연구보고서 개인정보03-03

각국의 개인정보피해구제제도 비교연구

A Comparative Study on Remedies for Personal Information Infringements

이창범/윤주연

PICO 개인정보분쟁조정위원회
Personal Information Dispute Mediation Committee

요 약 문

1. 제목

각국의 개인정보피해구제제도 비교연구

2. 연구의 목적 및 중요성

최근 개인정보침해가 급격히 증가하면서 어느 때보다도 개인정보보호의 필요성이 강조되고 있다. 그 중에서도 특히 어떠한 방법과 절차에 따라 개인정보침해에 따른 불만을 해결하고 피해를 구제할 것인가에 관심의 초점이 맞춰져 있다고 할 것이다. 특히 최근 들어 우리나라에서는 개인정보보호기본법의 제정, 개인정보보호 전문·전담기구의 설립과 실질적인 권한 부여, 실효성 있는 개인정보피해구제 절차 및 방법의 확립에 대한 관심이 꾸준히 증가하고 있다.

따라서 본 연구 보고서는 이러한 시대적 관심과 요구에 발맞춰 국내의 개인정보피해구제제도의 현황을 파악하고 세계 주요국의 개인정보피해구제제도를 조사하여 그 결과를 상호 비교함으로써, 보다 효율적인 개인정보피해구제제도의 정착과 발전을 위한 개선방안을 모색해보고자 한다. 이를 통해 분쟁조정제도와 같은 우리나라의 개인정보피해구제제도가 가지는 특징과 장단점을 분석하여 장점은 더욱 발전시킬 수 있을 것이며, 단점이나 문제점은 개인정보보호 선진국의 피해구제제도가 가지는 장점을 국내 실정에 맞게 도입함으로써 보완해 나갈 수 있을 것이다. 즉, 본 연구보고서는 국내외 개인정보피해구제제도의 정확한 현황파악 및 상호 비교·분석을 통해 보다 궁극적으로는 우리나라의 개인정보피해구제제도의 선진화 및 국내 환경에 적합한 피해구제제도의 정착을 목표로 할 수 있을 것이다.

3. 연구의 내용 및 범위

개인정보피해구제제도는 구체적으로 개인정보관련 법률이 제정되어 있는지 여부, 독립적이고 전문적인 개인정보보호기구가 존재하는지 여부, 소송외적 분쟁해결제도와 같은 적극적인 피해구제절차 및 방법이 갖추어져 있는지 여부 등 세 가지 측면에서 바라볼 수 있다. 이에 본 연구보고서에서는 우리나라를 비롯하여 영국, 프랑스, 독일, 스웨덴, 미국, 캐나다, 호주, 뉴질랜드, 홍콩, 일본 등 주요 개인정보보호 선진 10개국의 개인정보피해구제제도를 위와 같은 세 가지 측면에서 중점적으로 조사·분석하였다.

각 장에서 다루어질 구체적인 내용을 간략히 소개하면 다음과 같다. 먼저, 제2장에서는 본격적으로 국내외 개인정보피해구제제도를 살펴보기에 앞서 개인정보보호, 프라이버시권, 정보프라이버시의 개념과 상호관계에 대한 기본 이론을 중심으로 살펴보았다. 또한 전자상거래가 활성화되면서 더욱 각광받고 있는 소송외적 분쟁해결제도의 개념, 유형, 특징 등을 검토하였다.

제3장에서는 국내 개인정보피해구제제도의 현황을 분석하였다. 우선은 개인정보관련 법률의 제정현황과 공공부문과 민간부문을 대표하는 개인정보보호법의 주요내용을 검토해보았다. 또한 개인정보분쟁조정위원회, 정보통신부, 개인정보보호심의위원회, 한국소비자보호원, 금융감독원 등의 개인정보보호 및 피해구제 역할을 살펴보았다.

제4장에서는 국내에 이어 해외 주요국의 개인정보피해구제제도 현황을 조사·분석하였다. 먼저 개인정보와 관련된 OECD, UN, EU의 국제규범을 살펴본 뒤, 앞서 언급한 유럽과 북미, 오세아니아, 아시아 지역 총 10개국의 개인정보피해구제제도를 차례로 검토하였다. 주요 검토내용은 각국의 개인정보보호법제 현황과 개인정보보호기구의 설치 및 운영상황, 개인정보피해구제 절차 및 방법이다.

제5장에서는 제3장과 제4장에서 검토한 내용을 바탕으로, 각국의 개인정보피해구제제도를 상호 비교·분석하였다. 개인정보보호법의 존재형식 및 적용범위, 개인정보보호기구의 행정체계, 형태, 기능·권한, 개인정보피해구제의 주체, 내용, 절차 및 방법 등을 기준으로 각국의 피해구제제도를 구분하여 상호 비교하였다.

제6장은 제5장에서 비교·검토한 내용이 국내 개인정보피해구제제도에 시사하는 바는 무엇인지, 국내 개인정보피해구제제도가 가지는 문제점은 무엇인지를 확인하였다. 또한 더 나아가 국내 제도가 어떠한 방향으로 나아가야 할 것인지, 보다 더 효율적인 개인정보피해구제제도의 확립과 정착을 위해서 필요한 사항은 무엇인지를 살펴보았다.

마지막으로 제7장은 각 장에서 검토한 내용을 바탕으로 현대사회에서 개인정보가 가지는 중요성과 효율적인 개인정보피해구제제도 확립의 필요성, 우리나라의 개인정보피해구제제도가 나아갈 방향을 다시 한 번 언급하는 것으로 마무리하였다.

4. 활용에 대한 건의

본 보고서는 우리나라의 개인정보피해구제제도는 물론 유럽, 북미, 오세아니아, 아시아 지역의 개인정보피해구제제도를 법적·제도적·절차적 측면에서 상세하게 살펴보고 각각의 유사점과 차이점을 비교·분석하였다.

향후 이러한 비교·분석 자료가 개인정보분쟁조정위원회의 피해구제제도 발전은 물론, 더 나아가 우리나라의 개인정보피해구제제도의 선진화를 위한 유용한 참고자료가 될 수 있기를 기대한다.

키워드 : 개인정보 피해구제, 분쟁조정, 소송외적 분쟁해결제도, 개인정보, 정보보호, 프라이버시, 개인정보보호기구

SUMMARY

1. Title

A Comparative Study on Remedies for Personal Information Infringements

2. Purpose of the Study

As the number of personal information infringement cases have been dramatically increased, the significance of personal information protection has been emphasized more. Especially, there have been a lot of discussions about the methods and procedures for relieving complaints about personal information infringements.

Also in Korea, there have been demands for establishing remedial systems for personal information infringements including an enactment of comprehensive personal information protection law and an establishment of an independent authority for data protection and of effective Alternative Dispute Resolution(ADR) systems. Responding to such concerns and demands, this paper reviews other countries' remedial systems for personal information infringements. And the comparative analysis has been conducted with the aim of improving the Korean systems.

The ultimate purpose of this work is to advance the current systems of Korea for relieving damages caused by personal information infringements and to find out the systems that are suitable to domestic circumstance through comparative and precise analysis.

3. Contents and Scope

The remedial systems for personal information infringements can be examined from three angles. The first angle is whether there is a comprehensive law to protect personal information. The second is whether an independent data protection authority is established. The last is whether an ADR system for personal information disputes is practicable and effective. This study analyzes the remedial systems of the United Kingdom, France, Germany, Sweden, Australia, New Zealand, USA, Canada, Hongkong, and Japan compared with the system of Korea in these three angles.

In Chapter Ⅱ this report begins to examine the concept of the personal information protection, the right to privacy and the information privacy and the distinguishing marks of alternative dispute resolution systems. The Chapter Ⅲ analyzes the current systems of Korea for relieving damages caused by personal information infringements. It reviews legislations for the protection of personal information and their contents with focusing two representative acts each of which applies to the public and private sector, respectively. Additionally, the roles of the personal information protection authorities such as Personal Information Dispute Mediation Committee have been studied. The chapter Ⅳ analyzes the remedial systems for personal information infringements of foreign countries. After reviewing regulations related to personal information of OECD, UN, EU, it researches into remedies for personal information infringements of the ten countries of Europe, North America, Oceania and Asia.

The chapter Ⅴ analyzes more thoroughly remedies for personal information infringements of the countries under review in the

chapter Ⅲ and the chapter Ⅳ and compares them. The subjects of the comparison include the existence of the comprehensive law for personal information protection, the administrative systems, function and power of personal information protection authorities and procedures for relieving personal information infringements. The chapter Ⅵ argues the implication of the result of comparison in the chapter Ⅴ and the problems that the remedies for personal information infringements of Korea have. Further it also discusses what should be done in order to make the remedies of Korea more effective and what approach should be taken to make it fully developed. Finally, the chapter Ⅶ reaffirms the importance of personal information in modern society and the necessity of the establishment of remedial systems for personal information infringements.

4. Expected effects and applications

This paper has analyzed the legal, systematic and procedural aspects of remedial systems for personal information infringements. For this analysis, it conducts a comparative study which researches and compares the remedial systems of some countries in Europe, North America, Oceania and Asia including Korea.

This report could be a useful reference for developing the current systems of Korea for relieving damages caused by personal information infringements.

Key words : Remedies for personal information infringements, Mediation, Alternative dispute resolution system, Personal information, Data protection, Privacy, Data protection authority

목 차

제 1 장 서 론 ····· 1

제 1 절 연구배경 ····· 1
1. 컴퓨터 네트워크 시대의 도래 ····· 1
2. 정보사회의 도래와 개인정보침해의 증가 ····· 2
3. 개인정보침해문제에 대한 외국의 대응 ····· 4

제 2 절 연구목적 및 범위 ····· 6
1. 연구목적 ····· 6
2. 연구범위 ····· 6

제 3 절 연구방법 ····· 9
1. 문헌조사 ····· 9
2. 웹사이트 조사 ····· 9
3. 현장방문조사 ····· 10

제 2 장 개인정보와 효율적 피해구제 ····· 11

제 1 절 인터넷 정보사회와 개인정보보호 ····· 11
1. 프라이버시와 개인정보 ····· 12
가. 프라이버시의 개념 ····· 12
나. 프라이버시의 범주 및 유형 ····· 16
다. 프라이버시와 개인정보의 관계 ····· 19
2. 개인정보의 개념 ····· 21
3. 개인정보의 활용과 보호 ····· 26

제 2 절 개인정보 분쟁해결과 피해구제 ····· 29
1. 개인정보피해구제의 개념 ····· 29
2. 소송외적 분쟁해결제도 ····· 30
가. 소송외적 분쟁해결제도의 의의 ····· 30
나. 소송외적 분쟁해결제도의 유형 ····· 31
다. 주요 ADR 모델 ····· 34
(1) 협상 ····· 34
(2) 알선 ····· 35
(3) 조정 ····· 36
(4) 중재 ····· 37
3. 소송외적 분쟁해결제도와 개인정보피해구제 ····· 38

제 3 장 국내 개인정보피해구제제도 ····· 41

제 1 절 국내 개인정보보호법 ····· 42
1. 입법현황 ····· 42
2. 공공기관개인정보보호법 ····· 44
가. 적용범위 ····· 45
나. 정보주체의 권리 ····· 46
(1) 열람・정정청구권 ····· 46
(2) 불복청구권 ····· 48
다. 공공기관의 의무 ····· 49
(1) 수집・보유의 제한 ····· 49
(2) 개인정보파일의 사전통보 및 공고 ····· 50
(3) 개인정보파일의 안전성・정확성・최신성 확보 ····· 51
(4) 처리정보의 이용 및 제공 제한 ····· 52
(5) 개인정보취급자의 비밀누설금지의무 ····· 52
3. 정보보호법 ····· 53

가. 적용범위 ····· 53
나. 정보주체의 권리 ····· 54
(1) 동의권 및 동의철회권 ····· 54
(2) 열람·정정요구권 ····· 55
(3) 개인정보침해에 대한 손해배상청구권 ····· 56
다. 정보통신서비스제공자의 의무 ····· 56
(1) 필요최소한의 정보수집의무 ····· 57
(2) 고지·명시의무 ····· 57
(3) 목적외 이용 및 제3자 제공 금지의무 ····· 58
(4) 개인정보의 안전한 관리의무 ····· 59
(5) 이용자의 권리를 보장할 의무 ····· 59
(6) 개인정보의 즉시파기의무 ····· 60
라. 아동의 개인정보보호 ····· 61

제 2 절 국내 개인정보보호기구 ····· 62
1. 공공부문 ····· 63
가. 행정자치부 ····· 64
나. 개인정보보호심의위원회 ····· 66
다. 국민고충처리위원회 ····· 67
라. 행정구제 ····· 68
2. 민간부문 ····· 69
가. 정보통신부 ····· 69
나. 개인정보분쟁조정위원회 ····· 72
(1) 위원회의 구성 ····· 72
(2) 위원회의 조정범위 ····· 73
(3) 분쟁조정절차 ····· 74
(4) 분쟁조정의 효력 ····· 76
(5) 위원회의 피해구제 성과 ····· 76

다. 통신위원회 ····· 78
(1) 설립 및 기능 ····· 78
(2) 피해구제절차 ····· 79
(3) 개인정보보호 기능 및 역할 ····· 81
라. 한국소비자보호원 ····· 82
(1) 설립 및 기능 ····· 82
(2) 피해구제절차 ····· 83
(3) 개인정보보호 기능 및 역할 ····· 86
마. 전자거래분쟁조정위원회 ····· 86
(1) 설립 및 구성 ····· 86
(2) 분쟁조정절차 ····· 87
(3) 개인정보보호 기능 및 역할 ····· 89
바. 금융감독위원회 ····· 91
(1) 설립 및 구성 ····· 91
(2) 개인정보보호 기능 및 역할 ····· 92
3. 기타 ····· 94
가. 국가인권위원회 ····· 94
나. 경찰청 사이버테러대응센터 ····· 96

제 4 장 해외 개인정보피해구제제도 ····· 98

제 1 절 개인정보보호 국제규범 ····· 99
1. OECD 프라이버시 가이드라인 ····· 100
2. UN 개인정보 가이드라인 ····· 102
3. EU 개인정보보호 지침 ····· 104

제 2 절 유럽 ····· 108
1. 영국 ····· 109

가. 개인정보보호 법제현황 ····· 109
나. 정보보호법의 주요내용 ····· 112
다. 영국의 개인정보보호기구 ····· 114
(1) 정보커미셔너의 지위 ····· 114
(2) 정보커미셔너의 업무범위 ····· 115
(3) 정보커미셔너의 조직구성 ····· 115
(4) 정보커미셔너의 주요기능 ····· 116
라. 개인정보피해구제 절차 및 방법 ····· 118
2. 프랑스 ····· 121
가. 개인정보보호 법제현황 ····· 122
나. 정보처리축적및자유에관한법률의 주요내용 ····· 125
(1) 연혁 및 적용범위 ····· 125
(2) 정보주체의 권리 ····· 126
(3) 정보처리자의 의무 ····· 126
다. 프랑스의 개인정보보호기구 ····· 128
(1) CNIL의 지위 및 특징 ····· 129
(2) CNIL의 조직구성 ····· 131
(3) CNIL의 주요기능 ····· 133
라. 개인정보피해구제 절차 및 방법 ····· 136
3. 독일 ····· 137
가. 개인정보보호 법제현황 ····· 138
나. 연방정보보호법의 주요내용 ····· 139
(1) 적용범위 ····· 140
(2) 정보주체의 권리 ····· 140
(3) 정보처리자의 의무 ····· 141
다. 독일의 개인정보보호기구 ····· 142
(1) 연방정보보호청의 지위 및 특징 ····· 143
(2) 연방정보보호청의 조직구성 ····· 144
(3) 연방정보보호청의 주요기능 ····· 145

라. 개인정보피해구제 절차 및 방법 ····· 146
4. 스웨덴 ····· 150
가. 개인정보보호 법제현황 ····· 150
나. 정보보호법의 주요내용 ····· 151
다. 스웨덴의 개인정보보호기구 ····· 153
(1) 정보조사원의 지위 및 구성 ····· 153
(2) 정보조사원의 주요기능 및 권한 ····· 155
라. 개인정보피해구제 절차 및 방법 ····· 157

제 3 절 북미 ····· 160
1. 미국 ····· 160
가. 개인정보보호 법제현황 ····· 161
(1) 판례법상 프라이버시권의 인정 ····· 161
(2) 개인정보보호 법제현황 ····· 163
(3) 세이프하버 원칙(Safe Harbor Principles) ····· 164
나. 개인정보관련 법률의 주요내용 ····· 166
(1) 프라이버시법 ····· 166
(2) 금융부문의 프라이버시보호법 ····· 167
(3) 통신부문의 프라이버시보호법 ····· 169
(4) 가족의교육권및프라이버시에관한법률(FERPA) ····· 170
(5) 비디오프라이버시보호법 ····· 171
(6) 아동온라인프라이버시보호법(COPPA) ····· 172
다. 미국의 개인정보보호기구 ····· 173
(1) FTC의 설립 및 구성 ····· 174
(2) FTC의 개인정보보호 기능 및 역할 ····· 174
라. 개인정보피해구제 절차 및 방법 ····· 176
(1) 민간분쟁해결제도 ····· 177
(2) FTC의 개인정보피해구제 절차 및 방법 ····· 182

2. 캐나다 ····· 186
가. 개인정보보호 법제현황 ····· 186
나. 개인정보보호법의 주요내용 ····· 188
(1) 프라이버시법 ····· 188
(2) 개인정보보호및전자문서에관한법 ····· 190
다. 캐나다의 개인정보보호기구 ····· 192
(1) 프라이버시커미셔너의 지위 ····· 193
(2) 프라이버시커미셔너의 조직구성 ····· 194
(3) 프라이버시커미셔너의 주요기능 ····· 195
라. 개인정보피해구제 절차 및 방법 ····· 197

제 4 절 오세아니아 ····· 202
1. 호주 ····· 202
가. 개인정보보호 법제현황 ····· 202
나. 연방프라이버시법의 주요내용 ····· 203
(1) 적용범위 ····· 203
(2) 프라이버시 원칙 ····· 204
다. 호주의 개인정보보호기구 ····· 207
(1) 프라이버시커미셔너의 지위 ····· 208
(2) 프라이버시커미셔너의 조직구성 ····· 208
(3) 프라이버시커미셔너의 주요기능 ····· 209
라. 개인정보피해구제 절차 및 방법 ····· 211
2. 뉴질랜드 ····· 217
가. 프라이버시법의 주요내용 ····· 217
(1) 정보프라이버시원칙 ····· 218
(2) 정보등록부상의 프라이버시원칙(PRPP) ····· 221
나. 뉴질랜드의 개인정보보호기구 ····· 221
(1) 프라이버시커미셔너의 지위 ····· 222

(2) 프라이버시커미셔너의 조직구성 ····· 223
(3) 프라이버시커미셔너의 주요기능 ····· 224
다. 개인정보피해구제 절차 및 방법 ····· 225
(1) 프라이버시커미셔너의 피해구제 절차 및 방법 ····· 225
(2) 인권법원을 통한 피해구제 ····· 228

제 5 절 아시아 ····· 231
1. 일본 ····· 231
가. 개인정보보호 법제현황 ····· 232
나. 개인정보보호법의 주요내용 ····· 237
(1) 기본이념 및 국가 등의 책무 ····· 237
(2) 개인정보취급사업자의 의무 ····· 238
다. 개인정보보호기구 및 피해구제제도 ····· 239
(1) 정부차원의 개인정보피해구제 ····· 239
(2) 민간차원의 개인정보피해구제 ····· 240
2. 홍콩 ····· 243
가. 개인정보보호법의 주요내용 ····· 244
나. 개인정보보호기구 ····· 245
(1) 개인정보커미셔너의 설립 및 지위 ····· 245
(2) 개인정보커미셔너의 조직구성 ····· 246
(3) 개인정보커미셔너의 주요기능 ····· 247
다. 개인정보피해구제 절차 및 방법 ····· 248

제 5 장 각국의 개인정보피해구제제도 비교 ····· 254

제 1 절 개인정보보호법 비교 ····· 254
1. 입법의 존재형식에 따른 비교 ····· 255
가. 통합형 입법주의 ····· 255

나. 구분형 입법주의 ····· 258
2. 적용범위에 따른 비교 ····· 259
가. 개인정보의 자동처리 유무에 따른 분류 ····· 260
나. 정보주체의 성질에 따른 분류 ····· 262

제 2 절 개인정보보호기구 비교 ····· 265
1. 형태에 따른 분류 ····· 265
가. 사법기구형 ····· 267
나. 전문 독립기구형 ····· 268
다. 행정부 지원형 ····· 269
라. 행정부 소속형 ····· 271
마. 민간단체형 ····· 278
2. 개인정보보호기구의 기능 비교 ····· 278
가. 개인정보보호기구의 주요기능 현황 ····· 278
나. 중점적 기능에 따른 비교 ····· 281
3. 개인정보보호기구의 권한 비교 ····· 284
가. 사전 침해예방적 기능을 위한 권한 ····· 284
나. 사후 피해구제적 기능을 위한 권한 ····· 285

제 3 절 개인정보피해구제제도 비교 ····· 289
1. 주체에 따른 분류 ····· 289
가. 정부 주도의 피해구제 ····· 289
나. 민간 주도의 피해구제 ····· 290
다. 복합적 형태 ····· 290
2. 방법에 따른 분류 ····· 293
가. 합의권고 ····· 293
나. 조정・결정 ····· 294
다. 시정권고 ····· 296

라. 이행고지 ····· 296
마. 시정명령 또는 과태료 부과 ····· 297
바. 형사고발 및 소제기 ····· 298
3. 내용에 따른 분류 ····· 298
가. 선언적 구제 ····· 299
나. 교정적 구제 ····· 299
다. 보상적 구제 ····· 300

제 6 장 개인정보피해구제제도 개선방안 ····· 302

제 1 절 개인정보보호법 ····· 302
1. 개인정보보호법제의 문제점 ····· 302
2. 개인정보보호기본법의 제정 ····· 305

제 2 절 개인정보보호 행정체계 ····· 308
1. 개인정보보호 행정체계상의 문제점 ····· 308
2. 개인정보보호 전문·전담기구의 설립 ····· 309

제 3 절 개인정보보호기구의 기능·권한 ····· 312
1. 개인정보보호기구의 기능·권한상의 문제점 ····· 312
2. 개인정보보호기구에 통합적 기능과 권한 부여 ····· 314

제 7 장 결론 ····· 317

표 목차

〔표 2-1〕 다양한 프라이버시의 개념 정의 ····· 15
〔표 2-2〕 프라이버시의 범주 ····· 17
〔표 2-3〕 프라이버시의 유형 (EPIC & PI) ····· 18
〔표 2-4〕 개인정보의 개념 ····· 23
〔표 2-5〕 해외 법규범 속에서의 개인정보의 개념정의 ····· 23
〔표 2-6〕 국내법상 개인정보의 개념정의 ····· 25
〔표 2-7〕 개인정보의 유형 및 구체적 예 ····· 26
〔표 2-8〕 광의의 피해구제제도의 개념 및 유형 ····· 29
〔표 2-9〕 소송외적 분쟁해결제도의 유형 Ⅰ(NADRAC) ····· 32
〔표 2-10〕 소송외적 분쟁해결제도의 유형 Ⅱ(CDG) ····· 33
〔표 2-11〕 소송외적 분쟁해결제도의 유형 Ⅲ(CDG) ····· 33
〔표 2-12〕 개인정보침해의 특수성 ····· 39
〔표 3-1〕 국내 개인정보관련 입법현황 ····· 43
〔표 3-2〕 정보통신서비스제공자의 의무 ····· 56
〔표 3-3〕 정보통신서비스제공자가 고지·명시하여야 할 사항 ····· 58
〔표 3-4〕 국내 개인정보보호기구 현황 ····· 63
〔표 3-5〕 개인정보침해신고센터의 개인정보 상담·신고 접수현황 ···· 71
〔표 3-6〕 정보통신부의 조치내역 ····· 71
〔표 3-7〕 개인정보분쟁조정위원회의 위원구성 현황 ····· 73
〔표 3-8〕 개인정보분쟁조정위원회의 피해구제 신청현황 ····· 77
〔표 3-9〕 2003년도 개인정보분쟁조정위원회의 조정결정 ····· 77
〔표 3-10〕 전자거래분쟁조정위원회의 개인정보피해구제 현황 ····· 90
〔표 3-11〕 금융감독위원회의 개인정보보호 기능 ····· 93
〔표 4-1〕 OECD 프라이버시 8원칙 ····· 101
〔표 4-2〕 UN 개인정보 6원칙 ····· 103
〔표 4-3〕 EU 개인정보보호지침의 주요내용 ····· 106

［표 4-4］ 영국의 개인정보관련 법제현황 ····· 111
［표 4-5］ 영국의 정보보호 8원칙 ····· 112
［표 4-6］ 영국 정보커미셔너의 주요기능 ····· 117
［표 4-7］ 정보처리축적및자유에관한법률 및 하위법령 ····· 123
［표 4-8］ 기타 개인정보관련 법규 ····· 124
［표 4-9］ 정보처리축적및자유에관한법률의 주요 개정내용 ····· 125
［표 4-10］ CNIL의 위원구성 규정 ····· 129
［표 4-11］ CNIL의 위원구성 현황 ····· 130
［표 4-12］ CNIL의 조직체계 및 부서별 역할 ····· 132
［표 4-13］ CNIL의 주요기능 ····· 135
［표 4-14］ CNIL의 피해구제 현황 ····· 137
［표 4-15］ 독일 연방정보보호청의 주요기능 ····· 146
［표 4-16］ 스웨덴 정보보호법의 주요내용 ····· 152
［표 4-17］ 스웨덴 정보보호법상 개인정보처리 기본원칙 ····· 153
［표 4-18］ 스웨덴 DIB의 조직구성 및 주요업무 ····· 155
［표 4-19］ 스웨덴 DIB의 주요기능 ····· 156
［표 4-20］ 스웨덴 DIB의 주요 권한 ····· 157
［표 4-21］ 미국의 개인정보관련 법제현황 ····· 163
［표 4-22］ 세이프하버 7원칙 ····· 165
［표 4-23］ BBBOnLine의 항소 유형 ····· 181
［표 4-24］ 캐나다의 개인정보보호 법제현황 ····· 187
［표 4-25］ PIPEDA의 정보주체의 권리 및 정보처리자의 의무 ····· 191
［표 4-26］ 캐나다 개인정보보호원칙 ····· 192
［표 4-27］ 캐나다 개인정보보호기구 현황 ····· 193
［표 4-28］ 프라이버시커미셔너의 주요기능 ····· 197
［표 4-29］ 2002/03년도 프라이버시커미셔너의 민원처리현황 ····· 200
［표 4-30］ 2002/03년도 프라이버시커미셔너의 사건해결유형 ····· 200
［표 4-31］ 호주 연방프라이버시법의 적용범위 ····· 204
［표 4-32］ 호주 공공분야 정보보호원칙(IPP) ····· 205

［표 4-33］ 호주 민간분야 정보보호원칙(NPP) ····· 206
［표 4-34］ 호주의 개인정보보호기구 현황 ····· 207
［표 4-35］ 호주 프라이버시커미셔너의 주요기능 ····· 210
［표 4-36］ 민간영역에서의 분쟁해결주체 ····· 215
［표 4-37］ 뉴질랜드 정보프라이버시원칙 ····· 219
［표 4-38］ 뉴질랜드 프라이버시커미셔너의 주요기능 ····· 225
［표 4-39］ 뉴질랜드 프라이버시커미셔너의 피해구제현황 ····· 226
［표 4-40］ 뉴질랜드 프라이버시커미셔너의 권한 ····· 228
［표 4-41］ 일본 개인정보관련 입법현황 ····· 236
［표 4-42］ 일본 개인정보보호법상 개인정보취급사업자의 의무 ····· 238
［표 4-43］ 홍콩의 정보보호원칙 ····· 244
［표 4-44］ 홍콩 PCO의 주요기능 ····· 248
［표 4-45］ 홍콩 PCO의 피해구제현황 ····· 249
［표 4-46］ 홍콩 PCO의 피해구제조치 ····· 251
［표 5-1］ 공공·민간 통합형 입법주의 ····· 256
［표 5-2］ 구분형 개인정보보호법 ····· 258
［표 5-3］ 처리방법에 따른 개인정보의 범위 ····· 262
［표 5-4］ 법인정보와 사자의 정보에 대한 법적용 여부 ····· 264
［표 5-5］ 개인정보보호기구의 형태별 구분 ····· 266
［표 5-6］ 각국 개인정보보호기구의 구성 및 운영현황 ····· 274
［표 5-7］ 각국 개인정보보호기구의 주요기능 현황 ····· 278
［표 5-8］ 개인정보보호기구의 주요기능 ····· 281
［표 5-9］ 개인정보보호기구의 주요 역할에 따른 구분 ····· 282
［표 5-10］ 각국 기구의 사전예방적 권한 비교 ····· 285
［표 5-11］ 각국 기구의 사후구제적 권한 비교 ····· 286
［표 5-12］ 피해구제 주체에 따른 분류 ····· 292
［표 5-13］ 피해구제 내용에 따른 분류 ····· 301
［표 5-14］ 한국의 개인정보보호기구의 기능·권한 비교 ····· 313

그림 목차

(그림 3-1) 공공기관의 개인정보열람청구 처리절차 ····· 47
(그림 3-2) 공공기관의 개인정보보호기구 및 체계 ····· 64
(그림 3-3) 개인정보분쟁조정위원회의 분쟁조정절차 ····· 75
(그림 3-4) 국가인권위원회의 구성현황 ····· 95
(그림 4-1) 영국 정보커미셔너의 조직도 ····· 116
(그림 4-2) 영국 정보커미셔너의 피해구제 절차도 ····· 119
(그림 4-3) 프랑스 CNIL의 조직도 ····· 132
(그림 4-4) 독일 BfD의 조직도 ····· 145
(그림 4-5) 독일 BfD의 피해구제 절차도 ····· 149
(그림 4-6) 스웨덴 정보조사원 조직도 ····· 154
(그림 4-7) 스웨덴 정보조사원의 피해구제 절차도 ····· 159
(그림 4-8) BBBOnLine의 피해구제 절차도 ····· 179
(그림 4-9) FTC의 피해구제 절차도 ····· 185
(그림 4-10) 캐나다 프라이버시커미셔너 조직도 ····· 195
(그림 4-11) 캐나다 프라이버시커미셔너의 피해구제 절차도 ····· 199
(그림 4-12) 호주 프라이버시커미셔너 조직도 ····· 209
(그림 4-13) 호주 프라이버시커미셔너의 피해구제 절차도 ····· 214
(그림 4-14) 호주 공동규제체계에 따른 피해구제 절차도 ····· 216
(그림 4-15) 뉴질랜드 프라이버시커미셔너 조직도 ····· 223
(그림 4-16) 뉴질랜드 프라이버시커미셔너의 피해구제 절차도 ····· 230
(그림 4-17) 일본의 개인정보피해구제 절차도 ····· 242
(그림 4-18) 홍콩 PCO의 조직도 ····· 246
(그림 4-19) 홍콩 PCO의 피해구제 절차도 ····· 250

제 1 장 서 론

제 1 절 연구배경

1. 컴퓨터 네트워크 시대의 도래

지금으로부터 약 60여 년 전, 인류는 누구도 쉽게 상상하지 못할 만큼 급격한 생활상의 혁신과 변화를 가져오게 될 기념비적 창조품을 만들어 낸다. 그것은 '에니악'(ENIAC : Electronic Numerical Integrator and Calculator)이라는 이름을 가진 30톤의 무게가 나가는 거대한 전자계산기이자 세계 최초의 컴퓨터였다. '에니악'은 '전자적분계산기'라는 그 이름 그대로 복잡한 계산을 정확하게 수행해내어 전장에서 상대의 목표물을 명중시키기 위한 목적으로 만들어진 것이었지만, 이렇듯 군사적 용도를 위해 만들어진 컴퓨터는 이내 그 편리함과 효용성을 무기로 우리 사회 전반에 깊숙이 침투하게 되었다. 초대형 컴퓨터는 점점 더 작고 가벼워지고 휴대하기 편하게 바뀌었을 뿐 아니라 그 성능 또한 과거의 전자계산기와 비교할 바가 못 된다. 이제 사람들은 컴퓨터를 통해 회사업무를 하고 숙제를 하고 게임을 할 뿐 아니라 물품을 구매하고 텔레비전을 시청하거나 영화를 보며 음악을 듣는 등 살아가면서 필요한 모든 일상생활을 컴퓨터와 함께 하고 있다. 불과 60여년 만에 컴퓨터는 우리 생활에 없어서는 안 될 필수품으로 거듭나게 된 것이다.

그러나 컴퓨터의 성능이 개선된 것만으로 인류의 생활패턴이 이토록 급격히 변모된 것은 아니다. 여기에는 인터넷의 발달과 보급이라는 또 하나의 동인이 있다. 인터넷은 개개인이 가지고 있는 컴퓨터와 컴퓨터를 하나의 네트워크로 연결함으로써 '온라인 세상'이라는 가상공간을 만들어냈고, 이러한 가상공간에서 사람들은 실제 공간과 다름없이 거의 모든

일상생활을 영위할 수 있게 되었다.[1] 또한 컴퓨터와 디지털 정보처리기술의 발달을 바탕으로 한 인터넷의 개발과 네트워크의 강화는 '정보의 바다'라고 불릴 정도로 수많은 정보들이 오가는 공간을 만들어냄으로써, 새로운 정보사회의 출현을 앞당기는 정보혁명의 주도적 역할을 담당하게 되었다.

2. 정보사회의 도래와 개인정보침해의 증가

정보사회는 정보가 곧 가치이자 자산이며 기업과 개인의 경쟁력의 원천이 되는 사회, 얼마나 중요하고 핵심적인 정보를 많이 보유하고 있는가에 따라 권력의 중심이 이동하는 사회를 의미한다. 이러한 정보사회의 출현은 과거와는 전혀 다른 사회적·경제적·문화적 환경을 만들어냈는데, 무엇보다도 가장 큰 변화의 핵심은 가치대상의 이동이다. 과거에는 공장에서 제작된 상품이 중요한 금전적 가치를 가지는 대상이었다고 한다면, 오늘날은 인간의 지식과 각종 정보가 사회적·경제적 가치를 가지는 대상이 된 것이다. 일례로 최근 들어 국내 각종 포털 사이트에서는 '지식검색'이라는 새로운 서비스를 경쟁적으로 도입·시행하고 있는데, 이는 말 그대로 지식 그 자체가 상품가치를 가진다는 것을 의미하고 있다. 이러한 사회적 변화로 인해, 현대인들은 보다 많은 정보와 지식을 습득하려 하고 기업들도 정보가 곧 경쟁력이라는 인식을 바탕으로 다양한 원천으로부터 보다 많은 정보를 획득하고자 노력하고 있다.

---

1) 실례로 인터넷이 활발히 보급되기 시작하던 1990년대 후반, 전 세계적으로 인터넷서바이벌 게임(Internet Survival Game)이 여러 차례 개최되어 세간의 관심을 얻은 바 있다. 이 행사에 참가한 사람들은 외부와의 접촉이 금지된 폐쇄된 공간에서 인터넷이 연결되는 컴퓨터와 신용카드만으로 음식과 의류 등 필요한 물품을 구매하고 TV를 시청하고 인터넷 게임을 하였으며 채팅을 통해 외부 사람과 접촉하는 등 다양한 활동을 하며 100시간 이상을 지냈다. 본래 이 행사는 사이버공간에서 인간이 어떠한 행동양식을 보이는지를 관찰하기 위해 개최된 것이었지만, 컴퓨터와 인터넷이 인간의 삶에 얼마나 큰 영향을 끼치고 있는지를 단적으로 보여주는 예이기도 하다. (조선일보, 1999년 6월 30일 기사 참조)

그러나 농경사회에서 산업사회로 바뀌면서 급격한 도시의 팽창, 환경파괴, 전통적인 가족제도의 붕괴, 물질숭배주의의 만연 등 여러 사회적 문제들로 인해 진통을 겪었던 것처럼, 산업사회에서 정보사회로의 변화과정에서도 마찬가지로 많은 부작용이 발생하고 있다. 급속도로 기술이 발전되고 빠르게 정보사회로 진입해가고 있는 것에 비해, 이에 걸맞은 사회적·윤리적 규범을 정립하지 못하는 사회적 부조화 현상이 초래되고 있는 것이다.

대표적인 것이 바로 개인정보침해의 증가이다. 새로운 정보사회의 출현으로 인해 현대인들은 자신의 개인정보를 외부에 노출시키지 않고서는 정상적인 사회·경제활동을 영위하기 어렵게 되었고, 개인정보의 이용가치 증대는 공공부문은 물론 기업과 같은 민간 영역에서의 개인정보 수집·이용·보유를 증가시켰다. 또한 점점 지구가 하나의 단일한 경제·사회 공동체로 나아가게 되면서 국제 무역과 교류가 빈번히 이루어지게 되어 개인정보가 국내를 넘어 외국으로 이전되는 예도 증가하고 있다. 그러나 개인정보의 이용가치만 중요시할 뿐, 개인정보가 침해될 경우 당사자가 어떠한 피해를 겪게 될 것인지에 대한 인식은 아직 미비한 실정이다. 공공기관인지 사기업인지를 막론하고 개인정보 관리가 허술하여 외부로 유출된다거나 내부자에 의해 다른 곳에 제공되는 사례를 흔히 볼 수 있고, 또한 이렇게 외부로 유출된 다수의 개인정보 목록이 공공연히 매매되고 있다는 소식도 종종 듣게 된다.[2] 특히 최근에는 신용카드번호와 같이 유출될 경우 직접적인 경제적 피해를 양산할 수 있는 정보가 오·남용되는 사례[3]도 빈번히 발생하고 있는 등 개인정보침해사건이 연이어 발생하고

2) 지난 6월 5일에는 부도난 회사에서 유출된 개인신용정보를 인터넷 신용정보거래사이트를 통해 판매한 자 및 이 정보를 물품 구입 등에 사용한 신용카드 할인업자가 「여신전문금융업법」 위반 등 혐의로 구속되었고(한국일보, 2003년 6월 5일 기사 참조), 11일에는 인터넷 게임사이트(70만명) 운영자와 영화사이트(30만명) 운영자가 자신이 운영하는 사이트 가입자 등의 개인정보를 신용카드모집대행업자에게 각각 5천만원과 2700여만원을 받고 매매한 혐의로 경찰에 구속된 바 있다(한겨레신문, 2003년 6월 11일 기사 참조).

3) 최근 서울지방법원은 다른 사람의 신용정보를 이용해 게임사이트의 사이버머니를 만들어 판 사람과 이들에게 자신이 재직하던 금융기관이 보유하고 있는 개인신용정보 9백여 건을 몰래 빼내 준 직원 2명에게 벌금형을 선고하였다. 또한 재판부는 이들 직

있어 사회문제로 대두되고 있는 실정이다. 또한 개인정보침해행위는 온라인뿐 아니라 공공부문, 금융, 의료, 교육 등 분야를 가리지 않고 발생하고 있어 정보주체에게 심각한 피해를 끼치는 등 건전한 정보사회 구축의 커다란 장애물이 되고 있다.[4]

3. 개인정보침해문제에 대한 외국의 대응

개인정보침해의 증가는 비단 국내만의 문제는 아니다. 오늘날 세계 각국은 사기 등의 수단을 통한 신분도용(ID Theft), 내부자에 의한 개인정보 유출, 다이렉트 마케팅(Direct Marketing)을 위한 개인정보 불법수집·이용문제 등으로 인하여 골머리를 앓고 있다.[5] 이에 외국에서는 특히 유럽 등 선진국을 중심으로 개인정보의 적법한 이용을 보장함과 동시에 부당한 개인정보침해로 인한 피해를 최소화하여 건전하고 신뢰할 수 있는 정보사회의 구축을 위한 각종 법제도를 도입하기 시작하였다. 이러한 움직임은 1960년대 말부터 시작되어 1980년대와 90년대를 거치면서 OECD와 EU를 중심으로 개인정보보호를 위한 국제규범 제정이라는 결과물로 나타나게 되었다. 이러한 개인정보보호의 필요성에 대한 국제적 인식은 각국의 국내제도에도 큰 영향을 끼쳤다. 특히 오늘날 세계 각국

원들이 일하던 생명보험사 등 금융기관도 개인정보 유출에 대한 우려가 높아지는 상황에서 직원들의 불법 행위를 막지 못한 책임이 있다며 각각 3백만원의 벌금형을 내려, 이러한 개인정보침해행위 및 고객의 개인정보를 소홀히 관리한 업계의 관행에 대하여 경종을 울린 바 있다. (YTN, 2003년 11월 17일 뉴스 참조)

4) 2003년 개인 인터넷 이용자의 정보화 역기능 실태조사에 의하면, 평소 웹사이트를 이용하면서 자신이 제공한 개인정보를 통해 프라이버시를 침해당할 가능성에 대해 응답자의 절반에 가까운 49.3%가 '약간 우려한다', 35.1%가 '매우 우려한다'고 대답하여, 개인정보 제공시 프라이버시 침해에 대한 우려수준이 매우 높은 것으로 조사된 바 있다. ((주)아이클릭, "2003년도 개인 인터넷 이용자의 정보화 역기능 실태조사 보고서", 한국정보보호진흥원, 2003. 3, 74~76면)

5) 최근 미국에서는 신분도용이 심각한 사회문제로 떠오르고 있는데 미국 FTC의 조사(Synovate, "*Identity Theft Survey Report*", Federal Trade Commission, 2003. 9.)에 의하면, 지난 5년간 2,730만여명의 미국인이 신분도용과 관련된 피해를 입었으며 이 중 작년 한해만 피해자 수가 990만명에 이른다고 한다.(Washington Post, "*ID Theft Aid From Congress*", 2003. 11. 3일자 기사 참조)

은 기존의 소송체계를 통해서는 개인정보침해에 대한 적절한 피해구제를 도모할 수 없다는 인식에 따라 개인정보에 특유한 피해구제제도 및 절차를 확립하고자 많은 노력을 기울이고 있다. 해외 각국의 대응방안은 바로 세 가지 측면으로 요약할 수 있는데, 첫째는 개인정보보호를 위한 실체법을 정비하는 것이고, 둘째는 개인정보보호 전문기구를 설치하는 것이며, 마지막은 소송외 분쟁해결제도 등 다양한 방법을 통해 개인정보 피해를 실질적으로 구제할 수 있는 절차와 방법을 마련하고 활성화시키는 것이다.

이러한 세계 각국의 개인정보피해구제를 위한 각종 법적·제도적 장치들은 개인정보침해의 증가가 사회문제화가 되고 있는 우리나라의 개인정보보호제도의 발전과 제도개선 방안을 모색함에 있어 중요한 참고자료가 될 수 있을 것으로 생각된다. 이에 본 논문에서는 세계 각국의 개인정보와 관련된 법제현황 및 그 내용과 개인정보보호기구, 소송외적 분쟁해결제도를 중심으로 각국의 개인정보피해구제제도를 비교·검토하여 보고자 한다.

제 2 절 연구목적 및 범위

1. 연구목적

본 연구의 핵심목적은 국내 개인정보피해구제제도의 선진화를 위한 발전방안 모색에 있다. 우리나라는 세계 어느 국가보다도 초고속 인터넷 망이 잘 갖추어져 있고 IT 환경도 뛰어나다는 평가를 받고 있다. 이렇듯 우리나라는 기술발달의 측면이나 이러한 기술의 상용화를 바탕으로 한 새로운 상품과 서비스의 개발 및 이용의 측면에서는 세계의 정보화를 앞서가는 선도적 역할을 담당하고 있다. 그러나 정보화에 따른 역기능, 특히 국민의 프라이버시 침해와 관련한 법·제도적인 장치에 있어서도 세계 각국을 이끌어가는 선도국가로서의 역할을 다하고 있다고 자임할 수 있는 지위에 있는지에 대해서는 우리 모두 확신하기 어려운 것이 사실이다. 이에 최근 학계·시민단체 등을 중심으로 개인정보보호법제 정비에 대한 주장이 확산되고 있고 정부도 개인정보보호법의 제정에 적극적인 자세를 보이고 있지만, 진작 국내·외 개인정보보호제도에 대한 체계적인 비교 연구나 장단점에 대한 분석은 거의 없는 실정이다. 따라서 본 논문은 이러한 시대적 관심과 요구에 발맞춰 국내의 개인정보피해구제제도의 현황을 파악하고 세계 주요국의 개인정보피해구제제도를 조사하여, 그 결과를 상호 비교함으로써 보다 효율적인 개인정보피해구제제도의 정착과 발전을 위한 개선방안을 모색해보고자 한다. 이러한 과정을 통해 궁극적으로는 우리나라의 개인정보피해구제제도의 선진화 및 국내 환경에 적합한 피해구제제도의 정착을 목표로 할 수 있을 것이다.

2. 연구범위

본 연구는 '개인정보피해구제'에 초점을 두어 국내 제도와 현황을 분석하고 유럽과 북미, 아시아, 오세아니아 지역의 주요 개인정보보호 선진

국을 중심으로 개인정보피해구제제도를 살펴볼 예정이다. 특히 개인정보피해구제제도를 세 가지 측면에서 바라볼 예정인데, 이를 살펴보면 다음과 같다. 첫 번째는 개인정보보호를 위한 실체법적 측면이다. 이는 개인정보보호법의 체계 및 존재방식, 개인정보보호법에서 규정하는 정보주체의 권리 및 개인정보처리자가 준수하여야 할 의무, 개인정보피해구제를 위한 실체법적 근거와 같은 내용을 포함한다. 두 번째는 개인정보행정의 시스템 즉, 조직적·기구적 측면이다. 이는 개인정보보호법의 이행과 준수를 규율하고 개인정보피해구제의 기능을 담당하기 위한 개인정보보호기구의 설치현황과 그 기능 및 역할, 조직구성, 기구의 성격 등에 관한 부분이다. 마지막은 개인정보피해구제의 방법·절차적 측면이다. 통상 피해구제라고 하면 대표적으로 소송제도를 떠올리게 되는데, 본 연구보고서에서는 개인정보보호기구가 담당하여 행하는 소송외적 분쟁해결제도 등에 의한 개인정보피해구제 절차 및 방법, 현황 등에 관한 내용을 중점적으로 다룰 예정이다.

이와 같은 연구목적 및 범위를 중심으로 각 장에서 다루어질 구체적인 내용을 간략히 소개하면 다음과 같다. 먼저 본 장에서는 각국의 개인정보피해구제제도를 연구하게 된 배경으로 컴퓨터 등 정보처리기술의 발달과 정보사회의 출현, 개인정보침해의 증가, 이에 대처하는 각종 법제도를 발전시킨 주요국의 대처모습 등을 다루고 있다. 또한 본 연구를 행하는 목적 및 그 방법을 밝히도록 한다.

제2장에서는 본격적으로 국내외 개인정보피해구제제도를 조사하기에 앞서 먼저 선행되어야 할 기본 정의와 이론을 정립해보고자 한다. 따라서 먼저 오늘날의 정보사회에서 개인정보가 가지는 의미는 무엇인지, 개인정보와 프라이버시는 어떠한 관계에 있는지, 왜 개인정보를 보호하여야 하는지 그 개념과 보호의 필요성에 대하여 언급한다. 이어서 개인정보침해로 인해 입은 피해의 특수성, 피해구제 방법 중 하나인 소송외적 분쟁해결제도의 개념 및 개인정보와의 관련성, 효율적인 개인정보피해구제제도 확립의 필요성 등을 살펴보도록 하겠다.

제3장은 국내 개인정보피해구제제도 현황을 분석하는 과정이다. 먼저 국내 개인정보보호법의 제정현황과 주요내용을 살펴보고, 다음으로 국내 개인정보보호 및 피해구제 관련기구의 운영상황과 피해구제절차 및 방법 등을 살펴보기로 하겠다. 본 연구에서 언급할 개인정보관련 국내기구로는 개인정보분쟁조정위원회, 정보통신부, 행정자치부 개인정보보호심의위원회, 한국소비자보호원, 금융감독위원회, 경찰청사이버테러대응센터 등이다.

제4장은 국내에 이어 해외 주요국의 개인정보피해구제제도를 살펴보는 부분이다. 이 장에서는 먼저 개인정보와 관련된 OECD, UN, EU의 국제규범을 살펴보고 다음으로 유럽과 북미, 오세아니아, 아시아 지역 총 10개국의 개인정보피해구제제도를 검토한다. 주요 검토내용은 앞서 살펴본 연구범위를 중심으로, 각국의 개인정보보호법제 현황과 개인정보보호기구의 설치 및 운영상황, 개인정보피해구제 절차 및 방법이다. 이 장에서는 위와 같은 내용을 중심으로 각국의 피해구제제도 현황을 개괄적으로 설명하는 것으로 한다.

제5장에서는 제3장과 제4장에서 검토한 내용을 바탕으로, 각국의 개인정보피해구제제도를 상호 비교・분석한다. 개인정보보호기본법이 제정되어 있는지, 개인정보보호 전담기구가 설치되어 있는지, 개인정보보호기구의 성격과 기능・권한은 어떠한지, 소송외적 분쟁해결제도를 통한 개인정보피해구제제도의 차이점은 무엇인지 등을 중심으로 살펴보도록 한다.

제6장은 제5장에서 비교・검토한 내용이 국내 개인정보피해구제제도에 시사하는 바는 무엇인지, 국내 개인정보피해구제제도가 가지는 문제점은 무엇인지를 확인한다. 또한 국내 제도가 어떠한 방향으로 나아가야 할 것인지 및 보다 더 효율적인 개인정보피해구제제도의 확립과 정착을 위해서 필요한 사항은 무엇인지를 살펴보도록 한다.

마지막으로 제7장은 각 장에서 검토한 내용을 바탕으로 현대사회에서 개인정보가 가지는 중요성과 개인정보피해구제제도 확립의 필요성을 다시 한 번 언급하고, 국내 개인정보피해구제제도의 개선방안을 최종적으로 모색하여 정리하도록 하겠다.

제 3 절 연구방법

본 연구는 국내와 해외 주요국의 개인정보피해구제제도의 현황을 파악하고 이를 비교·분석하는 방법으로 진행된다. 먼저 국내외 피해구제제도의 정확한 현황 파악을 위해서는 문헌조사, 웹사이트 조사, 현장방문조사 등의 조사방법을 사용하였고, 이렇게 수집·정리·분석된 자료를 상호 비교함으로써 본 연구의 결론을 도출하였다. 각 연구방법에 대한 설명은 아래와 같다.

1. 문헌조사

가장 기본적인 연구방법으로 개인정보피해구제제도와 관련된 각종 국내외 문헌자료를 수집·정리·분석하는 방법을 활용하였다. 특히 법제도의 실체법적·절차법적 비교분석을 위해 각국의 개인정보보호법의 내용을 세밀히 검토하였으며, 기타 개인정보 및 프라이버시와 관련된 국내외 전문가들의 논문과 OECD, EU 등의 국제기구의 조사보고서 등을 참고하였다.

2. 웹사이트 조사

문헌조사와 함께 본 연구는 외국의 개인정보피해구제제도를 조사함에 있어 보다 정확한 최신의 정보를 수집하기 위해, 해당 국가의 개인정보보호기구 및 개인정보보호단체 등의 인터넷 웹사이트를 적극 이용하였다. 특히 웹사이트 조사는 외국의 개인정보보호기구의 설치근거, 주요 기능과 역할, 조직구성, 민원처리현황, 최근 개인정보 주요 이슈, 개인정보보호법제 현황 등을 파악하는데 있어 중요한 역할을 하였다.

3. 현장방문조사

문헌조사와 웹사이트 조사는 본 연구를 수행함에 있어 기본적으로 필요한 내용을 파악하는데 도움을 주었으나, 이를 통해서도 자세한 내용을 알아내기 어려운 점이 있었다. 이에 보다 더 살아있는 그리고 추가적인 정보를 파악하기 위해 직접 국내외 개인정보관련 기구를 방문조사하는 방법을 이용하였다. 국내 기구의 경우에는 한국소비자보호원, 금융감독원, 전자거래분쟁조정위원회, 대한상사중재원, 경찰청 사이버테러대응센터를 방문하여 각 기구에서 어떻게 개인정보피해구제의 역할을 하고 있는지 또는 소송외적 분쟁해결제도를 어떻게 활용하고 있는지 등을 조사하였다. 한편 직접 방문하기 어려운 해외 기구의 경우에는 현지유학생을 조사원으로 선정하여 필요한 조사항목을 의뢰하였으며, 독일 연방정보보호청과 캐나다 프라이버시커미셔너의 현지조사를 실시하였다. 주로 현지조사방법은 해당 기구 내 담당자와의 인터뷰 형식으로 진행되었으며, 그 외 각종 중요자료를 담당자로부터 건네받아 보다 구체적이고 정확한 내용을 조사할 수 있었다.

제 2 장 개인정보와 효율적 피해구제

제 1 절 인터넷 정보사회와 개인정보보호

컴퓨터의 보급과 이로 인한 대량적인 정보처리기술의 발달, 그리고 인터넷의 등장은 정보사회와는 분리할 수 없는 밀접한 연결고리를 가지고 있다. 또한 정보사회의 출현과 '개인정보' 또는 '정보프라이버시'라는 개념의 등장 역시 그러하다. IT의 획기적 발전은 인쇄술이라는 인류 최고의 발명을 컴퓨터로 대체하고 있으며, 종이에 수기로 기재되던 정보처리작업은 컴퓨터에 의한 대량 처리로 바뀌어가고 있다. 또한 인터넷의 발달로 전 세계의 컴퓨터가 하나로 연결되고 모든 인류가 '사이버세계'라고 하는 하나의 가상공간에 집결하는 것이 가능하게 되었다. 이러한 변화로 인하여, 과거 서류형태로 수집·보관되던 개인정보는 하나의 컴퓨터 안에 간단한 파일의 형태로 저장되어 쉽게 수정·이전·분류가 가능하게 되었고, 자연스럽게 많은 개인정보가 인터넷을 타고 사이버 가상공간에 모이게 되었다.

'개인정보'는 정보사회의 출현 이전에도 있었지만, 컴퓨터와 인터넷의 등장은 개인정보에 대해 사람들의 인식을 새롭게 바꾸고 있다. 특히 인터넷상에서는 개인정보가 '나'를 식별할 수 있는 구분인자의 역할을 하고 있어, 개인정보 자체가 바로 물리적인 나를 대신한다. 즉, 가상공간이 아닌 실제적 공간에서 물리적인 인간이 보호받고 존중받아야 할 존재인 것처럼, 인터넷이라는 가상공간에서 '나'를 대신하는 개인정보도 당연히 적절한 수준으로 보호받아야 할 대상이라는 인식이 차츰 퍼지게 된 것이다. 이같이 언제부터인가 사람들은 개인정보라는 개념을 인식하고 민감하게 다루어져야 할 성질의 것으로 받아들이기 시작하였는데, 이러한 경향은 20세기 후반 정보사회화가 진행되면서부터 더욱 뚜렷해지고 있다.

이렇듯 현대사회에서 개인정보는 하나의 중요한 의미와 가치를 가진 개념으로 떠오르고 있다. 그러나 아직까지 개인정보의 정확한 개념과 그 범주가 확정되지 못하고 다소 혼용되거나 여러 개념이 혼재되어 있는 것이 현실이다. 특히 개인정보는 적극적 의미의 프라이버시 개념과 아주 밀접한 관계에 있다고 할 수 있다. 따라서 개인정보와 프라이버시의 개념 및 양자의 관계, 인터넷 정보사회에서 개인정보가 가지는 의미 등을 살펴보는 것으로부터 본 연구를 시작해보고자 한다.

1. 프라이버시와 개인정보

사실 개인정보는 프라이버시와 깊은 관련을 가진다. 호주, 뉴질랜드, 미국, 캐나다 등의 경우 '프라이버시법(Privacy Act)'이라는 명칭을 가진 법률을 통해 개인정보의 오·남용을 규제하고 있는데, 이와 같은 예를 통해서도 양자가 얼마나 밀접한 관련을 가지고 있는지 알 수 있다. 그렇다면 프라이버시는 개인정보를 포함하는 개념인가. 먼저 프라이버시라는 개념이 어떻게 발생하였고 오늘날에는 어떠한 의미를 가지는지 살펴보도록 한다.

가. 프라이버시의 개념

프라이버시(Privacy)의 사전적 의미는 ① 다른 사람들의 주목이나 모임으로부터 떨어져 있는 상태, ② 다른 사람들의 주시 또는 모임을 피해 은둔하고 있는 장소, ③ 무슨 말을 했는지 또는 어떠한 행동을 하였는지를 드러내지 않는 것, ④ 사적인 일 또는 비밀을 뜻한다.[6] 이는 전통적인 프라이버시의 개념, 즉 '홀로 있을 권리(Right to be let alone)'를 의미하는 것으로 볼 수 있다. 이러한 프라이버시의 개념을 최초로 정립한 사람은 미국의 쿨리(T. M. Cooley) 판사이다.[7] 그러나 개인의 프라이버시를 보다

6) 웹스터 사전(Webster's Revised Unabridged Dictionary) 참조.

적극적으로 주장한 사람은 사무엘 워렌(Samuel D. Warren)과 루이스 브랜다이스(Louis D. Brandeis)이다. 당시 이들은 '황색 저널리즘'이라 불리던 선정적이고 감각적인 언론보도로 인하여 개인의 명예나 사생활이 심각하게 침해받고 간섭당하는 것을 비판하면서, '가장 포괄적인 권리이자 시민들에 의해 가장 가치 있는 것으로 인정받는 권리로서 일반적인 개인의 홀로 있을 권리'를 주장하였다.[8] 워렌과 브랜다이스의 프라이버시권에 대한 주장은 프라이버시를 '인간성 불가침의 원칙(Principle of inviolate personality)'에 의해 보호되는 하나의 권리로 인식하게 되는 결정적인 계기가 되었다.

그러나 "개인은 다른 사람의 간섭이나 이용으로부터 자신의 개인적이고 사적인 생활을 보호받을 자격을 가진다"[9]는 소극적인 의미가 강하였던 초창기 프라이버시의 개념은 20세기에 접어들면서 점차 복잡하고 다양한 의미로 변하게 된다. 이에 학자들은 종종 프라이버시의 개념을 정의하는 것 자체가 너무나도 어려운 작업이라고 실토하기도 한다.[10] 또한 '프라이버시'라는 개념 자체에 의미를 두는 것을 반대하고 비판하는 견해도 있다.[11] 그러나 대체적으로 프라이버시권을 인정하는 견해가 대두되어

---

7) 쿨리 판사는 1888년 저술한 '불법행위법에 관한 논문'을 통해 '홀로 있을 권리'를 언급하고 있다. T. M. Cooley, "A Treatise on the Law of Torts", 29, 2d ed., 1988. (심재훈, "미국의 프라이버시 보호와 침해 유형", 세계의 언론법제, 제12호, 2002. 12, 3면에서 재인용)

8) Samuel D. Warren/Louis D. Brandeis, "*The Right to Privacy*", Harvard Law Review, Vol. Ⅳ, No. 5, 1890. 12. 15. http://www.louisville.edu/library/law/brandeis/privacy.html

9) Gillmor/Barren/Simon/Terry, "*Mass Communication Law : Cases and Comment*", 5th ed., p. 281 (Defining Privacy & Personal Information, http://journalism.okstate.edu/faculty/jsenat/privacy/definition.html에서 재인용)

10) "프라이버시를 정의하기 위한 오랜 탐색작업은 종종 별 내용 없고 궁색한 그리고 가장 근본적인 사항에 대한 끊임없는 논쟁만을 발생시켰다."(R. Wacks(ed), "*Privacy*", Vol. 1, 1993, p. 17)

11) "프라이버시권은 없으며 프라이버시에 관한 어떠한 특별한 권리나 이익도 존재하지 않는다. 왜냐하면 사적인 것으로서 보호받아야 할 이익은 다른 수많은 이익이나 권리에 의해서도 설명될 수 있고 보호될 수 있기 때문이다. 그 중에서도 가장 대표적인 것이 재산권(property right)과 신체적 안전에 관한 권리(right to bodily security)이다." (J. Thompson, "*The Right to Privacy*", Philosophy and Public Affairs, Vol. 4, pp. 295~314), "개인의 프라이버시 보호로 인한 이익은 대부분 경제학적으로 비효율적

갔으며, 많은 학자들이 프라이버시에 대해 나름대로의 정의를 내리고자 노력하였다. 그 대표적인 예가 프로써(Prosser) 교수의 프라이버시에 대한 정의이다. 프로써 교수는 워랜과 브랜다이스의 프라이버시권 개념을 더욱 발전시켜 불법행위법을 바탕으로 프라이버시권에 대해 정의를 내리고자 시도하였다. 그는 프라이버시권의 네 가지 법익으로서 ① 개인의 격리된 공간이나 은둔지 또는 사적 생활에 대한 방해(Intrusion upon a person's seclusion or solitude, or into his private affairs), ② 개인에 관한 민감한 사적 사실의 대중적 공개(Public disclosure of embarrassing private facts about an individual), ③ 공중에게 오해를 불러일으킬 수 있는 부정확한 사실의 공표(Publicity placing one in a false light in the public eye), ④ 기타의 영리목적을 위한 타인의 성명이나 초상 등 신분의 무단 사용(Appropriation of one's name or likeness for the advantage of another)을 제시하면서, 위와 같은 법익이 침해당한 개인은 불법행위로 인해 입은 피해에 대한 배상을 청구하는 소송을 제기할 수 있는 권리를 가진다고 하였다.[12)]

프로써 교수 외에도 다양한 학자들이 프라이버시에 대한 개념을 정의하는 작업을 꾸준히 시도하였는데, 여기에는 자신과 관련된 정보에 대한 통제에 초점을 맞춘 것에서부터 인간 존엄성(Human Dignity)을 위해 필요한 보다 광범위한 법적 개념이라고 보는 입장까지 보다 다양한 양상을 띠고 있다. 이러한 다양한 프라이버시의 개념 정의를 크게 다섯 가지로 나누어 살펴보면 아래와 같다.

이다."(R. Posner, "*The Economics of Justice*", Harvard University Press, 1981), "프라이버시는 종종 여성이나 아동 등 사회적 약자에게는 유해하다. 프라이버시는 가정폭력을 방치함으로써 여성학대를 덮고 여성이나 아동에 대한 지배·통제·격하·침묵을 위한 보호막으로서 작용하기 때문이다."(C. MacKinnon, "*Toward a Feminist Theory of the State*", Harvard University Press, 1989)

12) W. L. Prosser, "*Privacy*", 48 California Law Review, 383, 1960.

〔표 2-1〕 다양한 프라이버시의 개념 정의

구분	개념 정의
인간존엄성 (Human Dignity)	프라이버시의 다양한 범주와 기준을 하나로 묶을 수 있는 개인프라이버시에 관한 일반이론을 만드는 것은 분명 가능하다. 이는 '손상될 수 없는 인격성(inviolate personality)'이라 불리는 모든 프라이버시 이익과 관련된 단일한 가치를 의미한다. 그러므로 프라이버시 침해는 인간 존엄성의 훼손으로 요약하여 이해할 수 있다.(Edward J. Bloustein, 1964)
사적 친근성 (Intimacy)	프라이버시는 인간이 존경, 사랑, 우정, 신뢰와 같은 친밀한 관계를 형성하는 것을 가능하게 하여 도덕적·사회적 인격성을 가지고 발달할 수 있도록 하는 기본적인 요소이다. 따라서 사적 친근성과 프라이버시는 밀접한 관련을 가지며, 프라이버시에 대한 위협은 인간의 본성에 대한 위협이다.(Fried, 1970 ; Gerety, 1977 ; Gerstein, 1978 ; Shoeman, 1984 ; Jule Inness, 1992)
사회적 관계 (Social Relationships)	프라이버시는 인간관계의 사적 친근성 뿐 아니라 전반적으로 다른 사람들과의 상호 인간관계를 향상시키는 데 있어 보다 중요한 개념이다.(Rachels, 1975)
제한적 접근 (Restricted Access)	프라이버시는 자신의 사적 영역에 대한 사람들의 접근을 배제하는 것을 의미한다. 프라이버시 보호는 권한없는 신체적 접근, 개인정보에 대한 보장받지 않은 접근, 불합리한 주목 등으로부터 개인을 보호하는 것이다. 그러므로 프라이버시 개념은 접근성의 제한으로 이해되어야 한다. 이에 의하면, 프라이버시는 비밀성(secrecy), 익명성(anonymity), 은둔(Solitude)과 같은 독립적인 요소들로 이루어진다.(Gavison, 1980 ; Sissela Bok, 1982 ; Anita Allen, 1988)
정보통제 (Cotrol over Information)	프라이버시란 자신에 관한 정보가 누구에게 언제 어느 정도까지 전해지는가를 결정할 수 있는 능력을 의미한다.(Westin, 1967) 대부분의 사람들은 일반적으로 이와 같은 능력을 행사하여 개인정보가 공개되지 않기를 선택하기 때문에, 다른 사람이 비문서화된 개인정보를 알고 있거나 보유하고 있는 상태는 곧 프라이버시 침해로 볼 수 있다.(Parent, 1983)

※ 참고 : Stanford Encyclopedia of Philosophy, "*Privacy*", http://plato.stanford.edu/entries/privacy

여기서 확인할 수 있는 것은 더 이상 프라이버시의 개념이 '홀로 있을 권리'에 머무르지 않는다는 것이다. 프라이버시를 보는 입장이나 시각은 각각 다르지만, 워랜과 브랜다이스 이후 20세기 후반 프라이버시 개념은 이미 단순히 간섭받지 않을 권리를 벗어나고 있음을 확인할 수 있다. 즉, '어떤 상황에서 어느 정도까지 다른 사람에게 자신을 노출시킬 것인지 또는 자신의 행동과 태도를 드러낼 것인지를 자유롭게 결정할 수 있는 권리'[13]가 강조되기 시작한 것이다.

한편 프라이버시가 이렇게 적극적인 의미로 변화하면서 오히려 그 개념 정의는 더욱 어려워졌다. 즉, 현대적인 의미의 프라이버시란 어느 정도의 범주를 가진 것이며 그 유형은 어떠한지 아직 확실히 정리된 바가 없는 것이다.

나. 프라이버시의 범주 및 유형

많은 학자들은 프라이버시 개념의 범주 또는 유형에 대해 서로 다르게 분류하고 있다. 가장 좁게 보는 입장은 앞서 살펴본 것처럼 프라이버시를 순수하게 자신의 정보에 대한 통제권만으로 보는 견해이다.[14] 이에 의하면, 프라이버시는 신체, 통신, 공간적 사생활 등의 개념과 완벽히 분리되며 사적 생활이나 가족적 생활과 관련된 중대한 개인적 결정을 할 수 있는 권능도 프라이버시의 범주에서 배제된다. 반면 프라이버시를 개인정보에 대한 통제가 아닌 자신의 사적 영역에 대한 타인의 접근을 통제하는 것으로 보는 견해도 있다. 이에 의하면, '국가에 의한 침해로부터의 개인의 자율적인 선택을 보호(Protection of individual autonomous choice from governmental interference)'하는 것은 프라이버시의 범주에서 배제된다.[15]

---

13) A. F. Westin, "*Privacy and Freedom*", Privacy and Freedom Atheneum, N. Y. 1967, p. 10.

14) W. Parent, "*Privacy, Morality and the Law*", Philosophy and Public Affairs 12, 1983, pp. 269-288. L. Henkin, "*Privacy and Autonomy*", Columbia Law Review, Vol. 74, 1974, pp. 1410~1433 ; R. Gavison, "*Privacy and the Limits of Law*", Yale Law Journal, Vol. 89, 1980, pp. 421~471 ; R. Bork, "*The Tempting of America : The Political Seduction of the Law*", Simon and Schuster (N.Y), 1990

그러나 대부분의 학자들은 프라이버시를 상당히 폭넓은 개념으로 이해하고 있다. 여기에는 개인정보에 대한 통제권 뿐 아니라 개인의 신체에 대한 통제권과 개인적 선택을 포함한다고 보는 입장[16], 자신에 관한 내적인 정보를 보호하고 접근을 통제하는 것은 물론, 사적인 친근한 관계를 보호하고 사적 행동에 관한 결정을 자유로이 내릴 수 있는 것을 모두 프라이버시의 범주에 포함시키는 입장[17], 다른 사람의 정보나 사적 결정과정에 대한 지나친 사회적 통제로부터의 보호를 프라이버시로 보는 입장[18] 등 다양한 견해가 있다. 한편 미국 연방대법원은 프라이버시를 자신에 관한 정보를 통제할 수 있는 권리와 특정한 중요사항에 대하여 결정할 수 있는 권능의 두 가지 범주로 구분하는 견해를 취하고 있다.[19] DeCew는 이러한 많은 학자들의 견해와 판례를 요약·정리하여 통제대상을 기준으로 크게 세 가지로 프라이버시의 범주를 밝히고 있다.

〔표 2-2〕 프라이버시의 범주

분류	내용
개인정보에 대한 통제	개인정보가 다른 사람에게 제공되거나 이용되는 것을 스스로 통제할 권리
접근통제	개인의 신체적·정신적 사항에 대한 타인의 접근여부를 통제할 권리
결정능력에 대한 통제	자신을 표현하고 다양한 상호관계를 형성하기 위해 중대한 가족생활이나 생활태도를 결정할 수 있는 능력을 통제할 권리

※ 참고 : J. DeCew, "*In Pursuit of Privacy : Law, Ethics, and the Rise of Technology*", Cornell University Press, 1997.

15) A. Allen, "*Uneasy Access : Privacy for Women in a Free Society*", Rowman and Littlefield, 1988.

16) J. Kupfer, "*Privacy, Autonomy and Self-Concept*", American Philosophical Quarterly, Vol. 24, 1987, pp. 81~89

17) J. Inness, "*Privacy, Intimacy and Isolation*", Oxford University Press, 1992.

18) F. Schoeman, "*Privacy and Social Freedom*", Cambridge University Press, 1992.

19) Whalen v. Roe, 429 U.S. 589, 1977.

한편, 프라이버시는 통제대상의 측면에서가 아니라 영역별로도 구분할 수 있다. 다음은 '전자프라이버시정보센터(Electronic Privacy Information Center)'와 '프라이버시인터내셔널(Privacy International)'의 분류이다.

〔표 2-3〕 프라이버시의 유형 (EPIC & PI)

분류	내용
신체 프라이버시 (Bodily Privacy)	압수수색이나 강제적인 마약테스트 등으로부터 자유로울 프라이버시
영역 프라이버시 (Territorial privacy)	집과 사무실 등 보호받아야 할 사적 영역에 대한 프라이버시
통신 프라이버시 (Privacy of Communications)	전화통화, 서신왕래 등의 자유에 관한 프라이버시로 통신비밀보호와 관련한 프라이버시
정보 프라이버시 (Information Privacy)	자신에 관한 정보의 이용·공개에 대하여 스스로 통제하고 개인정보에 접근할 수 있도록 허락할 것인지 여부를 결정할 수 있는 권한과 능력에 관한 프라이버시

※ 참고 : EPIC & PI, *"Privacy and Human Rights 2003 - An International Survey of Privacy Laws and Developments"*, http://www.privacyinternational.org/survey/phr2003

EPIC & PI는 전통적으로 사적 자유보호의 영역으로 이해되어 온 신체의 자유, 주거의 평온한 유지, 서신 등의 비밀보호를 각각 신체 프라이버시, 영역 프라이버시, 통신 프라이버시라 지칭하고, 여기에 정보프라이버시를 추가하고 있다.[20]

20) 로저 클라크(Roger Clarke)의 프라이버시 유형도 기본적으로는 EPIC & PI의 분류와 유사하다. 클라크는 프라이버시의 유형을 개인프라이버시(privacy of the person), 개인행동프라이버시(Privacy of personal behaviour), 개인통신프라이버시(Privacy of personal communications), 개인정보프라이버시(Privacy of personal data)로 구분하고 있는데, 이를 EPIC & PI의 분류와 비교해보면 개인프라이버시는 신체프라이버시와 유사하며 개인통신프라이버시는 통신프라이버시, 개인정보프라이버시는 정보프라이버시와 대응되는 개념이다. 다만, 개인행동프라이버시의 경우 EPIC & PI의 영역 프라이버시보다는 훨씬 넓은 개념으로 생각된다. 클라크는 이를 개인의 행동적 측면과 관련있는 프라이버시로, 특히 성적(性的) 기호나 습관, 정치적 활동, 종교 등과 같은 민감한 사항에 관한 '미디어 프라이버시'를 의미한다고 말하고 있다. (Roger Clarke, "*Introduction to Dataveillance and Information Privacy, and Definitions of Terms*", http://anu.edu.au/people/Roger.Clarke/DV/Intro.html)

다. 프라이버시와 개인정보의 관계

앞서 살펴본 것처럼 오늘날의 프라이버시 개념은 다양한 범주를 가진 폭넓은 가치 개념이다. '은둔', '배제' 등의 단어로 표현되던 과거의 소극적인 의미의 프라이버시뿐 아니라 적극적으로 요구할 권리, 통제할 권리, 결정할 권리를 포괄하고 있기 때문이다.

이 중에서도 최근 가장 주목받고 있는 것은 정보프라이버시이다. EPIC & PI의 프라이버시 유형 분류를 보아도 정보프라이버시는 현대적 의미의 프라이버시 개념에 있어 중요한 한 축을 이루고 있다. 이러한 정보프라이버시는 정보화의 진행과 더불어 1960년대부터 본격적으로 논의되기 시작한 것으로, 자신과 관련된 정보의 이용 및 공개에 대하여 스스로 통제하고 누구에게 자신과 관련된 정보에 접근할 수 있도록 허락할 것인지 여부를 결정할 수 있는 권한과 능력에 관한 프라이버시를 의미한다.[21] 즉, 정보주체가 자신의 정보에 대하여 가지는 개인정보자기결정권(Recht auf informationelle Selbstbestimmung)이 그 핵심이다. 이런 점에서 정보프라이버시는 개인정보와 아주 밀접한 관련성을 가진다고 볼 수 있다. 정보프라이버시는 개인정보에 대한 정보주체의 권리와 일맥상통하는 것으로 볼 수 있기 때문이다.

그러나 최근 실무적으로는 개인정보 및 개인정보보호라는 가치가 강학상의 또는 이론적인 정보프라이버시라는 개념을 벗어나 독자적인 의미를 가지는 방향으로 나아가는 듯하다. 각국의 법률에서도 프라이버시라는 개념이 주로 국가나 정부 등 공공영역으로부터의 자유 및 권리행사와 관련하여 주로 사용되고 있는 반면, 최근에는 이러한 공공부문과 민간부

---

21) Anne Cavoukian/Tyler J. Hamilton, "*Privacy Payoff - How Successful Business Build Customer Trust*", McGraw-Hill Ryerson, 2002, p.38. 국내 판례에서도 "헌법 제10조와 제17조는 인간으로서의 존엄과 가치 및 사생활의 비밀과 자유를 규정하고 있는 바, 이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다"고 하여, 이와 같은 취지에서 정보프라이버시의 개념을 언급한 바 있다.

문을 통틀어 정보(information) 또는 데이터(data)에 초점을 두어 '정보보호(data protection)' 또는 '개인정보보호(personal data protection 또는 personal information protection)'라는 용어를 사용하는 예가 증가하고 있다.[22] 이러한 경향의 주된 이유는 바로 개인정보가 프라이버시권과 관련하여 파생되고 강조된 개념이기는 하나 반드시 양자가 일치한다고 보기는 어렵기 때문이다. 즉, 프라이버시라는 용어는 기본적으로 보호받아야 할 대상이라는 가치가 내재되어 있지만 개인정보는 그 자체가 가치중립적인 용어이다. 정보가 곧 자원이자 경쟁력인 정보사회에서 개인정보는 보호대상임과 동시에 이용의 대상이기도 하기 때문에, 개인정보보호는 프라이버시권 보호와는 기본전제부터 상이한 특성을 가지는 것이다. 특히 프라이버시는 기본적으로 양도할 수 없는 불가침의 인격권이라는 측면에서 보호받는 대상이나, 개인정보는 반드시 인격권적 측면만 가지고 있다고 보기는 어렵다. 예를 들면, 미국에서는 개인정보를 재산권의 일부로 해석하는 경향이 있는데[23], 개인정보가 정보사회에서 하나의 자산으로서 재산적 가치를 가질 수 있는 것이고 일종의 계약과 같이 본인이 스스로 개인정보의 수집・이용・처리를 허용할 수 있다는 점을 고려하면 충분히 가능한 해석이다.[24] 따라서 오늘날에는 프라이버시의 한 영역으로서 개인

---

22) 영국(Data Protection Act), 독일(Bundesdatenschutzgesetz), 프랑스(Loi relative à l'informatique, aux fichiers et aux libertés), 스페인(Ley Organica 15/1999, de 13 de diciembre de Proteccion de Datos de Caracter Personal) 등 세계 주요국은 법령명에도 '프라이버시(privacy)'보다는 '정보(영국의 경우 data, 독일의 경우 daten, 프랑스의 경우 informatique, 스페인의 경우 Datos)'라는 용어를 선택하여 사용하고 있다.

23) 찰라포스키(Francis S. Chlapowski)는 프라이버시를 재산권의 일부로 보는 견해를 취하고 있는데, 그에 의하면 '개인정보는 인격(personality)의 한 측면일 뿐 아니라 하나의 객체'이기도 하다. 따라서 모든 사람은 재산권의 일부로서 자신의 모든 물건, 즉 객체를 통제하고 지배할 권리를 향유한다고 한다. Francis S. Chlapowski, "*The Constitutional Protection of Informational Privacy*", Boston University Law Review, vol. 71, 1991. 1. p. 133 (Fred H. Cate, "*Privacy in the Information Age*", Brooking Institution Press, 1997, p. 21에서 재인용)

24) 그러나 개인정보를 순수하게 재산적 가치로만 판단하여 개인정보침해를 전적으로 재산권 침해로만 볼 수는 없다. 왜냐하면 재산권적 입장에서 개인정보를 바라볼 경우, 개인정보를 순전히 금전적 가치를 가진 일종의 재화 또는 서비스로서 거래가 가능한 대상으로만 인식할 위험이 있기 때문이다. 따라서 개인정보는 인격권적 측면과 재산권적 측면이 모두 공존하는 것으로 보아야 한다.

정보보호를 논하는 경향에서 더 나아가, 개인정보의 이용가치와 보호가치를 조화시키는 목적범위 안에서 개인정보에 대한 정보주체의 권리나 이익 또는 정보처리자의 의무 등의 사항을 규정하고 보다 구체화시키는 방향으로 나아가고 있다.

결론적으로 개인정보와 프라이버시는 단편적으로 동일한 개념으로 볼 수는 없으며, 특히 프라이버시 개념을 본래의 의미로 좁게 해석할 때는 더욱 그러하다. 왜냐하면 개인정보는 넓은 의미의 프라이버시의 한 유형인 정보프라이버시와는 거의 동일선상에서 해석될 수 있지만, 통신비밀 침해, 신체·주거 등에 대한 부당한 압수·수색 등과 같은 기타의 프라이버시 영역과는 관련성이 떨어진다고 할 수 있기 때문이다. 즉, 개인정보는 프라이버시의 한 유형인 정보프라이버시의 핵심적인 개념요소로 볼 수 있다. 다만, 최근에는 이러한 정보프라이버시권을 이루는 핵심요소로서의 개인정보가 하나의 가치와 의미를 가지는 독자적인 개념으로 변화하고 있는 추세에 있다. 이하에서는 이러한 개인정보의 개념과 그 의미를 살펴보도록 하겠다.

2. 개인정보의 개념

개인정보의 개념이 무엇인가에 대해서는 다양하게 제시되고 있다. 가장 넓은 의미에서 개인정보란 '개인의 건강상태, 신체적 특징, 사상이나 신념과 같은 정신세계, 학력·경력·재산상태, 사회적·경제적 지위 등 개인에 관한 사실·판단·평가를 나타내는 모든 정보'를 의미한다.[25] 따라서 이에 의하면 생존하고 있는 自然人에 관한 정보 뿐 아니라 法人의 정보, 死者의 정보도 개인정보의 개념에 포함된다.

그러나 위와 같은 넓은 의미에서의 개인정보가 모두 '보호대상으로서의 개인정보'의 개념에 해당되는 것은 아니다. 보호되어야 할 대상으로서의

25) Wacks는 "개인정보는 개인이 사적이고 비밀스러운 것으로 취급되기를 합리적으로 기대할 만한 개인과 관련된 모든 사실, 통신 또는 의견이어서, 사람들은 그러한 개인정보의 유통을 허락하지 않거나 적어도 제한하고 싶어한다"고 하였다. (R. Wacks, supra note 10)

개인정보를 결정짓는 중요한 판단기준은 개인의 식별가능성 여부이다. 따라서 이에 의하면 개인정보란 '식별된 또는 식별가능한 개인에 관한 정보'를 의미한다. 이러한 의미의 개인정보에는 직접적으로 식별이 가능한 개인정보 뿐 아니라 간접적으로 식별이 가능한 개인정보도 모두 포함된다. 전자는 당해 정보만으로도 직접 개인을 식별할 수 있는 정보로서 대체로 얼굴(초상), 이름, 주민등록번호, 지문, 홍채, 운전면허번호 등이 이에 해당된다. 또한 후자는 당해 정보만으로는 특정 개인을 식별할 수 없으나 다른 정보들과 결합하여 용이하게 당해 개인을 식별할 수 있는 정보를 의미한다. 여기에는 주소, 전화번호, 직장, ID, 비밀번호, 소속, 성별, 나이 등이 해당된다.

한편 더 나아가 공개되지 않아 이용가능하지 않은 데이터만을 보호대상으로서의 개인정보로 보는 경우도 있다. 즉, 개인정보의 개념을 결정짓는 핵심적인 요소로서 정보와 개인과의 관련성 및 정보주체의 식별가능성 뿐 아니라 공개적으로 이용할 수 없는 정보일 것을 요구하는 것이다. 주로 사업자 협회에서 마련한 개인정보보호 가이드라인이나 규약에서 이러한 개념 정의를 찾아볼 수 있는데, 이에 의하면 개인정보란 '공개적인 통로를 통해서 이용가능하지 않은 데이터'[26] 또는 '파일에서 개인과 연결되어 있는 정보로서 공개적으로 이용할 수 없거나 찾아낼 수 없는 정보'[27]를 의미한다고 한다.[28]

---

26) 미국 정보오락광고협회(CASIE : Coalition for Advertising Supported Information and Entertainment)의 개인정보 개념 정의이다.

27) 미국 다이렉트 마케팅협회(DMA)의 개인정보보호 가이드라인상의 정의이다. 이러한 사업자협회의 주장은 미국 정부의 입장에도 상당부분 영향을 미치고 있다. 실제로 APEC 프라이버시 원칙(APEC Privacy Principles) 제정과정에서 미국 상무부는 개인정보의 개념에서 공개적으로 이용가능한 개인정보(publicly available information)는 제외하자는 주장을 굽히지 않고 있다.

28) "*Defining Privacy & Personal Information*", http://journalism.okstate.edu/faculty/jsenat/privacy/definition.html

［표 2-4］ 개인정보의 개념

범위	개념	개념요소
최광의	개인에 관한 사실·판단·평가를 나타내는 모든 정보	관련성
광의	식별된 또는 식별가능한 개인에 관한 정보	식별가능성
협의	공개되지 아니한, 식별가능한 개인에 관한 정보	공개여부

이렇듯 개인정보의 개념은 다양하지만, 일반적으로 개인정보란 '개인에 관한 정보로서 당해 개인을 식별할 수 있는 정보'를 의미하고 있다. 이는 개인정보관련 국제규범에서 정의하고 있는 개인정보의 개념을 통해서도 알 수 있으며, 현재 대부분의 국가들도 이러한 국제규범상의 개념을 바탕으로 자국의 국내법에서 개인정보를 정의하고 있다. 이러한 국제규범과 각국의 국내법 등의 법규범에서 규정하고 있는 개인정보의 정의를 살펴보면 다음과 같다.

［표 2-5］ 해외 법규범 속에서의 개인정보의 개념정의

구 분	개인정보의 개념
OECD 가이드라인 제1조b)항	식별된 또는 식별가능한 개인에 관한 정보 일체
EU 지침 제2조(a)항	식별된 또는 식별가능한 자연인(natural person)(정보주체)에 관한 모든 정보
영국 정보보호법 제1조(1)항	신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터(data) 또는 정보관리자가 보유하고 있거나 앞으로 그러할 가능성이 높은 기타 정보(information) 또는 데이터로부터 신원이 확인가능한 생존개인과 관련된 데이터
프랑스 정보처리축적및자유에관한법률 제4조	형식에 관계없이 직접 또는 간접으로 개인을 식별할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보
독일 연방정보보호법 제3조	신원이 확인되었거나 확인 가능한 정보주체의 인적·물적 환경에 관한 일체의 정보
호주 프라이버시법 제6조	당해 정보(information) 또는 의견(opinion)으로부터 신원이 명백하거나 확실시될 수 있는 개인에 관한 정보 또는 의견으로서, 데이터베이스에 포함된 정보 또는 의견을 포함하며 해당 정보가 진실인지 여부 및 물질적 형태(material form)로 기록되어 있는지 여부와 관계없다

캐나다 프라이버시법 제3조	모든 형식으로 기록된 신원을 확인할 수 있는 개인에 대한 정보
홍콩 개인정보법 제2조	생존하는 개인과 직·간접으로 관련된 모든 데이터로서, 개인의 신원을 직·간접적으로 확인하기 위해 사용할 수 있는 데이터 및 데이터 접근 또는 처리가 가능한 형식의 데이터

이처럼 각국의 법률에서 규정하고 있는 개인정보의 개념은 기본적으로 '식별된 또는 식별가능한 개인에 관한 모든 정보'를 의미한다. 다만, 영국과 같이 명백히 생존하고 있는 개인에 관한 정보일 것을 요구하는 경우도 있고, 홍콩의 예처럼 개인정보에 대한 접근 또는 처리가 실행될 수 있을 것(practicable)을 요구하여 보다 구체화한 경우도 있다. 또한 호주의 경우에는 개인정보인지 여부를 판단하는 데 있어 해당 정보의 진실성이나 기록형식은 관계가 없음을 명시적으로 밝히고 있다. 즉, 개인정보에 대한 법적 정의는 일반적으로 OECD 프라이버시 가이드라인[29]이나 EU 지침[30]과 같이 개인과 정보와의 관련성 및 개인의 식별가능성을 기본으로 하고 있다. 다만 각 국가별로 추가적으로 자연인에 관한 정보인지 여부, 개인의 생존여부, 개인정보가 기록된 형식 등의 요소가 기준으로 작용할 수도 있다.[31]

국내법상 개인정보의 개념도 대체로 이와 유사하다. 즉, 현재 한국의 공공부문과 민간부문을 대표하는 개인정보보호법인 「공공기관의개인정보보호에관한법률(이하 '공공기관개인정보보호법'이라 함)」 및 「정보통신망이용촉진및정보보호등에관한법률(이하 '정보보호법'이라 함)」에서는 개인정보의 개념을 아래와 같이 정의하고 있다.

---

29) 개인정보의 국경간 이동과 프라이버시보호에 관한 가이드라인 (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980)

30) 개인정보의 보호 및 자유로운 이전에 관한 유럽의회와 이사회 지침 (DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)

31) 각국의 다양한 개인정보의 법적 개념에 대해서는 제5장에서 보다 자세하게 비교해보도록 한다.

〔표 2-6〕 국내법상 개인정보의 개념정의

공공기관개인정보보호법 제2조제2호	정보보호법 제2조제1항제6호
생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 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)	생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

공공기관개인정보보호법과 정보보호법에서 규정하고 있는 개인정보의 개념은 대체로 비슷하다. 양자 모두 개인의 식별가능성을 개인정보 개념의 핵심요소로 삼고 있을 뿐 아니라 생존하고 있는 개인에 관한 정보일 것을 규정하고 있다. 또한 당해 정보만으로 개인을 식별할 수 없을지라도 다른 정보와 용이하게 결합하여 개인을 식별할 수 있으면 개인정보에 해당된다고 하고 있다. 그러나 전자의 경우에는 '당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여' 당해 개인을 식별할 수 있는 정보라고 하여 개인정보의 범위를 다소 한정하고 있다. 이는 동법이 기본적으로 공공기관에 의해 컴퓨터로 처리되는 정보에만 적용된다는 점에서 법률의 보호대상인 개인정보의 개념도 다소 제한적으로 규정한 것이 아닌가 싶다. 이에 반해 정보보호법은 정보통신망에서의 개인정보 처리를 규율하는 것이 원칙이기는 하나 이에 한정하지 않고 부분적으로 오프라인을 통한 개인정보 수집·이용·제공 등의 행위에도 적용되기 때문에, 공공기관개인정보보호법보다는 넓은 의미의 개인정보의 개념을 가지고 있다. 또한, 민간영역에서 다양하게 이용될 수 있는 개인정보의 구체적 형태를 '당해 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보'라고 하여 비문자적 정보도 개인정보에 해당됨을 명백히 하고 있다. 이러한 정보보호법상의 개인정보의 개념을 바탕으로 개인정보의 유형 및 구체적 예를 살펴보면 다음과 같다.

〔표 2-7〕 개인정보의 유형 및 구체적 예

구분		구체적 예
일반정보	일반정보	이름, 주민등록번호, 주소, 전화번호, 생년월일, 출생지, 이메일주소, ID/PW, 가족관계 및 가족구성원의 정보, IP주소 등
신체적 정보	신체정보	얼굴, 지문, 홍채, 음성, 유전자정보, 키, 몸무게 등
	의료・건강정보	건강상태, 진료기록, 신체장애, 장애등급 등
정신적 정보	기호・성향정보	도서・비디오 대여기록, 잡지구독정보, 여행 등 활동내역, 식료품 등 물품구매내역, 인터넷 웹사이트 검색내역 등
	신념・사상정보	종교 및 활동내역, 정당・노조 가입여부 및 활동내역 등
재산적 정보	개인금융정보	소득정보, 신용카드번호 및 비밀번호, 통장계좌번호 및 비밀번호, 동산・부동산 보유내역, 저축 내역 등
	신용정보	개인신용평가정보, 대출 또는 담보설정 내역, 신용카드 사용액 등
사회적 정보	교육정보	학력, 성적, 출석상황, 자격증 보유내역, 상벌기록, 생활기록부 등
	법적정보	전과・범죄 기록, 재판 기록, 과태료 납부내역 등
	근로정보	직장, 고용주, 근무처, 근로경력, 상벌기록, 직무평가기록 등
기타	통신정보	전화통화내역, 인터넷 웹사이트 접속내역, 이메일이나 전화메시지 등
	위치정보	IP주소, GPS 등에 의한 개인위치정보
	병역정보	병역여부, 군번, 계급, 근무부대 등

3. 개인정보의 활용과 보호

개인정보의 개념정의와 특성 및 프라이버시와의 차별성을 살펴보는 과정은 현대 정보사회에서 개인정보의 중요성에 대해 재인식하는 기회가 되었다. 이제 다시 본 논문의 원점으로 돌아와 왜 개인정보를 보호하여야 하고 개인정보로 인해 입은 피해를 구제해야 하는지를 상기시킬 필요가 있겠다.

오늘날에는 정보화로 인하여 사람들의 관심이 개인정보로 집중되고 있음은 이미 언급한 바와 같다. 기업들은 마케팅을 위해 보다 많은 고객 정보를 확보하려 하고, 정부는 보다 쉽고 편리한 행정서비스의 제공을 위해 단편적인 개인정보를 하나로 통합시키는 시스템을 구축하려 한다. 반면 정보주체인 개인은 개인정보의 이용이 증가하는 만큼 늘어나는 개인정보 오·남용에 대해 예의주시하고 있다. 또한 기업을 평가함에 있어서도 고객의 개인정보를 얼마나 소중히 관리하고 보호하는지 여부를 중요한 잣대로 삼고 있으며, 더 나아가 국가에 대하여 자신의 개인정보를 보호하기 위한 법적·제도적 시스템을 도입하여 시행하도록 요구하는 등 보다 적극적인 태도를 보이고 있다. 이러한 변화는 개인정보 처리의 대량성·용이성 등으로 인하여 개인정보침해가 증가하였기 때문이기도 하지만, 일반 정보주체들의 개인정보에 대한 인식 자체가 변화하였기 때문이다. 따라서 개인정보보호를 위한 제도를 확립하고 철저히 시행하는 것은 이미 시대적·국가적 과제가 되고 있다.

그러나 개인정보는 오늘날과 같은 디지털 정보사회에 있어서는 그 이용을 전면적으로 배제할 수 없다는 특성을 가지고 있다. 만약 타인이나 국가가 개인정보를 전혀 사용하지 못하게 막는다면, 당장 현대인들은 아무것도 할 수가 없을 것이다. 만약 자신의 개인정보를 전혀 외부에 제공하지 않고 그들이 이용할 수도 없도록 하고자 한다면, 오늘날과 같은 정보사회에서는 말 그대로 '은둔생활'을 감수해야 할 것이다. 그러므로 무조건적으로 개인정보를 이용하는 행위를 금지하거나 불법적인 것으로 취급해서는 안 된다.

개인정보는 칼날의 양 끝과 같다. 개인정보의 활용이 불가피한 반면 그러한 활용은 필연적으로 개인정보침해를 불러오고 있는 것이다. 여기서 중요한 것은 개인정보의 적정한 활용과 안정적인 보호의 균형의 추를 맞추는 일이 될 것이다. 개인정보보호는 개인정보의 적정한 수준의 활용을 보장할 수 있을 정도여야 하며, 개인정보의 활용은 개인정보보호를 위한 안전한 틀을 갖춘 상태에서 이루어져야 한다. 이러한 균형감각을 가지고 개인정보를 이해하는 것이 무엇보다도 필요한 시점이다. 다만, 오늘날의

현실은 아직까지 개인정보 활용의 필요성이나 당면성에 대해서는 관심이 많지만 이를 적절히 보호하여야 한다는 인식은 다소 부족하다고 할 것이다. 이러한 배경에서 최근에는 개인정보보호를 위한 제도 확립에 대해서 많은 사람들의 관심이 집중되고 있는 것이다.

개인정보보호를 위한 제도 확립에는 사전적 기틀마련과 사후적 보완장치의 확립이라는 두 가지 측면이 있다. 전자는 개인정보보호를 위한 법규범을 확고히 하고 사업자와 공공기관 등 개인정보를 많이 취급하는 단체 등의 개인정보보호 인식을 강화하는 행위 등을 의미하며, 후자는 개인정보침해가 발생할 경우 그로 인한 피해를 최소화하고 구제하기 위한 제도적 장치를 의미한다. 이 중 사후적 제도는 정보주체들이 자신들의 개인정보에 관한 권리를 보다 적극적으로 행사하려는 최근의 경향을 고려해보면, 더욱 중요한 것으로 강조될 수 있는 부분이다.

현대인들은 더 이상 개인정보가 불법적인 방법으로 수집되어 사용되거나 자신이 통제할 수 있는 범위를 넘어서 다른 사람에게 제공 또는 공개되는 등의 개인정보침해를 용납하지 않고 적극적으로 그 위법성과 부당성을 주장하고 있다. 그러나 만약 개인정보침해로 인한 피해를 사후적으로 구제해줄 수 있는 법적 장치가 미약하다면, 적절한 시기와 방법으로 정보주체의 권리를 보호할 수 없을 것이고 개인정보침해를 효과적으로 방지할 수도 없을 것이다. 따라서 법률의 제·개정 외에도 개인정보피해 구제를 위한 제도적 장치를 도입·시행할 필요가 있는 것이다.

제 2 절 개인정보 분쟁해결과 피해구제

1. 개인정보피해구제의 개념

넓은 의미에서의 피해구제제도는 민사·형사·행정적 피해구제를 모두 포괄하는 개념으로 볼 수 있다. 침해행위나 위법행위로 인해 입은 피해를 손해배상 등의 민사적 수단으로 구제해주는 것이 민사적 피해구제 방법이고, 형벌이 부과될 수 있는 위법행위에 대하여 검찰이나 경찰에 고소·고발이 있을 경우 형사소송 등을 통해 징역 또는 벌금 등의 형사제재조치를 부과하는 것이 형사적 피해구제 방법이다. 또한 행정적 피해구제는 위법행위에 대하여 감독행정기관에 신고가 접수될 경우 이를 조사하여 과태료를 부과하거나 시정명령을 내리는 등 행정조치를 부과하는 것을 의미한다.

〔표 2-8〕 광의의 피해구제제도의 개념 및 유형

분류	의미	담당기관
민사적 피해구제	손해배상결정 등 민사적 구제	법원, 민간·공공 분쟁해결기구
형사적 피해구제	형사고발 등으로 형벌 부과	법원, 검찰, 경찰
행정적 피해구제	과태료, 시정명령 등 행정처분 부과	감독행정기관

이렇게 피해구제제도의 의미를 넓게 생각하면, 형사기관이나 행정기관에 의한 형사적·행정적 제재도 그 범위에 포함된다 할 것이다. 침해자에 대한 제재가 간접적인 구제방법이 될 수도 있기 때문이다.[32] 그러나 흔히 피해구제라 함은 위법 등 침해행위로 인해 발생한 피해에 대하여 손해배상결정 등을 하는 민사적 피해구제를 의미하는 것이 일반적이다. 형벌

32) 물론 행정적 제재수단으로 과태료 부과를 제외한, 시정명령이나 원상회복명령 등의 행정명령은 침해행위를 제거하는 실질적인 구제수단이 될 수도 있다.

이나 행정벌 부과는 말 그대로 침해행위자에 대하여 부담적 행위로서 제재를 부과하는 측면이 강하지만 손해배상 등은 피해자가 입은 실질적 피해에 대하여 대가를 제공해 준다는 점에서 구제의 측면이 강하기 때문이다.

따라서 주된 피해구제 역할을 담당하는 것은 법원이며, 이는 민사소송을 통해 이루어진다. 통상 법원이 제공할 수 있는 구제방법으로는 손해배상, 원상회복, 강제조치, 확인판결 등이 있으며 강제조치에는 금지명령이나 이행명령 등이 포함된다.[33] 그러나 모든 분쟁을 법원의 소송절차를 통해서만 해결하려고 한다면, 소송적체로 인한 법원의 부담이 상당히 가중될 것이 명백할 뿐 아니라 소송지연으로 인해 피해구제의 실효를 담보하기 어려울 것이다. 이러한 의미에서 소송에 의한 분쟁해결수단을 갈음할 수 있는 대안적 분쟁해결제도 또는 소송외적 분쟁해결제도(ADR : Alternative Dispute Resolution Systems)가 새롭게 부각되고 있다.

2. 소송외적 분쟁해결제도

가. 소송외적 분쟁해결제도의 의의

소송외적 분쟁해결제도는 공식 소송절차를 거치지 않고 중재, 조정, 화해, 알선 등의 방법을 통해 분쟁을 해결하는 것을 의미한다. 여기에는 법관이 중재자로 관여하는 것은 물론, 행정기관이나 공공기관 또는 기타 민간단체가 소송에 앞서 분쟁을 쉽고 간편하게 해결하는 활동도 포함된다. 따라서 일반적으로 소송외적 분쟁해결제도라고 하면 '법정 밖에서 분쟁을 해결하는 모든 수단'을 의미한다.[34]

---

33) 이러한 민사소송을 통한 법원의 피해구제수단은 사실상 각국의 법제도에 따라 차이가 있다. 예를 들면, 한국의 경우 민사적 피해구제수단은 원칙적으로 경제적·정신적 피해에 대한 손해배상만이 가능하다. 반면 미국의 경우 실질적 피해가 없더라도 위법행위에 대한 징벌적 손해배상을 법원이 명령할 수 있다. 또한 개인정보피해구제를 위해 법원이 결정할 수 있는 구제수단의 종류와 방법에 대해서도 각 국가별로 다소 차이가 있다.

이러한 소송외적 분쟁해결제도는 전통적인 분쟁해결제도인 소송의 지나친 형식성, 과도한 비용부담, 신속한 피해구제의 곤란함 등을 보완할 수 있다는 점에서 각광받고 있다. 특히 소송은 당사자 쌍방간의 반복적이고 계속적인 항소를 야기할 수 있고 오랜 시간동안의 다툼으로 인해 상호간에 감정적 대립을 증대시키고 분쟁을 극단으로 치닫게 하는 것에 비해, 소송외적 분쟁해결제도는 근본적으로 당사자가 모두 만족할 수 있는 원만한 합의점을 찾는 것에 중점을 둔다는 점에서 소송을 갈음할 수 있는 대안적인 분쟁해결제도로 부각되고 있다. 즉, 소송외적 분쟁해결제도는 신속성, 간편성, 전문성, 접근용이성, 저비용, 비밀유지, 절차의 비형식성과 신축성, 조리에 따른 분쟁해결, 개별 사안에 대한 구체적 타당성 확보, 분쟁해결 전반에 대한 당사자의 통제가능성, 분쟁해결 이후 당사자간 우호적인 관계유지 등의 장점을 가지고 있다. 반면, 소송외적 분쟁해결제도는 극심한 감정적 대립이 심한 분쟁에는 적합지 않으며 강제성이 부족해 이행확보에 어려움이 있다는 한계도 있다.

나. 소송외적 분쟁해결제도의 유형

소송외적 분쟁해결제도는 구속력 여부, 제3자의 개입 여부, 분쟁 당사자의 주도적 역할 여부 등에 따라 그 형태나 기법이 다양하다. 따라서 소송외적 분쟁해결제도를 구분하는 방법도 천차만별이다. 먼저 호주의 '소송외적 분쟁해결제도 자문위원회(NADRAC : National Alternative Dispute Resolution Advisory Council)'는 분쟁 당사자 사이에 개입하는 제3자가 어느 정도의 권한을 가지고 있는지를 중심으로 소송외적 분쟁해결제도를 구분하고 있는 바, 이를 살펴보면 아래와 같다.

---

34) Hakim Ben Adjoua, "*Electronic Alternative Dispute Resolution*", 2000, http://www.paralegals.org/Reporter/On-line00/adr.htm

［표 2-9］소송외적 분쟁해결제도의 유형 Ⅰ(NADRAC)

분류	내용	예
지원 절차적 ADR (Facilitative process)	분쟁 당사자가 쟁점을 상호 확인하고 새로운 선택방안이나 대안을 개발하여, 합의에 도달할 수 있도록 도와주는 절차	지원협상(facilitated negotiation), 지원(facilitation), 調整(mediation)
권고 절차적 ADR (Advisory process)	분쟁의 사실관계나 법률에 대하여 조언하고 가능한 또는 바람직한 결론을 제시하는 절차	전문가 감정 (expert appraisal), 간이심리(mini-trial)
결정 절차적 ADR (Determinative process)	당사자로부터 공식적인 증거수집 및 의견청취 등의 절차를 통해 분쟁을 평가하고 결정을 내리는 절차	중재(arbitration), 전문가 결정(expert determination), 사적 재판(private judging)
복합적 형태의 ADR (Combined or hybrid process)	절차의 초기에는 당사자간 논의를 원활히 하도록 도와주거나 자문 등의 조정을 행하다가 후기에는 중재 등 다른 방법을 함께 이용하는 절차	조정-중재(med-arb)

※ 참조 : NADRAC, "*What is ADR?*", http://www.nadrac.gov.au

미국의 '민주주의통치센터(CDG : Center for Democracy and Governance)'도 NADRAC의 분류와 유사하게 '결과를 만들어내는 과정에서 제3자가 행하는 역할이 무엇인가'를 기준으로 소송외적 분쟁해결제도를 구분하고 있다. 즉, CDG에 의하면 소송외적 분쟁해결제도는 제3자의 개입이나 지원이 전혀 없는 협상(Unassisted negotiation), 제3자가 개입하여 분쟁해결과정을 지원하나 해결방안을 권고하지는 않는 형태의 지원협상(Facilitated negotiation - No advisory opinion), 제3자가 개입하여 분쟁해결방안을 당사자에게 권고하는 형태의 지원협상(Facilitated negotiation - Advisory opinion), 제3자의 결정이 당사자에게 구속력 있는 분쟁해결방안이 되는 구속력 있는 의견(Binding opinion)의 네 가지로 구분될 수 있다고 한다.[35]

35) Center for Democracy and Governance, "*Alternative Dispute Resolution Practitioner's Guide*", Appendix A, Technical Publication Series, 1998. 3.

［표 2-10］ 소송외적 분쟁해결제도의 유형 Ⅱ(CDG)

구분	의미	예
당사자간 협상	제3자의 개입이나 지원이 없는 순수한 당사자간의 분쟁해결	협상
지원협상 (제3자의 권고 無)	제3자가 개입하여 분쟁해결을 지원하나 해결방안을 권고하지는 않음	화해, 調整
지원협상 (제3자 권고 有)	제3자가 개입하며 실질적으로 분쟁해결 방안을 분쟁 당사자에게 권고	비구속적 중재
구속력 있는 의견제시	제3자가 당사자에게 구속력있는 분쟁해결방안을 결정	구속적 중재

※ 주 : 흔히 우리나라에서는 비구속적 중재(Non-binding arbitration)를 '조정(調停)'이라 한다. 그러나 이는 '조정(調整)'과는 구분되는 것으로 볼 수 있다. 전자는 제3자가 적극적으로 당사자에게 해결방안을 권고하나, 후자는 단지 분쟁의 사실관계를 정리하고 당사자간 의견교환을 원활히 하여 분쟁해결을 지원·알선하는 것을 의미하기 때문이다.

한편 CDG는 소송외적 분쟁해결제도를 기본적 형태의 분쟁해결 모델과 복합적 형태의 분쟁해결 모델로 나누어 설명하기도 한다.

［표 2-11］ 소송외적 분쟁해결제도의 유형 Ⅲ(CDG)

대분류	소분류	내용
기본적 ADR 모델	협상	분쟁 당사자가 자발적으로 분쟁해결을 위해 상호간에 모두 수용가능한 합의안을 도출하는 절차
	화해	제3자가 분쟁 당사자를 각각 만나서 분쟁의 근본원인을 이해하고 친밀한 방법으로 분쟁해결을 촉진하기 위해 노력하는 일련의 절차
	조정 (調整)	당사자에 의해 선택된 중립 제3자가 상호 수용가능한 분쟁해결에 도달할 수 있도록 당사자들이 서로의 이익에 합치되는 해결방안을 만드는 데 도움을 주는 과정
	중재	중재자가 증언, 주장, 증거 등을 바탕으로 일종의 결정을 내리는 절차
복합적 ADR 모델	여러 개의 ADR 모델이 복합적으로 진행되는 방법으로 초기에는 화해나 조정의 단계에 있다가 이 단계에서도 해결이 되지 않는 경우 중재로 나아가는 경우 등을 의미. 여기에는 조정-중재(Med-arb), 간이심리(Minitrial), 사적 재판(Private Judging), 약식배심원심리(Summary Jury Trial) 등이 있음	

※ 참조 : Center for Democracy and Governance, supra note 35, Appendix A

다. 주요 ADR 모델

위에서 살펴본 것처럼 소송외적 분쟁해결제도의 여러 가지 형태를 구분하고 분류하는 것이 언제나 명확한 것은 아니다. 하지만 소송외적 분쟁해결제도의 대표적인 모델이나 유형으로서 일반적으로 제시되고 있는 것들이 있다. OECD의 정보보안·프라이버시 작업반(OECD Working Party on Information Security and Privacy)은 지원협상, 조정, 중재를 그 예로 들고 있다.[36] 반면에 협상, 조정, 중재의 세 가지를 대표적인 ADR 모델로 제시하는 견해[37]도 있으며, 협상, 조정, 중재, 중간자에 의한 해결회의(moderated settlement conference), 조정-중재방법(med-arb)의 다섯 가지를 예로 드는 견해[38]도 있다. 그러나 이하에서는 협상, 알선, 조정, 중재의 네 가지 주요 ADR 모델의 의미를 살펴보도록 하겠다.

(1) 협상

협상(協商, negotiation)은 분쟁 당사자 쌍방이 분쟁해결의 주도적 역할을 하는 절차적 특징을 가진 가장 기초적이면서도 일반적인 분쟁해결수단이다. 즉, 중립적인 제3자가 개입하지 않은 상태에서 순수하게 분쟁 당사자들이 합의점을 찾기 위해 서로 이야기하고 협의하며, 상대방에게 분쟁해결로 인해 얻을 수 있는 이점을 설득해나가는 과정이다. 따라서 협상은 제3자가 개입하는 다른 ADR 기법에 비해 절차의 개시부터 종료까지 모든 부분에 대하여 당사자가 직접 통제하기 때문에, 협상의 진행과정은 당사자의 문제해결의지와 협력관계가 가장 중요한 기준이 된다.

---

36) OECD Working Party on Information Security and Privacy, "*Buiding Trust in the Online Environment : Business To Consumer Dispute Resolution(Report of the Joint Conference of the OECD, HCOPIL, ICC)*", Appendix, 2001. 4. 29.

37) S. Schroeder, "*Alternative Dispute Resolution Resources*", Risk Management, 45(6), 1998.

38) Hakim Ben Adjoua, supra note 34.

(2) 알선

알선(斡旋, Facilitation or Conciliation)은 협상과 달리 분쟁당사자 외 제3자가 개입하여 당사자간의 분쟁해결을 지원하는 제도이다. 즉, 알선은 분쟁 당사자들이 스스로 합의에 도달하여 분쟁을 해소할 수 있도록 제3자가 개입하여 상호 교섭, 주선, 촉진 등의 활동을 해나가는 협상지원제도(Assistant Negotiation)의 의미를 가진다. 그러므로 알선에서 제3자의 역할은 양 당사자 사이에서 문제해결이 잘 되도록 필요한 여러 가지 방편을 마련해 주는 것이지 어떤 분쟁해결방안을 제시하거나 권고하는 것은 아니다. 알선에는 지원(Facilitation)과 화해(conciliation)가 모두 포함될 수 있는 개념으로 볼 수 있다. 지원이라 함은 분쟁해결을 위한 각종 편의를 제공하고 당사자간 원활한 의사소통이 가능하도록 회의를 주재하거나 협의장소를 마련해주는 등의 방법을 의미하고, 화해는 보다 구체적으로 제3자가 당사자간의 대화를 통해 분쟁의 근본적인 원인을 파악하여 이해하고 이를 바탕으로 당사자 상호간 분쟁이 원만히 해결되도록 합의를 유도하는 것이다.[39] 즉, 알선은 중립적인 제3자의 역할이 당사자간의 협상과 타협을 옆에서 보조하고 촉진한다는 것에 한정된다.

국내에서는 환경분쟁조정위원회 및 대한상사중재원에서 이러한 알선 제도를 채택하고 있다.[40] 여기서 알선은 조정절차 또는 중재절차[41]의 전

39) 우리나라에서 화해는 자주적인 분쟁해결방법으로 재판외 화해와 재산상 화해를 의미한다. 그러나 우리나라에서 사용되는 '화해'의 개념은 위에서 말한 'conciliation'과 완벽히 들어맞는 것은 아니다. 왜냐하면 기본적으로 재판외 화해는 어떠한 형식상의 제한이 없이 분쟁당사자의 자주적 해결이라는 점에서 협상(negotiation)과 유사한 개념이기 때문이다. 또한 재판상 화해 역시 제소전 화해 또는 소송상 화해 모두 법관의 확인에 의하여 종국적인 분쟁해결의 효력을 가진다는 점에서 일반적인 의미의 'conciliation' 또는 'mediation'과도 차이가 있다.

40) 국내에서는 'Intercession'을 주로 알선으로 해석하고 있는데, 그 의미는 다소 불명확한 상태이다. 본 논문에서는 알선을 당사자간의 협상을 지원함으로써 분쟁당사자가 해결방안을 모색하고 합의점을 찾아 화해하는 데 도움을 주는 제도로 보아, 앞서 말한 조정(調整)의 의미와 유사한 것으로 보고 있다. 실무적으로도 대한상사중재원이나 환경분쟁조정위원회에서 행하고 있는 알선제도를 보건대, 제3자의 개입을 통한 협상촉진 또는 지원제도로 보는 것이 타당할 것이다.

41) 환경분쟁조정위원회의 경우 중재가 아닌 재정(裁定)제도를 시행하고 있는데, 이는 사

단계로 볼 수 있다. 환경분쟁조정위원회에서는 알선을 '당사자의 자리를 주선하여 분쟁당사자간의 합의와 화해를 유도하기 위해 진행되는 절차'라고 하고 있으며[42], 대한상사중재원은 중재원의 직원이 '양당사자의 의견을 듣고 해결합의를 위한 조언과 타협권유를 통하여 합의를 유도하는 제도'라고 표현하고 있다.[43] 이러한 알선을 통해 당사자간 합의가 이루어지면 이는 민사상 화해계약의 효력을 가진다.

(3) 조정

조정(調停, mediation)은 분쟁당사자가 합의하여 제3자를 조정자로 선임하거나 또는 독립적으로 구성된 제3의 조정자가 제시하는 해결방안, 즉 조정안에 합의함으로써 분쟁해결을 도모하는 방법이다. 일반적으로 조정(mediation)은 화해(conciliation)와 유사한 개념이어서 때때로 양자를 구분하지 않거나, 그 의미가 서로 혼용되는 경우가 있다.[44] 그러나 조정방법에서 조정자는 화해의 경우보다 폭넓은 행동 범위를 가지는데, 예를 들면 분쟁 당사자가 효율적으로 의사소통을 할 수 있도록 도와주거나 상호 협력적인 문제해결태도를 유지할 수 있도록 도와주는 것 외에도 분쟁의

실조사 및 당사자 심문을 통해 재정위원회가 피해배상액을 결정하는 준사법적 절차를 의미한다. 재정위원회의 결정이 있은 후, 재정문서의 정본이 당사자에게 송달된 날부터 60일 이내에 당사자 쌍방 또는 일방이 당해 재정의 대상인 환경피해를 원인으로 하는 소송을 제기하지 않은 때(제기했다가 소송을 철회한 경우 포함)에는 당사자간에 당해 재정내용과 동일한 합의가 성립된 것으로 보게 된다. (환경분쟁조정위원회 웹사이트, http://edc.me.go.kr 참조)

42) 환경분쟁조정위원회 웹사이트, http://edc.me.go.kr 참조.

43) 대한상사중재원 웹사이트, http://www.kcab.or.kr 참조.

44) 예를 들면, 캐나다에서는 화해(conciliation)를 제3자가 분쟁당사자를 따로따로 만나서 이야기를 듣는 과정을 통해 분쟁을 해결하는 것으로 이해하고 있다. 따라서 이 경우 제3자는 양 당사자간을 '왕복해서 오가는 외교술(shuttle diplomacy)'을 이용하게 된다. 반면에, 조정은 제3자가 당사자들이 모두 함께 참석한 자리에서 서로 협상을 하도록 지원하고 화해를 유도하는 것을 의미한다. 그러나 조정과 화해는 때때로 이와는 정반대로 이해되기도 한다. (Catherine Morris, What is *"'Alternative Dispute Resolution'(ADR)? : Some Ways of processing Disputes and Addressing Conflict"*, http://www.peacemakers.ca/publications/ADRdefinitions.html)

근본적인 문제나 당사자들의 이익을 확인하고 문제의 초점과 중요 쟁점을 분석하기도 한다. 또한 당사자 사이에 의견을 전달해주는 통로의 역할을 하기도 하며 합의에 도달할 수 있는 여러 가지 가능한 선택방안을 만들어내며 합의가 되지 않았을 경우의 결과에 대해서도 확인하여 당사자에게 이해시키는 등의 행위를 할 수 있다.[45] 한편 조정은 독립적인 제3자가 개입하여 분쟁해결을 위해 적극적인 역할을 한다는 점에서 중재와 유사하다. 그러나 조정은 일방 당사자가 조정안을 거부하면 그 효력이 없다는 점에서, 일반적으로 구속적 효력을 가진 중재와 구분된다.

국내에서는 법원에 의한 조정제도와 행정형 조정위원회에 의한 조정제도가 여기에 해당된다. 법원에 의한 조정제도는 가사소송법 제49조 이하에 근거를 둔 가사조정(家事調停)과 1990년 9월 1일부터 시행된 민사조정법에 근거한 민사조정(民事調停)이 있다. 특히 민사조정은 민사에 관한 모든 사건을 그 조정대상으로 하며 조정위원회에 의해 조정절차가 진행되며 합의가 될 경우 재판상 화해의 효력을 가지게 된다. 이러한 법원에 의한 조정제도의 특징은 민사조정법 제1조에서 규정하고 있는 목적을 통해서 더욱 명확히 알 수 있다. 즉, 동법 제1조는 민사에 관한 분쟁을 간이한 절차에 따라 당사자 사이의 상호양해를 통하여 조리를 바탕으로 실정에 맞게 해결함을 목적으로 한다고 규정하고 있는 바, 간편성과 조리에 의한 분쟁해결, 상황에 따른 적절한 분쟁해결을 그 특징으로 하고 있다고 할 것이다. 또한 국내에는 각종 법률에 의해 설치된 조정위원회에 의한 조정제도가 활성화되어 있다. 대표적인 것이 소비자분쟁조정위원회, 금융분쟁조정위원회, 의료심사조정위원회, 환경분쟁조정위원회, 전자거래분쟁조정위원회 등이며 개인정보분쟁조정위원회에서 행하는 조정도 이에 해당된다.

(4) 중재

중재(仲裁, arbitration)란 당사자간 합의로 사법상의 법률관계를 법원의

45) Center for Democracy and Governance, supra note 35, Appendix A, p. 3.

소송절차에 의하지 아니하고 제3자인 중재인을 선임하여 중재인의 판단에 맡기고, 양당사자는 이에 구속됨으로써 분쟁을 종국적으로 해결하는 방법이다. 따라서 중재는 다른 어떠한 소송외적 분쟁해결방법 보다도 소송절차에 가까운 특성을 지니고 있다. 왜냐하면 중재인에 의해 결정된 사안은 구속력과 강제성을 가지게 되어 그 효력이 법원의 확정판결과 동일하기 때문이다. 그러나 중재에 의한 분쟁해결은 중재에 대한 양 당사자의 합의가 전제되어야 한다.

이처럼 중재는 종국적인 분쟁해결을 가져온다는 점에서 소송과 유사하나, 단심제이기 때문에 절차의 진행이 신속하다는 점, 해당 분야의 전문가를 중재인으로 선정하여 사건의 적정한 해결을 도모할 수 있다는 점, 비용이 저렴하다는 점, 비밀이 보장될 수 있다는 점 등이 소송에서는 찾아볼 수 없는 장점으로 인정되고 있다. 국내의 중재법 제1조에서도 중재에 의해 사법상의 분쟁을 적정・공평・신속하게 해결함을 목적으로 한다고 하고 있어, 이러한 중재의 특징을 잘 보여주고 있다.

국내에서는 대한상사중재원에 의해 상사중재(商事仲裁)가 유용하게 활용되고 있으며, 특히 국제무역분쟁의 해결에 있어 소송외적 분쟁해결제도의 장점과 실효성이 적극 활용되고 있다.

3. 소송외적 분쟁해결제도와 개인정보피해구제

소송외적 분쟁해결제도는 전통적인 소비자분쟁이나 금융분쟁, 상사분쟁 등의 분야에서 많이 활용되어 왔다. 그러나 최근 들어서 인터넷의 보급으로 인해 급격히 증가한 전자상거래와 관련한 분쟁이나 저작권 분쟁, 도메인 분쟁, 개인정보침해로 인한 분쟁에 있어 그 유용성이 더욱 각광받고 있다. OECD 역시「전자상거래 환경에서의 소비자보호를 위한 가이드라인에 관한 이사회 권고(Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce)」에서 전자상거래 분쟁의 해결을 위해서는 소송

에 갈음할 수 있는 대안적 분쟁해결 및 피해구제제도를 적극 활용하는 것이 필요하다고 강조하고 있다.[46] 이러한 경향은 정보통신사회, 디지털 정보사회, 인터넷 네트워크 사회라고 불리는 오늘날, 이러한 사회적 변화로 인하여 새롭게 등장하고 있는 각종 분쟁은 기존의 분쟁과는 다른 특성을 가지기 때문이다.

개인정보침해로 인한 분쟁 역시 그러하다. 오늘날 개인정보침해로 인한 피해는 신체의 상해로 인한 피해 또는 재산권 침해로 인한 피해 등과는 차별성을 가진다. 즉, 개인정보침해로 인한 피해는 개인의 인격권이나 프라이버시와 밀접한 관련이 있다는 점, 경제적 손해가 아닌 정신적 손해만 인정되는 경우가 많아 소액사건이 대부분이라는 점, 온라인환경과 전자상거래의 발달로 지역적 제한이나 국경의 개념이 없이 피해가 발생한다는 점, 개인정보처리의 디지털화, 온라인화, 데이터베이스화로 인하여 대량처리가 가능해짐에 따라 피해의 파급속도가 빠르다는 점에서 고유한 특성을 가지고 있다.

［표 2-12］개인정보침해의 특수성

특성	필요사항
인격권이나 프라이버시 침해의 측면이 있음	민감하고 중대한 인격권이나 프라이버시침해로 인한 피해를 비공개적으로 해결할 수 있는 피해구제제도 필요
정신적 피해가 상당한 비중을 차지함	소액사건의 정신적 피해를 구제하기 위한 저비용의 간편한 피해구제제도 필요
국경의 개념이 없이 침해가 발생할 수 있음	국경이나 관할권 문제를 초월할 수 있는 유연한 피해구제제도 필요
피해의 파급속도가 빠름	피해의 급속한 확산을 방지할 수 있는 신속한 피해구제제도 필요

46) 동 권고문 제2장은 부당한 비용이나 부담없이 대안적 분쟁해결 및 피해구제제도를 공정·신속한 방법에 의해 이용할 수 있는 소비자의 권리와 B2C 전자상거래, 특히 국제거래에서 야기되는 소비자분쟁을 해결하고 소비자의 불만을 처리할 수 있는 대안적 분쟁해결제도를 비롯한 공정하고 효과적이며 투명한 자율규제 기타 필요한 피해구제 절차 및 정책을 개발하고 이용하여야 할 정부, 사업자, 소비자대표 등의 의무를 밝히고 있다.

따라서 이러한 특성을 감안하면, 보다 신속하고 간편하게 누구나 이용할 수 있고 지역적 제한이 없어야 하며 다양한 구제수단이 확보된 피해구제제도가 필요하다. 그러나 법원을 통한 기존의 소송체계는 국경을 넘어 발생한 사건일 경우 관할권 문제에 부딪힐 뿐 아니라, 만성적인 소송적체로 인해 시간이 과다하게 걸리며 법률전문가의 협조가 필요하여 비용이 많이 소요되는 문제점이 있다. 따라서 소송에 의할 경우, 정신적 피해의 측면이 크고 때로는 즉각적으로 침해상태를 배제하여 원상회복이 필요한 경우가 발생할 수 있는 개인정보침해사건을 적절한 시기와 방법으로 구제할 수 없게 된다.

이와 같이 개인정보침해로 인한 피해는 소송제도와 같은 기존의 피해구제제도의 테두리 안에서 다루기 어려운 점이 있기 때문에, 개인정보에 특유한 피해구제제도의 확립이 무엇보다 중요한 것으로 인식되고 있다. 이에 소송제도를 보완할 수 있는 대체적 방법으로 소송외적 분쟁해결제도의 활용이 중시되고 있는 것이다. 실제로 국내외의 민간 분쟁해결기구나 개인정보보호기구는 개인정보침해로 인한 분쟁을 해결하고 그로 인한 피해를 구제함에 있어 화해나 조정 등의 소송외적 분쟁해결방법을 적극 활용하고 있다. 이러한 국내외의 개인정보피해구제제도와 소송외적 분쟁해결제도의 활용 현황은 이어지는 장에서 보다 자세히 살펴볼 수 있을 것이다.

제 3 장 국내 개인정보피해구제제도

우리나라는 20여년 전부터 새로운 국가발전 동력으로 정보화를 선택하여 세계의 IT 혁명에 능동적으로 대처하기 위한 꾸준한 노력을 펼쳐 왔다. 그 결과 오늘날 전 세계로부터 정보통신 선도국가라는 평가를 받고 있다. 초고속 정보통신망이 2003년 9월 기준으로 이미 1,100만 가구에 보급되어 인구의 60%가 넘는 2,860만명이 인터넷을 이용하고 있을 뿐 아니라, 이동통신 가입자 역시 3,300만명을 넘어서는 등 세계 어디에서도 찾아볼 수 없는 정보통신 환경을 구축하였다.[47] 또한 우리나라의 IT 산업은 한국경제의 핵심 축을 정보통신기반산업으로 이동시켜 경제구조에 근본적인 변화를 가져오기도 하였다.

우리나라는 이러한 유·무선 정보통신망 구축이나 새로운 정보통신산업의 촉진 등을 통해 IT 기반을 생산해내는 것 외에도 적극적으로 IT 자원을 활용하고 새로운 기술을 선진적으로 수용하는 모습을 보이고 있다. 공공부문에서 한국정부는 1983년 정보화시대의 도래에 따른 행정환경의 변화추세에 부응하기 위해 '국가기간전산망기본계획'을 마련하여 행정·금융·교육·연구·공안전산망 등 5대 국가기간전산망 구축사업을 추진한 결과, 국민의 일상생활과 직접 관련된 주민등록, 부동산, 자동차를 중심으로 지역간·기관간 정보유통체제를 확립하였다. 이러한 전산망 구축 및 행정업무의 전산화는 빠르게 진행되어 오늘날 주민등록데이터베이스, 운전면허데이터베이스, 여권관리데이터베이스, 출입국관리데이터베이스 등이 구축되어 있는 상태이다.[48] 또한 정부는 꾸준히 세계 최고 수준의 전자정부 구현을 목표로 '전자정부 11대 사업'을 추진해왔고, 올 8월에는 31개 세부추진과제를 설정한 '전자정부 로드맵'을 발표하기도 하였다. 이러한 공공분야에서의 정보화의 촉진은 행정업무의 효율성과 혁신성 제

47) 정보통신부, "정보통신백서", 2003, 1~2면.

48) 행정자치부, "공공기관의 개인정보보호제도 이해와 해설", 2003. 3, 5~6면.

고, 인터넷을 통한 각종 대국민 민원서비스의 제공으로 인한 국민 편의 향상으로 이어지고 있다.

뿐만 아니라 민간부문에서도 정보화의 진전은 경제적·사회적·문화적으로 많은 변화를 불러일으키고 있다. 유·무선 정보통신과 같은 IT를 기반으로 한 다양한 신규사업의 등장은 우리 경제에 활력소가 되고 있고, 인터넷은 21세기 한국사회의 새로운 문화를 만들어내는 진앙이 되고 있다. 이제 인터넷은 한국인에게 필요한 지식과 정보를 쉽게 찾을 수 있는 백과사전과 같은 것이자, 갖고 싶은 물건의 가격을 언제라도 비교해보면서 살 수 있는 편리한 쇼핑장소이며, 사람들과 친밀한 인간관계를 더욱 공고히 할 수 있는 모임장소이고, 게임을 하거나 영화를 보거나 책을 읽을 수 있는 여가생활이 가능한 너무나도 친숙한 공간이다.

그러나 이러한 정보화의 진전과 발달로 인한 우리 삶의 변화는 항상 긍정적인 면만 있는 것은 아니었다. 우리나라에서는 특히 고도화된 정보통신망을 이용하는 사람들이 증가하면서 개인프라이버시의 침해 문제도 함께 대두되기 시작하였고, 이에 개인정보보호에 대한 국민적 관심도 높아지고 있다. 이러한 경향은 개인정보보호에 대한 법체계 정립과 개인정보보호기구의 설립에 대한 관심과 논의로 이어지고 있다. 이하에서는 이러한 변화 속에서 제정·시행되고 있는 국내 개인정보보호법의 주요 내용과 개인정보보호의 역할을 맡고 있는 국내 개인정보보호기구에 대하여 살펴보도록 한다.

제 1 절 국내 개인정보보호법

1. 입법현황

헌법 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인

권을 확인하고 이를 보장할 의무를 진다"고 하고, 헌법 제17조는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다"고 규정하여, 개인의 사생활의 비밀과 자유의 불가침성을 선언하고 있다. 국내에는 이러한 헌법원칙을 구현하기 위한 일반적인 개인정보보호법이 제정되어 있지는 않고 각 영역별로 개개 법률 규정이 있는데, 개인정보와 관련한 대표적인 법률로는 공공기관개인정보보호법, 정보보호법, 신용정보의이용및보호에 관한법률(이하 '신용정보보호법'이라 한다) 등이 있다. 이 외 통신비밀보호법은 도·감청 금지 및 개인의 통신비밀의 자유 보장에 관한 내용을, 형법은 개인의 비밀침해금지 및 업무상 취득한 비밀의 누설금지 규정을, 의료법은 의사·간호사·조무사 등이 의료행위 과정에서 취득한 환자의 비밀을 누설하는 것을 금지하는 내용을 각각 규정하고 있다. 먼저 이러한 개인정보보호 관련 입법현황을 살펴볼 수 있을 것이다.

〔표 3-1〕 국내 개인정보관련 입법현황

구분	법률	
공공부문	·공공기관의개인정보보호에관한법률(1994) ·전자정부구현을위한행정업무등의전자화촉진에관한법률(2001) ·주민등록법(1962) ·국가공무원법(1949) ·공직자윤리법(1981) ·민원사무처리에관한법률(1997)	
민간부문	정보통신분야	·정보통신망이용촉진및정보보호등에관한법률(1999) ·정보화촉진기본법(1999) ·전기통신사업법(1961) ·정보통신기반보호법(2001) ·통신비밀보호법(1948)
	상거래분야	·독점규제및공정거래에관한법률(1980) ·방문판매등에관한법률(1991) ·약관의규제에관한법률(1986) ·전자거래기본법(1999) ·전자서명법(1999) ·전자상거래등에서의소비자보호에관한법률(2002)
	금융·신용분야	·신용정보의이용및보호에관한법률(1995) ·금융실명거래및비밀보장에관한법률(1997) ·증권거래법(1962) ·증권투자신탁업법(1969)
	의료분야	·의료법(1962) ·약사법(1953) ·국민건강보험법(1999)
기타	·형법 제127조, 제316조제2항, 제317조 ·공증인법(1961) ·변호사법(1949) ·법무사법(1990)	

이렇듯 국내에는 다양한 개인정보 관련 규정이 여러 법률에 산재되어 있다. 그러나 이 중 공공기관개인정보보호법은 공공부문에서의 개인정보 처리절차 및 그 과정에서 준수하여야 할 사항 등을 규정하고 있고, 정보보호법은 정보통신사업자 및 일부 오프라인 사업자가 개인정보를 처리할 때 고객의 개인정보를 어떻게 관리하고 보호하여야 하는지를 규정하고 있는 바, 각각 공공부문과 민간부문을 대표하는 개인정보보호법이라 할 수 있을 것이다. 따라서 이하에서는 공공기관개인정보보호법과 정보보호법의 주요 내용을 살펴보도록 하겠다.

2. 공공기관개인정보보호법

우리나라의 공공부문에서는 모든 문서처리의 전자화와 인터넷 국민서비스의 고도화 등을 목적으로 한 전자정부 사업이 활발히 진행되어 왔다. 이러한 과정에서 개인정보를 컴퓨터를 통해 대량적으로 처리하고 저장하는 경우가 증가하고 각 단위별로 흩어져 별도로 존재하던 개인정보 대장이 하나의 시스템 속으로 집적되고 있는 추세이다. 그러나 이러한 개인정보의 전산처리는 개인정보를 대량으로 처리하는 것을 가능케 할 뿐 아니라 쉽게 복제되어 외부에 누출되거나 온라인을 통해 전송될 수 있는 취약점이 있어, 개인정보 전산처리에 따른 개인정보의 오·남용 및 유출이라는 문제점이 야기되었다. 그러나 본격적으로 개인정보 전산처리가 증가하던 초기 시기에는 국가공무원법, 주민등록법 등 개별법령의 선언적이고 처벌위주의 규제적인 법령체계가 있었을 뿐이어서 이러한 부작용을 효과적으로 예방하고 대처하는데 한계가 있었다.[49]

이에 공공기관개인정보보호법이 1994년 제정·시행되기에 이르렀다. 동법은 1999년 한 차례 개정을 거쳤으며, 두 번째 개정안이 지난 8월 입법예고된 상태이다.[50] 아래에서는 현재의 공공기관개인정보보호법의 내용

49) 행정자치부, 앞의 책, 6면.

50) 동 개정안은 정부가 추진하고 있는 전자정부사업과 관련하여 공공기관의 개인정보보호제도를 재정비할 필요성이 제기되면서 만들어진 것으로, 전자정부시대 네트워크를

을 중심으로 살펴보도록 하며 입법예고된 개정법률안의 내용도 추가적으로 검토해보도록 한다.

가. 적용범위

공공기관개인정보보호법 제1조는 "이 법은 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다"라고 밝히고 있는 바, 동법은 공공기관에서 컴퓨터로 처리하는 개인정보를 그 보호대상으로 하고 있음을 명확히 하고 있다. 따라서 공공기관개인정보보호법의 인적 적용범위는 공공기관이며 물적 적용범위는 컴퓨터로 처리되는 개인정보이다.

여기서 '공공기관'이라 함은 국가행정기관·지방자치단체 기타 공공단체 중 대통령령이 정하는 기관을 의미하며, '대통령령이 정하는 기관'에는 각급 학교, 금융기관을 제외한 정부투자기관 및 특수법인, 퇴직연금의 지급정지대상기관이 포함된다.[51] 또한 동법의 보호를 받는 '개인정보'의 범위는 제2장 〔표 2-6〕에서 살펴본 바와 같으며, 컴퓨터로 처리되는 개인정보에 한정되기 때문에 순수하게 오프라인에서 수집·보유·처리되는 개인정보는 제외된다.[52]

통한 개인정보 유통이 활발해질 것을 고려하여 '정보통신망', '개인정보데이터베이스', '개인정보시스템'이라는 용어를 도입하고 있다(안 제2조제3의2호, 제4호, 제4의2호). 이 밖에도 공공기관이 준수하여야할 개인정보보호원칙에 관한 규정을 새롭게 신설하였고(안 제3조의2), 공공기관의 개인정보침해신고의 상담·접수·조사·처리 등의 업무를 수행하는 개인정보침해신고센터의 설치(안 제18조의3) 및 개인정보보호심의위원회의 기능 강화(안 제20조) 등의 내용을 포함하고 있다.

51) 공공기관개인정보보호법 제2조 및 동법시행령 제2조.

52) 이렇듯 공공기관개인정보보호법은 컴퓨터에 의해 처리되는 개인정보로 그 적용범위가 한정되기는 하나, 사실상 공공기관이 수집·보유하는 개인정보의 대부분은 컴퓨터를 통해 입력·저장·편집·검색·삭제·출력되고 있다고 볼 수 있다. 따라서 오프라인 정보라고 하더라도 컴퓨터에서 출력되는 주민등록 등·초본과 같은 정보는 동법의 적용을 받는다고 볼 수 있다.

한편 공공기관개인정보보호법은 다른 법률에 특별한 규정이 있는 경우에는 해당 법률이 동법에 우선하여 적용된다. 또한 법인 또는 단체의 정보, 死者의 정보, 통계법에 의하여 수집되는 개인정보, 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공이 요청되는 개인정보에 대해서는 적용이 제한된다.[53]

나. 정보주체의 권리

공공기관개인정보보호법상 정보주체인 일반 국민은 공공기관이 보유하고 있는 자신에 관한 정보에 대하여 열람 및 정정을 요구할 수 있으며, 만약 공공기관 등이 정당한 사유없이 이를 거부하였을 때에는 행정심판을 청구할 수 있는 권리가 있다.

(1) 열람・정정청구권

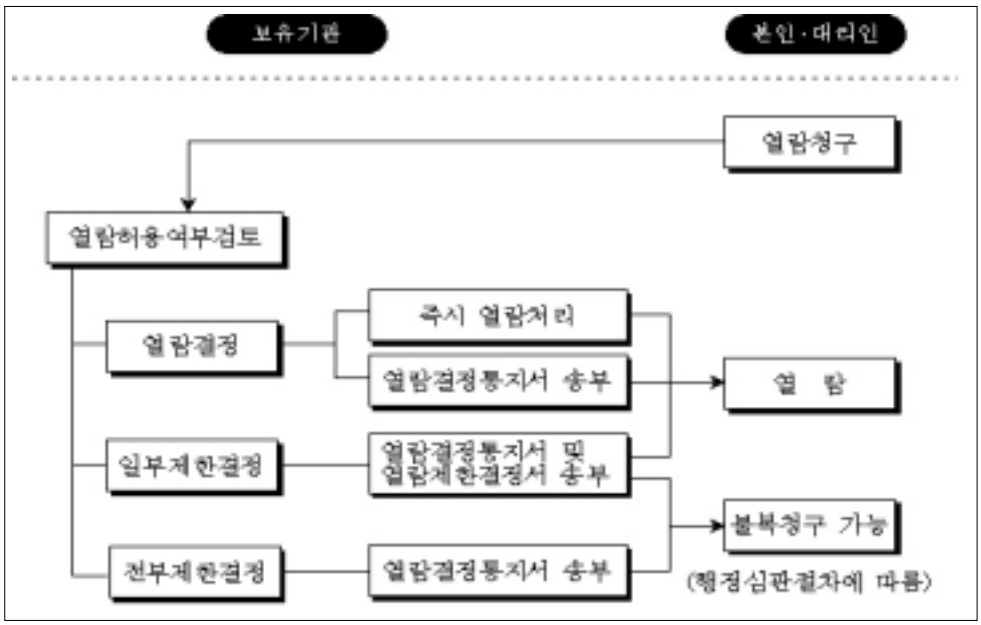
공공기관개인정보보호법에 의하면, 정보주체인 개인은 서면을 통해 자신의 개인정보를 보유하고 있는 공공기관의 장에게 자신에 관한 처리정보의 열람 및 정정을 청구할 수 있다.[54] 공공기관은 보유하고 있는 정보를 바탕으로 해당 개인에게 중대한 행정적 의사결정을 내릴 수 있다는 점에서 항상 정보의 정확성을 유지하여야 할 필요성이 있으며, 이러한 점에서 정보주체의 열람・정정청구권은 더욱 중요하다 할 것이다.

정보주체의 열람・정정청구권의 행사절차를 간략히 살펴보면 다음과 같다. 정보주체의 열람청구를 받은 기관은 7일 이내 열람의 허용여부, 열람일시 및 장소를 결정하여 '열람결정통지서'를 정보주체에게 발송하여야 한다. 열람의 실시는 별다른 사유가 없는 한 15일 이내에 하는 것이

53) 공공기관개인정보보호법 제3조.

54) 공공기관개인정보보호법 제12조제1항 및 제14조제1항. 한편, 개정법률안은 서면은 물론 인터넷을 통해서도 열람・정정・삭제청구를 할 수 있도록 규정하고 있다(안 제12조, 안 제14조).

원칙이나, 동 기한을 지키지 못할 '정당한 사유'가 있는 경우 보유기관은 정보주체에게 열람연기사유와 예정일시 등을 기재한 '열람연기통지서'를 송부하여야 한다. 그러나 정보주체의 열람청구권 행사는 개인정보파일대장에 기재되어 있지 않은 항목에 대해서는 불가능하다. 또한 공공기관개인정보보호법 제13조는 '개인의 생명·신체를 해할 우려가 있거나 개인의 재산과 기타의 이익을 부당하게 침해할 우려가 있는 경우' 등 열람제한사유를 열거하고 있는 바, 보유기관의 장이 위와 같은 사유에 해당된다고 판단하는 때에는 열람이 제한될 수 있다. 다만, 보유기관의 장은 부당한 열람청구제한이 발생하여 정보주체의 권익이 침해되는 일이 없도록, 반드시 정보주체의 자기정보열람권과 공익 및 제3자의 권리·이익을 비교·형량하여 신중히 판단하여야 한다. 또한 절차적으로도 청구권자가 자세한 사항을 알 수 있도록 '열람제한결정서'에 열람제한범위, 사유, 당해처분의 불복에 필요한 절차 등을 기재하여 청구인에게 통지하여야 한다.



(그림 3-1) 공공기관의 개인정보열람청구 처리절차

※ 주 : 행정자치부, "공공기관의 개인정보화일 목록집", 2002, 7면.

개인정보 열람 후 잘못된 사항에 대한 정정을 요구하는 절차도 이와 유사하다. 즉, 정보주체가 잘못된 내용에 대한 정정·삭제를 요구하는 내용의 '정정청구서'를 작성하여 개인정보의 원 보유기관에 제출하면, 보유기관의 장은 정정청구서를 받은 날부터 15일 이내에 필요한 조치를 한 후 '정정조치결과통지서'를 청구인에게 송부함으로써 종료된다. 다만, 보유기관의 장은 1회에 한해 정보주체의 정정청구를 연기할 수 있고, 정당한 근거 하에 정정을 거부할 때에는 '정정거부등결정통지서'를 청구인에게 발송하여야 한다. 정보주체가 정정 또는 삭제를 요청할 수 있는 사항은 실재하는 사실과 불일치하는 내용 뿐 아니라 전혀 존재하지 않는 사실에 관한 특정 항목의 삭제까지 포함된다. 그러나 불필요한 정보 또는 과다한 정보의 보유를 이유로 정보의 삭제를 청구하는 것은 인정되지 않는다.[55]

(2) 불복청구권

정보주체는 자신의 열람 또는 정정청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 경우, 행정심판법에 따라 해당 재결청에 불복청구를 할 수 있다.[56] 따라서 열람·정정청구권자는 열람·정정요구가 전부 또는 일부 거부되었을 때, 청구가 있음에도 불구하고 해당 공공기관이 정당한 사유 없이 30일을 초과하여 아무런 처분도 하지 않을 때에는 불복청구를 할 수 있다. 불복청구는 행정심판법에서 규정하고 있는 절차에 따르기 때문에, 정보주체는 해당 행정기관의 처분이 있음을 안 날로부터 90일, 처분이 있은 날로부터 180일 이내에 청구를 하여야 한다.[57]

---

55) 행정자치부, 앞의 책, 50면.

56) 공공기관개인정보보호법 제15조.

57) 한편 개정법률안은 권리 또는 이익의 침해를 입은 정보주체는 행정심판을 청구할 수 있음은 물론, 행정소송법이 정하는 바에 따라 행정소송을 제기할 수 있다고 명시적으로 밝히고 있다(안 제15조).

다. 공공기관의 의무

공공기관개인정보보호법은 공공기관이 컴퓨터에 의해 개인정보를 처리하고 보유하는 과정에서 발생할 수 있는 개인정보의 오·남용 및 유출을 방지하기 위해 공공기관이 준수하여야 할 의무사항을 규정하고 있다. 특히 동법은 컴퓨터로 처리되는 개인정보를 그 보호대상으로 한다는 점과 공공부문이라는 특성상 공익도 중요한 가치로 인정된다는 점을 기초로 하고 있기 때문에, 공공기관이 개인정보처리 과정에서 준수하여야 할 의무사항도 이러한 점을 반영하고 있다.[58]

(1) 수집·보유의 제한

공공기관은 원칙적으로 사상·신조 등 개인의 기본적 인격을 현저하게 침해할 우려가 있는 민감한 개인정보는 수집하여서는 안 된다. 그러나 이러한 개인의 인격을 현저하게 해할 우려가 있는 정보라 하더라도 정보주체의 동의가 있거나 법률의 근거가 있는 경우 적법하고 공정한 방법에 의해 개인정보를 수집할 수 있다.[59] 특히 공공기관의 경우 일반 국민들의 개인정보를 대량적으로 처리한다는 점에서 개별적인 동의를 얻기 보다는 개인정보의 수집·보유의 근거를 법률의 제정을 통해 규율하는 것이 일반적이다.

이렇게 수집한 개인정보는 소관업무를 수행하기 위하여 필요한 범위 내에서만 보유할 수 있다.[60] 여기서 '소관업무에 필요한 범위 내'라 함은 법에 의해 부여된 기관의 기능이나 활동 수행에 있어 개인정보파일의 보

58) 한편 개정법률안 제3조의2는 필요최소한의 개인정보 수집 및 개인정보 목적외 이용금지원칙, 개인정보의 정확성·완전성·최신성·안전성 확보의 원칙, 수집·이용목적의 명확성 원칙, 개인정보관리책임의 명확성 원칙 및 투명한 관리과정의 공개원칙, 개인정보의 분리 관리원칙 등 개인정보를 처리하는 공공기관이 준수하여야 할 개인정보보호원칙을 명시하고 있다. 이런 점에서 개정법률안은 현재의 법규정보다는 공공기관의 의무를 보다 구체화·명확화하고 있다고 볼 수 있다.

59) 공공기관개인정보보호법 제4조.

60) 공공기관개인정보보호법 제5조.

유가 전제되어야 하는 경우를 의미한다. 따라서 개인정보파일의 보유와 소관업무의 목적과는 필요성의 원칙 및 비례성의 원칙이 충족되어야 한다. 즉, 개인정보파일을 보유하는 경우에도 개별적인 개인정보의 항목, 범위, 보유기간 등이 소관업무에 필요한 범위 내에로 한정되어야 하며, 당해 개인정보의 수집·처리로 인한 개인 사생활의 침해와 그로 인해 얻는 공익상의 목적달성 사이의 비례관계도 충족되어야 한다.[61]

(2) 개인정보파일의 사전통보 및 공고

공공기관개인정보보호법 제2조에 의하면, 개인정보파일이란 '특정개인의 신분을 식별할 수 있는 사항에 의하여 당해 개인정보를 검색할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 컴퓨터의 자기테이프·자기디스크 기타 이와 유사한 매체에 기록된 것'을 의미한다. 동법은 공공기관이 이와 같은 개인정보파일을 보유하고자 할 때, 행정자치부장관 또는 관계 감독행정기관에 사전통보토록 하고 있다. 또한 행정자치부장관에게 통보받은 사항을 연 1회 이상 관보에 게재토록 의무를 부여하고 있으며, 보유기관 역시 사전통보를 마친 개인정보파일대장을 일반인들이 확인할 수 있도록 비치하여야 한다.[62]

이러한 사전통보제도의 취지는 감독행정기관이 각 기관별 개인정보 처리현황을 파악할 수 있도록 함은 물론 이를 통해 개인정보의 공정한 처리를 효율적으로 지도·감독할 수 있게 하기 위함이다. 또한 공고제도는 공공기관이 보유하고 있는 개인정보파일을 공개적으로 밝힘으로써, 공공기관의 개인정보 처리현황을 투명하게 공개하고 정보주체의 열람·정정 청구 등의 권리행사를 용이하게 하려는 목적을 가진 제도이다. 그러나 사전통보 및 공고제도는 폭넓은 예외를 가진다. 즉, 국가의 안전이나 외교상의 비밀과 같은 국가의 중대한 이익에 관한 사항을 기록한 개인정보

61) 행정자치부, 앞의 책, 25면.

62) 공공기관개인정보보호법 제6조~제8조.

파일, 범죄의 수사나 형의 집행 등 형사기록에 관한 개인정보파일, 1년 이내에 삭제되는 처리정보를 기록한 파일, 보유기관의 내부적 업무처리만을 위하여 사용되는 파일 등은 사전통보를 하지 않아도 되며, 통보를 받은 개인정보파일의 경우에도 공공기관의 적정한 업무수행을 현저하게 저해할 우려가 있다고 인정되는 때에는 대통령령에 의거 공고를 생략할 수 있다.[63]

(3) 개인정보파일의 안전성・정확성・최신성 확보

수집한 개인정보를 보유하고 있는 경우, 개인정보의 유출이나 부정사용을 방지하기 위해 반드시 필요한 것이 개인정보의 안전성이다. 공공기관개인정보보호법 제9조는 바로 이러한 개인정보의 안전한 관리와 보유를 확보함으로써 개인정보를 보호하기 위한 규정이다. 즉, 개인정보를 컴퓨터에 의해 처리하는 공공기관의 장은 개인정보가 분실・도난・누출・변조 또는 훼손되지 아니하도록 안전성 확보를 위해 필요한 조치를 강구하여야 하며, 이를 위해 자체적인 개인정보보호정책을 수립하여 시행하여야 한다. 여기서 '안전성 확보를 위한 조치'라 함은 개인정보파일이 비치되어 있는 장소나 시스템에 대한 접근통제 및 감시장비 설치, 사용자 등록 및 암호화, 보안업무규정의 제정 및 시행, 개인정보가 기록된 입・출력자료의 유출방지조치 강구, 개인정보취급자에 대한 정기적인 교육 등의 관리적・기술적 조치를 의미한다.

이 외에도 공공기관은 보유하고 있는 개인정보의 정확성과 최신성을 유지하기 위해 필요한 조치를 취하여야 한다. 여기에는 정보주체의 열람・정정청구절차를 구비하여 철저히 시행하는 것도 포함될 것이다. 단, 정확성과 최신성은 당해 개인정보의 수집 및 보유목적에 적합한 수준이면 된다.

63) 공공기관개인정보보호법 제6조제2항 및 동법시행령 제6조 ; 동법 제7조 및 동법시행령 제7조제2항~제3항.

(4) 처리정보의 이용 및 제공 제한

공공기관이 보유하고 있는 개인정보파일을 기관 내부에서 이용하거나 다른 기관에 제공할 때에는 법적 근거가 있어야 한다. 이러한 법적 근거가 없는 개인정보파일의 보유목적외 이용 및 타기관 제공은 명백한 불법행위이며 심각한 개인정보 침해를 가져올 수 있다.

그러나 역시 목적외 이용 및 제공금지 원칙도 동법 제10조제2항에 의해 광범위한 예외를 가진다. 즉, 공공기관은 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, 다른 법률에서 정하는 소관업무의 수행을 위해 처리정보를 이용할 상당한 이유가 있는 경우, 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우, 정보주체외의 자에게 제공하는 것이 명백히 정보주체에게 이익이 된다고 인정하는 경우 등에는 해당 개인정보파일을 보유목적 외로 이용하거나 제공할 수 있다. 다만, 이 경우에도 개인정보의 제공에 따른 관리책임은 보유기관에 있다. 따라서 개인정보를 제공하는 공공기관은 이용목적에 필요한 최소한의 개인정보만을 제공하여야 하고 안전성 확보를 위한 조치를 요청하여야 한다.

(5) 개인정보취급자의 비밀누설금지의무

개인정보의 처리를 행하는 공공기관의 직원이나 직원이었던 자 또는 공공기관으로부터 위탁받은 업무에 종사하거나 하였던 개인정보취급자는 직무상 취득하게 된 개인정보를 누설 또는 권한 없이 처리하거나 타인의 이용에 제공하는 등 부당한 목적을 위해서 사용하여서는 안 된다. 이러한 비밀누설금지의무에 위반하여 개인정보를 부당한 목적으로 사용한 자는 3년 이하의 징역 또는 1천만원 이하의 벌금에 처해진다.

3. 정보보호법

민간부문에서 개인정보침해 문제가 심각하게 대두된 이유는 역시 정보통신망을 통한 개인정보의 수집・이용・처리 행위가 증가되었기 때문이다. 이에 국내에서는 1999년 정보보호법이 시행되었다. 동법은 본래 1986년 제정된「전산망보급확장과이용촉진에관한법률」의 전문을 개정, 개인정보보호 부분을 추가한 것이다. 법령명과 입법연혁을 통해서도 알 수 있듯이, 동법은 정보통신망의 이용촉진과 개인정보의 보호라는 두 가지 목적을 함께 담고 있다.[64] 정보보호법은 이러한 목적을 바탕으로 하여 제정되었기 때문에, 주로 민간영역에서의 정보통신망을 통한 개인정보의 수집・이용・제공 등의 행위를 규율하고 있다. 그러나 동법은 정보통신망에 한하지 않고 일부 오프라인 사업자에 의한 개인정보 처리도 함께 규율함으로써 민간부문을 대표하는 개인정보보호법의 역할을 담당하고 있다. 또한 동법은 개인정보보호에 대한 국제규범 및 국제표준이라 할 수 있는 OECD 프라이버시 8원칙을 충실히 반영하고 있다.

한편 정보보호법은 지난 12월 29일 개정안이 국회 본회의를 통과하여 현재 공포만을 남겨두고 있는 상태이다. 동 개정안은 정보통신서비스제공자의 개인정보 위탁처리시 관리책임 및 수탁자의 개인정보보호 의무를 강화하고 이용자의 열람권을 세부적으로 규정하는 등의 내용을 담고 있다. 이하에서는 정보보호법의 개인정보보호 규정의 주요 내용을 살펴보고 개정안의 내용도 추가적으로 검토해보도록 한다.

가. 적용범위

정보보호법은 원칙적으로 '생존하는 자연인'으로서 정보통신서비스를 이용하는 이용자의 개인정보를 그 보호대상으로 삼고 있다. 따라서 동법은

64) 정보보호법 제1조는 "정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 하고 있다"고 규정하고 있어, 이러한 동법의 목적을 잘 표현하고 있다.

영리를 목적으로 정보통신서비스를 제공하는 사업자의 개인정보 수집·이용·처리·제공 등의 행위를 규율한다. 이러한 정보통신서비스제공자는 전기통신사업법 제2조제1항제1호의 규정에 의한 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 의미한다. 즉, 유·무선 전화, 초고속 인터넷서비스제공자와 같은 통신사업자 및 인터넷서비스제공자(ISP) 등이 해당된다. 그러나 정보보호법은 동법이 적용되는 대상을 정보통신서비스제공자에 한정하지 않고 있다. 즉, 정보통신서비스제공자 외의 자가 개인정보를 수집·저장·처리하는 경우에도 동법을 준용[65]하고 있는데, 이에 해당하는 오프라인 사업자로는 여행업·호텔업자, 항공운송사업자, 학원·교습소, 기타 회원제로 개인정보를 수집하여 재화·용역을 제공하는 사업자가 있다.[66]

나. 정보주체의 권리

(1) 동의권 및 동의철회권

정보보호법은 정보주체의 개인정보자기결정권을 보장하기 위해, 자신의 개인정보에 대한 통제권을 폭넓게 인정하고 있다. 이러한 정보주체의 자기정보통제권은 동의권에서부터 시작한다고 볼 수 있다. 즉, 정보주체는 정보보호법 제22조 및 제24조를 통해 자신에 관한 개인정보를 정보통신서비스제공자 등이 수집·이용·처리할 수 있도록 허용할 것인지 여부를

65) 정보보호법 제58조는 "제22조 내지 제32조의 규정은 정보통신서비스제공자 외의 자로서 재화 또는 용역을 제공하는 자 중 대통령령이 정하는 자가 자신이 제공하는 재화 또는 용역을 제공받는 자의 개인정보를 수집·이용 또는 제공하는 경우에 이를 준용한다. 이 경우 '정보통신서비스제공자' 또는 '정보통신서비스제공자등'은 '재화 또는 용역을 제공하는 자'로, '이용자'는 '재화 또는 용역을 제공받는 자'로 본다"고 규정하고 있어, 개인정보의 보호원칙 및 정보처리자의 의무, 정보주체의 권리 등의 규정이 오프라인에서 개인정보를 수집·처리하는 일정 범위의 사업자에게도 확대 적용되도록 하고 있다.

66) 정보보호법시행령 제28조.

스스로 결정할 수 있는 기회를 보장받고 있다. 또한, 정보주체는 개인정보 수집단계에서부터 이용 및 제3자 제공 등에 이르기까지 전 단계에서 자신의 개인정보를 통제할 수 있으며, 정보주체의 동의 유무가 개인정보 처리에 있어서 중요한 잣대가 된다. 따라서 정보통신서비스제공자는 개인정보를 수집할 때 수집 및 이용목적을 밝혀 정보주체의 동의를 얻어야 하며, 사기 또는 부정한 방법으로 개인정보를 수집해서는 안 된다. 또한 이용목적이 변경되었거나 이용목적 외로 이용하거나 제3자에게 제공하고자 할 때에도 별도로 정보주체의 동의를 얻어야 한다. 이는 정보통신서비스제공자 등이 일단 개인정보를 수집한 이후에도 정보주체의 통제권을 사실상 박탈하는 결과가 발생하지 않도록 하기 위함이다.

한편 정보주체는 동의철회권을 행사함으로써 사업자에 의한 자신의 개인정보 처리를 배제할 수 있다. 이용자는 언제든지 개인정보의 수집, 목적외 이용, 제3자 제공 등에 대한 동의철회권을 자유로이 행사할 수 있다. 정보통신서비스제공자는 이용자의 동의철회가 있는 경우 지체없이 수집한 개인정보를 파기하거나 목적외 이용을 중지하는 등 필요한 조치를 취하여야 한다.

(2) 열람・정정요구권

정보통신서비스제공자가 보유하고 있는 자신의 개인정보의 내용, 범위, 정확성 등을 확인하고 잘못된 경우 정정을 요구할 수 있는 열람・정정요구권은 정보주체가 자기 정보에 대한 통제권을 행사함에 있어 반드시 보장되어야 할 기본적이고도 필수적인 사항이다. 정보주체는 쉽고 간편하며 저렴한 비용으로 자신의 개인정보에 대하여 열람을 요구할 수 있어야 하고 오류를 손쉽게 정정함으로써 부당한 피해를 입지 않도록 보장받을 권리가 있다. 개정안에서는 이용자의 열람권을 보다 강화하여, 정보주체가 정보통신서비스제공자등이 개인정보를 이용하거나 제공한 명세를 요구할 수 있도록 하고 정보통신서비스제공자등에게는 정보주체의 이러한 요구에 응하여 지체없이 필요한 조치를 취할 의무를 부과하고 있다.[67]

(3) 개인정보침해에 대한 손해배상청구권

정보보호법은 이용자가 정보통신서비스제공자의 불법적인 행위나 부당한 개인정보침해로 인하여 경제적·정신적 손해를 입었을 경우, 당해 정보통신서비스제공자에게 손해배상을 청구할 수 있음을 명시적으로 규정함으로써 이용자의 피해구제를 강조하고 있다. 특히 정보보호법은 제32조에서 이용자의 손해배상요구에 대하여 당해 정보통신서비스제공자가 스스로 고의 또는 과실이 없음을 입증하지 못하면 손해배상책임을 면할 수 없도록 입증책임전환규정을 두고 있어 이용자 보호를 강조하고 있다.

다. 정보통신서비스제공자의 의무

정보보호법에 의하면 정보통신서비스제공자는 이용자의 개인정보를 오·남용하거나 유출되는 일이 없도록 주의를 다하여야 하며, 이용자의 개인정보에 대한 통제권을 보장하여 그 권리를 침해하는 일이 없도록 하여야 하는 등 개인정보보호를 위한 다양한 의무를 부담한다.

〔표 3-2〕 정보통신서비스제공자의 의무

구분	의무
수집	필요최소한의 개인정보 수집의무
	개인정보 수집 및 이용목적 등에 관한 사항을 고지·명시할 의무
이용	개인정보의 목적외 이용 및 제공행위를 하지 아니할 의무
관리	개인정보의 안전성 확보의무
	개인정보책임자의 지정의무
접근	정보주체의 열람·정정요구, 동의철회에 응할 의무
파기	동의철회 및 목적달성 후 개인정보 즉시파기의무

67) 정보보호법개정안 제30조제2항.

(1) 필요최소한의 정보수집의무

정보통신서비스제공자는 이용자의 개인정보를 수집할 때 이용자의 동의를 반드시 얻어야 한다.[68] 또한 이용목적에 필요한 최소한의 범위 내에서 정보를 수집하여야 하며, 지나치게 과도한 정보나 민감한 개인정보를 수집하여서는 안 된다. 이 경우 정보통신서비스제공자는 이용자가 필요최소한 정보 이외의 정보를 제공하지 아니한다는 이유로 서비스의 제공을 거부하여서는 안 된다. 예를 들어, 인터넷서비스제공자가 서비스 제공에 있어 필수적으로 요구되는 정보가 아닌 취미, 결혼여부, 직업, 수입정도, 학력 등을 요구하여 이를 기재하지 아니하면 회원가입자체가 되지 않도록 하는 행위는 이러한 필요최소한의 정보수집의무를 위반한 것이 된다.

(2) 고지·명시의무

정보통신서비스제공자가 준수하여야 할 중요한 의무 중 하나가 바로 개인정보의 수집·이용·처리 등에 관한 고지 또는 명시의무이다. 이는 이용자의 자기정보결정권을 보장하기 위해 정보통신서비스제공자에게 부과된 것으로, 이렇게 고지 또는 명시된 사항을 확인함으로써 이용자는 자신의 개인정보의 처리를 동의할 것인지 여부 등을 결정할 수 있다.

정보통신서비스제공자는 개인정보를 수집할 당시, 개인정보의 이용목적 변경시, 이용목적을 벗어난 이용 및 제3자 제공시 정보주체가 정보통신서비스제공자의 개인정보처리에 대해 알 수 있도록 고지하거나 이용약관에 명시하여야 한다. 정보보호법 제22조는 이러한 경우 정보통신서비스제공자가 이용자에게 고지·명시하여야 할 사항을 다음과 같이 구체적으로 규정하고 있다.

---

68) 그러나 정보통신서비스 이용계약의 이행을 위해 필요한 경우, 정보통신서비스 제공에 따른 요금정산을 위해 필요한 경우, 다른 법률에 특별한 규정이 있는 경우에는 이용자 동의 없이도 개인정보를 수집할 수 있다.(정보보호법 제22조제1항)

〔표 3-3〕 정보통신서비스제공자가 고지·명시하여야 할 사항

구분	고지·명시사항
개인정보 관리책임자	개인정보관리책임자의 성명·소속부서·직위, 전화번호 기타 연락처
항목 및 내용	정보통신서비스제공자가 수집하고자 하는 개인정보 항목
목적	개인정보의 수집 및 이용목적
기간	수집하는 개인정보의 보유기관 및 이용기간
제3자 제공에 관한 사항	개인정보를 제3자에게 제공하는 경우의 제공받는 자, 제공목적 및 제공할 정보의 내용
이용자의 권리	이용자의 개인정보 열람 및 정정요구권에 관한 사항
	이용자의 개인정보 동의철회 자유방법

이 외에도 정보통신서비스제공자는 영업의 양도·양수 및 합병시 이용자에게 통지하여야 할 의무를 부담하며, 고객상담업무의 위탁과 같이 제3자에게 개인정보의 수집·취급·관리 등을 위탁처리하는 경우에도 그와 같은 사실을 이용자가 인지할 수 있도록 고지하여야 할 의무가 있다.[69] 또한 정보보호법개정안 제22조제2항제5호는 정보통신서비스제공자가 인터넷 접속정보파일 등 자동으로 개인정보를 수집하는 장치의 설치·운영 및 그 거부에 관한 사항에 대해서 고지하거나 이용약관에 명시하도록 추가하고 있다.

(3) 목적외 이용 및 제3자 제공 금지의무

고지·명시된 개인정보의 수집 및 이용목적, 보유목적을 벗어나 개인정보를 부당하게 목적외로 이용하거나 제3자에게 제공하는 행위는 정보주체인 이용자의 자기정보결정권을 과도하게 박탈하는 심각한 개인정보 침해행위가 된다. 이에 정보보호법은 정보통신서비스제공자에게 원칙적으로 정보주체 본인의 동의가 있지 아니한 경우에는 이러한 목적외 이용 또는 제3자 제공을 엄격히 금지하고 있다. 단, 정보통신서비스의 제공에 따른 요금정산을 위해 필요한 경우, 통계작성 및 학술연구, 시장조사를

69) 정보보호법 제25조 및 제26조.

위해 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 가공하여 제공하는 경우, 다른 법률에 특별한 규정이 있는 경우에는 이용자의 동의 없이도 개인정보를 이용하거나 제공하는 것이 가능하다.[70]

(4) 개인정보의 안전한 관리의무

대부분 정보통신망을 통해 처리되는 개인정보는 대량복제·변조·수정·전송·저장 등이 매우 용이하기 때문에, 정보통신서비스제공자는 이러한 개인정보가 분실되거나 도난 또는 누출, 변조, 훼손되지 아니하도록 안전성을 확보할 의무가 있다.[71] 이를 위해서는 접근통제와 같은 물리적 보호조치, 암호인증이나 방화벽 설치와 같은 기술적 조치, 개인정보취급기준과 보안규정마련 또는 개인정보취급자의 정보보호의식 고취를 위한 교육 등과 같은 관리적 보호조치가 마련되어 시행되어야 한다.

또한 정보통신서비스제공자는 개인정보관리책임자를 지정하여 이용자의 개인정보를 보호하고 내부의 개인정보보호 관행을 향상시키며, 개인정보처리에 대한 이용자 불만을 처리할 수 있도록 하여야 하며[72], 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여 불필요한 개인정보침해의 가능성을 높여서는 안 된다.[73]

(5) 이용자의 권리를 보장할 의무

정보통신서비스제공자는 정보주체의 열람·정정요구권 및 자유로운 동의 철회권을 보장하여야 한다. 이를 위해 정보통신서비스제공자는 이용자가 열람·정정요구를 할 수 있는 담당자와 그 방법을 고지하여야 하고, 이

70) 정보보호법 제24조제1항.

71) 정보보호법 제28조.

72) 정보보호법 제27조.

73) 정보보호법 제24조제3항. 한편, 동조 제4항은 개별 개인정보취급자에게도 직무상 알게 된 개인정보의 훼손·침해 또는 누설을 금지하는 의무를 부과하고 있다.

용자의 자기 정보에 대한 열람 및 정정요구가 있는 때에는 지체없이 필요한 조치를 취하여야 한다.[74] 또한 오류의 정정요구를 받은 때에는 오류의 정정이 완료될 때까지 해당 개인정보를 이용하거나 제공하여서는 안 되며, 이용자가 사실상 동의철회를 하지 못하도록 방해하거나 어렵게 해서도 안 된다.[75] 예를 들어, 인터넷 사이트 가입시에는 특정한 서류를 요구하지 않았음에도 불구하고 회원 탈퇴시에는 본인확인이 필요하다는 명분으로 주민등록등본 또는 초본을 요구하는 것은 이용자의 동의철회권을 침해하는 것이다.[76]

(6) 개인정보의 즉시파기의무

정보통신서비스제공자는 개인정보의 수집 및 제공받은 목적을 달성한 때에는 당해 개인정보를 지체없이 파기하여야 하며, 이용자가 개인정보의 이용 및 제공 등에 관하여 동의철회를 한 때에도 이용자의 개인정보를 지체 없이 파기하는 등 필요한 조치를 취하여야 한다.[77] 그러나 다른 법률에서 개인정보를 보유하도록 의무를 부과하고 있거나, 이용자가 서비스 이용요금을 연체하는 등 당사자간 권리·의무관계가 정산되지 않은 경우에는 개인정보 즉시파기 의무는 적용되지 않는다.[78]

74) 정보보호법 제30조제4항.

75) 정보보호법 제30조제5항 및 제6항.

76) 제2차 개인정보분쟁조정위원회(2002. 1. 14)는 회원탈퇴시 주민등록등본을 팩스로 송부하도록 요구한 온라인 게임사이트의 행위는 이용자로부터 동의철회 요구를 받은 경우 개인정보의 수집방법보다 쉽게 할 수 있도록 필요한 조치를 취할 것을 규정한 정보보호법 제30조제6항 위반이라고 하면서, 회원탈퇴 절차를 개선할 것과 신청인의 개인정보를 즉시 파기할 것을 결정한 바 있다.

77) 정보보호법 제29조 및 제30조제3항.

78) 최근 이동통신업체가 해지고객의 개인정보를 모두 보유하고 있다는 주장이 제기되면서, 이러한 개인정보의 즉시파기의무가 다시 한 번 도마 위에 오르고 있다. 그러나 기업체의 경우 상법 제33조(상업장부등의 보존)의 적용을 받는데, 동조 제1항은 "상인은 10년간 상업장부와 영업에 관한 중요서류를 보존하여야 한다. 다만, 전표 또는 이와 유사한 서류는 5년간 이를 보존하여야 한다"고 규정하고 있어 정보보호법상 개인정보의 즉시파기의무와 배치될 수 있다. 따라서 해지고객이라 하더라도 어느 정도까지 고객정보를 보존하여야 하고 어느 정도를 파기하여야 하는지 논란이 될 수 있다.

라. 아동의 개인정보보호

정보보호법은 특히 만 14세 미만 아동의 개인정보를 보호하기 위한 특별 규정을 두고 있다. 이는 남녀노소를 가리지 않고 인터넷을 누구나 쉽게 이용할 수 있다는 점 및 아동을 대상으로 하는 게임이나 채팅 서비스를 제공하는 인터넷사업체가 증가하고 있다는 점에서 아직 판단능력과 식별력이 미숙한 미성년 아동을 보호할 필요성이 급증하였기 때문이다.[79] 이에 정보보호법 제31조는 정보통신서비스제공자가 만 14세 미만 아동의 개인정보를 수집·이용·제공하는 경우에는 반드시 법정대리인의 동의를 얻도록 규정하고 있다. 여기서 '법정대리인의 동의'는 진정한 의미의 동의를 의미하는 바, 우편이나 팩스를 통한 서면동의, 법정대리인의 전자서명이 있는 전자우편을 통한 동의, 기타 법정대리인의 진정한 동의가 있었음을 확인할 수 있는 합리적인 방법에 의한 동의가 있어야 한다.[80] 또한 동의를 얻는 주체는 아동이 아닌 정보통신서비스제공자이기 때문에, 단순히 아동으로부터 부모의 동의가 있었음을 확인하는 방법은 타당하지 않다.[81] 이 외에도 법정대리인은 아동의 개인정보에 대한 동의를 철회할 수 있으며, 아동의 개인정보에 대한 열람 또는 오류의 정정을 요구할 수 있다.

---

79) 실제로 인터넷으로 게임이나 채팅을 할 수 있는 웹사이트의 경우 아동을 대상으로 하는 것이 많은데, 이 때 아동의 개인정보를 수집하면서 부모 동의를 얻는 절차를 확실히 하지 않아 결과적으로 서비스 이용으로 인한 경제적 손해가 발생하는 등 사회 문제화가 되고 있다. 2003년 개인정보분쟁조정위원회에 제기된 민원 중에서도 이러한 법정대리인 동의없는 아동의 개인정보 수집 건은 전체 신청건수의 66.4%를 차지하여 가장 높은 비율을 보이고 있다.

80) 개인정보보호지침(정보통신부 고시 제2002-3호, 2002. 1월 고시) 제23조제3항. 한편, 정보통신부는 이를 더욱 구체화하여 '부모 동의를 얻는 요령'이라는 지침을 마련, 온라인 업체들이 참고할 수 있도록 하였다. 이에 의하면, 온라인 업체들은 자사가 제공하는 서비스의 특성이나 유·무료 여부, 회사정책 등을 고려하여 전자우편, 전화번호, 팩스, 우편, 신용카드번호 또는 신용카드 비밀번호, 핸드폰 인증번호 부여방식 등의 방법으로 부모 동의를 얻도록 하여야 한다고 규정하고 있다.

81) 제8차 개인정보분쟁조정위원회(2002. 7. 22)는 온라인게임사이트가 만 14세 미만 아동의 개인정보를 수집하면서 단지 '만 14세 미만 이용자로 부모님의 동의를 얻었습니다'라는 항목에 클릭토록 한 것은 정보보호법 제31조제1항에서 요구하는 진정한 법정대리인의 동의를 얻는 절차라고 보기 어렵다며, 이로 인해 청구된 이용요금 전액을 환불하고 아동의 개인정보를 즉시 파기토록 결정한 바 있다.

제 2 절 국내 개인정보보호기구

국내에서는 개인정보 관련 법률의 제정·시행과 함께 개인정보보호를 위한 환경을 조성하고 피해구제제도를 정착시킬 필요성이 꾸준히 제기되어 왔다. 특히 민간 사업자나 공공기관 등의 개인정보를 처리하는 자가 국내 개인정보 관련법령의 규정에 맞게 개인정보를 처리하고 보호하고 있는지를 관리·감독하고, 정보주체가 부당한 개인정보 침해로 인하여 입은 피해를 구제받을 수 있도록 지원하는 개인정보보호기구의 설치는 그 핵심내용이라 할 수 있다. 그러나 국내에는 개인정보에 관한 종합적 기능을 담당하는 전담 개인정보보호기구는 없다고 볼 수 있는 상태이다. 개인정보 관련 법규정이 산재해 있는 만큼, 개개 법령을 집행하고 관리·감독할 담당 행정부처 또는 동 법령에 의해 설립된 기구 등이 부분적으로 해당 분야의 개인정보보호 역할을 맡고 있을 뿐이다.

그러나 이러한 행정부처나 공공기관들을 모두 본래적 의미의 개인정보보호기구라고 확정짓기는 다소 어려움이 있다. 예를 들어, 신용정보보호법을 구체적으로 시행하고 신용정보 처리업자의 행위를 규율함으로써 일반 시민들의 개인신용정보를 보호하는 역할을 맡고 있는 것은 금융감독위원회(금융감독원)와 금융분쟁조정위원회이나 이들 기구의 주된 활동목적은 은행, 보험, 증권 등 금융 전반의 업무관행을 관리·감독하는 것이어서 개인정보보호는 그 중 극히 일부를 차지하고 있을 뿐이기 때문이다. 따라서 보다 정확한 의미에서 개인정보보호기구라고 함은 법률에 의해 명시적으로 개인정보보호기구로 지정된 기관만을 의미할 것이다. 이를 협의의 개인정보보호기구로 볼 수 있다. 그러나 우리나라의 현실상 이러한 협의의 개인정보보호기구가 개인정보와 관련된 모든 역할을 수행하는 것이 아니고 상당부분 다른 기구에 그 역할이 분산되어 있다는 것을 볼 때, 협의의 개인정보보호기구 뿐 아니라 실질적으로 개인정보 또는 프라이버시 보호의 역할을 담당하는 기구들을 폭넓게 살펴보는 것도 의미가 있을 것이다.

〔표 3-4〕 국내 개인정보보호기구 현황

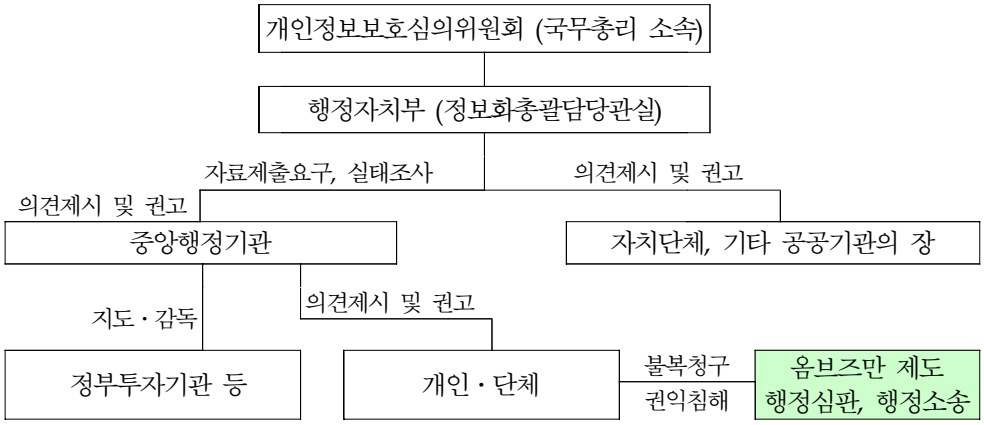
구분	기관명	관할범위	근거법령
공공부문	개인정보보호심의위원회	공공기관이 보유하는 개인정보	공공기관의개인정보보호에관한법률
	행정자치부		
	국민고충처리위원회	행정기관에 의한 민원사무처리로 인한 고충	민원사무처리에관한법률
민간부문	개인정보분쟁조정위원회	개인정보침해 일반	정보통신망이용촉진및정보보호등에관한법률
	한국정보보호진흥원	정보보호법 적용을 받는 자에 의한 개인정보침해	
	정보통신부		
	금융감독위원회	신용정보기관 등에 의한 신용정보처리 과정에서의 침해	신용정보의이용및보호에관한법률
	금융감독원		
	금융분쟁조정위원회		
	전자거래분쟁조정위원회	전자거래에서의 개인정보침해	전자거래기본법
	소비자보호원	소비자거래에서의 개인정보침해	소비자보호법
	소비자분쟁조정위원회		
기타	국가인권위원회	인권침해 일반	국가인권위원회법
	경찰청	형사처벌의 대상이 되는 개인정보침해	형법, 통신비밀보호법, 정보보호법 등

이하에서는 각 기구들의 특징, 주요 기능 등을 중심으로 살펴보도록 하겠다.

1. 공공부문

공공부문에서는 공공기관의 개인정보처리 현황과 실태를 조사하고 관리·감독을 총괄하는 행정자치부, 정부투자기관 등 공공기관에서 처리하는 개인정보를 보호하기 위해 의견을 제시하거나 지도·점검을 할 수 있는 관계 중앙행정기관의 장, 중요한 개인정보 관련 정책 및 입법사항을 심의·의결하는 개인정보보호심의위원회가 개인정보보호기구로서의 역할을 맡고

있다. 그러나 이러한 기구들은 모두 개인정보피해구제를 위한 적극적인 역할을 하지는 않고 있다. 따라서 정보주체는 행정심판 또는 행정소송을 제기하거나, 옴브즈만 제도의 하나인 국민고충처리위원회에 피해구제를 청구할 수 있다. 이러한 공공부문의 개인정보보호기구 및 그 체계는 아래 (그림 3-2)와 같다.



(그림 3-2) 공공기관의 개인정보보호기구 및 체계

※ 행정자치부, "공공기관의 개인정보보호제도 이해와 해설", 2003. 3, 8면.

가. 행정자치부

행정자치부는 공공기관의 개인정보보호제도의 전반을 총괄하는 성격을 가진 기관이다. 즉, 실질적인 지도·감독·점검 등의 관리책임은 관계 행정기관의 장에게 있다. 행정자치부가 공공기관에 의해 처리되고 있는 개인정보보호를 위해 수행하고 있는 기능과 권한은 아래와 같다.

첫째, 행정자치부장관은 정보주체의 개인정보자기결정권의 보장 및 공공기관 등의 개인정보처리 현황 파악 및 관리를 용이하게 하기 위한 목적으로 개인정보파일의 사전 통보 및 공고제도를 실시하고 있다. 이에 따라, 행정자치부장관은 관계 중앙행정기관의 장으로부터 해당 관할의

공공기관이 보유하고자 하는 개인정보파일의 명칭, 보유목적, 보유기관명, 개인정보의 모집방법, 처리정보를 통상적으로 제공하는 기관의 명칭 등을 사전 통보받을 수 있으며, 통보받은 개인정보파일은 연 1회 이상 관보에 공고한다.[82]

둘째, 행정자치부장관은 공공기관개인정보보호법의 시행을 위하여 필요한 경우 공공기관의 장에게 필요한 자료의 제출을 요구할 수 있다.행정자치부장관이 자료제출을 요구할 수 있는 기관은 개인정보를 보유하고 있는 모든 공공기관이며 개인정보처리 수탁기관이나 사전통보의무로부터 제외된 개인정보파일을 보유하고 있는 기관도 모두 해당된다. 행정자치부장관으로부터 자료제출요구를 받은 당해 공공기관은 정당한 사유가 있는 경우를 제외하고는 30일 이내에 자료를 제출하여야 한다. 행정자치부장관이 요구할 수 있는 자료는 ① 처리정보의 열람·정정청구현황 및 그 처리실적에 관한 자료, ② 처리정보가 기록된 자기매체·주전산기·입출력장치·전산실등의 보호대책에 관한 자료, ③ 처리정보의 제공실태와 제공에 따른 보호대책에 관한 자료, ④ 기타 개인정보보호에 관한 제도 및 정책의 수립·개선에 필요한 자료이다.[83]

셋째, 행정자치부장관은 필요한 경우 소속공무원으로 하여금 개인정보 보유 및 처리 실태조사를 실시할 수 있다. 실태조사대상은 관할 공공기관의 개인정보보호제도 전반에 관한 사항[84]이며, 행정자치부장관은 실태조사에 앞서 해당기관의 장에게 조사의 취지 및 내용, 담당공무원의 인적사항·조사일시 등을 미리 통보하여야 한다.[85]

---

82) 공공기관개인정보보호법 제6조～제7조 및 동법시행령 제4조～제7조.

83) 공공기관개인정보보호법 제18조 및 동법시행령 제22조.

84) 2003. 11월 행정자치부의 '개인정보처리 실태조사표' 양식을 통해 보면, ① 개인정보파일의 보유현황, ② 개인정보파일 보관 장소 및 형태, 보안 조치 등, ③ 개인정보파일의 공동이용(타기관 제공) 현황, ④ 개인정보파일의 제공거부사례, ⑤ 유출사고 등 법위반 사례 및 조치결과, ⑥ 개인정보의 전문업체 위탁처리 내역, ⑦ 개인정보의 열람 및 정정청구 현황 및 처리실적, ⑧ 산하기관에 대한 자체 지도 및 점검실적, ⑨ 개인정보 유출사고 접수사례 및 처리결과, ⑩ 단말기 및 입출력 자료의 관리 등이 실태조사 대상 및 항목에 해당된다. (행정자치부 홈페이지, http://www.mogaha.go.kr 참조)

85) 공공기관개인정보보호법 제18조 및 동법시행령 제23조.

넷째, 행정자치부장관은 자료제출요구 또는 실태조사 등을 통해 파악한 결과를 바탕으로 필요한 경우에 공공기관의 장에게 개인정보보호제도에 관하여 의견을 제시하거나 권고를 할 수 있다. 주로 해당 공공기관이 위법하거나 부당한 행위를 하여 개인정보가 침해되었거나 침해될 우려가 있는 경우에 이러한 의견제시 또는 권고를 행할 수 있다.[86]

이렇듯 행정자치부장관은 공공기관개인정보보호법에 의거하여 중앙행정기관이나 자치단체, 또는 기타 공공기관의 장에게 개인정보처리에 대한 의견을 제시하거나 권고 및 실태조사를 수행할 수 있으며, 정보주체의 열람권 보장 등을 위한 개인정보파일의 공고시행 등의 역할을 담당하고 있다. 그러나 이러한 기능에는 명백히 한계가 있다. 행정자치부가 공공기관에 대한 총괄적인 지도·감독의 기능을 수행한다고는 하나, 개인정보보호를 전담하는 부서 또는 인력이 전무하기 때문이다. 따라서 공공기관에서 처리되고 있는 개인정보가 침해되거나 유출 또는 오·남용되는 사례를 직접 적발하고 적절한 제재조치를 가하는 등 적극적인 역할을 담당하기에는 어려움이 있다고 할 것이다.

나. 개인정보보호심의위원회

개인정보보호심의위원회는 공공기관개인정보보호법 제20조에 근거하여 1995년 4월 설립된 법정기구이다. 개인정보보호심의위원회는 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의·의결하기 위해 국무총리 산하에 설립된 기구이다. 그러나 현실적으로 위원회의 구성·운영 및 인사·행정상의 지원 등은 국무총리실이 아닌 행정자치부가 맡고 있다.

위원회는 위원장 1인을 포함한 10인 이내의 위원으로 구성된다. 위원장은 행정자치부차관이 임명되며, 그 밖의 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자 중에서 위원장이 추천하여 국

86) 공공기관개인정보보호법 제19조 및 동법시행령 제24조.

무총리가 임명 또는 위촉한다.[87] 위원의 임기는 2년이나, 공공기관의 소속직원인 위원은 그 직에 있는 동안 재임한다.

위원회는 기본적으로 공공기관의 개인정보보호를 위해 필요한 사항이나 쟁점이 되는 문제 등을 심의하는 역할을 하고 있다. 위원회의 구체적인 심의사항은 ① 개인정보보호에 관한 정책 및 제도개선에 관한 사항, ② 처리정보의 이용 및 제공에 대한 공공기관간의 의견조정에 관한 사항, ③ 개인정보파일에 기록되어 있는 개인정보항목의 전부 또는 일부를 관보에 게재하지 아니하려는 경우 그에 관한 사항, ④ 기타 관련법령 등의 정비·개선에 관하여 위원장이 부의하는 사항이다. 즉, 위원회는 중요한 개인정보 정책이나 제도를 심의하는 기능만을 가질 뿐, 의견제시나 시정권고 등은 행정자치부가 담당하고 피해구제는 행정심판, 행정소송 등의 행정구제와 국민고충처리위원회가 그 역할을 하고 있다.

다. 국민고충처리위원회

국민고충처리위원회는 행정기관의 위법·부당한 처분(부작위 및 거부처분포함), 사실행위, 불합리한 행정제도 등으로 인하여 국민의 권리를 침해하거나 불편·부담을 주는 사항에 대한 민원을 신속하고 간편하게 처리해주는 피해구제 기구의 하나이다. 특히 국민고충처리위원회는 피해구제의 대상을 법률상 권리나 이익이 있는 자에 한정하고 그 판단도 합법성 여부를 기준으로 하는 형식적인 기존의 행정심판제도나 행정소송과 같은 피해구제제도의 단점을 극복하여, 법률상으로 해결할 수 없는 고충민원을 실질적으로 구제하기 위해 마련된 옴브즈만 제도의 일종이다. 즉, 국민고충처리위원회는 기존의 피해구제제도를 통해서 구제를 받지 못하는 국민의 권익을 제3자적 입장에서 간이·신속한 절차로 공정하게 조사·심의하고 있다는 특징을 가진다.[88]

---

87) 개인정보보호심의위원회의 위원은 당연직 5명과 위촉직 5명으로 구성되고 있는데, 당연직 5명은 정부부처 공무원이다.

88) 국민고충처리위원회 웹사이트, http://www.ombudsman.go.kr 참조.

이와 같이 국민고충처리위원회는 행정기관에 의한 부당한 처분 등을 관할대상으로 하고 있기 때문에, 행정기관이 정보주체의 열람·정정요구를 정당한 이유 없이 거부하거나 정보주체의 권리행사를 방해하는 등의 행위를 한 경우, 그로 인해 피해를 입은 자는 국민고충처리위원회에 민원을 제기할 수 있다. 국민고충처리위원회는 접수된 사건에 대하여 조사를 행한 결과, 행정기관의 처분 등이 위법·부당하다고 인정할만한 상당한 이유가 있는 경우에는 관계 행정기관의 장에게 시정조치를 권고할 수 있다. 또한 법령·제도·정책 등의 개선이 필요하다고 인정될 경우 해당 행정기관의 장에게 합리적인 개선을 권고하거나 의견을 표명할 수 있다. 그러나 현실적으로 위원회는 개인정보침해사건이나 프라이버시 침해문제를 직접 처리하지 않고 있으며 대부분 해당 부처나 행정자치부로 이첩하고 있다.

라. 행정구제

앞서 살펴본 것처럼 행정자치부장관은 개인정보피해구제보다는 공공기관의 개인정보처리에 대한 조사·감독을 총괄하는 기능이 강하고, 개인정보보호심의위원회 역시 정책적 제도개선에 대한 심의나 기관간 의견을 조정하는 역할을 주로 할 뿐, 정보주체의 권리구제의 역할은 담당하지 않고 있다. 이렇듯 기존의 행정자치부와 개인정보보호심의위원회의 제한적인 개인정보보호 역할만으로는 오늘날 시대가 요구하는 수준의 개인정보보호를 기대하기 어렵다는 한계가 있다. 이러한 문제점을 개선하기 위해 행정자치부는 지난 8월 공공기관개인정보보호법 개정안을 입법예고하였는데, 동 개정안은 공공기관의 개인정보처리과정에서 발생하는 각종 개인정보침해사고의 신고를 접수받아 처리하고 정보주체의 불만을 해소할 수 있는 개인정보보호 전담기구로서 '개인정보침해신고센터'를 설치하고, 개인정보보호심의위원회의 사전심의기능을 강화하는 것을 내용으로 하고 있다.

그러나 이러한 개선안에도 개인정보침해로 인한 피해를 구제해 주는 역할을 수행할 수 있는 기구의 설립이나 권한부여의 내용은 없다. 물론 현재도 국민고충처리위원회는 일종의 옴브즈만의 역할을 함으로써 이러한 공공부문 개인정보피해구제제도의 미비상태를 보완해줄 수 있지만, 실질적으로 개인정보침해로 인한 피해와 권익을 구제해주는 역할을 적극적으로 담당하지는 않고 있다. 따라서 현재로서는 정보주체의 열람 및 정정청구와 같은 권리가 거부되거나 침해되어 피해를 입은 경우 및 공공기관에서의 개인정보의 유출이나 오·남용으로 인한 피해를 입은 경우, 정보주체는 행정심판 또는 행정쟁송 등을 통해서 불복청구를 할 수 있을 뿐이다.[89]

2. 민간부문

민간부문의 개인정보보호기구 현황은 공공부문보다 더욱 복잡하다. 공공부문에서는 행정자치부에서 모두 총괄할 수 있지만, 민간부문은 개별법률을 시행하고 주관하는 행정부처가 정보통신부, 재정경제부, 산업자원부, 보건복지부 등 다양하기 때문이다. 따라서 이러한 개별 법률을 집행하면서 개인정보보호의 역할을 맡고 있는 기구도 다양함은 이미 살펴본 바와 같다. 그러나 이 중에서도 개인정보분쟁조정위원회는 개인정보침해 일반에 대한 피해구제의 기능을 수행하고 있는 바, 민간부문의 대표적인 개인정보보호기구로 볼 수 있을 것이다. 이하에서는 개인정보분쟁조정위원회를 비롯한 민간부문의 개인정보보호기구의 주요 기능과 특징 등을 살펴보도록 하겠다.

가. 정보통신부

정보통신부장관은 개인정보보호를 위한 정책을 수립하고 정보보호법이

89) 행정심판제도나 행정소송제도는 본 연구 목적상 자세히 다룰 만한 사항은 아니므로 그 피해구제절차나 방법을 여기서 논하지는 않겠다.

올바르게 시행되도록 할 책임이 있다. 이를 위해 정보통신부장관은 개인정보관리책임자의 지정요건 등 개인정보보호를 위해 필요한 사항을 지침 등을 통해 정할 수 있다. 뿐만 아니라 필요한 경우 정보통신서비스제공자 등에게 관계물품·서류 등을 제출하게 할 수 있고 소속공무원으로 하여금 정보통신서비스제공자 등의 사업장에 출입하여 업무상황·장부 또는 서류 등을 검사하게 할 수 있다. 정보통신부장관은 이러한 자료제출요구권 및 검사·조사권 외에도 법위반사실이 인정될 경우 해당 정보통신서비스제공자등에 대하여 필요한 시정조치를 명하거나 과태료를 부과할 수 있는 행정 제재권을 가진다.[90]

즉 정보통신부는 정보보호법의 적용을 받는 정보통신서비스제공자 등이 정보통신서비스이용자의 개인정보를 법률 규정에 맞게 보호하고 있는지를 조사하고 감시할 뿐 아니라 필요한 경우 적절한 제재조치를 취함으로써 정보보호법이 실효성을 가질 수 있도록 집행하는 역할을 맡고 있는 것이다. 이를 위해 정보통신부는 한국정보보호진흥원 내에 개인정보침해신고센터를 설치하여 운영하고 있다.[91] 2000년 4월 13일 설립된 개인정보침해신고센터는 개인정보침해방지 및 보호를 위하여 정통부가 시행하는 사업자에 대한 자료제출요구, 실태조사·검사 등을 지원하는 역할을 맡고 있으며, 개인정보침해 및 광고성 정보전송에 관련한 고충처리 및 상담, 개인정보침해대책 연구, 교육·홍보 등을 그 업무로 하고 있다.[92] 특히 정보보호법의 적용을 받는 관할 대상영역의 사업자의 개인정보침해에 대하여 상담을 하고 신고를 접수받는 역할을 주로 담당하고 있어, 신고가 접수된 위법사실에 대해서는 정보통신부에 통보하여 행정제재를 취할 수 있도록 조치하고 있다. 개인정보침해신고센터의 연도별 침해신고 및 상담접수 현황은 아래와 같다.

---

90) 정보보호법 제55조.

91) 정보보호법 제52조제3항제8호.

92) 정보보호법시행령 제26조.

［표 3-5］개인정보침해신고센터의 개인정보 상담·신고 접수현황

구 분	2000년	2001년	2002년	2003년	계
신 고	329	388	1,237	8,991	10,945
상 담	1,706	10,776	16,719	12,594	41,795
계	**2,035**	**11,164**	**17,956**	**21,585**	**52,740**

(단위 : 건)

정보통신부는 개인정보침해신고센터로부터 통보받은 개인정보침해사건에 대하여 과태료 부과, 시정명령, 형사기관 수사의뢰 등의 조치를 취할 수 있다. 다음은 정보통신부가 2000년부터 2003년까지 개인정보침해사업자에 대하여 취한 조치내역이다.

［표 3-6］정보통신부의 조치내역

구 분	과태료	시정명령	수사의뢰
2000년 7~12월	15	251	2
2001년	22	42	3
2002년	32	130	-
2003년	23	266	60
계	**92**	**689**	**65**

(단위 : 건)

정보통신부는 비록 규율 영역이 한정되어 민간 영역의 모든 개인정보침해사건에 대해 과태료를 부과하거나 시정명령을 내리는 등 제재권한을 행사할 수는 없다. 그렇지만 정보보호법에 따라 개인정보침해 가능성이 높은 온라인사업자, 통신사업자, 학원·여행사 등 일부 오프라인 사업자 등을 직접 규율함으로써 민간영역의 개인정보보호에 있어 중요한 역할을 담당하고 있다.

나. 개인정보분쟁조정위원회

개인정보분쟁조정위원회는 개인정보침해와 관련된 분쟁을 신속·간편·공정하게 해결하기 위한 목적으로, 정보보호법 제33조에 의거하여 설립되었다. 위원회가 행하는 피해구제 방법은 분쟁조정제도인데, 이는 개인정보 관련분쟁의 해결을 위해 위원회가 분쟁당사자의 주장과 사실관계를 기초로 하여 공정하고 합리적인 조정안을 제시함으로써 다툼을 평화적으로 해결하는 분쟁해결방법이다. 위원회는 국내에서 유일하게 개인정보와 관련된 분쟁을 전문적으로 조정하기 위해 설치된 기구라는 점에서 개인정보피해구제에 있어 중대한 역할을 담당하고 있다고 볼 수 있다.

(1) 위원회의 구성

위원회는 위원장 1인을 포함한 15인 이내의 위원으로 구성되며 이 중 1인은 상임으로 한다. 위원장과 위원은 정보통신부장관이 임명 또는 위촉하며, 위원장 및 위원의 임기는 3년으로 연임이 가능하고 법률에 의해 임기가 보장된다. 위원으로 임명 또는 위촉될 수 있는 자격조건은 정보보호법 제33조에서 상세히 규정하고 있다.[93] 현재 위원회는 이러한 자격요건에 따라 위촉된 교수, 법률가, 기술전문가, 사업자 및 소비자단체 추천인사, 관계공무원 등 각계의 전문가들로 구성되어 있다. 2003년 12월말 기준으로 개인정보분쟁조정위원회의 위원구성 현황은 아래와 같다.

---

93) 정보보호법 제33조에 의하면, 위원회는 다음 각호의 자격을 가진 자가 1인 이상 포함되어야 한다.
1. 대학이나 공인된 연구기관에서 부교수급 이상 또는 이에 상당하는 직에 있거나 있었던 자로서 개인정보보호관련 분야를 전공한 자
2. 4급 이상 공무원 또는 이에 상당하는 공공기관의 직에 있거나 있었던 자로서 개인정보보호업무에 관한 경험이 있는 자
3. 판사·검사 또는 변호사의 자격이 있는 자
4. 정보통신서비스이용자단체의 임원의 직에 있거나 있었던 자
5. 정보통신서비스제공자 또는 정보통신서비스제공자단체의 임원의 직에 있거나 있었던 자
6. 비영리민간단체지원법 제2조의 규정에 의한 비영리민간단체에서 추천한 자

［표 3-7］ 개인정보분쟁조정위원회의 위원구성 현황

구분	학계	법률가	기술 전문가	소비자 단체	사업자 단체	기타	계
위원수	5	5	1	1	1	1	14

(단위 : 명)

개인정보분쟁조정위원회는 신청된 사건의 개인정보침해 및 위법성 여부에 대하여 판단을 내리고 이를 바탕으로 조정결정을 내리기 때문에, 위원구성에 있어서도 학계와 법률가의 비중이 높은 편이다. 그러나 개인정보관련 분쟁이 기술적 측면과 상당부분 관련이 높아 기술전문가가 조정위원으로 참여하고 있으며, 공정성을 확보하기 위한 방안으로 사업자와 소비자대표가 각각 분쟁조정위원으로 위촉되어 활동하고 있다. 이러한 위원구성은 위원회의 전문성과 공정성을 확보하는 중요한 요소가 되고 있다.

(2) 위원회의 조정범위

위원회의 설립근거인 정보보호법 제33조에 의하면, 위원회는 '개인정보에 관한 분쟁'의 해결을 위하여 설립된 기구이다. 따라서 원칙적으로 정보보호법에서 정의하는 개인정보와 관련된 분쟁이면, 온라인・오프라인을 불문하고 모두 위원회의 조정대상이 된다. 그러나 공공기관개인정보보호법의 적용을 받는 국가, 정부단체, 지방자치단체, 학교, 공기업 등에서 수집・보유・관리하는 개인정보는 위원회의 조정범위에 포함되지 않는다. 즉, 위원회는 순수하게 민간영역에서의 개인정보 관련 분쟁만을 조정대상으로 보고 있으며, 그 중에서도 영리목적으로 서비스를 제공하는 사업자에 의한 개인정보침해 관련 분쟁이 위원회의 주요 조정대상이다. 그러나 분쟁조정위원회는 신용정보와 의료정보와 같이 당해 분쟁이 개인정보와 관련된 사안일지라도 다른 분쟁조정기구에서 처리하는 것이

더 합리적이고 타당하다고 판단할 경우에는 당해 사건을 이관하거나 신청인에게 안내할 수 있다.

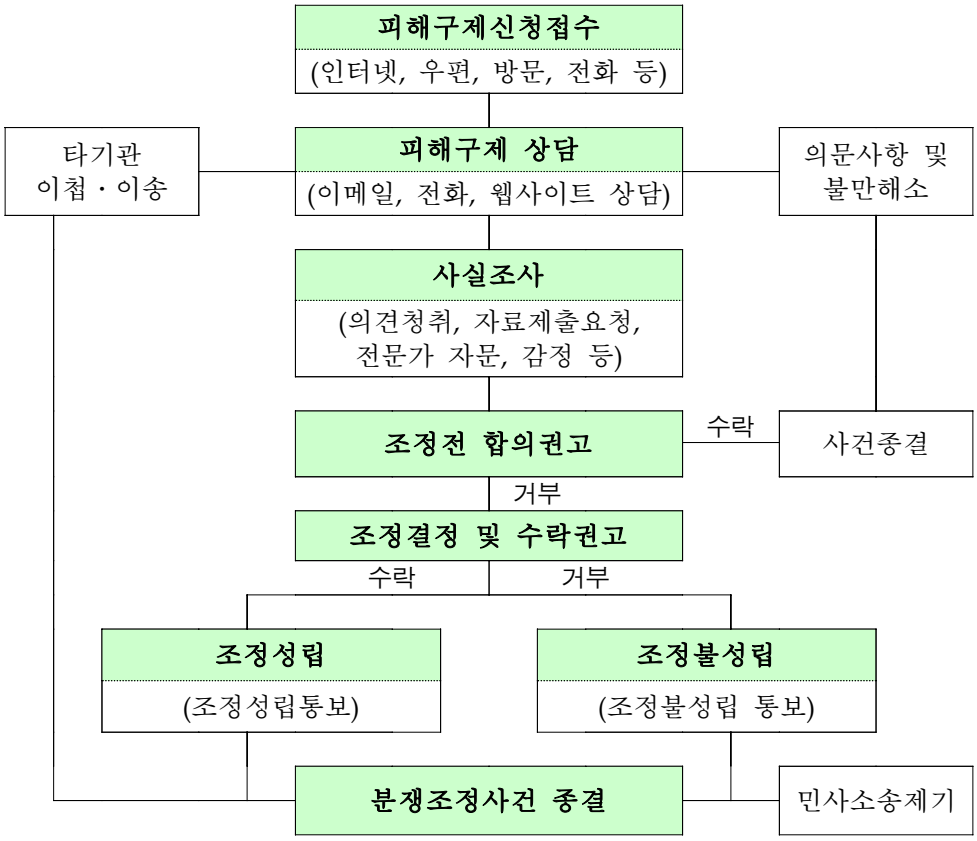
(3) 분쟁조정절차

분쟁조정절차의 첫 단계는 개인정보에 관한 분쟁조정신청의 접수이다. 현재 개인정보분쟁조정위원회는 전화, 인터넷 웹사이트, 우편, 방문, 팩스 등을 통해 분쟁조정신청을 접수받고 있으며, 이 중 인터넷을 통한 분쟁조정신청이 대다수를 차지하고 있다. 개인정보분쟁조정 신청은 무료이며, 개인정보침해를 입은 피해자는 물론 가해자인 사업자도 위원회에 분쟁조정신청을 할 수 있다.

위원회는 일단 사건이 접수되면, 당해 사건이 위원회의 관할범위에 해당되는지 여부를 판단하여 명백히 위원회의 관할범위가 아닌 경우에는 다른 기관을 안내 또는 이관할 수 있다. 또한 법제도에 대한 단순문의 등은 상담을 통해 종결할 수 있다. 그러나 이 외의 분쟁조정사건에 대해서는 양 당사자의 주장사실을 확인하고 증빙자료를 요청하여 사실관계를 조사하게 된다. 분쟁조정 신청자는 이러한 위원회의 사실조사에 협조하여 주장사실을 입증할 수 있는 최소한의 자료를 제출하여야 한다. 위원회는 당사자가 제출한 증거자료 및 당사자 쌍방의 의견청취, 외부 전문가 자문 또는 감정 등의 방법으로 사실확인을 거친다. 또한 위원회는 사실이 어느 정도 확인이 되면, 공식적인 조정결정을 내리기에 앞서 당사자에게 합의를 권고할 수 있다. 대부분 합의권고는 위원회 사무국의 사건 조사담당관이 사실조사 과정에서 분쟁 당사자에게 서로의 주장을 이해시키고 합의에 이르도록 유도함으로써 이루어진다.

위원회는 사전 합의권고에도 불구하고 분쟁이 원만히 해결되지 않은 복잡한 사건에 대해서는 조정결정을 내리게 된다. 위원회는 당사자의 주장 및 사실관계를 파악하여 개인정보침해행위가 있는지 여부, 법위반 사실이 명백한지 여부, 개인정보침해로 인해 신청인이 경제적·정신적 손해를 입었는지 여부 등을 종합적으로 판단하고 심의한다. 위원회는 심

의한 결과를 바탕으로 분쟁 당사자에게 합당한 조정안을 작성하여 제시하고 수락을 권고하게 된다. 만약 양 당사자가 위원회의 조정안을 수락하는 경우에는 조정성립으로, 일방 당사자가 거부하는 경우에는 조정불성립으로 조정절차는 종결되게 된다. 원칙적으로 이러한 분쟁조정절차는 조정신청이 있은 날로부터 60일 이내에 완료되어야 하는데, 이는 사건이 지연됨으로써 신청인이 불합리한 피해를 입는 것을 방지하기 위함이다.[94]



(그림 3-3) 개인정보분쟁조정위원회의 분쟁조정절차

94) 정보보호법 제36조제2항.

(4) 분쟁조정의 효력

분쟁조정위원회는 심의한 결과를 토대로 양 당사자에게 조정안을 제시할 수 있다. 만약 조정안을 제시받은 당사자 쌍방이 조정안을 받은 날로부터 15일 이내에 위원회에 수락의사를 표시한 때에는 당사자간 조정서와 동일한 내용의 합의가 성립한 것으로 본다.[95] 즉, 이 경우 분쟁조정을 통한 합의는 민사상 화해계약과 같은 효력을 가진다. 그러나 만약 당사자 중 일방이라도 조정안을 거부한 때에는 조정은 불성립으로 종결되며 피해자는 민사소송을 통해 피해구제를 요청할 수밖에 없다. 즉, 분쟁조정위원회의 조정은 어떠한 강제력이나 집행력도 가지지 않는다. 그렇기 때문에 분쟁조정의 실효성을 담보하지 못할 수도 있다는 우려가 있지만, 대부분의 개인정보침해의 경우 행정적·형사적 제재가 따르기 때문에 위원회는 정보통신부나 경찰청에 위법사실을 통보하여 처벌을 유도함으로써 분쟁조정의 실효성을 확보하고 있다.[96]

(5) 위원회의 피해구제 성과

개인정보분쟁조정위원회는 2001년 12월 3일 발족 이래 2003년 12월까지 약 2년여 간, 총 2,082건의 개인정보침해사건을 접수하여 처리하였으며 위원회도 총 25회 개최되어 960건의 분쟁조정안건을 심사하여 결정하였다. 분쟁조정위원회에 접수된 개인정보 피해구제 신청 현황은 아래와 같다.

---

95) 정보보호법 제38조.

96) 개인정보분쟁조정위원회는 2002년 2건, 2003년 3건의 위법사실을 정보통신부에 통보하였고, 2002년에는 1건을 경찰청에 이첩하기도 하였다. 위법사실을 통보하는 경우는 주로 위원회의 조정결정에 사업자가 불응하여 조정이 불성립된 사건 중 위법사실이 중하다고 판단되는 경우이다.

［표 3-8］ 개인정보분쟁조정위원회의 피해구제 신청현황

구분	1월	2월	3월	4월	5월	6월	7월	8월	9월	10월	11월	12월	계
‘02년	32	53	55	58	44	28	143	207	132	142	202	141	1,237
‘03년	100	57	93	35	32	37	70	60	46	89	46	180	845

(단위 : 건)

이와 같이 위원회는 2년여 간 2000건이 넘는 피해구제 신청사건을 접수하여 분쟁을 해결하고 처리함으로써, 민간영역에서의 개인정보피해구제의 중추적인 역할을 담당하였다.[97] 특히, 위원회는 2002년과 2003년 총 1,222건에 대하여 조정결정을 하였는데, 이 중 위원회를 통해 당사자간 분쟁이 원만히 해결되어 조정성립된 사건은 1179건(조정전 합의권고 포함)으로 전체 조정결정사건의 96.5%의 비율을 차지하여 매우 높은 조정성립율을 나타내고 있다. 또한 분쟁조정위원회는 개인정보침해로 인한 경제적 손해배상은 물론 정신적 손해배상도 적극적으로 인정하고 있어, 개인정보침해로 인한 피해를 보다 실질적으로 구제하는 모습을 보이고 있다.

［표 3-9］ 2003년도 개인정보분쟁조정위원회의 조정결정

조정결정 유형	건수	비율
경제적・정신적 피해보상	396	79.7%
경제적 피해보상	15	3%
정신적 피해보상	13	2.6%
회원탈퇴 등 기타 피해구제 조치	67	13.5%
기타	6	1.2%
계	**497**	**100%**

(단위 : 건)

97) 위원회 조정사건이 2002년에 비해 2003년도에 줄어든 이유는 2002년에는 위원회에서 모든 개인정보침해사건을 통일적으로 다루었으나, 2003년부터는 개인정보침해사건 중 피해구제사건은 위원회에서, 불만처리사건은 한국정보보호진흥원(개인정보침해신고센터)에서 각기 분할하여 처리하고 있기 때문이다.

다. 통신위원회

(1) 설립 및 기능

통신위원회는 1992년 3월 통신사업의 공정한 경쟁환경 조성 및 통신서비스 이용자의 권익보호에 관한 사항을 심의하고 통신사업자간 및 통신사업자와 이용자간의 분쟁을 재정하기 위하여, 전기통신기본법 제37조의 규정에 따라 정보통신부에 설치된 기구이다. 위원회는 위원장 1인과 상임위원 1인을 포함한 9인 이내의 위원 구성되며, 위원은 정보통신부 장관의 제청으로 대통령에 의해 임명 또는 위촉된다.[98] 또한 전기통신기본법 제39조에 따라 법률에 규정한 사항이 아니고서는 그 의사에 반하여 해임되거나 해촉되지 않도록 하고 있어 신분을 보장받고 있다. 현재 통신위원회에는 약관·법령심의위원회, 회계전문심의위원회, 통신요금심의위원회가 활동하고 있으며, 위원회 운영 및 업무를 지원하는 사무국을 두고 있다.

통신위원회의 기능은 크게 조사, 심의·의결, 재정, 관리의 네 가지로 볼 수 있다. 첫째, 통신위원회는 통신사업자의 이용약관 위반이나 협정위반 등 불공정행위 및 이용자의 이익을 저해하는 행위 등에 대하여 사실조사를 행할 수 있으며[99], 이러한 사실조사 결과 나타난 위법행위에 대해서 시정조치 및 과징금 부과에 관한 사항을 의결할 수 있다. 둘째, 전기통신번호관리세칙 등 정보통신부 장관이 검토를 요청하는 전기통신 관련 고시·기준·제도·계획 등에 대한 사항과 상호접속협정 등 통신사업자간 협정의 인가 여부 등에 관한 사항을 심의하는 기능을 담당한다. 셋째, 통신사업자간 협정의 체결 및 이행, 통신사업자와 이용자간 손해배상 등과 관련된 분쟁의 알선 또는 재정 의결 등을 통해 통신사업자의 부당행위로 인해 피해를 입은 소비자의 분쟁을 해결해주는 사후 피해구제의 역할도

98) 전기통신기본법 제37조~제38조.

99) 전기통신기본법 제43조에 따라, 통신위원회는 재정사건의 처리를 위하여 당사자 및 참고인에게 출석을 요구하여 의견청취를 할 수 있다. 또한 감정요구, 문서 또는 물건의 제출요구 및 영치, 분쟁사건과 관련된 사업장에 출입하여 관련 문서 또는 물건을 조사·열람 또는 복사할 수 있는 권한을 가진다.

맡고 있다. 넷째, 기간통신사업자 영업보고서의 검증, 전기통신번호의 부여 및 관리 등 관리 기능도 함께 수행하고 있다.[100] 이 중 첫 번째와 세 번째의 기능이 통신사업자의 개인정보침해행위로 인하여 소비자가 입은 피해를 구제하는 역할과 관련이 있는 것으로 볼 수 있는데, 통신위원회가 행하는 피해구제절차를 간략하게 살펴보면 아래와 같다.

(2) 피해구제절차[101]

통신위원회는 통신사업자의 불공정행위에 대하여 실태조사를 할 수 있는 권한을 부여받았을 뿐 아니라, 사업자와 이용자간 분쟁을 알선하고 재정하여 원만히 해결될 수 있도록 하는 준사법적 권한도 가지는 바, 이러한 통신사업자의 불공정행위의 사후 규제 및 소비자 권익보호를 위해 통신관련 민원을 접수받아 처리하고 있다. 여기에는 통신사업자의 협정위반행위, 이용약관위반행위, 소비자 이익저해행위와 같은 불공정행위 및 통신사업자와 이용자의 손해배상 및 실비보상 관련 분쟁 등 모든 통신관련 민원이 해당된다. 통신위원회가 행하는 피해구제를 제재적 측면과 분쟁해결적 측면으로 나누어 보면, 전자는 통신사업자의 불공정행위에 대한 처리가 해당되고 후자에는 재정사건의 처리가 해당된다.

먼저, 통신위원회는 전기통신사업자의 불공정행위에 대하여 직권 또는 신고에 의하여 불공정행위 조사에 착수할 수 있다. 실질적인 사실조사는 사무국에 의해 이루어지는데, 사무국은 접수·인지된 사건의 조사를 위하여 당사자 및 이해관계인 또는 참고인 등의 의견을 청취하거나 관련 자료를 요청할 수 있으며, 필요한 경우 현장조사를 실시하거나 전문가의 자문을 구할 수도 있다. 이렇게 1차 조사가 완료된 사건은 상임위원에게 보고되며 상임위원은 사실판단에 오인이 있는지, 추가적인 보완조사가 필요한지 등을 검토하여 필요한 조치를 명할 수 있다. 또한 상임위원은

100) 전기통신기본법 제40조 및 통신위원회 웹사이트, http://www.kcc.go.kr 참조.

101) 통신위원회의 불공정행위사건 및 재정사건에 대한 처리절차에 대해서는 통신위원회, "통신위원회 심결집", 2003, 5~8면을 참고하였다.

불공정행위에 대한 증거가 존재하지 않거나 전기통신사업자에 대한 시정조치가 필요하지 않은 것이 명백하다고 인정하는 경우에 한하여 조사절차를 종결할 수 있다. 그러나 불공정행위가 명백하여 시정조치가 필요하다고 판단될 경우, 사무국장은 불공정 행위의 정도와 시정조치에 따른 실익 등을 감안하여 시정조치안을 작성하고 당사자의 의견을 들은 후, 이를 통신위원회에 상정하게 된다. 통신위원회는 재적 과반수의 찬성으로 시정조치안을 심의·의결하며, 정보통신부 장관은 결과에 따라 상당한 기간을 정하여 당해 전기통신사업자에게 시정을 명한다. 그러나 이에 대해 불복이 있는 자는 그 처분의 통지를 받은 날부터 20일 이내에 사유를 갖추어 통신위원회에 이의신청을 할 수 있다. 통신위원회가 내리는 시정조치는 전기통신사업법 제37조의 규정에 의한 조치[102] 또는 동법 제37조의2의 규정에 의한 과징금 부과 등을 그 내용으로 한다.

또한 통신위원회는 전기통신기본법 제40조의2에 의거하여 사업자의 이용자에 대한 손해배상, 실비보상, 상호접속 등 협정의 체결·이행 또는 사업자간 손해배상에 관한 사항에 대하여 분쟁의 알선 및 재정결정을 내릴 수 있다. 단, 통신위원회에 대한 재정신청은 당사자간 재정사항에 대한 협의가 이루어지지 아니하거나 협의할 수 없는 경우에 한한다.

통신위원회는 재정신청이 접수되면 위원회 사무국 소속공무원으로 하여금 의견청취, 청문, 증거조사, 자료제출, 참고인 조사, 전문가 자문, 감정 등의 사실확인절차를 거치도록 한다. 이렇게 사실조사가 완료된 사건은 통신위원회에 상정되는데, 통신위원회는 재정신청이 이유 있다고 인정할 때에는 전부 또는 일부의 손해배상 및 실비보상과 일정한 의무를 부과한다는 내용의 협정체결 또는 협정이행을 명하는 재정결정을 할 수 있다. 통신위원회가 재정을 한 때에는 2주일 내에 재정서를 당사자에게

---

102) 여기에는 ① 전기통신역무 제공조직의 분리, ② 전기통신역무에 대한 내부회계규정 등의 변경, ③ 전기통신역무에 관한 정보의 공개, ④ 전기통신사업자간 협정의 체결·이행 또는 내용의 변경, ⑤ 전기통신사업자의 이용약관 및 정관의 변경, ⑥ 금지행위의 중지, ⑦ 금지행위로 인하여 시정조치를 명령받은 사실의 공표, ⑧ 금지행위의 원인이 된 전기통신설비의 수거 등 금지행위로 인한 위법사항의 원상회복에 필요한 조치, ⑨ 기타 대통령령이 정하는 사항이 해당된다.

송달한다. 당사자가 재정에 대하여 불복하는 경우에는 재정서 정본이 당사자에게 송달된 날로부터 60일 이내에 소송을 제기하여야 한다. 당사자가 60일내에 소송을 제기하지 아니하거나 소송이 취하된 때에는 당사자간에 당해 재정내용과 동일한 합의가 성립된다. 한편, 통신위원회는 재정신청을 받은 경우에 재정을 하기에 부적합하거나 기타 필요하다고 인정하는 때에는 분쟁사건별로 분과위원회를 구성하여 이에 관한 알선을 할 수 있다.[103]

(3) 개인정보보호 기능 및 역할

통신위원회는 통신사업자 상호간의 협정위반행위는 물론이고 통신사업자의 위법·부당한 행위로 인하여 소비자가 피해를 입은 경우 통신사업자에 대한 시정조치 및 과징금 부과와 같은 사항을 의결하고, 그로 인한 손해배상 등의 문제가 발생하였을 경우에는 재정결정을 함으로써 소비자의 권익을 보호하는 기능을 하고 있다.

유·무선 정보통신서비스가 활발히 이용되고 있는 것과 비례하여, 이동통신사, 인터넷 사업자, 거대 통신사업자 등에 의한 고객 개인정보의 유출이나 부당이용으로 인한 개인정보 침해가 사회적 문제가 되고 있는 오늘날의 현실을 볼 때, 통신위원회도 통신사업자의 개인정보 불법유출 및 오·남용 행위에 대해 조사하고 규제하는 기능을 행하고 있는 것으로 볼 수 있다. 실제로 통신위원회는 법정대리인의 동의 없는 미성년자의 인터넷 게임사이트 가입 및 이로 인한 요금청구 등과 관련된 사건에 대해 심의·의결하여 인터넷 게임사이트 등의 업체에게 시정명령을 부과하는 등 개인정보와 관련된 문제를 처리하고 있다.[104] 그러나 통신위원회의

---

103) 전기통신기본법 제40조의3.

104) 2003년 상반기 통신위원회에 접수된 민원 중 914건(25.7%)이 부모 등 법정대리인 동의 없이 미성년자를 가입시키는 등 미성년자 관련 민원이었다고 한다(2003. 7. 29일 통신위원회 보도자료 참고, http://kcc.go.kr). 이에 제81차(2002. 8. 22) 및 제96차(2003. 11. 10) 통신위원회는 (주)넥슨을 비롯한 15개 인터넷 게임업체에 대하여 시정명령 등을 부과한 바 있다.

관할영역 중 개인정보 유출이나 부당이용과 같은 개인정보 침해행위가 차지하는 비중은 극히 적은 수준이다. 인터넷 게임사이트에 대한 통신위원회의 시정조치도 '부모 동의없는 아동의 개인정보 수집'의 위법성 측면보다는 '부모 동의없는 이용요금 결제'의 위법성에 초점을 맞춘 것이라는 점이 이러한 사실을 잘 반영하고 있다.

라. 한국소비자보호원

(1) 설립 및 기능

한국소비자보호원은 1986년 개정된 소비자보호법을 근거로 1987년 7월 1일 재정경제부 산하 특수공익법인으로 설립되었으며, 현재 설립근거규정은 소비자보호법 제26조이다. 소비자보호원은 소비자의 기본 권익을 보호하고 소비생활의 합리화를 도모하며 나아가 국민경제의 건전한 발전에 기여한다는 목적 하에 ① 소비자상담 및 피해구제, ② 물품·용역의 규격·품질·안전성 등에 관한 시험검사 및 조사, ③ 소비자보호 관련 제도 및 정책의 연구·건의, ④ 소비생활의 합리화 및 안전을 위한 정보 제공, ⑤ 소비자보호 관련 교육 및 홍보, ⑥ 국민생활 향상을 위한 종합적 조사·연구 등의 기능을 수행하고 있다.

한편, 소비자분쟁조정위원회는 소비자보호법 제34조에 의거하여 1987년 한국소비자보호원에 설치되었으며, ① 소비자분쟁에 대한 조정결정, ② 소비자분쟁조정규칙의 제정 및 개폐, ③ 기타 원장이 부의하는 사항을 심의·의결하는 독립적인 준사법기구이다. 소비자분쟁조정위원회는 위원장 1인을 포함한 30인 이내의 위원으로 구성되며, 이 중 2인은 상임위원으로 한다. 위원은 소비자보호원장의 제청으로 소비자보호법 제22조에 따라 분쟁조정위원 자격기준에 부합하는 자로 재정경제부장관이 임명 또는 위촉하며, 위원장은 상임위원 중에서 재정경제부장관이 임명한다. 위원의 임기는 각 3년이며 신분은 법률로 보장되어 있다.

(2) 피해구제절차

소비자보호원과 분쟁조정위원회는 소비자문제에 있어서 상담, 조정전 합의권고, 분쟁조정의 기능이 조직적으로 역할분담되어 있을 뿐 아니라, 상호 유기적으로 연결되어 효율적인 피해구제제도를 확립하고 있다. 즉, 현재 소비자상담팀과 분쟁조정국 등은 상담, 사실조사, 합의권고의 역할을 하고 있으며, 분쟁조정위원회는 소비자분쟁에 대하여 조정결정을 내리는 역할을 하고 있다.

먼저 상담부터 살펴보면, 소비자보호원은 '소비자상담팀'을 운영하여 소비자불만 및 피해에 관한 각종 상담을 접수·처리하고 있다. 상담방법은 전화상담, 인터넷상담, 방문상담 등이 있으나 현재 전화상담이 주를 이루고 있으며 최근에는 인터넷 상담이 급증하고 있다.[105] 소비자보호원은 상담을 접수받으면 우선 각 사안별로 적절한 정보를 제공함으로써 소비자불만을 처리하거나 타기관 알선 또는 기타상담 등으로 처리하고 있다. 또한 소비자상담 중 소비자보호법상 피해구제가 가능한 사건에 대하여 청구인과 피청구인의 인적사항과 피해사실 등을 확인한 후, 피해구제 청구건으로 접수하여 분쟁조정국으로 사건을 인계한다. 한편 소비자보호원은 상담과정에서 변호사나 법무사의 조언이 필요한 사항에 대해서는 무료법률상담서비스를 제공하고 있다.[106]

분쟁조정국은 상담팀으로부터 이관된 사건에 대해 사실조사와 합의권

105) 2000년 인터넷 상담은 43,691건으로 13%를 차지하였으나, 2001년 63,027건으로 17.7%, 2002년 76,710건으로 24.6%를 차지하며 꾸준히 그 비중이 증가하고 있는 추세이다. 한편, 소비자보호원의 인터넷상담이 계속 증가함에 따라 상담지연에 따라 소비자의 불만 해소 및 사업자의 능동적인 소비자문제 해결을 위해, 상담건수가 많이 접수되는 사업체(통신, 자동차, 공산품 업체)를 대상으로 인터넷상담 자율처리사업자로 선정하여 소비자보호원에 접수되는 상담 건을 직접 처리하고 그 결과를 소비자보호원에 회신하는 인터넷상담 자율처리시스템을 2002년 4월 15일부터 도입 시행하고 있다. 인터넷상담 자율처리시스템은 48시간 이내에 처리가 완료된다는 점에서 신속한 처리로 소비자 만족도를 높이는 결과를 낳고 있다. 인터넷상담 자율처리시스템을 도입한 이후 2002년 인터넷상담 건 중 1,846건을 해당 사업자에게 통보하여 1,782건(96.5%)을 처리하였다.

106) 2002년 변호사 상담은 총 281건, 법무사 상담은 총 545건으로 총 826건의 무료법률상담서비스가 이루어졌다.

고를 하여 소비자분쟁을 해결하고 피해구제를 도모할 수 있다. 현재 이러한 기능을 담당하는 조직은 소비자보호원 내 분쟁조정 1, 2국과 사이버소비자센터이다. 분쟁조정1국은 공산품 및 일반서비스 분야(자동차통신, 주택공산품, 생활문화, 농업섬유)의 분야를 담당하고 있으며, 분쟁조정2국은 전문서비스분야(금융, 법무보험, 의료)를 담당하고 있다. 이 외 사이버소비자센터는 외국사업자의 전자상거래로 인한 피해구제업무를 담당하고 있다. 이렇듯 소비자보호원은 주요 영역별로 팀을 분류하여 피해구제의 전문화를 시도하고 있다. 이 단계에서 분쟁조정국은 일차적으로 당사자 서면답변요청, 사진・비디오 촬영, 자료수집 등의 현장조사, 자문의뢰 등의 방법을 통해 사실조사를 행한다. 또한 필요한 경우에는 전문위원회의 전문위원으로부터 자문을 구할 수 있으며[107], 검사실시부서[108] 또는 심의위원회를 통해 보다 정확한 사실조사가 가능하다. 한편 소비자보호원장은 이러한 사실조사과정에서 위법사실이 확인된 경우 관계기관에 위법사실을 통보할 수 있다.[109] 또한 소비자보호원장은 사실조사결과를 바탕으로 분쟁조정위원회로 조정신청을 하기 전에 먼저 양 당사자간에 합의를 권고할 수 있다. 그러나 소비자보호원은 피해구제의 청구를 받은 날로부터 30일 이내에 합의권고에 의하여 소비자와 사업자간에 합의가 이루어지지 않으면 지체 없이 분쟁조정위원회에 조정을 요청하여야 한다. 또한 분쟁 당사자 및 소비자보호단체는 소비자분쟁조정위원회에 직접 분쟁조정신청을 할 수 있다. 분쟁조정위원회는 조정신청을 받은 날로부터 30일 이내에 분쟁조정을 하여야 한다. 다만, 원인규명을 위한 시험・검사 등 부득이한 사정으로 조정결정기간이 연장되어야 하는 경우에는 그 사유와 기한을 명시하여 당사자에게 통보하도록 되어 있다.

---

107) 현재 소비자보호원은 약 200여명의 전문위원을 위촉하여 전문분야에 대한 자문을 구할 수 있도록 하고 있다.

108) 현재 소비자보호원은 피해구제과정에서 필요한 시험검사를 위하여 별도의 시험검사소를 운영하고 있다. 시험검사소는 29개 실험실로 운영되며 48종 583대의 시험장비를 보유하고 있다.

109) 소비자보호원이 2002년에 검찰 등 관계기관과 업무협조하거나 위법사실을 통보한 실적은 101건이다.

분쟁조정위원회는 위원장, 상임위원 및 위원장이 매 회의마다 지명하는 5인 이상 7인 이하의 위원으로 개최된다. 이 때 위원장은 각 사건별로 적합한 전문가를 조정위원으로 지정하나, 대부분 사업자단체대표, 소비자단체대표, 법률가는 항상 포함된다. 위원회의 조정결정 결과는 즉시 당사자에게 서면 통보되며, 당사자가 통보를 받은 날로부터 15일 이내에 조정을 수락하여 조정서에 기명·날인을 하거나, 동 기간 내에 서면으로 수락거부의 의사표시를 하지 않은 경우에는 조정이 성립된다. 조정이 성립된 경우, 조정내용은 '재판상 화해'와 동일한 효력을 갖는다. 따라서 조정이 성립된 후 당사자 일방이 이를 이행하지 않는 경우에는「각종분쟁조정위원회등의조정조서등에대한집행문부여에관한규칙」(대법원규칙, 제1198호)에 따라 법원으로부터 집행문을 부여받아 강제집행을 할 수 있다. 그러나 일방 당사자가 분쟁조정위원회의 조정결정을 수락하지 않은 때에는 조정이 불성립되며, 이 경우에는 민사소송을 통하여 피해구제를 받을 수 있다.[110]

한편, 소비자보호원은 소비자가 피해구제를 신청한 사건 중, ① 소비자보호원의 피해구제절차 또는 분쟁조정절차 진행 중에 사업자가 소송을 제기하여 해당 절차가 중단된 사건, ② 소비자분쟁조정위원회의 분쟁조정결정에 대해 사업자의 거부로 성립되지 아니한 사건, ③ 소비자분쟁조정위원회의 분쟁조정결정이 성립된 후 사업자가 조정결정을 이행하지 않은 사건 등에 대해서는 소비자의 소송제기 등을 지원하는 소송지원제도를 운영하고 있다. 다만, 위 조건에 해당되는 사건 중에서도 특히 중대하고 대량적인 소비자피해발생이 예측되는 경우, 1,000만원 이하의 소액사건인 경우, 승소가능성이 높고 법률 전문가의 조력이 필요한 경우에 대하여, 한국소비자보호원에서는 30인의 변호사로 구성된 '소송지원변호사단'의 변호인으로 하여금 소송을 지원토록 하고 있다. 이 제도는 소비자피해 사건은 보통 손해배상액이 적기 때문에 수임료가 충분하지 않다는 이유로 변호사의 선임이 쉽지 않는 점을 고려한 것이다. 소비자는 인지

110) 2000년부터 2002년까지 3년 동안 소비자분쟁조정위원회에서 조정결정된 총 건수는 1,459건으로, 이 중 1,097건이 성립되었고 265건이 불성립되어 평균 조정성립률은 80.5%이다.

대・송달료 등 소송 필수비용을 부담하고, 당해 소송이 승소할 경우에만 판결확정 후 법정수임료를 지불하며, 당해 소송에서 패소하거나 또는 승소하였지만 승소금액이 법정수임료보다 적을 경우에는 변호사 수임료를 지불하지 않아도 되도록 하고 있다. 다만 패소시에는 판결 결과에 따라 사업자의 소송비용을 소비자가 부담해야 하는 경우가 있다.[111]

(3) 개인정보보호 기능 및 역할

한국소비자보호원과 소비자분쟁조정위원회는 일반적인 소비자보호 및 피해구제의 기능을 맡고 있는 대표적인 소비자보호기구이다. 한국소비자보호원 등은 원칙적으로 모든 소비자문제를 다룬다. 그러므로 만약 개인정보침해문제가 민간부문의 사업자의 위법・부당한 개인정보 처리로 인해 발생한 것이라면 넓은 의미에서 소비자문제에 해당될 수 있기 때문에, 소비자보호원과 소비자분쟁조정위원회도 개인정보침해 문제에 관여하여 소비자가 입은 피해를 구제하는 기구로서의 역할을 수행할 수 있을 것이다. 그러나 실질적으로 한국소비자보호원 등은 물품구매 등으로 인한 거래관계로부터 발생하는 사업자와 소비자간 분쟁이 아닌 순수하게 개인정보의 침해문제가 접수되면, 대부분 개인정보 전문 피해구제기구인 개인정보분쟁조정위원회를 안내해주고 있다.

마. 전자거래분쟁조정위원회

(1) 설립 및 구성

전자거래분쟁조정위원회는 전자거래에 관한 분쟁을 신속・공정하게 해결하고 그 피해를 구제하기 위한 목적으로「전자거래기본법」제32조제1

111) 소비자보호원은 1994년 소송지원제도를 시작한 이후 2003년 12월 현재 55건을 변호사를 알선하여 소송지원을 하였으며, 그 결과 승소 27건, 패소 3건, 화해 7건, 나머지 15건이 소송 진행 중에 있다.

항에 근거하여, 2000년 4월 12일 설치된 소송외적 분쟁해결기관이다. 일반적인 소비자분쟁에 대해서는 앞서 살펴본 소비자보호원과 소비자분쟁조정위원회가 담당하고 있지만, 전자거래분쟁조정위원회는 전자상거래가 점포 없는 가상공간을 통한 거래여서 거리와 시간의 제한이 없다는 점, 선입금 후배송 거래라는 점 등의 특수성을 가지는 바, 이러한 점을 고려하여 온라인을 통한 전자상거래 환경에 적합한 피해구제절차를 마련하기 위해 설립된 것이다.

전자거래분쟁조정위원회는 전자거래기본법 제32조제2항에 따라, 위원장 1인을 포함한 15인 이상 50인 이하의 위원으로 구성되어 있다. 위원은 전자거래에 관한 학식과 경험이 풍부한 자 및 시민단체에서 추천한 자로서 전자거래기본법 제32조제3항 각호에 해당하는 자가 위촉되며, 위원장은 위원 중 호선을 통해 선출된다. 위원의 임기는 2년으로 연임이 가능하다. 전자거래분쟁조정위원회는 한국전자거래진흥원 내 설치된 사무국에 의해 위원회 운영 등에 관한 사항을 지원받고 있는데, 사무국은 분쟁조정신청접수 및 사실조사, 담당조정부 구성, 위원회 조정사례집 발간, 위원회 홍보 및 전자거래분쟁예방을 위한 교육 등을 담당한다.

(2) 분쟁조정절차

전자거래분쟁조정제도는 신속성, 공정성, 접근용이성(무료), 비밀유지의 조정원칙 하에 전자거래에 관한 모든 분쟁을 처리하고 있는데, 특히 신속한 피해구제를 중요원칙으로 삼아 분쟁조정신청을 받은 날로부터 45일 이내 피해구제가 가능하도록 처리하고 있다.[112]

전자거래분쟁조정위원회는 전화, 인터넷 홈페이지, 이메일, 방문 등으로 전자거래에 관한 상담을 접수하여 처리하고 있는데, 이 중 인터넷 홈페이지를 통한 상담이 가장 큰 비중을 차지하고 있다.[113] 이렇게 접수된

112) 이는 개인정보분쟁조정위원회 및 소비자분쟁조정위원회가 60일 이내 처리인 것에 비해 짧은 기간이다.

113) 전자거래분쟁조정위원회는 2002년 총 4,605건의 상담을 접수받았는데, 이 중 '상담

상담 중 전자거래에 관한 분쟁이 확인된 사안은 분쟁조정신청을 접수받게 된다. 또한 신청인은 인터넷 홈페이지의 '조정신청'을 통해 직접 분쟁조정을 신청할 수 있다. 위원회는 전자거래기본법 제33조제2항에 따라 분쟁조정신청이 접수된 후 10일 이내에 분쟁당사자에게 일차적 합의권고를 하고 있다. 이러한 합의권고를 통한 분쟁해결비율은 2000년 57.8%, 2001년 40.7%, 2002년 61.8%를 차지하고 있어, 상당부분 조정전 합의권고를 통해 분쟁조정사건이 해결되고 있음을 알 수 있다.

그러나 이러한 합의권고를 통해서도 분쟁이 해결되지 않으면 위원회는 담당조정부를 통해 사건을 심리하고 분쟁을 조정한다. 전자거래분쟁조정위원회는 50인 이내의 상당히 많은 조정위원이 위촉되어 있는데, 이 중 해당 사건별로 사안의 특성에 적합한 조정위원이 선정되어, 1인에서 3인 이내로 담당조정부가 구성된다. 담당조정부는 조정요구가 있은 후 35일 이내에 분쟁 당사자에게 조정안을 제시하여야 한다. 이렇듯 3인 이내의 소수 위원이 조정위원으로 참가하는 것은 전자거래 분쟁을 신속하고 효율적으로 처리하기 위함인데, 특히 전자거래가 온라인을 통해 이루어진다는 점에서 전자거래분쟁조정위원회가 도입·시행하고 있는 사이버조정과도 밀접한 관련이 있다.

현재 전자거래분쟁조정위원회는 대면조정과 사이버조정을 모두 행하고 있는데, 특히 사이버조정은 최근 국제적으로도 전자상거래 분쟁의 해결과 관련하여 각광받고 있는 온라인 분쟁해결제도라는 점에서 의미가 있다. 사이버조정은 조정관계인이 조정장소에 직접 출석하지 않고 정해진 조정기일과 시간에 맞추어 각자의 장소에서 사이버조정센터(www.ecmc.or.kr)를 이용, 실시간으로 동시에 참여함으로써 진행되는 조정을 의미한다. 사이버조정에는 온라인채팅을 통한 조정과 음성화상조정시스템을 통한 조정의 두 가지가 있으나, 대부분 온라인 채팅 방식으로 해결되고 있다.[114] 그

신청'코너, 게시판, Q&A 등 인터넷 홈페이지를 통한 상담이 1,995건으로 약 43%를 차지하고 있다.

114) 2002년 기준, 사이버조정을 통해 해결된 분쟁조정사건은 2001년 16건, 2002년 47건으로 총 63건인데, 이 중 3건만이 음성화상시스템을 통해 해결되었다.

이유는 음성화상시스템을 이용하기 위해서는 양 당사자 모두 컴퓨터, 화상카메라, 마이크 등 일정한 장비가 필요하나 아직까지는 그렇지 못한 경우가 많고, 또한 분쟁이 있는 당사자끼리 화상으로 대면하는 것을 원치 않기 때문이다.

이러한 사이버조정은 조정장소에 출석하기 위해 소요되는 시간과 비용을 절감함으로써, 비용절감과 신속성이라는 장점을 가진 전자거래환경에 적합한 분쟁해결방식이라는 장점을 가지고 있다. 따라서 소비자·사업자 등 분쟁당사자도 대면조정보다는 사이버조정을 선호하는 편이다. 실제로도 조정절차를 통하여 처리된 대부분의 사건이 사이버 조정으로 처리되었고, 대면조정은 주로 사안이 특수하고 복잡한 경우 또는 분쟁 당사자가 대면조정을 요구하는 경우에 주로 행하고 있다.[115]

전자거래분쟁조정위원회는 이러한 조정방법을 통해 분쟁당사자에게 조정안을 제시하고 그 수락여부를 묻게 되는데, 당사자가 7일 이내 수락여부에 대한 답변이 없는 경우 수락으로 간주한다. 이렇게 조정이 성립된 경우 민사상 화해계약으로서의 효력을 가진다.

(3) 개인정보보호 기능 및 역할

전자거래분쟁조정위원회는 전자거래와 관련한 모든 분쟁을 해결하는 피해구제기구인 바, 전자거래에서의 개인정보침해로 인한 분쟁을 처리할 수도 있다. 실제로 2001년 12월 개인정보분쟁조정위원회가 설립되기 전, 전자거래분쟁조정위원회는 개인정보와 관련된 상담이나 분쟁조정신청을 접수받아 처리한 바 있다. 예를 들어, 회원으로 가입한 사이트 이외의 곳에서 구매를 요청하는 전화가 걸려와 개인정보 유출이 문제가 된 사건, 본인이 가입하지 않은 사이트에서 회원가입 처리되어 서비스 이용대금을

115) 2001년 대면조정 156건, 사이버조정 16건이었으며, 2002년 대면조정 8건, 사이버조정 47건이었다. 그러나 2001년도 대면조정 156건 중 153건은 하나의 사건으로 병합처리된 것이므로 실질적으로 대면조정보다 사이버조정이 더 활발히 이용되고 있음을 알 수 있다. 2003년 8월 기준, 전자거래분쟁조정위원회는 한달 평균 약 6건의 조정안건을 사이버조정으로 처리하고 있다고 한다.

청구하는 경우, 사이트에 회원으로 가입하려고 하였으나 본인의 주민등록번호가 이미 사용 중이어서 회원가입이 이루어지지 않은 경우, 온라인 게임에서 해킹 관련 아이템을 보유했다는 사유만으로 개인 계정이 압류된 경우, 게임 사이트에 가입한 후 탈퇴하려고 하나 절차가 없는 경우와 같은 사건들을 접수받아 처리하였다.[116]

이와 같이 전자거래분쟁조정위원회는 전자거래에 관한 모든 분쟁을 처리하기 때문에 전자거래상의 개인정보 도용·침해·유출에 대하여 상담 및 조정의 역할을 담당해왔다. 그러나 실질적으로 전자거래분쟁조정위원회가 처리하는 개인정보 관련사건은 순수하게 개인정보가 침해된 경우라기보다는 전자거래계약과 관련되어 개인정보가 함께 문제가 된 사안인 경우가 대부분이다. 실제로 2001년 12월 개인정보분쟁조정위원회가 설립되어 개인정보에 관한 분쟁을 전문적으로 조정하고 처리한 이래로, 개인정보와 관련이 높은 분쟁을 전자거래분쟁조정위원회가 직접 처리하는 경우는 드문 것으로 나타나고 있다. 아래 〔표 3-10〕에서와 같이 전자거래분쟁조정위원회에서 처리한 개인정보관련 상담 및 피해구제 통계를 살펴보더라도, 2000년부터 2002년까지의 전체 피해구제신청에서 개인정보 관련 분쟁이 차지하는 비중이 계속해서 줄어들고 있음을 확인할 수 있다.

〔표 3-10〕 전자거래분쟁조정위원회의 개인정보피해구제 현황

구분	2000	2001	2002
개인정보상담(전체)	-	59(1,310)	79(2,987)
비율	-	4.50%	2.64%
개인정보분쟁조정신청(전체)	10(83)	28(457)	23(854)
비율	12.05%	6.13%	2.69%

(단위 : 건)

116) 한국전자거래진흥원, "2002 전자거래분쟁조정사례집", 2003. 1, 40면 참조.

바. 금융감독위원회

(1) 설립 및 구성

현재 국내에는 「금융감독기구의설치등에관한법률」에 의거, 금융감독위원회와 금융감독원이 통합적인 금융감독기구로서의 역할을 담당하고 있다. 금융감독위원회는 국무총리 소속 하에 설치된 합의제 행정기관으로 은행·증권·보험·여신전문업 등 전 금융권에 대한 감독업무를 통합하여 독립적으로 수행한다. 금융감독위원회는 금융감독원을 지휘·감독하는 기관으로서 금융감독과 관련된 주요 사항을 심의·의결[117]하며, 금융감독원은 금융감독위원회의 지시를 받아 금융기관의 업무 및 재산상황에 대한 검사·조사·제재 등과 금융감독위원회의 업무보좌 등을 수행함으로써 양 기관이 금융기관에 대한 감독·검사 등 커미셔너계 업무를 유기적으로 수행하고 있다.[118]

한편 금융감독원 내에는 금융분쟁조정위원회가 설치되어 있는데, 이는 은행·증권·보험 등의 분야에서 발생하는 금융분쟁을 조정하는 역할을 하는 소비자피해구제기구이다. 위원회는 위원장 1인을 포함한 30인 이내의 위원으로 구성되며, 위원장은 금융감독원장이 소속 부원장 중에서 지명한 자가 된다. 그 외 위원은 소속 부원장보 1인과 법조계, 소비자단체, 금융계, 학계 등 전문가로 위촉된다. 위원의 임기는 2년이나 위원장과 부원장보인 위원의 임기는 당해직 재직기간에 한한다.[119]

---

117) 금융감독위원회가 심의·의결할 수 있는 사안으로는 ① 금융기관 감독과 관련된 규정의 제정 및 개정, ② 금융기관의 설립·합병·전환·영업 양도(수) 등의 인·허가, ③ 금융기관의 경영과 관련된 인·허가, ④ 금융기관에 대한 검사·제재와 관련된 주요 사항, ⑤ 증권·선물시장의 관리·감독 및 감시 등과 관련된 주요 사항, 금융기관에 대한 시정조치 등 금융구조조정과 관련된 주요 사항 등을 심사하고 결정할 권한을 가진다.(금융감독기구의설치등에관한법률 제17조)

118) 금융감독위원회/금융감독원, "금융감독위원회·금융감독원 소개", 2002. 3, 12면.

119) 2003년 10월 기준, 금융분쟁조정위원회의 위원은 총 27명으로 2명의 내부위원(금융감독원 부원장, 부원장보)과 25명의 외부위원(은행·증권분쟁조정위원회 12인, 보험분쟁조정위원회 13인)으로 구성된다. 외부위원은 법조계 8인, 소비자단체 3인, 금융계 4인, 학계 6인, 의료계 2인, 손해사정 1인, 전자금융 1인이 위촉되어 있다.

(2) 개인정보보호 기능 및 역할

이와 같이 금융감독위원회는 일차적인 금융감독기구이며 금융감독원은 금융감독위원회의 지시를 받아 구체적으로 금융기관 등의 업무처리관행을 검사·감독하는 기능을 수행하는 기구로 활동하고 있다. 따라서 금융감독위원회와 금융감독원은 다른 금융관련 법률과 함께 신용정보보호법 및 금융실명거래법이 올바르게 준수되도록 관리·감독할 책임을 지고 있다고 볼 수 있다. 이를 위해 금융감독위원회는 신용정보보호법 제4조에 따라 신용정보업을 영위하고자 하는 자의 승인여부, 신용정보업의 정지 및 허가취소를 결정할 수 있고, 신용정보업자 및 신용정보집중기관과 신용정보제공·이용자의 건전한 영업을 위하여 그 업무를 감독하고 업무 또는 재산에 관한 보고 등 필요한 명령을 내릴 수 있다.[120] 또한 금융감독원은 금융감독위원회의 지시를 받아 신용정보주체의 시정요청에 대한 사실조사를 시행하고[121] 신용정보업자 등의 업무와 재산상황을 검사할 수 있으며, 검사를 위해 필요한 경우에는 신용정보업자 등에게 자료제출, 관계자 출석, 의견진술 등을 요구할 수 있다.[122] 또한 금융감독원은 금융기관의 임직원 등이 금융거래의 비밀보장 규정을 위반하였는지 여부를 검사하고 제재할 수 있는 권한을 가진다.

한편, 금융관련기관의 업무와 관련하여 발생한 권리·의무 또는 이해관계로 인한 분쟁을 신속·간편하게 조정하는 금융분쟁조정위원회는 원칙적으로 금융기관의 임직원의 위법·부당한 금융거래정보 유출이나 개인신용정보의 부당한 이용으로 인한 침해, 신용정보주체의 열람·정정요구권의 거부 등으로 인한 분쟁을 조정하는 역할을 담당할 수 있다. 그러나 현재 금융분쟁조정위원회는 계약을 기초로 한 금전적 이해관계가 전제되는 금융분쟁의 조정을 처리하는 것을 기본으로 하기 때문에, 분쟁처리과정에서 금융기관 임직원이 위법·부당하게 소비자 금융거래정보를

120) 신용정보보호법 제29조제1항.

121) 신용정보보호법 제25조제5항.

122) 신용정보보호법 제29조제2항, 제3항.

누설하는 등의 위법사실이 발견되면, 금융감독원에게 위법사실을 통보하여 감독 및 검사 차원에서 당해 금융기관 또는 임직원에 대하여 제재조치를 취하도록 처리하고 있다. 또한 신용정보의 부당한 이용에 대해서도 금융분쟁조정절차를 거치기보다는 금융감독원 신용감독국에서 조사·감독하고 잘못된 사항에 대해서는 시정조치, 주의와 같은 제재를 부과하는 방법으로 처리하고 있다.

결론적으로 금융감독위원회와 금융감독원은 금융소비자의 거래정보보호, 개인신용정보보호를 위해 사전적·사후적 감독 및 보호기능을 하고 금융분쟁조정위원회는 사후적 피해구제의 역할을 하는 것으로 볼 수 있다. 그러나 실질적으로 금융분쟁조정위원회는 금융분야에서의 개인정보침해로 인한 경제적·정신적 피해를 구제해주는 적극적인 역할을 담당하고 있지는 않다.

〔표 3-11〕 금융감독위원회의 개인정보보호 기능

구분	개인정보보호 기능	
금융감독위원회	사전적 기능	· 신용정보업 허가, 신용정보집중기관 등록 · 신용정보의 등록, 변경, 관리 등에 관한 기준과 절차 마련 및 고시
	사후적 기능	· 부적절한 신용정보업자의 영업정지 및 허가취소 · 감독을 위한 업무 또는 재산에 관한 사항 보고 등의 필요한 조치 명령 · 신용정보주체의 시정요청 접수처리 · 부당행위를 한 자에게 시정 등 필요한 조치 명령
금융감독원	· 금감위의 지시로 위법·부당한 행위를 조사·검사 · 시정권고, 주의, 불법행위를 한 임직원의 징계권고 등의 제재	
금융분쟁조정위원회	· 금융 분야의 계약을 기초로 한 권리의무 관계에서 발생하는 분쟁을 조정하여 합의유도	

3. 기타

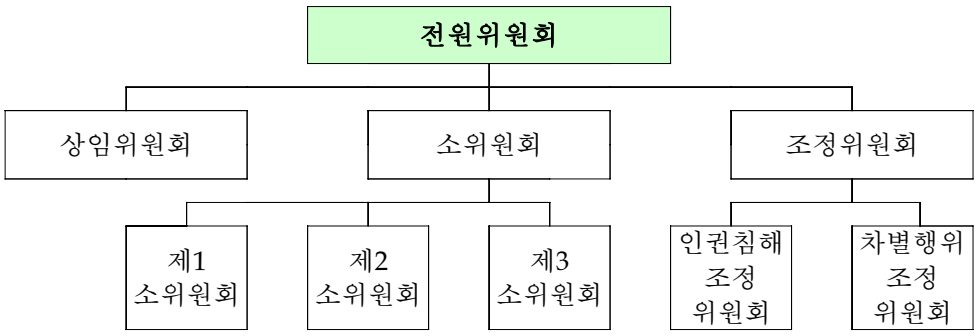
가. 국가인권위원회

국가인권위원회는 국가인권위원회법에 의해 인권의 보호와 향상을 위한 업무를 수행하기 위해 설립되어, 그 권한에 속하는 업무를 독립적으로 수행할 수 있는 독립행정청이다. 즉, 헌법상의 독립기관은 아니나 행정부의 감독으로부터 자유로운 제4의 독립기구로 볼 수 있다. 국가인권위원회는 위원장 1인과 3인의 상임위원을 포함한 11인의 인권위원으로 구성되며, 위원은 인권문제에 관하여 전문적인 지식과 경험이 있고 인권의 보장과 향상을 위한 업무를 공정하고 독립적으로 수행할 수 있다고 인정되는 자 중에서 국회가 선출하는 4인(상임위원 2인 포함), 대통령이 지명하는 4인, 대법원장이 지명하는 3인을 대통령이 임명한다.[123]

현재 위원회에는 인권위원 전원이 참석하는 전원위원회를 비롯하여 상임위원회, 소위원회, 조정위원회가 설치되어 운영되고 있다. 전원위원회는 위원회의 운영 및 예·결산에 관한 사항, 자문위원 또는 조정위원의 위촉에 관한 사항, 방문조사·인권침해 또는 차별행위 조사사건에 관하여 구제조치의 권고, 고발·징계권고 및 그 시행에 관한 사항, 법원 및 헌법재판소에 대한 의견 제출 등에 관한 사항을 심사하고 결정할 권한을 가진다. 상임위원회는 위원장과 상임위원 3인으로 구성되며 긴급구제조치의 권고 및 시행에 관한 사항, 인권상황에 관한 실태조사, 인권에 관한 교육·홍보 등의 사항을 결정한다. 또한 3개의 소위원회는 위원회의 주요업무에 관한 사항을 각각 세부적으로 나누어 담당하고 있으며, 각각 상임위원 1인과 비상임위원으로 구성되어 있다. 한편 조정위원회는 인권침해조정위원회와 차별행위조정위원회가 따로 있고, 각각 인권위원 2명과 외부인사 1명으로 구성된다. 조정위원회는 인권침해 등에 대한 사항을 조정하여 합의를 유도하며, 조정에 갈음하는 결정을 내릴 수 있다.[124]

---

123) 국가인권위원회법 제5조.



(그림 3-4) 국가인권위원회의 구성현황

※ 참고 : 국가인권위원회 웹사이트, http://www.humanrights.go.kr

국가인권위원회는 인권에 관한 법령・제도・정책・관행에 대한 조사・연구, 인권침해행위에 대한 조사와 구제, 차별행위에 대한 조사와 구제, 인권상황에 대한 실태조사, 교육・홍보, 인권침해의 유형・판단기준 및 그 예방조치 등에 관한 지침의 제시 및 권고 등의 역할을 담당하고 있다. 이러한 기능을 수행하기 위해 인권위원회는 필요한 경우 자료제출을 요구할 수 있고 청문회를 실시할 수도 있으며, 구금・보호 시설 등을 직접 방문하여 조사할 수도 있다. 또한, 인권향상을 위해 필요하다고 판단되는 경우 관계기관에 정책 또는 관행의 개선을 권고하거나 의견을 표명할 수 있는 권한을 가진다.

특히 인권위원회는 인권침해에 관한 진정을 접수받아 피해구제를 하는 역할도 맡고 있다. 즉, 진정이 접수되면 위원회는 사실조사를 하고 인권침해가 있다고 판단되는 사안에 대해서는 먼저 사전합의권고를 실시한다. 그러나 이에 의해서도 원만히 해결되지 않은 경우, 위원회는 당사자의 신청 또는 직권으로 조정위원회를 개최하여 조정을 할 수 있으며, 조정절차 중 당사자 합의가 이루어지지 않은 때에는 조정에 갈음하는 결정을 내릴 수 있다. 조정에 갈음하는 결정에는 조사대상 인권침해행위의 중지조치, 원상회복・손해배상 그 밖의 필요한 구제조치, 동일 또는 유사

124) 국가인권위원회 웹사이트, http://www.humanrights.go.kr 참조.

한 인권침해행위의 재발을 방지하기 위하여 필요한 조치의 시행이 해당된다. 위원회의 조정 및 조정에 갈음하는 결정은 당사자의 이의신청이 없는 한 재판상 화해의 효력을 가진다.

국가인권위원회는 이처럼 인권침해 전반에 대하여 조사하여 진정을 접수하고 조정 등을 통해 피해구제를 하는 역할을 맡고 있기 때문에, 개인정보침해 및 프라이버시침해의 문제에도 개입할 수 있는 여지는 충분히 있다.[125] 그러나 개인정보의 경우 순수하게 인권적 시각으로만 바라보는 것은 바람직하지 않다. 왜냐하면 오늘날 개인정보는 사회적 특성상 그 이용이 필수적인 것으로 전제되어 있는 것이어서, 단순히 개인정보침해를 인권침해로만 인식하여 개인정보의 적절한 활용을 현저하게 제한할 수 있는 위험이 있기 때문이다.

나. 경찰청 사이버테러대응센터

경찰청에 의한 개인정보침해의 수사, 피해자 검거, 형사처벌 등의 조치는 전형적인 의미에서 개인정보피해구제라 보기는 다소 어려움이 따르며, 경찰기구를 개인정보보호기구라 부르기도 적합하지 않다. 그러나 본 논문에서 경찰청을 개인정보보호기구의 하나로 소개하는 것은 오늘날 개인정보보호 및 침해의 방지에 사이버테러대응센터를 비롯한 경찰청 사이버수사대가 중요한 역할을 하고 있기 때문이다.[126]

2000. 7. 11일 설립된 경찰청 사이버테러대응센터는 법집행기구인 경찰청의 한 부속기구로 본래는 해킹이나 바이러스의 유포 등과 같은 사이버테러를 방지하기 위한 목적으로 설립되었으나, 최근에는 인터넷을 통한 사기행위, 사이버 명예훼손, 개인정보 및 개인의 비밀침해 사건의 증가로

---

125) 실제 국가인권위원회는 올 한해 국가교육행정정보시스템(NEIS)의 구축으로 인한 개인정보 침해가능성 문제에 대한 전교조 등 시민단체들의 진정을 접수받아 심사한 뒤 정부에 제도 개선을 권고한 바 있으며, 최근에는 '금융기관과 인터넷에서의 개인정보 공유현황'을 실태조사하여 발표하기도 하였다.

126) 2003년 8월 기준, 경찰청 사이버테러대응센터에 접수된 모든 개인정보침해사건 관련 상담은 총 13,618건에 이르고 있다.

그 업무범위가 확대되어 사이버에서 발생하는 모든 불법적인 행위에 대해 전담하여 수사를 펼치고 있다.[127]

특히 개인정보침해사건과 관련하여 사이버테러대응센터는 신고를 접수받아 위법사항이 발견된 경우 관련 법령에 따라 처벌을 하고 있다. 사이버테러대응센터에서 근거로 활동하고 있는 개인정보 관련법령으로는 비밀침해죄를 규정한「형법」제316조제2항, 「정보통신망이용촉진및정보보호등에관한법률」제49조의 '비밀 등의 보호' 및 제62조의 벌칙조항,「공공기관의개인정보보호에관한법률」제23조제2항,「통신비밀보호법」제3조의 '통신 및 대화비밀의 보호' 및 제26조의 벌칙조항,「주민등록법」제21조의 벌칙조항 등이 있다.

현재 사이버테러대응센터는 인터넷 웹사이트와 전화를 통해 사이버범죄에 관한 신고 및 상담을 접수받고 있으며, 접수받은 사건이 사법처리가 가능한 사이버범죄에 해당되는지 여부를 판단하여 수사여부를 결정한다. 만약 사이버범죄에 해당되나 사법처리대상은 아닌 경우에는 개인정보분쟁조정위원회 등 관련 기구에 안내를 해주며, 사이버범죄가 아닌 일반 사법처리 대상 범죄에 대해서는 관할 경찰서에 신고토록 상담처리하고 있다. 또한 사이버테러대응센터는 일반적으로 심각하고 중대한 해킹 등 정보통신망 공격행위와 같은 사이버테러형 범죄에 대해서는 직접 수사를 하나, 개인정보 유출과 같은 사건은 보통 관할 지방경찰청 사이버범죄수사대에 이관하여 처리토록 하고 있다. 즉, 개인정보침해사고와 관련하여 사이버테러대응센터는 단일한 범죄신고 접수창구의 역할을 하는 것으로 볼 수 있다.

---

127) 사이버테러대응센터는 접수되는 신고를 '사이버테러형범죄'와 '일반사이버범죄'로 나누고 있는데, '사이버테러형범죄'란 정보통신망 자체를 공격대상으로 하는 불법행위로서 해킹, 바이러스유포, 메일폭탄, DOS공격 등 전자기적 침해 장비를 이용한 컴퓨터시스템과 정보통신망을 공격하는 행위이며, '일반사이버범죄'란 사이버 공간을 이용한 일반적인 불법행위로서 사이버도박, 사이버 스토킹과 성폭력, 사이버명예훼손과 협박, 전자상거래 사기, 개인정보 유출 등의 행위를 의미한다. 그런데 2000년 들어서는 실제로 사이버테러형범죄보다 일반사이버범죄의 증가세가 두드러지고 있다. 2003년 11월 기준, 개인정보침해사건을 비롯한 일반사이버범죄는 총 49, 641건에 이르고 있어, 사이버테러형범죄의 세 배 이상이 접수된 것으로 나타나고 있다. (경찰청 사이버테러대응센터 웹사이트, http://ctrc.go.kr/statistics/index.html)

제 4 장 해외 개인정보피해구제제도

21세에 접어들면서, 오늘날 전 세계 국가들의 주된 관심사 중 하나는 정보통신 기술개발과 정보화 기반 구축을 통해 정보사회를 선도하는 것이다. 특히 정보통신 등 IT분야는 선진국과 후진국의 기술력이나 사회적 기반의 차이가 그다지 크지 않아, 상대적으로 기존 산업부분에서 뒤쳐져 있던 후진국들도 경쟁적으로 나날이 새로운 기술을 선보이는 등 정보화 대국을 선점하려는 노력을 보이고 있다. 그 결과 세계 각국의 정보화 수준은 큰 격차를 보이지 않고 있다. 컴퓨터는 이미 전 세계 각국에 보급되어 있고, 점점 그 성능이 발달하여 엄청난 양의 정보를 처리할 수 있다. 또한 전 세계 곳곳이 인터넷으로 연결되어 있어 정보처리 양이나 방법에 있어 불과 수십년 전 수기로만 모든 정보를 작성하고 처리하던 시대와 비길 만한 수준이 아니다.

그러나 경제적·사회적 변화로 인해 새롭게 문제로 인식될 수 있는 사안에 대해 규정하고 그 해결방법을 제시할 수 있는 법적·제도적 기반은 기술수준의 변화를 따라가기 어려운 것이 일반적인 모습이다. 이는 정보화 기술, 특히 정보처리기술의 발달과 그로 인한 개인정보침해의 심각성 문제에 있어서도 마찬가지이다. 따라서 현재 많은 국가들은 기존의 법제도만으로는 규율하기 힘든 새로운 사회적·기술적 환경에 대응할 수 있는 새로운 법제도를 도입하여 시행하고자 노력하여 왔다. 특히 정보처리기술의 발달로 인한 개인정보침해, 프라이버시침해의 문제를 다루기 위한 노력은 선진국에서도 불과 10여년의 역사를 가지고 있을 뿐이다. 이에 개인정보보호와 관련된 국제규범을 먼저 살펴보고, 구체적으로 주요국에서는 개인정보보호를 위해 어떠한 법률을 제정하여 시행하고 있는지, 개인정보침해로 인한 피해를 구제하기 위한 개인정보보호기구의 설치 및 운영상황은 어떠한지 살펴보기로 한다.

제 1 절 개인정보보호 국제규범

개인정보보호의 문제가 국제적으로 논의되기 시작한 시기는 불과 20여년 전이다. 1970년대 선진국에서는 과학기술의 발달, 특히 컴퓨터의 보급과 개인정보의 자동처리기술의 발달이 개인의 프라이버시에 미치는 영향에 대한 관심과 우려가 증대하였고, 이에 대한 대처방안을 입법·정책적으로 모색하기 위한 활발한 논의가 이루어졌다. 실제로 이러한 논의는 자국 내에서 개인정보의 자동처리를 규율하기 위한 법제도를 확립하는 방향으로 진행되었다. 이와 같은 개인정보보호를 위한 개별 국가차원의 논의는 1980년대 들어 국제적 차원의 논의와 국제규범의 정립으로 이어졌다. 특히 경제협력개발기구(OECD)는 각국의 입법현황을 전문가 그룹(Group of Experts)으로 하여금 조사·연구토록 하여, 그 결과를 바탕으로 1980년 「개인정보의 국경간 이동과 프라이버시보호에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」을 제정하였다.

정보사회로의 급속한 진입으로 인해, 개인정보보호에 대한 국제사회의 관심은 더욱 증대되었다. 유엔(UN : United Nations)은 1970년대부터 개인정보와 프라이버시 영역에 관심을 가지고 활동하기 시작하여, 1990년 12월 14일 총회 결의로 「컴퓨터화된 개인정보파일의 규제를 위한 가이드라인(Guidelines for the Regulation of Computerized Personal Data Files)」을 채택한 바 있다. 또한 유럽연합(EU)도 1995년 10월 24일 「개인정보의 보호 및 자유로운 이전에 관한 유럽의회와 이사회 지침(DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data)」을 마련한 데 이어, 1997년에는 「통신부문의 개인정보처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침(Directive 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF

THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)」을 제정하였다. 이후 EU는 1997년 통신부문에 적용되는 97/66/EC 지침을 「전자통신부문에서의 개인정보 처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침(DIRECTIVE 02/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the processing of personal data and the protection of privacy in the electronic communications sector)」으로 대체하였다.

1. OECD 프라이버시 가이드라인

1980년 제정된 OECD 프라이버시 가이드라인의 주된 목적은 각 국가별로 제정·논의되고 있는 개별적이고 상이한 프라이버시보호법을 조화시킴으로써, 국가간 정보의 자유로운 이동을 활성화하고 개인정보처리로 인한 프라이버시 침해를 방지하는 것이다. OECD는 서유럽 국가를 비롯한 선진국들이 모여 설립한 기구로 자유로운 시장경제체계와 다원화된 민주주의의 확립을 목적으로 활동하고 있기 때문에, OECD가 제시한 프라이버시 가이드라인의 기본 성격이나 방향도 그와 같은 특성을 반영하고 있다. 따라서 OECD 프라이버시 가이드라인은 회원국의 개인정보와 프라이버시의 보호 및 개인의 자유보호를 위한 최소한의 기준을 제시할 필요성은 물론, 국가간 개인정보 이동이 지속적으로 이루어지고 과도하게 방해받지 않도록 할 필요성과 정보의 경제적 가치 및 공정경쟁원칙에 따른 정보교역의 중요성 등을 염두에 두고 마련된 것으로 볼 수 있다.

OECD 가이드라인은 회원국에 강제적으로 적용되는 규범이 아니라 '가이드라인'이라는 이름 그대로 일종의 기준을 제공하는 역할을 한다. 따라서 동 가이드라인을 어떻게 이행할 것인지는 각 회원국에 일임되어 있다. 다만, 가이드라인 제4장제19조는 회원국이 동 가이드라인을 국내 차원에서 이행할 때 참고할 수 있는 전반적인 틀을 제공하고 있다. 이에

의하면, 회원국은 ① 적절한 국내 입법을 채택하고, ② 실행규약(Code of Conduct)이나 기타의 형식으로 자율규제를 장려하여야 하며, ③ 개인의 권리행사를 도울 수 있는 적절한 방법을 제공하여야 한다. 또한, ④ 개인정보보호원칙을 따르지 않는 경우 적절한 제재조치를 취하고 이로 인한 피해에 대한 구제수단을 마련하여야 하며, ⑤ 정보주체에 대한 불공정한 차별이 없도록 보장하여야 한다.

OECD 가이드라인은 자동처리되는 개인정보에 한정하지 않고 모든 개인정보를 그 대상으로 삼고 있다. 따라서 개인정보가 다루어지는 방법이나 수단에 관계없이 프라이버시와 개인의 자유에 위협을 가할 수 있는 모든 개인정보의 처리에 적용된다. 또한 여기서 말하는 개인정보란 식별되는 또는 식별가능한 개인에 관한 정보 일체를 뜻하기 때문에, 직접 또는 간접적으로 특정 자연인과 관련되는 모든 정보를 의미한다. 그 외에도 OECD 가이드라인은 정보관리자, 개인정보의 처리, 개인정보의 국외이전 등의 개념에 대해서 정의하고 있다. 특히 동 가이드라인은 여덟 가지 개인정보보호 기본원칙을 천명하고 있는데, 이러한 개인정보보호원칙은 UN 가이드라인이나 EU지침을 비롯하여 각국의 개인정보보호법에 큰 영향을 끼쳤다. OECD 가이드라인 역시 회원국 내에서 준수되어야 할 개인정보처리에 관한 최소한의 기준을 제시한 것이라고 밝히고 있고, 세계적으로도 개인정보보호를 위한 기본원칙과 기준으로서 인정받고 있다. 구체적인 OECD 가이드라인 제8원칙의 내용을 살펴보면 다음과 같다.

〔표 4-1〕 OECD 프라이버시 8원칙

원칙		내 용
제1원칙	수집제한의 원칙	· 적법하고 공정한 방법을 통한 개인정보의 수집 · 정보주체의 인지 또는 동의를 얻어 개인정보 수집 · 민감한 개인정보의 수집제한
제2원칙	정확성 확보의 원칙	· 이용목적과의 관련성 요구 · 이용목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성 확보

제3원칙	목적명시의 원칙	· 수집 이전 또는 당시에 개인정보의 수집목적 명시 · 명시된 목적에 적합한 개인정보의 이용
제4원칙	이용제한의 원칙	· 정보주체의 동의가 있거나 법규정이 있는 경우를 제외하고는 목적외 이용 및 공개 금지
제5원칙	안전성 확보의 원칙	· 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적 · 조직적 · 기술적 안전조치 확보
제6원칙	공개의 원칙	· 개인정보의 처리 및 보호를 위한 정책의 공개 · 개인정보관리자의 신원 및 연락처, 개인정보의 존재사실, 이용목적 등에 대한 접근 용이성 확보
제7원칙	개인참여의 원칙	· 정보주체의 개인정보 열람 · 정정 · 삭제청구권 보장 · 정보주체가 합리적 시간과 방법에 의해 개인정보에 접근할 수 있도록 보장
제8원칙	책임의 원칙	· 개인정보관리자에게 원칙 준수의무 및 책임 부과

2. UN 개인정보 가이드라인

유엔 가이드라인은 모든 공공부문과 민간부문에 적용되며 컴퓨터 파일뿐 아니라 구조화된 수작업 파일에도 적용되는 것으로, 회원국들이 이와 같은 개인정보 파일에 대하여 입법 등을 통해 규율하고자 할 때 참고하여 각국의 실정에 맞는 이행방안과 절차를 채택토록 하고 있다. 따라서 동 가이드라인은 강제력이나 구속력이 있는 지침은 아니다. 다만, 동 가이드라인은 개인정보 파일을 규율하는 여섯 가지 원칙을 제시하고 있는데, 이는 ① 합법성과 공정성의 원칙(Principle of Lawfulness and Fairness), ② 정확성 원칙(Principle of Accuracy), ③ 목적구체화의 원칙(Principle of the Purpose-specification), ④ 개인접근의 원칙(Principle of Interested-person Access), ⑤ 비차별 원칙(Principle of Non-discrimination), ⑥ 안전성 원칙(Principle of Security)이다.

〔표 4-2〕 UN 개인정보 6원칙

원칙		내 용
제1원칙	합법성과 공정성의 원칙	· 공정하고 합법적인 방법에 의한 개인정보 수집·처리 · UN 헌장의 목적과 원칙에 위배되는 개인정보 처리 금지
제2원칙	정확성 원칙	· 정확성과 관련성 확보를 위한 정기적 확인절차 필요 · 정보의 완전성과 최신성 확보를 위한 노력 필요
제3원칙	목적구체화의 원칙	· 목적과 이용에 관한 사항의 구체적 명시 및 정당성 확보 · 명시된 목적과의 적절성과 관련성 유지 · 동의가 있는 경우를 제외한 목적외 이용 및 공개 금지 · 목적달성에 필요한 기간 이상으로의 정보보유 금지
제4원칙	개인접근의 원칙	· 정보의 이용 또는 처리방법에 대한 정보주체의 알 권리 · 부정확한 정보에 대한 정정 또는 삭제요구권
제5원칙	차별금지 원칙	· 종교, 인종, 정치적 견해 등을 이유로 한 자의적이고 부당한 차별 금지
제6원칙	안전성 원칙	· 사고로 인한 정보의 손실이나 파괴 또는 정보의 남용, 권한없는 접근, 컴퓨터 바이러스 오염 등으로부터 정보를 안전하게 보호하기 위한 적절한 조치 필요

한편 UN 가이드라인은 제6조에서 정보보호원칙의 적용으로부터 배제되는 경우를 규정하고 있는데, 이에 의하면 국가안보·공공질서·공중보건 또는 공중도덕과 관련된 정보처리는 제1원칙부터 제4원칙의 적용을 받지 않는다고 한다. 단, 이 경우에도 회원국에서 이러한 적용제외에 대한 사항을 법률로 명시하고 있고 필요최소한의 수준으로 적용배제의 범위를 제한하고 있는 경우에만 가능하다. 또한 차별금지원칙의 적용제외는 오직 인권보호와 차별방지를 위한 국제인권법의 한계 내에서만 허용된다. 이 외에도 동 가이드라인은 프라이버시 보호에 관한 충분한 보호대책이 구비된 국가들 간의 자유로운 정보의 이동 및 상기 원칙의 준수여부를 감독할 독립기구의 설치 등에 대하여 규정하고 있다.

3. EU 개인정보보호 지침

EU의 95/46/EC 지침은 EU 회원국 시민들의 기본권과 자유를 보호하고 개인정보처리와 관련된 개인의 프라이버시를 보호하기 위한 일반적인 개인정보보호지침이다. 동 지침은 상이한 개인정보보호 수준을 가진 회원국의 개인정보보호 법체계를 통일하여, EU 내에서는 모든 회원국 시민들의 개인정보가 동일한 수준으로 보호될 것을 보장함을 목표로 하고 있다. 구체적으로는 EU 회원국 내에서 ① 개인정보 처리에 관한 의무와 책임을 확립하고, ② 개인정보처리의 투명성이 유지되도록 보장하며, ③ 민감한 정보에 대한 특별한 보호기준을 설정하고, ④ 개인정보처리에 대한 효과적인 감독권과 집행권을 확보하는 것이 그 목표이다. EU 지침은 유럽연합 의회와 이사회에 의해 채택된 지침이므로, 회원국은 동 지침의 이행을 위하여 새롭게 개인정보보호법을 제정하거나 기존의 법률을 개정할 필요가 있었다. 현재 15개국의 EU 회원국이 모두 EU 지침에 맞추어 자국의 개인정보보호법을 완비한 상태이다.

EU 지침은 OECD 가이드라인과는 달리, 기본적으로 자동화된 수단에 의한 개인정보의 처리에 적용된다. 물론 전적으로 자동화된 수단에 의할 것을 요구하지는 않으며 부분적으로 자동화된 수단에 의할 경우에도 적용될 수 있고, 더 나아가 자동화된 수단이 아닌 다른 방법에 의한다 하더라도 개인정보가 파일링시스템[128]의 일부를 구성하거나 그러한 의도로 처리되는 경우에도 적용된다.[129] 즉, EU 지침은 모든 개인정보의 자동화된 처리 및 '구조화된 수기파일(structured manual files)'에 적용되는 것으로 볼 수 있다. 또한 동 지침은 기본적으로 자연인(natural person)의 개인정보보호를 위한 것이므로, 법인(legal person)의 정보는 보호의 대상이 아니다. 다만, 회원국이 법인의 정보를 보호하는 내용의 규정을 두

128) EU 지침 제2조에 의하면, 파일링시스템(filing system)이란 기능적으로 또는 지리적으로 집중·분산·산재되어 있는지 여부와는 관계없이, 특정한 기준에 따라 접근할 수 있는 모든 개인정보의 구조화된 장치를 의미한다.

129) EU 지침의 적용범위는 UN 가이드라인과 기본적으로 유사하다.

는 것은 가능하다.

한편 EU 지침은 적용범위를 제외하고는 OECD 가이드라인의 개인정보보호 8원칙의 내용을 대부분 수용하고 있다. 다소 구분되는 점이 있다면, EU 지침은 원칙적으로 민감한 개인정보의 수집을 금지하고 있어 민감한 개인정보에 대한 더욱 강력한 개인정보보호의 입장을 취하고 있다는 점이다. 또한 수집된 개인정보를 제3자에게 제공하거나 공개하는 행위에 대해서 OECD 지침과는 달리 상세한 규정을 두어, 수집·이용목적 고지시 개인정보 제3자 제공에 대한 점도 함께 고지토록 하고 있다. 그 외에도 필요이상으로 정보주체가 식별되지 않도록 하고 장기간의 저장이 필요한 개인정보에 대해서는 적절한 보호 기준을 설정하도록 규정하고 있다.

그러나 무엇보다도 EU 지침의 가장 두드러지는 특징은 바로 독립적인 개인정보보호기구의 설립을 통한 개인정보처리의 관리·감독 및 개인정보의 제3국으로의 이전에 대한 엄격한 제한이다. EU지침은 개인정보처리자로 하여금 회원국 내 독립적인 개인정보보호기구에 개인정보 처리행위에 대해 고지토록 하고 있는데, 이는 개인정보보호기구가 고지받은 개인정보처리행위가 정보주체의 권리와 자유에 위협이 될 수 있는지 여부를 사전심사할 수 있도록 하기 위함이다. 또한 EU 지침은 제25조에서 회원국 외 제3국이 동 지침에서 밝히고 있는 개인정보보호의 적절한 수준을 갖추고 있지 아니한 경우에는 개인정보를 해당 국가에 이전하지 못하도록 하고 있는데, 이 규정은 일명 '프라이버시 라운드(Privacy Round)'라 불리는 사실상의 새로운 무역장벽으로 떠오르고 있다.[130]

130) EU 지침의 위와 같은 성격으로 인하여 다국적 기업이나 EU 회원국 내 기업과 무역을 하는 제3국의 기업은 큰 영향을 받게 되었다. 이에 각국에서는 1995년 EU 지침이 등장한 이후, 동 지침에 부합하는 수준의 개인정보보호 대책을 마련하여 EU로부터 개인정보를 이전해도 무방한 국가로 승인되려는 노력을 계속해오고 있다. 실제로 미국은 EU와의 협의를 위해 '세이프하버원칙(Safe Harbor Principles)'을 제정하기도 하였다.

〔표 4-3〕 EU 개인정보보호지침의 주요내용

구 분	내 용
적용범위	· 물적 범위 : 자동처리되는 개인정보 및 구조화된 파일링 시스템에 포함되는 개인정보 · 인적 범위 : 자연인의 개인정보
적용제외영역	· 국가안보, 공공의 안전 및 방위를 위한 개인정보 처리 · 형사법 영역에서의 개인정보 처리 · 서신왕래와 같은 지극히 개인적이고 사적인 목적의 개인정보 처리 · 언론보도, 문학, 예술적 표현을 위한 개인정보 처리
정보처리자의 의무	· 공정하고 적법한 개인정보의 처리 · 정보처리목적의 명시 · 정보처리목적과의 적절성과 관련성, 비례성 유지 · 개인정보의 정확성과 최신성 확보 · 기술적, 조직적 보안조치 확보 · 감독기구에 정보처리에 대하여 고지
정보주체의 권리	· 정보처리의 전반적인 사항에 대하여 통지받을 권리 · 정보처리에 대하여 협의할 권리 · 자신의 개인정보에 대해 수정을 요구할 권리 · 특정 상황에서의 개인정보 처리에 대하여 반대할 권리
제3국으로의 정보이전금지	· 적절한 보호수준을 갖추지 않은 제3국으로의 개인정보 이전 금지
독립기구의 설치	· 회원국 내 독립적인 개인정보보호기구의 설치

유럽연합은 또한 지난 2002년, 전자통신부문에서의 개인정보처리 및 프라이버시 보호에 관한 지침을 마련하였다. 동 지침은 지난 1995년 EU 지침에 규정된 기본원칙을 통신(Telecommunications)부문에 대한 세부규칙으로 전환하고 통신 영역에서의 개인정보와 프라이버시를 보호하기 위해 마련된 지침 97/66/EC을 폐기하고 대체하는 새로운 지침이다. 동 지침은 1997년 이후 새롭게 변화된 정보통신서비스 시장과 기술의 발전상황을 반영하고 통신서비스 사용자에게 사용기술과 관계없이 동일한 수준의 개인정보와 프라이버시 보호를 제공하기 위한 목적으로 개정되었다.

동 지침의 기본목적은 전자통신(Electronic Communications) 분야의 개인정보 처리와 관련하여 EU 회원국의 기본권과 자유, 특히 프라이버시의 보호수준을 동등하게 맞추고 EU 회원국 내에서 전자통신 장치와 서비스 및 개인정보가 자유롭게 이전될 수 있도록 보장하는 것이다. 따

라서 1995년 EU지침에서 규정한 개인정보보호를 위한 기본사항을 바탕으로, 전자통신과 관련한 이용자의 전송정보(traffic data)·위치정보·통신비밀의 보호, 쿠키사용에 대한 이용자의 거부기회 보장, 옵트인(opt-in) 제도 도입을 통한 스팸메일 등 원치 않는 통신으로부터의 이용자 보호, 전자통신서비스의 기술적·조직적 보안조치, 발신자번호·접속자번호의 표시 제한 등에 관한 사항을 규정하고 있다. 이와 같이 동 지침은 기술발달의 영향을 가장 빨리 그리고 가장 밀접하게 받고 있는 전자통신 분야에서 이용·전송되고 있는 개인정보를 어떻게 보호할 것인가에 대한 문제를 다루고 있을 뿐 아니라, 위치정보와 발신자번호표시, 스팸메일과 같은 최근 급격히 문제가 되고 있는 사안들에 대해 구체적으로 규율하고 있다는 점에서 의미가 있다. 동 지침은 2002. 7월부터 시행되었으며, EU 회원국들은 2003년 10월 31일까지 지침의 내용을 반영하는 법체계를 마련키로 하였다.[131]

131) 2003년 10월 현재 오스트리아, 벨기에, 덴마크, 이탈리아는 원하지 않는 상업적 이메일에 대한 옵트인(opt-in) 제도를 EU 지침에 따라 도입하였고, 그 외에도 8개국 정도가 3개월부터 1년까지 전송정보(traffic data)를 보유할 수 있는 기간을 규정한 법률을 채택하였다. (EPIC Alert, *"EU Set to Implement Privacy Directive"*, 2003. 10. 30)

제 2 절 유럽

근대 시민사회가 싹튼 유럽은 일찍부터 개인의 자유와 인권을 존중하는 법적·사회적 전통이 강하였다. 이러한 전통은 유럽이 현대 사회의 새로운 인권질서를 주도할 수 있도록 하였다. 즉, 1950년 「유럽인권협약(European Convention for the Protection of Human Rights and Fundamental Freedoms)」을 채택하는 것에서 시작하여, 단일 유럽체계로 변화하면서는 「유럽연합기본권헌장(charter of Fundamental Rights of the European Union)」을 마련하는 등 유럽은 개인의 인권보호를 위한 기본적인 보루를 마련하여 왔다. 이러한 경향으로 인하여, 유럽에서는 프라이버시보호 또는 개인정보보호를 인권과 자유의 측면에서 인식하는 것이 일반적이다.

이렇듯 유럽은 개인정보침해나 프라이버시침해를 개인의 자유나 인권을 침해하는 것으로 여겨 다른 어떠한 국가들보다도 적극적으로 보호하려는 움직임을 보여 왔다. 따라서 개인정보보호와 프라이버시보호 분야에 있어서 선구적인 역할을 담당하여 왔다고 할 수 있는데, 특히 정보처리 기술의 발달이 급속도로 진전된 1960년대 말부터는 개인의 사적 영역인 프라이버시 침해에 대한 우려가 증대되었고 프라이버시 침해로부터 개인의 자유와 기본권을 보호하기 위한 대책이 필요하다는 논의가 꾸준히 이어져 왔다.

특히 20세기 들어 지속적으로 하나의 단일 공동체를 형성해 나가는 과정에서, 유럽 각국은 유럽공동체(EU)를 중심으로 단일한 개인정보보호의 수준을 확보하려는 노력을 계속하였다. 이러한 노력은 앞서 살펴본 바와 같이, EU 개인정보보호지침을 마련하여 각 회원국이 이행토록 한 것에서도 충분히 알 수 있다.[132] 그러나 오늘날 EU 개인정보보호지침이나 제

132) 이 외에도 유럽이사회(Council of Europe)는 1981년 "개인정보의 자동화 처리에서의 인권보호를 위한 합의서"를 체결하고, 같은 해 회원국 각료회의에서 "자동화된 의료정보은행의 규제를 위한 권고문(Recommendation No.R(81) of the Committee of Ministers to Member States on regulations for automated medical data banks)"을 채택하는 등 이후에도 수많은 개인정보 관련 권고문을 채택하였다.

도는 비단 유럽 내에서만 의미를 가지는 것은 아니다. EU 개인정보보호 지침이 '프라이버시 라운드'의 효력을 가지는 것임은 주지의 사실이며, 세계 각국의 개인정보보호기구도 유럽 모델을 중심으로 만들어지고 있다. 따라서 유럽에서는 어떠한 개인정보보호법 체계를 가지고 있는지, 개인정보침해로 인한 피해는 어떠한 방법으로 구제하고 있는지, 주요 선진국들의 개인정보보호기구들은 어떻게 운영되고 있는지 등을 살펴볼 필요가 있을 것이다.

1. 영국

성문헌법이 없는 영국은 당연히 프라이버시권 또는 개인정보자기결정권에 대한 명시적·묵시적인 헌법상의 근거를 가지고 있지 않다. 그러나 영국은 1215년 마그나카르타(Magna Carta)에서 시작하여 인권선언의 의미를 가지는 권리청원(Petition of Right)과 권리장전(Bill of Rights)의 제정을 거치면서, 시민들의 사적 자유와 인권을 존중하는 법제도 도입에 선구적인 역할을 해왔다. 이러한 인권존중의 법적 전통은 당연히 프라이버시 및 개인정보의 법적 보호로 이어지게 되어, 영국은 「1984년 정보보호법(The Data Protection Act 1984)」을 제정하여 시행하게 되었다. 또한 유럽인권협약을 이행코자 제정한「1998년 인권법(The Human Rights Act 1998)」에서는 동법 제8조에서 프라이버시와 가정생활, 주거 및 통신의 자유와 권리를 규정함으로써, 명시적으로 프라이버시 보호의 필요성과 권리를 인정하고 있다.

가. 개인정보보호 법제현황

영국은 「1984년 정보보호법(The Data Protection Act 1984)」을 제정함으로써 개인정보보호를 위한 첫 번째의 발판을 마련하였다고 볼 수 있다. 그러나 동법은 개인정보보호를 위한 일반원칙을 모두 아우르고 있다

기보다는 개인정보를 처리하는 공공기관이나 사업자 등을 등록하여 '정보처리자 등록부'를 유지·관리하는 것에 더 큰 초점이 맞추어져 있었다. 그러던 중 1995년 EU지침이 제정되면서, 영국도 동 지침의 내용에 맞추어 국내법을 전면 수정할 필요가 생겼다. 이러한 이유에서 제정된 법률이 바로 「1998년 정보보호법(The Data Protection Act 1998)」이다. 동법은 공공과 민간부문의 구분 없이 영국에서 이루어지는 모든 개인정보 처리에 적용되는 개인정보보호 기본법의 역할을 하고 있다.

이렇듯 정보보호법은 영국의 개인정보보호 기본법으로서 적용범위가 광대함은 물론, 개인정보보호 기본원칙을 비롯한 개인정보와 관련된 사항을 포괄적으로 규정하고 있다. 그러나 기본법의 특성상 정보보호법은 각 개별 영역의 특수한 개인정보 처리상황을 모두 규정하고 있지는 않고, 특정 영역에 관하여는 다른 특별법이나 하위법령에 위임하고 있다. 대표적인 것이 전자통신 분야에서의 개인정보보호와 관련하여, 1997년 EU지침의 내용을 보충하고 구체화하기 위해 제정된 「1999년 전자통신(정보보호 및 프라이버시)규칙(The Telecommunications(Data Protection and Privacy) Regulations 1999(1999/2093)」, 「2000년 조사권에 관한 법률 규칙(RIPA 2000 : The Regulations of Investigatory Powers Act 2000)」, 「2000년 전자통신규칙(합법적인사업관행)(통신차단)(The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (2000/2699))」이 있다. 이 중 '1999년 전자통신규칙'은 종합정보통신망(ISDN), 공공디지털모바일네트워크(public digital mobile network), 주문형 비디오(VOD), 쌍방향 TV 등 새로운 전자통신분야에서의 개인정보보호를 위해 제정된 것으로, 원하지 않는 팩스나 전화와 같은 스팸통신에 대하여 규제하고 있다.[133] 또한 '2000년 조사권에 관한 법률 규칙'은 EU 전자통신 분야에서의 정보보호지침 제5조의 내용을 시행하는 별도의 입

133) 동법은 2003년 12월 11일부로 「2003 프라이버시와 전자상거래 규칙(EC 지침)(The Privacy and Electronic Communications (EC Directive) Regulations 2003」으로 대체되었다. 새롭게 제정된 규칙은 전자상거래의 발달상황을 규율을 위해 1999년 규칙보다 기술과 프라이버시에 관한 사항을 많이 포함하고 있다. (영국 헌법부 웹사이트, http://www.dca.gov.uk/ccpd/dpsubleg.htm 참조)

법으로 공공·민간 네트워크를 통한 전자통신의 비밀을 보호하기 위해 제정된 것이다.[134] 이 외에도 정보주체가 신용정보회사 등 평가기관에서 보유하고 있는 각종 개인정보에 대하여 접근권을 행사할 수 있도록 규정한 「1974년 소비자신용법(The Consumer Credit Act 1974」, 자신의 건강정보 또는 치료기록에 대한 접근을 요청할 수 있도록 한 「1988년 의료기록 접근에 관한 법률(The Access to Medical Reports Act 1988)」, 「1990년 건강기록 접근에 관한 법률(The Access to Health Records Act 1990)」등의 법률이 있다. 더하여 1998년 정보보호법은 하위법령으로 국가안보, 형사, 세금, 의료, 교육, 사회사업, 언론 등 특정 영역을 규율하는 규칙을 제정하여 시행하고 있다.

〔표 4-4〕 영국의 개인정보관련 법제현황

구분	법률
개인정보	· 1998년 정보보호법(The Data Protection Act 1998)
정보공개	· 2000년 정보공개법(The Freedom of Information Act 2000)
전자통신 분야의 정보보호	· 1999년 전자통신규칙(정보보호 및 프라이버시)(The Telecommunications (Data Protection and Privacy) Regulations 1999 (1999/2093) · 2000년 조사권에 관한 법률규칙(The Regulations of Investigatory Powers Act 2000)(RIPA 2000) · 2000년 전자통신규칙(합법적인 사업관행)(통신차단)(The Telecommunications (Lawful Business Practice)(Interception of Communications) Regulations 2000 (2000/2699))
신용정보	· 1974년 소비자신용법(The Consumer Credit Act 1974)
형사기록	· 1997 경찰법(The Police Act 1997)
의료정보	· 1988년 의료기록 접근에 관한 법률(The Access to Medical Reports Act 1988) · 1990년 건강기록 접근에 관한 법률(The Access to Health Records Act 1990)

134) Gerald Spindler/Fritjof Börner(Edit.), *"E-Commerce Law in Europe and the USA"*, Springer, 2002, p. 298.

나. 정보보호법의 주요내용

2000년 3월 1일부터 시행된 정보보호법은 영국의 개인정보보호 기본법의 역할을 하고 있다. 따라서 개인정보보호 기본원칙을 비롯하여 정보주체의 권리와 정보처리자의 의무, 개인정보보호기구의 설립 및 운영, 정보법원(Information Tribunal)의 설치, 개인정보의 국외이전 등에 관한 사항을 포괄적으로 규정하고 있다. 또한 적용범위에 있어서도 공공과 민간의 구분이 없다. 특히, 정보보호법은 주로 전자적인 형태로 처리되는 개인정보를 규율할 목적으로 제정된 것이나 그 후 적용범위가 더욱 확대되어 특정한 구조화된 수기 파일링시스템(manual filing systems)은 물론, 의료기록이나 교육기록에 대해서는 순수하게 수기로 처리되는 개인정보까지도 동법의 규율을 받는 것으로 포함시키고 있다.[135] 한편 동법은 생존하고 있는 개인에 관한 정보를 보호대상으로 함을 명시적으로 밝히고 있는 바, 법인정보나 死者의 정보는 제외된다.

1998년 정보보호법의 가장 큰 특징은 개인정보의 수집·처리 등을 규율하기 위한 정보보호 8원칙을 세부적으로 규정하고 있다는 것이다. 이 원칙은 기본적으로는 OECD 프라이버시 8원칙과 유사하나, EU 개인정보보호지침의 내용을 흡수하여 개인정보 국외이전 제한의 원칙을 규정하고 있다는 점과 민감한 개인정보에 대하여는 특별히 처리할 것을 포함시키고 있다는 점에서 특색이 있다. 정보보호 8원칙의 내용을 간략히 정리해 보면 다음과 같다.

〔표 4-5〕 영국의 정보보호 8원칙

원칙	주요내용
제1원칙	공정하고 합법적인 개인정보 처리 및 민감한 정보의 특별처리
제2원칙	제한된 목적 내에서의 개인정보 처리

135) 다만, 개인정보가 수기로만 작성되고 처리되는 특정한 경우에 대해서는 2007년 10월 24일까지 동법 일부조항의 적용이 배제된다.

제3원칙	목적과의 적절한 관련성을 가진 개인정보의 처리 및 과도한 개인정보 수집·처리 금지
제4원칙	개인정보의 정확성 확보 및 필요한 경우 최신성 확보
제5원칙	수집목적 달성을 위한 필요한도 내에서의 보유
제6원칙	정보주체의 권리를 존중하는 방법을 통한 개인정보 처리
제7원칙	적절한 기술적·관리적 조치를 통한 권한 없는 접근·수정·손실 등으로부터 개인정보보호
제8원칙	적절한 개인정보보호수준을 갖춘 국가 이외의 곳으로 개인정보 이전금지

정보보호 8원칙 외에도 정보보호법의 주요 내용 중 하나는 정보주체의 권리와 정보처리자의 의무에 대한 규정이다. 특히 동법은 정보주체가 개인정보자기결정권과 관련하여 어떠한 권리를 향유하는지를 구체적으로 밝히고 있다. 영국 정보보호법에서 보장하고 있는 정보주체의 권리를 살펴보면, ① 자신의 정보에 접근할 권리, ② 부정확한 개인정보를 정정·삭제할 권리, ③ 자신에 관한 정보가 처리되고 있는 목적, 방법, 내용 등에 대하여 고지받을 권리 및 이를 통해 자신과 관련된 정보의 처리에 대하여 반대할 권리와 같은 일반적인 정보주체의 권리 외에도 ④ 다이렉트 마케팅의 목적으로 자신의 정보를 이용하는 것을 배제할 권리, ⑤ 개인정보 침해로 인해 입은 피해에 대하여 보상을 받을 권리, ⑥ 자신에 관하여 전적으로 자동화된 방법에 의한 의사결정이 이루어지는 것에 반대할 권리, ⑦ 개인정보침해행위가 있다고 판단될 경우 이의제기를 할 권리, ⑧ 개인정보처리의 법규위반여부 심사를 청구할 권리가 인정되고 있다.[136]

반면에 정보처리자에 대해서는 개인정보처리행위를 고지·등록할 의무, 정보보호원칙을 준수할 의무 등을 규정하고 있다. 특히 정보처리자의 고지·등록의무는 정보처리의 투명성과 공개성을 확보하기 위한 것으로, 모든 개인정보처리자는 순수한 수기기록물, 사업 활동과 관련된 핵심적인 정보, 자선단체 회원기록을 제외한 모든 개인정보처리에 대하여 커미셔너에게 반드시 개인정보처리 상황을 고지하고 등록하여야 한다. 특히 커

136) 정보보호법(DPA) 제2장(제7조～제15조).

미셔너에 대한 고지의무는 등록부의 최신성과 현재성의 유지를 위해 매년 고지사항을 갱신할 의무도 포함한다. 만약 기한까지 정보처리를 고지하지 않거나 아무런 근거 없이 등록을 갱신하지 않는 것은 위법행위가 되어 형사처벌을 받을 수 있다.[137] 또한 정보처리자는 상기 정보보호원칙을 이행함으로써 올바르고 적절한 정보처리관행을 확립하여 실행하여야 할 의무를 가진다. 정보처리자가 이러한 의무에 위반하여 불법적이거나 부당한 개인정보침해행위를 하였을 경우에는 민사상 손해배상책임은 물론, 형사상 제재도 받을 수 있다.

다. 영국의 개인정보보호기구

영국은 1984년부터 정보보호등록관(Data Protection Registrar)을 설치하여 자국 내에서 이루어지는 모든 개인정보 처리행위를 사전 등록함으로써 개인정보를 보호하여 왔다. 이러한 정보보호등록관은 그 역할과 위상이 점차 증대하여, 1998년에는 전면 수정된 정보보호법에 따라 정보보호커미셔너(Data Protection Commissioner)로 개칭되었고, 2000년에는 정보공개법에 따라 정보커미셔너(Information Commissioner)로 변천되어 오늘날에 이르고 있다.

(1) 정보커미셔너의 지위

정보커미셔너는 정보보호법과 정보공개법에 근거하여 설립된 개인정보보호를 위한 독립법정기구이다. 커미셔너는 여왕의 특허장에 의해 임명되며 5년의 임기가 보장되고 두 차례에 걸쳐 재임이 가능하다. 단, 커미셔너는 65세 미만의 자이어야 한다. 영국의 정보커미셔너의 독립성과 자율성은 무엇보다도 행정부의 지시·감독을 받지 않고 독자적으로 운영된다는 점을 통해 확인할 수 있다. 즉, 커미셔너의 임금과 연금은 하원의

137) 정보보호법(DPA) 제3장(제16조~제26조).

결의를 통해 결정되고 별도 조성된 통합기금에서 지급받으며 기관의 운영예산도 직접 의회의 결의를 통해 지원받고 있기 때문에, 내무부로부터 행정적 지원이나 협조 외의 간섭을 받지 않는다. 또한 정보커미셔너는 기관의 각종 활동상황에 대해 의회에 직접 보고한다.

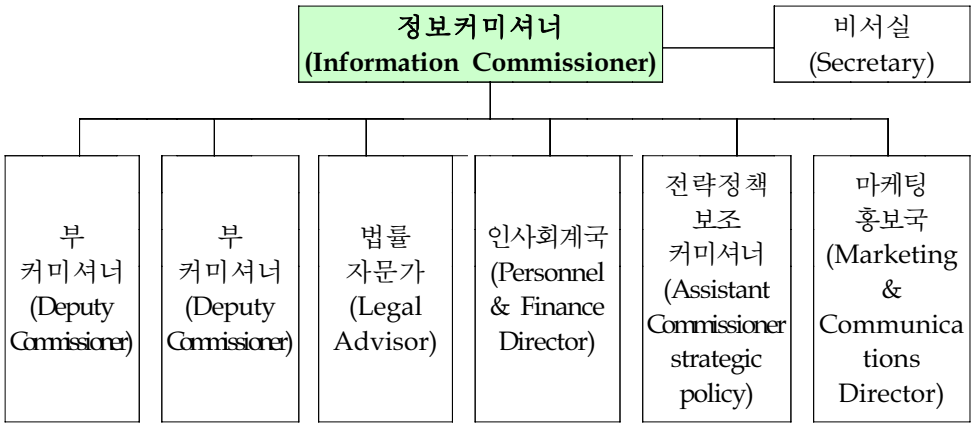
(2) 정보커미셔너의 업무범위

영국의 정보커미셔너가 활동하는 첫 번째의 근거법률은 1998년 정보보호법이다. 동법이 민간과 공공부문, 자동화된 개인정보파일과 구조화된 수기파일에 모두 적용되는 광범위한 적용범위를 가진 개인정보보호 기본법임은 이미 살펴본 바와 같다. 따라서 정보커미셔너 역시 민간과 공공부문의 모든 개인정보처리를 관할대상으로 삼고 있다. 따라서 온라인·오프라인을 구분하지 않고 일반 사업자에 의한 개인정보처리나 정부부처 등 공공기관에 의한 개인정보처리가 올바르게 이루어지고 있는지 감시하고 규율하는 역할을 하고 있다. 이에 더하여 특수한 영역별로는 의료정보, 신용정보, 교육정보, 정보통신분야에서 취급되는 개인정보, 근로자 정보 및 CCTV와 프라이버시 문제, 다이렉트 마케팅 문제 등에 대해서도 각종 규칙이나 지침 등의 법규를 통해 규율하고 있다.

(3) 정보커미셔너의 조직구성

정보커미셔너는 개인정보보호 전담기구인 만큼 그 규모가 상당히 큰 편이다. 조직구성을 살펴보면, 커미셔너 1인과 부커미셔너 2인, 인사회계국, 마케팅홍보국, 법률자문부서, 전략정책보조커미셔너의 6개 부서로 구성되어 있으며, 2003년 11월 현재 약 200여명의 직원이 활동하고 있다. 1인의 부커미셔너는 특히 전자통신 분야에서 개인정보처리자가 법규를 준수하고 있는지를 감독하고 개인정보침해행위를 조사하여 법위반 사항이 있다고 판단될 경우 각종 고지명령(Information Notice or Enforcement Notice)을 부과하는 업무를 담당하고 있으며, 다른 부커미

셔너는 의료정보, 신용정보, 금융기관, 연금, 보험 등의 분야에서 개인정보침해행위를 규제·감독하는 역할을 한다. 법률자문부서에서는 개인정보 관련법규의 해석이나 접수된 민원사건의 중대한 법적 쟁점사항에 대한 법률자문을 행하며, 전략정책보조커미셔너는 개인정보보호 정책연구 및 정보공개 관련 정책개발 등의 업무를 함께 수행한다. 또한 인사회계국에서는 직원채용에서부터 회계, 시설관리 등 행정일반에 관한 업무를 하며 마케팅홍보국에서는 대외홍보 및 캠페인 실시, 웹사이트 관리 등의 업무를 담당하고 있다.



(그림 4-1) 영국 정보커미셔너의 조직도

(4) 정보커미셔너의 주요기능

정보커미셔너는 처음 설립된 1984년 당시에는 정보처리에 대한 등록업무를 담당하는 기관이었으나, 1998년 정보보호법의 제정으로 전반적인 개인정보보호와 관련된 업무를 담당하게 되었다. 특히 2000년에는 정보공개법도 함께 관장하게 됨에 따라, 공공부문에 대한 정보공개요구에 대한 업무도 함께 수행하게 되었다. 따라서 정보커미셔너는 현재 정보보호 등록부를 유지·보관하고 정보보호원칙을 실행할 뿐 아니라, 개인정보보호 실행규약(Code of Practice)이나 가이드라인, 지침 등을 발행하여 올

바른 정보처리관행이 확립될 수 있도록 하는 역할을 하고 있다. 이러한 커미셔너의 주요 기능을 살펴보면 다음과 같다.

먼저, 커미셔너는 개인정보를 취급하는 개인이나 단체의 이름과 주소 등 연락처, 정보처리목적, 수집·보유하고 있는 개인정보항목 등 정보처리와 관련된 소정의 내용을 고지받아 기록하는 공공등록부(public register)를 유지·관리할 책임을 진다. 이러한 정보보호등록부(The Data Protection Register)는 인터넷 웹사이트를 통해 공개됨으로써 일반 국민들이 쉽게 접근하여 확인할 수 있도록 하고 있다.[138]

정보커미셔너는 또한 각종 개인정보침해사건이나 사업자나 공공기관 등의 개인정보처리행위에 대한 불만사항을 접수받아 사건을 조사·심사하여, 당사자간 분쟁을 해결하고 피해를 입은 자를 구제해주는 역할을 하고 있다. 또한 침해사건의 접수 여부와는 관계없이 사회적으로 문제가 되고 있어 자체 조사의 필요성이 있을 때에는 직권으로 개인정보보호 실태조사를 실시하여 법위반 여부를 심사하기도 한다. 이 외에도 개인정보에 관한 각종 지침이나 규칙 제정, 법률 및 기술자문, 사업자·소비자를 대상으로 한 정보제공, 교육·홍보, 개인정보보호를 위한 조사연구, 유관기관 협력 등의 기능을 수행하고 있다.

〔표 4-6〕 영국 정보커미셔너의 주요기능

주요기능	세부내용
등록업무	· 고지 접수를 통한 개인정보처리행위 등록업무 처리
피해구제	· 각종 불만사항이나 개인정보침해사건 접수 · 당사자 자료제출요구, 의견청취, 현장조사 등을 통한 사실조사 · 사실조사를 바탕으로 한 법규위반여부 심사 · 민원심사과정에서 화해권고 등 개인정보 분쟁조정 · 법위반사항에 대해 시정조치명령 또는 이행고지, 정보고지 부과 · 불이행시 정보법원에 소송지원 또는 형사기소
정보공개	· 정부, 공공기관 등에 대한 정보공개명령권 행사

138) 정보커미셔너에 등록된 정보처리 신고는 2002년 3월 31일 현재 198,519건이다. (EPIC & PI, *"Privacy and Human Rights 2003 - An International Survey of Privacy Laws and Developments"*, http://www.privacyinternational.org/survey/phr2003/countries/unitedkingdom.htm 참조)

조사・감독	・프라이버시 침해여부에 대한 직권 실태조사 및 모니터링 ・정보보호원칙 및 법규 준수여부 감독 ・개인정보침해행위 및 법위반사항에 대하여 이행명령(고지) 부과 ・이행명령 불이행시 및 법규위반 확인시 검찰 등 해당기관 고발
실행규약 제정	・각종 개인정보보호 실행규약(Code of practice)의 제정 및 고시
정보제공	・개인, 사업자, 정부, 공공기관에 대하여 각각 정보제공 및 자문 ・정보처리자 요청시 법률상담 및 평가정보 제공
정책 및 입법자문	・개인정보 관련 법안 심의 및 의견제시 ・정부의 각종 정책에 대하여 의견제시 및 자문
개인정보 보호연구	・개인정보 관련 기술동향 조사 및 연구
교육・홍보	・각종 단체에 대한 개인정보보호교육 실시 ・개인정보보호 공공캠페인 실시 ・언론 등에 대한 프라이버시커미셔너 활동 등 홍보
유관기관 협력	・국내 개인정보 유관기관 및 시민단체와의 협력 ・EU 등 해외 개인정보보호기구와의 국제협력

라. 개인정보피해구제 절차 및 방법

영국의 정보커미셔너는 앞서 살펴본 것처럼, 개인정보침해로 인한 정보주체의 피해를 구제하기 위한 각종 활동을 펼치고 있다. 먼저 당사자에게 자료제출요구나 의견청취 등을 통해 사실조사를 하고, 법위반사항이 있다고 판단될 경우 우선적으로는 당사자간 충분한 협의와 논의를 통해 분쟁을 원만히 해결토록 화해를 유도한다. 또한 법위반 단체가 법규를 적절하게 준수할 수 있도록 이끌어낸다. 그러나 이러한 접근방법이 만족스러운 결과를 내지 못하였을 때에는 추가적인 정보를 제공토록 요구하는 정보고지(Information Notice) 조치를 내리거나 시정해야할 사항 등을 알리는 이행고지(Enforcement Notice)를 내릴 수 있다. 그러나 만약 이렇게 부과된 고지명령을 이행하지 않거나 거부할 때에는 커미셔너는 형사기소를 하거나 정보법원(Information Tribunal) 등에 소를 제기할 수 있다. 또한 정보처리자 역시 커미셔너의 이행고지에 불복하여 정보법원에 소를 제기할 수 있다. 정보법원[139]은 이렇게 제기된 사건에 대하여

139) 정보법원은 정보보호법 제6조에 의해 설립된 사법기구로, 의장 1인과 부의장 및 기타 위원으로 구성된다. 의장은 검찰총장과의 협의 후 대법관(Lord Chancellor)이 임

정보커미셔너가 수행한 정보처리자의 법규위반여부에 대한 평가를 재심사하는 역할을 한다. 재심사를 통해 정보처리자가 정보보호 관련법령 또는 정보보호 8원칙의 위반하였는지를 결정하여 판결한다. 이 때 정보법원에서 정보커미셔너의 법위반에 대한 판단이 옳았던 것으로 결정되는 경우, 이행고지를 거부하거나 불이행한 정보처리자의 행위는 형사범죄로 성립되어 관계기관의 처벌을 받을 수 있다. 이러한 영국의 개인정보피해 구제 절차 및 방법은 아래와 같이 진행된다.

민원접수	· 정보보호 제8원칙 또는 1998년 정보보호법 위반 및 개인정보침해사건 접수
↓	
사실조사	· 자료제출요청(정보고지) 등을 통한 사실조사
↓	
심사 및 판단	· 원칙 및 법위반 여부에 대한 심사 및 판단
↓	
분쟁해결유도	· 화해, 조정 등의 방법으로 당사자간 합의유도
↓	
행정제재	· 법규를 준수하지 못하였다고 판단된 경우, 당사자간 합의가 되지 못하였거나 비공식적인 방법으로 해결될 수 없는 경우, 해당 정보처리자에게 시정요구 등 이행고지 · 정보처리자가 이행고지에 따른 경우 사건 종료 · 정보처리자가 이행고지에 따르지 않은 경우 소 제기
↓	
항소(Appeal)	· 정보처리자가 커미셔너의 집행고지에 이의를 제기하여 정보법원(Information Tribunal)에 소 제기 가능
↓	
형사범죄의 성립	· 정보법원에서 정보처리자가 원칙이나 법률을 위반한 것이라고 결정한 경우 형사범죄(criminal offence)가 성립
↓	
형사고소	· 범죄가 되는 경우 커미셔너는 관계기관에 형사고소 가능

(그림 4-2) 영국 정보커미셔너의 피해구제 절차도

명하며 부의장은 대법관이 그 수를 결정하여 임명한다. 또한 그 외의 위원들은 내무부 장관이 그 수를 정하여 임명한다. 정보법원의 위원들은 정보주체와 정보처리자의 이익을 각각 대변하는 자로서, 최소 7년 동안 법정변호인(advocates) 또는 상담변호인(solicitor)의 경력을 가진 자이어야 한다.

한편 정보보호법은 정보처리자의 법규 위반행위 또는 개인정보침해행위로 인하여 경제적 피해를 입거나 정신적 고통을 겪은 자는 손해배상청구를 할 수 있다고 규정하고 있다. 따라서 피해자는 법원에 경제적·정신적 손해 또는 정신적 손해에 대해서만도 손해배상청구소송을 제기할 수 있다.[140] 이 경우 손해배상청구를 받은 정보처리자는 법규에서 요구하는 필요사항을 준수하기 위해 합리적으로 요구되는 주의를 모든 상황에서 다하였음을 증명함으로써 자신을 변호할 수 있다.[141] 정보커미셔너는 민사적 손해배상과 관련하여 준사법적 결정을 내릴 권한은 없으나, 이와 관련하여 특정한 유형의 소송[142] 중 공적으로 상당히 중요한 의미를 가진 사건이라고 판단되는 경우에는 소송을 지원할 수 있다. 커미셔너가 소송지원을 하기로 결정한 경우에는 소송지원의 범위와 한계[143]를 정하여 신청자에게 통지하여야 하며, 그 반대의 경우에도 소송지원을 하지 않기로 한 결정 및 적합하다고 생각되는 경우에는 그 사유도 함께 신청자에게 통보하여야 한다.[144]

---

140) 특히 정보보호법은 경제적 피해보다는 정신적인 스트레스나 고통이 클 수 있다는 개인정보침해의 특수성을 인정하여, 정신적 피해에 대한 보상에 대해서도 명시적으로 규정하고 있는 바, 법원은 손해가 입증되면 기타의 정신적 고통에 대한 보상을 명령할 수 있다.

141) 정보보호법 제13조.

142) 정보보호법 제53조제1항은 이러한 유형의 소송을 열거하고 있다. 이에 의하면, 정보커미셔너는 법원이 정보처리자가 부당하게 정보주체의 열람청구를 거부하였다는 주장을 합당한 것으로 인정한 경우(동법 제7조제9항), 정보처리자가 정보주체의 개인정보 처리중지 통보를 한 뒤에도 이를 준수하지 않았음을 인정한 경우(동법 제10조제4항), 정보처리자가 정보주체의 자동화된 의사결정에 반대할 권리의 행사를 방해하거나 무시한 것을 인정한 경우(동법 제12조제8항), 부정확한 개인정보의 정정·삭제·폐쇄·파기명령을 내린 경우(동법 제14조), 언론, 학문, 문학과 같은 특수목적을 위한 개인정보의 처리와 관련한 경제적·정신적 손해배상청구소송 등의 경우에는 소송당사자의 요청에 의해 소송지원을 할 수 있다.

143) 정보보호법 부칙 10에 의하면, 커미셔너는 변호사나 법률 자문가의 상담 또는 수임비용을 지원할 수 있다. 또한 소송지원을 하는 경우 커미셔너는 신청자는 판결의 집행과 관련한 비용을 지불할 책임으로부터 면제된다는 합의 등을 하여야 한다.

144) 정보보호법 제53조제3항～제4항.

2. 프랑스

프랑스는 1789년 프랑스혁명과 근대시민사회의 지도적 이념을 보전하고 구현한 프랑스민법전(나폴레옹법전)의 법적 전통을 이어받은 입헌민주주의 국가이다. 따라서 프랑스 헌법은 무엇보다도 인권존중의 이념을 강조하며, 헌법에서 보장된 시민권(civil rights)과 시민의 공적 자유(public liberties)의 보장을 위해 부여된 기본권을 법률을 통해 구체적으로 실현토록 하고 있다. 특히 1958년 프랑스 헌법은 기본권에 관한 사항, 국적·시민권에 관한 사항, 상속에 관한 사항, 범죄행위에 대한 정의와 형벌 또는 과세에 관한 사항, 선거 규칙 및 절차에 관한 사항 등에 대해서는 프랑스 의회가 전속적이고 배타적인 법규 제정권을 가진다고 규정함으로써, 인권이나 시민권과 같은 핵심적이고 중요한 문제에 대한 행정부의 자의적인 규제를 방지하고 있다.[145]

이러한 개인의 핵심적인 자유와 권리를 보호하려는 법적 전통은 개인정보 또는 프라이버시 보호와 관련하여서도 이어지고 있다. 비록 1958년 프랑스 헌법은 명확하게 프라이버시권에 대해 규정하고 있지는 않지만, 프랑스 헌법재판소(Conseil Constistutionnel)는 "프라이버시 보호는 곧 헌법에 의해 보장된 기본적 자유를 보호하는 것이다"라고 결정[146]함으로써 프라이버시에 관한 시민의 권리는 헌법에 함축적으로 내포된 권리라고 밝힌 바 있다. 이는 프라이버시를 헌법전문 및 제66조를 포함한 기본권 규정[147]에서 그 근거를 찾을 수 있는 개인의 기본적 자유에 관한 사항으

145) Constitution du 4 Octobre 1958, Art. 34(2). 이렇게 제정된 모든 법률은 1958년 프랑스 헌법에 따라 국민의회(National Assembly)와 상원의 의결을 거친 후 공화국 대통령에 의해 공표된다. 그러나 위와 같이 명시적으로 법률에 의해 규제토록 한 사항이 아닌 기타의 영역은 최고행정법원(국참사원, Conseil d'État)의 자문을 거친 후 정부의 명령(decree)에 의해 규제될 수 있으며, 이러한 규제권은 행정부를 감독하는 총리(Prime Minister)에게 부여된다. (Joel R. Reidenberg/Paul M. Schwartz, "*Data Protection Law and On-line Services : Regulatory Responses*", http://europa.eu.int/comm/internal_market/privacy/studies_en.htm, 1998. 12.)

146) Décision n° 94-352 DC du 18 janvier 1995.

147) 프랑스 헌법 제66조 「개인적 자유(libert individuelle)」 : (1) 누구든지 자의적으로 구금되지 아니한다. (2) 개인적 자유의 수호자인 사법부는 법률에 의해 규정된 조건에 따

로 인정한 것이다. 이에 의하면, 프라이버시 또는 개인정보에 관한 법적 보호는 1958년 헌법 제34조제(2)항에 따라 반드시 의회에 의해서 만들어진 법률의 형식으로 이루어져야 함을 의미한다. 이러한 헌법적 근거를 바탕으로 하여 제정된 법률이 바로 1978년 「정보처리축적및자유에관한 법률(Loi n° 78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés)」이다. 이로써 프랑스는 자국에서 이루어지는 개인정보처리의 공정성과 적정성의 확보를 위한 법적·제도적 기본체계를 확립하게 되었다.

가. 개인정보보호 법제현황

프랑스에서 일반 국민들의 개인정보에 관한 관심이 증대된 계기는 1974년 프랑스 정부가 모든 행정기관이 개인신원확인대장을 검색·이용토록 하겠다는 내용의 사파리(Project SAFARI en 1974(Système automatisé pour les fichiers administratifs et le répertoire des individu)) 법안을 발표하면서부터이다. 프랑스에서는 1960년대부터 산업화와 정보화의 진전, 특히 컴퓨터 등 정보처리 기술의 발달에 대응하기 위한 새로운 법질서 확립에 대한 논의가 시작되었다. 이에 프랑스 최고행정법원(국참사원, Conseil d'État)에서는 '공적·사적 자유 및 행정결정에서의 정보처리발달의 결과'라는 연구보고서를 발간하였고, 여기서 언급된 해결방안이 위 입법안에서 구체화된 것이다. 그러나 이러한 정부의 계획은 개인정보를 보호하기 위한 제도적 장치가 마련되지 않은 상태에서 행정기관이 자신들의 개인정보를 아무런 제한없이 사용할 수 있도록 하는 것은 개인정보침해와 남용의 우려가 크다는 여론에 따라 보류될 수 밖에 없었다.[148] 일명 '사파리(SAPARI) 사건'이라고 불리는 이러한 일련의 과정을 겪으면서 프랑스에서는 체계적인 개인정보보호의 필요성이 제

라 이 원칙을 집행하여야 한다.

148) 그러나 동 입법안은 1891년 이후 프랑스에서 출생한 모든 사람들에 대해 국민식별번호를 부여하는 내용을 포함하고 있어 여론의 큰 반발에 부딪혔다.

기되었고, 이는 1978년 정보처리축적및자유에관한법률의 제정으로 이어지게 되었다.

동법은 프랑스에서 이루어지는 모든 정보처리에 관한 사항을 규율하는 포괄적이고도 가장 기본적인 원칙을 확립함과 아울러, 의료정보를 비롯한 다양한 영역의 개인정보를 보호하기 위한 세부 시행규정을 포함하고 있는데, 이를 살펴보면 다음과 같다.

〔표 4-7〕 정보처리축적및자유에관한법률 및 하위법령

구분	법규
기본규정	정보처리축적및자유에관한법률 (Loi n° 78-17 du 6 janvier 1978, Loi relative à l'informatique, aux fichiers et aux libertés)
형사제재에 관한 규정	동법 제41조～제44조
	형법 제226-16조～제24조 (Code Pénal Article 226-16 á 24)
	시행령 81-1142 (Décret 81-1142 du 23 décembre 1981)
세부적용에 관한 규정	법적용에 관한 시행령 (Décret 78-774 du 17 juillet 1978)
	국가안보를 위한 개인정보처리에 관한 시행령 (Décret 79-1160 du 28 décembre 1979)
	접근권 행사시 부과금에 관한 시행령 (Décret 82-525 du 16 juin 1982)
	의료정보에 관한 시행령 (Décret 95-682)
	개인건강정보의 처리에 관한 시행령 (Décret 99-919 du 27 octobre 1999)
	부과금 계산에 관한 시행규칙 (Arrêté du 23 septembre 1980)
	공공부문에서의 법적용에 관한 행정통첩 (Circulaire du 23 mars 1993)

또한 프랑스에서는 개인정보보호기본법의 역할을 하고 있는 정보처리축적및자유에관한법률 외에도 몇 가지 개인정보 내지 프라이버시와 관련있는 법규가 시행되고 있다.

〔표 4-8〕 기타 개인정보관련 법규

구분	법규
사회보장번호(NIR)의 이용에 관한 규정	RNIPP에 관한 시행령 (Décret 82-103 du 22 janvier 1982 relatif au RNIPP)
	RNIPP의 이용에 관한 시행령 (Décret 85-420 du 3 avril 1985 relatif á l'utilisation du RNIPP)
	RNIPP의 이용허가에 관한 시행령 (Décret 91-1404 du 27 décembre 1991 autorisant l'utilisation du RNIPP)
	과세절차규정에 관한 법률(288)규정의 적용을 위한 시행령 (Décret 2000-8 du 4 janvier 2000 pris pour l'application de l'article L. 288 du livre des procédures fiscales)
비디오 감시에 관한 규정	안보에 관한 법률 중 비디오 감시에 관한 제10조 (Loi n° 95-73 du 21 janvier 1995 sur la sécurité, art. 10 sur la vidéosurveillance)
	비디오감시에 관한 시행령 (Décret 96-926 du 17 octobre 1996 sur la vidéosurveillance)
	비디오감시에 관한 행정통첩 (Circulaire du 22/10/1996 sur la vidéosurveillance)
통신자유에 관한 규정	통신자유에 관한 법률 (Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication)
	신방송법(통신자유에관한법률의 수정법) (Loi n° 2000-719 du 1er août 2000 modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication)
공공문서 접근권 관련 규정	공공문서에 관한 법률 (Loi n° 78-753 du 17 juillet 1978, portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal)
	행정과 시민의 관계로부터 발생하는 시민의 권리에 관한 법률 (Loi n° 2000-321 du 12 avril 2000, relative aux droits des citoyens dans leurs relations avec les administrations)
고용에 관한 법률 (Loi n° 92-1446 du 31 décembre 1992)	
기록물에 관한 법률(Loi n° 79-18 du 3 janvier 1979)	

나. 정보처리축적및자유에관한법률의 주요내용

(1) 연혁 및 적용범위

오늘날 프랑스의 개인정보보호기본법의 역할을 하고 있는 정보처리축적및자유에관한법률은 입법 당시에는 정부와 공공기관의 전산시스템에서 수집·저장·처리되고 있는 개인정보를 보호하는 것이 일차적인 목표였다. 따라서 국가의 개인정보 처리에 대하여 일반 국민이 가질 수 있는 사적 권리를 보장하는 것이 동 법률의 주된 과제였다. 그러나 1980년 OECD 가이드라인에 이어 1990 UN 가이드라인, 1995년 EU지침과 같은 개인정보보호를 위한 국제규범들이 공공부문과 민간부문을 구분하지 않고 모두 그 보호대상으로 규정하는 등 차츰 개인정보보호법의 규율영역을 확대하는 것이 일반화됨에 따라, 프랑스의 개인정보보호법체계도 변화되었다. 동법은 제정 이래 총 6차례의 개정[149]을 거쳐, 오늘날에는 공공·민간부문에 모두 적용될 뿐 아니라 컴퓨터로 자동처리되는 개인정보와 수기파일로 처리되는 개인정보에도 함께 적용되는 광범위한 적용범위를 가지게 되었다.

〔표 4-9〕 정보처리축적및자유에관한법률의 주요 개정내용

개정	주요내용
1988년	· 제32조 규정 삭제
1992년	· 민감한 개인정보의 보호에 관하여 규정
1994년	· 의료행위를 목적으로 하는 개인정보의 처리 허용 · 연구목적의 의료정보처리에 관한 제한
1999년	· CNIL의 권한 위임에 관하여 규정 · 치료 및 예방활동의 평가나 분석을 목적으로 하는 의료부문에서의 개인정보처리에 관한 규정(제5-2장) 신설

149) La loi n° 88-227 du 11 mars 1988, article 13 relative à la transparence financière de la vie politique ; la loi n° 92-1336 du 16 décembre 1992 ; la loi n° 94-548 du ler juillet 1994 ; la loi n° 99-641 du 27 juillet 1999 ; la loi n° 2000-321 du 12 avril 2000 ; la loi n° 2002-303 du 4 mars 2002.

2000년	· 개인정보보유기간에 대한 제한규정을 구체화 · 의료정보 및 인터넷 전자정보에 관한 규정 개정
2002년	· 의료정보에 관한 접근권

(2) 정보주체의 권리

프랑스의 개인정보보호법에 의하면, 정보주체는 ① 자신에 관한 정보 수집에 대하여 고지받을 권리(제27조), ② 수집 이전 또는 이후 정보처리에 대해 반대할 권리(제26조), ③ 자기에 관한 정보에 대하여 열람·정정·삭제를 요구할 권리(제34～제40조)를 행사할 수 있다. 만약 정보처리자가 이러한 의무를 위반한 경우에는 벌금 또는 징역형에 처해진다. 특히 프랑스 형법(Code Pénal) 제226-18조는 사기·신의성실 위반 기타 불법적인 방법으로 개인정보를 수집·처리하거나, 정보주체의 명시적인 반대의사에도 불구하고 정보를 수집·처리하는 자는 최고 5년의 징역 또는 300,000 유로의 벌금에 처해진다고 규정하고 있어, 정보주체의 반대할 권리를 실질적으로 보장하고 있다.

(3) 정보처리자의 의무

정보처리자의 첫째 의무는 바로 자동화된 정보처리를 실시함에 앞서 CNIL의 사전 절차를 거치는 것이다. 따라서 모든 정보처리자는 개인정보의 자동화 처리에 대하여 CNIL에 고지하여야 한다. 정보처리축적및자유에관한법률 제19조는 정보처리자가 CNIL에 고지하여야 할 사항을 구체적으로 밝히고 있다.[150]

150) 정보처리자가 CNIL에 고지하여야 할 일반적인 사항은 다음과 같다. ① 서류를 제출하는 자 및 정보처리를 결정할 권리가 있는 자 또는 그 자가 외국에 거주하는 경우 프랑스에 있는 그의 대리인, ② 정보처리의 특징·목적 및 필요한 경우 명칭, ③ 정보처리를 실시하는 담당부서, ④ 접근권을 행사와 관련된 업무를 담당하는 부서 및 그 권리의 행사를 용이하게 하기 위하여 취한 조치, ⑤ 직무에 비례하여 또는 업무의 필요에 따라 입력된 정보를 직접 접촉하는 자들의 범위, ⑥ 처리된 개인정보 및 개인정보의 출처와 보존기간, 개인정보를 전달받을 자격이 있는 수취인 또는 수취인의 범위, ⑦ 전항에서 정한 정보의 접근·연결 또는 동 정보에 관련된 기타

그러나 이러한 사전 절차는 공공부문과 민간부문에 있어 다소 차이가 있다. 공공부문에서 행하는 자동화된 정보처리는 법률에 의해 허가된 경우를 제외하고는 CNIL의 정당한 의견을 청취한 뒤에 실시 여부를 결정하여야 한다. 이 경우, 자동화 정보처리의 실시에 대한 위원회의 반대의견은 오직 최고행정법원(국참사원)의 합당한 의견에 따른 명령이나 이와 같은 명령에 의해 승인된 의결기관이 내린 결정에 의해서만 무시될 수 있을 뿐이다.[151] 특히 개인정보처리를 위하여 국가의 개인신원확인대장을 사용하는 경우에는 위원회의 자문을 거쳐 정한 최고행정법원(국참사원)의 명령에 의해서만 허용될 수 있다.[152] 반면, 민간부문에서는 법률에서 정한 의무사항을 이행하겠다는 내용의 약속을 포함한 신고서를 CNIL에 제출하여 접수증을 교부받는 것으로 간결하게 절차를 완료할 수 있다.[153] 다만, CNIL은 민간부문은 물론 공공부문에서도 명백하게 사생활 또는 자유권을 침해하지 않는 보편적인 개인정보처리에 대해서는 그 특징을 고려한 신고 규준을 마련하여, 해당 규준에 적합한 신고서의 제출과 접수증의 교부만으로 정보처리를 행할 수 있도록 사전절차를 간소화할 수 있다.[154]

이렇듯 정보처리축적및자유에관한법률에 의하면 정보처리자는 자동화된 개인정보의 처리에 앞서 CNIL에 고지하여야 할 의무가 있는 바, 만약 이러한 사전절차를 준수하지 않는 경우에는 고의·과실 여부에 관계없이 3년의 징역 또는 45,000 유로의 벌금에 처해지게 된다.[155]

모든 처리형태 및 제3자에의 양도, ⑧ 정보처리와 정보의 안전 및 법률에 의하여 보호를 받는 비밀보장을 위하여 취한 처분, ⑨ 정보처리가 국외에서 이미 행한 정보처리작업에 입각하여 프랑스 영토에서 부분적으로 행하는 작업의 대상이 되는 경우 등 형식여하에 관계없이 프랑스와 외국간의 개인정보 이전이 예정되어 있는지의 여부 등이다.

151) 정보처리축적및자유에관한법률 제15조.

152) 정보처리축적및자유에관한법률 제18조.

153) 정보처리축적및자유에관한법률 제16조.

154) 정보처리축적및자유에관한법률 제17조.

155) 프랑스 형법 제226-16조.

한편 정보처리자는 위에서 설명한 고지의무 외에도 적법한 방법으로 개인정보를 수집하여야 할 의무, 정보주체의 열람·정정요청을 부당한 이유없이 거부하여서는 안 될 의무를 부담한다. 또한 정보주체의 접근권 행사와 관련하여 보유하고 있는 개인정보 사본 교부시 수수료 규정을 위반해서는 안 된다. 이러한 의무를 위반한 때에는 위경죄(違警罪)[156]에 해당되어 형사처벌을 받을 수 있다.[157]

다. 프랑스의 개인정보보호기구

앞서 언급한 1974년 사파리(SAFARI) 사건을 계기로, 프랑스 정부는 '공공·준공공·민간 부문에서 이루어지는 정보처리의 발달에 대비하여 개인의 사생활과 개인적 자유 및 공적 자유를 존중하고 보장하는 방안'을 마련하여 제안하는 역할을 담당하는 위원회를 법무부 소속 하에 설치하였다. 당시 위원회의 대표자였던 버나드 쉐노(Bernard Chenot)는 6개월 동안의 수많은 자문과 논쟁을 거쳐 개인정보보호기본법의 제정 및 동법의 적용을 감독하는 임무를 맡는 독립적인 기구의 설치를 주장하였는데, 이는 1969년 최고행정법원(국참사원, Conseil d'État)에서 수행한 연구를 구체화한 것이었다. 이 보고서를 기초로 하여 제정된 법률이 바로 1978년 정보처리축적및자유에관한법률이며, 동법 제6조를 근거로 하여 정보자유위원회(CNIL : Commission nationale de l'informatique et des libertés)가 설립되었다. 프랑스의 정보자유위원회는 프랑스 내에서 이루어지는 모든 개인정보 처리행위를 규율함으로써, 부당한 개인정보의 처

156) 프랑스 형법 제111-1조는 범죄에 대하여 선고될 형벌의 경중에 따라 범죄를 위경죄(contravention), 경죄(délit), 중죄(crime)의 세 가지로 분류하고 있다. 위경죄는 범죄의 법정형이 원칙으로 20,000프랑 이하의 벌금에 해당하는 범죄를 말하고(동법 제131-12조), 경죄는 구금형 및 이에 상당하는 벌금형 또는 원칙으로 25,000프랑 이상의 벌금형에 해당하는 범죄를 말하며(동법 제131-3조), 중죄란 유기 또는 무기의 금고형에 해당하는 중한 범죄를 말한다(동법 제131-1조). (조상제, "프랑스의 형사사법제도 - 형사법원의 구조와 검찰제도를 중심으로 - ", 비교형사법연구 제3권제1호, 한국비교형사법학회, 2001. 7. http://www.ajou.ac.kr/~ajlaw/sjcho.htm)

157) Décret 81-1142(1981. 12. 23).

리로 국민들의 개인정보가 침해되는 것을 방지하기 위해 설립된 프랑스의 대표적인 개인정보보호기구이다.

(1) CNIL의 지위 및 특징

정보자유위원회는 정보처리와 개인의 자유 즉, 기본권을 조화시키는 것을 목적으로 설립된 기관이다. 따라서 정보자유위원회는 법에 의해 보장된 권한을 보다 실질적으로 행사하여 부당한 개인정보침해로부터 개인의 자유와 기본권을 보호할 수 있도록 독립성과 전문성을 확보하기 위해 합의제 독립행정기관으로 설립되었다. 이러한 CNIL의 주요 특징을 살펴보면 다음과 같다.

첫째, 정보자유위원회는 17명의 위원으로 구성된 복수집단으로 합의제 기관이다. 특히 위원회를 구성하는 각각의 위원들은 그 자격이나 직위면에서 볼 때 프랑스의 입법·사법·행정부를 대표하는 자로 이루어져 있어 강력한 권한과 위상을 가지고 있다. 정보처리축적및자유에관한법률 제8조는 이러한 위원회의 구성방법에 대해 구체적으로 밝히고 위원회를 구성하는 17인의 위원들의 소속이나 임명(추천)권자, 임기, 위원수에 대해서 명시적으로 규정하고 있는 바, 이를 살펴보면 다음과 같다.

［표 4-10］ CNIL의 위원구성 규정

소속		직위	임명방법	인원
입법부	상원(le Sénat)	상원의원	상원에서 선출	2명
	국민의회(l'Assemblée nationale)	하원의원	국민의회에서 선출	2명
	경제사회위원회 (Conseil économique et social)	위원	국민의회에서 선출	2명
사법부	국참사원(최고행정법원) (Conseil d'État)	전·현직 법관	전원합의부에서 선출	2명
	파기원(대법원) (la Cour de cassation)	전·현직 법관	전원합의부에서 선출	2명
	심계원(회계원) (la Cour des comptes)	전·현직 구성원	전원합의부에서 선출	2명

기타(행정부 포함)	정보처리 전문가	상원의장과 국민의회의장이 각각 1명씩 추천	2명
	기타 전문가	각의(conseil des ministres)에서 지명	3명

현재 위원회는 1인의 위원장과 2인의 부위원장 및 기타 위원으로 구성·운영되고 있다. 한편 위원회를 구성하는 위원 외에도 정부로부터 파견된 2명의 위원이 활동하나, 합의제 위원회에 참석하여 활동하는 위원은 아니다. 또한 위원회는 필요한 경우 관할 행정법원에 법관의 파견을 요청하여 조사·심사과정에서 활용할 수 있다. 2003년 현재 CNIL의 위원구성현황을 살펴보면 다음과 같다.

〔표 4-11〕 CNIL의 위원구성 현황

직위	소속기관	
위원장	국참사원(Conseil d'État)의 명예부장	1명
대표부위원장	경제사회위원회(Conseil économique et social) 위원	1명
부위원장	Nord의 상원의원	1명
위원	NTIC(MCA Communication)의 설립·자문위원	1명
	국참사원 전직 법관(명예위원)	2명
	국참사원 현직 법관	1명
	Nord의 하원의원	1명
	Val-d'Oise의 하원의원	1명
	Ille et Vilaine의 상원의원	1명
	파기원의 전직 법관(수석명예위원, 명예위원)	2명
	회계검사원의 전임위원	3명
	Laser 총무부장 겸 Galeries Lafayette 이사회 공동대표	1명
	경제사회위원회 부대표	1명
기타	정부파견인사	2명

※ 주 : 2003. 6. 17일자 위원구성현황임(www.cnil.fr)

둘째, CNIL은 독립기관이다. 이는 위원회를 구성하는 위원 중 3분의 2 가량이 의회나 법원에 의해 선출된다는 것을 통해서도 확인할 수 있는 바이다. 특히 법률은 각각의 위원들의 독립적인 지위를 보장하기 위해 자신을 임명한 자 또는 소속기관의 지시·감독을 받지 않고 자유롭게 활동할 수 있도록 명시적으로 규정하고 있다.[158] 또한 정부의 장관이나 공공기관, 공기업, 사기업의 경영자 등은 여하한 이유로도 위원회의 활동을 방해할 수 없도록 규정[159]함으로써, 위원회의 독립성을 더욱 강화하고 있다. 따라서 위원회는 임무수행에 대해서도 대통령과 의회에 대해 직접 보고하며 직원의 임명도 위원장이 자유롭게 행한다.

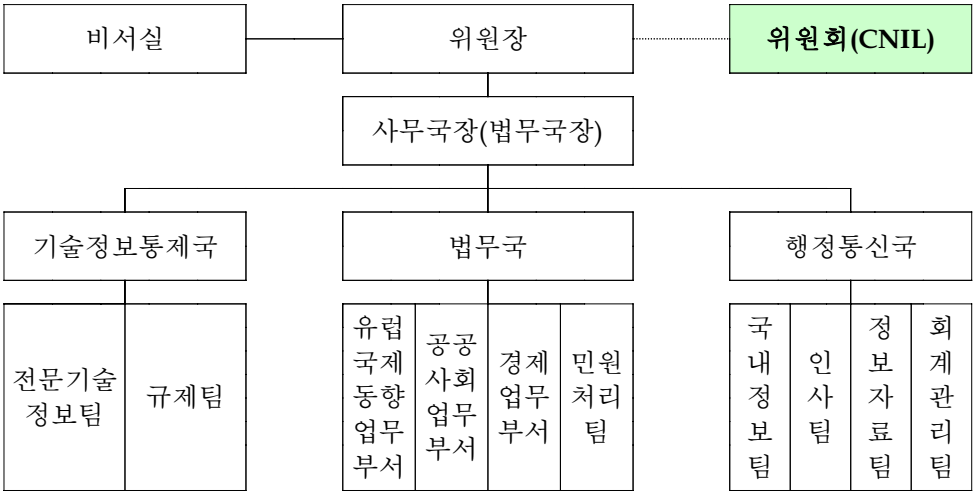
셋째, 위원회는 행정기관의 성격을 가진다. 따라서 위원회의 예산은 국가예산으로 편성되며, CNIL의 직원도 계약직 공무원이다. 또한 위원회가 내리는 결정은 최고행정법원(국참사원)의 상소대상이 될 수 있다.

(2) CNIL의 조직구성

정보자유위원회는 합의제기구이기 때문에, 위원회 회의개최를 포함한 각종 활동을 지원하는 사무국을 두고 있다. 따라서 CNIL은 위원장을 중심으로 사무국장과 3국 10개 부서로 구성되어 있으며, 현재 약 200여명의 직원이 활동하고 있다. CNIL의 조직도를 살펴보면 아래와 같다.

158) 정보처리축적및자유에관한법률 제13조제1항 : 「위원회의 위원은 그의 권한 행사에 있어 어떠한 기관의 지시도 받지 아니한다」

159) 정보처리축적및자유에관한법률 제21조 : 「관계 장관, 행정기관, 공사기업의 경영자, 각종 단체의 책임자 및 일반적으로 개인정보화일의 소지자 또는 이용자는 여하한 이유로도 위원회 또는 위원의 활동을 방해할 수 없고, 그 임무수행을 용이하게 하기 위하여 필요한 모든 조치를 취하여야 한다」



(그림 4-3) 프랑스 CNIL의 조직도

CNIL은 조직규모도 상당히 큰 편이어서 세부 영역별로 업무분장이 잘 이루어져 있다. CNIL의 각 부서에서 행하는 구체적인 업무를 살펴보면 다음과 같다.

〔표 4-12〕 CNIL의 조직체계 및 부서별 역할

상위부서	하위부서	주요업무
법무국	유럽・국제동향 업무부서	・유럽 등 국제관계업무 ・유럽 등 국제협력 ・국제입법동향 연구
	공공사회 업무부서	・재정, 지방자치, 통계업무 ・司法, 경찰, 간접적 접근권 행사, 공적 자유에 관한 업무 ・보건, 의료보험, 의료연구에 관한 업무 ・사회・노동・교육에 관한 업무
	경제업무부서	・은행, 신용, 금융, 보험관련 업무 ・네트워크, 통신, 인터넷경제관련 업무 ・자본, 마케팅, 기업관련 업무
	민원처리팀	・단체파트 : 정책, 인터넷, 은행, 중앙정보축적 관련 민원처리 ・노동파트 : 사회, 사회보장, 보건, 교육, 재정 관련 민원처리 ・시장파트 : 상사분쟁, 보험, 통신관련 민원처리

기술정보 통제국	전문기술정보팀	· 기술감정 : 권고요구 및 사전절차 실시 · 기술연구
	규제(감독)팀	· 정보처리자에 대한 규제임무 · 유럽경찰에 대한 협력업무
행정통신국	국내정보팀	· 네트워크, 전화, 정보광장운영 및 기술지원 · 문서의 전자화 관리, 문서보관 · 사전절차를 거친 정보의 이용에 관한 업무
	인사팀	· 행정관리 및 인사 등
	정보자료팀	· 법률자료관리 · 인터넷 사이트, 인트라넷 등 관리 · 자료실 및 일반정보 관리
	회계관리팀	· 예산, 경영관리, 회계 · 급여 및 기타 보상 · 총무, 주차장 관리

(3) CNIL의 주요기능

정보자유위원회는 공공·민간부문의 개인정보처리 등록 및 법규 준수 여부를 감독하는 독립 법정규제기구로서, 부당한 정보처리의 위협으로부터 개인의 사생활과 개인적·공적 자유를 보호하여야 할 주된 임무를 지니고 있다. 위원회에 부여된 주요 임무 및 기능을 살펴보면 다음과 같다.

첫째는 정보처리 내지 정보의 축적에 관하여 확인하고 조사하는 역할이다. 위원회는 프랑스 안에서 이루어지는 모든 정보처리 및 축적에 대하여 등록 또는 신고접수를 통해 그 현황을 파악하고 이를 바탕으로 정보처리과정을 규제하고 있다.[160] 등록 내지 신고를 통해 확인된 정보처리의 내용은 색인화 작업을 통해 정보처리등록부(fichier des fichiers)의 형태로 보관되며, 이렇게 만들어진 색인목록은 일반 시민들이 정해진 절차에 따라 언제든지 이용할 수 있도록 보장된다.[161]

160) 정보처리축적및자유에관한법률 제14조 : 「위원회는 개인정보의 공적·사적 자동화 정보처리가 이 법률의 규정에 따라 실시되는지 여부를 감독한다」

161) 정보처리축적및자유에관한법률 제22조에 의하면, 위원회는 ① 정보처리 목록의 설치를 정하는 법률이나 규칙 또는 신고일자, ② 정보처리목록의 명칭 및 목적, ③ 일반인의 자신의 정보에 대한 접근권 행사를 지원하는 부서, ④ 입력된 개인정보의 범위 및 동 정보를 전달받을 자격이 있는 수취인 또는 수취인이 범위를 명시한 정보처리목록을 일반대중이 자유로이 이용하게 하여야 한다.

둘째, 위원회는 정보처리자가 개인정보보호법규에 적합하게 개인정보를 처리하고 있는지 그 준수여부를 감독할 권한과 의무를 가진다. 정보처리 축적및자유에관한법률 제21조는 이러한 규제·감독기능의 수행을 위해 위원회가 행사할 수 있는 권한을 규정하고 있다. 이에 의하면 위원회는 ① 일반적으로 적용되는 법규적 성격을 가지는 결정을 내릴 수 있고, ② 위원 또는 직원이 직접 정보처리의 법규준수여부를 조사하고 필요한 정보와 자료를 제출받을 수 있도록 위임할 수 있으며, ③ 정보시스템의 안전을 위한 명령 내지 지침을 내릴 수 있고, ④ 형사범죄에 관해서는 관계기관에 고발조치 할 수 있으며, ⑤ 위원회의 의결에 따른 결과가 어떻게 처리되고 있는지를 확인할 수 있다.

셋째, 위원회는 정보처리에 관한 기준과 규범을 제시하는 규칙을 제정할 권한을 가진다.[162] 이러한 위원회의 규칙제정권은 보편적인 정보처리 또는 자유권을 해할 위험이 상대적으로 적은 정보처리를 위한 간소화된 절차와 기준을 마련하는 것에 있어 특히 유용하다.

넷째, 위원회는 정보주체의 접근권 및 정정요구권이 침해되지 않도록 보다 적극적인 역할을 담당하고 있다. 즉, 위원회는 정보처리의 신고 내지 등록접수를 받을 때 정보주체의 권리행사방법을 밝히도록 하여, 이러한 방법이 실질적으로 정보주체의 권리를 보장해주고 있는 것인지를 심사·감독한다. 또한 더 나아가 간접적인 접근권을 위원회가 직접 행사하는데, 특히 국가안보·방위·공공의 안전과 관련되어 축적된 정보 또는 공공기록에 대해 시민을 대신하여 접근권을 행사할 수 있다.[163]

다섯째, 위원회는 소송에 앞서 전문적이고 포괄적인 피해구제의 역할을 담당하고 있다. 즉, 위원회는 각종 고소사항이나 이의제기사항을 접수하고 예비적으로 심사하여, 해당 사건에 대해 기각결정 또는 경고조치결정, 제소결정 등의 조치를 취할 수 있다. 그러나 위원회는 경고 또는 형

---

162) 정보처리축적및자유에관한법률 제17조 :「명백하게 사생활 또는 자유를 침해하지 아니할 공적·사적 영역의 정보처리에 대한 가장 보편적인 범위를 정하기 위하여, 위원회는 제19조에서 정한 특징에 따라 간소화된 규준을 정하여 공포한다」

163) 정보처리축적및자유에관한법률 제21조제1항제5호 및 제39조.

사기관 고발이나 제소 등의 규제적인 조치뿐 아니라 당사자간 개인정보 침해 내지 정보처리의 부당함으로 인해 발생한 분쟁이 원만히 해결될 수 있도록 적극적인 조정자의 역할을 하고 있다.[164]

여섯째, 위원회는 상담, 자문, 검토, 제안 등을 통한 정보제공의 역할을 하고 있다. 위원회는 정보주체와 정보처리자에게는 각각의 권리·의무에 대해 알려주고 상담을 행하며, 정부에 대해서는 기술발달로 인한 자유권이나 프라이버시침해를 방지하기 위한 입법이나 규제조치를 제안할 수 있다. 특히 개인정보와 관련된 법률을 제정할 때에는 의회 통과 전에 반드시 위원회가 자문을 행하여야 한다. 또한 위원회는 소극적인 정보제공 역할에 그치는 것이 아니라 적극적으로 정보처리와 관련된 업체나 공공기관을 직접 점검·검토할 수 있는데, 관계 당사자는 위원회가 이러한 임무를 수행하기 위해 필요한 모든 조치를 취하고 협조하여야 한다.[165]

〔표 4-13〕 CNIL의 주요기능

구분	주요기능
정보처리 등록·신고	· 정보처리에 대해 의견제시 및 신고접수 · 정보등록부 관리 및 공개
법규준수 조사·감독	· 자료제출요구 및 직권조사 · 법위반자에 대한 경고조치 및 형사고발
각종 규칙(지침) 제정	· 보편적인 정보처리에 대한 규준 제정
접근권·정정권 보장	· 정보주체의 권리행사방법의 용이성 확보 · 공공기록에 대한 간접적 접근권 행사
고충처리 및 피해구제	· 각종 이의제기·신고·신청사항 등 민원처리 · 사전 사실조사 실시 및 당사자 합의유도 · 경고, 제소, 기각 등의 결정
자문·상담 등 정보제공	· 당사자의 권리·의무에 대한 정보제공 · 의회에 연차보고서 제출 · 정부에 대하여 정책자문 및 입법절차 참여

164) 정보처리축적및자유에관한법률 제21조제1항제6호.

165) 정보처리축적및자유에관한법률 제6조 및 제21조 ; 동법시행령 제78-774조 제1조제5항 및 제20조제3항.

라. 개인정보피해구제 절차 및 방법

정보처리축적및자유에관한법률의 개정으로 인해, CNIL은 개인정보처리행위의 법규 준수여부에 대하여 조사하여 법위반 단체에 대하여 경고 등의 제재조치를 취할 수 있는 등 그 권한이 증대되고 있다. 이러한 CNIL의 권한 증대는 동 기관이 행하는 각종 개인정보피해구제의 실효성을 높이는 중요한 원동력이 되고 있다.

CNIL은 정보처리축적및자유에관한법률 기타 개인정보 관련법규에 따라 개인정보침해사건이나 불만사항을 접수받아 처리함으로써, 부당한 개인정보침해를 입은 자를 보호하고 그 피해를 구제해주는 역할을 하고 있다. 특히 CNIL은 별도의 민원처리 부서를 두고 각종 개인정보침해상담을 접수받아 사건을 처리하고 있다. CNIL에 접수된 사건은 자료제출요구 등을 통해 사실조사를 거치며, 법위반이 발견된 경우 CNIL은 해당 사업자 등 정보처리자에게 시정을 권고하고 동일한 법위반 행위를 하지 않도록 경고한다. 물론 더 심각한 법위반행위가 있을 경우에는 형사고발이나 제소 등의 조치를 취할 수도 있다.[166]

이와 같이 CNIL은 개인정보침해나 법규위반 또는 정보주체의 권리행사에 관한 각종 상담을 행하고 이의제기 신청을 접수받아 사건처리를 행하는 등 개인정보피해구제의 역할을 하고 있다. 특히 CNIL은 위법한 행위를 한 개인정보처리자에 대하여 제재조치를 취하는 것으로 그치지 않고, 실제로 개인정보침해로 인해 피해를 입은 자가 만족할 수 있는 결과를 얻을 수 있도록 다양한 방법으로 지원하고 있다. 즉, CNIL은 개인정보처리자 등록부를 공개하여 일반 시민들이 자신의 개인정보가 어떻게 다루어지고 있는지 확인할 수 있도록 하고 있으며, 경찰이나 국가안보와 관련된 기구 등에서 보유하고 있는 개인정보에 대하여 필요한 경우 정보주체의 개인정보 열람청구를 대신하여 주기도 한다. 또한 상업적 파일에서

166) CNIL은 작년 한해 52차례 사기업에 대한 현장조사를 실시하여 이 중 2곳을 법위반으로 제소하였다고 한다. (EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/france.htm 참조)

개인정보 목록을 삭제해달라는 요청을 접수받아 삭제요청을 대신하여 주기도 한다.

1978년 이래 CNIL은 12,600여건의 상담접수를 받았으며 41,270건의 이의제기신청을 접수받아 처리하였다. 2002년에는 2001년에 비해 38% 증가한 총 7,909건의 민원을 접수받아 처리하였다고 한다. CNIL의 이러한 최근 피해구제 현황을 살펴보면 다음과 같다.

〔표 4-14〕 CNIL의 피해구제 현황

연도 / 유형	2001	2002	증감
이의제기신청	3,754	5,076	△ 42%
상담	973	1,126	△ 16%
접근권 행사요청	836	1,264	△ 51%
등록부 열람신청	252	333	△ 32%
상업파일 삭제요청	94	110	△ 17%
계	5,729	7,909	△ 38%

※ 참고 : EPIC & PI, *"Privacy and Human Rights 2003 - An International Survey of Privacy Laws and Developments"*, http://www.privacyinternational.org/survey/phr2003/countries/france.htm

3. 독일

독일은 유럽 내에서도 가장 엄격한 정보보호법을 가지고 있는 국가 중 하나이다. 세계 최초의 정보보호법이 1970년 독일 헤센(Hessen)州에서 제정된 것을 보더라도, 독일인들의 개인정보보호에 대한 관심을 짐작할 수 있다. 독일에서는 1960년대 후반부터 정보전자화의 급속한 진행에 따른 개인정보침해 위험에 대비하여 개인정보보호 입법안을 마련하여야 한다는 학계의 주장이 대두되었고, 이러한 개인정보보호의 필요성에 대한 자각과 인식은 헤센 주의 정보보호법을 시작으로 각 주와 연방차원에서 개인정보보호법의 제정으로 이어지게 되었다. 이하에서는 독일 연방을 중심으로 개인정보보호 법제현황과 개인정보보호기구에 대해 살펴보도록 하겠다.

가. 개인정보보호 법제현황

개인정보보호제도의 헌법적 근거로는 바로 독일기본법(Grundgesetz) 제1조 인간존엄성 조항과 제2조 인격의 자유로운 발현조항을 들 수 있을 것이다.[167] 물론 독일 기본법상 프라이버시권에 관한 명시적인 규정은 없으나, 기본법 제1조와 제2조를 프라이버시권에 대한 일차적인 근거조항으로 보기에 무리가 없다.[168] 독일 헌법재판소 역시 1983년 헌법소원 판결을 통해 '명확한 공공의 이익에 의해서만 제한받을 수 있는 정보자기결정권'을 선언하였는데, 특히 이러한 정보자기결정권은 인격권(Persönlichkeitsrecht)의 불가침성을 규정한 기본법 제1조제1항과 제2조제1항에서 직접적으로 파생되는 권리임을 명확히 하였다.[169] 이 외에도 기본법 제10조는 서신, 우편, 통신 등의 비밀과 프라이버시가 보호되어야 할 대상임을 밝히고, 이에 대한 제한은 반드시 법률로서 하여야 한다고 규정하고 있다.[170]

---

167) 독일 기본법 제1조(인간존엄의 보호) : 「① 인간의 존엄은 불가침이다. 이를 존중하고 보호하는 것은 모든 국가권력의 의무이다. ② 독일 국민은 불가침·불가양의 인권을 세계의 모든 인간 공동체, 평화 그리고 정의의 기초로서 인정한다. ③ 기본권은 직접효력을 갖는 권리로서 입법권, 집행권, 사법권을 구속한다」, 독일 기본법 제2조(일반적 인격권) : 「① 누구든지 타인의 권리를 침해하지 아니하고 헌법질서나 도덕률에 위반하지 않는 한, 자신의 인격을 자유로이 발현할 권리를 가진다. ② 누구든지 생명권과 신체를 훼손당하지 않을 권리를 가진다. 신체의 자유는 불가침이다. 이 권리들은 법률에 근거해서만 침해될 수 있다」

168) 독일 통일 이후 기본법 개정작업 과정에서, 정보보호권(Right to data protection)을 기본법에 포함하고자 하는 논의가 있기는 하였으나 독일 보수당의 반대로 그러한 권리가 기본법에 반영되지는 못하였다.

169) 독일 연방정부는 1982년 인구조사법에 근거하여 대대적인 인구조사를 실시하였는데, 인구조사를 하면서 개인의 수입 등 재정상태, 직업, 가족관계 등 지나치게 자세하고 많은 정보를 수집한다는 비판을 받게 되었다. 이에 많은 사람들은 자신의 개인정보가 다른 곳에 이용되거나 잘못 악용될 것을 염려하여 헌법재판소에 헌법소원을 제기하였다. (BVerfGE 65, 1)

170) 독일 기본법 제10조 : 「① 서신, 우편, 전기통신의 프라이버시는 침해되어서는 안된다. ② 이러한 프라이버시의 제한은 오직 법률에 의해서만 가능하다. 프라이버시의 제한이 독일연방국가의 자유로운 민주적 기본질서 및 실존과 안보를 보호하기 위한 것인 경우에는 그러한 프라이버시의 제한에 대하여 당해 주체에게 고지할 필요가 없음을 법률로 규정할 수 있으며, 법원으로의 소제기는 의회에서 임명된 기구 또는 그 보조기구에 의한 사건 심사로 대체할 수 있음을 법률로 규정할 수 있다」

이러한 헌법상의 근거를 바탕으로 독일 시민들의 개인정보를 보호하기 위한 기본법이 1977년 연방차원에서 제정되었는데, 「연방정보보호법(BDSG : Bundesdatenschutzgesetz)」이 바로 그것이다.[171] 동법은 1990년에 새롭게 전면 개편(BGB1.I 1990 S.2954)된 이래, 1994년과 1997년, 2001년, 2002년에 개정된 바 있다. 특히 2002년 개정은 EU 개인정보보호 지침의 내용을 반영하기 위한 것이다.

이러한 연방정보보호법 외에도 독일은 연방 차원에서 개인정보 관련 개별법을 제정하여 시행하고 있다. 대표적인 것이 정보통신 분야에서의 정보보호에 관하여 규율하고 있는 1997년 「정보통신서비스정보보호법(TDDSG : Teledienstdatenschutzgesetz)」(이하 '정보통신법'이라 한다) [172]으로, 동법은 연방정보보호법에 우선하여 적용된다. 특히 동법은 전자서비스 이용관계에서의 개인정보 이용에 대하여 규율하기 때문에, 인터넷 포탈사이트, 이메일 서비스제공자, 게임서비스제공자 등의 통신서비스제공자에 대해 직접 적용된다. 이 외에도 「우편법(Postgesetz)」, 「사회보장법(Sozialgesetzbuch)」, 「조세법(Abgabenordnung)」, 「소득세법(Einkommensteurgesetz)」 등의 법률에 개인정보관련 규정이 포함되어 있다.

나. 연방정보보호법의 주요내용

연방정보보호법은 개인정보의 정의에서부터 정보주체의 권리와 정보처리자의 각종 의무, 제3국으로의 정보이전, 비디오감시, 익명성과 가명성,

171) 연방 차원의 개인정보보호법인 동법이 제정되기 이전에는 주 차원에서 1970년 헤센주의 「정보보호법」과 라인란트팔츠(Rheinland-Pfalz) 주의 「정보남용금지법」이 제정된 바 있다.

172) 동법은 EU 지침(2000/31/EC)의 이행을 위해 전자상거래와 관련하여 새롭게 제정된 법률, 즉 정보통신서비스법 또는 멀티미디어법이라 불리는 「정보·통신서비스에관한기본조건의규율에관한법률(Gesetz zur Regelung der Rahmen- bedingungen fűr Information-und Kommunikationsdienste)」의 제2편으로 편입되었다. 「정보·통신서비스에관한기본조건의규율에관한법률」에는 이 외에도 제1편 「전자통신서비스법(Teledienstegesetz: TDG)」과 「전자서명법(Signaturegesetz: SigG)」이 개인정보보호와 관련하여 중요한 역할을 하고 있다.

스마트 카드, 민감한 정보의 수집 등에 대한 내용을 포함하고 있다. 동법의 주요내용을 살펴보면 다음과 같다.

(1) 적용범위

연방정보보호법은 독일 연방차원의 개인정보보호법으로서 원칙적으로 독일 전역에서 이루어지는 모든 개인정보의 수집・이용・처리에 대하여 적용된다. 따라서 연방과 주의 공공기관과 민간단체의 개인정보 처리행위에 대하여 동법이 적용된다. 이 중 민간단체에 대해서는 당해 단체가 상업적 또는 업무상의 목적으로 개인정보를 처리하고 이용하는 경우에 한하여 적용된다. 또한 공공기관에 대해서도 각 주에서 적용되는 개인정보보호법이 있는 경우에는 연방법의 적용이 배제되며, 영역별로 다른 개인정보 관련법률이나 규정이 있는 경우에도 동법은 적용되지 않는다.

연방정보보호법이 적용되는 개인정보의 범위는 특정되거나 또는 특정 가능한 '자연인'의 인적・물적 관계에 관한 일체의 정보를 의미한다.[173] 따라서 법인에 관한 정보는 동법의 적용을 받지 않는다. 또한 동법은 자동화된 정보처리시스템을 통한 개인정보의 수집・이용・처리 뿐 아니라 비자동화된 정보파일의 처리에 대해서도 적용된다. 여기서 비자동화된 정보파일이란 구체적 특성에 따라 유사하게 조직되어 있어서 이를 근거로 정보에 접근할 수 있고 평가할 수 있는 일련의 개인정보를 의미한다.[174]

(2) 정보주체의 권리

연방정보보호법은 제2장에서 '정보주체의 권리'라는 제목 하에, 정보주체의 접근권(제19조, 제34조), 통지받을 권리(제19a조), 정정・삭제・차단 요구권(제20조, 제35조), 이의제기를 할 권리(제20조제5항)에 대해 규정하고 있다. 특히 독일 연방정보보호법은 제6조에서 정보주체의 이러한 권

173) 연방정보보호법 제3조제1항.

174) 연방정보보호법 제3조제2항.

리는 계약 등 다른 법률행위에 의해 배제되거나 제한될 수 없는 불가침의 권리임을 명백히 밝히고 있다는 점에서 특색이 있다.

(3) 정보처리자의 의무

연방정보보호법은 동법의 적용을 받는 개인정보처리자가 준수하여야 할 의무사항에 대하여 규정하고 있는 바, 개인정보처리자의 주된 의무는 다음과 같다.

첫째, 연방정보보호법 제4d조제1항에 의하면 개인정보처리자는 연방정보보호청에 개인정보 처리행위와 관련된 소정의 사항을 고지하고 등록할 의무를 부담한다. 즉, 소관 커미셔너청의 사적 책임자, 연방정부의 공적 책임자, 우편 및 통신회사는 자동화된 개인정보 처리절차를 실행하기 전에 반드시 연방정보보호청에 신고하여 등록하여야 한다. 개인정보처리자가 신고하여야 할 내용은 다음과 같다.

- o 개인정보처리자의 이름 또는 단체명
- o 해당 단체의 소유자, 이사회, 이사 또는 기타 합법적으로 임명된 관리자, 정보처리에 관한 사항을 위임받은 자
- o 개인정보처리자의 주소
- o 정보처리의 수집・처리・이용목적
- o 관계되는 정보주체, 관련 정보 및 정보의 범주에 대한 설명
- o 정보를 제공받는 수신인 또는 그 범주
- o 정보 파기를 위한 기간
- o 제3국으로의 정보 전송 계획
- o 제9조에 따라 정보처리의 안전 보장을 위한 조치가 적절한지 여부를 판단할 수 있는 일반적인 설명

그러나 이러한 등록의무는 해당 개인정보처리자가 내부적으로 개인정보관리책임자(Data protection officer)[175]를 임명하였을 경우에는 면제된다.[176]

사실상 정보보호법 제4f조에 의하면, 자동화된 개인정보파일을 처리하는 모든 공공·민간기관 또는 비자동화된 개인정보파일을 처리하는 곳이라도 개인정보처리를 위해 최소 20명 이상의 인원이 고용되는 단체에서는 내부 개인정보관리책임자를 임명하여야 하기 때문에, 상당수의 정보처리자가 이러한 등록의무에서 면제된다고 볼 수 있을 것이다. 다만, 이 경우에도 제한이 있는데 정보처리자가 영리목적으로 정보를 전송하기 위해 또는 익명화된 정보전송을 위해 개인정보를 저장하고 있는 경우에는 등록의무 면제사유에 해당되지 않는다.[177]

다. 독일의 개인정보보호기구

연방국가인 독일은 현재 연방 차원의 개인정보보호법인 연방정보보호법 외에도 주 차원에서 각각 개인정보보호법이 마련되어 있고, 이를 바탕으로 개인정보보호기구들이 설치되어 활동 중이다.[178] 따라서 연방에서는 연방정보보호청(BfD : Bundesbeauftragter für den Datenshutz)이 주로 연방공공기관을 중심으로 규율하고 있으며, 현재 16개 주의 개인정보보호기구는 주 공공기관의 정보처리에 대해 규율하고 있다. 또한 독일에서는 일부 영역을 제외한 대부분의 민간부문에 대해서는 민간 감독기구를

175) 내부 개인정보관리책임자라 하면 연방이나 주의 각 행정청 혹은 연방정보보호법이나 주법의 적용대상이 되는 민간기업체에서 내부적으로 개인정보가 올바르고 공정하게 처리되고 있는지를 관리하고 조사·심사하는 자를 의미한다. 이러한 내부 개인정보관리책임자는 필요한 경우 자동화된 개인정보의 처리가 정보주체의 권리와 자유에 특별한 위험을 가져올 것으로 의심될 때에는 사전검사(Prior checking)를 할 수 있으며, 그 결과 개인정보 처리에 문제가 있다고 판단될 때에는 관계 감독청에 신고할 수 있다. 개인정보관리책임자는 이로 인해 고용관계에 있어서 불이익을 받지 않도록 보호받고 있다.

176) 연방정보보호법 제4d조제2항. 이 외에도 동조 제3항에서는 추가적인 등록의무 면제사유를 규정하고 있다.

177) 연방정보보호법 제4d조제4항.

178) 독일의 16개 모든 주에서는 공공부문에서의 개인정보보호를 위한 주 차원의 법체계를 가지고 있다. 또한 현재 작센(Sachsen) 주와 브레멘(Bremen) 주를 제외한 모든 주가 EU 지침에 적합한 새로운 법체계를 도입하고 있다.(http://europa.eu.int/comm/internal_market/privacy/law/implementation_en.htm#germany 참조)

각 주마다 설치하여 사적 영역의 개인정보 처리에 대해 관리·감독케 하고 있다.[179] 그러나 베를린(Berlin), 브레멘(Bremen), 함브르크(Hamburg), 남부작센(Lower Saxony), 쉴러비그-홀슈타인(Schlerwig-Holstein)과 같은 주에서는 주 개인정보보호기구가 민간부문에 대해서도 함께 규율하고 있다. 여기서는 독일의 대표적인 개인정보보호기구인 연방정보보호청을 중심으로 살펴보도록 하겠다.

(1) 연방정보보호청의 지위 및 특징

연방정보보호청은 1977년 연방정보보호법에 따라 설립된 법정기구로, 연방정보보호법과 전자통신법을 관장하고 있다. 연방정보보호청의 기관장은 연방정부의 제청에 따라 연방의회(하원)에서 과반수 이상의 동의를 얻어 선출되며, 선출된 자는 연방 대통령이 임명한다. 연방정보보호청의 장은 선출 당시 35세 이상이어야 하며 임기는 5년이고 1회에 한하여 재임할 수 있다. 동 기관은 행정조직상으로는 연방 내무부 소속으로 예산이나 인력지원과 같은 행정적 사안에 대해서는 연방 내무부장관으로부터 지원을 받으나, 직무수행에 있어서는 법률에 따라 독자적으로 활동할 수 있도록 보장받고 있다.

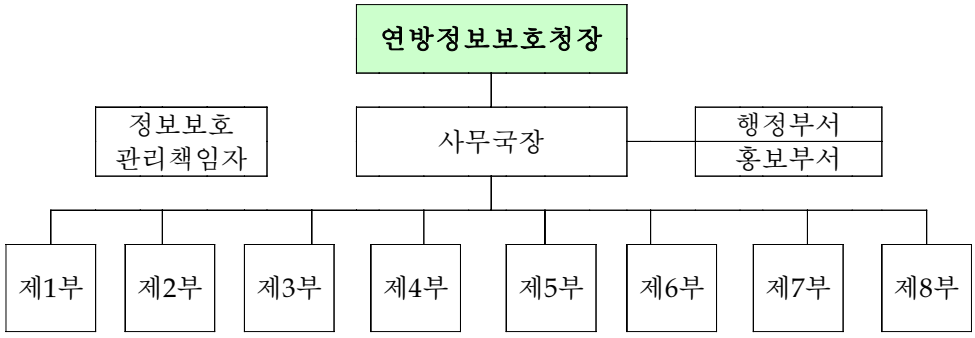
연방정보보호청은 개인정보의 수집, 처리, 사용과 관련하여 연방정보보호법이 적용되는 범위 내에서 활동하나, 주의 개인정보보호기구와 각 주

179) 민간 개인정보보호기구는 사적 영역의 개인정보처리단체의 개인정보보호법규 준수여부를 감독하는 행정기구로, 주 정부 또는 주 정부로부터 허가받은 기관은 본 법의 적용범위 내에서 정보보호의 이행을 감시할 민간 개인정보보호기구를 지정하여야 한다. 동 기구는 법규위반에 대한 충분한 가능성이 있다고 판단되는 경우 및 정보주체가 개인정보 침해에 대해 확인해 줄 것을 요청하며 증거자료를 제출한 때 개인정보침해여부에 대한 실태조사를 할 수 있으며, 필요한 경우 관할 내에 포함되는 단체 및 그 책임자에게 필요한 정보를 요청할 수 있다. 또한 동 기구는 기술적·관리적 측면에서 부적합한 행위에 대하여 시정할 것을 지시할 수 으며, 구체적인 프라이버시 침해, 특히 벌금 부과 등의 조치에도 불구하고 적절한 기간 내에 시정하지 않고 있는 경우에는 정보처리와 관련하여 특정절차의 사용을 금지할 수 있다. 특히 감독기관은 전문지식을 갖추지 못하였고 직무 수행에 필요한 신뢰성도 입증되지 않은 정보보호담당자의 해고를 요청할 수도 있으며, 사업자의 실행규약에 대하여 정보보호 법규에 부합되는지를 심사할 수 있다.

에서 설립한 민간 정보보호감독기구의 업무범위를 제외한 범위에서 활동한다. 따라서 실질적으로는 연방정부와 공공기관, 연방정부 산하단체, 연방법원, 여러 주에 걸쳐 사업하는 우편이나 통신사업자 등에 대해서만 관할하는 것으로 볼 수 있다. 그러나 최근에는 사회정보의 보호와 관련해서도 연방정보보호청이 개입하고 있고 환자, 사고, 연금보험, 실직보험과 관련된 정보영역에 대해서도 관할하는 등 점차 그 업무범위가 확장되고 있다. 즉, 독일에서는 연방과 주의 업무영역이 구분되어 각자 독립적으로 활동하고 있으며, 특히 연방정보보호법은 공공과 민간부문 모두에 적용되는 기본법이나 개인정보보호기구는 공공부문과 민간부문이 분리되어 설치·운영되고 있다는 점에서 다른 유럽 국가들의 개인정보보호기구와는 다소 차이가 있다.

(2) 연방정보보호청의 조직구성

연방정보보호청은 기관장을 중심으로 약 70여명의 직원이 활동하고 있으며 총 8개 부서로 나누어져 있다. 제1부는 업무총괄 및 국제협력을 맡고 있으며, 제2부에서 제8부는 각 영역별로 개인정보보호 업무를 담당하는 부서로 구분되어 있다. 제2부는 법제·금융·노동행정·국방·민원서비스·외국인 대상업무에 대한 정보보호 감독업무를 행하고 있으며, 제3부는 사회복지분야의 개인정보보호 문제 및 정보보호 협력업무를 행한다. 또한 제4부는 경제·의료 서비스·교통·우편·통계관련 개인정보보호업무를 담당하며, 제5부는 경찰·방송 업무 담당, 제6부는 기술안전정보보호 및 정보기술과 정보안전을 담당한다. 제7부는 일반 내무행정과 관련된 개인정보보호 및 형법 관련업무, 신고제 담당업무 등을 행하며, 제8부는 통신·전화 및 의료와 관련된 정보보호업무를 담당한다. 이 외 ZA부(Zentrale Aufgaben)는 사무국의 인사행정과 예산수립 및 집행업무를 담당하며, 홍보부(Pressearbeit)는 미디어와의 집중적인 접촉과 기자의 질문에 답변하는 업무를 담당한다. 또한 연방정보보호청에도 역시 조직 내부의 개인정보보호업무를 담당하는 내부 정보보호관리책임자가 임명되어 있다.



(그림 4-4) 독일 BfD의 조직도

(3) 연방정보보호청의 주요기능

연방정보보호법의 일반적인 목적은 '개인정보의 처리로 인한 개인의 권리침해에 대하여 당해 개인을 보호'하는 것이다. 따라서 이는 연방정보보호법에서 규정한 사항이 준수되고 있는지를 규율하기 위해 설립된 연방정보보호청의 활동목적이라고도 할 수 있을 것이다.

따라서 개인정보를 수집·이용·처리하는 연방정부 및 연방공공기관에 대하여 규제하고 관리·감독하는 임무를 맡고 있는 연방정보보호청은 연방정부 및 공공기관을 상대로 제기된 불만이나 민원신고를 접수하여 처리하고, 관할 영역에 해당되는 기관들의 개인정보처리현황을 점검하고 조사·감독하는 기능을 주로 하고 있다. 이 외에도 관할범위에 해당되는 개인정보처리자를 등록하는 등록부를 유지·관리하고[180], 의회 및 정부에 대하여 법률·정책자문을 행한다.[181] 또한 주 개인정보보호기구와 협력과 업무의 조화를 위해서 1년에 두 차례 연례회의를 하는 등 다른 개

180) 2003년에는 연방정보보호청에 등록된 정보처리자의 수가 약 20,000에 이르고 있다. 그러나 등록된 정보관리자의 수는 점차 줄어들고 있는 추세라고 하는데, 이는 2001년 개정법에 의해 등록의무가 내부 정보보호관리책임자를 임명하는 것에 의해 면제될 수 있었기 때문이다. (EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/germany.htm 참조)

181) 특히 정부에서는 행정내부의 규칙 등으로 개인정보와 관련된 문제에 대하여 연방정보보호청으로부터 자문이나 협조를 구하는 것이 의무로 되어 있는 경우가 많다.

인정보보호기구들과의 협력체계도 유지하고 있다. 이러한 연방정보보호청의 주요 기능을 살펴보면 다음과 같다.

〔표 4-15〕 독일 연방정보보호청의 주요기능

구분	주요기능
정보처리 등록	· 개인정보처리자로부터 소정의 사항을 신고받아 등록
법규준수 조사 · 감독	· 연방정부 등의 정보보호법 준수실태 모니터링 · 의회 · 연방정부의 요청시 정보보호시스템에 대하여 조사 · 위반행위에 대해 시정권고
피해구제	· 연방정부 등을 상대로 한 각종 개인정보침해신고접수 · 자료제출요구 및 현장조사 등을 통한 사실조사 · 침해행위자에 대하여 시정조치, 원상회복 등 권고 · 정보주체의 접근 · 정정 · 삭제요청 대신하여 행사
정보제공	· 개인정보보호 모니터링 결과에 대한 정보제공 · 정보주체, 정보처리자 등의 권리 · 의무에 대한 지침제공
법률 · 정책 자문	· 정부에 대하여 정책자문 · 매2년마다 연차보고서 작성 및 연방의회 보고 · 의회 · 정부 요구시 의견서, 조사서, 보고서 작성 및 제출 · 법률자문 및 권고
교육 · 홍보	· 개인정보보호를 위한 교육 실시 · 언론보도자료 배포 및 각종 위원회 발간물 작성
국내외 협력	· 주 개인정보보호기구 및 민간영역의 감독기구와의 협력 · 국제협력 강화

라. 개인정보피해구제 절차 및 방법[182)]

독일의 개인정보피해구제 절차 및 방법도 대표적으로 연방정보보호청을 중심으로 살펴볼 수 있을 것이다. 연방정보보호청은 앞에서 살펴본 바와 같이, 주로 연방 공공기관을 대상으로 한 개인정보침해사건을 접수받아 처리하고 있다. 예를 들면 연방 각 부처, 안보국(Secret Services), 연방노동청(Federal Labour Agency)과 같은 연방기관을 들 수 있고, 그 외 전

182) 독일연방정보보호청의 개인정보피해구제 절차 및 방법은 Der Bundesbeauftragte für den Datenschutz, “Complaints Handling Procedure in Germany”, Ⅶ Complaints Handling Workshop on March 10 and 11, 2003 in Warsaw 참조.

기통신서비스 및 우편서비스에 관한 민원도 함께 처리하고 있다. 따라서 이러한 기관이나 단체의 행위로 인하여 개인정보침해를 입었거나 열람·정정·삭제요구권과 같은 자신의 정당한 권리행사를 거부당한 자는 연방정보보호청에 이의제기를 할 수 있다. 이러한 이의제기의 권리(Right to appeal)는 독일 연방정보보호법에 의해 보장되고 있는 것이다. 따라서 연방정보보호청은 시민들의 이러한 권리 행사를 지원하기 위해, 불만사항이나 침해사건을 접수받아 간편한 절차에 따라 무료로 처리해주고 있다. 연방정보보호청은 작년 한 해약 3,000건 정도의 개인정보침해사건을 다루었다고 한다.

구체적으로 연방정보보호청이 정보주체의 권리보호와 피해구제를 위해 어떻게 활동하고 있는지 살펴볼 필요가 있을 것이다. 첫 번째 단계는 시민들로부터 연방공공기관 등에 의한 권리침해에 대하여 신고를 접수받는 것이다. 연방정보보호청은 사건을 접수받으면, 신고받은 기관으로부터 답변을 받을 필요가 있는지 및 신청인과 신청사실을 해당 기관에게 비밀로 하여 사건을 진행할 수 있는지 여부를 결정한다. 여기서 만약 민원인의 이름을 밝혀야 할 필요가 있다면 먼저 해당 민원인에게 동의를 구하여야 하나, 대부분의 경우 민원인들은 자신의 이름이 밝혀지기를 꺼려하는 경우가 많이 있기 때문에 연방정보보호청에서는 민원인의 이름을 밝히지 않고 직접 자체조사를 실시하기도 한다.

연방기관으로부터 서면답변서를 받은 이후에는 신청인이 한 신고내용과 답변서의 내용을 비교하고 사건을 평가하는 단계를 거친다. 그러나 서면 답변서만으로 충분한 사실조사가 어려운 경우에는 보다 자세하고 정밀한 정보를 얻기 위해 해당 기관에 직접 문의하고 협조를 구할 수 있다. 연방정보보호법에 따르면 연방기관은 연방정보보호청의 업무수행을 전적으로 지원하고 보조할 의무가 있다.[183] 특히 질문에 대해 정보를 제공하고 모든 문서와 정보처리 프로그램 및 업무장소에 접근할 수 있도록 언제든지 허락하여야 한다.

---

183) 독일연방정보보호법 제24조제4항.

이러한 사실조사 과정을 통해 법위반행위가 발견된 경우, 연방정보보호청은 당해 불법행위를 중지하거나 시정할 것을 권고하거나 중대한 침해행위를 한 자를 자체징계토록 유도한다. 그러나 반복적이거나 중대한 불법행위의 경우에는 형사고발[184]을 하거나 공식적인 문제제기(Formal complaint)를 할 수 있다. 연방정보보호청이 공식적으로 문제제기를 하는 경우 해당 정보처리자는 일정 기간 안에 답변서를 제출하여야 하는데, 답변서에는 향후 올바른 정보처리를 하기 위해 어떠한 조치를 취할 것인지에 대한 내용을 기술하여야 한다. 이렇게 연방정보보호청이 공식적으로 문제제기를 한 사건은 연차보고서에 기재되어 의회에 제출되며, 의회의 위원회에서 철저히 논의되고 때로는 추가적인 조치가 이루어지기도 한다. 또한 이러한 방법으로 일반 대중에게 해당 정보처리자의 개인정보침해행위가 공개되기도 한다.[185]

법률에 의하면, 연방정보보호청은 연방기관의 기술적 또는 관리상의 문제를 구속력이 있거나 강제력 있는 방법으로 규제할 법적 권한은 없다. 그러나 연방정보보호청의 높은 도덕적 권위와 독립적 권한, 의회와 연방정부와의 직접 접촉할 수 있는 권한 등으로 인하여, 사실상 불법행위를 한 정보처리자가 개인정보를 수집, 처리하는 방법을 변경하도록 강제되고 향후 개인정보를 더욱 보호할 수 있는 개인정보처리를 갖추고 추가적인 침해행위가 발생하지 않도록 하기 위한 필요한 관리적, 기술적 조치를 취하도록 강제하는 역할을 하고 있다.

---

184) 연방정보보호청은 검찰에 정보처리자의 위법행위를 고발조치할 수 있는데, 해당 형사범죄가 고의적으로 다른 사람을 해하거나 재산을 취득할 목적으로 또는 금전과 교환할 목적으로 이루어진 경우에 법원은 최고 2년의 징역 또는 벌금형을 부과할 수 있다.

185) 지난 제18차 연차보고서(biannual activity report)에서 독일 연방정보보호청은 총 14건의 개인정보침해사건을 공개하였고, 2003년 5월에 의회에 보고된 보고서에서는 총 22건의 침해사건을 언급하였다.

민원접수	· 개인정보침해사건 또는 정보주체의 권리행사요청을 거부한 사건에 대한 이의제기 신청접수 · 민원인의 실명공개여부 결정
↓	
사실조사	· 자료제출 요청, 현장조사, 불시점검 등을 통한 사실조사
↓	
심사 · 평가	· 원칙 및 법위반 여부에 대한 심사 및 판단
↓	
시정권고	· 경미한 침해사건에 대해 시정권고 등을 통해 사건해결
↓	
공식적인 문제제기	· 중대한 법위반사건에 대해 해당 정보처리자에게 공식적으로 문제제기 · 답변서를 제출토록 요구하여 시정조치 약속을 받음 · 연차보고서를 통한 의회 및 일반대중에게 법위반행위 공개
↓	
형사고발	· 중대한 법위반사건에 대하여 검찰 고발

(그림 4-5) 독일 BfD의 피해구제 절차도

그러나 한편 정보처리자가 정보주체의 개인정보를 수집 · 처리 · 이용하는 과정에서 정보주체에게 손해를 끼쳤다면 마땅히 보상을 하여야 할 것이다. 연방정보보호청은 구체적으로 손해배상과 관련하여 그 배상액에 대해 분쟁조정을 하는 등의 역할을 하고 있지는 않다. 그러나 개인정보처리자의 개인정보침해행위로 인하여 구체적인 피해를 입은 정보주체는 법원을 통해 독일민법상 인격권침해규정을 근거로 과실을 입증하여 정보처리자에게 손해배상청구, 금지청구, 방해배제청구를 주장할 수 있다. 즉, 정보처리자가 개인정보의 처리과정에서 정보주체의 인격권을 침해하여 불법행위를 한 것으로 인정된 때에는 민법 제823조 제1항[186]에 따라 일

186) 민법 제823조 제1항은 신체 · 건강 · 생명 · 자유권에 대해서만 규정하였으나, 연방대법원은 1954년 민법 제823조 제1항에서 규정하고 있는 기타의 권리로서 일반적 인격권을 인정함으로써 개인의 보호가치 있는 영역을 침해하는 것으로부터 보호받아야 할 프라이버시권의 개념을 인정하고 있다.

반적 인격권 침해에 기초한 민사책임을 부담하게 된다.[187] 한편 개인정보보호와 관련하여 공공기관은 일반 민간단체보다 더 중한 책임을 부담한다. 즉, 연방정보보호법 제7조에 의하면 공공기관이 중대한 인격권 침해를 한 경우에는 위험책임을 부담하게 된다. 따라서 피해자는 연방정보보호법에 따라 정보처리자에게 손해배상을 청구하는 경우, 입증책임 면에서 좀 더 유리한 입장을 차지하게 된다. 다만 연방정보보호법에서는 불법행위에 대해 민법 제1004조와 민법 제12조에 상응하는 일반적인 방해제거 및 부작위청구를 규정하지 않고 있어, 이는 민법상 구제수단에 따라야 한다.

4. 스웨덴

스웨덴은 「1973년 정보법(The Data Act of 1973)」을 제정하여 전자적인 형태로 개인정보를 기록한 모든 자의 정보처리를 규율한 바 있다. 동법은 국가 차원에서는 세계 최초로 제정된 개인정보보호법이라 할 수 있다. 전통적으로 사회보장제도가 잘 발달해 있고 시민들의 자유와 인권존중을 위한 제도가 잘 시행되고 있는 환경과 배경이 개인정보보호를 위한 법제도의 도입과 시행에도 영향을 미친 것으로 보인다.

가. 개인정보보호 법제현황

세계 최초로 국가차원에서 제정된 개인정보보호법인 스웨덴의 「1973년 정보법(The Data Act of 1973)」은 지난 1998년 10월 24일 시행된 「정보보호법(The Data Protection Act)」으로 대체되었다. 1973년에 제정된 정보법은 주로 공공기관을 중심으로 한 자동화된 정보처리에 대하여 규율하는 것이 주된 목적이었기 때문에, 모든 개인정보처리에 대하여

187) 이러한 민사책임이 발생하기 위한 불법행위 성립요건은 다음과 같다. 첫째, 당해 정보가 생존하는 개인을 특정할 수 있어야 하며 둘째, 개인정보는 인격권의 중대한 침해와 관련이 있어야 한다. 셋째, 개인정보가 비밀성을 유지하고 있어야 하며 넷째, 부정 취득·이용·공개행위와 같은 개인정보침해행위가 있어야 한다.

포괄적으로 규율하고 있는 1995년 EU 개인정보보호지침에는 부합하지 않았다. 이에 스웨덴은 포괄적 적용범위를 가진 EU 개인정보보호지침의 제정과 시행으로 인해 변화된 환경에 맞추어 1998년 새로운 개인정보 관련 법률을 제정한 것이다. 그러나 1998년 정보보호법은 동법 제정 이전에 행해진 개인정보처리에 대하여는 2001년 10월까지 1973년 정보법이 적용되도록 유예기간을 두고 있다.

새롭게 제정된 정보보호법은 스웨덴에서 이루어지고 있는 모든 개인정보의 수집・이용・저장・전송 등을 규율하고 관장하는 개인정보보호 기본법의 기능을 하고 있다. 그러나 이 외에도 특히 신용정보와 관련하여서 「채권추심법(The Debt Recovery Act, 1974)」과 「신용정보법(The Credit Information Act, 1973)」이 있어 은행・보험・신용정보회사・채권추심회사 등에서 고객의 신용정보를 어떻게 관리하고 보호하여야 하는지 규정하고 있다. 따라서 신용정보법에 의하면 신용정보 관련활동을 수행하는 모든 자는 통상 정보조사원으로부터 정보처리에 대한 허가를 받아야 한다. 정보조사원은 합법적인 적절한 방법으로 정보처리사업이 수행될 것이라는 추정이 있는 경우에 한하여 허가를 부여하며, 해당 정보처리자가 신용정보법을 준수하는지 여부에 대하여 조사할 권한을 부여받았다. 채권추심법에서도 마찬가지로 다른 사람을 위해 채권추심을 하는 자는 반드시 정보조사원으로부터 정보처리에 대한 허가를 받도록 규정하고 있다. 따라서 정보조사원은 동법에 근거하여 허가를 위한 필요요건이 충족되었는지 및 건전한 채권추심 관행이 준수되고 있는지에 대하여 판단하여야 한다.

나. 정보보호법의 주요내용

정보보호법은 앞에서 말한 바와 같이, 공공부문과 민간부문의 모든 개인정보처리에 대하여 규율하고 부당한 개인정보침해를 방지하기 위한 목적으로 1998년 시행된 것으로, 동법은 제1조를 통해 '개인정보 처리로 인하여 개인의 무결성(integrity)이 훼손되는 것을 방지'하기 위한 목적으로

제정되었음을 밝히고 있다. 또한 동법은 스웨덴의 개인정보보호에 관한 기본법적 특성을 가지는 바, 다른 법령의 규정이 동법과 상반되는 조항을 포함한 경우 동법이 우선 적용된다(동법 제2조).

1998년 정보보호법은 1973년 정보법과는 달리 자동화된 개인정보의 처리는 물론, 일부 구조화된 파일링시스템에 포함되는 개인정보의 처리에 대해서도 적용되며(동법 제5조), 민감한 개인정보에 대해서는 특칙을 두어 보호하고 있다(동법 제13조). 스웨덴 정보보호법의 주요내용을 간략히 요약하면 다음과 같다.

［표 4-16］스웨덴 정보보호법의 주요내용

구분	내용
효력발생	1998. 10. 24. 발효
목적	개인정보처리로 인한 프라이버시 침해 방지(공공/민간)
경과규정	과도기간을 두어 신법 발효 이전에 이루어진 행위에 대해서는 3년간(2001. 10. 24. 까지) 구법이 적용되도록 함
적용범위	자동화된 개인정보 및 일부 수동처리된 개인정보파일의 처리(§ 5)
적용배제	· 순수하게 사적으로 처리되는 개인정보(§ 6) · 공문서에 대한 공적 접근원칙, 언론의 자유, 표현의 자유에 해당하는 경우(§§ 7~8)
내용	· 개인정보처리에 관한 기본규정(§ 9) · 개인정보처리가 허용되는 경우에 대한 규정(§ 10) · 민감한 개인정보에 대한 특별제한규정(§§ 13~19) · 개인정보의 정정, 처리과정상 보안에 관한 정보제공 규정(§§ 23~26) · 고지의무 : 개인정보를 처리하는 자는 DPB에 고지하여야 함(§ 36) · 고지의무의 면제 : 개인정보보호책임자가 임명되는 경우(§§ 37~38) - 개인정보보호책임자는 개인정보처리자의 정보처리작용에 대하여 독립조사를 수행할 임무를 지님 · 강제적 고지사항 : 정보의 무결성(integrity)과 관련하여 특히 민감한 특정 정보처리작용은 반드시 정보조사원에서 사전조사를 받기 위해 고지되어야 함(§ 41) · DPB의 권한 등에 관한 규정(§ 43)

한편 스웨덴의 정보보호법은 제9조를 통해 일반적으로 개인정보처리자가 지켜야 할 아홉 가지 개인정보처리 기본원칙을 규정하고 있는 바, 이를 살펴보면 다음과 같다.

［표 4-17］스웨덴 정보보호법상 개인정보처리 기본원칙

원칙	내용
제1원칙	합법적인 경우에만 개인정보 처리
제2원칙	올바른 관행에 맞추어 정확한 방법으로 처리
제3원칙	특정하고 명시적인 정당한 목적에 따라 수집
제4원칙	수집목적에 부합하지 않는 목적으로의 처리 금지
제5원칙	처리목적과 비교할 때 적절하고 관련성이 있는 처리
제6원칙	처리목적에 견주어 불필요한 개인정보 처리 금지
제7원칙	처리되는 개인정보의 정확성 확보, 필요한 경우 최신성 확보
제8원칙	처리목적과 관련하여 부정확하거나 불완전한 개인정보를 정정, 차단, 삭제하기 위한 모든 합당한 조치를 취하여야 함
제9원칙	처리 목적에 필요한 이상의 기간동안 보존 금지

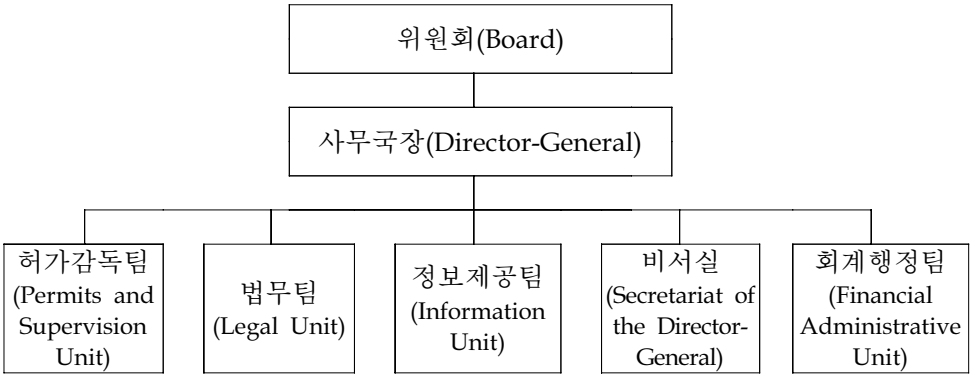
다. 스웨덴의 개인정보보호기구

스웨덴의 개인정보보호기구는 1974년 설립된 정보조사원(DIB : The Data Inspection Board)으로, 정보조사원은 1973년 정보법에 의해 설립되었다. 정보조사원은 개인정보에 관한 기본법인 정보보호법에 근거하여 활동하고 있는 바, 민간과 공공부문의 모든 개인정보처리에 대하여 규율한다. 또한 자동처리되는 개인정보 (일부분만 자동처리되는 경우도 포함) 및 특정기준에 따라 검색과 편집이 가능하도록 수집되어 처리되는 개인정보를 보호하며, 기타 신용정보보호의 역할도 함께 수행하고 있다.

(1) 정보조사원의 지위 및 구성

정보조사원은 스웨덴의 대표적인 개인정보보호기구로서, 중대하고 복잡한 개인정보 관련 문제에 대하여 심의하고 결정하는 역할을 하는 위원

회(Board)와 사무국으로 구성되어 있는 행정기관이다. 위원회는 사무국장(Director-General)을 포함하여 총 9인의 위원으로 이루어져 있으며, 사무국장을 제외한 8인의 위원이 모두 국회의원으로 임명된다. 따라서 위원구성과 기관의 성격 면에서 고도의 독립감독기구의 면모를 가지고 있다고 볼 수 있다. 한편 사무국은 재무부(Ministry of Finance)에서 예산을 지원받고 예·결산 보고서 및 연차보고서를 정부에 제출하며, 사무국장의 임명도 재무부 장관이 행한다.[188] 직원의 인력은 약 40여명 정도이며, 대부분 법률가나 IT 전문가이다. 정보조사원의 조직구성도를 살펴보면 다음과 같다.



(그림 4-6) 스웨덴 정보조사원 조직도

정보조사원은 허가감독팀, 법무팀, 홍보팀, 사무국장 비서실, 회계행정팀의 총 5개 부서로 나뉜다. 이 중 허가감독팀은 1973년 정보법에 따라 정보조사원이 주로 담당해왔던 정보처리자 등록 및 허가와 관련된 업무를 맡고 있다. 법무팀은 주로 법률이나 정책자문, 정보보호법에 대한 상담 및 법률해석에 대한 판단기준 제공 등의 업무를 하고 있다. 이와 같은 정보조사원 5개 부서가 행하는 주요업무는 다음과 같다.

188) 정보조사원의 관할을 재무부에서 법무부로 이전한다는 논의가 진행중이다.

［표 4-18］스웨덴 DIB의 조직구성 및 주요업무

부서	주요업무
허가감독팀	· 개인정보법, 구정보법, 채권추심법, 신용정보법에 따른 모든 정보처리 허가신청을 처리 · 사무국에 접수된 민원접수, 조사 및 감독 · 각종 법률에 대한 지침 및 규약(Code of statutes) 제정
법무팀	· 정부 입법안의 개인정보침해가능성 여부 심사 및 의견 제공 · 각종 규제활동(regulatory activity) · 허가감독팀이 제정하는 지침이나 상담의 복잡한 법률문제 지원 · 국제협력업무 담당
홍보팀	· 공공기관, 기업체, 민간단체, 언론, 시민에게 프라이버시 보호의 중요성 및 사무국 활동, 관련법률 등에 대해 정보제공 및 홍보 · 사무국 웹사이트, 전화상담센터 운영 · 개인정보 관련 회의 개최 및 교육·강의 지원
사무국장 비서실	· 사무국의 일반행정 및 인사업무 · 등록부(registry) 등 공공기록(archives) 관리 · 사무국 데이터시스템 개발·운영 및 보안담당 · 예산업무 및 연차보고서 작성
회계행정팀	· 사무국 내부회계업무 담당

(2) 정보조사원의 주요기능 및 권한

스웨덴의 정보조사원은 공식적으로는 개인정보처리 신고를 접수받아 등록 및 허가를 하는 기관(permits authority)이나, 감독, 상담, 정보제공 등의 업무도 담당하고 있다. 따라서 개인의 프라이버시 보호 및 신용정보보호, 채권추심에서 올바른 사업관행 확보를 위한 법규준수여부 모니터링을 행하며, 프라이버시 침해로 인한 민원을 접수받아 처리하고 조사하는 피해구제의 역할도 수행하고 있다. 그 외에도 규칙(regulation), 권고(recommendation) 제정, 정부입법 및 질의에 대한 의견제시, 사업자와 소비자 등을 위한 정보제공, 각종 규제활동을 통한 침해예방 등의 역할도 수행하고 있다. 세부적인 내용은 다음과 같다.

〔표 4-19〕 스웨덴 DIB의 주요기능

구분	세부내용
피해구제	· 피해자에 대한 불만처리 및 사실조사 · 지방행정법원(County Administrative Court)에 불법적인 방법으로 처리된 개인정보의 삭제 청구 · 위법행위에 대한 과태료 부과 및 시정권고
허가	· 정보법에 따라 자동화된 개인정보 처리에 대한 등록 및 허가 업무 수행(이러한 정보조사원의 결정에 대해서는 행정법원에 항소할 수 있음) · 1998 정보보호법은 정보조사원에 의한 허가를 규정하고 있지 않음
실태조사 및 감독	· 개인 또는 언론의 이의제기로 인한 실태조사 실시 및 감독 · 정보조사원 자체 실태조사 및 감독 · 영역별 개인정보처리 현황조사 · IT 보안여부 조사 · 침해행위시 과태료(default fine) 부과, 개인정보처리행위 금지 · 조사를 진행하는 중 형사범죄에 해당되는 사안일 경우 경찰에 이첩가능 (주로 웹사이트의 개인정보 공개를 통한 프라이버시 침해 및 적정한 근거없는 신용정보공개의 경우) · 사전심사(preliminary examination) : 범죄조사 목적의 경찰 및 국세청에 의해 수행되는 정보처리에 대한 사전심사
지침 제정	· 자동화된 개인정보처리에 대한 규칙 제정 : 개인정보처리가 허가되는 경우, 개인정보처리자의 자격요건, 개인식별번호의 사용이 허가되는 경우 등에 대한 규칙 제정 · 법률 규칙이나 기타 법규, 법해석에 대한 지침 등 제정 · 일반 권고문 제정 및 고시
상담 및 자문	· 공공기관, 일반기업체, 민간단체 등에게 개인정보 상담 · 상담센터 운영을 통한 개인정보침해상담 · 조사위원회(Commissions of inquiry) 보고서에 대한 의견제공 · 정부 입법안에 대한 개인정보침해가능성 자문 및 권고
연구	· 개인정보보호에 관한 조사·연구 · 개인정보에 영향을 미치는 신기술 개발과 프라이버시 보호 조사
자율규제 지원	· 민간영역의 개인정보처리에 관한 자율협약(Sector agreement)에 대하여 의견 제시(요청시) · 각 개인정보처리자의 개인정보보호책임자에게 정보제공 및 협의
교육홍보	· 개인정보보호 세미나 등 교육실시 · 웹사이트, 간행물 등 제작·홍보
대외협력	· EU Data Protection Working Party 등 국제기구와 협력 · 국내 유관기관과 협력

정보조사원은 위와 같은 기능을 수행하기 위해 조사권, 시정권고권, 과태료 부과 등의 권한을 가지고 있는 바, 정보조사원이 부여받은 권한을 살펴보면 아래와 같다.

〔표 4-20〕 스웨덴 DIB의 주요 권한

사실조사권(§ 43)	· 처리되고 있는 개인정보에 접근할 수 있는 권한 · 조사를 위해 필요한 정보 및 서류의 취득권한 · 정보처리 시설에 관한 접근권한
시정권고권(§ 45)	· 경고, 독촉 등의 방법으로 시정권고
과태료부과(§§ 44~45)	· 시정조치가 불가능한 경우, 긴급한 경우 등 과태료 부과
보안조치 결정(§ 32)	· 개개 사안별로 필요한 보안조치가 무엇인지를 결정 · 일종의 시종권고적 성격을 가짐
정보삭제청구권(§ 47)	· 불법적으로 처리된 개인정보의 삭제를 지방행정법원에 청구할 수 있음
위법사실 통보(§ 49)	· 형사조치가 가능한 위법사항에 대하여 관계기관에 통보할 수 있음

일반적으로 스웨덴의 정보조사원은 시정명령보다는 시정권고를 통해서 문제를 해결하고 있고, 만약 이러한 시정권고를 통해서도 적절히 해결될 수 없는 사안에 대해서는 해당 개인정보처리자에게 과태료를 부과하는 결정 권한을 행사하고 있다.

라. 개인정보피해구제 절차 및 방법

정보조사원은 설립 당시에는 자동화된 정보처리에 대하여 신고를 받아 등록 또는 허가를 해주는 기관이었다. 그러나 정보보호법의 제정으로 정보조사원의 성격이 당초의 허가기관에서 개인정보보호와 관련된 포괄적인 업무를 행하는 개인정보전담기구로 변화하였다. 특히, 개인정보보호를 위한 전담기구로 바뀌면서 정보조사원은 개인정보침해신고를 접수받아 불법적인 행위에 대해 제재조치를 취하는 등 개인정보처리와 관련된 불만이나 이의제기를 원만히 해결하는 역할을 담당하고 있다.

이를 위해 정보조사원은 상담전화를 운영하기도 하고, 개인 또는 해당 정보처리 사업자나 단체의 개인정보보호책임자로부터 개인정보침해행위나 법위반행위에 대한 신고나 불만을 접수받는다. 또한 정보조사원이 자체적으로 개인정보보호 실태조사를 실시하여 법위반여부를 조사하기도 한다. 이러한 과정을 통해 개인정보침해행위가 의심되는 경우, 정보조사원은 해당 정보처리 사업자나 기관에서 처리되고 있는 개인정보에 접근하거나 개인정보의 처리 및 안전성 확보를 위한 보안조치에 관련된 각종 자료를 취득할 수 있다. 또한 필요한 경우에는 직접 개인정보의 처리와 관련된 시설에 접근하는 방법을 통해서 사실조사를 거친다. 사실조사를 거친 결과, 개인정보처리행위가 불법적인 방법으로 이루어졌다고 판단되는 경우 정보조사원은 시정조치 요구 등의 권고 절차를 거칠 수 있고, 긴급한 경우에는 과태료를 부과할 수 있다.[189] 그러나 과태료 부과 결정을 준수하지 않는 개인정보처리자가 형사상 책임을 지는 것은 아니다.[190] 정보조사원은 또한 행정적 제재에 그치는 것뿐 아니라, 불법적인 방법으로 개인정보가 처리된 경우에는 피해자를 대신하여 해당 관할지방행정법원(County Administrative Court)에 정보처리자가 불법적으로 처리한 피해자의 개인정보를 삭제토록 청구할 수 있다. 또한 형사범죄가 성립되는 경우에는 검찰 등 형사기관에 고발할 수 있다.[191] 그러나 정보조사원은 다른 유럽의 개인정보보호기구와 마찬가지로 적극적인 방법으로 피해자가 입은 경제적·정신적 손해에 대한 배상에 대해 결정을 내리지는 않는다. 이는 민사법원의 몫으로 남겨져 있다.[192] 아래 그림은 지금까지 살펴본 정보조사원의 개인정보피해구제 절차도이다.

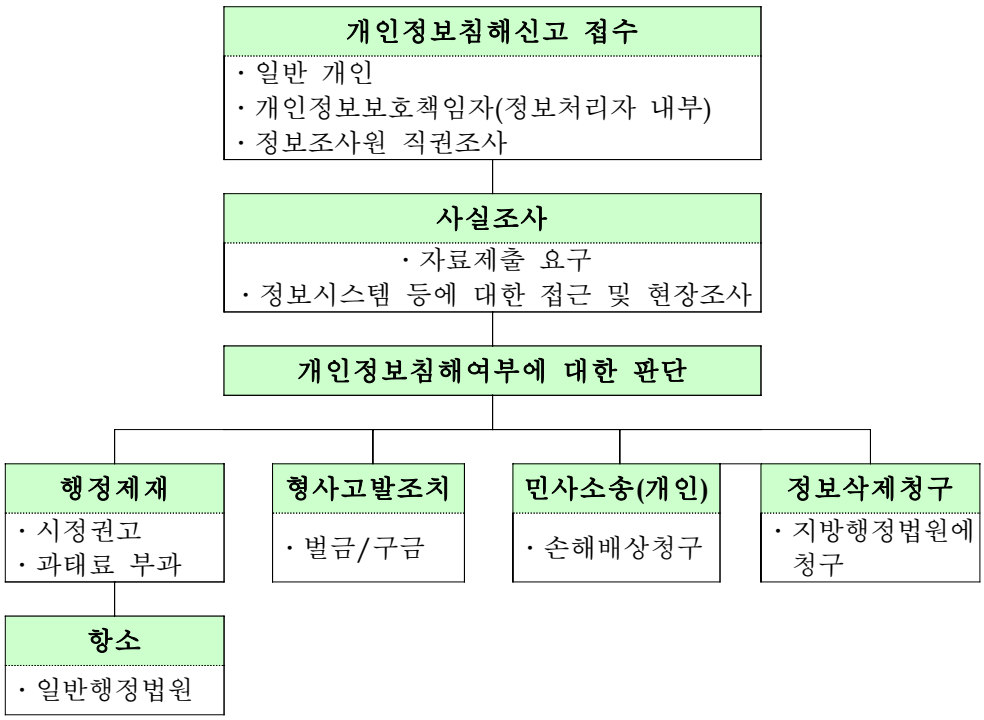
---

189) 이러한 정보조사원의 행정제재 결정에 대해서 불만이 있는 정보처리자는 이에 대해 일반행정법원에 항소할 수 있다(정보보호법 제51조).

190) 정보보호법 제49조.

191) 정보보호법은 제49조에서 정보처리자가 동법 제13조~제21조, 제33조~제35조, 제36조 전단, 제41조 등에 위반한 경우에는 벌금 및 구금 등의 형사제재를 받을 수 있다는 벌칙조항을 두고 있다.

192) 정보보호법 제48조는 개인정보처리자의 정보보호법을 포함한 법위반으로 인하여 정보주체의 개인정보 무결성이 훼손됨으로써 입은 경제적·정신적 피해를 배상할 책임이 있음을 규정하고 있다.



(그림 4-7) 스웨덴 정조보조사원의 피해구제 절차도

제 3 절 북미

1. 미국

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

이렇듯 미국은 개인정보보호를 위한 포괄적이고도 체계적인 기본법을 가지고 있지도 않고, 되도록이면 시장경제질서에 개입하는 제재조항을 담은 내용을 입법화하지 않으려는 것이 일반적이다. 그러나 미국에 개인정보 또는 프라이버시 관련 법률이 전혀 없는 것은 아니다. 오히려 기본법이 부재한 상황이기 때문에, 사회적 변화나 기술발달에 맞춰 공공·통

신·금융·온라인 등 각 영역별로 많은 개인정보 관련 법률을 마련해 두고 있다. 이하에서는 이러한 미국의 영역별 개인정보 관련 법률현황에 대해 살펴보고, 민간영역에서 소비자의 개인정보보호 기구로서의 역할을 일부 담당하는 연방거래위원회(FTC : Federal Trade Commission)에 대해서 살펴보도록 하겠다. 특히, 미국에서는 자율규제체계의 특성상, 정부에 의해 설립된 감독기구나 규제기구가 없어 민간 분쟁해결기구에 의한 개인정보피해구제제도가 발달하였다. 따라서 마지막으로 이러한 미국의 민간 소송외적 분쟁해결제도 현황과 그 성과 및 문제점에 대해 살펴보도록 하겠다.

가. 개인정보보호 법제현황

(1) 판례법상 프라이버시권의 인정

미국은 헌법상 명시적인 프라이버시권 규정을 가지고 있지는 않다. 그러나 미연방대법원(U.S. Supreme Court)은 사적 통신의 자유가 있음을 확고히 한 Katz v. United States 판결에서 제1차, 제3차, 제4차, 제5차 수정헌법을 간접적인 의미에서의 프라이버시권 조항으로 해석할 수 있다고 밝힌 바 있다. 특히 법원은 제4차 수정헌법(Fourth Amendment)[193]을 함축적인 의미의 프라이버시권 규정으로 볼 수 있다고 하면서, 개인이 '프라이버시에 대한 합리적 기대(reasonable expectation of privacy)'를 가진 영역에 있어서는 정부의 감시나 간섭으로부터 자유로울 권리를 가진다고 하였다.[194] 이로 인해 미국에서는 헌법상 명시적인 개인의 프라

193) 제4차 수정헌법은 "누구든지 불합리한 압수·수색으로부터 자신의 신체·주거·서신·물품을 안전하게 보호할 권리를 침해당하여서는 안 된다. 또한 압수·수색의 대상자, 물품, 장소를 명시한 법원의 결정과 같은 합당한 근거 없이는 영장이 발부되어서는 안 된다"라고 하여, 적정절차 원칙과 개인의 신체의 자유를 규정하고 있다.

194) Katz v. United States, 389 U.S. 347, 351-52(1967). 동 판례에서 18 U.S.C. 1084에 위반하여 전화로 내기정보(wagering information)를 제공한 혐의로 기소된 원고 Katz는 FBI가 자신의 전화내용을 도청하기 위해 공중전화부스 밖에 도청장치를 부착한 것은 공중전화 이용자의 프라이버시권을 침해한 것이라고 주장하였다.

이버시권에 대한 규정은 없지만, 다른 헌법상의 조항들을 통해 개인의 사적 자유가 존중되어야 할 프라이버시권을 가지는 것으로 해석되고 있다.[195]

한편 미연방대법원은 일반적인 프라이버시권 외 개인정보와 관련한 정보프라이버시권(Right to information privacy)에 대해서는 명확한 언급을 하고 있지 않다.[196] 다만, 법원은 Roe v. Wade 판결[197]에서 "프라이버시에 대한 독립적인 권리나 영역은 존재한다. 이는 아이를 낳을 것인지에 대한 결정 또는 낙태를 할 것인지에 대한 결정과 같이 한 개인에게 중요한 영향을 끼치는 문제에 대하여 스스로 결정할 권리를 포함하는 개념이다"라고 하였고, Whalen v. Roe 판결[198]에서는 "프라이버시 영역은 두 가지 유형의 이익(interest)을 포함한다. 첫 번째는 자신의 사적인 사항들이 공개되는 것을 회피할 수 있는 사적 이익이고, 두 번째는 특정한 중요결정을 내리는데 있어 독립성을 가지고 행할 수 있는 이익이다"라고 하여, 개인이 자신의 개인정보를 다른 간섭으로부터 자유로이 사적으로 관리하고 결정할 권리를 가지고 있음을 밝힌 바 있다.

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

---

195) 그러나 이러한 헌법상 근거는 기본적으로 국가, 즉 행정부 등 공권력에 대한 개인의 프라이버시 및 사적 자유의 보장을 의미하는 것으로 보아야 한다. 즉, 민간 기업이나 단체의 개인정보 침해행위로부터 개인의 자유를 보장하기 위한 헌법상 근거를 동 조항으로부터 바로 이끌어내기에는 다소 무리가 있다. Fred H. Cate, *"The Changing Face of Privacy Protection in the European Union and the United States"*, 33 Indiana Law Review 174, 203 (1999).

196) Jonathan P. Cody, *"Protecting Privacy Over the Internet : Has the Time Comer to Abandon Self-Regulation?"*, 48 Catholic University Law Review 1183, 1193 (1999) ; Domingo R. Tan, *"Personal Privacy in the Information Age : Comparison of Internet Data Protection Regulations in the United States and the European Union"*, 21 Loyola of Los Angeles International $ Comparative Law Journal 661, 669 (1999).

197) Roe v. Wade, 410 U.S. 113 (1973).

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

(2) 개인정보보호 법제현황

미국은 각 영역별로 많은 개인정보 또는 프라이버시 관련 법률을 제정하여 시행하고 있다. 이러한 제정법은 헌법이나 판례법에서 보장하는 권리보호를 해당 영역에서 더욱 명확하게 규정하여 원칙을 확고히 할 수 있다는 점에서 의미가 있다. 미국의 대표적인 개인정보관련 입법현황을 살펴보면 아래와 같다.

〔표 4-21〕 미국의 개인정보관련 법제현황

구분	개인정보 관련법
공공부문	· 프라이버시법(Privacy Act, 1974) · 정보공개법(Freedom of Information Act, 1974) · 프라이버시보호법(Privacy Protection Act, 1980) · 컴퓨터에의한정보조합과프라이버시보호에관한법률 (Computer Matching and Privacy Protection Act, 1988) · 전자정부법(E-Government Act, 2002)
금융부문	· 공정신용평가법(Fair Credit Reporting Act, 1970) · 금융프라이버시권에관한법률 (Right to Fianancial 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)
비디오감시	· 비디오프라이버시보호법 (Video Privacy Protection Act, 1988)
근로자정보	· 근로자기록보호법 (Employee Polygraph Protection Act, 1988)
아동의 개인정보	· 아동온라인프라이버시보호법 (Child Online Privacy Protection Act, 1998)
기타	· 운전자 프라이버시보호법 (Driver's Privacy Protection Act, 1994)

이와 같이 미국은 금융, 의료, 교육, 통신, 비디오감시, 근로자정보 등 각 영역별로 별도의 제정법을 마련하여 개인의 프라이버시 및 개인정보를 보호하고 있다. 이러한 개인정보관련 입법의 주요 내용은 이후에 살펴보도록 하겠다.

(3) 세이프하버 원칙(Safe Harbor Principles)

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

세이프하버 원칙은 기본적으로 유럽연합 회원국과의 국제교류와 관련하여 유럽 시민들의 개인정보를 전달받아 처리하는 미국 기업이 EU지침에서 규정한 '적정성(adequacy)'을 갖추고 있는지 여부를 판단하기 위한 기준이다. 이처럼 동 원칙은 국제조약의 성격을 가진 것이 아니고 개인정보 취급의 적정성 여부를 판단한다는 특정한 목적을 위해 합의된 사항이기 때문에, 미국에서 법적 효력을 가지고 전면적으로 시행되는 것은 아니다. 따라서 세이프하버 원칙에 참가할 것인지 여부는 전적으로 미국 기업의 자발적 의사에 달려 있다. 그러나 실질적으로 동 원칙에 참가할 경우 유럽위원회(European Commission)가 개인정보취급의 적정성을 확인하여 주는 효과를 가지므로 유럽연합 회원국과 개별적으로 별도 협의와 논의를 하여야 할 필요가 없고, 적정성이 추정되기 때문에 특별한 사안이 없는 한 계속해서 개인정보를 교류할 수 있다. 따라서 현재 미국에서는 이러한 세이프하버 원칙의 장점과 이점으로 인해 다수의 기업체가 참여하고 있다.[199]

세이프하버 원칙에 참여하려는 기업은 반드시 동 원칙의 내용을 준수할 것임을 공표하여야 한다. 공표방법은 미국의 상무부(Department of Commerce)에 서면확인서(Self certification letters)를 제출하고 자사의 프라이버시정책에 위와 같은 사실을 공개하는 것이다.[200]

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

［표 4-22］ 세이프하버 7원칙

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

세이프하버 원칙에 참여한 기업은 의무사항 중 하나로, 소비자의 이의제기와 분쟁을 적절히 해결하고 자사의 원칙 준수를 담보할 수 있는 대

199) 2003년 12월 현재 433개의 기업이 세이프하버 원칙에 자발적으로 참여하고 있다. (http://www.export.gov/safeharbor 참조)

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

안적인 분쟁해결제도를 갖추어야 한다. 따라서 이러한 대안적 분쟁해결 절차와 방법을 통해 소비자는 사업자의 원칙 불이행으로부터 입은 피해를 구제받을 수 있다. 그러나 민간차원의 자율규제 프로그램을 통해서도 해결되지 않은 경우에는 연방거래위원회와 미국 교통부(Department of Transportation)가 개입하여 위반 사업자에게 보다 강력한 제재를 부과할 수 있다.[201] 또한 지속적으로 원칙을 위반하는 사업자의 경우에는 상무부의 세이프하버 참여기업 목록에서 삭제될 수도 있다.

나. 개인정보관련 법률의 주요내용

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

(1) 프라이버시법

먼저, 공공부문의 대표적인 개인정보 관련법령은「프라이버시법」[202]이다. 1972년 닉슨 대통령이 민주당 선거대책본부를 도청하려다 발각된 사건과 연루되어 사임하게 된 '워터게이트 사건'은 미국 전 사회에 커다란 영향을 끼쳤는데, 프라이버시법도 이러한 워터게이트 사건의 영향으로 제정된 법률이다. 동법은 미연방정부를 비롯한 연방공공기관이 공정한 정보사용의 원칙에 맞추어 개인정보를 처리하고 정보주체의 권리를 보장하도록 규정하고 있다. 세부적인 내용은 1973년의 '공정정보관행규약(Code of Fair Information Practices)'[203]을 바탕으로 하여 제정되었으며,

---

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

202) 5 U.S.C. § 552a.

정보주체의 열람·정정요구권, 필요한 범위 내에서의 정보수집원칙, 어떠한 정보가 수집되었는지에 대한 고지의무, 정보공유의 원칙적 금지 등의 내용을 담고 있다. 그러나 동법은 공공기관이 본래의 수집목적과 양립될 수 있는 '일상적인 이용(routine use)'을 위해 해당 개인정보를 공개할 수 있도록 하고 있으며, 특정한 공공기관의 경우 정보 정확성이나 기타 법적 의무로부터 면제되도록 하고 있어 실효성을 가지고 있지 못하다는 비판을 받고 있다.[204]

(2) 금융부문의 프라이버시보호법

금융부문에는「공정신용평가법」[205]과「금융현대화법」[206]의 두 가지 대표적인 개인정보 관련 법률이 적용되고 있다. 공정신용평가법은 신용평가기관(CRA : Credit Reporting Agency)에 의한 개인정보의 오·남용을 막고 개인정보를 보호하기 위해 1970년 제정된 대표적인 개인신용정보보호법이다. 동법의 핵심 내용은 신용평가기관이 개인신용정보의 비밀

---

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

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

205) 15 U.S.C. § 1681 et seq.

206) 15 U.S.C. §§ 6801, et seq.

성과 정확성을 보호하기 위한 '합리적 절차(reasonable procedures)'를 준수할 것을 강제하는 것이다. 동법은 이러한 합리적 절차를 판단하기 위한 기준으로서, 개인의 정보접근권, 개인정보 보안, 개인정보의 파기, 필요한 사항에 대한 고지, 정보주체의 동의, 신용평가기관의 책임성에 관한 내용을 포함하는 공정한 정보관행체계를 규정하고 있는데, 이에 의하면, 신용평가기관은 은행, 신용카드회사, 사용자(회사), 임대업자 등의 사업자가 개인의 신용을 평가하기 위해서만 정보를 사용할 것이라는 합리적인 믿음이 있는 경우가 아닌 한 개인정보를 제공하여서는 안 된다. 한편 지난 12월 4일 미국의 부시 대통령이「공정하고 정확한 신용거래에 관한 법률(Fair and Accurate Credit Transactions Act of 2003)」에 서명함으로써, 내년 1월1일 만료되는 공정신용평가법의 관련 조항이 무기한 연장되었다. 동 법안은 ID도용을 제재하는 주 정부 법령이 연방정부의 관계 법령 범위에서 제정되도록 함으로써 주마다 법률이 다르게 만들어지는 것을 막고 있다.[207]

한편 'Gramm-Leach-Bliley Act(GLBA)'라고도 불리는 금융현대화법은 금융기관에 의해 보유되는 고객의 금융정보를 보호하기 위해 제정된 법률이다. 따라서 은행, 증권회사, 보험회사와 같은 금융기관 및 대부업 등 모든 대출서비스 제공회사, 중개업, 자금전송 또는 보관업, 금융자문이나 신용컨설팅을 제공하는 회사, 채권추심업 등과 같은 기타 금융상품 또는 서비스를 제공하는 모든 회사에 적용된다. 동법은 세 가지 주요한 내용을 담고 있는데, 금융프라이버시에 관한 원칙, 세이프가드 원칙, 프리텍스팅(pretexting) 규정이 바로 그것이다. 금융프라이버시 원칙은 금융기관에 의한 고객의 개인금융정보의 수집 및 이용을 규제하는 것으로, 금융기관으로부터 금융정보를 제공받는 기업(금융기관 여부를 불문)에도 적용된다. 따라서 이에 의하면, 금융기관은 소비자에게 회사의 개인금융정보에 대한 정책을 고지할 의무가 있고, 소비자 개인정보를 이해관계가 없는 제3자에게 제공하여 정보를 공유하기 전에 반드시 소비자에게 이

207) 연합뉴스, "부시, 개인 신용보호법률 서명", 2003. 12. 5일 기사 참조.

사실을 알리고 반대할 권리를 부여하여야 한다. 세이프가드 원칙은 모든 금융기관이 소비자의 정보를 보호하기 위한 안전장치를 고안하고 시행하며 유지할 것을 요구하는 것이다. 이 원칙은 소비자로부터 직접 정보를 수집하는 금융기관 뿐 아니라 다른 금융기관으로부터 고객 정보를 받는 신용평가회사 등의 금융기관에도 적용된다. 프리텍스팅 규정은 소비자를 속여서 개인의 금융정보를 취득하는 개인 또는 기업으로부터 소비자를 보호하기 위한 규정이다.[208]

(3) 통신부문의 프라이버시보호법

통신부문에 적용되는 대표적인 법률로는「케이블통신정책법」[209]과「전자통신프라이버시법」[210]이 있다. 1984년 미 의회는 케이블TV 기술의 진보, 특히 양방향 케이블 시스템의 개발은 부당한 개인정보의 수집을 불러올 위험에 대비하여 케이블통신정책법을 제정하기에 이르렀다. 동법은 케이블을 통해 서비스를 제공하는 사업자에게 여러 가지 의무를 부과하고 있다. 첫째, 동법은 케이블통신회사에게 적어도 1년에 한 번씩 고객에게 자사의 개인정보 수집 및 보유현황에 대해 고지토록 강제하여, 고객이 사업자의 개인정보 수집 및 이용을 제한할 수 있는 기회를 가질 수 있도록 하고 있다. 케이블통신회사가 고지하여야 할 내용으로는 수집목적, 수집되는 정보의 내용, 개인정보의 공개가 예상되는 경우, 보유기간, 개인정보 열람요구 절차 등에 관한 사항이다. 또한 동법에 의하면 고객에 관한 정보는 고객의 사전 동의없이 이용되거나 제3자에게 제공될 수 없다. 단, 서비스의 제공에 관한 합법적인 영업활동과정에서 이루어진 정보의 공개는 예외이다.[211]

---

208) *"In Brief : The Financial Privacy Requirements of the Gramm-Leach-Bliley Act"* ; *"Financial Privacy : The Gramm-Leach Bliley Act"* (미연방거래위원회 웹사이트, www.ftc.gov 참조)

209) 47 U.S.C. § 551.

210) 18 U.S.C. § 2701 et seq.

한편 전자통신프라이버시법은 전자기록에 관한 정부의 접근절차 및 방법에 대하여 통제함으로써, 전자기록의 비밀성을 보호하는 규칙을 확립하고 있다. 1986년 제정된 동법은 수색영장이나 수신자의 동의 없이 서신을 개봉하는 것을 금지하는 법률[212] 및 당사자 동의 없는 전화, 데이터 전송, 라디오 통신의 차단 또는 도청장치의 사용을 금지하는 법률[213]의 통신프라이버시보호의 내용을 전자메일이나 기타 컴퓨터를 통한 데이터 전송과 같은 새로운 통신분야에 확장시킨다는 의미를 가진다. 특히 동법은 저장된 '음성메일(voice mail)' 및 이메일에 대한 권한없는 접근이나 이용을 금지하고, 이러한 저장된 이메일 등의 내용을 해당 전자통신서비스제공자가 외부에 공개하지 못하도록 금지하고 있다. 이러한 금지규정을 위반한 자는 형사상 제재를 받음은 물론, 고의적이거나 의도적인 위반행위로 인해 피해를 입은 자는 민사소송을 통해 금지명령 등의 피해구제를 청구하거나 금전적 배상을 요구할 수 있다.[214]

(4) 가족의교육권및프라이버시에관한법률(FERPA)

1974년 제정된「가족의교육권및프라이버시에관한법률」[215]은 '버클리수정법(Buckley Amendment)'으로도 잘 알려져 있는 연방법으로서, 학생의 교육정보에 대하여 학부모와 학생의 자기정보결정권을 강화하고 프라이버시의 관점에서 교육정보를 보호하기 위해 제정된 법이다. 동법은 학교 등의 교육기관이 연방기금을 교부받지 못하게 되는 몇 가지 사항을 적시하고 이에 대한 감독권을 교육부에 부과함으로써 학생 및 학부모의 교육정보에 대한 권리를 보장하고 있다. 즉, 연방기금의 교부조건으로 정

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

212) 39 U.S.C. § 3623.

213) 18 U.S.C. §§ 2510 et seq. ; 47 U.S.C. § 605.

214) Ronald L. Plesser/Sheldon Krantz, *"Privacy and Related Issues"*, 「Internet and Online Law」(Kent D. Stuckey with Contributing Authors)」, Law Journal Press, 2000, § 5.02, pp. 5-8~9 참조.

215) 20 U.S.C. § 1232g.

보처리자인 학교 등의 교육기관이 교육정보를 수집·이용·보유·공개 등 처리하는 과정에 있어 지켜야할 몇 가지 의무를 부과하고 있기 때문에, 연방기금을 계속해서 교부받고자 하는 교육기관은 동법에서 규정하고 있는 의무를 준수하여야 한다. 동법에 의하면, 학생 또는 학부모는 학교 등의 교육기관이 보유하고 있는 자신 또는 아동의 교육정보에 대해 조사·심사하고 이를 통해 잘못된 내용이 있으면 정정을 요청할 수 있으며 나아가 개인식별정보(personally identifiable information)의 공개를 중지토록 요구하는 등의 권리를 행사할 수 있다. 또한 학교 등의 교육기관은 '교육기록 내 개인식별정보'를 학생 또는 학부모의 서면 동의없이 공개할 수 없으며, 학교가 유지·관리하고 있는 교육정보에 대해 자격있는 학생 및 학부모에게 고지하여야 한다.

(5) 비디오프라이버시보호법

「비디오프라이버시보호법」[216]은 비디오테이프 판매사업자 또는 대여사업자가 개인정보를 포함한 비디오 대여기록을 고객의 동의 또는 법원의 승인 없이 제3자에게 제공하는 것을 금지함으로써 상업 비디오테이프 이용자 또는 구매자의 프라이버시권을 보호하고 있다. 동법은 다음과 같은 경우에는 위와 같은 개인정보를 포함한 비디오 대여기록정보의 공개를 일부 허용하고 있다.

- o 당해 비디오를 빌려준 소비자에게 공개하는 경우
- o 소비자의 서면동의가 있는 경우
- o 연방형사법원 영장 및 관할 주법원 영장, 대배심 영장(grand jury subpoena) 또는 특별한 지침에 따른 법원 명령에 의한 공개의 경우
- o 제3자에게 비디오 대여자의 이름과 주소만 공개된다고 할 때, 이에 대해 해당 소비자가 반대할 기회를 가졌던 경우

216) 18 U.S.C. § 2710.

o 정보의 공개가 채권추심 등과 같이 비디오 대여사업자의 일상적인 영업행위 과정에서 부수적으로 발생하는 것일 경우
o 민사법원의 명령에 의한 경우

동법에 의하면, 비디오 대여사업자가 동법에 위반하였다고 주장하는 소비자는 언제든지 민사소송을 통해 손해배상을 청구할 수 있다. 또한 불법적으로 획득된 비디오 대여기록 정보는 모든 법원 소송에서 증거로 사용될 수 없으며, 이는 일정기간 안에 파기되어야 한다.[217]

(6) 아동온라인프라이버시보호법(COPPA)

「아동온라인프라이버시보호법」[218]은 13세 미만 아동의 개인정보를 온라인으로 수집하는 행위를 엄격히 제한하고 있는 법률이다. 동법의 적용을 받는 웹사이트는 13세 이하의 아동과 직접적으로 관련된 서비스를 제공하는 상업적 웹사이트 운영자 뿐 아니라 모든 일반인을 대상으로 한 서비스를 제공하더라도 13세 미만의 아동으로부터 개인정보를 수집하는 모든 웹사이트이다.

동법의 적용을 받는 웹사이트는 반드시 홈페이지에 프라이버시정책을 고지하고 개인정보 수집하는 페이지에 프라이버시 정책이 링크되도록 하여야 한다. 또한 웹사이트의 정보수집정책에 대해 부모에게 고지하고 아동으로부터 개인정보를 수집하기 전 부모의 명확한 동의를 구하여야 한다. 또한 접근권을 보장하여 부모에게 아동의 개인정보가 제3자에게 제공되도록 허락할 것인지 여부를 선택하거나 개인정보를 삭제할 기회를 보장하여야 한다. 또한 인터넷 웹사이트 운영자는 인터넷 게임이나 설문조사 등 기타 활동에 아동이 참여할 때 그러한 활동에 참여하는 데 합리

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

218) 15 U.S.C. § 6501 et seq.

적으로 필요한 수준 이상으로 더 많은 개인정보를 제공하여서는 안 되며, 아동으로부터 수집한 개인정보의 비밀성, 안전성, 무결성을 유지하기 위한 노력을 기울여야 한다.[219]

다. 미국의 개인정보보호기구

미국은 개인정보보호를 위한 별도의 전담기구는 없다. 다만, 공공부문과 민간부문에서 예산관리국(OMB : The Office of Management and Budget)과 연방거래위원회(FTC : The Federal Trade Commission)가 각각 개인정보보호기구로서의 역할을 담당하고 있을 뿐이다.

먼저 공공부문에 있어서는 예산관리국[220]이 「1974년 프라이버시법」에 따라 연방정부의 프라이버시 또는 개인정보보호 정책을 정립하는 역할을 맡고 있다. 그러나 예산관리국은 우리나라의 기획예산처와 같이 예산편성과 운용 등 국가재정운영 전반에 관한 정책을 수립하고 집행하는 역할을 하는 기구인 바, 프라이버시 보호와 관련하여서도 예산관리차원에서만 제한적인 역할을 맡고 있을 뿐이다. 한편 민간부문에 있어서는 연방거래위원회가 아동의 온라인 프라이버시, 소비자신용정보, 공정한 거래관행과 관련하여 개인정보 또는 프라이버시를 보호하는 법률을 집행하고 준수여부를 감독할 권한을 부여받아 행사하고 있다.

이렇듯 미국에는 포괄적인 개인정보보호기구는 없다. 다만, 민간부문에서 소비자보호의 일환으로 소비자 프라이버시보호의 기능을 함께 맡고 있는 연방거래위원회의 역할을 참고할 수 있을 것이다.

---

219) FTC, "*Children's Privacy : The Children's Online Privacy Protection Act*", http://www.ftc.gov

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

(1) FTC의 설립 및 구성

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

FTC는 대통령에 의해 임명되는 5인의 위원으로 구성되며, 동 위원의 임기는 7년이다. FTC의 조직은 총 4개 부서로 나뉜다. 일반자문부서(The Office of the General Counsel), 경쟁국(The Bureau of Competition), 경제담당국(The Bureau of Economics), 소비자보호국(The Bureau of Consumer Protection)이 그것이다. 일반자문부서는 위원회에 기관의 관할과 권한에 대한 정보를 제공하고 자문관은 위원회의 법적 대리인으로 활동한다. 경쟁국은 사업자간 과도한 경쟁을 억제하여 잘못된 업무관행을 방지토록 하고 있다. 경제담당국은 FTC의 행위가 경제에 미치는 영향을 연구한다. 마지막으로 소비자보호국은 불공정하고 부당한 사업관행으로부터 소비자를 보호하는 역할을 담당하고 있다. 현재 FTC는 약 1,000여명의 직원이 있으며, 이들 중 500명 이상은 변호사이고 20명 정도는 경제학자이다.

(2) FTC의 개인정보보호 기능 및 역할

FTC의 주요 임무는 과도한 제한을 가하지 않은 상태에서 시장기능이 효율적으로 작동되고 적절한 경쟁관계를 유지하도록 함으로써 불공정한 사업관행으로부터 자국의 소비자를 보호하는 것이다. 이는 개인정보와 관련해서도 마찬가지이다. 따라서 FTC는 개인정보 및 프라이버시의 중요성을 사업자와 소비자에게 알리는 역할을 하고 있고, 더 나아가 법위반행위나 불공정한 사업관행에 대해 모니터링을 하거나 조사권을 행사한

다. 또한 BBBOnLine이나 TRUSTe와 같은 자율규제 차원의 민간 프라이버시 단체로부터 법률이나 가이드라인을 준수하지 않는 사업자에 대한 보고(referral)를 받아 실질적인 제재조치를 취하기도 한다.

FTC가 잘못된 개인정보 처리관행을 가진 사업자를 제재하고 소비자의 개인정보를 보호하기 위한 근거조항으로 삼고 있는 것은 「연방거래위원회법(Federal Commission Act)」[221] 제5조이다. 동 조항은 '영리활동과정에서의 불공정하거나 사기적인 행위 또는 관행(unfair or deceptive acts or practices in or affecting commerce)'을 금지하고 있다. 따라서 만약 웹사이트 운영자가 자사 웹사이트에 고지된 프라이버시 정책을 준수하지 않았거나 적용을 받는 일체의 자율규제 차원의 가이드라인을 이행하지 않은 경우에는 사기적 수단 중 하나인 허위사실의 공언(misrepresentation)에 해당되어 FTC의 제재를 받을 수 있다.[222] 또한 아동과 관련된 개인정보의 수집 및 이용관행 또는 금융기록이나 의료기록과 같은 민감한 정보의 이용관행이 터무니없이 불공정한 경우에도 FTC는 동법 제5조를 적용하여 법위반행위로 보고 있다.[223] 이는 FTC가 개인정보보호와 관련하여 「금융현대화법」,「공정신용평가법」,「아동온라인프라이버시보호법」등에 대해 관장하고 있기 때문이다. 금융현대화법에 따라, 위원회는 금융

---

221) 15 U.S.C. §§ 41~58.

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

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

프라이버시의 중요성을 알리는 규범 및 금융기관에서의 개인정보의 행정적·기술적·물리적 안전조치를 확보하는 규범을 실행하고 있으며, 공정신용보고법 및 아동온라인프라이버시보호법에 따라 소비자를 보호하는 각종 역할을 맡고 있다.

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

이 외에도 FTC는 스팸메일 규제, 광고성 전화에 대해 소비자의 선택권을 부여하기 위한 광고성 전화거부 등록부(National Do Not Call Registry)의 운영, 신분도용 규제 등의 활동을 펼치고 있으며, 관할 영역에 대해 공정한 거래관행 규칙[224]을 제정하여 사업자들이 이를 준수토록 하는 역할을 맡고 있다.

라. 개인정보피해구제 절차 및 방법

미국에서 잘못된 관행이나 부주의한 개인정보의 취급 또는 고의적인 개인정보 오·남용으로 인해 피해를 입은 자가 그러한 피해를 구제받기 위한 방법은 크게 세 가지로 볼 수 있다. 가장 대표적인 방법은 역시 소송을 통한 피해구제방법이다. 앞서도 언급하였지만, 미국 판례는 프라이버시 침해를 불법행위로 인정하여 피해자가 입은 경제적·정신적 손해에

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

대한 배상청구를 인정함은 물론 징벌적 손해배상청구나 침해행위금지청구도 함께 인정하고 있기 때문에, 소송에 의하는 것이 가장 확실한 피해구제 방법 중 하나가 되고 있다.

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

(1) 민간분쟁해결제도

다른 사람들과의 다툼이나 분쟁, 특히 송사(訟事)에 휘말리는 것을 꺼리는 우리나라의 풍토와는 달리, 미국 사람들은 분쟁이 발생하였을 경우 적극적으로 자신의 권익을 주장하여 관철시키려는 경향이 강하다. 따라서 미국에서는 자연스럽게 소송제도 뿐 아니라 분쟁을 해결하기 위한 다양한 소송외적 해결제도가 발달해왔다. 또한 소송외적 분쟁해결제도의 발달 배경에는 업계의 자율규제를 장려하고 촉진하는 미국의 접근방식도 빠뜨릴 수 없다. 미국에서는 사업자 단체가 자율적으로 독립·비영리 민간단체를 설립하여 실행규약이나 원칙을 마련하고, 이러한 기준에 맞춰 소비자가 신뢰할 수 있는 사업자에게 신뢰마크(Trustmark)를 부여하는 자율규제가 활성화되어 있다. 이러한 신뢰마크 체계는 당해 마크를 제공하는 곳의 분쟁해결제도를 사업자가 반드시 이용하도록 하기 때문에, 실질적으로 사업자가 실행규약을 준수하고 분쟁해결절차에 적극적으로 참여하며 그 결과에 순응할 수 있도록 하는 실효성을 가지게 된다.[225]

225) Julia Hörnle, "*Online Dispute Resolution in Business to Consumer E-commerce Transactions*", Journal of Information Law & Technology, http://elj.warwick.ac.uk/

이러한 민간단체를 통한 소송외적 분쟁해결제도는 개인정보와 관련한 분쟁의 해결에 있어서도 중요한 역할을 담당하고 있다. 그 중에서도 특히 개인정보보호와 관련한 미국의 민간분쟁해결제도에 대해서 말하자면, BBBOnLine을 언급하지 않을 수 없다.[226] BBBOnLine의 소송외적 분쟁해결제도는 기본적으로 온라인상 소비자와 사업자의 신뢰구축과 개인정보보호라는 목적으로 마련된 '프라이버시 씰 프로그램(Privacy Seal Program)'[227]의 일환으로 운영되고 있다. 따라서 동 프로그램에 참여하고 있는 인터넷서비스제공자가 프라이버시 인증마크를 표시할 수 있는 자격을 부여받기 위해서는 BBBOnLine의 분쟁해결절차에 참여하여야 할 의무가 있다. 이러한 소송외적 분쟁해결제도는 주로 온라인을 통한 분쟁해결방법(ODR : Online Dispute Resolution)으로 운영되고 있다.

이하에서는 BBBOnLine의 이러한 온라인 분쟁해결절차와 방법을 자세하게 살펴볼 수 있을 것이다.[228] 먼저 BBBOnLine의 개인정보분쟁해결절차도는 아래와 같다.

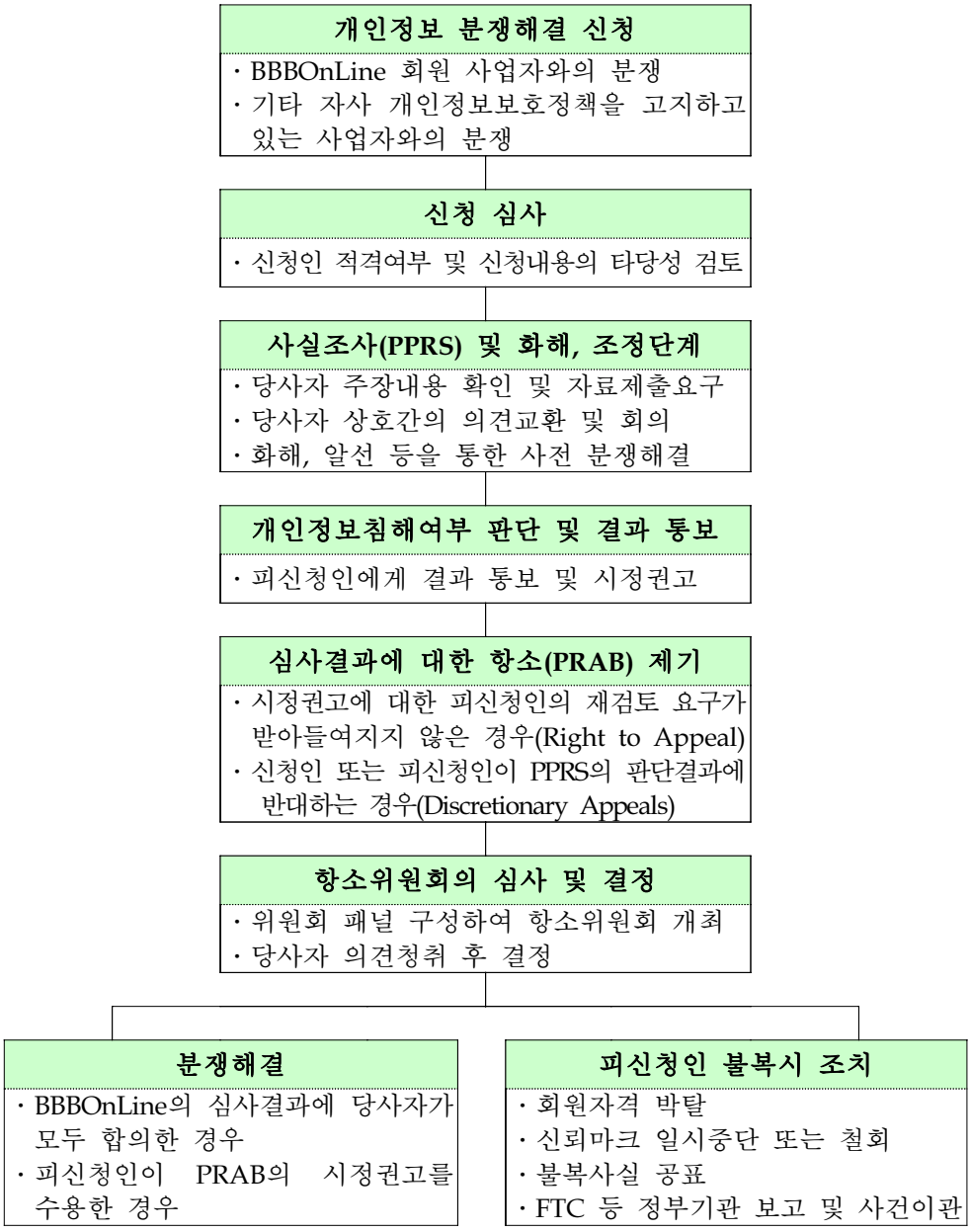
---

jilt/02-2/hornle.html.

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

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

228) BBBOnLine의 분쟁해결절차 및 방법은 BBBOnLine, *"BBBOnline Privacy Program, Dispute Resolution Process Procedures - Privacy Policy Review Service and Privacy Review Appeals Board"*, 1999. 2. 11, http://www.bbbonline.org/privacy/dr.pdf 참조.



(그림 4-8) BBBOnLine의 피해구제 절차도

위와 같이 BBBOnLine의 개인정보분쟁해결 절차는 분쟁해결신청, 사실조사, 심사 및 판단, 항소, 최종결정의 단계로 이어진다. 이를 단계별로 자세히 살펴보면 다음과 같다. 먼저, BBBOnLine의 프라이버시 프로그램 가입회원인

사업자가 BBBOnLine이 제정한 프라이버시 가이드라인을 위반하여 소비자가 피해를 입었거나, BBBOnLine의 회원이 아니더라도 개인정보를 수집하여 이용하는 조직 또는 개인이 자신의 개인정보보호정책을 고지하고 있는데 이를 위반하여 정보주체가 피해를 입은 경우, 이들은 BBBOnLine에 분쟁해결을 신청할 수 있다. BBBOnLine은 사건 신청을 접수받으면 우선 신청인의 적격여부와 신청내용의 타당성을 검토한다.[229] 이러한 과정을 거쳐 사실조사가 필요하다고 판단되는 사건은 '프라이버시 정책심사(PPRS : Privacy Policy Review Service)' 단계로 이관된다. 이 단계는 주로 신청인과 피신청인의 주장내용을 확인하고 증거자료를 제출받아 사실관계를 명확히 하는데 초점이 맞춰져 있다. 또한 양 당사자가 서로의 주장과 의견을 확실히 인식할 수 있도록 하여 분쟁이 원만히 해결될 수 있도록 하고 있다. 따라서 일방 당사자가 제출한 답변자료는 다른 당사자에게 제공되어 서로의 의견을 교환하는 과정을 거치며, 필요한 경우 당사자의 합의를 기초로 회의를 개최하기도 한다.

또한 BBBOnLine은 사실조사가 완료되면 그 결과 및 권고내용을 피신청인에게 제출하여 의견을 듣게 된다. BBBOnLine은 필요한 경우 피신청인에 시정을 요구하는 내용을 권고할 수 있는데, 이 경우 피신청인은 시정권고의 재검토를 요청할 수 있고 받아들여지지 않을 때는 '프라이버시 심사 항소 위원회(PRAB : Privacy Review Appeals Board)'에 항소할 수 있다. 항소 단계는 프라이버시 정책심사 단계에서 이루어진 결정 내용에 반대하는 신청인 또는 피신청인이 모두 신청할 수 있는데, 여기에는 재량적 항소(Discretionary Appeals)와 항소권(Right to Appeal)의 두 가지 유형이 있다.

---

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

［표 4-23］ BBBOnLine의 항소 유형

구분	재량적 항소	항소권
주체	BBBOnLine의 프라이버시 프로그램 회원을 대상으로 이의를 제기한 신청인 및 그 피신청인	BBBOnLine의 프라이버시 프로그램 회원인 피신청인
대상	프라이버시 정책심사의 결정내용	시정조치가 포함된 프라이버시 정책심사의 결정내용
허용 결정	항소 허용여부를 프라이버시심사 항소위원회가 결정	항소 허용여부 결정 불필요

※ 주 : 이은선, 앞의 글, 300면.

BBBOnLine은 항소가 허용될 경우, 항소위원회의 패널을 구성하여 당사자 의견청취(hearing)를 거친 후 신속하게 결정을 내린다. 그러나 만약 피신청인이 항소위원회의 시정조치 결정에도 불복할 경우, BBBOnLine은 ① 회원자격의 박탈, ② 신뢰마크의 일시 중단 또는 철회, ③ 피신청인의 불복사실 공표, ④ 정부기관에 사건 이관 등과 같은 조치를 취하여 분쟁해결의 실효성을 담보할 수 있다.[230]

일반적으로 BBBOnLine에 제기되는 개인정보 관련 사건은 메일링 리스트 또는 마케팅 목적을 위해 구축한 데이터베이스 상에서의 개인정보 삭제요구에 대한 무응답, 개인정보에 대한 접근요청 거절 등 주로 정보주체의 권리행사에 대한 피신청인의 거부나 미조치에 관한 내용이다. 올 9월까지 BBBOnLine에는 총 1,032건의 사건이 접수되었다. 이 중 단순 상담 및 질의가 516건이었고, 신청 부적격으로 종결된 사건이 485건으로 다수를 차지하고 있다. 그 외는 적격성 여부를 결정 중인 사건이 15건, 신청적격성이 인정되어 진행 중인 사건이 8건, 결정전 합의가 이루어진 사건이 8건이다.[231]

---

230) BBB/CBBB/BBBOnLine, *"Protecting Consumers in Cross-Border Transactions : a Comprehensive Model for Alternative Dispute Resolution"*, CBBB, 2000, p. 12.

231) BBBOnLine 웹사이트(http://www.bbbonline.org/privacy/dr/2003q3.asp) 참조.

(2) FTC의 개인정보피해구제 절차 및 방법[232]

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

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

이렇게 이의제기가 접수되면 FTC는 연방위원회법 제3조에 의거하여 임무수행에 필요한 각종 질의(inquiry)를 행할 수 있고 관련된 정보를 수집할 수 있으며 때때로 관할 영역에 대해 조사(investigate)할 수 있는 권한을 가진다. 특히 FTC의 소비자보호국(Bureau of Consumer Protection)은 개인정보침해 등 소비자보호와 관련된 사건을 조사하기 위해 '민사적 조사요구권(CIDs : civil investigative demands)'[233]을 행사할 수 있다. FTC는 민사적 조사요구권 행사를 통해 사건과 관련된 증거서류를 제출

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

233) 1980년 이전에는 소비자보호국도 조사를 위한 영장(subpoena)을 이용하였는데, 연방거래위원회진흥법(FTC Improvements Act of 1980)의 제정에 따라 새롭게 추가된 조항으로 인해 현재는 민사적 조사요구권만을 행사할 수 있게 되었다. 영장조사는 주로 경쟁국(Bureau of Competition)에서 행하는 조사방법이며, 영장을 통한 조사와 민사적 조사요구권(CIDs)에 의한 방법은 조사 범위에서도 다소 차이가 있다.

받고 구두 증언을 얻을 수 있으며, 당사자에게 질문에 대한 서면 응답 또는 보고서를 제출토록 요구할 수 있다.[234] 그러나 이러한 FTC의 조사 명령이 부당하다고 생각하는 사업자나 기타 조직은 지명위원(designated Commissioner)에게 취소청구(petition to quash)를 제출하여 이의를 제기할 수 있고, 지명위원의 결정에 대해서는 다시 전원위원회에서 이의를 제기할 수 있다.[235] 그러나 당사자가 취소청구를 하지 않은 채 조사권에 불응한 경우, FTC는 해당 지역의 관할 법원에 이행청구를 할 수 있고 법원은 당사자에게 조사에 응하도록 요구하는 명령을 내릴 수 있다. 법원의 이러한 이행명령(enforcement order)을 따르지 않을 경우에는 법정모독죄로 벌금이 부과될 수 있다.[236]

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

먼저 행정절차상의 조치를 살펴보면, FTC는 사업자의 위법사실이 있다고 믿을 만한 근거가 발견되면 바로 행정제재를 내리지 않고 사건을 검토하여, 해당 사업자에게 위법사실과 그에 따른 사업자 부담조치(charges)를 규정한 문제제기 서류를 제출한다. 사업자가 FTC의 이러한 부담조치를 자발적으로 수용하기로 한 경우, 양 당사자는 위 부담조치를 FTC의 최종명령(final order)으로 보고 위법사실에 대한 모든 소권(訴權)을 포기한다는 내용의 합의를 할 수 있다. 일종의 시정권고를 통한 당사자 합의로써 업계의 자율규제를 중시하는 FTC의 입장을 확인할 수 있는 부분이다. 그러나 사업자가 FTC의 부담조치를 따르지 않을 경우에는 심

---

234) 15 U.S.C. § 57b-1(c)(1).

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

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

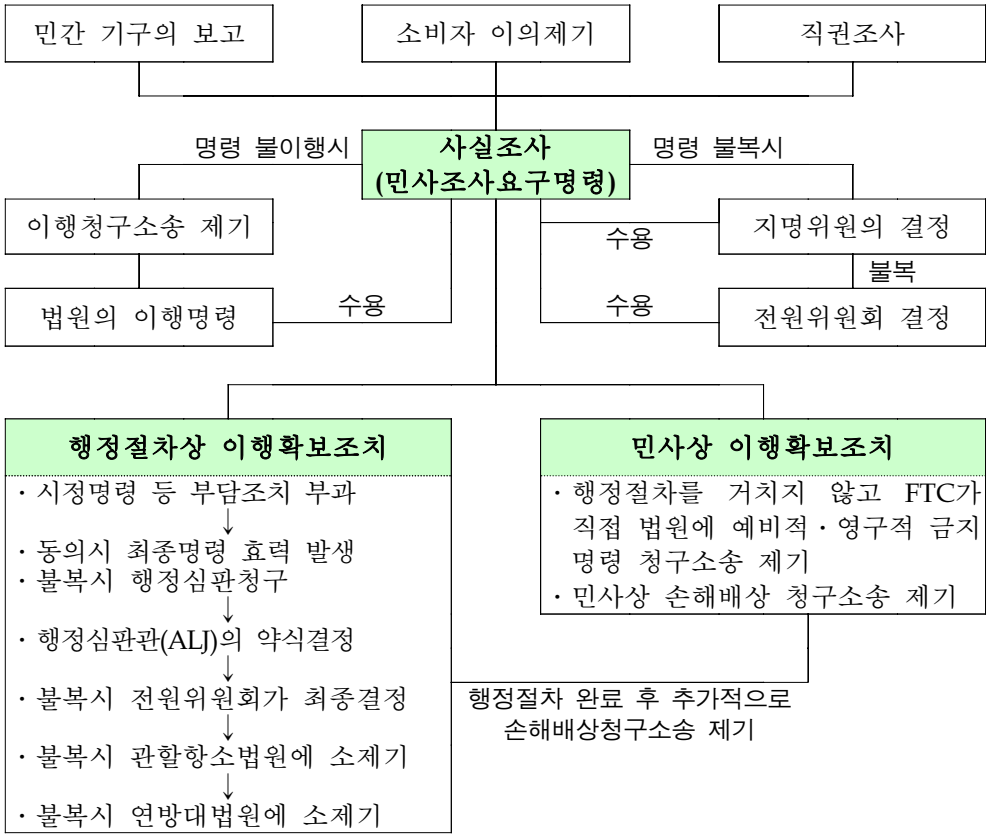
판절차(trial-type proceeding)를 통해 행정심판관(ALJ : administrative law judge)이 그 당부를 결정한다. 행정심판관은 심문을 통해 사실조사 내용과 법위반 여부에 대한 '약식 결정(initial decision)'을 내리고 FTC에 대하여 문제제기를 중단하거나 취소할 것을 명령할 수 있고 또 그 반대일 수도 있다. 행정심판관의 결정은 전원위원회에 회부되어 재심사될 수 있으며 전원위원회는 최종 결정과 명령을 내리게 되는데, 만약 사업자가 전원위원회의 결정에 불복하는 경우에는 관할 항소법원에 이의를 제기할 수 있다. 항소법원이 FTC의 최종결정을 확정하는 경우, 법원은 FTC의 부담조치 이행명령을 내릴 수 있다. 사업자가 항소법원의 결정에도 불복할 때에는 연방 대법원에 소를 제기하여야 한다.

FTC가 내리는 명령은 사업자의 특별한 이의제기가 없어 전원위원회 또는 법원에서 심사중인 경우가 아닌 한, 명령이 내려진 후 60일이 지나면 최종적인 명령으로 결정되어 당사자를 구속하게 된다. 따라서 만약 사업자가 최종명령을 위반할 경우에는 개개 위반행위마다 최고 11,000달러의 민사 범칙금(civil penalty)이 부과될 수 있다. 이러한 과태료의 액수는 FTC가 제기하는 명령 이행청구소송에서 법원이 결정하며, 법원은 또한 '강제 금지명령' 및 적절하다고 판단되는 '기타 형평에 맞는 추가적인 구제조치명령'을 내릴 수 있다.[237] 또한 FTC는 명령에 대한 사법심사가 모두 완료된 이후 추가적으로, 관할지방법원에 행정소송절차에서 문제가 된 사업자의 불법행위로 인해 소비자가 입은 피해의 구제를 위한 민사상 손해배상청구를 할 수 있다.

이러한 행정적 피해구제제도는 FTC가 사업자와의 협의를 통해 사전 합의에 이를 수 있는 기회를 줄 수 있고, 또한 사실관계나 법적인 문제가 복잡한 사안은 보다 철저히 조사할 수 있다는 장점이 있다. 그러나 계속해서 항소가 이어지게 되면 신속한 피해구제가 어렵다는 단점 또한 가지고 있다. 이에 최근에 FTC는 이러한 행정절차를 거치지 않고 바로 민사소송을 통해 예비적·영구적 금지명령(preliminary and permanent

237) 연방거래위원회법 제5(1)조.

injunctions) 청구소송을 제기하는 방법도 적극 활용하고 있다. FTC는 사업자가 '위법행위를 하였거나 또는 위법행위를 하려고 한다고 믿을 만한 이유'가 있는 경우, FTC의 행정절차를 통해 해당 행위가 불법하다는 최종적인 결론을 내리지 않았다 하더라도 법원에 그 위법성을 주장하여 금지청구를 할 수 있다. 또한 '적절한 경우'에는 영구적인 금지청구를 제기할 수도 있다.[238] 특히, 복잡한 행정절차를 거치지 않고 바로 민사소송을 제기하는 경우 위와 같은 금지청구 뿐 아니라 소비자가 입은 피해에 대한 금전적인 구제조치도 한꺼번에 해결할 수 있다는 점에서 최근 FTC는 소비자보호와 관련된 여러 문제들에 이러한 피해구제절차를 선호하고 있다.



(그림 4-9) FTC의 피해구제 절차도

238) 연방거래위원회법 제13(b)조.

2. 캐나다

캐나다는 1960년대 후반, 컴퓨터의 보급 확장과 더불어 프라이버시에 대한 논의가 함께 진행되면서 개인정보보호를 위한 법제도를 정비하기 시작하였다. 1969년 캐나다 연방 통신부와 법무부는 공동으로 프라이버시에 관한 연구를 시작하여 1972년 '프라이버시와 컴퓨터(Privacy and Computers)'라는 보고서를 발행한 바 있는데, 당시 이 보고서는 기존의 「캐나다 인권법(Canadian Human Rights Act)」의 적용범위를 확대하여 개인정보에 대해서도 포괄적으로 보호할 수 있는 일반적 근거를 마련하고, 세부적으로는 개인정보에 관한 별도의 입법을 제정할 필요가 있다고 제안하였다. 이 보고서에서 제안한 내용은 1977년 공공부문에서의 개인정보보호에 관한 내용을 담은「개인정보보호규칙(Protection of Personal Information Regulations)」이 캐나다 인권법에 의거하여 제정됨으로써 구체화되었다.

이후 1980년대 들어 본격적으로 공공부문의 개인정보보호를 위한 별도의 법률이 제정되었으며, 동법의 시행에 책임을 지는 개인정보보호기구도 설립되었다. 또한 21세기에 이르러서는 날로 발달하는 정보처리기술과 인터넷의 도입으로 인한 전자상거래의 급증으로 인하여, 이러한 특성을 반영하는 민간영역에 적용되는 새로운 개인정보보호법이 제정되었다.

오늘날 캐나다는 공공과 민간영역에 적용되는 별도의 입법체계를 잘 정비하여 시행하고 있으며, 개인정보침해로 인해 피해를 입은 시민들의 권리를 보호하고 구제해주기 위한 제도적 장치도 잘 마련되어 있어 개인정보보호 선진국으로 인정받고 있다.

가. 개인정보보호 법제현황

캐나다 연방은 유럽과 같이 공공영역과 민간영역에 모두 적용되는 개인정보보호 기본법을 가지고 있지 않고, 두 부문에 각각 적용되는 별도

의 입법을 제정하여 시행하고 있다. 또한 연방차원과는 별도로 각 주에서도 개인정보 관련 법률을 제정하여 시행하고 있다. 다만, 각 주 차원에서는 주 정부나 공공기관에 의해 처리되는 개인정보를 보호하기 위한 공공부문에 적용되는 법률만 제정되어 있는 것이 일반적이다. 캐나다의 개인정보보호법 현황을 표로 살펴보면 다음과 같다.

〔표 4-24〕 캐나다의 개인정보보호 법제현황

구분	법률
연방	· 프라이버시법(Privacy Act) · 개인정보보호및전자문서에관한법률(Personal Information Protection and Electronic Documents Act)
Alberta	· 정보공개및프라이버시보호에관한법률(Freedom of Information and Protection of Privacy Act) · 개인정보법(Personal Information Act)(2003 법안 44 - 현재 미시행) · 건강정보법(Health Information Act)
British Columbia	· 정보공개및프라이버시보호에관한법률(Freedom of Information and Protection of Privacy Act) · 개인정보법(Personal Information Act)(2003 법안 38 - 현재 미시행)
Manitoba	· 정보공개및프라이버시보호에관한법률Freedom of Information and Protection of Privacy Act · 개인건강정보법(Personal Health Information Act)
New Brunswick	· 개인정보보호법(Protection of Personal Information Act) · 정보권리에관한법(Right to Information Act) · 정보공개에관한법(Freedom of Information Act) · 프라이버시법(Privacy Act)
New foundland	· 프라이버시법(Privacy Act) · 정보공개법(Freedoom of Information Act)
Northwest Territories	· 정보접근및프라이버시보호에관한법률(Access to Information and Protection Privacy Act)
Nova Scotia	· 정보공개및프라이버시보호에관한법률(Freedom of Information and Protection of Privacy Act)
Nunavut	· 정보접근및프라이버시보호에관한법률(Access to Information and Protection Privacy Act)
Ontario	· 정보공개및프라이버시보호에관한법률(Freedom of Information and Protection of Privacy Act) · 수도지역의정보공개및프라이버시보호에관한법률(Muncipal Freedom of Information and Protection of Privacy Act)

Prince Edward Island	· 정보공개및프라이버시보호에관한법률(Freedom of Information and Protection of Privacy Act)
Quebec	· 공공기관에의해보유되고있는문서에관한접근및개인정보보호에관한법률(Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information) · 민간영역의개인정보보호에관한법률(Act Respecting the Protection of Personal Information in the Private Sector)
Saskatchewan	· 정보공개및프라이버시보호에관한법률(Freedom of Information and Protection of Privacy Act) · 지방의정보공개및프라이버시보호에관한법률(Local Freedom of Information and Protection of Privacy Act) · 프라이버시법(Privacy Act) · 공공공개법(Public Disclosure Act) · 건강정보보호에관한법률(Health Information Protection Act)(아직 시행되지 않음)
Yukon	· 정보접근및프라이버시보호에관한법률(Access to Information and Protection of Privacy Act)

나. 개인정보보호법의 주요내용

앞서 살펴본 바와 같이, 캐나다에서는 연방과 주에서 각각 개인정보관련 법률을 제정·시행하고 있지만, 여기서는 연방차원의 대표적인 개인정보관련 법률인 「프라이버시법(The Privacy Act)」과 「개인정보보호및전자문서에관한법((PIPEDA : The Personal Information and Electronic Documents Act))」에 대해서 살펴보기로 한다.

(1) 프라이버시법

공공부문에 적용되는 연방 차원의 개인정보보호법은 1982년 제정된 「프라이버시법(The Privacy Act)」이다. 동법은 공공기관에 의한 정보처리 과정에서 발생할 위험이 있는 개인정보 침해가능성에 대비하고, 공공기관에 의해 보유되고 있는 자신의 개인정보에 접근할 수 있는 시민들의 권리를 보장하기 위한 목적으로 제정되었다.

동법은 연방공공기관에 의해 보유되고 있는 개인정보의 수집・이용・공개 및 개인정보에 관한 정보주체의 접근권에 대하여 규율하고 있다. 이에 의하면, 공공기관은 기관의 운영・계획・활동과 직접적으로 관련이 없는 한 개인정보를 수집하여서는 안 되며 개인정보를 수집할 때에도 가능한 정보주체로부터 직접 수집하여야 한다.[239] 또한 본래의 행정목적을 벗어나 정보주체의 동의 없이 개인정보를 이용하거나 제3자에게 제공하여서는 안 되며, 행정목적으로 처리되고 있는 개인정보는 정보주체의 접근권을 보장하기 위하여 일정기간 보유하여야 한다.[240]

특히 동법은 공공기관에 의해 보유되고 있는 개인정보에 대한 정보주체의 접근권을 보장하기 위하여 상세한 규정을 두고 있다. 즉, 정보주체는 각 정부 부처의 개인정보은행(Personal Information Bank)[241]에서 보유되고 있는 개인정보에 대하여 접근할 권리, 오류 등의 정정을 요구할 권리, 정보접근권이 거부당하였을 때 그 내용을 해당 정보에 첨부하도록 요구할 권리 등을 행사할 수 있다. 정보주체는 해당 개인정보은행을 구체적으로 명시하여 서면으로 정부 부처에 접근요청을 할 수 있으며, 각 정부부처는 접근요청을 받은 후 30일 이내에 그 가부에 대하여 통보하여야 한다.

정보주체는 이러한 자신의 개인정보에 대한 접근권이 거부당하였거나, 공공기관이 부당하고 불법적인 방법으로 자신의 개인정보를 수집・이용・보유・공개한 경우, 프라이버시커미셔너에게 문제제기를 할 수 있으며 만약 이를 통해서도 해결이 되지 않는 경우에는 최종적으로 연방법원에 재심리를 요청할 수 있다.

---

239) 프라이버시법 제4조～제5조.

240) 프라이버시법 제6조～제8조.

241) 개인정보은행이란 프라이버시법 제10조에서 언급된 '개인정보의 수집물 또는 그 집합체'를 의미한다. 여기서 '개인정보의 수집물 또는 그 집합체'란 공공기관 등이 행정목적으로 사용하였거나, 사용 중이거나 또는 향후 입수가 가능한 개인정보 및 개인에게 부여된 증명번호, 기호, 기타 특정한 것으로 조직화되거나 검색될 의도가 있는 개인정보를 의미한다. 동법은 정부 부처의 장에게 이와 같은 개인정보를 개인정보은행에 포함시킬 것을 규정하고 있다.

(2) 개인정보보호및전자문서에관한법

캐나다는 연방차원에서 민간부문에 적용되는 개인정보보호법을 별도로 제정하여 시행하고 있는데, 이는 2000년 4월 13일 의회에서 최종 승인된 「개인정보보호및전자문서에관한법률(PIPEDA : The Personal Information and Electronic Documents Act)」이다. 동법은 앞서 언급한 바와 같이 1990년대 들어 정보사회화가 급속히 진행되면서 과거보다 민간영역에서 소비자의 개인정보를 수집・보유・이용하는 일이 증가함에 따라, 이러한 민간영역에 적용되는 새로운 법률을 제정하게 된 것이다. 또한 EU 개인정보보호지침 등의 제정으로 인하여, 유럽과 동등한 수준의 개인정보보호 체계를 갖출 필요가 있었던 것도 하나의 입법배경이 되었다.

동법은 기본적으로 민간부문에서 영리목적의 활동을 하는 과정에서 행하는 개인정보 관련 행위를 규율한다. 현재는 한 주의 경계를 넘어 활동하고 있는 민간단체, 예를 들어 통신업・방송업・은행・항공사 등에 대해 적용되나, 2004년 1월부터는 연방차원에서 규제될 수 있는 단체인지 아닌지를 불문하고 상업적 활동과정에서 개인정보를 수집・이용・보유하는 모든 민간단체에 적용될 예정이다.[242] 단, 순수하게 주 내에서 활동하는 민간단체의 경우에는 해당 주의 개인정보보호법이 충분한 보호체계를 갖추고 있는 경우에만 연방법의 적용이 배제될 것이다.[243]

PIPEDA는 시민들의 개인정보에 관한 권리를 보장함과 동시에 사업자들이 합법적인 사업목적을 위해 개인정보를 획득하고 처리할 수 있도록 양자 간의 균형을 맞추는 것을 목적으로 하고 있다. 따라서 동법은 정보

242) PIPEDA는 동법의 적용을 받는 범위에 대하여 총 3단계의 시행절차를 두고 있다. 첫 번째 단계는 2001년 1월 1일부로 연방차원에서 규제할 수 있는 민간영역에서 처리하고 있는 소비자 및 근로자의 개인정보에 적용되기 시작한 것으로 항공사, 은행, 방송사, 통신회사, 운송회사 등이 그것이다. 그 후 2002년 1월 1일부터는 2차 시행단계에 들어가, 이미 1차 단계에서 적용을 받고 있는 영역에서 처리하는 개인건강정보에 대해서도 적용되고 있다. 마지막 3차 단계는 2004년 1월 1일이며, 이 때부터는 기본적으로 영리목적으로 처리하는 모든 개인정보에 대하여 적용된다.

243) 현재 민간영역에서 처리되고 있는 개인정보를 보호하기 위한 법률을 연방법과 유사한 수준으로 마련하여 시행하고 있는 퀘벡 주의 경우 순수한 주 차원의 민간영역에 대해서는 연방법의 적용이 배제되고 있다.

주체가 자신의 개인정보에 대하여 가지는 여러 권리와 사업자가 준수해야할 의무를 규정하고 있다. 특히 동법의 적용을 받는 민간단체가 커미셔너의 조사 및 감사를 방해하거나 정보주체의 접근요청을 받은 개인정보를 임의로 파괴하거나, 내부 고발자를 징계하는 경우 범죄에 해당된다. 따라서 이 경우 즉결심판에서는 최고 10,000달러, 기소범죄에 대해서는 최고 100,000달러의 벌금형에 처해질 수 있다.

〔표 4-25〕 PIPEDA의 정보주체의 권리 및 정보처리자의 의무

정보주체의 권리	정보처리자의 의무
・개인정보 수집・이용・공개의 목적 및 이유를 알 권리 ・정보처리자에게 개인정보를 합리적으로 적절히 수집・이용・공개할 것을 요구할 권리 ・개인정보관리담당자가 누구인지 알 권리 ・정보처리자에게 개인정보의 안전성 확보를 위해 적절한 조치를 취할 것을 요구할 권리 ・정보처리자에게 정확하고 완전하며 최신의 개인정보를 보유토록 요구할 권리 ・개인정보 접근권과 정정요구권 ・정보처리자가 개인정보를 다루는 방법에 대한 이의제기의 권리	・개인정보의 수집, 이용, 공개에 대하여 정보주체의 동의를 구할 의무 ・특정 거래에 있어 당해 개인정보가 불가결한 요소가 아닌 경우, 정보주체가 개인정보의 수집・이용・공개에 대하여 동의하지 않은 때에도 상품이나 서비스 제공에 있어 개인에게 불이익을 주지 않을 의무 ・공정하고 합법적인 방법으로 정보를 수집할 의무 ・명확하고 이해가능하며 접근하기 용이한 방법으로 개인정보 관련 정책을 운용할 의무 ・명시된 목적을 달성한 이후에는 관련 개인정보를 삭제하거나 익명의 정보로 전환할 의무

또한 동법은 공정한 정보처리에 관한 10가지 정보보호원칙을 규정하고 있는데, 이는 OECD 프라이버시 8원칙과 1996년 캐나다표준협회(CSA : The Canadian Standards Association)에서 마련한「개인정보보호를 위한 모델 프라이버시규약(Model Privacy Code for the Protection of Personal Information)」을 바탕으로 만들어진 것이다.[244] 동 원칙은 개

244) CSA의 프라이버시 모델규약은 관련 단체들이 어떻게 개인정보를 수집하고 활용하며 타인에게 제공할 수 있는지 그 방법을 규정하고 있는 것으로, 공공부문과 민간부문을 모두 포함하는 캐나다 전 영역에 적용되는 개인정보보호 기본원칙이다. 특

인정보의 수집·이용·공개·보유·처분 등에 관한 10가지 원칙을 규정하고 있는 바, 이는 다음과 같다.

〔표 4-26〕 캐나다 개인정보보호원칙

구 분	내 용
책임의 원칙	· 정보처리자의 동 원칙 준수에 대한 책임 · 개인정보관리담당자의 지정
목적명확성의 원칙	· 개인정보 수집 이전 또는 당시에 수집목적 명확화
동의의 원칙	· 개인정보의 수집·이용·공개에 관한 정보주체의 인지 및 동의
수집제한의 원칙	· 명시된 목적에 필요한 개인정보 수집 · 공정하고 합법적인 방법에 의한 개인정보 수집
이용·공개·보유의 제한	· 명시된 목적외의 개인정보 이용·공개 금지 · 목적 달성에 필요한 기간을 초과한 개인정보 보유 금지
정확성 원칙	· 개인정보의 정확성, 완전성, 최신성 확보
안전성 원칙	· 개인정보의 민감성에 따른 적절한 안전조치 확보
공개성 원칙	· 정보처리자의 개인정보 관리현황, 정책에 대한 공개
정보접근권의 원칙	· 정보주체의 자기정보 접근권, 정정요구권
이의제기권의 원칙	· 상기 원칙의 준수여부에 대한 이의제기권

다. 캐나다의 개인정보보호기구

연방국가인 캐나다는 개인정보보호법의 제정현황과 마찬가지로 개인정보보호기구도 연방과 주 차원에서 각각 설립되어 운영되고 있다. 그러나 연방 프라이버시커미셔너는 순수하게 주 개인정보보호기구의 관할영역이 아닌 부분에 대하여 포괄적인 관할권을 가지며, 캐나다 전체 국민의 개인정보를 보호하고 올바른 개인정보 처리관행을 확립시키는 역할을 담당하고 있다.

히 동 규약은 프라이버시커미셔너와 연방정부, 연방차원에서 상업활동을 하는 방송사·통신회사·금융기관 등의 사업자, 소비자단체, 학계 등 각계 대표자가 함께 논의하여 마련한 것이라는 점에서 의미를 가진다.

〔표 4-27〕 캐나다 개인정보보호기구 현황

구분	기관명	
연방	연방프라이버시커미셔너	
주	Alberta	정보프라이버시커미셔너
	British Columbia	정보프라이버시커미셔너
	Manitoba	옴브즈만
	New Brunswick	옴브즈만
	New Foundland	법무부
	Northwest Territories	정보프라이버시커미셔너
	Nova Scotia	정보공개 및 프라이버시 심사국
	Nunavut	정보프라이버시커미셔너
	Ontario	정보프라이버시커미셔너
	Prince Edward Island	정보프라이버시커미셔너
	Quebec	정보보호위원회
	Saskatchewan	정보프라이버시커미셔너
	Yukon	옴브즈만 및 정보프라이버시커미셔너

(1) 프라이버시커미셔너의 지위

캐나다의 연방 프라이버시커미셔너는 연방 프라이버시법에 의해 1983년도에 설립된 법정기구로서, 영국 여왕을 대신하는 추밀원장(Governor in Council)이 상하원의 동의를 얻어 임명한다. 커미셔너의 임기는 7년이며 연임가능하나, 직무수행에 있어 문제가 있을 때는 상하원의 결의를 통해 해임될 수 있다. 커미셔너는 의회 소속기구(Officer of the Parliament)로서 활동결과에 대해 상하원에 직접 보고한다. 따라서 커미셔너는 공공부문과 민간부문에서의 개인정보처리에 관한 민원을 다룸에 있어 어떠한 정부부처나 기관의 간섭을 받지 않고 독립적으로 직무를 수행하며, 예산지원이나 인사관리 등에 있어 행정부의 지시·감독으로부터 자유롭다.

연방 프라이버시커미셔너는 연방의 공공부문과 민간부문에 적용되는 두 가지 법률을 관장한다. 따라서 순수하게 주의 관할영역이 아닌 영역

과 관련된 개인정보 문제에 대해서 포괄적인 업무범위를 가지고 있다. 물론 현재까지는 PIPEDA의 적용이 캐나다 연방 전체에서 활동하는 민간단체에 한하여 적용되고 있지만, 2004년부터는 법률이 적용되는 범위가 확대되는 만큼 연방 프라이버시커미셔너의 업무범위도 확장된다 할 것이다.

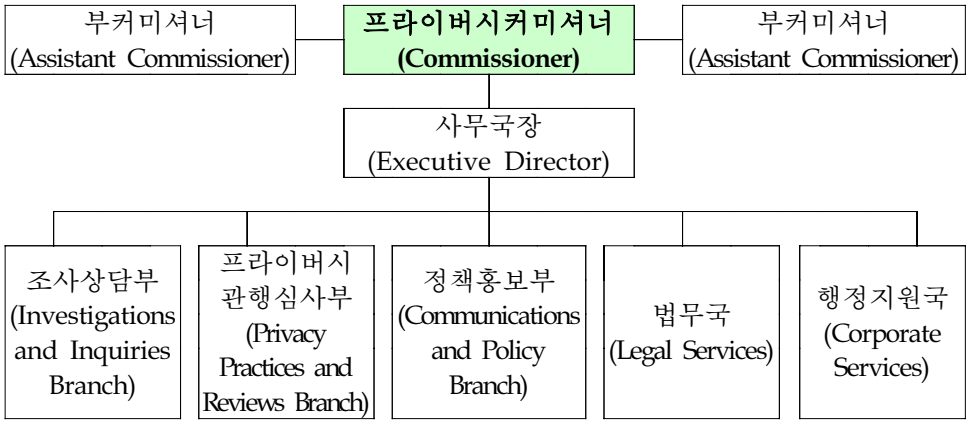
(2) 프라이버시커미셔너의 조직구성

연방 프라이버시커미셔너 사무국(OPC : The Office of the Privacy Commissioner of Canada)은 커미셔너 1인과 2인의 부커미셔너를 비롯하여, 공무원 고용법(The Public Service Employment Act)에 따라 임명된 100명(2003. 3월말 기준)의 정규직원이 있다. 이 외에도 프라이버시커미셔너가 자체적으로 임명하는 기술지원직(임시직)이 있으며, 기술지원직의 보수 및 운영비용은 재무부(Treasury Board)의 인가를 얻어 결정된다.

프라이버시커미셔너 사무국은 PIPEDA의 시행에 관한 업무를 주로 하는 부커미셔너 2인과 커미셔너의 활동을 지원하는 5개 부서로 이루어져 있다. 이 중 조사상담부(Investigations and Inquiries Branch)를 가장 규모가 큰 대표적인 부서로 볼 수 있는데, 조사상담부는 프라이버시법 제29조 및 PIPEDA 제11조에 근거하여 각종 민원처리 및 조사업무를 행한다. 또한 프라이버시 관행심사부(Privacy Practices and Reviews Branch)는 프라이버시 영향평가를 위한 심사 및 개인정보처리 현황에 대한 모니터링을 실시한다.[245] 이 외에도 정책홍보부는 각종 프라이버시 관련 기술 및 정책연구, 대외협력, 홍보 등의 업무를 담당하며, 법무국은 민원처리 과정에서의 법률자문이나 입법·정책에 대한 각종 커미셔너의 자문을 지원하고 있다. 마지막으로 행정지원국은 커미셔너와 사무국의 활동과

245) 프라이버시 관행심사부는 프라이버시 영향평가제도의 도입과 더불어 신설된 부서로, 지난 1년여 동안 사무국은 약 40여건 정도의 프라이버시 영향평가 보고서를 접수하여 처리하였다. 보고서의 대부분은 전자적 서비스 제공이나 새로운 기술적 기반구조 및 서비스 설계와 관련된 것이었으며, 검토결과는 대부분 사소한 사항의 보완을 요구하는 제안과 함께 해당 부처로 통보되었다.

관련된 각종 행정사항을 총괄하여 지원・관리하는 업무를 맡고 있다.



(그림 4-10) 캐나다 프라이버시커미셔너 조직도

(3) 프라이버시커미셔너의 주요기능

캐나다의 연방 프라이버시커미셔너의 주된 임무는 첫째, 모든 캐나다 국민들이 자신들의 프라이버시 권리를 보호하고 수호함에 있어 최고 수준의 서비스를 받을 수 있도록 하고, 둘째, 캐나다 전 지역의 많은 중요한 이해당사자는 물론 캐나다 의회의 신뢰도를 재확립하며, 셋째, 프라이버시법에서 요구하는 사항 및 정보주체의 권리에 대해 정보처리자가 이해하고 실천할 수 있도록 돕는 것이다. 이러한 임무 수행을 위해 커미셔너는 연방법에 따라 접수된 각종 민원이나 신고사건에 대해 사실조사를 하여 처리하고, 관할영역의 개인정보보호실태를 조사・감사하며, 정부와 의회에 대한 자문을 행한다. 또한 프라이버시 이슈에 관한 연구・조사를 행하며, 캐나다 국민들이 프라이버시 문제에 대해 인식하고 이해할 수 있도록 촉진하는 역할을 한다.

이 중에서도 가장 핵심적인 기능은 개인정보 피해구제 및 정부와 의회를 대상으로 한 입법・정책자문이다. 먼저 피해구제 기능부터 살펴보면, 커미셔너는 공공기관이나 사업자의 법규위반행위 및 개인정보침해행위에

대한 민원을 접수받아 처리하고 있다. 즉, 커미셔너는 개인정보보호를 위한 옴브즈만의 역할을 하는 기관으로 볼 수 있다. 커미셔너의 피해구제 기능에 대해서는 아래에서 좀 더 자세히 살펴보기로 한다.

또한 커미셔너는 개인정보보호와 관련된 정책수립과정이나 입법과정에서 자문을 제공하며, 특히 개인정보 관련하여 이슈가 되는 사안에 대해서는 의견을 제시하고 홍보하는 역할을 하고 있다. 대표적인 예가 공공기관의 새로운 정보처리시스템에 대한 프라이버시 영향평가(PIA : Privacy Impact Assessment) 작업에 참여하는 것이다. 프라이버시커미셔너는 예비 프라이버시 영향평가 과정이나 프라이버시 영향평가 초기단계에 직원을 해당 공공기관에 파견하여 함께 시스템에 대한 검토 작업을 하도록 지시할 수 있다. 이를 통해 프라이버시침해여부에 대한 자문이나 가이드라인을 제공하고 잠재된 프라이버시 문제의 해결책을 제시하는 역할을 한다. 또한 커미셔너는 정부기관으로부터 프로그램이나 서비스의 집행 전 단계에서 최종 프라이버시 영향평가 결과를 통보받아 검토한 뒤, 해당 기관의 장이나 차순위 책임자(Deputy heads)에게 자문을 제공한다.[246]

여기서 프라이버시 영향평가제도에 대해 간략히 살펴볼 수 있을 것이다. 프라이버시 영향평가제도는 2002년 5월 1일 시작된 것으로, 동 제도의 시행으로 인하여 캐나다중앙은행(The Bank of Canada)을 제외한 프라이버시법에서 지정한 모든 공공기관은 정보처리프로그램이나 서비스의 설계 및 재설계 초기 단계에서 프라이버시 영향평가를 하여야 한다. 즉, 모든 연방 부처의 개인정보 수집・이용・공개와 관련된 정책 및 프로젝트가 개인의 프라이버시에 미치는 영향을 평가하고 그에 따른 역효과를 완화하거나 방지할 수 있는 방법을 모색하는 것이 프라이버시 영향평가제도이다. 프라이버시 영향평가의 운영에 관한 책임을 지는 자는 정부 부처의 차순위 책임자이며[247], 장관 등 정부 부처의 장은 관할 공공기관이

246) 커미셔너는 각 부처의 프라이버시 영향평가제 운영에 있어 조언자와 상담자의 역할을 수행하는 것이지, 특정 프로젝트나 프로그램의 승인이나 거부를 하는 것은 아니다.

247) 특히 정부부처의 차순위 책임자는 프라이버시 영향평가제도를 운영함에 있어서 ①

프라이버시법 및 관련 규정을 준수하도록 할 책임이 있다. 앞서 살펴본 커미셔너의 주요 기능을 정리해보면 다음과 같다.

〔표 4-28〕 프라이버시커미셔너의 주요기능

주요기능	세부내용
피해구제	· 각종 불만사항이나 신고 접수 · 자료제출요구, 관계인소환, 현장조사 등을 통한 사실조사 · 민원사항에 대한 검토 및 화해유도, 분쟁조정 등을 통한 해결 · 정보주체의 개인정보 접근권 행사 거부시 연방법원에 소송제기
조사·감독	· 프라이버시 침해여부에 대한 직권 실태조사 및 모니터링 · 정보보호원칙 및 법규 준수여부 감독 · 법위반사항 발견시 시정권고
정보제공	· 프라이버시 관련 문제에 대한 상담 및 질의접수, 처리 · 개인정보 이슈에 대한 의견제시
정책 및 입법자문	· 개인정보 관련 법안 심의 및 의견제시 · 정부의 각종 정책에 대하여 의견제시 및 자문 · 프라이버시 영향평가 심사 시행 및 자문
개인정보연구	· 프라이버시 동향 및 현안에 대한 조사·분석
교육홍보	· 언론보도자료 작성 및 배포 · 기자회견, 회의, 워크샵 등 행사진행 및 웹사이트 관리
국내외 협력	· 주 개인정보보호기구 및 해외기구와의 협력

라. 개인정보피해구제 절차 및 방법

프라이버시법과 PIPEDA는 각각 공공기관과 민간기관의 개인정보 수집·이용·공개 등의 행위로 인하여 피해를 입은 자의 이의제기권을 규정하고 있다. 또한 각각의 정보처리자는 조직 내에 개인정보보호와 관련된 업무를 담당하는 개인정보관리담당자를 임명하여 이와 같은 민원을 처리할 수 있도록 하고 있다. 따라서 자신의 개인정보가 불합리하게 침

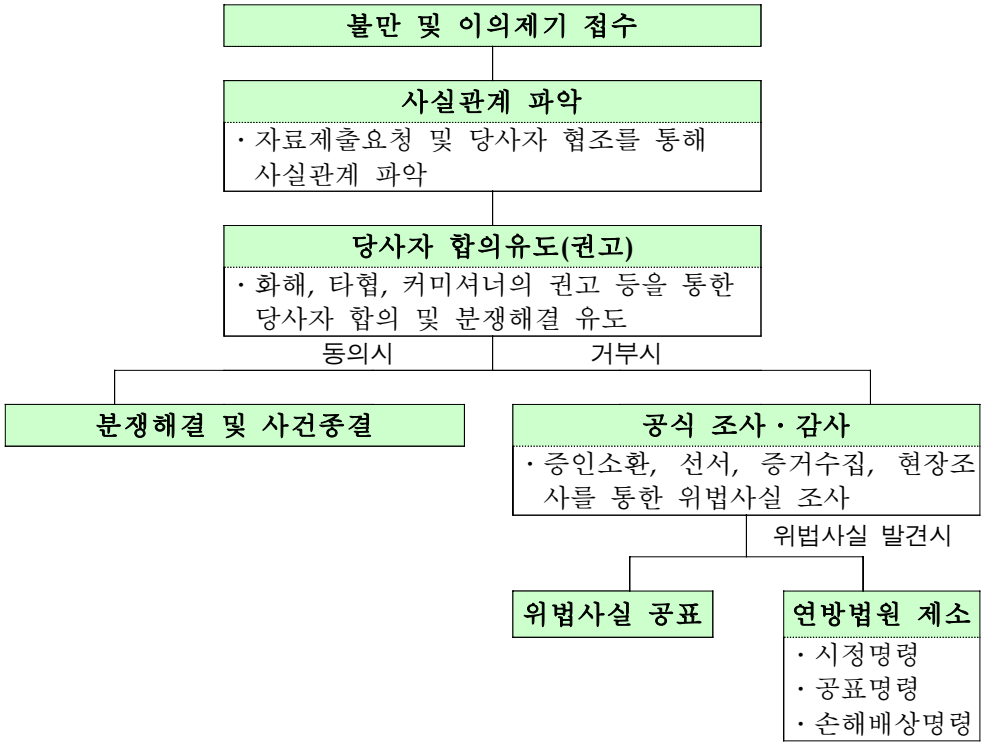
프라이버시커미셔너와 협의하여야 하고, ② 프라이버시커미셔너에게 제공될 프라이버시 영향평가 내용을 최종 승인하며, ③ 프라이버시커미셔너의 제안내용에 대하여 응답하여야 하고, ④ 영향평가 결과요약보고서를 시민들이 접근하여 이용할 수 있도록 보장하여야 한다.

해된 자는 해당되는 정보처리자의 개인정보관리담당자에게 이의제기를 할 수 있으며, 이를 통해 자체적으로 분쟁이 해결될 수 있다. 그러나 이러한 자체적인 개인정보 분쟁해결이 어려울 경우, 피해자는 프라이버시 커미셔너에게 문제제기를 할 수 있다.

프라이버시커미셔너는 캐나다 연방차원의 개인정보보호 전담기구로, 연방 프라이버시법과 PIPEDA에 따라 개인정보피해구제 기능을 하고 있다. 따라서 커미셔너는 관할영역의 개인정보처리자의 행위로 인하여 정보주체가 피해를 입었을 경우, 민원을 접수받아 조사·심사하여 관련 당사자간 분쟁을 해결하는 역할을 하고 있다. 특히 커미셔너는 무엇보다도 협상과 설득, 조정을 통한 분쟁해결에 최우선순위를 두고 활동하고 있는 옴브즈만으로서의 성격이 강하다.

프라이버시커미셔너가 행하는 개인정보피해구제 절차는 상담, 이의제기신청 접수, 사실관계 파악 및 화해, 권고 등을 통한 분쟁해결, 공식적인 사실조사 및 감사, 불법행위 공표 또는 연방법원 제소 등의 순서로 이어진다. 먼저, 커미셔너는 개인정보 상담을 거쳐 개인정보침해에 대한 이의제기를 접수받는데, 보통 공식적인 사실조사에 앞서 자료제출요청 등을 통해 당사자로부터 자발적인 협조를 얻어 사실관계를 파악한다. 그리고 협상과 설득을 통한 조정과 타협으로 분쟁을 해결하는 절차를 거친다. 커미셔너는 이 과정에서 정보처리자에게 잘못된 개인정보 취급관행을 수정토록 권고하거나 정보주체의 권리행사를 방해하지 않도록 권고할 수 있다. 그러나 당사자로부터 자발적인 협조가 불가능한 경우에는 증인을 소환하고 증인으로부터 선서를 받고 증거물을 확보할 권한을 행사하여 공식조사를 할 수도 있다. 조사결과 위법사항이나 개인정보침해행위가 발견되었음에도 불구하고 정보처리자가 커미셔너의 권고사항을 무시하였을 때에는 해당 정보처리자의 잘못된 개인정보 취급관행을 외부에 공표할 수 있으며, 분쟁이 해결되지 않을 때에는 개인을 대신해서 연방법원에 제소할 수도 있다. 물론 개인은 특정한 상황 하에서는 커미셔너로부터 조사결과를 통보받은 날로부터 45일 이내에 스스로 연방법원에 제소할 수 있다. 한편 연방법원은 소송이 제기되면 정보처리자의 잘못

된 개인정보 취급관행을 시정토록 명령할 수 있으며, 해당 사업자나 민간단체가 법원의 시정명령에 따라 취한 조치 또는 향후 취할 시정조치를 구체적으로 공표하도록 명령할 수 있다. 또한 연방법원은 수치심을 비롯하여 민원인이 입은 경제적·정신적 피해에 대하여 보상토록 결정할 수 있다.[248]



(그림 4-11) 캐나다 프라이버시커미셔너의 피해구제 절차도

캐나다의 프라이버시커미셔너는 위와 같은 절차와 방법을 통해 연방차원의 공공부문과 민간부문에서 개인정보피해구제의 역할을 하고 있는 바, 커미셔너가 지난 회계연도에 접수받아 처리한 사건현황을 살펴보면 다음과 같다.

248) Tamara L. Hunter/Chris Bennett, "*Personal Information Protection and Electronic Documents Act("PIPEDA") - Presentation to the Insurance, Investigation, Security and Human Resources Industries for Shepp Johnman - "*, Davis & Company, 2002. 2. 13.

〔표 4-29〕 2002/03년도 프라이버시커미셔너의 민원처리현황

공공부문		민간부문	
접근권 침해	486	금융기관	112
개인정보 불법수집	868	통신・방송부문	56
개인정보 불법보유 및 미파기	21	운송회사	46
개인정보 불법 이용・제공	1727	핵관련업체	38
보유기한 위반	381	기타(인터넷 서비스제공자 등)	48
계	**3,483**	**계**	**300**

(단위 : 건)

〔표 4-29〕를 보면, 프라이버시커미셔너가 연방차원에서 활동하는 기구라는 점 및 아직 민간부문을 관장하는 PIPEDA가 전면적으로 시행되지 않았다는 점으로 인하여, 주로 공공부문의 개인정보침해에 대한 이의제기가 민간부문에 비해 현저히 많은 편임을 확인할 수 있다. 한편 아래의 〔표 4-30〕은 접수된 사건이 처리된 결과이다. 가장 많은 유형을 차지한 것은 증거가 불충분하여 위법사실이 확인되지 않는다는 것으로 38%를 차지하고 있다. 그러나 커미셔너의 권고나 화해, 조정 등을 통해 분쟁해결이 이루어지는 비율도 25%를 차지하고 있다.

〔표 4-30〕 2002/03년도 프라이버시커미셔너의 사건해결유형

사건해결유형	공공부문	민간부문
법위반증거 불확실	2711	61(38%)
법위반사실 확인하였으나 커미셔너의 권고 거부	371	45(28%)
법위반사실 확인 및 권고에 따른 분쟁해결	77	41(25%)
커미셔너의 화해, 조정 등의 방법을 통한 분쟁해결	13	
조사 중 정보처리자의 자발적 조치 또는 커미셔너의 조사결과에 대한 민원인의 만족으로 인한 사건종결	235	
사실확인 불가 등으로 인한 민원처리 중단	76	15(9%)
계	**3483**	**300**

(단위 : 건)

캐나다는 앞서 살펴본 바와 같이, 공공부문과 민간부문에서 각각 적절한 수준의 개인정보보호법을 마련하여 시행하고 있다. 그러나 이러한 입법의 완비에도 불구하고, 캐나다의 개인정보보호제도는 그 집행력이나 강력한 감독이 뒷받침해주지 못하는 경향이 있다. 제도상으로는 철저히 개인정보가 보호되도록 갖추어놓고 있으나, 실질적으로 개인정보 침해행위에 대한 규제나 이로 인한 피해에 대한 민·형사상 피해구제는 다소 미흡한 실정이다. 또한 커미셔너는 악질적인 개인정보 침해자에 대해 그 이름을 공개할 수 있는 공표권을 가지며 이것은 가장 실효성 있는 개인정보 피해구제 또는 예방수단이 될 수 있음에도 불구하고, 커미셔너가 이 권한을 행사하는 것에는 다소 소극적이라는 비판이 있다.[249]

249) Toronto Star, *"Name names, or Privacy law toothless"*, 2003. 11. 17.

제 4 절 오세아니아

1. 호주

호주는 2003년 현재 인구 1,955만명의 연방국가이다. 따라서 프라이버시 또는 개인정보보호를 위한 법률이나 기구도 각각 연방과 주 차원에서 도입되어 운영되고 있다.[250] 그러나 현재 호주의 연방헌법에는 프라이버시권에 관한 명시적인 규정이 포함되어 있지 않다. 다만 호주의 연방법원과 주법원에서는 프라이버시권을 보통법(Common Law)상의 권리로 인정하고 있는 추세이다.[251] 이하에서는 호주의 대표적인 연방 프라이버시법을 중심으로 개인정보보호를 위한 법제도를 살펴보고, 동법에 근거하여 활동하고 있는 호주 연방의 프라이버시커미셔너에 대해 검토해보기로 한다.

가. 개인정보보호 법제현황

호주의 대표적인 프라이버시법은 연방차원에서 1988년 제정된 「연방 프라이버시법(The Federal Privacy Act 1988)」이다. 호주에서는 1980년대 중반, 전국민에게 신분증과 신원확인번호를 부여하려는 신분카드제도를 도입하려고 하였는데 이러한 계획에 대하여 당시 여론은 프라이버시 침

250) 호주에서는 법률상으로 정보보호(data protection), 개인정보보호(personal data protection)라는 용어보다는 포괄적으로 프라이버시 보호(privacy protection) 또는 정보프라이버시(information privacy)라는 용어를 주로 사용하는 것으로 보인다.

251) 호주 연방고등법원(High Court of Australia)은 Lenah v. ABC 판결에서 개인의 프라이버시 침해로 인한 불법행위의 성립가능성을 언급한 바 있다. (Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd［2001］HCA 63 (2001. 11. 15.). 또한 지난 2003년 6월 퀸스랜드 지방법원(Queensland District Court)은 Gross v. Purvis 판결에서 프라이버시 침해로 인해 상당한 기간동안 원고가 입은 정신적 고통에 대하여 178,000 호주달러를 배상토록 결정한 바 있다. (Grosse v Purvis［2003］QDC 151 (2003. 6. 16))

해 가능성을 제기하며 반대하였다. 이러한 과정에서 프라이버시 보호를 위한 입법의 필요성이 대두되어 동법이 제정되었다. 동법은 OECD 가이드라인과 「시민적·정치적 권리에 관한 국제협약(ICCPR : International Covenant on Civil and Political Rights)」 제17조[252]의 내용을 자국 법체계에 수용하고 있으며, 호주는 동법의 제정을 통해 개인정보보호법제도의 기틀을 마련한 것으로 볼 수 있다. 이후 동법은 개정을 거쳐 소비자신용정보와 세금파일번호(TFN : Tax File Number)의 이용에 대해서도 규율하게 되었으며, 「2000년 프라이버시수정법(민간영역)(The Privacy Amendment (Private Sector) Act 2000)」의 제정으로, 민간영역에서의 개인정보처리에 대해서도 폭넓게 규율하게 되었다. 이로 인해 비로소 동법은 호주의 개인정보보호 기본법의 특징을 갖출 수 있게 되었다.

호주에는 1988년 프라이버시법 외에도 「형법(Crimes Act 1914)」, 「정보조합프로그램법(Data-matching program Act (Assistance and Tax) 1990)」, 「국민건강법(National Health Act 1953)」, 「전기통신법(Telecommunications Act 1997)」 등에서 개인정보 관련규정을 두고 있다.

나. 연방프라이버시법의 주요내용

(1) 적용범위

연방프라이버시법은 원칙적으로 공공부문과 민간부문에 모두 적용되는 호주의 개인정보보호 기본법이다. 다만, 연방법이므로 주법이 적용되는 범위 내에서는 그 적용이 배제된다. 따라서 주의 공공기관이나 순수하게 주 내에서 이루어지는 민간 부문의 개인정보처리에는 동법이 적용되지 않는다. 보다 구체적으로 살펴보면, 연방프라이버시법의 적용범위는 크게 연방 및 수도자치구(ACT : Australia Capital Territory)의 공공기관에서

252) 시민적·정치적 권릭에 관한 국제협약 제17조 : 「① 어느 누구도 그의 사생활, 가정, 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 또는 그의 명예와 신용에 대한 불법적인 비난을 받지 아니한다. ② 모든 사람은 그러한 간섭 또는 비난에 대하여 법의 보호를 받을 권리를 가진다」

처리하는 개인정보, 법인 등 민간단체[253]에서 처리하는 개인정보, 소비자 신용정보, 세금파일번호의 처리에 대하여 적용된다. 구체적인 적용범위를 살펴보면 다음과 같다.

〔표 4-31〕 호주 연방프라이버시법의 적용범위

구분	적용범위
공공부문	· 연방 및 수도자치구의 정부기관에 의해 처리되는 개인정보 · 공공기관이 발행한 개인의 세금파일번호의 이용 · 공공기관이 보유하는 형법(1914)에 의한 형사기록정보 · 호주 국세청 등의 세금정보 이용을 위한 데이터대조프로그램 규제 · 의료보험위원회 및 보건당국에서 처리하는 개인의 의료정보 · 공공기관이 법집행기관에 개인정보를 공개하는 경우
민간부문	· 2000년 프라이버시 법 개정으로 민간부문까지 확대 · 비영리단체를 포함하는 개인, 법인, 파트너쉽, 비법인단체, 트러스트 등에 의해 처리되는 개인정보 · 개인 및 기관에 의해 이용되는 개인의 세금파일번호 · 신용기관 및 신용업자가 보유하는 신용정보 · 특정 소규모 사업자 : 소규모 사업자는 프라이버시 법상 '단체'의 정의에서 제외되나, 2002. 12. 21부터 ① 소규모 사업자가 의료서비스 제공업자이거나 ② 개인정보를 거래하는 사업자이거나 ③ 보다 대규모의 사업자와 관련이 있거나 ④ 연방기관과 계약을 체결한 자인 경우에는 프라이버시 법의 규율을 받게 됨
제외대상	· 소규모 사업자(small business operator) : 예외 有 · 정당 · 현 사용자 또는 이전의 사용자에 의해 보유되는 근로자 정보 · 방송, 언론 등

(2) 프라이버시 원칙

연방프라이버시법은 OECD 가이드라인에 기초하여, 모든 연방공공기관의 정보처리활동에 적용되는 정보프라이버시원칙(IPP : Information Privacy Principles)을 규정하고 있다. 또한 연방프라이버시법의 적용대상

253) 프라이버시법상 단체(organization)라 함은 소규모 사업자(small business operator), 등록정당, 주 또는 기타 영역(Territory)의 공공기관이나 단체 또는 대행기관이 아닌 개인, 법인, 파트너쉽, 다른 기타 비법인 협회 또는 트러스트를 의미한다.

을 민간영역으로 확대하도록 규정한 「2000년 프라이버시 수정법(민간영역) (Privacy Amendment (Private Sector) Act 2000)」은 민간영역에 적용되는 개인정보보호 기본원칙인 국가프라이버시원칙(NPP : National Privacy Principles)을 규정하고 있다.[254] 이처럼 호주에서는 공공분야와 민간분야에 적용되는 정보보호원칙이 별도로 규정하고 있는 바, 그 내용을 살펴보면 아래와 같다.

［표 4-32］호주 공공분야 정보보호원칙(IPP)

구분		주요 내용
수집	원칙 1	수집목적에 적합한 개인정보를 수집하여야 하고, 불법적이거나 불공정한 정보의 수집은 금지됨
	원칙 2	관련개인으로부터 직접 개인정보 수집시 정보수집의 목적, 법적 수집근거가 있는 경우 그 내용 등을 고지하여야 함
	원칙 3	개인정보 수집시, 정보의 수집은 목적과 관련성이 있어야 하고, 정보의 최신성과 완전성을 확보하여야 하며, 관련개인의 사생활을 불합리한 정도로 침해하여서는 안 됨
보유	원칙 4	개인정보를 포함한 공공기록을 보유·관리하는 자(기록보유자)는 안전장치를 통해 개인정보를 보호하여야 함
	원칙 5	기록보유자는 정보주체가 기록보유자의 개인정보 보유여부, 보유하고 있는 정보의 성격 및 주요목적, 접근권행사절차 등을 확인할 수 있도록 조치를 취하여야 함
주체의 권리	원칙 6	정보주체는 자신에 관한 개인정보가 공공기록에 포함되어 보유·관리되는 경우, 그러한 정보에 접근할 권리를 가짐
	원칙 7	기록보유자는 개인정보의 정확성, 관련성, 최신성, 완전성, 명확성을 확보하기 위해 정정, 삭제, 추가 등을 위한 절차를 마련하여야 함

254) NPP는 1998년 호주 연방프라이버시커미셔너가 정보처리자의 자율규제를 지원하기 위해 제정한 '공정한 개인정보처리를 위한 국가원칙(National Principles for Fair Handling of Personal Information)'을 기초로 하여 마련된 원칙이다. (EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/australia.htm 참조)

이용 및 제공	원칙 8	기록보유자는 개인정보를 이용하기 전에 당해 개인정보의 정확성 등을 확인하여야 함
	원칙 9	기록보유자는 개인정보를 목적외로 이용하여서는 안 됨
	원칙 10	원칙적으로 특정한 목적을 위해서 개인정보를 획득한 자는 그 외 다른 목적을 위해 정보를 이용해서는 안 됨
	원칙 11	기록보유자는 원칙적으로 관련개인이 아닌 다른 공공기관 등 제3자에게 개인정보를 제공해서는 안 됨

〔표 4-33〕 호주 민간분야 정보보호원칙(NPP)

구분		주요 내용
원칙 1	수집	· 목적달성에 필요한 정보의 수집 · 공정하고 합법적인 수단에 의한 정보수집 · 정보수집시 고지의무 · 정보주체로부터의 직접수집원칙
원칙 2	이용 및 제공	· 원칙적으로 부차적인 목적으로 개인정보를 이용, 제공하는 행위 금지 · 사법목적을 위한 이용 및 제공시 정보주체에게 서면고지
원칙 3	정보정확성	· 개인정보의 정확성, 완전성, 최신성 확보를 위한 합리적 조치를 하여야 함
원칙 4	정보보안	· 오용이나 손실, 권한없는 접근·수정·공개로부터 개인정보를 보호하기 위한 합리적 조치를 하여야 함 · 목적 달성 후 개인정보 파기 또는 영구적으로 개인식별이 불가능하도록 조치를 취하여야 함
원칙 5	공개	· 개인정보관리정책의 명시 · 보유되고 있는 개인정보의 종류, 보유목적, 수집·이용·보유·공개의 방법 등을 알리기 위한 합리적 조치를 하여야 함
원칙 6	접근 및 수정	· 정보주체의 접근 및 정정권 보장 · 정보주체의 요청거부시 근거를 반드시 제공하여야 함
원칙 7	식별인자	· 원칙적으로 국가가 개인에게 할당하는 식별인자의 이용금지
원칙 8	익명성	· 합법적이고 실행가능한 경우, 정보주체가 정보처리자와의 거래관계시 자신을 드러내지 않을 선택권을 보장받아야 함
원칙 9	국외이전	· 동 원칙에서 규정한 수준과 유사한 법체계 또는 계약이 있는 경우 등에만 국외이전 허용
원칙 10	민감한 정보	· 원칙적으로 민감한 개인정보의 수집 금지

IPP는 주로 공공분야에서는 개인정보의 수집이 법적 근거를 가지고 이루어지는 경우가 많은 점을 감안하여, 개인정보 주체로부터 직접 개인정보를 수집하는 경우와 그 외 일반적으로 개인정보를 수집하는 경우 수집자가 준수하여야 할 사항을 자세히 규정하고 있다는 점에서 특색이 있다. 반면에 NPP는 민간분야의 정보보호를 위한 원칙과 그 예외를 보다 구체적으로 규정하고 있다. 특히 국가 등이 개인에게 부여하는 사회보장번호, 운전면허번호 등의 개인식별인자의 사용, 민감한 개인정보의 수집을 원칙적으로 금지하고 있다. 그 외에도 개인정보의 국외이전, 정보주체의 익명성 보장에 관한 특별한 규정을 두고 있다는 점에서 IPP와는 차이가 있다.

다. 호주의 개인정보보호기구

호주는 연방국가이기 때문에 각 주(州)마다 개인정보 또는 프라이버시 보호의 역할을 담당하는 기구가 설치되어 있지만, 호주를 대표하는 개인정보보호기구는 바로 연방 프라이버시커미셔너(The Federal Privacy Commissioner)이다. 호주의 연방 프라이버시커미셔너는 2001년 국제 정보보호커미셔너회의에서 '자격 있는 개인정보보호기구'로 인정받음은 물론, 올 9월에는 제25차 국제정보보호커미셔너회의를 개최하는 등 선진 개인정보보호기구로서의 위상을 한층 높이고 있다.

［표 4-34］호주의 개인정보보호기구 현황

구분		기관명
연방 및 수도자치구 등		연방프라이버시커미셔너
주(州)	퀸즈 랜드	주 정부(법무부)
	뉴 사우스 웨일즈	프라이버시커미셔너
	빅토리아	프라이버시커미셔너
	타즈마니아	주 정부(법무부)
	사우스 오스트레일리아	프라이버시 위원회
	웨스턴 오스트레일리아	주 정부(법무부)

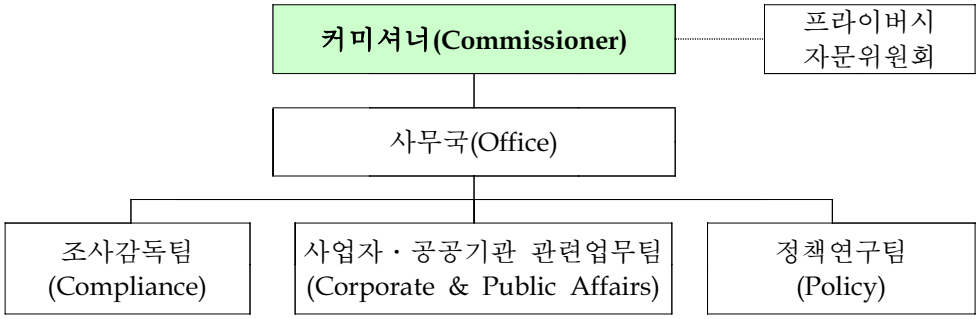
(1) 프라이버시커미셔너의 지위

연방 프라이버시커미셔너는 1988년 프라이버시법에 근거하여 설립된 이래, 몇 차례의 법률 개정을 통해 권한과 규율대상이 확대되면서 명실상부한 호주의 대표적인 개인정보보호기구로 발전하였다. 특히 2000년 프라이버시법 개정으로 커미셔너의 규율영역이 민간영역까지 대폭 확대됨에 따라, 그 권한과 역할이 더욱 강화되었다 할 것이다. 특히 2001. 12. 21일부터는 소규모 사업자 중 의료서비스제공업자, 개인정보거래사업자, 대규모 사업자의 협력업체, 연방공공기관과 계약을 체결한 소규모 사업자 등에 대해서도 관할하게 됨에 따라, 커미셔너의 업무영역이 더욱 확대되었다고 볼 수 있다. 커미셔너는 현재 연방 및 수도자치구의 공공기관에서 처리되는 개인정보, 신용정보, 일부 민간영역에서 처리되는 개인정보 등에 관하여 규율하고 있는 1988 프라이버시법 외에도 형법, 데이터대조프로그램법, 국민건강법, 전기통신법 등의 법률을 관장하고 있다.

연방 프라이버시커미셔너는 총독(Governor-General)에 의해 임명되는 독립기관으로, 임기는 7년이며 재임이 가능하다. 커미셔너는 위원회의 업무결과에 대해 의회 및 수상에게 직접 보고하며, 타 기관으로부터 간섭을 받지 않는 독립적인 지위를 가진 법정기구이다.

(2) 프라이버시커미셔너의 조직구성

호주의 연방개인정보보호기구는 커미셔너 1인과 커미셔너의 업무를 지원하고 보조하는 사무국으로 구성된다. 사무국은 조사감독팀, 사업자・공공기관 관련업무팀, 정책연구팀으로 나뉘며 2003년 현재 직원은 약 40명이다. 조사감독팀은 개인정보 관련 상담 및 피해구제 업무를 주로 행하며, 사업자・공공기관 관련업무팀은 개인정보를 취급하는 사업자 및 공공기관에 대한 개인정보보호교육의 실시 및 기관의 활동에 대한 홍보의 업무를 담당하며, 정책연구팀은 개인정보보호를 위한 각종 연구를 행한다. 호주의 프라이버시커미셔너 조직도는 아래와 같다.



(그림 4-12) 호주 프라이버시커미셔너 조직도

또한 연방 프라이버시커미셔너는 별도 조직으로 '프라이버시 자문위원회(Privacy Advisory Committee)'를 설치・운영하고 있다. 연방 프라이버시법에 의하면 프라이버시 자문위원회는 커미셔너 1인을 포함하여 7인 이내의 위원으로 구성되며, 2003년 현재는 프라이버시커미셔너를 포함하여 총 6인으로 구성되어 있다. 자문위원의 임명권자는 수상이며 위원의 임기는 5년이나 국회의원일 경우에는 의원의 임기에 따른다. 자문위원회는 프라이버시 및 개인정보보호문제와 관련된 사항에 대하여 연방프라이버시커미셔너에게 자문을 행하며, 연방 프라이버시커미셔너가 추진하는 주요사업에 대해서도 전략적인 자문을 하고 있다. 또한 개인의 프라이버시 보호를 보다 철저히 하기 위하여 주요 관련단체들과의 협력체계를 강화하고 호주의 사업자 및 정부에게 프라이버시의 중요성에 대한 인식을 증진시키는 역할을 담당하고 있다.

(3) 프라이버시커미셔너의 주요기능

연방프라이버시커미셔너는 개인(정보주체)이나 단체(정보처리자)에 대하여 개인정보보호 관련 정보를 제공하거나 상담을 함으로써, 전 국가적인 개인정보보호 인식을 제고하기 위한 활동을 펼치고 있다. 또한, 입법안에 대하여 프라이버시를 침해할 위험이 있는지를 사전심사하거나 법률자문을 실시하고 있다.

한편 프라이버시커미셔너는 공공기관이 정보프라이버시 원칙(IPP)에 위반하였는지 여부를 점검하고, 개인의 프라이버시를 침해할 우려가 있는 민간영역의 정보처리행위나 관행에 대하여 조사하기도 한다. 커미셔너가 행하는 이러한 조사는 개인정보침해신고와 같은 민원신청에 따라 이루어지기도 하지만, 민원과 관계없이 커미셔너가 프라이버시 침해여부를 조사할 필요가 있다고 판단될 때 직권조사(initiated investigation)를 할 수도 있다. 특히 중요한 공익과 관련된 프라이버시의 중대한 위반으로 판단되는 경우나 과거에 불만민원이 접수되었거나 침해신고가 있었던 정보처리단체에 대하여 이의제기가 접수된 경우에는 더욱 중점적으로 법규준수여부를 직권조사하고 있다. 커미셔너는 민원조사 또는 자체적인 조사와 관련하여 위법행위가 있다고 판단되는 경우에는 연방법원에 금지명령 또는 강제명령을 청구할 수 있는데, 금지명령은 해당 단체가 법위반이 될 수 있는 행위를 하지 않도록 금지하는 명령이고 강제명령은 단체가 법에 부합하는 조치를 취하도록 강제하는 명령이다.

이 외에도 커미셔너는 개인정보나 프라이버시에 영향을 주는 기술발달이나 사회적 변화에 대한 연구를 수행하며, 민간단체나 협의체에서 제정하는 프라이버시 규약이 법규범이나 정보보호원칙에 위반되지는 않는지를 심사하여 승인하는 역할을 한다.

〔표 4-35〕 호주 프라이버시커미셔너의 주요기능

주요기능	세부내용
피해구제	· 핫라인 구축을 통한 상담 및 이의제기 신청접수 · 민원신청에 따른 개인정보(프라이버시) 침해여부 사실조사 · 화해 또는 조정을 통한 분쟁해결 · 공식적 결정(determination)을 통한 사건해결 · 정보주체의 개인정보 접근권 행사 지원 및 보호
조사·감독	· 프라이버시 침해여부에 대한 직권 실태조사 및 모니터링 · 법규 준수여부 감독 · 법규위반 확인시 검찰 등 해당기관 이첩 · 공공기관의 데이터대조프로그램 사용현황 조사·감독

프라이버시 규약	· 민간부문의 프라이버시 규약(Code of practice) 심사 및 승인
정보제공	· 개인과 사업자, 정부에 대하여 각각 정보제공 · 각 영역별 지침 제공
정책 및 입법자문	· 입법시 프라이버시 관련 부문에 대하여 심사 · 정부의 각종 정책에 대하여 의견제시 및 자문
개인정보 보호연구	· 프라이버시 관련 기술 및 사회적 발달에 관한 연구수행
교육홍보	· 각종 단체에 대한 개인정보보호교육 실시 · 언론 등에 대한 프라이버시커미셔너 활동 등 홍보
유관기관 협력	· 국내 개인정보 유관기관 및 시민단체와의 협력 · 해외 개인정보보호기구와의 국제협력

라. 개인정보피해구제 절차 및 방법

호주의 프라이버시커미셔너는 유럽의 개인정보보호기구들과는 달리, 정보처리자에 대한 조사·감독을 통한 규율이나 제재의 측면보다는 개인정보침해 또는 프라이버시 침해로 인하여 고통받고 있는 피해자의 불편사항이나 어려움을 해소해주고 그 피해를 구제해주는 것에 더욱 중점을 두고 있다.[255]

커미셔너는 주로 핫라인과 같은 전화상담[256] 등을 통해 개인의 프라이버시를 침해할 수 있는 행위, 민간영역의 승인규약 위반[257] 또는 NPP 위반행위, 프라이버시법 제95조B에 따라 서비스 제공을 위해 연방기관과 계약을 체결한 서비스제공자의 프라이버시 침해행위, 소비자 신용정보, 세금정보, 범죄정보와 관련된 민간단체의 프라이버시 침해행위 등의 사

255) 프라이버시커미셔너는 2000년에는 194건, 2001년 632건, 2002년 1090건의 민원을 접수받아 처리하였으며, 올해 3월까지는 408건의 민원을 접수, 처리하였다. (http://www.privacy.gov.au/about/complaints/index.html)

256) 프라이버시커미셔너는 전화 또는 서면을 통한 질의·상담을 접수받아 처리하고 있는데, 작년 한해 전화상담은 총 21,290건이었으며 서면질의는 2,382건에 이르렀다. 올해 3월까지 접수된 상담건수도 전화상담 7,064건과 서면질의 804건에 이르고 있다. (http://www.privacy.gov.au/about/complaints/index.html 참조)

257) 커미셔너로부터 승인받은 규약에서 민간단체의 자체적인 민원처리절차를 규정하고 있지 않은 경우, 피해자는 커미셔너에게 직접 이의제기를 할 수 있다.

건을 접수받아 처리하고 있다.[258] 이와 같은 사건이 접수되면, 커미셔너는 프라이버시법 제36조에 따라 사실조사를 할 수 있다. 다만 커미셔너는 신청인이 피신청인에게 사전 이의제기 없이 바로 민원을 제기한 경우에는 조사를 거부할 수 있다.[259] 따라서 신청인이 피신청인과 일차적으로 직접적인 분쟁해결시도를 하였는지 검토하여, 피신청인의 자체적인 민원처리절차를 먼저 이용토록 권고하는 절차를 거친다.

이후 커미셔너는 접수된 사건에 대하여 자료제출 요청, 필요한 정보나 문서에 대한 접근권한의 행사, 증인소환 등의 방법을 통해 사실조사를 할 수 있다.[260] 커미셔너는 사실조사를 통해 접수된 사건을 심사하고 법위반행위가 있는지 여부를 평가하여 어떠한 조치를 취할 것인지를 결정하게 된다. 따라서 해당 사건과 관련하여 당사자간 분쟁이 있을 경우에는 소송외적 분쟁해결(ADR) 원칙에 의거하여 전화, 우편, 대면 등의 방법으로 합의권고 또는 조정을 행하며[261], 법위반행위가 명백한 것으로 판단된 때에는 프라이버시법 제49조에 따라 사실조사를 중지하고 관계 형사기관에 사건을 이첩시킨다. 이 외에도 커미셔너는 직접 연방법원에 개인정보침해행위의 금지명령 또는 강제명령을 청구할 수도 있다.

그러나 커미셔너의 분쟁해결 노력에도 불구하고 당사자간 조정이 실패하였거나, 당해 사안이 심각한 개인정보 침해행위라고 판단하는 경우에는 기관의 이름으로 공식적인 결정(Formal determination)을 내릴 수 있

258) 접수되는 민원 중에는 민간단체에 의한 NPP 위반행위가 상당수를 차지하고 있으며, 그 외 소비자신용정보 위반, 공공기관의 IPP 위반 등의 행위가 있다. 특히 NPP 위반에서는 개인정보의 불법적인 이용 및 제3자 제공이 33%를 차지하여 가장 높은 비율을 점하고 있으며, 그 다음으로는 개인정보의 불법수집(20%), 개인정보 접근권 행사거부(16%), 다이렉트 마케팅에 의한 프라이버시 침해(12%) 등이 그 뒤를 잇고 있다. (http://www.privacy.gov.au/about/complaints/index.html)

259) 프라이버시법 제41조는 커미셔너가 조사를 거부하거나 더 이상 조사하지 않을 것을 결정할 수 있는 경우를 규정하고 있다. 따라서 커미셔너는 제42조에 따라 제41조의 상황에 해당하는지 여부를 판단하기 위해 사전 질의를 할 수 있다. 그러나 커미셔너가 피신청인에 대하여 사전에 이의제기를 하거나 자체적인 민원처리절차를 거치는 것이 적절치 않다고 판단한 경우에는 조사가 가능하다.

260) 다만, 커미셔너는 프라이버시법 제43조에 따라 사실조사방법상 일정한 한계를 가진다.

261) 이러한 과정에서 커미셔너가 행하는 분쟁해결방법은 대부분 금전적 보상보다는 시정조치나 침해행위중지 등과 같은 주로 피신청인이 취하는 조치와 관련된 것이다.

다. 이 경우 커미셔너는 침해행위를 한 자에게 경제적·정신적 손해에 대한 배상명령이나 시정명령, 원상회복, 금지명령, 법위반사실 공표, 사과명령 등을 내릴 수 있는 권한이 있다.[262] 커미셔너의 이러한 '결정'은 피신청인이 이행을 회피할 경우, 신청인이 법원에 이행청구소송을 제기할 수 있다는 점에서 의미가 있다. 그러나 법원은 동 사건에 대한 이행청구소송이 제기되었을 때 커미셔너가 결정하고 심사한 내용과는 관계없이 독자적으로 자료 등을 수집하고 당사자로부터 소명자료를 제출받는 등 별도의 사실확인 및 심리절차를 거치는 바, 피신청인이 적극적으로 상대방과 협의하여 보상금을 지불하려 하지 않고 회피하거나 기타 커미셔너의 결정사항을 충실히 이행하지 않을 우려가 있다고 한다.[263]

또한 신청인은 결정 과정에서 절차상의 문제가 있었다고 판단되는 경우에는 「행정결정법(사법심사) 1977(Administrative Decisions (Judicial Review) Act 1977)」 제5조에 따라 연방법원에 사법심사를 청구할 수도 있는데, 이는 커미셔너의 결정이 절차적 공정성을 확보하도록 담보하고 있다. 다만, 신청인의 요청에 의해 가능한 심사사항은 결정 그 자체에 관한 것이 아니라, 법률상 오류(error of law)[264], 관할이 아닌 경우, 자연적 정의(natural justice)[265] 위반과 같은 절차적 문제이다.

---

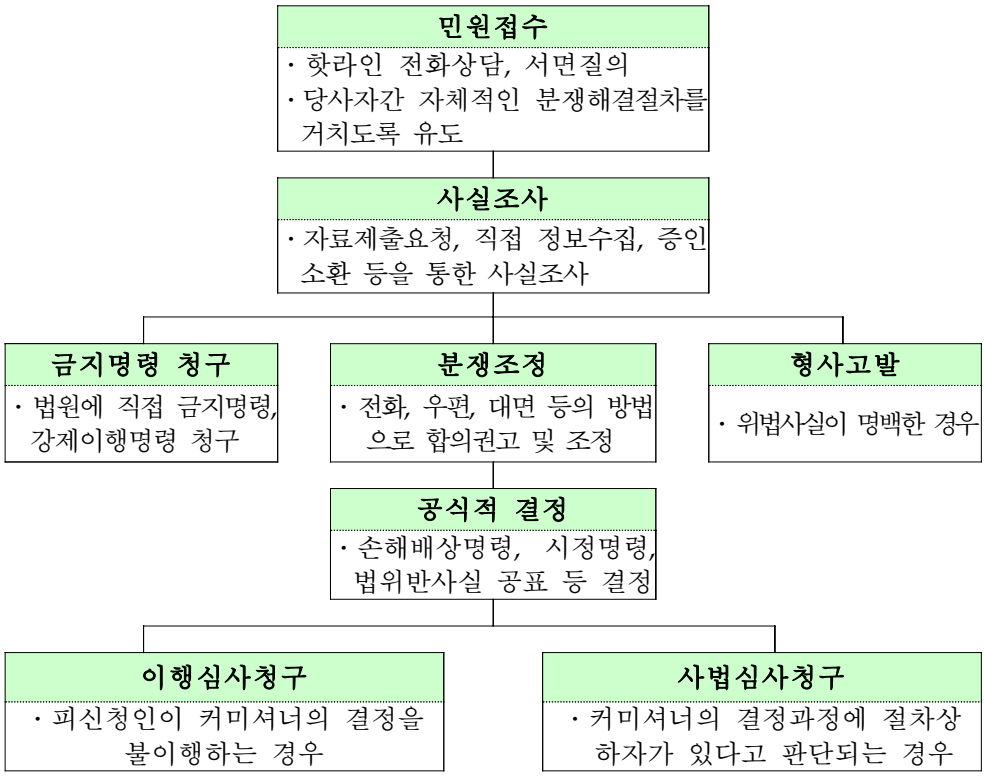
262) 호주의 프라이버시법 제52조는 이러한 프라이버시커미셔너의 결정권한을 규정하고 있다. 그러나 이러한 커미셔너의 권한은 이행을 위한 강제력을 가지지는 않는다.

263) 즉, 본래 피신청인은 사실조사에 관한 심사를 다시 하기 위한 수단으로 소송을 개시할 수는 없으나, 신청인의 이행심사청구로 인하여 법원이 새롭게 청문을 시작하게 되면 사실상 피신청인이 항소권을 가지게 되는 결과가 되는 것이다. 따라서 피신청인은 커미셔너의 결정에 대하여 사실상 사건의 본안(실체적 측면)에 대하여 항소권을 가지게 되는 효과를 얻는 반면, 신청인은 연방법원에 절차적 측면에 대한 심사청구만을 제한적 범위 내에서 할 수 있기 때문에 오히려 불합리한 결과가 발생한다. (Graham Greenleaf, *"Enforcement of the Privacy Act : Problems and Potential"*, 2001, http://austlii.edu.au/~graham/publications/2001/enforcement.html)

264) 법률상 오류(error of law)란, 법률상의 하자를 의미하는 것으로 사실심에서 허용되지 않는 증거를 허용하는 결정을 내린 경우에 그 법적 판단이 상소의 이유가 되는 것과 같은 오류를 말한다.

265) 자연적 정의(natural justice)란, (법원 이외의 기관에 의한) 결정 또는 재판에 대한 사법심사에 원용되는 지도원리로, (1) 재판관이 편견을 가지고 있지 않을 것이 요구되며(실제로 편견이 없을 것이 요구될 뿐 아니라 공정성의 외관을 겸비하고 있을 것이 요구됨), (2) 공정한 고지와 청문이 이루어져야 하고, (3) 별도의 중대한 이유

호주의 프라이버시커미셔너는 이와 같이 프라이버시법에 따라 개인정보보호기관이 법위반여부를 심사하여 결정할 수 있도록 권한을 가지고 있다. 그러나 실질적으로 호주의 프라이버시커미셔너가 동 권한을 행사하여 결정을 내린 사안은 1993년 이래 단 세 건에 그치고 있다.[266]



(그림 4-13) 호주 프라이버시커미셔너의 피해구제 절차도

한편 호주는 2000년 프라이버시법 개정으로 프라이버시법의 규율영역이 민간으로 확대됨에 따라, 민간부문의 분쟁해결을 위한 공동규제체계(Co-regulatory scheme)를 마련한 바 있다. 공동규제는 각 민간부문이 스스로 개발·실행하는 실행규약에 대한 공식적인 승인을 획득할 수 있는

가 없는 한 공개심리일 것이 요구된다.

266) 호주의 연방프라이버시커미셔너가 공식적 결정은 한 사건은 1993년 2건, 2003년 1건으로 총 3건이다.

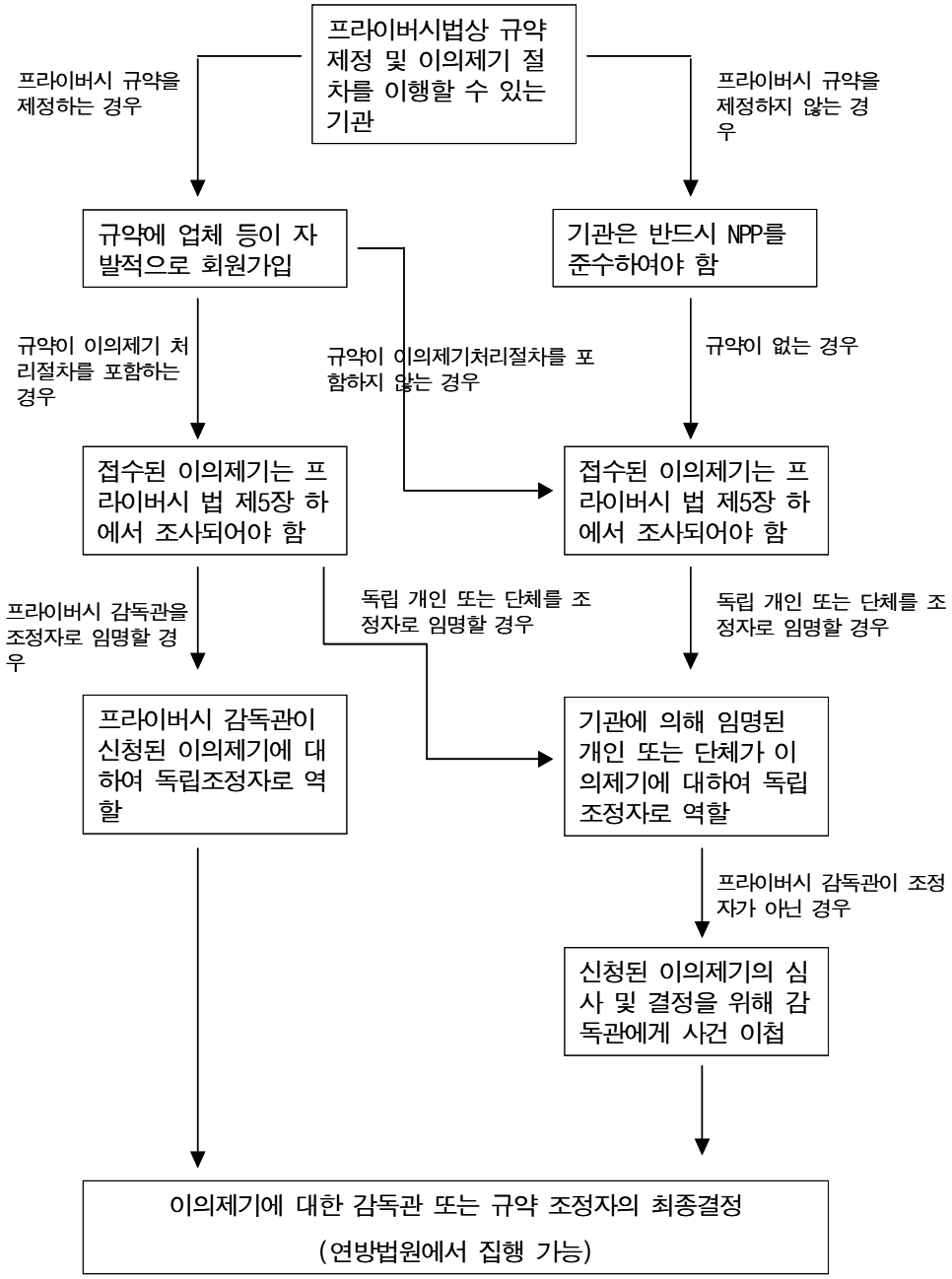
하나의 법적 체계로 생각될 수 있으며, 민간단체가 개별적으로 프라이버시 규약을 가질 수 있도록 보장함으로써 프라이버시에 보다 유연하게 접근할 수 있도록 하고, 동시에 소비자에게는 그들의 개인정보가 법의 최소한의 기준에 부합되는 기준에 따라 보호되도록 하는 기능을 하고 있다.[267] 호주의 공동규제체계는 민간단체가 법규범의 틀 안에서 NPP를 시장수요 또는 특정한 산업적 특성에 적합하게 변경할 수 있는 여지를 제공하며, 독립적인 규약 조정자로서 프라이버시커미셔너 또는 제3의 조정자를 산업계에 기반을 둔 민원처리 체계 내에 임명할 수 있도록 함으로써 자발적인 분쟁해결제도의 구축과 피해구제제도의 운영을 도모하고 있다. 그러나 이러한 공동규제 접근법이 업계의 특수성을 반영한 유연성을 제공한다고 할지라도, 개인의 프라이버시 권리가 규약의 사용으로 인하여 약화되어서는 안 된다.

공동규제체계로 인하여, 민간분야의 개인정보피해구제에 있어 호주 프라이버시커미셔너는 다소 다른 기능을 하고 있다. 즉, 민간단체나 특정분야의 사업자협의체에서 프라이버시 규약을 제정하여 커미셔너로부터 승인을 받은 경우, 해당 단체의 정보처리로 인하여 피해를 입은 자는 먼저 커미셔너로부터 승인을 받은 규약에서 정한 분쟁해결절차에 따라 피해구제를 받고자 시도하여야 한다. 이 경우 프라이버시 규약은 불만사항의 해결이나 분쟁조정을 위해 독립조정관을 임명할 수 있는데, 독립조정관은 커미셔너가 될 수도 있고 제3자가 될 수도 있다.

［표 4-36］ 민간영역에서의 분쟁해결주체

구분	분쟁조정의 역할담당자
NPP의 적용을 받는 일반단체	커미셔너
민원처리절차가 없는 규약을 가진 단체	커미셔너
민원처리절차가 있는 규약을 가진 단체	커미셔너 또는 기타 제3자

267) 이러한 점에서 호주의 '공동규제'는 '자율규제(Self-regulation)'와 구분된다고 할 수 있다. 즉 공동규제체계에 따르면, 법에 의해 규약을 가질 수 없도록 정해진 단체들은 반드시 프라이버시법의 NPP 원칙에 따라 개인정보를 처리해야 하고 NPP와 승인된 규약은 모두 법에 근거하여 실행가능한 것이어야 하기 때문이다.



(그림 4-14) 호주 공동규제체계에 따른 피해구제 절차도

2. 뉴질랜드

뉴질랜드는 호주·영국과 유사한 형태의 개인정보보호법제를 도입·운용하고 있다. 이러한 법질서의 가장 상위에 있는 것은 헌법과 같은 역할을 하는 「1990년 권리장전법(Bill of Right Act 1990)」이다. 동법은 시민의 기본적 자유와 인권에 관한 규정을 두고 있는데, 특히 "누구든지 신체·재산·서신 기타의 불합리한 압수·수색으로부터 보호되어야할 권리를 가진다"고 한 규정은 뉴질랜드 법원으로부터 프라이버시권을 구성하는 중대한 가치와 이익을 보호하기 위한 것으로 해석되어왔다.[268]

그러나 무엇보다도 직접적으로 개인의 사적 자유와 프라이버시, 개인정보에 대하여 법적으로 보장하고 있는 법률은 바로 「1993년 프라이버시법(The Privacy Act 1993)」이다. 이하에서는 동법을 중심으로 그 주된 내용을 살펴보고, 동법에서 규정한 개인의 권리와 그 구제방법 등 개인정보피해구제제도에 대해 살펴보기로 한다.

가. 프라이버시법의 주요내용

뉴질랜드의 프라이버시법은 프라이버시커미셔너의 설립과 정보조합(information matching)의 시행요건에 대해서 규정하고 있는 「1991년 프라이버시커미셔너법(The Privacy Commissioner Act 1991)」에 이어 제정된 법률로서 1993년 7월 1일부터 시행되었다. 동법은 1993년 제정된 이래 2000년까지 총 6차례의 개정을 거쳤다.

프라이버시법의 제정목적은 OECD 가이드라인에 따라 개인의 프라이버시를 보호하고 특정 개인을 식별할 수 있는 개인정보를 직접 규율함으로써 올바른 정보처리 관행을 확립하는 것이다. 이를 위해 동법은 순수하게 개인적인 목적이나 가족생활과 관련된 개인정보의 처리를 제외한 공공부문과 민간부문의 거의 모든 개인정보처리를 관장하고 있다.[269]

---

268) EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/newzealand.htm 참조.

특히 동법은 개인정보를 취급하는 공공기관이나 사업자, 기타 비영리 민간단체 등이 지켜야 할 12가지 정보프라이버시원칙(IPP : Information Privacy Principles)과 공공등록부의 부정사용을 금지하기 위한 「공공등록부상의 프라이버시원칙(PRPP : Public register privacy principles)」을 규정함으로써, 개인정보의 수집・이용・처리의 기준을 제시하고 있다. 이외에도 프라이버시법은 동법이 올바르게 시행될 수 있도록 권한과 의무를 부여받은 프라이버시커미셔너에 관한 사항을 규정하고 있으며, 기타 피해구제절차 및 방법, 공공기관에 의한 정보조합프로그램의 사용규제, 내부 프라이버시 담당관의 임명[270] 등에 대하여도 폭넓게 규정하고 있다. 이하에서는 프라이버시법의 주요 내용인 개인정보보호원칙의 내용을 살펴보기로 한다.

(1) 정보프라이버시원칙

뉴질랜드의 프라이버시법은 공공부문과 민간부문에 모두 적용되는 개인정보보호 기본원칙으로 '정보프라이버시원칙'을 규정하고 있다. 이는 OECD 가이드라인의 프라이버시 8원칙과 호주의 정보프라이버시원칙을 기초로 하여 제정된 것으로, 정보주체의 권리를 비롯하여 정보처리자가 준수하여야 할 의무사항 등에 대하여 규정하고 있다.

---

269) 뉴질랜드의 프라이버시법 제2조는 동법의 적용을 받지 않는 단체를 열거하고 있다. 이에 따르면 총독(Governor-General), 국회의원, 옴브즈만, 법원 등은 동법의 적용범위에서 제외되며, 언론기관도 취재 등 언론보도활동과 관련한 정보처리에 대해서는 동법의 적용을 받지 않는다.

270) 내부 프라이버시담당관(Privacy Officer)은 정보처리자로부터 임명되는 자로서, 정보처리단체가 올바르게 프라이버시법 내지 IPP 등을 이행하고 있는지 여부를 확인하고 검토하는 역할을 한다. 또한 프라이버시 및 개인정보와 관련된 각종 불만사항을 책임지는 자이며, 프라이버시커미셔너가 해당 정보처리단체의 프라이버시 침해여부를 조사할 때 협조할 의무를 부담한다.

〔표 4-37〕 뉴질랜드 정보프라이버시원칙

구분		주요 내용
수집	원칙 1	단체의 활동, 역할과 관계있는 합법적인 목적을 위한 개인정보 수집 및 목적에 적합한 개인정보의 수집
	원칙 2	정보주체로부터의 직접 수집원칙
	원칙 3	정보주체로부터 개인정보 수집시 고지의무
	원칙 4	불법적인 방법, 불공정하거나 개인의 사적 생활을 불합리할 정도로 침해하는 방법에 의한 개인정보 수집금지
관리	원칙 5	개인정보의 손실, 권한없는 접근·이용·변경·유출, 오남용의 방지를 위한 안전조치 확보
권리	원칙 6	개인정보의 보유여부 확인 및 열람에 관한 정보주체의 권리
	원칙 7	잘못된 개인정보에 대한 정정요구권
이용 공개	원칙 8	개인정보 이용 전 목적과의 관련성, 정보정확성·최신성·완전성 등 확보
	원칙 9	목적 달성 후 필요 이상의 개인정보 보유 금지
	원칙 10	수집 목적을 초과한 개인정보의 이용 금지
	원칙 11	수집 목적을 초과한 개인정보 제3자 제공 금지
	원칙 12	신원식별인자(Unique identifier)에 대한 제한

이 중 정보주체로부터 직접 개인정보를 수집토록 하고 있는 제2원칙은 사실상 폭넓은 예외를 규정하고 있는데, ① 다른 원천으로부터 개인정보를 수집하는 것에 해당 정보주체가 동의한 경우, ② 당초의 개인정보 수집목적이나 이유를 침해할 우려가 있는 경우, ③ 범죄수사, 탐지, 예방 등을 포함한 법집행을 위한 경우, ④ 공익을 위한 경우, ⑤ 다른 법에 의해 정보수집절차가 규정되어 있는 경우가 그것이다. 또한 제3원칙에 의하면, 정보처리자는 정보주체로부터 직접 개인정보를 수집할 때에는 수집 전후에 해당 정보주체에게 소정의 사항을 고지하여야 한다. 그러나 유사한 정보에 대하여 최근에 수집한 적이 있는 경우에는 다시 고지할 필요는 없다. 여기서 정보처리자가 고지할 사항은 ① 개인정보의 수집사실, ② 수집목적, ③ 개인정보를 제공받기로 예정되어 있는 제3자, ④ 개인정보를 수집하는 단체 및 향후 보유할 단체의 명칭 및 주소, ⑤ 개인

정보의 수집이 법에 의해 이루어지는 경우 해당 법규정 및 강제사항인지 여부, ⑥ 개인정보 수집에 반대할 경우 개인에게 미칠 수 있는 영향, ⑦ 정보주체의 열람·정정권에 관한 사항이다.

한편 정보프라이버시 제6원칙과 제7원칙은 정보주체의 권리에 대하여 규정하고 있다. 이에 따르면 정보주체는 자신의 개인정보가 보유되고 있는지를 확인하고 열람할 수 있으며, 잘못된 내용이 있을 때에는 정정을 요청할 수 있다. 정보처리자는 정보주체의 열람요청을 받은 경우 그 가부에 대한 답변을 업무일 20일 내에 하여야 한다. 단, 요청하는 정보의 양이 많거나 복잡한 자문이 필요하여 정해진 기간 내에 답변이 어려운 경우에는 20일 이내에 정보주체에게 시간이 더 소요될 것임을 밝혀야 한다. 또한 정보주체의 권리행사를 방해할 정도로 지나치게 과도한 비용을 청구하여서는 안 된다.

정보프라이버시원칙 중 특이한 사항은 당해 개인을 바로 특정할 수 있는 식별인자(Unique Indentifier)의 사용제한에 대한 내용을 담고 있다는 점이다. '식별인자'란 사회보장번호, 운전면허번호, 여권번호 등과 같이 특정한 개인을 바로 식별할 수 있는 고유인자를 의미한다. IPP는 공공단체는 물론 민간단체도 개인정보를 처리할 때 당초의 정보처리 목적과 직접적 관련성이 있거나 반드시 그 목적수행을 위해 필요한 경우가 아닌 이상 고유한 식별인자를 개인에게 할당하여서는 안 된다고 규정하고 있다.

이러한 정보프라이버시원칙은 일반적인 내용을 담고 있는 것인 바, 특정 영역에 적용될 수 있도록 동 원칙의 적용을 다소 변경하는 실행규약(Code of Practice)이 제정될 수 있다. 실행규약은 전면적으로 정보프라이버시원칙을 수정할 수도 있고 부분적으로 수정하거나 일부 원칙의 적용을 배제할 수 있다.[271] 그러나 개인정보보호를 위해 필수적인 사항에 대해서는 실행규약에 의해 침해할 수 없다.[272]

---

271) 실행규약은 특정 산업 또는 기관의 특수성이나 해당 단체에서 처리하는 개인정보 유형의 성격 등을 고려하여 IPP 원칙을 강화할 수도 있고 다소 완화시킬 수도 있다. 실행규약이 최종 제정되어 시행되기 위해서는 특별하고 긴급한 사유가 없는 한 일반 대중에게 공표하여 사전심사절차를 거쳐야 한다.

272) 현재 의료분야에 적용되는 「건강정보프라이버시규약(The Health Information

(2) 정보등록부상의 프라이버시원칙(PRPP)

정보등록부상의 프라이버시원칙은 공공등록부에서 정보를 이용할 수 있는 절차 및 방법에 대해 규율하고 있다. 공공등록부는 법에 의해 수집・보유・관리되는 것으로 선거인명부, 혼인신고대장, 부동산등기부, 출생・사망기록부, 법인등기부, 운전면허등록부, 자동차등록부 등이 해당된다. 이렇듯 공공등록부는 다른 법률에 의해 생성되고 개인정보의 수집 등 처리에 대해서도 다른 법률에 그 근거가 있는 것이어서 PRPP는 등록부를 생성하도록 규정하고 있는 법률의 내용을 무효로 할 수는 없다. 그러나 동 원칙은 상업적 목적을 위해 공공등록부상의 정보를 다른 정보와 상호결합하거나 재분류하는 행위, 공공등록부를 전자적으로 전송하는 행위, 공공등록부상의 정보에 대하여 접근을 요청하는 것에 대하여 불합리한 비용을 부담케 하는 행위 등을 제한함으로써 공공등록부의 적절하고 올바른 이용・관리를 장려하고 있다.

나. 뉴질랜드의 개인정보보호기구

뉴질랜드의 대표적인 개인정보보호기구로는 프라이버시커미셔너를 들 수 있다. 커미셔너는 프라이버시법과 정보프라이버시원칙을 이행하는 역할을 담당하고 있으며, 뉴질랜드의 개인정보보호 전담기구라는 특징을 가진다. 또한, 뉴질랜드에는 공공기관이 보유하고 있는 정보에 대한 시민들의 접근권 행사와 관련된 업무를 맡아온 옴브즈만(Ombudsman)이 설치되어 활동하고 있으며, 프라이버시커미셔너나 옴브즈만을 통해 해결되지 못한 사건을 심사하는 인권법원(The Human Rights Review Tribunal)이 있다.

Privacy Code 1994)」을 비롯하여, 「고령연금제도의 신분확인에 관한 규약(Superannuation Schemes Unique Identifier Code 1995)」,「EDS 정보프라이버시 규약(EDS Information Privacy Code 1997)」,「사법영역에서의 신원식별인자에 관한규약(Justice Sector Unique Identifier Code 1998)」, 「의무교육 이후과정에서의 신원식별인자에 관한 규약(Post-Compulsory Education Unique Identifier Code 2001)」, 「전자통신 정보프라이버시 규약(Telecommunications Information Privacy Code 2003)」이 제정되어 실행되고 있다.

이 중 옴브즈만은 「1982년 공공정보법(Official Information Act 1982)」 및 「1987년 지방정부공공정보법(Local Government Official Information and Meetings Act 1987)」에 근거하여, 프라이버시 법이 제정된 1993년 7월 1일 이전의 공공기관에 의해 보유되고 있는 '개인정보를 포함하는 공적 정보(official information)'에의 접근권 행사요청을 처리하고 있다. 옴브즈만이 처리할 수 있는 유형은 ① 일반 시민이 공공기관이 보유하고 있는 타인, 회사, 비법인 사회단체에 관한 공적 정보에 대한 접근요청을 하는 경우 또는 접근거부에 따른 이의제기를 하는 경우와 ② 공공기관에 의해 보유되고 있는 회사나 비법인 사회단체에 관한 정보를 당해 회사 및 단체가 요청하는 경우이다. 옴브즈만은 접근요청이나 민원이 접수되면 사실확인의 관점에서 관련 문제를 조사하여, 해당 사건에 대하여 접근요청 거부 등이 법위반사항인지 여부, 불합리하거나 불공정·부적절한 차별인지 여부, 불합리하거나 불공정·부적절한 차별일 가능성이 있는 법규 또는 관행에 따른 것인지 여부, 법률의 착오 내지 사실착오에 의한 행동인지 여부, 명백하게 잘못된 행동인지 여부 등을 판단한다. 옴브즈만은 최종적으로 잘못된 행위라고 판단된 경우에는 해당 기관에 시정을 권고함으로써 시민의 알 권리와 자기 정보에 관한 결정권을 보호하는 역할을 하고 있다.

그러나 무엇보다도 대표적인 뉴질랜드의 개인정보보호기구는 프라이버시커미셔너이다. 따라서 이하에서는 커미셔너를 중심으로 그 기구의 성격과 주요 기능, 피해구제 역할에 대해 살펴보도록 하겠다.

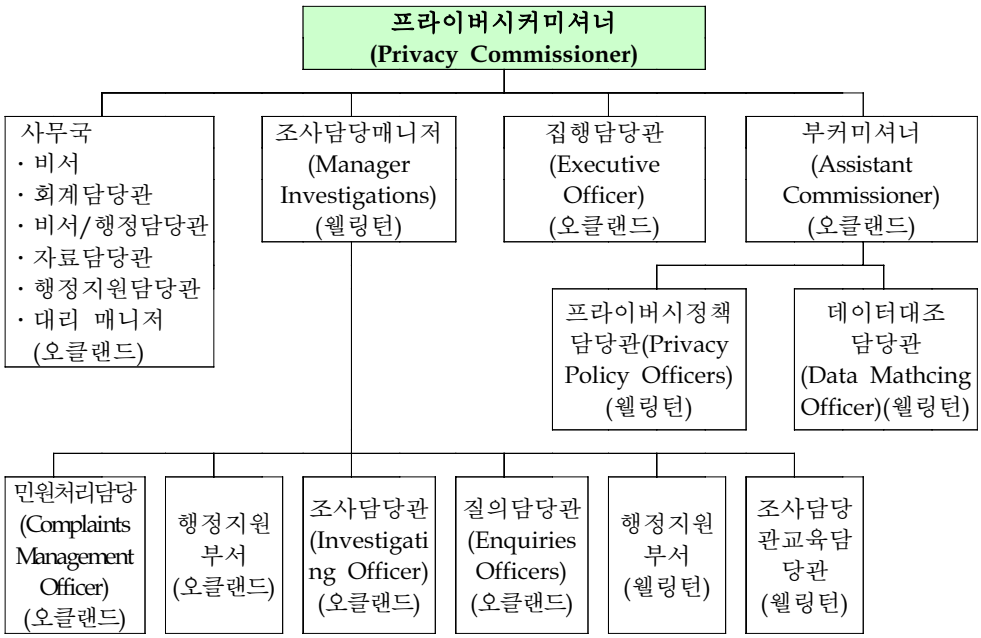
(1) 프라이버시커미셔너의 지위

프라이버시커미셔너는 왕권에 의해 직접 권한을 부여받은 독립행정기구로서 영속성을 지닌 법인으로서, 1991년 제정된 「프라이버시커미셔너법(The Privacy Commissioner Act 1991)」에 근거하여 설립된 법정기구이다. 프라이버시커미셔너는 법무부 장관의 추천에 따라 총독(Governor-General)이 임명하며 임기는 5년이며 재임이 가능하다. 프라이버시커미셔너는 개인의 프라이버시에 영향을 줄 수 있는 사안이나 문제

들에 대해 수상(Prime Minister)에게 직접 보고할 권리를 가진 독립 개인정보보호기구이다. 또한 프라이버시커미셔너는 예산 등 「1989년 공공재정에관한법률(The Public Finance Act 1989)」에서 정하는 사항에 대해서는 법무부장관을 통하여 의회에 보고할 의무가 있다.

(2) 프라이버시커미셔너의 조직구성

동 기구는 프라이버시커미셔너 1인과 부커미셔너 1인, 조사·행정 등의 업무를 담당하는 담당관 및 사무국으로 구성된다. 사무국은 2002년 6월말 기준, 행정업무 담당자와 비정규직을 포함한 32명의 직원으로 구성되어 있으며, 직원의 채용은 프라이버시커미셔너가 독자적으로 행한다.[273] 프라이버시커미셔너의 조직구성 체계를 살펴보면 다음과 같다.



(그림 4-15) 뉴질랜드 프라이버시커미셔너 조직도

273) Privacy Commissoner of New Zealand, *"Annual Report of the PRIVACY COMMISSIONER 2001-2002"*, p.12, http://www.privacy.org.nz/recept/rectop.html

(3) 프라이버시커미셔너의 주요기능

프라이버시커미셔너는 주로 뉴질랜드의 개인정보 또는 프라이버시 보호를 위한 기본법인 1993년 프라이버시법을 관장하고 있다. 따라서 개인정보보호 기본법인 프라이버시법이 적용되는 모든 영역에 대하여 관할하고 있다. 즉, 공공부문은 물론이고 원칙적으로 모든 민간부문의 개인정보 수집・이용・처리에 대하여 관리하고 감독한다. 다만, 1993년 7월 1일 이전에 공공기관에 의해 수집・보관되고 있는 개인정보를 포함한 공공문서에 대한 접근권의 행사 및 동 권리의 침해에 대해서는 옴브즈만이 담당하고 있음은 앞에서 살펴본 바와 같다.

프라이버시커미셔너는 개인정보 취급자가 프라이버시법과 정보프라이버시원칙 또는 실행규약에 따라 적절한 방법으로 개인정보를 취급하고 보호하도록 하는 임무를 맡고 있다. 이러한 임무를 수행하기 위해 프라이버시커미셔너가 행하는 구체적인 기능은 크게 ① 화해 또는 조정을 통한 개인정보피해구제, ② 공공기관의 정보조합프로그램 사용규제[274] 등 개인정보침해여부 실태조사 또는 법규준수여부 감독, ③ 각종 프라이버시 실행규약 제정, ④ 개인정보 관련 질의접수・처리 및 개인정보보호법령 등에 관한 정보제공, ⑤ 정부와 공공기관 및 의회에 대한 입법안 검토 및 정책자문, ⑥ 프라이버시 관련 조사 및 연구, ⑦ 개인정보보호 교육 및 홍보, ⑧ 국내외 유관기관 협력 등이다. 이를 자세히 살펴보면 다음과 같다.

---

274) 커미셔너는 정보조합프로그램의 사용규제를 위해, 일차적으로는 정보조합프로그램의 사용을 규정하는 입법에 대해 프로그램 사용으로 인한 중대한 이익이 있는지, 프라이버시를 침해하는 것은 아닌지, 정보조합을 대체할 수 있는 방법이 본래의 이익과 유사한 이익을 만들어낼 수 있는지, 여러 정보처리자가 보유하고 있는 개인정보를 지나치게 많이 이용하고 공유하는 것은 아닌지 등을 심사하여 법무부에 의견을 제시하는 역할을 한다. 또한 정보조합프로그램이 프라이버시법 기타 정보조합에 관한 규칙에 부합하는 것인지를 세부적으로 검토하고 평가하여 그 결과를 법무부에 매년 보고한다.

［표 4-38］ 뉴질랜드 프라이버시커미셔너의 주요기능

주요 기능	세부내용
피해구제	· 민원접수 및 프라이버시 침해여부에 대한 사실조사 · 당사자 의견청취, 회의 소집, 화해·조정 등을 통한 분쟁해결 · 분쟁사건에 대한 의견제시 · 인권소송담당관에게 미해결 민원사건 이관하여 인권법원으로 소제기 검토 및 결정 · 정보주체의 개인정보 접근권 행사 지원 및 보호
조사·감독	· 프라이버시 침해여부에 대한 직권 실태조사 및 모니터링 · 법규 준수여부 감독 · 정부의 정보조합프로그램 사용에 대한 인가 및 규제 · 법규위반 확인시 검찰 등 해당기관 이첩
실행규약	· 실행규약의 제정 및 고시 · 특정영역에 대해서 정보프라이버시원칙의 내용을 수정하는 프라이버시 규약 제정하여 적용
정보제공	· 개인과 사업자, 정부에 대하여 각각 정보제공 · 상담팀 운영하여 서면 및 전화질의 접수, 처리 · 사회적으로 문제되는 프라이버시 사안에 대하여 지침제공
자문	· 프라이버시 관련 법안 심의 및 의견제시 · 정부의 각종 정책에 대하여 의견제시 및 자문
연구	· 프라이버시 관련 기술발전상황 조사 및 연구
교육홍보	· 각종 단체에 대한 개인정보보호교육 실시 · 언론 등에 대한 프라이버시커미셔너 활동 등 홍보
유관기관 협력	· 국내 개인정보 관련 유관기관 및 시민단체와의 협력 · 해외 개인정보보호기구와의 국제협력

다. 개인정보피해구제 절차 및 방법

(1) 프라이버시커미셔너의 피해구제 절차 및 방법

뉴질랜드의 프라이버시커미셔너는 앞에서 살펴본 바와 같이 다양한 개인정보보호의 역할과 기능을 담당하고 있지만, 무엇보다도 개인정보침해를 입은 자의 피해를 구제해주는 기능에 중점을 두고 활동하고 있다. 실

제로 프라이버시커미셔너는 상당수의 '프라이버시 침해'[275]에 대한 불만이나 이의제기 사건을 다루고 있을 뿐 아니라, 정보주체의 개인정보 열람요구권과 관련된 각종 민원도 함께 처리하고 있다.

〔표 4-39〕 뉴질랜드 프라이버시커미셔너의 피해구제현황

구분	1997/98	1998/99	1999/00	2000/01	2001/02
상담	11,141	6,971	5,803	6,563	6,772
민원접수사건	1088	1003	798	881	1044
종결사건	804	895	956	806	1049

※ 참고 : Privacy Commissoner of New Zealand, *"Annual Report of the PRIVACY COMMISSIONER 2001-2002"*, p.12, http://www.privacy.org.nz/recept/rectop.html

이러한 침해행위에 대한 민원이 제기될 경우, 보통 커미셔너는 사실조사에 착수하기에 앞서 신청인이 해당 정보처리자에게 먼저 이의제기를 하여 분쟁을 해결해보도록 권고한다. 그러나 사전에 반드시 정보처리자의 자체적인 분쟁해결절차를 거쳐야 하는 것은 아니다. 또한 커미셔너는 접수된 사건이 관할대상이 아닌 때에는 프라이버시법 제71조의 규정에 따라 사실조사를 하지 않고 사건을 종결처리할 수 있으며, 특히 옴브즈만 등 다른 기관에 이첩함이 타당하다고 여겨지는 사건은 접수 즉시 이첩할 수 있다.

커미셔너는 접수된 사건에 대해 바로 공식적인 조사에 착수하지는 않으며, 신속한 피해구제를 위해 먼저 민원처리담당관의 일차평가과정을 거친다. 민원처리담당관은 전화, 서면 등을 통해 간단히 사실관계를 파악한 후 대부분 화해, 조정 등의 비공식적인 분쟁해결방법을 이용하여 사건해결을 도모하고 있다.[276] 그러나 첫 번째 단계에서 분쟁이 해결되지

275) 여기서 프라이버시 침해란 정보프라이버시원칙 위반, 공공등록부상의 정보프라이버시원칙 위반, 커미셔너가 제정한 실행규약 위반, 정보대조와 관련된 법률 규정 위반 행위를 의미한다.

276) 프라이버시커미셔너는 작년 한해 전체 처리한 사건 중 61.5%를 개인정보침해여부 조사에 착수하기에 앞서 민원처리담당관의 일차 평가과정에서 화해유도나 조정 등의 노력을 통해 비공식적으로 해결하였다고 한다.(Privacy Commissioner of New

않는 경우, 커미셔너는 사전 사실조사 및 확인작업을 거친다. 이 때에는 당사자 의견청취, 자료제출 요청 등을 통해 기초적인 사실관계를 확인한다. 커미셔너는 이 단계에서도 당사자간 화해를 유도하여 분쟁을 해결하는 역할을 계속한다. 그러나 때때로 민원담당관 등의 화해유도만으로는 분쟁이 원만히 해결되기 어려운 사건들이 있다. 이 경우 커미셔너는 당사자 소환, 증거자료 요청, 증인신문 등을 통해 공식적인 사실조사에 착수하게 된다. 이 때에는 다소 시일이 걸리더라도 정보처리자의 프라이버시 침해행위가 존재하는지 여부를 보다 더 철저하게 조사한다. 커미셔너는 이러한 추가적인 사실조사과정에서도 개인정보침해 여부에 대하여 중간의견을 제시할 수 있으며, 이를 신청인 또는 피신청인이 수용하여 사건이 종결되는 경우도 있다. 따라서 대부분의 사건이 커미셔너의 최종적인 의견을 구하는 단계까지 가지 않고 해결되고 있다.[277]

그러나 이러한 사전 조정절차가 실효를 거두지 못한 경우 커미셔너는 최종적인 의견(Final Opinion)을 제시하여 당사자에게 권고할 수 있다. 그러나 커미셔너의 의견제시는 어떠한 강제력이 있거나 법적 구속력을 가진 것은 아니다.

한편 이러한 절차를 통해서도 사건이 완결되지 못하는 경우, 커미셔너는 신청인에게 인권법원에 심사청구할 수 있는 권리가 있음을 알려주거나, 인권소송담당관(Director of Human Rights Proceedings)에게 사건을 이첩할 수 있다. 인권소송담당관은 이첩받은 사건을 인권법원(The Human Rights Review Tribunal)에 소제기를 할 것인지 여부를 결정하는 역할을 한다.

지금까지는 커미셔너가 행하는 개인정보피해구제 절차 및 방법에 관한 내용을 살펴보았으나, 사안별로 커미셔너가 행할 수 있는 피해구제방법은 다소 차이가 있는데 이를 살펴보면 아래와 같다.

Zealand, supra note 273, p.16)

277) 지난 회계연도 동안 처리된 사건 중 85%가 커미셔너의 공식적인 최종의견 없이 해결되었다고 한다. Ibid, p.17

〔표 4-40〕 뉴질랜드 프라이버시커미셔너의 권한

구분	IPP 1~4, 8~11 위반	IPP 5, 7, 12 위반	IPP 6 위반	정보대조 규정 위반	PRPP 위반	실행규약 위반
커미셔너의 조사권	○	○	○	○	○	○
커미셔너의 강제소집권	○	○	○	○	×	○
커미셔너의 소송담당관 사건이첩	△	○	○	○	×	○
커미셔너의 권고권	○	○	○	○	○	○
커미셔너의 정부장관에 대한 권고권	無	無	無	無	○	無
바로 기본법원에 소제기가 가능한지 여부	×	×	○(*)	×	×	×
바로 인권법원에 요청이 가능한지 여부	△	○	○	○	×	○

※ 주 : http://www.privacy.org.nz/recept/rectop.html
- △ : 1993년 7월 1일에서 1996년 6월 30일의 기간동안 이루어진 행위에 대한 민원제기에 대해서는 당해 권한이 없었음을 의미
- 無 : 해당 규정이 없음을 의미
- ○(*) : 공공영역에서 IPP 제6원칙을 위반한 경우에 대해서만 가능하며 민간영역은 제외

(2) 인권법원을 통한 피해구제

인권법원은 뉴질랜드의 인권침해와 관련된 사건을 심사하여 피해자를 사후적으로 구제하는 역할을 맡고 있는 사법적 성격을 가진 기구이다. 특히 인권법원은 프라이버시법 제82조에 따라 프라이버시법에 근거하여 프라이버시 침해에 대한 조사가 진행되었거나 화해 등 분쟁해결절차가 진행되었으나 합의에 이르지 못한 사건을 심의·결정하고 있다.

개인정보침해로 인해 피해를 입은 자는 커미셔너를 통해 그 피해를 구제받을 수 있으나, 바로 인권법원에 사후구제를 청구할 수도 있다. 또한 앞서 살펴본 바와 같이, 필요한 경우 프라이버시커미셔너가 직접 미해결 사건을 인권법원으로 소제기를 하는 경우가 있다. 지난 해 인권법원은

2000/01년도에 처리중이던 8건의 사건과 2001/02년도에 새롭게 접수된 22건의 사건으로 총 30건의 사건을 담당하였다.[278]

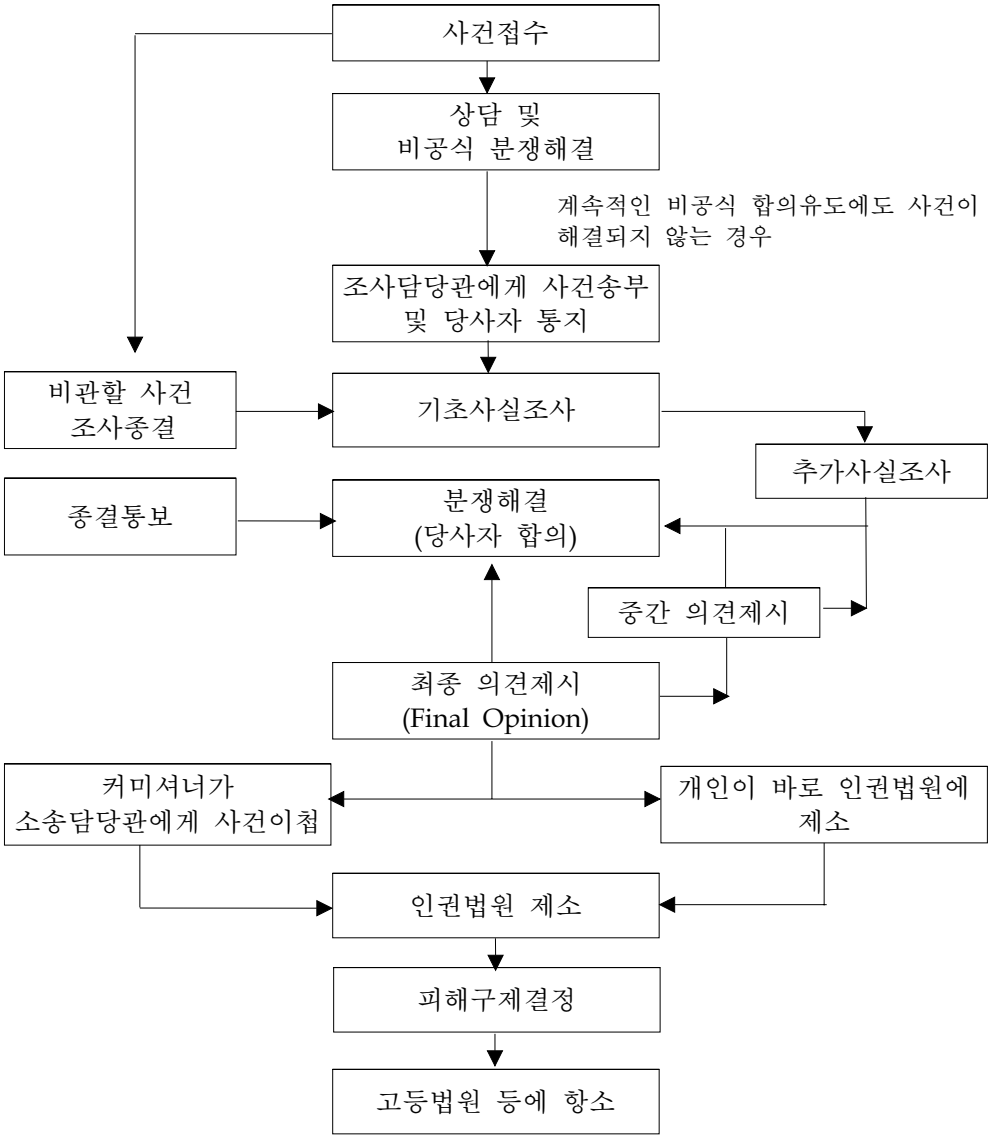
인권법원은 접수받은 사건의 프라이버시 침해여부를 심사하며, 만약 침해행위가 있다고 판단될 때에는 프라이버시법 제85조에 근거하여 법위반선언결정, 금지명령, 손해배상명령, 구제명령 등의 결정을 내린다. 이 중 금지명령은 침해의 계속 또는 반복하는 행위 및 유사한 행위를 유발·허용·개입하는 행위를 금지하는 명령이며, 구제명령은 침해교정 및 침해의 결과로 인해 발생한 개인의 손실이나 손상을 구제할 목적으로 특정행위를 실행하도록 하는 명령이다. 또한 인권법원은 정보처리자에게 프라이버시법 제88조에 따라 피해자가 입은 금전적 손해, 이익손실, 모욕·명예훼손·감정적 고통 등과 같은 정신적 손해에 대하여 배상토록 하는 명령을 내릴 수 있으며, 기타 법원이 적당하다고 생각하는 구제방법을 시행토록 결정할 수도 있다. 이렇듯 다양한 피해구제결정을 내릴 수 있기 때문에, 인권법원은 개인정보침해로 인한 피해를 보다 실질적으로 구제할 수 있다. 그러나 이러한 인권법원의 결정에 대해 불만족하는 당사자는 고등법원(High Court) 또는 항소법원(Court of Appeal)[279]에 항소할 수 있다.

마지막으로 지금까지 살펴본 프라이버시커미셔너 및 인권법원을 통한 뉴질랜드의 개인정보피해구제 절차도를 살펴보면 아래와 같다.

---

278) Privacy Commissioner of New Zealand, supra note 273, p.27

279) 실체적 법률문제에 관한 사안에 대하여 항소하는 경우에는 항소법원에 행한다.



(그림 4-16) 뉴질랜드 프라이버시커미셔너의 피해구제 절차도

제 5 절 아시아

아시아 지역에서는 대체로 '프라이버시'라는 개념이 자체적인 사회·문화적 환경으로부터 발생한 것이 아니라 서구로부터 유입된 다소 낯선 의미를 가진다. 따라서 프라이버시권 또는 정보프라이버시의 보호를 위한 법체계도 성숙되어 있지 못한 것이 현실이다. 그러나 최근 아시아 지역은 새로운 경제성장 동력의 하나로 IT기술의 발달을 적극 추진하면서 이로 인해 발생할 수 있는 개인정보 침해문제에 대응하기 위한 제도 마련에 관심을 가지기 시작하였다. 그 중에서도 홍콩은 영국 등 유럽과 유사한 형태의 개인정보보호 체계를 갖추는 등 아시아 지역에서는 가장 먼저 개인정보보호체계를 정비한 국가이며, 일본은 최근 개인정보 관련법을 제정하여 새로운 변화를 맞이하고 있다.

1. 일본

일본헌법 제21조는 표현의 자유와 통신비밀 보장에 관하여, 제35조는 주거 불가침 등을 규정하고 있어 간접적인 의미에서 프라이버시권을 보호하고 있다.[280] 그러나 헌법 제21조는 프라이버시의 측면에서 통신비밀의 보호라는 부분이 강조되고 있기는 하지만 전반적으로는 언론·출판 등 표현의 자유에 좀 더 비중이 있는 것으로 보인다.[281] 또한 제35조 역시

280) 제21조(집회·결사·표현의 자유와 통신비밀) : 「① 집회·결사 및 언론·출판 기타 모든 표현의 자유는 보장되어야 한다. ② 어떠한 검열도 행해져서는 안 되며 모든 통신비밀도 침해되어서는 안 된다」
제35조(주거불가침) : 「① 주거, 서류 및 소지품에 대한 침입 및 압수·수색을 받지 않을 권리는 제33조의 경우를 제외하고는 정당한 이유가 있는 경우에만 침해될 수 있을 뿐이고 수색장소 및 압수물건을 명시한 영장이 없는 한 침해되어서는 안 된다. ②각각의 수색 또는 압수는 권한 있는 사법 관헌이 발행한 별도의 영장에 의하여 행해져야 한다」

281) 실제로 표현의 자유는 일본 헌법상에서 다른 기본권보다 우월적 지위를 인정받고 있다고 한다. (한영학, "일본의 개인정보보호 법제", 세계언론법제동향, 2000. 12, 1면 참조)

소극적인 의미의 주거 불가침을 선언하고 이를 침해할 시에는 적정한 절차에 의하여야 한다는 원칙을 천명하는 수준이다. 따라서 적극적인 의미의 프라이버시권의 보장이나 또는 개인정보자기결정권에 대한 명시적인 헌법적 근거는 없는 것으로 보인다.

그러나 일본은 1970년대부터 개인정보보호를 위한 법체계를 도입하기 시작한 세계적인 흐름에 맞춰 공공부문을 중심으로 개인정보보호법 제정에 대한 논의를 본격적으로 시작하였고, 2003년에는 민간부문에 적용되는 개인정보보호법을 비롯하여 총 5개의 개인정보 관련 법령을 새롭게 정비하기에 이르렀다. 이렇듯 일본이 민간과 공공부문에서 '개인정보보호법'이라 불릴 만한 법제도를 정비한 것은 아주 최근의 일이다. 그 이전에는 미국과 유사한 개인정보보호 법제를 유지하고 있었기 때문에, 개인정보보호에 관한 기본법이라고 할 수 있는 법이 없었고 전문적인 개인정보보호기구도 없었다. 다만, 각 개별 법률을 관장하는 주무 행정부처가 부분적으로 개인정보보호의 역할을 담당하였을 뿐이다. 따라서 개인정보피해구제의 역할은 민간단체의 소송외적 분쟁해결제도나 법원의 소송에 의하는 것이 대부분이었다. 따라서 일본은 개인정보피해구제제도에 관해서 특별히 조사·분석할만한 제도적 특징이나 내용이 없다. 이하에서는 일본의 개인정보보호 관련 법제현황과 새롭게 제정된 개인정보보호법을 중심으로 변화된 개인정보보호제도를 간략히 소개하는 것으로 한다.

가. 개인정보보호 법제현황

일본은 1970년대 들어 전산화된 개인정보 처리가 활발히 진행되면서 공공부문을 중심으로 이러한 전산화된 방법을 통한 개인정보처리를 규율할 필요성이 제기되기 시작하였다. 이러한 움직임은 1975년 쿠니타치(國立)市가 최초로 개인정보보호조례를 제정하는 것으로 시작[282]되어, 1976년

282) 현재 일본에서는 지방자치단체가 보유하고 있는 개인정보의 처리는 대부분 해당 지방자치단체가 제정한 조례, 규칙 또는 규정에 의해 규율되고 있다. (김현수, "일본의 개인정보 관련 법제 동향과 법률 분석", IT법 연구회, 2003. 8, 1면)

공공부문의 컴퓨터로 처리되는 개인정보처리에 적용되는「전자계산기처리정보보호관리준칙」의 제정으로 이어졌다. 1970년대 중반을 전후로 하여 지방자치단체와 통상산업성(通商産業省) 및 기타 행정부처를 중심으로 시작된 정부 차원에서의 개인정보보호 문제에 대한 논의는 1980년대 들어 OECD 가이드라인의 영향으로 더욱 가속화되어, 1988년「행정기관이보유하는전자계산기처리에의한개인정보보호에관한법률(行政機關の保有する電子計算機處理に係る個人情報の保護に關する法律)」의 제정에 많은 영향을 끼쳤다. 동법은 행정기관이 보유하고 있는 개인정보를 컴퓨터 등 전자화된 방법에 의해 처리하는 경우 개인정보의 적정한 취급방법에 대해 규정하고 있다.

반면 민간분야에서는 개인정보보호법이라 불릴 만한 법규범은 없었다. 1988년 공공부문에 적용되는 개인정보보호법 제정 당시 민간부문의 개인정보도 포함할 것인지에 대한 논의가 있기는 하였으나, 행정부처간의 권한 분배 문제로 인한 갈등과 자유로운 기업 활동에 지장을 줄 우려가 있다는 주장으로 인하여 민간부문에 대한 개인정보 규정은 포함되지 못하였다.[283] 따라서 민간부문에서는 개인정보보호를 위해 적용할 수 있는 일반적인 법률은 없었으며, 대부분 정부의 지침이나 민간 자율단체의 가이드라인이 그 역할을 대신하여 왔다.[284] 따라서 일부 개별 법률에서 개인정보보호를 위한 관련 규정들[285]이 있어 개인정보침해에 대한 규제를

283) EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/japan.htm

284) 1989년 일본 통산성은 컴퓨터와 인터넷이 빠르게 보급에 따라 민간부문에서의 개인정보 침해가능성이 증가하자, 이에 대비하여「개인정보보호가이드라인」을 제정한 바 있다. 또한 1998년 10월에는「민간부문에서의전자계산기처리에관한개인정보보호가이드라인」을 제정하여 고시하였다. 한편 많은 사업자단체도 이러한 통산성의 가이드라인에 맞춰 업계의 자율적인 가이드라인을 마련하여 실행하였는데, 그 대표적인 예가 B2C 전자상거래 활성화를 위해 활동하고 있는 ECOM이 1998년 3월 마련한「민간부문의전자상거래에서의개인정보보호에관한ECOM가이드라인」이다. 동 가이드라인은 전자상거래 산업체가 준수하여야 할 적정한 개인정보취급관행을 규정하고 있다.

285) 전기통신분야의 통신비밀보호에 관한 규정으로 전기통신사업법 제4조제1항 및 제2항 등이 있으며, 개인신용분야에서는 「개인신용부정경쟁방지법」, 「할부판매법」, 「대금업의규제에관한법률」 등이 있다. 또한 의료분야에서는 「형법」 제134조의

가할 수 있었지만, 대부분의 경우 개인정보침해는 민법에 기초한 불법행위 책임의 문제로 다루어져 프라이버시 침해에 대한 손해배상청구만 가능하였을 뿐이다.

이렇듯 일본은 공공부문에 한정되어 적용되는 개인정보보호법만을 두고 있고 민간부문에 대해서는 특정 영역을 제외하고는 별도의 법적 규제를 가하지는 않았다. 그러나 1990년대 후반 들어 인터넷의 보급과 이용 증대로 인한 개인정보침해의 증가는 일본 정부로 하여금 업계의 자율적인 노력만으로 민간 부문에서 충분한 개인정보보호 체계를 확보하는 것은 한계가 있다는 판단을 하도록 하였다. 실제로 일본은 침체되어 있는 일본경제를 되살릴 수 있는 전략의 한 방안으로 전자상거래를 비롯한 정보통신기반산업의 육성을 정책으로 삼고 1994년 8월 내각에 총리대신을 본부장으로 하는 '고도정보통신사회추진전략본부(IT 전략본부)'를 설치하는 등 많은 노력을 기울인 결과, 정보화가 빠르게 진행되었다. 그러나 이러한 정보화의 급격한 진행은 공공부문은 물론이고 민간부문에서도 개인정보침해가 심각한 문제로 야기되는 결과를 초래하였다.[286] 이에 일본 정부는 2000년 '개인정보보호법제화전문위원회(個人情報保護法制化専門委員會)'를 설치[287]하여 새로운 개인정보보호법제 마련을 위한 검토 작업에 착수하게 되었고, 같은 해 10월 「개인정보보호기본법제에관한대강(個人情報保護基本法制に關する大綱)」을 마련하였다. 일본 정부는 이를 바탕으로 2001년 3월 국회에 「개인정보보호에관한법률(안)」을 제출하였

비밀누설금지의무 규정, 「의료방사선기사법」 제29조의 비밀준수의무 규정, 「의료법」 제21조 등이 있다. (ECOM, "ECで取"り扱われる個人情報に關する調査報告書(v. 3.0)", 2001. 3, p. 37~58 참조)

286) 최근 일본 내각부가 실행한 설문조사에 의하면, 일본 국민의 69%는 행정기관과 민간영역의 사업자가 관리하는 개인정보가 '본인 승낙없이 외부에 유출되고 있다고 느낀다'고 답하였고, 78.4%는 '프라이버시 침해가 증가한 것 같다'고 응답하였다. 이러한 결과를 통해서도 일본에서 개인정보침해 문제가 어느 정도로 심각하게 인식되고 있는지 알 수 있다. (디지털타임즈, "개인정보유출 불안 느낀다, 69%", 2003. 12. 9일자 기사 참조)

287) 개인정보보호법제화전문위원회의 전신은 1999년 7월 업계, 학계, 소비자단체, 재야법조인 등 14인의 위원으로 구성·설치된 '개인정보보호검토부회'이다. 검토부회는 1999년 11월 개인정보보호와 이용에 관한 바람직한 방안을 검토하여 중간보고를 공표한 바 있다. (한영학, 앞의 글, 11면 참조)

으나 2년이 넘게 논의를 거듭하다 결국 언론과 시민단체의 강력한 반대에 부딪쳐 2002년 12월 폐기되었다. 동 법안은 ① 이용목적에 의한 제한, ② 적정한 방법에 의한 취득, ③ 내용의 정확성 확보, ④ 안전보호조치의 실시, ⑤ 투명성의 확보라는 개인정보보호 기본 5원칙을 제시하였는데, 언론단체 및 야권과 시민단체는 동 원칙의 내용이 지나치게 포괄적이어서 헌법상 보장되는 언론의 취재보도의 자유를 침해할 가능성이 높다고 하여 반대의사를 밝혔었다. 이에 일본 정부는 당초의 입장에서 다소 후퇴하여 가장 논란이 되었던 다섯 가지 기본원칙을 삭제하고 적용범위를 다소 변경한 새로운 법률을 마련하여 의회에 제출하였다.[288] 이 법안은 2003년 5월 23일 참의원을 통과한 뒤 법률로 성립되어 5월 30일 공포되었다.[289]

이 때 새롭게 정비된 법률로는 ① 개인정보보호에관한법률(個人情報の保護に關する法律)(이하 '개인정보보호법'이라 한다), ② 행정기관이보유하는개인정보보호에관한법률(行政機關の保有する個人情報の保護に關する法律)(이하 '행정기관개인정보보호법'이라 한다), ③ 독립행정법인등이보유하는개인정보보호에관한법률(獨立行政法人等の保有する個人情報の保護に關する法律)(이하 '독립행정법인개인정보보호법'이라 한다), ④ 정보공개・개인정보보호심사회설치법(情報公開・個人情報保護審査會設置法)(이하 '심사회설치법'이라 한다), ⑤ 행정기관이보유하는개인정보보호에관한법률등의시행에따른관계법률의정비등에관한법률(行政機關の保有する個人

288) 새롭게 제출된 법안은 기존 법안과는 달리 ① 개인정보보호 기본 5원칙을 삭제하였고, ② 법적용 제외대상으로 보도기관, 학술연구기관, 종교단체, 정치단체 외 '저술업을 행하는 자'를 추가하였으며, ③ 적용제외대상 기관에 대해서는 개인정보보호주무장관이 권한을 행사하지 않는다는 것을 명문화하였다. 즉, 새 법안은 기존 법안에 대한 비판을 반영하여 개인의 표현의 자유와 언론보도의 자유를 최대한 보장하고 이에 대한 정부의 간섭을 최소화하고 있다.

289) 일본 야당 4당은 정부가 제출한 개인정보보호법안에 반대하여, 주무장관의 권한을 배제하고 내각 총리대신 관할의 '개인정보보호위원회'를 설치하는 내용을 담은 별도의 법안을 제출하였으나 부결되었다. 이렇듯 수정된 법안에 대해서도 야당을 비롯한 시민단체 등으로부터 반발이 있는 등 논란이 극심하자, 동 법안 통과시 의회는 법률 시행 3년 후 법개정 검토, 별도의 개인정보보호기구 설치, 가이드라인 작성 등 17개 항목의 부대 결의를 함께 채택하였다.

情報の保護に[redacted]する法律等の施行に伴う[redacted]係法律の整備等に[redacted]する法律)(이하 '관계법률정비법'이라 한다)이 있다.

［표 4-41］일본 개인정보관련 입법현황

법률명	적용범위	주요내용
개인정보보호법	민간부문 공공부문	· 개인정보의 적정한 취급에 관한 기본원칙 규정 · 국가, 지방자치단체의 책무 규정 · 민간 개인정보취급사업자의 의무 규정 · 사업자 및 인정개인정보보호단체에 의한 자율적인 피해구제제도 규정
행정기관 개인정보보호법	공공부문	· 일반 행정기관이 보유하는 행정문서에 기록된 개인정보의 적정한 취급 원칙 · 이용목적 달성에 필요한 범위내에서 개인정보 보유 · 개인정보 목적외 이용 및 제공 금지 · 정보주체의 열람, 정정, 이용정지청구권 인정
독립행정법인 개인정보보호법	공공부문	· 독립행정법인, 행정목적 수행을 위한 특수법인, 인가법인은 대상개인정보, 개인정보 취급규모, 관리규칙, 정보주체의 권리, 피해구제제도 등에 있어서 일반 행정기관과 동일하게 취급
심사회설치법	공공부문	· 정보공개심사회의 설립에 관한 규정 · 개인정보의 열람, 정정, 이용정지신청에 대한 행정기관 등의 결정에 대한 불복신청과 관련하여 자문을 행함
관계법률정비법	공공부문	· 등기, 형사소송, 특허 등과 관련된 정보에는 행정기관개인정보보호법 등 적용제외

이 중 개인정보보호법은 제4장 '개인정보취급사업자의 의무 등(個人情報取扱事業者の義務等)'에 관한 규정을 제외하고는 민간과 공공부문에서의 개인정보처리를 공히 아우르는 기본이념과 국가 및 지방자치단체의 개인정보보호를 위한 책무, 기본방침의 책정 등 개인정보보호 기본법적 사항을 규정하고 있다. 아래에서는 이러한 개인정보보호법의 주요내용을 간략하게 살펴보도록 하겠다.

나. 개인정보보호법의 주요내용

(1) 기본이념 및 국가 등의 책무

새롭게 제정된 일본의 개인정보보호법은 제3조에서 “개인정보는 개인의 인격존중의 이념 아래 신중하게 취급되어야 함에 따라 그 적정한 취급이 도모되어야 한다”라고 하여 민간부문과 공공부문을 총괄하는 개인정보 처리의 기본이념을 밝히고 있다는 점에서 무엇보다 중요한 의미를 가진다. 물론 2001년 국회에 제출한 법안에서는 구체적으로 다섯 가지의 개인정보보호 기본원칙을 규정하고 있었던 것과 비교할 때, 동법 제3조의 기본이념 규정은 다소 형식적인 ‘선언’에 그칠 수도 있지만, 개인정보의 ‘적정한 취급’이라는 기본이념이 모든 개인정보처리의 기준이 될 수 있다는 점에서 가치를 가진다 할 것이다.

한편 동법 제2장과 제3장은 기본이념인 개인정보의 적정한 취급을 확보하기 위해 국가와 지방자치단체에게 일정한 책무가 있음을 규정하고 있다. 즉, 국가 및 지방자치단체는 ① 개인정보의 적정한 취급을 위해 필요한 시책을 책정하고 실시하여야 하고, ② 행정기관이나 독립행정법인 등이 보유하고 있는 개인정보가 그 성질이나 보유목적, 업무내용 등 특성에 따라 적정히 취급될 수 있도록 법제상의 조치를 포함한 모든 필요조치를 취하여야 하며, ③ 시책의 강구 및 실행에 있어 상호 협력하여야 한다. 또한, ④ 정부는 개인정보보호를 위한 기본방침을 제정하여야 하고, ⑤ 지방공공단체의 시책을 지원하기 위해 필요한 정보를 제공하고 지침을 마련하여 고시하여야 하며, ⑥ 사업자와 개인과의 사이에서 개인정보 취급과 관련한 문제가 발생하였을 경우 이를 적절하고 신속하게 해결해 줄 수 있는 고충처리조치를 마련하여야 한다. 지방자치단체 역시 ⑦ 개인정보의 적정한 취급을 위해 구역 내 사업자와 주민을 지원할 수 있는 모든 필요한 조치를 취하여야 하고, ⑧ 사업자와 개인간에 발생하는 고충의 신속하고 적절한 처리를 위해 고충처리를 알선하는 등의 조치를 취하여야 한다.

(2) 개인정보취급사업자의 의무

개인정보보호법의 적용을 받는 개인정보취급사업자는 개인정보데이터베이스 등을 사업에 이용하고 있는 자이다. 다만, 국가기관·지방공공단체 등의 공공기관과 취급하는 개인정보의 양 및 이용방법으로 보아 개인의 권리이익을 해할 우려가 적은 자로 정령에서 정한 자는 제외된다.[290] 동법 제4장제1절은 개인정보취급사업자가 개인정보데이터베이스 등을 통해 개인정보를 전자적으로 처리할 경우, 다음과 같은 개인정보취급 의무가 있음을 밝히고 있다.

〔표 4-42〕 일본 개인정보보호법상 개인정보취급사업자의 의무

구 분	내 용
이용목적에 따른 제한	개인정보의 이용목적 특정 및 특정된 목적의 달성에 필요한 범위를 초과하여 개인정보를 취급하는 것을 원칙적으로 금지
개인정보 수집제한	부정한 수단을 통한 개인정보 취득금지 및 개인정보 취득시 반드시 수집 및 이용목적을 고지·공표 또는 명시
개인정보의 정확성 확보	이용목적의 달성에 필요한 범위 내에서 개인정보의 정확성과 최신성을 확보
개인정보의 안전한 관리	개인정보의 안전한 관리를 위해 필요한 안전조치 확보 및 직접 개인정보를 취급하는 직원과 개인정보위탁업체를 적절히 관리
개인정보 제3자 제공 제한	원칙적으로 본인의 명시적인 동의없이 개인정보를 제3자에게 제공하는 것 금지
정보주체의 접근권 보장	보유하고 있는 개인정보에 대한 접근절차 등을 고시하고 본인의 열람·정정·이용정지 요구를 보장
고충의 적절한 처리	개인정보 취급에 관한 소비자의 고충을 적절하고 신속하게 처리하기 위해 노력하여야 할 의무

이 외에 동법은 개인정보보호를 위한 주무대신의 역할과 민간개인정보보호인정단체에 대하여 규정하고 있는데, 이는 다음의 개인정보보호기구 및 피해구제절차를 살펴보면서 함께 보도록 한다.

290) 일본 개인정보보호법 제2조.

다. 개인정보보호기구 및 피해구제제도

올해 제정된 일본의 개인정보보호법, 행정기관개인정보보호법 등은 개인정보보호를 위한 특별 전담기구의 설치에 대하여 별도의 규정을 두고 있지 않다. 따라서 일본에서는 지금까지 개인정보보호기구라고 부를 만한 전문적인 기구가 없었기 때문에 개인정보보호기구를 통한 피해구제의 역할도 소극적일 수밖에 없었다. 즉, 정부 차원에서는 개별 영역을 담당하는 소관 주무부처가 개인정보보호의 역할을 부수적으로 수행하여 왔을 뿐 당사자간 분쟁해결 등을 통한 피해구제의 역할은 담당하지 않았다. 따라서 개인정보피해는 순수하게 법원 또는 사업자의 자율적인 소비자 불만해소 절차를 통하여 이루어지는 것이 대부분이었다. 그러나 새로 제정된 개인정보보호법은 국가, 지방자치단체, 사업자에게 각각 정보주체의 불만해소를 위한 고충처리제도를 마련토록 규정[291]함으로써, 신속하고 적절한 개인정보피해구제를 강조하고 있다. 이하에서는 이를 바탕으로 일본의 개인정보보호 및 피해구제제도를 정부차원과 민간차원으로 구분하여 살펴보도록 하겠다.

(1) 정부차원의 개인정보피해구제

정부차원에서는 각 개별법률 또는 해당 영역을 관장하는 소관 주무부처가 개인정보보호의 역할을 맡고 있다. 개인정보보호법도 주무대신[292]

291) 개인정보보호법 제9조는 "국가는 개인정보의 취급과 관련하여 사업자와 본인 간에 발생하는 고충의 적절하고 신속한 처리를 도모하기 위하여 필요한 조치를 강구하여야 한다"고 규정하고 있으며, 동법 제13조는 "지방공공단체는 개인정보의 취급과 관련하여 사업자와 본인 간에 발생하는 고충이 적절하고 신속하게 처리될 수 있도록 하기 위해 고충처리의 알선 기타 필요한 조치를 강구하도록 노력하여야 한다"고 하고 있다. 또한, 동법 제31조에서 "①개인정보취급사업자는 개인정보의 취급에 관한 고충의 적절하고 신속한 처리를 위해 노력하여야 한다. ② 개인정보취급사업자는 전항의 목적을 달성하기 위하여 필요한 체제의 정비에 노력하여야 한다"고 하여 사업자의 피해구제를 위한 노력의무를 규정하고 있다.

292) 여기서 주무대신은 개인정보취급사업자가 행하는 개인정보 취급 중 근로정보에 대한 사항을 제외한 나머지 부문에 대해서는 당해 사업자가 행하는 사업을 소관하는

에게 이러한 의미에서 개인정보보호를 위한 권한을 부여하고 있다. 개인정보보호법 제32조～제34조에서 규정하고 있는 주무대신의 권한을 살펴보면, ① 개인정보취급사업자 및 인정개인정보보호단체로부터 필요한 경우 개인정보 취급 등에 대한 보고를 받을 수 있으며, ② 사업자에게 필요한 사항을 조언할 수 있고, ③ 개인정보취급사업자가 의무규정을 위반하였을 경우 그러한 행위의 중지 또는 시정의 권고를 할 수 있다. 또한, ④ 사업자가 정당한 이유 없이 권고를 무시하여 개인의 중대한 권리·이익이 침해될 위험이 있을 경우에는 권고 이행명령을 내릴 수 있으며, 긴급한 조치가 필요하다고 인정될 때에는 사업자에게 의무위반행위의 중지명령 및 시정명령을 내릴 수 있다.

(2) 민간차원의 개인정보피해구제

일본은 민간영역의 경우 특히 사업자들의 자율적인 처리관행의 확립 및 당사자의 자율적인 분쟁해결을 기본으로 피해구제제도를 운영하여 왔다. 이러한 자율규제 차원에서 운영되고 있는 것이 신뢰마크 제도이다. 이에는 통산성 산하 일본정보처리개발센터(JIPDEC: Japan Information Processing Development Center)[293]가 운영하는 것과 우정성 산하 일본데이터통신협회가 운영하는 제도[294]가 있는데, 여기서는 JIPDEC가 운영하는 '프라이버시마크제도'를 간략히 살펴보도록 하겠다. 이 제도는 통산성의 가이드라인에 적합하게 개인정보를 처리하겠다고 약속한 사업자에게 특정한 기준에 따라 심사를 거친 뒤 프라이버시 마크를 부여하고 사후적으로 운영·감독하는 것이다. 프라이버시 마크제도는 기본적으로 사

대신을 의미한다. (일본 개인정보보호법 제36조제1항)

293) JIPDEC는 통산성 산하에 설립된 공공기관으로서, 전자상거래 활성화 차원에서 개인정보보호 가이드라인을 설정하고 인터넷에서의 개인정보보호 관련 연구를 수행하는 기관으로 프라이버시마크제도의 운영도 책임지고 있다.

294) 우정성 산하 일본데이터통신협회에서는 개인정보보호등록센터를 개설하여 1998년부터 개인정보보호마크제도를 시행하고 있다.(강신원, "B2C 활성화를 위한 개인정보보호제도와 정책방향", 개인정보연구 제2권 제1호, 2003. 7, 194면)

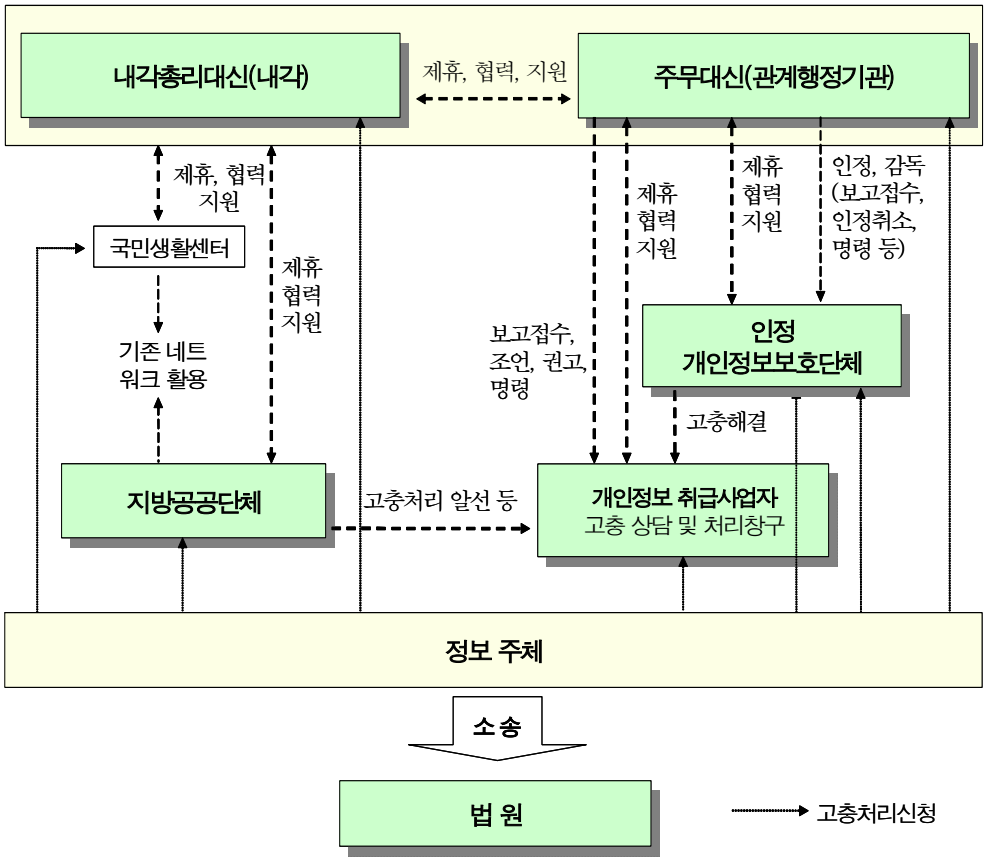
업자가 자율적으로 개인정보보호를 위해 노력하겠다는 의미를 담고 있는 것으로 강제적인 성격을 가지지는 않는다. 다만, JIPDEC는 통산성 산하 공공기관이라는 점으로 인하여 프라이버시 마크 프로그램에 참여한 사업자가 위법행위를 하였는지 여부를 조사하여 필요한 조언이나 제안을 하는 등 사후관리를 통해 이러한 자율규제 시스템을 촉진하고 보완하는 역할을 하고 있다. 현재 이러한 프라이버시 마크 프로그램에 참여한 기업체의 수는 꾸준히 증가하여 2003년 5월 499개 회사가 JIPDEC로부터 마크를 부여받았다.[295]

그러나 신뢰마크제도는 개인정보침해예방을 위한 사전적인 장치로서 작동될 뿐이고 미국의 BBBOnLine과 같이 신뢰마크 프로그램을 기초로 한 분쟁해결제도를 갖추고 있지는 않다. 이런 의미에서 새롭게 제정된 개인정보보호법은 '인정개인정보보호단체'라는 제도의 도입을 통해 민간 차원에서의 개인정보피해구제 및 고충처리의 역할을 보강하고 있다. 특히, 인정개인정보보호단체 제도는 주무대신이 민간 개인정보보호단체에 대하여 정부가 적절한 역할을 담당하는 개인정보보호기구임을 '인정'해 줌으로써, 민간 자율규제와 정부의 적절한 감독을 함께 조화시킬 수 있다는 점에서 의미를 가진다. 인정개인정보보호단체는 주로 개인정보취급사업자의 개인정보의 적정한 취급을 지원하고 확보할 목적으로 활동하는 단체로서, 사업자에게 필요한 정보를 제공하거나 사업자의 개인정보 취급관행으로 인해 피해를 입은 소비자의 문제제기를 원만히 해결하고 피해구제를 받을 수 있도록 도와주는 역할을 담당하는 기구를 의미한다. 주무대신으로부터 인정개인정보보호단체로 인정되면 개인정보보호지침을 작성하여 공표할 수 있는데, 이 경우 단체의 구성원인 대상사업자가 동 지침을 적절히 준수하도록 지도하고 조언하며 시정권고 기타 필요한 조치를 취하여야 한다.[296] 특히 인정개인정보보호단체는 사업자와 정보주

295) 한편, JIPDEC는 2000년 5월 미국의 BBBOnLine과 상호 프라이버시마크를 인정해주는 제휴를 맺어 2001년 6월부터 '온라인 상호인정 프라이버시마크 프로그램'을 시행하고 있다. (EPIC & PI, supra note 138, http://www.privacyinternational.org/survey/phr2003/countries/japan.htm)

296) 일본 개인정보보호법 제43조.

체 간의 개인정보침해로 인한 분쟁의 해결이나 고충처리를 위해 소비자의 민원신청을 접수하여 상담에 응하고 당사자에게 필요한 조언을 행하여야 한다. 또한 사건과 관련하여 문서나 구두로 설명을 요구하거나 자료제출을 요구함으로써 사실조사를 실시하고 사업자에게 민원내용을 통지하고 신속한 해결을 요구하여야 한다. 사업자 역시 인정개인정보보호단체의 이러한 요구를 정당한 이유 없이 거절하여서는 안 된다.[297]



(그림 4-17) 일본의 개인정보피해구제 절차도

※ 참고 : http://kantei.go.jp/jp/it/privacy/houseika/hourituan/ronten.html

297) 일본 개인정보보호법 제42조.

2. 홍콩

홍콩은 영국의 영향을 많이 받은 역사적 특수성으로 인하여, 아시아권에서는 비교적 빨리 개인정보보호를 위한 법제를 도입·운영하고 있다. 홍콩에서 개인정보보호를 위한 법제도의 도입에 대한 논의가 본격적으로 시작된 것은 1994년 법률개혁위원회(LRC : Law Reform Commission) 산하 프라이버시 소위원회가 정보보호를 위한 법제 도입에 관한 보고서를 제출하면서부터이다. 법률개혁위원회는 동 보고서에서 다른 국가의 프라이버시보호제도를 조사·분석한 내용을 바탕으로 각국이 개인정보보호를 위해 취하는 접근방법을 크게 다음 세 가지로 구분하였는데, ① 개인정보 관련 법률을 제정하고 전담규제기구를 설치하는 방안, ② 프라이버시 침해에 대한 불법행위를 인정하여 민사소송을 허용하는 방안, ③ 자발적인 실행규약이나 자율적인 시장감시 등 자율규제를 촉진하는 방안이 그것이다. 법률개혁위원회는 이러한 세 가지 방안 중 명확한 개인정보관련 제정법의 마련을 통한 법적 규율체계를 구비하고 이를 시행할 규제기구를 설치하는 접근방법을 채택하는 것이 홍콩의 이익에 가장 부합한다고 결론지었다.[298]

홍콩은 법률개혁위원회의 최종 보고서에 따라, 1995년 8월 3일 「개인정보법(Personal Data Ordinance)」을 제정하였으며, 동법에 근거하여 개인정보보호를 위한 프라이버시 감독기구로서 '개인정보(프라이버시)커미셔너(PCO : Privacy Commissioner for Personal Data)'를 설치하여 개인정보보호를 위한 제도를 정비하였다. 특히 홍콩은 개인정보보호법과 개인정보호호기구를 도입함에 있어 영국은 물론 호주나 뉴질랜드, 캐나다의 모델을 많이 참조하여 체계를 갖춘 것으로 보인다. 따라서 대체적으로 이들 국가들의 개인정보보호체계와 유사한 점이 많다.

---

298) Raymond Tang, *"Remedies for Personal Data Infringements under the Personal Data(Privacy) Ordinance"*, International Conference on Personal Data Protection 2002 in Seoul, 2002. 11. 28. p. 1

가. 개인정보보호법의 주요내용

1995년 제정된 개인정보법은 1996년 12월 20일 발효되어 시행되고 있다. 동법은 생존하고 있는 개인과 직·간접적으로 관련있는 모든 개인정보에 적용되며, 개인정보를 수집·보유·처리·이용하는 모든 자에게 적용된다. 따라서 기업, 비영리단체, 행정부처, 기타 공공기관 등 모든 정보이용자의 개인정보 처리행위를 규율하고 있다. 또한 동법 부칙은 국제적 표준에 맞춘 6가지의 기본적인 정보보호원칙(DPP : Data Protection Principles)을 규정하고 있는데, 동 원칙은 개인정보의 수집방법과 목적, 보유한 정보의 정확성 확보 및 보유기간, 개인정보의 이용 및 보호를 위한 안전조치 확보, 일반적으로 이용가능한 정보, 개인정보 접근에 관한 내용을 포함하고 있다.

［표 4-43］홍콩의 정보보호원칙

구 분	내 용
개인정보의 수집	· 불공정하고 불법적인 방법에 의한 개인정보 수집금지 · 개인정보의 수집목적 고지
개인정보의 보유	· 보유하고 있는 개인정보의 정확성, 최신성, 완전성 확보 · 목적달성 이후 개인정보 파기
개인정보의 이용	· 수집시 예정된 목적외 사용금지 · 명시된 목적과 직접적 관련이 있는 목적 외 사용금지
개인정보의 안전	· 개인정보의 손실 등으로부터의 안전조치 확보
일반적으로 제공되어야 할 정보	· 정보이용자의 개인정보보호방침에 대한 고지 · 정보이용자가 보유하는 개인정보를 정보주체에게 고지 · 정보이용자의 개인정보 이용목적을 정보주체에게 고지
개인정보 접근	· 정보주체의 개인정보 열람·정정권 보장

이러한 정보보호원칙을 비롯하여 정보주체는 개인정보법에 의해 많은 권리를 향유하고 있다. 즉, 정보주체는 ① 개인정보가 공정한 방법에 의해 수집될 권리, ② 이용목적에 대하여 고지받을 권리, ③ 오직 필요한 정보만을 제공할 권리, ④ 이용목적 변경 등에 대하여 기존의 동의를 보

류할 권리, ⑤ 정확하고 안전하게 개인정보가 보유되고 관리될 권리, ⑥ 개인정보 열람권, ⑦ 개인정보 정정권, ⑧ 공개요구권 등의 권리를 보장받고 있다. 이 외에도 동법은 개인정보보호기구인 홍콩의 개인정보커미셔너의 설립, 권한, 기능에 대한 규정과 정보조합프로그램의 사용규제, 실행규약의 제정 및 고시, 정보이용자의 등록 및 그 관리 등에 관한 규정을 함께 포함하고 있다.

나. 개인정보보호기구

(1) 개인정보커미셔너의 설립 및 지위

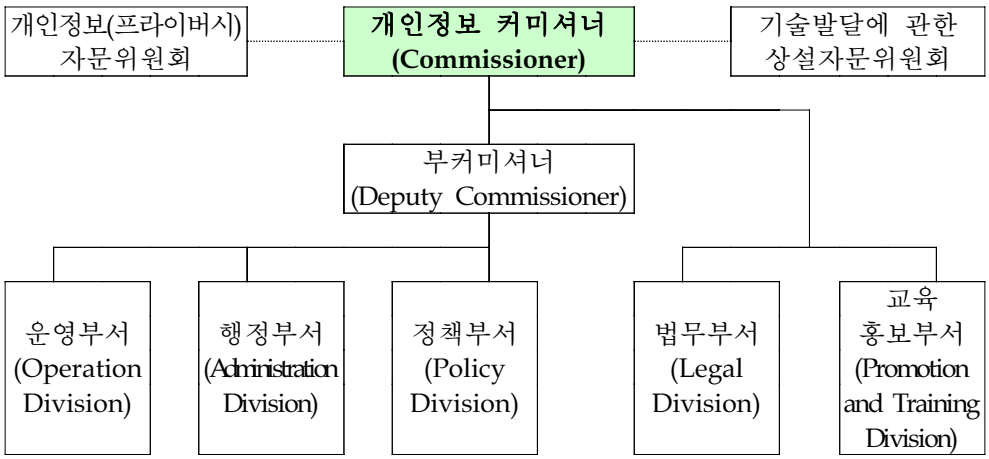
홍콩의 개인정보커미셔너는 정보처리자의 개인정보법 이행을 확보하고 개인의 정보프라이버시를 보호하는 임무의 실현을 위해, 1996년 8월 1일 설립된 독립법정기구이다. 개인정보커미셔너는 홍콩 행정특별구역 장관(Governor)에 의해 직접 임명되며, 임기는 5년이나 1회에 한해 재임할 수 있다. 또한 커미셔너는 법률에 의해 설립된 독립기구로서 예산지원은 재무부에서 받으나, 인사권 행사나 각종 활동을 독자적으로 수행한다.

앞서 말한 바와 같이 개인정보커미셔너는 홍콩의 개인정보법을 집행하는 역할을 맡고 있다. 동법은 민간과 공공부문에 모두 적용되는 개인정보보호기본법이기 때문에, 커미셔너는 홍콩 내에서 이루어지는 모든 개인정보의 처리행위, 즉 민간부문과 공공부문 모두에서의 개인정보 수집・이용・제공・저장 등에 대해서 조사하고 감독한다. 또한 커미셔너는 각 분야별로도 특별한 관심을 보이고 있다. 따라서 의료정보, CCTV를 통한 프라이버시 침해, 신용정보보호, 정보통신분야에서의 개인정보보호, 근로자정보의 보호, 다이렉트 마케팅과 개인정보보호 등에 관하여 각종 지침이나 프라이버시규약을 제정・고시하는 등 프라이버시와 관련된 모든 분야를 다루고 있다.

(2) 개인정보커미셔너의 조직구성

홍콩 PCO는 개인정보 커미셔너 1인과 부커미셔너 1인을 비롯하여 약 34명의 직원으로 구성되어 있으며, 커미셔너에게 중대한 사안에 대한 자문을 해주는 역할을 하는 두 개의 자문위원회가 설치되어 있다.

홍콩 PCO 사무국은 운영부서, 행정부서, 정책부서, 법무부서, 교육홍보부서의 총 5개 부서로 이루어져 있다. 운영부서는 개인정보법에 관한 질의접수 및 응답, 각종 민원접수 및 처리, 법규위반 조사, 정보조합프로그램의 사용신청서 접수 및 처리 등의 업무를 하며, 행정부서는 인사·회계·개인정보자문위원회 지원 등의 업무를 한다. 또한 정책부서는 개인정보 관련 이슈분석 및 실행규약의 제정 작업을 지원하며, 법무부서는 각종 법률자문 및 입법심사 지원업무를 담당한다. 끝으로 교육홍보부서는 교육프로그램의 개발 및 실시, 각종 세미나·발표회 행사 추진, 언론보도자료 및 발간물 작성·배포 등의 역할을 하고 있다.



(그림 4-18) 홍콩 PCO의 조직도

또한 홍콩 PCO는 두 개의 자문위원회를 활용하고 있다. '개인정보자문위원회(Personal Data Advisory Committee)'와 '기술발달에 관한 상설자문위원회(The Standing Committee on Technological Developments)'가 그

것이다. 전자는 홍콩의 개인정보보호법 제11조제(1)항에 의거하여 설립된 것으로 개인정보보호규약 또는 지침 제정 등 개인정보와 관련된 각종 프라이버시 문제에 대해 커미셔너에게 자문을 행할 수 있다. 개인정보자문위원회는 1996년 설치되었으며, 현재 자문위원회의 위원장을 역임하고 있는 커미셔너를 포함 총 9인의 위원으로 구성되어 있다. 개인정보법 제11조제(2)항에 의하면, 위원 중에서 1인은 반드시 정보처리 경력이 5년 이상인 자가 임명되어야 하고 1인은 공무원으로 임명되어야 한다. 또한 커미셔너를 제외한 자문위원회의 위원은 내무부(Secretary for Home Affairs)에 의해 임명된다. 한편 커미셔너는 개인정보법 제8조제(1)항제(f)호에 의해 각종 정보처리기술 및 컴퓨터 기술의 발달이 개인정보와 프라이버시에 미치는 영향을 조사하고 연구할 책임이 있는 바, 후자는 커미셔너가 이러한 기능을 수행하기 위해 설립한 상설자문위원회이다. 동 자문위원회는 1996년 설치되었으며, 현재 위원은 총 7인이고 위원장은 부커미셔너가 맡고 있다.

(3) 개인정보커미셔너의 주요기능

커미셔너의 주된 임무는 효율적이고 효과적인 방법을 통해 홍콩 개인정보법의 준수여부를 조사·감독하고 법규에 적합하게 개인정보를 취급하는 관행을 장려함으로써, 개인정보를 보호하고 개인의 프라이버시를 지키는 것이다. 이러한 임무를 수행하기 위한 홍콩 개인정보 커미셔너의 주된 기능을 살펴보면, ① 의견제시 및 분쟁조정을 통한 개인정보 피해구제, ② 정보보호원칙 등 법규준수여부 및 침해행위에 대한 개인정보보호 실태조사 및 감독·규제, ③ 실행규약 제정 등을 통한 자율규제활동의 지원, ④ 각종 법령질의 처리 및 정보제공, ⑤ 정책자문 및 입법안 검토 및 심의, ⑥ 개인정보관련 조사·연구, ⑦ 개인정보보호를 위한 교육 및 홍보, ⑧ 국내외 유관기관 협력이 있다. 세부적인 내용을 살펴보면 다음과 같다.

［표 4-44］ 홍콩 PCO의 주요기능

주요기능	세부내용
피해구제	· 각종 불만사항이나 개인정보침해신고 접수 · 민원내용에 대한 사실조사 및 법규위반여부 심사 · 민원심사를 통한 예비의견 통보 및 개인정보 분쟁조정 · 법규위반사항에 대해 행정명령 및 경고 · 정보주체의 개인정보 접근권 행사 지원 및 보호
조사·감독	· 프라이버시 침해여부에 대한 직권 실태조사 및 모니터링 · 정보보호원칙 및 법규 준수여부 감독 · 정부기관이나 기업체의 정보처리시스템 조사 · 정부의 데이터 매칭 프로그램 사용에 대한 승인 · 개인정보침해행위 및 법위반사항에 대하여 이행명령(고지) 부과 · 이행명령 불이행시 및 법규위반 확인시 검찰 등 해당기관 이첩
프라이버시 규약	· 각종 개인정보보호 실행규약(Code of practice)의 제정 및 고시
정보제공	· 개인과 사업자, 정부, 공공기관에 대하여 각각 정보제공 및 자문 · 법령관련 질의접수 및 처리
정책 및 입법자문	· 개인정보 관련 법안 심의 및 의견제시 · 정부의 각종 정책에 대하여 의견제시 및 자문
개인정보보호연구	· 개인정보 관련 기술동향 조사 및 연구
교육홍보	· 각종 단체에 대한 개인정보보호교육 실시 · 세미나, 발표회 등 개인정보보호 행사 실시 · 개인정보보호 공공캠페인 실시 · 개인정보(프라이버시) 설문수행 · 언론 등에 대한 프라이버시커미셔너 활동 등 홍보
유관기관 협력	· 국내 개인정보(프라이버시) 관련 유관기관 및 시민단체와의 협력 · 해외 개인정보보호기구와의 국제협력

다. 개인정보피해구제 절차 및 방법

홍콩 개인정보법에 의하면, 개인정보 침해로 인하여 피해를 입은 자는 민사소송이나 형사고소에 앞서 개인정보커미셔너에게 피해구제를 요청할 수 있다. 앞서 살펴본 바와 같이 홍콩 개인정보커미셔너는 개인정보법의 준수여부에 대하여 감시하고 정보처리자가 법규를 준수토록 하기 위해 법에 의해 설립된 독립기구이다. 따라서 커미셔너는 정보처리자의 법규

준수를 담보하고 개인정보를 보호하고 소중히 관리하는 관행을 촉진시키기 위해, 개인정보 또는 프라이버시와 관련된 민원을 접수받아 분쟁조정, 법위반행위 조사, 위법사실 통보 등의 방법을 통해 개인정보 침해로 인해 야기되는 각종 피해를 구제하는 일에 앞장서고 있다.[299] 홍콩 PCO가 2003년 9월까지 처리한 개인정보 상담 및 피해구제 건수는 아래와 같다.

〔표 4-45〕 홍콩 PCO의 피해구제현황

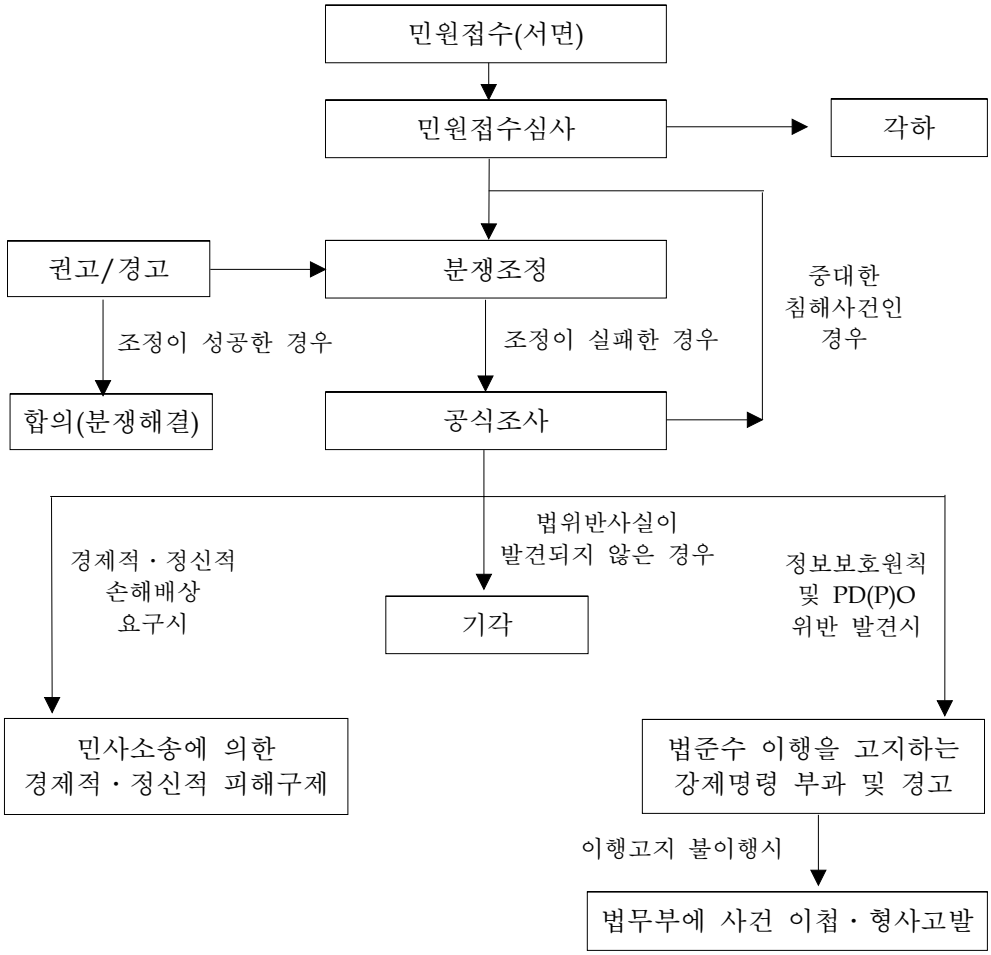
구분	1996	1997	1998	1999	2000	2001	2002	2003/9
상담	227	9,356	22,861	15,243	19,331	21,916	17,114	11,679
피해구제	10	227	392	541	692	921	843	745
계	237	9,583	23,253	15,784	20,023	22,837	17,957	12,424

※ 주 : http://www.pco.org.hk/english/enquiries/statistics.html 참고.

이와 같이 커미셔너는 독립행정기관으로서 개인정보피해구제의 기능을 적극적으로 수행해오고 있다. 커미셔너는 이러한 피해구제기능의 수행을 위해 ① 법규 위반여부에 대한 조사할 수 있는 권한, ② 피해자와 정보처리자 간의 분쟁을 조정할 수 있는 권한, ③ 필요시 강제명령을 통해 법위반사항을 중지하고 법규를 준수하도록 강제할 수 있는 권한을 부여받고 있다. 그러나 커미셔너는 민사적 배상결정의 권한이나 형사범죄에 대한 수사권 및 기소권은 없다. 따라서 피해자가 개인정보법 위반으로 인하여 입은 경제적·정신적 피해에 대한 손해배상을 요구하는 경우, 커미셔너는 당사자에게 민사소송을 통해 피해배상을 받도록 권고하고 있다. 즉, 커미셔너는 현재의 법위반행위를 중지하거나 피해자에게 사과를 하도록 조정하는 방식으로 위법행위로 인해 입은 피해를 구제해줄 뿐, 손해배상을 통한 피해구제 방식은 법원의 몫이다. 또한 커미셔너는 개인정보 침해행위가 심각한 형사범죄를 구성하게 되는 경우, 해당 사건을 형사기관

299) 홍콩 PCO는 개인정보 관련 민원이 개인정보법 제39조제(2)항에 해당되는 경우를 제외하고는, 동법 제37조에 따라 개인정보 관련 이의제기를 접수받아 처리할 권한과 책임이 있다.

에 이첩하여 수사토록 할 수 있으나 직접 수사하거나 형사기소할 수 있는 권한은 없다. 홍콩의 개인정보커미셔너는 이러한 권한을 바탕으로 각종 개인정보 침해사건을 접수받아 처리하고 있는데, 이러한 홍콩 개인정보커미셔너의 피해구제 절차 및 방법을 살펴보면 아래와 같다.



(그림 4-19) 홍콩 PCO의 피해구제 절차도

먼저 커미셔너는 개인정보침해사건을 접수받으면 이의제기를 한 신청인과 그 상대방에게 연락을 취하여 예비 질의를 통해 해당 사건의 사실관계를 파악하고 법규위반사항이 있는지, 커미셔너가 관할할 수 있는 사

건인지 아닌지를 심사한다. 그 결과, 접수된 민원이 법규위반사항에 해당되지 않거나 커미셔너의 관할범위를 벗어난 사건으로 판단되는 경우에는 커미셔너가 처리할 수 없음을 알리고 사건을 종결한다.[300] 반면, 접수된 민원이 법규위반사항에 해당되는 것으로 판단되지만 중대한 침해사건은 아닌 경우, 커미셔너는 일차적으로 조정을 통한 분쟁해결을 시도한다. 커미셔너는 우선 예비 질의를 통해 수집된 증거를 바탕으로 접수된 민원내용에 대한 예비의견을 작성하여, 당사자에게 통보하고 피신청인에게 침해행위의 중지 등 구제조치를 취할 것을 권고한다. 커미셔너가 일반적으로 분쟁조정과정에서 피해구제조치로 요구하는 사항은 아래와 같다.

〔표 4-46〕 홍콩 PCO의 피해구제조치

유형	피해구제 조치
당사자 사과	개인정보침해행위에 대하여 당사자 사과 유도
시정조치	개인정보 부당수집의 경우 정보의 반환 또는 폐기 권고
	부정확한 개인정보 보유시, 정정요구 수용토록 권고
	목적달성 후 필요이상으로 개인정보 보유시 파기토록 권고
	개인정보 이용목적 변경시 동의가 없는 경우, 해당 정보의 사용중지 권고
	개인정보 열람요구 불응시 보유하고 있는 정보의 사본을 제공토록 권고
재발방지	개인정보침해행위 재발방지를 위한 대책마련 권고

※ 주 : Office of the Privacy Commissioner for Personal Data(HK), *"Mediation v. Investigation"*, Privacy Agencies of New Zealand and Australia Plus Hong Kong, 16th PANZA+ Meeting, 2003. 3. 27.

궁극적으로 커미셔너의 분쟁조정은 당사자의 협력과 합의의사에 따라 결과를 달리한다. 즉, 커미셔너의 위와 같은 권고가 어떠한 구속력 있는 효력을 가지는 것은 아니며 조정을 통해 분쟁이 종국적으로 해결될지 여부는 당사자의 의사에 달려있다. 따라서 커미셔너의 권고를 양 당사자가

300) 커미셔너는 홍콩 개인정보법 제39조에 따라 접수된 사건을 처리하지 않을 것을 결정할 수 있는 재량을 가지고 있다. 커미셔너의 이러한 결정은 사건이 접수된 후 최대 45일 이내에 이루어져야 한다.

모두 받아들일 경우 분쟁은 원만히 해결되며 사건은 종결된다. 그러나 이러한 방법을 통해서도 분쟁해결이 되지 않을 경우, 커미셔너는 공식적인 조사를 수행할 수 있다. 또한 당해 사건이 중대한 사안일 때에는 합의권고나 조정을 통한 분쟁해결절차를 거치지 않고 즉시 공식조사에 착수할 수도 있다. PCO는 이러한 조사를 위해 개인정보법 제7장에 따라 일반적인 조사권을 부여받고 있다. 이에 의하면, PCO는 당사자에게 각종 정보와 문서를 제공토록 요구할 수 있고 관계인을 소환하여 조사할 수 있으며 증언을 청취할 수도 있다. 또한 직접 정보처리자를 방문하여 정보처리시스템을 조사하는 것도 가능하다.[301]

일반적으로 PCO가 조사하는 내용은 해당 사건이 개인정보법 및 정보보호원칙을 위반하였는지 여부이다. 만약 위반사항이 발견된 경우, 커미셔너는 관련 정보처리자에게 위법행위로 인한 피해를 구제할 수 있는 조치를 취하도록 강제력 있는 이행고지(enforcement notice)를 부과할 수 있다.[302] PCO는 이 경우 해당 개인정보침해행위가 반복적으로 발생하였는지 유무, 재발할 가능성이 있는지 여부, 침해행위로 인하여 경제적·정신적 손해가 발생하였거나 발생할 가능성이 있는지 여부 등을 종합적으로 고려하여 이행고지를 부과하고 있다. 이러한 강제명령을 이행하지 않는 것은 범죄행위가 되며 벌금 또는 구류의 형이 부과될 수 있는 바, 커미셔너는 이러한 명령을 불이행하는 경우에는 법무부에 사건을 이첩하여 제재를 받도록 할 수 있다.[303] 그러나 만약 정보처리자가 커미셔너의 이

301) 홍콩 개인정보법 제69조제(9)항에 의하면, 커미셔너의 합법적인 조사를 방해하거나 응하지 않는 정보처리자는 홍콩 형사소송법(The Criminal Procedure Ordinance) 부칙 8, 제113B조에 따라 최고 10,000 홍콩달러의 벌금형을 받을 수 있으며, 개인정보법 제69조제(9)항에 따라 최고 6개월의 징역형을 부과받을 수도 있다. (Office of the Privacy Commissioner for Personal Data(HK), "*Mediation v. Investigation*", Privacy Agencies of New Zealand and Australia Plus Hong Kong, 16th PANZA+ Meeting, 2003. 3. 27.)

302) 홍콩 개인정보(프라이버시)법령 제50조.

303) 커미셔너의 이행고지 불이행시에는, 홍콩의 형사소송법 부칙 8, 제113B조에 따라 최고 50,000 홍콩달러의 벌금이나, 홍콩 개인정보보호법 제64조제(7)항에 따라 최고 2년의 징역형에 처해질 수 있다. (Office of the Privacy Commissioner for Personal Data(HK), supra note 301)

행고지에 대하여 반대의견을 제시하고자 할 때는 행정항소위원회(Administration Appeals Board)에 항소할 수 있다. 한편 커미셔너는 이행고지를 내리는 등 공식적인 조사 절차가 완료된 이후에도, 공공의 이익에 필요하다고 판단될 때에는 조사결과와 커미셔너의 권고내용, 사건처리결과 등을 보고서로 출판하여 공표할 수 있다. 특히 커미셔너는 악의적인 정보이용자에 대한 강력한 제재 수단의 하나로 해당 정보이용자의 신원을 보고서에서 밝힐 수도 있다.

지금까지 살펴본 개인정보커미셔너의 피해구제절차를 이용하는 것 외에도, 정보주체는 개별적으로 소송을 통해 민사적·형사적 피해구제를 받을 수 있다. 홍콩 개인정보법 제66조에 의하면, 정보주체는 정보처리자가 동법에 위반하여 개인정보를 침해한 때에는 그로 인해 입은 경제적·정신적 피해를 배상받을 권리를 가지고 있다. 또한 정보주체는 개인정보 침해사건이 형사범죄라고 판단되는 경우 커미셔너에게 이의제기를 신청하지 않고 직접 홍콩 경찰에 형사고소를 할 수도 있다. 그러나 개별 정보주체가 행하는 형사고소나 민사소송은 커미셔너가 행하는 피해구제에 비해 실효성이 떨어지는 편이다. 특히 민사적 손해배상결정은 커미셔너의 권한 밖의 역할이므로 피해자가 손해배상을 원할 경우 민사소송에 통해 해결하는 방법 밖에는 없다. 그러나 형사고발과 같은 형사적 피해구제의 경우, 커미셔너의 역할이 큰 편이다. 커미셔너는 접수된 사건이 개인정보법 제64조제10항[304]에 해당되는 경우, 즉 형사범죄가 되는 경우에는 접수를 받은 즉시 또는 공식조사를 거친 이후 다른 형사기관에 이첩하여 추가 수사 및 법무부에 의한 기소가 이루어지도록 할 수 있다.[305]

---

304) 홍콩 개인정보법 제64조제(10)항 : 「정보이용자가 형벌규정이 명시되어 있지 아니한 동 법령 규정에서 요구하고 있는 사항을 합법적인 이유없이 위반(정보보호원칙 위반 제외)하는 경우에는 범죄가 성립되어 제3수준에 해당되는 벌금형에 처해질 수 있다」

305) 홍콩 개인정보법 제64조는 범죄가 되는 행위에 대하여 상세하게 규정하고 있는데, 이에 의하면 정보보호원칙(DPP) 위반은 형사범죄로 인정되지 않고 있다. 따라서 DPP 위반의 경우에는 먼저 커미셔너가 이행고지를 하고 불이행시에만 형사처벌을 할 수 있다.

제 5 장 각국의 개인정보피해구제제도 비교

지금까지 우리나라와 유럽, 아시아, 북미, 오세아니아 지역의 주요 국가의 개인정보보호법과 개인정보보호기구, 정보처리자와 정보주체의 분쟁해결 또는 정보주체의 권익을 구제하기 위한 절차 및 방법에 대하여 그 일반적인 현황을 살펴보았다. 이를 통해 각국은 자신들만의 고유한 사회·경제적 환경과 법적 전통, 정보화의 발달정도 등에 따라 다양한 모습을 보이고 있음을 확인할 수 있었다. 특히 개인정보피해구제제도는 그 나라의 사법(司法)제도, 국민들의 법감정, 국가의 역할이 어느 정도 중시되는지 여부 등에 따라 달라질 수 있기 때문에 더욱 그러하다.

본 장에서는 지금까지 살펴본 내용을 바탕으로 각국의 개인정보피해구제제도를 상호 비교·분석해보는 기회를 갖고자 한다. 이를 통해 우리나라의 개인정보피해구제제도가 세계적인 동향이나 추이와 비교해볼 때, 어떠한 모습을 보이고 있으며 차이점은 무엇인지를 살펴볼 수도 있을 것이다. 이를 위해서 먼저 실체법적 측면에서 각국의 개인정보보호 법제를 살펴보고, 다음으로 개인정보보호기구와 피해구제 절차 및 방법을 비교해보도록 하겠다.

제 1 절 개인정보보호법 비교

오늘날 세계 각국은 개인정보와 관련된 법률을 제정하여 시행함으로써 현대 정보사회에서는 필수불가결한 현상이 되고 있는 개인정보의 수집·이용·저장·제공행위를 규율하는 법적 근거를 마련하고 있다. 이하에서는 이러한 각국의 개인정보 관련 입법의 존재형식, 기본법의 제정 여부, 법률의 적용대상 및 범위 등의 측면에서 비교해보도록 한다.

1. 입법의 존재형식에 따른 비교

오늘날 세계 각국의 개인정보보호법은 법률의 적용범위나 영역이 특정 부문에 한정되어 있는지 아니면 개인정보보호를 위한 기본적인 사항을 규정하여 포괄적인 적용범위를 가지고 있는지에 따라, 통합형 입법주의와 구분형 입법주의로 나누어 볼 수 있다.

가. 통합형 입법주의

통합형 개인정보보호법이란 공공부문과 민간부문을 포괄적으로 규율하는 개인정보보호기본법을 의미한다. 그러나 통합형 입법주의라고 하여 개별 영역별 개인정보 법률이 전혀 없는 것은 아니다. 공공부문과 민간부문을 아우르는 기본법은 모든 영역에 적용될 수 있는 기본원칙과 같은 일반적인 사항을 규정하고 있고 세부적인 내용을 규정하지 않는 경우가 많다. 그렇기 때문에 개인정보 유형의 다양성, 정보처리기술의 복잡성, 개인정보처리 영역의 광범위성 등으로 인하여 새롭고 특수한 분야의 경우에는 별도의 개인정보 관련 특별법이 제정되어 시행되고 있는 경우가 많다. 또한 기본법에서 모두 포함할 수 없는 부분을 특별법 또는 하위법령으로 제정하는 형식 외에도, 개인정보커미셔너와 같은 개인정보보호기구에게 실행규약의 승인이나 제정을 통해 통합형 개인정보보호법에서 제시하고 있는 기본원칙의 적용범위를 영역별 특성에 적합하게 확대 또는 축소할 수 있도록 상당한 재량권을 부여하고 있는 경우도 많다.

아래 〔표 5-1〕은 공공·민간 통합형 입법주의 형식을 취하고 있는 국가들의 개인정보보호 기본법을 정리한 것이다. 오늘날 유럽 대부분의 국가들은 물론이고 호주, 뉴질랜드, 홍콩, 일본과 같은 다른 지역의 국가들도 이러한 통합형 개인정보보호법을 제정하여 시행하고 있다.

〔표 5-1〕 공공·민간 통합형 입법주의

국가	법률
영국	정보보호법(Data Protection Act, 1998)
프랑스	정보처리파일및자유에관한법률(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)
독일	연방정보보호법(Bundesdatenschutsgesetz, 1974)
스웨덴	개인정보법(Personal Data Act 1998)
스페인	개인정보보호기본법(Organic Law on the Protection of Personal Data, 1999)
네덜란드	개인정보보호법(Personal Data Protection Act, 1999)
오스트리아	연방개인정보보호법(Datenschutzgesetz, 1978)
벨기에	개인정보처리에관한프라이버시보호법(Law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data, 1992)
덴마크	개인정보처리에관한법(The Act on Processing of Personal Data, 2000)
핀란드	개인정보법(Personal Data Act, 1999)
그리스	개인정보처리에서의개인의보호에관한법(Law on the Protection of Individuals with regard to the Processing of Personal Data, 1997)
아일랜드	정보보호법(Data Protection Act, 1988)
이탈리아	개인정보처리에서의개인및기타주체의보호에관한법(Law on the Protection of individuals and other subjects with regard to the Processing of Personal Data, 1996)
룩셈부르크	개인정보처리에서의개인의보호에관한법(Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, 2002)
포르투갈	개인정보보호법(Act on the Protection of Personal Data, 1998)
노르웨이	개인정보법(Personal Data Act, 2000)
아이슬란드	개인정보처리및보호에관한법(Act on the Protection and Processing of Personal Data, 2000)
스위스	연방정보보호법(Federal Act on Data Protection, 1992)
호주	프라이버시법(Privacy Act, 1998)
뉴질랜드	프라이버시법(Privacy Act, 1993)

홍콩	개인정보법(Personal Data(Privacy) Ordinance, 1996)
일본	개인정보보호에관한법률(2003)

이처럼 유럽을 비롯하여 많은 국가들이 통합형 입법주의 형식의 개인정보보호법을 가지고 있다. 그러나 통합형 입법주의를 취하고 있다고 하더라도 실제로는 국가별로 상당히 다양한 유형을 보이고 있다. 예를 들어 독일은 '연방정보보호법'이라는 개인정보보호기본법을 가지고 있지만, 동법은 공공영역과 민간영역을 구분하여 각기 다른 규정을 두고 있다. 또한 호주의 개인정보보호기본법인 '프라이버시법'도 공공과 민간에 적용되는 개인정보보호원칙을 달리 규정하고 있다.

한편 일본은 2003년 '개인정보보호에관한법률'을 새로 제정하였는데, 동법은 개인정보보호 기본법적 성격을 가지고 있다고 볼 수 있다. 왜냐하면 동법은 개인정보보호를 위한 기본이념을 설정하고 있는데, 이는 공공부문과 민간부문의 구분없이 모든 개인정보처리를 함에 있어 기본으로 삼아야 하는 이념 내지 원칙이라는 성격을 가지기 때문이다. 또한 동법은 제4장 '개인정보취급사업자의 의무 등'에 관한 규정을 제외하고는 대부분 국가 및 지방공공단체가 개인정보보호를 위해 하여야 할 책무를 비롯하여 공공부문과 민간부문에 모두 적용되는 규정을 담고 있기도 하다. 따라서 통합형 입법주의를 취하고 있다고 볼 수 있을 것이다. 그러나 동법은 법률규정의 상당부분을 민간영역에서 영리목적으로 개인정보를 취급하는 자를 대상으로 하여 적용[306]되고 있어 한편으로는 민간영역에 적용되는 개인정보보호법으로 볼 수 있는 여지도 있다. 특히 일본은 「행정기관이보유하는개인정보보호에관한법률」,「독립행정법인등이보유하는개인정보보호에관한법률」과 같은 공공부문에 적용되는 별도의 입법을 가지고 있어, 공공부문과 민간부문에 대하여 별도의 개인정보보호법을 가진 구분형 입법주의로 구분할 수도 있을 것이다. 따라서 일본의 입법

306) 동법 제4장은 개인정보취급사업자의 의무에 관한 규정인 바, 이는 민간영역에서 개인정보 데이터베이스 등을 사업에 이용하고 있는 영리목적의 사업자에게만 적용되고 있다.

방식은 완전한 통합형으로 보기에 다소 어려움이 있다. 그러므로 보다 명확하게 말하자면, 본래 미국식의 영역별 입법방식을 가지고 있었던 일본은 올해 새로운 개인정보보호법을 제정함으로써 미국식의 영역별 입법방식과 유럽식의 통합형 입법방식의 중간단계적 성격을 가지는 입법체계를 갖춘 것으로 볼 수 있다.

나. 구분형 입법주의

통합형과는 달리 구분형 입법주의는 개인정보보호법의 적용을 받는 영역을 공공부문과 민간부문 또는 각 영역별로 구분하여 개별적으로 입법하는 방식이다. 이러한 구분형 입법주의를 취하고 있는 대표적인 국가는 캐나다와 미국이다.

〔표 5-2〕 구분형 개인정보보호법

국가	적용범위	법률
캐나다	공공	프라이버시법(Privacy Act, 1980)
	민간	개인정보보호및전자문서에관한법률(Personal Information Protection and Electronic Documents Act, 2000)
미국	영역별 입법	· 프라이버시법(Privacy Act, 1974) · 공정신용보고법(Fair Credit Reporting Act, 1970) · 가족의교육권및프라이버시에관한법률 (Family Educational Rights and Privacy Act, 1974) · 금융프라이버시권에관한법률 (Right to Fianancial Privacy Act, 1978) · 케이블통신정책법(Cable Communications Policy Act, 1984) · 전기통신프라이버시법 (Electronic Communications Privacy Act, 1986) · 비디오프라이버시보호법(Video Privacy Protection Act, 1988) · 근로자기록보호법(Employee Polygraph Protection Act, 1988) · 운전자 프라이버시보호법 (Driver's Privacy Protection Act, 1994) · 아동온라인프라이버시보호법 (Child Online Privacy Protection Act, 1998) · 건강보험휴대법(HIPPA) (Health Insurance Portability and Accountability Act)

〔표 5-2〕에서처럼, 캐나다는 공공부문과 민간부문에 적용되는 법률이 명확하게 구분되어 별도로 제정되어 있다. 반면 미국은 건강정보, 교육정보, 비디오감시, 신용정보, 금융정보, 전자통신분야, 공공분야 등 개개 영역별로 입법이 산재되어 있는 것을 확인할 수 있다.

한편 우리나라의 개인정보보호법도 이러한 구분형 입법주의 형식을 취하고 있다고 하겠다. 특히 구분형 중에서도 캐나다와 같이 공공부문과 민간부문에서 각각 대표적인 기본법적 성격을 가진 형식이라기보다는, 오히려 미국과 같이 개별입법을 가지고 있다고 보는 쪽이 더욱 가깝다. 공공기관개인정보보호법과 정보보호법이 어느 정도 공공부문과 민간부문에서 기본법적 역할을 하고 있기는 하지만[307], 양자 모두 적용범위에 있어서 다소 한계가 있기 때문이다. 공공기관개인정보보호법은 적용범위가 컴퓨터에 의해 전산처리되는 개인정보에 한정되고 있으며, 민간분야의 정보보호법도 원칙적으로 정보통신망을 통해 영리목적으로 개인정보를 처리하는 사업자에게만 적용된다는 점에서 그 규제대상이 한정적이기 때문에 각 분야를 대표하는 기본법의 성격을 가지고 있다고 보기 어렵다.

2. 적용범위에 따른 비교

앞서 개인정보보호법을 공공부문과 민간부문을 모두 포함하는 통합형 입법주의, 공공부문과 민간부문으로 구분하는 입법주의, 금융・의료・통신부문 등 영역별로 적용되는 입법주의로 구분한 것은 큰 틀로 바라본 적용대상의 측면이었다. 여기서는 영역(sector)을 기준으로 적용범위를 구분하지 않고, 세부적으로 법률의 보호대상이 되는 개인정보의 범위가 어느 정도인지에 따라 각국의 개인정보보호법을 구분해 보기로 한다.

---

307) 물론 공공기관 등은 행정업무 등을 함에 있어 대부분의 개인정보를 컴퓨터에 의해 전산처리하고 있기 때문에 사실상 그 적용범위가 포괄적이라고도 볼 수 있고, 민간부문에서도 정보보호법 제58조가 일부 개인정보를 많이 수집하고 이용하는 오프라인 사업자에게도 적용하고 있다는 점에서 각각 공공부문과 민간부문의 기본법적 역할을 하고 있다고도 볼 수 있다.

가. 개인정보의 자동처리 유무에 따른 분류

초기 개인정보 관련규정이 법체계 속에 등장하기 시작한 때, 이러한 개인정보 관련 법규범은 대체로 공공부문에서의 컴퓨터로 처리되는 개인정보를 보호하기 위한 제한적인 범위를 가지고 있었다. 그러나 오늘날은 개인정보를 다루는 영역이 공공부문에 한정되지 않고 민간 영역에서도 폭넓게 개인정보를 이용하는 예가 증대되고 있을 뿐 아니라, 오프라인에서 수집된 정보가 컴퓨터에 의해 저장·처리되고 컴퓨터에서 처리되는 정보가 오프라인의 출력물로 변환되어 이용되는 등 컴퓨터로 처리되는 개인정보와 오프라인으로 처리되는 개인정보의 구분이 더 이상 불필요한 상황이다. 이에 최근에는 개인정보보호법의 보호대상이 되는 개인정보의 범위가 점차 넓어지고 있다. 예를 들어, 스웨덴의 「개인정보법」[308]과 프랑스의 「정보처리파일및자유에관한법률」[309]은 EU지침과 유사하게 컴퓨터로 자동처리되는 개인정보 및 구조화된 파일링시스템의 일부를 구성하는 개인정보를 보호대상으로 삼고 있지만, 영국과 독일은 일부 비구조화된 수동파일에도 정보보호법의 적용을 확대하고 있으며[310], 오스트리아

308) 제5조(동법의 적용을 받는 개인정보처리) :「동법은 전체적으로 또는 부분적으로 자동화된 개인정보의 처리에 적용된다. 동법은 개인정보가 특정한 기준에 따라 검색되거나 편집될 수 있는 개인정보의 구조화된 수집의 한 부분에 포함되거나 이를 구성하는 경우, 자동화된 처리에 의하지 아니하더라도 그러한 개인정보의 처리에도 적용된다.」

309) 프랑스의 정보처리파일및자유에관한법률은 명시적으로 동법이 자동화처리되는 개인정보 또는 구조화된 파일링 시스템을 구성하는 개인정보에만 적용된다고 규정하고 있는 것은 아니다. 다만, 동법 제3조는 정보주체의 알 권리 및 이의제기의 권리를 규정하면서 '자동화 정보처리'라는 제한을 두고 있으며, 프랑스의 개인정보보호기구인 CNIL도 개인정보의 공적 또는 사적 자동화처리의 법준수 여부를 규율(제14조)하는 것을 통해 실질적으로 동법은 순수하게 수동처리되는 개인정보는 적용되지 않음을 알 수 있다.

310) 영국은 구조화되었는지 여부와는 관계없이 특정한 수동처리되는 의료기록 및 교육기록과 접근가능한 모든 공공기록도 정보보호법의 적용을 받는 것으로 하여 그 범위를 확장시키고 있고(정보보호법 § 2.1(c)), 독일의 경우 공공부문에서 정보주체의 권리에 관한 규정은 자동화된 수단으로 처리되거나 또는 구조화된 파일과 관련성이 있는지 여부와는 관계없이 처리되는 모든 개인정보에 적용되고 있다.(연방정보보호법 § 1(2), 12(4)).

는 모든 자동·수동 처리되는 개인정보에 대해 일반적으로 「연방개인정보보호법」을 적용하고 있다.[311]

또한 유럽 외 국가들을 살펴보면 호주, 뉴질랜드, 홍콩, 캐나다 등은 법적용을 받는 개인정보의 범위를 자동처리되는 개인정보 또는 구조화된 파일링시스템을 구성하는 개인정보에 한정하지 않고 있는 것이 일반적이다. 캐나다의 경우 민간부문에 적용되는 PIPEDA는 '영리목적'을 위해 활동하는 민간단체의 개인정보처리를 그 보호대상으로 하여 동법의 적용범위가 제한적이기는 하나, 자동처리 또는 수동처리를 기준으로 적용범위를 구분하고 있지는 않다.

그러나 우리나라의 공공기관개인정보보호법은 기본적으로 컴퓨터로 처리되는 개인정보에 적용되며, 민간부문의 대표적인 개인정보 관련법률인 정보보호법 역시 정보통신망을 통해 수집·이용·처리되는 개인정보에 한하여 적용되는 것이 기본사항임은 앞서 살펴본 바와 같다.[312] 물론 정보보호법 제58조 및 동법시행령 제28조는 일부 오프라인 영역에서의 개인정보 처리에 대해서도 정보통신망의 개입이나 개인정보의 자동처리 여부와는 관계없이 동법이 적용될 수 있음을 규정하고 있기는 하나 다소 범위가 제한적이다. 이하 [표5-3] 은 자동처리정보와 수동처리정보를 기준으로 각국의 개인정보보호법상 개인정보의 적용범위를 구분해본 것이다.[313]

---

311) 단, 정보주체의 권리와 같은 규정은 일부 그 적용범위를 제한하여 자동처리되는 개인정보 및 구조화된 수동파일에 의해 보유되는 개인정보에만 적용된다. (Douwe Korff, *"EU Study on Implementation of Data Protection Directive - Comparative summary of national laws"*, Human Rights Centre, University of Essex, 2002.p. 32)

312) 정보보호법은 명시적으로 개인정보의 범위를 제한하고 있지는 않지만, 동법 제4장 개인정보의 보호 규정은 정보통신서비스제공자와 이용자와의 관계에서 개인정보를 보호하고 있기 때문에 당연히 정보통신망에 의해 처리되는 개인정보로 그 보호범위가 한정된다.

313) 여기서 법적용을 받는 개인정보의 범위는 가장 원칙적인 적용범위를 의미하며, 각국의 법률은 세부적으로 적용이 제외되는 기관이나 단체를 나열 또는 명시하거나 그 범위를 한정하고 있는 경우가 대부분이다.

〔표 5-3〕 처리방법에 따른 개인정보의 범위

적용되는 개인정보의 범위	해당국가	법률규정
자동·수동처리 여부와는 관계없이 모든 개인정보에 적용	캐나다	프라이버시법 (§ 3)
		PIPEDA(§ 2(1)) (단, 영리목적으로 이용되는 개인정보에 한정 (§ 4(1))
	호주	프라이버시법 (§ 6(1))
	뉴질랜드	프라이버시법 (§ 2(1))
	일본	개인정보보호법 (제1조) (단, 민간영역의 경우 영리목적으로 이용되는 개인정보에 한정)
	홍콩	개인정보법 (§ 2(1))
· 자동처리되는 개인정보 · 구조화된 수동 파일링시스템을 구성하는 개인정보	프랑스	정보처리파일및자유에관한법률 (§ 4 등)
	스웨덴	개인정보법 (§ 3)
	미국	프라이버시법 (§ (a)(5))
· 자동처리되는 개인정보 · 구조화된 수동 파일링시스템을 구성하는 개인정보 · 순수하게 수동처리되는 의료·교육기록	영국	정보보호법 (§ 2.1(c))
· 공공부문 : 모든 자동·수동처리되는 개인정보 · 민간부문 : 자동처리되는 개인정보, 구조화된 수동 파일링 시스템을 구성하는 개인정보	독일	연방정보보호법 (§ 1(2), 12(4)) (단, 공공부문의 경우 적용되는 법률규정에 차별을 둠)
· 컴퓨터로 처리되는 개인정보	한국	공공기관개인정보보호법 (제1조)
· 정보통신망에 의해 처리되는 개인정보 · 일부 오프라인 개인정보		정보보호법 (제58조 ; 동법시행령 제28조) (단, 영리목적으로 이용되는 개인정보에 한정)

나. 정보주체의 성질에 따른 분류

각국의 법률은 법인정보와 사자의 정보를 보호대상으로 삼을 것인지에 대해서도 다양한 입장을 취하고 있다. 영국과 스웨덴, 홍콩, 한국, 일본은

명시적으로 생존하고 있는 개인에 관한 정보만을 보호대상으로 규정하고 있는 반면, 법인정보와 사자(死者)의 정보를 개인정보보호법의 적용대상으로 규정한 국가도 있다.

먼저 법인정보에 대해 살펴보면, 영국, 프랑스, 독일[314], 한국, 일본, 캐나다, 호주[315] 등 대부분의 국가들은 법인정보는 다른 영업비밀의 보호 등으로 인하여 보호될 수 있는 것이므로 개인정보보호의 차원에서 다룰 필요가 없다는 입장을 취하고 있다. 그러나 오스트리아, 덴마크와 같은 일부 국가에서는 법인정보는 일종의 집적된 개인정보를 의미하기 때문에 더욱 그 보호 수준을 강화하여야 한다고 보아 개인정보보호법의 적용대상으로 정하고 있기도 하다.[316]

다음으로 사자(死者)의 정보를 살펴볼 수 있다. 뉴질랜드의 경우, 명시적인 규정을 통해 개인정보는 사자의 정보를 포함한 것이라고 밝히고 있으며[317], 캐나다와 미국의「프라이버시법」도 법률의 적용대상을 생존하는 개인에 관한 정보로 한정하고 있지 않다. 각국에서 법인정보와 사자의 정보에 대해서 취하고 있는 입장을 살펴보면 아래와 같다.

---

314) 독일의 연방정보보호법은 기본적으로 자연인에 관한 정보만을 적용대상으로 하고 있다. 다만, 동법은 독일 헌법상 정보자기결정권을 구체화한 것이라는 점을 볼 때 명시적으로는 아닐지라도 법인정보도 적용대상에 포함되는 것으로 볼 수 있다는 견해가 있다. (Douwe Korff, supra note 311, p. 34)

315) 호주의 프라이버시법 제6조제(1)항 및 제(4)항은 개인(individual)이란 자연인(natural person)을 의미하는 것으로, 자연인 이외의 인(人)도 함축적으로 포함되는 것으로 볼 수 없다고 하여 법인이 동법 적용대상이 아님을 명백히 규정하고 있다.

316) 오스트리아 「연방개인정보보호법」 제4조제3항은 "정보주체는 정보관리자가 아닌 자로서 자신에 관한 정보가 처리되는 모든 자연인, 법인 또는 자연인의 연합체를 의미한다"고 규정하고 있다. 덴마크의 「개인정보처리에관한법률」도 법인정보를 동법 적용대상으로 규정하고 있기는 하나, 일반적으로 적용되는 것은 아니고 해당 법인정보가 신용정보기관을 위해 처리되는 경우 등에 한하여 제한적으로 일부 규정만 적용된다(제1조제(3)항～제(5)항).

317) 뉴질랜드 「프라이버시법」 제2조제(1)항은 "개인정보는 식별가능한 개인에 관한 정보를 의미하며, 1951년「출생및사망신고법(Births and Deaths Registration Act, 1951)」에 따라 사망신고자 명부에 등록된 자에 관한 정보도 포함된다"고 하여 명시적으로 사자의 정보를 개인정보의 범위에 넣고 있다.

［표 5-4］ 법인정보와 사자의 정보에 대한 법적용 여부

적용되는 개인정보의 범위	해당국가	법률규정
생존하고 있는 개인에 관한 정보만을 적용대상으로 함을 명시적으로 규정	영국	정보보호법 (§ 2.1)
	스웨덴	개인정보법 (§ 3)
	일본	개인정보보호법 (제2조제1항)
	홍콩	개인정보법 (제2조)
	한국	공공기관개인정보보호법 (제1조), 정보보호법 (제2조)
· 기본적으로 생존하고 있는 개인에 관한 정보에 적용 · 법인정보는 보호대상에서 제외	독일	연방정보보호법 (§ 3(1))
· 사자의 정보가 유족과 관계를 가진 경우 적용 · 법인정보는 보호대상에서 제외	프랑스	정보처리파일및자유에관한법률 (§ 4, (§40-4)
· 생존하고 있는 개인의 정보로 한정하고 있지 않음 · 법인정보는 보호대상에서 제외	미국	프라이버시법 (§ 552a (a)(4))
	호주	프라이버시법 (§ 6(1),(4))
· 사자의 정보도 적용하나, 사후 20년이 지난 자의 개인정보는 제외 · 법인정보는 보호대상에서 제외	캐나다	프라이버시법 (§ 3)
		PIPEDA (§ 2(1), § 7(3)(h)(ⅱ))
· 명시적 규정을 통해 사자의 정보도 적용대상에 포함 · 법인정보는 보호대상에서 제외	뉴질랜드	프라이버시법 (§ 2(1))
법인정보를 적용대상에 포함	오스트리아	연방개인정보보호법 (§ 4(3))
	덴마크	개인정보처리에관한법률 (§ 1(3)～(5)) (단, 일부 제한적으로 적용)

제 2 절 개인정보보호기구 비교

개인정보보호를 위한 각국의 노력은 실체법적 측면에서 개인정보 관련 법령을 정비하는 것에 그치지 않는다. 많은 국가들이 이러한 개인정보 관련법령이 제대로 정립되고 이행될 수 있도록 제도적인 측면에서 개인정보보호기구를 설치하여 운영하고 있다. 특히 영국, 프랑스, 캐나다, 호주 등과 같은 국가들은 개인정보보호 전담기구를 통해 보다 효과적으로 개인정보보호의 기능을 수행하고 있다. 이러한 개인정보보호 전담기구는 정보주체의 법적 권익을 보호하고 불법적인 개인정보침해행위를 보다 효과적으로 방지하여 올바른 정보처리관행을 확립하는 데 기여할 수 있다는 점에서 세계적인 추세가 되고 있다.

그러나 각국의 개인정보보호기구는 기능, 역할, 소속, 유형 등의 측면에서 그 나라의 법적 환경이나 사회·경제적 특성, 정보화 발달여부 등에 따라 각기 다른 모습을 보이고 있는 것 또한 사실이다. 예를 들어 미국은 별도의 전담기구를 설치하지 않고 독립규제기관인 연방거래위원회(FTC)가 소비자 프라이버시 및 개인정보보호의 역할도 함께 담당하고 있다. 이렇듯 각국에서 개인정보보호기구는 구조적 형태나 기능, 권한 등의 측면에서 차이점이 두드러지고 있는 바, 아래에서는 이를 중심으로 개인정보보호기구를 비교해보고자 한다.

1. 형태에 따른 분류

각국의 개인정보보호기관이 어떠한 형태로 구성·운영되고 있는지를 구분해보면, 크게 법원 형태의 사법기구형과 전문적인 독립기구형, 행정부 지원형, 행정부 소속형, 민간단체형의 다섯 가지로 나누어 볼 수 있다. 각각의 유형은 다시 세부적으로 구분될 수 있는데 이를 표로 비교해보면 다음과 같다.

［표 5-5］개인정보보호기구의 형태별 구분

대분류	소분류	내용	해당 국가
사법 기구형		개인정보 관련 사건 심사	영국(정보법원), 뉴질랜드(인권법원)
전문 독립 기구형	합의제형	독립위원회와 이를 지원하기 위한 사무국 자체 운영됨	프랑스(정보자유위원회)
	독임제형	커미셔너와 이를 지원하기 위한 사무국 자체 운영됨	영국, 캐나다, 호주, 홍콩, 뉴질랜드
	별도기구형	별도 독립기구가 설치·운영	스페인(개인정보보호원)
행정부 지원형	합의제형	위원회의 운영을 행정부가 지원하는 형태	오스트리아(정보보호위원회), 핀란드(정보보호위원회), 네덜란드(정보보호위원회)
	독임제형	옴브즈만을 지원하는 사무국을 행정부에서 지원	핀란드(정보보호옴브즈만)
	별도기구형	기구의 예산, 인력 등을 행정부가 지원하는 형태	독일(연방정보보호청)
정부부처 소속형	합의제형	행정부처에 의해 설립되고 지원되는 위원회 형태	아이슬란드(정보보호위원회),
	행정기관	행정부처 기타 소속기관이 개인정보보호 업무 수행	스웨덴(정보조사원), 그리스(정보보호원), 덴마크(정보보호원), 노르웨이(정보조사원)
민간 단체형		비영리 민간단체가 개인정보보호의 역할 수행	미국, 일본

이 중 그 성격이 다른 사법기구형과 민간단체형을 제외한 전문독립기구형, 행정부지원형, 행정부소속형을 구분하는 중요한 요소는 기관장의 임명권자, 위원회의 경우 위원의 자격 및 임명·위촉권자, 사무국의 자체 운영여부, 업무활동을 보고하는 기관이 누구인지 여부, 명시적인 법률상의 소속규정 등이다. 물론 각각의 유형을 선을 긋듯이 명확하게 구분한다는 것은 사실상 불가능하며 국가별로 다양한 형태의 기구들이 있어 한 유형에 꼭 들어맞는다고 보기도 어렵지만, 위에서 본 중요요소들을 중심으로 그 행정체계를 구분해보는 것도 의미는 있을 것이다.

대체로 전문독립기구형은 전문성과 독립성, 자율성을 실질적으로 확보하고 있는 형태의 개인정보보호기구를 의미한다. 따라서 기관장의 임명을 국왕이나 대통령, 수상, 의회 등의 상위기관에서 행하며, 업무활동에 대해서도 의회 등에 직접 보고를 하며, 예산·인력 등을 행정부로부터 지원받기도 하나 자체적으로 사무국 등 기관의 운영을 실질적으로 담당하고 있다. 반면에 행정부지원형은 활동하는 업무의 내용이나 기관의 성격, 기관장의 임명권자 등에 있어서 전문독립기구형과 유사하나, 개인정보보호기구의 사무국의 운영이나 예산 및 인력 등의 지원에 있어 행정부의 영향력이 전문독립기구형보다 큰 형태를 의미한다. 마지막으로 정부부처 소속형은 기관의 소속이 행정부처 소속이거나 행정부처의 일부를 구성하며, 기관장의 임명도 주로 행정기관에 의해서 이루어지는 특징을 가지고 있다. 그러나 이 경우에도 대부분 법률에 의하여 당해 행정부처가 개인정보보호기구의 임무에는 일체 간섭할 수 없다.

가. 사법기구형

사법기구형은 고도의 독립성이 유지되는 사법기구인 법원이 다른 개인정보보호기구와 연계하여 개인정보침해 및 법위반에 관한 사건을 처리하는 형태의 기관이다. 법원은 모든 국가에서 개인정보피해구제의 역할을 담당하는 대표적인 사후적 피해구제기관이다. 그럼에도 불구하고 사법기구형을 별도로 구분한 것은 일반 민사·형사·행정법원을 통해서가 아니라 별도로 개인정보와 관련된 사건을 처리하는 특별법원의 한 형태로 운영되는 경우가 있기 때문이다. 즉, 이러한 사법기구형 개인정보보호기구는 법원의 일종이나 개인정보 또는 인권, 프라이버시 등에 관한 사건을 개인정보(프라이버시) 보호기관으로부터 직접 이관 받아 심사하고 처리한다는 점에서 특색이 있다. 여기에는 개인정보와 정보공개 등의 사안을 심사하는 영국의 정보법원(Information Tribunal)과 개인정보 또는 프라이버시 침해를 포함하여 제반 인권문제에 대하여 모두 심사하는 인권법원(Human Right Review Tribunal)이 해당된다.

나. 전문 독립기구형

세계 각국의 개인정보보호기구가 참여하는 국제정보보호기구회의(The International Conference of Data Protection Commissioners)에서는 '효율적인 개인정보보호의 역할을 담당하고 있는 개인정보보호기구'를 승인하고 있는데, 그 승인 요건 중 하나가 바로 독립성과 자율성이다.[318] 전문독립기구형 개인정보보호기구는 바로 이러한 독립성과 자율성, 그리고 전문성을 담보할 수 있다는 점에서 의미가 있다. 즉, 앞서 살펴본 바와 같이 전문독립기구형 개인정보보호기구는 ① 한 국가 내에서 개인정보보호에 관한 모든 전반적인 업무를 처리한다는 점에서 전문성을 갖추고 있으며, ② 개별 행정부처가 아닌 국왕, 대통령, 수상, 의회 등에 소속된 기구로서 의회나 수상에게 기관의 업무결과나 실적과 같은 제반사항을 직접 보고한다는 점에서 독립성을 확보하고 있다. 또한, ③ 업무를 수행하는 사무국의 운영을 자체적으로 하고 있기 때문에 일반 행정기관의 간섭을 배제하고 독자적으로 활동해나갈 수 있다는 점에서 자율성을 갖추고 있다.

전문독립기구형은 다시 합의제형, 독임제형, 별도기구형의 세 가지 유형으로 나누어 볼 수 있다. 먼저 합의제형은 위원회 형태의 전문·독립기구로서 대표적인 예는 프랑스의 정보자유위원회(CNIL)이다. 정보자유위원회는 입법부, 사법부, 행정부 등에서 선출된 위원들로 구성된다는 점에서 각각의 위원들은 직무수행에 있어 독립성과 자율성을 보장받고 있다.[319] 특히 정보자유위원회는 3권 중 어느 권력에도 속하지 않으며 기관장인 위원장도 대통령이나 의회 등에서 임명하는 것이 아니라 위원 중

318) 2001년 파리에서 개최된 정보보호기관회의에서는 법적 근거, 자율성과 독립성, 다양한 국제협약이나 가이드라인의 준수 등을 개인정보보호기관의 승인기준으로 삼고 있다. (Blair Stewart, *"International Accreditation of Privacy and Data Protection Authorities"*, APEC Data Privacy Workshop(Panel Ⅱ), Chiang Rai, Thailand, 2003)

319) 「정보처리파일및자유에관한법률」제13조에 의하면, 정보자유위원회는 권한의 행사에 있어 다른 어떠한 기관의 지시·감독도 받지 않는 고도의 독립성을 가진다. 다만, 동법 제23조에 의해 위원들은 매년 대통령과 의회에 업무상황을 보고하여야 한다.

에서 호선한다는 점에서 다른 어떠한 형태의 기구들보다도 높은 독립성을 가졌다고 볼 수 있다.

한편, 전문・독립기구형의 대표적인 형태는 독임제형이다. 이는 1인의 커미셔너(Commissioner)가 개인정보보호를 책임질 단독기구로 임명되고 이를 지원하는 사무국이 운영되는 형태이다. 현재 영국, 캐나다, 호주, 뉴질랜드, 홍콩에서 이와 같은 형태의 개인정보보호기구를 운영하고 있는데, 커미셔너는 주로 국왕이나 대통령 등 최고통수권자에 의해 임명되며 개인정보보호법에서 규정한 역할과 기능을 수행할 수 있도록 폭넓은 권한을 부여받고 있다. 커미셔너는 개인정보 처리행위의 감독과 실행규약과 같은 각종 지침의 제정, 상담 및 피해구제 등 개인정보보호를 위한 업무를 전담하여 수행하고 있기 때문에 대표적인 전문독립기구로 볼 수 있다. 그러나 독임제형의 경우도 대부분 커미셔너의 전문성을 보강하는 한편 커미셔너의 독주를 견제하기 위해 일반적으로 각종 자문위원회, 전문위원회 등이 설치・운영되고 있다.

이 밖에도 커미셔너나 위원회 형태가 아닌 별도의 독립기관이 개인정보보호를 위한 전담 역할을 맡는 예가 있다. 대표적으로 스페인의 개인정보보호원(Agencia de Protección de Datos)이 이에 해당된다. 개인정보보호원의 기관장은 국왕에 의해 개인정보보호자문위원회(Consultative Council) 구성원 중에서 임명되는데, 자문위원회는 입법부와 행정부, 학계, 소비자・사업자 단체 대표들로 구성된다. 스페인의 「개인정보보호기본법(Organic law 15/1999 of 13 December on the Protection of Personal Data)」제36조에 의하면, 개인정보보호원은 독립적이고 객관적으로 직무를 수행하며 다른 어떠한 기관의 지시도 받지 않는다. 단, 기관의 실적이나 상황에 대해서는 직접 의회에 보고하여야 한다.

다. 행정부 지원형

많은 국가들이 개인정보보호와 관련된 업무를 전문적으로 행하는 법정기구를 운영하고 있지만, 사실 이러한 개인정보보호기구는 법률에서 규

정한 역할과 임무를 원활히 수행하기 위한 예산이나 인력 면에서 행정부의 지원을 받는 경우가 많다. 즉, 행정부 지원형은 전문·독립기구형과 비교해볼 때, 기관장의 임명권자나 구성원의 직위, 기능, 역할, 권한 등의 측면에서 그리 큰 차이는 없지만 사무국의 운영을 행정부로부터 지원받고 있다는 점에서 양자의 차이가 있다고 하겠다. 행정부 지원형도 역시 합의제형, 독임제형(옴브즈만형), 별도기구형으로 나눠볼 수 있다.

먼저, 합의제형에는 대표적으로 오스트리아의 정보보호위원회와 정보보호자문위원회(Data Protection Council)를 들 수 있다. 정보보호위원회의 위원은 사법부와 행정부, 지방자치단체, 정당대표 등으로 각각 구성되어 있고, 연방정부의 제청을 받아 연방수상이 후보자 중 선정하여 연방대통령이 직접 임명한다. 또한 자문위원회의 위원들도 정당대표, 연방정부 대표, 지방정부 대표 등으로 구성되며 각각의 소속기관으로부터 직접 임명되기 때문에 기관장의 임명이나 위원회의 구성인원의 자격 면에서 있어서 높은 독립성을 가지고 있다. 다만, 정보보호위원회와 자문위원회는 합의제 형태의 기구이기 때문에 별도의 사무국이 운영되고 있는데, 이 사무국은 연방수상관청 소속이며 연방정부로부터 예산을 지원받고 있다.[320] 또한 정보보호위원회는 연방정부에 대하여 연 2회 업무활동을 보고하여야 한다. 또한 네덜란드의 정보보호위원회(College bescherming persoonsgegevens)와 핀란드의 정보보호위원회(Data Protection Board)도 이와 유사한 형태이다. 네덜란드의 경우, 위원장과 위원은 법무부장관의 제청으로 국왕이 임명하며 특히 위원장은 법관의 자격을 갖춘 자 중에서 임명되나, 사무국의 직원과 자문이사회의 구성원은 위원장의 제청으로 법무부가 임명하고 있다. 핀란드의 정보보호위원회 역시 개인정보처리의 허가 및 기타 중대한 사안을 심의하여 결정하는 기구로서 국무회의에서 위원을 임명하고 있으나, 위원회는 별도 사무국을 운영하지 않으며 법무부로터 바로 행정적 지원을 받고 있다.

320) 프랑스의 CNIL과 오스트리아의 정보보호위원회 및 정보보호자문위원회는 모두 합의제형의 개인정보보호기구라는 점에서 유사하나, 위원회의 활동을 지원하고 실질적으로 업무를 수행하고 있는 사무국이 연방수상관청 소속이라는 점에서 프랑스의 CNIL과는 다소 구분된다.

한편, 핀란드는 독임제형 개인정보보호기구로서 정보보호옴브즈만(The Data Protection Ombudsman)을 설치하고 있다. 핀란드에서는 전통적으로 다양한 분야에서 옴브즈만 제도가 발달한 영향으로 개인정보와 관련하여서도 조사·감독 등 다양한 기능을 수행하고 있는 옴브즈만이 활동하고 있는 것이다. 옴브즈만은 독립적인 임무를 수행할 수 있는 개인이 임명된다는 점에서 커미셔너와 유사하나, 핀란드의 개인정보 옴브즈만은 법무부에서 옴브즈만의 활동을 지원하는 사무국의 인력과 예산을 지원하고 있다는 점에서 차이가 있다.[321]

이 외에도 행정부로부터 지원을 받고 있는 별도기구형의 개인정보보호기구가 있다. 대표적인 예가 독일의 연방정보보호청이다. 연방정보보호청의 기관장은 연방정부의 제청을 받아 의회가 선출한 자를 대통령이 임명하나, 연방내부무로부터 인력과 예산을 지원받으며 연방정부와 의회에 업무활동을 보고하도록 되어 있다.

라. 행정부 소속형

이상의 비교적 행정부로부터 독립된 형태의 개인정보보호기구와는 달리 행정기관이나 행정부 내 설치된 부속기관이 개인정보보호의 역할을 담당하는 경우도 있는데, 이는 행정부 소속형 개인정보보호기구로 분류할 수 있다. 여기에는 엄격한 의미의 행정부 소속형과 다소 포괄적인 의미의 행정부 소속형이 있다. 전자에는 개인정보보호기구가 개별 정부부처의 내청 또는 외청이나 그 산하기관으로 되어 있는 경우이고, 후자는 행정부에 의해 설립되고 운영지원을 받는 개인정보보호기구와 기관장을 각 정부부처가 임명 또는 위촉하는 경우를 포함한다.[322]

---

321) 핀란드의 정보보호옴브즈만은 1988년 설립된 기구로 5년 임기로 국무회의(Council of State)에 의해 임명되어 활동하고 있는 개인정보보호기구이다. 옴브즈만의 주요 기능은 정보처리자와 정보주체에게 상담이나 안내를 통해 정보를 제공하고, 정보처리자가 자발적인 실행규약을 제정할 수 있도록 자문을 해주거나 동 규약을 심사해 주는 것이다. 또한 정보주체의 요청이 있을 경우 정보처리자가 올바르게 법규를 준수하였는지, 정보주체의 권리를 침해하지 않았는지를 심사하여 결정한다. 정보처리실태에 관하여 조사하고 감독하는 것도 역시 옴브즈만의 주된 기능 중 하나이다.

행정부에 의해 설립되고 예산을 지원받으며 행정부처와 여러 가지 운영상 관계를 유지하고 있는 형태의 행정부 소속형 기구로 합의제 형태로 운영되고 있는 예는 아이슬란드의 정보보호위원회이다. 아이슬란드의 정보보호위원회는 법무부가 위원 및 사무국장을 임명 또는 위촉하여 설치된다.[323] 이러한 합의제형 개인정보보호기구는 법률로서 기구의 설치 및 구성이 보장되며 법률가나 교수 등의 각계 전문가로 구성된다는 점에서 개별 정부부처나 그 산하기관보다는 독립성과 전문성이 높은 편이라고 할 수 있다. 그러나 개별 행정부처의 행정적 지원을 받을 뿐 아니라 위원회의 구성과 설립도 행정부처에 의해 이루어진다는 점에서, 각 삼권에서 위원이 선출되는 프랑스의 정보자유위원회 및 국왕이나 국무회의에서 위원이 임명되는 네덜란드나 핀란드의 정보보호위원회와는 차이가 있다. 우리나라의 개인정보분쟁조정위원회도 아이슬란드와 유사한 형태의 개인정보보호기구로 볼 수 있다. 정보보호법에 의해서 설립된 법정기구이고 법조계와 학계, 시민단체 등의 전문가가 위원으로 활동하고 있기 때문에 그 독립성과 자율성이 보장되기는 하나, 정보통신부 장관에 의해 분쟁조정위원이 위촉 또는 임명된다는 점과 정보통신부 산하기관인 한국정보보호진흥원 내에 사무국을 두어 그 운영상 필요한 인력과 예산을 지원받고 있다는 점에서 행정부 소속형 합의제 기구로 볼 수 있을 것이다.

이러한 합의제형이 아닌 일반 행정기관 또는 그 소속기관이 개인정보보호의 역할을 맡는 경우가 있다. 대표적인 예가 일본의 경우이다. 일본은 별도의 개인정보보호기구를 두지 않고 각 주무 행정부처에서 개별적으로 개인정보보호의 업무를 처리하고 있다. 우리나라의 경우도 개인정

---

322) 오늘날의 개인정보보호기구들은 직무수행에 있어 독립성과 자율성이 요구되는 경우가 많기 때문에 대부분 법정기구에 해당되며, 명시적으로 어느 행정부처 소속으로 법률상 규정되어 있는 경우는 거의 없다. 따라서 법률상으로는 개인정보보호기구를 행정부 소속형으로 보기 어려운 경우가 많다. 그러나 실질적으로 기관장의 임명 또는 위촉을 각 정부부처가 행하고 사무국의 운영을 실질적으로 담당하는 경우, 행정부의 영향력을 배제하기가 쉽지 않다는 의미에서 행정부 소속형으로 구분하였다.

323) 아이슬란드의 정보보호위원회는 총 5인으로 구성되는 이사회 형태로 운영되며, 이사회의 의장과 부의장은 대법원과 아이슬란드 정보처리협의회에서 각각 추천한 자를 법무부가 임명한다.

보분쟁조정위원회가 설립되어 개인정보피해구제의 측면에서 활발히 운영되고 있다는 점을 제외하고는 기본적으로 일본과 유사하다. 즉, 행정자치부, 정보통신부, 재정경제부, 산업자원부, 보건복지부 등 각 주무부처가 해당 영역의 개인정보에 관련된 법률 규정을 마련하고 집행할 책임과 권한을 가지고 있다. 그러나 엄밀히 말해서 이런 형태의 정부부처는 본래적 의미의 개인정보보호기구라고는 볼 수 없다.

또한 스웨덴, 덴마크, 그리스, 노르웨이와 같은 유럽 일부국가의 경우도 행정부처에 소속된 행정기관이 개인정보보호기구로서 활동하고 있다. 스웨덴의 정보조사원은 중요사안을 결정하는 이사회의 구성원이 사무국장을 제외하고는 모두 현직 국회의원이라는 점에서 독립성을 가지나, 이사회의 활동을 지원하는 사무국은 재정부(Ministry of Finance)로부터 인력과 예산을 지원받으며 매년 정부에 보고를 할 뿐 아니라 사무국장과 이사회의 구성원은 모두 재정부가 임명 또는 위촉하고 있다. 덴마크의 정보보호원(Datatilsynet)도 정보이사회와 사무국으로 구성되어 운영되고 있는데, 운영을 위한 예산지원과 관련하여서는 법무부의 지원을 받으며, 정보보호원장과 이사회의 구성원은 법무부장관에 의해 임명 또는 위촉된다.[324] 또한 노르웨이의 정보보호원(Datatilsynet)의 기관장은 국왕이 임명하나 노동내무부(Ministry of Labour and Government Administration) 소속기관으로 설치되어 운영되고 있으며, 그리스 정보보호원(Hellenic Data Protection Authority)의 기관장은 현직 법관 또는 법관에 준하는 자로서 내각의 제청을 받아 대통령이 임명하나 동 기관은 법무부에 소속되어 있다.[325]

---

324) 사무국은 주로 일상적인 업무를 하며, 이사회는 공공·민간기구에 중대한 영향을 끼칠 수 있는 사건을 처리한다. 덴마크의 개인정보처리에관한법 제55조제(3)항과 제(4)항에 의하면, 정보이사회는 법관인 의장 1인과 그 외 6인의 위원으로 구성된다.

325) 노르웨이의 정보조사원은 이사회를 두고 있는데 동 이사회는 법관에 준하는 급의 3인의 교수와 3인의 개인정보보호 전문가로 구성되며, 이들은 법무부의 제청으로 의회에서 선출하며 대통령에 의해 임명된다. 또한 노르웨이에는 정보조사원 외 프라이버시 항소위원회(The Privacy Appeals Board)가 설치되어 있다. 항소위원회는 정보조사원의 결정에 불복하는 사건에 대해 심사하는 기구로서 역시 노동내무부 소속기구이나 위원회 의장과 부의장은 국회에 의해 임명된다.

지금까지 살펴본 기구들은 모두 행정부처 또는 그 소속기관이라는 점에서 행정부 소속형 기구라고 부를 수 있다. 그러나 엄격한 의미에서 유럽의 기구와 일본 및 우리나라의 경우는 다소 차이가 있다. 일본과 우리나라의 경우 각 행정부처가 소관 관할업무 내에서만 개인정보보호의 기능을 수행하나, 스웨덴 등 유럽의 기구들은 비록 특정 부처 소속하에 있기는 하지만 모든 영역에 걸쳐 개인정보보호 전담기구로서의 기능을 수행한다.[326]

〔표 5-6〕 각국 개인정보보호기구의 구성 및 운영현황

국가	기관명	구성현황	기관장임명	운영현황
프랑스	정보 자유위원회	· 위원회(총 17인) - 국회의원 6인 - 전·현직 법관 6인 - 국민의회의장이 1인 임명 - 상원의장이 1인 임명 - 국무회의가 3인 임명 · 사무국 약 80여명	위원 중에서 위원장 호선	· 위원장을 보좌하는 부서 운영 · 위원장 또는 위원장으로부터 위임받은 부위원장이 직원임명 · 대통령과 의회에 업무보고
영국	정보 커미셔너	· 커미셔너 1인 · 사무국 약 200여명	국왕	· 커미셔너가 부커미셔너와 직원 임명 · 커미셔너가 사무국 자체운영 · 의회에 보고
캐나다	연방 프라이버시 커미셔너	· 커미셔너 1인 · 사무국 약 108명	추밀원장 (Governor in Council)	· 커미셔너를 지원하는 사무국 자체 운영 · 의회소속 및 보고
호주	연방 프라이버시 커미셔너	· 커미셔너 1인 · 사무국 약 40여명	총독	· 커미셔너를 지원하는 사무국 자체 운영 · 의회 및 수상에 보고
	프라이버시 자문위원회	· 위원회(총 6인) - 자문위원 5인 - 프라이버시커미셔너	총독	· 위원회 지원 사무국 자체 운영 · 커미셔너가 자문위원회 소집권자

326) 주로 유럽에서는 공공부문에서의 개인정보침해방지를 위해 행정부 내 법무부 또는 내무부가 공공기관의 개인정보처리를 규제·감독하였으나, 점차 공공부문과 민간부문을 아우르는 개인정보보호를 위하여 행정부처 내 별도의 기구를 만들어 운영하는 것으로 체계가 변화하였다.

국가	기관명	구성현황	기관장임명	운영현황
뉴질랜드	프라이버시 커미셔너	· 커미셔너 1인 · 사무국	총독 (법무부 제청)	· 커미셔너를 지원하는 사무국 자체 운영 · 수상에게 보고
홍콩	개인정보 커미셔너	· 커미셔너 1인 · 사무국	특구 행정장관	커미셔너를 지원하는 사무국 자체 운영
	개인정보 자문위원회	· 위원회(9인 이하) - 의장 : 커미셔너 - 자문위원 : 4~8인	자문위원은 내무부가 임명	내무부가 위원회를 지원하는 사무국이 운영 지원
스페인	개인정보 보호원	· 기관 및 기관장 · 자문위원회(총 9인) - 국회의원 2인 - 행정부 대표 2인 - 왕립역사아카데미, 대학협회 추천 전문가 2인 - 소비자 및 민간정보처리자 대표 각 1인 - 민간개인정보보호기관협회 1인	국왕 (자문위원 중 임명)	· 기관장이 개인정보보호원을 대표하며 법인의 형태로 운영 · 의회에 보고
오스트리아	정보보호 위원회	· 위원회(총 10인) - 법관 1인(대법원장 추천) - 주 대표 2인 - 연방노동부 추천 3인 - 연방경제부 추천 3인 - 연방공무원(변호사 자격) 1인	연방대통령이 위원임명 (연방정부 제청 - 연방수상이 후보자 중 선정)	· 정보보호위원회 및 정보보호자문위원회의 지원을 위한 사무국 운영 · 사무국의 예산은 연방정부로부터 지원 · 사무국은 약 10명으로 연방수상관청 소속 · 정보보호위원회는 연방정부에 연2회 보고
	정보보호 자문위원회	· 위원회(총 15인) - 정당대표 8인 - 연방정부(노동부, 경제부) 대표 각 1인 - 지방자치단체 대표 4인 - 연방공무원(연방수상 임명) 1인	각 소속기관에서 위원 임명	
네덜란드	정보보호 위원회	· 정보보호위원회 - 위원장 1인 - 위원 2인 - 특별위원(일정수) · 자문위원회	국왕 (법무부 제청)	· 위원회 지원 위한 사무국 운영 · 사무국 직원과 자문위원회 구성원은 법무부가 임명

국가	기관명	구성현황	기관장임명	운영현황
핀란드	정보보호 옴브즈만	· 옴브즈만 1인 · 부 옴브즈만 1인 · 직원 약 18명	국무회의	· 옴브즈만을 지원하는 사무국 운영 · 사무국 운영은 법무부에서 지원
	정보보호 위원회	· 위원회(총 7인) - 의장 1인 - 부의장 1인 - 위원 5인	국무회의	별도 사무국 운영하지 않으면서 법무부에서 행정지원
독일	연방 정보보호청	· 기관장 · 직원 70여명	대통령 (연방정부 제청, 의회가 선출 한 자를 임명)	· 인력과 예산을 연방 내무부로부터 지원 · 연방정부와 의회에 보고
아이슬란드	정보보호 위원회	· 이사회 (총 5인) - 의장, 부의장 각 1인 (법관자격에 준하는 자) - 대법원, 정보처리협회에서 추천한 자 2인 - 기타 위와 유사한 자격을 가진 자 1인 · 정보보호위원(사무국장)	법무부	· 법무부에 의해 이사회 설립 및 구성 · 법무부가 이사회추천을 받아 정보보호위원 임명, 정보보호위원은 이사회를 지원하는 사무국 운영
스웨덴	정보조사원	· 이사회 (총 9인) - 현직 국회의원 8인 - 사무국장 1인 · 사무국 약 40여명	재정부	· 재정부가 이사회 운영을 위한 사무국의 인력과 예산 지원 · 정부에 보고
덴마크	정보보호원	· 정보이사회 (총 7인) - 의장 (법관에 준하는 자격을 가지는 자) - 6인의 위원 · 정보보호원장(사무국장) · 사무국 약 30명	법무부	· 법무부에 의해 이사회 설립 및 사무국 예산 지원 · 사무국장이 직원 채용 · 의회에 보고
그리스	정보보호원	· 정보보호기관장(법관에 준하는 자격을 가진 자) · 이사회 (총 6인) - 3인의 교수 - 3인의 전문가	대통령 (이사회 구성원은 법무부 제청에 따라 의회가 선출하여 대통령이 임명)	· 행정부 소속기관 · 사무국은 정보보호기관장이 자체운영 · 의회에 보고

국가	기관명	구성현황	기관장임명	운영현황
노르웨이	정보조사원	· 정보조사원장(법관에 준하는 자격을 가지는 자) · 사무국	국왕	· 국왕과 노동내무부 소속기관 · 국왕에게 보고
	프라이버시 항소위원회	· 위원회 (총 7인) - 의장 1인 - 부의장 1인 - 위원 5인(국왕 임명)	국회 (의장과 부의장)	· 국왕과 노동내무부 소속 기관임 · 국왕에게 보고
한국	개인정보 분쟁조정 위원회	· 위원회 (총 15인) - 4인의 법률가 - 6인의 교수 - 3인의 유관기관 전문가 - 2인의 소비자, 사업자 단체 대표 · 사무국	정보통신부	· 위원회를 지원하는 사무국이 한국정보보호진흥원에서 운영됨
	정보통신부	행정기관(정부부처)	대통령	· 개인정보보호 업무를 전담하는 정보이용보호과가 있음 · 개인정보침해신고 접수, 상담 등의 업무를 맡는 개인정보침해신고센터 운영
	개인정보보호 심의위원회	· 위원회 (총 10인) - 위원장 1인 포함 10인의 위원으로 구성 - 위원장 : 행정자치부차관 - 위원 : 국무총리가 임명 또는 위촉	국무총리	· 공공부문에서 컴퓨터에 의해 처리되는 개인정보의 보호에 관한 주요사항 심의
	행정자치부	행정기관(정부부처)	대통령	· 개인정보보호 업무 담당하는 부서가 있음 · 공공기관개인정보보호에 관한 사항을 심의하는 개인정보보호심의위원회 운영

마. 민간단체형

지금까지 살펴본 개인정보보호기구들은 모두 국가가 주도적으로 운영하는 경우였으나, 민간단체형은 국가가 아닌 일반 비영리 민간단체에서 개인정보보호의 역할을 담당하는 경우이다. 따라서 성격상 다른 유형의 기구들과는 차이가 있으나, 미국이나 일본에서는 이러한 민간단체형의 개인정보보호기구들이 중요한 역할을 담당하고 있어 하나의 유형으로 분류하였다. 이러한 민간단체형의 개인정보보호기구들은 특히 민간 영역에서 사업자들의 자율규제 차원에서 활동하고 있는 경우가 많으며, BBBOnLine과 같은 프라이버시보호단체 및 일본의 인정개인정보보호단체가 여기에 해당된다.

2. 개인정보보호기구의 기능 비교

가. 개인정보보호기구의 주요기능 현황

국내·외 개인정보보호기구들의 기능 및 역할을 비교함에 앞서, 먼저 제4장 해외 개인정보피해구제제도 현황 부분에서 살펴본 10개 주요국 및 기타 참고할 만한 국가들의 개인정보보호기구들이 수행하는 대표적인 몇 가지 기능과 역할을 정리해보면 다음과 같다.

〔표 5-7〕 각국 개인정보보호기구의 주요기능 현황

국가	기관명	주요기능
프랑스	정보자유위원회	· 불만접수 및 사실조사, 합의권고 및 화해유도 · 개인정보처리자 등록 및 국외이전 허가 · 개인정보 세부지침 및 실행규약 제정 · 법준수여부 조사, 감독 및 시정권고, 시정명령 · 개인정보보호 자문

국가	기관명	주요기능
영국	정보커미셔너	· 불만접수 및 사실조사, 합의권고 및 화해유도 · 개인정보처리자 신고접수 및 등록 · 법준수여부 감독 및 정보고지, 이행고지 부과 · 정보법원에 제소
캐나다	연방프라이버시 커미셔너	· 불만접수 및 사실조사, 합의권고 및 화해유도 · 가이드라인 제정 · 법준수여부 조사, 감독 및 시정권고 · 입법안 심사 및 의견제시
호주	연방프라이버시 커미셔너	· 불만접수 및 사실조사, 화해유도, 분쟁조정 및 결정 · 가이드라인 제정 및 프라이버시 규약 승인 · 법준수여부 조사, 감독 및 시정권고 · 입법안 심사 및 자문
	프라이버시 자문위원회	· 프라이버시 관련 문제에 대하여 커미셔너에게 자문 · 커미셔너가 가이드라인 제정시 참여 및 자문
뉴질랜드	프라이버시 커미셔너	· 불만접수 및 사실조사, 화해유도 및 의견제시 · 가이드라인 및 프라이버시 규약 제정 · 법준수여부 조사, 감독 및 시정권고 · 인권법원에 제소
홍콩	개인정보 커미셔너	· 불만접수 및 사실조사, 화해유도 및 분쟁조정 · 개인정보 지침 제정 및 프라이버시 규약 승인 · 법준수 조사, 감독 및 이행고지
	개인정보 자문위원회	· 개인정보(프라이버시)커미셔너에게 자문
스페인	개인정보보호원	· 불만접수 및 사실조사, 화해유도 · 법준수여부 조사, 감독 및 시정명령, 과태료부과 · 정보의 국외이전 감시 및 허가
오스트리아	정보보호위원회	· 민간분야 개인정보침해 상담 및 불만접수 · 민간분야 법준수여부 조사, 감독 및 행정규제 · 민간분야 개인정보 국외이전 규제 및 정보처리 등록 · 공공분야 정보처리현황 조사 및 연방정부 보고
	정보보호 자문위원회	· 정보보호를 위한 중요사안 심의 · 입법안 및 정책에 대한 의견제시 및 자문 · 공공분야의 정보처리자에 대한 정보공개 요구
네덜란드	정보보호위원회	· 불만접수 및 사실조사, 분쟁조정 · 법준수여부 조사, 감독 및 시정권고 · 프라이버시 실행규약 제정 및 심사

국가	기관명	주요기능
핀란드	정보보호 옴브즈만	· 불만접수 및 사실조사, 위법여부 심사 및 결정 · 프라이버시 실행규약 제정촉진 및 심사 · 복잡한 사건에 대하여 정보보호위원회에 이첩
	정보보호위원회	· 정보처리 허가 · 가이드라인 제정 · 중대한 법위반 사건 심사 및 결정
독일	연방정보보호청	· 불만접수, 실태조사를 통한 위법행위 발견 및 시정권고 · 정보처리자 신고접수 및 등록 · 입법안 및 정책에 대한 자문
스웨덴	정보조사원	· 개인정보처리 등록 및 허가 · 불만접수, 실태조사를 통한 위법행위 발견 및 시정권고 · 법준수여부 조사, 감독 및 시정명령, 과태료 부과 · 지침 제정 및 프라이버시 실행규약에 대한 의견제시
덴마크	정보보호원	· 불만접수, 사실조사 및 합의권고 · 법준수여부 조사, 감독 및 행정규제 · 입법안 검토 및 자문
아이슬란드	정보보호위원회	· 불만접수, 사실조사 및 합의권고 · 개인정보처리자 등록 · 법준수여부 조사, 감독 및 행정규제 · 가이드라인 제정
그리스	정보보호원	· 불만접수, 실태조사를 통한 위법사실 발견 및 고발 · 규칙 및 지침 등 제정
노르웨이	정보조사원	· 개인정보처리 허가 · 정보처리자의 실행규약 제정 협조 · 법규준수여부 조사, 감독 및 시정명령
	프라이버시 항소위원회	· 정보조사원의 결정에 대한 항소사건 심사

이상으로 각국의 개인정보보호기구들이 행하는 주요 기능 및 역할을 살펴볼 수 있었다. 각국의 개인정보보호기구들이 행하는 기능은 조금씩 차이가 있기는 하나, 대체적으로 가장 기본적인 기능인 상담·자문에서부터 피해구제, 각종 법률이나 정책에 대한 자문제공, 자율규제 활동의 지원, 교육·홍보, 개인정보보호법 준수여부 감시 등의 역할을 수행하고

있음을 확인할 수 있다. 이러한 개인정보보호기구들이 행하는 주된 기능을 분류하여 정리해보면 다음과 같다.

〔표 5-8〕 개인정보보호기구의 주요기능

구분	내용
상담 및 정보제공	· 정보주체 및 정보처리자의 권리·의무에 관한 정보제공 · 정보주체 등에 대한 교육실시 · 연차보고서 등 발간물을 통한 정보제공 및 홍보
자문기능	· 개인정보관련 입법안에 대해 의회 또는 행정부 자문 · 개인정보관련 법률이나 정책에 대한 검토의견 제시
피해구제	· 피해자의 불만접수 및 사실조사 · 당사자간의 분쟁해결을 위한 화해, 조정 등 · 접수된 피해자의 불만사건에 대한 의견제시 및 결정 · 피해구제 관련 소송지원
등록·허가	· 정보처리행위 신고접수 및 등록 또는 허가 · 개인정보 국외이전 등 허가
법준수 조사	· 법준수여부 실태조사 또는 감사
제재 기능	· 위법행위 사실 고지, 경고, 시정권고 · 법준수를 위한 시정명령, 이행고지 부과 · 과태료 등 행정벌 부과, 공표, 형사고소
준입법적 기능	· 규칙 등 하위법령 또는 지침 제정 · 자율규제 촉진을 위한 실행규약 제정 또는 승인
대외 협력	· 국내의 민간 개인정보보호단체 및 형사기관 등 사법기구와의 협력 · 해외 개인정보보호기구 및 국제기구와의 협력

나. 중점적 기능에 따른 비교

〔표5-8〕은 일반적으로 세계 각국의 개인정보보호기구들이 수행하는 기능을 8가지 유형으로 구분하여 정리한 것이다. 그러나 모든 개인정보보호기구들이 위에서 열거한 기능들을 모두 수행하고 있는 것은 아니다. 대부분 개인정보 상담이나 정보제공과 같은 역할은 기본적으로 하고 있지만, 적극적인 피해구제의 역할을 중시하는 기구가 있는 반면 개인정보 실태조사 등을 통해 법준수여부를 감시하고 규제하는 기능을 더 활발히

펼치는 기구도 있다. 따라서 개인정보보호기구를 그 기능이나 역할을 중심으로 비교해보기 위해서 우선 해당 기구가 '중점을 두고 수행하는 주된 기능이나 역할이 무엇이냐'를 기준으로 분석해 보았다.

여기에는 크게 감독형과 피해구제형이 있다. 일반적으로 감독형은 개인정보처리자에 대한 관리·감독을 통해 개인정보보호를 도모하고자 하는 기관을 말하며, 피해구제형은 관리·감독보다는 개인정보침해로 인한 피해구제를 주로 수행하는 기관을 말한다. 이와 같은 구별은 국가, 특히 여기서는 법원이 아닌 개인정보보호기관이 개인정보보호를 위해 담당할 수 있는 역할을 무엇으로 볼 것인가에 따른 것이다. 개인정보보호기관의 역할을 개인정보처리행위에 대한 관리·감독 및 이를 통한 개인정보 침해행위의 예방과 보호에 있다고 보는 때에는 전자에 해당하게 되나, 개인정보처리자에 대한 감독 외 개인정보침해로 인한 피해구제의 측면을 강조하고 소송외 분쟁해결방법을 적극적으로 제공하여야 한다고 보는 때에는 후자에 해당하게 된다. 따라서 감독형을 띠고 있는 개인정보보호기관은 관리·감독의 편의성과 효율성을 위해 개인정보처리자를 등록 또는 허가제도를 통해 규제하는 반면, 피해구제에 중점을 두고 있는 개인정보보호기관은 소송외 분쟁해결제도 마련과 이를 통한 분쟁해결에 중점을 두는 특징을 가진다.[327]

〔표 5-9〕 개인정보보호기구의 주요 역할에 따른 구분

구분	감독형	피해구제형
의미	주로 감독기능 수행	감독과 함께 피해구제기능 수행
특징	· 개인정보처리자의 등록 또는 허가를 통해 개인정보 처리를 관리·감독 · 침해행위에 대하여 행정적 규제 · 민사적 피해보상구제는 하지 않음	· 피해구제를 위해 개인정보보호기관이 적극 관여 · 당사자간 합의를 유도, 분쟁해결 도모 · 대안적 분쟁해결제도를 적극 활용
국가	영국, 프랑스, 독일, 스웨덴 등	캐나다, 호주, 뉴질랜드, 홍콩 등

327) 여기서의 구분은 개인정보보호기관의 주된 기능이 무엇인가에 따른 것이므로, 감독기능을 주로 수행하는 기관이라 할지라도 정보주체와 개인정보처리자와의 분쟁해결을 위한 알선이나 화해유도의 역할을 전혀 하지 않는 것은 아니다.

표를 통해 살펴본 바와 같이, 현재 주로 유럽에서는 개인정보처리자에 대한 관리·감독을 용이하게 하기 위해 등록 또는 허가제도를 활용하여 등록된 개인정보처리자의 개인정보 수집·이용·보유 등의 행위를 효과적으로 관리하고 감독하는 기능에 중점을 두고 있다. 물론, 감독형 개인정보보호기구들도 불법적인 개인정보침해행위로 인하여 피해를 입은 자가 불만을 신고하는 경우 이에 대한 사실조사를 하여 당사자간 원만히 해결되도록 화해를 유도하거나 알선 등의 방법으로 문제를 해결하기도 하지만, 적극적으로 소송외적 분쟁해결제도를 활용하여 분쟁조정이나 결정 등의 해결방법을 활용하고 있지는 않다. 특히 손해배상과 같은 민사적 피해구제는 법원의 고유영역이라고 하여 개인정보보호기관이 관여하는 것을 꺼리고 있다. 따라서 개인정보침해행위로 인한 피해자의 불만처리와 피해구제보다는 개인정보처리 등록 또는 허가를 통한 사전 확인과 침해예방 및 행정적 규제에 초점을 두고 있는 것으로 볼 수 있다. 반면 캐나다, 호주, 뉴질랜드, 홍콩 등의 개인정보보호기관은 개인정보침해행위로 인하여 피해를 입은 자가 민원을 제기하면 이에 대해 조사를 하여 화해나 조정 등의 방법을 통해 분쟁을 해결하는 등 보다 적극적인 피해구제 역할을 하고 있다. 소송을 통한 개인정보 피해구제가 복잡하고 어렵다는 측면을 감안하여 개인정보보호기관이 직접 당사자간 분쟁해결에 기여하고 피해구제기능을 제공하는 것이다. 전자상거래와 관련하여 소송외 분쟁해결제도가 활발히 이용되고 있다는 점을 미뤄볼 때, 개인정보에 관한 분쟁의 특수성을 고려하여 피해구제 기능을 개인정보보호기관이 제공할 필요성도 인정될 수 있을 것이다. 개인정보처리자의 법규 준수에 대한 관리·감독의 한계를 피해구제를 통해서 극복할 수도 있으며, 감독기능과 피해구제기능은 상호보완적으로 작용할 수도 있기 때문이다.

3. 개인정보보호기구의 권한 비교

앞서 살펴본 바와 같이, 각국의 개인정보보호기구들은 피해구제에서부터 법준수여부 조사, 규칙제정 등 다양한 역할과 기능을 수행해오고 있다. 각국의 개인정보보호법은 개인정보보호기구가 이러한 기능을 원활히 수행할 수 있도록 필요한 권한을 부여하고 있다. 따라서 각국의 개인정보보호기구가 피해구제 기능, 행정적 기능(등록・허가), 조사・감독 기능, 규제적 기능, 준입법적 기능 등을 수행하기 위하여 부여받은 권한을 정리해 볼 수 있을 것이다. 특히 여기서는 사전 침해예방적 기능 수행을 위한 권한과 사후 피해구제적 기능 수행을 위한 권한으로 구분하여 살펴보도록 하겠다.

가. 사전 침해예방적 기능을 위한 권한

먼저 사전 침해예방적 기능을 위한 권한으로 개인정보보호기구는 개인정보처리자의 등록요건을 명시하고 해당 조건에 적합한 자에 대해서만 처리행위의 등록을 받거나 허가를 해 줄 수 있다. 이러한 행정적 기능은 법을 침해할 가능성이 있거나 충분히 정보주체의 개인정보를 보호할 수 없을 것으로 판단되는 정보처리자의 처리행위 자체를 허가해주지 않거나 등록을 접수하지 않음으로써 침해예방적 성격을 가진다. 그러나 한편으로는 반복적이고 중대한 법위반자에 대하여 등록을 철회하거나 허가를 해주지 않는 것으로도 활용될 수 있어, 사전예방적 측면과 사후제재적 측면을 모두 가지고 있는 것으로 볼 수 있다. 또한 개인정보보호기구는 침해예방을 위한 가장 기본적인 권한으로 개인정보보호법률에 대하여 규칙이나 지침과 같은 하위법규를 제정하여 고시할 수 있다. 여기에는 자율규제 차원에서 정보처리자가 스스로 법규를 준수할 수 있도록 개인정보 실행규약(프라이버시규약)을 제정하여 고시할 수 있는 권한, 실행규약의 제정에 의견이나 자문을 제공할 수 있는 권한, 실행규약을 승인하여

일종의 법적 효력을 부여해 줄 수 있는 권한 등이 포함된다. 각국의 개인정보보호기구가 이러한 권한 중 어느 정도를 부여받아 행사하고 있는지 비교해보면 다음과 같다.

〔표 5-10〕 각국 기구의 사전예방적 권한 비교

국가	기관명	개인정보처리		규칙, 지침, 가이드라인	실행규약		
		등록 심사권	허가권	제정권	제정권	승인권	자문권
영국	정보커미셔너	○	×	○	○	×	○
프랑스	정보자유위원회	○ (민간)	○ (공공)	○	×	×	○
독일	연방정보보호청	○	×	○	×	×	○
스웨덴	정보조사원	○	×	○	×	×	○
미국	연방거래위원회	×	×	○	×	×	○
캐나다	연방프라이버시 커미셔너	×	×	○	×	×	○
호주	연방프라이버시 커미셔너	×	×	○	×	○	○
뉴질랜드	프라이버시 커미셔너	×	×	○	○	○	○
홍콩	개인정보커미셔너	○	×	○	○	○	○
일본	각 주무부처	×	×	○	×	×	○

※ 주 : 스웨덴 정보조사원은 1973년 정보법 하에서는 허가 업무를 담당하고 있었으나, 1998년 정보보호법에서는 이러한 허가권한을 규정하고 있지 않음

나. 사후 피해구제적 기능을 위한 권한

위법행위 등 개인정보침해행위로 인한 피해를 사후적으로 구제하기 위해 각국은 이에 대한 불만을 접수받아 처리할 뿐 아니라, 개인정보(프라이버시) 감사(audit) 또는 실태조사를 통해 위법사실을 발견하고 규제하

는 역할을 한다. 이를 위해 개인정보보호기구에 부여된 가장 기본적인 권한은 사실조사권이다. 사실조사권에는 각종 문서 등 자료의 제출을 요구할 수 있는 권한, 당사자인 정보주체와 정보처리자를 소환하여 의견을 청취할 수 있는 권한(당사자 소환 및 심문권), 관계인 기타 증인을 소환하여 의견을 듣고 증거를 확보할 수 있는 권한(증인 등 소환 및 심문권), 개인정보를 처리하는 시스템 및 구역에 접근하여 정보를 획득하고 조사할 수 있는 권한(정보처리시스템 접근권), 정보처리자의 업무영역 등을 방문하여 현장조사를 할 수 있는 권한(정보처리기관 방문조사권) 등이 있다. 이러한 사실조사권은 거부시 법률에 의해 형사처벌이 가해짐으로써 더욱 강력하게 보장되고 있는 경우가 많다.[328]

한편 개인정보보호기구는 사후 피해구제를 위해 의견제시 등 시정권고, 화해·알선 등을 통한 합의권고, 분쟁조정, 준사법적 결정권한을 가지며, 위법행위가 있을 경우 취할 수 있는 규제적 조치로서 이행고지 부과, 시정명령, 형사고발, 소송제기, 과태료 부과, 공공기관을 대상으로 한 정보공개명령권 등을 행사할 수 있다. 이러한 권한 중 사후적 피해구제 등의 기능 수행을 위해 각국의 개인정보보호기구가 어느 정도의 권한을 확보하고 있는지 비교해보면 다음과 같다.

［표 5-11］각국 기구의 사후구제적 권한 비교

권한		영국	프랑스	독일	스웨덴	미국	캐나다	호주	뉴질랜드	홍콩	일본
사실조사	자료제출 요구권	○	○	○	○	○	○	○	○	○	○
	당사자 의견청취권	○	○	○	○	○	○	○	○	○	○
	증인소환·심문권	○	×	×	×	×	○	○	○	○	×
	정보시스템 접근조사권	○	○	○	○	×	○	○	○	○	○

328) 일반적으로 홍콩, 영국, 프랑스, 독일 등에서는 개인정보보호기구의 사실조사를 방해하는 개인정보처리자는 형벌이 부과된다.

피해구제	시정권고(의견제시)	○	○	○	○	○	○	○	○	○	○
	합의권고	○	○	○	×	×	○	○	○	○	×
	분쟁조정	×	×	×	×	×	○	○	×	○	×
	준사법결정	×	○	×	×	○	×	○	×	×	×
규제조치	이행고지	○	×	×	×	×	×	×	×	×	×
	시정명령	×	○	×	△	×	×	×	×	○	○
	정보공개명령권	○	×	×	×	×	×	×	×	×	×
	과태료부과	×	×	×	○	×	×	×	×	×	○
	형사고발	○	○	○	○	○	○	○	○	○	○
	소제기	○	×	○	○	○	○	○	○	×	×

※ 주 : 스웨덴의 정보조사원은 직접 특정 행위를 취하도록 하거나 또는 금지하는 명령을 내리지는 않으나, 과태료를 부과함으로써 당해 행위를 금지하는 명령에 갈음하는 형식을 취하고 있다.

각국의 개인정보보호기구는 조금씩 차이점이 있기는 하지만 일반적으로 사실조사권과 시정권고권은 기본적으로 부여받고 있다. 왜냐하면 개인정보처리행위의 위법성 여부를 보다 정확하고 확실하게 조사하여 발견된 위법행위에 대해서 법준수를 촉구하는 것은 개인정보보호기구의 핵심적인 기능 중 하나이기 때문이다. 또한 이는 화해유도나 합의권고 또는 분쟁조정을 통한 원만한 분쟁해결을 위해서도 무엇보다도 필요한 권한이기도 하다. 특히 사실조사권 중에서도 필요한 문서, 정보, 자료를 제출받을 수 있는 권리 및 당사자의 의견을 청취할 권리는 일반적으로 대부분의 개인정보보호기구에 부여되고 있다. 더 나아가 호주, 뉴질랜드, 영국 등의 경우에는 당사자 및 증인을 소환하여 증언을 확보할 수 있고 직접 처리되고 있는 개인정보 및 정보시스템 등 시설에 접근하여 조사할 수 있는 권한도 행사하고 있다. 그러나 시정명령이나 과태료 부과, 이행고지 등의 행정제재권한 등의 규제권은 대체로 민간부문의 법령위반행위에 한할 뿐 아니라 모든 기구에서 폭넓게 운영되고 있지는 않다. 특히 다른

공공기관이나 행정기관의 법위반행위에 대하여는 의견제시나 시정권고에 그치는 경우가 대부분이다. 여기서는 각국의 개인정보보호기구가 어떠한 권한을 가지고 있는지 여부만을 살펴보도록 하고, 피해구제 및 규제조치와 관련된 권한의 자세한 내용은 이하 제3장의 '피해구제 방법 및 절차 비교' 부분에서 살펴보기로 한다.

제 3 절 개인정보피해구제제도 비교

입법방식과 같은 법적 측면, 그리고 개인정보보호 전담기구의 설치여부 및 기구의 성격, 기능, 권한 등의 구조적 측면을 국가별로 상호 비교분석해보는 것만큼 의미 있는 것이 바로 개인정보피해구제의 방법, 절차, 형태 등을 살펴보는 것이다. 본 절에서는 먼저 개괄적으로 개인정보피해구제제도를 주로 담당하고 있는 주체를 중심으로 비교한 뒤, 구체적으로 각국의 개인정보보호기구가 어떠한 방법과 절차를 통해 피해구제의 역할을 수행하고 있는지를 비교해보도록 한다.

1. 주체에 따른 분류

소송외 분쟁해결제도는 '누가 소송외 분쟁해결제도를 제공하고 있는가'라는 기준에 따라 크게 ① 정부가 설립, 자금을 지원 또는 운영하는 형태(Government-established, funded or run ADR), ② 공공·민간 혼합형(Mixed public-pirvate ADR), ③ 민간 소송외 분쟁해결제도(Private ADR)의 세 가지로 구분된다.[329] 따라서 이러한 구분을 기준으로 삼아 각국의 개인정보 피해구제제도를 비교해 본다.

가. 정부 주도의 피해구제

정부가 지원·운영하는 형태의 개인정보피해구제제도란 정부가 개인정보보호의 역할을 담당하는 기구 등을 설립하여 정보처리자와 정보주체간의 분쟁을 객관적인 입장에서 공정하게 해결함과 동시에 피해구제의 적극적 역할을 맡는 제도이다. 한국을 비롯하여, 캐나다, 뉴질랜드, 홍콩이 대표적으로 이와 같은 형태의 피해구제제도를 갖추고 있다.

329) OECD Working Party on Information Security and Privacy, *"Legal Provisions Related to Business-To-Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection"*, 2002, http://www.oecd.org

나. 민간 주도의 피해구제

개인정보피해구제는 민간 개인정보보호단체를 통해서도 이루어질 수 있다. 특히 앞에서도 잠깐 언급한 바 있지만, 민간단체의 개인정보보호의 역할이 중요하게 인식되고 있는 나라는 미국이다. 미국은 전통적으로 B2C 분쟁 등에서 다양한 민간기관이 소송외 분쟁해결제도를 제공하여 왔으며, 개인정보피해구제와 관련하여서도 BBBOnLine 등에서 활발한 역할을 담당하고 있다. 물론 미국에서도 연방거래위원회(FTC)가 일부 영역에서 개인정보보호의 역할을 담당하면서, 소비자로부터 직접 불만사항을 접수받아 조사하고 결정을 내리는 과정에서 당사자간 합의에 이르도록 화해를 유도하는 등의 피해구제 기능을 담당하고 있기는 하지만, 분쟁해결이나 피해구제에 적극 관여한다기보다는 소송외 분쟁해결제도를 제공하는 민간 기관을 지원·장려하고 개인정보 침해행위를 방지하기 위한 관리·감독의 측면에 비중을 두고 있다.[330]

다. 복합적 형태

정부주도형과 민간주도형의 중간적 형태의 피해구제제도를 활용하고 있는 곳으로 대표적인 국가가 호주와 일본이다.[331] 호주의 경우, 연방프라이버시커미셔너는 업계에서 마련한 실행규약이 개인정보보호원칙 및 프라이버시법에 부합하는지를 심사하여 이를 승인할 수 있는데, 이렇게 승인된 규약은 법적인 효력을 가지게 된다. 따라서 커미셔너의 승인을 받은 업계의 실행규약이 자체적으로 공정한 고충처리절차 내지 피해구제절차를 포함하고 있는 경우, 분쟁 당사자는 커미셔너에게 이의를 제기하기

330) Council of Better Business Bureaus, Inc., *"Alternative Dispute Resolution for Consumer Transactions in the Borderless Online Marketplace"*, 2000, http://www.bbbonline.org 참조.

331) 물론 미국도 민간 프라이버시단체에서 해결되지 않은 사건에 대해 FTC가 관여하여 해결하는 시스템을 갖추고 있으나, 이는 민간단체와 정부가 유기적으로 연결되어 협조함을 의미하지, 호주나 일본에서와 같은 복합적 형태와는 다소 차이가 있다.

전에 먼저 업계의 규약에 따른 절차를 이용하여야 한다.[332] 그러나 만약 이 절차를 거친 후에도 합의가 원만히 도출되지 않았거나 피해자가 적절한 구제를 받지 못하였다고 여기는 경우 또는 업계가 승인규약을 가지고 있지 않은 경우에는 프라이버시커미셔너가 바로 사건을 처리할 수 있다. 호주에서는 이를 '공동규제체계(Co-regulatory scheme)'라고 부르고 있는 바, 개인정보 침해행위가 발생한 민간영역이 스스로 적극적인 피해구제를 할 수 있도록 기회를 부여함과 동시에 프라이버시커미셔너가 이를 감독·보완할 수 있는 장치를 마련하고 있다는 점에서 특색이 있다.[333] 한편 일본도 최근 제정된 개인정보보호법을 통해 인정개인정보보호단체에 대한 규정을 두고 있다. 일본은 본래 별도의 개인정보보호기관을 두지 않고 개인정보로 인한 피해구제의 역할을 비영리민간기구에 일임하여 오는 등 미국과 같은 민간주도형 분쟁해결제도의 형태로 운영되고 있었다. 그러나 올해 5월 일본은 개인정보보호법 제정을 통해 민간부문의 개인정보보호의 실효성을 확보하기 위한 방안으로 인정개인정보보호단체제도를 도입하였다. 인정개인정보보호단체란 개인정보보호기관으로서 갖추어야 할 조건들을 충족한 기관이라고 각 주무부처의 장관이 인정한 기관을 의미한다. 즉, 개인정보보호의 기능을 하는 민간단체에 대해 일정기준이 충족되면 주무장관이 인정함으로써, 개인이 믿고 고충처리를 의뢰할 수 있도록 한 것이다. 일본은 이러한 인정개인정보보호단체제도를 도입하면서 민간의 자율성과 정부의 지도·감독간의 조화를 도모하고 있다. 인정개인정보보호단체제도는 정부의 주무대신이 특정 민간단체에 대하여 개인정보보호의 역할을 담당하는 기구임을 '인정'해줌으로써 정부가 다하지 못하는 피해구제 등의 역할을 민간단체가 적극적으로 수행할 수 있도록 보장해줌과 동시에 적절히 역할을 수행하고 있는지를 관리한다는 점에서 기본적으로는 호주의 공동규제체계와 유사한 것으로 볼 수 있다.

---

332) 이는 연방프라이버시커미셔너의 피해구제절차를 이용하고자 할 경우에 승인된 규약에 따른 피해구제절차를 거칠 것을 의미하는 것이지, 직접 법원에 소를 제기하는 것을 막는 것은 아니다.

333) The Office of the Federal Privacy Commissioner of Australia, *"Guidelines on Privacy Code Development"*, 2001, http://www.privacy.gov.au

［표 5-12］ 피해구제 주체에 따른 분류

구분	정부주도형	민간주도형	혼합형
의미	정부가 설립·지원 또는 운영하는 기관이 개인정보 피해구제 제공	민간기관의 고충처리절차를 이용토록 하고 이를 국가기관이 감독	주로 민간기관이 소송외 피해구제의 기능을 담당, 정부는 감독 및 규제활동
장점	· 정보산업에 대한 정부의 관리, 감독 강화 및 빠른 시간 내 개인정보보호 강화 · 객관적인 제3자의 입장에서 피해구제 가능	· 정부의 간섭을 최소화하여 자유로운 정보산업 조성 · 사업자의 고객서비스 차원의 맨투맨 침해구제 가능	· 민간기구의 자율성을 해치지 않으면서, 개인정보보호 및 침해방지 가능 · 자연스럽게 사업자의 개인정보보호 의식 고취
단점	· 정부의 지나친 간섭 · 사업자들의 자발적인 정보보호 의식 고취의 어려움	· 힘의 논리에 의한 사업자 횡포 우려 · 적절한 피해구제 확보의 어려움	· 자율규제에 대한 국가의 효율적 감독 필요 · 민간기구와 국가기관의 유기적 연결 필요
국가	한국, 캐나다, 홍콩 등	미국	호주, 일본

대체로 미국 등과 같이 전통적으로 민간분야의 소송외 분쟁해결제도가 활성화되어 있고 이를 담당하는 기관이나 민간단체가 발달되어 있는 국가에서는 개인정보에 관한 피해구제제도 역시 그러한 양상을 보이고 있다. 그러나 그러한 환경을 가지고 있지 못한 국가에서는 개인정보피해구제의 필요성은 있으나 적절한 구제수단을 가지지 못한 까닭에 정부가 주도적인 피해구제의 주체로 나서게 되었다. 개인정보의 특성상 피해보상도 중요하나, 침해행위의 즉각적인 중지 또는 원상회복 등의 피해구제가 필요한 경우가 많고 이는 개인정보보호기구의 영향력 있는 권고나 조정, 때로는 시정명령 등의 방법을 통해 확보될 수 있기 때문이다. 이러한 점에서 행정적 규제를 수행하여 실효성 확보가 가능한 개인정보보호기구의 피해구제제도가 단순히 민간단체에서 행해지는 분쟁해결보다 더 효과적인 것으로 볼 수 있을 것이다. 다만, 민간에서 이루어지는 다양한 형태의 분쟁해결방안이나 피해구제제도 역시 존중되어야 하며 장기적인 관점에

서는 민간분야에서의 피해구제 역할을 증대시키는 방향으로 나아가야 할 것이다.

2. 방법에 따른 분류

오늘날 각국의 개인정보보호기구들은 그 정도의 차이는 있지만 대부분 정보주체로부터 개인정보처리에 관한 불만사항이나 분쟁을 접수받아 이를 적절히 해결하고 구제하는 역할을 담당하고 있다. 다만, 각국의 기구들이 행하는 피해구제의 방법은 무척 다양한데, 여기에는 좁은 의미의 피해구제를 가리키는 소송외적 분쟁해결제도는 물론 행정적인 제재조치로 볼 수 있는 명령 등도 포함된다. 왜냐하면 대부분 개인정보보호기구들이 행하는 피해구제의 기능은 화해, 알선 등과 같은 권고적 의견표명에서부터 시정명령, 형사고발, 소제기 등의 강제적인 조치가 일련의 연속적인 절차로 이어지게 되기 때문이다. 따라서 아래에서는 대표적으로 각국에서 행하는 피해구제의 방법을 화해·알선 등 합의권고, 조정, 시정권고, 이행고지, 시정명령, 준사법적 결정, 과태료 부과, 형사고발, 소제기 등으로 나누어 살펴보도록 하겠다.

가. 합의권고

개인정보보호기구는 개인정보처리과정에서 불합리한 개인정보침해 등으로 인하여 정보주체와 정보처리자간 분쟁이 발생하는 경우 이를 원만히 해결하기 위해 당사자를 알선하여 화해를 유도하거나 합의를 권고할 수 있다. 대부분의 개인정보보호기구는 정보주체와 개인정보처리자의 불만을 해결하기 위한 방법으로 강제적인 행정제재를 부과하거나 형사고발, 소송제기 등의 조치를 취하기에 앞서 이러한 화해나 알선 등을 적극 활용하고 있다. 즉, 화해, 알선 등을 통한 합의권고는 피해구제기능에 중점을 두고 있는 캐나다, 호주, 뉴질랜드, 홍콩 등은 물론이고 조사·감독

형 개인정보보호기구들인 영국, 프랑스, 독일 등의 유럽국가에서도 가장 기본적으로 활용되고 있는 피해구제 방법이다. 또한 우리나라의 개인정보분쟁조정위원회가 행하는 조정전 합의권고도 이에 포함된다고 할 것이다. 그러나 가장 대표적으로 화해, 알선, 의견제시 등 합의권고를 통해 분쟁을 해결하고 개인정보침해로 인한 피해를 구제하는 예는 뉴질랜드와 캐나다의 개인정보보호기구이다.

개인정보보호기구는 사안에 대하여 의견을 제시하고 당사자가 모여 화해를 할 수 있도록 권고하여 상당수의 사건을 해결하고 있는데, 이는 개인정보보호기구가 가지는 영향력을 바탕으로 한 것이다. 그러나 개인정보보호기구의 의견표명이나 합의권고는 기관의 의사일 뿐이며 구속력이나 강제력은 인정되지 않는다. 따라서 당사자가 이를 받아들이지 않는다면 강제력을 가진 행정적 제재조치를 수반하는 방법을 취하거나 법원의 판단에 맡기게 된다. 특히 뉴질랜드에서는 프라이버시커미셔너가 합의유도를 하였으나 분쟁이 해결되지 않았거나 합의가 되었으나 이행되지 않은 사건을 인권법원에 이첩하여 프라이버시법 위반여부를 심사할 수 있도록 하고 있다.[334] 즉 프라이버시커미셔너와 인권법원이 유기적으로 연결되어 개인정보보호기관이 보다 적극적인 피해구제 역할을 해낼 수 있도록 한다는 점에서 특징이 있다.

나. 조정・결정

조정은 개인정보보호기구가 분쟁해결에 있어 중립적인 제3자로서 양당사자의 견해를 청취하고 조사를 통해 사건을 판단하여 조정안을 제시하는 것을 말한다. 단순히 의견을 제시하거나 권고를 함으로써 당사자를 화해로 이끄는 방법보다 좀 더 적극적인 형태라고 볼 수 있다. 다만 조정을 하는 형태에 있어서는 형식성의 강약에 다소 차이가 있다. 예를 들

334) 뉴질랜드의 프라이버시법 제82조에 의하면, 연방프라이버시커미셔너는 동법에 의거 프라이버시 침해와 관련한 소송을 수행하기 위한 소송수행담당관을 임명하여 개인을 대신하여 인권법원에 소를 제기할 수 있도록 하고 있다.

면, 호주나 홍콩 등의 개인정보보호기구가 행하는 조정보다는 한국의 개인정보분쟁조정위원회가 행하는 조정이 보다 형식성이 강화된 형태로 볼 수 있는데, 이는 다른 개인정보보호기구가 단독제 형태로 분쟁조정을 행하는 것과는 달리 우리나라의 개인정보분쟁조정위원회는 합의제형이기 때문이다.[335] 즉 개인정보침해 등 법위반에 대한 분쟁이 있는 경우 합의제인 위원회가 조정결정을 내림으로써 조정안을 제시한다는 점에서 차이가 있다.

한편 홍콩, 호주 및 우리나라의 개인정보분쟁조정위원회가 행하는 분쟁조정절차는 원칙적으로 화해유도나 알선 등 합의권고와는 구별되는 것이지만, 실질적으로 강제력이나 구속력이 없다는 점에서는 합의권고와 유사하다. 이에 따라 호주에서는 조정이 실패로 끝났고 당해 사안이 심각한 개인정보침해라고 판단된 경우에는 기관의 이름으로 '결정(Determination)'을 내릴 수 있으며, 이는 강제적 효력을 가진다.[336] 결정은 개인정보 침해자에 대하여 손해배상이나 시정명령, 원상회복, 금지명령, 법위반사실공표, 사과명령 등의 형태로 이루어진다. 그러나 침해자가 커미셔너의 결정을 이행하지 아니한 경우 신청인은 법원에 동 결정사항에 대한 이행을 강제해 주도록 이행청구소송을 제기할 수 있다. 또한 신청인은 결정 과정에 절차상의 문제가 있었다고 판단되는 경우에는 법원에 사법심사를 청구할 수도 있다. 그러나 법원은 이행청구소송이 제기되었을 때 커미셔너가 결정하고 심사한 내용과는 관계없이 독자적으로 자료 등을 수집하고 당사자로부터 소명자료를 제출받는 등 별도의 사실확인 및 심리절차를 거칠 수 있으며 커미셔너의 결정에 구속되지 않는다.[337] 하지만 호주 프라이버시커미셔너가 개인정보침해사건에 대하여 '결정'을 내린 예는 1993년 이래 단 3건에 그치고 있다.[338]

---

335) 호주나 홍콩의 개인정보보호기구가 행하는 조정은 '유연한 형태의 조정(Flexible mediation)'으로, 개인정보분쟁조정위원회가 행하는 조정은 '형식적 형태의 조정(Formal mediation)'에 해당하는 것으로 볼 수 있다.

336) 호주의 프라이버시법 제52조는 프라이버시커미셔너에게 이러한 결정권한을 부여하고 있다.

337) Graham Greenleaf, supra note 263.

다. 시정권고

개인정보보호기구는 불만이 접수된 사건에 대하여 사실조사를 하는 과정에서나 또는 자체적인 감사 및 실태조사를 통해서 법령 위반행위가 발견되었거나 프라이버시 침해가능성이 있는 행위를 발견한 때에는 개인정보처리자에게 시정을 권고할 수 있다. 시정권고는 개인정보보호기구가 해당 개인정보처리자에게 불법임을 알리고 경고를 하여 주의를 상기시키거나, 조사 결과에 대해 일종의 의견을 제시하는 것을 모두 포함하는 것으로 분쟁해결 방법의 하나로 이용되기도 한다. 시정권고는 거의 모든 개인정보보호기구가 행할 수 있는 피해구제 방법 중 하나인데, 그 중 대표적으로 독일의 연방정보보호청은 강제적 효력을 가진 시정명령이나 이행고지권은 없고 시정권고 및 의견표명의 방법으로 피해구제를 행하고 있다. 특히 독일 연방정보보호청이 해당 공공기관에 대하여 특정한 의견을 표명한 경우, 해당 공공기관은 반드시 어떠한 조치를 취할 것인지에 대한 답변서를 제출하여야 한다.

라. 이행고지

개인정보보호기구는 또한 개인정보보호법 위반 내지 침해 행위에 대하여 해당 개인정보처리자에게 그러한 행위를 시정 또는 금지하도록 고지할 수 있는데, 이를 이행고지(Enforcement Notice)라 한다. 이행고지는 영국에서 도입하고 있는 제도로, 개인정보처리자의 법위반 사실에 대한 신고가 있는 경우 정보커미셔너는 분쟁해결을 위하여 당사자간 사전 합의를 유도하게 되는데 사전합의에 의하여 분쟁이 해결되지 않고 법위반 행위 내지 침해행위가 중대하다고 판단될 때에는 그러한 행위를 시정토록 하거나 금지하는 이행고지를 발하고 있다. 영국의 정보커미셔너의 이행고지는 법위반 또는 개인정보침해에 대한 기관의 규제적 행정행위의

338) 지금까지 호주의 연방프라이버시커미셔너는 1993년 2건, 2003년 1건만을 '결정'을 통해 해결하였을 뿐이다.

성격을 가지므로 강제력이 있다. 그러나 기관의 이행고지에 대하여 개인정보처리자가 정보법원에 항소하는 경우, 항소와 함께 이행고지의 효력이 정지되기 때문에 즉각적인 개인정보 침해행위의 제거가 필요한 사건을 적절히 구제할 수 없다는 단점이 있다. 정보법원은 항소가 제기되면 커미셔너가 내린 이행고지가 타당한지를 판단하여 결정을 내리게 된다. 정보법원에서 이행고지가 타당한 것이라고 판단을 내렸을 경우에는 법위반사실이 있는 것으로 인정되므로, 당해 사건이 형사범죄를 구성하는 때 커미셔너는 형사기관에 이를 고발할 수 있다.[339]

마. 시정명령 또는 과태료 부과

명령부과는 개인정보침해행위가 있는 경우 또는 법위반의 사실이 있는 경우, 당해 행위를 시정토록 명령하거나 더 이상의 침해행위를 하지 못하도록 금지명령을 내리는 등 규제적 행정명령을 부과하는 것을 말한다. 우리나라 및 일본의 시정명령이나 과태료의 부과, 스웨덴의 과태료 부과, 홍콩의 명령부과 등이 이에 해당되며, 영국의 이행고지와 유사한 성격을 가진다. 주로 개인정보보호기구들은 분쟁해결을 위한 사전합의 노력 또는 조정이 실패하였거나 침해사실이 중대하고 심각하다고 판단되는 경우에 이러한 명령을 부과하고 있다. 이렇듯 개인정보보호기구에서 분쟁해결을 통한 피해구제와 행정적 규제가 상호 유기적으로 연결되어 행해지는 경우도 있으나, 개인정보보호기구의 조정이나 화해와 같은 분쟁해결제도와는 관계없이 행정기관이 별도로 명령을 부과하는 경우도 있다. 그러나 분쟁해결제도와 이와 같은 규제행위가 유기적으로 연결되어 있는 경우에는 명령부과가 사실상의 이행강제의 성격을 가질 수 있으므로 효과적인 피해구제를 담보할 수 있다는 장점이 있다. 특히 홍콩에서는 더 나아가 개인정보보호기구의 명령을 이행하지 않는 경우 위법행위가 되어 형사고발이 가능하다는 특색이 있다.[340] 또한 시정명령은 정보처리자가

339) Information Commissioner, *"Annual Report And Accounts For The Year Ending 31 March 2002"*, 2002, http://informationcommissioner.gov.uk

이에 대해 법원에 이의제기를 하더라도 원칙적으로 법원의 최종 판결이 있기 전까지 강제력을 유지된다는 점에서 전술한 이행고지와 다르다.

바. 형사고발 및 소제기

개인정보보호기구들은 화해, 합의권고, 시정권고 등 의견제시를 하는 단계에서 분쟁이 원만히 해결되지 않을 경우, 이행고지 또는 시정명령을 내리거나 과태료를 부과하는 등 행정명령을 내림으로써 개인정보침해행위를 중지 또는 금지한다. 그러나 때때로 이러한 방법을 통해서 문제가 해결되지 않거나 궁극적인 피해구제가 이루어지지 않는 경우가 있다. 또한 법위반사항이 심각하거나 형사처벌대상인 경우도 있다. 이러한 경우 대부분의 개인정보보호기구들은 위법행위를 한 정보처리자를 형사고발하거나 소송을 제기할 수 있다. 특히 별도의 개인정보와 관련된 사법기구를 가진 영국과 뉴질랜드의 경우, 개인정보보호기구는 해당되는 정보법원과 인권법원에 소를 제기할 수 있고 이를 담당하는 소송담당관이 별도로 임명되어 있다. 또한 미국의 FTC의 경우에도 개인정보침해 사업자와의 합의과정을 통해서도 분쟁이 해결되지 않은 경우, 민사법원 또는 행정법원에 과태료 부과나 시정명령 등을 구하는 소송을 제기할 수 있다.

3. 내용에 따른 분류

통상 법원이 제공할 수 있는 구제방법으로는 손해배상, 원상회복, 강제조치, 확인판결 등이 있으며 강제조치에는 금지명령이나 이행명령 등이 포함된다. 그러나 사법권을 가지지 않는 개인정보보호기구가 제시할 수 있는 구제는 그 내용 및 효력에 있어 한계가 있다. 따라서 이하에서는 개인정보보호기구가 행할 수 있는 구제방법을 선언적 구제, 교정적 구제, 보상적 구제로 나누어 살펴보도록 하겠다.[341]

340) Raymond Tang, 2002

가. 선언적 구제

먼저, 선언적 구제란 개인정보침해의 신고 또는 고충처리의 의뢰 등이 있을 때 개인정보보호기구가 제반 개인정보보호법령이나 개인정보보호원칙을 통해 위법여부를 판단하여 자신의 이름으로 법위반이 있음을 선언 또는 확인해주는 것이다. 물론 시정명령 등과 같은 조치는 법위반사실을 확인하였음을 전제로 하는 것이나, 여기서 말하는 선언적 구제는 개인정보보호기구가 양 당사자간 분쟁이 있는 사건에 대해 판단하여 어느 한쪽의 손을 들어주는 것을 의미한다. 따라서 구체적인 보상을 하도록 권고하거나 조정안을 제시하지는 않지만 법위반여부에 대한 판단을 함으로써 분쟁을 해결토록 유도하는 역할을 한다.

여기에는 개인정보보호기구가 의견을 표명하거나 권고하는 것과 같은 비공식적인 방법은 물론, 공식적으로 법위반이 있음을 선언하는 결정도 포함된다. 전자에 해당되는 경우가 캐나다와 뉴질랜드, 독일 등 개인정보 피해구제의 기능을 하는 대부분의 개인정보보호기구가 해당된다. 이러한 기구들은 피해구제신청이 접수된 사건에 대하여 사실조사 및 심사를 거쳐 법령이나 개인정보보호원칙 위반의 사실이 있는지를 판단하여 당사자에게 의견을 표명함으로써 간접적으로 법위반이 있음을 선언 또는 확인하고 있다. 한편 호주는 프라이버시법 제52조에 따라 개인정보처리자가 법률 또는 개인정보보호원칙을 위반하는 행위를 하였음을 공식적으로 선언하는 결정을 내릴 수 있다.

나. 교정적 구제

교정적 구제란 개인정보보호기구가 계속적인 개인정보침해행위에 대하여 중지명령, 원상회복명령, 금지명령 등과 같은 행정명령을 내리거나 과

341) Paul Roth, *"Remedies For Personal Data Infringements : The New Zealand Model"*, 2002 International Conference on Personal Data Protection - Personal Data Protection in the Digital Age -,Seoul, Korea, 2002

태료를 부과함으로써 피해구제를 도모하는 방법이다. 이러한 교정적 피해구제의 범위를 넓게 보면, 강제적 효력이 있는 행정명령 외에도 일정한 조치를 취할 것을 요구하는 시정권고도 포함시킬 수 있다. 그러나 엄격한 의미에서는 강제적 효력이 뒷받침된 이행고지 또는 시정명령, 과태료 부과 등을 교정적 피해구제를 위한 수단으로 볼 수 있을 것이다.

다. 보상적 구제

보상적 구제방법은 개인정보보호기구가 분쟁이 있는 사건을 조사·검토하여 법위반여부를 판단하며 구체적인 경제적·정신적 피해가 있는 경우 이를 보상토록 권고하거나 조정안을 제시함으로써 피해구제를 도모하는 방법이다. 호주, 뉴질랜드, 캐나다 등과 같이 소송외적 분쟁해결방법을 통해 민사적 피해구제의 역할도 적극적으로 수행하고 있는 국가들의 개인정보보호기구는 침해자의 위법행위로 인하여 경제적·정신적 피해가 발생한 경우, 이에 대한 의견을 당사자에게 알리고 화해와 조정 등의 방법으로 보상을 권고하고 있다. 반면에 우리나라의 분쟁조정위원회는 사건별로 피해자가 입은 경제적·정신적 피해를 고려하여 피해배상액을 결정하여 조정안으로서 제시하고 있다는 점에서 다른 국가들가 다른 특징을 가진다. 민사적 피해구제에 있어 법원에 앞서 신속하고 저렴한 피해구제방법을 제공할 필요가 있다는 점에서 개인정보보호기구가 소송외 분쟁해결제도의 일환으로 이러한 구제방법을 활용하는 것은 의미가 있다. 다만, 이는 분쟁당사자의 재판을 받을 권리의 침해가능성을 저해하지 않는 한도 내에서 이루어져야 할 것이다. 아래는 각국의 개인정보보호기구이 행하는 피해구제의 내용을 위와 같이 구분하여 표로 비교하여 본 결과이다.

［표 5-13］ 피해구제 내용에 따른 분류

국가	기구명	선언적 피해구제	교정적 피해구제	보상적 피해구제
영국	정보커미셔너	○	○	×
	정보법원	○	○	○
프랑스	정보자유위원회	○	○	×
독일	연방정보보호청	○	×	×
스웨덴	정보조사원	○	○	×
미국	FTC	○	○	×
캐나다	프라이버시커미셔너	○	×	○
호주	프라이버시커미셔너	○	○	○
뉴질랜드	프라이버시커미셔너	○	×	○
	인권법원	○	○	○
홍콩	프라이버시커미셔너	○	○	×
일본	주무대신	×	○	×
한국	개인정보분쟁조정위원회	○	×	○*
	정보통신부	×	○	×

※ ○* : 피해배상액을 결정하여 조정안으로 제시하는 경우를 의미

제 6 장 개인정보피해구제제도 개선방안

본 연구는 국내외의 개인정보피해구제제도의 현황을 파악하고 이를 상호 비교해 보는 과정을 통해 궁극적으로는 국내 개인정보피해구제제도가 선진화될 수 있는 방안을 모색해보고자 하는 목적을 가지고 있다. 이전 장에서는 각국의 개인정보피해구제제도를 유형화하여 각각에 해당되는 법제도, 개인정보보호기구, 개인정보보호기구의 기능 및 역할, 피해구제 절차 및 방법 등을 분류·비교하여 보았다. 특히 이러한 과정은 국내 개인정보피해구제제도는 어느 정도의 위치를 차지하고 있는지, 해외 주요국과 비교해보았을 때 개인정보보호 및 피해구제의 수준은 어느 정도인지, 무엇에 초점을 맞추고 있는지 등 그 현실을 파악하고자 한 것이었다. 즉, 지금까지의 작업이 국내외 개인정보피해구제제도의 현황을 파악하고 상호 비교하는 작업이었다고 한다면, 본 장에서는 국내 제도가 다른 국가의 피해구제제도에 비해 부족한 점 또는 보다 앞서나가고 있는 점 등을 분석하고 외국의 개인정보피해구제제도가 국내 제도에 시사하는 점 등을 통해 국내 개인정보피해구제제도의 개선방안을 도출하는 작업에 초점을 맞추고자 한다.

제 1 절 개인정보보호법

1. 개인정보보호법제의 문제점

우리나라의 개인정보보호 법제도가 가지는 대표적인 특징은 각 영역별로 개별법에서 개인정보보호와 관련된 규정을 두고 있다는 것이다. 즉, 공공, 민간, 전자상거래, 통신, 의료, 금융 등 각 분야별로 개인정보에 관

한 법률이 제정되어 있거나 관련 조항이 포함되어 있다. 이 중 대표적인 개인정보보호 관련 법률로 제시할 수 있는 것으로는 「공공기관의개인정보보호에관한법률」과 「정보통신망이용촉진및정보보호등에관한법률」, 「신용정보의이용및보호에관한법률」이 있다. 또한, 이 외에도 제3장 〔표 3-1〕에서 볼 수 있는 것처럼, 「금융실명거래및비밀보장에관한법률」을 비롯하여 「통신비밀보호법」, 「전자상거래등에서의소비자보호에관한법률」 등이 개인정보보호와 관련된 법률로 인용되고 있다. 이처럼 우리나라의 경우 개인정보와 관련된 법규정이 여러 법률에 산재되어 있는데, 개인정보 관련 규정이 여러 법률에서 개별적으로 존재하고 있기 때문에 통일적인 개인정보보호원칙에 입각하여 국가적 차원에서 개인정보정책을 수립·시행하기 어려운 문제점을 안고 있다. 우리나라 개인정보보호법제가 안고 있는 문제점은 아래와 같다.

첫째, 우리나라는 통일적인 개인정보보호원칙이나 법규범이 없기 때문에 개별적인 개인정보관련 법률규정이 존재하지 않은 영역에서 수집·이용되는 개인정보는 법적으로 보호받을 수 없는 사각지대가 발생할 수 있다. 예를 들어 부동산중개업소, 도서·비디오대여점, 이·미용실, 패스트푸드점, 슈퍼마켓 등의 오프라인 사업자는 회원제를 운영하거나 할인카드 등을 발급하면서 상당히 많은 개인정보를 고객으로부터 수집하여 이용하고 있지만, 현실적으로 이러한 개인정보처리를 규율할 법체계가 미비한 상황이다. 그러므로 현재의 입법체계는 새로운 기술의 등장 또는 변화하는 사회상에 따라 갑자기 개인정보 침해 문제가 제기되는 경우에는 반드시 그에 해당하는 법률 규정을 포함시켜야만 보호대상으로 삼을 수 있게 되어 있는데, 법률의 제정이 사회의 변화를 항상 충실히 반영하고 있지는 못하기 때문에 법적 보호와 현실의 간격이 커질 밖에 없는 한계가 있다.

둘째, 우리는 흔히 개인정보보호법이라는 용어를 많이 사용하고 있지만 우리나라에는 실질적으로 '개인정보보호법'이라고 말할 수 있는 법률이 몇 안 된다. 엄격한 의미에서 개인정보보호법이라고 하기 위해서는 입법목적이 개인정보보호와 관련이 있어야 하고 해당 영역에서 개인정보를 취급하는 자가 어떠한 방법으로 무엇을 기준으로 삼아 개인정보를 처리

하여야 하는지를 규정하고 있어야 할 것이나, 이러한 기준에 부합된다고 볼 수 있는 법률로는 공공기관개인정보보호법이나 정보보호법, 신용정보보호법 등을 언급할 수 있을 뿐이다. 따라서 개인정보취급자 또는 이용자가 업무상 지득한 정보의 '비밀누설의무' 조항을 두고 있을 뿐인 의료법, 변호사법, 보험업법 등의 법률들은 엄밀한 의미에서 개인정보보호법이라 말하기 어려운 점이 많다. 따라서 그렇지 않은 영역에서는 일반적인 의미에서 개인정보 또는 타인의 비밀을 누설하지 않아야 한다는 정도의 금지규정만 두고 있을 뿐 실질적으로 법이 그 기준이나 대안을 제시하고 있지 않아 충분한 개인정보보호 체계를 갖추기 어렵다는 문제가 있다.

마지막으로 개인정보보호법이라 일컬어지고 있는 법률들의 경우에도 실질적으로 관련되는 영역에 모두 적용되는 것이 아니고 그 중에서도 특정한 조건을 두어 적용범위를 한정시키고 있을 뿐 아니라, 그와 같은 법률 상호간에도 일관성이 없다는 문제점이 있다. 예를 들어 공공기관개인정보보호법은 공공기관에서 수집・이용・보관・공동 활용하는 모든 개인정보의 처리에 대하여 적용되기 보다는 특별하게 컴퓨터에 의해 전산처리되는 개인정보에 초점을 맞추고 있어 다소 그 적용범위가 한정되고 있다고 볼 수 있다. 정보보호법도 마찬가지이다. 동법도 원칙적으로 정보통신서비스제공자와 거래관계가 있는 이용자간의 개인정보처리에만 적용된다. 또한 공공기관개인정보보호법, 정보보호법, 신용정보보호법 상호간에도 그 내용이 상이하고 일관성이 부족하다. 이를테면 정보보호법의 경우 비교적 OECD 가이드라인의 개인정보보호 8원칙 및 EU 지침의 여러 기본 원칙들을 잘 반영하고 있는 반면, 공공기관개인정보보호법과 신용정보보호법은 그렇지 못한 점이 많다. 예를 들면, 수집된 개인정보의 제3자 제공에 대한 명확한 한계나 제한 규정을 두고 있지 않아 사실상 개인정보가 유통되거나 무제한 활용될 위험을 내포하고 있어 정보주체의 권리가 상당수 배제되는 결과를 낳고 있다. 물론 개인정보보호의 수준은 개개 영역별로 그 특성이나 우선되는 가치, 처리되고 있는 개인정보의 종류나 민감성의 정도 등에 따라 달라질 수밖에 없기 때문에 차별을 두는 것은 어찌 보면 너무나 당연한 일이다. 예를 들어, 신용정보보호법이 신용정보

의 보호만을 너무 강조하여 개인정보의 수집 및 이용, 제3자 제공시 모두 정보주체의 동의를 일일이 받도록 한다거나 제3자 제공을 엄격히 금지하는 등 OECD 개인정보보호원칙을 엄격하게 적용한다면, 신용정보업 등의 업무수행을 사실상 불가능하게 하여 결과적으로 신용거래 등 상거래에 부담을 주는 결과를 낳을 수도 있을 것이다. 그러나 원칙을 벗어나는 예외적인 규정들은 언제나 목적달성을 위해 필요한 최소한의 한도로 하여야 할 필요가 있다. 그리하여 예외가 원칙적인 사항을 능가하고 우선시되어서는 안 되도록 할 필요가 있으나, 우리나라의 개인정보보호법제는 개인정보 처리의 원칙이나 방법, 기준에 대하여 규정하고 있는 법률의 경우에도 서로 그 내용이 달라 개인정보보호를 위한 통일된 원칙이라고 부를 만한 것이 없는 상황이다. 그 뿐 아니라, 개인정보의 수집・이용에 관한 기준도 각기 다르고 처벌의 정도나 민사책임원칙도 다르다.

2. 개인정보보호기본법의 제정

우리나라의 개인정보보호법제가 가지는 문제점과 한계를 극복할 수 있는 방안으로 제시되고 있는 것이 바로 개인정보보호기본법의 제정이다. 최근 국내에서는 학계와 시민단체를 중심으로 이러한 개인정보보호기본법에 대한 논의가 한창인데, 여기서 개인정보보호기본법이란 세부적인 영역별로 개인정보 관련 규정을 두는 것이 아니라, 개인정보보호에 관한 기본원칙, 정보주체의 권리 및 정보처리자의 의무에 관한 사항, 국가 등이 개인정보보호를 위해 하여야 할 책무, 개인정보보호기구에 관한 사항 등 모든 영역에 적용될 수 있는 개인정보에 관한 일반적인 사항을 단일 법률을 통해 규정함으로써 하나의 일관성 있는 기준을 제시하자는 의미로 이해된다.

개인정보보호기본법에 대한 논의는 두 가지 방향에서 접근할 수 있는데, 하나는 공공분야와 민간분야를 모두 포괄하는 그야말로 단일한 개인정보보호기본법을 제정하는 것이고 다른 하나는 공공부문과 민간부문에 적용

되는 각각의 개인정보보호기본법을 제정하는 것이다. 일반적으로 개인정보보호기본법이라고 하면 전자를 의미하는 것으로 받아들여지고 있는 것이 사실이고 학계와 시민단체에서 이루어지고 있는 논의도 전자를 중심으로 하고 있다. 그러나 공공과 민간의 구분 없이 모든 영역에 적용되는 기본법을 만드는 것이 이상적일 수는 있지만, 우리나라의 법제현실이나 개인정보의 수집목적 및 방법 등에서 공공부문과 민간부문이 가지는 여러 차이점을 볼 때 양자를 구분해서 이원적으로 각각 고유의 특성에 맞는 기본법을 제정하는 것도 현실적인 대안이 될 수 있다. 즉, 우리나라의 법제는 적용범위의 한계가 있기는 하나 사실상 공공기관개인정보보호법과 정보보호법이 공공분야와 민간분야에서 각각 개인정보보호에 관한 기본법으로서의 기능을 하고 있는 것으로 볼 수 있는데, 현재 주로 문제가 되고 있는 적용범위, 피해구제 방법, 처벌규정에 관한 규정을 전면 정비하여 각각의 법률을 기본법으로 격상시키는 것도 가능한 방법이 될 수 있다.

실제로 캐나다가 이러한 입법체계를 보여주고 있는데, 공공부문에서는 「프라이버시법」을 제정하고 있고 민간부문에서는 「개인정보보호및전자문서에관한법률」을 제정하여 시행하고 있다. 이는 공공부문과 민간부문의 개인정보처리가 가지는 각기 다른 특성을 반영한 것으로 볼 수 있는데, 이러한 구분은 공공과 민간을 구분하지 않은 통합형 개인정보보호법을 가진 국가에서도 나타나고 있다. 예를 들어, 독일, 스페인과 같은 경우에는 기본법 내에서 장을 달리하여 공공부문과 민간부문의 개인정보처리를 각각 개별적으로 규정하고 있는데, 이는 공공부문과 민간부문은 개인정보의 수집단계에서부터 이용, 보유, 제3자 제공, 법위반에 대한 시정절차나 처벌정도, 개인정보보호기구가 관여할 수 있는 정도 등에 있어 차이를 둘 수밖에 없는 각각의 특성을 가지고 있음을 보여주는 것이라 할 것이다. 또한 프랑스, 영국, 스웨덴 등과 같이 개인정보보호에 관한 단일한 기본법을 두고 있는 대부분의 유럽 국가들도 기본법에서는 기본원칙이나 권리・의무, 개인정보보호기구의 기능 및 권한, 처벌규정 등 아주 기본적인 사항만을 규정할 뿐, 공공분야에서 행정목적으로 처리하는

개인정보나 신용정보, 정보통신분야에서 처리하는 개인정보, 의료정보, 교육정보 등에 대해서는 하위법률이나 별도의 법률을 제정하여 상세한 사항을 규정하고 있다. 이렇듯 공공과 민간을 구분하지 않고 단일한 개인정보보호기본법을 가진 국가들도 실질적으로 그 입법체계를 살펴보면 공공부문과 민간부문은 사실상 구분하고 있는 것이 일반적인 바, 이미 공공부문과 민간부문에서 실질적으로 기본법적 기능을 담당하고 있는 법률이 존재하고 있는 우리 법제에서는 이러한 현실을 인정하고 제도적인 개선책을 강구하는 것이 보다 효과적일 수도 있다.[342]

한편 기본법 제정의 논의에서 공공과 민간의 통합이냐 구분이냐의 여부보다 더욱 중요한 것은 개인정보보호법이 기본법적 성격을 가지기 위해 포함하여야 할 규정이 무엇인지를 살피는 것이다. 생각건대, 하나의 개인정보보호법이 기본법적 성격을 가지기 위해서는 OECD 프라이버시 8원칙 및 EU 개인정보보호지침에서 규정하고 있는 내용을 반영하여야 할 것이다. 그러므로 무엇보다도 정보주체의 권리 및 정보처리자의 의무에 관한 사항을 명시적으로 규정하는 것이 필요하다. 이러한 내용은 개인정보보호원칙의 형태로 규정되기도 하는데, 영국, 캐나다, 호주, 뉴질랜드, 홍콩, 스웨덴의 개인정보보호법이 그러하다. 개인정보보호 기본원칙을 규정하게 되면, 개인정보를 취급할 때 어떠한 목적 범위 안에서 무슨 방법으로 처리할 것인지를 보다 명확하게 제시할 수 있다는 장점이 있다. 또한 개인정보보호법은 실질적으로 개인정보의 침해예방 및 피해구제를 위한 역할을 담당할 수 있는 개인정보보호기구의 설치 및 기능과 권한, 법위반시 처벌규정 등과 같은 절차적 보호규정을 포함하여 개인정보보호법의 실현을 보장할 수 있어야 한다.

---

342) 우리나라의 개인정보보호법제 개선에 있어 일본의 예를 참고할 수 있을 것이다. 일본은 올 5월 개인정보보호법을 제정하였는데, 동법은 공공과 민간분야에 모두 적용되는 개인정보보호 기본이념, 국가 및 지방자치단체의 책무, 주무대신의 권한 등을 규정하여 기본법적 성격을 갖추고 있다. 그러나 한편으로 동법은 민간분야의 개인정보취급사업자가 준수하여야 할 사항을 중점적으로 규정하고 있어 민간분야의 개인정보보호법으로도 볼 수 있다. 이러한 입법형식은 일본이 기존에는 민간분야에 적용되는 개인정보보호법을 가지고 있지 못하여 이를 새롭게 제정하면서, 공공부문과 민간부문에 모두 적용되는 몇 가지 일반적 사항만을 추가한 것으로 볼 수 있다.

제 2 절 개인정보보호 행정체계

실체법적 측면에서 개인정보와 관련된 권리·의무 등에 관한 사항을 규정하는 것 외에도 강조될 수 있는 것이 개인정보보호법에서 규정하고 있는 사항을 집행하고 부당한 개인정보침해로 인한 피해를 구제할 수 있는 역할을 담당하는 개인정보보호기구가 존재하는지 여부이다. 이하에서는 우리나라의 개인정보보호기구가 어떠한 형식으로 존재하는지를 살펴보고 그 문제점을 분석하여 개선방안을 도출해보고자 한다.

1. 개인정보보호 행정체계상의 문제점

현재 우리나라에서 법정 개인정보보호기구로 설치된 기구로는 공공기관개인정보보호법 제20조에 의해 설립된 개인정보보호심의위원회와 정보보호법 제33조에 의해 설립된 개인정보분쟁조정위원회가 있다. 따라서 우리나라에서 엄격한 의미의 '개인정보보호기구'라고 할 만한 기구로는 개인정보보호심의위원회와 개인정보분쟁조정위원회를 들 수 있다. 그러나 현실적으로 우리나라에서 개인정보보호의 역할을 담당하거나 권한이나 관할대상의 측면에서 관련이 깊은 개인정보보호기구는 〔표3-4〕에서도 볼 수 있듯이 다양하다. 공공기관개인정보보호법과 정보보호법을 관장할 책임이 있는 행정자치부와 정보통신부는 물론이고, 국가인권위원회, 한국소비자보호원, 금융감독위원회 등이 모두 개인정보보호의 역할을 담당하고 있으므로 넓은 의미에서는 이러한 기구들을 모두 개인정보보호기구로 포함시킬 수도 있을 것이다. 이렇듯 우리나라는 여러 기구에서 개인정보보호의 역할을 수행하고 있는데, 이 중 개인정보보호심의위원회와 개인정보분쟁조정위원회를 제외한 다른 기구들은 개인정보보호를 전담하여 수행하는 기구가 아니다.

우리나라에 여러 개인정보보호기구가 존재하는 이유는 개인정보와 관련된 법규정이 여러 법률에 산재되어 있을 뿐 아니라 포괄적인 관할

대상과 강력한 권한과 위상을 가진 개인정보보호기구가 없기 때문인 것으로 생각된다. 이로 인해, 우리나라에는 개인정보정책을 국가적 차원에서 책임있게 추진할 책임주체가 없는 상태이다. 엄격한 의미에서의 개인정보보호기구인 개인정보보호심의위원회와 개인정보분쟁조정위원회도 각각의 관할 영역을 총괄하여 책임있게 개인정보침해예방에서부터 피해구제까지 모든 정책을 결정·추진해나갈 수 있는 권한과 위상을 갖고 있지 못하며, 단지 개인정보에 관한 심의기구와 분쟁조정기구로 인식되고 있을 뿐이다.

2. 개인정보보호 전문·전담기구의 설립

오늘날 개인정보보호기구의 필요성과 중요성에 대해서는 전 세계적인 공감대가 형성되어 있는 상황이다. 특히 EU 지침 제28조는 각 회원국에게 해당 영역의 개인정보처리를 감시하고 조사할 책임이 있는 공공기구로서 부여된 기능을 수행함에 있어 완전한 독립성을 가진 개인정보보호기구의 설치를 요구하고 있다. 이에 EU 회원국 각국은 물론 호주, 뉴질랜드, 홍콩, 캐나다 등 대부분의 국가들은 개인정보보호 기능을 수행하는 전담기구를 설치하여 운영하고 있다.

우리나라의 개인정보보호기구도 이러한 세계적 추세에 맞춰 여러 기관에 분산된 개인정보보호기능을 하나로 통합하여 수행하는 전문기관이 설립될 필요가 있다. 그러나 통합 개인정보보호기구가 반드시 공공부문과 민간부문을 함께 관장할 필요는 없다고 본다. 공공부문과 민간부문은 근본적으로 개인정보 침해의 태양이나 그 과정이 상이할 뿐 아니라, 피해구제 수단 및 방법과 그 절차도 다를 수밖에 없다. 또한 공공부문에서는 정부조직법상 개인정보보호기구가 가진 행정체계상 위치와 권한이 중요하게 작용할 수 있기 때문에, 무엇보다도 국가기관 상호 간의 견제가 가능한 고도의 독립된 국가기관이 개인정보보호의 기능을 수행하여야 할 필요가 있다. 반면에 민간부문에 있어서는 국가기관과 국민간의 관계이기

때문에, 다른 국가기관과의 권력관계가 그리 큰 작용을 하지는 않으므로 보다 유연한 조직을 통해서 개인정보보호의 역할을 담당케 하는 것이 바람직하다. 특히 우리나라는 다른 국가들처럼 공공부문을 시작으로 개인정보보호기구가 발달하여 민간부문까지 확대된 것이 아니고, 이와는 정반대로 민간부문과 공공부문이 각기 별도의 과정을 통해 발전해왔다는 특성을 가진다. 따라서 공공과 민간의 영역에서는 서로 상이한 개인정보보호기구가 있고 주로 수행하는 기능이나 권한, 실질적인 운영상황이 모두 상이하다. 무엇보다도 공공부문에서는 개인정보보호심의위원회가 거의 운영되고 있지 못하고 형식화된 기구에 불과하여 사실상 개인정보보호법을 집행할 기구가 없다고도 볼 수 있다. 따라서 이미 민간부문에서는 개인정보분쟁조정위원회가 개인정보침해 문제를 적극적으로 다루어 피해구제의 역할을 수행하고 있는 상황에서 이를 반드시 공공부문과 통합하여야 할 필요는 없고, 양자를 구분하여 현재 존재하고 있는 개인정보보호기구 및 제도를 개선하는 방향으로 나아가는 것이 바람직할 것이다.

한편 개인정보보호 전문·전담기구가 어떠한 형태로 설립되어야 하는지도 검토해볼 필요가 있다. 앞서 ［표 5-5］에서 살펴본 바와 같이 오늘날 각국 개인정보보호기구의 형태는 다양하지만, 크게 위원회 형태와 독임제 형태로 나누어 볼 수 있다. 프랑스의 CNIL이 대표적인 위원회 형태의 개인정보보호기구이며, 영국, 호주, 뉴질랜드, 홍콩, 캐나다 등이 '커미셔너'라 불리는 독임제 형태의 개인정보보호기구를 운영하고 있다. 그러나 개인정보보호기구가 독임제형이라고 하더라도 중요한 개인정보정책을 순수하게 커미셔너가 단독으로 결정하는 경우는 거의 없고, 내·외부에 자문기구나 심의기구를 두고 운영하는 형태가 대부분이다. 예를 들어, 호주의 프라이버시커미셔너는 프라이버시자문위원회를 통해 프라이버시와 관련된 중요한 정책결정사항이나 사회적 이슈가 되고 있는 문제들에 대한 자문을 구하고 있으며, 홍콩 역시 개인정보자문위원회와 기술상설자문위원회를 운영하고 있다. 이는 개인정보와 관련된 인식이나 연구가 아직은 발달과정 중에 있어, 중요한 개인정보정책을 실시하거나 결

정을 내리기 위해서는 사회적 합의를 도출하는 절차가 반드시 필요하기 때문이다. 이런 점에서 다수의 의견을 반영할 수 있고 다양한 분야에서 활동하는 위원들이 참여하기 때문에 전문성을 확보할 수 있는 위원회 형태의 개인정보보호기구의 장점이 부각될 수 있을 것이다.

제 3 절 개인정보보호기구의 기능·권한

개인정보보호기구가 실질적으로 개인정보보호법을 집행하고 개인정보보호의 역할을 다하기 위해서는 개인정보에 관한 전반적인 기능을 모두 수행할 수 있어야 하고, 이를 위한 권한이 확보되어야 한다. 아래에서는 우리나라의 개인정보보호기구가 현재 수행하고 있는 기능과 권한상 한계와 문제점을 분석하고 이에 대한 개선방안을 생각해본다.

1. 개인정보보호기구의 기능·권한상의 문제점

우리나라에서 개인정보보호의 역할이 여러 기관에 분산되어 있다는 것은 일견 각각의 기구들이 통합적인 개인정보보호 기능을 수행하고 있지 못하다는 것을 보여준다. 법률상 개인정보보호기구로 설립된 개인정보보호심의위원회 및 개인정보분쟁조정위원회도 기본적으로 그 기능이 각각 개인정보보호 법률이나 정책적 사안에 대하여 '심의'하는 역할과 개인정보에 관한 분쟁을 '조정'하는 역할로 한정되어 있다. 물론, 민간부문에서는 개인정보분쟁조정위원회와 정보통신부 그리고 한국정보보호진흥원(개인정보침해신고센터)가 유기적으로 협조하여 개인정보침해예방 및 피해구제 등의 기능을 수행하여 어느 정도 성과를 보여주고 있으나 한계가 있음은 부인할 수 없다. 또한, 이렇게 기능이 분산되어 있다보니 각각의 개인정보보호기구들이 행사할 수 있는 권한에도 제한이 따른다.

아래에서는 〔표 5-11〕에서 분류한 각국 개인정보보호기구의 권한을 국내의 공공부문과 민간부문의 대표적인 개인정보보호기구가 가지는 권한과 대비시켜 비교해본 내용이다.

〔표 5-14〕 한국의 개인정보보호기구의 기능·권한 비교

권한		민간부문			공공부문	
		정보통신부	KISA	개인정보분쟁조정위원회	행정자치부	개인정보보호심의위원회
지침 제정		○	×	×	○	△ (심의·의결)
자문		○	×	○	○	×
정책심의·의결		×	×	×	×	○
정책 연구		○	○	×	○	×
모니터링		○	○	×	○	×
상담·고충처리		○	○	×	×	×
사실조사	자료제출 요구권	○	○	△ (요청권)	○	×
	당사자소환·심문권	×	×	△ (출석요구권)	×	×
	증인소환·심문권	×	×	△ (협조요청)	×	×
	정보시스템 접근조사권	○	○	×	○	×
피해구제	화해, 합의권고	×	×	○	×	×
	분쟁조정	×	×	○	×	×
	준사법적 결정	×	×	×	×	×
	시정권고(의견)	○	×	×	○	×
규제조치	이행고지	×	×	×	×	×
	시정명령	○	×	×	×	×
	과태료부과	○	×	×	×	×
	위법사실통보	○	○	○	×	×
	소제기	×	×	△ (소송지원)	×	×

국내의 경우, 개인정보보호 전담기구라 할 만한 개인정보보호기구가 없기 때문에 각각의 기관이 행사할 수 있는 권한도 다소 제한적이다. 정보통신부와 행정자치부는 각각 공공기관개인정보보호법과 정보보호법을 관장하고 있는 행정기관이기 때문에, 해당 법률의 시행에 필요한 지침을 제정하여 고시하거나 실태조사[343]를 행하는 등의 기능을 하고 있다. 그

343) 정보보호법 제55조 ; 공공기관개인정보보호법 제18조.

러나 정보통신부는 민간부문의 개인정보처리실태를 조사·감독하여 위법사항이 발견될 경우 시정권고, 시정명령, 과태료 등 행정적 제재조치를 취할 수 있으나[344], 행정자치부는 기본적으로 공공부문의 개인정보처리 상황을 총괄할 뿐 직접적인 지도·감독은 각 관계행정기관의 장이 맡아하고 있다. 따라서 행정자치부는 필요한 경우 공공기관의 장에게 개인정보보호에 관한 의견을 제시하거나 권고하는 역할에 그칠 뿐이다.[345]

또한 공공부문과 민간부문에 각각 설치된 법정 개인정보보호기구인 개인정보보호심의위원회 및 개인정보분쟁조정위원회의 기능과 권한도 다소 제한적이다. 개인정보보호심의위원회는 공공부문의 개인정보처리에 관한 정책이나 제도개선, 공공기관간 의견조정 등에 관한 사항을 심의·의결하는 역할을 맡고 있을 뿐, 직접 개인정보침해행위를 한 기관이나 당사자에게 시정을 권고하거나 의견을 제시하는 등 사후적 피해구제의 역할을 담당하지는 않고 있다. 또한 업무를 담당할 전문 인력이나 예산도 전무하며 위원회의 실질적인 운영을 지원하는 사무국도 없는 상태이다. 개인정보분쟁조정위원회 역시 기능의 초점이 사후적 피해구제에 맞추어져 있어 개인정보침해로 인해 피해를 접수받아 사실조사를 하고 분쟁조정을 함으로써 당사자간 원만한 피해구제가 이루어지도록 하는 역할을 주로 담당하고 있을 뿐이며, 교육·홍보기능, 법률 및 기술자문, 정책연구 등은 KISA(개인정보침해신고센터)가 맡고 있다. 또한 KISA가 개인정보침해와 관련된 상담 및 고충처리를, 개인정보분쟁조정위원회가 분쟁조정을 맡고 있어 개인정보피해구제기능도 중복되고 있다.

2. 개인정보보호기구에 통합적 기능과 권한 부여

전문적으로 개인정보보호 기능을 전담하여 수행하는 기구를 설립한다고 할 때, 이러한 기구가 본래의 목적을 원활히 달성할 수 있기 위해서는

344) 정보보호법 제55조제3항 및 제67조.

345) 공공기관개인정보보호법 제19조.

무엇보다도 개인정보보호기구의 기능 및 권한에 지나친 제약이 있어서는 안 된다. 앞 절에서 제언한 바와 같이 공공부문과 민간부문의 개인정보 처리를 각각 관할할 수 있는 개인정보보호기구를 확립한다면, 각각의 기구는 해당 영역의 개인정보보호를 위한 사전 침해예방적 기능부터 사후 피해구제의 기능까지 총괄하여 담당할 수 있어야 한다. 물론 공공부문과 민간부문의 특징에 따라 개인정보보호기구의 세부적인 기능이나 권한상의 차이는 있을 수 있지만, 기본적으로 현재 분산되어 있는 개인정보보호 기능을 한 단계 높은 차원에서 통괄하여 시행할 수 있어야 할 것이다.

앞서 각국의 개인정보보호기구가 수행하는 주요 기능을 정리한 〔표 5-8〕의 내용은 우리나라의 개인정보보호기구가 어떠한 기능을 수행해야 하는 것인지를 판단하는데 좋은 기준이 될 수 있을 것이다. 생각건대, 개인정보보호기구는 우선 국민, 정부, 사업자, 의회 등을 대상으로 한 정보제공자의 역할을 충실히 담당하여야 한다. 따라서 개인정보와 관련된 지침제정, 정보주체의 권리와 정보처리자의 의무에 대한 상담 및 교육, 개인정보와 관련된 정책 및 법률 자문 등 총체적인 정보제공의 역할을 할 수 있어야 한다. 또한 개인정보보호기구는 개인정보보호를 위한 기준을 정립하고 정보처리자의 자율적인 개인정보보호 환경이 정착되도록 도와주며, 이를 위해 필요한 교육·홍보활동을 실시하는 등 각종 침해예방활동을 펼칠 수 있는 기능이 부여되어야 한다. 그러나 오늘날의 개인정보보호기구는 단순 침해예방적 활동을 하는 것에 그치지 않고 보다 적극적으로 개인정보침해 피해자의 권익을 보호하고 구제하는 사후적 피해구제의 기능을 수행할 수 있어야 한다. 특히 이러한 피해구제의 기능은 개인정보침해 피해자 또는 일반 국민이 누구나 쉽게 접근하여 이용할 수 있도록 소송외적 분쟁해결제도를 적극 활용함으로써 더욱 효과적으로 수행될 수 있을 것이다. 우리나라의 경우 민간영역에서는 어떠한 다른 국가보다도 개인정보보호기구의 분쟁조정제도가 활성화되어 있는 바, 이러한 제도를 더욱 발전시킬 수 있을 것이며 공공부문에서도 참고할 수 있을 것이다. 다만, 추가적으로 고려되어야 할 것은 분쟁조정제도가 신속하고 간편하게 분쟁을 해결할 수 있다는 장점이 있지만 강제력이나 구속력이

없어 당사자의 합의가 없는 경우에는 소송에 의하지 않고서는 실질적인 구제방법이 없다는 점이다. 따라서 이를 뒷받침할 수 있는 시정권고권이나 시정명령권 등 행정조치를 취할 수 있는 권한이 부여될 필요가 있다.[346] 그러나 개인정보보호기구의 법적 지위를 현재와 같이 반관반민(半官半民) 형태로 유지할 경우 현실적으로 시정명령권, 과태료 부과권 등을 직접 부여하기는 어렵기 때문에, 그러한 권한을 가진 행정기관에 대하여 위법사실을 통보하고 징벌을 요구할 수 있는 권한을 행사할 수 있도록 하는 것을 고려하여야 한다.[347] 또한 형사고발조치나 소제기·소송지원의 역할을 적극적으로 담당하여 사후적 관리기능을 수행할 필요도 있다.

346) 외국의 개인정보보호기구들도 대부분 개인정보 관련 민원이나 불만이 접수되면 당사자간의 대화와 타협을 유도하고 알선함으로써 사전 합의가 되도록 하고 있는데, 개인정보처리 등록 취소, 시정권고, 이행고지, 시정명령, 과태료 부과 등의 조치를 취할 수 있는 권한을 보유하고 있는 경우 당사자간 합의에 도달할 수 있도록 사실상 강제할 수 있어 더욱 효율적인 피해구제를 도모할 수 있다고 한다. (Douwe Korff, supra note 311, pp. 207~208)

347) 이와 관련해서는 통신위원회의 경우를 참고할 수 있는데, 정보통신부 장관은 전기통신사업법 제37조 및 제37조의2에 따라 통신위원회의 심의를 거쳐 전기통신사업자의 위법행위에 대한 시정조치 명령이나 과징금 부과 등의 조치를 취할 수 있도록 하고 있다. 따라서 사실상 통신위원회가 사업자의 위법행위에 대한 제재조치를 결정할 수 있는 권한을 가진 것으로 볼 수 있는데, 개인정보보호기구도 최소한 이러한 권한을 부여받아 행사할 수 있어야 할 것이다.

제 7 장 결론

최근 개인정보침해의 증가 현상에 따라 새롭게 강조되고 있는 것이 이러한 개인정보침해를 어떠한 방법과 절차를 통해 구제할 수 있을 것인가 하는 점이다. 법적으로 개인정보보호를 위한 규정을 마련하고 기준을 세우는 것도 중요하지만, 정립된 법적 기준에 맞추어 개인정보가 수집·이용·보유·처리될 수 있도록 필요한 제도적 장치를 마련하여 시행하는 것도 중요하다. 특히 부당한 방법으로 개인정보를 침해하는 행위 또는 개인정보보호법에 위반하여 개인정보를 처리하는 행위로 인하여 피해를 입은 사람들이 자신의 권익을 보호받을 수 있도록 도와주는 제도를 마련하고 확립하는 것은 개인정보보호를 위한 법적 정의를 실현하는 길이라 할 것이다.

본 연구는 이러한 개인정보피해구제제도를 우리나라에서 어떻게 정착하여 활성화시킬 것인가를 고민하고 살펴보기 위한 작업이었다고 말할 수 있다. 이를 위해 먼저 국내와 해외 주요 선진국의 개인정보피해구제제도 현황을 살펴보고 국내·외 제도를 상호 비교하는 과정을 거치면서, 우리나라의 개인정보피해구제제도를 보다 발전시키고 개선할 수 있는 방안으로는 무엇이 있을 것인지 검토해보았다.

현재 우리나라는 공공기관개인정보보호법, 정보보호법, 신용정보보호법 등을 제정·시행하고 있으며 이 외에도 통신비밀보호법, 의료법, 변호사법, 주민등록법, 금융실명제법 등 다양한 법률 속에 개인정보보호 또는 비밀보호와 관련된 규정을 두고 있다. 이 중 공공기관개인정보보호법은 공공부문, 정보보호법은 민간부문, 신용정보보호법은 신용정보 관련 부문에 대하여 규율하는 우리나라의 대표적인 개인정보보호법이라고 말할 수 있다. 그러나 이들 법률은 적용범위에 다소의 제한이 있어 해당되는 모든 영역을 아우르는 기본법적 성격을 가진 것으로 보기는 어렵다. 또한 그 외의 법률들도 일부 조항을 통해 간접적으로 비밀보호의 측면에서 개인정보

보호를 꾀하고 있는 경우가 대부분이어서 그러한 법률을 개인정보보호법이라 칭하기 어렵다. 이렇듯 우리나라는 실체법적 측면에서 살펴볼 때, 개인정보보호법이 완벽하게 정비되어 있다고 보기 어렵다. 이러한 법체계의 불완전성과 불충분 상태로 인하여 사실상 다양한 종류의 많은 개인정보가 법의 부재 상태에서 방치되고 있다고 하여도 과언이 아니다.

이러한 현상은 비단 실체법적 측면에서만 나타나는 것은 아니다. 법적 근거가 없기 때문에 당연히 통합적으로 개인정보를 보호할 수 있는 권한과 역할을 부여받은 전문적인 법정 개인정보보호기구 역시 미비한 상태이다. 개인정보분쟁조정위원회와 개인정보보호심의위원회가 각각 민간영역과 공공 영역에 설립된 법정 개인정보보호기구이지만, 이러한 기구들이 개인정보와 관련된 모든 기능을 전담하여 수행하고 있지는 못하다. 전자는 민간 영역에서는 사실상 명실상부한 개인정보피해구제기관으로서의 역할을 하고 있지만 소송외적 분쟁해결제도를 통한 사후 피해구제에 초점이 맞추어져 있다는 한계가 있으며, 후자는 개인정보와 관련된 정책이나 입법에 대한 중요사항을 심의·의결하는 것을 주된 기능으로 삼고 있고 그나마 활동이 거의 전무하다. 그러므로 우리나라에는 아직 개인정보에 관한 각종 상담, 자문·정보제공, 지침 제공, 민간 자율규제 유도, 정보제공에서부터 소송외적 분쟁해결수단을 통한 피해구제, 시정권고, 시정명령 및 과태료 부과 등의 행정제재 조치, 형사고발, 소송지원 등 일련의 개인정보와 관련된 모든 기능과 역할을 전담하여 수행하는 국민, 의회, 정부, 사업자를 대상으로 한 단일 창구이자 전문 서비스기관이라 할 만한 개인정보보호기구는 갖추어져 있지 않았다고 볼 수 있다.

일반적으로 외국의 개인정보피해구제제도가 우리나라의 제도와 다른 점은 폭넓은 적용범위를 가진 개인정보보호법이 제정되어 있고, 동법에 근거하여 설립된 개인정보보호기구 역시 폭넓은 관할대상과 광범위한 기능·권한을 가진다는 것이다. 그러나 각국의 제도는 그 나라의 법적·사회적·정치적 환경을 바탕으로 자연스럽게 만들어진 것이므로, 우리나라의 환경이나 사회적 배경과 많은 차이점을 보이고 있는 외국의 법·제도를 있는 그대로 수용하는 것은 바람직스럽지 못하다.

우리나라는 현재 공공부문과 민간부문의 개인정보보호체계가 분리되어 있고 그 보호수준도 격차가 심하다. 따라서 현 시점에서 공공부문과 민간부문을 통합하는 법제도를 도입한다고 할 경우, 자칫 민간부문에서 이룬 개인정보보호의 성과마저 퇴색시킬 위험성도 있다. 그러므로 궁극적으로는 공공부문과 민간부문을 통합하는 체계를 지향하더라도 현재로서는 공공부문과 민간부문을 별도로 분리하여 각각의 기본법을 제정하고 이를 집행할 개인정보보호기구를 설립하는 방안이 보다 실현가능성이 있지 않을까 판단된다. 그러나 무엇보다도 중시되어야 할 것은 실질적으로 각 분야의 개인정보처리가 법규범에 어긋남이 없이 적절히 이루어짐으로써 정보주체의 개인정보를 침해하는 일이 없도록 개인정보보호기구의 권한과 역할이 강화되어야 할 것이라는 점이다. 따라서 개인정보보호기구가 상담, 자문, 교육 등 '정보제공자' 또는 '컨설턴트'의 역할을 할 수 있음은 물론 지침 제정 및 입법·정책설립과정에의 참여 등을 통해 일부 '규범설정자'의 역할도 담당할 수 있어야 한다. 또한, 개인정보침해 실태를 조사하고 위법사실에 대하여 제재를 가하는 '규제·감독자'의 역할과 개인정보침해로 인해 발생한 분쟁을 조정하고 해결하는 '조정자'의 역할도 모두 해낼 수 있어야 할 것이다. 특히 우리나라는 개인정보피해와 관련한 분쟁조정제도가 세계 어느 나라보다도 잘 발달되어 있을 뿐 아니라 온라인을 통한 분쟁해결절차와 방법이 활발히 운영되어 신속·간편·공정한 개인정보피해구제를 실현하고 있는 바, 개인정보보호 전문·전담기구는 이러한 분쟁조정제도의 독창성과 장점을 더욱 발전시킬 수 있어야 할 것이다.

참고 문헌

1. 국내문헌

[1] 강경근, “인터넷에서의 개인정보보호”, 「인터넷법률」, 제4호 2001. 1.

[2] 강달천, “프라이버시 보호를 위한 사전적 권한 검토”, 「제2회 워크숍 : 프라이버시 보호 법제, 어떤 모습이어야 하는가?」(연속 워크숍 - 프라이버시 보호법제 개선의 쟁점들), 2003. 8. 21.

[3] 강신원, “B2C 활성화를 위한 개인정보보호제도와 정책방향”, 「개인정보연구」, 제2권 제1호, 2003. 7.

[4] 길준규, “정보보호법의 체계와 그 구제”, 「개인정보연구」, 제1권 제1호, 2002. 12.

[5] 금융감독위원회/금융감독원, “금융감독위원회·금융감독원 소개”, 2002. 3.

[6] 김주환 외, “유네스코한국위원회 기획 정보사회 성찰 시리즈 ① - 디지털 시대와 인간 존엄성”, 나남출판, 2001. 12.

[7] 김현수, “일본의 개인정보 관련 법제 동향과 법률 분석”, IT법 연구회, 2003. 8.

[8] 남광, “소송절차에 의한 소비자분쟁해결”, 「제7회 소비자의 날 기념토론회 자료집」, 2002.

[9] 박종찬, “정보화시대의 개인정보보호방안 연구”, 「인터넷법률」, 제4호, 2001. 1.

[10] 박훤일, “개인정보침해구제제도의 발전방향”, 「디지털시대의 개인정보보호와 과제」, 2002.

[11] 백병성, “소비자분쟁조정의 역할과 효율적인 조정기구 운영”, 「소비자문제연구」, 제23호, 2000.

[12] 서경대학교(정영화 외), “개인정보보호 감독기구 도입을 위한 법제도 개선방안연구”, 한국정보보호센타, 2000. 11.

[13] 신군재, “ADR을 통한 전자상거래 분쟁 해결방안에 관한 연구 : 중재제도의 활용을 중심으로”, 「국제상학」, 제17권 제2호, 한국국제상학회, 2002. 8.

[14] 심재훈, “미국의 프라이버시 보호와 침해 유형”, 「세계의 언론법제」, 제12호, 2002. 12.

[15] 원숙경, “한일공공기관에 의한 개인정보보호제도에 대한 일고찰”, 「개인정보연구」, 제2권 제1호, 2003. 7.

[16] 유상현, “영국의 행정심판제도에 관한 연구”, 「법제」, 제484호, 1998. 4.

[17] 이도헌, “Cyberspace에서의 분쟁조정제도에 관한 연구 - 전자거래분쟁조정위원회를 중심으로 - ”, 「법학연구」, 제11권 제1호, 연세대학교 법학연구소, 2001. 3.

[18] 이성환, “ADR제도와 소비자 피해구제”, 「제7회 소비자의 날 기념 토론회 - 효율적 소비자피해구제 어떻게 할 것인가」, 한국소비자단체협의회, 2002. 12.

[19] 이은선, “온라인을 통한 소송외적 분쟁해결에 관한 고찰”, 「개인정보연구」, 제2권 제1호, 2003. 7.

[20] 이인호, “개인정보보호에 대한 국제적 동향 분석”, 「인터넷법률」, 제18호, 2003. 7.

[21] 이종영, “독일의 멀티미디어법”, 「법제」, 제489호, 1998. 9.

[22] 이호룡, “각국의 개인정보보호법제 동향 - 개인정보보호법의 제정 논의에 즈음하여 - ”, 「인터넷법률」, 제8호, 2001. 9.

[23] 장영두, “협상에 기초한 대안적 분쟁해결(ADR)방안”, 2001 춘계학술대회 발표자료, 한국정부학회, 2001.
(http://www.tkpa.or.kr/proceeding/2001s/j.hwp)

[24] 조상제, “프랑스의 형사사법제도 - 형사법원의 구조와 검찰제도를 중심으로 - ”, 「비교형사법연구」, 제3권 제1호, 한국비교형사법학회, 2001. 7.
[25] (주)아이클릭, “2003년도 개인 인터넷 이용자의 정보화 역기능 실태조사 보고서”, 한국정보보호진흥원, 2003. 3.
[26] 전학선, “프랑스 헌법재판소와 기본권 보장” (http://www.kpla.or.kr/FileBoard/87haksul/bal-6.html)
[27] 정보통신부, “정보통신백서”, 2003.
[28] 정영화, “인터넷상 개인정보보호 및 분쟁해결에 관한 연구”, 「인터넷법연구」, 제1호, 2002. 6.
[29] _____, “해외 프라이버시 위원회의 국가별 위상과 역할 비교 검토”, 「제2회 워크숍 - 프라이버시 보호 법제, 어떤 모습이어야 하는가?」(연속 워크숍 - 프라이버시 보호법제 개선의 쟁점들), 2003. 8. 21.
[30] 정완용, “전자거래에 있어서 개인정보침해에 대한 법적 구제”, 「인터넷법률」, 제10호, 2002. 1.
[31] 정준현, “프라이버시 보호를 위한 사후적 권한 검토”, 「제2회 워크숍 - 프라이버시 보호 법제, 어떤 모습이어야 하는가?」(연속 워크숍 - 프라이버시 보호법제 개선의 쟁점들), 2003. 8. 21.
[32] 정진명, “인터넷관련 독일의 법제 동향과 전망”, 한국법제연구원, 2001. 12.
[33] 통신위원회, “통신위원회 심결집”, 2003.
[34] 한국전자거래진흥원, “2002 전자거래분쟁조정사례집”, 2003. 1.
[35] 한국정보보호진흥원, “2002 개인정보보호백서”, 2003.
[36] 한국정보보호진흥원, “2002 개인정보분쟁조정사례집”, 2003.
[37] 한국통신정보보호학회, “주요국가의 개인정보보호기관 운영상황 연구”, 한국정보보호센터, 1998.
[38] 한영학, “일본의 개인정보보호 법제”, 「세계언론법제동향」, 2000. 12.
[39] 행정자치부, “공공기관의 개인정보보호제도 이해와 해설”, 2003. 3.
[40] 행정자치부, “개인정보화일목록집”, 2002.

[41] 현대호, "인터넷상의 정보보호에 관한 법제연구", 한국법제연구원, 2000.

[42] 홍승진, "미국의 Internet 규제의 최근 동향 - 입법례와 법원의 위헌성 판단을 중심으로 - ", 「법제」, 제552호, 2003. 12.

[43] 황상철, "일본의 개인정보보호를 위한 입법동향 - 개인정보의보호에 관한법률안을 중심으로 - ", 「법제」, 제541호, 2003. 1.

2. 국외문헌

[1] Advisory Committee on Automated Personal Data Systems, *"Records, Computers and the Rights of Citizens"*, Department of Health, Education and Welfare, 1973. (http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm)

[2] Anne Carblanc, *"Privacy Protection and Redress in the Online Environment : Fostering Effective Alternative Dispute Resolution"*, 22nd International Conference on Privacy and Personal Data Protection, 2000. (http://www.ops2.moc.go.th/PDF/venice_paper.pdf)

[3] Anne Cavoukian/Tyler J. Hamilton, *"Privacy Payoff - How Successful Business Build Customer Trust"*, McGraw-Hill Ryerson, 2002.

[4] BBB/CBBB/BBBOnLine, *"Protecting Consumers in Cross-Border Transactions : a Comprehensive Model for Alternative Dispute Resolution"*, CBBB, 2000. (http://www.bbbonline.org/about/press/whitePaper.doc)

[5] BBBOnLine, *"BBBOnline Privacy Program, Dispute Resolution Process Procedures - Privacy Policy Review Service and Privacy Review Appeals Board"*, 1999. 2. 11. (http://www.bbbonline.org/privacy/dr.pdf)

[6] BBBOnLine/CBBB, *"A Review of Federal and State Privacy Laws"*, (http://www.bbbonline.org/UnderstandingPrivacy/library/fed_statePrivLaws.pdf)

[7] Blair Stewart, *"International Accreditation of Privacy and Data Protection Authorities"*, APEC Data Privacy Workshop(Panel Ⅱ), Chiang Rai, Thailand, 2003.

[8] Catherine Morris, *What is "'Alternative Dispute Resolution'(ADR)? : Some Ways of processing Disputes and Addressing Conflict"*, (http://www.peacemakers.ca/publications/ADRdefinitions.html)

[9] Center for Democracy and Governance, *"Alternative Dispute Resolution Practitioner's Guide"*, Technical Publication Series, 1998. 3. (www.usaid.gov/democracy/pdfs/pnacb895.pdf)

[10] Colin J. Bennett, *"The Office of the Privacy Commissioner of Canada : Regulator, Educator, Consultant and Judge"* (http://www.ccmd-ccg.gc.ca/research/publications/pdfs/CBennett_e.pdf)

[11] CBBB, *"Alternative Dispute Resolution for Consumer Transactions in the Borderless Online Marketplace"*, 2000. (www.bbbonline.org/about/press/FTC_ADR.doc)

[12] Department of Commerce(U.S.), *"Damages for Breaches of Privacy, Legal Authorizations and Mergers and Takeovers in U.S. Law"*, Memorandum to European Commission, 2000. 7. 14. (http://www.privacilla.org/business/privacytorts.html)

[13] Department of Commerc(U.S.), *"SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE U.S. DEPARTEMNT OF COMMERCE ON JULY 21, 2000"* (http://www.export.gov/safeharbor)

[14] Der Bundesbeauftragte für den Datenschutz, *"Complaints Handling Procedure in Germany"*, Ⅶ Complaints Handling Workshop on March 10 and 11, 2003 in Warsaw.

[15] Domingo R. Tan, *"Personal Privacy in the Information Age : Comparison of Internet Data Protection Regulations in the United States and the European Union"*, 21 Loyola of Los Angeles International & Comparative Law Journal 661, 669 (1999).

[16] Douwe Korff, *"EU Study on Implementation of Data Protection Directive - Comparative summary of national laws"*, Human Rights Centre, University of Essex, 2002.

[17] ECOM, "ECで取"り扱われる個人情報に關する調査報告書(ver. 3.0)", 2001. 3.

[18] EPIC Alert, *"EU Set to Implement Privacy Directive"*, 2003. 10. 30.

[19] EPIC & PI, *"Privacy and Human Rights 2003 - An International Survey of Privacy Laws and Developments"*, 2003 (http://www.privacyinternational.org/survey/phr2003/countries/unitedkingdom.htm)

[20] European Commission, *"Data Protection In the European Union"* (http://europa.eu.int/comm/internal_market/privacy/guide_en.htm)

[21] European parliament and the council, *"DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"*, European Commission, 1995. (http://europa.eu.int/comm/internal_market/privacy/law_en.htm)

[22] European parliament and the council, *"Directive 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector"*, European Commission, 1997. (http://europa.eu.int/comm/internal_market/privacy/law_en.htm

[23] European parliament and the council, *"DIRECTIVE 02/58/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the processing of personal data and the protection of privacy in the electronic communications sector"*, European Commission, 2002. (http://europa.eu.int/comm/internal_market/privacy/law_en.htm)

[24] Fred H. Cate, *"Privacy in the Information Age"*, Brooking Institution Press, 1997.

[25] _____, *"The Privacy Problem - A broader view of information privacy and the costs and consequences of protection it"*, A First Amendment Center Publication, The Freedom Forum, vol 4. No. 1, 2003. 3. (http://www.law.indiana.edu/directory/publications/fcate/privacyproblem.pdf)

[26] Fred H. Cate/Robert Litan, *"Constitutional Issues in Information Privacy"*, 9 Mich. Telecomm. Tech. L. Rev. 35 (2002). (http://www.mttlr.org/volnine/cate.pdf)

[27] FTC, *"A Brief Overview of the Federal Trade Commission's Investigative and Law enforcement Authority"*, 2002. 9. (http://www.ftc.gov/ogc/brfovrvw.htm)

[28] ____, *"Privacy Online : A Report to Congress"*, 1998. 6.

[29] Gerald Spindler/Fritjof Börner(Edit.), *"E-Commerce Law in Europe and the USA"*, Springer, 2002.

[30] Graham Greenleaf, *"Enforcement of the Privacy Act : Problems and Potential"*, 2001. (http://austlii.edu.au/~graham/publications/2001/enforcement.html)

[31] Hakim Ben Adjoua, *"Electronic Alternative Dispute Resolution"*, 2000. (http://www.paralegals.org/Reporter/On-line00/adr.htm)

[32] Information Commissioner(U.K.), *"Annual Report And Accounts For The Year Ending 31 March 2003"*, 2003. (http://www.informationcommissioner.gov.uk/cms/DocumentUploads/AR03.pdf)

[33] Information Commissioner(U.K.), *"Data Protection Act Claiming Compensation"*, 2003. (http://informationcommissioner.gov.uk)

[34] Joel R. Reidenberg/Paul M. Schwartz, *"Data Protection Law and On-line Services : Regulatory Responses"*, 1998. 12. (http://europa.eu.int/comm/internal_market/privacy/studies_en.htm)

[35] Jonathan P. Cody, *"Protecting Privacy Over the Internet : Has the Time Comer to Abandon Self-Regulation?"*, 48 Catholic University Law Review 1183, 1193 (1999).

[36] Julia Hörnle, *"Online Dispute Resolution in Business to Consumer E-commerce Transactions"*, Journal of Information Law & Technology, 2002. (http://elj.warwick.ac.uk/jilt/02-2/hornle.html)

[37] Kent D. Stuckey with Contributing Authors, *"Internet and Online Law"*, Law Journal Press (N.Y.), 2000.

[38] Marc Rotenberg, *"The Privacy Law Sourcebook 2002 - United States Law, International Law, and Recent Developments"*, Electronic Privacy Information Center, 2002.

[39] Michael Chissick/Alistair Kelman, *"Electronic Commerce : Law and Practice"*, Sweet & Maxwell(London), 1999.

[40] NADRAC, *"What is ADR?"* (http://www.nadrac.gov.au)

[41] _____, *"Dispute Resolution Terms - The use of terms in (alternative) dispute resolution - ?"*, 2003. 9. (http://www.nadrac.gov.au)

[42] Nigel Waters, *"Codewatch : Privacy Codes - What are they? Where are they?"*, Privacy Law and Policy Reporter 6, 2001. (http://www.austlii.edu.au/au/journals/PLPR/2001/6.html)

[43] OECD, *"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data"*, 1980.
(http://www1.oecd.org/publications/e-book/9302011E.PDF)

[44] OECD, *"Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce"*, 1999.
(http://www1.oecd.org/publications/e-book/9300023E.PDF)

[45] OECD Working Party on Information Security and Privacy, *"Buiding Trust in the Online Environment : Business To Consumer Dispute Resolution(Report of the Joint Conference of the OECD, HCOPIL, ICC)"*, 2001. 4. 29.

[46] OECD Working Party on Information Security and Privacy, *"Legal Provisions Related to Business-To-Consumer Alternative Dispute Resolution in Relation to Privacy and Consumer Protection"*, 2002.

[47] Paul Roth, *"Remedies For Personal Data Infringements : The New Zealand Model"*, 2002 International Conference on Personal Data Protection - Personal Data Protection in the Digital Age -, Seoul, Korea, 2002.

[48] Privacy Commissioner of Canada, *"Annual Report to Parliament 2002-2003"*
(http://www.privcom.gc.ca/information/ar/02_04_e.asp)

[49] Privacy Commissioner of New Zealand, *"Annual Report of the PRIVACY COMMISSIONER 2001-2002"*
(http://www.privacy.org.nz/recept/rectop.html)

[50] R. Wacks(ed), "Privacy", Vol. 1, 1993.

[51] Raymond Tang, *"Remedies for Personal Data Infringements under the Personal Data(Privacy) Ordinance"*, 2002 International Conference on Personal Data Protection - Personal Data Protection in the Digital Age -, Seoul, Korea, 2002.

[52] Roger Clarke, *"Introduction to Dataveillance and Information Privacy, and Definitions of Terms"* (http://anu.edu.au/people/Roger.Clarke/DV/Intro.html)

[53] S. Schroeder, *"Alternative Dispute Resolution Resources"*, Risk Management, 45(6), 1998.

[54] Samuel D. Warren/Louis D. Brandeis, *"The Right to Privacy"*, Harv. L. Rev., Vol. Ⅳ, No. 5, 1890. 12. 15. (http://www.louisville.edu/library/law/brandeis/privacy.html)

[55] Stan Karas, *"Privacy, Identity, Databases"*, 52 Am. U. L. Rev. 393 (2002. 12)

[56] Swedish Data Inspection Board, "1999 The Swedish Data Inspection Board", 2000. (http://www.datainspektionen.se/pdf/arsredovisningar/eng_1999.pdf)

[57] Synovate, *"Identity Theft Survey Report"*, Federal Trade Commission, 2003. 9.

[58] Tamara L. Hunter/Chris Bennett, *"Personal Information Protection and Electronic Documents Act("PIPEDA") - Presentation to the Insurance, Investigation, Security and Human Resources Industries for Shepp Johnman - "*, Davis & Company, 2002. 2. 13.

[59] The Office of the Federal Privacy Commissioner of Australia, *"Guidelines on Privacy Code Development"*, 2001. (http://www.privacy.gov.au/act/guidelines/index.html)

[60] The Office of the Federal Privacy Commissioner of Australia, "Privacy in Australia", 2002. (http://www.privacy.gov.au)

[61] The Office of the Federal Privacy Commissioner of Australia, *"The Operation of the Privacy Act - Annual Report 1 July 2002 - 30 June 2003"*, 2003. (http://www.privacy.gov.au/publications/03annrep.pdf)

[62] The Office of the Privacy Commissioner for Personal Data(HK), *"Mediation v. Investigation"*, Privacy Agencies of New Zealand and Australia Plus Hong Kong, 16th PANZA+ Meeting, 2003. 3. 27.

[63] The Office of the Privacy Commissioner for Personal Data(HK), *"Annual Report 2002-2003"*, 2003.
(http://www.pco.org.hk/english/publications/annualreport.html)

[64] UN, *"International Covenant on civil and political rights"*, General Assembly Resolution 2200A(XXI), 1966.
(http://www.unhchr.ch/html/menu3/b/a_ccpr.htm)

[65] UN, *"Guidelines for the Regulation of Computerized Personal Data Files"*, General Assembly resolution 45/95, 1990.
(http://www.unhchr.ch/html/menu3/b/71.htm)

3. 참고 사이트

[1] 경찰청 사이버테러대응센터, http://ctrc.go.kr

[2] 국가인권위원회, http://www.humanrights.go.kr

[3] 국민고충처리위원회, http://www.ombudsman.go.kr

[4] 금융감독원, http://www.fss.or.kr

[5] 대한상사중재원, http://www.kcab.or.kr

[6] 전자거래분쟁조정위원회, http://www.ecme.or.kr

[7] 정보통신부, http://www.mic.go.kr

[8] 통신위원회, http://www.kcc.go.kr

[9] 한국소비자보호원, http://cpb.or.kr

[10] 행정자치부, http://www.mogaha.go.kr

[11] 환경분쟁조정위원회, http://edc.me.go.kr

[12] 네덜란드 정보보호위원회, http://www.cbpweb.nl

[13] 노르웨이 정보조사원, http://www.datatilsynet.no
[14] 뉴질랜드 프라이버시커미셔너, http://www.privacy.org.nz
[15] 뉴질랜드 옴브즈만, http://www.ombudsmen.govt.nz
[16] 그리스 정보보호원, http://www.dpa.gr
[17] 독일 연방정보보호청, http://www.bfd.bund.de
[18] 미국 상무부, http://www.export.gov
[19] 미국 연방거래위원회, http://www.ftc.gov
[20] 스웨덴 정보조사원, http://www.datainspektionen.se
[21] 스페인 개인정보보호원, http://www.agpd.es
[22] 아이슬란드 정보보호위원회, http://www.personuvernd.is
[23] 영국 정보커미셔너, http://www.dataprotection.gov.uk
[24] 영국 헌법부, http://www.dca.gov.uk
[25] 오스트리아 정보보호위원회, http://www.bka.gv.at/datenschutz
[26] 일본 총무성, http://www.soumu.go.jp
[27] 일본 수상, http://www.kantei.go.jp/jp/it/privacy
[28] 캐나다 프라이버시커미셔너, http://www.privcom.gc.ca
[29] 핀란드 정보보호옴브즈만, http://www.tietosuoja.fi
[30] 프랑스 정보자유위원회, http://www.cnil.fr
[31] 호주 연방프라이버시커미셔너, http://www.privacy.gov.au
[32] 홍콩 개인정보프라이버시커미셔너, http://www.pco.org.hk
[33] EU, http://europa.eu.int/comm/internal_market/privacy
[34] BBBOnLine, http://www.bbbonline.org/privacy
[35] *"Defining Privacy & Personal Information"*, (http://journalism.okstate.edu/faculty/jsenat/privacy/definition.html)
[36] *"Privacy"* (http://plato.stanford.edu/entries/privacy)
[37] *"A Primer on Privacy Law"* (http://www.dla.org/downloads/1)

이 창 범
<주요 학력 및 경력>
동국대학교 및 동 대학원 법학과 졸
(법학박사)
현 개인정보분쟁조정위원회 사무국장
현 한국법률문화연구원 부원장
현 한국소비자교육지원센터 이사
현 건국대학교 겸임교수
전 한국소비자보호원(책임연구원)
전 재정경제부 소비자정책전문위원
<저서 및 논문>
광고와 법(공역), 소비자법과 정책(저서)
소비자피해구제론(저서) 등

윤주연
<주요 학력 및 경력>
성신여자대학교 및 동 대학원 법학과 졸
(법학석사)
현 개인정보분쟁조정위원회 사무국
연구원

각국의 개인정보피해구제제도 비교연구

2003년 12월 인쇄
2003년 12월 발행
발 행 인 박 준 수
발 행 처 개인정보분쟁조정위원회
서울시 송파구 가락동 78번지 IT벤처타워 서관 7층
URL : http://www.kopico.or.kr 또는 개인정보.kr
TEL : 02-405-4747, FAX : 02-405-4729
인 쇄 처 일지사 (Tel : 02-503-6971)
<비매품>