러한 이유로 일본의 동법은 다양한 개인정보의 내용과 성질, 이용방법 등에 의한 구별을 하지 않고, 오히려 모든 개인정보에 대하여 개인의 인격존중의 이념아래 신중히 취급할 것을 기본이념(제3조)로 하여 개인정보취급사업자가 개인정보의 취급을 필요최소한도로 할 것을 정하고 그 적정한 취급이 확보되도록 재고하고 있어 참고할 만하다.

(5) 수집 및 이용시 정보주체의 동의문제

동법 제17조에는 개인정보취급사업자가 허위 기타의 방법으로 개인정보를 취득할 수 없다고 한다. 따라서 수집목적은 은닉하거나 수집 목적을 거짓으로 하여 취득할 수 없도록 규정하고 있다. 물론 동법 제23조의 동의 없이 제3자에 제공 가능한 경우의 규정을 위반한 제3자에 제공도 할 수 없다. 이러한 부정한 수단으로 취득한 개인정보 데이터는 본인의 이용정지 등의 요구에 대하여 개인정보취급사업자는 따를 의무가 있다(동법 제27조 명시).³⁹⁸⁾ 또한 동법 제18조에서 개인정보를 취득하는 경우, 사전에 이용목적은 공표하고 있는 경우를 제

397) 三上・清水・新田, 前掲書, 39면.

398) 三上・清水・新田, 前掲書, 42.

외하고는 본인에게 통지 또는 공포하지 않으면 안 된다. 동법은 이용 목적을 본인에게 통지하거나 공포하여 본인에게 알릴 기회를 설정하여 개인정보의 취급에 관한 본인의 불안을 완화하는 것이다.

제18조 2항에는 계약 신청과 질문에 대답하는 경우와 같이 개인정보를 본인으로부터 직접서면(전자적 방식 등에 작성되는 기록을 포함)으로 취득하는 경우에는 공포에 의한 취득은 인정되지 않고 취득 시, 사전에 본인에게 이용목적을 명시해야만 하도록 하고 있다(제18조2항). 한편 일본의 정보통신 분야 등의 가이드라인에서 계약약관에 의해 직접 본인 동의를 얻는 경우도 상정되고 있다. 국내 입법평가 과정에서 본인의 동의를 얻을 것인가, 어떠한 경우에 본인의 동의가 필요한가에 대한 명확한 검토가 필요하다.

3. 자율규제 모델

일본 개인정보보호법제의 사전적 입법평가는 내각책임제의 특성과 맞물려 내각에 관련부서를 두어 검토하고, 의회에서도 관련 사전적 입법평가를 통한 입법 과정을 거쳤다. 사후적 입법평가는 현재 규정의 개정필요성 및 개정범위의 논의 보다는 구체적인 현황과 과제를 검토하여 앞으로 행정부가 추진해야할 사업을 정비하는 측면이 강하다.

일본은 내각부 국민생활심의회의 개인정보보호위원회와 같은 심의기관을 두고, 개인정보보호법의 사후평가를 위한 추행조사를 하며 관련 사업을 추진하고 있다. 꾸준히 문제점과 향후과제를 제시하고 있고, 일부 시행령의 개정작업도 하고 있다.

즉 개인정보보호법은 그 시행령, 동법 제7조1항의 규정에 근거한 “개인정보 보호에 관한 기본방침”, 소관부처별 가이드라인 그리고 사업자의 개인정보보호 폴리시를 통하여 이르러 개인정보보호를 위한 구체적으로 집행된다. 또한 정부가 규제일변도가 아니라 사업자를 권

고하거나 보고하게 하고 사업자는 정부와 함께 개인정보 보호 사업을 추진하는 방향을 지향하고 있다. 이런 면은 우리에게도 좋은 자율규제의 모델로 모범이 될 수 있다.

이러한 사전적 사후적 입법평가와 법제정추진 과정의 모습은 향후 우리 개인정보보호법제정에도 시사하는 바가 크다. 일본의 개인정보보호법은 입법을 위한 사전적 입법평가 행위에 그친 것이 아니라, 이후에 꾸준히 법 시행을 위한 추진사업을 검토·시행하고 사후적 입법평가를 계속하여 실질적인 법의 규범력을 재고하고 높이는데 기여하고 있다.

또한 개인정보규제를 위하여 독립된 행정기관에 의한 것인지, 각 행정부에 소관 사업에 맞는 개인정보보호사업을 추진하게 할 것인지의 논의도 결국 이러한 자율규제 사업을 원활히 할 수 있는 행정시스템을 구축한다는 목적에 비추어 결정해야 할 것이다.

4. 과잉반응의 문제

일본은 개인정보보호법 시행 후의 변화에 대한 질문으로 “사회전체로 개인정보에 관한 취급이 너무 신중해져서 불편해 졌다”는 응답이 4,822명(68.0%)으로 가장 많았고, 사회전체가 개인정보의 취급에 관하여 신중하게 되었다고 느끼는 사람이 많았다. 이는 개인정보 보호의 의식이 높아진 것을 의미하나 일본의 여러 분석에서 이미 지적한 바와 같이 일본 국민이 정확한 개인정보의 개념과 본법의 규정을 이해하지 못하는 현실에도 원인이 있다.

따라서 일본 정부는 상당한 노력을 들여 개인정보보호를 위한 광고·계발(啓發) 사업에 힘쓰며 개인정보의 적절한 취급이 정착화 되도록 힘쓰고 있음은 본문에서 서술한 바와 같다. 국내 개인정보보호법 입법평가에서도 그러한 과잉반응을 고려한 명확한 입법과 국민 홍보

가 중요하리라 생각한다.

또한 일본에서 개인정보보호법의 입법이후에도 권유전화와 스팸메일 등이 줄어들지 않고 있다는 보고도 고려하여 국내 개인정보보호법 입법평가에도 참고 해야 할 것이다.

5. 공공기관과 사업자의 개인정보 침해

조사에 의하면 일본은 2007년에 사업자가 공표한 개인정보유출사안은 총 848건이다(2005년에는 1,556건, 2006년에는 893건)이다.

한편 개인정보 누출, 멸실, 손상이 발생한 것으로 인정된 사건이 2007년 행정기관에서는 약 75%가 오송부, 오교부, 오송신에 의한 것이다. 행정기관 320건. 독립법인 855건이 있었다.

단순히 숫자로는 공공기관과 사업자 중 어느 쪽이 개인정보를 더 침해 하였는지를 알 수는 없다. 그러나 사업자의 경우 오류가 아닌 법외의 개인정보 매매, 정보보안상의 문제로 침해될 수 있으므로 국내 입법평가 시 공공기관과 사업자 양자를 어떻게 고려할지도 검토해야할 문제이다.

제 3 편
개인정보보호의 입법체계에
관한 병행적 입법평가

제 1 장 비교법적 고찰

오늘날 개인정보침해의 상당수가 민간부문에서 이루어지고 있음에 주목하여 대부분의 국가에서는 민간부문에 적용되는 각종의 개인정보보호에 관한 법률들을 제정하여 시행하고 있다. 각국의 개인정보보호법제도는 공공분야와 민간분야 모두에 적용되는 예도 있는 반면, 공공분야에서만 입법한 경우도 있다. 유럽 각국(EU 회원국)과 호주, 뉴질랜드 등의 국가들은 모두 공공부문과 민간부문을 아우르는 개인정보보호법을 제정·시행하고 있다.

그러나 정보통신분야, 의료분야, 금융분야 등과 같이 보다 세부적인 규정을 두어야 하거나 분야별 특성을 반영할 필요가 있는 경우에는 분야별 개인정보보호법 또는 관련 법률에서 개인정보보호규정을 두는 경우가 많다.

개인정보보호를 강조하고 있는 유럽에서도 대부분의 국가들이 공공부문과 민간부문을 함께 규율하는 개인정보보호법제를 갖추고 있음에도 불구하고 정보통신분야, 의료분야 등에 대하여는 별도의 법령을 통하여 규율하고 있다.

즉, 유럽연합(EU)은 1995년도에 마련한 개인정보보호지침 외에도 정보통신분야에 특별히 적용되는 지침을 1997년(2002년 전문개정)에 제정하여 회원국들에게 이를 준수토록 하고 있으며, 영국, 독일, 핀란드, 스페인, 이탈리아, 호주, 뉴질랜드 등에서는 개인정보보호법 외에도 정보통신분야의 개인정보보호와 관련된 별도의 법률이나 하위규칙을 제정하여 시행하고 있다.

기본법을 두고 있는 국가에서 정보통신분야의 개인정보보호에 관한 법률 또는 규정을 마련하고 있는 사례는 다음과 같다.

[표 3-1-1] 기본법의 개별법을 규정한 해외사례

국가	기본법	개별 법령
영국	정보보호법 (Data Protection Act, 1998)	프라이버시와 전기통신 규칙 (Privacy and Electronic Communications (EC Directive) Regulations 2003)
독일	연방정보보호법 (Bundesdatenschutzgesetz, 1974)	전기통신법 제7장 (Telekommunikationsgesetz TKG PART 7)
		전기통신소비자보호규칙 (Telekommunikations-Kundenschutzverordnung (TKV))
이탈리아	개인정보보호법(Legislative Decree no. 196 of 30 Jun 2003)	
스페인	개인정보보호통합법 (Organic Law on the Protection of Personal Data, 1999)	연방 전기통신법 (Act 32/2003 of 3 November (State Telecommunications Act))
뉴질랜드	프라이버시법(Privacy Act 1993)	전기통신 정보 프라이버시 실행규약 (TELECOMMUNICATIONS INFORMATION PRIVACY CODE 2003)
호주	프라이버시법 (Privacy Act 1988)	전기통신법 제13장 (TELECOMMUNICATIONS ACT 1997 PART 13)
핀란드	개인정보법 (Personal Data Act, 1999)	전기통신에서 프라이버시보호에 관한 법률 (Act on the Protection of Privacy in Electronic Communications)

그러면 이하에서는 미국, 캐나다, 영국, 독일, 프랑스, 이탈리아, 스페인, 일본 등의 개인정보보호에 관한 법제도를 소개하기로 한다. 다만 여기서는 각 입법의 구체적인 내용까지 고찰하지는 않고, 입법체계의 비교분석에 꼭 필요한 사항을 중심으로만 살펴보고자 한다. 따라서 각국의 입법과정, 적용범위, 구성의 체계, 부문별 관련 법제의 현황, 개인정보보호기구 등을 위주로 하여 언급한다.

제 1 절 미 국

1. 개인정보보호법제 현황

미국에서 개인정보보호의 문제는 프라이버시권의 체계 안에서 취급되고 있다. Alan F. Westin, Arthur R. Miller 등이 프라이버시에 적극적 성격을 부여하는 이른바 현대적 프라이버시권으로서 자기정보통제권을 주창한 이래로 개인정보는 프라이버시의 한 내용으로서 이해되기 시작하였다. 이는 연방대법원에 의해 수용되지는 않았지만, 의회의 입법에는 상당한 영향을 끼친 것으로 평가된다. 1970년의 공정신용조사법(Fair Credit Reporting Act)은 현대적 프라이버시권에 관한 최초의 입법이라고 할 수 있는데, 이는 소비자의 신용정보를 수집·축적·제공하는 기관들에게 비밀보호와 정확성의 담보 등에 관한 의무를 부과하고 소비자의 정보열람권을 보장하는 것을 내용으로 하고 있다. 한편, 1974년 12월 31일에 공포된 프라이버시법(Privacy Act)은 그 명칭에서 프라이버시라는 용어를 사용하고 있지만 사실상 개인정보를 보호의 대상으로 하는 것이라고 할 수 있다.³⁹⁹⁾ 이 법은 공공기관이 보유하는 개인에 대한 기록에 관하여 규율하는데, 세계적으로 공공부문에 있어서 개인정보자기결정권을 법제화한 선구적 입법례로 인정받고 있다.

그러나 미국은 공공부문과 민간부문을 아우르는 종합적이고 포괄적인 입법의 방식을 채택하지 않고, 민간부문에 있어서는 개별적인 단행법에 의해서 개인정보를 보호하는 부문별 접근방법(sectoral approach)을 취하고 있다. 그리고 전자상거래에 관련되는 개인정보보호의 문제에 대해서는 법적 규제가 자칫 정보의 자유로운 유통을 저해하고 인터넷

399) 1974년의 프라이버시법은 미국법전 제5편 제522(a)조에서 규정되고 있는데, 그 표제를 보면 “개인에 관하여 보유하고 있는 기록”(records maintained on individuals)으로 되어 있다.

상거래시장을 위축시킬 수 있다는 지적에 따라 민간과 시장기능에 위임하는 자율규제의 방식을 채택하고 있다. 이 점은 EU의 입장과 구별되는 주요한 특징이라 할 수 있다.⁴⁰⁰⁾ 이는 탈중심적 권위에 대한 선호, 사적 부문의 월권보다 정부의 월권에 관한 보다 큰 우려 등 미국의 법적 전통에서 기인하는 것이라 할 수 있다.⁴⁰¹⁾

현재 연방 차원의 개인정보보호는 1970년의 공정신용조사법(Fair Credit Reporting Act), 1974년의 프라이버시법(Privacy Act), 1978년의 금융프라이버시권법(Right to Financial Privacy Act), 1986년의 전자통신프라이버시법(Electronic Communication Privacy Act), 2002년의 전자정부법에서 도입한 프라이버시 영향평가제도 등을 통해 구현되고 있다.

[표 3-1-2] 미국의 개인정보관련 법제 현황⁴⁰²⁾

연도	입법안	목적 및 내용
1968	집단범죄 규제 및 가두안전법	대통령이 특권을 행사하는 경우와 범죄의 경우에 한하여 법관의 영장을 발급받아 도청을 할 수 있도록 프라이버시 침해 제한
1970	공정신용 보고법	자동 정보 처리시스템의 발전단계에 대응하여 개인정보의 당사자에게 자기에 관한 정보를 통제할 수 있는 권리를 보장
1974	프라이버시법	행정기관에 의해 침해받을 수 있는 프라이버시권을 보호
1986	전자통신 프라이버시법	전자통신의 무단도청을 방지하고 새로운 컴퓨터와 전자통신기술의 급격한 변화를 감안하여 새롭고 명확한 연방프라이버시 보호 기준을 규정
1988	컴퓨터연결과 프라이버시법	연방기관이 예외규정에 근거하여 연방 데이터베이스간에 광범위한 전자적 비교를 정당화하고 있다는 우려에 따라 프라이버시법을 개정

400) 성낙인 외, 『개인정보보호를 위한 정책방안 연구』 (정보통신부, 1999), 45면.

401) Barbara S. Wellsberry, “Bridging the Difference: The Safe Harbor and Information Privacy in the United States and the European Union,” *Privacy and Information Law Report*(1 NO. 6 *Privacy Info. L. Rep.* 13), 2001.

402) 한국통신정보보호학회, 『주요국가의 개인정보보호기관 운영상황 연구』 (한국정보보호센터, 1998), 163면.

연도	입법안	목적 및 내용
1996	전기통신법	통신사업자가 사용자 정보를 이용, 공개 또는 접근하는데 새로운 제한을 부과하여 개인정보를 보호
1998	자유와 사생활 회복에 관한 법안	연방정부기관에 대한 개인 신상관계 확인 등의 목적으로 신상관련 서류의 중복접수 금지
1998	시민개인정보 보호법(안)	연방정부기관에 대한 국가 신분증의 발급 또는 기타 목적으로 연방기관에 국가 신분증 발급에 대한 권한을 부여하도록 하는 연방법 해석 금지
1998	의료프라이버시법(안)	연방정부에 대한 국가의료 신분증 발급 또는 기타 목적으로 연방기관에 국가 의료 신분증 발급에 대한 권한을 부여하도록 하는 연방법 해석금지

2. 연방 프라이버시법

(1) 제정과 개정

미국에서 프라이버시는 전통적으로 보통법상의 불법행위에 의하여 보호되어 왔으며, 프라이버시가 판례에 의하여 헌법상의 권리로서 승인되면서부터는 프라이버시 사건은 부당한 수색·압수를 금지한 수정헌법 제4조나 결사의 자유를 보장한 수정헌법 제1조 등의 개별 규정을 근거로 하여 해결하여 왔다.

그러나 1960년대부터 미국은 고도정보화사회로 접어들게 되면서 행정업무가 복잡·다양해지고 행정기관이 보유한 개인정보의 양은 비약적인 증가를 가져왔다. 이처럼 증가된 정보량을 처리하기 위하여 컴퓨터기술을 최대한 활용할 필요성이 제기되었고, 예산관리처(Office of Management and Budget; OMB)는 연방의 각 행정기관에 분산되어 있는 개인기록의 집중화 및 전산화와 연방정부의 정보수집과 기록보존 시스템을 개혁하기 위하여 국립정보센터(National Data Center)라는 연

방절차의 단일 통계센터를 설치할 계획을 세웠다. 이러한 구상이 알려지면서 국민적 여론은 개인의 프라이버시 침해를 우려하여 거부반응을 보였으며, 1968년 하원의 정치활동위원회가 충분한 대응책을 마련한 다음 이를 설치할 것을 권고함에 따라 결국 정부의 이러한 구상은 일단 포기되었다.

한편 행정기관에 못지않게 민간조사기관이 개인의 프라이버시를 침해하는 문제가 빈발하자 1970년에는 공정신용조사법(Fair Credit Reporting Act)이 제정·공포되었다(Pub. L. No. 91-508, 84 Stat. 1136). 이 법률은 소비자신용조사업자에 대하여 소비자신용, 인사, 보험 기타 정보와 비밀의 보호, 정확성·관련성 등에 관하여 합리적인 조치를 취할 의무를 부과하였다. 한편, 공공기관에 의한 프라이버시침해를 방지하기 위한 입법도 꾸준히 시도되었는데, 특히 1973년에 공포된 보건교육복지부(HEW) 장관의 자문위원회 보고서는 기록시스템 공시의 원칙, 개인 액세스의 원칙, 목적외 이용금지의 원칙, 개인구제의 원칙, 충분한 안전조치의 원칙 등 5원칙을 제시하였는데, 이는 후에 프라이버시법의 골간을 이루게 되었다.

1974년 하반기에 들면서 연방의회는 그간의 논의를 토대로 마련된 프라이버시법안을 심의하게 되었고, 프라이버시 법안 가운데 권리보호에 엄격한 상원안 S.3418과 규제가 완화된 하원안 H.R. 166373이 각각 원내에서 압도적인 다수의 찬성을 얻어 통과되었다. 그러나 이 두안의 내용에는 상당한 차이가 있어서 양원협의회를 거쳐야 했지만, 회기가 만료되기 전에 입법을 완료하려는 양원의 의지가 강하게 반영되어 1974년 12월 31일에 결국 프라이버시법(Privacy Act)이 공포되기에 이르렀다(Pub. L. No. 93-579, 88 Stat. 1896).⁴⁰³⁾ 1966년의 정보공개법(Freedom of Information Act)⁴⁰⁴⁾이 행정기관의 문서에 대한 국민들의

403) 법제처, 『각국의 개인정보보호관계법』(법무자료 제150집, 1989), 33-34면; 이관기, 『알 권리와 프라이버시』(한국교육문화원, 1993), 119면 등 참조.

404) 5 U.S.C. § 552. “Public information; agency rule, opinion, orders, records, and pro-

접근을 보장하기 위하여 제정되었던 반면에, 1974년의 프라이버시법(Privacy Act)⁴⁰⁵은 개인에게 민감한 문서가 일반대중에게 공개되는 것을 방지하기 위하여 제정되었다. 이러한 프라이버시법은 명칭상 프라이버시 일반에 관한 보호입법인 듯한 인상을 주고 있다. 그러나 “개인에 관하여 보유된 기록(Records maintained on individuals)”라는 표제가 붙어 있음을 감안한다면, 동법은 행정기관이 보유하는 개인정보에 관한 보호를 목적으로 하는 이른바 개인정보보호에 관한 법이라고 할 수 있다. 동법은 연방의 행정기관에 의한 개인정보의 공개에 제한을 두고 있으며, 이를 공개할 경우 본인에게 액세스권을 보장하고 있다. 그리고 개인에 관한 정보의 수집에 제한을 두어 필요최소한으로 정보를 보유할 것, 수집은 가능한 한 본인으로부터 수집할 것 등을 의무로 하고 있다. 또한 정보의 보유에 관해서는 정확성 및 비밀유지 등의 규제를 가하고 있다.

동법은 1988년의 Computer Matching and Privacy Protection Act⁴⁰⁶에 의하여 컴퓨터연결프로그램(computer matching program)에 이용하기 위한 개인정보의 제공을 제한하는 내용들⁴⁰⁷이 추가되었다.⁴⁰⁸

(2) 프라이버시법의 적용범위

동법에 의하여 보호를 받는 대상은 행정기관이 관리하는 기록시스템에 포함되어 있는 모든 기록, 즉 행정기관이 개인에 관하여 보유하는 기록이다. 개인에 관하여 보유된 기록(Records maintained on individuals)의 구체적인 의미에 대해서는 정의규정을 두고 있는데, 이에 의하면 “개인(individual)”은 미국의 시민이나 영주권을 합법적으로 취득한 외

ceedings”.

405) Pub. L. No. 93-579. 5 U.S.C. § 552a. “Records maintained on individuals”.

406) Pub. L. No. 100-503.

407) 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o), (p), (q), (u) 등.

408) 이호룡, “각국의 개인정보보호법제 동향 - 개인정보보호법의 제정 논의에 즈음하여 -”, 『인터넷법률』 제8호(법무부, 2001. 9), 154면 참조.

국민을 의미하고(§ 552a(a)(2)), “보유(maintain)”는 보관·수집·이용이나 유포를 포함하며(§ 552a(a)(3)), “기록(record)”은 “행정기관이 보유하고 있는 개인에 관한 정보의 모든 항목 혹은 그것이 수집되거나 집합된 것을 의미한다. 여기에는 학력·금융거래·의료병력·전과기록·취업경력 등이 포함되나 이에 한정되는 것은 아니며, 개인의 성명, 식별번호나 기호 혹은 지문, 聲紋(voice print) 또는 사진 등과 같이 신원을 확인할 수 있는 특기사항을 포함한다(§ 552a(a)(4)).

또한 “기록시스템(system of records)”은 행정기관이 보유하는 기록의 집합으로서 정보가 개인의 이름이나 식별번호, 기호 기타 개인에게 배정된 신원확인을 위한 특기사항에 의하여 검색되는 것을 말한다(§ 552a(a)(5)). 이것은 자동처리된 것이든 수작업에 의한 것이든 불문한다.

이처럼 일정한 기록시스템으로 동법의 적용범위를 한정시킨 것은 어떻게든 검색된 자료들을 모두 보호의 대상으로 삼을 경우 행정기관의 부담이 과도할 수 있을 뿐만 아니라 국민의 알권리를 보장하려는 정보공개법과의 조화를 모색하지 않을 수 없는 사정이 반영된 결과라고 할 수 있다.⁴⁰⁹⁾

동법의 적용을 받는 “행정기관(agency)”에 대해서는 모든 행정관청, 군사관청, 정부법인, 정부관리법인, 기타 연방정부의 행정기관(대통령 직속 사무국 포함) 및 모든 독립규제위원회를 의미한다는 정보공개법의 ‘행정기관’에 관한 규정(§ 552(f)(1))⁴¹⁰⁾을 준용하여 정의하고 있다 (§ 552a(a)(1)).⁴¹¹⁾ 이들 가운데 일부 행정기관의 장은 특정 기록에 대한 동법의 적용을 면제하는 규칙을 제정하여 공포할 수 있는데, 이 경우 행정기관은 그 규칙에서 면제사유를 설명하여야 한다(§ 552a(j)). 동

409) 법제처, 『각국의 개인정보보호관계법』 (법제자료 제150집, 1989), 37-38면 참조.

410) <<http://www4.law.cornell.edu/uscode/5/552.html>> 참조.

411) “agency” ... includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

법적용이 명시적으로 면제되는 기록으로는 중앙정보국(Central Intelligence Agency; CIA)이 보유하는 기록, 범죄예방이나 수사 혹은 형벌의 집행을 담당하는 기관이 보유하는 기록⁴¹²⁾ 등이 있다(§ 552a(j)(1), (2)).

(3) 프라이버시법의 주요 규율사항

연방 프라이버시법에서는 목적구속성과 정보의 직접수집 등을 규정하고(§§552a(e)(1)-(3)), 기록의 정확성·완전성 유지, 기록시스템의 고시 등(§§552a(e)(5)-(10)), 자기정보의 열람과 정정(§§552a(d)), 컴퓨터결합(computer matching)을 위한 정보제공의 제한(§§552a(o)-(q)),⁴¹³⁾ 개인정보의 공개 제한(§§552a(b)-(c)), 형사처벌과 손해배상(§552a(g)), 예산관리처(§552a(v))에 의한 감독 등을 규정하고 있다.⁴¹⁴⁾

3. 기타 공공부문에서의 개인정보보호 입법

그 밖에도 개별 분야별로 정부와 행정기관에 의한 개인정보의 취득에 제한을 가하는 연방차원의 법률들이 상당수 제정되어 왔다.

예컨대 금융기관이 보유하는 개인정보의 보호를 위하여 1978년의 금융프라이버시권법(Right to Financial Privacy Act)을 제정하였다. 이 법률은 금융기관보유의 개인정보에 대한 정부의 액세스를 원칙적으로 금지하되, 정부가 그 비밀보장을 전제로 할 경우에만 그에 대한 액세스를 허용하고 있다.⁴¹⁵⁾ 그리고 도청 등과 관련하여서는 연방통신법(Telecommunication Act)이 누구라도 송신자의 동의 없이 유선으로 통신을 감청하거나 그 존재나 내용 등을 타인에게 누설하지 못하도록 규정하고 있으며,⁴¹⁶⁾ 1968년의 ‘범죄방지와 가두의 안전을 확보하기

412) *Doe v. FBI*, 936 F. 2d 1346 (D.C. Cir. 1991).

413) 이는 1988년의 ‘컴퓨터매칭 및 프라이버시보호법(Computer Matching and Privacy Protection Act)’에 의하여 추가된 것이다.

414) 이에 관한 자세한 내용은 <<http://www.usdoj.gov/oip/privstat.htm>>을 참조할 것.

415) 12 U.S.C. §§ 3401-3422.

416) 47 U.S.C. § 605.

위한 종합법률’에서 유선통신 및 무선통신에 관한 감청을 원칙적으로 금지하되, 예외적으로 허용되는 수사기관의 전화감청에는 영장을 발부받을 것을 요하고 있다.⁴¹⁷⁾ 이러한 보호는 1986년의 전자통신프라이버시법(Electronic Communications Privacy Act, ECPA)⁴¹⁸⁾에 의해 전자통신에도 확대되어 있으며, 감청의 방법에 관해서도 “기타의 취득”으로 규정함으로써 널리 금지의 범위를 확대하였다. 또한 1980년의 프라이버시보호법(Privacy Protection Act, PPA)은 보도기관에 종사하는 자에 대한 수사·압수를 원칙적으로 금지하고, 나아가 보도기관 종사자와 그 정보원의 프라이버시를 보호하고 있다.⁴¹⁹⁾ 그리고 1988년의 비디오프라이버시보호법(Video Privacy Protection Act, VPPA)은 대역비디오의 정보에 대한 압수·수색에 필요한 영장의 요건을 엄격하게 규정하고 있다.⁴²⁰⁾

한편, 전과정보와 관련하여 연방수사국과 주의 당국이 정보를 공유하는 시스템을 허용하면서도, 수사 이외의 목적으로 전과정보를 이용하는 경우 그 이용방법 등에 대한 제한규정을 두고 있다.⁴²¹⁾

또한 정보의 개시·제공과 관련해서도 프라이버시에 대한 배려를 하고 있다. 즉, 1966년의 정보공개법(Freedom of Information Act, FOIA)은 공개하는 것이 프라이버시에 대해 명백히 부당한 침해가 되는 경우에는 정보공개 의무의 예외를 인정하고 있다. 또 법집행기관의 기록에 포함되어 있는 것과 같은 프라이버시에 관해서는 보다 넓게 비공개를 인정하고 있다.⁴²²⁾

그리고 1978년의 성범죄피해자의 프라이버시보호법(Privacy Protection for Rape Victims Act)은 성폭행사건에서 피해자의 과거의 성관계 등에

417) U.S.C. Title18 Chapter 119 Wire and Electronic Communications Interception and Interception of Oral Communications.

418) 18 U.S.C. §§ 2510-2522, 2701-2711.

419) 42 U.S.C. § 2000 aa.

420) 6 U.S.C. § 2710.

421) 42 U.S.C. § 14611.

422) 5 U.S.C. § 552. <<http://www4.law.cornell.edu/uscode/5/552.html>> 참조.

관한 증거를 배제함으로써 피해자의 프라이버시를 보호하고 있다.

4. 민간부분에서의 개인정보보호

민간부분에서의 개인정보보호에 관하여 포괄적인 입법은 존재하지 않는다. 다만 개별적인 영역에서 그때그때의 필요에 따라 보호입법이 제정되어 왔다.

그러나 이러한 입법적 규율에까지 이르지 못한 영역에 있어서는 사업자의 자율적인 규제에 맡겨져 있다. 이하에서는 민간에서의 개인정보보호를 위한 입법례를 제정의 순서대로 살펴보기로 한다.⁴²³⁾

[표 3-1-3] 민간부분에서의 개인정보보호입법

구 분	개인정보 관련법
금융부문	· 공정신용조사법(Fair Credit Reporting Act, 1970) · 금융프라이버시권법(Right to Financial Privacy Act, 1978) · 금융현대화법(The Financial Modernization Act of 1999)
통신부문	· 케이블통신정책법(Cable Communications Policy Act, 1984) · 전자통신프라이버시법(Electronic Communications Privacy Act, 1986) · 전기통신법(Telecommunications Act, 1996)
교육부문	· 가족의교육권및프라이버시에관한법률 (Family Educational Rights and Privacy Act, 1974)
의료부문	· 건강보험책임법(HIPPA, Health Insurance Portability and Accountability Act, 1996)
비디오감시	· 비디오프라이버시보호법(Video Privacy Protection Act, 1988)
근로자정보	· 근로자기록보호법(Employee Polygraph Protection Act, 1988)
기타	· 운전자프라이버시보호법(Driver's Privacy Protection Act, 1994) · 아동온라인프라이버시보호법(Child Online Privacy Protection Act, 1998)

423) 이하: Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," *Stanford Law Review* 53, pp. 1440-1444 참조.

구 분	개인정보 관련법
-----	----------

(1) 공정신용조사법

1970년에 제정된 공정신용조사법(Fair Credit Reporting Act, FCRA)은 소비자의 신용 등에 관한 조사기관의 보고에 관해서 보고가 허락되는 목적과 사항을 제한하고, 소비자의 접근권을 보장하고 있다.⁴²⁴⁾

동법은 통상적으로 제3자에게 소비자에 관한 기록들을 제공할 목적으로 소비자신용에 관한 정보를 수집하거나 평가하는 일에 종사하는 신용조사기관에게 여러 가지 의무들을 부과한다.⁴²⁵⁾ 이러한 개인기록에는 영업적 신용기록도 포함되지 않고, 조사기관의 요구들에 의하여 준비되는 보험기록에 관한 요구들도 포함되지 않는다. 그리고 동법은 정보주체에게 정보를 제공할 의무를 부과하는 동시에, 신용조사기관으로 하여금 ① 이러한 기관이 보유하고 있는 파일들 속에 있는 모든 정보의 내용, ② 소송이 관련되지 않는 한 조사기록들의 출처를 제외한 정보에 관한 기타 다른 출처, ③ 6개월 이내 소비자기록을 획득한 사람의 명단⁴²⁶⁾ 등을 공개하도록 하고 있다. 또한 정보주체에게 해당 정보가 정확하지 않을 경우 그에 대한 정정을 요구할 수 있도록 하고 있다.⁴²⁷⁾ 이러한 정정의 요구에 대하여 신용조사기관은 재조사를 실시하여 문제된 정보의 현재 상황을 기록하고 그 정보가 더 이상 유효하지 않거나 정확하지 않을 경우 해당 기관은 해당 정보를 삭제하여야 한다. 정보가 삭제되지 않을 경우 정보주체는 100단어를 넘지 않는 한도 내에서 그에 관한 해명을 할 수 있는 기회가 부여되고, 이러한 정보주체의 해명은 장래의 보고서에 기록되어야 한다.⁴²⁸⁾ 이러한 신용

424) 15 U.S.C. §§1681a-1681u

425) 15 U.S.C. §1681a(f)

426) 15 U.S.C. §1681g.

427) §1681i.

428) §1681i(b), (c).

기록의 사용자들은 위 조사기관의 정보에 근거하여 반대되는 결정을 내릴 때 이러한 정보주체에게 통지를 해야 한다. 관련자의 요구에 따라 위 기록들의 사용자는 신용기록들에 동반되지 않은 반대되는 결정들을 내렸을 때 이에 관한 근거를 관련자에게 공개해야 한다.⁴²⁹⁾ 그리고 동법은 권한 없이 정보를 받는 사람에 대한 처벌규정을 두고 있다.⁴³⁰⁾ 만일 이상의 규정에 위반하는 경우에는 민사책임을 지게 되는데, 이에 관해서는 연방거래위원회(FTC)가 집행권한을 가지고 있다.

하지만 동법은 신용조사기관이 정보를 부차적으로 이용하거나 공개하는 것에 대하여 적절히 대응하지 못하는 한계를 보여주고 있다. 신용조사회사가 신용기록의 “credit header” 부분(성명, 주소, 이전 주소, 전화번호, 사회보장번호, 고용정보, 생일 등)을 다양한 상업적 경제주체들에게 판매하는 것을 용인하고 있다. 이는 신용조사업계의 효과적인 로비가 영향을 미친 결과로 짐작되고 있다.⁴³¹⁾ 아무튼 FCRA는 개인과 신용조사회사간의 불균형적인 역학관계를 평등하게 해결하지는 못했다는 평가를 받고 있다.⁴³²⁾

(2) 가족의 교육권 및 프라이버시에 관한 법률

1974년의 가족의 교육권 및 프라이버시에 관한 법률(Family Educational Rights and Privacy Act, FERPA)⁴³³⁾은 일명 “Buckley Amendment”로도 알려져 있는데, 이 법에서는 연방의 보조를 받는 모든 교육기관과 조직에 교육상의 기록을 보호자에게 열람할 수 있도록 하면서도, 학생과 학부모의 동의 없이 그 기록을 공개하거나 제3자에게 제공하는 것을 제한하고 있다.⁴³⁴⁾ 하지만 그 적용범위는 교육분야에 한정되며, 그 가운

429) §1681m.

430) §1681q, r.

431) Priscilla M. Regan, *Legislating Privacy* (1995), p. 101.

432) Daniel J. Solove, *op. cit.*, pp. 1440-41.

433) Pub. L. No. 93-380, 88 Stat. 484. (codified at 20 U.S.C. § 1232g (2000)).

데서도 일부의 기록만을 대상으로 하고 있을 뿐이다. 교육공무원⁴³⁵⁾에 의해 보유되는 기록 및 건강기록과 심리적 기록은 제외된다.⁴³⁶⁾

(3) 금융프라이버시권법

1978년의 금융기록프라이버시법(Financial Records Privacy Act, FRPA)은 법에 규정된 경우를 제외하고는 행정기관이 금융기록들을 획득하는 것을 금지한다.⁴³⁷⁾ 예외가 인정되는 기관들은 은행을 감독하는 기관, 내국세수입국(Internal Revenue Service) 등이다. 금융기록들은 금융기관과 소비자간 관계를 담고 있는 금융기관에 의하여 보관되는 기록정보로 정의된다. 이러한 기록에는 개인소비자에 관한 기록만이 포함된다. 금융기관이란 은행, 저축은행(savings banks), 수신여신협회(savings and loan associations), 신용조합(credit unions), 소비자금융기관, 신용카드발급업자를 포함하는 것으로 정의된다.⁴³⁸⁾ 정부기관은 국가기관이나 공무원, 그 고용인을 뜻한다.⁴³⁹⁾ 소비자는 이러한 정보의 공개에 동의할 수는 있으나, 이러한 정보가 이러한 금융기관의 업무활동조건으로서 공개하도록 요구될 수는 없다.⁴⁴⁰⁾ 다만 이러한 기록들이 정당한 범집행을 위하여 구해진다고 믿을 만한 이유가 있거나 이러한 기록의 복사가 소비자를 위한 것이거나 금융기관에 봉사하는 경우에만 행정상 명령이나 소환장에 따라서 이러한 기록들은 공개될 수 있다.⁴⁴¹⁾ 또한 연방형사절차규칙에 따른 영장발부를 위하여 이러한 기록들이 획득될 수 있다.⁴⁴²⁾ 그래서 이러한 기록들의 공개는 영장이나 다른 합법적으

434) 20 U.S.C. §1232g.

435) 20 U.S.C. § 1232g(a)(4)(B)(ii)(2000).

436) § 1232g(a)(4)(B)(iv).

437) 12 U.S.C. §3402.

438) §3401(1).

439) §3401(3).

440) §3401(a), 3404(b).

441) §3405.

442) §3406.

로 요구되는 범위를 넘어서는 안 된다.

그리고 보험회사나 보험정보의 수집기관들은 이들이 소유하거나 통제하는 보험거래를 위하여 기록한 개인정보를 해당 개인이 이용할 수 있도록 해야만 한다. 이에 따라서 관련개인은 보험회사나 다른 보험정보수집기관들이 갖고 있는 자신에 관한 정보의 공개를 서면으로 요구할 수 있다. 이렇게 정보주체가 요구하는 경우에 해당 보험회사나 다른 보험정보수집기관들은 보통 30일 이내에 이러한 요구에 응답해야만 한다. 관련개인이 개인정보를 요구할 때 신청자와 보험계약자는 보험회사나 다른 보험정보수집기관들의 기록으로부터 본인에 관한 정보를 수정, 개정, 삭제하도록 요구할 수 있으며 보험회사나 다른 보험정보수집기관들은 30일 이내에 이러한 개인의 요구에 응답해야만 한다. 또한 보험회사나 다른 보험정보수집기관들이 개인정보를 수정, 개정 또는 삭제한다면 해당 개인에게 이에 관하여 서면으로 통지해야만 한다. 보험회사나 다른 보험정보수집기관들이 위에서 언급된 개인의 요구를 거절한다면 개인에게 거절, 거절이유, 이에 관한 개인의 진술권, 심사를 요구할 개인의 권리를 통지해야만 한다. 이러한 진술권은 개인이 동의하지 않는 정보에 관한 것으로서 보험회사나 다른 보험정보수집기관들은 이를 정리해야만 한다. 이들 회사나 기관이 일단 개인으로부터 진술을 받은 한, 개인자신의 기록들 속에 이렇게 논란이 되는 개인정보에 관한 진술을 기록, 정리하고 이러한 자료를 나중에 살펴보고 접근할 수 있도록 해야만 한다. 논란이 되는 정보를 계속적으로 공개할 때 보험회사나 다른 보험정보수집기관은 논쟁이 되는 문제를 분명하게 확인하고, 이러한 개인의 진술을 공개되는 정보와 함께 제공해야만 한다. 추가로 이들 회사나 기관들은 과거에 이들로부터 해당개인에 관하여 정보를 받은 기관이나 회사들에게 이러한 새로운 진술을 해야 한다. 일반적으로 보험회사나 다른 보험정보수집기관

들은 보험거래와 연결되어 수집되거나 접수된 개인에 관한 정보를 공개할 수 없다. 그러나 이러한 규정은 아주 많은 예외들 밑에 있기 때문에 이러한 예외가 허용되려면 정보의 가능한 수령자 및 어떤 목적으로 정보들이 공개될 수 있는지를 구체화한다. 그리고 정보가 제공되고 어떤 상황에서 정보가 제공되는지를 개인에게 일반적으로 통지해야만 한다. 그리고 공개에 관한 또 다른 제한은 해당개인에 의한 승인이다. 일반적으로 보험회사나 보험정보수집기관은 개인에 의하여 공개가 승인된 정보만을 공개할 수 있다.⁴⁴³⁾

(4) 케이블통신정책법

1984년의 케이블통신정책법(Cable Communications Policy Act, CCPA)⁴⁴⁴⁾은 개인을 식별하는 정보에 관해서는 가입자에 대한 고지의무를 두고 있다.⁴⁴⁵⁾ 또 가입자의 동의가 없는 한 가입자의 시청습관을 드러내는 일체의 정보를 사업자가 수집하거나 개시하지 못하도록 하고,⁴⁴⁶⁾ 가입자에게 정보에 대한 액세스권을 보장하면서 정보의 삭제도 요구할 수 있도록 하고 있다. 이에 대한 위반행위는 소송의 대상이 된다.⁴⁴⁷⁾

하지만 그 법령은 단지 유선방송운영자에게만 적용되며 개인적 자료가 “정당한 영업활동”을 위해 공개될 수 있는 폭넓은 예외를 두고 있다.⁴⁴⁸⁾ 그럼에도 불구하고 동법은 소비자들에게 자신의 유선방송 관련기록에 대한 통제권을 부여하는 최초의 시도라고 할 수 있다.⁴⁴⁹⁾

443) 이상 김일환, 『개인정보보호법제의 정비방안에 관한 연구』 (한국법제연구원, 1997), 130- 131면.

444) 47 U.S.C. § 551 (2000).

445) § 551(a)(1).

446) § 551(c)(2)(C)(ii).

447) § 551(f)(1).

448) § 551(c)(2)(A).

449) Daniel J. Solove, *op. cit.*, p. 1441.

(5) 전자통신프라이버시법

1986년의 전자통신프라이버시법(Electronic Communications Privacy Act, ECPA)⁴⁵⁰⁾은 1968년의 Federal Wiretap Act⁴⁵¹⁾의 보호를 무선전화, 이메일 혹은 기타 컴퓨터 전송수단을 포함하여 새로운 형태의 목소리, 정보, 비디오통신에까지 확대하였다.

동법은 정보서비스제공자 및 관리인에게 개인의 프라이버시보호에 관한 의무를 부과하고 있다. 그리고 통신도청을 범죄로서 처벌하고 있으며,⁴⁵²⁾ 특히 전자통신을 도청하기 위해서는 영장을 받도록 규정하고 있다. 또한 전자통신서비스사업자에게도 통신내용을 외부로 개시하는 것을 금지하고 있으며,⁴⁵³⁾ 축적된 통신에 대한 부정한 액세스를 금지하고 있다.⁴⁵⁴⁾

이 축적된 통신에 대한 액세스 금지규정은 1988년의 비디오프라이버시보호법(Video Privacy Protection Act)으로 개정되어 새롭게 비디오 테이프 대여·판매업자가 그 기록을 부당하게 개시하는 것을 금지하고 위반행위에 대해 민사상의 책임을 지우고 있다.⁴⁵⁵⁾

하지만 동법에서는 개인정보의 수집과 이용에 대해서는 특별히 제한을 가하지 않고 있다. 나아가 인터넷서비스의 제공은 동법의 적용에서 면제된다. 그 결과 가입자의 이메일을 조사하는 것은 자유롭다.⁴⁵⁶⁾

450) 18 U.S.C. §§ 2510-2522, 2701-2709, 2711 (2000).

451) 1968년에 연방의회는 Title III of Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-20 (흔히 “Title III” 혹은 “The Federal Wiretap Act”로 지칭)을 입법화하였다. 이 법은 연방, 주, 민간의 전자적 대화감시에 대한 규율대상을 전국으로 확대한 것이었다.

452) 18 U.S.C. §2510.

453) 18 U.S.C. §2511.

454) 18 U.S.C. §2701.

455) 18 U.S.C. §2710.

456) Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) : “§ 2701(c)(1)은 서비스제공자들이 전자저장장치에서 통신에 접근할 경우 그들이 원하는 대로 할 수 있도록 허용한다.”

(6) 비디오프라이버시법

1988년의 비디오프라이버시법(Video Privacy Protection Act, VPPA)⁴⁵⁷⁾은 흔히 “Bork Bill”로 알려지고 있는데, 그것은 연방대법원판사 지명자인 Robert Bork의 비디오카세트 대여기록이 어떤 신문기자의 손에 들어간 것이 입법의 직접적인 계기가 되었던 데서 연유한다. VPPA는 비디오테이프 서비스제공자가 비디오카세트 대여 혹은 구입의 제목과 같은 개인정보를 개인의 서면동의를 받지 아니하고 고의로 공개하는 것을 금지하고 있으며,⁴⁵⁸⁾ 이에 반하는 행위를 소송의 대상으로 인정하고 있다.⁴⁵⁹⁾ 그러나 VPPA는 단지 비디오카세트테이프에만 적용될 뿐이고,⁴⁶⁰⁾ 서점, 레코드가게, 기타 형태의 소매점, 잡지출판사, 혹은 카탈로그회사에는 비슷한 제한을 전혀 두지 않고 있다.

(7) 전화소비자보호법

1991년의 전화소비자보호법(Telephone Consumer Protection Act, TCPA)⁴⁶¹⁾은 텔레마케팅에 대해서 소비자의 프라이버시를 보호하기 위하여 자동전화 시스템과 팩스를 사용하여 권유전화를 하는 것에 제한을 두고 있으며, 가입자의 프라이버시를 보호하기 위한 규제도 두고 있다.⁴⁶²⁾ 동법은 거부의를 밝혔음에도 불구하고 통신판매인의 전화가 계속될 경우 개인은 그 통신판매인을 상대로 500달러 이하의 손해배상을 청구하는 소송을 제기할 수 있도록 하고 있다.⁴⁶³⁾ 만일 그 통신판매인에

457) Pub. L. No. 100-618, 102 Stat. 3195, (codified at 18 U.S.C. §§ 2710-11 (2000)).

458) 18 U.S.C. § 2710(b) (2000).

459) §§ 2710(b)(1), (c)(1).

460) §§ 2710(a)(4), (b).

461) Pub. L. No. 102-243, 105 Stat. 2394, (codified at 47 U.S.C. § 227 (2000)).

462) 47 U.S.C. §227.

463) 47 U.S.C. § 227(c)(5) (2000).

게 고의성이 있으면, 그 손해의 3배에 해당하는 금액을 배상하도록 하고 있다.⁴⁶⁴⁾

하지만 동법은 파괴적인 전화의 피해를 구제하는 것을 목적으로 하고 있기 때문에, 개인적 자료의 수집, 사용이나 판매에 대해서는 규율하지 않고 있다.

(8) 운전자프라이버시보호법

1994년의 운전자프라이버시보호법(Driver's Privacy Protection Act, DPPA)⁴⁶⁵⁾은 자동차기록에 담긴 개인정보를 판매하는 많은 주의 오랜 관행에 제동을 걸고 나섰다. 동법은 자동차관련 개인정보를 판매상들에게 제공하기 전에는 반드시 운전자의 동의를 얻도록 하였다.⁴⁶⁶⁾ 하지만 그것은 단지 자동차기록의 상황에서만 적용될 뿐이다. 주는 그들이 보유하고 있는 무수한 가타 형태의 기록들 속에 포함되어 있는 정보를 공개함에 있어 제한을 받지 않고 있다.

(9) 텔레커뮤니케이션보호법

1996년의 텔레커뮤니케이션보호법은 통신법을 상당 부분 개정하였는데, 거기에서는 텔레커뮤니케이션 사업자에게 소비자정보의 보호를 의무화하고 있다. 이에 따라 사업자는 일정한 정보에 관하여 비밀유지의 의무를 지게 되며, 이용자에게는 개시청구권이 보장되고, 또 가입자의 리스트를 제공하는 등 제한을 두고 있다.⁴⁶⁷⁾

464) *Id.*

465) 18 U.S.C. §§ 2721-2725 (2000).

466) 18 U.S.C. § 2721(b)(12). 동법은 최근 연방주의(federalism)의 도전에 대응하여 연방대법원의 지지를 받았다. *Reno v. Condon*, 528 U.S. 141 (2000) 참조.

467) 47 U.S.C. §222.

(10) 건강보험책임법

1996년의 건강보험책임법(Health Insurance Portability and Accountability Act, HIPAA)⁴⁶⁸⁾에서는 의료분야에 관련되는 개인정보의 문제를 규율하고 있다. 동법은 보건후생부(HHS)로 하여금 의료기록에 관한 프라이버시를 통제하기 위한 행정입법을 제정하도록 규정하고 있다.⁴⁶⁹⁾ 이에 따라 보건후생부는 치료, 보상 혹은 수술의 목적을 벗어난 모든 사용과 공개에는 위임을 요한다는 명령을 공포하였다.⁴⁷⁰⁾

(11) 아동온라인프라이버시보호법

1998년의 아동온라인프라이버시보호법(Children's Online Privacy Protection Act, COPPA)⁴⁷¹⁾은 인터넷상에서 아동의 개인정보를 수집하는 행위를 규율하는 법률이다.⁴⁷²⁾ 이는 사이버스페이스에서의 프라이버시를 직접적으로 취급하는 최초의 연방입법이라 할 수 있다.

동법에 의하면 아동을 겨냥한 웹사이트는 프라이버시정책을 게시하여야 하고,⁴⁷³⁾ 서비스제공자는 아동으로부터 개인정보를 수집하거나 이를 사용 혹은 공개하기 전에 “부모의 진정한 동의”(verifiable parental

468) Pub. L. No. 104-191, 110 Stat. 1936 (1996).

469) 110 Stat. at 2033-34.

470) 45 C.F.R. § 164.508(a)는 의료단체가 개인정보의 그와 같은 이용에 대한 개인의 위임에 관하여 자격을 제한하지 못하도록 하고 있다. 45 C.F.R. §164.508(b)(iv) 참조. 이 규정에 대해서는 Clinton 행정부의 말기에 최종적으로 승인이 이루어졌지만, Bush 행정부가 이 규정을 비난하고 그 적용을 연기하기로 약속한 바 있다. Robert Pear, “White House Plans to Revise New Medical Privacy Rules,” *N.Y. Times*, Apr. 8, 2001, at 22, 참조. 그러나 Bush 행정부는 최근에 들어 이 규정을 일단 시행하되 훗날 조정할 것이라고 발표하였다. Robert Pear, “Bush Accepts Rules to Guard Privacy of Medical Records,” *N.Y. Times*, Apr. 13, 2001, at A 1. 참조.

471) 15 U.S.C. §§ 6501-6506 (2000). 이에 관한 자세한 내용은 이인호, “아동온라인개인정보보호법과 그 효율적 집행방안”, 『법과 사회』 제20호(동성출판사, 2001), 245-269면 참조.

472) § 6502(a)(1).

473) § 6502(b)(1)(A)(i).

consent)를 얻어야 한다.⁴⁷⁴⁾ 동법은 부모의 동의를 획득하는 구체적인 절차와 방법에 대하여 이 법의 집행기관인 연방거래위원회가 규칙으로 정하도록 하고, 이 규칙을 위반하면 불법행위가 된다고 규정하고 있다.⁴⁷⁵⁾ 이러한 COPPA의 규정에 따라, 연방거래위원회는 1999년 10월 Children's Online Privacy Protection Rule을 공표하였다.

이에 의하면 아동을 상대로 하는 서비스 사업자에게는 인터넷상으로 아동들의 개인정보의 수집·사용에 관한 불공정한 행위와 사기적인 행위를 할 수 없도록 금지하면서, 프라이버시정책에 대한 고지(notice)에 포함되어야 할 내용⁴⁷⁶⁾과 부모의 동의(parental consent)를 획득하는 방법⁴⁷⁷⁾ 등에 대한 규정을 두고 있다.

그러나 이 법의 적용범위는 매우 제한적이다. 즉, COPPA는 단지 “어떤 웹사이트나 아동을 겨냥한 온라인서비스의 운영자, … 혹은 … 아동으로부터의 개인정보를 수집한다는 실질적 인식을 가진 운영자”에게만 적용된다.⁴⁷⁸⁾ 게다가 동법은 오로지 13세 이하의 아동으로부터 개인정보를 수집하는 웹사이트 운영자에게만 적용된다.⁴⁷⁹⁾

474) § 6502(b)(1)(A)(ii).

475) § 6502(b).

476) Rule § 312.4(b)(2)(iv). 제3자에 대한 제공의 경우 고지의 내용으로 정보가 제공될 제3자의 신원과 기업형태, 개인정보의 비밀성, 보안성, 완전성을 유지할 것을 약속했는지 여부, 부모동의의 거부가능성 등이 제시되고 있다. 이인호, 앞의 논문, 256면 참조.

477) Rule § 312.5. 부모의 동의를 획득하기 위한 방법으로 법정대리인에게 동의서를 제공하고 거기에 부모가 서명하여 우편이나 팩스로 서비스제공자에게 전달하는 방법, 특정의 온라인거래와 관련하여 부모가 신용카드를 사용하도록 요구하는 방법, 부모로 하여금 수신자부담의 무료전화를 하도록 하고 숙련된 응답직원을 통하여 동의를 확인하는 방법, 공개키기술(public key technology)을 이용한 디지털인증을 이용해서 동의를 받는 방법, 부모가 위에 열거한 방법 중의 하나를 통해 얻은 개인 식별번호(Personal Identification Number)나 패스워드가 딸린 이메일로 동의를 표시하는 방법 등을 제시하고 있다. 이인호, 앞의 논문, 259면.

478) § 6502(b)(1)(A).

479) § 6501(1).

(12) 금융지주회사 관련법

1999년의 금융지주회사 관련법, 일명 Gramm-Leach-Bliley Act⁴⁸⁰⁾는 합병되는 은행, 보험회사, 투자회사가 각 자회사들이 소유하고 있는 “사적인 개인정보(nonpublic personal information)”를 공유할 수 있도록 허용하고 있다. 자회사들은 고객에게 그들이 이러한 정보를 공유하고 있는지 설명해야 하지만, 개인이 이러한 정보의 공유를 차단할 방법은 없다. 개인은 자신의 정보를 제3자에게 공개하지 못하도록 할 수 있을 뿐이다.⁴⁸¹⁾ 오늘날 매우 활발하게 이루어지고 있는 기업간의 결합이나 합병 등을 생각할 때, 이러한 정보의 공유에 대한 규제로서는 매우 미흡한 입법이라고 할 수 있다.⁴⁸²⁾

5. 자율규제론과 세이프하버 원칙

(1) 자율규제론

최근 특히 문제가 되고 있는 것은 인터넷상의 프라이버시의 보호, 특히 전자상거래와 프라이버시의 보호이다. 이 점에 관하여 미국에서는 기본적으로 사업자의 자율규제로 미루는 경향을 보이고 있다.⁴⁸³⁾

연방거래위원회는 1996년 6월 ‘Consumer Protection in New Hi-tech Global Market’라는 제하의 보고를 제출하고 사이버-스페이스에서 프라이버시 침해의 위험성에 주의를 촉구하였으며, 그 후에도 1998년 6월에는 ‘On-line Privacy’ 1999년에 7월에는 ‘자율규제와 온라인의 프라이버시’라는 보고서를 연방의회에 제출한 바 있다. 또 2000년 6월 및 7월에 제출된 ‘온라인의 프로파일링에 관하여’라는 보고서에서는 자율

480) Pub. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. §§ 6801-6809 (2001)).

481) 15 U.S.C. § 6802(a), (b) (2001).

482) Daniel J. Solove, *op. cit.*, p. 1444.

483) 이호룡, 앞의 논문, 156면.

규제를 요구하면서 또 이것을 지원하기 위한 입법의 필요성을 강조하고 있다. 이 보고서에 따르면 다음과 같은 4 원칙을 강조하고 있다. ① 온라인에서 정보를 수집하고 이용하는 사업자는 소비자에게 그 행위를 고지할 것 ② 소비자에게는 그 행위를 면할 선택의 여지가 보장될 것 ③ 수집된 정보에 대해서는 소비자에게 액세스권과 진실성을 확인할 권리가 보장될 것 ④ 사업자에게는 정보의 비밀보호와 정확성 확보를 위한 조치 요구될 것 등이다. 또 이에 더하여 이를 집행하기 위한 실효성 있는 메카니즘이 필요함을 강조하고 있다.⁴⁸⁴⁾

또한 미국에서는 표준 프라이버시 준수 운영방안을 제시하고 일정 조건을 충족하는 업체에 “TRUSTe” 나 “BBB 온라인 마크”와 같은 인증마크를 부여하는 제도를 시행해 오고 있으며, 정부 및 비영리단체는 “Privacy Policy”를 작성하여 홈페이지에 게시함으로써 그들 기관의 개인정보취급방침 등에 관하여 자세히 설명하고 있다.⁴⁸⁵⁾

(2) 세이프하버원칙

한편 1998년 11월에 미국 상무부는 개인정보보호를 위한 세이프하버원칙(Safe Harbor Principles)을 제시하였다. 이 원칙을 충족하는 미국 기업은 EU 기준에 적합한 개인정보보호에 충실한 기업으로 추정되어 향후 아무런 제재없이 EU와의 개인정보를 이전할 수 있도록 하기 위한 것이었다. 이는 미국산업계에 개인정보보호에 과한 원칙을 자율적으로 준수할 것을 권고하는 것으로, 개인정보보호를 둘러싸고 빚어진 EU와의 통상마찰을 타개하기 위한 전략으로 활용되었다.

세이프하버 원칙에서는 수집하는 개인정보의 유형, 해당 정보의 수집방법, 당해정보의 수집목적, 조직체의 유형, 당해 조직체가 정보주

484) 이호룡, 앞의 논문, 157면.

485) 박광진 등, 『정보통신서비스에서의 개인정보보호에 관한 지침(안) 연구』(한국정보보호센터, 1999). 12. 7면.

체에게 당해 정보의 이용과 공개를 제한할 수 있는 선택권과 조치를 제공하고 있음을 알려주도록 규정하고 있다. 세이프하버원칙을 구체적으로 살펴보면 다음과 같다.⁴⁸⁶⁾

- ① 통지(notice) : 개인정보를 수집이나 이용하는 기관은 그 목적을 정보주체에게 알려주어야 하고 가능한 한 명확하고 용이한 용어를 사용해야 한다.
- ② 선택(choice) : 개인정보를 제3자에게 제공하는 경우 또는 원래의 수집 목적과 양립할 수 없는 목적으로 이용하는 경우에는 정보주체에게 선택권을 주어야 한다.
- ③ 이전성(onward transfers) : 기관이 제3자에게 정보를 제공하기 위해서는 통지와 선택의 원칙을 준수해야 한다.
- ④ 안전성(security) : 기관이 개인정보의 수집, 보유, 이용 또는 배포의 경우에 상실, 오용, 무단접근, 공개, 변경 및 파괴를 막을 합리적인 조치를 해야만 한다.
- ⑤ 정보의 무결성(data integrity) : 개인정보는 수집된 목적과 양립할 수 없는 용도로 이용되어서는 안 된다. 이를 위하여 기관은 정보가 의도된 이용, 정확성, 완전성 및 최신성에 신뢰할 수 있는 합리적인 조치를 해야 한다.
- ⑥ 접근(access) : 개인정보를 보유한 기관은 부정확한 정보에 대하여 정보주체에게 정정, 삭제할 수 있는 접근을 허용해야 한다. 이 원칙은 OECD의 가이드라인상의 개인참여의 원칙보다 좁게 개인의 참여를 보장하는 것으로, 부정확한 정보의 경우에만 이를 삭제할 권리를 허용하고 있다.
- ⑦ 실행(enforcement) : 위의 원칙을 준수하기 위하여 제도적 장치를 마련하고 기관의 준수를 보증할 만큼 제재는 적절해야 한다.

486) 현대호, 『인터넷상의 정보보호에 관한 법제연구』 (한국법제연구원, 2000), 31-32면.

6. 전자정부법상 프라이버시영향평가제도

(1) 개 요

미국은 2002년 12월 공포된 ‘전자정부법’(E-Government Act of 2002)⁴⁸⁷⁾에서 국민 중심의 전자정부를 구현하는 과정에서 개인정보 및 프라이버시가 충분히 보호될 수 있도록 프라이버시 영향평가(Privacy Impact Assessment)를 실시할 것을 명문화하였다(제208조). 이 제도는 각종 전자정부 사업을 추진함에 있어 당해 사업이 프라이버시에 미치는 영향을 사전에 조사함으로써 전자정부 사업에 따른 국가기관에 의한 프라이버시 침해를 최소화하는 데 그 의의가 있다.⁴⁸⁸⁾

(2) 구체적 내용

프라이버시 영향평가는 ① 신원확인이 가능한 정보를 수집·유지·관리·유포하기 위해 정보기술을 개발하거나 조달하는 경우, ② 정보기술을 이용하여 수집·유지·관리·유포될 정보를 새로이 수집하는 경우, ③ 연방정부기관, 그 대행기관 또는 직원을 제외한 10인 이상의 자에 대하여 신원확인에 관한 문제가 제기되거나 신원에 관한 보고의 무가 부과되는 경우에 특정 개인에 대하여 물리적 또는 온라인 접촉을 허용하는 신원확인이 가능한 모든 정보 등을 새로이 수집하는 등의 업무를 수행하기 전에 실시하여야 한다(§208(b)(1)(A)).

예산관리처장은 지침을 통해 평가되는 정보시스템의 규모, 당해 시스템에서 개인을 식별할 수 있는 정보의 민감성, 당해 정보의 무단 공개로 초래되는 위험 등에 관해서 프라이버시 영향평가가 이루어지

487) Public Law No: 107-347.

488) 구병문, “캐나다 및 미국의 프라이버시 영향평가 제도 분석과 국내 전자정부 법 제로의 도입방향 검토”, 『정보화이슈분석』 03-16(2003. 7). 6면.

도록 해야 한다(§208(b)(2)(B)(i)). 그리고 영향평가에서는 수집할 정보, 당해 정보를 수집하는 이유, 당해 정보의 용도, 정보 공유의 기관, 수집되는 정보 내용과 이를 공유하는 방식과 관련하여 개인의 동의를 얻기 위한 고지 등의 절차, 정보보호 방안, 프라이버시보호법에 따른 기록체계의 생성 여부 등에 관한 사항을 다루도록 해야 한다(§208(b)(2)(B)(ii)).

(3) 평가기관 및 절차

전자정부 관련 사업을 수행하는 각 기관은 필요한 범위 내에서 프라이버시 영향평가를 수행해야 하며(§208(b)(1)(B)(i)), 당해 기관장의 결정에 따라 정보화책임관 또는 그에 준하는 공무원은 프라이버시 영향평가를 검토해야 한다(§208(b)(1)(B)(ii)). 전자정부기금의 출원이 필요한 시스템의 경우, 당해 기관은 이에 대한 프라이버시 영향평가서 1부를 예산관리처장에게 제출하여야 한다(§208(b)(1)(D)).

(4) 평가결과의 공개

위와 같은 대상에 대해 평가대상이 되는 정보체계의 규모, 당해 체계에서 신원확인을 가능하게 하는 정보의 민감성, 당해 정보의 무단 공개로 초래되는 위험에 관하여 평가하게 되는데, 평가의 결과는 가능한 범위에서 공개하도록 되어 있다(§208(b)(1)(B)(iii)). 다만 공개하는 경우에도 보안상 이유로 또는 프라이버시 영향 평가에 포함되어 있는 민감한 정보나 개인정보를 보호하기 위하여 공개에 관한 사항을 변경하거나 공개 자체를 배제할 수 있도록 하였다(§208(b)(1)(C)).

(5) 예산관리처장의 직무

예산관리처장은 기관의 프라이버시 영향 평가 수행을 위한 정책 및 지침을 개발하고, 범정부적으로 프라이버시 영향 평가의 시행을 감독

하며, 적절하다고 판단하는 범위 내에서 각 기관에 대해 기존 정보 체계나 신원확인이 가능한 정보의 지속적 수집에 관한 프라이버시 영향평가를 수행하도록 해야 한다(§208(b)(3)(C)).

7. 입법체계에 대한 평가

미국의 개인정보보호에 관한 입법은 사후적·점진적으로 이루어지고 있으며, 그 규율방식 또한 공공부문과 민간부문이 분리된 채 분야별 개별법주의에 입각해 있다. 따라서 개인정보보호에 관한 법률은 많이 존재하지만 충분한 보호는 담보되지 않고 있다고 지적되고 있다.⁴⁸⁹⁾ 앞서 살펴본 바와 같이 실제로 적용범위의 협소성으로 인한 법적 공백의 발생은 여러 군데서 눈에 띄고 있다. 예컨대 연방법률은 연방기관의 기록, 교육상의 기록, 케이블텔레비전의 기록, 비디오대여 기록 그리고 주의 자동차기록을 규율하지만, 주와 지방의 공무원들이 보관하는 대부분의 기록들뿐만 아니라 도서관, 자선단체, 슈퍼마켓, 백화점, 우편주문목록, 서점 등을 경영하는 상인들이 보유하는 다수의 기타 기록들을 커버하지 못한다.

그리고 여러 법률에서는 제한된 개인정보와 매우 제한적인 형태의 통제권만을 부여하고 있으며, 때로는 그러한 규정들마저 실효성을 담보하기 위한 장치를 확보하지 못하는 경우도 있다. 또한 개인정보의 유통이 복잡한 경로를 거쳐서 이루어지는 경우 그에 대한 법집행의 효율적 수단을 확보하는 데 어려움이 있다. 무엇보다도 개인정보가 언제 어디서 어떻게 수집·추적·유통되는지를 인식하는 것부터가 쉬운 일이 아니다. 설령 부당하게 그 정보가 취급되고 있다는 사실을 안다고 하더라도 관련 법률을 준수하지 않은 자가 정확히 누구인지를

489) Colin Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?," *Technology And Privacy: The New Landscape* 99, p. 113 (Phillip E. Agre & Marc Rotenberg eds., 1997).

밝혀내는 것은 매우 곤란한 때가 많다.⁴⁹⁰⁾

제 2 절 캐나다

1. 개인정보보호법제의 개관

캐나다는 당초 캐나다 인권법에 의거하여 1977년 공공부문의 개인정보보호에 관한 내용을 담은 개인정보보호규칙이 제정되어 운용되고 있었다. 이후 공공부문의 개인정보보호를 위한 별도의 법률은 1980년대 들어 제정되었고, 이 법의 주관기구인 개인정보보호기구도 이때부터 설립되었다. 캐나다의 정보보호 법제는 1982년에 공공부문에 적용되는 개인정보보호법이 먼저 제정되고, 민간부문에 적용되는 정보보호 법률들이 제정되었다. 캐나다의 법체계는 공공부문과 민간부문의 이원적 법체제로 운영되고 있다. 공공부문의 경우 연방차원의 법률이 제정되어 있지만, 각 주에서도 개인정보관련 법률을 별도로 제정하여 시행하고 있는데, 주 차원의 경우에는 각 주의 정부나 공공기관에 의해 처리되는 개인정보를 보호하기 위한 공공부문에 적용되는 법률만이 제정되어 있는 것이 일반적이다.

이하에서는 연방차원의 정부부문에 적용되는 일반법인 프라이버시법(The Privacy Act)과 민간부문에 적용되는 일반법인 ‘개인정보보호 및 전자문서에 관한 법률(PIPEDA : The Personal Information and Electronic Documents Act)’을 중심으로 검토한다.

2. 프라이버시법의 적용범위와 구성

1982년에 제정된 프라이버시법(Privacy Act)은 1983년 1월 1일부터 발효되었으며, 이후 1985년에 개정된 바 있다.⁴⁹¹⁾

490) Daniel J. Solove, *op. cit.*, pp. 1444-1445 참조.

491) <<http://laws.justice.gc.ca/en/P-21/index.html>> 참조.

이 법은 공공기관에 의한 정보처리과정에서 발생할 위험이 있는 개인정보 침해가능성에 대비하고, 공공기관에 의해 보유하고 있는 자신의 개인정보에 접근할 수 있는 시민들의 권리를 보장할 목적으로 제정되었다(제2조).

(1) 적용범위

동법은 약 150개의 연방행정기관에 개인정보의 수집, 사용, 공개를 제한함으로써 프라이버시권을 보장할 의무를 부과하고 있다.

한편, 동법에 의해 보호되는 “개인정보(personal information)”는 어떤 형식으로든 기록된, 신원을 확인할 수 있는 개인에 관한 정보를 말한다. 여기에는 (a) 개인의 인종, 국가·민족적 배경, 피부색, 종교, 연령 및 결혼 유무에 관한 정보, (b) 개인의 교육·건강·범죄·고용 기록에 관한 정보, 개인이 관련한 금융 거래와 관한 정보, (c) 개인에게 부여된 증명번호·기호 또는 기타 특정한 것, (d) 개인의 주소, 지문, 혈액형, (e) 법령에서 정한 정부기관 혹은 그 부서가 어떤 개인에게 보조금이나 상을 수여하도록 제안하는 사실 또는 개인적 의견 및 견해, (f) 개인이 정부기관에게 보낸 묵시적 또는 명시적인 사적인 비밀성의 통신문 및 원통신문의 내용을 공개할 수도 있는 통신문에 대한 정부기관의 응답, (g) 개인에 대한 타인의 견해 및 의견, (h) 법령에서 정한 기관 혹은 그 부서가 개인에게 보조금이나 상을 수여하도록 하기 위한 제안에 관한 타인의 견해 및 의견, (i) 개인과 관련된 다른 개인정보와 함께 표현되거나 이름 자체의 공개가 개인정보의 공개가 될 수도 있는 개인의 이름 등이 원칙적으로 포함된다.

하지만 정부기관의 공무원 혹은 피고용자이었던 개인에 관한 정보로서 개인의 직위 및 임무와 관련되는 정보, 수행한 활동과 관련된 정부기관과의 계약 하에 활동을 수행하는 중이거나 수행했던 개인에 관한 정보, 재정상의 재량 이득에 관한 정보, 사후 20년이 지난 개인

정보 등은 제외된다(제3조).

(2) 구 성

- 약 칭

제 1 조: 약칭

- 입법의 취지

제 2 조: 목적

- 해 석

제 3 조: 정의

- 책 임

제 3 조의1: 주무장관의 권한

- 개인정보의 수집·유지·처분

제 4 조: 개인정보의 수집

제 5 조: 개인정보의 직접수집

제 6 조: 개인정보의 보유

- 개인정보의 보호

제 7 조: 개인정보의 이용

제 8 조: 개인정보의 공개

제 9 조: 이용·공개기록의 보관

- 개인정보은행(Personal Information Banks)

제10조: 개인정보은행

- 개인정보색인(Personal Information Index)

제11조: 개인정보의 색인

- 개인정보의 열람(Access to Personal Information)

제12조: 열람권(right of Access)

제13조-제16조: 열람청구

제17조: 열람의 방식

- 면제(Exemptions)

제18조: 적용제외 은행(exempt banks)

제19조-제25조: 개인정보 공개의 거부

제26조: 타인의 개인정보

제27조: 법률서비스정보의 특권(Solicitor-Client Privilege)

제28조: 의료기록

- 진정(Complaints)

제29조: 진정

제30조: 서면청구

- 조사(Investigations)

제31조: 조사목적의 통지

제32조-제35조: 절차의 결정, 민간부분의 조사, 프라이버시감독관의 권한, 정보의 열람 등

- 적용배제 은행의 감독(Review of Exempt Banks)

제36조: 적용배제 은행의 조사

- 제4조-제8조의 준수 감독

제37조: 제4조 내지 제8조 준수의 심사

- 의회 보고서(Reports of Parliament)

제38조-제40조: 연차보고서, 특별보고서, 경과보고서

- 연방법원의 재심리

제41조-제52조: 연방법원의 재심리

- 프라이버시감독관의 직무

제53조-제67조: 프라이버시감독관(Privacy Commissioner)

- 위 반

제68조: 위반 (1,000달러 이하의 벌금 부과)

- 적용배제

제69조-제70조의1: 적용배제 (문학, 미술, 캐나다방송사, 추밀원 기밀 사항 등)

- 통 칙

제71조-제77조: 통칙 (주무장관의 임무 등)

- 부칙(Schedule)

- 정부기구

3. 개인정보보호 및 전자문서에 관한 법률

(1) 제정과 개정

2000년 4월 13일에 제정된 ‘개인정보보호 및 전자문서에 관한 법률’(Personal Information Protection and Electronic Documents Act, PIPEDA)은 연방차원에서 적용되는 민간부문의 개인정보보호 일반법이다. 이 법은 EU개인정보보호지침 등의 제정으로 인해 유럽과 동등한 수준의 개인정보보호 체계를 구비할 필요가 제기되었고, 정보사회가 진전되면서 민간부문에서 소비자의 개인정보의 집적·이용·유통이 증가하면서 이를 규율할 필요성이 제기되면서 입법되었다.⁴⁹²⁾

492) 이창범·유주연, 『각국의 개인정보피해구제제도 비교연구』 (개인정보분쟁조정위

이 법률은 개인정보의 유형에 따라 세 단계에 걸쳐서 시행하도록 되어 있었다. 동법은 개인정보의 유형에 따라 3단계에 걸쳐 시행하도록 되어 있다. 제1단계는 2001년 1월 1일부터 시행되는 경우로, 연방의 작업장, 사업체, 사무실(은행, 통신사, 무역회사 등 연방의 규제를 받는 조직 포함)에 의해 상업적 활동의 과정에서 수집, 이용, 제공된(건강정보를 제외한) 개인정보, 그러한 조직에 의해 수집, 이용, 제공된 근로자들에 관한 개인정보, 주의 경계나 국경을 통과하는 자의 조사를 위해 제공하거나 혹은 신용조사기관이나 메일링리스트 기타 개인정보를 대여, 판매, 교환하는 조직에 제공된 개인정보 등이 여기에 해당된다. 제2단계는 2002년 1월 1일부터 시행되는 경우로, 건강에 관한 개인정보가 여기에 속한다. 이러한 개인의 건강정보에는 개인의 정신적, 육체적 건강에 관한 정보, 개인의 치료, 검진 등에 관한 정보가 포함된다. 제3단계는 2004년 1월 1일부터 시행되는 경우로, 역내의 모든 상업적 활동의 과정에서 수집, 이용, 제공된 개인정보에 적용이 확대된다. 다만 실질적으로 유사한 수준의 프라이버시법이 채택되어 있는 지역에서 활동하는 조직에 대해서는 적용이 면제된다. 이후 이 법률은 2006년 3월 3일에 개정되어 오늘에 이르고 있다.

(2) 적용범위

PIPEDA은 프라이버시법과 달리 캐나다의 민간부문에 적용된다. 동법은 상업적 거래의 과정에서 개인정보를 수집, 이용, 제공하는 조직에 적용된다. 원래 동법은 은행, 항공사, 통신사 등과 같이 연방의 규제를 받는 민간부문에 의해 상업적 활동의 과정에서 수집·이용·제공된 고객이나 직원들에 대한 개인정보에만 적용되었으나, 이제는 소매상, 출판사, 서비스산업, 제조사 등 주의 규제를 받는 조직에 의해 수집·이용·제공된 개인정보에 대해서도 적용이 된다. 하지만 이러한 주의 규

원회, 2003), 190면.

제를 받는 조직의 직원들의 개인정보에는 적용되지 않는다.

(3) 구 성

동법은 다섯 부분으로 나누어져 있다. 제1장은 민간부문에서의 개인정보 처리를 위한 주요 원칙들을 설정하고 있다. 제2장부터 제5장은 원본문서와 서명을 법적으로 대체하는 전자문서와 전자서명의 이용에 관해 규율하고 있다. 구체적인 법률의 구성체계는 다음과 같다.

- 약칭(SHORT TITLE)

제 1 조: 약칭

- 제1장 민간부문에서의 개인정보 보호

제 2 조: 해석

제 3 조: 목적

제 4 조: 적용범위

제 1 절 개인정보의 보호

제 5 조-제10조: 적법한 목적, 동의에 의한 수집, 이용, 제공, 기한, 정보의 보유, 열람거부, 통지 등

제 2 절 구제(REMEDIES)

제11조-제17조: 감독관(Commissioner)의 진정, 진정의 조사, 감독관의 보고, 법원의 심리 등

제 3 절 감독(AUDITS)

제18조-제19조: 이행의 확보, 권한의 위임 등

제 4 절 통칙(GENERAL)

제20조-제29조: 비밀유지, 감독관의 보호, 연차보고, 상담, 규제, 명령, 신고, 위반행위와 처벌(제28조) 등

제 5 절 경과규정(TRANSITIONAL PROVISIONS)

제30조: 시행

- 제2장 전자문서(ELECTRONIC DOCUMENTS)

제31조: 해석

제32조: 목적

제33조: 전자적 대체수단(Electronic Alternatives)

제48조: 규제와 명령(Regulations and Orders)

- 제 3 장 THE CANADA EVIDENCE ACT의 개정 (제52조-제57조)
- 제 4 장 THE STATUTORY INSTRUMENTS ACT의 개정
(제58조-제59조)
- 제 5 장 THE STATUTE REVISION ACT의 개정 (제60조-제71조)
- 제 6 장 시행시기 (제72조)
- 부칙1
- 부칙2
- 부칙3

4. 기타 개별법

Alberta, Saskatchewan, Manitoba, Ontario 등에서는 의료진과 병원 등에 의한 개인의 건강정보의 수집·이용·제공을 특별히 다루기 위한 법률을 제정한 바 있다. 그리고 연방의 차원에서도 개인정보의 보호를 위한 규정이 포함된 여러 특별법을 두고 있다. 예컨대 연방 은행법(Bank Act)은 연방의 규제를 받는 금융기관에 의한 개인의 금융정보의 이용과 제공을 규율하는 조항을 포함하고 있다. 그리고 대부분의 주에서는 소비자신용조사에 관한 법률을 두고 있는데, 여기서 대체로 정보의 정확성 확보, 정보공개의 한계 설정, 고객의 열람권과 정정권

부여 등을 신용조사기관의 의무로 규정하고 있다.⁴⁹³⁾

5 프라이버시영향평가

(1) 개 관

캐나다는 2002년 5월, 프라이버시 영향평가 정책(Privacy Impact Assessment Policy)을 발표하고, 같은 해 8월 이를 구체화한 프라이버시 영향평가 지침을 고시하였다.⁴⁹⁴⁾

이에 따라 각 기관은 대국민 프로그램 및 서비스를 개발 및 시행함에 있어 프라이버시 영향평가를 의무적으로 실시하게 되었다. 이를 통해 대국민 프로그램 및 서비스가 프라이버시 관련 법률을 준수하고 있는지를 판단하고, 관리책임자 또는 정책결정자로 하여금 프라이버시 침해 가능성을 해소하거나 경감할 수 있도록 지원하며, 철저한 검증을 거쳐 각종 정책이나 프로그램, 시스템의 이용을 촉진할 수 있도록 지원하고 있다.

동 정책 및 지침은 캐나다 국민에 대해 프라이버시 영향평가 방법의 개발 및 유지에 관한 사항을 고지하고, 프라이버시 영향평가 결과를 정기적으로 공개함으로써 캐나다 정부가 프라이버시 침해 가능성이 있는 프로그램 및 서비스를 추진함에 있어 프라이버시보호원칙을 적극 반영하고 있음을 주지시키는 것을 목적으로 하고 있다.

(2) 도입배경

정부기관은 당해 기관이 제공하는 프로그램 및 서비스의 구상, 분석, 고안, 개발, 시행 및 사후 검토에 이르기까지 전 과정에 걸쳐 개

493) <http://www.privcom.gc.ca/fs-fi/02_05_d_15_e.asp> 참조.

494) 이하: 구병문, “캐나다 및 미국의 프라이버시 영향 평가 제도 분석과 국내 전자정부 법제로의 도입방향 검토”, 『정보화이슈분석』 03-16(한국전산원, 2003. 7). 2-6면 참조.

인정보의 수집, 이용 및 공개 등과 관련하여 프라이버시법 및 프라이버시 보호 원칙을 준수하고 있음을 명백히 밝힐 책임이 있다. 또한 정부기관은 개인정보의 수집이유, 개인정보의 이용 및 공개방법 등에 관하여 일반 국민과 지속적으로 의견을 교환해야 하며, 신규 프로그램 및 서비스를 제공하는 경우에는 동 프로그램 및 서비스가 프라이버시에 미치는 영향 및 그 해결방안에 대해 설명할 책임이 있다.

따라서 캐나다 정부는 프라이버시 영향평가 정책 및 지침을 발표 및 시행함으로써 정부의 프로그램이나 서비스의 구상에서부터 시행에 이르는 모든 단계에서 프라이버시 보호 문제가 적극 고려되도록 하고, 프로그램 관리자 및 기타 관련자에 대하여 프라이버시 문제에 관한 책임을 명확히 하여야 한다. 그리고 프라이버시에 대한 이해를 바탕으로 철저한 검증을 거쳐 정책이나 시스템 등을 도입할 수 있도록 정책결정자에 대하여 필요한 정보를 제공하고, 사업추진 후에 프라이버시 문제를 이유로 사업을 중단하거나 변경하는 위험을 감소시켜야 한다. 나아가 정부기관이 이용하는 개인정보 관련 업무절차 및 흐름을 문서화하여 고객들과의 협의를 위한 기초 자료로 활용하고, 프라이버시감독관 및 일반 국민에 대하여 프라이버시 침해 가능성이 있는 신규 또는 변경된 프로그램 및 서비스 계획에 관한 정보를 제공함으로써 적극적인 프라이버시 보호에 관한 인식을 고취시켜야 한다.

(3) 법적 근거 및 적용범위

이러한 프라이버시 영향평가 제도는 캐나다 프라이버시법 제71조 제(1)항 제(d)호와, 재무부장관으로 하여금 프라이버시법에 관한 지침을 시행할 수 있도록 한 재무관리법 제7조에 근거를 두고 있다.

이러한 영향평가의 실시 의무는 모든 국가기관 및 공공기관에 대해 적용된다.

(4) 프라이버시 영향 평가의 내용 및 절차

1) 1단계: 프라이버시 영향평가 필요성 판단(Project Initiation)

이는 프라이버시 침해 가능성이 있는 신규 프로그램 및 서비스에 대하여 사전에 프라이버시 영향평가의 필요성을 판단하고 평가 범위를 확정하는 단계이다.

프라이버시 영향평가가 실시되어야 할 경우로는 ① 개인의 동의 여부를 불문하고 개인정보를 신규로 수집, 이용, 공개하거나 기존의 개인정보 수집, 이용, 공개 범위 확대, (b) 개인정보의 수집대상 확대, (c) 개인정보의 수집방법을 직접적인 방법에서 간접적인 방법으로 변경, (d) 프로그램의 통합, 관리 등을 목적으로 한 개인정보의 수집 확대, (e) 프로그램간, 기관간, 공공·민간부문간 개인정보의 일치 및 공유, (f) 공통된 개인 식별자의 신규 개발 또는 사용 확대, (g) 개인정보의 물리적 또는 논리적 분리와 관계있는 업무절차나 업무시스템, 또는 개인정보에 대한 접근을 관리 및 통제하기 위하여 사용되는 보안체계의 중대한 변화, (h) 계약 등을 통한 프로그램이나 서비스의 정부기관 또는 민간부문 이전 등이 있다. 다만, 이 정책의 시행 전에 추진된 프로그램이나 서비스의 경우에는 전자정부의 특성상 개인정보의 수집, 이용 또는 공개되는 형태 등에 있어 본질적인 부분에 대한 변경이 있는 경우에만 프라이버시 영향평가의 필요성이 인정된다.

한편, 프로그램이나 서비스에 대한 구체적 사업계획이 수립되기 전 초기 단계에서는 예비적 프라이버시 영향평가(Preliminary PIA)를 실시할 수 있으며, 이후 필요에 따라 전면적인 프라이버시 영향평가 실시한다. 예비적 프라이버시 영향평가의 필요성에 대해서는 각 기관의 담당자가 판단하며, 프라이버시 영향평가의 필요성이 명백히 드러나지 않는 경우에도 예비적 프라이버시 영향평가는 실시할 수 있다. 예

비적 프라이버시 영향평가에서는 수집, 이용, 공개되는 개인정보의 양 및 유형 확인, 당해 프로그램 또는 서비스에 관한 법률 및 정책상의 권한 확인, 주요 관계자의 역할, 책임 및 법적 지위 확인, 프로그램 또는 서비스에서 프라이버시 침해 가능성이 있는 부분 확인, 프라이버시감독관과의 협의절차 구상, 최종평가 범위 및 일정 확정 등의 작업이 이루어진다.

프로그램이나 서비스 사업계획의 범위 및 복잡성 등에 따라 프라이버시 영향평가에 요구되는 전문적 기술이 다양하다. 따라서 프로그램 및 프로젝트 매니저, 프라이버시 정책 및 법률 전문가, 기능별 또는 기술 전문가 등 관련자에 대해 공동관리책임이 부여된다. 다만, 프라이버시 영향평가의 필요성 여부를 판단할 수 있는 권한은 정부기관의 부기관장에게 있다.

2) 2단계: 정보흐름의 분석(Data Flow Analysis)

이는 당해 사업계획상에 나타나는 업무절차, 아키텍처, 정보흐름 등을 기술하고 분석하는 단계로서 개인정보의 흐름을 파악하고자 실시된다. 정보흐름 분석의 3대 구성요소는 다음과 같다.

- 업무절차 다이어그램: 특정 활동 관련 정보흐름에 대한 일반적 기술
- 정보흐름도 : 누구의 개인정보가 누구에 의하여 어떠한 방식으로 수집, 이용, 공개 및 보존되는가?
- 시스템 및 인프라 아키텍처 : 개인정보의 물리적 또는 논리적 구분, 개인정보에 대한 부당한 접근을 방지하기 위한 보안체계 등을 문서화

3) 3단계: 프라이버시 분석(Privacy Analysis)

이는 프라이버시 관련 법률 및 정책 하에서 정보흐름을 검토하는 단계이다. 여기서는 당해 사업계획과 관련된 주요 프라이버시 침해

가능성이나 취약점을 용이하게 확인하기 위하여 질문서를 활용한다.

정부기관은 프로그램 및 서비스를 제공하는 과정에서 프라이버시 원칙, 정책 및 법률을 준수하고, 관련 프라이버시 영향 및 침해 가능성이 해소되거나 경감되도록 할 의무가 있다.

4) 4단계: 프라이버시 영향분석 보고(Privacy Impact Analysis Report)

이는 프라이버시 침해 가능성 평가, 프라이버시 침해 가능성 및 관련 문제 해소 또는 경감을 위한 방안 등을 포함하여 이전 단계에서 나온 산출물을 문서화하는 단계이다.

[그림 3-1-1] 프라이버시 영향평가 절차도



주: *PIA는 Privacy Impact Assessment의 약어

6. 입법체계상 특징

캐나다는 개인정보보호를 위하여 연방차원의 정부부문에 적용되는 프라이버시법(PA)과 민간부문에 적용되는 ‘개인정보보호 및 전자문서

에 관한 법률’(PIPEDA)을 두고 있다. 공공부문의 경우 연방차원의 법률이 제정되어 있지만, 각 주에서도 개인정보관련 법률을 별도로 제정하여 시행하고 있다. 주 차원의 경우에는 각 주의 정부나 공공기관에 의해 처리되는 개인정보를 보호하기 위한 공공부문에 적용되는 법률만이 제정되어 있는 것이 일반적이다. 아무튼 캐나다의 입법체계는 공공부문과 민간부문을 분리하여 규율하는 이원적 법체계로 운영되고 있다고 할 수 있다.

한편, 프라이버시법(PA)은 주무장관의 책임, 개인정보의 수집·보유·이용·공개 등의 제한, 개인정보은행과 개인정보색인, 정보주체의 권리, 구제절차, 개인정보보호기구(Privacy Commissioner), 벌칙 등 구체적인 사항까지 규율하고 있다. 그리고 ‘개인정보보호 및 전자문서에 관한 법률’(PIPEDA)에서도 민간부문에서의 개인정보보호와 관련하여 개인정보의 처리에 대한 제한, 정보주체의 권리, 구제절차, 감독기관(Commissioner), 벌칙 등에 관한 규정을 두고 있으며, 전자문서와 관련하여서도 전자적 대체수단, 규제와 명령 등 비교적 상세한 규정을 두고 있다. 이러한 점에서 PA는 공공부문에 대한 일반법, PIPEDA는 민간부문에 대한 일반법으로서의 성격을 각각 띠다고 할 수 있을 것이다. 물론 그 밖에도 전술한 바와 같이 특수한 영역에서의 개인정보보호를 위해 은행법이나 신용조사보고법 등과 같은 개별 법률에서 관련 규정을 두고 있다. 이러한 점을 종합적으로 검토할 때 캐나다의 개인정보보호 관련 법제는 이원적 일반법주의, 즉 부문별 일반법의 체계에 입각하고 있다고 평가할 수 있을 것이다.

제 3 절 영 국

1. 정보보호법의 제정과 개정

그 동안 영국에서는 비밀정보유통의 보호를 위한 보통법상의 권리가 주로 거래비밀을 중심으로 판례법상 인정되어 왔다. 하지만 막대

한 양의 개인에 관한 개인정보가 전산파일의 형태로 수집·관리되면서 그 남용에 대한 종래의 구제방법에 일정한 한계가 드러나게 되었다. 즉, 개인정보의 남용에 대하여 구제를 받으려면 반드시 비밀침해에 대한 배심원평결(finding)이 필요하였는데, 그러려면 청구인이 관련된 정보가 원래 ‘비밀리에’ 취득되었다는 것과 수신자가 그 비밀의 성질에 대한 통지를 받았다는 것을 입증하지 않으면 안 되었다.⁴⁹⁵⁾

이에 프라이버시 소위원회(Younger Committee on Privacy)⁴⁹⁶⁾는 컴퓨터의 개인정보를 수집하고 처리하는 기술을 심사하기 위한 입법을 권고하였다. 1975년에 정보주체를 보호하기 위한 백서(white paper)가 발간되었으며 그 이듬해에 린돕 정보보호위원회(Lindop Committee on Data Protection)가 구성되었다. 1978년에 이 위원회는 정보보호관청(Data Protection Authority)⁴⁹⁷⁾의 설립을 권고하였다. 하지만 그 제안이 채택되지는 못했다.

1980년대에 들어서면서 프라이버시보호문제에 관한 국제적 관심이 증대되면서 1980년에 국제경제협력기구(OECD)의 “프라이버시보호와 개인정보의 국제유통에 관한 가이드라인에 관한 이사회권고”(1980)와 유럽평의회(Council of Europe)의 “개인정보의 자동처리에 관한 개인의 보호를 위한 유럽협약”(1980)⁴⁹⁸⁾이 채택되기에 이르렀다. 이들 국제기구의 회원국인 영국으로서는 이러한 시대적 요청을 외면할 수 없었고, 결국 1984년에 가서 정보보호법(Data Protection Act 1984)을 제정하게 되었다. 이러한 입법은 OECD “프라이버시보호와 개인정보의 국제유통에 관한 가이드라인에 관한 이사회권고”(1980)를 받아들이는 조치의 일환이었다.⁴⁹⁹⁾ 그러나 이 법률은 1998년 7월 16일에 제정된 1998

495) R. Clayton · H. Tomlinson, *The Law of Human Rights*, Oxford University Press, 2000, p. 794.
496) *Report of the Committee on Privacy*, Cmnd 5012 (1972) para 621.
497) *Report of the Committee on Data Protection* (1978) Cmnd 7341.
498) European Convention for the Protection of the Individual With Regard to the Automatic Processing of Personal Data.
499) R. Clayton · H. Tomlinson, *op. cit.*, p. 794.

년 정보보호법(Data Protection Act 1998)으로 대체되어 2000년 3월 1일부터 부분적으로 시행되고 있다. 이 개정법은 1995년 유럽공동체의 개인정보보호지침(Directive 95/46/EC)을 국내법적으로 구체화하기 위한 입법으로 성립된 것이다.

동법에서는 1997년 유럽연합의 텔레커뮤니케이션 지침(Directive 97/66/EC)을 준용하고 있으며, 이후 1999년 5월 1일 공포되었던 텔레커뮤니케이션 법(정보보호 및 프라이버시에 관한 법률과 다이렉트마케팅 법)을 대체하였다.

2. 정보보호법의 적용범위

1998년 정보보호법에 의해 보호되는 정보(data)는 원칙적으로 자동처리의 형식으로 처리된 것, 관련 파일링시스템의 일부로서 기록된 것이나 혹은 그러한 의도로써 기록된 것, 그리고 그 밖의 동법 제68조에서 말하는 접근 가능한 정보의 일부를 이루는 것을 의미한다(제1조 제1항). 당해 정보 및 정보관리자가 보유하고 있거나 보유할 가능성이 있는 정보나 기타의 정보로부터 신원을 확인할 수 있는 생존하는 개인에 관한 정보를 의미하며, 또한 여기에는 개인에 대하여 표현된 의견이나 정보관리자의 모든 지시사항, 그 사람과 관계있는 모든 타인에 관한 의견도 포함된다(제1조 제1항).

1984년법은 자동처리된 정보에만 적용되었으나, 1998년법⁵⁰⁰⁾은 Directive 95/46/EC에 부응하기 위하여 정보를 정의하면서 “관련 파일링시스템의 일부로서 기록된 정보”를 포함시킴으로써 수작업처리 정보도 원칙적으로 정보보호법의 적용대상에 포함되었다. 여기서 수작업처리 정보란 “관련 파일링시스템(relevant filing system)의 일부로서 기록된 것이어야 한다. 관련파일링시스템이란 자동처리형식으로 수집된 정보

500) <<http://www.hmso.gov.uk/acts/acts1998/19980029.htm>> 참조.

는 아닐지라도 쉽게 접근할 수 있는 일정한 개인에 관한 특정한 정보로 개인과 관련이 있는 일련의 정보를 말한다.

원칙적으로 영국에서 설립된 정보관리자와 영국이나 유럽경제지역(EEA) 국가에서 개설되지는 않았지만 영국에 있는 정보처리기구를 이용하거나 영국으로 정보를 이전할 목적으로 정보를 처리하는 자에게 적용된다(제5조 제1항).

한편, 국가안보, 범죄·조세, 건강·교육·사회사업, 언론·예술·문학, 연구·통계·역사, 법적 절차에 의한 공개, 가정적 필요 등의 목적을 위한 정보의 처리에 대해서는 정보주체의 권리와 정보보호원칙에 관한 규정들을 제외한 조항의 적용에 있어서 예외가 인정된다(제27조 내지 제36조). 또한 내무부장관은 예외조항을 위한 그 밖의 명령을 제정할 권한을 가진다(제38조).

동법에 의하면 EU 밖으로 개인정보를 전송하는 것은 제3국이 정보주체의 권리와 자유를 위한 보호가 적절한 수준에 이를 것을 보증할 수 있는 경우에 한하여 인정된다(부칙1 제1장 제8호). 그리고 동법은 모든 진행중인 처리에 관해서는 3년간의 이행기간을, 수작업 파일링 시스템으로 이미 얻어진 정보에 대해서는 2007년까지 유예기간을 두고 있다.

3. 정보보호법의 구성⁵⁰¹⁾

- 제 1 장 서문
- 제 1 조: 기본 설명 조항
- 제 2 조: 민감한 개인정보
- 제 3 조: 특수 목적
- 제 4 조: 정보보호원칙

501) <<http://www.hms0.gov.uk/acts/acts1998/19980029.htm>>; Peter Carey, Blackstone's Guide to Data Protection Act 1998, Blackstone Press, Ltd, 1998 등 참조.

제 5 조: 법률의 적용

제 6 조: 감독관 및 심판원

- 제 2 장 정보주체 및 기타인의 권리

제 7 조: 개인정보에 접근할 권리

제 8 조: 제7조에 대한 보충 규정

제 9 조: 정보관리자가 신용조사기관인 경우 제7조 적용

제10조: 손해나 고통을 초래할 수 있는 처리를 방지할 권리

제11조: 다이렉트마케팅을 위한 처리를 방지할 권리

제12조: 자동화된 결정과 관련된 권리

제13조: 일정한 요건을 위반한 경우에 대한 보상

제14조: 정정, 차단, 말소 및 파기

제15조: 관할권 및 절차

- 제 3 장 정보관리자에 의한 통보

제16조: 서문

제17조: 미등록 처리 금지

제18조: 정보관리자에 의한 통지서

제19조: 통지서의 등록

제20조: 변경통보의 의무

제21조: 위반

제22조: 감독관에 의한 예비평가

제23조: 정보보호관리자의 임명규정을 만들 수 있는 권한

제24조: 특정 정보를 사용할 수 있게 하는 특정 정보관리자의 의무

제25조: 통지규약의 선정과 관련된 감독관의 임무

제26조: 수수료 법규

- 제 4 장 예외 조항

제27조: 서문

제28조: 국가안보

제29조: 범죄 및 과세

제30조: 보건, 교육 및 사회사업

제31조: 규율 활동

제32조: 언론, 문학, 예술

제33조: 연구, 역사, 통계

제34조: 관계 법령에 의한 또는 이에 따른 공공에게 공개된 정보

제35조: 법률에서 요구하는 또는 법적 소송과 관계된 공개

제36조: 가정적 목적

제37조: 기타 예외사항

제38조: 명령에 의한 기타 예외 조항

제39조: 과도기적 구제

- 제 5 장 집행

제40조: 집행의 통지

제41조: 집행통지의 취소

제42조: 사정 신청

제43조: 정보공개요구통지서

제44조: 특수 정보공개요구통지서

제45조: 특수 목적에 대한 감독관의 결정

제46조: 특수 목적을 위한 처리의 경우 집행 제한

제47조: 통지서 이행 거부

제48조: 상소권

제49조: 소송의 판결

제50조: 점유권 및 감독권

- 제 6 장 기타 규칙 및 일반 규칙

- 감독관의 기능

제51조: 감독관의 일반 의무

제52조: 의회에 제출되는 신고서 및 실무규약

제53조: 특수 목적 처리 경우의 감독관의 조력

제54조: 국제협력

- 개인정보의 불법적 취득 등

제55조: 개인정보의 불법적 취득 등

- 정보주체의 열람권에 따라 취득한 기록

제56조: 특정기록의 제작에 대한 요구 금지

제57조: 건강기록과 관련된 어떤 계약 조건의 무효

- 감독관이나 심판원에 제공된 정보

제58조: 정보의 공개

제59조: 정보의 비밀성

- 위반과 관련된 일반 규약

제60조: 기소 및 벌칙

제61조: 기타 관리자의 책임

- 『소비자 신용법(Consumer Credit Act) 1974』 수정

제62조: 『소비자 신용법 1974』 수정

- 총 칙

제63조: 국왕에게 적용

제64조: 전자적 또는 기타 수단에 의한 통지서 등의 전달

제65조: 감독관에 의한 통지서 집행

제66조: 스코틀랜드에서의 어린이의 권리 행사

제67조: 명령, 법규, 규칙

제68조: “접근 가능한 기록”의 의미

제69조: “건강전문가”의 의미

제70조: 보충적 정의

제71조: 명시된 표현의 주해

제72조: 법령의 수정

제73조: 경과 규정과 유예

제74조: 부분개정 및 연속개정, 무효화 및 폐지

제75조: 약칭, 시행과 범위

• 부 칙

<부칙 1> 정보처리원칙

<부칙 2> 제1원칙의 목적과 관련된 조건: 개인정보의 처리

<부칙 3> 제1원칙의 목적과 관련된 조건: 민감한 개인정보의 처리

<부칙 4> 제8원칙이 적용되지 않는 경우

<부칙 5> 정보보호감독관 및 정보보호심판원

<부칙 6> 항소(Appeal) 소송

<부칙 7> 기타 예외 조항

<부칙 8> 과도기적 보호

<부칙 9> 점유권과 사정권

<부칙 10> 본문 53조에 따른 조력에 관련된 추가 규정

<부칙 11> 교육적 기록

<부칙 12> 접근 가능한 공공 기록

<부칙 13> 2007년 10월 24일 이전에 효력을 가질 본 법령의 수정안

<부칙 14> 경과규정 및 보류조항

<부칙 15> 부가 개정안 및 간접 개정안

<부칙 16> 폐기 및 폐지

4. 개인정보보호기구

1998년법상 정보보호감독관(Data Protection Commissioner)은 개인정보를 처리하려는 정보관리자의 신고를 받아 등록하고(제19조), 정보관

리자의 모범적 업무처리를 장려하며(제51조), 특수목적의 개인정보처리에 관한 소송에서 당사자의 요청이 있는 경우 조력하는 임무도 수행한다(제53조). 또한 정보관리자의 의무위반에 대한 시정명령(제40조)과 관리자의 처리의 적절성에 대한 평가를 위한 정보제공의 요구(제43조) 등을 할 수 있다. 나아가 동법의 위반행위에 대한 소송의 제기에도 관여할 권한을 가진다(제60조 제1항).

그러나 종래의 정보보호감독관은 2000년 정보자유법(Freedom of Information Act)에 의하여 정보감독관(Information Commissioner)으로 대체되었다(동법 제18조 제1항⁵⁰²; 동법 부칙2 제1조 제1항⁵⁰³). 이에 따라 정보감독관은 1998년 정보보호법과 2000년 정보자유법을 집행하고 감독한다. 그는 영국 의회에 직접 보고하는 독립적 감독관청으로서 국내외에 걸쳐 임무를 수행한다.⁵⁰⁴

5. 기타 개인정보보호법제

영국에는 개인에게 개인정보에 대한 접근권을 부여하는 성문의 규정들은 다수 존재한다. 1987년 개인파일접근법(Access to Personal Files Act)의 적용대상인 사회후생파일⁵⁰⁵과 주택파일,⁵⁰⁶ 1990년 건강기록 접근법(Access to Health Records Act 1990)에 따른 1989년 11월 1일 이후의 건강기록, 1988년 의료기록접근법(Access to Medical Reports Act 1988)상 건강전문인들에 의하여 혹은 그들을 위하여 수집된 육체적 또는 정신적 건강에 관한 정보,⁵⁰⁷ 잉글랜드⁵⁰⁸와 웨일즈⁵⁰⁹의 특수교

502) <<http://www.hmso.gov.uk/acts/acts2000/00036--d.htm#18>>.

503) <<http://www.hmso.gov.uk/acts/acts2000/00036--w.htm#sch2>>.

504) <<http://www.dataprotection.gov.uk/commissioner.htm>>.

505) Access to Personal Files (Social Services) Regulations 1989, SI 1989/206, as amended by SI 1991/1587.

506) Access to Personal Files (Housing) Regulations 1989, SI 1989/503.

507) Access to Health Records (Control of Access) Regulations 1993, SI 1993/746 참조.

508) Education (Special Educational Needs) (Information) Regulations 1994, SI 1994/1048.

509) Education (Special Educational Needs) (Information) Regulations 1999, SI 1999/1442.

육적 수요, 환경정보⁵¹⁰⁾ 등이 그것이다.⁵¹¹⁾

여기서 1987년의 개인파일접근법(Access to Personal Files Act)은 1984년 정보보호법처럼 적용대상을 자동처리된 파일로 한정하지 않고 “그 정보로부터 식별할 수 있는 생존하는 개인에 관한 정보”라고 포괄적으로 규정함으로써(제2조 제2항), 수기식 파일들도 적용의 대상으로 하였다. 그리고 모든 공공기관으로 하여금 개인에게 자기정보에 대한 접근권을 인정하는 규칙을 제정하여 시행하도록 하였다(제1조).

그러한 규칙은 접근이 가능한 개인정보에 대하여 정보주체의 접근과 정정이나 말소를 보장하는 데 적당한 열람권과 정정청구권을 인정하여야 하며, 열람과 정정청구의 절차를 규정하고 불복이나 재심 등의 구제제도가 마련되어야 한다(제3조). 그리고 접근규칙은 위임명령의 형식으로 제정되어야 하며, 미리 공공기관 등의 의견을 청취하고, 위임명령의 형식으로 제정되어야 하며, 미리 의회의 양원에 제출하여 승인을 얻어야 한다(제3조 제4항·제5항).⁵¹²⁾

그러나 동법은 광범한 예외조항이 존재할 뿐만 아니라, 접근가능한 개인정보라 하더라도 그 적용대상은 사회복지부(social service departments)⁵¹³⁾와 주택부(housing departments)⁵¹⁴⁾에 의하여 보유되는 파일에 제한되어 있다(부칙1 제1조). 그리고 동법에는 정보보호감독관에 상당하는 것이 존재하지 않아 실효성을 담보하기 어렵다. 따라서 동법은 매우 제한적인 의미밖에 가지지 못하는 것으로 평가된다.⁵¹⁵⁾

510) Environment Information Regulations 1992, SI 1992/1711, as amended by SI 1998/1447.

511) R. Clayton · H. Tomlinson, *op. cit.*, p. 798.

512) 법제처, 『각국의 개인정보보호관계법』 (법제자료 제150집, 1989), 147면 이하 참조.

513) Access to Personal Files (Social Services) Regulations 1989, SI 1989/206, as amended by SI 1991/1587.

514) Access to Personal Files (Housing) Regulations 1989, SI 1989/503.

515) R. Clayton · H. Tomlinson, *op. cit.*, p. 797.

6. 입법체계의 평가

‘1998년 정보보호법(The Data Protection Act 1998)’은 공공과 민간부문의 구분 없이 영국에서 이루어지는 모든 개인정보 처리에 적용되는 통합입법의 형식을 취하고 있다.

그리고 동법은 개인정보보호에 관한 기본적 사항만 규정하는 데 그치지 않고, 개인정보보호원칙, 정보주체의 권리와 정보처리자의 의무, 개인정보보호기구의 조직과 운영, 정보심판원(Information Tribunal)의 운영, 개인정보의 국외이전 등 일반적인 사항까지 폭넓게 규정하고 있다. 특이한 것은 보건, 교육, 사회사업, 신용 관련 정보에 대해서도 동법이 별도의 규율조항을 두고 있다는 점이다. 아무튼 영국의 정보보호법은 개인정보보호에 관한 일반법의 역할을 수행한다고 할 수 있다. 하지만 그 밖에도 전술한 바와 같이 개인의 건강기록, 의료정보, 교육정보, 환경정보 등에 관한 특수한 규율을 위한 개별법도 다수 존재함을 볼 수 있다.

이러한 점에서 영국의 개인정보보호법제는 일원적 일반법주의, 즉 통합형 일반법의 체계로서 평가할 수 있을 것이다.

제 4 절 독일

1. 연방정보보호법의 제정과 개정

(1) 연방정보보호법의 제정

독일의 Hessen주에서는 1970년에 이미 정보보호법률(Datenschutz-gesetz)을 제정한 바 있었는데, 이는 개인정보보호에 관한 세계 최초의 입법으로 평가되고 있다. 이후 1974년에는 Rheinland-Pfalz주에서도 정보남용방지법률(Landesgesetz gegen Mißbräuchliche Datennutzung)이 제정되

었다. 연방의 차원에서는 1977년 1월 27일에 제정된 연방정보보호법(Bundesdatenschutzgesetz; BDSG), 즉 『정보처리에 있어서 개인에 관한 정보의 남용방지에 관한 법률』이 제정되었다. 그 밖에도 개별연방법률로서 1980년에 연방신고기본법(Melde-rechtsrahmengesetz)이 제정되었다. 이러한 독일의 개인정보보호법제는 다른 주로 확산되었을 뿐만 아니라 해외의 각국에도 많은 영향을 주었다. 그러나 1977년 제정된 연방정보보호법은 이후 1986년, 1990년, 1993년, 1994년, 1997년, 2001년, 2002년, 2003년 등 수 차례에 걸쳐 개정되었다.

(2) 연방정보보호법의 개정

1986년 2월 18일의 개정은 1983년의 연방헌법재판소의 인구조사판결⁵¹⁶⁾의 영향을 받아 ① 목적구속의 강화, ② 개인본인의 권리의 강화, ③ 온라인 정보처리의 허가요건의 확정, ④ 정보감찰관의 권한의 강화 등의 새로운 과제에 대응하기 위하여 이루어졌다. 그리고 1990년 12월 20일에는 1977년의 연방정보보호법이 전면 개정되었다. 이는 1986년과 1990년에 각각 제정된 제조물책임법과 소비자금융법을 하나로 통합하여 사실상 새로운 연방정보보호법을 제정하는 것이었다. 그러나 이 1990년의 전면개정법률(BGBl. I S. 2954)도 1993년 12월 27일(BGBl. I S. 2378), 1994년 9월 14일(BGBl. I S. 2325), 1997년 12월 16일(BGBl. I S. 3094), 1997년 12월 17일(BGBl. I S. 3108)에 다시 부분적으로 개정되었다.

이 가운데 1997년 12월 17일에 개정된 법률은 『전자통신법에 수반되는 법률』(Begleitgesetz zum Telekommunikationsgesetz) 제2조 제5항에 의하여 기존의 1990년 연방정보보호법을 변경하는 것이었다.⁵¹⁷⁾ 그리고 EU 회원국의 개인정보보호에 관한 국내입법의 조화와 통일을

516) Bverf GE 65,1.

517) <<http://www.datenschutz-berlin.de/recht/de/bdsg/bdsg1.htm>> 참조.

도모하기 위한 국내법의 정비의무를 3년 안에 이행하도록 규정한 1995년의 유럽공동체지침(Directive 95/46/EC)에 따라 2001년 5월 18일(BGBl. I S. 904), 2001년 6월 26일(BGBl. I S. 1254), 2001년 12월 3일(BGBl. I S. 3306)에 동법의 개정이 이루어졌다. 사실 이러한 개정은 Directive 95/46/EC가 설정한 이행기한인 1998년 10월 25일을 넘겨서 이루어진 것이었다.

독일정부는 1997년 12월 법률개정안을 의회에 제출한 바 있었지만 그 법안은 다른 정치일정으로 인하여 심의가 보류된 채 폐기되고 말았고,⁵¹⁸⁾ 결국 독일은 1999년 12월 유럽평의회의 협약 위반으로 유럽 법원에 제소당하기에 이르렀다.⁵¹⁹⁾ 이에 독일정부는 입법을 서둘렀고, 2001년 5월 18일 새로운 연방정보보호법이 의회에서 채택되자 5월 23일부터 시행에 들어갔다(BGBl. I Nr. 23/2001, S. 904).

이후 개인정보보호법제의 현대화 방안을 마련하기 위 독일연방내무부는 연방정보보호법의 2단계 개혁을 준비하기 위하여 카셀대학의 Alexander Roßnagel 교수와 드레스덴 공과대학의 Andreas Pfitzmann 교수 및 베를린 개인정보보호관인 Hansjürgen Garstka 교수에게 “개인정보보호법의 현대화, 특히 연방정보보호법의 기본적 개정”이라는 주제에 대한 검토보고서(Gutachten)를 위탁하였다. 2001년 11월에 제출된 “독일 개인정보보호법의 현대화에 관한 연구”(Die Studie zur Modernisierung des deutschen Datenschutzrechts)라는 보고서에서 Hansjürgen Garstka 교수는 독일의 정보보호법제의 문제점을 분석하고 그 개선방안을 제시하였으며, 장래의 연방정보보호법의 구조와 내용에 대한 제안을 하였다. 당시의 개인정보보호법제에 대해서는 여전히 물리적으로 매우 제한된 정보처리의 구상에만 얽매어 있었고, 개인정보의 새로운 형태와

518) 한국정보보호진흥원, 『2002 개인정보보호백서』(2003), 295면.

519) <http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/00/10|0|AGED&lg=EN &display=>>.

그 정보처리를 충분히 수용하지 못했으며, 정보처리의 새로운 기술에 대한 위험과 기회도 충분히 고려하지 못했다고 평가하였다. 나아가 기존의 개인정보보호법제는 그 구성에 있어서 모순된 경우가 많았으며, 수많은 특별법 형식의 규범화로 인하여 불명료하고 그 집행에도 어려움이 많았다는 점을 지적하였다.⁵²⁰⁾

이에 따라 연방정보보호법은 2001년 12월 20일(BGBl. I S. 3926)에 개정되었으며, 이후에도 2002년 7월 19일(BGBl. I S. 2674), 2002년 8월 21일(BGBl. I S. 3322), 2003년 1월 14일(BGBl. I S. 66)에 부분적이 개정이 이루어졌다.⁵²¹⁾ 그리고 최근 2006년 8월 22일(BGBl. I S. 1970)에는 개인정보보호기관의 명칭을 변경하는 법률의 개정이 있었다.

2. 연방정보보호법(BDSG)의 적용범위

동법의 대상정보는 자동화된 정보파일뿐만 아니라 비자동화 정보파일도 포함한다(제1조 제3항). 대상기관도 공공기관에 한하지 않으며, 사적 기관에 관해서도 적용범위에 포함하고 있다(제1조 제2항).

또 온 라인에서의 개인정보의 제공에 관해서도 요건을 정하여 인정한 규정을 두고 있으며(제10조), 기술적 조직적인 조치에 관해서도 상세한 부칙과 함께, 적극적 규정을 두고 있는 것도 특징이다(제9조).

하지만 개인정보의 보호에 관한 주의 법률이 적용되는 경우와 개인적 또는 가족적 활동(persönlich oder familiär Tätigkeit)을 목적으로 개인정보의 수집, 처리, 이용이 이루어지는 경우에는 동법은 적용되지 않는다(제1조 제2항 제2호 b) 및 제3호).

520) 이형규, 『독일 개인정보보호법제 현대화 추진방안에 관한 연구』 (한국정보보호진흥원, 2002. 12). 6면 참조.

521) <<http://www.brandenburg.de/land/lfdbbg/gesetze/bdsg.pdf>> 참조.

3. 연방정보보호법(BDSG)의 구성⁵²²⁾

- 제 1 장 총 칙

제 1 조: 목적 및 적용범위

제 2 조: 공공부문과 민간부문(Öffentliche und nicht-öffentliche Stellen)

제 3 조: 추가적인 개념규정

제 3 조a: 정보의 최소화(Datenvermeidung und Datensparsamkeit)

제 4 조: 개인정보의 수집, 처리, 이용의 조건

제 4 조a: 동의(Einwilligung)

제 4 조b: 외국 및 국제기구로의 개인정보 전송

제 4 조c: 예외

제 4 조d: 신고의무(Meldepflicht)

제 4 조e: 신고의무의 내용

제 4 조f: 개인정보보호책임자(Beauftragter für den Datenschutz)

제 4 조g: 개인정보보호책임자의 임무

제 5 조: 정보의 비밀(Datengeheimnis)

제 6 조: 정보주체의 필수적 권리

제 6 조a: 자동화된 개별결정

제 6 조b: 광전자설비에 의한 공공장소의 감시

제 6 조c: 이동성 있는 개인정보의 저장·처리매체

제 7 조: 손해배상(Schadensersatz)

제 8 조: 공공부문을 통한 자동화된 개인정보 처리의 경우의 손해배상

제 9 조: 기술적·조직적 조치

제 9 조a: 인증제도(Datenschutzaudit)

제 10 조: 자동화된 검색절차(Abrufverfahren)의 설치

522) <http://www.datenschutz-berlin.de/attachments/171/BDSG_2006.pdf?1175603444>참조. (2008. 9. 23. 방문)

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

제11조: 위임에 따른 개인정보의 수집, 처리, 이용

- 제2장 공공부문의 개인정보의 처리

제 1 절 정보처리의 법적 근거

제12조: 적용범위

제13조: 개인정보의 수집

제14조: 개인정보의 저장, 변경, 이용

제15조: 공공부문으로의 전송

제16조: 민간부문으로의 전송

제17조 - 삭제

제18조: 연방행정에 있어 개인정보보호의 실행

제 2 절 정보주체의 권리

제19조: 열람청구권

제19조a: 통지받을 권리

제20조: 정정·삭제·차단청구권 및 이의제기권

제21조: 연방정보위원회에의 진정(Anrufung)

제 3 절 연방정보위원(Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)

제22조: 연방정보위원의 선출

제23조: 연방정보위원의 법적 지위

제24조: 연방정보위원회에 의한 통제

제25조: 연방정보위원회에 의한 이의제기

제26조: 연방정보위원의 추가적인 임무

- 제3장 민간부문과 공기업의 개인정보 처리

제 1 절 개인정보 처리의 법적 근거

제27조: 적용범위

제28조: 고유목적을 위한 정보의 수집, 처리, 이용

제29조: 전송을 위한 영업상 정보의 수집과 저장

제30조: 익명형태에 의한 전송을 위한 영업상 정보의 수집 · 저장

제31조: 특별한 목적구속성(Zweckbindung)

제32조 - 삭제

제 2 절 정보주체의 권리

제33조: 통지받을 권리

제34조: 열람청구권

제35조: 정정 · 삭제 · 차단청구권

제 3 절 감독관청

제36조 - 삭제

제37조 - 삭제

제38조: 감독관청

제38조a: 정보보호법 규정의 실행을 촉진하기 위한 행동지침

- 제 4 장 특별규정

제39조: 직업상 비밀 또는 특수한 공무상 기밀의 준수가 요구되는
개인정보에서의 목적구속

제40조: 연구기관에 의한 개인정보의 처리와 이용

제41조: 언론매체에 의한 개인정보의 수집, 처리, 이용

제42조: 독일방송사(Deutsche Welle)의 개인정보보호책임자

- 제 5 장 최종규정

제43조: 과태료규정

제44조: 형벌규정

- 제 6 장 경과규정
제45조: 잠정적 적용
제46조: 개념규정의 추가규정
- 부속서(제9조와 관련하여)

4. 전기통신서비스정보보호법

(1) 제정과 개정

인터넷 등 새로운 정보통신수단의 급속한 확산으로 개인정보침해의 양상이 종래와는 사뭇 다른 형태로 전개되자, 정보통신서비스를 효율적으로 규율하기 위한 특별법을 제정할 필요성이 대두되었다.

이에 연방정보보호법(BDSG)의 특별법으로서 「1997년 7월 22일 전기통신서비스에 있어서의 정보보호에 관한 법률」(Das Gesetz über den Datenschutz bei Telediensten vom 22. Juli 1997)이 제정되었다.⁵²³⁾

동법은 약칭 ‘전기통신서비스정보보호법’(Teledienstschutzgesetz; TDDSG)으로 불리기도 한다. 이 법률은 2000년 6월 8일의 유럽의회 전자거래지침이 2002년 1월 17일까지 국내법적 규정을 두도록 함에 따라 2000년 6월 27일에 개정되었다. 이후 2001년 12월 14일을 비롯하여 여러 차례 개정되는 과정을 거쳐, 최종적으로 2007년 2월 26일에 개정되어 오늘에 이르고 있다.⁵²⁴⁾

(2) 적용범위

동법은 전기통신서비스를 이용하는 자의 개인정보를 보호하기 위해 서비스제공자가 개인정보를 수집·처리·이용을 하는데 적용된다. 다

523) BGBl I S. 1870.

524) <<http://www.umwelt-online.de/recht/anlasi/tddsg.htm>> 참조.

만 개인정보의 수집·처리·이용이 오직 직업적으로만 혹은 서비스를 목적으로 해서만 전기통신서비스의 이용이 이루어질 경우에는 그 서비스관계와 근로관계에 적용이 되지 않는다. 또한 오로지 노동소송이나 영업소송의 조정을 위해서만 전기통신서비스의 이용이 이루어지는 경우에는 기업 내부나 기업간 혹은 공공기관 내부나 공공기관간에 적용되지 않는다.

(3) 주요 내용

동법은 개인정보의 처리에 관한 기본원칙을 명시하고 있는 바, 서비스제공자(자신 또는 타인의 전기통신서비스를 이용하도록 하거나 이용을 중개하는 자연인, 법인 또는 인적 집단)는 다른 법률에 의해 허용되거나 전기통신서비스의 수요자인 자연인, 법인 또는 인적 집단인 이용자가 동의한 경우에 한하여 개인에 관한 정보를 수집·가공·이용할 수 있도록 하고 있다(제3조).

서비스제공자는 개인정보를 이용하기 이전에 사용자에게 개인정보의 수집·처리·이용의 종류, 범위, 장소 및 목적을 고지해야 한다. 그리고 자동화된 검색절차의 경우에는 그 절차의 개시 이전에 사용자에게 사용자의 식별장치, 개인정보의 수집, 처리, 이용 등에 대해서도 고지해야 한다(제4조 제1항).

또한 서비스제공자가 사용자에게 전자적 동의를 받으려면, 사용자의 분명하고 확실한 의사표시가 있어야 하고, 동의의 내용을 사용자가 언제든지 검색할 수 있어야 한다(제4조 제2항). 그리고 서비스제공자가 사용자가 동의를 하기 전에 언제든지 동의를 철회할 수 있음을 설명해야 한다(제4조 제3항).

또한 서비스제공자는 이용자가 전기통신서비스 요금을 가명 또는 익명으로 할 수 있다는 가능성, 정산목적 이외에 검색·처리과정 또는 기타 이용에 의해서 수집된 정보의 즉각적 파기, 개인정보의 분리

처리, 이용내역의 가명사용 등의 의무를 진다(제4조 제6항 및 제7항).

5. 개인정보보호법의 현대화 방안

Alexander Roßnagel 교수 등은 전술한 ‘개인정보보호법의 현대화 방안’ 보고서에서 단순하고 이행하기 쉬우며, 새로운 형태의 정보처리에 수반되는 위험에 효과적으로 대응할 수 있는 현대적 정보보호법을 마련할 것을 주장하였다. 그 구체적인 입법의 방안으로 제시된 내용 가운데 입법체계와 관련된 부분을 소개하면 다음과 같다.⁵²⁵⁾

첫째, 현대적 입법은 특정한 분야에 한정된 규정에 우선하는 일반법에 기초를 두어야 하며, 이러한 일반법은 개인정보의 처리에 관한 원칙적이고 엄격한 규정을 두어야 한다. 그래야만 규범의 범람이나 법의 산만함을 최소화할 수 있고, 법률간의 모순도 피할 수 있을 것이다.

둘째, 분야별 특별법상의 특별규정은 오로지 일반규정에 대한 예외적 사항만을 규정하여야 한다. 가령 “연방정보보호법 제○조와는 달리...”와 같은 문언을 사용하여 일반원칙의 명시적인 적용배제를 명시적으로 밝힘으로써 특별법적 성격을 명확히 할 필요가 있다.

셋째, 통신법(TKG) 제85조와 제89조 및 전기통신서비스업 정보보호규칙(TDSV), 전기통신서비스정보보호법(TDDSG) 등을 연방정보보호법(BDSG)에 통합시킬 필요가 있다. 이를 통해 적용범위의 중복이나 가치적 모순을 제거하고 입법체계상의 통일성을 제고할 수 있다.

넷째, 일반적인 개인정보보호의 원칙은 공공부문뿐만 아니라 민간부문에서도 마찬가지로 적용되어야 한다. 다만 민간부문에서는 그 규정의 수범자가 기본권의 주체이고, 공공부문에서는 공익의 추구가 필요하다는 점을 고려하여 양 부문에 대해 차별적으로 규율하는 것은 필요하다고 본다.

525) 이형규, 『독일 개인정보보호법제 현대화 추진방안에 관한 연구』 (한국정보보호진흥원, 2002. 12). 6-9면 참조.

6. 현행 입법의 체계상 특징

현행의 연방정보보호법은 공공부문과 민간부문을 구분하지 않고 개인정보의 처리와 관련된 사항을 폭넓게 규율하는 통합입법의 형식을 취하고 있다. 물론 양 부분에 대한 규율의 내용이 달리 설정되어 있어서 이 부분에 대한 새로운 접근이 필요하다는 지적이 있음은 위에서 언급한 바 있다. 또한 동법은 구조화된 수기과일링시스템(manual filing systems)은 물론, 의료기록이나 교육기록에 대해서는 순수하게 수기로 처리되는 개인정보까지도 규율의 대상에 포함시키고 있다.

한편, 동법은 개인정보보호의 기본원칙을 비롯하여 정보주체의 권리와 정보처리자의 의무, 벌칙, 개인정보보호기구의 설립 및 운영, 개인정보의 국외이전 등에 관한 사항까지 망라하고 있다. 그리고 정보보호법은 각 개별 영역의 특수한 개인정보 처리상황까지 규정하고 있지 않고, 특정 영역에 관하여는 ‘전기통신서비스정보보호법’(TDDSG) 등과 같은 특별법을 두고 있다.

이러한 점을 종합적으로 검토할 때 독일의 개인정보보호법제는 일원적 일반법주의, 즉 통합형 일반법의 체계를 취하고 있다고 평가할 수 있다.

제 5 절 프랑스

1. ‘정보처리·추적 및 자유에 관한 법률’의 제정과 개정

(1) 제 정

프랑스에서는 1960년대 후반부터 행정기관을 중심으로 컴퓨터에 의한 정보처리가 급속히 확산되었다. 1967년에는 세무당국이 그 업무 전반에 대한 전산망을 설치하였고 1969년에는 국민건강보험의 전산화

가 이루어졌다. 그리고 1970년에 접어들어서는 ‘도로교통에 관한 자료의 집중화에 관한 1970년 6월 24일 법률’(Loi n° 70-539 du 24 juin 1970)에 의하여 운전자파일이 구축되었다. 이러한 상황에서 정부는 컴퓨터기술의 발전이 개인의 자유에 미치는 영향에 대하여 본격적으로 검토하기 시작하여 1972년에 법무부내에 연구반을 설치하고 구체적인 조사·검토에 들어갔다. 하지만 다른 한편에서는 행정의 효율화에 대한 사항도 꾸준히 검토되었는데, 1974년 초에는 행정부문에서의 정보처리를 대폭적으로 확대하는 계획이 내무부를 중심으로 수립되기 시작하였다. 그리고 대통령이 1974년 11월 8일자 데크레(décret)를 통하여 법무부 산하에 정보위원회(CNIL)를 설치하여 공공부문과 민간부문에 있어서 정보처리기술의 발전에 따른 개인의 사생활과 자유 및 공적 자유의 침해를 방지하고 이를 보호할 수 있는 사항을 구체적으로 마련하도록 지시하였다. 이에 따라 정보위원회는 관계 행정기관, 기업가 및 노동조합의 의견을 청취하는 등 기초조사를 실시하여 1975년 6월 27일에 보고서를 대통령에게 제출하였다. 이 보고서에서는 개인정보의 보호를 위하여 독립된 기관을 설치하여 정보시스템의 감독을 실시하고, 공공기관에 의한 시스템설치에 대한 사전 허가제를 실시하며, 정보 당사자인 개인에게는 자기의 정보에 대하여 접근권을 인정할 것 등이 제시되었다. 정부는 이러한 위원회의 보고서를 토대로 하여 작성된 법률안의 1976년 8월 9일 국민의회에 상정하였다.

이 법안은 1977년 10월 5일에 국민의회에서, 1977년 11월 17일에 상원에서 각각 부분적인 수정을 거쳐 통과되었으며, 결국 양원합동조정위원회를 거쳐 1978년 1월 6일 ‘정보처리·축적 및 자유에 관한 1978년 1월 6일 법률’(Loi n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés)⁵²⁶⁾이 제정되기에 이르렀다.⁵²⁷⁾

526) Journal officiel du 7 janvier 1978 et rectificatif au JO du 25 janvier 1978.

527) 법제처, 『각국의 개인정보보호관계법』(법제자료 제150집, 1989), 153-154면; 성

(2) 개 정

위 법률(이하 ‘정보처리법’이라 함)은 개인정보의 보호를 강화하기 위하여 또는 정보화의 진전에 따라 새롭게 제기되는 문제에 대처하기 위하여 1988년(n° 88-227)⁵²⁸⁾, 1992년(n° 92-1336)⁵²⁹⁾, 1994년(n° 94-548)⁵³⁰⁾, 1999년(n° 99-641)⁵³¹⁾, 2000년(n° 2000-321)⁵³²⁾, 2002년(n° 2002-303)⁵³³⁾에 개정된 바 있으며, 최근에는 1995년 10월 24일 유럽인 법령 95/46/EC의 효력을 부여하기 위한 개정이 이루어져 2004년 8월 7일 공포되었다(JO du 182).

그 가운데 1994년 7월 1일의 개정법에서는 보건분야의 연구를 목적으로 하는 개인정보의 자동처리에 관한 제5장의1이 신설되었다. 여기서 개인의 치료를 위해서는 정보의 처리가 허용되고, 보건분야에서의 연구를 위하여도 일정한 조건하에서 개인정보의 자동처리가 허용되지만 정보처리는 정보위원회(CNIL)의 허가를 받아야 하고, 개인을 식별할 수 있는 정보를 송부할 때에는 암호화하여 보내도록 규정하였다(동법 제40조의1, 제40조의2, 제40조의3). 이러한 의료정보의 보호와 이용에 관하여는 1999년 7월 27일의 개정법과 2000년 4월 12일의 개정법에서도 부분적인 변경이 가해졌다(제40조의3 제2항). 아울러 2000년 4월 12일의 개정법에서는 이 외에도 記名情報의 처리목적과 보존

낙인, 『프랑스헌법학』 (법문사, 1995), 852-856면; 성낙인, 『언론정보법』 (나남출판, 1998), 553-557면; 박균성, 『프랑스의 전자정부법제』 (한국법제연구원, 2001.11), 82-83면; David H. Flaherty, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, 1989, pp. 165-169 등 참조.

528) Loi n° 88-227 du 11 mars 1988, article 13 relative à la transparence financière de la vie politique (JO du 12 mars 1988).

529) Loi n° 92-1336 du 16 décembre 1992 (JO du 23 décembre 1992).

530) Loi n° 94-548 du 1er juillet 1994 (JO du 2 juillet 1994).

531) Loi n° 99-641 du 27 juillet 1999 (JO du 28 juillet 1999).

532) Loi n° 2000-321 du 12 avril 2000 (JO du 13 avril 2000).

533) Loi n° 2002-303 du 4 mars 2002 (JO du 5 Mars 2002).

기간에 관한 변경이 있었다(제28조).

한편 Directive 95/46/EC가 부과한 국내법화 의무를 기한까지 이행하지 못하였다는 이유로 프랑스는 1999년 12월 EC 집행위원회로부터 유럽법원에 제소당하기에 이르렀다. 이에 프랑스는 뒤늦게나마 의무이행을 위하여 Draft Information law of July 2001을 마련한 바 있다.⁵³⁴⁾

그리고 2002년 3월 4일에 개정된 정보처리법⁵³⁵⁾에서는 치료와 예방활동의 평가나 분석을 위한 개인의 건강정보의 처리에 관한 제5장의2가 신설되었으며, 그 밖에도 다른 법률 및 행정명령과의 관계(제29조의1)와 제4장의 적용방법에 관한 데크레(제33조의1)에 관한 규정이 신설되었다.

2. 정보처리법의 적용범위

프랑스의 정보처리법은 공공부문과 민간부문에 모두 적용될 뿐 아니라, 컴퓨터로 자동처리되는 개인정보와 수기파일로 처리되는 개인정보에도 함께 적용되는 광범위한 적용범위를 갖고 있다.

동법의 보호대상이 되는 정보는 개인정보(information nominative), 즉 “그 형식 여하를 불문하고 직·간접적으로 자연인의 신원을 확인할 수 있게 하는 정보로서 자연인 또는 법인에 의해서 처리되는 정보”이다(제4조). 이러한 개인정보의 수집·입력·보유에 관한 규정은 비자동화파일 또는 비천공카드파일에 대해서도 적용되며(제45조 제1항), 정부는 정보위원회의 제의에 따라 정보처리된 파일의 사용으로 자유보호를 위협할 경우 동법의 전부 또는 일부를 적용할 수 있다(제45조 제4항). 따라서 동법의 보호대상에는 컴퓨터에 의해 처리된 정보뿐만 아니라 수작업으로 처리되는 정보도 포함된다고 할 수 있다.

534) <<http://www.justice.gouv.fr>> 참조.

535) <http://www.cnil.fr/droits/index_droit.htm> 참조.

그리고 공공부문뿐만 아니라 민간부문(자연인 및 법인)에 의하여 처리되는 개인정보까지도 포함이 된다. 하지만 정보의 주체는 자연인에 한하여 보호되며, 법인의 정보는 그 보호대상이 되지 않는다.

한편 제30조에 규정된 범죄에 관한 개인정보의 수집제한 및 제31조에 규정된 정치적·사상적·종교적 의견 등에 관한 개인정보의 수집제한에 관해서는 “... 그 적용이 표현의 자유의 행사를 제한하는 것을 목적으로 하는 경우 인쇄매체 또는 방송매체에 의해 취급된 개인정보에는 적용되지 않는다.”는 규정을 두고 있다(제33조).

3. 정보처리법의 주요 규율사항

(1) 정보처리의 기본원칙

정보처리에 의하여 사람의 신분·인종·사생활 및 개인적 또는 공적 자유가 침해되어서는 안 된다(제1조).

그리고 정보시스템에 의하여 처리되는 정보의 공적·사적 결정과정을 감안하여 재판의 기초자료로 사용될 수 없으며(제2조 제1항), 개인의 행동에 대한 평가를 전제로 하는 행정적 또는 사적인 결정은 어떠한 경우에도 당사자의 프로필이나 인격을 명확하게 나타내는 자동정보처리를 유일한 근거로 할 수 없다(제2조 제2항).

또한 정보처리의 결과가 본인에게 불이익이 되는 경우에는 그 정보와 근거에 대하여 알 권리(*droit de connaître*)가 있고 이의제기권(*droit de contester*)을 가진다(제3조).

(2) 정보시스템의 설치에 대한 제한

이 법은 개인의 사생활이나 자유를 침해할 우려가 있는 개인정보의 자동처리는 물론이고 그에 선행하는 정보처리시스템의 설치 그 자체에 대해서도 제한을 가하고 있다. 다만 정보처리시스템설치의 제한에

있어서는 직접적인 규제의 방식을 피하고 정보위원회를 통한 간접적 감독의 방식을 채택하고 있다.

정보처리시스템의 설치는 공공부문과 민간부문에 있어서 그 규율을 달리하고 있다. 전자의 경우 미리 위원회의 동의를 요하고 후자의 경우 위원회에 신고할 것을 요구하고 있다. 즉, 국가·공공기관이나 지방자치단체 또는 공익사업을 영위하는 사법상 법인을 위하여 행하는 개인정보의 자동처리는 원칙적으로 위원회의 정당한 의견을 청취한 후에 정한 법규에 의하여 이를 결정하는 데 비하여(제15조 제1항), 그 밖의 자를 위하여 행하는 개인정보의 자동처리는 사전에 정보위원회에 신고하여야 한다(제16조 제1항).

(3) 개인정보의 수집·기록·보존에 대한 제한

이 법에 의해 규제를 받는 행위는 주로 개인정보의 자동처리이다. 이는 “개인정보의 수집·기록·축적·변경·보존·삭제에 관한 것으로서 자동적 수단으로 행하는 일체의 작용 및 정보축적이나 데이터베이스의 설치, 특히 개인정보의 자동처리방식에 의한 상호 연결이나 조회 또는 전달에 관한 일체의 작용”을 말한다(동법 제5조). 이러한 개인정보의 처리활동에 대해서는 각종의 규제가 가해지고 있다.

먼저, 개인정보의 수집과 관련하여 사기·부정 또는 불법의 방법으로 정보를 수집하는 것이 금지되고(제25조), 모든 자연인은 본인과 관계되는 개인정보가 정보처리의 대상이 되는 것에 반대할 권리를 가진다(제26조 제1항). 그리고 개인정보의 주체에게 답변의 임의성 유무, 답변불응시 초래될 수 있는 결과, 그 정보의 이용자, 접근권과 정정권이 있다는 사실 등을 통지하여야 한다(제27조 제1항).

다음, 개인정보의 기록과 관련하여 사람의 혈통, 정치적·철학적·종교적인 견해, 노동조합의 소속 또는 품행을 직접 또는 간접적으로 노출시키는 개인정보를 당사자의 명백한 동의없이 정보시스템에 입력

시키는 것은 원칙적으로 금지된다(제31조 제1항).

다음, 종래에는 원칙적으로 정보위원회에서 그 보존을 허가하지 아니한 의견요구서 또는 신고서에 정한 기간을 초과하여 정보를 기명의 형태로 보존하는 것은 금지되었다(제28조). 그러나 2000년 개정법에서는 이러한 제28조를 개정하여 “정보는 역사적·통계적·과학적 목적의 처리를 위해서만 그 정보가 수집되고 처리된 목적의 실현에 필요한 기간 이상으로 개인정보의 형식으로 보관될 수 있다. 이와 같이 보관될 정보의 선택은 「기록물에 관한 1979년 1월 3일의 법률」(LOI n° 79-18)의 제4조의1에 규정된 조건에 따라 행하여진다.”고 규정하였다.⁵³⁶⁾

역시 2000년 개정법에서 신설된 내용으로, 기간을 초과하여 보관하고 있는 제31조의 민감한 정보(사람의 혈통, 정치적·철학적 또는 종교적인 견해, 노동조합의 소속 또는 품행 등을 직접 또는 간접적으로 노출시키는 개인정보)에 해당하지 않더라도 관계인의 명시적인 동의나 위원회의 허가를 받지 않는 한 역사적·통계적·과학적 목적 이외의 목적으로 처리의 대상이 될 수 없으며, 그러한 민감한 정보를 포함하는 경우에는 관계인의 명시적 동의나 위원회의 제안 또는 동의에 근거한 국사원의 심사를 거친 명령에 의하여 허가되지 않는 한 처리될 수 없다(제28조의2).⁵³⁷⁾

(4) 접근권의 행사

개인정보의 자동처리에 의하여 개인의 권리와 이익이 침해되지 않도록 하기 위하여 정보주체에게 자신의 정보를 기록하고 있는 정보시스템에 대한 액세스권(le droit d'accès)을 제5장에서 인정하고 있다. 먼저, 자신의 신분을 증명하는 자는 모두 자동정보처리가 본인과 관계되는 개인정보를 대상으로 하는지의 여부를 알고 경우에 따라 그 정

536) 박균성, 『프랑스의 전자정부법제』 (한국법제연구원, 2001.11), 84면 참조.

537) 위의 논문. 82-84면 참조.

보를 전달받기 위하여, 제22조에 의하여 일반대중이 목록을 열람할 수 있는 정보의 자동처리담당기관에 문의할 권리를 가진다(제34조).

다음, 접근권이 있는 자는 그에게 관계되는 정보를 전달받을 수 있으며, 명백하게 언어로 전달하는 경우에는 기록내용과 일치하여야 한다(제35조 제1항). 그리고 정보를 은폐 또는 분실할 우려가 있는 경우 소송을 제기하기 전이라도 관할법원판사에게 그 정보를 은폐 또는 분실하지 아니할 수 있는 모든 조치를 명하도록 요구할 수 있다(제35조 제4항).

다음, 접근권이 있는 자는 본인과 관계되는 정보로서 부정확·불완전 또는 모호하거나 기한이 지나고 수집·이용·전달 또는 보존을 금지하고 있는 정보를 수정·보완·명백화·최신화 또는 말소할 것을 요구할 수 있다(제36조 제1항). 이 경우 개인정보파일은 이를 소유하고 있는 기관이 그 파일에 포함된 개인정보의 부정확성 또는 불완전성을 알게 된 때 이를 보완 또는 수정하여야 한다(제37조).

마지막으로, 의료정보에 접근권을 행사하는 경우 그 정보는 지정된 의사를 통하여서만 이를 당사자에게 전달할 수 있다(제40조). 이러한 의료정보는 제3자의 개입을 통해서만 행사할 수 있는 간접적 액세스권이라 할 수 있다.⁵³⁸⁾

(5) 보건 분야의 조사를 목적으로 하는 개인정보의 자동처리

의료정보의 자동처리는 1994년 7월 1일의 개정법에서 신설된 제5-2장에서 규정하고 있다. 이에 의하면, 보건분야조사관계정보처리자문위원회는 정보처리의 실시를 요구하는 경우 정보위원회에 앞서 조사방법, 개인정보에 의뢰할 필요성 및 조사의 목적을 위한 개인정보의 적합성에 대한 의견을 표명한다(제40-2조 제1항). 정보처리는 정보위원회의 허가를 얻어야 한다(제40-2조 제4항).

⁵³⁸⁾ 성낙인, 『언론정보법』 (나남출판, 1998), 584면 참조.

보건직에 근무하는 자는 허용된 정보자동처리의 범위 내에서 소유하고 있는 개인정보를 전달할 수 있으나(제40-3조 제1항), 개인정보로 동일인임을 확인할 수 있는 경우에는 그 정보를 전달하기 전에 코드화하여야 한다(제40-3조 제2항). 정보처리의 결과를 발표할 때에는 어떠한 경우에도 관계자의 신원을 직접 또는 간접적으로 확인하는 것을 허용할 수 없다(제40-3조 제3항). 정보처리를 하도록 요청받은 자 및 처리대상의 자료에 접근하는 자는 업무상 알게 된 비밀을 준수하여야 하며, 이를 위반한 경우 형사처벌의 대상이 된다(제40-3조 제5항). 모든 사람은 본인과 관계되는 개인정보가 보건분야에서의 조사를 목적으로 자동처리의 대상이 되는 데 대하여 반대할 권리를 가지며(제40-4조 제1항), 조사상 동일시되는 생물전본의 수집이 필요한 경우에는 정보처리를 행하기 전에 관계자의 명백한 동의를 얻어야 한다(제40-4조 제2항).

자신의 개인정보가 수집되거나 그러한 정보가 전달되는 경우 본인은 동 정보의 처리를 시작하기 전에 개별적으로 전달된 정보의 종류, 정보처리의 목적, 정보수취인, 접근권·정정권, 반대권 또는 관계자의 동의를 얻을 의무 등에 대한 통보를 받는다(제40-5조 제1항). 그러나 주치의가 정직하게 평가하는 합당한 이유 때문에 환자가 자세한 진단 또는 예측내용을 통보받지 못한 경우에는 그 정보를 전달할 수 없다(제40-5조 제2항). 처리 이외의 목적으로 정보를 처음 수집한 경우에는 개인정보의 당사자를 찾아내기 곤란하더라도 그 개인정보의 의무에 위반될 수 있다(제40-5조 제3항).

미성년자의 경우 친권자 또는 법적보호조치 대상자의 경우 후견인은 정보의 수취인이 되며 본인의 권리를 행사한다(제40-6조).

(6) 치료와 예방활동의 평가나 분석을 위한 개인의 건강정보 처리

2002년 개정법은 제5장의2를 신설하여 치료와 예방활동의 평가 또는 분석을 위한 개인의 건강정보의 처리에 관하여 규정하고 있다(제

40조의11, 제40조의12, 제40조의13, 제40조의14, 제40조의15).

(7) 벌 칙

동법에 의해 개정된 Code Penal에서는 사기·신의성실의 위반, 기타 불법적인 방법으로 개인정보를 수집하고 처리함으로써 법률상 승인된 규칙에 따라 국사위원회의 시정명령을 받았음에도 그 기한이 넘도록 그 개인정보를 계속 저장하고 있을 경우 30만유로의 벌금 또는 5년의 징역에 처한다(제226-30). 다만 그러한 저장이 법률에 의해 제공되는 역사적이거나 통계, 과학적인 목적으로 사용되었을 경우에는 예외가 인정된다.

(8) 개인정보보호기구

프랑스의 정보위원회(Commission nationale de l'informatique et des libertés: CNIL)는 프랑스 내에서 이루어지는 모든 개인정보 처리행위를 규율한다. 이 위원회는 부당한 개인정보의 처리로 국민들의 개인정보가 침해되는 것을 방지하기 위해 설립된 독립된 행정관청이다(제 8조 제1항).

4. 입법체계의 평가

프랑스의 정보처리법은 공공부문과 민간부문에 모두 적용될 수 있도록 되어 있다. 그리고 컴퓨터로 자동처리되는 개인정보와 수기파일로 처리되는 개인정보에도 함께 적용되는 광범위한 적용범위를 갖고 있다. 한편, 동법에서는 정보처리의 기본원칙, 정보시스템의 설치에 대한 제한, 개인정보의 처리에 대한 제한, 접근권의 행사, 보건분야의 조사를 목적으로 하는 개인정보의 자동처리, 개인의 건강정보 처리, 벌칙, 개인정보보호기구인 정보위원회(CNIL) 등의 규정을 두고 있다.

이는 개인정보보호에 관한 기본적 사항만 규율한 것이라고 보기 어렵다. 이러한 점에서 동법은 일반법의 체계를 취하고 있다고 볼 수 있다. 하지만 그 밖에 특수한 영역에 대해서는 개별법에 의해 개인정보의 보호가 이루어지도록 하고 있다.

이렇게 볼 때 프랑스의 정보처리법은 일원적 일반법주의, 즉 통합형 일반법의 입법체계로 평가할 수 있을 것이다.

제 6 절 이탈리아

1. 개 관

이탈리아의 헌법은 주거의 불가침에 대해 규정하고(제14조), 나아가 모든 형태의 통신에 있어서의 자유를 규정하고 있다(제15조).⁵³⁹⁾ 이러한 헌법상의 규정들은 개인의 프라이버시를 보호하기 위한 것으로, 오늘날 개인정보보호에 있어서 간접적인 근거가 되는 것으로 이해될 수 있다.

2. 개인정보보호법제의 현황

(1) 1996년 개인정보처리법

이탈리아에서는 1996년 12월 31일에 개인정보보호에 관한 법률로 ‘개인정보 처리에서의 개인 및 기타 주체의 보호에 관한 법’(Law on the Protection of individuals and other subjects with regard to the Processing of Personal Data)이 제정되었다. 이 법은 유럽연합의 정보보호지침(95/46/EC)을 이행하기 위한 것으로, 1990년부터 6년간의 논의 끝에 제정된 것이었다. 1996년의 제정법은 전자적인 정보와 수기 정보를 모두 포함한 것으로 적용 주체는 공공부문과 민간부문 모두에게 적용되었다. 이에 따라 관련 법령을 조정하는 작업이 수년간 진행되었다.

539) <http://www.servat.unibe.ch/law/icl/it00000_.html> 참조.

특히 안보, 의료정보, 사법정보, 연구와 관련된 정보 등에 대해 규율하는 세부 명령이 발효되었다.

(2) 2003년의 개인정보보호법

다양한 법률에 산재한 개인정보보호관련 법률을 하나로 통합하기 위해 2003년 6월 30일에 개인정보보호법(Legislative Decree no. 196 of 30 Jun 2003)을 제정하였다.

이 법률은 일반적 영역은 물론, 특수한 영역까지 아우르고 있는 것이 특징이다. 그리고 국내에서 혹은 국가의 주권이 미치는 지역에 설립된 단체에 의해 실행되는 국내외 보유의 개인정보 처리에 적용된다(제5조 제1항). 이러한 개인정보처리법을 제정함에 있어서는 단순화(simplification), 조화(harmonisation), 효과성(effectiveness) 등 세 가지에 초점이 맞추어졌다.

3. 2003년 개인정보보호법의 구성⁵⁴⁰⁾

◆ 제 1 편 총칙

- 제 1 장 일반원칙

제 1 조: 개인정보보호에 관한 권리

제 2 조: 목적

제 3 조: 정보최소화의 원칙

제 4 조: 정의

제 5 조: 적용범위

제 6 조: 처리운영에 대한 규제

- 제 2 장 정보주체의 권리

540) <<http://www.garanteprivacy.it/garante/document?ID=1219452>> 참조.

제 7 조: 개인정보 열람권과 기타의 권리

제 8 조: 권리의 행사

제 9 조: 권리행사의 절차

제10조: 정보주체의 대응

- 제 3 장 정보처리의 일반원칙

제 1 절 공통원칙

제11조: 처리조건과 정보의 질

제12조: 행위준칙과 직업적 관행

제13조: 정보주체에 대한 설명

제14조: 정보주체와 제3자의 분류

제15조: 처리로 인한 손해

제16조: 처리운영의 기한

제17조: 특수한 위험이 따르는 처리운영

제 2 절 공공부문에 적용되는 특칙

제18조: 공공기관에 의한 모든 처리운영에 대한 원칙

제19조: 민감정보와 사법적 정보 이외의 정보처리에 대한 원칙

제20조: 민감정보의 처리에 대한 원칙

제21조: 사법적 정보의 처리에 대한 원칙

제22조: 민감정보 및 사법적 정보의 처리에 대한 원칙

제 3 절 민간부문에 적용되는 특칙

제23조: 동의

제24조: 정보처리에 동의가 요구되지 않는 경우

제25조: 제공과 전달의 금지

제26조: 민감정보에 관한 보호기준

제27조: 사법적 정보에 관한 보호기준

- 제 4 장 처리운영의 주체

제28조: 정보관리자

제29조: 정보처리자

제30조: 처리책임자

- 제 5 장 정보와 시스템의 안전

제 1 절 안전조치

제31조: 안전성의 요구

제32조: 특수한 정보관리자

제 2 절 최소한의 안전조치

제33조: 최소안전조치

제34조: 전자적 수단에 의한 처리

제35조: 전자적 수단에 의하지 않은 처리

제36조: 개선

- 제 6 장 특별임무의 수행

제37조: 처리의 통보

제38조: 통보절차

제39조: 제공의무

제40조: 일반적 위임

제41조: 위임요구

- 제 7 장 정보의 국제적 전송

제42조: 유럽연합에서의 정보유통

제43조: 승인된 제3국으로의 정보전송

제44조: 기타의 승인된 정보전송

제45조: 금지된 정보전송

◆ 제 2 편

• 제 1 장 사법부에서의 처리운영

제 1 절 총론(제46조-제49조)

제 2 절 아동(제50조)

제 3 절 법률정보서비스(제51-제52조)

• 제 2 장 경찰청에 의한 처리운영

제 1 절 총론(제53조-제57조)

• 제 3 장 국방과 안전

제 1 절 총론(제58조)

• 제 4 장 공공부문에서의 처리운영

제 1 절 행정기록의 열람(제59조-제60조)

제 2 절 공적 등록부와 사적 등록부(제61조)

제 3 절 출생, 사망, 결혼의 등록부 및 센서스 등록부와 전자리스트
(제62조-제63조)

제 4 절 중대한 공익적 활동의 경우(제64조-제73조)

• 제 5 장 의료부문에서의 개인정보 처리

제 1 절 총론(제75조-제76조)

제 2 절 설명에 의한 동의를 위한 간이조치(제77조-제84조)

제 3 절 중대한 공익적 활동이 경우(제85조-제86조)

제 4 절 의학적 처치(제87조-제89조)

제 5 절 유전정보(제90조)

제 6 절 기타 규정(제91조-제94조)

• 제 6 장 교 육

제 1 절 총론(제95-제96조)

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

- 제 7 장 역사적 · 통계적 · 과학적 목적을 위한 처리

제 1 절 총론(제97조-제100조)

제 2 절 역사적 목적의 처리(제101조-제103조)

제 3 절 통계적 또는 과학적 목적의 처리(제104조-제110조)

- 제 8 장 직업적 또는 사회적 안전의 문제

제 1 절 총론(제111조-제112조)

제 2 절 취업기록 및 고용정보(제113조-제115조)

제 3 절 원격감시와 전자근무의 금지(제116조)

- 제 9 장 은행, 금융과 보험 시스템

제 1 절 정보시스템(제117조-제120조)

- 제10장 전자통신

제 1 절 전자거래서비스(제121조-제132조)

제 2 절 인터넷과 전자네트워크(제133조)

제 3 절 비디오감시(제134조)

- 제11장 고용한 전문탐정과 사설탐정

제 1 절 총론(제135조)

- 제12장 출판, 문학, 예술 표현

제 1 절 총론(제136조-제138조)

제 2 절 시행규칙(제139조)

- 제13장 다이렉트 마케팅

제 1 절 총론(제140조)

◆ 제 3 편 구제와 제재

- 제 1 장 행정적 구제 및 사법적 구제

제 1 절 정보주체의 구제수단(제141조-제151조)

제 2 절 사법적 구제(제152조)

- 제 2 장 감독관청

제 1 절 개인정보보호위원회(제153조-제154조)

제 2 절 위원회의 조직(제155조-제156조)

제 3 절 조사와 통제(제157조-제160조)

- 제 3 장 제재

제 1 절 행정법규의 위반(제161조-제166조)

제 2 절 범죄행위(제167조-제172조)

- 제 4 장 개정, 폐지, 경과규정 및 종결규정

제 1 절 개정(제173조-제179조)

제 2 절 경과규정(제180조-제182조)

제 3 절 폐지(제183조)

제 4 절 종결규정(제184조-제186조)

◆ 부 칙

- 부칙A : 행위준칙

- 부칙B : 최소안전조치에 관한 기술적 특화

4. 2003년 개인정보보호법의 주요 내용

(1) 통칙적 규정(제1편)

각 기관은 위험성이 높은 민감한 개인정보를 처리할 때 개인정보보호위원회에 신고하여야 한다. 이러한 개인정보로는 유전적 자료, 개인을 분류하고 분석할 목적으로 처리되는 자료, 신용관련 정보 등이 있다. 이러한 신고절차는 정보처리과정을 개인에게 더욱 투명하게 하는

것을 보장할 목적을 갖고 있다.

또한 개인정보를 수집할 때는 최소한도에 그쳐야 한다. 법에 따라 개인정보를 수집·활용하고자 하는 기관들은 가능한 한 비개인적 정보를 사용하도록 되어 있다. 개정법에서는 정보주체의 권리행사를 보다 쉽게 하고, 위반사항에 대한 심리진행절차의 간소화를 꾀했다. 개인정보취급자의 침해행위에 대한 구체 심리에서 정보주체는 자신의 개인정보보호에 대한 권리가 침해된 사실만 주장하면 되고, 이들이 입은 피해가 침해행위에서 비롯된다는 것에 대한 입증책임을 하지 않도록 하여 입증책임의 전환을 명문화하였다.

한편, 개인정보의 국외이전과 관련 EU의 지침을 받아들여 EU의 영역내에서 개인정보를 다른 국가에 이전하는 경우 위원회에 신고하여 지시를 받도록 하였고, EU의 영역 밖의 나라에 개인정보를 이전하는 경우에는 상호주의 원칙에 입각해 이전받는 나라의 개인정보보호 수준이 이태리의 수준에 미치지 못하는 경우 개인정보를 이전하지 못하도록 제한하고 있다.

(2) 각론적 규정

개정법의 각론부분인 제2편(Part 2)은 개별법에 산재하던 개인정보 관련 중요 사항들을 통합하여 규정하고 있다. 이 각론부분에서 특히 중요한 부분은 인사에 관한 자료, 보전에 관한 자료, 전자통신 관련 자료 등이다.

인사에 관한 자료는 EU지침 중에서 민감한 정보와 관련된 자료로 취급된다. 신규채용시 수집하는 개인정보의 처리절차와 관련하여 개인의 신앙, 노조가입여부, 정치적 신념, 결혼상태, 건강상태, 유전적 정보 등에 대한 사항을 수집하지 못하도록 규정하고 있다.

한편, 보전에 관한 자료는 반드시 서면동의를 요하지 않고, 구술에 의한 동의만으로도 수집할 수 있도록 하였다.

전자통신정보와 관련하여서, 정보통신서비스 제공자는 요금징수 등을 목적으로 개인정보를 6개월 동안 까지만 보유할 수 있도록 하였고, 6개월이 지난 정보는 폐기하도록 하였다. 그러나 전화사용내역 (telephone traffic data)에 대해서는 범죄의 수사 및 예방을 위해 적어도 4년 동안 의무적으로 해당 자료를 보유하도록 하였다.

(3) 개인정보보호기구

개인정보보호위원회(Garante per la protezione dei dati personali)는 독립적인 지위에서 개인정보의 보호에 관한 업무를 총괄한다(제153조 제1항). 개인정보보호위원회에서는 개인정보침해에 따른 피해구제를 위한 개인정보심판권, 개인정보의 등록, 개인정보위반사항에 대한 조사권 등을 가진다.

5. 입법체계상 특징

이탈리아의 2003년 개인정보보호법은 공공부문과 민간부문을 포괄적으로 규율하는 방식을 취하고 있다. 나아가 동법은 본문이 전부 186개의 조항에 이를 만큼 방대하다. 제1편에서 정보주체의 권리, 정보처리의 일반원칙(공공부문과 민간부문의 특칙 포함), 정보와 시스템의 안전, 정보의 국제적 전송 등을 규정하고 있을 뿐만 아니라, 제3편에서 행정적 구제와 사법적 구제, 개인정보보호기구, 제재 등에 관해 규정하고 있다. 나아가 제2편에서는 경찰, 국방, 공익적 활동, 보건, 교육, 금융, 전자통신 등 특수한 영역에 적용되는 규정을 두고 있다. 제2편의 내용은 다른 나라에서 개별법으로 규율하는 사안이라고 할 수 있음에도 이를 동법에서 모두 규율하고 있다는 점이 특이하다고 할 수 있다. 이처럼 분야별로 다양한 법률에 산재하고 있는 개인정보보호 관련 개별 법률들을 한데 모아서 하나의 법률에서 규율하는 방식

을 취하고 있다는 점에서 이 법률은 단행법의 체계를 지향하고 있다.

이렇게 볼 때 이탈리아의 개인정보보호법은 일원적 단일법주의로 분류해도 무방할 것으로 본다. 이는 다른 국가에서 그 유례를 찾아보기 힘들 정도로 매우 독특한 입법적 모델이라고 평가할 수 있다.

제 7 절 스페인

1. 개 관

스페인은 세계에서 헌법에 프라이버시권(Privacy right)에 대한 명문의 규정을 두고 있는 몇 안 되는 나라들 가운데 하나이다.⁵⁴¹⁾ 즉 1978년의 스페인 헌법은 제18조에서 개인의 명예권·프라이버시권·초상권(제1항)(제1항) 및 우편·전보·전화통화의 비밀(제3항)을 보호하는 한편으로, “개인의 명예·품위·시민의 관계를 보장하기 위하여 정보처리의 이용을 법률로써 제한한다.”고 규정하고 있다(제4항).⁵⁴²⁾ 이러한 헌법적 근거와 EU 지침을 근거로 1992년 최초의 스페인 정보보호법(LORTAD)이 제정되었고, 이 후 1999년에 개인정보보호통합법(LOPD)으로 개정되었다. 1999년의 개정은 EU의 새로운 지침을 이행하기 위한 개정이었다.

여기서 개인정보를 포함하는 자동화된 파일의 보안조치에 대해 규정하였다. 동법은 모든 보안문서의 발급에 있어 관련자들의 동의를 얻어야 한다고 명시하고 있다. 최소 보안문서의 동의조건에는 애플리케이션과 보안문서의 범위, 보안측정치, 관련자의 기능과 책임, 개인정보를 포함하는 파일의 구조와 이 파일을 처리하는 컴퓨터 시스템의 구조 등이 제시되어야 하고, 불충분한 보안조치에 대한 통보 및 관리,

541) 1961년의 터키헌법 제15조, 1971년의 이집트헌법 제57조, 1975년의 포르투갈헌법 제33조 내지 제35조, 1978년의 스페인헌법 제18조 등이 있다. 권영성, 『신고헌법학원론』 (법문사, 1981), 337면 참조.

542) <http://www.servat.unibe.ch/law/icl/sp00000_.html> 참조.

추적의 절차에 대해서도 상세히 설명되어야 한다. 또한 정보의 백업 사본과 복구절차의 실행의 내용 등을 보안문서의 동의의 최소조건으로 규정하였다.⁵⁴³⁾

2 개인정보보호통합법(LOPD)의 구성

- 제 1 장 총 칙

제 1 조: 주체

제 2 조: 적용범위

제 3 조: 정의

- 제 2 장 정보보호의 원칙

제 4 조: 정보의 질

제 5 조: 정보수집에 대한 통보권

제 6 조: 정보주체의 동의

제 7 조: 특수한 정보의 보호

제 8 조: 건강에 관한 정보

제 9 조: 정보의 보안

제 10 조: 비밀유지의 의무

제 11 조: 정보의 전달

제 12 조: 제 3 자를 위한 정보의 열람

- 제 3 장 개인의 권리

제 13 조: 이의제기권

제 14 조: 정보보호등록국장과의 상담권

제 15 조: 열람권

제 16 조: 정정 · 파기권

543) 양용석, “해외 개인정보보호 관련 법과 제도의 고찰(3)”, 『정보보호 21c』 통권 제92호(보안뉴스, 2008. 4. 29) 참조.

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

제17조: 권리행사의 절차

제18조: 권리의 감독

제19조: 손해배상권

- 제 4 장 각칙

제 1 절 공공기관 보유의 파일

제20조: 구축, 조정, 폐기

제21조: 공공기관간의 정보 전달

제22조: 보안기관의 파일

제23조: 열람·정정·파기권의 배제

제 2 절 민간부문 보유의 파일

제25조: 구축

제26조: 통지와 등록

제27조: 정보전송의 통보

제28조: 공개된 자료에 포함된 정보

제29조: 신용정보서비스의 제공

제30조: 광고와 시장조사를 위한 처리

제31조: 광고의 등록

제32조: 개인정보보호지침

- 제 5 장 정보의 국제적 이동 (제33조-제34조)

- 제 6 장 정보보호청(Agencia de Proteccion de Datos)

제35조: 성격과 법적 지위

제36조: 기관장

제37조: 기능

제38조: 자문위원회

제39조: 정보보호등록국장

제40조: 조사권

제41조: 자치단체의 관련 기관

제42조: 자치단체의 파일

- 제 7 장 위반행위와 벌칙

제43조: 정보관리자

제44조: 위반행위의 유형

제45조: 벌칙

제46조: 공공기관에 의한 침해

제47조: 기한

제48조: 벌칙부과 절차

제49조: 비이동성 파일에 대한 권한

- 부가규정
- 경과규정

3. 개인정보보호통합법(LOPD)의 특징과 주요 내용

(1) 특 징

스페인의 개인정보보호통합법의 특징은 강력한 집행력에 있다. 다른 EU 국가들과 달리 600-60만 유로의 벌금을 개인정보보호 법규를 위반한 기업에게 부과할 수 있는 강력한 권한이 정보보호청(Agencia de Proteccion de Datos, APD)에 부여되었다. 이와 관련하여 스페인 헌법재판소는 2001년 판결에서 스페인 정보보호청의 강력한 권한보유가 헌법을 위반하는 것이 아니라는 판결을 내려 이를 정당화하였다. 정보보호청의 결정에 대해서 법원에 제소가 가능한데, 정치적·행정적 통제보다는 사법적 통제를 받고 있다.

(2) 개인정보보호의 원칙

스페인에서 컴퓨터 파일화된 개인정보는 다음과 같은 3단계의 보호가 이루어진다.⁵⁴⁴⁾

- ① **Basic Level** : 모든 종류의 개인정보에 적용되는 것이다. 이는 일반정보로 통상적인 개인정보 관리 절차에 의해 규율 받는다.
- ② **Medium Level** : 행정, 형사법, 금융, 세금관련 정보에 적용되는 것이다. 이는 보안정보로 특정한 보안담당관이 관리해야 하며, 정보관리활동을 감사대상으로 규정하고 있다.
- ③ **High Level** : 사상, 종교, 이념, 성적 취향, 건강, 인종, 경찰정보 등에 관련된 것으로 관련 당사자의 동의 없이 수집된 정보에 적용되는 것이다. 이와 관련된 정보의 배포는 해당 정보가 암호화되어 알아보기 어렵거나 식별하기 곤란하게 된 경우에만 가능하도록 하여 엄격하게 제한하고 있다.

위에서 개정정보의 수집자가 민감하지 않은 개인정보를 수집 또는 활용할 경우, 정보제공자의 사전동의(opt-in)를 받을 필요가 없으며, 또한 정보제공자가 정보를 수집하려는 사람의 고객일 경우 매 통신시에 opt-out 옵션을 부여하지 않아도 된다. 하지만 상업적 팩스나 이메일 등과 같은 통신 발송자의 고객이 아닌 일반 사람에게로의 발송을 원할 경우에는 반드시 사전동의(opt-in)의 방식을 통해서만 발송이 가능하다. 또한 opt-out 옵션을 위한 특정한 방법은 존재하지 않으나 정보제공자가 자신의 정보를 제공하고 있는 한 언제나 어떻게든 opt-out 옵션 사용(수정, 취소, 접근 방법 등)에 대해 숙지할 수 있도록 해야 한다.

개인정보의 활용과 유통을 위해서는 그 사용의 목적을 확실하고 명확하게 명시해야 한다. 구체적으로 개인정보의 수집인과 유통인은 항

544) Royal Decree 994/1999, of 11 June, which approves the Regulation on Mandatory Security Measures for the Computer Files which contain Personal Data

상 정보수집의 내용을 특정 단체에 보고할 때 그 목적을 확실히 하고 정보제공자의 사용목적에 대한 사전 동의를 받아야 한다.

만약 개인정보가 다른 곳으로 전송될 경우 그 정보 전송의 목적과 정보 수취인의 사용목적 또는 활용에 대한 내용도 정보제공자에게 알려야 하며, 이때 정보제공자가 이러한 전송에 대해 동의를 하지 않을 경우 정보수집자는 개인정보를 다른 곳으로 전송할 수 없다. 또한 정보제공자는 정보수집의 목적과 수취인, 정보에 대한 접속, 변경 또는 삭제 등의 권리를 가지고 법에 의해 보호받게 된다.

정보가 전산화가 됐든 안 됐든 개인정보가 수집되고 저장, 수정, 차단 등의 조작 행위가 일어났을 경우 이 모든 행위에 대해서는 그 정보가 활용되었다고 간주된다. 일반적인 개인정보의 활용에 대한 동의는 필요하지만, 필수사항으로 규정하고 있지는 않다. 하지만 민감한 개인정보로 분류되는 정보의 경우 그 활용 및 유통에 대해서는 정보제공자의 사전 동의가 필수적이다.

(3) 정보주체의 권리

정보주체의 권리로는 개인정보의 열람권, 정정권, 제3자 제공시 통보·동의권 등이 주어져 있다.

우선 정보제공자는 자신의 정보를 열람할 수 있는 권리를 가진다. 정보제공자는 자신의 신원을 증명 한 후 그 권리를 행사할 수 있다. 정보관리인은 정보제공자의 요청에 1개월 이내에 응해야 하며, 만약 정보관리인이 열람을 허용할 경우, 정보제공자는 통지가 있을 후 10일 이내에 정보의 열람이 이루어져야 한다. 만약 정보열람을 거부하였을 경우 정보관리인은 그 거부의 이유를 정보보호청에 보고하여야 한다. 다음으로 개인정보의 정정이 필요할 경우 정보제공자는 자세한 사유를 기재한 요청서를 정보관리인에게 송부하여야 한다. 정보관리인은 요청을 받은 후 10일 이내에 데이터베이스를 수정해야 하며, 또

한 정보제공자로부터 확인을 받아야 한다. 그러나 정정의 요청이 수용될 수 없을 경우에는 정보관리자는 항상 그 이유를 밝혀야 한다. 정보관리자는 정보보호청(APD)에게 이러한 개정에 대해 보고할 수 있고, 정보보호청은 그 거부의 이유가 타당한지의 여부를 확인한다.

(4) 개인정보의 국외이전

EU 회원국이 아닌 다른 나라의 정보처리자에게 전송을 원할 경우 정보보호청(APD)은 해당 관리자에게 데이터베이스의 등록에 있어 모델 조항의 사용 여부에 대한 서명된 협약서의 사본을 요구할 수 있다. 추가적인 국제전송에 대한 정보는 정보보호청이 발간하는 정보에서 찾아볼 수 있다. 컴퓨터 시스템의 어떠한 종류의 정보전송과 지원 정보 간의 우편 또는 다른 형식으로 스페인이 아닌 다른 곳에 상주하고 있는 정보처리자에게 정보를 전송하는 행위를 국제전송으로 규정한다. 스페인 법률상 이러한 정보의 국제전송은 스페인 법과 비슷한 수준의 개인정보보호법이 제정되어 있는 나라에 대해서만 할 수 있다. 만약 정보가 충분한 개인정보보호법이 제공되지 않는 나라로 전송하려면, 정보제공자의 동의나 정보보호청의 승인이 있어야만 한다. 하지만 다수의 예외, 즉 정보제공자의 동의와 정보보호청의 승인이 필요하지 않은 경우가 법에 정해져 있다.

정보보호청에서 승인한 특정 정보의 국제전송에 관한 지침이 존재하는데, 본 규칙은 개인정보를 스페인 밖으로 전송시키는 관리인은 정보제공자에게 정보수취인의 정보와 국제전송의 이유를 알려야 하고 정보관리인이 국제전송을 원할 경우 정보보호청에게 정보가 전송될 국가와 이유를 통지해야만 한다.

(5) 벌 칙

만약 정보관리자 및 관련자가 스페인 법에서 규정하는 법률을 위반하였을 경우 정보보호청은 직접 그 위반의 정도에 따라 10만~1억 Ptas의 벌금을 부과할 수 있다(제45조). 경우에 따라 위반 데이터베이스를 폐지 및 동결시킬 수 있다.⁵⁴⁵⁾

(6) 개인정보보호기구

스페인에서 개인정보보호에 관한 업무를 담당하는 기구는 정보보호청(Agencia de Proteccion de Datos, APD)이다. 정보보호청은 개인정보보호통합법의 위반에 대한 조사권, 벌금 부과권, 동법 위반기관이 보유한 개인정보의 차단권 등을 포함한 집행권을 갖고 있으며, 중앙정부와 민간기업을 모두 대상으로 법을 집행한다.

4. 입법체계상 특징

스페인의 개인정보보호법제 시스템은 개인정보보호통합법이라는 이름에서 보듯이 공공부문과 민간부문을 포괄하여 규율하는 방식을 택하고 있다.

그리고 정보보호의 원칙(제2장), 개인의 권리(제3장), 공공기관 보유 파일에 관한 규율(제4장 제1절), 민간부문 보유 파일에 대한 규율(제4장 제2절), 정보의 국제적 이동(제5장), 개인정보보호기구로 설치된 정보보호청(제6장), 위반행위와 벌칙(제7장) 등을 규정하고 있는 점에 비추어 볼 때 개인정보보호통합법은 개인정보보호에 관한 기본법이라기보다는 일반법의 체제를 취하고 있다고 할 수 있다. 그 밖에 특수한

⁵⁴⁵⁾ 이상 양용석, “해외 개인정보보호 관련 법과 제도의 고찰(3)”, 『정보보호 21c』 통권 제92호(보안뉴스, 2008. 4. 29) 참조.

분야에 대한 규율은 개별법에 의해 개인정보의 보호가 이루어지고 있다고 볼 수 있다.

결국 스페인의 입법체계는 일원적 일반법주의, 즉 통합형 일반법의 체계로 평가할 수 있을 것이다.

제 8 절 일 본

1. 개인정보보호법의 제정과 개정

1970년대의 소위 國民總背番号制의 도입을 둘러싼 논란을 계기로 개인정보보호에 대한 국민적 관심은 크게 증대되었다. 이후 1975년 도쿄도(東京都)의 구니타치시(國立市)의 프라이버시보호조례가 제정되었고, 사회당의 「개인정보보호기본법안(요강)」과 「개인정보에 관련된 컴퓨터규제법안」 발표 등이 뒤를 이었다. 그리고 1980년에 채택된 OECD의 “프라이버시보호와 개인정보의 국제유통에 대한 가이드라인에 관한 이사회권고”가 나오자, 이에 대한 중앙정부의 차원에서 대응책이 본격적으로 모색되기 시작되었다. 1981년 1월부터 행정관리청에 프라이버시보호연구회가 설치되었고, 1982년 7월에 “개인정보처리에 따른 프라이버시 보호대책”이라는 검토결과가 발표되었다.

이러한 상황을 거쳐서 마침내 1988년 4월 28일에 “행정기관이 보유하는 전자계산기 처리에 따른 개인정보의 보호에 관한 법률안”이 일본의 의회에 제출되었다. 이 법안에 대해서는 당초 정부 부처들 사이에 상당한 이견이 노출되었다. 당시 주무 부서인 郵政省은 동법의 제정이 수상실의 권한을 강화할 것이라고 우려하였으며, 국민연금과 의료처리에 관한 개인 정보를 보유하고 있는 厚生省도 달갑지 않은 태도를 보였다. 그리고 국가경찰청은 범죄수사에 대한 개인기록의 적용이 제외되어 있었음에도 이 법안의 효과에 대해서 우려를 표명하고

나섰다.⁵⁴⁶⁾ 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」(行政機關の保有する電子計算器處理に係る個人情報保護に關する法律)로서 공포되었으며(법률 95호), 1989년 10월부터 부분적인 시행을 거쳐 1990년 10월부터 總務廳을 주무관청으로 하여 전면 시행에 들어갔다.

동법은 1999년 12월 8일에 제1차 개정이 있었고(법률 151호), 동년 동월 22일에 제2차 개정이 있었으며(법률 160호), 2002년 7월 31일에 제3차 개정이 있었다(법률 100호). 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, 정보관리자인 공공기관의 책임자에 대한 처벌규정이 미비하다는 점 등이 문제점으로 지적되고 있었다.⁵⁴⁷⁾

한편, 일본에서는 공공부문과 민간부문에 모두에 적용할 기본법을 제정하기 위한 노력이 활발하게 전개되어 왔다. 특히 고도정보통신사회추진본부 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) 보

546) UNCTAD, "Data Protection," Trade and Development Report(TDR), 1988, p. 25; 이원부 등, "정보통신망에서의 개인정보 침해사례 분석 및 이용규제방안 연구", 『기술정책연구 98-6』(한국정보보호센터, 1998. 12). 93면 재인용.

547) UNCTAD, "Japan Adopt Privacy Protection Act," Trade and Development Report(TDR), 1989, pp. 24-25.

도·출판·학술·연구분야에 대해서는 원칙의 적용을 제외하는 방안이 검토되었다.⁵⁴⁸⁾

이후 정부의 정보통신기술(IT) 전략본부에 개인정보보호법법제화전문위원회가 설치되어 2000년 초부터 검토작업에 들어갔다. 이 위원회는 그간의 논의를 토대로 하여 같은 해 6월에 『개인정보보호기본법제에 관한 대강안(중간정리)』, 같은 해 10월 11일에 『개인정보보호기본법제에 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 中間整理에서는 “표현의 자유, 학문의 자유 등에 충분히 유의한다”라고만 되어 있어서 표현의 자유를 침해한다는 야당, 언론, 시민단체 등의 강력한 반대에 부딪치게 되었다. 같은 해 8월에는 일본신문협회, 일본민간방송연맹과 일본방송협회가 공동성명을 발표하고 수상관저에서 관방장관에게 성명문을 전달하기도 하였다. 결국 보도기관에 대해서는 사업자의 업무에 관한 규정을 大綱의 적용에서 제외하기로 하였다. 이러한 과정을 거쳐 2001년 3월 27일에 『개인정보보호에 관한 법률안』(個人情報の保護に関する法律案)이 국회에 제출되었고, 이에 대해 같은 해 가을의 임시국회에서 논의를 거듭하였다. 이듬해인 2002년 봄의 통상국회에서는 행정기관개인정보보호법, 독립행정법인등개인정보보호법, 정보공개·개인정보보호심사회설치법, 정비법의 각 법안도 제출되었고, 이들을 포함한 個人情報保護關連5法案이 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.⁵⁴⁹⁾

548) 박광진 등, “정보통신서비스에서의 개인정보보호에 관한 지침(안) 연구”, 『기술정책연구 99-2』 (한국정보보호센터, 1999. 12), 9면.

549) 정상호, “일본 개인정보보호법 제정 추진동향”, 『해외정보보호동향』 (한국정보보호진흥원, 2003. 2), 13면; 황상철, “일본의 개인정보보호를 위한 입법동향 - 개인정보

이후 여당 3당에 의해 그 수정안이 마련되어 2003년 통상국회에서 다시 입법화가 추진되었고, 마침내 2003년 5월 23일에 「개인정보의 보호에 관한 법률」(平成15年 법률 제57호), 「행정기관이 보유하는 개인정보의 보호에 관한 법률」(平成15年 법률 제58호), 「독립행정법인등이 보유하는 개인정보의 보호에 관한 법률」(平成15年 법률 제59호), 「정보공개·개인정보보호심사회설치법」(平成15年 법률 제60호), 「행정기관이 보유하는 개인정보의 보호에 관한 법률등의 시행에 따른 관계 법률의 정비등에 관한 법률」(平成15年 법률 제61호) 등 個人情報保護關連5法이 국회에서 성립되어 5월 30일 공포되기에 이르렀다.⁵⁵⁰⁾

2. 개인정보보호법제의 체계

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 함)을 두게 되었다. 그리고 공공부문을 규율하는 일반법으로 「행정기관이 보유하는 개인정보의 보호에 관한 법률」(이하, ‘공공기관 개인정보보호법’이라 함)과 「독립행정법인등이 보유하는 개인정보의 보호에 관한 법률」(이하, ‘독립행정법인등 개인정보보호법’이라 함)이 존재한다.

지방자치단체에 있어서는 개인정보보호조례에 의해 규율이 이루어진다. 이 밖에 개별분야의 개인정보보호에 대하여서는 기본법에 정하여 두고 있지 않고, 개별법에 산재하여 개인정보를 보호하고 있다. 이러한 개인정보보호법제의 체계를 도표화하면 아래와 같다.⁵⁵¹⁾

보의보호에관한법률안을 중심으로-”, 『법제』(법제처, 2003. 1), 67면 등 참조.
550) 이상 :岡村久道, 『新法解説 個人情報保護法入門』(商事法務, 2003), 65-71頁 참조.
551) 岡村久道, 『新法解説 個人情報保護法入門』(商事法務, 2003), 2면 참조.

[표 3-1-4] 일본의 개인정보보호 법률체계

구 분	공 공 부 문			민 간 부 문
대상	국가행정기관	독립행정기관, 특수법인, 행정기관에 준 하는 기관	지방 공공단체	민간부문
기본법	‘개인정보의 보호에 관한 법률’ [기본이념 등 기본법 부분] - 개인정보의 적절한 취급에 관한 기본원칙 - 국가, 지방자치단체의 책무 - 민간 개인정보취급사업자의 의무 - 사업자 및 인정개인정보보호단체에 의한 자율적인 피해구제제도			
일반법	‘행정기관이 보유하는 개인 정보의 보호에 관한 법률’ - 일반행정기관 보유 개인 정보의 적절한 취급원칙 - 이용목적 내의 정보보유 - 목적외 이용·제공금지 - 정보주체의 열람, 정정, 이용정지청구권 인정	‘독립행정법인 등이 보유하는 개인정보의 보 호에 관한 법률’ - 일반행정기관과 동일하게 취급됨	개인정보 보호조례	‘개인정보보호에 관한 법률’에서 규율 [개인정보취급사 업자의 의무 등 일반법 부분]
개별법				전기통신사업법, 대금업법, 노동 자파견법 등
	유전자기술규제법(クローン기술규제법), 직업안정법 등			

이렇게 볼 때 일본의 개인정보보호법제는 통합형 기본법과 부문별 일반법, 그리고 개별법이 병존하는 구조라고 할 수 있고, 이를 굳이 유형화하자면 ‘일원적 기본법주의’에 속하는 것으로 평가할 수 있을 것이다.

제 9 절 외국 입법체계의 종합적 분석

1. 개인정보보호법제의 비교

[표 3-1-5] 미국·캐나다·영국·독일의 개인정보보호법제 비교

	미국	캐나다	영국	독일
법률의 명칭	프라이버시법 (PA)	프라이버시법(PA) / 개인정보보호법 (PIPEDA)	정보보호법 (DPA)	연방정보 보호법 (BDSG)
규율 범위	공공부문	공공부문 / 민간부문	공공부문, 민간부문	공공부문, 민간부문
보호 범위	비전산 정보 포함	비전산 정보 포함	비전산 정보 포함	비전산 정보 포함
개인정보보호 원칙			§4, 부칙1	
일반적 수집의 제한	§552a(e)(2)-(3)	§§4-5	§4, 부칙1	§§4, 13, 28-31
특수정보의 수집 제한	§552a(e)(7)		§2, 부칙1	§§3(ix), 13②
보유의 제한	§§552a(e)(1), (5),(6),(9),(10)	§6	부칙1	§§3a, 5, 9
시스템 설치의 제한	연방관보 고시 §552a(e)(4), (11)	DB색인 발행 §§10-11	신고 (§§18-19)	신고 (§§4d-4e)

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

	미국	캐나다	영국	독일
이용·제공의 제한	§§552a(e)(1), (5),(6),(8)	§§7-8	부칙1 제3 원칙, §§28-36	§§4, 14-16, 28-31
국외 전송 제한			부칙1 제8 원칙	§§4b, 4c
영향 평가 실시	전자정부법 §208	PA §71(1)(d) / 재무관리법 §7		
정보주체의 권리	열람·정정 §§552a(d)	열람·정정·보완 (§§12-17)	열람·정정·차단 등 (§§7-15)	열람·정정·말소 등 (§§6, 19-20, 33-35)
손해 배상	§552a(d)(g)			§§7-8
보호 기구 설치	(예산관리처) §552a(v)	프라이버시감독관 (§§38-40, 53-54)	정보감독관 (§§18-19, 51)	연방정보위원 (§§22-26)
벌칙	§552a(d)(g)	§16	§60②,④	§§43-44

[표 3-1-6] 프랑스·이탈리아·스페인·일본의 개인정보보호법제 비교

	프랑스	이탈리아	스페인	일본
법률의 명칭	정보처리법 (2004)	개인정보보호법 (2003)	개인정보보호통합법(1999)	개인정보보호법 (2003)
규율 범위	공공부문, 민간부문	공공부문, 민간부문	공공부문, 민간부문	공공부문, 민간부문
보호 범위	비전산 정보 포함	비전산 정보 포함	비전산 정보 포함	비전산 정보 포함

	프랑스	이탈리아	스페인	일본
개인정보보호 원칙		제1편 제3장	§§4-12	
일반적 수집의 제한	§§25, 40-4	제1편 제3장	§§5-6	§§17-18
특수 정보의 수집 제한	§§1, 31 (입력제한)	§§20-22, 26-27	§§7-8	
보유의 제한	§§28, 28-2, 31	§§31-36	§§9-10	§§19-22
시스템 설치의 제한	등록부 공시 (§11), 신고(§16)		통지, 등록 (§26)	공표 (§24)
이용·제공의 제한	§§2, 40-3, 40-5	제1편 제3장	§§11-12, 21, 27-31	§23
국외 전송 제한		제1편 제7장	§§33-34	
영향 평가 실시				
정보주체의 권리	열람·정정·말소 등 (§§34-41, 3, 27)	열람·정정·삭제 등 (§7)	열람·정정·파기 (§§13-17)	개시·정정·추가 등 (§§25-28)
손해 배상		§15	§19	

	프랑스	이탈리아	스페인	일본
보호 기구 설치	정보위원회 §§6-8, 21-35	정보보호위원회 (제3편 제2장)	정보보호청 (§§35-42)	주무대신 (§§33-36)
벌칙	§45	제3편 제3장	§45, 48	§§56-59

2. 입법방식의 분류

지금까지 살펴본 해외의 개인정보보호법제를 비교·분석해볼 때, 그 입법체계상의 특징은 대체로 다음의 다섯 가지의 입법모델로 나누어서 살펴볼 수 있다.⁵⁵²⁾

(1) 이탈리아식 입법모델

이탈리아의 경우 공공부문과 민간부문을 통합적으로 규율하면서도 개별적인 분야에서의 규율대상까지 포괄적으로 아우르는 단일의 개인정보보호법을 갖고 있는바, 이는 통합형 단일법의 체계, 즉 ‘일원적 단일법주의’라고 평가할 수 있다.

(2) 유럽식 입법모델

영국, 독일, 프랑스, 스페인 등 유럽 제국은 개인정보보호법에서 공공부문과 민간부문에 공통적으로 적용될 수 있는 추상적이고 기초적인 원칙뿐만 아니라 각 부문별로 준수해야 할 개인정보의 취급상 의무, 정보주체의 권리, 피해구제, 보호기구 등을 세세하게 규정하고 있다는 점에서 통합형 일반법을 두고 있으면서,⁵⁵³⁾ 각 분야별로 특수하

552) 입법체계의 유형별 분석은 홍준형, 『개인정보보호법제 정비를 위한 기본법 제정 방안 연구』(한국전산원, 2004), 87-88면을 참조.

게 규율되어야 할 사항들을 구체화시키는 입법의 방식을 채택하고 있는바, 이는 통합형 일반법과 분야별 개별법의 체계, 즉 ‘일원적 일반법주의’로 분류할 수 있다.

(3) 일본식 입법모델

일본의 경우 통합형 기본법에 속하는 개인정보보호법, 공공부문의 일반법에 속하는 행정기관개인정보보호법, 민간부문의 일반법에 속하는 개인정보보호법, 기타 전기통신사업법, 대금업법, 노동자과건법, 유전자기술규제법, 직업안정법 등의 개별입법이 존재하므로, 이는 통합형 기본법, 부문별 일반법, 개별법의 체계, 즉 ‘일원적 기본법주의’로 분류할 수 있다.

(4) 캐나다식 입법모델

캐나다의 경우 공공부문과 민간부문을 통합하는 기본법 없이 각각 공공부문에 적용되는 일반법과 민간부문에 적용되는 일반법을 두고 있는데, 이는 부문별 일반법의 체계, 즉 ‘이원적 일반법주의’라고 말할 수 있다.

(5) 미국식 입법모델

미국의 경우 공공부문과 민간부문의 통합형 입법이 존재하지 않고, 다만 공공부문의 일반법에 속하는 프라이버시법과 각종 개인정보보호 관련 사항을 규정한 개별법에 의존하고 있다. 이는 제한적 일반법과 분야별 개별법의 체계, 즉 ‘이원적 개별법주의’라고 할 수 있다.⁵⁵⁴⁾

553) 홍준형 교수는 유럽 제국의 개인정보보호법을 ‘기본법’으로 파악하면서, 입법체계를 ‘일원적 개별법주의’로 분류하고 있다. 동인, 『개인정보보호법제 정비를 위한 기본법 제정방안 연구』(한국전산원, 2004), 87-88면.

554) 미국식의 경우, 공공부문을 여러 분야 중 한 분야로 놓고 보면, 공공부문의 프라이버시, 교육의 프라이버시, 금융 프라이버시, 전기통신 프라이버시, 운전자 프라

[표 3-1-7] 각국의 개인정보보호 법률체계

분류	법률체계(입법방식)	국가, 법률명
이탈리아식 모델	일원적 단일법주의	개인정보보호법
유럽식 모델	일원적 일반법주의 (일반법-개별법)	영국, 정보보호법
		독일, 연방정보보호법
		프랑스, ‘정보처리과일 및 자유에 관한 법률’
		스페인, 개인정보보호통합법
일본식 모델	일원적 기본법주의 (복합형: 기본법-일반법)	공·사부문 기본법: ‘개인정보 보호에 관한 법률’
		공공부문 일반법: 행정기관개인정보보호법 ⁴
		민간부문 일반법 : ‘개인정보 보호에 관한 법률’
캐나다식 모델	이원적 일반법주의 (부문별 일반법)	공공부문 일반법: 프라이버시법
		민간부문 일반법: ‘개인정보 보호 및 전자 문서에 관한 법률’
미국식 모델	이원적 개별법주의 (기본법·일반법 없음)	관련 개별법에 산재

3. 입법모델별 장단점 분석

(1) 이탈리아식 입법모델

통합형 단일법의 체계, 즉 ‘일원적 단일법주의’는 수범자의 혼란이나 보호체계상의 불균형을 최소화할 수 있다는 점에서 장점이 있다. 하지만 단일법의 체계를 취할 경우 예기치 못한 새로운 문제를 커버

이버시 등의 개별법 중 하나로 분류될 수 있을 것이다. 홍준형, 위 보고서, 88면, 각주 101번.

하지 못해 법적 공백이 발생하는 것이 불가피하며, 분야별 특수한 상황에 대처하기 위하여 수시로 법률의 개정에 나서야 한다는 점에서는 문제가 적지 않다. 한편, 개인정보보호법의 집행에 관한 통일적인 감독체계가 갖추어져 개인정보보호의 정도를 강화할 수 있을 것으로 기대된다. 하지만 단일법의 체계를 취할 경우 감독관청도 일원화되어야 할 것이므로 법을 집행하기 위한 매우 큰 규모의 감독기구가 필요하게 된다. 이렇게 되면 조직이 비대해지는 만큼 운영상의 경비가 증대될 것이다. 뿐만 아니라 단일법으로의 전환에 따라 입법과정에 소요되는 비용도 막대할 것으로 예상된다.

(2) 유럽식 입법모델

통합형 일반법과 분야별 개별법의 체계, 즉 ‘일원적 일반법주의’는 현행의 법체계에 크게 변경을 가하지 않으면서도 법적 공백을 최소화할 수 있다는 장점이 있다. 일반법이 분야별 개별법에 특별한 규정을 두지 않을 경우에 대비하여 일차적으로 적용될 수 있는 사항들을 폭넓게 규정하게 되면, 개별법에서는 각 영역의 특수성에 맞게 개인정보보호방안을 강구할 수 있을 것이기 때문이다. 물론 이 경우에도 수범자의 혼란이나 보호체계상의 불균형을 최소화할 수 있는 장점이 있다. 또한 법제정의 비용이나 제정 이후 집행상의 비용도 그리 크지는 않을 것으로 예상된다.

(3) 일본식 입법모델

통합형 기본법, 부문별 일반법, 개별법의 체계를 취하는 이른바 ‘일원적 기본법주의’는 만일 기본법의 체제를 취하면서도 각 부문별 일반법을 별도로 두지 않을 경우 다수의 개별법으로써 전 영역의 개인정보를 커버할 수 있어야 하는 부담이 생긴다. 아무리 많은 개별법을 제정하더라도 그들 입법의 보호범위에 속하지 않는 분야가 생겨날 경우에

는 법적 보호의 공백이 발생할 수밖에 없다. 기본법의 특성상 보충적인 성격의 실체적 사항까지 규정되어 있지 않을 것이기 때문이다.

(4) 캐나다식 입법모델

공공부문과 민간부문을 통합하는 기본법 없이 각각 공공부문에 적용되는 일반법과 민간부문에 적용되는 일반법을 두는 부문별 일반법의 체계, 즉 ‘이원적 일반법주의’에서는 개인정보보호의 사각지대는 크게 우려하지 않아도 되겠지만, 법제를 정비하는 과정에서 소요되는 비용이 통합형 일반법주의에 비해 클 수밖에 없을 것이다.

(5) 미국식 입법모델

제한적 일반법과 분야별 개별법의 체계, 즉 ‘이원적 개별법주의’는 원론적인 측면에서 볼 때 개별법적 규율의 방식에 의한 접근이 개인정보의 활용에 대한 과도한 억제를 방지할 수 있다는 장점이 있다. 하지만 새로운 개인정보침해의 양상에 대처하기 위해 끊임없이 새로운 입법을 해야 하므로 입법에 소요되는 비용이 만만치 않다는 점에 문제가 있다. 또한 다수의 개별 법률들이 양산될 경우 수범자의 법적 혼란이 야기된다는 점도 무시할 수 없는 단점이라고 하겠다.

제 2 장 실증적·경험적 조사결과 분석

제 1 절 설문조사의 개요

1. 설문조사의 배경

우리나라에서는 현재 공공부문과 민간부문이 분야별로 각기 다른 법률에 의해 규율되고 있다. 하지만 개인정보보호의 입법이 다수 존재함에도 불구하고 우리나라에서는 사회 각 분야의 개인정보 침해 사례가 줄어들지 않고 오히려 새로운 형태의 그 피해가 확산되어 가는 추세에 있다.

이에 따라 현행의 입법체계로는 개인정보처리의 위험성으로부터 개인의 존엄과 자기결정권을 보호하기 어렵다는 인식하에 개인정보보호법에 관한 입법체계를 새롭게 정비하려는 움직임이 가시화되어 왔다. 그 동안 국회의원들이나 정부에서도 개인정보보호 관련 법안들을 수차례에 걸쳐 제출한 바 있으나, 아직도 개인정보보호에 관한 입법체계에 관한 정비작업이 성과를 거두지 못하고 있다.

입법체계의 정비방향과 관련하여서는 현행과 유사하게 공공부문과 민간부문을 분리하여 별도의 입법체계로 가져가자는 입장과 공공과 민간을 통합한 입법체계를 새로이 마련하자는 입장이 대립되고 있다. 후자의 통합입법론에서도 공공부문과 민간부문에서의 개인정보처리에 관한 일반적 사항을 모두 규정하는 통합일반법의 형태로 가자는 방안과 공공과 민간의 양 부문에 공통적으로 적용될 기본적인 사항만 규정하는 통합기본법의 형태로 가자는 방안이 제시되고 있다.

개인정보보호법제의 정비는 어느 입법의 체계가 개인정보보호에 있어서 더 실효적이며 법집행에 있어서 실효성이 있겠는가 하는 점을 면밀히 분석하여 추진되어야 할 것으로 본다.

이러한 문제의식을 가지고 연구진은 개인정보보호를 위한 최적의 입법체계가 무엇인지를 모색하기 위해 일반 수범자와 관련 전문가들을 대상으로 하여 각각 다음과 같은 설문조사를 실시하게 되었다.

2. 일반인 대상 조사의 내용

[질문 1] 그 동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

- ① 있다
- ② 없다

[질문 1-1] 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

- ① 어려움이 있었다
- ② 어려움이 별로 없었다

[질문 1-2] 어려움을 느낀 이유는 무엇이라고 생각하십니까?

- ① 개인정보보호법의 존재를 몰라서
- ② 개인정보보호에 관한 법률이 하나로 되어 있지 않아서
- ③ 분야별로 관련 법률이 잘 구분되어 있지 않아서
- ④ 새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않아서
- ⑤ 기타()

[질문 2] 다음 법률 가운데 개인정보의 보호를 위한 내용이 포함되어 있을 것으로 짐작되는 법률을 모두 선택하여 주십시오.

- ① 공공기관의 개인정보보호에 관한 법률
- ② 정보통신망 이용 촉진 및 정보보호 등에 관한 법률

- ③ 신용정보의 이용 및 보호에 관한 법률
- ④ 전자정부법
- ⑤ 금융실명거래 및 비밀보장에 관한 법률
- ⑥ 통신비밀보호법
- ⑦ 보건의료기본법
- ⑧ 주민등록법
- ⑨ 국세기본법
- ⑩ 특정범죄신고자 등 보호법
- ⑪ 형법
- ⑫ 위의 법률 어느 것에도 포함 되어 있지 않을 것 같음

[2-1] 우리나라의 현행 개인정보보호 관련 입법은 공공부문과 민간 부문으로 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[2-2] 공공부문의 개인정보보호에 적용되는 「공공기관의 개인정보보호에 관한 법률」은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

- ① 잘 알고 있다
- ② 막연히 짐작하고 있는 정도이다
- ③ 공공기관이 보유하는 개인정보는 모두 보호의 대상이 되는 줄 알았다
- ④ 컴퓨터로 처리되지 않는 개인정보도 보호를 받을 수 있는 줄 알았다
- ⑤ 모든 개인정보가 그 보호의 대상이 되는 줄 알았다
- ⑥ 전혀 몰랐다

[2-3] 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며 개별 분야별로 적용되는 법률이 따로 존재합니다.

이러한 사실에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[질문 3] 현재 본인의 개인정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보호되고 있다고 느끼십니까?

답란	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
	①	②	③	④	⑤

[질문 4] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이라고 생각하십니까 1순위부터 3순위까지 응답하여 주십시오.

1순위 _____ 2순위 _____ 3순위 _____

- ① 법률규정의 미비 내지는 복잡성
- ② 교육이나 홍보부족
- ③ 정부나 사업자의 인식부족
- ④ 일반인의 인식부족
- ⑤ 개인정보 활용의 필요성
- ⑥ 기타()

[질문 5] 현재는 개인정보가 부분적으로 보호되고 있습니다. 개인정보 보호를 보다 강화하기 위한 『개인정보보호법』의 제정이 필요하

다고 생각하십니까?

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 보통이다
- ④ 시급하지는 않지만 필요하다
- ⑤ 시급히, 매우 필요하다

3. 전문가 대상 조사의 내용

(1) 개인정보보호법제의 현황에 대한 인식 조사

[문1] 그 동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

- ① 있다
- ② 없다

[문1-1] 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

- ① 어려움이 있었다
- ② 어려움이 별로 없었다

[문1-2] 어려움을 느낀 이유는 무엇이라고 생각하십니까?

- ① 개인정보보호법의 존재를 몰라서
- ② 개인정보보호에 관한 법률이 하나로 되어 있지 않아서
- ③ 분야별로 관련 법률이 잘 구분되어 있지 않아서
- ④ 새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않아서
- ⑤ 기타 ()

[문2] 다음 법률 가운데 개인정보의 보호를 위한 내용이 포함 되어 있을 것으로 짐작되는 법률을 모두 선택하여 주십시오.

- ① 공공기관의 개인정보보호에 관한 법률
- ② 정보통신망 이용 촉진 및 정보보호 등에 관한 법률
- ③ 신용정보의 이용 및 보호에 관한 법률
- ④ 전자정부법
- ⑤ 금융실명거래 및 비밀보장에 관한 법률
- ⑥ 통신비밀보호법
- ⑦ 보건의료기본법
- ⑧ 주민등록법
- ⑨ 국세기본법
- ⑩ 특정범죄신고자 등 보호법
- ⑪ 형법
- ⑫ 위의 법률 어느 것에도 포함 되어 있지 않을 것 같음

[문3] 우리나라의 현행 개인정보보호 관련 입법은 공공부문과 민간 부문으로 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[문4] 공공부문의 개인정보보호에 적용되는 『공공기관의 개인정보보호에 관한 법률』은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

- ① 잘 알고 있다
- ② 막연히 짐작하고 있는 정도이다

- ③ 공공기관이 보유하는 개인정보는 모두 보호의 대상이 되는 줄 알았다
- ④ 컴퓨터로 처리되지 않는 개인정보도 보호를 받을 수 있는 줄 알았다
- ⑤ 모든 개인정보가 그 보호의 대상이 되는 줄 알았다
- ⑥ 전혀 몰랐다

[문5] 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며 개별 분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[문6] 현재 본인의 개인 정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보호되고 있다고 느끼십니까?

답란	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
	①	②	③	④	⑤

[문7] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이라고 생각하시는지 1순위부터 3순위까지 응답하여 주십시오.

1순위 _____ 2순위 _____ 3순위 _____

- ① 법률규정의 미비 내지는 복잡성
- ② 교육이나 홍보부족
- ③ 정부나 사업자의 인식부족
- ④ 일반인의 인식부족

- ⑤ 개인정보 활용의 필요성
- ⑥ 기타()

[문8] 현재는 개인정보가 부분적으로 보호되고 있습니다. 개인정보 보호를 보다 강화하기 위한 「개인정보보호법」의 제정이 필요하다고 생각하십니까?

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 보통이다
- ④ 시급하지는 않지만 필요하다
- ⑤ 시급히, 매우 필요하다

(2) 개인정보보호법제의 입법체계에 대한 인식 조사

[1] 최근 우리나라에서 새로운 개인정보보호법을 제정하려는 움직임이 있는 것에 대해 알고 계십니까?

- ① 알고 있다
- ② 모르고 있다

[2] 개인정보보호를 위해 공공부문과 민간부문을 별도로 규율하고 있는 현행의 방식에서 탈피해서 양 부문을 모두 포괄할 수 있는 통합적 법률의 제정이 필요하다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

- ① 찬성한다
- ② 반대한다
- ③ 모르겠다

[2-1] 통합적 법률의 제정에 찬성하시는 이유는 다음 중 어느 것입니까? 순서대로 2가지를 선택하여 주십시오.

1순위: _____ 2순위: _____

- ① 양 부문을 굳이 달리 규율해야 할 이유가 없다
- ② 일반 국민들의 법적 혼란을 줄이기 위해 필요하다
- ③ 법적 보호의 공백을 최소화하기 위해 불가피하다
- ④ 양 부문에 걸쳐 법집행의 통일을 기할 필요가 있다
- ⑤ 기타 ()

[2-2] 통합적 법률의 제정에 반대하신다면 그 이유는 무엇입니까? 순서대로 2가지를 선택하여 주십시오.

1순위: _____ 2순위: _____

- ① 통합적 법률의 제정은 공공부문과 민간부문의 차이점을 무시하는 것이다
- ② 법적 보호의 공백은 각 부문별 법률의 제정이나 개정을 통해서도 해소할 수 있다
- ③ 분야별 개별법이 존재하는 이상 수범자의 법적 혼란은 불가피하다
- ④ 민간부문에 관한 특칙을 둘 경우 법제통합의 의미는 크지 않다
- ⑤ 기타 ()

[3] 통합적 법률을 제정할 경우 기본법의 체계(공공부문과 민간부문에 관한 기본적인 사항만 정하고, 나머지는 특수한 분야별 개별 법률에 의해 규율하도록 하는 입법형식)와 일반법의 체계(공공부문과 민간부문에 관한 일반적 사항을 모두 규정하도록 하고, 특수한 분야에 대해서는 별도의 특별법에 의해 규율하도록 하는 입법형식)를 고려할 수 있습니다. 이 가운데 어느 입법체계가 바람직하다고 생각하십니까?

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

- ① 기본법의 체계
- ② 일반법의 체계
- ③ 어느 것이든 무방하다
- ④ 모르겠다

[3-1] 기본법의 체계로 갈 경우 기본법에서 규율해야 할 것으로 생각하시는 항목에 모두 체크해주시기 바랍니다.

- ① 개인정보보호의 기본이념
- ② 기본개념의 정의
- ③ 개인정보취급상의 기본원칙
- ④ 개인정보보호를 위한 국가의 책무와 시책
- ⑤ 권리행사의 방법과 절차
- ⑥ 개인정보보호기구
- ⑦ 피해의 구제와 제재
- ⑧ 기타

[4] 현행과 같이 공공부문과 민간부문 간에 분리된 입법의 방식을 취한다고 하더라도 민간부문에 대한 일반법을 별도로 제정할 필요가 있다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

- ① 찬성한다
- ② 반대한다
- ③ 모르겠다

제 2 절 설문조사의 결과

1. 일반인 대상 조사

(1) 법제현황에 대한 인식

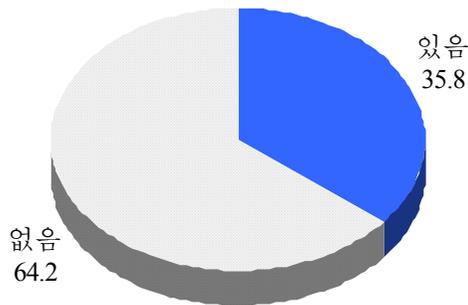
문) 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

문) 그 동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

1) 개인정보보호 법조항 검색 관련

[그림 3-2-1] 개인정보보호 관련 법조항 검색 여부

(Base: 1,000명, 단위: %)



제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가



전체 응답자의 35.8%는 개인정보보호 관련 법조항을 찾아본 경험이 있는 것으로 나타남



개인정보보호 관련 법조항을 검색한 경우는 상대적으로 남성(43.0%), 연령별로는 20대(43.8%)에서 높게 나타남

[표 3-2-1] 개인정보보호 관련 법조항 검색 여부

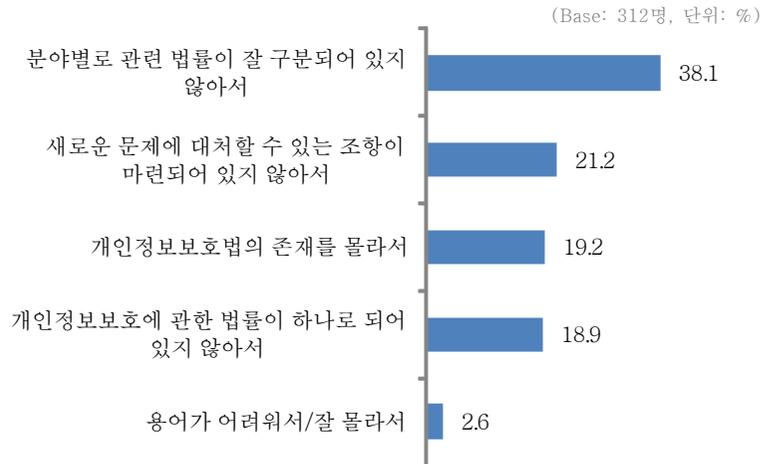
(단위:%)

		사례수(명)	경험 있음	경험 없음	계
■ 전체		(1000)	35.8	642	100.0
성별	남성	(509)	43.0	570	100.0
	여성	(491)	28.3	717	100.0
연령	20대	(242)	43.8	562	100.0
	30대	(285)	35.1	649	100.0
	40대	(281)	31.7	683	100.0
	50대	(192)	32.8	672	100.0
직업	화이트	(434)	42.9	57.1	100.0
	블루	(189)	33.9	66.1	100.0
	주부	(200)	24.0	76.0	100.0
	학생	(120)	31.7	68.3	100.0
소득 수준	상	(187)	35.8	64.2	100.0
	중	(640)	35.8	64.2	100.0
	하	(173)	35.8	64.2	100.0
지역	서울	(221)	33.0	67.0	100.0
	경기	(285)	35.8	64.2	100.0
	강원	(29)	37.9	62.1	100.0
	충청	(98)	39.8	60.2	100.0
	전라	(99)	44.4	55.6	100.0
	경상	(268)	33.2	66.8	100.0
학력	고졸이하	(252)	36.5	63.5	100.0
	대졸	(634)	34.9	65.1	100.0
	대학원졸 이상	(114)	39.5	60.5	100.0

[그림 3-2-2] 개인정보보호 법조항 검색시 어려움 있었는지 여부



[그림 3-2-3] 검색시 어려움을 느낀 이유



제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

[표 3-2-2] 개인정보보호 법조항 검색시 어려움 있었는지 여부

(단위:%)

		사례수(명)	어려움 있었다	어려움이 별로 없었다	계
■ 전체		(358)	87.2	128	100.0
성별	남성	(219)	85.4	146	100.0
	여성	(139)	89.9	10.1	100.0
연령	20대	(106)	89.6	104	100.0
	30대	(100)	87.0	130	100.0
	40대	(89)	87.6	124	100.0
	50대	(63)	82.5	175	100.0
직업	화이트	(186)	88.2	118	100.0
	블루	(64)	81.3	188	100.0
	주부	(48)	89.6	104	100.0
	학생	(38)	86.8	132	100.0
소득 수준	상	(67)	89.6	104	100.0
	중	(229)	86.5	135	100.0
	하	(62)	87.1	129	100.0
지역	서울	(73)	80.8	192	100.0
	경기	(102)	88.2	118	100.0
	강원	(11)	72.7	273	100.0
	충청	(39)	87.2	128	100.0
	전라	(44)	81.8	182	100.0
	경상	(89)	95.5	4.5	100.0
학력	고졸이하	(92)	89.1	109	100.0
	대졸	(221)	88.7	113	100.0
	대학원졸 이상	(45)	75.6	244	100.0

[표 3-2-3] 검색시 어려움을 느낀 이유

(단위:%)

		사례수 (명)	분야별로 관련 법 률이 잘 구분되어 있지 않 아서	새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않 아서	개인정보 보호법의 존재를 몰라서	개인정보 보호에 관한 법 률이 하 나로 되 어 있지 않아서	용어가 어려워 서/잘 몰 라서	계
■ 전체		(312)	38.1	21.2	19.2	18.9	2.6	100.0
성별	남성	(187)	39.0	20.3	18.2	19.8	2.7	100.0
	여성	(125)	36.8	22.4	20.8	17.6	2.4	100.0
연령	20대	(95)	43.2	18.9	21.1	13.7	3.2	100.0
	30대	(87)	35.6	16.1	23.0	20.7	4.6	100.0
	40대	(78)	38.5	23.1	15.4	21.8	1.3	100.0
	50대	(52)	32.7	30.8	15.4	21.2		100.0
직업	화이트	(164)	39.6	20.7	16.5	20.7	2.4	100.0
	블루	(52)	34.6	34.6	15.4	15.4		100.0
	주부	(43)	27.9	14.0	34.9	20.9	2.3	100.0
	학생	(33)	48.5	18.2	18.2	12.1	3.0	100.0
소득 수준	상	(60)	35.0	20.0	20.0	21.7	3.3	100.0
	중	(198)	41.4	21.2	16.7	18.7	2.0	100.0
	하	(54)	29.6	22.2	27.8	16.7	3.7	100.0
지역	서울	(59)	35.6	23.7	25.4	11.9	3.4	100.0
	경기	(90)	35.6	18.9	17.8	24.4	3.3	100.0
	강원	(8)	12.5	50.0	12.5		25.0	100.0
	충청	(34)	41.2	14.7	20.6	23.5		100.0
	전라	(36)	36.1	33.3	11.1	19.4		100.0
	경상	(85)	44.7	16.5	20.0	17.6	1.2	100.0
학력	고졸이하	(82)	34.1	23.2	23.2	17.1	2.4	100.0
	대졸	(196)	38.8	19.9	18.9	19.4	3.1	100.0
	대학원졸 이상	(34)	44.1	23.5	11.8	20.6		100.0

*강원 지역은 사례수가 적어 해석 시 주의 요함



개인정보보호 관련 법조항을 검색 시 어려움이 있었다고 응답한 경우는 87.2% 수준으로 높은 편이며, 어려움을 느낀 이유로 ‘분야별로 관련 법률이 잘 구분되지 않아서(38.1%)’가 가장 많이 언급됨



문) 우리나라의 개인정보보호 관련 입법은 공공부문과 민간부문으로 나누어 각각 별도의 법률로 적용되는 형태로 되어 있습니다. 이러한 점에 대하여 알고 계십니까?

남성보다 여성이, 학력에서는 학력이 낮을수록 어려움을 느낀 것으로 보임. 어려움을 느낀 이유로 ‘분야별로 관련 법률 구분이 잘 안 되어서’는 20대와 대학원졸 이상에서, 새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않아서’는 50대, ‘개인정보보호법의 존재를 몰라서’는 주부층에서 상대적으로 보다 언급한 특성을 보임

2) 개인정보보호법제 개념 이해 및 인지 수준

문) 다음 법률 가운데 개인정보의 보호를 위한 내용이 포함되어 있을 것으로 짐작되는 법률을 모두 선택하여 주십시오.



‘신용정보의 이용 및 보호에 관한 법률’> ‘정보통신망 이용 촉진 및 정보보호 등에 관한 법률’> ‘금융실명거래 및 비밀보장에 관한 법률’

순으로 개인정보보호 관련 내용이 포함되어 있을 것 같다고 응답함

[그림 3-2-4] 개인정보보호 관련 내용이 포함되어 있을 것 같은 법률

(Base: 1,000명, 단위: %)



별도의 법률이 적용되는 것을 잘 알고 있다고 응답한 경우는 9.1% 수준이며, 70.5%는 몰랐다고 응답하고 있음

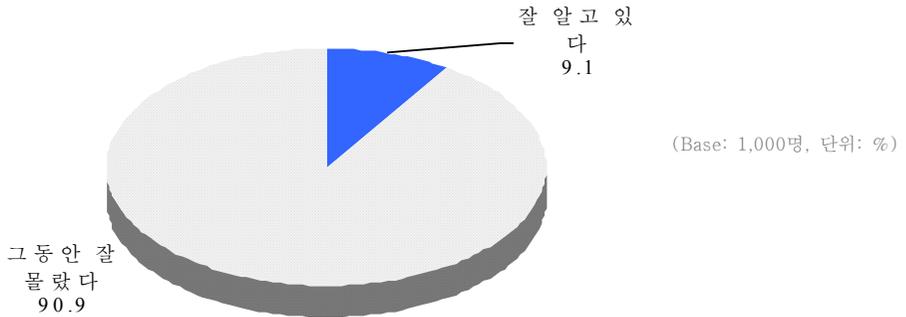


남성, 50대, 대학원졸 이상이 상대적으로 높게 응답된 특성을 보임



제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

[그림 3-2-5] 개인정보보호법 공공부문과 민간부문 별도 적용의 인지 여부



[표 3-2-4] 개인정보보호법 공공부문과 민간부문 별도 적용의 인지 여부

		사례수(명)	잘 알고 있다	그 동안 잘 몰랐다	계
■ 전체		(1000)	9.1	90.9	100.0
성별	남성	(509)	10.6	89.4	100.0
	여성	(491)	7.5	92.5	100.0
연령	20대	(242)	8.7	91.3	100.0
	30대	(285)	6.0	94.0	100.0
	40대	(281)	9.6	90.4	100.0
	50대	(192)	13.5	86.5	100.0
직업	화이트	(434)	9.9	90.1	100.0
	블루	(189)	10.6	89.4	100.0
	주부	(200)	7.0	93.0	100.0
	학생	(120)	5.0	95.0	100.0
소득 수준	상	(187)	9.1	90.9	100.0
	중	(640)	9.1	90.9	100.0
	하	(173)	9.2	90.8	100.0
지역	서울	(221)	10.9	89.1	100.0
	경기	(285)	8.1	91.9	100.0
	강원	(29)	6.9	93.1	100.0
	충청	(98)	12.2	87.8	100.0
	전라	(99)	9.1	90.9	100.0
	경상	(268)	7.8	92.2	100.0
학력	고졸이하	(252)	7.9	92.1	100.0
	대졸	(634)	8.5	91.5	100.0
	대학원졸 이상	(114)	14.9	85.1	100.0

문) 공공부문의 개인정보에 적용되는 ‘공공기관의 개인정보보호에 관한 법률’은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

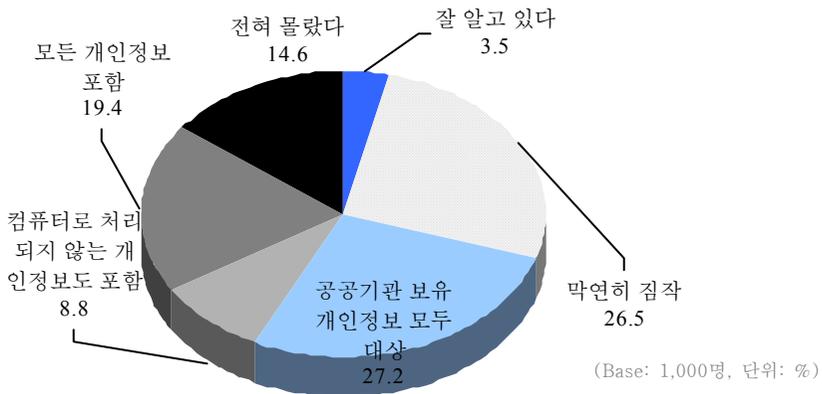


컴퓨터로 처리된 것만 보호대상인 사실을 ‘잘 알고 있다’고 응답한 경우는 전혀 응답자 가운데 3.5% 수준이며, ‘막연히 짐작’이 26.5% 수준임



여성보다 남성이 ‘잘 알고 있다’고 응답하였으며, 연령별로는 40대의 인지도가 다소 높은 것으로 나타남

[그림 5-2-6] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호대상인 점의 인지 여부



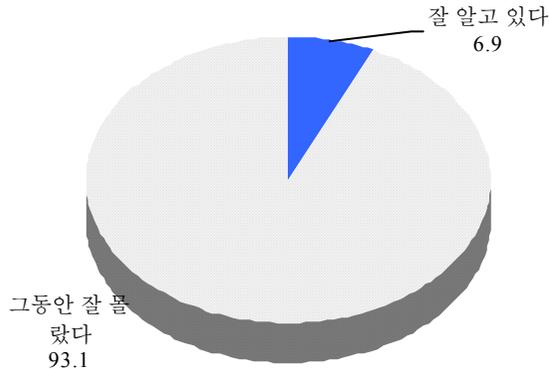
제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

[표 3-2-5] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호 대상으로 하고 있다는 사실의 인지 여부

(단위:%)

		사례수 (명)	잘 알고 있다	막연히 짐작	공공기관 보유 개 인정보는 모두 대 상	컴퓨터로 처리되지 않는 개 인정보도 포함	모든 개 인정보 포함	전혀 몰 랐다	계
■ 전체		(1000)	3.5	26.5	27.2	8.8	19.4	14.6	1000
성별	남성	(509)	4.1	29.1	25.5	9.4	17.3	14.5	1000
	여성	(491)	2.9	23.8	28.9	8.1	21.6	14.7	1000
연령	20대	(242)	4.1	19.4	23.1	13.6	22.3	17.4	1000
	30대	(285)	0.7	26.7	27.0	8.4	20.4	16.8	1000
	40대	(281)	5.7	28.8	28.1	6.0	18.1	13.2	1000
	50대	(192)	3.6	31.8	31.3	7.3	16.1	9.9	1000
직업	화이트	(434)	3.2	27.2	30.9	10.4	15.4	12.9	1000
	블루	(189)	4.2	31.7	27.0	5.3	19.0	12.7	1000
	주부	(200)	3.0	25.0	26.5	6.5	22.0	17.0	1000
	학생	(120)	4.2	20.0	15.0	13.3	30.0	17.5	1000
소득 수준	상	(187)	2.7	27.8	26.7	7.0	21.9	13.9	1000
	중	(640)	3.6	26.9	28.1	9.5	18.1	13.8	1000
	하	(173)	4.0	23.7	24.3	8.1	21.4	18.5	1000
지역	서울	(221)	2.7	26.7	26.7	7.2	21.3	15.4	1000
	경기	(285)	4.9	24.9	26.7	10.2	18.9	14.4	1000
	강원	(29)	6.9	20.7	10.3	3.4	20.7	37.9	1000
	충청	(98)	7.1	29.6	24.5	12.2	15.3	11.2	1000
	전라	(99)	2.0	32.3	29.3	7.1	15.2	14.1	1000
	경상	(268)	1.5	25.4	30.2	8.6	21.3	13.1	1000
학력	고졸이하	(252)	5.2	23.0	28.6	9.9	18.3	15.1	1000
	대졸	(634)	3.0	28.2	24.6	8.7	20.5	15.0	1000
	대학원졸 이상	(114)	2.6	24.6	38.6	7.0	15.8	11.4	1000

[그림 3-2-7] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부



p(Base: 1,000명, 단위: %)

문) 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며, 개별분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?



민간부문의 경우 개별분야별로 법률이 적용된다는 사실을 아는 경우는 전체의 6.9% 수준이며, 93.1%가 모른다고 응답하여 대부분은 잘 알지 못하는 것으로 보임



성별로는 여성이, 연령별로는 20대가 타 집단대비 보다 인지하고 있는 것으로 조사됨

[표 3-2-6] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부

(단위:%)

		사례수(명)	잘 알고 있다	그동안 잘 몰랐다	계
■ 전체		(1000)	69	93.1	100.0
성별	남성	(509)	83	917	100.0
	여성	(491)	55	945	100.0
연령	20대	(242)	9.1	909	100.0
	30대	(285)	35	965	100.0
	40대	(281)	75	925	100.0
	50대	(192)	83	917	100.0
직업	화이트	(434)	7.1	929	100.0
	블루	(189)	7.4	926	100.0
	주부	(200)	5.0	95.0	100.0
	학생	(120)	5.0	95.0	100.0
소득 수준	상	(187)	9.1	909	100.0
	중	(640)	56	944	100.0
	하	(173)	92	908	100.0
지역	서울	(221)	68	932	100.0
	경기	(285)	46	954	100.0
	강원	(29)	10.3	897	100.0
	충청	(98)	15.3	847	100.0
	전라	(99)	8.1	919	100.0
	경상	(268)	56	944	100.0
학력	고졸이하	(252)	60	940	100.0
	대졸	(634)	7.1	929	100.0
	대학원졸 이상	(114)	79	92.1	100.0

3) 개인정보보호의 현황에 대한 인식

문) 현재 본인의 개인정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보호되고 있다고 느끼십니까?



본인의 개인 정보가 제대로 보호되고 있다고 생각하는 경우는 5.2%(매우 그렇다+그렇다) 수준에 그쳤으며, 그렇지 않다고 생각하는 경우가 72.3%(그렇지 않다 +전혀 그렇지 않다)로 나타남



남성보다 여성이, 연령은 30대, 소득수준 상인 경우 보다 신뢰하지 못하는 것 또한 보임

[그림 3-2-8] 개인정보가 제대로 보호되고 있는지에 대한 동의



제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

[표 3-2-7] 개인정보가 제대로 보호되고 있는지에 대한 동의

(단위:%)

		사례수 (명)	매우 그렇다	그렇다	Top2	보통이 다	그렇지 않다	전혀 그렇지 않다	Bo tto m 2	M ean (점)
▣ 전체		(1000)	0.5	4.7	5.2	22.5	52.0	20.3	72.3	(2.13)
성별	남성	(509)	0.6	5.3	5.9	23.6	49.3	21.2	70.5	(2.15)
	여성	(491)	0.4	4.1	4.5	21.4	54.8	19.3	74.1	(2.11)
연령	20대	(242)	1.2	6.2	7.4	28.5	42.1	21.9	64.0	(2.23)
	30대	(285)		2.5	2.5	17.9	60.4	19.3	79.6	(2.04)
	40대	(281)		5.0	5.0	19.9	54.1	21.0	75.1	(2.09)
	50대	(192)	1.0	5.7	6.8	25.5	49.0	18.8	67.7	(2.21)
직업	화이트	(434)	0.5	3.7	4.1	23.3	51.6	21.0	72.6	(2.11)
	블루	(189)		4.2	4.2	22.2	52.9	20.6	73.5	(2.1)
	주부	(200)	0.5	4.5	5.0	20.0	56.5	18.5	75.0	(2.12)
	학생	(120)	0.8	8.3	9.2	27.5	44.2	19.2	63.3	(2.28)
소득 수준	상	(187)		5.3	5.3	20.9	50.3	23.5	73.8	(2.08)
	중	(640)	0.5	4.7	5.2	23.1	53.0	18.8	71.7	(2.15)
	하	(173)	1.2	4.0	5.2	22.0	50.3	22.5	72.8	(2.11)
지역	서울	(221)	0.5	3.6	4.1	21.7	50.2	24.0	74.2	(2.06)
	경기	(285)	0.4	3.5	3.9	18.2	57.9	20.0	77.9	(2.06)
	강원	(29)	3.4	3.4	6.9	27.6	37.9	27.6	65.5	(2.17)
	충청	(98)		6.1	6.1	22.4	48.0	23.5	71.4	(2.11)
	전라	(99)	1.0	7.1	8.1	31.3	41.4	19.2	60.6	(2.29)
	경상	(268)	0.4	5.6	6.0	23.9	54.1	16.0	70.1	(2.2)
학력	고졸이하	(252)	1.2	4.0	5.2	20.2	52.4	22.2	74.6	(2.1)
	대졸	(634)	0.3	5.2	5.5	23.5	52.4	18.6	71.0	(2.16)
	대학원졸 이상	(114)		3.5	3.5	21.9	49.1	25.4	74.6	(2.04)

문) 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이라고 생각하십니까 1순위부터 3순위까지 응답하여 주십시오.



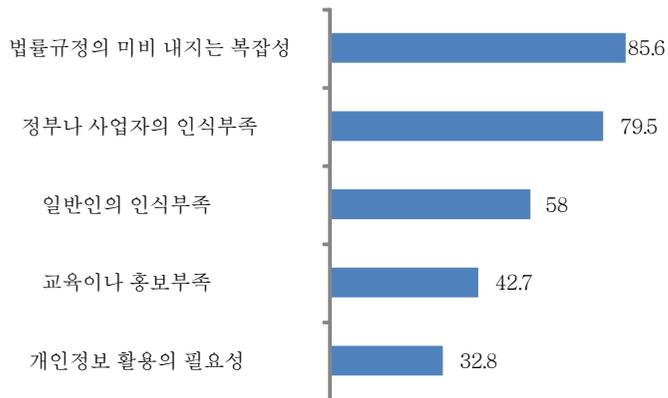
개인정보가 제대로 보호되고 있지 않다고 생각하는 이유로 ‘법률규정의 미비 내지는 복잡성’(85.6%), ‘정부나 사업자의 인식 부족’(79.5%) 순으로 지적됨



‘법률규정의 미비 내지는 복잡성’은 30대에서, ‘정부나 사업자의 인식 부족’은 학생 및 대학원 졸업 이상자가 상대적으로 높게 응답함
‘일반인의 인식 부족’은 20대에서 보다 언급된 특징을 보임

[그림 3-2-9] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유

(Base: 그렇지 않다+ 전혀 그렇지 않다 723명, 단위:%, 복수응답)



[표 3-2-8] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유

(단위: %, 복수응답)

		사례수 (명)	법을규정 의 미비 내지는 복잡성	정 부나 사 업 자의 인식 부족	일반인의 인식부족	교육이나 홍보 부족	개인정보 활용의 필요성
■ 전체		(723)	85.6	79.5	58.0	42.7	32.8
성별	남성	(359)	86.4	83.0	57.7	43.5	28.7
	여성	(364)	84.9	76.1	58.2	42.0	36.8
연령	20대	(155)	81.9	83.2	64.5	36.1	32.9
	30대	(227)	89.0	80.6	54.6	41.0	33.0
	40대	(211)	84.8	80.6	58.8	43.1	32.2
	50대	(130)	85.4	71.5	54.6	53.1	33.1
직업	화이트	(315)	87.9	83.2	56.8	41.6	28.9
	블루	(139)	86.3	77.0	55.4	43.2	36.0
	주부	(150)	83.3	70.0	59.3	46.7	40.0
	학생	(76)	80.3	88.2	65.8	35.5	28.9
소득 수준	상	(138)	85.5	80.4	56.5	41.3	33.3
	중	(459)	85.8	79.3	57.1	45.3	31.4
	하	(126)	84.9	79.4	62.7	34.9	37.3
지역	서울	(164)	81.7	81.7	61.6	37.8	35.4
	경기	(222)	87.4	79.3	64.0	39.6	27.9
	강원	(19)	78.9	78.9	47.4	68.4	26.3
	충청	(70)	81.4	80.0	51.4	50.0	35.7
	전라	(60)	85.0	80.0	58.3	38.3	38.3
	경상	(188)	89.4	77.7	51.1	46.8	34.0
학력	고졸이하	(188)	87.2	78.7	57.4	42.0	31.9
	대졸	(450)	86.2	79.1	58.4	42.7	32.7
	대학원졸 이상	(85)	78.8	83.5	56.5	44.7	35.3

문) 현재는 개인정보가 부분적으로 보호되고 있습니다. 개인정보의 보호를 보다 강화하기 위한 『개인정보보호법』의 제정이 필요하다고 생각하십니까?



현재보다 강화된 ‘개인정보보호법’의 제정이 필요하다는 데에는 대부분 동의하는 것으로 나타남(92.8% 시급히, 매우 필요하다+시급하지는 않지만 필요하다)



연령별 특징을 미비하며, 소득수준이 상인 경우 보다 높게 동의한 특징을 보인다

[그림 3-2-10] 강화된 ‘개인정보보호법’ 제정 필요도



[표 3-2-9] 강화된 ‘개인정보보호법’ 제정 필요도

(단위: %)

		사례수 (명)	시급하 매우 필요하 다	시급하 지는 않지만 필요하 다	TOP 2	보통이 다	필요하 지 않 다	전혀 필요하 지 않 다	BO TTO M 2	Mean (점)
■ 전체		(1000)	70.3	22.5	92.8	4.8	2.2	0.2	2.4	(4.61)
성별	남성	(509)	69.5	23.6	93.1	4.5	2.0	0.4	2.4	(4.6)
	여성	(491)	71.1	21.4	92.5	5.1	2.4		2.4	(4.61)
연령	20대	(242)	62.8	28.5	91.3	4.5	3.7	0.4	4.1	(4.5)
	30대	(285)	71.6	21.8	93.3	4.9	1.8		1.8	(4.63)
	40대	(281)	77.2	16.0	93.2	5.0	1.8		1.8	(4.69)
	50대	(192)	67.7	25.5	93.2	4.7	1.6	0.5	2.1	(4.58)
직업	화이트	(434)	73.3	20.0	93.3	4.4	1.8	0.5	2.3	(4.64)
	블루	(189)	70.9	21.2	92.1	5.8	2.1		2.1	(4.61)
	주부	(200)	68.5	24.0	92.5	5.0	2.5		2.5	(4.59)
	학생	(120)	61.7	32.5	94.2	2.5	3.3		3.3	(4.53)
소득 수준	상	(187)	71.1	24.1	95.2	3.2	1.6		1.6	(4.65)
	중	(640)	70.9	22.3	93.3	4.5	2.0	0.2	2.2	(4.62)
	하	(173)	67.1	21.4	88.4	7.5	3.5	0.6	4.0	(4.51)
지역	서울	(221)	75.1	18.6	93.7	4.5	1.4	0.5	1.8	(4.67)
	경기	(285)	68.4	24.6	93.0	4.2	2.8		2.8	(4.59)
	강원	(29)	72.4	17.2	89.7	3.4	6.9		6.9	(4.55)
	충청	(98)	72.4	17.3	89.8	5.1	4.1	1.0	5.1	(4.56)
	전라	(99)	63.6	30.3	93.9	4.0	2.0		2.0	(4.56)
	경상	(268)	69.8	23.1	92.9	6.0	1.1		1.1	(4.62)
학력	고졸이하	(252)	71.0	22.2	93.3	4.4	2.4		2.4	(4.62)
	대졸	(634)	70.7	22.6	93.2	4.3	2.2	0.3	2.5	(4.61)
	대학원졸 이상	(114)	66.7	22.8	89.5	8.8	1.8		1.8	(4.54)

2. 전문가 대상 조사

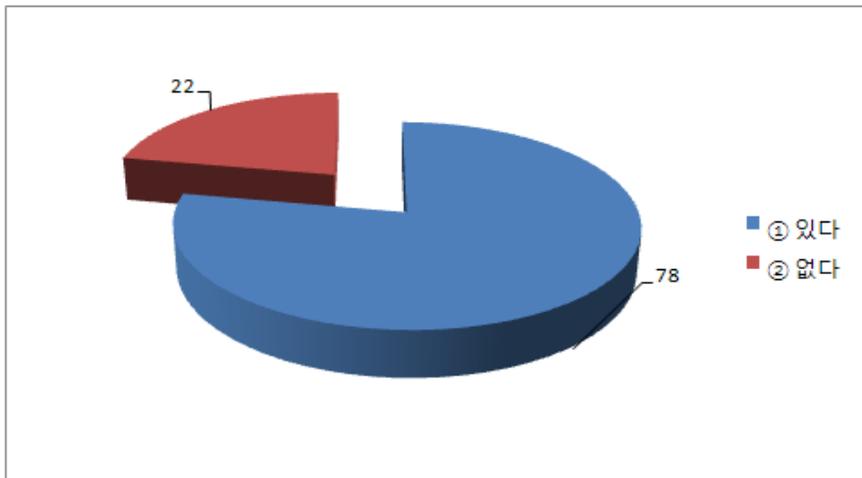
(1) 법제의 현황에 대한 인식

1) 개인정보보호 법조항 검색 관련

문) 그 동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

[그림 3-2-11] 개인정보보호 관련 법조항 검색 여부

(Base : 41명, 단위 %)



- 전 체

전체 응답자의 78%는 개인정보보호 관련 법조항을 찾아본 경험이 있는 것으로 나타남

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

- 응답자 특성별

상대적으로는 남성(80.56%), 근무직장으로는 법학교수(93.75%)가 높게 나타남

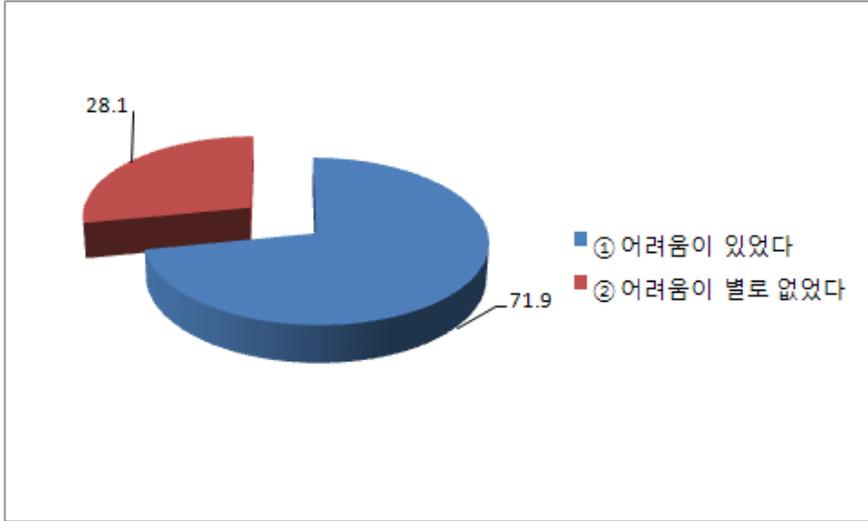
[표 3-2-10] 개인정보보호 관련 법조항 검색 여부

(단위:%)

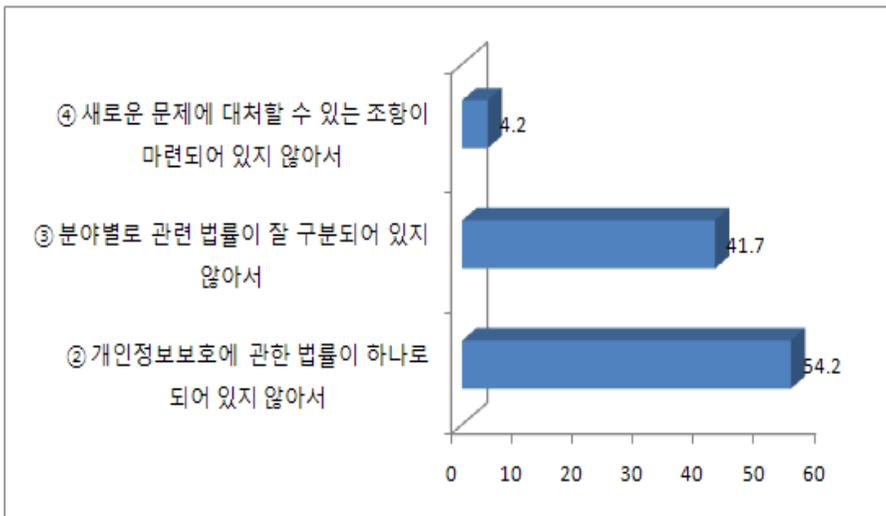
		사례수(명)	경험 있음	경험 없음	계
전체		41	78.00	22.00	100.00
성별	남	36	80.56	19.44	100.00
	여	5	60.00	40.00	100.00
근무 기간	1년미만	8	50.00	50.00	100.00
	1~5년미만	20	80.00	20.00	100.00
	5~10년미만	7	100.00	0.00	100.00
	10년이상	6	83.33	16.67	100.00
근무 직장	기업	13	76.92	23.08	100.00
	법학교수	16	93.75	6.25	100.00
	법실무	12	58.33	41.67	100.00

문) 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

[그림 3-2-12] 개인정보보호 법조항 검색시 어려움 있었는지 여부
(Base : 32명, 단위 %)



[그림 3-2-13] 검색시 어려움을 느낀 이유 (Base : 24명, 단위 %)



[표 3-2-11] 개인정보보호 법조항 검색시 어려움 있었는지 여부

(단위:%)

		사례수(명)	어려움이 있었다	어려움이 별로 없었다	계
전체		32	71.88	28.13	100.00
성별	남	29	80.56	19.44	100.00
	여	3	60.00	40.00	100.00
근무기간	1년미만	4	100.00	0.00	100.00
	1~5년미만	16	68.75	31.25	100.00
	5~10년미만	7	71.43	28.57	100.00
	10년이상	5	60.00	40.00	100.00
근무직장	기업	10	60.00	40.00	100.00
	법학교수	15	66.67	33.33	100.00
	법실무	7	100.00	0.00	100.00

- 전체

개인정보보호 관련 법조항의 검색 시 어려움이 있었다고 응답한 경우는 71.88% 수준으로 높은 편이며, 어려움을 느낀 이유로, ‘개인정보 보호에 관한 법률이 하나로 되어 있지 않아서(54.17%)’가 가장 많이 언급됨

- 응답자별 특성

여성보다 남성이 직장에서는 법실무자가 더 어려움을 느낌. 어려움을 느낀 이유 중 ‘분야별로 관련 법률이 잘 구분되어 있지 않아서’는 여자와 10년이상 근무한 사람들에서, ‘개인정보보호에 관한 법률이 하나로 되어 있지 않아서’는 근무기간이 5~10년사이의 사람들과 법실무

자들에서 상대적으로 많이 언급함

[표 3-2-12] 검색시 어려움을 느낀 이유

(단위:%)

		사례수 (명)	① 개인정보 보호법 의 존재를 몰라서	② 개인정보 보호에 관한 법률이 하나로 되어 있지 않아서	③ 분야별로 관련 법률이 잘 구분되어 있지 않아서	④ 새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않아서	⑤ 기타	계
전체		24		54.17	41.67	4.17		100.00
성별	남	22		59.09	36.36	4.55		100.00
	여	2		0.00	100.00	0.00		100.00
근무 기간	1년미만	4		50.00	50.00	0.00		100.00
	1~5년미만	12		58.33	33.33	8.33		100.00
	5~10년미만	5		60.00	40.00	0.00		100.00
	10년이상	3		33.33	66.67	0.00		100.00
근무 직장	기업	6		33.33	66.67	0.00		100.00
	법학교수	10		50.00	40.00	10.00		100.00
	법실무	8		75.00	25.00	0.00		100.00

2) 개인정보법제 개념 이해 및 인지 수준

문) 다음 법률 가운데 개인정보의 보호를 위한 내용이 포함 되어 있을 것으로 짐작 되는 법률을 모두 선택하여 주십시오.

- 전 체

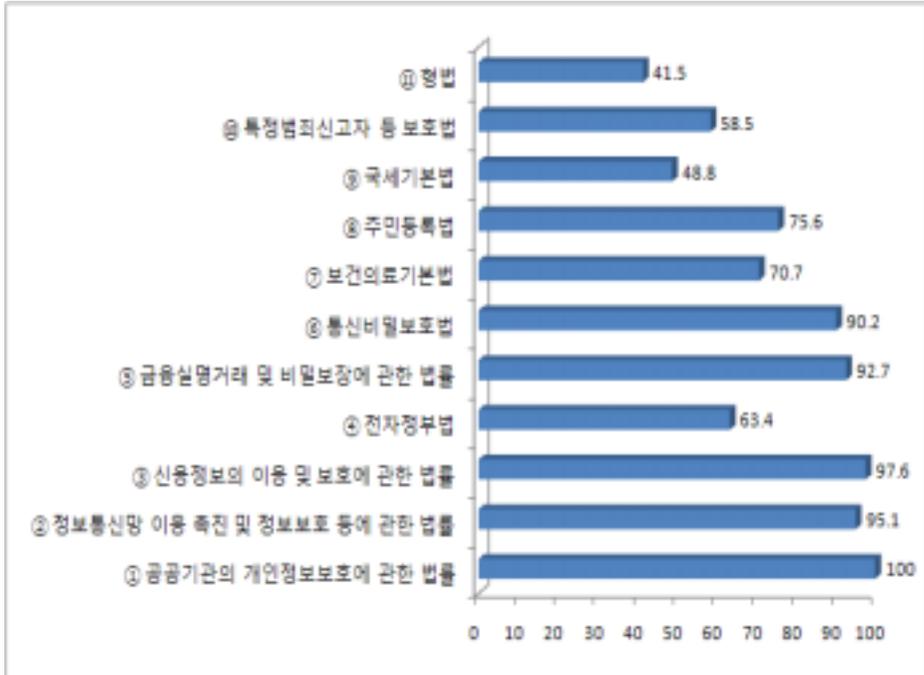
「공공기관의 개인정보보호에 관한 법률」> 「신용정보의 이용 및 보호에 관한 법률」> 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」>

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

『금융실명거래 및 비밀보장에 관한 법률』의 순으로 개인정보보호 관련 내용이 포함되어 있을 것 같다고 응답함

[그림 3-2-14] 개인정보보호 관련 내용이 포함되어 있을 것 같은 법률

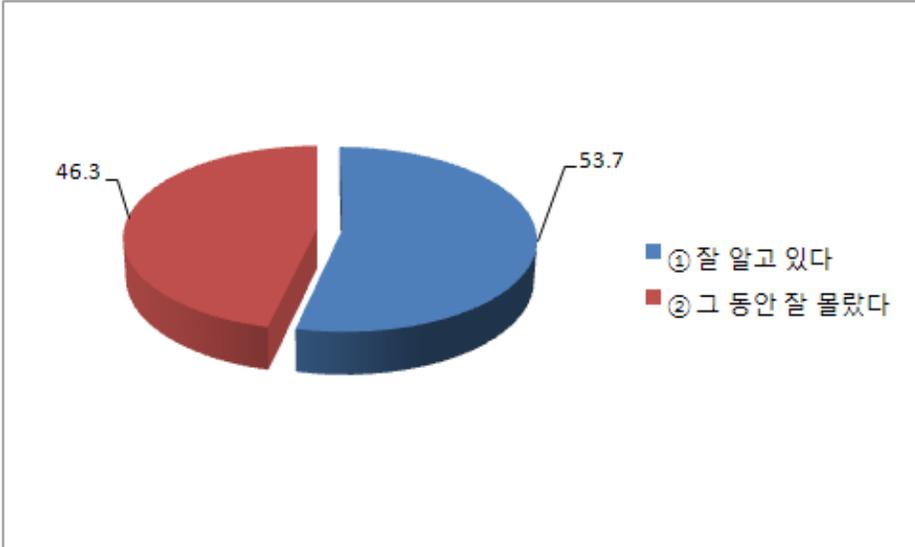
(Base : 41명, 단위 %)



문) 우리나라 현행 개인정보보호 관련 입법은 공공부문과 민간부문으로 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대하여 알고 계십니까?

[그림 3-2-15] 개인정보보호법 공공부문과 민간부문 별도 적용의 인지 여부

(Base : 41명, 단위 %)



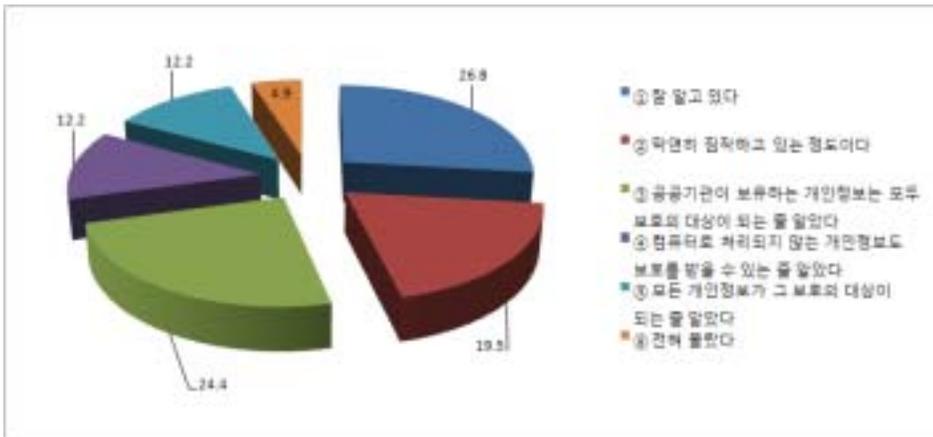
[표 3-2-13] 개인정보보호법과 공공부문과 민간부문 별도 적용의 인지 여부

(단위:%)

		사례수(명)	잘 알고있다	그동안 몰랐다	계
전체		41	53.66	46.34	100.00
성별	남	36	58.33	41.67	100.00
	여	5	60.00	40.00	100.00
근무 기간	1년미만	8	37.50	62.50	100.00
	1~5년미만	20	60.00	40.00	100.00
	5~10년미만	7	71.43	28.57	100.00
	10년이상	6	33.33	66.67	100.00
근무 직장	기업	13	38.46	61.54	100.00
	법학교수	16	75.00	25.00	100.00
	법실무	12	41.67	58.33	100.00

문) 공공부문의 개인정보에 적용되는 ‘공공기관의 개인정보보호에 관한 법률’은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

[그림 3-2-16] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호의 대상이 된다는 사실의 인지 여부



- 전 체

‘공공기관이 보호하는 개인정보는 모두 처리 대상인줄 알았다’고 응답한 경우는 전체 24.4% 수준이며, ‘전혀 몰랐다’는 4.9% 수준임

- 응답자별 특성

여성보다 남성이 잘 알고 있다고 응답하였으며, 근무기간에 따라서는 5~10년, 근무직장에 따라서는 법학교수가 가장 높게 나타남

[표 3-2-14] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호의 대상이 된다는 사실의 인지 여부

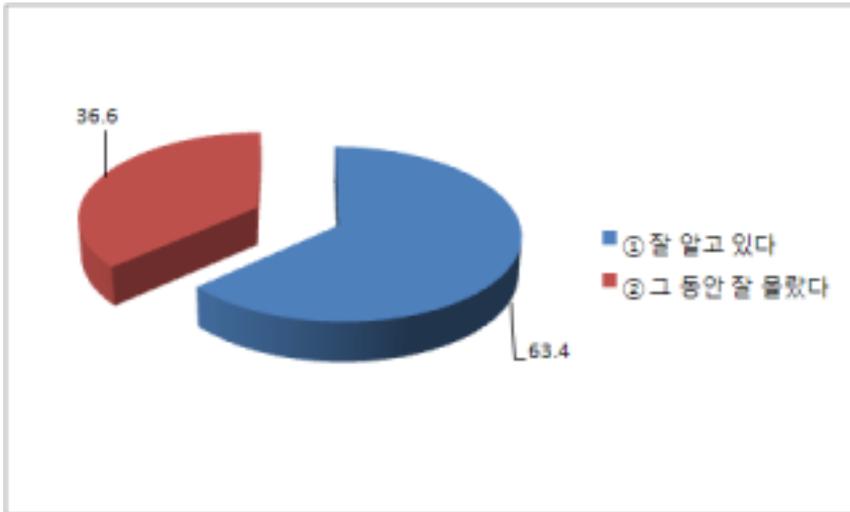
(단위:%)

		사 례 수 (명)	① 잘 알고 있다	② 막연히 짐작 하고 있는 정도 이다	③ 공 공 기 관 이 보 유 하 는 개 인 정 보 는 모 두 보 호 의 대 상 이 되 는 줄	④ 컴 퓨 터 로 처 리 되 지 않 는 개 인 정 보 도 보 호 를 받 을 수 있 는 줄	⑤ 모 든 개 인 정 보 가 그 보 호 의 대 상 이 되 는 줄 알 았 다	⑥ 전 혀 몰 랐 다	계
전체		41	26.83	19.51	24.39	12.20	12.20	4.88	100.00
성별	남	36	27.78	22.22	25.00	11.11	11.11	2.78	100.00
	여	5	20.00	0.00	20.00	20.00	20.00	20.00	100.00
근무 기간	1년미만	8	12.50	25.00	37.50	12.50	12.50	0.00	100.00
	1~5년미만	20	25.00	25.00	25.00	10.00	10.00	5.00	100.00
	5~10년미만	7	42.86	14.29	28.57	0.00	0.00	14.29	100.00
	10년이상	6	33.33	0.00	0.00	33.33	33.33	0.00	100.00
근무 직장	기업	13	23.08	15.38	23.08	15.38	23.08	0.00	100.00
	법학교수	16	43.75	18.75	18.75	6.25	6.25	6.25	100.00
	법실무	12	8.33	25.00	33.33	16.67	8.33	8.33	100.00

문) 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며, 개별분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?

[그림 3-2-17] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부

(Base : 41명, 단위 %)



[표 3-2-15] 민간부문의 경우 개별분야별 법률만 존재한다는 사실의 인지 여부

(단위:%)

		사례수(명)	잘 알고있다	그동안 몰랐다	계
전체		41	63.41	36.59	100.00
성별	남	36	66.67	33.33	100.00
	여	5	40.00	60.00	100.00
근무 기간	1년미만	8	62.50	37.50	100.00
	1~5년미만	20	55.00	45.00	100.00
	5~10년미만	7	85.71	14.29	100.00
	10년이상	6	66.67	33.33	100.00
근무 직장	기업	13	46.15	53.85	100.00
	법학교수	16	75.00	25.00	100.00
	법실무	12	66.67	33.33	100.00

- 전 체

별도의 법률이 적용되는 것을 잘 알고 있다고 응답한 경우는 63.4% 수준이며, 36.6%는 몰랐다고 응답

- 응답자별 특성

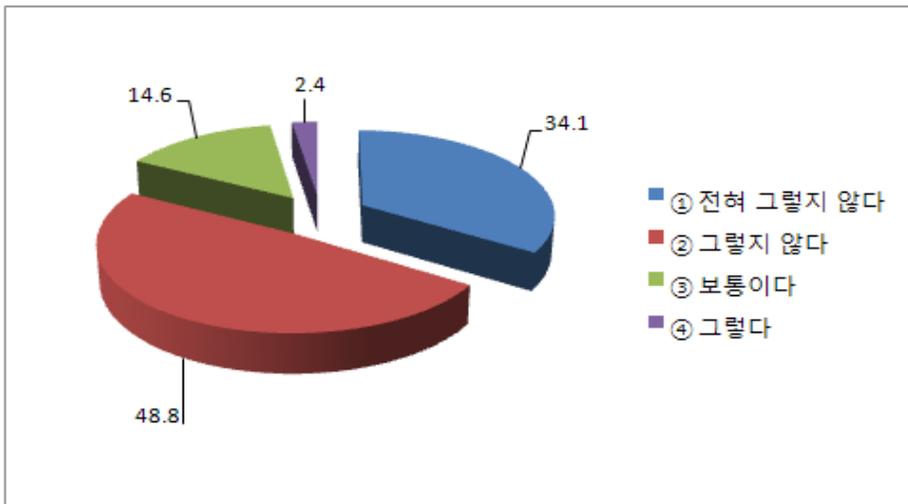
성별에 따라서 남성이 ‘잘 알고 있다’고 대답한 경우가 상대적으로 높게 나타나며, 법학교수가 다른 직장에 비해서 잘 알고 있다고 나타남

3) 개인정보보호의 현황에 대한 인식

문) 현재 본인의 개인 정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보호되고 있다고 느끼십니까?

[그림 3-2-18] 개인정보가 제대로 보호되고 있는지에 대한 동의

(Base : 41명, 단위 %) 평균(점) : 1.85



[표 3-2-16] 개인정보가 제대로 보호되고 있는지에 대한 동의

(단위:%)

		사례수 (명)	① 전혀 그렇지 않다	② 그렇지 않다	Bottom2	③ 보통이다	④ 그렇다	Top2	계
전체		41	34.15	48.78	82.93	14.63	2.44	2.44	100.00
성 별	남	36	36.11	47.22	83.33	13.89	2.78	2.78	100.00
	여	5	20.00	60.00	80.00	20.00	0.00	0.00	100.00
근 무 기 간	1년미만	8	50.00	37.50	87.50	12.50	0.00	0.00	100.00
	1~5 년미만	20	35.00	55.00	90.00	10.00	0.00	0.00	100.00
	5~10 년미만	7	42.86	42.86	85.71	14.29	0.00	0.00	100.00
	10년 이상	6	0.00	50.00	50.00	33.33	16.67	16.67	100.00
근 무 직 장	기업	13	46.15	38.46	84.62	7.69	7.69	7.69	100.00
	법학교수	16	25.00	62.50	87.50	12.50	0.00	0.00	100.00
	법실무	12	33.33	41.67	75.00	25.00	0.00	0.00	100.00

문) 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이라고 생각하십니까 1순위부터 3순위까지 응답하여 주십시오.

- 전 체

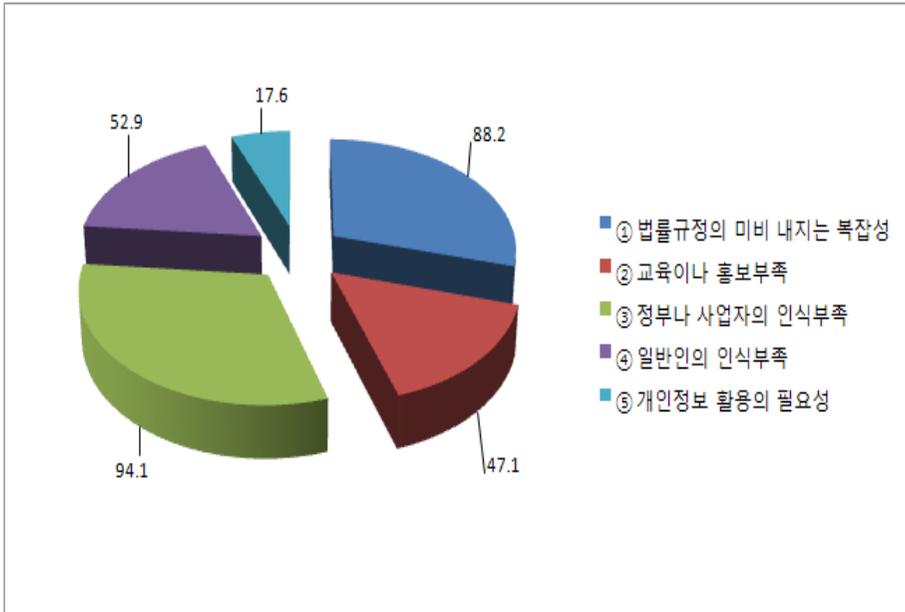
본인의 개인 정보가 제대로 보호되고 있다고 생각하는 경우는 2.4% (매우 그렇다+그렇다)수준에 그쳤으며, 그렇지 않다고 생각하는 경우가 82.9%(그렇지 않다+전혀 그렇지 않다)로 나타남

- 응답자 특성별

대부분의 응답자가 개인정보가 제대로 보호되고 있지 않다고 생각함

[그림 3-2-19] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유

(Base : 그렇지 않다+매우 그렇지 않다 34명, 단위 %, 복수응답)



- 전 체

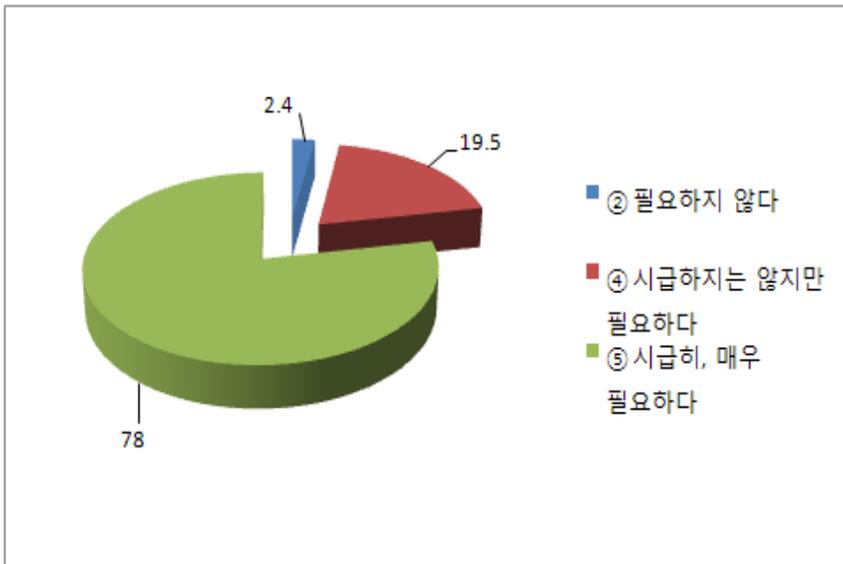
개인정보가 제대로 보호되고 있지 않다고 생각하는 이유로 ‘정부나 사업자의 인식부족’(94.1%), ‘법률규정의 미비 내지는 복잡성’(88.2%) 순으로 지적됨

- 응답자 특성

개인정보가 제대로 보호되고 있지 않다고 생각하는 이유로 ‘정부나 사업자의 인식부족’(94.1%)은 거의 대부분의 응답자 특성에서 높게 나타났으며, ‘법률규정의 미비 내지는 복잡성’(88.2%)은 10년이상 근무한 경우와 근무직장이 기업인 경우로 나타남

문) 현재는 개인정보가 부분적으로 보호되고 있습니다. 개인정보 보호를 보다 강화하기 위한 『개인정보보호법』의 제정이 필요하다고 생각하십니까?

[그림 3-2-20] 강화된 ‘개인정보보호법’ 제정 필요성



[표 3-2-17] 강화된 ‘개인정보보호법’ 제정 필요도

(단위:%)

		사례수 (명)	② 필요 하지 않다	④ 시급 하지는 않지만 필요하다	⑤ 시급히 매우 필요하다	Top2	계
전체		41	2.44	19.51	78.05	97.56	100
성별	남	36	2.78	16.67	80.56	97.22	100
	여	5	0.00	40.00	60.00	100.00	100
근무 기간	1년미만	8	0.00	37.50	62.50	100.00	100
	1~5년미만	20	0.00	10.00	90.00	100.00	100
	5~10년미만	7	0.00	42.86	57.14	100.00	100
	10년이상	6	16.67	0.00	83.33	83.33	100
근무 직장	기업	13	0.00	15.38	84.62	100.00	100
	법학교수	16	0.00	18.75	81.25	100.00	100
	법실무	12	8.33	25.00	66.67	91.67	100

- 전 체

현재보다 강화된 ‘개인정보보호법’의 제정이 필요하다는 데에는 대부분 동의하는 것으로 나타남(97.5% 시급히, 매우 필요하다+시급하지는 않지만 필요하다)

- 응답자 특성별

성별, 근무기간, 근무직장별로 필요하다고 나타남

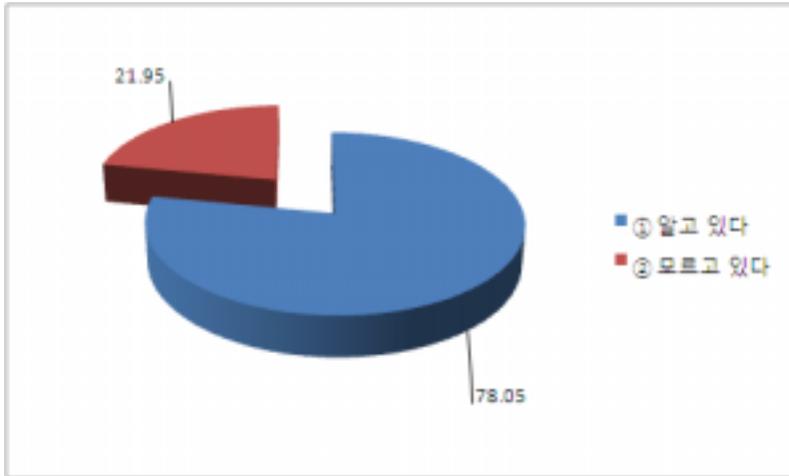
(2) 입법체계에 대한 인식

1) 입법동향의 인지

문) 개인정보보호법을 제정하려는 움직임이 있는 것에 대해 알고 계십니까?

[그림 3-2-21] 개인정보보호법 제정에 대한 인지

(Base : 41명, 단위 %)



[표 3-2-18] 개인정보보호법 제정에 대한 인지

(단위:%)

		사례수(명)	① 알고 있다	② 모르고 있다	계
전체		41	78.05	21.95	100
성별	남	36	77.78	22.22	100
	여	5	80.00	20.00	100
근무 기간	1년미만	8	50.00	50.00	100
	1~5년미만	20	85.00	15.00	100
	5~10년미만	7	100.00	0.00	100
	10년이상	6	66.67	33.33	100
근무 직장	기업	13	61.54	38.46	100
	법학교수	16	81.25	18.75	100
	법실무	12	91.67	8.33	100

- 전 체

개인정보보호법을 제정하려는 움직임이 있는 것에 대해 알고 있다고 78.05%가 응답함

- 응답자 특성별

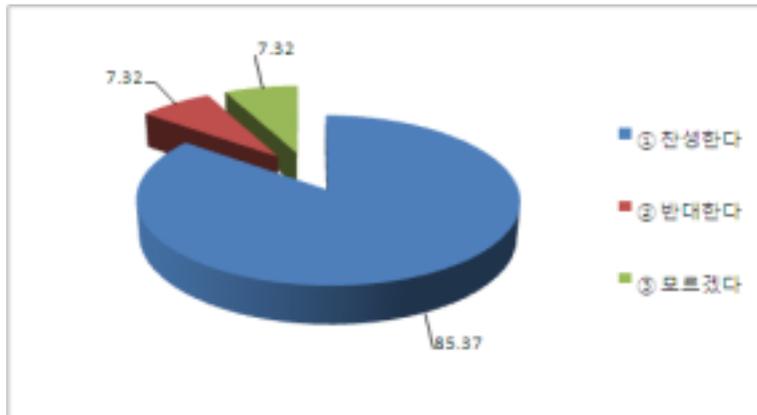
근무기간에 따라서 5~10년 미만 응답자 100%가 알고 있다고 응답하였고, 근무직장에 따라서 법실무 응답자가 91.67%수준으로 나타났으며, 근무직장이 기업인 응답자 38.46%는 모르고 있다고 응답함

2) 통합적 법률의 제정 필요성

문) 개인정보보호를 위해 공공부문과 민간부문을 별도로 규율하고 있는 현행의 방식에서 탈피해서 양 부문을 모두 포괄할 수 있는 통합적 법률의 제정이 필요하다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

[그림 3-2-22] 통합적 법률 제정에 대한 찬성/반대 의견

(Base : 41명, 단위 %)



문) 통합적 법률의 제정에 찬성하시는 이유는 다음 중 어느 것입니까? 순서대로 2가지를 선택하여 주십시오.

[표 3-2-19] 통합적 법률 제정에 대한 찬성/반대 의견

(단위:%)

		사례수(명)	① 찬성한다	② 반대한다	③ 모르겠다	계
전체		41	85.37	7.32	7.32	100.00
성별	남	36	86.11	8.33	5.56	100.00
	여	5	80.00	0.00	20.00	100.00
근무기간	1년미만	8	87.50	0.00	12.50	100.00
	1~5년미만	20	80.00	10.00	10.00	100.00
	5~10년미만	7	100.00	0.00	0.00	100.00
	10년이상	6	83.33	16.67	0.00	100.00
근무직장	기업	13	92.31	0.00	7.69	100.00
	법학교수	16	93.75	6.25	0.00	100.00
	법실무	12	66.67	16.67	16.67	100.00

- 전체

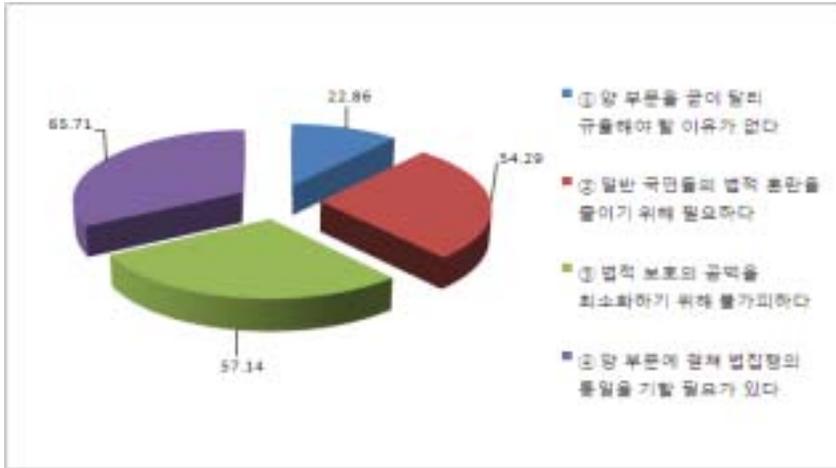
통합적 법률제정에 대한 찬성이 85.37%로 나타났으며, 반대와 모르겠다는 각각 7.32%로 나타남

- 응답자 특성별

응답자들 대부분이 찬성한다고 응답하였으며, 근무기간이 5~10년 미만인 경우 100%로 찬성한다고 나타났으며, 근무직장에 따라서 법실무 66.67%가 상대적으로 낮은 수준으로 찬성한다고 나타남

[그림 3-2-23] 통합적 법률 제정의 찬성 이유

(Base : 35명, 단위 %), 복수응답



[표 3-2-20] 통합적 법률 제정의 찬성 이유

(단위:%)

		사례수 (명)	① 양 부문을 같이 달리 규 율해야 할 이 유가 없다	② 일반 국민 들의 법적 혼란 을 줄이기 위해 필요하다	③ 법적 보호의 공백을 최소화하기 위해 불가피하다	④ 양 부문에 걸 쳐 법집행의 통 일을 기할 필요 가 있다
전체		35	22.86	54.29	57.14	65.71
성 별	남	31	22.58	51.61	61.29	64.52
	여	4	25.00	75.00	25.00	75.00
근 무 기 간	1년미만	7	0.00	42.86	71.43	85.71
	1~5년미만	16	31.25	43.75	62.50	62.50
	5~10년미만	7	42.86	71.43	42.86	42.86
	10년이상	5	0.00	80.00	40.00	80.00
근 무 직 장	기업	12	16.67	66.67	41.67	75.00
	법학교수	15	26.67	46.67	60.00	66.67
	법실무	8	25.00	50.00	75.00	50.00

- 전 체

통합적 법률의 제정에 찬성하는 이유 중 법적 보호의 공백을 최소화하기 위해 불가피하다가 57.14% 수준으로 응답하였고, 양 부문에 걸쳐 법집행의 통일을 기할 필요가 있다가 65.71%로 응답함

- 응답자 특성별

법의 혼란을 줄이기 위해 필요하다는 응답자들 중 근무기간이 5~10년 미만에서 71.43%의 수준에서 응답하였고, 근무기간이 1년 미만인 응답자들 중에서 양 부문에 걸쳐 법집행의 통일을 기할 필요가 있다고 85.71%의 수준에서 응답함

문) 통합적 법률의 제정에 반대하신다면 그 이유는 무엇입니까? 순서대로 2가지를 선택하여 주십시오.

통합적 법률의 제정에 반대하는 응답자는 전체 41명 가운데 3명이 있었다(7.3%).

1순위 문항에 대한 응답문항이 단일문항(① 양 부문을 굳이 달리 규율해야 할 이유가 없다)으로 나타났다.

반대한 3명은 모두 남성이었으며, 근무기간에 따라 1~5년 미만 2명, 10년 이상 1명, 근무직장에 따라 법학교수 1명, 법실무 1명으로 나타났다.

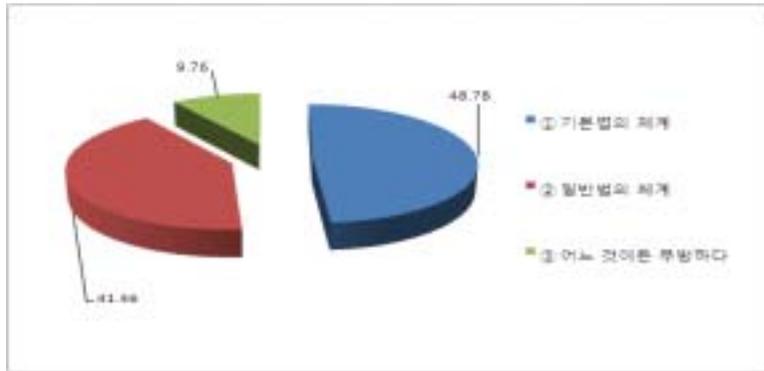
2순위 역시 3명의 응답자가 대답을 같은 항목(②법적 보호의 공백은 각 부문별 법률의 제정이나 개정을 통해서도 해소할 수 있다)에 응답하였다.

3) 통합적 법률제정시의 입법체계

문) 통합적 법률을 제정한 경우 기본법의 체계(공공부문과 민간부문에 관한 기본적인 사항만 정하고, 나머지는 특수한 분야별 개별 법률에 의해 규율하도록 하는 입법형식)와 일반법의 체계(공공부문과 민간부문에 관한 일반적인 사항을 모두 규정하도록 하고, 특수한 분야에 대해서는 별도의 특별법에 의해 규율하도록 하는 입법형식)를 고려할 수 있습니다. 이 가운데 어느 입법체계가 바람직하다고 생각합니까?

[그림 3-2-24] 통합적 법률 제정시 입법체계

(Base : 35명, 단위 %)



[표 3-2-21] 통합적 법률 제정시 입법체계

(단위:%)

		사례수 (명)	① 기본법의 체계	② 일반법의 체계	③ 어느 것이든 무방하다	계
전체		41	48.78	41.46	9.76	100.00
성 별	남	36	47.22	44.44	8.33	100.00
	여	5	60.00	20.00	20.00	100.00
근 무 기 간	1년미만	8	62.50	37.50	0.00	100.00
	1~5년미만	20	55.00	35.00	10.00	100.00
	5~10년미만	7	14.29	57.14	28.57	100.00
	10년이상	6	50.00	50.00	0.00	100.00

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

(단위:%)

		사례수 (명)	① 기본법의 체계	② 일반법의 체계	③ 어느 것이든 무방하다	계
근 무 직 장	기업	13	46.15	46.15	7.69	100.00
	법학교수	16	31.25	50.00	18.75	100.00
	법실무	12	75.00	25.00	0.00	100.00

- 전 체

통합적 별률 제정 시 입법체계에 대한 문항에 대해서 기본법의 입법체계를 따라야 한다고 48.78%가 응답하였고, 41.46%수준에서 일반법의 체계를 따라야 한다고 응답함

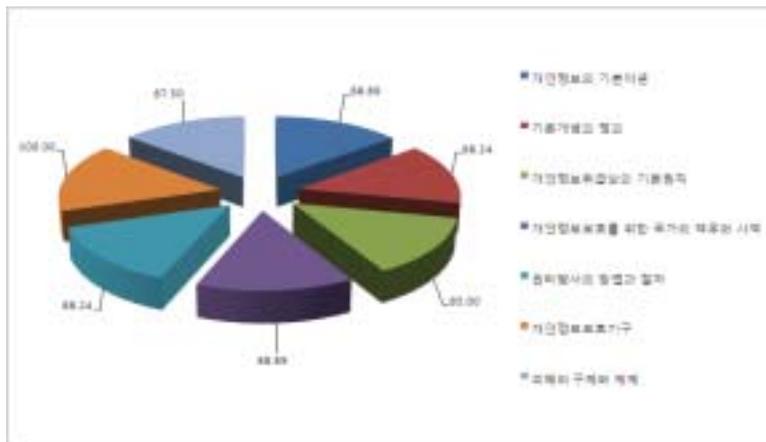
- 응답자 특성별

대체적으로 비슷하게 기본법의 체계에 많은 응답을 보였으며, 근무직장에 따라서 법실무 응답자들은 기본법의 체계를 따라야 한다고 75%가 응답함

문) 기본법의 체계로 갈 경우 기본법에서 규율해야 할 것으로 생각하시는 항목에 모두 체크해주시기 바랍니다.

[그림 3-2-25] 기본법에서 규율해야 할 경우 항목

(Base : 20명, 단위 %), 복수응답



4) 기본법이 규율할 사항

[표 3-2-22] 기본법에서 규율해야 할 경우 항목

(단위:%)

		사례수 (명)	개인정보의 기본이념	기본개념 의 정의	개인정보취 급상의 기본원칙	개인정보보호 를 위한 국가의 책무와 시책	권리행사의 방법과 절차	개인정보보 호기구	피해의 구제와 제제
성별	남	36	88.89	88.24	85.00	88.89	88.24	100.00	87.50
	여	5	11.11	11.76	15.00	11.11	11.76	0.00	12.50
근무 기간	1년미만	8	27.78	23.53	25.00	27.78	23.53	26.67	25.00
	1~5년미만	20	55.56	58.82	55.00	50.00	52.94	60.00	56.25
	5~10년미만	7	0.00	0.00	5.00	5.56	5.88	0.00	6.25
	10년이상	6	16.67	17.65	15.00	16.67	17.65	13.33	12.50
근무 직장	기업	13	27.78	23.53	30.00	22.22	29.41	20.00	31.25
	법학교수	16	22.22	29.41	25.00	27.78	23.53	33.33	25.00
	법실무	12	50.00	47.06	45.00	50.00	47.06	46.67	43.75

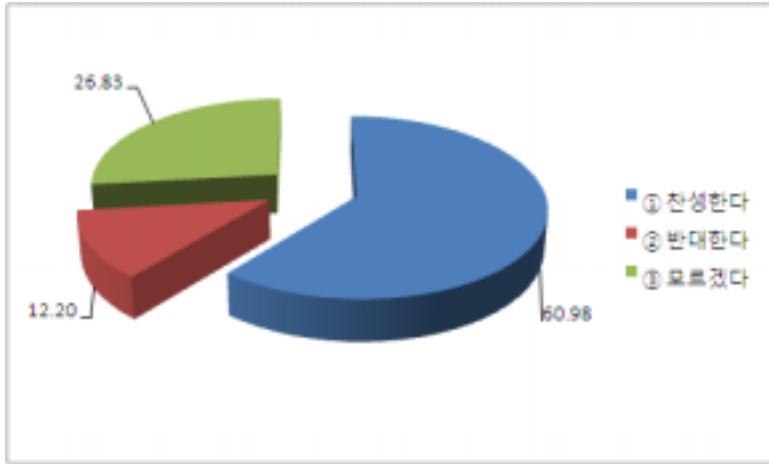
기본법의 체계로 갈 경우 기본법에서 규율해야 할 것으로 생각하는 항목은 개인정보보호기구 100%로 나타났고, 대체적으로 80%수준으로 나타났음

5) 민간부문의 일반법 제정 필요성

문) 현행과 같이 공공부문과 민간부문 간에 분리된 입법의 방식을 취한다고 하더라도 민간부문에 대한 일반법을 별도로 제정할 필요가 있다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

[그림 3-2-26] 민간부문에 대한 일반법 별도 제정 필요성

(Base : 41명, 단위 %)



민간부문에 대한 일반법도 별도로 제정해야 한다고 60.98%가 응답하였으며, 26.83%가 모른다고 응답함

제 3 절 설문조사의 분석

1. 수범자의 친숙도

첫째, 일반인을 대상으로 한 조사에서 개인정보보호 관련 법조항을 한 번도 검색해본 적이 없었다는 응답이 64.2%에 이르는데 비해, 전문가를 대상으로 한 조사에서는 22%에 그치고 있다. 이를 통해서 볼 때, 개인정보보호법제에 대해 일반 국민들이 느끼는 심리적 거리감이 상당한 것으로 판단된다. 무릇 입법은 인간의 행위를 규율하고 조정하는 준칙을 마련하는 작용이므로, 법규범은 수범자가 어떠한 결정을 내리는 경우 그 결정에 영향을 받도록 가능한 한 이해하기 쉽게 형성

되어야 한다.⁵⁵⁵⁾ 더욱이 법규범은 수범자에게 특정한 행위를 하도록 유도하는 정보로 이해될 수 있다. 이러한 점에서 현행의 개인정보보호법이 수범자에 대한 정보제공적 기능을 제대로 수행하지 못하고 있음을 보여준다고 할 수 있다.

둘째, 개인정보보호 관련 법조항을 검색해본 적이 있다는 사람들 중에서도 관련 법조항을 찾는 데 어려움이 있었다는 응답이 일반인 87.2%, 전문가 71.88%로 나타났다. 일반인들이 어려움을 느낄 경우 수범자의 예측가능성을 보장해주지 못한다는 점에서 법치주의의 관점에서 적잖은 문제가 있다고 볼 수도 있다. 검색이 어려운 이유로 “용어가 어려워서” 혹은 “잘 몰라서”라는 응답이 2.6%에 불과한 것으로 보아서, 입법체계의 불완전성에서 비롯된 측면이 큰 것으로 판단된다. 이는 전문가들조차 관련 법조항을 검색하는 데 어려움을 겪었다는 점에서도 확인이 된다. 어려움을 느낀 이유를 “분야별 관련 법률이 잘 구분되어 있지 않아서”라고 응답한 비율이 일반인과 전문가 모두에게서 가장 높게 나왔으나, 근무기간이 장기간인 경우와 법실무자들에게서는 “개인정보보호에 관한 법률이 하나로 되어 있지 않아서”라고 응답한 비율이 상대적으로 높게 나온 것이 이채롭다. 법률전문가가 아닌 사람들의 입장에서는 그 사안에 딱 맞아떨어지는 법조항이 있어야 찾기가 쉬운데 실제로 그렇지가 못하다는 느낌을 많이 받았던 것이 아닌가 짐작된다. 이를 두고 입법체계의 방향성을 가늠하는 기준으로 삼기에는 무리가 있을 것으로 보인다.

셋째, 개인정보보호 관련 내용이 포함되어 있을 것으로 생각되는 법률로 일반인 조사에서 ‘신용정보의 이용 및 보호에 관한 법률’(86.2%), ‘정보통신망 이용 촉진 및 정보보호 등에 관한 법률’(84.2%), ‘금융실명거래 및 비밀보장에 관한 법률’(82.4) 등이 ‘공공기관의 개인정보보호에 관한 법률’(81.0%)보다 다소 높게 나온 것이 놀랍다. 이에 비해

555) 박영도, 『입법평가의 이론과 실제』 (한국법제연구원, 2007), 59면.

전문가 조사에서는 ‘공공기관의 개인정보보호에 관한 법률’(100%)이 가장 높게 나왔다는 점에서 더욱 그러하다. 일반인들이 개인정보의 침해 가능성을 공공부문보다 민간부문에서 더 높게 볼 뿐만 아니라, 개인의 신용정보나 금융정보 혹은 인터넷상의 개인정보 등이 대량으로 유출되거나 부당하게 이용되는 사례를 자주 접하기 때문이 아닐까 추측된다.

2. 입법체계에 대한 숙지의 정도

첫째, 개인정보보호법이 공공부문과 민간부문에 각기 별도로 적용되고 있음을 알고 있는 비율이 일반인의 경우 9.1%에 그치지만, 전문가는 53.66%에 이르는 것으로 나타났다. 양 측에 편차가 아주 심하다는 것을 알 수 있다.

둘째, 공공기관개인정보보호법이 전산처리된 파일만을 보호의 대상으로 하고 있다는 점에 대해 막연하게나마 알고 있다고 응답한 비율은 일반인들의 경우 30.0%, 전문가의 경우 46.34%로 큰 차이가 없는 것으로 나타났다. 하지만 이 가운데 정확히 알고 있다는 응답에서는 3.5%와 26.83%로 뚜렷한 차이를 보여준다.

셋째, 민간부문의 일반법 부존재에 대한 인식 여부에 대한 설문에서 “잘 알고 있다”는 응답이 일반인의 경우 6.9%에 그쳤지만, 전문가의 경우 63.4%로 나타났다. 예상할 수 있었던 바와 같이 실제로도 매우 현격한 차이를 보여주고 있다.

3. 입법체계의 방향성

첫째, 개인정보보호법의 제정 동향에 대해 전문가의 78.05%가 인식을 하고 있는 것으로 나타났다. 근무기간이 장기간일수록, 그리고 법 실무에 종사하는 사람일수록 그 인식률이 높았다.

둘째, 통합적 법률 제정에 대한 의견에서 전문가의 85.37%가 찬성을 하였고, 반대는 7.32%에 그쳤다. 통합적 법률에 찬성한 이유는 “양 부문에 걸쳐 법집행의 통일을 기할 필요가 있다”(65.71%), “법적 보호의 공백을 최소화하기 위해 불가피하다”(57.14%), “일반 국민들의 법적 혼란을 줄이기 위해 필요하다”(54.29%), “양 부문을 굳이 달리 규율해야 할 이유가 없다”(22.86%)의 순서로 나타났다. 여기에 반대한 의견은 3명에 그쳐서 의미 있는 결과를 도출하기 어려울 것으로 본다.

셋째, 민간부문에 대한 별도의 일반법 제정 필요성에 대해 전문가의 60.98%가 찬성을 하였다. 하지만 이는 현행과 같이 공공부문과 민간 부문 간에 분리된 입법을 취한다고 가정할 때의 응답이어서 그 자체를 이원적 일반법주의에 대한 선호도로 볼 수는 없다.

넷째, 통합적 법률제정시의 입법체계에 관해서 기본법의 입법체계를 따라야 한다는 응답이 48.78%, 일반법의 체계를 따라야 한다는 응답이 41.46%를 각각 차지하였다. 양측의 의견이 거의 엇비슷하게 나타나고 있는데, 기본법주의와 일반법주의 가운데 어떠한 형식을 취할 것인지에 대한 의미 있는 결론을 도출하기는 어려울 것으로 본다. 다만 기본법의 체계로 취할 경우에 기본법에서 규정해야 할 사항으로 선택된 모든 항목이 85%를 상회하고 있다. 이는 기본법이라고 하더라도 가급적이면 개인정보보호에 필요한 다수의 규정을 두자는 취지로 받아들일 수 있다. 물론 기본법의 체계를 선택한 응답자들의 의견에도 이와 같은 의중이 상당 부분 반영되어 있을 것으로 짐작된다. 왜냐하면 기본법에서 권리행사의 방법과 절차, 개인정보보호기구, 피해의 구제와 제재 등도 규정하게 되면, 최소한의 기본적 사항의 규율로 보기 어려울 것이기 때문이다. 따라서 본 설문조사에서는 사실상 일반법주의에 가까운 입법의 체계를 선호하는 것으로 볼 여지가 있는 만큼, 이 부분에 관한 한 단순한 수치의 대비만으로 성급한 결론을 내리는 것은 곤란하다고 본다.

4. 조사결과의 분석

이상의 조사결과를 놓고 볼 때, 현행의 개인정보보호법제는 수범자에게 있어 수용성이 떨어지고, 정보제공의 기능도 원활하게 수행되고 있지 못한 것으로 파악된다. 어떤 법규범이 수범자의 관점에서 그 대략적 의미조차 파악하기 어렵게 되어 있다면, 국민들의 예측가능성이나 법적 안정성을 확보하기 어렵다. 이러한 경우에는 입법의 공정성이나 효율성, 나아가 법의 실효성 등에 있어서도 적잖은 문제를 일으킬 수 있다.

현행법제의 적용범위나 입법체계의 형태에 대해 수범자인 일반인들이 인식하는 수준은 매우 낮은 편이라고 볼 수 있다. 하지만 그럼에도 불구하고, 산재해 있는 여러 개인정보보호법제를 정비할 필요가 있다는 점에 공감하는 것을 엿볼 수 있다.

구체적인 입법체계의 개선방향에 대해서는 전문가들은 통합적 법률 제정에 대해 압도적 다수가 찬성의 의견을 밝혔다. 통합적 법률을 제정하더라도 기본법의 입법체계를 따라야 한다는 응답이 좀 더 높게 나왔지만, 그 차이는 의미가 있다고 하기 어렵다. 오히려 기본법에서 규정해야 할 사항으로 선택된 항목을 보면 사실상 일반법의 체계에 가까운 입법의 체계를 선호하는 것으로 볼 여지도 있는 것이다. 따라서 이에 관한 한 본 설문결과는 그 자체로서 통합적 법률의 제정방향을 결정하는 기준으로 활용되기에 한계가 있다고 하겠다.

제 3 장 우리 개인정보보호법의 입법체계 평가

제 1 절 개인정보보호법제의 개관

우리나라의 정보프라이버시 보호를 위한 법제는 아래의 <표>에서 보는 바와 같이 공공부문과 민간부문으로 구분되어 그 법적 근거와 집행의 체계를 달리하고 있다.

[표 3-3-1] 개인정보보호 관련법제의 현황

적 용 분 야		법 률 명	비 고
공공부문		『공공기관의 개인정보 보호에 관한 법률』	1994년 제정, 1999년 개정
민 간 부 문	온라인 사업자	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	2001년 전문개정, 2002년 개정
기타분야 (개별법)		『신용정보의 이용 및 보호에 관한 법률』, 『위치정보의 보호 및 이용 등에 관한 법률』, 전자정부법, 주민등록법, 국세기본법, 통신비밀보호법, 보건의료기본법, 『특정범죄신고자 등 보호법』, 『금융실명거래 및 비밀보장에 관한 법률』, 형법 등	개별 분야별로 업무상 비밀보호 및 정보보호규정 산재

다만 공공부문에 있어서는 전산처리된 개인정보의 보호에 관한 일반법으로 『공공기관의 개인정보 보호에 관한 법률』이 제정되어 있으며, 민간부문에 있어서는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』이 정보통신망에서의 개인정보보호에 관한 일반법으로 기능하고 있다. 개별 분야별로 개인정보보호에 관한 특별규정을 두고 있는 경우로서 대표적인 법률과 관련 규정의 주요 내용을 개략적으로 살펴보면 아래의 표와 같다.

[표 3-3-2] 개별 분야별 개인정보보호입법과 주요 내용

대상 정보	관련 법률	규 정 내 용
정부 기록 정보	『공공기관의 개인정보 보호에 관한 법률』	○ 국가, 지방자치단체 등 정부기관 보유의 개인정보 보호
	『공공기관의 정보공개에 관한 법률』	○ 국민의 알 권리 보장을 위한 공공기록의 공개, 열람
	전자정부법	○ 당사자의사에 반하는 개인정보사용의 금지 등
	주민등록법	○ 전국민에 대한 주민등록번호의 부여 등
통신 비밀	통신비밀보호법 등	○ 우편물의 검열, 전기통신의 감청, 통신사실 확인 자료의 제공, 타인간의 대화를 녹음 또는 청취 금지 등 통신관련 생활의 보호
	『통신제한조치의 허가절차 및 비밀유지에 관한 규칙』	○ 범죄수사나 개인안보를 위한 통신제한조치의 허가절차
	전기통신사업법	○ 개별이용자에 관한 정보의 공개 및 유용금지 등
보건 의료 정보	보건의료기본법	○ 보건의료정보의 누출, 변조 금지
	의료법, 전염병예방법 등	○ 업무상 비밀 누설 금지
	『생명윤리 및 안전에 관한 법률』	○ 유전정보의 보호 등
소비자 정보	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	○ 정보통신망사업자의 개인정보보호
	『위치정보의 보호 및 이용 등에 관한 법률』	○ 위치정보사업자 등의 개인위치정보의 보호
	『신용정보의 이용 및 보호에 관한 법률』	○ 금융기관, 백화점, 할부회사 등의 고객 신용정보 보호
	『금융실명거래 및 비밀보장에 관한 법률』	○ 신용정보주체의 열람 및 정정 청구 등
	증권거래법 등	○ 금융실명거래에 따른 금융기관이용자의 개인정보 이용 등
사생활 일반	형법 제316조(비밀침해죄)	○ 봉합 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록 등 특수매체기록에 대한 기술적 침해

제 2 절 입법체계상의 특징과 문제점

1. 입법체계상의 특징

(1) 이원적 규율체계와 개별입법주의

우리나라 개인정보보호 법률체계는 공공부문과 민간부문에 각각 적용되는 법률을 따로 두고 있는 이원적 시스템으로 되어 있다. 또한 각 부문을 규율하는 기본법이 있어서 원칙이 규정되고, 개별법에 특수한 부분이 규율되는 시스템이 아니라 개별법에 개인정보보호 관련 조항이 있어 이를 토대로 개인정보가 보호되고 있다. 결국 우리나라 현행 개인정보보호법제의 특징은 공·사부분의 이원적 규율체계와 개별입법주의로 요약될 수 있다.

[표 3-3-3] 현행 개인정보보호법제의 체계⁵⁵⁶⁾

공공부문	구 분	민간부문
『공공기관의 개인정보 보호에 관한 법률』	일반법 (전산처리정보)	『정보통신망 이용 촉진 및 정보보호 등에 관한 법률』
개별법		
전자정부법, 정보화촉진기본법, 정보통신기반보호법, 전자거래기본법, 전자서명법, 통신비밀보호법, 『위치정보의 보호 및 이용 등에 관한 법률』, 『전자상거래 등에서의 소비자보호에 관한 법률』, 『신용정보의 이용 및 보호에 관한 법률』, 보험업법령, 예금자보호법, 『금융실명거래 및 비밀보장에 관한 법률』, 주민등록법, 호적법, 도로교통법, 형법, 『특정범죄신고자 등 보호법』, 국세기본법, 의료법, 보건의료기본법, 『응급의료에 관한 법률』, 사회보장기본법		

556) 최월화, 『전자정부와 정보프라이버시 보호』 (2003), 29면.

(2) 전산화된 개인정보의 우선적 보호

현행 개인정보의 보호를 주된 목적으로 하여 제정된 주요 법률들은 대개 전산화된 개인정보를 보호대상으로 하고 있다. 이에 따라 현재 수기식 개인정보의 보호는 개인정보보호에 관한 특별법이나 관련 규정을 두고 있는 전통적인 개별 법률에 의존할 뿐, 일반적인 개인정보보호법의 보호대상에서 제외되고 있는 실정이다. 이러한 점에서 현행 개인정보보호법제에 있어서 보호대상이 되는 개인정보는 일차적으로 전산화된 개인정보이고, 이차적으로 수기식 개인정보라고 할 수 있다.

2. 입법체계상의 문제점

(1) 수범자의 혼란 야기

이원적 규율체계와 개별입법주의는 개인정보보호에 관한 수범자의 규범에 대한 이해도와 법적 규율의 실효성을 저하시킬 가능성이 높다. 즉, 개인정보보호에 관한 포괄적인 단일의 법률이 존재하지 않기 때문에 수범자의 입장에서는 개인정보보호법제의 준수나 권리구제 등을 위해 산재해 있는 수많은 관련 법률들을 뒤져 봐야 하는 문제가 있다. 그리고 분야별로 달리 규율하는 법률의 내용에 대해 기본적인 이해가 없을 경우 그것마저도 쉽지가 않다. 설령 관련 조항을 찾아서 확인하더라도 개별 법률마다 적용되는 원리나 기준이 다를 경우 규범의 준수나 권리의 구제에 있어서 적잖은 혼돈을 느끼게 될 수 있다.

예컨대 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』은 당초의 논의과정에서 개인정보보호에 관한 사항을 중점적으로 다루고 불법정보에 대한 대책으로서의 건전한 정보통신윤리에 관한 사항은 새로운 법률을 제정하는 방향으로 설계되었다. 하지만 개인정보보호와 불법정보 문제를 동법에서 통합적으로 규제함으로써 법률의 명칭에

개인정보보호가 아닌 정보보호로 규정하게 되었다. 그러나 불법정보에 관한 문제는 개인정보보호의 문제와는 그 접근시각이나 규제의 방식이 상이하다고 해야 할 것이다. 이러한 점에서 일반 국민인 수범자의 입장에서 동법이 정보통신망의 이용과 관련된 개인정보보호의 일반법으로서 인식할 수 있을 것이라고 기대하기는 결코 쉬운 일이 아닐 것이다.

한편 정보통신망법은 전기통신사업법 제2조 제1항 제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 “정보통신서비스제공자”라는 용어로 정의하고 있다.⁵⁵⁷⁾ 그리고 이를 바탕으로 정보통신서비스제공자의 의무를 여러 곳에서 부과하고 있다. 한편 저작권법은 다른 사람들이 저작물이나 실연·음반·방송 또는 데이터베이스를 정보통신망(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호의 정보통신망을 말한다)을 통하여 복제 또는 전송할 수 있도록 하는 서비스를 제공하는 자를 “온라인서비스제공자”로 정의하고 역시 여러 곳에서 의무를 부과하고 있다.⁵⁵⁸⁾ 다만 「공공기관의 개인정보 보호에 관한 법률」은 관리주체로 공공기관 등으로 규정하여 상당히 자세한 정도로 규범의 수범자를 정하고 있다. 이러한 점에서 민간부문의 경우 법적 규범의 수범자로서 과연 누가 개인정보를 처리 또는 취급하는 자인가(관리주체)에 대한 법적 정의는 아직 없다고 볼 수 있다.⁵⁵⁹⁾ 이러한 모호한 개인정보관리주체의 정의는 개인정보의 관리상의 소홀 내지는 피해 발생시 제1차적인 책임자를 확정하기 어렵게 만들고, 관리주체의 관리소홀을 야기할 우려가 크다.

557) 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 제2조.

558) 저작권법 제2조.

559) 성선제, “개인정보취급자의 의무와 규제수단”, 제3회 개인정보보호정책포럼, 2004. 6, 2-3면.

(2) 규율체계상의 불균형 발생

공공부문과 민간부문의 이원적 규율체계는 민간부문과 공공부문 사이에 개인정보보호의 불균형을 야기하고 있는 문제가 있다.

예컨대 『공공기관의 개인정보 보호에 관한 법률』에 규정된 개인정보는 “생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보”이고, 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 규정된 개인정보는 “생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보”를 말한다. 이들 법률이 보호하고 있는 개인정보는 모두 식별가능성을 개인정보의 핵심요소로 삼고 있고, “생존하는 개인”에 관한 정보를 대상으로 한다는 공통점이 있지만, 『공공기관의 개인정보 보호에 관한 법률』상의 개인정보는 성명과 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보로 한정하여 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』에 비해 그 보호범위가 좁은 편이다. 이는 이 법이 기본적으로 공공기관에 의해 컴퓨터로 처리되는 정보에만 적용된다는 점에서 법률의 보호대상인 개인정보의 개념도 다소 제한적으로 규정한 것이다.⁵⁶⁰⁾

또한 공공부문의 경우 『공공기관의 개인정보 보호에 관한 법률』이 개인정보를 보유하고 관리하는 대부분의 행정기관에 적용됨으로써 일반적인 개인정보관리상의 의무가 부과된다. 이에 비하여 민간부문의 경우 전 민간부문에 적용되는 일반법이 제정되지 않고 특정 분야별로 적용되는 법률과 관련 조항이 산재하기 때문에 개인정보관리상의 기본적 보호조치가 강구되지 않고 주로 사후 처방적인 보호가 중심이

560) 이창범·윤주연, 『각국의 개인정보피해구제제도 비교연구』(개인정보분쟁조정위원회, 2003), 25면.

되고 있다. 이처럼 민간부문에 비해 공공부문의 개인정보보호의 강도와 범위가 상대적으로 약하게 설정한 것은 개인정보침해의 위험도를 고려할 때 합리적인 비례관계에 있다고 보기 어려운 측면이 있다.

(3) 법적 보호의 공백 발생

일반적으로 『공공기관의 개인정보 보호에 관한 법률』은 공공기관이 보유한 개인정보의 보호하기 위한 일반법으로서의 성질을 가진다고 보고 있으나, 엄밀히 말해 공공부문에서의 일반법으로서 기능하는 데 일정한 한계가 있는 것이 사실이다. 동법은 컴퓨터로 처리되는 개인정보만을 대상으로 하고 있어서, 수기식 파일이나 자료에 담긴 개인정보까지 보호의 대상으로 삼고 있지 못하기 때문이다.

한편, 민간부문의 경우에서도 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』은 정보통신망의 이용에 따른 개인정보만을 보호의 대상으로 하고 있을 뿐, 기타 민간부문에 있어서는 개인정보보호에 관한 일반법으로서 기능하지 못한다. 이렇게 볼 때 공공기관개인정보보호법과 정보통신망법은 각각 공공부문과 민간부문에서의 개인정보보호에 관한 대표적인 입법이라고 부르는 것이 보다 정확한 평가라 할 것이다. 이러한 제한적 일반법의 존재와 개별법주의가 맞물리게 될 경우 개인정보보호의 사각지대가 발생하는 것은 불가피한 현상일지도 모른다.

현재 개인정보의 컴퓨터 화일화가 상당히 진행되었다고 해도 여전히 수기문서로 남아 있는 개인정보가 상당히 존재하고, 수기문서와 컴퓨터문서가 공존하거나 전산화가 진행되고 있는 수기문서가 상당부분 존재하기 때문에, 수기문서의 오남용의 문제는 단지 업무상비밀누설과 관련된 부분만 통제될 뿐 관리상의 효율성이나 오남용 예방을 위한 관리체계는 거의 존재하고 있지 않은 상태이다. 이러한 문제는 오남용된 다음의 수기문서가 컴퓨터 화일화되는 경우 컴퓨터 화일화

된 개인정보의 남용과 동일한 문제점을 갖고 있다는 점에서 수기식 개인정보도 통상적인 개인정보보호와 동일하게 보호되어야 하고, 그렇지 않는 경우 개인정보보호의 사각지대로 남아 있게 된다는 문제를 갖게 된다. 이와 관련하여 의료분야의 경우 통상적인 개인정보보호의 원칙이 일률적으로 적용되어야 하고, 특히 수기로 처리되던 개인정보가 컴퓨터로 처리되면서 문제점이 증폭하여 수기의 의무기록도 중요한 보호대상 개인정보에 포함해야 한다는 주장이 제기되고 있다.⁵⁶¹⁾

한편, 개인정보보호는 정보사회에서 비롯되고 있음에 비추어 그것은 공공부문과 사적 부문의 구별이 불투명해질 정도로 심각한 지경에 이르고 있다. 종래 개인에 관한 정보는 주로 공공기관이나 언론기관 등만이 제대로 수집·관리할 수 있었으나 정보사회의 진전에 따라 재벌기업 등 사적 기관도 이들 기관 못지않게 엄청난 정보를 수집·관리할 수 있게 되었다. 이에 각국의 개인정보보호법제는 사적 기관의 개인정보처리에 관한 규율까지를 통합적으로 관리하는 법제도 취하고 있지만 우리의 법제는 공공기관에 한정하고 있다. 이에 사적 기관에 의한 개인정보에 관한 규율을 보다 체계화시킬 수 있는 법제의 정립이 요망되고 있다.

그간 우리나라에서도 사적 기관에 의하여 개인정보의 불법적인 수집·처리 등에 따라 이미 많은 문제점이 적시되고 있다. 행정전산망, 동창회명부, 신용카드업자 등이 보유·처리하고 있는 개인정보가 홍보물 발송대행업체에게 유출된 사례, 수집이 금지되고 있는 개인정보가 통신판매업체의 통신판매에 이용되고 있는 사례, 전국적으로 수백개에 이르는 개인정보 전문유통업체 및 브로커의 개인정보 판매행위가 드러난 사례, 개인정보 취급자가 개인정보를 몰래 팔아넘긴 사례 등이 발생하고 있다. 현재 사적 부문에 관한 통일적인 규율법제가 없는 상황하에 개인의 금융정보를 보호하기 위하여 「금융실명거래 및

561) 서정욱, “보건의료 분야의 개인정보보호”, 『개인정보보호정책포럼』, 2004, 6면.

비밀보장에 관한 법률』(제4조, 제12조)에서, 개인의 신용정보를 보호하기 위하여 「신용정보의 이용 및 보호에 관한 법률」을 제정하고 있다. 그 밖에 형법(제184조, 제316조 제2항 등), 의료보험법(제71조의3, 제75조), 증권거래법(제5조, 제208조), 신용카드업법(제14조, 제25조) 등에서도 비밀누설시 처벌규정을 두고 있다.

그런데 이와 같은 사적 부분에서의 개인정보보호가 법제적으로 미흡한 상황하에서 이를 보다 종합적이고 포괄적으로 규율할 수 있는 법적 장치를 마련하고자 하는 요구가 제기되어 왔지만, 사적 부문에서의 규율이 갖는 한계로 인하여 이의 현실적 구현에 이르지 못하고 있다. 비록 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이 정보통신망을 이용한 개인정보보호에 관한 일반법으로 기능하고 있지만, 민간부문에서 발생할 수 있는 개인정보침해의 사례에 빠짐없이 대처하기에는 공백이 많이 존재하는 것이 현실이다. 따라서 민간부문 전체를 포괄할 수 있는 일반법으로서의 개인정보보호법을 정립할 필요가 있다.

제 3 절 개인정보보호법(안)에 대한 분석

1. 법제화 동향

1999년부터 시민단체들은 인터넷상의 개인정보보호를 위한 법제를 정비할 것을 촉구하는 운동을 시작하였다. 신뢰성 있는 정보사회를 구축하기 위해서는 개인정보 보호를 위한 사회적 시스템의 마련이 필요하다며, 개인정보보호기본법 제정과 공공·민간 부문을 포괄하는 독립적인 개인정보보호위원회 설립이 반드시 통과되기를 촉구하였다.⁵⁶²⁾

562) 문화연대·민주사회를위한변호사모임·지문날인반대연대·진보네트워크센터·참여연대·한국노동네트워크협의회·함께하는시민행동, 프라이버시법제정을위한연석회의, 2004. 10. 20.

2003년 10월 개인정보보호기본법 제정 추진이 결정된 이후 정부혁신위원회는 개인정보보호가 전자정부의 성패를 좌우하는 문제라는 점을 인식하게 되었으며, 정보사회의 신뢰성과 안전성을 확보하기 위한 개인정보보호기본법의 입법을 추진하였다.

이후 2004년 11월 22일에 민주노동당 노회찬 의원이 개인정보보호에 관한 기본원칙 정립, 권리구제의 방법 현실화, 개인정보보호위원회를 독립기구로 설립, 개인정보침해에 대한 집단소송제도 도입 등을 골자로 하는 「개인정보보호기본법안」을 발의하였다.

2005년 2월 1일에는 정성호 의원이 독자적으로 마련한 「개인정보보호법안」을 발의하였다. 2005년 2월 2일에는 이은영 의원이 개인정보보호의 기본원칙 천명, 정보주체의 참여권 보장, 국가인권위원회의 개인정보특별위원회를 통한 권리구제 등을 골자로 하는 「개인정보보호기본법안」을 발표하였다. 그리하여 개인정보보호기본법이 2005년 상반기 중으로 입법될 것으로 전망되었으나,⁵⁶³⁾ 이 두 안은 개인정보보호기구의 문제 등으로 인하여 4월 15일에 철회되었다.

이후 열린우리당의 당론으로 같은 해 7월 11일 이은영 의원이 대표로 발의한 「개인정보보호법안」이 다시 제출되었다. 그리고 2005년 10월 17일에는 한나라당 이해훈 의원이 「개인정보보호법안」을 발의하였다.

그러나 이들 법률안은 의원들의 관심부족으로 인하여 제17대 국회에서 결실을 보지 못하였다. 최근 제18대 국회에 들어서면서 행정안전부가 방송통신위원회와 뜻을 모아 새로운 개인정보보호법안을 마련하여 국회에 제출한 바 있고, 2008년 8월 8일 이해훈 의원도 재차 개인정보보호법제정안을 발의한 상태이다.

563) 한국전산원 정보화정책팀, 『개인정보보호법제의 현황과 그 발전전망』 (한국전산원, 2005. 3. 31), 11면.

2. 각 법안의 소개

우선 과거 17대 국회에서 관련 상임위원회에 회부되어 검토작업을 거친 바 있는 (구)이혜훈의원 대표발의 법안(이하 ‘(구)이혜훈법안’이라 한다.), 이은영의원 대표발의 법안(이하 ‘이은영법안’이라 한다.), 노회찬의원 대표발의 법안(이하 ‘노회찬법안’이라 한다.) 등 3개 법안을 구성체계상 특징을 중심으로 살펴보고, 이어서 최근 18대 국회에서 발의된 행정안전부 법안과 (신)이혜훈 의원 대표발의 법안(이하 ‘(신)이혜훈법안’이라 한다.)을 소개하면서 그 입법체계와 관련된 사항을 비교분석하기로 한다.

(1) (구)이혜훈 법안

1) 제안경과

2005년 10월 17일 이혜훈 의원 등 국회의원 13인은 「개인정보보호법안」(의안번호 제2953호) 및 「공공기관의개인정보보호에관한법률 일부개정법률안」(의안번호 제2954호)과 더불어 「정보통신망이용촉진및정보보호등에관한법률 일부개정법률안」(의안번호 제2955호)을 국회에 제출하였고, 이 법안들은 같은 해 10월 19일자로 소관위원회인 국회 행정자치위원회와 과학기술정보통신위원회에 각각 회부되었다. 하지만 17대 국회가 임기만료로 해산되면서 이 법안은 자동적으로 폐기되었다.

2) 법안의 입법체계상 특징

① 개인정보보호법안

이 법안은 공공영역과 민간영역의 개인정보보호를 포괄하는 종합적인 개인정보보호법의 제정을 목표로 하고 있다. 하지만 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 적용을 제외하고 있다(안 제62조).

그리고 개인정보처리에 관한 원칙을 개인정보처리 일반에 적용되는 원칙을 정하고(안 제2장 및 제3장), 공공부문과 민간부문에 각각 적용되는 특칙으로 구분하여 규정하고 있다(안 제4장 및 제5장).

한편, 개인정보보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리소속으로 개인정보위원회를 두도록 하였다.

② 다른 법률의 정비

개인정보보호 행정체계를 일원화함으로써 이중규제를 방지하기 위하여 『공공기관의 개인정보보호에 관한 법률』을 폐지하고, 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』중 개인정보보호 관련 조항을 삭제하는 내용의 개정법률안도 함께 제출하였다.

(2) 이은영 법안

1) 제안경과

2005년 7월 11일 이은영 의원은 국회의원 145인의 찬성을 얻어 『개인정보보호법안』(의안번호 제2219호)과 『공공기관의개인정보보호에 관한법률 일부개정법률안』(의안번호 제2220호) 및 『정보통신망이용촉진 및정보보호등에관한법률 일부개정법률안』(의안번호 제2221호)을 국회에 제출하였으며, 이 법안들은 같은 해 7월 13일자로 소관위원회인 행정자치위원회와 과학기술정보통신위원회에 각각 회부되었다. 하지만 17대 국회가 임기만료로 해산되면서 이 법안도 역시 자동적으로 폐기되었다.

2) 법안의 입법체계상 특징

① 개인정보보호법안

이는 「공공기관의 개인정보보호에 관한 법률」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 존치시키는 것을 전제로 마련된 법안이다.

여기서는 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 하였다(안 제6조). 그리고 일정수준의 개인정보취급자에게 개인정보보호담당자를 지정하도록 하여 개인정보취급자가 자율적으로 규제할 수 있도록 하였다(안 제16조).

한편, 국가의 개인정보보호 시책의 강구와 제도 및 사회적 관행의 개선을 위한 책무를 규정하고 개인정보보호위원회가 개인정보에 관한 시책을 관장하도록 하였다(안 제18조 및 제19조).

② 다른 법률의 정비

개인정보보호법의 입법추진에 따라 국민들의 개인정보 보호기능을 효율적으로 수행하기 위하여 공공기관의 개인정보보호에 관한 법률 일부조항을 개정하고자 「공공기관의개인정보보호에관한법률 일부 개정법률안」을 제출하였다. 여기서는 개인정보에 관한 분쟁조정 절차를 일원화하기 위하여 공공기관과 관련한 개인정보분쟁에 관하여 개인정보보호위원회의 개인정보분쟁조정위원회에 분쟁조정을 신청할 수 있도록 하고(안 제15조), 개인정보에 관한 사항을 심의하는 개인정보심의위원회를 폐지하였다(안 제22조).

그와 동시에 개인정보보호법의 입법추진에 따라 국민들의 개인정보 보호기능을 효율적으로 수행하기 위하여 「정보통신망이용촉진및정보

보호등에 관한 법률 일부개정법률안』도 함께 제출하였다. 여기서는 개인정보의 파기 청구시 필요한 사항을 이용자에게 고지하도록 하고(안 제29조), 이용자가 개인정보의 이용에 관한 동의를 철회하거나 열람·내역 및 정정요구를 하는 경우 필요한 사항을 이용자에게 고지하도록 하였다(안 제30조). 아울러 개인정보에 관한 분쟁조정 절차를 일원화하기 위하여 개인정보와 관련한 분쟁에 관하여 개인정보분쟁조정위원회 관련 규정을 삭제하였다(안 제33조 내지 제40조).

(3) 노회찬 법안

1) 제안 경과

『개인정보보호기본법안』(의안번호 938)은 노회찬 의원 등 22인의 국회의원에 의해 2004년 11월 22일 제출되었으며, 같은 해 11월 24일자로 소관위원회인 행정자치위원회에 회부되었다. 하지만 이 법안도 이후 시일만 끝나다가 17대 국회가 임기만료로 해산되면서 자동적으로 폐기되는 운명을 맞았다.

2) 법안의 입법체계상 특징

① 개인정보보호기본법안

공공부문과 민간부문을 포괄적으로 규율하는 통합형 입법주의를 채택하고 있다. ‘기본법’이라는 명칭을 쓰고 있지만, 그 내용을 보면 상당히 일반적인 사항까지 정하고 있다.

여기서는 개인정보보호에 관한 기본원칙을 정하고, 공공부문과 민간부문의 개인정보보호를 포괄하여 담당하는 독립된 기구를 설치하는 동시에, 개인정보와 밀접한 관계를 가지는 기술이나 설비의 도입을 효과적으로 관리함으로써 개인정보의 불법유출과 이를 이용한 불법행위들을 차단하는 등의 내용을 담고 있다. 특히 눈에 띄는 내용을 살

펴보면, 개인정보 데이터베이스를 보유하고자 하는 자가 공공기관의 개인정보 데이터베이스에 해당하는 경우에는 사전에 개인정보보호위원회에 등록하도록 하고(안 제20조 제1항 제1호), 국가안전보장·사회질서유지 및 공공복리를 위하여 개인정보위원회가 필요하다고 인정한 경우, 정보주체의 동의가 있는 경우 등을 제외하고는 자기가 수집·보관하는 개인정보 데이터베이스를 공공기관이 처리하는 개인정보 데이터베이스와 결합할 수 없도록 하였다(안 제23조 제1호 및 제2호). 그리고 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(안 제29조), 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 신청하도록 하였다(안 제95조).

한편, 이 법 및 개인정보 보호에 관한 다른 법률의 준수여부를 감독하기 위하여 개인정보보호위원회를 두고(안 제60조), 개인정보침해행위가 계속 중에 있다는 상당한 개연성이 있고, 이를 방지할 경우 회복하기 어려운 피해발생의 우려가 있다고 인정할 때에는 그 진정에 대한 결정 이전에 피진정인, 그 소속기관등의 장에게 개인정보의 수집, 이용의 중단, 기타 필요한 조치를 하도록 권고할 수 있게 하였다(안 제93조).

② 다른 법률의 정비

먼저 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」중 개인정보 보호 관련 규정(제22조 내지 제40조)을 삭제하고(부칙 제3조), 다음으로 「공공기관의 개인정보 보호에 관한 법률」을 폐지하고 있다(부칙 제4조).

(4) 행정안전부 법안

1) 제안경과

새 행정부가 들어서면서 공공부문과 민간부문을 포괄적으로 규율하는 새로운 내용의 법안을 마련하여 행정안전부가 2008년 7월 국회에 ‘개인정보보호법 제정법률안’을 제출하기에 이르렀다.

2) 법안의 입법체계상 특징

① 개인정보보호법안

이 법안은 공공·민간을 망라하여 국제 수준에 부합하는 개인정보 처리원칙을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화하여 개인정보의 안전한 이용 환경을 조성하고 개인의 권리와 이익을 보장하기 위해 마련되었다.

구체적으로 개인정보보호법 적용대상을 공공·민간 모든 개인정보 처리자로 하고(안 제2조), 개인정보의 수집·이용·제공 등 단계별 보호기준을 정하고 있다(안 제15조 내지 제20조). 그리고 고유식별정보의 처리제한 강화(안 제23조), ㉔ 영상정보처리기의 설치제한 근거 마련(안 제24조), ㉕ 개인정보파일의 등록 및 공개제도 도입(안 제30조), ㉖ 개인정보 영향평가제도 도입(안 제31조), ㉗ 개인정보 유출사실의 통지제도 도입(안 제32조), ㉘ 정보주체의 권리 보장(안 제4조, 제33조 내지 제36조), ㉙ 개인정보침해사실의 신고(안 제51조) 등을 규정하고 있다.

한편, 개인정보보호 기본계획, 법령 및 제도 개선 등 개인정보에 관한 주요 사안을 심의하기 위하여 국무총리 소속하에 개인정보보호위원회를 두고 있다(안 제9조 내지 제10조).

② 다른 법률의 정비

우선 「공공기관의 개인정보 보호에 관한 법률」을 폐지하도록 하고 있다(안 부칙 제5조 제1항).

다음으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」중 제33조부터 제40조까지의 규정, 제52조제3항제8호, 제66조제1호 및 제67조를 각각 삭제하고, 나아가 제4조제1항·제3항, 제64조의2제3항, 제65조제1항 및 제69조 중 “행정안전부장관, 지식경제부장관 또는 방송통신위원회”를 각각 “지식경제부장관 또는 방송통신위원회”로 하며, 제64조제1항·제3항·제4항·제5항·제6항·제9항·제10항, 제64조의2제1항·제2항·제3항, 제65조제3항, 제76조제1항제12호, 제76조제4항·제5항·제6항 중 “행정안전부장관 또는 방송통신위원회”를 각각 “방송통신위원회”로 개정하도록 하고 있다(안 부칙 제5조 제2항).

(5) (신)이혜훈 법안

1) 제안경과

17대 국회에서 자신의 법안이 폐기된 바 있는 이혜훈 의원은 2008년 8월 8일 14인의 국회의원을 대표하여 새로 마련한 ‘개인정보보호법’ 제정안을 18대 국회에 제출하였다. 제안이유는 기존의 법률안과 차이가 없지만, 법안의 내용에 있어서는 다소간 차이를 보이고 있다.

2) 법안의 입법체계상 특징

① 개인정보보호법안

공공부문과 민간부문을 포괄적으로 규율할 수 있는 종합적인 개인정보보호법안을 제안하고 있다. 하지만 단순히 개인·가족의 이용을 목적으로 개인정보를 수집·처리하는 경우, 통계·연구 등을 목적으

로 식별성을 제거하고 개인정보를 수집·처리하는 경우에는 이 법의 적용을 제외하고, 취재 및 보도, 종교활동, 정치 및 정당활동을 목적으로 개인정보를 수집·처리하는 경우에는 이 법의 일부의 적용을 제외하고 있다(안 제62조). 주목할 만한 내용을 소개하면, 소비자단체, 근로자단체, 사업자단체, 공공단체 등에 의한 자율규제활동을 촉진·장려하기 위하여 자율규제원칙을 선언하고(안 제3조), 이 같은 정책을 구체화하기 위하여 표준개인정보처리방침의 사용 및 표시 제도(안 제7조), 개인정보보호단체 등의 등록 및 지원제도(안 제28조) 등을 도입하고 있으며, 개인정보 영향평가의 자율적 실시 및 개인정보보호 신뢰마크 활성화 등을 지원하기 위해 평가·인증기관 지정제도를 도입하고 있다(안 제52조). 또한 개인정보보호원칙의 통일적 집행을 위하여 개인정보의 수집·처리에 관한 기본원칙과 개인정보의 수집·처리와 관련하여 정보주체가 향유하는 기본적 권리를 천명하고(안 제5조 및 제22조), 주민등록번호 등 고유식별정보를 정보주체의 명시적인 동의 없이 해당 법령에서 의도한 고유 목적 이외의 용도로 수집·처리하지 못하도록 하였으며(안 제12조), CCTV, RFID, 전자우편감시시스템 등 각종 개인정보처리장치를 이용한 감시·추적으로부터 정보주체의 사생활 보호를 위하여 개인정보처리장치의 설치·운영에 관한 기준·절차·방법 등을 마련하였다(안 제14조). 그리고 개인정보를 이용하여 다른 사람의 선전·광고, 마케팅, 상품·서비스 판매, 회원가입 등을 대리·대행하거나 다른 사람에게 개인정보를 제공하는 사업을 하고자 하는 자는 보다 엄격한 동의 절차를 거치도록 하고 개인정보위원회에 등록하여 관리·감독을 받도록 하고(안 제17조), 개인정보의 누출·공개·도용에 따른 피해 확산을 방지하고 정보주체의 권리보호를 위하여 개인정보 누출 등의 사고 발생 시 정보주체에 대한 통지의무와 개인정보위원회에 대한 신고의무를 제도화하였으며(안 제20조), 공공부문과 민간부문의 차이를 명확히 하기 위하여 공공기관에 대해

서만 적용되는 특례 규정을 별도의 장으로 구분하여 규정하였다(안 제 4장). 공공기관의 개인정보처리에 대하여는 원칙적으로 법률유보주의를 채택하고(안 제30조), 공공기관의 개인정보 수집·처리를 투명하게 하기 위하여 개인정보파일 등록제(안 제31조)를 도입하였으며, 공공기관에 의한 개인정보 오남용 방지를 위해 개인정보 영향평가제(안 제32조) 및 개인정보파일의 연동·연계 심사제도(안 제33조)를 도입하였다.

한편, 개인정보보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리소속으로 개인정보위원회를 두도록 하였다(안 제34조). 개인정보에 관한 분쟁조정 업무를 신속하고 공정하게 처리하기 위하여 개인정보위원회에 개인정보분쟁조정위원회를 두고(제55조), 개인정보피해의 집단성·단체성을 반영하고 최근 소비자기본법의 개정 취지를 고려하여 개인정보피해에 대해서도 집단분쟁조정제도를 도입하였다(안 제60조).

② 다른 법률의 정비

『공공기관의 개인정보 보호에 관한 법률』을 폐지하고(안 부칙 제5조 제1항), 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』 중 제33조 내지 제40조 및 제67조를 각각 삭제하도록 하고 있다(안 부칙 제5조 제2항).

3. 각 법안의 비교 분석

(1) 각 법안의 구성

1) (구)이혜훈 법안

제 1 장 총칙 1. 목적 2. 정의 3. 다른 법률과의 관계 제 2 장 개인정보보호 일반원칙	제 1 절 개인정보의 수집과 처리 4. 개인정보의 처리원칙 5. 개인정보처리방침의 공개 6. 개인정보의 수집 및 처리 7. 민감정보의 수집 및 처리 8. 동의의 방법 등
--	---

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

<p>9. 목적의 이용 및 제공 금지</p> <p>10. 고유식별정보의 보호</p> <p>11. 개인정보파일의 구성 등</p> <p>12. 자동정보처리장치의 활용 제한</p> <p>13. 개인정보의 처리위탁</p> <p>14. 개인정보취급자에 대한 감독 등</p> <p>제 2 절 개인정보의 보호조치</p> <p>15. 안전조치의무</p> <p>16. 개인정보보호책임자의 지정</p> <p>17. 개인정보 누설금지</p> <p>제 3 장 정보주체의 권리보호</p> <p>18. 정보주체의 권리</p> <p>19. 개인정보의 열람·정정</p> <p>20. 개인정보의 이용·제공 정지</p> <p>21. 개인정보의 파기·삭제</p> <p>22. 이의제기절차 등</p> <p>23. 아동의 개인정보보호</p> <p>24. 손해배상책임</p> <p>제 4 장 공공부문에 대한 특칙</p> <p>25. 법률유보의 원칙</p> <p>26. 개인정보파일의 등록</p> <p>27. 개인정보사전영향평가</p> <p>28. 개인정보파일의 연동 등</p> <p>제 5 장 민간부문에 대한 특칙</p> <p>29. 개인정보의 수집 및 처리</p> <p>30. 영리목적의 개인정보 이용 및 제공</p> <p>31. 자율규제의 원칙</p> <p>32. 개인정보보호단체 등의 등록 및 지원</p> <p>33. 표준개인정보처리방침의 사용 및 표시</p> <p>제 6 장 개인정보위원회</p> <p>제 1 절 개인정보위원회의 구성</p> <p>34. 개인정보위원회의 설치</p> <p>35. 위원회의 구성</p> <p>36. 위원의 결격사유 및 신분보장</p> <p>37. 위원장</p> <p>38. 위원회의 의결</p> <p>39. 사무처의 설치</p>	<p>40. 위원회의 조직 및 운영</p> <p>제 2 절 위원회의 업무와 권한</p> <p>41. 위원회의 업무</p> <p>42. 의견제시</p> <p>43. 개선권고</p> <p>44. 자료제출 및 현황조회</p> <p>45. 방문조사</p> <p>46. 처리결과의 공개</p> <p>47. 시정명령 등</p> <p>48. 이의신청 및 집행정지</p> <p>49. 고발 및 징계권고</p> <p>50. 개인정보보호지침의 제정</p> <p>51. 관계기관의 장의 협조</p> <p>52. 개인정보영향평가·인증기관의 지정</p> <p>53. 평가·인증의 공정화</p> <p>54. 연차보고</p> <p>제 3 절 개인정보분쟁조정위원회</p> <p>55. 개인정보분쟁조정위원회의 설치</p> <p>56. 분쟁조정위원회의 구성</p> <p>57. 분쟁조정의 신청 등</p> <p>58. 조정의 효력</p> <p>59. 조정의 거부 및 중지</p> <p>60. 조정규칙 등</p> <p>61. 국가배상법과의 관계</p> <p>제 7 장 보 칙</p> <p>62. 적용제외</p> <p>63. 공무원 등의 파견</p> <p>64. 비밀준수의무</p> <p>65. 별칙적용에서의 공무원 의제</p> <p>66. 불이익금지</p> <p>67. 금지행위</p> <p>68. 국제협력</p> <p>69. 위임규정</p> <p>제 8 장 별 칙</p> <p>70. 별칙</p> <p>71. 별칙</p> <p>72. 양벌규정</p> <p>73. 과태료</p> <p>부칙</p>
--	---

2) 이은영 법안

<p>제 1 장 총 칙</p> <p>1. 목적</p> <p>2. 기본이념</p> <p>3. 정의</p> <p>4. 다른 법률과의 관계</p> <p>제 2 장 정보주체의 권리와 개인정보취급자의 의무</p> <p>5. 자기결정권</p> <p>6. 개인정보의 수집</p> <p>7. 민감정보의 특별관리</p> <p>8. 차별목적의 개인정보 수집 등의 금지</p> <p>9. 자동수집장치에 의한 수집 등</p> <p>10. 개인정보의 이용 및 제공</p> <p>11. 열람 및 정정청구권</p> <p>12. 개인정보의 삭제·과기 등</p> <p>13. 안전조치의무</p> <p>14. 개인정보누설금지</p> <p>15. 고유식별자의 보호</p> <p>16. 개인정보보호담당자의 지정</p> <p>17. 입증책임의 전환</p> <p>제 3 장 개인정보보호정책의 수립 등</p> <p>18. 국가 등의 책무</p> <p>19. 개인정보보호 시책의 수립</p> <p>20. 추진체계 등</p> <p>21. 국제협력</p> <p>22. 연차보고 등</p> <p>23. 기술개발 등</p> <p>제 4 장 개인정보보호위원회</p> <p>제1절 개인정보보호위원회의 설치 및 운영</p> <p>24. 개인정보보호위원회의 설치</p> <p>25. 위원회의 구성</p> <p>26. 위원장</p> <p>27. 위원의 결격사유 및 신분보장</p> <p>28. 분과위원회</p>	<p>29. 전문위원</p> <p>30. 위원회의 의결</p> <p>31. 사무처의 설치</p> <p>32. 개인정보침해신고센터</p> <p>33. 조직에 관한 규정 등</p> <p>제2절 위원회의 업무와 권한</p> <p>34. 위원회의 업무</p> <p>35. 의견의 제시 등</p> <p>36. 관계 행정기관의 장의 협조</p> <p>37. 자료제출 및 현황조회</p> <p>38. 방문조사</p> <p>39. 처리결과의 공개</p> <p>40. 시정명령 등</p> <p>41. 이의신청 및 집행정지</p> <p>42. 고발 및 징계권고</p> <p>제3절 개인정보분쟁조정위원회</p> <p>43. 개인정보분쟁조정위원회의 설치</p> <p>44. 분쟁조정위원회의 구성</p> <p>45. 분쟁조정의 신청 등</p> <p>46. 조정의 효력</p> <p>47. 조정의 거부 및 중지</p> <p>48. 조정규칙 등</p> <p>49. 국가배상법과의 관계</p> <p>제 5 장 보 칙</p> <p>50. 비밀유지 등</p> <p>51. 벌칙적용에서의 공무원 의제</p> <p>52. 위임규정</p> <p>제 6 장 벌 칙</p> <p>53. 벌칙</p> <p>54. 벌칙</p> <p>55. 양벌규정</p> <p>56. 과태료</p> <p>부 칙</p>
--	---

3) 노회찬 법안

<p>제 1 장 총칙</p> <p>1. 목적</p> <p>2. 용어의 정의</p> <p>3. 다른 법률과의 관계</p> <p>제 2 장 개인정보보호원칙</p> <p>4. 개인정보 보호원칙</p> <p>5. 개인정보의 수집 동의 등</p> <p>6. 개인정보의 수집의 제한 등</p> <p>7. 개인정보의 이용 및 제공 등</p> <p>8. 개인정보의 파기</p> <p>9. 개인정보의 갱신 등</p> <p>10. 동의의 철회</p> <p>11. 개인정보 열람 및 정정</p> <p>12. 개인정보의 열람제한</p> <p>13. 개인정보의 보호조치</p> <p>14. 개인정보 누설금지</p> <p>15. 고유식별자의 보호</p> <p>16. 개인정보의 익명처리</p> <p>제 3 장 개인정보보유자의 의무</p> <p>17. 아동의 보호</p> <p>18. 사업의 양도·양수 등</p> <p>19. 개인정보의 처리 위탁</p> <p>제 4 장 개인정보데이터베이스의 보호</p> <p>20. 개인정보 데이터베이스의 등록</p> <p>21. 개인정보보호책임자</p> <p>22. 정기감사</p> <p>제 5 장 개인정보데이터베이스의 결합 제한</p> <p>23. 개인정보 데이터베이스의 결합 제한</p> <p>24. 개인정보 데이터베이스 결합시 정보주체의 보호</p> <p>25. 개인정보보호위원회에 보고</p> <p>제 6 장 정보주체의 권리보호</p> <p>26. 공공기관이 보유한 개인정보의 처리정지 청구</p> <p>27. 처리정지 청구에 대한 조치</p>	<p>28. 손해배상</p> <p>29. 개인정보관련 집단소송</p> <p>30. 개인정보관련 집단소송의 소송대리인의 선임</p> <p>31. 개인정보관련 집단소송의 소의 제기 및 소송허가 신청</p> <p>32. 개인정보관련 집단소송의 소장의 기재사항</p> <p>33. 개인정보관련 집단소송의 소송허가 신청서의 기재사항 및 첨부서류</p> <p>34. 개인정보관련 집단소송의 소제기 사실의 공고 및 대표당사자의 선임</p> <p>35. 개인정보관련 집단소송의 소송허가 요건</p> <p>36. 개인정보관련 집단소송의 소송허가 절차</p> <p>37. 개인정보관련 집단소송 허가신청의 경합</p> <p>38. 개인정보관련 집단소송의 소송허가 결정</p> <p>39. 개인정보관련 집단소송의 소송불허가 결정</p> <p>40. 개인정보관련 집단소송의 소송허가결정의 고지</p> <p>41. 개인정보관련 집단소송의 복수의 대표당사자의 소송수행</p> <p>42. 공동피해자의 대표당사자 선임</p> <p>43. 개인정보관련 집단소송의 대표당사자의 소송수행금지</p> <p>44. 개인정보관련 집단소송의 대표당사자의 사임</p> <p>45. 개인정보관련 집단소송의 중단</p> <p>46. 개인정보관련 집단소송의 대표당사자 변경의 고지</p> <p>47. 개인정보관련 집단소송의 소송대리인의 사임 등</p> <p>48. 개인정보관련 집단소송의 공동피해자의 범위의 변경</p> <p>49. 개인정보관련 집단소송의 시효중단 효력소멸</p> <p>50. 공동피해자 및 대표당사자의 신문</p> <p>51. 개인정보관련 집단소송의</p>
---	--

<p>문서제출명령 등</p> <p>52. 개인정보관련 집단소송의 증거보전</p> <p>53. 직권에 의한 증거조사</p> <p>54. 개인정보관련 집단소송의 손해배상액의 산정</p> <p>55. 개인정보관련 집단소송의 소의 취하·화해 또는 청구포기의 제한</p> <p>56. 개인정보관련 집단소송의 판결서의 기재사항 등</p> <p>57. 개인정보관련 집단소송의 기관력의 주관적 범위</p> <p>58. 개인정보관련 집단소송의 상소취하·상소권포기의 제한</p> <p>59. 대법원규칙</p> <p>제 7 장 개인정보보호위원회</p> <p>제1절 개인정보보호위원회의 구성</p> <p>60. 개인정보보호위원회</p> <p>61. 위원회의 구성</p> <p>62. 위원장의 직무</p> <p>63. 위원장 및 위원의 임기</p> <p>64. 위원의 신분보장</p> <p>65. 위원의 결격사유</p> <p>66. 소위원회</p> <p>67. 회의 의사 및 의결정족수</p> <p>68. 의사의 공개</p> <p>69. 자문기구</p> <p>70. 사무처</p> <p>71. 징계위원회의 설치</p> <p>72. 지역 개인정보보호위원회</p> <p>73. 위원회의 조직과 운영</p> <p>제 2 절 개인정보보호위원회의 업무</p> <p>74. 위원회의 업무</p> <p>75. 국가기관의 협의의무 등</p> <p>76. 규정의 제정</p> <p>77. 자료제출 및 사실조회</p> <p>78. 청문회</p> <p>79. 정책 및 관행의 개선 또는 시정권고</p> <p>80. 개인정보보호 교육과 홍보</p> <p>81. 법원 및 헌법재판소에 대한 의견제출</p>	<p>82. 보고서 작성 등</p> <p>제 3 절 개인정보침해에 대한 조사와 피해구제</p> <p>83. 진정 및 조사 등</p> <p>84. 수사기관과 위원회의 협조</p> <p>85. 조사의 방법</p> <p>86. 질문·검사권</p> <p>87. 위원의 제척 등</p> <p>88. 진정의 각하와 기각</p> <p>89. 합의의 권고</p> <p>90. 결정</p> <p>91. 고발 및 징계권고</p> <p>92. 의견진술기회의 부여</p> <p>93. 긴급구제조치</p> <p>94. 불이익 금지 등</p> <p>제 8 장 개인정보 사전영향평가</p> <p>95. 개인정보 사전영향평가의 실시</p> <p>96. 평가의 기준</p> <p>97. 의견수렴</p> <p>98. 평가결과의 활용</p> <p>99. 국가 예산편성과 영향평가</p> <p>제 9 장 보칙</p> <p>100. 자격사칭의 금지</p> <p>101. 비밀누설의 금지</p> <p>102. 유사명칭사용의 금지</p> <p>103. 공무원 등의 파견</p> <p>104. 불이익금지와 지원</p> <p>제10장 벌칙</p> <p>105. 벌칙</p> <p>106. 자격사칭</p> <p>107. 긴급구제조치방해</p> <p>108. 과태료</p> <p>109. 양벌규정</p> <p>110. 벌칙적용에 있어서의 공무원 의제</p> <p>부 칙</p>
--	---

4) 행정안전부 법안

<p>제 1 장 총칙</p> <p>1. 목적</p> <p>2. 정의</p> <p>3. 개인정보보호원칙</p> <p>4. 정보주체의 권리</p> <p>5. 국가 등의 책무</p> <p>6. 다른 법률과의 관계</p> <p>제 2 장 개인정보보호정책의 수립 등</p> <p>7. 기본계획의 수립 등</p> <p>8. 시행계획의 수립</p> <p>9. 개인정보보호위원회</p> <p>10. 보호위원회의 기능 등</p> <p>11. 실태조사</p> <p>12. 개인정보보호지침</p> <p>13. 자율규제의 촉진</p> <p>14. 국제협력</p> <p>제 3 장 개인정보의 처리</p> <p>제 1 절 개인정보의 수집, 이용, 제공 등</p> <p>15. 개인정보의 수집·이용</p> <p>16. 개인정보의 수집 제한</p> <p>17. 개인정보의 제공</p> <p>18. 개인정보의 이용·제공 제한</p> <p>19. 개인정보를 제공받은 자의 이용·제공 제한</p> <p>20. 개인정보의 파기</p> <p>21. 동의를 받는 방법</p> <p>제 2 절 개인정보의 처리 제한</p> <p>22. 민감정보의 처리 제한</p> <p>23. 고유식별정보의 처리 제한</p> <p>24. 영상정보처리기기의 설치·운영 제한</p> <p>25. 업무위탁에 따른 개인정보의 처리 제한</p> <p>26. 영업양도 등에 따른 개인정보의 이전 제한</p> <p>제 4 장 개인정보의 안전한 관리</p>	<p>27. 안전조치의무</p> <p>28. 개인정보처리방침의 수립 및 공개</p> <p>29. 개인정보관리책임자의 지정</p> <p>30. 개인정보파일의 등록 및 공개</p> <p>31. 개인정보 영향평가</p> <p>32. 개인정보 유출 통지</p> <p>제 5 장 정보주체의 권리 보장</p> <p>33. 개인정보의 열람</p> <p>34. 개인정보의 정정·삭제</p> <p>35. 권리행사방법 및 절차 등</p> <p>36. 손해배상책임</p> <p>제 6 장 개인정보분쟁조정위원회</p> <p>37. 설치 및 구성</p> <p>38. 위원의 신분보장</p> <p>39. 위원의 제척·기피·회피</p> <p>40. 조정의 신청 등</p> <p>41. 처리기간</p> <p>42. 자료의 요청 등</p> <p>43. 조정전 합의</p> <p>44. 분쟁의 조정</p> <p>45. 조정의 거부 및 중지</p> <p>46. 조정절차 등</p> <p>제 7 장 보 칙</p> <p>47. 적용의 일부제외</p> <p>48. 금지행위</p> <p>49. 비밀유지 등</p> <p>50. 의견제시 및 개선권고</p> <p>51. 침해사실의 신고 등</p> <p>52. 자료제출요구 및 검사</p> <p>53. 시정조치 등</p> <p>54. 고발 및 징계권고</p> <p>55. 결과의 공표</p> <p>56. 권한의 위임·위탁</p> <p>57. 벌칙적용에 있어서의 공무원 의제</p> <p>제 8 장 벌 칙</p> <p>58. 벌칙</p> <p>59. 벌칙</p>
--	--

60. 벌칙	63. 과태료
61. 벌칙	
62. 양벌규정	부 칙

5) (신)이혜훈 법안

<p>제 1 장 총 칙</p> <p>1. 목적</p> <p>2. 정의</p> <p>3. 자율규제의 원칙</p> <p>4. 다른 법률과의 관계</p> <p>제 2 장 개인정보보호 일반원칙</p> <p>제1절 개인정보의 수집과 처리</p> <p>5. 개인정보의 수집·처리원칙</p> <p>6. 개인정보처리방침의 공개</p> <p>7. 표준개인정보처리방침의 사용 및 표시</p> <p>8. 개인정보의 수집 및 처리</p> <p>9. 민감정보의 수집 및 처리</p> <p>10. 동의의 방법 등</p> <p>11. 목적외 이용 및 제공 금지</p> <p>12. 고유식별정보의 보호</p> <p>13. 개인정보파일의 설계 및 구축</p> <p>14. 개인정보수집장치의 이용 제한</p> <p>15. 개인정보의 처리위탁</p> <p>16. 개인정보취급자에 대한 감독 등</p> <p>17. 영리목적의 개인정보 이용 및 제공</p> <p>제 2 절 개인정보의 보호조치</p> <p>18. 안전조치의무</p> <p>19. 개인정보보호책임자의 지정</p> <p>20. 개인정보 누출등의 통지 및 신고</p> <p>21. 개인정보 누설금지</p> <p>제 3 장 정보주체의 권리보장</p> <p>22. 정보주체의 권리</p> <p>23. 개인정보의 열람·정정</p> <p>24. 개인정보의 이용·제공 정지</p> <p>25. 개인정보의 파기·삭제</p> <p>26. 권리행사의 방법등</p> <p>27. 아동의 개인정보보호</p>	<p>28. 개인정보보호단체 등의 등록 및 지원</p> <p>29. 손해배상책임</p> <p>제 4 장 공공기관에 대한 특칙</p> <p>30. 법률유보의 원칙</p> <p>31. 개인정보파일의 등록</p> <p>32. 개인정보영향평가</p> <p>33. 개인정보파일의 연동 등</p> <p>제 5 장 개인정보위원회</p> <p>제1절 개인정보위원회의 구성</p> <p>34. 개인정보위원회의 설치</p> <p>35. 위원회의 구성</p> <p>36. 위원의 결격사유 및 신분보장</p> <p>37. 위원장</p> <p>38. 위원회의 의결</p> <p>39. 사무처의 설치</p> <p>40. 위원회의 조직 및 운영</p> <p>제 2 절 위원회의 업무와 권한</p> <p>41. 위원회의 업무</p> <p>42. 의견제시</p> <p>43. 개선권고</p> <p>44. 자료제출 및 실태조사</p> <p>45. 방문조사</p> <p>46. 처리결과의 공개</p> <p>47. 시정명령 등</p> <p>48. 이의신청 및 집행정지</p> <p>49. 고발 및 징계권고</p> <p>50. 개인정보보호기준의 제정</p> <p>51. 관계기관의 장의 협조</p> <p>52. 개인정보영향평가·인증기관의 지정</p> <p>53. 평가·인증의 공정화</p> <p>54. 연차보고</p>
--	--

제3절 개인정보분쟁조정위원회 55. 개인정보분쟁조정위원회의 설치 56. 조정위원회의 구성 57. 조정의 개시 등 58. 조정의 효력 등 59. 조정의 거부 및 중지 60. 집단분쟁조정 61. 『민사조정법』의 준용	65. 벌칙적용에서의 공무원 의제 66. 불이익금지 67. 금지행위 68. 국제협력 69. 위임규정
제 6 장 보 칙 62. 적용제외 63. 공무원 등의 파견 64. 비밀준수의무	제 7 장 벌 칙 70. 벌칙 71. 벌칙 72. 양벌규정 73. 과태료 부 칙

(2) 입법체계의 분석

1) 명 칭

	(구)이혜훈 법안	이은영 법안	노회찬 법안	행정안전부 법안	(신)이혜훈 법안
법률 명칭	개인정보보 호법	개인정보보호법	개인정보 보호기본법	개인정보 보호법	개인정보 보호법

노회찬 법안을 빼고는 모두 『개인정보보호법』이라는 명칭을 사용하고 있다. 다만, 노회찬 법안에서는 유일하게도 『개인정보보호기본법』이라는 명칭을 사용하고 있다. 하지만 전술한 바와 같이 노회찬 법안에서 사용된 ‘기본법’이라는 표현은 개인정보보호에 관한 기본적 사항을 정한다기보다 개인정보보호에 관한 일반적인 사항을 모두 망라적으로 규정함으로써 개인정보보호에 있어서 중추적 역할을 하는 입법이 될 수 있도록 하기 위한 의도를 드러내는 것으로 이해할 수 있다.

2) 구 성

모든 법안은 아래의 표에서 보는 바와 같이 공통적으로 총칙, 개인정보보호에 관한 일반사항, 개인정보(보호)위원회, 보칙, 벌칙, 부칙 등

으로 구성되어 있다. 총칙에서는 각각 목적, 정의, 다른 법률과의 관계가 규정되어 있다. 하지만 이은영 법안에서는 그에 더하여 기본이념을 제시하고 있는 점이 특이하다. 그리고 개인정보보호에 관한 일반사항에서는 개인정보보호의 일반원칙, 정보주체의 권리보호, 개인정보보유자의 의무 등이 규정되어 있다. 여기서 주목할 만한 것은 (구)이혜훈 법안에서 공공부문 및 민간부문에 대한 특칙을 각각 규정하였다는 점이다. 그리고 노회찬 법안에서는 개인정보데이터베이스의 보호 및 그 결합의 제한, 개인정보 사전영향평가 등을 별도의 장으로 규정하고 있는 점에서 특징적이다.

구분	(구)이혜훈법안	이은영법안	노회찬법안
법안 구성	제 1 장 총칙 제 2 장 개인정보보호 일반원칙 제 1 절 개인정보의 수집과 처리 제 2 절 개인정보의 보호조치 제 3 장 정보주체의 권리보호 제 4 장 공공부문에 대한 특칙 제 5 장 민간부문에 대한 특칙 제 6 장 개인정보위원회 제 1 절 개인정보위원회의 구성 제 2 절 위원회의 업무와 권한 제 3 절 개인정보분쟁조정위원회 제 7 장 보칙 제 8 장 벌칙 부 칙	제 1 장 총칙 제 2 장 정보주체의 권리와 개인정보취급자의 의무 제 3 장 개인정보보호 정책의 수립 등 제 4 장 개인정보보호위원회 제 1 절 개인정보보호위원회의 설치 및 운영 제 2 절 위원회의 업무와 권한 제 3 절 개인정보분쟁조정위원회 제 5 장 보칙 제 6 장 벌칙 부 칙	제 1 장 총칙 제 2 장 개인정보보호원칙 제 3 장 개인정보보유자의 의무 제 4 장 개인정보데이터베이스의 보호 제 5 장 개인정보데이터베이스의 결합 제한 제 6 장 정보주체의 권리보호 제 7 장 개인정보보호위원회 제 1 절 개인정보보호위원회의 구성 제 2 절 개인정보보호위원회의 업무 제 3 절 개인정보침해에 대한 조사와 피해구제 제 8 장 개인정보 사전영향평가 제 9 장 보칙 제 10 장 벌칙 부 칙

제 3 편 개인정보보호의 입법체계에 관한 병행적 입법평가

구분	행정안전부 법안	(신)이혜훈법안
법안 구성	제 1 장 총칙 제 2 장 개인정보보호정책의 수립 등 제 3 장 개인정보의 처리 제 1 절 개인정보의 수집, 이용, 제공 등 제 2 절 개인정보의 처리 제한 제 4 장 개인정보의 안전한 관리 제 5 장 정보주체의 권리 보장 제 6 장 개인정보분쟁조정위원회 제 7 장 보칙 제 8 장 벌칙 부 칙	제 1 장 총칙 제 2 장 개인정보보호 일반원칙 제 1 절 개인정보의 수집과 처리 제 2 절 개인정보의 보호조치 제 3 장 정보주체의 권리보장 제 4 장 공공기관에 대한 특칙 제 5 장 개인정보위원회 제 1 절 개인정보위원회의 구성 제 2 절 위원회의 업무와 권한 제 3 절 개인정보분쟁조정위원회 제 6 장 보칙 제 7 장 벌칙 부칙

3) 적용범위

① 각 법안

	(구)이혜훈 법안	이은영 법안	노회찬 법안
적용 대상	· 업무 목적으로 개인정보를 처리하는 자(공공·민간 불문) (제2조 제6호)	· 업무상 개인정보를 수집하여 이를 처리, 이용하는 자(공공·민간 불문) (제3조 제3호)	· 개인정보 처리 업무에 종사하는 자(공공·민간 불문) (제21조)
적용 제외	① 단순히 개인 또는 가족의 이용을 목적으로 개인정보를 처리하는 경우, ② 정보주체에게 미칠 급박한 생명·신체·재산상의 위험을 예방하기 위하여 부득이하게 개인정보를 처리하는 경우, ③ 통계, 연구 기타 이와 유사한 목적을 위하여 특정 개인을 식별할 수 없는 형태(과다한 비용과 노력을 들이지 않고는 식별이 어려운 경우도 포함한다)로 개인정보를 처리하는 경우, ④ 언론·출판기관, 종교단체, 정당 등이 고유의 활동을 목적으로 개인정보를 처리하는 경우(제62조 제1항)		

	행정안전부 법안	(신)이혜훈 법안
적용 대상	· 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 타인을 통하여 개인정보를 처리하는 자(공공·민간 불문)	· 업무를 목적으로 스스로 또는 다른 사람을 통하여 개인정보를 수집 또는 처리하는 자(공공·민간 불문)
적용 배제	① 국가안전보장, 공공질서유지, 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 개인정보를 처리하는 경우, ② 전쟁·테러 등 국제분쟁의 해결을 위하여 불가피하게 필요한 경우로서 일시적으로 개인정보를 처리하는 경우, ③ 언론, 종교단체, 정당이 취재·보도목적, 종교활동, 정당활동의 고유 목적을 위하여 개인정보를 처리하는 경우(제47조 제1항) 단, 영상정보처리기기 운영자인 경우, 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 일부 규정의 적용을 배제(제47조 제2항 및 제3항)	① 단순히 개인 또는 가족의 이용을 목적으로 개인정보를 수집·처리하는 경우, ② 통계, 연구 그 밖에 이와 유사한 목적을 위하여 특정 개인을 식별할 수 없는 형태(과다한 비용과 노력을 들이지 않고는 식별이 어려운 경우도 포함한다)로 개인정보를 수집·처리한 경우(제62조 제1항) 단, 종교 및 선교 활동, 정당 및 정치활동, 취재 및 보도 등을 목적으로 개인정보를 수집·처리하는 경우에는 일부 규정의 적용을 배제(제62조 제2항)

② 검토

다섯 법안은 약간의 표현만 다를 뿐이지, 모두 개인정보의 처리를 업무로 하는 자를 적용대상으로 삼고 있으며, 공공부문과 민간부문을 불문한다는 점에서 차이가 없다. 이러한 점에서 모든 법안이 통합형 입법주의를 채택하고 있다고 할 수 있다. 한편, 동법의 적용이 전면적으로 배제되는 경우로 (구)이혜훈법안에서는 4가지가 제시되었으나, (신)이혜훈법안에서는 2가지로 줄어들었다. 한편, 행정안전부 법안에서는 적용배제의 사유로 3가지를 들고 있다. 하지만 나머지 법안에서는

그러한 적용배제의 사유를 인정하지 않고 있다. 이러한 점에서 법안의 적용범위가 가장 넓은 것은 이은영법안과 노회찬법안이라 할 수 있고, 가장 좁은 것은 (구)이혜훈법안이었다고 할 수 있다. 제18대 국회에서 제출된 (신)이혜훈법안과 행정안전부 법안 가운데는 전자가 더 적용범위가 넓다고 볼 수 있을 것이다. 이에 반비례하여 개인정보보호 범위의 광협을 논할 수 있을 것으로 본다.

4) 평 가

지금까지 살펴본 다섯 가지 법안을 입법체계상 특징을 중심으로 살펴볼 때, 모든 법안은 통합형 입법주의를 취하면서도, 내용적으로는 일반법주의를 택하고 있다고 판단된다. 모든 법안이 공통적으로 개인정보보호에 관한 일반사항, 정보주체의 권리, 구제절차, 개인정보보호 기구, 벌칙 등을 포함하고 있기 때문이다.

제 4 절 입법체계론의 내용과 평가

1. 서 언

Wolfgang Hoffmann-Riem은 개인정보보호법의 발전과 그로 인한 법제의 산발적 형성이 초래하는 문제점에 대해 예리한 지적을 하고 있다. 즉, 지금까지 개인정보보호를 위한 법적 규율은 과거 법적으로 형성되지 않은 생활영역뿐만 아니라, 이미 일반화되기는 하였으나 종래에는 개인정보보호법제에 의해 포섭되지 않았던 사회적 관계에까지 확대되어 왔다. 게다가 대체로 특수한 영역을 규율하는 개별법상의 복잡한 규제프로그램은 상위의 법규범이나 일반적인 개인정보보호법상의 조항과의 관계에서 경합을 벌이고 있다. 또한 복잡화된 시행규정, 혼재되어 있는 위임, 다양한 분야별 규율 그리고 공공연히 형성된 재량권 등으로 인하여 그 적용의 실태가 매우 복잡한 양상으로 나타

나고 있다. 이로 인하여 오늘날 개인정보보호법은 전문가에게조차도 더 이상 해석하여 적용하기가 쉽지 않게 되었다. 무엇보다도 법률문 외한인 일반 수범자들에 대해 법적 정보를 제공하고 행위의 방향을 설정해주는 기능을 상실해가고 있다. 이는 뜻밖에도 다수의 개인정보 보호 관련 법제 사이에 존재하는 공백이나 모순에서 비롯되는 경우가 많다. 바로 ‘규범의 홍수(Normenflut)’가 법적 보호의 불완전성을 야기한다고 할 수 있다. 이는 집행력의 결여에 영향을 받는 신뢰가치의 문제나 보호체계적 완결성의 상실을 가져와 개인정보의 보호라는 이념의 성과는 법을 통한 개인정보보호의 실패를 낳을 우려도 있다.⁵⁶⁴⁾

굳이 이러한 지적이 아니더라도 우리나라에서는 공공부문과 민간부문을 통합적으로 규율하는 기본법 내지 일반법이 존재하지 않아서 발생하는 법적 보호의 공백을 해소하기 위한 법률안이 여러 차례 제출된 바 있다. 그리고 분야별로 이미 다수의 개인정보보호 관련 법제가 산재해 있지만, 그 법률에 개인정보의 침해적 측면과 보호적 측면이 혼재되어 있어서 집행기구의 법적 혼동을 초래하고 모순적인 법적 효과를 낳는 경우도 적지 않다.

다수의 개인정보보호 관련 규정이 있지만, 그를 통해 다양한 개인정보의 침해에 충분히 대응하기에 어려움이 많은 것도 사실이다. 그렇다고 하여 개인정보침해의 양상이 새롭게 전개될 때마다 번번이 관련 법률의 제정에 나설 수도 없는 노릇이다. 이러한 점에서 개인정보보호법에 있어서 입법체계를 어떻게 설정하는 것이 위와 같은 문제점을 최소화할 수 있는 방안인지 면밀히 검토해볼 필요가 있다고 본다. 개인정보보호정책의 성공을 제도적으로 뒷받침하기 위해서는 관련 입법의 체계를 최적화하려면, 법적 규율의 효율성이나 비용적 측면이 중

564) Wolfgang Hoffmann-Riem, “Informationelle Selbstbestimmung in der Informationsgesellschaft-Auf dem Wege zu einem neuen Konzept des Datenschutzes-”, *AöR*, Band 123, 1998, SS. 513-514.

요하게 고려되어야 할 것이다. 하지만 이에 못지않게 수범자의 규범에 대한 친속도를 제고하고, 관련되는 여러 가치나 해당 규범간의 충돌을 해결하고 데도 초점이 맞추어져야 할 것이다.

2. 입법체계의 분석틀

각국의 개인정보보호법제를 입법체계에 초점을 맞추어 비교분석함에 있어서, 입법체계에 관한 용례를 분석하는 작업이 선행되어야 할 것으로 본다. 왜냐하면 일반적으로 개인정보보호법제의 입법체계와 관련하여 통합형 입법주의(일원주의)와 분리형 입법주의(이원주의), 혹은 기본법, 일반법, 개별법 등의 표현이 많이 사용되고 있으나, 논자에 따라서 그 쓰임새가 약간씩 달라서 정확히 의미하는 바를 파악하기 어려운 점이 있기 때문이다. 이와 같은 문제점은 실제로 개인정보보호법제의 입법체계를 분석함에 있어서도 많은 혼란을 야기하고 있는 것으로 판단된다.

그러면 이하에서는 우선 개인정보보호법제에 있어서 통합형 입법주의와 분리형 입법주의의 쓰임새가 어떠한지 설명한 다음, 이어서 기본법과 일반법의 일반적 용례는 어떠한지 살펴본다. 그리고 이에 기초하여 향후 관련 법제의 입법체계를 분석하는 과정에서 기본법의 입법체계와 일반법의 입법체계를 각각 어떠한 의미로 사용할 것인지에 대해 정리하기로 한다.

(1) 통합형 입법주의와 분리형 입법주의

개인정보보호법제가 공공부문과 민간부문을 달리하여 규율하는 입법의 체계의 유형을 띠고 있는지, 통합적으로 규율하는 입법체계에 입각하고 있는지에 따라 입법체계를 통합형 입법주의와 분리형 입법주의로 나눌 수 있다.

우선 ‘통합형’ 입법주의는 공공부문과 민간부문을 하나의 법률을 통해 포괄적으로 규율하는 입법의 형태를 취하고 있는 것으로, 이러한 입법태도를 ‘일원주의’라고도 할 수 있을 것이다.

다음으로 ‘분리형’ 입법주의는 공공부문과 민간부문을 구분하여 각기 별개의 법률에 의해 규율하는 입법의 형태를 택하고 있는 것으로, 이러한 입법태도를 ‘이원주의’라고도 할 수 있을 것이다.

(2) 기본법의 체계와 일반법의 체계

일반적으로 법률용어상 ‘일반법’은 ‘특별법’과 대응되는 것이고, ‘기본법’은 ‘개별법’에 대응되는 것으로 이해되고 있다. 하지만 ‘기본법’과 ‘일반법’의 개념이 실제의 용례에 있어서 뚜렷한 기준이 없이 편의에 따라 사용되고 있을 뿐만 아니라, 심지어는 우리 법률의 공식명칭에서도 그 쓰임새가 일정치 않음을 볼 수 있다.

1) 일반법과 특별법

통상적으로 특별법은 특정의 사람·사물·행위 또는 지역에 국한하여 적용되는 법을 의미하는 데 반하여, 일반법은 그러한 제한이 없이 일반적으로 적용되는 법을 말한다. 그러나 양자의 관계는 상대적인 것으로, 예컨대 사법에 있어서 가장 일반적인 법인 민법에 대하여 상사(商事)만에 관하는 상법은 특별법이라고 할 수 있으나, 담보부사채 신탁법은 일반법인 상법에 대하여는 특별법이 된다. 원래 특별법은 정의 또는 형평의 관념에 입각하여 일반법 중에서 특수한 사항을 골라내어, 그것을 특별히 취급하려고 하는 취지에서 나온 것이다. 그러므로 특별법은 일반법에 우선하는 것이 원칙이며, 일반법은 특별법에 규정이 없는 경우에만 보충적으로 적용된다(상법 1조 참조). 이러한 두 개념을 구별하는 실익은 법의 효력 및 적용의 순서를 명확히 하는

데에 있다고 할 수 있다.

2) 기본법의 유형

우리나라의 현행법령에서 ‘기본법’이라는 명칭이 붙은 법률은 2008년 9월 현재 50종이 있는 것으로 파악된다.⁵⁶⁵⁾ 이들을 입법체계상의 특징을 기준으로 분류할 때 ‘기본법’에는 다양한 유형이 존재하는 것으로 파악된다. 하지만 크게 분류를 해보면 대략 다음과 같은 3가지의 유형으로 나누어볼 수 있을 것이다.

첫째, 당해 분야에서 국가의 기본적인 정책방향이나 계획수립의 근거로서 기능하는 기본법이 있다. 여기서는 주로 기본이념, 정의, 국가 및 지방자치단체의 책무, 기본계획의 수립, 기본적 사업, 추진기관 등에 관한 규정을 두고 있으나, 구체적인 행정권한이나 관련자의 권리, 피해구제의 수단 등에 관한 내용은 일반적으로 포함하고 있지 않다. 이러한 기본법은 개별적인 영역의 교육 관련법에 대한 하나의 해석지침으로서 기능할 수 있다.

이러한 유형에 속하는 대표적인 법률로는 『교육기본법』을 들 수 있는데, 여기서는 교육영역에서의 기본이념과 추구하는 가치와 그 실현을 위한 국가·지방자치단체의 책임을 추상적으로 선언하고, 나아가

565) 법제처 종합법령정보센터(<http://klaw.go.kr/>)의 법령정보검색을 통해 조사한 결과, 2008년 9월 19일 현재 ‘기본법’이라는 명칭을 쓰고 있는 법률로는 건강가정기본법, 건강검진기본법, 건설산업기본법, 건축기본법, 고용정책기본법, 과학기술기본법, 관광기본법, 교육기본법, 국가보훈기본법, 국가표준기본법, 국세기본법, 국어기본법, 국토기본법, 군인복지기본법, 근로자복지기본법, 농업·농촌 및 식품산업 기본법, 문화산업진흥 기본법, 물류정책기본법, 민방위기본법, 보건의료기본법, 부담금관리 기본법, 사회보장기본법, 산림기본법, 소방기본법, 소비자기본법, 식품안전기본법, 에너지기본법, 여성발전기본법, 영상진흥기본법, 인적자원개발 기본법, 자격기본법, 자원봉사활동 기본법, 재난 및 안전관리기본법, 재한외국인 처우 기본법, 저출산·고령사회기본법, 전기통신기본법, 전자거래기본법, 정보화촉진기본법, 정부업무평가 기본법, 중소기업기본법, 지방자치단체 기금관리기본법, 지속가능발전 기본법, 진실·화해를 위한 과거사정리 기본법, 철도산업발전기본법, 청소년기본법, 토지이용규제 기본법, 해양수산발전기본법, 행정규제기본법, 행정조사기본법, 환경정책기본법 등 50개가 있는 것으로 파악되었다.

교육제도와 그 운영에 관한 기본적 사항을 규정하고 있다. 이 밖에도 「국어기본법」, 「건강가정기본법」, 「건축기본법」, 「산림기본법」, 정부업무 등의 평가에 관한 기본법, 「자원봉사활동 기본법」, 「자격기본법」 등도 이러한 유형에 해당한다고 볼 수 있을 것이다.

둘째, 당해 분야의 각 개별입법에서 공통적으로 적용될 수 있는 기본적인 사항이나 기본적인 권리, 공통적인 권리구제절차나 권리구제기관의 설립 등에 관하여 규정하기 위한 법률로서의 기본법이 있다. 여기서는 대체로 구체적인 행정권한의 수권이나 집행에 관한 조항은 원칙적으로 포함하지 않는다.

대표적으로 국세에 관한 기본적인 사항 및 공통적인 사항과 위법 또는 부당한 국세처분에 대한 불복절차를 규정하고 있는 「국세기본법」이 여기에 속한다고 볼 수 있을 것이다. 그 밖에도 「사회보장기본법」, 「소방기본법」, 「전자거래기본법」, 「행정조사기본법」, 「행정규제기본법」 등이 이 유형에 속하는 예라고 할 수 있을 것이다.

셋째, 사실상 일반법의 기능을 수행하는 기본법이 있다. 당해 분야를 일반적으로 규율하기 위하여 행정권한을 수권하고, 그 위반에 대해 행정제재나 형사제재를 규정하는 등 집행법제의 내용을 담고 있다. 물론 이 유형의 기본법에서는 국가의 정책방향이나 계획수립의 근거조항 또는 조직설립의 근거조항 등이 함께 포함될 수 있다.

대표적인 예로는, 소비자의 권리와 책무, 한국소비자원, 소비자안전, 소비자안전센터의 설치, 소비자분쟁의 해결절차, 벌칙 등은 물론이고, 물품등의 자진수거 등, 수거·과기 등의 권고 및 명령, 소비자단체소송 등에 대해서까지 규정하고 있는 「소비자기본법」을 들 수 있겠다. 이것 말고도 「청소년기본법」, 「환경정책기본법」, 「진실·화해를 위한 과거사정리 기본법」, 「보건의료기본법」, 「건설산업기본법」 등이 이 유형에 해당하는 것으로 판단된다.

그러나 이 유형의 기본법은 ‘기본법’이라기보다는 ‘일반법’의 성격을 더 강하게 띠다고 할 수 있다. 여기서 ‘기본법’이라는 명칭을 사용하고 있는 것은 공연히 오해를 낳을 수 있어서 바람직하다고 보기 어렵다고 하겠다.⁵⁶⁶⁾

3) 용어의 정리

일반적으로 일반법은 특별법과, 기본법은 개별법과 각각 대립되는 개념으로 분류된다. 이렇게 볼 때 일반법과 기본법은 동일한 평면에서 서로 구분되는 것이 아니라, 서로 차원을 달리하는 존재양식이라고 할 수 있다. 따라서 기본법이면서 일반법인 경우도 있고, 개별법이면서도 일반법인 경우가 있을 수 있다. 또한 ‘기본법’의 용례 또한 우리의 실정법상 공식명칭에서도 볼 수 있듯이 매우 다양한 유형이 있는 것으로 분석된다. 이러한 상황에서 각 용어가 포섭할 수 있는 범위를 구획함에 있어서 어느 것이 딱히 정답이라고 내세울 것을 기대하기는 어렵다고 판단된다. 요컨대 ‘기본법’과 ‘일반법’의 틀을 가지고 입법의 체계를 논의한다는 것은 적절치 않을 수 있다.

하지만 개인정보보호법제에 있어서 입법체계와 관련하여 한 동안 기본법과 일반법의 용어가 구분되어 사용되어 왔으므로, 이러한 용어를 무시하고 관련법제의 입법체계를 논의할 경우 그간의 논의를 충분히 수렴하기 어려운 측면이 있다. 이에 본 연구에서 우리리가 사용하고자 하는 양자의 의미에 대해 일정한 기준을 세움으로써, 향후의 논의에서 일관된 흐름을 이어갈 수 있도록 할 필요가 있다.

생각건대 기본법과 일반법의 차이는 규율사항의 밀도, 구체성, 실천성 등에서 찾아야 할 것으로 본다. 즉, 기본적 이념과 원칙, 개념의 정의 등과 같은 기본적 사항만 규율하고 있는 수준이면 ‘기본법’이고, 거기서 더 나아가 구체적인 권리나 의무 등 실제적인 사항 또는 그

566) 이인호 외, 『개인의 사생활, 국가적 감시, 그리고 규범』 (정보통신정책연구원, 2006), 79면.

실현을 위한 구체적인 절차적 사항까지 다루고 있으면 ‘일반법’이라고 할 수 있다. 가령 민법의 예를 들어보면 여기에는 총칙규정은 물론, 물권, 채권, 친족, 상속 등 개별적 분야에 대해 함께 규정하고 있는바, 이를 민사관계에 관한 ‘기본법’이라고 하기보다는 ‘일반법’으로서의 지위를 부여하는 것이 자연스러울 것이다. 하지만 민법상의 임대차나 소비대차에 대한 특별한 규율을 내용으로 하는 주택임대차보호법이나 이자제한법 등은 특별민법에 해당한다고 보아야 할 것이다. 한편, 민법에 대한 특별법으로 이해되고 있는 상법에서도 역시 회사법, 어음법, 수표법, 보험법, 해상법 등 개별적 영역에 관한 규율도 함께 이루어지고 있으므로, 상법을 상거래에 관한 ‘기본법’의 범주를 넘어선다고 할 수 있다. 이러한 관점에서 볼 때 여기서 ‘기본법’은 개인정보보호에 관한 정책방향이나 개인정보보호에 관한 기본원칙, 집행체계 등과 같은 기본적 사항을 중심으로 규율하고 기타 구체적인 권리와 의무 등에 관한 사항들은 개별법에서 별도로 규율하도록 하는 경우를 말하고, ‘일반법’은 특별한 법률의 규정이 없는 경우에 보충적으로 적용될 수 있도록 개인정보보호를 위한 기본적인 사항 이외에도 각종의 권리와 의무 등에 관한 실체적 사항 및 그 실현을 위한 절차적 사항까지 빠짐없이 규율하는 경우를 지칭한다.⁵⁶⁷⁾ 그리고 ‘개별법’은 분야별로 취급되는 개인정보의 특수성을 고려하여 특별한 보호의 기준이나 의무사항 등을 설정한 규정을 둔 경우를 의미하는 것으로 본다.

3. 입법체계론의 전개

(1) 논의의 방향

우리나라의 현행 법률체계는 공공부문과 민간부문이 분리된 이원적 일반법과 다수의 개별법이 존재하므로 이원적 개별법주의에 가깝다고

567) 이에 관한 자세한 논의는 권현영, “전자정부개인정보쟁점”, 『정보화정책』 (2004), 71-72면을 참조할 것.

할 수 있다. 하지만 각 부문의 일반법도 보호대상의 개인정보가 제한적이라는 특징을 가지고 있다. 이러한 입법체계는 전술한 바와 같이 수범자의 혼란을 발생시키고, 보호체계상의 불균형을 유발하며, 법적 보호의 공백을 야기하는 등의 문제를 낳고 있다.

이처럼 현행의 입법체계로서는 고도정보사회에서 개인정보처리의 이익과 필요를 수용하면서도 그 위험성으로부터 개인의 존엄과 자기결정권을 보호하기에 역부족이라는 점에 대해서는 학계와 시민단체, 그리고 정부에서도 거의 일치된 견해를 보이고 있는 것으로 보인다. 또한 세계적으로는 민간부문에서 종래의 자율규제에 의존하는 것이 한계를 드러냄에 따라 보호입법을 통한 공법적 규제가 필요하다는 점에 대해서 거의 모든 국가가 공통된 입장을 취하고 있는 것으로 판단된다. 요컨대, 공공부문과 민간부문 모두에서 개인정보보호법을 통한 보호장치가 필요하다는 점에 대해서는 세계적 합의가 있고, 우리나라에서도 마찬가지이다. 문제는 우리의 현실에서 향후 어떤 입법체계를 마련할 것인가에 있다.

그 동안 국내에서는 학계나 시민단체들을 중심으로 개인정보보호에 관한 통합법제를 마련하자는 주장이 줄기차게 제기되고 있다. 기업의 대규모화 및 사회적 책임이 강조되는 현실에서 민간에 대한 규제가 필요하다는 점, 민간부문의 정보수집이 자유의사에만 의하는 것이 아니므로 정보주체의 개인정보자기결정권을 인정할 필요가 있다는 점, 민간부문을 적용대상에 포함시키는 결과 초래되는 비용보다 국민의 기본권보장이 우선한다는 점 등이 논거로 제시되었다.

물론 여기서 통합법제가 구체적으로 어떤 것을 의미하는지는 입장에 따라 각기 다를 수 있지만, 적어도 공공부문과 민간부문에 공통적으로 적용되는 실효적인 법적 규율사항을 통합적인 법제에 담아내야 한다는 점에 대해서는 공감대가 형성되어 있는 것으로 보인다.⁵⁶⁸⁾

568) 홍준형, 『개인정보보호법제 정비를 위한 기본법 제정방안 연구』 (한국전산원,

하지만 각론으로 들어가면, 포괄적인 단일의 통합법을 제정하는 방안, 공공부문과 민간부문을 모두 규율할 수 있는 일반법으로서의 통합법을 제정하는 방안, 공공부문과 민간부문을 모두 규율할 수 있는 기본법으로서의 통합법을 제정하고 양 부문별로 각각의 일반법을 두는 방안 등이 거론되고 있다. 그 가운데 단일통합법의 제정을 절대적으로 고수하는 견해는 별로 발견되지 않고 있으며, 기존의 양대 법률을 토대로 공·사 부문의 각개통합을 시도하는 방안 등이 실현가능한 대안으로 검토되고 있는 것으로 파악된다. 이와는 별도로 현행의 체계와 같이 공공부문과 민간부문을 분리된 상태로 두면서 각 부문을 규율하는 일반법을 부분적으로 손질하고, 개별적 영역에 있어서는 다수의 분야별 법률로 정비하여 보호의 공백을 제거하자는 방안도 소관 기관을 중심으로 최근 들어 강력하게 주장되고 있다.

(2) 입법체계론의 유형

그 동안 국내에서 현실적인 방안으로 주장되어 왔던 개인정보보호법제의 입법체계에 관한 입장은 대체로 다음의 세 가지 정도로 대별해볼 수 있다.

첫째, 현행과 유사하게 공공부문과 민간부문이 분리된 상태로 각 부문별 일반법과 분야별 개별법을 정비하여 법적 공백에 대처하자는 입장(분리형 일반법제정론)이다.

둘째, 공공부문과 민간부문을 통합한 입법체계를 지향하면서도 일반적으로 개인정보의 취급자가 준수해야 의무와 정보주체의 각종 권리 등에 관한 실체적 사항은 물론 권리행사의 방법과 절차, 피해구제, 감독기관 등 절차적 사항까지 폭넓게 규정하자는 입장(통합형 일반법제정론)이다.

2004), 96-97면 참조.

셋째, 공공부문과 민간부문을 통합한 입법체계를 지향하면서 개인정보의 취급상 준수해야 할 기본원칙이나 정책방향, 보호기구 등 기본적인 사항만 담고 나머지는 각 부문별 일반법과 분야별 개별법에 의해 대처하도록 하자는 입장(통합형 기본법제정론)이다.

이러한 입법론은 실체법적 문제, 즉 개인정보처리기관에게 어떤 의무를 부과하고 정보주체에게 어떤 권리를 배분할 것인가에 관한 문제뿐만 아니라, 법집행체계, 즉 개인정보보호기구의 구성, 관할범위, 권한 등에 관한 입장의 차이와 깊이 관련되어 있다. 다만, 분리형 입법론이든 통합형 입법론이든 모두 민간부문을 규율하는 일반법이 필요하다는 점에 대해서는 대체로 일치된 견해를 보이는 것으로 판단된다.⁵⁶⁹⁾ 구 정보통신부도 정보통신망법상의 개인정보보호에 관한 부분(제4장)을 떼어내어 민간의 모든 개인정보처리를 규율하는 일반법으로서 이른바 『민간부문의 개인정보보호에 관한 법률(안)』을 마련하여 2004년 5월 19일 입법예고(정보통신부공고 제2004-32호)를 한 바 있다.

그러면 이하에서는 개인정보보호법제에 관한 입법론 가운데 입법체계에 관한 세 가지 입장의 주요 내용을 살펴보기로 한다.⁵⁷⁰⁾

4. 입법체계론의 주요 내용

(1) 분리형 일반법제정론

분리형 일반법제정론은 공공부문과 민간부문을 분리하여 각각 별도의 일반법을 제정하자는 입장이다. 물론 일반법만 두는 것으로 그치는 것이 아니고, 각 부문에서 특별히 보호수준을 높일 필요가 있거나

569) 정준현, “개인정보보호법제 현황과 법제 정비의 필요성”, 정보통신부 주최 『민간부문의 개인정보보호에 관한 법률 제정 공청회』자료집, 14면; 임건면, “개인정보침해에 대한 민사법적 대응”, 『비교사법』 제8권 제1호(하)(통권 제14호)(한국비교사법학회, 2001), 1051면.

570) 이하 이인호 외, 『개인의 사생활, 국가적 감시, 그리고 규범』(정보통신정책연구원, 2006), 74-81면 참조.

또는 개인정보처리의 필요성이 특별히 더 높은 분야에서는 특별법을 마련할 수 있음을 전제로 한다.

1990년대 초반의 분리입법론은 구체적으로 다음과 같은 논거에 입각하고 있다. 첫째, 공공부문과 민간부문은 개인정보의 수집근거와 방법이 다르다는 점이다. 즉 공공부문에서의 정보수집은 대부분 법령에 근거를 두고 의무적·강제적 방법을 사용하는 반면에, 민간부문에서는 계약에 의해 자발적으로 제공되는 경우가 대부분이라는 것이다. 둘째, 민간부문에의 적용은 민간의 경제적 자율성을 저해하기 쉽고 제도운영에 따르는 비용으로 인해 정보산업의 위축을 가져와 정보사회의 추진에 지장을 초래할 우려가 크다는 점이다. 셋째, 민간부문은 현행 법령의 적정한 운영을 통해서, 즉 사생활보호에 관한 현행의 형법 및 각종 개별법률의 엄격한 적용을 통해서 개인의 사생활보호가 가능하다는 것이다.⁵⁷¹⁾ 이와 같은 입법론은 1993년에 공공기관개인정보보호법을 제정할 당시에 이미 제기되었으며, 법률개정의 과정에서 결국 관철되었다.⁵⁷²⁾ 하지만 민간부문에서 1995년에 신용정보보호법이 제정되고 1999년에 정보통신망법이 개정되면서 개인정보보호에 관한 별도의 장을 두게 되면서, 종래의 논거는 유효하지 않게 되었다. 그리고 정보통신기술의 비약적 발달로 개인정보침해의 위험성이 그 당시와는 비교할 수 없을 정도로 증대되었다고 할 수 있다.

이에 따라 최근의 분리입법론은 민간부문에서의 개인정보보호를 위한 일반법이 필요하다는 것을 인정하면서, 다만 민간부문의 일반법을 공공부문의 일반법과 통합할 필요까지는 없다는 방향으로 전개되고 있다. 즉, 양 부문에 있어서 개인정보의 수집근거와 방법이 서로 다르기 때문에 그 구체적인 법리나 규율내용이 다를 수밖에 없다는 관점

571) 이상의 설명은 황인호, “개인정보보호제도에서의 규제에 관한 연구”, 『공법연구』 제30집 제4호(한국공법학회, 2002), 248-249면에서 인용.

572) 총무처, 『축조해설 개인정보보호법』(총무처, 1994), 26-28면 참조.

에서, 양 부문을 별도로 규율하는 일반법이 병존시킬 필요가 있다는 것이다. 실제로 과거 행정자치부의 경우 법제의 통합은 장기과제로 검토하면서 현행 공공기관개인정보보호법을 개정·보완하는 쪽으로 방향을 잡은 적이 있었으며, 구 정보통신부 역시 공공부문과 민간부문을 분리하되 민간부문의 경우 정보통신망법을 중심으로 통합하는 방안을 추진한 바 있었다. 그에 비해 시민단체들은 지속적으로 통합기본법 내지 통합일반법을 제정하는 방안을 선호하는 경향을 보여 왔다.

과거 정부에서는 행정자치부와 정보통신부의 시절 각기 분리입법론에 입각한 입법정책을 추진하였던 적이 있었다. 행정자치부의 경우 법제의 통합은 장기과제로 검토하면서 현행 공공기관개인정보보호법을 개정·보완하는 쪽으로 방향을 잡았으며, 구 정보통신부 역시 공공부문과 민간부문을 분리하되 민간부문의 경우 정보통신망법을 중심으로 통합하는 방안을 추진한 바 있었다. 실제로 구 행정자치부는 기존 공공기관개인정보보호법의 소관부처로서 최근 이 법률의 취약성이 문제되자 그 보호수준을 다소 강화시킨 개정안을 마련하여 2003년 8월 21일 입법예고한 바 있으며(행정자치부 공고 제2003-124호), 구 정보통신부도 별도로 2004년 5월 19일 민간부문 일반법(제정안)을 마련하여 입법예고한 바 있다. 물론 이러한 상황은 소관부처의 권한을 둘러싼 이해관계가 작용했던 결과라고도 볼 수 있을 것이다.

하지만 정보통신부의 후신이라 할 수 있는 방송통신위원회에서는 2008년 7월 22일 통합적인 개인정보보호법의 제정을 시사하는 계획을 발표한 바 있다. 이후 이러한 계획은 행정안전부의 이름으로 제출된 개인정보보호법 제정안을 통해서 구체화되고 있다.

(2) 통합형 일반법제정론

이는 공공부문과 민간부문을 통합한 입법체계를 지향하면서도 일반적으로 개인정보의 취급자가 준수해야 의무와 정보주체의 각종 권리

등에 관한 실체적 사항은 물론 권리행사의 방법과 절차, 피해구제, 감독기관 등 절차적 사항까지 폭넓게 규정하자는 입장이다.

이 입장의 논거는 다음과 같다.⁵⁷³⁾ 첫째, 개인정보보호는 개인정보의 적정한 이용 및 관리에 그 핵심이 있고, 적정 관리라는 점에서 보면 공공기관과 민간기관의 구분은 무의미하다. 더구나 위험성의 측면에서도 민간기관이 더 위험할 수도 있다. 민간기업은 개인정보를 이용하여 경제적 이익을 추구하기 때문에 개인정보보호에 상대적으로 덜 관심을 가지게 된다는 점에서 개인정보침해의 위험성이 더 클 수 있다. 둘째, 프라이버시권 내지 개인정보자기결정권은 인간존엄에서 유래하는 것으로 최우선적으로 존중되어야 하는데, 영업의 자유를 명분으로 프라이버시권을 제한하는 것은 본말이 전도된 것이다. 셋째, 공공기관이나 민간기관이나 프라이버시권을 침해한다는 점과 그것이 위법하다는 점에서는 차이가 없으므로 양 부문 모두 개인정보처리업무를 행함에 있어서 동일한 법적 규율을 받아야 한다. 예컨대, 국립병원과 사립병원을 구별하여 보호정도를 달리하는 것은 타당하지 않다. 넷째, 공공기관과 민간기관의 중간 영역에 위치하는 기관의 경우에는 어느 부문의 법의 적용을 받아야 하는지가 문제된다. 요컨대, 이 통합 일반법론은 개인정보보호가 공공기관이나 민간기관이나에 따라서 달라질 수는 없으며, 취급되는 개인정보의 성격에 따라서 달라져야 한다는 것이다. 예컨대, 의료정보는 그 취급기관이 공공기관이든 민간기관이든 동일하게 엄격한 보호가 주어져야 한다는 것이다.⁵⁷⁴⁾

573) 황인호, “개인정보보호제도에서의 규제에 관한 연구”, 『공법연구』 제30집 제4호 (한국공법학회, 2002), 251-252면의 주장을 정리한 것임. 그 밖에 같은 입장으로 정완용, “전자거래에 있어서 개인정보침해에 대한 법적 구제”, 『인터넷법률』 제10호 (법무부, 2002), 101-102면; 최상호, “전자거래에 있어서 소비자보호 - 특히 프라이버시 및 개인정보보호를 중심으로 -”, 『비교사법』 제8권 제1호(하)(한국비교사법학회, 2001), 998면.

574) 황인호, 위의 글, 252면.

물론 이러한 입장에서도 반드시 공공과 민간의 모든 개인정보처리를 통합형 일반법에 의해 전적으로 규율할 수 있도록 해야 한다는 것은 아니다. 개인정보의 성격에 따라 개별 영역에서 특별법의 형태로 특별하게 규율할 수 있다는 논지이다.

즉 “공적부문과 사적부문을 포괄하는 통합일반법을 제정하고, 공적부문과 사적부문에서 개별분야의 특성에 따라 그에 적합한 개별법을 제·개정하여 규율하는 방식을 취하고, 사적부문에 있어서는 사적자치의 원칙을 존중하여 민간사업자 등의 자율적 규제에 해결할 수 있는 분야에 대해서는 자율규제를 인정하는 것이 일본과는 다르게 사적부문에서 개인정보보호에 대한 법제가 다수 제정되어 있는 우리나라의 특성을 충분히 고려한 입법방안이라고 할 수 있다.”⁵⁷⁵⁾는 것이다.

이러한 통합일반법론의 기초에 서서 현재 입법적 노력을 기울이고 있는 것이 시민사회단체의 입장이라고 할 수 있다. 7개 시민사회단체로 구성된 ‘프라이버시법 제정을 위한 연석회의’는 2004년 5월 27일 『개인정보보호법 인권시민사회단체(안)』을 마련하고 이를 토대로 공청회를 개최한 바 있으며, 2004년 9월 24일에는 민주노동당 노회찬 국회의원의 후원 하에 “개인정보보호기본법 제정을 위한 입법공청회”를 개최한 바도 있다.

이 공청회에서 시민사회단체가 내놓은 법안의 명칭은 『개인정보보호기본법(안)』이지만, 그 실질 내용은 위 통합형 일반법제정론자의 주장과 같이 공공부문과 민간부문을 포괄하는 ‘일반법’의 성격을 가진다고 하겠다. 여기서 개인정보처리기관이 준수하여야 할 의무, 컴퓨터결합(computer matching)에 대한 제한, 정보주체의 권리와 구제절차, 개인정보사전영향평가제도, 그리고 개인정보감독기구로서의 개인정보보호위원회의 설립 등 상세한 실체법적 내용과 보호기구 및 구제절차 등

575) 위의 글, 248면.

에 대해 상세한 규정을 두고 있기 때문이다.

(3) 통합형 기본법제정론

이는 공공부문과 민간부문을 통합한 입법체계를 지향하면서 개인정보의 취급상 준수해야 할 기본원칙이나 정책방향, 보호기구 등 기본적인 사항만 담고 나머지는 각 부문별 일반법과 분야별 개별법에 의해 대처하도록 하자는 입장이다.

이러한 기본법제정론은 공공부문과 민간부문을 포괄한다는 측면에서는 통합형 일반법제정론과 다르지 않다. 그러나 근본적으로 ‘기본법’이나, ‘일반법’이나 하는 점에서 차이가 난다고 하겠다. 통상적으로 법률용어상 ‘기본법’은 ‘개별법’에 대응되는 것이고, ‘일반법’은 ‘특별법’과 대응되는 것으로 이해되고 있다.⁵⁷⁶⁾ 이러한 점에서 양자의 차이는 규율사항의 밀도, 구체성, 실천성 등에서 찾아야 할 것으로 본다. 즉, 기본적 이념과 원칙, 개념의 정의 등과 같은 기본적 사항만 규율하고 있는 수준이면 ‘기본법’이고, 거기서 더 나아가 구체적인 권리나 의무 등 실체적인 사항 또는 그 실현을 위한 구체적인 절차적 사항까지 다루고 있으면 ‘일반법’으로 보아야 한다는 것이다.

이러한 관점에서 볼 때 개인정보보호와 관련한 통합형 기본법제정론에서 상정하고 있는 ‘기본법’에는 개인정보보호의 기본이념, 개인정보보호를 위한 국가의 책무와 시책, 기본개념의 정의, 공공부문과 민간부문에 공통되는 개인정보취급상의 기본원칙, 보호기구의 설치 등의 내용이 담길 수 있을 것이다. 하지만 다수의 개별법을 제정하더라도 그들 입법의 보호범위에 속하지 않는 영역이 남아 있을 경우에는 결국 보호의 공백이 생기게 된다. 따라서 이러한 문제를 해결하기 위해서는 통합형 기본법에 모든 개인정보처리기관이 준수하여야 할 최

576) ‘기본법’이라는 용어의 실제 쓰임새에 대한 분석은 이인호 외, 『개인의 사생활, 국가적 감시, 그리고 규범』(정보통신정책연구원, 2006), 79면을 참조할 것.

소한의 기본적 책무, 그 위반에 대한 최저한의 제재수단, 감독기관 등에 대해서도 규정을 두는 방향으로 논의가 전개되는 경향이 있다. 그렇게 될 경우에는 “개인정보보호기본법”이란 것은 결국 ‘기본법’인 동시에 ‘일반법’으로서의 성격도 함께 가지게 될 것이다.

과거 참여정부 시절 정부혁신지방분권위원회가 2004년 7월 경에 마련한 바 있는 『개인정보보호기본법(시안)』도 역시 ‘일반법’의 성격도 함께 지니는 ‘기본법’으로 평가할 수 있을 것이다.

5. 입법체계의 평가

(1) 입법평가의 기준

입법평가에서는 일반적으로 법률상의 정책을 실시하기 위하여 필요한 비용, 당해 정책을 실시하는 때에 정책의 수범자에 대하여 미치는 영향, 나아가 널리 사회에 미치는 영향 등이 고려된다. 하지만 입법평가의 구체적인 기준으로는 다양한 것이 있을 수 있으며, 실제로 학자마다 그 용어법도 혼재하고 있다. 대표적으로 C. Böhrer/W. Huffer는 실효성과 효율성 이외에도, ㉠ 사법심사와 법의 집행에 즈음하여 적정성을 유지하는 것, ㉡ 수범자에 있어서의 적정성(이해가능성, 정보비용, 시민과의 친화성, 권리구제의 방도), ㉢ 목적의 충족과 합목적성(법률과 사회적 사실의 관련성, 목적의 일관성, 법률로 규정되는 사항과 당해 사항의 원인과의 관련성 등), ㉣ 규율형태(법의 체계상의 위치, 규율밀도), ㉤ 규율필요성, ㉥ 실행가능성 등도 고려되어야 한다고 주장한다.⁵⁷⁷⁾ 한편, 박영도 박사는 입법평가의 기준으로 ㉠ 법경제성(규율필요성, 규율대안, 규율밀도, 규율강약 등), ㉡ 영향(효과, 성과,

577) Carl Böhrer/Werner Huffer, *Test und Prüfungen von Gesetzentwürfen, Anleitung zur Vorabkontrolle und Verbesserung von Rechtsvorschriften*(Köln/Bonn, 1980), S.22ff. 박영도, 『입법평가의 이론과 실제』(한국법제연구원, 2007), 44면 참조.

부작용 등), ㉔ 실효성(목표달성도, 최적효과 등), ㉕ 비용(발생비용, 국가재정수요, 경제적 비용, 국민경제적 비용 등), ㉖ 유효성 또는 효율성(행정적 효용, 경제적 효용, 국민경제적 효용, 비용과 성과 등), ㉗ 친숙성(이해성, 예측가능성과 법적 안정성, 실생활에의 적합성, 비용최소화 등), ㉘ 적용적합성(수용가능성, 행정실제성, 행정비용의 최소화, 실행가능성, 관찰적합성 등), ㉙ 법합치성(상위법, 체계성, 완비성, 관련성 등) 등 8가지를 제시하고 있다.⁵⁷⁸⁾ 이러한 평가기준에서의 심사항목과 방법론은 다음의 표로 나타내고 있다.⁵⁷⁹⁾

[표 3-3-4] 입법평가의 기준

평가기준(요소)	심사항목	방법론(선택)
법경제성 (Rechtsökonomie)	<ul style="list-style-type: none"> • 규율필요성, 규율대안 • 규율밀도, 규율강약 	<ul style="list-style-type: none"> • 필요성심사, 비교법, 실험입법
영향 (Wirkung)	<ul style="list-style-type: none"> • 효과, 성과, 부작용 • 사전평가로의 전환 	<ul style="list-style-type: none"> • 효과분석, 도상연습, 시물레이션, 실무테스트, 실험입법
실효성 (Effektivität)	<ul style="list-style-type: none"> • 목표달성도, 최적효과 	<ul style="list-style-type: none"> • 효과분석, 실무테스트, 실험입법
비용 (Kosten)	<ul style="list-style-type: none"> • 발생비용, 국가재정수요(1회, 반복), 경제적 비용 • 국민경제적 비용 	<ul style="list-style-type: none"> • 비용분석, 시물레이션, 비교법, 벤치마킹, 전문가감정
유효성(효율성) (Effizienz)	<ul style="list-style-type: none"> • 행정적 효용, 경제적 효용, 국민경제적 효용 • 비용/성과, 비용/효용 	<ul style="list-style-type: none"> • 효용분석, 성과분석, 전문가감정, 실무테스트
친숙성 (Betroffenen freundlichkeit)	<ul style="list-style-type: none"> • 이해성 • 예측가능성/법적 안정성 • 실생활에의 적합성 • 비용최소화 	<ul style="list-style-type: none"> • 실무테스트, 실험입법, 도상연습
적용적합성 (Vollzugstauglichkeit)	<ul style="list-style-type: none"> • 수용가능성, 행정실제성 • 행정비용의 최소화 • 실행가능성, 관찰적합성 	<ul style="list-style-type: none"> • 실무테스트, 실험입법, 도상연습, 직무분석, 교차분석
법합치성 (Rechtkonformität)	<ul style="list-style-type: none"> • 상위법, 체계성 • 완비성, 관련성 	<ul style="list-style-type: none"> • 정합성심사, 전문문헌분석, 판결문분석, 완전성심사, 간결성테스트

578) 이에 관한 구체적인 설명은 박영도, 앞의 연구보고서, 46-68면을 참조할 것.

579) 박영도, 앞의 연구보고서, 45-46면.

이상과 같은 다양한 입법평가의 기준들이 제시되고 있지만, 반드시 이 모든 기준을 활용하여야 한다는 의미는 아니다. 주어진 여건과 현실을 고려하여 가능한 한 많은 기준을 활용할 수 있으면 보다 정확한 입법평가가 될 수 있을 것이라는 정도로 이해할 수 있다.

그런데 위에서 살펴본 개인정보보호 관련 국내의 입법론에서는 주로 보호의 사각지대 해소, 관련 법제의 재정비, 감독기구의 일원화, 규범체계의 간명화 등을 둘러싸고 다소간의 차이를 보여주고 있다. 따라서 입법체계의 평가와 관련하여서는 ㉠ 효율성, ㉡ 비용, ㉢ 적용적합성, ㉣ 친숙성 등이 유용한 기준이 될 수 있을 것으로 본다. 다만 여기서 ㉠ 효율성은 개인정보의 법적 보호에 있어서 사각지대를 어느 정도 줄일 수 있는가, ㉡ 비용은 개인정보보호 관련 법제를 정비하고 새로운 입법적 수요에 대처하는 데 소요되는 비용이 어느 정도인가, ㉢ 적용적합성은 개인정보보호법의 집행기구의 관할이 얼마나 적합하게 설정되어 있는가, ㉣ 친숙성은 수범자의 입장에서 볼 때 개인정보보호 관련 법제의 현황에 대한 인식이나 적용될 법조항에 대한 접근이 얼마나 용이한가에 각각 초점을 맞추어 평가기준으로 삼고자 한다.

(2) 각 입법론의 입법체계 평가

1) 분리형 일반법제정론

현행의 공공기관개인정보보호법을 공공부문의 일반법으로 개정하고, 기타 민간부문에 산재한 법률들을 통합하여 민간부문에 적용될 일반법을 제정할 경우에는 ㉠ 개인정보보호의 사각지대는 크게 우려하지 않아도 될 것이나(효율성), ㉡ 법제를 정비하는 과정에서 소요되는 비용이 통합형 일반법주의에 비해 클 수밖에 없을 것이다(비용). ㉢ 공공부문과 민간부문에 각기 다른 법집행기구가 존재하게 되어 부문별 특성에 적합한 집행력을 신속하게 확보할 수 있는 장점이 있는 반면

에, 양 부문을 포괄적으로 규율해야 하는 상황에서는 통일적 집행을 기대하기 어려운 단점이 있다(적용적합성). ㉔ 일반법이 부문별로 별도로 존재할 경우 수범자로서는 단일의 일반법의 체계에 비해 법제의 현황에 대한 인식의 정도나 관련 법제에 대한 접근가능성이 떨어질 수밖에 없을 것으로 판단된다(친숙성).

2) 통합형 일반법제정론

공공부문과 민간부문을 통합적으로 규율하면서도 개인정보보호에 필요한 일반적인 사항을 폭넓게 규정할 경우에는, ㉑ 공공부문과 민간부문을 포괄하는 일반법의 제정으로 무엇보다도 법적 보호의 공백을 최소화할 수 있는 효과를 기대할 수 있다(효율성). ㉒ 한 번의 입법으로 중복되는 법제를 모두 통폐합하는 효과가 있고, 일차적으로 적용될 수 있는 사항들을 폭넓게 규정함으로써 새로운 문제에 대응하기 위한 개별 법률의 제정을 수시로 해야 하는 번거로움을 덜어줄 수 있다. 이러한 점에서 후속적인 법률의 개정이나 빈번한 개별 법률의 제정에 따른 입법비용의 증대를 막을 수 있을 것으로 본다(비용). ㉓ 공공부문과 민간부문을 통괄하는 하나의 법집행기구가 존재하게 되어 통일적 집행력의 확보가 용이하고, 특히 단일의 개인정보보호기구를 둘 경우 개인정보보호에 관한 종합적인 정책의 추진으로 법집행의 효율성이 증대될 것이다(적용적합성). ㉔ 단일의 통합형 일반법의 체계로 갈 경우 수범자로서는 개인정보보호법제의 현황에 대한 인식가능성이 높아지고 적용될 조항에 대한 접근이 용이해질 것을 충분히 예상해볼 수 있다(친숙성).

3) 통합형 기본법제정론

만일 기본법의 체제를 취하면서도 각 부문별 일반법을 별도로 두지 않을 경우에는 다수의 개별법으로써 전 영역의 개인정보를 커버할 수 있어야 하는 부담이 생긴다.

㉑ 아무리 많은 개별법을 제정하더라도 그들 입법의 보호범위에 속하지 않는 분야가 생겨날 경우에는 법적 보호의 공백이 발생할 수밖에 없다(효율성). ㉒ 개인정보보호기본법을 제정하는 외에도, 공공부문의 일반법과 민간부문의 일반법을 제정하기 위해 현행의 공공기관개인정보보호법, 정보통신망법, 신용정보법 등을 대폭 개정해야 하는 점에서 그에 소요되는 입법비용이 막대할 것으로 예상된다(비용). ㉓ 단일의 개인정보보호기구를 둘 경우 개인정보보호에 관한 종합적인 정책의 추진으로 법집행의 효율성이 증대될 것이나, 공공부문과 민간부문을 따로 관할하는 법집행기구를 둘 경우에는 통일적 집행력의 확보가 어려운 점이 있을 것이다(적용적합성). ㉔ 기본법 이외에 부문별 일반법이 존재할 경우 수범자로서는 통합형 일반법의 체계에 비해 개인정보보호법제의 현황에 대한 인식도나 적용 조항에 대한 접근도가 상대적으로 떨어지게 될 것으로 예상된다(친숙성).

(3) 분석의 결과

각 입법체계적 특성을 ㉑ 법적 보호의 공백(효율성), ㉒ 법제정비에 소요되는 비용(비용), ㉓ 법집행과정의 용이성(적용적합성), ㉔ 수범자의 이해가능성(친숙성) 등을 기준으로 서로 비교분석을 한 결과를 최종적으로 정리해보면, 그 결과는 다음의 표와 같이 나타낼 수 있을 것이다.⁵⁸⁰⁾

580) 이러한 분석은 기본적으로 홍준형 교수가 사용한 분석의 틀을 참조하여 재구성한 결과이다. 하지만 홍 교수는 유럽식 모델을 일원적 개별주의(‘기본법-개별법’안)로 파악하면서 이를 가장 우월한 것으로 평가를 내리고 있다. 하지만 영국, 독일, 프랑스 등의 개인정보보호법을 ‘기본법’이라기보다는 ‘일반법’에 속하는 것으로 보아야 할 것이다. 동인, 『개인정보보호법제 정비를 위한 기본법 제정방안 연구』(한국전산원, 2004), 99면 참조.

[표 3-3-5] 각 모델의 비교

구분	효율성	비용	적용적합성	친숙성
	법적 공백의 해소	법제정비 소요 비용	집행기구의 관할적합성	수법자의 이해가능성
분리형 일반법 제정론	×	△	△	×
통합형 일반법 제정론	◎	○	◎	◎
통합형 기본법 제정론	○	×	○	○

【법례】 ◎ 매우 높음, ○ 높음, △ 보통, × 낮음

이러한 분석을 토대로 할 때 통합형 일반법의 체계가 가장 유리하다는 결론을 도출할 수 있었다.

(4) 규율사항

이처럼 통합형 일반법의 체계를 취할 경우 개인정보보호법에서는 개인정보보호의 기본이념, 개인정보보호를 위한 국가의 책무와 시책, 기본개념의 정의, 개인정보취급상의 기본원칙, 개인정보처리자의 의무, 정보주체의 권리, 권리행사의 방법과 절차, 피해구제, 보호기구의 설치, 제재수단 등도 함께 규정하는 것이 바람직할 것이다.

제 4 편
개인정보처리의 입법기준에
관한 병행적 입법평가

제 1 장 서 언

2008년 2월 이명박 정부가 출범하고 『정부조직법』의 개정에 의하여 정보보호 전반을 소관 업무로 일원화하게 된 행정안전부는 2008년 8월 12일 『개인정보보호법 제정법률안』을 입법예고하였다. 이 법률안은 공공부문과 민간부문을 모두 포괄하여 모든 개인정보의 처리에 적용되는 “일반법”으로서의 성격을 갖는다. 본 제4편에서는 이 제정법률안(이하 “입법예고안”이라 한다)에서 규정하고 있는 개인정보처리의 입법기준이 적정하고 타당한지를 비교법적 관점 등에 의거하여 평가하고자 한다.

우선 아래 제2장에서는 입법예고안이 제시하고 있는 기본용어의 정의규정에 대하여 그 적정성 및 이해가능성을 분석·평가하고 수정대안을 제시하며 일부 누락된 중요한 기본용어의 개념정의를 제시한다. 개인정보보호법의 핵심개념을 담고 있는 이 부분은 법률안의 실제적 기준과 방향을 설정함에 있어서 매우 중요한 요소이다.

다음으로 제3장에서는 개인정보의 수집·이용·제공의 허용기준에 대한 적정성 평가를 하고 그 수정대안을 제시한다. 현재 우리 사회의 일반인이나 일부 전문가들 중에는 개인정보의 수집·이용·제공에 있어서 정보주체의 동의를 합법성 요건으로 해야 한다는 인식과 주장이 존재하고 있다. 그러나 이는 개인정보보호법제에서 균형적 시각이라고 볼 수 없다. 제1절에서는 개인정보자기결정권에 대한 정확한 이해를 도모하고, 오해의 경향을 분석·비판한다. 그리고 제2절에서는 개인정보의 수집·이용·제공의 허용기준을 외국의 입법례에서는 어떻게 설정하고 있는지를 분석한다. 이에 기초하여 제3절에서는 입법예고안의 허용기준에 어떤 점에서 어떻게 문제가 있는지 그 타당성 여부를 평가하고 그 수정대안을 제시한다.

이어 제4장에서는 개인정보의 수집·이용·제공에 있어서의 절차적 요건에 대하여 그 적정성 여부를 평가하고 수정대안을 제시한다. 개인정보처리자는 그 수집·이용·제공이 제3장의 허용기준을 충족한다 하더라도 추가적으로 절차적 요건을 준수하여야 한다. 이 절차적 요건에는 목적명시 요건, 품질관리 요건, 고지 요건, 그리고 보고 요건이 있다. 외국의 입법례에서는 이들 절차적 요건을 어떻게 입법화하고 있는지를 면밀히 분석한 다음, 입법예고안의 절차적 요건의 적정성을 평가하고 그 수정대안을 제시한다.

마지막으로 제5장에서는 공공부문의 개인정보처리의 입법기준을 평가하고 문제점을 지적한다. 특히 개인정보 공동이용의 효용성과 위험성을 평가하고 대안을 제시한다.

종합적으로 볼 때, 현재의 입법예고안은 일반법으로서의 개인정보의 “이용”의 가치보다 “보호”의 가치에 지나치게 편향되어 있는 것으로 평가된다. 절차적 요건에 대한 규율은 소홀히 하고 있는 반면에, 이용과 제공에 대해 정보주체의 동의를 원칙적 요건으로 설정함으로써 필요한 개인정보의 이용을 과도하게 제한하는 입법기준을 설정하고 있는 것으로 평가된다. 그러나 한편으로 공공부문에서는 개인정보의 공동이용을 전자정부의 핵심적인 전제로 받아들이면서 각 공공기관이 보유·운영하고 있는 개인정보DB들의 통합·연계를 쉽게 허용하는 등 “이용”의 가치에 경도되어 있다. 전체적으로 이용과 보호의 균형이 맞지 않아 재조정이 필요한 것으로 평가된다.

제 2 장 기본용어의 정의규정에 대한 평가와 대안제시

제 1 절 개 관

입법예고안 제2조는 7가지의 기본용어에 대하여 개념규정을 하고 있다: “개인정보”(제1호), “처리”(제2호), “정보주체”(제3호), “개인정보파일”(제4호), “개인정보처리자”(제5호), “공공기관”(제6호), “영상정보처리기기”(제7호).

이들 개념규정은 대체로 적정한 것으로 평가되지만, 좀 더 세밀한 개념정의를 요구된다. 또한 여기에는 개인정보보호법에서 그 개념을 분명히 해야 할 몇 가지 중요한 기본용어가 누락되어 있는 것으로 분석된다. 이하에서는 각호의 개념규정에 대하여 그 적정성 및 이해가능성에 대한 평가를 하고, 이어 누락된 중요한 기본용어를 대안으로 제시한다.

제 2 절 개인정보 · 개인기록 · 고유식별정보의 세 가지 개념의 구별필요성

입법예고안 제2조 제1호는 “개인정보란 생존하는 개인에 관한 정보로서 해당 정보에 의하여 개인을 식별할 수 있는 정보(해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.”고 규정하고 있다.

그런데 개인정보보호법이 개인정보처리의 실태를 정확하게 반영하기 위해서는 “개인정보”, “개인기록”, “고유식별정보”의 세 가지 개념을 분명하게 상정하고 있어야 한다. 그런데 입법예고안에는 이 점이 불분명하다. 특히 “개인기록”의 개념이 상정되어 있지 않을 뿐만 아니

라 규율의 대상이 되는 개인정보의 범위를 판단하는 기준이 불분명하여 나중의 적용과정에서 혼란을 일으킬 수 있는 여지를 주고 있다. 이하에서는 입법예고안이 규정하고 있는 “개인정보”의 개념상의 한계를 비교법적 관점에서 평가하고 그 수정대안을 제시한다.

개인정보보호법에서 보호하는 “개인정보”는 ‘개인에 관한 일체의 정보’를 의미한다. 특정 개인에 ‘관한’ 것이면 모든 형태와 내용의 정보가 여기에 해당한다. 이름, 주소, 전화번호, 이메일주소, 몸무게, 사진, 물건을 산 시각과 산 물건의 내용, 병력, 학력, 퇴근하는 시간, 춤추는 모습을 담은 동영상 등 일체의 정보가 개인정보이다.

물론 이들 개인정보는 ‘특정한 개인’, 즉 ‘신원을 확인할 수 있는 (identifiable) 개인’에 관한 것이어야 한다. 신원확인이 불가능하게 익명으로 처리되는 개인정보는 개인정보보호법의 보호대상에서 제외된다. 왜냐하면 개인정보보호법이 종국적으로 보호하고자 하는 것은 ‘정보’ 그 자체가 아니라 그 정보의 오·남용으로 인해 침해될 특정 개인(정보주체)의 권리나 이익이기 때문이다. 신원확인이 ‘불가능한’ 개인정보는 아무리 오·남용하더라도 그로 인해 누구의 권리나 이익도 침해되는 바가 없기 때문이다.

여기서 신원확인이 가능한 개인정보인지 여부를 어떻게 판단할 것인가 하는 문제가 발생한다. 이에 관한 법적 기준이 어느 정도 분명하게 제시될 필요가 있다. 이는 어떤 정보의 수집·처리가 개인정보보호법의 규율대상이 되는지를 판단하는 기준이 되기 때문이다. 예컨대, 인터넷에 게시되어 있는 이메일주소만을 수집하여 다른 신원확인 정보와 결합 없이 광고메일의 발송에 활용하는 경우 그 이메일주소정보를 처리(수집·이용·제3자 제공)하는 자는 개인정보보호법의 규율을 받는가가 문제될 수 있다. 이메일주소는 누군가의 정보이긴 하지만, 그 정보만으로 그것이 특정한 개인의 이메일주소인지 여부를 판단하는 것이 가능한가 하는 문제가 제기된다. 다시 말해서, 이메일주

소만으로 그 정보의 주체를 확인할 수 있는가 하는 문제이다. 일반적으로 이메일주소만으로는 그 정보의 주체를 확인할 수 없다고 보아야 할 것이다. 그렇다면 이메일주소만을 수집하여 광고메일의 발송에 활용하는 자는 개인정보보호법의 규율을 받지 않는다고 보아야 한다.⁵⁸¹⁾

여기서 우리는 “개인정보”(personal information) 외에 추가적으로 두 가지 중요한 기본개념을 상정해 볼 수 있다. 하나는 “개인기록”(personal record)이고, 다른 하나는 정보주체의 신원을 나타낼 수 있는 “고유식별자”이다. 오늘날 개인정보를 수집하고 처리하는 실제의 관행을 보면, 이름·주민등록번호·주소·전화번호 등 개인에 관한 여러 정보들을 함께 묶어 처리하고 있다. 또 그럴 때에 비로소 그 개인정보들은 사회적으로 의미를 지닌다. 이처럼 한 개인에 관한 정보들의 ‘묶음’을 지칭하는 용어로 “개인기록”이라는 개념을 채택할 필요가 있다. 그리고 그 개인기록 안에는 당해 정보주체를 식별할 수 있게 해주는 고유식별자(예컨대, 이름, 주민등록번호)⁵⁸²⁾가 포함되어 있기 마련이

581) 개인정보보호법의 직접적인 규율의 대상이 되는 것과는 무관하게, 이메일주소 정보 수집행위를 금지하거나 제한하는 규율이 있을 수 있다. 신원확인이 불가능한 이메일주소지만 스팸메일의 발송에 활용할 수 있고 그로 인한 해악이 있을 수 있기 때문이다. 실제로 우리의 현행 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』(2004. 12. 30 개정된 것) 제50조의2는 인터넷 홈페이지 운영자의 사전 동의 없이 인터넷 홈페이지에서 자동수집프로그램을 이용하여 전자우편주소를 수집하는 행위를 금지하고 있고 나아가 그렇게 수집된 전자우편주소의 판매·유통·이용을 금지하고 있다. 위반의 경우 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하여진다. 그러나 이는 광고표현의 자유를 충분히 고려하지 않은 지나친 규율이 아닌가 생각된다. 스팸의 해악을 방지하고자 하는 것이라면 당해 법률은 제50조에서 영리목적의 광고성 정보전송을 opt-out 방식으로 제한하는 규율을 이미 하고 있다. 스팸의 해악을 직접 일으키는 행위를 규율하는 것을 넘어서서, 공개되어 있는 전자우편주소의 수집 행위 자체를 금지하고 이를 형사처벌하는 것이 타당한 규율인지는 입법정책적으로 재평가되어야 할 것으로 보인다. 스팸규제의 정책방향에 관해서는 이인호, “스팸(SPAM) 규제입법에 대한 평가와 정책방향”, 『정보법학』 제8권 제1호(한국정보법학회, 2004. 7) 참조.

582) 『실종아동 등의 보호 및 지원에 관한 법률』제2조 제7호는 이러한 고유식별자를 “신상정보”라고 표현하고 있다. 동조 동호는 “신상정보라 함은 이름·나이·사진 등 특정인임을 식별하기 위한 정보를 말한다.”고 규정하고 있다. 다만, ‘나이’를 고유식별자라고 할 수 있는지는 의문이다.

다. 개인정보보호법은 이러한 개인기록들의 체계적인 묶음, 즉 개인정보 데이터베이스(개인정보DB)를 구축하여 활용하는 과정에서 이루어지는 개인정보의 수집·저장·가공·편집·검색·정정·이용·제공 등의 처리를 규율하는 법이다.

미국과 유럽의 개인정보보호법을 보면 위와 같은 “개인기록”, “개인정보”, “고유식별자”의 세 가지 개념이 모두 들어 있음을 알 수 있다.

예컨대, 미국의 공공부문 개인정보보호법인 『프라이버시법』(Privacy Act)은 “개인기록”(record)을 이렇게 규정하고 있다: “개인기록(record)이라 함은 행정기관이 보유하는 개인에 관한 정보(information about an individual)의 개개 항목 또는 그 집합을 말한다. 그 기록에는 당해 개인의 교육, 금전적 거래(financial transactions), 병력(medical history), 전과(criminal history) 또는 취업경력(employment history)에 관한 정보가 담기지만 이에 한정되지 않는다. 그리고 그 기록에는 당해 개인의 이름, 또는 식별번호나 식별부호 혹은 지문(finger print)·성문(voice print)·사진(photograph)과 같은 당해 개인에게 고유한 식별자(identifying particular)가 포함되어 있어야 한다.”⁵⁸³⁾ 이처럼 미국의 『프라이버시법』은 규율의 대상이 되는 “개인기록”(record)안에 적어도 신원을 확인할 수 있는 식별자가 포함되어 있어야 하고, 그 식별자로 기능할 수 있는 것으로서 (i) 이름, (ii) 공적으로 부여한 식별번호나 식별부호, (iii) 기타 생체식별정보(지문, 성문, 사진)를 명시하고 있다. 그리고 미국의 법은 이러한 개인기록들의 체계적인 묶음, 즉 개인정보 데이터베이스를 “개인기록시스템”(system of records)이라고 이름을 붙이고 있다.

한편, 유럽연합의 개인정보보호지침(95/46/EC)도 이와 유사하게 다음과 같이 규정하고 있다. 즉 “개인기록”(personal data)이라 함은 “신원이 확인된(identified) 또는 신원확인이 가능한(identifiable) 자연인(즉,

583) 5 U.S.C. §552a(a)(4).

정보주체 data subject)에 관한 일체의 정보(any information)를 말하며; 신원확인이 가능한 개인(identifiable person)이라 함은 직접 또는 간접적으로, 특히 신원확인번호(an identification number)나 그의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 동일성(identity)을 고유하게 나타내는 하나 또는 그 이상의 요소를 참조하여 그 신원이 확인될 수 있는 사람을 가리킨다.”⁵⁸⁴⁾

영국의 개인정보보호법(Data Protection Act 1998)도 “신원확인이 가능한 개인기록”이라는 개념을 사용하고 있다. 즉 “개인기록”(personal data)이라 함은 “신원확인이 가능한 생존하는 개인에 관한 기록(data)으로서, (a) 그 기록으로부터, 또는 (b) 당해 개인정보처리자(data controller)가 보유하고 있거나 또는 앞으로 보유하게 될 다른 정보(information)로부터 신원확인이 가능한 것을 말하며, 그리고 이 개인기록에는 당해 개인에 관한 일체의 의견표명 및 당해 개인과 관련해서 개인정보처리자나 그 밖의 다른 사람이 드러낸 일체의 의견이 모두 포함된다.”⁵⁸⁵⁾

우리의 입법예고안은 일본의 개인정보보호법에서 규정하고 있는 개념규정과 유사하다. 일본의 개인정보보호법은 “이 법률에서 개인정보라 함은 생존하는 개인에 관한 정보로서, 당해 정보에 포함되어 있는 성명, 생년월일 그 밖의 記述 등에 의하여 특정의 개인을 식별할 수 있는 것(다른 정보와 용이하게 대조할 수 있고, 그로써 특정의 개인을 식별할 수 있도록 되어 있는 것을 포함한다)을 말한다.”(제2조 제1항)고 규정하고 있다.

그러나 일본의 개인정보보호법은 “당해 정보에 포함되어 있는” 고 유식별정보(성명, 생년월일 그 밖의 기술 등)를 적시하면서 이러한 고 유식별정보에 의하여 개인의 신원이 확인될 수 있어야 한다고 규정하고 있다. 적어도 일본의 법률은 “당해 정보에 포함되어 있는”이라는

584) EU 95/46/EC, 제2조 (a)항.

585) Data Protection Act 1998, 제1조 제1항.

표현을 사용함으로써 개인정보의 묶음, 즉 “개인기록”의 개념을 상정하고 있고 또 그 기록 안에 고유식별정보가 포함되어야 한다고 규정하고 있다. 이 같은 일본의 개념규정과 거의 유사하게 규정하고 있는 것이 현행의 「공공기관의 개인정보보호에 관한 법률」이다. 동법 제2조 제2호는 “개인정보라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.”고 규정하고 있다.

그런데 입법예고안은 “해당 정보에 의하여 개인을 식별할 수 있는 정보”라고 표현함으로써 마치 개인정보 하나하나 그에 의해 개인을 식별할 수 있어야 하는 것처럼 표현하고 있다. 이 개념규정 속에는 개인정보의 묶음, 즉 “개인기록”이라는 개념이 상정되어 있지 않을 뿐만 아니라, “고유식별정보”의 개념 또한 상정되어 있지 않다. 이러한 개념규정은 개인정보처리의 현실을 반영하지 못하는 개념규정이다. 또한 괄호 속의 표현, 즉 “해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다.”는 문언은 그 의미가 상당히 불명확하다. 어떤 개인정보의 수집과 처리가 법의 규율대상이 되는지 그 입법기준을 보다 분명하게 제시하는 것이 법문의 이해가능성과 규율의 예측가능성을 높인다는 관점에서 타당할 것이다. 따라서 다음과 같은 수정대안을 제시한다.

[수정대안]

“개인정보”란 생존하는 개인에 관한 정보 또는 그 정보의 묶음으로서, 그 정보 속에 포함되어 있는 개인의 성명, 식별번호나 부호, 또는 지문·사진·화상과 같은 당해 개인에게 고유한 식별자에 의하여 개인을 식별할 수 있는 정보를 말한다. 이 개인정보에는 당해 개인에

관하여 내린 다른 사람의 평가나 의견이 모두 포함된다.

제 3 절 “개인정보파일” 개념의 중요 의의와 용어선택의 부적합성

입법예고안은 제2조 제4호에서 “개인정보파일”의 개념을 도입하고 있다. “개인정보파일이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.”고 규정하고 있다. 이는 물론 개인정보데이터베이스(개인정보 DB) 혹은 개인정보처리시스템을 가리킨다.

이러한 개인정보데이터베이스는 개인정보보호법제에서 매우 중요한 개념이다. 외국의 입법례들은 모두 “개인정보데이터베이스”의 개념을 가지고 있다. 개인정보데이터베이스란 각 개인에 관한 정보들이 담긴 수많은 개인기록들(records)을 일정한 기준에 의해 검색할 수 있도록 조직화해 놓은 것을 말한다. 즉, 개인기록들의 체계적인 묶음(system of records)이다. 이 개념이 중요한 의미를 지니는 까닭은 개인정보의 오·남용의 문제는 대부분 이 개인정보데이터베이스의 구축·운용과 관련해서 일어나기 때문이다.

때문에 외국의 개인정보보호법들은 그 적용범위를 개인정보데이터베이스에 의하여 처리되는 또는 처리될 개인정보에 한정하고 있다. 또한 OECD 8대 원칙 중의 하나인 시스템공개의 원칙(Openness Principle)을 구체화하는 개인정보데이터베이스 등록제를 채택함에 있어서, 또는 개인정보영향평가제를 도입함에 있어서 그 전제되는 개념이 “개인정보데이터베이스”의 개념이다. 이 개인정보데이터베이스 내지 개인정보처리시스템은 컴퓨터를 이용한 전자적 데이터베이스일수도 있고 수동적인 작업에 의한 수기파일일 수도 있다. 미국과 일본, 그리고 유럽은 두 시스템을 모두 규율의 대상으로 고려하고 있지만, 수기파일에 대해서는 약간 다른 입장들을 취하고 있다.

우선, 유럽연합의 개인정보보호지침(95/46/EC)은 “개인기록파일링시스템”(personal data filing system)이라는 용어를 채택하고 있다. “개인기록편철시스템”이라고도 번역할 수 있을 것이다. 동 지침 제2조 (c)호는 “개인기록파일링시스템(personal data filing system)이라 함은 특정한 기준(specific criteria)에 따라 접근할 수 있도록 조직화된 개인기록의 묶음(any structured set of personal data)을 말한다. 이 경우 그 묶음이 기능적으로 또는 지리적으로 한 곳에 통합되어 있든, 여러 곳에 분산되어 있든 그것은 문제 삼지 않는다.”고 규정하고 있다. 이 개념 규정에서 컴퓨터에 의한 전자적 처리를 언급하고 있지 않은 것은 수기처리도 포함하기 위한 것이다. 실제로 동 지침 제3조 제1항은 지침의 적용범위를 이렇게 규정하고 있다: “이 지침은 그 처리의 전부 또는 일부가 자동수단(automatic means)에 의하여 이루어지는 개인기록의 처리에, 그리고 자동수단 이외의 방식에 의한 개인기록의 처리가 개인기록파일링시스템의 일부를 이루고 있거나 또는 예정되어 있는 그러한 개인기록의 처리에 적용된다.”

영국의 개인정보보호법은 “관련파일링시스템”(relevant filing system)이라는 용어를 채택하고 있지만, 그 개념내용은 위 유럽연합의 지침과 동일하다(제1조 제1항).

한편, 미국의 공공부문 개인정보보호법인 『프라이버시법』은 “개인기록시스템”(system of records)이라는 용어를 채택하고 있다: “개인기록시스템이라 함은 특정 행정기관이 관리하는(under the control) 개인기록들의 집합(a group of any records)으로서, 개인의 이름 또는 식별번호나 식별부호 혹은 기타 개인에게 고유한 식별자에 의하여 정보를 검색하도록(retrieve) 되어 있는 것을 말한다.”⁵⁸⁶⁾

또한 일본의 민간부문 개인정보보호법은 “개인정보데이터베이스 등”의 용어를 채택하고 있다. 동법 제2조 제2항은 이렇게 규정하고 있다:

586) 5 U.S.C. 552a(a)(5)

“이 법률에서 개인정보데이터베이스 등이라 함은 개인정보를 포함한 정보의 집합물로서 다음 각 호의 1에 해당하는 것을 말한다. 1. 특정의 개인정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것 2. 전호의 것 이외에, 특정의 개인정보를 용이하게 검색할 수 있도록 체계적으로 구성한 것으로서 정령으로 정하는 것.” 여기서 “데이터베이스”라는 용어는 전자계산기를 이용한 자동처리의 개념만을 지칭하는 것이며, 수기파일은 별도로 정령으로 정하는 범위 내에서 이 법의 적용대상으로 삼아 “등”이라는 용어로 포섭시키고 있다.

우리의 현행 『공공기관의 개인정보보호에 관한 법률』도 개인정보데이터베이스 내지 개인정보처리시스템의 개념을 나타내는 용어로 “개인정보화일”이라는 표현을 채택하고 있다. “개인정보화일이라 함은 특정개인의 신분을 식별할 수 있는 사항에 의하여 당해 개인정보를 검색할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 컴퓨터의 자기테이프·자기디스크 기타 이와 유사한 매체에 기록된 것을 말한다.”(제2조 제4호). 다만, 이 법률은 수기파일에 대해서는 처음부터 그 적용을 배제하고 있다(제1조).

입법예고안이 이러한 개인정보데이터베이스 내지 개인정보처리시스템의 개념을 채택하고 있고 그에 의해 처리되는 개인정보를 보호하는 것으로 그 적용범위를 제한적으로 설정하고 있는 것은 매우 타당해 보인다. 개인정보 오·남용의 문제는 대부분 이 개인정보데이터베이스의 구축·운용과 관련해서 일어나는 것인데, 그렇지 않고 개인정보의 ‘개별적인’ 수집·이용·제3자 제공까지 개인정보 보호의 이름으로 규율한다면, ‘보호와 이용의 균형’을 현저히 상실한 지나친 보호일 뿐만 아니라 그 사회적 결과는 치명적일 것이다. 예컨대, 친구에게 선물을 보내기 위해 그 친구의 주소를 다른 친구에게 물어 수집하고 이를 이용하여 선물을 보내는 경우와 같은 ‘개별적인 수집·이용’에 대해 굳이 개인정보보호법에서 규율할 필요는 없는 것이다. 만일 이러한

‘개별적인 수집·이용·제3자 제공’에 대해서까지 개인정보보호법으로 규율한다면, 그리하여 개별적인 수집에 있어서 정보주체의 동의나 다른 정당한 사유의 존재를 요구한다든지 또는 사전 또는 사후의 고지의무를 부과하게 된다면 사회의 정상적인 기능은 아마도 심각하게 마비현상을 보일 것이다.

물론 ‘개별적인 수집’이 개인의 사생활 내지 프라이버시를 침해하는 경우가 있을 수 있다. 예컨대, 일반적으로 용인되기 어려울 정도로 특정 개인을 추적·감시(tracing & surveillance)하여 개인의 일거수일투족에 관한 정보를 수집한다면 그 추적·감시행위의 위법성을 인정할 수 있을 것이다. 이러한 행위는 그 자체로 민사상의 불법행위책임을 지게 될 것이다.⁵⁸⁷⁾ 또 특정 개인의 숨기고 싶은 은밀한 비밀을 제3자에게 알려(제3자 제공) 그 개인의 사생활 내지 프라이버시를 심각하게 훼손하는 경우에도 또한 민사상의 불법행위책임을 지게 될 것이다.

요컨대, ‘개별적인 수집·이용·제3자 제공’은 개인정보보호법의 규율대상이 될 필요가 없고 또 그러해서도 안 된다. 따라서 그러한 행위는 일반적으로 허용되며, 다만 그 행위의 태양이 우리 사회가 용납할 수 없을 정도로 지나친 경우에는 민사 불법행위의 일반 법리에 의해서 규율되어지게 된다.

그런데 제17대 국회에 제출되었던 『이은영 법안』은 개인정보데이터베이스 내지 개인정보처리시스템의 개념을 아예 채택하지 않고 있었기 때문에, ‘개별적인 수집·이용·제3자 제공’에까지 그 규율이 적용되는 것으로 예정하고 있었다. 다행히 입법예고안은 개인정보데이터베이스의 개념을 채택하고 있고, 법률의 적용범위를 데이터베이스의

587) 국군보안사 민간인사찰 사건(대법원 1998. 7. 24 선고 96다42789 판결)에서 대법원은 국군보안사령부가 군과 관련된 첩보 수집, 특정한 군사법원 관할 범죄의 수사 등 법령에 규정된 직무범위를 벗어나 민간인들을 대상으로 평소의 동향을 감시·파악할 목적으로 지속적으로 개인의 집회·결사에 관한 활동이나 사생활에 관한 정보를 미행, 망원 활용, 탐문채집 등의 방법으로 비밀리에 수집·관리한 경우, 이는 헌법에 의하여 보장된 기본권을 침해한 것으로서 불법행위를 구성한다고 판단하였다.

형태로 개인정보를 처리하는 경우에 한정하고 있다. 매우 타당하고 적절한 입법안이라고 평가된다.

다만, 개인정보데이터베이스 내지 개인정보처리시스템을 지칭하는 용어로 사용하는 “개인정보파일”이라는 표현은 디지털시대를 반영하지 못하는 부적절한 표현인 것으로 평가된다. 사실 “파일”이라는 용어는 손으로 작성된 ‘수기파일’이라는 표현에서 어울리는 용어이다. 컴퓨터 등에 의한 전자적 처리시스템을 지칭하는 용어로는 ‘데이터베이스’라는 표현이 더 적절하다.⁵⁸⁸⁾

때문에 일본의 개인정보보호법은 전자적 데이터베이스와 수기파일을 함께 나타내기 위하여 “개인정보데이터베이스 등”이라고 표현하고 있다. 따라서 입법예고안에서처럼 수기파일까지 포함하고자 한다면, “개인정보처리시스템”이라는 표현이 적정한 것으로 평가된다. 입법예고안에서 개인정보의 수집·기록·저장·검색·이용·제공 등 개인정보를 다루는 일체의 작용을 포괄적으로 묶어 “처리”라는 용어로 나타내고 있다는 점에서도 그러하다.

그리고 입법예고안에서 “개인정보파일”의 개념규정에는 데이터베이스 구축이나 정보검색에 이용되는 ‘고유식별자’의 요소가 빠져 있다. 위에서 본 바와 같이, 미국이나 유럽의 개인정보보호법과 우리의 현행 『공공기관의 개인정보보호에 관한 법률』에서는 모두 ‘고유식별자’의 요소를 포함하고 있다. 그리하여 수정대안을 제시하면 다음과 같다.

588) 현행의 여러 법령에서는 전자적 정보처리시스템을 가리키는 표현으로서 “데이터베이스”라는 용어를 채택하여 사용하고 있다: ① 『국가지리정보체계의 구축 및 활용 등에 관한 법률』 제15조 - “지리정보 데이터베이스”; ② 『공직후보자에 관한 정보의 수집 및 관리에 관한 규정』(대통령령) 제2조 - “국가인재데이터베이스”; ③ 『물류정책기본법』 제30조 - “국가물류통합데이터베이스”; ④ 『실종아동 등의 보호 및 지원에 관한 법률』 제8조 - 실종아동 등의 신상정보데이터베이스; ⑤ 『저작권법』 제2조 제19호(“데이터베이스는 소재를 체계적으로 배열 또는 구성한 편집물로서 개별적으로 그 소재에 접근하거나 그 소재를 검색할 수 있도록 한 것을 말한다.”).

[수정대안]

“개인정보처리시스템”이라 함은 개인의 성명, 식별번호나 부호, 또는 지문·사진·화상과 같은 당해 개인에게 고유한 식별자에 의하여 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다. 이 경우 개인정보들이 기능적으로 또는 지리적으로 한 곳에 통합되어 있든, 여러 곳에 분산되어 있든 그것은 문제 삼지 아니한다.

제 4 절 “처리”의 개념규정의 적정성

입법예고안 제2조 제2호는 “처리란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위를 말한다.”고 규정하고 있다.

개인정보보호법이 규율대상으로 삼는 기본적인 행위는 개인정보를 수집, 이용, 제공하는 행위이다. 이 과정에서 수집된 개인정보를 개인정보처리시스템에 기록, 저장, 수정, 검색, 삭제 등의 작용이 이루어지게 된다. 이처럼 개인정보를 다루는 일체의 작용을 포괄적으로 묶어 “처리”라는 개념을 사용하는 것은 적정한 것으로 평가된다.

이러한 접근방식은 유럽연합의 개인정보보호지침과 유사하다. 유럽연합의 개인정보보호지침(95/46/EC)은 이들 일련의 행위들을 “처리”(processing)라는 단일의 개념으로 묶어 일괄적으로 규율하는 방식을 취하고 있다. 동 지침 제2조 (b)호는 “개인정보처리(processing of personal data)라 함은 자동수단에 의한 것이든 아니든 개인기록(personal data)에 가해지는 일체의 작용(any operation or set of operations)을 가리킨다. 예컨대, 수집(collection), 기록(recording), 편성(organization), 저장(storage), 수정(adaptation or alteration), 검색(retrieval), 참조(consultation), 이용(use), 전송·공표 기타의 제공 방식에 의한 공개(disclosure by transmission,

dissemination or otherwise making available), 배열이나 조합(alignment or combination), 접근차단(blocking), 삭제(erasure) 또는 파괴(destruction)를 말한다.”고 규정하고 있다.

그러나 독일의 연방개인정보보호법은 “정보처리”라는 단일의 개념을 채택하지 않고, “수집”(Erheben; collection), “처리”(Verarbeiten; processing), “이용”(Nutzen; use)이라는 개념을 구분하여 규정하고 있다. 여기서 “처리”(Verarbeiten)라 함은 “개인정보의 저장(Speichern; storage), 수정(Verändern; modification), 제공(Übermitteln; communication), 접근차단(Sperren; blocking) 그리고 삭제(Löschen; erasure)”를 말한다(제3조 제4항). “이용”(Nutzen)이라 함은 “처리 이외에 개인정보를 활용하는 것”을 말한다(제3조 제5항).

한편, 일본의 개인정보보호법은 “정보처리”라는 용어 대신에 포괄적인 개념으로 “취급”이라는 용어를 채택하고 있다. 그러나 “취급”의 용어에 대한 명시적인 개념규정을 두고 있지는 않다. 다만, 법문에서는 “취급”이라는 일반적 용어 외에 그때그때 상황에 따라 “취득”, “이용”, “제3자 제공”, “개시”, “정정” “이용의 정지” 등의 표현을 사용하고 있다.

우리나라의 경우에는 그 동안의 개인정보보호법제에서 “처리”라는 용어를 사용해 왔다. 『공공기관의 개인정보보호에 관한 법률』도 “처리”의 개념규정을 두고 있고,⁵⁸⁹⁾ 『신용정보의 이용 및 보호에 관한 법률』 제2조 제12호도 “처리”라는 개념을 규정하고 있으며,⁵⁹⁰⁾ 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』도 “처리”라는 용어의 개념

589) 제2조 제3호 : “처리”라 함은 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치(이하 “컴퓨터 등”이라 한다)를 사용하여 정보의 입력·저장·편집·검색·삭제 및 출력 기타 이와 유사한 행위를 하는 것을 말한다. 다만, 문장만을 작성하는 등의 단순업무처리를 위한 행위로서 대통령령이 정하는 행위를 하는 것을 제외한다.

590) 제2조 제12호 : “처리”라 함은 컴퓨터를 이용하여 신용정보를 입력·저장·가공·편집·검색·삭제·출력하는 행위, 신용정보를 배달·우송·전송 등의 방법으로 타인에게 제공하는 행위 기타 이와 유사한 행위를 말한다.

정의를 하고 있지는 않지만 개인정보와 관련해서 “처리”라는 표현을 사용하고 있다. 요컨대, 개인정보보호법의 규율의 대상이 되는 행위를 포괄적으로 지칭하는 용어로 “처리” 또는 “정보처리”라는 표현방식이 가장 적절한 것으로 평가된다.

제 5 절 개인정보처리자와 정보처리대행자의 개념구분의 필요성

1. 개인정보처리자의 개념규정에 대한 평가와 수정대안

개인정보보호법의 규율을 받는 수범자로서 법률이 정하는 기준에 따른 정보처리의 의무와 책임을 지는 자를 어떻게 규정할 것인가가 문제된다. “개인정보를 처리하는 자”(개인정보처리자)는 일반적인 권리·의무의 주체, 즉 법인격자(자연인 또는 법인)와는 그 개념이 완전히 일치하지 않는다. 특히 공공부문에서 각 공공기관은 자신의 소관 업무에 따라 독자적으로 개인정보처리시스템을 구축·운영하고 있기 때문에, 이 때 각 공공기관(“행정청”)은 그 자체가 단독으로 개인정보보호법의 수범자가 된다.

그런데 개인정보보호법에서 개인정보처리자의 “단위범위”를 명확히 설정하는 것은 매우 중요한 문제이다. 단위범위 내의 자체적인 이용인지 아니면 제3자 제공인지 여부에 따라 규율내용이 달라질 수 있기 때문이다. 판단컨대, 개인정보보호법의 의무와 책임을 독자적으로 지는 기본단위를 나타내는 표현으로 “개인정보처리자” 또는 “개인정보처리기관”이라는 용어를 사용하는 것이 적절해 보인다.

현행의 「공공기관의 개인정보보호에 관한 법률」은 “보유기관”이라는 용어를 사용하고 있고, 보유기관이라 함은 “개인정보파일을 작성 또는 취득하거나 유지·관리하는 기관(개인정보의 처리를 다른 기관·단체 등에 위탁하는 경우를 포함하되, 다른 기관·단체 등으로부

터 위탁받은 경우를 제외한다)”이라고 정의하고 있다(제2조 제6호 및 제7호). 이는 미국의 공공부문 개인정보보호법인 『프라이버시법』의 개념규정에 영향을 받은 것으로 보인다.⁵⁹¹⁾ 그러나 개인정보를 “가지고 있다”는 우리의 통상적인 의미의 “보유자”라는 개념으로는 개인정보보호법의 의무와 책임을 지는 주체를 나타내는 데에는 적절하지 못한 것으로 평가된다. 정보처리를 대행하는 자도 개인정보를 보유하는 것이기 때문이다. 사실상 미국의 “보유”의 개념은 우리의 “처리”에 대응하는 것이기 때문에 “개인정보처리자” 또는 “개인정보처리기관”이라는 표현이 적절한 것으로 평가된다. 입법예고안은 “개인정보처리자”의 용어를 채택하고 있다. 이하에서는 개인정보보호법의 의무와 책임을 독자적으로 지는 기본단위를 나타내는 용어로 “개인정보처리자”라는 표현을 일관되게 사용하기로 한다.

그런데 이런 표현의 문제보다 더 중요한 문제는 누가 “개인정보처리자”가 되는가, 다시 말해서 개인정보처리자를 어떻게 개념정의할 것인가 하는 문제이다. 개념정의에 따라서 개인정보보호법의 규율대상자의 범위가 달라질 수 있기 때문이다.

입법예고안 제2조 제5호는 다음과 같이 정의를 내리고 있다: “개인정보처리자란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 타인을 통하여 개인정보를 처리하는 자를 말한다.” 우선 이러한 개념정의를 외국의 입법례와 비교해 볼 필요가 있다.

먼저, 유럽연합의 개인정보보호지침(95/46/EC)은 공공부문과 민간부문의 개인정보처리자를 포괄적으로 나타내는 표현으로 “controller”라는 용어를 채택하면서, 그 개념규정을 이렇게 하고 있다: “개인정보처리자(controller)라 함은 단독으로 또는 타자와 공동으로 개인정보처리

591) 미국의 『프라이버시법』은 “보유한다”(maintain)라는 개념을 채택하고 있다: “보유한다(maintain)라고 함은 보유하거나(maintain), 수집하거나(collect), 이용하거나(use), 또는 제공(disseminate)하는 것을 말한다.” 5 U.S.C. 552a(a)(3).

의 목적과 수단을 결정하는 자연인이나 법인(natural or legal person), 공공기관(public authority or agency) 또는 기타 단체(any other body)를 말한다.”(제2조 (d)항). 요컨대, 개인정보처리자는 “개인정보를 처리하는 목적과 수단을 결정하는 자”로서, 정보처리의 주체이면서 동시에 개인정보보호법의 의무와 책임의 주체이기도 하다.

영국의 개인정보보호법도 유럽연합의 지침을 그대로 따르고 있다. “개인정보처리자(data controller)라 함은 단독으로 또는 타자와 공동으로 개인정보가 처리되는 목적과 방법을 결정하는 자를 말한다.”(제1조 제1항). 그리고 “법령에 근거하여 정보처리가 행해지는 경우에는 당해 법령으로부터 그 정보처리의 의무를 부여받은 자가 개인정보처리자(data controller)가 된다.”(제1조 제4항).

독일의 연방개인정보보호법은 개인정보처리자를 나타내는 표현으로 “verantwortliche Stelle”라는 용어를 사용하고 있다. “책임 있는 기관”으로 직역될 수 있을 것이나, “개인정보처리기관”이라는 번역술어를 사용하는 것이 더 적절해 보인다. “개인정보처리기관(verantwortliche Stelle)이라 함은 자체적으로 개인기록을 수집, 처리 또는 이용하거나 또는 자신을 대신해서 타인에게 그 일을 맡기는 자 또는 기관(Person oder Stelle)을 말한다.”(제3조 제7항).

한편, 일본의 경우 민간부문 일반법으로서의 성격을 가지고 있는 개인정보보호법에서는 “개인정보취급사업자”라는 표현을 사용하고 있다. 일본은 이 “개인정보취급사업자”의 개념규정에서 법의 적용범위를 함께 정하고 있다. “개인정보취급사업자라 함은 개인정보데이터베이스 등을 사업용으로 이용하고 있는 자를 말한다. 다만, 다음의 者를 제외한다. 1. 국가기관 2. 지방자치단체 3. 독립행정법인등 (독립행정법인등이보유하는개인정보의보호에관한법률[2003년 법률 제59호] 제2조 제1항에 규정된 독립행정법인등을 말한다. 이하 같다.) 4. 그 취급하는 개인정보의 양 및 이용방법에 비추어 개인의 권리이익을 해할 우려가

적은 것으로서 정령에서 정하는 자.”(제2조 제3항).

이처럼 일본의 민간부문 개인정보보호법은 개인정보를 “대량으로 취급하는 사업자”만을 규율의 대상으로 정하고 있다. 법문에서 “사업용으로 이용하고 있다”고 하는 것의 의미는, 단순히 일정한 목적을 가지고 계속·반복적으로 동종의 행위를 수행하는 것만으로는 충분하지 않고, 그 행위가 사회성을 띠므로써 사회적인 맥락에서 사업이라고 인정될 수 있는 것을 말한다.⁵⁹²⁾ 따라서 연하장 등을 발송하는 등 개인의 사적인 활동이라면 그 활동이 계속·반복적인 것이라 하더라도 여기의 개인정보취급사업자에 해당하지 않고, 따라서 본 법률의 규율을 받지 않는다.

이상의 비교법적 관점에서 볼 때, 입법예고안은 두 가지 점에서 외국의 입법례와 차이가 있다. 첫째, 입법예고안은 개인정보보호법의 규율을 받는 책임단위를 나타내는 개념요소로서 ‘개인정보파일(개인정보처리시스템)을 운용하는 자’라는 개념을 채택하고 있다. 그런데 ‘운용’의 의미가 다소 불분명하다. 보다 명확하게 하기 위해서는 ‘개인정보파일을 자신의 책임 하에 관리·운용하는 자’라는 개념이 더 적절해보인다. 나아가, 의무와 책임의 주체라는 점을 보다 분명히 드러내기 위해서는 유럽연합과 영국처럼 “개인정보처리의 목적과 수단을 결정하는 자”라는 개념요소가 들어가는 것을 고려해 볼 필요가 있다.

둘째, 입법예고안은 규율대상자의 범위를 나타내는 개념요소로서 “업무를 목적으로 개인정보파일을 운용하는 자”라는 개념을 채택하고 있다. 일본의 민간부문 개인정보보호법이 “개인정보데이터베이스 등을 사업용으로 이용하고 있는 자”라는 개념을 사용하고 있는 것과는 다소 다르다. 우리의 입법예고안은 공공부문과 민간부문을 모두 포함하는 법률이기 때문에 ‘사업’이라는 단어를 쓰기보다는 ‘업무’라는 용어

592) 三上明輝, “個人情報保護に関する法律の概要”, 『ジュリスト』1253號(2003. 10. 1), 27頁.

를 사용한 것으로 보인다.

그런데 이 “업무”의 개념이 다소 불명확하여 사후의 적용과정에서 약간의 혼란을 초래할 수 있는 것으로 판단된다. 우리의 현행 법질서에서 “업무”에 대한 해석을 보면, 형법의 업무방해죄에서 “업무”라 함은 “직업 또는 계속적으로 종사하는 사무나 사업”을 말한다고 대법원은 해석하고 있다.⁵⁹³⁾ 그런데 ‘일정한 목적을 가지고 계속 반복적으로 동종의 행위를 수행하는 것’이라는 의미의 “업무” 개념에는 예컨대 개인이 사적으로 연하장 발송업무를 위해 개인정보파일을 운영하는 것도 포함될 수 있다. 그렇지만 ‘개인의 순전한 사적 업무’는 여기에서 제외되는 것이 타당할 것으로 판단된다. 이런 경우에는 개인정보의 오·남용에 따른 위험성이 극히 적을 뿐만 아니라 이런 사적인 업무 수행에 필요한 개인정보의 수집과 이용에 대해서까지 동의획득 또는 고지의 의무를 부과하는 것은 결코 타당하지 않기 때문이다.

한편, 일본의 개인정보보호법처럼 민간의 경우 처리되는 개인정보가 소량인 경우에까지 개인정보보호법의 규율대상으로 할 것인지는 정책 판단의 문제이다. 이 문제는 법률에서 명시적으로 규정하기보다는 일정한 기준을 제시하면서 대통령령에 위임하는 것이 적절한 것으로 평가된다.

[수정대안]

“개인정보처리자”라 함은 업무를 수행할 목적으로 개인정보처리시스템을 자신의 책임 하에 관리·운용하는 자로서 개인정보처리의 목적·내용·방법을 결정하는 자연인, 법인, 공공기관 또는 그 밖의 단체를 말한다. 다만, 처리하는 개인정보의 양과 이용방법에 비추어 정보주체의 권리나 이익을 해할 우려가 적은 경우로서 대통령령이 정하는 자는 제외한다.

593) 대법원 2006. 3. 9 선고 2006도382 판결

2. 정보처리대행자의 개념설정 및 책임소재규정의 필요성

한편, 개인정보처리자 개념과는 별도로 그의 지시를 받아 단순히 정보처리를 대행하는 자(“정보처리대행자”)의 개념을 상정할 필요가 있다. 그리하여 양자의 법적 책임관계를 분명하게 하여야 한다. 그런데 입법예고안에는 개인정보처리자의 정의규정 중에 “타인을 통하여”라는 개념요소로써 정보처리대행자의 개념을 소극적으로 상정해 놓고 있을 뿐 “정보처리대행자”의 개념을 적극적으로 명시하고 있지 않으며, 그 책임에 관한 규정도 달리 두고 있지 않다. 입법예고안 제25조는 “업무위탁에 따른 개인정보의 처리 제한”이라는 제목 하에 업무수탁자의 개인정보처리에 관하여 규율하고 있는데, 그러나 이는 정보처리대행자에 관한 규정이 아니다.

유럽연합의 개인정보보호지침은 개인정보처리자의 지시를 받아 정보처리를 대행하는 자의 개념을 설정하고 있다. 정보처리대행자를 나타내는 말로 “processor”라는 용어를 사용하고 있다: “정보처리대행자(processor)라 함은 개인정보처리자(controller)를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공기관 또는 그 밖의 단체를 말한다.”(제2조 (e)항). 마찬가지로 영국의 개인정보보호법도 정보처리대행자의 개념을 규정해 놓고 있다: “정보처리대행자(data processor)라 함은 개인정보처리자의 직원 이외에 개인정보처리자를 대신하여 정보를 처리하는 자를 말한다.”(제1조 제1항).

정보처리를 위탁한 경우 그 수탁자에 의한 정보처리의 오·남용에 따르는 책임관계를 분명히 하기 위한 입법방안으로는 (i) “정보처리대행자”의 법적 지위를 “개인정보처리자”에 종속되는 존재로 규정하거나(유럽의 경우), 혹은 (ii) 적어도 개인정보처리자에게 감독책임을 부여하는 방안(일본의 경우)을 검토해 볼 수 있다.

유럽의 개인정보보호법은 정보처리를 위탁한 경우에 정보처리와 관련한 법적 책임과 의무는 그 처리를 위탁한 자, 즉 개인정보처리의 목적과 수단을 결정하는 자인 개인정보처리자에게 지우고 있다. 유럽연합의 개인정보보호지침(95/46/EC) 제16조는 “정보처리의 종속성”이라는 제목 하에 다음과 같이 규정하고 있다.

제16조(정보처리의 종속성) 개인정보처리자(controller)나 정보처리대행자(processor)의 지시를 받아 개인정보에 접근하는 권한을 가진 사람(정보처리대행자 본인도 포함)은 누구든지 개인정보처리자의 지시에 의하지 않고서는 개인정보를 처리해서는 안 된다. 다만, 법률이 달리 요구하고 있는 때에는 그러하지 아니하다.

또한 동 지침 제17조 제3항은 정보처리의 위탁을 받드시 “계약”에 의해서만 하도록 하고, 그 계약에서 정보처리대행자는 개인정보처리자의 지시에 따라서만 업무를 수행한다는 점을 명시하도록 하고 있다.

제17조(정보처리의 안전성) (3) 정보처리대행자에 의한 정보처리의 수행은 그 대행자를 구속하는 계약(contract)이나 법률행위(legal act)에 의하여 규율되어야 하고, 이 때 그 계약은 특히 다음의 사항을 규정하고 있어야 한다.

- (i) 정보처리대행자는 개인정보처리자의 지시(instructions)에 의해서만 행동한다는 점
 - (ii) 제1항의 의무는, 당해 정보처리대행자가 존재하는 회원국의 법률이 정하는 바에 따라, 정보처리대행자에게도 똑 같이 부과된다는 점
- (4) 증거의 보존을 위해서, 위탁계약 중 개인정보보호에 관한 부분 및 제1항에서 규정된 안전조치에 관한 요구사항들은 서면 또는

그 밖에 그에 상응하는 형식으로 작성되어야 한다.

또한 영국의 개인정보보호법도 제1부칙 제2절 제12조에서 유럽연합의 지침과 같은 취지의 규정을 두고 있다.

12. 정보처리가 정보처리대행자에 의하여 수행되는 경우, 개인정보처리자는 다음의 요건을 갖추지 못하면 제7원칙⁵⁹⁴⁾을 준수한 것으로 간주되지 않는다. [적어도 다음의 요건을 갖춘 때에 한하여 제7원칙을 준수한 것으로 인정될 수 있다.]

- (a) 정보처리대행자에 의한 정보처리의 수행은 (i) 서면으로 작성된 계약에 의하여 이루어지고, (ii) 그 계약상 정보처리대행자는 개인정보처리자의 지시(instructions)에 의해서만 행동할 것, 그리고
- (b) 그 계약에는 제7원칙에 의해 개인정보처리자가 지는 의무와 동등한 의무를 정보처리대행자도 진다는 내용이 포함될 것.

한편, 유럽과 달리 일본의 개인정보보호법은 단순히 정보처리대행자에 대한 개인정보처리자의 감독책임을 규정하고 있다. 유럽에 비하면 정보처리대행자의 종속성을 약하게 규정하고 있다고 하겠다.

제22조(수탁자에 대한 감독) 개인정보취급사업자는 개인데이터의 취급의 전부 또는 일부를 위탁한 경우에 그 취급을 위탁한 개인데이터의 안전관리가 도모될 수 있도록 위탁을 받은 자에 대한 필요하고 적절한 감독을 하여야 한다.

594) 제7원칙은 소위 “보안의 원칙”을 말하는 것으로, 개인정보보호법 제1부칙 제1절 제7조에 규정되어 있다: “권한 없는 또는 불법적인 정보처리가 행해지지 않도록, 그리고 개인기록이 뜻밖에 소실되거나 파괴되거나 손상되지 않도록 적절한 기술적 및 조직적 조치(appropriate technical and organizational measures)가 취해져야 한다.”

제 6 절 “동의”의 개념규정 신설의 필요성

입법예고안은 정보주체의 동의를 개인정보의 수집·이용·제3자 제공의 합법성 기준의 하나로 명시하고 있다. 그러나 입법예고안에는 어떤 승낙의 의사표시가 “동의”에 해당하는지에 대해 정의규정을 두고 있지는 않다. 그런데 정보주체가 어떤 방식으로 정보처리를 승낙하는 것이 이 “동의”의 요건을 충족하는 것으로 볼 것인지가 문제되는 경우가 흔히 있다. 이 때문에 유럽연합의 개인정보보호지침(95/46/EC)은 승낙의 의사표시에 ‘임의성’, ‘명확성’, 그리고 ‘충분한 인식’의 세 가지 요소가 포함되어야 적법한 “동의”로 보고 있다. 동 지침 제2조 (h)호는 다음과 같이 규정하고 있다.

(h) “정보주체의 동의”(the data subject’s consent)라 함은 자신의 개인 정보가 처리되는 것을 승낙한다는 것을 나타내는 의사의 표시로서, 정보주체가 사전에 잘 알고 임의로 내린 분명한 의사표시(any freely given specific and informed indication)를 말한다.

우리도 이러한 유럽연합의 “동의”의 개념정의를 수용할 필요가 있는 것으로 판단된다. 향후 법률의 적용과정에서 동의의 존재 여부를 판단하는 법적 기준을 제시해 줄 필요가 있기 때문이다.⁵⁹⁵⁾

다만, 입법예고안 제21조는 동의를 받는 방법에 관하여 규정하고 있다: 선택적 동의가 가능하도록 함(제1항), 광고목적의 처리에 대해서 명확히 인식할 수 있도록 알리고 동의를 받아야 함(제2항), 민감정보

595) 온라인상에서 아동의 개인정보보호를 위한 법정대리인의 동의 요건과 관련하여 합리적인 동의획득방식에 관한 입법정책적 방안에 대해서는, 이인호, “아동온라인 개인정보보호법과 그 효율적 집행방안”, □□법과 사회□□ 제20호(법과사회이론학회, 2001. 6) 참조.

와 고유식별정보의 처리에 대한 별도의 동의를 받을 때 일반개인정보의 동의와 구분하여 별도의 동의를 받는다는 점을 명확히 인식할 수 있도록 해야 함(제3항), 법정대리인의 동의방법은 대통령령에 위임(제4항), 기타의 동의획득방법은 수집매체를 고려하여 대통령령에 위임(제5항).

제 3 장 개인정보처리의 입법기준에 대한 평가와 대안제시

제 1 절 정보주체의 동의 요건에 대한 비판

1. 개인정보자기결정권에 대한 오해와 이해

개인정보보호의 문제를 법제화하기 시작한 이래⁵⁹⁶⁾ 지난 10여 년 동안 보호수준과 관련하여 우리 사회에서 가장 논쟁적이었던 이슈를 든다면, 개인정보의 처리(=수집·이용·제공)에 있어서 정보주체의 동의 요건을 합법적인 정보처리의 원칙적인 기준으로 설정할 것인가 하는 문제였다. 다시 말해서, 개인정보처리자는 정보주체의 동의 없이는 타인의 개인정보를 원칙적으로 처리할 수 없도록 해야 하는가? 바꿔 말하면, 정보주체의 동의를 받지 않고 합법적으로 처리(=수집·이용·제공)할 수 있는 경우를 어느 정도 허용할 것인가? 헌법상 인정되는 개인정보자기결정권 내지 자기정보통제권(Recht auf informationelle Selbstbestimmung; Information Privacy)⁵⁹⁷⁾이라고 하는 것이 정보주체의 동의 없는 개인정보의 처리를 원칙적으로 금지시키는 것인가?

596) 개인정보보호를 최초로 법제화한 것은 1994년 1월 7일 공포된 『공공기관의 개인정보보호에 관한 법률』(1995. 1. 8 시행)이었으며, 곧 이어 민간부문에서 『신용정보의 이용 및 보호에 관한 법률』이 1995년 1월 5일 공포되었다(1995. 7. 6 시행). 그리고 온라인상의 개인정보보호를 최초로 법제화한 것은 1999년 2월 8일 기존의 『전산망 보급 확장과 이용촉진에 관한 법률』을 개정하여 정보통신망에서의 개인정보 보호규정을 제4장에서 새로이 신설했던 『정보통신망 이용촉진 등에 관한 법률』(2000. 1. 1 시행)이다.

597) 독일 연방헌법재판소는 1983년의 인구조사판결(BVerfGE 65, 1)에서 “정보적 자기결정권”(Recht auf informationelle Selbstbestimmung)을 처음으로 인정하였다. 이 판결의 법리에 대한 상세하고 유익한 분석은 정태호, “현행 인구주택총조사의 위헌성 - 독일의 인구조사판결(BVerfGE 65, 1)의 법리분석과 우리의 관련법제에 대한 반성 -”, 『법률행정논총』 제20집(전남대학교 법률행정연구소, 2000), 202-218면; 김일환, “독일 연방헌법법원의 인구조사판결”, 김계환교수회갑기념논문집, 1996, 66면 이하 참조.

2005년 5월 26일 헌법재판소는 「주민등록 지문날인제도 사건」⁵⁹⁸⁾에서 처음으로 개인정보자기결정권을 정식으로 인정하는 판시를 하였다. 이 사건에서 헌법재판소는 시장·군수 또는 구청장이 주민등록증을 발급하면서 개인의 지문정보를 수집하고 경찰청장이 이를 보관·전산화하여 범죄수사목적에 이용하는 공권력작용으로 인하여 청구인들의 개인정보자기결정권이 제한되고 있음을 인정하였다.⁵⁹⁹⁾ 이 사건에서 헌법재판소는 “개인정보자기결정권”이란 “자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리”라고 규정하고 있다.

그러나 이러한 개념정의는 자칫 오해를 불러일으킬 수 있다. 마치 수집에서부터 이용 및 제공에 이르기까지 정보주체가 그 과정을 직접적으로 결정하거나 통제할 수 있는 권리인 것처럼 오해될 소지가 있다. 그러나 ‘사생활비밀의 공표’에 대한 통제를 넘어서서, 모든 개인정보의 자체적인 수집·이용과 또 자체적인 이용 목적에 부수하는 제3자 제공에 대하여 정보주체에게 절대적인 결정권 내지 통제권을 부여하는 것이라고 이해되어서는 안 된다. 그러나 최근 우리 사회에서 개인정보보호를 절대화하려는 경향이 발견되고 있다. 이런 경향에 의하면, 정보주체의 동의 없는 개인정보의 수집·이용·제공은 원칙적으로 불법이라고 평가된다. 그러나 이것은 보호와 이용의 균형을 잃은 위험한 사고이다.

개인정보자기결정권은 타인이 행하는 개인정보처리과정에 정보주체가 함께 참여하는 권리이다. 즉 개인정보자기결정권은 “자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 수집·이용·제공되는지를 정보주체가 명확하게 인식하고 그러한 정보처리의 과정에 함께 참여

598) 헌재 2005. 5. 26. 99헌마513등, 판례집 17-1, 668.

599) 헌법재판소는 개인정보자기결정권에 대한 제한은 인정하였지만, 과잉된 제한이 아니라는 이유로 6(합헌) : 3(위헌)으로 합헌결정을 내렸다.

할 수 있는 권리”로 이해되어야 한다. 그러한 참여를 통하여 혹시라도 있을 수 있는 개인정보의 오·남용에 따르는 정보주체의 권리와 이익의 침해를 방지하고자 하는 데 그 존재의의가 있는 것이다.

개인정보가 정보주체의 인격적 징표이지만 그 인격적 징표 그 자체를 가두어두고 보호하려고 해서 안 된다. 사회의 존립과 기능유지는 많은 경우 타인에 대한 정확한 평가에 기초하고 있다. 그리고 타인에 대한 평가가 가능하기 위해서는 그의 인격적 징표가 유통될 수 있어야 한다. 만일 개인정보를 인격적 징표라는 이유만으로, 그리하여 마치 정보주체의 동의 없는 개인정보의 유통의 금지를 인격권의 한 내용으로 오해한다면, 누구든지 자신에게 불리한 인격적 징표의 유통을 금지하고자 할 것이고 그렇게 되면 사회는 그에 대한 정확한 평가를 내리는 것이 불가능하게 될 것이다. 그 종국적 결과는 사회의 정상적인 기능의 마비 내지 위축으로 나타날 것이다.

그 동안 개인의 인격적 이익을 보호하기 위한 민사법제와 형사법제로서 명예훼손법과 사생활보호법이 존재하여 왔다. 또 최근에는 개인의 성명과 초상을 보호하는 법원의 판례가 나오기도 하였다. 그러나 이들 법제와 판례법은 부분적이고 제한적으로만 개인의 인격적 이익을 보호한다.

명예훼손법은 민사법제와 형사법제 모두 개인에 관한 정보 중 그 개인의 사회적 평가를 저하시키는 사실적 정보를 공개적으로 공표하여 그 개인의 명예를 훼손하는 경우에 적용되는 법제이다. 명예훼손법은 개인에 관한 사실적 정보 그 자체를 보호하고자 하는 것이 아니라 그러한 정보의 공표로 인해 훼손되는 인격적 이익인 명예를 보호하고자 하는 법이다. 그리고 이때의 명예도 개인의 명예감정이 아니라 사회적 평가로서의 외부적 명예를 의미한다.

한편 민사법제로서의 사생활보호법은 민사상의 불법행위법으로서 존재하는데, 개인이 숨기고자 하는 은밀한 사생활정보를 공표하거나

또는 개인의 사생활 영역에 무단히 침입하여 평온을 해치는 경우에 손해배상책임을 지우는 법제이다. 우리 대법원은 “사생활의 비밀에 관한 사항을 함부로 타인에게 공개당하지 아니할 법적 이익”을 사생활 권리(프라이버시권)로 인정하고 있을 뿐이다.⁶⁰⁰⁾ 이처럼 대법원이 인정하는 사생활권리라는 것도 개인에 관한 모든 정보를 보호하는 것이 아니라 ‘사생활의 비밀에 관한 정보가 외부에 공개되지 않도록 보호’하는 것이다. 비밀정보 그 자체를 보호한다기보다는 그것이 외부에 공개됨으로써 정보주체가 입게 될 인격적 훼손을 방지하고자 하는 데 기본취지가 있다.

이처럼 명예훼손이나 사생활침해의 경우 그 위법성은 ‘한정된 종류의 사실적 개인정보’(사회적 평가를 저하시킬 수 있는 사실 또는 숨기고자 하는 은밀한 사적인 사실)를 여러 사람에게 널리 ‘공표하는 경우’에 비로소 인정된다. 그리고 설령 그러한 사실의 공표가 있다 하더라도 일정한 사유가 있는 때에는 그 위법성이 인정되지 않는다(위법성조각).

예컨대, 명예훼손의 경우 형법 제310조는 명예훼손적 표현이 “진실한 사실로서 오로지 공공의 이익에 관한 때”에는 위법성이 조각되는 것으로 규정하고 있다. 이 규정에 대해 대법원은 그 동안 언론자유 보장과 명예이익의 보호 사이의 조화를 도모한다는 관점에서 이를 제한적으로 해석하고 있다. 즉 대법원은 1988. 10. 11. 선고, 85다카29 판결(공1988, 1392)에서 “형사상이나 민사상으로 타인의 명예를 훼손하는 행위를 한 경우에도 그것이 ① 공공의 이해에 관한 사항으로서 ② 그 목적이 오로지 공공의 이익을 위한 것일 때에는 ③ 진실한 사실이라는 증거가 있으면 위 행위에 위법성이 없으며 또한 그 증거가 없더라도 행위자가 그것을 진실이라고 믿을 상당한 이유가 있는 경우에는 위법성이 없다.”(번호는 필자 붙임)고 판시한 이래 지금까지 일

600) 대법원 1998. 9. 4. 선고 96다11327 판결.

관되게 위 3가지 요건을 위법성조각요건으로 제시하고 있고, 이는 민사명예훼손과 형사명예훼손에서 모두 동일하게 적용되고 있다.⁶⁰¹⁾

또한 사생활침해의 경우에도 위법성조각사유가 인정되고 있다. 즉 은밀한 사생활정보를 공표한 경우라 하더라도 그 정보가 “공공의 이해와 관련되어 공중의 정당한 관심의 대상이 되는 정보”인 때에는 위법성이 인정되지 않는다.⁶⁰²⁾

요컨대, 지금까지의 명예훼손법과 사생활보호법은 개인정보 중에서도 개인의 사회적 평가를 저하시킬 수 있는 정보나 은밀한 사생활정보에 한정하여 그것도 그러한 정보의 외부적 공개에 대해서만 규율하는 법이다. 또 그 경우에도 일정한 사유가 있는 때에는 위법성을 인정하지 않는다. 이러한 법적 한계 내에서 정보주체의 인격적 이익이 보호되고 있다.

그런데 모든 개인정보를 정보주체의 인격적 징표라는 이유로 해서, 그리하여 타인이 수집·이용·제공하는 나에 관한 정보는 나의 것이라는 과장된 논리로, 만일 정보주체의 동의 없는 개인정보의 수집·이용·제공을 불법으로 금지시킨다거나 당해 정보주체의 인격적 이익을 침해하는 것으로 규정한다면, 이는 인격권에 관한 기존의 법리를 오해한 것일 뿐만 아니라 개인정보의 수집·이용·제공이 가지는 다양한 사회적 이익과 가치를 전혀 고려하지 않은 것이다.

다시 강조하지만, 최근 우리 사회에서 주장되고 있고 또 법원과 헌법재판소에서 부분적으로 받아들여지고 있는 개인정보자기결정권 내지 자기정보통제권이란 정보주체에게 전면적 동의권을 인정해주는 권리는 아니다. 제한적 참여권 내지 통제권을 인정해주는 것임을 분명히 하여야 한다. 그리고 개인정보보호법제란 개인정보의 수집·이

601) 우리나라의 명예훼손법리에 관한 비판적 분석은 이인호, “범죄보도와 면책사유의 적용”, 『언론중재』 제19권 제3호(언론중재위원회, 1999. 9); 한위수, “명예의 훼손과 민사상의 제문제”, □□사법논집□□ 제24집(법원행정처, 1993) 등 참조.

602) 대법원 1998. 9. 4. 선고 96다11327 판결.

용·제공 과정에서 흑여 있을 수 있는 오·남용을 막고 그리하여 정보주체의 이익침해를 예방하기 위하여, 정보처리의 실체적 및 절차적 요건들을 설정하고 또 정보주체에게 정보처리과정에 참여할 수 있는 권리, 즉 열람권, 정정권, 거부권 등을 입법화해 놓은 것이다.

2. 개인정보자기결정권에 대한 오해의 경향에 대한 분석과 비판

위에서 언급한 개인정보자기결정권에 대한 오해는 (i) 일반인의 인식과 태도, (ii) 언어용례, 그리고 (iii) 입법례에서 각 확인되고 있다. 이하에서는 각 사례에서 나타난 오해의 모습을 밝혀내고 이를 비판하고자 한다.

(1) 일반인의 의식과 태도 : 설문조사의 결과분석

1) 분석의 개관

자신에 관한 정보를 정부나 기업이 수집해서 이를 이용하거나 제3자와 공유하는 것에 대하여 일반인들은 물론이고 심지어 전문가들조차도 부정적으로 인식하고 있다는 것이 이번 설문조사의 종합적 결론이라고 할 수 있다.

심지어 정부나 기업의 정당한 업무수행을 위한 개인정보의 처리에 대해서도 위험하다거나 불쾌하다고 생각하는 의견이 압도적으로 많았다.⁶⁰³⁾ ‘정부기관이 소관업무의 수행을 위해 개인정보DB를 구축하여 이용하는 것에 대하여 위험 또는 불쾌하다고 생각하는가?’ 하는 질문에 일반인의 74.5%, 전문가의 85.4%가 ‘위험하다’, 일반인의 74.6%, 전문가의 65.9%가 ‘불쾌하다’고 답변하였다.

603) 자세한 분석결과는 앞의 제2편 제1장 참조.

또 ‘기업이 자신의 목적에 의해 구축한 개인정보DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 위험 또는 불쾌하다고 생각하는가?’ 하는 질문에 일반인의 93.9%, 전문가의 92.7%가 ‘위험하다’, 일반인의 92.5%, 전문가의 85.4%가 ‘불쾌하다’고 답변하였다.

또한 ‘정부나 기업이 자기의 비용으로 수집·이용하고 있는 나의 관한 개인정보는 누구의 것이라고 생각하는가?’ 라는 질문에 일반인의 88.6%, 전문가의 73.2%가 ‘나의 개인정보는 나의 인격적 징표로서 나의 것이다’고 답변하였고, ‘정부나 기업의 자산이다’고 답한 사람은 일반인은 6.4%, 전문가는 24.4%에 불과하였다. 전체적으로 보면 일반인 이든 전문가든 많은 사람들이 정부나 기업이 자기 비용으로 처리하고 있는 개인정보를 그들의 자산으로 인정하기를 꺼려하고 있는 것이다.

또한 ‘정부나 기업이 자신의 업무를 수행하는 과정에서 타인의 개인정보를 수집하는 7가지 예시적 형태에 대해 각 수집행위가 정보주체의 동의 없이 이루어진다면 프라이버시 침해 등의 문제가 발생한다고 생각하는가?’ 라는 질문에 ‘침해가능성이 높다 + 매우 높다’고 응답한 비율이 일반인의 경우 평균 78.9%, 전문가의 경우 평균 63%에 이르렀다.

요컨대, 이상의 조사결과는 정부나 기업의 정당한 업무수행을 위한 개인정보처리에 대해서조차도 일반인이나 전문가나 모두 부정적인 인식을 가지고 있는 것으로 나타났다. 물론 전문가의 경우에는 일반인에 비해 개인정보처리의 필요성을 어느 정도 인정하고 있는 것으로 분석된다.

다만, 이번의 설문조사는 조사대상자와 조사시기의 두 가지 점에서 일정한 한계가 있다. 먼저 조사대상자와 관련해서, 설문조사에 참여한 사람들은 업무상 타인의 개인정보를 이용하고자 하는 정보처리자의 입장이 아니라 그 이용되는 개인정보의 주체의 입장에 서 있는

사람들이었다. 정보주체의 입장에서는 개인정보의 사회적 이용과 유통의 이익을 객관적인 입장에서 바라볼 수 있는 입장에 놓여 있지 않은 것이다.

특히 이러한 경향은 보관·처리되고 있던 개인정보가 대량으로 유출되는 사고가 발생하여 사회적으로 커다란 이슈가 될 때마다 더욱 강화된다. 설문조사를 한 시기도 이런 대형사고가 터지고 난 직후인 지라 설문조사의 결과도 그것을 반영하고 있는 것으로 분석된다.

물론 고의 또는 과실에 의한 대량유출은 당연히 불법화해야 한다. 그러나 대량유출의 위험성이 있다고 해서 그 때문에 정당한 업무 수행에 따르는 개인정보의 자체적인 수집과 이용에 대해서까지 이를 전면적으로 불법화한다든지 혹은 정보주체의 동의 없는 수집과 이용을 원칙적으로 금지시키는 것은 개인정보처리의 위험성만을 강조하는 시각으로서 개인정보처리의 사회적 효용성에 대한 평가를 정당하게 하지 못한 결과이다.

2) 정부나 기업이 보유하고 있는 개인정보에 대한 소유관계

① 일반인 대상 설문조사결과

문) 다른 사람(기업 또는 정부 포함)이 자신의 비용으로 수집·이용하고 있는 나에게 관한 개인정보는 누구의 것이라고 생각하십니까?



- 기업이나 정부 등이 수집한 개인정보는 누구의 것이라고 생각하느냐에 대한 질문에 88.6%가 나의 것이라고 인식하고 있으며,

전체

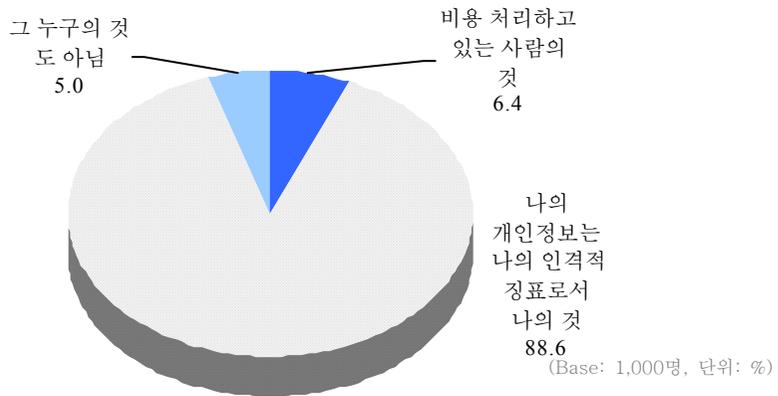
비용처리하고 있는 기업이나 정부의 것이라고 생각하는 경우가 6.4%, 그 누구의 것도 아니라고 하는 경우가 5.0%인 것으로 나타남



- 상대적으로 ‘비용처리하고 있는 사람의 것’은 소득수준이 상인 경우 높게 응답한 특징을 보임

이
의
의

[그림 4-3-1] 수집된 개인정보의 소유권자



제 4 편 개인정보처리의 입법기준에 관한 병행적 입법평가

[표 4-3-1] 수집된 개인정보의 소유권자

(단위:%)

		사례수(명)	비용처리하고 있는 사람의 것	나의 개인 정보는 나의 인격적 지표로서 나의 것	그 누구의 것도 아님	계
■ 전체		(1000)	6.4	88.6	5.0	100.0
성별	남성	(509)	7.9	87.4	4.7	100.0
	여성	(491)	4.9	89.8	5.3	100.0
연령	20대	(242)	7.4	88.0	4.5	100.0
	30대	(285)	4.9	90.9	4.2	100.0
	40대	(281)	6.8	86.1	7.1	100.0
	50대	(192)	6.8	89.6	3.6	100.0
직업	화이트	(434)	7.6	88.2	4.1	100.0
	블루	(189)	3.7	89.9	6.3	100.0
	주부	(200)	5.0	89.5	5.5	100.0
	학생	(120)	8.3	88.3	3.3	100.0
소득 수준	상	(187)	7.5	85.6	7.0	100.0
	중	(640)	6.4	88.8	4.8	100.0
	하	(173)	5.2	91.3	3.5	100.0
지역	서울	(221)	7.7	86.4	5.9	100.0
	경기	(285)	4.6	90.2	5.3	100.0
	강원	(29)	6.9	93.1		100.0
	충청	(98)	12.2	83.7	4.1	100.0
	전라	(99)	5.1	91.9	3.0	100.0
	경상	(268)	5.6	88.8	5.6	100.0
학력	고졸이하	(252)	5.2	90.1	4.8	100.0
	대졸	(634)	7.3	87.7	5.0	100.0
	대학원졸 이상	(114)	4.4	90.4	5.3	100.0

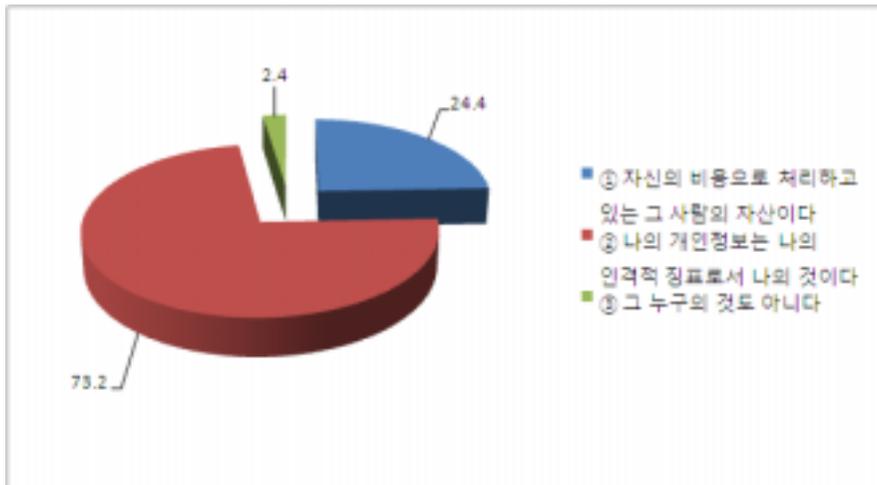
② 전문가 대상 설문조사결과

[전 체]

기업이나 정부 등이 수집한 개인정보는 누구의 것이라고 생각하는지에 대한 질문에 73.2%가 나의 것이라고 인식하고 있으며, 그 누구의 것도 아니다가 2.4%로 나타남

[그림 4-3-2] 수집된 개인정보의 소유권자

(Base : 41명, 단위 %)



[응답자별 특성]

상대적으로 ‘처리하고 있는 사람의 것’은 근무기간 1년미만의 경우 없으며, 근무직장에 따라서 법학교수가 18.75%로 자신의 비용으로 처리하고 있는 사람의 것이 제일 낮았고, 81.25%로 개인정보는 개인의 것이라고 대답하였음

[표 4-3-2] 수집된 개인정보의 소유권자

(단위:%)

		사례수(명)	① 자신의 비용으로 처리하고 있는 그 사람의 자산이다	② 나의 개인정보는 나의 인격적 징표로서 나의 것이다	③ 그 누구의 것도 아니다	계
전체		41	24.39	73.17	2.44	100
성별	남	36	22.22	75.00	2.78	100
	여	5	40.00	60.00	0.00	100
근무기간	1년미만	8	0.00	87.50	12.50	100
	1~5년미만	20	40.00	60.00	0.00	100
	5~10년미만	7	14.29	85.71	0.00	100
	10년이상	6	16.67	83.33	0.00	100
근무직장	기업	13	23.08	69.23	7.69	100
	법학교수	16	18.75	81.25	0.00	100
	법실무	12	33.33	66.67	0.00	100

3) 정보주체의 동의 없는 개인정보의 수집에 대한 부정적 태도

문) 정부나 기업 등 개인정보처리자가 자신의 업무를 수행하는 과정에서 타인의 개인정보를 수집하게 됩니다. 다음의 수집행위가 본인의 동의 없이 이루어진다면 프라이버시 침해 등의 문제가 발생한다고 생각하십니까?

① 일반인 대상 설문조사결과



- 전체
 홈페이지에 수집을 금한다는 경고문이 있는 경우에도 나의 홈페이지에서 게시된 나의 관련 개인정보를 수집하는 행위(88.4%, 매우 가능성 높다+가능성 높다)를 제시된 7개 항목 중 가장 프라이버시 침해 등 문제가 발생하는 행위로 여기고 있으며, 무료만화를 제공하는 인터넷사이트가 이용자의 만화 취향이나 읽는 습

관을 알아보기 위하여 관련 정보를 수집하는 행위(65.8%, 매우 가능성 높다+가능성 높다)를 가장 낮게 응답하였음

[표 4-3-3] 개인정보수집 관련 프라이버시 침해 등 문제 발생 동의 정도

(Base : 1,000명, 단위:%)

	매우 가능성 높다	가능성 높다	TOP 2	보통이다	가능성 없다	전혀 가능성 없다	Bottom 2	Mean (점)
광고기획사가 연예인에 관하여 시중에 떠도는 스캔들소문을 수집하는 행위	40.5	40.6	81.1	14.6	3.8	0.5	4.3	(4.17)
기업이 입사원서를 낸 사람들의 평판, 업무능력에 대한 주위사람들의 평가 등의 정보를 수집하는 행위	40.2	41.3	81.5	14.2	3.8	0.5	4.3	(4.17)
은행이 대출신청자의 신용도를 평가하는데 필요한 개인정보를 수집하는 행위	42.4	34.7	77.1	16.2	6.0	0.7	6.7	(4.12)
인터넷쇼핑몰이 이용자의 소비취향에 관한 정보를 수집하는 행위	41.4	33.8	75.2	18.4	5.9	0.5	6.4	(4.1)
무료 만화를 제공하는 인터넷사이트가 이용자의 만화취향이나 읽는 습관을 알아보기 위하여 관련 정보를 수집하는 행위	32.3	33.5	65.8	25.5	7.5	1.2	8.7	(3.88)
(홈페이지에 수집을 금한다는 경고문이 없을 경우)공개된 나의 홈페이지에 게시된 나의 개인 정보를 수집하는 행위	43.9	39.1	83.0	14.0	2.6	0.4	3.0	(4.24)
(홈페이지에 수집을 금한다는 경고문이 있는 경우)공개된 나의 홈페이지에 게시된 나의 개인 정보를 수집하는 행위	52.3	36.1	88.4	10.2	1.1	0.3	1.4	(4.39)

② 전문가 대상 설문조사결과

[전 체]

홈페이지에 수집을 금한다는 경고문이 있는 경우에도 나의 홈페이지에 게시된 나의 관련 개인 정보를 수집하는 행위(92.7% 그렇다+매우 그렇다)를 제시된 7개 항목 중 가장 프라이버시 침해 등 문제가 발생하고 있으며, 나의 홈페이지에 게시된 나의 관련 정보를 수집하는 행위(2.4% 매우 그렇지 않다+매우 그렇다)를 가장 낮게 응답하였음

[표 4-3-4] 개인정보수집 관련 프라이버시 침해 등 문제 발생 동의 정도

(Base : 41명, 단위 %)

	매우 그렇지 않다	그렇지 않다	Bottom 2	보통 이다	그렇다	매우 그렇다	Top2	Mean (점)
① 광고기획사가 연예인에 관하여 시중에 떠도는 스캔들소문을 수집하는 행위		14.60	14.60	26.80	34.10	24.40	58.50	3.68
② 기업이 입사원서를 낸 사람들의 평판, 업무능력에 대한 주위사람들의 평가 등의 정보를 수집하는 행위	2.4	14.60	17.00	29.30	31.70	22.00	53.70	3.56
③ 은행이 대출신청자의 신용도를 평가하는데 필요한 개인정보를 수집하는 행위	4.9	9.80	14.70	29.30	31.70	24.40	56.10	3.61
④ 인터넷쇼핑몰이 이용자의 소비취향에 관한 정보를 수집하는 행위		7.30	7.30	31.70	39.00	22.00	61.00	3.76
⑤ 무료만화를 제공하는 인터넷사이트가 이용자의 만화취향이나 읽는 습관을 알아보기		9.80	9.80	31.70	39.00	19.50	58.50	3.68

	매우 그렇지 않다	그렇지 않다	Bottom 2	보통 이다	그렇다	매우 그렇다	Top2	Mean (점)
위하여 관련 정보를 수집하는 행위								
⑥ (홈페이지에 수집을 금한다는 경고문이 없을 경우)공개된 나의 홈페이지에 게시된 나의 관한 개인정보를 수집하는 행위		14.60	14.60	24.40	36.60	24.40	61.00	3.71
⑦ (홈페이지에 수집을 금한다는 경고문이 있는 경우)공개된 나의 홈페이지에 게시된 나의 관한 개인정보를 수집하는 행위	2.4		2.40	4.90	51.20	41.50	92.70	4.29

(2) “개인정보침해”의 언어사용례 분석과 비판

사실 개인정보보호의 측면을 중시하는 위의 경향은 우리의 일상적인 언어사용에서도 반영되어 나타나고 있다. “개인정보침해”라는 용어가 그것이다. 개인정보 그 자체는 ‘침해’가 될 수 있는 것이 아니고, 개인정보의 처리와 관련하여 그 정보주체의 인격적 이익이나 권리가 ‘침해’되는 것이다. 우리의 언어사용에 있어서 “비밀침해”라는 개념은 존재한다. 형법 제35장의 “비밀침해의 죄”가 그것이다. 그러나 여기의 침해의 의미는 ‘비밀장치가 되어 있는 것을 파괴하고 그 안의 내용을 지득한다’는 의미이다. 법적으로 특별하게 보호되어야 하는 “비밀”에 관한 법을 모든 “개인정보”에 적용할 수는 없다. 개인정보보호법은 비밀보호법이 아니라는 점에 유의하여야 한다.

그런데도 무단히 ‘개인정보를 침해했다’고 하는 인식은 정보주체의 동의 없는 개인정보의 수집과 이용을 무조건 정보주체의 인격권 침해와 연결시키는 사고가 바탕에 깔려 있는 것으로 보인다.

“개인정보침해”라는 표현은 2001년에 전문 개정된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2001. 1. 16 법률 제6360호, 이하 “정보통신망법”)에서 온라인에서의 개인정보보호를 강화하면서 정보통신서비스제공자가 보유하는 이용자의 개인정보를 마치 “비밀”로 취급한 데서 유래한다.

동법 제24조 제4항은 “이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다.”고 규정하였고, 이를 위반할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하였다(제62조 제3호).⁶⁰⁴⁾ 이는 형법의 비밀침해죄와 비교해도 형벌체계상의 균형이 전혀 맞지 않는다. 형법상 비밀장치한 문서나 전자기록을 기술적 수단을 이용하여 알아내거나(제316조 비밀침해죄) 또는 의사·변호사 등이 그 업무처리 중 지득한 타인의 비밀을 누설하는 행위(제317조 업무상비밀누설죄)도 법정형이 최고 3년 이하의 징역이다. 그것도 이들 범죄는 피해자의 고소가 있어야 공소를 제기할 수 있는 친고죄로 되어 있다(형법 제318조).

그런데 온라인 개인정보보호법인 정보통신망법은 정보통신서비스제공자가 보유하고 있는 일체의 개인정보를 “비밀”로 취급하여 보호하고 있는 것이다. 그것도 형법상의 비밀침해죄보다 무거운 법정형인 형벌로써 보호하고 있다. 이는 정보통신서비스제공자와 이용자 사이의 서비스이용관계를 의사·변호사 등의 전문가와 의뢰인간의 전문적 신뢰관계보다 더 엄격한 관계로 취급하는 것으로서 전혀 균형이 맞지 않는다.

아무튼 “개인정보침해”라는 잘못된 언어는 위 2001년의 정보통신망법에서 한국정보보호진흥원을 설립하면서 그 안에 “개인정보침해신고센터”를 설치·운영하도록 규정한 이래 일반인의 의식 속에 부지불식

604) 현행법에서도 제28조의2(개인정보의 누설금지) 제1항에서 동일한 내용을 규정하고 있고 동일한 벌칙이 제71조(벌칙) 제5호에 규정되어 있다.

간에 자리를 잡아 갔다. 그러면서 정보주체의 동의를 받지 않은 개인 정보의 수집·이용·제공을 모두 불법으로 간주하는 인식을 강화시키는 데 기여하고 있다.

(3) 정보주체의 동의를 절대화하는 입법에 대한 평가

1) 정보통신망법상의 동의 요건에 대한 비판

우리나라에서 정보주체의 동의를 개인정보처리(=수집·이용·제공)의 기본적인 요건으로 인식하게 된 것은 온라인 개인정보보호법인 정보통신망법에서 유래한다. 그러나 정보통신망법은 애초부터 ‘온라인에서의 강력한 개인정보보호’를 정책의제로 설정하고 그런 목표 하에 입법화를 추진하였던 당시의 정보통신부에 의한 다소 기형적인 산물이다.

정보통신망법은 정보통신서비스제공자가 이용자의 개인정보를 수집하는 경우 ① 개인정보의 수집·이용목적 ② 수집하는 개인정보의 항목 ③ 개인정보의 보유·이용기간을 사전에 고지하고 정보주체의 동의를 받아야 한다고 규정하고 있다(제22조 제1항). 그리고 이를 위반한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하고 있다(제71조 제1호). 이용자의 동의 없는 개인정보의 수집 자체를 불법화하고 그것도 무거운 법정형의 형사처벌로 규율하고 있는 것이다. 물론 이에는 아주 제한적인 예외가 있다. 즉, ① 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 ② 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 ③ 이 법 또는 다른 법률에 특별한 규정이 있는 경우가 그것이다(제22조 제2항).

또한 정보통신망법은 정보통신서비스제공자가 이용자의 개인정보를 제3자에게 제공하려면 ① 개인정보를 제공받는 자 ② 개인정보를 제

공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간을 사전에 고지하고 이용자의 동의를 받아야 한다고 규정하고 있다(제24조의2 제1항). 이를 위반한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하여진다(제71조 제3호). 다만, ① 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 ② 이 법 또는 다른 법률에 특별한 규정이 있는 경우에는 예외로 하고 있다.

이처럼 정보통신망법은 동의 요건을 온라인상에서의 모든 개인정보 처리(=수집·이용·제공)가 합법적이기 위한 절대적인 기준으로 설정하고 그 위반에 대해 5년 이하의 징역에 처하고 있다. 이러한 엄격한 동의 요건은 어떻게 보면 정보통신서비스사업자에게는 과중한 부담이 될 수도 있다. 그런데도 이러한 동의 요건이 정보통신서비스제공자에게 특별한 부담을 지우지 않는 것은 이용계약을 체결하면서 이용자의 신상정보를 수집할 때 이용자의 동의를 함께 받기 때문이다.

그런데 정보통신망법이 이렇게 동의 요건을 절대적인 합법성 기준으로 설정한 것은 회원가입시 이용자가 직접 제공해주는 정보(이름, 주민등록번호, 전화번호, 이메일주소, 우편주소, 직업, 직장명, 학력, 결혼여부 등)를 수집하는 경우만을 상정한 때문인 것으로 보인다.

그러나 인터넷 이용과정에서는 실로 무수히 많은 개인정보가 자동으로 수집된다. 인터넷쇼핑몰의 경우 회원이 구매한 물건, 가격, 일시, 결제방법, 그리고 이를 분석하여 2차적으로 생성되는 회원의 소비성향과 구매패턴, 설령 구매하지 않았더라도 열어 본 웹페이지 등 실로 다양한 개인정보가 수집될 수 있다. 게임사이트에서는 회원의 게임머니, 즐기는 게임의 종류, 게임 중의 대화 등 모든 것이 기록된다. 포털사이트에는 실로 엄청난 개인정보가 매일 매일 기록되고 저장된다.

또한 인터넷에서 온라인 광고회사가 개인정보를 수집하는 과정을 간략히 소개하면 이러하다. 온라인광고의 대부분은 배너광고(banner

ads)의 형태이다. 세계적으로 수백억 개의 배너광고가 매달 인터넷을 서핑하는 이용자들에게 전달된다.⁶⁰⁵⁾ 통상 이들 광고들은 이용자가 방문하는 웹사이트 자체에 의해서 선택되고 제공되는 것이 아니고, 상호 관련성이 없는 수많은 웹사이트들을 위하여 광고를 관리하고 제공해주는 네트워크광고회사(network advertising company)에 의해서 선택되고 제공된다.

일반적으로, 이들 네트워크광고회사들은 단순히 배너광고만을 제공하는 것이 아니다. 그들은 동시에 자신들의 광고를 보는 이용자들에게 관한 정보를 수집하여 이용자프로파일⁶⁰⁶⁾을 구축한다. 이러한 정보수집은 기술적으로는 “cookies”와 “Web bugs”의 사용을 통해 이루어진다. 그리고 이들 광고회사가 수집할 수 있는 정보유형에는 ① 이용자가 방문한 웹사이트 및 당해 사이트내의 페이지들에 관한 정보 ② 방문시간과 체류기간 ③ 검색엔진에 입력한 검색어 ④ 구입한 물건 ⑤ 배너광고를 클릭하여 광고상품에 대해 추가정보를 요청한 상황 ⑥ 광고회사가 모니터하는 사이트에 들어오기 전에 이용자가 머물렀던 웹 페이지 등이 포함된다. 아울러 이 모든 정보는 설령 이용자가 특정 배너광고를 클릭한 적이 없는 경우에도 수집된다.

605) 미국에서 가장 규모가 큰 온라인 광고회사인 DoubleClick사는 매일 평균 15억 개의 배너광고를 서비스하며, 한 달에 약 450억 개의 배너광고를 서비스하는 것으로 추산되고 있다. 두 번째 큰 회사인 Engage사와 24/7Media사는 한 달에 각각 86억 개와 33억 개의 배너광고를 서비스하고 있다.

606) 모든 프로파일이 네트워크광고회사(보통 “online profiler”라고 부름)에 의해서 구축되는 것은 아니다. 일부 웹사이트들은 고객과의 상호작용에 기초해서 고객들의 프로파일을 작성한다. 또 일부 회사들은 소비자에게 제품할인을 하거나 또는 소비자가 한번 방문했던 사이트의 주제와 동일한 주제를 다루는 유용한 웹사이트의 목록을 제공하는 서비스의 일환으로서 프로파일을 구축하기도 한다. 예컨대, Megan Barnett, “The Profilers: Invisible Friends”, *The Industry Standard*, Mar. 13, 2000, p. 220; Ben Hammer, “Bargain Hunting”, *The Industry Standard*, Mar. 13, 2000, p. 232. 이들 프로파일은 소비자를 알고 있고 직접적인 관계를 맺고 있는 회사에 의해서 구축되는 것으로, 제3자인 네트워크광고회사가 구축하는 프로파일과는 다른 것이다.

실로 네트워크광고회사가 구축하는 프로파일은 대단히 구체적이고 상세할 수 있다. 광고회사가 심어 놓은 쿠키는 그 광고회사가 서비스하는 웹사이트에서 모든 이용자의 온라인 활동을 추적할 수 있도록 한다. 나아가 그 쿠키는 계속 존재하기 때문에 이용자가 인터넷에 접속할 때마다 그 추적활동을 재개한다. 한편, 이러한 네트워크광고회사의 프로파일링활동은 인터넷 이용자의 눈에는 보이지 않는 상태로 이루어진다.

물론 네트워크광고회사가 수집하는 정보는, 반드시 그런 것은 아니지만, 통상적으로는 익명이다. 즉 사용자프로파일은 일반적으로 특정 개인의 이름과 연결되어 있는 것이 아니고, 광고회사가 이용자의 컴퓨터에 심어 놓은 쿠키의 고유번호와 연결되어 있다. 그러나 이러한 프로파일은 다음의 몇 가지 방식으로 개인식별정보(PII)⁶⁰⁷⁾와 쉽게 연결되거나 통합될 수 있다. 첫째, 광고회사가 자신의 웹사이트를 운영하여 이용자의 개인식별정보를 제공받은 경우, 그 개인식별정보는 당해 광고회사가 이용자의 컴퓨터에 심어 놓은 쿠키의 고유번호와 결합될 수 있다. 둘째, 배너광고가 설치된 웹사이트가 등록된 이용자의 개인식별정보를 네트워크광고회사에게 제공할 수 있다. 셋째, 그 웹사이트가 등록된 이용자의 개인식별정보를 처리하고 검색하는 방식에 따라 일정한 경우에는 그 개인식별정보가 URL에 통합되어 자동으로 네트워크광고회사에게 전달될 수 있다.⁶⁰⁸⁾ 넷째, 오프라인의 마케팅회사가 구축한 개인식별정보와 결합될 수 있다.⁶⁰⁹⁾

607) 개인식별정보(personally identifiable information)란 이름, 전화번호, 주민등록번호, 운전면허번호, 이메일주소, 지문, 홍채, 사진 등과 같이 특정 개인을 알아볼 수 있는 정보를 가리킨다.

608) 이러한 방식의 정보전송은 웹사이트들이 “GET”(“POST”와는 반대) 정보처리방식을 사용하는 경우에 일어난다. Janlori Goldman, Zoe Hudson, and Richard M. Smith, California HealthCare Foundation, □□Privacy: Report on the Privacy Policies and Practices of Health Web Sites□□ (Jan. 2000). “GET” 기술의 결과로서 URL속에 담겨져 네트워크광고회사에게 전달된 개인식별정보가 어떻게 인식되고, 저장되며, 이용되는지는 현재로서는 분명하지 않다.

609) 미국 제1의 네트워크광고회사인 DoubleClick사는 작년에 오프라인 direct mar-

이렇게 해서 수집된 개인정보는 다른 제3자가 온라인 또는 오프라인에서 수집한 이용자의 다른 개인정보와 결합되어 더욱 세밀하게 분석될 수 있다. 그 결과 특정 이용자가 어떤 소비성향, 취미, 기호, 수요를 가지고 있는지를 예측할 수 있게 하는 상세한 이용자프로파일을 구축하는 것이 가능하게 되고, 이에 따라 네트워크광고회사는 이용자의 구체적 관심에 꼭 들어맞는 맞춤형광고를 제공할 수 있게 된다.

이상에서 살핀 바와 같이, 정보통신망 특히 인터넷을 이용하는 과정에서 무수히 많은 개인정보가 여러 다양한 형태로 수집되고 그 수집은 많은 경우 이용자의 동의가 없거나 인식이 없는 상태에서 이루어지는 경우가 허다하다. 그렇다면 이러한 이용자의 동의 없는 수집을 전부 금지시켜야 하는가? 현행 우리의 정보통신망법에 의하면 모두 5년 이하의 징역에 해당하는 범죄행위이다.

우리의 현행 정보통신망법은 회원가입시 이용자가 제공하는 개인정보의 수집만을 상정해 놓고 그러한 수집에 대해서 이용자의 사전 동의를 받도록 규정해 놓은 것이다. 그러나 이는 인터넷에서의 개인정보의 처리에 대한 현실을 전혀 고려하지 않은 입법이 아닐 수 없다.

정보통신망에서의 일체의 개인정보의 수집에 대해 절대적인 동의요건을 설정해 놓은 것은 아마도 세계 유례가 없는 것으로 보인다. 개인정보를 강하게 보호한다고 평가받는 유럽의 경우도 정보통신망에서의 모든 개인정보의 수집·이용·제공에 대해 동의요건을 절대적인 합법성 기준으로 설정하고 있지 않다.

유럽연합은 1995년에 일반법으로서의 개인정보보호지침(Directive 95/46/EC)을 제정하였고, 온라인상의 프라이버시보호를 위한 지침을 별도로 두고 있다. 유럽연합의 온라인프라이버시보호지침⁶¹⁰⁾에 의하면,

keting회사인 Abacus Direct사를 매입하여 그 보유하고 있던 엄청난 규모의 마케팅 데이터베이스를 이런 식으로 결합하고자 시도하였으나, 비판여론에 직면하여 그 계획을 유보한 바 있다.

610) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

정보통신망에서의 일반적인 개인정보의 처리(=수집·이용·제공)가 합법적인 것이 되기 위한 실체적 및 절차적 요건은 일반법인 1995년의 개인정보보호지침(Directive 95/46/EC)에 따른다. 아래에서 살펴는 바와 같이, 1995년의 지침에서 동의 요건은 절대적인 합법성 기준이 아니다. 이에 의하면, 정보통신서비스제공자 또는 그로부터 개인정보를 제공받는 제3자가 추구하는 정당한 이익을 달성하기 위하여 필요한 때에는 개인정보를 처리(=수집·이용·제공)할 수 있다. 다만, 그 처리의 이익보다 정보주체의 기본적인 권리와 자유를 보호해야 하는 이익이 더 클 때에는 그러하지 아니하다(지침 제7조 (f)항).⁶¹¹⁾

유럽연합의 온라인 프라이버시 보호 지침이 특별히 규율하는 주요 내용은 통신비밀의 보장(제5조), 통신사실확인자료(traffic data)에 대한 보호(제6조), 위치정보에 대한 보호(제9조), 스팸메일에 대한 opt-in 방식의 채택(제13조) 등이다. 이에 의하면, 통신의 전송 목적을 위해 처리되는 통신사실확인자료(traffic data)⁶¹²⁾는 정보주체의 동의를 얻어 정보

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). 유럽연합의 개인정보보호를 위한 기본지침은 1995년에 제정된 “Directive 95/46/EC”이다. 이 지침은 일반법이다. 이후 1997년에 유럽연합은 전기통신부문(telecommunications sector)에 적용되는 특별지침(Directive 97/66/EC)을 제정하였다가, 다시 2002년에 디지털 기술이 활용되는 정보통신망(electronic communications network)과 정보통신서비스(electronic communications services)에 대응하기 위해 “Directive 97/66/EC”를 폐기하고 위 “Directive 2002/58/EC”를 제정하여 시행하고 있다. 2002년의 이 지침은 “Directive 2006/24/EC”에 의하여 부분 개정되었다. 개정내용은 테러 방지 목적에서 통신사실확인자료를 일정 기간 보관하도록 요구하는 것이다.

611) 1995년의 개인정보보호지침상의 실체적 요건 및 절차적 요건에 대한 상세는 아래 제3장 제1절 3(2) 및 제2절 참조.

612) “traffic data” means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. (제2조 (b)). 우리나라의 『통신비밀보호법』 제2조 제11호의 “통신사실확인자료”에 해당한다: ① 가입자의 전기통신일시 ② 전기통신개시·종료시간 ③ 발·착신 통신번호 등 상대방의 가입자번호 ④ 사용도수 ⑤ 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료 ⑥ 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료 ⑦ 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는

통신서비스의 마케팅 목적으로 이용할 수 있도록 허용하고 있다. 그리고 위치정보는 익명 또는 정보주체의 동의에 의해서만 처리가 가능하도록 하고, 동의를 얻기 전에 사전고지(처리대상 위치정보의 종류, 처리의 목적 및 기간, 부가가치서비스의 제공목적에서 당해 위치정보를 제3자에게 제공하는지 여부)의 의무를 지우며, 정보주체는 언제든지 동의철회를 가능하게 하고 있다. 이처럼 유럽연합의 온라인프라이버시보호지침은 통신사실확인자료를 마케팅 목적으로 이용하는 경우와 위치정보의 처리에 대해서만 정보주체의 동의를 요건으로 하고 있을 뿐이다.⁶¹³⁾

요컨대, 우리의 정보통신방법은 이용자의 사전 동의 없이는 일체의 개인정보를 수집·이용·제공하는 것을 금지시키고 있다. 이는 지나치게 동의 요건을 절대화하고 있는 것이다. 통신사실확인자료나 위치정보의 처리(=수집·이용·제공)의 경우에만 요구될 수 있는 동의 요건을 모든 개인정보의 처리에 요구하고 있는 것이다.

동의 없는 개인정보의 처리를 5년 이하의 징역에 처할 만큼 정보통신서비스제공자가 수집·이용·제공하는 모든 개인정보가 그 개인의 사생활비밀에 해당하는 것인가? 형법상의 비밀침해죄는 ‘비밀장치에 의해 보존되어 있는 정보’를 그 비밀장치를 깨고 열어 보는 행위를 3년 이하의 징역에 처하고 있다. 그런데 정보통신방법은 정보통신서비스를 제공하고 이용하는 관계에서 정보통신서비스제공자가 이용자의 사소한 개인정보라도 그 이용자의 동의 없이 수집했다면 그 행위를 5년 이하의 징역에 처하고 있다. 또 형법상의 업무상비밀누설죄는 의

정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료.

613) 우리나라도 위치정보의 수집·이용·제공에 대해서는 정보주체의 동의를 합법성의 기본 요건으로 하고 있다. 『위치정보의 보호 및 이용 등에 관한 법률』 제15조 제1항 : “누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니된다. 다만, 제29조의 규정에 의한 긴급구조기관의 긴급구조 또는 경보발송 요청이 있거나 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.”

사·변호사 등의 전문가가 의뢰인과의 신뢰관계 속에서 주고받은 의뢰인의 비밀을 제3자에게 누설하는 행위를 3년 이하의 징역에 처하고 있다. 그런데 정보통신망법은 서비스제공이라는 상업적 이용관계에서 생성된 어떤 사소한 개인정보라도 그 이용자의 동의 없이 제3자에게 제공했다면 그 행위를 5년 이하의 징역에 처하고 있다. 과연 이렇게 까지 온라인상의 이용관계에서 처리되는 개인정보를 보호해야 할 필요가 있는 것인가?

문제의 발단은 온라인의 서비스이용관계에서 수집·이용·제공되는 개인정보를 모두 “비밀”로 잘못 이해하고 있는 데서부터 시작한다. 그리하여 현행 정보통신망법의 개인정보보호규정은 ‘개인정보보호법’이 아니라 ‘비밀보호법’으로 기능하고 있다. 개인정보의 이용과 보호의 균형을 현저히 상실한 법이라고 하지 않을 수 없다.

더 나아가, 문제는 정보통신망법에 그치지 않고 있다. 정보통신망법의 비밀보호법으로서의 성격과 내용이 지난 17대 국회에서 제안되었던 일반법인 개인정보보호법(안)에 거의 그대로 반영되어 나타났다. 온라인을 규율하는 특별법도 아닌 일반법에서 정보주체의 동의 요건을 개인정보처리의 합법성 기준으로 설정하고 있었던 것이다.

2) 제17대 국회의 노회찬 법안과 이은영 법안에 대한 비판

지난 17대 국회에 제출되었던 개인정보보호법(안) 중 ‘노회찬 법안’과 ‘이은영 법안’은 개인정보의 처리(=수집·이용·제공)에 있어서 정보주체의 동의 요건을 정보처리가 합법적인 것이 되기 위한 원칙적인 기준으로 설정하고 있었다. 그리하여 정보주체의 동의 없는 개인정보의 처리를 원칙적으로 금지하는 내용을 법안에 담고 있었다.

노회찬 법안은 개인정보의 수집단계에서부터 정보주체의 ‘사전 동의’를 합법성 요건으로 설정하고 있었고, 이은영 법안은 수집에 있어서 ‘사후 동의’를 합법성 요건으로 규정하고 있었다. 최저한의 기준을

설정해야 할 일반법으로서는 다른 나라에서 보기 어려운 매우 강도 높은 보호수준을 설정한 셈이다. 더구나, 두 법안은 모두 이러한 합법성 요건을 위반한 경우에 최고 징역 1년 또는 징역 3년의 형사처벌의 제재를 규정하였다. 특히 이들 합법성 요건은 형사처벌의 구성요건으로 삼기에는 매우 불명확한 규정으로 되어 있다.

① 노회찬 법안의 사전동의 요건

노회찬 법안은 ‘일반 개인정보’를 ‘수집’하고자 하는 경우 원칙적으로 정보주체의 사전 동의를 받도록 하고, 다만 다섯 가지의 예외를 좁게 인정하고 있다(제5조 제1항). 그리고 ‘민감 개인정보’의 수집은 원칙적으로 금지시키고 있다(제6조 제1항). 또한 이렇게 수집 시에 동의 받은 범위를 넘어선 ‘이용’이나 ‘제3자 제공’은 원칙적으로 금지된다(제7조). 나아가, 정보주체는 언제든지 그 동의를 철회할 수 있다(제10조).

더구나, 이러한 합법성의 요건을 위반하는 경우에는 강력한 형사처벌의 제재를 규정하고 있다. 제5조 제1항을 위반하여 사전 동의 없이 일반 개인정보를 수집하거나 제6조 제1항을 위반하여 민감 개인정보를 수집한 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처하여야 한다(제105조 제6항 제1호 및 제3호). 그런데 제7조를 위반하여 동의 받은 범위를 넘은 이용 또는 제3자 제공에 대해서는 아무런 형사 및 행정적 제재를 규정하고 있지 않다.

[노회찬 법안]

제 5 조(개인정보의 수집 동의 등) ①타인의 개인정보를 수집하는 자는 당해 정보주체에게 제2항의 내용을 고지하고, 정보주체의 동의를 얻어야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 계약의 이행을 위하여 필요한 경우

2. 용역의 제공에 따른 요금정산을 위하여 필요한 경우
3. 언론·출판을 위한 필요한 최소한의 정보
4. 정보주체의 급박한 생명, 신체, 재산의 침해위험을 막기 위하여 부득이한 경우
5. 이 법 또는 다른 법률에 특별한 규정을 두고 있는 경우

제 6 조(개인정보의 수집의 제한 등) ①누구든지 사상·신념·과거의 병력 등 개인의 권리·이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.

제 7 조(개인정보의 이용 및 제공 등) ①개인정보의 이용자는 당해 정보주체의 동의가 있거나 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 동의 받은 범위를 넘어 이를 이용하거나 제3자에게 제공하여서는 아니 된다.

1. 계약의 이행을 위하여 필요한 경우
2. 통계작성·학술연구 또는 시장조사를 위하여 필요한 경우로서 정보주체를 식별할 수 없는 형태로 가공하여 제공하는 경우
3. 다른 법률에 특별한 규정이 있는 경우

②개인정보를 제공받은 자는 당해 정보주체의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이를 이용하거나 제3자에게 제공하여서는 아니 된다.

제10조(동의를 철회) ①정보주체는 언제든지 개인정보 보유자에 대하여 정보수집에 대한 동의를 철회할 수 있다.

②제1항의 규정에 따라 정보주체가 정보수집에 대한 동의를 철회한 경우에는 개인정보 보유자는 지체 없이 수집된 개인정보를 파기하고 기타 필요한 조치를 취하여야 한다. 다만, 개인정보 보유자가 법률상 개인정보를 보유하여야 할 의무가 있는 경우에는 그렇지 아니하다.

② 이은영 법안의 사후동의 요건

이은영 법안은 ‘일반 개인정보’를 ‘수집’할 수 있는 경우를 다섯 가지 설정해 놓고(제6조), 그 수집 이후에 정보주체의 동의를 받도록 요구하고 있다(제7조 제2항). 그리고 ‘민감 개인정보’의 수집은 원칙적으로 금지시키고 있다(제8조). 또한 이렇게 수집 시에 동의 받은 목적 이외의 목적으로 ‘이용’ 또는 ‘제3자 제공’하는 것은 원칙적으로 금지된다(제10조 제1항). 특히 영리목적으로 판매, 유포하고자 하는 때에는 정보주체의 ‘명시적인 동의’를 얻어야 한다(제10조 제2항). 나아가, 정보주체는 그 동의를 철회할 수 있도록 허용하고 있다(제12조).

더구나, 이러한 법적 기준을 위반한 때에는 강력한 형사처벌의 제재를 가하고 있다. 제8조의 규정을 위반하여 민감 개인정보를 수집한 때에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하여지며(제34조 제1항 제1호), 제10조 제2항의 규정을 위반하여 영리를 목적으로 개인정보를 판매 및 유포한 때에도 동일한 형사처벌이 가하여진다(동조 동항 제3호). 그런데 묘하게도 제6조와 제7조의 규정을 위반하여 일반 개인정보를 수집한 행위에 대해서는 아무런 형사 및 행정적 제재를 규정하고 있지 않다.

[이은영 기본법안]

제 6 조(개인정보의 수집) 개인정보취급자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있다.

1. 정보주체의 동의를 얻은 경우
2. 법률의 규정에 의하여 개인정보를 수집할 수 있는 경우
3. 개인정보를 수집하지 아니하고서는 당해 법률행위의 목적을 달성할 수 없는 경우
4. 언론·출판을 위한 필요한 최소한의 정보
5. 정보주체의 급박한 생명, 신체, 재산의 침해위험을 막기 위하여 부득이한 경우

제 7 조 (개인정보의 수집 동의 등) ①개인정보를 수집하는 자는 적법하고 공정한 방법으로 수집해야 하며, 정보주체의 사생활 침해를 최소화하도록 노력하여야한다.

②제1항의 규정에 따라 개인정보를 수집하거나 생성한 경우에는 **사후에** 개인정보를 수집 혹은 생성한 사실을 정보주체에게 알리고 **동의를** 얻어야한다. 다만, 정보주체에 알리는 것이 당해 정보주체의 생명이나 신체에 중대한 위험을 초래하는 경우는 그러하지 아니하다.

제 8 조(개인정보의 수집제한) ①누구든지 사상·신념·과거의 병력 등 개인의 권리·이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 정보주체의 동의를 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.

②누구든지 타인을 부당하게 차별할 목적으로 개인정보를 수집, 처리 및 이용하여서는 아니된다.

제10조(개인정보의 이용 및 제공) ①개인정보취급자는 다음 각 호의 어느 하나에 해당하는 경우 이외에는 개인정보를 수집목적 이외

의 목적으로 이용하거나 타인에게 제공하여서는 아니된다.

1. 정보주체의 동의를 얻은 경우
2. 법률의 규정에 의하여 개인정보를 이용 또는 제공할 수 있는 경우
②개인정보취급자가 개인정보를 판매, 유포하는 영리행위를 하고자 하는 경우에는 정보주체의 명시적인 동의를 얻어야 한다.

제12조(개인정보의 삭제·파기 등) ①개인정보취급자는 정보주체의 명시적인 동의 철회가 있거나 개인정보의 취급목적을 달성한 경우에는 당해 개인정보에 대하여 삭제·파기 및 접근차단 등 필요한 조치를 취하여야 한다. 다만, 다음 각호의 경우에는 그러하지 아니하다.

1. 개인정보의 삭제·파기 및 접근차단 등이 불가능하거나 개인정보취급자의 정당한 이익을 현저히 해할 우려가 있는 경우
2. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

제 2 절 수집·이용·제공의 허용기준에 관한 외국의 입법사례 분석

1980년의 OECD 가이드라인과 유럽연합·영국·독일의 개인정보보호법은 정보주체의 동의를 여러 합법성 요건 ‘중의 하나’로 인정하는 접근방법을 취하고 있다. 그리고 일본의 민간부분 개인정보보호법은 개인정보의 자체적인 수집과 이용에 있어서는 달리 정보주체의 동의를 합법성 요건으로 하고 있지 않다. 또한 민간부분 일반법이 없는 미국의 경우에도 동의 없는 정보처리가 일반적으로 허용되고 있다. 다만, 뒤에서 살펴보는 바와 같이 여러 가지 절차적 요건이 마련되어 있어 그 요건들을 충족해야만 한다.

1. OECD 가이드라인상의 수집제한의 원칙의 내용

1980년의 OECD 개인정보보호 가이드라인⁶¹⁴⁾이 제시한 8대 개인정보보호원칙 중 수집제한의 원칙(Collection Limitation Principle)은 다음과 같다.

『7. 수집제한의 원칙 : 개인정보의 수집에는 제한(limits)이 있어야 하고, 어떠한 개인정보도 합법적이고 공정한 방법으로(by lawful and fair means) 획득되어야 하며, 그렇게 하는 것이 적절한 경우에는(where appropriate) 정보주체의 인식이나 동의하에 획득되어야 한다.⁶¹⁵⁾』

이 수집제한의 원칙은 우선 무제한적인 수집에 대해서는 부정적인 입장을 보이고 있다. 무제한적인 수집은 위험성이 있기 때문에 무언가 ‘제한’이 있어야 한다는 점을 선언하고 있다. 그 제한의 내용에 대해서는 구체적으로 명시하고 있지 않지만, 수집목적이 ‘정당해야 하고’ 그 목적에 ‘필요한 만큼’만 수집해야 한다는 취지라고 생각된다.

그리고 개인정보를 수집할 때에는 ‘합법적이고 공정한 방법’으로 해야 한다고 선언하고 있다. 예컨대, 법이 허용하지 않는 불법적인 도청의 방법으로 수집한다든지, 망원경을 통하여 개인의 일거수일투족을 추적·감시하듯이 수집한다든지, 또는 개인의 사생활공간에 침입하여 사생활을 조사하듯이 정보를 수집하는 방식은 허용되지 않는다고 보아야 할 것이다.

또한 동 원칙은 개인정보를 수집할 때 그렇게 하는 것이 적절하다면 정보주체가 그 수집에 대해 인식할 수 있도록 해 주거나 또는 정

614) 『프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인』 (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).

615) PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

보주체의 동의를 받아 수집하여야 한다고 선언하고 있다. 여기서 정보주체의 동의는 절대적인 요건이 아니다. 동의를 받는 것이 ‘적절하다면’(where appropriate) 그렇게 하는 것이 타당하다는 취지이다. 바꿔 말하면, 동의를 받는 것이 ‘부적절하다면’ 동의 없이도 수집이 가능하다는 것이다. 또 설령 동의는 받지 않더라도 정보주체에게 수집에 대해 인식할 수 있게 해 주는 것이 ‘적절하다면’ 그렇게 하는 것이 타당하다는 취지이다.

요컨대, OECD 개인정보보호 가이드라인은 정보주체의 동의를 개인 정보 수집에 있어서 요건으로 반드시 상정하고 있지 않으며, ‘동의를 받는 것이 적절한 경우’에 한하여 동의를 받을 것을 요구하고 있다.

다만, 유의할 점은 정보주체의 동의에 의하여 수집이 이루어지든, 아니면 정보주체의 동의 없는 합법적인 수집이든 간에 모든 개인정보의 수집과 이용에 대해서는 별도로 “목적명시의 원칙”(Purpose Specification Principle)이 요구된다는 것이다. 목적명시의 원칙은 다음과 같다. 이에 관해서는 아래 제3장 제2절에서 자세하게 살핀다.

『9. 목적명시의 원칙 : 개인정보를 수집하는 목적은 늦어도 정보를 수집하는 시점에는 명시되어야 하고, 그 후의 이용⁶¹⁶⁾은 그 명시한 목적이나 혹은 그 명시한 목적과 양립할 수 있는 다른 목적을 달성하는데 한정되어야 하며, 목적의 변경이 있을 때에는 그때마다 그것을 명시하여야 한다.』⁶¹⁷⁾

616) 여기서의 “이용”은 개인정보처리자의 자체 이용과 제3자 제공을 포함하는 개념이다. 가이드라인의 “이용제한의 원칙”(Use Limitation Principle)에서 “이용”(use)이라는 용어는 제3자 제공을 포함하는 개념으로 사용하고 있다.

617) PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

2. 유럽연합 개인정보보호지침상의 허용기준

유럽연합의 개인정보보호지침(95/46/EC)은 정보주체의 동의를 여러 허용기준 중의 하나로 제시할 뿐, 개인정보처리의 허용기준으로 정보주체의 동의를 “원칙”으로 설정하고 있지 않다는 점에 유의하여야 한다. 또한 동 지침은 “일반개인정보”와 “특수개인정보”를 구분하고 후자에 대해서는 보다 강화된 법적 기준을 설정하고 있다. 아울러 동 지침은 공공부문과 민간부문의 양 부문을 포괄하는 일반법이지만, 각 부문에 대해서 다소 다른 허용 기준을 제시하고 있다.

특히 유럽연합 지침은 수집단계, 이용단계, 제공단계를 각각 나누어 합법성 기준을 설정하는 방식이 아니라, 수집·이용·제공을 모두 합한 “처리”(processing)⁶¹⁸의 합법성 기준을 단일적으로 제시하고 있는 점에 유의할 필요가 있다.

또 한 가지 유의할 점은 처리의 허용기준과는 별도로 여러 절차적 요건이 마련되어 있다는 점이다. 즉 목적명시의 요건, 고지의 요건, 시스템공개의 요건 등이 그것이다. 이러한 절차적 요건을 위반하는 경우에는 위법한 정보처리가 된다. 이 절차적 요건에 대해서는 아래 제3장 제2절에서 구체적으로 분석한다.

(1) 일반개인정보 수집·이용·제공의 허용기준

유럽연합 지침 제7조는 “일반개인정보”의 처리(=수집·이용·제공)가 정당한 것이 되기 위한 요건을 다음과 같이 6개 항목으로 나누어 열

618) “개인정보처리(processing of personal data)”라 함은 자동수단에 의한 것이든 아니든 개인정보(personal data)에 가해지는 일체의 작용(any operation or set of operations)을 가리킨다. 예컨대 수집(collection), 기록(recording), 편성(organization), 저장(storage), 수정(adaptation or alteration), 검색(retrieval), 참조(consultation), 이용(use), 전송·공표 기타의 제공 방식에 의한 공개(disclosure by transmission, dissemination or otherwise making available), 배열이나 조합(alignment or combination), 접근차단(blocking), 삭제(erasure) 또는 파괴(destruction)를 말한다. (제2조 (b)호)

거하고 있다.

- (a) 정보주체가 명확하게(unambiguously) 동의를 한 때; 또는
- (b) 정보주체가 한 쪽 당사자인 계약의 이행을 위하여 또는 계약체결에 앞서 정보주체의 요청에 따라 일정한 조치를 취하기 위하여 정보처리가 필요한 때; 또는
- (c) 개인정보처리자가 지는 법적 의무를 준수하기 위하여 정보처리가 필요한 때; 또는
- (d) 정보주체의 중대한 이익(vital interests)을 보호하기 위하여 정보처리가 필요한 때; 또는
- (e) 공공의 이익을 위하여 수행되는 업무의 처리를 위하여, 또는 개인정보처리자나 개인정보를 제공받는 제3자에게 주어진 공적 권한(official authority)의 행사를 위하여 정보처리가 필요한 때; 또는
- (f) 개인정보처리자나 개인정보를 제공받는 제3자가 추구하는 “정당한 이익”(legitimate interests)을 달성하기 위하여 정보처리가 필요한 때. 다만, 그러한 이익보다 정보주체의 기본적인 권리와 자유(fundamental rights and freedoms)를 보호해야 하는 이익이 더 클 때에는 그러하지 아니하다.

이처럼 유럽연합 지침은 정보주체의 동의 없이도 “일반개인정보”를 처리(=수집·이용·제공)할 수 있는 경우를 5가지로 광범위하게 규정하고 있다. 특히 (e)호는 공공기관에 대하여 법적인 권한 행사에 필요하다면 동의 없이도 광범위하게 개인정보를 처리하는 것을 허용하고 있으며, (f)호는 민간기관이 정보주체의 기본권적 이익을 과도하게 해하지 않는 한 자신의 정당한 이익을 위하여 정보주체의 동의 없이 개인정보를 처리할 수 있도록 허용하고 있다.

이 지침의 법적 기준에 의하면, 민간기관은 정보주체의 동의 없이도 원칙적으로 자신의 “정당한 이익”을 위하여 개인정보를 수집·이용·

제공할 수 있고, 다만 이익형량의 관점에서 그 정보처리로 인해 정보주체의 기본권적 이익의 침해가 더 클 때에 한하여 위법한 것이 된다. 물론 이런 추상적인 법적 기준은 집행과정에서 개인정보감독기구나 법원에 의하여 구체화될 것이다.

(2) 특수개인정보 수집·이용·제공의 허용기준

유럽연합 지침 제8조는 “특수개인정보”의 처리(=수집·이용·제공)가 정당한 것이 되기 위한 특별기준을 다음과 같이 원칙과 예외로 나누어 규정하고 있다.

- (1) 인종적 또는 민족적 출신(racial or ethnic origin), 정치적 견해(political opinions), 종교적 또는 철학적 신념(religious or philosophical beliefs), 노동조합 가입여부(trade union membership)를 드러내는 개인기록 및 건강이나 성생활(health or sex life)에 관한 기록의 처리는 금지된다.
- (2) 위 제1항은 다음 각 호의 경우에는 적용되지 아니한다.
 - (a) 정보주체가 그 처리에 대한 명시적인 동의(explicit consent)를 한 때. 다만, 회원국은 국내법으로써 정보주체의 동의가 있더라도 특수개인정보의 처리를 금지시킬 수 있다; 또는
 - (b) 적절한 안전장치를 규정한 국내법이 허용하고 있다면, 노동법의 영역에서 개인정보처리자의 의무와 구체적 권리를 실현하기 위한 목적에서 정보처리가 필요한 때; 또는
 - (c) 정보주체가 물리적으로나 법적으로 동의를 할 수 없는 경우에, 당해 정보주체나 제3자의 중대한 이익(vital interests)을 보호하기 위하여 정보처리가 필요한 때; 또는
 - (d) 정치적, 학문적, 종교적 또는 노동조합의 목적을 가진 법인이거나 단체 기타 비영리단체가 그 단체의 정당한 활동(legitimate

activities)과 관련하여 적절한 안전장치(appropriate guarantees)를 갖추고 정보처리가 수행되는 때. 다만, 그 정보처리는 오로지 그 단체의 구성원들 또는 단체의 목적과 관련하여 정규적인 관계(regular contact)를 맺고 있는 사람들에 관한 것이어야 하고, 또한 정보주체의 동의 없이는 그 처리정보를 제3자에게 공개하여서는 아니 된다.

- (e) 정보주체가 명백히(manifestly) 공개한 정보를 처리하는 때, 또는 법적 권리(legal claims)를 입증하거나 행사하거나 또는 방어하기 위하여 정보처리가 필요한 때.
- (3) 다음의 경우에는 위 제1항이 적용되지 아니 한다: 예방의학(preventive medicine), 의학적 진단(medical diagnosis), 치료(the provision of care and treatment) 또는 건강관리서비스의 관리(management of healthcare services)를 위하여 정보처리가 요구되고, 또 그 정보처리가 법령에 따라 전문가적인 비밀유지의무를 지는 의료전문가(health professional) 또는 그에 상응하는 비밀유지의무를 지는 자에 의하여 수행되는 경우.
- (4) 회원국은 중요한 공익(substantial public interest)을 이유로 국내법령 또는 개인정보감독기구의 결정에 의하여 위 제2항에 열거한 것 이외의 예외를 더 둘 수 있다. 이 경우 적절한 안전장치에 관한 규정을 두어야 한다.
- (5) 범죄행위, 유죄선고, 또는 질서유지와 관련한 개인정보의 처리는 공공기관(official authority)의 관리 하에서만 수행될 수 있다. 다만, 적절한 구체적인 안전장치를 법률에서 규정하고 있다면, 공공기관이 아니더라도 법률로 정하는 기관에서 처리할 수 있다. 그러나 종합적인 유죄선고기록은 공공기관의 관리 하에서만 보관될 수 있다. 회원국은 행정적 제재 또는 민사판결과 관련한 개인기록은 또한 공공기관의 관리 하에서 처리될 수 있음을 규정할 수 있다.

- (6) 제4항과 제5항에 의하여 제1항의 원칙을 완화한 내용은 집행위원회(Commission)에 통지하여야 한다.
- (7) 회원국은 전국민고유식별번호(national identification number) 또는 그 밖에 일반적으로 사용되는 고유식별자(any other identifier of general application)를 처리할 수 있기 위한 요건들을 규정하여야 한다.

이처럼 유럽연합 지침은 의료정보 등 민감한 개인정보의 처리에 대해서는 공공부문과 민간부문의 구분 없이 이를 원칙적으로 금지시키면서, 그러나 다소 넓은 예외를 “구체적”으로 설정하고 있다. 그리하여 노동법의 영역이나 정치적·학문적·종교적 비영리단체의 정당한 활동과 관련해서 정보주체의 동의 없는 정보처리를 제한적으로 허용하고 있으며, 또 의학적 목적의 정보처리에 대해서도 광범위하게 정보처리를 허용하고 있다. 한편, 고유식별자의 처리에 대해서는 각 회원국이 그 처리의 허용기준을 구체적으로 정하도록 요구하고 있다.

3. 영국 개인정보보호법상의 허용기준

영국의 개인정보보호법도 기본적으로는 위 유럽연합의 지침과 유사한 내용을 규정하고 있다. 영국의 개인정보보호법은 제1부칙(Schedule 1) 제1절(Part 1)에서 8가지 개인정보처리의 기본원칙을 규정하고 있다. 그 중에서 제1조는 “일반개인정보”는 적어도 제2부칙(Schedule 2)이 정하는 요건 중의 하나가 충족되는 경우에 한하여 처리할 수 있으며, “민감개인정보”는 적어도 제3부칙(Schedule 3)이 정하는 요건 중의 하나가 충족되는 경우에 한하여 처리될 수 있다고 규정하고 있다.

(1) 일반개인정보 수집·이용·제공의 허용기준

제2부칙(Schedule 2)은 “일반개인정보”를 처리(=수집·이용·제공)할 수 있는 기준을 다음과 같이 6가지로 규정하고 있다.

1. 정보주체가 정보처리에 동의를 한 때; 또는
2. 정보주체가 한 쪽 당사자인 계약의 이행을 위하여 또는 계약체결을 목적으로 정보주체의 요청에 따라 일정한 조치를 취하기 위하여 정보처리가 필요한 때; 또는
3. 계약상의 의무 이외에, 개인정보처리자가 지는 법적 의무(any legal obligation)를 준수하기 위하여 정보처리가 필요한 때; 또는
4. 정보주체의 중대한 이익(vital interests)을 보호하기 위하여 정보처리가 필요한 때; 또는
5. (a) 사법기능의 수행, (b) 법령에 의하여 누군가에게 부여된 기능의 수행, (c) 국왕, 장관 또는 정부부처의 기능의 수행, 또는 (d) 그 밖에 누구에 의하든지 간에 공익을 위한 공익적 성격의 기능의 수행을 위하여 정보처리가 필요한 때;
6. (1) 개인정보처리자나 개인정보를 제공받는 제3자가 추구하는 “정당한 이익”(legitimate interests)을 달성하기 위하여 정보처리가 필요한 때. 다만, 당해 정보처리가 구체적인 사안에서(in any particular case) 정보주체의 권리와 자유 또는 정당한 이익을 침해하여 정당화될 수 없을 때에는 그러하지 아니하다.
(2) 국무장관(Secretary of State)은 이 요건이 충족되거나 충족되지 않는다고 인정되어지는 구체적인 상황(particular circumstances)을 명령으로써(by order) 상세히 규정할 수 있다.

(2) 민감개인정보 수집·이용·제공의 허용기준

제3부칙(Schedule 3)은 민감개인정보(sensitive personal data)를 처리(=수집·이용·제공)할 수 있는 기준을 다음과 같이 10가지로 규정하고 있다.

1. 정보주체가 그 정보처리에 명시적인 동의(explicit consent)를 한 때;
2. (1) 고용(employment)과 관련해서 개인정보처리자가 법적으로 가지는 권리나 의무의 행사 또는 이행을 위하여 정보처리가 필요한 때;

- (2) 국무장관(Secretary of State)은 명령으로써(by order) (a) 구체적인 경우를 정하여 위 (1)항의 적용을 배제시킬 수 있으며, 또는 (b) 위 (1)항의 요건이 충족되지 않는 것으로 인정되는 구체적인 경우를 규정할 수 있는데, 다만 이 때 당해 명령에서 보다 강화된 요건(further conditions)을 구체적으로 정할 수 있다.
3. (a) 정보주체가 직접 또는 대리인에 의하여 동의를 표시할 수 없는 경우거나, 또는 개인정보처리자가 정보주체의 동의를 받는 것이 합리적으로 기대할 수 없는 경우에, 당해 정보주체나 다른 사람의 중대한 이익(vital interests)을 보호하기 위하여 정보처리가 필요한 때; 또는 (b) 정보주체가 불합리하게(unreasonably) 동의를 하지 않고 있는 경우에, 다른 사람의 중대한 이익(vital interests)을 보호하기 위하여 정보처리가 필요한 때
4. (a) 정치적, 철학적, 종교적 또는 노동조합의 목적을 가진 비영리 단체가 그 단체의 정당한 활동(legitimate activities)을 하는 과정에서 수행되는 정보처리로서, (b) 정보주체의 권리와 자유를 보호하기 위한 적절한 안전장치(appropriate safeguards)를 갖추고 정보처리가 수행되고, (c) 그 정보처리는 오로지 그 단체의 구성원들이나 단체의 목적과 관련하여 정규적인 관계(regular contact)를 맺고 있는 사람들에 관한 것이어야 하며, 또한 (d) 그 정보처리에 정보주체의 동의 없는 제3자 제공이 포함되지 않는 때.
5. 민감개인기록에 포함된 정보가 정보주체의 의도적인 조치의 결과로서 이미 공개된 것인 때.
6. (a) 법적 절차(예상되는 법적 절차 포함)를 밟기 위해서 또는 그 절차와 관련해서 정보처리가 필요하거나, (b) 법적 자문(legal advice)을 얻기 위한 목적에서 정보처리가 필요하거나, 또는 (c) 그 밖에 법적 권리(legal rights)를 입증하거나 행사하거나 또는 방어하

기 위하여 정보처리가 필요한 때.

7. (1) (a) 사법기능의 수행, (b) 법령에 의하여 부여된 기능의 수행, 또는 (c) 국왕, 장관 또는 정부부처의 기능의 수행을 위하여 정보처리가 필요한 때.

(2) 국무장관(Secretary of State)은 명령으로써(by order) (a) 구체적인 경우를 정하여 위 (1)항의 적용을 배제시킬 수 있으며, 또는 (b) 위 (1)항의 요건이 충족되지 않는 것으로 인정되는 구체적인 경우를 규정할 수 있는데, 다만 이 때 당해 명령에서 보다 강화된 요건(further conditions)을 구체적으로 정할 수 있다.

8. (1) 의학적 목적(medical purposes)을 위하여 정보처리가 필요하고, 그 정보처리가 (a) 의료전문가(health professional), 또는 (b) 의료전문가에 상응하는 비밀유지의무(duty of confidentiality)를 지는 자에 의하여 수행될 때.

(2) 본 조의 “의학적 목적”(medical purposes)에는 예방의학(preventive medicine), 의학적 진단(medical diagnosis), 의학적 연구(medical research), 치료(the provision of care and treatment) 그리고 건강관리서비스의 관리(management of healthcare services)가 포함된다.

9. (1) (a) 인종적 또는 민족적 출신에 관한 정보로 구성된 민감 개인기록(sensitive personal data consisting of information as to racial or ethnic origin)에 대한 정보처리로서, (b) 서로 다른 인종적 또는 민족적 출신의 사람들 사이에 기회나 처우의 평등을 유지 또는 개선할 목적으로 그 평등이 존재하는지 아니면 결여되어 있는지 여부를 확인하거나 심사하기 위하여 그 정보처리가 필요하고, (c) 정보주체의 권리와 자유를 보호하기 위한 적절한 안전장치를 갖추고 그 정보처리가 수행되는 때.

(2) 국무장관(Secretary of State)은 명령으로써(by order) 어떤 상황에서 위 (1)항에 해당하는 정보처리가 인정될 것인지를 구체적으로

로 정할 수 있다.

10. 그 밖에 국무장관이 명령으로써 구체적으로 정하는 상황에서 정보처리가 이루어지는 때.

4. 독일 개인정보보호법상의 허용기준

독일의 연방개인정보보호법은 공공부문과 민간부문을 함께 규율하는 일반법의 성격을 가지고 있지만, 개인정보처리의 구체적인 법적 기준은 공공부문과 민간부문을 각각 나누어 별도의 장에서 서로 달리 규정하고 있다. 공공기관에 의한 개인정보처리는 제2장(Zweiter Abschnitt)에서, 민간기관에 의한 개인정보처리는 제3장(Dritter Abschnitt)에서 규정하고 있으며, 그리고 제1장(Erster Abschnitt)에서는 양 부문에 공통되는 사항들을 규정하고 있다.

이하에서는 제3장에서 규정하고 있는 민간기관에 의한 개인정보처리의 합법성 기준에 대해서만 살핀다. 독일도 유럽연합의 지침과 마찬가지로 “일반개인정보”와 “특수개인정보”를 구분하여 다르게 그 법적 기준을 규정하고 있다. 특히, 독일은 민간기관이 자신이 이용하기 위해 개인정보를 처리하는 경우(제28조)와 광고 등 처음부터 제3자에게 제공하기 위한 목적(판매목적)에서 개인정보를 처리하는 경우(제29조)를 나누어 규정하고 있다.

(1) 자신의 업무수행을 위한 수집·이용·제공의 허용기준

독일의 연방개인정보보호법은 “일반개인정보”를 자신의 업무를 수행하기 위하여 수집·이용·제공하는 경우에는 정보주체의 동의를 아예 요건으로 하고 있지 않다(제28조 제1항). 그렇지만 개인정보처리자는 ① 수집할 때 정보처리의 목적을 명시하여야 하고, ② 그 목적은 자신의 업무를 달성하기 위한 것이어야 하며, ③ 자신의 정당한 이익

을 보호하기 위하여 필요한 범위 내에서 처리할 수 있다. 즉, 이러한 요건 하에서 개인정보처리자는 정보주체의 동의 없이 수집·이용·제공할 수 있다. 다만, ④ 그러한 처리를 금지시켜야 할 압도적인 정보주체의 이익이 존재한다고 인정될 때에 한하여 그러한 처리는 적법하지 않게 된다.

한편, “특수개인정보”(인종적 또는 민족적 출신, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강이나 성생활에 관한 기록)를 수집하는 경우에는 정보주체의 동의를 원칙적인 요건으로 하고 있다. 따라서 민간기관이 자신의 업무를 수행하기 위하여 특수개인정보를 동의 없이 수집하는 것은 원칙적으로 불법이다. 그러나 여기에는 상당한 예외가 설정되어 있다(제28조 제6항 내지 제9항).

첫째, 다음의 4가지 경우에는 동의 없는 수집과 이용이 가능하다: ① 동의를 받는 것이 사실상 또는 법적으로 불가능하지만, 정보주체나 제3자의 중대한 이익을 보호하기 위하여 필요한 때 ② 정보주체가 스스로 명시적으로 공개한 때 ③ 법적 권리의 입증·행사·방어에 필요한 때. 다만 수집과 이용을 금지시켜야 할 압도적인 정보주체의 이익이 존재한다고 인정될 때에는 그러하지 아니하다. ④ 학문적 연구의 수행을 위하여 필요한 때. 다만, 그 학문적 이익이 수집을 금지시켜야 할 정보주체의 이익보다 월등히 우월해야 하고, 달리 다른 수단에 의해서는 그 연구의 목적을 달성하기 어려운 경우라야 한다(제6항).

둘째, 예방의학, 의학적 진단, 치료 또는 건강관리서비스의 제공 목적인 경우에는 정보주체의 동의 없이도 특수개인정보(주로 건강정보나 성생활정보)의 수집이 가능하다. 다만, 그 정보는 의료전문가 또는 그에 상응하는 비밀유지의무를 지는 자에 의하여 처리되어야 한다(제7항).

셋째, 위 첫째와 둘째의 요건이 충족되는 경우에는 처음에 수집된 목적과는 다른 목적을 위하여 정보주체의 동의 없이 이용되거나 제공될 수 있다. 또한 중대 범죄의 수사를 위해서 또는 국가안보나 공공

의 안전에 대한 상당한 위험을 피하기 위하여 필요한 때에는 그 이용 또는 제공은 합법적이다(제8항).

넷째, 정치적, 학문적, 종교적 목적이나 노동조합의 목적을 가진 비영리단체는 그 단체의 활동을 위하여 필요한 때에는 정보주체의 동의 없이 특수개인정보를 수집·이용할 수 있다. 다만, 그 단체 구성원들의 개인정보 또는 단체의 목적과 관련하여 정규적인 관계를 맺고 있는 사람들의 특수개인정보에 한정된다. 그러나 특수개인정보를 단체의 외부 사람이나 기관에게 제공하는 것은 오직 정보주체의 동의 요건 하에서만 합법적인 것이 된다(제9항).

제28조 (자신의 목적을 위한 개인정보의 수집, 처리 및 이용)

(1) 자신의 업무목적(eigener Geschäftszwecke)을 달성하기 위한 수단으로서 개인정보를 수집, 저장, 수정, 제3자 제공 또는 이용하는 것은 다음 각 호의 1에 해당하는 경우에 허용된다.

1. 정보주체와의 계약 또는 준계약적 신뢰관계를 위한 목적인 때
2. 개인정보처리자의 정당한 이익을 보호하기 위하여 필요하고, 또한 그 처리나 이용을 하지 못하게 할 압도적인 정당한 이익이 정보주체에게 있다고 볼 만한 근거가 전혀 없는 때
3. 그 개인정보가 일반적으로 접근이 가능한 것인 때, 또는 개인정보처리자가 합법적으로 개인정보를 공표할 수 있는 때. 다만, 그 정보처리를 배제해야 할 정보주체의 정당한 이익이 당해 개인정보처리자의 정당한 이익보다 명백히 우월한 때에는 그러하지 아니하다.

개인정보를 수집할 때 정보처리의 목적은 구체적으로 명시되어야 한다.

(2) 위 제1항 제1문 제2호 및 제3호의 요건이 충족되는 경우에 한하여, 수집된 개인정보는 다른 목적을 위하여 이용되거나 제공

될 수 있다.

(3) 다른 목적을 위한 이용 또는 제공은 또한 다음 각 호의 경우에 한하여 적법하다.

1. 제3자의 정당한 이익을 보호하기 위하여 필요한 때
2. 범죄의 수사를 위하여, 또는 국가안보나 공공의 안전에 대한 위협을 피하기 위하여 필요한 때
3. 광고, 시장조사 그리고 여론조사를 위한 목적인 때. 다만 이 경우 이용 또는 제공되는 개인정보는 일정 범위의 사람들에 관한 명부형식으로 된 개인정보여야 하고, 그에 포함되는 개인정보는 (a) 당해 정보주체가 그 명부에 포함되는지 여부, (b) 직업, (c) 이름, (d) 직책, (e) 대학학위, (f) 주소, 그리고 (g) 출생연도에 한정되어야 하며, 그리고 당해 정보주체가 그 제공이나 이용을 못하게 할 정당한 이익을 가지고 있다고 믿을만한 근거가 일체 없어야 한다.
4. 학문적 연구를 수행하는 연구기관의 이익을 위하여 필요한 때. 다만, 이 경우 그 연구를 수행하는 학문적 이익이 그 목적의 변경을 못하게 할 정보주체의 이익보다 월등히 우월해야 하고, 또한 그 연구의 목적이 비상한 노력이 없이는 다른 수단으로는 달성될 수 없는 것이어야 한다.

(4) 정보주체가 자신의 정보를 광고, 시장조사 또는 여론조사를 목적으로 이용 또는 제공하지 못하도록 개인정보처리자에게 이의를 제기하는 때에는, 그러한 목적의 이용 또는 제공은 허용되지 아니한다. 광고, 시장조사 또는 여론조사의 목적으로 연락을 받았을 때, 정보주체는 그 개인정보처리자의 신원과 자신의 거부권에 대하여 통지를 받아야 한다. 자신이 알지 못하는 개인정보처리자가 가지고 있던 개인정보를 이용하여 [위 목적으로] 연락을 취하는 자는 그 개인정보의 출처를 정보주체가 알

수 있도록 보장하여야 한다. 정보주체가 위 제3항에 의하여 개인정보를 제공받는 제3자에게 광고, 시장조사 또는 여론조사를 목적으로 하는 처리나 이용을 하지 못하도록 이의를 제기한 때에는, 그 수령인은 그 제공받은 개인정보가 위 목적으로 처리 또는 이용되지 않도록 차단시켜야 한다.

- (5) 개인정보를 제공받은 제3자는 그 제공받은 목적을 위해서만 그 정보를 처리하거나 이용할 수 있다. 민간기관이 다른 목적을 위하여 제공받은 개인정보를 처리하거나 이용하고자 하는 경우에, 위 제2항 및 제3항의 요건이 충족되는 때에 한하여 그것이 허용된다. 공공기관이 다른 목적을 위하여 제공받은 개인정보를 처리하거나 이용하고자 하는 경우에, 제14조 제2항의 요건이 충족되는 때에 한하여 그것이 허용된다. 제공하는 기관은 이 점을 그에게 알려주어야 한다.

여기까지는 “일반개인정보” 처리의 허용 기준이다. “특수개인정보” 처리의 허용 기준은 동조(제28조) 제6항 내지 제9항에서 다음과 같이 규정하고 있다.

- (6) 자신의 업무목적을 위한 특수개인정보(제3조 제9항)⁶¹⁹의 수집, 처리 또는 이용은, 정보주체가 제4a조 제3항의 방식에 따라 동의를 하지 않은 경우라 하더라도, 다음 각 호의 1의 경우에는 합법적이다.

1. 정보주체가 물리적으로 또는 법적으로 동의를 할 수 없는 경우에, 그 정보주체나 제3자의 중대한 이익을 보호하기 위하여 필요한 때

619) “특수 개인정보라 함은 인종적 또는 민족적 출신, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강이나 성생활에 관한 기록을 말한다.” (제3조 제9항)

2. 문제의 특수개인정보가 정보주체에 의하여 공공의 영역에 명백히 놓이게 된 때
 3. 법적 권리를 입증하거나 행사하거나 또는 방어하기 위하여 필요하고, 그 수집, 처리 또는 이용을 하지 못하게 할 압도적인 정당한 이익이 정보주체에게 있다고 믿을만한 근거가 전혀 없는 때
 4. 학문적 연구를 수행하기 위하여 필요하고, 그 연구를 수행하는 학문적 이익이 그 수집을 하지 못하게 할 정보주체의 이익보다 월등히 우월하며, 그리고 그 연구의 목적이 비상한 노력이 없이는 다른 수단에 의해서는 달성될 수 없는 때
- (7) 특수개인정보(제3조 제9항)의 수집은 또한 다음의 경우, 즉 예방 의학, 의학적 진단, 치료 또는 건강관리서비스의 제공을 위하여 필요하고, 또한 그 정보가 의료전문가 또는 그에 상응하는 비밀유지의무를 지는 자에 의하여 처리되는 때에는 합법적이다. 위 제1문의 목적을 위한 특수 개인정보의 처리 및 이용은 위 제1문의 의료전문가 등이 지는 비밀유지의무에 따라 이루어져야 한다.
- (8) 특수개인정보(제3조 제9항)는 다른 목적을 위하여 이용되거나 제공될 수 있는데, 다만 이 경우 제6항 제1호 내지 제4호의 요건이 충족되거나 또는 제7항 제1문의 요건이 충족되어야 한다. 중대 범죄의 수사를 위해서 또는 국가안보나 공공의 안전에 대한 상당한 위험을 피하기 위하여 필요한 때에는 그 이용이나 제공은 또한 합법적이다.
- (9) 정치적, 학문적, 종교적 목적이나 노동조합의 목적을 가진 비영리단체는 그 단체의 활동을 위하여 필요한 때에는 특수개인정보(제3조 제9항)를 수집, 처리, 이용할 수 있다. 제1문은 그 단체 구성원들의 개인정보 또는 단체의 목적과 관련하여 정규적인 관계를 맺고 있는 사람들의 개인정보에 한해서만 적용된다. 이들 개인정보를 단체의 외부 사람이나 기관에게 제공하는 것은 오직 제

4a조 제3항[정보주체의 동의방식]의 요건 하에서만 합법적이다.
위 제3항 제2호는 준용된다.

(2) 제3자 제공목적의 수집·제공의 허용기준

한편, 독일의 연방개인정보보호법은 민간기관이 광고, 정보제공서비스, 상업적인 주소목록작성, 시장조사나 여론조사를 위하여 처음부터 제3자에게 제공하기 위한 목적에서 개인정보를 수집·처리하는 경우에 그 수집 및 기록의 합법성 요건을 제29조에서 별도로 규정하고 있다.

아래에서 보는 바와 같이, 자신의 업무수행 목적이 아닌 처음부터 제3자 제공을 목적으로 개인정보를 수집하는 경우에는 (i) 그 수집을 금지시켜야 할 정보주체의 정당한 이익이 있다고 인정될 수 있는 경우를 제외하고는, 정보주체의 동의 없이 개인정보를 수집할 수 있고, (ii) 특히, 일반적으로 접근이 가능한 출처로부터 얻을 수 있는 개인정보인 경우에는 그 수집을 금지시켜야 할 압도적인 정당한 이익이 정보주체에게 있는 경우를 제외하고는 정보주체의 동의 없이 수집할 수 있다. 물론 개인정보처리자는 수집할 때 정보처리의 목적을 분명히 명시하여야 한다(제29조 제1항).

제29조 (제3자 제공을 목적으로 하는 업무의 수행에 있어서 개인정보의 수집 및 기록)

(1) 제3자 제공의 목적, 특히 광고, 정보제공서비스, 상업적인 주소 목록작성, 시장조사나 여론조사를 목적으로 하는 업무를 수행함에 있어서 개인정보를 수집, 저장 또는 수정하는 것은 다음 각 호의 1의 경우에 허용된다.

1. 자신의 개인정보가 수집, 저장, 수정되지 못하게 할 정당한 이익이 정보주체에게 있다고 볼만한 근거가 전혀 없는 때

2. 당해 개인정보가 일반적으로 접근이 가능한 출처로부터 얻을 수 있는 것이거나 또는 당해 개인정보처리자가 그 개인정보를 공표할 수 있는 권리가 있는 때. 다만, 자신의 개인정보가 수집, 이용 또는 처리되지 못하게 할 압도적인 정당한 이익이 정보주체에게 명백히 있는 경우에는 그러하지 아니하다.

개인정보를 수집할 때 정보처리의 목적은 구체적으로 명시되어야 한다.

(2) 위 제1항의 목적과 관련한 제3자 제공은 다음의 경우에 허용된다.

1. (a) 개인정보를 제공받는 제3자가 그 개인정보를 알아야 할 정당한 이익을 확실하게 증명하거나 또는 (b) 제28조 제3항 제3호에 열거한 개인정보가 명부형식으로 편집되어 광고 또는 시장조사나 여론조사의 목적으로 제공되는 경우, 및

2. 자신의 개인정보가 제3자에게 제공되지 못하게 할 정당한 이익이 정보주체에게 있다고 볼만한 근거가 전혀 없는 때.

(3) 생략

(4) 이 법 제28조 제4항 및 제5항은 제공받은 개인정보를 처리하거나 이용하는 경우에 적용된다.

(5) 제28조 제8항 및 제9항은 준용된다.

5. 일본 개인정보보호법상의 허용기준

일본의 민간부문 일반법인 개인정보보호법은 유럽의 경우보다 민간기관이 정보주체의 동의 없이도 개인정보를 합법적으로 처리할 수 있는 경우를 더욱 폭넓게 인정하고 있는 것으로 분석된다. 예컨대, 위에서 본 바와 같이 유럽연합, 영국, 독일은 정보처리가 허용되기 위한 요건으로서, 정보주체의 동의 외에 여러 가지 정당한 목적과 상황에 관한 요건들을 구체적으로 열거해 놓고 있다. 그리고 정당한 업무수

행을 위한 정보처리의 경우에도 그로 인해 정보주체가 입는 불이익이 현저히 클 때에는 허용되지 않는다는 이익형량 분석을 정당성 판단기준으로 제시해 놓고 있다. 이에 반해, 일본은 자체적인 이용목적의 수집·처리의 허용기준과 관련해서는 목적과 상황에 관한 구체적인 요건을 설정하지 않고 있으며 또 정당한 업무수행의 이익과 정보주체의 권리보호의 이익 사이의 형량을 달리 요구하고 있지 않다. 즉, 자체적인 이용 목적의 개인정보 수집은 정보주체의 동의 없이 개인정보처리자가 자신의 업무 수행을 위해 얼마든지 할 수 있도록 허용하고 있다. 다만, 이용목적을 특정하도록 하고 그 목적에 필요한 한도 내에서만 이용하도록 하는 요건과 고지의무를 부과하고 있다. 그러나 제3자 제공에 대해서는 다소 엄격한 기준을 설정하고 있다.

(1) 자체 이용목적의 수집의 허용기준

일본의 민간부문 일반법인 개인정보보호법은 민간의 개인정보처리기관(“개인정보취급사업자”)이 자신의 사업상의 목적을 위하여 정보주체의 동의 없이 개인정보를 수집 및 이용할 수 있도록 허용하지만, 그러나 그 이용목적은 “가능한 한 특정”하도록 요구하고 있다(제15조 제1항). 그리고 그 이용목적의 변경을 원칙적으로 허용하지 않고, 다만, 처음에 특정했던 이용목적과 “상당한 연관성이 있다고 합리적으로 인정되는 범위” 내의 다른 목적은 목적의 변경으로 보지 아니한다(제15조 제2항).

개인정보취급사업자는 이러한 목적달성에 필요한 범위 내에서 자유롭게 개인정보를 자체적으로 ‘이용’할 수 있다(제16조 제1항).⁶²⁰ 또한 개인정보취급사업자가 합병 등의 사유로 다른 사업을 승계함에 따라 다른 사업자가 취급하고 있던 개인정보를 취득한 경우에는 승계 이전의 이용목적의 달성에 필요한 범위 내에서 자유롭게 그 개인정보를

620) ‘제3자 제공’에 대해서는 달리 규율하고 있다(제23조). 이에 관해서는 뒤에서 살핀다.

이용할 수 있다(제16조 제2항). 이 범위를 넘어선 이른바 ‘목적 외 이용’은 원칙적으로 금지된다. 그러나 다음의 다섯 가지 경우에는 목적 외 이용이 허용된다: ① 미리 본인의 동의를 얻은 경우(제16조 제1항 및 제2항) ② 법령에 근거한 경우(제16조 제3항 제1호) ③ 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우(제16조 제3항 제2호) ④ 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위해 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우(제16조 제3항 제3호) ⑤ 국가기관 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 경우(제16조 제3항 제4호).

제15조 (이용목적의 특정) ① 개인정보취급사업자는 개인정보를 취급함에 있어서 그 이용의 목적(이하 “이용목적”이라 한다)을 가능한 한 특정하여야 한다.

② 개인정보취급사업자는 이용 목적을 변경하는 경우에는 변경전의 이용목적과 상당한 연관성이 있다고 합리적으로 인정되는 범위를 초과해서 변경하여서는 아니 된다.

제16조 (이용목적에 의한 제한) ① 개인정보취급사업자는, 미리 본인의 동의를 얻지 않고서는, 전조의 규정에 의해 특정된 이용목적의 달성에 필요한 범위를 넘어서 개인정보를 취급하여서는 아니 된다.

② 개인정보취급사업자는, 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 개인정보

보를 취급하여서는 아니 된다.

③ 전 2항의 규정은 다음 각 호의 1에 해당하는 경우에는 적용하지 아니한다.

1. 법령에 근거한 경우
2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우
3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위해 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우
4. 국가기관 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 경우.

(2) 제3자 제공의 허용기준

일본의 민간부문 일반법인 개인정보보호법은 민간의 개인정보처리자(“개인정보취급사업자”)가 수집한 개인정보를 제3자에게 제공 혹은 공유하는 것을 원칙적으로 금하고 있다(제23조 제1항). 그러나 여기에는 세 가지 유형의 예외를 넓게 인정하고 있다.

1) 예외 1 : 수집목적 외 제공

다음의 여섯 가지 경우에는 수집목적의 범위를 벗어난 제3자 제공 혹은 공유가 허용된다(제23조 제1항).

- (i) 사전에 동의를 받은 경우
- (ii) 법령에 근거한 경우
- (iii) 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
- (iv) 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특

히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
(v) 국가기관 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 때

2) 예외 2 : 제3자 제공이 수집목적인 경우 opt-out 방식의 허용

일본의 개인정보보호법은 유럽과 마찬가지로 민간의 개인정보처리자가 제3자의 정당한 업무수행을 위하여 또는 광고나 마케팅 목적을 위하여 수집·처리한 개인정보를 정보주체의 동의 없이 제3자에게 제공하는 것을 합법적으로 허용하고 있다. 다만, 이 때 정보주체에게는 사전 고지와 사후 거부권(right to object)을 주어 통제할 수 있도록 하고 있다.

즉, 사후에 정보주체의 요청이 있으면 제3자 제공을 정지한다는 조건 하에, 4가지 사항을 미리 통지 또는 쉽게 알 수 있도록 하고 있는 경우에는 정보주체의 사전 동의 없이도 제3자 제공이 가능하다. 미리 알려 주어야 할 4가지 사항은 (i) 제3자 제공을 이용목적으로 한다는 점, (ii) 제3자에게 제공되는 개인정보의 항목 (iii) 제3자 제공의 수단 또는 방법 (iv) 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인정보의 제3자 제공을 정지한다는 점이다(제23조 제2항). 그리고 위 (ii)와 (iii)의 사항을 변경하는 때에는 그 변경내용을 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다(제23조 제3항).

3) 예외 3 : 제3자 제공으로 보지 않는 경우

다음의 3가지 경우에는 제3자 제공으로 보지 않는다(제23조 제4항).
(i) 개인정보취급사업자가 이용목적의 달성에 필요한 범위 내에서

개인데이터의 취급의 전부 또는 일부를 위탁하는 경우

(ii) 합병 기타의 사유에 의한 사업의 승계에 수반하여 개인데이터가 제공되는 경우

(iii) 개인데이터를 특정의 자와의 사이에서 공동으로 이용하는 경우로서, 그 취지 및 공동으로 이용되는 개인데이터의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인데이터의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때.

제23조(제3자 제공의 제한) ① 개인정보취급사업자는, 다음 각 호의 1에 해당하는 경우를 제외하고, 미리 본인의 동의를 얻지 않고서는 개인데이터를 제3자에게 제공하여서는 아니 된다.

1. 법령에 근거한 경우
2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때
4. 국가기관 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 때

② 개인정보취급사업자는 제3자에게 제공되는 개인데이터에 대하여, 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지하는 것으로 하고 있는 경우에 있어서, 다음에 열거하는 사항에 대하여 미리 본인에게 통지하거나 또는 본인이 용이하게 알 수 있는 상태에 두고 있는 때에는, 전항의 규

정에 불구하고, 당해 개인정보를 제3자에게 제공할 수 있다.

1. 제3자 제공을 이용목적으로 한다는 점
2. 제3자에게 제공되는 개인정보의 항목
3. 제3자 제공의 수단 또는 방법
4. 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인정보의 제3자 제공을 정지한다는 점

③ 개인정보취급사업자는 전항 제2호 또는 제3호에 해당하는 사항을 변경하는 경우에는 변경하는 내용에 대해 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다.

④ 다음 각호의 1에 해당하는 경우에 있어서 당해 개인정보의 제공을 받는 자는 전 3항의 규정의 적용에 대해서는 제3자에 해당하지 않는 것으로 한다.

1. 개인정보취급사업자가 이용목적의 달성에 필요한 범위내에서 개인정보의 취급의 전부 또는 일부를 위탁하는 경우
2. 합병 기타의 사유에 의한 사업의 승계에 수반하여 개인정보가 제공되는 경우
3. 개인정보를 특정의 자와의 사이에서 공동으로 이용하는 경우로서, 그 취지 및 공동으로 이용되는 개인정보의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인정보의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때

⑤ 개인정보취급사업자는, 전항 제3호에서 규정하는 이용하는 자의 이용목적 또는 개인정보의 관리에 대해 책임을 지는 자의 성명 혹은 명칭을 변경하는 경우에, 변경하는 내용에 대해 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다.

제 3 절 입법예고안의 수집 · 이용 · 제공의 허용기준에 대한 입법평가

1. 종합적 평가

위에서 살핀 바와 같이, 유럽연합과 영국은 수집 · 이용 · 제공(=처리)이 허용되는 법적 기준을 단일적으로 규정하는 입법방식을 취하고 있는 반면, 독일은 자신의 업무수행 목적의 수집 · 이용 · 제공과 제3자 제공목적의 수집 · 제공을 나누어 법적 기준을 설정하고 있고, 일본은 이와는 약간 달리 자체 이용목적의 수집과 제3자 제공을 나누어 다르게 법적 기준을 설정하는 입법방식을 취하고 있다.

그러나 자세하게 분석해 보면, 이들 제 외국의 개인정보보호법은 약간의 차이는 있지만 기본적으로 수집, 이용, 제공에 대해 거의 유사한 법적 허용기준을 마련하고 있음을 알 수 있고, 또 그 허용기준은 합리적이고 안전한 수집 · 이용 · 제공이 가능하도록 세밀하고 세심한 주의를 기울여 법제화되어 있음을 알 수 있다. 개인정보의 보호와 이용을 균형 있게 조화시키고 있다는 평가가 가능하다. 그러나 우리의 입법예고안은 이들 외국의 입법례와 비교해 보면 허용기준에 있어서 상당한 차이가 있고, 입법기준이 매우 거칠게 법제화되어 있다는 느낌을 지울 수 없다. 일반개인정보의 수집 · 이용의 허용기준은 유럽연합의 입법례와 유사하게 법제화하고 있어, 이전에 제17대 국회에 제출되었던 「노회찬 법안」과 「이은영 법안」에 비해 진일보한 측면이 있다. 그러나 유럽이나 일본과는 달리, 일반개인정보의 제3자 제공을 과도하게 제한하고 있을 뿐만 아니라, 민감정보의 수집 · 이용 · 제공의 허용기준이 너무 엄격하여 향후 시행되었을 때 매우 심각한 사회적 혼란과 비용을 초래할 것으로 평가된다.

이러한 입법예고안의 기저에는 여전히 개인정보를 “비밀”로 취급하는 그릇된 오해와 그에 따라 정보주체의 동의를 절대화하려는 잘못된 인식이 깔려 있는 것으로 분석된다. 보다 면밀하고 세밀한 분석을 통해 개인정보의 이용과 보호를 균형 있게 조화시키려는 노력이 절실히 필요하다. 우리의 입법예고안이 수집·이용·제공의 허용기준을 입법화하는 방식을 보면, 우선 공공부문과 민간부문을 장을 나누어 달리 규정하지 않고 동일 조항에서 함께 묶어 규정하고 있다. 이 점은 유럽연합과 영국의 입법례와 유사하다. 그러나 ‘자체 이용’과 ‘제3자 제공’을 분리하여 그 허용기준을 달리 입법화하고 있는 점에서는 일본의 입법방식에 유사하다. 또한 우리의 입법예고안은 일반개인정보와 민감개인정보를 나누고 그 처리의 허용기준을 달리 정하고 있는 점에서는 유럽의 입법방식에 유사하다.

이하에서는 우리의 입법예고안의 허용기준에 대해 그 타당성과 적정성 여부를 평가하고 그 수정대안을 제시하고자 한다.

2. 일반개인정보 수집·이용의 허용기준의 타당성

입법예고안 제15조 제1항은 ‘일반개인정보’의 수집·이용이 정당화되기 위한 실체적 요건을 6가지로 제시하고 있다.⁶²¹⁾ 유럽연합, 영국, 독일의 개인정보보호법과 같이 정보주체의 동의를 여러 합법성 요건 중의 하나로 제시하면서, 정보주체의 동의가 없더라도 ‘정당한 업무수행에 필요한 범위 내에서’ 개인정보의 수집·이용을 허용하고 있다. 이는 타당하고 균형 잡힌 법적 기준이라고 평가된다.

621) 입법예고안 제15조는 “일반개인정보”라는 표현을 사용하고 있지만, 제22조에서 별도로 “민감정보”의 처리(수집·이용·제공)를 규율하고 있기 때문에, 이 제15조 제1항은 민감정보를 제외한 일반개인정보의 수집·이용에 관한 실체적 요건을 규정한 것이 된다.

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 소관 업무의 수행을 위하여 불가피한 경우
4. 계약의 이행을 위하여 불가피하게 수반되는 경우
5. 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체의 사전 동의를 받기 곤란한 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우

다만, 다음의 몇 가지 점에서 유럽이나 일본의 법적 기준에 비하여 약간 더 강화되어 있는 것으로 평가된다.

첫째, 입법예고안은 위 제3호에서 공공기관의 수집·이용의 허용요건을 소관 업무의 수행을 위하여 “불가피한 경우”로 설정하고 있는데, 이 “불가피한 경우”라는 개념이 “필요한 경우”라는 개념보다 우리의 언어사용례에서는 더 엄격하게 느껴진다. 현행의 「공공기관의 개인정보보호에 관한 법률」 제5조는 “공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다.”고 규정하고 있는 것과 굳이 비교한다면, 수집·이용의 정당성 요건을 좀 더 강화하고 있다는 느낌을 받는다. 물론 실제의 적용에 있어서는 별반 차이가 나지 않을 수도 있을 것으로 짐작된다.

둘째, 위 제6호는 민간기관이 정보주체의 동의 없이 적법하게 수집·이용할 수 있는 실체적 요건을 설정한 조항인데, 정보주체의 권리보호의 이익과의 **형량기준**이 유럽의 경우보다 약간 더 엄격하게 설

정되어 있다. 즉, 제6호에 의하면 정보처리의 이익이 “명백히 정보주체의 권리보다 우선하는 경우”에 한하여 그 수집·이용은 적법한 것이 된다. 이에 비해, 유럽연합 지침에서는 민간기관의 정보처리의 이익이 “정보주체의 기본적인 권리와 자유를 보호해야 하는 이익보다 더 클 때”에 그 수집·이용은 허용된다(제7조 f항). 또한 영국의 개인정보보호법은 수집·이용이 “구체적인 사안에서 정보주체의 권리와 자유 또는 정당한 이익을 침해하여 정당화될 수 없을 때” 그것은 금지된다. 그리고 독일 연방개인정보보호법의 형량기준은 두 가지 경우로 나누어 설정되어 있다. (i) “일반적으로 접근이 가능한 개인정보”(공개된 개인정보)의 경우에는 “그 수집·이용을 금지시켜야 할 정보주체의 정당한 이익이 개인정보처리자의 정당한 이익보다 **명백히 우월한 때**”에 한하여 금지된다. (ii) 그 외의 개인정보는 “그 수집·이용을 금지시켜야 할 **압도적인 정당한 이익**이 정보주체에게 있다고 볼 만한 근거가 있는 때”에는 그 수집·이용이 금지된다. 한편, 일본의 개인정보보호법에는 이러한 형량기준 자체가 없다. 그리하여 개인정보취급사업자는 스스로 특정하여 제시한 이용목적의 달성에 필요한 범위 내에서 자유로이 수집·이용할 수 있다.

또한, 우리의 입법예고안의 문안 중 정보처리의 이익이 “명백히 정보주체의 권리보다 우선하는 경우”라는 표현은 이익형량의 기준으로서는 다소 어색해 보인다. 정보주체의 “권리가 우선”한다고 하기보다는 “수집·이용을 금지시켜야 할 정보주체의 이익이 우선”한다고 규정하는 것이 타당해 보인다.

[수정대안]

6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우. 다만, 수집·이용을 금지시켜야 할 정보주체의 이익이 더 우월한 때에는 그러하지 아니하다.

3. 정보주체의 동의권 인정 조항의 문제점

입법예고안 제15조 제1항이 개인정보의 수집·이용에 있어서 정보주체의 동의 요건을 절대화하지 않고 정당한 업무수행을 위해 필요한 범위 내에서 동의 없이 수집·이용할 수 있다고 규정한 것은 타당한 것으로 평가되지만, 그런데 입법예고안 제4조 제2호의 규정내용은 이러한 제15조 제1항과 모순되고 상호 충돌한다.

제15조 제1항은 정보주체의 동의 없는 정당한 수집·이용을 허용하고 있는 반면, 제4조 제2호는 “정보주체의 권리”의 하나로서 “정보주체는 자신의 개인정보 처리와 관련하여 개인정보의 처리에 관한 동의, 동의범위 등을 선택하고 결정할 권리를 가진다.”고 규정하고 있기 때문이다.

이 제4조 제2호의 의미가 정보주체에게 자신의 개인정보 처리(=수집·이용·제공)와 관련하여 동의권을 부여하는 것이라면, 그리하여 정보주체의 동의 없는 개인정보의 처리를 금지하는 것이라면, 이는 정면으로 제15조 제1항과 충돌하게 된다. 그러나 그것이 명백히 잘못된 입법방향임은 위에서 강조한 바 있다. 만약 그런 취지라면 제2호는 삭제되어야 마땅하다. 특히 입법예고안은 민간부문뿐만 아니라 공공부문에 공통적으로 적용되는 법률인데, 공공기관의 업무수행에 필요한 개인정보의 처리에 대하여 정보주체의 동의권을 인정한다면 공적 업무의 수행은 거의 불가능하게 될 것이다.

다만, 제4조 제2호의 의미가 ‘제15조 제1항 제1호에 해당하는 경우, 즉 개인정보처리자가 정보주체의 동의를 받아 수집·이용하려고 하는 경우에 정보주체는 동의를 할 것인지, 또 동의를 한다면 어느 범위까지 동의를 할 것인지에 관하여 자유롭게 결정할 권리가 있다’는 것이라면, 제15조 제1항과 특별히 충돌하는 것은 아니라고 하겠다. 그러나

이 같은 ‘자유롭게 동의를 할 수 있는 권리’는 너무나 당연한 것으로서 굳이 정보주체에게 개인정보보호법이 인정하는 특별한 권리로서 명문화할 필요가 없는 것이 아닌가 생각된다.

요컨대, 제4조 제2호는 자칫 오해를 일으킬 수 있는 규정이거나 아니면 굳이 명시할 필요가 없는 규정으로서 삭제하는 것이 타당한 것으로 평가된다.

4. 일반개인정보 제공의 과도한 제한과 그 문제의 심각성

(1) 평가의 관점 : 제3자 제공의 효용성과 위험성

개인정보를 수집하는 것은 크게 ‘자체 이용’을 위한 경우와 ‘제3자 제공’을 위한 경우로 나누어진다. 일반적으로는 주로 자체 이용을 위하여 개인정보가 수집된다. 공공기관이 법적으로 주어진 자신의 소관 업무를 수행하기 위하여 개인정보를 수집하거나 또는 민간기업이 고객관리나 자사제품의 홍보를 위하여 수집하기도 한다. 그리고 이러한 자체 이용이 주된 목적이지만, 부수적으로 제3자 제공이 이루어지는 경우가 있다. 예컨대, 판매계약에 따른 상품의 송달을 위해 제3자인 배송업자에게 주소정보를 제공하는 경우이다.

그러나 한편 처음부터 제3자 제공을 목적으로 수집되는 경우가 있다. 예컨대, 민간의 경우 정보판매업자(조선일보나 중앙일보의 인물정보서비스, 법조인대관 출판)나 신용정보업자는 제3자 제공을 목적으로 개인정보를 수집하고 이를 가공하여 그 정보를 원하는 고객이나 의뢰인에게 제공한다. 또 기업의 홍보나 광고 또는 여론조사를 위한 목적에서 개인정보를 수집하여 제공하기도 한다. 이러한 개인정보의 유통은 업무제휴의 방식으로 이루어질 수도 있고 또는 수익을 위한 판매의 형태로 이루어지기도 한다.

어떤 방식이든지 간에 개인정보의 사회적 유통은 많은 사회적 효용을 가지고 있다. 예컨대, 마케팅(marketing)⁶²²의 사회적 효용은 여기서 새삼 언급할 필요가 없을 정도로 지대하고, 이러한 마케팅 목적의 개인정보의 수집·이용과 그 유통 또한 사회적으로 필요할 뿐만 아니라 그 사회적 효용이 매우 크다. 오늘날의 마케팅에 있어서 고객의 개인정보의 수집·처리는 불가결의 필수조건이기 때문이다.

특히 직접 마케팅(direct marketing)⁶²³ 방식은 판매자(marketer)들에게는 매우 매력적이다. 왜냐하면 많은 경우에 그 긍정적 효과를 직접 측정할 수 있기 때문이다. 예컨대, 백만 건의 광고 메일을 보냈는데 거기에 만 명의 고객이 긍정적인 반응을 했다면 직접 그 효과를 측정할 수 있게 된다. 그러나 그 광고 메일을 불쾌하게 생각하는 고객의 부정적인 반응은 쉽게 측정되지 않는다. 최근 대량의 광고메일이 원치 않는 고객에게 무작위로 전달됨에 따라 또 다른 사회적 비용이 지불되고 있다. 원치 않는 광고메일(spam)에 의한 고객의 불쾌감이나 사생활의 평온 방해 외에도 그 처리에 드는 시간 낭비나 환경적 문제 등이 야기되고 있다.

이 경우 만일 고객에 관한 보다 정확하고 상세한 정보를 판매자가 가지고 있다면 그 고객에 대한 맞춤형광고를 할 수 있을 것이고, 그 결과 스팸의 문제가 일정한 정도 해결될 수 있을 것이다. 이 부분은 개

622) 일반적으로 “마케팅”(marketing)이란 광고나 브랜드화를 통해 상품의 판매를 촉진하는 활동을 말한다. 그러나 전문적인 용어로는 이 보다 더 넓은 개념으로 사용된다. 미국마케팅협회(American Marketing Association)는 이렇게 규정하고 있다: “마케팅이란 가치를 생산해서 이를 고객에게 전달하기 위한 그리고 당해 기업과 주주들에게 이익이 되는 방식으로 고객과의 관계를 관리하기 위한 조직적 활동 및 일련의 과정이다.”

623) 직접 마케팅(direct marketing)은 두 가지 점에서 다른 유형의 마케팅 방식과 차이가 있다. 하나는 중간의 매개체(방송·신문 등) 없이 직접 고객에게 메시지를 전달한다는 점이다. 직접우편, 이메일, 텔레마케팅 등의 방식으로 이루어지며 통상 그 메시지를 원치 않는 고객에게도 전달된다. 또 다른 특징은 고객의 긍정적 반응을 측정하거나 추적할 수 있다는 점이다.

인정보처리의 긍정적 측면이다. 그러나 한편으로 고객에 관한 상세하고 정확한 개인정보의 보유와 유통은 고객의 사생활 침해의 문제를 야기할 수도 있다. 이 점은 마케팅에 있어서 개인정보처리의 부정적 측면이다.

이처럼 마케팅 목적의 개인정보처리(=수집·이용·제공)가 긍정적 측면과 부정적 측면을 동시에 가지고 있을 때 그 개인정보처리에 관하여 법적으로 어떻게 규율하는 것이 바람직한가 하는 문제가 제기된다.

여기에는 몇 가지 대안을 상정해 볼 수 있다.

첫째, 마케팅 목적의 개인정보처리(=수집·이용·제공)를 전면 금지시키는 방안이 있을 수 있지만, 그러나 이는 결코 바람직한 대안이라고 볼 수 없다. 마케팅 행위가 반사회적이거나 불법적인 행위가 아닌 한 그것을 위한 개인정보처리를 불법화할 수는 없다. 세계적으로도 그러한 사례는 찾아볼 수 없다.

둘째, 정보주체에게 일정한 통제권을 주는 방안을 고려할 수 있다. 이 경우 통제권을 주더라도, 사전 동의 없는 개인정보의 처리를 금지시킬 것인지(opt-in 방식), 아니면 사전 동의가 없더라도 개인정보의 처리(=수집·이용·제공)를 허용하되 사후적으로 그 처리를 거부할 수 있는 권리(거부권)를 줄 것인지(opt-out 방식)를 나누어 고려할 수 있다. 유럽과 일본은 후자의 방식을 채택하고 있다.

셋째, opt-out 방식을 채택한다 하더라도 마케팅 목적으로 처리되는 개인정보의 범위를 제한하는 방안을 고려할 수 있다. 특히 민감개인정보의 처리를 어느 정도 허용할 것인지가 검토되어야 한다.

넷째, 자신의 마케팅 목적을 위하여 개인정보를 수집·가공·이용하는 것과 타인의 마케팅 목적을 위하여 개인정보를 수집·가공·제공하는 것을 구별하여 달리 규율할 것인가 하는 문제가 있다.

이상의 평가요소와 관점을 전제로 개인정보의 제3자 제공 또는 공유의 문제를 법적으로 어떻게 규율할 것인지, 제3자 제공의 허용 요

건을 어떻게 설정할 것인지에 관하여 현행의 입법예고안을 평가해 보고자 한다.

(2) 입법예고안의 내용 분석과 비판

입법예고안은 일반개인정보와 민감개인정보를 나누어 허용기준을 정하고 있고, 일반개인정보는 다시 수집·이용의 허용 요건(제15조 및 제18조)⁶²⁴⁾과 제3자 제공의 허용 요건(제17조 및 제18조)을 나누어 달리 규정하고 있다. 한편, 민감개인정보의 처리(=수집·이용·제공)의 허용기준은 제22조에서 규정하고 있다.⁶²⁵⁾

그런데 입법예고안 제17조와 제18조는 제3자 제공을 유럽이나 일본의 개인정보보호법에 비교하여 지나치게 제한적으로 허용하고 있어서 사회적으로 필요한 개인정보의 유통을 막고 있는 것으로 평가된다. 그 사회적 파장은 매우 크고 심각할 것으로 보인다.

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호, 제3호 및 제5호에 따라 개인정보를 수집한 목적 범위 안에서 제공하는 경우

② 개인정보처리자는 제1항에 따른 동의를 받을 때에는 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보를 제공받는 자
2. 제공하는 개인정보의 항목
3. 개인정보를 제공받는 자의 개인정보 이용목적

624) 이에 대한 분석과 평가는 위 제3장 제3절 2. 참조.

625) 이에 대한 분석과 평가는 아래 제3장 제3절 5. 참조.

4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

③ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 제3자에게 제공하는 근거 및 제2항 각 호의 사항을 명확히 제시하여야 한다.

제18조(개인정보의 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조 제1항 또는 제17조 제1항에 따른 범위를 초과하여 이용하거나 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니하는 범위 안에서 개인정보를 목적 외로 이용하거나 제3자에게 제공할 수 있다. 다만, 제5호부터 제8호까지는 공공기관의 경우에 한한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우
5. 개인정보를 목적 외로 이용하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의를 거친 경우
6. 조약 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우

8. 법원의 재판업무수행을 위하여 필요한 경우

③ 개인정보처리자는 제2항 제1호에 따른 동의를 받을 때에는 다음 각 호의 해당되는 사항을 정보주체에게 알려야 한다.

1. 개인정보의 이용목적(제공시에는 제공받는 자의 이용 목적을 말한다)

2. 개인정보의 보유 및 이용기간(제공시에는 제공받는 자의 보유 및 이용기간을 말한다)

3. 개인정보를 제공받는 자

4. 이용 또는 제공하는 개인정보의 항목

④ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 근거 및 제3항 각 호의 해당되는 사항을 명확히 제시하여야 한다.

⑤ 공공기관은 제2항 제2호부터 제8호까지에 따라 개인정보를 목적 외로 이용하거나 제공하는 경우에는 그 이용 또는 제공의 법적 근거·목적 및 범위 등에 관하여 필요한 사항을 행정안전부령이 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

입법예고안은 일반개인정보를 제3자에게 제공할 수 있는 ‘일반적 허용기준’을 제17조 제1항에서 정하고, 제18조 제2항에서는 ‘예외적 허용기준’을 정하고 있다.

우선 일반적 허용기준을 보면, 제17조 제1항 제1호와 제2호는 공공이나 민간의 개인정보처리자가 개인정보를 제3자에게 제공(공유 포함)할 수 있는 경우를 다음의 4가지로 제한하고 있다: (i) 정보주체의 동의를 받은 경우(제1호); (ii) 제15조 제1항 제2호(“법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우”)에 따라 개인정보를 수집한 목적 범위 안에서 제공하는 경우(제2호); (iii) 제15조 제1항 제3호(“공공기관이 소관 업무의 수행을 위하여 불가피한 경

우”)에 따라 개인정보를 수집한 목적 범위 안에서 제공하는 경우(제2호); (iv) 제15조 제1항 제5호(“정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체의 사전 동의를 받기 곤란한 경우”)에 따라 개인정보를 수집한 목적 범위 안에서 제공하는 경우(제2호).

그러나 이 제17조의 규정내용은 몇 가지 심각한 문제점을 안고 있다.

첫째, 제15조 제1항의 제2, 3, 5호와 연결하여 법률문장을 구성하고 있는데, 그 의미내용이나 취지가 애매할 뿐만 아니라 규정 상호간의 정합성이 결여되어 있다. 제15조(개인정보의 수집·이용)는 제1항 제2, 3, 5호의 경우에 정보주체의 동의 없이 개인정보를 “수집·이용”할 수 있다는 규정이다. 이 제15조는 문언표현상 개인정보처리자 내부의 자체적인 이용을 목적으로 하는 수집에 관한 규정이다. 그렇다면 제17조 제1항은 “내부이용을 전제로 수집한 개인정보를 그 내부이용 목적의 범위 안에서 제3자에게 제공할 수 있다”는 것이 되는데, 무슨 의미인지 이해하기 어렵다. 예컨대, 제15조 제1항 제3호의 경우 공공기관의 개인정보파일 보유목적은 자신의 소관 업무의 수행을 위한 것이다. 그런데 어떻게 그 보유목적의 범위 안에서 다른 공공기관에게 제공할 수 있는 것인지 의문이 생긴다. 다만, 제17조 제1항이 의미가 있으려면, 수집목적 안에 처음부터 제3자 제공을 예정한 것이 있을 수 있다는 것인데, 그렇다면 제15조의 제목이 “수집·이용”이라고 하는 것은 맞지 않다. 물론 자신의 소관 업무를 수행하기 위해서 제3자와의 업무제휴가 필요하고 그 한도에서 개인정보를 공유할 수는 있는데, 그것이 처음부터 예정되어 있고 그리하여 수집 당시 제3자 제공을 목적으로 하고 있었다면 그러한 목적 범위 안에서 제3자에게 제공할 수 있도록 허용한 것으로 이해될 수 있다. 사실 처음부터 제3자 제공 혹은 공유를 목적으로 수집되는 경우가 있다. 그렇다면 굳이 수집·이용에 관한 제15조 제1항 제2, 3, 5호와 연결하여 제3자 제공을

허용하는 기준을 정할 것이 아니라, 독자적으로 표현문구를 사용하는 것이 타당할 것이다.

둘째, 더욱 심각한 문제는 민간의 개인정보처리자가 “자신이나 제3자의 정당한 업무수행을 위해서” 개인정보를 제공 혹은 공유할 수 있는 길을 원천봉쇄하고 있다는 점이다. 유일하게 정보주체의 사전 동의를 받아야만 제3자 제공이 가능하도록 하고 있다(opt-in 방식). 이는 세계 유례가 없는 입법이다. 그러면서도 공공기관의 제3자 제공은 아무런 제한 없이 허용하고 있다.

제17조는 “민간의 개인정보처리자”가 정보주체의 동의 없이 제3자에게 개인정보를 제공할 수 있는 경우를 딱 두 가지 경우, 즉 ① 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(제15조 제1항 제2호) ② 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체의 사전 동의를 받기 곤란한 경우(제15조 제1항 제5호)에 한정하고 있다. 그리고 제18조에서는 제3자 제공이 허용되는 예외적인 경우로서, ① 정보주체로부터 별도의 동의를 받은 경우(제2항 제1호) ② 다른 법률에 특별한 규정이 있는 경우(제2항 제2호)⁶²⁶⁾ ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(제2항 제3호) ④ 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우(제2항 제4호)에 한하여 제3자 제공을 예외적으로 허용하고 있다.

이들 규정에 따르면, 민간의 개인정보처리자가 “자신 또는 제3자의 정당한 업무수행을 위하여” 개인정보를 공유하거나 제3자에게 제

626) 제17조에서 제3자 제공이 허용되는 경우로 “정보주체의 사전 동의”와 “법률의 규정”을 들고 있는데, 또 다시 제18조에서 이를 제시하는 것은 어떤 의미가 있는지 불명확하다. 매우 혼란스러운 입법안이다.

공할 수 있는 경우는 유일하게 정보주체의 사전 동의를 받는 방법(opt-in 방식)뿐이다. 정보판매업자(조선일보나 중앙일보의 인물정보서비스, 법조인정보서비스)나 신용정보업자는 제3자 제공을 목적으로 개인정보를 수집하고 이를 가공하여 그 정보를 원하는 고객이나 의뢰인에게 제공하게 되는데, 입법예고안에 의하면 정보주체의 사전 동의 없는 이러한 제3자 제공은 모두 불법이 된다. 또 기업의 홍보나 광고 또는 여론조사를 위한 목적에서 우편주소나 이메일주소를 수집하여 제공하는 행위도 정보주체의 사전 동의를 받지 않으면 모두 불법이 된다. 심지어 그 위반행위에 대해서는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하여진다(제59조 제1호 및 제2호). 심지어 입법예고안에 의하면, 판매계약에 따른 상품의 송달을 위해 제3자인 배송업자에게 주소정보를 제공하는 경우나 또는 마케팅 목적으로 고객의 이메일정보를 위탁업자에게 제공하는 경우도 사전 동의가 없다면 모두 불법이 될 것이다.

특별법인 『신용정보의 이용 및 보호에 관한 법률』에서 신용정보업자는 정보주체의 동의 없이 개인의 신용정보를 수집하여 의뢰인에게 제공하는 것을 허용하고 있는데, 일반법인 개인정보보호법에서 금지시킨다고 하는 것은 입법체계상으로도 전혀 균형이 맞지 않은 입법이다.

실로 개인정보의 필요한 사회적 유통과 이용의 가치를 전혀 고려하지 않은 세계 유례가 없는 기형적인 입법안이라고 평가할 수밖에 없다.

(3) 대안의 제시

제3자 제공의 허용기준에 관해서는 적어도 유럽의 입법례나 일본의 입법례를 참조할 필요가 있다.

위에서 살핀 바와 같이, 유럽은 제3자 제공의 허용기준을 일반개인정보와 민감개인정보로 나누어서 규정하고 있는데, (i) 일반개인정보는 개인정보처리자나 제3자의 정당한 이익을 달성하기 위한 경우에

정보주체의 동의 없는 제3자 제공을 넓게 허용하되, 다만 정보주체에 사후에 그 제공을 거부할 수 있는 권리(right to object)를 주고 있다. (ii) 그러나 민감개인정보는 제3자 제공을 원칙적으로 금지하면서, 정보주체의 동의가 있거나 또는 그 밖에 제3자 제공이 필요한 경우를 구체적으로 열거하고 있다.⁶²⁷⁾ 일반개인정보에 관하여 좀 더 설명하면 다음과 같다.

유럽연합의 개인정보보호지침은 일반개인정보의 수집·이용 및 제3자 제공이나 공유가 허용되기 위한 법적 기준으로서, “개인정보처리자나 개인정보를 제공받는 제3자가 추구하는 정당한 이익(legitimate interests)을 달성하기 위하여 정보처리가 필요한 때. 다만, 그러한 이익보다 정보주체의 기본적인 권리와 자유(fundamental rights and freedoms)를 보호해야 하는 이익이 더 클 때에는 그러하지 아니하다.”고 규정하고 있다(제7조 f항). 이처럼 유럽연합은 정보주체의 동의 없는 제3자 제공을 개인정보처리자 또는 제3자의 정당한 이익을 달성하기 위하여 필요한 범위 내에서 넓게 인정하고 있다. 다만, “opt-out 방식(사후거부방식)”에 의해 정보주체의 통제권을 인정하고 있다. 즉, 정보주체에게 다음과 같이 사후거부권(right to object)을 주고 있다. 그리고 이 경우에도 거부권의 행사요건을 일반적인 목적의 정보처리(=수집·이용·제공)의 경우와 직접마케팅 목적의 정보처리의 경우를 나누어 달리 규정하고 있다. 후자의 경우에는 조건 없는 거부권의 행사를 인정하고 있다.

제14조 (정보처리에 대한 거부권: right to object) 정보주체는

- (a) 적어도 [공공기관이나 민간기관이 자신의 정당한 업무수행을 위하여 동의 없이 합법적으로 개인정보를 처리할 수 있는 경우

627) 유럽연합과 영국에서 민감개인정보의 제3자 제공을 예외적으로 허용하는 기준에 관해서는 위 제3장 제2절 2.와 3. 참조.

에(제7조 e호 및 f호)], 언제든지 자신의 특별한 상황과 연관된 불가피한 정당한 사유를 제시하면서(at any time on compelling legitimate grounds relating to his particular situation) 자신에 관한 정보의 처리를 거부할 수 있는 권리를 가진다. 다만, 회원국이 국내법으로 이와 달리 규정할 수 있다. 정당한 거부(a justified objection)가 있는 경우에, 당해 개인정보처리기관이 하고 있는 정보처리에서 거부 요청된 정보가 더 이상 포함되어서는 안 된다.

- (b) 직접마케팅(direct marketing) 목적으로 처리될 것이 예상되는 자신에 관한 정보의 처리를, 비용부담 없이 신청에 의하여, 거부할 권리를 가지거나, 아니면 직접마케팅(direct marketing) 목적으로 제3자에게 최초로 제공되기 전이나 자체적으로 이용하기 전에 그 사실을 통지받고 그 목적의 제공이나 이용을 비용부담 없이 거부할 권리를 가진다.

회원국은 위 (b)호 제1문 소정의 권리가 있음을 정보주체가 알 수 있도록 필요한 조치를 취하여야 한다.

또한 독일의 연방개인정보보호법은 민간의 개인정보처리자가 자신의 업무수행을 위한 제3자 제공의 경우와 처음부터 제3자 제공목적으로 수집하는 경우를 나누어 제공의 허용기준을 다르게 정하고 있다. 우선 다음의 경우에는 자신의 업무수행을 위한 제3자 제공이 정보주체의 동의 없이 일반적으로 허용된다(제28조 제1항 제1문).

1. 정보주체와의 계약 또는 준계약적 신뢰관계를 위한 목적인 때
2. 개인정보처리자의 정당한 이익을 보호하기 위하여 필요하고, 또한 그 처리나 이용을 하지 못하게 할 압도적인 정당한 이익이 정보주체에게 있다고 볼 만한 근거가 전혀 없는 때
3. 그 개인정보가 일반적으로 접근이 가능한 것인 때, 또는 개인정보 처리자가 합법적으로 개인정보를 공표할 수 있는 때. 다만, 그 정

보처리를 배제해야 할 정보주체의 정당한 이익이 당해 개인정보처리자의 정당한 이익보다 명백히 우월한 때에는 그러하지 아니하다.

그리고 자신의 업무수행을 위한 경우가 아니라도, (i) “제3자의 정당한 이익을 보호하기 위하여 필요한 때”(제28조 제3항 제1호), 또는 (ii) “광고, 시장조사 그리고 여론조사를 위한 목적인 때”(제28조 제3항 제3호)에는 수집·이용하고 있던 개인정보를 제3자에게 제공하는 것이 허용된다. 다만, 위 (ii)의 경우에는 다음의 조건 하에서만 가능하다. 이용 또는 제공되는 개인정보는 일정 범위의 사람들에 관한 명부형식으로 된 개인정보여야 하고, 그에 포함되는 개인정보는 (a) 당해 정보주체가 그 명부에 포함되는지 여부, (b) 직업, (c) 이름, (d) 직책, (e) 대학학위, (f) 주소, 그리고 (g) 출생연도에 한정되어야 하며, 그리고 당해 정보주체가 그 제공이나 이용을 못하게 할 정당한 이익을 가지고 있다고 믿을만한 근거가 일체 없어야 한다.

그리고 이 경우에 정보주체에게는 다음과 같은 거부권이 주어진다(제28조 제4항).

정보주체가 자신의 정보를 광고, 시장조사 또는 여론조사를 목적으로 이용 또는 제공하지 못하도록 개인정보처리자에게 이의를 제기하는 때에는, 그러한 목적의 이용 또는 제공은 허용되지 아니한다. 광고, 시장조사 또는 여론조사의 목적으로 연락을 받았을 때, 정보주체는 그 개인정보처리자의 신원과 자신의 거부권에 대하여 통지를 받아야 한다. 자신이 알지 못하는 개인정보처리자가 가지고 있던 개인정보를 이용하여 [위 목적으로] 연락을 취하는 자는 그 개인정보의 출처를 정보주체가 알 수 있도록 보장하여야 한다. 정보주체가 위 제3항에 의하여 개인정보를 제공받는 제3자에게 광고, 시장조사 또는 여론조사를 목적으로 하는 처리나 이용을 하지 못하도록 이의를 제기한 때에는, 그 수령인은 그 제공받은 개인정보가 위 목적으로 처리 또는 이용되지 않도록 차단시켜야 한다.

더 나아가, 독일의 연방개인정보보호법은 민간의 기업이 광고, 정보 제공서비스, 상업적인 주소목록작성, 시장조사나 여론조사를 위하여 처음부터 제3자에게 제공하기 위한 목적에서 개인정보를 수집·처리하는 것을 일정한 조건 하에 허용하고 있고(제29조 제1항), 이러한 목적을 위한 제3자 제공을 다음의 경우에 허용하고 있다(제29조 제2항). 물론 이렇게 제3자 제공이 허용된 경우 정보주체에게는 당연히 거부권이 인정된다(제29조 제4항).

1. (a) 개인정보를 제공받는 제3자가 그 개인정보를 알아야 할 정당한 이익을 확실하게 증명하거나 또는 (b) 제28조 제3항 제3호에 열거한 개인정보가 명부형식으로 편집되어 광고 또는 시장조사나 여론조사의 목적으로 제공되는 경우, 및
2. 자신의 개인정보가 제3자에게 제공되지 못하게 할 정당한 이익이 정보주체에게 있다고 볼만한 근거가 전혀 없는 때.

한편, 일본의 민간부문 일반법인 개인정보보호법도 유럽과 마찬가지로 민간의 개인정보처리자가 제3자의 정당한 업무수행을 위하여 또는 광고나 마케팅 목적을 위하여 수집·처리한 개인정보를 정보주체의 동의 없이 제3자에게 제공하는 것을 합법적으로 허용하고 있다. 다만, 이 때 정보주체에게는 사전 고지와 사후 거부권(right to object)을 주어 통제할 수 있도록 하고 있다. 즉, 사후에 정보주체의 요청이 있으면 제3자 제공을 정지한다는 조건 하에, 4가지 사항을 미리 통지 또는 쉽게 알 수 있도록 하고 있는 경우에는 정보주체의 사전 동의 없이도 제3자 제공이 가능하다.⁶²⁸⁾

628) 미리 알려 주어야 할 4가지 사항은 (i) 제3자 제공을 이용목적으로 한다는 점, (ii) 제3자에게 제공되는 개인데이터의 항목 (iii) 제3자 제공의 수단 또는 방법 (iv) 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지한다는 점이다(제23조 제2항). 그리고 위 (ii)와 (iii)의 사항을 변경하는 때에는 그 변경내용을 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다(제23조 제3항).

또한 다음의 3가지 경우에는 제3자 제공으로 보지 않는다(제23조 제4항).

- (i) 개인정보취급사업자가 이용목적의 달성에 필요한 범위 내에서 개인정보의 취급의 전부 또는 일부를 위탁하는 경우
- (ii) 합병 기타의 사유에 의한 사업의 승계에 수반하여 개인정보가 제공되는 경우
- (iii) 개인정보를 특정의 자와의 사이에서 공동으로 이용하는 경우로서, 그 취지 및 공동으로 이용되는 개인정보의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인정보의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때.

5. 민감개인정보에 대한 과도한 보호의 문제점

입법예고안 제22조는 민감개인정보의 처리(수집·이용·제공)에 대하여 일반개인정보와 달리 특별하게 규율하고 있다. 이는 유럽의 입법례를 따른 것으로서, 일본의 경우에는 민감개인정보에 대하여 달리 특별한 규율을 하고 있지 않다. 그런데 입법예고안은 유럽의 입법례에 비하여 이용보다 보호 쪽으로 지나치게 기울어져 있다. 입법예고안은 민감개인정보의 수집·이용·제공을 원칙적으로 금지하면서 그 예외를 ① 정보주체의 사전 동의와 ② 법률의 규정이라는 두 가지 경우로 매우 좁게 설정하고 있어서 그 적용과정에서 심히 불합리한 결과가 예상된다.

제22조(민감정보의 처리 제한) 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는

개인정보로서 대통령령이 정하는 정보(이하 “민감정보“라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 해당되는 사항을 알리고 별도의 동의를 받은 경우
2. 다른 법률에서 명시적으로 민감정보의 처리를 요구하거나 허용하는 경우

이처럼 민감개인정보의 수집·이용·제공을 원칙적으로 금지하는 입법태도는 현행의 「공공기관의 개인정보보호에 관한 법률」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 비롯된 것으로 보인다. 「공공기관의 개인정보보호에 관한 법률」제4조 제1항은 “공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다.”고 규정하고 있다. 또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제23조 제1항은 “정보통신서비스제공자는 사상·신념·과거의 병력 등 개인의 권리·이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항의 규정에 따른 이용자의 동의를 얻거나 다른 법률에 따라 특별히 수집대상 개인정보로 허용된 경우에는 그러하지 아니하다.”고 규정하고 있다.

이하에서는 민감정보의 개념정의의 문제와 민감정보의 과도한 보호 문제를 짚어 보고자 한다.

(1) 민감정보의 개념정의

우선, 민감정보의 개념을 위 두 법률에서는 “사상·신념·과거의 병력 등 개인의 권리·이익이나 사생활을 현저하게 침해할 우려가 있는

개인정보”라고 정의하고 있으나, 입법예고안은 이를 좀 더 구체적으로 정의하고 있다. 입법예고안은 “민감정보”의 개념을 “사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령이 정하는 정보”라고 정의하고 있다.

입법예고안의 개념정의는 유럽연합 개인정보보호지침이나 독일 연방개인정보보호법의 그것과 유사하다. 유럽연합 지침은 특수개인기록을 “인종적 또는 민족적 출신(racial or ethnic origin), 정치적 견해(political opinions), 종교적 또는 철학적 신념(religious or philosophical beliefs), 노동조합 가입여부(trade union membership)를 드러내는 개인기록 및 건강이나 성생활(health or sex life)에 관한 기록”이라고 정의하고 있고, 독일의 법률은 “인종적 또는 민족적 출신, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강이나 성생활에 관한 기록”이라고 규정하고 있다.

그런데 입법예고안의 개념정의 중 막연히 “사상·신념”을 모두 민감정보로 분류하여 특별취급을 하는 것은 그 개념범위가 너무 넓어져서 타당하지 못한 것으로 평가된다. “종교적 신념” 정도로 축소하여 분명하게 명시하는 것이 적절해 보인다. 또한 입법예고안은 “정당의 가입·탈퇴 정보”를 민감정보로 분류하고 있는데, 이를 민감정보로 분류하여 특별히 보호해야 할 필요가 있는지는 의문이다.

(2) 민감정보의 과도한 보호에 대한 비용효과분석

위에서 살핀 바와 같이, 유럽의 개인정보보호법들은 정보주체의 동의 없는 민감정보의 처리(수집·이용·제공)를 원칙적으로 금지하고 있지만, 그에 대한 예외를 넓게 인정하고 있다. 예컨대, 독일 연방개인정보보호법상 민간기관이 정보주체의 동의 없이 민감정보를 처리할 수 있는 경우는 다음과 같다.

첫째, 다음의 4가지 경우에는 동의 없는 수집·이용·제공이 가능하다: ① 동의를 받는 것이 사실상 또는 법적으로 불가능하지만, 정보주체나 제3자의 중대한 이익을 보호하기 위하여 필요한 때 ② 정보주체가 스스로 명시적으로 공개한 때 ③ 법적 권리의 입증·행사·방어에 필요한 때. 다만 수집과 이용을 금지시켜야 할 압도적인 정보주체의 이익이 존재한다고 인정될 때에는 그러하지 아니하다. ④ 학문적 연구의 수행을 위하여 필요한 때. 다만, 그 학문적 이익이 수집을 금지시켜야 할 정보주체의 이익보다 월등히 우월해야 하고, 달리 다른 수단에 의해서는 그 연구의 목적을 달성하기 어려운 경우라야 한다(제28조 제6항).

둘째, 예방의학, 의학적 진단, 치료 또는 건강관리서비스의 제공 목적인 경우에는 정보주체의 동의 없이도 특수개인정보(주로 건강정보나 성생활정보)의 수집이 가능하다. 다만, 그 정보는 의료전문가 또는 그에 상응하는 비밀유지의무를 지는 자에 의하여 처리되어야 한다(제28조 제7항).

셋째, 위 첫째와 둘째의 요건이 충족되는 경우에는 처음에 수집된 목적과는 다른 목적을 위하여 정보주체의 동의 없이 이용되거나 제공될 수 있다. 또한 중대 범죄의 수사를 위해서 또는 국가안보나 공공의 안전에 대한 상당한 위험을 피하기 위하여 필요한 때에는 그 이용 또는 제공은 합법적이다(제28조 제8항).

넷째, 정치적, 학문적, 종교적 목적이나 노동조합의 목적을 가진 비영리단체는 그 단체의 활동을 위하여 필요한 때에는 정보주체의 동의 없이 특수개인정보를 수집·처리·이용할 수 있다. 다만, 그 단체 구성원들의 개인정보 또는 단체의 목적과 관련하여 정규적인 관계를 맺고 있는 사람들의 특수개인정보에 한정된다. 그러나 특수개인정보를 단체의 외부 사람이나 기관에게 제공하는 것은 오직 정보주체의 동의 요건 하에서만 합법적인 것이 된다(제28조 제9항).

그런데 우리의 입법예고안은 민감정보의 처리(수집·이용·제공)를 금지시키면서, 단 두 가지 예외를 설정하고 있다. 즉 ① 정보주체의 사전 동의가 있는 경우와 ② 다른 법률에서 명시적으로 민감정보의 처리를 요구하거나 허용하는 경우가 그것이다. 이렇게 되면 다른 법률에서 명시적으로 허용하지 않는 한 동의 없는 민감정보의 처리는 모두 불법이 된다.

예컨대, 정당이 정당활동의 목적으로 동의 없이 당원들의 정치적 견해를 수집하는 것은 그 자체 불법이 될 것이다. 또는 학문적 연구를 수행하기 위하여 또는 제3자의 중대한 이익을 보호하기 위하여 정보주체의 동의 없이 건강정보를 수집하거나 제공하는 것도 불법이 된다. 또 학생의 건강정보를 학생생활기록부에 기록할 때마다 교사는 학생의 동의를 받아야 할 것이다. 또는 정부가 예방의학적 목적에서 개인의 건강정보를 관련 공공기관들 상호간에 주고받는 경우에 그에 대한 ‘명시적인’ 법률규정이 없다면 일일이 그 정보주체의 동의를 받아야 할 것이다. 입법예고안은 정보주체의 동의를 받기 위한 절차적 요건으로 수집·이용목적, 이용기간, 제공받는 자, 제공하는 개인정보 항목 등 여러 사항을 사전에 고지하는 의무를 지우고 있다.

이러한 사전고지에 의한 동의와 법률의 명시적인 허용규정이 없는 한 일체의 민감정보의 수집·이용·제공을 불법화하는 것은 보호와 이용의 균형을 현저히 상실한 것으로 평가된다.

만일 개인의 민감정보가 “일반인에게 공표되거나” 또는 “민감정보의 공유를 통해 정보주체에게 수인할 수 없는 차별적 혹은 불리한 결정이 내려진다면” 그에 따르는 정보주체의 사생활 또는 인격적 이익의 침해나 불합리한 차별로 인한 정보주체의 불이익이 크다고 할 수 있다.⁶²⁹⁾ 그러나 개인의 민감정보라도 정당한 업무수행을 목적으로 하

629) 헌법재판소는 ‘공직자 병역면제사유 질병명 공개 사건’(헌재 2007. 5. 31. 2005헌마1139)에서 4급 이상 공무원들의 병역면제사유인 질병명을 관보와 인터넷을 통해

는 수집·이용·제공이 있을 수 있고, 또 그것이 널리 공포되는 것이 아니라 비밀의무를 지는 한정된 소수의 사람들에 한정해서 이용된다. 는 안전장치가 있다면, 그리고 그러한 정보처리의 이익보다 정보처리를 금지시켜야 할 정보주체의 이익이 더 크지 않는 한, 민감정보 처리의 위험성은 그렇게 높지 않다고 보아야 할 것이다.

이처럼 민감정보 처리의 위험성이 그렇게 높지 않은 상황을 전제로 할 때 그럼에도 불구하고 사전고지에 의한 동의획득을 민감정보 처리의 허용요건으로 한다면, 보호하고자 하는 정보주체의 이익은 적은 반면 동의획득에 수반되는 상당한 사회적 비용을 요구하는 것이 된다. 다시 말해서, 지출되어야 할 사회적 비용은 상당히 높은 반면 그로 인한 긍정적 효과는 미약하다.

요컨대, 사전고지에 의한 정보주체의 동의획득이나 또는 일일이 처리를 허용하는 법률의 제정에 수반되는 상당한 사회적 비용을 감안할 때, 그 대신에 위험성을 줄일 수 있는 안전장치를 마련해 놓고 그 한도 내에서 정당한 수집·이용·제공을 허용하는 것이 입법정책상 비용-효과 면에서 바람직한 방안이라고 평가된다.

공개하도록 요구하는 법률조항은 위헌이라고 판단하였다. 이 사건에서 9인의 헌법재판관 모두 위헌의견이었지만 다만 헌법불합치 주문을 놓고 의견이 갈렸다.

제 4 장 수집 · 이용 · 제공의 절차적 요건에 대한 입법평가와 대안제시

제 1 절 4가지 절차적 요건의 개요

정보주체의 동의에 의하여 수집 · 이용이 이루어지든, 아니면 정보주체의 동의 없는 합법적인 수집 · 이용이든 간에, 모든 개인정보의 수집 · 이용 · 제공에 대해서는 4가지의 절차적 요건이 추가적으로 요구된다. ① 목적명시 요건, ② 품질관리 요건, ③ 고지 요건, ④ 보고 요건이 그것이다. 이 4가지 요건은 개인정보처리의 오 · 남용을 방지하기 위해 절차적으로 요구되는 것으로서, OECD 개인정보보호 가이드라인, 유럽연합 개인정보보호지침, 영국, 독일, 일본 등 세계 각국의 개인정보보호법에서 공통적으로 요구하고 있다. 물론 이들 요건의 입법화는 각국마다 약간의 차이가 있다.

1. 목적명시 요건

목적명시 요건(Purpose Specification Requirement)이란 개인정보처리자는 수집 · 이용 · 제공의 목적을 (i) 늦어도 수집 당시에 명시하여야 (=분명하게 드러내 보여야) 하고(목적의 명시성), (ii) 그 후의 이용 · 제공은 그 명시된 목적에 부합하는 것이어야 한다(목적에의 부합성)는 법적 요청이다. 이 요건은 OECD 가이드라인에서는 “목적명시의 원칙”(Purpose Specification Principle)으로 다음과 같이 표현되어 있다.⁶³⁰⁾

630) 독일에서는 “목적구속의 원칙”이라고 불리어지고 있다. 김일환, “개인정보보호법의 개정필요성과 내용에 관한 연구”, □□공법연구□□ 제26집 제2호(한국공법학회, 1998), 235면; 김연태, “행정상 개인정보보호”, □□저스티스□□ 제34권 제5호(한국법학원, 2001. 10), 210면 참조.

『9. 목적명시의 원칙 : 개인정보를 수집하는 목적은 늦어도 정보를 수집하는 시점에는 명시되어야 하고, 그 후의 이용⁶³¹⁾은 그 명시한 목적이나 혹은 그 명시한 목적과 양립할 수 있는 다른 목적을 달성하는데 한정되어야 하며, 목적의 변경이 있을 때에는 그때마다 그것을 명시하여야 한다.』⁶³²⁾

이 목적명시의 원칙에 의하면 수집 당시의 목적을 수집 이후에 변경하는 것은 제한적으로만 허용된다. 즉 수집 당시의 목적과 “양립할 수 있는”(not incompatible) 다른 목적으로의 변경만이 허용된다. 그리고 그 변경된 목적은 명시하여야 한다. 이러한 내용의 목적명시 요건은 유럽연합의 개인정보보호지침과 영국·독일 등 회원국의 개인정보보호법, 그리고 일본의 개인정보보호법에서도 기본적으로 요구된다.

다만, 수집 이후의 목적변경을 제한하는 정도에 있어서 일본과 독일이 다소 다르게 규율하고 있다. 일본의 개인정보보호법은 “변경 전의 이용목적과 상당한 연관성이 있다고 합리적으로 인정되는 범위” 내의 변경만을 허용하고 있다(제15조 제2항). 한편, 독일의 연방개인정보보호법은 민간부문의 개인정보처리자가 수집의 정당성 요건(제28조 제1항 제1문 제2호 및 제3호)⁶³³⁾과 같은 요건을 갖춘 때에는 수집된 개인

631) 여기서의 “이용”은 개인정보처리자의 자체 이용과 제3자 제공을 포함하는 개념이다. 가이드라인의 “이용제한의 원칙”(Use Limitation Principle)에서 “이용”(use)이라는 용어는 제3자 제공을 포함하는 개념으로 사용하고 있다.

632) PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

633) “개인정보처리자의 정당한 이익을 보호하기 위하여 필요하고, 또한 그 처리나 이용을 하지 못하게 할 압도적인 정당한 이익이 정보주체에게 있다고 볼 만한 근거가 전혀 없는 때”(제2호); “그 개인정보가 일반적으로 접근이 가능한 것인 때, 또는 개인정보처리자가 합법적으로 개인정보를 공표할 수 있는 때. 다만, 그 정보처리를 배제해야 할 정보주체의 정당한 이익이 당해 개인정보처리자의 정당한 이익보다 명백히 우월한 때에는 그러하지 아니하다.”(제3호).

정보를 다른 목적으로(=목적은 변경하여) 이용하거나 제공할 수 있다고 규정하고 있다(제28조 제2항). 이처럼 일본과 독일은 수집 이후의 목적변경을 허용하는 기준이 약간 다르다. 아무튼 이러한 목적변경 허용범위 내에서의 이용 · 제공은 “목적 내 이용 · 제공”에 해당하게 된다. 그러나 그 이상의 이용 · 제공은 “목적 외 이용 · 제공”에 해당하고 이는 원칙적으로 금지된다. 다만, 여기에도 예외가 있다.

예컨대, OECD 가이드라인은 “이용제한의 원칙”(Use Limitation Principle)이라는 제목 하에, 수집 당시에 명시한 목적 범위 내에서 이용 또는 제공하는 것을 원칙으로 하되, 예외적으로 ① 정보주체의 동의가 있거나 ② 법적 근거가 있는 때에는 명시한 목적 범위를 넘어서서 이용 또는 제공할 수 있다고 선언하고 있다. 여기서 정보주체의 동의가 사전 동의인지 사후 동의인지 여부는 언급하지 않고 있으나, 사후 동의로도 가능한 것으로 이해될 수 있다.

「10. 이용제한의 원칙 : 개인정보는 위 제9항[목적명시의 원칙]에 따라 명시한 목적 이외의 다른 목적을 위해서 제공되거나 이용되어서는 아니 된다. 다만, a) 정보주체의 동의가 있거나; 또는 b) 법적 근거가 있는 때에는 그러하지 아니하다.」⁶³⁴⁾

2. 품질관리 요건

품질관리 요건(Data Quality Requirement)이란 개인정보처리자는 이용 목적에 관련이 있는 개인정보만을 목적달성에 필요한 만큼만 보유하여야 하고, 정보의 정확성 · 완전성 · 최신성을 유지하여야 한다는 법

634) Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:
a) with the consent of the data subject; or
b) by the authority of law.

적 요청이다. 목적달성에 관련이 없는 개인정보까지 보유할 필요는 없으며, 또 틀린 정보나 불완전한 정보 혹은 낡은 정보를 가지고 정보주체에 대한 평가나 결정을 내린다면 정보주체는 예상하지 못한 불이익을 받게 될 것이기 때문이다. OECD 가이드라인은 “정보품질의 원칙”(Data Quality Principle)이라는 제하에 다음과 같이 표현하고 있다.

「개인정보는 그것을 이용하려는 목적에 관련이 있는 것이라야 하고, 그 목적달성에 필요한 정도만큼만 보유하여야 하며, 그리고 정확하고 완전하며 최신의 것으로 갱신되어야 한다.」⁶³⁵⁾

3. 고지 요건

고지 요건(Notification Requirement)이란 개인정보처리자는 정보처리의 과정을 정보주체가 인식할 수 있도록 수집·이용의 목적 등 정보처리와 관련한 사항을 정보주체에게 알려주어야 한다는 법적 요청이다. 그리하여 정보주체는 자신의 개인정보가 누구에 의해 어떻게 처리되고 있는지를 알고 그 과정에 열람·정정 등 참여할 수 있게 된다. 그럼으로써 혹시라도 있을 수 있는 오·남용을 방지하여 또 다른 피해를 사전에 막을 수 있다. 이 고지의 요건은 OECD 가이드라인에서 “수집제한의 원칙”(Collection Limitation Principle)과 “공개의 원칙”(Openness Principle) 안에 담겨 있다. 수집제한의 원칙 중 “개인정보는 ... 그렇게 하는 것이 적절하다면 정보주체의 인식 하에 획득되어야 한다.”고 표현하고 있으며, 공개의 원칙은 다음과 같다.

635) PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

『개인정보와 관련한 방침, 업무관행, 사태전개에 관해서 그것을 공개하는 일반정책이 마련되어 있어야 한다. 개인정보처리자의 신원과 주사무소는 물론이고 개인정보의 존재 여부와 그 성격, 그리고 주된 이용목적은 확인할 수 있는 방법이 쉽게 이용될 수 있어야 한다.』⁶³⁶⁾

이 고지 요건은 위의 OECD 가이드라인에서보다 이후 제정된 유럽 연합 개인정보보호지침과 그 회원국들의 개인정보보호법에서 더욱 구체적으로 입법화되고 있다.

4. 보고 요건

마지막으로, 보고 요건(Reporting Requirement)이란 개인정보처리자는 개인정보처리시스템의 구축 목적, 정보처리방식, 처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등을 개인정보감독기구에 신고하거나 등록하여야 한다는 요청이다. 비밀리에 운용되는 개인정보처리시스템은 오·남용의 위험성이 매우 크기 때문이다. 이 보고의 요건은 공공기관이 개인정보처리시스템을 구축하는 경우에 주로 적용되는데, 유럽의 경우에는 민간기관의 경우에도 부분적으로 적용되고 있다.

위의 4가지 절차적 요건은 위 제2절에서 살핀 정당한 개인정보처리의 실체적 요건과는 별도로 요구된다. 이하에서는 이들 절차적 요건을 비교법적으로 분석해 보고, 이어서 우리의 입법예고안은 이들 절차적 요건을 어떻게 입법화하고 있는지 그리고 그 입법내용이 적정한지 여부를 평가해보고자 한다.

636) Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

제 2 절 절차적 요건에 대한 비교법적 분석

1. 유럽연합 개인정보보호지침상의 절차적 요건

유럽연합의 개인정보보호지침(95/46/EC)은 목적명시 요건(Purpose Specification Requirement)과 품질관리 요건(Data Quality Requirement)을 제 6조에서 다음과 같이 규정하고 있다.

- (a) 개인기록은 공정하고 합법적으로(fairly and lawfully) 처리되어야 하며;
- (b) 개인기록(personal data)은 구체적이고 명시적이며 정당한 목적(specific, explicit and legitimate purposes)을 위하여 수집되어야 하고, 그 목적에 부합하지 않는 방식으로는(in a way incompatible with those purposes) 더 이상 처리되어서는 아니 된다. 적절한 안전장치(appropriate safeguards)가 있다면, 역사적, 통계적 또는 학술적 목적(historical, statistical or scientific purposes)을 위한 추가적인 정보처리는 ‘본래의 수집목적에 부합하지 않는 것’으로 간주되지 않는다.
- (c) 본래의 수집목적이나 추가적인 정보처리의 목적과 관련하여 개인정보는 그 목적에 적합하고, 관련성이 있어야 하며 과도해서는 아니 된다(adequate, relevant and not excessive).
- (d) 개인기록은 정확해야 하고(accurate), 필요한 때에는 최신의 것으로 갱신되어야 한다. 본래의 수집목적이나 추가적인 정보처리의 목적과 관련하여 부정확하거나 불완전한(inaccurate or incomplete) 개인정보는 삭제되거나 수정되어야 하는데, 이를 위해 필요한 모든 합리적인 조치가 취해져야 한다.
- (e) 개인기록은 본래의 수집목적이나 추가적인 정보처리의 목적에 필요한 기간 동안만(for no longer than is necessary) 정보주체의 신원확인이 가능한 형태로 유지되어야 한다.

또한 고지 요건(Notification Requirement)과 관련해서, 유럽연합의 개인정보보호지침은 개인정보를 정보주체로부터 “직접” 수집하는 경우(제10조)와 “다른 출처로부터” 수집하는 경우(제11조)를 나누어 정보주체에게 일정한 사항들을 고지하도록 의무지우고 있다. 고지의 시점은 직접 수집의 경우에는 “수집 당시”이며, 다른 출처로부터 수집하는 경우에는 개인정보처리시스템에 기록하는 시점 또는 제3자에게 제공하기 이전으로 규정하고 있다. 그리고 고지사항의 내용은 위 두 경우에 약간의 차이를 두고 있다.

이처럼 고지를 개인정보처리기관의 “의무”로 규정하고 정보주체의 “권리”로 규정하지 않는 것은, 의무위반 시 행정적 또는 형사적 제재가 가해질 수 있지만 이 고지의무의 이행을 법원에 청구할 수 있는 권리는 인정하지 않는 것으로 이해된다.

제10조 (정보주체로부터 직접 수집하는 경우의 고지사항) 정보주체로부터 직접 그의 개인정보를 수집하는 경우에, 당해 개인정보처리자는 적어도 다음의 사항을 제공해주어야 한다. 다만, 이미 정보주체가 알고 있는 경우에는 그러하지 아니하다.

- (a) 개인정보처리자와 그 대표자의 신원(identity)
- (b) 정보처리의 목적
- (c) 개인정보가 수집되는 구체적인 상황과 관련해서, 공정한 정보처리를 보장하기 위하여 추가정보가 필요한 경우에는, 다음의 추가 정보
 - i) 개인정보를 제공받는 자(recipients) 또는 제공받는 자의 범위(categories of recipients)
 - ii) 질문에의 답변이 의무적인지 아니면 임의적인 것인지 여부 및 답변하지 않았을 때 어떤 결과가 초래될 수 있는지
 - iii) 열람권과 정정권이 있는지 여부

제11조 (정보주체로부터 직접 얻은 것이 아닌 경우의 고지사항)

1. 개인정보가 정보주체로부터 직접 얻은 것이 아닌 경우에, 다음의 사항을 사후에 알려주어야 한다. 그리고 알려주는 시점은 (i) 개인정보를 기록하는 때(at the time of undertaking the recording of personal data) 또는 (ii) 제3자에게 제공이 예정되어 있는 경우에는, 적어도 처음의 제공이 이루어지기 이전(no later than the time when the data are first disclosed)이다.

(a) 개인정보처리자와 그 대표자의 신원(identity)

(b) 정보처리의 목적

(c) 개인정보가 처리되는 구체적인 상황과 관련해서, 공정한 정보처리를 보장하기 위하여 추가정보가 필요한 경우에는, 다음의 추가정보

i) 처리되고 있는 개인정보의 범위 (the categories of data concerned)

ii) 개인정보를 제공받는 자(recipients) 또는 제공받는 자의 범위(categories of recipients)

iii) 열람권과 정정권이 있는지 여부

2. 제1항은 다음의 경우에는 적용되지 아니한다.

(a) 통계목적이나 역사적 또는 과학적 연구 목적을 위하여 정보처리가 수행되는 경우에, 고지가 불가능하다고 판명되거나, 고지하는 것이 너무 지나친 노력(a disproportionate effort)을 요하는 때, 또는

(b) 기록(recording)이나 공개(disclosure)가 법에 의하여 명시적으로 규정되어 있는 때.

이들 적용제외의 경우에 회원국은 국내법으로 적절한 안전장치를 마련하여야 한다.

한편, 보고 요건(Reporting Requirement)과 관련하여, 유럽연합의 개인정보보호지침 제18조는 자동처리되는 개인정보처리시스템을 개인정보감독기구에게 통보하도록 요구하고 있다. 물론 회원국은 국내법으로 이 통보의무를 완화하거나 면제시킬 수 있다.

제18조 (개인정보감독기구에게 통보 의무)

1. 개인정보처리기관은 단일의 목적 또는 몇 가지 연관된 목적들에 봉사하기 위한 의도에서 행하여지는 자동정보처리(automatic processing operation or set of such operations)에 대하여 그것을 수행하기 전에 개인정보감독기구에게 알려야 한다.
2. 회원국은 다음의 경우에 다음의 조건 하에서만 제1항의 통보의무를 완화 내지 면제할 수 있다. (이하 생략)

3. 영국 개인정보보호법상의 절차적 요건

영국의 개인정보보호법은 제1부칙(Schedule 1) 제1절(Part 1)의 제2조 내지 제5조에서 목적명시 요건과 품질관리 요건을 유럽연합의 지침과 유사한 내용으로 다음과 같이 규정하고 있다.

2. 개인기록(personal data)은 오로지 하나 또는 그 이상의 구체적이고 합법적인 목적(one or more specified and lawful purposes)을 위해서만 작성되어야 하고, 그 목적에 부합하지 않는 방식으로는(in any manner incompatible with that purpose or those purposes) 더 이상 처리되어서는 아니 된다.
3. 개인기록은 그 처리의 목적에 적합하고, 관련성이 있어야 하며 과도해서는 아니 된다(adequate, relevant and not excessive).
4. 개인기록은 정확해야 하고(accurate), 필요한 때에는 최신의 것으로 갱신되어야 한다.

5. 개인기록은 그 처리의 목적에 필요한 기간 이상으로(for longer than is necessary) 존속해서는 안 된다.

보고 요건과 관련하여, 영국의 개인정보보호법은 위 유럽연합의 개인정보보호지침의 요구에 따라, 일정한 개인정보처리에 관한 사항을 정보보호청장(Information Commissioner)에게 신고하여 등록하도록 하고 이러한 등록 없이는 개인정보를 처리할 수 없도록 하고 있다(제16조 및 제17조). 주요한 신고사항은 개인정보처리자의 명칭과 주소, 개인정보처리의 목적, 보유하고 있는 개인정보의 항목, 개인정보를 제공받는 자, 개인정보를 유럽경제지역(European Economic Area)의 역외로 이전하는 경우에 그 제공받는 국가나 지역 등이다. 물론 이 등록의무가 면제되는 경우를 함께 규정하고 있다. 정보보호청장은 신고한 사항을 토대로 공공등록부(public register)를 작성한다. 이 공공등록부는 인터넷을 통하여 국민에게 공개된다.

4. 독일 개인정보보호법상의 절차적 요건

독일 연방개인정보보호법은 공공과 민간의 개인정보처리자가 개인정보를 수집하는 경우에 원칙적으로 정보주체로부터 직접 수집할 것을 요구하고 있다. 다만, 몇 가지 경우에는 예외를 인정하고 있다(제4조 제2항).

그리고 개인정보처리자는 정보주체로부터 개인정보를 수집하는 경우에 ① 자신의 신원, ② 수집목적, 그리고 ③ 제3자에게 제공하는 경우에는 그 제공받는 자의 범위(단, 정보주체가 그 제공에 관해 알 수 있는 상황에서는 제외)에 대해 고지를 하도록 요구하고 있다(제4조 제3항 제1문). 또한, 개인정보처리자(주로 공공기관)가 법률에 의해서 개인정보를 수집하거나 정보주체에게 일정한 혜택을 주는 조건으로 개인

정보를 수집하는 경우에는 정보주체에게 그 점을 알려주어야 하고, 그렇지 않은 경우에는 개인정보의 제출이 임의적인 것임을 알려주어야 한다. 또한 정보주체의 요구가 있으면, 개인정보의 제출을 거부했을 때 발생하는 결과에 대해서 설명해주어야 한다(제4조 제3항 제2문).

제 4 조(수집·처리 및 이용의 합법성) (1) 생략

(2) 개인정보는 정보주체로부터 수집되어야 한다. 다만, 다음 각 호의 경우에는 정보주체의 관여 없이 수집될 수 있다.

1. 법률의 규정이 그렇게 규정하거나 또는 요구하는 경우; 또는
2. a) 수행되는 행정상의 업무가 그 성격상 다른 사람이나 기관으로부터 수집하는 것을 필요로 하는 경우; 또는
b) 정보주체로부터의 수집이 비상한 노력을 수반하고 그리고 정보주체의 우월적인 정당한 이익이 침해된다고 믿을만한 근거가 전혀 없는 경우

(3) 개인정보가 정보주체로부터 수집되는 경우 정보주체는 당해 개인정보처리자로부터 다음 각 호의 사항을 고지받아야 한다. 다만, 정보주체가 다른 방법에 의해 그러한 정보를 이미 받은 때에는 그러하지 아니하다.

1. 개인정보처리자의 신원;
2. 수집, 처리 또는 이용의 목적; 그리고
3. 제공받는 자의 범주. 다만, 정보주체가 그러한 제공에 대해 알고 있다고 볼 수 없는 특별한 경우에 한한다.

개인정보의 제출을 요구하는 법률의 규정에 근거해서 정보주체로부터 개인정보가 수집되는 경우, 또는 법률에 따라 일정한 혜택을 얻기 위한 전제조건으로 개인정보가 제출되는 경우에, 정보주체는 그 점에 대해 고지를 받아야 하고, 만일 그렇지 아니한 경우에는 정보주체는

당해 개인정보의 제출이 임의적인 것임을 고지받아야 한다. 구체적인 상황에서 필요하다면 또는 정보주체의 요청이 있는 경우에, 정보주체는 관련 법률의 규정 및 개인정보의 제출을 거부하게 되면 어떤 결과가 발생하는지에 관하여 고지받아야 한다.

한편 보고 요건과 관련하여, 독일의 연방개인정보보호법은 개인정보처리시스템 현황정보를 공공부문의 경우에는 개인정보감독기구인 연방개인정보보호청장에게, 민간부문의 경우에는 각주의 정보감독청장에게 사전신고하도록 요구하고 있다.

우선, 공공부문의 경우 컴퓨터에 의한 개인정보처리시스템을 운영하고자 하는 공공기관은 법 제4e조가 정하는 사항, 즉 당해 시스템의 현황정보를 사전에 연방개인정보보호청에 신고하여야 한다(법 제4d조 제1항). 그러나 이러한 등록의무는 당해 공공기관이 자체적으로 개인정보보호책임자(Beauftragter für den Datenschutz)를 임명하는 경우에는 면제된다(법 제4d조 제2항).

그리고 위 등록의무에 대해서는 예외가 인정된다(법 제4d조 제3항). 즉, 당해 공공기관의 자체적 목적을 위하여 최대 4명의 개인정보취급자가 정보를 수집·처리·이용하는 경우, 당사자의 동의가 있는 경우, 그리고 정보의 수집·처리·이용이 계약의 목적 혹은 당사자와의 유사계약에 근거한 신뢰관계에 기여하는 경우에 등록의무는 면제된다.

그러나 등록의무가 있는 개인정보처리의 경우에는 다음의 사항을 신고하여야 한다(제4e조) : (i) 개인정보처리기관의 명칭, (ii) 소유자, 회장단, 총무, 그 외의 법적 또는 사규에 따른 회사관리인, 개인정보보호책임자, (iii) 개인정보처리기관의 주소, (iv) 정보수집·처리·이용 규정, (v) 당사자 집단 및 관련정보의記述, (vi) 개인정보제공의 수신자 또는 수신자 범위, (vii) 정보해제에 관한 기간규정, (viii) 제3국에 대한 정보전송의 계획, (ix) 기술적·조직적 조치(법 제9조)가 정보처리의 안전보장을 위하여 적절한지 평가할 수 있는 일반적記述에

관한 사항.

한편, 컴퓨터에 의한 개인정보처리시스템을 운영하고자 하는 민간의 개인정보처리기관도 위 공공기관과 마찬가지로 당해 시스템의 현황정보를 사전에 신고하여야 한다. 다만, 그 신고기관은 연방개인정보보호청이 아니라, 각 주정부가 지정한 정보감독청(Aufsichtsbehörde)이다. 그 밖에 자체적인 개인정보보호책임자를 두는 경우 등록의무가 면제되는 점, 등록의무에 대한 예외 등은 위 공공부문에서와 똑 같은 규율을 받는다.

5. 일본 개인정보보호법상의 절차적 요건

(1) 목적명시 요건

일본의 민간부문 일반법인 개인정보보호법은 민간의 개인정보처리기관(“개인정보취급사업자”)이 자신의 사업상의 목적을 위하여 정보주체의 동의 없이 개인정보를 수집 및 이용할 수 있도록 허용하지만,⁶³⁷⁾ 그러나 그 이용목적은 “가능한 한 특정”하도록 요구하고 있다(제15조 제1항). 그리고 그 이용목적의 변경을 원칙적으로 허용하지 않고, 다만, 처음에 특정했던 이용목적과 “상당한 연관성이 있다고 합리적으로 인정되는 범위” 내의 다른 목적은 목적의 변경으로 보지 아니한다(제15조 제2항). 개인정보취급사업자는 이러한 목적달성에 필요한 범위 내에서 자유롭게 개인정보를 자체적으로 ‘이용’할 수 있다(제16조 제1항). 그러나 이 범위를 넘어선 이른바 ‘목적 외 이용’은 원칙적으로

637) 위에서 살핀 바와 같이, 유럽과 달리 일본은 자체적인 이용목적에 대해서는 아무런 실체적 제한을 두고 있지 않다. 유럽은 개인정보처리자 본인 또는 제공받는 제3자의 정당한 이익을 보호하기 위한 목적에서, 그리고 그 정보처리의 이익이 정보주체의 자유와 권리를 보호해야 할 이익보다 더 큰 경우에 한하여 수집·이용·제공이 허용되는데 반해, 일본은 자체 이용목적인 경우에는 달리 이러한 제한을 두고 있지 않다.

금지되고, 정보주체의 동의 등 다섯 가지 경우에는 목적 외 이용을 허용하고 있다(제16조 제3항).

- 제15조 (이용목적의 특정) ① 개인정보취급사업자는 개인정보를 취급함에 있어서 그 이용의 목적(이하 “이용목적”이라 한다)을 가능한 한 특정하여야 한다.
- ② 개인정보취급사업자는 이용 목적을 변경하는 경우에는 변경전의 이용목적과 상당한 연관성이 있다고 합리적으로 인정되는 범위를 초과해서 변경하여서는 아니 된다.

(2) 품질관리 요건

일본의 민간부문 일반법인 개인정보보호법은 제19조에서 개인정보취급사업자에게 처리하는 정보의 정확성을 유지하는 노력의무를 부과하고 있다. 그러나 유럽연합이나 영국과 같이 존속기간을 제한하고 있지는 않다.

- 제19조 (데이터 내용의 정확성의 확보) 개인정보취급사업자는 이용 목적의 달성에 필요한 범위 내에서 개인데이터를 정확하고 최신의 내용으로 유지하도록 노력하여야 한다.

(3) 고지 요건

일본의 민간부문 일반법인 개인정보보호법은 자체적인 수집·이용의 경우에는 고지의 요건을 엄격하게 정하고 있지 않다. 그리고 고지의 대상항목을 “이용목적”과 “보유개인데이터에 관한 항목”으로 나누어 고지의무의 내용을 약간 달리 규정하고 있다.

① **이용목적의 고지** : 개인정보취급사업자는 개인정보를 정보주체로부터 직접 수집하든 직접 수집하지 아니하든 정보주체에게 적어도 그 이용목적은 수집의 사전 또는 사후에 알려주어야 한다. 그 고지의 방법은 통지 또는 공표에 의하도록 하고 있다. 그러나 4가지의 경우에는 고지를 하지 않아도 되도록 하고 있다.

우선, 정보주체로부터 직접 수집하는 경우, 즉 ‘정보주체와의 계약체결에 따라 계약서 등의 서면(전자서면을 포함)에 기재된 개인정보를 수집하거나 또는 계약체결과 관계없이 정보주체로부터 직접 서면에 의하여 개인정보를 수집하는 경우’에는, ‘사전에’ 당해 정보주체에게 그 이용목적은 명시하여야 한다(제18조 제2항 본문). 그렇지만 이러한 사전고지의무도 사람의 생명·신체·재산의 보호를 위하여 긴급한 필요가 있는 경우에는 면제된다(제18조 제2항 단서).

다음으로, 정보주체로부터 직접 수집하는 것이 아닌 경우에는, 개인정보취급사업자는 개인정보를 수집하고 나서 ‘사후적으로 신속하게’ 그 이용목적은 정보주체에게 통지하거나 공표하여야 하는 의무를 진다. 그러나 사전에 이용목적은 공표하고 있는 경우에는 사후 통지나 공표를 할 의무를 지지 아니한다. 즉, 이용목적은 반드시 사전에 고지하도록 요구하지는 않고, 사후고지를 의무로 하되, 임의로 사전고지를 한 경우에는 사후고지의 의무가 면제된다(제18조 제1항). 사후고지의 방법으로는 당해 정보주체에게 “통지”를 하거나 아니면 “공표”를 할 수 있도록 하고 있다.

한편, 처음의 수집목적에 부합하는 범위 내에서 이용목적은 임의로 변경하는 경우에는 그 변경된 이용목적은 정보주체에게 통지하거나 공표하여야 한다(제18조 제3항).

그러나 위의 사전고지의무 내지 사후고지의무도 4가지 예외적인 상황에서는 면제된다(아래 제18조 제4항 참조).

제18조 (취득시 이용목적의 통지 등) ① 개인정보취급사업자는 개인 정보를 취득한 경우에는, 미리 그 이용 목적을 공표하고 있는 경우를 제외하고, 신속히 그 이용 목적을 본인에게 통지하거나 공표하여야 한다.

② 개인정보취급사업자는 전항의 규정에 불구하고 본인과의 사이에 계약을 체결함에 따라 계약서 기타의 서면(電子的 방식, 磁氣的 방식 기타 사람의 지각에 의해서는 인식할 수 없는 방식으로 작성된 기록을 포함한다. 이하 이 항에서 같다.)에 기재된 당해 본인의 개인정보를 취득하는 경우 기타 본인으로부터 직접 서면에 기재된 당해 본인의 개인정보를 취득하는 경우에는, 미리 본인에 대해 그 이용 목적을 명시하여야 한다. 다만, 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급히 필요가 있는 경우에는 그러하지 아니하다.

③ 개인정보취급사업자는 이용 목적을 변경한 경우에는 변경된 이용 목적에 대해 본인에게 통지하거나 공표하여야 한다.

④ 전 세 항의 규정은 다음 각 호의 1에 해당하는 경우에는 적용하지 아니한다.

1. 이용 목적을 본인에게 통지하거나 공표함으로써 본인 또는 제3자의 생명, 신체, 재산 기타의 권리의익을 해할 우려가 있는 경우
2. 이용 목적을 본인에게 통지하거나 공표함으로써 당해 개인정보취급사업자의 권리 또는 정당한 이익을 해할 우려가 있는 경우
3. 국가기관 또는 지방자치단체가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 이용 목적을 본인에게 통지하거나 공표함으로써 당해 사무의 수행에 지장을 줄 우려가 있는 경우
4. 취득 상황에 비추어 이용 목적이 명확하다고 인정되는 경우

② **관련 사항의 고지** : 일본의 민간부문 개인정보보호법은 이용목적 외에 보유개인데이터⁶³⁸⁾에 관한 사항을 정보주체가 알 수 있도록 해 줄 의무를 개인정보취급사업자에게 지우고 있다(제24조). 그러나 이 의무는 이용목적의 고지의 경우처럼 반드시 통지나 공표의 방법에 의해 이행하여야 하는 것은 아니고, 정보주체의 요청이 있으면 그에 회답하는 방법으로 이행할 수도 있도록 하고 있다.

제24조 (보유개인데이터에 관한 사항의 공표 등) ① 개인정보취급사업자는 보유개인데이터에 관해서 다음 각 호의 1에 해당하는 사항에 대하여 본인이 알 수 있는 상태(본인의 요청에 응해 지체 없이 회답하는 경우를 포함한다.)에 두어야 한다.

1. 당해 개인정보취급사업자의 성명 또는 명칭
2. 모든 보유개인데이터의 이용목적(제18조 제4항 제1호 내지 제3호에 해당하는 경우를 제외한다)
3. 제24조 제2항, 제25조 제1항, 제26조 제1항 또는 제27조 제1항 혹은 제2항의 규정에 의한 요청에 응하는 절차(제30조 제2항의 규정에 의해 수수료의 액을 정한 때에는 그 수수료의 액을 포함한다)
4. 전 3호에 해당하는 것 이외에, 보유개인데이터의 적정한 취급의 확보에 관해 필요한 사항으로서 정령으로 정하는 것

② 개인정보취급사업자는 본인으로부터 당해 본인의 식별이 가능한 보유개인데이터의 이용목적의 통지를 요청받은 때에는 본인에 대하여 지체 없이 그것을 통지하여야 한다. 다만, 다음의 각호 중 어느 하나에 해당하는 경우에는 그러하지 아니하다.

638) 제2조 제5항 : 이 법률에서 “보유개인데이터”라 함은 개인정보취급사업자가 開示, 내용의 정정·추가·삭제, 이용의 정지, 消去 및 제3자제공의 정지를 행할 수 있는 권한을 가지는 개인데이터로서, 그 존부가 밝혀짐에 따라 공익 기타의 이익이 침해될 수 있는 것으로서 정령으로 정하는 것 또는 1년 이내에서 정령으로 정하는 기간내에 삭제하게 되어 있는 것 이외의 것을 말한다.

1. 전항의 규정에 의하여 당해 본인의 식별이 가능한 보유개인데이터의 이용목적이 명확한 경우
2. 제18조 제4항 제1호 내지 제3호에 해당하는 경우
- ③ 개인정보취급사업자는 전항의 규정에 근거하여 요청된 보유개인데이터의 이용목적을 통지하지 않는다는 취지의 결정을 한 때에는 본인에 대하여 지체 없이 그 취지를 통지하여야 한다.

(4) 보고 요건

일본의 민간부문 일반법인 개인정보보호법은 민간기관(“개인정보취급사업자”)이 처리하고 있는 개인정보시스템에 관해서는 유럽과 같이 그것을 개인정보감독기구에 등록하는 제도는 두고 있지는 않다.

제 3 절 입법예고안의 절차적 요건에 대한 입법평가와 대안제시

1. 목적명시 요건에 대한 평가와 수정대안

목적명시 요건(purpose specification requirement)은 개인정보를 처리(=수집·이용·제공)하기 전에 그 목적을 명시하고(=분명하게 밝히고) 그 명시한 목적 범위 내에서 개인정보를 처리하라는 법적 요청이다. 다시 말해서, 미리 분명하게 밝히지 않은 목적으로 개인정보를 처리해서는 안 된다는 것이다.

그리고 여기서 특별히 유의하여야 할 점은, 유럽이든 일본이든 수집목적의 설정과 그 범위 내의 이용에는 정보주체의 동의를 요건으로 하지 않고 있다는 점이다. 위 수집·처리의 동의 요건에서 분석한 바와 같이,⁶³⁹⁾ 유럽은 정보주체의 동의 없이 적법하게 처리(=수집·이

639) 제4편 제3장 제1절 참조.

용·제공)할 수 있는 5가지 경우를 규정하고 있는 바, 예컨대 민간기관의 경우에 개인정보처리자나 개인정보를 제공받는 제3자가 추구하는 “정당한 이익”(legitimate interests)을 달성하기 위하여 개인정보를 정보주체의 동의 없이 처리(=수집·이용·제공)하는 것은 법적으로 허용된다. 다만, 정보주체의 기본적인 자유와 권리를 보호해야 하는 이익이 더 클 때에 한하여 그 정보처리(=수집·이용·제공)는 허용되지 않는다. 한편, 일본은 이 같은 이익형량 요소를 입법화하지 않은 채 목적명시 요건만을 규정하고 있다.

개인정보를 수집하는 목적을 엄밀하게 구분한다면 자체 이용 목적과 제3자 제공 목적으로 나누어질 수 있다. 민간기업의 경우 자체 이용 목적에는 예컨대 고객관리 목적이나 혹은 자사제품의 광고 목적이 포함될 것이다. 일반적으로는 이러한 자체 이용이 주된 목적이겠지만, 부수적으로 제3자 제공이 이루어지는 경우가 있다. 예컨대, 판매계약에 따른 상품의 송달을 위해 제3자인 배송업자에게 주소정보를 제공하는 경우이다. 이 같은 제3자 제공은 설령 처음의 수집목적에서 명시하지 않았다고 하더라도 ‘처음에 명시한 수집목적과 양립할 수 있는(not incompatible) 목적’(OECD 가이드라인 또는 유럽연합 개인정보 보호지침) 혹은 ‘처음의 이용목적과 상당한 연관성이 있다고 합리적으로 인정되는 목적’(일본 개인정보보호법)에 해당되어 ‘목적의 변경’으로 간주되지 않는다. 한편 제3자 제공은 이렇게 자체 이용에 따르는 부수적인 경우도 있지만, 처음부터 제3자 제공을 목적으로 수집되는 경우가 있다. 예컨대, 직원 채용에 있어서 가장 적합한 인물을 선정하기 위한 목적에서 그 신청자에 관한 조사업무를 수행하는 업체가 그 신청자에 관한 정보를 수집하여 의뢰자에게 제공하는 경우에 그러하다.

이상의 관점에서 입법예고안의 목적명시 요건을 평가해 보면, 다소 보완을 요하는 부분이 있는 것으로 판단된다. 우선 목적명시 요건을 분명하게 설정하고 있지 않다. 물론 제15조 제1항은 개인정보를 합법

적으로 수집할 수 있는 6가지 경우(정보주체의 동의 포함)를 적시하면서, 그렇게 합법적으로 수집한 경우에 “해당 수집목적 범위 안에서 이용할 수 있다.”고 규정하고 있기 때문에 “수집 목적” 개념을 당연한 전제로 하고 있다. 또한 제15조 제2항에서는 만일 정보주체의 동의를 받아 수집하는 경우에는 “수집·이용 목적”을 정보주체에게 “알려야 하는” 의무를 개인정보처리자에게 지우고 있고, 동조 제3항에서는 정보주체의 요구가 있는 경우에는 “수집·이용 목적을 명확히 제시하여야 한다.”고 규정하고 있다.

그러나 이러한 규율만으로는 목적명시 요건의 입법화와 관련한 몇 가지 규범적 요소들이 분명하게 드러나지 않게 된다.

첫째, 목적을 제시할 때 어느 정도 구체적이어야 하는가 하는 문제가 있다. 이 점과 관련해서 유럽연합의 개인정보보호지침은 “**구체적이고 명시적이며 정당한 목적**”(specific, explicit and legitimate purposes)이라고 규정하고 있다. 즉 제시되는 목적은 구체성·명백성·정당성의 요건을 갖추어야 한다는 것이다. 그러니까 애매하고 포괄적인 목적의 제시는 허용되지 않으며 또 그 목적은 정당해야 한다는 것이다.

둘째, 처음에 명시되었던 수집·이용목적에는 명확하게 포함되지 않았지만 그 처음의 목적 취지에 반하지 않는 선에서의 목적변경을 허용할 것인가 하는 문제가 있다. 위에서 살핀 바와 같이 OECD 가이드라인, 유럽의 개인정보보호법, 그리고 일본의 개인정보보호법은 모두 이 점을 허용하고 있다. 즉, 처음에 명시된 목적과 “양립하는”(not incompatible) 다른 목적(OECD, 유럽) 또는 명시된 “이용목적과 상당한 연관성이 있다고 합리적으로 인정되는” 다른 목적(일본)은 목적의 변경으로 보지 않는다.

요컨대, 위 첫째와 둘째의 규범적 요소의 핵심은 ‘개인정보처리자는 정당한 수집목적을 구체적이고 분명하게 적시하여야 하고, 그 명시된 목적 또는 그와 합리적으로 연관성이 있는 다른 목적을 위해서 이용

할 수 있다’는 것이다.

그런데 입법예고안은 이 점을 분명하게 규정하고 있지 않다. 이렇게 되면, 우리의 그 동안의 관행에 비추어 볼 때 개인정보처리자는 목적을 애매하고 포괄적으로 제시해 놓고 다양한 목적이 거기에 다 포섭될 수 있도록 할 가능성이 충분히 예상된다. 이 점에 관해 분명한 입법기준이 제시되지 않는다면 사후의 적용과정에서 상당한 혼란이 초래될 것으로 판단된다.

[수정대안]

제15조에 제2항을 다음과 같이 삽입한다.

“② 제1항의 경우 개인정보처리자는 정당한 수집·이용목적에 구체적이고 분명하게 명시하여야 하고, 그 명시한 목적 및 그와 합리적으로 연관성이 있는 다른 목적을 위해서 이용할 수 있다. 통계적 또는 학술적 목적을 위한 추가적인 이용은 명시한 목적과 합리적 연관성이 없는 것으로 취급되지 아니한다.”

2. 품질관리 요건에 대한 평가와 수정대안

품질관리 요건과 관련한 규범적 요소는 두 가지이다. 첫째는 개인정보는 목적 달성에 적합하고 필요한 만큼만 수집·이용되어야 한다는 점이고(필요성 요소), 둘째는 수집·이용되는 개인정보는 정확성과 최신성을 유지하여야 한다는 점이다(정확성 요소).

입법예고안은 제16조에서 이른바 품질관리 요건 중 위 첫 번째의 필요성 요소만을 다소 엄격하게 규정하고 있고, 두 번째의 정확성 요소를 규정하고 있지 않다. 그러나 필요성 요소 못지않게 정확성 요소는 개인정보보호법에 있어서 매우 중요한 규범적 요소임에 유의하여야 한다. 잘못된 틀린 정보거나 낡은 정보를 가지고 정보주체를 평가

하고 그에 기초해서 어떤 결정을 내린다면 그것은 정보주체에게 예상하지 못한 피해를 입힐 수 있기 때문이다.

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 따라 개인정보를 수집하는 경우에는 해당 목적에 필요한 최소한의 개인정보를 수집하여야 한다.

② 개인정보처리자는 정보주체가 필요한 최소한의 정보 이외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 합리적인 이유 없이 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

우선, 필요성의 요소와 관련해서 입법예고안 제16조 제1항은 수집·이용목적에 “필요한 최소한의 개인정보를 수집”하도록 의무지우고 있다. 그리고 제2항은 그 범위를 넘어서는 개인정보 수집에 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부하지 못하게 하면서 다만 합리적인 이유가 있는 때에는 제공을 거부할 수 있도록 하고 있다.

위 제1항의 “목적에 필요한 최소한의 정보 수집” 요건은 유럽연합의 개인정보보호지침이 개인정보는 “목적에 적합하고, 관련성이 있어야 하며 과도해서는 아니 된다(adequate, relevant and not excessive)”고 규정하고 있는 것과 비교된다. 또한 OECD 가이드라인은 이 점과 관련해서 “개인정보는 그것을 이용하려는 목적에 관련이 있는 것이라야 하고, 그 목적달성에 필요한 정도만큼만 보유하여야 한다.”고 규정하고 있다. 그리고 일본은 “이용목적의 달성에 필요한 범위 내에서” 개인정보를 보유하여야 한다고 규정하고 있다. 비교법적으로 보면, 우리 입법예고안의 “목적에 필요한 최소한의 정보 수집” 요건은 다소 엄한 요건이라고 하겠다. “과도하게 수집해서는 안 된다”(유럽)는 것과 “필요한 최소한만 수집하라”(입법예고안)는 것의 양자 사이에는 뉘앙스의 차이를 넘어서서 실질적인 차이가 있는 것으로 보인다.

다음으로, 정확성 요소와 관련해서 입법예고안은 이에 대한 규정을 두고 있지 않은데, 다음과 같은 규정을 두어야 할 것으로 판단된다.

[수정대안]

제16조의2를 다음과 같이 신설한다.

“제16조의2(처리정보의 정확성) 개인정보처리자는 수집·이용하는 개인정보를 정확하고 최신의 것으로 유지하도록 노력하여야 한다.

3. 고지 요건에 대한 평가와 수정대안

고지 요건은 누가 무슨 목적으로 나에게 관한 개인정보를 얼마만큼 수집·이용하는지에 관하여 정보주체가 알 수 있도록 하기 위한 것이다. 그에 따라 개인정보처리자는 일정한 사항을 정보주체에게 알려 줄 의무를 지게 된다.

이러한 고지 요건을 입법화할 때 고려되어야 하는 규범적 요소는 (i) 고지의 상황, (ii) 고지의 시점, (iii) 고지의 항목, 그리고 (iv) 고지의 방법의 네 가지이다. “고지 상황 요소”는 어떤 경우에 고지 의무를 지우고 어떤 경우에 면제해 줄 것인가 하는 문제이고, “고지 시점 요소”는 어느 시점에 알려주어야 하는가 하는 문제이다. 그리고 “고지 항목 요소”는 무엇을 알려 주어야 하는가 하는 문제이며, “고지 방법 요소”는 어떻게 알려 주어야 하는가 하는 문제이다. 위에서 살핀 바와 같이 유럽과 일본의 개인정보보호법은 이들 4가지 요소에 대하여 자세하게 규정하고 있다. 그런데 우리의 입법예고안은 불완전하게 규정하고 있다.

우선, 고지 상황 요소와 관련해서, 입법예고안 제15조는 ① 정보주체의 동의를 받아서 개인정보를 수집·이용하는 경우(제2항)와 ② 정보주체의 요구가 있을 때(제3항)의 두 가지 경우에만 고지의무를 부여

하고 있다. 그리고 고지의 대상항목으로서 ① 수집·이용목적 ② 개인정보의 항목 ③ 보유 및 이용기간의 3가지를 적시하고 있다. 그 외에 고지의 방법에 관해서는 구체적으로 정하고 있지 않다.

제15조(개인정보의 수집·이용) ① 생략

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집·이용목적
2. 수집하고자 하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간

③ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 수집·이용하는 근거 및 제2항 각 호의 사항을 명확히 제시하여야 한다.

그런데 이렇게 규정하게 되면, 제15조 제1항 제2호 내지 제6호의 동의 없는 합법적인 수집·이용의 경우에는 모두 고지의무가 면제되게 되고, 다만 정보주체의 요구가 있을 때에 한하여 고지의무가 발생하게 된다. 그러나 이는 고지 요건을 설정하는 본래의 취지에 완전하게 들어맞지 않는다. 즉 정보주체는 원칙적으로 자신의 개인정보의 처리(=수집·이용·제공)에 대하여 최소한의 인식을 가질 수 있어야 하는데, 위 입법예고안에 의하면 이러한 법적 요청은 거의 충족되지 못하게 된다. 그리하여 동의 없이 합법적으로 수집·이용되는 경우(제15조 제1항 제2호 내지 제6호)에 정보주체가 그 수집·이용을 인식할 수 있는 가능성은 유일하게 정보주체가 적극적으로 고지의 요구를 해야 비로소 열리게 된다.

물론 입법예고안의 규정은 개인정보처리자에게는 고지 의무의 부담을 경감시켜주는 효과가 있긴 하지만, 정보주체의 인식가능성은 그

만큼 줄어들게 된다. 입법예고안의 입안자가 이 부분에 대한 입법형량을 정확하게 한 결과인지는 분명하지 않다.

사실 개인정보처리자의 입장에서 보면 자신의 정당한 업무 수행을 위해서 다른 출처로부터 개인정보를 수집할 때마다 당해 정보주체에게 일일이 통지한다는 것은 상당한 비용과 부담이 될 것임이 분명하다. 때문에 개별적인 통지를 의무화하는 것은 지나치게 부담을 지우는 것으로서 타당한 입법기준이라고 할 수 없다. 또 개인정보를 수집한 이후 모든 경우에 고지의무를 부과하는 것도 타당하지 못하다. 타당한 예외를 반드시 두어야 한다.

이 점과 관련해서는 유럽과 일본의 개인정보보호법의 입법기준이 의미 있는 참고자료가 될 수 있을 것으로 판단된다. 위에서 살핀 바와 같이, 일본의 개인정보보호법은 (i) 이용목적의 고지와 (ii) 정보처리에 관한 사항의 고지를 나누고, 전자는 다시 정보주체로부터의 직접 수집의 경우와 직접 수집이 아닌 경우로 구분하고 있다. 그리하여 적어도 이용목적의 고지와 관련해서는 직접 수집이든 아니든 정보주체에게 사후에라도 그 목적을 알려주도록 요구하고 있다. 다만 그 고지의 방법은 통지뿐만 아니라 공표에 의해서도 가능하도록 하고 있다. 그리고 이러한 고지의무가 면제되는 4가지 경우를 입법화해 놓고 있다.

[수정대안]

제15조 제2항과 제3항을 삭제하고, 제15조의2를 다음과 같이 신설한다.

제15조의2(고지의 의무) ① 개인정보처리자는 정보주체로부터 직접 개인정보를 수집하는 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다만, 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급한 때에는 그러하지 아니하다.

1. 개인정보처리자의 성명 또는 명칭
2. 개인정보의 수집 · 이용목적

3. 처리되는 개인정보의 종류와 범위

② 개인정보처리자는 다른 출처로부터 개인정보를 수집하는 경우에는 수집한 후 가능한 한 신속하게 제1항 각 호의 사항을 정보주체에게 통지하거나 공표하여야 한다. 다만, 미리 공표하고 있는 경우에는 그러하지 아니하다.

③ 제1항과 제2항의 고지의무는 다음 각 호의 1에 해당하는 때에는 요구되지 아니한다.

1. 고지함으로써 정보주체 또는 제3자의 생명, 신체, 재산 기타의 권리의익을 해할 가능성이 있는 경우
2. 고지함으로써 당해 개인정보처리자의 권리 또는 정당한 이익을 해할 가능성이 있는 경우
3. 고지함으로써 당해 개인정보처리자의 업무 수행에 지장을 줄 가능성이 있거나 과도한 노력이나 비용을 요하는 경우
4. 수집·이용이 법령에 의하여 명시적으로 규정되어 있는 경우

4. 보고 요건에 대한 평가

입법예고안은 민간기관이 운용하는 개인정보데이터베이스에 대해서는 달리 등록하는 규정을 두고 있지 않지만, 공공기관이 운용하는 개인정보데이터베이스에 대해서는 행정안전부장관에게 등록하도록 규정하고 있다(제30조).

제30조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 법적 근거, 목적 및 기간 등 대통령령이 정하는 사항을 행정안전부장관에게 등록하여야 한다. 등록된 사항이 변경된 경우에도 또한 같다.

② 제1항은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 이를 적용하지 아니한다.

1. 국가의 안전 및 외교상의 비밀 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
 2. 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안 처분과 출입국관리에 관한 사항을 기록한 개인정보파일
 3. 『조세범처벌법』에 따른 조세범칙조사 및 『관세법』에 따른 관세범칙조사에 관한 사항을 기록한 개인정보파일
 4. 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
 5. 그 밖에 이에 준하는 개인정보파일로서 대통령령이 정하는 개인정보파일
- ③ 행정안전부장관은 필요한 경우 제1항에 따른 개인정보파일의 등록사항 및 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다.
- ④ 행정안전부장관은 제1항에 따른 개인정보파일의 등록현황을 누구든지 쉽게 열람할 수 있도록 대통령령이 정하는 바에 따라 공개하여야 한다.
- ⑤ 제1항에 따른 등록과 제4항에 따른 공개의 방법 및 절차에 관하여 필요한 사항은 행정안전부령으로 정한다.
- ⑥ 국회·법원·헌법재판소 및 중앙선거관리위원회(그 소속기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙·대법원규칙·헌법재판소규칙 및 중앙선거관리위원회규칙으로 정한다.

제 5 장 공공기관의 개인정보처리기준에 대한 입법평가

제 1 절 개인정보처리의 입법기준에 대한 평가

입법예고안은 공공부문과 민간부문의 개인정보처리를 함께 규율하는 일반법으로서, 그 처리(=수집·이용·제공)의 허용기준을 별도의 장으로 나누어 따로 규율하지 않고 같은 조에서 함께 규율하고 있다. 다만, 일반개인정보 처리의 경우에는 공공과 민간의 허용기준을 약간 달리하고 있다. 그러나 민감개인정보와 고유식별정보의 처리에 있어서나 또는 영상정보처리기의 설치·운영에 있어서는 양자를 전혀 구분하지 않고 있다. 이하에서는 이러한 규율내용에 대해 분석하고 그 타당성 여부를 간략히 평가하고자 한다.

1. 개인정보처리의 허용기준의 적정성

입법예고안에 의하면, 공공기관은 자신의 “소관 업무의 수행을 위하여 불가피한 경우”에는 정보주체의 동의를 받지 않고 개인정보를 수집·이용할 수 있다(제15조 제1항 제3호). 이는 현행의 「공공기관의 개인정보보호에 관한 법률」(이하 “공공기관 개인정보보호법”)이 공공기관은 “소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다.”(제5조)는 규정을 대체하는 조항이다. 입법예고안이 “불가피한 경우”라는 상당히 제한적 개념을 사용하고 있으나, “필요한 경우”로 표현의 수위를 낮추는 것이 적정해 보인다.

그리고 입법예고안은 공공기관이 자신의 소관 업무의 수행을 위하여 필요한 경우에 처리하는 개인정보를 정보주체의 동의 없이 제3자에게 제공할 수 있도록 허용하고 있다(제17조 제1항 제2호). 그러나

이러한 자신의 소관업무수행 목적을 넘어선 이용이나 제3자 제공(목적 외 이용과 제공)은 원칙적으로 금지하고 다만 일정한 예외를 규정하고 있다.⁶⁴⁰⁾

이처럼 공공기관이 자신의 공적 업무를 수행하기 위하여 개인정보 DB를 구축하고 관련된 국민의 개인정보를 그 정보주체의 동의 없이 수집·이용·제공하는 것을 허용하는 것은 모든 국가의 법률에서 거의 동일하다.

2. 일부 절차적 요건의 흠결

각국의 개인정보보호법이 공공기관의 경우 정보주체의 동의 없는 개인정보처리를 넓게 인정하고 있지만, 그러나 그 정보처리에 따르는 오·남용의 위험성을 사전에 예방하기 위하여 목적명시 요건·고지 요건·보고 요건 등의 절차적 요건을 엄격하게 요구하고 있다. 그런데 입법예고안은 이 절차적 요건의 입법화에 있어서 상당한 입법적 결함과 흠결을 가지고 있는 것으로 평가된다.

우선, 입법예고안은 공공기관이 개인정보를 수집할 때 그 수집목적 등에 관하여 고지의무를 전혀 지우고 있지 않다. 제15조 제2항은 정보주체의 동의를 받는 경우에만 ‘수집목적, 개인정보의 항목, 보유 및 이용기간’의 사항을 정보주체에게 알려주도록 하고 있을 뿐이다. 그러

640) 소관업무수행 목적 이외의 이용 또는 제공이 허용되는 경우로 제18조 제2항에서 8가지 예외를 설정하고 있다: 1. 정보주체로부터 별도의 동의를 받은 경우, 2. 다른 법률에 특별한 규정이 있는 경우, 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우, 4. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우, 5. 개인정보를 목적 외로 이용하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의를 거친 경우, 6. 조약 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우, 7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우, 8. 법원의 재판업무수행을 위하여 필요한 경우.

나 공공기관은 정보주체의 동의 없이 자신의 소관업무의 수행에 필요한 개인정보를 수집할 수 있을 뿐만 아니라, 많은 경우에는 법률에 근거하여 수집이 이루어진다. 그러나 이런 경우에도 적어도 수집의 법적 근거, 수집목적, 다른 기관이나 제3자와 공동 이용하는지 여부, 정보제공이 강제적인 것인지 임의적인 것인지의 여부, 요청된 정보를 제공하지 않는 경우 당해 정보주체에 미칠 효과 등이 고지되어야 할 것이다. 미국의 공공부문 개인정보보호법인 「연방프라이버시법」(Privacy Act)은 수집되는 개인정보가 당해 정보주체에게 불리한 결정을 야기할 수 있을 때에는 직접 수집하도록 요구하고 있고⁶⁴¹⁾, 정보 수집 시에 법적 근거와 이용목적 등의 사항을 알려주도록 요구하고 있다.⁶⁴²⁾

5 U.S.C. §552a(e)

- (2) 수집되는 정보가 당해 개인의 권리(rights), 복지혜택(benefits), 그리고 연방프로그램에서 인정되는 특권(privileges)에 관하여 불리한 결정을 초래할 수 있는 때에는, 당해 정보주체로부터 가능한 한 직접(to the greatest extent practicable directly from the subject individual) 수집하여야 한다.
- (3) 정보를 제공하라고 요청한 각 개인에게 다음 각호의 사항들을 당해 정보를 수집할 때 사용한 그 양식이나 아니면 당해 개인이 계속 가질 수 있는 별도의 양식을 통해 알려주어야 한다.
 - (A) 당해 정보의 요청을 승인하는 법적 근거 (법률 또는 대통령의 집행명령) 및 그 정보의 제공이 강제적인(mandatory) 것인지 임의적인(voluntary) 것인지의 여부
 - (B) 의도하는 당해 정보의 이용목적

641) 5 U.S.C. §552a(e)(2).

642) 5 U.S.C. §552a(e)(3).

(C) 본 (e)항의 (4)(D)에 따라 공표되는 바대로, 있을 수 있는 당해 정보의 일상적 이용(routine uses)

(D) 요청된 정보의 전부 또는 일부를 제공하지 않는 경우 당해 개인에게 미칠 효과 (혹시 있다면)

또한 독일의 연방개인정보보호법은 공공과 민간의 개인정보처리자가 개인정보를 수집하는 경우에 몇 가지 예외가 인정되지만 원칙적으로 정보주체로부터 직접 수집할 것을 요구하고 있다. 그리고 공공기관은 정보주체로부터 개인정보를 수집하는 경우에 ① 자신의 신원, ② 수집목적, 그리고 ③ 제3자에게 제공하는 경우에는 그 제공받는자의 범위(단, 정보주체가 그 제공에 관해 알 수 있는 상황에서는 제외)에 대해 고지를 하도록 요구하고 있다(제4조 제3항 제1문). 또한, 공공기관이 법률에 의해서 개인정보를 수집하거나 정보주체에게 일정한 혜택을 주는 조건으로 개인정보를 수집하는 경우에는 정보주체에게 그 점을 알려주어야 하고, 그렇지 않은 경우에는 개인정보의 제출이 임의적인 것임을 알려주어야 한다. 또한 정보주체의 요구가 있으면, 개인정보의 제출을 거부했을 때 발생하는 결과에 대해서 설명해 주어야 한다(제4조 제3항 제2문).⁶⁴³⁾

일본의 공공부문 개인정보보호법인『행정기관이 보유하는 개인정보의 보호에 관한 법률』도 공공기관이 정보주체로부터 직접 수집하는 경우에는 원칙적으로 이용 목적을 명시하도록 요구하고 있다(제4조).

제 4 조 (이용목적의 명시) 행정기관은 본인으로부터 직접 서면(電子的 방식, 磁氣的 방식 기타 사람의 지각에 의해서는 인식할 수 없는 방식으로 작성된 기록[제24조 및 제55조에 있어서 “電磁的 記錄”이라 한다]을 포함한다)에 기록된 당해 본인의 개인정보를 취

643) 법문의 상세는 위 제4편 제4장 제2절 3. 참조.

득하는 때에는, 다음 각호의 1에 해당하는 경우를 제외하고, 사전에 본인에게 그 이용목적을 명시하여야 한다.

1. 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급한 필요가 있는 경우
2. 이용목적을 본인에게 명시함으로써 본인 또는 제3자의 생명, 신체, 재산 기타의 권리의익을 침해할 우려가 있는 경우
3. 이용목적을 본인에게 명시함으로써 국가기관, 독립행정법인등(독립행정법인등이보유하는개인정보의보호에관한법률[평성 15년 법률 제59호. 이하 “독립행정법인등개인정보보호법”이라 한다.] 제2조 제1항에서 규정하는 독립행정법인등을 말한다. 이하 같다.) 또는 지방자치단체가 행하는 사무 또는 사업의 적정한 수행에 지장을 초래할 우려가 있는 경우
4. 취득상황에 비추어 이용목적이 명확하다고 인정되는 경우

다만, 입법예고안은 수집목적 외의 이용 및 제공의 경우(제18조 제2항 제2호 내지 제8호)에 공공기관은 그 이용 또는 제공의 법적 근거, 목적 및 범위 등의 사항을 관보 또는 인터넷 홈페이지 등에 게재하도록 요구하고 있다(제18조 제5항).⁶⁴⁴⁾

3. 민감개인정보 및 고유식별정보의 처리에 대한 과도한 제한

먼저, 입법예고안은 민간기관뿐만 아니라 공공기관이 민감개인정보를 수집·이용·제공하는 것을 원칙적으로 금지하면서 그 예외를 ① 정보주체의 사전 동의와 ② 법률의 규정이라는 두 가지 경우로 매우 좁게

644) 한편, 입법예고안은 공공기관의 경우와는 달리 민간기관의 목적 외의 이용 및 제공의 경우에는 정보주체의 요구가 있을 때에 그 목적 외 이용 및 제공의 근거, 이용·제공의 목적, 이용·제공하는 개인정보의 항목, 개인정보를 제공받는 자를 명확히 제시하도록 요구하고 있다(제18조 제4항).

설정하고 있어서 그 적용과정에서 심히 불합리한 결과가 예상된다.⁶⁴⁵⁾

또한 입법예고안은 민간기관과 공공기관에 의한 고유식별정보의 처리를 상당히 제한하고 있다. 즉 제23조 제1항은 “누구든지” 고유식별정보(법령에 의하여 개인을 고유하게 구별하기 위하여 부여된 식별정보)를 처리하는 것을 금지하고, 다만 ① 정보주체로부터 “별도의 동의”를 받은 경우와 ② 법령에서 명시적으로 고유식별정보의 처리를 요구하거나 허용하는 경우에 한하여 예외를 인정하고 있다.

그러나 이에 의한다면 현재 공공기관이 주민등록번호를 기본코드로 해서 개인정보DB를 구축하고 있는 현실은, 각 개인정보DB의 구축근거가 되는 법률에서 주민등록번호의 사용을 명시적으로 허용하지 않는 한, 이 규정에 위반될 가능성이 높다. 주민등록번호의 오·남용을 막을 필요성은 충분히 인정되지만, 공공기관이 공적 업무의 수행을 위한 주민등록번호의 합리적인 사용을 원칙적으로 금지시켜야 할 것 인지는 면밀한 비용효과분석을 필요로 한다. 이 부분에 대한 분석은 여기서는 하지 않기로 하고 다만 면밀한 분석을 요한다는 지적으로 그치기로 한다.

제 2 절 개인정보 공동이용의 입법기준에 대한 평가

1. 개인정보 공동이용에 대한 현행법의 규율상황

정보기술의 활용을 통하여 작고 효율적인 시민위주의 질 좋은 행정 서비스를 제공하는 이른바 전자정부를 실현하기 위해 2001년 3월 28일 제정된 「전자정부 구현을 위한 행정업무 등의 전자화 촉진에 관한 법률」⁶⁴⁶⁾(이하 “전자정부법”)은 전자정부의 운영원칙의 하나로서 행정

645) 이 점에 대한 비판은 위 제4편 제3장 제3절 5. 참조.

646) 이 법령은 2007. 1. 3. 법률 제8171호에 의하여 「전자정부법」으로 개명되었다.

정보공동이용의 원칙을 선언하고 있다. 즉, 제11조(행정정보공동이용의 원칙)는 “행정기관은 수집·보유하고 있는 행정정보⁶⁴⁷⁾를 필요로 하는 다른 행정기관과 공동 이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니 된다.”고 규정하고 있다.

또한 동법 제21조는 행정기관 간에 행정정보를 공동이용하도록 의무지우고 있고, 특히 “『공공기관의 개인정보보호에 관한 법률』 제10조 제3항의 규정에 의하여 다른 기관에 제공할 수 있는 처리정보”를 공동이용 대상정보의 하나로 규정하고 있다. 특히 동법 제22조의2는 행정기관⁶⁴⁸⁾이 보유하고 있는 행정정보(개인정보 포함)를 공공기관⁶⁴⁹⁾과 민간의 금융기관이 행정정보공동이용센터를 통하여 공동 이용할 수 있도록 허용하고 있다.⁶⁵⁰⁾

이처럼 현행의 『전자정부법』은 행정의 효율성과 민원서비스의 신속하고 원활한 제공을 위하여 개인정보의 공동이용을 법적으로 요구하고 있다. 그러나 공동이용에 따르는 위험성⁶⁵¹⁾을 상쇄시킬 수 있는 안

647) “행정정보”라 함은 “행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·영상 등으로 표현된 것”을 말한다(법 제2조 제4호). 따라서 개인정보도 여기의 행정정보의 개념에 속한다.

648) 이 법률에서 “행정기관”이라 함은 “국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관 및 국무총리 소속기관을 포함한다. 이하 같다) 및 그 소속기관, 지방자치단체를 말한다.”(제2조 제2호).

649) 이 법률에서 “공공기관”이라 함은 위 행정기관이 아닌 ‘정부투자기관, 정부산하기관, 지방공사 및 지방공단, 특별법에 의해 설립된 특수법인, 각급 학교, 기타 대통령령이 정하는 법인·기관·단체’를 말한다(제2조 제9호).

650) 『전자정부법』상 공동이용의 대상이 되는 개인정보는 “행정기관”이 보유하고 있는 개인정보에만 한정되고, “공공기관”이나 민간의 금융기관이 보유하고 있는 개인정보는 포함되지 않는다는 점에 유의할 필요가 있다. 때문에 건강보험공단이나 국민연금관리공단 등의 공공기관이 보유하고 있는 개인정보는 공동이용의 대상이 되지 않는다. 『전자정부법』과 『공공기관의 개인정보보호에 관한 법률』상의 “공공기관” 개념이 서로 달라 혼란을 일으키고 있다. 후자의 “공공기관” 개념은 행정기관이 포함된 개념이다.

651) 행정기관이 보유하고 있는 개인정보를 다른 기관 또는 민간의 금융기관과 공유하는 것에 대하여 일반인 및 전문가가 인식하는 위험의 정도에 관한 설문조사의

전장치는 동법에서 특별히 마련하고 있지 않으며, 다만 현행의 「공공기관의 개인정보보호에 관한 법률」에 의해서 규율될 수 있다. 그러나 공공기관개인정보보호법은 컴퓨터매칭(computer matching) 등 개인정보 데이터베이스의 연동 내지 연계에 대해서는 특별한 규율을 담고 있지 않다.⁶⁵²⁾ 단지 제3자 제공의 허용기준에 대해서만 규정하고 있을 뿐이다. 즉, 공공기관은 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 제3자에게 제공할 수 없다는 것을 원칙으로 하면서도(제10조 제1항), 목적 외 제3자 제공을 할 수 있는 예외를 상당히 광범위하게 허용하고 있다.⁶⁵³⁾ 즉 개별 법률에서의 명시적인 근거나 정보주체

결과는 위 제2편 제1장 제1절 4. 참조.

652) 2001년 7월에 행정자치부가 발간한 □□전자정부법의 이해와 해설□□, 56면은 당시 Data 가공여부에 따른 행정정보공동이용의 방식에는 다음의 4가지가 있는 것으로 설명하고 있다.

- (i) Data Integration 방식 : 관련 DB의 요약본을 수집하여 하나의 DB로 통합 구축하고, 개별 수요자에게 제공하는 방식. 사실상 이중적 DB가 구축된다는 문제점 있음.
 - (ii) Data Pool 방식 : 관련 DB의 요약 DB를 수집하여 pool로 관리하고, 통합활용 시스템에 요약 DB를 제공하는 방식. 주민, 부동산, 호적 등 DB의 요약 DB 등 시군구 공통 21개 업무 DB의 pool을 구축하고 이를 시군구 행정종합정보화시스템에 제공하여 일선 민원처리시 활용하고 있음.
 - (iii) Data Profiling 방식 : 일관된 정보를 집적하는 DB complex에 변동되는 DB 구성요소를 전송, 업데이트하는 Super DB를 제공하는 방식. 자동차등록기록 등 자동차 관련 사항을 발생시점별로 입력하여 일관된 관리를 도모함.
 - (iv) Data matching 방식 : DB를 보유기관에 그대로 두고, 대조할 DB를 대조될 DB와 대조하여 목적을 달성하는 시스템 방식. 여권전산망에서 여권신청자의 신청항목을 주민 DB에 보내어 그 항목의 진위여부를 yes/no로 회신 받는데 활용하고 있음.
- 653) (i) 다른 법률에 제공의 근거가 있는 경우(제10조 제1항), (ii) 정보주체의 동의가 있는 경우(제10조 제3항 제1호), (iii) 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 제20조에 따른 공공기관개인정보보호심의위원회의 심의를 거친 경우(제10조 제3항 제2호), (iv) 조약 기타 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하는 경우(제3호), (v) 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정개인을 식별할 수 없는 형태로 제공하는 경우(제4호), (vi) 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수 없는 경우로서 정보주체외의 자에게 이용하게 하거나 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정되는 경우(제5호), (vii) 범죄의 수사와 공소의 제기 및 유지에 필요한 경우(제6호), (viii) 법원의 재판업무수행을 위하여 필요한 경우(제7호).

의 동의가 없더라도, 제공받는 다른 기관의 소관업무의 수행에 필요하다면 보유목적 외의 제공이 가능하다(다만, 이 경우 공공기관개인정보보호심의위원회의 심의를 거침).

더구나 「전자정부법」은 행정정보의 공동이용을 모든 행정기관의 의무로 규정하고 있고(제21조), 또한 행정기관이 보유하는 개인정보를 공공기관과 민간의 금융기관에까지 제공할 수 있도록 허용하고 있다(제22조의2). 「전자정부법」의 이 법률조항은 공공기관개인정보보호법이 보유목적 외의 제3자 제공의 허용기준으로 설정하고 있는 “다른 법률”에 해당하는 것으로 볼 수 있고, 만일 그렇게 해석한다면 행정기관이 보유하는 모든 개인정보는 아무런 제한 없이 다른 기관과의 공동이용이 얼마든지 가능하게 된다. 나아가 이 때 공공기관개인정보보호심의위원회의 심의를 거칠 필요도 없게 된다. 이 경우에 유일한 절차적 통제장치는 제10조 제6항의 제공사실에 대한 공시인데,⁶⁵⁴⁾ 그마저도 동 조항의 해석상 「전자정부법」에 근거한 제3자 제공에는 적용되지 않는 것으로 보인다.⁶⁵⁵⁾

요컨대, 「전자정부법」상의 “개인정보 공동이용제도”는 공공기관개인정보보호법의 허술한 안전장치마저도 해체시키는 기능을 하고 있다. 아쉽게도 입법예고된 「개인정보보호법 제정법률안」에도 이 점에 관한 고려가 전혀 없다. 다만, 입법예고안은 다른 법률에 근거한 수집목적 외의 이용 및 제공의 경우에도 공공기관은 그 제공의 법적 근거, 목적 및 범위 등의 사항을 관보 또는 인터넷 홈페이지 등에 게재하도록 요구하고 있을 뿐이다(제18조 제5항). 그러나 이 규정은 개인정보의 공동이용을 염두에 둔 조항이 아니라 일반적인 제3자 제공을 전제로

654) 제10조 제6항 : “보유기관의 장은 제3항 제2호 내지 제5호 및 제7호에 따라 보유목적 외의 목적으로 이용하게 하거나 제공하는 경우에는 그 이용 또는 제공의 법적 근거·목적 및 범위 등에 관하여 필요한 사항을 정보주체가 쉽게 확인할 수 있도록 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.”

655) 제10조 제6항은 제공사실의 공시 요건을 ‘동조 제3항 제2호 내지 제5호 및 제7호’에 따른 제공에 한정하고 있기 때문이다.

한 것이다.

“개인정보 공동이용”이 개인정보보호의 측면에서 안고 있는 문제는 단순히 보유정보를 다른 기관에게 개별적으로 제공하는 것과는 차원이 다른 문제이다. 『전자정부법』상의 “행정정보 공동이용”이란 행정기관이 보유·관리하고 있는 행정정보(개인정보 포함)를 다른 행정기관 또는 공공기관 등이 “정보시스템을 통하여” 공동이용하는 것을 말한다.⁶⁵⁶⁾ 따라서 개인정보 공동이용은 각 행정기관이 보유·관리하고 있는 개인정보파일, 즉 개인정보DB들을 상호 연동 내지는 연계하는 방식으로 이루어진다.

개인정보DB의 연동 내지는 연계를 통한 개인정보 공동이용에 대한 규율의 흠결 문제를 해결하기 위하여 최근 행정안전부는 2008년 9월 5일 공청회를 열고 입법예고한 『전자정부법 전부개정법률안』의 제4장에서 “행정정보의 공동이용”이라는 제목 하에 제32조에서 제41조에 걸쳐 구체적으로 규율하고 있다. 이러한 시도는 일단 긍정적으로 평가된다.

2. 개인정보 공동이용의 효용성과 위험성

그런데 개인정보 공동이용은 전자정부의 필수조건인가? 『전자정부법』은 개인정보 공동이용을 전자정부의 핵심개념으로 상정하고 있고, 정부도 행정정보공유추진위원회와 행정정보공동이용센터를 설치해 범정부적 차원에서 적극적으로 추진해 나가고 있다.⁶⁵⁷⁾ 물론 개인정보의 공동이용이 갖는 효용성은 무시할 수 없다.⁶⁵⁸⁾

656) 행정자치부가 2008년 2월에 발간한 □□2007 전자정부법의 이해와 해설□□, 63면 참조.

657) 행정정보 공동이용의 추진과정과 상황에 관해서는 행정정보공유추진위원회가 2007년 12월에 발간한 『2007 행정정보공동이용 백서』, 24-140면 참조.

658) 정부는 행정정보 공동이용의 효과를 다음의 4가지로 설명하고 있다. (i) 대국민서비스 향상 : 국민이나 기업이 행정서비스를 받을 때 행정기관들이 필요정보를 연계하여 처리함으로써 윈스톱/논스톱 서비스를 제공할 수 있어 시간적·경제적 비용의 절감과 높은 만족감 향유; (ii) 불필요한 서류제출 부담 경감 : 국민과 기업으

그런데 여기에는 반드시 진지하게 되짚어보아야 하는 문제가 있다. 당연히 “일반적인 행정정보”는 행정기관 상호간에 공유하는 것이 바람직하다. 나아가 행정의 민주성과 투명성을 위해서는 행정정보를 행정기관 상호간에만 공유할 것이 아니라 오히려 국민(기업 포함)과도 공유하여야 한다. 행정정보는 당해 행정기관의 자산이 아니라 국민의 자산이자 정보(public information)이기 때문이다. 이것이 헌법이 인정하는 정보공개청구권의 기본취지이며 『공공기관의 정보공개에 관한 법률』의 입법취지이다.

그러나 행정기관이 보유하고 있는 개인정보는 그 모두가 다 공적 정보(public information)가 되는 것은 아니다. 『공공기관의 정보공개에 관한 법률』은 “개인의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보”는 정보공개 대상에서 제외하고 있다(제9조 제1항 제6호). 물론 개인정보 공동이용에서는 개인정보를 일반인에게 “공개”하는 것은 아니다. 공동이용이 필요한 기관 상호간에 개인정보를 주고받아 “내부적으로 이용”하는 것이다. 때문에 충분한 안전장치를 갖춘다면 정보주체의 프라이버시 침해 등의 문제를 최소화할 수 있다. 이 경우 입법정책상의 쟁점은 과연 어느 정도의 안전장치가 충분한 것인가 하는 것이다. 이런 안전장치의 법제화를 고려함에 있어서 항상 염두에 두어야 하는 핵심쟁점은 ‘개인정보DB의 통합에 따르는 Big Brother의 출현가능성’이라는 위험성이다.

현행의 『전자정부법』과 입법예고된 『전자정부법 전부개정법률안』은 “개인정보 공동이용”과 “일반행정정보 공동이용”을 구분하지 않은 채 “행

로부터 기본적인 주민정보, 기업정보 등을 한번만 요구하여 이를 DB화하고 공동 활용함으로써 동일한 정보를 반복적으로 요구하는 일이 없게 되고 불필요한 서류 제출 등의 부담을 덜어 줌; (iii) 행정기관의 능률성 향상 : 업무에 필요한 정보와 자료를 신속하고 정확히 입수 활용함으로써 능률성 제고; (iv) 중복투자방지 : 각 행정기관별로 구축되어 있는 데이터베이스를 공동 이용함으로써 유사 데이터베이스의 중복적인 개발 방지. 행정자치부, □□2007 전자정부법의 이해와 해설□□, 2008. 2. 63-64면 참조.

정정보 공동이용”이라는 단일의 이름으로 묶어 개인정보 공동이용을 규율하고 있다. “개인정보 공동이용”이라는 용어는 법률의 어디에서도 나오고 있지 않지만, 사실상 행정정보 공동이용에 관한 규율내용은 전적으로 개인정보 공동이용에 관한 것이다. 그러면서 공동이용의 원칙을 선언하고 있고 나아가 공동이용을 행정기관에게 의무지우고 있다. 특히 입법예고된 『전자정부법 전부개정법률안』은 제48조에서 정보통신망의 통합·연계를 요구하고 있고, 제50조에서는 정보자원의 통합관리를 규정하고 있다. 아울러 현행법과 입법예고안은 공동이용을 행정정보공동이용센터를 통하여 이루어지도록 요구하고 있다.

요컨대, 입법예고안은 각 행정기관이 자신의 소관업무를 수행하기 위하여 각자 별도로 구축·운영하고 있는 개인정보DB를 통합적으로 연동 내지는 연계할 수 있는 가능성을 열어주고 있는 것으로 보여 상당한 우려를 낳고 있는 것으로 평가된다. 그러나 정부가 보유하고 있는 수많은 개인정보DB를 시스템적으로 통합이 가능하도록 허용하는 것은, 설령 그것이 실제로는 부분적이고 일시적인 연계에 의한 개인정보의 공동이용이라 하더라도, 개별적으로 제3자 제공을 허용하는 것과는 비교할 수 없을 정도의 위험성을 안고 있는 문제이다.

행정정보공유추진위원회는 행정정보공동이용체계를 구축할 때 기본방향으로 다음의 5가지를 제시하고 있다. 첫째, 행정·공공·금융기관 간의 범정부적 정보공동이용을 위해 교두보 역할을 할 행정정보공동이용센터를 설치하여 운영하는 것; 둘째, 정보공동이용 DB를 실시간 이용이 가능하도록 구축하는 것. DB의 위치는 정보보유기관의 시스템에 두되, 행정정보공동이용센터에 그 색인DB를 구축함; 셋째, 행정정보공동이용센터를 중심으로 정보보유기관과 정보이용기관을 연계하는 것. 정보유통 시 전체 연계를 관장할 행정정보공동이용센터를 통해야만 정보유통에 따른 각 기관별 책임을 명확히 할 수 있음; 넷째, 행정정보공동이용 범위 확대에 따른 정보유출 및 오·남용 방지를 위해

보안 및 인증체계를 강화하는 것; 다섯째, 범정부정보공유의 기반이 되는 법·제도를 우선 정비하는 것.⁶⁵⁹⁾

아울러 행정정보공유추진위원회는 행정정보공동이용센터의 역할을 다음의 5가지로 정의하고 있다.⁶⁶⁰⁾

첫째, 행정정보공동이용센터는 범정부적인 정보공동이용서비스를 제공하고 이를 위한 시스템을 구축한다. 구비서류 열람, 대량정보 제공, 정보의 진위여부 확인 등의 서비스 제공을 통해 행정·공공·금융기관의 민원 및 업무처리를 지원하고, 이를 위한 기반으로 기관별·주제별 정보시스템을 연계하고 관련 시스템을 구축한다. 또, 민원 및 업무처리 지원을 위해 구축한 정보공유 기반을 통해 국가 정책정보를 수집·가공·분석하여 제공한다.

둘째, 체계적인 서비스 제공을 위하여 행정정보공동이용체계를 운영하고 유지·관리한다. 정보제공기관 및 이용기관에 대한 심사·승인관리, 정보 이용자에 대한 등록·인증·접근권도 관리한다. 정보의 연계성 유지를 위해 기관·코드 정보 등 메타정보도 관리하며, 정보공유의 정합성(整合性) 유지를 위해 실시간 모니터링을 실시하고 공유상황을 관리한다.

셋째, 공유DB를 연계하고 색인DB를 구축한다. 정보공동이용 대상정보에 대해 정보를 보유하고 있는 기관에서 실시간 정보공동이용이 가능하도록 DB를 연계하고, 기관보유 운영DB의 실시간 정보공동이용이 어려울 경우 요약DB를 구축하여 연계한다. 또, 기본사항 열람 외에도 정책정보 가공 시 활용할 수 있도록 공유센터에 색인DB를 구축하고 각 정보보유기관과 연계하여 자료의 현행성을 유지한다.

넷째, 제공기관과 이용기관을 연계한다. 공동이용 대상정보를 보유하고 있는 기관별 정보시스템과 행정정보공동이용시스템을 전자정부통합망을 통해 연계함으로써 정보를 공동이용 할 수 있도록 한다. 이때 공

659) 행정정보공유추진위원회, 『2007 행정정보공동이용 백서』, 2007. 12, 55면 참조.

660) 위의 백서 56-57면 참조.

동이용 대상정보의 DB를 고려하여 연계한다. 행정기관은 기존의 전자정부통합망을 이용하여 공유센터와 연계하고 공공기관과 금융기관은 행정정보공동이용센터구축과 병행하여 단계별로 연계를 추진한다.

다섯째, 행정정보 제공 및 이용에 관한 구체적인 절차를 제도화하고 행정정보 이용에 관한 지침을 수립한다. 정보이용 신청 및 심사에 대한 절차, 정보시스템 및 DB연계 절차, 정보이용기관 및 이용자를 등록하고 관리하는 절차, 이용정보의 관리 및 운영 절차, 행정·공공·금융기관의 이용정보 보관 및 관리 절차 등 각종 절차를 규정화한다. 그리고 접근권한과 정보이용 시의 책임소재, 정보이용 방법, 보안관리 등 행정정보이용에 관한 지침을 수립하고 관련 기관에 제공한다.

이상 행정정보공유추진위원회가 설정하고 있는 행정정보공동이용체계의 기본방향과 행정정보공유센터의 역할과 기능에 의하면, 각 행정기관이 보유하고 있는 개인정보DB와 기업정보DB를 통합 연계하는 것을 기본전제로 하고 있다. 그러나 정부가 국민의 개인정보와 기업의 정보를 통합할 수 있는 가능성을 열어 두는 것 자체는 자유민주주의체제에서 경계해야 될 일이다. “개인정보 공동이용”을 전자정부의 핵심개념이자 기본전제로 여기는 사고는 정부기능의 효율성만을 강조한 것으로서 행정의 민주성과 투명성의 가치를 경시한 것이라고 평가하지 않을 수 없다.

비교법적으로 미국은 행정기관간의 개인정보의 컴퓨터결합(computer matching)을 개별적으로만 제한적으로 허용하고 있다. 그러면서 내부적인 절차적 안전장치를 상세하게 마련해 놓고 있다. 이러한 내용은 정부 측의 무분별한 컴퓨터결합으로부터 개인정보의 완전성을 보호하기 위하여 1988년에 컴퓨터결합 행위 자체를 규율하는 내용의 □□컴퓨터결합과 프라이버시보호법□□(Computer Matching and Privacy Protection Act)에 담겨 있다.⁶⁶¹⁾

661) 이 법률의 내용은 『연방프라이버시법』(Privacy Act)에 편입되어 현재 연방법률집

참고로, 지난 2002년 9월 19일자 미국의 연방관보(Federal Register)에 고시된 교육부(Department of Education)와 연방이민국(Immigration and Naturalization Service) 사이에 운용되는 컴퓨터결합프로그램에 관한 내용을 소개한다.⁶⁶²⁾ 우리의 규범상태와 크게 비교된다.⁶⁶³⁾

두 기관 사이에 운용되는 컴퓨터결합프로그램은 “연방이민국과 교육부간의 자격확인용 외국인조회시스템”(Systematic Alien Verification for Entitlement INS/ED)이라는 타이틀을 가진다. 이 프로그램은 교육부가 연방학생보조금을 받고 있거나 또는 신청을 한 외국인학생의 입국 자격(immigration status)을 조회할 수 있도록 허용할 것이다.

입국자격정보는 1986년의 입국개혁및통제법(Immigration Reform and Control Act of 1986)에 근거하여 연방이민국이 외국인자격조회색인(Alien Status Verification Index)이라는 개인정보DB를 통해 보유하고 있다. 한편, 교육부는 1965년의 고등교육법(Higher Education Act of 1965)에 근거하여 위 외국인자격조회색인에 접근할 수 있는 권한을 부여받고 있고, 또 연방이민국은 입국및국적법(Immigration and Nationality Act) 제103조의 일반적 권한에 따라 입국자격을 다른 기관에게 확인해 줄 수 있다. 연방학생보조금을 받고 있거나 신청을 한 외국인학생이 그러한 자격이 있는지를 검증하기 위한 목적에서 교육부가 연방이민국

제5편 제552a조의 (o)(p)(q)(r)(u)항에 수록되어 있다. 이 법상의 컴퓨터결합이란 연방복지프로그램의 수혜자 자격을 심사하거나 검증하기 위한 목적에서 각 공공기관이 보유하는 개인기록시스템 상호간을 전산처리에 의해 자동으로 대조하거나, 또는 연방의 인사기록시스템들(personnel systems of records)이나 급여기록시스템들(payroll systems of records) 상호간 또는 하나의 연방 인사기록시스템이나 급여기록시스템과 비연방의 개인기록(non-Federal records) 상호간을 전산처리에 의해 자동으로 대조하는 것을 말한다(제552a조 (a)(8)항). 미국의 행정기관 간의 개인정보 컴퓨터결합에 대한 절차적 통제에 관한 상세는, 이인호, “미국의 개인정보보호법제에 대한 분석과 시사점”, 『법학논문집』 제29집 제1호(중앙대학교 법학연구소, 2005) 참조.

662) Notice of Computer Matching Program, 67 Fed. Reg. 59056, 59056 (Sept. 19, 2002)

663) 미국과 독일의 개인정보 공동이용의 통제와 감독에 관한 비교법적 분석은, 김일환, “개인정보 공동이용의 통제와 감독에 관한 비교법적 고찰 - 미국과 독일의 법제를 중심으로”, 『헌법학연구』 제13권 제2호(한국헌법학회, 2007. 6) 참조.

의 외국인자격조회색인 데이터베이스에 접속하는 것을 허용하는 두 기관 사이의 컴퓨터결합협정(matching agreement)이 최초로 승인된 것은 1990년이였다.⁶⁶⁴⁾

위 컴퓨터결합프로그램의 운용을 통해, 교육부는 자신이 보유하는 “연방학생보조금신청화일”(Federal Student Aid Application File)에 담겨 있는 외국인학생의 데이터(외국인등록번호와 생년월일을 포함해서)를 연방이민국에 전송할 것이다.

이 데이터를 이용해서, 외국인자격조회색인 데이터베이스에서 검색이 이루어질 것이고, 서로 일치하는 개인기록들이 있으면, 그 데이터베이스는 교육부에게 당해 외국인학생의 입국자격정보를 제공하게 될 것이다.

그러나 교육부는 무자격자를 발견했더라도 곧 바로 보조금지급과 관련한 불이익결정을 내릴 수 없다. 즉, (i) 교육부가 무자격이라는 정보의 정확성을 독자적으로 확인하거나, 아니면 (ii) 교육부 소속의 자료보전위원회(Data Integrity Board)가 그 정보가 정확하다는 점 및 당해 외국인학생이 교육부로부터 그 요지와 그에 대해 다룰 수 있는 기회가 있음을 통지받았다는 점을 상당한 확신을 가지고 판단을 내리기 전에는 달리 불이익결정을 할 수 없다.

또한 교육부는 당해 외국인학생이 위 컴퓨터결합프로그램에 의한 무자격 인정사실을 통지받은 후 최소 30일 이내에는 그 불이익결정을 집행할 수 없다. 위 컴퓨터결합프로그램은 양 기관의 자료보전위원회가 승인한 컴퓨터결합협정(matching agreement)의 사본이 연방의회에 제출되어 관리예산국(Office of Management and Budget)의 승인을 받은 후 40일이 지나 발효한다.

664) 55 Fed. Reg. 5904 (1990).

3. 「전자정부법 전부개정법률(안)」에 대한 평가

행정안전부가 2008년 9월 5일 공청회를 열고 입법예고한 「전자정부법 전부개정법률안」은 제4장에서 “행정정보의 공동이용”이라는 제목 하에 제32조에서 제41조에 걸쳐 구체적으로 규율하고 있다.

그 내용을 간략히 살펴보면, 행정기관은 민원사항의 처리를 위하여 필요한 행정정보와 「공공기관의 개인정보보호에 관한 법률」제10조 제3항에 의하여 보유목적 이외로 다른 기관에 제공할 수 있는 처리정보 등을 공동 이용해야 한다(제33조 제1항). 공공기관개인정보보호법상으로는 보유목적 외의 제공이 보유기관의 재량사항이었지만, 전자정부법 입법예고안은 공동 이용을 의무화하고 있는 것이다. 또한 보유기관은 다른 공공기관이나 민간의 금융기관과 처리정보를 공동 이용할 수 있다(제33조 제5항). 그리고 이러한 공동이용은 행정안전부장관 소속 하에 있는 행정정보공동이용센터를 통하여 이루어지며(제32조 제4항 및 제33조 제5항), 공동이용의 집행책임은 행정안전부장관에게 주어져 있다.

그러나 개인정보의 공동이용에는 승인절차가 마련되어 있다. 즉, “행정안전부장관은 … 행정정보를 공동이용하게 하는 경우 … 「개인정보보호법」…에 따른 개인정보보호위원회의 의결(개인정보가 포함된 행정정보에 한한다)을 거쳐 공동이용의 목적, 공동이용 대상 행정정보와 그 범위, 공동이용의 방식, 그 밖에 공동이용의 조건을 정하여 이를 승인할 수 있다.”(제34조 제1항). 승인의 여부는 행정안전부장관에게 달려 있으며, 다만 몇 가지 경우에는 승인이 금지된다(제34조 제1항 단서 각 호).

그러나 이 승인절차를 규정한 법안 내용은 두 가지 점에서 문제가 있다. 첫째, 승인절차의 대상이 되는 행정정보를 “개인정보가 포함된

행정정보”라고 규정하고 있는데, 그러나 이 개념은 너무 포괄적이다. 이렇게 넓은 개념의 행정정보의 공동이용에 대해 승인 등의 통제를 한다면, 오히려 필요한 행정정보의 공동이용이 원활하게 이루어지기 어렵고, 그리고 공동이용에 따른 업무가 가중될 우려가 있다. 이 조항의 존재이유 내지 입법취지는 현행의 공공기관개인정보보호법 및 입법예고된 『개인정보보호법(안)』상의 “개인정보파일”에서 처리되는 처리정보(즉, 개인정보)를 공동 이용함에 따르는 프라이버시침해 문제에 대응하고자 하는 것이다. 그런데 “개인정보가 포함된 행정정보”라고 하면 일반적인 행정정보 안에 몇 가지 개인정보가 포함되는 것이면 모두 여기의 행정정보에 포함될 수도 있다.

전자정부법 입법예고안은 계속해서 공동이용에 대한 승인 등의 통제를 받는 대상정보를 무단히 “행정정보”라고 하고 있는데, 차라리 “개인정보”라고 하는 것이 혼란을 초래하지 않을 것으로 보인다. 그리하여 이 조의 제목도 “제34조(개인정보 공동이용의 승인)”이라고 하는 것이 정직하다. 사실, ‘개인정보의 공동이용에 따르는 통제의 문제’(이 법안의 제34조~제38조)는 원칙적으로 입법예고된 『개인정보보호법(안)』에서 다루는 것이 입법체계상 적절할 것으로 평가된다.

승인절차를 규정한 법안 제34조 제1항의 두 번째 문제점은 공동이용의 승인과 관련하여 행정안전부장관과 개인정보보호위원회의 권한 배분 관계가 애매하다는 점이다. “의결을 거쳐 승인할 수 있다.”고 하고 있는데, ‘심의’가 아닌 ‘의결’이라고 하고 있기 때문에 구속력이 있는 것으로 판단된다. 그런데 ‘의결의 대상범위’가 불명확하다. 즉, 공동이용 대상정보의 범위, 공동이용의 방식이나 조건을 ‘정하는 자’는 장관인지, 아니면 개인정보보호위원회인지 불명확하다. 또 제1항 단서 규정에서 승인해서는 안 되는 공동이용에 대해 ‘판단하는 자’는 장관인지, 아니면 개인정보보호위원회인지 역시 불명확하다. 판단컨대, 개인정보의 공동이용에 대한 통제권한은 행정안전부장관보다는 국무총

리 소속의 개인정보보호위원회로 넘기는 것이 타당하다고 생각된다. 행정안전부장은 전자정부의 주관책임자로서 개인정보의 공동이용에 적극적인 입장에 설 수 밖에 없는데, 이와 같은 행정안전부장이 한편으로 개인정보의 공동이용을 통제하는 권한을 가진다는 것은 이해충돌이 있는 사안을 동일 기관이 모두 관장하게 되는 것이기 때문이다.

한편, 이러한 승인절차 외에 「전자정부법 전부개정법률안」은 사후에 이용기관이 법률상의 의무나 조건을 위반한 때에는 행정안전부장이 승인을 철회하거나 공동이용을 중단시킬 수 있도록 하고 있다(제36조).

나아가, 법률안은 개인정보를 공동이용하는 경우 이용기관으로 하여금 정보주체의 사전 동의를 받도록 요구하고 있다(제37조 제1항). 이 사전 동의 요건은 정보주체에게 공동이용에 대한 절대적인 통제권을 주는 것으로서 우선 긍정적으로 평가할 수 있지만, 그러나 한편으로 개인정보의 공동이용을 의무화하고 있는 규정과 어떻게 조화될 수 있는지 의문이다.

그리고 법률안은 사전 동의 요건이 면제되는 예외적인 경우를 규정하면서, 이러한 경우에는 공동 이용 후에 공동이용의 목적 등을 정보주체가 알 수 있도록 하여야 한다고 규정하고 있다(제37조 제2항).⁶⁶⁵⁾ 그런데 사전 동의 요건이 면제되는 예외적인 경우 4가지 중 3가지는 모두 정보주체에게 불이익한 결정을 내리는 경우이다. 즉, 불이익한 결정을 내리는 경우에는 정보주체의 동의 없이 행정정보공동이용체제를 활용하여 다른 기관의 개인정보를 이용할 수 있다는 것이다.

665) 사전 동의 요건이 면제되는 예외적인 경우는 다음과 같다: “1. 정보주체의 생명 또는 신체의 보호를 위하여 긴급하게 공동이용할 필요가 있는 경우, 2. 법령에 의하여 상대방에게 의무를 부과하거나 권리·이익을 취소·철회하는 업무를 수행하기 위하여 공동이용이 불가피한 경우, 3. 법령을 위반한 자에 대한 조사 또는 처벌 등 제재와 관련된 업무의 수행을 위하여 공동이용이 불가피한 경우, 4. 정보주체의 신청에 의하지 아니하고 법령에 따라 정보주체에 대한 권리·자격의 부여, 의무의 면제·감경 또는 사실의 조사·확인을 위하여 공동이용이 불가피한 경우.”

그러나 행정기관이 개인에게 불리한 결정을 내릴 때 그 판단자료로 활용되는 개인정보를 정보주체에게 직접 수집하지 아니하고 다른 행정기관이 보유하고 있는 개인정보를 이용하는 것에 대해서는 재검토를 요한다. 위에서 언급한 바와 같이, 미국의 공공부문 개인정보보호법인 「연방프라이버시법」(Privacy Act)은 수집되는 개인정보가 당해 정보주체에게 불리한 결정을 야기할 수 있을 때에는 가능한 한 직접 수집하도록 요구하고 있고⁶⁶⁶, 정보 수집 시에 법적 근거와 이용목적 등의 사항을 알려주도록 요구하고 있다.⁶⁶⁷

666) 5 U.S.C. §552a(e)(2).

667) 5 U.S.C. §552a(e)(3).

제 5 편
개인정보보호의 집행체계에
관한 병행적 입법평가

제 1 장 개인정보감독기구의 설립방향성

제 1 절 서 언

오늘날 하루가 다르게 발전해가는 정보통신기술은 개인정보를 매우 간이하고 신속하게 그리고 대량적으로 수집하고 처리할 수 있게 하였다. 새로운 전자적 감시장비에 의하여 개인의 일상적 생활이 낱알이 포착될 수 있고, 그렇게 포착된 개별 정보들이 컴퓨터에 의하여 하나의 데이터베이스로 집적되고 그것이 다시 개인별로 색인화될 수 있다.

그런데 개인정보의 수집과 처리의 기법이 다양화되었고 교묘해지면서, 개인은 자신에 관한 정보를 쉽사리 통제하기 어렵게 되었다. 무엇보다도 자신에 관한 정보가 언제 어디서 어떻게 수집되고 처리되며 활용되는지를 그 정보의 주체가 인식하기 어렵기 때문이다.

이러한 상황에서 개인정보자기결정권의 효과적 보장을 위한 국가적 노력은 그 어느 때보다도 중요하다. 여기서는 물론 개인정보침해자로서의 국가가 아니라 개인정보보호의 책임자로서의 국가가 강조된다.

즉 개인정보보호를 위한 국가의 책무는 개인정보를 스스로 침해하는 일이 없도록 주의를 기울이는 소극적 측면에 머물지 않고, 개인정보침해의 가능성에 대처하기 위한 법적·제도적 방안을 확충해야 하는 적극적 측면에까지 미치는 것이다.

이러한 적극적 책무에는 기술적·조직적 안전대책을 마련하는 것도 포함되어야 한다. 특히 조직적 안전망의 구축과 관련하여서는 개인정보의 침해를 예방하고 정보주체의 통제권 행사를 원조하기 위하여 개인정보보호에 관한 업무를 전담하는 독립적 조직을 설치·운영하는 것이 필요하다.⁶⁶⁸⁾ 이러한 기구는 개인정보침해의 가능성을 면밀히 점검하여 예방책을 제시할 수 있을 정도의 전문적 식견을 가진 사람들

668) 김동희, 『행정법 I』 (박영사, 2001), 389면.

로 구성될 때 그리고 개인정보보호법의 준수를 지도·감독하며 분쟁발생시 당사자간의 원만한 해결을 위해 관여하는 등의 권한이 부여될 때 그 실효성을 기대할 수 있을 것이다. 이러한 개인정보감독기구의 중요성은 독일연방헌법재판소의 인구조사판결에서도 강조된 바 있다.⁶⁶⁹⁾

오늘날 국가나 사회의 정보처리를 통제하는 개인정보감독기구를 설치하여 운영하고 있는 나라가 상당수에 이르고 있다.

현재 OECD 회원국 가운데 29개 국가가 개인정보감독기구를 설치·운영하고 있으며,⁶⁷⁰⁾ 유럽연합은 Directive/ 95/46/EC에서 회원국들에게 완전히 독립적 지위를 가지는 감독기관을 설치할 것을 의무화하면서, 그 감독기관에는 특히 처리행위의 대상을 구성하는 정보에 대한 접근 권한 및 감독임무를 수행하는 데 필요한 모든 정보의 수집 등 조사권한, 의견진술권, 정보의 차단·삭제·파기 등의 명령권, 처리의 중지 내지 금지처분권, 관리자에 대한 징계권, 이 지침에 따른 국내법의 위반행위에 대한 소송개시나 고발에 관한 권한 등의 권한을 부여하도록 하고 있다(제28조).

우리의 현행 개인정보보호체계에서 중요한 결함 중의 하나는 독립적인 개인정보감독기구가 존재하지 않는다는 점이다. 독립된 개인정보감독기구의 존재는 ‘안전한 개인정보의 이용’이라는 개인정보보호법의 입법목표를 달성하기 위한 가장 핵심적인 요소이자 안전장치이다. 우리의 현행 보호체계에서 “예방적 집행 기능”이 제대로 작동하지 못하고 있는 가장 큰 구조적 이유는 바로 이러한 독립적인 개인정보감독기구가 존재하지 않기 때문이다. 개인정보감독기구의 독립성이 강조되는 이유는 감독을 받는 개인정보처리기관이 바로 정부기관들이기

669) BVerfGE 65, 1 (46) : 『자동정보처리의 상황하에서 시민들이 정보의 이용과 저장을 제대로 파악하기 곤란하기 때문에 그 적절한 예방조치를 통한 권리보호를 위하여 독립된 정보보호위원의 참여가 필요하며, 따라서 정보보호위원은 정보자기결정권의 효율적인 보호를 위하여 중요한 의미를 가진다.』

670) 정영화, “인터넷상 개인정보보호 및 분쟁해결에 관한 연구”, 『인터넷법연구』 제 1호(법무부, 2002. 6), 41면.

때문이다. 최근에는 기업과 같은 민간기관도 기업의 운영과 경제활동을 위해 방대한 개인정보데이터베이스를 구축하여 이용하고 있지만, 전통적으로 정부기관들은 소관업무의 수행을 위하여 국민 개개인의 개인정보를 데이터베이스화하여 처리하고 있다. 따라서 개인정보를 처리하는 정부기관들이야말로 개인정보보호법의 규율을 받는, 그리하여 개인정보감독기구로부터 감독을 받는 전형적인 기관들이다. 그리하여 감독을 하는 자와 감독을 받는 자가 기능적으로 분리되어야 함은 물론이고, 감독기구가 피감독기관으로부터 독립하여 독자적으로 감독 업무를 수행할 수 있어야 한다.

여기서 중요한 요소는 감독기구의 “기능상의 독립성”이다. 개인정보감독기구의 독립성은 조직체계상으로 완전한 분리독립을 의미하는 것이라기보다 기능상의 분리 독립을 의미한다. 따라서 개인정보감독기구를 조직체계상으로 대통령이나 국무총리 소속 하에 둔다고 해서 그 자체만으로 독립성이 없다고 단정할 수는 없다.

그리하여 지난 17대 국회에 발의되어 자동폐기된 3건의 개인정보보호법안들은 개인정보감독기구의 독립성을 확보하기 위하여 개인정보보호위원회를 국무총리 소속하에 두거나, 국가인권위원회 성격의 독립성을 제안하고 있었다. 그런데 올해 6월 27일 행정안전부가 개최한 제1차 공청회에서 제시된 법안설명에서는 행정안전부장관이 개인정보보호법의 집행 및 감독책임을 지는 주무부처이고 그 소속 하에 분쟁조정기능만을 주된 업무로 하는 개인정보분쟁조정위원회를 두도록 하고 있었다.⁶⁷¹⁾ 이에 대해 진보넷 등의 시민단체와 일부 논자들은 법안이 개인정보감독기구의 독립성을 포기한 것이라고 비판하였다. 비판 의견을 수렴한 행정안전부는 8월 12일 『개인정보보호법 제정법률안』을 정식으로 입법예고하고 8월 28일 제2차 공청회를 열었다. 이 입법예고된 법률안에 의하면, 여전히 행정안전부장관이 집행 및 감독책임

671) 행정안전부, 『『개인정보보호법』 제정을 위한 공청회 자료집』, 2008. 6. 27 참조.

을 지는 주무부처이고 개인정보분쟁조정위원회가 분쟁조정기능을 수행하되, 몇 가지 사항에 대해 심의기능을 하는 개인정보보호위원회를 신설하여 국무총리 소속 하에 두는 것으로 하고 있다. 이 법안의 개인정보보호위원회를 개인정보감독기구라고 볼 수 있는지, 그리고 법안상의 집행 및 감독체계를 독립된 감독체계라고 볼 수 있는지가 문제되고 있다.

이하에서는 우선 개인정보감독기구가 왜 독립성을 확보해야 하는지, 그리고 감독기구의 기능을 어떻게 이해해야 하는지를 비교적 관점에서 세계의 감독기구들을 참조하여 논술하고자 한다. 그리하여 향후의 입법과정에서 개인정보감독기구의 설립방향을 모색하는 데 참고자료로 삼고자 한다.

제 2 절 독립된 개인정보감독기구의 존재이유

개인정보보호를 위한 훌륭한 법제가 잘 정비되어 있고 개인의 권리를 충분히 법적으로 보장하고 있다고 하더라도 그 법제운용이 미숙하거나 권리실현이 사실상 불가능 내지는 어렵게 되어 있는 경우 개인정보보호의 이념은 충분히 실현될 수 없다. 자기정보에 대한 열람청구권과 갱신청구권 등 개인정보자기결정권을 법률에서 구체화하고 있다고 하더라도 그 실현을 위한 이니셔티브는 각 정보주체에게 있기 때문에 언제나 일정한 한계를 지닐 수밖에 없다.⁶⁷²⁾ 개인정보보호를 위한 독립된 감독기구가 왜 필요한지 그 이유를 상설하면 다음과 같다.

첫째, 개인정보보호와 관련한 문제의 심각성은 당해 정보주체가 인식하지도 못한 상태에서 개인정보가 정부나 기업에 의해 광범위하게

672) 김일환 교수도 “오늘날 새로운 기술들의 발전 및 적용가능성이라는 점에서 볼 때 ... 더 이상 개인 스스로 자신의 정보를 보호하고 통제할 수 없다”고 지적하면서, “시민을 효율적으로 보호하기 위해서는 국가나 사회의 정보처리를 통제하는 통제기관의 설치 및 활동이 절대적으로 요구된다.”고 역설하고 있다. 김일환, □□개인정보보호법제의 정비방안에 관한 연구□□(한국법제연구원, 1997), 195면.

수집·축적·처리·제3자 제공 내지 공유된다는 사실에 있다. 이러한 현실에서 정보주체인 개인에게 주어지는 자기정보통제권은 그 실효성이 극히 미약할 수밖에 없다. 자신의 개인정보에 대한 침해사실을 인식조차 하지 못하는 정보주체가 권리구제절차를 밟을 수 있는 가능성이 없기 때문이다.

둘째, 설령 개인정보처리의 원칙 중 수집제한의 원칙과 시스템공개 원칙이 잘 지켜져 개인정보의 수집과 처리에 대한 정보주체의 인식이 있다 하더라도, 처리기관 내부에서 이루어지는 위법적인 상황을 외부자인 정보주체가 충분히 파악할 수 없을 뿐만 아니라 조사할 수도 없다. 기술적으로 복잡한 처리과정이나 은밀하게 이루어지는 목적외 이용 및 제3자 제공에 관한 상황을 외부의 비전문가인 정보주체가 제대로 알 수 없기 때문이다.

셋째, 더 나아가 설령 그것을 정보주체가 충분히 파악했다고 하더라도, 자신의 노력과 주도 하에 법원을 통한 그 복잡하고 장기적인 소송절차를 밟아서 권리구제를 받는다는 것은 결코 손쉬운 일이 아니다. 또한 법원을 통한 권리구제는 언제나 사후적인 것이다. 개인정보 보호에 있어서는 예방적인 권리구제가 더욱 절실히 요청된다.

넷째, 통상 개인정보DB에 의한 개인정보처리는 특정 개인이 아니라 수많은 개인들을 대상으로 하는 것이기 때문에 위법적인 개인정보처리의 영향은 그들 모두에게 똑 같이 미칠 수 있다. 즉 위법한 개인정보처리에 따르는 피해는 대규모적이고 집단적인 성격을 지닌다.

다섯째, 개인정보감독기구는 그 기능이 독립적으로 이루어져야 한다. 개인정보보호의 가치는 개인정보처리를 통해 얻어지는 효율성의 가치와 본질적으로 양립하기 어렵다. 이 양 가치는 서로 상반된 관계에 있기 때문이다. 따라서 이 상반된 가치들을 단일의 특정기관이 함께 추구한다는 것은 사실상 불가능한 일이다. 어느 한 쪽으로 균형이 기울어질 수밖에 없다.

요컨대, 정부나 기업에 의한 위법한 개인정보처리로부터 정보주체의 개인정보자기결정권을 실질적으로 보장하기 위해서는 예방적이고 사전적인 차원에서 개인정보처리를 감시·감독하며, 또 피해가 발생한 경우 법원의 소송절차 외에 보다 효과적이고 효율적인 권리구제를 실질적으로 가능하게 해주는 독립된 개인정보감독기구의 존재가 필수적이다. 아래에서 살펴는 바와 같이 독립된 개인정보감독기구의 설립은 국제규범이 요구하는 바이다.

제 3 절 개인정보감독기구의 기능과 권한

세계 각국의 개인정보감독기구는 7가지의 서로 연관된 역할과 기능을 수행하고 있는 것으로 분석된다. ① 옴부즈맨(ombudsmen)으로서, ② 감사관(auditor)으로서, ③ 자문역(consultant)으로서, ④ 교육자(educator)로서, ⑤ 교섭자(negotiator)로서, ⑥ 정책조언자(policy adviser)로서, 그리고 ⑦ 집행자(enforcer)로서의 역할과 기능이 그것이다.

물론 모든 감독기구가 이 모든 역할을 동일한 비중을 가지고 수행하는 것은 아니다. 또한 이들 기능이 개인정보감독기구에 의해서만 배타적으로 수행되는 것도 아니다. 일부 국가에서는 다른 정부부처도 개인정보보호에 있어서 중요한 책임을 떠맡기도 한다. 이하에서는 이들 기능에 대하여 구체적으로 살펴본다.⁶⁷³⁾

1. 옴부즈맨(ombudsmen)으로서의 민원해결기능

우선 모든 개인정보감독기구들은 정보주체로부터의 불만이나 민원(claims)을 접수받고, 사실관계를 조사하며, 그리고 그 민원사항을 해결하는 기능을 수행한다. 이러한 “민원의 접수·조사·해결”이라고

673) 이들 기능에 대한 설명은 Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*(Ashgate, 2003), pp. 109-114에서 크게 참조함.

하는 옴부즈맨의 전통적인 기능은 모든 개인정보보호체계의 효율적인 감독기능에 있어서 가장 핵심적인 것이다. 물론 그것은 시간을 소요하고 상당한 자원을 필요로 하는 일이다.

이러한 민원처리시스템을 구축함에 있어서는 그 기능이 원활히 수행되기 위해서 어떤 권한들이 감독기구에 주어져야 할 것인지에 대해서 면밀한 검토가 필요하다. 국가마다 다양성이 있긴 하지만, 대체로 이들 권한으로는 i) 개인정보처리기관의 구내에 출입하는 권한, ii) 개인정보처리과정에서 산출된 관련 기록을 요구할 수 있는 권한, 그리고 iii) 개인정보처리에 책임이 있는 자를 소환할 수 있는 권한을 들 수 있다. 이와 관련해서 한 가지 어려운 문제는, 정보주체에 의한 민원신청이 없더라도 감독기구가 독자적으로 범위반사실을 조사할 수 있는 권한을 행사할 수 있을 것인가 하는 문제이다. 일부 국가에서는 감독기구의 직권에 의한 조사권한을 부여하고 있다.

한편, 민원해결의 방식은 매우 다양한 형태를 가질 수 있는데, 예컨대 영국에서와 같이 구속력 있는 집행명령(binding enforcement order)의 형태에서부터 캐나다, 뉴질랜드, 호주와 같이 구속력이 약한 권고(less mandatory recommendations)에 이르기까지 다양하다. 화해(conciliation)와 조정(mediation)에 의존하는 감독기구들은 개인정보처리기관이 일반인에게 나쁜 이미지를 심어주지 않기 위해서 민원제기에 대해 적극적으로 화해를 하려고 하는 경향에 의존하게 되는데, 감독기구로서는 그러한 경향을 적극 활용하여야 한다.

2. 감사관(auditor)으로서의 감사기능

민원의 조사와 해결은 그 본질이 수동적이고 소극적인 과정이다. 그러나 개인정보감독기구는 여러 정보에 근거해서 특정 개인정보처리기관의 처리행태에 대해 의심을 가질 수 있으며, 따라서 그 기관이나

특정 기술에 대하여 보다 일반적인 감사를 실시할 수 있다. 감사(audits)는 보다 체계적일 뿐만 아니라 구체적인 민원제기에 따른 조사에 비하면 덜 대립적이다.

독일의 연방정보보호청은 그 설립 초기부터 개인정보처리시스템에 대한 감사를 실시해 오고 있다.⁶⁷⁴⁾ 독일의 감독기구들은 한 개인정보처리기관 내에서 이루어지는 개인정보처리의 모든 측면에 대한 조사 기법을 발전시켜 왔다.⁶⁷⁵⁾

감사는 그것을 얼마나 자주 행하느냐 그리고 얼마나 엄격하느냐에 따라 다양한 유형을 지닌다. 캐나다와 같은 국가에서는, 감사프로그램(an audit programme)은 비록 연방프라이버시법(Privacy Act)에서 그것을 명문화하고 있지는 않았지만 처음부터 연방프라이버시보호청의 상시적인 업무의 하나가 되어 왔다. 그 밖에 캐나다의 주 차원에서는 보다 비공식적인 현장방문(site visit)이 행하여질 수 있다. 예컨대, 캐나다의 British Columbia주의 개인정보보호청장이었던 David Flaherty는 보호청장 당시 당해 주의 대규모 공공기관에 대하여 비공식적이고 부담을 주지 않는 형태의 현장방문을 촉구하기도 하였다고 한다.⁶⁷⁶⁾

한편, 일부 국가의 보호법은 명시적으로 감독기구에게 감사기능을 부여하고 있다. 예컨대, 캐나다 연방 차원의 민간부문 개인정보보호법인「개인정보보호 및 전자문서법」(Personal Information Protection and Electronic Documents Act)은 감사기능이 주의 개인정보보호청이나 회계법인 또는 표준인증기구에게 위임될 수 있음을 예정하고 있다. 또한 네덜란드의 개인정보보호청장은 일정한 경우에는 공인된 감사기관에 의해서 감사가 실시되도록 요구하고 있다.

674) David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*(1989), p. 77.

675) Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*(Cornell University Press, 1992), p. 182.

676) David H. Flaherty, "How to Do a Privacy and Freedom of Information Act Site Visit" <<http://www.oipcbc.org/>> 참조.

3. 자문역(consultant)으로서 자문기능

각 국의 모든 개인정보감독기구들은 각 개별 개인정보처리기관에게 어떻게 하면 개인정보보호법을 준수할 수 있는지에 관하여 언제나 조언과 자문을 행한다. 개인정보보호법의 이행은 법적 권한의 준부를 떠나서 개인정보감독기구가 얼마나 자문기능을 충실히 수행하느냐에 달려 있다고 해도 과언이 아니다. 사후에 강제력을 발동하기보다는 사전에 개인정보보호시스템을 갖추도록 장려하고 조언하는 것이 무엇보다 중요하다. 자문과 조언은 규제자와 피규제자라는 대립적 관계보다 훨씬 더 나은 것으로 간주되고 있는데, 대립적인 관계는 많은 비용을 요하고 비효율적일 수 있기 때문이다.

특히 프라이버시 침해적인 새로운 기술이나 시스템을 도입하는 경우에 개인정보감독기구의 자문역할과 기능은 매우 중요한 의미를 지닌다. 통상 개인정보처리기관들은 도입을 계획하고 있는 시스템이 개인정보보호법을 준수하게 되는지 여부를 미리 알고자 한다. 이러한 자문기능은 흔히 공식적인 절차 밖에서 이루어지는 경향이 있는데, 이 때 감독기구는 나중에 당해 처리기관에 대한 민원이 제기되지 않도록 그 자문과 조언을 그 독립성이 훼손되지 않는 선에서 신중하고 공정하게 할 수 있도록 조심해야 할 것이다.

4. 교육자(educator)로서의 교육기능

개별적인 자문기능 외에, 개인정보감독기구는 보다 광범위한 교육 및 연구기능을 수행한다. 보다 큰 차원에서 감시의 문제와 프라이버시 문제를 분석·연구하고 또 개인정보처리기관과 정보주체들을 계속해서 교육시키며 정부와 사회 전반에 걸쳐 프라이버시 보호 문화를 촉진시키는 것은 매우 중요한 기능이다. 세계의 모든 감독기구는 이

러한 기능을 부여받고 있으며, 다만 그 활동범위와 강도에 있어서 다양한 차이를 보이고 있다.

비록 한정된 자원이긴 하지만, 개인정보감독기구는 개인정보보호의 이념과 보호원칙들을 이해시키고 프라이버시보호문화를 신장하는 데 주력할 필요가 있다. 세계적으로도 각국의 감독기구들은 이러한 기능과 관련해서 흥미 있는 사례들을 보여주고 있다.

예컨대, 캐나다의 연방프라이버시보호청(Office of the Privacy Commissioner of Canada)은 민간부문의 일반법인 『개인정보보호 및 전자문서법』의 내용을 일반인에게 정확히 그리고 널리 알리기 위해 “기업과 단체를 위한 지침”(Guide for Businesses and Organizations)을 공표하고 있다.⁶⁷⁷⁾ 이 지침은 법률의 이행을 확보하기 위하여 법률의 규율범위, 공정정보처리의 원칙들, 권리구제절차 등을 알기 쉬운 언어로 풀어서 상세하게 설명하고 있다. 그 밖에도 캐나다의 연방프라이버시보호청은 기업들이 어떻게 하면 이 법률을 준수할 수 있는지를 돕기 위하여 여러 가지 정보들을 제공하고 있다.⁶⁷⁸⁾ 한편, 캐나다 Ontario주의 감독기구인 『정보 및 프라이버시보호청』은 개인정보보호원칙의 준수 여부에 대한 자가진단과 자체평가를 돕기 위하여 “프라이버시 진단 툴”(Privacy Diagnostic Tool)을 주요 회계법인들과 공동으로 개발하여 공표해 놓고 있다.⁶⁷⁹⁾

그 밖에도 각국의 감독기구들은 이처럼 법준수를 위한 자가진단프로그램을 개발하는 데 상당한 노력을 하고 있다. 예컨대, 홍콩의 프라이버시보호청(PCO: Office of Privacy Commissioner for Personal Data)은 2000년에 공공부문과 민간부문의 개인정보처리기관들이 개인정보보호법(Personal Data [Privacy] Ordinance)의 준수 여부에 대한 자체평가를 돕기 위하여 “Privacy.SAFE: Guidance Notes for Self-Assessment”를 개

677) 이 지침의 내용은 <http://www.privcom.gc.ca/information/guide_e.asp> 참조.

678) 이들 정보자원들은 <http://www.privcom.gc.ca/ekit/ekit_e.asp>에서 확인할 수 있다.

679) “프라이버시 진단 툴”의 내용은 <http://www.privcom.gc.ca/ekit/ct_01_e.asp> 참조

발하여 공표하였다.

이처럼 각국의 감독기구들은 특별한 영역이나 기술 분야에 있어서의 프라이버시 쟁점들을 조사하고 그 해결방안을 연구하며 때때로 여론조사를 수행하기도 한다. 그 연구결과물인 각종의 보고서들은 새로운 기술에 내재된 프라이버시위험을 정부나 기업 그리고 일반인에게 경고하는 매우 유용한 수단으로 활용되고 있다.

5. 정책조언자(policy adviser)로서의 조언기능

각국의 개인정보보호법은 대부분 개인정보감독기구에게 새로운 입법안이 프라이버시보호에 어떤 의미를 지니는지, 그리고 새로 도입되는 자동개인기록시스템이 어떤 영향을 미칠 것인지에 대하여 논평이나 조언을 하는 책무를 부여하고 있다. 예컨대, 캐나다의 공공부문 보호법인 「프라이버시법」(Privacy Act)은 연방프라이버시보호청에게 그 관할 범위 내에서 특정 쟁점에 관하여 의회에게 특별보고를 할 수 있는 권한을 부여하고 있다.⁶⁸⁰⁾

많은 나라에서 그러하지만, 예컨대 캐나다의 경우 연방프라이버시보호청은 인구조사과정(census process)에서 항상 연방정부와 충돌과 갈등을 빚고 있다.⁶⁸¹⁾ 한편, 영국의 경우 정보보호청장은 정부의 공공서비스 확대와 사기방지를 위한 광범위한 정보공유(data-sharing)를 계획하는 정부안에 대하여 그것이 가지는 프라이버시 영향에 관하여 정책적 조언을 한 바 있다.⁶⁸²⁾ 그리고 일부 국가에서는 새로운 기술이 도입될 때마다 “프라이버시영향평가서”(privacy impact statement)를 작성

680) Privacy Act, Sec. 39(1).

681) Canada, Office of the Privacy Commissioner(OPC), *Annual Report 1999-2000*(Minister of Public Works and Government Services Canada, Ottawa, 2000), pp. 49-52 참조.

682) United Kingdom, Performance and Innovation Unit, Cabinet Office, *Privacy and Data-Sharing: The Way Forward for Public Services*(Cabinet Office, 2002) 참조.

<<http://www.number-10.gov.uk/su/privacy/downloads/piu-data.pdf>>

하도록 요구된다.⁶⁸³⁾

또한 각국의 감독기구들은 의회의 청문절차에서 흔히 관련 쟁점에 관해 증언을 하기도 하고, 정부의 정책에 대응해서 반대 입장을 공식적으로 표명하기도 한다. 후자의 잘 알려진 사례로서는 1995년에 영국의 내무부(Home Office)가 추진하려고 했던 신분카드제에 대해 당시의 감독기구였던 정보등록청(UK Registrar: 지금의 Information Commissioner의 전신)이 깊은 우려를 표명한 사례를 들 수 있다. 당시 정보등록청은 내무부의 사실조사와는 별도로 신분카드제에 대한 국민의 태도를 자체 조사하여 그 결과를 공표하였다.

6. 자율규제의 조정자(negotiator)로서의 유도기능

일부 국가의 개인정보감독기구는 민간기관의 자율규제규범인 실무규약(privacy code of practice)에 대하여 협상하는 책무를 명시적으로 부여받고 있다.

자율규제규범으로서의 실무규약은 비록 국가법인 개인정보보호법이 존재하더라도 그 자체 뚜렷한 장점을 가지고 있다. 이 실무규약을 협상하는 과정에서 여러 상이한 부문과 영역에서 독특하게 안고 있는 프라이버시 문제에 대하여 상호 이해를 증진시킬 수 있다. 실무규약은 매우 유연한 규범이며 경제상황과 기술발전의 변화에 쉽게 적응해 나갈 수 있다. 실무규약은 또한 개인정보처리기관들이 자신들의 개인정보보호정책(privacy policy)을 공표하게 함으로써 부당한 개인정보처리행태에 관한 의심을 제거할 수 있게 하여 준다. 요컨대, 실무규약은 감독기구와 개인정보처리기관 상호간의 이해를 증진시키는 데 크게

683) 미국과 캐나다의 프라이버시영향평가제도에 관해서는 구병문, “프라이버시 영향평가 제도의 국내법적 도입방안 - 공공부문을 중심으로 -”, 『제3차 개인정보보호 정책 포럼』 (정부혁신지방분권위원회, 2004. 6. 16), 38-46면; 이규정·구병문, 『공공부문 프라이버시 영향평가제도』 (한국전산원, 2003) 참조.

기여할 수 있다.

그러나 자율규제규범인 실무규약과 국가법인 개인정보보호법의 관계와 관련해서 아주 어려운 문제가 있다. 실무규약을 활용하거나 장려해 온 국가들의 사례를 분석해 보면 거기에는 미묘한 차이를 지닌 3가지 모델을 발견할 수 있다.

첫째, 가장 엄격한 모델로서, 뉴질랜드의 『프라이버시법』(Privacy Act)이 채택하고 있는 방식이다.⁶⁸⁴⁾ 뉴질랜드 방식의 핵심 포인트는 『프라이버시법』에 따라 협의하여 결정된 실무규약은 법적 구속력(force of law)을 가진다는 점이다. 따라서 승인된 실무규약을 위반하는 것은 프라이버시법에서 명시한 개인정보보호원칙을 위반하는 것과 동일하고, 그 결과 법이 정한 민원처리절차 및 집행절차가 작동하게 된다.

두 번째 모델은 다소 유연한 방식으로서 네덜란드의 방식을 들 수 있다. 네덜란드 방식은 많은 점에서 뉴질랜드와 비슷하고 또 실무규약에 대한 신중한 협상과정을 담고 있긴 하지만, 종국적으로 그 실무규약은 법원에 대하여 정식의 구속력을 가지지 않는다. 물론 만일 특정의 개인정보처리기관이 그 실무규약이 요구하는 사항들을 준수하였음을 입증할 수 있다면, 그것은 상당한 설득력을 가질 수 있을 것이다. 그러나 역으로, 실무규약의 규정을 위반하였다는 원고의 입증이 있다면, 그것은 개인정보보호법에 따른 책임을 근거지우는 일응의 증거(prima facie evidence)가 된다. 그러므로 실무규약은 직접적인 것은 아니지만 간접적인 법적 효과를 갖는다.

세 번째 모델은 영국과 캐나다가 취하는 방식으로서, 개인정보보호법이 단순히 감독기구에게 실무규약의 제정을 촉구하는 권한을 주고 있는 모델이다. 이 모델에 있어서 실무규약은 간접적인 법적 효과마저도 갖지 않는다. 사실 이 세 번째 모델은 유럽연합의 개인정보보호 지침(Directive 95/46/EC) 제27조가 예정하고 있는 바이다.

684) New Zealand Privacy Act 1993, Secs. 46-53.

포괄적인 개인정보보호법을 가지고 있는 입법체계에 있어서 이 자율규제규범인 실무규약의 활용에는 중요한 딜레마가 놓여 있는 것으로 보인다. 만일 감독기구가 실무규약을 정식으로 승인하지 않는다면, 그 실무규약에는 개인정보보호법의 내용과 상충하는 내용이 담길 수 있고 그렇게 되면 법의 적용과 집행에 있어서 혼란이 야기될 수도 있다. 그러나 한편으로, 만일 뉴질랜드와 네덜란드와 같이 보다 정식의 승인절차가 있는 경우에는, 그것은 본래 자율규제의 유연성을 인정하고자 의도된 실무규약의 제정을 관료화하는 결과가 초래될 수 있다.

7. 집행자(enforcer)로서의 집행기능

개인정보감독기구의 기능과 권한 중에 개인정보보호원칙의 이행을 직접 명령할 수 있는 권한을 부여할 것인가 하는 점이 중요한 문제가 된다. 이 집행권한은 개인정보처리기관의 행위를 변경하도록 직접 명령하는 것으로서, 조사 및 권고기능과는 구별된다.

논자에 따라서는 집행자로서의 기능보다는 권고적 기능에 더 중점을 두어야 한다는 주장이 있다. 그리고 만일 개인정보처리기관이 개인정보보호에 충실하지 못한 행태를 보이는 경우 그 사실을 일반인에게 공표하는 것만으로도 매우 효과적인 제재가 될 수 있다고 주장한다.

그러나 한편으로, 다른 논자들은 설령 집행권한이 드물게 행사되더라도 그 권한의 존재 자체가 개인정보처리기관의 법 준수를 이끌어내는 효과적인 기능을 수행한다고 주장한다. 더구나 개인정보처리기관인 공공기관과 민간기관은 개인정보보호원칙을 적용함에 있어서 확실성과 일관성을 유지할 필요가 있다. 정식의 집행권한을 행사하는 절차는 시간이 흐름에 따라 법의 적용에 있어서 매우 높은 수준의 일관성과 투명성, 그리고 책임성을 보장해 줄 수 있을 것이다. 그리하여 시간이 흐름에 따라 법이 준수되는 비율을 높일 수 있을 것이다.

대부분 국가들의 개인정보보호법에서는 종국적인 권리구제는 법원에서 이루어지도록 하고 있고, 감독기구에 의한 민원해결절차에 대해서는 법원에서 재심사할 수 있도록 하고 있다. 한편, 일부 국가에서는 비교적 전문적이고 기술적인 분쟁을 다루기에는 법원이 반드시 가장 적합한 기관은 아니라는 판단 하에, 준사법적 기능(quasi-judicial function)을 수행하는 전문가집단으로 구성되는 소규모의 심판원(tribunal)을 설립하고 있다. 예컨대, 영국은 1998년의 개인정보보호법(Data Protection Act)에서 정보보호심판원(Data Protection Tribunal)을 설립하고, 정보보호청장(Information Commissioner)의 결정에 불복하고자 하는 개인이나 개인정보처리기관이 정보보호심판원에 불복신청을 할 수 있도록 하고 있다. 이 심판원은 필요하다면 전문가패널로 구성되기도 한다.

제 2 장 개인정보감독기구의 비교법적 고찰

제 1 절 비교법적 개관

오늘날 독립된 개인정보감독기구의 설립은 개인정보보호에 관한 각종 국제규범에서 지속적으로 요구하고 있는 필수적인 요소이다. 국제연합(UN)의 개인정보보호가이드라인(1990년), 유럽연합의 개인정보보호지침(1995년), OECD 각료선언(1998년), 유럽평의회의 개인정보보호협약 추가의정서(2001년)는 모두 개인정보처리의 기본원칙의 이행과 준수 여부를 감독할 독립된 기구의 설립을 요구하고 있다.

이러한 상황에서 세계 각국은 공공부문과 민간부문을 통합하여 감독하는 단일의 개인정보감독기구를 설립하는 추세를 보이고 있다. 이 추세는 비단 유럽연합이나 유럽평의회 회원국에 한정되는 것이 아니고, 비회원국들도 새로운 개인정보보호법을 제정하면서 독립된 통합감독기구를 설립하고 있음을 볼 수 있다.

1. 국제규범상의 설립 요구

(1) 국제연합(UN)의 개인정보보호가이드라인 : 독립된 보호기구의 설치 요구

국제연합은 1990. 12. 14. 총회결의로 「컴퓨터화 된 개인정보파일의 규율에 관한 가이드라인」(Guidelines for the Regulation of Computerized Personal Data Files)⁶⁸⁵을 채택·공포하였다.

이 가이드라인은 모두 10개의 개인정보보호원칙을 담고 있는데, 그 중 8번째 원칙(감독과 제재)에서 개인정보보호원칙을 감독할 독립된 기관의 설치를 요구하고 있다.

685) Marc Rotenberg, *The Privacy Law Sourcebook* 1999(EPIC, 1999), pp. 215-218.

⑧ 감독과 제재(supervision and sanctions) : 위에 열거된 원칙의 준수여부를 감독할 독립된 기관을 설치하여야 하고, 이들 원칙이 위배된 경우에 적용할 수 있는 처벌규정 및 개인정보보호규정을 제정하여야 한다.

(2) 유럽연합의 개인정보보호지침 : 독립적인 감독기구의 의무화

유럽연합(EU)은 개인정보보호 일반법인 1995년의 개인정보보호지침(Directive 95/46/EC)에서 회원국으로 하여금 개인정보의 수집·관리·이용활동 등을 모니터하고 조사할 수 있는 권한을 가진 독립적인 기구를 설치하도록 의무화하고 있다. 동 지침 제28조(감독기구) 제1항은 “각 회원국은 하나 이상의 공공기관(public authorities)이 본 지침에 따라 제정된 국내보호입법의 자국내 집행을 감시하는(monitoring) 책임을 갖도록 하여야 한다. 이 감독기구는 그 기능을 수행함에 있어서 완전히 독립적으로(with complete independence) 행동하여야 한다.”고 규정하고 있다. 여기서 “완전한 독립성”은 기능적인 독립성을 의미하는데, 감독기구의 의사결정이나 조치에 대하여 외부에서 어떠한 영향력도 행사할 수 없다는 것을 의미한다.⁶⁸⁶⁾

(3) 1998년의 OECD 각료선언 : 효과적인 집행메커니즘의 확보요구

1998년 10월 캐나다에서 열린 OECD 각료회의에서는 1980년의 가이드라인에서 제시되었던 8개 원칙을 재확인하는 ‘범세계 네트워크상의 개인정보보호를 위한 각료선언’(Ministerial Declaration on the Protection of Privacy on Global Networks)⁶⁸⁷⁾을 채택하고, 회원국의 정부에 대하여 온라인 환경에서 신뢰를 구축하고 데이터의 자유로운 국제적 유통을 촉진하기 위해 범세계적 네트워크에서의 개인정보보호에 관한 관

686) Dammann, U./Simitis, S., EG-Datenschutzrichtlinie, Kommentar, Art. 28 Rn. 6, Baden-Baden, 1997.

687) <<http://www.oecd.org/dataoecd/39/13/1840065.pdf>>

심을 새롭게 가져 줄 것을 촉구하고 있다. 이 각료선언은 1980년의 가이드라인이 효과적으로 시행되는 것을 보장하기 위하여 필요한 조치로서 6개 사항을 선언하고 있는데, 그 중의 하나가 “효과적인 집행 메커니즘의 확보”이다.

O 개인정보보호원칙과 개인정보보호정책의 불이행에 대처하고 동시에 권리구제를 보장하기 위하여 효과적인 집행메커니즘(effective enforcement mechanisms)이 작동할 수 있도록 보장한다.

(4) 유럽평의회 의 개인정보보호협약 추가의정서 : 독립적인 감독 기구의 의무화

유럽평의회 개인정보보호협약의 2001년 추가의정서는 그 전문(Preamble)에서 효율적인 개인정보보호를 위한 한 요소로서 완전히 독립적인 기능(functions in complete independence)을 수행하는 감독기구(supervisory authorities)가 필요함을 인정하고 있다. 그에 따라 제1조는 감독기구의 제목 하에 다음과 같은 내용을 규정하고 있다.

제 1 조 감독기구 (Supervisory authorities)

1. 각 가입국은 본 협약 제2장 및 제3장, 그리고 본 의정서에서 규정된 원칙들을 구현하는 국내법상의 조치들을 준수하도록 하기 위하여 그에 대한 책임을 지는 한 개 또는 그 이상의 감독기구를 마련하여야 한다.
2. a. 이 목적을 위해서, 감독기구는 특히 조사권한(powers of investigation)과 개입권한(powers of intervention)을 가져야 할 뿐만 아니라 위 제1항에서 언급된 원칙들을 구현하는 국내법규정의 위반에 대하여 권한 있는 사법기관에 제소할 수 있는 권한(power to engage in legal proceedings)을 가져야 한다.
b. 각 감독기구는 그의 관할범위 내에서 개인정보의 처리와 관련한 개인의 권리와 기본적 자유를 보호하기 위하여 그 개인이 제기한 민원을 심사하여야 한다.
3. 감독기구는 완전히 독립하여(in complete independence) 그 기능을 수행하여야 한다.

- | |
|--|
| 4. 감독기구의 결정에 대하여 불만이 있는 경우 법원을 통해 다룰 수 있다. |
| 5. 본 협약 제4장의 규정에 따라, 그리고 협약 제13조의 규정취지를 손상함이 없이, 감독기구들은 임무수행에 필요한 범위 내에서 특히 모든 유용한 정보를 교환하는 등 서로 협력하여야 한다. |

2. 독립된 감독기구 설립의 세계적 추세

세계 각국은 유럽연합 개인정보보호지침(95/46/EC)의 주도적인 영향 하에서 공공부문과 민간부문을 통합하여 감독하는 단일의 개인정보감독기구를 설립하는 추세를 보이고 있다. 이 추세는 비단 유럽연합이나 유럽평의회 회원국에 한정되는 것이 아니고 비회원국들도 새로운 개인정보보호법을 제정하면서 독립된 통합감독기구를 설립하고 있음을 볼 수 있다. 그 경향을 정리하면 아래 표와 같다.⁶⁸⁸⁾

[표 5-2-1] 유럽평의회 회원국의 감독기구 현황

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
오스트리아	Büro der Daten-schutz-kommission	www.dsk.gov.at	룩셈부르크	Commission nationale de la protection des données	www.cnpd.lu
벨기에	Commission de la Protection de la vie privée	www.privacy.fgov.be	네덜란드	College Bescherming Persoonsgegevens	www.dutchdpa.nl
불가리아	Personal Data Protection Commission	www.cdpd.bg	노르웨이	Datatylsinet	www.datatilsynet.no
크로아티아	Personal Data Protection Agency	www.azop.hr	폴란드	Bureau of Inspector General for Personal Data Protection	www.giodo.gov.pl
키프로스	Office of Personal Data Protection Commissioner	www.dataprotection.gov.cy	포르투갈	Comissão Nacional de Protecção de Dados	www.cnpd.pt

688) 이 표의 내용은 유럽평의회(Council of Europe) 홈페이지에 게시된 내용을 정리함<www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/Supervisory_authorities>

제 2 장 개인정보감독기구의 비교법적 고찰

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
체코 공화국	Office for Personal Data Protection	www.uouu.cz	루마 니아	National Supervisory Authority for Personal Data Processing	www.dataprotection.ro
덴마크	Datatilsynet	www.datatilsynet.dk	슬로바 키아	Commissioner For Personal Data Protection	www.dataprotection.gov.sk
핀란드	Office of Data Protection Ombudsman	www.tietosuoja.fi	슬로베 니아	Information Commissioner	www.ip-rs.si
프랑스	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr	스페인	Agencia Española de Protección de Datos	www.agpd.es
독일	Bundesbeauftragte für den Datenschutz	www.datenschutzhutz.de	스웨덴	Datainspektionen	www.datainspektionen.se
그리스	Data Protection Commission	www.dpa.gr	스위스	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter	www.edoeb.admin.ch
헝가리	Data Protection Commissioner	www.obh.hu	영국	Office of the Information Commissioner	www.ico.gov.uk
아이 슬란드	Persónuvernd (Data Processing Authority)	www.personuvernd.is	이탈 리아	Garante per la protezione dei dati personali	www.garanteprivacy.it
아일 랜드	Data Protection Commissioner	www.dataprivacy.ie	에스토 니아	Inspection of Data Protection	www.dp.gov.ee

[표 5-2-2] 유럽평의회 비회원국의 감독기구 현황

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
캐나다	Privacy Commissioner	www.privcom.gc.ca	호주	Privacy Commissioner	www.privacy.gov.au
홍콩	Office of the Privacy Commissioner for Personal Data	www.pco.org.hk	모나코	Commission de contrôle des informations nominatives	www.ccin.mc

국가명	개인정보감독기구	홈페이지	국가명	개인정보감독기구	홈페이지
뉴질랜드	Privacy Commissioner	www.privacy.org.nz	태국	Official Information Commission's Office	www.oic.thaigov.go.th

3. 소 결

개인정보보호를 위한 독립된 감독기구가 필요하다는 인식은 개인정보보호 분야에서 세계적 권위를 자랑하는 뛰어난 분석가들에 의해서도 확인되고 있다.

캐나다의 Colin J. Bennett 교수(University of Victoria)와 영국의 Charles D. Raab 교수(University of Edinburgh)는 이렇게 분석하고 있다. “강력한 감독기구의 존재는 훌륭한 프라이버시 보호체계의 필수조건(sine qua non)으로 간주되어 오고 있다.

왜냐하면 법이란 스스로 집행되는 것이 아니고, 또 프라이버시 문화는 권위 있는 옹호자가 없이는 그 스스로 확립될 수 없기 때문이다.”⁶⁸⁹⁾

또한 일찍이 캐나다의 British Columbia주의 개인정보보호청장이었던 David Flaherty도 “개인정보감독기구는 프라이버시 보호를 위한 일종의 경보체계이다(an alarm system for the protection of privacy).”고 역설하였다.⁶⁹⁰⁾

요컨대, 이제 개인정보보호를 위한 독립된 감독기구의 설립은 더 이상 선택의 문제가 아니다. OECD 회원국으로서, 그리고 세계 12대 교역국인 우리나라는 국제규범에 충실할 필요가 있으며, 또한 정보기술의 강국으로서 21세기 인간존엄이 보장되는 고도정보사회로의 기반을

689) Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*(Ashgate, 2003), p. 107.

690) David H. Flaherty, *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*(1989), p. 383.

구성하기 위해서는 독립된 개인정보감독기구의 존재가 필수적이라고 하겠다.

제 2 절 감독기구에 관한 입법례

1. 미 국

미국은 독립적인 개인정보보호기관이 존재하지 않는다. 다만 공공부문에서는 예산관리처(OMB)가, 민간부문에서는 연방거래위원회(FTC)가 각각 간접적인 개인정보보호로서의 역할을 담당하고 있다.

예산관리처(Office of Management and Budget; OMB)는 우리나라의 과거 기획예산처⁶⁹¹⁾와 유사한 기능을 수행하는 기관으로, 프라이버시의 보호와 관련하여 예산관리의 차원에서만 제한적인 기능을 담당하고 있다. 연방 프라이버시법에 의하면, 예산관리처의 장은 동법 규정의 시행에 있어서 의견을 표명하고 지침을 제정하며, 기관의 이용을 규제하는 권한을 가지며(§552a(v)(1)), 기관들에 의한 동법의 적용을 지원하고 감독할 권한도 가진다(§552a(v)(2)). 하지만 프라이버시법의 집행은 각 정부기관의 장이 책임지는 것으로 되어 있으며, 부분적으로 OMB가 그 이행에 관한 감독을 담당한다고 할 수 있다.

한편, 연방거래위원회(FTC)는 소비자보호의 일환으로 소비자의 프라이버시를 보호하는 기능도 함께 수행하고 있다. 특히 아동의 온라인 프라이버시, 소비자의 신용정보, 공정거래의 관행에 관한 개인정보보호 관련 법규를 집행하고 준수 여부를 감독한다.

전체적으로 볼 때 미국에 있어서는 프라이버시보호에 관한 포괄적 권한을 가지는 감독기관이 존재하지 않는다고 할 수 있다.⁶⁹²⁾

691) 예산과 재정에 관한 사무를 관장했던 국무총리 산하의 정부기관이었으나, 2008년 2월 정부조직법 개정에 따라 재정경제부와 통합, 기획재정부로 개편되었다.

692) 김일환, 『개인정보보호법제의 정비방안에 관한 연구』(한국법제연구원, 1997), 191면 참조.

2. 캐나다

캐나다는 공공부문을 규율하는 프라이버시법(PA)에서는 감독기구로 프라이버시 감독관(privacy commissioner)을 두고 있고, 민간부문을 규율하는 ‘개인정보보호 및 전자문서에 관한 법률’(PIPEDA)에서는 감독기구로 감독관(Commissioner)을 두고 있다.

(1) 프라이버시법의 감독기구

1) 조 직

캐나다 연방 프라이버시법 제53조에 의해 설립된 연방 프라이버시 감독관(privacy commissioner)은 의회 소속하에 있으면서, 상·하원에 직접 보고한다(제38조 내지 제40조). 공공부문이나 민간부문에서의 개인정보처리에 관한 민원을 다룸에 있어서 어떤 정부부처나 기관의 간섭을 받지 않고 독립적으로 직무를 수행하면서, 예산이나 인사관리 등에 있어 행정부의 지시, 감독으로부터 자유로운 독립된 독립제기관이다(제54조). 연방 프라이버시감독관은 2명의 부감독관과 사무국으로 구성된다. 사무국은 각종 민원처리 및 조사업무를 수행하는 조사상담부, 프라이버시영향평가를 위한 심사 및 개인정보처리 현황에 대한 모니터링을 실시하는 프라이버시 관행심사부, 각종 프라이버시 관련 기술 및 정책연구 홍보 등의 업무를 담당하는 정책홍보부, 민원처리 과정에서 법률자문이나 입법정책에 대한 각종 자문을 담당하는 법무국과 행정사항을 총괄하는 행정지원국으로 구성된다.

2) 기 능

연방 프라이버시감독관의 주요기능은 다음과 같다. 첫째, 피해구제의 기능으로 각종 불만사항이나 신고를 접수하고, 자료제출을 요구하

고 관계인 소환, 현장조사 등을 통한 사실조사를 실시하고, 민원사항에 대한 검토 및 화해유도, 분쟁조정 및 정보주체의 개인정보 접근권 행사 거부시 연방법원에 제소하는 기능을 수행한다. 둘째, 조사감독의 기능으로 프라이버시 침해여부에 대한 직권 실태조사 및 모니터링을 실시하고, 정보보호원칙 및 법규 준수여부를 감독하며, 범위반사항 발견시 시정권고 하는 기능을 담당한다. 셋째, 정보제공의 기능으로 프라이버시 관련 문제에 대한 상담 및 질의접수, 처리, 개인정보 관련 문제에 대한 의견제기를 담당한다. 넷째, 정책 및 입법자문의 기능으로 개인정보관련 법안의 심의 및 의견제시, 정부의 각종 정책에 대한 의견제시 및 자문, 프라이버시 영향평가 심사 및 자문을 담당한다.

(2) PIPEDA의 감독기구

민간부문에서의 개인정보보호를 규율하기 위한 ‘개인정보보호 및 전자문서에 관한 법률’(PIPEDA)에서 피해의 구제를 위하여 정보주체에게 감독관(Commissioner)에 진정할 권리를 부여하고 있다. 이에 따라 감독관은 진정에 대해 조사하여 정보주체에게 통보해주거나 법원에 제소할 권한을 가진다(제11조-제17조).

3. 영 국

(1) ‘정보보호감독관’에서 ‘정보감독관’으로

1984년법의 정보보호등록관(Data Protection Registrar)은 1998년법에서 정보보호감독관(Data Protection Commissioner)으로 명칭이 변경되었다(제6조 제1항⁶⁹³); 부칙5 제1조 제1항). 정보보호감독관은 개인정보를 처리하려는 정보관리자의 신고를 받아 등록하는 업무(제19조) 이외에도 정보관리자의 모범적 업무처리를 장려하는 등의 일반적 임무를 수

693) <<http://www.hmso.gov.uk/acts/acts1998/80029--a.htm#6>>.

행한다(제51조). 또한 그는 매년 본 법령의 집행에 대한 일반보고서를 의회에 제출하여야 하며(제52조), 특수목적의 개인 정보처리에 관한 소송에서 당사자의 요청이 있는 경우 조력하는 임무도 수행한다(제53조). 그리고 1998년 정보보호법 제5장의 법집행절차를 통하여 정보관리자의 법령준수를 담보할 권한을 가진다. 구체적으로 그는 정보관리자의 의무위반에 대한 강제처분의 통지(제40조)와 관리자의 처리의 적절성에 대한 평가를 위한 정보제공의 요구(제43조) 등을 할 수 있다. 나아가 동법의 위반행위에 대한 소송의 제기에도 관여할 권한을 가진다(제60조 제1항). 이러한 정보보호감독관의 지위, 임기, 처우 등에 관해서는 부칙5에서 별도의 규정을 두고 있다.⁶⁹⁴⁾

그러나 종래의 정보보호감독관은 2000년 정보자유법(Freedom of Information Act)에 의하여 정보감독관(Information Commissioner)으로 대체되었다(동법 제18조 제1항⁶⁹⁵⁾; 동법 부칙2 제1조 제1항⁶⁹⁶⁾). 이에 따라 정보감독관은 1998년 정보보호법과 2000년 정보자유법을 집행하고 감독한다. 그는 영국 의회에 직접 보고하는 독립적 감독관청으로서 국내외에 걸쳐 임무를 수행한다.⁶⁹⁷⁾

(2) 정보감독관의 지위

영국의 정보감독관(Information Commissioner)은 독립제의 구조를 가진 독립된 법정기구이다. 감독관의 임명은 여왕이 하고, 임기는 5년으로 두 차례에 걸쳐 재임이 가능하다. 영국의 정보감독관은 행정부의 지시나 감독을 받지 않고 독자적으로 운영되기 때문에 독립성과 자율성이 보장된다.

694) <<http://www.hmso.gov.uk/acts/acts1998/80029--q.htm#sch5>>.

695) <<http://www.hmso.gov.uk/acts/acts2000/00036--d.htm#18>>.

696) <<http://www.hmso.gov.uk/acts/acts2000/00036--w.htm#sch2>>.

697) <<http://www.dataprotection.gov.uk/commissioner.htm>>.

(3) 기 능

정보감독관은 1998년 정보보호법을 집행하고 감독하기 때문에 종전의 정보보호감독관의 권한을 그대로 가진다. 이에 따라 정보감독관은 개인 정보를 처리하려는 정보관리자의 신고를 받아 등록하는 업무(제19조) 이외에도 정보관리자의 모범적 업무처리를 장려하는 등의 일반적 임무를 수행한다(제51조). 또한 감독관은 매년 본 법령의 집행에 대한 일반보고서를 의회에 제출하여야 하며(제52조), 특수목적의 개인 정보처리에 관한 소송에서 당사자의 요청이 있는 경우 조력하는 임무도 수행한다(제53조). 그리고 정보감독관은 1998년 정보보호법 제5장의 법집행절차를 통하여 정보관리자의 법령준수를 담보할 권한을 가진다.

구체적으로 정보감독관은 정보관리자의 의무위반에 대한 강제조치의 통지(제40조)와 그 철회(제41조), 관리자의 처리의 적절성에 대한 평가(제42조)와 그 평가를 위한 정보제공의 요구(제43조) 및 그 평가요청에 대한 응답(제44조), ‘특별한 목적’으로만 정보가 처리되지 않은 경우에 그 효과에 대한 감독관의 결정에 관한 규정(제45조), 특별한 목적으로 정보를 처리하는 경우의 강제조치의 제한에 관한 규정(제46조), 항소권 등(제48조, 제49조), 조사권한(제50조) 등을 할 수 있다. 나아가 동법의 위반행위에 대한 소송의 제기에도 관여할 권한을 가진다(제60조 제1항). 이러한 정보감독관의 지위, 임기, 처우 등에 관해서는 부칙5에서 별도의 규정을 두고 있다.⁶⁹⁸⁾

본법의 목적을 위하여 정보보호심판원(data protection tribunal)을 둔다(제6조 제3항). 정보보호심판원은 원장(검찰총장과의 협의를 거쳐 대법관이 임명), 부원장(대법관이 그 수를 결정하여 임명), 위원(내무장관이 그 수를 정하여 임명)으로 구성되며, 심판원 구성원의 자격으로는 7년 이상의 경력을 갖춘 법관, 변호사 또는 정보주체나 정보관

698) <http://www.hmsso.gov.uk/acts/acts1998/80029--q.htm#sch5>.

리자의 이익대변자일 것이 요구된다(제6조 제4항 내지 제6항).

4. 독일

(1) 연방정보보호관(BfD)에서 연방정보위원(BfDI)으로

연방국가인 독일은 현재 연방 차원의 개인정보보호법인 연방정보보호법 외에도, 주의 차원에서 각자의 개인정보보호법이 마련되어 있고 이를 바탕으로 독자적인 개인정보감독기구들이 설치되어 활동 중이다.

종래 독일의 개인정보보호에 관한 임무를 수행하던 ‘연방정보보호관’(BfD, Bundesbeauftragter für den Datenschutz)은 2006년에 개정된 연방정보보호법에 의해 ‘연방정보위원’(BfDI, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit)이 대신 그 역할을 맡게 되었다. 연방정보위원(BfDI)은 연방의 관청 기타 공공기관 및 통신회사와 우편회사에서의 개인정보 처리를 감독하고, 나아가 신원조사법(Sicherheitsüberprüfungsgesetz)의 적용을 받는 연방과 민간기업을 위한 신원조사를 감독하는 업무를 수행한다.⁶⁹⁹⁾ 또한 동 위원은 2006년 1월 1일부터 발효된 연방정보공개법(Informationsfreiheitsgesetzes des Bundes)에 따른 정보공개에 관한 업무도 함께 관장한다. 한편, 주의 차원에서는 산하 공공기관의 정보처리에 대하여 16개 주의 개인정보보호기구가 설치되어 각자의 임무를 수행하고 있다.

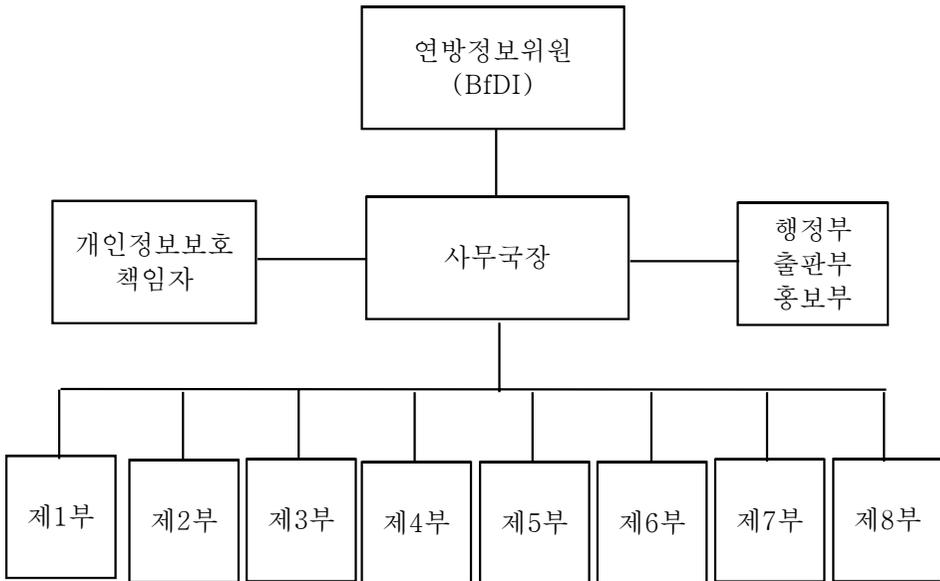
(2) 연방정보위원의 지위

연방정보보호법상 연방정보위원은 연방정부의 제청에 따라 하원(Bundestag)이 재적 과반수의 동의로써 선출하며, 연방대통령에 의하여 임명된다(제22조 제1항). 연방정보위원의 임기는 5년이며, 1회에 한하여 연임할 수 있다(제22조 제3항). 행정조직상으로는 연방내무부(Bundes-

699) <<http://www.datenschutz-berlin.de/content/Deutschland/Bundesbeauftragter>> 참조.

ministerium des Innern) 소속으로 예산이나 인력자원과 같은 행정적 사안에 대해서는 연방내무부장관으로부터 지원을 받는다. 직무를 수행함에 있어서는 독립적이어야 하며, 오직 법률에 따라야 한다. 하지만 연방정부와 연방내무부장관의 감독을 받는다(제22조 제4항). 연방정보위원이 자신의 직무를 일시적으로 수행하지 못할 경우, 연방 내무부 장관은 정보보호위원회와 협의하여 그 직무대리인을 선임할 수 있다(제22조 제6항).

[그림 5-2-1] 독일 연방정보위원회의 조직



(3) 연방정보위원회의 주요 기능

연방정보위원회는 주로 개인정보를 수집 이용 처리하는 연방정부 및 연방공공기관에 대한 규제, 관리, 감독 등의 기능을 수행한다. 즉, 그는 연방 공공기관의 본 법률 규정 및 기타 정보보호규정의 준수 여부를 감독한다(제24조 제1항). 그 밖에 연방 공공기관에 의해 취득된 서신, 우편, 전기통신의 내용과 특수한 사정에 관한 개인정보와 직업상

비밀이나 특수한 직무상 비밀, 특히 세법 제30조에 기초한 조세비밀에 속하는 개인정보에 대해서는 연방정보위원회가 감독할 수 있다(제24조 제2항). 연방법원도 행정적 활동을 하는 한도에서만 연방정보위원회의 감독을 받는다(제24조 제3항). 연방 공공기관은 연방정보위원회와 그 보좌관의 직무수행을 지원하여야 한다(제24조 제4항). 연방정보위원회는 감독의 결과를 공공기관에게 알려야 하고, 정보보호를 개선하기 위하여 특히 개인정보의 처리·사용에서 발견된 부적합성을 시정하기 위하여 감독결과를 제안서에 포함시킬 수 있다(제24조 제5항). 개인관련 정보의 처리·이용에 있어서 연방정보위원회가 동법이나 다른 정보보호의 규정의 위반 혹은 기타의 침해행위를 발견할 때, 그는 연방의 최고관할관청 등에 대해 항의할 수 있고 일정한 기간내에 그 해명을 요구할 수 있다(제25조 제1항). 특히 그 침해행위가 사소하거나 조속히 시정될 경우 그 항의나 관계기관으로부터의 해명을 무시할 수 있다(제25조 제2항). 연방정보위원회는 2년마다 하원에 활동보고서를 제출하여야 한다. 동 보고서는 민간부문에서의 정보보호에 관한 주요 진전사항에 대한 기술을 포함하여야 한다(제26조 제1항). 하원 또는 연방정부가 요청한 경우, 연방정보위원회는 의견서와 보고서를 작성하여야 한다. 하원, 항소위원회, 내무위원회, 연방정부가 요청한 경우, 연방정보위원회도 연방 공공기관에서의 정보보호 및 발생 사실을 조사하여야 한다. 연방정보위원회는 언제든지 하원에 자문을 제공할 수 있다(제26조 제2항).

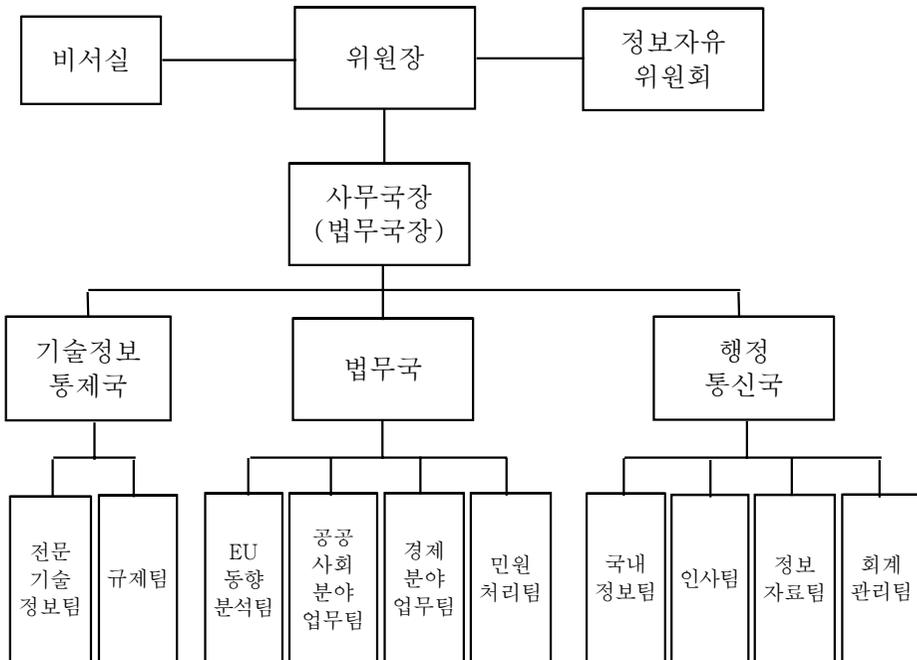
5. 프랑스

정보위원회(Commission nationale de l'informatique et des libertés; CNIL)는 프랑스 내에서 이루어지는 모든 개인정보 처리행위를 규율함으로써, 부당한 개인정보의 처리로 국민들의 개인정보가 침해되는 것을 방지하기 위해 설립된 대표적인 개인정보보호기구이다.

(1) 구 성

프랑스의 정보처리법상 정보위원회는 독립된 행정기관으로 한다(제8조 제1항). 국민의회의원 2명과 상원의원 2명, 경제사회자문위원회(Conseil économique et social) 위원 2명, 국참사원(Conseil d'Etat)의 전·현직 구성원 2명, 대법원(Cour de cassation)의 전·현직 대법관 2명, 감사원(Cour des comptes)의 전·현직 감사위원 2명, 국민의회의장 및 상원의장의 추천에 의해 임명된 정보관련 전문가 2명, 국무회의(Conseil des ministres)의 포고(décret)에 의해 임명된 전문가 3명 등 17명의 위원으로 구성되며, 위원의 임기는 5년이다(제8조 제2항). 이 정보위원회는 자체 내에서 위원장과 2명의 부위원장을 선출하며, 그의 임기는 각각 5년으로 한다(제8조 제3항).

[그림 5-2-2] 프랑스의 정보자유위원회



(2) 기 능

정보위원회는 우선 정보처리법의 규정이 제대로 준수되고 있는가를 감시하는 것을 임무로 한다(제6조).

구체적으로 정보자유위원회는 ① 정보처리 내지 정보의 축적에 관하여 확인하고 조사하는 기능을 수행하는데, 프랑스 안에서 이루어지는 모든 정보처리 및 축적에 대하여 등록 또는 신고접수를 통해 그 현황을 파악하고 이를 바탕으로 정보처리과정을 규제하고 있다. ② 정보관리자가 개인정보보호법규에 적합하게 개인정보를 처리하고 있는지 그 준수여부를 감독하는 기능을 수행한다. ③ 위원회는 정보처리에 관한 기준과 규범을 제시하는 규칙을 제정할 권한을 가진다. ④ 위원회는 정보주체의 접근권 및 정정요구권이 침해되지 않도록 보다 적극적인 역할을 담당하고 있다. ⑤ 위원회는 소송에 앞서 전문적이고 포괄적인 피해구제의 역할을 담당하고 있다. ⑥ 위원회는 상담, 자문, 검토, 제안 등을 통한 정보제공의 역할을 하고 있다.

이를 위해 위원회는 개별적 결정권(제21조 제1항 제2호), 내규(règlement intérieur)·간소규칙(normes simplifiées)·안전규칙(règlementtypes de sécurité)의 제정권(제8조 제4항, 제17조, 제21조 제1항 제3호), 개인정보의 처리를 통제하고 법령의 준수를 감독할 권한(제6조), 개인정보의 공적 또는 사적인 자동처리를 이 법률의 규정에 따라 행하는지의 여부를 감시할 권한(제14조), 각종의 제안·의견표명권 등의 권한을 가진다(제18조, 제45조 등).

6. 이탈리아

이탈리아의 개인정보보호법상 개인정보보호위원회(The Garante)는 독립적인 지위에서 개인정보의 보호에 관한 업무를 총괄한다(제153조 제1항).

(1) 조 직

개인정보보호위원회는 4인의 위원으로 구성되고, 의회에서 임명하도록 되어 있어 의회에 대한 책임을 지는 독립된 합의제기구이다. 위원의 임기는 4년으로 보장되며 1회에 한해 연임할 수 있다. 이러한 개인정보보호위원회의 성격은 이태리가 의원내각제의 전통을 갖고 있기 때문이었는데 그 결과 행정기관에 대한 위원회의 독립성은 강하게 보장받게 되었다.

(2) 기 능

개인정보보호위원회의 주요 업무는 개인정보주체의 개인정보침해에 대한 피해구제인 개인정보심판이 있다. 이는 변론주의에 입각하여 양 당사자의 변론에 기초로 위원회에서 결정하는 것을 말하며, 결정에 불복하는 당사자는 법원에 제소할 수 있다. 이와 관련하여 제소기간을 종래 30일에서 60일로 상향조정하여 제척기간의 도과로 인한 피해를 줄이게 하였다.⁷⁰⁰⁾ 개인정보보호위원회는 이러한 심리 이외에도 개인정보의 등록, 개인정보위반사항에 대한 조사권이 있는데, 조사와 관련하여서는 자료요구권도 있다. 행정기관에 대한 조사도 가능하지만, 기관의 독립성으로 인해 협조가 쉽지 않은 편이다.

7. 스페인

(1) 구 성

스페인에서 개인정보보호에 관한 업무를 담당하는 기구는 정보보호청(Agencia de Proteccion de Datos, APD)이다. 이 정보보호청은 독립성

700) Garante per la protezione dei dati personali, Annual Report for the year 2003, submitted to parliament on April 28, 2004.

을 지닌 독립민간법인으로 설립되어 운영된다. 정보보호청은 임기 4년의 의장을 중심으로 한 4명의 위원회와 4개의 집행부서로 이루어져 있다. 기관장은 각계에서 11명의 대표가 선발되고 이들 중 1명이 선정되는데, 대부분 법률전문가들이 맡고 있다. 그러나 기관의 직원은 모두 공무원이다. 정보보호청의 예산과 결산은 국회에 보고되지만, 재원은 이들 기관이 민간기업에 부과하는 벌금으로 운영하고 있다. 개인정보등록국(Personal Data General Registry)은 개인정보에 관련된 데이터베이스를 등록하는 기관으로, 2001년 12월 현재 271,875건의 개인정보관련 database가 등록되어 있다. 조사국은 개인정보침해에 대한 법률적·기술적 조사를 담당하는 기관이다. 그리고 사무국은 각종 정보보호관련 교육과 홍보를 담당하고 각계의 자문에 응하고 있다.

(2) 기 능

정보보호청은 개인정보보호기본법의 위반에 대한 조사권, 벌금 부과권, 동법 위반기관이 보유한 개인정보의 차단권 등을 포함한 집행권을 갖고 있으며, 중앙정부와 민간기업을 모두 대상으로 법을 집행한다.

공공부문이 개인정보보호법을 위반한 경우 정보보호청은 긴급상황을 조성하여 해당 기관에 시정을 요구한다. 만약 시정요구에도 불구하고 시정이 되지 않는 경우 관련 정보보호청이 직접 관련정보를 차단하거나, 해당 기관의 상급관서에 지시하여 고치도록 권고한다. 만약 그래도 시정되지 않는 경우 시민법에 존재하는 제도, ombudsman제도 등을 통해 시정하도록 한다. 또한 정보보호청은 관련기관의 정보남용 공무원의 징계권 또한 보유하고 있다. 따라서 관련기관 직원들이 법을 위반한 경우 감봉과 해직조치를 취할 수 있다.

한편, 민간기업이 개인정보보호법을 위반하여 개인정보를 남용한 경우 정보보호청은 이들에게 600-60만 유로의 벌금을 부과할 수 있는데, 이를 통해 정보보호청은 강력한 집행력을 보유하고 있다.

8. 일 본

(1) 공공부문

일본은 2003년 5월 ‘정보공개·개인정보보호심사회설치법’을 제정하여 개인정보의 보호에 대한 행정기관의 자문과 개인정보보호 사무를 처리하는 정보공개·개인정보보호 심사회가 설치되었다. 동 심사회는 행정기관이 보유하는 정보의 공개와 행정기관 등이 보유하는 개인정보의 보호에 관한 업무를 담당하는 기관이다. 이를 위해 관계 행정기관 등의 자문에 응하고, 불복청구에 대한 조사심의를 담당하며, 행정기관의 장등에게 답신을 한다. 이러한 업무를 수행하기 위해 심사회는 자문을 한 행정기관의 장등에게 보유개인정보의 제시를 요구할 수 있다.

한편, 행정기관개인정보보호법상 행정기관의 장은 행정기관에 있어서 개인정보취급에 관한 불평의 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).

(2) 민간부문

민간부문에 대한 개인정보감독기구와 관련하여 일본은 미국과 마찬가지로 독자적인 국가차원의 개인정보감독기구가 존재하지 않는다. 다만, 각 개별법률 또는 해당영역을 관할하는 소관주무부처가 개인정보보호 기관의 역할을 담당한다. 이와 관련하여 개인정보보호법 제32

조 내지 제34조는 개인정보보호를 위한 주무대신의 권한을 규정하고 있다. 개인정보보호법이 규정하고 있는 주무대신의 권한은 ㉠ 개인정보취급사업자 및 인정개인정보보호단체로부터 필요한 경우 개인정보취급 등에 대한 보고를 받을 수 있으며, ㉡ 사업자에게 필요한 사항을 조언할 수 있고, ㉢ 개인정보취급사업자가 의무규정을 위반하였을 경우 그러한 행위의 중지 또는 시정의 권고를 할 수 있으며, ㉣ 사업자가 정당한 이유 없이 권고를 무시하여 개인의 중대한 권리와 이익이 침해될 위험이 있는 경우 권고이행명령을 내릴 수 있으며, 긴급한 조치가 필요하다고 인정될 경우에는 사업자에게 의무위반행위의 중지 명령 및 시정명령을 내릴 수 있다. 이는 정부차원의 민간부문 개인정보감독기구라 할 수 있다.

이에 비해 민간차원의 개인정보감독기구로 개인정보피해구제의 역할을 담당하는 기관은 ‘인정개인정보보호단체’가 있다. 인정개인정보보호단체는 주무대신이 민간 개인정보보호단체에 대하여 적절한 역할을 담당하는 개인정보감독기구임을 인정해 줌으로써 민간의 자율규제와 정부의 적절한 감독을 함께 조화시킬 수 있다는 점에서 의미있는 기관이다.⁷⁰¹⁾ 인정개인정보보호단체는 주로 개인정보취급사업자의 개인정보의 적정한 취급을 지원하고 확보할 목적으로 활동하는 단체로서, 사업자에게 필요한 정보를 제공하거나 사업자의 개인정보 취급관행으로 인한 피해를 입은 소비자의 문제제기를 원만히 해결하고 피해구제를 받을 수 있도록 도와주는 역할을 담당한다.⁷⁰²⁾ 이러한 일본의 민간부문에 대한 개인정보감독기구의 운용형태는 일본의 오랜 정·관·민사이의 공조의 전통에서 기인한 것으로 볼 수 있다.

701) 이창범·윤주연, “각국의 개인정보피해구제제도 비교연구”, 개인정보분쟁조정위원회, 2003, 241면.

702) 『개인정보의 보호에 관한 법률』 제37조 내지 제49조에는 민간단체에 의한 개인정보의 보호에 관한 내용이 규정되어 있다.

제 3 절 개인정보감독기구의 유형별 분석

해외 사례에서 나타난 각국의 개인정보감독기구의 특징을 구성현황, 기관장임명, 운영현황, 주요기능을 중심으로 분류하면 다음과 같다.

[표 5-2-3] 각국의 개인정보감독기구 현황

국가	기관명	구성현황	기관장임명	운영현황	주요기능
캐나다	연방프라이버시감독관	· 감독관 1인 · 사무국 약 108명	추밀원장 (Governor in Council)	감독관을 지원하는 사무국 운영 (감독관 자체 운영) (의회에 보고)	· 피해구제(합의권고) · 가이드라인 제정 · 조사감독 및 행정규제
영국	정보감독관	· 감독관 1인 · 사무국 약 200여명	국왕	감독관이 부감독관과 직원 임명 (위원 자체 운영) (의회에 보고)	· 사전합의권고 · 개인정보처리 등록 · 개인정보지침 제정 · 감독 및 행정규제 · 법원에 이첩
독일	연방정보위원회	· 위원 1인 · 사무국	대통령 (연방정부를 의회로부터 받아 선출한 자를 임명)	정보위원을 지원하는 사무국 운영 (연방내무부로부터 인력과 예산 지원) (연방정부와 의회에 보고)	· 연방공공기관 감독 · 고충처리 · 정보처리자 등록, 관리 · 의회 및 정부에 대한 프라이버시 정책 자문
프랑스	정보위원회	· 위원회(총 17인) · 사무국 약 80여명	위원 중 4인 위원이 위문장 호선	위원장을 보좌하는 부서 운영, 직원은 위원장으로부터 위임받은 부위원장이 임명 (대통령과 의회에 보고)	· 피해구제(합의권고) · 개인정보처리자 등록 · 개인정보세부지침·실행규약 제정 · 법규준수여부 감독 · 개인정보보호 자문 및 권고
이태리	개인정보보호위원회	· 위원회(4인)	의회	위원장이 대표, 4인의 위원으로 구성(행정부에 대한 독립성 확보.의원 내각제국가)	· 당사자간 분쟁해결 · 조사감독 및 행정규제 · 의회 보고
스페인	정보보호청	· 기관 및 기관장 · 자문위원회(총 11인)	국왕 (개인정보보호자문위원 중 임명)	기관장이 개인정보보호위원을 대표하며, 법인의 태로 운영됨 (의회에 보고)	· 개인정보처리 등록 · 법규준수 조사, 감독 · 고충처리 · 시정명령, 벌금 등 행정적 규제 · 정보 제공 · 정보의 국제이전 감시 및 허가

제 5 편 개인정보보호의 집행체계에 관한 병행적 입법평가

국가	기관명	구성현황	기관장임명	운영현황	주요기능
일본	정보공개 · 개인정보 보호심사 사회	· 위원회(총 15인) - 상임위원 (5인이내)	양원의 동의를 얻어 내각총리 대신 임명	2003년 5월 법 제 정으로 종래 정보 공개심사 사회를 개 편한 것	· 정보공개 · 개인정보 보호 관한 자문 · 불복청구에 대해 조 사심의 · 행정기관장, 법인에 대한 답신
한국	개인정보 분쟁조정 위원회	· 위 원 회 (총 15인) · 사무국	행정안전부	위원회를 지원하 는 사무국이 한 국 정보보호 진흥 원에서 운영됨	· 개인정보에 관한 민 사 분쟁의 해결 · 정보통신부에 위법사 실 통보
	공공기관 개인정보 보호심의 위원회	· 위 원 회 (총 10인) - 위원(국 무총리 위촉)	국무총리	공공부문에 컴 퓨터에 의해 처 리되는 개인 정보 의 보호에 관한 주요사항 심리	· 주요 정책의 심의 및 자문 기능
미국	독자적인 개인정보감독기구 부재				

이러한 분류를 통하여 각국 개인정보보호기구의 유형과 성격을 도출할 수 있다. 우선 정보처리에 대한 통제권을 갖는 기구로서는 ㉠ 정보처리자 내부의 자율규제에 맡기는 방식(미국, 일본), ㉡ 감독기관에 의한 외부통제방식(프랑스, 스웨덴, 영국), ㉢ 양자를 절충하여 모두 채택하는 방식(독일)으로 나누어 볼 수 있다.

외부규제를 통한 감독기구를 설치하여 개인정보의 처리를 통제·감독하는 경우에도 어떤 성격의 기구가 통제·감독임무를 수행할 것인가에 관해서 ㉠ 음부즈만제도를 도입하는 방안(스웨덴, 프랑스, 독일), ㉡ 독립된 위원회를 설치하는 방안(프랑스, 캐나다), ㉢ 대통령 또는 국무총리 직속하에 행정위원회를 설치하는 방안으로 나누어 볼 수 있다.

개인정보의 처리·이용을 규제·감독하기 위하여 감독기구를 설치할 경우에, 어떠한 기능과 권한을 부여할 것인가는 감독기구의 성격과 규제의 내용·정도 등에 따라 정해질 문제이다. 외국의 입법례상 감독기구의 기능 및 권한의 내용을 분석해 보면 다음과 같다.

㉠ 정보파일(정보시스템) 설치에 대한 신고·등록의 접수 및 심사와 허가 등의 통제기능(스웨덴, 프랑스, 독일, 영국, 캐나다), ㉡ 정보시스

템의 설치, 수집·이용·보관 및 적정관리 등 법준수 상태를 조사·지도·감독하고 그 위반에 대해 시정을 권고·명령하는 기능, ㉓ 시정명령·권고의 불이행, 기타 범위반에 대해 사법기관에 고발하는 권한(프랑스), ㉔ 정보당사자의 민원·고충과 정보처리자의 이의신청 등을 접수하고 심사·처리하는 기능(프랑스, 독일, 영국, 캐나다), ㉕ 기타 정보색인부의 작성·공시, 제도발전을 위한 연구·건의·조언, 의회 등에서의 정기·부정기적인 보고 등 개인정보 보호를 위한 방안을 강구하는 기능 등이 있다.

제 3 장 우리의 집행체계에 대한 평가

제 1 절 개인정보감독기구의 현황

1. 앞에서 살펴본 바와 같이 외국에는 개인정보보호에 관한 정책의 수립과 추진, 개인정보의 침해에 대한 예방과 구제, 개인정보의 처리에 대한 관리와 감독 등을 전담하는 별도의 개인정보감독기구를 두는 경우가 적지 않다. 하지만 개인정보보호에 관한 전담기구를 두지 않는 경우에도 일반적인 행정기관 산하에 개인정보의 처리를 관리감독하고 관련 분쟁을 해결하기 위한 특수한 기구를 설치하여 운영하는 것이 보통이다.

그런데 개인정보감독기구는 엄밀히 개인정보보호에 관한 업무를 전담하는 기구를 지칭하는 것으로 파악할 수 있다. 하지만 이를 광의로 보아서 실질적으로 개인정보보호의 기능을 수행하는 기관을 모두 포괄하는 개념으로 이해할 수도 있다. 여기서는 후자의 개념에 따라 우리나라의 현행 개인정보감독기구의 현황을 살펴보기로 한다.

2. 우선 공공기관개인정보보호법을 살펴보면, 행정안전부장관은 동법의 시행을 위하여 필요하다고 인정되는 경우에는 공공기관의 장에 대하여 개인정보의 처리에 관한 자료의 제출을 요구할 수 있으며, 소속공무원으로 하여금 실태조사를 하게 할 수 있다(제18조). 또한 동법의 목적을 달성하기 위하여 필요하다고 인정되는 경우에는 공공기관의 장에게 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다(제19조).

3. 다음으로, 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위하여 국무총리소속하에 공공기관개인정

보보호심의위원회를 둔다(제20조 제1항). 이 위원회는 개인정보보호에 관한 정책 및 제도개선, 처리정보의 이용 및 제공에 대한 공공기관간의 의견조정, 개인정보화일에 기록되어 있는 항목의 전부 또는 일부를 관보에 게재하지 아니하려는 경우 그에 관한 사항, 기타 관련법령 등의 정비·개선에 관하여 위원장이 부의하는 사항 등에 관한 사항을 심의한다(법 제20조 제2항, 시행령 제28조). 이위원회는 위원장 1인을 포함한 10인 이내의 위원으로 구성된다(시행령 제27조 제1항). 위원장은 행정자치부차관으로 하고, 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자중에서 위원장의 추천으로 국무총리가 임명 또는 위촉한다(시행령 제27조 제2항). 위원의 임기는 2년으로 한다(시행령 제27조 제3항). 공공기관개인정보보호법이 공공부문을 규율하는 일반법적인 성질을 가진다고 볼 때 동 위원회는 공공부문에 있어서 전산처리된 개인정보의 보호를 위한 정책을 추진하는 중추적 기관이라고 할 수 있다.

4. 한편, 관계중앙행정기관의 장도 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 필요한 때에는 국가행정기관 및 지방자치단체 외의 공공기관에 대하여 개인정보의 보호에 관하여 의견을 제시하거나 지도·점검 등을 할 수 있다(제21조). 정부투자기관등에 대한 관계중앙행정기관의 장의 지도·감독은 그 내용, 사유 및 기간 등을 명시한 서면으로 하여야 하고, 지도·감독을 받은 공공기관의 장은 그에 따라 필요한 조치를 취하며, 그 결과를 지도·감독기관의 장에게 서면으로 통보하여야 한다(시행령 제25조).

5. 민간부문에 있어서는 개별 법률의 규율에 따라 개인정보보호법의 집행체계가 달리 구성된다. 우선 행정안전부 또는 방송통신위원회도 정보통신망법상의 개인정보보호에 관한 규정의 준수에 관한 포괄적인

감독권한을 가진다고 볼 수 있다. 다음으로 정보통신망의 이용과 관련하여 행정안전부에 개인정보분쟁조정위원회가 설치되어 개인정보침해 관련 분쟁의 해결을 꾀하고 있다. 또한 개인정보침해신고센터, 전자거래분쟁조정위원회 등도 개인정보침해와 관련된 분쟁을 해결하는데 일익을 담당하고 있다. 나아가 전자상거래상의 개인정보보호를 위해 금융위원회가 개인정보침해에 대한 관리감독을 하고 있으며, 금융분야에서의 정보보호는 금융감독원과 금융감독위원회에 맡겨져 있다.

한편, 국민권익위원회, 국가인권위원회, 한국소비자원 등도 국민의 일반적인 권익의 옹호기관으로서 개인정보의 침해로 인한 분쟁도 해결해줄 수 있다.

[표 5-3-1] 공공부문의 개인정보감독기구

기관명	근거법률	관할범위	주요 기능
공공기관개인정보보호심의위원회	『공공기관의 개인정보 보호에 관한 법률』	공공기관이 보유하고 있는 개인정보	- 정책 및 제도개선 사항 심의 - 공공기관간 의견조정 사항 심의 - 법령 등의 정비, 개선 사항 심의
행정안전부	『공공기관의 개인정보 보호에 관한 법률』	공공기관이 보유하고 있는 개인정보	- 개인정보파일 보유 공공기관 접수·공고 - 의견제시 및 권고
국민권익위원회	『부패방지 및 국민권익위원회의 설치와 운영에 관한 법률』 (2008.2.29)	행정기관관련 민원사무 일반	- 민원사항 안내 및 상담 - 고충민원의 조사·처리, 시정권고 등 - 위법·부당한 처분 등의 시정권고 등 - 행정 제도 및 운영의 개선 권고 등
국가인권위원회	국가인권위원회법	인권침해 일반	- 법령·제도·정책·관행의 조사·연구 - 개선권고 및 의견표명 - 침해구제 - 지침의 제시 및 권고

[표 5-3-2] 민간부문의 개인정보감독기구 현황

기관명	근거법률	관할범위	주요 기능
개인정보분쟁 조정위원회	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	정보통신망상에서의 개인정보침해 일반	- 사실조사 및 청문 - 합의권고 - 분쟁조정 - 위법사실통보 등
개인정보침해 신고센터	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	- 정보통신서비스 - 호텔·항공사·학원 등	- 상담 및 고충처리 - 교육·홍보 - 기술적 자문 등
행정안전부	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	정보통신망상에서의 개인정보침해 일반	- 법률 위반 등 조사 - 시정명령 및 위반사실 공표
방송통신 위원회	『정보통신망 이용촉진 및 정보보호 등에 관한 법률』	정보통신망상에서의 개인정보침해 일반	- 법률 위반 등 조사 - 시정명령 및 위반사실 공표 - 과징금 부과
금융위원회· 금융감독원	『신용정보의 이용 및 보호에 관한 법률』	금융거래	- 상담 및 피해구제 - 시정 권고 및 명령 - 기준제정 등
전자거래분쟁 조정위원회	전자거래기본법	전자거래	- 상담 및 피해구제
한국소비자원	소비자기본법 (2007.3.28)	소비자거래	- 소비자불만처리와 피해구제

제 2 절 현행 개인정보감독기구의 문제점

1. 공공기관개인정보보호심의위원회

공공부문에 있어서 전산처리된 개인정보의 보호에 관해서는 공공기관개인정보보호심의위원회가 정책추진, 관리감독, 피해구제 등의 업무를 수행하는 총괄적 기구로서 기능한다.

하지만 공공기관개인정보보호심의위원회의 위원장은 행정안전부차관이 맡고, 그 위원도 위원장의 추천으로 국무총리가 임명하도록 되어 있다. 또한 위원의 임기는 2년으로 임기가 보장되지 않기 때문에 위원의 독자적이고 자주적인 활동보장이 되어 있지 않다. 뿐만 아니라 동 위원회는 자체조사권이나 명령권 등을 가지지 못하고, 단지 심의기능만을 담당할 뿐이다. 이러한 점에서 동 위원회는 공공기관을 관리·감독하기에 기관의 독립성이 충분히 확보하고 있지 못하다고 볼 수 있고, 그 결과 개인정보보호의 업무를 수행함에 있어서 적잖은 한계를 드러낼 수밖에 없게 되어 있다.

다른 한편으로, 전자정부의 추진을 책임지고 있는 행정안전부에 공공기관이 보유한 개인정보의 처리에 대한 감독까지 맡기고 있기 때문에 법적 지위의 혼동이 발생한다. 이는 하나의 행정기관이 이용촉진과 처리규제라는 상반된 기능을 동시에 수행해야 하는 것을 의미한다. 이로 말미암아 병존하는 두 가지의 기능을 어느 하나도 제대로 수행하기 어렵게 될 수도 있다. 요컨대 공공기관개인정보보호심의위원회를 통한 감독시스템은구체적인 피해의 구제나 오남용에 대한 시정 등에 있어서 실효성을 기대하기 어려울 것으로 보인다.

2. 행정안전부와 방송통신위원회

공공부문이 보유한 전자화된 개인정보의 처리에 대해서는 현재 행정안전부가 공공기관의 개인정보보호정책을 집행하는 주무관청으로 설정되어 있다. 한편, 민간부문에서는 정보통신망상의 개인정보보호정책을 집행하는 기관으로 행정안전부와 방송통신위원회가 있다. 하지만 이러한 법의 집행체계는 다음과 같은 문제점을 안고 있다.

첫째, 행정안전부 중심의 보호체계는 행정에 대한 내부통제로서 관료적 관점에서 개인정보의 활용에 따른 직무수행의 효율성을 강조하는 결과를 가져올 위험이 있다.

둘째, 공공부문의 개인정보보호정책을 집행하는 행정안전부는 동시에 전자정부의 추진을 주관하는 기관이다. 이 경우 전술할 바와 마찬가지로 전자정부의 추진과 전자화되어 보유된 개인정보의 보호라는 두 가지 상충되는 가치를 조화시키기 쉽지 않다는 문제가 있다.

셋째, 민간부문의 경우 정보통신망상의 개인정보보호정책을 집행하는 기관으로 행정안전부와 방송통신위원회가 있다. 하지만 최근 정보통신망법의 개정으로 행정안전부 또는 방송통신위원회가 법률 위반사실의 조사와 시정명령 및 공표를 할 수 있도록 규정하고 있기 때문에(제64조), 두 기관 사이에 업무의 중복이나 의견의 대립 혹은 권한 다툼 등 복잡한 문제들이 발생할 소지가 있다. 또한 방송통신위원회는 기본적으로 정보통신기반의 구축과 정보통신산업의 진흥을 주로 담당하는 기관이다. 이러한 기관이 개인정보보호라는 충돌하는 업무를 수행하는 경우에 위에서 본 공공부문과 동일한 문제점이 발생할 수 있고, 지나치게 산업계의 논리에 끌려 다닐 위험성도 배제할 수 없다.

넷째, 현재의 개인정보보호기구는 부문별로 부분적인 영역에서만 보호기구가 존재하기 때문에, 해당 영역 이외의 부문은 보호체계 밖에 놓이게 된다는 문제점을 안고 있다.⁷⁰³⁾ 그나마 행정안전부 산하의 개인정보침해신고센터와 개인정보분쟁조정위원회의 노력을 제외한다면, 다른 기관들은 개인정보보호기구로서의 기능을 거의 하지 못하고 있다고 해도 과언이 아니다. 이와 같은 정보보호의 공백이 발생하게 됨으로써 보건의료, 과학연구 및 통계조사 등 특정 영역에서 특정 목적을 위해 수집된 개인정보의 보호에 특히 취약하게 만들고 정보의 오남용 예방과 피해구제를 불가능하게 하여 더 큰 피해를 낳을 여지를 제공한다.

다섯째, 각 부문의 감독기구는 제한적인 기능만을 수행하기 때문에 개인정보보호에 취약하다. 특히 개인정보보호가 활발한 정보통신부문

703) 이인호·권현영, “개인정보보호를 위한 통합감독기구의 설립방안”, 『제4회 개인정보보호 정책포럼』, 2004. 6.

의 경우 보호기능은 주로 정보주체의 침해에 대한 구제신청을 처리하는 데 머물러 있고, 적극적인 조사나 정보의 등록 및 관리·감독의 기능은 수행하지 않는다. 이러한 문제는 특히 공공부문의 경우 두드러진다. 공공기관이 개인정보의 관리를 잘못하고 있거나, 오남용하고 있는 경우 이 정보의 차단이나 폐기에 관련된 명령을 할 수 있는 권한이 법적으로 확보되어 있지 않고 있다. 또한 정보관리자의 정보관리상의 잘못된 행위에 대한 인사상조치권 등이 확보되지 않고 있기 때문에 다른 부처가 관리하는 개인정보의 오남용을 예방할 정도의 억제력을 갖고 있지 않은 게 현실이다. 이러한 제한적 보호기능을 갖고 있는 개인정보보호기구는 결국 개인정보의 침해의 빈도와 정도를 심화시킬 가능성을 열어놓고 있는 것이 된다.

3. 금융위원회와 금융감독원

금융위원회와 금융감독원은 주로 금융거래질서의 유지를 일차적 목적으로 하기 때문에 금융기관 등이 보유한 개인정보의 보호에 큰 관심을 갖지 않다. 따라서 이를 통해서도 개인정보침해에 대한 예방과 감독의 기능이 충실하게 수행될 것으로 기대하기 어려운 것이 현실이다. 이러한 문제는 개별분야의 정보보호에 관한 일반적이고 공통적인 기준이나 지침이 결여되어 있기 때문에 초래되는 측면이 크다고 할 수 있다.

제 3 절 법률안의 감독기구 관련 내용

1. (구)이혜훈 법안

동 법안에서는 개인정보보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리소속으로 ‘개인정보위원회’를 두도록 하였다. 위원회의 임무가 개인정보의 보호와 이용의 균형적 발전에 있음을 명확히 하기 위하여 명칭을 ‘개인정보위원회’로 하였음을 밝히고 있다(안 제34조).

- ㉠ 개인정보위원회의 주요 기능을 정책연구, 제도개선, 상담 및 피해구제, 교육·홍보, 기술 개발 및 지원 등에 둬으로써 지원·촉진기능을 강화하고 규제적 기능을 최소화함(안 제41조).
- ㉡ 개인정보위원회가 효율적으로 업무를 수행할 수 있도록 하기 위해 개인정보위원회에게 자료제출요구권, 현황조회권, 방문조사권, 시정권고, 시정명령, 고발 및 징계권고권 등의 권한을 부여함(안 제43조 내지 제49조).
- ㉢ 개인정보처리자의 자율적 준수를 유도하기 위하여 개인정보위원회가 개인정보침해의 유형·판단기준 및 그 예방조치 등에 관한 지침을 정하여 고시할 수 있게 함(제50조).
- ㉣ 개인정보에 관한 분쟁조정 업무를 신속하고 공정하게 처리하기 위하여 개인정보위원회에 개인정보분쟁조정위원회를 둬(제55조).
- ㉤ 개인정보보호 행정체계를 일원화함으로써 이중규제를 방지하기 위하여 「공공기관의 개인정보보호에 관한 법률」을 폐지하고, 그와 아울러 「정보통신망이용촉진및정보보호등에관한법률 일부개정법률안」 제22조 내지 제40조를 삭제하며(안 제22조 내지 제40조), 제52조 제3항 제7호 및 제8호도 삭제함(안 제52조 제3항 제7호 및 제8호).

2. 이은영법안

동 법안에서는 개인정보보호 업무의 체계적·일관적 집행을 위해 국무총리 소속하에 ‘개인정보보호위원회’를 설치하고 있다(안 제24조).

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

- ② 개인정보보호위원회가 개인정보 침해사건에 대하여 필요한 경우 시정명령 등을 발할 수 있도록 하여 신속한 피해구제 및 구제의 실효성을 확보함(안 제40조).
- ③ 개인정보에 관한 분쟁 조정업무를 신속하고 공정하게 처리하기 위하여 개인정보보호위원회에 개인정보분쟁조정위원회를 둠(제43조).
- ④ 개인정보에 관한 분쟁조정 절차를 일원화하기 위하여 『공공기관의개인정보보호 관한법률 일부 개정법률안』의 개인정보심의위원회 관련 조항을 폐지하고(안 제22조), 『정보통신망이용촉진및정보보호등에관한법률 일부개정법률안』의 개인정보분쟁조정위원회 관련 규정을 삭제함(안 제33조 내지 제40조).

3. 노회찬법안

동 법안에서도 이 법 및 개인정보 보호에 관한 다른 법률의 준수여부를 감독하기 위하여 ‘개인정보보호위원회’를 두고 있다(안 제60조).

- ① 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 소속기관등의 장에게 개인정보의 수집, 이용의 중단, 기타 필요한 조치를 하도록 권고할 수 있음(안 제93조).
- ② 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 함(안 제95조).

4. 행정안전부 입법예고법안

동 법안에서도 이 법 및 개인정보 보호에 관한 다른 법률의 준수여부를 감독하기 위하여 ‘개인정보보호위원회’를 두고 있다(안 제60조).

- ㉠ 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 소속기관등의 장에게 개인정보의 수집, 이용의 중단, 기타 필요한 조치를 하도록 권고할 수 있음(안 제93조).
- ㉡ 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 함(안 제95조).

5. (신)이혜훈 법안

개인정보보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 ‘개인정보위원회’를 두고 있다(안 제34조). 위원회의 임무가 개인정보의 보호와 이용의 균형적 발전에 있음을 명확히 하기 위하여 명칭을 ‘개인정보보호위원회’가 아닌 ‘개인정보위원회’로 한다고 설명하고 있다.

- ㉠ 개인정보위원회의 주요 기능을 법제도 및 정책연구, 제도개선, 상담 및 피해구제, 교육·홍보, 기술 개발 및 지원 등에 둠으로써

지원·촉진기능을 강화하고 관리·감독 및 규제적 기능은 최소화함(안 제41조).

- ㉞ 개인정보위원회가 효율적으로 업무를 수행할 수 있도록 하기 위해 개인정보위원회에게 자료제출요구권, 실태조사권, 방문조사권, 시정권고, 시정명령, 고발 및 징계권고권 등의 권한을 부여함(안 제43조 내지 제49조).
- ㉟ 이 법의 효율적 집행을 위하여 위원회가 분야별 또는 품목별로 개인정보의 수집·처리 요건, 절차, 방법 등을 포함하여 개인정보의 보호 및 이용에 관한 구체적인 기준을 정한 개인정보보호기준을 제정·고시할 수 있도록 함(안 제50조).
- ㊱ 개인정보에 관한 분쟁조정 업무를 신속하고 공정하게 처리하기 위하여 개인정보위원회에 개인정보분쟁조정위원회를 둠(제55조).
- ㊲ 개인정보피해의 집단성·단체성을 반영하고 최근 소비자기본법의 개정 취지를 고려하여 개인정보피해에 대해서도 집단분쟁조정 제도를 도입함(안 제60조).

제 4 절 개인정보보호법(안)의 분석

1. 명 칭

다섯 법안 모두 개인정보감독기구를 모두 도입하고 있지만, 그 명칭은 동일하지 않다. 즉, (구)이혜훈법안 및 (신)이혜훈법안에서는 ‘개인정보위원회’라고 하고 있으며, 나머지 세 법안에서는 모두 ‘개인정보보호위원회’라고 명명하고 있다.

2. 지 위

노회찬법안은 인권위원회와 같은 성격의 독립위원회를 설치하고 있는 데 비해, 나머지 네 법안은 모두 국무총리 소속의 중앙행정기관으

로 설치하고 있다.

3. 구 성

(1) (구)이혜훈법안

위원장 1인과 상임위원 1인을 포함한 5인의 위원으로 구성하되, 위원장과 상임위원은 국회의 동의를 얻어 대통령이 임명하고, 비상임위원은 국회의장이 임명하도록 하고 있다.

(2) 이은영법안

국회가 추천하는 3인, 대법원장이 추천하는 3인, 대통령이 임명하는 3인으로 총 9인으로 구성하되, 위원장은 국무총리의 제청으로 대통령이 임명하도록 하고 있다.

(3) 노회찬법안

국회가 선출하는 5인과 대통령이 지명하는 4인으로 총 9인으로 구성하되, 위원장은 호선하도록 하고 있다.

(4) 행정안전부 법안

위원장 1명을 포함한 15명 이내의 위원으로 구성하되, 위원장과 위원을 국무총리가 위촉 또는 임명하도록 하고 있다.

(5) (신)이혜훈법안

위원장 1인과 상임위원 1인을 포함한 9인의 위원으로 구성하되, 위원장과 상임위원을 국무총리가 제청하고 대통령이 임명하도록 하며, 비상임위원은 위원장이 추천한 자 중에서 국무총리가 임명하도록 하고 있다.

4. 업 무

(1) (구)이혜훈법안

① 개인정보의 보호 및 이용에 관한 시책의 수립 및 집행, ② 개인정보에 관한 법령·제도 및 관행의 개선 연구, ③ 개인정보보호지침의 제정·고시, ④ 개인정보침해에 대한 조사·고충처리 및 피해구제, ⑤ 개인정보에 관한 분쟁의 조정, ⑥ 개인정보의 처리실태, 처리현황 등에 관한 조사·연구, ⑦ 개인정보보호에 관한 기술개발의 지원 및 보급, ⑧ 개인정보의 이용 및 보호에 관한 교육 및 홍보, ⑨ 개인정보보호를 위한 국제기구 및 외국의 개인정보보호기구와의 교류·협력, ⑩ 이 법 및 다른 법령에 의하여 위원회의 소관으로 규정된 사항, ⑪ 그 밖에 개인정보의 이용 및 보호를 위하여 필요하다고 인정하는 사항 등(제41조)

(2) 이은영법안

① 개인정보의 보호 및 이용에 관한 시책의 수립 및 집행, ② 개인정보에 관한 법령 및 제도의 개선, ③ 개인정보 침해에 대한 조사·고충처리 및 피해구제, ④ 개인정보에 관한 분쟁의 조정, ⑤ 개인정보보호에 관한 기술개발의 지원 및 보급, ⑥ 개인정보보호관련 민간단체의 지원, ⑦ 개인정보의 이용 및 보호에 관한 교육 및 홍보, ⑧ 개인정보보호를 위한 국제기구 및 외국의 개인정보보호기구와의 교류·협력, ⑨ 그 밖에 개인정보의 이용 및 보호를 위하여 필요하다고 인정하는 사항 등(제34조)

(3) 노회찬법안

① 개인정보보호 보호에 관한 법령(입법과정 중에 있는 법령안을 포함한다)·제도·정책·관행의 조사와 연구 및 그 개선이 필요한 사항에 관한 권고 또는 의견의 표명, ② 개인정보보호에 관한 고시, 지침,

가이드라인의 제정, ③ 개인정보 침해행위에 대한 조사와 구제, ④ 개인정보보호 기술의 연구 지원, ⑤ 개인정보보호 현황에 대한 실태조사, ⑥ 개인정보보호에 관한 교육 및 홍보, ⑦ 개인정보보호침해의 유형·판단기준 및 그 예방조치 등에 관한 지침의 제시 및 권고, ⑧ 국제개인정보보호 관련된 국제기구 및 외국의 개인정보기구와의 교류·협력 활동, ⑨ 개인정보보호의 옹호와 신장을 위하여 활동하는 단체 및 개인과의 협력, ⑩ 개인정보 데이터베이스의 등록, ⑪ 개인정보영향평가의 시행과 연구, ⑫ 그 밖에 이 법률에 규정된 사항과 기타 개인정보보호의 보장과 향상을 위하여 필요하다고 인정하는 사항 등(제74조)

(4) (신)이해훈법안

① 개인정보의 보호 및 이용에 관한 시책의 수립 및 집행, ② 개인정보에 관한 법령·제도 및 관행의 조사·연구 및 개선, ③ 개인정보보호기준의 제정·고시, ④ 정보주체의 권리침해에 대한 조사, ⑤ 개인정보의 수집·처리와 관련한 고충처리·피해구제 및 분쟁조정, ⑥ 개인정보의 수집·처리 실태 등에 관한 조사·연구, ⑦ 개인정보보호에 관한 기술개발의 지원 및 보급, ⑧ 개인정보의 이용 및 보호에 관한 교육 및 홍보, ⑨ 개인정보보호단체의 지원 및 자율규제활동의 촉진, ⑩ 개인정보보호를 위한 국제기구 및 외국의 개인정보보호기구와의 교류·협력, ⑪ 이 법 및 다른 법령에 따라 위원회의 소관으로 규정된 사항, ⑫ 그 밖에 개인정보의 보호 및 이용을 위하여 필요하다고 인정하는 사항 등(제41조)

(5) 행정안전부 법안

개인정보보호 기본계획 및 시행계획, 개인정보보호에 관한 정책, 법령 및 제도의 개선에 관한 사항, 개인정보 처리에 관한 공공기관 간

의 의견조정에 관한 사항, 개인정보보호에 관한 법령의 해석·운용에 관한 사항, 개인정보의 목적외 이용·제공에 관한 사항, 영향평가 결과에 관한 사항, 의견제시 및 개선권고에 관한 사항, 처리결과의 공표에 관한 사항 등의 심의(제10조)

5. 권 한

(1) (구)이해훈법안

의견제시, 개선권고, 자료제출요구·현황조사, 방문조사, 처리결과의 공개, 시정명령(침해행위중지, 개인정보처리 일시정지 등), 고발·징계권고, 개인정보영향평가·인증기관의 지정 등

(2) 이은영법안

의견제시, 자료제출요구·현황조회, 방문조사, 처리결과의 공개, 시정명령(침해행위중지, 개인정보처리·이용일시정지 등), 고발·징계권고 등

(3) 노회찬법안

규칙·고시 제정, 자료제출요구·사실조회, 청문회, 개선·시정권고, 교육·홍보, 의견제출, 직권조사, 질문·검사권, 합의 권고, 직권배상, 고발·징계권고, 긴급구체조치 등

(4) (신)이해훈법안

의견제시, 개선권고, 자료제출 요구 및 실태조사, 방문조사, 시정명령 등, 고발, 징계권고, 처리결과의 공개, 연차보고, 개인정보보호기준의 제정 등

(5) 행정안전부 법안

개인정보보호위원회는 심의권만 가질 뿐이다.⁷⁰⁴⁾

6. 하위기구

(1) (구)이혜훈법안

개인정보분쟁조정위원회를 설치·운영함

(2) 이은영법안

개인정보분쟁조정위원회, 개인정보침해신고센터를 설치·운영함

(3) (신)이혜훈법안

개인정보분쟁조정위원회를 설치·운영함

(4) 행정안전부 법안

개인정보분쟁조정위원회를 두되, 위원장과 위원을 행정안전부장관이 위촉 또는 임명하도록 하고 있다.

7. 평 가

개인정보보호위원회를 국무총리 소속의 중앙행정기관으로 하고 있는 법안 가운데, 특히 행정안전부 법안은 위원장과 위원의 임명까지 국무총리의 권한으로 하고 있어서 직무상의 독립성을 확보하기에 어

704) 동 법안에서는 의견제시·개선권고, 실태조사, 자료제출 요구 및 검사, 시정명령, 고발, 징계권고, 결과공표, 개인정보보호지침 제정 등은 행정안전부장관의 권한으로 규정하고 있다.

려운 점이 있다. 더구나 동 위원회의 기능을 개인정보보호에 관한 여러 사항들을 심의하는 데 그치도록 하고, 개인정보보호에 관한 실질적 활동을 행정안전부장관에게 맡기고 있다. 이는 개인정보보호위원회의 역할을 지나치게 축소시키는 것이라고 할 수 있다. 이렇게 될 경우 현재의 공공기관개인정보보호심의위원회가 드러내고 있는 한계를 그대로 답습하게 될 것이다. 이러한 점은 개인정보분쟁조정위원회를 두면서도 그 구성을 행정안전부장관에게 맡겨둠으로써 조직상의 독립성을 확보하기 어렵게 한 것에서도 찾을 수 있다.

한편, (신)이혜훈법안은 위원장 1인과 상임위원 1인을 포함한 9인의 위원으로 구성하되, 위원장과 상임위원을 국무총리가 제청하고 대통령이 임명하도록 하며, 의견제시, 개선권고, 자료제출 요구 및 실태조사, 방문조사, 시정명령 등, 고발, 징계권고, 처리결과의 공개, 연차보고, 개인정보보호기준의 제정 등의 권한을 부여하고 있다. 개인정보의 보호와 이용의 균형적 발전을 동시에 고려하여 개인정보보호기구의 직무와 권한을 설정하고 있다는 점에서 긍정적으로 평가받을 만하다고 본다.

제 4 장 감독기구의 설치방안

제 1 절 감독기구의 통합 필요성

(1) 감독기구를 마련한다고 할 때, 공공부문과 민간부문을 분리하여 각각 별개의 감독기구를 두는 것이 타당한가, 아니면 양 부문을 통합하여 감독하는 통합된 감독기구를 설치하는 것이 바람직한가에 관하여 대립된 입장이 있다. 그 동안 시민사회단체와 학계의 다수는 통합된 개인정보감독기구의 설립을 주장하여 왔다.⁷⁰⁵⁾ 한편, 단기적으로는 공공부문과 민간부문을 분리하여 일반법을 제정하고 장기적으로는 통합기본법을 제정하자는 입장에서도 감독기구는 공공과 민간을 총괄하여야 한다는 주장도 있다.⁷⁰⁶⁾ 이에 반하여 우리나라에서는 두 개의 영역을 통합할 경우 민간부문까지 프라이버시보호가 위축될 우려가 있다고 하면서, 공공부문에 대하여는 국가기관간 상호 견제가 가능한 고도의 독립된 국가기관에서 프라이버시 문제를 관장하도록 하되, 민간부문에 대하여는 보다 소프트하고 유연한 조직에서 관장하게 하는 것이 바람직하다는 의견도 있다.⁷⁰⁷⁾

(2) 물론 개인정보처리의 위험성의 정도는 공공부문과 민간부문에서 각각 다르고, 민간부문 내에서도 처리하는 개인정보의 종류와 성격에

705) 정영화, “개인정보감독기구의 법적책 고찰”, 『프라이버시보호법제, 어떤 모습이어야 하는가?』, 9개 시민사회단체 연석 워크숍, 2003. 8. 21; 권현영, “전자정부시대 개인정보보호법제의 쟁점”, 『정보화정책』 제11권 제3호(한국전산원, 2004), 72면; 장여경, “한국의 프라이버시보호 감독기구의 위상과 역할”, 『프라이버시보호법제, 어떤 모습이어야 하는가?』, 9개 시민사회단체 연석 워크숍, 2003. 8. 21; 최경진, “개인정보의 법적 규율과 관련한 공적 영역과 사적 영역의 구별 여부”, 『프라이버시보호법제의 규율대상과 범위』, 9개 시민사회단체 연석 워크숍 제3회, 2003. 8. 26 등 참조.

706) 이민영, “개인정보보호법제의 개편논의와 개선방안”, 『정보통신정책』 제16권 제1호(정보통신정책연구원, 2004), 42면.

707) 이창범, “현행 프라이버시 보호 담당기구의 성과와 한계”, 『프라이버시 보호 법제, 어떤 모습이어야 하는가?』 (9개 시민단체 연석 워크숍, 2003. 8. 21), 21-22면.

따라 다르게 마련이다. 그렇지만 개인정보처리에 있어서 공공부문과 민간부문을 엄밀히 구분한다는 것이 무의미한 경우도 적지 않다. 놀라운 속도로 발전해가고 있는 정보기술은 개인정보보호와 관련해서 공공부문과 민간부문의 경계를 허물어뜨리고 있다. 일단 개인정보가 디지털형태로 변환되고 네트워크상에서 접근 및 이용할 수 있게 되면, 그 개인정보는 부문의 경계를 넘어 결합되거나 공유될 수 있다.⁷⁰⁸⁾ 더욱이 정보주체는 자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 이용되는지를 명확하게 인식하고 그러한 정보처리의 과정에 함께 참여할 수 있어야 한다는 요청은 민간부문이나 공공부문이나 동일하다.

(3) 한편 감독기구의 통합은 정보주체인 시민의 권리를 실현하고 보호하는 데 있어 매우 효과적이다. 정보주체의 입장에서 보면, 자신의 개인정보가 민간부문이나 공공부문이나 그 어디에서 처리되고 있는 상관없이 단일의 통합기구에서 통일되게 감독기능이 이루어질 것이라는 믿음을 가질 수 있고, 또 권리침해가 있다고 주장하는 경우에 통합된 감독기구라는 단일의 창구를 통해서 권리구제를 요청할 수 있다는 점에서 감독기구의 통합이 요청된다고 하겠다. 그리고 국가적인 차원에서 개인정보보호를 위한 종합적인 정책의 방향을 마련하는 일은 통합된 감독기구에서 수행될 수밖에 없다. 물론 이 단일의 감독기구가 각 부문별 차이점을 확인하고 그에 따라 개별적이고 효과적인 법의 준수가 이루어질 수 있도록 조정하는 역할도 마땅히 수행하여야 할 것이다.

그렇다면 따라서 개인정보처리의 기본원칙과 개인정보보호의 헌법 이념이 단일의 감독기구에 의해서 공공과 민간 모두에서 함께 실현될

708) Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection*(Michie Law Publishers, 1996), p. 20.

수 있어야 할 것이다.

제 2 절 독립적 감독기구의 형태

1. 독립성의 의미

정보의 가치 증대, 개인정보 수집, 가공기술의 발달 등을 놓고 볼 때, 개인정보 수집과 이용에 의한 인권과 기본권 침해 사례는 앞으로 더욱 늘어날 것이다. 그리고 이러한 개인정보침해의 문제는 개인적인 문제로만 그치지 않고, 공동체의 원리에 대한 침해의 문제로 연결될 가능성이 크다. 그래서 이러한 위협에 효과적으로 대처할 수 있는 효과적인 방안으로서 독립적인 감독기구의 설치·운영이 필요하다.

여기서 감독기구의 독립성은 기능적 독립성을 의미하는 것이지, 반드시 조직상의 독립성을 요구하는 것은 아니다. 국제개인정보보호기구 회의(ICDPC; International Conference of Data Protection Commissioners)도 그러한 맥락에서 독립성 기준을 기능적 측면에서 찾고 있다. 즉 “감독기구는 그 기능을 수행함에 있어서 필요한 정도의 자율성과 독립성을 보장받아야만 한다.” 여기서 ‘자율성’이라 함은 다른 기관의 허가를 받을 필요 없이 필요한 조치와 직무를 수행할 수 있는 법적 및 실제적인 권한을 부여받아야 한다는 것을 의미한다. 그리고 ‘독립성’이라 함은 정치적인 간섭 또는 정부의 간섭 없이 자유롭게 직무를 수행할 수 있어야 하고, 기득권 세력의 영향을 거부할 수 있어야 한다는 것을 의미한다.

2. 감독기구의 설치방안

감독기구의 설립형태와 관련하여서는 국가인권위원회 소속으로 합의를 개인정보감독기구를 설치하여 그 임무를 수행하도록 하는 방안,

대통령 소속으로 정보보호를 위한 독립위원회를 설치하는 방안, 정부 부처형 감독기구로서 개인정보보호위원회를 만드는 방안 등을 고려해 볼 수 있다. 각 방안의 내용과 장단점을 살펴보면 다음과 같다.

(1) 국가인권위원회의 부서로 하는 방안

이는 개인정보보호도 인권의 보장이라는 측면에서 다루어질 수 있는 문제이므로, 별도의 기구를 설립하여 운영하는 것보다 기존의 국가인권위원회에서 개인정보보호업무를 총괄하도록 하자는 방안이다.

이 경우 국가인권위원회의 독립성으로 인해 강한 독립성의 확보가 가능하다. 또한 종래 존재하는 조직의 인력과 재정을 일부 이용할 수 있고, 신규조직을 별도로 설립할 필요가 없다는 측면에서 정부조직 확대에 따른 부담을 줄여 기구설립이 비교적 용이한 편이다.⁷⁰⁹⁾

하지만 권리구제기능이 정책기능과 분리됨으로써 효율적인 개인정보보호를 기할 수 없다는 문제가 있다. 더구나 국가인권위원회로서는 실효성 있는 행정적 지원이 불가능하다. 기관의 역량이 정보보호 이외에 다른 분야의 인권침해로 분산되고, 개인정보보호에 관련된 전문가의 역량이 결집되기 어렵기 때문이다. 또한 제3의 독자적인 인권기구로서의 특성에 비추어 볼 때 국가인권위원회라는 특별기구에서 개인정보보호업무에 전념하기 어려운 구조적 한계가 또 다른 문제점으로 지적될 수 있다.

(2) 대통령 소속 독립위원회 설치방안

이는 개인정보감독기구를 대통령 직속의 기구로 만들되 그 독립성을 보장해 주는 방안이다. 대통령 소속이라 함은 기관장 및 위원의 임명권자가 대통령으로, 위원의 신분은 보장되며, 위원회는 대통령에

709) 홍준형, 앞의 보고서, 111-112면 참조.

대해 직접 보고하는 것을 의미한다. 또한 기관의 운영상 독립성이 확보되어 인사상·재정상의 독립성이 확보된 경우를 독립위원회라고 할 수 있다. 이러한 감독기구는 프랑스 등 외국의 입법례에서도 찾아 볼 수 있다.

이 경우 대통령소속 독립위원회로 하는 경우, 비록 중앙행정기관은 아니지만 대통령에 대한 직접적인 정책보고와, 위원회의 보고를 토대로 대통령의 직접적인 지침하달로 인해 강력한 개인정보보호정책을 집행할 수 있고, 관련전문가들을 집중적으로 결집시킬 수 있기 때문에 전문성도 높아진다. 따라서 중앙행정기관 등 다른 행정기관이나 국가기관의 영향으로부터 비교적 독립적으로 개인정보보호정책을 수립·집행할 수 있게 된다.⁷¹⁰⁾

하지만 대통령의 직접적인 관여는 경우에 따라서 오히려 조직의 독립성을 저해하는 요인이 될 수도 있다. 그리고 헌법 제86조 제2항의 취지에 비추어 국무총리의 통할을 받지 않는 중앙행정기관의 설치에 정부조직의 체계정합성에 어긋날 소지가 있다. 그리고 집행과 감독의 기능을 직접 수행하는 행정기구를 대통령실에 설치하는 것은 집행력과의 연계성이 떨어지는 문제가 있을 수 있다. 다른 한편으로 독립성 확보가 반드시 자율성을 확보하는 것은 아니기 때문에 대통령 직속 독립위원회라 할지라도 대통령의 개인정보보호의 의지가 없으면 그 자율성 확보는 어려워지게 된다.

(3) 중앙행정기관화의 방안

중앙행정기관으로서 개인정보보호기구를 설치하는 방안은 정부와 분리된 독자적인 기구의 설립보다는 정부기구로 존속하게 하는 것이 더 제도의 실효성을 살릴 수 있다는 측면에서 강점이 있다. 하지만 기관의 인사권과 재정권이 타 부처에 의해 강하게 영향을 받기 때문

710) 홍준형, 앞의 보고서, 113면 참조.

에 독립위원회보다는 독립성의 확보가 부족할 수 있다. 또한 업무의 영역이 다르고 대등한 지위에 있는 다른 중앙행정기관의 개인정보침해행위를 제재하기 위한 강력한 집행력의 확보가 쉽지 않고, 선거를 통해 구성되는 지방자치단체에 대한 개인정보보호정책의 집행력 확보에도 어려운 점이 있다. 그리고 중앙행정기관화안도 대통령직속의 독립위원회 안처럼 기구설립의 용이성은 확보되기 어렵다. 감축관리와 작은정부 지향의 현대적 행정개혁의 조류 하에서 또 다른 중앙행정기관의 설립은 비판의 대상이 될 가능성이 크기 때문이다.⁷¹¹⁾

3. 검 토

먼저, 국가인권위원회에 개인정보보호업무를 총괄하도록 하는 방안은 권리구제기능이 정책기능과 분리됨으로써 효율적인 개인정보보호를 기할 수 없다는 문제가 있다. 더구나 국가인권위원회로서는 실효성 있는 행정적 지원이 불가능하다. 특히 국가인권위원회의 권고적 권한에 대해서는 회의적인 평가가 지배적이다. 실례로 교육부의 NEIS에 대한 국가인권위원회의 권고안이 제대로 수용되지 못하고 있거나 강남구에서의 CCTV설치 등이 현안으로 등장하고 있음에도 불구하고 국가인권위원회가 실효적인 대응을 하지 못하고 있다는 비판이 제기된 바 있다. 오히려 제3의 독자적인 인권기구로서의 특성에 비추어 볼 때 국가인권위원회라는 특별기구에서 개인정보보호업무에 전념하기 어려운 구조적 한계가 또 다른 문제점으로 지적될 수 있다.

다음으로, 대통령 소속하의 독립위원회 설치방안과 관련하여 만일 개인정보보호기구를 독자적인 제3의 기구로 설치한다면 정부로서는 또 다시 정부의 개인정보보호정책을 다루는 행정관청을 둘 수밖에 없을 것이다. 예컨대 방송의 독립성을 제고하기 위하여 설치된 과거의

711) 홍준형, 앞의 보고서, 112-113면 참조.

방송위원회가 제3의 독립기구로 설치됨으로 인하여 정부의 방송정책과의 직접적인 견련성을 확보하지 못하였던 점에서 교훈을 얻을 수 있을 것으로 생각한다. 그리고 헌법상 정부조직의 체계에 비추어 본다면 그 독립적인 성격에도 불구하고 집행과 감독의 기능을 직접 수행하는 행정기구를 대통령실에 설치하는 것은 바람직하지 않다. 헌법 제86조 제2항의 취지에 비추어 국무총리의 통할을 받지 않는 중앙행정기관의 설치에 비추어 정부조직의 체계정합성에 어긋날 소지가 있기 때문이다. 경우에 따라서는 대통령의 직접적인 관여가 오히려 조직의 자율성과 독립성을 위협하는 결과를 초래할 수도 있다.

오히려 정부의 개인정보보호정책의 일환으로서의 개인정보보호기구를 염두에 둔다면, 정부와 분리된 독자적인 기구의 설립보다는 정부기구로 존속하게 하는 편이 더 제도의 실효성을 살릴 수 있을 것으로 본다. 물론 독립위원회의 형태보다는 독립적인 직무수행을 기대하기 어렵고 다른 행정부처와의 관계에 있어서 집행력에 한계를 드러낼 수도 있다. 하지만 전술한 바와 같이 감독기구의 독립성을 좌우하는 결정적인 요인은 조직상의 독립성이 아니라 기능적 독립성이다. 따라서 기능적 독립성을 확보할 수 있다면, 기관을 어디에 소속시키느냐 하는 것은 오히려 부차적인 문제가 될 수 있다. 기구의 기능적 독립성을 확보하는 방도는 다만 임기제, 징계와 소추의 엄격한 제한, 정치적 중립성 보장, 의견제시, 조사권, 시정명령 등의 실질적 감독권한 보장 등을 통해 개인정보보호기구의 자율성과 독자성이 확보될 수 있도록 해야 할 것이다.

이러한 기능적 독립성을 확보하는 것을 전제로 할 때 국무총리 직속기구로서 개인정보보호위원회를 설치·운영하는 것은 한국적 법과 제도의 현실과 개인정보보호업무의 효율성을 기하기 위한 현실적 대안이 될 수 있다고 본다.

제 3 절 감독기구의 기능과 역할

감독기구의 권한과 관련하여 유럽의 경우 독임제를 취하든 합의제를 취하든 감시기능과 조사권한, 피해구제, 개인정보관리원칙의 준수와 관련된 시정명령권과 이와 관련된 사전예방적 조치, 자체적인 규칙제정권을 보유하는 것이 일반적으로 나타난다. 통합된 감독기구와 관련해 다음과 같은 기능과 권한의 보유가 검토되어야 한다.⁷¹²⁾

1. 감시기능과 조사권한

개인정보감독기구의 감시기능은 개인정보취급자가 법규정으로 구체화된 개인정보처리원칙을 위반되는지 여부를 추적하는 것을 말한다.

2. 시정권고 및 침해정지명령권

개인정보감독기구가 조사결과 개인정보취급자의 범위반 사실이 인정될 경우 당해 정보처리자에게 시정명령을 할 수 있는지 여부는 개인정보보호와 관련하여 기관의 핵심적인 기능 중 하나이다. 개인정보감독기구에 시정명령권이 부여된다면 개인정보의 실질적 보호기능은 크게 강화될 수 있을 것이다. 그러나 시정명령의 범위와 내용에 관해서 아무런 제한없이 개인정보감독기구가 시정명령을 내릴 수 있는 권한이 부여된다면, 개인정보감독기구는 시정명령을 통해서 정부와 민간기업들의 개인정보 정책과 구체적인 기술적 조치까지 좌지우지할 수 있을 수 있고, 특히 고객들과 밀접한 관계를 가지고 고객의 수요를 충족시켜 주어야 할 민간기업의 효율적 경영 자체에 개입함으로써 효율적 경영을 심각하게 위축시킬 수도 있다. 개인정보감독기구가 시

712) 이인호·권현영, “개인정보보호를 위한 통합감독기구의 설립방안”, 『2004 개인정보보호 정책포럼』, 2004. 6.

정명령을 통해서 민간기업의 경영을 대체할 수는 없다. 따라서 개인 정보감독기구에 포괄적인 시정명령권을 부여하는 것은 극도로 신중을 기해야 하고, 부여하더라도 포괄적인 내용의 시정은 권고하고 구체적인 침해정지는 명령할 수 있는 권한으로 국한되어야 할 것이 아닌가 생각된다. 다만, 개인정보침해정지명령에 대해서는 우선적인 효력(공정력)을 인정하여야 할 필요가 있다. 이러한 정지명령에 불복이 있는 경우 법원에 제소할 수 있을 것이다.

3. 피해구제기능과 분쟁조정권한

자신의 권리를 침해당한 정보주체에게 효과적이고 효율적인 권리구제를 하기 위해서는 감독기구가 통합적으로 일정한 구제기능을 수행할 필요가 있다.

4. 사전적 예방기능

개인정보감독기구는 사전적 예방기능으로서 예컨대 민감한 개인정보를 수집·처리하는 데이터베이스, 개인정보처리시스템간의 연동·결합 기타 개인정보처리의 위험성이 높은 개인정보처리시스템에 대하여 사전에 신고나 등록을 하게 하거나 또는 허가를 받도록 하여 그 시스템의 설계에서부터 개인정보처리원칙이 준수될 수 있도록 관여할 수 있어야 할 것이다.

5. 종합적인 정책 입안 기능 및 규칙제정권

감독기구는 개인정보보호를 위한 업무의 체계적이고 일관성 있는 추진을 위하여 종합적인 정책과 시책을 입안하고, 아울러 개인정보보호기본법과 개별 법률의 규정들을 집행함에 있어서 필요한 구체적인 시행규칙이나 영역별 가이드라인을 제정할 수 있어야 한다.

제 4 절 기존의 집행기구와의 관계설정

이렇게 향후 통합감독기구가 새로이 설립된다면, 통합감독기구가 공공기관과 민간기관의 개인정보처리에 대하여 최소한 예방적 기능, 사후적 민원해결기능, 정책조언기능을 모두 일괄해서 수행하되, 현재 공공부문과 민간부문에서 개인정보보호기능을 부분적이거나 수행하고 있는 각 집행기관들(행정안전부, 방송통신위원회, 금융감독위원회, 보건복지부 등)은 위 기능들을 통합감독기구로 넘기고 집행기능과 정책결정기능만을 수행하도록 하는 것이 바람직하다고 본다. 그리고 기존의 집행기관들은 통합감독기구와의 유기적인 협조관계를 유지하게 한다면, 보다 효과적이고 융통성 있는 개인정보보호체계를 구축할 수 있을 것이다. 감독기구 내지 정보보호기구의 중복은 개인정보의 보호에 관한 모순충돌을 초래할 수 있고 중복규제로 인해서 경영의 효율성을 크게 떨어뜨리며 개인정보의 활용과 유통을 심각하게 위축시킬 수 있다. 한편, 민간부문의 경우 개인정보분쟁조정위원회가 수행하는 분쟁조정기능은 통합감독기구로 이관되어야 할 것이다. 그리고 위에서 언급한 바와 같이 분쟁조정기능은 민원신청에 따른 조사기능과 분리될 수 없기 때문에, 현재 한국정보보호진흥원의 개인정보침해신고센터가 수행하는 민원접수 및 조사기능도 함께 통합감독기구로 이관되어야 할 것이다. 신용정보 분야의 감독기구라고 할 수 있는 금융위원회나 금융감독원은 어차피 지금도 신용정보보호를 위한 감독기능을 수행하고 있지 않기 때문에 그 기능을 통합감독기구로 이관하는 데 큰 어려움은 없을 것으로 보인다.⁷¹³⁾

하지만 통합감독기구가 존재한다고 해서 그것이 곧 바로 효과적인 개인정보보호체계의 확립으로 이어지는 것은 아니다. 공공부문과 민

713) 이인호, “프라이버시의 개념 및 역감시체계에 대한 분석과 전망”, 『제2회 미래 감시사회와 법 포럼』, 2006. 6. 15.

간부문의 그 수많은 개별 개인정보처리기관에 대해 한정된 자원의 통합감독기구가 일일이 감독기능을 수행할 수도 없다. 따라서 공공부와 주요 민간부문에 있어서 개인정보처리자로 하여금 내부적으로 독자적인 기능을 수행하는 개인정보보호책임자를 두도록 할 필요가 있다.

제 6 편
대안의 제시와 권고

제 1 장 입법체계에 대한 대안과 권고

제 1 절 대안의 제시

1. 대안 1: 분리형 일반법 제정 방안

현행의 공공기관개인정보보호법을 공공부문의 일반법으로 개정하고, 기타 민간부문에 산재한 법률들을 통합하여 민간부문에 적용될 일반법을 제정하는 방안이다.

이러한 입법의 체계를 채택할 경우 개인정보보호의 사각지대는 크게 우려하지 않아도 되는 장점이 있다. 하지만 법제를 정비하는 과정에서 소요되는 비용이 통합형 일반법주의에 비해 클 수밖에 없다는 것이 단점이다.

2. 대안 2: 통합형 일반법 제정 방안

공공부문과 민간부문을 통합한 입법체계를 지향하면서도 일반적으로 개인정보의 취급자가 준수해야 의무와 정보주체의 각종 권리 등에 관한 실체적 사항은 물론 권리행사의 방법과 절차, 피해구제, 감독기관 등 절차적 사항까지 폭넓게 규정하는 방안이다. 일반법에는 분야별 개별법에 특별한 규정을 두지 않을 경우에 대비하여 일차적으로 적용될 수 있는 사항들을 폭넓게 규정하게 되면, 개별법에서는 각 영역의 특수성에 맞게 개인정보보호방안을 강구할 수 있다.

이러한 점에서 현행의 법체계에 크게 변경을 가하지 않으면서도 법적 공백을 최소화할 수 있다는 점에서 매력적이다. 물론 이 경우에도 수범자의 혼란이나 보호체계상의 불균형을 최소화할 수 있는 장점이 있다. 또한 법제정의 비용이나 제정 이후 집행상의 비용도 그리 크지는 않을 것으로 예상된다.

3. 대안 3: 통합형 기본법 제정 방안

개인정보보호의 기본이념, 개인정보보호를 위한 국가의 책무와 시책, 기본개념의 정의, 공공부문과 민간부문에 공통되는 개인정보취급상의 기본원칙, 보호기구의 설치 등에 대해 규율하는 기본법을 두고 그 밖의 사항에 대해서는 개별법에 의해 규율하도록 하는 방안이다.

하지만 기본법의 체제를 취하면서도 각 부문별 일반법을 별도로 두지 않을 경우 다수의 개별법으로써 전 영역의 개인정보를 커버할 수 있어야 하는 부담이 생긴다. 아무리 많은 개별법을 제정하더라도 그들 입법의 보호범위에 속하지 않는 분야가 생겨날 경우에는 법적 보호의 공백이 발생할 수밖에 없다.

따라서 이러한 입법모델을 채택할 경우 개인정보보호기본법을 제정하는 외에도, 공공부문의 일반법과 민간부문의 일반법을 제정하기 위해 현행의 공공기관개인정보보호법, 정보통신망법, 신용정보법 등을 대폭 개정해야 하는 점에서 그에 소요되는 입법비용이 막대할 것으로 예상된다.

제 2 절 각 대안의 비교

1. 분리형 일반법제정론

현행의 공공기관개인정보보호법을 공공부문의 일반법으로 개정하고, 기타 민간부문에 산재한 법률들을 통합하여 민간부문에 적용될 일반법을 제정할 경우에는 ① 개인정보보호의 사각지대는 크게 우려하지 않아도 될 것이나(효율성), ② 법제를 정비하는 과정에서 소요되는 비용이 통합형 일반법주의에 비해 클 수밖에 없을 것이다(비용). ③ 공공부문과 민간부문에 각기 다른 법집행기구가 존재하게 되어 부문별

특성에 적합한 집행력을 신속하게 확보할 수 있는 장점이 있는 반면에, 양 부문을 포괄적으로 규율해야 하는 상황에서는 통일적 집행을 기대하기 어려운 단점이 있다(적용적합성). ④ 일반법이 부문별로 별도로 존재할 경우 수범자로서는 단일의 일반법의 체계에 비해 법제의 현황에 대한 인식의 정도나 관련 법제에 대한 접근가능성이 떨어질 수밖에 없을 것으로 판단된다(친숙성).

2. 통합형 일반법제정론

공공부문과 민간부문을 통합적으로 규율하면서도 개인정보보호에 필요한 일반적인 사항을 폭넓게 규정할 경우에는, ① 공공부문과 민간부문을 포괄하는 일반법의 제정으로 무엇보다도 법적 보호의 공백을 최소화할 수 있는 효과를 기대할 수 있다(효율성). ② 한 번의 입법으로 중복되는 법제를 모두 통폐합하는 효과가 있고, 일차적으로 적용될 수 있는 사항들을 폭넓게 규정함으로써 새로운 문제에 대응하기 위한 개별 법률의 제정을 수시로 해야 하는 번거로움을 덜어줄 수 있다. 이러한 점에서 후속적인 법률의 개정이나 빈번한 개별 법률의 제정에 따른 입법비용의 증대를 막을 수 있을 것으로 본다(비용). ③ 공공부문과 민간부문을 통할하는 하나의 법집행기구가 존재하게 되어 통일적 집행력의 확보가 용이하고, 특히 단일의 개인정보보호기구를 둘 경우 개인정보보호에 관한 종합적인 정책의 추진으로 법집행의 효율성이 증대될 것이다(적용적합성). ④ 단일의 통합형 일반법의 체계로 갈 경우 수범자로서는 개인정보보호법제의 현황에 대한 인식가능성이 높아지고 적용될 조항에 대한 접근이 용이해질 것을 충분히 예상해볼 수 있다(친숙성).

3. 통합형 기본법제정론

① 만일 기본법의 체제를 취하면서도 각 부문별 일반법을 별도로 두지 않을 경우에는 다수의 개별법으로써 전 영역의 개인정보를 커버할 수 있어야 하는 부담이 생긴다. 아무리 많은 개별법을 제정하더라도 그들 입법의 보호범위에 속하지 않는 분야가 생겨날 경우에는 법적 보호의 공백이 발생할 수밖에 없다(효율성). ② 개인정보보호기본법을 제정하는 외에도, 공공부문의 일반법과 민간부문의 일반법을 제정하기 위해 현행의 공공기관개인정보보호법, 정보통신망법, 신용정보법 등을 대폭 개정해야 하는 점에서 그에 소요되는 입법비용이 막대할 것으로 예상된다(비용). ③ 단일의 개인정보보호기구를 둘 경우 개인정보보호에 관한 종합적인 정책의 추진으로 법집행의 효율성이 증대될 것이나, 공공부문과 민간부문을 따로 관할하는 법집행기구를 둘 경우에는 통일적 집행력의 확보가 어려운 점이 있을 것이다(적용적합성). ④ 기본법 이외에 부문별 일반법이 존재할 경우 수범자로서는 통합형 일반법의 체계에 비해 개인정보보호법제의 현황에 대한 인식도나 적용 조항에 대한 접근도가 상대적으로 떨어지게 될 것으로 예상된다(친숙성).

4. 분석의 결론

각 입법체계적 특성을 법적 보호의 공백(효율성), 법제정비에 소요되는 비용(비용), 법집행과정의 용이성(적용적합성), 수범자의 이해가능성(친숙성) 등을 기준으로 서로 비교분석을 한 결과를 토대로 할 때, 통합형 일반법의 체계가 가장 유리하다는 결론을 도출할 수 있었다.

제 3 절 입법정책적 권고

1. 공·사 부문 통합형 입법의 지향

그동안 우리나라는 개인정보보호에 있어서 공공·민간부문 분리입법의 체계를 견지해 왔다. 여기에는 공공부문과 민간부문은 개인정보를 취급하는 이유와 방식이 다르다는 점, 개인정보의 침해로 인한 피해의 강도 또한 차이가 난다는 점 등이 고려된 것으로 보인다.

하지만 오늘날 개인정보의 처리양상은 어느 특정한 시간과 공간에 한정되지 않는다는 특징을 보이고 있다. 공공부문에서 생산된 개인정보도 언제든지 민간부문으로 흘러나갈 수 있고, 그것이 편집 또는 가공되거나 새로운 형태로 데이터베이스화되어 다시 공공부문으로 흘러들어가기도 한다. 이처럼 개인정보가 부문별 장벽에도 아랑곳하지 않고 자유롭게 유통될 수 있는 상황에서 개인정보보호의 문제를 부문별로 분리된 시스템에 의해 해결해나가는 것은 한계가 있을 수밖에 없다. 다시 말해 개인정보취급상의 원칙을 설정하고 정보주체의 권리를 보장하며, 개인정보침해로 인한 피해를 구제하기 위한 제도를 마련함에 있어서 민간부문과 공공부문을 나누어 별도의 법률로 규율하는 것은 바람직하지 못하다. 또한 민간부문의 경우 경제적 이익을 추구하는 과정에서 개인정보의 오용과 남용의 위험성이 오히려 더 클 수도 있는 것이다.

이러한 점에서 향후 제정될 개인정보보호법에서는 공공부문과 민간부문을 통합적으로 규율하는 방식을 취할 필요가 있다고 본다. 이 경우 개인정보보호에 관한 입법의 체계를 간명하게 하는 장점이 있으며, 수범자에게는 규범의 산만함에서 오는 법적 혼란을 막고 법제도에 대한 친숙감을 높여주는 효과가 있을 것으로 생각된다.

2. 통합형 일반법의 체계

앞의 장에서 살펴본 입법론들을 종합해 볼 때, 분리형 일반법제정론의 입장에서 현행의 공공기관개인정보보호법을 공공부문의 일반법으로 개정하고, 기타 민간부문에 산재한 법률들을 통합하여 민간부문에 적용될 일반법을 제정하는 방식을 채택할 경우 개인정보보호의 사각지대는 크게 우려하지 않아도 되는 장점이 있다. 하지만 법제를 정비하는 과정에서 소요되는 비용이 통합형 일반법주의에 비해 클 수밖에 없다는 것이 단점이다.

한편, 통합형 기본법제정론에 있어서는 기본법의 체제를 취하면서도 각 부문별 일반법을 별도로 두지 않을 경우 다수의 개별법으로써 전 영역의 개인정보를 커버할 수 있어야 하는 부담이 생긴다. 아무리 많은 개별법을 제정하더라도 그들 입법의 보호범위에 속하지 않는 분야가 생겨날 경우에는 법적 보호의 공백이 발생할 수밖에 없다. 기본법의 특성상 보충적인 성격의 실체적 사항까지 규정되어 있지 않을 것이기 때문이다. 또한 개인정보보호기본법을 제정하는 외에도, 공공부문의 일반법과 민간부문의 일반법을 제정하기 위해 현행의 공공기관 개인정보보호법, 정보통신망법, 신용정보법 등을 대폭 개정해야 하는 점에서 그에 소요되는 입법비용이 막대할 것으로 예상된다.

그에 비해 통합형 일반법의 입법체계는 현행의 법체계에 크게 변경을 가하지 않으면서도 법적 공백은 물론, 수범자의 혼란이나 보호체계상의 불균형을 최소화할 수 있는 장점이 있다. 또한 법제정의 비용이나 제정 이후 집행상의 비용도 그리 크지는 않을 것으로 예상된다. 이러한 점에서 개인정보보호법의 제정에 있어서는 공공부문과 민간부문을 모두 아우르는 통합형 일반법의 체계를 취하는 것이 바람직할 것으로 본다.

다만 행정, 교육, 금융, 의료, 노동 등 사회 각 분야별로 개인정보의 취급 양상 및 취급하는 개인정보의 내용은 모두 상이하므로 모든 분야에 대하여 구체적으로 적용하여야 할 사항을 하나의 법률에서 일률적으로 모두 규정하는 것은 곤란하다. 취급되는 개인정보의 성격에 따라서 법의 규율방식도 달라져야 하는 만큼, 특수분야에 대한 효과적 대처를 위해 개별법을 따로 두는 방향으로 갈 필요가 있다. 가령 영역별 특성에 맞추어 개인정보처리기관이 준수하여야 할 의무와 정보주체의 권리를 구체적이고 상세하게 규정하고 그 위반에 대해 행정 제재나 형사제재 등 집행수단을 규정하는 개별법이 다수 마련될 필요가 있다. 또한 새로운 기술력의 등장으로 인하여 특별한 보호가 요청되는 경우에는 분야별로 개별 입법을 통하여 기본법보다 더욱 엄격한 개인정보보호수준을 정하거나 신기술의 개발과 활용에도 유의할 수 있는 장치도 함께 마련할 수 있도록 배려하는 것이 필요하다고 본다.

3. 정보통신망법의 개인정보보호 관련 규정의 삭제

현행의 정보통신망법상 개인정보보호 관련 규정들은 일반법인 개인정보보호법과의 관계에 있어서 정보통신망이라는 특수한 영역을 규율하는 특별법적 지위를 가진다고 할 수 있다. 아울러 민간부문에서 개인정보보호법제가 불비한 현실에서 이들 규정은 정보통신서비스를 이용하는 자의 개인정보를 보호하는 일반법으로서의 성격도 가지는 것으로 인식되고 있다. 하지만 새롭게 개인정보보호법을 제정하려고 하는 시점에서 정보통신망법의 성격과 위상에 대한 재검토가 필요하다.

이와 관련하여 국회 과학기술정보통신위원회는 정보통신망법의 개인정보보호 관련 규정의 삭제를 내용으로 하고 있는 노회찬법안에 대해 다음과 같은 의견을 내놓고 있다. 즉, 개인정보보호기본법에서는 현재의 정보통신망법 등이 규율하지 못하는 사각지대를 해소한다는

차원에서 개인정보보호를 위한 기본적인 사항들만을 규정하되, 정보통신망에서와 같이 대량으로 개인정보가 수집·이용·전송되거나 개인정보의 오·남용 또는 유출시 대규모의 침해가 예상되는 경우에는 분야별로 개별 입법을 통하여 기본법보다 더욱 엄격한 개인정보보호수준을 정하도록 하는 것이 실효성의 측면에서도 바람직하다는 것이다.⁷¹⁴⁾

물론 정보통신망에서와 같이 대량으로 개인정보가 수집·이용·전송되거나 개인정보의 오·남용 또는 유출시 대규모의 침해가 예상되는 경우 특별 입법을 통하여 일반법에서보다 더욱 엄격한 개인정보보호수준을 정할 필요가 있을 것이다. 하지만 다른 한편으로 오늘날 개인정보보호의 주된 관심사는 고도의 정보통신기술에 의한 개인정보침해의 문제에 집중되고 있는 만큼, 이에 관한 사항을 더 이상 특별법의 영역에 둘 것이 아니라 통합기본법에서 일반적 사항으로 포섭하여 규정하는 편이 나을 것이다.

물론 통합기본법의 체계를 취한다고 하더라도 개별 영역별로 그 영역의 특성에 맞추어 개인정보처리기관이 준수하여야 할 의무와 정보주체의 권리를 구체적이고 상세하게 규정하고 그 위반에 대해 행정제재나 형사제재 등 집행수단을 규정하는 개별법이 다수 마련되어야 할 것이다. 그런데 이들 개별법의 적용영역은 보호의 대상이 되는 개인정보의 성격을 기준으로 결정되는 것이 바람직할 것이다. 이러한 점에서 신용정보보호법, 유전정보보호법, 위치정보보호법, 소비자정보보호법 등과 같은 개별입법은 통합기본법의 체제에서도 여전히 독자적 의의를 지닐 수 있다고 본다.

하지만 본격적인 정보화사회의 단계로 접어든 오늘날 대다수의 개인은 일상적으로 정보통신서비스를 이용할 수밖에 없고, 그에 따라 자신에 관한 일체의 정보가 인터넷 기타 정보통신망을 통해 처리되는

714) 과학기술정보통신위원회, 『개인정보보호기본법안(노회찬 의원 대표발의) 관련위원회 의견제시의 건 검토보고서』(2005. 4. 8), 10면 참조.

상황을 피해가기 어렵게 되었다. 이러한 점에서 개인정보 처리의 방법이나 수단은 더 이상 큰 의미를 가질 수 없다고 할 수 있으며, 오히려 정보통신망에 있어서의 개인정보보호는 더 이상 특수한 문제라기보다는 일반적인 법적 과제가 되었다고 하는 편이 옳을 것이다. 정보통신망법상의 개인정보보호 관련 규정이 민간부문에서의 개인정보 보호에 관한 일반법적 지위를 가지는 것으로 인식되고 있는 것도 이와 같은 맥락에서라고 할 수 있다. 그렇다면 정보통신서비스를 이용하는 자의 개인정보에 대해서는 이제 개별법을 통해 특수하게 규율할 것이 아니라, 새롭게 제정되는 통합기본법에서 보다 효과적이면서도 현실성 있는 개인정보보호의 방안을 마련할 필요가 있을 것이다. 이것은 개인정보보호의 행정체계를 일원화함으로써 이중규제를 방지하는 의미도 가질 수 있다.

4. 부문별 특칙의 필요성

개인정보의 보호와 활용의 양 측면을 함께 고려하는 개인정보보호 기본법을 지향한다고 할 때, 모든 수범 대상자가 자신이 취급하는 개인정보를 최대한으로 보호하면서도 각 분야의 정상적인 업무와 국민의 원활한 경제활동을 위축시키지 않을 수 있는 방안을 모색해야 할 것이다.

아무래도 공공부문과 민간부문에 있어서 개인정보는 각기 다른 목적으로 유통되거나 활용되는 양상을 보이는 것은 부인할 수 없는 것이 사실이다. 공공부문에서는 다양한 행정적 목적에 따라 국민 개개인에 관한 정보를 필요로 하지만, 이는 정보주체의 기본권을 공권력에 의해 제한하는 측면을 가지고 있기 때문에 국가로서는 개인정보의 침해상황에 대응하기 위한 사전적·사후적 규제장치를 강구할 필요가 있다. 이에 비하여 민간부문에 있어서는 정보주체의 자기결정에 따라

개인정보의 유통을 적극적으로 희망할 수도 있고, 심지어는 개인은 자신의 개인정보를 매개로 하여 재화나 용역상의 편익을 대가로 누리기를 선호하기도 한다. 이렇게 볼 때 민간 사이의 법률관계에 있어서는 사적 자치의 이념은 개인정보보호법제에 있어서도 강조될 수밖에 없다. 다른 한편으로 모든 사람은 원칙적으로 모든 타인에 대한 자신의 의견을 가질 권리를 가지며, 의사소통권의 행사에 있어서 타인에 관한 자신의 의견을 표현하고 타인의 개인정보를 타인에게 전달할 권리도 가지는 것이다.

또한 기업으로서도 시장조사를 통해 파악하거나 거래과정에서 정보주체에 의해 제공받은 개인정보를 활용함으로써 이윤을 증대시켜나갈 수 있는 권리도 있다고 봐야 할 것이다. 따라서 개인정보의 보호에 있어서도 가령 기업의 경우에는 영업의 자유, 종교단체의 경우에는 종교의 자유, 언론기관의 경우에는 언론·출판의 자유, 학술연구기관의 경우에는 학문의 자유 등과 같은 기본권적 가치를 존중할 필요가 있다. 이처럼 공공부문과 민간부문에서의 개인정보보호는 각자 기초하고 있는 법적 원리가 다를 수밖에 없는 것이다.

다른 한편으로 개인정보보호법이 민간부문에 대해서 공공부문과 대등한 수준의 개인정보보호 관련 의무를 부과할 경우 자칫 민간의 기업활동을 위축시켜 경제적·사회적 효율성을 저하시킬 가능성도 배제할 수 없다. 인터넷기업협회나 전국경제인연합 등에서 우려하듯이 정보통신 제조업 및 정보통신서비스 산업 등 관련 산업계, 특히 중소기업의 경쟁력이 약화되는 결과를 초래할 수도 있는 것이다. 따라서 개인정보보호법의 제정에 있어서는 관련 업계가 당면할 수 있는 이러한 여러 가지 애로사항도 충분히 배려하지 않으면 안 될 것이다.

위와 같은 사정들을 종합적으로 감안할 때, 개인정보보호법제에 있어서 공공부문과 민간부문에 대한 접근은 서로 다른 관점에서 이루어져야 할 필요가 있다. 이는 어떤 면에서 법으로 보호하려는 법익에

비례하는 규제수단을 선택하는 길이 될 수도 있을 것이다. 결론적으로 개인정보보호법에서는 민간부문의 특성을 고려하여 공공부문·민간부문에 대한 특칙을 두는 것이 바람직하다고 본다.

제 2 장 개인정보처리의 입법기준에 대한 대안과 권고

제 1 절 기본개념의 정의규정에 대한 수정대안

입법예고안	수정대안
<p>제 2 조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.</p> <p>1. “개인정보”란 생존하는 개인에 관한 정보로서 해당 정보에 의하여 개인을 식별할 수 있는 정보(해당 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다.</p> <p>2. “처리”란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위를 말한다.</p> <p>3. “정보주체”란 처리되는 정보에 의하여 식별되거나 식별될 수 있는 자로서 해당 정보의 주체가 되는 자를 말한다.</p> <p>4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다.</p>	<p>제 2 조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.</p> <p>1. “개인정보”란 생존하는 개인에 관한 정보 또는 그 정보의 묶음으로서, 그 정보 속에 포함되어 있는 개인의 성명, 식별번호나 부호, 또는 지문·사진·화상과 같은 당해 개인에게 고유한 식별자에 의하여 개인을 식별할 수 있는 정보를 말한다. 이 개인정보에는 당해 개인에 관하여 내린 다른 사람의 평가나 의견이 모두 포함된다.</p> <p style="text-align: center;"><적정함></p> <p style="text-align: center;"><적정함></p> <p>4. “개인정보처리시스템”이란 개인의 성명, 식별번호나 부호, 또는 지문·사진·화상과 같은 당해 개인에게 고유한 식별자에 의하여 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개</p>

입법예고안	수정대안
<p>5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 타인을 통하여 개인정보를 처리하는 자를 말한다.</p> <p>6. “공공기관”이란 다음 각 목의 기관을 말한다. (이하 생략)</p> <p>7. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치를 말한다.</p> <p style="text-align: center;"><추 가></p> <p style="text-align: center;"><추 가></p>	<p><u>인정보의 집합물을 말한다. 이 경우 개인정보들이 기능적으로 또는 지리적으로 한 곳에 통합되어 있든, 여러 곳에 분산되어 있든 그것은 문제 삼지 아니한다.</u></p> <p>5. “개인정보처리자”라 함은 업무를 수행할 목적으로 개인정보처리시스템을 자신의 책임 하에 관리·운용하는 자로서 개인정보처리의 목적·내용·방법을 결정하는 자연인, 법인, 공공기관 또는 그 밖의 단체를 말한다. 다만, 처리하는 개인정보의 양과 이용 방법에 비추어 정보주체의 권리나 이익을 해할 우려가 적은 경우로서 대통령령이 정하는 자는 제외한다.</p> <p style="text-align: center;"><적정함></p> <p style="text-align: center;"><적정함></p> <p>8. “정보처리대행자”란 개인정보처리자를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공기관 또는 그 밖의 단체를 말한다.</p> <p>9. “동의”란 자신의 개인정보가 처리되는 것을 승낙한다는 것을 나타내는 의사의 표시로서, 정보주체가 사전에 잘 알고 임의로 내린 분명한 의사표시를 말한다.</p>

제 2 절 수집 · 이용 · 제공의 허용기준에 대한 수정대안

1. 일반개인정보의 수집 · 이용 · 제공의 허용기준

입법예고안	수정대안
<p>제 4 조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.</p> <ol style="list-style-type: none"> 1. (생략) 2. <u>개인정보의 처리에 관한 동의, 동의범위 등을 선택하고 결정할 권리</u> 3. ~ 5. (생략) <p>제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 <u>이용할 수 있다.</u></p> <ol style="list-style-type: none"> 1. 정보주체의 동의를 받은 경우 2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 3. 공공기관이 소관 업무의 수행을 위하여 불가피한 경우 4. 계약의 이행을 위하여 불가피하게 수반되는 경우 5. 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체 	<p>제 4 조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.</p> <ol style="list-style-type: none"> 1. (생략) 2. <삭제> 3. ~ 5. (생략) <p>제15조(개인정보의 수집·이용·제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 <u>이용·제공할 수 있다.</u></p> <ol style="list-style-type: none"> 1. <동일> 2. 법률에 근거가 있거나 법령상 의무를 준수하기 위하여 <u>필요한 경우</u> 3. 공공기관이 소관 업무의 수행을 위하여 <u>필요한 경우</u> 4. 계약의 이행을 위하여 또는 계약체결에 앞서 정보주체의 요청에 따라 일정한 조치를 취하기 위하여 <u>정보처리가 필요한 경우</u> 5. 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 <u>정보처리가 필요한 경우</u>

입법예고안	수정대안
<p><u>의 사전 동의를 받기 곤란한 경우</u></p> <p>6. 개인정보처리자의 <u>정당한 이익을 달성하기 위하여 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우</u></p>	<p>6. 개인정보처리자나 개인정보를 제공하는 제3자가 추구하는 <u>정당한 이익을 달성하기 위하여 정보처리가 필요한 때. 다만, 그러한 이익보다 정보주체의 기본적인 자유와 권리를 보호해야 하는 이익이 더 클 때에는 그러하지 아니하다.</u></p>

2. 제3자 제공의 허용기준에 대한 외국 입법례와의 대비

입법예고안 (일반개인정보 - 공공/민간)	독일 연방개인정보보호법 (일반개인정보 - 민간부문)
<p>제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.</p> <ol style="list-style-type: none"> 1. 정보주체의 동의를 받은 경우 2. 제15조제1항제2호, 제3호 및 제5호에 따라 개인정보를 수집한 목적 범위 안에서 제공하는 경우 <p>② 개인정보처리자는 제1항에 따른 동의를 받을 때에는 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.</p> <ol style="list-style-type: none"> 1. 개인정보를 제공받는 자 2. 제공하는 개인정보의 항목 3. 개인정보를 제공받는 자의 개인 	<p>제28조(자신의 목적을 위한 개인정보의 수집, 처리 및 이용)</p> <p>① 자신의 업무목적을 달성하기 위한 수단으로서 개인정보를 수집, 저장, 수정, 제3자 제공 또는 이용하는 것은 다음 각 호의 1에 해당하는 경우에 허용된다.</p> <ol style="list-style-type: none"> 1. 정보주체와의 계약 또는 준계약적 신뢰관계를 위한 목적인 때 2. 개인정보처리자의 <u>정당한 이익을 보호하기 위하여 필요하고, 또한 그 처리나 이용을 하지 못하게 할 압도적인 <u>정당한 이익이 정보주체에게 있다고 볼 만한 근거가 전혀 없는 때</u></u> 3. 그 개인정보가 일반적으로 접근이 가능한 것인 때, 또는 개인정보처리

입법예고안 (일반개인정보 - 공공/민간)	독일 연방개인정보보호법 (일반개인정보 - 민간부문)
<p>정보 이용목적</p> <p>4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간</p> <p>③ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 제3자에게 제공하는 근거 및 제2항 각 호의 사항을 명확히 제시하여야 한다.</p> <p>제18조(개인정보의 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조 제1항 또는 제17조제1항에 따른 범위를 초과하여 이용하거나 제3자에게 제공하여서는 아니 된다.</p> <p>② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니하는 범위 안에서 개인정보를 목적 외로 이용하거나 제3자에게 제공할 수 있다. 다만, 제5호부터 제8호까지는 공공기관의 경우에 한한다.</p> <ol style="list-style-type: none"> 1. 정보주체로부터 별도의 동의를 받은 경우 2. 다른 법률에 특별한 규정이 있는 경우 3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 4. 통계작성 및 학술연구 등의 목 	<p>자가 합법적으로 개인정보를 공표할 수 있는 때. 다만, 그 정보처리를 배제해야 할 정보주체의 정당한 이익이 당해 개인정보처리자의 정당한 이익보다 명백히 우월한 때에는 그러하지 아니하다.</p> <p>개인정보를 수집할 때 정보처리의 목적은 구체적으로 명시되어야 한다.</p> <p>② 위 제1항 제1문 제2호 및 제3호의 요건이 충족되는 경우에 한하여, 수집된 개인정보는 다른 목적을 위하여 이용되거나 제공될 수 있다.</p> <p>③ 다른 목적을 위한 이용 또는 제공은 또한 다음 각 호의 경우에 한하여 적법하다.</p> <ol style="list-style-type: none"> 1. 제3자의 정당한 이익을 보호하기 위하여 필요한 때 2. 범죄의 수사를 위하여, 또는 국가안보나 공공의 안전에 대한 위협을 피하기 위하여 필요한 때 3. 광고, 시장조사 그리고 여론조사를 위한 목적인 때. 다만 이 경우 이용 또는 제공되는 개인정보는 일정 범위의 사람들에 관한 명부형식으로 된 개인정보여야 하고, 그에 포함되는 개인정보는 (a) 당해 정보주체가 그 명부에 포함되는지 여부, (b) 직업, (c) 이름, (d) 직책, (e) 대학학위, (f) 주소, 그리고 (g) 출생연도에 한정되어야 하며, 그리고 당해 정보주체가 그 제공이나 이용을 못하게 할 정당한 이익을 가지고 있다고 믿을

입법예고안 (일반개인정보 - 공공/민간)	독일 연방개인정보보호법 (일반개인정보 - 민간부문)
<p>적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우</p> <p>5. 개인정보를 목적 외로 이용하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의를 거친 경우</p> <p>6. 조약 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우</p> <p>7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우</p> <p>8. 법원의 재판업무수행을 위하여 필요한 경우</p> <p>③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 해당되는 사항을 정보주체에게 알려야 한다.</p> <p>1. 개인정보의 이용목적(제공시에는 제공받는 자의 이용 목적을 말한다)</p> <p>2. 개인정보의 보유 및 이용기간(제공시에는 제공받는 자의 보유 및 이용기간을 말한다)</p> <p>3. 개인정보를 제공받는 자</p> <p>4. 이용 또는 제공하는 개인정보의 항목</p> <p>④ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 근거 및 제3항 각 호의 해당되는 사항을 명확히 제시하여야 한다.</p>	<p>만한 근거가 일체 없어야 한다.</p> <p>4. 학문적 연구를 수행하는 연구기관의 이익을 위하여 필요한 때. 다만, 이 경우 그 연구를 수행하는 학문적 이익이 그 목적의 변경을 못하게 할 정보주체의 이익보다 월등히 우월해야 하고, 또한 그 연구의 목적이 비상한 노력이 없이는 다른 수단으로는 달성될 수 없는 것이어야 한다.</p> <p>④ 정보주체가 자신의 정보를 광고, 시장조사 또는 여론조사를 목적으로 이용 또는 제공하지 못하도록 개인정보처리자에게 <u>이의</u>를 제기하는 때에는, 그러한 목적의 이용 또는 제공은 허용되지 아니한다. 광고, 시장조사 또는 여론조사의 목적으로 연락을 받았을 때, 정보주체는 그 개인정보처리자의 신원과 자신의 거부권에 대하여 통지를 받아야 한다. 자신이 알지 못하는 개인정보처리자가 가지고 있던 개인정보를 이용하여 [위 목적으로] 연락을 취하는 자는 그 개인정보의 출처를 정보주체가 알 수 있도록 보장하여야 한다. 정보주체가 위 제3항에 의하여 개인정보를 제공받는 제3자에게 광고, 시장조사 또는 여론조사를 목적으로 하는 처리나 이용을 하지 못하도록 이의를 제기한 때에는, 그 수령인은 그 제공받은 개인정보가 위 목적으로 처리 또는 이용되지 않도록 차단시켜야 한다.</p> <p>⑤ 개인정보를 제공받은 제3자는 그</p>

입법예고안 (일반개인정보 - 공공/민간)	독일 연방개인정보보호법 (일반개인정보 - 민간부문)
<p>⑤ 공공기관은 제2항제2호부터 제8호까지에 따라 개인정보를 목적외로 이용하거나 제공하는 경우에는 그 이용 또는 제공의 법적 근거·목적 및 범위 등에 관하여 필요한 사항을 행정안전부령이 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.</p>	<p>제공받은 목적을 위해서만 그 정보를 처리하거나 이용할 수 있다. 민간기관이 다른 목적을 위하여 제공받은 개인정보를 처리하거나 이용하고자 하는 경우에, 위 제2항 및 제3항의 요건이 충족되는 때에 한하여 그것이 허용된다. 공공기관이 다른 목적을 위하여 제공받은 개인정보를 처리하거나 이용하고자 하는 경우에, 제14조 제2항의 요건이 충족되는 때에 한하여 그것이 허용된다. 제공하는 기관은 이 점을 그에게 알려주어야 한다.</p> <p>제29조(제3자 제공을 목적으로 하는 업무의 수행에 있어서 개인정보의 수집 및 기록)</p> <p>① 제3자 제공의 목적, 특히 광고, 정보제공서비스, 상업적인 주소목록작성, 시장조사나 여론조사를 목적으로 하는 업무를 수행함에 있어서 개인정보를 수집, 저장 또는 수정하는 것은 다음 각 호의 1의 경우에 허용된다.</p> <ol style="list-style-type: none"> 1. 자신의 개인정보가 수집, 저장, 수정되지 못하게 할 정당한 이익이 정보주체에게 있다고 볼만한 근거가 전혀 없는 때 2. 당해 개인정보가 일반적으로 접근이 가능한 출처로부터 얻을 수 있는 것이거나 또는 당해 개인정보처리자가 그 개인정보를 공표할 수 있는 권리가 있는 때. 다만, 자신의 개인정보가 수집, 이용 또는 처리되지 못하게 할 압도적인 정당한 이익이 정보주체에

제 6 편 대안의 제시와 권고

입법예고안 (일반개인정보 - 공공/민간)	독일 연방개인정보보호법 (일반개인정보 - 민간부문)
	<p>게 명백히 있는 경우에는 그러하지 아니하다.</p> <p>개인정보를 수집할 때 정보처리의 목적은 구체적으로 명시되어야 한다.</p> <p>② 위 제1항의 목적과 관련한 제3자 제공은 다음의 경우에 허용된다.</p> <p>1. (a) 개인정보를 제공받는 제3자가 그 개인정보를 알아야 할 정당한 이익을 확실하게 증명하거나 또는 (b) 제28조 제3항 제3호에 열거한 개인정보가 명부형식으로 편집되어 광고 또는 시장조사나 여론조사의 목적으로 제공되는 경우, 및</p> <p>2. 자신의 개인정보가 제3자에게 제공되지 못하게 할 정당한 이익이 정보주체에게 있다고 볼만한 근거가 전혀 없는 때.</p> <p>③ 생략</p> <p>④ 이 법 제28조 제4항 및 제5항은 제공받은 개인정보를 처리하거나 이용하는 경우에 적용된다.</p> <p>⑤ 제28조 제8항 및 제9항은 준용된다.</p>

일본 개인정보보호법 (일반/민감개인정보 공통 - 민간부문의 수집·이용·제공의 허용기준)
<p>제15조 (이용목적의 특정) ① 개인정보취급사업자는 개인정보를 취급함에 있어서 그 이용의 목적(이하 “이용목적”이라 한다)을 가능한 한 특정하여야 한다.</p> <p>② 개인정보취급사업자는 이용목적을 변경하는 경우에는 변경전의 이용목적과 상당한 연관성이 있다고 합리적으로 인정되는 범위를 초과해서 변경하여서는 아니 된다.</p>

일본 개인정보보호법 (일반/민감개인정보 공통 - 민간부문의 수집·이용·제공의 허용기준)
<p>제16조 (이용목적에 의한 제한) ① 개인정보취급사업자는, 미리 본인의 동의를 얻지 않고서는, 전조의 규정에 의해 특정된 이용목적의 달성에 필요한 범위를 넘어서 개인정보를 취급하여서는 아니 된다.</p> <p>② 개인정보취급사업자는, 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 아니 된다.</p> <p>③ 전 2항의 규정은 다음 각 호의 1에 해당하는 경우에는 적용하지 아니한다.</p> <ol style="list-style-type: none"> 1. 법령에 근거한 경우 2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우 3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위해 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 경우 4. 국가기관 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 경우. <p>제23조 (제3자 제공의 제한) ① 개인정보취급사업자는, 다음 각 호의 1에 해당하는 경우를 제외하고, 미리 본인의 동의를 얻지 않고서는 개인데이터를 제3자에게 제공하여서는 아니 된다.</p> <ol style="list-style-type: none"> 1. 법령에 근거한 경우 2. 사람의 생명, 신체 또는 재산의 보호를 위하여 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때 3. 공중위생의 향상 또는 아동의 건전한 육성의 추진을 위하여 특히 필요가 있는 경우로서, 본인의 동의를 얻는 것이 곤란한 때 4. 국가기관 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 때 <p>② 개인정보취급사업자는 제3자에게 제공되는 개인데이터에 대하여, 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지하는 것으로 하고 있는 경우에 있어서, 다음에 열거하는 사항에 대하여 미리 본인에게 통지하거나 또는 본인이 용이하게 알 수 있는 상태에 두고 있는 때에는, 전항의 규정에 불구하고, 당해 개인데이터를 제3자에게 제공할 수 있다.</p> <ol style="list-style-type: none"> 1. 제3자 제공을 이용목적으로 한다는 점

일본 개인정보보호법 (일반/민감개인정보 공통 - 민간부문의 수집·이용·제공의 허용기준)
<p>2. 제3자에게 제공되는 개인정보의 항목</p> <p>3. 제3자 제공의 수단 또는 방법</p> <p>4. 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인정보의 제3자 제공을 정지한다는 점</p> <p>③ 개인정보취급사업자는 전항 제2호 또는 제3호에 해당하는 사항을 변경하는 경우에는 변경하는 내용에 대해 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다.</p> <p>④ 다음 각호의 1에 해당하는 경우에 있어서 당해 개인정보의 제공을 받는 자는 전 3항의 규정의 적용에 대해서는 제3자에 해당하지 않는 것으로 한다.</p> <p>1. 개인정보취급사업자가 이용목적의 달성에 필요한 범위내에서 개인정보의 취급의 전부 또는 일부를 위탁하는 경우</p> <p>2. 합병 기타의 사유에 의한 사업의 승계에 수반하여 개인정보가 제공되는 경우</p> <p>3. 개인정보를 특정의 자와의 사이에서 공동으로 이용하는 경우로서, 그 취지 및 공동으로 이용되는 개인정보의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인정보의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때</p> <p>⑤ 개인정보취급사업자는, 전항 제3호에서 규정하는 이용하는 자의 이용목적 또는 개인정보의 관리에 대해 책임을 지는 자의 성명 혹은 명칭을 변경하는 경우에, 변경하는 내용에 대해 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다.</p>

3. 민감개인정보의 수집·이용·제공의 허용기준에 대한 외국 입법례와의 대비

입법예고안	독일 연방개인정보보호법 (민감개인정보 - 민간부문)
제22조(민감정보의 처리 제한) 개인정보보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건	제28조(자신의 목적을 위한 개인정보의 수집, 처리 및 이용) ①~⑤ 생략 (일반개인정보 참조)

입법예고안	독일 연방개인정보보호법 (민감개인정보 - 민간부문)
<p>강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보(이하 “민감정보“라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none"> 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 해당되는 사항을 알리고 별도의 동의를 받은 경우 2. 다른 법률에서 명시적으로 민감정보의 처리를 요구하거나 허용하는 경우 	<p>⑥ 자신의 업무목적을 위한 특수개인정보[제3조 제9항]715)의 수집, 처리 또는 이용은, 정보주체가 제4a조 제3항의 방식에 따라 <u>동의를 하지 않은 경우라 하더라도</u>, 다음 각 호의 1의 경우에는 합법적이다.</p> <ol style="list-style-type: none"> 1. 정보주체가 물리적으로 또는 법적으로 동의를 할 수 없는 경우에, 그 정보주체나 제3자의 중대한 이익을 보호하기 위하여 필요한 때 2. 문제의 특수개인정보가 정보주체에 의하여 공공의 영역에 명백히 놓이게 된 때 3. 법적 권리를 입증하거나 행사하거나 또는 방어하기 위하여 필요하고, 그 수집, 처리 또는 이용을 하지 못하게 할 압도적인 정당한 이익이 정보주체에게 있다고 믿을만한 근거가 전혀 없는 때 4. 학문적 연구를 수행하기 위하여 필요하고, 그 연구를 수행하는 학문적 이익이 그 수집을 하지 못하게 할 정보주체의 이익보다 월등히 우월하며, 그리고 그 연구의 목적이 비상한 노력이 없이는 다른 수단에 의해서 달성될 수 없는 때 <p>⑦ 특수개인정보 [제3조 제9항] 의 수집은 또한 다음의 경우, 즉 예방의학, 의학적 진단, 치료 또는 건강관리서비스의 제공을 위하여 필요하고, 또한 그 정보가 의료전문가 또는 그에 상응하는 비밀유지의무를 지는 자에 의하</p>

입법예고안	독일 연방개인정보보호법 (민감개인정보 - 민간부문)
	<p>여 처리되는 때에는 합법적이다. 위 제1문의 목적을 위한 특수 개인정보의 처리 및 이용은 위 제1문의 의료전문가 등이 지는 비밀유지의무에 따라 이루어져야 한다.</p> <p>⑧ 특수개인정보 [제3조 제9항] 는 다른 목적을 위하여 이용되거나 제공될 수 있는데, 다만 이 경우 제6항 제1호 내지 제4호의 요건이 충족되거나 또는 제7항 제1문의 요건이 충족되어야 한다. 중대 범죄의 수사를 위해서 또는 국가안보나 공공의 안전에 대한 상당한 위험을 피하기 위하여 필요한 때에는 그 이용이나 제공은 또한 합법적이다.</p> <p>⑨ 정치적, 학문적, 종교적 목적이나 노동조합의 목적을 가진 비영리단체는 그 단체의 활동을 위하여 필요한 때에는 특수개인정보 [제3조 제9항] 를 수집, 처리, 이용할 수 있다. 제1문은 그 단체 구성원들의 개인정보 또는 단체의 목적과 관련하여 정규적인 관계를 맺고 있는 사람들의 개인정보에 한해서만 적용된다. 이들 개인정보를 단체의 외부 사람이나 기관에게 제공하는 것은 오직 제4a조 제3항[정보주체의 동의방식]의 요건 하에서만 합법적이다. 위 제3항 제2호는 준용된다.</p>

715) “특수 개인정보라 함은 인종적 또는 민족적 출신, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강이나 성생활에 관한 기록을 말한다.” (제3조 제9항)

제 3 절 수집 · 이용 · 제공의 절차적 요건에 대한 수정대안

1. 목적명시 요건에 대한 수정대안

입법예고안	수정대안
<p>제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 <u>이용할 수 있다.</u></p> <p>1. ~ 6. (생략) <추 가></p> <p>② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.</p> <p>1. 개인정보의 수집·이용목적 2. 수집하고자 하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간</p> <p>③ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 수집·이용하는 근거 및 제2항 각 호의 사항을 명확히 제시하여야 한다.</p>	<p>제15조(개인정보의 수집·이용·제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 <u>이용·제공할 수 있다.</u></p> <p>1. ~ 6. (생략) <위 참조></p> <p>② 제1항의 경우 개인정보처리자는 <u>정당한 수집·이용 목적을 구체적이고 분명하게 명시하여야 하고, 그 명시한 목적 및 그와 합리적으로 연관성이 있는 다른 목적을 위해서 이용할 수 있다. 통계적 또는 학술적 목적을 위한 추가적인 이용은 명시한 목적과 합리적 연관성이 없는 것으로 취급되지 아니한다.</u></p> <p>② <아래 고지 요건 부분 참조></p> <p>③ <아래 고지 요건 부분 참조></p>

2. 품질관리 요건에 대한 수정대안

입법예고안	수정대안
<p><추 가></p>	<p>제16조의2(처리정보의 정확성) 개인정보 처리자는 수집·이용하는 개인정보를 정확하고 최신의 것으로 유지하도록 노력하여야 한다.</p>

유럽연합 개인정보보호지침상의 품질관리 요건 (공공/민간 공통)
<p>제 6 조(품질관리에 관한 원칙)</p> <p>(a) 개인기록은 공정하고 합법적으로(fairly and lawfully) 처리되어야 하며;</p> <p>(b) 개인기록(personal data)은 구체적이고 명시적이며 정당한 목적(specific, explicit and legitimate purposes)을 위하여 수집되어야 하고, 그 목적에 부합하지 않는 방식으로는(in a way incompatible with those purposes) 더 이상 처리되어서는 아니 된다. 적절한 안전장치(appropriate safeguards)가 있다면, 역사적, 통계적 또는 학술적 목적(historical, statistical or scientific purposes)을 위한 추가적인 정보처리는 ‘본래의 수집목적에 부합하지 않는 것’으로 간주되지 않는다.</p> <p>(c) 본래의 수집목적이나 추가적인 정보처리의 목적과 관련하여 개인정보는 그 목적에 적합하고, 관련성이 있어야 하며 과도해서는 아니 된다(adequate, relevant and not excessive).</p> <p>(d) 개인기록은 정확해야 하고(accurate), 필요한 때에는 최신의 것으로 갱신되어야 한다. 본래의 수집목적이나 추가적인 정보처리의 목적과 관련하여 부정확하거나 불완전한(inaccurate or incomplete) 개인정보는 삭제되거나 수정되어야 하는데, 이를 위해 필요한 모든 합리적인 조치가 취해져야 한다.</p> <p>(e) 개인기록은 본래의 수집목적이나 추가적인 정보처리의 목적에 필요한 기간 동안만(for no longer than is necessary) 정보주체의 신원확인이 가능한 형태로 유지되어야 한다.</p>

3. 고지 요건에 대한 수정대안

입법예고안	수정대안
<p>제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 <u>이용할 수 있다.</u></p> <p>1. ~ 6. (생략)</p> <p>② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.</p> <p>1. 개인정보의 수집·이용목적 2. 수집하고자 하는 개인정보의 항목 3. 개인정보의 보유 및 이용 기간</p> <p>③ 개인정보처리자는 정보주체의 요구가 있으면 개인정보를 수집·이용하는 근거 및 제2항 각 호의 사항을 명확히 제시하여야 한다.</p> <p style="text-align: center;"><신 설></p>	<p>제15조(개인정보의 수집·이용·제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 해당 수집목적 범위 안에서 <u>이용·제공할 수 있다.</u></p> <p>1. ~ 6. (생략) <위 참조> <삭 제></p> <p style="text-align: center;"><삭 제></p> <p>제15조의2(고지의 의무) ① 개인정보처리자는 정보주체로부터 직접 개인정보를 수집하는 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다만, 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급한 때에는 그러하지 아니하다.</p> <p>1. 개인정보처리자의 성명 또는 명칭 2. 개인정보의 수집·이용목적 3. 처리되는 개인정보의 종류와 범위</p> <p>② 개인정보처리자는 다른 출처로부터 개인정보를 수집하는 경우에는 수집한</p>

제 6 편 대안의 제시와 권고

입법예고안	수정대안
	<p>후 가능한 한 신속하게 제1항 각 호의 사항을 정보주체에게 통지하거나 공표하여야 한다. 다만, 미리 공표하고 있는 경우에는 그러하지 아니하다.</p> <p>③ 제1항과 제2항의 고지의무는 다음 각 호의 1에 해당하는 때에는 요구되지 아니한다.</p> <ol style="list-style-type: none"> 1. 고지함으로써 정보주체 또는 제3자의 생명, 신체, 재산 기타의 권리의 이익을 해할 가능성이 있는 경우 2. 고지함으로써 당해 개인정보처리자의 권리 또는 정당한 이익을 해할 가능성이 있는 경우 3. 고지함으로써 당해 개인정보처리자의 업무 수행에 지장을 줄 가능성이 있거나 과도한 노력이나 비용을 요하는 경우 4. 수집·이용이 법령에 의하여 명시적으로 규정되어 있는 경우

유럽연합지침상의 고지 요건	일본 개인정보보호법상의 고지 요건
<p>제10조 (정보주체로부터 직접 수집하는 경우의 고지사항) 정보주체로부터 직접 그의 개인정보를 수집하는 경우에, 당해 개인정보처리자는 적어도 다음의 사항을 제공해주어야 한다. 다만, 이미 정보주체가 알고 있는 경우에는 그러하지 아니하다.</p> <p>(a) 개인정보처리자와 그 대표자의 신원</p> <p>(b) 정보처리의 목적</p>	<p>제18조 (취득시 이용목적의 통지 등) ① 개인정보취급사업자는 개인정보를 취득한 경우에는, 미리 그 이용 목적을 공표하고 있는 경우를 제외하고, 신속히 그 이용 목적을 본인에게 통지하거나 공표하여야 한다.</p> <p>② 개인정보취급사업자는 전항의 규정에 불구하고 본인과 사이에 계약을 체결함에 따라 계약서 기타의 서면(電子的 방</p>

유럽연합지침상의 고지 요건	일본 개인정보보호법상의 고지 요건
<p>(c) 개인정보가 수집되는 구체적인 상황과 관련해서, 공정한 정보처리를 보장하기 위하여 추가정보가 필요한 경우에는, 다음의 추가정보</p> <p>i) 개인정보를 제공받는 자 또는 제공받는 자의 범위(categories of recipients)</p> <p>ii) 질문에의 답변이 의무적인지 아니면 임의적인 것인지 여부 및 답변하지 않았을 때 어떤 결과가 초래될 수 있는지</p> <p>iii) 열람권과 정정권이 있는지 여부</p> <p>제11조 (정보주체로부터 직접 얻은 것이 아닌 경우의 고지사항)</p> <p>1. 개인정보가 정보주체로부터 직접 얻은 것이 아닌 경우에, 다음의 사항을 사후에 알려주어야 한다. 그리고 알려주는 시점은 (i) 개인정보를 기록하는 때 또는 (ii) 제3자에게 제공이 예정되어 있는 경우에는, 적어도 처음의 제공이 이루어지기 이전이다.</p> <p>(a) 개인정보처리자와 그 대표자의 신원(identity)</p> <p>(b) 정보처리의 목적</p> <p>(c) 개인정보가 처리되는 구체적인 상황과 관련해서, 공정한 정보처리를 보장하기 위하여 추가정보가 필요한 경우에는, 다음의 추가정보</p> <p>i) 처리되고 있는 개인정보의 범위(the categories of data con-</p>	<p>식, 磁氣的 방식 기타 사람의 지각에 의해서는 인식할 수 없는 방식으로 작성된 기록을 포함한다. 이하 이 항에서 같다.)</p> <p>에 기재된 당해 본인의 개인정보를 취득하는 경우 기타 본인으로부터 직접 서면에 기재된 당해 본인의 개인정보를 취득하는 경우에는, 미리 본인에 대해 그 이용 목적을 명시하여야 한다. 다만, 사람의 생명, 신체 또는 재산의 보호를 위하여 긴급히 필요가 있는 경우에는 그러하지 아니하다.</p> <p>③ 개인정보취급사업자는 이용 목적을 변경한 경우에는 변경된 이용 목적에 대해 본인에게 통지하거나 공표하여야 한다.</p> <p>④ 전 세 항의 규정은 다음 각 호의 1에 해당하는 경우에는 적용하지 아니한다.</p> <p>1. 이용 목적을 본인에게 통지하거나 공표함으로써 본인 또는 제3자의 생명, 신체, 재산 기타의 권리의익을 해할 우려가 있는 경우</p> <p>2. 이용 목적을 본인에게 통지하거나 공표함으로써 당해 개인정보취급사업자의 권리 또는 정당한 이익을 해할 우려가 있는 경우</p> <p>3. 국가기관 또는 지방자치단체가 법령이 정하는 사무를 수행하는 것에 대하여 협력할 필요가 있는 경우로서, 이용 목적을 본인에게 통지하거나 공표함으로써 당해 사무의 수행에 지장을 줄 우려가 있는 경우</p> <p>4. 취득 상황에 비추어 이용 목적이 명확하다고 인정되는 경우</p>

유럽연합지침상의 고지 요건	일본 개인정보보호법상의 고지 요건
<p>cerned)</p> <p>ii) 개인정보를 제공받는 자 또는 제공받는 자의 범위(categories of recipients)</p> <p>iii) 열람권과 정정권이 있는지 여부</p> <p>2. 제1항은 다음의 경우에는 적용되지 아니한다.</p> <p>(a) 통계목적이나 역사적 또는 과학적 연구 목적을 위하여 정보처리가 수행되는 경우에, 고지가 불가능하다고 판명되거나, 고지하는 것이 너무 지나친 노력을 요하는 때, 또는</p> <p>(b) 기록이나 공개가 법에 의하여 명시적으로 규정되어 있는 때.</p> <p>이들 적용제외의 경우에 회원국은 국내법으로 적절한 안전장치를 마련하여야 한다.</p>	<p>제24조 (보유개인데이터에 관한 사항의 공표 등) ① 개인정보취급사업자는 보유개인데이터에 관해서 다음 각 호의 1에 해당하는 사항에 대하여 본인이 알 수 있는 상태(본인의 요청에 응해 지체 없이 회답하는 경우를 포함한다.)에 두어야 한다.</p> <ol style="list-style-type: none"> 1. 당해 개인정보취급사업자의 성명 또는 명칭 2. 모든 보유개인데이터의 이용목적(제18조 제4항 제1호 내지 제3호에 해당하는 경우를 제외한다) 3. 제24조 제2항, 제25조 제1항, 제26조 제1항 또는 제27조 제1항 혹은 제2항의 규정에 의한 요청에 응하는 절차(제30조 제2항의 규정에 의해 수수료의 액을 정한 때에는 그 수수료의 액을 포함한다) 4. 전 3호에 해당하는 것 이외에, 보유개인데이터의 적정한 취급의 확보에 관해 필요한 사항으로서 정령으로 정하는 것 <p>② 개인정보취급사업자는 본인으로부터 당해 본인의 식별이 가능한 보유개인데이터의 이용목적의 통지를 요청받은 때에는 본인에 대하여 지체 없이 그것을 통지하여야 한다. 다만, 다음의 각호 중 어느 하나에 해당하는 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none"> 1. 전항의 규정에 의하여 당해 본인의 식별이 가능한 보유개인데이터의 이용목적에 명확한 경우 2. 제18조 제4항 제1호 내지 제3호에 해당하는 경우

유럽연합지침상의 고지 요건	일본 개인정보보호법상의 고지 요건
	③ 개인정보취급사업자는 전항의 규정에 근거하여 요청된 보유개인데이터의 이용 목적을 통지하지 않는다는 취지의 결정을 한 때에는 본인에 대하여 지체 없이 그 취지를 통지하여야 한다.

제 4 절 공공기관의 개인정보처리기준에 대한 권고

1. 고지 요건의 명시화 필요

입법예고안	미국 연방프라이버시법 (공공부문 - 고지 요건)
<민간 또는 공공기관이 개인정보를 수집할 때 그 수집목적 등에 관하여 고지의무를 지우고 있지 않음. 제15조 제2항은 <u>정보주체의 동의를 받는 경우에만</u> ‘수집목적, 개인정보의 항목, 보유 및 이용기간’의 사항을 정보주체에게 알려주도록 하고 있을 뿐임>	5 U.S.C. §552a(e) (2) 수집되는 정보가 당해 개인의 권리 (rights), 복지혜택(benefits), 그리고 연방프로그램에서 인정되는 특권(privileges)에 관하여 불리한 결정을 초래할 수 있는 때에는, 당해 정보주체로부터 가능한 한 직접(to the greatest extent practicable directly from the subject individual) 수집하여야 한다. (3) 정보를 제공하라고 요청한 각 개인에게 다음 각 호의 사항들을 당해 정보를 수집할 때 사용한 그 양식이나 아니면 당해 개인이 계속 가질 수 있는 별도의 양식을 통해 알려주어야 한다. (A) 당해 정보의 요청을 승인하는 법

입법예고안	미국 연방프라이버시법 (공공부문 - 고지 요건)
	적 근거(법률 또는 대통령의 집행명령) 및 그 정보의 제공이 강제적인(mandatory) 것인지 임의적인(voluntary) 것인지의 여부 (B) 의도하는 당해 정보의 이용목적 (C) 본 (e)항의 (4)(D)에 따라 공표되는 바대로, 있을 수 있는 당해 정보의 일상적 이용(routine uses) (D) 요청된 정보의 전부 또는 일부를 제공하지 않는 경우 당해 개인에게 미칠 효과 (혹시 있다면).

2. 개인정보 공동이용의 규율에 대한 권고

첫째, 현행 「공공기관의 개인정보보호에 관한 법률」이나 입법예고된 「개인정보보호법 제정법률(안)」에도 개인정보DB의 연동 내지는 연계를 통한 개인정보 공동이용에 대한 규율이 없다. 다만, 행정안전부는 2008년 9월 5일 입법예고한 「전자정부법 전부개정법률안」의 제4장에서 “행정정보의 공동이용”이라는 제목 하에 제32조에서 제41조에 걸쳐 구체적으로 규율하고 있다. 이 공동이용에 관한 규율을 일반법으로 입법예고된 「개인정보보호법 제정법률(안)」에서 다루는 것이 입법체계상 적절할 것으로 평가된다.

둘째, 현행의 「전자정부법」과 입법예고된 「전자정부법 전부개정법률안」은 모두 개인정보의 공동이용을 전자정부의 핵심개념으로 상정하고 있고, 정부도 행정정보공유추진위원회와 행정정보공동이용센터를 설치해 범정부적 차원에서 적극적으로 추진해 나가고 있다. 그러나 개인정보 공동이용을 전자정부의 필수조건이자 기본개념으로 전제하

고 있는 것에 대하여 진지한 재검토가 필요하다. 특히 「전자정부법 전부개정법률안」은 각 행정기관이 자신의 소관업무를 수행하기 위하여 각자 별도로 구축·운영하고 있는 개인정보DB를 통합적으로 연동 내지는 연계할 수 있는 가능성을 열어주고 있는 것으로 보여 상당한 우려를 낳을 것으로 보인다. 그러나 정부가 보유하고 있는 수많은 개인정보DB를 시스템적으로 통합이 가능하도록 허용하는 것은, 설령 그것이 실제로는 부분적이고 일시적인 연계에 의한 개인정보의 공동이용이라 하더라도, 개별적으로 제3자 제공을 허용하는 것과는 비교할 수 없을 정도의 위험성을 안고 있는 문제이다. 개인정보 공동이용을 전자정부의 핵심개념이자 기본전제로 여기는 사고는 정부기능의 효율성만을 강조한 것으로서 행정의 민주성과 투명성의 가치를 경시한 것으로 평가될 수 있다. 비교법적으로 미국은 행정기관간의 개인정보의 컴퓨터결합(computer matching)을 개별적으로만 제한적으로 허용하고 있다. 그러면서 내부적인 절차적 안전장치를 상세하게 마련해 놓고 있다.

셋째, 「전자정부법 전부개정법률안」은 공동이용의 승인절차의 대상이 되는 행정정보를 “개인정보가 포함된 행정정보”라고 규정하고 있는데, 그러나 이 개념은 너무 포괄적이다. 또한 법률안은 공동이용에 대한 승인 등의 통제를 받는 대상정보를 무단히 “행정정보”라고 하고 있는데, 차라리 “개인정보”라고 하는 것이 혼란을 초래하지 않을 것으로 보인다. 그리하여 제34조의 제목도 “개인정보 공동이용의 승인”이라고 하는 것이 정직하다.

제 3 장 집행체계에 대한 대안과 권고

제 1 절 일반적 대안과 권고

1. 독립적 개인정보보호기구의 설치

오늘날 개인정보의 수집과 처리의 기법이 다양화되었고 교묘해지면서, 개인은 자신에 관한 정보를 쉽사리 통제하기 어렵게 되었다. 무엇보다도 자신에 관한 정보가 언제 어디서 어떻게 수집되고 처리되며 활용되는지를 그 정보의 주체가 인식하기 어렵기 때문이다.

이러한 상황에서 개인정보자기결정권의 효과적 보장을 위한 국가적 노력은 그 어느 때보다도 중요하다. 여기서는 물론 개인정보 침해자로서의 국가가 아니라 개인정보보호의 책임자로서의 국가가 강조된다. 즉 개인정보보호를 위한 국가의 책무는 개인정보를 스스로 침해하는 일이 없도록 주의를 기울이는 소극적 측면에 머물지 않고, 개인정보침해의 가능성에 대처하기 위한 법적·제도적 방안을 확충해야 하는 적극적 측면에까지 미치는 것이다.

이러한 적극적 책무에는 기술적·조직적 안전대책을 마련하는 것도 포함되어야 한다. 특히 조직적 안전망의 구축과 관련하여서는 개인정보의 침해를 예방하고 정보주체의 통제권 행사를 원조하기 위하여 개인정보보호에 관한 업무를 전담하는 독립적 조직을 설치·운영하는 것이 필요하다.

이러한 기구는 개인정보침해의 가능성을 면밀히 점검하여 예방책을 제시할 수 있을 정도의 전문적 식견을 가진 사람들로 구성될 때 그리고 개인정보보호법의 준수를 지도·감독하며 분쟁발생시 당사자간의 원만한 해결을 위해 관여하는 등의 권한이 부여될 때 그 실효성을 기대할 수 있을 것이다.

2. 개인정보보호기구의 기능

개인정보감독기구는 공공부문과 민간부문의 정보처리를 지속적으로 체크하고 법률에 규정된 목표를 준수하는지 감독하여야 한다. 나아가 개인정보감독기구는 개인정보침해의 위협을 느끼는 국민의 권리를 보호하는 역할을 수행하여야 한다. 그리고 다양한 방법을 통하여 국가 및 민간기업의 정보처리과정에서 개인정보가 보호될 수 있도록 일반적이고 체계적인 감독과 대안제시를 위하여 노력하여야 한다. 이를 통하여 새로운 정보통신기술의 도입이 개인의 자율을 희생시키면서 더욱 더 정교하고 통합된 개인정보시스템을 만들 위험성을 막아야 한다. 따라서 개인정보감독기구는 새로운 정보기술형태의 잠재적 영향력과 효과를 판단하여서 이러한 정보통신기술의 적용이 계획단계에서부터 개인정보보호와 조화될 수 있도록 노력하여야 한다. 이에 따라서 개인정보감독기구에는 상담과 조정기능 외에 위협예방기능이 요구된다. 그리고 개인정보처리와 관계되는 중요사항에 대하여 매년 국회에 연차보고서를 제출하고, 개인정보보호와 관련되는 사안에 대하여 여론매체 등을 이용하여 널리 알리고 시민에게 홍보하여야 한다.

3. 개인정보보호기구의 소속

(1) 대안 1: 국가인권위원회의 부서로 하는 방안

별도의 기구를 설립하여 운영하는 것보다 기존의 국가인권위원회에서 개인정보보호업무를 총괄하도록 하자는 방안은 국가인권위원회의 독립성으로 인해 강한 독립성의 확보가 가능하고, 신규조직을 별도로 설립할 필요가 없다는 측면에서 정부조직 확대에 따른 부담을 줄여 기구설립이 비교적 용이한 편이다. 하지만 권리구제기능이 정책기능과 분리됨으로써 효율적인 개인정보보호를 기하기 어렵다는 문제가

있고, 제3의 독자적인 인권기구로서의 특성에 비추어 볼 때 국가인권 위원회라는 특별기구에서 개인정보보호업무에 전념하기 어려운 구조적 한계가 있다.

(2) 대안 2: 대통령 소속 독립위원회 설치방안

개인정보감독기구를 대통령 직속의 기구로 만들되 그 독립성을 보장해 주는 방안은 중앙행정기관 등 다른 행정기관이나 국가기관의 영향으로부터 비교적 독립적으로 개인정보보호정책을 수립·집행할 수 있으며, 대통령의 직접적인 지침하달로 인해 강력한 개인정보보호정책을 집행할 수 있다. 또한 관련전문가들을 집중적으로 결집시킬 수 있기 때문에 전문성도 높아진다는 장점도 있다.

하지만 대통령의 직접적인 관여는 경우에 따라서 오히려 조직의 독립성을 저해하는 요인이 될 수도 있다. 그리고 헌법 제86조 제2항의 취지에 비추어 국무총리의 통할을 받지 않는 중앙행정기관의 설치에 정부조직의 체계정합성에 어긋날 소지가 있다. 그리고 집행과 감독의 기능을 직접 수행하는 행정기구를 대통령실에 설치하는 것은 집행력과 연계성이 떨어지는 문제가 있을 수 있다. 다른 한편으로 독립성 확보가 반드시 자율성을 확보하는 것은 아니기 때문에 대통령 직속 독립위원회라 할지라도 대통령의 개인정보보호의 의지가 없으면 그 자율성 확보는 어려워지게 된다.

(3) 대안 3: 중앙행정기관화의 방안

중앙행정기관으로서 개인정보보호기구를 설치하는 방안은 정부와 분리된 독자적인 기구의 설립보다는 정부기구로 존속하게 하는 것이 더 제도의 실효성을 살릴 수 있다는 측면에서 강점이 있다.

하지만 기관의 인사권과 재정권이 타 부처에 의해 강하게 영향을 받기 때문에 독립위원회보다는 독립성의 확보가 부족할 수 있다. 또

한 업무의 영역이 다르고 대등한 지위에 있는 다른 중앙행정기관의 개인정보침해행위를 제재하기 위한 강력한 집행력의 확보가 쉽지 않고, 선거를 통해 구성되는 지방자치단체에 대한 개인정보보호정책의 집행력 확보에도 어려운 점이 있다. 그리고 중앙행정기관화안도 대통령직속의 독립위원회 안처럼 기구설립의 용이성은 확보되기 어렵다. 감축관리와 작은 정부 지향의 현대적 행정개혁의 조류 하에서 또 다른 중앙행정기관의 설립은 비판의 대상이 될 가능성이 크기 때문이다.⁷¹⁶⁾

(4) 각 대안의 검토

국가인권위원회에 개인정보보호업무를 총괄하도록 하는 방안은 권리구제기능이 정책기능과 분리됨으로써 효율적인 개인정보보호를 기할 수 없다는 문제가 있다. 국가인권위원회는 행정적 지원을 하기 어려우며, 특히 그 권고적 권한에 대해서는 실효성에 적잖은 의문이 제기되고 있는 실정이다. 또한 인권 전반에 관한 업무를 총괄하다 보면 개인정보의 보호에 대한 집중력은 아무래도 떨어질 수밖에 없을 것이다.

한편, 개인정보보호기구를 대통령 직속의 독자적인 제3의 기구로 설치할 경우 정부의 개인정보보호정책과 연계성을 갖추기 위해 별도의 전담 행정관청을 필요로 할 것이다. 그리고 헌법상 정부조직의 체계에 비추어 본다면 집행과 감독의 기능을 직접 수행하는 행정기구를 국무총리의 통할을 받지 않는 조직으로 두는 것은 바람직하지 않다.

오히려 개인정보보호의 정책이 실효적인 집행력을 확보하기 위해서는 정부와 분리된 독자적인 기구의 설립보다는 정부기구로 존속하게 하는 편이 더 나을 것으로 본다. 다만 임기제, 징계와 소추의 엄격한 제한, 정치적 중립성 보장, 의견제시, 조사권, 시정명령 등의 실질적 감독권한 보장 등을 통해 개인정보보호기구의 자율성과 독자성이 확보될 수 있도록 해야 할 것이다.

716) 홍준형, 앞의 보고서, 112-113면 참조.

이러한 기능적 독립성을 확보하는 것을 전제로 할 때 국무총리 직속기구로서 개인정보보호위원회를 설치·운영하는 것은 한국적 법과 제도의 현실과 개인정보보호업무의 효율성을 기하기 위한 현실적 대안이 될 수 있다고 본다.

4. 감독기능의 일원화

이렇게 향후 통합감독기구가 새로이 설립된다면, 현재 공공부문과 민간부문에서 개인정보보호기능을 부분적이거나 수행하고 있는 각 집행기관들(행정안전부, 방송통신위원회, 금융감독위원회, 보건복지부 등)은 위 기능들을 통합감독기구로 넘기고 집행기능과 정책결정기능만을 수행하도록 하는 것이 바람직하다고 본다. 또한 민간부문의 경우 개인정보분쟁조정위원회가 수행하는 분쟁조정기능은 통합감독기구로 이관되어야 할 것이다. 그리고 분쟁조정기능은 민원신청에 따른 조사기능과 분리될 수 없기 때문에, 현재 한국정보보호진흥원의 개인정보침해신고센터가 수행하는 민원접수 및 조사기능도 함께 통합감독기구로 이관되어야 할 것이다. 그와는 별도로 공공부분과 주요 민간부분에 있어서 개인정보처리자로 하여금 내부적으로 독자적인 기능을 수행하는 개인정보보호책임자를 두도록 할 필요가 있다.

제 2 절 구체적 수정안의 제시

(신)이혜훈 법안은 집행과 감독의 체계에 있어서 개인정보의 활용 및 보호의 양 측면을 비교적 잘 절충하고 있는 것으로 파악되는바, 이를 기본적인 모델로 삼아도 무방할 것으로 판단된다. 다만 그 개인정보보호기구의 명칭을 ‘개인정보위원회’에서 ‘개인정보보호위원회’로 고치고, 세부적인 내용을 약간 수정하는 정도로 대안을 제시하고자 한다.

제 6 조(개인정보처리방침의 공개) ⑤개인정보보호위원회는 개인정보처리방침을 위반하여 개인정보를 처리한 개인정보처리자에 대하여 시정을 권고하거나 그 밖의 필요한 조치를 명할 수 있다.

제 7 조(표준개인정보처리방침의 사용 및 표시) ①사업자단체 또는 2 이상의 개인정보처리자가 특정 분야에서 개인정보처리의 기준이 될 개인정보처리방침(이하 “표준개인정보처리방침”이라 한다)을 정한 때에는 미리 개인정보보호위원회에 등록하여야 한다.

②개인정보보호위원회는 개인정보피해가 빈발하거나 다수의 정보주체의 피해가 예상되는 분야에 대하여 표준개인정보처리방침을 마련하여 등록할 것을 권고할 수 있다.

③개인정보보호위원회는 제1항 및 제2항의 규정에 의하여 등록을 받은 표준개인정보처리방침이 이 법에 위반되지 않는다고 판단할 때에는 지체 없이 등록증을 교부하고 이를 공시하여야 한다.

④개인정보보호위원회는 표준개인정보처리방침이 이 법의 취지에 위반된다고 판단한 때에는 변경을 권고하거나 그 밖의 필요한 조치를 명할 수 있다.

⑤개인정보보호위원회는 표준개인정보처리방침의 사용을 활성화하기 위하여 필요한 경우에는 당해 개인정보처리방침이 표준개인정보처리방침임을 나타내는 표시(이하 “표준개인정보처리방침표시”라 한다)를 정하여 고시할 수 있다.

제12조(고유식별정보의 보호) ②개인정보처리자는 제1항 각 호에 해당하는 경우에도 고유식별정보 이외의 수단 또는 방법(이하 “대체수단”이라 한다)으로 신분·연령 등의 확인이 가능한 경우에는 대체수단을 강구하여 정보주체가 선택할 수 있게 하여야 한다.

③ 개인정보보호위원회는 제2항에 따라 대체수단을 강구해야 할 개인정보처리자의 범위를 정하여 고시할 수 있다.

제17조(영리목적의 개인정보 이용 및 제공) ① 개인정보처리자가 개인정보를 이용하여 다음 각 호의 어느 하나에 해당하는 사업을 영위하고자 하는 경우에는 미리 개인정보보호위원회에 등록하여야 한다.

1. 마케팅 등 대행사업 : 개인정보를 이용해 영리목적으로 다른 사람의 선전·광고, 마케팅, 시장조사, 여론조사, 상품 또는 서비스의 판매, 회원가입 등을 대행·대리·중개해 주는 사업
2. 개인정보제공사업 : 영리목적으로 다른 사람에게 개인정보를 제공하는 사업

제20조(개인정보 누출등의 통지 및 신고) ① 개인정보처리자는 개인정보가 누출·공개·도용(이하 “누출등”이라 한다)된 사실을 안 때에는 즉시 피해를 최소화하기 위한 조치를 취하고 누출등된 개인정보의 항목, 누출등의 일시, 피해예방 및 확산방지 방법, 피해구제절차 등을 대통령령이 정하는 바에 따라 해당 정보주체에게 알려야 한다.

② 개인정보처리자가 제1항의 조치등을 취한 경우에는 그 결과를 지체없이 개인정보보호위원회에 신고하여야 한다. 이 경우 개인정보보호위원회는 피해확산방지, 피해복구 등을 위한 기술을 지원할 수 있다.

제28조(개인정보보호단체 등의 등록 및 지원) ① 다음 각 호의 업무를 수행하고자 하는 개인정보보호단체 또는 사업자단체(이하 “개인정보보호단체 등”이라고 한다)는 대통령령이 정하는 바에 따라

개인정보보호위원회에 등록할 수 있다.

1. 개인정보처리와 관련한 상담 및 정보제공
2. 개인정보처리와 관련한 불만처리 및 피해구제
3. 개인정보처리에 관한 실태 조사 및 연구
4. 개인정보보호에 관한 교육 및 홍보
5. 개인정보보호정책의 연구 및 건의
6. 개인정보보호기술의 개발 및 보급
7. 그 밖에 개인정보보호를 위하여 대통령령이 정하는 업무

⑤ 개인정보보호위원회는 등록된 개인정보보호단체 등의 건전한 발전을 위하여 예산의 범위 안에서 필요한 지원을 할 수 있다.

⑥ 개인정보보호위원회는 이 법의 시행에 필요한 범위 안에서 개인정보보호단체 등에 대하여 해당 업무에 관한 보고를 하게 할 수 있다.

제31조(개인정보파일의 등록) ① 공공기관이 개인정보파일을 구축·운영하고자 하는 때에는 미리 개인정보보호위원회에 다음 각 호의 사항을 등록하여야 한다.

1. 개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 정상적으로 제공하는 경우에는 그 제공받는 자
7. 그 밖에 대통령령이 정하는 사항

② 개인정보보호위원회는 개인정보파일의 등록대장을 작성·비치하고 누구든지 쉽게 열람할 수 있도록 이를 공개하여야 한다.

③공공기관은 제1항 각 호의 어느 하나에 변경이 있는 경우에는 지체 없이 변경사실을 개인정보보호위원회에 신고하여야 한다.

④제1항에도 불구하고 개인정보파일의 보유 여부를 공개하는 것이 국가안보 또는 외교에 중대한 영향을 미칠 우려가 있는 경우로서 개인정보보호위원회가 인정한 때에는 개인정보파일의 등록을 면제할 수 있다.

제32조(개인정보영향평가) ①공공기관이 대통령령에서 정하는 개인정보파일을 새로 구축하거나 확대 또는 변경하고자 하는 경우 또는 다른 개인정보파일과 연계하거나 연동하고자 하는 경우에는 다음 각 호의 모든 사항을 고려하여 미리 그것이 개인정보에 미칠 영향을 평가(이하 “영향평가”라 한다)하여야 한다.

1. 취급하는 개인정보의 양과 내용
2. 개인정보의 제3자 제공 여부
3. 개인정보파일의 연동·연계 여부
4. 정보주체의 권리를 해할 가능성
5. 그 밖에 대통령령으로 정한 사항

②개인정보보호위원회는 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 해당 공공기관으로 하여금 영향평가를 실시하도록 권고할 수 있다.

1. 제1항의 사유가 발생하였음에도 해당 공공기관이 사전평가를 실시하지 아니한 경우
2. 해당 공공기관이 운영하고 있는 개인정보파일과 관련하여 개인정보 유출·도용·오남용 등의 사례가 자주 발생한 경우
3. 해당 공공기관이 운영하거나 운영하고자 하는 개인정보파일과 관련하여 개인정보의 유출·도용·오남용 위험이 현저히 우려되는 경우

③제1항과 제2항의 규정에 따라 영향평가를 받은 공공기관은 평가결과를 대통령령이 정하는 바에 따라 지체 없이 개인정보보호위원회에 제출하여야 하며 개인정보보호위원회는 이를 대통령령이 정하는 방법에 따라 일반인에게 공개하여야 한다.

④공공기관은 영향평가를 제52조제1항의 규정에 의하여 지정된 지정평가·인증기관에 의뢰하여 할 수 있다.

⑤개인정보파일의 확대, 변경 등이 경미한 경우에는 그 사실을 개인정보보호위원회에 통지하고 제1항의 규정에 의한 영향평가를 생략할 수 있다.

제33조(개인정보파일의 연동 등) ①개인정보처리자가 자동으로 처리되는 개인정보파일을 다른 개인정보파일과 대조하여 처리하거나 처리하게 할 목적으로 상호 연계 또는 연동하고자 하는 경우에는 다음 각 호의 모든 사항을 사전에 개인정보보호위원회와 협의하여야 한다.

1. 연동의 목적
2. 연동기관
3. 연동하는 개인정보의 범위와 종류

②제1항의 규정에 의하여 협의하여야 할 개인정보파일의 범위와 종류는 대통령령으로 정한다.

제 5 장 개인정보보호위원회

제 1 절 개인정보보호위원회의 구성

제34조(개인정보보호위원회의 설치) 이 법이 정한 개인정보의 보호에 관한 업무를 독립적으로 수행하기 위하여 국무총리소속 하에 개인정보보호위원회(이하 “위원회”라 한다)를 둔다.

제35조(위원회의 구성) ①위원회는 위원장 1인과 상임위원 1인을 포함한 9인의 위원으로 구성한다.

②위원장과 상임위원은 국무총리가 제청한 자를 대통령이 임명하고, 비상임위원은 위원장이 추천한 자 중에서 국무총리가 임명한다.

④위원이 궐위된 때에는 지체 없이 새로운 위원을 임명하여야 한다.

⑤위원회의 업무를 효율적으로 수행하기 위하여 필요한 경우 위원회에 분야별로 분과위원회를 둘 수 있다. 분과위원회의 구성 및 운영에 관한 사항은 위원회규칙으로 정한다.

⑥위원장은 위원회의 업무를 효율적으로 지원하고 전문적인 연구 업무를 수행하기 위하여 필요하다고 인정할 때에는 위원회의 의결을 거쳐 관련 분야의 전문가를 전문위원으로 둘 수 있다.

제36조(위원의 결격사유 및 신분보장) ① 다음 각 호의 어느 하나에 해당하는 자는 위원이 될 수 없다.

1. 대한민국 국민이 아닌 자
2. 「국가공무원법」 제33조 각 호의 어느 하나에 해당하는 자
3. 정당의 당원
4. 「공직선거법」에 따라 실시하는 선거에 후보자로 등록한 자

②위원이 제1항 각 호의 어느 하나에 해당하게 된 때에는 당연히 퇴직한다.

③위원장과 위원의 임기는 각각 3년으로 하되, 1차에 한하여 연임할 수 있다.

④위원은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 그 의사에 반하여 면직되지 아니한다.

1. 제1항 각 호의 어느 하나에 해당하는 때
2. 신체상 또는 정신상의 장애로 직무수행이 현저히 곤란한 때

제 6 편 대안의 제시와 권고

⑤제4항제2호의 경우에는 전체 위원 3분의 2 이상의 찬성에 의한 의결을 거쳐 위원장의 제청으로 국무총리가 면직 또는 해촉한다.

제37조(위원장) ①위원장은 위원회를 대표하고 그 사무를 통할한다.

②위원장이 부득이한 사유로 직무를 수행할 수 없는 때에는 상임 위원이 그 직무를 대행한다.

제38조(위원회의 의결) 위원회 및 분과위원회는 재적위원 과반수의 출석으로 개의하고 출석위원 과반수의 찬성으로 의결한다.

제39조(사무처의 설치) ①위원회의 사무를 처리하기 위하여 위원회에 사무처를 둔다.

②사무처에 사무처장 1인과 그 밖의 필요한 직원을 둔다.

제40조(위원회의 조직 및 운영) ①이 법에 규정된 것 외에 위원회의 조직에 관하여 필요한 사항은 대통령령으로 정한다.

②이 법에 규정된 것 외에 위원회의 운영 등에 관하여 필요한 사항은 위원회규칙으로 정한다.

제 2 절 위원회의 업무와 권한

제41조(위원회의 업무) 위원회는 다음 각 호의 업무를 수행한다.

1. 개인정보의 보호 및 이용에 관한 시책의 수립 및 집행
2. 개인정보에 관한 법령·제도 및 관행의 조사·연구 및 개선
3. 개인정보보호기준의 제정·고시
4. 개인정보침해에 대한 조사·고충처리 및 피해구제
5. 개인정보의 수집·처리와 관련한 분쟁의 조정
6. 개인정보의 수집·처리 실태 등에 관한 조사·연구
7. 개인정보보호에 관한 기술개발의 지원 및 보급

8. 개인정보의 이용 및 보호에 관한 교육 및 홍보
9. 개인정보보호단체의 지원 및 자율규제활동의 촉진
10. 개인정보보호를 위한 국제기구 및 외국의 개인정보보호기구와의 교류·협력
11. 이 법 및 다른 법령에 의하여 위원회의 소관으로 규정된 사항
12. 그 밖에 개인정보의 보호 및 이용을 위하여 필요하다고 인정하는 사항

제42조(의견제시) ①국가 또는 지방자치단체가 개인정보보호에 영향을 미칠 내용을 포함한 법령이나 조례를 제정 또는 개정하고자 하는 경우에는 이 법에 부합되도록 하여야 한다.

②제1항의 경우 국가 또는 지방자치단체는 위원회에 의견을 요청할 수 있다.

③위원회는 제정 또는 개정 중이거나 제정 또는 개정된 법령 또는 조례가 개인정보보호에 영향을 미칠 내용을 포함한 경우에는 해당 행정기관, 국회, 지방자치단체, 지방의회 등에 의견을 제시할 수 있다.

제43조(개선권고) ①위원회는 개인정보보호를 위하여 필요하다고 인정하는 때에는 개인정보처리자에 대하여 정책·관행의 개선을 권고할 수 있다.

②제1항의 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실히 노력하여야 하며, 그 조치결과를 위원회에 통보(정보통신망에 의한 통보를 포함한다)하여야 한다.

제44조(자료제출 및 실태조사) ①위원회는 제41조에 의한 업무를 수행하는데 필요하다고 인정하는 경우에는 개인정보처리자에 대

하여 필요한 자료 등의 제출(정보통신망에 의한 제출을 포함한다)을 요구하거나 개인정보의 처리실태를 조사할 수 있다.

②제1항에 따른 요구 또는 조사를 받은 개인정보처리자는 정당한 사유가 없는 한 지체 없이 이에 따라야 한다.

③위원회는 제41조에 따른 업무를 수행하는 데 필요한 사실을 알고 있거나 전문적 지식 또는 경험을 가지고 있다고 인정되는 자에게 필요한 의견의 제출(정보통신망에 의한 제출을 포함한다)을 요청할 수 있다.

제45조(방문조사) ①위원회는 제41조에 따른 업무를 수행하기 위하여 필요하다고 인정할 때에는 그 의결로 소속공무원(제63조의 규정에 의하여 파견된 자를 포함한다)으로 하여금 개인정보처리자의 업무 현장을 방문하여 조사하게 할 수 있다.

②제1항의 규정에 의하여 방문조사를 하는 공무원은 그 권한을 표시하는 증표를 지니고 이를 관계인에게 제시하여야 한다.

제46조(처리결과의 공개) 위원회는 이 법에 따른 의견제시, 개선권고, 시정명령, 실태 및 방문조사 결과 등을 공표(정보통신망에 의한 공표를 포함한다)할 수 있다. 다만, 다른 법률에 의하여 공표가 제한되거나 개인의 권리 및 사생활의 비밀이 침해될 우려가 있는 경우에는 그러하지 아니하다.

제47조(시정명령 등) ①위원회는 조사 등의 결과 정보주체의 권리가 침해되었다고 판단할 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해발생의 우려가 있다고 인정할 때에는 개인정보처리자에게 다음 각 호의 하나에 해당하는 조치를 하도록 명할 수 있다.

1. 권리침해행위의 중지

2. 개인정보 수집·처리의 일시적인 정지

3. 그 밖에 개인정보의 보호 및 침해방지를 위하여 필요한 조치

②제1항의 규정에 불구하고 개인정보처리자가 국가기관·지방자치단체인 경우에는 해당 국가기관 또는 지방자치단체의 직근 상급기관으로 하여금 제1항의 명령을 발하도록 권고할 수 있다.

③제2항의 규정에 의한 권고를 받은 기관은 특별한 사유가 없는 한 이를 존중하여야 하며, 그 처리결과를 위원회에 통보하여야 한다.

제48조(이의신청 및 집행정지) ①위원회의 시정명령에 대하여 불복이 있는 자는 그 처분의 통지를 받은 날부터 30일 이내에 그 사유를 갖추어 위원회에 이의신청을 할 수 있다.

②위원회는 제1항에 따른 이의신청에 대하여 60일 이내에 재결을 하여야 한다. 다만, 부득이한 사정으로 그 기간 이내에 재결을 할 수 없을 경우에는 30일의 범위 안에서 결정으로 그 기간을 연장할 수 있다.

③제1항에 따른 이의신청을 제기한 경우로서 그 명령의 이행 또는 절차의 속행으로 인하여 발생할 수 있는 회복하기 어려운 손해를 예방하기 위하여 필요하다고 인정하는 때에는 당사자의 신청이나 직권에 의하여 그 명령의 이행 또는 절차의 속행에 대한 정지(이하 “집행정지”라 한다)를 결정할 수 있다.

④위원회는 집행정지의 결정을 한 후에 집행정지의 사유가 없어진 경우에는 당사자의 신청 또는 직권에 의하여 집행정지의 결정을 취소할 수 있다.

제49조(고발 및 징계권고) ①위원회는 조사 등의 결과 개인정보처리자, 개인정보보호책임자등, 개인정보취급자 등의 행위가 범죄행

제 6 편 대안의 제시와 권고

위에 해당하고 이에 대하여 형사처벌이 필요하다고 인정할 때에는 검찰총장에게 그 내용을 고발할 수 있다. 다만, 피고발인이 군인 또는 군무원인 경우에는 소속 군참모총장 또는 국방부장관에게 고발할 수 있다.

②위원회는 조사 등의 결과 법규위반행위가 있다고 인정할 때에는 책임이 있는 자에 대한 징계를 소속 기관·단체 등의 장에게 권고할 수 있다.

③제2항의 규정에 의하여 위원회로부터 권고를 받은 소속 기관·단체 등의 장은 이를 존중하여야 하며 그 결과를 위원회에 통보하여야 한다.

제50조(개인정보보호기준의 제정) ①위원회는 이 법의 효율적인 집행을 위하여 대통령령이 정하는 바에 따라 분야별 또는 품목별로 개인정보의 수집·처리 요건, 절차, 방법 등을 포함하여 개인정보의 보호 및 이용에 관한 구체적인 기준(이하 “개인정보보호기준”이라 한다)을 정하여 고시할 수 있다.

②위원회는 제1항의 규정에 의한 개인정보보호기준을 정하여 고시하고자 하는 경우에는 미리 이해당사자의 의견을 수렴하고 관계 행정기관의 장과 협의하여야 한다.

제51조(관계기관의 장의 협조) ①위원회는 이 법의 시행을 위하여 필요하다고 인정하는 때에는 관계기관의 장의 의견을 들을 수 있다.

②위원회는 이 법의 규정에 의한 의무의 이행을 확보하기 위하여 필요하다고 인정하는 때에는 관계기관의 장에게 필요한 협조를 의뢰할 수 있다.

제52조(개인정보영향평가·인증기관의 지정) ①개인정보보호위원회는 개인정보의 안전하고 합법적인 처리를 지원하기 위하여 개인

정보영향 평가 및 인증에 필요한 시설, 인력 및 기술 등을 갖춘 자를 평가·인증기관으로 지정(이하 “지정평가·인증기관”이라 한다)하여 다음 각 호의 업무를 수행하게 할 수 있다.

1. 개인정보 영향평가 및 인증표시의 부여
2. 개인정보 영향평가기법의 개발 및 보급
3. 개인정보보호 및 영향평가와 관련한 전문인력의 양성
4. 개인정보보호를 위한 교육 및 지도
5. 개인정보보호기술의 개발 및 보급
6. 그 밖에 개인정보의 안전한 처리를 지원하기 위하여 대통령령이 정하는 사업

②제1항에 따라 지정평가·인증기관으로 지정받고자 하는 자는 대통령령이 정하는 바에 따라 개인정보보호위원회에 지정신청을 하여야 한다.

③제1항에 따른 지정평가·인증기관의 지정요건, 지정절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

④지정평가·인증기관은 제1항에 의한 업무를 행함에 있어서 정관이 정하는 방법에 따라 수수료를 받을 수 있다.

⑤개인정보보호위원회는 예산의 범위안에서 지정평가·인증기관이 제1항 각호의 사업을 실시하는데 필요한 지원을 할 수 있다.

⑥개인정보보호위원회는 이 법의 시행에 필요한 범위 안에서 지정평가·인증기관에 대하여 해당 업무에 관한 보고를 하게 할 수 있다.

⑦개인정보보호위원회는 지정평가·인증기관이 다음 각 호의 하나에 해당하는 경우에는 그 지정을 취소하거나 6개월 이내의 기간을 정하여 그 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호의 경우에는 그 지정을 취소하여야 한다.

1. 허위 기타 부정한 방법으로 지정을 받은 경우
2. 정당한 사유 없이 1년 이상 계속하여 평가·인증업무를 행하지

아니한 경우

3. 제3항의 규정에 의한 지정요건에 적합하지 아니하게 된 경우
 4. 허위 기타 부정한 방법으로 평가·인증업무를 수행한 경우
- ⑧ 제6항의 규정에 의하여 지정평가·인증기관의 지정이 취소된 후 2년이 경과하지 아니한 자는 지정평가·인증기관으로 지정을 받을 수 없다.

제53조(평가·인증의 공정화) ①개인정보의 수집·처리와 관련한 평가 또는 인증업무에 종사하는 자는 정확하고 공정하게 평가·인증하여야 한다.

③개인정보보호위원회는 필요한 경우 지정평가·인증기관에 대하여 평가·인증의 기준·방법 및 절차, 인증취소의 사유 및 절차, 운용상황 등에 관한 자료를 제출하게 할 수 있다.

④개인정보보호위원회는 제2항의 규정에 의한 기준, 방법, 절차, 사유 등이 불합리하다고 인정될 때에는 해당 지정평가·인증기관에 대하여 개선을 권고하거나 그 밖의 필요한 조치를 명할 수 있다.

제54조(연차보고) ①위원회는 매년 개인정보보호시책의 수립 및 집행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.

②제1항의 보고서에는 다음 각 호의 내용이 포함되어야 한다.

1. 정보주체의 권리침해 및 그 구제현황
2. 개인정보처리에 관한 실태조사 등의 결과
3. 개인정보관련 시책의 추진 현황 및 실적
4. 개인정보관련 해외의 입법 및 정책 동향

5. 그 밖에 개인정보보호시책에 관하여 공개 또는 보고하여야 할 사항

제 3 절 개인정보분쟁조정위원회

제55조(개인정보분쟁조정위원회의 설치) 개인정보와 관련한 분쟁을 조정하기 위하여 위원회에 개인정보분쟁조정위원회(이하 “조정위원회”)를 둔다.

제56조(조정위원회의 구성) ①조정위원회는 조정위원장 1인을 포함한 15인 이내의 조정위원으로 구성한다.

②조정위원은 위원회의 위원(위원장을 제외한다)과 다음 각 호의 자 중에서 위원장이 위촉한 자가 된다.

1. 「고등교육법」에 의한 대학에서 조교수 이상의 직에 있거나 있었던 자

2. 판사·검사 또는 변호사의 자격이 있는 자

3. 3급 이상 공무원 또는 이에 상당하는 공공부문 및 관련단체의 직에 있거나 있었던 자로서 개인정보보호업무에 관한 경험이 풍부한 자

4. 그 밖에 개인정보보호에 관하여 학식과 경험이 풍부한 자

③조정위원장은 위원회의 상임위원이 이를 겸직한다.

④조정위원의 위촉 및 임기, 조정위원회의 구성·운영, 조정의 절차 등에 관하여 필요한 사항은 위원회의 규칙으로 정한다.

제57조(조정의 개시 등) ①개인정보의 수집·처리로 인하여 권리를 침해받거나 피해를 입은 자는 위원회에 권리침해 등의 구제를 신청할 수 있다.

②국가·지방자치단체, 개인정보보호단체, 개인정보처리자 등은 정보주체로부터 권리침해 등의 구제신청을 받은 때에는 위원회에

그 처리를 의뢰할 수 있다.

③위원회는 제1항 및 제2항에 따라 권리침해 등의 구제신청을 받은 경우에는 권리침해의 중지, 침해된 권리의 회복, 피해보상 등의 구제조치를 당사자에게 제시하고 합의를 권고할 수 있다.

④위원회는 제3항에 따른 합의가 이루어지지 아니한 때에는 지체 없이 조정위원회에 조정을 요청하여야 하고, 조정위원회는 당사자에게 조정절차의 개시 사실을 통지(정보통신망에 의한 통지를 포함한다)하여야 한다.

제58조(조정 효력 등) ①조정위원회의 위원장은 분쟁조정을 마친 때에는 지체 없이 당사자에게 그 분쟁조정 내용을 통지(정보통신망에 의한 통보를 포함한다)하여야 한다.

②제1항에 따른 통지를 받은 당사자는 그 통지를 받은 날부터 15일 이내에 분쟁조정 내용에 대한 수락 여부를 조정위원회에 통보하여야 한다. 이 경우 15일 이내에 수락 여부에 대한 의사표시가 없는 때에는 수락한 것으로 본다.

③제2항에 따라 당사자가 분쟁조정 내용을 수락하거나 수락한 것으로 보는 경우 조정위원회는 조정조서를 작성하고, 조정위원회의 위원장 및 각 당사자가 기명·날인(전자서명을 포함한다. 이하 같다)하여야 한다. 다만, 수락한 것으로 보는 경우에는 각 당사자의 기명·날인을 생략할 수 있다.

④제2항에 따라 당사자가 분쟁조정 내용을 수락하거나 수락한 것으로 보는 때에는 그 분쟁조정 내용은 재판상 화해와 동일한 효력을 갖는다.

제59조(조정 거부 및 중지) ①조정위원회는 분쟁의 성질상 분쟁 조정위원회에서 조정하는 것이 적합하지 아니하다고 인정되거나

부정한 목적으로 조정을 신청하였다고 인정되는 때에는 당해 조정을 거부할 수 있다. 이 경우 조정거부의 사유를 신청인에게 통보(정보통신망에 의한 통보를 포함한다)하여야 한다.

②조정위원회는 당사자 중 일방이 조정을 거부한 경우에는 그 거부사실과 거부이유를 상대방에게 통보(정보통신망에 의한 통보를 포함한다)하여야 한다.

③조정위원회는 당사자 중 일방이 소를 제기한 때에는 조정을 중지하고 이를 상대방에게 통보(정보통신망에 의한 통보를 포함한다)하여야 한다.

제60조(집단분쟁조정) ①국가·지방자치단체, 개인정보보호단체등 및 개인정보처리자는 정보주체의 피해가 다수의 정보주체에 같거나 비슷한 유형으로 발생하는 경우로서 대통령이 정하는 사건에 대하여는 조정위원회에 일괄적인 분쟁조정(이하 “집단분쟁조정”이라 한다)을 의뢰 또는 신청할 수 있다.

②제1항의 규정에 따라 집단분쟁조정을 의뢰받거나 신청받은 조정위원회는 조정위원회의 의결로써 제3항 내지 제7항의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 조정위원회는 대통령이 정하는 기간동안 그 절차의 개시를 공고하여야 한다.

③조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.

④조정위원회는 조정위원회의 의결로써 제1항 및 제3항의 규정에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표당사자로 선임할 수 있다.

⑤조정위원회는 개인정보처리자가 조정위원회의 집단분쟁조정 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서

피해를 입은 정보주체에 대한 보상계획서를 작성하여 조정위원회에 제출하도록 권고할 수 있다.

⑥제59조제3항의 규정에 불구하고 조정위원회는 집단분쟁조정 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.

⑦집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제61조(「민사조정법」의 준용) 위원회의 조정절차에 관하여 이 법 및 위원회의 규칙에 규정되지 아니한 사항은 「민사조정법」의 규정을 준용한다.

제62조(적용제외) ②종교 및 선교 활동, 정당 및 정치 활동, 취재 및 보도 등을 목적으로 개인정보를 수집·처리하는 경우에는 제8조제1항 및 제9조의 규정을 적용하지 아니한다.

③제2항에 해당하는 개인정보처리자는 개인정보의 안전한 관리를 위한 기술적·관리적 조치, 고충처리창구의 마련 등 정보주체의 권리를 보호하기 위하여 필요한 조치를 스스로 강구하여야 한다.

④개인정보보호위원회는 정보주체의 권리를 보호하기 위하여 필요하다고 인정된 때에는 제2항에 의한 개인정보처리자에게 개인정보의 적절한 수집·처리를 위한 조치를 강구하도록 권고할 수 있다.

참 고 문 헌

I. 국내문헌

1. 단행본

- 강남훈, 『정보혁명의 정치경제학』, 문화과학사, 2002
- 경상대학교 사회과학연구소(편), 『디지털 혁명과 자본주의의 전망』, 한울아카데미, 2000
- 계희열, 『헌법학(상) (신정2판)』, 박영사, 2005
- 고영삼, 『전자감시사회와 프라이버시』, 도서출판 한울, 1998
- 국립국어연구원(편), 『표준국어대사전』, 두산동아, 1999
- 권건보, 『개인정보보호와 자기정보통제권』, 경인문화사, 2005
- 권영성, 『헌법학원론(개정판, 2005년판)』, 법문사, 2005
- _____, 『신고헌법학원론』, 법문사, 1981
- 김갑중, 『디지털시대의 정보 프라이버시』, 학영사, 2003
- 김기태, 『디지털 미디어 시대의 저작권』, 이채, 2005
- 김동희, 『행정법 I』, 박영사, 2001
- 김민정·김성숙, 『디지털 경제와 소비자』, 태일사, 2005
- 김범환, 『(인문사회분야 학생을 위한) 정보통신경제론 디지털 경제론』, 청목출판사, 2001
- 김연수, 『개인정보보호 - 고도 지식정보 사회의 개인정보와 Cyberlaw』, 사이버출판사, 2001

참 고 문 헌

- 김종호, 『국가정보보호법의 필요성과 기본방향』, 경희대학교 출판국, 2004
- 김철수, 『헌법학개론 (제18전정신판)』, 박영사, 2006
- 김호기(편), 『현대 비판사회이론의 흐름』, 도서출판 한울, 2001
- 박영도, 『입법평가의 이론과 실제』, 한국법제연구원, 2007
- 박영도, 『입법학 입문』, 한국법제연구원, 2008
- 박윤훈, 『행정법강의(상)』, 박영사, 2001
- 백윤철·이창범·장교식, 『개인정보보호법』, 한국학술정보, 2008
- 송영식·이상정, 『저작권법개설(제3판)』, 세창출판사, 2003
- 성낙인, 『헌법학(제7판)』, 법문사, 2007
- 성낙인, 『언론정보법』, 나남출판, 1998
- _____, 『프랑스헌법학』, 법문사, 1995
- 이관기, 『알권리와 프라이버시 - 전통적 대립과 정보사회의 갈등』, 한국교육문화원, 1993
- 이민영, 『개인정보법제론』, 진한M&B, 2005
- 이준구·이창용, 『경제학원론(제3판)』, 법문사, 2005
- 이준구, 『미시경제학(제4판)』, 법문사, 2002
- 임홍빈, 『기술문명과 철학』, 문예출판사, 1995
- 전석호, 『정보사회론: 커뮤니케이션 혁명과 뉴미디어(개정4판)』, 나남, 2004
- 정중섭, 『헌법학원론(제2판)』, 박영사, 2007

- 최 영, 『뉴미디어시대의 네트워크 커뮤니케이션』, 커뮤니케이션북스, 1998
- 최정호·강현두·오택섭, 『매스미디어와 사회』, 나남출판, 1995
- 한국정신문화연구원(편), 『한국민족문화대백과사전』, 한국정신문화연구원, 1991
- 홍준형, 『행정법총론』, 한울, 1997
- 홍준형, 『법정책의 이론과 실제』, 법문사, 2008
- 허 영, 『한국헌법론』, 박영사, 2001
- Anthony Giddens, *Central Problems in Social Theory-Action, Structure and Contradiction in Social Analysis*, 윤병철·박병래(공역), 『사회이론의 주요 쟁점』, 문예출판사, 1991[2003 print]
- Anthony Giddens, *The Constitution of Society*, 황명주·정희태·권진현(공역), 『사회구성론』, 자작아카데미, 1998
- Anthony Giddens, *Nation state and Violence*, 진덕규(역), 『민족국가와 폭력』, 삼지원, 1991
- Esther Dyson, *Release 2.0: A Design for Living in the Digital Age*, 남경태(역), 『인터넷, 디지털 문명이 열린다』, 경향신문사, 1997
- Frank Webster, *Theories of the Information Society*, 조동기(역), 『정보사회이론』, 사회비평사, 1997
- George Orwell, *Nineteen Eighty Four*, 김병익(역), 『1984년』, 문예출판사, 1999
- Hans Jonas, *Technik, Medizin und Ethik zur Praxis des Prinzips Verantwortung*, 이유택(역), 『기술 의학 윤리 책임 원칙의 실현』, 솔, 2005

- Jean Jacques Rousseau, *Essai sur l'origine des langues:ou il est parlé de la mélodie et de l'imitation musicale*, 주경복·고봉만(공역), 『언어 기원에 관한 시론』, 책세상, 2002
- Kazufumi Orikasa, 高度情報化社會の諸相 - 歴史・學問・人間・哲學・文化, 김재홍, 『고도 정보화사회의 여러 모습 - 역사, 학문, 인간, 철학, 문화』, 커뮤니케이션북스, 2004
- Kenneth H. Tucker, *Anthony Giddens and Modern Social Theory*, 김용규·박형신(공역), 『앤서니 기든스와 현대사회이론』, 일신사, 1999
- Manuel Castells, *The Rise of the Network Society*(2nd ed.), 김목한·박행웅·오은주(공역), 『네트워크 사회의 도래』, 한울아카데미, 2003 [2005 print]
- Mark Poster, *The Mode of Information Poststructuralism and Social Context*, 김성기(역), 『뉴미디어의 철학』, 민음사, 1994
- Nicholas Negroponte, *Being Digital*, 백옥인(역), 『디지털이다』, 커뮤니케이션북스, 1995
- Marshall McLuhan, *The Gutenberg Galaxy: the making of typographic man*, 임상원(역), 『구텐베르크 은하계 - 활자 인간의 형성』, 커뮤니케이션북스, 2001
- Manuel Castells, *The Internet Galaxy: Reflection on the Internet, Business, and Society*, 박행웅(역), 『인터넷 갤러시 - 인터넷, 비즈니스, 사회적 성찰』, 한울, 2004
- Nathan Weinberg, *Computers in Information Society*, 통신개발연구원, 『정보사회와 컴퓨터』, 통신개발연구원, 1992

- Michel Foucault, *Surveiller et punir: naissance de la prison*, 오생근 (역), 『감시와 처벌: 감옥의 역사』, 나남출판, 1994[1996 print]
- Richard A. Posner, *Economic Analysis of Law Part 2*, 정기화(역), 『법 경제학(하)』, 자유기업원, 2004

2. 연구보고서 및 정부보고서

- 감사원, “감사결과 처분요구서 -행정정보 공유 및 관리실태-”, 2008. 5
- 과학기술정보통신위원회, “개인정보보호기본법안(노회찬 의원 대표 발의) 관련위원회 의견제시의 건 검토보고서”, 2005. 4
- 구병문, “캐나다 및 미국의 프라이버시 영향 평가 제도 분석과 국내 전자정부 법제로의 도입방향 검토”, 『정보화이슈분석』 03-16, 한국전산원, 2003. 7
- 김병도 외, 『우리나라 데이터베이스마케팅 관련 산업의 현황과 발전 방향』, 서울대학교 경영연구소, 2004
- 김일환, 『개인정보보호법제의 정비방안에 관한 연구』 연구보고 97-5, 한국법제연구원, 1997
- 김철완·이민영, 『인터넷 개인정보보호에 관한 법제도 연구』 정책 00-10, 정보통신정책연구원, 2000
- 문화연대·민주사회를위한변호사모임·지문날인반대연대·진보네트 워크센터·참여연대·한국노동네트워크협의회·함께하는시민행동, 『프라이버시법제정을위한연석회의』, 2004. 10. 20
- 박광진 외, 『정보통신서비스에서의 개인정보보호에 관한 지침(안) 연구』 기술정책연구 99-2, 한국정보보호센터, 1999. 12

참 고 문 헌

- 박균성, 『프랑스의 전자정부법제』 현안분석 2001-7, 한국법제연구원, 2001. 11
- 박영도, 『입법평가의 이론과 실제』 입법평가 연구 07-06, 한국법제연구원, 2007
- 법제처, 『각국의 개인정보보호관계법』 법무자료 제150집, 1989
- 성낙인 외, 『개인정보보호를 위한 정책방안 연구』, 정보통신부, 1999
- 이원부 외, 『정보통신망에서의 개인정보 침해사례 분석 및 이용규제 방안 연구』 기술정책연구 98-6, 한국정보보호센터, 1998. 12
- 이인호 외, 『개인의 사생활, 국가적 감시, 그리고 규범』, 정보통신정책연구원, 2006
- 이창범·윤주연, 『각국의 개인정보피해구제제도 비교연구』, 개인정보분쟁조정위원회, 2003
- 이형규, 『독일 개인정보보호법제 현대화 추진방안에 관한 연구』, 한국정보보호진흥원, 2002. 12
- 정보통신부, 『정보통신망이용촉진등에관한법률 개정을 위한 공청회 자료집』, 2000. 7. 20
- 총무처, 『축조해설 개인정보보호법』, 총무처, 1994
- 한국전산원 정보화정책팀, “개인정보보호법제의 현황과 그 발전전망”, NCA CIO REPORT (05-6호), 한국전산원, 2005. 3. 31
- 한국정보보호진흥원, 『2007 정보보호 실태조사 기업편』, 2007
- 한국정보보호진흥원, 『2007 정보보호 실태조사 개인편』, 2007
- _____, 『2007년 하반기 민간기업 정보보호 실태조사』, 2007

- _____, 『2003 개인 인터넷 이용자의 정보화 역기능 실태조사보고서』, 2003
- _____, 『2002 개인정보보호백서』, 2003
- 한국정보산업연합회, 『CRM Fair 2007』, 2007
- _____, 『CRM Fair 2006』, 2006
- 한국통신정보보호학회, 『주요국가의 개인정보보호기관 운영상황 연구』, 한국정보보호센터, 1998
- 행정자치부, 『2007 전자정부법의 이해와 해설』, 2008
- _____, 『희망대한민국 행정자치부 정책백서 (2003~2007)』, 2008. 2
- _____, 『공공기관의 개인정보보호제도 이해와 해설』, 2003. 3
- 행정정보공유추진위원회, 『2007 행정정보공동이용 백서』, 2007. 12
- 현대호, 『인터넷상의 정보보호에 관한 법제연구』, 한국법제연구원, 2000
- 홍준형, 『개인정보보호법제 정비를 위한 기본법 제정방안 연구』, 한국전산원, 2004

3. 논 문

- 강경근, “정보보호의 헌법규범적 접근과 전망”, 『공법학연구』 제6권 제2호, 한국비교공법학회, 2005
- 강대오, “디지털경제하 저작권 문제에 대한 경제학적 고찰”, 『한국비블리아 발표논집』 제5집, 한국비블리아학회, 2001. 11
- 경 건, “정보공개청구제도에 관한 연구 - 일반 행정법이론체계와의 관련에서 -”, 서울대학교 법학박사학위논문, 1998

참고문헌

- 고영삼, “정보지배사회의 전자감시와 개인정보침해”, 부산대학교 사회학박사 학위논문, 1998. 2
- 고시면, “공공장소들에서 CCTV를 통한 감시의 위법성 여부에 관한 독일 칼스루허 행정재판소의 판결”, 『사법행정』, 한국사법행정학회, 2005. 2
- 권건보, “자기정보통제에 관한 연구 공공부문에서의 개인정보보호를 중심으로”, 서울대학교 법학박사학위논문, 2004
- 권현영, “전자정부시대 개인정보보호법제의 쟁점”, 『정보화정책』 제11권 제3호, 한국전산원, 2004
- 권형준·허순철, “직장내 이메일(e mail) 감청과 프라이버시”, 『헌법학연구』 제10권 제3호, 한국헌법학회, 2004. 9
- 권형준, “자기정보통제권에 관한 고찰”, 『헌법학연구』 제10집 제2호, 한국헌법학회, 2004. 6
- 김경동, “기술혁신과 사회변동: 정보사회의 생성전개에 대한 이해”, 정보사회학회(편), 『정보사회의 이해(개정증보판)』, 나남, 1998
- 김동원, “개인정보수집에서 프라이버시와 경쟁가치들의 경합과 균형”, 『정보화정책』 제10권 제4호, 한국전산원, 2003
- 김배원, “정보기본권의 독자성과 타당범위에 대한 고찰 헌법개정과 관련한 체계구성을 중심으로”, 『헌법학연구』 제12권 제4호, 한국헌법학회, 2006. 11
- 김배원, “정보기본권(상)”, 『고시계』, 2002년 9월호, 고시계사, 2002.8
- 김배원, “정보기본권(하)”, 『고시계』, 2002년 10월호, 고시계사, 2002.9
- 김승환, “정보자기결정권”, 『헌법학연구』 제9집 제3호, 한국헌법학회, 2003. 10

- 김연태, “행정상 개인정보보호”, □□저스티스□□ 제34권 제5호, 한국법학원, 2001. 10
- 김용규, “디지털경제의 특징과 시사점”, 『디지털경제연구』 제6권, 한양대학교 디지털경제연구소, 2001. 12
- 김용섭, “정보공개와 개인정보보호의 충돌과 조화”, 『공법연구』 제29집 제3호, 한국공법학회, 2001. 5
- 김원동, “정보사회에 관한 이론적 전망”, 정보사회학회(편), 『정보사회의 이해 (개정증보판)』, 나남, 1998
- 김일환·김민호, “개인정보보호기구 법제정비의 원칙과 방향에 관한 공법체계적 고찰”, 『토지공법연구』 제36집, 한국토지공법학회, 2007. 5
- 김일환, “개인정보 공동이용의 통제와 감독에 관한 비교법적 고찰 - 미국과 독일의 법제를 중심으로”, 『헌법학연구』 제13권 제2호, 한국헌법학회, 2007. 6
- _____, “교육행정정보시스템(NEIS)의 법적 정비에 관한 연구”, 『성균관법학』 제17권 제3호, 성균관대학교 비교법연구소, 2005. 12
- _____, “개인정보보호기구의 법적 지위와 권한에 관한 헌법적 고찰”, 『공법연구』 제33집 제3호, 한국공법학회, 2005
- _____, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 『공법연구』 제29집 제3호, 한국공법학회, 2001. 5
- _____, “개인정보보호법의 개정필요성과 내용에 관한 연구”, □□공법연구□□ 제26집 제2호, 한국공법학회, 1998
- _____, “독일연방헌법법원의 인구조사판결”, 김계환교수회갑기념논문, 1996

참 고 문 헌

- 김재중, “한국의 전자감시제도 및 그 발전방안”, 『법학연구』 제18권 제1호, 충북대학교 법학연구소, 2007
- 김종철, “전자정부와 개인정보보호의 조화”, 『세계헌법연구』 제12권 제2호, 국제헌법학회 한국학회, 2006
- _____, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 『인터넷법률』 제4호, 법무부, 2001
- 김태정, “근로자 사생활의 의미와 보호범위”, 『노동법학』 제22호, 한국노동법학회, 2006. 6
- 김효진, “정보공개와 개인정보의 법적 보호”, 『헌법규범과 헌법현실』 권영성교수 정년기념논문집, 법문사, 1999
- 문성제, “온라인상에서의 개인정보보호에 관한 국제동향 - 미국의 제도를 중심으로”, 『비교법학연구』 제3집, 한국비교법학회, 2004. 2
- 문정민, “성범죄자 전자감시제도에 대한 고찰”, 『법학연구』 제29집, 한국법학회, 2008. 2
- 박영철, “생체정보의 보호”, 『헌법학연구』 제10집 제4호, 한국헌법학회, 2004. 12
- 박종보, “공공정보공개제도와 알 권리의 헌법적 근거”, 『헌법규범과 헌법현실』 권영성교수 정년기념논문집, 법문사, 1999
- _____, “공동정보공개제도와 알 권리의 헌법적 근거”, 『공법연구』 제28집 제1호, 한국공법학회, 1999
- 박준식, “정보기술의 발전”, 『정보사회학회(편), 『정보사회의 이해(개정증보판)』, 나남, 1998

- 배대현, “정보의 귀속, 유통에 관한 민사법적 접근 On Line상 개인 정보의 보호를 중심으로,” 『비교사법』 제8권 제2호(통권 제15권), 한국비교사법학회, 2001. 12
- 백윤철, “우리나라에서 의료정보와 개인정보보호”, 『헌법학연구』 제11집 제1호, 한국헌법학회, 2005. 3
- 백윤철, “헌법상 자기결정권과 개인정보자기결정권”, 『헌법학연구』 제9집 제3호, 한국헌법학회, 2003. 10
- 변재옥, “입법소개: 1988년의 컴퓨터연결 및 프라이버시보호법”, 『미국헌법연구』 제1호, 미국헌법연구소, 1990
- 서계원, “정보 프라이버시와 개인정보의 보호”, 『세계헌법연구』 제11권 제1호, 국제헌법학회 한국학회, 2005
- 성낙인, “행정상 개인정보보호”, 『공법연구』 제22집 제3호, 한국공법학회, 1994
- _____, “정보보호와 인권”, 『법학』 제41권 제1호, 서울대학교 법학연구소, 2004
- _____, “프라이버시와 개인정보보호를 위한 입법정책적 과제”, 『영남법학』 제9·10호, 영남대학교 법학연구소, 1999
- 서주실, “Warren · Brandeis의 ‘The Right to Privacy’”, 『미국헌법연구』 제6호, 미국헌법학회, 1995. 7
- 유일상, “정보공개법상 비공개정보의 범위에 관한 비교법제적 연구 - 한, 미, 영, 일을 중심으로 -”, 『헌법학연구』 제11집 제3호, 한국헌법학회, 2005. 9
- 이강혁, “정보화사회에서의 정보접근의 자유와 개인정보의 보호”, 『외법논집』 제16집, 한국외국어대학교 외국학종합연구센터 법학연구소, 2004. 8

참고문헌

- 이동훈, “전자민주주의를 구현하는 액세스권의 헌법적 함의”, 『성균관법학』 제18권 제1호, 성균관대학교 비교법연구소, 2006. 6
- 이민영, “개인정보보호법제의 개편논의와 개선방안”, 『정보통신정책연구』 제16권 제1호, 정보통신정책연구원, 2004. 1
- 이승훈, “네트워크 산업의 경쟁정책”, 권오승(편), 『공정거래와 법치』, 법문사, 2004
- 이완수·허원무, “LG생활건강 백화점 화장품 브랜드 오위의 CRM 전략”, 『한국마케팅저널』 제7권 제1호, 한국마케팅학회, 2005
- 이인호, “한국 정보법의 발전동향 - 정보공개법과 개인정보보호법을 중심으로”, 『공법연구』 제35집 제4호, 한국공법학회, 2007. 6
- _____, “미국의 개인정보보호법제에 대한 분석과 시사점”, 『법학논문집』 제29집 제1호, 중앙대학교 법학연구소, 2005
- _____, “스팸(SPAM) 규제입법에 대한 평가와 정책방향”, 『정보법학』 제8권 제1호, 한국정보법학회, 2004. 7
- _____, “학생의 정보프라이버시와 교육행정정보시스템(NEIS)”, 『인권과 정의』 제329호, 대한변호사협회, 2004. 1
- _____, “개인정보보호에 대한 국제적 동향 분석 -3가지 집행모델과 그 통합론을 중심으로-”, 『인터넷법률』 통권 제18호, 법무부, 2003
- _____, “디지털시대의 정보법질서와 정보기본권”, 『법학논문집』 제26집 제2호, 중앙대학교 법학연구소, 2002. 11
- _____, “공공부문 개인정보보호법제에 대한 분석과 비판”, 『정보법학』 제6권 제1호, 한국정보법학회, 2002. 7
- _____, “아동온라인개인정보보호법과 그 효율적 집행방안”, 『법과사회』 제20호, 법과사회이론연구회, 2001

- _____, “범죄보도와 면책사유의 적용”, 『언론중재』 제19권 제3호, 언론중재위원회, 1999. 9
- 이준일, “개인정보에 관한 기본권”, 『고려법학』 제41집, 고려대학교 법학연구원, 2003
- 이창범, “사업장내 전자우편감시제도에 관한 연구”, 『노동정책연구』 제5권 제4호, 한국노동연구원, 2005
- 이창범, “정보기술 발달과 개인정보 침해에 관한 법적 고찰”, 『공법연구』 제32집 제5호, 한국공법학회, 2004. 6
- _____, “현행 프라이버시 보호 담당기구의 성과와 한계”, 『프라이버시 보호 법제, 어떤 모습이어야 하는가?』 9개 시민단체 연석 워크숍, 2003. 8. 21
- 이호룡, “각국의 개인정보보호법제 동향-개인정보보호법의 제정 논의에 즈음하여-”, 『인터넷법률』 제8호, 법무부, 2001. 9
- 이희성, “작업장내에서의 전자메일 및 CCTV의 감시와 근로자의 프라이버시보호”, 『비교사법』 제10권 제1호, 한국비교사법학회, 2003. 3
- 임건면, “개인정보침해에 대한 민사법적 대응”, 『비교사법』 제8권 제1호(하)(통권 제14호), 한국비교사법학회, 2001
- 임규철, “유럽연합의 개인정보보호 - 제3국으로의 개인정보전송의 경우를 중심으로”, 『아태공법연구』 제11집, 아세아태평양공법학회, 2003
- _____, “정보화사회에서의 개인정보자기결정권에 대한 연구 독일에서의 논의를 중심으로”, 『헌법학연구』 제8집 제3호, 한국헌법학회, 2002. 10

- 장여경, “한국의 프라이버시보호 감독기구의 위상과 역할”, 『프라이버시 보호 법제, 어떤 모습이어야 하는가?』 9개 시민단체 연석 워크숍, 2003. 8. 21
- 장영민, “정보통신망발전에 따른 개인정보보호”, 『형사정책연구』 제26호, 한국형사정책연구원, 1996 여름
- 전영주, “의료정보와 개인정보보호”, 『법학연구』 제23집, 한국법학회, 2006. 8
- 정상호, “일본 개인정보보호법 제정 추진동향”, 『해외정보보호동향』, 한국정보보호진흥원, 2003. 2
- 정영화, “개인정보감독기구의 법정책 고찰”, 『프라이버시 보호 법제, 어떤 모습이어야 하는가?』 9개 시민단체 연석 워크숍, 2003. 8. 21
- 정영화, “생성되고 있는 정보기본권에 관한 고찰”, 『세계헌법연구』 제7호, 국제헌법학회 한국학회, 2003. 5
- 정영화, “정보법령에 관한 법이론”, 『세계헌법연구』 제5호, 국제헌법학회 한국학회, 2000. 10
- 정완용, “전자거래에 있어서 개인정보침해에 대한 법적 구제”, 『인터넷법률』 제10호, 법무부, 2002
- 정준현, “개인정보와 국가의 과제”, 『성균관법학』 제15권 제2호, 성균관대학교 비교법연구소, 2003. 10
- 정태호, “CCTV 감시에 대한 개인정보보호법의 규율에 대한 헌법적 평가”, 『헌법학연구』 제14권 제1호, 한국헌법학회, 2008. 3
- _____, “현행 인구주택총조사의 위헌성 - 독일의 인구조사판결(BVerfGE 65, 1)의 법리분석과 우리의 관련법제에 대한 반성 -”, 『법률행정논총』 제20집, 전남대학교 법률행정연구소, 2000

- 조규범, “전자감시제도에 대한 헌법적 소고”, 『성균관법학』 제19권 제3호, 성균관대학교 비교법연구소, 2007. 12
- 조동기, “정보화사회와 프라이버시”, 『정보화시대의 미디어와 문화』, 한국언론학회·한국사회학회 엮음, 세계사, 1998
- 채승완, “일본의 개인정보보호체계와 개인정보의 경제적 가치”, 『한일경상논집』, 한일경상학회, 2007
- 최경진, “개인정보의 법적 규율과 관련한 공적 영역과 사적 영역의 구별 여부”, 『프라이버시 보호 법제, 어떤 모습이어야 하는가?』 9개 시민단체 연석 워크숍, 2003. 8. 21
- 최상호, “전자거래에 있어서 소비자보호 - 특히 프라이버시 및 개인정보보호를 중심으로 -”, 『비교사법』 제8권 제1호(하), 한국비교사법학회, 2001
- 하경효, “새로운 근로감시기술의 도입에 따른 법적 문제”, 『노동법학』 제18호, 한국노동법학회, 2004. 6
- 한상희, “정보화와 헌법”, 『법학논문집』 제26집 제2호, 중앙대학교 법학연구소, 2002. 11
- _____, “국가감시와 민주주의”, 『개인정보의 국가등록·관리제도의 문제점』 프라이버시보호 네트워크 제2차 공동토론회 요지집, 2001. 8. 22
- 한위수, “명예의 훼손과 민사상의 제문제”, 『사법논집』 제24집, 법원행정처, 1993
- 홍성욱, “벤담의 파놉티콘(Panopticon)에서 전자 시놉티콘(Synopticon)까지”, 『한국과학사학회지』 제23권 제1호, 한국과학사학회, 2001

참고문헌

- 홍준형, “전자정부와 개인정보보호”, 『정보과학회지』 제22권 제11호, 한국정보과학회, 2004. 11
- _____, “정보공개청구권과 정보공개법”, 『법과사회』 제6호, 법과사회이론연구회, 1992
- 황상철, “일본의 개인정보보호를 위한 입법동향 -개인정보의보호에 관한법률안을 중심으로-”, 『법제』 통권 제541호, 법제처, 2003. 1
- 황인호, “개인정보보호제도에서의 규제에 관한 연구 - 제도의 재구조화를 위한 입법론을 중심으로”, 『공법연구』 제30집 제4호, 한국공법학회, 2002

II. 외국문헌

1. 영미권

- Anthony. Giddens, *Social Theory and Modern Sociology*, Cambridge, UK: Polity Press, 1987
- Barbara S. Wellsberry, “Bridging the Difference: The Safe Harbor and Information Privacy in the United States and the European Union,” *Privacy and Information Law Report*(1 NO. 6 Privacy Info. L. Rep. 13), 2001
- Colin J. Bennett & Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, 2003
- Colin J. Bennett, *Regulating Privacy : Data Protection and Public Policy in Europe and the United States*, Ithaca : Cornell University Press, 1992

- Colin Bennett, "Convergence Revisited: Toward a Global Policy for the Protection of Personal Data?," *Technology And Privacy: The New Landscape* 99, Phillip E. Agre & Marc Rotenberg eds., 1997
- Daniel J. Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy," 53 *Stanford Law Review* 1393, 2001
- David Banisar/Simon Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments", 18 *J. Marshall J. Computer & Info. L.* 1, 1999
- David Harvey, *The Condition of Postmodernity - an Enquiry into the Origins of Cultural Change*, Cambridge, Mass: Blackwell, 1989
- David H. Flaherty, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, 1989
- David W. Leebron, "The Right to Privacy's Place in the Intellectual History of Tort Law", 41 *Case W. Res. L. Rev.* 769, 1991
- Douwe Korff, *Data Protection Law in the European Union*, DMA, 2005
- Erik Brynjolfsson and Brian Kahin, *Understanding the Digital Economy Data, Tools, and Research*, Cambridge, Mass.: MIT Press, 2000
- M. Ethan Katsh, *The Electronic Media and the Transformation of Law*, New York: Oxford University Press, 1989
- Fred H. Cate, *Privacy in the Information Age*, Brookings Institution Press, 1997

참 고 문 헌

- Henry H. Perrit Jr., *Law and the Information Superhighway*, Wiley Law Publications, 1996
- Herbert J. Spiro, “Privacy in Comparative Perspectives”, in: *Privacy Nomos XIII*, J. Roland Pennock & John W. Chapman eds., 1971
- James Michael, *Privacy and Human Rights*, Hampshire: Dartmouth, 1994
- Janlori Goldman, Zoe Hudson, and Richard M. Smith, California Health Care Foundation, *Privacy: Report on the Privacy Policies and Practices of Health Web Sites*, Jan. 2000
- Joel R. Reidenberg, “A New Legal Paradigm? Resolving Conflicting International Data Privacy Rules in Cyberspace”, *52 Stan. L. Rev.* 1315, 1342, May, 2000
- Joel R. Reidenberg, “Restoring Americans’ Privacy in Electronic Commerce”, *14 Berkeley Tech. L. J.* 771, 1999
- Joel R. Reidenberg, “Privacy Protection and the Interdependence of Law, Technology and Self-Regulation”, *23rd International Conference on Data Protection Commissioners*
- John Locke, *The Second Treatise of Government*(1690), Thomas P. Peardon ed., Liberal Arts Press, 1952
- Joseph I. Rosenbaum, “Privacy on the Internet: Whose Information is it Anyway?”, *38 Jurimetrics* 565, 1998
- J.W.K. Burnside, “The Fundamentals of Computer Technology,” Gordon Hughes(ed.), *Essays on Computer Law*, Melbourne, Australia: Longman Professional, 1990

- Lynn Margherio, *The Emerging Digital Economy*, Washington, D.C.: U.S. Department of Commerce, 1998
- Nigel Waters, “Re-thinking Information Privacy - A Third Way in Data Protection?”, *21st International Conference on Privacy and Personal Data Protection*, 1999. 9. 13
- Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection*, Michie Law Publishers, 1996
- Peter Knight and James Fitzsimons, *The legal environment of computing*, Sydney Reading, Mass: Addison Wesley Pub. Co., 1990
- Peter Carey, *Blackstone's Guide to Data Protection Act 1998*, Blackstone Press, Ltd, 1998
- Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Data Protection Directive*, 1998
- Philip Agre, “Introduction”, in: *Technology and Privacy: The New Landscape*, Philip E. Agre & Marc Rotenberg eds., 1997
- R. Gellman, “Conflict and Overlap in Privacy Regulation: National, International, and Private”, in: B. Kahin & C. Nesson (eds.), *Borders in Cyberspace*, MIT Press, 1997
- R. Clayton · H. Tomlinson, *The Law of Human Rights*, Oxford University Press, 2000
- Samuel D. Warren and Louis D. Brandeis, “The Right to Privacy”, 4 *Harv. L. Rev.* 193, 1890
- Swift, Ronald, “The new economic opportunity for business-creating increased profitability through CRM,” *CRM Project*, 2, 2001

참 고 문 헌

Thomas C. Cooley, *Laws of Torts*, 1st ed. 1880

William L. Prosser, “Privacy”, 48 *Cal. L. Rev.* 383, 1960

Yves Poullet, “Data Protection Between Property and Liberties: A Civil Law Approach”, in: *Amongst Friends in Computers and Law*, H.W.K. Kaspersen & A. Oskamp eds., 1990

2. 독 일

Hans H. Wohlgemuth, *Datenschutzrecht*, 2. Aufl., Berlin: Lutherhand, 1993

Konrad Hesse, *Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland*, 18. Aufl., Heidelberg: C. F. Müller Juristischer Verlag, 1991

Rudolf Schomerus/Peter Gola, *Bundesdatenschutzgesetz(BDSG)*, 5. Aufl. München: C. H. Beck, 1992

Wolfgang Hoffmann-Riem, “Informationelle Selbstbestimmung in der Informationsgesellschaft - Auf dem Wege zu einem neuen Konzept des Datenschutzes -”, *AöR*, Band 123, 1998

Carl Böhret/Werner Huffer, *Test und Prüfungen von Gesetzentwürfen, Anleitung zur Vorabkontrolle und Verbesserung von Rechtsvorschriften*, Köln/Bonn, 1980

3. 일 본

榎原猛, プライバシー權の総合的研究, 京都: 法律文化社, 1998

岡村久道, 新法解説 個人情報保護法入門, 商事法務, 2003

부
속

목 차

부록 I. 일반인 설문조사지 및 설문조사결과표	1003
I -1. 일반인 설문조사지	1003
I -2. 일반인 설문조사결과표	1017
1. 개인정보보호법제 입법체계에 대한 일반적 인식	1019
2. 개인정보보호 관련 일반적 인식	1025
부록 II. 전문가 설문조사지 및 설문조사결과표	1057
II-1. 전문가 설문조사지	1057
II-2. 전문가 설문조사결과표	1073
부록 III. 일본의 개인정보보호법 관련 자료	1113
III-1. 2004년도 일본 ‘행정기관개인정보보호법’ 시행상황 조사결과보고서	1113
III-2. 일본 ‘개인정보보호설명회참가자의 설문결과보고서 (2008.3) : 소비자 의식-집계결과표-	1149
III-3. 일본 개인정보보호에 관한법률시행령의 일부를 개정하는 정령(2008년정령제166호) 신구대조	1159
III-4. 개인정보보호에 관한 기본방침(2008.4.24)	1160

【부 록】

부록 I. 일반인 설문조사지 및 설문조사결과표

I -1. 일반인 설문조사지

최근 개인정보 이용에 대한 여러 의견들이 혼재되어 여론을 형성하고 있습니다. 한국법제 연구원에서는 ‘개인정보 보호법’ 입법을 위한 국민 여론을 조사하고 있습니다. 잠시만 시간을 내어 협조하여 주십시오. 감사합니다.

Quota	
선문1. 성별	① 남자 ② 여자
선문2. 연령	① 20대 ② 30대 ③ 40대 ④ 50대
선문3. 지역	① 서울 ② 부산 ③ 대구 ④ 인천 ⑤ 광주 ⑥ 대전 ⑦ 울산 ⑧ 경기 ⑨ 강원 ⑩ 충북 ⑪ 충남 ⑫ 전북 ⑬ 전남 ⑭ 경북 ⑮ 경남

[질문 1] 그 동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

- ① 있다 → [질문1-1]로 갈 것
- ② 없다 → [질문2]로 갈 것

[질문 1-1] 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

- ① 어려움이 있었다 → [질문1-2]로 갈 것
- ② 어려움이 별로 없었다 → [질문2]로 갈 것

[질문 1-2] 어려움을 느낀 이유는 무엇이라고 생각하십니까?

- ① 개인정보보호법의 존재를 몰라서 → [질문2]로 갈 것
- ② 개인정보보호에 관한 법률이 하나로 되어 있지 않아서 → [질문2]로 갈 것
- ③ 분야별로 관련 법률이 잘 구분되어 있지 않아서 → [질문2]로 갈 것
- ④ 새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않아서 → [질문2]로 갈 것
- ⑤ 기타 → [질문1-2-1]로 갈 것

[질문 1-2-1] 그 외 어려움을 느낀 이유는 무엇인지 응답하여 주십시오.

[질문 2] 다음 법률 가운데 개인정보의 보호를 위한 내용이 포함되어 있을 것으로 짐작 되는 법률을 모두 선택하여 주십시오.

- ① 공공기관의 개인정보보호에 관한 법률
- ② 정보통신망 이용 촉진 및 정보보호 등에 관한 법률
- ③ 신용정보의 이용 및 보호에 관한 법률
- ④ 전자정부법
- ⑤ 금융실명거래 및 비밀보장에 관한 법률
- ⑥ 통신비밀보호법
- ⑦ 보건의료기본법
- ⑧ 주민등록법
- ⑨ 국세기본법
- ⑩ 특정범죄신고자 등 보호법
- ⑪ 형법
- ⑫ 위의 법률 어느 것에도 포함 되어 있지 않을 것 같음

[2-1] 우리나라의 현행 개인정보보호 관련 입법은 공공부문과 민간 부문으로 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[2-2] 공공부문의 개인정보보호에 적용되는 『공공기관의 개인정보보호에 관한 법률』은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

- ① 잘 알고 있다
- ② 막연히 짐작하고 있는 정도이다
- ③ 공공기관이 보유하는 개인정보는 모두 보호의 대상이 되는 줄 알았다
- ④ 컴퓨터로 처리되지 않는 개인정보도 보호를 받을 수 있는 줄 알았다
- ⑤ 모든 개인정보가 그 보호의 대상이 되는 줄 알았다
- ⑥ 전혀 몰랐다

[2-3] 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며 개별 분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[질문 3] 현재 본인의 개인 정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보

호되고 있다고 느끼십니까?

답란	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
	①	②	③	④	⑤
	→질문 4로 갈 것		→질문 5로 갈 것		

[질문 4] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이라고 생각하시는지 1순위부터 3순위까지 응답하여 주십시오.

1순위 _____ 2순위 _____ 3순위 _____

- ① 법률규정의 미비 내지는 복잡성
- ② 교육이나 홍보부족
- ③ 정부나 사업자의 인식부족
- ④ 일반인의 인식부족
- ⑤ 개인정보 활용의 필요성
- ⑥ 기타 → [질문4-1]로 갈 것

[질문 4-1] 그 외 어려움을 느낀 이유는 무엇인지 응답하여 주십시오.

[질문 5] 현재는 개인정보가 부분적으로 보호되고 있습니다 개인정보 보호 보호를 보다 강화하기 위한 「개인정보보호법」의 제정이 필요하다고 생각하십니까?

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 보통이다
- ④ 시급하지는 않지만 필요하다
- ⑤ 시급히, 매우 필요하다

[질문 6] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 *위험하다고* 생각하십니까?

- ① 위험하다 ② 위험하지 않다 ③ 잘 모르겠다

[질문 6-1] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 *불쾌하다고* 생각하십니까?

- ① 불쾌하다 ② 불쾌하지 않다 ③ 잘 모르겠다

[질문 7] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 *위험하다고* 생각하십니까?

- ① 위험하다 ② 위험하지 않다 ③ 잘 모르겠다

[질문 7-1] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 *불쾌하다고* 생각하십니까?

- ① 불쾌하다 ② 불쾌하지 않다 ③ 잘 모르겠다

[질문 8] 앞의 질문6,7 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 *위험하다고* 생각하십니까?

- ① 위험하다 ② 위험하지 않다 ③ 잘 모르겠다

[질문 8-1] 앞의 질문6,7 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이

나 기업과 공유하는 것에 대하여 **불쾌하다**고 생각하십니까?

- ① 불쾌하다 ② 불쾌하지 않다 ③ 잘 모르겠다

[질문 9] 정부, 기업 각각의 개인정보처리 관련해서 오/남용 가능성은 얼마나 된다고 생각하십니까?

	매우 가능성 높다	가능성 높다	보통이다	가능성 없다	전혀 가능성 없다
정부의 개인정보처리 오/남용 가능성	⑤-----	④-----	③-----	②-----	①-----
기업의 개인정보처리 오/남용 가능성	⑤-----	④-----	③-----	②-----	①-----

[질문 10] 정부, 기업에서 개인정보처리가 오/남용 되었을 경우 얼마나 위험하다고 생각하십니까?

	매우 위험하다	위험하다	보통이다	위험하지 않다	전혀 위험하지 않다
정부의 개인정보처리 오/남용 되는 경우 위험성	⑤-----	④-----	③-----	②-----	①-----
기업의 개인정보처리 오/남용 되는 경우 위험성	⑤-----	④-----	③-----	②-----	①-----

[질문 11] 정부나 기업 등 개인정보처리자가 자신의 업무를 수행하는 과정에서 타인의 개인정보를 수집하게 됩니다. 다음의 수집행위가 본인의 동의 없이 이루어진다면 프라이버시침해 등의 문제가 발생한다고 생각하십니까?

행 위	매우 그렇다	그렇다	보통이다	그렇지 않다	매우 그렇지 않다
① 광고기획사가 연예인에 관하여 시중에 떠도는 스캔들소문을 수집하는 행위	⑤-----	④-----	③-----	②-----	①-----

행 위	매우 그렇다	그렇다	보통 이다	그렇지 않다	매우 그렇지 않다
② 기업이 입사원서를 낸 사람들의 평판, 업무능력에 대한 주위사람들의 평가 등의 정보를 수집하는 행위	⑤	④	③	②	①
③ 은행이 대출신청자의 신용도를 평가하는데 필요한 개인정보를 수집하는 행위	⑤	④	③	②	①
④ 인터넷쇼핑몰이 이용자의 소비취향에 관한 정보를 수집하는 행위	⑤	④	③	②	①
⑤ 무료만화를 제공하는 인터넷사이트가 이용자의 만화취향이나 읽는 습관을 알아보기 위하여 관련 정보를 수집하는 행위	⑤	④	③	②	①
⑥ (홈페이지에 수집을 금한다는 경고문이 없을 경우)공개된 나의 홈페이지에 게시된 나의 관한 개인정보를 수집하는 행위	⑤	④	③	②	①
⑦ (홈페이지에 수집을 금한다는 경고문이 있는 경우)공개된 나의 홈페이지에 게시된 나의 관한 개인정보를 수집하는 행위	⑤	④	③	②	①

[질문 12] CCTV의 설치와 관련하여 아래의 행위는 프라이버시침해 등의 문제가 발생한다고 생각하십니까? (이 CCTV는 범죄가 발생할 경우 문제의 상황이나 장면을 다시 볼 수 있도록 하는 기능만 있음)

행 위	매우 그렇다	그렇다	보통 이다	그렇지 않다	매우 그렇지 않다
① 아파트의 안전을 목적으로 지하주차장에 CCTV를 설치하여 오가는 사람들의 모습을 단순 녹화하는 행위	⑤	④	③	②	①
② 아파트관리원이 입구에 설치된 CCTV를 활용하여 302호에 사는 A씨의 출퇴근시간을 계속적으로 기록하는 행위	⑤	④	③	②	①

행 위	매우 그렇다	그렇다	보통 이다	그렇지 않다	매우 그렇지 않다
③ 대중목욕탕에서 도난사고가 잦아 탈의실에 CCTV를 설치하여 사람들의 모습을 단순 녹화하는 행위	⑤---④---③---②---①				

[질문 13] 다른 사람(기업 또는 정부 포함)이 자신의 비용으로 수집·이용하고 있는 나에 관한 개인정보는 누구의 것이라고 생각하십니까?

- ① 자신의 비용으로 처리하고 있는 그 사람의 자산이다
- ② 나의 개인정보는 나의 인격적 징표로서 나의 것이다
- ③ 그 누구의 것도 아니다

[질문 14] 기업이 거래과정에서 고객으로부터 받은 연락정보(주소, 전화번호, 이메일주소)를 이용하여 자사의 다른 상품이나 서비스를 광고하는 것은 허용될 수 있다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 고객의 사전 동의가 있으면 허용 된다
- ③ 사후에 고객이 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 이용하는 것은 허용될 수 있다
- ④ 동의나 다른 조건 없이 자유롭게 허용 된다

[질문 15] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 소비자의 생활방식, 취미, 소비성향 등을 조사·분석하여 개인별 프로파일(카드사용내역을 조사하여 생활방식)을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 고객의 사전 동의가 있으면 허용 된다
- ③ 사후에 고객이 거부를 하면 더 이상 이용하지 않는다는 조건으

로 일단 이용하는 것은 허용될 수 있다

- ④ 동의나 다른 조건 없이 자유롭게 허용 된다

[질문 16] 대통령이 정부의 중요 직책에 적합한 인물을 임명하기 위하여 사회지도층에 해당하는 사람들의 인물정보를 수집하여 개인별 프로파일을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용되어서는 안 된다
- ② 해당자의 사전 동의가 있으면 허용 된다
- ③ 사후에 해당자가 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 이용하는 것은 허용될 수 있다
- ④ 꼭 필요한 범위 내에서는 동의나 다른 조건 없이 허용 된다
- ⑤ 공익상의 목적이므로 어떠한 정보를 수집하든 자유롭게 허용 된다

[질문 17] 기업이 수집한 나의 연락정보(이름, 주소, 전화번호, 이메일주소에 한함)를 제3자에게 돈을 받고 판매하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용되어서는 안 된다
- ② 나의 사전 동의가 있으면 허용 된다
- ③ 사후에 내가 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 판매하는 것은 허용될 수 있다 (판매에 관한 사실을 판매 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공 받은 제3자도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 나에게 수익의 일부나 혜택이 제공된다면 허용 된다
- ⑤ 동의나 다른 조건 없이 자유롭게 허용 된다

[질문 18] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 만든 (연락 정보를 제외한) 개인별 프로파일을 다른 기업에게 판매하는

것이 허용되어야 한다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 소비자의 사전 동의가 있으면 허용 된다
- ③ 사후에 소비자가 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 판매하는 것은 허용될 수 있다 (판매에 관한 사실을 판매 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 제3자도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 소비자에게 수익의 일부나 혜택이 제공된다면 허용 된다
- ⑤ 동의나 다른 조건 없이 자유롭게 허용 된다

[질문 19] 기업이 보유하고 있는 소비자의 개인정보를 수사기관의 요청에 따라 법관이 발부한 영장 없이 제공하는 것에 대하여 어떻게 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 개인의 사전 동의가 있으면 허용될 수 있다
- ③ 사후에 개인이 거부를 하면 더 이상 제공하지 않는다는 조건으로 일단 제공하는 것은 허용될 수 있다 (제공에 관한 사실을 제공 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 수사기관도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 수사기관에 개인정보를 제공하는 것이 법률에 따른 것이라면 허용 된다
- ⑤ 공익을 이유로 한 것이므로 자유롭게 허용 된다

[질문 20] 정부의 각 기관들은 자신의 소관업무의 수행을 위하여 관련 국민의 개인정보를 수집하여 각각 개인정보DB를 구축하고 이를 관리·이용하고 있습니다. 자신의 소관업무 수행목적 이외에 국민의 개인정보를 다른 기관에게 제공하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용되어서는 안 된다
- ② 개인의 사전 동의가 있으면 허용될 수 있다
- ③ 사후에 개인이 거부를 하면 더 이상 제공하지 않는다는 조건으로 일단 제공하는 것은 허용될 수 있다. (제공에 관한 사실을 제공 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 다른 기관도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 그 제공이 법률에 따라 행해진 것이면 허용 된다
- ⑤ 다른 기관의 이용목적이 ‘정당한 업무수행’이라면 동의나 조건 없이 허용될 수 있다

[질문 21] 앞의 질문에서 제공받는 기관이 수사기관이라고 한다면 그 정보제공에 대하여 어떻게 생각합니까?

- ① 절대 허용되어서는 안 된다
- ② 개인의 사전 동의가 있으면 허용될 수 있다
- ③ 사후에 개인이 거부를 하면 더 이상 제공하지 않는다는 조건으로 일단 제공하는 것은 허용될 수 있다 (제공에 관한 사실을 제공 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 수사기관도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 수사기관에 개인정보를 제공하는 것이 법률에 따른 것이면 허용 된다
- ⑤ 공익을 이유로 한 것이므로 자유롭게 허용 된다

[질문 22] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 각 정부기관들이 자신의 소관업무의 수행을 위하여 공유하는 것에 대하여 어떻게 생각하십니까? (민원업무의 처리가 빠르고 행정기관에 필요한 서류를 제출하지 않아도 되는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

- ① 전혀 바람직하지 않다
- ② 바람직하지 않다
- ③ 그저 그렇다
- ④ 바람직하다
- ⑤ 매우 바람직하다

[질문 23] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 금융기관의 업무수행을 위하여 금융기관들과 공유하는 것이 필요하다고 생각하십니까? (금융기관 이용자는 금융기관에 제출하여야 하는 서류를 줄일 수 있고 금융기관은 이용자가 제출한 정보가 진실한 것인지를 확인할 수 있는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 그저 그렇다
- ④ 필요하다
- ⑤ 반드시 필요하다

[질문 24] 인터넷사이트 회원 가입시 정확한 신상정보(실명, 주민등록번호, 주소, 전화번호 등)의 입력을 요구하는 경우가 대부분입니다. 이 때 회원가입을 하십니까?

- ① 별다른 거리낌 없이 정확한 신상정보를 입력하고 가입 한다
- ② 마지못해 입력하고 대부분 가입 한다
- ③ 신상정보를 요구하면 대부분 가입하지 않는다
- ④ 신상정보를 요구하면 절대 가입하지 않는다

[질문 25] 실명확인을 하지 않는 인터넷사이트에 회원가입을 할 때
당신은 자신의 정확한 신상정보를 입력하십니까?

- ① 언제나 정확한 신상정보를 입력한다
- ② 가끔 틀린 신상정보를 입력한다
- ③ 언제나 틀린 신상정보를 입력한다

[질문 26] 인터넷게시판실명제에 대하여 어떻게 생각하십니까?

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 그저 그렇다
- ④ 필요하다
- ⑤ 매우 필요하다

[질문 27] 인터넷에서 이용자의 신원이 쉽게 확인될 수 없도록 익명
또는 가명으로 인터넷을 이용할 수 있는 법적 환경 및 시스템이
갖추어진다면 이에 대해 어떻게 생각하십니까?

- ① 전혀 바람직하지 않다
- ② 바람직하지 않다
- ③ 그저 그렇다
- ④ 바람직하다
- ⑤ 매우 바람직하다

[질문 28] 인터넷게시판실명제가 시행되고 있습니다. 공공기관 홈페이지와 포털 등의 게시판에 글을 쓰기 위해서는 반드시 신원을 확인하도록 요구하고 있습니다. 신원확인을 하더라도 게시판에 글을 올리십니까?

부 록

- ① 별다른 거리낌 없이 정확한 정보를 입력하고, 글을 올린다
- ② 마지못해 입력하고 대부분 글을 올린다
- ③ 대부분 글을 올리지 않는다
- ④ 절대 글을 올리지 않는다

※ 마지막으로 통계분류를 위해 몇 가지만 여쭙보겠습니다.

[배문1] 직업으로 하시는 일은 무엇인가요?

- ① 농/임/어업 ② 자영업 ③ 판매/영업/서비스직
- ④ 생산/기능/노무직 ⑤ 사무/관리/전문직 ⑥ 주부
- ⑦ 학생 ⑧ 무직/퇴직/기타

[배문2] __님께서는 학교를 어디까지 마치셨나요?

- ① 고등학교 졸업 이하 ② 대학교 졸업 ③ 대학원 졸업 이상

[배문3] __님 닥의 한달 가구소득은 얼마인가요? 보너스, 은행이자 등을 모두 포함하여 말씀해 주세요.

- ① 99만원 이하 ② 100-199만원 ③ 200-299만원 ④ 300-399만원
- ⑤ 400-499만원 ⑥ 500만원 이상

I -2. 일반인 설문조사결과표

1. 조사방법: HRC 마스터 패널을 이용한 온라인 조사 2. 조사대상: 전국 성인 남녀 만20세~50세 3. 표본크기: 1000명 4. 표본구성					
	20대	30대	40대	50대	계
남성	125	145	143	96	509
여성	117	140	138	96	491
계	242	285	281	192	1000
* 표본 구성은 2007년 통계청 인구센서스 자료에 근거하여 구성하였음					
5. 표본추출방법: 표본 할당 추출(Quota Sampling) 6. 조사기간: 2008년 9월 2일 ~ 2008년 9월 8일 7. 표본오차: 95% 신뢰수준에서± 3.1%					

응답자 분포표

Base= 전체		사례수(명)	%
전체		(1,000)	100.0
성별	남성	(509)	50.9
	여성	(491)	49.1
연령	20대	(242)	24.2
	30대	(285)	28.5
	40대	(281)	28.1
	50대	(192)	19.2
학력	고졸이하	(252)	25.2
	대졸	(634)	63.4
	대학원졸	(114)	11.4
직업	화이트	(434)	43.4
	블루	(189)	18.9
	주부	(200)	20.0
	학생	(120)	12.0
	무직/퇴직/기타	(57)	5.7
소득	상(500만원 이상)	(187)	18.7
	중(200만원-499만원 이하)	(640)	64.0
	하(199만원 이하)	(173)	17.3
지역	서울	(221)	22.1
	경기/인천	(285)	28.5
	강원	(29)	2.9
	충청	(98)	9.8
	전라	(99)	9.9
	경상	(268)	26.8

* 성/연령/지역 비중은 사전에 인구센서스 자료
(통계청 2007년)에 의하여 할당하였음

1. 개인정보보호법제 입법체계에 대한 일반적 인식

1) 개인정보보호 법조항 검색 관련

[표 1] 개인정보보호 관련 법조항 검색 여부

[문 1] 그동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

(단위:%)

		사례 수 (명)	경험 있음	경험 없음	계
■ 전체		(1000)	35.8	642	100.0
성별	남성	(509)	43.0	57.0	100.0
	여성	(491)	28.3	71.7	100.0
연령	20대	(242)	43.8	56.2	100.0
	30대	(285)	35.1	64.9	100.0
	40대	(281)	31.7	68.3	100.0
	50대	(192)	32.8	67.2	100.0
직업	화이트	(434)	42.9	57.1	100.0
	블루	(189)	33.9	66.1	100.0
	주부	(200)	24.0	76.0	100.0
	학생	(120)	31.7	68.3	100.0
소득 수준	상	(187)	35.8	64.2	100.0
	중	(640)	35.8	64.2	100.0
	하	(173)	35.8	64.2	100.0
지역	서울	(221)	33.0	67.0	100.0
	경기	(285)	35.8	64.2	100.0
	강원	(29)	37.9	62.1	100.0
	충청	(98)	39.8	60.2	100.0
	전라	(99)	44.4	55.6	100.0
	경상	(268)	33.2	66.8	100.0
학력	고졸이하	(252)	36.5	63.5	100.0
	대졸	(634)	34.9	65.1	100.0
	대학원졸 이상	(114)	39.5	60.5	100.0

부 록

[표 2] 개인정보보호 법조항 검색시 어려움 있었는지 여부

[문 1-1] 개인정보보호를 위한 관련 법조항을 찾는데 어려움은 없었습니까?

(단위:%)

		사례수(명)	어려움 있었다	어려움이 별로 없었다	계
■ 전체		(358)	87.2	128	100.0
성별	남성	(219)	85.4	146	100.0
	여성	(139)	89.9	10.1	100.0
연령	20대	(106)	89.6	10.4	100.0
	30대	(100)	87.0	13.0	100.0
	40대	(89)	87.6	12.4	100.0
	50대	(63)	82.5	17.5	100.0
직업	화이트	(186)	88.2	11.8	100.0
	블루	(64)	81.3	18.8	100.0
	주부	(48)	89.6	10.4	100.0
	학생	(38)	86.8	13.2	100.0
소득 수준	상	(67)	89.6	10.4	100.0
	중	(229)	86.5	13.5	100.0
	하	(62)	87.1	12.9	100.0
지역	서울	(73)	80.8	19.2	100.0
	경기	(102)	88.2	11.8	100.0
	강원	(11)	72.7	27.3	100.0
	충청	(39)	87.2	12.8	100.0
	전라	(44)	81.8	18.2	100.0
	경상	(89)	95.5	4.5	100.0
학력	고졸이하	(92)	89.1	10.9	100.0
	대졸	(221)	88.7	11.3	100.0
	대학원졸 이상	(45)	75.6	24.4	100.0

[표 3] 검색시 어려움을 느낀 이유

[문 1-2] 어려움을 느낀 이유는 무엇이라고 생각하십니까?

(단위:%)

		사례수 (명)	분야별로 관련 법 률이 잘 구분되어 있지 않 아서	새로운 문제에 대처할 수 있는 조항이 마련 되어 있지 않 아서	개인정보 보호법의 존재를 몰라서	개인 정보 보호에 관한 법 률이 하 나로 되 어 있지 않아서	용어가 어려워 서/잘 몰 라서	계
■ 전체		(312)	38.1	21.2	19.2	18.9	2.6	100.0
성별	남성	(187)	39.0	20.3	18.2	19.8	2.7	100.0
	여성	(125)	36.8	22.4	20.8	17.6	2.4	100.0
연령	20대	(95)	43.2	18.9	21.1	13.7	3.2	100.0
	30대	(87)	35.6	16.1	23.0	20.7	4.6	100.0
	40대	(78)	38.5	23.1	15.4	21.8	1.3	100.0
	50대	(52)	32.7	30.8	15.4	21.2		100.0
직업	화이트	(164)	39.6	20.7	16.5	20.7	2.4	100.0
	블루	(52)	34.6	34.6	15.4	15.4		100.0
	주부	(43)	27.9	14.0	34.9	20.9	2.3	100.0
	학생	(33)	48.5	18.2	18.2	12.1	3.0	100.0
소득 수준	상	(60)	35.0	20.0	20.0	21.7	3.3	100.0
	중	(198)	41.4	21.2	16.7	18.7	2.0	100.0
	하	(54)	29.6	22.2	27.8	16.7	3.7	100.0
지역	서울	(59)	35.6	23.7	25.4	11.9	3.4	100.0
	경기	(90)	35.6	18.9	17.8	24.4	3.3	100.0
	강원	(8)	12.5	50.0	12.5		25.0	100.0
	충청	(34)	41.2	14.7	20.6	23.5		100.0
	전라	(36)	36.1	33.3	11.1	19.4		100.0
	경상	(85)	44.7	16.5	20.0	17.6	1.2	100.0
학력	고졸이하	(82)	34.1	23.2	23.2	17.1	2.4	100.0
	대졸	(196)	38.8	19.9	18.9	19.4	3.1	100.0
	대학원졸 이상	(34)	44.1	23.5	11.8	20.6		100.0

*강원 지역은 사례수가 적어 해석시 주의를 요함

2) 개인정보보호법제 개념 이해 및 인지 수준

[표 4] 개인정보보호법 공공부문과 민간부문 별도 적용 인지 여부

[문 2-1] 우리나라의 현행 개인정보보호 관련 입법은 공공부문과 민간부문으로 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대해 알고 계십니까?

(단위:%)

		사례수(명)	잘 알고 있다	그동안 잘 몰랐다	계
■ 전체		(1000)	9.1	909	100.0
성별	남성	(509)	10.6	894	100.0
	여성	(491)	7.5	925	100.0
연령	20대	(242)	8.7	913	100.0
	30대	(285)	6.0	940	100.0
	40대	(281)	9.6	904	100.0
	50대	(192)	13.5	865	100.0
직업	화이트	(434)	9.9	90.1	100.0
	블루	(189)	10.6	89.4	100.0
	주부	(200)	7.0	93.0	100.0
	학생	(120)	5.0	95.0	100.0
소득 수준	상	(187)	9.1	90.9	100.0
	중	(640)	9.1	90.9	100.0
	하	(173)	9.2	90.8	100.0
지역	서울	(221)	10.9	89.1	100.0
	경기	(285)	8.1	91.9	100.0
	강원	(29)	6.9	93.1	100.0
	충청	(98)	12.2	87.8	100.0
	전라	(99)	9.1	90.9	100.0
	경상	(268)	7.8	92.2	100.0
학력	고졸이하	(252)	7.9	92.1	100.0
	대졸	(634)	8.5	91.5	100.0
	대학원졸 이상	(114)	14.9	85.1	100.0

[표 5] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호 대상인 점 인지 여부

[문 2-2] 공공부문의 개인정보보호에 적용되는 「공공기관의 개인정보보호에 관한 법률」은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

(단위: %)

		사례수 (명)	잘 알고 있다	막연히 짐작	공공기관 보유 개 인정보는 모두 대 상	컴퓨터로 처리되지 않는 개 인정보도 포함	모든 개 인정보 포함	전혀 몰 랐다	계
□ 전체		(1000)	3.5	26.5	27.2	8.8	19.4	14.6	100.0
성별	남성	(509)	4.1	29.1	25.5	9.4	17.3	14.5	100.0
	여성	(491)	2.9	23.8	28.9	8.1	21.6	14.7	100.0
연령	20대	(242)	4.1	19.4	23.1	13.6	22.3	17.4	100.0
	30대	(285)	0.7	26.7	27.0	8.4	20.4	16.8	100.0
	40대	(281)	5.7	28.8	28.1	6.0	18.1	13.2	100.0
	50대	(192)	3.6	31.8	31.3	7.3	16.1	9.9	100.0
직업	화이트	(434)	3.2	27.2	30.9	10.4	15.4	12.9	100.0
	블루	(189)	4.2	31.7	27.0	5.3	19.0	12.7	100.0
	주부	(200)	3.0	25.0	26.5	6.5	22.0	17.0	100.0
	학생	(120)	4.2	20.0	15.0	13.3	30.0	17.5	100.0
소득 수준	상	(187)	2.7	27.8	26.7	7.0	21.9	13.9	100.0
	중	(640)	3.6	26.9	28.1	9.5	18.1	13.8	100.0
	하	(173)	4.0	23.7	24.3	8.1	21.4	18.5	100.0
지역	서울	(221)	2.7	26.7	26.7	7.2	21.3	15.4	100.0
	경기	(285)	4.9	24.9	26.7	10.2	18.9	14.4	100.0
	강원	(29)	6.9	20.7	10.3	3.4	20.7	37.9	100.0
	충청	(98)	7.1	29.6	24.5	12.2	15.3	11.2	100.0
	전라	(99)	2.0	32.3	29.3	7.1	15.2	14.1	100.0
	경상	(268)	1.5	25.4	30.2	8.6	21.3	13.1	100.0
학력	고졸이하	(252)	5.2	23.0	28.6	9.9	18.3	15.1	100.0
	대졸	(634)	3.0	28.2	24.6	8.7	20.5	15.0	100.0
	대학원졸 이상	(114)	2.6	24.6	38.6	7.0	15.8	11.4	100.0

부 록

[표 6] 민간부문의 개인정보보호법 개별분야별 법률만 있는 점 인지 여부

[문 2-3] 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며 개별 분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?

(단위:%)

		사례수(명)	잘 알고 있다	그동안 잘 몰랐다	계
■ 전체		(1000)	6.9	93.1	100.0
성별	남성	(509)	8.3	91.7	100.0
	여성	(491)	5.5	94.5	100.0
연령	20대	(242)	9.1	90.9	100.0
	30대	(285)	3.5	96.5	100.0
	40대	(281)	7.5	92.5	100.0
	50대	(192)	8.3	91.7	100.0
직업	화이트	(434)	7.1	92.9	100.0
	블루	(189)	7.4	92.6	100.0
	주부	(200)	5.0	95.0	100.0
	학생	(120)	5.0	95.0	100.0
소득 수준	상	(187)	9.1	90.9	100.0
	중	(640)	5.6	94.4	100.0
	하	(173)	9.2	90.8	100.0
지역	서울	(221)	6.8	93.2	100.0
	경기	(285)	4.6	95.4	100.0
	강원	(29)	10.3	89.7	100.0
	충청	(98)	15.3	84.7	100.0
	전라	(99)	8.1	91.9	100.0
	경상	(268)	5.6	94.4	100.0
학력	고졸이하	(252)	6.0	94.0	100.0
	대졸	(634)	7.1	92.9	100.0
	대학원졸 이상	(114)	7.9	92.1	100.0

2. 개인정보보호 관련 일반적 인식

1) 개인정보보호의 현황에 대한 인식

[표 7] 개인 정보가 제대로 보호되고 있는지에 대한 동의

[문 3] 현재 본인의 개인 정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보호되고 있다고 느끼십니까?

(단위:%)

		사례수 (명)	매우 그렇다	그렇다	Top2	보통이다	그렇지 않다	전혀 그렇지 않다	Bottom2	Mean (점)
□ 전체		(1000)	0.5	4.7	5.2	22.5	52.0	20.3	72.3	(2.13)
성별	남성	(509)	0.6	5.3	5.9	23.6	49.3	21.2	70.5	(2.15)
	여성	(491)	0.4	4.1	4.5	21.4	54.8	19.3	74.1	(2.11)
연령	20대	(242)	1.2	6.2	7.4	28.5	42.1	21.9	64.0	(2.23)
	30대	(285)		2.5	2.5	17.9	60.4	19.3	79.6	(2.04)
	40대	(281)		5.0	5.0	19.9	54.1	21.0	75.1	(2.09)
	50대	(192)	1.0	5.7	6.8	25.5	49.0	18.8	67.7	(2.21)
직업	화이트	(434)	0.5	3.7	4.1	23.3	51.6	21.0	72.6	(2.11)
	블루	(189)		4.2	4.2	22.2	52.9	20.6	73.5	(2.1)
	주부	(200)	0.5	4.5	5.0	20.0	56.5	18.5	75.0	(2.12)
	학생	(120)	0.8	8.3	9.2	27.5	44.2	19.2	63.3	(2.28)
소득 수준	상	(187)		5.3	5.3	20.9	50.3	23.5	73.8	(2.08)
	중	(640)	0.5	4.7	5.2	23.1	53.0	18.8	71.7	(2.15)
	하	(173)	1.2	4.0	5.2	22.0	50.3	22.5	72.8	(2.11)
지역	서울	(221)	0.5	3.6	4.1	21.7	50.2	24.0	74.2	(2.06)
	경기	(285)	0.4	3.5	3.9	18.2	57.9	20.0	77.9	(2.06)
	강원	(29)	3.4	3.4	6.9	27.6	37.9	27.6	65.5	(2.17)
	충청	(98)		6.1	6.1	22.4	48.0	23.5	71.4	(2.11)
	전라	(99)	1.0	7.1	8.1	31.3	41.4	19.2	60.6	(2.29)
	경상	(268)	0.4	5.6	6.0	23.9	54.1	16.0	70.1	(2.2)
학력	고졸이하	(252)	1.2	4.0	5.2	20.2	52.4	22.2	74.6	(2.1)
	대졸	(634)	0.3	5.2	5.5	23.5	52.4	18.6	71.0	(2.16)
	대학원졸 이상	(114)		3.5	3.5	21.9	49.1	25.4	74.6	(2.04)

[표 8] 개인 정보가 제대로 보호되고 있지 않다고 생각하는 이유

[문 4] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이
라고 생각하시는지 1순위부터 3순위까지 응답하여 주십시오.

(단위: %, 복수응답)

		사례 수 (명)	법률규정 의 미비 내지는 복잡성	정 부 나 사 업 자 의 인 식 부 족	일 반 인 의 인 식 부 족	교 육 이 나 홍 보 부 족	개 인 정 보 활 용 의 필 요 성
■ 전체		(723)	85.6	79.5	58.0	42.7	32.8
성별	남성	(359)	86.4	83.0	57.7	43.5	28.7
	여성	(364)	84.9	76.1	58.2	42.0	36.8
연령	20대	(155)	81.9	83.2	64.5	36.1	32.9
	30대	(227)	89.0	80.6	54.6	41.0	33.0
	40대	(211)	84.8	80.6	58.8	43.1	32.2
	50대	(130)	85.4	71.5	54.6	53.1	33.1
직업	화이트	(315)	87.9	83.2	56.8	41.6	28.9
	블루	(139)	86.3	77.0	55.4	43.2	36.0
	주부	(150)	83.3	70.0	59.3	46.7	40.0
	학생	(76)	80.3	88.2	65.8	35.5	28.9
소득 수준	상	(138)	85.5	80.4	56.5	41.3	33.3
	중	(459)	85.8	79.3	57.1	45.3	31.4
	하	(126)	84.9	79.4	62.7	34.9	37.3
지역	서울	(164)	81.7	81.7	61.6	37.8	35.4
	경기	(222)	87.4	79.3	64.0	39.6	27.9
	강원	(19)	78.9	78.9	47.4	68.4	26.3
	충청	(70)	81.4	80.0	51.4	50.0	35.7
	전라	(60)	85.0	80.0	58.3	38.3	38.3
	경상	(188)	89.4	77.7	51.1	46.8	34.0
학력	고졸이하	(188)	87.2	78.7	57.4	42.0	31.9
	대졸	(450)	86.2	79.1	58.4	42.7	32.7
	대학원졸 이상	(85)	78.8	83.5	56.5	44.7	35.3

[표 9] 강화된 ‘개인정보보호법’ 제정의 필요도

[문 5] 현재는 개인정보가 부분적으로 보호되고 있습니다 개인정보 보호를 보다 강화하기 위한 『개인정보보호법』의 제정이 필요하다고 생각하십니까?

(단위:%)

		사례수 (명)	시급히 매우 필요하다	시급하 지는 않지만 필요하다	TO P 2	보통이다	필요하 지 않 다	전혀 필요하 지 않 다	BO T T O M 2	M ean (점)
■ 전체		(1000)	70.3	22.5	92.8	4.8	2.2	0.2	2.4	(4.61)
성별	남성	(509)	69.5	23.6	93.1	4.5	2.0	0.4	2.4	(4.6)
	여성	(491)	71.1	21.4	92.5	5.1	2.4		2.4	(4.61)
연령	20대	(242)	62.8	28.5	91.3	4.5	3.7	0.4	4.1	(4.5)
	30대	(285)	71.6	21.8	93.3	4.9	1.8		1.8	(4.63)
	40대	(281)	77.2	16.0	93.2	5.0	1.8		1.8	(4.69)
	50대	(192)	67.7	25.5	93.2	4.7	1.6	0.5	2.1	(4.58)
직업	화이트	(434)	73.3	20.0	93.3	4.4	1.8	0.5	2.3	(4.64)
	블루	(189)	70.9	21.2	92.1	5.8	2.1		2.1	(4.61)
	주부	(200)	68.5	24.0	92.5	5.0	2.5		2.5	(4.59)
	학생	(120)	61.7	32.5	94.2	2.5	3.3		3.3	(4.53)
소득 수준	상	(187)	71.1	24.1	95.2	3.2	1.6		1.6	(4.65)
	중	(640)	70.9	22.3	93.3	4.5	2.0	0.2	2.2	(4.62)
	하	(173)	67.1	21.4	88.4	7.5	3.5	0.6	4.0	(4.51)
지역	서울	(221)	75.1	18.6	93.7	4.5	1.4	0.5	1.8	(4.67)
	경기	(285)	68.4	24.6	93.0	4.2	2.8		2.8	(4.59)
	강원	(29)	72.4	17.2	89.7	3.4	6.9		6.9	(4.55)
	충청	(98)	72.4	17.3	89.8	5.1	4.1	1.0	5.1	(4.56)
	전라	(99)	63.6	30.3	93.9	4.0	2.0		2.0	(4.56)
	경상	(268)	69.8	23.1	92.9	6.0	1.1		1.1	(4.62)
학력	고졸이하	(252)	71.0	22.2	93.3	4.4	2.4		2.4	(4.62)
	대졸	(634)	70.7	22.6	93.2	4.3	2.2	0.3	2.5	(4.61)
	대학원졸 이상	(114)	66.7	22.8	89.5	8.8	1.8		1.8	(4.54)

2) 정부/기업 개인정보DB 구축 및 이용에 관한 태도

[표 10] 정부의 개인정보DB 구축 및 이용에 대한 위험성

[문 6] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 *위험하다고* 생각하십니까?

(단위:%)

		사례 수(명)	위험하다	위험하지 않다	잘 모르겠다	계
■ 전체		(1000)	74.5	5.0	20.5	100.0
성별	남성	(509)	79.8	4.7	15.5	100.0
	여성	(491)	69.0	5.3	25.7	100.0
연령	20대	(242)	81.4	3.7	14.9	100.0
	30대	(285)	76.1	4.6	19.3	100.0
	40대	(281)	74.7	3.9	21.4	100.0
	50대	(192)	63.0	8.9	28.1	100.0
직업	화이트	(434)	78.6	5.1	16.4	100.0
	블루	(189)	70.4	5.8	23.8	100.0
	주부	(200)	64.0	4.5	31.5	100.0
	학생	(120)	83.3	2.5	14.2	100.0
소득 수준	상	(187)	72.2	6.4	21.4	100.0
	중	(640)	75.0	4.4	20.6	100.0
	하	(173)	75.1	5.8	19.1	100.0
지역	서울	(221)	76.9	4.1	19.0	100.0
	경기	(285)	75.1	2.5	22.5	100.0
	강원	(29)	79.3	6.9	13.8	100.0
	충청	(98)	74.5	7.1	18.4	100.0
	전라	(99)	70.7	7.1	22.2	100.0
	경상	(268)	72.8	6.7	20.5	100.0
학력	고졸이하	(252)	67.5	4.4	28.2	100.0
	대졸	(634)	76.5	4.4	19.1	100.0
	대학원졸 이상	(114)	78.9	9.6	11.4	100.0

[표 11] 정부의 개인정보DB 구축 및 이용에 대한 불쾌감

[문 6-1] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 *불쾌하다*고 생각하십니까?

(단위:%)

		사례 수 (명)	불쾌하다	불쾌하지 않다	잘 모르겠다	계
■ 전체		(1000)	74.6	11.7	13.7	100.0
성별	남성	(509)	72.3	14.5	13.2	100.0
	여성	(491)	77.0	8.8	14.3	100.0
연령	20대	(242)	74.0	12.4	13.6	100.0
	30대	(285)	75.1	11.2	13.7	100.0
	40대	(281)	78.3	10.7	11.0	100.0
	50대	(192)	69.3	13.0	17.7	100.0
직업	화이트	(434)	77.2	13.4	9.4	100.0
	블루	(189)	72.0	10.1	18.0	100.0
	주부	(200)	76.5	6.0	17.5	100.0
	학생	(120)	68.3	18.3	13.3	100.0
소득 수준	상	(187)	73.8	13.9	12.3	100.0
	중	(640)	74.8	11.6	13.6	100.0
	하	(173)	74.6	9.8	15.6	100.0
지역	서울	(221)	78.7	11.3	10.0	100.0
	경기	(285)	74.0	11.9	14.0	100.0
	강원	(29)	65.5	13.8	20.7	100.0
	충청	(98)	76.5	13.3	10.2	100.0
	전라	(99)	67.7	16.2	16.2	100.0
	경상	(268)	74.6	9.3	16.0	100.0
학력	고졸이하	(252)	75.0	8.7	16.3	100.0
	대졸	(634)	75.6	11.0	13.4	100.0
	대학원졸 이상	(114)	68.4	21.9	9.6	100.0

[표 12] 기업의 개인정보DB 구축 및 이용에 대한 위험성

[문 7] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 *위험하다*고 생각하십니까?

(단위:%)

		사례수(명)	위험하다	위험하지 않다	잘 모르겠다	계
■ 전체		(1000)	93.9	1.8	4.3	100.0
성별	남성	(509)	94.3	2.0	3.7	100.0
	여성	(491)	93.5	1.6	4.9	100.0
연령	20대	(242)	94.2	2.1	3.7	100.0
	30대	(285)	91.6	2.1	6.3	100.0
	40대	(281)	94.7	1.4	3.9	100.0
	50대	(192)	95.8	1.6	2.6	100.0
직업	화이트	(434)	94.9	2.5	2.5	100.0
	블루	(189)	91.0	2.6	6.3	100.0
	주부	(200)	93.5	0.5	6.0	100.0
	학생	(120)	96.7	0.8	2.5	100.0
소득 수준	상	(187)	96.3	2.7	1.1	100.0
	중	(640)	93.0	1.7	5.3	100.0
	하	(173)	94.8	1.2	4.0	100.0
지역	서울	(221)	95.9	1.8	2.3	100.0
	경기	(285)	94.0	1.4	4.6	100.0
	강원	(29)	93.1		6.9	100.0
	충청	(98)	93.9	2.0	4.1	100.0
	전라	(99)	92.9	1.0	6.1	100.0
	경상	(268)	92.5	2.6	4.9	100.0
학력	고졸이하	(252)	92.9	1.6	5.6	100.0
	대졸	(634)	93.7	1.9	4.4	100.0
	대학원졸 이상	(114)	97.4	1.8	0.9	100.0

[표 13] 기업의 개인정보DB 구축 및 이용에 대한 불쾌감

[문 7-1] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보 DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 불쾌하다고 생각하십니까?

(단위:%)

		사례수(명)	불쾌하다	불쾌하지 않다	잘 모르겠다	계
■ 전체		(1000)	92.5	2.6	4.9	100.0
성별	남성	(509)	92.5	2.9	4.5	100.0
	여성	(491)	92.5	2.2	5.3	100.0
연령	20대	(242)	92.6	3.3	4.1	100.0
	30대	(285)	90.2	3.5	6.3	100.0
	40대	(281)	94.3	1.8	3.9	100.0
	50대	(192)	93.2	1.6	5.2	100.0
직업	화이트	(434)	93.1	3.9	3.0	100.0
	블루	(189)	91.0	2.1	6.9	100.0
	주부	(200)	91.5	1.0	7.5	100.0
	학생	(120)	95.0	1.7	3.3	100.0
소득 수준	상	(187)	95.2	2.1	2.7	100.0
	중	(640)	91.6	2.7	5.8	100.0
	하	(173)	93.1	2.9	4.0	100.0
지역	서울	(221)	94.6	2.7	2.7	100.0
	경기	(285)	91.9	3.2	4.9	100.0
	강원	(29)	89.7	3.4	6.9	100.0
	충청	(98)	92.9	4.1	3.1	100.0
	전라	(99)	90.9	1.0	8.1	100.0
	경상	(268)	92.2	1.9	6.0	100.0
학력	고졸이하	(252)	92.9	1.2	6.0	100.0
	대졸	(634)	92.3	2.7	5.0	100.0
	대학원졸 이상	(114)	93.0	5.3	1.8	100.0

[표 14] 정부/기업의 개인정보DB 공유에 대한 위험성

[문 8] 앞의 질문 6, 7 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 *위험하다고* 생각하십니까?

(단위:%)

		사례수(명)	위험하다	위험하지 않다	잘 모르겠다	계
■ 전체		(1000)	88.4	3.8	7.8	100.0
성별	남성	(509)	90.8	3.1	6.1	100.0
	여성	(491)	85.9	4.5	9.6	100.0
연령	20대	(242)	90.5	3.7	5.8	100.0
	30대	(285)	88.4	3.5	8.1	100.0
	40대	(281)	87.9	3.6	8.5	100.0
	50대	(192)	86.5	4.7	8.9	100.0
직업	화이트	(434)	90.8	4.1	5.1	100.0
	블루	(189)	88.4	4.2	7.4	100.0
	주부	(200)	83.0	3.5	13.5	100.0
	학생	(120)	93.3	0.8	5.8	100.0
소득 수준	상	(187)	90.9	3.7	5.3	100.0
	중	(640)	88.3	3.4	8.3	100.0
	하	(173)	86.1	5.2	8.7	100.0
지역	서울	(221)	91.0	2.7	6.3	100.0
	경기	(285)	88.1	3.9	8.1	100.0
	강원	(29)	86.2	3.4	10.3	100.0
	충청	(98)	91.8	4.1	4.1	100.0
	전라	(99)	89.9	1.0	9.1	100.0
	경상	(268)	85.1	5.6	9.3	100.0
학력	고졸이하	(252)	87.7	4.0	8.3	100.0
	대졸	(634)	87.9	4.4	7.7	100.0
	대학원졸 이상	(114)	93.0		7.0	100.0

[표 15] 정부/기업의 개인정보DB 공유에 대한 불쾌감

[문 8-1] 앞의 질문 6, 7 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 불쾌하다고 생각하십니까?

(단위:%)

		사례수(명)	불쾌하다	불쾌하지 않다	잘 모르겠다	계
■ 전체		(1000)	86.9	5.0	8.1	100.0
성별	남성	(509)	88.6	4.7	6.7	100.0
	여성	(491)	85.1	5.3	9.6	100.0
연령	20대	(242)	88.0	5.8	6.2	100.0
	30대	(285)	87.0	3.5	9.5	100.0
	40대	(281)	87.2	5.0	7.8	100.0
	50대	(192)	84.9	6.3	8.9	100.0
직업	화이트	(434)	89.4	5.1	5.5	100.0
	블루	(189)	86.2	3.2	10.6	100.0
	주부	(200)	82.5	6.0	11.5	100.0
	학생	(120)	89.2	4.2	6.7	100.0
소득 수준	상	(187)	88.2	4.3	7.5	100.0
	중	(640)	86.3	5.6	8.1	100.0
	하	(173)	87.9	3.5	8.7	100.0
지역	서울	(221)	88.2	5.9	5.9	100.0
	경기	(285)	86.7	4.6	8.8	100.0
	강원	(29)	86.2	3.4	10.3	100.0
	충청	(98)	87.8	6.1	6.1	100.0
	전라	(99)	86.9	5.1	8.1	100.0
	경상	(268)	85.8	4.5	9.7	100.0
학력	고졸이하	(252)	84.1	4.8	11.1	100.0
	대졸	(634)	87.1	5.5	7.4	100.0
	대학원졸 이상	(114)	92.1	2.6	5.3	100.0

[표 16] 정부의 개인정보 처리 관련 오/남용 가능성

[문 9] 정부, 기업 각각의 개인정보처리 관련해서 오/남용 가능성은 얼마나 된다고 생각하십니까?

(단위:%)

		사례수 (명)	매우 가 능성 높 다	가능성 높다	TOP 2	보통이 다	가능성 없다	전혀 가 능성 없 다	Bo ttom 2	M ean (점)
□ 전체		(1000)	29.2	53.7	82.9	15.9	1.0	0.2	1.2	(4.11)
성별	남성	(509)	32.6	50.1	82.7	15.9	1.2	0.2	1.4	(4.14)
	여성	(491)	25.7	57.4	83.1	15.9	0.8	0.2	1.0	(4.08)
연령	20대	(242)	31.4	48.3	79.8	18.2	1.7	0.4	2.1	(4.09)
	30대	(285)	28.8	53.7	82.5	16.5	1.1		1.1	(4.1)
	40대	(281)	33.1	52.7	85.8	13.9		0.4	0.4	(4.18)
	50대	(192)	21.4	62.0	83.3	15.1	1.6		1.6	(4.03)
직업	화이트	(434)	30.0	53.7	83.6	15.2	0.9	0.2	1.2	(4.12)
	블루	(189)	34.4	52.9	87.3	12.2	0.5		0.5	(4.21)
	주부	(200)	22.0	57.0	79.0	19.5	1.0	0.5	1.5	(3.99)
	학생	(120)	28.3	54.2	82.5	15.8	1.7		1.7	(4.09)
소득 수준	상	(187)	29.4	52.4	81.8	16.6	1.6		1.6	(4.1)
	중	(640)	29.5	53.8	83.3	15.8	0.8	0.2	0.9	(4.12)
	하	(173)	27.7	54.9	82.7	15.6	1.2	0.6	1.7	(4.08)
지역	서울	(221)	34.8	54.3	89.1	10.4	0.5		0.5	(4.24)
	경기	(285)	24.2	55.8	80.0	18.2	1.8		1.8	(4.02)
	강원	(29)	27.6	51.7	79.3	17.2		3.4	3.4	(4.)
	충청	(98)	40.8	40.8	81.6	15.3	2.0	1.0	3.1	(4.18)
	전라	(99)	28.3	54.5	82.8	16.2	1.0		1.0	(4.1)
	경상	(268)	26.1	55.6	81.7	17.9	0.4		0.4	(4.07)
학력	고졸이하	(252)	27.8	55.2	82.9	15.1	1.6	0.4	2.0	(4.08)
	대졸	(634)	30.1	53.3	83.4	15.8	0.6	0.2	0.8	(4.13)
	대학원졸 이상	(114)	27.2	52.6	79.8	18.4	1.8		1.8	(4.05)

[표 17] 기업의 개인정보 처리 관련 오/남용 가능성

[문 9] 정부, 기업 각각의 개인정보처리 관련해서 오/남용 가능성은 얼마나 된다고 생각하십니까?

(단위:%)

		사례수 (명)	매우 가 능성 높 다	가능성 높다	TOP 2	보통이 다	가능성 없다	전혀 가 능성 없 다	Bo ttom 2	M ean (점)
■ 전체		(1000)	55.5	40.4	95.9	3.9	0.1	0.1	0.2	(4.51)
성별	남성	(509)	59.9	36.9	96.9	2.8	0.2	0.2	0.4	(4.56)
	여성	(491)	50.9	44.0	94.9	5.1				(4.46)
연령	20대	(242)	61.6	33.1	94.6	4.5	0.4	0.4	0.8	(4.55)
	30대	(285)	55.8	41.4	97.2	2.8				(4.53)
	40대	(281)	55.9	39.9	95.7	4.3				(4.52)
	50대	(192)	46.9	49.0	95.8	4.2				(4.43)
직업	화이트	(434)	59.2	36.9	96.1	3.5	0.2	0.2	0.5	(4.55)
	블루	(189)	52.4	43.9	96.3	3.7				(4.49)
	주부	(200)	43.5	52.5	96.0	4.0				(4.4)
	학생	(120)	65.0	33.3	98.3	1.7				(4.63)
소득 수준	상	(187)	59.9	36.4	96.3	3.7				(4.56)
	중	(640)	55.5	40.6	96.1	3.9				(4.52)
	하	(173)	50.9	43.9	94.8	4.0	0.6	0.6	1.2	(4.44)
지역	서울	(221)	60.2	36.2	96.4	3.6				(4.57)
	경기	(285)	53.3	43.2	96.5	3.2	0.4		0.4	(4.49)
	강원	(29)	58.6	41.4	100.0					(4.59)
	충청	(98)	62.2	33.7	95.9	3.1		1.0	1.0	(4.56)
	전라	(99)	53.5	39.4	92.9	7.1				(4.46)
	경상	(268)	51.9	43.7	95.5	4.5				(4.47)
학력	고졸이하	(252)	50.8	44.0	94.8	4.8	0.4		0.4	(4.45)
	대졸	(634)	55.5	40.5	96.1	3.8		0.2	0.2	(4.51)
	대학원졸 이상	(114)	65.8	31.6	97.4	2.6				(4.63)

[표 18] 정부의 개인정보 처리 관련 오/남용시 위험성

[문 10] 정부, 기업에서 개인정보처리가 오/남용 되었을 경우 얼마나 위험하다고 생각하십니까?

(단위:%)

		사례수 (명)	매우 가 능성 높 다	가능성 높다	TOP 2	보통이 다	가능성 없다	전혀 가 능성 없 다	Bo ttom 2	M ean (점)
■ 전체		(1000)	44.2	45.2	89.4	9.7	0.8	0.1	0.9	(4.33)
성별	남성	(509)	46.2	42.8	89.0	10.0	0.8	0.2	1.0	(4.34)
	여성	(491)	42.2	47.7	89.8	9.4	0.8		0.8	(4.31)
연령	20대	(242)	47.9	37.2	85.1	14.0	0.4	0.4	0.8	(4.32)
	30대	(285)	45.6	47.7	93.3	6.7				(4.39)
	40대	(281)	44.5	44.8	89.3	9.6	1.1		1.1	(4.33)
	50대	(192)	37.0	52.1	89.1	8.9	2.1		2.1	(4.24)
직업	화이트	(434)	47.7	42.4	90.1	8.5	1.2	0.2	1.4	(4.36)
	블루	(189)	46.6	45.5	92.1	7.9				(4.39)
	주부	(200)	37.0	53.0	90.0	9.0	1.0		1.0	(4.26)
	학생	(120)	42.5	41.7	84.2	15.8				(4.27)
소득 수준	상	(187)	46.0	43.9	89.8	9.1	1.1		1.1	(4.35)
	중	(640)	44.8	44.5	89.4	9.8	0.8		0.8	(4.33)
	하	(173)	39.9	49.1	89.0	9.8	0.6	0.6	1.2	(4.27)
지역	서울	(221)	43.4	45.7	89.1	10.9				(4.33)
	경기	(285)	44.6	43.9	88.4	10.2	1.4		1.4	(4.32)
	강원	(29)	37.9	44.8	82.8	13.8	3.4		3.4	(4.17)
	충청	(98)	54.1	36.7	90.8	8.2		1.0	1.0	(4.43)
	전라	(99)	42.4	47.5	89.9	9.1	1.0		1.0	(4.31)
	경상	(268)	42.2	48.5	90.7	8.6	0.7		0.7	(4.32)
학력	고졸이하	(252)	40.5	47.6	88.1	10.3	1.6		1.6	(4.27)
	대졸	(634)	46.2	44.0	90.2	9.3	0.3	0.2	0.5	(4.36)
	대학원졸 이상	(114)	41.2	46.5	87.7	10.5	1.8		1.8	(4.27)

[표 19] 기업의 개인정보 처리 관련 오/남용시 위험성

[문 10] 정부, 기업에서 개인정보처리가 오/남용 되었을 경우 얼마나 위험하다고 생각하십니까?

(단위:%)

		사례수 (명)	매우 가 능성 높 다	가능성 높다	TOP 2	보통이 다	가능성 없다	전혀 가 능성 없 다	Bottom 2	Mean (점)
■ 전체		(1000)	61.6	35.9	97.5	2.2	0.2	0.1	0.3	(4.59)
성별	남성	(509)	64.8	33.2	98.0	1.6	0.2	0.2	0.4	(4.62)
	여성	(491)	58.2	38.7	96.9	2.9	0.2		0.2	(4.55)
연령	20대	(242)	69.8	26.4	96.3	3.3		0.4	0.4	(4.65)
	30대	(285)	60.7	37.5	98.2	1.4	0.4		0.4	(4.59)
	40대	(281)	58.0	40.2	98.2	1.8				(4.56)
	50대	(192)	57.8	39.1	96.9	2.6	0.5		0.5	(4.54)
직업	화이트	(434)	66.1	31.8	97.9	1.8		0.2	0.2	(4.64)
	블루	(189)	56.1	41.3	97.4	2.1	0.5		0.5	(4.53)
	주부	(200)	52.5	44.5	97.0	2.5	0.5		0.5	(4.49)
	학생	(120)	68.3	29.2	97.5	2.5				(4.66)
소득 수준	상	(187)	65.8	31.0	96.8	2.7	0.5		0.5	(4.62)
	중	(640)	62.7	35.2	97.8	2.0	0.2		0.2	(4.6)
	하	(173)	53.2	43.9	97.1	2.3		0.6	0.6	(4.49)
지역	서울	(221)	64.3	33.0	97.3	2.3	0.5		0.5	(4.61)
	경기	(285)	57.9	40.0	97.9	1.8	0.4		0.4	(4.55)
	강원	(29)	65.5	34.5	100.0					(4.66)
	충청	(98)	72.4	24.5	96.9	2.0		1.0	1.0	(4.67)
	전라	(99)	58.6	38.4	97.0	3.0				(4.56)
	경상	(268)	60.1	37.3	97.4	2.6				(4.57)
학력	고졸이하	(252)	56.7	40.1	96.8	2.4	0.8		0.8	(4.53)
	대졸	(634)	62.6	34.9	97.5	2.4		0.2	0.2	(4.6)
	대학원졸 이상	(114)	66.7	32.5	99.1	0.9				(4.66)

부 록

[표 20] 개인정보 수집 관련 프라이버시 침해 등 문제 발생의 동의 정도

[문 11] 정부나 기업 등 개인정보처리자가 자신의 업무를 수행하는 과정에서 타인의 개인정보를 수집하게 됩니다. 다음의 수집행위가 본인의 동의 없이 이루어진다면 프라이버시침해 등의 문제가 발생한다고 생각하십니까?

(Base : 1,000명, 단위:%)

	매우 가능성 높다	가능성 높다	TOP 2	보통이다	가능성 없다	전혀 가능성 없다	Bottom 2	Mean (점)
광고기획사가 연예인에 관하여 시중에 떠도는 스캔들소문을 수집하는 행위	40.5	40.6	81.1	14.6	3.8	0.5	4.3	(4.17)
기업이 입사원서를 낸 사람들의 평판, 업무능력에 대한 주위사람들의 평가 등의 정보를 수집하는 행위	40.2	41.3	81.5	14.2	3.8	0.5	4.3	(4.17)
은행이 대출신청자의 신용도를 평가하는데 필요한 개인정보를 수집하는 행위	42.4	34.7	77.1	16.2	6.0	0.7	6.7	(4.12)
인터넷쇼핑몰이 이용자의 소비취향에 관한 정보를 수집하는 행위	41.4	33.8	75.2	18.4	5.9	0.5	6.4	(4.1)
무료만화를 제공하는 인터넷사이트가 이용자의 만화취향이나 읽는 습관을 알아보기 위하여 관련 정보를 수집하는 행위	32.3	33.5	65.8	25.5	7.5	1.2	8.7	(3.88)
(홈페이지에 수집을 금한다는 경고문이 없을 경우)공개된 나의 홈페이지에 게시된 나의 개인 정보를 수집하는 행위	43.9	39.1	83.0	14.0	2.6	0.4	3.0	(4.24)
(홈페이지에 수집을 금한다는 경고문이 있는 경우)공개된 나의 홈페이지에 게시된 나의 개인 정보를 수집하는 행위	52.3	36.1	88.4	10.2	1.1	0.3	1.4	(4.39)

[표 21] CCTV 설치 관련 프라이버시 침해 등 문제 발생의 동의 정도

[문 12] CCTV의 설치와 관련하여 아래의 행위는 프라이버시침해 등의 문제가 발생한다고 생각하십니까? (이 CCTV는 범죄가 발생할 경우 문제의 상황이나 장면을 다시 볼 수 있도록 하는 기능만 있음)

(Base: 1,000명, 단위: %)

	매우 가능성 높다	가능성 높다	TOP 2	보통이다	가능성 없다	전혀 가능성 없다	Bottom 2	Mean (점)
아파트의 안전을 목적으로 지하 주차장에 CCTV를 설치하여 오가는 사람들의 모습을 단순 녹화하는 행위	62	150	212	302	387	99	486	(2.69)
아파트관리원이 입구에 설치된 CCTV를 활용하여 302호에 사는 A씨의 출퇴근시간을 계속적으로 기록하는 행위	404	414	818	114	59	09	68	(4.15)
대중목욕탕에서 도난사고가 찾아탈의실에 CCTV를 설치하여 사람들의 모습을 단순 녹화하는 행위	415	354	769	152	62	17	79	(4.09)

[표 22] 수집된 개인정보의 소유권자

[문 13] 다른 사람(기업 또는 정부 포함)이 자신의 비용으로 수집·이용하고 있는 나에 관한 개인정보는 누구의 것이라고 생각하십니까?

(단위:%)

		사례수(명)	비용 처리하고 있는 사람의 것	나의 개인정보는 나의 인격적 지표로서 나의 것	그 누구의 것도 아님	계
■ 전체		(1000)	6.4	88.6	5.0	100.0
성별	남성	(509)	7.9	87.4	4.7	100.0
	여성	(491)	4.9	89.8	5.3	100.0
연령	20대	(242)	7.4	88.0	4.5	100.0
	30대	(285)	4.9	90.9	4.2	100.0
	40대	(281)	6.8	86.1	7.1	100.0
	50대	(192)	6.8	89.6	3.6	100.0
직업	화이트	(434)	7.6	88.2	4.1	100.0
	블루	(189)	3.7	89.9	6.3	100.0
	주부	(200)	5.0	89.5	5.5	100.0
	학생	(120)	8.3	88.3	3.3	100.0
소득 수준	상	(187)	7.5	85.6	7.0	100.0
	중	(640)	6.4	88.8	4.8	100.0
	하	(173)	5.2	91.3	3.5	100.0
지역	서울	(221)	7.7	86.4	5.9	100.0
	경기	(285)	4.6	90.2	5.3	100.0
	강원	(29)	6.9	93.1		100.0
	충청	(98)	12.2	83.7	4.1	100.0
	전라	(99)	5.1	91.9	3.0	100.0
	경상	(268)	5.6	88.8	5.6	100.0
학력	고졸이하	(252)	5.2	90.1	4.8	100.0
	대졸	(634)	7.3	87.7	5.0	100.0
	대학원졸 이상	(114)	4.4	90.4	5.3	100.0

[표 23] 기업이 수집한 고객정보 이용에 대한 태도

[문 14] 기업이 거래과정에서 고객으로부터 받은 연락정보(주소, 전화번호, 이메일주소)를 이용하여 자사의 다른 상품이나 서비스를 광고하는 것은 허용될 수 있다고 생각하십니까?

(단위: %)

		사 례 수 (명)	절 대 허 용 되어 서 는 안 된 다	고 객 의 사 전 동 의 가 있 으면 허 용 된 다	사 후 고 객 거 부 시 이용 않 는 다 는 전 제 하에 허 용	동 의 나 다 른 조 건 없 이 자 유 롭 게 허 용 된 다	계
■ 전 체		(1000)	34.9	54.3	10.5	0.3	100.0
성 별	남 성	(509)	35.8	54.2	9.8	0.2	100.0
	여 성	(491)	34.0	54.4	11.2	0.4	100.0
연 령	20대	(242)	37.2	55.0	7.9		100.0
	30대	(285)	35.8	50.2	13.7	0.4	100.0
	40대	(281)	36.7	53.0	10.3		100.0
	50대	(192)	28.1	61.5	9.4	1.0	100.0
직 업	화 이 트	(434)	34.3	54.6	11.1		100.0
	블 루	(189)	38.6	50.3	10.1	1.1	100.0
	주 부	(200)	31.5	59.0	9.0	0.5	100.0
	학 생	(120)	35.0	54.2	10.8		100.0
소 득 수 준	상	(187)	36.4	57.8	5.9		100.0
	중	(640)	34.4	54.4	10.8	0.5	100.0
	하	(173)	35.3	50.3	14.5		100.0
지 역	서 울	(221)	36.7	51.6	11.3	0.5	100.0
	경 기	(285)	36.1	52.6	11.2		100.0
	강 원	(29)	41.4	51.7	6.9		100.0
	충 청	(98)	35.7	54.1	9.2	1.0	100.0
	전 라	(99)	33.3	56.6	10.1		100.0
	경 상	(268)	31.7	57.8	10.1	0.4	100.0
학 력	고 졸 이 하	(252)	35.3	51.6	12.3	0.8	100.0
	대 졸	(634)	35.2	55.0	9.6	0.2	100.0
	대 학 원 졸 이 상	(114)	32.5	56.1	11.4		100.0

[표 24] 기업의 개인별 프로파일 이용에 대한 태도

[문 15] 기업이 소비자에게 맞춤형서비스를 제공하기 위하여 소비자의 생활방식, 취미, 소비성향 등을 조사·분석하여 개인별 프로파일(카드사용내역을 조사하여 생활방식)을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

(단위 : %)

		사례수(명)	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부 시 이용 않는다는 전체 하에 허용	계
■ 전체		(1000)	25.8	62.6	11.6	100.0
성별	남성	(509)	28.7	59.7	11.6	100.0
	여성	(491)	22.8	65.6	11.6	100.0
연령	20대	(242)	25.2	64.0	10.7	100.0
	30대	(285)	25.3	62.8	11.9	100.0
	40대	(281)	26.7	61.2	12.1	100.0
	50대	(192)	26.0	62.5	11.5	100.0
직업	화이트	(434)	26.5	61.8	11.8	100.0
	블루	(189)	31.2	57.1	11.6	100.0
	주부	(200)	19.5	69.5	11.0	100.0
	학생	(120)	25.0	62.5	12.5	100.0
소득 수준	상	(187)	25.1	62.0	12.8	100.0
	중	(640)	25.0	64.4	10.6	100.0
	하	(173)	29.5	56.6	13.9	100.0
지역	서울	(221)	23.1	65.2	11.8	100.0
	경기	(285)	26.0	62.8	11.2	100.0
	강원	(29)	31.0	62.1	6.9	100.0
	충청	(98)	31.6	56.1	12.2	100.0
	전라	(99)	28.3	59.6	12.1	100.0
	경상	(268)	24.3	63.8	11.9	100.0
학력	고졸이하	(252)	28.6	59.9	11.5	100.0
	대졸	(634)	24.9	64.0	11.0	100.0
	대학원졸 이상	(114)	24.6	60.5	14.9	100.0

[표 25] 대통령의 개인별 프로파일 이용에 대한 태도

[문 16] 대통령이 정부의 중요 정책에 적합한 인물을 임명하기 위하여 사회지도층에 해당하는 사람들의 인물정보를 수집하여 개인별 프로파일을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

(단위 : %)

		사례 수 (명)	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부 시 이용 않는다는 전제하에 허용	꼭 필요한 범위 내에서 동의/조건 없이 허용	공익상의 목적으로 자유롭게 허용	계
■ 전체		(1000)	15.8	52.1	15.9	12.0	4.2	100.0
성별	남성	(509)	18.5	49.7	15.7	12.6	3.5	100.0
	여성	(491)	13.0	54.6	16.1	11.4	4.9	100.0
연령	20대	(242)	20.2	54.1	12.8	8.7	4.1	100.0
	30대	(285)	14.0	56.1	15.1	10.9	3.9	100.0
	40대	(281)	14.9	49.8	18.1	12.8	4.3	100.0
	50대	(192)	14.1	46.9	17.7	16.7	4.7	100.0
직업	화이트	(434)	13.6	55.3	15.4	12.0	3.7	100.0
	블루	(189)	24.3	45.0	13.8	11.1	5.8	100.0
	주부	(200)	10.0	54.5	19.5	10.5	5.5	100.0
	학생	(120)	20.0	51.7	14.2	11.7	2.5	100.0
소득 수준	상	(187)	12.8	48.7	19.3	11.8	7.5	100.0
	중	(640)	15.5	55.6	14.5	11.6	2.8	100.0
	하	(173)	20.2	42.8	17.3	13.9	5.8	100.0
지역	서울	(221)	11.8	53.4	18.6	11.3	5.0	100.0
	경기	(285)	15.8	50.5	14.4	14.0	5.3	100.0
	강원	(29)	20.7	41.4	20.7	13.8	3.4	100.0
	충청	(98)	20.4	53.1	13.3	10.2	3.1	100.0
	전라	(99)	15.2	57.6	9.1	13.1	5.1	100.0
	경상	(268)	17.2	51.5	18.3	10.4	2.6	100.0
학력	고졸이하	(252)	18.7	48.8	17.1	11.5	4.0	100.0
	대졸	(634)	15.5	54.4	14.4	11.5	4.3	100.0
	대학원졸 이상	(114)	11.4	46.5	21.9	15.8	4.4	100.0

[표 26] 기업이 수집한 나의 연락 정보 판매에 대한 태도

[문 17] 기업이 수집한 나의 연락정보(이름, 주소, 전화번호, 이메일 주소에 한함)를 제3자에게 돈을 받고 판매하는 것은 허용되어야 한다고 생각하십니까?

(단위 : %)

		사례 수 (명)	절대 허용 안 됨	사전 동의 의 있으면 허용	사후 거부 시 이 용 않는다는 전 제하에 허용	나에게 수 익/혜택 제공 되면 허용	동의/조 건 없이 허용	계
■ 전체		(1000)	82.7	12.1	3.8	1.2	0.2	100.0
성별	남성	(509)	80.9	13.6	3.5	1.6	0.4	100.0
	여성	(491)	84.5	10.6	4.1	0.8		100.0
연령	20대	(242)	76.9	16.9	4.5	1.7		100.0
	30대	(285)	83.2	9.1	5.3	1.8	0.7	100.0
	40대	(281)	84.0	12.5	2.8	0.7		100.0
	50대	(192)	87.5	9.9	2.1	0.5		100.0
직업	화이트	(434)	82.7	13.6	3.2	0.5		100.0
	블루	(189)	82.5	9.0	4.8	3.2	0.5	100.0
	주부	(200)	85.0	10.5	3.5	1.0		100.0
	학생	(120)	77.5	15.8	5.0	1.7		100.0
소득 수준	상	(187)	85.6	10.2	3.2	1.1		100.0
	중	(640)	80.9	13.8	4.4	0.9		100.0
	하	(173)	86.1	8.1	2.3	2.3	1.2	100.0
지역	서울	(221)	76.5	16.3	5.0	2.3		100.0
	경기	(285)	87.4	10.2	1.8	0.4	0.4	100.0
	강원	(29)	93.1	6.9				100.0
	충청	(98)	87.8	8.2	3.1	1.0		100.0
	전라	(99)	78.8	15.2	4.0	2.0		100.0
	경상	(268)	81.3	11.6	5.6	1.1	0.4	100.0
학력	고졸 이하	(252)	85.7	10.7	2.8	0.8		100.0
	대졸	(634)	82.0	12.5	3.8	1.4	0.3	100.0
	대학원졸 이상	(114)	79.8	13.2	6.1	0.9		100.0

[표 27] (기업→기업) 개인별 프로파일 판매에 대한 태도

[문 18] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 만든 (연락 정보를 제외한) 개인별 프로파일을 다른 기업에게 판매하는 것이 허용되어야 한다고 생각하십니까?

(단위 : %)

		사례수 (명)	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부 시 이 용 않는 다는 전 제하에 허용	소비 자에 게 수익 / 혜택 제 공 되면 허용	동의/조 건 없이 허용	계
■ 전체		(1000)	76.7	16.9	4.2	2.1	0.1	100.0
성별	남성	(509)	76.2	17.3	4.3	2.2		100.0
	여성	(491)	77.2	16.5	4.1	2.0	0.2	100.0
연령	20대	(242)	73.1	19.8	4.1	2.9		100.0
	30대	(285)	76.1	14.7	6.7	2.5		100.0
	40대	(281)	78.6	17.1	3.2	1.1		100.0
	50대	(192)	79.2	16.1	2.1	2.1	0.5	100.0
직업	화이트	(434)	80.4	14.5	3.9	1.2		100.0
	블루	(189)	74.1	16.4	4.2	4.8	0.5	100.0
	주부	(200)	74.5	19.0	5.0	1.5		100.0
	학생	(120)	69.2	24.2	3.3	3.3		100.0
소득 수준	상	(187)	78.6	15.5	4.8	1.1		100.0
	중	(640)	75.0	18.3	4.7	1.9	0.2	100.0
	하	(173)	80.9	13.3	1.7	4.0		100.0
지역	서울	(221)	69.2	22.2	4.1	4.5		100.0
	경기	(285)	79.3	16.5	2.8	1.4		100.0
	강원	(29)	86.2	10.3	3.4			100.0
	충청	(98)	82.7	10.2	4.1	2.0	1.0	100.0
	전라	(99)	73.7	21.2	4.0	1.0		100.0
	경상	(268)	78.0	14.6	6.0	1.5		100.0
학력	고졸이하	(252)	78.6	16.3	4.0	0.8	0.4	100.0
	대졸	(634)	76.3	17.2	3.9	2.5		100.0
	대학원졸 이상	(114)	74.6	16.7	6.1	2.6		100.0

[표 28] (기업→수사기관) 개인별 프로파일 제공에 대한 태도(영장 없이)

[문 19] 기업이 보유하고 있는 소비자의 개인정보를 수사기관의 요청에 따라 법관이 발부한 영장 없이 제공하는 것에 대하여 어떻게 생각합니까?

(단위 : %)

		사례수 (명)	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부 시 이용 않는다는 전제하에 허용	법률에 따른 것이면 허용	공익 목적이므로 자유롭게 허용	계
■ 전체		(1000)	49.3	30.9	7.4	11.9	0.5	100.0
성별	남성	(509)	50.1	32.2	7.1	10.2	0.4	100.0
	여성	(491)	48.5	29.5	7.7	13.6	0.6	100.0
연령	20대	(242)	51.2	31.0	6.2	11.2	0.4	100.0
	30대	(285)	45.3	28.1	10.2	15.4	1.1	100.0
	40대	(281)	49.8	32.0	6.4	11.4	0.4	100.0
	50대	(192)	52.1	33.3	6.3	8.3		100.0
직업	화이트	(434)	48.8	30.9	8.5	11.8		100.0
	블루	(189)	50.8	30.7	6.9	10.6	1.1	100.0
	주부	(200)	44.5	34.5	7.0	13.5	0.5	100.0
	학생	(120)	53.3	27.5	5.8	12.5	0.8	100.0
소득 수준	상	(187)	46.5	29.4	9.6	13.9	0.5	100.0
	중	(640)	48.8	32.8	7.7	10.3	0.5	100.0
	하	(173)	54.3	25.4	4.0	15.6	0.6	100.0
지역	서울	(221)	44.8	33.5	7.2	14.5		100.0
	경기	(285)	46.7	31.9	7.0	13.7	0.7	100.0
	강원	(29)	62.1	17.2	3.4	13.8	3.4	100.0
	충청	(98)	54.1	28.6	7.1	9.2	1.0	100.0
	전라	(99)	48.5	32.3	7.1	12.1		100.0
	경상	(268)	53.0	29.5	8.6	8.6	0.4	100.0
학력	고졸 이하	(252)	46.8	34.5	7.1	10.7	0.8	100.0
	대졸	(634)	49.7	30.3	7.4	12.1	0.5	100.0
	대학원졸 이상	(114)	52.6	26.3	7.9	13.2		100.0

[표 29] (정부→정부) 개인정보 제공에 대한 태도

[문 20] 정부의 각 기관들은 자신의 소관업무의 수행을 위하여 관련 국민의 개인정보를 수집하여 각각 개인정보DB를 구축하고 이를 관리·이용하고 있습니다. 자신의 소관업무 수행목적 이외에 국민의 개인정보를 다른 기관에게 제공하는 것은 허용되어야 한다고 생각하십니까?

(단위 : %)

		사례수 (명)	절대 허용 안 됨	사전 동의 의 있으면 허용	사후 거 부 시 이 용 않는 다는 전 제하에 허용	법률에 따른 것 이면 허 용	다른 기 관의 목 적이 정 당한 업 무수행이 면 허용	계
■ 전체		(1000)	53.7	33.4	7.4	4.3	1.2	100.0
성별	남성	(509)	50.9	36.3	6.7	4.9	1.2	100.0
	여성	(491)	56.6	30.3	8.1	3.7	1.2	100.0
연령	20대	(242)	50.4	37.6	7.9	2.9	1.2	100.0
	30대	(285)	54.0	30.2	8.1	5.6	2.1	100.0
	40대	(281)	54.1	34.9	6.0	3.9	1.1	100.0
	50대	(192)	56.8	30.7	7.8	4.7		100.0
직업	화이트	(434)	52.1	34.1	8.5	4.6	0.7	100.0
	블루	(189)	53.4	33.9	6.3	3.2	3.2	100.0
	주부	(200)	60.0	26.5	7.5	5.5	0.5	100.0
	학생	(120)	53.3	34.2	6.7	4.2	1.7	100.0
소득 수준	상	(187)	55.6	30.5	7.5	5.3	1.1	100.0
	중	(640)	52.8	35.2	7.3	3.8	0.9	100.0
	하	(173)	54.9	30.1	7.5	5.2	2.3	100.0
지역	서울	(221)	49.8	37.6	7.7	3.6	1.4	100.0
	경기	(285)	53.0	35.4	4.6	4.9	2.1	100.0
	강원	(29)	62.1	31.0	3.4	3.4		100.0
	충청	(98)	55.1	31.6	8.2	5.1		100.0
	전라	(99)	56.6	27.3	11.1	5.1		100.0
	경상	(268)	55.2	31.0	9.0	3.7	1.1	100.0
학력	고졸 이하	(252)	61.1	29.4	6.7	2.4	0.4	100.0
	대졸	(634)	50.8	35.2	7.7	4.7	1.6	100.0
	대학원졸 이상	(114)	53.5	32.5	7.0	6.1	0.9	100.0

[표 30] (정부→수사기관) 개인정보 제공에 대한 태도

[문 21] 앞의 질문에서 제공받는 기관이 수사기관이라고 한다면 그 정보제공에 대하여 어떻게 생각합니까?

(단위:%)

		사례수 (명)	절대 허용 안 됨	사전 동의 있으면 허용	사후 거부 시 이용 않는다는 전제하에 허용	법률에 따른 것이면 허용	공익 목적적이므로 자유롭게 허용	계
■ 전체		(1000)	15.8	50.7	12.0	20.5	1.0	100.0
성별	남성	(509)	20.4	48.7	10.0	19.4	1.4	100.0
	여성	(491)	11.0	52.7	14.1	21.6	0.6	100.0
연령	20대	(242)	16.5	53.3	9.1	19.8	1.2	100.0
	30대	(285)	12.6	47.7	14.7	24.6	0.4	100.0
	40대	(281)	16.4	53.0	11.4	18.5	0.7	100.0
	50대	(192)	18.8	48.4	12.5	18.2	2.1	100.0
직업	화이트	(434)	16.4	49.3	11.1	22.8	0.5	100.0
	블루	(189)	16.4	53.4	12.2	17.5	0.5	100.0
	주부	(200)	11.5	52.5	16.0	19.0	1.0	100.0
	학생	(120)	19.2	49.2	8.3	20.8	2.5	100.0
소득 수준	상	(187)	17.6	45.5	12.8	23.5	0.5	100.0
	중	(640)	15.3	51.4	12.8	19.4	1.1	100.0
	하	(173)	15.6	53.8	8.1	21.4	1.2	100.0
지역	서울	(221)	13.1	49.8	16.3	20.4	0.5	100.0
	경기	(285)	13.7	51.2	9.5	24.6	1.1	100.0
	강원	(29)	27.6	51.7	13.8	6.9		100.0
	충청	(98)	21.4	40.8	13.3	24.5		100.0
	전라	(99)	14.1	54.5	11.1	17.2	3.0	100.0
	경상	(268)	17.5	53.0	10.8	17.5	1.1	100.0
학력	고졸이하	(252)	15.9	51.6	13.5	18.7	0.4	100.0
	대졸	(634)	15.6	51.4	10.9	20.8	1.3	100.0
	대학원졸 이상	(114)	16.7	44.7	14.9	22.8	0.9	100.0

[표 31] (정부→정부) 개인정보 공유에 대한 태도

[문 22] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 각 정부기관들이 자신의 소관업무의 수행을 위하여 공유하는 것에 대하여 어떻게 생각하십니까? (민원업무의 처리가 빠르고 행정기관에 필요한 서류를 제출하지 않아도 되는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

(단위:%)

		사례수 (명)	매우 바람직하다	바람직하다	TOP 2	그저 그렇다	바람직하지 않다	전혀 바람직하지 않다	Bottom 2	Mean (점)
■ 전체		(1000)	0.1	6.9	7.0	30.7	45.4	16.9	62.3	(2.28)
성별	남성	(509)	0.2	8.1	8.3	27.7	43.4	20.6	64.0	(2.24)
	여성	(491)		5.7	5.7	33.8	47.5	13.0	60.5	(2.32)
연령	20대	(242)		5.0	5.0	30.6	42.1	22.3	64.5	(2.18)
	30대	(285)	0.4	5.3	5.6	36.1	45.3	13.0	58.2	(2.35)
	40대	(281)		6.8	6.8	25.6	48.0	19.6	67.6	(2.2)
	50대	(192)		12.0	12.0	30.2	45.8	12.0	57.8	(2.42)
직업	화이트	(434)	0.2	8.3	8.5	25.8	47.9	17.7	65.7	(2.25)
	블루	(189)		6.3	6.3	31.2	41.8	20.6	62.4	(2.23)
	주부	(200)		4.5	4.5	40.0	43.5	12.0	55.5	(2.37)
	학생	(120)		5.0	5.0	32.5	45.8	16.7	62.5	(2.26)
소득 수준	상	(187)		11.2	11.2	27.8	42.8	18.2	61.0	(2.32)
	중	(640)	0.2	5.8	5.9	30.5	46.9	16.7	63.6	(2.26)
	하	(173)		6.4	6.4	34.7	42.8	16.2	59.0	(2.31)
지역	서울	(221)		5.0	5.0	28.1	50.2	16.7	67.0	(2.21)
	경기	(285)		8.8	8.8	35.4	42.5	13.3	55.8	(2.4)
	강원	(29)		6.9	6.9	17.2	44.8	31.0	75.9	(2.)
	충청	(98)		4.1	4.1	33.7	33.7	28.6	62.2	(2.13)
	전라	(99)	1.0	7.1	8.1	29.3	42.4	20.2	62.6	(2.26)
	경상	(268)		7.5	7.5	28.7	50.0	13.8	63.8	(2.3)
학력	고졸이하	(252)		7.1	7.1	32.1	44.4	16.3	60.7	(2.3)
	대졸	(634)	0.2	6.3	6.5	29.7	46.8	17.0	63.9	(2.26)
	대학원졸 이상	(114)		9.6	9.6	33.3	39.5	17.5	57.0	(2.35)

[표 32] (정부→금융기관) 개인정보 공유에 대한 태도

[문 23] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 금융기관의 업무수행을 위하여 금융기관들과 공유하는 것이 필요하다고 생각하십니까? (금융기관 이용자는 금융기관에 제출하여야 하는 서류를 줄일 수 있고 금융기관은 이용자가 제출한 정보가 진실한 것인지를 확인할 수 있는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

(단위:%)

		사 례 수 (명)	반 드 시 필 요 하 다	필 요 하 다	T O P 2	그 저 그 렇 다	필 요 하 지 않 다	전 혀 필 요 하지 않 다	Bo ttom 2	M ean (점)
□ 전체		(1000)	0.6	10.1	10.7	26.8	40.8	21.7	62.5	(2.27)
성 별	남 성	(509)	0.6	10.6	11.2	23.4	39.5	25.9	65.4	(2.2)
	여 성	(491)	0.6	9.6	10.2	30.3	42.2	17.3	59.5	(2.34)
연 령	20대	(242)	0.8	7.4	8.3	28.9	38.8	24.0	62.8	(2.22)
	30대	(285)	0.4	7.0	7.4	30.9	41.8	20.0	61.8	(2.26)
	40대	(281)	0.7	12.1	12.8	23.5	40.6	23.1	63.7	(2.27)
	50대	(192)	0.5	15.1	15.6	22.9	42.2	19.3	61.5	(2.35)
직 업	화 이 트	(434)	0.2	8.8	9.0	26.3	40.3	24.4	64.7	(2.2)
	블 루	(189)	0.5	11.1	11.6	23.8	39.7	24.9	64.6	(2.23)
	주 부	(200)	0.5	12.0	12.5	30.5	44.0	13.0	57.0	(2.43)
	학 생	(120)	0.8	9.2	10.0	30.8	41.7	17.5	59.2	(2.34)
소 득 수 준	상	(187)		13.4	13.4	24.6	39.6	22.5	62.0	(2.29)
	중	(640)	0.5	10.0	10.5	27.0	41.7	20.8	62.5	(2.28)
	하	(173)	1.7	6.9	8.7	28.3	38.7	24.3	63.0	(2.23)
지 역	서 울	(221)		8.1	8.1	30.3	41.2	20.4	61.5	(2.26)
	경 기	(285)	0.7	9.8	10.5	31.2	41.1	17.2	58.2	(2.36)
	강 원	(29)		6.9	6.9	13.8	48.3	31.0	79.3	(1.97)
	충 청	(98)	1.0	5.1	6.1	24.5	43.9	25.5	69.4	(2.12)
	전 라	(99)	1.0	12.1	13.1	27.3	36.4	23.2	59.6	(2.31)
	경 상	(268)	0.7	13.4	14.2	21.3	39.9	24.6	64.6	(2.26)
학 력	고 졸 이 하	(252)	1.2	8.7	9.9	28.6	41.7	19.8	61.5	(2.3)
	대 졸	(634)	0.3	10.4	10.7	26.0	41.2	22.1	63.2	(2.26)
	대 학 원 생 이 상	(114)	0.9	11.4	12.3	27.2	36.8	23.7	60.5	(2.29)

3) 온라인상 개인정보 보호 관련 인식

[표 33] 정확한 신상정보 요구시 회원의 가입 태도

[문 24] 인터넷사이트 회원 가입시 정확한 신상정보(실명, 주민등록번호, 주소, 전화번호 등)의 입력을 요구하는 경우가 대부분입니다. 이 때 회원가입을 하십니까?

(단위 : %)

		사례수(명)	언제나 정확한 신상정보를 입력	가끔 틀린 신상정보를 입력	언제나 틀린 신상정보를 입력	계
■ 전체		(1000)	61.2	35.5	3.3	100.0
성별	남성	(509)	56.8	38.9	4.3	100.0
	여성	(491)	65.8	32.0	2.2	100.0
연령	20대	(242)	51.7	45.9	2.5	100.0
	30대	(285)	54.0	41.8	4.2	100.0
	40대	(281)	68.7	27.0	4.3	100.0
	50대	(192)	72.9	25.5	1.6	100.0
직업	화이트	(434)	57.1	39.6	3.2	100.0
	블루	(189)	64.6	30.2	5.3	100.0
	주부	(200)	71.5	27.0	1.5	100.0
	학생	(120)	50.0	47.5	2.5	100.0
소득 수준	상	(187)	61.0	35.3	3.7	100.0
	중	(640)	60.5	35.9	3.6	100.0
	하	(173)	64.2	34.1	1.7	100.0
지역	서울	(221)	55.7	40.7	3.6	100.0
	경기	(285)	62.1	35.1	2.8	100.0
	강원	(29)	72.4	17.2	10.3	100.0
	충청	(98)	66.3	33.7		100.0
	전라	(99)	57.6	39.4	3.0	100.0
	경상	(268)	63.1	32.8	4.1	100.0
학력	고졸이하	(252)	63.9	31.7	4.4	100.0
	대졸	(634)	60.4	36.3	3.3	100.0
	대학원졸 이상	(114)	59.6	39.5	0.9	100.0

[표 34] 인터넷사이트 회원 가입시 신상정보 기입 태도

[문 25] 실명확인을 하지 않는 인터넷사이트에 회원가입을 할 때 당신은 자신의 정확한 신상정보를 입력하십니까?

(단위:%)

		사례수(명)	언제나 정확한 신상정보를 입력	가끔 틀린 신상정보를 입력	언제나 틀린 신상정보를 입력	계
▣ 전체		(1000)	61.2	35.5	3.3	100.0
성별	남성	(509)	56.8	38.9	4.3	100.0
	여성	(491)	65.8	32.0	2.2	100.0
연령	20대	(242)	51.7	45.9	2.5	100.0
	30대	(285)	54.0	41.8	4.2	100.0
	40대	(281)	68.7	27.0	4.3	100.0
	50대	(192)	72.9	25.5	1.6	100.0
직업	화이트	(434)	57.1	39.6	3.2	100.0
	블루	(189)	64.6	30.2	5.3	100.0
	주부	(200)	71.5	27.0	1.5	100.0
	학생	(120)	50.0	47.5	2.5	100.0
소득 수준	상	(187)	61.0	35.3	3.7	100.0
	중	(640)	60.5	35.9	3.6	100.0
	하	(173)	64.2	34.1	1.7	100.0
지역	서울	(221)	55.7	40.7	3.6	100.0
	경기	(285)	62.1	35.1	2.8	100.0
	강원	(29)	72.4	17.2	10.3	100.0
	충청	(98)	66.3	33.7		100.0
	전라	(99)	57.6	39.4	3.0	100.0
	경상	(268)	63.1	32.8	4.1	100.0
학력	고졸이하	(252)	63.9	31.7	4.4	100.0
	대졸	(634)	60.4	36.3	3.3	100.0
	대학원졸 이상	(114)	59.6	39.5	0.9	100.0

[표 35] 인터넷게시판실명제의 필요도

[문 26] 인터넷게시판실명제에 대하여 어떻게 생각하십니까?

(단위:%)

		사례수 (명)	반드시 필요하 다	필요하 다	TOP 2	그저 그 렇다	필요하 지 않다	전혀 필 요하지 않다	Bo ttom 2	M ean (점)
▣ 전체		(1000)	217	44.4	66.1	16.6	11.5	5.8	17.3	(3.65)
성별	남성	(509)	25.0	39.5	64.4	14.7	12.4	8.4	20.8	(3.6)
	여성	(491)	18.3	49.5	67.8	18.5	10.6	3.1	13.6	(3.69)
연령	20대	(242)	17.8	44.2	62.0	21.1	12.4	4.5	16.9	(3.58)
	30대	(285)	21.8	44.6	66.3	16.5	11.6	5.6	17.2	(3.65)
	40대	(281)	24.2	43.4	67.6	15.3	9.6	7.5	17.1	(3.67)
	50대	(192)	22.9	45.8	68.8	13.0	13.0	5.2	18.2	(3.68)
직업	화이트	(434)	22.8	43.5	66.4	15.2	11.8	6.7	18.4	(3.64)
	블루	(189)	22.2	42.9	65.1	15.3	11.1	8.5	19.6	(3.59)
	주부	(200)	17.5	50.5	68.0	16.5	11.5	4.0	15.5	(3.66)
	학생	(120)	17.5	45.8	63.3	23.3	11.7	1.7	13.3	(3.66)
소득 수준	상	(187)	24.6	46.0	70.6	13.9	7.5	8.0	15.5	(3.72)
	중	(640)	22.0	44.7	66.7	16.4	11.7	5.2	16.9	(3.67)
	하	(173)	17.3	41.6	59.0	20.2	15.0	5.8	20.8	(3.5)
지역	서울	(221)	24.0	45.2	69.2	15.8	9.5	5.4	14.9	(3.73)
	경기	(285)	22.5	42.8	65.3	16.5	11.2	7.0	18.2	(3.62)
	강원	(29)	20.7	41.4	62.1	24.1	10.3	3.4	13.8	(3.66)
	충청	(98)	21.4	40.8	62.2	16.3	12.2	9.2	21.4	(3.53)
	전라	(99)	15.2	40.4	55.6	23.2	16.2	5.1	21.2	(3.44)
	경상	(268)	21.6	48.5	70.1	14.2	11.6	4.1	15.7	(3.72)
학력	고졸이하	(252)	19.4	43.7	63.1	18.3	13.5	5.2	18.7	(3.59)
	대졸	(634)	22.6	44.5	67.0	17.2	10.3	5.5	15.8	(3.68)
	대학원졸 이상	(114)	21.9	45.6	67.5	9.6	14.0	8.8	22.8	(3.58)

부 록

[표 36] 익명/가명으로 인터넷 이용할 수 있는 법적 환경에 대한 태도

[문 27] 인터넷에서 이용자의 신원이 쉽게 확인될 수 없도록 익명 또는 가명으로 인터넷을 이용할 수 있는 법적 환경 및 시스템이 갖추어진다면 이에 대해 어떻게 생각하십니까?

(단위:%)

		사례수 (명)	매우 바 람직하 다	바람직 하다	TO P 2	그저 그 렇다	바람직 하지 않 다	전혀 바 람직하 지 않다	Bo ttom 2	M ean (점)
■ 전체		(1000)	5.5	17.3	22.8	27.2	34.4	15.6	50.0	(26.3)
성별	남성	(509)	7.3	19.3	26.5	25.5	30.8	17.1	47.9	(26.9)
	여성	(491)	3.7	15.3	18.9	28.9	38.1	14.1	52.1	(25.6)
연령	20대	(242)	4.5	13.2	17.8	33.5	35.1	13.6	48.8	(2.6)
	30대	(285)	3.9	16.1	20.0	32.6	32.6	14.7	47.4	(26.2)
	40대	(281)	7.5	16.4	23.8	22.1	36.7	17.4	54.1	(2.6)
	50대	(192)	6.3	25.5	31.8	18.8	32.8	16.7	49.5	(27.2)
직업	화이트	(434)	4.8	18.2	23.0	27.2	33.4	16.4	49.8	(26.2)
	블루	(189)	9.5	16.9	26.5	23.3	32.8	17.5	50.3	(26.8)
	주부	(200)	3.0	16.5	19.5	29.0	37.0	14.5	51.5	(25.7)
	학생	(120)	3.3	15.8	19.2	30.0	37.5	13.3	50.8	(25.8)
소득 수준	상	(187)	5.9	20.3	26.2	18.2	39.0	16.6	55.6	(2.6)
	중	(640)	4.5	18.0	22.5	27.5	34.4	15.6	50.0	(26.1)
	하	(173)	8.7	11.6	20.2	35.8	29.5	14.5	43.9	(27.1)
지역	서울	(221)	5.9	15.4	21.3	20.8	43.0	14.9	57.9	(25.4)
	경기	(285)	6.3	15.4	21.8	33.0	32.6	12.6	45.3	(2.7)
	강원	(29)		24.1	24.1	20.7	37.9	17.2	55.2	(25.2)
	충청	(98)	3.1	15.3	18.4	29.6	29.6	22.4	52.0	(24.7)
	전라	(99)	5.1	29.3	34.3	28.3	26.3	11.1	37.4	(29.1)
	경상	(268)	6.0	16.4	22.4	25.7	33.6	18.3	51.9	(25.8)
학력	고졸이하	(252)	6.0	19.4	25.4	28.2	32.5	13.9	46.4	(27.1)
	대졸	(634)	5.0	16.2	21.3	26.8	35.6	16.2	51.9	(25.8)
	대학원졸 이상	(114)	7.0	18.4	25.4	27.2	31.6	15.8	47.4	(26.9)

[표 37] 신원확인 요구시 게시판에 글 올리는 태도

[문 28] 인터넷게시판실명제가 시행되고 있습니다. 공공기관 홈페이지와 포털 등의 게시판에 글을 쓰기 위해서는 반드시 신원을 확인하도록 요구하고 있습니다. 신원확인을 하더라도 게시판에 글을 올리십니까?

(단위 : %)

		사 례 수 (명)	별 다른 거 리낌 없이 정 확한 정 보 를 입력 하 고 , 글 을 올 린 다	마 지 못 해 입 력 하 고 대 부 분 글 을 올 린 다	대 부 분 글 을 올 리 지 않 는 다	절 대 글 을 올 리 지 않 는 다	계
■ 전 체		(1000)	33.4	29.3	34.0	3.3	100.0
성 별	남 성	(509)	36.0	34.2	26.7	3.1	100.0
	여 성	(491)	30.8	24.2	41.5	3.5	100.0
연 령	20 대	(242)	31.8	31.0	32.6	4.5	100.0
	30 대	(285)	30.9	29.5	37.2	2.5	100.0
	40 대	(281)	36.7	29.2	31.3	2.8	100.0
	50 대	(192)	34.4	27.1	34.9	3.6	100.0
직 업	화 이 트	(434)	34.1	31.3	31.6	3.0	100.0
	블 루	(189)	33.9	28.0	33.9	4.2	100.0
	주 부	(200)	31.0	23.0	42.5	3.5	100.0
	학 생	(120)	34.2	34.2	28.3	3.3	100.0
소 득 수 준	상	(187)	35.8	27.3	32.6	4.3	100.0
	중	(640)	33.3	29.7	33.6	3.4	100.0
	하	(173)	31.2	30.1	37.0	1.7	100.0
지 역	서 울	(221)	35.3	27.1	32.6	5.0	100.0
	경 기	(285)	33.0	31.6	31.9	3.5	100.0
	강 원	(29)	48.3	24.1	27.6		100.0
	충 청	(98)	32.7	33.7	33.7		100.0
	전 라	(99)	22.2	39.4	33.3	5.1	100.0
	경 상	(268)	35.1	23.9	38.4	2.6	100.0
학 력	고 졸 이 하	(252)	30.6	25.4	40.9	3.2	100.0
	대 졸	(634)	33.9	30.1	32.5	3.5	100.0
	대 학 원 졸 이 상	(114)	36.8	33.3	27.2	2.6	100.0

부록 Ⅱ. 전문가 설문조사지 및 설문조사결과표

Ⅱ-1. 전문가 설문조사지

◆ 다음은 개인정보보호법제의 현황에 대한 일반적 인식을 알아보기 위한 질문입니다.

[문 1] 그 동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

- ① 있다 → 1-1로
- ② 없다 → 2로

[문 1-1] 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

- ① 어려움이 있었다 → 1-2로
- ② 어려움이 별로 없었다 → 2로

[문 1-2] 어려움을 느낀 이유는 무엇이라고 생각하십니까?

- ① 개인정보보호법의 존재를 몰라서
- ② 개인정보보호에 관한 법률이 하나로 되어 있지 않아서
- ③ 분야별로 관련 법률이 잘 구분되어 있지 않아서
- ④ 새로운 문제에 대처할 수 있는 조항이 마련되어 있지 않아서
- ⑤ 기타()

[문 2] 다음 법률 가운데 개인정보의 보호를 위한 내용이 포함되어 있을 것으로 짐작되는 법률을 모두 선택하여 주십시오.

부 록

- ① 공공기관의 개인정보보호에 관한 법률
- ② 정보통신망 이용 촉진 및 정보보호 등에 관한 법률
- ③ 신용정보의 이용 및 보호에 관한 법률
- ④ 전자정부법
- ⑤ 금융실명거래 및 비밀보장에 관한 법률
- ⑥ 통신비밀보호법
- ⑦ 보건의료기본법
- ⑧ 주민등록법
- ⑨ 국세기본법
- ⑩ 특정범죄신고자 등 보호법
- ⑪ 형법
- ⑫ 위의 법률 어느 것에도 포함 되어 있지 않을 것 같음

[문 3] 우리나라의 현행 개인정보보호 관련 입법은 공공부문과 민간 부문으로 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[문 4] 공공부문의 개인정보보호에 적용되는 「공공기관의 개인정보 보호에 관한 법률」은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 ‘컴퓨터로 처리되는 것’만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

- ① 잘 알고 있다
- ② 막연히 짐작하고 있는 정도이다
- ③ 공공기관이 보유하는 개인정보는 모두 보호의 대상이 되는 줄 알았다

- ④ 컴퓨터로 처리되지 않는 개인정보도 보호를 받을 수 있는 줄 알았다
- ⑤ 모든 개인정보가 그 보호의 대상이 되는 줄 알았다
- ⑥ 전혀 몰랐다

[문 5] 민간부문의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며 개별 분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?

- ① 잘 알고 있다
- ② 그 동안 잘 몰랐다

[문 6] 현재 본인의 개인 정보(성명, 주소, 주민등록번호, 이메일 주소, 생체정보(지문, 홍채, 유전자 등), 병원 진료 기록, 전과기록, 금전적 거래 기록, 본인 은행계좌번호, 학력, 경력 등)가 제대로 보호되고 있다고 느끼십니까?

답란	전혀 그렇지 않다	그렇지 않다	보통이다	그렇다	매우 그렇다
	①	②	③	④	⑤
	→문 7로 갈 것		→문 8로 갈 것		

[문 7] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이 라고 생각하시는지 1순위부터 3순위까지 응답하여 주십시오.

1순위 _____ 2순위 _____ 3순위 _____

- ① 법률규정의 미비 내지는 복잡성
- ② 교육이나 홍보부족
- ③ 정부나 사업자의 인식부족
- ④ 일반인의 인식부족
- ⑤ 개인정보 활용의 필요성
- ⑥ 기타()

[문 8] 현재는 개인정보가 부분적으로 보호되고 있습니다 개인정보 보호를 보다 강화하기 위한 「개인정보보호법」의 제정이 필요하다고 생각하십니까?

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 보통이다
- ④ 시급하지는 않지만 필요하다
- ⑤ 시급히, 매우 필요하다

[문 9] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 위험하다고 생각하십니까?

- ① 위험하다 ② 위험하지 않다 ③ 잘 모르겠다

[문 10] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 불쾌하다고 생각하십니까?

- ① 불쾌하다 ② 불쾌하지 않다 ③ 잘 모르겠다

[문 11] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보 DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 위험하다고 생각하십니까?

- ① 위험하다 ② 위험하지 않다 ③ 잘 모르겠다

[문 12] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보 DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 불쾌하다고 생각하십니까?

- ① 불쾌하다 ② 불쾌하지 않다 ③ 잘 모르겠다

[문 13] 앞의 문6,7 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 **위험하다고** 생각하십니까?

- ① 위험하다 ② 위험하지 않다 ③ 잘 모르겠다

[문 13-1] 앞의 문항과 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 **불쾌하다고** 생각하십니까?

- ① 불쾌하다 ② 불쾌하지 않다 ③ 잘 모르겠다

[문 14] 정부, 기업 각각의 개인정보처리 관련해서 오/남용 가능성은 얼마나 된다고 생각하십니까?

	매우 가능성 높다	가능성 높다	보통 이다	가능성 없다	전혀 가능성 없다
정부의 개인정보처리 오/남용 가능성	⑤	④	③	②	①
기업의 개인정보처리 오/남용 가능성	⑤	④	③	②	①

[문 15] 정부, 기업에서 개인정보처리가 오/남용 되었을 경우 얼마나 위험하다고 생각하십니까?

	매우 위험 하다	위험 하다	보통 이다	위험 하지 않다	전혀 위험하지 않다
정부의 개인정보처리 오/남용 되는 경우 위험성	⑤	④	③	②	①
기업의 개인정보처리 오/남용 되는 경우 위험성	⑤	④	③	②	①

[문 16] 정부나 기업 등 개인정보처리자가 자신의 업무를 수행하는 과정에서 타인의 개인정보를 수집하게 됩니다. 다음의 수집행위가 본인의 동의 없이 이루어진다면 프라이버시침해 등의 문제가 발생한다고 생각하십니까?

행 위	매우 그렇다	그렇다	보통 이다	그렇지 않다	매우 그렇지 않다
① 광고기획사가 연예인에 관하여 시중에 떠도는 스캔들소문을 수집하는 행위	⑤	④	③	②	①
② 기업이 입사원서를 낸 사람들의 평판, 업무능력에 대한 주위사람들의 평가 등의 정보를 수집하는 행위	⑤	④	③	②	①
③ 은행이 대출신청자의 신용도를 평가하는데 필요한 개인정보를 수집하는 행위	⑤	④	③	②	①
④ 인터넷쇼핑몰이 이용자의 소비취향에 관한 정보를 수집하는 행위	⑤	④	③	②	①
⑤ 무료만화를 제공하는 인터넷사이트가 이용자의 만화취향이나 읽는 습관을 알아보기 위하여 관련 정보를 수집하는 행위	⑤	④	③	②	①
⑥ (홈페이지에 수집을 금한다는 경고문이 없을 경우)공개된 나의 홈페이지에 게시된 나의 관한 개인정보를 수집하는 행위	⑤	④	③	②	①
⑦ (홈페이지에 수집을 금한다는 경고문이 있는 경우)공개된 나의 홈페이지에 게시된 나의 관한 개인정보를 수집하는 행위	⑤	④	③	②	①

[문 17] CCTV의 설치와 관련하여 아래의 행위는 프라이버시침해 등의 문제가 발생한다고 생각하십니까? (이 CCTV는 범죄가 발생할 경우 문제의 상황이나 장면을 다시 볼 수 있도록 하는 기능만 있음)

행 위	매우 그렇다	그렇다	보통 이다	그렇지 않다	매우 그렇지 않다
① 아파트의 안전을 목적으로 지하주차장에 CCTV를 설치하여 오가는 사람들의 모습을 단순 녹화하는 행위	⑤	④	③	②	①
② 아파트관리원이 입구에 설치된 CCTV를 활용하여 302호에 사는 A씨의 출퇴근 시간을 계속적으로 기록하는 행위	⑤	④	③	②	①
③ 대중목욕탕에서 도난사고가 잦아 탈의실에 CCTV를 설치하여 사람들의 모습을 단순 녹화하는 행위	⑤	④	③	②	①

[문 18] 다른 사람(기업 또는 정부 포함)이 자신의 비용으로 수집·이용하고 있는 나에 관한 개인정보는 누구의 것이라고 생각하십니까?

- ① 자신의 비용으로 처리하고 있는 그 사람의 자산이다
- ② 나의 개인정보는 나의 인격적 징표로서 나의 것이다
- ③ 그 누구의 것도 아니다

[문 19] 기업이 거래과정에서 고객으로부터 받은 연락정보(주소, 전화번호, 이메일주소)를 이용하여 자사의 다른 상품이나 서비스를 광고하는 것은 허용될 수 있다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 고객의 사전 동의가 있으면 허용 된다
- ③ 사후에 고객이 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 이용하는 것은 허용될 수 있다
- ④ 동의나 다른 조건 없이 자유롭게 허용 된다

[문 20] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 소비자의 생활방식, 취미, 소비성향 등을 조사·분석하여 개인별 프로파일(카

드사용내역을 조사하여 생활방식)을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 고객의 사전 동의가 있으면 허용 된다
- ③ 사후에 고객이 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 이용하는 것은 허용될 수 있다
- ④ 동의나 다른 조건 없이 자유롭게 허용 된다

[문 21] 대통령이 정부의 중요 직책에 적합한 인물을 임명하기 위하여 사회지도층에 해당하는 사람들의 인물정보를 수집하여 개인별 프로필을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 해당자의 사전 동의가 있으면 허용 된다
- ③ 사후에 해당자가 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 이용하는 것은 허용될 수 있다
- ④ 꼭 필요한 범위 내에서는 동의나 다른 조건 없이 허용 된다
- ⑤ 공익상의 목적이므로 어떠한 정보를 수집하든 자유롭게 허용 된다

[문 22] 기업이 수집한 나의 연락정보(이름, 주소, 전화번호, 이메일 주소에 한함)를 제3자에게 돈을 받고 판매하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 나의 사전 동의가 있으면 허용 된다
- ③ 사후에 내가 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 판매하는 것은 허용될 수 있다 (판매에 관한 사실을 판매 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공 받은 제3자도 더 이상 이용하지 못한다는 조건이 함께 있음)

- ④ 나에게 수익의 일부나 혜택이 제공된다면 허용 된다
- ⑤ 동의나 다른 조건 없이 자유롭게 허용 된다

[문 23] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 만든 (연락 정보를 제외한) 개인별 프로파일을 다른 기업에게 판매하는 것이 허용되어야 한다고 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 소비자의 사전 동의가 있으면 허용 된다
- ③ 사후에 소비자가 거부를 하면 더 이상 이용하지 않는다는 조건으로 일단 판매하는 것은 허용될 수 있다 (판매에 관한 사실을 판매 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 제3자도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 소비자에게 수익의 일부나 혜택이 제공된다면 허용 된다
- ⑤ 동의나 다른 조건 없이 자유롭게 허용 된다

[문 24] 기업이 보유하고 있는 소비자의 개인정보를 수사기관의 요청에 따라 법관이 발부한 영장 없이 제공하는 것에 대하여 어떻게 생각하십니까?

- ① 절대 허용 되어서는 안 된다
- ② 개인의 사전 동의가 있으면 허용될 수 있다
- ③ 사후에 개인이 거부를 하면 더 이상 제공하지 않는다는 조건으로 일단 제공하는 것은 허용될 수 있다 (제공에 관한 사실을 제공 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 수사기관도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 수사기관에 개인정보를 제공하는 것이 법률에 따른 것이라면 허용 된다
- ⑤ 공익을 이유로 한 것이므로 자유롭게 허용 된다

[문 25] 정부의 각 기관들은 자신의 소관업무의 수행을 위하여 관련 국민의 개인정보를 수집하여 각각 개인정보DB를 구축하고 이를 관리·이용하고 있습니다. 자신의 소관업무 수행목적 이외에 국민의 개인정보를 다른 기관에게 제공하는 것은 허용되어야 한다고 생각하십니까?

- ① 절대 허용되어서는 안 된다
- ② 개인의 사전 동의가 있으면 허용될 수 있다
- ③ 사후에 개인이 거부를 하면 더 이상 제공하지 않는다는 조건으로 일단 제공하는 것은 허용될 수 있다. (제공에 관한 사실을 제공 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 다른 기관도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 그 제공이 법률에 따라 행해진 것이면 허용 된다
- ⑤ 다른 기관의 이용목적이 ‘정당한 업무수행’이라면 동의나 조건 없이 허용될 수 있다

[문 26] 앞의 문에서 제공받는 기관이 수사기관이라고 한다면 그 정보제공에 대하여 어떻게 생각하십니까?

- ① 절대 허용되어서는 안 된다
- ② 개인의 사전 동의가 있으면 허용될 수 있다
- ③ 사후에 개인이 거부를 하면 더 이상 제공하지 않는다는 조건으로 일단 제공하는 것은 허용될 수 있다 (제공에 관한 사실을 제공 직후에 알 수 있도록 알려 주며, 거부하는 경우 제공받은 수사기관도 더 이상 이용하지 못한다는 조건이 함께 있음)
- ④ 수사기관에 개인정보를 제공하는 것이 법률에 따른 것이면 허용 된다
- ⑤ 공익을 이유로 한 것이므로 자유롭게 허용 된다

[문 27] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 각 정부기관들이 자신의 소관업무의 수행을 위하여 공유하는 것에 대하여 어떻게 생각하십니까? (민원업무의 처리가 빠르고 행정기관에 필요한 서류를 제출하지 않아도 되는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

- ① 매우 바람직하지 않다
- ② 바람직하지 않다
- ③ 그저 그렇다
- ④ 바람직하다
- ⑤ 매우 바람직하다

[문 28] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 금융기관의 업무수행을 위하여 금융기관들과 공유하는 것이 필요하다고 생각하십니까? (금융기관 이용자는 금융기관에 제출하여야 하는 서류를 줄일 수 있고 금융기관은 이용자가 제출한 정보가 진실한 것인지를 확인할 수 있는 이점이 있는 반면, 개인정보의 오·남용이 있을 수도 있음)

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 그저 그렇다
- ④ 필요하다
- ⑤ 반드시 필요하다

[문 29] 인터넷사이트 회원 가입시 정확한 신상정보(실명, 주민등록번호, 주소, 전화번호 등)의 입력을 요구하는 경우가 대부분입니다. 이 때 회원가입을 하십니까?

- ① 별다른 거리낌 없이 정확한 신상정보를 입력하고 가입 한다
- ② 마지못해 입력하고 대부분 가입 한다
- ③ 신상정보를 요구하면 대부분 가입하지 않는다
- ④ 신상정보를 요구하면 절대 가입하지 않는다

[문 30] 실명확인을 하지 않는 인터넷사이트에 회원가입을 할 때 당신은 자신의 정확한 신상정보를 입력하십니까?

- ① 언제나 정확한 신상정보를 입력한다
- ② 가끔 틀린 신상정보를 입력한다
- ③ 언제나 틀린 신상정보를 입력한다

[문 31] 인터넷게시판실명제에 대하여 어떻게 생각하십니까?

- ① 전혀 필요하지 않다
- ② 필요하지 않다
- ③ 그저 그렇다
- ④ 필요하다
- ⑤ 매우 필요하다

[문 32] 인터넷에서 이용자의 신원이 쉽게 확인될 수 없도록 익명 또는 가명으로 인터넷을 이용할 수 있는 법적 환경 및 시스템이 갖추어진다면 이에 대해 어떻게 생각하십니까?

- ① 전혀 바람직하지 않다
- ② 바람직하지 않다
- ③ 그저 그렇다
- ④ 바람직하다
- ⑤ 매우 바람직하다

[문 33] 인터넷게시판실명제가 시행되고 있습니다. 공공기관 홈페이지와 포털 등의 게시판에 글을 쓰기 위해서는 반드시 신원을 확인하도록 요구하고 있습니다. 신원확인을 하더라도 게시판에 글을 올리십니까?

- ① 별다른 거리낌 없이 정확한 정보를 입력하고, 글을 올린다
- ② 마지못해 입력하고 대부분 글을 올린다
- ③ 대부분 글을 올리지 않는다
- ④ 절대 글을 올리지 않는다

◆ 다음은 개인정보보호법제의 입법체계에 대한 일반적인 인식을 알아보기 위한 질문입니다.

[문 1] 최근 우리나라에서 새로운 개인정보보호법을 제정하려는 움직임이 있는 것에 대해 알고 계십니까?

- ① 알고 있다
- ② 모르고 있다

[문 2] 개인정보보호를 위해 공공부문과 민간부문을 별도로 규율하고 있는 현행의 방식에서 탈피해서 양 부문을 모두 포괄할 수 있는 통합적 법률의 제정이 필요하다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

- ① 찬성한다 → 2-1로
- ② 반대한다 → 2-2로
- ③ 모르겠다 → 3으로

[문 2-1] 통합적 법률의 제정에 찬성하시는 이유는 다음 중 어느 것입니까? 순서대로 2가지를 선택하여 주십시오.

1순위: _____ 2순위: _____

- ① 양 부문을 굳이 달리 규율해야 할 이유가 없다
- ② 일반 국민들의 법적 혼란을 줄이기 위해 필요하다
- ③ 법적 보호의 공백을 최소화하기 위해 불가피하다
- ④ 양 부문에 걸쳐 법집행의 통일을 기할 필요가 있다
- ⑤ 기타 ()

➔ 응답 후 [3] 으로

[문 2-2] 통합적 법률의 제정에 반대하신다면 그 이유는 무엇입니까? 순서대로 2가지를 선택하여 주십시오.

1순위: _____ 2순위: _____

- ① 통합적 법률의 제정은 공공부문과 민간부문의 차이점을 무시하는 것이다
- ② 법적 보호의 공백은 각 부문별 법률의 제정이나 개정을 통해서도 해소할 수 있다
- ③ 분야별 개별법이 존재하는 이상 수범자의 법적 혼란은 불가피하다
- ④ 민간부문에 관한 특칙을 둘 경우 법제통합의 의미는 크지 않다
- ⑤ 기타 ()

[문 3] 통합적 법률을 제정할 경우 기본법의 체계(공공부문과 민간 부문에 관한 기본적인 사항만 정하고, 나머지는 특수한 분야별 개별 법률에 의해 규율하도록 하는 입법형식)와 일반법의 체계(공공 부문과 민간부문에 관한 일반적 사항을 모두 규정하도록 하고, 특수한 분야에 대해서는 별도의 특별법에 의해 규율하도록 하는 입법형식)를 고려할 수 있습니다. 이 가운데 어느 입법체계가 바람직하다고 생각하십니까?

- ① 기본법의 체계 → 3-1로
- ② 일반법의 체계 → 4로
- ③ 어느 것이든 무방하다 → 4로
- ④ 모르겠다 → 4로

[문 3-1] 기본법의 체계로 같 경우 기본법에서 규율해야 할 것으로 생각하시는 항목에 모두 체크해주시기 바랍니다.

- ① 개인정보보호의 기본이념
- ② 기본개념의 정의
- ③ 개인정보취급상의 기본원칙
- ④ 개인정보보호를 위한 국가의 책무와 시책
- ⑤ 권리행사의 방법과 절차
- ⑥ 개인정보보호기구
- ⑦ 피해의 구제와 제재
- ⑧ 기타

[문 4] 현행과 같이 공공부문과 민간부문 간에 분리된 입법의 방식을 취한다고 하더라도 민간부문에 대한 일반법을 별도로 제정할 필요가 있다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

- ① 찬성한다
- ② 반대한다
- ③ 모르겠다

※ 마지막으로 통계분류를 위해 몇 가지만 여쭙보겠습니다.

배문1. 성별	① 남자	② 여자
배문2. 직장		

부 록

배문3. 부서	
배문4. 근무 기간	년 개월
배문5. 직급	

Ⅱ-2. 전문가 설문조사결과표

<p>1. 조사방법: HRC 마스터 패널을 이용한 온라인 조사</p> <p>2. 조사대상: 전국 개인정보보호 관련 전문가</p> <p>3. 표본크기: 41명</p> <p>4. 표본구성</p>		
성 별	남	36
	여	5
근무기간	1년 미만	8
	1~5년 미만	20
	5~10년 미만	7
	10년 이상	6
근무직장	기업	13
	법학교수	16
	법실무	12
<p>5. 표본추출방법: 표본 할당 추출(Quota Sampling)</p> <p>6. 조사기간: 2008년 9월 9일 ~ 2008년 9월 18일</p>		

부 록

[표 1] 개인정보보호 관련 법조항 검색 여부

[문 1] 그동안 개인정보보호와 관련하여 궁금한 점이 있어서 관련 법조항을 찾아보신 적이 있습니까?

(단위:%)

		사례수(명)	경험 있음	경험 없음	계
전체		41	78.00	22.00	100.00
성별	남	36	80.56	19.44	100.00
	여	5	60.00	40.00	100.00
근무기간	1년미만	8	50.00	50.00	100.00
	1~5년미만	20	80.00	20.00	100.00
	5~10년미만	7	100.00	0.00	100.00
	10년이상	6	83.33	16.67	100.00
근무직장	기업	13	76.92	23.08	100.00
	법학교수	16	93.75	6.25	100.00
	법실무	12	58.33	41.67	100.00

[표 2] 개인정보보호의 법조항 검색시 어려움 있었는지 여부

[문 1-1] 개인정보보호를 위한 관련 법조항을 찾는 데 어려움은 없었습니까?

(단위:%)

		사례수(명)	어려움있었다	어려움이 별로 없었다	계
전체		32	71.88	28.13	100.00
성별	남	29	80.56	19.44	100.00
	여	3	60.00	40.00	100.00
근무기간	1년미만	4	100.00	0.00	100.00
	1~5년미만	16	68.75	31.25	100.00
	5~10년미만	7	71.43	28.57	100.00
	10년이상	5	60.00	40.00	100.00
근무직장	기업	10	60.00	40.00	100.00
	법학교수	15	66.67	33.33	100.00
	법실무	7	100.00	0.00	100.00

[표 3] 검색시 어려움을 느낀 이유

(단위:%)

		사례수 (명)	① 개인정보 보호법의 존 재를 몰라서	② 개인정보 보호에 관한 법률이 하나 로 되어 있지 않아서	③ 분야별 로 관련 법 률이 잘 구 분되어 있지 않아서	④ 새로운 문제에 대 처할 수 있는 조항 이 마련되 어 있지 않아서	⑤ 기타	계
전체		24		54.17	41.67	4.17		100.00
성별	남	22		59.09	36.36	4.55		100.00
	여	2		0.00	100.00	0.00		100.00
근무 기간	1년 미만	4		50.00	50.00	0.00		100.00
	1~5년 미만	12		58.33	33.33	8.33		100.00
	5~10년 미만	5		60.00	40.00	0.00		100.00
	10년 이상	3		33.33	66.67	0.00		100.00
근무 직장	기업	6		33.33	66.67	0.00		100.00
	법학 교수	10		50.00	40.00	10.00		100.00
	법실무	8		75.00	25.00	0.00		100.00

[표 4] 개인정보보호법과 공공부문과 민간부문 별도 적용 인지 여부

[문 3] 우리나라의 현행 개인정보보호 관련 입법은 공공부문과 민간부문을 나누어 각각 별도의 법률이 적용되는 형태로 되어 있습니다. 이러한 점에 대해 알고 계십니까?

(단위:%)

		사례수(명)	잘알고있다	그동안몰랐다	계
전체		41	53.66	46.34	100.00
성별	남	36	58.33	41.67	100.00
	여	5	60.00	40.00	100.00
근무기간	1년미만	8	37.50	62.50	100.00
	1~5년미만	20	60.00	40.00	100.00
	5~10년미만	7	71.43	28.57	100.00
	10년이상	6	33.33	66.67	100.00
근무직장	기업	13	38.46	61.54	100.00
	법학교수	16	75.00	25.00	100.00
	법실무	12	41.67	58.33	100.00

[표 5] ‘공공기관의 개인정보보호에 관한 법률’ - 컴퓨터로 처리된 것만 보호 대상인 점 인지 여부

[문 4] 공공부문에 개인정보보호에 적용되는 공공기관의 개인정보보호에 관한 법률은 국가나 지방자치단체 등 공공기관이 보유하고 있는 개인정보로서 컴퓨터로 처리되는 것만을 보호의 대상으로 하고 있습니다. 이러한 사실을 알고 계십니까?

(단위:%)

		사례수 (명)	① 잘 알고 있다	② 막 연히 짐작하 고 있 는 정 도이다	③ 공공 기관이 보 유하는 개 인정보는 모두 보호 의 대상이 되는 줄	④ 컴퓨 터로 처리 되지 않는 개인정보 도 보호를 받을 수 있는 줄	⑤ 모든 개인정보 가 그 보 호의 대상 이 되는 줄 알았다	⑥ 전 혀 몰 랐다	계
전체		41	26.83	19.51	24.39	12.20	12.20	4.88	100.00
성별	남	36	27.78	22.22	25.00	11.11	11.11	2.78	100.00
	여	5	20.00	0.00	20.00	20.00	20.00	20.00	100.00
근무 기간	1년미만	8	12.50	25.00	37.50	12.50	12.50	0.00	100.00
	1~5년 미만	20	25.00	25.00	25.00	10.00	10.00	5.00	100.00
	5~10년 미만	7	42.86	14.29	28.57	0.00	0.00	14.29	100.00
	10년 이상	6	33.33	0.00	0.00	33.33	33.33	0.00	100.00
근무 직장	기업	13	23.08	15.38	23.08	15.38	23.08	0.00	100.00
	법학 교수	16	43.75	18.75	18.75	6.25	6.25	6.25	100.00
	법실무	12	8.33	25.00	33.33	16.67	8.33	8.33	100.00

[표 6] 민간부문의 개인정보보호법 개별분야별 법률만 있는 점에 대한 인지 여부

[문 5] 민간부문에서의 개인정보보호와 관련하여 일반적으로 적용되는 법률은 없으며 개별 분야별로 적용되는 법률이 따로 존재합니다. 이러한 사실에 대해 알고 계십니까?

(단위:%)

		사례수(명)	잘알고있다	그동안몰랐다	계
전체		41	63.41	36.59	100.00
성별	남	36	66.67	33.33	100.00
	여	5	40.00	60.00	100.00
근무기간	1년미만	8	62.50	37.50	100.00
	1~5년미만	20	55.00	45.00	100.00
	5~10년미만	7	85.71	14.29	100.00
	10년이상	6	66.67	33.33	100.00
근무직장	기업	13	46.15	53.85	100.00
	법학교수	16	75.00	25.00	100.00
	법실무	12	66.67	33.33	100.00

[표 7] 개인정보가 제대로 보호되고 있는지에 대한 동의

[문 6] 현재 본인의 개인정보가 제대로 보호되고 있다고 느끼십니까?

(단위:%)

		사례수(명)	① 전혀 그렇지 않다	② 그렇지 않다	Bottom2	③ 보통이다	④ 그렇다	Top2	계
전체		41	34.15	48.78	82.93	14.63	2.44	2.44	100.00
성별	남	36	36.11	47.22	83.33	13.89	2.78	2.78	100.00
	여	5	20.00	60.00	80.00	20.00	0.00	0.00	100.00
근무기간	1년미만	8	50.00	37.50	87.50	12.50	0.00	0.00	100.00
	1~5년미만	20	35.00	55.00	90.00	10.00	0.00	0.00	100.00
	5~10년미만	7	42.86	42.86	85.71	14.29	0.00	0.00	100.00
	10년이상	6	0.00	50.00	50.00	33.33	16.67	16.67	100.00
근무직장	기업	13	46.15	38.46	84.62	7.69	7.69	7.69	100.00
	법학교수	16	25.00	62.50	87.50	12.50	0.00	0.00	100.00
	법실무	12	33.33	41.67	75.00	25.00	0.00	0.00	100.00

[표 8] 개인정보가 제대로 보호되고 있지 않다고 생각하는 이유

[문 7] 개인정보가 제대로 보호되고 있지 않다면 그 원인이 무엇이 라고 생각하시는지 1순위부터 3순위까지 응답하여 주십시오.

(단위:%)

		사례수 (명)	① 법률규 정의 미비 내지는 복잡성	③ 정부나 사업자의 인식부족	④ 일반인 의 인식 부족	⑤ 개인정 보 활용의 필요성	계
전체		34	32.35	58.82	2.94	5.88	100
성별	남	34	33.33	56.67	3.33	6.67	100
	여	30	25.00	75.00	0.00	0.00	100
근무기간	1년미만	4	28.57	71.43	0.00	0.00	100
	1~5년 미만	7	27.78	55.56	5.56	11.11	100
	5~10년 미만	18	33.33	66.67	0.00	0.00	100
	10년이상	6	66.67	33.33	0.00	0.00	100
근무직장	기업	3	54.55	45.45	0.00	0.00	100
	법학교수	11	21.43	71.43	7.14	0.00	100
	법실무	14	22.22	55.56	0.00	22.22	100

[표 9] 강화된 ‘개인정보보호법’ 제정의 필요도

[문 8] 현재는 개인정보가 부분적으로 보호되고 있습니다. 개인정보 보호를 보다 강화하기 위한『개인정보보호법』의 제정이 필요하다고 생각하십니까?

(단위:%)

		사례수 (명)	② 필요하 지 않다	④ 시급 하지는 않 지만 필요 하다	⑤ 시급 히, 매우 필요하다	Top2	계
전체		41	2.44	19.51	78.05	97.56	100
성별	남	36	2.78	16.67	80.56	97.22	100

(단위:%)

		사례수 (명)	② 필요하 지 않다	④ 시급 하지는 않 지만 필요 하다	⑤ 시급 히, 매우 필요하다	Top2	계
	여	5	0.00	40.00	60.00	100.00	100
근무기간	1년미만	8	0.00	37.50	62.50	100.00	100
	1~5년 미만	20	0.00	10.00	90.00	100.00	100
	5~10년 미만	7	0.00	42.86	57.14	100.00	100
	10년이상	6	16.67	0.00	83.33	83.33	100
근무직장	기업	13	0.00	15.38	84.62	100.00	100
	법학교수	16	0.00	18.75	81.25	100.00	100
	법실무	12	8.33	25.00	66.67	91.67	100

[표 10] 정부의 개인정보DB 구축 및 이용에 대한 위험성

[문 9] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 위험하다고 생각하십니까?

(단위:%)

		사례수(명)	① 위험 하다	② 위험하 지 않다	③ 잘 모 르겠다	계
전체		41	85.37	12.20	2.44	100
성별	남	36	86.11	13.89	0.00	100
	여	5	80.00	0.00	20.00	100
근무기간	1년미만	8	87.50	12.50	0.00	100
	1~5년미만	20	85.00	10.00	5.00	100
	5~10년미만	7	100.00	0.00	0.00	100
	10년이상	6	66.67	33.33	0.00	100
근무직장	기업	13	92.31	7.69	0.00	100
	법학교수	16	81.25	12.50	6.25	100
	법실무	12	83.33	16.67	0.00	100

[표 11] 정부의 개인정보DB 구축 및 이용에 대한 불쾌감

[문 10] 정부의 각 기관들이 자신의 소관업무의 수행을 위해 본인의 개인정보DB를 구축하여 이용하는 것에 대하여 불쾌하다고 생각하십니까?

(단위:%)

		사례수 (명)	① 불쾌 하다	② 불쾌하지 않다	③ 잘 모르겠다	계
전체		41	65.85	26.83	7.32	100
성별	남	36	61.11	30.56	8.33	100
	여	5	100.00	0.00	0.00	100
근무 기간	1년미만	8	87.50	12.50	0.00	100
	1~5년미만	20	70.00	15.00	15.00	100
	5~10년 미만	7	71.43	28.57	0.00	100
	10년이상	6	16.67	83.33	0.00	100
근무 직장	기업	13	76.92	23.08	0.00	100
	법학교수	16	50.00	31.25	18.75	100
	법실무	12	75.00	25.00	0.00	100

[표 12] 기업의 개인정보DB 구축 및 이용에 대한 위험성

[문 11] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보 DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 위험하다고 생각하십니까?

(단위:%)

		사례수 (명)	① 위험 하다	② 위험하지 않다	③ 잘 모르겠다	계
전체		41	92.68	4.88	2.44	100
성별	남	36	94.44	5.56	0.00	100
	여	5	80.00	0.00	20.00	100
근무 기간	1년미만	8	100.00	0.00	0.00	100

(단위:%)

		사례수 (명)	① 위험 하다	② 위험하지 않다	③ 잘 모르겠다	계
	1~5년미만	20	90.00	5.00	5.00	100
	5~10년미만	7	100.00	0.00	0.00	100
	10년이상	6	83.33	16.67	0.00	100
근무 직장	기업	13	92.31	7.69	0.00	100
	법학교수	16	93.75	0.00	6.25	100
	법실무	12	91.67	8.33	0.00	100

[표 13] 기업의 개인정보DB 구축 및 이용에 대한 불쾌감

[문 12] 민간의 각 기업들이 각자의 목적에 의해 구축한 개인정보 DB에서 나의 개인정보를 필요에 따라 이용하는 것에 대하여 불쾌하다고 생각하십니까?

(단위:%)

		사례수 (명)	① 불쾌 하다	② 불쾌하지 않다	③ 잘 모르겠다	계
전체		41	85.37	9.76	4.88	100
성별	남	36	88.89	8.33	2.78	100
	여	5	60.00	20.00	20.00	100
근무 기간	1년미만	8	100.00	0.00	0.00	100
	1~5년미만	20	85.00	5.00	10.00	100
	5~10년미만	7	85.71	14.29	0.00	100
	10년이상	6	66.67	33.33	0.00	100
근무 직장	기업	13	76.92	15.38	7.69	100
	법학교수	16	87.50	6.25	6.25	100
	법실무	12	91.67	8.33	0.00	100

[표 14] 정부/기업의 개인정보DB 공유에 대한 위험성

[문 13] 앞의 문 11, 12 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 위험하다고 생각하십니까?

(단위:%)

		사례수(명)	① 위험하다	② 위험하지 않다	③ 잘 모르겠다	계
전체		41	90.24	7.32	2.44	100
성별	남	36	88.89	8.33	2.78	100
	여	5	100.00	0.00	0.00	100
근무기간	1년미만	8	100.00	0.00	0.00	100
	1~5년미만	20	95.00	5.00	0.00	100
	5~10년미만	7	100.00	0.00	0.00	100
	10년이상	6	50.00	33.33	16.67	100
근무직장	기업	13	92.31	0.00	7.69	100
	법학교수	16	93.75	6.25	0.00	100
	법실무	12	83.33	16.67	0.00	100

[표 15] 정부/기업의 개인정보DB 공유에 대한 불쾌감

[문 13-1] 앞의 문항과 관련하여, 정부의 각 기관과 민간의 각 기업이 각자가 구축한 DB를 정당한 업무수행을 위하여 다른 기관이나 기업과 공유하는 것에 대하여 불쾌하다고 생각하십니까?

(단위:%)

		사례수(명)	① 불쾌하다	② 불쾌하지 않다	③ 잘 모르겠다	계
전체		41	85.37	12.20	2.44	100
성별	남	36	88.89	11.11	0.00	100

부 록

(단위:%)

		사례수 (명)	① 불쾌 하다	② 불쾌하지 않다	③ 잘 모르겠다	계
	여	5	60.00	20.00	20.00	100
근무 기간	1년미만	8	100.00	0.00	0.00	100
	1~5년미만	20	85.00	10.00	5.00	100
	5~10년미만	7	100.00	0.00	0.00	100
	10년이상	6	50.00	50.00	0.00	100
근무 직장	기업	13	84.62	15.38	0.00	100
	법학교수	16	87.50	6.25	6.25	100
	법실무	12	83.33	16.67	0.00	100

[표 16] 정부의 개인정보 처리 관련 오/남용 가능성

[문] 정부, 기업 각각의 개인정보처리 관련해서 오/남용 가능성은 얼마나 된다고 생각하십니까?

(단위:%)

		사례수 (명)	가능성 없다	보통 이다	가능성 높다	매우 가능 성 높다	Top2	Mean (점)
전체		41	4.88	12.20	48.78	34.15	82.93	4.12
성별	남	36	5.56	11.11	47.22	36.11	83.33	4.14
	여	5	0.00	20.00	60.00	20.00	80.00	4
근무 기간	1년미만	8	0.00	12.50	75.00	12.50	87.50	4
	1~5년 미만	20	5.00	10.00	50.00	35.00	85.00	4.15
	5~10년 미만	7	0.00	0.00	42.86	57.14	100.00	4.57

(단위:%)

		사례수 (명)	가능성 없다	보통 이다	가능성 높다	매우 가능 성 높다	Top2	Mean (점)
	10년 이상	6	16.67	33.33	16.67	33.33	50.00	3.67
근무 직장	기업	13	0.00	23.08	23.08	53.85	76.92	4.31
	법학 교수	16	6.25	6.25	62.50	25.00	87.50	4.06
	법실무	12	8.33	8.33	58.33	25.00	83.33	4

[표 17] 기업의 개인정보 처리 오/남용 가능성

[문] 정부, 기업 각각의 개인정보처리 관련해서 오/남용 가능성은 얼마나 된다고 생각하십니까?

(단위:%)

		사례수 (명)	보통이다	가능성 높다	매우 가능 성 높다	Top2	Mean (점)
전체		41	7.32	26.83	65.85	92.68	4.59
성별	남	36	2.78	30.56	66.67	97.22	4.64
	여	5	40.00	0.00	60.00	60.00	4.2
근무 기간	1년미만	8	0.00	25.00	75.00	100.00	4.75
	1~5년미만	20	10.00	20.00	70.00	90.00	4.6
	5~10년 미만	7	0.00	28.57	71.43	100.00	4.71
	10년이상	6	16.67	50.00	33.33	83.33	4.17
근무 직장	기업	13	7.69	30.77	61.54	92.31	4.54
	법학교수	16	6.25	37.50	56.25	93.75	4.5
	법실무	12	8.33	8.33	83.33	91.67	4.75

[표 18] 정부의 개인정보 처리 관련 오/남용시 위험성

[문] 정부, 기업에서 개인정보처리가 오/남용되었을 경우 얼마나 위험하다고 생각하십니까?

(단위:%)

		사례수 (명)	위험하지 않다	보통 이다	위험 하다	매우위험 하다	Bottom 2	mean (점)
전체		41	2.44	4.88	39.02	53.66	92.68	4.44
성별	남	36	2.78	5.56	38.89	52.78	91.67	4.42
	여	5	0.00	0.00	40.00	60.00	100.00	4.60
근무 기간	1년미만	8	0.00	12.50	37.50	50.00	87.50	4.38
	1~5년 미만	20	0.00	5.00	40.00	55.00	95.00	4.50
	5~10년 미만	7	0.00	0.00	42.86	57.14	100.00	4.57
	10년 이상	6	16.67	0.00	33.33	50.00	83.33	4.17
근무 직장	기업	13	0.00	0.00	38.46	61.54	100.00	4.62
	법학교수	16	0.00	6.25	37.50	56.25	93.75	4.50
	법실무	12	8.33	8.33	41.67	41.67	83.33	4.17

[표 19] 기업의 개인정보 처리 관련 오/남용시 위험성

[문] 정부, 기업에서 개인정보처리가 오/남용되었을 경우 얼마나 위험하다고 생각하십니까?

(단위:%)

		사례수 (명)	보통이다	위험하다	매우위험하다	Bottom2	mean (점)
전체		41	2.44	34.15	63.41	97.56	4.61
성별	남	36	2.78	33.33	63.89	97.22	4.60
	여	5	0.00	40.00	60.00	100.00	4.61
근무 기간	1년미만	8	0.00	50.00	50.00	100.00	4.50
	1~5년미만	20	0.00	25.00	75.00	100.00	4.75

(단위:%)

		사례수 (명)	보통이다	위험하다	매우위험하다	Bottom2	mean (점)
	5~10년 미만	7	0.00	57.14	42.86	100.00	4.43
	10년이상	6	16.67	16.67	66.67	83.33	4.50
근무 직장	기업	13	0.00	53.85	46.15	100.00	4.46
	법학교수	16	0.00	37.50	62.50	100.00	4.63
	법실무	12	8.33	8.33	83.33	91.67	4.75

[표 20] 개인 정보 수집 관련 프라이버시 침해 등 문제 발생 동의 정도

[문] 정부나 기업 등 개인정보처리자가 자신의 업무를 수행하는 과정에서 타인의 개인정보를 수집하게 됩니다. 다음의 수집행위가 본인의 동의 없이 이루어진다면 프라이버시 침해 등의 문제가 발생한다고 생각하십니까?

(Base : 41명, 단위 %)

	매우 그렇지 않다	그렇지 않다	Bottom 2	보통 이다	그렇다	매우그 렇다	Top2	Mean (점)
① 광고기획사가 연예인에 관하여 시중에 떠도는 스캔들소문을 수집하는 행위		14.60	14.60	26.80	34.10	24.40	58.50	3.68
② 기업이 입사원서를 낸 사람들의 평판, 업무능력에 대한 주위사람들의 평가 등의 정보를 수집하는 행위	2.4	14.60	17.00	29.30	31.70	22.00	53.70	3.56

부 록

	매우 그렇지 않다	그렇지 않다	Bottom 2	보통 이다	그렇다	매우그 렇다	Top2	Mean (점)
③ 은행이 대출신청자의 신용도를 평가하는데 필요한 개인정보를 수집하는 행위	4.9	9.80	14.70	29.30	31.70	24.40	56.10	3.61
④ 인터넷쇼핑몰이 이용자의 소비취향에 관한 정보를 수집하는 행위		7.30	7.30	31.70	39.00	22.00	61.00	3.76
⑤ 무료만화를 제공하는 인터넷사이트가 이용자의 만화 취향이나 읽는 습관을 알아보기 위하여 관련 정보를 수집하는 행위		9.80	9.80	31.70	39.00	19.50	58.50	3.68
⑥ (홈페이지에 수집을 금한다는 경고문이 없을 경우) 공개된 나의 홈페이지에 게시된 나의 관련 개인정보를 수집하는 행위		14.60	14.60	24.40	36.60	24.40	61.00	3.71
⑦ (홈페이지에 수집을 금한다는 경고문이 있는 경우) 공개된 나의 홈페이지에 게시된 나의 관련 개인정보를 수집하는 행위	2.4		2.40	4.90	51.20	41.50	92.70	4.29

[표 21] CCTV 설치 관련 프라이버시 침해 등 문제 발생 등의 정도

[문] CCTV와 관련하여 아래의 행위는 프라이버시 침해 등의 문제가 발생한다고 생각하십니까? (이 CCTV는 범죄가 발생할 경우 문제의 상황이나 장면을 다시 볼 수 있도록 하는 기능만 있음)

(Base : 41명, 단위 %)

	매우그 렇지 않다	그렇지 않다	Bottom 2	보통 이다	그렇다	매우그 렇다	Top2	Mean (점)
① 아파트의 안전을 목적으로 지하주차장에 CCTV를 설치하여 오가는 사람들의 모습을 단순 녹화하는 행위	12.2	29.3	41.50	46.3	7.3	4.9	12.20	2.63
② 아파트관리원이 입구에 설치된 CCTV를 활용하여 302호에 사는 A씨의 출퇴근 시간을 계속적으로 기록하는 행위			0.00	9.8	39	51.2	90.20	4.41
③ 대중목욕탕에서 도난사고가 잦아 탈의실에 CCTV를 설치하여 사람들의 모습을 단순 녹화하는 행위		9.8	9.80	9.8	36.6	43.9	80.50	4.15

[표 22] 수집된 개인정보의 소유권자

[문 18] 다른 사람(기업 또는 정부 포함)이 자신의 비용으로 수집, 이용하고 있는 나에 관한 개인정보는 누구의 것이라고 생각하십니까?

(단위:%)

		사례수(명)	① 자신의 비용으로 처리하고 있는 그 사람의 자산이다	② 나의 개인정보는 나의 인격적 징표로서 나의 것이다	③ 그 누구의 것도 아니다	계
전체		41	24.39	73.17	2.44	100
성별	남	36	22.22	75.00	2.78	100
	여	5	40.00	60.00	0.00	100
근무기간	1년미만	8	0.00	87.50	12.50	100
	1~5년미만	20	40.00	60.00	0.00	100
	5~10년미만	7	14.29	85.71	0.00	100
	10년이상	6	16.67	83.33	0.00	100
근무직장	기업	13	23.08	69.23	7.69	100
	법학교수	16	18.75	81.25	0.00	100
	법실무	12	33.33	66.67	0.00	100

[표 23] 기업이 수집한 고객정보 이용에 대한 태도

[문 19] 기업이 거래과정에서 고객으로부터 받은 연락정보(주소, 전화번호, 이메일주소)를 이용하여 자사의 다른 상품이나 서비스를 광고하는 것은 허용될 수 있다고 생각하십니까?

(단위:%)

		사례수(명)	① 절대 허용되어서는 안 된다	② 고객의 사전 동의가 있으면 허용된다	③ 사후에 고객이 거부할 하면 더 이상 이용하지 않는다는 조건	계
전체		41	7.32	73.17	19.51	100
성별	남	36	8.33	77.78	13.89	100
	여	5	0.00	40.00	60.00	100
근무기간	1년미만	8	12.50	62.50	25.00	100
	1~5년미만	20	5.00	70.00	25.00	100
	5~10년미만	7	0.00	85.71	14.29	100
	10년이상	6	16.67	83.33	0.00	100
근무직장	기업	13	7.69	61.54	30.77	100
	법학교수	16	0.00	75.00	25.00	100
	법실무	12	16.67	83.33	0.00	100

[표 24] 기업의 개인별 프로파일 이용에 대한 태도

[문 20] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 소비자의 생활방식, 취미, 소비성향 등을 조사,분석하여 개인별 프로파일을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

(단위:%)

		사례수(명)	① 절대 허용되어서는 안 된다	② 고객의 사전 동의가 있으면 허용 된다	③ 사후에 고객이 거부할 하면 더 이상 이용하지 않는다는 조건	④ 동의나 다른 조건 없이 자유롭게 허용 된다	계
전체		41	4.88	80.49	12.20	2.44	100
성별	남	36	5.56	86.11	8.33	0.00	100
	여	5	0.00	40.00	40.00	20.00	100
근무 기간	1년 미만	8	12.50	75.00	12.50	0.00	100
	1~5년 미만	20	5.00	70.00	20.00	5.00	100
	5~10년 미만	7	0.00	100.00	0.00	0.00	100
	10년 이상	6	0.00	100.00	0.00	0.00	100
근무 직장	기업	13	0.00	76.92	15.38	7.69	100
	법학 교수	16	0.00	81.25	18.75	0.00	100
	법실무	12	16.67	83.33	0.00	0.00	100

[표 25] 대통령의 개인별 프로파일 이용에 대한 태도

[문 21] 대통령이 정부의 중요 정책에 적합한 인물을 임명하기 위하여 사회지도층에 해당하는 사람들의 인물정보를 수집하여 개인별 프로파일을 만들어 이용하는 것은 허용되어야 한다고 생각하십니까?

(단위:%)

		사례수 (명)	① 절대 허용되어 서는 안 된다	② 해당 자의 사 전 동의 가 있으 면 허용 된다	③ 사후 에 해당자 가 거부를 하면 더 이상 이용 하지 않는 다는 조건	④ 꼭 필 요한 범 위 내에 서는 동 의나 다 른 조건 없이 허 용 된다	⑤ 공익 상의 목 적이므로 어떠한 정보를 수집하든 자유롭게 허용	계
전체		41	2.44	56.10	17.07	21.95	2.44	100.00
성별	남	36	2.78	55.56	19.44	19.44	2.78	100.00
	여	5	0.00	60.00	0.00	40.00	0.00	100.00
근무 기간	1년 미만	8	0.00	37.50	37.50	12.50	12.50	100.00
	1~5년 미만	20	5.00	60.00	15.00	20.00	0.00	100.00
	5~10년 미만	7	0.00	71.43	0.00	28.57	0.00	100.00
	10년 이상	6	0.00	50.00	16.67	33.33	0.00	100.00
근무 직장	기업	13	0.00	76.92	7.69	7.69	7.69	100.00
	법학 교수	16	0.00	56.25	12.50	31.25	0.00	100.00
	법실무	12	8.33	33.33	33.33	25.00	0.00	100.00

[표 26] 기업이 수집한 나의 연락 정보 판매에 대한 태도

[문 22] 기업이 수집한 나의 연락정보를 제3자에게 돈을 받고 판매하는 것은 허용되어야 한다고 생각하십니까?

(단위:%)

		사례수(명)	① 절대 허용되어서는 안 된다	② 고객의 사전 동의가 있으면 허용 된다	③ 사후에 고객이 거부하면 더 이상 이용하지 않는다는 조건	④ 동의나 다른 조건 없이 자유롭게 허용 된다	계
전체		41	63.89	30.56	5.56	0.00	100.00
성별	남	36	40.00	40.00	0.00	20.00	100.00
	여	5	50.00	50.00	0.00	0.00	100.00
근무기간	1년미만	8	70.00	20.00	10.00	0.00	100.00
	1~5년미만	20	57.14	28.57	0.00	14.29	100.00
	5~10년미만	7	50.00	50.00	0.00	0.00	100.00
	10년이상	6	61.54	30.77	0.00	7.69	100.00
근무직장	기업	13	56.25	31.25	12.50	0.00	100.00
	법학교수	16	66.67	33.33	0.00	0.00	100.00
	법실무	12	60.98	31.71	4.88	2.44	100.00

[표 27] (기업→기업) 개인별 프로파일 판매에 대한 태도

[문 23] 기업이 소비자에게 맞춤서비스를 제공하기 위하여 만든 개인별 프로파일을 다른 기업에게 판매하는 것이 허용되어야 한다고 생각하십니까?

(단위:%)

		사례수 (명)	① 절대 허용 되어서는 안 된다	② 고객의 사전 동의를 있으면 허용 된다	③ 사후에 고 객이 거부를 하면 더 이상 이용하지 않는 다는 조건	계
전체		41	56.10	39.02	4.88	100
성별	남	36	58.33	36.11	5.56	100
	여	5	40.00	60.00	0.00	100
근무 기간	1년미만	8	50.00	50.00	0.00	100
	1~5년 미만	20	75.00	15.00	10.00	100
	5~10년 미만	7	42.86	57.14	0.00	100
	10년이상	6	16.67	83.33	0.00	100
근무 직장	기업	13	53.85	46.15	0.00	100
	법학교수	16	56.25	31.25	12.50	100
	법실무	12	58.33	41.67	0.00	100

[표 28] (기업→수사기관) 개인별 프로파일 제공에 대한 태도(영장 없이)

[문 24] 기업이 보유하고 있는 소비자의 개인정보를 수사기관의 요청에 따라 법관이 발부한 영장 없이 제공하는 것에 대하여 어떻게 생각합니까?

(단위:%)

		사례수 (명)	① 절대 허용 되어서는 안 된다	② 개인의 사전 동의가 있으면 허용될 수 있다	③ 사후에 개인이 거부할 하면 더 이상 제공하지 않는다는 조건	④ 수사기관에 개인정보를 제공하는 것이 법률에 따른 것이면 허용	계
전체		41	48.78	17.07	4.88	29.27	100
성별	남	36	52.78	16.67	2.78	27.78	100
	여	5	20.00	20.00	20.00	40.00	100
근무 기간	1년 미만	8	50.00	25.00	0.00	25.00	100
	1~5년 미만	20	50.00	15.00	5.00	30.00	100
	5~10년 미만	7	57.14	28.57	0.00	14.29	100
	10년 이상	6	33.33	0.00	16.67	50.00	100
근무 직장	기업	13	53.85	7.69	7.69	30.77	100
	법학 교수	16	37.50	25.00	6.25	31.25	100
	법실무	12	58.33	16.67	0.00	25.00	100

[표 29] (정부→정부) 개인정보 제공에 대한 태도

[문 25] 자신의 소관업무 수행목적 이외에 국민의 개인정보를 다른 기관에게 제공하는 것은 허용되어야 한다고 생각하십니까?

(단위:%)

		사례수 (명)	① 절대 허용되어서 는 안 된다	② 해당자 의 사전 동의가 있 으면 허용 된다	③ 사후에 해당자가 거부를 하 면 더 이 상 이용하 지 않는다 는 조건	④ 꼭 필 요한 범위 내에서는 동의나 다 른 조건 없이 허용 된다	⑤ 공익 상의 목 적이므로 어떠한 정보를 수집하든 자유롭게 허용	계
전체		41	29.27	29.27	2.44	36.59	2.44	100.00
성별	남	36	30.56	27.78	2.78	36.11	2.78	100.00
	여	5	20.00	40.00	0.00	40.00	0.00	100.00
근무 기간	1년 미만	8	37.50	25.00	0.00	37.50	0.00	100.00
	1~5년 미만	20	25.00	40.00	5.00	30.00	0.00	100.00
	5~10년 미만	7	42.86	14.29	0.00	42.86	0.00	100.00
	10년 이상	6	16.67	16.67	0.00	50.00	16.67	100.00
근무 직장	기업	13	38.46	30.77	7.69	23.08	0.00	100.00
	법학 교수	16	18.75	31.25	0.00	50.00	0.00	100.00
	법실무	12	33.33	25.00	0.00	33.33	8.33	100.00

[표 30] (정부→수사기관) 개인정보 제공에 대한 태도

[문 26] 앞의 질문에서 제공받는 기관이 수사기관이라고 한다면 그 정보제공에 대하여 어떻게 생각합니까?

(단위:%)

		사례수 (명)	① 절대 허용되어서 는 안 된다	② 개인의 사전 동의 가 있으면 허용될 수 있다	③ 사후에 개인이 거 부를 하면 더 이상 제공하지 않는다는 조건	④ 수사기 관에 개인 정보를 제 공하는 것 이 법률에 따른 것이 면 허용	⑤ 공익 을 이유로 한 것이므 로 자유롭 게 허용 된다	계
전체		41	17.07	26.83	7.32	43.90	4.88	100.00
성별	남	36	19.44	27.78	8.33	41.67	2.78	100.00
	여	5	0.00	20.00	0.00	60.00	20.00	100.00
근무 기간	1년 미만	8	25.00	37.50	0.00	37.50	0.00	100.00
	1~5년 미만	20	10.00	40.00	15.00	30.00	5.00	100.00
	5~10년 미만	7	28.57	0.00	0.00	71.43	0.00	100.00
	10년 이상	6	16.67	0.00	0.00	66.67	16.67	100.00
근무 직장	기업	13	30.77	15.38	15.38	38.46	0.00	100.00
	법학 교수	16	12.50	31.25	0.00	50.00	6.25	100.00
	법실무	12	8.33	33.33	8.33	41.67	8.33	100.00

[표 31] (정부→정부) 개인정보 공유에 대한 태도

[문 27] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 각 정부기관들이 자신의 소관업무의 수행을 위하여 공유하는 것에 대하여 어떻게 생각하십니까?

(단위:%)

		사례수 (명)	① 매우 바람직하 지 않다	② 바람직 하지 않다	Bottom2	③ 그저 그렇다	④ 바람 직하다	Mean (점)
전체		41	9.76	53.66	63.41	21.95	14.63	2.41
성별	남	36	11.11	52.78	63.89	19.44	16.67	2.42
	여	5	4.00	22.00	26.00	9.00	6.00	2.40
근무 기간	1년 미만	8	0.00	75.00	75.00	12.50	12.50	2.38
	1~5년 미만	20	10.00	50.00	60.00	35.00	5.00	2.35
	5~10년 미만	7	14.29	57.14	71.43	14.29	14.29	2.29
	10년 이상	6	16.67	33.33	50.00	0.00	50.00	2.83
근무 직장	기업	13	15.38	61.54	76.92	7.69	15.38	2.23
	법학 교수	16	12.50	50.00	62.50	31.25	6.25	2.31
	법실무	12	0.00	50.00	50.00	25.00	25.00	2.75

[표 32] (정부→금융기관) 개인정보 공유에 대한 태도

[문 28] 정부의 각 기관들이 보유하고 있는 국민 개개인의 개인정보를 금융기관의 업무수행을 위하여 금융기관들과 공유하는 것이 필요하다고 생각하십니까?

(단위:%)

		사례수 (명)	① 전혀 필요하지 않다	② 필요 하지 않다	Bottom 2	③ 그저 그렇다	④ 필요 하다	Mean(점)
전체		41	19.51	48.78	68.29	21.95	9.76	2.22
성별	남	36	22.22	50.00	72.22	16.67	11.11	2.17
	여	5	0.00	40.00	40.00	60.00	0.00	2.60
근무 기간	1년미만	8	0.00	87.50	87.50	0.00	12.50	2.25
	1~5년 미만	20	15.00	50.00	65.00	35.00	0.00	2.20
	5~10년 미만	7	57.14	28.57	85.71	14.29	0.00	1.57
	10년 이상	6	16.67	16.67	33.33	16.67	50.00	3.00
근무 직장	기업	13	23.08	46.15	69.23	15.38	15.38	2.23
	법학 교수	16	18.75	56.25	75.00	25.00	0.00	2.06
	법실무	12	16.67	41.67	58.33	25.00	16.67	2.22

[표 33] 정확한 신상 정보 요구시 회원 가입의 태도

[문 29] 인터넷사이트 회원 가입시 정확한 신상정보의 입력을 요구하는 경우가 대부분입니다. 이 때 회원가입을 하십니까?

(단위:%)

		사례수(명)	① 별다른 거리낌 없이 정확한 신상정보를 입력하고 가입한다	② 마지못해 입력하고 대부분 가입 한다	③ 신상정보를 요구하면 대부분 가입하지 않는다	계
전체		41	4.88	70.73	24.39	100
성별	남	36	5.56	69.44	25.00	100
	여	5	0.00	80.00	20.00	100
근무 기간	1년 미만	8	0.00	75.00	25.00	100
	1~5년 미만	20	5.00	70.00	25.00	100
	5~10년 미만	7	0.00	71.43	28.57	100
	10년 이상	6	16.67	66.67	16.67	100
근무 직장	기업	13	0.00	76.92	23.08	100
	법학 교수	16	6.25	62.50	31.25	100
	법실무	12	8.33	75.00	16.67	100

[표 34] 인터넷사이트 회원 가입시 신상 정보 기입 태도

[문 30] 실명확인을 하지 않는 인터넷사이트에 회원가입을 할 때 당신은 자신의 정확한 신상정보를 입력하십니까?

(단위:%)

		사례수 (명)	① 언제나 정확한 신상 정보를 입력한다	② 가끔 틀린 신상 정보를 입력한다	계
전체		41	60.98	39.02	100
성별	남	36	58.33	41.67	100
	여	5	80.00	20.00	100
근무 기간	1년미만	8	75.00	25.00	100
	1~5년 미만	20	60.00	40.00	100
	5~10년 미만	7	42.86	57.14	100
	10년이상	6	66.67	33.33	100
근무 직장	기업	13	61.54	38.46	100
	법학교수	16	62.50	37.50	100
	법실무	12	58.33	41.67	100

[표 35] 인터넷게시판 실명제 필요도

[문 31] 인터넷게시판실명제에 대하여 어떻게 생각하십니까?

(단위:%)

		사례수 (명)	① 전 혀 필 요하지 않다	② 필 요하지 않다	Bottom 2	③ 그 저 그 렇다	④ 필 요하다	⑤ 매 우 필 요하다	Top2	Mean (점)
전체		41	9.76	24.39	34.15	19.51	29.27	17.07	46.34	3.2
성별	남	36	11.11	25.00	36.11	19.44	30.56	13.89	44.44	3.11
	여	5	0.00	20.00	20.00	20.00	20.00	40.00	60.00	3.80
근무 기간	1년미만	8	12.50	25.00	37.50	12.50	25.00	25.00	50.00	3.25
	1~5년 미만	20	10.00	20.00	30.00	25.00	35.00	10.00	45.00	3.15
	5~10년 미만	7	14.29	28.57	42.86	14.29	28.57	14.29	42.86	3.00
	10년이상	6	0.00	33.33	33.33	16.67	16.67	33.33	50.00	3.50
근무 직장	기업	13	7.69	15.38	23.08	7.69	38.46	30.77	69.23	3.69
	법학교수	16	6.25	25.00	31.25	31.25	31.25	6.25	37.50	3.06
	법실무	12	16.67	33.33	50.00	16.67	16.67	16.67	33.33	2.83

부 록

[표 36] 익명/가명으로 인터넷 이용할 수 있는 법적 환경에 대한 태도

[문 32] 인터넷에서 이용자의 신원이 쉽게 확인될 수 없도록 익명 또는 가명으로 인터넷을 이용할 수 있는 법적 환경 및 시스템이 갖추어진다면 이에 대해 어떻게 생각하십니까?

(단위:%)

		사례수 (명)	① 전혀 바람직하지 않다	② 바람직하지 않다	Bottom 2	③ 그저 그렇다	④ 바람직하다	⑤ 매우 바람직하다	Top2	Mean (점)
전체		41	12.20	24.39	36.59	29.27	29.27	4.88	58.54	2.90
성별	남	36	11.11	25.00	36.11	27.78	30.56	5.56	58.33	2.94
	여	5	20.00	20.00	40.00	40.00	20.00	0.00	60.00	2.60
근무 기간	1년미만	8	12.50	25.00	37.50	25.00	37.50	0.00	62.50	2.88
	1~5년 미만	20	0.00	20.00	20.00	30.00	45.00	5.00	75.00	3.35
	5~10년 미만	7	28.57	14.29	42.86	57.14	0.00	0.00	57.14	2.29
	10년이상	6	33.33	50.00	83.33	0.00	0.00	16.67	0.00	2.17
근무 직장	기업	13	30.77	38.46	69.23	30.77	0.00	0.00	30.77	2.00
	법학교수	16	0.00	18.75	18.75	31.25	37.50	12.50	68.75	3.44
	법실무	12	8.33	16.67	25.00	25.00	50.00	0.00	75.00	3.17

[표 37] 신원확인 요구시 게시판에 글 올리는 태도

[문 33] 공공기관 홈페이지와 포털 등의 게시판에 글을 쓰기 위해서는 반드시 신원을 확인하도록 요구하고 있습니다. 신원확인을 하더라도 게시판에 글을 올리십니까?

(단위:%)

		사례수 (명)	① 별다른 거리 낌 없이 정확한 정보를 입력하 고, 글을 올린다	② 마지못해 입 력하고 대부분 글을 올린다	③ 대부분 글 을 올리지 않 는다	계
전체		41	17.07	21.95	60.98	100
성별	남	36	19.44	19.44	61.11	100
	여	5	0.00	40.00	60.00	100
근무 기간	1년미만	8	0.00	0.00	100.00	100
	1~5년 미만	20	15.00	25.00	60.00	100
	5~10년 미만	7	14.29	42.86	42.86	100
	10년이상	6	50.00	16.67	33.33	100
근무 직장	기업	13	23.08	30.77	46.15	100
	법학교수	16	12.50	18.75	68.75	100
	법실무	12	16.67	16.67	66.67	100

[표 38] 개인정보보호법 제정에 대한 인지

[문 1] 개인정보보호법을 제정하려는 움직임이 있는 것에 대해 알고 계십니까?

(단위:%)

		사례수(명)	① 알고 있다	② 모르고 있다	계
전체		41	78.05	21.95	100
성별	남	36	77.78	22.22	100
	여	5	80.00	20.00	100
근무 기간	1년미만	8	50.00	50.00	100
	1~5년미만	20	85.00	15.00	100
	5~10년미만	7	100.00	0.00	100
	10년이상	6	66.67	33.33	100
근무 직장	기업	13	61.54	38.46	100
	법학교수	16	81.25	18.75	100
	법실무	12	91.67	8.33	100

[표 39] 통합적 법률 제정에 대한 찬성/반대 의견

[문 2] 개인정보보호를 위해 공공부문과 민간부문을 별도로 규율하고 있는 현행의 방식에서 탈피해서 양 부문을 모두 포괄할 수 있는 통합적 법률의 제정이 필요하다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

(단위:%)

		사례수(명)	① 찬성한다	② 반대한다	③ 모르겠다	계
전체		41	85.37	7.32	7.32	100.00
성별	남	36	86.11	8.33	5.56	100.00
	여	5	80.00	0.00	20.00	100.00
근무 기간	1년미만	8	87.50	0.00	12.50	100.00
	1~5년미만	20	80.00	10.00	10.00	100.00
	5~10년미만	7	100.00	0.00	0.00	100.00
	10년이상	6	83.33	16.67	0.00	100.00
근무 직장	기업	13	92.31	0.00	7.69	100.00
	법학교수	16	93.75	6.25	0.00	100.00
	법실무	12	66.67	16.67	16.67	100.00

[표 40] 통합적 법률 제정의 찬성 이유

[문 2-1] 통합적 법률의 제정에 찬성하시는 이유는 다음 중 어느 것
 입니까? 순서대로 2가지를 선택하여 주십시오.

(단위:%)

		사례수(명)	① 양 부문을 굳이 달리 규율해야 할 이유가 없다	② 일반 국민들의 법적 혼란을 줄이기 위해 필요하다	③ 법적 보호의 공백을 최소화하기 위해 불가피하다	④ 양 부문에 걸쳐 법집행의 통일을 기할 필요가 있다
전체		35	22.86	54.29	57.14	65.71
성별	남	31	22.58	51.61	61.29	64.52
	여	4	25.00	75.00	25.00	75.00
근무 기간	1년미만	7	0.00	42.86	71.43	85.71
	1~5년미만	16	31.25	43.75	62.50	62.50
	5~10년미만	7	42.86	71.43	42.86	42.86
	10년이상	5	0.00	80.00	40.00	80.00
근무 직장	기업	12	16.67	66.67	41.67	75.00
	법학교수	15	26.67	46.67	60.00	66.67
	법실무	8	25.00	50.00	75.00	50.00

[표 41] 개인정보보호법 제정시 입법체계

[문 3] 통합적 법률을 제정한 경우 기본법의 체계(공공부문과 민간 부문에 관한 기본적인 사항만 정하고, 나머지는 특수한 분야별 개별 법률에 의해 규율하도록 하는 입법형식)와 일반법의 체계(공공 부문과 민간부문에 관한 일반적인 사항을 모두 규정하도록 하고, 특수한 분야에 대해서는 별도의 특별법에 의해 규율하도록 하는 입법형식)를 고려할 수 있습니다. 이 가운데 어느 입법체계가 바람직하다고 생각합니까?

(단위:%)

		사례수 (명)	① 기본법의 체계	② 일반법의 체계	③ 어느 것이 든 무방하다	계
전체		41	48.78	41.46	9.76	100.00
성별	남	36	47.22	44.44	8.33	100.00
	여	5	60.00	20.00	20.00	100.00
근무 기간	1년미만	8	62.50	37.50	0.00	100.00
	1~5년 미만	20	55.00	35.00	10.00	100.00
	5~10년 미만	7	14.29	57.14	28.57	100.00
	10년이상	6	50.00	50.00	0.00	100.00
근무 직장	기업	13	46.15	46.15	7.69	100.00
	법학교수	16	31.25	50.00	18.75	100.00
	법실무	12	75.00	25.00	0.00	100.00

[표 42] 기본법에서 규율해야 할 경우 항목

[문3-1] 기본법의 체계로 갈 경우 기본법에서 규율해야 할 것으로 생각하시는 항목에 모두 체크해주시기 바랍니다.

(단위:%)

		사례수 (명)	① 개인 정보보 호의 기 본이념	② 기 본개념 의 정의	③ 개 인정보 취급상 의 기 본원칙	④ 개 인정보 보호를 위한 국가의 책무와 시책	⑤ 권 리행사 의 방 법과 절차	⑥ 개인 정보보 호기구	⑦ 피 해의 구제와 제재	계 (700% 기준)
전체		20	90.00	85.00	100.00	90.00	85.00	75.00	80.00	605.00
성 별	남	17	94.12	88.24	100.00	94.12	88.24	88.24	82.35	635.29
	여	3	66.67	66.67	100.00	66.67	66.67	0.00	66.67	433.33
근 무 기 간	1년미만	5	100.00	80.00	100.00	100.00	80.00	80.00	80.00	620.00
	1~5년 미만	11	90.91	90.91	100.00	81.82	81.82	81.82	81.82	609.09
	5~10년 미만	1	0.00	0.00	100.00	100.00	100.00	0.00	0.00	300.00
	10년 이상	3	100.00	100.00	100.00	100.00	100.00	66.67	100.00	666.67
근 무 직 장	기업	6	83.33	66.67	100.00	66.67	83.33	50.00	83.33	533.33
	법학 교수	5	80.00	100.00	100.00	100.00	80.00	100.00	80.00	640.00
	법실무	9	100.00	88.89	100.00	100.00	88.89	77.78	77.78	633.33

[표 43] 민간부문에 대한 별도의 일반법 제정 필요성

[문 4] 현행과 같이 공공부문과 민간부문 간에 분리된 입법의 방식을 취한다고 하더라도 민간부문에 대한 일반법을 별도로 제정할 필요가 있다는 주장이 있습니다. 이에 대해 어떻게 생각하고 계십니까?

(단위:%)

		사례수 (명)	① 찬성한다	② 반대한다	③ 모르겠다	계
전체		41	60.98	12.20	26.83	100
성별	남	36	66.67	11.11	22.22	100
	여	5	20.00	20.00	60.00	100
근무 기간	1년미만	8	62.50	12.50	25.00	100
	1~5년미만	20	65.00	5.00	30.00	100
	5~10년 미만	7	28.57	42.86	28.57	100
	10년이상	6	83.33	0.00	16.67	100
근무 직장	기업	13	46.15	23.08	30.77	100
	법학교수	16	62.50	6.25	31.25	100
	법실무	12	75.00	8.33	16.67	100

부록 Ⅲ. 일본의 개인정보보호법 관련 자료

Ⅲ-1. 2004년도 일본 ‘행정기관개인정보보호법’ 시행상황 조사결과보고서

2004년 6월

일본 총무성 행정관리국

목 차

- 조사목적
- 대상기관
- 대상기간
- 개인정보 파일의 보유현황
- 개인정보 보호에 관한 연수 실행 현황
- 개인정보의 이용·제공 현황
- 공개청구 등의 현황

자료편

- 자료 1
- 자료 2
- 자료 3
- 자료 4
- 자료 5

■ 조사목적

2004년도의 행정기관이 보유하는 전자계산기 처리에 관한 개인정보 보호에 관한 법률(1988년 법률 제95호. 이하 「법」이라 한다) 시행현황을 정확히 파악하여, 일본국민들에게 널리 명확하게 데에 그 목적이 있다.

■ 대상기관

법 제2조 제1호가 규정하는 모든 행정기관

- 법 제2조 제1호 이(イ)에 해당되는 기관(인사원을 제외한) 34개의 행정기관

부(府)·성(省)	위원회	청(庁)
내각부	공정거래위원회	궁내청
	국가공안위원회	방위청 방위시설청
총무성	공해 등 조정위원회	소방청
법무성		공안조사청
외무성	중앙노동위원회	국세청
재무성		문화청
문부과학성		사회보험청
후생노동성		임야청
농림수산업성		수산청
경제산업성		자원에너지청
		특허청
	중소기업청	
국토교통성	선원노동위원회	해상보안청
		해난심판청
		기상청
환경성		

- 법률의 규정에 근거하여 내각의 관할 하에 두어지는 기관 : 인사원
- 법 제2조 제1호 口의 규정에 의해 정부령(政令)에서 정해지는 기관 : 경찰청, 검찰청(주1)

(주1) 검찰청에 관해서는 최고검찰청, 고등검찰청, 지방검찰청 및 구(區)검찰청 각각은 법률상의 행정기관에 해당하지만, 이 조사에서는 하나의 행정기관으로 취급하였다.

■ 대상기간

2004년 4월 1일부터 2005년 3월 31일까지. 단, 개인정보 파일의 보유현황에 관해서는 2005년 3월 1일(법 아래에서 최후의 관보공시를 행한 날짜) 현재의 현황이다.

■ 개인정보 파일의 보유현황

- 법 제6조 제1항 및 제8조 제1항의 규정에 근거하여, 총무성에 통지되고, 관보에 공시되어 있는 개인정보파일(공시대상 개인정보 파일)을 보유하고 있는 곳은 24개 행정기관이며, 공시대상 개인정보파일 수는 3,013개였다.

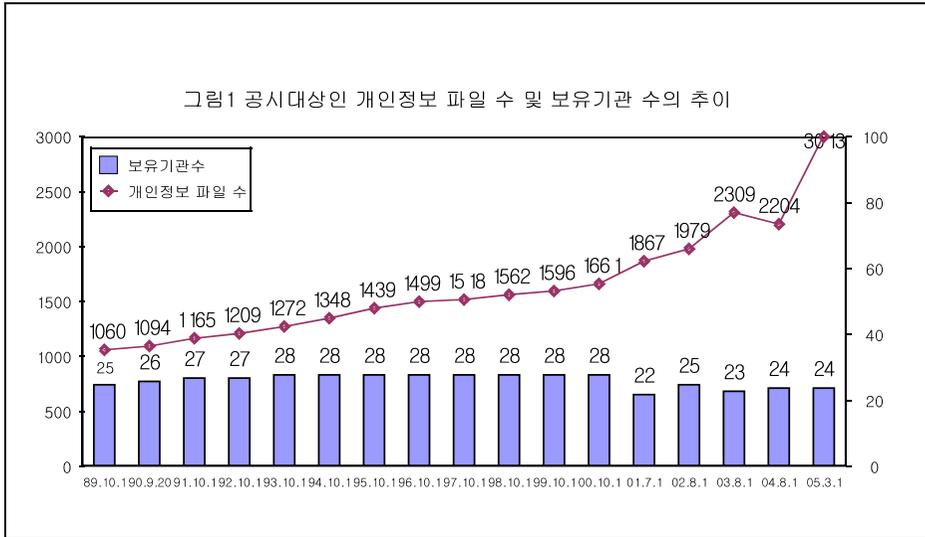
■ 개인정보 보호에 관한 연수 실행 현황

- 2004년에는 21개 행정기관의 내부부국(內部部局), 지방지분부국 등에서, 138 종류의 연구 중 개인정보 보호에 관한 연수(주2)가 총 2,202회 실시되었다.

(주2) 연수내용 일부에 개인정보 보호에 관련하는 것이 있는 것도 포함하였다. 또한, 2005년 4월부터 시행된 ‘행정기관이 보유하는개인정보보호에관한법률(2004년 법률 제58호)에 관련한 연구 등도 포함하였다.

더욱이 이 외에도 총무성이 시행했던 ‘행정기관이보유하는개인정보보호에관한법률’의 설명회나 정보시스템 통일

연수에서 개인정보 보호에 관한 연수를 각 행정기관의 직원이 수강하고 있다.



■ 개인정보의 이용·제공 현황

- 2004년에는 5개 행정기관이 **법 제9조 제1항(법률의 규정에 근거한 이용·제공)**의 규정에 근거하여, 파일보유 목적 이외의 목적을 위하여 처리정보를 이용·제공하고 있다.

표1 법 제9조 제1항의 규정에 근거한 이용·제공 현황

행정 기관명	개인정보 파일의 명칭	이용·제공처(주1)
총무성	연금(恩給) 등 수급자 데이터베이스	지방자치단체(市町村), 관할세무서
	아마추어 무선국 파일	인터넷에서 일부사항 공개
	퍼스널 무선 파일	인터넷에서 일부사항 공개
후생 노동성	원호(援護)연금수급자 데이터 파일	국민생활금융공고, 오키나와진 흥개발금융공고

부 록

행정 기관명	개인정보 파일의 명칭	이용·제공처(주1)
사회 보험청	건강보험후생연금현재피보험자 파일	독일 보험자(주2), 영국 연락 기관(주3)
	건강보험후생연금상실피보험자 파일	독일 보험자
	건강보험후생연금임계(任繼)제4 종피보험자 파일	독일 보험자, 영국 연락기관
	선원보험후생연금(船保厚年)피보 험자 파일	독일 보험자, 영국 연락기관
	국민연금피보험자 파일	독일 보험자, 영국 연락기관
	연금수급권자 파일	독일 보험자
특허청	기초연금번호관리 파일	독일 보험자, 영국 연락기관
	산업재산권 심판업무용 파일	(재) 일본특허정보기구, 불특 정다수에게 열람
	산업재산권 출원업무용 파일	(재) 일본특허정보기구, 불특 정다수에게 열람
국토 교통성	산업재산권등록 파일	(재) 일본특허정보기구, 불특 정다수에게 열람
	측량업자등록정보 파일	불특정다수에게 열람
	자동차등록 파일	등록사항 등 증명서 신청자, (재) 자동차검사등록협력회

- (주) 1 이용·제공에 관계된 법률상의 근거규정에 관해서는 자료 3 참조
 2 『독일보험자』라는 것은, 독일연금제도 운영에 책임이 있는 보험기관 및 연
 금조직을 말한다.
 3 『영국 연락기관』라는 것은, 사회보장에 관한 일본국과 대영제국 및 북부아
 일랜드 연합왕국과의 사이의 협정에 근거한 대영제국 및 북부 아일랜드 연합
 왕국의 연락기관을 말한다.

○ 2004년에는, 8개 행정기관이 **법 제9조 제2항의 규정(본인의 동의에 의한 제공 등)**에 근거하여, 파일보유목적 이외의 목적을 위해 처리정보를 이용·제공하고 있었다.

표2 법 제9조 제2항의 규정에 근거한 이용·제공 현황

행정 기관명	개인정보 파일의 명칭	이용·제공처
경찰청	운전자관리 파일	법무성(3호), 자동차안전운전센터(4호), 미국 뉴햄프셔주(4호)
법무성	후견등록 등에 관한 법률 제4조의 후견등기 등 파일 일본인출귀국기록 마스터파일 사법시험 제2차 시험 파일	지방자치단체(市町村)(3호) 외무성(3호) 국립대학법인(3호), 사립대학(4호) 외무성영사국 해외방인(邦人) 안전과, 동방인(同邦人)테러대책실(이상 2호), 법무성입국관리국(3호)
외무성	여권관리 마스터파일	(사) 일본신문협회(4호)
국세청	재일외국보도관계자 파일 납세지 등 필수정보 파일 납세지 등 종속정보 파일 데이터베이스자료파일 과세사적(事績)가산세정보 파일 납세지 등 개별정보 파일 과세사적(事績)정보 파일 원천징수의무자 파일	지방공공단체(3호) 지방공공단체(3호) 지방공공단체(3호) 지방공공단체(3호) 지방공공단체(3호) 지방공공단체(3호) 지방공공단체(3호) 인사원(3호)
후생 노동성	고용보험지급대장 고연령자고용계속급부대장 원호(援護)연금수급자 데이터파일 노동자재해보상보험연금수급권자 파일 노동자재해보상보험피해자일원관리대장	사회보험청(3호) 사회보험청(3호) 국민생활금융공고, 오키나와진흥개발금융공고(이하 1호) 복지의료기구(3호), (재)노재(勞災)연금복지협회(4호) (재)노해(勞災)연금복지협회(4호)

부 록

행정 기관명	개인정보 파일의 명칭	이용·제공처
사회보 험청	진료록 및 진료자기록 파일	의사, 간호사, 임상실험기사, 진료 방사선기사, 레지던트 (이상 4호) (재)사회보험건강사업재단, 도 도부현(都道府県)의회의원공제 회, 시의회의원공제회, 정촌(町 村)의회의원공제회(이하 4호) 연금자금운영기금(3호), 후생 연금기금연합회, 도도부현(都 道府県)의회의원공제회, 시의 회의원공제회, 정촌(町村)의회 의원공제회(이하 4호) 연금자금운영기금, (재)선원보 험회, 도도부현(都道府県)의회 의원공제회, 시의회의원공제 회, 정촌(町村)의회의원공제회 (이하 4호) 연금자금운용기금, 농업자연 금기금(이하 3호), 국민연금기 금연합회(4호) 후생노동성보험국국민건강보 험과, 연금자금운영기금, 복 지의료기구(이하 3호), 후생연 금기금연합회, 국민생활금융 공고, 오키나와진흥개발금융 공고(이하 4호) 국가공무원공제조합연합회, 지방공무원공제조합연합회, 일본사립학교진흥·공제사업 단, 농림어업단체직원공제조 합(이하 4호) 지방공무원공제조합연합회(4호) 자원에너지청 전력시장정비 과(3호)
	건강보험후생연금현재피보험자 파일	
	건강보험후생연금상실피보험자 파일	
	선원보험후생연금피보험자 파일	
	국민연금피보험자 파일	
	연금수급권자 파일	
	고용정보 파일	
경제 산업성	개호보험정보 파일	
	자가용전기공작물 데이터베이스	

행정 기관명	개인정보 파일의 명칭	이용·제공처
국토 교통성	이륜자동차검사 파일	(재) 자동차검사등록협력회(4호)
	건설건설터트등록정보 파일	불특정다수에게 열람(4호)
	지질조사사업자등록정보 파일	불특정다수에게 열람(4호)
	보상건설터트등록정보 파일	불특정다수에게 열람(4호)

(주) 『이용·제공처 등』란 () 내의 『1호』내의 법 제9조 제2항 제1호(본인의 동의 등), 『2호』는 동항 제2호(내부이용), 『3호』는 동항 제3호(행정기관 등에 제공), 『4호』는 동항 제4호(통계, 학술연구목적 등)를 각각 표시하도록 하고 있다.

■ 공개청구 등의 현황

○ 2004년에는 법 제13조의 규정에 근거하여, 3개 행정기관이 보유하는 5개 개인정보 파일에 관하여 총 785건의 공개청구가 있었고, 일부공개 31건 및 처리 중 사안 1건(주1)을 제외하고 전부 공개되었다.

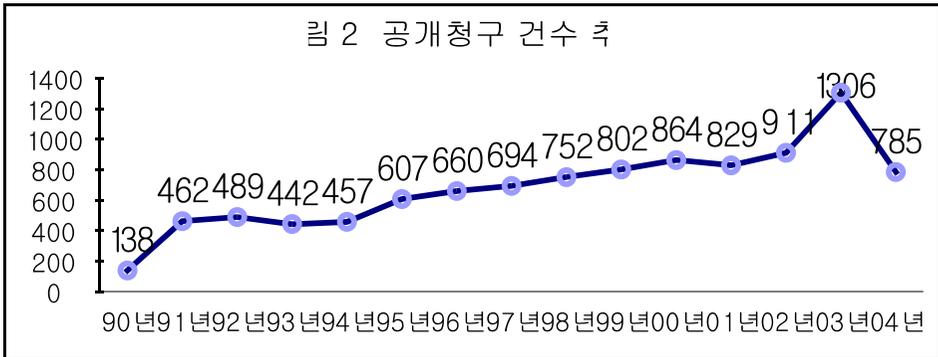
또한 법 제17조의 규정에 근거하여 1개 행정기관이 보유하는 1개 개인정보 파일에 관하여, 정정 등의 신고와 재조사 신고가 각 1건씩이었다.

(주1) 2005년 4월에 전부 공개되었다.

표3 공개청구 등의 현황(2004년)

행정 기관명	개인정보파일의 명칭	공개청구 건수	공개건수 (전부공개)	정정 등 신고건수	재조사 신고건수	처리중 건수
경찰청	운전자관리 파일	3	3	1	1	0
총무성	전기통신소비자상담 파일	1	0	0	0	1
법무성	일본인출귀국기록 마 스터파일	346	346	0	0	0
	외국인출입국기록 마 스터파일	231	231	0	0	0
	사법시험 제2차 시험 파일	204	173	0	0	0
계		785	753	1	1	1

부 록



(주) 1990년에 관해서는, 공개 및 정정 등에 관한 규정이 시행된 1990년 10월 1일부터 1991년 3월 31일까지 건수이다.

자료편

자료 1

일본행정기관별 공시대상 개인정보 파일 수

2005년 3월 1일 기준

보유기관 명칭	파일 수	법 적용관계				(참고) 2004년8월1일 파일 수
		전항목 공개 청구대상	일부항목 타법(他法) 공개	전항목 타법(他法) 공개	공개청구 대상 외	
내각부	12	11	1	0	0	10
공정거래 위원회	1	1	0	0	0	1
경찰청	10	2	7	0	1	10
방위청	18	4	0	0	14	18
금융청	1	0	1	0	0	1
총무성	10	4	3	3	0	10
법무성	2,365	5	2	2,358	0	1,567
검찰청	1	1	0	0	0	1
외무성	11	10	1	0	0	11
재무성	67	44	23	0	0	61
국세청	109	85	22	2	0	109
문부 과학성	10	8	1	0	1	10
문화청	1	1	0	0	0	1
후생 노동성	45	8	8	6	23	45
사회 보험청	12	0	0	11	1	12
농림 수산성	227	226	1	0	0	227
경제 산업성	44	14	22	8	0	44

부 록

보유기관 명칭	파일 수	법 적용관계				(참고) 2004년8월1일 파일 수
		전항목 공개 청구대상	일부항목 타법(他法) 공개	전항목 타법(他法) 공개	공개청구 대상 외	
자원 에너지청	15	6	3	6	0	15
특허청	3	0	0	3	0	3
중소 기업청	1	0	1	0	0	1
국토 교통성	41	15	12	13	1	41
기상청	1	0	1	0	0	2
해상 보안청	1	1	0	0	0	1
환경성	7	7	0	0	0	3
합계	3,013	453	109	2,410	41	2,204
구성비(%)	100.0	15.0	3.6	80.0	1.4	-

(주) 「공개청구 대상 외」는 법 제13조 제1항 단서에 해당하는 개인정보 파일을 말한다.

자료 2

공시대상 개인정보 파일일람

2005년 3월 1일 현재

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법량에 의한 공개	전항목 타법량에 의한 공개	공개청구의 대상 외
내각부	12	정부연구개발 데이터베이스 춘추서훈수장자 파일 춘추호장수장자 파일 감수포장수장자 파일 고령자서훈수장	자가용 전기 공작물 데이터베이스		

부록 III. 일본의 개인정보보호법 관련 자료

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		자 파일 여성인재 데이터 베이스 시스템 위험업무종사자 서훈수장자 파일 영빈관참관관리 정보 파일 생산자 마스터파일 재무성소관보통 재산 데이터베이스 증권외무원등록 파일			
공정 거래 위원회	1	도서문헌정보 파일			
경찰청	10	가출인 파일 이륜차방법등록 파일	풍속영업등 관리 파일 경비업자격 자 등 파일 선임경비원 지도교육책 임자 및 선 임기계경비 업무관리자 파일 업종·공기총 등 관리 파일 운전자관리 파일 고물상 및 고 물시장주관리 파일 전당포관리 파일		유치정보 파일
소방청	18	도서목록 데이터 베이스(4)			의사(医事) 데이터 베이스(3)

부 록

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
					진료 데이터 베이스 진료 데이터 파일(2) 투약 데이터 파일 환자별 병명 마스터파일 환자별 병명 파일 환자상병자명 파일 환자정보 마스터파일 병명 데이터 파일 임상검사 데이터파일(2)
금융청	1		대금업자 파일		
총무성	10	행정상담위원 파일 국소상담 파일 고충처리포 데이터 베이스 전기통신소비자상담 파일	연금 등 수급자 데이터 베이스 아마추어무선국 파일 퍼스널 무선 파일	공사담임자 파일 전기통신주임 기술자 파일 무선종사자 파일	
법무성	2,365	법률문헌정보 데이터파일 도서목록 데이터파일 도서관이용자 데이터파일 인권옹호위원 파일 사법시험 제2차 시험 파일	일본인출귀국기록 마스터파일 외국인출입 기록 마스터 파일	외국인등록 기록 마스터 파일 부동산등기법 제151조 /2 제1항의 등기부(466) 상업등기법 제113조 /2 제1항의 상호 등기부 (472)	

부록 Ⅲ. 일본의 개인정보보호법 관련 자료

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
				상업등기법 제113조 2 제1항의 미성년자등기부(472) 상업등기법 제113조 2 제1항의 후견인등기부(472) 상업등기법 제113조 2 제1항의 지배인등기부(472) 채권양도에 대한항요건에 관한민법특례등에 관한법률 제2조 제1항의 채권양도등기 파일 후견등기등에 관한 법률 제4조의 후견등기등 파일 후견등기등에 관한 법률 제9조의 폐쇄등기파일	
검찰청	1	통역인명부 데이터베이스 시스템			
외무성	11	방인(邦人)서훈명부 재일외국공관구성원 파일 재일외교관용자 동차등록 파일	여권관리 마스터파일		

부 록

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개 청구의 대상 외
		외국서훈수장자 명부 외국인서훈 명부 UN안 보 리 결 의 1267,1333 및 1390에 근거한 자산동결대상리스트 UN안 보 리 결 의 1373에 근거한 자산동결조치대상리스트 재류(在留)신고리스트 주요국국제기관의 일본인직원명부 파일 재일외국보도관계자 파일			
재무성	67	수입통관정보 파일 수출통관정보 파일 분석실적 파일 매뉴얼신고(수입) 정보 파일 조사정보 파일 사후조사사무처리 관리정보 파일 통화·증권 등 반환사무 파일(8) 통관업자·통관사관리대장(6) 도착통지서 파일(8) 통관예정(결과) 데이터 통관사시험수험자명부 여객명부 파일 관세정률법 제21조 제1항 제4호 해당통지서 파일	지적재산권 단속정보 파일 징세조서 파일(9) 통관사시험합격자명부(3) 과세통지서 파일(8) 선륙교통·지정지외교통허가자관리시스템 매뉴얼수출입신고관련 파일(クラリファイ파일)		

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		재무성소관보통재산 데이터베이스 여객 및 승조원(乗組員)성명정보 파일 증권외무원 등록 파일(10)			
국세청	109	증여특례정보 파일 원천징수의무자 파일 채권관리수신인 명 파일 미도래채권관리 파일 납세지 등 종속 정보 파일 납세지 등 필수 정보 파일 납세지 등 개별 정보 파일 신청서 등 사적(事績)관리 파일 결산서 등 손익 정보(일반) 파일 결산서 등 손익 정보(농업) 파일 결산서 등 손익정 보(부동산) 파일 결산서 등 손익 정보(현금주의) 파일 소비세신고이력 파일 소비세신고·결 의사적(事績) 파일 소비세중간신고 사적(事績) 파일 불복제기사안간 이처리 파일	세무사명부 정보 파일 소비세가산 세사적(事 績) 파일 지가가산세 정보 파일 채권관리 파일 과세사적(事 績)정보 파일 과세사적(事 績)공적연금 정보 파일 환부(還付) 관리 파일 조사시부인 (是否認)정 보 파일 상속세신고 정보 파일 증여신고정 보 파일 불복경과 파일 과세처리관 리정보 파일 과세처리중 가산세정보 파일 과세처리과 소신고가산 세정보 파일 예정납세사	세무사시험 일부과목합 격자명부 파일 과세사적(事 績)가산세정 보 파일	

부 록

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개 청구의 대상 외
		개인격(格)수신인 명정보 파일 특정내부사무 시 스템 징수시스템(대납 총괄정보·대납 구좌정보) 세무사관여상황 조사표 파일 소비세신규과세 사업자 파일 대표자가족정보 파일 대표자배우자정 보 파일 실질경영자정보 파일 불복제기쟁점 파일 불복사안연결 파일 불복제기기초 파일 불복제기사무사 적(事績) 파일 개인격(格)종속정 보 파일 개인격(格)통칭명 정보 파일 납세지 등 관리 정보 파일 납세지 등 이동 이력정보 파일 개인격(格)이동이 력정보 파일 이동사적(事績)정 보 파일 관계자공통정보 파일 관계자고유정보 파일 개인격(格)필수정	적(事績) 파일 증명사적(事 績)파일 과세처리과 세정보 파일 조사신고정 보 파일 소비세조사 사적(事績) 파일 지가부과처 분정보 파일 지가신고정 보 파일		

부록 Ⅲ. 일본의 개인정보보호법 관련 자료

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		보 파일 관계자수신인명 정보 파일 과세사적(事績)관 리정보 파일 결산서 등 관리 정보 파일 결산서 등 급여 정보 파일 신규예상자관리 파일 납세상담사적(事 績) 파일 적정신고의 상용 (しょうよう)사적 (事績) 파일 신고심리기본정 보 파일 신고심리사적(事 績) 파일 신고심리조건정 보 파일 신고심리분석기 본정보 파일 신고심리분석수 입정보 파일 사후처리관리 파일 조사사적(事績) 파일 조사손익정보(일 반) 파일 조사손익정보(농 업) 파일 조사손익정보(부 동산) 파일 개황(概況)확인사 적(事績) 파일 소비세조사처리 상태 파일			

부 록

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		소비세비위(非違) 내역 파일 소비세조사사적 (事績)비위(非違) 내역 파일 소비세과세기간 구좌 파일 취소소비세신고 사적(事績) 파일 개별관리정보 파일 양도사안정보 파일 양도자주소정보 파일 양도납세상담정 보 파일 양도신고심리정 보 파일 양도조사사적(事 績)정보 파일 양도조사사적(事 績)명세정보 파일 지가세예상자정 보 파일 지가자료축적정 보 파일 지가과세정보 파일 지가신고심리정 보 파일 지가조사정보 파일 지가사적(事績)관 리정보 파일 상속세조사정보 파일 증여기본정보 파일 증여수증(受贈)자 정보 파일 증여사안정보 파일 비과세저축한도 액관리 파일			

부록 III. 일본의 개인정보보호법 관련 자료

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		명기완료자료 파일 징수시스템(정리사적(事績)) 징수시스템(재산정보) 계속관리적요상세정보 파일 초거대자산가상세정보 파일 계속관리대상자정보 파일 특별관계자상세정보 파일			
문부 과학성	10	방사선역학조사 파일 도서관소장도서 목록 데이터베이스 국비외국인유학생 파일 교육연구소·자료센터간행논문(CENTER) 교육학계박사·석사학위논문과제(JEDI) 교육소프트웨어(EDUSOFT) 초등학교국어교과서(BKTEXT) 초등학교국어교과서게재작품정보(BKWORK)	고등학교교원자격인정시험수험자 파일		대학입학자격검정출원 파일
문화청	1	중요무형문화재 및 선정보존기술보지자(保持者) 정보 파일			
후생 노동성	45	중국귀국교아 등 조회 마스터파일 중국잔류일본인교아 마스터파일	원호(援護) 연금수급자 데이터파일 노동자재해	노동안전위생법에 의한 구면허대장	진료보수명세서 파일(8) 진료록 및 진료자기록

부 록

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		<p>독극물영업자등록 시스템 후생노동과학연구비 데이터베이스 특정구직자고용개발조성금지급 파일 노동자재해보상보험 애프터케어 대상자관리대장 국립한센병요양소 등 퇴소자급여금 명부 공중위생심의회 예방접종건강피해인정부회자료</p>	<p>보상보험연금수급권자 파일 노동안전위생법에 의한 신면허대장 고용보험피보험자 파일 노동자재해보상보험피해자일원관리대장 관리영양사 명부 노동자재해보상보험2차 건강진단 등 급부청구자 관리대장 급수장치공사주입기술자명부</p>	<p>고용보험지급대장 고연령자용계속급부대장 육아휴업급부대장 교육훈련급부대장 개호휴업급부대장</p>	<p>파일 환자 마스터파일 전국암등록자궁경부암 파일 전국암등록자궁암 파일 전국암등록난소암 파일 전국암등록유방암 파일 전국암등록악성골수암 파일 전국암등록양성골수암 파일 전국암등록방광암 파일 전국암등록뇌종양 파일 생화학검사 파일 혈액 검사 파일 환자기본정보 파일 추적조사 데이터파일 등록자정보 파일</p>
사회 보험청	12			<p>기초연금번호관리 파일 공제조합원 정보 파일 공제수급권자정보 파일 건강보험후</p>	<p>건보급부 파일</p>

부록 III. 일본의 개인정보보호법 관련 자료

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
				생연금현존 피 보 험 자 파일 건강보험후생 연금소실피보 험자파일 건강보험후 생연금입계 제4종 피보 험자 파일 선원보험후 생연금피보 험자 파일 국연(国年) 피 보 험 자 파일 연금수급권 자 파일 고 용 정 보 파일 개호보험정 보 파일	
농림 수산성	227	농림수산시험연 구 과 제 파 일 (RECRAS-II) 일본농학문헌기 사색인파일(JASI) 세계농학문헌색 인파일(AGRIS) 생산자 마스터파 일(169) 일필대장 파일(54)	품종등록 파일		
경제 산업성	44	석유제품판매업 자 파일(8) 계량사등록부 파일 특정채권서면열 람 시스템 상담접수 카드 (Data3)을중전기	인정전기공사 종사자 데이 터베이스(6) 특종전기공사 자격자 데이 터베이스(6) 자가용전기공	광업권등록 파일(8)	

부 록

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		용품제조사업자 산업구조심의회 위원명부 광산보안표창수 상자명부	작물 데이터 베이스(9) 알콜유통관 리시스템		
자원에 너지청	15	에너지관리자 파일 에너지관리원 파일 에너지관리원강 습수료자 파일 보안기술직원선해 임(選解任) 대장(2) 총합자원에너지 조사회위원명부	주입기술자 면허장교부 명부 데이터 베이스 가스주입기 술자면허장 교수명부 데 이터베이스 에너지관리 사자격보유 자 파일	보안기술직 원국가시험 합격자대장 (2) 유자격자증 명서교부대 장(4)	
특허청	3			산업재산권 출원업무용 파일 산업재산권 등록 파일 산업재산권 심판업무용 파일	
중소 기업청	1		중소기업진 단사등록부 파일		
국토 교통성	41	건설기술문헌 파일(8) 문헌검색 파일 건설건설턴트등 록정보 파일 지질조사업자등 록정보 파일 건설건설턴트기 술관리자인정신 청자정보 파일 보상건설턴트등 록정보 파일	도로점용허가 마스터파일 하천점용허가 마스터파일 자동차등록 파일 이륜자동차 검사 파일 해기(海技) 면허원명부 항공조사자 파일	항공신체검 사 파일 선원원부 도로점용허 가 파일(8) 택지건물거 래업자면허 정보 파일 측량업자등 록정보 파일 선박원부	자동차손해 배상보장사 업 시스템파일

부록 III. 일본의 개인정보보호법 관련 자료

보유 기관명	파일수	전항목 공개 청구대상	일부항목 타법령에 의한 공개	전항목 타법령에 의한 공개	공개청구의 대상 외
		하수도처리시설 유지관리업자등 특정보 파일	체약국(締約 国)자격수유 자승인원부 건설업허가 정보 파일 일급건축사 등록 마스터 파일 측량사·측량 사보 등록자 마스터파일 건축기준 적 합판정자격 자등록부 선박검사 등 정보관리 시 스템		
기상청	1		기상예보사 명부 파일		
해상 보안청	1	선박명세정보파일			
환경성	7	수은관련문헌 데 이터파일 환경카운셀러등 록부 산업폐기물 처 리·처리시설에 관한 행정처분정 보제공시스템 정화조관리사 파일 환경보건감시조 사 파일 심사청구사건 데 이터베이스 자연공원지도원 명부			
합계	3,013	453	109	2,410	41

자료 3

파일보유목적 이외의 이용·제공 현황(2004년) (법 제9조 제1항)

행정 기관명	개인정보파일의 명칭	이용·제공처	근거법률명	제공 처의 공시
총무성	연금 등 수급자 데이터베이스	지방자치단체(市 町村)	지방세법 제317 조의 6 제3항	有
		관할세무서	소득세법 제226 조 제3항	有
	아마추어무선국 파일	인터넷에 일부 사항 공개(불특 정다수에게 제공)	전과법 제25조	有
	아마추어무선 파일	인터넷에 일부사 항 공개(불특정 다수에게 공개)	전과법 제25조	有
후생 노동성	원호(援護)연금수급 자 데이터파일	국민생활금융공 고, 오키나와진 흥개발금융공고	국민생활금융공 고가 행한 연금 담보금융에 관 한 법률 제8조	有
사회 보험청	건강보험후생연금현 재피보험자 파일	독일보험자(주1)	사회보장에 관 한 일본국과 독 일연방공화국 사이의 협정 시 행에 따른 후생 연금보험법 등 의 특례 등에 관한 법률	有
	건강보험후생연금상 실피보험자 파일	독일보험자	上同	有

부록 III. 일본의 개인정보보호법 관련 자료

행정 기관명	개인정보파일의 명칭	이용·제공처	근거법률명	제공처의 공시
	건강보험후생연금임계 제4종 피보험자 파일	독일보험자	上同	有
	선원보험후생연금피보험자 파일	독일보험자	上同	有
	국민연금피보험자 파일	독일보험자	上同	有
	연금수급권자 파일	독일보험자	上同	有
	기초연금번호관리 파일	독일보험자	上同	有
	건강보험후생연금현재피보험자 파일	영국 연락기관 (주2)	사회보장에 관한 일본국과 대영제국 및 북부아일랜드연합왕국 사이의 협정 시행에 따른 후생연금보험법의 특례 등에 관한 법률	有
	건강보험후생연금임계 제4종 피보험자 파일	영국 연락기관	上同	有
	선원보험후생연금피보험자 파일	영국 연락기관	上同	有
	국민연금피보험자 파일	영국 연락기관	上同	有
	기초연금번호관리 파일	영국 연락기관	上同	有
특허청	산업재산권심판업무용 파일	(재) 일본특허정보기구, 불특정 다수에게 열람	특허법	無
	산업재산권출원업무용 파일	(재) 일본특허정보기구, 불특정 다수에게 열람	上同	無
	산업재산권등록 파일	(재) 일본특허정보기구, 불특정 다수에게 열람	上同	無

부 록

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거법률명	제공 처의 공시
국토 교통성	측량업자등록정보 파일	불특정다수에게 열람	측량법	無
	자동차등록 파일	등록사항 등 증명서의 신청자, (재) 자동차검사 등록협력회	도로운송차량법 제22조	有

- (주) 1 『독일보험자』라는 것은, 독일연금제도의 운영에 책임이 있는 보험기관 및 그 연합조직을 말한다.
 2 『영국연락기관』이라는 것은, 사회보장에 관한 일본국과 대영제국 및 북부아일랜드연합왕국 사이의 협정에 근거한 대영제국 및 북부아일랜드연합왕국의 연락기관을 말한다.

자료 4

파일보유목적 이외의 이용 · 제공 현황(2004년) (법 제9조 제2항)

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
경찰청	운전자관리 파일	법무성	3호	은사(恩赦)조사 및 시행에 관한 사무
		자동차 안전운전센터	4호	사업용자동차의 교통사고억제대책으로 유효한 시책에 관한 조사연구를 위해
		미국뉴햄프셔주	4호	운전면허증취득현황의 설명
법무성	후견등록 등에 관한 법률 제4조의 후견등록 등 파일	지방자치단체(市町村)	3호	인감등록자격의 유무를 판단하기 위해
	일본인출귀국 기록 마스터파일	외무성	3호	여권의 이중발급을 방지하는 등 여권발급의 사무처리를 위해
	사법시험 제2차 시험 파일	국립대학법인	3호	대학에서의 교육 효과 검증 및 교육개선

부록 III. 일본의 개인정보보호법 관련 자료

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
	사법시험 제2차 시험 파일	사립대학	4호	上同
외무성	여권관리 마스터파일	외무성 영사국 해외방인(邦人)안전과 및 방인(邦人)테러대책실	2호	해외에서의 사고 및 사건에 조우(遭遇)한 일본인 신원확인을 위해
		법무성 입국관리국	3호	여권발급사실과 출입국일본인의 조회를 하는 것에 있어 출입국에 관한 부정행위를 방지하기 위해
	재일외국보도관계자 파일	(사) 일본신문협회	4호	일본신문협회가 제공하는 『일본보도에 관한 정보』는 동협회가 주최하는 재일외국정보관계자초대리셉션이나 국제교류사업의 안내, 뉴스레터 등이다. 일본에서의 취재·보도활동을 하는 재일외국보도관계자에게 이러한 정보 제공이 이루어지고 있고, 일본 정보계의 동향에 관한 이해 증진, 취재 자료의 증가, 기자간의 네트워크형성의 촉진 등, 일본에서의 취재·보도활동의 이편(利便)성향에 이바지한다고 하는 관점에서, 명확하게 재일외국보도관계자 본인의 이익이 된다고 인정할 수 있다.
국세청	납세지 등 필수정보 파일	처리정보의 제공요망이	3호	지방세의 적정과세를 위해

부 록

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
		있었던 지방 공공단체		
	납세지 등 종속정보 파일	上同	3호	上同
	인명자료 파일	上同	3호	上同
	과세사적(事績)가산세정보 파일	上同	3호	上同
	납세지 등 개별정보 파일	上同	3호	上同
	과세사적(事績)정보 파일	上同	3호	上同
	원천징수의무자 파일	인사원	3호	인사원에서는 직종별 민간급여 실태조사의 사업소별대장을 작성하고 있어, 해당작업에 필요한 기초데이터를 제공하였다.
후생 노동성	고용보험지급대장	사회보협청	3호	노령후생연금과의 병합조정
	고연령자고용계속급여대장	上同	3호	上同
	원호(援護)연금수급자 데이터파일	국민생활금융공고	1호	전상병자전물자유족 등 원호법 제46조에 근거하여 담보권설정자에 관한 사무의 원활하고 효율적인 운영을 도모하기 위해
		오키나와진흥개발금융공고	1호	上同
	노동자재해보상보험연금수급권자 파일	독립행정법인복지의료기구	3호	피재(被災)노동자원호업무에 관한 사무에 제공하기 위해
		(재)노재(勞災)연금복지협회	4호	上同

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
	노동자재해보상 보험 피재 (被災)자일원 관리대장	(재) 노재(勞災) 연금복지협회	4호	上同
	진료록 및 진료자기록 파일 (국립성육의료센터)	의사, 간호사, 임상검사기사, 진료방사선기사, 레지던트	4호	학회에서의 증례(症例)보고, 의학잡지에 논문발표 계 69건
사회 보험청	건강보험후생연금현재피보험자 파일	(재) 사회보험건강사업재단	4호	생활습관병 예방검진의 수급자격 확인을 위해
		도도부현(都道府県)의 회의원 공제회 · 시의회의원 공제회 · 정촌(町村)의회의원 공제회	4호	지방의원가입기간과 후생연금피보험자기간의 중복기간을 확인하기 위해
	건강보험후생연금상실피보험자 파일	연금자금 운용자금	3호	대부조건의 심사를 위해
		후생연금기금 연합회	4호	후생연금기금이 행한 연금급부 및 연금상담을 원활하기 시행하기 위해
		도도부현(都道府)	4호	지방의원가입기간과 후생연금피보험자기간의 중복기간을 확인하기 위해

부 록

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
		県)의회 의원공제회·시의회의원공제회·정촌(町村)의회의원공제회		기 위해
	선원보험후생연금보험자 파일	연금자금운용기금	3호	대부조건의 심사를 위해
		(재) 선원보험회	4호	생활습관병 예방검진의 수급자격을 확인하기 위해
		도도부현(都道府県)의회 의원공제회·시의회의원공제회·정촌(町村)의회의원공제회	4호	지방의원가입기간과 후생연금피보험기간의 중복기간을 확인하기 위해
	국민연금피보험자 파일	연금자금운용기금	3호	대부조건의 심사를 위해
		국민연금기금연합회	4호	국민연금기금 가입자격을 확인하기 위해
		독립행정법인농업자연금기금	3호	국민연금과 농업자연금의 피보험자기록의 정합성 확인을 위해
	연금수급권자 파일	연금자금운용기금	3호	대부조건의 심사를 위해

부록 Ⅲ. 일본의 개인정보보호법 관련 자료

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
		독립 행정 법인 복지 의 료기구	3호	上同
		후생노동성보통성보험국국민건강보험과	3호	퇴직자의료제도대상자의 적절한 적용을 위해
		후생연금기금연합회	4호	후생연금기금이 행한 연금급부 및 연금상담을 원활하게 하기 위해
		국민생활금융공고	4호	대부조건의 심사를 위해
		오кина와진흥개발금융공고	4호	上同
	고용정보 파일	국가공무원공제조합연합회	4호	실업보험 및 고령자고용계속급부와의 병합조정을 위해
		지방공무원공제조합연합회	4호	上同
		일본사립학교진흥·공제사업단	4호	上同
		농림어업단체직원공제조합	4호	上同

부 록

행정 기관명	개인정보파일의 명칭	이용 · 제공처	근거 구분	이용 · 제공이유
	개호보험정보 파일	지방공무원공제조합연합회	4호	특별징수대상자의 확인을 위해
경제 산업성	자가용 전기공작물 데이터 베이스	자원에너지청전력시장장비과	3호	전력소매의 자유화대상인 수요가(需要家) 전기요금의 실태 등을 파악하기 위해 실시한 통계 보고조정법에 근거한 승인통계 조정에 이용하기 위해서이며, 또한 해당개인정보 파일의 처리 정보를 이용하는 이외에 조사대상의 객체정보를 파악하는 방법이 없기 때문에
국토 교통성	이륜자동차검사 파일	(재) 자동차검사등록협력회	4호	징세사무, 자동차의 안전확보 및 통계에 관하여
	건설건설터트 등록정보 파일	불특정 다수에게 열람	4호	등록업자의 업무내용을 공시, 보다 명확히 하여 발주자의 편의를 도모함과 동시에 일의 적정한 운영과 건전한 발달을 도모하기 위해
	지질조사사업자 등록정보 파일	上同	4호	上同
	보상건설터트 등록정보 파일	上同	4호	上同

(주) 근거구분 란의 『1호』는 법 제9조 제2항 제1호(본인의 동의 등), 『2호』는 동항 제2호(내부이용), 『3호』는 동항 제3호(행정기관 등에서의 제공), 『4호』는 동항 제4호(통계, 학술연구목적 등)을 각각 표시한다.

자료 5

개인정보 파일별 공개청구 현황

보유 기관	개인정보파일명칭	93 년도	94 년도	95 년도	96 년도	97 년도	98 년도	99 년도	00 년도	01 년도	02 년도	03 년도	04 년도
경찰청	운전자관리 파일	3			1				1			1	3
	선임경비원지 도교육책임자 및 선임 기계 경비업무관리 자 파일		1										
총무성	전기통신소비 자상담 파일												1
법무성	일본인출귀국 기록 마스터 파일	387	396	460	484	486	501	499	481	506	462	371	346
	외국인출입국 기록 마스터 파일	52	60	130	170	205	243	300	381	312	360	321	231
	사법시험 제2 차 시험 파일 (주)			6	5	3	3	3		9	89	612	204
국세청	세무사명부정 보 파일(세무 사명부 파일)			1			1			1			
	소득세확정납 세액 파일			1									
	소득세납세자 원부관리 파일			1									

부 록

보유 기관	개인정보파일명칭	93 년도	94 년도	95 년도	96 년도	97 년도	98 년도	99 년도	00 년도	01 년도	02 년도	03 년도	04 년도
	간주(みなし) 법인과세선택 자 파일			1									
	소비세신청이 력 파일						1						
	소비세신고· 결의사적(事績) 파일						1						
	소비세중간신 고사적(事績) 파일						1						
	한자 파일			1									
	소비세 파일			1									
	채권관리 파일			1									
	채권관리수신 인명 파일			1									
	연납수신인명 파일			1									
	미도래채권관 리 파일			1									
	원천징수의무 자 파일			1			1		1	1		1	
계		442	457	607	660	694	752	802	864	829	911	1,306	785

(주) 사법시험 제2차 시험파일은 2003년 12월 말까지는, 사법시험관리위원회(2004년 1월 1일 폐지)가 보유하였다.

Ⅲ-2. 일본 ‘개인정보보호설명회참가자의 설문
결과보고서(2008.3) : 소비자 인식 - 집계
결과표 -

1. 당신의 속성에 대해서 질문하겠습니다. 적합한 것을 선택하여, ○ 표시를 해주세요.

	인수	전체(%)
① 남성	5062	71.4
② 여성	1924	27.1
③ 무응답	105	1.5
합계	7091	100

【 연령 】	인수	전체(%)
① 10대	3	0.04
② 20대	488	6.9
③ 30대	1477	20.8
④ 40대	1869	26.4
⑤ 50대	1933	27.3
⑥ 60대	866	12.2
⑦ 70대 이상	392	5.5
⑧ 무응답	63	0.9
합계	7091	100

【 직업 】	인수	전체(%)
① 회사원	541	7.6
② 공무원	4066	57.3
③ 단체직원	850	12.0
④ 자영업·자유업자	219	3.1
⑤ 학생	3	0.04

부 록

【 직업 】	인수	전체(%)
⑥ 무직	620	8.7
⑦ 그 외	469	6.6
⑧ 무응답	323	4.6
합계	7091	100

【 속한 단체 】	인수	*전체(%)
① 자치회	1037	14.6
② 자주방재조직	477	6.7
③ 학교	1517	21.4
④ PTA 단체	294	4.1
⑤ 민생위원	924	13.0
⑥ 아동위원	434	6.1
⑦ 일반	559	7.9
⑧ 사업자	574	8.1
⑨ 지방공공단체직원	2244	31.6
⑩ 그 외	478	6.7

* 비율은 총 건수 7,091 명을 전체로 한 구성비

2-1. 당신이, 개인정보보호법에 기대하는 것은 무엇입니까? 해당하는 것 전부에 ○ 표시를 해주세요.

	인수	*전체(%)
① 모르는 사업자에게서 오는 권유전 화나 스팸메일을 제한하거나, 방지하는 것이 가능하다,	3561	50.2
② 자신의 개인정보가 납득할 수 있는 범위 내에서 이용된다.	2916	41.1
③ 자신의 개인정보에 관해서 간편한 절차로 공개 청구가 가능하다.	963	13.6
④ 사업자 종업자(從業者)의 열람책임 강화	1328	18.7

	인수	*전체(%)
⑤ 사업자가 보유하고 있는 개인정보의 안전관리책임 강화	3588	50.6
⑥ 정보의 누설이나 악용에 관해 벌칙 강화	3580	50.5
⑦ 기대하지 않는다	160	2.3
⑧ 그 외	73	1.0
⑨ 무응답	198	2.8

* 비율은 총 건수 7,091 명을 전체로 한 구성비

2-2. 개인정보보호법이 시행되어 어떠한 변화가 있었습니까 ? 해당하는 것 전부에 ○ 표시를 해주세요.

	인수	*전체(%)
① 자기자신의 개인정보 취급이 신중해졌다.	3227	45.5
② 사업자·단체의 개인정보 취급이 적절해졌다.	1309	18.5
③ 사회전체의 개인정보 취급이 적절해졌다.	646	9.1
④ 사회 전체적으로 개인정보에 관한 취급이 너무 신중해져서 불편해졌다.	4822	68.0
⑤ 특별한 변화는 없는 것 같다.	325	4.6
⑥ 무응답	113	1.6

* 비율은 총 건수 7,091 명을 전체로 한 구성비

2-3. 개인정보보호법이 시행되어 곤란한 것은 무엇입니까 ? 해당되는 것 전부에 ○ 표시를 해주세요.

부 록

	인수	*전체(%)
① 명부, 연락망의 작성이 중지되었다.	2469	34.8
② 사진, 비디오 등의 촬영이 어려워졌다.	934	13.2
③ 일, 사업 활동의 사무 절차가 번거로워졌다.	2156	30.4
④ 일, 사업 활동이 어려워졌다.	1879	26.5
⑤ 사고 시 등 긴급한 상황에도 개인정보보호를 앞세워 개인정보를 가르쳐 주지 않는 일이 있다.	1535	21.6
⑥ 걸핏하면 개인정보라고 말한다	4071	57.4
⑦ 그 외	120	1.7
⑧ 무응답	433	6.1

* 비율은 총 건수 7,091 명을 전체로 한 구성비

2-4. 권유전화나 스팸메일에 관해 어떻게 생각합니까 ? 해당하는 것 하나에 ○ 표시를 해주세요.

	인수	*전체(%)
① 모르는 사업자에게서의 권유전화나 스팸메일은 금지 되었으면 좋겠다.	4793	67.6
② 모르는 사업자에게서의 권유전화는 금지되었으면 좋겠지만, 스팸메일은 상관없다.	1021	14.4
③ 모르는 사업자에게서의 권유전화는 상관없지만, 스팸메일은 금지했으면 좋겠다.	40	0.6
④ 모르는 사업자에게서의 권유전화나 스팸메일, 차후 거절할 수 있다면 상관없다.	782	11.0

	인수	*전체(%)
⑤ 모르는 사업자에게서의 권유전화나 스팸메일은 와도 상관없다.	122	1.7
⑥ 그 외	41	0.6
⑦ 무응답	292	4.1
합계	7091	100

2-5. 개인정보보호법으로 인하여 사업자에게 자신의 개인정보를 어떻게 입수하였는지 대답하게 하는 것이 어려워졌는데, 이것에 대해 어떻게 생각하십니까? 해당하는 것 하나에 ○ 표시를 해주세요.

	인수	전체(%)
① 어디서 자신의 개인정보를 입수하였는지, 알 수 있었으면 좋겠다.	4469	63.0
② 어디서 자신의 개인정보를 입수하였는지, 알 수 있으면 좋겠지만 어려울 거라고 생각한다.	2288	32.3
③ 특별히 생각하지 않는다.	191	2.7
④ 무응답	143	2.0
합계	7091	100

2-6. 자신이 모르는 곳에서 의미 없이 자신의 개인정보가 유통되는 것에 관하여 어떻게 생각하십니까? 해당하는 것 하나에 ○ 표시를 해주세요.

	인수	*전체(%)
① 자신이 동의했던 곳만 개인정보가 유통되었으면 좋겠다.	4460	62.9

부 록

	인수	*전체(%)
② 개인정보의 유용성에서 보면, 동의가 없이 개인 정보가 유통되어도 특별히 문제 없다.	588	8.3
③ 유통하는 것은 상관없지만, 자신의 의사로 이용을 멈추었으면 좋겠다.	1848	26.1
④ 무응답	195	2.7
합계	7091	100

2-7. 개인정보가 누설되는 문제에 관하여, 개인정보보호법이 얼마나 도움이 되고 있다고 생각합니까? 자신의 사고방식에 가까운 것을 한 가지 골라 ○ 표시를 해주세요.

	인수	전체(%)
① 사업자가 재빠르게 대응하는 등 누설 방지에 도움이 되고 있다.	1856	26.2
② 누설 문제가 여전히 발생하고 있기 때문에, 도움이 되지 않고 있다.	2214	31.2
③ 누설을 확실히 방지하는 것은 법률로서는 불가능 하다고 생각한다.	2661	37.5
④ 무응답	360	5.1
합계	7091	100

2-8. 개인정보보호법에 근거하여 자신의 정보에 관해 공개 청구를 한 적이 있습니까? 해당하는 것을 한가지 골라 ○ 표시를 해주세요.

	인수	*전체(%)
① 공개청구 한 적이 있다.	107	1.5

	인수	*전체(%)
② 공개청구를 하려고는 했으나, 방법을 모른다.	803	11.3
③ 공개청구의 필요성을 느끼지 못했다.	5965	84.1
④ 무응답	216	3.0
합계	7091	100

2-9. 계약서 등에는 「개인정보의 취급에 관하여」 등의 기록사항이 있으며, 개인정보의 이용목적, 제3자 제공 등에 관해 자세히 쓰여져 있는 항목도 있습니다. 이것을 읽은 적이 있습니까? 또한 그 내용을 이해할 수 있었습니까? 해당하는 것 하나를 골라 ○ 표시를 해주세요.

	인수		인수	전체(%)
① 자세히 읽는다.	901	(①에 ○를 표시한 분은, 아래의가부터 라에도 ○ 표시를 해주세요)	/	12.7
		가 잘 알고 있다	140	2.0
		나 대부분 알고 있다	641	9.0
		다 잘 모른다	115	1.6
		라 전혀 모른다	5	0.1
② 읽은 적은 있다	4292	(②에 ○를 표시한 분은 아래의가부터 라에도 ○ 표시를 해주세요)	/	60.5
		가 잘 알고 있다	203	2.9
		나 대부분 알고 있다	2958	41.7

부 록

	인수		인수	전체(%)
		다 잘 모른다	1114	15.7
		라 전혀 모른다	17	0.2
③ 읽은 적이 없다	1239			17.5
④ 『개인정보 취급에 관하여』등의 항목이 있다는 자체를 모른다	121			1.7
⑤ 무응답	538			7.6
합계	7091			100

2-10. 당신은, 자신에 관한 정보의 취급에 관하여 특별히 신경을 쓰고 있는 점이 있습니까? 해당하는 곳에 전부 ○ 표시를 해주세요.

	인수	*전체(%)
① 인터넷에서 자신의 개인정보를 직접 발신하지 않는 등, 사업자에게 정보를 제공하는 것은 필요최소한으로 제한한다.	4064	57.3
② 성명·주소 등 개인정보를 기입할 필요가 있는 양케이트 등에는 최대한 대답하지 않는다.	3663	51.7
③ 개인정보 관리에 별로 신경을 쓰지 않는 상품이나 서비스를 이용하지 않는다.	2818	39.7
④ 개인정보 제공을 요구받았을 때 개인정보의 내용이나 이용목적이 자신의 뜻에 맞지 않는 경우 그 상품이나 서비스를 이용하지 않는다.	2898	40.9
⑤ 사업자가 보유하고 있는 자신의 개인정보의 내용을 확인한다.	381	5.4

	인수	*전체(%)
⑥ 사업자의 개인정보에 대한 정책 등을 확인한다	694	9.8
⑦ 프라이버시 마크 등 개인정보 보호 대책에 관한 인증 등의 취득 유무를 확인한다.	469	6.6
⑧ 특별히 신경 쓰고 있는 점이 없다	458	6.5
⑨ 그 외	37	0.5
⑩ 무응답	290	4.1

* 비율은 총 건수 7,091 명을 전체로 한 구성

2-11. 개인정보 상담 창구가 각 지자체, 또는 인증받은 개인정보보호단체 등에 설치되어 있다는 것을 알고 있었습니까?

	인수	전체(%)
알고 있다	3815	53.8
몰랐다	3015	42.5
무응답	261	3.7
합계	7091	100

2-12. 당신은 지금까지 개인정보 상담 창구에서 상담받은 적이 있습니까? 해당하는 것에 전부 ○ 표시를 해주세요.

	인수	*전체(%)
① 지자체의 상담창구에서 상담받은 적이 있다.	150	2.1
② 국민생활 센터의 상담창구에서 상담받은 적이 있다.	88	1.2

부 록

	인수	*전체(%)
③ 인증받은 개인정보 보호단체가 설치한 창구에서 상담받은 적이 있다.	14	0.2
④ 해당 사업자의 개인정보 상담창구에서 상담받은 적이 있다.	33	0.5
⑤ 상담하고 싶은 것이 있었으나, 상담받은 적은 없다.	1014	14.3
⑥ 상담하고 싶은 것이 없으므로, 상담받은 적이 없다.	5348	75.4
⑦ 무응답	479	6.8

* 비율은 총 건수 7,091 명을 전체로 한 구성비

Ⅲ-3. 일본 개인정보보호에 관한법률시행령의 일부를 개정하는 정령(2008년정령제166호) 신구대조

개 정 전	개 정 후
<p>제 2 조(개인정보취급사업자로부터 제외되는 자) 법제2조제3항 제5호 정령에서 정한 자는, 그 사업용으로 제공하는 개인정보 데이터베이스 등을 구성하는 개인정보에 의해 식별된 특정 개인의 수(당해개인정보데이터 등의 전부 또는 일부가 개인작성에 관한 개인정보데이터베이스 등에 개인정보로서 성명 또는 주소 혹은 거소(지도상 또는 전자계산기의 영상면에 있어서 주소 또는 거소의 소재를 지를 보인 표시를 포함한다) 혹은 전화번호만이 포함된 경우에, 이것을 편집 또는 가공하는 것 없이 그 사업용으로 제공한 때에는, 당해 개인정보데이터 등의 전부 또는 일부를 구성하는 개인정보에 의해 식별된 특정의 개인 수를 제외)의 합계가 과거 6월 이내의 어느 날도 5천을 넘지 않는 자로 한다.</p>	<p>제 2 조(개인정보취급사업자로부터 제외되는 자) 법제2조제3항 제5호의 정령에서 정한 자는 그 사업용으로 제공하는 개인정보 데이터베이스 등을 구성하는 개인정보에 의해 식별된 특정 개인의 수(당해 개인정보데이터베이스 등의 전부 또는 일부가 타인의 작성에 관한 개인정보데이터베이스 등이며, 다음 각 호의 어딘가에 해당하는 것을 편집하고, 또는 가공하지 않고 그 사업의 용에 제공할 때에는, 당해 개인정보 데이터베이스 등의 전부 또는 일부를 구성하는 개인정보에 의해 식별된 특정의 개인 수를 제외)의 합계가 과거 6월 이내의 어느 날도 5천을 넘지 않는 자로 한다.</p> <p>① 개인정보로서 다음 기재한 것을 포함하는 것.</p> <p>가. 성명 나. 주소 또는 거소(지도상 또는 전자계기의 영상면에 있어 주소 또는 거소의 소재 장소를 표시를 포함한 것) 다. 전화번호</p> <p>② 불특정 또는 다수의 자에 판매할 것을 목적으로 발행되거나 또는 다수 자에 의해 수시로 구입할 수 있는 것 또는 있었던 것</p>

Ⅲ-4. 개인정보보호에 관한 기본방침(2008.4.24)

개인정보보호에 관한 기본방침(2008년4월25일 일부변경)

일본 정부는 개인정보 보호에 관한 법률(2003년법률제57호) 제7조 제1항 규정에 근거하여 “개인정보 보호에 관한 기본방침”(이하, 기본방침)을 책정 하였다. 기본 방침은 개인정보의 보호에 만전을 기하기 위하여 개인정보 보호에 관한 시책의 추진 기본적인 방향 및 국가가 강구해야 할 조치를 정하면서 지방공공단체, 개인정보취급사업자 등이 해야할 조치의 방향성을 제시하고, 정부로서 민관(民官)의 폭넓은 주체(主體)가 이 기본방침에 따라 개인정보 보호를 위한 구체적인 실천에 힘쓰도록 하고 있다.

본 기본 방침은 국민생활심의회 개인정보보호심의회를 통하여 연구 검토 되어 2008년 4월 25일 일부 수정되었다.1) 그 수정 내용을 중심으로 일본정부가 2008년 4월 25일에 정한 개인정보 보호에 관한 기본 방침을 정리 한다.

*수정한 부분에 밑줄.

1. 개인정보에 관한 시책의 추진에 관한 기본적인 방향

(1) 법제정의 배경

경제·사회정보화 추진에 따라 민관을 통하여 컴퓨터 네트워크를 이용하여 대량의 개인정보가 처리 되고 있다, 이러한 개인정보의 취급은 앞으로 더욱 확대할 것으로 예상되지만, 개인정보는 그 성질상 일단

1) 閣議決定、『個人情報保護の保護に関する基本方針』(平成20年4月25日一部変更) .

잘못 취급되면, 개인에게 되돌릴 수 없는 피해를 줄 우려가 있다.

실제로 사업자로부터 고객정보 등의 대규모 유출과 개인정보 매매 사건이 다발하고, 사회문제화 되고 있다. 이에 따라 국민의 프라이버시에 관한 불안도 높아지고 있고, 안전관리를 중심으로 기업 개인정보보호의 노력을 요구하는 목소리도 높아지고 있다.

국제적으로는 1970년부터 구미제국에서 개인정보보호에 관한 법제정비가 추진되고 1980년에는 각국 규제 내용의 조화를 도모하는 관점에서 경제협력개발기구(OECD) 이사회권고에 “프라이버시보호와 개인데이터의 국제유통에 대하여 가이드라인”이 제시되었다. 이후 각국에서 급속히 개인정보보호법제의 정비가 추진되었고, OECD가맹국 대다수가 공적부문 및 민간부문의 쌍방을 대상으로 개인정보보호법제를 갖게 되었다. 기업 활동 등의 글로벌화가 추진 중, 일본도 국제적으로 정합성을 갖춘 법제의 정비와 운용이 요구된다.

이러한 상황아래 개인정보 보호의 현주소와 정보의 자유를 시작으로 한 헌법상의 요청과 조화에 관한 다양한 국민적인 논의를 거쳐, 누구라도 안심하고 고도정보통신사회의 편의를 향유하기위한 제도적 기반으로 민관을 통한 개인정보보호의 기본이념 등을 정한 기본법에 상당하는 부분과 민간사업자가 준수해야할 의무 등을 정한 일반법이 2003년5월에 성립, 공포되어 2005년 4월 1일에 전면 시행되었다. 또 법 취지를 따라 공적부문에 상응하는 개인정보보호 규정을 정한 “행정기관이 보유하는 개인정보 보호에 관한법률”(2003년법률제58호, 이하 “행정기관개인정보보호법”이라 함), “독립행정법인등이보유하는개인정보보호에관한법률”(2003년법률제59호, 이하 “독립행정법인등개인정보보호법”이라 함)등 관련4법이 함께 성립·공포되어 2005년 4월 1일에 시행되었다.

(2) 법의 이념과 제도 구상

법률3조는 개인정보가 개인 인격과 밀접한 관련을 갖은 것이고, 개인이 “개인으로 존중된다”고 정하고 있는 일본 헌법 제13조 아래 신중히 취급되어야만 하는 것을 의미하며, 개인정보를 취급한 자는 그 목적과 양태를 묻지 않고 이러한 개인정보의 성격과 중요성을 충분히 인식하고, 그 적당한 취급을 도모하지 않으면 안 된다는 기본이념을 나타내고 있다. 관계 각 주체는 이 기본이념을 충분히 따르면서 이하에 제시하는 제도 구상을 기본으로 개인정보 보호에 힘쓸 필요가 있다.

① 개인정보 보호와 유용성의 배려

법은 경제, 사회 정보화 추진에 따라 개인정보 이용이 확대 되고 있는 중에, 법제3조의 기본이념에 따라 프라이버시 보호를 포함한 개인 권리이익을 보호하는 것을 목표로 하며, 한편 정보통신기술 활용에 의한 개인정보의 다양한 이용이 개인 유저(user)의 사업에 정확한 반영과 신속한 서비스 등의 제공을 실현하고 사업활동 면에서도, 국민생활 면에서도 빼놓을 수 없는 것이 되었다는 것을 배려하고 있는 것이다.

개인정보 보호와 유용성에 관한 본법의 구상은 실제 개인정보 취급에 있어서도 충분히 근거를 둘 필요가 있고, 개인정보 보호에 만전을 기하는 것이 개인정보 이용에 관한 사회의 신뢰를 높이고, 국민 개개인이 그 편익을 향수할 수 있는 건전한 고도정보통신사회 실현을 가능하게 하는 것이다.

② 이른바 “과민반응”에의 대처

작금 프라이버시 의식 고양과 개인정보 취급의 미숙을 이유로, 사회적 필요성이 있음에도 불구하고 법규정이상으로 개인정보 제공을 꺼리거나 운용상작성가능한 명부의 작성을 그만두게 되는 등 이른바

“과잉반응”이 발생되고 있다.

국민생활심의회는 “개인정보보호에 관한 총괄의견”(2007년6월29일)에서 법의 구체적인 내용의 광고·계발(啓發)등, 이른바 “과잉반응”대책에 만전을 기하도록 요구하고, 정부도 개인정보보호관련성청 관련 회의를 추진하여, 앞으로 대책을 결정(개인정보시책의 앞으로 추진에 대하여(2007년6월29일 결정)하고 시행하고 있다.

일본정부는 2의(4)와 같이, 사업자 및 국민에 대한 광고·계발(啓發)을 적극적으로 하려 한다. 또 각 지방공공단체에서는 3의(2)의1에 있는 것 같이, 주민에게 주지하기 위하여 적극적인 광고활동에 힘쓸것이 촉구된다.

또 이른바 “과잉반응”이 발생한 배경에는 개인정보에 의해 식별된 특성의 개인(이하, 본인이라 함)이 스스로 개인정보의 취급에 불안을 느끼고 있는 것도 하나의 이유로 생각되기 때문에 법의 적절한 운용 등에 의해 개인정보의 적절한 취급을 도모해 나갈 필요가 있다.

③ 각사업자의 자율적인 대처와 각 주체의 연대

고도정보통신사업에서는 업종을 묻지 않고 정보통신기술을 활용한 대량 다양한 개인정보가 넓게 이용되게 되고 있다. 이 때문에 법은 개인정보를 사업용에 제공하는 자를 넓게 인정하고 개인정보를 취급하는 자에게 각각의 사업 등의 분야의 실정에 따라, 자율적으로 개인정보의 보호에 만전을 기하는 것을 기대하고 있다. 또, 이러한 사업자의 자율적인 구조에 관하여, 국가의 행정기관 등의 지원이 중요하고, 법은 국가가 사업자등에 지원, 고충처리를 위한 조치를 강구해야만 하는 것을 정하면서 사업자 등을 소관 하는 관청(이하 ‘각 관청’이라 함)이 각 사업등분야에서 개인정보 취급에 대하여 권한과 책임을 갖는 구조를 채용하고 있지만, 이러한 다층적인 개인정보 보호를 위한 조치가 종합적으로 실효성을 올려 가기 위해서는 사업자, 지방공공단

체, 국가의 행정기관 등이 상호협력하고 연대를 확보해 나가는 것이 중요하다.

(3) 국제적인 협조

개인정보 보호에 있어 국제적인 구조로서 1980년 OECD프라이버시 가이드라인에서, 이른바 8원칙이 나타나 있고, 그 원칙이 이후 국제적인 구조와 각국의 대처방식에 기본이 되고 있다. OECD프라이버시 가이드라인에서는 8원칙의 각국 내에서 실시해 있어 상세는 각국에 맡겨져 있지만, 개인정보취급사업자의 의무에 관한 법제4장의 규정은 일본의 실정에 비추어 8원칙을 구체화한 것이고, 앞으로 법 및 기본 방침에 따른 대처에 의해 그 실효성을 확보하는 것이 중요하다.

또, 법의 룰 및 기본방침에 근거하여 개인정보보호의 대처를 함에 있어, OECD를 시작으로 아시아태평양경제협력(APEC), 구주연합(EU) 등 다양한 곳에서 추진되고 있는 국제적인 대응을 따라, 프라이버시 보호에 관한 국경을 초월한 집행 협력 등, 국제적인 협조를 도모해가면서, 일본의 법제도에 대하여도 국제적인 이해를 구해가는 것이 중요하다.

2. 국가가 강구해야 하는 개인정보 보호를 위한 조치에 관한 사항

(1) 각 행정기관이 보유하는 개인정보의 보호 추진

국가의 행정기관이 보유하는 개인정보 보호에 대하여 행정기관개인정보보호법을 적절히 운용하기 위해 동법 운용의 통일성·법적합성을 확보하는 입장에서 총무성은 ‘행정기관이 보유하는 개인정보의 적절한 관리를 위한 조치에 관한 지침(2004년 9월 14일총무성행정관리국장통지)’를 책정하고 개인정보의 적절한 관리를 철저히 해 왔고, 계속 각 행정기관 및 국민에 대하여 판플렛 배포와 설명회 실시 등을 하여 동법을 주지(周知) 시키며, 시행상황 개요를 공표하는 등 국민에 대하

여 정보제공을 하는 제도의 운용의 투명성을 확보한다.

또 각 행정기관은 총무성이 책정한 지침 등을 참고로 하여, 그 보유 개인정보의 취급 실정에 따른 개인정보의 적절한 관리에 관한 규정 등을 정비를 하고 있는 것이 있지만, 계속 ①직원에의 교육연수, ②적절한 정부 시큐리티 시스템 정비, ③관리체제와 국민에 대한 상담창구의 정비, ④개인정보의 적절한 관리를 도모하기 위하여 강구한 조치 등에 관한 정보 제공을 한다.

또 국가의 행정기관에서 개인정보 제공에 대하여 행정기관개인정보 보호법상 필요성이 인정되는 경우에는 개인정보 공표 등은 가능하며, 정보제공 의의(意義)에 따라 동법의 적절한 운용을 도모하도록 한다.

(2) 정부전체의 제도의 통일적 운용을 위한 지침

① 개별 사안이 발생한 경우 내각부와 각 성청의 연대

대규모 개인정보 누설 등 개별 사안이 발생한 경우 각 성청은 각 사업 등 분야에서 개인정보 적정한 취급을 확보하기 위하여 필요한 정보의 수집에 노력하면서 해당 개별사안의 피해 확대와 사회적 영향을 근거하여 신속히 법 제4장의 규정에 근거한 조치 등을 검토 한다.

또 내각부는 개인정보보호관계성청연락회의도 활용하면서 정보제공 등의 각 성청의 협력을 얻어 개별 사안에 대하여, 대응사례를 축적·정리를 하면서 필요한 정보를 각 성청에 제공하고, 개인정보 보호를 위한 시책의 충실에 이바지 하도록 한다.

② 공관(共管)의 경우 주무대신의 연대 모습

개인정보취급사업자가 다각적으로 사업을 하고 있는 경우와 그 취급 개인정보에 고용관리에 관한 것을 포함하고 있는 경우 등에 있어, 특정 사안에 대하여 복수의 주무대신이 공관하는 경우를 생각 할 수 있다. 이러한 사안에서 사업자의 부담경감 및 각 성청 간에 복합적인

제도 운용 확보 관점으로, 공동관리 하게 되는 각 성청간에 충분한 연대를 도모하고 권한을 행사하는 것을 기본으로 한다.

③ 소관이 명확하지 않은 경우의 주무대신 지정

복합적인 사업의 창출 등에 의해, 개인정보취급사업자가 행하는 사업을 소관 하는 대신 등이 명확하지 않은 경우에도 생길 수 있기 때문에, 법제36조는 내각총리대신이 주무대신을 지정할 수 가 있다. 이 경우 내각부는 각 성청의 소관사무에 비취 관계가 깊은 성청을 조회한 후 특정 또는 필요한 경우에는 관계성청연락회의를 활용하여 지정을 하는 것으로 한다.

④ 각 성청에서 창구의 명확화·직원에게 교육연수

각 성청은 타 성청, 지방공공단체와 연락·조정을 강화하면서, 고충상담기관으로부터 정보를 수집하고 상담 등에 응하기 위하여, 법에 관한 창구를 명확히 한다. 당해 창구는 성청내 사업 등 관리부국으로부터의 상담에 응하면서 연수 등에 의해 직원에게 지식 보급을 한다.

⑤ 법 시행의 상황의 내각부에의 보고와 공포

관계행정기관은 법제53조제1항 규정에 근거, 매년도 법 시행상황으로서 법제4장에 근거한 보고의 징수·조언 등의 규정의 실시 상황 외에 사업 등 분야에 있어 가의드라인 등 정책 및 시행 상황, 인정개인정보보호단체의 고충 처리 등의 대처상황, 개인정보취급사업자로부터의 개인정보누설 등의 상황에 대하여 내각부에 보고하는 것으로 한다.

내각부는 관계행정기관으로부터의 보고를 총괄하여, 그 개요를 공표하며 국민생활심의회에 보고하는 것으로 한다.

(3) 분야마다 개인정보 보호 추진에 관한 방침

① 각 성청이 소관 하는 분야에 있어 강구해야할 시책

개인정보 보호에 관하여 법의 시행 전에도 사업자 취급 개인정보의 성질과 이용방법 등의 실태를 근거하여 사업자분야별 가이드 등에 근거하여 자주적인 대응을 추진하여 왔다.

이러한 자주적 대처는 법의 시행 후에도, 법이 정하는 룰의 준수를 보아, 개인정보 보호 실효를 높이도록 계속 기대되며 존중되고 또 촉진될 필요가 있다. 이 때문에 각 성청은 법의 개인정보 취급에 관하여 룰이 각 분야에 공통하는 필요최소한의 것인지를 중심으로 각각 사업 등의 분야의 실정에 맞는 가이드라인 등의 책정·재검토를 하면서 사업자단체 등이 주체적으로 정한 가이드라인의 책정 등에 대하여도 정보 제공, 조언 등의 지원을 하는 것으로 한다.

또 악질적인 사업자의 감독을 위해, 개인정보취급사업자에 대하여 보고의 징수 등의 주무대신의 권한 등에 대하여 이를 적절히 행사하는 등 법의 엄격한 적용을 도모하도록 한다.

② 특히, 적정한 취급을 확보해야하는 개별분야에 있어 강구되어야할 시책

개인정보의 성질과 이용방법 등으로부터 특히 적정한 취급의 엄격한 실시를 확보할 필요가 있는 분야에 대하여는 각 성청에서 개인정보를 보호하기위한 각별한 조치를 각 분야(의료, 금융·신용, 정보통신 등)마다 강구하도록 한다.

(4) 광고·계발, 정보제공 등에 관한 방침

법은, 개인정보를 이용하는 사업자에 대하여 사업의 분야, 이용 목적을 묻지 않고 폭넓게 개인정보 취급에 관한 의무를 과하면서 본인이 개인정보취급사업자에 대하여 스스로 개시·정정·이용정지를 요

구하는 등, 사업자 개인정보 취급에 관여해온 구상을 채용하고, 개인정보의 보호 실효를 기대하기 위하여, 사업자 및 국민에 대하여 법제도의 주지(周知)를 철저히 하는 것이 매우 중요하다.

이 때문에, 내각부 및 각 성청은, 계속 사업자 및 국민에 충분한 정보제공이 행해지도록 인터넷 활용, 포스터의 게시, 판플렛의 배포, 설명회의 실시 등 다양한 매체를 사용하여, 광고·계발(啓發)에 적극적으로 힘쓰도록 한다. 이때 개인정보의 취급에 관심 등에 대하여, 세대간, 사업 분야에 따라 차이가 있으므로 매체의 선정 등도 배려하여 매우 세부적인 대응을 하면서, ‘개인정보의 유용성을 배려하면서, 개인의 권리이익을 보호하는 것(법제1조)’를 목적으로 하는 법의 구상이 각 주제에 의해 실제 개인정보 취득에서 충분 반영되도록 한다.

특히 이른바 ‘과잉반응’에 대한 대처의 일환으로 ‘개인정보보호정책의 금후 추진에 대하여’(1의 (2)의 ②참조)를 근거하여 광고·계발(啓發) 등을 더욱 적극적으로 하도록 한다.

(5) 개인정보 보호에 관한 국제적인 구조에의 대응

OECD에는 프라이버시법 집행이 국경을 초월한 과제로 검토되고, APEC는 국경을 초월한 프라이버시 규칙의 구축과 정보공유, 조사·집행의 국경을 초월한 협력 과제가 검토되고 있다. 이러한 OECD, APEC에서의 대응과 EU등에서 추진되고 있는 대응에 따라, 사업자의 자율적인 대처를 존중하는 일본 법제도(1의 (2)의 ③참조)와의 적합성에 유의하며, 1의 (3)에 근거하여 국제적인 협조 관점으로, 일본에 필요한 대응을 검토해 나간다. 또 ‘프라이버시보호법의 집행에 관한 국경을 초월한 협력에 관한 OECD권고’(2007년 6월 12일 채택)에 근거, 내각부는 각 성청과 협력하고 필요한 대응·조치를 검토한다.

3. 지방공공단체가 강구해야할 개인정보 보호를 위한 조치의 기본적인 사항

(1) 지방공공단체가 보유하는 개인정보 보호 추진

지방공공단체가 보유하는 개인정보 보호대책에 대하여는 법제11조 제1항의 취지에 따라, 개인정보의 보호에 관한 조례의 제정에 힘쓸 필요가 있다. 또 이미 조례를 제정하고 있는 단체에서도 소요(所要)를 재검토할 것이 요구된다.

조례 제정 또는 재검토에 있어서, 법 및 행정기관개인정보보호법 등의 내용을 따르면서 이른바 매뉴얼처리에 관한 개인정보를 보호 대책으로 하는, 행정기관개인정보보호법을 참고하면서, 사무 특성에 배려하여 대상기관의 현황 자기정보 개시·정정·이용정지 등의 본인관여의 구조를 충실·적절한 고충처리와 불복신청제도 등의 구제조치의 정비, 외부위탁에 관한 개인정보 보호초지의 정비, 개인정보 누설 등에 관한 특칙의 검토, 이른바 ‘오프라인금지규정’의 재검토 등의 사항에 대하여 유의할 것이 요구된다.

또 이른바 ‘과잉반응’이 일부에서 보여짐에 따라 지방공공단체에서도 법의 취지에 따라, 조례의 적절한 해석·운용을 하는 것이 요구된다.

(2) 광고·계발(啓發)등 주민·사업자에의 지원의 모습

① 광고·계발 등 주민·사업자에의 지원 모습

개인정보보호 추진에 있어 주민·사업자에 가까운 행정을 맡는 지방공공단체의 역할은 중요하며, 법에서 구간내의 실정에 따라 주민·사업자에의 지원과 고충 처리의 알선 등에 대하여 필요한 조치를 강구할 노력을 하지 않으면 안 되는 것으로 되어 있다.

특히, 법의 적절한 정착을 향하여 각 지방공공단체에서는, 개인정보의 이념과 구체적인 구조 등을 주민 등에 주지하기위하여 적극적인 광고활동에 힘쓰면서, 구역 내 사업자 등의 주체적인 대처를 촉진하기위하여, 사업자로부터의 상담 등에 적절히 대응하는 것이 요구된다.

또 개인정보의 취급에 관한 사업자와 본인 간의 룰에 대하여 국가의 입법과 병행하거나 선행하여 지방공공단체에서 검토되어 일부에서 이미 조례의 제정 등에 의해 실시되고 있는 것이다. 이러한 지방공공단체의 대응은 구역의 특성에 따른 조치로서 중요하지만, 그 운용은 법과 각성청의 가이드라인 등과의 적합성에 배려할 필요가 있다. 또 지방공공단체가 그 실정에 따라 강구하려하는 조치에 대하여, 사업자 등의 활동이 전국의 광역에 걸친 것이 있을 수 있음을 고려하여, 타 지방자치단체와의 연대에 유의하면서 특히 사업자에게 새로운 의무를 과하게 될 경우에는 당해 지방자치단체의 구역 특성과 조례·규칙의 내용 등을 충분히 설명하고, 이해를 구하는 것이 필요하다.

② 지방공공단체의 부국간의 상호연대

지방공공단체는 법의 시행에 관하여 스스로 보유할 개인정보 보호, 그 구역내의 사업자 등에의 지원, 고충 처리의 알선 등, 게다가 법제 51조 및 영제11조의 규정에 의해 주무대신의 권한을 행사하는 것 까지 광범하고 다양한 시책이 실시되고 있다. 지방공공단체에는 이러한 다양한 시책은 개인정보 보호에 관한 조례의 소관부국, 주민으로부터 고충의 상담을 맡은 부국, 각 사업·사업자의 진흥·지원을 맡은 부국등상당수의 부국에 걸친 것이 고려되지만, 개인정보에 관한 주민의 권리의익의 보호 실효성을 확보하기 위하여 광범위한 실책이 일체적·종합적으로 강구되도록 관계부국이 상호 충분한 연대를 강구할 필요가 있다. 또 사업자들이 상담과 주민으로부터의 고충 등의 상담 편리성의 관점으로부터 연대체제의 확보와 함께, 관계부국간의 역할

분담과 창구를 분명히 하여, 이를 공표하는 것 등에 의해 주지하는 것이 요망된다.

(3) 국가·지방자치단체의 연대 모습

개인정보취급사업자에 대하여 보고의 징수 등의 주무대신의 권한에 대하여, 법제51조 및 영제11조제1항이 정한 바에 의해 지방공공단체가 그 사무를 처리하도록 되어 있지만, 지방공공단체의 구역을 걸쳐 사업자가 활동하고 있는 경우 등에 있어 지방공공단체가 충분히 사업자의 사업 활동을 파악하는 것이 어렵다는 것도 고려해야 된다. 이 때문에 지방공공단체의 각 성청은, 기본방침에 근거하여 각 창구를 활용하고 충분한 연대를 도모하고 지방자치단체는 각 성청에 필요한 정보의 제공 등의 협력을 구하면서, 각 성청은 필요한 경우에는 영제11조제3항에 근거 스스로 권한을 행사하도록 한다.

또 법제도에 대하여 광고·계발(啓發), 고충의 상담 등의 업무에 대하여도, 주민과 사업자 등에 혼란이 생기지 않도록, 국가와 지방공공단체가 서로 협력하는 것이 중요하며, 이를 위하여 내각부, 각 성청 및 독립행정법인국민생활센터는 광고자료와 고충처리 매뉴얼 등의 정보 제공을 도모하면서, 각 창구의 활용에 의해 개별 상담사례로부터 얻은 식견을 축적하고 그 공유를 도모하도록 한다.

4. 독립행정법인 등이 강구해야 하는 개인정보 보호를 위한 조치에 관한 기본적인 사항

독립행정법인 등이 보유하는 개인정보 보호에 관하여 독립행정법인 등개인정보보호법을 적절히 운용하기위하여, 동법의 운용의 통일성·법적합성을 확보하는 입장에 있는 총무성은 ‘독립행정법인 등이 보유하는 개인정보의 적절한 관리를 위한 조치에 관한 방침’(2004년9월14일총무성행정관리국장통지)를 책정하고, 개인정보의 적절한 관리를 철

저히 할 것을 계속하고, 각 행정기관, 독립행정법인등 및 국민에 대하여 판플렛의 배포와 설명회의 실시 등을 행한 동법의 주지(周知)를 도모하면서, 시행상황의 개요의 공포 등 국민에 대하여 정보제공을 행한 제도 운용의 투명성을 확보한다.

또 각행정기관은 소관 하는 독립행정법인 등에 대하여 그 업무운영에 있어 자주적이고 충분히 배려하면서, 필요한 지도, 조언, 감독을 한다. 독립행정법인 등은 총무성이 책정하는 지침 등을 참고하고, 그 보유하는 개인정보 취급의 실정에 따라 개인정보의 적절한 관리에 관한 규정 등의 정비를 행하고 있는 것이 있지만, 계속, ① 직원에 교육연수, ② 적절한 정부시큐리티의 정비, ③ 관리체제와 국민에 대한 상담창구의 정비, ④ 개인정보의 적절한 관리를 도모하기 위하여 강구한 조치 등에 관한 정보 제공을 한다.

또 독립행정법인 등에 있어서의 개인정보 제공에 대하여는 독립행정법인등개인정보보호법 상, 필요성이 인정되는 경우는 개인정보의 공포 등은 가능하고, 정보제공의 의의를 따르면서 동법의 적절한 운용을 도모하도록 한다.

5. 지방독립행정법인이 강구해야하는 개인정보 보호를 위한 조치에 관한 기본적인 사항

지방독립법인에 있어 개인정보 보호에 대하여 지방공공단체는 법제 11조제2항에서 필요한 조치를 취하도록 요구되고 있다. 이에 따라 각 지방공공단체는 그 설립에 관한 지방독립행정법인의 성격 및 업무내용에 따라 각 단체가 제정하는 개인정보보호조례에 있어 소요(소요) 규정을 정비하는 등, 적절한 개인정보 보호조치가 강구되도록 힘쓸 것이 요구된다.

6. 개인정보취급사업자 등이 강구해야하는 개인정보 보호를 위해 조치에 관한 기본적인 사항

(1) 개인정보취급사업자에 관한 사항

개인정보취급사업자는 법의 규정에 따르는 외에 2의(3)의 ①각 성청의 가이드라인 등에 따라, 개인정보 보호에 대하여 주체적으로 힘쓸 것이 기대 되고 있는바, 사업자는 계속 체제의 정비 등에 적극적으로 힘쓸 것이 요구된다. 각 성청 등에 있어 가이드라인 등의 검토 및 각 사업자의 대처에 있어서 특히 이하의 점이 중요하다고 생각된다.

① 사업자가 한 조치의 대외적 명확화

사업자가 개인정보보호를 추진함에 있어 생각과 방침(이른바, 프라이버시 폴리시, 프라이버시 도큐먼트 등)을 책정·공표하는 것에 의해 개인정보를 목적 외에 이용하지 않을 것과 고충처리에 적절히 힘쓸 것 등을 선언하면서, 사업자가 관련법령 등을 준수하고, 이용목적의 통지, 공표, 개시 등의 개인정보 취급에 관하여 제 절차에 대하여, 사전에 대외적으로 알기 쉽게 설명하는 것이 사업 활동에 대한 사회적 신뢰를 확보하기위하여 중요하다.

② 소비자등의 권리의익의 한층 보호

상기 ①에서 제시한, 사업자의 개인정보보호를 추진하는 이상 구상과 방침에 이어, 소비자 등 본인의 권리의익보호 관점으로부터, 이하에 게재하는 점을 고려한 기술을 포함시키고, 본인으로부터의 요구를 한층 대응해가는 것도 중요하다.

- 보유개인데이터에 대하여 본인으로부터 요구가 있는 경우에는 스펀메일의 발송 정지 등 자주적인 이용정지등에 대응하는 것.

- 위탁의 유무, 위탁하는 사무의 내용을 명확히 하는 등, 수탁처리의 투명성을 진척시키는 것.
- 사업자가 그 사업내용을 기안하여 고객의 종류마다 이용목적을 한정하여 표시하고, 사업자가 본인의 선택에 의한 이용목적의 한정에 자주적으로 힘쓰는 것 등, 본인에게 이용목적보다 명확히 하는 것.
- 개인정보 취득원 또는 그 취득방법(취득원의 종류 등)을 가능한 한 구체적으로 명기하는 것.

또 사업자에서 개인정보 누설 등의 사안이 발생한 경우에는 이차피해의 발생, 유사사안의 방생회피 등의 관점에서 가능한 사실관계 등을 공표하는 것이 중요하다.

③ 책임체제의 확보

사업운영에 대하여 개인정보 보호를 적절히 자리매김하는 관점에서, 외부로부터의 부정 액세스의 방제 대책 외에, 개인정보보호관리자의 설치, 내용관계자의 액세스 관리와 유출 방지 등, 개인정보의 안전관리에 대하여 사업자 내부에의 책임체제를 확보하기 위한 구조를 정비하는 것이 중요하다. 또 개인정보 취급을 외부에 위탁할 때에는 위탁계약 중에 개인정보 유출방지를 시작으로 하는 보호를 위한 조치가 위탁처에 있어 확보되도록, 위탁원과 위탁처의 각각 책임 등을 명확히 정하는 것에 의해 재 위임된 경우를 포함하여 실효적 감독체제를 확보하는 것이 중요하다.

④ 종업자의 계발(啓發)

사업자에 있어 개인정보 누설 등의 방지 등, 그 취급 개인정보의 적절한 보호가 확보되기 위하여 교육연수의 실시 등을 통하여 개인정보

를 실제에 업무에서 취급하는 것이 된 종업자의 계발을 도모하는 것에 의해, 중법자의 개인정보보호 의식을 철저히 하는 것이 중요하다.

⑤ 안전관리조치의 정도

사업자에 있어, 그 취급하는 개인정보의 적절한 보호가 확보되기 위하여 누설, 멸실 또는 손해가 발생한 경우에는 본인이 피해 권리의익의 침해의 크기를 고려하고 사업의 성질 및 개인정보의 취급상황 등에 기인하는 리스크에 따라 필요하고 적절한 조치를 강구하는 것이 중요하다.

이때에는 개인정보를 기록한 매체의 성질에 응한 안전관리조치를 강구하는 것이 중요하다. 예를 들어, 불특정다수자가 서점에서 수시로 구입가능한 명부에서, 사업자에 있어 전혀 가공을 하지 않은 것은 개인의 권리의익을 침해할 우려는 적다는 것을 고려할 수 있기 때문에, 그것을 처분하기 위하여 문서 세절기 등에 의한 처리를 하지 않고 폐기하고, 또는 폐품회수로 제출한 것이라도 사업자의 안전관리조치의 의무위반이 되지 않는 것으로 취급할 수 있는 것으로 한다.

(2) 인정개인정보보호단체에 관한 사항

① 각 성청에서의 인증 촉진

인정개인정보보호단체는 고충처리에 있어, 개인정보취급사업자 자신에 의한 대응을 보완하고, 문제를 자주적, 실제적인 해결을 도모하면서, 각 사업분야에서 가이드라인 책정 등을 통하여 사업자의 개인정보보호의 대처를 지원하는 등 민간분야에서의 주체적인 대응에, 매우 중요한 역할이 기대되고, 그 구조가 충분히 활용될 것이 필요하다.

이러한 중, 각 인정개인정보보호단체의 활동 정도에는 차이가 보인다는 지적이 있기 때문에, 활동이 충분히 되지 않는 단체에 있어는 적극적으로 고충처리와 정보제공 등에 힘쓰는 것이 요망된다.

또, 사업분야에 의하면, 인정개인정보보호단체의 인정이 충분히 행해지지 않는 것도 있기 때문에, 이러한 분야를 소관 하는 각 성청에 서는 더욱 인정 촉진에 힘쓸 것이 필요하다.

② 가이드라인(개인정보보호지침)등의 책정·재검토

개인정보 보호에 관한 사업 분야별 대처에 있어서는 종래로부터, 각 성청이 책정하는 가이드라인과 병행하여 사업자단체 등이 책정한 가이드라인이 각 사업자 대책을 촉진하면서, 중요한 역할을 해 왔다. 이 때문에, 사업자 단체 등에 있어 계속 사업 분야의 실정에 따라, 가이드라인(개인정보보호지침)등을 책정·재검토와 그 공표를 하면서 사업자에 대하여 필요한 지도 등에 노력을 다하는 것이 요망된다. 이 때 사업자단체 등의 유저에 따라 각 성청은 2의 (3)의 ①에 의해 필요한 지원을 하도록 한다.

7. 개인정보 취급에 관한 고충의 원활한 처리에 관한 사항

개인정보 이용·제공 혹은 개시·불개시에 관한 본인의 불평과 불만은 소송 등에 의한 것이 아니라, 사안의 성질에 의해, 신속성·경제성 등의 관점으로부터 오히려 고충처리의 제도에 의해 해결하는 것이 적당한 것이 많다고 생각된다. 법은 고충처리에 의한 국민 권리이익의 보호의 실효를 기대하기위하여, 개인정보취급사업자 자체의 대처에 의해 고충을 해결하는 것을 기본으로 하면서, 인정개인정보보호단체, 지방공공단체 등이 고충의 처리에 고나한 복층적인 구조를 채택하고 있다. 이 구조가 원만히 기능하기 위하여 이러한 관계기관이 각각 그 역할분담에 따라 적절히 대처하면서 긴밀한 연대를 확보하는 것이 필요하다.

(1) 사업자자신에 의한 대처의 모습

법은 고충처리에 대하여 우선 제1로 개인정보취급사업자의 책임에 있어 절절하고 신속한 처리에 노력해야하는 것을 명확히 하고 있다. 이러한 책무를 완수하기 위하여 사업자에는 필요한 체제정비로서의 고충접수창구의 설치, 고충처리 수순의 책정 등이 요구된다.

(2) 인정개인정보보호단체의 대체 모습

인정개인정보단체의 고충처리는 각사업자가 행한 대처를 보완하고, 국민의 이익을 효율적·효과적으로 실현하는 중요한 역할이 기대된다. 이를 위하여, 인정개인정보보호단체는 본인으로부터의 다양한 고충에 간이·신속히 대처하고 공정한 제3자로서의 입장에서부터 국민의 기대에 부응하려, 인재의 양성, 확보를 포함한 체제를 정비하는 것이 요구된다.

(3) 지방공공단체에 있어 대처의 모습

지방공공단체가 맡은 처리의 알선 등은 당사자 간의 문제가 해결되지 않는 경우 등에 있어, 사업 분야를 묻지 않고 고충처리의 구조로서, 고충처리의 알선, 조언, 지도, 정보제공 등의 역할이 요구되고 있다. 지방공공단체가 고충의 처리 알선 등에 힘쓰는 것에는 넓게 주민 일반에 알기 쉽고 친숙한 대응이 요구된다. 이 때, 개인정보에 관한 고충의 상당부분은 사업자가 소비자의 개인정보를 이용한 결과로서 발생하는 소비자생활상의 고충이라고 생각되는 것, 상담자의 입장에서부터 소비생활에 관한 고충으로부터 기존의 소비생활센터와 소비자상담창구 등을 개인정보에 관한 고충의 창구로서 이를 축으로 각 사업·사업자의 진흥·지원을 맡은 부국 등의 관계부서가 실효 있는 연대를 확보하는 구조가 상담자의 편리성 등의 관점에서부터 요구된

다. 또, 지방공공단체에 있어 조례 등에 근거 별도의 고충창구를 정하고 있는 경우 등, 직접 상기의 구조에 따르기 어려운 경우에 있어서는 특히 창구와 관계부국의 역할분담을 명확히 하고, 주지를 도모하면서 소비생활센터 등에 의뢰된 고충의 이송 등의 구조를 충분히 확보할 필요가 있다.

(4) 국민생활센터 및 각 성청에 있어서의 대처

① 국민생활 센터의 대처

각 지방공공단체와 인정개인정보보호단체에 의뢰된 고충이 주민·사업자의 혼란을 일으킴 없이 원만히 처리되기 위하여 소비생활센터 등의 상담원의 개인정보보호에 관한 전문지식의 습득을 긴급히 촉진하면서 각 상담기관에 있어 식견의 축적과 그 활용이 중요하다.

이를 위하여 국민생활센터는 스스로 개인정보에 관한 고충상담에 힘쓰는 외, 소비생활센터 등의 각종 상담기관과 연대를 도모하면서, 연수 등의 실시에 의한 전문지식을 갖춘 상담원을 육성, 고충처리에 관한 매뉴얼의 작성·배포 등에 의해 창구대응의 강화를 지원한다. 또, 이러한 대처에 대하여 필요에 응하여 인정개인정보보호단체 등의 협력을 얻으면서 실시하면서 인정개인정보보호단체에의 매뉴얼의 배포와 그 직원의 연수 등에 참가를 도모하도록 한다. 또, 국민생활센터는 개인정보에 관한 고충상담의 사례를 집약, 분석하고, 대응사례집 등의 자료를 작성하는 것 등에 의해, 각종 상담기관에 있어서 개별의 상담사례로부터 얻은 신견을 축적하고, 그 공유를 도모한다.

② 각 성청에 있어서의 대처

내각부 및 각 성청에 있어서 지방공공단체, 국민생활센터, 인정개인정보보호단체등과 연대하여 소관분야에 있어 개인정보의 적정한 취급을 확보하는 관점으로부터 2의 (2)의 ④에 의한 창구에 있어, 필요에

따라 각 성청의 대응 등에 대하여 정보를 제공하도록 한다.

또, 내각부에서는 각 성청 및 지방공공단체의 고충상담기관 등 창구 등에 관한 정보를 수집, 정리하고, 인터넷의 활용 등에 의해 제공한다.

8. 기타 개인정보 보호에 관한 시책의 추진에 관한 중요사항

(1) 정보수집·조사연구의 추진

개인정보 수집, 이용 등 그 취급의 태양은 정보통신기술의 발전, 신 분야에 있어 사업의 창출 등에 의해, 많은 변화가 있을 수 있는 것이고, 기본방침과 이를 근거로 한 조치에 대해서도 이러한 변화와 국제적인 개인정보보호제도의 동향 등에 따라 재검토를 할 필요가 있다, 이를 위하여 내각부 및 국민생활센터는 각 성청과의 연대 아래, 신기술과 개인정보의 이용 동향, 제외국의 제도 운용의 동향 등에 관한 정보수집, 조사연구를 하도록 한다.

(2) 국민생활심의회의 역할

내각부는 경제·사회사정의 변화에 따라 기본방침의 재검토에 있어, 국민생활심의회의 의견을 듣는 외에 2의(2)의 ⑤에 근거, 법의 시행상황에 대하여 국민생활심의회에 보고를 하면서 동심의회는 법의 시행상황의 추행 한다.