| 발 간 등 록 번 호 |
| --- |
| 11-1620000-000204-01 |

# 개인정보 수집·유통 실태조사

**연 구 기 관 :  진보네트워크센터**
**연구 책임자 :  오 병 일**

**2009 년 12 월**

국가인권위원회

본 보고서는 연구용역수행기관의 결과물로서, 국가인권위원회의 입장과 다를 수 있습니다.

# 제 출 문

국가인권위원회 위원장 귀하

본 보고서를 「개인정보 수집·유통 실태조사」에 관한 2009년도 국가인권위원회 인권상황 실태조사 연구용역 보고서로 제출합니다.

2009. 12.


연 구 기 관 : 진보네트워크센터
연 구 기 간 : 2009.5.8 ~ 2009.12.7
연구 책임자 : 오병일 (진보네트워크센터 코디네이터)
연 구 원 : 장여경 (진보네트워크센터 정책총괄)
김지성 (진보네트워크센터 활동가)
이은우 (법무법인지평 변호사)
김 철 (서울대학교 한국행정연구소)

# 목 차

**제1장 서 론** ····· 1
제1절 연구의 목적 및 필요성 ····· 1
1. 연구의 필요성 ····· 1
2. 연구의 목적 ····· 4
제2절 연구의 내용 및 연구 방법 ····· 4
1. 선행연구 및 관련연구 분석 ····· 4
2. 연구의 대상과 방법 ····· 9

**제2장 사회영역별 개인정보 수집·유통실태** ····· 14
제1절 행정정보공동이용시스템/행정기관 간 개인정보 공유 ····· 14
I. 행정정보공동이용시스템 ····· 14
1. 개 요 ····· 14
2. 행정정보 공동이용시스템을 통한 개인정보 수집·유통 실태 ····· 21
3. 소결 ····· 50
II. 행정기관 간 개인정보 공유 ····· 51
1. 개요 ····· 51
2. 행정기관 간 개인정보의 수집·유통 실태 ····· 55
3. 개인정보파일의 수집·유통 실태 ····· 69
4. 소결 ····· 79
제2절 수사/범죄경력(경찰) 영역 ····· 80
I. 수사자료표 ····· 82
1. 개요 ····· 82
2. 개인정보의 수집·유통 실태 ····· 82
3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 90
4. 소결 ····· 94
II. 범죄정보관리시스템(CIMS) ····· 95
1. 개요 ····· 95
2. 개인정보의 수집·유통 실태 ····· 97

3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 103
4. 소결 ····· 105
제3절 정보통신 영역 ····· 106
I. 포털 업체 ····· 106
1. 개 요 ····· 106
2. 개인정보 수집 실태 ····· 110
3. 개인정보 유통 실태 ····· 117
4. 정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 121
5. 소 결 ····· 128
II. 이동통신사 및 초고속인터넷업체 ····· 129
1. 개 요 ····· 129
2. 개인정보 수집·유통 실태 ····· 131
3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 162
4. 소 결 ····· 172
제4절 금융 영역 ····· 175
1. 개 요 ····· 175
2. 개인신용정보의 개념과 법제도 ····· 176
3. 개인신용정보의 수집·유통 실태 ····· 180
4. 신용정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 204
5. 결 론 ····· 211
제5절 보건의료영역 ····· 213
1. 개요 ····· 213
2. 의료정보 보호 관련 법제도 실태 ····· 214
3. 생성기관에서의 의료정보의 수집·유통 실태 ····· 218
4. 취급기관에서의 의료정보 수집·유통 실태 ····· 235
5. 소결 ····· 251
제6절 교육 영역(NEIS 도입 및 통합) ····· 254
1. 개요 ····· 254
2. 개인정보 수집·유통 실태 ····· 259
3. 개인정보의 열람 및 정정·삭제 청구권 보장 실태 ····· 272
4. 소결 ····· 273

**제3장 특성별 개인정보 수집·유통 실태** ····· 275

제1절 CCTV ····· 275
1. 개요 ····· 275
2. 개인정보의 수집·유통 실태 ····· 285
3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 303
4. 소결 ····· 307
제2절 위치정보 ····· 310
1. 개요 ····· 310
2. 위치정보사업에서의 개인정보 수집·유통 실태 ····· 312
3. 교통 관련 위치정보의 수집·유통 실태 ····· 325
4. 소 결 ····· 345
제3절 유전정보 ····· 347
1. 개요 ····· 347
2. 유전정보의 수집·유통 실태 ····· 351
3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태 ····· 356
4. 소결 ····· 357
제4절 통신 비밀 ····· 358
1. 개요 ····· 358
2. 개인정보의 수집·유통 실태 ····· 366
3. 정보주체의 열람 및 통지에 대한 권리 보장 실태 ····· 375
4. 소결 ····· 382

**제4장 설문조사 결과 분석** ····· 384
제1절 일반 시민 대상 설문조사 결과 분석 ····· 384
1. 조사 개요 ····· 384
2. 종합결과 ····· 385
3. 설문별 분석 결과 ····· 386
제2절 개인정보보호 책임자 대상 설문조사 결과 분석 ····· 401
Ⅰ. 조사 개요 ····· 401
Ⅱ. 설문별 분석 결과 ····· 404
1. 개인정보 침해 위험 및 개인정보보호 체계와 관련한 사항 ····· 405
2. 개인정보 수집단계에서 발생할 수 있는 개인정보 침해 문제와 관련한 사항 · 412
3. 개인정보의 이용·제공·공유, 보유 및 파기 등과 관련한 사항 ····· 416
4. 개인정보 처리의 위탁 등과 관련한 사항 ····· 419

5. 정보주체의 권리보장 조치와 관련한 사항 ····· 422
6. 개인정보 보호를 위한 인적 통제 ····· 427

**제5장 결 론** ····· 429
제1절 연구결과 ····· 429
제2절 연구의 한계 및 향후 과제 ····· 432

**참고문헌** ····· 434

**<부록 1> 시민인식조사 설문지** ····· 442
**<부록 2> 개인정보 보유기관 담당자 대상 실태조사 설문지** ····· 446
**<부록 3> 행정정보공유추진위원회 소위원회 회의록 중 개인정보 보호 관련 내용** 452

## [표 차례]

<표 1-1> 본 연구에서 정보주체 열람청구를 수행한 대상 기관 및 업체 ····· 12
<표 2-1> 행정정보 공동이용시스템의 단계별 확대구축 사업 현황 ····· 16
<표 2-2> 민원사무 1건 당 구비서류 종수 현황 ····· 17
<표 2-3> 개인정보 보호의 주요 원칙 ····· 21
<표 2-4> 행정정보 공동이용 대상정보 ····· 22
<표 2-5> 행정정보공동이용 이용기관 현황(379개) ····· 31
<표 2-6> 연도별 행정정보 공동이용 실적 ····· 34
<표 2-7> 지난 3년간 행정정보 공동이용 점검대상 기관수 ····· 35
<표 2-8> 행정정보 오·남용 적출 유형 ····· 39
<표 2-9> 행정정보 중계시스템의 주요 보안조치 ····· 41
<표 2-10> 행정정보공동이용센터의 기능 ····· 43
<표 2-11> 행정정보공유추진위원회(소위원회) 회의 안건 ····· 45
<표 2-12> 공공기관 개인정보보호심의위원회 회의개최 여부('05~'09) ····· 58
<표 2-13> 공공기관 개인정보보호심의위원회 회의일자 및 안건 ····· 59
<표 2-14> 지방세 체납처분을 위한 건강보험 직장가입자 정보 제공에 대한 의견 65
<표 2-15> 퇴직공직자 취업제한 확인을 위한 건강보험 직장가입자 정보 제공에 대한 의견 ····· 67

<표 2-16> 개인정보 보유 기관수 및 보유 파일 수 ····· 72
<표 2-17> 연도별 수사자료표 작성 현황 ····· 83
<표 2-18> 연도별 범죄(수사)경력 조회 현황 및 건수(경찰관서) ····· 85
<표 2-19> 경찰관의 수사자료표 조회와 관련한 국가인권위원회 결정례 ····· 85
<표 2-20> 연도별 범죄(수사)경력 조회 현황 및 건수(타기관 제공) ····· 86
<표 2-21> 연도별 수사자료표 삭제 현황 및 건수 ····· 89
<표 2-22> 연도별 범죄(수사)경력 조회 현황 및 건수(개인 신청) ····· 90
<표 2-23> 수사자료표와 범죄정보관리시스템의 개인정보 생성과 유통 ····· 97
<표 2-24> 범죄정보관리시스템에 기록된 사건 건수 ····· 99
<표 2-25> 범죄정보관리시스템에 저장된 개인정보 현황 ····· 99
<표 2-26> 범죄정보관리시스템 입력 주요 서식 종류 (모두 301종) ····· 100
<표 2-27> 범죄정보관리시스템 정보에 대한 조회현황 ····· 102
<표 2-28> 범죄정보관리시스템 오남용에 대한 징계건수 ····· 103
<표 2-29> 「정보통신망법」의 개인정보보호 관련법령 제·개정 현황 ····· 108
<표 2-30> 조사대상 사이트 ····· 109
<표 2-31> 주요 포털의 약관 기준 필수수집항목 ····· 111
<표 2-32> 주요 포털의 약관 기준 자동수집항목 ····· 115
<표 2-33> 각 포털 개인정보 취급방침 조사항목 ····· 119
<표 2-34> 각 포털별 개인정보 열람청구 및 정책질의 결과 ····· 123
<표 2-35> 연도별 통신서비스 가입자 수 ····· 129
<표 2-36> 초고속인터넷 가입자 수 현황 ····· 130
<표 2-37> 한 이동통신업체가 개인정보를 제공하는 제3자 업체의 목록 ····· 135
<표 2-38> 한 이동통신업체가 개인정보를 제공하는 취급위탁 업체의 목록 ····· 138
<표 2-39> 개인정보 유용행위 등에 대한 방송통신위원회 시정조치 현황 ····· 140
<표 2-40> 개인정보 제공 내역 ····· 143
<표 2-41> “개인정보보호방침” 내 “개인정보 수집 및 활용목적” 추가사항 ····· 144
<표 2-42> 각 통신업체별/업무별 제3자 제공 및 취급위탁 구분 사례 ····· 150
<표 2-43> 각 이동통신사의 ‘개인정보의 보유기간 및 이용기간’ 내용 ····· 157
<표 2-44> 각 초고속인터넷업체의 ‘개인정보의 보유기간 및 이용기간’ 내용 ····· 161
<표 2-45> 업체별 열람 청구권 관련 내용 ····· 164
<표 2-46> 이용 과정에서 자동으로 생성되는 정보 ····· 167
<표 2-47> 초고속인터넷 서비스 이용기록 열람청구 ····· 168
<표 2-48> 제3자 제공 내역 청구에 대한 답변 ····· 169

<표 2-49> 신용정보의 종류 ····· 176
<표 2-50> 종합신용정보집중기관을 통하여 집중관리·활용되는 신용정보 범위(제21조제3항 관련) ····· 182
<표 2-51> 개별신용정보집중기관의 집중관리, 활용대상 정보 ····· 184
<표 2-52> 금융지주회사 및 개인신용정보를 공유하는 계열사 현황 ····· 196
<표 2-53> 주요 금융기관 홈페이지에 공시된 개인정보보호 관련 정책 ····· 201
<표 2-54> 신용조회회사 무료 신용조회 서비스 제공 정보 ····· 206
<표 2-55> 의료기관(국립병원 및 국립대학교 병원) 개인정보 보유 현황 ····· 219
<표 2-56> 의료기관(국립병원 및 국립대학교 병원) 개인정보의 제3자 제공 현황 224
<표 2-57> 전자의무기록의 적정보존기간에 대한 의사 대상 설문조사 결과 ····· 227
<표 2-58> 의료기관(국립병원 및 국립대학교 병원)의 의료정보 보유 기간 ····· 227
<표 2-59> 의료기관(국립병원 및 국립대학교 병원)의 의료정보 보호를위한 정책 229
<표 2-60> 환자정보 보호 관련 9개 사항 ····· 230
<표 2-61> 의료기관별 정보화 현황 ····· 232
<표 2-62> 정보업무 총괄 조직 여부 ····· 232
<표 2-63> UPS 또는 자가발전설비 구축여부 ····· 233
<표 2-64> 네트워크 백업 예비선로 여부 ····· 233
<표 2-65> 의료기관(국립병원 및 국립대학교 병원)에서 자기정보 열람방법 ····· 234
<표 2-66> 각 취급기관이 보유하고 있는 개인정보파일목록 ····· 236
<표 2-67> 각 취급기관의 개인정보 수집 방법 ····· 237
<표 2-68> 건강보험공단에 시스템연계를 통해 개인정보를 제공하는 기관 현황 ·· 237
<표 2-69> 건강보험심사평가원이 보유하고있는 개인정보의 수집방법및제공기관 238
<표 2-70> 취급기관으로부터 개인정보를 제공받는 기관 현황 ····· 239
<표 2-71> 건강보험심사평가원으로부터 개인정보를 제공받는 기관 현황 ····· 239
<표 2-72> 국민건강보험공단으로부터 시스템 연계를 통해 개인정보를 제공받는 기관 현황 ····· 239
<표 2-73> 국민건강보험공단 부서별 건강보험 자료제공 현황 ····· 240
<표 2-74> 건강보험공단으로부터 건강보험자료를 제공받은 기관 ····· 241
<표 2-75> 국민건강보험공단에 건강보험 자료를 요청한 사유 ····· 242
<표 2-76> 국민건강보험공단에 건강보험 자료를 요청한 법적 근거 ····· 243
<표 2-77> 2009년 공공기관 개인정보보호심의위원회 회의일자 및 안건 ····· 244
<표 2-78> 취급기관이 영구 혹은 준영구적으로 보존하고 있는 개인정보파일 ····· 246
<표 2-79> 국민건강보험공단 직원의 개인정보 무단열람 사례 ····· 247

<표 2-80> 최근 2년간 건강보험공단 직원, 개인정보 관련 징계현황 ····· 248
<표 2-81> 초기 교육행정업무서비스 내역 ····· 260
<표 2-82> 국가인권위원회 결정문 ····· 262
<표 2-83> 교육정보의 수집・활용・관리 원칙 ····· 263
<표 2-84> 2009년 학부모 서비스 제공 항목 38종 ····· 265
<표 2-85> 시도별 연도별 학부모서비스 누적 이용자 수 ····· 266
<표 2-86> 학부모서비스 매뉴얼 상세 이용 현황 ····· 267
<표 3-1> 국가인권위원회 CCTV 관련 민원현황 ····· 277
<표 3-2> CCTV 관련 법률 ····· 279
<표 3-3> 국회 발의 중인 개인정보보호법안 중 CCTV 관련 규정 ····· 282
<표 3-4> 공공기관 CCTV의 설치목적별 현황 ····· 283
<표 3-5> 지방자치단체 방범용 CCTV 설치 현황 ····· 284
<표 3-6> 방범용 CCTV 설치 시 의견수렴 방법 (서울 자치구) ····· 288
<표 3-7> CCTV 설치 및 운영 규정 혹은 지침 인터넷 주소 (서울 자치구) ····· 295
<표 3-8> 방범용 CCTV에 대한 위탁 운영 현황 (서울 자치구) ····· 298
<표 3-9> 방범용 CCTV 기록 조회 현황 (서울 자치구 수탁 경찰관서) ····· 300
<표 3-10> 방범용 CCTV 모니터 요원 현황 (서울 자치구 수탁 경찰관서) ····· 302
<표 3-11> 개인정보파일대장에 CCTV 개인화상정보 파일을 공개한 서울 자치구 현황 (2008년) ····· 304
<표 3-12> 방범용 CCTV 위치 공개 여부 (서울 자치구) ····· 305
<표 3-13> 위치정보서비스 업체 현황 ····· 313
<표 3-14> 위치정보사업 허가 현황 ····· 313
<표 3-15> 위치기반서비스 현황 ····· 314
<표 3-16> 위치정보의 정확도 비교 ····· 319
<표 3-17> 아동 위치추적 서비스 현황 ····· 320
<표 3-18> 긴급구조를 위한 위치정보 조회수 ····· 321
<표 3-19> 승용차 요일제 참여 준수차량 관리파일 대장 ····· 328
<표 3-20> 승용차 요일제 관련 정보공개 청구 답변(1) ····· 328
<표 3-21> 승용차 요일제 관련 정보공개 청구 답변(2) ····· 329
<표 3-22> 한국도로공사가 공개한 하이패스플러스카드 고객파일 대장 ····· 331
<표 3-23> 한국도로공사가 공개한 OBU 고객파일 대장 ····· 332
<표 3-24> 하이패스 이용 고객 관리를 위한 개인정보파일대장 ····· 333
<표 3-25> 하이패스 진・출입 요금소 수집 정보 관리 데이터베이스 ····· 333

<표 3-26> 서울시 교통카드 수록 정보 ····· 340
<표 3-27> 국립과학수사연구소가 보유중인 연도별 유전정보 건수 ····· 351
<표 3-28> 유전자 데이터베이스에서 폐기된 유전정보 건수 ····· 355
<표 3-29> 실종아동전문기관이 폐기를 요청한 건수 ····· 356
<표 3-30> 통신 관련 자료 제공의 절차 현황 (2009년 10월) ····· 365
<표 3-31> 통신수단별 통신자료 제공 건수 ····· 366
<표 3-32> 기관별 통신자료 제공 건수 ····· 367
<표 3-33> 통신수단별 통신사실 확인자료 제공 건수 ····· 367
<표 3-34> 기관별 통신사실 확인자료 제공 건수 ····· 368
<표 3-35> 통신사실 확인자료 청구 및 기각률 ····· 368
<표 3-36> 통신수단별 통신 감청 건수 ····· 370
<표 3-37> 기관별 통신 감청 건수 ····· 370
<표 3-38> 통신감청 영장 청구 및 기각률 ····· 371
<표 3-39> 통신제한조치 통지 건수와 통지유예 건수 (검찰) ····· 377
<표 3-40> 통신사실 확인자료 요청 통지 건수와 통지유예 건수 (검찰) ····· 379
<표 3-41> 주요 포털사 정보주체 열람권 행사 현황 ····· 381
<표 4-1> 성별 개인정보 유출과 같은 프라이버시 침해의 심각성 ····· 387
<표 4-2> 연령별 개인정보 유출과 같은 프라이버시 침해의 심각성 ····· 387
<표 4-3> 성별 공공기관의 국민 개인정보 관리의 안전성 ····· 389
<표 4-4> 성별 민간기업의 고객 개인정보 관리의 안전성 ····· 389
<표 4-5> 연령별 공공기관의 국민 개인정보 관리의 안전성 ····· 390
<표 4-6> 연령별 민간기업의 고객 개인정보 관리의 안전성 ····· 390
<표 4-7> 성별 주민번호를 다른 번호로 대체하는 것에 대한 의견 ····· 391
<표 4-8> 연령별 주민번호를 다른 번호로 대체하는 것에 대한 의견 ····· 391
<표 4-9> 개인정보 취급 방침을 공개해야 한다는 사실의 인지 여부 ····· 392
<표 4-10> 성별 개인정보 열람을 청구할 수 있다는 사실의 인지 여부 ····· 392
<표 4-11> 성별 개인정보 확인을 위해 개인정보 열람을 청구한 경험 여부 ····· 393
<표 4-12> 개인정보를 다른 기관과 공유/제공하는 사실의 인지 여부 ····· 394
<표 4-13> 연령별 개인정보를 다른 기관과 공유/제공하는 사실의 인지 여부 ····· 394
<표 4-14> 연령별 CCTV를 인식할 수 있도록 해야 한다는 사실의 인지 여부 ···· 396
<표 4-15> 성별 CCTV가 설치된 것을 보면 안심되는 정도 ····· 398
<표 4-16> 연령별 CCTV가 설치된 것을 보면 안심되는 정도 ····· 398
<표 4-17> 연령별 CCTV에 찍힌다는 사실에 위축되는 정도 ····· 398

<표 4-18> CCTV에 위축되는 정도와 안심되는 정도 사이의 상관관계 ····· 399
<표 4-19> CCTV 설치 관련 위축과 안심 정도 간의 상관계수(n=500) ····· 400
<표 4-20> 설문 개인정보보호 책임자들의 소속기관 ····· 401
<표 4-21> 성별 및 공사 구분 ····· 402
<표 4-22> 개인정보 침해사고의 발생 여부 ····· 405
<표 4-23> 개인정보 침해신고 접수 여부 ····· 406
<표 4-24> 개인정보 영향평가 수행 여부 ····· 406
<표 4-25> 개인정보 보호업무 이외의 별도 업무수행 여부 ····· 407
<표 4-26> 개인정보 담당자의 주된 업무가 개인정보 보호업무인지 여부 ····· 408
<표 4-27> 소속기관별 개인정보보호업무의 주된 업무 정도 ····· 408
<표 4-28> 개인정보관리 담당자의 개인정보 보호 관련 교육 이수 여부 ····· 409
<표 4-29> 개인정보 보호 관련 교육의 효과성 ····· 410
<표 4-30> 개인정보 보호규정의 공개 여부 ····· 411
<표 4-31> 개인정보 보호 관련 규정의 충실한 반영 여부 ····· 411
<표 4-32> 개인정보 보호정책이 수시로 변경·공개되는지 여부 ····· 412
<표 4-33> 최소한의 개인정보만 수집 여부 ····· 413
<표 4-34> 정보주체의 민감한 개인정보 수집 여부 ····· 414
<표 4-35> 정보주체의 주민등록번호 수집 여부 ····· 415
<표 4-36> 개인정보 수집항목을 구분하는 절차·시스템의 구성 여부 ····· 415
<표 4-37> 개인정보의 목적외이용이나 제3자제공시 동의절차·방법 마련여부 ··· 417
<표 4-38> 제3자 제공 정보의 폐기관리 ····· 417
<표 4-39> 제3자 제공내역이 대장 등에 기록·보관되고 있는지 여부 ····· 418
<표 4-40> 개인정보 열람·출력기록의 저장·보관 여부 ····· 418
<표 4-41> 목적 달성 시 해당 개인정보의 파기 여부 ····· 419
<표 4-42> 수탁기관에 대한 적절한 관리·통제시스템의 구축 여부 ····· 420
<표 4-43> 위탁관리자 등에 대한 개인정보 보호 관련 교육 시행 여부 ····· 420
<표 4-44> 수탁기관 등의 접근가능 개인정보 설정 여부 ····· 421
<표 4-45> 위탁 종료 시 수탁기관의 개인정보 회수·파기 절차 수립 여부 ····· 421
<표 4-46> 수탁기관의 개인정보 처리과정에 대한 정기 감사 실시 여부 ····· 422
<표 4-47> 개인정보취급방침 변경의 통지 여부 ····· 423
<표 4-48> 정보주체의 개인정보 열람·정정절차 수립 여부 ····· 423
<표 4-49> 정보주체의 제3자 제공 내역요청 절차 마련 여부 ····· 424
<표 4-50> 개인정보 열람청구 처리 경험 유무 ····· 424

<표 4-51> 열람청구 후 정정·삭제 청구받은 경험 유무 ····· 425
<표 4-52> 정보주체의 개인정보 정정요구 후 정보 이용방지 절차 마련 여부 ····· 426
<표 4-53> 정보주체의 동의철회에 대한 제약 유무 ····· 426
<표 4-54> 전산담당자에 대한 개인정보보호 교육 프로그램 유무 ····· 427
<표 4-55> 각 직무별로 특화된 교육시스템 마련 여부 ····· 428
<표 4-56> 내부직원의 개인정보 접근권한 및 권한별 직무범위의 차등설정 여부 428

## [그림 차례]

<그림 2-1> 행정정보 공유시스템 구성도 ····· 33
<그림 2-2> 영상판독시스템 내 개인정보 열람 청구 이의신청(기각)결정통지서 ····· 77
<그림 2-3> 수사자료표 일반 현황에 대한 정보주체의 열람 청구 ····· 91
<그림 2-4> 수사자료표 이용 현황에 대한 정보주체의 열람 청구 ····· 92
<그림 2-5> 범죄정보관리시스템 일반 현황에 대한 정보주체의 열람 청구 ····· 104
<그림 2-6> 이동통신 유통망 구조 현황 ····· 152
<그림 2-7> 개인신용정보의 제공·이용 흐름도 ····· 181
<그림 2-8> (구) 개인신용정보의 제공·활용 동의서 ····· 189
<그림 2-9> 2009년 개정된 표준 개인신용정보 제공 동의서 ····· 190
<그림 2-10> 한 은행의 전화수신거부 및 동의철회 관리 화면 ····· 210
<그림 2-11> NEIS 시스템 개념도 ····· 259
<그림 3-1> 주민설문 조사서 (은평구) ····· 289
<그림 3-2> 주민 의견 조사서 (용산구) ····· 290
<그림 3-3> CCTV 위탁관리 프로세스 ····· 298
<그림 3-4> CCTV 영상 기록의 사본 보유 사례 (서울 경찰관서) ····· 299
<그림 3-5> 정보주체 화상정보 열람결정통지 ····· 306
<그림 3-6> 후불하이패스카드 홈페이지, 사용내역 확인방법 ····· 337
<그림 3-7> 교통카드시스템의 주요 구성요소 ····· 339
<그림 3-8> T-money 거래내역 조회 화면 ····· 342
<그림 3-9> T-money 업무택시카드 서비스 ····· 343
<그림 3-10> 유전자검사 동의서 ····· 353
<그림 3-11> 감청 허가서 (일부 예시) ····· 372
<그림 3-12> 감청에 대한 통지서 (일부 예시) ····· 378
<그림 3-13> 통신사실 확인자료 제공에 대한 통지서 (일부 예시) ····· 380

<그림 4-1> 개인정보 유출과 같은 프라이버시 침해의 심각성 ····· 386
<그림 4-2> 공공기관의 국민 개인정보 관리의 안전성 ····· 388
<그림 4-3> 민간기업의 고객 개인정보 관리의 안전성 ····· 389
<그림 4-4> 개인정보 열람 후, 정정/삭제를 청구한 경험 여부 ····· 393
<그림 4-5> 어떤 기관에 어떤 개인정보를 제공하는지에 대한 인지 여부 ····· 395
<그림 4-6> CCTV를 인식할 수 있도록 해야 한다는 사실의 인지 여부 ····· 396
<그림 4-7> CCTV가 설치된 것을 보았을 때 안심되는 정도 ····· 397
<그림 4-8> CCTV에 찍힌다는 사실에 위축되는 정도 ····· 397

# 요 약 문

## 제1장 서론

### 제1절 연구의 목적 및 필요성

정보사회에서 디지털화된 개인정보는 대규모로 수집되고 집적될 수 있다. 원격 거래와 원격 행정의 발달은 개인정보의 이용과 오용을 동시에 유발한다. 개인정보의 상업적 가치가 증가하면서 개인정보의 확보는 기업 경쟁력의 주요 요소로 간주되고 있다. 이에 따라 공공 부문과 민간 부문을 통틀어 사회 전체적으로 개인정보의 방대한 수집과 이용을 독려하고, 다른 한편으로 그에 따른 권리 침해를 유발하는 요인이 되고 있다.

자신의 개인정보가 어떠한 경로로 수집되어 어떻게 이용되고 제공되고 있는지 갈수록 정보주체가 정확히 파악하기 어려워지고 있으며, 그 과정에 개입하여 자신의 권리를 행사하기도 쉽지 않다. 또한 개인정보의 무단 수집과 이용을 방관하는 것은, 그 정보에 기초한 사람의 분류, 낙인, 차별을 고착화시키는 결과를 낳을 수도 있다. 최근에는 CCTV 화상정보, 위치정보, 유전정보, 통신비밀 등이 정보처리기술의 발달에 힘입어 방대하게 수집·이용되면서 국가에 의한 시민의 감시와 통제 사회가 도래할 수 있다는 우려의 목소리가 나오기도 한다.

따라서 사회 각계에서 정보주체의 권리를 실질적으로 보장해야 한다는 문제제기가 잇따르고 개인정보 보호와 관련한 법제도에 대한 일정한 정비가 진행되어 왔다. 17대 국회에 이어 18대 국회에서도 다시 한 번 「개인정보보호법」 제정을 두고 논쟁이 일고 있는 오늘의 시점에서, 올바른 입법을 위해서는 우리 현실 속에서 개인정보가 수집되고 유통되는 실태를 정확히 파악할 필요가 있다. 특히 지금까지 진행되어 온 법률 정비에도 불구하고 정보주체의 권리 행사가 충분히 보장받고 있지 못하다면 어째서 그런지가 주요 관심사 중 하나일 것이다.

본 연구는 공공 및 민간의 주요 영역별로 개인정보가 수집되고 관리되는 상황 및 유통 경로를 조사, 연구하여 국민의 개인정보 관리 실태를 파악하고

자 하였다. 특히, 공공 및 민간 영역에서 정보주체의 열람 및 정정·삭제 청구권을 보장할 수 있는 절차 및 실제 이행 수준을 조사함으로써 개인정보에 대한 열람 및 정정·삭제 청구권 보장 실태를 파악하고자 하였다. 또한 CCTV 화상정보, 위치정보, 유전정보, 통신비밀 등 최근 새로운 개인정보 처리 영역으로 사회적 관심을 받고 있는 분야의 실태 또한 그 특성별로 살펴보았다.

또한, 본 연구는 개인정보 보호 및 정보주체의 열람 및 정정·삭제 청구권 보장을 위해 마련되어 있는 기존의 법령 및 가이드라인을 검토하였다. 이러한 검토 과정을 통하여 기존 법령 및 가이드라인의 개선 방안을 모색하였으며, 미비한 부분에 대해서는 바람직한 지침을 제시하고자 하였다.

## 제2절 연구의 내용 및 연구 방법

개인정보에 대한 자기결정권에 대한 선행연구들은 입법론적으로 그리고 비교법적으로 다양한 연구 성과가 축적되어 있는 편이었다. 다만 대개의 연구가 입법론적인 문제제기 수준에 그치고 있을 뿐, 거론된 개인정보 영역과 각 법률이 경험적 현실에서 실제 작동하는 방식에 대한 검토는 이루어지고 있지 못하였다. 이에 본 연구는 선행연구의 한계를 극복하기 위해 법제도적 분석과 개인정보 자기결정권 보장 실태에 대한 분석을 동시에 진행하여 양쪽 연구의 장점을 살리고자 하였다.

또한 개인정보에 대한 권리 실태를 효과적으로 파악하기 위하여 개인정보의 생애주기별 조사가 이루어질 필요가 있으며, 본 연구에서도 이러한 측면에서 실태조사를 진행하였다. 한편, 정보주체의 열람 및 정정·삭제 청구권 등 적극적인 의미에서의 개인정보자기결정권의 행사는 개인의 주도성에 달려 있는 만큼, 일반 시민의 인식에 대한 설문조사를 실시하였다.

본 연구에서 대상으로 선정한 사회영역은 다음과 같다. △ 행정정보공동이용시스템 및 행정기관 간 개인정보 공유, △ 경찰청에서 보유하고 있는 수사/범죄경력 정보, △ 정보통신 영역, △ 금융 영역, △ 보건의료 영역, △ 교육 영역. 이와 함께 CCTV, 위치정보, 유전정보, 통신비밀 등 특수한 유형의 개인정보에 대한 실태조사도 병행하였다. 본 연구에서 정보주체의 열람청구를 진행한 영역은 다음과 같다.

| 대상 영역 | 열람청구 대상 기관/업체 | 열람청구 내용 |
|---|---|---|
| 수사, 범죄 경력 정보 | 경찰청 | 수사자료표 및 범죄정보관리시스템(CIMS)에 수록된 개인정보에 대한 열람 청구 |
| 정보통신 영역 통신비밀 | 각 포털업체 | 자기정보 및 제3자 제공내역에 대한 열람 청구, 각 포털업체의 개인정보 보호 정책에 대한 질의 병행. |
| 정보통신 영역 위치정보 통신비밀 | 이동통신사 및 초고속인터넷업체 | 통화내역, 위치정보, 인터넷 이용내역, 제3자 제공내역에 대한 열람 청구 |
| 금융 영역 | 은행, 신용조회업체 | 무료열람권, 신용정보제공사실 통보요구권 보장여부 확인 |
| CCTV | 지방자치단체 및 경찰서 | CCTV에 찍힌 본인 화상정보에 대한 열람청구 |

# 제2장 사회영역별 개인정보 수집·유통실태

## 제1절 행정정보공동이용시스템/행정기관 간 개인정보 공유

### Ⅰ. 행정정보공동이용시스템

최근 정부 측에서 행정정보 공동이용과 관련하여 논의되는 사항들은 대부분 행정정보공동이용시스템을 통해 이루어지는, 민원처리를 위해 필요한 행정정보로 한정하고 있다. 행정정보공동이용시스템은 국민들이 서류를 직접 발급받는 불편을 해소하고 민원서류를 감축하기 위해 각 기관에서 민원사무 처리 시에 구비서류를 제출받는 대신 구비서류에 해당되는 주민등록 등 행정정보를 직접 조회·확인하는 시스템을 말한다. 현재 행정정보공동이용시스템을 통하여 행정기관 등에서 열람할 수 있는 구비서류는 71종이다.

그러나 현재의 행정정보공동이용시스템은 사실상 개인정보의 공동이용을 다루고 있으면서도 이를 언급하지 않은 채 '일반행정정보 공동이용'과 '개인정보 공동이용'을 묶어서 다루고 있다. 또한, 행정정보공동이용센터조차 행정정보공동이용 제공정보 중에서 개인정보를 포함하고 있는 정보에 대해 파악

하지 못하거나 파악하지 않고 있어 문제가 더욱 심각하다.

현재 행정정보공동이용시스템을 통해 행정정보를 공동이용하고 있는 이용기관은 379개로 나타나고 있다. 이에는 52개 중앙 행정기관, 262개 지방자치단체, 49개 공공기관, 16개 금융기관이 포함된다. 행정정보공동이용시스템을 통한 이용 실적은 2003년 306만 건에서 2007년 2,786만 건으로 크게 증가하였다. 행정정보공유추진단은 매년 정기 또는 수시로 일정 기관을 선정하여 실태점검을 하고 있으나, 개인정보의 오·남용에 대해서는 점차 주의를 기울이지 않고 있는 추세에 있다.

행정정보공동이용시스템을 이용한 담당공무원의 무단 열람이나 외부 유출 문제를 배제하기 어렵다. 담당공무원에 의한 정보유출은 행정정보공동이용시스템이 구축되면서 출현한 문제는 아니지만, 자신이 근무하는 기관의 개인정보DB만 볼 수 있었던 기존시스템과는 달리 다른 기관이 보유하고 있는 개인정보에까지 접근이 가능하게 되므로 정보유출의 파괴력이 훨씬 커지게 된다. 감사원 역시 정보열람자가 열람내역을 수동으로 입력하게 하여 열람내역 조작이 가능해지는 등 행정정보공동이용시스템의 정보 오·남용 방지 기능이 부실하게 개발되어 정보보호 안전성 확보가 곤란하다고 지적한 바 있다. 이에 2008년 국정감사에서 행정안전부는 향후에는 행정정보공동이용시스템과 시군구 행정정보시스템을 연계하여 상호간의 기록내역이 비교되도록 관계기관과 협의하여 추진하며, 정보주체의 열람청구권 보장 등 행정정보 열람내역에 대한 모니터링이 보다 강화될 수 있도록 제도 개선을 하겠다고 밝혔다.

한편, 행정정보공유추진위원회와 행정정보공유추진단은 행정정보의 공유를 확대하는데 주된 업무의 초점을 맞추고 있으며, 행정정보 공동이용에 따르는 개인정보 보호의 문제에는 별로 신경을 쓰지 않고 있고, 그 와중에 개인정보 공동이용이 무분별하게 이루어지고 있는 실태에 대해서도 별다른 관심이 없는 것으로 보인다. 이는 최근까지 23차에 걸쳐 있었던 행정정보공유추진위원회(소위원회)의 회의 안건에서도 잘 나타난다. 행정정보공유추진위원회는 시종일관 행정정보 보유기관이 공공·금융기관의 개인정보 오·남용에 대한 불안감으로 개인정보 공동이용을 꺼리는 것에 대해 이를 설득하는 입장을 취하고 있다.

행정기관 간에 개인정보를 공유하는 것에 대한 설문조사에서 60% 이상이 바람직하지 않다는 의견을 표명한 것을 감안하면, 행정정보공동이용시스템을 통한 개인정보 공동이용에 대해서는 좀 더 신중한 접근이 요구된다 하겠다.

## Ⅱ. 행정기관 간 개인정보 공유

「전자정부법」상의 ‘행정정보 공동이용’이란 개인정보를 포함하여 행정기관이 보유·관리하고 있는 행정정보를 다른 행정기관 또는 공공기관 등이 “정보시스템을 통하여” 공동이용하는 것을 말한다. 여기에서 개인정보의 공동이용은 구체적으로 언급되고 있지 않으나, 각 행정기관이 보유·관리하고 있는 개인정보파일, 즉 개인정보DB들을 상호 연동내지는 연계하는 방식으로 이루어질 것이다.

행정기관 간 개인정보의 이용 및 제공 문제와 관련하여, 제 역할을 해야 하는 공공기관 개인정보보호심의위원회가 거의 기능을 하지 못하고 있는 상황이며, 오히려 논란의 소지가 있는 개인정보의 이용 및 제공을 정당화해주는 역할마저 하고 있어 문제가 되고 있다.

개인정보보호심의위원회는 1995년 10월 18일 운영세칙제정을 위해 제1차 위원회가 열린 이래 2008년 3월 27일 회의까지 단 10번만 개최되었을 뿐이다. 1999년과 2000년, 2007년에는 단 한 번도 위원회가 열리지 않았고, 1997년과 2001년, 2002년에 각각 한 차례씩 있었던 위원회는 서면심의로 대신하였다. 2009년 들어서도 개인정보보호심의위원회 회의는 정례화 되고 있지 않으며 서면심의가 이루어지고 있어 운영이 활성화되고 있다고 보기 어렵다. 최근 교육행정정보시스템(NEIS)의 통합 문제가 논란이 되고 있는데, 이 또한 개인정보 보호와 관련된다는 점에서 개인정보보호심의위원회가 다루어야 할 사안이 분명함에도 불구하고 교과부에서 이에 대한 안을 제출하면서 개인정보보호심의위원회의 검토를 거치지 않았다.

개인정보보호심의위원회의 심의 사항 중 하나는 ‘처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용 또는 제공하는 것에 관한 사항’(「공공기관의 개인정보보호에 관한 법률」 제10조 제3항 제2호)인데, 현재까지의 심의 결과를 보면 개인정보의 목적 외 이용 또는 제공을 제대로 검토하는 것이 아니라 오히려 논란의 여지가 있는 사안들을 정당화해주는 역할을 하고 있다. 이는 근본적으로 공공기관 개인정보보호심의위원회를 거칠 경우 목적 외 활용도 용인될 수 있도록 하고 있는 「공공기관의 개인정보보호에 관한 법률」 규정 자체가 문제임을 보여준다.

공공기관 개인정보보호심의위원회의 심의를 거치지 않고 이루어지는 개인

정보 이용·제공 요청이 개인정보 공동이용에서 더 큰 문제가 되는데, 이는 주로 개인정보파일 관리에 관한 사항이어서 이에 대한 수집·유통 실태를 살펴보았다. 2008년 공공기관이 보유한 개인정보 파일을 전수 조사한 결과 2008년 말 현재 2만3652개 기관에서 총 32만2357개 파일을 보유하고 있는 것으로 나타났다. 이 중 일반인의 열람대상에서 제외되고 행정안전부장관의 공고대상에서도 제외되고 있는 개인정보파일을 감안하면, 실제 작성·활용되는 개인정보파일은 당연히 통계수치보다 많을 것이다.

이 중 파일 약 8만1천여 개를 유정현 의원실에서 분석한 결과에 따르면, 보유 파일의 양태도 문제가 심각한 것으로 드러났다. 뚜렷한 이유 없이 영구 및 준영구 보존하고 있고, 주민등록번호는 관행처럼 대부분 수집하고 있는 것으로 나타났다. 만약 영구보존 파일 15,406개(19%)와 보존기간이 거의 영구인 준영구 파일 24,638개(30.4%) 등 총 약 4만 개(전체의 49.4%)의 파일이나, 주민번호가 포함된 파일 60,693개(74.9%)가 제대로 관리가 안 된다면 언젠가 유출, 도용, 불법 제공될 것이라는 점에서 문제가 심각하다.

또한, 전체 보유 개인정보파일 중 15.2%의 파일에서 개인정보를 제공하는 것으로 조사되었다. 이는 대부분 법률에 근거하여 제공되는 것이지만, 일부 업무상 필요에 의해 제공하거나 제공 근거가 없는 경우도 있었다. 또한 문서를 통한 이용·제공이 잘 이루어지지 않고 있는 것으로 나타났으며, 처리정보이용제공대장의 관리도 잘 되지 않고 있었다. 또한, 공공기관이 보유하고 있는 개인정보파일의 파기 현황이 제대로 파악되지 않고 있는 점도 문제로 지적할 수 있다.

## 제2절 수사/범죄경력(경찰) 영역

경찰은 일차적인 범죄수사기관으로서 수사 및 범죄 경력과 관련한 자료를 생성하고 관리하고 있지만 그 실태에 대해서는 잘 알려져 있지 않다. 이는 범죄의 수사에 관한 사항을 기록한 개인정보파일의 경우 「공공기관의 개인정보보호에 관한 법률」에서 규정한 여러 의무에서 포괄적으로 예외를 인정하는데 따른 것으로 보인다.

### Ⅰ. 수사자료표

수사자료표 상의 개인정보의 수집과 유통 및 정보주체의 참여권은 「형의

실효 등에 관한 법률」에 의하여 규정되어 있다. 이는 전과자의 정상적인 사회복귀를 보장하기 위한 법률상 목적을 달성하기 위한 것으로서, 수사경력이나 범죄경력에 대한 조회의 오남용 등으로 전과기록 등 민감한 개인정보가 부당하게 유출되는 것을 방지하고자 한 것이다.

그러나 수사자료표에 대한 조회의 경우, 일차적으로 자조직인 경찰관서 내에서의 오남용에 따른 인권침해와 불법성이 문제로 지적되어 왔다. 이는 관련 법령에서 조회의 목적을 '범죄수사 또는 재판을 위하여 필요한 경우'라고 포괄적으로 규정한 데 따른 문제로 보인다. 관련 규칙의 경우에도 구체적인 목적을 한정하지 않아 오남용될 위험성이 상존한다.

타기관에 제공할 수 있는 사유 역시 보다 세밀하게 명시되어야 할 것으로 보인다. 특히 「보안업무규정」에 따른 신원조회를 위해 수사자료표가 제공되는 경우는 인권침해 소지가 크며, 형의 실효 이후에도 범죄경력자료가 삭제되지 않는 상황에서 사실상 기간 제한 없이 그 자료가 타기관에 제공되는 것은 문제가 있다.

수사경력자료와 범죄경력자료에 대한 삭제 규정 역시 필요하다. 검사의 혐의없음・공소권없음・죄가안됨 또는 기소유예의 불기소처분이 있는 경우, 법원의 무죄・면소 또는 공소기각의 판결이 확정된 경우, 법원의 공소기각의 결정이 확정된 경우에도 수사경력자료가 즉시 삭제되지 않고 법정형에 따른 보존기간을 두고 있는 것은 문제이다. 범죄경력자료에 대해서는 해당자가 사망할 경우를 제외하고는 그 삭제에 대한 규정이 아예 존재하지 않는다. 형이 실효한 때에는 수사자료표를 함께 삭제하는 것이 바람직해 보인다.

또한 수사자료표에 대한 정보주체의 열람권 행사를 보장함에 있어서, 수사자료표의 현 상태 뿐 아니라 수사자료표의 조회 및 타기관 제공 현황에 대해서도 함께 공개되어야 하며 그 정정 및 삭제 청구권도 보다 적극적으로 보장될 필요가 있다.

## Ⅱ. 범죄정보관리시스템(CIMS)

범죄정보관리시스템이 방대한 양의 개인정보의 수집과 관리를 하면서도 마땅한 법률적 근거를 갖추지 않은 채 운영되고 있는 점은 시급히 시정될 필요가 있다. 특히 범죄정보관리시스템의 범죄정보는 수사자료표 상의 수사경력자료 및 범죄경력자료와 별도로 구축되어, 수사 및 범죄에 관한 개인정보의 수집과 유통에 대한 「형의 실효 등에 관한 법률」상의 법률적 의무를 형해

화할 우려가 높다.

범죄정보관리시스템에는 피의자를 상대로 받은 신문조서는 물론 피해자와 참고인에게서 받은 진술조서, 수사보고서, 체포・구속・압수수색영장 신청서, 의견서 등이 모두 들어가 있다. 소년신원조사표, 비행성예측 자료표 등 매우 민감한 내용도 포함되어 있다. 이와 같은 서식의 종류가 모두 301가지에 이른다. 피의자 뿐 아니라 피해자 및 참고인에 대한 개인정보도 포함되어 기본적 인권을 침해할 가능성이 높고, 피해자 정보 등 민감한 개인정보가 유출될 위험성도 존재한다. 특히 수사보고서와 조서까지 저장하고 있는 점은, 경찰 수사가 종료되면 사건 기록을 검찰에 송치하도록 한 원칙에 배치될 뿐 아니라 부정확한 정보의 저장으로 인한 추가적인 인권 침해를 유발할 가능성이 있다. 특히 범죄정보관리시스템에서 수사 및 범죄 관련 개인정보의 생성과 관리가 수사자료표와 별도로 이루어지고 있는 점은 큰 문제이다. 단적인 예로, 경찰의 조사 이후에 검찰이 무혐의로 처분하였거나 법정에서 무죄 판결을 받은 사건의 경우 수사자료표는 「형의 실효 등에 관한 법률」에 따라 삭제가 되지만 범죄정보관리시스템에서는 경찰이 수사할 당시의 자료가 그대로 남아 있을 수 있는 것이다.

한편, 범죄정보관리시스템에 입력된 개인정보를 자조직 내에서 조회하거나 타기관에 제공하는 데 대한 구체적인 제한이 존재하지 않기 때문에 그로 인한 오남용과 불법적인 이용 사례가 지적되어 왔다. 또한 자료의 삭제를 원칙적으로 금지하고 있기 때문에 잘못된 정보가 잔존할 위험성이 더욱 높으며, 그에 따른 정보주체의 권리 행사 또한 제약하고 있다.

범죄정보관리시스템에 입력된 개인정보에 대해 정보주체가 열람청구권을 행사할 수 있도록 보장한 명시적 규정은 존재하지 않으나 「공공기관개인정보보호법」에 의해 일반적인 열람이 허용되고 있다. 그러나 제3자의 제공내역은 비공개 대상정보로 청구할 수 없다. 불법적 조회나 제공에 대해서는 국가의 책임이 인정되어 온 만큼 정보주체 역시 자신의 개인정보에 대한 조회와 제공 현황을 언제든지 직접 확인하고 그에 따른 권리 행사가 이루어질 수 있어야 한다.

## 제3절 정보통신 영역

### Ⅰ. 포털 업체

포털에 집적되어있는 개인정보의 양은 실로 방대하다. 2009년 2월 현재 네이버의 가입자 수는 3,300만 명, 다음의 가입자 수는 3,500만 명으로서 거의 대부분의 대한민국 국민의 개인정보를 보유하고 있다.

본 연구에서는 네이버, 다음 등 주요 7개 국내 포털과 외국계 회사인 구글, MSN을 대상으로 개인정보 수집 및 유통실태를 조사하였다. 이를 위해 각 포털의 약관과 개인정보 취급방침(2009년 7월 기준)을 상호 대조 및 분석하였으며, 포털의 이용자를 섭외하여 정보공개청구 및 정책질의를 통해 이용자의 열람 및 정정·삭제 청구권 보장 실태조사를 진행하였다.

포털이 필수수집항목으로 수집하고 있는 개인정보 중에는 주소, 연락처, 성별, 심지어 직업까지 서비스 이용에 필수적이라고 보기 힘든 정보들이 포함되어 있었다. 대체본인확인 수단으로 지난 2005년 10월 도입된 i-PIN 이용자는 전체 인터넷 이용 인구의 3% 수준에 머물고 있으며, 주요 포털들은 여전히 주민등록번호를 수집하고 있었다. 포털들은 자동수집항목을 고시하고 있었지만, 그 구체적인 내용은 업체마다 차이가 있었고 대부분 세부적인 내용은 영업비밀이라는 이유로 공개하고 있지 않았다.

포털들은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 규정된 개인정보취급방침 공개 의무를 형식적인 측면에 있어서는 비교적 잘 준수하고 있었다. 그러나 개인정보 제3자 제공의 경우, 현재 제공을 하고 있는지, 제공을 하였다가 계약이 파기되어 현재는 게시를 하지 않는 상태인지 등에 대한 구체적인 언급을 통해 정보주체인 이용자에게 정확한 정보를 제공해야 할 필요가 있다. 또한 공개된 개인정보취급방침이 제대로 이행되고 있는지는 별개의 문제이다. 지난 2008년 방송통신위원회는 해지자의 개인정보 미파기, 법정대리인의 요건에 맞지 않는 자를 법정대리인으로 등록하는 등의 개인정보 유용행위를 한 포털에 대해 시정조치 및 과태료를 부과한 바 있다.

포털에 개인정보 열람청구를 진행한 결과, 포털에서는 가입 시 수집한 개인정보에 대한 DB만 구축하고 있는 것으로 보인다. 포털측은 로그인 시 이용정보와 비로그인시 이용정보를 매칭하여 관리하지 않는다고 공식적으로 답변하였다. 타겟 마케팅은 이용자가 포털 가입 시 입력한 기본 정보(성별, 나이, 지역)에서 개인정보를 제거한 통계정보와 IP주소를 근거로 이루어지고 있는 것으로 보인다. 포털측은 이용자의 포털 이용 패턴과 이용자의 개인정보 DB가 서로 연동되어 관리되지는 않는다고 밝혔다.

이메일이나 개인정보 등을 수사기관에 제공한 내역에 대한 열람 청구에 대해서는 포털별 정책에 따라 확인내역을 제공 해주거나 확인자체가 관계법령

에 의해 불가능하다는 답변을 하기도 하였다.

전반적으로 포털의 개인정보취급방침은 유사한 구조를 보였으나 세부적인 내용은 각 사별로 차이를 보였다. 이용자들이 개인정보 관리 실태를 보다 정확하게 알 수 있도록 더 세부적이고 정확한 정보를 공개하도록 할 필요가 있다.

## Ⅱ. 이동통신사 및 초고속인터넷업체

전 국민 대다수가 이동통신 서비스 및 초고속인터넷 서비스를 이용하고 있다고 봐도 과언이 아니다. 그만큼 통신업체들은 대규모의 개인정보 데이터베이스를 구축·운용하고 있다. 따라서 약간의 관리 소홀로도 대규모 개인정보 유출, 혹은 유용으로 이어질 수 있다. 2008년 하나로텔레콤이 600여 만 명의 고객정보를 유용한 사례가 대표적이다.

통신업체들은 이용자들이 제공한 개인정보 외에도 서비스 이용 과정에서 생성된 개인정보를 보유하고 있다. 그러나 각 통신업체들이 공개하고 있는 개인정보 취급방침만을 보아서는 생성정보에 구체적으로 어떠한 개인정보 항목이 포함되어 있는지 모호하다. 특히, 결합상품의 출시가 증가하고 있는 만큼, 각 서비스 별로 수집되는 개인정보 항목을 구체적으로 명시할 필요가 있다.

통신업체들이 업무위탁이나 제휴관계 등을 통해 개인정보를 제공하는 업체가 수천 개에 달한다는 사실은 주목할 필요가 있다. 제공 업체가 증가할수록 통신업체의 이들에 대한 관리, 통제는 취약해질 수밖에 없다. 이런 상황임에도 통신업체는 제휴업체나 위탁업체의 전체 목록을 개인정보 취급방침에 공개하고 있을 뿐, 해당 정보주체별로 제3자 제공 내역에 대한 열람은 대체적으로 허용하고 있지 않고 있다. 또한, 개인정보 취급방침만 보아서는 제3자 제공에 자신의 동의가 필요한 것인지, 필수적으로 제공되는 것인지 알기 힘들다. 지난 2008년에는 대다수 이동통신사 및 초고속인터넷업체에서 정보주체의 동의나 고지 없이 취급위탁을 한 이유로 방송통신위원회의 시정조치를 받은 바 있다.

서비스 가입 내역이나 결제 기록과 같은 개인정보를 통신업체 홈페이지를 통해 정보주체가 열람할 수 있도록 제공하고 있는 것과 같이, 정보주체별 제3자 제공 내역과 동의의 방법(예를 들어, 요금 정산과 같이 동의가 없어도 되는 것인지, 별도의 동의가 필요한 것인지 등)에 대해서도 홈페이지를 통해

쉽게 열람할 수 있도록 할 필요가 있다. 자신의 개인정보가 어디에 제공되었는지 알 수 없다면, 정보주체가 자기정보에 대한 결정권을 행사하기는 불가능할 것이다. 또한, 현재 각 통신업체별로 제3자 제공이나 위탁과 관련하여 자의적으로 구분하고 있기 때문에, 방송통신위원회에서 이와 관련한 구체적인 가이드라인을 마련할 필요가 있다.

또한, 통신사들은 1만여 개가 넘는 판매점을 통해 고객 유치 및 관리를 하고 있는데, 판매점의 부실한 개인정보 관리 문제는 이미 몇 년 전부터 반복적으로 지적되어 왔다. 방송통신위원회는 2009년 5월 1일, 판매점을 통한 개인정보 유출을 막기 위해 이동통신 3사가 공동으로 '개인정보 관리체계 자율개선방안'을 마련했다고 발표하였다. 그러나 이동통신사와 판매점 사이의 불명확한 계약관계에 대한 해결책은 제시되지 않아 판매점의 개인정보 보호조치를 제대로 통제할 수 있을지 의문이다.

각 통신업체의 개인정보취급방침도 각 사별로 차이가 있었는데, 개인정보취급방침을 통해 공개해야할 사항이 누락되거나 법 조항 등이 잘못 기술된 경우도 있었다. 수백만 명의 가입자를 보유하고 있는 업체라면 개인정보취급방침을 좀 더 세심하게 관리할 필요가 있다.

한편, 본 연구에서 각 통신업체에 대해 정보주체의 열람권 보장 실태에 대한 조사를 수행한 결과, 법에 명시된 열람권이 제대로 보장되고 있지 않음을 확인할 수 있었다. 각 통신업체들은 홈페이지를 통해 본인 정보에 대해 열람 및 수정할 수 있도록 하고 있으나, 제3자에게 제공한 내역을 열람할 수 있도록 하고 있는 사업자들은 없었다. 각 업체가 개인정보취급방침에 공개한 취급위탁업체 및 제휴업체의 목록만으로는 실제로 내 개인정보가 어떤 업체에 제공되었는지 파악하기 힘들다. 각 이동통신사들은 대리점 방문을 통해 일정 기간 동안의 통화내역을 열람할 수 있도록 하고 있으나 기지국 정보는 공통적으로 포함하고 있지 않았다. 개인정보의 제3자 제공내역 역시 제대로 보장되지 않고 있었다. 일부 업체는 제3자 제공내역을 제공하였지만, 개인정보취급방침을 확인하라고 한 경우가 많았으며, 수사기관 등에 제공한 내역에 대해서는 대부분이 제공할 수 없다고 답변하였다.

서비스 간 융합 등으로 인해 업체 간 개인정보의 유통이 급증하고 있는 상황에서, 정보주체가 자신의 개인정보에 대한 결정권을 확실히 보장받기 위해서는 내 개인정보가 어떻게 유통되고 있는지에 대해 정확히 알 수 있어야 한다. 즉, 이제 '개인정보'에 대한 열람뿐만 아니라, '개인정보의 제3자 제공 내역'에 대한 열람이 더욱 중요해지고 있는 것이다. 특히, 방대한 개인정보를

수집하고 있고, 수많은 업체들과 위탁이나 제휴 관계를 맺고 있는 통신 영역에서는 두 말할 나위도 없다.

## 제4절 금융 영역

금융 분야는 개인정보의 집중 및 공동 활용이 가장 광범위한 분야 중 하나다. 개별 금융기관에서 생성된 개인신용정보와 공공기관에서 보유하고 있는 개인정보가 종합/개별신용정보집중기관 및 신용조회회사를 통해 집중되며, 이렇게 집중된 정보는 개별 금융기관 및 공공기관에 활용된다.

2009년 10월 2일 시행된 개정 「신용정보의 이용 및 보호에 관한 법률」은 △ 개인의 동의제도 강화, △ 신용정보관리·보호인의 지정·운용 의무화, △ 개인신용정보 제공·이용 동의 철회권 신설 등 개인신용정보주체의 권리를 강화한 측면이 있지만, 다른 한편으로는 △ 신용정보회사의 업무 확대, △ 신용조회회사 또는 신용정보집중기관의 공공기관에 대한 신용정보 제공 요청 근거를 확대하는 등 신용정보 공동 활용의 폭을 넓혔다.

신용정보회사등과 공공기관의 개인정보 공유가 지나치게 광범위하게 이루어지고 있다. 관련법에서 규정한 개인정보 보호 규정에도 불구하고, 공공기관이 보유하고 있는 개인정보가 신용정보라는 명목으로 민간에 제공될 수 있고, 또한 그 범위마저 자의적으로 규정될 수 있어 신용정보와 관련해서는 자칫 개인정보의 보호를 위한 관련법의 취지가 훼손될 위험이 있다. 「신용정보의 이용 및 보호에 관한 법률」에서 신용정보회사등과 공공기관 간에 공유할 수 있는 신용정보의 범위에 대해서 활용 목적에 맞게 보다 세부적이고, 제한적으로 규정할 필요가 있다.

또한, 개인신용정보의 집중·활용과 관련하여 '개인신용정보의 제공·활용 동의서'를 받고 있으나 제공대상 기관이나 이용목적이 추상적으로 규정되어 있고, 동의를 하지 않으면 서비스를 제공받지 못할 수도 있어 형식적인 것에 머물고 있다. 신용정보제공·활용 동의서가 진정한 동의 절차가 되기 위해서는, 정보주체의 동의 없이는 신용정보집중기관 및 신용조회회사에 신용정보를 제공할 수 없도록 하고, 동의 여부를 서비스 거부의 근거로 삼을 수 없도록 법에서 명확하게 규정할 필요가 있다.

영업의 양도·양수와 관련한 개인신용정보의 이전과 관련한 규제는 오히려 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」보다 낮은 수준인데, 최소한 그와 비슷한 수준으로 높아질 필요가 있다. 한편, 금융지주회사 내에

서는 금융거래정보와 개인신용정보가 자회사간에 공유된다. 이는 금융지주회사의 경영 효율성을 높이기 위한 것인데, 정보주체의 입장에서는 개인정보 자기결정권에 대한 중대한 침해가 아닐 수 없다.

각 금융기관들은 개인정보취급방침, 신용정보활용체제 등 여러 개의 개인정보 보호규정을 홈페이지를 통해 공시하고 있는데, 정보주체가 쉽게 이해할 수 있도록 체계적으로 정리될 필요가 있다. 특히, 개인정보의 제3자 제공과 관련한 사항(제3자 제공기관이나 위탁기관, 제공되는 개인정보의 종류, 목적 등)이 보다 상세하게 명시될 필요가 있다.

개인정보를 서로 다른 기관 간에 공유하는 경우가 증가하면서, 개인정보의 열람이나 제공내역을 정보주체가 인식할 필요성이 증가하고 있다. 「신용정보의 이용 및 보호에 관한 법률」은 신용정보에 대한 열람 및 정정 청구권, 무료열람권, 신용정보제공사실의 통보요구권, 개인신용정보 제공·이용 동의 철회권 등을 보장하고 있다. 이에 따라 신용정보집중기관이나 신용조회회사 등의 홈페이지를 통해서는 이를 열람할 수 있지만, 개별 금융기관의 홈페이지를 통해서도 개인신용정보의 조회 내역이나 제3자 제공내역을 쉽게 열람할 수 있도록 제공할 필요가 있다.

## 제5절 보건의료 영역

개인 의료정보는 가장 민감한 개인정보 중 하나로서 엄격한 보호가 필요함에도 불구하고, 보건의료 관련 법률에서는 아직 개인정보 보호원칙을 체계적으로 반영하지 못하고 있다. 아직 보건의료 영역에서 보호해야 할 '개인정보'의 개념과 보호범위조차 명확하게 정의되어 있지 못한 상황이다. 본 연구에서는 병원, 약국, 보건소 등 의료정보를 생성하는 '생성기관'과 국민건강보험공단, 건강보험심사평가원 등 생성기관으로부터 정보를 제공받아 건강보험 업무 등을 위해 활용하는 '취급기관'으로 나누어 의료정보의 수집, 유통 실태를 분석하였다.

생성기관에서의 개인정보 수집·유통실태 조사를 통해 파악된 문제점과 개선방안은 다음과 같다.

일부 병원의 경우 결혼여부, 학력, 종교 등 민감한 개인정보도 수집하고 있는 반면, 개인정보의 수집이나 제3자 제공과 관련한 동의나 고지 체계는 제대로 갖춰져 있지 않았다. 병원에서 보유하고 있는 의료정보는 타 병원, 약국, 국민건강보험공단 등 취급기관, 경찰이나 법원 등 공공기관에 제공된다.

의료정보의 제3자 제공과 관련한 근거와 절차를 법률에서 구체적이고 명확하게 규정할 필요가 있다. 또한, 「의료법」에서는 진료기록부의 보존 기간을 10년으로 규정하고 있으나, 상당수의 병원에서 의료기록을 사실상 준 영구적으로 보존하고 있는 것으로 나타났다. 환자의 치료나 건강을 위해 꼭 필요한 경우가 아니라면, 보존기간 이후에는 의료기록을 파기하도록 법에서 명시할 필요가 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 개인정보 취급방침이나 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보활용체제와 달리 보건의료 관련 법률에서는 규정이 없어, 개인 의료정보의 수집, 제3자 제공, 보호정책, 정보주체의 권리 등에 대한 개별 의료기관의 정책에 대해 파악하기 힘들다. 개별 의료기관마다 개인 의료정보의 보호와 보안을 위한 대책을 담은 지침을 마련하고, 그 주요 내용에 대해 공개하도록 해야 한다. 의료정보의 유출이나 무단 열람 등의 전반적인 실태는 파악하기 힘드나, 언론보도나 설문조사 결과에 의하면 의료정보에 대한 무단 열람 사례도 적지 않을 것으로 짐작된다. 또한, 병원 정보화에 따라 전자의무기록(EMR)과 같은 새로운 시스템이 도입되고 있음에도 불구하고, 적절한 정보보안 시스템 구축은 미흡한 것으로 보인다. 의료기관의 정보보안에 대한 정확한 실태조사와 함께, 보건복지가족부는 개인정보 보호와 보안을 위한 지침을 제시할 필요가 있다.

「의료법」등에서 환자의 열람권을 규정하고는 있으나, 정정·삭제권은 규정하고 있지 않다. 열람권의 경우에도, 자신의 의료기록에 대한 열람뿐만 아니라, 조회 내역 및 제3자 제공 내역에 대한 열람권을 포함할 필요가 있다.

국민건강보험공단 등 취급기관에서의 개인정보 수집·유통실태는 보다 심각하다.

취급기관에는 각 의료기관에서 생성된 의료정보가 집적된다. 국민건강보험공단의 경우에는 의료정보뿐만 아니라, 주민등록정보, 사업자등록자료, 출입국 기록, 장애인자료, 토지 및 자동차 자료, 연금자료 등 개인의 인적사항 및 재산 등에 대한 방대한 기록을 보유하고 있다. 취급기관이 보유하고 있는 개인정보는 정보주체의 동의를 받고 직접 수집한 것이라기보다는 법에 근거하여 타 기관으로부터 제공받는 경우가 대부분이다. 그런데 취급기관이 개인정보를 제공받아 보유할 수 있는 법적 근거가 포괄적인 경우가 많다. 이는 자칫 과도한 개인정보의 수집을 초래할 수 있는데, 관련 법률에서 각 취급기관이 업무 수행을 위해 수집할 수 있는 개인정보의 범위를 엄격하게 규정할 필

요가 있다.

취급기관이 보유하고 있는 개인정보는 시스템 연계를 통해, 혹은 요청에 의해 타 기관에 제공된다. 특히, 국민건강보험공단의 경우 2008년부터 2년 동안, 공단 내 각 부서에서 총 733회, 1억 건이 넘는 개인정보를 요청에 의해 타 기관에 제공한 것으로 나타났다. 즉, 공단의 본래 업무를 수행하기 위한 목적 외로 공단이 보유하고 있는 건강보험 정보가 수시로 제공되고 있음을 확인할 수 있었다. 이렇게 광범위하게 애초 수집 목적 외로 개인정보가 제공된다면, 수집목적 내 이용이라는 개인정보 보호 원칙은 거의 의미가 없게 된다. 국민건강보험공단을 포함하여 취급기관이 보유하고 있는 개인정보의 제3자 제공을 엄격하게 제한할 필요가 있으며, 개인정보가 제공될 경우 정보주체의 동의 혹은 최소한의 통지 절차가 필요하다.

취급기관이 보유하고 있는 개인정보파일 중에서도 영구, 혹은 준영구적으로 보존되는 것들이 다수 존재했다. 적절한 보유기간에 대한 전문가들의 검토가 필요하며, 보유목적 달성 시 폐기의무를 의료 관련 법률에서 세밀하게 규정할 필요가 있다.

국민건강보험공단, 건강보험심사평가원 등을 통한 정보 유출이나 무단 열람의 문제는 거의 매해 언론이나 국정감사 등을 통해 불거지고 있다. 이러한 무단 열람의 문제는 국민건강보험공단이 모니터링 시스템을 가동한 이후에도 발생하고 있다. 직원들에 대한 교육, 정보유출이나 무단열람에 대한 중징계 등의 조치와 함께, 취급기관 자체가 보유하고 있는 개인정보 자체를 최소한으로 제한할 필요가 있다.

취급기관의 경우 「공공기관의 개인정보 보호에 관한 법률」에 따라 정보주체의 열람 및 정정·삭제 청구권을 보장하고 있지만, 정보주체가 자기정보에 대한 제3자 제공 내역을 열람할 수 있도록 법에서 명확하게 규정할 필요가 있다.

의료정보는 가장 민감한 개인정보임에도 불구하고, 의료관련 법률이 개인정보 보호원칙을 제대로 반영하지 못하고 있는 것은 심각한 문제이다. 개인의료정보의 보호를 위한 법안 마련이 시급해 보인다. 이에는 의료정보의 열람 내역이나 제3자 제공 내역에 대한 정보주체의 열람권이 반드시 보장될 필요가 있다. 왜냐하면, 보건의료 영역에서는 생성기관에서 보유하고 있는 의료정보가 다수의 취급기관에 집적되고, 또 이렇게 집적된 개인정보가 타 공공기관을 통해 공유되고 있기 때문이다. 이런 상황에서 개인정보자기결정권은 유명무실해질 수밖에 없다.

## 제6절 교육 영역(NEIS 도입 및 통합)

NEIS는 추진과정에서 개인정보 유출 가능성이 제기되면서 전교조 등 인권단체들이 반대하자, 2004년 3월 정부는 인권침해 소지가 제기된 교무・학사, 입(진)학, 보건 업무를 새로 구축하기로 방침을 확정하고, 2006년 2월에 개발을 완료하여 2006년 3월 전면 시행에 들어갔다. 교육부는 2006년 9월부터 '학부모서비스'를 시작했으며, 2009년 현재 4개 영역 38종의 서비스를 제공하고 있다. 서울시 교육청이 학부모를 대상으로 관심있게 이용한 항목을 조사한 결과에 따르면, 가장 많은 응답자가 성적을 꼽았다(19%). 학부모서비스는 2009년 현재 171만 2,366명이 누적 이용한 것으로 나타났다.

NEIS는 2006년부터 교무업무(교무・학사, 입・진학, 보건)를 학교급별 단독 또는 그룹서버 형태로 3,000여대의 서버를 분리 운영하고 있다. 그런데 2009년 교육부는 지난 4년간 그룹서버를 시범 운영하는 과정에서 단 한건의 개인정보 유출이나 보안침해 사고가 없었다는 것을 근거로, 서버운영의 비효율성 제거와 노후서버 교체 등 서버운영의 최적화 방안을 마련하기 위해 NEIS를 시・도 교육청 단위로 통합하겠다고 밝혀 논란이 되고 있다. 또한 정부는 학생들의 상・벌점제도인 그린마일리지를 NEIS와 연계해 상벌점 기록이 평생 남도록 하는 방안을 추진하고 있는데, 이에 대해 학생들은 사생활 침해와 학생 진학 영향 등을 우려하고 있다. 나아가 교육부는 일선 시・도교육청을 통해 시범운영 중인 학교회계시스템 '에듀파인'(edufine)을 2010년 3월부터 전국 학교를 상대로 확대 시행할 계획으로 있다.

한편, 국가인권위원회는 정보주체인 재학생이 NEIS에 수집된 본인정보를 정보주체 스스로 열람할 수 없도록 한 것은 인권침해라고 판단하고, 관계기관에 대책 마련을 권고하였다.

NEIS의 통합 및 다른 시스템과의 연계에 따른 논란이 막대한 사회적 비용을 초래할 가능성을 염두에 둔다면 NEIS 도입 시의 시행착오 경험에서 교훈을 얻어 이를 전격적으로 추진하기에 앞서 사회적인 합의를 도출해내는 노력이 선행될 필요가 있다고 본다.

# 제3장 특성별 개인정보 수집·유통 실태

## 제1절 CCTV

2002년 12월 서울시 강남구에 범죄예방을 위한 CCTV가 시범 설치된 후 방범용 CCTV를 비롯한 공공기관의 CCTV가 크게 증가하여왔다. 2009년 4월 현재 총 241,415대의 공공기관 CCTV가 설치·운영되고 있는 것으로 나타났다. 그러나 이를 규제하는 법률은 비교적 최근에야 마련되었는데, 2007년 11월 「공공기관의 개인정보 보호에 관한 법률」에 CCTV에 대한 규정이 포함된 것이다. 그러나 그 구체적인 규정 및 실태가 법률의 제정 취지와 어긋나는 경우가 많았다.

CCTV는 매우 광범위한 규모로 다양한 개인정보를 수집하는 개인정보 자동수집장치이기 때문에 필요최소한으로 설치하도록 설치 시점부터 사전적으로 규제하는 것이 중요하다. 그러나 법률상 공공기관의 CCTV 설치가 매우 폭넓게 인정되고 있는 반면, 의견수렴은 형식적으로 이루어지고 있었다. 실제로 본 연구에서 서울시 자치구를 대상으로 방범용 CCTV 설치 과정에서 주민 의견수렴과정에 대하여 조사한 결과, 대개가 홈페이지 등을 통한 행정예고 등의 방법으로 안내하거나 소극적인 설문조사를 하는 데 그치고 있었다. 다수 주민들의 동의서를 받거나 공청회와 같이 비교적 적극적인 여론수렴 절차를 거친 자치구는 소수에 불과하였다. 법률상 CCTV 설치 목적을 명확히 한정하고, 주민 등 이해관계인에게 CCTV의 설치에 대한 동의 여부를 물을 때는 정보주체가 동의권을 충분히 행사할 수 있도록 상세한 정보제공과 함께 공청회 등 적극적인 의견수렴 형식을 갖추는 것이 바람직하다.

특히 공공기관의 CCTV 기록의 이용 및 제공에 대한 현행 규정이 그리 엄격하지 않은 상태에서, 각 자치구가 경찰관서에 위탁운영하고 있는 방범용 CCTV의 문제가 심각하였다. 위탁기관인 자치구가 수탁기관인 경찰관서에 일체의 운영을 일임한 채 그 구체적인 실태를 파악하고 있지 않았다. 특히 정해진 기간에 따라 삭제되는 CCTV 영상기록 원본과 별도로 경찰관서는 법률적 근거 없이 별도의 사본을 보유하고 있었는데 이러한 관행은 시정될 필요가 있다. 또한 서울 경찰관서 31개 가운데 12개 관서가 민간인 모니터 요원을 두고 있었으며, 일부 경찰서의 경우 모니터 요원 전원을 민간인 가운데 선발하는 등 그 실태가 심각하였다. 수사의 한 과정으로 이루어지는 방범용

CCTV 모니터링을 많은 경우 민간인이 담당하는 것은 우려스런 일이다. 자치구와 경찰의 역할분담에 있어 편의적인 측면이 있는 것이 사실이라 하더라도, CCTV의 운영주체와 그에 따른 책임 관계를 명확히 할 필요가 있다.

또한 정보주체가 CCTV에 대한 권리를 행사하는 것도 여의치 않았다. CCTV를 운영하는 많은 자치구가 개인화상정보 파일을 공개하지 않았으며 (서울의 경우 개인화상정보 파일을 보유하고 있음을 공개한 자치구가 전체 25개 구 중 동대문구, 동작구, 양천구, 중구 등 4개 구에 불과하였다), 방범용 CCTV의 경우 그 위치를 공개하지 않는 경우가 대다수였다. 이러한 이유에서인지 사실상 열람과 삭제 등 정보주체의 권리 행사가 이루어진 경우는 거의 보고되지 않았다.

최근 목적별·지역별로 CCTV 통합관제센터가 주목을 받고 있다. 그러나 기관 내 CCTV를 통합 관리하는 것은 방범용, 쓰레기 투기방지, 시설물 관리, 주차관리, 교통정보 수집 등 고유의 목적으로 설치된 CCTV를 다목적으로 사용하겠다는 것으로서, 개인정보 수집장치를 목적 외의 용도로 활용할 수 없도록 한 개인정보보호원칙과 현행 법률에 반하는 것이다. 기관 간 CCTV를 통합 관리하는 것은 지역 주민 등 이해관계인으로부터 의견수렴 및 동의를 받고 설치된 CCTV의 이용 범위를 넘어선 것으로서 정보주체의 권리를 형해화할 위험이 있다.

## 제2절 위치정보

정보통신기술의 발전으로 사물의 위치를 파악하는 능력이 고도화되고 있으며, 수집된 사물의 위치정보가 개인정보 데이터베이스와 연계됨으로써 개인 위치정보에 대한 접근이 가능해지게 된다. 개인 위치정보는 우선 「위치정보의 보호 및 이용 등에 관한 법률」에 의해 규제되는데, 동법이 위치정보를 수집하는 모든 종류의 기관/업체에 적용되는 것은 아니다. 예를 들어, 본 연구에서 주로 다룬 승용차 요일제, 고속도로 하이패스, 교통 카드같은 경우 주 운영기관/업체의 관련 규정은 (일부 연관된 조항이 있기는 하지만) 동법에 근거하지 않고 있었다.

2009년 10월 현재, 191개의 사업자가 위치정보사업자 혹은 위치기반서비스사업자로 허가를 받거나 신고되어 있었다. 위치정보는 위치정보사업자에 의해 수집되어, 위치기반서비스사업자에게 제공된다. 위치정보사업자가 위치기반서비스사업을 겸하는 경우도 많다. 위치기반서비스 현황에 따르면, 위치

정보사업자가 직접 위치기반서비스사업을 하는 경우가 아닌 경우, 대부분의 위치기반서비스사업자가 3개 이동통신사로부터 위치정보를 제공받고 있다. 위치정보사업자가 수집한 개인위치정보는 정보주체의 동의를 얻어 위치기반서비스사업자에게 제공된다. 그러나 이와 같은 위치기반 서비스는 비록 적법하게 이루어진다고 하더라도, 위치가 수집되는 대상의 프라이버시 침해 가능성을 배제할 수 없다. 자녀, 노인, 장애인 등에 대한 신변보호 서비스의 경우, 사회적 약자에 대한 보호라는 명분을 가지고 있지만, 경우에 따라 이들에 대한 감시로 기능할 수 있다. 차량 관제 서비스의 경우에도 물류 사업의 효율성을 높이기 위한 목적을 가지고 있지만, 동시에 차량을 운전하는 노동자 입장에서는 자신에 대한 감시로 인식될 수 있다. 한편, 방송통신위원회에 대한 정보공개 청구 결과에 의하면, 긴급구조를 위한 위치정보 제공건수는 매해 증가하고 있음을 알 수 있다.

위치기반서비스사업자에게 위치정보를 제공하는 주요 위치정보사업자는 이동통신사이다. 「위치정보의 보호 및 이용 등에 관한 법률」 제24조는 본인에 대한 위치정보 수집·이용·제공사실 확인자료 및 제3자에게 제공된 이유 및 내용 등을 열람할 수 있는 정보주체의 권리를 규정하고 있으나, 한 이동통신사에 대해 개인위치정보에 대한 열람청구를 해본 결과 이 권리가 제대로 보장되지 않고 있음을 확인할 수 있었다. 수사기관에는 제공되는 통화내역을 제3자도 아닌 정보주체에게 제공하지 않는 것은 정보주체의 알 권리를 과도하게 제한하는 것이다.

승용차 요일제의 경우, 서울 시내에 설치된 인식기를 통해 차량에 부착된 전자태그의 정보를 인식하여 위치정보를 수집하고 있으며, 전자태그 고유번호를 매개로 승용차 요일제 참여자 데이터베이스와 연계될 수 있어, 프라이버시 침해 논란이 제기되고 있다. 가입 시 '이용자 유의사항'에는 개인 위치정보의 수집 사실이 공지되고 있지 않았으며, 인식기를 통해 수집되는 위치정보도 10년 동안이나 보관되고 있었다. RFID 가이드라인에서 규정하고 있듯이, 지금이라도 프라이버시 영향평가를 실시할 필요가 있다.

하이패스의 경우에도 차량 통과 시에 고속도로 요금소에서 단말기 및 카드정보가 수집되고, 이를 매개로 고객정보와 연계됨으로써 개인 위치정보를 수집하고 있다. 하이패스 이용자는 선불/후불하이패스 홈페이지를 통해 위치정보를 포함한 거래내역을 조회할 수 있다. 이렇게 수집된 개인(위치)정보는 수사기관 등에 제공되고 있는데, 수사상 목적을 위한 것일지라도 개인위치정보를 제공받기 위해서는 영장을 제시하도록 하는 등 제공 절차를 보다 엄격하

게 할 필요가 있다.

버스, 지하철 등 대중교통 요금결제를 위한 교통카드 사용도 일반화되고 있다. 교통카드는 각 지자체별로 운영되고 있다. 서울시 교통카드의 경우 교통카드 이용 시 카드 내에 25개 정보가 기록이 되는데, 카드번호를 매개로 개인신상정보와 연계되면 개인위치정보가 된다. 버스 등 단말기에 기록된 교통카드 이용내역은 정산회사의 시스템에 집적되게 된다. 신용카드와 결합된 후불 교통카드는 은행 홈페이지에서 승하차 정보를 포함한 이용내역을 열람할 수 있다. 선불 교통카드의 경우에도 카드회사의 홈페이지를 통해 이용내역을 열람할 수 있는데, 「위치정보의 보호 및 이용 등에 관한 법률」을 근거로 승하차 정보는 제공하지 않고 있다. 그러나 기업 등을 대상으로 한 교통카드 상품의 경우에는 직원들의 교통카드 이용내역을 구매 기업에 제공하고 있었는데, 이는 자칫 노동감시의 수단이 될 수 있어 우려된다.

## 제3절 유전정보

「실종아동등의 보호 및 지원에 관한 법률」은 보호자가 있는 곳으로 복귀하고 싶은 아동등에게 그럴 수 있는 지적능력이나 판단능력이 충분하지 않은 경우 그들의 조속한 발견과 복귀를 돕기 위한 법률인 만큼, 검사대상자이자 정보주체인 실종아동등의 의사를 계속적으로 확인하고 반영할 수 있는 구조가 필요하다. 또한 유전정보는 사회적 차별로 이어질 수 있는 매우 민감한 개인정보인 만큼 그 수집 및 이용과 제공을 엄격하게 제한하려는 법률의 제정 취지를 훼손하는 일이 없어야 할 것이다.

그러나 국가가 유전정보를 채취하고 데이터베이스를 구축·운영하는 과정에서 다소 미흡한 점이 발견되었다. 특히 검사 시점에 본인이 아닌 법정대리인의 동의하에 채취가 이루어진 경우 이후 정보주체의 동의 철회 및 폐기 의사를 확인하여 반영할 수 있는 구조가 보장되어 있지 않았다. 한때 유전정보 데이터베이스에 그 유전정보가 편입되었다 하더라도, 유전정보의 주체인 시설 아동 등이 성년에 도달하거나 심신미약상태를 벗어나는 경우 폐기되어야 한다. 따라서 검사대상자가 과거 검사에 대한 동의 철회 여부를 확인하고 그에 따른 폐기 조치를 취할 수 있는 절차가 구체적으로 마련되어야 법률상 취지와 목적에 부합한다 할 것이다.

또한 기본적인 유전정보 관리 및 통계에 있어 국립과학수사연구소와 실종아동전문기관 간에 차이가 있는 것으로 드러났다. 이는 유전정보 관리의 허

술함으로 이어질 수 있기 때문에 개선될 필요가 있다.

## 제4절 통신 비밀

「통신비밀보호법」과 「전기통신사업법」 등 국가안보 및 범죄수사 등의 목적으로 통신의 비밀을 제한하는 현행 법률들은 통신 및 대화의 비밀과 자유에 대한 제한에 있어 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다. 그러나 그 실제 집행 실태를 검토하여 보면, 이 목적에 맞게 현행 법률이 정비되어 있고 그에 따른 집행이 이루어지고 있는지 의구심이 들지 않을 수 없다.

먼저 「전기통신사업법」에 의해 가입자 성명, 전화번호, 주민등록번호, 주소, 인터넷 아이디 등 이용자 인적사항에 대한 통신자료가 수사기관 등에 제공되는 건수는 해마다 급증하여 한해 제공건수 5백만 건을 넘어섰다. 통신자료 제공건수가 이처럼 높은 것은 현행 법률이 통신자료 제공을 요청할 때 필요한 절차를 엄격히 규정하지 않은데 따른 결과이다.

통화내역, 위치정보, 인터넷 IP주소 등 통신사실 확인자료를 정보수사기관에 제공하는 건수 역시 해마다 증가하는 추세에 있다. 이 역시 현행 법률이 통신사실 확인자료 제공을 요청할 때 범죄사실의 입증 등 필요한 절차를 엄격히 규정하지 않은 데 따른 결과이다. 특히 장래의 위치정보에 대하여 과거의 통신사실 확인자료에 대한 조항을 적용하여 완화된 절차로 그 제공이 이루어지도록 한 것은 통신사실 확인자료를 과거의 통신사실에 대한 자료로서 규정하였던 법률 개정 취지와 목적을 위배하는 것이다.

이메일 등 공개되지 않은 통신의 내용에 대한 감청은 대부분 국가정보원에 의해 집행되고 있었다. 이는 법원의 영장 심사 등 정보수사기관에 대한 감독이 제대로 이루어지지 못한 데 따른 것으로서, 허가서 한 장으로 우편물 검열과 유선전화·휴대전화·인터넷 메일에 대한 감청은 물론 인터넷 회선 전체와 대화에 대한 감청까지 한 번에 모두 실시하는 저인망식 감청이 이루어지고 있었다. 또한 현행 법률이 영장주의의 예외를 인정함으로써 편법·불법 감청으로 이어질 수 있다는 우려를 낳고 있고, 반면 영장 발부 후 감청을 실제 집행하는 과정에서는 아무런 사후 감독 규정을 두고 있지 않은 점은 큰 문제이다. 더불어 인터넷 회선을 오가는 신호 전체에 대한 패킷 감청은 그 사생활 침해 정도가 매우 심각하고, 대상자와 대상 통신내용을 특정할 수 없다는 점에서 재고되어야 할 필요가 있다.

한편 「통신비밀보호법」은 대상자의 알권리를 위하여 감청과 통신사실 확인자료 제공 및 송수신이 완료된 통신에 대한 압수·수색·검증의 대상자에게 그 집행을 통지하는 제도를 규정하고 있다. 그러나 수사기관의 수사 진행 여부에 따라 이러한 통지가 지연되거나 유예되고 있고, 「전기통신사업법」에 따른 통신자료의 경우에는 통지에 대한 규정 자체가 없기 때문에 실제 통지에 대한 권리는 충분히 보장되고 있지 않다.

# 제4장 설문조사 결과 분석

## 제1절 일반 시민 대상 설문조사 결과 분석

자신들의 개인정보가 수집되고 유통되는 시민들을 대상으로 한 설문조사를 통해 개인정보 수집·유통 실태와 개인정보 열람 및 정정·삭제 청구권 보장 실태에 관한 시민의식을 측정하여 우리나라 개인정보 보호와 권리에 관한 법제도 현황과 그 보장 등 실태분석을 위한 기초자료로 활용하고자 하였다. 설문대상은 전국 19세 이상 성인남녀 500명이며, 조사기간은 2009년 7월 18일 하루에 진행하였다. 총 13개의 선택형 설문문항으로 구성된 구조화된 질문지를 가지고 전화면접조사를 하였으며, 최대 허용 오차는 95% 신뢰수준 하에서 ±4.4%이다.

설문조사 결과 전반적으로 시민들은 개인정보 관리에 대한 인식에 있어 그 심각성을 절감하고 있다. 우선 개인정보 유출과 같은 프라이버시 침해가 심각하다고 보는 사람이 대다수(82.2%)이고, 심각하지 않다고 보는 사람은 별로 되지 않는다(4.8%). 이와 관련하여 공공기관이나 민간기업의 개인정보 관리의 안전성에 대해서도 부정적인 인식을 보였다. 안전하지 않다고 보는 사람이 과반수 가까이 되었기 때문이다(48.4%, 47.6%). 이는 우리 사회의 개인정보 관리 양태에 대한 전반적인 불신을 보여준다. 시민들은 주민번호를 다른 번호로 대체하는 것에 대해 동의한다는 의견(65.8%)이 많았는데, 이는 주민번호가 개인 식별자로 사용되는 것에 대한 거부감이 많음을 보여준다.

한편 개인정보 취급 방침을 공개해야 한다는 사실을 '알고 있는' 응답자(20.6%)보다는 '모르고 있는' 응답자(79.4%)가 압도적으로 많았고, 개인정보 열람을 청구할 수 있다는 사실을 '알고 있는' 응답자(24.2%)보다 '모르고 있

는’ 응답자(75.8%)가 압도적으로 많은 것으로 조사되어 개인정보 관련 인지도는 낮은 편으로 나타났다. 그 연장선에서 개인정보 확인을 위해 개인정보 열람을 청구한 경험이 있는 사람(5.6%)이나 개인정보 열람 후, 정정・삭제를 청구한 경험이 있는 사람(10.7%)이 소수인 것은 당연하다.

하지만 자신의 개인정보를 가지고 있는 기관이 개인정보를 다른 기관과 공유하거나 제공하는 경우가 있다는 것에 대한 인지도는 과반수를 넘어서(53.6%) 제3자 제공에 대해 알고 있음을 보여주고 있으나, 인지자 중에서 구체적으로 알고 있는 이는 4분의 1이 채 되지 않았다(22.8%).

이상의 설문과는 별개로 CCTV에 대한 인식을 물었는데, 공공기관에서 CCTV를 설치하는 경우 이를 쉽게 인식할 수 있도록 해야 한다는 사실을 몰랐던 경우가 과반수를 넘었으며(55.8%), 알고 있다고 응답한 경우는 22.6%에 불과하였다. 그리고 CCTV가 설치된 것을 보면 안심이 되는 사람이 과반수를 넘고(50.2%), CCTV에 찍히더라도 이에 위축되지 않는다는 사람이 과반수를 넘어(54.8%) CCTV의 프라이버시 침해 가능성에 대해서는 크게 개의치 않는 모습을 보여주었다.

## 제2절 개인정보보호 책임자 대상 설문조사 결과

공공 및 민간의 주요 기관에서의 개인정보 수집・유통 현황을 조사・분석하기 위해 각 기관에서 개인정보 수집・유통 실태를 가장 잘 알고 있고, 가장 많이 다루고 있는 공공기관 및 민간기업의 개인정보보호 책임자들을 대상으로 설문조사를 하였다. 설문대상 선정을 위해 공공기관의 경우 국가인권위원회를 통해 총 88곳의 공공기관에 공문서를 보내 협조를 구했고, 민간기관의 경우 정보통신서비스제공자 66, 준용사업자 41, 기타사업자 30, 총 137곳을 선정하여 설문지를 보냈다. 그 결과 2009.8.20 - 9.10에 공공기관 45곳, 민간업체 31곳, 총 76곳의 개인정보보호 책임자가 답변을 하였다. 설문문항은 개인정보의 수집・유통 실태를 6개의 영역으로 나누어 각 영역에 대해 3개에서 7개 정도의 선택 문항으로 구성하였다.

이 설문은 각 기관의 객관적인 실태를 나타내기보다 실태에 대한 책임자들의 주관적인 인식을 반영한 경우가 많았다. 설문조사의 특성상 응답자의 주관이 반영될 수 있고, 각 기관/업체의 평가에 부정적으로 작용할 수 있는 답변을 회피할 가능성이 높기 때문이다. 공공기관 및 민간기업의 개인정보 보호에 대한 객관적인 실태를 정확하게 파악하기 위해서는 설문조사의 방식보

다는 실제 운영 실태에 대한 점검이 이루어질 필요가 있다. 이번 설문 응답을 보면, 본 연구의 실태조사 결과와 일정하게 괴리가 있는 응답 결과가 나온 경우도 있었다.

개인정보 침해 위험 및 개인정보보호 체계와 관련한 설문과 관련하여, 우선 과거 개인정보 침해 사고가 발생한 적이 있는지를 조사한 결과 민간기업의 19.4%는 발생한 경험이 있다고 답변하였다. 개인정보 침해사고는 일상적으로 발생하면 당연히 안되는 것이라는 점에서 이 수치는 상당히 높은 것이라고 볼 수 있다. 답변이 보수적으로 이루어질 가능성까지 고려하면, 전체적으로 거의 10%에 가까운 기관/기업에서 개인정보 침해사고가 발생한 적이 있다는 사실은 개인정보 침해사고가 빈발하고 있음을 말해준다.

개인정보관리 책임자 및 개인정보관리 담당자는 응답한 76개 기관 모두가 지정되어 있었다. 그러나 개인정보관리 담당자의 대부분이 개인정보 보호업무와 함께 별도의 업무를 함께 수행하고 있는 것으로 나타났다.(89.5%) 더구나 그 중 개인정보 보호에 관한 업무가 주된 업무인 경우는 더 적었다.(32.4%) 비록 소규모 기관이나 업체의 경우 겸업이 불가피하다고 하더라도, 전반적으로 개인정보 보호 업무를 부차적으로 취급하고 있는 것은 아닌지 우려된다. 개인정보관리담당자가 개인정보 보호 등 담당 업무를 맡은 기간을 물어본 결과 평균적으로 1.84년에 불과하였다.

조직 내 개인정보 보호정책이 개인정보보호 관련 법령의 제·개정, 보안기술의 발전 등에 따라 수시로 변경되고 공개되는지 여부에 대해서도 긍정하는 비율이 높았는데(89.5%), 이러한 설문조사 결과는 앞 장들에서 수행한 실태조사와는 다소 괴리가 있다. 이번 실태조사의 대상이 되었던 지방자치단체나 공공병원 등의 경우 개인정보파일대장과 홈페이지의 개인정보보호정책에서 법령의 제·개정 상황을 제때 반영하지 않은 기관이 많았기 때문이다.

개인정보 수집단계에서 발생할 수 있는 개인정보 침해 문제와 관련한 설문조사 결과, 우선 소속기관이 '사업목적 달성에 필요한 최소한의 개인정보만을 수집하는지 여부'에 대해 대부분의 기관에서 그렇다고 답변하였으나(97.4%), 앞 장의 실태조사에서 나타난 결과는 서비스 제공에 필요한 정도 이상의 개인정보를 수집하는 기관·기업들이 많았다. 주민등록번호 수집 비율은 공공기관이 75.6%, 민간기업이 90.3%로 공공기관보다 민간기업에서 더 높은 것으로 나타났다. 이는 주민등록번호의 이용을 제한하려는 노력에도 불구하고, 여전히 대부분의 민간기업에서 주민등록번호를 수집하고 있음을 보여준다.

개인정보의 이용·제공·공유, 보유 및 파기 등과 관련한 설문조사 결과,

대부분의 응답자가 제대로 관리되고 있다는 답변을 하였다. ‘목적 외 이용 및 제3자 제공의 경우 추가동의 절차가 있는지' 여부에 대해서는 89.0%가, '타 기관 제공시 목적 달성 후 폐기'에 대해서는 98.6%가, ‘제3자 제공내역이 대장 등에 기록・보관되고 있는지 여부’에 대해서는 95.8%가, ‘개인정보의 열람・출력에 대한 기록 여부’에 대해서는 80.0%가, '목적 달성 시 해당 개인정보의 파기 여부'에 대해서는 98.7%가 '그렇다'고 답변하였다. 이 역시 앞장에서 보고된 실태조사 결과와는 약간 괴리가 있었다. 예를 들어 지난 2008년 상당수의 포털, 초고속인터넷업체, 이동통신사 등이 해지정보의 미파기로 인해 방송통신위원회의 시정조치를 받은 바 있다. 이러한 답변에는 응답자의 당위론적 인식이 반영된 것으로 보인다.

정보주체의 권리보장과 관련하여, 대부분이 정보주체의 열람・정정 청구절차를 마련해놓고 있었다.(98.7%) '제3자 제공 내역요청 절차 마련 여부'에 대해서도 78.1%가 그렇다고 답변하였는데, 반면 이번 실태조사에서는 정보주체의 제3자 제공 내역에 대한 열람권은 전반적으로 제한이 되고 있는 것으로 나타났다. 이 설문문항에 대한 개인정보보호 책임자들의 답변은 각 기관/업체의 개인정보보호정책이나 취급방침 등을 통해 개인정보 제3자 제공과 관련한 내용을 공개하고 있는 현실을 반영한 것으로 보인다. ‘개인정보의 열람절차에 따른 개인정보 열람 청구를 처리한 경험이 있는지’를 조사한 결과 76.0%가 그러한 경험이 없다고 답변하였다. 민간기업에서 개인정보 열람청구 처리 경험이 있는 경우가 51.6%로 나왔지만, 이는 그리 높은 수치가 아니다. 왜냐하면, 각 기업은 수많은 고객들을 상대하고 있기 때문에, 개인 고객 입장에서는 그러한 경험이 거의 없거나 낮을지라도, 기업 입장에서 보면 최소한 1번 이상은 열람청구 처리 경험을 할 수 있을 것이기 때문이다. 따라서 오히려 이는 개인정보 열람청구권이 일반 시민들에게 제대로 인식되지 않아 의미가 없는 상태에 있다는 것을 보여주고 있다. '열람청구 후 정정・삭제청구 받은 경험 유무'에 대해서는 47.4%가, '정보주체의 개인정보 정정요구 후 정보 이용 방지 절차 마련 여부'에 대해서는 67,1%가 그렇다고 답변하였다.

# 제5장 결론

## 제1절 연구결과

이번 연구를 통해 드러난 개인정보 수집·유통의 전반적인 실태를 간단히 정리하면 다음과 같다. 첫째, 공공 및 민간영역에서 보유하고 있는 개인정보의 제3자 제공 규모가 방대하다는 것을 확인할 수 있었다. 이러한 현상은 공공영역에서는 '공공적 목적'과 '효율성'을 이유로, 그리고 민간영역에서는 서로 다른 서비스 간의 '제휴'나 '융합'에 따라 강화되고 있다. 물론 이는 정보주체의 동의 혹은 법률에 근거한 것으로 그 자체로는 불법이 아니지만, 개인정보의 제3자 제공과 공유가 증가하면 할수록 정보주체의 자기정보에 대한 통제력은 약화될 수밖에 없다. 국민건강보험공단의 사례에서 볼 수 있다시피, 한번 집적된 개인정보는 '효율성' 등의 이유로 애초 수집목적 외로 활용될 수 있는 다양한 유인을 갖게 마련이다. 또한, 아무리 법제를 강화하고 보안 시스템을 갖춘다고 해도 제3자 제공이나 시스템 연계를 통해 개인정보에 접근할 수 있는 사람들이 많아지게 되면, 무단/불법 열람이나 유출의 위험 역시 커질 수밖에 없다.

따라서 개인정보 보호법제는 앞으로 개인정보의 수집 목적 외 제3자 제공을 제한하는 것에 초점을 맞출 필요가 있다. 이번 연구에서 각 기관/업체에 대한 열람청구를 진행해본 결과, 각 기관/업체가 보유하고 있는 개인정보에 대해서는 대체적으로 열람이 허용되었으나, 내 개인정보의 제3자 제공 내역에 대해서는 대부분의 기관/업체에서 제공을 거부하였다. 개인정보의 제3자 제공이 방대하게 이루어지는 현실에서, 정보주체의 개인정보 자기결정권을 효과적으로 보장하기 위해서는 제3자 제공 내역에 대한 열람권의 보장이 더욱 중요해진다. 또한, 애초 수집목적 외로 개인정보를 활용할 수 있도록 하는 것은 최소한으로 제한하도록 관련 법제가 개선될 필요가 있다. 불가피하게 개인정보를 제공하는 경우라면 정보주체에게 통지를 의무화할 필요가 있으며, 개인정보를 취득한 기관에 대해서는 정보주체가 자기 정보의 취득경위를 요구할 수 있도록 법적 근거를 마련할 필요도 있다.

둘째, 개인정보 보유의 법적 근거가 모호하거나, 개인정보 보호를 위한 법적 체계가 미진한 영역이 여전히 존재하고 있다. 예를 들어, 범죄정보관리시스템의 경우 방대한 양의 개인정보의 수집과 관리를 하면서도 엄밀한 법률적

근거를 갖추지 않은 채 운영되고 있었다. 국민건강보험공단 등이 수집하는 개인정보의 경우에도, 수집의 근거를 추상적으로 규정하고 있어 업무상 필요한 정보를 자체적으로 판단하여 수집하고 있는 실정이다. 특히, 의료 영역의 경우 여타 사회 영역과 달리 개인 의료정보의 보호를 위한 법제가 아직 마련되어 있지 않아 개인정보 보호의 사각지대로 남아있는 것은 심각한 문제이다. 방대한 개인정보를 보유하고 있는 기관에 대해서 개인정보 수집의 범위와 근거, 활용 및 제3자 제공의 근거와 한계, 정보주체의 권리 보호 등에 대한 명확하고 상세한 규정을 포함한 법제 정비가 시급히 필요하다.

셋째, 공공기관에서 추진하고 있는 정보화 사업들이 국민의 프라이버시권을 침해할 우려가 있음에도 불구하고, 정보인권의 관점에서 이를 견제할만한 제도적 장치가 마련되어 있지 않다. 공공기관이 추진하고 있는 사업의 프라이버시 침해 문제가 제대로 검토되지 않는 이유는 '공공기관 개인정보보호심의위원회'가 거의 유명무실하기 때문이다. 이런 점에서 독립적이고 실효성 있는 '개인정보 감독기구' 설립의 필요성을 다시 한 번 절감할 수 있다. 더불어, 공공기관이 정보화와 관련된 사업을 추진할 경우, 사업을 추진하기 전에 '프라이버시 영향평가'를 반드시 거치도록 제도화할 필요가 있겠다.

넷째, 법률에서 개인정보주체의 열람 및 정정·삭제 청구권을 보장하고 있음에도 불구하고, 이에 대한 정보주체의 인식은 매우 부족한 것으로 드러났다. 본 연구에서 수행한 설문조사 결과, 시민들의 대다수는 우리 사회의 프라이버시 침해정도가 심각하다고 느끼고 있었고, 공공기관이나 민간기업의 개인정보 관리 실태에 대해서도 부정적인 인식을 보였다. 그러나 정작 개인정보 취급방침을 공개해야 한다는 사실이나 정보주체가 열람 및 정정·삭제 청구권을 보장받고 있다는 사실에 대해서는 모르고 있는 경우가 압도적으로 많았다. 정규교육이나 언론 등 다각적인 경로를 통해 일반 시민을 대상으로 한 정보인권 교육이 절실하게 필요한 상황이다.

## 제2절 연구의 한계 및 향후 과제

본 연구는 법제에 대한 고찰 보다는 사회 주요 영역의 개인정보 수집·유통 실태와 정보주체의 열람 및 정정·삭제 청구권이 실제 보장되고 있는지를 파악하고자 노력하였다. 그러나 다루고자 했던 영역이 광범위했던 것에 비해, 7개월이라는 한정된 시간과 연구자 역량의 부족으로 각 영역의 조사에서 미진한 부분이 있을 수밖에 없었다는 점은 아쉬움으로 남는다. 이번 조사를 기

반으로 향후에는 각 개인정보 영역에 대해 보다 면밀한 실태 조사가 시행될 수 있기를 기대한다.

이번 연구에서 많은 사회 영역, 그리고 특수한 개인정보 영역을 다루기는 했으나, 중요하지만 이번 연구에서는 빠진 사회 영역이 당연하게도 많이 존재한다. 예컨대, 형사·사법 영역, 사회복지 영역, 세무 영역 등이나 생체정보, 노동감시, 주민등록제도 등의 주제가 포함될 수 있을 것이다.

정보주체의 열람 및 정정·삭제 청구권 보장 실태 조사의 경우에는 해당 영역에 관련된 당사자를 섭외하는데 어려움이 있었다. 특정 영역의 관련 업체나 기관이 많기 때문에 특정 영역 내에서 각 기관/업체별 차이나 전반적인 실태를 보다 정확히 분석하기 위해서는 더 많은 기관/업체에 대한 열람청구가 이루어질 필요가 있겠다.

정확한 실태조사를 위해 필요한 정보 접근의 한계도 존재했다. 공공영역의 경우 여타 문헌이나 국회 등을 통한 정보 접근 외에 각 기관에 대한 정보공개 청구를 통해 정보를 얻고자 했으나, 아예 답변을 하지 않거나 부실한 답변을 제공하는 경우가 많았다. 특히, 민간 업체의 경우에는 자기정보에 대한 열람청구 외에는 각 업체의 내부 실태와 관련된 정보에 접근하는데 한계가 많았다. 따라서 민간 영역의 개인정보 보호 실태를 파악하기 위해서는 개인정보 보호와 관련된 각 기업의 정책이나 실태의 일정한 공개를 법에서 규정하거나 개인정보 감독기구와 같은 권한있는 기관에서 각 영역의 주요 기관이나 업체의 협조를 얻어 실태조사를 수행할 필요가 있다.

# 제1장 서 론

## 제1절 연구의 목적 및 필요성

### 1. 연구의 필요성

개인정보 보호가 우리 사회의 주요 화두로 등장하고 있다. 개인정보 보호 문제는 더 이상 전문가들의 법률 담론에 머무르는 화제가 아니라 언론과 시민의 일상에서 자주 접하는 문제가 된 지 오래다. 특히 2008년에는 옥션 회원 1천81만 명의 개인정보가 유출된 데 이어 하나로텔레콤이 600여 만 명의 고객정보 8천530여 만 건을 유출한 것으로 드러나 사회적으로 큰 충격을 주었다. 하나로텔레콤 사건은 해킹이나 부주의에 의한 것이 아니라 본사 차원의 조직적 지시로 텔레마케팅 업체에 개인정보가 제공된 경우였다.

정보사회에서 개인정보 유출은 필연적인 사건이다. 수기로 기록이 이루어지고 수집되던 과거와 달리 디지털화된 개인정보는 대규모로 수집되고 집적될 수 있다. 발전된 DBMS(Database Management System)의 활용으로 인해 개인에 대한 정보의 입력, 처리, 검색, 출력이 신속하고 정확하게 이루어질 뿐만 아니라 더 나아가 표준식별번호에 의한 컴퓨터 결합을 통해 분산되어 있는 개인정보들을 용이하고 효율적으로 통합·처리할 수 있게 되었다(이인호, 2001). 따라서 디지털 개인정보는 가공하여 이용하기에도, 제3자에게 제공하기에도 훨씬 용이한 형태이며 그에 따른 권리 침해 역시 일상적으로 일어날 수밖에 없다. 오늘날 개인정보 유출, 무단이용, 조작이 대규모로 이루어질 수 있는 기술적 환경이 갖추어져 있는 것이다.

또한 원격 거래와 원격 행정의 발달은 개인정보의 이용과 오용을 동시에 유발한다. 최근 온라인화에 따른 비대면 접촉이 늘어나고 원격 거래와 원격 행정이 활발해진 것은 일정하게 국가조직과 기업 업무의 효율적인 수행을 꾀하기 위한 것이지만, 동시에 개인정보를 매개로 한 신원확인 요구가 사회적으로 증가하는 결과를 가져왔다. 타인의 개인정보에 대한 요구나 그에 대응하는 신원 절도가 과거보다 급증할 수밖에 없는 것이다.

다른 한편으로 개인정보의 상업적 가치가 증가하면서 그에 따른 개인정보의 수집이 증가해 왔다. 기업들은 불특정 다수를 대상으로 한 대중 마케팅의 한계를 넘어 개인별 특성에 맞춘 마케팅 기법(데이터베이스 마케팅)을 개발

해 왔으며, 여기서 개인정보가 매우 중요한 역할을 수행한다. 주소, 전화번호, 이메일 주소 뿐 아니라 직업, 계층, 구매이력, 취향 등 특성별로 분류한 고객의 개인정보를 보유하고 있으면, 구매력을 중심으로 한 고객관계관리(CRM: Customer Relationship Management)와 정교한 타겟 마케팅이 가능하다. 따라서 개인정보의 확보는 기업 경쟁력의 주요 요소로 간주되고 있다.

이런 사회경제적 배경은 종합적으로 공공 부문과 민간 부문을 통틀어 사회 전체적으로 개인정보의 방대한 수집과 이용을 독려하고, 다른 한편으로 그에 따른 권리 침해를 유발하는 요인이 되고 있다. 눈에 보이지 않는 개인정보 데이터베이스의 방대한 구축을 토대로 이루어지는 거래와 행정 서비스는 생활의 편리함을 가져오기도 하였지만, 정보의 주체인 개인의 권리를 제한하기도 한다. 실제 자신의 개인정보가 어떠한 경로로 수집되어 어떻게 이용되고 제공되고 있는지를 정보주체가 정확히 파악하기가 갈수록 어려워지고 있으며, 그 과정에 개입하여 자신의 권리를 행사하기도 쉽지 않다.

또한 개인정보의 무단 수집과 이용을 방관하는 것은, 그 정보에 기초한 사람의 분류, 낙인, 차별을 고착화시키는 결과를 낳을 수도 있다. 개인정보 데이터베이스에 실현되어 있는 한 개인의 정보가 그에 대한 행정서비스와 고객서비스의 수준을 결정하기 때문이다. 정보사회에서는 개인의 사회적 정체성이 디지털화된 개인정보에 의해 좌우될 위험성이 상존하고 있다. 일례로, 잘못된 개인정보에 의해 개인의 사회적 정체성이 왜곡되는 경우 그 개인의 사회적 활동에 미치는 위험성은 지대할 뿐만 아니라, 나아가 개인의 인격 자체에도 치명적인 위해를 가할 수 있다(이인호, 2001). 더 나아가 개인정보를 축적·처리하는 공·사의 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이 된다. 그리하여 이들 개인정보를 토대로 일정 부류의 사람들을 사회적으로 낙인을 찍는 일(예컨대, 신용불량자나 취업기피인물명단의 작성·유통)이 얼마든지 가능해지게 되고, 그 결과 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다(성낙인 외, 2008: 80).

최근에는 CCTV 화상정보, 위치정보, 유전정보, 통신비밀 등이 정보처리기술의 발달에 힘입어 방대하게 수집·이용되면서 국가에 의한 시민의 감시와 통제 사회가 도래할 수 있다는 우려의 목소리가 나오기도 한다. CCTV로 수집되는 개인의 영상정보나 위치정보의 경우, 과거 국가기관에 의한 미행이나 동태파악 등 인적 방식의 감시가 문제가 되었다고 한다면 오늘날에는 같은 정보가 디지털 네트워크 기술을 통해 수집·처리되는 것으로 인하여 달리 문제시되고 있다. 또한 통신비밀의 경우 전통적인 도감청의 문제에서 확대되어

휴대전화, 이메일, 패킷 감청 등 새로운 통신수단에 대한 비밀의 침해가 문제시되고 있다. 이러한 신기술의 경우 자동화된 방식으로 방대한 양의 개인정보를 수집함으로 인하여 과거와 질적으로 다른 효과를 주고 있다.

따라서 사회 각계에서 정보주체의 권리를 실질적으로 보장해야 한다는 문제제기가 잇따르고 개인정보 보호와 관련한 법제도에 대한 일정한 정비가 진행되어 왔다.[1] 특히 2003년 교육행정정보시스템(NEIS)에 대한 정보인권 침해 논란을 거치면서 17대 국회에서 개인정보보호법 제정을 위한 노력이 이루어졌지만, 모든 법안이 회기만료로 폐기되면서 성과를 낳지는 못하였다.

18대 국회 들어 다시 한 번 「개인정보보호법」 제정을 두고 논쟁이 일고 있는 오늘의 시점에서, 올바른 입법을 위해서는 우리 현실 속에서 개인정보가 수집되고 유통되는 실태를 정확히 파악할 필요가 있다. 특히 지금까지 진행되어 온 법률 정비에도 불구하고 정보주체의 권리 행사가 충분히 보장받고 있지 못하다면 어째서 그런지가 주요 관심사 중 하나일 것이다. 입법 현실과 경험적 현실 사이에 괴리가 있을 때 그 지점을 조망하고 개선책을 모색하는 과정 속에서 향후 「개인정보보호법」 제정 및 관련 법률 정비에 주요한 시사점이 제시될 수 있을 것으로 기대되기 때문이다.

본 연구에서는 이러한 측면에서 공공 및 민간의 주요 영역에 있어서의 개인정보 수집과 유통 실태를 파악하고 정보주체의 권리에 대한 보장 여부를 조사하고자 하였다. 더불어 실태조사 과정에서 확인된 각 영역의 문제점들에 대해서는 바람직한 개선 방향을 모색해 보았다. 본 연구 결과가 궁극적으로 개인정보에 대한 정보주체의 권리 의식을 재고하고 국민의 정보인권에 대한

---

1) 성낙인 외(2008: 43-45)는 우리나라에서 개인정보의 처리에 관하여 규율한 입법으로, 1980년 제정·공포된 「형의 실효 등에 관한 법률」을 시작으로, 1994년 공포된 「공공기관의 개인정보보호에 관한 법률」, 1995년 공포된 「신용정보의 이용 및 보호에 관한 법률」, 1999년 제정된 「정보통신망 이용촉진 등에 관한 법률」, 2004년 제정된 「생명윤리 및 안전에 관한 법률」, 2005년 제정된 「위치정보의 보호 및 이용 등에 관한 법률」 등을 들었다. 이상의 개인정보보호법 외에도 상당히 많은 비밀보호 규정들이 「형법」 상의 비밀침해죄(제316조)와 업무상 비밀누설죄(제317조), 「통신비밀보호법」, 「의료법」, 「국민건강보험법」, 「국세기본법」, 「공직자윤리법」, 「전염병예방법」, 「후천성면역결핍증 예방법」, 「금융실명거래 및 비밀보장에 관한 법률」, 「공증인법」, 「변호사법」 등에 산재해 있다. 필자는 이 글에서 개인정보와 비밀을 엄격히 구분하며 개인정보는 그 이용에 대한 '원칙적 허용, 예외적 제한'의 규율방식이 적용된다는 측면에서 '원칙적 금지, 예외적 허용'의 규율방식이 적용되는 비밀과 다르다고 주장하였다. 그러나 그간 비밀로 간주되었던 의료정보의 민간보험사 제공 논란이나, 인터넷 통신내용의 맞춤광고 활용 논란에서 살펴볼 수 있듯이 갈수록 비밀의 경계가 불분명해지는 경향이 있다. 이는 개인정보나 비밀의 객관적 구분과 무관하게 사회전체적으로 그 활용이 늘고 있는 추세를 방증한다.

인식을 높일 수 있는 계기가 될 수 있기를 바란다.

## 2. 연구의 목적

### 1) 공공 및 민간영역에서 개인정보 수집과 유통 실태 조사 및 분석

본 연구는 공공 및 민간의 주요 영역별로 개인정보가 수집되고 관리되는 상황 및 유통 경로를 조사, 연구하여 국민의 개인정보 관리 실태를 파악하고자 하였다. 여기서 주요 영역은 개인정보의 이용이 상당히 활발한 수준에 이른 것으로 평가되는 행정정보 공동이용시스템 및 행정기관 간 개인정보 공유 영역, 수사 및 범죄경력 영역, 포털 및 이동통신사·초고속인터넷업체 등 정보통신 영역, 개인신용정보 등 금융 영역, 보건의료영역, 교육영역을 대상으로 하였다. 특히, 공공 및 민간 영역에서 정보주체의 열람 및 정정·삭제 청구권을 보장할 수 있는 절차 및 실제 이행 수준을 조사함으로써, 개인정보에 대한 열람 및 정정·삭제 청구권 보장 실태를 파악하고자 하였다. 또한 CCTV, 위치정보, 유전정보, 통신비밀 등 최근 새로운 개인정보 처리 영역으로 사회적 관심을 받고 있는 분야의 실태 또한 그 특성별로 살펴보았다.

### 2) 개인정보 보호 및 정보주체의 열람 및 정정·삭제 청구권 보장을 위한 대안 제시

본 연구는 개인정보 보호 및 정보주체의 열람 및 정정·삭제 청구권 보장을 위해 마련되어 있는 기존의 법령 및 가이드라인을 검토하였다. 이러한 검토 과정을 통하여 기존 법령 및 가이드라인의 개선 방안을 모색하였으며, 미비한 부분에 대해서는 바람직한 지침을 제시하고자 하였다.

# 제2절 연구의 내용 및 연구 방법

## 1. 선행연구 및 관련연구 분석

개인정보의 수집과 유통 실태를 조사하기 전에 이 연구가 관심을 두고 있는 개인정보의 권리에 대한 일반적 이론에 대한 검토를 진행하였다.

우리나라에서는 2003년 사회적으로 큰 관심을 끌었던 교육행정정보시스템

(NEIS)에 대한 국가인권위원회 결정에서 볼 수 있었듯이, 「헌법」 제17조 '사생활의 비밀과 자유'의 불가침의 내용으로 자기정보접근권, 자기정보정정청구권, 자기정보사용중지청구권을 포함한 정보관리통제권, 즉 개인정보에 대한 자기결정권이 함께 인정되고 있다.[2)]

> 첫째, 사생활의 비밀과 자유는 국가안전보장·질서유지 또는 공공복리를 위하여만 제한할 수 있다 할 것이므로, 개인의 정보의 수집과 기록을 함에 있어서도 위와 같은 목적이 반드시 존재하여야 하며, 그 목적에 부합하는 범위 내에서만 개인정보가 수집되어야하고, 수집된 자료가 다른 목적에 유용될 가능성이 봉쇄되어 있어야 할 것이다.
> 둘째, 사생활과 비밀의 자유에 대한 제한은 법률로써만 하여야 하므로, 개인정보를 수집하기 위해서는 적법하고 공정한 절차를 거쳐야 할 것인바, 개인정보의 수집은 법령에 의한 적법한 권한을 가진 기관이 하여야 하며, 그 수집되는 자료에 있어서도 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다 할 것이다. 또한 개인정보의 수집은 본인으로부터 직접 수집하는 것을 원칙으로 하며, 또한 개인정보시스템이 원칙적으로 공개되어 있어 본인에게 자신에 대한 정보를 열람하고 정정을 요구할 수 있는 절차가 마련되어 있어야 할 것이다.
> 셋째, 사생활 비밀과 자유에 대한 제한은 필요한 경우에 한하여 본질적 내용을 침해하지 않는 범위 내에서 할 수 있는 것이므로, 개인정보는 계속적, 포괄적, 무제한적으로 수집될 수 없다 할 것이다.[3)]

이러한 개인정보에 대한 자기결정권은 "개인이 자신에 관한 정보의 흐름을 파악하여 통제할 수 있는 권리"로 정의할 수 있다. 이는 자신에 관한 정보의 생성과 유통, 소멸 등에 주도적으로 관여할 법적 지위를 보장하는 것이라고 할 수 있다(성낙인 외, 2008: 168).

권영성(1998: 404-405)에 따르면, 정보관리통제권, 즉 개인정보에 대한 자기결정권은 다시 광의와 협의로 나누어지는데, 광의의 의미는 자신에 관한 정보를 보호받기 위하여 자신에 관한 정보를 자율적으로 결정하고 관리할 수 있는 권리이며, 협의의 의미는 자기정보의 열람·정정·사용중지·삭제 등을 요구할 있는 권리라고 한다.

즉 개인정보자기결정권은 단순히 타인에 의한 개인정보의 취급을 억제하는

---

2) 이론가 및 판례에 따라 개인정보의 권리에 대한 헌법적 근거로서 제17조 외에 제10조 인간의 존엄과 가치 및 행복추구권, 제37조제1항 헌법에 열거되지 아니한 권리로 이해하는 경우도 있다. 이상명(2008: 239-244) 참조.

3) 국가인권위원회. 2003.5.17. 교육행정정보시스템(NEIS) 관련 권고.

이외에도 개인이 자신에 관한 정보의 유통을 적극적으로 형성하고 조절한다는 측면에서 이해될 수 있다(성낙인 외, 2008: 177). 여기서 개인정보자기결정권의 적극적 측면은 대단히 중요하다. 오늘날 대부분의 개인정보가 자신도 모르게 처리되는 현실 속에서 정보주체가 이 유통 과정에 개입하기 위해서는 적극적인 권리를 완전히 인정받을 수 있어야 하기 때문이다. 특히 본 연구는 협의의 개인정보자기결정권으로서 정보주체의 열람 및 정정·삭제 청구권에 특별히 주목하였다. 정보주체에게는 열람·정정·거부권 등을 주고 이들 권리의 행사를 통해 정보처리의 과정에 참여하게 하는 것은 사전에 개인정보처리의 오·남용을 막음으로써 정보주체의 인격적 이익이나 파생되는 다른 권리와 이익의 침해를 예방하고자 하는 데 그 기본 목적이 있기 때문이다(성낙인 외, 2008: 375).

이인호(2001)는 개인정보 자기결정권의 실현모델을 시장규제 모델, 자율규제 모델, 정보주체에 의한 통제 모델, 허가제 모델, 등록제 모델, 옴부즈만 모델로 구분하고, 이중 정보주체에 의한 통제 모델은 2가지 방식으로 이루어진다고 하였다. 개인정보에의 자유로운 접근권 및 정정권을 인정하고, 이들 권리의 침해 시 소송에 의한 권리구제를 보장하는 것이 그것이다. 여기서 전자로서 정보통제권의 행사는 3가지의 과정을 거쳐 행하여지는데, 우선 정보주체에게 개인정보처리시스템의 존재, 그 목적, 그리고 그 정보의 내용이 알려져야 하기 때문에 처리시스템을 운영하는 자는 그 명칭, 정보의 내용, 소재지 등에 대해 공표할 의무를 진다. 두 번째로 정보주체에게는 보존·처리된 자신에 관한 정보의 열람을 청구할 권리가 인정되고, 세 번째로 정보가 부정확, 낡거나 또는 불완전하다고 증명된 경우에는 그 정정 및 삭제의 절차가 마련되어야 한다. 정보사회에서 매우 위험한 요소는 한번 입력된 정보가 자동으로 지워지지 않는다는 사실에 있는 만큼, 낡고 틀린 정보가 지워지지 않은 상태로 계속 존재하면서 실존인격에 영향을 미칠 수 있는 가능성을 차단하기 위해서는 이 같은 권리가 확실하게 보장되어야 한다.

성낙인 외(2008: 177-182)는 개인정보자기결정권은 수집에 대한 통제권, 보유에 대한 통제권, 이용에 대한 통제권 등을 내용으로 한다고 하였다. 수집에 대한 통제권이 수집동의권, 설명청구권, 민감한 개인정보의 수집금지로 볼 수 있다면, 이용·제공에 대한 통제권은 중단청구권, 추가적 동의권으로 볼 수 있다. 앞서의 열람청구권, 정정청구권, 삭제·차단청구권 등은 보유에 대한 통제권에 속하는데, 이는 부정확하고 불완전한 개인정보를 토대로 공권력이 행사되거나 외부로 유출되어 정보주체가 자신에 관한 정보로부터 소외되

지 않도록 해주는 최소한의 통제장치라고 할 수 있다.

이와 같은 개인정보에 대한 열람 및 정정·삭제 청구권은 개인정보보호에 관한 국제 규범 및 입법에 있어서 원칙으로 인정받아 왔다. 개인정보보호에 대한 최초의 국제규범인 1980년 OECD 「개인정보보호가이드라인」[4]에서는 소위 '참여의 권리'로서 이를 보장하였다. '개인 참여의 원칙'(Individual Participation Principle)에 의하면, 정보주체는 자신에 관한 정보를 개인정보처리자가 가지고 있는지 여부를 확인할 권리(소재확인권)를 가지며, 자신에 관한 정보를 합리적인 기간 내에 과도하지 않은 비용으로 합리적인 방법에 의해 알기 쉬운 형태로 전달받을 권리(열람권)를 가진다. 소재확인권과 열람권이 거부되는 경우에 개인은 그 이유를 구하고(거부이유를 알 권리) 그 거부에 대하여 다툴 수 있는 권리(이의청구권)가 있으며, 그 다툼에서 이기는 경우에는 해당 정보의 삭제·정정·수정·보완을 요구할 권리(처리정보변경권)를 가진다.[5] 이러한 원칙은 OECD 「개인정보보호가이드라인」 이후에도 1990년 UN의 「전산처리된 개인정보파일의 규제에 관한 지침」[6] 및 1995년 EU 「개인정보보호에 관한 유럽의회와 각료회의 지침」(이하 EU 「개인정보보호지침」)[7]에서도 확인되고 있다.

UN의 「전산처리된 개인정보파일의 규제에 관한 지침」에서는 "이해관계인에 의한 접근 원칙(Principle of Interested person Access)"하에 정보가 수집되거나 저장된 해당 개인은 이러한 정보가 어떻게 처리되며 사용되는지에 관하여 알 권리를 가지고 있으며 잘못되거나 정확하지 못한 정보의 삭제

---

4) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980.

5) Individual Participation Principle
13. An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

6) Guidelines for the Regulation of Computerized Personal Data Files, Adopted by General Assembly resolution 45/95 of 14 December 1990.

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

권 등 여러 권리들이 이러한 개인을 위하여 제공되어야만 한다고 규정하고 있다. EU 「개인정보보호지침」에서는 “제12조(열람권)”에서 회원국이 모든 정보주체에게 합리적인 간격으로 제한 없이, 지나친 지연이나 비용 없이 자신에 관한 정보가 처리되고 있는지 여부를 확인하고, 더불어 처리의 목적, 관련정보의 범주, 그리고 정보가 제공되는 이들에 대해서나 그들의 범주에 대한 고지를 개인정보관리자로부터 받을 수 있는 권리를 보장하도록 규정하였다. 또한 처리되고 있는 정보와 정보의 처리에 관한 유용한 사항에 대해 알기 쉬운 형식으로 통지받을 권리도 보장하였으며, 자동처리된 결정의 경우 정보주체와 관련한 정보의 자동적 처리에 포함된 로직에 관한 정보를 제공받을 수 있는 권리 역시 보장하였다. 불완전, 부정확한 정보나 이 지침에 위배되어 처리된 정보에 대하여 정정, 삭제 또는 차단의 권리도 인정하였다.

유럽연합, 영국, 독일, 일본 등 대부분 국가의 개인정보보호법도 기본적으로 이러한 권리 규정을 두고 있다. 더 나아가, 유럽과 일본은 정보주체의 동의 없는 정보처리를 광범위하게 허용하면서도, 일정한 경우 정보처리에 대한 사후거부권(right to object)을 정보주체에게 부여하고 있다. 또한 유럽은 일정한 형태의 ‘자동결정에 구속되지 않을 권리’를 정보주체에게 인정하고 있다(성낙인 외, 2008: 83-84).

최근에는 열람권의 내용으로, 정보주체가 보유중인 개인정보에 대한 소재확인을 하고 상태를 열람할 수 있는 데에서 더 나아가 개인정보처리자가 개인정보를 이용한 내역과 제3자에게 제공한 내역을 확인할 수 있는 권리까지 포함하고 있다.[8)]

우리의 경우에도 정보주체의 열람 및 정정·삭제 청구권은 「공공기관의 개인정보 보호에 관한 법률」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」, 「위치정보의 보호 및 이용 등에 관한 법률」 등 관련 법률에 원칙으로서 포함되어 있다. 다만 그 수준은 각기 다르다.

이처럼 개인정보에 대한 자기결정권에 대한 선행연구들은 입법론적으로 그리고 비교법적으로 다양한 연구 성과가 축적되어 있는 편이었다. 다만 대개의 연구가 입법론적인 문제제기 수준에 그치고 있을 뿐, 거론된 개인정보 영역과 각 법률이 경험적 현실에서 실제 작동하는 방식에 대한 검토는 이루어지고 있지 못하였다. 특히 개인정보의 열람 및 정정·삭제 청구권 등 정보주체의 권리 행사는 당위론적 규정에 그치는 경우가 많았다. 따라서 선행연구

8) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제30조제2항.

들의 문제제기를 구체화시키기 위해서라도 기입법된 법률들이 현실 속에서 작동하고 정보주체와 관계 맺는 실태를 조사해볼 필요가 있다. 이에 본 연구는 선행연구의 한계를 극복하기 위해 법제도적 분석과 실태에 대한 분석을 동시에 진행하여 양쪽 연구의 장점을 살리고자 하였다.

또한 개인정보에 대한 권리 실태를 효과적으로 파악하기 위하여 개인정보의 생애주기별 조사가 이루어질 필요가 있다. 신영진·강원영(2008)은 개인정보보호수준을 측정하기 위해 정책·기술적 보호기반, 생애주기별 정보관리, 정보침해 대응대책으로 크게 구분하여 3개 영역 18개 구성요소를 구성하였다. 그 중 생애주기별 정보관리는 개인정보를 수집·보유, 이용·제공, 파기 등과 같은 개인정보 생명주기(life-cycle)를 중심으로 정보를 보호하고 관리하는 수준을 파악하고자 하였다. ① 개인정보의 수집·보유와 관련하여 법적인 근거나 정보주체의 동의 등의 절차를 통해 수집하고 보유하는 정도를 측정하고, ② 개인정보의 이용·제공과 관련하여 법률상 이용·제공 및 입·출력 시에 준수사항, 관리대장, 로그 및 접근기록 등에 대한 관리정도를 조사하며, ③ 개인정보의 파기는 저장매체, 이동매체, 출력물 등의 파기목적을 달성한 후 파기절차, 방법 등에 관한 적절성을 측정하였다(신영진·강원영, 2008: 112-113). 이향수(2009)는 개인정보의 생애주기에 대하여, 정보주체로부터 개인정보를 수집하는 수집단계, 개인정보 수집기관에서 수집된 개인정보를 저장하고 보관하는 관리단계, 개인정보를 이용하는 이용단계, 끝으로 수집된 목적이 달성된 후 개인정보를 폐기하는 파기단계로 파악하였다. 본 연구에서도 이와 같은 논의를 참고하여 생애주기별 조사방법을 취하였다.

한편, 정보주체의 열람 및 정정·삭제 청구권 등 적극적인 의미에서의 개인정보자기결정권의 행사는 개인의 주도성에 달려 있다(이인호, 2001). 즉 시민 개개인의 의식과 의지 및 능력에 그 실효성이 달려 있는 만큼, 일반 시민의 인식에 대한 설문조사를 실시할 필요도 있다. 더불어 시민들의 청구를 받는 입장인 개인정보보호책임자들의 인식 조사 역시 병행하여 이루어져야 그 권리 행사의 실효성 정도에 대한 윤곽이 잡힐 수 있을 것이다.

## 2. 연구의 대상과 방법

### 1) 연구의 대상

본 연구는 우리 사회 전반의 개인정보 수집·유통의 실태 파악 및 정보주체의 열람 및 정정·삭제 청구권의 보장 실태를 파악하는 것을 목적으로 하

고 있다. 그러나 개인정보를 수집하고 있는 사회 영역이 워낙 다양하기 때문에, 전체 사회 영역 중에서 중요하다고 판단되는 영역을 선정하여 진행할 수 밖에 없었다. 또한, 특정 영역 내에서도 그 범위가 넓은 경우 조사 연구의 대상을 한정하였다.

본 연구에서 대상으로 선정한 사회영역은 다음과 같다.

- 행정정보 공동이용시스템 및 행정기관 간 개인정보 공유
- 경찰청에서 보유하고 있는 수사/범죄경력 정보 : 수사자료표 및 범죄정보관리시스템(CIMS)
- 정보통신 영역 : 포털, 이동통신사, 초고속인터넷업체를 중심으로
- 금융 영역
- 보건의료 영역
- 교육 영역

이와 함께, 현재 쟁점이 되고 있는 특수한 유형의 개인정보에 대한 수집·유통 실태조사도 병행하였다. 본 연구에서 다룬 특수한 유형의 개인정보는 다음과 같다.

- CCTV : 방범용 CCTV를 중심으로
- 위치정보
- 유전정보 : 실종아동등의 유전자 데이터베이스를 중심으로
- 통신비밀 : 수사기관에 의한 통신비밀 침해를 중심으로

### 2) 연구의 방법

특정 영역의 개인정보 수집·유통 실태를 객관적이고 전면적으로 파악하기 위해서는 해당 기관이나 업체의 정보 제공이 필수적이다. 그러나 민간업체의 경우에는 법에서 의무화한 사항 외에는 공개의 의무가 없고, 개인정보에 대한 관리 정책이나 시스템이 내부 보안사항에 해당하는 경우도 있기 때문에 협력을 얻기는 힘들다. 무엇보다 공공기관이든 민간업체든 개인정보 관리 실태에 대한 조사를 통해 자 조직의 문제점이 드러날 것에 대한 우려 때문에, 특별한 권한을 가진 기관이 연구를 수행하지 않는 한, 각 기관/업체의 자발적인 협력을 기대하기 힘들다. 이에 본 연구에서는 각 영역의 개인정보 수집·유통 실태를 파악하기 위해 다양한 방식의 조사방법을 동원하였다.

(1) 기존 문헌/자료 검토

기존의 연구 논문, 공공기관의 보고서, 백서, 지침 및 매뉴얼, 관련 이슈에 대한 토론회, 국가인권위원회의 결정례, 시민단체의 성명이나 의견서, 각 기관의 보도자료, 국회의 국정감사 자료 및 법안 제정 과정에서의 각종 자료, 언론 보도 등 조사 대상과 관련된 다양한 자료를 활용하였다.

(2) 정보공개 청구

조사 대상인 공공기관, 혹은 각 영역의 주무부처에 대해 개인정보 수집·유통 실태 및 관련 정책에 대한 정보공개 청구를 수행하였다.

(3) 각 기관/업체의 공개된 정책문서 검토

민간업체의 경우에는 '개인정보 취급방침'을, 공공기관의 경우에는 '개인정보 보호방침'을 홈페이지를 통해 공개하고 있다. 또한, 서비스 약관이나 공공기관의 개인정보파일대장도 공개되어 있다. 이러한 각 기관/업체의 개인정보 관련 정책은 그 자체로 각 기관/업체의 개인정보 수집·유통 실태를 파악할 수 있는 자료임과 동시에, 그것의 준수여부를 확인하는 것이 본 연구가 수행하고자 하는 바이기도 하다.

(4) 추적조사: 자기정보에 대한 정보주체의 열람청구

본 연구는 개인정보 수집·유통 실태의 중요한 한 부분으로서 정보주체의 열람 및 정정·삭제 청구권의 보장 실태를 알아보고자 하였다. 이에 따라, 각 영역에서 개인정보 열람청구의 자격이 있는 사람을 선정하여, 실제 각 기관/업체에 자기정보에 대한 열람청구를 진행하였다. 그러나 각 영역의 특성 상, 열람 청구의 자격이 있는 사람을 구할 수 없거나(예를 들어, 의료정보나 유전자정보 등이 이에 해당한다), 혹은 연구 자원의 제약으로 본 연구의 대상이 되는 모든 영역에서 열람청구를 진행하지는 못했다. 본 연구에서 정보주체의 열람청구를 진행한 영역은 다음과 같다.

<표 1-1> 본 연구에서 정보주체 열람청구를 수행한 대상 기관 및 업체

| 대상 영역 | 열람청구 대상 기관/업체 | 열람청구 내용 |
|---|---|---|
| 수사, 범죄 경력 정보 | 경찰청 | 수사자료표 및 범죄정보관리시스템(CIMS)에 수록된 개인정보에 대한 열람 청구 |
| 정보통신 영역 통신비밀 | 각 포털업체 | 자기정보 및 제3자 제공내역에 대한 열람 청구, 각 포털업체의 개인정보 보호 정책에 대한 질의 병행. |
| 정보통신 영역 위치정보 통신비밀 | 이동통신사 및 초고속인터넷업체 | 통화내역, 위치정보, 인터넷 이용내역, 제3자 제공내역에 대한 열람 청구 |
| 금융 영역 | 은행, 신용조회업체 | 무료열람권, 신용정보제공사실 통보요구권 보장여부 확인 |
| CCTV | 지방자치단체 및 경찰서 | CCTV에 찍힌 본인 화상정보에 대한 열람청구 |

(5) 설문조사

개인정보 수집·유통 실태에 대한 일반 시민의 인식을 알아보기 위해 전문 리서치업체에 의뢰하여 설문조사를 진행하였다. 기존의 설문조사와 달리, 이번 설문조사에서는 정보주체가 법에서 보장하고 있는 정보주체의 열람 및 정정·삭제 청구권에 대해 어느 정도나 인지하고 있는가에 초점을 맞추었다. 정보주체의 열람 및 정정·삭제 청구권이 의미를 갖기 위해서는 이에 대한 개인정보 보유기관의 인식과 이를 보장하기 위한 실제적인 절차 마련이 중요하기는 하지만, 이와 함께 정보주체 당사자가 자기 권리에 대해 인지하고 적극적으로 행사하려는 의지가 있어야 하기 때문이다. 설문대상은 전국 19세 이상 성인남녀 500명이며, 조사기간은 2009년 7월 18일 하루에 진행하였다. 총 13개의 선택형 설문문항으로 구성된 구조화된 질문지를 가지고 전화면접 조사를 하였으며, 최대 허용 오차는 95% 신뢰수준 하에서 ±4.4%이다.

일반 시민을 대상으로 한 설문조사와 별개로, 각 기관/업체의 개인정보보호책임자(혹은 담당자)를 대상으로 한 설문조사를 진행하였다. 이는 각 기관/업체의 개인정보보호책임자 운용 실태 자체를 파악하기 위한 목적과 함께, 자조직의 개인정보 수집·유통 실태에 대한 간접적인 파악 및 개인정보보호책임자의 인식을 알아보기 위한 목적으로 진행한 것이다. 설문대상 선정을 위해 공공기관의 경우 국가인권위원회를 통해 총 88곳의 공공기관에 공문서를

보내 협조를 구했으며, 민간기관의 경우에는 정보통신서비스제공자 66곳, 준용사업자 41곳, 기타사업자 30곳, 총 137곳을 선정하여 설문지를 보냈다. 각 업체의 개인정보보호책임자의 목록은 개인정보취급방침 상에 공개된 것을 참고하였다. 설문지 발송 결과, 2009. 8. 20 ~ 9. 10일에 공공기관 45곳, 민간업체 31곳, 총 76곳의 개인정보보호 책임자가 답변을 하였다.

# 제2장 사회영역별 개인정보 수집·유통실태

여기서는 사회영역별로 개인정보가 수집·유통되는 실태를 살펴보았다. 우선 행정안전부를 중심으로 행해지는 개인정보 공동이용 및 개인정보파일 관리와 관련한 개인정보의 수집·유통실태에 대해 검토하고, 경찰청이 관련되는 수사/범죄경력 영역의 수사자료표, 범죄정보관리시스템(CIMS)을 살펴보며, 정보통신 영역의 포털 업체와 이동통신사 및 초고속인터넷업체의 개인정보 수집·유통실태, 그리고 금융 영역, 보건의료 영역, 교육 영역에서의 개인정보 수집·유통실태를 분석하였다.

## 제1절 행정정보공동이용시스템/행정기관 간 개인정보 공유

행정안전부는 현재 개인정보보호를 위한 주관부처이다. 따라서 이번 연구진행과정에서 행정안전부에 상당한 정보공개 청구를 했으나, 그에 따른 소득은 그리 많지 않았다. 여기에서는 행정안전부가 중심이 되는 행정정보공동이용시스템 및 행정기관 간 개인정보 공유에 대해 살펴보도록 한다.

### I. 행정정보공동이용시스템

#### 1. 개 요

##### 1) 행정정보 공동이용과 개인정보보호

행정정보공동이용의 정의에 대해서는 그 근거법률이라고 할 수 있는 「전자정부법」도 구체적인 개념정의를 내리지 않고 있으며, 다만 제11조 '행정정보공동이용의 원칙'에서 "행정기관은 수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관과 공동이용하여야 하며, 다른 행정기관으로부터 신뢰할 수 있는 행정정보를 제공받을 수 있는 경우에는 동일한 내용의 정보를 따로 수집하여서는 아니된다"고 규정하고 있다.

법령 외에 각 부처의 행정규칙까지 찾아보더라도 행정정보 공동이용에 대해서는 이를 정의한 경우가 드물다.[9] 다만 '국가보훈처 행정정보 공동이용

지침'[제34호, 국가보훈처예규, 2009.9.1] 제3조제1호에서 "공동이용"이란 '행정정보의 전부나 일부를 「전자정부법」 등에서 정한 절차에 따라 행정정보공동이용시스템을 통하여 조회하거나 전송받는 것'이라고 규정하고 있다. 그렇다면 여기에서 중심이 되는 것은 행정정보공동이용시스템이라고 할 수 있다. 이에 대해 교육인적자원부의 '행정정보 공동이용에 관한 운영지침'(2006. 3. 2. 시행)은 "공동이용시스템"이 교육행정정보시스템과 행정자치부 등 관계 중앙행정기관이 구축·운영하는 정보시스템을 연계하여 운영하는 일련의 정보관리체계라고 규정하고 있으며, 행정안전부에서 제정한 '행정정보 공동이용 지침'[제267호, 행정안전부예규, 2009.8.28]은 공동이용센터가 보유기관이 유지·관리하는 행정정보 데이터베이스 및 전자적 체계와 이용기관이 관리하는 전자적 체계를 연계하여 공동이용 대상 행정정보를 공동이용하기 위하여 구축·운영하는 시스템이 행정정보공동이용시스템이라고 하고 있다(동지침 제3조).

여기에서 보면 행정정보공동이용이란 대부분 행정기관 사이에서 행해지는 것임을 알 수 있는데, 최근에는 이를 민원 편의와 연결시켜 파악하고 있다. 즉 민원인이 행정기관에 제출하는 각종 구비 및 첨부서류의 대부분이 다른 행정기관에서 발급받은 것이므로, 행정기관 간 정보공동이용을 통하여 국민의 기관 방문 횟수를 줄이고 관련 서류의 중복 제출을 축소한다는 것이다(송희준, 2008). 그 추진 현황을 보면(감사원, 2008: 3-4), 구 행정자치부는 행정정보 공동이용 활성화를 위해 2000년 1월 행정기관의 시스템을 서로 연계하여 필요한 정보를 다량으로 주고받을 수 있도록 지원하는 행정정보 중계시스템을 개발·운영하고, 2002년 11월에는 민원서비스혁신(G4C)시스템을 구축하여 민원담당 공무원이 민원처리를 위하여 주민등록정보 등 20종의 행정정보를 기관 간 공동이용을 통하여 실시간으로 열람할 수 있도록 하였다. 그리고 2003년 8월부터는 아래 표와 같이 '행정정보 공동이용 확대'를 전자정부사업의 핵심과제로 선정·추진하고 행정정보 공동이용 기관과 공동이용 대상 정보를 꾸준히 확대하여 왔다.

9) 각 부처별로 별도의 '행정정보공동이용 지침'이 있는 듯하나, 모두 확인하지는 못했다.

<표 2-1> 행정정보 공동이용시스템의 단계별 확대구축 사업 현황

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

자료: 행정정보공유추진위원회(2007: 31).

이러한 행정정보공동이용 확대사업은 민원발급서류 현황분석을 통하여 가장 빈도가 높고 대민 서비스 혁신 효과가 큰 74종의 공유를 확대하는 사업을 선정하였고, 전자정부특별위원회가 출범한 직후인 2005년 7월 국정과제회의에 보고함으로써 공식적으로 추진되었다. 이 보고에서 정부부처는 2006년 말까지, 그리고 공공기관과 금융기관은 2007년 말까지 정보공유를 확대하는 계획을 확정하였다.

행정안전부도 행정정보 공동이용 실적이 증가하였음을 제시하는 보도자료에서 "행정정보공동이용은 민원인이 다수의 기관을 일일이 방문하여 구비서류를 발급받아 제출하는 대신 민원공무원이 온라인으로 관계 기관 서류를 직접 열람, 확인하는 제도"이라고 언급하고 있다(행정안전부, 2009b). 이에 따르면 행정정보공동이용이란 증가하면 할수록 바람직한 것으로 바뀌게 된다. 법제처에서도 이와 유사하게 행정정보의 공동이용을 통하여 공공기관, 은행을 이용할 때 공동이용대상이 되는 행정정보는 민원신청시 구비해야 할 서류가 필요 없이 행정기관에서 확인할 수 있으므로, 민원인은 보다 편리하게 민원을 처리할 수 있다고 밝히고 있다.[10]

이에 입각하여 만들어진 민원서비스 사이트가 e하나로민원 사이트이다. 사이트 소개글에 따르면, e하나로민원(http://pr.share.go.kr/)은 민원인이 "혼인신고" 등 민원 신청시, 관공서에서 직접 발급받아 제출해야 했던 "주민등록등본" 등의 구비서류를 관공서간 전자적으로 공동이용하여, 민원인들이 구비서류를 발급받아 제출해야 했던 불편함을 해결해주는 민원서비스이다. 여기

10) 법제처, 찾기쉬운 생활법령정보 [청원·민원 및 국민제안>민원>편리한 민원제도>민원서비스의 전자화], http://oneclick.moleg.go.kr/(검색일: 2009.9.4).

에서 민원인이 제출 생략한 구비서류는 민원처리담당자가 전자적으로 확인하여 민원을 처리하게 된다. 국민의 입장에서는 행정기관 방문횟수를 줄여 시간과 비용을 절약함은 물론 보다 신속한 서비스를 제공받을 수 있으며, 한 장의 신청서 작성으로 민원을 처리하는 편리함을 누릴 수 있다는 것이다.

『2007 행정정보공동이용 백서』에 따르면, 국민들이 각종 인·허가 등을 받기 위해 행정기관 등에 제출하는 서류가 2005년에는 4억4천만여 건에 이르고, 다음과 같이 하나의 민원을 해결하기 위하여 여러 종의 구비서류를 제출해야 했다. 이는 곧 국민의 불편과 자원의 낭비[11]로 이어진다.

그런데 행정정보 공동이용으로 구비서류를 줄이게 되면 4억4천만여 통의 종이증명서 중 약 67%인 2억 9천만 통을 절약할 수 있을 것으로 보았다(행정정보공유추진위원회, 2007: 23). 행정안전부에 따르면 2007년 한 해 동안 행정정보공동이용으로 8,700만 건의 구비서류를 절감할 수 있었고, 이를 통해 약 5,400억 원의 사회적 비용을 절약할 수 있었다고 한다(성낙인 외, 2008: 220).

<표 2-2> 민원사무 1건 당 구비서류 종수 현황

(2005년 10월 말 기준, 단위: 건)

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

자료: 행정정보공유추진위원회(2007: 26).

또한, 행정·공공·금융기관에서 업무처리를 위해 여러 기관의 정보를 활용하여야 하는 경우 서면으로 정보보유기관에 협조를 요청하거나 민원인에게 증명서 첨부를 요구하는 방식으로는 업무효율을 높이는 데 한계가 있었고, 기관별로 정보시스템을 구축하여 동일한 정보를 여러 기관에서 중복 수집·관리하는 등 낭비가 있었다. 이에 따라 업무프로세스 혁신을 통한 행정능률 향상과 민원서비스 개선을 위해 민원처리부서에서 각종 구비서류를 전자시스템을 통해 확인하고 각종 정책정보 등 가치 있는 정보를 상호 공동 활용할 수 있도록 범정부적인 정보공유체계를 구축할 필요가 있었다는 것이다(행정정보공유추진위원회, 2007: 23-24). 범정부적인 행정정보공동이용체계의 구

11) 이는 1년에 2조7천억 원이라는 사회적 비용을 야기했는데, 이는 GDP의 0.5%에 달하는 금액이다(행정정보공유추진위원회, 2007: 21).

축은 부처 간, 민관 간 협업기반의 막힘없는 업무처리를 구현할 수 있다. e하나로민원(http://pr.share.go.kr/)은 여권 신청 시[12]를 예로 들어 변화된 민원 서비스를 제시하고 있다.

그리고 행정정보공동이용이 활성화되면 일선 창구에서의 증명서 발급업무가 줄어들고, 이에 따라 이 업무를 담당했던 인력들을 대민서비스 제공업무에 재배치함으로써 한층 더 내실 있는 서비스 제공이 가능해진다고 한다(성낙인 외, 2008: 222).[13]

하지만 개인정보의 투명한 관리가 이루어지지 않는 상황에서의 정보 공유는 국민의 막연한 불안감을 일으키고 이러한 두려움은 개인적 불안정과 사회적 불신을 야기한다(권해수, 2006: 9-10). 이 점에서 행정정보공동이용은 개인정보 보호 문제를 해결한다는 전제 위에서 추진되어야 하나, 위에서 본 것처럼 민원 편의 및 행정의 효율성과 연결하여 개인정보 공동이용에 따른 효용성만이 부각되고 있어 문제가 되고 있다.

### 2) 개인정보 공동이용의 법적 근거

「전자정부법」은 전자정부의 운영원칙의 하나로서 제11조에서 행정정보공동이용의 원칙을 선언하고 있으며, 동법 제21조(행정정보공동이용)에서 공동이용해야 하는 행정정보를 정하고 있고, 제22조에서 행정정보공동이용의 절차를 규정하고 있으며, 제22조의2(공공기관등의 행정정보 공동이용)에서 공공기관[14]과 민간의 금융기관들이 행정정보공동이용센터를 통하여 행정기관[15]이 보유하고 있는 행정정보를 공동이용할 수 있도록 허용하고 있다. 그리고 행정정보 공동이용에 따른 개인정보 침해를 방지하기 위해 「전자정부

12) 과거에 여권을 새로 만들기 위해서는 주민등록등본, 병적증명서, 출입국사실증명서를 각각 관할 구청, 병무청, 출입국관리사무소를 방문하여 준비해야 하는 등 번거로웠지만, 이제는 이러한 증명서를 제출할 필요 없이 신분증과 사진2장만 준비하면 여권을 발급받을 수 있도록 민원신청이 편리해졌다는 것이다.

13) 정부는 이상과 같이 제시된 행정정보공동이용의 효과를 대국민서비스 향상, 불필요한 서류제출 부담 경감, 행정기관의 능률성 향상, 중복투자방지로 정리하고 있다(행정자치부, 2008: 63-64).

14) 이 법률에서 "공공기관"이라 함은 '정부투자기관, 정부산하기관, 지방공사 및 지방공단, 특별법에 의해 설립된 특수법인, 각급 학교, 그 밖에 대통령령으로 정하는 법인·기관 및 단체'를 말한다(제2조제9호). 이 중에서 정부투자기관과 정부산하기관은 2007. 4월 제정된 「공공기관의 운영에 관한 법률」상의 '공공기관'으로 바뀌었으나, 「전자정부법」은 아직 용어를 고치지 않고 있다.

15) 이 법률에서 "행정기관"이라 함은 "국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관 및 국무총리 소속기관을 포함한다) 및 그 소속기관, 지방자치단체를 말한다"(제2조제2호).

법」 제22조의3에서 행정정보를 취급·이용함에 있어서 개인정보를 누설, 말소, 유포하는 등의 행위를 금지하고[16] 제53조에서 처벌의 근거를 마련하고 있다.

행정정보 공동이용 상의 개인정보 보호와 관련해서는, 「전자정부법」에서 행정기관[17]이 ① 다른 행정기관으로부터 신뢰할 수 있는 행정정보[18]를 제공받을 수 있는 경우 중복 수집을 금지하고(제11조), ② 행정기관 간에 전자적으로 확인할 수 있는 사항을 민원인에게 확인하여 제출하도록 요구하지 않도록 하며(제10조), ③ 행정정보 공동이용 등을 통해 종이문서 등을 최대한 감축하여야 하고(제40조), ④ 행정정보를 권한 없이 처리하거나 누설하는 등의 행정정보 오·남용 행위를 금지하고 있다(제22조의3). 또한 ⑤ 국가의 안전보장과 관련된 행정정보와 비밀 또는 이에 준하는 행정정보는 공동이용의 대상이 되는 정보에서 제외할 수 있으며, 행정기관 간 공동이용되는 행정정보의 제공기관은 당해 행정정보의 정확성을 유지하여야 한다(제21조제2항 및 제4항)고 규정하고 있다.

「전자정부법 시행령」 제18조 내지 제31조 '제4장 행정정보의 공동이용'에서도 개인정보 보호와 관련하여 행정정보 공동이용의 원칙이 표명되고 있다. ① 행정기관이 정보파일을 구축하여 보유하고자 하는 경우 정보파일의 행정정보 보호대책을 통보하여야 하며(제21조제1항), ② 행정정보의 제공요청은 필요한 최소한의 범위에 한정하여야 하고(제22조제2항), ③ 행정정보공동이용센터(전자정부본부가 그 기능을 수행한다)는 공동이용한 행정정보의 유지·관리에 힘쓰고, 행정정보 공동이용 및 개인정보보호 실태에 대한 현황을 파악해야 한다(제26조)는 것이다.

---

16) 제22조의3 (행정정보취급·이용자의 의무) 누구든지 행정정보를 취급·이용함에 있어서 다음 각 호의 행위를 하여서는 아니 된다.
1. 행정정보의 처리업무를 방해할 목적으로 행정정보를 변경하거나 말소하는 행위
2. 행정정보를 변경하거나 말소하는 방법 및 프로그램을 공개·유포하는 행위
3. 행정기관에서 처리하고 있는 행정정보를 누설하는 행위
4. 행정기관에서 처리하고 있는 행정정보를 권한 없이 처리하는 행위
5. 행정기관에서 처리하고 있는 행정정보를 권한 없이 타인으로 하여금 이용하게 하는 행위
6. 거짓 그 밖의 부정한 방법으로 행정기관으로부터 행정정보를 열람하거나 제공받는 행위

17) 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관 및 국무총리 소속기관 포함) 및 그 소속기관, 지방자치단체를 말한다.

18) 행정기관이 직무상 작성 또는 취득하여 관리하고 있는 자료로서 전자적 방식으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것을 말한다.

「전자정부법」은 행정의 효율성과 민원서비스의 신속하고 원활한 제공을 위하여 개인정보의 공동이용을 법적으로 요구하고 있지만, 공동이용에 따르는 위험성을 제어하기 위한 안전장치는 마련되어 있지 않다. 오히려 「전자정부법」상의 '개인정보 공동이용'은 「공공기관의 개인정보보호에 관한 법률」을 통한 규율마저 해체시키는 역할을 한다(성낙인 외, 2008: 837).

「전자정부법」은 행정정보공동이용을 모든 행정기관의 의무로 규정하고 있고, 행정정보의 공동이용을 활성화하기 위하여 공동이용 대상 정보의 범위를 민원처리를 위해 필요하거나 행정업무 수행에 참고가 되는 행정정보(제21조) 등으로 폭넓게 인정하고 있다. 행정기관이 공동이용해야 하는 행정정보, 즉 행정정보공동이용의 대상은 다음과 같다(「전자정부법」 제21조 제1항).

- 민원사항의 처리를 위하여 필요한 행정정보
- 통계정보·문헌정보 등 행정업무의 수행에 참고가 되는 행정정보
- 「공공기관의 개인정보보호에 관한 법률」 제10조 제3항에 의하여 다른 기관에 제공할 수 있는 처리정보
- 「국가정보화 기본법」 제9조의 규정에 따른 국가정보화전략위원회가 행정기관간 공동이용이 필요하다고 인정하는 행정정보

다만, 국가의 안전보장과 관련된 행정정보와 비밀 또는 이에 준하는 행정정보는 이를 공동이용의 대상이 되는 정보에서 제외할 수 있다(「전자정부법」 제21조 제2항).

이 중에서 「전자정부법」상 공동이용의 대상이 되는 개인정보는 "행정기관"이 보유하고 있는 개인정보에만 한정되고, 공공기관이나 민간의 금융기관이 보유하고 있는 개인정보는 포함되지 않는다. 따라서 국민건강보험공단이나 국민연금관리공단 등의 공공기관이 보유하고 있는 개인정보는 「전자정부법」상의 행정정보공동이용의 대상이 되지 않는다(성낙인 외, 2008: 835). 「전자정부법」을 제외한 다른 법률에서 공동이용의 대상이 되는 개인정보를 명확하게 규정하지 않고 있으며, 「전자정부법」과 「공공기관의 개인정보보호에 관한 법률」상의 "공공기관" 개념이 서로 달라서, 혼란이 빚어지고 있다.[19]

개인정보 공동이용을 포함한 행정정보 공동이용은 단순히 e하나로민원 사이트에 적시되어 있는 71종의 정보에 국한되는 것이 아니며, 행정기관과 공공기관 및 민간 금융기관 사이에서 이용 및 제공이 이루어지는 광범위한 행

19) 「공공기관의 개인정보보호에 관한 법률」에서 "공공기관"은 국가행정기관·지방자치단체 그 밖의 공공단체 중 대통령령이 정하는 기관으로 행정기관이 포함되어 있다.

정정보가 이에 포함된다. 그러나 최근 정부 측에서 행정정보 공동이용과 관련하여 논의되는 사항들은 대부분 행정정보공동이용시스템을 통해 이루어지는, 민원처리를 위해 필요한 행정정보로 한정하고 있는데다 일반적인 제3자 제공을 전제로 하고 있어, 실제 논란이 될 수 있는 개인정보 공동이용의 보유목적 외 이용 또는 제공과 관련된 사항은 논의의 사각지대에 남겨지고 있다. 하지만 사실 개인정보 보호와 관련하여 문제되는 영역은 바로 행정기관들이 행정업무 수행에 참고하기 위해 이용 및 제공을 요청하는 개인정보들이라는 점에 유의해야 한다. 아래에서는 이를 행정정보 공동이용시스템을 통한 개인정보 수집·유통 실태에 대해 검토하고자 한다.

## 2. 행정정보 공동이용시스템을 통한 개인정보 수집·유통 실태

행정정보공동이용시스템은 국민들이 서류를 직접 발급받는 불편을 해소하고 민원서류를 감축하기 위해 각 기관에서 민원사무 처리 시에 구비서류를 제출받는 대신 구비서류에 해당되는 주민등록 등 행정정보를 직접 조회·확인하는 시스템을 말한다(행정안전부, 2008d: 54-59). 이러한 행정정보공동이용시스템에서도 다음과 같은 개인정보 보호의 원칙이 준수되어야 한다.

<표 2-3> 개인정보 보호의 주요 원칙

| 구분 | 수집 및 보유 | 다른 기관 제공 |
|---|---|---|
| 범위 | 목적달성에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집 | 업무수행에 필요한 최소한의 범위 안에서 사용목적·방법 등을 제한해 제공 |
| 활용 | 보유목적 외 활용 금지 | 사용목적 등 제한사항 불이행시 정보제공 중단 |
| 관리 | 정보의 정확성과 최신성 유지, 안전성 확보조치 | |
| 공개 | 개인정보의 수집·활용 등 사항 공개 → 정보열람권 등 정보주체의 권익보장 | |
| 파기 | 보유목적 달성 시 지체 없이 파기조치 | |

자료: 감사원(2008: 44).

### 1) 개인정보의 수집·구축

'일반적인 행정정보'는 행정기관 상호간에 공유하는 것이 바람직하며, 기업을 포함한 국민과도 공유될 필요가 있다. 이 점에서 행정정보공동이용 대상

정보를 확대하고 있는 것은 바람직하다.

현재 행정정보공동이용시스템을 통하여 행정기관 등에서 열람할 수 있는 구비서류는 71종이다. 행정안전부에 정보공개 청구하여 받은 자료나 행정안전부의 '행정정보 공동이용 지침'[제267호, 행정안전부예규, 2009.8.28]에 따르면 71종으로 나와 있고, 행정정보 공동이용 사이트인 e하나로민원(http://pr.share.go.kr)에서도 현재 민원 신청시 행정기관에 제출하지 않아도 되는 구비서류가 71종이라고 밝히고 있다. 하지만 국가보훈처의 '행정정보공동이용 지침'[제34호, 국가보훈처예규, 2009.9.1]에 따르면 대법원의 법원행정처에서 관리하는 가족관계정보, 혼인관계정보, 입양관계정보, 그리고 기본정보 4종이 추가되어 17개 기관 75종으로 나와 있으며, e하나로민원에서 밝힌 '행정정보공동이용 보유정보(구비서류)별 이용기관 및 주요 이용사무 현황'('09.7.14기준)에 따르면 행정정보 공동이용 대상정보는 대법원의 가족관계정보를 포함 총 72종으로 나와 있어, 공식적인 발표와 다르게 되어 있다.

공공기관·금융기관의 경우에도 제출하지 않아도 되는 구비서류가 있는데, 이는 기관별로 다르며, 그에 대해서는 e하나로민원 사이트에서 공공기관 고객업무[20]와 은행 고객업무[21]로 나누어서 해당 기관이나 은행의 고객업무별로 제출하지 않아도 되는 구비서류를 확인할 수 있도록 하고 있다.

<표 2-4> 행정정보 공동이용 대상정보

| 보유기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| 외교통상부 (2종) | 여권정보 | 여권과 | 2006 | 여권법 제4조 및 제7조 | 국외여행허가자 관리, 국세 체납처분, 근로기준법 위반사실 신고사건처리, 병역의무 이행일자 연기신청, 국외이주자 관리 등 |
| | 해외이주신고확인서 | 재외동포정책2과 | 2006 | 해외이주법 제6조<br>해외이주법 시행령 제5조 제2항 | 주민생활지원대상자 조사·관리, 국세 체납처분, 국외여행허가자 관리, 국민기초생활보장 수급자관리, 국외이주신고등 |
| 법무부 (4종) | 국내거소신고사실증명 | 외국적동포과 | 2006 | 재외동포의 출입국과 법적 지위에 관한 법률 제7조제5항, 재외동포의 출입국과 법적지위에 관한 법률 시행규칙 제11조 | 장애인자동차표지 발급(재발급), 재산제세 과세자료 수집 및 처리, 재산제세 세무조사 대상선정 및 조사, 재산제세 관련 감면 사후관리, 보호관찰대상자등의 조사업무 등 |
| | 출입국사실 | 출입국 | 2005 | 출입국관리법 제88조제1항 | 민방위교육훈련유예(면제)신청, 민방 |

20) http://pr.share.go.kr/fa/fa010/ehanaro/popular_public.jsp?menuId=A4&subMenuId=AS2
21) http://pr.share.go.kr/fa/fa010/ehanaro/popular_finance.jsp?menuId=A4&subMenuId=AS3

| 보유 기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| | 증명 | 심사과 | | 출입국관리법 시행규칙 제75조 | 위대편성 및 관리, 주민생활지원대상자 조사 및 관리, 일반여권발급신청, 주민등록사실조사 등 |
| | 외국인등록사실증명 | 출입국심사과 | 2005 | 출입국관리법 제32조 및 제88조제2항, 출입국관리법 시행규칙 제47조 | 시·도간 자동차 변경등록 신청, 균등할주민세 관리, 장애인자동차표지발급(재발급), 자동차 신규등록(부활차) 신청, 국내원천소득원천징수 세원관리 등 |
| | 외국인부동산 등기등록증명 | 체류정책과 | 2008 | 부동산등기법 제41조의2제1항제4호, 법인 아닌 사단·재단 및 외국인의 부동산 등기용 등록번호 부여절차에 관한 규정 제15조 | 국세 체납처분, 재산형 집행(벌금, 추징금, 과태료 등) 통합업무 등 |
| 행정안전부 (6종) | 상훈수여증명 | 상훈담당관 | 2007 | 상훈법 제2조, 상훈법 시행령 제31조제4항 및 제5항 | 국가유공자(유족)등록, 독립유공자(유족)등록, 국립묘지안장(이장)신청, 포상업무, 군사범죄수사 등 |
| | 주민등록등(초)본 | 주민제도과 | 2002 | 주민등록법 제7조, 주민등록법 시행령 제6조, 주민등록법 시행규칙 제15조 | 직불제사업·산지유통사업 등 농림사업 신청, 지방세 비과세감면, 자동차 및 건설기계 등록 변경, 등기신청업무, 예금신규 등 |
| | 지방세납세증명서 | 지방세분석과 | 2002 | 지방세법 제38조, 지방세법 시행령 제19조, 지방세법 시행규칙 제14조 | 대금지불용, 신용보증 업무, 지방세납세증명서 발급, 차량 변경·이전 등록, 온라인대금청구 등 |
| | 지방세 과세(납세) 증명서(자동차세) | 지방세분석과 | 2002 | 지방세법 제196조의3 및 제196조의13 | 차량변경·이전 등록, 대금지불용, 국민기초·긴급복지·차상위계층조사, 사회복지, 긴급복지지원 등 |
| | 세목별과세증명서(건물/주택/토지) | 지방세분석과 | 2008 | 지방세법 제195조 | 재산제세 과세자료 수집 및 처리, 공익사업을 위한 토지 등의 취득 및 보상업무, 재산제세 세무조사 대상선정 및 조사 등, 종합부동산세 부과자료 검토, 근로장려세제 심사업무 등 |
| | 인감정보 | 주민제도과 | 2009 | 인감증명법 제4조<br>인감증명법 시행규칙 제12조 | 관광(단)지 조성사업 허가(협의).<br>게임제작(배급)업 등의 영업자 지위승계 신고, 부동산거래정보 사업자지정, 나라장터 경쟁입찰 참가자격 등록, 학원설립자 변경등록 등 |
| 농림수산식품부 (4종) | 선박국적증서 (어선) | | 2008 | 어선법 제13조제3항제1호<br>어선법 시행규칙 제33조 | 기업대출(신용 및 담보), 기업대출(부산은행), 신용조사 및 여신심사, 시험어업 신청, 원양어업허가 등 |
| | 선적증서 | | 2008 | 어선법 제13조제3항제2호<br>어선법 시행규칙 제33조 | 중소기업 신용대출, 중소기업 정책자금 지원 및 ABS 후순위채 인수, 영농상속신고 등 |
| | 어선등록필증 | | 2008 | 어선법 제13조제3항제3호<br>어선법 시행규칙 제33조 | 국세 체납처분, 신용조사 및 여신심사, 정책자금대출, 재활용 부과금, 법 |

| 보유 기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| | | | | | 률구조신청, 어업인 등 |
| | 어업면허증 | | 2008 | 수산업법 제8조 | 기업자금대출, 사증발급 인정서 발급, 지방세 부과징수, 영농상속신고, 법률구조신청, 어업인 등 |
| 지식경제부 (2종) | 공장등록증명 | 입지총괄과 | 2007 | 산업집적활성화 및 공장설립에 관한 법률 제16조, 산업집적활성화 및 공장설립에 관한 법률 시행규칙 제10조 | 나라장터 경쟁입찰 참가자격 등록, 입찰 및 수의시담, 지방세 부과징수, 국세 체납처분, 공장등록증명 등 |
| | 석유판매업 등록증 | 석유산업과 | 2008 | 석유 및 석유대체연료사업법 제10조, 동법 시행규칙 제4조 | - |
| 보건복지 가족부 (2종) | 국민기초생활 수급자증명 | 기초생활보장과 | 2006 | 국민기초생활 보장법 제2조제2호<br>국민기초생활 보장법 시행규칙 제40조 | 복지할인 신청 접수, 학비지원 및 감면, 영업일반업무·TV 대수 등록 면제 말소, 자동차사고 피해가족 지원사업, 제증명발급시수수료감면대상(국가유공자)확인 등 |
| | 장애인증명 | 장애인정책과 | 2006 | 장애인복지법 제32조<br>장애인복지법 시행규칙 제9조 | 복지할인 신청 접수, 영업일반업무·TV 대수 등록 면제 말소, 장애인등록업무, 가사사정으로 인한 병역감면 신청, 장애인등록증 기재사항 변경신청 등 |
| 환경부 (7종) | 사업장폐기물배출자신고증명서(제18조제2항제1호 및 제2호) | 산업폐기물과 | 2008 | 폐기물관리법 제17조제2항, 폐기물관리법 시행규칙 제18조제2항제1호 및 제2호 | 재활용부과금, 올바로시스템 승인 처리 및 기초정보 구축 등 |
| | 사업장폐기물배출자 신고증명서(제18조제2항제3호) | 사업폐기물과 | 2008 | 폐기물관리법 제17조제2항, 폐기물관리법 시행규칙 제18조제2항제3호 | 올바로시스템 승인 처리 및 기초정보 구축, 재활용 부과금, 도로 및 하천공사 폐기물관리 등 |
| | 폐기물수집운반업 허가증 | | 2008 | 폐기물관리법 제25조제3항, 폐기물관리법 시행규칙 제28조제3항제1호 및 제6항 | 재활용부과금, 올바로시스템 승인 처리 및 기초정보 구축 등 |
| | 폐기물(중간/최종/종합)처리업허가증 | | 2008 | 폐기물관리법 제25조제3항, 폐기물관리법 시행규칙 제28조제3항제2호 및 제6항 | 재활용부과금, 올바로시스템 승인 처리 및 기초정보 구축 등 |
| | 폐기물처리시설 설치승인서 | | 2008 | 폐기물관리법 제29조제2항, 폐기물관리법 시행규칙 제39조제1항 및 제2항 | 재활용부과금, 올바로시스템 승인 처리 및 기초정보 구축 등 |
| | 폐기물처리시설 설치신 | | 2008 | 폐기물관리법 제29조제2항, 폐기물관리법 시행규칙 | 재활용부과금, 올바로시스템 승인 처리 및 기초정보 구축 등 |

| 보유기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| | 고증명서 | | | 제40조제1항 및 제2항 | |
| | 폐수배출시설 설치(허가증/신고증명서) | 산업폐수과 | 2008 | 수질 및 수생태계 보전에 관한 법률 제33조제1항, 수질 및 수생태계 보전에 관한 법률 시행규칙 제36조 | 지방세 부과징수, 재활용 부과금, 폐기물 위탁·처리신고, 신용조사·보증심사·기술평가, 공장설립(변경)승인신청 등 |
| 노동부 (1종) | 국가기술자격증(한국산업인력공단 발급분에 한함) | 자격제도팀 | 2006 | 국가기술자격법 제13조, 국가기술자격법 시행규칙 제28조 및 제31조 | 공무원신규임용(교육과학기술부), 이(미)용사 면허, 신용보증 업무, 건설기계조종사 면허증 발급신청, 골재채취업등록 등 |
| 국토해양부 (23종) | 토지대장 | 국토정보센터 | 2002 | 지적법 제2조제1호가목 | 쌀소득등보전직접지불제, 공익사업을 위한 토지 등의 취득 및 보상업무, 국유재산 관리업무, 등기신청서 부본 입력 및 정정, 재산제세 과세자료 수집 및 처리 등 |
| | 임야대장 | 국토정보센터 | 2002 | 지적법 제2조제1호가목 | 복식부기 회계제도관련 자산 및 부채 실사 평가, 국유재산 사용수익허가·대부·매수(기획재정부), 국세 체납처분, 농지관리, 상시전력 신규신청 등 |
| | 지적도 | 국토정보센터 | 2008 | 지적법 제2조제1호가목 | 공익사업을 위한 토지 등의 취득 및 보상업무, 국유재산 관리업무, 지방세 체납관리, 재산제세 과세자료 수집 및 처리, 국공유재산관리 등 |
| | 임야도 | 국토정보센터 | 2008 | 지적법 제2조제1호가목 | 공익사업을 위한 토지 등의 취득 및 보상업무, 국유재산 관리업무, 지방세 체납관리, 재산제세 과세자료 수집 및 처리, 국공유재산관리 등 |
| | 건설기계등록증 | 건설인력기재과 | 2008 | 건설기계관리법 제3조제3항, 건설기계관리법 시행규칙 제2조제1항 | 지방세 체납관리, 운행제한위반차량운전자/차주주소와차량소유자확인, 가계대출(신용 및 담보), 신용조사 및 여신심사, 기업여신등 |
| | 건설기계등록원부(갑/을) | 건설인력기재과 | 2002 | 건설기계관리법 제7조 건설기계관리법 시행규칙 제11조제1항 | 국세 체납처분, 신용보증·신규 증액·신용조사, 건설업등록, 폐기물수집·운반증 발급, 건설기계등록등 |
| | 건설기계검사증 | 건설인력기재과 | 2008 | 건설기계관리법 제13조제4항, 건설기계관리법 시행규칙 제28조 | 기업여신, 가계대출(신용 및 담보), 기업대출(신용 및 담보), 신용조사 및 여신심사, 여신(기업담보) 등 |
| | 건설기계사업등록증 | 건설인력기재과 | 2008 | 건설기계관리법 제21조 건설기계관리법 시행규칙 제2조 | 신용조사 및 여신심사, 신용보증·기보증회수보증, 운행제한위반차량운전자/차주주소와차량소유자확인, 기업담보대출, 신용보증·신용조사 심사 등 |
| | 건설업등록증 | 건설정책과 | 2008 | 건설산업기본법 제9조, 건설산업기본법 시행규칙 제 | 지방세 부과징수, 신용보증 업무, 기업담보여신, 기업신용여신, 기업대출 |

| 보유 기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| | | | | 9조 및 제10조 | (신용대출) 등 |
| | 건축허가서 | 건축기획과 | 2006 | 건축법 제11조, 건축법 시행규칙 제8조 | 상시전력 신규신청, 지장배전선로 이설신청, 신용보증업무, 개별공시지가 조사 및 통보관련업무, 국유재산관리업무 등 |
| | 사용승인서 | 주택건설과 | 2002 | 건축법 제22조, 건축법 시행규칙 제16조 | 국민주택기금 전세자금대출, 적격심사·계약체결·대금지급, 국민주택기금대출 조건변경 업무, 종합부동산세 부과자료 검토, 신용보증·신규 증액·보증심사 |
| | 건축물관리대장 (일반/집합) | 건축기획과 | 2002 | 건축법 제38조, 건축물대장의 기재 및 관리 등에 관한 규칙 제4조 및 제7조 | 소방검사, 등기신청서 부본 입력 및 정정, 사용자 기본사항 변경(명의 변경 등), 공익사업을 위한 토지 등의 취득 및 보상업무, 상시전력 신규신청 등 |
| | 건축사업무 신고필증 | 건축기획과 | 2008 | 건축사법 제23조, 건축사법 시행규칙 제16조 | 지방세 부과징수, 신용카드회원업무, 개인신용대출, 적격심사·계약체결·대금지급 중소기업 정책자금 지원 및 ABS 후순위채 인수 등 |
| | 토지이용계획확인서 | 국토정보센터 | 2008 | 토지이용규제 기본법 제10조제1항, 토지이용규제 기본법 시행규칙 제2조제1항 | 공익사업을 위한 토지 등의 취득 및 보상업무, 국유재산 관리업무, 재산제세 과세자료 수집 및 처리, 지방세 체납관리, 국공유재산관리 등 |
| | 개별공시지가확인서 | 부동산평가과 | 2002 | 부동산 가격공시 및 감정평가에 관한 법률 제11조, 부동산 가격공시 및 감정평가에 관한 법률 시행규칙 제20조 | 국유재산 관리업무, 등기신청서 부본 입력 및 정정, 지방세 체납관리, 주민생활지원대상자 조사 및 관리, 공공용지 취득 및 손실보상업무 등 |
| | 자동차등록원부(갑/을) | 자동차관리과 | 2002 | 자동차관리법 제7조 자동차등록규칙 제5조 | 무인교통단속에 의한 과태료 부과·징수, 보험료(기타징수금)체납처분, 주민생활지원대상자 조사 및 관리, 국세 체납처분, 보험료(기타징수금)결손처분 등 |
| | 자동차등록증 | 자동차관리과 | 2008 | 자동차관리법 제8조제2항 자동차등록규칙 제4조 | 국세 체납처분, 운행제한위반차량운전자/차주주소와차량소유자확인 등 |
| | 이륜자동차사용신고필증 | 자동차관리과 | 2002 | 자동차관리법 제48조제1항 자동차관리법 시행규칙 제99조 | 이륜자동차사용폐지신고, 부동산 비과세감면 접수처리, 각종 급여신청, 이륜자동차신고사항변경신고, 가사사정으로 인한 병역감면신청 등 |
| | 주택건설사업사용검사필증 | 주택건설과 | 2002 | 주택법 제29조제1항 주택법 시행규칙 제15조 | 국민주택기금 전세자금대출, 신용보증, 신규 증액, 보증심사 등 |
| | 선박원부 | 해상안전정책 | 2007 | 선박법 제8조, 선박법 시행규칙 제11조 | 지방세 감면신청, 신용보증 업무, 국민기초생활보장 수급자관리, 어장정 |

| 보유 기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| | | 과 | | | 화·정비업 등록, 영농상속신고 등 |
| | 선박국적증서 (상선) | | 2008 | 선박법 제8조, 선박법 시행규칙 제12조 | 선박원부변경등록, 선박국적증서(가선박국적증서) 영역서교부 등 |
| | 선박검사증서 | | 2008 | 선박안전법 제9조제1항 선박안전법 시행규칙 제13조 | 기업대출(부산은행), 정책자금대출, 여객선 종선 심사신청, 해수면 유·도선사업 면허(신고), 사증발급 인정서 발급 등 |
| | 부동산등기용 등록번호증명 | | 2008 | 부동산등기법 제41조의2제1항제1호 및 제3호, 법인 아닌 사단·재단 및 외국인의 부동산등기용 등록번호 부여절차에 관한 규정 제7조 및 제8조 | 공익사업을 위한 토지 등의 취득 및 보상업무, 종합부동산세 부과자료 검토, 중소기업 정책자금 지원 및 ABS 후순위채 인수, 개인대출-주택담보-신규연장 조건변경-개인, 비축토지·비축토지 관리 등 |
| 국가보훈처 (2종) | 국가유공자 (유족)확인 | 보상관리과 | 2005 | 국가유공자 등 예우 및 지원에 관한 법률 제6조 | 복지할인 신청 접수, 자동차세 감면, 주민생활지원대상자 조사 및 관리, 민방위대편성 및 관리, 영업일반업무·TV 대수 등록 면제 말소 등 |
| | 취업지원(보호) 대상자증명 | 생활안정과 | 2006 | 국가유공자 등 예우 및 지원에 관한 법률 제29조, 특수임무수행자 지원 및 단체설립에 관한 법률 제19조 | 소방공무원 채용시험, 인력채용, 갱생보호서비스 업무수행 직원 인사·갱생보호업무수행직원 인사사무처리, 공무원신규임용 및 건강보험증발급, 직원채용 등 |
| 국세청 (6종) | 소득금액증명 | 소득세과 | 2002 | 소득세법 제4조 | 피의자보상급 지급청구, 정비사업전문관리업등록, 유족구조금 지급 신청 |
| | 납세사실증명 | 징세과 | 2002 | 소득세법 제76조 부가가치세법 제18조 및 제19조 | 범죄수사, 군사범죄수사생계유지곤란, 병역감면처리, 공직선거후보자 등록신청 접수 |
| | 폐업사실증명 | 부가가치세과 | 2002 | 부가가치세법 제5조 | (사업장적용시)등록사업자 확인, 지방세 부과징수, 행정업무 처리, 주민생활지원대상자 조사 및 관리, 국민기초생활보장 수급자관리 등 |
| | 휴업사실증명 | 부가가치세과 | 2002 | 부가가치세법 제5조 | (사업장적용시)등록사업자 확인, 지방세 부과징수, 사업장 체납보험료 등 징수독려, 행정업무 처리, 가입자 소득 유무 확인 등 |
| | 국세납세증명서 | 징세과 | 2002 | 국세징수법 제6조 | 대금수령, 온라인대금청구, 거주여권발급신청, 토지보상업무, 보세구역내 물품 및 용역공급업의 등록(갱신) 등 |
| | 사업자등록증명 | 부가가치세과 | 2002 | 법인세법 제111조, 부가가치세법 제5조 | (사업장적용시)등록사업자 확인, 지방세 부과징수, 나라장터 경쟁입찰 참가자격 등록, 행정업무 처리, 시·도간 자동차 변경등록 신청 |
| 관세청 (2종) | 수출신고필증 | 통관기획과 | 2008 | 관세법 제248조제1항 | 신용보증 업무, 자동차 신규등록(신조차·수입차) 신청, 외환거래업무, |

| 보유 기관 | 대상정보 | 부서 | 서비스 시기 | 관련 법령 | 주요 이용사무 |
|---|---|---|---|---|---|
| | | | | | 수출입관련 자금영수 및 지급, 수출환어음매입(추심) 등 |
| | 수입신고필증 | 통관기획과 | 2008 | 관세법 제248조제1항 | 자동차 신규등록 신청, 폐기물부담금 부과·징수·체납·결손 처분, 외환거래업무, 재활용 부과금, 신용보증 업무 등 |
| 병무청 (1종) | 병적증명서 | 공개심사팀 | 2005 | 병역법 제5조제3항<br>병역법 시행규칙 제7조 및 제8조 | 일반여권발급신청, 의무경찰 모집 업무, 저소득확인, 주민생활지원대상자 조사 및 관리, 국가유공자(유족)등록 등 |
| 경찰청 (1종) | 운전면허정보 | 교통기획담당관 | 2006 | 도로교통법 제80조 | 개인택시운송사업 대리운전신고, 건설기계조종사 면허증 발급신청, 현역병지원, 건설기계 조종사 면허 발급, 재해보상·보상심사 업무(유족보상금, 장해급여,공무상요양) 등 |
| 특허청 (4종) | 특허등록원부 | 등록서비스팀 | 2007 | 특허법 제85조, 특허등록령 제1조의2 | 신용조사·보증심사·기술평가, 신용보증·보증상담, 신용보증 업무, 계약·지출업무, 국세 체납처분 등 |
| | 실용신안등록원부 | 등록서비스팀 | 2007 | 실용신안법 제18조<br>실용신안등록령 제2조 | 신용조사·보증심사·기술평가, 신용보증 업무, 계약·지출업무, 기업대출(신용 및 담보), 관세법 위반수사 등 |
| | 디자인등록원부 | 등록서비스팀 | 2007 | 디자인보호법 제37조<br>디자인등록령 시행규칙 제1조의2 | 신용조사·보증심사·기술평가, 신용보증 업무, 계약·지출업무, 연구개발특구 입주변경승인, 징수관리 등 |
| | 상표원부 | 등록서비스팀 | 2007 | 상표법 제39조, 상표등록령 제1조의2 | 상표권(전용사용권) 신고, 신용조사·보증심사·기술평가, 국세 체납처분, 관세법 위반수사, 신용보증 업무 등 |
| 해양경찰청 (1종) | 폐기물 위탁처리 신고증명서 | 해양배출물관리과 | 2007 | 해양환경관리법 제76조제1항, 해양환경관리법 시행규칙 제45조제2항 | 계약, 지출업무, 세무조사, 범죄수사, 재활용 부과금 등 |
| 대법원 (7종) | 건물등기부등본 | 등기호적심의관 | 2002 | 부동산등기법 제14조 | 지방세과세자료확인, 토지소유자 정리 등, 지방세 체납관리, 국세 체납처분, 부동산.법인 등기전산정보자료 열람등 |
| | 토지등기부등본 | 등기호적심의관 | 2002 | 부동산등기법 제14조 | 토지소유자 정리, 공익사업을 위한 토지 등의 취득 및 보상업무, 지방세과세자료확인, 국유재산 관리업무, 부동산.법인 등기전산정보자료 열람 등 |
| | 법인등기부등본 | 등기호적심의관 | 2002 | 상업등기법 제5조 | 지방세과세자료확인, 지방세 체납관리, 부동산.법인 등기전산정보자료 열람, 법인세무조사, 나라장터 경쟁입찰 참가자격 등록등 |

자료: 행정정보 공동이용 지침[제267호, 행정안전부예규, 2009.8.28]; 국가보훈처 행정정보공동이용 지침[제34호, 국가보훈처예규, 2009.9.1]; e하나로민원 제출하지 않아

도 되는 구비서류; ‘행정정보공동이용시스템 관련 정보공개 청구’에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.14) 중 공동이용 행정정보(구비서류) 현황(17개 기관 71종); 행정정보공동이용 보유정보(구비서류)별 이용기관 및 주요 이용사무 현황(’09.7.14기준).

행정정보 공동이용 민원사이트인 e하나로민원(http://pr.share.go.kr/)은 행정정보 공동이용이 개인정보 보호에도 이점이 있다고 밝히고 있지만, 한 쪽 면만을 보고 있어 이를 전적으로 받아들이기는 어렵다.

첫째, 종이서류에는 모든 정보가 기재되어 불필요한 개인정보가 노출될 수 있지만, e하나로민원에서는 필요한 정보만 제공되므로 더 안전하다고 본다. 예를 들어, 본인의 주소 확인을 위하여 주민등록등(초)본을 제출하는 경우, 가족관계 및 가족의 주민등록번호까지 함께 노출되지만, e하나로민원에서는 그렇지 않다는 것이다. 하지만 종이서류의 경우에도 필요정보만 노출되도록 통제할 수 있다는 점에서 e하나로민원이 더 안전하다고 할 수는 없다.

둘째, e하나로민원은 개인정보가 중복 수집되는 것을 막을 수 있다는 이점이 있다고 한다. 예를 들어, 여권신청을 할 때도 주민등록등(초)본을 제출해야 하고, 신용보증기금을 신청할 때도 주민등록등(초)본을 제출해야 하는데, 이는 개인의 입장에서 보면 중복제출인 셈이다. 하지만 온라인으로 필요한 정보만 열람하게 할 경우 개인정보의 중복 수집과 노출을 방지할 수 있게 된다는 것이다. 물론 e하나로민원이 민원인의 편의를 제공하는 것은 사실이지만, 어차피 온라인으로 필요한 정보를 수집하는 것이므로 개인정보의 중복 수집 자체를 막는 것은 아니라고 봐야 한다.

셋째, 종이서류의 위변조 및 유출 우려를 해소하는 이점이 있다. 각 이용기관에서 수집한 종이서류는 언제든지 위변조될 우려가 있으며, 유출될 염려가 있지만, e하나로민원에서는 온라인으로 필요한 정보만 실시간으로 열람할 수 있게 되어 종이서류의 위변조 및 유출문제를 근본적으로 방지할 수 있다는 것이다. 이에 대해서도 위변조 문제가 종이서류 뿐만 아니라 디지털 정보의 경우에도 발생할 수 있다는 사실을 간과하고 있다고 지적할 수 있다. 또한 공무원에 의한 개인정보 유출 문제는 디지털 정보의 경우 그 범위와 피해정도가 훨씬 크다는 점도 염두에 두어야 한다.

넷째, e하나로민원은 법적 근거에 따라 안전하게 이용되며 보호받고 있다고 하면서, 「전자정부법」 제22조의2 (공공기관 등의 행정정보 공동이용), 「전자정부법」 제22조의3 (행정정보취급·이용자의 의무), 제53조(벌칙), 「공공기관의 개인정보보호에 관한 법률」 제10조 제3항을 들고 있다. 하지만 이

러한 규정들은 행정정보공동이용에 대한 근거를 제공할지는 몰라도 개인정보 보호를 위한 근거는 되지 않는다.

다섯째, 현재 e하나로민원에서는 민원처리시마다 반드시 본인의 사전동의가 있는 경우에만 정보를 열람할 수 있도록 되어 있다. 만약, 행정정보 공동이용을 원하지 않는 경우 종이서류를 발급받아 제출해도 된다. 이 또한 개인정보 열람이 합법적으로만 진행된다고 가정하고 있다. 본인의 사전 동의를 받는다고 하지만, 사전 동의를 거치지 않은 무단 열람이 존재할 가능성을 배제할 수 없으며, 이를 감안하면 오히려 개인정보 보호측면에서 더 취약해지는 셈이 된다.

결국 전반적으로 e하나로민원이 민원인의 편의를 제공하기는 하지만, 개인정보 보호문제를 해결하는 것은 아니라고 봐야 한다. 온라인에 의한 민원서비스 제공을 통해 개인정보를 전산화하기에 앞서, 과연 꼭 필요한 정보들만 수집되고 있는지, 즉 현재 제출이 요구되고 있는 민원서류들이 반드시 필요한 것인지 자체에 대한 검토가 선행되어야 할 것이다.

나아가 e하나로민원을 통한 행정정보공동이용이 설사 이점이 있다고 하더라도, 이는 단지 국민들을 대상으로 한 민원서비스에게만 의미가 있을 뿐이며, 행정기관간 개인정보의 제공 및 공동이용에 따른 부작용 문제는 간과되고 있다는 점도 주목해야 한다. 그리고 우리 국민들은 개인정보 공동이용의 효용성에도 불구하고 공공기관이 개인정보 DB를 구축하거나 그것을 다른 기관과 공유하는 것, 그리고 행정정보의 공동이용에 대해 전반적으로 부정적인 입장을 가지고 있다는 점(성낙인 외, 2008: 223-243) 또한 무시해선 안된다.

행정기관이 보유하고 있는 개인정보 모두가 공적 정보(public information)인 것은 아니며, “개인의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보”는 정보공개의 대상에서 제외되어야 한다(「공공기관의 개인정보보호에 관한 법률」 제9조 제1항 제6호). 개인정보 공동이용은 행정기관 상호간에 필요한 개인정보를 주고받아 ‘내부적으로 이용’하는 것이라는 점에서 외부로 공개하는 것은 아니지만, ‘개인정보DB 통합에 따른 빅브라더의 출현가능성’과 함께 행정정보공동이용의 확대와 함께 개인정보 공동이용이 무차별적으로 이루어질 가능성이 있어 문제가 된다.

현재는 ‘일반행정정보의 공동이용’과 ‘개인정보의 공동이용’이 구분되지 않고, 행정정보공동이용이라는 이름 아래 함께 다루어지고 있다. 실제 ‘개인정보 공동이용’이라는 용어는 법률의 어디에도 나오고 있지 않지만, 행정정보공

동이용에 관한 법 규정은 사실상 개인정보 공동이용에 관한 것이다(성낙인 외, 2008: 839-840). 현행법은 공동이용을 행정기관의 의무로 하면서 행정정보공동이용센터를 통해 이루어지도록 강제하고 있다.

그래서 행정정보공동이용 제공정보 중에서 개인정보를 포함하고 있는 정보에 대해 행정안전부에 정보공개 청구한 결과, 행정안전부 행정정보공유추진단에서는 각 정보의 개인정보 포함여부는 각 정보 보유기관에서 파악하도록 하고 있으며, 행정정보공동이용시스템 제공정보 선정 절차에 대해서도 공동이용시스템을 통하여 제공하는 정보는 각 기관에서 업무 처리 시 필요로 하는 행정정보(구비서류)를 조사한 후, 이 중 이용 빈도수가 높고 해당 정보(구비서류)가 전자화(DB화)되어 있는 정보를 우선적으로 선정하여 서비스하고 있다고만 밝히고 있다.[22] 만약 그렇다면 더욱 심각한 문제라 할 수 있다. 왜냐하면 「전자정부법 시행령」 제26조는 행정정보공동이용센터가 공동이용한 행정정보의 유지·관리에 힘쓰고, 행정정보 공동이용 및 개인정보보호 실태에 대한 현황을 파악해야 한다고 규정하고 있는데, 개인정보보호 실태 파악에서 빼놓을 수 없는 것 중의 하나가 개인정보의 공동이용 현황 파악인데도, 행정정보공동이용센터조차 개인정보의 공동이용 현황을 파악하지 못하거나 파악하지 않고 있다는 의미가 되기 때문이다.

### 2) 개인정보의 이용 및 제공

(1) 이용 및 제공 실태

현재 행정정보공동이용시스템을 통해 행정정보를 공동이용하고 있는 이용기관은 379개로 나타나고 있다.

<표 2-5> 행정정보공동이용 이용기관 현황(379개)

('09. 8. 7.)

| 중 앙 기 관 | |
|---|---|
| 52개 | 대통령실, 감사원, 국가정보원, 방송통신위원회, 민주평화통일자문회의, 국가인권위원회, 국무총리실, 법제처, 국가보훈처, 공정거래위원회, 금융위원회, 국민권익위원회, 기획재정부, 교육과학기술부, 외교통상부, 통일부, 법무부, 국방부, 행정안전부, 문화체육관광부, 농림수산식품부, 지식경제부, 보건복지가족부, 환경부, 노동부, 여성부, 국토해양부, 국세청, 관세청, 조달청, 통계청, 대검찰청, 병무청, 방위사업청, 경찰청, 소방방재청, 문화재청, 농촌진흥 |

22) '행정정보공동이용시스템 관련 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.14).

| | |
|---|---|
| | 청, 산림청, 중소기업청, 특허청, 식품의약품안전청, 기상청, 해양경찰청, 행정중심복합도시건설청, 진실화해를위한과거사정리위원회, 친일반민족행위자재산조사위원회, 태평양전쟁전후국외강제동원희생자지원위원회, 국회, 대법원, 헌법재판소, 중앙선거관리위원회 |
| 자 치 단 체 | |
| 262개 | 시・도(16개), 시・군・구(230개), 시・도 교육청(16개) |
| 공 공 기 관 | |
| 49개 | 기술신용보증기금, 농수산물유통공사, 대한법률구조공단, 대한주택보증주식회사, 대한지적공사, 사립학교교직원연금관리공단, 한국예탁결제원, 한국법무보호복지공단, 한국공항공사, 한국농어촌공사, 한국산업인력공단, 한국수출보험공사, 한국자산관리공사, 한국장애인고용촉진공단, 한국전기안전공사, 한국토지공사, 교통안전공단, 공무원연금관리공단, 국민건강보험공단, 국민연금공단, 근로복지공단, 대한주택공사, 신용보증기금, 중소기업진흥공단, 한국전력공사, 한국주택금융공사, 부산광역시시설관리공단, 한국전기공사협회, 한국철도시설공단, 한국환경자원공사, 평생교육진흥원, 한국산업단지공단, SH공사, 서울신용보증재단, 부산신용보증재단, 대구신용보증재단, 인천신용보증재단, 광주신용보증재단, 대전신용보증재단, 울산신용보증재단, 경기신용보증재단, 강원신용보증재단, 충북신용보증재단, 충남신용보증재단, 전북신용보증재단, 전남신용보증재단, 경북신용보증재단, 경남신용보증재단, 제주신용보증재단 |
| 금 융 기 관 | |
| 16개 | 우리은행, 기업은행, 신한은행, 하나은행, 외환은행, 국민은행, 대구은행, 부산은행, 광주은행, 제주은행, 전북은행, 경남은행, SC제일은행, 씨티은행, 농업협동조합중앙회, 수산업협동조합중앙회, |

※ 대통령실(경호처), 제주도(제주시), 제주도(서귀포시)는 기관특성을 고려하여 별도로 인정.

자료: e하나로민원 사이트(http://pr.share.go.kr/).

행정정보공동이용시스템은 기관총괄책임자(행정안전부 관리), 권한부여책임자 및 업무처리담당자(기관 직접 관리) 등 3가지로 사용자를 구분하고 있는데, 이들이 행정정보공동이용시스템에 접근할 수 있는 접근권한이 등록되어 있다. 행정정보 공동이용시스템 접근권한은 행정정보공동이용센터에서 기관총괄책임자(부서장)를 승인하면 각 이용기관별 기관총괄책임자가 기관 내 부서별로 권한부여 책임자를 지정하고, 각 기관의 권한부여책임자는 업무분장 등을 확인한 후 업무처리 시 필요한 공동이용정보(구비서류)에 대한 접근권한을 업무처리담당자에게 부여하게 된다고 한다. 행안부는 제278회 국회(정기회) 행안위 국정감사 서면답변에서 실제 시스템에 접속하는 사용자의 관리를 기관에 위임하여 사실상 실태 파악이 안 되고 있다는 지적에 대해 업무처

리담당자에게 직접 접근권한을 부여하는 이유는 '행정정보 공동이용기관수가 많아 공동이용센터에서 업무처리담당자의 접근권한을 일일이 관리하는 것은 사실상 불가능하고, 업무처리담당자의 담당사무와 그에 필요한 구비서류 정보가 무엇인지를 확인한 후 이루어져야 하는 접근권한의 부여는 각 이용기관에서 가장 잘 수행할 수 있기 때문'이라고 밝히면서, 행정정보공동이용센터에서는 각 이용기관에서 등록한 접근권한 현황을 파악하고 있다고 언급하고 있다(행정안전부, 2008d: 54-59).

<그림 2-1> 행정정보 공유시스템 구성도


하지만 행정정보 공동이용시스템에 대해 각 이용기관에서 등록한 접근권한 현황(각 이용기관별 열람권자)을 직접 정보공개 청구하였더니, 행정안전부 행정정보공유추진단은 「공공기관의 정보공개에 관한 법률」 제9조제1항제5호[23]에 의거하여 제공이 불가하다고 통보하였다.[24]

23) 「공공기관의 정보공개에 관한 법률」 제9조 (비공개대상정보) ①공공기관이 보유·관리하는 정보는 공개대상이 된다. 다만, 다음 각호의 1에 해당하는 정보에 대하여는 이를 공개하지 아니할 수 있다.
5. 감사·감독·검사·시험·규제·입찰계약·기술개발·인사관리·의사결정과정 또는 내부검토과정에 있는 사항 등으로서 공개될 경우 업무의 공정한 수행이나 연구·개발

현재 행정정보 공동이용 서비스는 민원인을 위한 'e하나로민원'(http://pr.share.go.kr/), 공무원의 열람업무를 위한 'e하나로민원'(http://www.share.go.kr/), 공무원의 업무처리시스템에 심겨진 '표준API', 제공기관과 이용기관 사이에서 대량정보를 중계하는 '중계서비스', 금융기관을 위한 '전용브라우저' 등의 형태로 구현되어 있다.

2006년 8월 행정정보 공동이용 확대를 안정적으로 지원하기 위해 G4C시스템에서 행정정보 공동이용 기능을 분리하여 행정정보 공동이용시스템을 별도로 구축하고, 기존에 구축한 행정정보 중계시스템[25]도 기능을 고도화하는 작업을 수행하였다.

『2007 행정정보공동이용 백서』에 따르면, 행정정보 공동이용시스템의 확충과 이용기관 확대에도 주력한 결과, 아래와 같이 행정정보 공동이용시스템과 행정정보 중계시스템을 통한 행정정보 공동이용 건수가 2003년의 1,737만 건에서 2007년의 5,103만 건으로 크게 증가하였다.

<표 2-6> 연도별 행정정보 공동이용 실적

(단위: 만 건)

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

자료: 행정정보공유추진위원회(2007).

이와 관련하여 행정안전부에 행정정보공동이용시스템의 이용기관별·조회목적별 이용현황(최근 3년간)을 정보공개 청구한 결과, 행정정보공유추진단에서 행정정보공동이용시스템 조회(열람)현황은 2006년도에 23,684천 건, 2007년도 27,659천 건, 2008년도에 27,187천 건이라고 답변하였으며, 그 상세현황은 「공공기관의 정보공개에 관한 법률」 제9조제1항제5호에 의거하여 제공되지 않았다. 이는 행정정보 중계시스템의 행정정보 공동이용 실적

---

에 현저한 지장을 초래한다고 인정할 만한 상당한 이유가 있는 정보

24) '행정정보공동이용시스템 관련 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.14).

25) 60개 중앙행정기관, 248개 지방자치단체, 20개 공공기관이 연계되어 있다(감사원, 2008: 3).

을 포함하지 않은 것이며, 2007년의 행정정보 공동이용 현황은 『2007 행정정보공동이용 백서』의 것과도 어긋나고 있다.

2008년 9월 2일부터 8일에 걸쳐 전국의 성인남녀 1,000명을 대상으로 하여 이루어진 일반인 조사에 따르면, 시민들은 개인정보DB의 구축과 구축한 기관이 이를 이용하는 것보다 다른 기관과 공유하는 것이 더 위험하고 불쾌하다는 입장을 나타내, 구축한 DB를 공유하는 것에 민감한 반응을 보였다. 정당한 업무수행을 위하여 개인정보DB의 공유가 필요하고 경우에 따라서는 필수적일 수도 있는데, 이에 대해 국민들이 부정적인 반응을 보이는 것은 아직까지 정부가 국민의 개인정보를 정당하고 필요한 목적 범위 내에서만 수집·이용·공유한다는 점에 대해 충분한 신뢰를 주지 못했기 때문일 것이다(성낙인 외, 2008: 225).

한편, 행정정보공유추진단은 행정정보 공동이용기관의 불편사항, 이용이 저조한 원인 등을 파악한 후 이를 시스템 및 제도 개선에 반영하여 행정정보 공동이용의 활성화를 도모하고 공동이용 과정에서의 개인정보 오·남용을 방지할 목적으로 매년 정기(분기별 1회) 또는 수시로 공동이용실적이 높거나 낮은 기관, 공동이용 과정에서 특이사항이 발견된 기관 등 15개 기관 정도를 선정하여 행정정보 공동이용 실태점검에 나서고 있다. 2006년에는 이용기관 불편사항 파악 및 공동이용 안내를 위해 비교적 자주 현지 방문에 나서 14회 125개 기관을 점검하였으며, 2007년부터는 점검내실화에 따라 대상 기관수 및 점검횟수를 줄여 2007년 5회 54개 기관, 2008년 3회 40개 기관 등 총 219개 기관을 대상으로 점검하였고, 2009년 6월 현재 378개 이용기관이 자체점검 중에 있다(행정정보공유추진단, 2009).

<표 2-7> 지난 3년간 행정정보 공동이용 점검대상 기관수

| 연도 | 점검 회수 | 점검대상 기관수 | | | | |
|---|---|---|---|---|---|---|
| | | 계 | 중앙부처 | 자치단체 | 공공기관 | 금융기관 |
| 계 | 22 | 219 | 53 | 108 | 44 | 14 |
| 2006년 | 14 | 125 | 35 | 79 | 11 | |
| 2007년 | 5 | 54 | 7 | 18 | 28 | 1 |
| 2008년 | 3 | 40 | 11 | 11 | 5 | 13 |

자료: 행정정보공유추진단(2009).

행정정보 공동이용 실태점검의 주요 점검내용에는 우선 행정정보공동이용

활성화를 위한 노력으로, 행정정보공동이용과 관련 자체 교육 실시 여부,[26] 행정정보공동이용 관련 홍보 여부, 행정정보공동이용 이용사무와 정보별 열람 현황 주기적 비교분석 및 실적저조에 대한 이용 독려 여부, 불필요한 구비서류 징구 여부 등이 있고, 행정정보공동이용 오남용 예방 등과 관련하여 ① 개인정보보호 및 정보 오남용에 대한 자체점검 등 오남용 예방 노력 여부, ② 일정기간 오남용 사용 여부(열람대상자 정보에 담당자 등 기타 정보를 입력하고 열람, 업무처리담당자가 본인 담당업무명과 다른 사무명칭의 열람권한을 승인받아 정보를 열람하는 경우가 있는지 여부 등), ③ 권한신청 사무 외의 사무를 열람하는지 여부, ④ 일용직·공익근무요원 등 권한 미승인자의 대리 업무 여부 등, ⑤ 개정 민원서식 사용, 사전동의서 존재 및 사전동의 이행 여부 등이 포함된다.

하지만 앞으로 보다 발전적인 점검을 통하여 국민에겐 양질의 민원서비스를, 이용기관에는 업무 효율성 제고라는 본래의 목적을 살리는 데 일조하기 위하여 노력해야 한다고 밝히고 있을 뿐, 행정정보 공동이용에 따른 개인정보의 오·남용에 대해서는 점차 주의를 기울이지 않고 있는 추세에 있다.

구체적으로 보면, 2006년 행정정보공동이용기관에 대한 점검의 경우 전체적으로 상반기에는 행정정보공동이용에 대한 업무 숙지도, 개인정보 보호 의식이 높지 않았으나, 이에 대한 집중적인 홍보와 점검을 실시한 결과 하반기에 들어서는 기관총괄책임자를 비롯한 이용기관 실무 담당자들의 인식이 호전되었으며, 전체적인 열람 실적 또한 10% 가량 증가하는 등 이용기관의 행정정보공동이용은 대체로 원활하게 추진되었다고 한다.

중앙행정기관은 업무가 상당부분 지방자치단체에 위임되어 있어 직접적인 민원 업무는 많지 않은 편이며, 행정정보공동이용에 대한 관심도 상대적으로 낮은 편이지만, 개인정보 보호에 대한 인식이 높고, 개인정보 보호를 위한 노력 등은 대체로 잘 이루어지고 있다고 평가되었다. 하지만 권한관리 부적절 및 오남용 사항으로서, 해당 업무와 관련이 없는 정보에 대해서도 권한을 부여한 사례, 인사 이동시 즉시에 권한 변경되지 않거나 퇴직자에 대하여 열람권한을 해지하지 않은 경우가 있었다.

지방자치단체의 이용 실적은 전체 이용 실적의 70%를 상회하고 있으나 기존 시·군·구의 경우 민원행정시스템의 혼용으로 행정정보공동이용의 실적 향상에 많은 어려움이 있었기에 행정정보를 적극 공유할 수 있도록 대한 지

26) 행정정보공동이용 절차와 방법, 개인정보보호 및 오남용 예방(집합, 소규모 단위, 기타 방법).

도 점검을 강화해 나가고 있다고 밝히고 있다. 하지만 공유 개인정보 오남용 등의 사항에 대해서는 역시 구체적으로 제시하고 있지 않다.

공공기관은 2006년 9월부터 국민건강보험공단 등 5개 기관에 대하여 시범적으로 점검을 실시하였다. 시범 기관에 대하여 공공기관 본부와 산하 소속기관 담당자를 대상으로 행정정보공동이용 전반에 대한 교육을 실시하였으나 이용 실적이 그다지 높지 않았다고 한다(행정정보공유추진위원회, 2007: 162-164).

2006년 행정정보공동이용 1일 목표량이 15만 건인데 비해 2007년에는 30만 건으로 대폭 상향 설정됨에 따라, 2007년 이용기관 점검은 기존 2006년도 점검 항목에 더하여, 특히 이용실적 향상에 초점을 맞추고 이용 실적이 저조한 기관을 대상으로 집중적으로 실시하였다(행정정보공유추진위원회, 2007: 165-66).

중앙행정기관의 경우 2007년 상반기 현재 6개 기관을 대상으로 실시하였으며, 행정정보공동이용의 편리성으로 인해 비교적 적극 활용하고 있는 편으로 나타났고, 지방자치단체도 행정정보공동이용에 대한 지방자치단체의 운영이 체계를 잡아가고 있고 이용 실적도 전반적으로 향상되었다고 평가하고 있다. 공공기관은 2007년 4월부터는 43개 공공기관으로 확대하였으나, 행정정보공동이용에 대한 인지도가 높지 않고 행정정보공동이용이 정착되지 않은 기관이 적지 않았다(행정정보공유추진위원회, 2007: 166-167). 2007년 상반기 행정정보공동이용기관에 대한 점검에서는 개인정보 오남용 등의 사항이 전혀 언급되고 있지 않다.

감사원은 이러한 문제 이외에도 행정정보 공동이용 추진분야의 문제점을 지적하고 있다(감사원, 2008: 8-42). 첫째, 공동이용 대상 선정을 위한 기관별 행정정보 보유현황조사가 부실하고 원활한 정보공유에 필요한 표준코드의 활용 및 관리가 미흡한 등 정보 공유기반이 취약하였다는 점, 둘째, 정보공유 관련 이견이 장기간 해결되지 않고 있는데도 이견조정절차 등 실효성 있는 조정방안이 마련되지 않고 있었다는 점, 셋째, 공동이용이 가능한 정보를 기관 간 업무협조 미흡으로 공유하지 않아 예산낭비 등 비효율을 초래하고 있었다는 점이 그것이다.

(2) 개인정보 오·남용 및 담당공무원에 의한 다량의 정보유출 가능성

행정정보공유추진위원회는 행정정보공동이용의 실태와 관련하여 행정정보공동이용 관련 개인정보보호 등 보안대책을 철저하게 강화하였다고 평가하고

있다(행정정보공유추진위원회, 2007: 198). 개인의 정보보호를 위하여 각종 정보열람 시 본인의 사전 동의를 의무화하였고, 공동이용 내역에 대한 본인의 열람청구권을 보장하도록 하였으며, 행정정보 오·남용 시 처벌조항을 엄정하게 적용하였다. 또한 행정정보공유추진위원회를 통한 공동이용 승인·중단 등 심의절차를 강화하기로 하였다. 그리고 행정정보 공동이용시 행정기관에서 발급한 행정전자서명(인증서)만 사용하고 정보유통 전 과정의 암호화 및 전자인증체계를 도입하고 로그정보 관리·분석, 공동이용 대상정보 접근을 통제하고 데이터 레벨링을 통해 필요한 정보만 제공하도록 하였다.

행정정보공유추진위원회는 행정정보공동이용의 보완·개선사항 및 향후 과제에 있어서 행정정보공동이용 대상정보 및 대상기관 확대, 업무효율성 증대를 위한 서비스 기능 개선, 안정적인 서비스 인프라 제공, 별도의 정책정보 제공을 위한 맞춤형 정보 제공 등과 함께 개인정보보호 및 서비스 관리의 강화를 제시하고 있다. 정보제공의 범위가 확대되고 서비스를 편리하게 이용할 수 있게 된데 반해, 동시에 불필요한 정보의 남용이나 개인정보의 유출 등에 대한 우려가 제기되고 있으며, 제공정보의 신청, 승인, 활용 등 전 단계에 걸쳐 권한과 이용현황 등을 철저하게 분석, 관리할 수 있는 서비스관리체계에 대한 필요성이 증대되고 있다는 것이다(행정정보공유추진위원회, 2007: 206).

그리고 향후에는 공동이용의 대상이 되는 행정정보들 중 개인정보들은 모두 사전에 정보주체들의 동의가 있어야 열람 가능하며, 사후에도 사용자와 업무 목적 등이 구체적으로 파악될 수 있도록 관리되어 공동이용된 정보들의 해당 당사자들이 그 활용 내역을 알 수 있도록 이를 통지해주어야 한다고 밝히면서, 사고를 미연에 최대한 예방하도록 하고, 사후에는 사고 원인을 신속하게 파악하고 적절히 대응할 수 있도록 관리체계의 고도화를 제안한다.

하지만 이러한 제안은 행정정보공동이용에 따른 개인정보 오남용을 방지하기 위한 대책으로는 미흡하다. 우선 여기에서는 공동이용의 대상이 되는 행정정보들 중 개인정보들은 모두 사전에 정보주체들의 동의가 있어야 열람 가능하도록 하였고, e하나로민원에서도 민원처리시마다 반드시 본인의 사전동의가 있는 경우에만 정보를 열람할 수 있도록 되어 있다. 그러나 이러한 조치는 '일반행정정보의 공동이용'과 '개인정보의 공동이용'이 구분되고 있음을 전제한 것인데, 지금도 여전히 행정정보 공동이용시스템에서는 이러한 구분은 행해지고 있지 않으며, 행정정보공동이용이라는 이름 아래 함께 다루어지고 있다는 점에서 전제 자체가 충족되고 있지 않다고 봐야 한다. 나아가 이는 개인정보 열람이 합법적으로만 진행된다고 가정하고 있으며, 본인의 사전

동의를 거치지 않은 무단 열람이 존재할 가능성을 배제하고 있다는 점에서 한계가 있다. 이에 대해서 감사원은 '행정정보 공유 및 관리실태'에 대한 감사[27]에서 행정정보 공동이용시스템을 이용하여 담당공무원이 개인정보를 사적으로 무단 열람하고, 외부로 유출하는 문제를 완전히 차단하긴 어렵다고 보고 있다(감사원, 2008: 46-48). 담당공무원에 의한 정보유출은 행정정보공동이용시스템이 구축되면서 출현한 문제는 아니지만, 자신이 근무하는 기관의 개인정보DB만 볼 수 있었던 기존시스템과는 달리 행정정보 공동이용시스템을 이용하게 되면 다른 기관이 보유하고 있는 개인정보에까지 접근이 가능하게 되므로, 정보유출의 파괴력이 훨씬 커지게 되었다고 할 수 있다.

행정정보공유추진단이 대국민 민원서비스 혁신을 위해 구축한 행정정보 공동이용시스템은 「공공기관의 개인정보보호에 관한 법률」 제3조의2와 제9조에서 정한 바와 같이 공동 이용하는 정보가 안전하게 관리·유통될 수 있도록 내부통제, 이용자 접근통제, 정보이용 실태에 대한 상시 모니터링 등 신뢰할 수 있는 개인정보 보호 및 오·남용 방지체계를 갖춰야 한다. 이에 행정정보 공동이용시스템에는 행정정보 오·남용을 방지하기 위하여 아래와 같이 정보이용 유형을 실시간으로 분석하는 기능을 '범정부 행정정보공유체계 구축사업'에 포함하여 개발하였다.

<표 2-8> 행정정보 오·남용 적출 유형

| 구 분 | 유형 그룹 | 유형 |
|---|---|---|
| 사용 인증 | 이용시간 외 접속 | 업무요일이 아닌 시점에 접속 |
| | | 업무시간이 아닌 시점에 접속 |
| | 동일 인증서/단말기 다중접속 | 비인가 IP 주소, MAC 주소, HDD 정보를 이용한 단말기 접속 |
| | | 본인 인증서로 비인가 단말기 반복 접속 |
| | | 하나의 단말기에 여러 이용자 접속 |
| | 비인가 인증서 접속 | 유효하지 않은(유효기한 만료, 폐지) GPKI 인증서 접속 |
| 정보 이용 | 과도한 이용정보 열람 | 이용횟수 과다 열람 |
| | | 동일 정보 반복 열람 |
| | 비정상적 열람 | 신청자와 열람자 동일 입력 |
| | | 열람자와 열람대상자 동일 입력 |

자료: 구 행정자치부(행정정보공유추진단); 감사원(2008: 47) 재인용.

27) 감사원은 각 기관에서 개인정보가 포함된 행정정보를 다른 기관에 제공하면서 정보유출 방지를 위한 조치를 제대로 하고 있는지, 그리고 개인정보의 실시간 열람기능을 제공하는 행정정보공동이용시스템의 정보보안기능이 적정한지 등을 중점적으로 감사하였다.

그러나 감사원은 정작 행정정보의 오·남용 등을 파악하기 위해서 필요한 정보열람기록은 정보열람자가 정보를 열람하는 목적(업무명)과 열람정보명 등을 시스템에서 자동으로 기록되게 하지 않고 정보열람자로 하여금 입력하도록 개발하여 부주의로 잘못 입력하거나 의도적으로 조작할 수 있을 뿐만 아니라 정보이용에 대한 모니터링기능이 없어 정보 오·남용 방지체계를 신뢰할 수 없게 되어 있다고 지적하였다(감사원, 2008: 46-47). 정보열람자가 열람내역을 수동으로 입력하게 하여 열람내역 조작이 가능해지는 등 행정정보공동이용시스템의 정보 오·남용 방지 기능이 부실하게 개발되어 정보보호 안전성 확보가 곤란하였다는 것이다.

실제 행정정보 공동이용 관련 정보 오·남용 실태를 확인하기 위해 2007년 4월부터 같은 해 9월 사이에 서울특별시 ○○구청 등 20개 시·군·구에서 민원사무처리를 위해 위 공동이용시스템을 이용하여 행정정보를 열람한 명세와 시·군·구 행정정보시스템에 기록된 민원사무처리 명세를 비교한 결과 민원사무를 위해 공동이용(열람)한 행정정보 41,332건 중 25,916건(63%)은 민원사무처리부에 기록되지 않아 실제 민원사무를 위해 정보를 열람한 것인지 확인할 수 없게 되어 있었다. 하지만 행정안전부 행정정보공유추진단은 정보열람기록이 정확히 기록되도록 행정정보 공동이용시스템의 정보 오·남용 방지체계를 개선하는 방안을 마련하지 않았고, 2006년, 2007년 행정정보 공동이용기관 실태점검에서도 정보이용자의 민원 또는 행정업무처리 명세와 정보이용 명세를 비교하는 등 개인정보의 오·남용 여부에 대한 점검은 하지 않았다. 결국 행정정보 공동이용시스템은 행정정보 오·남용을 완전하게 방지할 수 없어 주민등록정보 등 개인정보의 유출 소지가 있다는 것이다(감사원, 2008: 48).

행정안전부가 제278회 국회(정기회) 행정안전위원회 국정감사 서면답변에서 밝힌 내용에서도 행정정보 공동이용시스템은 구비서류 정보 단위로 정보열람내역을 관리하고 있고 기록시점도 실제 처리되는 시점에 이루어지는 데에 비하여, 시군구 행정정보시스템에서 관리하는 민원사무처리부는 민원 신청시점에 기록되도록 하고 있어 행정정보공동이용 열람내역과 시군구 민원사무처리부의 기록내역이 일치하고 있지 않음을 적시하고 있다. 다만, 행정정보 공동이용 열람내역과 시군구 「민원사무처리부」 간의 기록내역 불일치로 인한 정보 오·남용에 대한 우려를 해소시키기 위하여 향후에는 행정정보공동이용시스템과 시군구 행정정보시스템을 연계하여 상호간의 기록내역이 비교되도록 관계기관과 협의하여 추진하며, 정보주체의 열람청구권 보장 등 행정

정보 열람내역에 대한 모니터링이 보다 강화될 수 있도록 제도 개선도 병행해 나가기로 하였다(행정안전부, 2008c: 13).

감사원은 행정정보 공동이용시스템과 관련하여 다음과 같은 문제점도 지적하고 있다(감사원, 2008: 43-49).

우선 구 해양수산부 등 22개 기관에서 비밀번호 설정 등 최소한의 안전성 확보조치도 없이 다량의 개인정보를 CD 등 매체에 수록, 인편 또는 우편으로 다른 기관에 제공하여 개인정보 유출위험이 상존하였다고 지적하였다. 「공공기관의 개인정보보호에 관한 법률」 제9조의 규정에 따르면 행정기관이 개인정보를 다른 기관에 제공할 때에는 분실·도난·유출·변조 또는 훼손이 되지 않도록 안전성 확보에 필요한 조치를 하도록 되어 있고, 「전자정부법 시행령」 제23조의 규정에 따르면 행정정보의 제공요청을 받은 행정기관의 장은 정당한 사유가 없는 한 행정정보공동이용센터를 통하여 해당 행정정보를 제공하도록 하고 있으며, 이는 아래와 같이 정보 공동이용에 필요한 보안장치를 구비하고 있는 행정정보 중계시스템을 이용하도록 되어 있다.

<표 2-9> 행정정보 중계시스템의 주요 보안조치

| 구 분 | 주요 보안조치 |
|---|---|
| 로그인 및 사용권한 관리 | □□전자서명을 통한 사용자 인증으로 중계서버 접속<br>□□사용자의 인증서가 중계시스템과 정부디렉토리서버에 등록되어 있는지 여부 확인 |
| 자료전송 | □□자료를 압축/암호화 전송<br>□□해당 인증서를 가진 사용자만 복호화 가능 |
| 사후관리 | □□모니터링 및 로그관리를 통해 사후관리 수행 |

자료: 구 행정자치부 자료 재구성; 감사원(2008: 45) 수정.

그런데 감사원이 각 행정기관의 개인정보 공동이용 실태를 점검한 결과, 국세청 등 38개 기관에서는 행정정보 중계시스템과 이미 연계되어 있어 이를 이용하여 자료를 제공할 수 있는데도 주민등록자료 등 다량의 개인정보를 CD 등 기록매체에 수록하여 인편 또는 우편으로 다른 기관에 제공하고 있었으며, 이들 기관 중 구 해양수산부 등 22개 기관에서는 CD 등 매체에 비밀번호 설정 등 자료유출 방지를 위한 안전성 확보조치도 하지 않았다. 그런데도 구 행정자치부에서는 이러한 실태조차 파악하지 아니하여 이들 기관에 대해 행정정보 중계시스템을 통해 자료를 공동이용하도록 권고하는 등의 조치

를 취하지 않았다. 그 결과 인편 등으로 자료를 전달하는 데 따른 행정력의 낭비와, 자료 전달과정에서 고의적 유출 또는 분실로 인한 다량의 개인정보 유출 가능성이 상존하고 있다는 것이다(감사원, 2008: 44).

그리고 행정정보 공동이용시스템 자체의 보안 문제도 있다. 행정정보공유추진위원회는 금융기관에 제출하는 민원서류가 전체 발급건수의 37%를 차지하는 것을 감안하여 금융기관에 대한 개인정보보호를 강화하여, 은행이 필요로 하는 11종 내에서 업무별로 필요한 정보만 제공하고, 열람은 상위관리자로부터 승인을 받은 후 가능하도록 하였고, 사용자 권한관리가 철저한 행정전자서명을 통해서만 시스템에 접근할 수 있도록 하였으며, 사용자, 처리기간, 열람목적, 열람일시 등을 로그기록으로 남겨 사후 증적관리를 철저히 하도록 하였다고 밝힌 바 있다(행정정보공유추진위원회, 2007: 198). 하지만 2005년 전자민원창구인 G4C를 통해 발급되는 문서가 간단한 방법으로 위·변조될 수 있음이 밝혀진 것처럼, 행정정보공동이용시스템의 경우도 보안상의 문제가 발생할 수 있다. 행정정보공동이용센터를 통해 유통되는 정보가 모두 암호화되어 유통되고, 이용기관이 직접 제공기관의 DB에 접속하여 정보를 열람하는 것은 아니기 때문이다. 행정정보공동이용센터 안에 증적관리시스템이 구축되어 있고, 그 증적관리시스템에 이용기관이 확인한 정보가 축적되는데, 그 정보를 암호화된 상태로 보관하고, 증적관리를 철저하게 하고 있지만, 그 시스템 자체가 해킹되어 암호가 풀렸을 경우에는 엄청난 피해를 야기할 수 있다. 증적관리시스템에 해당 정보들을 저장하는 것 자체가 문제되는 것이다. 게다가 이는 정보처리 원칙 중 정보분리의 원칙[28]에서 벗어난 것이다(성낙인 외, 2008: 237-239).

행정정보공유추진위원회는 『2007 행정정보공동이용 백서』에서 향후 과제로서 두 가지를 제시하였다. 우선, 정보보안시스템의 고도화 측면에서 현재의 보안관제를 보다 개선 및 고도화하여 통합모니터링시스템과 연계된 종합적인 예·경보체계를 구축하며, 기관별로 오남용패턴을 상세화하여 적용하고, 웹방화벽을 도입하여 웹환경에서 외부로부터의 침입방지를 강화하며, 철저하고 통합적인 로그관리 및 감사추적을 할 수 있도록 한다. 그리고 개인정보보

28) 정보분리의 원칙은 특정 목적을 위해 수집된 개인정보가 다른 기관에서 다른 목적을 위해 수집된 개인정보와 원칙적으로 통합되지 않고 분리된 상태로 유지되어야 한다는 요청이다. 이에 따르면, 데이터베이스의 물리적인 통합뿐만 아니라 컴퓨터결합이나 컴퓨터프로파일링(computer profiling)의 기법에 의한 정보통합은 필요불가결한 경우가 아닌 한 원칙적으로 허용되어서는 안 된다는 것이다. 통합된 개인정보를 보유하게 되면 당해 정보주체에게 무한한 권력 행사가 가능해지기 때문이다.

호측면에서는 인감증명정보 등 사용자 동의가 필요한 정보에 대해 정보주체자의 동의를 받을 수 있도록 하며, 정보주체자(민원인)에게 정보 열람결과를 통지할 수 있도록 할 것이며, 또한 개인정보 침해사실에 대한 의견 창구와 시정조치 체계를 확립한다(행정정보공유추진위원회, 2007: 209). 그러나 위에서 지적된 문제점들이 여전히 제대로 보완되지 않은 상태에서 이상의 과제를 제시하는 것은 한계가 있을 수밖에 없고, 사실상 행정정보 공동이용의 확대에만 치중하는 것은 문제가 있다고 본다.

(3) 행정정보공동이용에 따른 개인정보보호 문제의 경시

정부는 2001. 3. 28. 구 「전자정부 구현을 위한 행정업무 등의 전자화촉진에 관한 법률」(2007. 1. 3. 「전자정부법」으로 법명 변경하기 전의 것)을 제정하여 행정기관이 수집하여 보유한 행정정보의 공동이용을 의무화하는 등 행정정보 공동이용을 위한 제도적 기반을 마련하였다. 그러나 정부는 행정정보의 공동이용이 행정기관 간에만 한정되었고, 구 행정자치부의 전자정부본부에서 맡아 수행하는 행정정보 공동이용센터의 기능도 주로 행정정보의 공동이용을 위한 기술적 업무를 수행하도록 하고 있어서 한계가 있다고 보았다.[29)]

29) 즉 「전자정부법」 제21조와 제22조, 그리고 「국가정보화 기본법」(구 「정보화촉진기본법」) 제5조의 규정에 따라 공공부문의 정보화와 관련한 정책 등을 심의하는 국가정보화전략위원회(구 정보화추진위원회, 공동위원장: 국무총리와 대통령 위촉인사 1인)에서 행정정보의 공동이용과 관련한 주요 사항을 심의하도록 되어 있고, 「전자정부법」 제22조와 같은 법 시행령 제31조의 규정에 따라 행정안전부가 행정정보 공동이용과 관련한 위 위원회의 심의를 지원하는 등 행정정보의 공동이용을 실무적으로 총괄하도록 되어 있다. 또한, 같은 법 시행령 제26조의 규정에 따라 행안부에서 업무를 효율적으로 추진하도록 지원하기 위하여 아래의 기능을 수행하는 '행정정보공동이용센터'를 설치하고 행정안전부의 전자정부본부에서 그 기능을 수행하도록 하였다.

<표 2-10> 행정정보공동이용센터의 기능

| 실무부서 | 주요 기능 |
|---|---|
| 행정안전부<br>전자정부본부 | · 행정기관 간 행정정보의 공동이용을 위한 정보통신망 및 중계시스템의 설치·운영<br>· 행정기관의 행정정보 목록 및 개인정보파일에 관한 공고내용의 DB화와 이에 대한 안내서비스 제공<br>· 행정기관 간 행정정보의 공동이용을 위한 정보통신망의 지정·연계 및 정보통신망 및 중계시스템의 보호를 위한 조치<br>· 정보파일 보호대책의 수립·운영<br>· 공동이용 행정정보의 전자서명 및, 공동이용의 신청절차 등에 관한 지침의 제정·시행<br>· 공동이용한 행정정보 및 행정정보 공동이용 기록의 유지·관리<br>· 행정정보 공동이용 및 개인정보보호 실태에 대한 현황 파악 |

이에 정부는 2005. 7. 20. 제63회 국정과제회의에서 행정정보 공동이용 확대를 정부정책으로 채택하여 추진체계를 강화하고 '범정부적 행정정보 공유체계'를 구축하기로 하였다. 그리고 2005. 10. 18. '행정정보공유추진위원회 규정'을 제정·공포하여 행정정보 공동이용 확대를 위한 정책 수립과 제도 개선, 공유시스템 개발 등 실질적으로 행정정보 공동이용의 총괄기구로서 역할을 수행하는 행정정보공유추진위원회와 이를 실무적으로 지원하는 행정정보공유추진단을 설치하여(권해수, 2006: 11; 감사원 2008: 2-3), 사실상 행정정보 공동이용센터의 기능을 하도록 하고 있다.

이처럼 행정정보 공동이용에서 사실상 행정정보 공동이용센터의 기능을 하고 있는 기구는 행정정보 공동이용 확대를 위한 정책 수립과 제도 개선, 공유시스템 개발 등 실질적으로 행정정보 공동이용의 총괄기구로서 역할을 수행하는 행정정보공유추진위원회와 이를 실무적으로 지원하는 행정정보공유추진단이다.

행정정보공유추진위원회는 ① 행정정보의 공유를 확대하기 위한 정책의 수립·추진 및 법령·제도의 개선, ② 행정정보의 공유를 확대하기 위한 업무흐름의 재설계, 정보화추진 전략의 수립 및 시스템의 개발, ③ 행정정보의 공유 현황에 대한 확인·점검, ④ 행정정보의 공유 및 공유 확대를 위하여 필요한 사항 등을 심의하는데, 위원장 2인을 포함한 20인 이내의 위원으로 구성한다. 위원회는 행정정보의 공유와 관련된 추진사항을 정기적으로 대통령에게 보고하도록 하고 있다. 그리고 행정정보공유추진단은 행정정보공유추진위원회의 심의안건 작성 등 회의 준비, 위원회의 기능과 관련된 조사·연구 및 점검, 그 밖에 위원회의 업무 지원에 관한 사항을 처리하기 위해 설치되었으며, 관계행정기관에서 파견된 공무원과 공공기관에서 파견된 임·직원 등으로 구성(단장: 행정안전부 정보화전략실장)된다(행정정보공유추진위원회 규정[대통령훈령 제235호, 2008.12.11, 일부개정]). 행정정보 공동이용과 관련하여 일반 정보공개 청구를 하였을 때에도 이에 대한 답변은 행정정보공유추진단에서 하였다.

행정정보공유추진위원회(2007: 56-57)에 따르면, 행정정보공동이용센터의 역할은 ① 범정부적인 정보공동이용서비스 제공 및 이를 위한 시스템 구축, ② 체계적인 서비스 제공을 위한 행정정보공동이용체계의 운영 및 유지·관리, ③ 공유DB 연계 및 색인DB 구축, ④ 제공기관과 이용기관의 연계, ⑤ 행정정보 제공 및 이용에 관한 구체적인 절차 제도화 및 행정정보 이용에 관한 지침 수립 등 5가지이다. 이러한 행정정보공동이용체계의 기본방향과 행

정정보공동이용센터의 역할과 기능에 의하면, 각 행정기관이 보유하고 있는 개인정보DB와 기업정보DB의 통합 연계가 기본전제로 되고 있다. 그러나 이처럼 개인정보 공동이용을 전자정부의 기본전제로 하는 것은 정부기능의 효율성만을 강조한 것으로서 행정의 민주성과 투명성을 도외시한 것이라고 할 수 있다(성낙인 외, 2008: 842).

행정정보공유추진위원회와 행정정보공유추진단은 행정정보의 공유를 확대하는데 주된 업무의 초점이 맞춰져 있으며, 행정정보 공동이용에 따르는 개인정보보호의 문제에는 별로 신경을 쓰고 있지 않고, 그 와중에 개인정보 공동이용이 무분별하게 이루어지고 있는 실태에 대해서도 별다른 관심이 없는 것으로 보인다. 이는 최근까지 23차에 걸쳐 있었던 행정정보공유추진위원회(소위원회)의 회의 안건에서도 잘 나타난다. 여기에는 행정정보 공동이용에 따른 개인정보의 수집·유통과 관련된 문제를 거의 다루고 있지 않다. 행정정보공유추진위원회(소위원회)의 회의록을 검토한 결과 논의사항 중에 개인정보 보호가 다루어지는 경우는 정리하여 별도로 첨부하였다.

<표 2-11> 행정정보공유추진위원회(소위원회) 회의 안건

| 회차 | 일 자 | 회의 안건 |
|---|---|---|
| 1 | '05.11.18(금) | - 「행정정보공유추진위원회」 현황 및 향후 활동계획<br>- 행정정보공유추진위원회 운영세칙(안) (심의안건)<br>- 행정정보 공유 종합추진계획 (보고안건)<br>- 민원구비서류 감축계획 (보고안건) |
| 2 | '06.1.12(목) | - 1차 자문회의 결과 주요내용에 대한 조치사항 보고<br>- 행정정보공유추진 로드맵(안) 검토<br>- 행정정보공유추진 관련 연구개발 과제 검토 |
| 3 | '06.1.26(목) | - T/F운영 및 벤치마킹 계획 보고<br>- 자문단 회의 결과 보고('06.1.12, '06.1.19)<br>- 행정정보공유 로드맵(안) 보고 및 토의 |
| 4 | '06.3.9(목) | - 문서감축법령개정안 및 추진일정 보고<br>- 행정정보공유시나리오 설명 및 시스템 시연<br>- 행정정보공동이용법(안) 입법계획 보고 |
| 5 | '06.3.23(목) | - 행정정보공유 국내외 벤치마킹 사례 보고<br>- 국민인식조사 추진상황 보고<br>- 행정정보공유추진 관련 정책연구과제 보고 |
| 6 | '06.5.18(목) | - ISP 추진경과 보고<br>- 행정정보 공유 확대를 위한 ISP 종합 보고(사업단) |

| | | |
|---|---|---|
| | | - 공공·금융기관 연계 적용방안(사업단) |
| 7 | '06.6.1(목) | - 행정정보공동이용 관련 법령 추진상황 보고<br>- ISP 주요 이슈사항 보고<br>- 행정정보공동이용 국무총리 보고계획 |
| 8 | '06.6.29(목) | - 행정정보공유 추진상황 보고<br>- 5개 공공기관 시범운영계획 보고<br>- 이용기관 행정정보공동이용 절차 및 규정<br>- 정책정보 TF 구성 및 운영상황 보고<br>- 개인정보보호를 위한 주민등록번호대체 관련 보고 |
| 9 | '06.8.4(금) | - 행정정보공유추진 상황 보고 - 기획총괄팀<br>- 행정정보공동이용법 제정 추진상황 보고 - 제도팀<br>- 5개 공공기관 정보이용승인 추진상황 보고 - 구축팀 |
| 10 | '06.8.24(화) | - 행정정보 공유확대 시험운영 추진현황 보고<br>- 공공기관 시범서비스 대상 심의<br>- 행정정보 공유확대 홍보계획 보고<br>- 범정부 정책정보공유 방안 보고 |
| 11 | '06.12.13(수) | - 행정정보공유 추진단 주요업무 추진현황 보고<br>- 범정부 행정정보공유체계 구축사업 추진계획 보고<br>- 행정정보공유 열람실태 점검 및 정책연구과제 추진현황보고<br>- 행정정보 공동이용 및 문서감축 관련 법령 제·개정 추진현황 보고 |
| 12 | '07.2.15(목) | - 행정정보공유 추진현황 및 계획 보고(구축팀)<br>- 행정정보공유 대국민 홍보계획 보고(기획총괄팀)<br>- 행정정보공유 정책 연구과제 관리 보고(조정평가팀) |
| 13 | '07.3.15(목) | - 행정정보공동이용 확대를 위한 공공·금융기관 이용협약 승인(공유체계구축팀)<br>- 행정정보공유 브랜드·슬로건 및 홍보포스터(안) 검토·선정(기획총괄팀)<br>- 행정정보공동이용 지침(안)검토(문서감축팀) |
| 14 | '07.3.21(목) | - 미 제공 행정정보 보유기관과 협의 추진현황 보고(공유체계구축팀)<br>- 행정정보 보유기관의 미 제공 사유 설명 및 토론 |
| 15 | '07.4.12(목) | - 공공·금융기관 서비스 추진현황 보고(구축팀)<br>- 공공기관 확대관련 일반·민원사무 재분류 결과보고<br>- 행정정보공유서비스 브랜드 명 재검토(총괄팀) |
| 16 | '07.7.12(목) | - 『행정정보 공동이용 확대구축 사업계획』 보고<br>- 정책연구용역 과제 추진계획 보고<br>- 『e하나로 민원』 서비스 홍보계획 보고 |

| | | |
|---|---|---|
| | | - 법령 제・개정 추진현황 보고 |
| 17 | '07.10.25(목) | - '07 하반기 주요업무 추진현황<br>- 이용사무 근거법률 조사현황<br>- 행정정보공동이용 확대 구축사업 추진현황 |
| 18 | '08.1.22(화) | -『행정정보공동이용 확대구축사업』 착수보고<br>- 행정정보공동이용(e하나로민원)시스템 이용사무별 적정성 검토・분석 보고<br>- 행정정보공동이용(e하나로민원)시스템 실태점검 계획보고 |
| 19 | '08.4.11(목) | - 행정정보공동이용 확대대상기관(공공・금융기관) 선정계획(안)<br>- 행정정보공동이용시스템 통합전산센터 이전관련 과업변경(안) |
| 20 | '08.5.15(목) | - 시범은행 대상 행정정보공동이용 실태점검 결과보고<br>- 행정정보공동이용 확대 대상기관(공공・금융기관) 선정(안) |
| 21 | '08.7.8(목) | - 행정정보공동이용 확대 대상기관(공공・금융기관) 선정(안)<br>- 행정정보공동이용 시 열람정보 종이출력 허용기준(안) |
| 22 | '09.4.30(목) | - 행정정보공동이용시스템 소개용 동영상 시청<br>- 행정정보공유추진위원회 일반현황 보고<br>- 행정정보공동이용 추진현황 및 향후계획 보고, 공동이용시스템 시연 |
| 23 | '09.6.30(화) | - 행정정보공동이용 중기 전략계획(안)<br>- 수요자 맞춤형 행정정보공동이용체계 기반구축 사업계획(안) |

자료: 행정정보공유추진위원회(2007); '행정정보공동이용시스템 관련 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.14) 중 행정정보공유추진위원회 소위원회 회의록 일체 수정・보완.

특히 행정정보공유추진위원회 제14차 소위원회(2007. 3. 21) 회의록을 보면, 미 제공 행정정보 보유기관과의 협의 추진과 관련하여 정보제공기관에 1,505건을 요청했는데 608건(40%)을 승인받았고, 국세청, 법무부 등에서 승인을 거부하고 있어 승인률이 매우 저조한 실정이라고 밝히면서, 행정정보 보유기관의 미 제공 사유 설명 및 토론 내용을 제시하고 있다. 이에 따르면 행정정보공유추진위원회는 시종일관 행정정보 보유기관이 공공・금융기관의 개인정보 오・남용에 대한 불안감으로 개인정보 공동이용을 꺼리는 것에 대해 이를 설득하는 입장을 취하고 있다. 즉 개인정보 보호를 개인정보 보유기관이 행정정보 공동이용에 참여하지 않기 위한 핑계거리 정도로 파악하고 있는 것이다.

구체적으로 살펴보면, 보건복지부가 “공공기관의 경우에는 장애인증명서를 활용하고자 하는 목적이 분명하고 구체적으로 명시가 되어 있어 승인을 하였으나, 금융기관은 이용사무의 목적이 분명하지 못할 뿐 아니라 정보의 주체인 장애인들이 정보가 노출되는 것을 꺼려하고 있어 승인을 보류하였다”고 밝힌 것에 대해, 행정정보공유추진단에서 장애인 단체와 만나 개인정보 노출에 문제가 없음 등을 설명하고 설득하여 동의를 얻을 수 있도록 보건복지부에서 준비해달라고 요청하고 있으며, “34개 공공기관에 대하여는 모두다 승인 예정이나, 금융기관은 정보주체의 금융거래제한 등 권익침해 목적에도 사용할 우려가 있고, 오남용을 제어할 충분한 장치가 없다고 판단하여 정보제공이 곤란하다”고 한 부분에 대해서도 행정정보공유추진위원회는 실제적으로 현재의 종이문서가 오남용을 오히려 제어할 수 없고, 종이문서는 오남용을 통제할 수 없으나 공유시스템은 통제가 가능하고 정보공유는 정보공개가 아닌 최소한의, 미니멈적 정보공유 개념이라고 답변하고 있다.

그리고 대법원이 제도적, 기술적으로 미비점이 있는 상태에서 개인의 프라이버시에 관해 본질적인 내용을 이루고 있는 호적·제적정보를 공공·금융기관에까지 제공하는 것은 원칙적으로 제외하는 것이 타당하다고 의견을 표명하자, 행정정보공유추진위원회는 기술적인 측면은 이용기관 담당자가 자기인증서를 이용해서 담당자만이 접근할 수 있도록 하였으며, 인터넷 망에서 해킹을 방지할 수 있는 강한 암호화와 증적관리시스템을 구축하는 등 현재의 기술 중에서 가장 완벽한 기술을 사용하여 오남용의 우려는 크지 않을 것이라고 답변하고 있다. 또한 개인정보 보호의 원칙 중에는 「공공기관의 개인정보보호에 관한 법률」에 정보주체가 자기정보를 스스로 통제할 수 있는 권리가 있으므로 본인동의라는 절차 하에 호적정보를 제공하는 것은 문제가 없으며, 호적정보를 항목마다 코드를 정하여 데이터 레벨링하여 제공하고 있으므로 종이문서보다 개인정보가 보호되고 있고, 전자정부 추진사업이 효율성만 강조하면서 다른 가치를 희생시키는 것이 아니고, 효율성도 높이고 프라이버시 보호라는 가치도 올릴 수 있다는 마인드로 접근해야 한다고 밝히고 있다. 덧붙여 행정정보 공유시스템은 오프라인상의 종이문서에서 생기는 여러 가지 불필요하고 민감한 정보들을 보완해주는 수단이 되고, 종이문서는 제출 후 악용이 확인이 안 되지만 행정정보공유시스템은 증적관리가 되기 때문에 이런 문제가 해결될 것이라고 설득한다.

법무부가 공동이용의 법적근거, 오·남용 시 제공기관의 책임소재, 일반사무에 대한 정형화 문제 등이 있는 상황에서 공공·금융기관에까지 확대하는

것은 곤란하다는 의견을 내비친 것에 대해서도 추진위원회는 현재의 법적인 환경에서 최소한 제공기관이 적법한 절차에 따라서 정보제공을 할 수 있는 법적환경은 갖추어졌다고 보고 있고, 법도 시대 상황에 따라 변천·발전되어 온 것이기 때문에 완벽한 법제도에 맞추어 시행하여야 한다는 마인드를 버리고 문제가 생기면 보완·발전시키는 방향으로 추진하여야 할 것이며, 행정정보공유시스템 자체가 현재의 문제점 등을 보완할 수 있는 보완 시스템의 역할을 할 수 있다는 점과 법적근거는 상세하고, 구체적인 근거 외에 포괄적인 근거로 크게 보아 접근할 수도 있다고 주장하고 있다.

한편 국세청은 「국세기본법」 제81조의10 비밀유지조항에서 국세정보제공을 기본적으로 금지하고 있어 「행정정보공동이용법」이 통과된다 하더라도 공공·금융기관에 정보를 제공하는 것은 곤란하다는 입장을 피력하고 있는데, 이에 대해 행정정보공유추진위원회는 법리적인 문제라면 국세청과 추진단이 법제처와 협의를 해서 유권해석을 받아 해결하면 될 것이라고 밝히고 있다.

이와 같이 행정정보공유추진위원회 소위원회의 회의록을 살펴보면, 행정정보 공동이용과 개인정보 보호간의 관계에 대한 행정정보공유추진위원회의 입장은 행정정보 공동이용 상에서 발생하는 개인정보의 수집·유통의 문제를 통제하기 어려울 것이며, 개인정보DB의 통합 연계에 따른 문제를 간과하고 있음을 잘 보여주고 있다.

행정정보 공동이용과 관련된 문헌이나 관련기사를 보면 행정정보 공동이용의 핵심은 개인정보 보호에 있다고 하면서도 실질적으로 이에 대한 대책은 향후 입법될 「개인정보보호법」에서 다룰 사항으로 유보되고 있다. 현재 개인정보 보호 문제를 제대로 다루지 않는 것도 문제일뿐더러 향후 「개인정보보호법」에 행정정보 공동이용에 따른 개인정보 보호의 문제를 다룬다 하더라도 이 법이 일반법적 성격을 갖는 이상 행정정보 공동이용에 따른 개인정보 보호대책과 관련한 구체적인 내용을 포함하지 않는다면 문제는 상존하게 될 것이다. 더욱이 행정안전부가 2008년 8월에 입법예고한 「전자정부법 전부개정법률안」은 각 행정기관이 자신의 소관업무를 수행하기 위하여 각자 별도로 구축·운용하고 있는 개인정보DB를 통합적으로 연동 내지는 연계할 수 있는 가능성을 열어놓고 있다. 그러나 각 행정기관이 보유하고 있는 수많은 개인정보DB를 시스템적으로 통합 가능하도록 허용하는 것은, 설사 그것이 실제로는 부분적이고 일시적인 연계에 의한 개인정보의 공동이용이라 하더라도, 상당한 위험성을 지닌 문제라고 할 것이다(성낙인 외, 2008: 840).

개인정보보호정책에서 있어서 정부의 인식이 미흡하다는 것은 개인정보보호와 관련된 예산이 정보화와 관련된 예산 중 0.2%에 불과하다는 사실에서 잘 드러난다. 특히 공공기관에 의한 개인정보 침해사건이 급격히 증가하고 있음을 감안하면, 우리 정부의 정책은 정보화의 추진에만 급급할 뿐, 그 역기능을 최소화할 수 있는 정책을 적절히 병행하지 못하고 있다고 볼 수 있다(성낙인 외, 2008: 240).

### 3) 개인정보의 열람 및 정정・삭제 청구권 보장실태

정보주체의 자기정보 및 제3자 제공 내역에 대한 열람청구방법, 정정・삭제 청구방법에 대해 행정안전부에 문의한 결과, 행정정보공동이용센터에서는 국민의 개인정보에 관한 사항을 보유하고 있지 않으며, 이에 따라 제3자 제공도 하고 있지 않다고 답변하였다. 다만, 타 기관이 보유한 행정정보를 제3의 기관이 열람할 수 있도록 자료를 중계하고 있으며, 이에 대한 각 개인정보의 열람, 정정, 삭제 등은 각 정보를 보유하고 있는 기관에 청구하여야 하며, 각 개인정보의 열람, 정정, 삭제에 관하여는 각 기관 소관의 법령 및 내부규정・규칙 또는 「공공기관의 개인정보보호에 관한 법률」 및 「공공기관의 정보공개에 관한 법률」에 의한다고 밝히고 있다.[30] 그리고 이러한 내용과 관련한 관리책임자는 각 이용기관의 기관총괄책임자 및 권한부여책임자 등이라고 한다.

## 3. 소결

이상에서 행정정보공동이용시스템을 통한 개인정보 수집・유통 실태에 대해 살펴보았다. 현재의 행정정보공동이용시스템은 사실상 개인정보의 공동이용을 다루고 있으면서도 이를 언급하지 않은 채 '일반행정정보 공동이용'과 '개인정보 공동이용'을 묶어서 다루고 있으며, 그 과정에서 개인정보가 무단으로 열람되거나 유출될 가능성을 배제하지 못하고 있다. 이러한 문제는 이미 행정정보공유추진단의 '행정정보공동이용 실태점검 결과'에서 반복적으로 지적되고 있고, 감사원 감사에서도 지적되었지만, 여전히 미비한 상태로 남아 있다. 게다가 입법예고된 「전자정부법 전부개정법률안」에서는 각 행정기관이 자신의 소관업무를 수행하기 위하여 각자 별도로 구축・운용하고 있는 개

30) '행정정보공동이용시스템 관련 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.14).

인정보DB를 통합적으로 연동 내지는 연계할 수 있는 가능성을 열어놓고 있어 문제를 확대재생산하고 있다.

정부가 강조하고 있는 것처럼, 행정정보 공동이용을 통한 효용성이 있는 것은 사실이지만, 2008년 9월 2일부터 8일에 걸쳐 전국의 성인남녀 1,000명을 대상으로 하여 이루어진 일반인 조사에 따르면, 시민들은 개인정보 공동이용을 부정적으로 인식하고 있다. '개인정보 정부의 각 기관들이 보유하고 있는 개인정보를 서로 공동이용함으로써 민원업무의 신속한 처리나 제출 서류의 간소화 등의 이점이 있는 반면, 개인정보의 오·남용이 있을 수 있다는 점을 적시하면서, 그러한 개인정보를 소관업무의 수행을 위하여 공유하는 것에 대해 어떻게 생각하는지'를 질문한 결과, 시민들은 정부의 각 기관 상호간은 물론 정부와 금융기관의 개인정보 공유에 대해서도 60% 이상이 바람직하지 않거나 불필요하다는 의견을 보였다. 정부 간 개인정보 공유에 대해서는 바람직하지 않다 45.4%, 전혀 바람직하지 않다 16.9%로 나타났고, 정부에서 금융기관에로의 개인정보 공동이용에 대해서는 필요하지 않다 40.8%, 전혀 필요하지 않다 21.7%로 나타났다(성낙인 외, 2008: 232-234). 이러한 결과는 행정정보공유추진위원회가 발간한 『2007 행정정보공동이용 백서』(2007: 83)상의 국민인식조사결과와 차이가 난다. 『2007 행정정보공동이용 백서』에서는 행정정보공동이용의 공공기관 확대에 대해 필요하다는 의견이 89.5%였고, 필요하지 않다는 의견이 0.5%였으며, 금융기관 확대에 대해서도 필요하다는 의견이 67.9%였고, 필요하지 않다는 의견이 10%였다.

이러한 국민들의 의견을 감안한다면, 행정정보 공동이용시스템을 통한 개인정보 공동이용에 대해서는 좀더 신중한 접근이 요구된다 하겠다.

# II. 행정기관 간 개인정보 공유

## 1. 개요

「전자정부법」상의 '행정정보 공동이용'이란 개인정보를 포함하여 행정기관이 보유·관리하고 있는 행정정보를 다른 행정기관 또는 공공기관 등이 "정보시스템을 통하여" 공동이용하는 것을 말한다(행정자치부, 2008: 63). 여기에서 개인정보의 공동이용은 구체적으로 언급되고 있지 않으나, 각 행정기관이 보유·관리하고 있는 개인정보파일, 즉 개인정보DB들을 상호 연동내지는 연계하는 방식으로 이루어질 것이다(성낙인 외, 2008: 838). 그러나 현

행법상 이와 같이 개인정보DB의 연동 내지는 연계를 통한 개인정보 공동이용에 대한 규율은 행해지지 않고 있다.

개인정보 오·남용 문제를 비롯한 개인정보의 공동이용과 관련하여 발생하는 문제들은 제대로 지적되지 않고 있으며, 행정기관 간 행정정보의 제공 및 공동이용에 따른 부작용도 통제의 사각지대에 남아 있다. 나아가 개인정보보호를 위해서는 개인정보의 공동이용 문제가 별도로 검토되어야 함에도 불구하고 그 자체가 논의되고 있지 않다.

개인정보파일이란 처리정보를 쉽게 검색할 수 있도록 일정한 형식에 따라 체계적으로 배열하거나 구성된 개인정보의 집합물로서, 업무수행 중 발생되는 파일 중 개인을 식별, 판단, 평가하게 하는 개인정보를 포함하는 파일을 말한다.[31] 이는 PC, 서버 등을 기반으로 생성되며, 문서파일, 데이터베이스 파일, 화상파일 등 다양한 형태로 생성될 수 있다. 개인정보파일을 보유한다는 것은 업무 처리를 목적으로 개인정보파일을 생성하여 가지고 있거나, 공유 및 연계정보를 처리하여 저장하고 있는 경우로(단순열람 제외), 개인정보파일에 대한 처리 업무를 다른 기관·단체 등에 위탁한 경우에는 위탁기관이 보유하고 있는 것이 된다(수탁기관 제외)(행정안전부, 2009d: 2). 따라서 개인정보파일의 범위에는 개인 PC에 저장하여 관리되는 파일, 시스템(DB) 단위로 저장되어 관리되는 파일, 위탁 관리되는 파일이 모두 포함된다.

2009년 4월 행정안전부가 제정한 「공공기관 개인정보파일 관리지침」은 「공공기관의 개인정보보호에 관한 법률」에 근거하여 개인정보파일 범위 및 분류, 개인정보파일 생성 및 처리, 개인정보파일 열람 및 변경, 개인정보파일 파기, 개인정보파일 대장 작성 요령 및 표준목록 등 개인정보파일 관리에 관한 세부사항을 규정하고 있다.

「공공기관의 개인정보파일 관리지침」은 「정부조직법」에 따른 중앙행정기관 및 그 소속기관으로서, 중앙행정기관(소속·부속기관, 특별지방행정기관 포함), 합의제 행정기관, 대통령 자문기구, 독립·한시위원회 등과, 「지방자치법」에 따른 지방자치단체, 「지방교육자치에 관한 법률」에 따른 교육기관(교육위원회, 교육청(보조기관, 소속기관 포함), 하급교육행정기관 등), 「초

31) 「공공기관의 개인정보보호에 관한 법률」은 제2조제4호에서 '개인정보파일'이라 함은 컴퓨터등에 의하여 처리할 수 있도록 체계적으로 구성된 개인정보의 집합물로서 자기테이프·자기디스크 등 전자적인 매체에 기록된 것을 말한다고 규정하고 있으며, 행정안전부가 2008년 8월 12일 입법예고한 「개인정보보호법 제정법률안」은 제2조제4호에서 "개인정보파일"이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말한다고 규정하고 있다. 이는 물론 개인정보데이터베이스 혹은 개인정보처리시스템을 의미한다(성낙인 외, 2008: 705).

·중등 및 고등교육법」, 그 밖의 법률에 따른 각급학교, 「공공기관의 운영에 관한 법률」에 따른 공공기관, 「지방공기업법」에 따른 지방공사 및 지방공단, '특별법'에 의해 설립된 특수법인을 적용대상으로 하고 있다.[32] 그 적용분야는 「공공기관의 개인정보보호에 관한 법률」을 적용 받는 공공기관에서 업무처리를 목적으로 보유·처리하고 있는 전자적 형태의 개인정보파일이며, 「통계법」에 의해 수집되는 개인정보나 국가안전보장과 관련된 정보분석을 목적으로 수집되는 정보는 적용에서 제외된다(행정안전부, 2009d: 1-2).

「공공기관의 개인정보파일 관리지침」에 따르면, 개인정보파일은 업무분장표 또는 정보시스템에 의해 처리하는 단위업무의 유형별로 구분하여 분류해야 하는데, 공공기록물 분류체계인 부서별 기록관리기준표를 준용할 경우 업무관리시스템의 단위과제, 전자결재시스템의 단위과제(기록물철) 수준으로 분류할 수 있다. 전국 단일의 공통업무를 집행하고 있는 기관(특별지방행정기관, 자치단체, 교육기관)의 경우 행정안전부가 제공하는 당해 '개인정보파일 표준목록'을 우선하여 관리해야 한다(행정안전부, 2009d: 3). 표준 개인정보파일이란 전국 단일의 공통업무 집행을 위해 다수의 기관에서 동일하게 발생하는 개인정보파일을 말한다.[33]

「공공기관의 개인정보보호에 관한 법률」은 공공기관이 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 제3자에게 이용 또는 제공할 수 없다는 것을 원칙으로 하면서도(제10조제1항), 목적 외 제3자 제공을 할 수 있는 예외를 상당히 광범위하게 허용하고 있다. 즉 ① 다른 법률에 따라 이용 또는 제공의 근거가 있는 경우(제10조제1항), ② 정보주체의 동의가 있거나 정보주체에게 제공하는 경우, ③ 당해 정보를 이용 또는 제공하지 않고서는 다른 법률에서 정한 소관 업무를 수행할 수 없다고 공공기관 개인정보보호심의위원회가 인정한 경우, ④ 조약 기타 국제협정의 이행을 위하여 외국정부나 국제기구에 제공하는 경우, ⑤ 통계작성 및 학술연구 등의 목적을 위해 특정개인을 식별할 수 없는 형태로 제공하는 경우, ⑥ 정보주체나 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 동의를 할 수

32) 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관은 제외된다.

33) 예를 들면, 노동부의 경우 구직관리, 사회적 일자리 사업관리, 명예고용평등감독관관리 등, 기상청의 경우 홈페이지 회원정보 파일, 병무청의 경우 공익근무요원 소집대상자 파일, 예비군 자원관리 파일 등, 시도의 경우 공익근무요원관리, 민방위교육훈련관리, 산림자격증관리 등, 그리고 교육청 및 각급학교의 경우 취학대상자 관리(초, 특), 학적, 성적 등이 이에 해당한다.

없는 경우에 그 이용 또는 제공이 명백히 정보주체에게 이익이 되는 경우, ⑦ 범죄의 수사와 공소의 제기 및 유지에 필요한 경우, ⑧ 법원의 재판업무 수행을 위하여 필요한 경우(이상 제10조제3항 각호)에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있도록 하고 있는 것이다. 특히 개별 법률에서의 명시적인 근거나 정보주체의 동의가 없더라도, 제공받는 다른 기관의 소관업무의 수행에 필요하다면 공공기관 개인정보보호심의위원회의 심의를 거쳐 보유목적 외의 이용 또는 제공이 가능하다는데 주목할 필요가 있다.

그리고 「국세기본법」, 「관세법」 및 「지방세법」상에도 이와 유사한 규정이 있다. 「국세기본법」 제81조의10 제1항에서도 과세정보를 타인에게 제공 또는 누설하거나 조세의 부과 또는 징수의 목적 외의 용도로 이용하는 것을 금지하되, 지방자치단체 등이 법률이 정하는 조세의 부과 또는 징수의 목적 등에 사용하기 위하여나, 국가기관이 조세쟁송 또는 조세범의 소추목적을 위하여, 법원의 제출명령 또는 법관이 발부한 영장에 의하여, 세무공무원 상호간에 조세의 부과·징수 또는 질문·검사상의 필요에 의하여, 통계청장이 국가통계작성 목적으로, 그리고 다른 법률의 규정에 따라 과세정보를 요구하는 경우에는 그 사용목적에 맞는 범위 안에서 납세자의 과세정보를 제공할 수 있다고 하여 공동이용이 가능한 정보에 대해 규정하고 있으며, 「관세법」 제116조제1항 및 「지방세법」 제69조제1항에도 이와 유사한 규정을 두고 있다. 「국세기본법」, 「관세법」 및 「지방세법」상의 과세정보는 "행정기관"이 보유하고 있는 개인정보로서, 예외적으로 「전자정부법」상 공동이용의 대상이 되는 개인정보라고 할 수 있을 것이다.

2007. 1. 3. 개정된 「전자정부법」은 제22조의2(공공기관등의 행정정보 공동이용)를 신설하여 행정기관이 보유하는 개인정보를 공공기관과 민간의 금융기관에까지도 제공할 수 있도록 확대하였다. 이에 따라 행정정보공유추진단에서는 2007년부터 각 공공기관과 금융기관까지 행정정보공동이용 실태점검에 나서고 있다. 문제는 「전자정부법」 제21조와 제22조의2 규정이 「공공기관의 개인정보보호에 관한 법률」이 보유목적 외의 제3자 제공의 허용기준으로 설정하고 있는 "다른 법률"에 해당하는 것으로 해석될 수 있다는 점이다. 만약 그렇다면 행정기관이 보유하는 대부분의 개인정보는 별다른 제한 없이 다른 기관과의 공동이용이 얼마든지 가능하게 된다.[34] 이 경우에는

34) 해석상 그렇게 될 가능성이 있다는 것인지, 실제로 그렇게 되고 있는지 여부에 대한 실태를 파악해야 하나, 현재의 행정정보공동이용시스템은 행정정보와 개인정보를 별도

공공기관 개인정보보호심의위원회의 심의를 거칠 필요도 없게 되고, 제10조 제6항의 제공사실의 공시 규정을 통해서만 절차적으로 통제할 수 있는데, 이 또한 그 요건을 '동조 제3항 제2호 내지 제5호 및 제7호'에 따른 제공으로 한정하고 있기 때문에 해석상 「전자정부법」에 근거한 제3자 제공에는 적용되지 않는다(성낙인 외, 2008: 837).

이처럼 '개인정보 공동이용'이 개인정보보호의 측면에서 안고 있는 문제는 단순히 보유정보를 다른 기관에게 개별적으로 제공하는 차원에서 발생하는 문제가 아니다. 아래에서는 공공기관 개인정보보호심의위원회를 중심으로 행정기관 간 개인정보의 수집·유통 실태에 대해 살펴보고, 개인정보파일의 수집·유통 실태에 대해서는 별도로 검토한다.

## 2. 행정기관 간 개인정보의 수집·유통 실태

### 1) 공공기관 개인정보보호심의위원회의 역할 미흡

행정정보 공동이용시스템에 의한 개인정보의 수집·유통이 주로 e민원사이트를 통한 행정정보 공동이용의 문제라면, 행정기관 간 개인정보의 이용 및 제공 문제 또한 별도로 검토할 필요가 있다. 이에 대해서는 앞에서 본 바와 같이 행정정보공동이용을 확대하는데 업무의 초점이 가있는 행정정보공유추진위원회가 전혀 관여하지 못하고 있을 뿐만 아니라 제 역할을 해야 하는 공공기관개인 정보보호심의위원회가 거의 기능을 하지 못하고 있는 상황이며, 오히려 논란의 소지가 있는 개인정보의 이용 및 제공을 정당화해주는 역할마저 하고 있어 문제가 되고 있다.

공공기관 개인정보보호심의위원회는 「공공기관의 개인정보보호에 관한 법률」 제20조에 근거하여 설치되며, 「공공기관의 개인정보에 관한 법률 시행령」에 관련 규정이 있다.

「공공기관의 개인정보보호에 관한 법률」[법률 제8871호, 2008.2.29, 타법개정]
제20조 (공공기관개인정보보호심의위원회) ①공공기관의 컴퓨터등에 의하여 처리되는 개인정보의 보호에 관한 사항을 심의하기 위하여 국무총리소속하에 공공기관개인정보보호심의위원회(이하 "위원회"라 한다)를 둔다.
②위원회는 다음 각 호의 사항을 심의한다.
1. 개인정보보호에 관한 정책 및 제도 개선에 관한 사항

로 구분하지 않고 있기 때문에 명확하게 알기는 어려운 상황이다.

2. 처리정보의 이용 및 제공에 대한 공공기관 간의 의견조정에 관한 사항
3. 제6조제5항에 따라 심의요청을 받은 사항
4. 제10조제3항제2호에 따른 처리정보의 이용 또는 제공에 관한 사항
5. 그 밖에 개인정보의 보호에 관하여 대통령령으로 정하는 사항

③위원회는 위원장 1인을 포함한 10인 이내의 위원으로 구성한다.

④위원장은 행정안전부차관으로 하고, 위원은 공공기관의 소속직원과 개인정보에 관한 학식과 경험이 풍부한 자 중에서 위원장의 추천으로 국무총리가 임명 또는 위촉한다.

⑤위원의 임기는 2년으로 한다. 다만, 공공기관의 소속 직원인 위원은 그 직에 있는 동안 재임한다.

⑥그 밖에 위원회의 조직 및 운영에 관하여 필요한 사항은 대통령령으로 정한다.

「공공기관의 개인정보보호에 관한 법률 시행령」[대통령령 제21025호, 2008.9.22, 타법개정]

제24조의2 (공공기관개인정보보호심의위원회의 기능) 법 제20조제2항제5호에서 "대통령령으로 정하는 사항"이란 국무총리 또는 법 제20조에 따른 공공기관개인정보보호심의위원회의 위원장이 개인정보보호와 관련하여 위원회에 부의하는 사항을 말한다.

제24조의3 (위원장) ① 위원회의 위원장은 위원회를 대표하고 위원회의 사무를 총괄한다.

② 위원장이 부득이한 사유로 그 직무를 수행할 수 없는 때에는 위원장이 지명하는 위원의 순으로 그 직무를 대행한다.

제24조의4 (위원회의 회의) ① 위원장은 위원회의 회의를 소집하고 그 의장이 된다.

② 위원장이 회의를 소집하는 때에는 회의 개최 7일 전까지 회의 일시·장소 및 심의사항 등을 각 위원에게 통지하여야 한다. 다만, 긴급을 요하거나 부득이한 사유가 있는 경우에는 그러하지 아니하다.

③ 위원회의 회의는 재적위원 과반수의 출석으로 개의하고, 출석위원 과반수의 찬성으로 의결한다.

제24조의5 (위원회의 간사) ① 위원회의 사무를 처리하기 위하여 위원회에 간사 1명을 둔다.

② 제1항의 간사는 행정안전부의 개인정보보호업무를 담당하는 공무원 중에서 위원장이 임명하는 자가 된다.

제24조의6 (분과위원회의 설치 등) ① 위원회는 위원회 심의사항의 사전 검토 등을 위하여 필요하면 분과위원회를 설치·운영할 수 있다.

② 위원회는 효율적이고 전문적인 심의를 위하여 필요하면 관계전문가의 자문을 구하거나 이해관계자 등의 의견을 들을 수 있다.

제24조의7 (수당) 위원회 또는 분과위원회에 출석한 위원, 관계전문가 등에 대하여는 예산의 범위에서 수당을 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접 관련되어 위원회 또는 분과위원회에 출석한 경우에는 그러하지 아니하다.

제24조의8 (운영세칙) 이 영에 규정된 사항 외에 위원회 또는 분과위원회의 운영에 관하여 필요한 사항은 위원회의 의결을 거쳐 위원장이 정한다.

1995. 4. 3일에 설치된 개인정보보호심의위원회는 ① 개인정보보호에 관한 정책 및 제도 개선 심의, ② 처리정보의 이용 및 제공에 대한 공공기관 간의 의견조정 심의, ③ 「공공기관의 개인정보보호에 관한 법률」 제6조제5항에 따라 행정안전부장관이 개인정보파일의 보유·변경 시 개인정보의 보호를 위하여 필요하다고 인정하는 때에 공공기관 개인정보보호심의위원회에 협의사항에 관하여 심의를 요청한 사항 심의, ④ 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우 당해 개인정보파일의 보유목적외의 목적으로 처리정보의 이용 또는 제공에 관한 사항 심의 등의 기능을 한다. 개인정보보호심의위원회는 행정안전부 제2차관을 위원장으로 국가정보원 사이버안전센터장, 방송통신위 이용자네트워크국장/네트워크정책관, 교육과학기술부 평생직업교육국장, 행정안전부 정보기반정책관 등 정부 당연직 위원과, 외부의 민간 전문가로 구성된다.[35)]

행정안전부가 원유철 의원에게 제출한 '공공기관 개인정보보호심의위원회 개최현황'에 따르면, 개인정보보호심의위원회는 1995년 10월 18일 운영세칙 제정을 위해 제1차 위원회가 열린 이래 2008년 3월 27일 회의까지 단 10번만 개최되었을 뿐이다. 1999년과 2000년, 2007년에는 단 한번도 위원회가 열리지 않았고, 1997년과 2001년, 2002년에 각각 한 차례씩 있었던 위원회는 서면심의로 대신하였다. 심의안건 역시 위원회 운영세칙의 제·개정이 네 건을 차지하는 등 "개인정보보호에 관한 정책 및 제도개선"이라는 당초 설립 취지가 무색하게 한다(유정현, 2008: 3; 원유철, 2008).

35) 현재 민간 전문가는 정보통신 관련전공 교수 2인, 변호사 1인, 시민단체 전문가 1인, 정보통신 학회 또는 정부출연기관 관련인사 1인으로 구성되어 있다.

<표 2-12> 공공기관 개인정보보호심의위원회 회의개최 여부('05~'09)

| 연 도 | 2005 | 2006 | 2007 | 2008 | 2009.6 |
|---|---|---|---|---|---|
| 회 수 | - | 1 | - | 2 | 3 |

2004. 12. 22일에 있었던 제7차 개인정보보호심의위원회에서는 ''04년도 개인정보보호처리실태 조사결과 및 향후 조치계획'에 대해 토론하면서 NEIS 사업에 대한 모니터링 등 감독·조정 역할 등 개인정보보호심의위원회의 역할 정립과 기능강화를 논의하였다. 하지만 그 구체적인 내용은 언급되어 있지 않다.

한해를 건너뛰어 2006. 1. 25일에 열린 제8차 개인정보보호심의위원회에서는 「공공기관의 개인정보보호를 위한 기본지침(안)」을 안건으로 상정하여 심의하였다. 그 토론에서는 개인정보에 대한 접근권한, 기술적 조치 등도 필요하지만 개인정보보호책임관의 관심과 개인정보 관리자 등에 대한 지속적인 교육이 중요하므로 이를 업무계획에 반영토록 하고, 개인정보의 오·남용 등 법 위반 시 이를 적발하는 메커니즘 구축 필요성에 대해 추가검토하며, 시대적인 변화에 따라 정보공유의 이점이 많음에도 개인정보의 보호적 관점만 강조하면 안된다는 얘기도 나왔다. 자기정보가 어떻게 이용 및 제공되는지와, 개인정보의 오·남용에 따른 부작용 사례 등에 대하여 국민적 홍보를 하도록 하고, 개인정보보호심의위원회를 수시 개최하여 위원회의 기능 활성화를 도모하기로 하였다. 하지만 제9차 공공기관 개인정보보호심의위원회는 2년 후에 개최되어 이러한 논의를 무색하게 하였다.

옥션 등 대형 개인정보침해사고가 발생하는 등 개인정보에 대한 사회적 관심이 증가함에 따라 2008년에 "공공기관 개인정보보호 종합대책(안)" 심의 등을 위한 회의를 2회 개최하여 총 10건의 안건을 처리했고, 2009년에는 상반기에만 3회에 걸쳐 회의가 개최되는 등 운영이 활성화되는 양상을 보였다. 하지만 그 속을 들여다보면 공공기관 개인정보보호심의위원회의 심의가 반드시 요구되는 사안이 발생한 경우 단지 이 사안 하나만을 처리하기 위해 소집한 것뿐이며, 모두 서면심의로 대체하여 논의를 형식화하고 있다. 심의요청자료에 대해 「공공기관의 개인정보보호에 관한 법률」 제10조에서 정한 '처리정보의 보유목적외 이용·제공' 요건(예외적 제공 요건)의 충족 여부를 검토하는 데 있어서 위원 개개인이 자신의 의견만 적어내고 이를 취합하여 다수의견을 수용하는 방식으로 처리하는 서면심의방식은 적절치 않다. 위원들 사이의 토론과정에서 입장을 바꿀 수 있는 여지를 봉쇄하고 사실상 위원회의

합의제가 가진 장점을 박탈하고 있기 때문이다. 심의결과 보고에는 행정안전부 개인정보보호과가 서면심의로 한 이유가 드러나 있지 않다.

<표 2-13> 공공기관개인정보보호심의위원회 회의일자 및 안건

| 회차 | 일자 | 회의안건 |
|---|---|---|
| 7차 | '04.12.22 | (1) '04년도 개인정보처리실태 조사결과 및 향후 조치계획<br>(2) 개인정보보호기본법 제정 추진 현황 : 보고 |
| 8차 | '06.1.25 | ○ 안건심의 : 공공기관의 개인정보보호를 위한 기본지침(안)<br>○ 보고사항<br>- 개인정보보호 관련법안 제·개정 추진 상황<br>- '05년도 하반기 개인정보 처리실태 조사결과<br>- '05년도 공공기관 홈페이지 개인정보 노출 모니터링 결과<br>- '05년도 개인정보 노출진단 연구용역 결과 |
| 9차 | '08.1.22 | <제1호> 공공기관 개인정보보호심의위원회 운영세칙(안)<br><제2호> 원전종사자 및 주변주민 역학조사연구 대상자 암 발병 수진자료 이용·제공 심의요청<br><제3호> 공공기관 개인정보보호 종합대책(안)<br><제4호> 공공기관의 개인정보보호에 관한 법률 개정내용 : 보고<br><제5호> 웹사이트 개인정보 노출 점검결과 및 향후 대책 : 보고 |
| 10차 | '08.3.27 | <제1호> 공공기관 개인정보보호심의위원회 운영세칙(안)<br><제2호> 2008년도 공공기관 개인정보보호 기본지침(안)<br><제3호> 헌혈부적격자로 인한 혈액사고 방지목적으로 헌혈금지 약물 복용자 명단 이용·제공 심의요청<br><제4호> 공공기관 CCTV 관리실태 조사 결과 : 보고<br><제5호> 2008년도 공공기관 개인정보보호 수준진단 기본계획(안) : 보고 |
| 11차 | '09.1.19 ~ 1.21 | <1건> 지방세체납처분을 위한 「국민건강보험 직장가입자 자격취득 및 상실정보 이용·제공」(요청기관: 지자체, 제공기관: 건보공단) |
| 12차 | '09.3.16 ~ 3.18 | <1건> 퇴직공직자 취업제한 위반여부 확인을 위한 「국민건강보험 직장가입자자격 취득 및 상실정보 이용·제공」(요청기관: 공직자윤리위원회, 제공기관: 건보공단) |
| 13차 | '09.4.15 ~ 4.17 | <1건> 공직자 쌀직불금 부당수령 여부 확인을 위한 「공무원연금관리공단 공무원 재직자정보 이용·제공」(요청기관: 행정안전부, 제공기관: 공무원연금관리공단) |

자료: '개인정보파일 대장 등 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.13) 중 제7차~13차 공공기관 개인정보보호심의위원회 회의 결과보고.

행정안전부에 2004년 이후의 개인정보보호심의위원회 회의록 및 안건지 일체를 정보공개 청구한 결과 개인정보보호심의위원회 안건은 보관기간 경과로 인해 존재하지 않거나 인쇄본으로만 보관 중이라고 밝히고 있으며, 간략한 회의내용이 담긴 심의결과 보고문서만 공개하였다. 이를 통해 각 회의의 논의안건이 무엇인지는 알 수 있지만, 정작 안건지가 공개되지 않음으로써 개인정보 이용·제공과 관련된 공공기관 개인정보보호심의위원회의 논의내용을 구체적으로 파악하기는 어렵다.

행정안전부는 2008년 국정감사 서면답변에서 개인정보보호심의위원회의 기능을 확대하고, 실효성 있는 기관으로 제 역할을 할 수 있는 방안으로, 「개인정보보호법」이 제정되면 공공기관 개인정보보호심의위원회는 폐지하고 개인정보보호위원회를 신설할 예정이며, 신설 개인정보보호위원회는 위원장을 민간인으로 위촉하는 등 운영의 독립성을 강화하고 심의 대상을 대폭 확대하여 운영에 내실을 기할 계획이라고 밝히고, 「개인정보보호법」제정 전까지는 현행 공공기관 개인정보보호심의위원회 회의를 정례화하여 운영을 활성화하겠다고 밝힌 바 있다(행정안전부, 2008c). 하지만 2009년 들어 공공기관 개인정보보호심의위원회 회의는 정례화되고 있지 않으며, 서면심의가 이루어지고 있어 운영이 활성화되고 있다고 보기 어렵다. 또한 현재 정부가 입법예고한 「개인정보 보호법안」(의안번호 제1802369호)에 따르더라도 개인정보보호위원회는 심의기능만을 가지는데, 이래서는 개인정보 보호기능을 다할 수 없다.[36)]

최근 NEIS의 통합 문제가 논란이 되고 있는데, 이 또한 개인정보 보호와 관련된다는 점에서 공공기관 개인정보보호심의위원회가 다루어야 할 사안이 분명함에도 불구하고 교과부에서 이에 대한 안을 제출하면서 개인정보보호심의위원회의 모니터링을 거치지 않았다. 정부의 「개인정보 보호법안」(의안번호 제1802369호)에 따르면 "중앙행정기관의 장"은 시행계획의 수립(제8조), 자료제출 요구(제11조), 개인정보 보호지침의 수립(제12조), 의견제시 및 개선권고(제51조), 자료제출 요구 및 검사(제53조), 시정조치(제54조), 고발 및 징계권고(제55조), 결과의 공표(제56조)를 독자적으로 실시할 수 있도록 하고 있다. 결국 사실상 개인정보 감독기능이 하나로 모아지는 것이 아니라 소관 부처에게 제각기 맡겨짐으로써 감독기능이 형해화되었다고 평가할 수 있다.

36) 정부는 국무총리 소속으로 설치되는 개인정보 보호위원회가 개인정보 보호와 관련한 중요 사항에 대하여 의사결정의 신중성·전문성·객관성을 확보할 것이라고 기대하고 있으나, 개인정보 보호 기본계획, 법령 및 제도 개선 등 개인정보에 관한 주요 사항을 심의하는 것에 기능이 한정되고 있다.

NEIS의 통합 문제와 같은 사안이 발생하더라도 개인정보보호위원회가 감독할 수 없는 것이다.

그래서 「개인정보보호법」에 규정되는 개인정보보호위원회는 유럽연합에서처럼 행정부로부터 독립된 조직으로서 침해조사권, 구제권, 개인정보보호지침 제정권과 같은 실질적인 권한을 가져야 한다는 의견이 제시되기도 하지만(원유철, 2008), '개인정보보호법'이라는 일반법적 성격이나 법체계를 감안하면 그렇게 구체적인 권한부여가 규정되기는 어렵다. 향후 「개인정보보호법」이 제정되어 개인정보 보호위원회가 설립된다면, 제 기능을 못하는 현재의 공공기관 개인정보보호심의위원회와는 달라져야 한다. 즉, 행정정보를 공동이용하는 정부 각 부처로부터 독립적이며 개인정보 보호와 관련한 사항에 대하여 실질적인 감독 권한을 가진 감독기구가 설립되어야 하는 것이다.

### 2) 개인정보의 이용 및 제공 실태

행정기관 간 개인정보의 이용·제공의 문제는 공공기관 개인정보보호심의위원회에서 안건으로 다루어진 사안을 중심으로 검토하기로 한다. 공공기관 개인정보보호심의위원회는 처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용 또는 제공하는 것에 관한 사항을 심의하기 때문이다.

이에 따라 공공기관 개인정보보호심의위원회는 「공공기관의 개인정보보호에 관한 법률」 제10조에서 정한 '처리정보의 보유목적외 이용·제공' 요건(예외적 제공 요건)의 충족 여부, 즉 요청자료 미제공시 법률상 수행 소관 업무 가능 여부(요청사항이 법률에 정한 소관업무에 해당할 것, 해당 자료가 이용·제공되지 않으면 요청기관의 소관업무를 수행할 수 없을 것), 정보주체 또는 제3자의 권리와 이익에 대한 부당한 침해 여부, 요청자료의 최소 범위 여부 및 제공시 안전성 확보 조치 여부를 중심으로 안건의 내용을 심의하게 된다.[37]

(1) 원전종사자 및 주변주민 역학조사연구 대상자 암 발병 수진자료 이용·제공

2008. 1. 22일 개최된 제9차 공공기관 개인정보보호심의위원회는 '원전종

37) '개인정보파일 대장 등 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.13) 중 제7차~13차 공공기관 개인정보보호심의위원회 회의 결과보고.

사자 및 주변주민 역학조사연구 대상자 암 발병 수진자료 이용·제공' 심의 요청에 대해 '처리정보를 보유목적 외의 목적으로 이용하게 하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 「공공기관의 개인정보보호에 관한 법률」 제20조에 따른 공공기관 개인정보보호 심의위원회의 심의를 거친 경우'로 보았다.

우선 요청자료 미제공시 법률상 수행 소관 업무 가능 여부, 즉 요청자료가 「원자력법」 제9조의2(원자력연구개발사업의 추진)에 근거한 '원전종사자 및 주변주민 등 역학조사연구'의 업무수행에 필수불가결한 최소한의 자료인지 여부에 대해서는, 다른 법률에서 정한 소관업무를 수행할 수 없는 경우에 대하여 시행령 또는 심의위원회에서 기준을 제시할 필요가 있다는 의견과, '다른 법률에서 정하는 소관업무를 수행할 수 없는 경우'의 판단은 법률에서 위임된 것이므로 구체적 사안에 대해서는 심의위원회에서 결정할 사항이라는 의견, 그리고 근본적 제도개선·기준마련은 해당 팀에서 연구하는 것으로 하고, 위원회에서는 개별사안별로 판단해야 한다는 의견이 제출되었다.

요청자료의 최소 범위 여부 및 제공시 안전성 확보 조치 여부에 대해서는 역학조사 목적의 취지를 살펴서 개인정보보호 대책이 안전하게 수립된 경우는 제공해야 한다는 의견, 개인정보보호 대책 및 장치를 마련하고 순수한 학술연구 목적인 경우 제공해야 한다는 의견, 역학조사의 목적은 순수학술이나, 과학기술부가 국민에게 20년 전 약속한 내용을 수행하여 지켰다는 의미가 크며, 분석과정에는 일부 개인 식별이 불가피하나 최종연구결과는 개인 식별 불가능한 경우로 발표된다는 의견, 요청정보를 주고받는 경우에는 개인 식별이 불가피하지만, 분석 시에는 개인 식별이 불가능하도록 코드화하여 매칭할 수 있는 장치가 필요하다는 의견이 제시되었다.

정보주체의 권리와 이익에 대한 부당한 침해 여부와 관련해서는, 건강보험심사평가원 개인정보의 보유목적은 요양급여의 적절성평가인데, 정보주체가 인식하지 못하는 상태에서 타기관에 자료제공하는 것에 우려가 많다고 하자, 「건강보험법」을 공익목적으로는 개인정보 활용이 가능하도록 개정할 것을 보건복지부에 권고할 필요가 있다는 의견, 개인정보보호심의위원회의 취지는 개인정보를 보호하는데 있으며, 개별법인 「건강보험법」보다는 일반법인 「공공기관의 개인정보보호에 관한 법률」에서 기준을 정하는 것이 바람직하다는 의견, 그리고 정보의 민감도 등 개인정보를 등급화하여, 보유 및 이용·제공에 따른 책임·의무 사항을 세분화하기 위한 연구가 필요하다는 의견이 제시되었다.

결국 개인정보보호를 위한 기술적, 관리적 장치를 마련하고, 국정원의 전문지식·기술검증을 거치는 것을 전제조건으로 공공기관 개인정보보호심의위원회는 원안의결을 하였다. 하지만, 「국가정보원법」 제3조의 국가기밀에 속하는 문서·자재·시설 및 지역에 대한 보안업무(제2호)나 정보 및 보안업무의 기획·조정(제5호) 등 국정원의 직무는 본 사안과 거리가 있다는 점에서 국정원의 전문지식·기술검증을 거치는 것이 타당한지 의문이다. 그리고 공개된 심의결과와 토론내용만 가지고는 과학기술부가 건보심사평가원에 원전종사자 및 주변주민 역학조사연구 대상자 암 발병 수진자료를 요청하여 이를 이용할 수 있도록 조치한 것의 적절성을 판단하기는 어렵다.

(2) 헌혈부적격자로 인한 혈액사고 방지목적으로 헌혈금지 약물 복용자 명단 이용·제공

보건복지부는 2007. 5. 31일 「혈액관리법」 제8조의2(혈액사고발생시 조치 등)에 근거하여 “혈액사고방지조회시스템 구축을 위한 유관기관 임무수행 지침”을 제정(2007.5.31)하고, 국고보조금 531,068,300원을 지원하여, 대한적십자사가 혈액사고방지정보조회시스템을 구축하도록 하였다.

2008. 3. 27일 개최된 제10차 공공기관 개인정보보호심의위원회는 ‘헌혈부적격자로 인한 혈액사고 방지목적으로 헌혈금지 약물 복용자 명단 이용·제공’이 안건으로 상정되었는데, 요양급여심사 목적으로 건강보험심사평가원에서 수집한 ‘헌혈금지 약물복용자 명단’ 자료를 보유목적과 다르게 제공하는 것은 근본적 문제이며, 혈액사고방지 정보조회시스템이 구축되더라도 개인적으로 구입한 약물 적용배제 등 시스템구축 효율성에 의문이 있는 의견이 제출되었고, 위원 공통으로 ‘헌혈금지약물 복용자’ 명단 DB를 별도로 구축하는 것만이 유일한 방법이 아니고, 사전문진과 헌혈참여자에 한해 동의를 받고 건강보험심사평가원에 조회하는 것이 바람직하며, 자료의 현행성을 담보할 수 없어(1주 단위 갱신) 수혈자 보호 목적을 달성하기 어려운데도 헌혈에 동의하지 않은 헌혈금지 약물 복용자의 자료까지 DB화한다는 것은 부당한 개인정보 침해가 우려된다고 지적하였다. 이에 공공기관 개인정보보호심의위원회는 심의요청사항이 「공공기관의 개인정보보호에 관한 법률」 제10조의 법률요건을 충족하지 못하여 부결처리하는 동시에, 사전문진·복약지도를 강화하고, 헌혈참여자에 대해서만 약물복용정보를 조회하는 등 다른 방법을 강구할 것을 권고하였다. 헌혈금지 약물 복용자 명단 일체에 대한 이용·제공이 불가피한 수단이라 인정하더라도 명단의 일체를 이용·제공하는 것은, 헌혈

에 참여하지 않는 일반 국민의 프라이버시권을 침해할 우려가 있다는 것이다(공공기관의 개인정보보호에 관한 법 제10조제3항의 단서조항 요건 불비).

(3) 국민건강보험 직장가입자 자격취득 및 상실정보 이용・제공

국민건강보험 직장가입자 자격 취득 및 상실정보 이용・제공은 두 차례나 공공기관 개인정보보호심의위원회의 심의가 요청되었다. 2009. 1. 19 ~ 21일의 제11차 회의에서는 지방자치단체가 지방세 체납처분을 위해 국민건강보험공단에 대해 '국민건강보험 직장가입자 정보'를 제공받을 수 있도록 심의를 요청한 건에 대해, 2009. 3. 16 ~ 3. 18일의 제12차 회의에서는 공직자윤리위원회가 퇴직공직자 취업제한 위반여부 확인을 위해 심의를 요청한 건에 대해 서면심의가 행해졌다.

우선 지방세 체납처분과 관련하여 살펴보면, 국민건강보험공단은 직장 존재여부, 급여액 등의 자료를 지방자치단체에 제공해왔었으나, 2007년 11월 「공공기관의 개인정보보호에 관한 법률」이 개인정보의 보유목적외 제공시 공공기관 개인정보보호심의위원회의 심의를 거치도록 개정되면서 관련 자료 제공을 중단한 것이 배경이 되었다.

이에 공공기관 개인정보보호심의위원회는 「공공기관의 개인정보보호에 관한 법률」 제10조상 법률요건 적합 여부를 검토한 결과, 해당 자료 미제공시 소관업무 수행가능 여부에 대해서는 '지방세 체납처분' 업무는 「지방세법」이 정한 지방자치단체의 소관업무로, '직장가입자정보' 제공이 재산을 보유하지 않은 체납자에 대한 '지방세 체납처분'의 불가피한 수단이고, 정보주체의 권리와 이익에 대한 부당한 침해 여부에 대해서는 체납처분으로 받는 불이익이 법률이 규정하는 납세의무 미이행시 예측가능한 사항으로, 정보주체의 권리와 이익을 부당하게 침해한다고 볼 수 없으며, 요청자료의 최소 범위 여부 및 제공시 안전성 확보 조치 여부에 대해서는 요청자료가 사업장명, 주소, 전화번호로서 최소한의 범위라 할 수 있고, 자료제공 시 암호화 조치 등을 통해 안전성이 확보될 수 있으므로 자료를 제공할 수 있다고 보았다. 이는 심의위원 9명 중 8명이 찬성하고, 1명이 반대한 결과이다.

<표 2-14> 지방세 체납처분을 위한 건강보험 직장가입자 정보 제공에 대한 의견

| 소 속 | 심의 결과 | 의 견 |
|---|---|---|
| 국가정보원 사이버안전센터장 | 可 | - |
| 방통위 이용자네트웍 국장 | 可 | ◦건강보험공단은 체납자처분을 위해 건보공단의 직장정보가 제공될 수 있음을 홈페이지 공시 및 정보주체에게 정보제공 내역을 반드시 통보 |
| 교과부 평생직업교육국장 | 可 | - |
| 행안부 정보기반정책관 | 可 | ◦지방세체납절차에 필요한 최소한의 정보제공 |
| 고려대 교수 | 可 | ◦'자료요청시'로 되어 있는 정보제공 시기는 적정 주기의 명시가 바람직<br>◦제공자료의 목적달성 후 파기조치 필요 |
| 상명여대 교수 | 可 | ◦자료제공 요청의 이유가 타당성이 높음<br>◦개인정보유출 방지를 위한 보안성 확보 필요 |
| 녹색소비자단체 위원 | 不 | ◦납세의무자의 재산에 대한 압류가 가능하여 급여 압류를 하지 않아도 체납처분이 가능함<br>◦소속직장을 알리는 것은 사생활의 비밀과 자유를 침해하는 것으로 보아야 함 |
| 한국전자통신연구원 소장 | 可 | ◦지방자치단체와 건강보험공단간 처리정보 제공시 암호화조치 및 요청자료 범위 최소화 |
| 법무법인 율촌 변호사 | 可 | ◦정보제공이 없을 경우 체납처분이 현저히 어려울 것으로 판단되며 철저한 보안대책 필요<br>◦조속히 지방세법에 법적근거 마련 필요 |

법제처도 지방자치단체가 체납된 지방세를 징수하기 위해 국민건강보험공단에 과태료 체납자의 직장 정보의 제공을 요청할 경우 건보공단이 이를 거부할 수 있는지 여부를 의뢰한 파주시의 법령해석 요청에 대해 2009년 9월 21일 "체납자의 직장 정보의 제공 자체를 거부할 수 없다"는 회신을 하였다.

하지만 국민건강보험공단이 과태료 체납자 직장가입내역 정보제공 요청을 거부하자, 2009년 10월 13일 파주시는 서울행정법원에 정보제공거부처분 취소소송을 냈다. 지난 2월부터 5월까지 모두 세 차례에 걸쳐 국민건강보험공단 파주지사에 공문을 보내 과태료 체납자 급료를 압류하기 위한 직장가입내역 정보제공을 요청했으나 거부당했다는 것이다. 이에 「질서위반행위규제

법」상 건보공단이 행정청의 정당한 요구를 거부한 것은 법 집행에 대한 협조를 거부하고 공공의 이익보호를 방해한 것이며, 건강보험공단이 임금 압류 등 가입자의 불이익이 예상된다는 이유로 정보제공을 거부하고 있으나 과태료 부과·징수에 필요한 최소한 범위 내에서 정보를 제공할 의무가 있다고 주장한다.[38]

법원이 이 사안에 대해 판결을 내린다면 그 방향이 긍정적이든 부정적이든 지방세 체납처분을 위한 국민건강보험 직장가입자 정보 제공과 관련한 개인정보 공동이용의 문제를 명확하게 하는 계기가 될 것이다. 현재는 행정정보 공동이용과 개인정보 공동이용의 경계가 불분명하기 때문이다.

둘째, 퇴직공직자 취업제한 확인과 관련하여 살펴보면, 국민건강보험공단은 공직자윤리위원회에 퇴직공직자의 직장 정보를 제공해왔으나, 2007년 11월 「공공기관의 개인정보보호에 관한 법률」이 개인정보의 보유목적외 제공시 공공기관 개인정보보호심의위원회의 심의를 거치도록 개정되면서 관련 자료 제공을 중단한 것이 배경이 되었다.

이에 공공기관 개인정보보호심의위원회는 「공공기관의 개인정보보호에 관한 법률」 제10조상 법률요건 적합 여부를 검토한 결과, 해당 자료 미제공시 소관업무 수행가능 여부에 대해서는 '퇴직공직자 취업제한' 업무는 「공직자윤리법」이 정한 공공기관(정부, 대법원, 국회)관할 공직자윤리위원회 소관업무로, '직장가입자정보' 제공이 '퇴직공직자 취업제한 업무'의 불가피한 수단이고, 정보주체의 권리와 이익에 대한 부당한 침해 여부에 대해서는 취업제한 위반여부 확인은 취업제한 관련사항 교육 및 사전안내문을 통해 인지할 수 있고, 취업제한 위반여부 확인을 위해서는 직장가입자정보의 조사를 예상할 수 있기 때문에 정보주체의 권리와 이익을 부당하게 침해한다고 볼 수 없으며, 요청자료의 최소 범위 여부 및 제공시 안전성 확보 조치 여부에 대해서는 요청자료가 사업장명, 사업장등록번호, 직장보험 가입일 및 상실일로서 최소한의 범위라 할 수 있고, 자료제공 시 암호화 조치 등을 통해 안전성이 확보될 수 있으므로 자료를 제공할 수 있다고 보았다. 「공공기관의 개인정보보호에 관한 법률」제10조에 의거한 심의요건을 충족한 것으로 판단한 것이다. 이 또한 심의위원 9명 중 8명이 찬성하고, 1명이 반대한 결과이다.

---

38) 중부일보. 2009.10.14. "파주시 건보공단에 체납자 정보공개 소송."
39) 공직자윤리법의 입법 취지를 구현하기 위해서는 예컨대 해당 공무원의 퇴직시에 ①

<표 2-15> 퇴직공직자 취업제한 확인을 위한 건강보험 직장가입자 정보 제공에 대한 의견

| 소 속 | 심의 결과 | 의 견 |
|---|---|---|
| 국가정보원 사이버안전센터장 | 可 | - |
| 방통위 이용자네트워크국장 | 可 | ◦개인정보의 안전한 관리를 위하여 충분한 보안조치<br>◦공무원 퇴직시 건보공단으로부터 개인정보 일부를 제공받을 수 있음을 고지받을 필요가 있음 |
| 교과부 평생직업교육국장 | 可 | - |
| 행안부 정보기반정책관 | 可 | - |
| 고려대 교수 | 可 | ◦향후, PETI 시스템에서 송·수신 사용하는 암호화 SEED 알고리즘은 표준알고리즘으로 대체가 바람직<br>◦제공자료의 목적달성 후 파기조치 필요 |
| 상명여대 교수 | 可 | ◦요청자료의 최소 범위가 제한적이고 안전성 확보를 위한 조치를 취하는 등의 제반 사항들이 반영되고 있다고 판단됨 |
| 녹색소비자단체 위원 | 不 | ◦퇴직후 2년간 국민연금 납부증명을 제출 또는 국민연금 납부기록조회 동의 등 방법이 존재함에 건강보험정보가 유일한 또는 최우선적 방법이 아님[39]<br>◦건강보험정보는 개인건강기록과 연결된 민감정보로 조회·검색 자체도 개인정보가 누출될 수 있는 본질적 위험성에 해당함 |
| 한국전자통신연구원 소장 | 可 | - |
| 법무법인 율촌 변호사 | 可 | ◦공무집행의 공정성 및 공직자윤리확립의 공익은 큰 반면 퇴직공직자 개인정보제공으로 인한 권리침해는 제한적일 것으로 판단 |

하지만 국민건강보험공단이 보유하고 있는 건강보험정보가 개인건강기록과 연결된 민감한 개인정보라고 할 때, 이러한 공공기관 개인정보보호심의위원

---

해당 퇴직공직자의 경우 퇴직후 정한 기간에 2년간 국민연금납부증명을 제출케 하거나, ② 본인의 국민연금납부기록을 조회하는 것에 동의하는 서면을 작성케 함으로써 사기업이나 사기업관련 기관의 취업여부 및 취업시 사업장을 확인할 수 있을 것이며 이러한 조치는 공무원직무규정이나 시행령을 보완하는 것만으로도 충분하다.

회의 결정은 민감한 개인정보를 보호하기 위해 보유 목적외 이용을 엄격하게 제한해야 한다는 요청을 무시하고, 행정정보 공동이용의 효율성 측면만을 지나치게 강조한 것이라고 할 수 있다. 목적 외 이용을 열어놓은 것 자체가 문제인 것이다.

특히 공직자윤리위원회의 요청과 관련하여 「국민건강보험법」은 “국민의 질병·부상에 대한 예방·진단·치료·재활과 출산·사망 및 건강증진에 대하여 보험급여를 실시함으로써 국민보건을 향상시키고 사회보장을 증진함을 목적”으로 하고 있으므로(제1조), 이를 위해 제공되는 건강보험 관련 개인정보를 「공직자윤리법」에 따른 퇴직공무원의 취업제한 여부 확인에 사용하는 것은 OECD 개인정보보호 가이드라인 8원칙 중 하나인 목적 구체성(purpose specification)의 원칙과 이용제한(use limitation)의 원칙에 위배되는 것이다. 그리고 정보주체가 관련 정보의 조회 및 제공에 동의하지 않았다면 이러한 이용·제공은 정보주체의 개인정보자기결정권을 침해하는 것이기도 하다.

위의 사안에서 나타난 것과 같이 지방자치단체나 공직자윤리위원회가 행정적 편의내지 효율성 제고를 목적으로 국민건강보험공단에 개인정보의 이용·제공 요청을 하는 것이 정당화된다면 대다수 다른 기관들의 행정정보 공동이용 또한 합리화될 가능성이 높다. 국민건강보험공단 또한 스스로 방대한 양의 개인정보를 보유하고 있어 이에 대한 공개 요구로 인해 권한을 남용한 유용 또는 유출 가능성이 내재해 있음을 인정하고 있다(국민건강보험공단, 2009: 98). 공공기관 개인정보보호심의위원회가 「공공기관의 개인정보보호에 관한 법률」 제10조 제3항 제2호에서 ‘처리정보의 보유목적외 이용·제공’ 요건(예외적 제공 요건)의 충족 여부를 검토하도록 한 것은 개인의 민감정보를 편법적으로 활용하는 길을 열어두려는 것이 아니라 ‘처리정보의 보유목적외 이용·제공’을 엄격하게 제한하고자 하는 것임을 명심할 필요가 있다. 물론 이 점은 공공기관 개인정보보호심의위원회가 제대로 역할을 하지 못하고 있음을 보여준다기보다 공공기관 개인정보보호심의위원회를 거칠 경우 목적 외 활용도 용인될 수 있도록 하고 있는 「공공기관의 개인정보보호에 관한 법률」 규정 자체가 문제임을 보여준다고 하겠다.

법률에 근거하여 이루어지기에 법적으로는 문제가 없을지라도 한 기관에서 수집된 정보가 소관업무의 수행 목적이 아닌 경우에도 다른 기관에 폭넓게 제공되고 있는 현실을 감안하면 개인정보의 수집 자체가 엄격하게 행해질 필요가 있다. 그 필요성은 엄청난 개인정보를 다른 기관에 제공하고 있는 국민건강보험공단의 사례를 통해 잘 알 수 있는데, 국민건강보험공단은 2008

년~2009년 8월말까지 각 부서에서 총 733회, 1억 건이 넘는 120,138,454건의 개인정보를 다른 기관에 제공한 것으로 드러났다.[40]

2008년 9월 2일부터 8일에 걸쳐 전국의 성인남녀 1,000명을 대상으로 하여 이루어진 일반인 조사에 따르면, 시민들은 정부의 각 기관들이 자신의 소관업무의 수행을 위하여 수집한 개인정보를 소관업무의 수행목적 이외에 다른 기관에 제공하는 것에 대해 절대 허용 안 된다는 응답이 53.7%, 사전 동의가 있는 경우에만 허용된다는 응답이 33.4%로 부정적인 입장을 보였다.[41] 이러한 입장을 감안한다면, 국민건강보험공단의 개인정보 이용 또는 제공은 좀더 신중해질 필요가 있다.

사실 국민건강보험공단의 개인정보 공동이용에서 더 큰 문제가 되는 것은 공공기관 개인정보보호심의위원회의 심의를 거치지 않고 이루어지는 개인정보 이용·제공 요청이다. 대부분이 공공기관 개인정보보호심의위원회의 통제 범위 밖에 있기 때문이다. 이는 주로 개인정보파일 관리에 관한 사항이라고 할 수 있는 데, 그 수집·유통 실태는 아래에서 따로 논한다.

## 3. 개인정보파일의 수집·유통 실태

### 1) 개인정보파일의 수집 및 보유

공공기관이 소관업무 수행을 위해 보유하는 개인정보파일에 대한 종합적인 사항을 일정한 양식에 따라 기록한 장부인 개인정보파일대장은 개인정보취급자 별로 직접 작성하여 보관해야 하는데, 개인정보파일을 신규 보유하게 되거나 다른 기관으로부터 제공받아 보유하는 경우에 작성하되, 1개의 개인정보파일에 대해 1개의 개인정보파일대장을 작성해야 한다. 「공공기관의 개인정보보호에 관한 법률」 제6조제3항에 해당하는 개인정보파일 보유 사전협의 제외 대상은 대장작성에서 제외한다(행정안전부, 2009d: 5).

개인정보파일의 보유기간은 전체 데이터가 아닌 개별 데이터의 보유부터 삭제까지의 생애주기로서 보유목적에 부합된 최소 기간으로 산정해야 하며, 보유기간 산정은 □'개별법령의 규정'에 명시된 자료 보존기간에 따르거나,[42] □

40) 이에 대한 구체적인 내용은 본 연구 제2장 제5절 참고.

41) 그러나 정부기관이 수집한 개인정보를 수사기관에 제공하는 것에 대해서는 15.8%가 절대 허용이 안 된다고 응답하여 보다 수용적인 입장을 보였다.

42) 주민등록 관계 서류는 「주민등록법 시행령」 제60조에 따라 보존기간이 정해져 있다.
1. 세대별·개인별 주민등록표: 영구

개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우 개인 정보 총괄 부서의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 정책고객, 홈페이지 회원 등의 홍보 및 대국민서비스 목적의 외부고객명부의 경우 특별한 경우를 제외하고 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속 보유할 수 있다.[43] 보유기간은 「공공기록물 관리에 관한 법률 시행령」에 따른 기록물의 보존기간별 책정기준 및 기록관리기준표를 상회할 수 없다(행정안전부, 2009d: 4-5). 그리고 보유기간 내에서 개별 데이터에 대한 삭제변경 요청이 가능함을 명시하여야 한다. 단, 다른 법률에서 영구보유를 하게 하는 경우는 해당 법률을 반드시 함께 명시하여 공개한다.

문제는 해당 법률이 쓸모가 없어진 개인정보파일을 보관하도록 하고 있을 경우이다. 로또 복권 당첨자 파일, 이미 끝난 근로복지공단의 근로복지복권파일, 산림공제조합(산림청 등)에서 보관하고 있는 녹색복권, 추첨식 파일 등은 사실상 영구 보존 파일이라고 할 수 있는데, 이는 「복권 및 복권기금법」 제33조 (복권에 관한 자료의 보존의무)에서 “복권사업자는 복권의 발행·관리 및 판매에 관한 서류·장부 등을 5년 이상 보존하여야 한다”고 규정하고

---

2. 말소된 세대별·개인별 주민등록표: 영구
3. 주민등록번호 부여대장 및 주민등록번호 조립부: 영구
4. 주민등록증 발급대장 및 주민등록증 발급신청서: 영구(주민등록증 발급신청서는 대상자가 사망한 경우에는 파기)
5. 국외이주신고서 접수대장: 10년
6. 주민등록증의 습득·회수·파기대장: 5년
7. 주민등록지 통보 관계 서류: 5년
8. 주민등록사항 신고 관계 서류: 5년(다만, 전입신고서는 10년으로 한다)
9. 사실조사 및 직권조치 관계 서류: 5년
10. 과태료 부과·징수 관계 서류: 5년
11. 주민등록번호 정정 관계 서류: 5년
12. 세대명부, 주민등록 전출자 명부 및 주민등록 전입자 명부: 5년
13. 제4호 외의 주민등록증 발급 관계 서류: 5년
14. 주민등록 및 주민등록증 발급상황 보고 서류: 5년
15. 직권정리 및 일일처리 결산 관계 서류: 5년
16. 주민등록표 이송 관계서류: 5년
17. 이의신청 관계 서류: 3년
18. 주민등록표 열람 및 등·초본 교부대장: 3년
19. 전산자료 이용·승인대장: 3년
20. 제8호 외의 통지서 및 공고 관계 서류: 3년
21. 국외이주(현지이주) 통보 관계 서류: 3년
22. 다른 읍·면·동 거주자 주민등록증 주소변경대장: 3년
23. 주민등록사항의 진위확인 신청 관계 서류: 3년
24. 주민등록표의 열람 및 등·초본 교부신청 관계 서류: 3년

43) 예를 들면, 정책고객관리매뉴얼 상 6개월 이상 비활동자 삭제(00 기관).

있어서 당첨자 파일도 5년 이상, 영구적으로 보존해도 아무런 문제가 없기 때문이다. 하지만 이미 쓸모가 없는 개인정보 파일들을 보관할 경우 문제가 생길 수밖에 없다. 불필요한 파일은 우선 파기해야 개인정보 유출, 근거 없는 제공, 불법도용 등의 문제가 발생하지 않을 것이다(유정현, 2008: 7).

개인정보파일의 입출력 관리를 위한 입출력자료관리대장의 경우 개인정보를 생성 처리하는 부서에서 기록하고 관리해야 하나, 해당 개인정보보호 총괄부서에서도 주기적으로 현황 관리를 할 필요가 있다.

공공기관의 개인정보 보유는 그 수집 및 관리에서 적정해야 함에도 불구하고 개인정보의 보유 기관과 보유파일 수는 지속적으로 증가하고 있으며, 이에 따른 개인정보의 유출 가능성 또한 증가하고 있다. 현재 「공공기관의 개인정보보호에 관한 법률」 제10조의2에 의거하여 관보 또는 인터넷에 매년 게재하고 있는데, 2008년 전수조사 결과에 따르면, 공공기관은 약 32만 건의 개인정보파일을 보유하고 있는 것으로 조사되었다. 여기에는 「공공기관의 개인정보보호에 관한 법률」 제3조제2항에 따라 「통계법」 및 국가안전보장과 관련된 정보 분석을 목적으로 수집되는 개인정보 및 동법 제6조제3항에 따른 개인정보파일은 공개되지 않아 일반인의 열람대상에서 제외되고 행정안전부장관의 공고대상에서도 제외되는 것을 감안하면, 실제 작성·활용되는 개인정보파일은 당연히 통계수치보다 많을 것이다. 또한 개인정보파일에 담기는 정보는 성명, 주민등록번호, 주소는 기본이고, 파일마다 차이는 있지만, 연락처(전화번호, 휴대전화번호, 이메일주소, 팩스번호), 종교, 학력, 경력, 병역사항, 직장정보(직업, 직급, 근무지 등), 각종 등록번호 또는 면허번호, 각종 변동내역, 진료정보(질병명, 진료내역, 처방전 내용, 접종기록 등), 보호자나 친족에 대한 정보, 결혼여부, 계좌번호, 상담내용, 민원처리내역, 각종 세금 납부내역 등이 포함되어 있다. 이렇게 형성한 개인정보파일의 일부는 공공기관 상호간, 혹은 공공기관과 금융기관이 공동이용할 것이 의무화되는 정보로 분류되어 활용되고 있다(성낙인 외, 2008: 209).

이 중 파일 약 8만1천여 개를 유정현 의원실에서 분석한 결과에 따르면, 보유 파일의 양태도 문제가 심각한 것으로 드러났다. 뚜렷한 이유 없이 영구 및 준 영구 보존하고 있고, 주민등록번호는 관행처럼 대부분 수집하고 있는 것이다. 만약 영구보존 파일 15,406개(19%)와 보존기간이 거의 영구인 준영구 파일 24,638개(30.4%) 등 총 약 4만 개(전체의 49.4%)의 파일이나, 주민번호가 포함된 파일 60,693개(74.9%)가 제대로 관리가 안 된다면 언젠가 유출, 도용, 불법 제공될 것이라는 점에서 문제가 심각하다(유정현, 2008: 6).

현재 영구, 혹은 준영구적으로 보존하도록 되어 있는 개인정보파일에 대해 보존기간이 적절한 것인지 해당 영역의 전문가들의 검토가 필요하다. 또한, 현재 각 기관에게 개인정보 정보를 제공하거나, 개인정보를 제공받을 수 있도록 규정하고 있는 법률에서는 해당 정보의 적절한 보유기간, 그리고 보유 목적 달성 시 폐기의무를 규정해야 한다.

개인정보 총괄부서는 입출력관리대장, 개인정보파일대장 등에 대한 보유(이용・제공을 포함)・파기현황을 주기적으로 조사하여 그 결과를 기관 홈페이지의 개인정보보호방침에 포함하여 공개 관리해야 한다.

<표 2-16> 개인정보 보유 기관수 및 보유 파일 수

| 연도 | 구분 | 보유 기관수 | 보유 파일종류 | 보유 파일 수 |
|---|---|---|---|---|
| 05년 | 계 | 1,095 | 1,078 | 10,510 |
| | 중앙행정기관 | 56 | 235 | 326 |
| | 지방자치단체 | 250 | 377 | 8,703 |
| | 교육청 및 각급학교 | 603 | 61 | 1,004 |
| | 정부투자기관 및 기타 | 186 | 405 | 477 |
| 06년 | 계 | 11,748 | 1,144 | 28,081 |
| | 중앙행정기관 | 87 | 277 | 407 |
| | 지방자치단체 | 286 | 397 | 9,264 |
| | 교육청 및 각급학교 | 11,189 | 67 | 17,935 |
| | 정부투자기관 및 기타 | 186 | 403 | 475 |
| 07년 | 계 | 20,315 | 1,360 | 92,855 |
| | 중앙행정기관 | 84 | 309 | 445 |
| | 지방자치단체 | 250 | 510 | 40,960 |
| | 교육청 및 각급학교 | 19,683 | 102 | 50,896 |
| | 정부투자기관 및 기타 | 298 | 439 | 554 |
| 08년 | 계 | (조사기관수)23,654 | | 323,566 |
| | 중앙행정기관 | 481 | | 2,753 |
| | 지방자치단체 | 1,825 | | 46,033 |
| | 교육청 및 각급학교 | 20,666 | | 269,631 |
| | 기타 공공기관 | 680 | | 5,149 |

자료: 유정현(2008); 행정안전부(2008e) 보완.

중앙행정기관, 광역자치단체, 시도교육청 등 최상위기관은 하위(하급)기관의 보유・파기현황을 주기적으로 조사하여 관리해야 하며, 전국 단일의 공통업무를 집행하고 있는 특별지방행정기관, 지방자치단체, 교육기관(학교 포함)이 소속된 최상위기관은 하위(하급)기관의 '개인정보파일 표준목록'을 함께

관리해야 한다. 행정안전부는 매년 전 공공기관의 개인정보파일 보유현황을 조사하여 관보에 관련 내용을 공고하며, 중앙행정기관, 광역자치단체, 시도교육청 등 행정계층별 최상위기관은 행안부 요청에 따라 하위(하급), 산하기관에 대한 보유 및 파기현황 제출에 협조해야 한다(행정안전부, 2009d: 7).

'08년 전수조사 결과 국가행정기관에서 가장 많이 가진 개인정보는 개인속성정보와 기본식별정보로 나타났으며, 개인속성정보 중에서는 성명, 주소, 전화번호, 기본식별정보 중에서는 주민등록번호, 휴대폰번호, 이메일 주소를 가장 많이 보유하였다. 그리고 국가행정기관에서는 사회보장, 의료정보, 법 위반정보, 기타 민감정보 등을 포함한 다양한 개인정보를 보유하여 처리하는 것으로 나타났다.[44] 교육기관에서 가장 많이 보유하고 있는 개인정보의 유형은 개인속성정보였으며, 성명, 전화번호, 주소, 성별, 생년월일, 세대원 정보, 연령의 순으로 많이 보유하고 있었다(행정안전부, 2008e: 5-11).

본 연구의 실태조사를 통해서도 개인정보파일과 관련된 문제점들이 곳곳에서 발견되었다. CCTV와 관련된 개인영상정보파일의 경우 개인정보파일 목록에 포함되어 있은 경우가 많았고, 경찰청은 범죄정보관리시스템에 대한 정보가 행정안전부에서 공고하는 개인정보파일목록집에 포함되지 않았으며, 개인정보파일대장도 작성하지 않는다고 밝혔다. 국립대학의 병원 및 민간 병원 등의 경우에도 국립병원 등과는 달리 어떠한 개인정보파일을 보유하고 있는지, 어떤 개인정보를 기록하고 있는지 공개하고 있지 않았다. 그리고 각 병원의 개인정보파일목록 및 홈페이지에 공개된 정책에서 수집 근거가 다르게 명시된 곳이 있었고, 개인정보파일목록과 홈페이지에 공개된 정책에 명시된 법적 근거가 다른 곳도 있었다.[45]

한편, '08년 전수조사 결과 공공기관이 개인정보를 수집하는 방법으로는 개인의 신청서 등을 통한 오프라인 수집이 62.5%로 가장 많았으며, 업무시스템의 연계에 의한 개인정보의 수집이 37.8%, 온라인 수집이 16.2% 순이었다. 기관유형별로 보면, 국가행정기관만이 오프라인 수집보다는 온라인으로 수집하는 정도가 더 많은 것으로 나타났다(행정안전부, 2008e: 13).

### 2) 개인정보파일의 이용 및 제공

---

44) 광역자치단체도 보유현황이 이와 비슷하나, 기본식별정보의 경우에는 성명, 주소, 전화번호, 연령의 순으로 많이 보유하고 있었다. 그리고 기초자치단체에서 가장 많이 보유하고 있는 개인정보의 유형은 개인속성정보였으며, 의료정보 및 인종과 민족, 종교, 노조가입 등의 기타 민감 정보에 대해 광역자치단체보다 더 다양하게 보유하고 있었다.

45) 자세한 내용은 제2장 제5절 참고.

개인정보파일은 다른 '법률'에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보가 이용되거나 제공되어서는 아니 된다(「공공기관의 개인정보보호에 관한 법률」 제10조 제1항). 보유정보에 대해 다른 기관이 이용·제공을 요청한 경우 개별 법령의 근거 규정을 확인하여 '처리정보이용제공대장'에 기록하여 제공해야 한다. 보유정보를 다른 기관에 제공하고자 할 때에는 문서를 통해 보유목적, 범위 등을 확인하여야 하는데, 최소한의 범위로 제한하여 제공하고, 보유기관의 동의 없이 제3자에게 이용·제공할 수 없도록 조치해야 한다(행정안전부, 2009d: 5-6).

다만, 「공공기관의 개인정보보호에 관한 법률」 제10조 제3항에 해당하는 경우에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보가 이용되거나 제공될 수 있다. 물론 이 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다. 제공시에는 해당 법률을 반드시 명시해야 한다.

행정안전부가 2008년 실시한 공공기관 보유 개인정보파일 전수조사 결과에 따르면, 전체 보유 개인정보파일 중 15.2%의 파일에서 개인정보를 제공하는 것으로 조사되었다. 국가행정기관(특히 소속기관)에서 제공하는 경우가 가장 많았고, 개인속성정보와 기본식별정보의 제공이 가장 많았다. 교육기관의 경우 민감정보(국적, 인종, 종교, 본적 및 출신지)에 대한 다른 기관 제공이 상대적으로 많았으며, 제공근거의 경우 법률에 의한 제공이 가장 많았으나, 일부 업무상 필요에 의한 제공(2.8%), 제공근거 없음(0.5%), 업무지침 혹은 계획(0.8%) 등의 응답도 있었다. 기타 공공기관과 시·군·구에서 제공근거 없이 제공한다는 응답이 많이 나왔다.

또한 문서를 통한 이용·제공이 이루어지고 있는가에 대해 38.6%만이 잘되고 있다고 응답하였다. 문서를 통한 이용·제공이 잘 되지 않는 것 같다는 응답은 국가행정기관의 경우 소속기관과 기타 공공기관, 지방자치단체의 경우 광역자치단체, 교육기관의 경우 초·중·고등학교와 기타 교육기관의 담당자들 중에 많았다.

그리고 개인정보파일은 처리정보이용제공대장에 기록하여 관리해야 하는데, 2008년 전수조사 결과에 따르면, 처리정보이용제공대장 관리와 관련하여 31.5%만이 잘되고 있다고 응답하였다. 국가행정기관의 소속기관과 기타 공공기관, 대학, 기타 교육기관에서 잘 되지 않는다는 응답이 많았다.

### 3) 개인정보파일의 파기

개인정보파일의 보유 목적 달성 등 해당 개인정보파일의 보유가 불필요하게 된 경우 해당 개인정보파일을 지체 없이 파기해야 하며, 개인정보처리부서의 장은 해당 파기사항에 대해 입출력자료관리대장에 개인정보파일명과 주요기록항목, 폐기일, 처리담당자성명, 처리부서장을 기재하여 관리해야 한다. 다만, 다른 법령에 따라 보존이 필요한 경우 파기하지 않을 수 있다.

보유하고 있는 개인정보파일의 파기는 복구할 수 없는 기술적 방법을 이용하여 원본 및 백업본을 파기해야 하며, 다수가 공동 이용하는 데이터베이스 형태의 개인정보파일은 '행정정보데이터베이스 표준화지침'[제2008-47호, 행정안전부고시, 2008.11.25]의 폐기절차에 따라 조치해야 한다(행정안전부, 2009d: 9). 「기업의 개인정보 영향평가 수행을 위한 가이드」에서도 전자적으로 기록되어 있는 개인정보를 파기할 때에는 다시 재생할 수 없는 기술적 방법으로 삭제하거나 개인정보가 기록된 매체를 물리적으로 분쇄 또는 소각하여야 한다고 권고하고 있다(정보통신부・한국정보보호진흥원, 2005: 43).

공공기관이 보유하고 있는 개인정보파일을 파기할 경우, 개인정보취급부서는 그 사실을 즉시 개인정보 총괄부서에 통보하여야 하며, 개인정보 총괄부서는 파기현황을 매월 조사하여 그 결과를 관보 또는 홈페이지에 공고해야 한다. 하지만 이러한 사항이 제대로 이행되지 않아서 파기된 파일 현황은 파악되지 않고 있는 상황이다. 유정현 의원이 몇 개 산하기관을 샘플링해서 대조해 본 결과 관보에 게재되지 않은 것도 상당한 것으로 드러났다(유정현, 2008: 6-7). 2008년 전수조사 결과에 따르면, 보유하고 있는 개인정보파일 파기 사실에 대한 공고에 대해 전체 응답자의 13.2%만이 잘된다고 응답하였으며, 기관 유형의 차이 없이 대부분의 기관에서 파기사실에 대한 공고가 잘 안되는 것으로 나타났다.

### 4) 개인정보파일의 열람 및 정정・삭제 청구권 보장 실태

본인에 관한 처리정보의 열람은 개인정보파일대장에 기재된 범위 안에서 정보주체인 본인(대리인 포함)만 가능하며, 타인의 정보는 열람할 수 없다. 따라서 개인정보파일의 열람 및 정정・삭제 청구권은 개인정보파일대장에 기재된 범위 안에서 그 행사가 한정된다.[46]

문제는 개인정보파일 목록 자체가 공개되지 않는 경우가 많다는 점이다.

---

46) 공공기관의 개인정보보호에 관한 법률
제12조 (처리정보의 열람) ①정보주체는 개인정보파일대장에 기재된 범위안에서 문서로 본인에 관한 처리정보의 열람(문서에 의한 사본의 수령을 포함한다. 이하 같다)을 보유기관의 장에게 청구할 수 있다. <개정 2007.5.17>

개인정보파일 목록이 공개되지 않는다면, 그에 대한 열람 및 정정·삭제 청구권도 제한받을 수밖에 없다. 물론 정보주체가 개인정보파일의 열람 청구권을 행사하려 할 때 각 기관의 개인정보파일대장 공개 여부와 무관하게 열람이 가능할 수도 있다. 그러나 정보주체의 권리 행사를 위하여 개인정보파일 대장에 대한 작성과 더불어 그 이용사실에 대한 공개가 보다 적극적으로 이루어질 필요가 있다. CCTV를 통해 확보되는 개인화상정보 파일의 경우가 그 대표적인 예인데, 정보주체가 자신의 개인정보가 CCTV에 의해 처리·이용되는지 여부를 알기 어려우면 개인에게 보장된 자신의 열람 및 정정·삭제 청구권을 의미 있게 행사하기 어렵다.[47]

경찰청에 수사자료표 외에 범죄정보관리시스템(CIMS) 및 영상판독시스템 내 개인정보 입력내용을 열람 청구한 결과 영상판독시스템에 대해서는 비공개결정이 났다. 이에 대해 이의신청을 했는데 경찰청은 기각 결정을 내렸다. <그림 2-2>의 영상판독시스템 내 개인정보 입력내용에 대한 열람 청구 이의신청(기각)결정통지서를 보면, 정보공개심의회 심의결과 "「공공기관개인정보보호법」 제12조제1항은 '정보주체가 개인정보파일대장에 기재된 범위 안에서 문서로 본인에 관한 처리정보의 열람을 청구하도록 하는 규정'으로서 그 대상은 동법 제8조에 따른 '개인정보파일대장 작성'을 전제로 하고 있으나, 채증영상판독시스템 자료는 동법 제6조제3항제2호의 '범죄의 수사, 공소의 제기 및 유지 등에 관한 자료'로서, 이는 동법 제8조에 의해 '개인정보파일대장' 작성의 대상이 되지 않는 개인정보파일에 해당하므로 정보주체의 열람대상이 되지 않음"이라고 적시하고 있다. 개인정보파일 목록에 포함되지 않는다는 사실이 정보주체의 열람대상이 되지 않는 근거가 되고 있는 것이다.

개인정보파일대장은 법 제8조에 의해 개인정보 보유기관이 작성하여 일반인이 열람할 수 있도록 원칙적으로 공개하게 되어 있는데, 개인정보파일대장이 공개되지 않을 경우 정보주체의 열람 및 정정·삭제 청구권 또한 제한을 받는 결과로 이어지는 것이다. 여기서 지적해야 할 것은 개인정보파일대장의 작성과 공개 의무에서 포괄적인 예외가 인정되고 있다는 사실이다. 국가의 안전 및 외교상의 비밀 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일, 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보파일, 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보파일의 경우가 그렇다(동법 제6조제3항).

---

47) 이와 관련된 내용은 제3장 제1절 참고.

<그림 2-2> 영상판독시스템 내 개인정보 열람 청구 이의신청(기각)결정통지서

[redacted]

인쇄일자 : 2009.08.20

# 이의신청(기각)결정통지서

수 신 자 [redacted]

| 접 수 일 자 | 2009.08.05 | 접 수 번 호 | [redacted] |
|---|---|---|---|
| 이의신청내용 | - 영상판독시스템 내 본인에 관한 개인정보 입력내용에 대한 열람 청구에 대하여<br>- 귀 청은 [정보공개법] 제9조 1항의 비공개대상 정보라는 이유로 비공개 결정을 내렸습니다.<br>- 이러나 어번 열람청구는 [공공기관의 정보공개에 관한 법률]에 의한 것이 아니라 [공공기관의 개인정보보호에 관한 법률](개인정보보호법)에 의한 것이었고,<br>- 현행 개인정보보호법 제13조에 따르면 정보주체에게 자신에 대한 개인정보의 열람을 제한할 수 없습니다. 이 점은 [공공기관의 개인정보파일 관리지침](행정안전부, 2009)에서도 [공공기관이 보유하고 있는 개인정보파일의 경우는 처리정보의 당사자인 정보주체에게 열람을 제한할 수 없음]이라고 명시되어 있습니다.(10쪽)<br>- 이에 귀청의 불법적인 비공개 결정에 대하여 이의를 제기하며 본인 정보에 대한 열람을 다시한번 청구하는 바입니다. | | |
| 비공개(전부 또는 일부)내용 및 사유 | 1. 근거 : 공공기관의 정보공개에관한 법률 제18조<br>2. 사유<br>귀하의 이의신청에 대해 '09.08.13. 정보공개심의회 심의결과 아래와 같은 사유로 이의신청이 기각되었음을 알려드리오니 양지하여 주시기 바랍니다<br><br>○ 첫째,「공공기관의 개인정보 보호에 관한법률」제12조제1항은 '정보주체가 개인정보파일대장에 기재된 범위 안에서 문서로 본인에 관한 처리정보의 열람을 청구하도록 하는 규정' 으로서 그 대상은 同法 제8조에 따른 '개인정보파일대장 작성' 을 전제로 하고 있음<br>- 그러나, 채증영상판독시스템 자료는 同法 제6조제3항제2호의 '범죄의 수사, 공소의 제기 및 유지 등에 관한 자료' 로서, 이는 同法 제8조에 의해 '개인정보파일대장' 작성의 대상이 되지 않는 개인정보파일에 해당하므로 정보주체의 열람대상이 되지 않음<br>○ 둘째, 채증영상판독시스템內 있는 채증자료는「공공기관의 정보공개에 관한법률」제9조제1항제4호에 의해 범죄의 수사, 공소의 제기 및 유지 등에 관한 사항으로서, 공개할 경우 그 직무수행을 현저히 곤란하게 할 우려가 있어 비공개 대상정보에 해당함<br>○ 셋째, 채증영상판독시스템內 자료는<br>- 경찰청 내부규칙에 따라 신원이 확인된 자료는 수사기능에 통보후 폐기하고, 신원 미확인 자료는 공소시효 기간만 보관후 폐기하고 있음<br>- 따라서, 신청인들이 기히 신원확인되어 사법처리 되었을 경우에는 열람할 자료가 없을 뿐만 아니라<br>- 신청인들에 대한 자료 유무를 확인하기 위해 보유중인 모든 신원 미확인 자료를 열람하는 것은 타인의 개인정보 침해가 우려됨 | | |

그러나 개인정보파일대장에 포함되지 않았다는 사유로 정보주체의 열람 및 정정·삭제 청구권을 제한하는 것은 개인정보에 대한 정보주체의 권리를 부당하게 제한하는 것이다. 정보주체가 자신에 관한 정보에 접근하여 그 열람 및 정정·삭제를 청구할 수 있는 권리의 보장 여부가, 자신의 정보가 개인정보파일대장에 기재되어 있느냐라는 형식적인 차이에 따라 좌우되는 것은 「공공기관의 개인정보 보호에 관한 법률」의 제정 목적과도 맞지 않는다. 법 제1조에서는 “이 법은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다.”고 명시되어 있다.

열람을 위해서는 개인정보에 대한 열람을 청구할 수 있는 열람창구를 지정하고 기관홈페이지의 개인정보보호방침을 통해 공지해야 한다. 통합 열람창구를 운영할 경우 개인정보 총괄부서 또는 민원부서가 적합하다. 열람창구에는 정보주체가 열람을 요청할 수 있도록 개인정보 열람청구서를 비치하며 열람청구를 받은 때에는 10일 이내에 조치해야 한다(행정안전부, 2009d: 7).

공공기관이 보유하고 있는 개인정보파일의 경우는 처리정보의 당사자인 정보주체에게 열람을 제한할 수 없다. 그러나 「공공기관의 개인정보보호에 관한 법률」 제13조에 해당하는 아래의 사항은 열람을 제한할 수 있다.

- 조세의 부과·징수 또는 환급에 관한 업무, 「초·중등교육법」 및 「고등교육법」에 따른 각급학교와 「평생교육법」에 따른 평생교육시설에서의 성적의 평가 또는 입학자의 선발에 관한 업무, 학력·기능 및 채용에 관한 시험, 자격의 심사, 보상금·급부금의 산정 등 평가 또는 판단에 관한 업무, 다른 법률에 의한 감사 및 조사에 관한 업무로서 당해 업무의 수행에 중대한 지장을 초래하는 경우
- 개인의 생명·신체를 해할 우려가 있거나 개인의 재산과 기타의 이익을 부당하게 침해할 우려가 있는 경우
- 그밖에 다른 법률에서 정보주체에 대한 열람제한이 명시되어 있는 경우: 토지 및 주택 등에 관한 부동산 투기를 방지하기 위한 업무, 불공정 증권 거래를 방지하기 위한 업무

이와 같이 열람제한을 결정한 경우에는 “열람제한결정서”를 청구인에게 통지해야 한다(행정안전부, 2009d: 8).

개별 개인정보에 대한 변경 또는 수정사항, 보유기간 만료 등 보유 불필요,

삭제 청구가 발생되었을 때는 이를 반영하여 관리해야 한다. 개인정보를 열람한 정보주체(대리인 포함)가 본인의 처리정보에 대하여 정정 및 삭제를 청구한 경우 즉시 조치해야 하는데, 열람 장소에 '정정·삭제청구서'를 함께 비치하여 정보주체의 청구 시 정당한 사유가 없는 한 10일 이내에 조치해야 한다. 개인정보를 삭제할 경우 재사용이 불가능하도록 영구 삭제해야 한다.

이 때 개인정보파일의 보유기관은 정보주체의 청구가 있어도 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있어 이를 보유해야 하는 경우 정정 또는 삭제 청구를 거부할 수 있는데, 삭제청구에 대한 제한 사유가 발생한 경우 결정의 내용 및 사유와 당해 결정에 대한 불복절차에 관한 사항을 기재한 '정정·삭제 거부 등 결정통지서'를 청구인에게 송부해야 한다(행정안전부, 2009d: 8-9).

## 4. 소결

행정기관간 개인정보의 수집·유통 실태를 보면, 개인정보의 이용 및 제공과 관련해서는 현재 개인정보의 목적 외 이용 또는 제공을 제대로 검토하는 것이 아니라 오히려 논란의 여지가 있는 사안들을 정당화해주는 역할을 하고 있는 공공기관 개인정보보호심의위원회의 역할이 강화될 필요가 있음을 알 수 있었다.

그리고 공공기관 개인정보보호심의위원회의 심의를 거치지 않고 이루어지는 개인정보 이용·제공 요청이 개인정보 공동이용에서 더 큰 문제가 되는데, 이는 주로 개인정보파일 관리에 관한 사항이어서 이에 대한 수집·유통 실태를 살펴보았다. 2008년 공공기관이 보유한 개인정보 파일을 전수 조사한 결과 2008년 말 현재 2만3652개 기관에서 총 32만2357개 파일을 보유하고 있는 것으로 나타났다.[48] 이 중 일반인의 열람대상에서 제외되고 행정안전부 장관의 공고대상에서도 제외되고 있는 개인정보파일을 감안하면, 실제 작성·활용되는 개인정보파일은 당연히 통계수치보다 많을 것이다. 이 중에서 15.2% 정도가 개인정보를 제공하고 있고, 제공근거 없이 이를 제공하는 경우도 있었는데, 공공기관이 보유하고 있는 개인정보파일의 파기 현황이 제대로 파악되지 않고 있어 문제가 되고 있음이 밝혀졌다. 이는 정부가 공공부문의 개인정보 보호에 대해 별다른 관심을 갖고 있지 않으며, 민감한 개인정보가 무방비로 노출될 우려가 높다는 사실을 반증한다.

48) 동아일보. 2009.7.9. "구멍뚫린 IT강국… 공공기관 67% 정보보호 전담직원 全無."

# 제2절 수사/범죄경력(경찰) 영역

2008년 경찰청에서 공개한 개인정보파일대장은 11개로서, △마이페이지회원파일, △뉴스레터신청파일, △인터넷명예경찰관회원파일, △운전면허정보(운전면허마스터, 운전면허종별내역), △운전면허행정처분내역, 위반·사고벌점내역, △운전면허결격정보(운전면허응시제한내역, 결격내역), △교통법규 위반자과태료 및 통고처분정보, △무인단속카메라에 의한 단속정보(과속, 신호위반), △자동차운전기능검정원 강사정보, △자동차운전학원교육생정보, △정책고객파일 등 주로 인터넷 홈페이지 운영과 운전면허 및 교통단속에 집중되어 있다. 경찰은 일차적인 범죄수사기관으로서 수사 및 범죄 경력과 관련한 자료를 생성하고 관리하고 있지만 그 실태에 대해서는 잘 알려져 있지 않다.

이는 범죄의 수사에 관한 사항을 기록한 개인정보파일의 경우 「공공기관의 개인정보보호에 관한 법률」(이하 「공공기관개인정보보호법」)에서 규정한 여러 의무에서 포괄적으로 예외를 인정하는데 따른 것으로 보인다. 「공공기관개인정보보호법」에서는 개인정보 수집에 대한 안내, 개인정보파일의 보유·변경시 사전협의, 공고, 대장의 작성과 일반인 열람 등에 대한 의무를 규정하고 있지만, 제6조제3항제2호 '범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보파일'은 이러한 의무에서 예외가 인정되고 있다.

「공공기관의 개인정보보호에 관한 법률」
제4조 (개인정보의 수집)
②공공기관의 장은 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서(「전자정부법」 제2조제5호에 따른 전자문서를 포함한다. 이하 같다) 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여야 한다. 다만, 제6조제3항 각 호의 어느 하나에 해당하는 개인정보파일을 보유할 목적으로 개인정보를 수집하는 경우에는 그러하지 아니하다.

제6조 (개인정보파일의 보유·변경시 사전협의 <개정 2007.5.17>) ①공공기관의 장이 개인정보파일을 보유하고자 하는 경우(다른 공공기관으로부터 처리정보를 제공받아 보유하고자 하는 경우를 제외한다)에는 다음 각 호의 사항을 행정안전부장관과 협의하여야 한다. 다음 각 호의 어느 하나에 해당하는 사항을 변경하고자 하는 경우에도 또한 같다. <개정 1999.1.29, 2007.5.17, 2008.2.29>
1. 개인정보파일의 명칭

2. 개인정보파일의 보유목적
3. 보유기관의 명칭
4. 개인정보파일에 기록되는 개인 및 항목의 범위
5. 개인정보의 수집방법과 처리정보를 통상적으로 제공하는 기관이 있는 경우에는 그 기관의 명칭
6. 개인정보파일의 열람예정시기
7. 열람이 제한되는 처리정보의 범위 및 그 사유
8. 그 밖에 대통령령이 정하는 사항
③제1항의 규정은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 이를 적용하지 아니한다. <개정 2007.5.17>
1. 국가의 안전 및 외교상의 비밀 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 조세범처벌법에 의한 조세범칙조사 및 관세법에 의한 관세범칙조사에 관한 사항을 기록한 개인정보파일
4. 삭제 <2007.5.17>
5. 삭제 <2007.5.17>
6. 보유기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
7. 삭제 <2007.5.17>
8. 그 밖에 이에 준하는 개인정보파일로서 대통령령이 정하는 개인정보파일

제8조 (개인정보파일대장의 작성) 보유기관의 장은 제6조제3항 각 호에 따른 개인정보파일을 제외하고는 당해 기관이 보유하고 있는 개인정보파일별로 제6조제1항 각 호에 따른 사항을 기재한 대장(이하 "개인정보파일대장"이라 한다)을 작성하여 일반인이 열람할 수 있도록 하여야 한다. [전문개정 2007.5.17]

수사 및 범죄 경력은 민감한 개인정보로서 그 수집 목적을 벗어나 이용되거나 제공될 경우 개인의 기본적 인권을 현저하게 침해할 우려가 있다. 실제로 국가인권위원회에는 전과를 이유로 한 인권 침해에 대하여 다수의 진정이 제기되어 왔으며, 일부 사례의 경우 인권침해가 인정되기도 하였다.[49] 수사 및 범죄 경력에 대한 사항은 「공공기관개인정보보호법」과 별도로 「형의 실효 등에 관한 법률」에서 규정하고 있다.

이 절에서는 경찰이 수사자료표를 생성, 조회, 정리(삭제)하는 과정에서 개인정보가 수집, 유통되는 현황과 정보주체의 열람 및 정정·삭제 청구권 보장에 대해 살펴보았다. 다른 한편으로 경찰이 수사자료표와 별도로 구축하는 범죄정보관리시스템에 대해서도 검토하였다.

---

49) 국가인권위원회. 2003.1.27. 02진차47 결정; 국가인권위원회. 2006.11.13. 06진차530, 06진차564 병합 결정 등.

# I. 수사자료표

## 1. 개요

수사자료표란 “수사기관이 피의자의 지문을 채취하고 피의자의 인적사항과 죄명 등을 기재한 표(전산입력되어 관리되거나 자기테이프, 마이크로필름 그 밖에 이와 유사한 매체에 기록·저장된 표를 포함한다)로서 경찰청에서 관리하는 것”을 말한다. 수사자료표에는 피의자의 인적사항, 죄명, 입건관서, 입건일자, 처분·선고결과 등 수사경력 또는 범죄경력에 관한 사항을 기재한다.

수사자료표 중 벌금이상의 형의 선고·면제, 선고유예, 보호감호, 치료감호, 보호관찰, 선고유예실효, 집행유예취소, 벌금이상의 형과 함께 부과된 몰수·추징·사회봉사명령·수강명령 등의 선고 또는 처분에 관한 자료를 ‘범죄경력자료’라 하고, 수사자료표 중 벌금 미만의 형의 선고 및 검사의 불기소처분에 관한 자료 등으로서 범죄경력자료를 제외한 나머지 자료를 ‘수사경력자료’라 한다. ‘전과기록’이란, 수형인명부·수형인명표 및 범죄경력자료를 말한다.

수사자료표의 개인정보에 대한 수집과 유통에 대한 법적 근거는 「형의 실효 등에 관한 법률」이다. 전과기록 및 수사경력자료의 관리에 관한 기준을 법률로써 정하는 것은 전과자의 정상적인 사회복귀를 보장하기 위한 목적에서이다.[50]

## 2. 개인정보의 수집·유통 실태

### 1) 개인정보의 생성

수사자료표의 생성은, 사법경찰관이 피의자를 조사할 때 이루어진다. 각 사법경찰관이 피의자 조사 과정에서 생성한 자료는 경찰청에 송부된다. 다만 즉결심판대상자, 불기소처분사유에 해당하는 사건의 피의자는 제외된다. 경찰청장은 수사자료표를 범죄경력자료와 수사경력자료로 구분하여 전산입력을 한 후 이를 관리하여야 한다.

수사자료표의 작성, 열람 및 삭제 현황은 다음과 같다.

---

50) 「형의 실효 등에 관한 법률」 제1조, 제2조, 제5조의2 제2항.

<표 2-17> 연도별 수사자료표 작성 현황

(단위: 건)

| 연도별 / 관서별 | 2009.7 | 2008 | 2007 | 2006 |
|---|---|---|---|---|
| 총계 | 1,240,708 | 2,033,280 | 1,843,795 | 1,676,006 |
| 경찰관서 | 1,114,682 | 1,884,358 | 1,679,579 | 1,534,404 |
| 타수사기관 | 126,026 | 148,922 | 164,216 | 141,602 |

자료: 경찰청.[51)]

### 2) 개인정보의 이용 및 제공

수사자료표에 대한 이용은 자조직인 경찰관서에서 이루어지는 조회와 제3자인 타기관에의 제공으로 나눌 수 있으며, 그 기본적인 사항에 대하여 「형의 실효 등에 관한 법률」에서 규정하고 있다.

수사자료표에 의한 범죄경력조회 및 수사경력조회와 그 회보는 다음에 해당하는 경우에 그 전부 또는 일부에 대하여 조회목적에 필요한 최소한의 범위 내에서 할 수 있다. △범죄수사 또는 재판을 위하여 필요한 경우 △형의 집행 또는 사회봉사·수강명령의 집행을 위하여 필요한 경우 △보호감호·치료감호·보호관찰 등 보호처분 또는 보안관찰업무의 수행을 위하여 필요한 경우 △수사자료표의 내용을 확인하기 위하여 본인이 신청하는 경우 △「국가정보원법」 제3조제2항의 규정에 따른 보안업무에 관한 대통령령에 근거하여 신원조사를 하는 경우 △외국인의 체류허가에 필요한 경우 △각군 사관생도의 입학 및 장교의 임용에 필요한 경우 △병역의무의 부과와 관련하여 현역병 및 공익근무요원의 입영에 필요한 경우 △다른 법령에서 규정하고 있는 공무원임용, 인·허가, 서훈, 대통령표창, 국무총리표창 등의 결격사유 또는 공무원연금 지급제한사유 등을 확인하기 위하여 필요한 경우 △그 밖에 다른 법률에서 범죄경력조회 및 수사경력조회와 그 회보를 하도록 규정되어 있는 경우. 이에 위반하여 수사자료표의 내용을 회보하거나 누설한 자는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처해진다.

수사자료표를 관리하는 자 또는 직무상 수사자료표에 의한 범죄경력조회 또는 수사경력조회를 하는 자는 그 수사자료표의 내용을 누설하여서는 아니되며, 이에 위반하여 수사자료표의 내용을 회보하거나 누설한 자는 5년 이하

51) '수사자료표, 범죄정보관리시스템 관련 정보공개 청구'에 대한 경찰청의 정보(공개)결정통지서(2009.09.01). 문서번호: 과학수사센터-66519 (2009.09.01). 이 장에서 별도의 표시가 없으면 수사자료표의 현황에 대한 출처는 이하 같다.

의 징역 또는 5천만 원 이하의 벌금에 처해진다.

또 누구든지 위에서 정하는 경우외의 용도에 사용할 목적으로 범죄경력자료 또는 수사경력자료를 취득하여서는 아니되며, 이에 위반하여 범죄경력자료 또는 수사경력자료를 취득한 자는 2년 이하의 징역 또는 2천만 원 이하의 벌금에 처해진다.

이러한 규정에 의하여 범죄경력자료 또는 수사경력자료를 회보받거나 취득한 자는 법령에 규정된 용도 외에는 이를 사용하여서는 아니되며, 이에 위반하여 범죄경력자료 및 수사경력자료를 사용한 자도 2년 이하의 징역 또는 2천만 원 이하의 벌금에 처해진다.

위 법 시행령에 따르면 경찰청의 관리책임자가 전과기록 또는 수사경력자료의 조회·회보대장을 비치하고 조회목적, 조회요청자의 소속·성명, 작성자 및 작성일시 그 밖에 필요한 사항을 기재하도록 하고, 그 내용이 불법 유출되거나 범죄수사·재판 등 법 및 다른 법령에 규정된 목적 외의 다른 목적으로 사용되지 아니하도록 조회·회보대장을 수시로 점검하는 등 필요한 조치를 하여야 한다.

경찰의 「지문 및 수사자료표 등에 관한 규칙」에 따로 명시되어 있는 관련 규정으로는, 범죄경력·수사경력자료를 조회하는 경우 조회의뢰서에 조회대상자를 기재, 관리책임자(일과 후 상황실장)의 승인을 받아야 한다. 다만 경찰청 과학수사센터에서 입건내용 입력, 처분내용 정정 등의 업무를 처리하기 위하여 조회하는 경우에는 전산상의 작업이력으로 대신할 수 있다. 범죄수사 목적으로 긴급을 요하여 조회의뢰서의 승인을 받을 수 없을 때에는 조회처리부에 그 사유를 기재한 후 조회할 수 있으나 조회의뢰자는 반드시 조회의뢰서에 의한 사후승인을 받아야 한다(동규칙 제13조제1항과 제2항). 범죄경력·수사경력조회의 의뢰를 받은 경찰관서의 장은 출력물에 그 용도, 작성자·조회자의 성명 및 작성일시 등 필요한 사항을 기재하거나 서식 등에 의해 회보할 수 있다(동규칙 제14조).

또한 「경찰정보통신운영규칙」에 따르면 범죄경력조회(수사자료)는 조회의뢰서에 의해서만 가능하며, 수사 목적으로 긴급조회 필요시는 유·무선 통신수단으로 가능하나 반드시 조회의뢰서에 의한 사후 승인을 받아야 한다(동규칙 제102조제7항). 타 기관에서 요청한 조회는 개인정보 타 기관 제공 관리대장에 기재하여야 하며, 조회자료 송부 시에는 수령자의 확인서를 징구하여 요청 공문에 첨부하여야 한다. 단, 우편 송부 시에는 등기우편으로 하고 “제공방법”란에 우편 접수번호 등 발송근거를 기록하여야 한다(동규칙 제102

조제6항). 경찰청은 전국 온라인 조회사항을 매일 전산테이프 등 보조기억매체에 수록하고 이를 5년간 보관하고 있다(동규칙 제53조제1항).

<표 2-18> 연도별 범죄(수사)경력 조회 현황 및 건수(경찰관서)

(단위: 건)

| 구분 \ 연도별 | 2009.6 | 2008 | 2007 | 2006 |
|---|---|---|---|---|
| 경찰관서 | 465,424 | 795,245 | 523,391 | 404,945 |

이러한 수사자료표에 대한 조회의 경우, 일차적으로 자조직인 경찰관서 내에서의 오남용에 따른 인권침해와 불법성이 문제로 지적되어 왔다. 이는 관련 법령에서 조회의 목적을 '범죄수사 또는 재판을 위하여 필요한 경우'라고 포괄적으로 규정한 데 따른 문제로 보인다. 관련 규칙의 경우에도 구체적인 목적을 한정하지 않아 오남용될 위험성이 상존한다. 그 결과 경찰관이 목적 외로 범죄경력을 조회한 데 대하여 국가가 배상해야 할 책임을 법원이 인정하기도 하였다.[52] 국가인권위원회에서도 관련한 결정례가 다수 존재한다.

<표 2-19> 경찰관의 수사자료표 조회와 관련한 국가인권위원회 결정례

| 일 시 | 사 례 |
|---|---|
| 2003.7.18 | 경찰관이 전과기록을 위법하게 조회한 뒤 이를 제3자에게 알려준 것은 피진정인의 인권을 침해하고 법을 위반한 것으로 확인하고 지방경찰청장에 해당 경찰관의 징계를 권고 |
| 2006.5.18 | 가족에게 발송하는 구속통지서의 범죄사실의 요지에 피의자의 전과를 기재하는 것은 사생활의 비밀 침해에 해당함 |
| 2008.2.13 | 경찰서장이 행정심판 과정에서 진정인에 대하여 범죄경력을 조회하고 그 범죄경력자료를 사용한 것은 「헌법」제17조에 보장된 진정인의 사생활의 비밀을 침해한 것으로 판단 |

특히 경찰청에서 수사자료표를 조회하고 타기관에 제공하는 경우, 그로 인한 고용차별로 이어질 수 있기 때문에 매우 신중할 필요가 있다. 그러나 범죄(수사)경력에 대한 타기관의 이용은 상당히 폭넓게 보장되어 있다. 형의 실효 이후에도 범죄경력자료가 삭제되지 않는 상황에서 사실상 기간 제한 없이 그 자료가 타기관에 제공되는 것은 문제가 있다.

52) 의정부지방법원 2009.6.6. 2008가단51793 판결.

<표 2-20> 연도별 범죄(수사)경력 조회 현황 및 건수(타기관 제공)

(단위: 건)

| 구분 \ 연도별 | | 2009.6 | 2008 | 2007 | 2006 |
|---|---|---|---|---|---|
| 경찰청 | 국민연금공단 (기초노령연금 지급제한) | 3,693,293 | 3,596,055 | - | - |
| | 국가보훈처 (국가유공자, 국립묘지안장) | 1,898,834 | 2,859,662 | 2,457,210 | 1,402,237 |
| | 병무청(병역 부과) | 520,116 | 1,028,920 | 1,011,212 | 1,117,131 |
| | 사립학교교직원연금관리공단 (연금지급 제한) | 432,403 | 56,871 | 49,854 | 46,355 |
| | 공무원연금관리공단 (연금지급 제한) | 272,930 | 420,518 | 908,041 | 1,015,821 |
| | 기타 (서훈, 대통령·국무총리표창 인·허가 등) | 75,911 | 278,167 | 626,926 | 143,179 |

주목해서 살펴보아야 할 부분은 「보안업무규정」에 따른 신원조회이다. 「보안업무규정」 제31조는 공무원 임용예정자, 비밀취급인가예정자, 해외여행을 하고자 하는 자, 국가중요시설·장비 및 자재 등의 관리자, 공공단체 임직원, 기타 법령이 정하는 자 등을 대상으로 신원조사를 실시하도록 하고, 같은 규정 제34조는 신원조사 결과 국가안전보장 상 유해로운 정보가 있는 것으로 확인된 자에 대해서는 관계기관의 장에게 통보하도록 되어 있으며, 「형의 실효 등에 관한 법률」 제6조 및 동법 시행령 제7조에 "신원조사의 경우 수사자료표를 활용할 수 있다"고 명시돼 있다.[53] 신원조사 실시 관행과

53) 경찰청의 정보공개와 별도로, 2007년 국회 행정자치위원회 경찰청 국정감사 자료에 따르면, 범죄경력 조회 결과가 제공된 전체 기관은 다음과 같다. 행정자치부, 문화관광부, 건설교통부, 국세청, 국방부, 중소기업청, 관세청, 농림부, 보건복지부, 정보통신부, 법무부, 환경부, 철도청, 산업자원부, 재정경제부, 방송위원회, 과학기술부, 국가보훈처, 병무청, 금융감독원, 공무원연금관리공단, 노동부, 특허청, 통일부, 감사원, 기상청, 농촌진흥청, 의문사진상규명위원회, 국립중앙박물관, 국무조정실, 여성가족부, 민주화운동관련자명예회복및보상심의위, 부패방지위원회, 식품의약품안전청, 국무총리실, 대법원(법원행정처), 국가정보원, 질병관리본부, 민주평화통일자문회의, 국토지리정보원, 국가청렴위원회, 국정홍보처, 서울양천구청, 외교통상부, 해양수산부, 공군본부, 중소기업특별위원회, 교육인적자원부, 이북5도위원회, 소방방재청, 문화재청, 국민고충위원회, 청소년위원회, 사립학교교직원연금관리공단, 공정거래위원회, 울산광역시, 서울특별시, 국토관리청, 서울올림픽기념국민체육진흥공단, 부산광역시, 재단법인광주비엔날레, 한국철도기술연구원, 한국철도대학, 국립국어원, 국립중앙도서관, 강원도, 경기남양주시, 경기화성시, APEC정상회의준비기획단, 방위사업청, 서울중구, 육군3275부대, 한국냉동공조협회, 친일반민족행위자재산조사위원회, 한국산업단지공단, 충청남도, 해양경찰청, 기

관련, 국가인권위는 사면·복권된 범죄 경력을 통보하여 진정인이 교원으로 임용되지 못한 불이익을 받은 것은 헌법 제10조에 정한 행복추구권을 침해하는 것이라고 판단하였다.[54]

### 3) 개인정보의 삭제

수사자료표 중 수사경력자료의 보존 기간 및 삭제는 「형의 실효 등에 관한 법률」에 따라 이루어지고 있다. 즉, 검사의 혐의없음·공소권없음·죄가안됨 또는 기소유예의 불기소처분이 있는 경우, 법원의 무죄·면소 또는 공소기각의 판결이 확정된 경우, 법원의 공소기각의 결정이 확정된 경우에 한하여, 해당 처분이 있거나 결정 또는 판결이 확정된 날부터 기산하여 그 법정형에 따른 보존기간 후 삭제하도록 하였다(동법 제8조의2).

「형의 실효 등에 관한 법률」
제8조의2 (수사경력자료의 정리) ①다음 각 호의 어느 하나에 해당하는 경우 제2항 및 제3항의 해당 기간이 경과한 때에 전산입력된 수사경력자료의 해당 사항을 삭제한다. <개정 2008.3.14>
1. 검사의 혐의없음·공소권없음·죄가안됨 또는 기소유예의 불기소처분이 있는 경우
2. 법원의 무죄·면소 또는 공소기각의 판결이 확정된 경우
3. 법원의 공소기각의 결정이 확정된 경우
②제1항 각 호에 대한 수사경력자료의 보존기간은 다음 각 호와 같다. 이 경우 기간은 해당 처분이 있거나 결정 또는 판결이 확정된 날부터 기산한다.

---

획예산처, 통계청, 대전고법, 서울종로구, 경남마산시, 부산구치소, 영등포교도소, 마산교도소, 서울서부지법, 국가균형발전위원회, 우정사업본부, 경기도, 한국직업능력개발원, 부산보훈지청, 서울중랑구, 국립현충원, 경기군포시, 통일교육원, 병무민원상담소, 조달청, 제주도, 한국부품소재산업진흥원, 서울대학, 국가인권위원회, 대통령비서실, 농협중앙회, 정부청사관리소, 서울마포구, 국가기록원, 서울시교육청, 서울중앙지법, 경기안산시, 제천소방서, 경상대학, 충남금산군, 전남진안군, 인천구치소, 강동교육청, 전남신안군, 서울노동청관악지청, 서울시선거위원회, 경기양평군, 홍성교도소, 광주광역시, 경기부천시, 해군본부, 농수산유통공사, 비상기획위원회, 수원지법, 대전광역시, 서울고법, 제주화북동, 경찰병원, 강원대학, 대전교육청, 인천부천지원, 대구소년원, 전주소년원, 대전소년원, 대통령경호실, 원미고등학교, 진주교육대, 국립농수산물품질관리원, 국립현충원, 도로교통협회, 전라북도, 일제강점기강제동원피해진상규명위원회, 서울가정법원, 수원안산지원, 법제처, 국가안전보장회의사무처, 중앙신체검사소, 서울북부지법, 산림청, 전북무주군, 충북음성군, 대전교정청, 부산교도소, 영등포구치소. 이 자료에서 국가정보원의 경우 2006년 단1건만을 조회한 것으로 나타나, 보안업무규정에 따른 신원조사 현황이 특정되어 있지 않다. 그러나 재단법인, 민간협회, 일선학교 등에 대한 회보는 신원조사의 일환으로 이루어진 것으로 유추할 수 있다.

54) 국가인권위원회. 2003.1.27. 형의 효력이 실효된 전과를 이유로 한 교원임용 차별 사건. 02진차47 결정.

1. 법정형이 사형, 무기징역·무기금고, 장기 10년 이상의 징역·금고에 해당하는 죄는 10년
2. 법정형이 장기 2년 이상의 징역·금고에 해당하는 죄는 5년
3. 법정형이 장기 2년 미만의 징역·금고, 자격상실·자격정지, 벌금, 구류 또는 과료에 해당하는 죄는 즉시 삭제. 다만, 제1항제1호의 기소유예 처분이나 제1항제2호·제3호의 판결 또는 결정이 있는 경우는 5년간 보존한다.
③ 제2항에도 불구하고 제1항 각 호의 처분 당시나 판결 또는 결정의 확정 당시 「소년법」 제2조에 따른 소년에 대한 수사경력자료의 보존기간은 다음 각 호와 같다. <신설 2008.3.14>
1. 제1항제1호의 기소유예의 불기소처분의 경우는 그 처분일부터 3년
2. 제1항제1호의 혐의없음·공소권없음·죄가안됨의 불기소처분의 경우는 그 처분 시까지, 같은 항 제2호의 판결이나 같은 항 제3호의 결정의 경우는 그 판결 또는 결정의 확정 시까지
④제1항에 따라 수사경력자료의 해당 사항을 삭제하는 방법은 대통령령으로 정한다. <개정 2008.3.14>

동법 시행령에서는 수사경력자료의 해당사항의 삭제는 법률에서 규정된 기간이 경과한 때에 해당사항을 지체 없이 전산자료에서 삭제하는 방법으로 하되, 삭제한 사람의 소속·성명, 삭제일시 등 삭제에 관한 사항을 삭제한 날부터 5년간 전산으로 관리하도록 하였다(동시행령 제8조제2항).

위 법률에 따라 「범죄수사규칙」에서도 사법경찰관은 수리한 고소·고발사건에 대하여 기소, 기소중지 또는 참고인중지의견으로 송치한 후 관할지방검찰청 또는 지청으로부터 그 사건에 대하여 혐의없음·공소권없음·죄가안됨, 각하의 처분결과와 함께 피의자에 대한 수사자료표를 폐기하도록 통보받은 때에는 그 수사자료표가 지체 없이 폐기될 수 있도록 처분결과를 보고하는 등 필요한 조치를 하여야 한다고 규정하였다(동규칙 제193조). 또한 「지문 및 수사자료표 등에 관한 규칙」에서도 검찰로부터 “송치사건 처리결과 통지 및 처분결과 통보서”를 접수한 경우에는 범죄사건부, 송부표 부본대장 등 관련서류를 정리하되 통보서 제11항의 비고란에 수사자료표를 폐기하도록 기재되었을 때에는 해당 수사자료표가 폐기될 수 있도록 그 처리·처분결과를 지체없이 경찰청에 보고하도록 하였다(동규칙 제8조제3항). 수사경력조회시 처분결과가 미상(수사중, 재판중 포함)인 경우 또는 앞서의 규정에도 불구하고 전산삭제되지 않은 자료를 발견한 경우에는 대검찰청의 사건조회단말기를 통하여 조회하거나 경찰청 과학수사센터에 문의하여 처분·선고결과를 반드시 확인한 후 그 내용을 기재하여 회보하도록 하였다(동규칙 제14조제2항).

그밖에 경찰청장은 수사자료표에 등재된 사람이 사망한 때에는 그 수사자

료표를 폐기할 수 있고, 수사자료표를 마이크로필름 또는 전산자료의 형태로 관리·보존하는 경우에는 종전의 수사자료표를 폐기할 수 있다(동시행령 제9조).

<표 2-21> 연도별 수사자료표 삭제 현황 및 건수

(단위: 건)

| 구분 \ 연도별 | 2009.7 | 2008 | 2007 | 2006 |
|---|---|---|---|---|
| 계 | 323,655 | 935,291 | 140,332 | 576,220 |
| 즉시삭제 | 38,543 | 81,625 | 22,301 | 102,747 |
| 5년보관삭제 | 278,517 | 852,467 | 117,129 | 473,261 |
| 10년보관삭제 | 6,595 | 1,199 | 902 | 212 |

그러나 검사의 혐의없음·공소권없음·죄가안됨 또는 기소유예의 불기소처분이 있는 경우, 법원의 무죄·면소 또는 공소기각의 판결이 확정된 경우, 법원의 공소기각의 결정이 확정된 경우에도 수사경력자료가 즉시 삭제되지 않고 법정형에 따른 보존기간을 두고 있는 것은 문제로 지적될 수 있다. 특히 범죄경력자료에 대해서는 해당자가 사망할 경우를 제외하고는 그 삭제에 대한 규정이 아예 존재하지 않는다. 그러나 동법에서 일정 기간이 지나면 형이 실효하도록 규정되어 있는 만큼, 형이 실효한 때에 수사자료표 또한 함께 삭제하는 것이 바람직해 보인다.

「형의 실효 등에 관한 법률」
제7조 (형의 실효) ①수형인이 자격정지 이상의 형을 받음이 없이 형의 집행을 종료하거나 그 집행이 면제된 날부터 다음 각호의 기간이 경과한 때에는 그 형은 실효된다. 다만, 구류·과료는 형의 집행을 종료하거나 그 집행이 면제된 때에 그 형이 실효된다.
1. 3년을 초과하는 징역·금고는 10년
2. 3년 이하의 징역·금고는 5년
3. 벌금은 2년
②하나의 판결로 수개의 형이 선고된 경우에는 각 형의 집행을 종료하거나 그 집행이 면제된 날부터 가장 중한 형에 대한 제1항의 기간이 경과한 때에는 형의 선고는 효력을 잃는다. 다만, 제1항제1호와 제2호의 규정을 적용함에 있어서 징역과 금고는 동종의 형으로 보고 각 형기를 합산한다.

장기간 수사자료표의 보존이 이루어짐에 따라 추후 삭제가 원활히 이루어

지지 않는 경우가 발생할 수 있고, 실제로 그로 인한 인권 침해 논란이 일기도 한다. 법원은 무죄 확정판결을 받은 원고의 범죄경력자료에 잘못된 전과가 기재되어 장기간 방치된 경우 국가의 손해배상책임을 인정하였다.[55]

## 3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태

정보주체에게는 「형의 실효 등에 관한 법률」에 따라 수사자료표에 대한 열람이 보장된다. 수사자료표의 내용을 확인하기 위하여 본인이 신청하는 경우 그 전부 또는 일부에 대하여 범죄경력조회와 수사경력조회를 할 수 있다(동법 제6조제1항제4호). 정보주체는 범죄경력·수사경력 조회신청서를 작성하고 경찰관서를 방문하여 수사자료표를 열람할 수 있다.[56]

그밖에 「지문 및 수사자료표 등에 관한 규칙」에서는 경찰관서의 장이 신청한 본인에게 열람시키거나 서식에 따라 회보하도록 하였고, 다만 질병, 입원 등의 부득이한 사정으로 본인이 직접 신청할 수 없을 경우에는 위임장에 의거하여 대리 신청할 수 있도록 하였다(동규칙 제14조제1항제2호).

본 연구의 목적을 위하여 실제로 열람 청구권을 행사하여 본 결과 경찰청에서 범죄경력·수사경력 조회 형식으로 정보주체의 열람권 행사가 이루어질 수 있었다(<그림 2-3>).

<표 2-22> 연도별 범죄(수사)경력 조회 현황 및 건수(개인 신청)

(단위: 건)

| 구분 \ 연도별 | 2009.6 | 2008 | 2007 | 2006 |
|---|---|---|---|---|
| 경찰관서(경찰청 포함) | 120,451 | 147,149 | 93,199 | 89,171 |

그러나 현행 법률과 관련 규칙에서는 정보주체에게 수사자료표의 조회 및 타기관 제공 현황에 대해 공개하지 않는다. 본 연구의 목적을 위하여 실제로 조회 및 제공 현황에 대하여 열람 청구권을 행사해 보았지만 그 열람이 제한되는 결정이 났다(<그림 2-4>). 이는 다른 법률에서 정보주체가 개인정보의 현 상태 뿐 아니라 개인정보를 이용한 내역과 제3자에게 제공한 내역을 이용자가 언제든지 확인할 수 있도록 규정한 것과 대비되는 대목이다.[57]

55) 서울중앙지방법원 2006.5.12. 2005나25877 판결.
56) 정보공개시스템(http://www.open.go.kr)을 이용할 수도 있다.
57) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제30조제2항

<그림 2-3> 수사자료표 일반 현황에 대한 정보주체의 열람 청구

[redacted]

인쇄일자 : 2009.08.20

# 정보(부분공개)결정통지서

수 신 자 [redacted]

| | | | |
|---|---|---|---|
| 접 수 일 자 | 2009.07.11 | 접 수 번 호 | [redacted] |
| 청구정보내용 | [공공기관의 개인정보보호에 관한 법률]에 의거하여 다음과 같은 본인에의 개인정보에 대한 열람을 청구합니다.<br><br>1. 본인에 관한 수사자료표의 보유 여부와 열람 청구<br>2. 범죄정보관리시스템(CIMS) 내 본인에 관한 개인정보 입력내용 열람 청구<br>3. 영상판독시스템(불법집회 등을 채증한 사진 및 영상 자료 데이터베이스) 내 본인에 관한 개인정보 입력내용 열람 청구<br>4. 위 1, 2, 3 각 자료/정보의 수집 시점과 수집 경로<br>5. 위 1, 2, 3 각 자료/정보의 자조직내 열람(조회)권자 현황<br>6. 위 1, 2, 3 각 자료/정보의 타기관 제공(조회) 현황(기관별/목적별/최근3년간)<br>7. 위 1, 2, 3 각 자료/정보의 보유 혹은 삭제 기간<br>8. 위 1, 2, 3 각 자료/정보에 대한 정정 혹은 삭제청구 방법<br>8. 위 1, 2, 3 자료/정보의 개인정보 관리책임자<br>9. 이상의 모든 내용과 관련한 법적근거 | | |
| 공 개 내 용 | 청구정보 "1~2, 4~9번 항목은 신분증 지참하여 경찰청 과학수사센터 방문시 열람가능 | | |
| 비공개(전부 또는 일부)내용 및 사유 | 청구정보<br>3. 번 항목<br>공공기관의 정보공개에 관한 법률 제9조1항 비공개대상 정보에 해당됨<br>---------- | | |
| 공 개 방 법 | 공개형태 | 열람 · 시청 | |
| | 교부방법 | 직접방문 | |
| 공개일시 (기간) | 2009.07.22 19 시 | 공 개 장 소 | 경찰청 과학수사센터 |

| 수 수 료 (A) | 우 송 료 (B) | 수수료감면액 (C) | 계 (A+B-C) |
|---|---|---|---|
| 0원 | 0원 | 0원 | 0원 |
| 수수료산정내역 | | 수수료 납입계좌(입금시) | |

귀하의 정보공개 청구에 대한 결정내용을 공공기관의 정보공개에관한법률 제13조 제1항 및 제4항의 규정에 의거하여 위와 같이 통지합니다.

2009 년 07 월 22 일

경찰청장

| 처 리 과 명 | 과학수사센터 | 문 서 번 호 | 과학수사센터 -55047(2009.07.22) |
|---|---|---|---|

참고: 이 정보공개청구의 경우 수사자료표와 범죄정보관리시스템, 그리고 영상판독시스템에 대하여 동시에 이루어졌다. 본 연구에서는 이 가운데 정보가 공개된 수사자료표와 범죄정보관리시스템에 대해서만 다루었다.

<그림 2-4> 수사자료표 이용 현황에 대한 정보주체의 열람 청구

정보공개

인쇄일자 : 2009.08.25

# 정보(부분공개)결정통지서

수 신 자 [redacted]

| 접 수 일 자 | 2009.08.13 | 접 수 번 호 | [redacted] |
|---|---|---|---|
| 청구정보내용 | [공공기관의 개인정보보호에 관한 법률](개인정보보호법)에 의거하여 다음과 같은 본인의 개인정보에 대한 열람을 청구합니다.<br><br>1. 본인에 관한 수사자료표(수사경력/범죄경력)에 기재된 각 경력자료에 대한 경찰관서 내 조회(열람) 현황 (최근 3년간/경찰관서별)<br><br>2. 본인에 관한 수사자료표(수사경력/범죄경력)에 기재된 각 경력자료에 대한 타수사기관 조회(열람) 현황 (최근 3년간/수사기관별)<br><br>3. 위 1, 2 각 경력자료의 보유 혹은 삭제 기간<br><br>4. 위 1, 2 각 경력자료의 정정 혹은 삭제 방법<br><br>5. 위 1, 2 각 경력자료의 관리책임자<br><br>6. 이상의 모든 내용과 관련한 법적근거<br><br>참고로, 이번 열람청구는 현행 개인정보보호법 제13조에 따르면 정보주체에게 자신에 대한 개인정보의 열람을 제한할 수 없습니다. 이 점은 [공공기관의 개인정보파일 관리지침](행정안전부, 2009)에서도 [공공기관이 보유하고 있는 개인정보파일의 경우는 처리정보의 당사자인 정보주체에게 열람을 제한할 수 없음]이라고 명시되어 있습니다.(10쪽) | | |
| 공 개 내 용 | 관련사항 : 3. 위 1, 2 각 경력자료의 보유 혹은 삭제 기간<br><br>4. 위 1, 2 각 경력자료의 정정 혹은 삭제 방법<br><br>5. 위 1, 2 각 경력자료의 관리책임자<br><br>6. 이상의 모든 내용과 관련한 법적근거<br>3. 위 1, 2 각 경력자료의 보유 혹은 삭제 기간<br><br>범죄경력 및 수사경력은 "형의 실효 등에 관한 법률 시행령" 제9조에 의거 수사자료표에 등재된 사람이 사망한 때에는 그 수사자료표를 폐기할 수 있습니다.. 또한, 사망전의 범죄경력자료는 현행법상 삭제할 수 있는 규정이 없어 삭제가 되지 않고 있으나, "형의 실효 등에 관한 법률" 제8조의2에 규정을 근거로 수사경력자료 중 "1. 검사의 혐의없음, 공소권없음, 죄가안됨 또는 기소유예의 불기소처분이 있는 경우 2. 법원의 무죄, 면소 또는 공소기각의 판결이 확정된 경우 3. 법원의 공소기각의 결정이 확정된 경우" 의 보존기간은 법정형에 따라 즉시삭제, 5년후 삭제, 10년후 삭제, 소년법상 소년이며 기소유예는 3년 후 삭제하고 있습니다. | | |

| | |
|---|---|
| | 4. 위 1, 2 각 경력자료의 정정 혹은 삭제 방법<br><br>"지문 및 수사자료표 등에 관한 규칙" 제7조 내지 제9조에 규정을 근거로 경찰청 과학수사센터에서 신원을 확인하고, 대검찰청으로부터 전송받은 처분결과 등을 확인하는 과정 및 본인 또는 그 친족이 수사자료표의 기록내용이 사실과 다르다고 이의제기나 진정을 한 경우에 정정 또는 삭제하고 있습니다.<br><br>5. 위 1, 2 각 경력자료의 관리책임자<br><br>경찰청 과학수사센터장입니다.<br><br>6. 이상의 모든 내용과 관련한 법적근거<br>형의 실효 등에 관한 법률, 형의 실효 등에 관한 법률 시행령, 지문을 채취할 형사 피의자의 범위에 관한 규칙, 지문 및 수사자료표 등에 관한 규칙이 관련 법적근거입니다.<br>---------- |
| 비공개(전부 또는 일부)내용 및 사유 | 요청하신 1번,2번자료는 수사기관 등에서 범죄예방이나 수사 목적등으로 조회한 결과만을 기록한 내부적 업무처리 자료로 사용되는 것이며, 이는『공공기관의 정보공개에 관한 법률』 제9조①항 4호에 의거 정보 비공개 대상입니다.<br>단, 개인정보의 부당한 유출로 인하여 피해를 입으신 경우에는 가까운 수사기관의 민원실에 진정 등을 통한 피해신고를 하시면 필요한 조치를 받으실 수 있음을 알려드립니다.<br>1번,2번 보유근거는『경찰정보통신운영규칙』제53조①항 입니다 |

| 공 개 방 법 | | |
|---|---|---|
| | 공개형태 | 전자파일 |
| | 교부방법 | 온라인 |

| 공개일시 (기간) | 2009.08.25 08 시 | 공 개 장 소 | |
|---|---|---|---|
| 수 수 료 (A) | 우 송 료 (B) | 수수료감면액 (C) | 계 (A+B-C) |
| 0원 | 0원 | 0원 | 0원 |
| 수수료산정내역 | | 수수료 납입계좌(입금시) | |

귀하의 정보공개 청구에 대한 결정내용을 공공기관의 정보공개에관한법률 제13조 제1항 및 제4항의 규정에 의거하여 위와 같이 통지합니다.

2009 년 08 월 25 일

경찰청장

| 처 리 과 명 | 정보통신2담당관 | 문 서 번 호 | 정보통신2담당관 -8131(2009.08.25) |
|---|---|---|---|

수사자료표의 조회 및 타기관 제공은 그 사유와 절차가 법률적으로 규정되어 있고 불법적 조회나 제공에 대해서는 국가의 책임이 인정되어 온 만큼 정보주체 역시 자신의 개인정보에 대한 조회와 제공 현황을 언제든지 직접 확인하고 그에 따른 권리 행사가 이루어질 수 있어야 한다.

한편 수사자료의 생성 및 관리가 법률에 따라 이루어지기 때문에 이에 대한 정보주체의 정정 및 삭제 청구권은 인정되지 않는다. 그러나 법원이 범죄경력자료에 잘못된 전과가 기재된 데 대해 국가의 손해배상책임을 인정한 만큼, 정보주체의 열람권 행사에서 더 나아가 수사자료표에 대한 정정권을 적극적으로 인정되는 절차가 마련될 필요가 있다. 또한 법률에서 규정된 대로 형이 실효한 때에는 수사자료표에 대한 정보주체의 삭제권의 인정도 고려해 볼 필요가 있다.

## 4. 소결

수사자료표 상의 개인정보의 수집과 유통 및 정보주체의 열람 청구권은 법률에 의하여 규정되어 있다. 이는 전과자의 정상적인 사회복귀를 보장하기 위한 법률상 목적을 달성하기 위한 것으로서, 수사경력이나 범죄경력에 대한 조회의 오남용 등으로 전과기록 등 민감한 개인정보가 부당하게 유출되는 것을 방지할 수 있다.

그러나 수사자료표에 대한 조회 오남용으로 인한 인권침해와 불법성이 인정되어 온 만큼 관련 법령 및 규칙을 보완할 필요가 있다. 자조직인 경찰관서 내에서 조회할 때 '범죄수사 또는 재판을 위하여 필요한 경우' 포괄적으로 허용하기보다 명확하게 규정할 필요가 있으며, 타기관에 제공할 수 있는 사유 역시 보다 세밀하게 명시되어야 할 것으로 보인다. 「보안업무규정」에 따른 신원조회를 위해 수사자료표가 제공되는 경우는 인권침해 소지가 크며, 형의 실효 이후에도 범죄경력자료가 삭제되지 않는 상황에서 사실상 기간 제한 없이 그 자료가 타기관에 제공되는 것은 문제가 있다.

수사경력자료와 범죄경력자료에 대한 삭제 규정 역시 필요하다. 검사의 혐의없음・공소권없음・죄가안됨 또는 기소유예의 불기소처분이 있는 경우, 법원의 무죄・면소 또는 공소기각의 판결이 확정된 경우, 법원의 공소기각의 결정이 확정된 경우에도 수사경력자료가 즉시 삭제되지 않고 법정형에 따른 보존기간을 두고 있는 것은 문제이다. 범죄경력자료에 대해서는 해당자가 사망할 경우를 제외하고는 그 삭제에 대한 규정이 아예 존재하지 않는다. 형이

실효한 때에는 수사자료표를 함께 삭제하는 것이 바람직해 보인다.

또한 수사자료표에 대한 정보주체의 열람권 행사를 보장함에 있어서, 수사자료표의 현 상태 뿐 아니라 수사자료표의 조회 및 타기관 제공 현황에 대해서도 함께 공개되어야 하며 그 정정 및 삭제 청구권도 보다 적극적으로 보장될 필요가 있다.

## II. 범죄정보관리시스템(CIMS)

### 1. 개요

범죄정보관리시스템(CIMS: Crime Information Management System)이란 수사지식정보・사건관리・범죄통계・전자지도・One-Call검색・신원종합검색 등이 통합・연계된 시스템을 말한다.[58] 경찰수사연수원이 발간한 「범죄정보시스템 분석」에서는 범죄정보관리시스템에 대하여, 경찰관서에서 발생하는 모든 사건 기록을 데이터베이스화해 사건을 체계적으로 관리하고 이를 토대로 다양한 통계 및 범죄분석 자료를 산출할 수 있으며, 또한 네트워크를 통해 일선 경찰들 사이에 다양한 수사지식 정보를 공유함으로써 범죄의 예방과 검거 능력의 극대화를 기할 수 있는 시스템이라고 보았다.[59]

범죄정보관리시스템은 지난 5년에 걸친 여러 정보시스템의 운영과 수정이라는 지속적인 노력의 결과로 생겨난 것이다. 서울 노량진 경찰서의 범죄분석 프로그램 활용을 시작으로 서울지방경찰청의 컴스텟개발, 경찰청의 범죄예측분석시스템(컴스텟)개발이 진행되었으며, 2002년 12월부터 컴스텟에 대한 전면적인 개편작업이 시작되어 2004년 1월 현재의 범죄정보관리시스템이 도입되었다(이건 외, 2005: 8).

범죄정보관리시스템의 개인정보에 대한 수집과 유통에 대한 법률적 근거로서 경찰은 「경찰법」 제3조, 「경찰관직무집행법」 제2조제3호, 「공공기관 개인정보보호법」 제5조, 제10조제3항제6호를 들고 있다.[60]

---

58) 「범죄정보관리시스템 운영지침」 제2조제1호.

59) 한겨레21. 2009.6.26. “경찰은 지난 여름 네가 한 일을 알고 있다”. 제766호에서 재인용.

60) ‘범죄정보관리시스템 관련 정보공개 청구’에 대한 경찰청의 정보(부분공개) 결정통지서(2009.07.14). 문서번호: 과학수사센터-52272 (2009.07.14). 이 절에서 별도의 표시가 없으면 범죄정보관리시스템에 대한 경찰의 입장에 대한 출처는 이하 같다.

「경찰법」
제3조 (국가경찰의 임무) 국가경찰은 국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압 및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 임무로 한다. <개정 2006.7.19>

「경찰관직무집행법」
제2조 (직무의 범위) 경찰관은 다음 각호의 직무를 행한다.
3. 치안정보의 수집·작성 및 배포

「공공기관의 개인정보보호에 관한 법률」
제5조 (개인정보파일의 보유범위) 공공기관은 소관업무를 수행하기 위하여 필요한 범위안에서 개인정보파일을 보유할 수 있다. <개정 2007.5.17>
제10조 (처리정보의 이용 및 제공의 제한)
③보유기관의 장은 제1항의 규정에 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에도 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있다고 인정되는 때에는 그러하지 아니하다. <개정 1999.1.29, 2007.5.17>
6. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우

그러나 이 조항들은 일반적인 경찰 직무에 관한 사항으로서 범죄정보관리시스템의 방대한 개인정보 수집 및 유통에 대한 법률적 근거가 되기가 어렵다.

「공공기관개인정보보호법」에서는 “공공기관의 장은 개인정보를 수집하는 경우 개인정보 수집의 법적 근거, 목적 및 이용범위, 정보주체의 권리 등에 관하여 문서 또는 인터넷 홈페이지 등을 통하여 정보주체가 그 내용을 쉽게 확인할 수 있도록 안내하여야 한다”고 규정하고 있다(동법 제4조제2항). 다만, “범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보파일”은 이에 따른 의무에서 제외하고 있다(제6조제3항제2호). 경찰은 같은 이유에서 범죄정보관리시스템에 대한 정보가 행정안전부에서 공고하는 개인정보파일목록집에 미포함되었으며, 개인정보파일대장도 작성하지 않는다고 밝혔다. 그러나 이미 처리된 사건의 조서와 수사보고서 등은 이후 수사와 직접적 관련이 없고 공소 제기나 치안정보 수집과도 관련이 없기 때문에 “심스의 정보 수집은 원천적으로 불법”이라는 주장이 제기된다.[61]

범죄정보관리시스템의 개인정보의 관리에 대한 법률적 통제가 없는 상황에

61) 한겨레21, 앞의 기사.

서, 그에 따른 오남용과 유출 가능성이 상존한다. 수사자료표의 경우에는 그 생성과 보유가 「형의 실효 등에 관한 법률」에 따라 이루어진다. 따라서 수사자료표에 기재된 개인정보를 경찰이 조회하거나 타기관에 제공할 수 있는 사유에 대해서 법률적으로 규정되어 있으며 일정한 요건에 의해 삭제도 가능하다. 범죄정보관리시스템의 범죄정보는 수사자료표 상의 수사경력자료, 범죄경력자료와 별도로 구축되어, 수사 및 범죄에 관한 개인정보의 수집과 유통에 대한 「형의 실효 등에 관한 법률」상의 법률적 의무를 형해화할 우려가 높다.

## 2. 개인정보의 수집·유통 실태

범죄정보관리시스템의 구축 및 운영에 대한 근거 법률이 없는 상태에서 그 개인정보 수집과 유통에 대한 사항은 「범죄정보관리시스템 운영지침」에서 규정하고 있다. 이를 「형의 실효 등에 관한 법률」상 수사자료표의 개인정보 생성과 유통의 흐름과 비교하면 다음과 같다.

<표 2-23> 수사자료표와 범죄정보관리시스템의 개인정보 생성과 유통

| 구분 | 작성 | | 제공 및 이용 | 삭제 |
|---|---|---|---|---|
| | 작성자 | 작성일시 | | |
| 수사자료표 | 사법 경찰관 | 피의자 조사시 작성 작성후 경찰청 송부 | (본인 포함) 법률에 규정된 목적 하에 조회 및 회보 | 수사경력자료의 경우 무혐의·무죄 처분 등에 대하여 그 법정형에 따라 즉시 / 5년 / 10년 보관 후 삭제 범죄경력자료의 경우 삭제 규정 없음 |
| | 경찰청 | 범죄경력자료와 수사경력자료로 구분하여 전산입력 | | |
| 범죄정보관리시스템 | 범죄수사 및 범죄수사 지원 기능에 종사하는 경찰공무원, 일반직공무원, 기능직공무원 | 고소·고발·이송사건은 접수 즉시 입력 인지·발생·검거사건은 수사팀 인계 즉시 입력 모든 사건의 종결 내용은 기록 송치 이전에 입력 | 범죄수사 목적으로 활용 본인 정보 열람은 공공기관의개인정보보호에 관한법률에 따름 | 원칙적으로 삭제 불가 |

이에 대한 「범죄정보관리시스템 운영지침」의 규정은 다음과 같다.

제3조 (시스템 관리, 운영 및 권한) ① 범죄정보관리시스템의 관리 및 운영 담당은 범죄수사 및 범죄수사 지원 기능에 종사하는 경찰공무원, 일반직공무원, 기능직공무원으로 지정한다. 단, 시스템 관리 및 운영을 보조하는 기타 직렬의 공무원 또는 보조자의 경우 담당 책임 공무원의 감독 하에 제한된 범위 내에서 시스템 관리, 운영 등을 보조할 수 있다.
② 수용자확장검색의 승인권자는 경찰청·지방청의 경우 1차 승인권자는 담당반장, 2차 승인권자는 담당계장으로 하고, 경찰서의 경우 1차 승인권자는 담당팀장, 2차 승인권자는 담당과장으로 한다.
③ One-Call검색의 승인권자는 경찰청·지방청의 담당반장으로 하고, 경찰서의 경우 담당팀장으로 한다.
④ 긴급One-Call검색은 사안이 긴급하고, 승인권자가 부재인 경우에 한하고 검색 후 반드시 사후 승인을 득하여야 한다.
⑤ 각 경찰관서의 관리자는 시스템 사용자의 작업권한에 대하여 사용자별 업무성격과 자료의 보안성을 고려하여 그 등급을 정하여 체계적으로 관리하여야 한다.

제6조 (사건자료의 입력기준) ①고소·고발·이송사건은 접수 즉시 입력하고, 인지·발생·검거사건은 수사팀 인계 즉시 입력한다.
②모든 사건의 종결 내용은 기록 송치 이전에 입력한다.

제9조 (전산자료의 삭제 및 변경) ① 전산 입력된 자료는 임의로 삭제할 수 없다. 다만, 특별한 사유가 발생된 경우 관서별 시스템 관리자가 그 적정성을 심사하여 이를 삭제·변경할 수 있다.
② 본청 관리자는 사회상규 또는 경찰윤리에 반하거나 경찰업무 수행에 지장을 주는 게시물은 게시자 의견에 불구하고 즉시 삭제할 수 있다.

제10조 (자료의 분석 및 활용) ① 범죄정보관리시스템에 입력된 자료는 범죄수사 목적으로 활용되어야한다.

제12조 (보안관리) ① 각 경찰관서 주무과장은 개인정보의 보호를 위하여 매월 시스템 운영에 관한 전반적인 보안점검을 실시하고 필요한 조치를 강구하여야 한다.
② 시스템 운영시 알게 된 사건관련정보는 법령 또는 업무상 필요한 절차 외에는 이를 누설·이용하거나 제공할 수 없다.
③ 소년보호사건에 대하여는 소년법 제70조에 따라 그 사건내용에 관하여 재판, 수사 또는 군사상 필요한 경우 외의 어떠한 조회에도 응하여서는 아니된다.
④ 범죄정보관리시스템 사용자는 자신의 업무 및 권한을 벗어난 조회·검색을 하여서는 아니 된다.
⑤ 각 경찰관서의 범죄정보관리시스템 부서별 관리자는 매일 업무종료 전 조회 및 검색현황을 파악하고, One-Call승인대장 및 수사대상자 조회처리부는 매일 그 결과를 출력하여 담당 계장(팀장)·과장의 결재를 받아 편철하며, 신원종합검색대장, 수용자조회 처리부, 수용자확장조회 처리부는 매주 그 결과를 출력하여 담당 계장(팀장)·과장의 결재를 받아 각 과별 또는 기능별 편철하여야 한다.
⑥ 기타 이 지침에 정하는 바가 없는 사항에 대하여는 '경찰정보통신운영규칙'을

준용한다.

### 1) 개인정보의 생성

「범죄정보관리시스템 운영지침」에 따르면, 범죄정보관리시스템의 개인정보 생성은 범죄수사 및 범죄수사 지원 기능에 종사하는 경찰공무원, 일반직 공무원, 기능직공무원에 의해 이루어진다(동지침 제3조제1항). 고소·고발·이송사건은 접수 즉시 입력하고, 인지·발생·검거사건은 수사팀 인계 즉시 입력하고, 모든 사건의 종결 내용은 기록 송치 이전에 입력하도록 하였다(동지침 제6조).

범죄정보관리시스템의 사건별 작성, 활용 현황은 다음과 같다.

<표 2-24> 범죄정보관리시스템에 기록된 사건 건수

| 구분 | 2004년 | 2005년 | 2006년 | 2007년 | 2008년 | 2009.8. |
|---|---|---|---|---|---|---|
| 건수 | 2,413,276 | 2,208,221 | 2,188,015 | 2,308,408 | 2,662,449 | 1,800,917 |

※ 사건건수는 시스템을 통해 입력된 건수로 사건통계와 다름.

자료: 김유정(2009).[62]

개인정보별 현황은 다음과 같다.

<표 2-25> 범죄정보관리시스템에 저장된 개인정보 현황

| 구분 | 소계 | 피의자 | 피해자 | 참고인 |
|---|---|---|---|---|
| 2009.6 | 2,830,985 | 1,546,856 | 1,084,843 | 199,286 |
| 2008년 | 5,551,451 | 3,099,082 | 2,096,072 | 356,297 |
| 2007년 | 4,891,081 | 2,744,888 | 1,866,634 | 279,559 |
| 2006년 | 4,581,744 | 2,622,720 | 1,839,995 | 119,029 |
| 2005년 | 4,517,838 | 2,597,662 | 1,853,152 | 67,024 |
| 2004년 | 4,860,543 | 2,801,533 | 2,003,677 | 55,333 |
| 2004년 이전 | 16,934,225 | 9,505,275 | 7,379,148 | 49,802 |
| 총계 | 44,167,867 | 24,918,016 | 18,123,521 | 1,126,330 |

※ 대상자는 중복자료 포함.

62) 이 장에서 별도의 표시가 없으면 범죄정보관리시스템의 현황에 대한 출처는 이하 같다.

그런데 범죄정보관리시스템에는 피의자를 상대로 받은 신문조서는 물론 피해자와 참고인에게서 받은 진술조서, 수사보고서, 체포·구속·압수수색영장 신청서, 의견서 등이 모두 들어가 있다. 소년신원조사표, 비행성예측 자료표 등 매우 민감한 내용도 포함되어 있다. 이와 같은 서식의 종류가 모두 301가지에 이른다.

<표 2-26> 범죄정보관리시스템 입력 주요 서식 종류 (모두 301종)

| | | |
|---|---|---|
| 감청 | 5종 | 감정의뢰, 감정처분허가장신청, 감정유치장신청 등 |
| 수사보고 | 29종 | 방문조사, 외근수사, 피의자체포, 영상녹화, 내사착수, 범죄인지 등 |
| 수사서식 | 50종 | 내사지휘서, 수사지휘건의, 사망통보, 출석요구서, 증인신문신청 등 |
| 수사지원 | 35종 | 고정정보원명부, 위조통화감정처리표, 미검거중요범죄사건부 등 |
| 조서 | 30종 | 피의자신문조서, 진술조서, 수색조서, 압수조서 등 |
| 통신 | 40종 | 긴급통신사실확인자료제공요청, 통신자료제공요청, 긴급통신제한조치통보, 통신제한조치집행조서 등 |
| 출입국 | 8종 | 범법자출입국규제(입국시통보)요청지휘, 출입국공문(출국정지요청) 등 |
| 팀분야별 | 15종 | 소변검사시인서, 소변모발채취동의서, 거짓말탐지 검사결과 보고 및 결과서 등 |
| 강제수사 | 70종 | 지명수배서, 지명수배자검거보고, 압수목록, 압수수색검증영장신청부, 현행범인체포서 등 |
| 송치서식 | 8종 | 사건송치, 의견서, 소년보호사건송치 |
| 대상별 | 11종 | 공무원범죄수사개시통보, 변호인참여현황피해신고서, 영사기관사망통보서 등 |

자료: 경찰청.[63]

방대한 범죄정보관리시스템의 자의적 구축과 운영은 다른 경찰관의 수사 때 해당 경찰관의 선입견을 부추기고 예단을 심어주고 피의자의 인권을 무시할 수 있다는 우려가 제기되고 있다. 또한 민감한 '피해자' 정보도 노출될 가능성도 있다. 특히 수사보고서와 각종 조서는 저장해서는 안될 정보로 지목되고 있다. 수사보고서는 형사가 수사 과정에서 얻은 정보를 자의적으로 기록해 남긴 것으로서 사실인 내용과 그렇지 않은 내용이 혼재돼 있다. 조서는

63) 한겨레21, 앞의 기사에서 재인용.

당사자의 무인이나 도장을 이용한 날인과 간인이 없는 경우 재판에서 증거로 효력을 갖지 못하고 오류가 있을 수 있다. 부정확한 내용이 남아 있을 가능성이 높은 것이다.

「범죄수사규칙」에 따르면, 경찰은 수사를 종결하였을 때 사건을 모두 관할지방검찰청 검사장 또는 지청장에게 송치하여야 한다(동규칙 제189조). 다만 처리한 사건 중 중요도나 특이성 그 밖의 보존의 필요가 있다고 판단되는 사건에 대하여는 해당 사건의 수사서류의 사본을 작성하여 이를 보존하여야 한다(동규칙 제199조). 범죄정보관리시스템의 경우 특별한 사유가 없어도 신문조서 등 모든 수사서류의 사본을 보관하고 있어 이러한 원칙과 배치된다.

특히 범죄정보관리시스템에서 수사 및 범죄 관련 개인정보의 생성과 관리가 수사자료표와 별도로 이루어지고 있는 점은 큰 문제이다. 단적인 예로, 경찰의 조사 이후에 검찰이 무혐의로 처분하였거나 법정에서 무죄 판결을 받은 사건의 경우 수사자료표는 「형의 실효 등에 관한 법률」에 따라 삭제가 되지만 범죄정보관리시스템에서는 경찰이 수사할 당시의 자료가 그대로 남아 있을 수 있는 것이다.

### 2) 개인정보의 이용 및 제공

「범죄정보관리시스템 운영지침」에 따르면, 범죄정보관리시스템 상의 개인정보 이용은 “범죄수사 목적”으로 가능하도록 포괄적으로 규정되어 있다(동지침 제10조).

구체적인 자조직내 이용(조회) 권한은 다음과 같다. ‘수용자확장검색’의 경우 담당반장/담당계장(경찰청・지방청) 혹은 담당팀장/담당과장(경찰서)의 승인을 받고, ‘One-Call검색’의 경우 담당반장(경찰청・지방청) 혹은 담당팀장(경찰서)의 승인을 받으며, ‘긴급One-Call검색’은 사안이 긴급하고, 승인권자가 부재인 경우에 한하고 검색 후 사후 승인을 득해야 한다(동지침 제3조). 각 경찰관서의 범죄정보관리시스템 부서별 관리자는 매일 업무종료 전 조회 및 검색현황을 파악하고, One-Call승인대장 및 수사대상자 조회처리부는 매일 그 결과를 출력하여 담당 계장(팀장)・과장의 결재를 받아 편철하며, 신원종합검색대장, 수용자조회 처리부, 수용자확장조회 처리부는 매주 그 결과를 출력하여 담당 계장(팀장)・과장의 결재를 받아 각 과별 또는 기능별 편철하여야 한다(동지침 제12조제5항).

<표 2-27> 범죄정보관리시스템 정보에 대한 조회현황

| 구분 | 2004년 | 2005년 | 2006년 | 2007년 | 2008년 | 2009.8. |
|---|---|---|---|---|---|---|
| 건수 | 1,279,648 | 2,548,104 | 2,978,978 | 3,882,031 | 2,004,654 | 1,344,529 |

그런데 김유정(2009)에 따르면 수사대상자검색의 상세검색을 들어가 보면 '대상자 정보'라는 메뉴 안에 피해자와 참고인 정보도 함께 나타나게 되어 있어서 관련 정보가 유출될 경우 보복범죄 등에 그대로 노출될 위험성이 있다. 특히 성명과 주민번호만 입력하면 해당 당사자의 피의사실(사건개요란), 피해사실(피해상황란)을 구별하지 않고 모든 자료가 검색 가능하게 되어 있어 성범죄 피해자의 경우 정보 노출로 인한 심각한 인권 침해의 가능성이 있다.

반면 범죄정보관리시스템의 조회에 필요한 승인은 같은 경찰관서에서 비교적 간단한 절차로 이루어지고, 자기관에서 조회하거나 다른 경찰관서를 비롯한 타기관에 제공할 때 그 사유와 목적을 상세하게 규정한 지침이나 법률이 존재하지 않는다. 따라서 그에 따른 사건사고가 계속되고 있다.[64] 경찰이 범죄정보관리시스템을 불법적으로 조회하고 제공한 사건에 대하여 법원이 실형을 선고하거나, 현직 경찰관이 범죄정보관리시스템에 정보를 허위로 입력한 혐의로 검찰에 구속되기도 하였다.[65] 이러한 사건들은 경찰이 범죄정보관리시스템을 이용하는 데 있어 감시·감독이 제대로 이루어지고 있지 않음을 보

64) "경찰청 수사국에 근무하던 김아무개 경위는 2007년 중반께 지인의 형사고소건과 관련해 상대방의 진술조서와 신문조서 등을 심스에 여러 차례 접근해 출력했다. 사건의 상대방이 경찰에 와서 한 진술 내용을 확인해 맞대응 전략을 짬으로써 지인의 고소건을 유리하게 끌고 가기 위한 목적이었다. 김 경위는 이를 위해 해당 고소건을 수사하던 서울 강남경찰서 간부 2명에게 돈을 건네고 심스에 접속하는 아이디와 패스워드를 건네받기도 했다. 형사들이 본인이 처리 중이거나 완료한 사건 정보에는 언제나 제한없이 심스를 통해 접근할 수 있다는 시스템의 허점을 노린 것이다. 결국 수원지법은 지난해 10월 김 경위와 강남경찰서 두 간부에게 실형을 선고했다. 재판부는 "자신의 직위를 이용해 범죄정보관리시스템에 침입하는 등의 방법으로 관련 형사사건에 적극적으로 관여해 국가수사권을 오로지 사적인 이익을 위해 사용하는 등 경찰공무원으로서는 도저히 해서는 안 되는 일을 한 것"이라며 김 경위에게 징역 2년을 선고했다. 애초 심스에 조서가 담기지 않았다면 일어나지 않았을 사건이다. 지난 2월에는 서울 강서경찰서의 40대 경찰관이 개인적인 목적으로 특정인의 주민정보와 수배정보를 2007년 4월부터 1년 동안 46차례나 불법 조회한 것으로 검찰 수사 결과 드러났다. 지난해 4월에는 서울 강남경찰서 소속 이아무개 경사가 친분이 있는 사람의 부탁을 받고 장아무개씨의 주민등록과 수배 기록을 여러차례 조회했다 덜미를 잡혔다. 경찰에 정보공개를 청구해 불법 조회 사실을 파악한 장씨는 이 경사를 서울중앙지검에 고소했다. 모두 일선 경찰관들이 적절한 정보 접근을 하고 있는지 감시하는 경찰 내부 장치가 제대로 작동하지 않고 있음을 보여주는 사례들이다." 한겨레21, 앞의 기사.

65) 법률신문. 2008.10.13. "금품 받고 수사기록 열람해준 전직 경찰관 3명에 징역형."; 연합뉴스. 2009.4.27. "'뇌물' 경찰관 2개월만에 또 쇠고랑."

여주고 있으며, 감시·감독 체계가 미비한 것은 근거 법률이 미비한 상태에서 거대한 개인정보 데이터베이스를 자의적으로 운영하는 데 따른 문제라는 비판을 피해갈 수 없다.

<표 2-28> 범죄정보관리시스템 오남용에 대한 징계건수

| 연도 | 유출사례 | 유출경위 및 목적 | 징계내용 |
|---|---|---|---|
| 2005 | '05. 10월경 수사대상자 검색 | 형부 부탁 | 견책 |
| 2007 | '07.6.28 등 4회 수사대상자검색 | 지인 부탁 | 정직 3월 |
| 2008 | '07.7.2, '08.1.23 수사대상자검색 | 남편 부탁 | 해임 |
| | '08.4.26 수사서류 열람 | 지인 부탁 및 뇌물수수 | 파면 |

### 3) 개인정보의 삭제

「범죄정보관리시스템 운영지침」에 따르면, "전산 입력된 자료는 임의로 삭제할 수 없다. 다만, 특별한 사유가 발생된 경우 관서별 시스템 관리자가 그 적정성을 심사하여 이를 삭제·변경할 수 있다"라고 규정하고 있어 자료의 삭제를 원칙적으로 금지하고 있다(동지침 제9조).

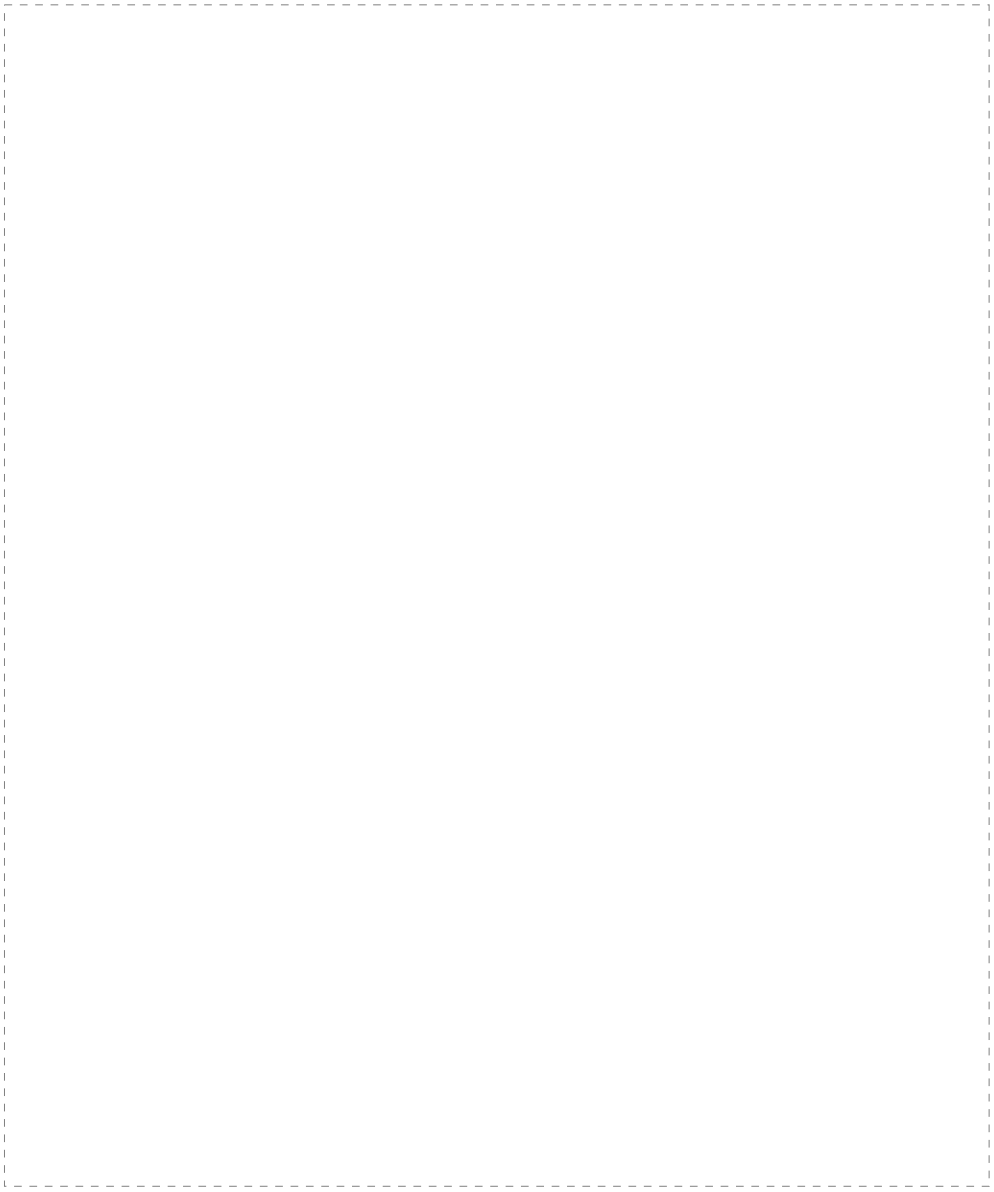
이는 「형의 실효 등에 관한 법률」에서 일정한 요건 하에 수사자료표의 삭제를 의무적으로 규정하고 있는 것과 크게 다르다. 범죄정보관리시스템에 입력된 수사와 범죄 경력에 대한 내용에서 잘못된 부분이 있어도 당사자가 이를 인지하고 적극적으로 청구권을 행사하지 않는 한 이에 대한 정정이나 삭제가 사실상 이루어지기 어려운 것이다.

## 3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태

범죄정보관리시스템에 입력된 개인정보에 대해 정보주체가 열람청구권을 행사할 수 있도록 보장한 명시적 규정은 존재하지 않는다. 그러나 「공공기관개인정보보호법」에 의해 일반적인 열람이 허용되고 있다.

본인여부 확인이 가능한 신분증을 지참하여 경찰청 과학수사센터를 방문하면 범죄정보관리시스템에 입력된 개인정보를 열람하는 것이 가능하다. 또한 잘못 기록된 정보에 대해서는 그 정정과 삭제를 청구할 수 있으며, 이때 관서별 시스템 관리자가 그 적정성을 심사한다. 제3자의 제공내역은 비공개 대상정보로 청구할 수 없다. 다만 개인정보 유출로 인해 피해를 입은 경우 수사기관에 진정·고소를 통한 피해신고를 하여 조치 받을 수 있다.

<그림 2-5> 범죄정보관리시스템 일반 현황에 대한 정보주체의 열람 청구



본 연구의 목적을 위하여 실제로 열람 청구권을 행사하여 본 결과 경찰청과 사건 담당 경찰관서에서 정보주체의 열람권 행사가 이루어질 수 있었다(<그림 2-5>). 그러나 앞서 지적하였다시피 범죄정보관리시스템의 개인정보 수집과 관리에 대한 법률적 근거가 존재하지 않고 관련 지침에서는 자료의 삭제를 원칙적으로 금지하고 있기 때문에 정보주체의 권리 행사는 제한적일 수밖에 없다. 특히 정보주체에게 자신의 개인정보가 타기관에게 제공된 내역을 공개하지 않는 것은 큰 문제이다. 정보주체의 열람권은 개인정보의 현 상태에 대해서 뿐 아니라 개인정보를 이용하거나 제3자에게 제공한 내역에 대해서도 보장되어야 한다. 불법적 조회나 제공에 대해서는 국가의 책임이 인정되어 온 만큼 정보주체 역시 자신의 개인정보에 대한 조회와 제공 현황을 언제든지 직접 확인하고 그에 따른 권리 행사가 이루어질 수 있어야 한다.

## 4. 소결

범죄정보관리시스템이 방대한 양의 개인정보의 수집과 관리를 하면서도 마땅한 법률적 근거를 갖추지 않은 채 운영되고 있는 점은 시급히 시정될 필요가 있다. 특히 범죄정보관리시스템의 범죄정보는 수사 및 범죄에 관한 개인정보의 수집과 유통에 대한 「형의 실효 등에 관한 법률」상의 법률적 의무를 형해화할 우려가 높다.

피의자 뿐 아니라 피해자 및 참고인에 대한 개인정보도 포함되어 기본적 인권을 침해할 가능성이 높고, 피해자 정보 등 민감한 개인정보가 유출될 위험성도 존재한다. 특히 수사보고서와 조서까지 저장하고 있는 점은, 경찰 수사가 종료되면 사건 기록을 검찰에 송치하도록 한 원칙에 배치될 뿐 아니라 부정확한 정보의 저장으로 인한 추가적인 인권 침해를 유발할 가능성이 있다.

범죄정보관리시스템에 입력된 개인정보를 자조직 내에서 조회하거나 타기관에 제공하는 데 대한 구체적인 제한이 존재하지 않기 때문에 그로 인한 오남용과 불법적인 이용 사례가 지적되어 왔다. 또한 자료의 삭제를 원칙적으로 금지하고 있기 때문에 잘못된 정보가 잔존할 위험성을 더욱 높이며, 그에 따른 정보주체의 권리 행사 또한 제약하고 있다.

# 제3절 정보통신 영역

인터넷, 이동통신 등 정보통신 서비스는 주로 온라인을 통한 개인정보의 집적과 활용이 이루어지는 영역이다. 우리나라 국민 대다수는 초고속 인터넷 서비스와 이동통신 서비스를 이용하고 있으며, 인터넷을 통해 포털, 쇼핑몰, 게임 등 수많은 사이트에 가입을 한다. 따라서 정보통신 서비스 영역은 타 분야에 비해 상대적으로 대규모 개인정보를 보유하고 있다. 제3절에서는 정보통신 영역을 포털 영역과 이동통신사 및 초고속인터넷서비스업체 영역으로 나누어 개인정보 수집·유통 실태를 파악하였다.

## I. 포털 업체

### 1. 개 요

현재 대한민국의 인터넷 이용률은 2009년 9월 기준, 3세 이상 대한민국 국민의 77.2%(3,658만 명)에 달하고 있으며(한국인터넷진흥원, 2009: 2), 초고속 인터넷 가입자 수 2009년 6월 기준, 1,593만 명이다. 전체 가구의 인터넷 보급률은 2008년 6월, 81%로서 대한민국 국민에게 인터넷은 중요한 생활 수단으로 자리 잡았다.[66]

인터넷이 우리의 삶에 깊숙이 들어오면서 여러 사건사고들이 발생하고 있으며 그 중에서도 개인정보 관련 사건사고의 발생도 끊이지 않고 있다. 2008년도의 개인정보침해 신고 및 상담 건수는 39,811건으로 2007년의 25,965건, 2006년의 23,333건에 비해 큰 폭으로 증가했다(한국정보화진흥원, 2009: 16). 2008년 IT 및 소프트웨어 업계 종사자와 관련 전문가를 대상으로 선정한 IT 10대 이슈 1위로 꼽힌 것 역시 보안·정보보호였다(한국소프트웨어진흥원, 2008).

이처럼 개인정보를 둘러싼 사회적 관심과 사건사고가 증가하고 있는 가운데 인터넷 이용의 중심인 포털을 대상으로 개인정보의 수집 및 유통 실태와 이용자의 개인정보 열람 및 정정·삭제 청구권 보장 실태를 알아보고자 하는 것이 본 연구의 목적이다.

---

66) 인터넷통계정보시스템 ISIS 2008년 6월 통계 http://isis.nida.or.kr/sub02/#

### 1) 포털의 현황

이용자가 인터넷 망을 통해 인터넷 상의 여러 컨텐츠를 이용하는 관문이 바로 포털이다. 대한민국 최대 포털인 네이버의 경우 2009년 9월 기준 주당 순방문자 약 2,600만 명, 주당 페이지뷰 약 48억 회, 포털 2위인 다음의 경우 주당 순방문자 약 2,200만 명, 주당 페이지뷰 약 44억 회[67]에 달하고 있다. 포털은 단순히 인터넷의 여러 컨텐츠로 접근하는 관문일 뿐만 아니라, 컨텐츠가 소비되고 커뮤니티가 꾸려지고 이용자들 서로가 의견을 주고받는 등의 포괄적인 기능을 하는 우리 사회의 중요한 소통수단으로 자리 잡았다.

이러한 포털에 집적되어있는 개인정보의 양 또한 실로 방대하다. 2009년 2월 현재 네이버의 가입자 수는 3,300만 명, 다음의 가입자 수는 3,500만 명[68]으로서 포털 가입자의 대부분이 대한민국 국민임을 감안한다면, 포털이 가지고 있는 개인정보의 거의 대부분은 대한민국 국민의 개인정보이기도 하다. 이에 따라 개인정보 보호와 관련된 여러 법, 제도 및 기술적 조치의 중요성이 높아지고 있는 상황이다. 그러나 본 연구의 설문조사에 의하면 포털 이용자들은 포털의 개인정보 유출 등의 프라이버시 침해에 대해서는 높은 우려를 나타내면서도 자신이 포털 측에 제공한 정보들이 무엇인지, 어떻게 관리되고 있는지, 정보주체로서 제공된 정보에 대한 자신의 권리는 무엇인지에 대한 인식은 낮은 상황이다[69].

### 2) 법적 근거

포털은 정보통신서비스 제공자로서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 「정보통신망법」)의 적용을 받고 있다. 「정보통신망법」에서는 정보통신서비스 제공자, 이용자, 개인정보를 다음과 같이 정의하고 있다.

---

67) 다음디렉토리 http://directory.search.daum.net/site_list.daum 2009.10.16 접속

68) 아시아경제. 2009.2.27. “新네이트 출범…포털 2위 노린다.”

69) 본 연구의 제4장 제1절의 시민인식 조사 결과에 따르면, 개인정보 유출과 같은 프라이버시 침해의 심각성을 묻는 질문에는 응답자의 82.2%가 ‘심각하다’고 응답했으나, 개인정보 취급 방침을 공개해야 한다는 사실을 아느냐는 질문에는 응답자의 20.6%, 개인정보 열람을 청구할 수 있다는 사실을 아느냐는 질문에 응답자의 24.2%만 ‘예’라고 답하였다. 이용자들은 개인정보 유출의 심각성에 대해서는 높은 우려를 가지고 있지만, 정보주체로서 지니는 권리내용에 대한 인지도는 낮은 것으로 나타난 것이다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다.<개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13>
2. “정보통신서비스”란 「전기통신기본법」 제2조제7호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.
3. “정보통신서비스 제공자”란 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
4. “이용자”란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
6. “개인정보”란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.
② 이 법에서 사용하는 용어의 뜻은 제1항에서 정하는 것 외에는 「정보화촉진기본법」으로 정하는 바에 따른다.<개정 2008.6.13>

위의 법적 정의에 따라 네이버를 운영하고 있는 NHN이나 다음을 운영하고 있는 다음커뮤니케이션은 정보통신서비스 제공자이며, 네이버나 다음에서 아이디를 만들어 각종 서비스를 이용하는 이들은 이용자이다. 그리고 이용자들이 포털을 이용하기 위하여 회원가입시 제공하는 정보가 개인정보이다. 개인정보 중에서 이메일, 사진, 음성의 경우 단독으로 사용되면 누군지 알 수 없다 하더라도 성명이나 주민등록번호가 결합된 상태의 정보라면 「정보통신망법」에 따라 개인정보로 분류 된다[70].

「정보통신망법」의 개인정보보호 관련 법령 제·개정 현황을 보면 다음과 같다(한국정보화진흥원, 2009: 328).

<표 2-29> 「정보통신망법」의 개인정보보호 관련법령 제·개정 현황

| 일자 | 제·개정 변경 사항 |
|---|---|
| 1999.2.8 | 정보통신서비스 이용자의 개인정보 수집 시 동의, 목적 외 이용 및 제3자 제공 금지 조항 신설 / 이용자 자신의 개인정보 열람 및 오류정정 요구권 신설 |
| 2000.1.16 | 정보통신서비스 제공자가 개인정보 위탁 시 수탁자의 행위에 대한 |

70) “이메일 주소는 당해 정보만으로는 특정 개인을 알아볼 수 없을지라도 다른 정보와 용이하게 결합할 경우 당해 개인을 알아볼 수 있는 정보라 할 것이므로 개인정보에 해당한다.” 서울중앙지법 2007.2.8. 선고 2006가합33062,53332 판결 : 항소【손해배상(기)】[각공2007.4.10.(44),816]

| | |
|---|---|
| | 책임 조항 신설 / 준용사업자를 규제 대상에 포함 / 14세 미만 아동의 개인정보 수집시 법정대리인의 동의 조항 신설 / 분쟁조정위원회 설립 및 운영 근거 조항 신설 |
| 2002.12.18 | 한국정보보호진흥원에 개인정보 침해시 자료제출 및 검사 권한 부여 조항 신설/개인정보 부정 목적으로 제공 받은 자 처벌 조항 신설 |
| 2004.1.29 | 개인정보 수집시 쿠키 설치에 대한 관한 사항 이용약관에 명시 조항 신설/개인정보 제3자에게 제공 내역 열람 요구 조항 신설/분쟁조정위원회에 5인 이하의 분쟁조정부 조항 신설 |
| 2004.12.30 | 정보통신부에서 개인정보보호기술의 개발 및 보급 시책 마련 조항 신설 |
| 2006.10.04 | 사업자 규모 및 서비스에 따른 개인정보관리책임자지정 조항 신설 / 사업자가 개인정보 오류 정정 요구에 대한 수용이 어려운 경우 필요한 조치를 취한 후 개인정보 제공 및 이용할 수 있도록 조항 수정 |
| 2007.1.26 | 개인정보의 수집·이용·제공에 대한 고지 및 동의제도 개선·보완 / 개인정보의 취급위탁에 따른 관리·감독 강화 |
| 2008.5.22 | 부당이득 환수를 위한 과징금제도 신설 / 과태료 부과대상의 벌칙으로 상향 조정/누설된 개인정보를 제공받는 자에 대한 처벌/주민등록번호를 사용하지 않는 회원가입방법 제공 의무화 |

### 3) 조사대상, 방법, 목적

본 연구에서는 네이버, 다음 등 주요 7개 국내 포털과 외국계 회사인 구글, MSN을 대상으로 개인정보 수집 및 유통실태를 조사하였다[71]. 이를 위해 각 포털의 약관과 개인정보 취급방침(2009년 7월 기준)을 상호 대조 및 분석하였으며, 포털의 이용자를 섭외하여 정보공개청구 및 정책질의를 통해 이용자의 열람 및 정정·삭제 청구권 보장 실태조사를 진행하였다. 이번 실태조사는 포털의 고객센터나 이메일을 통해 직접 질의를 하는 방식으로 2009년 7월 7일부터 9월 3일까지 진행되었다.

<표 2-30> 조사대상 사이트

(가나다순)

| 업체명 | 사이트주소 |
|---|---|
| 구글 | http://www.google.co.kr |
| 네이버 | http://www.naver.com |

71) 조사 대상 사이트는 네이버, 다음, 구글, 야후코리아, 싸이월드, 네이트, MSN코리아, 천리안, 파란. 조사 기간 중인 2009년 9월 28일 싸이월드와 네이트가 통합되었다.

| | |
|---|---|
| 네이트 | http://www.nate.com |
| 다음 | http://www.daum.net |
| 싸이월드 | http://www.cyworld.com |
| 야후코리아 | http://kr.yahoo.com |
| MSN코리아 | http://kr.msn.com |
| 천리안 | http://www.chol.com |
| 파란 | http://www.paran.com |

포털의 약관과 개인정보 취급방침에 대한 조사를 통해 △개인정보 필수수집 항목, △자동수집 항목, △「정보통신망법」에 규정된 개인정보 취급방침의 준수 여부 등을 파악하고자 했으며, 각 포털 이용자의 정보공개청구 및 정책질의 결과분석을 통해 실제 이용자의 열람및 정정·삭제 청구권 보장 실태를 조사하였다.

## 2. 개인정보 수집 실태

### 1) 필수수집항목

포털은 개인정보를 회원가입의 방식을 통해 수집하고 있으며, 수집방법 및 항목을 이용약관에 명시하고 있다. 그 중에서 포털을 이용하기 위해 반드시 입력해야 하는 항목을 '필수수집항목'으로 규정하고 이용자들로부터 수집하고 있다. 2007년부터 시행된 '제한적 본인확인제'로 인해 네이버, 다음 등 일일평균 이용자 10만 명 이상의 정보통신서비스제공자의 사이트에 회원 가입을 하기 위해서는 반드시 실명인증을 해야 한다[72]. 실명인증은 주민등록번호나 대체본인확인 수단인 i-PIN(Internet Personal Identification Number)을 통해 이루어지며. 실명인증을 한 이용자만이 포털에서 제공하는 게시판, 카페, 블로그, 덧글 등의 기능을 이용할 수 있다.

포털의 약관을 조사한 결과 각 포털의 필수수집항목 중에는 성명, 주민등록번호 이외에도 주소나 전화번호 등 포털서비스를 이용하는데 있어서 필수적이라 하기 힘든 정보들이 포함되어 있었다. 몇몇 포털은 약관에 직업이나

72) 2007년 7월 27일 시행시 공공기관 1365곳, 이용자수 20만 또는 30만 이상의 정보통신서비스를 제공하는 35개 사업자를 선정하여 통보하였다. 2008년 11월 시행령 개정 결과 제한적 본인확인제를 실시해야 하는 사이트는 일일방문자 수 10만 이상의 사이트로 범위가 확대되었고, 2009년 1월 30일 방송통신위원회에서 정보통신서비스 운영자 중 게시판 및 댓글 서비스를 제공하는 153개 사이트를 선정, 발표하였다.

성별 등 포털 이용과 전혀 무관한 정보들도 수집하고 있는 것으로 나타났다. 다음은 국내 대형 포털을 중심으로 조사된 개인정보 필수수집항목 목록이다. 조사 자료는 각 포털이 게시하고 있는 개인정보 취급방침 및 약관(2009년 7월 기준)을 근거로 하여 작성되었다.

<표 2-31> 주요 포털의 약관 기준 필수수집항목

(2009년 7월 기준)

| 업체명 | 필수수집항목 | | | | |
|---|---|---|---|---|---|
| | 성명 | 주민등록번호 | i-PIN 추가사항 | 주소 | ID |
| A | O + 본인확인문답 | O | 생년월일, 성별 | | O |
| B | O | 서비스제한 | | O | O |
| C | O | | i-PIN 미사용 | | |
| D | O | O | | O | O |
| E | O | O | | | O |
| F | O | O | | O | O |
| G | O | | i-PIN 미사용 | O | 이메일 아이디 |
| H | O | O | | O | O |
| I | O + 본인확인문답 | O | 중복가입정보, 생년월일, 성별, 내/외국인 구분 | | O |

| 업체명 | 필수수집항목 | | | | | |
|---|---|---|---|---|---|---|
| | 비밀번호 | 이메일 | 전화번호 | 생년월일 | 휴대폰번호 | 특이수집사항 |
| A | O | O | | | | |
| B | O | | O | O | O | 이동통신사, 성별 |
| C | O | O | | | | |
| D | O | | O | O | | 직업 |
| E | O | | O | | | |
| F | O | O | O | | | 직업 |
| G | | O | O | | | |
| H | O | O | | | O | |
| I | O | O | O | | | 뉴스레터/SMS 수신설정 |

외국계 회사인 C사와 G사를 제외한 국내 포털은 가입시 주민등록번호 또는 i-PIN을 필수적으로 수집하고 있다. B사의 경우 주민등록번호를 통해 실

명인증을 받지 않고 핸드폰이나 전화로도 가입이 가능하지만, 실명인증이 없을 경우 메일을 제외한 덧글, 까페 등 대부분의 포털 기능을 이용할 수 없다. 사실상 주민등록번호 또는 i-PIN을 입력해야만 포털을 이용할 수 있다. 「정보통신망법」에서는 다음과 같이 주민등록번호 외의 회원가입 방법을 규정하고 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제23조의2(주민등록번호 외의 회원가입 방법) ① 정보통신서비스 제공자로서 제공하는 정보통신서비스의 유형별 일일 평균 이용자 수가 대통령령으로 정하는 기준에 해당하는 자는 이용자가 정보통신망을 통하여 회원으로 가입할 경우에 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.
② 제1항에 해당하는 정보통신서비스 제공자는 주민등록번호를 사용하는 회원가입 방법을 따로 제공하여 이용자가 회원가입 방법을 선택하게 할 수 있다.
[본조신설 2008.6.13]

동법 시행령에서는 일일평균 이용자수의 기준을 두고 포탈 등 정보통신서비스 제공자로 하여금 주민등록번호 외의 회원가입 방법을 의무적으로 제공하게 하고 있다.

「정보통신망이용촉진및정보보호등에관한법률시행령」
제9조의2(주민등록번호 외의 회원가입 방법 제공 의무자 등) ① 법 제23조의2 제1항에서 "대통령령으로 정하는 기준에 해당하는 자"란 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 포털서비스(다른 인터넷주소·정보 등의 검색과 전자우편·커뮤니티 등을 제공하는 서비스를 말한다)의 경우는 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 5만명 이상인 정보통신서비스 제공자
2. 게임서비스(「게임산업진흥에 관한 법률」 제2조제1호 및 제1호의2에 따른 게임물과 사행성게임물을 정보통신망을 이용하여 제공하는 서비스를 말한다)의 경우는 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 1만명 이상인 정보통신서비스 제공자
3. 전자상거래 서비스(「전자상거래 등에서의 소비자보호에 관한 법률」 제2조제1호 및 제2호에 따른 전자상거래 및 통신판매를 정보통신망을 이용하여 제공하는 서비스를 말한다)의 경우는 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 1만명 이상인 정보통신서비스 제공자
4. 그 밖의 정보통신서비스의 경우는 전년도 말 기준 직전 3개월간의 일일평균 이용자수가 1만명 이상인 정보통신서비스 제공자

② 방송통신위원회는 법 제23조의2에 따른 주민등록번호 외의 회원가입 방법 제공에 필요한 준비기간, 적용기간 및 제1항 각 호에 해당하는 자 등을 인터넷 홈페이지에 게시하는 방법으로 공시하여야 한다.
[본조신설 2009.1.28]

이처럼 「정보통신망법」에서는 주민등록번호 이외의 회원가입 방법을 제공하게끔 규정하고 있으나 현재로서는 i-PIN 정도만이 주민등록번호 이외의 회원가입 방법으로 사용되고 있다[73]. 주민등록번호에는 번호 소지자의 생년월일 및 성별 등 민감한 개인정보가 포함되어 있으므로 주민등록번호의 수집은 번호가 표시하고 있는 내용으로 인해 개인식별을 넘어서는 정보를 수집하는 것이다. 또한 주민등록번호는 i-PIN과 달리 재발급이 불가능하기에 유출 시 개인의 사생활을 심대하게 침해할 수 있다.

주민등록번호의 수집 및 유출과 관련된 여러 사회적 문제가 불거지자 2005년 10월부터 방송통신위원회에 의해 대체본인확인 수단으로 도입된 i-PIN은 널리 확산되지 않고 있다. 4년이 지난 2009년 10월 현재 주요 포털의 i-PIN이용자 수는 전체 이용자의 0.2%도 안 되고 있으며[74], 2009년 9월 대한민국 인터넷 이용자 수가 약 3,658만 명임에 비해 2009년 6월 30일 기준 전체 i-PIN 발급건수는 약 110만 건이다. 중복발급을 감안하지 않더라도 i-PIN이용자는 전체 인터넷 이용 인구의 3% 수준에 머물고 있는 것이다[75]. i-PIN을 사용하기 위해서는 기존의 주민등록번호로 가입한 아이디를 해지한 후 다시 i-PIN을 이용해 포털에 가입해야 하는 불편함이 있고[76], 도입 초기의 i-PIN 1.0은 다섯 개의 발급기관[77]별로 따로 발급을 해 이용자가 본인발급기관을 확인해서 이용해야 했었다. 사업자 역시 주민등록번호와 달리 사이트 간 연계기능이 미비한 i-PIN 도입을 꺼려했다.

더욱이 주민등록번호를 대체하기 위해 도입했다는 i-PIN을 사용하기 위해서는 또다시 주민등록번호를 기입하여 이용자 인증을 받아야 한다. 따라서

---

73) "방통위는 주민등록번호 유출 및 피해 예방을 위해 개정된 정보통신망법령에 따라 지난 6월 주민번호 외 회원가입 수단을 도입해야 하는 대상 사업자로 1천39개 웹사이트를 공시하고 이들 사이트에서는 개인식별번호인 아이핀(i-PIN)만으로 가입이 가능하도록 했다." 연합뉴스. 2009.7.2. "주민번호 대체 i-PIN 2.0 설명회 개최".

74) 경제투데이. 2009.1.13. "네이버 등 주요 포털 '아이핀' 도입 1% 미만".

75) 한국인터넷진흥원. "「IP주소의 지역별 분류 가이드」에 대한 정보 공개 청구에 대한 답변". 2009.8.13.

76) 하나포스닷컴은 2009년 10월 21일 회원인증 없이 아이핀 가입을 할 수 있는 페이지를 열었다. http://help3.hanafos.com:9090/se/faq/Main.jsp

77) 행정안전부, 한국정보인증, 한국신용정보, 한국신용평가정보, 서울신용평가정보

주민등록번호의 유출을 막고자 하는 이용자가 또다시 주민등록번호를 입력해야 하는 부담감 또한 i-PIN의 확산을 어렵게 하였다. 어떤 포털의 경우 i-PIN으로 가입할 시 생년월일과 성별을 필수적으로 기입해야만 이용이 가능하게 하는 경우도 있었다. 이에 방송통신위원회는 이용절차의 통일, 가입절차의 간소화, 사이트 간 연계 확산, 온-오프라인 연동을 기반으로 한 i-PIN 2.0을 2009년 7월 7일부터 보급하기 시작했으나, 위에서 살펴본 바와 같이 이용자수의 확산에 어려움을 겪고 있는 중이다.

몇몇 포털은 주소나 연락처(전화, 휴대폰) 또한 필수적으로 수집하고 있다. 포털에서는 수집의 목적을 서비스 및 회원관리 등으로 한정하고 있지만, 대부분의 포털 서비스 고지가 메일을 통해 이루어지고 있는 현 상황에서 주소나 연락처가 포털 이용에 있어서 필수적이라 판단하긴 어렵다. 주소 및 연락처가 필요한 경우의 대부분은 인터넷 상에서 거래 및 물물 교환을 할 경우인데, 대부분의 거래는 거래당사자간 필요정보를 주고받음으로써 이루어진다. 현재는 거래가 발생할 시 포털이 아닌 금융관련기관이나 기타 인증기관을 통해 거래의 안전성이 확보되고 있는 상황이다. 이용자들이 포털에서 주로 사용하는 게시판, 블로그, 카페, 덧글 등에 있어서도 연락처나 주소가 필수적이라 보기 힘들며, 이처럼 포털의 이용에 필수적이지 않은 정보를 강제적으로 수집 및 집적하는 것은 불필요하며 개인정보 유출에 따른 위험부담도 가중시킨다. 성별이나 직업의 수집 역시 마찬가지이다.

따라서 포털의 이용에 항시적으로 필요한 정보가 아닌 한 선택정보 항목으로 옮겨 이용자로 하여금 정보기입을 선택할 수 있게 해야 한다. 주소 및 연락처의 경우에도 이러한 정보가 없을 시 발생할 서비스 이용의 제한 및 불이익을 명시한 후 선택정보로 옮겨 놓아야 한다. 이를 통해 이용자가 개인정보 제공과 서비스 이용 제한 사이에서 선택할 수 있게 해야 한다.

### 2) 자동수집항목

자동수집항목은 이용자의 생성정보(인터넷 이용 시 이용자에 의해 발생하는 정보, 쿼리, 이용정보, IP정보, 쿠키 등) 중 포털에서 기계적으로 수집하는 정보의 목록이다. 포털은 생성정보를 자동으로 수집해 이용자의 이용 패턴을 분석하고 이를 기반으로 광고마케팅 및 맞춤서비스를 하는 등의 수익 사업을 한다. 자동수집 항목 중에서 이용자의 현재 위치 정보를 대략적으로 드러내는 IP정보나, 이용자가 어떤 서비스를 이용했는가 하는 선호와 빈도를 알 수 있는 쿠키정보의 경우 그 수집 및 운용실태에 대한 사회적 관심도가 높아지

고 있다.

다음은 국내 대형 포털을 중심으로 조사된 개인정보 자동수집항목 목록이다. 조사자료는 각 포털이 게시하고 있는 개인정보 취급방침(2009년 7월 기준)을 근거로 하여 작성되었다.

<표 2-32> 주요 포털의 약관 기준 자동수집항목

(2009년 7월 기준)

| 업체명 | 자동수집항목 | | | | | |
|---|---|---|---|---|---|---|
| | 접속로그 | IP Address | 불량이용기록 | 쿠키 | 브라우저유형/버전 | 특이수집사항 |
| A | O | O | O | O | | |
| B | O | O | O | O | | |
| C | O | O | | O | O | URL |
| D | O | O | O | O | | |
| E | O | O | O | O | | 결재기록 |
| F | O | O | O | O | | 결재기록 |
| G | O | O | | O | O | 웹 탐지장치 |
| H | | | | O | | |
| I | | | | O | | |

<표 2-32>은 고시된 개인정보취급방침을 정리한 것이다. 그러나 각 포탈이 고시한 내용이 포탈이 무엇을 자동으로 수집하는가를 정확하게 보여준다고 할 수는 없다. 왜냐하면 접속로그에는 접속일시와 IP주소, 브라우저 유형/버전, 유입된 사이트 경로 등이 모두 기록 될 수 있다. 따라서 위의 표에서 브라우저 유형/버전, URL 등이 취급방침 상에 명시 되지 않았다 하여 수집되지 않는다고 보기는 어렵다. 이런 수집의 목적을 포털은 약관상에서 '불량이용 방지와 보다 나은 서비스의 제공을 위함'이라 밝히고 있다. 이용자는 포털 사이트 내에서 자신이 어떤 IP로 언제 어떤 서비스를 이용하고 있는지 확인할 수 있는 페이지가 마련되어 있어 자신의 생성정보 중 몇 가지를 확인할 수 있다[78].

IP Address(IP주소)에서 IP란 Internet Protocol의 약어로 인터넷상의 컴퓨터 주소라 할 수 있다. 컴퓨터가 인터넷에 연결되면 해당 연결 주소가 할

78) 네이버 로그인 기록보기 서비스:
https://nid.naver.com/user/help.nhn?a=privateInfo&m=certLoginLog
다음 로그인 기록 https://user.daum.net/daumuser/loginhistorylist.daum

당되는데 이것이 IP주소이다. 현재 우리나라의 경우 각 기간통신사업자가 IP를 분배하고 있고, 포털에서는 기간통신사업자의 망을 이용해 접속하는 이용자들의 IP주소를 로그기록을 통해 파악하고 있다. IP주소의 지역적 분배 정보를 알 수 있다면, 이를 통해 포털은 이용자의 대략적인 위치정보를 파악할 수 있으며, 이렇게 파악된 위치정보를 기반으로 지역별 맞춤 광고나 선거 시기 후보자 광고, 날씨 등을 알려주는 서비스를 하게 된다.

접속 로그(서버 로그)를 통해 포털은 사이트 운용과 관련한 여러 정보 등을 취합한다. 포탈은 서비스 이용 기록이나 불량 이용 기록을 통해 포털 서비스 개선 및 외부의 공격 시도 대응 등을 한다고 밝히고 있다. 그러나 접속 로그나 불량이용기록의 구체적인 항목에 대해서는 공시하지 않고 있다. 구글에서 접속 로그의 한 예[79]를 볼 수 있었다.

쿠키 또한 자동수집 항목 중 상세내역이 고지되지 않고 있다. 쿠키란 인터넷 웹사이트(웹 서버)와 인터넷 이용자(웹 브라우저) 자신의 컴퓨터 사이에서 통신을 매개 해주는 정보를 기록하는 것을 말한다. 쿠키에는 이용자의 행적이 담겨 이용자 컴퓨터의 하드디스크에 저장된다. 이용자가 다시 해당 사이트에 접속하면 이 사이트의 서버는 이용자 컴퓨터에 있는 쿠키를 불러 이용자가 누구인지, 어떤 정보를 많이 찾았는지 파악할 수 있다.

조사대상이 된 모든 포털은 이용자들로 하여금 쿠키의 설치/운영 및 거부

---

79) http://www.google.co.kr/intl/ko/privacy_glossary.html

서버 로그

대부분의 웹사이트와 마찬가지로 Google 서버는 사용자가 Google 사이트를 방문할 때 요청한 페이지를 자동으로 기록합니다. 이러한 "서버 로그"에는 일반적으로 웹 요청, 인터넷 프로토콜 주소, 브라우저 유형, 브라우저 언어, 요청 날짜 및 시간, 사용자의 브라우저를 고유하게 식별할 수 있는 하나 이상의 쿠키가 포함됩니다.

다음은 "car"를 검색한 경우 전형적인 로그 항목의 예를 보여줍니다. 그 아래에는 각 부분에 대한 자세한 설명이 나와 있습니다.

```
123.45.67.89 - 25/Mar/2003 10:15:32 -
http://www.google.com/search?q=cars -
Firefox 1.0.7; Windows NT 5.1 - 740674ce2123e969
```

* 123.45.67.89는 사용자의 ISP에서 사용자에게 할당한 인터넷 프로토콜 주소입니다. 사용자의 서비스에 따라 서비스 제공업체는 사용자가 인터넷에 접속할 때마다 다른 주소를 할당할 수 있습니다.

* 25/Mar/2003 10:15:32는 검색 날짜 및 시간을 나타냅니다.

* http://www.google.com/search?q=cars는 요청된 URL(검색어 포함)입니다.

* Firefox 1.0.7; Windows NT 5.1은 사용 중인 브라우저와 운영체제입니다.

* 740674ce2123a969는 특정 컴퓨터가 Google을 처음 방문했을 때 컴퓨터에 할당된 고유한 쿠키 ID입니다. (사용자는 쿠키를 삭제할 수 있습니다. 사용자가 Google을 마지막으로 방문한 이후에 컴퓨터에서 쿠키를 삭제한 경우 이 쿠키는 다음에 사용자가 특정 컴퓨터에서 Google을 방문할 때 사용자에게 할당되는 고유한 쿠키 ID가 됩니다.

를 선택사항으로 두고 있다. 거의 모든 브라우저에서도 쿠키와 관련하여 자동저장, 확인 후 저장, 저장안함 등의 선택사항을 제공하고 있다. 포털은 쿠키 저장을 거부할 경우 로그인이 필요한 일부 서비스의 이용이 제한된다고 개인정보 취급방침을 통해 밝히고 있다. 일반적인 인터넷 이용자들에게 있어 쿠키가 무엇인가에 대한 이해가 낮고 쿠키 미사용에 따른 불이익이 명확하지 않다는 점을 생각해 본다면 이용자가 일부러 쿠키 거부를 선택할 개연성은 낮다. 대부분의 인터넷 이용자의 컴퓨터에서 쿠키가 운용되고 있다고 할 수 있는 것이다. 조사 대상이 된 포털에 쿠키의 내용 및 구체적인 운용과 관련한 질의를 보냈지만, 포털 측에서는 자사의 영업비밀이라는 이유로 공개를 거부하였다.

## 3. 개인정보 유통 실태

### 1) 「정보통신망법」 관련 개인정보 취급방침 분석

포털에서 개인정보 유통의 핵심은 취급위탁과 제3자 제공일 것이다. 개인정보 취급위탁이라 함은 포털에서 해야 할 업무를 다른 개인이나 업체에 의뢰하여 처리하기 위해 개인정보를 넘기는 것이고, 제3자 제공이라 함은 포털의 업무와 무관하게 기업 이벤트나 회원 확대의 등을 위해 다른 업체에 개인정보를 제공하는 것을 말한다. 「정보통신망법」에서는 다음과 같이 제3자 제공을 규정하고 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제24조의2(개인정보의 제공 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
② 제1항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

또한 「정보통신망법」에서는 다음과 같이 개인정보의 취급방침을 공개하

도록 규정하고 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제27조의2(개인정보 취급방침의 공개) ① 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보 취급방침을 정하여 이용자가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
② 제1항에 따른 개인정보 취급방침에는 다음 각 호의 사항이 모두 포함되어야 한다.
1. 개인정보의 수집·이용 목적, 수집하는 개인정보의 항목 및 수집방법
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인인 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적과 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 파기방법(제29조 각 호 외의 부분 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
4. 개인정보 취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에만 취급방침에 포함한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항
7. 개인정보 관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처
③ 정보통신서비스 제공자등은 제1항에 따른 개인정보 취급방침을 변경하는 경우에는 그 이유 및 변경내용을 대통령령으로 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아 볼 수 있도록 조치하여야 한다.

### 2) 분석 결과 정리

다음은 이에 따른 각 포털의 개인정보 취급방침을 조사한 항목이다.

아래 조사대상에 포함된 포털 중 국내포털의 경우 「정보통신망법」 제27조의2(개인정보 취급방침의 공개)를 비교적 잘 준수하고 있는 것으로 나타난다. 포털의 경우 포털에서 제공하는 서비스의 특성 상 이벤트나 인수/합병의 절차 중 이용자의 동의를 구하는 경우가 아닌 한 가입절차를 통해 이용자의 개인정보를 수집한다. 따라서 1.0, 1.1 항목인 수집이용목적, 항목, 방법에 있어서 개인정보를 자의적으로 수집·유통을 할 우려는 다른 업체에 비해 상대적으로 낮은 편이다.

<표 2-33> 각 포털 개인정보 취급방침 조사항목

(2009년 7월 기준)

| 업체명 | 「정보통신망법」 제27조의2(개인정보 취급방침의 공개)에 따른 조사항목 | | | | |
|---|---|---|---|---|---|
| | 1.0 수집이용목적 | 1.1 수집 항목/방법 | 2.0 제3자 성명(법인명) | 2.1 제3자 이용목적/항목 | 3.0 보유/ 이용기간 |
| A | O | O | O | O | O |
| B | O | O | O | O | O |
| C | O | O | 미기재 | 항목 미기재 | 미기재 |
| D | O | O | 미기재 | 항목 미기재 | O |
| E | O | O | 미기재 | 항목 미기재 | O |
| F | O | O | 미기재 | 항목 미기재 | O |
| G | O | O | 미기재 | 항목 미기재 | 미기재 |
| H | O | O | O | 항목 미기재 | O |
| I | O | O | O | O | O |

| 업체명 | 「정보통신망법」 제27조의2(개인정보 취급방침의 공개)에 따른 조사항목 | | | | |
|---|---|---|---|---|---|
| | 3.1 파기절차/방법 | 4.0 위탁업무 내용/ 수탁자 | 5.0 이용자 및 법정대리인의 권리/행사방법 | 6.0 자동수집장치의 설치/운영/거부 | 7.0 관련 연락처 |
| A | O | O | O | 쿠키 | O |
| B | O | O | O | 쿠키 | O |
| C | 각 서비스 별도 | 미기재 | 미기재 | 쿠키 | O |
| D | 삭제신청 | O | O | 쿠키 | O |
| E | O | O | O | 쿠키 | O |
| F | O | O | O | 쿠키 | O |
| G | 각 서비스 별도 | 미기재 | O | 쿠키 | O |
| H | O | O | O | 쿠키 | O |
| I | 탈퇴신청 | O | O | 쿠키 | O |

2.0 항목을 보면, 포털은 개인정보를 제공하는 제3자의 성명이나 법인명을 기재하지 않은 경우가 많았다. 이용자 입장에서 민감할 수 있는 제3자 제공의 경우 제공사가 없을 시에는 없다는 것을 명확히 기재할 필요가 있다. 또한 제3자 제공 시 이용자의 동의를 받는다는 내용만 게시 하는데 그칠 것이 아니라 보다 정확한 정보를 이용자에게 제공해야 한다. 현재 제공을 하고 있는지, 제공을 하였다가 계약이 파기되어 현재는 게시를 하지 않는 상태인지에 대한 구체적인 언급을 통해 정보주체인 이용자에게 정확한 정보를 제공해

야 할 필요가 있다.

2.1항인 제3자 이용목적/항목 중 항목이 미기재 되어있는 것 또한 문제이다. 제3자 제공을 할 경우 제공되는 항목에 무엇이 포함되어있는지를 분명히 하지 않는다면 이용자로서는 제3자 제공시 어떤 정보가 제공되는지 알 수가 없다. 참고로 네이버의 제3자 제공 항목[80]을 보면 각 제공업체, 제공목적, 제공항목 및 보유기간 등이 명시되어 있다. 다음 역시 서비스, 이벤트 별로 구체적인 제3자 제공내역을 공시[81]하고 있다.

3.0 항목, 개인정보의 보유 및 이용기간의 경우 각 포털별로 회원 탈퇴시 부정이용방지 등의 목적으로 일부 개인정보를 1년 정도 보유하고 있으며, 그 외에 관련 법령에 의해 다음과 같은 개인정보를 일정 기관 보유하고 있다.

서비스 이용기록, 접속 로그, 접속 IP 정보 : 3개월 (통신비밀보호법)
표시/광고에 관한 기록: 6개월 (전자상거래등에서의 소비자보호에 관한 법률)
계약 또는 청약철회 등에 관한 기록: 5년 (전자상거래등에서의 소비자보호에 관한 법률)
대금결제 및 재화 등의 공급에 관한 기록: 5년 (전자상거래등에서의 소비자보호에 관한 법률)
소비자의 불만 또는 분쟁처리에 관한 기록: 3년(전자상거래등에서의 소비자보호에 관한 법률)

이에 따라 수집된 개인정보가 결재나 온라인상의 민원관련 기록과 함께 3~5년간 포털에 보유되고 있다. 결재나 민원기록은 이용자의 주소, 아이디, 이름, 전화번호, 주민등록번호, 카드나 계좌번호 등의 금융정보 등이 포함되어 있어 유출시 이용자의 피해 정도가 포털에서 일반적으로 수집하는 정보에 비해 크다. 이러한 정보들의 긴 보유기간은 포털의 입장에서도 부담이 될 뿐만 아니라, 이용자의 입장에서도 일상적인 상품 구매 기록이 주민등록번호, 성명, 주소 등의 개인정보와 함께 저장된다는 것은 과도하다 할 수 있다.[82]

---

80) 네이버 개인정보의 공유 및 제공 http://www.naver.com/rules/privacy_pop.html
81) 다음 개인정보 제공 동의 서비스 제공내역:
http://www.daum.net/doc/service_offer_list.html
다음 개인정보 제공 동의 이벤트 제공내역:
https://user.daum.net/privagree/childservicelist.do?svcId=67&codeName=event
82) 공정거래위원회는 2009년 8월 7일 「전자상거래 등에서의 소비자보호에 관한 법률」일부개정법률(안)을 입법예고했다. 개정안에 따르면 전자상거래 사업자가 보존해야 하는 개인정보 관련 예시 항목인 성명, 주소, 주민등록번호를 삭제하여 사업자들이 주민등록번호 등을 보존하는 근거로 오용함을 방지하는 것을 목적으로 한다.

3.1 파기 방법, 5.0 이용자 및 법정대리인의 권리와 행사방법에 대해 포털은 개인정보 취급방침에서 그 내용을 공시하고 있다. 그러나 해지자의 개인정보 미파기, 법정대리인의 요건에 맞지 않는 자를 법정대리인으로 등록하는 등의 개인정보 유용행위가 발생하였고 방송통신위원회는 유용행위를 한 포털에 대해 시정조치 및 과태료를 부과하였다(방송통신위원회, 2008d).

## 4. 정보주체의 열람 및 정정·삭제 청구권 보장 실태

### 1) 조사 개요

「정보통신망법」은 정보통신서비스제공자(ISP)의 의무뿐만 아니라, 개인정보와 관련한 이용자의 권리를 다음과 같이 규정하고 있다.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
제30조(이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.
② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.
1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황
③ 정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.
④ 정보통신서비스 제공자등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.
⑤ 정보통신서비스 제공자등은 제2항에 따라 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그 개인정보를 제공하거나 이용할 수 있다.
⑥ 정보통신서비스 제공자등은 제1항에 따른 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집 방법보다 쉽게 하여야 한다.
⑦ 영업양수자등에 대하여는 제1항부터 제6항까지의 규정을 준용한다. 이 경우 “정보통신서비스 제공자등”은 “영업양수자등”으로 본다.

[전문개정 2008.6.13]

개인정보 이용·제공 등의 동회철회, 열람 및 정정, 제3자 제공내역 등을 규정한 「정보통신망법」 제30조를 바탕으로 이용자가 포털을 상대로 「정보통신망법」에 규정된 대로 이용자의 권리를 행사할 수 있는지를 확인하기 위해 각 포털을 대상으로 정보주체 열람청구를 진행하였다. 아울러 각 포털의 개인정보 수집·유통과 관련된 정책을 질의하였다.

열람청구 대상은 포털사이트 네이버, 다음, 구글, 야후코리아, 싸이월드, 네이트, MSN코리아, 천리안, 파란으로 각 포털의 이용자를 섭외하여 진행하였다[83]. 정보공개청구 및 정책질의는 각 포털의 고객센터나 이메일을 통해 직접 질의를 하는 방식으로 2009년 7월 7일부터 9월 3일까지 진행되었다. 각 포털에 문의한 사항은 다음과 같다.

1. 문의자의 개인정보 일체
2. 문의자의 각 개인정보 파일의 종류/목적/개인정보항목 일체/보유 혹은 삭제 기간
3. 문의자의 쿠키 정보, IP주소 등 자동수집항목의 상세한 내용
4. 타겟마케팅을 위해 문의자와 관련하여 분석된 정보 예) 성별, 지역, 선호도 등
5. 문의자가 웹사이트 상에서 확인 가능한 개인정보와 확인할 수 없는 개인정보
6. 문의자의 개인정보가 비 로그인 시에도 IP매칭 등을 통해 저장된 정보와 통합 관리되는지 여부
7. 문의자의 개인정보 파일을 귀사 내 어느 부서/직책의 몇 사람이 열람/조회하고 있는지
8. 문의자의 각 개인정보 파일에 대한 정정이나 파기 방법
9. (2009년 6월 31일 기준) 지난 3년간, 문의자의 각 개인정보 파일을 포함한 문의자의 개인정보를 제공/공유한 제3자 존재 여부, 과거와 현재의 위탁업체를 비롯한 해당 기관/개인의 이름과 제공/공유 목적
10. 문의자의 개인정보중 특히 수사기관에 형사소송법에 의해 이메일 등이 압수수색되었거나 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등에 따라 제공된 여부(통신비밀보호법에 따른 감청/통신사실확인자료 제공과 별도)

이를 통해 「정보통신망법」에서 규정하는 이용자 권리의 보장 여부, 자동

83) C사의 경우 답변이 오지 않음. H사의 경우 문의자의 주민등록번호를 요구하여 진행 불가.

수집되는 항목(쿠키, IP주소)의 개인정보 연동 여부, 이용자 개인정보의 제3자 제공 여부 등을 파악해보았다.

### 2) 조사 결과 분석

<표 2-34> 각 포털별 개인정보 열람청구 및 정책질의 결과

| 업체명 | 각 포털별 개인정보 열람청구 및 정책질의 문의사항 답변내용 | | | | |
|---|---|---|---|---|---|
| | 1. 개인정보 일체 | 2, 개인정보 파일 종류/목적/항목/보유기간 | 3. 자동수집항목 상세 내역 | 4. 문의자 분석정보 | 5. 개인정보 확인 가능/불가 정보 |
| A | 회원정보페이지 확인 | 가입시 정보외에 없음 | 영업비밀 공개불가 | 통계정보 활용, 타겟마케팅 없음 | 회원정보페이지 확인 |
| B | 무응답 | 개인정보 취급방침 참조 | 개인정보 취급방침 참조 | 통계정보 활용, 타겟마케팅 없음 | 확인불가기록은 통계정보로만 활용된 것들 |
| D | 제공 | 개인정보 취급방침 참조 | 개인정보 취급방침 참조 | 통계정보 활용 | 회원정보페이지 확인 |
| E | 무응답 | 개인정보 취급방침 참조 | 개인정보 취급방침 참조 | 통계정보 활용 | 회원정보페이지 확인, 불가능 정보는 자동수집정보 |
| F | 무응답 | 개인정보 취급방침 참조 | 개인정보 취급방침 참조 | 통계정보 활용 | 회원정보페이지 확인, 불가능 정보는 자동수집정보 |
| G | 회원정보페이지 확인 | 개인정보 취급방침 참조 | 개인정보 취급방침 참조 | 무응답 | 무응답 |
| I | 회원정보페이지 확인 | 개인정보 취급방침 참조 | 쿠키와 IP외에 없음 | 없음 | 회원정보페이지 확인 |

| 업체명 | 각 포털별 개인정보 열람청구 및 정책질의 문의사항 답변내용 | | | | |
|---|---|---|---|---|---|
| | 6. 개인정보 IP매칭 | 7. 개인정보 열람/조회자 | 8. 개인정보 삭제/정정 방법 | 9. 제3자 제공 이름/내역/목적 | 10. 수사기관 제공여부 |
| A | IP정보는 개인정보 아님[84] | 공개불가 | 공개 | 공개 | 확인 및 공개 |
| B | IP정보는 개인정보 아님 | 공개불가 | 공개 | 공개 | 공개불가 |
| D | 개인정보 취급방침 참조 | 최소인원 | 공개 | 공개 | 확인 및 공개 |
| E | IP정보는 개인정보 아님 | 연락요망 | 무응답 | 위탁업체만 공개 | 공개불가 |
| F | IP정보는 개인정보 아님 | 연락요망 | 무응답 | 위탁업체만 공개 | 공개불가 |
| G | 개인정보 취급방침 참조 | 무응답 | 계정중지 270일 후 삭제 | 개인정보 취급방침 참조 | 확인 및 공개 |
| I | IP매칭정보 활용되지 않음 | 공개불가 | 공개 | 공개 | 공개불가 |

1번 문항, 개인정보 일체의 제공 요청과 관련해서 포털들은 회원정보페이지에서 직접 확인하라는 답변을 많이 보냈다. 포털의 경우 이용자가 회원정보페이지에서 자신의 개인정보를 직접 열람·정정할 수 있기 때문인 것으로 추측된다. 이 질의의 목적은 온라인 회원정보페이지에서 열람할 수 있는 개인정보 외의 개인정보를 포털이 보유하고 있는지 여부 및 그 열람 가능성을 파악하기 위한 것이었다. 이에 대해 포털들은 자신들이 보유하고 있는 개인정보는 회원정보페이지에서 열람할 수 있는 것 뿐 이라고 답변한 것이다.

2번 문항, 포털이 보유하고 있는 개인정보 파일의 종류와 목적을 질의한 이유는 이용자가 포털에 가입될 시 기입한 개인정보를 포털이 어떻게 보관하는지(어떤 파일로 만드는지, 어떤 DB를 생성하는지), 가입 시 기입하는 정보 외에 다른 개인정보 파일이 있는지, 어떠한 목적으로 개인정보 파일들을 사용하는지를 물어본 것이었다. 포털들은 대부분 개인정보 취급방침에 명시된 개인정보만을 수집하고, 개인정보 취급방침에 명시된 목적으로만 사용한다는 답변을 보내왔다.

쿠키나 IP주소 등의 구체적인 저장내용이 무엇인가를 물어보는 3번 문항에 대해 포털들은 그저 개인정보 취급방침을 참조하라는 답변을 보내왔다. 재질의를 통해 쿠키에 저장되는 상세내용을 특정해서 물어본 경우 쿠키는 개인정보와 연동되지 않기에 개인정보가 아니므로 구체적인 내용을 제공할 필요가 없으며, 쿠키의 세부 항목은 자사의 영업비밀이므로 공개가 불가능하다는 답변이 돌아왔다.

개인정보 분석정보(성별, 지역, 선호도)등을 제공해 달라는 4번 문항에 대해 포털에서는 이용자의 개인식별 정보가 제거된 상태에서 통계정보나 타겟 마케팅 용으로 활용된다는 답변을 보내왔다. 이용자의 개인식별 정보가 사라진 상태이므로 개인정보로서 판단할 수 없고 따라서 정보주체의 열람요구에 대해 응할 이유가 없다는 것이다.

5번 문항, 웹상에서 확인할 수 있는 개인정보와 확인할 수 없는 개인정보의 유무를 묻는 것에 대해 포털은 ① 웹상에서 확인할 수 있는 정보는 회원정보밖에 없으며 ② 확인불가기록은 개인식별 정보가 없는 통계정보로서 영업상 대외비에 속한다는 대답을 했다. 대부분의 포털에서 개인정보는 로그인 과정을 거치면 확인이 가능하다. 각 포털이 이용자의 이용관련 통계를 운용

84) IP정보는 개인정보가 아니며 따라서 IP정보와 개인정보를 매칭하느냐의 질의에 대해서 대답 할 수 없다는 뜻.

하고 있으며 그것이 개인식별 정보가 제거된 상태에서 운용된다면 이는 개인정보라 규정하기 힘들다.

개인정보와 IP주소를 매칭 여부를 6번 문항에서 물어보았다. 포털은 IP주소는 개인정보가 아니기에 제공할 수 없으며 개인정보 취급방침에 나와 있는 것 이외의 수집목적은 없다고 밝혔다. 그런데 B업체는 광고주들을 상대로 한 웹상에 공개된 문서에서 한국인터넷진흥원을 통해 IP주소를 받고 이를 다시 회원 로그인 IP주소와 통합하여 지역정보 타겟마케팅[85]을 한다고 밝히고 있다. 포털에 IP주소 정보를 제공하는지 여부를 파악하기 위해 한국인터넷진흥원에 정보공개를 청구한 결과, “한국인터넷진흥원은 관리대행자(ISP)에게 IP주소를 할당하며 관리대행자(ISP)는 일반사용자 고객에게 IP주소를 할당”한다는 답변이 왔다. “IP주소의 지역별 분류 가이드는 없”으며 “IP주소 할당에 대한 개별 지역정보는 관리대행자(ISP)가 보유”하고 있다고 한국인터넷진흥원은 밝혔다. 한국인터넷진흥원이 지정한 관리대행자 목록을 살펴본 결과 B업체 등의 포털은 포함되어 있지 않았다. 이에 한국인터넷진흥원이 B업체에 IP주소 정보를 제공하고 있지 않음에도, 어떻게 현재 B업체에서 IP주소 정보를 제공받으며 이를 통해 타겟마케팅을 하고 있는가에 대하여 재차 B업체에 문의한 결과, B업체측은 영업비밀이라는 이유로 답변을 거부하였다.

개인정보 파일의 열람·조회자를 묻는 7번 질문에 대해 대부분의 포털이 영업비밀이라는 이유로 대답하지 않았다.

개인정보의 삭제 및 정정 방법을 묻는 8번 질문에 대해서는 각 포털별로 방법을 대답해왔다. 대부분의 포털은 회원탈퇴 및 회원정보수정의 과정을 통해 개인정보의 삭제 및 정정이 가능했다.

문의자의 개인정보를 제3자에게 제공했다면, 제공받은 제3자의 이름, 제공된 개인정보 내역, 제공의 목적을 묻는 9번 문항에 대해 포털은 이용자의 제공내역을 확인하여 답변해주었다. 약관이나 개인정보 취급방침에서 제3자 제공사를 밝히지 않은 포털의 경우 이번 질의에서도 위탁업체만을 명시했다.

문의자의 이메일이나 개인정보 등을 수사기관에 제공했느냐는 10번 문항에 대해 포털별로 ①확인 결과 제공한 적 없다, ②관계법령에 의해 확인해 줄

85) 각 이용자의 접속 지역 IP정보를 기반으로 한 개인별 맞춤 서비스. 선거기간동안의 각 지역별 후보자의 광고가 로그인 없이도 바로 보인다거나 지도검색 초기 화면이 각 이용자의 현재 위치지역이 보이는 경우, 꽃이나 음식 배달 등을 알아보기 위해 검색을 하면 현재 이용자 위치 중심의 검색결과가 나오는 경우 등을 지역기반 타겟 마케팅을 이용한 사례라 할 수 있다. 이러한 지역기반 타켓 마케팅을 하기 위해서는 IP주소 및 IP주소의 지역별 할당을 맡고 있는 관리대행자가 제공하는 개별 지역정보가 필요하다.

수 없다는 대답을 보내 왔다. 포털별 정책에 따라 확인 및 확인내역을 제공해주는 곳과 확인자체가 관계법령에 의해 불가능하다는 상반된 태도를 보인 것이다.

B업체의 경우 확인이 불가능한 이유를 “형사소송법, 통신비밀보호법, 전기통신사업법에 따른 정보 제공 여부는 개별적인 비밀유지의무에 따라 제공된 사실 여부를 확인해드릴 수 없다”고 들고 있다. I업체의 경우 다음과 같이 답변하였다. “통신비밀보호법을 확인해보시면 [통신사실확인자료]를 범죄수사를 위한 수사기관에 제공하는 경우(제13조), 법원에 제공하는 경우(제13조의2), 정보수사기관에 제공하는 경우(제13조의4) 등을 규정하면서, 그러한 제공 사실 자체를 비밀로 유지할 의무를 규정하고 있습니다(제13조의5). 동법 제3조제1항에서 보면, 그 공개금지의 대상이 제한되지 않았으므로 이메일 발송자에 대해서도 위 비밀유지의무는 그대로 적용된다고 볼 수 있으며, 수사의 기밀성을 유지한다는 목적을 고려한다면 이와 같이 해석하는 것이 타당하다고 봅니다(가사 향후 법원에서 달리 해석한다고 하더라도, 아직까지 이에 관한 유권해석이 없는 상태에서 당사가 위 명시적 법령 의무를 위반하여 공개를 할 수도 없다는 점을 양해해 주시기 바랍니다). 또한, 법률에는 명시되어 있지 않습니다만, 2007년 당시 정보통신부와 한국정보보호진흥원에서 제작한 개인정보보호와 i-PIN 가이드에 따르면 전기통신사업자는 가입자에게 통신사실확인자료 등을 수사기관에 제공한 사실 등을 통지하여서는 아니 되며, 기타 외부에 이를 누설하여서도 안된다고 명시[86]되어 있습니다.”

통신비밀보호법에서 통지 제도를 두고 있는 취지로 살펴보건대 자신의 개인정보가 수사기관에 제공되었는지 여부를 이용자가 통지받을 수 있는 권리가 있다는 점은 명백하다. 다만 통신비밀보호법, 전기통신사업법, 형사소송법 등 관련 법률이 이 부분에 있어 포털 등 사업자의 의무를 모호하게 처리한 측면이 있다. 이에 수사기관으로의 개인정보 제공 여부를 답변하지 않은 포

86) 정보통신부. 2007. "통신사실확인자료 및 통신자료 제공 FAQ". 57p 참조.
(2) 경찰에 정당한 절차에 따라 회원의 통신사실확인자료를 제공하였습니다. 그런데 나중에 그 회원이 자신의 통신사실확인자료를 경찰에 제공했는지 알려 달라고 합니다. 어떻게 해야 합니까?
통신사실확인자료 또는 통신자료의 제공여부를 본인에게 알려도 되는지에 대해 통신비밀보호법, 전기통신사업법은 명문의 규정을 두고 있지 않습니다. 그러나 통신사실확인자료 또는 통신자료의 제공취지가 범죄수사, 형의집행, 국가안전 보장에 대한 위해방지 등임을 고려하여 볼 때, 제공사실을 본인에게도 통보한다면 이는 제도의 취지를 훼손하는 것이 될 수 있습니다.
따라서 전기통신사업자는 해당 가입자에게 통신사실확인자료 등을 수사기관에 제공한 사실 등을 통지하여서는 아니되며, 기타 외부에 이를 누설하여서도 안됩니다.

털들을 대상으로 다시 한 번 정보제공을 요구하였으나, 1차 질의와 같은 이유로 거부하는 답변을 보내왔다.

서울지방법원은 2009년 10월 18일 “통신비밀보호법에는 검찰에게 통신기록 조회에 대한 통지 의무를 부과하고 있을 뿐, 당사자가 검찰이 조회한 통신기록을 열람할 수 있는 근거 규정이 없다”며 “통신기관의 직원은 수사기관에 제공한 통신사실확인자료를 외부에 공개하거나 누설해선 안 될 의무가 있다”고 밝혔다[87]. 그러나 2009년 상반기동안 통신감청 799건, 인터넷 로그기록 등 통신사실확인자료 12만6천371건, 가입자 인적사항 같은 통신자료 28만1천221건 등 총 41만여 건의 자료가 국정원과 검경・군수사 기관 등에 넘어갔다. 같은 기간 동안 네이버(NHN)・다음・네이트/싸이월드(SK커뮤니케이션)・야후코리아・파란(케이티하이텔KTH)에 본인의 정보가 수사기관 등에 제공됐는지 확인을 요청한 건수는 7건에 불과했다(김창수, 2009). 수사기관 제공 41만 건 대 제공확인 7건이라는 수치의 불균형은 이용자들의 자기정보 결정권에 대한 인식이 낮음과 자기정보 제공내역에 대한 정보주체의 권리를 보장하지 않는 법적 미비 등이 복합된 결과이다. 현행 「통신비밀보호법」 제13조의3[88]은 30일 이내에 이용자에게 수사기관이 통보하는 것과 포털측의 비밀준수의무만을 규정하고 있을 뿐, 제공내역을 열람할 수 있는 정보주체의 권리에 대해서는 어떠한 규정도 하고 있지 않다.

포털의 공식적인 답변들을 종합해 볼 때, 포털에서는 가입 시 수집한 개인정보에 대한 DB만 구축하고 있는 것으로 보인다. 포털측은 로그인 시 이용정보와 비로그인시 이용정보를 매칭하여 관리하지 않는다고 공식적으로 답변하였다. 타겟 마케팅은 이용자가 포털 가입 시 입력한 기본 정보(성별, 나이, 지역)에서 개인정보를 제거한 통계정보와 IP주소를 근거로 이루어지고 있는 것으로 보인다. 포털측은 이용자의 포털 이용 패턴과 이용자의 개인정보 DB가 서로 연동되어 관리되지는 않는다고 밝혔다. 개인정보와 로그인시 이용패턴의 연동에 대해서는 현재 새로운 서비스가 등장하고 있다.[89]

---

87) 서울중앙지방법원 2009.10.13 선고 2009가합27655 【열람등사】.

88) 제13조의3 (범죄수사를 위한 통신사실 확인자료제공의 통지) ①제13조의 규정에 의하여 통신사실 확인자료제공을 받은 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 통신사실 확인자료제공을 받은 사실과 제공요청기관 및 그 기간 등을 서면으로 통지하여야 한다.
②제1항에 규정된 사항 외에 통신사실 확인자료제공을 받은 사실 등에 관하여는 제9조의2(동조제3항을 제외한다)의 규정을 준용한다.

89) http://history.search.naver.com/ 네이버 검색히스토리 서비스, 2009.10.13.

## 5. 소 결

포털이 제공하는 개인정보 취급방침은 「정보통신망법」이 요구하는 각각의 항목들을 나열하고 있다. 개인정보 및 자동수집항목에 있어서 보다 구체적인 저장방식과 설명, 예시 등이 제공된다면 정보주체인 이용자들이 자신의 개인정보와 생성정보가 어떻게 수집 및 유통되는지에 대해 명확한 상을 가지게 될 것이다.

포털은 정보주체의 질의에 대해 답변을 회피하거나, 질문에 대한 내부처리 지침을 문의자에게 잘못 보내기도 했으며, 광고상으로 이용자의 로그데이터나 IP주소정보를 이용해 광고주를 상태로 마케팅을 하고 있으면서도 이러한 사실의 확인을 거부하는 경우도 있었다. 동일한 법 적용을 받는 포털 간에도 이용자의 통신내용이나 통신사실을 수사기관이나 제3자에 제공했느냐는 질의에 대해 서로 다른 대답을 하였다. 어떤 포탈은 적극적이고 구체적으로 취급실태를 공개하고 있는 반면, 다른 곳은 구체적이지 않은 태도를 보인 곳도 있었다. 이러한 차이는 각 포탈 나름의 법 해석에 기인한 것으로서 포털의 개인정보 취급 실태에 대한 구체적인 가이드라인이 제공 될 필요가 있다.

과도한 개인정보 수집 및 주민등록번호 등의 보유문제 또한 지적할 수 있다. 과도한 개인정보의 수집은 포탈에게 개인정보 관리 부담을 가중시키며 해킹의 위협에 노출되게 만든다. 포털의 입장에서도 최소한의 개인정보만으로 서비스를 운용하는 것이 부담도 덜하고 이용자를 안심시키는 방법이 될 것이다. 직업이나 학력, 성별 등 포털 서비스를 이용하는데 있어 필요 없는 개인정보는 더 이상 수집되지 말아야 하며 기존의 불필요한 정보들은 삭제되어야 한다. 연락처, 계좌번호, 카드번호 등 유출시 피해가 우려되는 정보들은 적어도 주민등록번호와 연계되지 않는 방식으로 저장되어야 한다.

우리 사회에서 포털의 역할이 사회적 논의와 정보소통의 중심이라는 것을 생각해 본다면 포털역시 준(準)공적 성격을 가지고 있다. 더욱이 거대 포털이 보유한 개인정보는 네이버의 회원수가 3,300만 명, 다음(Daum)의 회원수는 3,500만 명으로 대한민국 국민 거의 대부분이라 해도 과언이 아니다. 그러나 이번 연구 결과에서 보듯이 포털은 영업비밀 속에 많은 내용들을 숨기려 해 그 규모와 사회적 위상에 걸맞지 않는 모습을 보였다. 포털들이 이용자들의 개인정보와 생성정보를 통해 이익을 얻으면서 동시에 그러한 정보를 제공하

---

로그인 상태에서 검색한 검색어가 정리되어 이용자에게 제공되며, 이용자에게 자신이 사용한 검색어 빈도수 및 사이트 접속 통계 등을 제공한다.

는 정보주체 이용자들에게는 폐쇄적인 모습을 보이는 것은 스스로가 기업의 외형만을 강조하는 것이다. 포털이 가지는 사회적 역할과 중요성을 생각할 때 이용자의 개인정보를 다룸에 있어서 이용자와 포털, 양자 간에 균형을 찾아야 하며, 이용자의 권리를 존중하고 보다 많은 내용들이 공개되어야 한다.

## II. 이동통신사 및 초고속인터넷업체

### 1. 개 요

우리나라 이동전화 보급률은 2008년 기준으로 94.8%에 이른다. 초고속인터넷 서비스의 경우, 2008년 기준으로 KT는 약 670만 명의 초고속 인터넷 가입자를 보유하고 있으며, SK브로드밴드는 약 354만 명, LG파워콤은 약 220만 명의 가입자를 보유하고 있다(한국정보화진흥원, 2009). 더구나 이동통신 및 초고속인터넷 서비스가 통합되는 추세[90]를 고려하면, 이들 통신 그룹들은 거의 전 국민에 대한 개인정보를 분할하여 보유하고 있다고 볼 수 있다.

<표 2-35> 연도별 통신서비스 가입자 수

(단위: 천 명)

| 구분 | 시내전화서비스 | 이동통신서비스 | 인구수(이동전화보급률(%)) |
|---|---|---|---|
| 1999 | 20,712 | 26,605 | 46,617 (57.1) |
| 2000 | 21,932 | 27,589 | 47,008 (58.7) |
| 2001 | 22,725 | 29,554 | 47,357 (62.4) |
| 2002 | 23,490 | 32,774 | 47,622 (68.8) |
| 2003 | 22,877 | 34,050 | 47,859 (71.1) |
| 2004 | 22,871 | 37,054 | 48,039 (77.1) |
| 2005 | 22,920 | 38,819 | 48,138 (80.6) |
| 2006 | 23,119 | 40,658 | 48,297 (84.2) |
| 2007 | 23,130 | 43,970 | 48,456 (90.7) |
| 2008[p] | 22,132 | 46,092 | 48,607 (94.8) |

※ 1. p는 잠정치임(2010년초 연보결과에 따라 변할 수 있음)

90) 지난 2008년 SKT가 하나로텔레콤을 인수한데 이어, 2009년 6월 1일에는 KT와 KTF가 합병하였으며(디지털타임즈. 2009.6.1. “합병 KT 공식출범”), 2009년 11월 27일에는 LG텔레콤, LG데이콤, LG파워콤 등 LG그룹 통신3사가 합병하였다. (한국일보. 2009.11.27. “LG '통신삼총사' 합병 승인”)

2. 보급률 = 서비스 가입자 수/총 인구 수 (통계청)
3. 이동통신서비스 = 이동전화 + 무선호출 + TRS + 무선데이터통신
자료: 지식경제부·방송통신위원회·KEA·KAIT. 각 연도. 정보통신산업통계연보.

<표 2-36> 초고속인터넷 가입자 수 현황

(단위: 천 가구, %)

| 사업자 | 2003 | 2004 | 2005 | 사업자 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|---|---|
| KT | 5,589 (50.2) | 6,078 (51.0) | 6,242 (51.2) | KT | 6,353 (45.2) | 6,516 (44.3) | 6,712 (43.4) |
| 하나로텔레콤 | 2,726 (24.2) | 2,749 (23.1) | 2,773 (22.7) | SK브로드밴드 | 3,613 (25.7) | 3,658 (24.9) | 3,544 (22.9) |
| 두루넷 | 1,293 (11.5) | 1,288 (10.8) | 837 (6.9) | | | | |
| 온세통신 | 423 (3.5) | 391 (3.3) | 353 (2.9) | 온세텔레콤 | 220 (1.6) | - | - |
| 드림라인 | 150 (1.3) | 134 (1.1) | 100 (0.8) | 드림라인 | 28 (0.2) | 1.5 | 0.4 |
| 데이콤 | 202 (1.8) | 206 (1.7) | 213 (1.8) | LG데이콤 | 112 (0.8) | 67.8 (0.5) | 28.6 (0.2) |
| LG파워콤 | - | - | 262 (2.1) | LG파워콤 | 1,204 (8.6) | 1,721 (11.7) | 2,182 (14.1) |
| 부가/별정 | 796 (7.2) | 1,075 (9.0) | 1,411 (11.6) | 종합유선방송 | 2,262 (16.1) | 2,507 (17.0) | 2,786 (18.0) |
| | | | | 중계유선방송 | 15 (0.1) | 16 (0.1) | 13 (0.1) |
| | | | | 전송망(NO) | 55 (0.4) | 58 (0.4) | 50 (0.3) |
| | | | | 별정통신사업자 | 180 (1.3) | 164 (1.1) | 158 (1.0) |
| 합계 | 11,178 | 11,921 | 12,191 | - | 14,043 | 14,710 | 15,475 |

※ ( )안은 각 년도 점유율(각 연도 말 기준).
자료: 방송통신위원회. 2009.2. “초고속인터넷가입자 수”.

이렇게 집적된 개인정보는 업무 위탁 등을 통해 타 업체에 제공되며, 텔레마케팅을 위한 수단으로 이용되기도 한다.[91] 특히 타겟 마케팅의 중요성이 부각되고 그 기법이 고도화되면서 좀 더 정확하고 많은 개인정보 수집에 대

한 요구도 증가하고 있다. 또한, 다양한 업체들이 제휴 등을 통해 새롭고, 복합적인 서비스를 내놓으면서 개인정보 수집, 제3자 제공 등의 경계도 모호해지고 있다. 이에 따라 본인의 동의없는 개인정보의 수집 및 제3자 제공, 개인정보의 유출과 유용 등의 위험성도 커질 수밖에 없다.

이 절에서는 이동통신 및 초고속인터넷 서비스 영역에서의 개인정보 수집·유통 실태를 검토하였다. KT show, SK텔레콤, LG텔레콤 3개 이동통신사와 KT(Qook), SK브로드밴드, LG파워콤 등 3개 초고속인터넷업체를 대상으로 조사를 하였다. 아래 본문에서는 이를 A/B/C이동통신사, A/B/C초고속인터넷업체로 표시하였는데, 앞서 열거한 순서와는 무관하다.

## 2. 개인정보 수집·유통 실태

### 1) 개인정보의 수집

이동통신 및 초고속인터넷 서비스 가입 시, 개인정보를 제공하게 된다. 이동통신 및 초고속인터넷 서비스 역시 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 「정보통신망법」)의 적용을 받기 때문에, 각 통신업체들은 개인정보 취급방침을 통해 수집되는 개인정보의 종류, 수집 목적, 수집 방법 등을 공개하고 있다.

수집되는 개인정보의 종류는 각 업체마다 유사하다. 기본적으로 △ 신청인 및 (미성년자의 경우) 법정대리인의 이름, 주민등록번호 등 식별정보, △ 주소, 전화번호 등 연락처 정보, △ 신청인 혹은 요금납부자의 주민등록번호, 계좌정보, 신용카드 등 요금결제 관련 정보, △ 요금감면대상 등의 확인을 위한 증명서류 등이다.

통신업체들은 이와 같은 기본 정보와 함께, 서비스 이용 과정에서 생성되는 생성정보를 보유하고 있다. 생성정보에는 △ 접속 로그, 접속 IP, 쿠키 등 서비스 이용기록, △ 결제정보, △ 이용정지기록 등이 포함된다. 특히, 이동통신 서비스의 경우에는 발·수신번호, 통화시각, 사용도수, 위치정보(기지국위치, GPS정보) 등이 이용기록에 포함된다. IPTV 서비스의 경우에는 유료 콘

91) 통신분야의 경우 대규모의 개인정보 수집 및 활용이 발생함에 따라 수집 및 이용 자체를 주로 외부 기관에 위탁 수행하는 경우가 많았으며 이와 더불어 이미 수집한 막대한 양의 개인정보를 활용하여 새로운 서비스의 마케팅에 활용하거나 제휴관계를 통해 개인정보를 제공하고 그에 대한 수익을 얻는 구조가 대부분인 것으로 나타났다(정연수, 2004: 130).

텐츠 이용기록도 포함될 수 있다. 한 이동통신사의 개인정보 취급방침[92]에 의하면, 이동전화 및 무선인터넷의 서비스 사용 통계(호접속, 호절단, 호실패시 망환경, 다운로드 실행오류, 무선인터넷 접속실패 및 접속시간 등) 및 사용 패턴 정보(메뉴 이동경로, 주로 이용하는 서비스, 서비스 이용횟수, 사용량 등)도 수집되고 있었다.

그런데 포털업체와 마찬가지로 개인정보 취급방침에는 '생성정보'에 어떠한 개인정보가 포함되는지 구체적으로 나와 있지 않다. 또한 각 통신업체들은 초고속인터넷, 인터넷전화, 전화, IPTV, 이동통신 등의 결합상품을 출시하고 있음에도 불구하고, 각 서비스별로 구분해서 제시하지 않고 있는 것은 문제이다.

정보통신부가 제정하여 2005년 10월 1일 시행된 「이동통신서비스제공자의 개인정보 보호 지침」에 따르면, 개입정보의 수집은 서비스 제공에 필요한 최소한의 정보를 수집해야 하며, 필수항목과 선택항목으로 구분하도록 하고 있다.

제4조(개인정보 수집의 제한) ①이동통신서비스제공자는 적법하고 공정한 수단에 의하여 서비스 제공에 필요한 범위 내에서 최소한의 정보를 수집하여야 한다.
②이동통신서비스제공자는 제1항의 규정에 따라 최소한의 정보를 수집하기 위하여 다음 각호와 같이 필수항목과 선택항목으로 구분하여 당해 가입고객이 선택적으로 자신의 개인정보를 제공할 수 있는 조치를 취하여야 한다.
1. 필수항목
가. 서비스 계약 유지를 위해 필요한 정보 : 성명, 주민번호, 주소, 전화번호, 단말기 일련번호 등

---

92) 개인정보 자동수집장치의 설치, 운영 및 그 거부방법
회사는 고객님의 정보를 수시로 저장하고 찾아내는 '쿠키(cookie)', 이동전화 및 무선인터넷의 사용 기록(이하 "통계데이터")을 자동으로 수집하는 장치를 설치·운영할 수 있습니다.
<중략>
② 통계데이터란?
이동전화 및 무선인터넷 서비스 이용시 단말기의 특정영역에 저장되고, 주기적으로 회사의 서버로 전달되는 아래와 같은 정보입니다. - 서비스 사용 통계(호접속, 호절단, 호실패시 망환경, 다운로드 실행오류, 무선인터넷 접속실패 및 접속시간 등) - 사용 패턴 정보(고객님의 메뉴 이동경로, 주로 이용하는 서비스, 서비스 이용횟수, 사용량 등) 고객님께서는 서비스 제공에 관한 회사의 계약이행을 위하여 필요한 경우와 요금정산을 위하여 필요한 경우 및 법령에서 정한 경우를 제외하고 단말기의 통계데이터 차단 옵션을 통하여 회사의 통계데이터 수집·이용을 거부할 수 있습니다.
<후략>

나. 이용요금 정산을 위해 필요한 정보 : 계좌이체의 경우 예금주명・은행명・계좌번호, 신용카드결제의 경우 신용카드이용자명・카드종류・카드번호
2. 선택항목 : 이메일 주소 등 필수항목 이외에 서비스 제공을 위하여 필요한 정보
③이동통신서비스제공자는 가입고객이 선택항목에 해당하는 개인정보를 제공하지 아니한다는 이유로 당해 서비스 제공을 거부하여서는 아니된다.

그러나 A이동통신사와 B이동통신사의 개인정보취급방침 '개인정보의 수집항목 및 이용목적'을 보면, 필수항목과 선택항목의 구분이 되어 있지 않다. C이동통신사의 경우에는 필수와 선택항목을 구분하기는 하였지만, 웹사이트 가입을 위해 수집하는 고객명, 생년월일, 로그인 ID, 비밀번호, 비밀번호 질문과 답변, 자택 전화번호, 자택주소, 휴대전화번호, 이메일 주소, 직업, 결혼여부, 주민등록번호, 닉네임, 학력, 추천인 ID를 모두 필수번호로 분류하여, 지나치게 광범위한 개인정보를 필수정보로 수집하고 있었다.

### 2) 개인정보의 이용 및 제3자 제공

(1) 개인정보 제3자 제공 현황

통신업체들은 업무 위탁이나 업무 제휴 등을 통해 타 업체에 고객들의 개인정보를 제공하는 경우가 많다. 고객의 개인정보를 제공받는 업체는 크게 취급위탁 계약을 맺은 수탁자와 제3자로 구분될 수 있다. 고객 관리나 장애처리 등 자신의 서비스 계약을 이행하기 위해 개인정보를 제공하는 것이 '취급위탁'이라며, 새로운 상품의 판매와 같이 또 다른 목적을 위해 개인정보를 제공하는 것이 '제3자 제공'이다. 「정보통신망법」에서도 이를 구분하고 있다. 「정보통신망법」 제24조의2는 제3자 제공을 규정하고 있으며, 제25조는 개인정보의 취급위탁을 규정하고 있는데, 제3자 제공의 경우가 더욱 엄격하다. 즉, 취급위탁의 경우에는 수탁자와 위탁업무 내용을 알리고 동의를 얻어야 하지만, '정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 경우'에는 '개인정보 취급방침'으로 공개하거나 전자우편 등을 통해 알린 경우에는 고지와 동의절차를 거치지 않아도 된다. 반면, 제3자 제공의 경우에는 개인정보를 제공받는 자, 이용 목적, 제공하는 개인정보의 항목, 개인정보 보유 및 이용 기간 등을 알리고 동의를 얻어야 한다.

「정보통신망법」
제24조의2(개인정보의 제공 동의 등) ①정보통신서비스제공자는 이용자의 개인

정보를 제3자에게 제공하려는 경우 제22조제2항제2호 및 제3호의 규정에 해당하는 경우를 제외하고는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
②제1항의 규정에 따라 정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

제25조(개인정보의 취급위탁) ①정보통신서비스제공자와 그로부터 제24조의2제1항의 규정에 따라 이용자의 개인정보를 제공받은 자(이하 “정보통신서비스제공자등”이라 한다)는 제3자에게 이용자의 개인정보를 수집·보관·처리·이용·제공·관리·파기 등(이하 “취급”이라 한다)을 할 수 있도록 업무를 위탁(이하 “개인정보취급위탁”이라 한다)하는 경우에는 다음 각 호의 사항 모두에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
1. 개인정보취급위탁을 받는 자(이하 “수탁자”라 한다)
2. 개인정보취급위탁을 하는 업무의 내용
②정보통신서비스제공자등은 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항의 규정에 따라 공개하거나 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지한 경우에는 개인정보취급위탁에 따른 제1항의 고지 및 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.
③정보통신서비스제공자등은 개인정보취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는 이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.
④정보통신서비스제공자등은 수탁자에 대하여 이 장의 규정을 위반하지 아니하도록 관리·감독하여야 한다.
⑤수탁자가 개인정보취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시킨 경우에는 그 수탁자를 손해배상책임에 있어서 정보통신서비스제공자등의 소속직원으로 본다.

동법에 따라, 통신업체들은 ‘개인정보 취급방침’을 통해 개인정보를 제공받는 제3자(업체) 및 위탁업체를 공개하고 있다. 제3자 제공의 경우 제공받는

자, 제공목적, 제공정보의 종류 등을 구분하여 공개하고 있으며, 위탁처리의 경우 수탁자 및 위탁업무내용을 공개하고 있다. 통신업체들이 요금결제, 이용료 정산, 본인 인증, 제휴 서비스, 콘텐츠 서비스 등의 목적으로 개인정보를 제공하는 타 업체의 수는 수백 개에 이른다. 또한, 수많은 대리점 혹은 판매점을 운영하고 있기 때문에, 업무위탁을 통해 개인정보를 제공하는 업체 수는 대리점 등을 포함하여 무려 1000~2000개에 달한다.

예를 들어, 한 이동통신업체가 개인정보를 제공하는 제3자 업체의 목록 및 위탁업체의 목록은 다음과 같다.

<표 2-37> 한 이동통신업체가 개인정보를 제공하는 제3자 업체의 목록

| 제공받는자 | 제공목적 | 제공정보종류 | 보유 및 이용기간 |
|---|---|---|---|
| 국민카드, 금융결제원, 롯데카드, 삼성카드 등 12개사 | 신용카드 자동이체 | 전화번호, 카드번호, 유효기간, 주민등록번호 등 | 정보 제공일 부터 서비스 해지 또는 제공 계약 종료 일 중 먼저 도래하는 시점까지 이 용 하 며, 이용 기 간 이 종료 한 시 점 에 파기. 단, 다른 법령에 특별한 규정이 있을 경우 관련 법령에 따라 보관. |
| 국민카드, 금융결제원, 롯데카드, 삼성카드 등 11개사 | 신용카드 즉시납부 | 전화번호, 카드번호, 유효기간, 주민등록번호 등 | |
| KIBNET | 요금 즉시출금 요청, 환불 | 주민등록번호, 계좌번호 등 | |
| 경남은행, 광주은행, 국민은행, 금융결제원 등 24개사 | 은행자동이체 출금 및 출금의뢰 정정 서비스 | 전화번호, 주민등록번호 등 | |
| 금융결제원 | 지로 수납 | 청구계정번호, 지로번호, 전자납부번호, 금액 등 | |
| 미래신용정보, 한국신용정보, 한국신용평가정보 | 채권추심 | 전화번호, 고객명, 주민등록번호, 주소 등 | |
| 국민은행, 기업은행, 농협, 대구은행 등 11개사 | 모바일(VM)/ 뱅크온 뱅킹 서비스 | 전화번호 | |
| 경남은행, 광주은행, 부산은행, 수협 등 6개사 | 뱅크온 뱅킹 서비스 | 전화번호,모델명 | |
| 에이티솔루션, 유라클 | BANK-ON 증권 | 전화번호,모델명 | |
| LIG 손해보험 | 보험가입 | 전화번호, 주민등록번호 | |
| 한국인터넷진흥원 | 스팸 신고자 정보제공 및 이용제한 업무처리 | 스팸 신고된 고객명, 전화번호, 주민등록번호 | |
| 이지투게더 | 철도공사SMS티켓서비스 | 고객명, 모델명 등 | |

| | | | |
|---|---|---|---|
| 하이플러스 카드 | 충전카드 발급 및 수수료정산 | 고객명, 주민등록번호 | |
| LG파워콤 | 파워콤 결합서비스 | 고객명, 주민등록번호, 전화번호, 주소 등 | |
| 한화리조트㈜ | 한화리조트 콘도/영화/여행상품 할인제공 *마이콘도/레저요금제 가입 고객에 한함 | 고객명, 전화번호, 주민등록번호, 주소 등 | |
| 아시아나 항공㈜ | 항공마일리지 제휴 서비스 제공 | 고객명,전화번호, 주민등록번호, e-mail 주소 | |
| 갤럭시아커뮤니케이션즈, 다날, 모모캐쉬, 모빌리언스 등 9개사 | 휴대폰 소액결제 승인관리 | CTN과 명의자 주민등록번호 일치여부 정보, 휴대폰요금 연체정보, 단말기모델명, 휴대폰 소액결제 이용한도 정보 | |
| 주식회사 G마켓 | G마켓 할인 제휴서비스 가입 | 전화번호, 주민등록번호 | |
| GS칼텍스 | GS칼텍스 보너스 (GS &point)카드 이용 및 주유할인을 위한 인증수단 *주유할인 프로그램 가입 고객에 한함 | 전화번호, 주민등록번호, e-mail 주소 등 | |
| 갤럭시아커뮤니케이션즈, 다우기술, 롯데정보통신, 메트라이프생명보험 등 17개사 | 모바일광고 서비스 (Mobiletown 설문조사 서비스) | 전화번호, 주민등록번호 인증 | |
| 모지트, 비온시스템 | 모바일 레저 회원권 서비스 | 전화번호, 모델명 | |
| 누토커뮤니케이션즈, 로코모, 바인아이엔지, 블루인포 등 11개사 | 모바일복권 서비스 | 전화번호,주민등록번호 | |
| 옥션, 칼라짚테크놀로지 | 모바일 옥션서비스 제공 | 전화번호, 모델명 | |
| 대우증권, 로코모, 매경인터넷, 아이넥스 등 10개사 | 우리투자, 현대증권 VM 서비스 | 전화번호,모델명 | |
| 이지 투게더, 코레일 | 철도 티켓 예매 서비스 제공 | 전화번호, 주민등록번호, 모델명 등 | |
| 엠씨페이, 엠필러, 인포 | 휴대폰인증서 | 전화번호,고객명,주민등 | |

| | | | |
|---|---|---|---|
| 바인, 제노모바일 등 7개사 | | 록번호,모델명 | |
| 메타미디어, 서울시청, LG CNS, NHN | 서비스제공을 위한 회원인증 | 전화번호 조회/LGT 고객인지 조회/SID로 CTN 조회/CTN으로 SID 조회 | |
| 강일리테일, 광신엔터프라이즈, 글레어주드, 대한통운 등 31개사 | 손안에 서비스 주문 상품 판매 및 배송 | 전화번호, 배송정보(수령자명, 주문상품, 주소) | |
| 광주극장, 광주엔터시네마, 논산시네마, 대구아카데미 등 66개사 | 영화예매 서비스 제공 *멤버십 고객에 한함 | 고객명, 전화번호, 주민등록번호, ID | |
| (유)엔와이텔, (재)강원정보문화진흥원, (주)게임로프트, (주)모빌씨앤씨 등 244개사 | 컨텐츠 공급, 서비스, 이벤트 운영 | 전화번호, 주민번호 일부 등 | |
| 네모텔, 네비웨이, 동부엔티에스, 북토피아 등 15개사 | 컨텐츠 공급, 이벤트 진행 | 인증정보,고객설정정보, 이용내역 | |
| 네오위즈, 에듀박스, 엠조이넷, 한빛소프트 등 5개사 | 쿠폰 상품 발송 | 전화번호 | |
| 이니텍, BCN | MOTP | 전화번호 | |
| 티모넷 | 모바일티머니 서비스 | 전화번호,모델명 | |
| 핑거 | 모바일학생증 서비스 | 전화번호,모델명 | |
| KT | 국제전화 사용료 청구 | 고객명, 전화번호, 주민등록번호, 주소 등 | |
| 나래텔레콤, 몬티스타텔레콤, 삼성네트웍스, 세종텔레콤 등 13개사 | 국제전화 요금정산 | 고객명, 주민등록번호 | |
| LIG 손해보험 | 휴대폰보험(분실/파손) 가입, 보험처리 *휴대폰 보험 가입 고객에 한함 | 고객명, 전화번호, 주민등록번호, 주소, 모델명, 일련번호 등 | |
| 파민스 | 휴대폰분실보험 가입안내 및 휴대폰보험(분실/파손) 상담 *휴대폰보험 안내 동의 및 가입 고객에 한함 | 고객명, 전화번호, 성별, 모델명, 일련번호 등 | |
| 서울보증보험 | 휴대폰 할부 보증보험 가입 및 보험처리 *휴 | 고객명, 전화번호, 주민등록번호, 주소, 모델명 | |

| | | | |
|---|---|---|---|
| | 대폰 할부구매 고객에 한함 | | |

<표 2-38> 한 이동통신업체가 개인정보를 제공하는 취급위탁 업체의 목록

| 수탁자 | 위탁업무내용 |
|---|---|
| 아인텔레서비스, CS리더 | 고객상담 및 관리 등 |
| 와이드모바일, 케이티하이텔솔루션 | 로밍서비스 신청 |
| 미래신용정보, 한국신용정보, 한국신용평가정보 | 채권추심 |
| 나온웍스, 넷진테크, 섬넷, 엔텔리아 등 15개사 | 네트워크 시스템 운영 및 유지보수 |
| 대경넷, 민원감동사, 바이토넷, 비엠텍 등 9개사 | 통화품질 민원처리, 네트워크 유지보수 |
| NH모바일, (유)온정보통신, (유)전북무선통신, (유)제우스텔레콤 등 1032개사 | 이동통신, 부가서비스 판매 등 |
| 리서치 인터네셔널, 마케팅 인사이트, 코리아 리서치 센터, 테일러 넬슨 소프레스 등 5개사 | 서비스 만족도 조사 |
| YBL | 멤버쉽카드 제작 발송 대행 |
| 티앤비아이 | 멤버십 관련 Hot Line(콜센터)운영 |
| 라온팩토리, 모비엠, 새얀아이엔씨, 애드사운드 등 9개사 | 비즈링 영업 대행 |
| 디지털다임, 메가존, 씨네로, 엔터케이투어 등 7개사 | 홈페이지 등 온라인 이벤트 마케팅 대행 |
| 디지털다임, 야후, 옴니텔 | 대기화면서비스 운영, 이벤트진행, 경품지급 |
| 지어 소프트 | 메시징서비스 운영 |
| 엠넷미디어 | 뮤직온,동영상서비스 운영 |
| 매드인코리아, 피플링크 | 비즈링 서비스 운영 |
| 옴니텔 | 생활문자 등 서비스 운영 |
| 인터랙티비, 팻마우스 | 손안의쇼핑,모바일 광고 및 메시지쿠폰 운영 |
| 데이콤멀티미디어인터넷 | 유무선 인터넷 서비스 개발, 운영 및 정산 |
| 로코모, DMI | 증권타운,위젯증권서비스 운영대행 |
| (주)아레오커뮤니케이션즈, (주)포엠시스, 가바플러스, 기주I&T 등 10개사 | 컨텐츠 공급, 서비스 운영 |
| 텔코인 | 홈페이지 문자서비스 운영 |
| 한국신용평가정보 | 실명인증, 신용정보 조회 |

| | |
|---|---|
| 금융결제원, LG데이콤 | 자동이체 등록계좌 유효성 인증 |
| 에프알에스 | 중고폰 재생 |
| 대흥엠엔티 | 중고폰 폐기 |
| 미니스톱, 바이더웨이, 세븐일레븐, 훼밀리마트 등 5개사 | 요금수납 |
| 한국정보통신산업협회 | 방송통신신용정보 공동관리 등 |
| 아이투에스, 조우니 | 청구서 |
| ㈜밸류포인트 | CRM, 우편물 발송 |
| 네오플러스, 두잇시스템, 디지털베이시스템, 메가존 등 26개사 | 전산시스템 운영/개발 |
| 메가존 | 홈페이지 개발,운영 |

이와 같이 무수히 많은 제3자에게 개인정보를 제공하는 과정에서 개인정보가 수집 목적 외로 활용되거나 유출될 가능성도 높아지게 된다.[93] 수백만 명의 고객 정보를 전자적인 방식으로 보유하고 있는 통신업체의 특성 상 대량의 피해가 발생할 가능성이 높으며, 개인정보가 한번 유출되면 2차·3차의 피해를 연쇄적으로 야기할 수 있으며, 고객의 신용정보를 포함하고 있기 때문에 재산상의 손해를 발생시킬 가능성도 크다.[94]

(2) 개인정보의 유용 - 하나로텔레콤 사례를 중심으로

지난 2008년 4월, 서울지방경찰청이 '하나로텔레콤의 600만 명의 고객 개인정보 유출 사건'을 발표한 이후, 통신업체의 개인정보 관리 부실문제가 크게 주목을 받았다. 이후 방송통신위원회는 초고속인터넷업체, 포털, 이동통신사 등에 대한 개인정보 관리실태 점검[95]에 들어갔으며, 대부분의 업체들이

93) 방통위 한 관계자는 "최근 개인정보 유출 경로를 역추적했더니 이동전화 판매점이나 온라인 번호이동, 초고속인터넷 텔레마케팅처럼 사업자와 2~3단계 떨어진 유통 과정에서 유출되는 게 대부분이었다"며 "개선책을 찾고는 있지만 정부의 규제정책이 먹히기 어렵고 통신사업자를 통해 강제할 수도 없는 경우가 많아 뾰족한 대안을 찾지 못하고 있다"고 말했다. 파이낸셜뉴스. 2008.10.8. "['유통의 덫'에 빠진 통신시장] ③ 통제불능 유통망."

94) 더구나, 신용사회, 정보화사회가 급속하게 진전됨에 따라 개인정보 도용에 따른 문제는 ① 피해의 연쇄성(1회의 개인정보 도용으로 2차·3차의 피해가 발생됨) ② 피해의 대량성(전자적인 방법으로 대량의 개인정보 도용이 가능해짐) ③ 신용정보와의 관련성(신용정보와 관련된 개인정보 도용으로 재산상의 손해가 직접 발생함) 등을 특징으로 하고 있다(공정거래위원회, 2008).

95) 방송통신위원회는 2008년 5월부터 SK브로드밴드(舊하나로텔레콤)에 대한 조사를 시작으로, 6월에는 KT, LG파워콤 등 2개 초고속인터넷사업자, 9월에는 4개 복수종합유선방송사업자 및 4개 포털사업자, 10월부터는 3개 이동전화사업자 등 총 14개사에 대

방송통신위원회의 제재를 받았다.

<표 2-39> 개인정보 유용행위 등에 대한 방송통신위원회 시정조치 현황

| 업체명 | 시정조치 내용 | 시정조치 이유 |
|---|---|---|
| 하나로텔레콤 | '08.7.1~8.9일까지(40일간) 신규가입자 모집정지 | 개인정보 유용 |
| KT | '08.8.30~9.28(30일간) 신규가입자 모집정지 | 개인정보 유용 |
| LG파워콤 | '08.8.30~9.28(30일간) 신규가입자 모집정지 | 개인정보 유용 |
| SKT | 과태료 5,000만 원 | 고객정보를 동의 없이 또는 고지 없이 취급 위탁한 행위, 해지자 개인정보를 파기하지 않은 행위 등 |
| KTF | 과태료 3,000만 원 | 고객정보를 동의 없이 취급 위탁한 행위, 동의철회 고객에 대해 필요한 조치를 하지 않은 행위 등 |
| LGT | 과태료 5,000만 원 | 고객정보를 동의 없이 또는 고지 없이 취급 위탁한 행위, 해지자 개인정보를 파기하지 않은 행위 등 |
| 티브로드한빛방송 | 과태료 3,000만 원 | 초고속인터넷 가입자 정보를 동의 없이 또는 고지 없이 취급 위탁한 행위 및 기술적·관리적 조치미비 |
| CJ헬로비젼 | 과태료 1,000만 원 | 개인정보 전송 시 암호화 조치 미흡 등 기술적·관리적 조치미비 |
| 씨엔엠 | 과태료 3,000만 원 | 초고속인터넷 가입자 정보를 동의 없이 또는 고지 없이 취급 위탁한 행위 및 기술적·관리적 조치미비 |
| 큐릭스 | 과태료 3,000만 원 | 초고속인터넷 가입자 정보를 고지 없이 취급 위탁한 행위, 해지자 개인정보를 파기하지 않은 행위 및 기술적·관리적 조치미비 |
| NHN | 과태료 3,000만 원 | 해지자 개인정보 미파기, 법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적·관리적 조치미비 |
| 다음커뮤니케이션 | 과태료 3,000만 원 | 포털가입자 정보를 동의 없이 취급 위탁한 행위, 법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적·관리적 조치 미비 |
| SK커뮤니케이션스 | 과태료 2,000만 원 | 법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적·관리적 조치미비 |
| 야후코리아 | 과태료 2,000만 원 | 법정대리인의 요건에 맞지 않은 자를 법정대리인으로 등록한 행위 및 기술적·관리적 조치미비 |

자료: 방송통신위원회 보도자료에서 취합.[96]

---

해서 연속적으로 개인정보 관리실태를 점검하였다(방송통신위원회, 2008e).

위 표에 명시된 시정조치 외에 티브로드한빛방송 등 초고속인터넷서비스를 제공하는 케이블TV 사업자 4개사는 개인정보에 대한 불법접근을 방지할 수 있도록 접근절차를 개선하고, 연체정보 제공 시 본인확인 절차를 명확히 하는 등의 업무처리 절차 개선을 명령받았다. 포털 4개사는 14세 미만 아동의 개인정보 수집 시 정당한 법정대리인 여부를 확인할 수 있도록 업무처리 절차개선을 명령받았다. 이동통신 3사는 개인정보 활용 동의와 서비스 계약체결을 분리토록 하는 등의 업무처리 절차 개선을 명령받았다.

위 표에서 볼 수 있는 바와 같이 대부분의 통신업체들이 개인정보를 동의 없이 취급위탁해 왔음을 알 수 있다. 또한, 해지자 개인정보를 파기하지 않는 경우도 많았다.

그런데, 취급위탁과 제3자 제공의 경계가 명확하지 않은 측면이 있고, 업체들은 규제가 적은 취급위탁을 선호할 수밖에 없다는 점에서 고객 개인정보가 취급위탁이라는 방식으로 쉽게 제3자에게 제공될 가능성이 존재한다. '하나로텔레콤의 600만 명의 고객 개인정보 유출 사건'은 이러한 문제점을 잘 드러내준다.

하나로텔레콤을 비롯한 초고속 인터넷 서비스 업체의 개인정보 도용의 문제가 제기된 것은 2007년부터이다. 지난 2007년 8월 8일, 서울지방경찰청 사이버범죄수사대는 "통신업체들이 초고속 인터넷망 설치 고객들의 정보를 도용, 자회사인 인터넷 포털 사이트 회원으로 무단 가입시키고, 자신들의 별도 상품을 판매하는 위탁업체 및 프로그램 판매업체에 마구 제공하는 방법으로 고객정보를 부정사용하여 부당이득을 취했다"고 발표했다(서울지방경찰청. 2007). 보도자료에 의하면, 일부 통신업체의 경우 수집된 고객들의 개인정보를 분석하는 프로그램을 개발하여, 연령별, 이용 상품별로 고객을 구분하고, 바이러스 치료 등 프로그램을 판매하는 회사와 위탁 계약을 체결하여 텔레마케팅(TM) 용도로 DB 자료를 제공하였는데, 이렇게 부정 사용된 건수는 약 5,000만 건에 달했다.[97]

---

96) 방송통신위원회(2008b); 방송통신위원회(2008c); 방송통신위원회(2008d); 방송통신위원회(2008e).

97) 서울지방경찰청의 수사결과 발표에 고객 개인정보의 제3자 제공문제만 문제가 된 것은 아니다. 고객 개인정보의 동의없는, 혹은 동의받은 목적을 벗어나는 이용 및 유출, 그리고 명의 도용으로 인한 피해 등도 문제가 되었다. 보도자료에 의하면, 고객에게 설명이나 동의를 받지 않고, 주민등록번호 등 개인정보를 도용하여 홈페이지에 회원으로 무단 가입시키는 방법으로 개인정보를 도용당한 피해자는 730만 명에 달했다. 이들은 구 정보통신부 산하 개인정보분쟁조정위원회에서 고객이 가입신청서를 직접 작성하고, ID, 비밀번호를 고객이 직접 생산하도록 조정결정을 내렸음에도 불구하고, 계속적으로

2008년 4월 22일, 서울지방경찰청 사이버범죄수사대는 후속 수사결과를 발표하였다(서울지방경찰청, 2008b).[98] 이에 따르면, 하나로텔레콤은 2006년 1월 1일부터 2007년 12월 31일까지 약 600만 명의 개인정보, 8천 530여만 건을 전국 1000여 곳의 텔레마케팅 업체에 제공하였다. 하나로텔레콤은 모 은행과 신용카드 모집에 대한 업무제휴 계약을 체결한 후 신용카드 발급을 위한 텔레마케팅 업체를 지정하여 이용자의 개인정보 96만 건을 제공하였으며, 자사의 신상품 판매, 아직 구입하지 않은 통신상품의 판매, 바이러스 치료 상품의 판매를 위하여 전국 수백 개의 텔레마케팅 업체에 개인정보를 배포하였다. 이에는 해지 고객들의 정보까지 포함된 것으로 나타났다. 서울지방경찰청은 이러한 개인정보 도용 행위가 통신업체가 지금까지 변명해왔듯이 일부 대리점들의 실적을 높이기 위한 독자적 행위가 아니라, 본사 차원의 지시에 의한 것이라고 밝혔다.

2008년 6월 27일, 공정거래위원회는 하나로텔레콤에 소비자에 대해 본인의 명의도용여부 확인이나 피해의 회복 등 필요한 조치를 취하라는 내용의 시정명령을 하기로 의결하였는데, 공정거래위원회의 의결서에 의하면, 구체적인 사실 관계는 다음과 같다(공정거래위원회, 2008: 7).

[1] 피심인(하나로텔레콤 - 편집자 주)의 제휴마케팅 개요
피심인은 2006. 9. 28. 주식회사 한국스탠다드차타드제일은행(이하 '제일은행'이라 한다)과 피심인의 초고속인터넷서비스인 '하나포스'에 가입된 고객 중에서 추가적으로 피심인의 '하나TV' 또는 전화서비스에 가입하는 고객에게 제일은행의 "하나포스SC멤버스카드"(이하 '하나카드'라 한다)[99]를 발급해주는 것을 내용으로 하는 "업무제휴계약"을 체결하였다.
또한, 피심인은 2006년 9월경 텔레마케팅 사업자인 주식회사 예드림씨앤엠(이하 '예드림'이라 한다)과 예드림이 하나포스 고객을 대상으로 텔레마케팅을 하여 하나TV

---

불법행위를 하였다. 또한, 부정하게 발급된 ID와 비밀번호가 유출되어 인터넷 상의 게임 사이트에서 아이템 구입을 위해 사용되기도 했다. 이로 인해 이용대금의 변제 책임을 지게 된 피해자들이 경찰청에 신고된 것만 3,000건 이상이라고 한다. 또한, 이용자에 대한 확인절차 없이 초고속 통신망에 가입하게 함으로써 명의 도용 피해가 발생하였고, 이 중 일부는 신용불량자로 등재되어 이중피해를 입었다. 서울경찰청은 통신업체 고위급 임원 등 간부직원 26명, 대형 모집업체 40명 등 총 66명에 대해 수사를 하고 있다고 밝혔다.

98) 연합뉴스. 2008.4.23. "하나로텔레콤 고객 600만명 개인정보 `불법 사용'."

99) 위 카드를 발급받아 주 사용카드로 사용하는 고객에게는 하나포스요금 10% 할인 등의 혜택이 주어진다.

또는 하나카드 등의 신청자를 모집하는 것을 내용으로 하는 “고객관리업무 위탁 및 제휴프로그램 운영관리 대행 협약”을 체결하였다.
이러한 제휴마케팅은 ① 피심인이 자신의 ‘하나포스’ 고객의 개인정보를 예드림에게 제공하고 ② 예드림이 개인정보를 제공받은 고객을 대상으로 전화를 이용하여(텔레마케팅) 하나카드 신청자를 모집하여 ③ 제일은행이 카드발급심사를 통하여 하나카드를 발급하는 것을 주요내용으로 한다.

[2] 개인정보 도용에 따른 필요한 조치 미실시행위
피심인은 위와 같은 제휴마케팅계약에 따라 다음 <표 2-40>와 같이, 2006. 9. 30.부터 2007. 7. 31.까지의 기간 동안 자신의 ‘하나캠페인프로세스’[100]를 통하여 예드림에게 ‘하나포스’ 가입자 515,206명의 개인정보인 이름, 서비스명, 전화번호, 주민등록번호의 생년월일과 앞자리 1자, 주소, 사용요금조회 등을 전산망을 통하여 총 25회에 걸쳐 제공하였다.

<표 2-40> 개인정보 제공 내역

| 연번 | 캠페인명 | 캠페인기간 | DB할당수량 | 접촉고객수 |
|---|---|---|---|---|
| 1 | 전략 하나TV카드 | ’06.09.30~10.31 | 3,930 | 119 |
| 2 | 전략1차 하나TV카드 | ’06.10.04~11.16 | 15,984 | 5,623 |
| 3 | 전략2차 하나TV카드 | ’06.10.13~11.17 | 13,740 | 4,607 |
| 4 | 전략3차 하나TV카드 | ’06.10.20~11,21 | 27,459 | 7,702 |
| 5 | 전략6차 하나TV카드 | ’06.11.11~12.07 | 6,705 | 2,470 |
| 6 | 전략7차 하나TV카드 | ’06.11.15~12.08 | 2,187 | 904 |
| 7 | 전략8차 하나TV카드 | ’06.11.22~12.08 | 41,243 | 10,588 |
| 8 | 전략9차 하나TV카드 | ’06.12.09~’07.01.17 | 15,718 | 4,906 |
| 9 | 전략11차 하나TV카드 | ’06.12.14~’07.01.16 | 34,427 | 15,306 |
| 10 | 전략12차 하나TV카드 | ’06.12.31~’07.01.31 | 27,103 | 12,041 |
| 11 | 전략15차 하나TV카드 | ’07.01.12~02.16 | 21,425 | 7,353 |
| 12 | 전략16차 하나TV카드 | ’07.01.24~02.28 | 20,156 | 11,163 |
| 13 | 전략17차 하나TV카드 | ’07.02.01~02.28 | 52,194 | 29,776 |
| 14 | 전략18차 하나TV카드 | ’07.02.15~03.16 | 16,061 | 9,685 |
| 15 | 전략19차 하나TV카드 | ’07.02.18~03.16 | 21,000 | 12,143 |

100) 피심인이 자신의 상품정보를 소개하기 위한 텔레마케팅의 대상자(하나포스 가입자 중 하나TV 미가입자)를 선정하여 텔레마케팅업체에 송부하는 절차를 말한다.

| | | | | |
|---|---|---|---|---|
| 16 | 전략20차 하나TV카드 | '07.03.01~03.12 | 22,333 | 11,177 |
| 17 | 전략21차 하나TV카드 | '07.03.11~03.31 | 14,222 | 7,903 |
| 18 | 전략22차 하나TV카드 | '07.03.16~03.23 | 10,118 | 5,208 |
| 19 | 전략23차 하나TV카드 | '07.03.20~03.27 | 6,894 | 2,892 |
| 20 | 전략24차 하나TV카드 | '07.03.22~03.30 | 11,715 | 4,475 |
| 21 | 전략25차 하나TV카드 | '07.03.25~04.13 | 12,674 | 5,366 |
| 22 | 전략26차 하나TV카드 | '07.05.10~06.05 | 26,296 | 12,589 |
| 23 | 전략27차 하나TV카드 | '07.06.07~07.13 | 42,389 | 15,796 |
| 24 | 전략28차 하나TV카드 | '07.06.23~07.27 | 35,382 | 15,502 |
| 25 | 전략33차 하나TV카드 | '07.07.15~07.31 | 13,851 | 4,187 |
| 총 25회 합계 | | | 515,206 | 219,481 |

※ 4차, 10차, 13차는 기획자의 실수로 순번이 잘못 기재된 경우이고, 5차, 14차는 취소, 29차~32차는 미실시된 행사이다.

자료: 피심인 제출 자료

피심인은 위와 같은 제휴마케팅에 앞서 2006. 9. 21. 소비자 이용약관의 "개인정보 보호방침"의 "개인정보 수집 및 활용목적"에 다음 <표 2-41>와 같이 추가된 내용을 피심인의 사이버몰에 고지하였으나, 소비자로부터 별도의 동의는 받지 아니하였다.

<표 2-41> "개인정보보호방침" 내 "개인정보 수집 및 활용목적" 추가사항

| 구분 | 당초 | 추가내용 |
|---|---|---|
| 활용목적 | 고객만족프로그램<br>(서비스만족도 조사, 상품소개 등) | 하나포스멤버스 카드 소개 |
| 상품명 | 가디언 등 18종(기타내용 포함) | 하나포스멤버스 카드 소개 |
| 업체명 | 하나지엘 등 유통망과 전산업체 다수 | (주)예드림C&M |
| 요금관련정보 | 이용요금 청구/수납/미수채권관리 | 하나포스멤버스카드 발급 |

자료: 피심인 제출 자료

피심인의 위와 같은 일련의 행위와 관련하여 서울지방경찰청(사이버범죄수사대)은 2008. 4. 22. 피심인이 고객의 동의 없이 개인정보를 판촉업체에게 제공하였다고 발표하였고, 이에 따라 소비자들은 피심인에게 자신의 개인정보가 도용되었는지에 대한 확인 등을 요청하였다.

그럼에도 불구하고, 피심인은 도용여부의 확인 및 처리상황의 통지 등의 어떠한 조치

도 하지 아니하고 다만, “양해의 말씀” 또는 “정확한 내역을 파악하고 있는 중” 등의 내용으로 민원인에게 답변하였다.

경찰은 하나로텔레콤의 행위에 대해 본인의 동의없는 개인정보 제3자 제공으로 판단하여, 「정보통신망법」 제24조의2 및 제71조를 적용했다고 밝혔다. 제71조는 벌칙 조항으로 제24조의2 위반 행위에 대해 ‘5년 이하의 징역 또는 5천만 원 이하의 벌금’에 처하도록 하고 있다.

그러나 하나로텔레콤의 입장은 다르다. 언론보도에 의하면, 하나로텔레콤은 “고객 정보를 돈을 받고 제3자에게 팔아넘긴 것이 아니라 법이 허용하는 범위 안에서 위탁 계약업체를 통해 텔레마케팅을 한 것이다”[101]라고 주장하고 있다. 즉, 텔레마케팅 업체를 활용한 마케팅은 개인정보 위탁에 해당하고, 따라서 「정보통신망법」 제25조제2항이 적용되어야 하며, 하나로텔레콤은 “홈페이지를 통해서 정보를 제공받은 업체를 고지했고 정부의 약관 심사를 받았다”는 것이다.[102] 또한 SC제일은행과 제휴카드를 제공한 것은 요금할인을 통해 고객에게 더 많은 혜택을 부여하기 위해서라고 해명했다.[103] 하나로텔레콤을 인수한 SK브로드밴드 개인정보취급방침에 의하면, 예드림씨앤엠은 현재도 위탁업체로 되어 있으며, 위탁업무는 가정 상품 고객유치 가입 유치점으로 되어 있다. 다만, 현재 제휴카드의 경우 제3자 제공으로 되어 있다.

따라서 쟁점이 되고 있는 것은 제휴카드에 대한 텔레마케팅을 위한 고객 개인정보의 제공이 ‘위탁’인지 ‘제3자 제공’인지 여부이다. 하나로텔레콤은 이를 ‘위탁’으로 본 것이고, 경찰은 신용카드 발급은 또 다른 영리 목적을 위한 것이므로 ‘제3자 제공’에 해당한다는 것이다. 제3자 제공에 해당할 경우에는 「정보통신망법」 제24조의2에 따라, 모든 사항에 대해 이용자에게 알리고 동의를 얻어야 한다. 그런데 취급위탁의 경우에도 고지절차와 동의절차를 거치지 않을 수 있는 경우는 ‘서비스의 제공에 관한 계약의 이행을 위하여 필요한 경우로서’라고 「정보통신망법」 제25조 제2항에 명시되어 있다. 신용카드 발급은 분명 ‘초고속 인터넷 서비스’의 이행과는 무관한 듯이 보인다. 다만, 제휴카드를 주 사용카드로 이용하는 고객에게는 하나포스 요금 10% 할인 등의 혜택이 주어진다는 점에서 서비스 이행과 연관이 있는지 논란의 여지가 있다.

---

101) 스포츠서울. 2008.4.30. “하나로텔레콤 상대 집단소송 봇물.”; 미디어오늘. 2008.5.2. “하나로텔레콤 등 개인정보 유출에 소비자들 ‘집단반발’.”
102) 연합뉴스. 2008.5.4. “하나로텔 `불법'...옛 정통부 유권해석이 빌미?”
103) 아이뉴스24. 2008.7.6. “하나로텔 “공정위, 고객정보 '도용' 지적, 사실과 달라”.”

하나로텔레콤을 인수한 SK브로드밴드에 대해 피해자들은 집단 소송을 제기했으며, 2009년 1월 검찰은 벌금 3,000만 원에 약식 기소하였다. 그러나 법원은 이를 정식 재판에 회부해 서울중앙지법에서 재판이 진행 중인 상황이다. 아직 법원의 판단은 나오지 않았지만, 이 사안에 대한 각 기관의 판단은 다르다.

소비자 집단 소송을 주도하고 있는 녹색소비자연대 등 시민단체들은 이는 '개인정보 제3자 제공'에 해당하며, 하나로텔레콤의 약관은 해당 법조항의 요건조차 갖추지 않은 불법약관이라고 비판하고 있다.[104)]

방송통신위원회는 2008년 6월 24일, 전체회의를 통해 하나로텔레콤의 '개인정보 유용행위' 등에 대해 "초고속인터넷서비스 신규가입자 모집정지 40일, 과징금 1억4천8백만 원 및 3천만 원의 과태료를 부과하고, 관련 위반행위의 중지 및 업무처리 절차를 개선하도록 명령하기로 의결"하였다(방송통신위원회, 2008a). 이에 대해 '개인정보 유용에 대한 중징계'라는 평가[105)]가 있기는 했지만, 방통위가 적용한 법 조항은 「정보통신망법」 제24조의2나, 제25조가 아니라, 「전기통신사업법」 제15조[106)]와 제37조의2[107)], 그리고 「정보통신망법」 제28조, 제29조, 제30조[108)]였다. 「전기통신사업법」 제

---

104) 녹색소비자연대전국협의회 등. 2008.5.8. "<성명> 하나로텔레콤의 반성없는 반소비자적인 태도의 즉각 중단을 촉구한다."

105) 아이뉴스24. 2008.6.24. "하나로텔 개인정보 유용 중징계 의미는?"

106) 제15조(허가의 취소등) ① 방송통신위원회는 기간통신사업자가 다음 각 호의 어느 하나에 해당하는 때에는 그 허가를 취소하거나 1년이내의 기간을 정하여 사업의 전부 또는 일부의 정지를 명할 수 있다.
1. 사위 기타 부정한 방법으로 허가를 받은 때
2. 제5조제5항 및 제13조제6항의 규정에 의한 조건을 이행하지 아니한 때
3. 제7조제2항의 규정에 의한 명령을 이행하지 아니한 때
4. 제9조제1항의 규정에 의한 기간(제9조제2항의 규정에 의한 기간의 연장을 받은 경우에는 연장된 기간)내에 사업을 개시하지 아니한
5. 제29조제1항의 규정에 의하여 인가를 받거나 신고한 이용약관을 준수하지 아니한 때
6. 제37조제1항 또는 제65조제1항에 따른 시정명령을 정당한 사유 없이 이행하지 아니한 때

107) 제37조의2(금지행위에 대한 과징금의 부과등) ① 방송통신위원회는 제36조의3제1항의 규정에 따른 행위 또는 제36조의4제1항 내지 제6항의 규정을 위반한 행위가 있는 경우에는 당해 전기통신사업자에게 대통령령이 정하는 매출액의 100분의 3이하에 해당하는 금액의 과징금을 부과할 수 있다. 이 경우 전기통신사업자가 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 때에는 해당 전기통신사업자 및 동종 유사 역무제공사업자의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령이 정하는 때에는 10억원이하의 과징금을 부과할 수 있다.

108) 제28조(개인정보의 보호조치) ① 정보통신서비스 제공자등이 개인정보를 취급할 때

15조는 방송통신위원회가 기간통신사업자에 대해 허가취소나 사업정지 명령

---

에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영
3. 접속기록의 위조·변조 방지를 위한 조치
4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치
5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.

제29조(개인정보의 파기) 정보통신서비스 제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 해당 개인정보를 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.

1. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 수집·이용 목적이나 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
2. 제22조제1항, 제23조제1항 단서 또는 제24조의2제1항·제2항에 따라 동의를 받은 개인정보의 보유 및 이용 기간이 끝난 경우
3. 제22조제2항에 따라 이용자의 동의를 받지 아니하고 수집·이용한 경우에는 제27조의2제2항제3호에 따른 개인정보의 보유 및 이용 기간이 끝난 경우
4. 사업을 폐업하는 경우

제30조(이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.

② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.

1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

③ 정보통신서비스 제공자등은 이용자가 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 파기하는 등 필요한 조치를 하여야 한다.

④ 정보통신서비스 제공자등은 제2항에 따라 열람 또는 제공을 요구받으면 지체 없이 필요한 조치를 하여야 한다.

⑤ 정보통신서비스 제공자등은 제2항에 따라 오류의 정정을 요구받으면 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 알리는 등 필요한 조치를 하여야 하고, 필요한 조치를 할 때까지는 해당 개인정보를 이용하거나 제공하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그 개인정보를 제공하거나 이용할 수 있다.

⑥ 정보통신서비스 제공자등은 제1항에 따른 동의의 철회 또는 제2항에 따른 개인정보의 열람·제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.

⑦ 영업양수자등에 대하여는 제1항부터 제6항까지의 규정을 준용한다. 이 경우 “정보통신서비스 제공자등”은 “영업양수자등”으로 본다.

을 내릴 수 있는 경우를 규정한 것이고, 제37조의2는 과징금 부과 조항이다. 「정보통신망법」 제28조, 제29조, 제30조는 △ 하나로텔레콤이 자사 포탈인 하나포스닷컴에 고객을 무단으로 가입시킨 행위, △ 해지자 개인정보를 별도의 DB로 관리하지 않은 행위, △ 개인정보 활용 동의를 철회했음에도 불구하고 이를 파기하지 않은 행위 등에 적용된 것이다. 언론보도에 의하면, 방통위는 하나로텔레콤의 고객 개인정보 제공에 대해 '하나로 영업점에게 이뤄진 것'이므로, '제3자 제공으로 보기는 어렵고, 자기 명의로 서비스하는 부수적인 부가 서비스'를 위한 취급위탁으로 보고 있다고 밝혔다.[109)]

반면, 공정거래위원회는 고객 개인정보의 '도용'이라고 결정하였는데, 그 내용을 보면 '제3자 제공'으로 판단하였다. 공정위가 '도용' 개념을 쓴 것은 '전자상거래 등에서의 소비자보호에 관한 법률'[110)]에 근거하여 판단하였기 때문이다. 공정위는 "정보의 '도용'여부는 '정보주체의 동의 없는 개인정보의 부당한 이용'에 해당되는지를 기준으로 판단"한다고 밝히며, 하나로텔레콤의 경우 다음과 같은 세 가지 이유로 도용에 해당한다고 판단하였다(공정거래위원회, 2008: 10).

첫째, 개인정보에 대한 활용 동의 시 '상품소개' 등 지나치게 포괄적이고 모호한 내용으로 표시하거나 개인정보 활용내역을 사후에 사이버몰에 단순히 기재하는 것만으로는 개인정보 활용에 필요한 소비자의 동의를 얻었다고 볼 수 없다. 둘째, 통신서비스 사업자인 피심인이 자신의 업종과 무관한 신용카드발급과 관련하여 소비자의 개인정보를 이용한 행위는 개인정보를 부당하게 이용한 경우에 해당된다. 셋째, 개인정보 도용의 주요 원인은 개인정보를 대량으로 수집·이용하는 사업자의 고의·과실인 점, 소비자 권익을 보호하고 시장의 신뢰도 제고가 목적인 법 취지 및 사업자에 대하여 정보도용에 따른

---

109) 아이뉴스24. 2008.6.24. "[일문일답] 사상 첫 영업정지 부과한 방통위 이기주 국장."
- 이번에 조사하면서 경찰처럼 하나로텔레콤이 제3자에게 고객정보를 제공한 것으로 봤나, 아니면 취급위탁 부주의로 봤나?
"제3자 제공으로 보기는 어렵고, 자기 명의로 서비스하는 부수적인 부가 서비스로 봤다. 행정처분이기 때문에, 검찰이나 경찰이나 수사기관에서 하거나 하는 사법절차와는 별개다."
"내 업무를 위해 위탁하는 것은 취급위탁이고, 남의 업무를 위해 위탁하는 건 제3자 정보 제공이다. 이번 하나로 건의 경우 제일은행 관련 정보위탁도 하나로 영업점에게 이뤄진 것이니 취급위탁으로 봤다"(조영훈 개인정보보호과장).

110) 「전자상거래 등에서의 소비자보호에 관한 법률」 제11조 (소비자에 관한 정보의 이용 등) ②사업자는 재화등을 거래함에 있어서 소비자에 관한 정보가 도용되어 당해 소비자가 재산상의 손해가 발생하였거나 발생할 우려가 있는 특별한 사유가 있는 경우에는 본인 확인이나 피해의 회복 등 대통령령이 정하는 필요한 조치를 취하여야 한다.

조치의무를 부과한 법 제11조제2항의 규정 등을 고려할 때, 개인정보가 정보주체의 의사에 반하여 부당하게 이용되어 정보주체인 소비자의 재산상 손해를 야기할 우려가 있는 상황이 초래되면 법 제11조제2항의 '도용'에 해당되고, 이러한 도용의 주체가 정보수집자인 사업자인지 또는 제3자인지 여부 등은 법 제11조제2항의 '도용'이 있었는지 여부를 판단함에 있어 직접적인 고려요소는 아니다.

이에 대해 하나로텔레콤 측은 "개인정보를 단순히 텔레마케팅에 이용한 것에 불과하므로 사업자에 의한 개인정보의 부당한 이용인 '유용'에 해당됨은 별론으로 하더라도 제3자에 의한 개인정보의 '도용'과는 무관하다"고 주장하였다. 이에 대해 공정위는 "정보화사회 및 신용사회로의 급속한 이행에 따른 사업자에 의한 소비자 개인정보 도용의 확산 가능성 및 그에 따른 소비자보호 필요성의 증대, 개인정보주체의 프라이버시 보호욕구와 사업자의 마케팅 등을 위한 개인정보의 수집 및 활용 사이에는 항상 이해관계가 상충되는 현실 등을 종합적으로 고려할 때, 법 제11조제2항의 '도용'의 개념적 범위에는 해킹 등과 같이 제3자의 불법적인 행위로 인한 경우는 물론이고, 이 사건의 경우와 같이 정보수집사업자와 제3자의 계약에 의하여 정보주체인 소비자의 의사에 반하여 정보가 이용되는 경우도 포함된다고 보는 것이 타당하다"고 반론하였다.

정리하자면, 하나로텔레콤이 제휴카드의 텔레마케팅을 위해 고객의 개인정보를 제공한 것에 대해 경찰, 시민단체, 공정거래위원회는 '제3자 제공'으로, 하나로텔레콤과 방송통신위원회는 '취급위탁'으로 판단하고 있다. 이에 대한 법원의 최종 판결은 아직 내려지지 않았다.

(3) 취급위탁과 제3자 제공 - 통신업체의 개인정보취급방침

「정보통신망법」에서 '취급위탁'에 대해 제3자 제공에 비해 완화된 규정을 둔 것은 기업들의 원활한 사업을 고려한 것이다. 서비스 제공에 필수적인 업무를 처리하기 위해 위탁이 불가피한 경우가 있는데, 이 과정에서 일일이 동의를 받도록 할 경우 원활한 업무 처리에 부담이 될 수 있기 때문이다. 그러나 위탁과 제3자 제공 업무의 경계는 명확하지 않으며, 업체들은 규제가 적은 위탁을 선호할 수밖에 없다. 따라서 자칫 고객의 개인정보가 위탁이라는 방식으로 쉽게 제3자에게 제공될 가능성이 높아진다.

통신업체들의 개인정보 취급방침을 검토해보면 위탁과 제3자 제공 사이의 모호함을 확인할 수 있다.[111] 어떤 업무가 위탁이고, 어떤 업무가 제3자 제

공인지 명확하지 않기 때문에, 업체들마다 자체적인 판단에 따라 개인정보 취급방침을 작성하고 있으며, 이에 따라 업체에 따라 위탁과 제3자 제공에 대한 판단이 달라지고 있다. 예를 들어, 요금 납부(지로, 은행 자동이체, 신용카드 결제 등) 업무의 경우, A이동통신사, A초고속인터넷업체는 제3자 제공으로, C이동통신사, B초고속인터넷업체, C초고속인터넷업체는 위탁으로, B이동통신사의 경우에는 제3자 제공과 위탁에 모두 포함시켜 놓았다. 또한, A이동통신사의 경우에는 금융결제원, 은행 및 신용카드사의 세부 목록, KS-NET 등을 모두 제시해놓고 있는 반면, B이동통신사는 금융결제원, KS-NET 등과 함께 은행/카드사로만 제시하고 있으며, C이동통신사 및 C초고속인터넷업체의 경우 금융결제원, KS-NET 등만 명시되어 있다. 신용정보업체에 의한 채권추심 업무와 같이 제3자 제공이나 위탁에 모두 명시되어 있는 경우도 종종 볼 수 있다. B이동통신사의 경우, 장애인, 국민기초생활보장 수급자, 국가유공자 확인 등의 목적으로 한국정보통신산업협회와 함께, 행정안전부, 보건복지부, 국가보훈처에 제공한다고 되어 있으나, C이동통신사의 경우에는 복지할인 조회로 한국정보통신산업협회만 명시되어 있었고, A이동통신사는 관련 내용이 없었다. 한국정보통신산업협회를 통해 정부 부처에도 정보가 제공되는 것인지, 아니면 각 업체마다 복지 할인 대상자 확인 방법이 다른 것인지 모호하다. 또한, 통신업체들은 실명 인증, 연체 확인 등 방송통신신용정보 공동관리를 위해 정보통신산업협회에 개인정보를 제공하고 있는데, 이를 제3자 제공으로 볼 것인지, 취급위탁으로 볼 것인지도 업체마다 차이가 있었다. 이처럼 제3자 제공업무와 위탁 업무에 대한 가이드라인이 없다 보니, 각 업체마다 제각각 판단하고 있으며, 법적 안정성을 위해 제3자 제공과 위탁 모두에 포함시킨 경우도 있다.

<표 2-42> 각 통신업체별/업무별 제3자 제공 및 취급위탁 구분 사례

| | A이동통신사 | B이동통신사 | C이동통신사 | A초고속인터넷업체 | B초고속인터넷업체 | C초고속인터넷업체 |
|---|---|---|---|---|---|---|
| 요금납부 | 제3자제공 | 제3자제공/취급위탁 | 취급위탁 | 제3자제공 | 취급위탁 | 취급위탁 |
| 채권추심 | 제3자제공/ | 취급위탁 | 취급위탁 | 제3자제공 | 취급위탁 | 취급위탁 |

111) 각 통신업체의 개인정보 취급방침 상에 공개되는 제3자 제공업체와 위탁업체 목록은 계속 변경된다. 따라서 각 업체의 제3자 제공 업체나 위탁 업체와 관련된 본문의 내용은 이후의 내용과 일치하지 않을 수 있다. 조사 내용은 2009년 10월 현재의 내용이다.

| | | | | | | |
|---|---|---|---|---|---|---|
| | 취급위탁 | | | | | |
| 정보통신산업협회제공 | 취급위탁 | 제3자제공/취급위탁 | 취급위탁 | 제3자제공 | 취급위탁 | 취급위탁 |

위탁업무의 경우, 서비스 제공에 필수적인 업무만 위탁하는 것은 아니다. 특히 이동통신사들의 경우, 핸드폰을 통해 콘텐츠 서비스나 예약 서비스 등을 제공하고 있는데, 이들 서비스들은 주로 제3의 업체를 통해 제공된다. 이들 서비스들은 선택적으로 가입을 해야 하는 서비스이지만, 개인정보 위탁으로 되어 있다. 예를 들어, B이동통신사의 경우 모블로그 서비스 운영, 모바일 운세 서비스 운영, 인물검색서비스, 금융·재테크 부가서비스, 학습·여성·육아 부가서비스 등을 위해 개인정보를 위탁하고 있고, C이동통신사의 경우에도 영화요금제 고객 영화관람 제공을 위해 개인정보를 위탁하고 있으며, A이동통신사는 쇼핑, 증권 서비스 등을 위해 제3의 업체에 개인정보를 위탁하고 있다. 업체 관계자에 의하면, 이용자들이 선택적으로 이용하는 서비스의 경우에는 위탁으로 되어 있다고 하더라도, 서비스를 처음 이용할 때 동의를 받는다고 한다.

그러나 이용자 입장에서는 제3자 제공이든, 이용자 선택 서비스에 대한 위탁이든 자신이 언제, 어떻게 동의했는지, 포괄적으로 동의한 것인지, 아니면 개별 서비스에 대해 동의를 한 적이 있는지 등을 확인하기 쉽지 않다. 또한, 하나로텔레콤 사례에서와 같이 서비스 제공에 필수적인 업무인지 아닌지 등을 개인정보 취급방침만 봐서는 확인하기 쉽지 않다. 다만, A초고속인터넷업체의 경우에는 고객 개인정보를 제공받는 제3자 업체를 필수사항(실명확인, 신용도판단, 요금결제, 채권추심 등)과 선택사항으로 구분하고 있으며, 위탁의 경우에도 회사 서비스 신청 고객과 홈페이지 회원서비스 가입고객으로 위탁 현황을 구분, 제시하고 있으며, 기본업무 위탁과 고객 동의 위탁을 구분하고 있었다. 간단한 구분이지만, 이런 방식으로만 제공하더라도, 이용자 입장에서는 자신의 개인정보를 어떻게 취급하는지에 대한 이해를 높일 수 있다.

「정보통신망법」에서는 요금정산에 필요한 경우에는 개인정보의 수집이나 제3자 제공시 정보주체의 동의를 받지 않아도 되도록 규정[112]하고 있으며, '서비스 제공에 관한 계약의 이행을 위해 필요한 경우'에는 취급위탁에 따른 고지절차와 동의절차를 거치지 않아도 되도록 규정하고 있다. 그러나 통신업체들의 개인정보 취급방침만을 보아서는 별도의 동의가 필요한 업무인지 아

112) 제22조제2항제2호 및 제24조의2제1항

닌지를 정보주체가 명확하게 판단하기 힘들다. 서비스 가입 내역이나 결제 기록과 같은 개인정보를 통신업체 홈페이지를 통해 정보주체가 열람할 수 있도록 제공하고 있는 것과 같이, 정보주체별 제3자 제공 내역과 동의의 방법(예를 들어, 요금 정산과 같이 동의가 없어도 되는 것인지, 별도의 동의가 필요한 것인지 등)에 대해서도 홈페이지를 통해 쉽게 열람할 수 있도록 할 필요가 있다.

현재와 같이 제3자 제공에 해당하는 업무와 취급위탁에 해당하는 업무의 구분이 모호하고, 업체마다 제각각 판단할 수밖에 없는 상황은 정보주체에게도 이와 관련한 명확한 정보를 제공하기 힘들다. 하나로텔레콤 사례와 같은 분쟁이 발생하지 않기 위해서는, 제3자 제공과 위탁 업무의 구분 및 서비스 제공에 필수적인 정보와 선택적인 정보의 구분에 대한 좀 더 구체적인 가이드라인을 방송통신위원회에서 제공할 필요가 있다.

### 3) 개인정보의 관리 – 판매점 관리의 문제

이동통신사가 고객 유치 및 관리를 위해 관계를 맺고 있는 대리점은 1000여개, 판매점은 1만 여개에 달한다. 이렇게 많은 곳에서 고객의 개인정보를 취급하다보니, 대리점과 판매점에 대한 관리가 제대로 이루어지지 않을 경우, 개인정보의 유출이나 남용의 위험성은 클 수밖에 없다.

<그림 2-6> 이동통신 유통망 구조 현황

('09. 3월 현재)

| 이통3사 | | 대리점(개통, A/S업무) | | 판매점(판매) |
|---|---|---|---|---|
| SKT | → 개통 등 업무위탁 | 1,170개(3,200매장) | → 판매대행 | 12,000여개 |
| KTF | | 1,073개(2,350매장) | | 12,000여개 |
| LGT | | 1,181개(1,800매장) | | 4,500여개 |

※「정보통신망법」은 정보통신서비스 제공자(이통3사)와 그의 수탁자(대리점)에 대해서만 개인정보 보호조치 의무 및 벌칙 사항을 명시적으로 규정.

자료: 방송통신위원회(2009).

2008년 4월 22일, 서울지방경찰청은 이동통신사 서버에 고객정보 위탁업체가 접속하는 계정을 알아내 고객정보를 실시간으로 조회할 수 있는 웹페이지를 구축한 유명포탈업체 직원 1명을 검거했다고 발표했다(서울지방경찰청, 2008a). 이로 인해 2008년 3월 21일부터 25일까지 LG텔레콤 가입자 170명

가량의 주민등록번호와 199명의 주민등록번호 앞자리가 유출되었다.[113] 서울지방경찰청의 발표에 따르면, '이동통신사에서는 제휴 업체의 계정과 연동된 고객자료를 단순 평문으로 송신하고 IP 접근 제한 등의 다른 보안장치를 하지 않는 등 보안 취약점을 노출'하였으며, '접속 계정을 통해 인터넷에 접속만 하면 누구라도 이동통신사 고객망에 연동할 수 있는 상태로 5년간 방치'해 왔다. 물론 도용된 계정은 대리점의 것이 아니었지만, 이는 위탁업체 전반이 안고 있는 문제이다.

또한, 한 언론보도[114]에 의하면, 이름과 주민등록번호 등이 쓰인 통신사 가입서류, 전화번호가 그대로 드러난 번호이동 신청서류, 주민등록증 사본과 심지어 가족의 개인정보까지 알 수 있는 주민등록등본 등 개인정보가 담긴 서류들이 쓰레기통에 버려지는 등 판매점의 개인정보 관리 실태가 허술한 것으로 드러났다.

이에 따라, 방송통신위원회는 2009년 5월 1일, 판매점을 통한 개인정보 유출을 막기 위해 이동통신 3사가 '개인정보 관리체계 자율 개선방안'을 마련했다고 발표하였다. 이 자료에 따르면, 판매점의 개인정보 관리 실태가 매우 취약한 것으로 나타난다(방송통신위원회, 2009).

이동통신 판매점은 대리점과의 수수료 정산이나 고객 불만처리 등을 위해 가입신청서 사본, 주민등록증 사본, 주민등록등본 등 고객정보 서류를 별도로 복사하여 보관해왔다. 또한, 일별 영업실적 관리를 위해 고객정보 목록을 별도로 작성하기도 했다. 그러나 고객정보 서류를 무단으로 방치하거나 고객들에게 반환하지 않는 사례가 있는 등 개인정보 보호 수준이 미약한 것으로 나타났다.

그러나 판매점은 이동통신사 본사와의 계약관계가 불명확하기 때문에, 이동통신사 차원의 관리는 제대로 이루어지고 있지 않았다. 이동통신사는 대리점에 대해서만 위탁 계약을 체결하며, 판매점과는 직접적으로 영업 대행 계약을 체결하지 않는다. 각 이동통신사의 '개인정보 취급방침'에도 위탁 계약한 대리점의 목록만이 고지되어 있을 뿐이다. 판매점은 이동통신사의 대리점과 계약하거나, 혹은 계약이 없이 영업 업무를 대행한 후에 휴대폰 판매・개통 실적에 따라 대리점으로부터 사전에 약정된 수수료를 지급받는다. 또한, 판매점은 여러 이동통신사와 복수로 계약하여 영업하고 있으며, 개・폐업이 잦고 일부 판매점은 사업자등록증도 없이 영업을 하고 있는 것으로 나타났

113) 뉴시스. 2008.4.22. "LGT, 170명 주민번호 등 개인정보 유출."
114) 한겨레. 2008.12.17. "용산전자상가 쓰레기통엔 개인정보 '가득'".

다.

이동통신 대리점 및 판매점의 개인정보 관리 문제는 이미 오래전부터 지적되어 왔다. 이동통신 대리점에 의한 고객 정보 유출 문제가 심각해지자, 지난 2001년 정보통신부는 이동전화 사업자들의 개인정보 관리실태 점검을 위한 현장조사를 실시한 바 있는데, 그 결과 지적한 사항 중 하나가 '판매점에 대한 관리감독 소홀 문제'이다(한국정보보호진흥원, 2003: 153). 당시 지적사항을 보면, 그 당시나 현재나 여전히 문제가 지속되고 있음을 알 수 있다.

> "이동전화사는 대리점이나 대리점과 유사한 영업활동을 하는 소위 판매점의 가입계약서를 통해 개인정보를 수집한다. (업계에 따르면 가입계약이 판매점을 통해 이루어지는 경우가 전체의 약 50%라고 함) 그러나 판매점의 경우 영세성, 인식부족 등으로 가입계약서 보관 등 개인정보 관리가 매우 허술하게 이루어지고 있었다. 그러나 대리점과 달리 계약관계가 없다는 이유로 본사 차원의 어떠한 관리감독도 이루어지지 않고 있었으며, 판매점 주인은 영업활동을 중단한 이후에도 가입계약서 원부를 본사나 대리점으로 이송하지 않고 자체 처리하고 있었다."(한국정보보호진흥원, 2003: 154)

실태조사 결과 드러난 문제점들을 개선하기 위해 정보통신부는 몇 가지 개선방안[115]을 제시하였는데, '판매점에 대한 관리감독 강화'도 그 중 하나이다. 이에 따르면, "본사에서 판매점에 대한 체계적인 관리지침을 세워 관리감독을 강화하고, 판매점 직원에 대한 정기적인 교육을 실시하도록 하였다. 특히, 지금까지 판매점에서 보유해오던 가입계약서 원부에 대해서는 앞으로 가입계약을 체결한 직후 본사 또는 본사의 직접적인 관리감독이 가능한 대리점으로 송부하여 보관토록 하였다."

2003년 개인정보보호백서에서도 동일한 지적이 이어졌다. "위탁 업체에 의해 가입자 유치율이 60~70%에 달하고 있음에도 이에 대한 관리 감독 또는 직원 교육 등이 미비하고, 본사와 직접 계약을 맺지 않고 위탁업체와 계약을

115) 개선방안으로 정보통신부는 2001년 12월「이동전화 가입자의 개인정보보호 강화를 위한 조치계획」을 마련하였다. 세부적인 조치계획의 내용은 다음과 같다.
1) 개인정보 업무총괄 책임자 지정
2) 자체 점검활동 강화
3) 체계적인 개인정보 업무처리지침 수립
4) 개인정보 고지의무 준수강화
5) 개인정보 위탁처리 업체에 대한 관리강화
6) 판매점에 대한 관리감독 강화
7) 고객정보DB 관리시스템의 개선
8) 개인정보 보호인식 제고를 위한 교육・홍보 강화

맺은 서브 위탁업체의 경우 관리 감독이 전무해 이들에 의한 개인정보 유출 등 오남용 위험성이 존재했다"고 지적하고 있다(한국정보보호진흥원, 2004: 91).

2004년 한국전산원에서 민간분야 총 9개 분야 500개 사업자를 대상으로 설문면접 조사 및 현장 방문 조사를 통해 파악한 개인정보관리 현황조사에서도 "초고속 인터넷 사업자의 경우 대규모 마케팅 특성상 본사 외의 업체와 위탁계약을 맺어 개인정보를 수집하고 있으며 위탁업체에 의한 가입자 유치 비율이 60~70%에 달하고 있으나, 이들 위탁업체에 대한 관리 감독 및 직원 교육 등이 미비하고 본사와 직접적인 계약을 맺지 않고 위탁업체와 2차 계약을 맺은 서브 위탁점등에 대한 관리감독이 전무하여 이들에 의한 개인정보유출 위험성이 크다"고 지적하였다(정연수, 2004: 130). 2개 업체 이상과 계약을 맺은 서브 위탁업체(판매점)들은 A사의 고객정보를 B사 신규 고객 유치에 활용하여, 이와 관련된 민원이 종종 발생하기도 했다고 한다.

2005년 9월 29일에는 정보통신부에서 「이동통신서비스제공자의 개인정보보호지침」을 제정하였다. 이 지침에서도 '대리점·판매점의 개인정보보호 강화'를 위한 규정을 담고 있는데, △ 대리점 및 판매점에서 이용자의 가입신청서 등 구비서류 보관 금지, 고객정보의 출력·저장 금지 등 개인정보보호 기술적··관리적 조치에 따른 개인정보보호를 의무화, 대리점 및 판매점에 대한 교육 강화(제10조), △ 이통사가 자체 대리점·판매점의 개인정보 관리 방안을 마련하여 준수하도록 하고 매년 2회 이행 여부를 제출토록 함(10조), △ 개인정보 영향평가 실시 권장 및 내부 직원에 의한 개인정보 유출 등에 대한 방지 방안을 마련토록 함(제12조 및 제14조) 등이다.

2009년 5월 1일 발표된 '개인정보 관리체계 자율 개선방안'에서도 판매점의 개인정보 보호조치를 강화하기 위한 방안을 제시하고 있는데, 이는 다음과 같다.

△ 2009년 3월부터 '개인' 영업점에 대하여 추가로 신규 영업점을 개설하지 않도록 하고, 기존 개인 영업점은 2009년 8월말까지 사업자등록증을 보유하도록 계도하여 전환시켜, 2009년 9월부터는 사업자등록증이 있는 자만 판매점 영업을 할 수 있도록 개선한다.

△ 판매점이 기존에 보유하고 있는 서류는 이동통신 3사가 자비용으로 수거, 폐기한다.

△ 판매점에서는 개인정보 서류를 서면(사본) 형태로 보관할 수 없도록 하고, 가입신청서 등 필요 서류는 전자문서로 변형하여 판매점에서 이동통신사

서버에 실시간 전송・보관하도록 보호조치를 강화한다.(2009년 하반기)

△ 이동통신사는 판매점에 대리점과의 정산 업무 및 고객 응대 등에 필요한 제한적인 조회시스템을 제공한다.(2009년 9월) 판매점을 인증하여 시스템 접속 권한을 부여하고, 고객정보 조회 가능 기간은 개통일부터 6개월 이내로 제한적으로 운영한다. 이동통신사는 판매점이 조회할 수 있는 개인정보의 항목별 표시제한 규칙을 마련하여, 조회시스템에 적용하도록 한다.

△ 가입 시 제출한 개인정보 관련 서류를 반환받아 가도록, 현수막이나 신청서 안내문구 등을 통해 홍보한다.

그러나 고객 서류 보관 금지 등 일부 대책들은 이미 오래전부터 반복적으로 제시되어온 것들이다. 이동통신사가 판매점과 직접적인 계약 관계를 맺고 있지 않은 상황에서, 과연 판매점들이 제대로 정보보호 조치를 수행하도록 통제할 수 있을지 의문이다. 2009년 5월의 조치에서도 이동통신사와 판매점 사이의 불명확한 계약관계에 대한 해결책은 제시되지 않았다. 개인정보 보호의 측면에서는 판매점 역시 이동통신사와 위탁 관계를 맺고 있는 대리점과 같은 수준으로 관리되는 것이 적절할 것이다. 물론 이동통신사 입장에서는 만 개가 넘는 판매점을 직접 관리하는 것이 큰 부담일 수 있으나, 자사의 필요성에 의해 수많은 판매점과 관계를 맺고 있는 것인 만큼, 그에 따른 부담도 질 필요가 있을 것이다.

### 4) 개인정보의 파기

「이동통신서비스제공자의 개인정보 보호지침」[116] 제5조에 따르면, 이동통신사는 가입정보의 보유기간 및 이용기간을 해지 후 6개월 이내로 정해야 한다. 즉, 해지 후 6개월 이상 보유해서는 안된다. 다만, 「통신비밀보호법」, 「국세기본법」 규정에 따른 경우, 해지고객이 이용요금을 미납한 경우, 고객과의 분쟁이 발생하여 보유기간 내에 분쟁이 해결되지 않은 경우 등에는 필요한 범위 내에서 보관할 수 있도록 하고 있다. 또한,「통신비밀보호법」및 「국세기본법」에 의해 해당 정보를 보유하는 경우 가입고객 데이터베이스와 분리하여 별도의 해지고객 데이터베이스에 보관・관리하도록 하고 있다.

> 제5조(가입정보의 이용 및 보관) ①이동통신서비스제공자는 제3조의 규정에 의해 가입정보 수집에 대한 동의를 얻고자 하는 경우에는 수집하는 가입정보의 보유기간 및 이용기간을 가입고객이 쉽게 확인할 수 있도록 미리 고지하거나

116) 2005년 9월 29일 정보통신부 제정.

서비스이용약관에 명시하여야 한다.
②이동통신서비스제공자는 가입정보의 보유기간 및 이용기간을 해지 후 6개월 이내로 정하여야 한다. 다만, 다음 각 호의 1에 해당하는 경우에는 그 기간이 도래하거나, 조건이 성취되는 때까지 필요한 범위 내에서 가입정보를 보관할 수 있다.
1. 통신비밀보호법 제15조의2 규정에 의하여 당해 사업자가 통신사실확인자료 제공 시 필요한 성명, 주민번호, 전화번호의 경우 12개월
2. 국세기본법 제85조의3 규정에 의하여 보관하는 성명, 주민번호, 전화번호, 청구지 주소, 요금납부내역(청구액, 수납액, 수납일시, 요금납부 방법)의 경우 5년
3. 해지고객이 이용 요금을 납부하지 않은 경우
4. 이동통신서비스제공자와 가입고객 간 요금 관련 분쟁이 발생한 경우에 보유기간 내에 당해 분쟁이 해결되지 않은 경우
③이동통신서비스제공자는 제2항 각호의 규정에 의하여 개인정보를 보유하고자 하는 경우에는 보유근거, 보유목적, 보유기간 및 보유하는 개인정보 항목을 가입고객에게 미리 고지하거나 서비스 이용약관에 명시하여야 한다.
④이동통신서비스제공자는 제2항 제1호 및 제2호의 규정에 따라 해당 정보를 보유하는 경우 가입고객 데이터베이스와 분리하여 당해정보를 별도의 해지고객 데이터베이스에 보관·관리하고 그 접근권한을 최소화하여야 한다.

그런데 각 이동통신사의 개인정보취급방침에는 위 내용이 포함되어 있지 않은 경우도 있었고, 각 이동통신사마다 내용에 많은 차이를 보였다. 다음은 각 이동통신사의 개인정보취급방침 중 '개인정보의 보유기간 및 이용기간' 항목의 내용이다.

<표 2-43> 각 이동통신사의 '개인정보의 보유기간 및 이용기간' 내용

| | 개인정보의 보유기간 및 이용기간 |
|---|---|
| A이동통신사 | ① 고객님의 개인정보는 다음과 같이 개인정보의 수집 목적 또는 제공받은 목적이 달성되면 파기됩니다.<br>- 회원가입정보의 경우: 회원가입을 탈퇴하거나 회원에서 제명된 때<br>- 대금지급정보의 경우: 대금의 완제일 또는 채권 소멸시효 기간이 만료된 때<br>- 배송정보의 경우: 물품 또는 서비스가 인도되거나 제공된 때<br><br>② 단, 다음 각호의 1에 해당하는 경우에는 그 기간이 도래하거나, 조건이 성취되는 때까지 필요한 범위 내에서 가입정보를 보관할 수 있습니다(회원가입정보의 경우, 회원가입을 탈퇴하거나 회원에서 제명된 경우 등에 대해서는 사전에 보유목적, 기간 및 보유하는 개인정보 항목을 명 |

| | |
|---|---|
| | 시하여 동의를 구합니다).<br>가. 상법 등 관련법령의 규정에 의하여 거래 관련 권리·의무관계의 확인 등을 이유로 일정기간 보유하여야 할 필요가 있을 경우에는 일정기간 보유합니다. 이와 같은 정보의 종류와 보유기간, 근거 법령의 예는 아래와 같습니다.<br>- 상업장부와 영업에 관한 중요서류에 포함된 개인정보: 10년(상법)<br>- 전표 또는 이와 유사한 서류에 포함된 개인정보: 5년(상법)<br>- 국세기본법 제85조의3 규정에 의하여 보관하는 성명, 주민번호, 전화번호, 청구지 주소, 요금납부내역(청구액, 수납액, 수납일시, 요금납부 방법), 기타 거래에 관한 장부 및 등기서류: 관련 국세의 법정신고기한이 경과한 날부터 5년(국세기본법)<br>- 계약 또는 청약철회 등에 관한 기록(전자상거래등에서의 소비자보호에 관한 법률): 계약 또는 청약 철회시로부터 5년<br>- 대금결제 및 재화 등의 공급에 관한 기록: 공급시로부터 5년(전자상거래등에서의 소비자보호에 관한 법률)<br>- 소비자의 불만 또는 분쟁처리에 관한 기록: 불만 또는 분쟁 처리시로부터 3년 (전자상거래등에서의 소비자보호에 관한 법률)<br>- 표시/광고에 관한 기록 : 6개월(전자상거래등에서의 소비자보호에 관한 법률)<br>- 신용정보의 수집/처리 및 이용 등에 관한 기록: 3년(신용정보의 이용 및 보호에 관한 법률)<br>- 통신비밀보호법 제15조의2 규정에 의하여 통신사실확인자료 제공 시 필요한 성명, 주민등록번호, 이동전화번호: 12개월<br>- 통신비밀보호법 시행령 제21조의4 제2항 규정에 의하여 가입자의 전기통신일시, 전기통신 개시·종료 시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료 등: 12개월<br>- 통신비밀보호법 시행령 제21조의4 제2항 규정에 의하여 컴퓨터 통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그 기록자료, 컴퓨터 통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료: 6개월<br>나. 기타 개별적으로 이용자의 동의를 받은 경우: 동의 받은 기간<br>다. 해지신청한 고객이 이용 요금을 납부하지 않은 경우: 요금 완납시까지<br>라. 이동통신서비스제공자와 가입고객 간 요금 관련 분쟁이 발생한 경우에 보유기간 내에 당해 분쟁이 해결되지 않은 경우: 분쟁 완결시까지<br><br>③ 고객님의 동의를 받아 보유하고 있는 거래정보 등의 열람을 요구하는 경우, 회사는 지체 없이 그 열람을 허용합니다. |

| | |
|---|---|
| | ④ 회사와 가입자 간에 분쟁 발생할 가능성이 있을 경우 입증자료 보관을 위하여 5년 동안 회사는 해지고객님의 개인정보 중 성명, 주민번호, (해지)이동전화번호, 요금청구내역과 납부내역, 부가서비스 내역, 통화내역, 상담내역 등 7개 항목을 보관할 수 있습니다. |
| B이동통신사 | 1. 고객의 개인정보는 (B이동통신사)이 고객에게 서비스를 제공하는 기간 동안에 한하여 보유 및 이용됩니다. 다만, 관계법령의 규정에 의하여 보존할 필요성이 있는 경우에는 관계법령에 따라 보존합니다.<br><br>2. 관계법령의 규정에 의하여 보존할 필요성이 있는 정보 및 보유기간은 아래와 같습니다.<br>가. 요금의 정산, 요금 과오납 등 분쟁 발생 시 입증을 위하여 해지 후 개인정보(과금정보포함) : 해지일로부터 6개월. 단, 해지고객이 이용대금을 납부하지 않았거나 고객과 요금관련분쟁이 있는 때에는 해결 시까지 보유<br>나. 통신비밀보호법 제15조의2 규정에 의하여 통신사실확인자료 제공 시 필요한 성명, 주민등록번호, 이동전화번호 : 12개월<br>다. 통신비밀보호법 시행령 제21조의4 제2항의 규정에 따라 가입자의 전기통신 일시, 전기통신 개시·종료시간, 통신번호 등 상대방의 가입자 번호, 사용도수, 정보통신망에 접속된 정보통신기기의 위치자료: 12개월<br>라. 국세기본법, 법인세법, 부가가치세법에 따른 성명, 주민등록번호, (해지)이동전화번호, 청구서 배달 주소, 요금 등 거래내역 관련 정보 : 5년 |
| C이동통신사 | ① (C이동통신사)는 고객님의 개인정보를 서비스 가입기간 또는 분쟁처리 기간 동안 이용하고, 요금정산, 요금과오납 등 분쟁 대비를 위해 해지후 6개월까지 보유 합니다. 단, 요금의 과납 또는 미납이 있을 경우와 분쟁이 있을 경우 해결 시까지 보유 합니다. 단, 관계법령의 규정에 의하여 보존할 필요가 있는 경우 (C이동통신사)는 아래와 같이 관계 법령에서 정한 일정한 기간 동안 고객정보를 보관합니다.<br>- 보존 항목: 고객명, 고객식별번호(주민등록번호/여권번호/외국인등록번호 등), 전화번호(이동/일반), 요금내역(청구액, 부가세액, 납부액, 청구년월일, 납부연월일), 요금납부방법, 요금납부자명, 이용서비스, 감액금액 및 사유, 요금 청구지 주소 등<br>- 보존 근거: 국세기본법 제85조의3<br>- 보존 기간: 5년<br>② 기타<br>- 표시/광고에 관한 기록: 6개월(전자상거래등에서의 소비자보호에 관한 법률)<br>- 계약 또는 청약철회 등에 관한 기록: 5년(전자상거래등에서의 소비자보호에 관한 법률)<br>- 대금결제 및 재화 등의 공급에 관한 기록: 5년(전자상거래등에서의 |

| | |
|---|---|
| | 소비자보호에 관한 법률)<br>- 소비자의 불만 또는 분쟁처리에 관한 기록: 3년(전자상거래등에서의 소비자보호에 관한 법률)<br>- 신용정보의 수집/처리 및 이용 등에 관한 기록: 3년(신용정보의 이용 및 보호에 관한 법률) |

A이동통신사는 B, C이동통신사와 달리 해지 후 6개월 동안 보관한다는 규정이 없다. 물론 A이동통신사의 경우 회원 탈퇴 즉시 삭제하고 있다면 바람직한 일이다. 다만, 분쟁가능성이 있을 경우에는 5년 동안 보관한다고 하여, 「이동통신서비스제공자의 개인정보 보호 지침」을 따르지 않았다. 또한, A이동통신사는 B, C이동통신사와 비교하여 관련 법령에 의해 보존하는 개인정보의 항목, 보유근거, 보유목적, 보유기간을 상세히 제시하였다. B, C이동통신사도 사실상 A이동통신사와 마찬가지로 관련 정보를 보존하고 있다면, 그 내용을 상세히 공개할 필요가 있다. C이동통신사의 경우에는 「통신비밀보호법」에 따른 기록 보존에 대해서도 명시하고 있지 않다. A이동통신사와 B이동통신사의 경우, 「통신비밀보호법」에 따른 개인정보의 보존을 명시하고 있지만, 내용이 다소 수정될 필요가 있다. 「통신비밀보호법」 시행령 제21조의4는 현재 동법 시행령 제41조로 개정되었다. 또한, 인터넷 로그기록 등의 보존기간은 3개월로 되어있는데, A이동통신사는 이를 6개월로 잘못 기술하였다. 개인정보취급방침도 약관의 하나인데, 수백만 명의 가입자를 보유하고 있는 이동통신사라면 개인정보취급방침을 좀 더 세심하게 관리할 필요가 있다.

한편, 해지고객의 데이터베이스를 별도로 보관하라는 위 지침 제4항의 규정도 C이동통신사 외에는 명시하고 있지 않았다. 위 <표 2-39>을 보면, 지금까지 다수의 통신업체에서 해지자의 정보를 파기하지 않고 있음이 드러난 바 있다. 해지 후에도 수년 동안 개인정보가 통신업체에 보관되고 있다는 점에서 개인정보 유출이나 남용의 가능성은 열려 있다.

초고속인터넷업체의 경우에도 마찬가지이다. 아래 <표 2-44>에서 볼 수 있다시피, A초고속인터넷업체가 가장 상세하게 규정하고 있다. B초고속인터넷업체의 경우에는 관련 법령이라고 되어 있을 뿐, 보유근거나 보유항목 등을 명시하지 않고 있다.

<표 2-44> 각 초고속인터넷업체의 '개인정보의 보유기간 및 이용기간' 내용

| | 개인정보의 보유기간 및 이용기간 |
|---|---|
| A초고속인터넷업체 | 회사는 원칙적으로 다음과 같이 개인정보 수집 및 이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다.<br>- 회원가입정보의 경우: 회원가입을 탈퇴하거나 회원에서 제명된 때<br>- 대금지급정보의 경우: 대금의 완제일 또는 채권 소멸시효 기간이 만료된 때<br>- 배송정보의 경우: 물품 또는 서비스가 인도되거나 제공된 때<br><br>1. 회사 서비스 신청고객: 서비스 가입일~해지일까지 이용하고, 요금 정산분쟁 대비를 위해 해지 후 또는 요금 완납 후 6개월까지 보유합니다. 단, 요금의 과납 또는 미납이 있을 경우와 분쟁이 있을 경우 해결 시까지 보유합니다. 또는 관련법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 관계법령이 정한 일정한 기간 동안 고객정보를 보관합니다.<br><br>2. 홈페이지 회원서비스 가입고객 : 회원 탈퇴 시 즉시 파기합니다.<br>단, 관계법령의 규정에 의하여 보존할 필요가 있는 경우 회사는 관계법령에서 정한 일정한 기간 동안 회원정보를 보관합니다. 이 경우 회사는 보관하는 정보를 그 보관의 목적으로만 이용하며 보존이유 및 기간은 아래와 같습니다.<br>- 상업장부와 영업에 관한 중요서류에 포함된 개인정보: 10년(상법)<br>- 전표 또는 이와 유사한 서류에 포함된 개인정보: 5년(상법)<br>- 법인세법, 부가가치세법, 국세기본법 제85조의3 규정에 의하여 보관하는 성명, 주민번호, 전화번호, 청구지 주소, 요금납부내역(청구액, 수납 액, 수납 일시, 요금납부 방법), 기타 거래에 관한 장부 및 등기서류: 관련 국세의 법정신고기한이 경과한 날부터 5년(국세기본법)<br>- 계약 또는 청약철회 등에 관한 기록 : 계약 또는 청약 철회 시로부터 5년(전자상거래등에서의 소비자보호에 관한 법률)<br>- 소비자의 불만 또는 분쟁처리에 관한 기록: 불만 또는 분쟁 처리시로부터 3년 (전자상거래등에서의 소비자보호에 관한 법률)<br>- 표시/광고에 관한 기록 : 6개월(전자상거래등에서의 소비자보호에 관한 법률)<br>- 신용정보의 수집/처리 및 이용 등에 관한 기록: 3년(신용정보의 이용 및 보호에 관한 법률) |
| B초고속인터넷업체 | 가. 회사는 수집된 고객의 개인정보를 고객의 계약 해지일까지 이용하며, 요금정산 · 요금 오납 등의 분쟁 대비를 위해 해지 후 6개월, 요금<br>정산시 미완료된 경우 해결완료일부터 6개월까지 보유합니다. 이 경 |

| | |
|---|---|
| | 우 회사가 개인정보등을 제3자에게 제공하는 경우에는 제3자에게 파기하도록 지시합니다. 회사는 개인정보의 수집 · 이용목적을 달성하거나, 개인정보의 보유 및 이용기간이 종료한 경우, 사업을 폐지 하는 경우에는 개인정보를 지체 없이 파기합니다. 다만, 법률에 특별한 규정이 있는 경우에는 관계 법령에 따라 보관합니다.<br>- 보관기간 : 5년 |
| C초고속인터넷업체 | 1. (C초고속인터넷업체)은 고객님의 개인정보를 고객님께 서비스를 제공하는 기간(이용기간) 또는 분쟁처리 기간(보유기간) 동안에 한하여 보유하고 이를 활용합니다. 다만, 법률에 특별한 규정이 있는 경우에는 관계 법령에 따라 보관됩니다.<br>- 이용기간 : 서비스 가입일 ~ 해지일까지<br>- 보유기간 :요금정산, 요금과오납 등 분쟁 대비를 위해 해지후 6개월까지 (단, 요금 미납이 있을 경우 해결시까지 보유)<br>2. 해지고객 개인정보는 국세기본법 제85조의3 규정에 따라 다음 항목의 정보를 보관합니다.<br>- 보관항목 :고객명, 고객식별번호, 전화번호, 요금내역(청구액, 부가세액, 수납액, 청구년월일, 수납년월일), 요금납부자명, 이용서비스, 감액금액 및 사유, 요금 청구지 주소 등<br>- 보관기간 : 5년 |

## 3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태

### 1) 열람 및 정정·삭제 청구권 보장 방식

앞서 하나로텔레콤의 고객 정보 제3자 제공 사건에 대해 검토한 바 있다. 이 사건은 개인정보주체의 열람 및 정정·삭제 청구권 보장 실태와도 연관되어 있다. 2008년 6월 27일, 공정거래위원회는 하나로텔레콤의 개인정보 도용 사건과 관련하여 소비자에 대해 본인의 명의도용여부 확인이나 피해의 회복 등 필요한 조치를 취하라는 내용의 시정명령을 하기로 의결하였다(공정거래위원회, 2008).

2008년 4월 22일, 서울지방경찰청이 하나로텔레콤에 대한 수사결과를 발표한 이후, 소비자들은 하나로텔레콤에 자신의 개인정보가 도용되었는지에 대한 확인을 요청하였다. 그러나 하나로텔레콤은 도용여부의 확인이나 처리상황의 통지 등 어떠한 조치도 하지 않고, 다만 '양해의 말씀' 또는 '정확한 내역을 파악하고 있는 중' 등의 내용으로 민원인에게 답변했다고 한다. 공정위는 이에 대해 「전자상거래 등에서의 소비자보호에 관한 법률」(이하 「전자상거래법」) 제11조제2항[117] 위반이라고 보았다.

동법 시행령 제12조[118]는 법률에서 규정한 '필요한 조치'의 상세한 내용을 담고 있는데, '도용여부의 확인 및 당해 소비자에 대한 관련거래 기록의 제공', '변조된 소비자에 관한 정보의 원상회복', '도용에 의한 피해의 회복' 등이다. 하나로텔레콤을 인수한 SK브로드밴드는 공정위의 시정명령에 대해 행정소송을 제기하였으나, 2009년 7월 21일 서울고등법원은 시정명령이 정당하다고 판결했다. SK브로드밴드는 대법원에 항소한 상태이다. 한 언론은 개인정보 피해자들이 피해사실 입증을 위해 '개인정보 이용 및 제공 내역'을 요구했으나, 업체에서 이에 응하지 않고 있으며, 다른 통신업체 역시 마찬가지라고 보도했다.[119] 「전자상거래법」 제11조제2항에 의하지 않더라도, 정보주체의 열람권은 「정보통신망법」 제30조에 의해 보장되고 있다. 이에 따르면, 이용자들은 자신의 '개인정보를 이용하거나 제3자에게 제공한 현황'에 대한 열람을 요구할 수 있다.

제30조(이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.
② 이용자는 정보통신서비스 제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람이나 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다.
1. 정보통신서비스 제공자등이 가지고 있는 이용자의 개인정보
2. 정보통신서비스 제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 현황
3. 정보통신서비스 제공자등에게 개인정보 수집·이용·제공 등의 동의를 한 현황

---

117) 제11조 (소비자에 관한 정보의 이용 등) ①사업자는 전자상거래 또는 통신판매를 위하여 소비자에 관한 정보를 수집 또는 이용(제3자에게 제공하는 경우를 포함한다. 이하 같다)하고자 하는 경우에는 정보통신망이용촉진및정보보호등에관한법률 등 관련 규정에 따라 이를 공정하게 수집 또는 이용하여야 한다.
②사업자는 재화등을 거래함에 있어서 소비자에 관한 정보가 도용되어 당해 소비자가 재산상의 손해가 발생하였거나 발생할 우려가 있는 특별한 사유가 있는 경우에는 본인확인이나 피해의 회복 등 대통령령이 정하는 필요한 조치를 취하여야 한다.

118) 제11조제2항에서 규정한 '대통령령이 정하는 필요한 조치'는 전자상거래에 등에서의 소비자보호에 관한 법률 시행령 제12조에 규정되어 있다.
시행령 제12조 (소비자에 관한 정보의 확인 등) 법 제11조제2항에서 "대통령령이 정하는 필요한 조치"라 함은 다음 각호의 1을 말한다.
1. 소비자 본인이 요청하는 경우 도용여부의 확인 및 당해 소비자에 대한 관련거래 기록의 제공
2. 도용에 의하여 변조된 소비자에 관한 정보의 원상회복
3. 도용에 의한 피해의 회복

119) 한겨레. 2009.8.4. "'내 개인정보 어떻게 이용했나'-통신업체, 열람요구 묵살 여전."

본 연구는 이동통신사와 초고속인터넷 서비스 사업자들의 정보주체의 열람 및 정정·삭제 청구권 보장 실태에 대해 조사하였다.

각 업체의 '개인정보 취급방침' 상의 '이용자 및 법정대리인의 권리와 그 행사방법'이라는 항목에서 정보주체의 개인정보 열람·정정·삭제 청구권 및 행사방법을 알리고 있다. A이동통신사 및 A초고속인터넷업체의 경우에는 개인정보의 이용·제공 내역에 대한 열람권을 명시하고 있으나, 타 업체의 경우에는 개인정보에 대한 열람·정정 등에 대해 규정하고 있을 뿐 제공 내역에 대한 열람권은 명시하고 있지 않았다. 개인정보의 열람·정정 등을 청구하는 방식에 대한 설명도 각 업체마다 차이가 있다. 예를 들어, A이동통신사나 B이동통신사의 경우, 개인정보에 대한 '열람·증명'을 위해서는 대리점에 방문해야 한다. C초고속인터넷업체는 전화, 이메일을 통한 '열람·증명'도 허용하며, 다른 업체들은 '열람·증명'과 관련된 내용이 없다.

<표 2-45> 업체별 열람 청구권 관련 내용

| 업체명 | 열람 청구권 관련 내용 (일부) |
|---|---|
| A이동통신사 | 고객님은 언제든지 회사가 보유하는 개인정보, 개인정보의 이용·제공 내역, 수집·이용·제공에 대한 동의내역을 열람하거나 정정하실 수 있습니다. 해당 개인정보에 오류가 있거나 보존기간이 경과한 것이 판명되는 등 정정·삭제를 할 필요가 있다고 인정되는 경우에는 지체 없이 시행하겠습니다.<br>- 고객님은 직영대리점 및 위탁업무계약을 맺은 대리점에 방문하여 개인정보에 대한 열람·증명을 요구할 수 있고, 방문하신 곳이나 방문하신 분에 따라 열람 가능한 정보가 제한적일 수 있습니다.<br>- 온라인 가입 정보의 열람 및 정정을 하고자 할 경우에는 웹사이트 내 "회원정보변경" 을 클릭하여 직접 열람 또는 정정하거나, 사이버 고객센터 온라인 문의 또는 고객센터(****-****) 전화 문의 및 웹마스터에게 E-mail로 연락하시면 지체 없이 조치하겠습니다. |
| B이동통신사 | - (B이동통신사)는 고객이 개인정보에 대한 열람·증명 또는 정정을 요구하는 경우에는 고객의 요구에 성실하게 대응하고, 해당 개인정보에 오류가 있거나 보존기간을 경과한 것이 판명되는 등 정정·삭제를 할 필요가 있다고 인정되는 경우에는 지체 없이 정정·삭제를 합니다.<br>- 고객은 (B이동통신사)와 위탁업무계약을 맺은 지점에 방문하여 개인정보에 대한 열람·증명을 요구할 수 있고, 고객이 제공한 개인정보를 보다 철저하게 보호하기 위하여 고객의 지점 방문 이외의 전화·우편·FAX 등 기타의 신청방법에 의하여는 고객의 개인정보에 대한 열람·증명을 제공하지 않습니다. |

| | |
|---|---|
| C이동통신사 | 1. 고객님은 언제든지 등록되어 있는 고객님의 개인정보를 조회하거나 수정할 수 있으며 가입해지를 요청할 수도 있습니다.<br>2. 고객님의 개인정보 조회, 수정을 위해서는 '개인정보변경'(또는 '고객정보수정' 등)을, 가입 해지(동의철회)를 위해서는 '해지신청서'를 작성하여 (C이동통신사)에 제출하거나, 웹사이트 고객님의 경우 '가입탈퇴'를 클릭하여 본인 확인 절차를 거치신 후 직접 열람, 정정 또는 탈퇴가 가능합니다. |
| A초고속인터넷업체 | 1. 고객(만 14세 미만의 아동의 경우 법정대리인 포함)은 언제든지 등록되어 있는 자신의 개인정보의 수집.이용.제공내역을 열람하거나 정정하실 수 있습니다.<br>2. 홈페이지 회원서비스 고객의 개인정보를 조회 수정을 위해서는 홈페이지에서 로그인후 고객센터-회원정보 조회/변경-'회원정보수정, 회원탈퇴'를 선택하면 직접 열람, 정정 또는 탈퇴가 가능합니다. 혹은 개인정보관리책임자 및 회사 고객센터(****-****)로 서면, 전화 또는 이메일로 연락하시면 지체없이 조치하겠습니다.<br>3. 인터넷 관련 서비스 고객들의 개인정보를 조회 수정하기 위해서는 회사 고객센터(****-****)로 연락하시거나 사이버고객센터(www.****.com)로 요청하시면 지체없이 조치하겠습니다. |
| B초고속인터넷업체 | 고객은 자신의 개인정보를 열람하거나 정정, 동의의 철회를 하실 수 있습니다. 개인정보의 열람 및 정정, 동의를 철회 하고자 할 경우에는 유선전화(***)를 통하여 개인정보의 수집 및 활용에 대한 동의의 철회, 열람, 정정이 가능하며 회사는 지체 없이 그에 필요한 조치를 취합니다. 한편, 고객께서 개인정보의 오류에 대한 정정을 요구한 경우 정정을 완료하기 전까지 당해 개인정보를 이용하지 않습니다. |
| C초고속인터넷업체 | 고객님(만 14세 미만 아동의 경우 법정대리인 포함)께서는 언제든지 개인정보에 대한 열람, 정정을 요구하시거나 가입해지 및 개인정보의 수집과 이용, 위탁 또는 제공에 대한 동의를 철회를 하실 수 있습니다. 고객님의 개인정보 열람 및 정정을 위해서는 '개인정보변경'(또는 '고객정보수정' 등)을, 가입해지(동의철회)를 위해서는 '해지신청서'를 작성하여 회사에 제출하거나, 웹사이트 고객님의 경우 '가입탈퇴'를 클릭하여 본인 확인 절차를 거치신 후 직접 열람, 정정 또는 탈퇴가 가능합니다.<br>- 고객님(법정대리인)께서는 (C초고속인터넷업체)를 직접 방문하시거나 전화, 이메일 등을 통하여 개인정보에 대한 열람증명을 요구할 수 있습니다. |

### 2) 정보주체의 열람 및 정정·삭제 청구권 보장 실태

대부분의 사업자들은 이용자 본인의 개인정보를 홈페이지를 통해 열람, 수정할 수 있도록 제공하고 있다. 예를 들어 한 초고속인터넷업체의 경우에도

해당 이용자의 개인정보 및 이용하는 서비스의 요금을 조회할 수 있도록 제공한다. 온라인으로 열람할 수 있는 개인정보에는 가입 시 입력했던 연락처, 주소 외에도 서비스에 관련된 내용, 즉 약정 기간, 시작일, 종료일, 임대장비 정기계약 등이 포함된다. 요금조회를 통해 당월 청구내역, 지난 요금조회, 가입자별/서비스별 청구내역 등을 볼 수 있다.

그러나 개인정보를 제3자에게 제공한 내역을 열람할 수 있도록 허용하고 있는 사업자들은 없었다. 물론 각 업체의 '개인정보 취급방침'에는 개인정보를 취급위탁하는 업체와 개인정보를 제공받는 제휴업체(제3자)의 목록이 공개되어 있다. 그러나 이는 각 업체가 취급위탁, 혹은 제3자 제공 관계를 맺고 있는 업체들의 목록일 뿐, 이것만으로는 내 개인정보가 실제로 어떤 업체에 제공되었는지 알기 힘들다. 또한 개인정보의 제3자 제공의 경우에는 이용자의 '동의'가 필요한데, 실제로 내가 언제, 어떻게 동의를 했는지에 대한 사실관계를 각 업체의 홈페이지를 통해 파악하기는 힘들다.

기본적인 개인정보와 서비스 이용현황은 각 업체의 홈페이지를 통해 열람할 수 있기 때문에, 본 연구는 △ (이동통신사의 경우) 통화내역, △ (초고속 인터넷 업체의 경우) 인터넷 이용내역, △ 개인정보 제3자 제공 내역에 대해 정보주체 열람청구를 진행하였다.

각 이동통신사들은 이용자들의 통화내역을 홈페이지를 통해 기본적으로 제공하고 있지는 않지만, 대리점 방문을 통해 열람할 수 있는 절차를 마련해두고 있었다. 기본적으로 본인 혹은 대리인이 대리점을 방문해서, 본인 확인 후 열람할 수 있다. 열람가능 기간은 각 이동통신사별로 약간 차이가 있었는데, A이동통신사는 최근 4개월, B이동통신사는 최근 7개월, C이동통신사은 최근 6개월까지 열람을 허용하였다. 수신한 통화의 내역은 열람할 수 없으며, 발신 통화 내역만 열람 가능한데, 세부적으로는 통화일시, 상대방 전화번호, 사용시간, 통화요금 등을 열람할 수 있다.[120] 각 이동통신사마다 통신내역 열람을 허용하는 기간이 다른 것은 정보주체의 열람권한을 이동통신사들이 자의적으로 제한하고 있음을 보여준다.

직접 방문이 어려운 경우에는 팩스로도 열람 가능한데, 열람신청서를 작성한 후 신분증과 함께 팩스로 전송하면 된다. 다만, 이 경우 일부 번호가 *로 표시된다고 한다. 또한, 별도의 온라인 열람 신청서를 작성한 이용자의 경우

120) A이동통신사의 경우, 실제 통화내역에 대한 열람청구를 해 본 결과, 발신번호, 통화시각, 이용한서비스(일반 음성통화인지 문자메시지인지 등), 사용시간, 통화량 도수(kb), 할인 전 금액, 할인 금액, 청구 금액, 할인 내용 서비스 설명 등의 정보를 포함하고 있었다.

에는 온라인에서 통화내역을 열람할 수 있도록 하고 있다. 이 경우 열람가능 기간, 조회 횟수 등에 제한이 있었다. 통화 내역에 통화한 기지국 정보(이용자의 위치정보)는 공통적으로 포함하고 있지 않았다.[121] 그러나 이동통신사가 4개월 내지 7개월 치의 통신내역 열람을 허용한다고 해서, 그 기간만큼만 보관하고 있는 것은 아니다. 「통신비밀보호법」 시행령 제41조 2항은 전기통신사업자의 통신사실 확인자료 의무 보관기간을 규정하고 있는데, 통화내역 및 기지국 정보 등은 12개월 동안 보관하도록 하고 있다. 수사기관에는 제공되는 통화내역이 정작 정보주체인 당사자에게는 제한적으로 제공되고 있는 것이다.

국가정보원의 인터넷 감청이나 패킷 모니터링을 통한 타겟 마케팅 등이 언론에 보도되면서, 초고속인터넷 서비스 업체들이 이용자들의 인터넷 이용 내역을 기록하고 있는지, 기록하고 있다면 어느 정도 구체적으로 기록하고 있는지에 대한 관심이 높아지고 있다. 즉, 인터넷 서비스 업체들은 내가 어떤 사이트에 접속하고 있는지, PC에서 어떤 프로그램을 이용하고 있는지 등을 모니터링하고 있을까하고 궁금해 하고 있는 것이다.

우선, 각 업체의 '개인정보 취급방침'에서 공개하고 있는 '수집하고 있는 개인정보 항목' 중에서 서비스 이용 과정에서 자동으로 생성되는 정보는 다음과 같이 되어 있다.

<표 2-46> 이용 과정에서 자동으로 생성되는 정보

| 업체명 | 이용 과정에서 자동으로 생성되는 정보 |
|---|---|
| A초고속인터넷업체 | 서비스 이용기록, 접속 로그, 쿠키, 접속 IP정보, 결제기록, 이용정지기록 등 |
| B초고속인터넷업체 | 이용서비스 종류, 이용시간, 이용량, 이용 금액, 결제기록, 접속로그, 접속IP 정보, 쿠키, 이용정지기록, 발/착신전화번호, 이용컨텐츠 ("서비스이용정보") |
| C초고속인터넷업체 | 서비스 이용 또는 업무처리 과정에서 생성되어 수집될 수 있는 정보<br>○ 서비스 이용시간/이용기록, 접속로그, 이용컨텐츠, 쿠키, 접속IP 정보, 결제기록, 이용정지기록<br>○ 착/발신 전화번호, 통화시각, 사용도수, 위치정보(기지국위치, GPS정보) 등 |

위의 항목은 초고속인터넷 서비스에 대한 것만은 아니다. 각 업체는 초고

121) 이와 관련해서는 본 연구의 제3장 제2절 위치정보에서 자세히 다루었다.

속인터넷 서비스 외에도 IPTV 서비스, 전화 서비스 등을 제공하고 있기 때문이다. 그런데 개인정보 취급방침만 보아서는 서비스 이용기록이 구체적으로 무엇인지 명확하지 않다. 이에 각 업체에서 보관하고 있는 이용자의 인터넷 이용 내역에 대해 개인정보 열람을 청구하였다. 그 결과는 아래와 같은데, B, C초고속인터넷업체 모두 각 업체가 보유하고 있는 정보주체의 서비스 이용기록을 제공하지 않았다. 다만, B초고속인터넷업체는 접속 로그가 남지 않는다고 답변하였으나, C초고속인터넷업체의 경우에는 접속시작시간, 종류시간, 접속 IP 등을 남기는 것으로 보인다. 그런데, 이 외에 추가적으로 기록하는 정보가 있는지는 명확하지 않다.

<표 2-47> 초고속인터넷 서비스 이용기록 열람청구

| 업체명 | 서비스 이용기록에 대한 열람 청구 |
|---|---|
| A초고속인터넷업체 | 열람청구 진행하지 못함. |
| B초고속인터넷업체 | 인터넷 서비스의 경우, 장애처리를 위해 온/오프 상태 여부와 접속을 몇 시간째 유지하고 있는지 여부만을 체크하며, 접속 로그는 남지 않는다고 답변함. IPTV 서비스의 경우에도, 무료 콘텐츠의 이용내역은 남지 않는다고 답변함. 다만, 유료콘텐츠의 경우, 2개월 간 이용내용을 셋탑박스에서 확인할 수 있다고 함. |
| C초고속인터넷업체 | 개인이 요청시 확인이 불가능하나, 전기통신사업법 제54조, 통신비밀보호법 제13조, 제13조의2에 의거하여 수사기관, 법원, 행정기관에서 요청 시 제공이 가능함.<br>서류 : 법원허가서, 공문, 신분증<br>제공범위 : 접속시작시간, 종료시간, 접속IP (접속자 있을시 ID, 계약자명, 주소) |

그러나 개인정보의 제3자 제공 내역에 대한 열람권은 제대로 보장되지 않는 것으로 조사되었다. 위탁업체 및 제휴업체(개인정보를 제공한 제3자 업체)에 대한 개인정보 제공 내역 요구에 대해 A이동통신사와 C초고속인터넷업체는 개인정보 취급방침에서 확인할 수 있다고만 답변하였다. 다만, A이동통신사의 경우 특정 제3자에게 유출되어 피해가 발생할 경우, 특정 업체에 제공되었는지에 대해 확인해줄 수는 있다고 답변했다. 또한, 수사기관이나 법원 등 공공기관에 대한 제공 내역 역시 제공이 불가하다고 답변하였다.

B이동통신사와 B초고속인터넷업체는 제3자 제공 내역을 제공했다. B초고속인터넷업체의 경우, 고객센터를 통한 1차 요청 시에는 타 업체와 마찬가지

로 제3자 제공내역 열람은 불가하며, 개인정보취급방침에서 확인 가능하다고만 답변하였으나, 이에 항의한 2차 청구에서는 제3자 제공내역을 제공해주었다. B초고속인터넷업체는 “제3자 제공 내역은 열람 가능한데, 상담원에 대한 교육이 불충분하여 제대로 안내되지 못하였다. 2009년 6월 이전에는 시스템상 불가능하였으나, 이후 열람하도록 하고 있다”고 해명하였다. 그러나 수사기관 등에 대한 정보제공 내역에 대해서는 B이동통신사는 수사비밀 준수 의무 때문에 공개가 불가능하다고 답변하였으며, B초고속인터넷업체는 수사기관 등에 제공한 내역은 이용자별로 검색할 수 없다고 답변하였다. 즉, 사건번호 등을 특정해서 문의할 경우 확인할 수는 있지만, 주민등록번호 등으로 이용자별 검색은 불가하다는 것이다. C초고속인터넷업체의 경우에는 제휴업체 및 수사기관 등 제3자에 대한 제공내역이 없다고 답변하였다. 제공 내역이 있을 경우에는 제공할 수 있다는 것인지는 모호하다. 위탁에 의해 제공된 내역의 열람청구에 대해서는 개인정보취급방침을 확인하라고 답변하였다.

<표 2-48> 제3자 제공 내역 청구에 대한 답변

| 업체명 | 제3자 제공 내역 청구에 대한 답변 |
|---|---|
| A이동통신사 | - 제3자 제공 내역은 제공 불가. 다만, 특정 제3자에게 유출되어 피해를 입을 경우, 그 업체에 제공되었는지 확인해줄 수는 있음.<br>- 위탁업체와 제휴사에 대해서는 가입신청시 동의서를 통해 안내하고 있으며, 개인정보 취급방침에서 확인할 수 있음. |
| B이동통신사 | - 제3자 제공내역 제공<br>- 제3자 제공 내역 중 수사기관에 제공한 내역 관련해서는 수사비밀을 준수해야할 의무가 있어 공개 불가. |
| C이동통신사 | - 위탁 및 제3자 제공 내용은 개인정보취급방침으로 확인 가능<br>- 수사기관 및 법원에 제공된 내역은 제공 불가 |
| A초고속인터넷업체 | 개인정보열람청구 못함. |
| B초고속인터넷업체 | - ‘개인정보 이용, 제공 내역서’를 문서로 받음. 위탁 및 제3자 제공업체, 제공목적(부가서비스 소개, TV서비스 소개, 전화서비스 소개 등)이 나와 있음.<br>- 수사기관 등에 대한 제공 목록은 이용자별로 검색할 수 없다고 함. 수사기관 등에서 공문을 받고 제공하고 있는데, 사건번호 등을 특정해서 문의할 경우 확인할 수는 있지만, 주민등록번호 등으로 이용자별 검색은 불가하다고 함. |
| C초고속인터넷업체 | - 제휴업체에 대한 제공 내역 없음.<br>- 수사기관 등에 대한 제공내역 없음.<br>- 취급위탁은 개인정보취급방침을 확인하기 바람. |

상당수의 통신업체들이 내 정보의 제3자 제공 내역과 위탁업체에의 제공 내역을 제공하지 않았으며, 개인정보취급방침을 확인하라고 답변하였다. 그러나 나의 개인정보가 모든 위탁업체에 제공되는 것은 아닐 것이다. 수사기관 등에 대한 제공내역에 대해서는 대부분이 제공할 수 없다고 답변하였다.

### 3) 수사기관등에 제공한 내역에 대한 정보주체의 열람권 제한의 타당성

이와 같이 통신업체에서 자신의 개인정보를 수사기관 등에 제공한 내역에 대한 정보주체의 열람권을 제한하는 것이 타당한지 검토할 필요가 있다. 통신업체에서 보유하고 있는 내 개인정보는 크게 이름, 주민등록번호, 주소 등 기본 신상정보인 '통신자료'와 통화 내역이나 로그기록과 같은 '통신사실확인자료'로 나눌 수 있다. 통신업체에서 내 개인정보를 수사기관 등에 제공한 내역의 열람을 거부하는 근거를 명시하지는 않았지만, 「전기통신사업법」 제54조 및「통신비밀보호법」 제13조의5에 근거한 것으로 보인다.

우선 「전기통신사업법」 제54조(통신비밀의 보호)는 통신비밀을 준수할 사업자의 의무와 수사기관 등이 사업자에게 통신자료를 요청할 수 있는 근거를 규정하고 있다. 그러나 통신자료 제공사실이 제1항의 '통신의 비밀' 및 제2항의 '통신에 관하여 알게 된 타인의 비밀'에 해당한다고 할지라도, 정보주체에 제공하는 것 까지 금지하고 있는 것인지는 의문이다. 정보주체에게 제공하는 것을 '누설'이라고 보기는 힘들다.

제54조(통신비밀의 보호) ①누구든지 전기통신사업자가 취급중에 있는 통신의 비밀을 침해하거나 누설하여서는 아니된다.
②전기통신업무에 종사하는 자 또는 종사하였던 자는 그 재직중에 통신에 관하여 알게 된 타인의 비밀을 누설하여서는 아니된다.
③전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장으로부터 재판, 수사(「조세범처벌법」 제11조의2제1항, 제4항 및 제5항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청받은 때에 이에 응할 수 있다.<개정 2002.12.26, 2007.1.3>
1. 이용자의 성명
2. 이용자의 주민등록번호
3. 이용자의 주소

4. 이용자의 전화번호
5. 아이디(컴퓨터시스템이나 통신망의 정당한 이용자를 식별하기 위한 이용자 식별부호를 말한다)
6. 이용자의 가입 또는 해지 일자
④제3항의 규정에 의한 통신자료제공의 요청은 요청사유, 해당이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 "자료제공요청서"라 한다)으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있는 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 해소된 때에 지체없이 전기통신사업자에게 자료제공요청서를 제출하여야 한다.<신설 2000.1.28>
⑤ 전기통신사업자는 제3항 및 제4항의 절차에 따라 통신자료제공을 한 때에는 당해 통신자료제공사실 등 필요한 사항을 기재한 대통령령이 정하는 대장과 자료제공요청서 등 관련자료를 비치하여야 한다.<신설 2000.1.28, 2008.2.29>
⑥ 전기통신사업자는 대통령령이 정하는 방법에 따라 통신자료제공을 한 현황 등을 년 2회 방송통신위원회에 보고하여야 하며, 방송통신위원회는 전기통신사업자가 보고한 내용의 사실여부 및 제5항에 따른 관련자료의 관리상태를 점검할 수 있다.<신설 2000.1.28, 2007.5.11, 2008.2.29>
⑦ 전기통신사업자는 제3항에 따라 통신자료제공을 요청한 자가 소속된 중앙행정기관의 장에게 제5항에 따른 대장에 기재된 내용을 대통령령이 정하는 방법에 따라 통보하여야 한다. 다만, 통신자료제공을 요청한 자가 법원인 경우에는 법원행정처장에게 통보하여야 한다.<신설 2000.1.28, 2002.12.26, 2007.5.11, 2008.2.29>
⑧ 전기통신사업자는 이용자의 통신비밀에 관한 업무를 담당하는 전담기구를 설치·운영하여야 하며, 그 전담기구의 기능 및 구성 등에 관한 사항은 대통령령으로 정한다.<신설 2000.1.28, 2008.2.29>
⑨ 제4항의 규정에 의하여 전기통신사업자에게 제출되는 서면에 대한 결재권자의 범위 등에 관하여 필요한 사항은 대통령령으로 정한다.<신설 2000.1.28, 2008.2.29>

「통신비밀보호법」 제11조, 제12조 및 제13조의5는 통신제한조치 및 통신사실확인자료의 제공에 관한 사항을 외부에 공개하거나 누설해서는 안된다고 규정하고 있다. 여기서 '외부'를 '통신기관' 외부로 해석한다면, 정보주체까지 포함하여 누구에라도 공개해서는 안되는 것으로 해석될 수 있다.[122] 그리고 정보주체에게는 감청 사실, 이메일 등에 대한 압수수색 집행, 통신사실확인자료 제공 등에 대해 사후적으로 통지하도록 하고 있다(동법 제9조의2, 제9조의3, 제13조의3). 그런데, 제13조의5에 따르면, 제11조(비밀준수의 의무) 및 제12조(통신제한조치로 취득한 자료의 사용제한)가 준용되는 경우는

122) 2009년 10월 18일, 법원은 이동통신사가 수사기관에 제공한 통신기록의 내역을 정보주체가 열람할 근거가 없다고 판시하였다. 국민일보. 2009.10.18. "수사기관 '통화조회' 본인도 열람 안돼" 참조.

수사기관이나 정보수사기관에 제공한 경우이며, 법원에 제공되는 경우는 제외하고 있기 때문에, 현행법상으로도 최소한 법원에 제공한 내역에 대해서는 정보주체의 열람권이 보장되어야 할 것으로 보인다.

> 제11조(비밀준수의 의무) ①통신제한조치의 허가·집행·통보 및 각종 서류작성 등에 관여한 공무원 또는 그 직에 있었던 자는 직무상 알게 된 통신제한조치에 관한 사항을 외부에 공개하거나 누설하여서는 아니된다.
> ②통신제한조치에 관여한 통신기관의 직원 또는 그 직에 있었던 자는 통신제한조치에 관한 사항을 외부에 공개하거나 누설하여서는 아니된다.
> ③제1항 및 제2항에 규정된 자외에 누구든지 이 법의 규정에 의한 통신제한조치로 지득한 내용을 이 법의 규정에 의하여 사용하는 경우외에는 이를 외부에 공개하거나 누설하여서는 아니된다.
> ④법원에서의 통신제한조치의 허가절차·허가여부·허가내용 등의 비밀유지에 관하여 필요한 사항은 대법원규칙으로 정한다. [전문개정 2001.12.29]
>
> 제13조의5(비밀준수의무 및 자료의 사용 제한) 제11조 및 제12조의 규정은 제13조의 규정에 의한 통신사실 확인자료제공 및 제13조의4의 규정에 의한 통신사실 확인자료제공에 따른 비밀준수의무 및 통신사실확인자료의 사용제한에 관하여 이를 각각 준용한다.

그러나 「통신비밀보호법」 상 수사기관에 제공한 통신사실확인자료의 내역을 정보주체가 열람할 권한이 없다고 하더라도, 현행 법 규정이 올바른 것인가는 의문이다. 통신제한조치, 즉 감청과 관련해서는 정보주체에게 알릴 경우, 감청의 취지가 무력화될 수 있으므로, 정보주체에게도 관련 사항을 공개하지 않는 것이 일정하게 타당성을 가진다고 할지라도, 통신사실확인자료의 경우에는 이미 완료된 통신에 대한 것이기 때문에 정보주체가 그 사실을 인지하더라도 변경할 수 없기 때문이다.

## 4. 소 결

전 국민 대다수가 이동통신 서비스 및 초고속인터넷 서비스를 이용하고 있다고 봐도 과언이 아니다. 그만큼 통신업체들은 대규모의 개인정보 데이터베이스를 구축·운용하고 있다. 따라서 약간의 관리 소홀로도 대규모 개인정보 유출, 혹은 유용으로 이어질 수 있고, 2008년 하나로텔레콤 사례와 같이 이 같은 사고가 실제로 발생하고 있다.

통신업체들은 이용자들이 제공한 개인정보 외에도 서비스 이용 과정에서

생성된 개인정보를 보유하고 있다. 그러나 각 통신업체들이 공개하고 있는 개인정보 취급방침만을 보아서는 생성정보에 구체적으로 어떠한 개인정보 항목이 포함되어 있는지 모호하다. 특히, 결합상품의 출시가 증가하고 있는 만큼, 각 서비스 별로 수집되는 개인정보 항목을 구체적으로 명시할 필요가 있다.

통신업체들이 업무위탁이나 제휴관계 등을 통해 개인정보를 제공하는 업체가 수천 개에 달한다는 사실은 주목할 필요가 있다. 제공 업체가 증가할수록 통신업체의 이들에 대한 관리, 통제는 취약해질 수밖에 없기 때문이다. 이런 상황임에도 통신업체는 제휴업체나 위탁업체의 전체 목록을 개인정보 취급방침에 공개하고 있을 뿐, 해당 정보주체별로 제3자 제공 내역에 대한 열람은 대체적으로 허용하고 있지 않고 있다. 또한, 개인정보 취급방침만 보아서는 제3자 제공에 자신의 동의가 필요한 것인지, 필수적으로 제공되는 것인지 알기가 힘들다. 지난 2008년에는 대다수 이동통신사 및 초고속인터넷업체에서 정보주체의 동의나 고지 없이 취급위탁을 한 이유로 방송통신위원회의 시정조치를 받은 바 있다.

서비스 가입 내역이나 결제 기록과 같은 개인정보를 통신업체 홈페이지를 통해 정보주체가 열람할 수 있도록 제공하고 있는 것과 같이, 정보주체별 제3자 제공 내역과 동의의 방법(예를 들어, 요금 정산과 같이 동의가 없어도 되는 것인지, 별도의 동의가 필요한 것인지 등)에 대해서도 홈페이지를 통해 쉽게 열람할 수 있도록 할 필요가 있다. 자신의 개인정보가 어디에 제공되었는지 알 수 없다면, 정보주체가 자기정보에 대한 결정권을 행사하기는 불가능할 것이다. 또한, 현재 각 통신업체별로 제3자 제공이나 위탁과 관련하여 자의적으로 구분하고 있기 때문에, 방송통신위원회에서 이와 관련한 구체적인 가이드라인을 마련할 필요가 있다.

또한, 통신사들은 1만여 개가 넘는 판매점을 통해 고객 유치 및 관리를 하고 있는데, 판매점의 부실한 개인정보 관리 문제는 이미 몇 년 전부터 반복적으로 지적되어 왔다. 방송통신위원회는 2009년 5월 1일, 판매점을 통한 개인정보 유출을 막기 위해 이동통신 3사가 공동으로 '개인정보 관리체계 자율개선방안'을 마련했다고 발표하였는데, 이동통신사와 판매점 사이의 불명확한 계약관계에 대한 해결책은 제시되지 않아 판매점의 개인정보 보호조치를 제대로 통제할 수 있을지 의문이다.

각 통신업체의 개인정보취급방침도 각 사별로 차이가 있었는데, 개인정보 취급방침을 통해 공개해야할 사항이 누락되거나 법 조항 등이 잘못 기술된

경우도 있었다. 수백만 명의 가입자를 보유하고 있는 이동통신사라면 개인정보취급방침을 좀 더 세심하게 관리할 필요가 있다.

한편, 본 연구에서 각 통신업체에 대해 정보주체의 열람권 보장 실태에 대한 조사를 수행한 결과, 법에 명시된 열람권이 제대로 보장되고 있지 않음을 확인할 수 있었다. 우선 일부 통신업체는 개인정보취급방침에서 개인정보의 이용·제공내역에 대한 열람권을 명시하고 있지 않았다. 각 통신업체들은 홈페이지를 통해 본인 정보에 대해 열람 및 수정할 수 있도록 하고 있었으나, 제3자에게 제공한 내역을 열람할 수 있도록 하고 있는 사업자들은 없었다. 각 업체가 개인정보취급방침에 공개한 취급위탁업체 및 제휴업체의 목록만으로는 실제로 내 개인정보가 어떤 업체에 제공되었는지 파악하기 힘들다. 각 통신업체에 대해서 △ (이동통신사의 경우) 통화내역, △ (초고속인터넷 업체의 경우) 인터넷 이용내역, △ 개인정보 제3자 제공 내역에 대한 열람청구를 진행하였는데, 우선 각 이동통신사들은 대리점 방문을 통해 일정 기간 동안의 통화내역을 열람할 수 있도록 하고 있었다. 그러나 기지국 정보는 공통적으로 포함하고 있지 않았다. 개인정보의 제3자 제공내역 역시 제대로 보장되지 않고 있었다. 일부 업체는 제3자 제공내역을 제공하였지만, 개인정보취급방침을 확인하라고 한 경우가 많았으며, 수사기관 등에 제공한 내역에 대해서는 대부분이 제공할 수 없다고 답변하였다.

지난 수 년 동안 개인정보 보호에 대한 사회적 인식이 높아지고 법적 규제도 강화되면서 개인정보 취급방침의 공개와 같이 개인정보 보호를 위한 형식적인 조치의 준수 정도는 높아지고 있다. 또한, 인터넷/통신에 기반한 대부분의 업체들은 기본적인 개인정보나 서비스 이용과 관련한 내용을 홈페이지를 통해 열람할 수 있도록 하고 있다. 그러나 서비스 간 융합 등으로 인해 업체간 개인정보의 유통이 급증하고 있는 상황에서, 정보주체가 자신의 개인정보에 대한 결정권을 확실히 보장받기 위해서는 내 개인정보가 어떻게 유통되고 있는지에 대해 정확히 알 수 있어야 한다. 즉, 이제 '개인정보'에 대한 열람뿐만 아니라, '개인정보의 제3자 제공 내역'에 대한 열람이 더욱 중요해지고 있는 것이다. 특히, 방대한 개인정보를 수집하고 있고, 수많은 업체들과 위탁이나 제휴 관계를 맺고 있는 통신 영역에서는 두 말할 나위도 없다.

# 제4절 금융 영역

## 1. 개 요

금융 분야는 서비스의 특성상 개인정보의 집중 및 공동 활용이 가장 광범위한 분야 중 하나다. 타 업종에 비해 신용거래가 많기 때문에 거래 상대방에 대한 신용도를 판단하는 것이 매우 중요한데, 보다 정확한 신용도 판단을 위해서는 다양한 개인정보의 활용이 요구되고 있기 때문이다(한국정보보호진흥원, 2004: 100). 은행연합회와 같은 신용정보집중기관과 신용정보회사들은 대한민국 성인 거의 대부분의 정보를 보유하고 있다고 보아도 과언이 아니다. 신용정보회사들이 전 국민의 본인확인 서비스를 할 수 있는 것도 이 때문이다. 특히 국내 금융회사의 영업형태는 IMF 경제위기 이후, 기업대출의 비중이 줄어드는 대신 개인대출이 급격히 확대되는 모습을 보이고 있으며, 2003년 발생한 신용카드사의 유동성 위기 사태를 거치면서 개인 신용평가의 중요성이 크게 부각되고 있다(한정미, 2007: 9).

금융 시스템의 원활한 작동을 위해 보다 많은 개인신용정보의 수집과 공유가 필요한 반면, 정보주체의 입장에서 이는 프라이버시 침해 위험성이 높아지는 것을 의미한다. 인터넷 뱅킹, 모바일 뱅킹 등 전자적 방식의 금융 거래 증가는 철저한 보안이 이루어지지 않을 경우 해킹이나 시스템 오작동 등으로 인한 개인정보 유출의 위험성을 높인다. 금융회사 간 업무제휴나 자본시장 통합에 따라 개인정보의 공유 범위도 확대되고 있다.[123] 개인정보의 데이터베이스로의 방대한 집적과 여러 기관의 공유는 개인의 개인정보자기결정권을 약화시킨다. 특히, 개인신용정보는 정보주체의 재산이나 경제활동에 치명적인 영향을 미칠 수 있는 매우 민감한 정보이다. 따라서 금융 영역은 개인정보가 보다 엄격하게 보호되어야 할 영역이기도 하다.

123) '자본시장과 금융투자업에 관한 법률'이 2007년 7월 3일 국회를 통과하여, 2009년 2월 4일 시행되었다. 이 법은 자본시장 관련 금융업감의 겸영을 허용하고 자본시장에서 영위하거나 취급할 수 있는 금융업 또는 금융상품의 규제를 철폐하여 증권업·선물업·자산운용업·신탁업 등 자본시장 관련 금융업을 종합적으로 영위하는 금융투자회사의 설립을 허용하는 것을 주된 내용으로 하고 있다(한정미, 2007:10).

## 2. 개인신용정보의 개념과 법제도

### 1) 개인신용정보의 개념

신용정보의 개념은 「신용정보의 이용 및 보호에 관한 법률」(이하 「신용정보법」)에 명시되어 있다. 「신용정보법」 제2조제1호에 의하면, "'신용정보란 금융거래 등 상거래에 있어서 거래 상대방의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보"를 말한다. 이는 2009년 10월 2일 시행된 개정 「신용정보법」에 따른 규정이다.

<표 2-49> 신용정보의 종류

| 구 분 | 내용 | 동의 여부 |
|---|---|---|
| 식별정보 | · 특정 신용정보주체를 식별할 수 있는 정보<br>· 개인의 성명·주소·주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호)·성별·국적 및 직업<br>· 기업 및 법인의 상호·법인등록번호·사업자등록번호·본점 및 영업소의 소재지·설립연월일·목적 및 임원에 관한 사항 등 | O |
| 신용거래정보 | · 상거래와 관련하여 신용정보주체의 거래내용을 판단할 수 있는 정보<br>· 대출·보증·담보제공·가계당좌예금 또는 당좌예금·신용카드·할부금융·시설대여 등의 금융거래 등 | O |
| 금융질서문란정보<br>(불량정보) | · 신용정보주체의 신용도를 판단할 수 있는 정보<br>· 금융거래 등 상거래와 관련하여 발생한 연체·부도·대지급 또는 허위 기타 부정한 방법에 의한 신용질서 문란 행위 등 | X |
| 신용능력정보 | · 신용정보주체의 신용거래능력을 판단할 수 있는 정보<br>· 개인의 재산·채무·소득의 총액, 납세실적 등<br>· 기업 및 법인의 연혁·주식 또는 지분보유현황등 회사의 개황, 판매내역·수주실적·경영상의 주요계약등 사업의 내용, 재무제표등 재무에 관한 사항, 「주식회사의 외부감사에 관한 법률」의 규정에 의한 감사인의 감사의견 및 납세실적 등 | O |
| 공공기록정보 | · 금융거래등 상거래에 있어서 신용정보주체의 식별·신용도 및 신용거래능력을 판단할 수 있는 법원의 심판·결정정보, 조세 또는 공공요금등의 체납정보, 주민등록 및 법인등록에 관한 정보 및 기타 공공기관이 보유하는 정보 | X |

개정 이전의 법률에서는 "'신용정보'라 함은 금융거래등 상거래에 있어서 거래상대방에 대한 식별·신용도·신용거래능력 등의 판단을 위하여 필요로 하는 정보로서 대통령령이 정하는 정보를 말한다."고 규정하여, 식별정보를 신용정보에 포함하고 있었다.

개정 「신용정보법」은 '개인신용정보'를 "신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보를 말한다"(제2조제2호)고 별도로 규정하고 있다. 신용정보가 모두 개인정보인 것은 아니다. 신용정보의 주체는 개인뿐만이 아니라, 기업도 될 수 있다. 신용정보와 개인정보의 구분이 모호하던 것을 이번 개정을 통해 해결한 것이다.

「신용정보법」 시행령 제2조제1항은 신용정보의 종류를 보다 상세히 규정하고 있다.

이와 함께, 예금 등 금융자산을 대상으로 하는 거래에 관한 정보인 '금융거래정보'와 '질병정보'도 개인 신용정보에 포함될 수 있을 것이다. 금융거래정보는 「금융실명거래 및 비밀보장에 관한 법률」(이하 「금융실명제법」)에서 규정하고 있으며, 개인질병정보는 「신용정보법」 제16조에 규정되어 있다.

개인 신용정보에 포함되는 식별정보는 신용거래정보 등 여타 신용정보와 결합되어 있는 식별정보에 한정된다. 식별정보를 신용정보와 구분해서 규정한 이유는 그 처리나 동의의 수준을 달리하기 위해서로 보인다. 개정 「신용정보법」 제34조[124]는 '개인식별정보의 제공·이용'을 규정하고 있는데, 식별정보의 제공시 개인 동의를 원칙으로 하되, 개인신용정보를 제공받기 위하여 신용정보주체를 특정할 목적으로 제공·이용되는 경우, 채권추심 등의 목적으로 사용하는 경우 등은 예외로 하고 있다.

---

124) 제34조(개인식별정보의 제공·이용) ① 신용정보제공·이용자가 개인을 식별하기 위하여 필요로 하는 정보로서 대통령령으로 정하는 정보(이하 "개인식별정보"라 한다)를 신용정보회사등에 제공하려는 경우에는 해당 개인의 동의를 받아야 한다.
② 개인식별정보는 해당 개인이 동의한 목적 또는 해당 개인으로부터 직접 제공받은 경우에는 그 제공받은 목적의 범위에서만 이용되어야 한다.
③ 개인식별정보가 이 법에 따라 개인신용정보를 제공받기 위하여 신용정보주체를 특정할 목적으로 제공·이용되는 경우에는 제1항 및 제2항을 적용하지 아니한다. 이 경우 개인식별정보를 제공받은 자는 제공 요구에 따르기 위한 목적 외의 용도로 그 정보를 이용하거나 제3자에게 제공하여서는 아니 된다.
④ 개인식별정보가 제32조제4항제4호부터 제9호까지의 규정에 따라 제공·이용되는 경우에는 제1항 및 제2항을 적용하지 아니한다.

### 2) 금융부문 개인정보 보호를 위한 법제도

금융부문의 개인정보를 규율하는 주된 법제는 「금융실명제법」과 「신용정보법」이다. 「금융실명제법」은 금융거래정보의 보호에 한정되는 반면, 「신용정보법」은 금융거래정보를 포괄한 식별정보, 대출정보, 연체정보 등 거래처의 신용도 판단여부와 관련되는 정보의 보호에 관한 내용을 규율하고 있다(정연수, 2004: 106).

「금융실명제법」 제4조는 “금융기관에 종사하는 자는 명의인(신탁의 경우에는 위탁자 또는 수익자를 말한다)의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니되며, 누구든지 금융기관에 종사하는 자에게 거래정보등의 제공을 요구하여서는 아니된다”고 규정하고 있다. 다만, △ 법원의 제출명령, 혹은 영장에 따른 제공, △ 조세에 관한 법률에 따른 제공, △ 국정감사 및 조사에 관한 법률에 따른 제공, △ 금융기관에 대한 감독·검사를 위하여 필요로 하는 거래정보의 제공, △ 금융기관 내부나 상호간의 업무상 필요에 따른 제공, △ 외국 금융감독 기관과의 업무협조에 따른 제공, △한국거래소의 필요에 따른 투자매매업자·투자중개업자가 보유한 거래정보의 제공 등은 예외로 한다. 비밀의무는 거래정보를 제공받은 자에게도 적용된다(제4조제4항 및 제5항). 또한, 거래정보를 제공했을 경우, 금융기관은 제공한 거래정보 등의 주요내용·사용목적·제공받은 자 및 제공일자 등을 명의인에게 서면으로 통보해야 한다(제4조의2).

「신용정보법」은 신용정보의 수집, 제3자 제공, 신용정보의 관리, 신용정보주체의 권리 등 개인신용정보 보호를 위한 전반적인 조치를 포함하고 있다. 물론 「신용정보법」은 신용정보의 ‘보호’만을 다루지 않으며, 신용정보의 효율적인 이용을 위한 제반 조치 역시 포함하고 있다. 「신용정보법」상의 개인정보 보호에 대해서는 아래에서 자세히 다루도록 한다.

「금융실명제법」 및 「신용정보법」에서 금융거래정보의 비밀보장과 신용정보의 제공·활용을 제한하고 있음에도 불구하고, 「금융지주회사법」 제48조의2는 금융거래정보 및 신용정보를 금융지주회사 및 자회사에서 영업상 목적으로 이용할 수 있도록 허용하고 있다. 다만, 개인신용정보의 엄격한 관리를 위해 ‘신용정보관리인’을 선임하고, 개인신용정보등의 취급방침을 정하여 공고하도록 하고 있다.

「전자금융거래법」은 전자금융거래와 관련된 관계를 규율하는데, 제3장에서 ‘전자금융거래의 안전성 확보 및 이용자 보호’와 관련된 내용을 담고 있

다.

한편, 대부분의 금융기관들도 온라인 뱅킹 등을 위해 인터넷을 통한 회원 가입을 받고 있는데, 이에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 「정보통신망법」)의 적용을 받는다. 이에 「신용정보법」에 근거한 신용정보활용체제나 「금융지주회사법」에 근거한 개인신용정보 취급방침과 별도로, 금융기관들은 홈페이지 상에 개인정보취급방침을 공개하고 있다.

### 3) 개정 신용정보법 관련 주요 개정 내용

2009년 10월 2일부터 개정된 「신용정보법」이 시행되었다. 이는 박선숙 의원 대표발의안(의안번호 제1800647호), 임두성 의원 대표발의안(의안번호 제1800910호), 정부가 제출한 전부개정안(의안번호 제1802338호)을 병합 심사하여, 국회 정무위원회에서 대안(의안번호 제1804015호)을 만든 것이다. 2009년 3월 3일 국회를 통과하여, 10월 2일 시행되었다.

정무위원회 대안의 의안원문에 의하면, 이번 개정안은 △ 신용정보회사의 업무 확대 △ 신용정보주체의 자기정보통제권 강화, △ 신용조회회사 등에 신용정보를 보호하기 위한 엄격한 내부통제 절차 마련 등을 목적으로 하고 있다.

이 중 개인신용정보의 보호와 관련된 개정 내용은 다음과 같다.

・개인질병정보의 수집・조사・제공에 대한 동의의 예외를 인정한 규정을 삭제하였다(제16조제2항).[125] 개정 전의 「신용정보법」 제15조[126]도 질병에 관한 정보를 수집할 경우에는 반드시 개인의 동의를 받도록 하고 있었다. 정부 발의 개정안에서는 이 조항에 '다만, 이 법 또는 다른 법률에 따라 제공・이용이 허용되는 경우에는 그러하지 아니하다.'라는 단서를 달아 동의 없이도 수집・제공할 수 있도록 하였는데, 위원회 대안을 만드는 과정에서 다시 삭제된 것이다.

・각 기관의 신용정보의 관리 및 보호를 책임지는 신용정보관리・보호인의 지정・운용을 의무화하였다(제20조제3항 내지 제5항).

---

125) 제16조(수집・조사 및 처리의 제한) ② 신용정보회사등이 개인의 질병에 관한 정보를 수집・조사하거나 타인에게 제공하려면 미리 제32조제1항에 따른 해당 개인의 동의를 받아야 하며 대통령령으로 정하는 목적으로만 그 정보를 이용하여야 한다.

126) 제15조(수집・조사의 제한) ② 신용정보업자등이 개인의 질병에 관한 정보를 수집・조사하고자 할 경우에는 본인의 동의를 얻어야 하며 대통령령이 정하는 목적에 한하여 당해 정보를 이용하여야 한다.

・신용조회회사 또는 신용정보집중기관의 공공기관에 대한 신용정보 제공 요청 근거를 확대하였다(제23조제2항).

・신용조회회사를 통한 개인신용정보 집중・활용에 대한 개인의 동의제도를 강화하였다(제32조제1항 및 제2항). 제32조제1항에서는 동의의 의무와 함께, 동의의 방법을 명시하고 있는데, 제1호부터 제3호까지는 기존 「신용정보법」에서도 규정한 동의 방식이었다. 여기에 제4호를 추가하여 금융기관의 편의를 위해 전화 등을 통해 동의를 받을 수 있도록 하되, 음성녹음 등으로 증거자료를 확보하고 사후 고지하도록 하였다. 또한, 기존에는 금융기관에서 신용조회회사나 신용정보집중기관으로부터 고객의 신용평점 등을 조회할 때 고객의 동의가 필요하지 않았는데, 개정 법은 신용조회 시에도 고객의 동의를 받도록 하였고, 신용조회에 의해서 신용등급이 하락할 수 있음을 고지하도록 하였다.

・신용정보제공・이용자가 신용조회회사 등으로부터 제공받은 개인신용정보에 근거하여 상대방과의 상거래 설정을 거절하는 경우, 거절의 근거가 된 정보를 본인에게 고지하도록 하였다(제36조).

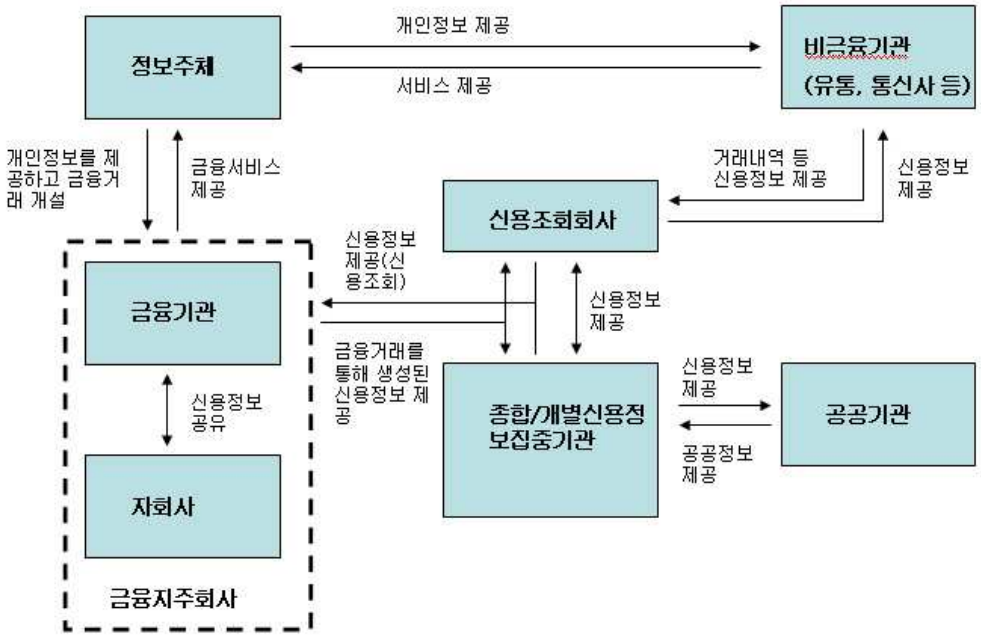
・지금까지 「신용정보법」은 개인신용정보의 수집・제공에 대한 동의 규정만이 있었을 뿐 철회 절차는 규정하고 있지 않았는데, 개정 「신용정보법」은 신용정보주체의 개인신용정보의 제공・이용 동의 철회권을 신설하였다. 그러나 개인의 신용도 평가 목적의 정보에 대해서는 동의를 철회할 수 없다. 또한, 상품 판촉 목적의 전화를 받지 않을 수 있도록 이의 중지를 요청할 수 있도록 하였다. 그리고 개인신용정보의 제공・이용 동의 철회권과 구매권유 중지청구권의 고지방법을 서면, 전자문서, 구두 등으로 구체화하고, 구두에 의한 경우 사후고지절차를 거치도록 하였다(제37조).

## 3. 개인신용정보의 수집・유통 실태

### 1) 개인신용정보의 흐름

개인신용정보가 수집, 집중, 제공, 이용되는 경로는 대체적으로 아래 그림과 같다. 개별 금융기관(신용정보제공・이용자)를 통해 수집된 고객의 신용정보는 신용정보집중기관 및 신용조회업자를 통해 집중된다. 신용정보제공・이용자는 고객의 신용정보를 확인하기 위해, 이렇게 집중된 신용정보집중기관 및 신용조회업자의 정보를 제공받는다. 신용정보제공・이용자 사이에 협약을 통해 신용정보를 공유하기도 한다.

<그림 2-7> 개인신용정보의 제공·이용 흐름도




(1) 신용정보제공·이용자

'신용정보제공·이용자란 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자와 그 밖에 이에 준하는 자로서 대통령령으로 정하는 자'(「신용정보법」 제2조제7호)를 의미한다. 여기에는 은행, 보험사, 증권사, 신용카드사 등 당국의 인·허가를 받는 제도권 금융기관 뿐만 아니라 중소기업진흥공단, 공제조합, 신용보증재단, 감사인, 할부판매업자, 유통사업자, 중소기업, 자산총액 1조원 이하 기업, 전기통신사업자 등도 이에 해당한다(한정미, 2007: 21).

신용정보제공·이용자는 정보주체로부터 개인정보를 제공받고, 금융서비스를 제공한다. 그리고 정보주체의 식별정보와 금융 거래를 통해 생성된 신용정보를 신용정보집중기관 및 신용조회업자에 제공한다. 또한 영업상 목적으로 신용정보집중기관 및 신용조회업자로부터 신용정보를 제공받아 이용하기도 한다. 「금융지주회사법」 제48조의2에 의해, 금융지주회사 및 자회사는 금융거래정보와 신용정보를 영업상 목적으로 공유할 수 있다.

(2) 신용정보집중기관

신용정보제공·이용자가 수집한 개인신용정보는 금융위원회에 등록[127]된 신용정보집중기관에 제공되어 집중 관리·활용된다. 신용정보집중기관은 종합신용정보집중기관과 개별신용정보집중기관으로 구분된다.

종합신용정보집중기관은 '금융기관 전체로부터의 신용정보를 집중관리·활용하는 신용정보집중기관'[128]으로 현재 전국은행연합회가 종합신용정보집중기관으로 등록되어있다. 전국은행연합회는 금융기관으로부터 대출정보, 채무보증현황, 가계당좌예금 개설 및 해지 사실, 신용카드 발급 및 해지 사실 등 금융거래정보 및 대출금, 신용카드 대금 등의 연체 사실 등 신용불량정보를 제공받으며, 공공기관으로부터는 국세, 지방세 등 체납정보 등을 제공받아 '신용정보관리규약'[129]에 따라 집중·관리한다. 그리고 이를 신용정보 제공·이용기관은 물론 금융위원회, 한국은행, 금융감독원 등의 공공기관 및 신용정보업자 등에게 제공하고 있다. 종합신용정보집중기관을 통해 집중관리·활용되는 신용정보의 범위는 「신용정보법」 시행령 [별표2]에 규정되어 있는데, 아래 <표 2-50>와 같다.

<표 2-50> 종합신용정보집중기관을 통하여 집중관리·활용되는 신용정보 범위(제21조제3항 관련)

Ⅰ. 개인

| 구분 | 집중관리·활용 대상 정보 |
|---|---|
| 1. 식별정보 | 성명, 주소, 주민등록번호(외국인의 경우 여권번호 또는 외국인등록번호) |
| 2. 신용거래정보 | 가. 대출 현황<br>나. 당좌예금·가계당좌예금의 개설 및 해지 사실<br>다. 신용카드의 발급·해지 사실 및 결제·미결제 금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우만 해당한다)<br>라. 담보 및 채무보증 현황 |
| 3. 신용도판단정보 | 가. 대출금 등의 연체 내용 |

127) 신용정보집중기관은 신용정보법 제25조제1항에 따라 금융위원회에 등록해야 한다.
128) 「신용정보법」 제25조제2항제1호.
129) 신용정보관리규약은 각 금융기관들이 공통으로 협의·제정한 규약으로 신용정보와 관련된 관리 기준을 정하고 있다. 동 규약의 개정에 관한 사항은 각 금융기관 대표자로 구성된 '신용정보협의회'의 의결을 거쳐 이루어진다(한국정보보호진흥원, 2004: 102).

| | |
|---|---|
| | 나. 대위변제·대지급 발생 사실<br>다. 어음 또는 수표의 거래정지처분을 받은 사실<br>라. 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실(금융질서 문란정보) |

Ⅱ. 기업 및 법인

| 구분 | 집중관리·활용 대상 정보 |
|---|---|
| 1. 식별정보 | 기업의 상호 또는 법인명, 대표자 성명 및 주민등록번호, 사업자등록번호, 법인등록번호, 본점 소재지 |
| 2. 신용거래정보 | 가. 대출·지급보증 등 신용공여 현황<br>나. 시설대여 현황<br>다. 신용보증 현황<br>라. 보증보험 현황<br>마. 담보 및 채무보증 현황<br>바. 당좌예금·가계당좌예금의 개설 및 해지 사실<br>사. 신용카드의 발급·해지 사실 및 결제·미결제 금액(결제금액은 해당 신용정보를 보유한 신용카드업자가 동의하는 경우만 해당한다) |
| 3. 신용도판단정보(제2조제1항제3호 각 목의 어느 하나에 해당하는 자의 정보도 포함한다) | 가. 대출금 등의 연체 내용<br>나. 대위변제·대지급 발생 사실<br>다. 신용보증기금이 대위변제한 사실<br>라. 어음 또는 수표 거래정지처분을 받은 사실<br>마. 리스자금 및 리스료의 연체 사실<br>바. 무보증사채 상환불이행 사실<br>사. 대출금 등을 용도 외로 유용한 사실 및 부정한 방법으로 대출을 받는 등 신용질서를 문란하게 한 사실(금융질서 문란정보) |
| 4. 신용능력정보 | 가. 계열기업체 현황 등 회사의 개황<br>나. 사업의 내용<br>다. 재무제표 등 재무에 관한 사항<br>라. 자본금 증자 및 사채 발행 현황 |

개별신용정보집중기관은 ‘같은 종류의 금융기관으로부터의 신용정보를 집중관리·활용하거나 금융기관 외의 같은 종류의 사업자가 설립한 협회 등의 협약 등에 따라 신용정보를 집중관리·활용하는 신용정보집중기관’[130]을 말한다. 2009년 10월 현재, 여신금융협회, 생명보험협회, 손해보험협회, 금융투

130) 「신용정보법」 제25조제2항제2호.

자협회, 정보통신산업협회 등이 개별신용정보집중기관으로 등록되어 있다. 개별신용정보집중기관은 각 업권에서 고유하게 필요로 하는 신용정보를 집중·관리해 개별회원사에게 제공하는 역할 외에 각 회원사와 종합신용정보집중기관을 중개하는 역할을 수행하는 경우도 있다(한국정보보호진흥원, 2004: 103).

개별신용정보집중기관을 통해 집중관리·활용되는 신용정보의 범위에 대해서는 종합신용정보집중기관과 달리 법에서 규정하고 있지 않다. 정보공개 청구에 대한 금융위원회의 답변에 따르면, 각 개별신용정보집중기관의 집중관리, 활용대상 정보는 다음과 같다.[131]

<표 2-51> 개별신용정보집중기관의 집중관리, 활용대상 정보

| 기관 | 대상 정보 |
|---|---|
| 여신금융협회 | 복수(4개이상)신용카드 소지자 및 신용카드 이용실적 정보, 신용카드 가맹점 및 보상회원 정보 |
| 생명보험협회, 손해보험협회 | 대출 및 연체정보, 보험계약 및 보험금지급정보 |
| 금융투자협회 | 미수발생정보, 신용거래의 무담보 미수채권정보 |
| 정보통신산업협회 | 개인 및 기업의 서비스요금 연체 정보 등 |

(3) 신용조회업자

신용정보업에는 신용조회업, 신용조사업, 채권추심업, 신용평가업 등 4가지 업무가 있으며, 신용정보업을 하려는 자는 각 업무별로 금융위원회의 허가를 받아야 한다.[132] 2009년 8월 말 현재 신용정보업자 현황[133]을 보면, 6개 업체가 신용조회업자로 허가를 받아 업무를 수행하고 있는데, 이 중 서울신용평가정보, 코리아크레딧뷰로, 한국신용정보, 한국신용평가정보 등 4개사가 개인에 대한 신용조회업무를 수행하고 있다. 신용조회업자는 전국은행연합회에 집중된 개인신용정보를 제공받는 것 외에 백화점, 통신사업자, 중소기업 등 주로 비금융기관으로부터 거래기록정보(일정 금액을 3개월 이상 연체한 정보), 단기 연체정보, 신용개설정보 들을 제공받아 집중·관리하며 각각의 회

131) '신용정보집중기관에 대한 정보공개 청구'에 대한 금융위원회의 정보(부분공개) 결정 통지서(2009.10.15), 문서번호: 은행과-2861 (2009.10.15).
132) 「신용정보법」 제4조제1항 및 제2항.
133) 신용정보업자 현황은 금융감독원 홈페이지에 공개되어 있다.

원사에게 제공하고 있다(한국정보보호진흥원, 2004: 104).

### 2) 개인신용정보의 수집

「정보통신망법」은 제22조에서 개인정보를 수집할 경우, 1. 개인정보의 수집·이용 목적, 2. 수집하는 개인정보의 항목, 3. 개인정보의 보유·이용 기간 등을 알리고 동의를 받도록 하고 있다. 그러나 「신용정보법」은 개인정보의 수집과 관련하여 일반적인 동의 규정을 두고 있지 않다. 다만, 「신용정보법」 제16조제1항제3호에서 '개인의 정치적 사상, 종교적 신념, 그 밖에 신용정보와 관계없는 사생활에 관한 정보'에 대한 수집을 금하고 있으며, 제16조제2항에서 '개인의 질병정보'[134]를 수집할 경우 해당 개인의 동의를 받아야 함을 명시하고 있을 뿐이다. 이는 개인신용정보가 주로 은행 등 신용정보제공·이용자가 최초로 개인정보(개인식별정보)를 수집한 이후 금융거래 등에 따라 자동으로 생성되는 정보이기 때문인 것으로 보인다.

신용정보집중기관 및 신용조회회사가 수집하는 개인정보에는 신용정보제공·이용자 및 공공기관이 제공하는 개인 신용정보이므로 아래에서 다룬다.

### 3) 개인신용정보의 이용 및 제3자 제공

(1) 신용정보집중기관 및 신용조회회사에의 개인신용정보 제공

신용정보집중기관과 신용조회회사도 방대한 개인신용정보를 보유하고 있다. 「신용정보법」 제25조 및 동법 시행령 제21조는 신용정보집중기관의 종류, 집중관리·활용되는 신용정보의 범위 및 교환 대상자 등에 대해 규정하고 있다. 이는 신용정보집중기관이 개별 금융기관 등으로부터 신용정보를 제공받아 집중관리하는 근거가 된다.

동법 제32조제1항은 신용정보제공·이용자가 개인신용정보를 제3자에게 제공하기 위해 정보주체의 동의를 받을 것을 규정하고 있다.

신용정보집중기관이 공공기관으로부터 신용정보를 제공받을 수 있는 근거는 「신용정보법」 제23조[135]이다. 제23조에 따르면 신용조회회사 역시 공

---

134) 「신용정보법」 시행령 제13조에 의하면, 개인의 질병에 관한 정보는 '그 정보가 필요한 보험의 계약 및 보험금 지급업무'와 관련해서만 수집, 조사, 제공할 수 있다.

135) 제23조(공공기관에 대한 신용정보의 열람 및 제공 요청 등) ① 신용조회회사나 신용정보집중기관은 국가·지방자치단체 또는 대통령령으로 정하는 공공단체(이하 "공공기관"이라 한다)에 해당 공공기관이 보유하고 있는 신용정보 중 관계 법령에 따라 공개할 수 있는 신용정보의 열람 또는 제공을 요청할 수 있다. 이 경우 요청을 받은 공공기관은 특별한 사유가 없으면 그 요청에 따라야 한다.

② 신용조회회사 또는 신용정보집중기관이 공공기관의 장에게 신용정보주체의 신용도

공기관에 신용정보의 제공을 요청할 수 있다. 그러나 제23조제1항의 '관계법령에 따라 공개할 수 있는 신용정보'의 범위가 어디까지인지 모호하기 때문에, 자칫 공공기관에서 보유하고 있는 개인정보가 과도하게 신용정보집중기관이나 신용조회회사로 제공될 위험이 있다.

또한, 개정 「신용정보법」은 △ 고용보험, 산업재해보상보험, 국민건강보험 및 국민연금에 관한 정보로서 보험료 납부 정보, △ 전기사용에 관한 정보로서 전력사용량 및 전기요금 납부 정보, △ 정부 납품 실적 및 납품액, △ 사망자 정보, 주민등록번호 및 성명 변경 정보, △ 국외 이주신고 및 이주포기신고의 정보 등은 관련 법령의 보호조항에도 불구하고 제공할 수 있도록 허용하고 있다. 이 경우 신용정보의 구체적인 제공 범위는 공공기관의 장과 신용조회회사 또는 신용정보집중기관이 협의하여 결정한다고 되어 있다(동법 시행령 제19조제2항). 관련 법에서 규정한 개인정보 보호 규정에도 불구하고, 공공기관이 보유하고 있는 개인정보가 신용정보라는 명목으로 민간에 제공될 수 있고, 또한 그 범위마저 자의적으로 규정될 수 있어, 신용정보와 관련해서는 자칫 개인정보의 보호를 위한 관련 법의 취지가 훼손될 위험이 있다. 더구나 제23조제7항[136]은 신용정보회사 등이 보유하고 있는 신용정보를 공공기관이 '공무상 목적'으로 이용하기 위해 제공할 수 있도록 허용하고 있는데, 공공기관의 업무가 대부분 공무상 목적이라고 한다면, 이는 거꾸로 공공기관도 사실상 자신의 업무를 위해 신용정보에 제한없이 접근할 수 있도록 하는 것이나 다름없다. 「신용정보법」에서 신용정보회사등과 공공기관 간에 공유할 수 있는 신용정보의 범위에 대해서 수집 목적을 명확히하고, 보다 세부적이고 제한적으로 규정할 필요가 있다.

「신용정보법」 제32조제4항[137]은 신용정보회사가 정보주체의 동의 없이

---

・신용거래능력 등의 판단에 필요한 신용정보로서 대통령령으로 정하는 신용정보의 제공을 요청하면 그 요청을 받은 공공기관의 장은 다음 각 호의 법률에도 불구하고 해당 신용조회회사 또는 신용정보집중기관에 정보를 제공할 수 있다. 공공기관의 장이 신용조회회사 또는 신용정보집중기관에 정보를 제공하는 기준과 절차 등은 대통령령으로 정한다.

1. 「공공기관의 정보공개에 관한 법률」
2. 「공공기관의 개인정보보호에 관한 법률」
3. 「국민건강보험법」
4. 「국민연금법」
5. 「한국전력공사법」
6. 「주민등록법」

136) ⑦ 신용정보회사등은 공공기관의 장이 관계 법령에서 정하는 공무상 목적으로 이용하기 위하여 신용정보의 제공을 문서로 요청한 경우에는 그 신용정보를 제공할 수 있다.

도 다른 신용정보회사 혹은 신용정보집중기관과 공유할 수 있도록 허용하고 있다. 더구나 종합신용집중기관의 경우에는 신용정보법에 집중 관리·활용되는 신용정보의 범위[138]를 규정하고 있는 반면, 신용정보회사가 다루는 신용정보의 범위는 법에 규정되어 있지 않다. 신용정보회사는 민간기업임에도 불구하고, 신용정보제공·이용자, 신용정보집중기관, 공공기관, 기타 사업자들, 그리고 다른 신용정보회사로부터 방대한 신용정보를 수집할 수 있는 셈이다. 신용정보회사의 개인신용정보 수집의 범위에 대해서도 「신용정보법」에서 구체적으로 규정할 필요가 있다.[139]

(2) 제3자 제공에 대한 개인신용정보주체의 동의

① 동의의 방법

개인정보의 보호를 위해서는 수집된 개인정보를 수집 목적 내에서만 이용하는 것이 원칙이다. 「신용정보법」도 개인신용정보를 상거래관계의 설정 및 유지 여부 등을 판단하기 위한 목적, 혹은 그 외 개인이 동의한 목적으로만 사용하도록 하고 있다(제33조). 제34조에서는 '개인식별정보'에 대해 특별히 규정하고 있는데, 이 역시 동의받은 목적 내에서만 이용하거나 신용정보회사등에 제공할 수 있도록 하고 있다.

개정 「신용정보법」은 개인신용정보를 제3자에 제공할 경우 신용정보주체의 동의 권한을 강화하였다. 신용정보 제공·이용자가 개인신용정보를 제3자에게 제공할 경우에는 법에 명시된 방법으로 정보주체의 동의를 받아야 한다(제32조제1항). 제1항제1호부터 제3호는 기존 「신용정보법」에서도 규정한 동의 방식이었다. 여기에 제4호를 추가하였는데, 이는 금융기관 등이 전화 등을 통해 동의를 받을 수 있도록 하되, 음성녹음 등으로 증거자료를 확보하고 사후 고지하도록 함으로써, 금융기관 등의 편의를 위한 것으로 보인다.

---

137) ④ 신용정보회사등이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제3항까지를 적용하지 아니한다.
1. 신용정보회사가 다른 신용정보회사 또는 신용정보집중기관과 서로 집중관리·활용하기 위하여 제공하는 경우

138) 「신용정보법」 시행령 <별표2>.

139) 이는 개정 신용정보법에 대한 국회 정무위원회 논의 과정에서도 지적되었다. 박선숙 의원은 "신용조회 업무를 업으로 하고 있는 CB사 등의 신용정보업자가 다루는 신용정보에 대해서는 범위를 규정하는 법률적 혹은 법률에 위임되어 있는 규정이 없습니다. 그래서 신용정보업자가 임의적으로 개인의 신용정보를 현재 수집·처리하고 있다고 봐야 됩니다"라고 발언하였다(2009년 2월 25일, 국회 정무위원회 전체회의 회의록 p.14).

「신용정보법」 제32조(개인신용정보의 제공・활용에 대한 동의) ① 신용정보제공・이용자가 대출, 보증에 관한 정보 등 대통령령으로 정하는 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 개인으로부터 다음 각 호의 어느 하나에 해당하는 방식으로 미리 동의를 받아야 한다.

1. 서면
2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다)
3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식
4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보・유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지 절차를 거친다.
5. 그 밖에 대통령령으로 정하는 방식

제32조제1항에서 '대출, 보증에 관한 정보 등 대통령령으로 정하는 개인신용정보'는 시행령 제28조제1항에서 규정하고 있는데, 개인신용정보 중 금융질서문란정보와 공공기록정보는 제외된다. 즉, 신용불량정보와 국세 체납 등 공공기록정보 등 신용정보주체의 신용도를 판단할 수 있는 정보는 동의없이 제공할 수 있다. 동의를 받을 때에 개인신용정보를 제공받는 자, 이용목적, 제공하는 개인신용정보의 내용, 정보 보유기간 및 이용기간(신용조회회사 및 신용정보집중기관은 제외한다)을 미리 알려야 한다(「신용정보법」 시행령 제28조제2항).[140]

② 동의가 서비스 제공의 조건이 될 수 있는지 여부

2009년 10월 1일 시행된 개정 시행령 이전의 구 시행령에서는 동의의 내

140) 「신용정보법」 시행령 제28조(개인신용정보의 제공・활용에 대한 동의) ② 신용정보제공・이용자는 법 제32조제1항에 따라 해당 개인으로부터 동의를 받으려면 다음 각 호의 사항을 미리 알려야 한다. 다만, 동의 방식의 특성상 동의 내용을 전부 표시하거나 알리기 어려운 경우에는 해당 기관의 인터넷 홈페이지 주소나 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을 안내하고 동의를 받을 수 있다.
1. 개인신용정보를 제공받는 자
2. 개인신용정보를 제공받는 자의 이용 목적
3. 제공하는 개인신용정보의 내용
4. 개인신용정보를 제공받는 자(신용조회회사 및 신용정보집중기관은 제외한다)의 정보 보유 기간 및 이용 기간

용이 다소 모호하게 규정되어 있었다.[141] 2008년 4월 7일 개정된, 금융위원회의 구 '신용정보업감독규정' <별지 제7호 서식>에는 표준 '개인신용정보 제공·활용동의서'가 다음과 같이 나와 있다. 이를 보면, 개인신용정보를 제공하는 목적도 추상적으로 제시되어 있고, 어느 기관에 제공하는지 구체적으로 명시되어 있지 않음을 알 수 있다.

<그림 2-8> (구) 개인신용정보의 제공·활용 동의서

**개인신용정보의 제공·활용동의서**

_____기관(신용정보제공·이용자) 귀하

이 계약과 관련하여 귀사가 본인으로부터 취득한 다음 신용정보는 신용정보의이용및보호에관한법률 제23조의 규정에 따라 타인에게 제공·활용시 본인의 동의를 얻어야 하는 정보입니다. 이에 본인은 귀사가 다음의 신용정보를 신용정보집중기관, 신용정보업자, 신용정보제공·이용자등에게 제공하여, 본인의 신용을 판단하기 위한 자료로서 활용하거나 또는 공공기관에서 정책자료로서 활용하도록 하는 데 동의합니다.

* 제공할 신용정보의 내용 :

년 월 일

_____서명 또는 인

2009년 9월 30일 전부개정된 '신용정보업감독업무시행세칙'[142] 별지 제2호 서식 <표준 개인신용정보 제공 동의서>는 다음과 같다.

141) 구 「신용정보법 시행령」 제12조(개인신용정보의 제공·활용에 대한 동의등) ① 법 제23조제1항에 따라 해당 개인으로부터 동의를 얻으려는 경우에는 금융위원회가 정하는 바에 따라, 제공할 신용정보의 내용과 제공 대상자 등을 적은 문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 포함한다)로써 신용정보주체에게 설명하고 알려야 한다.

142) 금융감독원 금융감독법규정보시스템(http://law.fss.or.kr/lmx/main.jsp) 참고.
그런데, 이상하게도 신용정보업감독규정은 개정되지 않았다(2009년 10월 6일 현재).

<그림 2-9> 2009년 개정된 표준 개인신용정보 제공 동의서

**표준 개인신용정보 제공 동의서**

기관(신용정보제공·이용자) 귀하

본 계약과 관련하여 귀사가 본인으로부터 취득한 개인신용정보는 「신용정보의 이용 및 보호에 관한 법률」 제32조제1항에 따라 타인에게 제공할 경우에는 본인의 사전 동의를 얻어야 하는 정보입니다. 이에 본인은 귀사가 본인의 개인신용정보를 아래와 같이 제3자에게 제공하는 것에 대해 동의합니다.

**(1) 신용정보집중기관 및 신용조회회사에 개인신용정보 제공**

□ 제공 대상 기관

(예) 신용정보집중기관 : 전국은행연합회, 한국여신전문금융업협회 등
신용조회회사 : 한국신용정보(주), 한국신용평가정보(주), 코리아크레딧뷰로(주) 등

□ 이용 목적

(예) 본인의 신용을 판단하기 위한 자료로 활용하거나 공공기관에서 정책자료로 활용

□ 제공하는 개인신용정보 내용

(예) 개인식별정보(성명, 주소, 주민등록번호, 성별, 국적, 연락처 등)
신용거래정보(본 계약 이전 및 이후의 실적을 포함한 거래내용)
신용능력정보(재산·채무·소득의 총액·납세실적 등)

※ 채무불이행정보(연체, 대위변제, 대지급, 부도, 관련인 발생사실 등)는 신용정보법 제32조제1항에 의하여 동의 없이 신용정보집중기관 및 신용조회회사에게 제공될 수 있습니다.

**(2) 제휴회사에 개인신용정보 제공**

□ 제공 대상 기관

(예) 제휴회사 명칭(구체적으로 제공 대상 기관명을 나열할 것)

□ 이용 목적

(예) '보험료 할인, 포인트 제공 등 고객에 대한 편익 및 서비스 제공 목적
□ 제공하는 개인신용정보 내용
(예) 개인식별정보(성명, 주민등록번호, 주소, 전화번호, e메일)
(예) 카드거래정보(카드번호, 거래일시, 사용금액)
□ 정보 보유・이용기간

※ 이 동의서는 계약의 갱신 등으로 변경되는 경우에도 유효합니다.
※※ 상기내용이 변동하는 경우 인터넷 홈페이지에 게시 등을 통해 그 내용을 알릴 예정입니다.

년 월 일
성명 : 서명 또는 (인)

이를 보면, 그 이전의 동의서 양식보다 제공 대상 기관, 이용목적, 제공하는 개인신용정보의 내용 등을 구분하여 명시하도록 하고 있다. 그러나 이용목적은 '본인의 신용을 판단하기 위한 자료로 활용하거나 공공기관에서 정책자료로 활용'이라고 규정하여 추상적이고 포괄적으로 제시되어 있다. 그만큼 신용정보집중기관이나 신용조회회사 등으로 집중된 신용정보가 다목적으로 이용될 수 있다는 것을 의미한다.

그리고 신용정보집중기관 및 신용조회회사에 제공되는 정보와 제휴회사에 제공되는 정보를 구분하고 있다. 이는 제휴회사에 제공되는 정보의 경우 금융 거래에 필수적인 것이 아니며, 이에 동의하지 않았다고 하여 서비스 제공을 거부할 수 없기 때문이다. 2009년 8월 7일 시행된 여신전문금융업감독규정 제24조의7[143]에 따르면, 신용정보 제공・활용 동의를 받을 경우, 신용카

143) 제24조의7(신용정보 보호) ①법 제24조 및 시행령 제7조의2제2항제5호의 규정에 의하여 신용카드업자는 신용카드회원등의 신용에 관한 자료 또는 제반 정보가 업무외의 목적에 사용되거나 외부에 유출되지 아니하도록 하여야 한다.
②신용카드업자는 신용카드회원등의 신용정보를 제3자에게 제공하기 위하여 신용정보의이용및보호에관한법률 제23조 및 제24조제1항제1호에서 정하는 동의를 얻고자 할 경우 신용카드회원등으로부터 신용카드등발급신청서와 분리된 신용정보제공동의서에 신용정보의 제공목적별로 각각 신용카드회원등의 동의를 얻어야 한다.
③신용카드업자는 신용카드회원등이 신용정보제공동의서에 신용정보의이용및보호에관한법률 제2조의 신용정보업자 및 신용정보집중기관 이외의 제3자에 대한 신용정보제공 동의를 하지 않을 경우 동 거절을 사유로 신용카드등의 발급을 거절하여서는 아니된다.

드 등 발급신청서와 분리된 동의서에 제공목적별로 각각 동의를 얻도록 하고 있으며, 신용정보업자 및 신용정보집중기관 이외의 제3자에 대한 신용정보제공에 동의를 하지 않았다고 하여 신용카드 등의 발급을 거절해서는 안된다고 규정하고 있다.

그런데 신용정보업자 및 신용정보집중기관에 대한 신용정보제공에 동의하지 않으면 금융 서비스 제공을 받을 수 없는지, 다시 말하면 신용정보업자 및 신용정보집중기관에 대한 신용정보제공은 필수적인 것인지 여부는 모호하다. 만일 신용정보업자 및 신용정보집중기관에의 제공을 거부하는 것을 근거로 금융 서비스 제공을 거부할 수 있다면, 이는 사실상 '동의'라고 하기 힘들며, 개인신용정보 제공에 대한 '통지'와 다를 바 없다.

여신전문금융업감독규정 제24조의7에 따르면, 신용정보업자 및 신용정보집중기관에 대한 신용정보제공에 동의하지 않으면 신용카드 등의 발급을 거절할 수 있는 것으로 해석할 수 있다. 「신용정보법」 제32조는 개인신용정보를 타인에게 제공할 경우 동의를 받아야함을 명시하고 있을 뿐이다. 「보험업감독업무 시행세칙(2009년 7월 7일 시행)」 제35조에도 "개인에 관한 신용정보를 타인에게 제공·활용하기 위해서는 신용정보의 이용 및 보호에 관한 법규에 따라 개인신용정보의 제공·활용 동의서에 계약자 및 보험대상자(피보험자)의 동의를 받아야" 함을 명시하고 있을 뿐, 동의하지 않을 경우 서비스를 거부할 수 있는지 여부에 대한 내용은 없다.

한편, 「신용정보법」 제25조에서 신용정보집중기관이 신용정보를 집중관리·활용할 수 있도록 규정해놓았기 때문에, 정보주체의 동의가 없더라도 신용정보집중기관에 제공하는 것이 가능하다고 할 수도 있다. 또한, 제37조제1항은 개인신용정보 제공·이용 동의 철회권을 규정해놓았지만, '신용조회회사 또는 신용정보집중기관에 제공하여 개인의 신용도 등을 평가하기 위한 목적 외의 목적으로 행한 개인신용정보 제공 동의'만을 대상으로 하고 있어, 신용조회회사나 신용정보집중기관에 대한 제공 동의는 철회할 수 없도록 하고 있다.

이렇게 해석한다면, 신용조회회사와 신용정보집중기관에의 신용정보 제공과 관련해서는 제32조의 동의 규정은 의미가 퇴색되며, 신용정보제공·활용 동의서 역시 형식적인 것이 되고 만다. 신용정보제공·활용 동의서가 진정한 동의 절차가 되기 위해서는, 정보주체의 동의 없이는 신용정보집중기관 및 신용조회회사에 신용정보를 제공할 수 없도록 하고, 동의 여부를 서비스 거부의 근거로 삼을 수 없도록 법에서 명확하게 규정할 필요가 있다(윤영민,

2004:43).

(3) 신용조회 시 동의 의무화

기존에는 은행 등 금융기관에서 신용조회회사나 신용정보집중기관으로부터 고객의 신용평점 등을 조회할 때 정보주체의 동의가 필요하지 않았다. 개정 「신용정보법」은 신용조회 시에도 정보주체의 동의를 받도록 하였고, 신용조회에 의해서 신용등급이 하락할 수 있음을 고지하도록 하였다. 신용조회회사나 신용정보집중기관은 정보를 제공할 때 동의 여부를 확인하여야 한다. 다만, 「신용정보법」 제2조제1항제3호에서 규정한 신용불량정보와 제5호에서 규정한 공공기관정보 등 신용정보주체의 신용도를 판단할 수 있는 정보는 동의를 받을 필요가 없다(「신용정보법 시행령」 제28조제5항).

「신용정보법」 제32조(개인신용정보의 제공·활용에 대한 동의)
② 신용조회회사 또는 신용정보집중기관으로부터 대통령령으로 정하는 개인신용정보를 제공받으려는 자는 대통령령으로 정하는 바에 따라 해당 개인으로부터 제1항 각 호의 어느 하나에 해당하는 방식으로 동의를 받아야 한다. 이 때 개인신용정보를 제공받으려는 자는 해당 개인에게 개인신용정보의 조회 시 신용등급이 하락할 수 있음을 고지하여야 한다.
③ 신용조회회사 또는 신용정보집중기관이 개인신용정보를 제2항에 따라 제공하는 경우에는 해당 개인신용정보를 제공받으려는 자가 제2항에 따른 동의를 받았는지를 대통령령으로 정하는 바에 따라 확인하여야 한다.

(4) 동의없이 개인신용정보를 제공할 수 있는 경우

「신용정보법」 제32조제4항은 정보주체의 동의 없이도 개인신용정보를 제공할 수 있는 경우를 명시하고 있다. △ 신용정보회사가 개인신용정보의 집중관리·활용을 위해 제공, △ 계약의 이행을 위해 필요한 개인신용정보의 위탁처리, △ 영업양도·분할·합병 등, △ 채권추심(추심채권을 추심하는 경우만 해당한다), 인가·허가의 목적, 기업의 신용도 판단, 유가증권의 양수 등 대통령령으로 정하는 목적, △ 법원의 제출명령이나 영장, △ 긴급한 상황에서 검사 등이 요구, △ 조세에 관한 법률에 따른 조세자료의 제출, △ 국제협약에 따라 외국 금융감독기구에의 제공하는 등의 경우이다. 이 경우에도 제공하는 자 및 제공받는 자는 개인신용정보의 제공사실 및 이유 등을 정보주체에게 알리거나 공시해야 한다(동법 제32조제5항).

(5) 영업의 양수・양도시 개인정보의 이전

계약의 이행을 위해 필요한 개인신용정보의 위탁처리의 경우에는 '신용정보활용체제'에 공시하도록 하고 있으므로, 정보통신망법의 규제 수준[144]과 비슷하다. 그러나 영업의 양도・양수와 관련한 개인신용정보의 이전과 관련한 규제는 오히려 「정보통신망법」보다 낮은 수준이다. 「정보통신망법」 제26조는 영업의 양도・합병 등으로 개인정보를 이전할 경우, △개인정보를 이전하려는 사실, △개인정보를 이전받는 자의 성명・주소・전화번호 및 그 밖의 연락처, △동의를 철회할 수 있는 방법과 절차 등을 알리도록 하고 있다. 알리는 방법 역시 전자우편・서면 등 개인에 대한 통지를 우선으로 하고, 연락처를 알 수 없는 경우 홈페이지에 최소 30일 이상 게시하도록 하고 있다(「정보통신망법 시행령」 제11조). 그러나 「신용정보법」에서는 서면, 전자우편, 인터넷 홈페이지 게시 등의 방법으로 개인신용정보의 제공 사실 및 이유 등을 알리도록 모호하게 규정하고 있을 뿐이며, 동의철회와 관련된 내용도 없다. 예를 들어, 단지 홈페이지에만 게시를 해놓는다면, 정보주체가 이 사실을 인지하기 힘들 수밖에 없다. 또한, 「정보통신망법」 제26조제3항은 영업양수자 등이 당초 목적범위 내에서 개인정보를 이용하도록 하고 있는데, 「신용정보법」에서도 이를 명확하게 규정할 필요가 있다. 개인신용정보가 여타 정보에 비해 보호수준이 높아야한다는 점에서 영업의 양도・합병과 관련한 신용정보법의 규제는 최소한 「정보통신망법」과 비슷한 수준으로 높아져야 한다. 또한, 앞서 지적했듯이, 신용정보회사의 개인신용정보 수집범위에 대해 법에서 구체적으로 명시할 필요가 있다.

(6) 금융지주회사 내 개인신용정보의 공유

개인신용정보가 정보주체의 동의없이 제공・공유되는 경우가 또 하나있다. 금융지주회사 내에서는 금융거래정보와 개인신용정보가 자회사간에 공유된다. 「금융지주회사법」 제48조의2에 따른 것이다.[145]

---

144) 「정보통신망법」 제25조제2항.

145) 본문의 제48조의2 내용은 현행 법률의 내용이며, 이는 2009년 7월 31일 개정되어, 2010년 2월 1일 시행예정이다. 개정된 제48조의2는 다음과 같다.
제48조의2 (고객정보의 제공 및 관리) ① 금융지주회사등은 「금융실명거래 및 비밀보장에 관한 법률」 제4조제1항 및 「신용정보의 이용 및 보호에 관한 법률」 제32조・제33조에도 불구하고 「금융실명거래 및 비밀보장에 관한 법률」 제4조에 따른 금융거래의 내용에 관한 정보 또는 자료(이하 "금융거래정보"라 한다) 및 「신용정보의 이용 및 보호에 관한 법률」 제32조제1항에 따른 대통령령으로 정하는 개인신용정보(이하 "개인신용정보"라 한다)를 그가 속하는 금융지주회사등에게 영업상 이용하게 할 목

제48조의2 (개인신용정보등의 제공 및 관리) ①금융지주회사등은 「금융실명거래 및 비밀보장에 관한 법률」 제4조제2항 및 「신용정보의 이용 및 보호에 관한 법률」 제32조·제33조에도 불구하고 「금융실명거래 및 비밀보장에 관한 법률」 제4조에 따른 금융거래의 내용에 관한 정보 또는 자료 및 「신용정보의 이용 및 보호에 관한 법률」 제32조제1항에 따른 대통령령으로 정하는 개인신용정보(이하 "개인신용정보"라 한다)를 그가 속하는 금융지주회사등에게 영업상 이용하게 할 목적으로 제공할 수 있다.
②금융지주회사의 자회사등인 「자본시장과 금융투자업에 관한 법률」에 따른 투자매매업자 또는 투자중개업자는 해당 투자매매업자 또는 투자중개업자를 통하여 증권을 매매하거나 매매하고자 하는 위탁자가 예탁한 금전 또는 증권의 총액에 관한 정보를 그가 속하는 금융지주회사등에게 영업상 이용하게 할 목적으로 제공할 수 있다.
③제1항 및 제2항의 규정에 의하여 자회사등이 개인신용정보 및 금전 또는 증권의 총액에 관한 정보(이하 "개인신용정보등"이라 한다)를 제공하는 경우에는 「신용정보의 이용 및 보호에 관한 법률」 제32조제7항을 적용하지 아니한다.
④금융지주회사등은 개인신용정보등의 엄격한 관리를 위하여 그 임원중에 1인 이상을 개인신용정보등을 관리할 자(이하 "신용정보관리인"이라 한다)로 선임하여야 한다.

---

적으로 제공할 수 있다.
② 금융지주회사의 자회사등인 「자본시장과 금융투자업에 관한 법률」에 따른 투자매매업자 또는 투자중개업자는 해당 투자매매업자 또는 투자중개업자를 통하여 증권을 매매하거나 매매하고자 하는 위탁자가 예탁한 금전 또는 증권에 관한 정보 중 다음 각 호의 어느 하나에 해당하는 정보(이하 "증권총액정보등"이라 한다)를 금융지주회사등에게 영업상 이용하게 할 목적으로 제공할 수 있다.
1. 예탁한 금전의 총액
2. 예탁한 증권의 총액
3. 예탁한 증권의 종류별 총액
4. 그 밖에 제1호부터 제3호까지에 준하는 것으로서 금융위원회가 정하여 고시하는 정보
③ 제1항 및 제2항에 따라 자회사등이 금융거래정보·개인신용정보 및 증권총액정보등(이하 "고객정보"라 한다)을 제공하는 경우에는 「신용정보의 이용 및 보호에 관한 법률」 제32조제7항을 적용하지 아니한다.
④ 금융지주회사등은 고객정보의 엄격한 관리를 위하여 그 임원 중에 1인 이상을 고객정보를 관리할 자(이하 "고객정보관리인"이라 한다)로 선임하여야 한다.
⑤ 고객정보관리인은 고객정보의 엄격한 관리를 위하여 금융위원회가 정하는 바에 따라 업무지침서를 작성하고, 그 내용을 금융위원회에 보고하여야 한다.
⑥ 금융지주회사등은 대통령령이 정하는 바에 따라 고객정보의 취급방침을 정하여야 하며, 이를 당해 금융지주회사등의 거래상대방에게 통지하거나 공고하고 영업점에 게시하여야 한다.
⑦ 제1항부터 제6항까지의 규정에 따른 적용을 받는 금융지주회사등 및 자회사등의 구체적인 범위는 대통령령으로 정한다.

⑤신용정보관리인은 개인신용정보등의 엄격한 관리를 위하여 금융위원회가 정하는 바에 따라 업무지침서를 작성하고, 그 내용을 금융위원회에 보고하여야 한다.
⑥금융지주회사등은 대통령령이 정하는 바에 따라 개인신용정보등의 취급방침을 정하여야 하며, 이를 당해 금융지주회사등의 거래상대방에게 통지하거나 공고하고 영업점에 게시하여야 한다.

이 조항은 2002년 4월 27일 개정에서 신설되었는데, 그 취지를 다음과 같이 밝히고 있다.

금융지주회사의 경영의 효율성을 높이기 위하여 동일한 금융지주회사에 속하는 금융기관간에는 금융거래정보 등 일정한 개인신용정보를 서로 제공할 수 있도록 하되, 금융지주회사.자회사 및 손자회사는 그 임원중에 1인 이상을 신용정보관리인으로 선임하도록 하는 등 금융지주회사에 속하는 금융기관간에 제공되는 개인신용정보 등이 엄격히 관리될 수 있도록 함(법 제48조의2 신설).

<표 2-52> 금융지주회사 및 개인신용정보를 공유하는 계열사 현황

| 금융지주회사 | 개인신용정보를 공유하는 계열사 목록 |
|---|---|
| KB금융지주 | KB금융지주, 국민은행, KB부동산신탁, KB자산운용, KB선물, KB투자증권, KB생명보험 |
| 우리금융지주 | 우리금융지주회사, 우리은행, 광주은행, 경남은행, 우리투자증권, 우리아비바생명보험, 우리자산운용, 우리파이낸셜 |
| 한국투자운용지주 | 홈페이지 없음 |
| 신한금융지주 | 신한금융지주회사, 신한은행, 신한카드, 굿모닝신한증권, 신한생명, 신한캐피탈, 제주은행, SH자산운용, 신한BNP Paribas 투자신탁운용, SH&C생명보험 |
| 한국투자금융지주 | 한국투자운용지주㈜, 한국투자증권㈜, ㈜한국투자상호저축은행, 한국투자신탁운용㈜, 한국투자밸류자산운용㈜ |
| 하나금융지주 | 하나금융지주, 하나은행, 하나대투증권, 하나HSBC생명보험, 하나캐피탈 |
| 한국스탠다드차타드금융지주 | 홈페이지 없음 |

자료: 각 업체 홈페이지의 <개인신용정보등의 취급방침>을 참고.

즉, 금융지주회사의 경영 효율성을 높이기 위한 것인데, 정보주체의 입장에서는 개인정보자기결정권에 대한 중대한 침해가 아닐 수 없다. 금융지주회사

내의 한 은행에 계좌를 개설할 경우, 계열사인 타 은행, 증권사, 보험사, 자산운용사 등에 금융거래정보와 개인신용정보가 아무런 동의 없이 제공되는 것이기 때문이다. 금융감독원 제도권 금융회사 조회[146]에 따르면, 현재 금융지주회사로 KB금융지주, 한국투자운용지주, 우리금융지주, 신한금융지주회사, 한국투자금융지주, 하나금융지주, 한국스탠다드차타드금융지주 7개가 지정되어 있다.

### 4) 개인신용정보의 관리

(1) 관련 규정

신용정보를 비롯한 디지털 정보는 복제와 전송이 용이하기 때문에 외부 감독기관의 규제를 통한 보호에는 한계가 있을 수밖에 없다. 따라서 각 기관의 신용정보 보호 강화를 위해서는 내부적인 통제를 강화할 필요가 있다. 개정 「신용정보법」은 제20조에서 각 기관의 신용정보의 관리 및 보호를 책임지는 신용정보관리·보호인의 지정·운용을 의무화하였다. 신용정보관리·보호인의 업무는 시행령 제17조제2항에서 규정하고 있는데, △ 내부관리규정의 제정·개정, △ 신용정보주체의 고충 처리, △ 법령 및 내부관리 규정 준수여부 점검, △ 신용정보주체의 권리보장 여부 점검, △ 교육의 실시 등이다.

「신용정보법」 제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존)
① 신용정보회사등은 신용정보의 수집·처리 및 이용 등에 대하여 금융위원회가 정하는 바에 따라 내부관리규정을 마련하여야 한다.
② 신용정보회사등은 다음 각 호의 사항에 대한 기록을 3년간 보존하여야 한다.
1. 의뢰인의 주소와 성명 또는 정보제공·교환기관의 주소와 이름
2. 의뢰받은 업무 내용 및 의뢰받은 날짜
3. 의뢰받은 업무의 처리 내용 또는 제공한 신용정보의 내용과 제공한 날짜
4. 그 밖에 대통령령으로 정하는 사항
③ 신용정보회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 신용정보를 보호하고 신용정보와 관련된 신용정보주체의 고충을 처리하는 등 대통령령으로 정하는 업무를 하는 신용정보관리·보호인을 1명 이상 지정하여야 한다.
④ 제3항에 따른 신용정보관리·보호인의 자격요건과 그 밖에 지정에 필요한 사항은 대통령령으로 정한다.
⑤ 「금융지주회사법」 제48조의2제4항에 따라 선임된 신용정보관리인이 제4

146) http://www.fcsc.kr/D/fu_d_01_05.jsp.

항의 자격요건에 해당하면 제3항에 따라 지정된 신용정보관리·보호인으로 본다.

이미 「금융지주회사법」 및 「정보통신망법」에서는 신용정보관리·보호인과 유사한 관리 책임자의 지정을 의무화하고 있다. 「금융지주회사법」 제48조의2[147]에서 금융지주회사 등은 '신용정보관리인'(이는 개정 신용정보법에 의한 신용정보관리·보호인이 된다)을 두도록 하고 있으며, 「정보통신망법」 제27조[148] 역시 '개인정보관리책임자'의 지정을 의무화하고 있다.

개정 「신용정보법」 제31조는 신용정보회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자로 하여금 신용정보활용체제, 즉 관리하는 신용정보의 종류, 이용 목적, 제공 대상 및 신용정보주체의 권리 등에 관한 사항을 공시하도록 하고 있다. 기존 「신용정보법」은 신용정보회사와 신용정보집중기관에게만 공시 의무를 부과하였으나, 개정 법안은 이를 신용정보제공·이용자로 확대하였다.

「신용정보법」 제31조(신용정보활용체제의 공시) 신용정보회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 관리하는 신용정보의 종류, 이용 목적, 제공 대상 및 신용정보주체의 권리 등에 관한 사항을 대통령령으로 정하는 바에 따라 공시하여야 한다.

공시의 방법은 시행령에 규정되어 있는데, 기존에는 인터넷 홈페이지, 신문 또는 방송을 통해 매년 1회 이상 공시하도록 하고 있었는데[149], 개정된 시행

147) 「금융지주회사법」 제48조의2 (개인신용정보등의 제공 및 관리)
④ 금융지주회사등은 개인신용정보등의 엄격한 관리를 위하여 그 임원중에 1인 이상을 개인신용정보등을 관리할 자(이하 "신용정보관리인"이라 한다)로 선임하여야 한다.
⑤ 신용정보관리인은 개인신용정보등의 엄격한 관리를 위하여 금융위원회가 정하는 바에 따라 업무지침서를 작성하고, 그 내용을 금융위원회에 보고하여야 한다.

148) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조 (개인정보 관리책임자의 지정)
① 정보통신서비스 제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보 관리책임자를 지정하여야 한다. 다만, 종업원수, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자등의 경우에는 지정하지 아니할 수 있다.

149) 구 「신용정보법」 시행령 제11조 (신용정보활용체제의 공시) 신용정보업자 및 신용정보집중기관은 법 제22조에 규정된 사항을 그 기관의 인터넷 홈페이지, 전국을 대상으로 발간되는 「신문 등의 자유와 기능보장에 관한 법률」에 따른 일반일간신문 또는 전국을 대상으로 전파되는 방송을 통하여 매년 1월 31일까지 1회 이상 공시하여야 한다.

령[150]에서는 점포·사무소 안에 비치하는 방법, 혹은 인터넷 홈페이지를 통해 열람하도록 하고 있다. 또한, 개정 시행령에서는 신용정보활용체제에 포함될 내용을 구체적으로 규정하고 있는데, △ 관리하는 신용정보의 종류 및 이용목적, △ 제3자 제공시 제공하는 신용정보의 종류, 제공대상, 이용목적, △ 신용정보의 보유 및 이용기간, 파기의 절차 및 방법, △ 위탁 업무의 내용 및 수탁자, △ 신용정보주체의 권리와 행사방법, △ 신용정보관리·보호인 등으로 정보통신망법 제27조의2에 따른 '개인정보 취급방침'과 유사하다.

그런데, 개정된 시행령에서 신용정보활용체제 공시 방법을 점포·사무소 안에 비치, 혹은 인터넷 홈페이지에 게시하도록 하였는데, 인터넷 홈페이지에 게시하지 않을 경우 일반 이용자들은 신용정보활용체제를 사실상 접근하기 힘들다. 따라서 점포·사무소 안에 비치하는 것과 함께 인터넷 홈페이지에도 동시에 게시하도록 개선될 필요가 있다.

(2) 관련 기관/업체의 실태

은행, 보험사 등 금융기관들의 홈페이지에는 개인정보 보호와 관련하여 조금씩 문구나 형식은 다르지만 다음과 같은 종류의 안내문을 공지하고 있다. △ 개인정보취급방침, △ 신용정보제공활용에 대한 고객권리안내문, △ 개인신용정보관리보호정책 및 개인신용정보등의취급방침, △ 신용정보활용체제 등이다.

개인정보취급방침은 해당 금융기관이 보유·이용하고 있는 개인신용정보에 대한 것이 아니라, 웹사이트에 가입하여 인터넷 뱅킹 등을 이용하는 고객의

---

150) 「신용정보법」 시행령 제27조(신용정보활용체제의 공시)
② 신용정보회사, 신용정보집중기관 및 제1항에 해당하는 자는 법 제31조에 따라 다음 각 호의 사항을 공시하여야 한다.
1. 관리하는 신용정보의 종류 및 이용 목적
2. 신용정보를 제3자에게 제공하는 경우 제공하는 신용정보의 종류, 제공 대상, 제공받는 자의 이용 목적(제1항에 해당하는 자로 한정한다)
3. 신용정보의 보유 기간 및 이용 기간이 있는 경우 해당 기간, 신용정보 파기의 절차 및 방법(제1항에 해당하는 자로 한정한다)
4. 법 제17조에 따라 신용정보의 처리를 위탁하는 경우 그 업무의 내용 및 수탁자
5. 신용정보주체의 권리와 그 행사방법
6. 법 제20조제3항에 따른 신용정보관리·보호인이나 같은 항에 따라 신용정보 관리·보호 관련 고충을 처리하는 사람의 성명, 부서 및 연락처
③ 신용정보회사, 신용정보집중기관 및 제1항에 해당하는 자는 제2항 각 호의 사항을 공시하는 경우에는 다음 각 호의 어느 하나에 해당하는 방법으로 하여야 한다.
1. 점포·사무소 안의 보기 쉬운 장소에 갖춰 두고 열람하게 하는 방법
2. 해당 기관의 인터넷 홈페이지를 통하여 해당 신용정보주체가 열람할 수 있게 하는 방법

개인정보에 대한 보호정책을 명시한 것이다.

신용정보제공활용에 대한 고객권리안내문은 신용정보활용체제가 보편적으로 공시되기 이전부터 상당수 금융기관의 홈페이지에 공시되어 있었다. 금융서비스의 이용범위(고객의 신용정보는 이용 동의한 목적 내에서만 이용되며, 제휴회사 등에 대한 정보의 제공·이용 동의여부와 관계없이 금융서비스를 이용할 수 있음), 개인신용정보의 제공 및 이용중단 신청 방법, 신용정보 제공사실 통보 요구 및 오류정보 정정 요구 방법 등의 내용을 담고 있다.

개인신용정보의 취급방침은 금융지주회사인 금융기관의 홈페이지에 포함되어 있다. 이는 「금융지주회사법」 제48조의2제6항[151]에 따른 것이다. 동법 제48조의2에 따라 개인신용정보를 금융지주회사 등에게 영업상 이용하게 할 목적으로 제공할 수 있다는 것, 제공되는 개인신용정보의 종류, 개인신용정보의 제공처(금융지주회사 내 제공처를 말함), 개인신용정보 보호를 위한 내부방침 등의 내용을 담고 있다.

신용정보활용체제는 2009년 10월 2일 발효된 개정 신용정보법 제31조에 따른 것이다. 신용정보회사 및 신용정보집중기관은 구 법률에서도 신용정보활용체제 공시 의무 대상이었다. 관리하는 신용정보의 이용목적 및 종류, 제공대상자, 제공받는 자의 이용목적 및 제공하는 신용정보의 종류, 보유 및 이용기간, 신용정보 파기절차 및 방법, 신용정보처리 위탁 업무의 내용 및 수탁자, 신용정보주체의 권리 및 행사방법, 신용정보관리·보호인 등의 내용을 담고 있다.

주요 금융기관 홈페이지에 공시된 개인정보보호 관련 정책 현황은 다음과 같다. 이 결과는 2009년 10월 7일 기준으로 작성된 것이며, 이후 변동될 수 있다. 조사에 포함된 금융기관은 다음과 같다.[152]

△ 은행 : 국민은행, 기업은행, 농협, 신한은행, 우리은행, 하나은행, 씨티은행 등 7개 은행

△ 보험사 : 교보생명, 대한생명, 삼성생명 등 3개 생명보험사, 동부화재, 삼성화재, 현대해상 등 3개 손해보험사

△ 신용카드사 : 롯데카드, 비씨카드, 삼성카드 등 3개사

---

151) 「금융지주회사법」 제48조의2 (개인신용정보등의 제공 및 관리)
⑥금융지주회사등은 대통령령이 정하는 바에 따라 개인신용정보등의 취급방침을 정하여야 하며, 이를 당해 금융지주회사등의 거래상대방에게 통지하거나 공고하고 영업점에 게시하여야 한다.

152) 아래 표에는 A, B, C 등으로 익명 표기했으며, 아래 조사 대상 금융기관의 순서와 상관없다.

△ 신용정보집중기관 : 생명보험협회, 손해보험협회, 정보통신산업협회, 전국은행연합회 등 4개 기관

△ 신용조회회사 : 서울신용평가정보, 코리아크레딧뷰로, 한국신용정보, 한국신용평가정보 등 4개사

<표 2-53> 주요 금융기관 홈페이지에 공시된 개인정보보호 관련 정책

| 구분 | 기관명 | 개인정보취급방침 | 고객권리안내문 | 신용정보활용체제 |
|---|---|---|---|---|
| 은행 | A은행 | O | O | O |
| | B은행 | O | O | O |
| | C은행 | O | O | X |
| | D은행 | O | O | O |
| | E은행 | O | O | O |
| | F은행 | O | O | O |
| | G은행 | O | O | O |
| 보험사 | A보험사 | O | X | O |
| | B보험사 | O | O | X |
| | C보험사 | O | X | X |
| | D보험사 | O | X | O |
| | E보험사 | O | X | X |
| | F보험사 | O | O | O |
| 카드사 | A카드사 | O | O | X |
| | B카드사 | O | O | O |
| | C카드사 | O | O | X |
| 신용정보집중기관 | A기관 | O | X | O |
| | B기관 | O | X | X |
| | C기관 | O | X | O |
| | D기관 | O | X | X |
| 신용조회회사 | A신용조회회사 | O | X | O |
| | B신용조회회사 | O | X | X |
| | C신용조회회사 | O | X | O |
| | D신용조회회사 | O | X | X |

이를 좀 더 자세히 분석해보면 다음과 같다.

개인정보취급방침은 모든 업체/기관에서 채택을 하고 있었으며, 위 표에는 포함하지 않았지만, 금융지주회사의 경우 '개인신용정보등의 취급방침'을 포함하고 있었다. A은행, B은행, C은행, B보험사, C보험사, A카드사 등 일부 금융기관의 경우 위 표에 포함된 개인정보보호 관련 정책과 별개로, 개인신용정보 관리·보호정책을 포함하고 있었다.

그러나 개정 「신용정보법」이 10월 2일 시행되었음에도 불구하고, 신용정보활용제제를 공시하고 있지 않은 업체/기관이 많았다. 이는 아직 시행초기이기 때문인 것으로 보인다. 그러나 신용정보집중기관과 신용조회회사는 개정법률 시행 이전부터 신용정보활용체제 공시 의무가 있었음에도 불구하고, 홈페이지를 통해 공시하지 않은 경우가 많았다. 물론 신문 등 다른 방법을 통해 공시 의무를 수행했을 수도 있지만, 이용자들이 언제든지 쉽게 확인할 수 있도록 하기 위해서는 홈페이지에 공시하도록 의무화할 필요가 있다.

신용평가회사의 경우, 회사 자체를 소개하는 홈페이지와 신용조회·평가 등의 서비스를 위한 홈페이지가 분리되어 있는데, 신용정보활용체제는 회사 홈페이지에만 공시되어 있었다. 이용자들이 실제 이용하는 홈페이지가 서비스 홈페이지라고 했을 때, 서비스 홈페이지에도 공시될 필요가 있다.

한편, 개인정보취급방침, 개인신용정보·관리보호정책, 개인신용정보제공·이용에 대한 고객권리안내문, 개인신용정보등의 취급방침, 신용정보활용체제 등 개인정보 보호와 관련된 정책들이 너무 많아 혼란스럽다. 정보주체(고객)의 권리도 신용정보활용체제와 고객권리안내문 등에 구분되어 표시되어 있다. 정보주체가 좀더 쉽게 접근할 수 있도록 체계적으로 정리될 필요가 있다.

신용정보활용체제 등을 통해 공시되는 내용의 구체성도 천차만별이다. C신용평가회사의 경우, 신용정보활용체제의 내용이 단순하고 추상적이며, 제공대상도 명시되어 있지 않다. 이는 개인신용정보를 잘 보호하겠다는 선언일 뿐, 이것만 보아서는 어떠한 개인신용정보를 수집하고 있는지, 어떤 목적으로 어디에 제공하는지 등에 대해 파악하기 힘들다. 금융업체의 신용정보활용체제에서도 제공 대상을 신용정보집중기관, 타보험회사, 제휴업체 등과 같이 포괄적으로 명시한 경우도 있었으며, 제공대상 업체/기관을 일부만 나열한 경우도 많았다. 통신업체들의 개인정보취급방침에서 개인정보를 제공하는 수백개의 위탁업체나 제3자 제공업체들을 공개하고 있는 것과 비교했을 때, 금융업체들의 신용정보활용체제의 구체성은 전반적으로 떨어진다고 평가할 수 있다. 개인신용정보를 제공받는 제3자 업체/기관이나 수탁업체 등의 이름, 제공

정보, 제공목적 등을 상세하게 명시할 수 있도록 정부의 지침이 필요할 것으로 보인다. 또한, 신용정보활용체제의 '신용정보주체의 권리 및 행사방법'에는 △ 본인신용정보 제공·열람청구권, △ 본인신용정보 정정청구권, △ 신용정보제공사실의 통보요구권, △ 개인신용정보 제공·이용 동의 철회권 등이 명시되어 있고, 간략한 설명이 있었다. 그러나 전화수신거부권(Do-Not-Call)에 대한 설명은 없었다. 또한, 정부주체가 쉽게 이러한 권리를 행사할 수 있기 위해서는 각 권리를 행사할 수 있는 구체적인 방법이나 홈페이지 상의 주소를 제공할 필요가 있다. 신용정보활용체제가 다소 법적 규제에 따른 형식적인 조치에 머물고 있음을 볼 수 있다.

(3) 신용정보의 보안과 유출

「신용정보법」 제19조는 신용정보 전산시스템의 안전보호를 위한 기술적·물리적·관리적 보안대책을 수립할 것을 규정하고 있으며, 제20조는 신용정보관리·보호인의 지정을 의무화하고 있다. 그러나 지난 2009년 5월 알려진 금융기관 고객정보 약 400만 건의 불법거래 사건은 금융기관의 보안조치가 내부자의 불법적인 접근을 차단하는데 한계가 있음을 보여준다.

2009년 5월 18일, 서울지방경찰청 사이버범죄수사대는 은행 고객정보 DB를 이메일로 거래하는 등 신용정보 약 4백만 건을 불법거래하여 광고전화, SMS 발송 등 대출업무에 사용한 은행 대출상담사 등 49명과 소속 금융기관 10개를 포함한 12개 사업체 등 총 61명을 검거하였다고 발표하였다(서울지방경찰청, 2009). 기존의 불법거래는 주로 대부업체 등에서 발생하였으나, 이번 사건에서는 최초로 제1금융권의 대출상담사가 관여된 것으로 나타났다. 입건된 사람은 제1금융권 대충상담사 24명을 포함한 49명이었으며, 은행 4개, 저축은행 3개, 캐피탈 3개, 대출알선 1개, 홈페이지제작업체 1개 등 총 12개 법인이 입건되었다.

개인신용정보의 불법유출이 문제가 되었지만, 국민건강보험공단 내부 직원의 무단/불법열람이 매해 문제가 되고 있는 것처럼, 방대한 개인신용정보를 구축하고 있는 금융기관에서도 내부 직원에 의한 무단/불법열람이 발생할 가능성을 배제할 수 없다.[153] 한편으로는 금융기관 내부의 보안을 철저히 해야겠지만, 방대한 개인정보 데이터베이스의 구축 자체가 이러한 위험성을 내포하고 있다고 했을 때, 개인정보의 수집 자체부터 엄격하게 제한하도록 할 필요가 있다.

153) 매일경제, 2009.5.22, "당신의 연봉·출입국기록까지 다 알고있다."

## 4. 신용정보주체의 열람 및 정정·삭제 청구권 보장 실태

개정 「신용정보법」 제35조에서 제39조는 개인신용정보에 대한 정보주체의 권리를 명시하고 있다.

### 1) 신용정보에 대한 열람 및 정정 청구권

신용정보주체는 본인확인을 받아 신용정보제공·이용자, 신용정보집중기관, 신용정보회사 등이 보유하고 있는 본인의 개인신용정보에 대해 제공 또는 열람할 수 있으며, 본인정보가 사실과 다른 경우 정정을 청구할 수 있다.

「신용정보법」 제38조(신용정보의 열람 및 정정청구 등) ① 신용정보주체는 신용정보회사등에 본인의 신분을 나타내는 증표를 내보이거나 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법으로 본인임을 확인받아 신용정보회사등이 가지고 있는 본인정보의 제공 또는 열람을 청구할 수 있으며, 본인정보가 사실과 다른 경우에는 금융위원회가 정하여 고시하는 바에 따라 정정을 청구할 수 있다.

신용정보회사 등은 정정청구에 정당한 사유가 있다고 인정하면 즉시 문제의 신용정보에 대해 정정청구 중 또는 사실조회 중임을 기입하고, 지체없이 해당 신용정보의 제공·이용을 중단해야 한다. 이후 사실인지를 조사하여 사실과 다르거나 확인할 수 없는 신용정보는 삭제하거나 정정해야 한다. 신용정보회사 등의 처리결과에 이의가 있을 경우 금융위원회에 그 시정을 요청할 수 있다.

또한, 은행 등 신용정보 제공·이용자가 신용정보회사나 신용정보집중기관에의 신용정보 조회를 통해 상거래관계 설정을 거절한 경우, 신용정보주체는 그 거절의 근거가 된 정보를 본인에게 고지할 것을 요구할 수 있으며, 그 내용에 이의가 있으면 신용조회회사나 신용정보집중기관에 그 정보의 정확성을 확인하도록 요청할 수 있다(동법 제36조).

신용조회회사는 1년에 1회 이상 신용정보주체가 본인정보를 무료로 열람할 수 있도록 해야 한다. 무료열람권은 이번 법 개정으로 신설된 것이다.

「신용정보법」 제39조(무료 열람권) 신용조회회사는 1년 이내로서 대통령령으로 정하는 일정한 기간마다 개인인 신용정보주체가 본인정보를 1회 이상 무료로 제공받거나 열람할 수 있도록 하여야 한다.

신용조회회사 홈페이지를 통해 확인해본 결과, 서울신용평가정보, 코리아크레딧뷰로, 한국신용정보, 한국신용평가정보 등 신용조회회사 4개사 모두 서비스 홈페이지[154]를 통해, 1년 1회 무료 신용조회 서비스를 제공하고 있었다. 무료 신용조회 서비스와 별개로 신용조회 및 평가 등 유료 신용관리 서비스를 제공하고 있다. 다만, 무료 신용조회 서비스를 받기 위해서도 신용조회회사 홈페이지에 회원가입을 해야 했다.

무료 신용조회 서비스를 통해 제공받을 수 있는 정보는 다음과 같다.

- 신용개설정보 혹은 카드발급정보 : 신용카드 개설 등 신용거래 내역
- 대출정보 : 금융기관에서 내출받은 내역
- 현금서비스 내역 : 금융기관에서 신용카드 현금서비스를 받은 내역
- 채무보증 정보 : 타인의 대출에 대해 보증을 해준 내역
- 채무불이행 정보 : 은행연합회에서 등록한 연체정보와 신용조회회사 회원사(통신사, 백화점 등)에서 등록한 연체정보.
- 금융질서문란정보 : 금융질서를 문란하게 한 사실 내역
- 특수기록정보 : 신용회복지원위원회의 신용회복지원 내용과 법원으로부터 소비자 파산 등에 대한 정보
- 공공기록정보 : 공공기관으로부터 받은 세금체납정보 등
- 신용조회정보 : 자신의 신용정보를 열람한 금융기관의 내역
- 신용평점 : 각 신용조회회사가 산정한 신용점수 및 등급

신용(카드)개설정보, 대출정보, 현금서비스정보 등은 각 신용정보사 모두 동일한 정보를 보유하고 있었다. 그러나 신용조회 내역은 각 신용조회회사마다 다르게 나타났는데, 이는 각 금융기관마다 이용하는 신용조회회사가 다르기 때문이다. 신용평점도 각 신용조회회사마다 매우 다르게 나타났다. 신용평점은 객관적인 사실 정보가 아니라, 각 신용조회회사 고유의 방법에 의한 평가정보이기 때문이다.

종합신용정보집중기관인 전국은행연합회 역시 무료 신용조회 서비스(크레딧포유, http://www.credit4u.or.kr)를 제공하고 있다. 여기서도 연체정보내역, 공공기록정보내역, 대출정보내역, 현금서비스정보내역, (신용)개설/발급정보내역, 채무보증정보내역 등을 확인할 수 있다. 전국은행연합회는 신용등급 관리는 하지 않는다.

---

154) 서울신용평가정보 : 싸이렌24 http://www.siren24.com
코리아크레딧뷰로 : 올크레딧 http://www.allcredit.co.kr
한국신용정보 : 마이크레딧 http://www.mycredit.co.kr
한국신용평가정보 : 크레딧뱅크 http://www.creditbank.co.kr

<표 2-54> 신용조회회사 무료 신용조회 서비스 제공 정보

| A 신용조회회사 | B 신용조회회사 | C 신용조회회사 | D 신용조회회사 |
|---|---|---|---|
| 신용평점<br>신용개설정보<br>대출거래내역<br>현금서비스내역<br>채무보증내역<br>채무불이행(은행연합회)<br>금융질서문란정보<br>특수기록정보<br>공공기록정보<br>채무불이행(신용정보사)<br>조회처내역 | 신용개설정보<br>신용조회정보<br>대출정보<br>채무보증정보<br>현금서비스정보<br>금융질서문란정보<br>특수기록정보<br>공공기록정보<br>채무조정정보<br>채무불이행(은행연합회)정보<br>채무불이행(신용정보사)정보<br>단기연체정보<br>개인신용평점및등급 | 카드발급정보<br>채무불이행정보(은행연합회)<br>금융질서문란정보<br>채무불이행정보(신용정보사)<br>특수기록정보<br>공공기록정보<br>신용조회기록정보<br>대출정보<br>현금서비스정보<br>보증정보 | 카드개설정보<br>현금서비스정보<br>대출정보내역<br>신용회복위원회정보<br>연대보증정보<br>채무불이행정보(은행연합회, 신용정보사)<br>기타연체관련정보(공공기록정보, 금융질서문란정보, 특수기록정보)<br>신용조회정보<br>신용평점정보 |

개별신용정보집중기관인 방송통신산업협회, 손해보험협회, 생명보험협회, 여신금융협회 등은 홈페이지를 통해 동 기관이 보유하고 있는 개인신용정보의 열람 방법을 제공하지 않고 있었다. 다만, 방송통신산업협회의 경우 '방송통신 신용정보 공동관리' 홈페이지(http://www.credit.or.kr/broadcast/delayCheck.html)를 통해서 본인연체정보(방송통신산업협회 회원사인 방송통신 사업자의 서비스 요금 연체정보)를 확인할 수 있도록 하였으며, M-safer라는 이름의 명의도용방지서비스 홈페이지(http://www.msafer.or.kr)를 통해서 휴대폰, 무선인터넷, 유선전화, 초고속인터넷, 인터넷전화 가입현황을 조회할 수 있도록 제공하고 있다. 손해보험협회와 생명보험협회는 홈페이지를 통해 생존자/사망자 보험계약조회 서비스를 제공하고 있으나, 이를 이용하기 위해서는 먼저 협회를 방문하여 신청을 해야 한다.

### 2) 신용정보제공사실의 통보요구권

신용정보주체는 신용정보회사 등에 본인에 관한 신용정보를 제공한 내역 - 신용정보를 제공받은 자, 그 이용목적, 제공한 날짜, 제공한 본인정보의 주요 내용 등 - 을 통보할 것을 요구할 수 있다. 시행령[155]에 따르면, 신용정보주

155) 「신용정보법 시행령」 제30조(신용정보 제공사실의 통보요구 등) ② 신용정보회사 등은 제1항에 따라 통보를 요구받은 경우에는 요구받은 날부터 7일 이내에 최근 1년간 그 신용정보주체의 본인정보를 직접 제공받은 자, 그 정보의 이용 목적, 제공일 및 주요 내용 등(이하 "신용정보제공내역"이라 한다)을 금융위원회가 정하여 고시하는 서식에 따라 그 신용정보주체에게 통보하여야 하고, 종합신용정보집중기관, 신용조회회

체는 최근 1년간의 신용정보 제공내역을 인터넷 홈페이지를 통해 조회할 수 있다. 있다. 신용정보회사 등은 통보나 조회의 비용을 신용정보주체에게 부담하게 할 수 있지만, 1년에 1회 이상은 홈페이지를 통해 무료로 조회할 수 있도록 해야 한다.

「신용정보법」 제35조(신용정보 제공사실의 통보요구) 신용정보주체는 신용정보회사등이 본인에 관한 신용정보(이하 “본인정보”라 한다)를 제공하는 경우에는 대통령령으로 정하는 바에 따라 제공받은 자, 그 이용 목적, 제공한 날짜, 제공한 본인정보의 주요 내용 등을 알리도록 요구하거나 인터넷 홈페이지를 통하여 조회할 수 있도록 하여 줄 것을 요구할 수 있다. 이 경우 신용정보회사 등은 특별한 사유가 없으면 그 요구에 따라야 한다.

4개 신용조회회사 모두 무료로 신용정보제공내역을 조회할 수 있는 메뉴를 마련해두고 있었다. 이용기관(업종, 지점 등), 이용일자, 이용목적, 제공된 본인정보의 주요 내용을 확인할 수 있다. 그러나 제공된 본인정보의 주요 내용은 신용정보 혹은 일반신용정보/신용거래정보 등으로 포괄적으로 표기되어 있었는데, 좀 더 구체적으로 표기하도록 개선될 필요가 있다.

앞서 언급한 바와 같이 신용정보제공내역은 회사마다 다르게 나타난다. 신용정보제공내역은 ‘금융기관 등에 제공되는 정보’와 ‘본인만이 확인할 수 있는 정보’, 두 부분으로 나뉘어져있다. 금융기관 등에 제공되는 정보는 금융기관 등에서 신용정보주체의 신용정보를 조회하는 경우, 조회한 기관 외의 타 금융기관 등에서도 조회 기록을 확인할 수 있는 정보를 말한다. 본인만이 확인할 수 있는 정보는 이 조회기록을 의뢰한 금융기관과 정보주체 본인만이 확인할 수 있는 정보를 말한다. 후자의 경우 주로 금융기관의 대출실행이나 카드 발급 전 승인가능여부의 재확인을 하거나 기존의 회원관리 및 민원처리 등의 목적으로 금융기관 등에서 조회를 의뢰하는 경우 혹은 신용정보주체 본인이 본인의 신용정보 관리 목적으로 조회하는 경우들이 이에 해당한다.

---

사, 그 밖에 금융위원회가 정하여 고시하는 신용정보제공·이용자는 인터넷 홈페이지를 통하여 신용정보주체가 최근 1년간 그 신용정보주체의 신용정보제공내역을 조회할 수 있도록 하여야 한다.

③ 신용정보회사등은 제2항에 따라 신용정보제공내역을 통보하거나 인터넷 홈페이지를 통하여 조회할 수 있도록 한 경우에는 통보나 조회에 직접 드는 비용을 그 신용정보주체에게 부담하게 할 수 있다.

④ 신용정보회사등은 제2항에 따라 인터넷 홈페이지를 통하여 신용정보제공내역을 조회할 수 있도록 한 경우에는 제3항에도 불구하고 신용정보주체가 1년에 1회 이상 무료로 조회할 수 있도록 하여야 한다.

전국은행연합회 역시 무료 신용조회 서비스와 함께, 신용정보 제공내역에 대한 열람 서비스도 제공하고 있다. 신용정보제공·이용자, 신용정보회사, 신용정보집중기관, 그리고 본인이 신용정보를 조회한 내역을 열람할 수 있다. 제공일자, 이용자(기관명 혹은 본인), 이용목적, 제공된 정보 등을 확인할 수 있다.

방송통신산업협회 등 개별신용정보집중기관들은 홈페이지를 통해 신용정보 제공내역을 열람할 수 있는 서비스를 제공하지 않고 있다. 시행령 제30조제2항은 "종합신용정보집중기관, 신용조회회사, 그 밖에 금융위원회가 정하여 고시하는 신용정보제공·이용자는 인터넷 홈페이지를 통하여 신용정보주체가 최근 1년간 그 신용정보주체의 신용정보제공내역을 조회할 수 있도록 하여야 한다"고 규정하고 있어, 개별신용정보집중기관은 예외로 하고 있다.

그런데, 신용정보집중기관이나 신용조회회사의 신용정보제공내역은 개별 금융기관이 정보주체의 신용정보를 조회한 내역이다. 개별 금융기관이 제3자에게 제공한 내역은 개별 금융기관에서 확인할 수 있어야 한다. 그러나 개별 금융기관은 신용정보제공내역을 온라인 상에서 제공하지 않는 것으로 보인다.[156] A은행의 경우 홈페이지 상에서 신용정보제공내역을 조회할 수 있는 메뉴를 찾을 수 없었으며, 다만 '개인신용정보 제공·이용에 대한 고객권리안내문' 상에 "동 권리를 행사하고자 하는 고객은 당행 각 영업점 앞으로 신청하여 주시기 바랍니다"라고 안내되어 있었다. B은행 역시 마찬가지였다. 신용정보주체가 보다 쉽게 본인 신용정보의 제3자 제공 내역을 알 수 있도록 개별 금융기관의 홈페이지를 통해 열람을 제공할 필요가 있다.

### 3) 개인신용정보 제공·이용 동의 철회권

정보주체의 개인정보자기결정권은 개인정보의 수집 시 동의를 얻도록 하는 것만이 아니라, 잘못된 정보에 대한 정정 청구와 동의의 철회를 포함한다. 「정보통신망법」도 제30조[157]에서 동의 철회권을 규정하고 있다. 지금까지 「신용정보법」은 개인신용정보의 수집·제공에 대한 동의 규정만이 있었을 뿐 철회 절차는 규정하고 있지 않았는데, 개정 법 제37조는 신용정보주체의 개인신용정보의 제공·이용 동의 철회권을 신설하였다. 그러나 개인의 신용도 평가 목적의 정보에 대해서는 동의를 철회할 수 없다. 또한, 상품 판촉 목

156) 이번 연구에서는 신용정보제공사실 통보요구에 대한 신용정보제공·이용자들의 전반적인 보장 실태는 수행하지 못했으며, 일부 기관에 대해서만 확인하였다.

157) 제30조 (이용자의 권리 등) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.

적의 전화를 받지 않을 수 있도록 이의 중지를 요청할 수 있도록 하였다(전화수신거부권, Do-Not-Call). 그리고 개인신용정보의 제공·이용 동의 철회권과 전화수신거부권의 고지방법을 서면, 전자문서, 구두 등으로 구체화하고, 구두에 의한 경우 사후고지절차를 거치도록 하였다.

이번 개정에서 전화수신거부권을 신설한 것은 바람직한 일이나, 개인신용정보의 활용이 사전 동의(opt-in) 방식이 아니라, 사후 거부(opt-out) 방식을 취하고 있음을 알 수 있다. 전화수신거부권의 신설은 정보주체의 최소한의 권리를 보장한 것일 뿐, 기본적으로 정보주체의 결정권 보다는 금융기관에 의한 신용정보의 활용에 중점을 두고 있는 것이다. 물론 이는 「신용정보법」만의 문제는 아니며, 「정보통신망법」에서도 동일한 접근을 취하고 있다.[158] 그러나 이미 많은 업체에서 회원가입 시 광고성 정보 전송에 대한 별도의 동의를 받고 있고, 시민들이 느끼는 불법스팸의 폐해가 심각하다는 점[159]에서 광고성 정보의 전송에 대한 정책의 기조가 전환될 필요가 있다. 즉, 사전 동의를 전제로 광고성 정보를 전송할 수 있도록 「신용정보법」뿐 아니라, 「정보통신망법」도 개정될 필요가 있다.

「신용정보법」 제37조(개인신용정보 제공·이용 동의 철회권 등)
① 개인인 신용정보주체는 제32조제1항 각 호의 방식으로 동의를 받은 신용정보제공·이용자에게 신용조회회사 또는 신용정보집중기관에 제공하여 개인의 신용도 등을 평가하기 위한 목적 외의 목적으로 행한 개인신용정보 제공 동의를 대통령령으로 정하는 바에 따라 철회할 수 있다. 다만, 동의를 받은 신용정보제공·이용자 외의 신용정보제공·이용자에게 해당 개인신용정보를 제공하지 아니하면 해당 신용정보주체와 약정한 용역의 제공을 하지 못하게 되는 등 계약 이행이 어려워지거나 제33조 각 호 외의 부분 본문에 따른 목적을 달성할 수 없는 경우에는 고객이 동의를 철회하려면 그 용역의 제공을 받지 아니할 의사를 명확하게 밝혀야 한다.

158) 「정보통신망법」 제50조제1항은 전자우편 등을 이용한 영리목적의 광고성 정보의 전송을 위해 사전 동의을 받는 것이 아니라, 다만 '명시적인 수신거부의사'만 없으면 보낼 수 있도록 하고 있다. 제2항에서 전화, 팩스를 이용한 전송의 경우에는 사전 동의를 받도록 하고 있지만, 거래관계가 있던 업체의 경우에는 동의를 받지 않아도 되도록 하고 있다.

159) 한국정보보호진흥원이 발간한 「2008 정보보호실태조사: 개인편」에 따르면, 정보화 역기능 유형별 피해의 심각성에 대한 인식 조사에서 '불법스팸(전화/이메일)'이 3.57점으로 가장 높게 나타났다(4점 척도 기준. 매우 심각하다: 4점, 심각한 편이다: 3점, 심각하지 않은 편이다: 2점, 전혀 심각하지 않다: 1점). 그 다음은 '개인정보/프라이버시 침해'(3.52점)로 나타났다. 이를 응답 비율로 보면, 불법스팸이 심각하다는 응답이 61.5%, 심각한 편이다라는 응답이 34.3%에 달했다(한국정보보호진흥원, 2008b).

② 개인인 신용정보주체는 대통령령으로 정하는 바에 따라 신용정보제공·이용자에 대하여 상품이나 용역을 소개하거나 구매를 권유할 목적으로 본인에게 연락하는 것을 중지하도록 청구할 수 있다.
③ 신용정보제공·이용자는 서면, 전자문서 또는 구두에 의한 방법으로 제1항 및 제2항에 따른 권리의 내용, 행사방법 등을 거래 상대방인 개인에게 고지하고, 거래 상대방이 제1항 및 제2항의 요구를 하면 즉시 이에 따라야 한다. 이 때 구두에 의한 방법으로 이를 고지한 경우 대통령령으로 정하는 바에 따른 추가적인 사후 고지절차를 거쳐야 한다.

개정 「신용정보법」이 시행된 이후, 한 은행은 정보주체의 '고객정보관리' 메뉴에 아래와 같이 전화수신거부 및 개인신용정보 제공·활용에 대한 동의 철회를 할 수 있도록 서비스하고 있었다.

<그림 2-10> 한 은행의 전화수신거부 및 동의철회 관리 화면

## 5. 결 론

금융 분야는 개인정보의 집중 및 공동 활용이 가장 광범위한 분야 중 하나다. 개별 금융기관에서 생성된 개인신용정보와 공공기관에서 보유하고 있는 개인정보가 종합/개별신용정보집중기관 및 신용조회회사를 통해 집중되며, 이렇게 집중된 정보는 개별 금융기관 및 공공기관에 활용된다.

2009년 10월 2일 시행된 개정 「신용정보법」은 △ 개인의 동의제도 강화, △ 신용정보관리·보호인의 지정·운용을 의무화, △ 개인신용정보 제공·이용 동의 철회권 신설 등 개인신용정보주체의 권리를 강화한 측면이 있지만, 다른 한편으로는 △ 신용정보회사의 업무 확대, △ 신용조회회사 또는 신용정보집중기관의 공공기관에 대한 신용정보 제공 요청 근거를 확대하는 등 신용정보 공동활용의 폭을 넓혔다.

금융 시스템의 원활한 작동을 위해 개인 신용정보의 수집과 공유가 일정하게 필요하기는 하나, 개인신용정보는 정보주체의 재산이나 경제활동에 치명적인 영향을 미칠 수 있는 매우 민감한 정보인 만큼, 엄격하게 보호되어야 하고 정보주체의 결정권이 확실하게 보장될 필요가 있다. 그러나 현행 「신용정보법」 규정과 금융기관의 신용정보 보호 실태는 몇 가지 문제점을 드러내고 있다.

첫째, 개인신용정보의 집중·활용과 관련하여 개인신용정보의 제공·활용 동의는 형식적인 것에 머물고 있다.

둘째, 신용정보회사등과 공공기관의 개인정보 공유가 지나치게 광범위하게 이루어지고 있다. 관련 법에서 규정한 개인정보 보호 규정에도 불구하고, 공공기관이 보유하고 있는 개인정보가 신용정보라는 명목으로 민간에 제공될 수 있고, 또한 그 범위마저 자의적으로 규정될 수 있어, 신용정보와 관련해서는 자칫 개인정보의 보호를 위한 관련 법의 취지가 훼손될 위험이 있다. 「신용정보법」에서 신용정보회사등과 공공기관 간에 공유할 수 있는 신용정보의 범위에 대해서 활용 목적에 맞게 보다 세부적이고, 제한적으로 규정할 필요가 있다.

셋째, 신용정보활용체제 등 각 금융기관에서 공시하고 있는 개인정보 보호 규정들이 정보주체가 쉽게 이해할 수 있도록 체계적으로 정리될 필요가 있다. 특히, 개인정보의 제3자 제공과 관련한 사항(제3자 제공기관이나 위탁기관, 제공되는 개인정보의 종류, 목적 등)이 보다 상세하게 명시될 필요가 있다.

넷째, 개인정보를 서로 다른 기관간에 공유하는 경우가 증가하면서, 개인정보의 열람이나 제공내역을 정보주체가 인식할 필요성이 증가하고 있다. 신용정보집중기관이나 신용조회회사 등의 홈페이지를 통해서는 이를 열람할 수 있지만, 개별 금융기관의 홈페이지를 통해서도 개인신용정보의 조회 내역이나 제3자 제공내역을 쉽게 열람할 수 있도록 제공할 필요가 있다.

# 제5절 보건의료영역

## 1. 개요

개인의 의료정보, 혹은 건강정보는 가장 민감한 개인정보 중의 하나다. 통상 의료정보는 환자의 질환에 대한 의사의 진단 및 처방, 간호기록, 의료 장비에 의한 측정 데이터 등으로 구성되어 있다. 그래서 의료 정보는 환자의 개인정보라기 보다는 병원 혹은 의사들이 생산·통제하는 정보로 인식되어 왔다. 그러나 의료정보 역시 특정 개인을 떠나 존재할 수 없다는 점에서 개인정보임을 부인하기 힘들다(민주노총 공공연맹 의료연대노동조합, 2006:12). 나아가 정보통신 기술의 발전과 건강에 대한 관심의 증가 등에 따라, 환자가 치료 목적으로 병원을 찾아가던 환경에서 개인의 질병 예방과 건강 증진을 위해 언제 어디서나 의료 서비스가 찾아가는 소위 u-Health 환경으로 패러다임이 전환되고 있다. 이에 따라, 의료영역의 개인정보의 범위도 의료기관 내부에서 생성되는 '의료정보'에서 가정이나 건강관리센터 등에서 수집될 수 있는 모든 생체정보, 혹은 '건강정보'[160]로 그 범위가 확대되고 있다(정혜정·김남현, 2009a: 115).

의료정보의 유출이나 오남용은 개인에게 여러 측면에서 피해를 야기할 수 있다. 자신의 병력정보가 외부에 알려지는 것 자체가 정보주체에게는 수치심을 불러일으키거나 사회적 관계를 위축시킬 수 있다. 또한, 병력정보가 보험

160) 보건의료 영역에서 '개인정보'로서 보호해야할 대상을 어떤 용어로, 어떻게 규정할 것인가부터 아직 모호한 상황이다. 「보건의료기본법」이나 「의료법」에는 '자신의 보건의료와 관련한 기록'(「보건의료기본법」 제11조제2항), '환자에 관한 기록'(「의료법」 제21조제1항), '전자처방전 및 전자의무기록에 저장된 개인정보'(「의료법」 제18조제3항), '다른 사람의 비밀'(「의료법」 제19조) 등으로 규정하고 있을 뿐, 이에 대해 정의하고 있지 않다. 18대 국회에 발의된 「개인건강정보 보호법안」(전현희 의원 대표발의)은 '건강정보'를 정의하고 있으나, '보건의료인이 진료과정에서 얻은 개인의 과거· 현재·미래의 신체적이거나 정신적인 건강상태, 상병·치료 및 과거병력, 가족병력 등의 진료정보'로 제한하여 진료과정 외의 건강정보는 제외하고 있다. 백원우 의원이 대표발의 한 「건강정보보호법안」은 '건강정보'를 '질병·부상에 대한 예방·진단·치료·재활과 출산·사망 및 건강증진에 관한 지식 또는 부호·숫자·문자·음성·음향·영상 등으로 표현된 모든 종류의 자료'로 폭넓게 정의하고 있는데 이는 비개인정보까지 포함하는 것이고, 이와 별개로 '건강기록'(국민 개개인의 건강정보를 기록한 것)이라는 개념을 두고 있다. 어쨌든 보호대상인 개인정보를 어떻게 정의할 것인가부터 논의가 필요할 것으로 보인다. 이 글에서는 개인 건강정보에 대해 포괄적으로 다루는 것이 아니라 의료기관이 보유하고 있는 개인정보를 주로 다루기 때문에 '(개인)의료정보'라는 용어를 사용하기로 한다.

회사에 알려져 보험 가입을 거부당하거나, 에이즈 감염을 이유로 직장에서 부당 해고되는 등 개인에 대한 차별의 원인이 될 수 있다. 시스템 불안정이나 고의적인 조작으로 정보가 잘못될 경우 생명에 치명적인 영향을 줄 수도 있다(민주노총 공공연맹 의료연대노동조합, 2006:16).

이러한 위험성은 보건의료의 정보화가 진척되면서 더욱 커질 수 있다. 디지털 형태로 집적되는 개인정보의 양과 폭이 증가할 뿐더러, 의료기관 간 정보공유가 확대되면서 개인정보에 접근할 수 있는 사람들도 늘게 된다. 방대한 개인정보 데이터베이스는 그 가치를 높여 개인정보 유출의 유혹 역시 커질 수밖에 없으며, 접근할 수 있는 사람이 많아지면 그만큼 유출의 경로도 증가하게 된다. 이와 같이 정보화의 진척에 따라 해킹이나 내부자에 의한 개인정보의 유출, 권한 없는 접근(무단 열람) 등의 위험성도 커질 수밖에 없는데, 실제로 해마다 국민건강보험공단이나 국민연금관리공단 등 공공기관에서의 정보 유출이나 무단 열람 등의 문제가 불거지고 있다.

의료정보의 민감성에도 불구하고, 이의 보호를 위한 법제도는 다른 영역에 비해 턱없이 미비한 상황이다. 아직 사회 전 부문을 아우르는 「개인정보보호법」 제정이 지체되고 있지만, 이제 「공공기관의 개인정보보호에 관한 법률」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」 등 주요 법률들은 OECD의 「개인정보의 국제유통과 프라이버시 보호에 관한 가이드라인」의 주요 원칙들을 반영해 나가고 있다. 그러나 보건의료 관련 법률들은 개인정보 보호 원칙들을 체계적으로 반영하지 못하고 있다.

## 2. 의료정보 보호 관련 법제도 실태

의료정보의 보호와 관련된 규정은 「보건의료기본법」, 「의료법」 등 보건의료 관련 법률에 일부 포함되어 있다.

「보건의료기본법」 제12조는 보건의료서비스에 관한 자기결정권을 규정하고 있다. 그러나 이는 '보건의료서비스'에 관한 자기결정권이지 개인정보에 관한 자기결정권은 아니다.

「보건의료기본법」 제11조제2항[161] 및 「의료법」 제21조제1항[162]은 정

161) 제11조 (보건의료에 관한 알 권리) ②모든 국민은 관계 법령이 정하는 바에 의하여 보건의료인 또는 보건의료기관에 대하여 자신의 보건의료와 관련한 기록 등의 열람이나 사본의 교부를 요청할 수 있다. 다만, 본인이 요청할 수 없는 경우에는 그 배우자·직계존비속 또는 배우자의 직계존속이, 그 배우자·직계존비속 및 배우자의 직계존속

보주체의 자기정보에 대한 열람권을 보장하고 있다. 그러나 정정·삭제 청구권은 규정되어 있지 않다.

개인정보의 수집·이용에 대한 동의 및 제3자 제공과 관련된 내용은 명확하게 규정되어 있지 않다. 다만, 「의료법」 제21조제2항 및 제3항에서 "같은 환자의 진료에 필요하여 다른 의료기관에서 그 환자에 대한 기록, 임상소견서 및 치료경위서의 열람이나 사본 송부를 요청하거나 환자가 검사 기록, 방사선 필름 등의 사본 교부를 요구하면 이에 응하여야"하며, "응급환자를 다른 의료기관으로 이송할 때에는 환자 이송과 함께 초진기록을 보내"도록 하고 있어 제3자 제공의 일부 근거가 되고 있다. 그러나 병원 등의 의료기록이 건강보험심사평가원 등에 대량 제공되고 있음에도 불구하고 이에 대한 제공 근거가 없었는데, 2010년 1월 31일 시행 예정인 「의료법」에 그 근거 조항을 마련하였다. 개정된 제21조제2항[163] 에 따르면, △ 환자의 배우자 등

---

이 없거나 질병 기타 요청을 할 수 없는 부득이한 사유가 있는 경우에는 본인이 지정하는 대리인이 기록의 열람 등을 요청할 수 있다.

162) 제21조 (기록 열람 등) ①의료인이나 의료기관 종사자는 이 법이나 다른 법령에 따로 규정된 경우 외에는 환자에 관한 기록을 열람하게 하거나 그 사본을 내주는 등 내용을 확인할 수 있게 하여서는 아니 된다. 다만, 환자, 환자의 배우자, 환자의 직계존비속 또는 배우자의 직계존속(배우자, 직계존비속 및 배우자의 직계존속이 없는 경우에는 환자가 지정하는 대리인)이 환자에 관한 기록의 열람이나 사본 교부 등 그 내용 확인을 요구하는 경우에는 환자의 치료를 위하여 불가피한 경우가 아니면 확인할 수 있게 하여야 한다.

163) 개정된 「의료법」이 2010년 1월 31일 시행될 예정이다.

제21조 (기록 열람 등) ② 제1항에도 불구하고 의료인이나 의료기관 종사자는 다음 각 호의 어느 하나에 해당하면 그 기록을 열람하게 하거나 그 사본을 교부하는 등 그 내용을 확인할 수 있게 하여야 한다. 다만, 의사·치과의사 또는 한의사가 환자의 진료를 위하여 불가피하다고 인정한 경우에는 그러하지 아니하다. <개정 2009.1.30>

1. 환자의 배우자, 직계 존속·비속 또는 배우자의 직계 존속이 환자 본인의 동의서와 친족관계임을 나타내는 증명서 등을 첨부하는 등 보건복지가족부령으로 정하는 요건을 갖추어 요청한 경우
2. 환자가 지정하는 대리인이 환자 본인의 동의서와 대리권이 있음을 증명하는 서류를 첨부하는 등 보건복지가족부령으로 정하는 요건을 갖추어 요청한 경우
3. 환자가 사망하거나 의식이 없는 등 환자의 동의를 받을 수 없어 환자의 배우자, 직계 존속·비속 또는 배우자의 직계 존속이 친족관계임을 나타내는 증명서 등을 첨부하는 등 보건복지가족부령으로 정하는 요건을 갖추어 요청한 경우
4. 「국민건강보험법」 제13조, 제43조, 제43조의2 및 제56조에 따라 급여비용 심사·지급·대상여부 확인·사후관리 및 요양급여의 적정성 평가·가감지급 등을 위하여 국민건강보험공단 또는 건강보험심사평가원에 제공하는 경우
5. 「의료급여법」 제5조, 제11조, 제11조의3 및 제33조에 따라 의료급여 수급권자 확인, 급여비용의 심사·지급, 사후관리 등 의료급여 업무를 위하여 보장기관(시·군·구), 국민건강보험공단, 건강보험심사평가원에 제공하는 경우
6. 「형사소송법」 제106조, 제215조 또는 제218조에 따른 경우
7. 「민사소송법」 제347조에 따라 문서제출을 명한 경우

친족이 요청하는 경우, △ 환자가 지정하는 대리인이 요청하는 경우, △ 급여비용 심사 등을 위해 국민건강보험공단 또는 건강보험심사평가원에 제공하는 경우, △ 의료급여 업무를 위하여 보장기관(시・군・구), 국민건강보험공단, 건강보험심사평가원에 제공하는 경우, △ 민・형사소송법 등에 따라 제공하는 경우, △ 산재보험 관련하여 근로복지공단에 제공하는 경우, △ 진료기관으로부터 자동차보험진료수가를 청구받은 보험회사가 관계 진료기록의 열람을 청구한 경우, △ 징병검사대상자의 진료기록 등을 지방병무청에 제공하는 경우, △ 공제회가 공제급여의 지급 여부를 결정하기 위해 요양기관에 관계 진료기록의 제공을 요청하는 경우, △ 「고엽제후유의증 환자지원 등에 관한 법률」에 따른 진료기록의 제공 등 개인 의료기록의 제3자 제공의 근거를 보다 구체적으로 명시하고 있다.

의료정보의 관리와 관련해서는 「의료법」 제18조제2항 및 제23조제3항에서 “누구든지 정당한 사유 없이 전자처방전(전자의무기록)에 저장된 개인정보를 탐지하거나 누출・변조 또는 훼손하여서는 아니 된다”고 규정하고 있

---

8. 「산업재해보상보험법」 제118조에 따라 근로복지공단이 보험급여를 받는 근로자를 진료한 산재보험 의료기관(의사를 포함한다)에 대하여 그 근로자의 진료에 관한 보고 또는 서류 등 제출을 요구하거나 조사하는 경우
9. 「자동차손해배상 보장법」 제12조제2항 및 제14조에 따라 의료기관으로부터 자동차보험진료수가를 청구받은 보험회사등이 그 의료기관에 대하여 관계 진료기록의 열람을 청구한 경우
10. 「병역법」 제11조의2에 따라 지방병무청장이 징병검사와 관련하여 질병 또는 심신장애의 확인을 위하여 필요하다고 인정하여 의료기관의 장에게 징병검사대상자의 진료기록・치료 관련 기록의 제출을 요구한 경우
11. 「학교안전사고 예방 및 보상에 관한 법률」 제42조에 따라 공제회가 공제급여의 지급 여부를 결정하기 위하여 필요하다고 인정하여 「국민건강보험법」 제40조에 따른 요양기관에 대하여 관계 진료기록의 열람 또는 필요한 자료의 제출을 요청하는 경우
12. 「고엽제후유의증 환자지원 등에 관한 법률」 제7조제3항에 따라 의료기관의 장이 진료기록 및 임상소견서를 보훈병원장에게 보내는 경우

③ 의료인은 다른 의료인으로부터 제22조 또는 제23조에 따른 진료기록의 내용 확인이나 환자의 진료경과에 대한 소견 등을 송부할 것을 요청받은 경우에는 해당 환자나 환자 보호자의 동의를 받아 송부하여야 한다. 다만, 해당 환자의 의식이 없거나 응급환자인 경우 또는 환자의 보호자가 없어 동의를 받을 수 없는 경우에는 환자나 환자 보호자의 동의 없이 송부할 수 있다. <개정 2009.1.30>

④ 진료기록을 보관하고 있는 의료기관이나 진료기록이 이관된 보건소에 근무하는 의사・치과의사 또는 한의사는 자신이 직접 진료하지 아니한 환자의 과거 진료 내용의 확인 요청을 받은 경우에는 진료기록을 근거로 하여 사실을 확인하여 줄 수 있다. <신설 2009.1.30>

⑤ 의료인은 응급환자를 다른 의료기관에 이송하는 경우에는 지체 없이 내원 당시 작성된 진료기록의 사본 등을 이송하여야 한다. <신설 2009.1.30> [시행일 : 2010.1.31]

다. 그러나 다른 법에서 규정된 것과 같은 개인정보 관리 책임자의 지정, 개인정보 보호정책의 공시, 관리·기술적 보호조치 등에 대한 구체적인 규정은 없다.

한편, 보건의료 관련 제반 법률에서는 비밀누설 금지조항을 포함하고 있다. 「보건의료기본법」 제13조는 "모든 국민은 보건의료와 관련하여 자신의 신체·건강 및 사생활의 비밀을 침해받지 아니한다"고 선언하고 있으며, 「의료법」 제19조는 의료인에게 비밀누설 금지의무를 부과하고 있다. 이 외에 「약사법」 제87조, 「정신보건법」 제42조, 「전염병예방법」 제54조의6, 「후천성면역결핍증 예방법」 제7조, 「장기등 이식에 관한 법률」 제27조, 「응급의료에 관한 법률」 제40조, 「국민건강보험법」 제86조 등에서 직무상 지득한 비밀의 누설 금지 조항을 포함하고 있다.

지금까지 본 바와 같이, 보건의료 관련 법률은 의료정보의 보호를 위한 몇 개 조항을 포함하고 있기는 하지만, 의료정보의 보호나 정보주체의 권리에 대해 아직 체계적으로 규정하고 있지 않고 있다. 물론 국립서울병원과 같은 국립병원이나 국민건강보험공단과 같은 공공기관이 보유하고 있는 개인정보는 「공공기관의 개인정보보호에 관한 법률」의 적용을 받을 수 있다. 그러나 이는 여타 민간 병원이 보유하고 있는 개인정보에 적용될 수 있는 것은 아니다. 또한, 병원 등 의료기관이 홈페이지를 통해 진료 예약 등 서비스를 제공하는 경우, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 적용을 받을 수 있다. 그러나 이 역시 홈페이지를 통해 수집된 개인정보에 대해서만 적용될 뿐, 해당 의료기관이 보유하고 있는 의료정보 일체에 대해 적용되는 것은 아니다.

따라서 보건의료 영역의 개인정보 보호를 체계적으로 규율하기 위한 입법이 절실한 상황이다. 지난 2006년 10월 정부는 「건강정보 보호 및 관리운영에 관한 법률안」을 입법예고하였으나, 17대 국회에서 처리되지 못하고 폐기되고 말았다. 18대 국회에는 백원우 의원이 대표발의 한 「건강정보보호법안」(의안번호 제1800137호), 전현희 의원이 대표발의 한 「개인건강정보보호법안」(의안번호 제1802206호), 유일호 의원이 대표발의 한 「개인건강정보 보호법안」(의안번호 제1803076호) 등이 계류되어 있는 상황이다. 세 법안 모두 세부적인 내용은 차이가 있지만, 개인 건강정보에 대해 OECD에서 규정한 개인정보 보호원칙을 보장하고자 하고 있다.

## 3. 생성기관에서의 의료정보의 수집・유통 실태

생성기관이란 병원, 약국, 보건소 등 의료정보를 생성하는 기관을 지칭한다. 「보건의료기본법」이나 「의료법」에는 생성기관에 대한 정의가 없다. 다만, 백원우 의원이 대표발의한 「건강정보보호법안」 및 전현희 의원이 대표발의 한 「개인건강정보 보호법안」에는 생성기관에 대한 정의를 두고 있다.[164]

본 연구에서는 국립 의료기관 및 국립대학교 병원을 대상[165]으로 의료정보의 수집・유통 실태에 대한 정보공개를 청구하였으며, 그 답변 결과를 정리하였다. 민간 영역의 의료기관의 실태에 대해서는 정보접근의 한계로 인해 다루지 못하였으나 공공 의료기관이 「공공기관의 개인정보보호에 관한 법률」의 적용을 받는다는 것 외에는 큰 차이는 없을 것으로 보인다.

### 1) 의료정보의 수집

환자들의 의료기록은 진료기록부 등에 기록된다. 「의료법」 제22조에서 이를 규정하고 있다. 진료기록부에 기재될 세부적인 내용은 동법 시행규칙 제14조(진료기록부 등의 기재 사항)[166]에서 명시하고 있다.

---

164) 백원우 의원안은 생성기관을 “보건의료 관계 법령이 정하는 기관 중 의료기관, 약국(「약사법」제91조에 따른 한국희귀의약품센터를 포함한다), 보건기관(보건소, 보건의료원, 보건지소, 보건진료소를 포함한다) 및 그 밖에 제11조에 따른 건강정보보호위원회의 심의를 거쳐 보건복지가족부령으로 정하는 기관”으로 정의하고 있으며, 전현희 의원안은 “건강정보를 생성하는 기관으로서 다음 각 목에 해당하는 기관을 말한다. 가. 「의료법」 제3조에 따른 의료기관, 나. 「약사법」 제2조에 따른 약국 및 같은 법 제91조에 따른 한국희귀의약품센터, 다. 「지역보건법」 제7조에 따른 보건소, 같은 법 제8조에 따른 보건의료원 및 같은 법 제10조에 따른 보건지소, 라. 「농어촌 등 보건의료를 위한 특별조치법」 제2조에 따른 보건진료소, 마. 그 밖의 다른 법령에 따라 건강정보를 생성할 수 있는 기관”으로 정의하고 있다.

165) 조사 대상 국립병원 및 국립대학교 병원은 다음과 같다 : 경찰병원, 국립공주병원, 국립마산병원, 국립목표병원, 국립부곡병원, 국립서울병원, 국립춘천병원, 서울대병원, 전남대병원, 전북대병원, 충남대병원. 부산대병원, 경북대병원, 경상대병원, 충북대병원, 강원대병원 등에서는 정보공개 청구에 답변을 하지 않았다.

166) 1. 진료기록부
가. 진료를 받은 자의 주소・성명・주민등록번호・병력(病歷) 및 가족력(家族歷)
나. 주된 증상, 진단 결과, 진료경과 및 예견
다. 치료 내용(주사・투약・처치 등)
라. 진료 일시분(日時分)
2. 조산기록부
가. 조산을 받은 자의 주소・성명・주민등록번호
나. 생・사산별(生・死産別) 분만 횟수

「의료법」 제22조 (진료기록부 등) ①의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록(이하 "진료기록부등"이라 한다)을 갖추어 두고 그 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다. ②의료인이나 의료기관 개설자는 진료기록부등[제23조제1항에 따른 전자의무기록(電子醫務記錄)을 포함한다. 이하 제40조제2항에서 같다]을 보건복지가족부령으로 정하는 바에 따라 보존하여야 한다.

국립병원 등에서는 「공공기관의 개인정보보호에 관한 법률」에 따라 보유하고 있는 개인정보파일대장을 공개하고 있었다. 그러나 국립대학의 병원 및 민간 병원 등은 어떠한 개인정보파일을 보유하고 있는지, 어떤 개인정보를 기록하고 있는지 공개하지 않아 정확히 알 수 없었다. 다만,「의료법」및 시행규칙에서 기록 의무를 부여하고 있으므로, 이에 준하여 환자의 개인정보 및 의료정보를 보유하고 있을 것으로 보인다.

국립병원 및 국립대학교 병원 등에서 개인정보파일대장 및 정보공개 청구에 대한 답변을 통해 공개한 개인정보 보유 현황은 다음과 같다.

<표 2-55> 의료기관(국립병원 및 국립대학교 병원) 개인정보 보유 현황

| | 개인정보파일목록 | 수집동의방법 | 법적근거[167] |
|---|---|---|---|
| A국립병원 | 환자진료정보<br>1. 진료를 받은 자의 주소·성명·주민등록번호·병력(病歷) 및 가족력<br>2. 주된 증상, 진단 결과, 진료경과 및 예견<br>3. 치료 내용(주사·투약·처치 등) | 「공공기관의 개인정보보호에 관한 법률」 제4조에 의하여 정보주체의 동의가 없더라도 「의료법 시행규칙」 제14조에 명시된 개인정보를 수집할 수 있음 | 공공기관 개인정보보호법 제4조 및 제5조, 의료법 제22조 의료법 시행규칙 제14조 및 제15조 |

---

다. 임신 후의 경과와 그에 대한 소견 및 보건지도 요령
라. 임신 중 의사에 의한 건강진단의 유무(결핵·성병에 관한 검사를 포함한다)
마. 분만 장소 및 분만 연월일시분(年月日時分)
바. 분만의 경과 및 그 처치
사. 산아(産兒) 수와 그 성별 및 생·사의 구별
아. 산아와 태아부속물에 대한 소견
자. 임부(姙婦)·해산부(解産婦)·산욕부(産褥婦) 또는 신생아에 대한 지도 요령
차. 산후의 의사의 건강진단의 필요성 유무
3. 간호기록부
가. 체온·맥박·호흡·혈압에 관한 사항
나. 투약에 관한 사항
다. 섭취 및 배설물에 관한 사항
라. 처치와 간호에 관한 사항

| | | | |
|---|---|---|---|
| | 4. 진료 일시분(日時分) | | |
| B국립병원 | 환자진료정보<br>성명, 주소, 주민등록번호, 연락처, 성별, 직업, 혼인상태, 학력, 종교, 보호자, 관계, 장애정보, 건강보험정보 | 오프라인 수집 (개인의 신청서를 통한 수집)<br>법적인 근거를 가지고 있으므로 별도의 동의 절차 필요없음 | 정신보건법 제26조의2, 국민건강보험법 제43조 |
| C국립병원 | 환자자격관리<br>주민등록번호, 휴대폰 번호, 의료보험번호, 성명, 전화번호, 주소, 생년월일, 성별, 연령 | 환자 정보 수집시 개인정보 수집동의는 법적 근거를 가지고 있으면 별도의 동의 절차 필요 없음 | (대장) 국민건강보험법 시행규칙, 국민건강보험법 제43조 및 의료급여법 제11 조<br>(홈페이지)의료법 제22조, 시행규칙 제18조 |
| D국립병원 | 환자진료파일<br>성명, 주민등록번호, 휴대폰번호, 의료보험번호, 피보험자성명, 전화번호, 주소, 생년월일, 성별, 연령, 진료일, 상병명, 처방내역, 진료기록, 각종검사 및 결과 | 접수담당이 인적사항입력, 의료인이 진료정보 직접입력<br>보유 근거에 따라 본인이 직접제공하며 양식에 의한 동의서는 받지 않음. | (대장) 의료법 제21조, 의료법시행규칙 제17조 및 제18조, 보건복지가족부와 그 소속기관 직제, 보건복지가족부와 그 소속기관 직제 시행규칙, 국립목포병원 운영규정<br>(홈페이지) 의료법 제22조 의료법시행규칙 제18조 |
| E국립병원 | 환자정보파일<br>주민등록번호, 휴대폰 번호, 의료보험번호, 계약(정부-일반국민)시 발생하는 식별번호, 성명, 전화번호, 주소, 생년월일, 성별, 직업, 연령, 혼인상태, 세대원 정보, 학력, 현직장정보(회사명, 부서, 직위, 고용형태), 행정서비스정보(민원처리내용, 공공서비스 수혜기록), 진료정보(정신질환기록 포함), 본적 및 출신지, 종교 | 오프라인 수집(개인의 신청서를 통한 수집)<br>의료법 및 의료법 시행규칙에 따라 별도동의 필요 없음 | (대장) 의료법 제18조, 제21조<br>(홈페이지) 의료법 제22조, 의료법시행규칙 제18조 |
| F국립병원 | 환자진료정보<br>주민등록번호, 휴대폰 번호, 의료보험번호, 회원번호, 성명, 전화번호, 주소, 생년월일, 성별, 직업, 연령, 과거병력, 진 | 진료 신청서 접수<br>의료법 제22조에 따라 환자의 동의 없이 개인 정보 수집 가능 | 의료법 제22조, 의료법시행규칙 제15조 |

| | | | |
|---|---|---|---|
| | 료정보(정신질환기록 포함), 가족병력, 장애정보 | | |
| G국립병원 | 환자진료정보<br>주민등록번호, 이메일주소, 휴대폰번호, 의료보험번호, 성명, 전화번호, 주소, 생년월일, 성별, 연령, 일반신체정보(키,몸무게,혈액형등), 계급, 과거병력, 진료정보(정신질환기록포함),가족병력, 장애정보 | 진료의뢰서 | |
| A대학병원 | 의무기록복사대장 (등록번호, 환자명 신청인, 복사용도)<br>연구용 의무기록 대출승인(등록번호, 환자명 신청인 성명, 조회기간)<br>인적사항 변경대장(등록번호, 환자명 환자구분, 주민번호, 주소, 변경전후이름) | 의료정보운영규정 제31조(직원 및 제3자의 개인정보 보호) 에 의거 병원업무 수행상 개인정보의 수집이 필요한 경우 의료정보센터장의 승인을 얻은 후 최소한의 개인정보(외래 접수 및 입원 수속시 필요한 기본 인적사항, 홈페이지 이용시 입력하는 기본 인적사항)만을 수집, 활용하며. 업무수행과 무관한 사생활 정보는 수집할 수 없음. | 의료법, 의료법 시행규칙, 의료정보운영규정(자체), 의무기록관리 규정·지침(자체) |
| B대학병원 | 전자의무기록 : 성명, 주민등록번호, 주소, 전화번호 기타 진료정보<br>홈페이지 회원정보 | 진료를 목적으로 병원을 방문한 환자는 스스로 제공하는 방법으로 정보 수집이 되지만 학구용(연구용) 정보수집 시는 동의서를 받음 | 의료법 제22조 내지 제23조 |
| C대학병원 | 홈페이지 회원, 환자정보관리 | 진료 및 선택진료 신청서 | 의료법 제21조 |
| D대학병원 | 퇴원환자대장(등록번호, 환자명 입원일, 퇴원일, 퇴원과, 환자구분 주민번호, 병동호실, 재원일수)<br>왜래과별미납반대장(등록번호, 환자명 주민번호, 대출일시, 진료과)<br>인적사항변경대장(등록번호, 환자명 환자구분, 주민번호, 주소, 변경전후이름) | 직무상 외래 접수 및 입원 수속 시 입력된 기본 인적 사항과 진료 시 의료진이 OCS에 입력한 상병, 진찰료, 입원료, 투약, 주사, 마취, 이학요법, 정신요법, 처치 및 수술, 검사, 방사선, 식대 등 진료행위가 발생하는 데이터와 각종 검사결과 데이터 | |

전술했듯이, 현재 의료정보 보유근거는 「의료법」 제22조 및 동법 시행규칙 제14조이다. 각 병원의 개인정보파일목록 및 홈페이지에 공개된 정책에서 수집 근거가 다르게 명시된 곳이 있었고, 일부 병원의 경우 개인정보파일목록과 홈페이지에 공개된 정책에 명시된 법적 근거가 달랐는데, 이는 법 개정 과정에서 근거 조항 번호가 변경된 것이 반영되지 않았기 때문인 것으로 보인다. A 및 D대학병원이 공개한 개인정보파일목록은 환자 진료기록부를 제외한 여타 목록을 제공한 것으로 보인다.

각 병원들이 기록하고 있는 개인정보 항목을 모두 공개한 것은 아닐 수도 있으나, 일부 병원의 경우는 의료정보 외의 개인정보 항목에 결혼여부, 학력, 종교 등 민감한 개인정보도 수집하고 있음을 알 수 있다.

또한, 의료기관에서의 개인정보 수집은 '진료신청서' 등을 통해 기본 인적사항을 입력한 후, 의료진들의 진료행위를 통해 발생하며, 개인정보의 수집, 이용, 제3자 제공과 관련한 별도의 동의서는 받지 않는 것으로 나타났다. 다른 사회영역과 달리, 의료영역에서는 개인정보 수집 시 필수정보와 선택정보의 구분이나 수집된 개인정보가 어떻게 이용·제공되는지에 대한 동의 혹은 고지 체계가 갖춰져 있지 않은 상황이다.

### 2) 의료정보의 제3자 제공

병원에서 보유하고 있는 의료정보는 약국, 타 병원, 국민건강보험공단 등 공공기관, 시·군·구, 경찰서 및 법원 등 다양한 기관에 제공된다.

환자에게 의약품을 투여할 필요가 있을 경우, 「의료법」제18조에 따라 처방전을 작성하여 환자에게 내주거나 전자처방전을 발송한다. 전자처방전은 성명, 주민등록번호, 처방 의약품의 명칭 등이 포함된 처방전[168]을 병원과 제휴 관계에 있는 약국에 인터넷 등 전산 시스템을 통하여 전송하는 시스템

---

167) (대장)이라고 표시된 것은 각 병원이 공개하고 있는 개인정보파일대장의 내용을 참고했다는 의미이며, (홈페이지)는 홈페이지에 공개된 내용을 참고했다는 의미이다.

168) 「의료법」 시행규칙 제12조는 처방전의 기재사항을 규정하고 있다. 이에 따르면, 처방전에는 다음과 같은 사항이 기록된다.

1. 환자의 성명 및 주민등록번호
2. 의료기관의 명칭 및 전화번호
3. 「통계법」 제22조제1항 전단에 따른 한국표준질병·사인 분류에 따른 질병분류기호
4. 의료인의 성명·면허종류 및 번호
5. 처방 의약품의 명칭(일반명칭, 제품명이나 대한약전에서 정한 명칭을 말한다)·분량·용법 및 용량
6. 처방전 발급 연월일 및 사용기간
7. 의약품 조제시 참고 사항

이다.

환자가 타 병원으로 이송될 경우, 환자의 동의하에 진료기록을 제공한다. 일부 대형 병원은 1차, 2차 진료기관과의 업무 제휴를 통해 3차 기관으로 이송되어 온 환자가 재차 1차, 2차 진료 기관에서 진료를 받는 경우 해당 기관에서 대형 병원의 전산시스템에 접속하여 해당 환자의 진료내역을 조회할 수 있도록 하고 있다(정연수, 2004: 140). 이번 조사 대상 병원들 중에는 타 병원과 환자정보를 공유하는 병원은 없었으며, 타 병원에서의 진료시 환자 동의에 따라 진료정보(검사결과 및 영상, 투약내용, 치료계획 등)를 제공한다고 답변하였다.

건강보험업무나 저소득층에 대한 의료지원 등을 위해 병원 등이 보유한 의료정보가 건강보험심사평가원, 국민건강보험공단, 근로복지공단, 시・군・구 등 공공기관에 제공된다.

병원은 「국민건강보험법」 제43조[169]에 따라 건강보험 진료비 청구를 위해 건강보험심사평가원에 진료 내역을 제공한다. 심사 후, 이 정보는 건강보험심사평가원에서 건강보험공단으로 보내진다. 건강보험심사평가원에 제공되는 의료정보의 내용은 동법 시행규칙 제12조제2항에 규정되어 있다. 이에 따르면, △ 가입자(지역가입자의 경우에는 세대주를 말한다)의 성명 및 건강보험증번호, △ 요양급여를 받은 자의 성명 및 주민등록번호, △ 질병 또는 부상명, △ 요양개시 연월일 및 요양일수, △ 요양급여비용의 내용, △ 본인부담금 및 비용청구액, △ 처방전 내용 등을 요양급여비용명세서에 기재하여야 한다.

저소득층 등 의료비 지원의 대상이 되는 환자의 진료정보는 「의료급여법」 제11조[170]에 따라 건강보험심사평가원(동법 시행규칙 제20조에 의하면,

---

169) 제43조 (요양급여비용의 청구와 지급 등) ①요양기관은 요양급여비용의 지급을 공단에 청구할 수 있다. 이 경우 제2항의 규정에 의한 심사청구는 이를 공단에 대한 요양급여비용의 청구로 본다.

②제1항의 규정에 의한 요양급여비용의 청구를 하고자 하는 요양기관은 제55조의 규정에 의한 건강보험심사평가원에 요양급여비용의 심사청구를 하여야 하며, 심사청구를 받은 건강보험심사평가원은 이를 심사한 후 지체없이 그 내용을 공단 및 요양기관에 통보하여야 한다.

170) 제11조 (급여비용의 청구와 지급) ①의료급여기관은 제10조의 규정에 따라 의료급여기금에서 부담하는 급여비용의 지급을 시장・군수・구청장에게 청구할 수 있다. 이 경우 제2항의 규정에 의한 심사청구는 이를 시장・군수・구청장에 대한 급여비용의 청구로 본다.

②제1항의 규정에 의한 급여비용의 청구를 하고자 하는 의료급여기관은 급여비용심사기관에 급여비용의 심사청구를 하여야 하며, 심사청구를 받은 급여비용심사기관은 이를 심사한 후 지체없이 그 내용을 시장・군수・구청장 및 의료급여기관에 알려야 한다.

제11조의 급여비용심사기관은 건강보험심사평가원이다)에 제공되며, 이 정보는 의료비용을 실제 부담하는 시・군・구에 전달된다. 산재보험 대상 환자의 의료정보는 「산업재해보상보험법」 제45조[171]에 따라 근로복지공단에 제공된다. 동법 시행규칙 제27조에 따라, 개인별 진료비 명세서와 처방전의 내용을 포함한다.

아래 표(예를 들어, C대학병원)에서 볼 수 있는 바와 같이, 환자들의 성명, 주민등록번호, 의료보험증번호 등의 정보가 선천성이상아현황, 암환자현황 등 실태조사 목적으로 보건복지부에 제공되기도 한다.

수사 목적으로 경찰에 제공되는 경우나 법원의 요청에 따라 법원에 제공되는 경우도 적지 않은 것으로 보인다. B대학병원의 경우, 수사협조 목적으로 경찰서에 제공되는 의료정보(성명, 주민등록번호, 병명, 치료내용, 치료결과 등)가 연간 120건~150건 정도나 된다. 또한, 법원의 신체감정 의뢰에 대한 회신 건수도 2007년 363건, 2008년 504건, 2009년 327건에 달했다.

아래는 조사 대상 의료기관들의 개인정보 제3자 제공 현황에 대한 답변을 정리한 것이다. 근로복지공단, 경찰서, 보건복지부, 시・군・구 등에 대한 정보 제공 사실이 없는데, 이는 제공을 하지 않는다기 보다는 답변에 포함시키지 않은 것으로 보인다. 그러나 대체적인 현황을 파악하는데는 무리가 없을 것이다.

<표 2-56> 의료기관(국립병원 및 국립대학교 병원)
개인정보의 제3자 제공 현황

| | 타병원과의공유 | 제3자 제공 | 법적근거 |
|---|---|---|---|
| A국립병원 | 타병원과 환자정보를 공유하지 않음 | 건강보험심사평가원(건강보험환자 및 의료급여환자), 근로복지공단(산재환자)<br>법원, 경찰서 등 소송 및 수사관련 협조<br>동사무소, 보건소 등 공공기관의 행정업무협조 | 공공기관 개인정보보호법 제10조, 국민건강보험법 제43조, 국민건강보험법 시행규칙 제12조, 의료급여법 제11조, 의료급여법 시행규칙 제20조, 산업재해보상보험법 제45조, 산업재해보상보험법 시행규칙 |

171) 제45조 (진료비의 청구 등) ① 산재보험 의료기관이 제40조제2항에 따라 요양을 실시하고 그에 드는 비용(이하 "진료비"라 한다)을 받으려면 공단에 청구하여야 한다.
② 제1항에 따라 청구된 진료비에 관한 심사 및 결정, 지급 방법 및 지급 절차는 노동부령으로 정한다.

| | | | |
|---|---|---|---|
| | | | 제27조 |
| B국립병원 | | 국민건강보험공단(가입자, 성명, 주민등록번호, 질병, 요양일수, 본인부담금, 비용 청구액, 처방전내용) | 국민건강보험법 제43조 |
| C국립병원 | | 건강보험심사평가원(주민등록번호,의료보험번호, 성명, 주소, 생년월일, 과거병력, 진료정보(정신질환기록 포함), 장애정보) | 국민건강보험법 및 의료급여법 |
| D국립병원 | | 건강보험심사평가원(의료보험번호, 피보험자성명, 수진자성명, 주민등록번호, 진료개일, 상병명, 진료기간, 진료결과, 처방내역)<br>시군구보건소(성명, 주민등록번호, 연령, 국적, 직업, 주소, 결핵과거치료력, 결핵예방접종, 결핵초회진단) | 국민건강보험법 제43조, 의료급여법(진료비청구), 결핵예방법, 전염병예방법 |
| E국립병원 | 해당사항 없음 | 건강보험심사평가원(주민등록번호,의료보험번호,성명,진료정보(정신질환기록 포함))<br>국가행정기관, 민간 및 개인 등 | 국민건강보험법 |
| F국립병원 | 해당사항 없음 | 건강보험심사평가원, 건강보험관리공단, 동사무소, 경찰서 등 공공기관, 보험회사, 환자 본인, 환자 외 타인(환자의 위임장 필요) | 공공기관의 개인정보보호에 관한 법률, 국민건강보험법 |
| G국립병원 | 타병원으로 외래진료 및 전원(입원) 시 환자동의에 따라 제공<br>- 환자정보 항목 : 진료정보(검사결과 및 영상, 투약내용, 치료계획 등) | 심사평가원, 국민건강보험공단, 각 지방경찰청 등 건수 | 국민건강보험법 제83조, 공공기관의 개인정보보호에 관한법률 제10조(처리정보의 이용 및 제공의 제한) |
| A대학병원 | 환자가 타병원으로 전원할 경우 본인 요청에 한하여 기록 제공 | | 의료법, 의료법 시행규칙, 의료정보운영규정(자체), 의무기록관리 규정·지침(자체) |
| B대학병원 | 개인정보보호를 위하여 타 병원과의 공유프로그램 없음 | 심사평가원 : 해당사항 없음<br>국민건강보험공단(중증환자 등록/급여제한여부조회 : 성명, 주민등록번호, 주소, 병명, 연락처, 챠트사본 등)<br>경찰서(수사협조 : 성명, 주민등록번호, 병명, 치료내용, 치료결과 등) | 의료법 제21조, 형사소송법 제199조, 경찰관 직무집행법 제8조, 민사소송법 제341조, 정보통신망이용등에 관한 법률상 |

| | | | |
|---|---|---|---|
| | | 법원(신체감정 의뢰에 대한 회신 : 성명, 주민등록번호, 기타 병명 등 감정의뢰사항에 대한 답변) | 의 개인정보보호규정 등 |
| C대학병원 | 공유하지 않음. | 국민건강보험공단, 건강보험심사평가원(건강보험증번호, 의료급여증별구분, 피보험자성명, 주민등록번호, 수진자성명, 상병명, 상병분류기호,처방내역, 내원일, 진료결과, 진료과목(11))<br>보건복지부(실태조사 목적 : 선천성이상아현황, 암환자현황, 본인부담진료비실태조사 : 성명, 주민등록번호, 의료보험증번호 등 제공) | 국민건강보험법 제83조, 동법시행규칙 제12조 |
| D대학병원 | 타 병원과 환자 현황 공유 | 보건복지가족부(환자조사, 퇴원환자조사, 선천성이상아조사, 영아모성사망조사, 임산부 사망, 사산 및 미숙아 선천성 이상아 보고서) | |

### 3) 의료정보의 폐기

의료기록의 보존 기간은 「의료법」 시행규칙 제15조에서 정하고 있다.

「의료법」 시행규칙

제15조 (진료에 관한 기록의 보존) ① 의료기관의 개설자 또는 관리자는 진료에 관한 기록을 다음 각 호에 정하는 기간 동안 보존하여야 한다.

1. 환자 명부 : 5년
2. 진료기록부 : 10년
3. 처방전 : 2년
4. 수술기록 : 10년
5. 검사소견기록 : 5년
6. 방사선사진 및 그 소견서 : 5년
7. 간호기록부 : 5년
8. 조산기록부: 5년
9. 진단서 등의 부본(진단서·사망진단서 및 시체검안서 등을 따로 구분하여 보존할 것) : 3년

② 제1항의 진료에 관한 기록은 마이크로필름이나 광디스크 등(이하 이 조에서 "필름"이라 한다)에 원본대로 수록하여 보존할 수 있다.

③ 제2항에 따른 방법으로 진료에 관한 기록을 보존하는 경우에는 필름촬영책임자가 필름의 표지에 촬영 일시와 본인의 성명을 적고, 서명 또는 날인하여야 한다.

그러나 이는 의무적 보존기간일 뿐, 이 기간 이후 폐기해야 한다는 명시적 규정은 없다. 아래 표에서와 같이, 일부 병원에서는 기록을 영구 보존하는 경우도 있었다. 보유기간을 10년이라고 답변한 경우에도, 실제로는 그 이상 보존하고 있음에도 불구하고 단지 법에서 규정하는 의무 보존 기간을 답변했을 수도 있다. 이는 현장에 대한 실태조사가 필요한 부분이다. 한 연구에 따르면, 의사에 대한 설문조사 결과 전자의무기록의 적정보존기간에 대해 36.7%가 영구보존의 필요성을 제기한 것으로 나타났다(이미정, 2008). 어쨌든 현행법상 의료정보의 파기에 대한 근거가 없는 만큼, 보유의 필요성에 대한 전문적 판단을 거쳐 보존기간 및 파기에 대해 법에서 명시할 필요가 있다.

<표 2-57> 전자의무기록의 적정보존기간에 대한 의사 대상 설문조사 결과

| 전체 | 현행 의료법상 보존기간과 동일 | 현행 보존기간 보다 2배연장 | 현행 보존기간 보다 3배연장 | 현행 보존기간 보다 4배연장 | 영구보존 |
|---|---|---|---|---|---|
| 275(100.0) | 79(28.7) | 54(19.6) | 20(7.3) | 21(7.6) | 101(36.7) |

자료: 이미정(2008).

<표 2-58> 의료기관(국립병원 및 국립대학교 병원)의 의료정보 보유 기간

| | 보유기간 및 폐기방법 |
|---|---|
| A국립병원 | -보유기간 : 「의료법 시행규칙」 제15조 규정에 따름<br>환자 명부(5년), 진료기록부(10년), 처방전(2년), 수술기록(10년),<br>검사소견기록(5년), 방사선사진 및 그 소견서(5년), 간호기록부(5년),<br>조산기록부(5년), 진단서 등의 부본(3년)<br>- 폐기방법: 파기 |
| B국립병원 | 10년 |
| C국립병원 | 10년 |
| D국립병원 | 10년 (마지막내원일기준) |
| E국립병원 | 의료법 및 의료법시행규칙 제15조 (진료에 관한 기록의 보존) |
| F국립병원 | - 영구<br>- 의료법 시행규칙<br>- 현재 모든 환자 정보를 보유(폐기 하지 않음) |
| G국립병원 | 의무기록은 의료법 시행규칙 제15조(진료에 관한 기록의 보존)에 의거하여 최대 10년 보존, 폐기는 소각을 원칙. 보유하고 있는 개인정보파일을 파기할 경우 복구할 수 없는 기술적 방법을 통해 원본 및 백업본을 파기. 다수가 공동 이용하는 데이터베이스 형태의 개인정보파일은 행정정보 데이터베이스 표준화 지침(행정안전부고시 제2008-47호)의 폐기절차에 따라 폐기. |
| A대학병원 | - 의무기록 관리규정 제13조 (의무기록의 보존) |

| | |
|---|---|
| | 1) 의무기록은 다음 각 호와 같이 보존하여야 한다.<br>2)「의료법 시행규칙」 제15조제2항에 따라 제1호의 진료에 관한 기록은 마이크로필름·광디스크 또는 전산기억장치 등에 원본대로 수록·보존할 수 있다.<br>3) 보존 기한이 경과한 의무기록은 위원회의 심의를 거쳐 폐기 여부를 결정한다.<br>4) EMR 스캔 이후 1년이 경과된 기록지 중 동의서를 제외한 별도서식(타병원기록 등)은 위원회의 심의를 거쳐 폐기할 수 있다.<br>- 보존기한이 지난 기록물은 해당 부서인 의료정보운영실에서 내부결재를 득하고 총무과에 폐기요청을 하게 됩니다(폐기는 문서 폐기를 전문으로 하는 정부기관에 의뢰하여 실시, 폐기시에는 각서 등을 받아 향후 문서의 유출이 되지 않도록 철저히 관리). 폐기 후에는 목록 및 내용을 내부결재 후 보관 합니다. |
| B대학병원 | 의료법 시행 규칙 제15조(진료에 관한 기록의 보존)를 준수하여 보존 및 폐기하고, 이는 의무기록관리위원회의 심의를 한 후 병원장의 승인을 받아 적법한 절차에 의함 |
| C대학병원 | 영구보관 |
| D대학병원 | 1. 의무기록은 특별한 규정이 있는 경우를 제외하고는 10년간 보존하여야 한다. 다만, 영상관리시스템이나 전산기억장치에 저장된 의무기록은 원장 승인 후 폐기할 수 있다.<br>2. 의무기록의 영상관리시스템은 수기 및 전산으로 출력한 모든 기록을 원본 그대로 저장함을 원칙으로 한다.<br>3. 영상의무기록은 컴퓨터 서버에 저장하며 별도의 백업서버를 두어 의무기록 원본이 훼손된 경우 복구할 수 있도록 한다.<br>4. 의무기록 영상관리서버 및 백업서버는 의료정보팀에서 관리한다. |

### 4) 의료정보의 관리

의료정보의 관리와 관련해서는 「의료법」 제18조제2항 및 제23조제3항에서 “누구든지 정당한 사유 없이 전자처방전(전자의무기록)에 저장된 개인정보를 탐지하거나 누출·변조 또는 훼손하여서는 아니 된다”고 규정하고 있다. 그러나 다른 법과 같은 개인정보 관리 책임자의 지정, 개인정보 보호정책의 공시, 관리·기술적 보호조치 등에 대한 구체적인 규정은 없다.

국립병원의 홈페이지에서는 ‘개인정보보호정책’에서 ‘홈페이지 이용자의 개인정보보호’ 및 ‘컴퓨터에 의해 처리되는 개인정보보호’ 두 부분으로 나누어 설명하고 있다. ‘컴퓨터에 의해 처리되는 개인정보보호’ 부분이 병원에서 보유하고 있는 환자 의료정보에 대한 것인데, △ 개인정보의 수집 및 보유, △ 개인정보의 이용 및 제공의 제한, △ 개인정보파일의 열람 및 정정청구, △ 권익침해 구제방법, △ 개인정보보호책임관의 이메일 등 연락처 등의 내용을 담고 있다. 개인정보 수집 및 보유 항목에서는 환자 의료정보 파일의 파일명,

근거, 목적, 주요항목, 보유기간 등을 고지하고 있으나, 개인정보의 이용 및 제공의 제한 등 여타 항목은 「공공기관의 개인정보 보호에 관한 법률」의 관련 조항을 설명하고 있을 뿐, 의료정보의 제공 기관, 제공되는 정보항목 등에 대한 구체적인 실태는 명시하고 있지 않았다.

국립대학교 병원들의 홈페이지 역시 마찬가지였으며, 홈페이지를 통해 가입한 이용자의 개인정보 보호정책에 한정된 경우가 많았다. 서울아산병원, 연세세브란스병원 등 민간 병원의 경우에도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따라 홈페이지 이용자의 개인정보취급방침을 고시하고 있을 뿐이다. A대학병원, C대학병원, D대학병원 등 일부 병원의 경우 개인 의료정보 보호를 위한 내부 지침을 가지고 있다고 답변하였다. A대학병원의 경우 자체 의료정보운영규정 및 의무기록관리규정을, C대학병원의 경우 개인정보 보호를 위한 기본지침을, D대학병원의 경우 환자정보보호 및 보안지침을 가지고 있었다.

<표 2-59> 의료기관(국립병원 및 국립대학교 병원)의 의료정보 보호를 위한 정책

| | 개인정보보호정책 |
|---|---|
| A국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| B국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| C국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| D국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| E국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| F국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| G국립병원 | 홈페이지 이용자의 개인정보보호, 컴퓨터에 의해 처리되는 개인정보보호 |
| A대학병원 | 홈페이지 이용자의 개인정보 보호, 컴퓨터에 의해 처리되는 개인정보보호, 의료법 제21조 준수, 자체 의료정보운영규정 준수, 자체 의무기록관리규정, 지침 준수, 의료법 제21조(기록열람등), 제23조(전자의무기록) |
| B대학병원 | 홈페이지의 개인정보보호정책 (정보통신망법 준수) |
| C대학병원 | 홈페이지 이용자의 개인정보 보호, 컴퓨터에 의해 처리되는 개인정보보호, 개인정보보호를위한기본지침 운영 |
| D대학병원 | 홈페이지 이용자의 개인정보 보호, 컴퓨터에 의해 처리되는 개인정보보호, 환자정보보호 및 보안지침 |

「의료법」 제19조 등에서 의료인들의 비밀준수 의무를 규정하고 있기는 하지만, 병원에서 보유하고 있는 의료정보에 대해 권한없는 열람이나 유출이 문제가 될 수 있다. 한 기사에 따르면, 2001~2005년 환자의 진료기록부를 불법적으로 작성·열람케 한 혐의로 총 253건의 행정처분이 의사에게 내려졌다.[172] 지난 2006년 의료연대노조가 한 병원 노동자를 대상으로 한 설문조사에서도 환자정보가 무단 열람이나 유출에 노출되어 있는 것으로 드러났다. 설문조사에서 담당환자 이외의 환자정보를 수정할 수 있다는 응답비율이 26.4%, 주변 부탁으로 환자진료기록을 검색해 본 적이 있다는 응답비율이 48.6%, 다른 사람이 주변 부탁으로 환자진료기록을 검색하고 있는 것을 목격한 적이 있다는 응답비율이 59.9%에 이르렀다. 또한, 전자의무기록(EMR)에서 담당환자 이외의 환자정보를 수정 가능하다는 응답이 26.4%였으며, EMR 로그인 상태에서 자리를 비운 채 이동하여 업무를 본 경험이 있다는 답변은 75.7%나 되었다. 인증카드의 비밀번호로 주민등록번호를 사용한다는 응답도 절반에 달했다(민주노총 공공연맹 의료연대노동조합, 2006). 해외에서도 브리트니 스피어스, 마이클 잭슨 등 유명 인사들의 의료정보를 병원 직원들이 불법 열람한 사실이 드러난 바 있다.[173]

<표 2-60> 환자정보 보호 관련 9개 사항

| 항 목 | 『예』 응답 비율(%) |
|---|---|
| EMR에서 담당환자 이외의 환자정보 수정 가능 | 26.4 |
| EMR 로그인(인증키를 꽂고) 상태에서 자리 비운 채 이동 | 75.7 |
| EMR 인증카드 비밀번호로 주민등록번호 사용 | 50.0 |
| EMR 관련 환자정보 보호에 관한 교육 이수 | 35.4 |
| EMR 관련 환자정보 보호교육 내용 만족 | 27.7 |
| 개인정보 안전관리 | 9.7 |
| EMR 시스템 불안정으로 업무지연 경험 | 86.8 |
| 주변 부탁으로 EMR에서 환자진료기록 검색 목격 | 59.9 |
| 주변 부탁으로 EMR에서 환자진료기록 검색 | 48.6 |

172) 경향신문. 2006.7.3. “병원-보험사 환자기록 ‘뒷거래’.”
173) 마이데일리. 2008.3.15. “브리트니 스피어스 의료기록 훔쳐본 병원직원 무더기 해고”; 헤럴드경제. 2009.7.28. “잭슨 사망진단서, 불법열람 300번?”

조사대상 한 병원의 「환자정보보호 및 보안지침」에는 아래와 같은 내용이 '금기사항'으로 규정되어 있었다. 역으로 생각하면, 의료 종사자가 아래 의무에 충실하지 못할 경우, 환자 의료정보가 외부에 유출될 위험이 있는 것이다.

가. 공개된 장소(복도, 엘리베이터, 직원식당 등)에서 환자에 관한 대화를 나누는 경우
나. 외래 진료대기자 명단이나 병동 환자현황표, 침상이름표 등에 환자이름과 개인신상정보 또는 진단명, 수술명이 동시에 게시되는 경우
다. 업무용 전산화면의 환자개인정보가 외부인에 노출되는 경우
라. 근무자가 부재 시 진료용 모니터가 켜진 채 방치되거나, 챠트가 외부에 노출되어 있는 경우
마. 접근권한이 없는 직원이 환자의 의무기록을 열람하거나 OCS에 진료정보를 조회하는 경우
바. 의무기록사본 또는 출력된 진료정보를 이면지로 사용하거나 폐기하지 않고 부주의하게 관리되는 경우
사. Log-out하지 않고 다른 근무자에게 업무를 계속하게 허용하는 경우
아. ID와 Password가 동일하거나, Password로 사원번호, 주민등록번호, 전화번호 등 노출이 쉬운 번호를 사용하는 경우

한편, 지난 2005년 12월, 건강보험심사평가원과 대한의료정보학회가 채영문 교수를 통해 수행한 연구보고서에 따르면, 국내 의료기관의 정보보안 수준이 상당히 미흡한 것으로 나타났다.

요양기관 종류별 인적, 관리적 정보보안 현황을 보면 40% 이상의 병원에서 보안교육 및 보안서약서 작성을 모두 시행하지 않고 있었다. 관리적 측면에서도 접근통제 및 사용통제를 모두 적용하고 있는 병원은 43.9%에 불과하였다(건강보험심사평가원 외, 2005; 민주노총 공공연맹 의료연대노조, 2006: 21 재인용).

<표 2-61> 의료기관별 정보화 현황

| 구 분 | | 종합전문병원 | 종합병원 | 병원 | 계 |
|---|---|---|---|---|---|
| 인적 정보보안 | 보안교육실시 및 보안서약서 작성 | 8(20.0) | 9(12.7) | 11(6.4) | 28(9.9) |
| | 보안교육만 실시 | 12(30.0) | 30(42.3) | 67(39.0) | 109(38.5) |
| | 보안서약서만 작성 | 4(10.0) | 4(5.6) | 7(4.1) | 15(5.3) |
| | 적용안함 | 16(40.0) | 28(39.4) | 87(50.6) | 131(46.3) |
| | 계 | 40(100.0) | 71(100.0) | 172(100.0) | 283(100.0) |
| 관리적 정보보안 | 접근통제 및 사용통제 적용 | 29(70.7) | 40(55.6) | 57(32.8) | 126(43.9) |
| | 접근통제 적용 | 4(9.8) | 12(16.7) | 28(16.1) | 44(15.3) |
| | 사용통제 적용 | 7(17.1) | 14(19.4) | 49(28.2) | 70(24.4) |
| | 적용안함 | 1(2.4) | 6(8.3) | 40(23.0) | 47(16.4) |
| | 계 | 41(100.0) | 72(100.0) | 174(100.0) | 287(100.0) |

정보업무 총괄조직이 없는 곳도 50% 이상이 훨씬 넘었다. EMR, OCS, PACS[174]를 모두 도입한 병원의 경우에도 46.2%의 병원만이 총괄조직을 두고 있었다.

<표 2-62> 정보업무 총괄 조직 여부

| | 구 분 | | | | 계 |
|---|---|---|---|---|---|
| | OCS & PACS & EMR | OCS & PACS | OCS OR PACS | 해당없음 | |
| 예 | 12(46.2) | 15(22.1) | 11(16.4) | 11(20.0) | 49 |
| 아니오 | 14(53.8) | 53(77.9) | 56(83.6) | 44(80.0) | 167 |
| 계(100.0) | 26 | 68 | 67 | 55 | 216 |

정전 등에 대비한 UPS 및 자가발전설비를 구축하고 있는 곳도 OCS, PACS, EMR를 모두 갖춘 기관만 50%를 넘었을 뿐, 나머지는 50%가 되지 않는 것으로 나타났다. 즉, 갑작스러운 정전이나 사고가 발생할 경우, 의료서비스가 중지되거나 의료 정보가 유실될 수 있는 위험을 안고 있는 것이다.

174) EMR(Electronic Medical Record)은 전자의무기록시스템, OCS(Order communication System)는 처방전달시스템, PACS(Picture Archiving and Communication System)는 의료영상저장전송시스템으로 의료영상을 디지털화한 것을 의미한다.

<표 2-63> UPS 또는 자가발전설비 구축여부

| | 구 분 | | | | 계 |
|---|---|---|---|---|---|
| | OCS & PACS & EMR | OCS & PACS | OCS OR PACS | 해당없음 | |
| UPS & 자가발전설비 | 19(57.6) | 37(43.5) | 29(35.8) | 14(24.6) | 99 |
| UPS | 9(27.3) | 37(43.5) | 30(37.0) | 26(45.6) | 102 |
| 자가발전설비 | 2(6.1) | 3(3.5) | 12(14.8) | 6(10.5) | 23 |
| 없음 | 3(9.1) | 8(9.4) | 10(12.3) | 11(19.3) | 32 |
| 계(100.0) | 33 | 85 | 81 | 57 | 256 |

네트워크 백업 설비 역시 50% 이상의 병원들이 구축하지 못하고 있었다.

<표 2-64> 네트워크 백업 예비선로 여부

| | 구 분 | | | | 계 |
|---|---|---|---|---|---|
| | OCS & PACS & EMR | OCS & PACS | OCS OR PACS | 해당없음 | |
| 모두 갖춤 | 8(25.8) | 13(16.3) | 7(9.5) | 4(7.1) | 32 |
| 일부 갖춤 | 9(29) | 14(17.5) | 11(14.9) | 13(23.2) | 47 |
| 없음 | 14(45.2) | 53(66.3) | 56(75.7) | 39(69.6) | 162 |
| 계 | 31 | 80 | 74 | 56 | 241 |

위 조사는 2005년 조사이며, 4년 이상 지난 현재에는 이 보다 보안 수준이 나아졌을 수도 있다. 의료기관의 보안실태에 대한 최신 조사가 필요할 것으로 보인다. 그러나 아직 보건복지가족부 차원에서 각 병원의 개인 의료정보 보호나 보안에 대한 구체적인 지침이 없는 것은 문제라고 할 수 있다. 건강정보 보호를 위한 보건복지가족부 차원의 지침이 있는지에 대한 질의에 대해, 보건복지가족부는 “공공의료기관은 「공공기관의 개인정보보호에 관한 법률」을, 민간의료기관은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 적용을 받고 있”고, “국민건강보험공단 등 산하공공기관도 「공공기관의 개인정보보호에 관한 법률」의 적용을 받고 있”으며, “동 관계법령의 주관부처(행정안전부 등)에서 배포한 관련 지침을 준용하고 있”다고 답변하였다.

### 5) 정보주체의 열람 및 정정・삭제 청구권

앞서 언급했다시피, 「보건의료기본법」 제11조제2항 및 「의료법」 제21조제1항은 정보주체의 자기정보에 대한 열람권을 보장하고 있다. 그러나 정정・삭제 청구권은 규정되어 있지 않다. 국립병원의 경우에는 「공공기관의 개인정보보호에 관한 법률」에 따라 열람권을 보장하고 있었고, 일부 국립병원의 경우 내부 지침에 관련 내용을 포함하고 있었다.

<표 2-65> 의료기관(국립병원 및 국립대학교 병원)에서 자기정보 열람방법

| | 자기정보열람방법 |
|---|---|
| A국립병원 | - 자기정보의 열람방법 : 개인정보파일대장에 기재된 범위 안에서 문서로 열람을 청구할 수 있음<br>- 열람이 거부될 경우 이의신청 방법 : 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판청구나 행정소송을 제기할 수 있음 |
| B국립병원 | 공공기관개인정보법 |
| C국립병원 | 공공기관개인정보법 |
| D국립병원 | 공공기관개인정보법 |
| E국립병원 | 공공기관개인정보법 |
| F국립병원 | 개인정보에 대한 열람・정정은 「공공기관의 개인정보보호에 관한 법률」 등 관련법령의 규정이 정하는 바에 따라 서식에 의하여 입・퇴원계에서 열람・정정을 청구 가능. |
| G국립병원 | 열람청구서 제출, 열람제한 결정서를 받은 날부터 90일 이내에 처분청 또는 재결청에 행정심판 청구 또는 법원에 행정소송. 제3자가 의료정보를 요구할 시 의료법 제19조(비밀 누설 금지), 제21조(기록 열람 등) 또는 다른 법령에 따로 규정된 경우 외에는 의료정보를 제공하지 않음. |
| A대학병원 | 의무기록관리지침 제19조 (의무기록 사본발급 및 출력요청 절차)에 의거 환자 본인이 의무기록 사본을 요청할 때에는 의사가 작성한 의무기록사본 신청서(의무기록의 사용목적을 명시해야함)를 신분증과 함께 제출해야 합니다. 다만 환자가 사망, 의식불명, 미성년, 금치산자 등인 경우에는 환자의 친권자가 환자를 대신할 수 있습니다. |
| B대학병원 | 의료법 제21조(기록 열람 등) 규정에 의해 열람 가능하고, 거부 시 병원 감사과 또는 관할 보건소에 민원 제기 가능 |
| C대학병원 | 진료기록사본 발급지침 |
| D대학병원 | 의무기록관리규정 제18조 (의무기록 열람)<br>환자의 승인서와 담당의사의 허락이 있어야 한다. 다만, 미성년자, 정신병자, 법적 무능력자 및 사망의 경우는 환자와의 관계를 증명하는 서류를 제시하여야 한다. |

그러나 의료기록에 대한 열람 내역이나 제3자 제공 내역에 대한 정보주체의 열람권은 보장하고 있지 않다. 본인에 대한 명시적인 동의나 고지절차 없이, 생성기관에서 보유하고 있는 환자의 의료기록이 다수의 취급기관에 제공되고, 또 취급기관에서도 보유하고 있는 개인정보를 시·군·구 등 타 공공기관에 제공하는 현실을 감안하면, 정보주체의 개인정보자기결정권은 유명무실해질 수밖에 없다. 최소한 자신의 의료정보를 누가 열람했는지, 어떠한 기관에 제공되었는지에 대한 내역을 정보주체가 열람할 수 있도록 보장할 필요가 있다.

의료기록은 의사 등이 진단, 치료 과정에서 생성한 정보이기 때문에, 정정·삭제권을 부여하는 것에 대해서 논란이 있을 수 있다. 그러나 기록된 정보가 명백히 사실과 다른 경우에는 정정 청구를 할 수도 있을 것이다.[175] 2009년 10월 현재, 18대 국회에 계류 중인 「건강정보보호법안」(백원우 의원 대표발의) 및 「개인건강정보 보호법안」(전현희 의원 대표발의) 모두 열람 및 정정청구권을 보장하고 있다.

## 4. 취급기관에서의 의료정보 수집·유통 실태

취급기관이란 국민건강보험공단, 질병관리본부, 건강보험심사평가원, 대한적십자사 등 생성기관으로부터 정보를 제공받아 취급하는 기관[176]을 지칭한다. 이 역시 「보건의료기본법」이나 「의료법」에는 정의되어 있지 않다.

---

175) 한 연구에서 의사 대상 설문조사를 한 결과, 응답자의 40.9%가 의무기록의 내용에 대한 정정요청을 받은 경험이 있는 것으로 나타났다. 정정을 요청한 사람은 환자본인 34.4%, 보호자 및 법정대리인 21.9%, 보험회사직원 7.0%, 시설관리자 2.6%, 기타 환자와 대립되는 기관 3.3%였다. 정정이 가능한 정도를 묻는 질문에는 명백한 오류(성별, 주민번호, 오른쪽 또는 왼쪽 등의 위치 등)가 가장 높게 나타났고, 그 다음은 '확인할 수 없는 과거력, 가족력, 사고경위 등에 관한 내용(예, 흡연력 있음↔없음, 낙상↔싸움 등등)'이 차지했다(이미정, 2008).

176) 백원우 의원안은 취급기관을 "보건의료 관계 법령에 따라 생성기관의 정보를 제공받아 취급하는 기관 중 질병관리본부, 국민건강보험공단, 건강보험심사평가원 및 그 밖에 건강정보보호위원회의 심의를 거쳐 보건복지가족부령으로 정하는 기관"으로 정의하고 있으며, 전현희 의원안은 "보건의료 관계 법령에 따라 생성기관의 정보를 제공받아 취급하는 기관으로서 다음 각 목에 해당하는 기관을 말한다. 가. 질병관리본부, 나. 「국민건강보험법」 제12조에 따른 국민건강보험공단 및 같은 법 제55조에 따른 건강보험심사평가원, 다. 「혈액관리법」 제6조에 따른 대한적십자사, 라. 그 밖의 다른 법령에 따라 건강정보를 취급할 수 있는 기관"으로 정의하고 있다.

### 1) 의료정보의 수집

취급기관에서 보유하고 있는 개인정보 현황은 각 취급기관에서 공개하고 있는 개인정보파일목록을 통해 확인할 수 있다. 국민건강보험공단은 총 44개, 건강보험심사평가원은 4개, 질병관리본부는 12개의 개인정보파일을 보유하고 있다.

<표 2-66> 각 취급기관이 보유하고 있는 개인정보파일목록

| 기관명 | 개인정보파일목록 |
|---|---|
| 국민건강보험공단(44개) | 의료급여 개인급여, 자격상세내역, 급여정지, 주민번호/성명 변경, 직장가입자보수월액내역, 지역자동이체내역, 직장자동이체내역, 지역가입자부과내역, 직장가입자부과내역, 보험료부과내역, 압류내역, 체납고지내역, 체납처분 승인내역, 분할납부 신청내역, 개인별 건강검진결과, 현금급여내역, 진료내역통보 회신내역, 관리의약품 투여자 내역, 요양급여내역, 급여사후관리 결정내역, 요양기관 진료비 압류내역, 홈페이지 회원 가입업무, 건강위험평가(HRA) 내역, 합리적 의료이용 지원대상자 관리 내역, 중증암등록 내역, 기타징수금 고지내역, 기타징수금 압류 및 체납처분 승인내역, 사례관리 대상자 내역, 보장구 대여 신청자 및 사용자 관리내역, 건강보험상담센터 상담내역, 진료비 적정확인 신청내역, 의료이용고충 상담내역, 법률자문 내역, 노인장기요양 보험등급 판정심의요청자료, 노인장기요양보험 장기요양인정자 내역, 노인장기요양보험 이용지원 상담관리내역, 표준장기요양이용계획서 관리내역, 노인장기요양인정 등급자의 장기요양급여 계약 내역서 관리, 노인장기요양업무 관리내역, 장기요양급여내역, 장기요양 비수급자 내역, 장기요양기관 지정내역, 요양보호사 자격증 발급내역, 복지용구 계약내역 |
| 건강보험심사평가원(4개) | 청구명세서, 민원신청 고객정보, 요양기관현황관리, 포탈회원정보 |
| 질병관리본부(12개) | 집단설사환자 및 급성전염병환자정보, 입국자정보, 전염병 환자 명부, 결핵정보감시체계 결핵환자 신고화일, 예방접종기록, 국민건강영양조사 데이터 파일, 고혈압·당뇨병 환자 데이터 파일, 급성 심정지/급성 심근경색증/뇌졸중 심층조사 파일, 급성이완성마비감시, 연구과제 관리시스템 회원관리, 희귀난치성질환자 파일, 코호트 역학 정보파일 |

취급기관은 개별 의료기관으로부터 의료정보를 제공받아 방대한 데이터베이스를 구축하고 있다. 특히 국민건강보험공단의 경우에는 의료정보뿐만 아니라, 주민등록정보, 사업자등록자료, 출입국 기록, 장애인자료, 토지 및 자동차 자료, 연금자료 등 개인의 인적사항 및 재산 등에 대한 방대한 기록을 보

유하고 있다. 각 기관이 개인정보를 수집하는 방법은 다음과 같다(각 취급기관의 정보공개 청구에 대한 답변에 근거한 것이다).

<표 2-67> 각 취급기관의 개인정보 수집 방법

| 취급기관명 | 수집방법 | 수집기관명 |
|---|---|---|
| 국민건강보험공단 | 직접수집(정보주체) 및 시스템 연계에 의한 수집 | 행정안전부, 국세청, 시군구, 건강보험심사평가원, 국민연금공단, 근로복지공단, 출입국관리사무소, 그 외 필요시 법률에 의해 해당기관에 요청 |
| 건강보험심사평가원 | 서면, 전자매체(디스켓, CD), 전자통신(EDI, WEB) | 요양기관 79,569기관<br>(09년 7월현재) |
| 질병관리본부 | 전염병예방법, 검역법 등에 의거한 보유 | 시스템연계를 통한 제공기관 : 보건소, 병원 등에서 자료 등록 |

2009년 국정감사에서 국민건강보험공단 및 건강보험심사평가원이 박은수 의원실에 제출한 자료에 따르면, 시스템 연계를 통해 국민건강보험공단에 개인정보를 제공하는 기관 현황과 건강보험심사평가원이 보유하고 있는 개인정보의 수집방법 및 제공기관은 다음과 같다.

<표 2-68> 건강보험공단에 시스템 연계를 통해 개인정보를 제공하는 기관 현황

| 수집기관명 | 제공개인정보 | 개인정보 파일개수 | 비고 |
|---|---|---|---|
| 행정안전부 | 주민등록변동자료 | 1개 | 행정전산망 |
| 국세청 | 사업자등록자료 | 1개 | 4대보험 정보연계망 |
| 출입국관리사무소 | 내국인・외국인・재외국민・해외선원승무원・남북왕래자 | 1개 | 4대보험 정보연계망 |
| 보건복지가족부 | 등록장애인자료 | 1개 | 4대보험 정보연계망 |
| 전국지자체 | 토지자료 | 1개 | CD 및 행정전산망 |
| 16개광역시・도 | 자동차등록자료 | 1개 | CD 및 행정전산망 |
| 연금(사학, 공무원, 군인, 국민) | 연금자료 | 1개 | 행망 및 4대포탈 |
| 심사평가원 | 진료비명세서 | 1개 | 통신망 |

자료: 국민건강보험공단. 2009 국정감사 자료.

<표 2-69> 건강보험심사평가원이 보유하고 있는 개인정보의 수집방법 및 제공기관

| 수집자료명 | 수집방법 | 제공기관 | 제공기관수 |
|---|---|---|---|
| 요양급여비용 청구명세서 | 서면, 전자매체(디스켓,CD), 전자통신(EDI, WEB) | 요양기관 | 79,569기관 (09년 7월현재) |
| 요양기관현황 | 서면, 전자통신(포털) | | |
| 민원신청고객정보 | 서면, 전화, 전자통신(포털), 모사전송(FAX) | | |
| 포털회원정보 | 전자통신(포털) | | |

자료: 건강보험심사평가원. 2009 국정감사 자료.

취급기관이 보유하고 있는 개인정보는 정보주체의 동의를 받고 직접 수집되기 보다는 법에 근거하여 타 기관으로부터 제공받는 경우가 대부분이다. 그런데 취급기관이 개인정보를 제공받아 보유할 수 있는 법적 근거가 포괄적인 경우가 많다. 예컨대, 국민건강보험공단이 보유하고 있는 개인정보파일 중 '자격상세내역', '급여정지' 등 다수의 개인정보파일의 수집 근거가 「국민건강보험법」 제13조로 되어 있다. 이 조항은 국민건강보험공단의 '업무'를 규정한 것이다. 주어진 업무에 필요한 개인정보를 스스로 판단해서 수집하고 있는 것이다. 이는 자칫 과도한 개인정보의 수집을 초래할 수 있다.[177] 관련 법률에서 각 취급기관이 업무 수행을 위해 수집할 수 있는 개인정보의 범위를 엄격하게 규정할 필요가 있다.

### 2) 의료정보의 제3자 제공

각 취급기관이 보유하고 있는 개인정보는 다른 공공기관에 제공된다. 각 취급기관으로부터 개인정보를 제공받는 공공기관 현황은 다음과 같다.

177) 2008년 8월 22일 전현희 의원실 주최로 열린 <개인건강정보 보호법안 전문가 간담회>에서도 이러한 점이 지적되었다. 김주한 서울대 교수는 '개인 건강정보 보호법안에 대한 검토의견'에서 "다른 법률에 의하여 수집대상인 건강정보의 명시"가 '소관업무에 필요한 유관 정보'와 같이 매우 포괄적으로 규정된 것이 현실이다. 이는 현 시점에서 개인 건강정보의 어느 특정 항목이 어떠한 업무수행에 필요한가에 대한 논의와 연구가 부족함에 기인한 것으로 판단된다. 명료화되지 않은 규정은 자의적인 해석을 통한 개인정보의 과잉수집과 남용을 유발할 수 있다. 국제적 동향을 살펴보면 이와 같은 진료목적 외의 개인 건강정보의 2차사용(Secondary Use)에 대한 모든 항목들을 구체화하는 노력들이 진행되고 있다. 각각의 2차사용별 필요 최소항목 등을 정하는 등의 사회적 합의와 연구의 촉진을 명시하는 것이 필요할 것으로 판단된다"고 지적했다(김주한, 2008).

<표 2-70> 취급기관으로부터 개인정보를 제공받는 기관 현황

| 취급기관 | 제공기관 |
|---|---|
| 국민건강보험공단 | 행정안전부, 국세청, 시군구, 건강보험심사평가원, 국민연금공단, 근로복지공단, 그 외 요청기관의 법률적 근거가 있을 경우 보유기관장이 제공여부 결정 |
| 건강보험심사평가원 | 시·군·구청, 국민건강보험공단, 한국보훈복지의료공단, 해당 요양기관 |
| 질병관리본부 | 국민건강보험공단 |

각 기관별로 구체적인 현황을 보면 다음과 같다. 건강보험심사평가원이 타 기관에 개인정보를 제공하는 현황은 아래와 같다.

<표 2-71> 건강보험심사평가원으로부터 개인정보를 제공받는 기관 현황

| 기관구분 | 기관명 | 자료명 |
|---|---|---|
| 정부기관 | 시·군·구청 | 의료급여 청구명세서 |
| 공공기관 | 국민건강보험공단 | 건강보험 청구명세서,<br>요양기관현황, 민원신청 고객정보 |
| | 한국보훈복지의료공단 | 보훈환자 청구명세서 |
| 요양기관 | 해당 요양기관 | 민원신청고객정보 |

국민건강보험공단의 경우 보유하고 있는 자료가 워낙 방대하다보니, 수많은 기관에서 정보제공 요청이 이루어지고 있다. 국민건강보험공단이 박은수 의원실에 제공한 자료에 따르면, 시스템 연계를 통해 개인정보를 제공하는 현황은 아래와 같다.

<표 2-72> 국민건강보험공단으로부터 시스템 연계를 통해 개인정보를 제공받는 기관 현황

| 제공기관명 | 제공개인정보 | 개인정보 파일개수 | 비고 |
|---|---|---|---|
| 국민연금공단 | 직장가입자자료 등 4개 | 4개 | 국민연금법 제123조 |
| 건강보험심사평가원 | 직장가입자 및 피부양자자료 | 1개 | 국민건강보험법 제83조<br>자료연계협약 |
| 사립학교교직원 | 직장가입자자료 | 1개 | 사립학교연금법 제19조 |

| | | | |
|---|---|---|---|
| 연금공단 | | | |
| 공무원연금관리공단 | 직장가입자 | 1개 | 공무원연금법 제85조 |
| 보건복지부<br>(기초생활보장과) | 직장가입자 및<br>피부양자자료 | 1개 | 국민기초생활보장법<br>제22조,23조 |
| 국세청 | 진료비본인부담금<br>자료 | 1개 | 과세자료의 제출 및 관리에 관한<br>법률 제4조 및 동법 시행령 제2조 |
| 근로복지공단 | 요양급여내역 | 1개 | 산재보상보험법 제31조 |

자료: 국민건강보험공단. 2009 국정감사 자료.

또한, 「공공기관의 개인정보보호에 관한 법률」 제10조 등에 따라 타 기관에 제공하는 경우도 있다. 개인정보의 제공은 문서, 시스템 연계, 외부저장매체, 내부메일 등을 통해 이루어진다. 아래 자료는 2008년~2009년 8월말까지 국민건강보험공단이 타 기관에 건강보험 자료를 제공한 현황을 분석한 것이다. 2년 동안 공단 내 각 부서에서 총 733회, 1억 건이 넘는 120,138,454건의 개인정보를 제공한 것으로 나타났다.[178]

<표 2-73> 국민건강보험공단 부서별 건강보험 자료제공 현황

| 제공부서명 | 제공 회수 | 개인정보 건수 |
|---|---|---|
| 건강관리실 | 13 | 9,638,797 |
| 고객지원실 | 20 | 830,194 |
| 급여관리실 | 66 | 2,022,887 |
| 보험급여실 | 8 | 29 |
| 요양급여실 | 4 | 37,566 |
| 요양운영실 | 1 | 1,043 |
| 자격징수실 | 573 | 107,607,878 |
| 재정관리실 | 48 | 60 |
| 계 | 733 | 120,138,454 |

이를 제공받은 기관별, 요청사유별, 근거법률별로 분석하면, 제공받은 기관은 약 209개[179], 요청사유는 약 140여 개[180], 근거법률은 약 53개[181]였다.

178) 이 수치는 정확한 것은 아니다. 제공건수가 기록되지 않은 경우도 있었다. 이 경우 1건으로 간주했다.

179) 제공받은 기관 목록을 산출하는 과정에서 감사원, 감사원장과 같이 동일한 기관을 다르게 기록한 경우로 보이는 것들은 하나로 통일하였다. 그러나 광주지방법원 목포지

<표 2-74> 건강보험공단으로부터 건강보험자료를 제공받은 기관
(08년~09년 8월)

(주)부산솔로몬상호저축, (주)GS리테일, 감사원, 강동소방서, 강서경찰서장, 강원도지방경찰청, 강원지방병무청, 건강보험심사평가원, 경기일산경찰서장, 경기지방경찰청, 경기평택경찰서, 경남은행(주), 경인지방노동청 안양지청, 경찰청, 경찰청(사이버테러응대센터), 고양경찰서, 공군중앙관리단장, 공무원연금관리공단, 관세청, 관악소방서, 광주고등법원, 광주북부경찰서, 광주지방검찰청, 광주지방법원, 광주지방법원 목포지원, 광주지방법원 순천지원, 광주지방보훈청, 교육과학기술부, 구로경찰서, 국가보훈처, 국가인권위원회, 국가정보원, 국군제1363부대, 국군제7535부대, 국군제7539부대, 국립암센터, 국립포항검역소, 국무총리실, 국민고충처리위원회, 국민권익위원회, 국민연금공단 강남신사지사, 국민연금공단 파주지사, 국민연금관리공단, 국민연금관리공단 정읍지사장, 국민연금수원지사, 국방부, 국방부 보건정책팀, 국세청, 국회, 국회도서관, 국회예산정책처, 군의문사진상규명위원회, 군포시, 근로복지공단, 금융정보분석원, 급여관리실, 기술보증기금, 김제시, 네오건설, 노동부, 노원구청, 농협중앙회, 대검찰청, 대구동부경찰서, 대구지방법원, 대구지방보훈청, 대전광역시, 대전지방법원, 대전지방법원 가정지원, 대전지방법원 천안지원, 대전지방보훈청, 대전충남지방병무청, 대통령소속 군의문사 진상규명위원회 위원장, 대통령실, 대한주택공사, 도봉구, 마산세무서, 마포경찰서, 마포구, 무주군, 문화관광부, 민주평화통일자문회의사무처, 민주화운동관련자명예회복및보상심의위원회, 별정우체국연합회, 병무청, 보건복지가족부, 부산검찰청동부지청, 부산고등법원, 부산광역시, 부산지방검찰청, 부산지방법원, 부산지방법원 가정지원, 부산지방보훈청, 분당경찰서, 분당소방서, 삼성비자금의혹관련특별검사, 서대문경찰서, 서산경찰서, 서울동부지방법원, 서울가정법원, 서울강남경찰서, 서울강서경찰서, 서울고등법원, 서울구치소, 서울남부보훈지청, 서울남부지방검찰청, 서울남부지방법원, 서울동부지방법원, 서울동작경찰서장, 서울북부보훈지청, 서울북부지방검찰청, 서울북부지방법원, 서울서부지방검찰청
서울서부지방법원, 서울서초경찰서장, 서울세관, 서울시 중구, 서울용산경찰서장, 서울은평경찰서, 서울중앙지방검찰청, 서울중앙지방법원, 서울지방검찰청, 서울지방경찰청, 서울지방국세청, 서울지방법원, 서울지방변호사회, 서울지방병무청, 서울지방보훈청, 서울특별시, 서울시 성북소방서, 서울행정법원, 서초구, 서초소방서, 속초시, 수원보훈지청, 수원지방검찰청, 수원지방법원, 수원지방법원 성남지원, 수원지방법원 안산지원, 수원지방법원 평택지원, 순천경찰서, 식품의약품안전청, 신길1동, 신용보증기금, 안산시청, 안양경찰서장, 양천구, 연세대학교, 영등포구, 영등포소방서, 예금보험공사, 외교통상부, 용산구, 울산광역시 남구, 울산광역시 중구, 울산광역시지방경찰청, 울산보훈지청, 울산지방법원, 울주군, 원주경찰서, 육군제2672부대, 육군중앙경리단, 의정부지방검찰청 고양지청장, 의정부지방법원, 의정부지방법원 고양지원, 인천경기지방병무청, 인천광역시, 인천남동경찰서, 인천보훈지청, 인천보훈처, 인천연수경찰서, 인천지방검찰청, 인천지방검찰청 부천지청, 인천지방경찰청, 인천지방법원, 인천지방법원 부천지원, 일산경찰서, 전주지방법원, 정부공직자윤리위원회, 제주지방법원, 종로구청, 진실화해를위한과거사정리위원회, 질병관리본부장, 창원지방법원, 창원지법진주지원, 창원지법통영지원, 청주보훈지청, 청주지방법원 충주지원, 춘천지구배상심의회 위원장, 춘천지법, 통일부, 평창경찰서, 평택상호저축은행, 포항종합고용지원센터, 프로포즈성형외과, 하남시, 한국국제보건의료재단, 한국산업안전공단 산업안전보건연구원, 한국산업은행총재, 한국예탁결제원, 한국자산관리공사, 한국장학재단, 한국주택금융공사, 한국학술진흥재단, 한국희귀의약품센터소장, 해양경찰청, 행정안전부, 화성시

---

원 등과 같이 어떤 기관의 지원이 요청한 경우는 별개로 취급하였다. 제공받은 기관의 정확한 숫자는 개별적으로 확인하기도 힘들고, 기관 구분 기준에 따라 달라질 수도 있기 때문에 제공받은 기관의 개수는 대략적인 수치로 이해할 필요가 있다.

180) 요청 사유 역시 기록자에 따라 비슷한 사유를 여러 가지 형태로 기록했기 때문에(예를 들어, 수사, 수사협조, 살인사건 수사 등), 유사한 사유를 제거하기는 했지만, 요청 사유의 정확한 개수는 파악하기 힘들다.

181) 기록한 사람의 오류일 수도 있지만 요청 근거가 법률이 아닌 경우도 많았다. 예를 들어, 민원서류, 사실조회서, 업무처리요령 제3절 사업장관리, 장관표창, 정부포상지침 등이 근거로 제시된 경우도 있었다.

<표 2-75> 국민건강보험공단에 건강보험 자료를 요청한 사유

(08년~09년 8월)

| |
|---|
| 2008년도 암 조기검진사업 수행, 가출인 소재 수사, 감사 활용(감사청구조사팀), 강도사건 수사, 개인정보 불법이용 수사, 건강보험목적, 결핵환자 자료요청, 계약금반환 사건 심리, 고객만족도조사, 고등교육기관 졸업자 취업통계조사, 고엽제환자자녀 '07년도 총진료비, 고충민원, 공공근로사업 활용, 공무상재해, 공무원연금지급업무 활용, 공상 등 국가유공자 등록실태 적정성 2단계 감사, 공상공무원 등 국가유공자 등록실태 감사, 공적자금회수, 과태료 체납자 관리, 교정직 공무원 건강관리 사업, 구상채무자에 대한 재산조사 및 구상권 회수활동에 활용, 국가보안법위반내사, 국가보훈대상자 생활실태조사, 국가보훈대상자 의료지원업무, 국가유공자 국민임대아파트 지원 관련 활용, 국가유공자 및 유족 생활 실태 조사, 국가유공자 선정심사 참고자료, 국가유공자 수발서비스, 국가유공자 실태 파악, 국가유공자비해당결정처분취소, 국가유공자에대한 장기요양급여비용의 본인일부부담금지원, 국가채권자 관리, 국민기초생활보장수급자의 수급자격 및 급여의 적정성 확인, 국민연금지급적정성, 국보훈대상자의 생활실태조사, 군인 보건정책 수립, 근로기준법위반수사 활용, 근로복지사업안내 활용, 근로자 건강정책 관련 사업, 근로장려금, 글리벡환자진료 사실여부 확인, 금품사기수사, 기관감사, 기금 업무 관리, 기금 채무관계자 관리, 기술인력에 대한 이중취업 여부 확인, 기초노령연금수급자 선정및관리, 기초생활보장대상자확인, 노인장기요양보험제도 시행 관련 활용, 대불금회수, 대여금사건심리, 대체복무자 관리, 민원조사, 민주화운동보상, 범죄수사, 범죄수익은닉의규제및처벌등에관한법률 위반 여부를 규명하기 위한 심사분석업무에 필요함, 변사자 진료확인, 병역법위반, 병역업무활용, 보건복지부요양기관현지조사, 보건의료인력사후관리, 보상금 부정수취 확인, 보상심의활용, 보훈업무활용, 부당이득금반환관련 사건 심리, 비위면직자 취업제한, 사건 조사, 사건심리, 사망률및유병률비교, 사망사건 진상규명, 사실조회, 살인사건 수사, 서울시 관내 30대 여성 중 여성암(자궁경부암) 비대상자 검진 실시, 서울특별시 직원 건강증진사업에 활용, 세무조사 관련, 소유권말소등기사건심리, 손해배상(기), 수급체계개선, 실종사건 수사, 실태조사, 심사를 위한 장기요양기관 촉탁의 자료, 심의관련, 아이디 도용 수사, 업무수행, 연금지급활용, 외국인 건강관리 참고, 요양급여비용 심사 평가 관련 연구, 요양급여적정성평가업무활용, 요양기관 평가용 설문조사 대상발췌 요청, 요청기관의 건강보험 가입자 확인, 원인규명 역학조사, 위기가구 발굴, 위기가구발굴 및 보호지원, 유행성이하선염 환자의 요양급여내역, 육군본부제출, 응급의료비용 미수금 대불업무 활용, 의료기관 평가를 위한 환자만족도 설문조사용, 의료기관평가 설문자료, 의료법위반, 의료이용실태파악, 의료자원이용연구자료, 의료평가설문조사, 의문사확인, 이중가입자 조사, 이중취업 여부 확인, 인권유린 등 확인, 장려금지급, 장애인 차량 LPG 지원사업 활용, 재산형집행, 재판 활용, 저소득근로가구의 근로장려금 지원(근로장려세제시행), 전시가족급여 수령권자 구축 활용, 절도 사건 수사, 정보통신망이용촉진및정보보호등에관한법률위반 사건 수사, 정부포상 대상 확인, 정책과제수행, 제대군인 실태조사, 제대군인 전직지원 및 보훈정책 활용, 조사업무 활용, 종합전문요양기관인정평가관련자료, 주민등록번호 도용수사, 주민등록법위반 수사, 지방세 체납자 관리, 진료내역유무진위확인, 진료확인, 집시법위반 수사, 징병검사대상 확인, 채무부존재확인, 취업보호관련, 통계작성 및 학술연구, 퇴직공직자 취업제한, 특정경제가중수사활용, 특정병원특정청구코드 요양급여내역, 특정인에 대한 요양급여내역, 포상대상자 적격여부 확인, 폭력 사건 수사, 표창수여, 피보험자자격관리, 학자금대출미상환자 구상채권확인차, 학자금대출신청자 자격확인, 학자금융자, 현황파악, 형집행, 형집행 수사, 환자만족도조사, 휴업급여업무활용 |

<표 2-76> 국민건강보험공단에 건강보험 자료를 요청한 법적 근거
(08년~09년 8월)

| |
|---|
| 감사원법 제27조제1항, 제30조, 제50조의2, 제52조의2, 경찰관직무집행법 제8조, 고용보험법 제110조, 공공기관개인정보보호에관한법률 제10조, 제10조제2항, 제10조제3항제2호, 제16조, 제17조, 공무원연금법 제31조, 제85조, 공무원연금법 시행령 제41조, 공직자윤리법 제17조, 공직자윤리법 시행령 제35조, 국가기술자격법 제7조, 국가배상법 제11조, 국가보훈기본법 제17조, 제19조제1항, 국가유공자등 예우 및 지원에 관한 법률 제33조, 제82조의2, 제82조의6, 국가유공자 등 예우 및 지원에 관한 법률 시행령 제9조, 국가인권위원회법 제22조, 국가정보원법 제15조, 제16조, 국가채권관리법 시행규칙 제18조, 제23조, 국민건강보험법 제2조, 제83조, 국민건강증진법 제4조, 국민고충위원회의설치및운영에관한법률 제31조, 국민기초생활보장법 제22조, 제22조제4항, 국민연금법 제123조, 국세기본법 제41조, 제84조, 군사법원법 제44조, 군의문사진상규명등에관한특별법 제19조, 제19조제1항제5호, 근로자복지기본법 제10조, 금융실명거래및비밀보장에관한법률 제4조제1항, 민사소송법 제294조, 기술신용보증기금법 제50조, 기초노령연금법 제7조, 기초생활보장법 제22조, 노인장기요양보험법, 민사소송법 제223조, 제237조, 제294, 제344조, 민주화운동관련자 명예회복 및 보상등에 관한법률 제20조, 변호사법 제75조2, 별정우체국법 제19조, 병역법 제80조, 부패방지 및 국민권익위원회의 설치와 운영에 관한 법률 제82조, 산업안전보건법 제9조, 제14조의2, 산업재해보험보상법 제39조, 소방시설공사업법 제27조, 신용보증기금법 제43조, 암관리법 제9조, 예금자보호법 제21조, 응급의료에 관한 법률 제22조의2, 전염병 예방법 제2조, 제대군인 지원에 관한 법률 제8조, 제18조, 조세특례제한법 제100조, 제100조의13, 지방세법 제64조, 진실화해를위한과거사정리기본법 제3조, 제22조, 제23조 등, 질서위반행위규제법 제23조, 청소년의성보호에관한법률제42조, 통계법 제24조, 특정금융거래정보의보고및이용등에관한법률 제10조1항, 학술진흥 및 학자금대출 신용보증기금 등에 관한 법률 제55조 및 동법시행령 제22조, 한국장학재단설립에 관한법률 제50조, 형사소송법 제119조, 제199조, 제199조제2항, 제200조, 제272조, 제477조 |

위 표를 보면, 국민건강보험공단의 본래 업무를 수행하기 위한 목적 외로 공단이 보유하고 있는 건강보험 정보가 수시로 제공되고 있음을 확인할 수 있다. 이와 같은 정보제공은 정보주체의 동의하에 이루어지고 있다기보다는 법률에 근거해서 이루어지고 있었는데, 정보주체의 입장에서는 자신도 모르는 사이에 공단에 집적된 개인정보가 수많은 기관에 제공되고 있는 것이다. 국민건강보험공단에 정보제공 요청이 많은 것은 그만큼 공단이 방대한 정보를 집적하고 있기 때문이다. 한번 구축된 개인정보 데이터베이스는 애초 수집 목적 외의 다양한 목적을 위해 이용될 수 있음을 보여준다. 국민건강보험공단에의 정보 요청이 비록 공익적인 목적을 위한 것이라 하더라도, 이 정도로 광범위하게 애초 수집 목적 외로 개인정보가 제공된다면, 수집목적 내 이용이라는 개인정보 보호 원칙은 거의 의미가 없는 것이나 마찬가지다.

국민건강보험공단이 보유하고 있는 개인정보가 제3자에게 상시적으로 제공되고 있는 현실은 현행 「공공기관의 개인정보보호에 관한 법률」이 갖고 있는 문제를 보여준다. 즉, 동 법률은 제10조제1항에서 '보유기관의 장은 다른 법률에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거

나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보를 이용하게 하거나 제공하여서는 아니 된다'고 규정함으로써, 다른 법률에 따라 보유목적 외로 이용하거나 제3자에게 제공할 수 있도록 허용하고 있다. 제10조제3항에서는 '개인정보파일의 보유목적외의 목적으로 처리정보를 이용하게 하거나 제공할 수 있'는 예외 사유를 광범위하게 규정하고 있다. 특히, 제10조제3항제2호에서는 '공공기관개인정보보호심의위원회'(이하 심의위원회)의 심의를 거치면 보유목적 외로 이용하게 하거나 제공할 수 있도록 하고 있는데, 실제로 2009년 개최된 3차례의 심의위원회 회의에 상정된 3개의 안건 중 2개가 국민건강보험공단이 보유하고 있는 개인정보를 요구하는 것이어서, 이에 대한 요구가 높음을 짐작할 수 있다. 이러한 요구에 대해 심의위원회는 자료를 제공하도록 결정하였는데, 이는 OECD 개인정보보호 가이드라인 8원칙 중 하나인 목적 구체성(purpose specification)의 원칙과 이용제한(use limitation)의 원칙에 위배되는 것으로, 심의위원회의 결정이 자칫 보유목적 외 제3자 제공을 합리화하는 수단이 될 수 있음을 보여준다. 더구나 2009년에 진행된 심의위원회 회의는 서면심의로 이루어져 심의위원회의 심의가 충실하게 이루어진 것인지 의문이 제기될 수 있다.[182)]

<표 2-77> 2009년 공공기관개인정보보호심의위원회 회의일자 및 안건

| 차수 | 일자 | 안 건 |
|---|---|---|
| 11차 | '09.1.19 ~ 1.21 | <1건> 지방세체납처분을 위한 「국민건강보험 직장가입자 자격취득 및 상실정보 이용·제공」(요청기관: 지자체, 제공기관: 건보공단) |
| 12차 | '09.3.16 ~ 3.18 | <1건> 퇴직공직자 취업제한 위반여부 확인을 위한 「국민건강보험 직장가입자자격 취득 및 상실정보 이용·제공」(요청기관: 공직자윤리위원회, 제공기관: 건보공단) |
| 13차 | '09.4.15 ~ 4.17 | <1건> 공직자 쌀직불금 부당수령 여부 확인을 위한 「공무원연금관리공단 공무원 재직자정보 이용·제공」(요청기관: 행정안전부, 제공기관: 공무원연금관리공단) |

자료: '개인정보파일 대장 등 정보공개 청구'에 대한 행정안전부의 정보(부분공개) 결정통지서(2009.07.13) 중 제7차~13차 공공기관 개인정보보호심의위원회 회의 결과보고.

182) 공공기관개인정보보호심의위원회 및 제3자 제공과 관련된 본문의 사례에 대한 상세한 검토는 본 연구 제2장 제1절 참고.

이처럼 타 법률에 의해, 혹은 동법의 예외 조항에 의해 보유목적 외로 제3자 제공을 광범위하게 허용한다면, 이는 동법이 선언하고 있는 목적 구체성(purpose specification)의 원칙을 형해화할 우려가 있다(윤영민, 2004: 17). 국민건강보험공단을 비롯하여 공공기관이 보유하고 있는 개인정보의 목적 외 제3자 제공을 엄격하게 제한하도록 할 필요가 있으며, 불가피하게 개인정보가 제공될 경우에도 정보주체의 동의를 받거나 혹은 정보주체에게 통지하는 절차를 마련할 필요가 있다.[183]

### 3) 의료정보의 폐기

수집 목적이 완료된 경우 수집된 개인정보는 폐기하는 것이 원칙이다. 「공공기관의 개인정보보호에 관한 법률」 제10조의2[184] 역시 다른 법률에 근거가 없는 한, 보유목적을 달성한 정보는 폐기해야 함을 명시하고 있다. 그러나 취급기관의 개인정보 수집 근거를 제공하는 법률은 많은 반면, 이렇게 수집된 정보는 보존기간도 명시되어 있지 않고, 폐기되지 않고 있다.[185]

각 취급기관의 보유하고 있는 개인정보파일 중 보존기간이 영구 혹은 준영구로 되어 있는 개인정보파일은 다음과 같다.

---

183) 「공공기관의 개인정보보호에 관한 법률」 제10조제6항은 '보유기관의 장은 제3항 제2호 내지 제5호 및 제7호에 따라 보유목적 외의 목적으로 이용하게 하거나 제공하는 경우에는 그 이용 또는 제공의 법적 근거·목적 및 범위 등에 관하여 필요한 사항을 정보주체가 쉽게 확인할 수 있도록 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.'고 규정하고 있다. 그러나 필요한 경우가 아니면 관보나 공공기관 홈페이지를 방문하는 경우가 많지 않는다고 할 때, 관보나 홈페이지에 게재하는 것으로 얼마나 실효성 있게 정보주체가 인지하도록 할 수 있는지 의문이다. 또한, 동조 제1항에서 규정한, 다른 법률에 의해 제공되는 경우에도 정보주체가 이를 인지할 수 있도록 할 필요가 있다.

184) 제10조의2 (개인정보파일의 파기) ①보유기관의 장은 개인정보파일의 보유목적 달성 등 당해 개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체없이 파기하여야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

185) 개인건강정보 보호법안 전문가 간담회에서 서울대 김주한 교수는 취급기관에 진료정보의 제공 근거를 명시한 법안에 보유기간 및 이후 파기를 명시한 개정이 필요함을 지적하고 있다(김주한, 2008: 36).

<표 2-78> 취급기관이 영구 혹은 준영구적으로 보존하고 있는 개인정보파일

| 취급기관 | 개인정보파일 |
|---|---|
| 국민건강보험공단 | 자격상세내역, 급여정지, 주민번호/성명 변경, 직장가입자 보수월액내역, 지역 자동이체내역, 직장 자동이체내역, 압류내역, 관리의약품 투여자내역, 홈페이지 회원 가입업무, 건강위험평가(HRA) 내역, 중증암등록 내역 |
| 건강보험심사평가원 | 요양기관현황관리, 포털회원정보(탈퇴시 자동삭제) |
| 질병관리본부 | 집단설사환자 및 급성전염병환자정보 파일, 전염병 환자 명부, 결핵정보감시체계 결핵환자 신고화일, 예방접종기록, 국민건강영양조사 데이터 파일, 고혈압·당뇨병 환자 데이터 파일, 급성심정지· 급성 심근경색증·뇌졸중 심층조사 파일, 급성이완성마비감시, 연구과제 관리시스템 회원관리, 코호트 역학 정보파일 |

위 개인정보파일이 실제로 영구적으로 보존해야 할 필요가 있는 것인지, 본 연구에서 하나하나 검토하기는 힘들다. 이를 위해서는 각 업무와 개인정보파일에 대한 정확한 이해가 필요하기 때문이다. 하지만, 예를 들어 질병관리본부가 보유하고 있는 특정 질병 환자에 대한 개인정보파일의 경우, 해당 환자의 치료가 완료되었을 수도 있는데, 영구적으로 기록을 남겨둘 필요가 있는지 의문이다. 현재 영구, 혹은 준영구적으로 보존하도록 되어 있는 개인정보파일에 대해 보존기간이 적절한 것인지 의료 영역의 전문가들의 검토가 필요하다. 또한, 현재 취급기관에게 개인정보 정보를 제공하거나, 취급기관으로부터 개인정보를 제공받을 수 있도록 규정하고 있는 법률에서는 해당 정보의 적절한 보유기간, 그리고 보유목적 달성 시 폐기의무를 규정할 필요가 있다.

### 4) 의료정보의 관리

「공공기관의 개인정보보호에 관한 법률」 제9조는 개인정보가 분실·도난·누출·변조 또는 훼손되지 않도록 안전성 확보에 필요한 조치를 취하도록 의무화하고 있다. 또한, 「의료법」 제19조를 비롯한 보건의료 관련 법률에서는 비밀누설 금지의 의무를 규정하고 있다. 그러나 국민건강보험공단, 건강보험심사평가원 등을 통한 정보 유출이나 무단 열람의 문제는 거의 매해 언론이나 국정감사 등을 통해 불거지고 있다.

앞서 언급했다시피, 국민건강보험공단 등 취급기관은 방대한 개인정보를

보유하고 있다. 때문에 수시로 타 기관의 정보 요청 대상이 되기도 하지만, 불법적인 방법을 통한 정보 유출이나 혹은 내부 직원의 권한없는 열람의 유혹으로부터 자유로울 수 없다. 2008년 7월 22일 전현희 의원실의 보도자료에 따르면, 2007년 11월 복건복지부가 특별 감사를 실시하였는데, 조사결과 국민건강보험공단 직원들이 연예인 등 유명인사 정보를 호기심으로 열람하거나, 논문 작성을 위한 기초자료로 이용하거나, 지인을 찾기 위한 목적 등으로 무단 열람한 사례들이 적발되었다.

<표 2-79> 국민건강보험공단 직원의 개인정보 무단열람 사례

| 구분 | 복지부 조사결과 | 비고 |
|---|---|---|
| 대선후보 무단열람자(123명)의 여타 가입자 개인정보 무단열람 | - 연예인 등 유명인사 10명을 호기심으로 조회 (총 30건)<br>- 성금모금위해 공단직원의 가족관계 조회<br>- 대학원 사회복지실습일지 작성위해 사례관리 대상자의 당뇨사례관리 요구사정표 등 활용 | (10명) |
| 학위논문 작성목적 | - 지사가 관리하는 사업장 2개소 소속 579명의 건강검진 수검내역 및 개인급여내역 무단열람 (총 2,609건)<br>- 장애인 개인정보(성명, 주민번호, 장애유형, 주소 등)를 논문작성 위한 기초자료 및 설문 대상자 선정에 부당이용(총 5,199건) | 2명 |
| 국회 보건복지위원회 소속의원 개인정보 무단열람 | - 혹시 보험료를 문의하는 경우 답변할 명목<br>- 건강보장 30주년 기념행사 초청장 발송목적 등 | 3명 |
| 일반가입자 개인정보 무단열람 (임의로 10% 무작위 추출) | - 사적 호기심으로 가입자 정보 조회<br>- 건강보장 30주년 기념행사 초청장 발송목적 (16명 조회)<br>- 자신의 군대후배와 동명이인 검색하기<br>- 회의참석자의 분실물 반환을 위해<br>- 상해요인 폭행사건과 관련하여 가해자의 이름과 성씨가 다른 가입자를 조회<br>- 공단이사장 개인정보를 사전에 열람(카드수납 유선취소)<br>- 성명입력 방식으로 개인정보 조회하면서 조건 설정하지 않아 전국의 동명이인 가입자가 임의로 조회되기도 함 | (2명) |

자료: 전현희(2008).

2008년 이후에도 국민건강보험공단 내부 직원에 의한 무단/불법 열람 및 개인정보 유출 건수는 적지 않다. 변웅전 의원실의 보도자료에 따르면, 2008년부터 2009년 9월까지 국민건강보험공단 직원 33명이 개인정보 관련으로 징계를 받았는데, 이 중 9명은 개인정보의 불법 유출, 24명은 무단 열람이 이유였다(변웅전, 2009).[186] 여전히 지인의 요청이나 학위논문 작성 등을 위해 개인정보를 무단 열람한 사례가 있었다. 또한, 가입자의 개인정보를 불법으로 유출해 이를 알선 유인하거나, 장기요양기관에 제공한 사례도 있었다.

<표 2-80> 최근 2년간 건강보험공단 직원, 개인정보 관련 징계현황

| 연번 | 직급 | 성명 | 징계일자 | 징계유형 | 징계상세내용 |
|---|---|---|---|---|---|
| 1 | 3급 | 이○○ | 2008.01.01 | 감봉1월 | 개인정보관련 |
| 2 | 4급 | 조○○ | 2008.01.01 | 정직2월 | 개인정보관련 |
| 3 | 4급 | 김○○ | 2008.02.03 | 견책 | 개인정보 무단열람 |
| 4 | 3급 | 오○○ | 2008.03.07 | 해임 | 개인정보 무단열람 및 이용 |
| 5 | 5급 | 김○○ | 2008.03.17 | 정직1월 | 지인의 부탁으로 가입자 주소 유출 |
| 6 | 4급 | 김○○ | 2008.04.10 | 견책 | 업무목적외 개인정보 불법열람 |
| 7 | 4급 | 김○○ | 2008.04.10 | 견책 | 학위논문 작성목적 개인정보 불법열람 |
| 8 | 4급 | 고○○ | 2008.04.10 | 견책 | 업무목적외 개인정보 불법열람 |
| 9 | 3급 | 황○○ | 2008.04.10 | 감봉1월 | 학위논문 작성목적 개인정보 불법열람 |
| 10 | 4급 | 공○○ | 2008.04.10 | 견책 | 업무목적외 개인정보 불법열람 |
| 11 | 4급 | 김○○ | 2008.04.10 | 견책 | 업무목적외 개인정보 불법열람 |
| 12 | 4급 | 정○○ | 2008.06.05 | 정직2월 | 개인정보 무단열람 및 유출 |
| 13 | 5급 | 하○○ | 2008.07.28 | 감봉3월 | 개인정보 무단열람 의뢰 |
| 14 | 4급 | 최○○ | 2008.09.26 | 감봉1월 | 직원 개인정보 무단열람 |
| 15 | 4급 | 문○○ | 2008.11.14 | 감봉1월 | 지인의 개인정보 무단열람 |

186) 그런데, 변웅전 의원의 보도자료가 나오기 전 나흘 전인 2009년 10월 8일, 심재철 의원은 보도자료를 통해 “2008년에는 22명의 직원이 개인정보 무단열람 및 유출, 업무목적외 개인정보 불법열람 등의 이유로 징계를 받았으며, 2009년에는 8명의 직원이 개인정보 불법열람 및 장기요양기관에 개인자료 제공, 업무목적 외 동료직원 개인정보 불법조회, 수급자 개인정보 유출 및 알선유인 등의 불법로 인해 징계를 받았다.”고 밝혔다(심재철, 2009). 징계수치가 변웅전 의원의 것과 조금 다르게 나타난다. 또한, 국민건강보험공단이 박은수 의원실에 제공한 자료에 따르면, 무단열람 적발건수는 2008년에 4명(4건), 2009년 3월까지 3명(3건)이고, 개인정보가 외부로 유출된 건수는 2007년 1건, 2008년 4건, 2009년 5건이다. 의원실에서 실수를 한 것이 아니라면, 국민건강보험공단에서 수치를 다르게 제공한 것인데, 이는 구체적인 사례를 어떻게 분류하느냐—즉, 개인정보 유출, 무단 열람, 불법 열람 등—에 따라 달라진 것으로 보인다.

| | | | | | |
|---|---|---|---|---|---|
| 16 | 5급 | 김○○ | 2008.12.04 | 감봉1월 | 직원 개인정보 무단 열람 |
| 17 | 5급 | 김○○ | 2008.12.04 | 감봉1월 | 개인정보(내부직원)무단열람 |
| 18 | 4급 | 조○○ | 2008.12.09 | 감봉1월 | 동료직원개인정보무단열람 |
| 19 | 2급 | 변○○ | 2008.12.12 | 파면 | 지인에게 개인정보 불법유출 등 |
| 20 | 4급 | 조○○ | 2009.05.01 | 정직3월 | 개인정보 무단열람 및 유출 |
| 21 | 4급 | 윤○○ | 2009.05.21 | 정직3월 | 개인정보 불법열람 및 장기요양기관에 개인자료 제공 |
| 22 | 4급 | 전○○ | 2009.06.01 | 감봉1월 | 개인정보 불법열람 |
| 23 | 4급 | 이○○ | 2009.06.01 | 견책 | 동료직원 개인정보 불법조회 |
| 24 | 5급 | 박○○ | 2009.06.01 | 파면 | 수급자 개인정보 유출 및 알선유인 |
| 25 | 5급 | 백○○ | 2009.06.26 | 정직3월 | 직원의무위반 및 개인정보 무단열람 |
| 26 | 6급 | 백○○ | 2009.06.29 | 견책 | 동료직원 개인정보 열람 |
| 27 | 4급 | 김○○ | 2009.06.30 | 견책 | 업무목적 외 동료직원 개인정보 열람 |
| 28 | 4급 | 오○○ | 2009.08.01 | 감봉3월 | 수급자개인정보무단열람 |
| 29 | 4급 | 이○○ | 2009.08.01 | 감봉1월 | 수급자 개인정보 유출 |
| 30 | 6급 | 장○○ | 2009.08.05 | 정직3월 | 장기요양시설에 수급자개인정보 유출 및 알선 |
| 31 | 2급 | 박○○ | 2009.08.20 | 감봉3월 | 수급자 개인정보 무단열람 |
| 32 | 5급 | 임○○ | 2009.09.01 | 정직1월 | 가입자 개인정보 무단열람 및 유출 |
| 33 | 4급 | 이○○ | 2009.09.04 | 감봉2월 | 동료직원개인정보 무단열람 |

자료: 변웅전(2009).

2009 국정감사에서 박은수 의원실에 제출된 자료에 따르면, 건강보험심사평가원의 경우 2008년 무단열람 건수가 10건(조회건수, 열람자는 3명)이며, 개인정보가 외부로 유출된 건수는 없다고 하였다. 질병관리본부는 개인정보 불법열람 및 유출 건수가 전혀 없다고 밝혔다.

국민건강보험공단은 불법열람을 막기 위해 2008년에는 매월 전 직원의 2%를 대상으로 수작업으로 정기점검을 실시[187]하였으며, 2008년 1월부터 9월까지 '개인정보관리시스템'을 개발하여, 12월까지 시험가동을 거친 후, 2009년 1월 1일부터 공공기관 최초로 시스템을 가동하고 있다고 밝혔다. 그러나 2009년에도 여전히 국민건강보험공단 내에서 개인정보의 무단 열람이나 유출 사건이 발생한 것으로 보아, 무단 열람 자체를 시스템적으로 방지하

187) 국민건강보험공단은 개인정보 열람내역 모니터링을 2008년 1월부터 시행했다고 밝혔다.

지는 못하는 것으로 판단된다. 건강보험심사평가원은 보건복지가족부 통합 개인정보 상시 모니터링 시스템을 2009년 5월부터 9월 현재까지 구축 중이라고 밝혔으며, 질병관리본부 역시 현재 구축중이라고 답변하였다.

전현희 의원이 주최한 <개인건강정보 보호법안 전문가 간담회> 자료집에 포함된 '건강보험심사평가원 의견서'에 따르면, 건강보험심사평가원은 "취급기관 일부 직원의 호기심 또는 사적용도에 의한 조회 및 유출은 개인의 도덕적 해이로 기인하는 바가 크며 법령미비의 문제로 보기는 어려움"이라고 평가했다. 그러나 매해 이와 같은 문제가 반복되고 있는 것에 대해서 직원들의 '도덕적 해이'에만 책임을 묻는다면 문제를 해결하기 어려울 것이다. 역으로 이는 법적·기술적인 대책의 한계를 토로한 것으로, 방대한 개인정보 보유 자체가 유출의 위험성을 가지고 있을 수밖에 없음을 나타낸다. 정당한 권한을 가진 사람이 목적 내의 용도로만 이용할 수 있도록 시스템을 구축할 필요가 있으며, 보유하고 있는 개인정보를 최소화할 수 있는 방안을 모색할 필요가 있다.

### 5) 정보주체의 열람 및 정정·삭제 청구권

취급기관에서 보유하고 있는 개인정보는 「공공기관의 개인정보 보호에 관한 법률」 제12조 및 제14조에 따라, 열람·정정·삭제청구를 할 수 있다.[188] 그러나 열람의 범위는 '개인정보파일대장에 기재된 범위' 내에서인데, 개인정보파일대장에 타 기관에 제공되는 정보의 종류 및 제공대상 기관 등이 명시되어 있기는 하지만, 각 정보주체별로 제3자 제공 내역을 열람할 수 있는지는 명확하지 않다.

앞서 본 바와 같이 취급기관이 보유하고 있는 개인정보는 다수의 제3자에게 제공되고 있었다. 따라서 자기정보의 제3자 제공 내역에 대해 정보주체가 결정권을 행사할 수 있기 위해서는 「공공기관의 개인정보 보호에 관한 법률」 혹은 의료관련 법률의 개정을 통해 정보주체가 제3자 제공 내역을 열람할 수 있도록 명확하게 규정될 필요가 있다.

---

188) 제12조 (처리정보의 열람) ①정보주체는 개인정보파일대장에 기재된 범위안에서 문서로 본인에 관한 처리정보의 열람(문서에 의한 사본의 수령을 포함한다. 이하 같다)을 보유기관의 장에게 청구할 수 있다.

제14조 (처리정보의 정정 및 삭제 등) ①제12조에 따라 본인의 처리정보를 열람한 정보주체는 보유기관(다른 기관으로부터 처리정보를 제공받아 보유하는 기관을 제외한다. 이하 이 조에서 같다)의 장에게 문서로 당해 처리정보의 정정 또는 삭제를 청구할 수 있다. 다만, 다른 법률에 당해 처리정보가 수집대상으로 명시되어 있는 경우에는 그 삭제를 청구할 수 없다.

## 5. 소결

개인 의료정보는 가장 민감한 개인정보 중 하나로서 엄격한 보호가 필요함에도 불구하고, 보건의료 관련 법률에서는 아직 개인정보 보호원칙을 체계적으로 반영하지 못하고 있다. 아직 보건의료 영역에서 보호해야 할 '개인정보'의 개념과 보호범위조차 명확하게 정의되어 있지 못한 상황이다. 본 연구에서는 병원, 약국, 보건소 등 의료정보를 생성하는 '생성기관'과 국민건강보험공단, 건강보험심사평가원 등 생성기관으로부터 정보를 제공받아 건강보험 업무 등을 위해 활용하는 '취급기관'으로 나우어 의료정보의 수집, 유통 실태를 분석하였다.

생성기관에서의 개인정보 수집, 유통실태 조사를 통해 파악된 문제점과 개선방안은 다음과 같다.

첫째, 일부 병원의 경우 결혼여부, 학력, 종교 등 민감한 개인정보도 수집하고 있는 반면, 개인정보의 수집이나 제3자 제공과 관련한 동의나 고지 체계는 제대로 갖춰져 있지 않았다.

둘째, 병원에서 보유하고 있는 의료정보는 타 병원, 약국, 국민건강보험공단 등 취급기관, 경찰이나 법원 등 공공기관에 제공된다. 의료정보의 제3자 제공과 관련한 근거와 절차를 「의료법」에서 구체적이고 명확하게 규정할 필요가 있다.

셋째, 「의료법」에서는 진료기록부의 보존 기간을 10년으로 규정하고 있으나, 상당수의 병원에서 의료기록을 사실상 준 영구적으로 보존하고 있는 것으로 파악된다. 환자의 치료나 건강을 위해 꼭 필요한 경우가 아니라면, 보존기간 이후에는 의료기록을 파기하도록 법에서 명시할 필요가 있다.

넷째, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 따른 개인정보 취급방침이나 「신용정보의 이용 및 보호에 관한 법률」에 따른 신용정보활용체제와 달리 보건의료 관련 법률에서는 규정이 없어, 개인 의료정보의 수집, 제3자 제공, 보호정책, 정보주체의 권리 등에 대한 개별 의료기관의 정책에 대해 파악하기 힘들다. 개별 의료기관마다 개인 의료정보의 보호와 보안을 위한 대책을 담은 지침을 마련하고, 그 주요 내용에 대해 공개하도록 해야 한다.

다섯째, 의료정보의 유출이나 무단 열람 등의 전반적인 실태는 파악하기 힘드나, 언론보도나 설문조사 결과에 의하면 의료정보에 대한 무단 열람 사례도 적지 않을 것으로 짐작된다. 또한, 병원 정보화에 따라 전자의무기록

(EMR)과 같은 새로운 시스템이 도입되고 있음에도 불구하고, 적절한 정보보안 시스템 구축은 미흡한 것으로 보인다. 의료기관의 정보보안에 대한 정확한 실태조사와 함께, 보건복지가족부는 개인정보 보호와 보안을 위한 지침을 제시할 필요가 있다.

여섯째, 「의료법」 등에서 환자의 열람권을 규정하고는 있으나, 정정·삭제권은 규정하고 있지 않다. 열람권의 경우에도, 자신의 의료기록에 대한 열람뿐만 아니라, 열람 내역 및 제3자 제공 내역에 대한 열람권을 포함할 필요가 있다.

국민건강보험공단 등 취급기관에서의 개인정보 수집, 유통실태는 보다 심각하다.

첫째, 취급기관에는 각 의료기관에서 생성된 의료정보가 집적된다. 국민건강보험공단의 경우에는 의료정보뿐만 아니라, 주민등록정보, 사업자등록자료, 출입국 기록, 장애인자료, 토지 및 자동차 자료, 연금자료 등 개인의 인적사항 및 재산 등에 대한 방대한 기록을 보유하고 있다. 취급기관이 보유하고 있는 개인정보는 정보주체의 동의를 받고 직접 수집한 것이라기보다는 법에 근거하여 타 기관으로부터 제공받는 경우가 대부분이다. 그런데 취급기관이 개인정보를 제공받아 보유할 수 있는 법적 근거가 포괄적인 경우가 많다. 이는 자칫 과도한 개인정보의 수집을 초래할 수 있는데, 관련 법률에서 각 취급기관이 업무 수행을 위해 수집할 수 있는 개인정보의 범위를 엄격하게 규정할 필요가 있다.

둘째, 취급기관이 보유하고 있는 개인정보는 시스템 연계를 통해, 혹은 요청에 의해 타 기관에 제공된다. 특히, 국민건강보험공단의 경우 2008년부터 2년 동안, 공단 내 각 부서에서 총 733회, 1억 건이 넘는 개인정보를 단지 요청에 의해 타 기관에 제공한 것으로 나타났다. 즉, 공단의 본래 업무를 수행하기 위한 목적 외로 공단이 보유하고 있는 건강보험 정보가 수시로 제공되고 있음을 확인할 수 있었다. 이렇게 광범위하게 애초 수집 목적 외로 개인정보가 제공된다면, 수집목적 내 이용이라는 개인정보 보호 원칙은 거의 의미가 없게 된다. 국민건강보험공단을 포함하여 취급기관이 보유하고 있는 개인정보의 제3자 제공을 엄격하게 제한할 필요가 있으며, 개인정보가 제공될 경우 정보주체의 동의 혹은 최소한의 통지 절차가 필요하다.

셋째, 취급기관이 보유하고 있는 개인정보파일 중에서도 영구, 혹은 준영구적으로 보존되는 것들이 다수 존재했다. 적절한 보유기간에 대한 전문가들의 검토가 필요하며, 보유목적 달성시 폐기의무를 의료 관련 법률에서 세밀하게

규정할 필요가 있다.

넷째, 국민건강보험공단, 건강보험심사평가원 등을 통한 정보 유출이나 무단 열람의 문제는 거의 매해 언론이나 국정감사 등을 통해 불거지고 있다. 이러한 무단 열람의 문제는 국민건강보험공단이 모니터링 시스템을 가동한 이후에도 발생하고 있다. 직원들에 대한 교육, 정보유출이나 무단열람에 대한 중징계 등의 조치와 함께, 취급기관 자체가 보유하고 있는 개인정보 자체를 최소한으로 제한할 필요가 있다.

다섯째, 취급기관의 경우 「공공기관의 개인정보 보호에 관한 법률」에 따라 정보주체의 열람 및 정정·삭제 청구권을 보장하고 있지만, 정보주체가 자기정보에 대한 제3자 제공 내역을 열람할 수 있도록 법에서 명확하게 규정할 필요가 있다.

의료정보는 가장 민감한 개인정보임에도 불구하고, 의료관련 법률이 개인정보 보호원칙을 제대로 반영하지 못하고 있는 것은 심각한 문제이다. 개인의료정보의 보호를 위한 법안 마련이 시급해 보인다. 이에는 의료정보의 열람 내역이나 제3자 제공 내역에 대한 정보주체의 열람권이 반드시 보장될 필요가 있다. 왜냐하면, 보건의료 영역에서는 생성기관에서 보유하고 있는 의료정보가 다수의 취급기관에 집적되고, 또 이렇게 집적된 개인정보가 타 공공기관을 통해 공유되고 있기 때문이다. 이런 상황에서 개인정보자기결정권은 유명무실해질 수밖에 없다.

# 제6절 교육 영역(NEIS 도입 및 통합)

교육기관의 개인정보 수집·유통 실태 분석은 주로 NEIS 도입 및 통합과 관련된 논의를 중심으로 살펴보았다.

## 1. 개요

교육행정정보시스템(National Education Information System, 이하 NEIS)은 기존에 학교단위로 구축되어 있던 정보시스템을 개편하여 교육인적자원부, 교육청, 등 모든 교육행정기관과 초·중등학교를 인터넷으로 연결하여 교육행정 업무를 전자적으로 연계·처리할 수 있도록 구축한 시스템을 의미한다. NEIS 도입 당시 교육인적자원부(이하 교육부)로 대표되는 정책추진세력은 이를 통해 결국 교원, 학생, 학부모의 교육정보에 대한 요구를 충족시킬 수 있을 것으로 보았다. 즉, 대국민 교육행정서비스를 개선하고, 학부모의 교육에 대한 관심과 참여를 확대하며 교육행정 업무의 효율성을 향상시키고 교원들이 교육 본연의 임무에 충실한 환경을 조성할 수 있다고 보았던 것이다.

NEIS는 각급 학교 - 시도 및 지방 교육청 - 교육부 - 학부모를 연계하는 인터넷 기반의 교육행정 시스템으로서 2001년 전자정부 11대 사업의 하나로 추진되었다. 이러한 NEIS의 추진목적으로는 ① 초고속 인터넷망과 정보통신기술의 발전에 따라 기존의 문서위주의 행정을 디지털 행정으로 전환하여 선진 교육행정서비스를 제공할 필요성 증가, ② 시·도교육청 내·외부의 각종 정보시스템간 호환성 문제로 자료의 효율적 관리 및 이용상 어려움, ③ 2001년 현재 전체 공공기관 보안사고 중 70%가 각급학교에서 발생하는 등 기존의 학교 시스템(C/S, SA)의 보안상 문제점을 해결할 필요성, ④ 시·도교육청별 업무단위 별 프로그램의 중복 개발 및 시스템 관리 비용 과다 소요 등에 따라 효율적인 시스템 관리 및 예산 절감의 필요성, ⑤ 교육행정의 효율화를 통한 학교현장의 업무경감 방안 추진으로 학생중심의 수준별 교육과정 도입 등에 따른 교사의 연구시간 확보 지원의 필요성, ⑥ 21세기 국가 경쟁력 확보 및 국민 편익 증진을 위한 범정부적 전자정부 구현 활동의 확대 강화 및 NEIS를 통한 교사의 정보화 역량제고 등이 제시되었다.

NEIS는 교육인적자원부, 16개 시·도 교육청, 180개 지방교육청, 그리고 전국의 1만 여개 초·중등학교를 인터넷으로 연결하는 통합 정보관리 시스템

이다. 일반교육행정 22개 영역, 학교행정 5개 영역 등 27개 업무를 2003년 3월에 개발 완료하였다. 원안대로라면, 이 시스템은 기존의 교무·학사행정은 물론, 인사, 회계, 물품, 시설 등 단위학교의 업무사항과 교육청을 비롯한 교육행정기관의 연계업무를 총망라하는 효과적인 시스템으로 보였다. 그러나 이 사업은 전자주민카드 도입사업과 마찬가지로 인권침해 가능성으로 인하여 정보인권단체의 반대에 직면하여 시행에 차질을 빚었으며, 개인정보 보호 및 정보인권의 중요성을 제기하는 계기를 마련해주었다.[189]

NEIS는 추진과정에서 개인정보 유출 가능성이 제기되면서 전교조 등 인권단체들이 반대하자 정부는 2004년 3월 정부는 인권침해 소지가 제기된 교무·학사, 입(진)학, 보건 업무를 새로 구축하는 방침을 확정하고, 2006년 2월에 개발을 완료하여 2006년 3월 전면 시행에 들어갔다.[190] NEIS에 대한 현장 이용자의 의견수렴을 통한 안정화 및 기능개선 작업과 함께 평생교육시설 학력인정학교를 위한 교무업무 시스템 응용 S/W의 추가개발사업(2006. 7~2007. 3)을 비롯하여 민원인 및 특수학교 시각장애 교사를 위한 NEIS 추가개발(2006.10)을 완료하고, 디지털 교육재정사업(2005~2008)을 추진하여 2007년 말 현재 시범사업을 하고 있으며, Home-Edu 민원서비스를 개시하였다.

NEIS 성과에 대하여는 교육인적자원부와 교육학술정보원이 매년 집계하는 통계자료를 바탕으로 산출한 각종 편익을 교육정보화백서 등을 통하여 발표하고 있다. 그러나 시스템 사용자 입장에서 NEIS 성과에 대한 인식 및 평가가 어떤지는 또 다른 문제이다(송희준 외, 2008). 교육행정정보화사업이 원래 의도한 목표를 충분히 달성하였는가에 대해서는 다양한 반응이 나오고 있다. 특히 시스템의 가장 큰 사용자인 초중등학교 현직교사들의 반응에 대한 체계적인 조사 및 분석은 이루어지지 못하고 있다. 국내의 NEIS 관련 연구 대부분은 NEIS 개발 및 보급과정에서 발생한 갈등(강창동, 2005; 나태준,

189) 물론 정책기획위원회(2008)는 NEIS 도입사업을 교육부정책 중 가장 오랜 시간동안 표류한 사업 중 하나라고 파악하고 있다. 하연섭 외(2006)는 NEIS의 시행을 둘러싼 표면적인 갈등의 내면에 정책의 시행측과 반대측 양 집단이 정책내용에 관해 인식하고 있는 나름의 틀(frame)이 존재하며, 그 틀은 철저하게 집단이 중요하게 여기는 가치와 태도에 근거하여 형성되는 것이고, 궁극적으로는 이러한 인식차이에 대한 조정과 소통구조의 제도적 불비로 인해 갈등이 교착상태에 빠졌다고 본다.

190) NEIS를 전국단위로 운영하려던 계획이 반발에 부딪쳐 3개 영역을 고등학교는 학교별로, 초·중학교는 15개 학교들을 권역별로 묶어 관리하게 되어 발생한 예산부족 문제를 해결하기 위하여 교육인적자원부는 개발비용이 상대적으로 저렴한 오픈 소프트웨어 시스템을 도입하였다. Linux 기반의 시스템은 정보보안 문제없이 잘 가동 중이다(송희준 외, 2008).

2006; 송광용・김수윤, 2004; 박상준・임정빈, 2004; 하연섭 외, 2006)과 이 과정에서 상호작용하는 집단간 역학관계 또는 네트워크(김덕근, 2006a; 2006b)에 대한 사례 연구를 중심으로 이루어졌다. NEIS 성과를 인과관계모형으로 설명한 연구(송희준 외, 2008)가 있기는 하나, NEIS를 전면적으로 도입할 만큼 충분한 검토가 이루어지지는 않았다. 하지만 교육과학기술부는 2009년 NEIS 사용자들의 활용에 대한 체계적인 검토 없이 전격적으로 NEIS 통합을 시도하여 논란이 되고 있다.

NEIS의 법적 근거로는 「교육기본법」[법률 제8915호, 2008.3.21, 일부개정]과 「초・중등교육법」, 「학교보건법」, 그리고 「교육정보시스템의 운영 등에 관한 규칙」 등을 들 수 있다. 우선 「교육기본법」 제23조의2(학교 및 교육행정기관업무의 전자화)는 “국가와 지방자치단체는 학교 및 교육행정기관의 업무를 전자적으로 처리할 수 있도록 필요한 시책을 마련하여야 한다”고 하여 법적근거를 두었고, 「교육기본법」 제23조의3(학생정보의 보호원칙) 역시 학교생활기록부 등의 학생정보가 교육적 목적으로 수집・처리・이용 및 관리되어야 하는 원칙과 법률이 정하는 경우를 제외하고는 당해 학생(학생이 미성년자인 경우에는 학생 및 학생의 부모 등 보호자)의 동의 없이 제3자에게 제공되어서는 아니 된다는 원칙을 천명하고 있다.

그리고 「초・중등교육법」은 제25조(학교생활기록)에서 학교의 장은 학생의 학업성취도 및 인성 등을 종합적으로 관찰・평가하여 학생지도 및 상급학교의 학생선발에 활용할 수 있는 인적사항, 학적사항, 출결상황, 자격증 및 인증취득상황, 교과학습발달상황, 행동특성 및 종합의견, 그 밖에 교육목적에 필요한 범위 안에서 교육과학기술부령이 정하는 사항의 자료를 교육과학기술부령이 정하는 기준에 따라 작성・관리하여야 하고, 이 자료를 제30조의4의 규정에 의한 교육정보시스템으로 작성・관리하여야 한다고 규정하고 있다. 그리고 교육과학기술부 장관 및 교육감이 학교 및 교육행정기관의 업무를 전자적으로 처리할 수 있도록 교육정보시스템을 구축・운영할 수 있다고 하면서(제30조의4), 교육과학기술부 장관 및 교육감은 소관 업무의 전부 또는 일부를 정보시스템을 이용하여 처리하여야 한다고 규정하고 있다(제30조의5).

「초・중등교육법」
제30조의4 (교육정보시스템의 구축・운영 등) ①교육과학기술부장관 및 교육감은 학교 및 교육행정기관의 업무를 전자적으로 처리할 수 있도록 교육정보시스템(이하 "정보시스템"이라 한다)을 구축・운영할 수 있다.
②교육과학기술부장관 및 교육감은 정보시스템의 운영 및 지원을 위하여 정보

시스템운영센터를 설치·운영하거나 정보시스템의 효율적 운영을 위하여 필요하다고 인정되는 경우 정보시스템의 운영 및 지원업무를 교육의 정보화를 지원하는 법인 또는 기관에게 위탁할 수 있다.
③제1항의 규정에 의한 정보시스템의 구축·운영·접속방법 및 제2항의 규정에 의한 정보시스템운영센터의 설치·운영 등에 관하여 필요한 사항은 교육과학기술부령으로 정한다.

제30조의6 (학생 관련 자료제공의 제한) ①학교의 장은 제25조의 규정에 의한 학교생활기록 및 「학교보건법」 제7조의3의 규정에 의한 건강검사에 관한 자료를 당해 학생(학생이 미성년자인 경우에는 학생 및 학생의 부모 등 보호자)의 동의 없이 제3자에게 제공하여서는 아니 된다. 다만, 다음 각호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 학교에 대한 감독·감사의 권한을 가진 행정기관이 그 업무를 처리하기 위하여 필요한 경우
2. 제25조의 규정에 의한 학교생활기록을 상급학교의 학생선발에 이용하기 위하여 제공하는 경우
3. 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우
4. 범죄의 수사와 공소의 제기 및 유지에 필요한 경우
5. 법원의 재판업무수행을 위하여 필요한 경우
6. 그 밖에 관계법률의 규정에 의하여 제공하는 경우
②학교의 장은 제1항 단서의 규정에 의하여 자료를 제3자에게 제공하는 때에는 당해 자료를 제공받은 자에 대하여 사용목적·사용방법 그 밖에 필요한 사항에 대하여 제한을 하거나 당해 자료의 안전성 확보를 위하여 필요한 조치를 강구하도록 요청할 수 있다.
③제1항의 규정에 의하여 자료를 제공받은 자는 그 본래의 목적 외의 용도로 이를 이용하여서는 아니된다.

「학교보건법」
제7조의3 (건강검사기록) ① 학교의 장은 제7조에 따라 건강검사를 하였을 때에는 그 결과를 교육과학기술부령으로 정하는 기준에 따라 작성·관리하여야 한다.
② 학교의 장이 제1항에 따라 건강검사 결과를 작성·관리할 때에 「초·중등교육법」 제30조의4에 따른 교육정보시스템을 이용하여 처리하여야 하는 자료는 다음과 같다.
1. 인적사항
2. 신체의 발달상황 및 능력
3. 그 밖에 교육목적을 이루기 위하여 필요한 범위에서 교육과학기술부령으로 정하는 사항
③ 학교의 장은 소속 학교의 학생이 전출하거나 고등학교까지의 상급학교에

진학할 때에는 그 학교의 장에게 제1항에 따른 자료를 넘겨 주어야 한다.

특히 「교육정보시스템의 운영 등에 관한 규칙」은 총 12개조에 「초·중등교육법」 제30조의4의 규정에 의하여 교육정보시스템의 구축·운영·접속방법 및 정보시스템운영센터의 설치·운영 등에 관하여 필요한 사항을 규정하고 있으며, 2002. 12. 20일에 제정된 「교육행정정보시스템 운영 규정」(교육과학기술부훈령)에 이에 대한 구체적인 내용이 들어있다. 「교육행정정보시스템 운영 규정」의 주요 내용을 살펴보면 다음과 같다.

1) 교육과학기술부 장관은 시·도교육청의 실정에 맞게 기존의 업무체계를 행정시스템의 활용을 기반으로 하는 업무체계로 대체하여 구현하도록 한다(제6조).

2) 시·도교육감은 행정시스템을 활용하기 위한 제반 시설 및 설비를 확충하고 적정 성능을 유지할 수 있도록 관리하고 활용을 위한 사용자 연수계획을 수립하여 실시하도록 한다(제7조 및 제8조).

3) 시·도교육감과 시스템 적용기관의 장은 행정시스템 운영계획을 수립·시행하도록 하되, 동 계획에는 시스템 관리자 및 사용자 지정, 권한 설정, 각종 장부 정비계획, 보안 및 전산자료의 확정 등에 관한 사항이 포함되도록 한다(제10조).

4) 행정시스템의 관리 운영을 위하여 교육과학기술부와 시·도교육청에 각각 총괄센타와 지역센타를 설치하고, 교육과학기술부 장관은 총괄센타를 한국교육학술정보원장에게 위탁하여 관리·운영하도록 한다(제11조).

5) 행정시스템 적용기관은 「초·중등교육법」 제2조의 각 호에서 정한 학교, 교육행정기관 및 각 센타의 장이 지정한 기관으로 하고, 각 센타의 장은 행정시스템의 구축 정도에 따라 적용시기와 범위 등을 조정할 수 있도록 한다(제12조).

6) 행정시스템에서 생성된 전산자료는 적용기관 간 제증명 발급등을 위하여 공동활용함을 원칙으로 하고, 시스템을 활용한 민원서류 교부기관의 범위는 각 센타의 장이 정하되 인터넷을 이용한 민원 신청·발급은 각 시·도교육감이 담당하며, 제증명발급수수료는 교부기관의 수입으로 한다(제13조 및 제14조).

7) 학교생활기록부 등 전산자료에 대하여 보호자에게 제공할 수 있도록 한다(제15조).

8) 각 센타의 장은 행정시스템의 보안 및 정보보호를 위하여 보안담당자를

지정·운영하고, 행정시스템의 설치공간을 마련하여 통제구역으로 설정하여, 정기적인 자체 보안점검 등을 통해 시스템 및 전산자료의 보안관리에 힘쓰도록 한다(제16조 및 제17조).

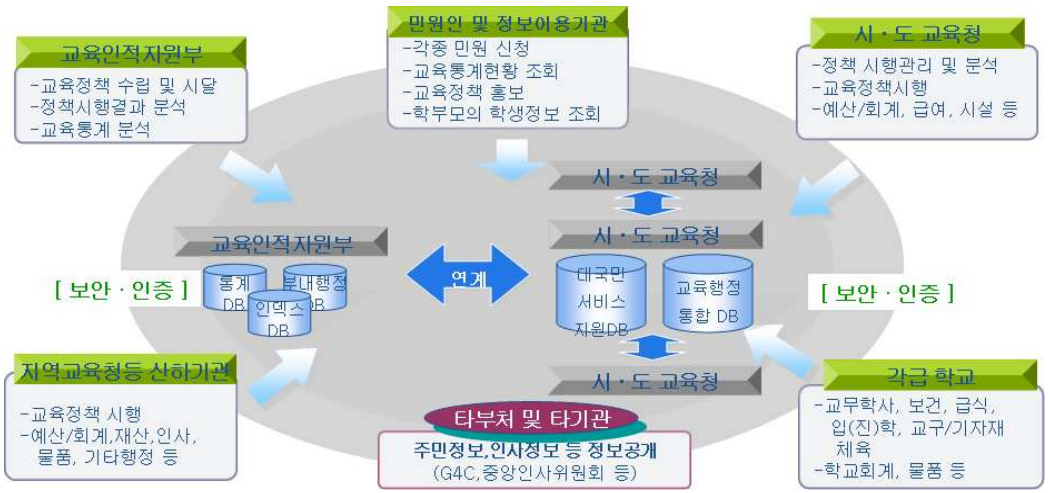
9) 행정시스템의 업무 사용자 접속은 교육과학기술부 장관이 정한 공인인증서를 발급 받은 자에 한한다(제18조).

10) 시스템운영자 등은 「공공기관의 개인정보보호에 관한 법률」과 「교육과학기술부 및 교육기관의 개인정보보호지침」 등 관련법규에 의거 개인정보를 보호하여야 한다(제19조).

## 2. 개인정보 수집·유통 실태

### 1) NEIS 시스템 개념도

<그림 2-11> NEIS 시스템 개념도




### 2) 개인정보의 수집·구축

NEIS는 '국민의 정부' 시절 중장기적인 국가 과제로서 설정된 「전자정부 11대 과제」중의 하나였다. 또한 1990년대 이후 급속도로 보급된 인터넷과 정부 주도적으로 구축한 세계 최고 수준의 IT 인프라는 NEIS가 요구하는 든든한 환경적 기반이 될 수 있었다. 뿐만 아니라 교육부는 이 사업이 안고 있는 기술적 문제에 미리 대비하는 한편, 이 사업의 기초공사로서 기존 교육행정업무를 재설계(BRP)하고 이를 기반으로 정보화전략계획(ISP)을 이미 수립

한 바 있었다(정책기획위원회, 2008: 2).

2001년 6월 26일엔 NEIS 구축을 위한 토론 및 공청회가 전자정부특위, 교육청, 한국전산원, 각급학교 교원 등 40여 명이 참석한 가운데 개최되었다. 공청회 참석자들의 의견에 따르면, 교육정보시스템을 학교 단위로 구축하는 것(14.3%)보다 시·도교육청 단위로 구축하는 것(64.3%)이 더 나은 것으로 밝혀졌다. 이에 따라 2001년 7월 10일 드디어 NEIS 구축 계획이 확정되었다. 그리고 2001년 10월부터 2002년 10월까지 NEIS의 분석, 설계, 개발이 진행되었다. 특히 2001년 8월 21일에는 교육정보시스템을 개발하는 비용 명목으로 '정보화촉진기금' 약 95억 원의 지원이 확정되었다. 시스템의 프로그램 개발 기간인 2001년 5월부터 2002년 10월까지 교원, 일반직교육공무원 등이 참여했고 교육청, 학교 등 관련 기관의 방문 및 협의가 진행되었다. 그 과정에서 총 437회에 걸친 업무회의가 있었으며 32개교 학교 방문을 통해 현장 교원 연인원 2,456명이 참여했다. 행정정보 서비스에서 다루어질 내용 구성은 다음과 같이 대영역과 중영역으로 정리되었다(정책기획위원회, 2008: 8).

<표 2-81> 초기 교육행정업무서비스 내역

| 대영역 | 중영역 | 내 용 |
|---|---|---|
| 기 획 | 기 획 | · 기획, 교육통계, 감사, 학생수용계획 등 교육행정 관리 |
| 교 원 인 사 | 교 원 인 사 | · 교원인력정책의 기본이 되는 교육공무원의 인사정보 및 통계자료 관리, 교육공무원의 임용 및 발령, 교원연수, 자격연수 및 관리, 교육장학과의 연계 등 교육공무원 인사 전반을 지원(국·공립·사립 교원 및 교육전문직 등) |
| 일 반 직 인 사 | 일 반 직 인 사 | · 일반직 공무원인력관리를 위해 정·현원관리, 인사기록 및 통계관리, 임용, 복무 등의 일반직 공무원 인사 전반을 지원(국·공립·사립 등) |
| 급 여 | 급 여 | · 급여, 연말정산, 연금, 보험 등 보수관련업무 지원<br>· 호봉제와 연봉제를 모두 지원(국·공립·사립 등) |
| 교육장학 | 장 학 | · 학교교육과정 운영 및 장학지도관리를 지원하는 업무 |
| | 시 험 | · 초등학교 취학 및 중·고 진학을 관리<br>· 검정고시 및 대학수학능력시험을 지원 |
| | 교무/학사 | · 학교단위에서 발생하는 학교교육과정편성, 성적, 학적, 학생생활지도, 교과용도서, 학교생활기록부 관리절차에 대한 관리 체제 지원 |
| | 평생교육 | · 평생교육운영, 평생교육시설, 학원(교습소)에 대한 관리지원 |

| | | |
|---|---|---|
| 보건체육 | 보건체육 | ·보건, 전염병, 급식, 위생정화구역 등 포괄적인 보건업무 지원<br>·체육특기자 및 학교체육시설에 대한 관리 지원 |
| 재 정 | 예 산 | ·예산편성, 예산에 의거 경영활동이 실시되는지 관리, 예산과 경영활동의 비교/검토/원인분석과 관련되는 일련의 활동 지원 |
| | 회 계 | ·세입·세출 등 회계자료의 초기발생부터 마감까지의 전 과정을 관련법령에 맞게 관리하며 관련부처 등과 연계시키도록 지원 |
| | 학교회계 | ·학교예산회계제도에 적합하도록 학교의 예산 및 회계 업무 관리지원 |
| | 재 산 | ·재산현황, 변상금, 재해복구공제회 관리를 통해 국·공유 재산을 관리 |
| | 물 품 | ·각 기관별 물품과 기자재 정보에 대한 통합관리 지원 |
| 시 설 | 시 설 | ·공사, 시설현황, 학교시설건축승인 등 교육시설관리업무전반을 지원 |
| 법 인 | 법 인 | ·법인정보 및 법인재산 등에 대한 관리 지원 |
| 기타행정 | 비상계획 | ·직장예비군 및 직장민방위 관리지원 |
| | 기타행정 | ·차량, 위원회, 신분증 등 행정업무관리 지원<br>·민원의 One-stop, Non-stop 서비스 지원 |
| | 시스템 관리 | ·코드, 사용자 권한, 로그 등에 대한 관리 지원 |

자료: 정책기획위원회(2008: 9-10).

교육부는 2002년 11월 인사, 예산, 회계, 시설 등 22개 영역의 1단계 서비스사업을 시범으로 실시하였고, 같은 해 12월에는 경력증명서, 졸업증명서, 검정고시 등 13종의 인터넷 민원서비스를 실시했다. 교육부 등 교육행정기관은 NEIS가 각종 학사민원 서비스와 통계처리를 편리하게 해주고 학부모들이 자녀의 학교생활을 확인할 수 있도록 해주는 훌륭한 교육정보화 도구이며, 학생의 주요문제가 무엇인지 이해하는데 크게 기여하여 학생지도의 질적 수준을 높일 것이라고 주장하였다. 그러나 전교조로 대표되는 반대 입장에서는 NEIS가 학생 및 학부모의 인권과 사생활을 침해하고 교사를 통제하는 '반인권적 국가통제 시스템'이라고 반박하였다. 학생의 민감한 각종 개인 정보를 개별 당사자의 동의 없이 일방적으로 국가가 수집하는 것 자체가 불법이며, 지나치게 자세히 학생 및 학부모의 신상정보가 기록되고 학생의 사전 동의 없이 정보가 수집되고 집적된다는 것이었다. 전교조는 NEIS의 반인권적인 측

면을 문제 삼아 2003년 2월 참여연대, 참교육학부모회 등 24개 교육 관련 시민단체와 함께 교육부총리를 국가인권위원회에 제소한데 이어 3월에는 서울지방법원과 행정법원에 NEIS 관련 손해배상 소송을 제기하기도 하였다. 2003년 4월 11일 교육부가 NEIS 27개 전 영역을 전면 개통하자, 전교조는 NEIS 시행을 전면 거부키로 하고 국가인권위원회에 제소하였다. 국가인권위원회는 NEIS가 인권침해의 소지가 있다고 지적하면서 2003년 5월에 다음의 세 가지 요지를 담은 권고사항을 발표하였다.

<표 2-82> 국가인권위원회 결정문

제 목 : 교육행정정보시스템(NEIS) 관련권고

주 문

교육부가 추진하는 교육행정정보시스템(NEIS)의 운영에 관하여 교육부장관에게,

1. 교육행정정보시스템의 27개 개발영역 가운데
   가. 사생활의 비밀침해 등 인권침해 소지가 있는 교무/학사, 입(진)학 및 보건 영역은 입력 대상에서 제외하고,
   나. 교원인사 기록 중 별지목록 기재 항목은 사생활의 비밀침해 등 인권 침해 소지가 있으므로 입력항목에서 제외되도록 '교육공무원인사기록및인사사무처리규칙'을 개정하고,
2. 개인정보의 누출로 인한 사생활 비밀침해 등 인권침해가 없도록 학교종합정보시스템(CS)에 대한 보안체계 강화 조치를 강구할 것을 각 권고한다.

자료: 국가인권위원회(2003).

또한 NEIS의 수록정보가 개인의 행복추구권과 사생활 비밀 및 자유 등을 침해한다는 헌법소원[191]에 대하여 헌법재판소는 학교에서 수집하는 불필요한 개인정보의 불법 유통을 금지하도록 결정하면서, 개인인격과 밀접하게 연관된 민감 정보로 보기 어려운 졸업생 성명, 생년월일 및 졸업일자만을 NEIS에 보유하는 행위는 수권 법률의 명확성을 특별히 요구하지 않는 정보로 판결하였으며, 개인정보 자기결정권에 대한 상대적, 제한적 권리로 정의하였다. 이것은 전자정부를 선도하는 개인정보보호에 대한 국민적 인식을 획기적으로 제고시켰다.

191) 2003헌마282, 2003헌마425.

2003년 11월 27일 48개 교육·인권단체로 구성된 'NEIS 반대와 정보인권 수호를 위한 공동대책위원회'는 정보인권을 중심내용으로 하는 8개 항의 '교육정보 수집·활용·관리 원칙'을 발표하였다. NEIS 논쟁을 계기로 학교를 비롯하여 사회 전반적인 정보인권 인식이 높아지긴 했지만, 정보인권 보호를 위한 '교육정보의 수집·활용·관리 원칙'을 통해 이를 확고히 할 필요가 있으며, 교육정보화위원회가 이를 천명해야 한다는 것이다. 이는 최근 NEIS 통합에 따른 논란을 바라봄에 있어서도 교육정보의 수집·활용·관리를 위한 일종의 가이드라인으로 검토해볼 만하다.

<표 2-83> 교육정보의 수집·활용·관리 원칙

1) 교육 목적과 무관하게 수집·활용·제공되어서는 안된다.
2) 개인의 사상·신조와 같은 극도로 민감한 정보는 수집이 금지되어야 한다.
3) 교육정보를 수집할 경우, 수집제한의 원칙과 목적구속의 원칙이 준수되어야 한다. 수집 당시에 구체적인 목적이나 용도가 미리 특정되어 있어야 하고(목적의 특정성), 그 목적은 정당해야 하며(목적의 정당성), 그 목적이나 용도에 필요한 범위 내의 정보만 수집되어야 하며(수집범위의 필요최소성), 공정하고 합리적인 방식으로 수집되어야 하고(수집방식의 합리성), 정보주체인 학생 또한 학부모의 분명한 인식 또는 동의하에 수집되어야 한다(정보주체의 인식명확성).
4) 정보주체인 학생·학부모는 수집, 보관되는 교육정보에 대해 통지를 받을 권리가 있으며, 교육정보를 열람하고 삭제·정정할 권리를 보장받아야 한다.
5) 정보의 공개나 제3자에 대한 제공은 엄밀하게 교육적인 목적으로 제한하고, 당사자의 동의 하에서만 허용되어야 한다. 예외적으로 당사자의 동의 없이 제공할 수 있는 경우는 법률로써 규정되어야 한다.
6) 수집된 교육정보는 교육 목적에 맞는 기간에 한정하여 보관되어야 하며, 그 이후에는 폐기되어야 한다.
7) 수집하는 정보마다 관리 주체와 공유 범위가 분명하게 구분되어야 한다. 원칙적으로는 개인에 대한 정보는 단위학교에서 해당 교사가 수집, 관리하여야 하며, 단위학교에서도 담당자 외의 접근을 차단하고, 정보의 통합이 이루어지지 않도록 분리, 수집되고 관리되어야 한다.
8) 수집된 정보의 보완을 위한 기술적·제도적 장치가 마련되어야 하며, 관리 책임자가 명확하게 설정되어야 한다.

자료: NEIS 반대와 정보인권 수호를 위한 공동대책위원회(2003).

이에 국무총리실 산하 교육정보화위원회는 2003년 12월 15일 NEIS 운영과 관련해서 교무・학사, 보건, 입(진)학 등 3개 영역은 학교별 서버에 담아 민간・국가기관・학교 등이 공동관리(co-location)하기로 결정했다. 이와 함께 보안성을 높이기 위해 공개키기반구조(PKI) 기술을 도입하여 자료를 암호화하고 기록은 실시간으로 남기도록 했다(정충식, 2009: 359).

교육과학기술부(학교, 교육청 포함)는 NEIS의 도입으로 정보주체의 학교생활기록 및 건강검사에 관한 자료를 체계적으로 수집・집적・이용・공개하고 있다며, 2006년 9월부터 '내자녀바로알기 학부모서비스'(www.parents.go.kr)를 운영하고 있다. 교육부가 NEIS "학부모 서비스"를 통해 학부모에게 제공하고 있는 정보는 학교정보 9종과 학생정보 16종, 그리고 학부모 상담관리 1종으로 총 26종[192]이었다.[193] 보건기록은 보건교사가 입력해야 하나, 이 또한 업무이므로 업무부담[194]으로 인해 제대로 통합되지 않고 있으며, 학부모 재산기록(가정형편) 등은 입력하지 않고 있다.

교육과학기술부의 학부모서비스는 지난 2006년 9월 자녀의 학교생활 및 학교정보 등 6종의 정보 제공을 시작으로, 2007년 9월에 26종으로 확대하였으며, 2008년 4월에는 152개 교육전문사이트와 연계한 학부모서비스 포탈사이트(http://www.parents.go.kr)로 개편되었고, 2009년 4월에는 12종을 확대하여 4개영역 38종의 서비스를 제공하고 있다. 추가 대상은 교육과학기술

192) 학부모서비스는 26종을 제공하지만 주간학습(초등), 특별활동조회, 성적통지표(중・고)는 학교장이 제공여부를 결정하며 나머지는 기본적으로 제공된다. 흡연적발시 봉사활동과 같은 징계기록의 경우 징계심사위원회에서 처리한 회의록이 남아 있으며, 그 결과만이 생활기록부에 기록된다.

193) NEIS에 포함된 학생정보는 자녀에 대한 적절한 정보를 전달함으로써 학교생활에 대한 학부모의 이해를 증진시키고 성장과정을 객관적으로 파악하게 될 뿐 아니라 학부모의 알권리도 충족시키게 되며, 학교와 가정간의 상호이해까지도 증진시키는 측면이 있다(이보영, 2005). 반면, 학부모의 과도한 참여로 이어져 학교행정에 혼란이 발생할 수도 있고 학부모간 정보격차(digital divide)가 발생할 수도 있다(강창동, 2005; 하연섭 외, 2006 재인용).

194) NEIS 도입 과정에서 교육부는 NEIS를 통해 교원의 일하는 방식이 변화되고, 보다 간편하고 신속・정확한 업무처리로 효율성이 제고되어 궁극적으로는 교원의 업무가 경감된다고 주장하였다. 기존의 시스템으로부터 데이터를 이관하는 작업은 노력이 들겠지만, 일단 새로운 시스템이 구축되면 교원들의 업무는 현저히 감소하게 된다는 것이다. 반면 전교조는 이러한 주장을 전면 반박하여, NEIS를 통해 출결관리, 시간표관리, 성적처리, 시스템관리 등 전반적인 업무가 증가할 뿐 아니라, NEIS를 통해 교육에 대한 정부의 통제가 강화된다고 보았다. 정보입력업무를 통해 교사의 업무는 증가될 수밖에 없으며 단순 행정노동자가 될 것을 우려하였다. NEIS 체제의 도입으로 인하여 새롭게 발생하는 막대한 자료의 가공과 입력업무는 차치하고서라도, 잦은 기술상의 오류 때문에 기존의 CS와 비교할 수 없을 정도로 업무가 가중된다는 것이다(정책기획위원회, 2008: 62).

부가 인터넷이 서투른 학부모를 위해 개발 중인 모바일서비스를 비롯해 개인별 맞춤형 학업성적, 학부모 상담관리, 진로정보관리, 가정통신문 회신 현황 등이다.

<표 2-84> 2009년 학부모 서비스 제공 항목 38종

| 구 분 | 서비스 내역 |
|---|---|
| 학교정보(9종) | ◦ 학교기본정보<br>◦ 교육과정: 과목 및 담당교사, 반별시간표, 주간학습(초등)<br>◦ 학사일정: 연간학사일정, 월간학사일정<br>◦ 급식식단표 : 월간식단, 주간식단<br>◦ 가정통신문 |
| 학생정보(21종) | ◦ 학교생활기록부, 학생건강기록부<br>◦ 학습안내: 교내/교외학습자료, 개인별 맞춤학습(중, 고)<br>◦ 학교생활: 월출결통계, 출결사항, 특별활동(자치/적응/행사/계발/봉사활동) 조회, 치료교육활동조회(특)<br>◦ 성적<br>- 고사별 정・오답표(중,고), 성적통지표(중,고,특), 성적(초,특)<br>- 표준점수분석표(중,고,특), 성적변화표(중,고,특), 학업성취도(초,중,고)<br>◦ 진로/상담자료: 진로상담을 위한 도움자료, 심리검사 결과(중,고) |
| 학부모 상담 관리(3종) | 상담공지사항, 선생님과의 상담, 상담내역 조회 |
| 자녀교육 활용정보(5종) | 학업지도, 인성지도, 진학지도, 진로지도, 특수아지도 |

### 3) 개인정보의 이용 및 제공

서울시교육청이 NEIS의 '내 자녀 바로 알기 서비스'를 이용하는 학부모 1만 명을 대상으로 관심 있게 이용한 항목을 조사한 결과에 따르면, 응답자의 19%가 성적을 꼽아서 가장 많았고, 학교생활기록부(17%), 학교생활・교육과정・학사일정(각 11%), 학교 기본정보(8%) 순이었다. 반면에 급식식단표(4%)와 건강검사 결과를 확인할 수 있는 건강기록부(3%) 및 선생님과의 상담(2%)에 관한 관심도는 낮았다. 학부모의 관심이 성적 쪽에 편중되어 있음을 알 수 있다.[195]

195) 연합뉴스. 2009.3.16. "학부모의 자녀 관심사는 역시 '성적'."

김춘진 의원에 따르면, NEIS 학부모서비스는 2006년 9월부터 서비스를 시작하여 2009년 10월 10일까지 총 171만 2,366명에게 38종의 서비스를 제공하였는데, 이를 연도별로 살펴보면, 2006년 13만 9,282명에서 2007년 69만7,528명, 2008년 115만9,557명, 2009년 현재 171만2,366명이 누적 이용하였다. 시도별로 살펴보면, 학부모서비스 누적 이용자 수는 경기 47만7,528명으로 가장 많았고, 다음으로 서울(25만6,808명), 인천(25만2,782명), 경남(9만4,769명) 순이었다(김춘진, 2009).

<표 2-85> 시도별 연도별 학부모서비스 누적 이용자 수

(단위: 명)

| 시·도 | 2006년 | 2007년 | 2008년 | 2009년 |
|---|---|---|---|---|
| 서울 | 23,430 | 94,303 | 179,054 | 256,808 |
| 부산 | 6,080 | 22,045 | 49,987 | 74,453 |
| 대구 | 5,829 | 18,667 | 55,243 | 94,010 |
| 인천 | 5,865 | 183,200 | 218,283 | 252,782 |
| 광주 | 4,494 | 10,668 | 14,736 | 37,374 |
| 대전 | 5,278 | 19,652 | 41,228 | 68,640 |
| 울산 | 4,552 | 14,676 | 18,949 | 25,114 |
| 경기 | 47,676 | 182,926 | 314,751 | 477,528 |
| 강원 | 5,294 | 16,562 | 25,530 | 42,440 |
| 충북 | 4,957 | 14,288 | 21,002 | 32,929 |
| 충남 | 5,963 | 24,438 | 46,377 | 76,985 |
| 전북 | 3,843 | 10,386 | 13,003 | 17,440 |
| 전남 | 2,727 | 24,005 | 32,956 | 57,835 |
| 경북 | 7,044 | 25,288 | 51,867 | 90,735 |
| 경남 | 5,113 | 30,801 | 68,640 | 94,769 |
| 제주 | 1,137 | 5,821 | 7,951 | 12,524 |
| 계 | 139,282 | 697,726 | 1,159,557 | 1,712,366 |

자료: 김춘진(2009).

2009년 4월에서 9월까지의 학부모서비스 매뉴얼 상세 이용현황을 살펴보면, 총 18,999,684회 중에서 가정통신문 이용률이 18.2%로 가장 높았으며, 다음으로 성적변화표(12.9%), 학교생활기록부(10.8%), 월출결통계(5.1%), 성적통지표(5.0%) 순이었다. 그러나 학부모상담관리 메뉴인 선생님과의 상담,

상담내역조회, 상담공지사항은 총 662,719회(3.5%)에 불과했다.

<표 2-86> 학부모서비스 매뉴얼 상세 이용 현황

| 구 분 | 세 부 내 역 | 이용 횟수 | 이용률(%) |
|---|---|---|---|
| 가정통신문 | 가정통신문 | 3,467,226 | 18.2% |
| 성적 | 성적변화표 | 2,459,682 | 12.9% |
| 학생기록부 | 학교생활기록부 | 2,045,898 | 10.8% |
| 학생생활 | 월출결통계 | 964,377 | 5.1% |
| 성적 | 성적통지표 | 952,587 | 5.0% |
| 건강기록부 | 건강기록부 | 848,288 | 4.5% |
| 성적 | 학업성취도(초) 학기별 | 761,336 | 4.0% |
| 학습안내 | 교외학습자료 | 675,105 | 3.6% |
| 교육과정 | 과목및담당교사 | 611,425 | 3.2% |
| 학교기본정보 | 학교기본정보 | 574,902 | 3.0% |
| 학사일정 | 연간학사일정 | 566,307 | 3.0% |
| 진로/상담자료 | 진로/상담자료 | 538,013 | 2.8% |
| 성적 | 고사별정·오답표 | 484,647 | 2.6% |
| 성적 | 표준점수분석표 | 440,904 | 2.3% |
| 심리검사 | 심리검사 | 309,513 | 1.6% |
| 교육과정 | 반별시간표 | 273,171 | 1.4% |
| 학생생활 | 봉사활동조회 | 254,454 | 1.3% |
| 학부모상담관리 | 선생님과의상담 | 247,153 | 1.3% |
| 급식식단표 | 월간식단 | 246,033 | 1.3% |
| 학부모상담관리 | 상담교사조회/예약신청 | 239,031 | 1.3% |
| 학사일정 | 월간학사일정 | 235,098 | 1.2% |
| 학부모상담관리 | 상담내역조회 | 220,615 | 1.2% |
| 학습안내 | 교내학습자료 | 220,129 | 1.2% |
| 학생생활 | 출결사항 | 202,166 | 1.1% |
| 학생생활 | 자치활동조회 | 195,623 | 1.0% |
| 학부모상담관리 | 상담공지사항 | 194,951 | 1.0% |
| 학생생활 | 적응활동조회 | 176,665 | 0.9% |
| 학생생활 | 행사활동조회 | 173,904 | 0.9% |
| 학생생활 | 계발활동조회 | 165,667 | 0.9% |
| 학생기록부 | 학교생활기록부(시각장애인용) | 114,947 | 0.6% |

| | | | |
|---|---|---|---|
| 급식식단표 | 주간식단 | 84,357 | 0.4% |
| 교육과정 | 주간학습 | 55,390 | 0.3% |
| 학생생활 | 치료교육활동 | 120 | 0.0% |
| 계 | | 18,999,684 | 100.0% |

자료: 김춘진(2009).

NEIS는 2006년부터 교무업무(교무・학사, 입・진학, 보건)를 학교급별 단독 또는 그룹서버 형태로 3,000여대의 서버를 분리 운영하고 있다. 교육부는 지난 4년간 그룹서버를 시범 운영하는 과정에서 단 한건의 개인정보 유출이나 보안침해 사고가 없었고, 오히려 서버가 학교단위로 분리 운영되는 단독서버의 경우 시설유지비용, 공간문제, 시스템간 연계 어려움 등 비효율적인 요소가 많아 이를 개선해야 한다는 의견이 꾸준히 제기되어 왔다고 주장한다. 그리고 그 근거로 지난 2008년 10월 한국교육학술정보원(교무업무시스템 평가위원회)이 평가한 교무업무 서버 운영평가 결과에 따르면, 보안 측면에서 단독서버와 그룹서버 모두 단 한건의 침해사고가 없는 등 보안상 안전성에는 차이가 없으나, 경제성 측면에서 단독서버가 그룹서버보다 학교당 설비비용은 17배, 유지보수 비용은 5배 더 많이 소요되는 것으로 나타났으며, 시스템 품질면에서도 단독서버가 그룹서버에 비해 장애 빈도는 2배, 장애시간은 7배 더 많은 것으로 나타났다고 보고, 이제는 서버운영의 비효율성 제거와 노후서버 교체 등 서버운영의 최적화 방안을 마련하기 위해 NEIS를 시・도 교육청 단위로 통합하겠다는 것이다(교육과학기술부, 2009).

교과부의 전신인 (구)교육인적자원부는 NEIS가 기존의 C/S시스템보다 기술적으로 높은 수준의 보안이 가능하며 자료의 신뢰성이 뛰어나다고 주장해 왔다. 현재 정보기술로 볼 때 인터넷뱅킹 수준의 안전한 보안체제를 갖추고 있으며, 강력한 방화벽과 권한설정방식 등의 조처를 통하여 전교조가 우려하는 인권침해와 정보유출을 사전에 충분히 방지할 수 있다고 보았던 것이다. 여기에서 권한 설정방식이란 학급 담임, 교과 담당 등 정당한 권한을 가진 자만이 자료에 접근할 수 있도록 하는 조처로, 시・도교육청과 교육부가 학생개인의 자료에 접근할 수 없도록 되어 있다. 즉 이들 기관들은 원자료(raw data)에는 접근할 수 없고 익명으로, 집단으로 분석되는 2차적인 통계 자료에만 접근이 가능하기 때문에 모든 자료가 익명으로 처리되는 상황에서 학생개인의 신상정보 유출과 개별교사의 국가통제란 기우에 지나지 않는다는 것이다.

이에 대해 전교조와 인권단체들은 집권적 중앙관리시스템인 NEIS체제하에서는 정보 유출의 가능성이 더 커지며, 그럴 경우 피해규모도 더욱 크다고 반박한 바 있다. NEIS는 학생 상담 내용뿐만 아니라 성적, 각종 행동 특성, 몸무게, 키, 학부모 주소 및 이름 등과 같이 학생과 학부모 2,000만 명의 개인정보 200여 항목을 담고 있기 때문에 이 같은 정보들이 이익을 추구하는 기업 등에 의해 상업적으로 이용될 수 있고, 또한 국가가 이를 국민통제 수단으로 이용할 수 있다는 것이다. 실제로 NEIS에서 침입탐지시스템으로 채택된 보안프로그램에서 약점이 발견되기도 하였다(김태우, 2006; 하연섭 외, 2006 재인용).

이대식・정주영의 NEIS 운영실태에 대한 인식조사(이대식・정주영, 2006: 119-120 재인용)에 따르면, 첫째, C/S에 대한 인식 조사에서는 C/S 도입 초기에 논란은 많았지만 기능 면에 만족하고 있고 프로그램 운영에 문제가 없으나, 업무량 감소 정도 측면에서는 수기로 작성할 때와 비교해 수기장부나 업무가 감소되었다는 반응이 적었고, 서버로 인한 업무중단에 대한 측면에서도 서버 다운과 잦은 프로그램패치(patch)로 인한 업무 차질에 대해 부정적 견해를 갖고 있는 교사들이 많았다.

둘째, NEIS 도입 및 추진과정에서 ① NEIS도입은 전자정부 추진사항으로서는 필요할지 모르나 시기가 적절하지 못했다는 의견이 많았고, ② NEIS 운영에 앞서 일선교사들의 의견을 충분히 수렴하지 않고 너무 성급하게 시행했다는 견해가 많았다. 또한 ③ 교육정보화 시스템이 SA에서 C/S로, C/S에서 NEIS로 정착될만하면 새로운 시스템으로 변경되어 업무에 혼선을 야기하는 것으로 나타났다. 물론 NEIS의 정상적인 정착 여부에 대해서는 대부분의 교사들이 시행 초기여서 여러 가지 문제에 부딪히고 있지만 앞으로 정상적으로 정착될 것이라고 기대하는 측면이 높았다. 하지만 이것이 지금처럼 교육부가 NEIS 통합을 추진하기 위한 근거가 되는 것은 아니다.

셋째, NEIS 교무 학사 세부업무별 만족도 측면에서 '자료이관후 학생/성적자료수정' 메뉴에서는 부정적인 응답이 높았으나 나머지는 긍정적인 반응이 높았다. 이는 '자료이관후 학생/성적자료수정' 항목은 과년도 자료를 수정해야 할 경우나 전입생의 과년도 성적을 입력해야 할 경우 사용하는 항목으로 특정 권한을 부여받아야 사용할 수 있기 때문인 것으로 보인다. 그러나 다른 메뉴에서는 모두 만족스러운 반응이 나타났으므로 교무 학사 세부업무별 만족도는 높은 것으로 분석된다.

넷째, NEIS 기능 및 효율성 중 ① NEIS에 대한 인지 정도에서는 대부분의

교사들이 NEIS에 대한 기능을 알고 있고, ② 기존 C/S보다 NEIS가 편리하다고 인식하고 있는 것으로 나타났다. ③ 업무경감 측면에서는 C/S때와 마찬가지로 업무가 경감되었다고 느끼는 교사들이 적었다. ④ 초·중·고·대학의 업무연계 측면에서는 전국의 모든 학교에서 NEIS를 사용하고 있는 것이 아니므로 전 출입이나 진학시 업무연계가 어려운 것으로 나타났다. ⑤ 학부모 서비스의 경우 학교에서 학부모들에게 NEIS에 대한 유인물을 통해 의견수렴을 해야 하고, 학부모 승인을 위한 절차가 번거로워 기피하는 현상이 있는 것으로 나타났다. ⑥ 출결 등 통계처리의 수월성 면에서는 긍정적 응답이 높았고, ⑦ 전 출입시 첨부서류는 별로 줄어들지 않은 것으로 나타났다. ⑧ NEIS를 운영함에 있어 업무에 따라 별도의 검증된 보조 전산요원을 필요로 했고, ⑨ 성적처리 측면에서는 교과목별로 담당교사가 성적처리를 따로 해야 하는 불편함과 출력물이 다양하지 못하다는 이유로 외부 프로그램을 사용하는 학교들이 있었다. 이는 NEIS가 아직 정착단계의 시스템이 아니므로 부정적인 견해를 갖고 있는 교사들이 있기 때문인 것으로 분석된다.

다섯째, NEIS의 보안 및 기술적 측면에서는 ① 개인정보유출의 가능성이 있고, ② NEIS 보안문제를 공인인증체계가 완전히 해결해 줄 수는 없다고 보는 견해가 많았다. ③ 중앙서버의 집중화 문제는 시험기간이나 학기초, 학년말 등 업무가 집중되는 시기에는 서버 접속이 느려지는 등의 문제가 발생하는 것으로 나타났다. ④ NEIS 도입의 당위성에 대한 측면에서는 대부분의 교사들이 NEIS가 정보화 시대에 꼭 필요한 시스템으로 인식하고 있는 것으로 나타났고, ⑤ 각급 학교별 유동성 있는 시스템 운영에 대한 측면에서는 학교별로 시스템에 대한 선택권을 주어 자율적으로 운영해야 된다는 견해가 많았다.

현재는 NEIS 외의 다양한 정보시스템을 시도교육청별로 구축하고 있으며, 교과부에서 이들 시스템을 통합하려 하였으나, 어려울 것으로 파악되었다. 예산이 시도교육청으로 내려갔다가 다시 올라오는 구조에서 시도교육청에게는 별다른 인센티브가 없기에 열의를 갖는 사업이 아니기 때문이다. 더욱이 위의 NEIS 운영실태에 대한 인식조사에 나타난 것처럼, NEIS에 대한 교육현장의 수용도가 높다고 보기도 어렵다.

그러나 교육과학기술부는 전국 시·도교육청과 초·중등학교에서 활용하고 있는 현 교육행정정보시스템(NEIS)의 노후화된 서버와 비효율적인 서버운영을 개선하기 위해 연내 정보화전략계획(ISP)을 수립하고 2010년부터 서버시스템 교체와 통합을 추진한다고 밝혔다. 전국 11,000여개 학교와 16개 시도

교육청에서 활용하는 NEIS의 서버시스템과 업무프로그램을 2010년부터 전면 교체하겠다는 것이다(교육과학기술부, 2009).

또한 정부는 학생들의 상·벌점제도인 그린마일리지를 NEIS와 연계해 상벌점 기록이 평생 남도록 하는 방안을 추진하고 있는데, 이에 대해 학생들은 많이 걱정하고 있었다. 전교조 경남지부와 청소년인권행동 '아수나로'(경남중부지역모임)가 지난 2009년 7월 5일~15일 사이에 시범학교 중고교생 1,133명을 대상으로 설문조사를 실시한 결과에 따르면, 그린마일리지를 NEIS와 연계하여 기록이 남게 하는 방안에 대해 75.8%의 학생들이 부정적으로 응답했다.[196] 사생활 침해 우려와 학생 진학 영향 등이 그 이유이다. 교과부가 NEIS의 긍정적 효과로 파악하고 있는 것에 대해 학생들은 부정적으로 파악하고 있는 것이다. 교과부에서 이러한 조사결과 등을 충분히 검토했는지 의문이다.

나아가 교과부는 일선 시·도교육청을 통해 시범운영 중인 학교회계시스템 '에듀파인'(edufine)을 2010년 3월부터 전국 학교를 상대로 확대 시행할 계획으로 있다. 개발 및 인프라 구축비용으로 수백억 원이 투입된 것으로 알려진 이 시스템은 교사가 직접 예산계획을 세우고 재정성과까지 평가받을 수 있도록 한 것이 핵심이다. 모든 절차가 전산망을 통해 이뤄지므로 상위 교육기관은 개별 학교의 전체 예산 흐름을 한눈에 파악할 수 있다. 지금까지는 교사가 특정물품을 구입하거나 교육프로그램을 진행할 경우 해당 사업에 대해 교장 결재를 받은 뒤 행정실에 넘겨주면 됐지만, 에듀파인이 도입되면 일반 교사들이 직접 행·재정업무를 수행하게 된다. 이 시스템은 학생들의 학사업무를 전산처리하기 위해 NEIS와도 연동되어 활용된다.

교과부는 에듀파인시스템이 자리를 잡으면 투명한 회계보고가 정착돼 학교별 성과를 정확히 파악할 수 있을 뿐 아니라 교사들이 행·재정업무에 적극 참여하게 된다는 점에서 학교자치 기능도 확대될 것으로 기대하고 있지만, 업무가 복잡해 교원의 근무부담과 학교행정처리의 혼선을 초래할 수 있다는 점에서 일선 교사들이 반발하고 있다고 한다.[197] NEIS 도입 과정에서 나타난 갈등 양상을 감안한다면 이러한 시스템의 전면 도입에 앞서 충분한 검토와 보완이 필요하나 현재로서는 그러한 움직임이 보이지 않아 우려를 자아내고 있다.

196) 오마이뉴스. 2009.8.25. "'학교 상벌점제 시행 뒤 체벌 사라졌다" 2.3% 그쳐."
197) 연합뉴스. 2009.8.28. "교사들이 교육사업비 직접 편성·지출."

## 3. 개인정보의 열람 및 정정·삭제 청구권 보장 실태

NEIS에 수집된 학생에 관한 정보는 개인의 건강기록, 학생 생활기록 등 사생활 정보 등에 관한 광범위하고, 고도의 보호가 필요한 사생활 정보로 비록 본인 확인에 의해 이미 공개된 정보라 하더라도 위 정보는 개인의 인격주체성을 특정 짓는 정보로서 「공공기관의 개인정보보호에 관한 법률」 제2조제2호에 의한 개인정보에 해당되고, 각급 학교는 이법에 정한 바[198]에 따라 재학 중인 학생에게 열람청구권, 정정청구권 등을 보장하여 개인정보를 보호해야 한다(국가인권위원회, 2008). 「교육기본법」, 「초·중등교육법」도 이와 동일한 취지에서 개인정보의 이용, 제공을 정보주체 스스로 결정하고 통제할 수 있도록 보호하고 있으며, 「교육정보시스템의 운영 등에 관한 규칙」은 재학생이 정보시스템에 접속하여 전산자료를 열람할 수 있는 개인정보열람청구권을 명시적으로 인정하고 있다.

「교육정보시스템의 운영 등에 관한 규칙」 [교육과학기술부령 제1호, 2008.3.4, 타법개정]
제9조 (학생 전산자료의 열람 및 제공) ①정보시스템을 활용하는 학교에 재학중인 학생 또는 학생의 부모 등 법정대리인은 정보시스템에 접속하여 당해 학생의 전산자료를 열람할 수 있다.
②학교의 장은 제1항의 규정에 의하여 전산자료의 열람을 신청한 자가 본인 또는 정당한 법정대리인인지 여부를 「전자서명법」 등 다른 법률의 규정에 의한 공인인증서를 통하여 확인한 후 당해 학생의 전산자료에 대한 열람을 승인하여야 한다.
③제3자가 법 제30조의6제1항의 규정에 의하여 학생 전산자료의 제공을 요청하는 경우 학교의 장은 정보시스템을 이용하여 인터넷으로 제3자에게 학생 전산자료를 제공할 수 있다.

국가인권위원회는 인천 소재 한 고등학교 재학생이 “NEIS에 집적된 재학생 본인의 정보를 열람할 수 없게 한 것은 개인정보자기결정권을 침해한 것”이라며 2008년 1월 10일에 국가인권위에 진정을 접수하자, 지난 2008년 12월 15일 재학생이 NEIS에 수집된 본인 정보를 담임선생님 또는 학부모를 통해서만 열람하도록 하는 것은 「헌법」에 근거한 개인정보자기결정권 및 「공공기관의 개인정보보호에 관한 법률」 등에 보장된 열람청구권, 정정청

198) 「공공기관의 개인정보보호에 관한 법률」 제3조의2(개인정보 보호의 원칙), 제12조(처리정보의 열람), 제14조(처리정보의 정정 및 삭제 등).

구권 등을 침해하는 행위라고 판단하고, △교육과학기술부장관에게 재학생이 교육행정정보시스템에 수집된 본인정보를 열람할 수 있도록 기술적 보안체계를 확립하고, 서버 등 물적기반 시스템을 확대하는 등의 대책을 수립할 것과, △각 시·도 교육청 교육감에게 재학생의 개인정보자기결정권을 침해하는 유사 사례가 재발하지 않도록 관련 대책을 수립해 각급 학교에 시달할 것을 권고한 바 있다(국가인권위원회, 2008).

국가인권위원회의 조사 결과에 따르면, 교육과학기술부(학교, 교육청 포함)는 2000년 9월부터 개발이 시작된 NEIS의 도입으로 정보주체의 학교생활기록 및 건강검사에 관한 자료를 체계적으로 수집, 집적, 이용, 공개하고 있으며, NEIS “학부모 서비스”를 통해 2006. 9.부터 학부모에게 제공하고 있는 학교정보 9종과 학생정보 16종, 학부모 상담관리 1종의 정보는 여러 의견 수렴을 통해 학부모를 대상으로 제공되는 서비스이며, 재학 중인 학생의 경우에는 NEIS “학부모 서비스”를 통해 학부모에게 제공하는 26개의 정보 대부분을 학교생활을 통해 이미 알고 있기 때문에 제공 대상을 학부모로 제한하였다고 밝혔다. 그리고 NEIS 재학생 서비스를 확대하기 위해서는 학생의 신원 확인 방안과 보안 대책의 강구, 서비스 범위 확대 등을 고려해야 하는데, 이를 위해 시스템 용량 증대 및 예산확보, 서비스 제공대상 선정 및 공인인증 발급 등을 종합적으로 고려한 NEIS 중장기 발전계획 수립을 추진 중에 있다고 하였다.

하지만 국가인권위 조사에 따르면, 「교육정보시스템의 운영 등에 관한 규칙」 제9조에서 재학생이 정보시스템에 접속하여 전산자료를 열람할 수 있는 개인정보열람청구권을 명시적으로 인정하고 있음에도 불구하고, 재학 중인 학생이 NEIS에 직접 접속하여 자신에 관한 정보를 열람할 수 있는 방법이 마련되어 있지 않았다. 이에 국가인권위는 정보주체인 재학생이 NEIS에 수집된 본인정보를 정보주체 스스로 열람할 수 없도록 한 것은 인권침해라고 판단하고, 관계기관에 대책 마련을 권고하였다.

## 4. 소결

교육기관은 개인정보의 유출이 빈번하게 이루어지고 있음에도 불구하고 그 실태가 제대로 포착되고 있지 않은 영역이다. 특히 NEIS의 도입 이후 학부모 서비스의 제공을 통해 광범위한 개인정보가 수집되고 유통되고 있음에도 불구하고 이에 따른 부작용의 측면은 별로 검토되고 있지 않다. 또한 교육과학

기술부는 그 와중에 NEIS 운영에 대한 구체적인 평가 없이 이를 통합하려 하고 있으며, 일선 시·도교육청을 통해 시범운영 중인 학교회계시스템 '에듀파인'(edufine)을 2010년 3월부터 전국 학교를 상대로 확대 시행할 계획으로 있어 논란이 되고 있다.

NEIS의 통합 및 다른 시스템과의 연계에 따른 논란이 막대한 사회적 비용을 초래할 가능성을 염두에 둔다면 NEIS 도입시의 시행착오 경험에서 교훈을 얻어 이를 전격적으로 추진하기에 앞서 사회적인 합의를 도출해내는 노력이 선행될 필요가 있다고 본다.

# 제3장 특성별 개인정보 수집·유통 실태

제3장에서는 CCTV, 위치정보, 유전정보, 통신비밀 등 사회적으로 쟁점이 되고 있는 특수한 유형의 개인정보에 대해 분석하였다. 여기서 다룬 특수한 유형의 개인정보는 여러 사회 영역에 걸쳐 수집되고 있으나, 본 연구에서는 방범용 CCTV, 교통 관련 위치정보, 실종아동등의 유전자 데이터베이스, 수사기관 등에 의한 통신비밀 침해 문제 등에 집중하여 분석하였다. 그러나 각 정보의 특성에 따른 침해의 양상이나 및 개인정보 보호를 위한 특별한 조치의 필요성 등을 분석하는데 무리는 없을 것으로 보인다.

## 제1절 CCTV

### 1. 개요

#### 1) CCTV와 개인정보에 대한 권리

'폐쇄회로 텔레비전'(CCTV)이란 정지 또는 이동하는 사물의 순간적 영상 및 이에 따르는 음성·음향 등을 특정인이 수신할 수 있는 장치를 말한다.[199]

CCTV 종류는 형태에 따라 스탠다드, 돔, 핀홀 카메라로 나뉘고, 기능에 따라 고정, 팬/틸트/줌, 스피드돔, 줌일체형 카메라로 나뉘며, 조도에 따라 일반, 저조도, 적외선 카메라로 나뉜다. 전송방법에 따라서는 일반 CCTV(아날로그 CCTV)와 네트워크 카메라를 구분하는데, 일반 CCTV는 촬영된 영상을 동축케이블을 통해 전송하고 비디오 테이프나 DVR(Digital Video Record)에 저장할 수 있고 네트워크 카메라에는 IP주소가 할당되어 촬영된 영상을 IP 네트워크 망을 통해 전송하고 DVR이나 비디오 서버에 저장할 수 있다(행정안전부, 2009a: 12).

CCTV는 당초 일반인의 출입이 통제되어 있는 사적 공간이나 특수 시설 내에 한정하여 설치·운용되는 것이었기 때문에 일반인의 인권 침해가능성이 상대적으로 낮은 것으로 평가되었다. 그러나 정보화기술이 고도화되어 매체간 융합이나 디지털 전송·녹화 기술이 도입되고 범죄예방 목적으로 일반 공

199) 「공공기관의 개인정보 보호에 관한 법률」 제2조제5의2호.

중의 자유로운 출입이 허용된 공간에 대하여도 CCTV를 설치하게 됨으로써 일반 대중의 초상권 침해를 비롯한 정보인권 침해의 문제가 대두되었다. 특히, CCTV를 통해 감시당하고 있는 일반 대중은 그 감시자가 누군지도 알 수 없는 상태에 놓이게 되어 헌법이 보장하고 있는 자유로운 인격발현 활동을 제어 내지 통제당하는 결과를 야기하게 된다(정준현, 2007: 15).

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

특히 범죄 예방 및 범죄 수사를 위하여 공공기관이 CCTV 등 무인단속장비를 공공장소에 설치·운영하는 것은 그 설치지역과 운영방법 등에 따라 개인의 초상 그 자체뿐만 아니라 특정시간에 어디서 어떤 모습으로 누구와 함께 있었는지 등에 관한 개인정보를 취득하는 것이며, 설치·작동 방법에 따라서는 개인의 사생활 영역내의 모습을 녹화·저장하는 것도 가능하다. 따라서, CCTV 등 무인단속장비의 설치·운영은 촬영되는 사람들에 대하여 초상권과 개인정보자기결정권(헌법 제10조), 사생활, 가정, 주거의 자유와 이를 법으로 보호받을 수 있는 권리(헌법 제17조, 시민적및정치적권리에관한국제규약 제17조294)를 제한하고 침해할 수 있다(국가인권위원회, 2004a).

즉 CCTV로 정보주체를 촬영하고 그 이미지를 저장하는 것은 개인의 권리에 영향을 미치는 행위이다. 개인의 영상정보에 대한 수집·처리에서 배제될 권리를 부당히 제한하고 자기정보에 대한 통제를 무력화할 수 있을 뿐만 아니라 해당지역의 주민이 사생활내용을 공개당하지 아니할 자유가 침해될 개연성이 높다(행정안전부, 2008a: 118). 특히 범죄예방을 목적으로 24시간 CCTV로 거리를 촬영할 경우 국민을 잠재적 범죄자로 취급하는 것이 될 뿐만 아니라, 개인의 일상에 관한 정보를 무차별적으로 수집하는 것이 된다(권건보, 2009: 23).

일반 시민들이 CCTV에 대해 가지고 있는 인식은 양면성을 가지고 있다. 일면적으로는 CCTV가 설치된 것을 보면 안심된다는 생각으로 범죄예방을

위해 사생활에 대한 권리를 유보할 수 있다는 인식이 존재한다(제4장 제1절 참조). 하지만 국가인권위원회에 CCTV에 대한 진정 및 상담 등이 꾸준하게 제기되는 현황을 보면, CCTV로 인한 권리 침해를 우려하는 시각도 상당하다고 볼 수 있다.

<표 3-1> 국가인권위원회 CCTV 관련 민원현황

(2009년 8월 말 현재)

| 연도별 | 합계 | 진정 | 상담 | 민원 | 안내 |
|---|---|---|---|---|---|
| 합 계 | 1,015 | 409 | 399 | 102 | 105 |
| 2001년 | 1 | 1 | 0 | 0 | 0 |
| 2002년 | 8 | 7 | 0 | 1 | 0 |
| 2003년 | 27 | 16 | 5 | 3 | 3 |
| 2004년 | 83 | 53 | 14 | 6 | 10 |
| 2005년 | 131 | 52 | 38 | 21 | 20 |
| 2006년 | 124 | 30 | 50 | 18 | 26 |
| 2007년 | 194 | 73 | 72 | 19 | 30 |
| 2008년 | 221 | 85 | 96 | 18 | 22 |
| 2009년 | 238 | 92 | 124 | 16 | 6 |

자료: 국가인권위원회.[200]

### 2) 법적 근거

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

그러나 2007년 11월까지 CCTV에 대한 어떠한 법률적 규제도 존재하지 않았다. CCTV 등 무인단속장비를 설치·운영하여 범죄 수사 등에 활용하는 것이 국회가 제정한 법률이 아니라 지방자치단체나 경찰서장의 재량에 의하고 있었던 것이다. 이에 CCTV의 성능이 점차 향상돼 국민의 기본권을 침해할 수 있다는 우려가 늘어감에 따라 CCTV 설치·운영에 필요한 사항 및 개

200) '인권위 CCTV 관련 민원현황'에 대한 국가인권위원회의 정보(공개) 결정통지서 (2009.11.02). 문서번호: 행정법무담당관-2345 (2009.11.02).

인의 화상정보 보호를 위한 사항을 법률에 규정하여 국민의 권리를 보호할 필요가 있다는 문제제기가 이어졌다.

국가인권위원회는 2004년 4월 국회의장과 행정자치부 장관에게, 지방자치단체, 경찰청 등에서 설치·운영하고 있는 범죄예방 및 범죄수사를 위한 CCTV 등 무인단속장비의 설치·운영에 관한 법적 기준을 마련할 것을 권고하였다(국가인권위원회, 2004a). 또한 같은 이유로 CCTV에 대한 규정을 포함한 2개 법률이 발의되어 국회에서 논의되었다.[201]

마침내 2007년 11월 처음으로 「공공기관의 개인정보보호에 관한 법률」(이하 「공공기관개인정보보호법」)에 CCTV에 대한 규정이 삽입되었고, 이 법률은 공공기관 CCTV 설치·운영에 관한 일반적인 규제 법률로 오늘에 이른다.[202]

「공공기관의 개인정보보호에 관한 법률」
제4조의2 (폐쇄회로 텔레비전의 설치 등) ①공공기관의 장은 범죄예방 및 교통단속 등 공익을 위하여 필요한 경우에 「행정절차법」 제2조제6호에 따른 공청회(이하 "공청회"라 한다) 등 대통령령으로 정하는 절차를 거쳐 관련 전문가 및 이해관계인의 의견을 수렴한 후 폐쇄회로 텔레비전을 설치할 수 있다.
②설치된 폐쇄회로 텔레비전은 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추어서는 아니 되며, 녹음기능은 사용할 수 없다.
③공공기관의 장은 폐쇄회로 텔레비전을 설치하는 경우 정보주체가 이를 쉽게 인식할 수 있도록 다음 각 호의 사항을 기재한 안내판을 설치하는 등 필요한 조치를 취하여야 한다.
1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자 및 연락처
④국가안전보장과 관련된 국가중요시설 중 원자력발전소 등 대통령령으로 정하는 시설에 대하여는 제3항을 적용하지 아니할 수 있다.
⑤폐쇄회로 텔레비전의 설치, 안내판 설치 등에 관하여 필요한 사항은 대통령령으로 정한다.
[본조신설 2007.5.17]

---

201) 「공공기관의 개인정보보호에 관한 법률중 개정법률안(김재경의원 대표발의안, 의안번호 제171070호)」, 「공공기관의 폐쇄회로 텔레비전 설치 및 개인의 화상정보 보호에 관한 법률안(김충환의원 대표발의안, 의안번호 제171287호)」.

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

제4조의3 (폐쇄회로 텔레비전의 설치 및 관리에 대한 위탁) ①공공기관의 장은 폐쇄회로 텔레비전의 설치 및 관리에 관한 사무를 위탁할 수 있다.
②제1항에 따른 수탁기관의 자격요건, 위탁절차 등에 관하여 필요한 사항은 대통령령으로 정한다.
[본조신설 2007.5.17]

위 법률이 시행되기 전까지는 2007년 5월 시점으로 11만여 대에 달하는 것으로 산출되었던 공공기관 CCTV를 규제할 수 있는 법률적 규범이 전혀 존재하지 않았다(행정자치부, 2007). CCTV를 통해 개인정보를 수집하고 이용하는 과정에서 개인정보 보호가 제대로 이루어지지 않은 것이다. 이 사실은 법 시행 직후에 실시된 정부의 자체 조사 결과에서도 잘 드러난다. 많은 공공기관 CCTV가 설치사실을 공지하지 않은 채 운영되고 있었고, 개인정보 제공에 대해 대장을 작성하지 않았으며, 「통신비밀보호법」에서 금지하고 있는 음성녹음기능을 사용하고 있는 경우도 있었다(행정안전부 개인정보보호팀, 2008).[203]

현재 위 법률에 더하여 보다 구체적인 공공기관 CCTV에 대한 규정으로서 「공공기관 CCTV 관리 가이드라인」이 존재한다. 그밖에 CCTV 설치와 관련한 규정을 두고 있는 특별한 법률은 아래와 같다.

<표 3-2> CCTV 관련 법률

(2009년 9월말 현재)

| 법률 | | CCTV 관련 규정 |
|---|---|---|
| 공공영역 | 형의 집행 및 수용자의 처우에 관한 법률 시행규칙 | 제162조(영상정보처리기기 설치) ① 영상정보처리기기 카메라는 교정시설의 주벽(주벽)·감시대·울타리·운동장·거실·작업장·접견실·전화실·조사실·진료실·복도·통용문(통용문), 그 밖에 법 제94조제1항에 따라 전자장비를 이용하여 계호하여야 할 필요가 있는 장소에 설치한다.<br>② 영상정보처리기기 모니터는 중앙통제실·관구실 그 밖에 교도관이 계호하기에 적정한 장소에 설치한다.<br>③ 거실에 영상정보처리기기 카메라를 설치하는 경우에는 용변을 보는 하반신의 모습이 촬영되지 아니하도록 카메라의 각도를 한정하거나 화장실 차폐시설을 설치하여야 한다. |

203) 개정된 법률 시행일시는 2007년 11월 18일이었고 조사 기간은 2008년 1월 24일부터 1월 30일이었다. 당시 조사결과는 14개 공공기관 12,778대의 CCTV를 대상으로 이루어졌을 뿐이지만, “안내판 설치 64%, 음성 녹음 1.3%” 등 많은 문제점을 드러내었다.

| | | |
|---|---|---|
| | 외국인 보호규칙 | 제37조(안전대책)<br>②소장[출입국관리사무소장·출장소장 또는 외국인보호소장]은 예산의 범위 내에서 제1항의 규정에 의한 안전대책에 필요한 시설을 하여야 하며 폐쇄회로영상장치 등의 장비를 설치할 수 있다. |
| | 아동복지법 | 제9조의2 (아동보호구역에서의 폐쇄회로 텔레비전 설치 등) ① 국가와 지방자치단체는 유괴 등 범죄의 위험으로부터 아동을 보호하기 위하여 필요하다고 인정하는 때에는 다음 각 호의 어느 하나에 해당되는 시설의 주변구역을 아동보호구역으로 지정하여 폐쇄회로 텔레비전을 설치하거나 그 밖의 필요한 조치를 할 수 있다.<br>1. 「유아교육법」 제2조에 따른 유치원, 「초·중등교육법」 제38조 및 제55조에 따른 초등학교 또는 특수학교<br>2. 「영유아보육법」 제10조에 따른 보육시설<br>3. 「도시공원 및 녹지 등에 관한 법률」 제15조에 따른 도시공원<br>② 제1항에 따른 아동보호구역의 지정기준 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.<br>③ 이 법으로 정한 것 외에 폐쇄회로 텔레비전의 설치 등에 관한 사항은 「공공기관의 개인정보보호에 관한 법률」에 따른다. |
| | 도로교통법 | 제87조 (권한의 위임에 따른 주차단속의 특례 등)<br>②특별시장·광역시장이 제1항에 따라 주차위반사실을 직접 적발·단속한 때에는 행정안전부령이 정하는 과태료부과대상차표지(제13조 제1항에 따른 과태료 또는 범칙금 부과 및 견인대상차 표지를 포함한다. 이하 같다)를 붙인 후 그 표지가 붙은 해당 차를 촬영한 사진·비디오테이프나 그 밖의 영상기록매체(이하 "사진증거"라 한다) 또는 무인단속장비에 의하여 해당 차를 촬영한 사진증거 등의 증거자료와 위반장소·위반내용 및 차량번호 등을 기재한 서류를 갖추어 위반장소를 관할하는 구청장 또는 군수에게 통보하여야 한다. <개정 2008.2.29> |
| | 국회에서의 중계방송 등에 관한 규칙 | 제11조(폐쇄회로 시스템) 의장은 본회의 및 예산결산특별위원회등 국회의 주요 의사진행과정을 국회구내에서 시청하고 음성 및 영상자료를 중계방송용으로 제공할 수 있도록 하는 폐쇄회로시스템을 연차적으로 개발·추진하여야 한다. |
| | 지하공공보도시설의 결정·구조 및 설치기준에 관한 규칙 | 제12조 (부대시설의 종류 및 설치기준) 지하공공보도시설에 설치하여야 하는 부대시설의 종류 및 설치기준은 다음과 같다.<br>2. 중앙방재실은 다음 각 목의 기준에 적합하게 설치할 것<br>다. 민방위기관·소방기관·경찰기관·가스사업자 및 지하역 방재기관(지하역과 접속되는 경우에 한한다) 등 관계 기관과 유무선 교신이 가능한 설비와 자체 감시카메라(CCTV) 설비를 갖출 것 |
| 민간영역 | 근로자참여 및 협력증진에 관한 법률 | 제20조 (협의 사항) ① 협의회[노사협의회]가 협의하여야 할 사항은 다음 각 호와 같다.<br>14. 사업장 내 근로자 감시 설비의 설치 |
| | 공중위생관 | [별표 1] |

| | | |
|---|---|---|
| | 리법 시행규칙 | 사. 목욕실·발한실 및 탈의실 외의 시설에 무인감시카메라(CCTV)를 설치할 수 있으며, 무인감시카메라를 설치하는 경우에는 반드시 그 설치여부를 이용객이 잘 알아볼 수 있게 안내문을 게시하여야 한다. |
| | 주차장법 시행규칙 | 제6조(노외주차장의 구조 및 설비기준)<br>10. 주차대수 30대를 초과하는 규모의 자주식 주차장으로서 지하식 또는 건축물식에 의한 노외주차장에는 관리사무소에서 주차장 내부 전체를 볼 수 있는 폐쇄회로 텔레비전 및 녹화장치를 포함하는 방범설비를 설치·관리하여야 하되, 다음 각 목의 사항을 준수하여야 한다.<br>가. 방범설비는 주차장의 바닥면으로부터 170센티미터의 높이에 있는 사물을 식별할 수 있도록 설치하여야 한다.<br>나. 폐쇄회로텔레비전과 녹화장치의 모니터 수가 일치하여야 한다.<br>다. 선명한 화질이 유지될 수 있도록 관리하여야 한다.<br>라. 촬영된 자료는 컴퓨터보안시스템을 설치하여 1월 이상 보관하여야 한다. |
| | 폐광지역개발 지원에 관한 특별법 시행령 | 제14조(카지노업의 영업에 관한 제한 등)<br>②카지노사업자는 호텔의 내부 및 외부의 주요 지점에 폐쇄회로 텔레비전을 설치·운영하여야 한다. |
| | 관광진흥법 | 제28조(카지노 사업자 등의 준수사항)<br>②카지노사업자는 카지노업의 건전한 육성·발전을 위하여 필요하다고 인정하여 문화체육관광부령으로 정하는 영업준칙을 지켜야 한다. 이 경우 그 영업준칙에는 다음 각 호의 사항이 포함되어야 한다.<br>4. 전산시설·환전소·계산실·폐쇄회로의 관리기록 및 회계와 관련된 기록의 유지 의무 |

자료: 행정안전부(2009a: 13) 보완.

한편, 2009년 9월 시점으로 250만 대로 추산되는 민간 영역의 CCTV를 종합적으로 규제하는 법률은 지금까지 제정된 바 없다(행정안전부, 2009c). 다만 최근 몇 년 동안 개인정보보호법 제정에 대한 논의가 이루어지면서 관련 법률안에서 CCTV에 대한 규정이 포함되어 왔다. 개인정보보호법이 제정되면 민간 영역 CCTV에 대한 일반적인 규제가 가능해질 것으로 기대된다. 2009년 10월 현재 국회에 계류되어 있는 개인정보보호법안들에서 규정하고 있는 CCTV 관련 내용들은 다음과 같다.

<표 3-3> 국회 발의 중인 개인정보보호법안 중 CCTV 관련 규정

(2009년 9월 말 현재)

| 구 분 | 내 용 |
|---|---|
| 이혜훈의원 대표발의 (의안번호 : 제1800570호) | 제14조(개인정보수집장치의 이용 제한) ① 개인정보처리자는 개인정보를 수집·처리하는 장치 또는 기기(이하 “개인정보처리장치”라 한다)를 설치하여 불특정 다수의 개인정보를 수집·처리하고자 하는 때에는 정보주체가 그 사실을 쉽게 알 수 있도록 대통령령으로 정하는 바에 따라 게시, 고지 등의 필요한 조치를 취하여야 한다.<br>② 개인정보처리장치를 설치·운영하는 개인정보처리자는 대통령령으로 정하는 바에 따라 개인정보처리장치 운영·관리지침을 정하여 게시 또는 공개하고 정보주체의 요구가 있는 때에는 이를 열람(사본의 교부를 포함한다. 이하 같다)할 수 있게 하여야 한다.<br>③ 개인정보보호위원회는 정보주체의 권리를 보호하기 위하여 필요하다고 인정하는 경우에는 개인정보처리장치의 종류, 설치목적, 설치장소 등에 따라 설치 및 운영의 절차, 방법 등에 관한 세부적인 사항을 정하여 고시할 수 있다.<br>④ 개인정보처리자가 제1항부터 제3항까지의 조치·절차·방법 등을 이행한 경우에는 제6조에 따른 개인정보취급방침의 공개의무, 제8조제1항에 따른 고지 및 동의 획득 의무를 면제한다.<br>⑤ 제1항에 따른 개인정보처리장치의 종류는 대통령령으로 정한다. |
| 변재일의원 대표발의 (의안번호: 제1801598호) | 제18조(자동정보처리장치를 통한 처리 제한) ① 자동화된 방법으로 개인정보를 처리하거나 정보주체를 감시·추적할 수 있는 장치 또는 기기(이하 “자동정보처리장치”라 한다)를 설치·운영하고 하는 자는 대통령령으로 정하는 바에 따라 정보주체가 그 사실을 쉽게 알 수 있게 하여야 한다. 다만, 정보주체에게 그 사실을 알리는 것이 자동정보처리장치의 설치·운영 목적을 달성하는데 현저한 지장을 미칠 우려가 있는 경우로서 대통령령으로 정하는 경우에는 그러하지 아니할 수 있다.<br>② 개인정보처리자가 제1항에 따라 자동정보처리장치를 이용하여 개인정보를 처리하는 때에는 대통령령으로 정하는 바에 따라 자동정보처리장치의 설치·운영 내역 등을 기록·관리하고 공개하여야 한다.<br>③ 개인정보보호위원회는 자동정보처리장치의 용도, 설치금지 구역, 설치 절차 및 방법, 이용 방법 및 조건, 수집된 정보의 보호 및 폐기 그 밖에 정보주체의 사생활 보호를 위하여 필요한 사항을 정하여 고시할 수 있다.<br>④ 개인정보처리자가 제1항에 따라 자동정보처리장치의 설치·운영 사실을 알린 경우에는 제7조제1항에 따른 수집·이용에 대한 동의 의무와 제10조제1항의 고지·설명 의무를 면제하고, 제2항에 따라 설치·운영 내역 등을 공개하는 경우에는 제12조에 따른 개인정보취급방침의 공개 의무를 면제한다.<br>⑤ 자동정보처리장치의 범위 또는 종류는 대통령령으로 정한다. |
| 정부제출 | 제24조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호 |

| | |
|---|---|
| (의안번호: 제1802369호) | 의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영해서는 아니 된다.<br>1. 법령에서 구체적으로 허용하고 있는 경우<br>2. 범죄의 예방 및 수사를 위하여 필요한 경우<br>3. 시설안전 및 화재 예방을 위하여 필요한 경우<br>4. 교통단속을 위하여 필요한 경우<br>5. 그 밖에 대통령령으로 정하는 공익적 목적을 위하여 필요한 경우<br>② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영해서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.<br>③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장은 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.<br>④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기 운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 대통령령으로 정하는 바에 따라 안내판 설치 등 필요한 조치를 하여야 한다. 다만, 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.<br>⑤ 영상정보처리기기 운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.<br>⑥ 영상정보처리기기 운영자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 영상정보처리기기의 운영·관리 지침을 마련하고 제27조에 따라 안전성 확보에 필요한 조치를 하여야 한다.<br>⑦ 영상정보처리기기 운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다. |

본 연구는 현재 국가가 「공공기관개인정보보호법」과 관련 가이드라인에 의해 일반적으로 설치·운영하고 있는 CCTV를 일차적인 대상으로 한다.

<표 3-4> 공공기관 CCTV의 설치목적별 현황

(2009년 4월 말 현재)

| 설치목적(비율) | 대 수 | 비 고 |
|---|---|---|
| 합 계 | 241,415 | |
| 공공안전 (27%) | 65,597 | 방범, 재난·산불관리 등 |

| | | |
|---|---|---|
| 사회질서유지 (6%) | 14,769 | 과속, 주정차 단속 등 |
| 일반시설관리 (34%) | 81,136 | 시설 및 주차관리 등 |
| 특수시설관리 (24%) | 59,143 | 지하철・공항시설관리 등 |
| 기타 (9%) | 20,770 | 기타 |

자료: 행정안전부.[204]

2009년 4월 현재 방범, 재난・산불관리, 과속・주정차 단속, 시설・주차 관리, 지하철・공항시설관리 등으로 전국에 총 241,415대의 공공기관 CCTV가 설치・운영중이다. 이중 프라이버시와 밀접한 목적으로 설치된 것이 방범용 CCTV로서,[205] 지역별로는 서울에 집중적으로 설치되어 있다. 본 연구는 특히 서울 자치구에서 설치한 방범용 CCTV의 실태를 집중적으로 분석하였다.

<표 3-5> 지방자치단체 방범용 CCTV 설치 현황

(2009년 4월 기준)

| 기관명 | 설치대수 | 기관명 | 설치대수 |
|---|---|---|---|
| 서울특별시 | 4,062 | 경기도 | 2,422 |
| 부산광역시 | 292 | 강원도 | 325 |
| 인천광역시 | 861 | 충청북도 | 315 |
| 대전광역시 | 123 | 충청남도 | 691 |
| 울산광역시 | 112 | 경상북도 | 827 |
| 대구광역시 | 926 | 경상남도 | 846 |
| 광주광역시 | 88 | 전라북도 | 447 |
| 제주특별자치도 | 20 | 전라남도 | 845 |

자료: 행정안전부.[206]

---

204) '공공기관 CCTV 관련 정보공개 청구'에 대한 행정안전부의 정보(공개) 결정통지서 (2009.7.23). 문서번호: 개인정보보호과-2405 (2009.07.23).

205) 방범용 CCTV는 "주로 차량을 촬영하는 교통관련 CCTV나 한정된 지역을 촬영하는 쓰레기 무단투기 단속용 CCTV와는 달리 주택가 골목길등 비교적 넓은 공간을 사람에 초점을 맞춰 감시하기 때문에 그만큼 프라이버시 침해 소지가 많"다(함께하는 시민행동, 2003b). "CCTV의 설치와 그 자료의 범죄수사에의 활용은 국민의 프라이버시권 중 특히 일반적 행동자유권을 침해하면서, 국가를 벤담, 푸코, 오웰 등이 염려했던 감시국가로 만들 수 있다"(임지봉, 2007).

206) '공공기관 CCTV 현황'에 대한행정안전부의 정보(공개) 결정통지서(2009.10.30). 문서번호: 개인정보보호과-3457 (2009.10.30).

## 2. 개인정보의 수집・유통 실태

### 1) CCTV의 설치

공공기관 CCTV를 통한 개인정보의 수집은 필요최소한으로 이루어져야 한다. 이는 「공공기관개인정보보호법」에서 개인정보보호의 원칙에 대한 일반적인 서술 규정에 명시된 바 대로이다.

「공공기관의 개인정보보호에 관한 법률」
제3조의2 (개인정보보호의 원칙) ①공공기관의 장은 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 아니 된다.
②공공기관의 장은 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 한다.
③공공기관의 장은 개인정보관리의 책임관계를 명확히 하여야 한다.
④공공기관의 장은 개인정보의 수집・활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다.

행정안전부의 「공공기관 CCTV 관리 가이드라인」에서는 보다 구체적으로 개인화상정보의 보호원칙으로 네 가지를 제시하고 있다. 첫째, 공공기관의 장은 CCTV의 설치목적에 부합하는 필요최소한의 범위 안에서 화상정보를 수집하여야 한다. 둘째, 공공기관의 장은 설치목적을 정보주체가 명확히 인식할 수 있도록 하여야 하며, 화상정보를 그 목적 이외의 용도로 활용하여서는 아니된다. 셋째, 공공기관의 장은 화상정보의 정확성 및 최신성을 확보하여 이를 안전하게 관리하도록 노력하여야 한다. 넷째, 공공기관의 장은 화상정보의 취급에 관한 일반사항을 공개하고, 화상정보에 대한 정보주체의 권리를 보장하여야 한다(동가이드라인 제4조).

이처럼 CCTV를 통한 개인정보의 수집을 목적내로 최소화할 것을 명시한 것은 CCTV가 일단 설치된 후에 매우 광범위한 규모로 다양한 개인정보를 수집하는 개인정보 자동수집장치이기 때문이다. 구 정보통신부의 「CCTV 개인영상정보보호 가이드라인」에서는 CCTV를 설치할 때 “정보주체의 초상권, 사생활의 비밀과 자유 등의 침해할 위험이 없는지를 사전에 분석・검토하여 이를 최소화할 수 있는 수단을 강구하여야 한다”고 하였으며, “특정인을 감시할 목적으로” CCTV를 설치해서는 안된다고 명시하였다(동가이드라인 제4조).[207]

CCTV가 엄격하게 설치 목적 내로 운영되도록 하려면, 설치 후 규제도 중요하지만 CCTV를 필요최소한으로 설치하도록 사전적으로 규제하는 것이 무엇보다 중요하다.

국가인권위원회는 CCTV 등 무인단속장비의 설치와 운영이 법률에 근거를 두더라도 그 내용이 명확하고 상세하지 않으면 이 역시 국민의 기본권에 대한 과잉 제한이 되므로, 범죄예방과 범죄수사의 효율성을 높이기 위한 원칙적이고 일반적인 조처들이 검토되고 강구된 후 그러한 조처들로도 범죄예방과 수사라는 목적을 효율적으로 달성할 수 없는 "필요한 경우에 한하여" 동원되는 보충적 수단임을 명확히 해야 한다고 지적한 바 있다(국가인권위원회, 2004a).

그러나 실제로 공공기관 CCTV가 필요최소한으로 설치되는지는 의문이다. 법률에 그 설치 사유를 '범죄예방 및 교통단속 등 공익을 위하여 필요한 경우'라고 규정하여 매우 폭넓게 인정하고 있기 때문이다(동법 제4조의2 제1항). 법률이 규제 대상으로 삼고 있는 것이 '공익을 위하여' 업무를 수행하는 공공기관인 만큼 사실상 공공기관 CCTV의 설치에 대한 사유 제한은 없는 것이나 마찬가지이다. 이러한 상황에서 실제로 개별 공공기관이 CCTV 설치 여부를 결정할 때 그 사유나 목적이 고려되기는 어려울 것이고, 오히려 구축이나 운영비용 등 동원할 수 있는 자원의 문제가 중점적인 고려 사항이 될 수 밖에 없다.[208]

구 정보통신부의 「CCTV 개인영상정보보호 가이드라인」에서는 관련 법령에 명시적인 규정이 있는 경우를 제외하고는 범죄예방 및 증거확보, 시설안전 및 화재예방, 출입통제, 아동의 보호를 위해서만 CCTV 설치를 허용하였으며, 욕실·화장실·탈의실 등 정보주체의 사생활이 엄격하게 보호되어야 하는 장소에는 CCTV 설치를 금지하였다(동가이드라인 제5조). 이 가이드라인이 설치가 금지되는 장소를 구체적으로 제시하는 이유는, 사전에 CCTV로 인한 정보주체의 권리 침해를 최소화할 수 있는 수단을 강구하도록 하기 위

---

207) 캐나다 비디오감시가이드라인(Guidelines for the Use of Video Surveillance of Public Places by Police and Law Enforcement Authorities)에서는 CCTV가 "현존하는 실질적 문제에 대응하기 위해서만 설치되어야" 하며, "프라이버시 침해를 대체할 만한 수단이 없을 때에만 예외적으로 시행되어야" 하고, "시행 이전에 프라이버시에 대한 영향평가가 이루어져야" 한다고 명시하고 있다(정보통신부, 2007: 35).

208) 이와 관련하여 2009년 국회 행정안전위원회 국정감사에서 "CCTV의 증가률이 범죄취약지역 또는 범죄 발생률이 높은 지역에 대한 사전 조사·분석 후 반영된 것이 아니라 지역의 재정상태와 주민요구에 의한 것이라 실효성 논란이 되고 있다."는 지적이 나오기도 하였다(강기정, 2009).

한 것이다.[209] 이와 비교해볼 때, 현행 법률이 CCTV 설치 자체를 금지하는 규정이나 그 기준을 정하지 않은 것은 불충분한 입법이라는 비판을 피할 수 없다. 자칫하면 그러한 법적 규제가 CCTV의 설치를 사실상 추인하는 근거로만 사용될 수 있기 때문이다.

「공공기관개인정보보호법」은 CCTV 설치 목적 규제 상의 약점을 보완하는 절차로서 CCTV 설치에 앞서 공청회 등을 통해 관련 전문가 및 이해관계인의 의견수렴을 하도록 하였다(동법 제4조의2 제1항). 시행령에서는 다음과 같이 비교적 구체적으로 사전 의견수렴 절차를 규정하였다.

「공공기관의 개인정보보호에 관한 법률 시행령」
제4조 (폐쇄회로 텔레비전의 설치) 법 제4조의2제1항에 따라 폐쇄회로 텔레비전을 설치하려는 공공기관의 장은 다음 각 호의 구분에 따른 방법으로 관련 전문가 및 이해관계인의 의견을 수렴하여야 한다.
1. 일반인의 자유로운 출입이 제한되는 시설(제2호에 해당하는 시설은 제외한다) 또는 장소 안에 설치하는 폐쇄회로 텔레비전: 해당 시설을 이용하는 공무원 또는 임직원 등의 대표로 구성되는 위원회의 심의를 거치는 방법
2. 제4조의2제3항 각 호의 시설에 설치하는 폐쇄회로 텔레비전: 개인정보보호에 관하여 해당 시설의 관리자·보안책임자 또는 관련 전문가의 의견을 듣는 방법
3. 제1호 또는 제2호 외의 시설 또는 장소에 설치하는 폐쇄회로 텔레비전: 다음 각 목의 어느 하나에 해당하는 방법
가. 「행정절차법」에 따른 행정예고의 실시 또는 공청회의 개최
나. 그 밖에 해당 폐쇄회로 텔레비전의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사·여론조사 등의 실시
[전문개정 2007.11.13]

그러나 이러한 절차를 통해 실제로 CCTV 도입이 중단된 사례가 보고된 바는 없다. 일차적으로 CCTV를 설치하려는 주체인 공공기관이 주도하는 의견수렴 과정에서 지역 주민들의 반대 의견을 적극적으로 수용하기 어렵기 때문이다. 주민들 입장에서는 문서로 된 고지나 동의 절차 없이 CCTV 설치

209) 이 가이드라인에 따르면 호주 CCTV 운용지침(Guidelines for the Establishment and Implementation of CCTV in Public Places)에서는 CCTV 설치 허용장소를 그 설치목적과 연계하여 우범지역, 은행 및 현금인출기, 버스 및 택시정류소, 주차장, 기차역, 공공화장실, 전화부스 등 지역의 공공시설 및 노약자 위험지역 등 구체적으로 한정하였다(정보통신부, 2007: 40). 미국 워싱턴 D.C.의 경우 주거지나 상업지역의 개방공간에 CCTV를 설치하려면, 그곳에서 특정범죄가 자행되고 있고 감시가 범행의 탐지나 억제에 기여한다고 판단되는 경우에만 허용되며 적합성요건의 구체화를 통해 허용된 목적의 범위 내에서만 CCTV 감시조치가 이루어질 수 있다(권건보, 2009: 9).

사실을 사전에 인지하는 것도 쉽지 않다. 따라서 CCTV의 설치 여부를 주민들의 의견에 따라 결정한다는 취지의 '의견 수렴'이 사실상 형식적으로 이루어질 가능성이 높은 것이다.

실제로 본 연구에서 서울시 자치구를 대상으로 방범용 CCTV 설치 과정에서 주민 의견수렴과정에 대하여 조사한 결과, 대개가 홈페이지 등을 통한 행정예고 등의 방법으로 안내하거나 소극적인 설문조사를 하는 데 그치고 있었다. 다수 주민들의 동의서를 받거나 공청회와 같이 비교적 적극적인 여론수렴 절차를 거친 자치구는 소수에 불과하였다.[210]

<표 3-6> 방범용 CCTV 설치시 의견수렴 방법 (서울 자치구)

| 구분 | 의견수렴 방법 |
|---|---|
| 소극적 | 행정예고, 통반장이나 동주민센터를 통한 여론수렴, 설문조사 |
| 비교적 적극적 | 주민공청회 3회 개최·카메라 가시거리 50m 내 모든 세대 설치동의서 수령(중랑구), 반경 50m이내 적극적 주민 설문조사(은평구), 상세한 설치내역 안내(용산구), 14,650명의 주민에 대한 의견수렴(강서구), 당해 장소 인근 주민의 2/3이상 동의(성동구) |

자료: 각 자치구.[211]

비교적 적극적인 의견수렴 과정을 거친 것으로 평가되는 자치구조차도, 의견수렴에 사용된 서면 양식들을 살펴보면 주민들의 권리를 충분히 행사하기에 부족한 측면이 있었다. 즉, CCTV의 구체적인 성능, 정보주체의 권리행사 방법, 개인정보의 관리 및 이용 범위 등 구체적 사항에 대한 고지가 누락된 채 단순 찬반을 묻는 형식에 그쳤으며, 이러한 형식으로는 정보주체가 CCTV 설치로 인해 자신들에게 미치는 영향을 정확히 인식하고 동의권을 행사하기에 부족해 보였다.[212]

---

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

211) '지방자치단체 CCTV 관련 정보공개 청구'에 대한 서울 각 자치구의 정보(공개) 결정통지서(2009.7.20~2009.8.13).

212) "우리나라 공공장소 CCTV 설치를 해당지역주민의 80% 이상이 찬성하고 있다는 사실을 들며 CCTV 설치의 정당성을 이야기하는 입장이 있다. 그러나, 이것은 제대로 된 주민의견으로 볼 수 없는 면도 있다. CCTV 설치에 대한 주민의견을 물으려면, CCTV 설치의 좋은 점과 함께 통행인의 프라이버시권 침해를 위시한 여러 가지 CCTV 설치의 나쁜 점에 대한 대국민 계도도 있어야 한다. 그것이 없이 범죄 감소 등

<그림 3-1> 주민설문 조사서 (은평구)

## 방범용 CCTV 설치 주민설문 조사

안녕하십니까?

우리구에서는 각종 범죄로부터 주민의 생명과 재산을 보호하고 범죄 없는 안전한 은평을 만들기 위하여 서부·은평경찰서와 협력하여 범죄 취약지역에 방범용 CCTV를 설치 운영하고자 합니다.

이에 귀하의 사생활 및 초상권에 침해 가능성이 있어 의견을 구하니 **작성하신 후 회송용 봉투에 넣어 우체통에 투입하여 주시기 바랍니다.**

☞ 조사기간 : 2008. 3. 10 ~ 3. 21

**※ 방범용 CCTV 설치 예정지역의 설문조사 참여자 중 2/3 이상의 동의가 없으면 "해당없음" 으로 간주하여 다른 지역으로 이동 설치됩니다.**

2008년 3월

서 울 특 별 시 은 평 구 청 장

※ 본 설문조사는 세대별로 한 분만 참여하실 수 있으며, 아래의 개인정보 및 답변사항은 은평구 방범용 CCTV 설치를 위한 기초자료 이외에는 이용되지 않을 것이오니, 주민 여러분의 적극적인 참여를 부탁드립니다.

① 성 명 : _____ ② 성 별 : 남, 여

③ 주 소 : _____ 동 _____ 번지 _____ 호

**1. 범죄로부터 주민을 보호하기 위하여 방범취약지점에 CCTV를 설치하고자 합니다.**

**설치예정위치 : _____ 동 _____ 번지 _____ 호 _____ 앞**

설치에 동의하십니까?

① 동의한다 ② 동의하지 않는다

**2. 기타 CCTV 설치에 대하여 좋은 의견이 있으시면 기재하여 주시기 바랍니다.**

---

CCTV 설치의 좋은 점만을 집중적으로 홍보한 뒤 실시한 주민의견조사의 결과는 제대로 된 주민의견으로 보기 힘든 점이 있다"(임지봉, 2007).

<그림 3-2> 주민 의견 조사서 (용산구)

## <후 방범용 CCTV 설치 의견 수렴

□ 설치 목적 : 범죄 발생 사전 예방 및 주민 체감치안도 제고

□ 방범용 CCTV 설치 개요

○ 설치기한 : ~ 2009. 6월

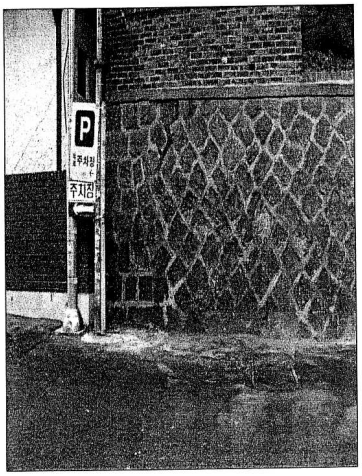
○ 설치내역

- 카메라(촬영), 함체(저장장치), 안내표지판
- 경광등, 비상벨, 스피커 → 비상시 경찰(지구대)과 직접 통화 가능

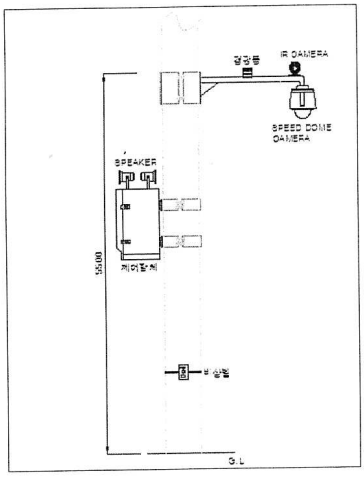
□ 기 타

○ 설치는 용산구청 자치행정과에서, 운영 및 모니터링은 경찰서(지구대)에서 담당

○ 활용 가능한 전신주가 없으므로 전용지주 설치




↑설치위치




↑설치도면

□ 설치 의견

| 성 명 | 주 소 | 설 치 의 견 | | 서명(인) |
|---|---|---|---|---|
| | | 찬 성 | 반 대 | |
| | | | | |

이는 일차적으로 법률이나 관련 가이드라인 어디에서도 CCTV 설치에 대한 주민들의 의사를 실질적으로 반영할 수 있는 의견수렴의 요건을 명확히 규정하지 않은데 따른 문제로 볼 수 있다.[213]

이 점과 관련하여, 과거 국가인권위원회에서는 CCTV 등 무인단속장비를 설치할 때 그로 인해 영향을 받는 이들에게 사전에 그 설치목적, 장소, 기기의 성능, 관리책임자(기관) 등의 내용에 대하여 충분히 고지하여야 한다고 권고한 바 있다. 동의를 구해야 하는 경우에는 동의의 절차, 대상 등에 대해 규정해야 한다고 하였다(국가인권위원회, 2004a). 국회에서도 공공기관 CCTV 관련 법률이 논의될 당시 적극적인 주민 의견수렴 절차가 검토되었지만 법률에 반영되지 않았다. 2005년 4월 행정자치위원회에서 검토된 「공공기관의 폐쇄회로 텔레비전 설치 및 개인의 화상정보 보호에 관한 법률안(김충환의원 대표발의안, 의안번호 제171287호)」에서는 CCTV를 설치하고자 하는 때 수집의 '법적 근거', '목적', '이용 범위' 및 '정보주체의 권리' 등에 관하여 '문서' 등을 통하여 미리 정보주체가 그 내용을 쉽게 확인 할 수 있도록 필요한 조치를 하고 정보주체의 '동의'를 얻을 수 있도록 하였다. 그러나 이 안은 CCTV 정보의 수집 대상이 불특정 다수인이기 때문에 정보주체에게 미리 동의를 얻거나 인식할 수 있게 하는 것이 방법상 어렵다는 이유로 반영되지 않았다.[214]

참고로, 행정안전부의 「공공기관 CCTV 관리 가이드라인」에서는 공공기관의 장이 CCTV 설치·운영 사항을 별도 규정 또는 지침을 수립할 때 △CCTV 설치의 목적, △CCTV시설 담당부서·책임관 및 연락처, △설치·운영되는 CCTV 카메라 대수·위치·성능 및 촬영범위, △안내판의 규격 및 부착장소, △정보주체의 권리행사 및 불복수단에 관한 내용·절차 및 방법, △CCTV 촬영시간, 화상정보의 보유기간, 화상정보의 보관·관리·삭제의 방법, 화상정보의 보관 장소, △CCTV에 의하여 전송되는 화상정보가 실제로

213) 관련하여, CCTV의 설치에 있어서 요구되는 전제조건에 대하여 '범죄예방 및 공익을 위하여 필요한 경우'라는 예시적 사항을 드는 것은 공공기관이 설치하는 CCTV가 지니는 관할로 인하여 한정적인 열거에 따른 제한적인 설정이 태생적으로 억제되어 있고 '행정절차법 소정의 공청회'를 절차적 필수사항으로 규정하고 있는 것은 행정처분이나 입법예고에 있어서 의견청취방식이 아니라 행정예고에 관한 공청회를 규정하고 있는 조항이 되어야 할 것으로 본다는 의견이 있다(이민영, 2007: 31).

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

열람・재생되는 장소 및 출입통제현황, △녹화된 화상정보를 제3자에게 제공하거나 열람・재생토록 할 수 있는 사유와 그 절차 및 방법을 포함하도록 권고하였다(행정안전부, 2009a: 13-14). 정보주체에 CCTV의 동의 여부를 물을 때도 CCTV 설치 및 운영에 관한 규정 또는 지침에 포함될 위 구체 사항들에 대한 정보제공이 함께 이루어지는 것이 바람직하다. 이러한 의견수렴의 내용적 요건 외에도 형식적 요건으로 다수 주민들의 동의서를 받거나 공청회와 같이 비교적 적극적인 여론수렴 절차를 규정할 필요가 있다. 더불어, 기설치된 CCTV에 대해서도 주민들의 동의 계속 여부를 물어 CCTV 설치를 지속할 것인지의 여부를 평가하는 절차가 모색될 필요도 있다.[215]

의견 수렴이 정보주체의 의사를 반영하기 위한 사전적인 조치라면, 사후적인 조치로는 안내판 설치를 들 수 있다. 법률에서는 공공기관의 장이 CCTV를 설치할 경우 설치목적 및 장소, 촬영범위 및 시간, 관리책임자 및 연락처를 기재한 안내판을 설치하여 정보주체가 이를 사후에 인식할 수 있도록 하였다(동법 제4조의2 제3항). 동시행령에서는 보다 구체적으로 안내판의 설치 요건을 명시하였다.

「공공기관의 개인정보보호에 관한 법률 시행령」
제4조의2 (안내판의 설치) ① 법 제4조의2제3항에 따라 공공기관의 장은 폐쇄회로 텔레비전을 설치한 장소마다 안내판을 설치하여야 한다. 다만, 공공기관의 건물 안에 다수의 폐쇄회로 텔레비전을 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 폐쇄회로 텔레비전 설치지역임을 표시하는 안내판을 설치할 수 있다.
② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치에 갈음하여 인터넷 홈페이지에 법 제4조의2제3항 각 호의 사항을 게재할 수 있다.
1. 원거리 촬영, 과속・신호위반단속 또는 교통흐름조사 등의 목적으로 폐쇄회로 텔레비전을 설치하는 경우로서 개인정보침해의 위험이 적은 경우
2. 산불감시용 폐쇄회로 텔레비전 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 이를 쉽게 알아볼 수 없는 경우
③ 법 제4조의2제4항에 따라 공공기관의 장은 다음 각 호의 어느 하나에 해당

215) 관련하여, 미국 워싱턴 D.C. 「공공장소와 안전에 관한 조례」에서 경찰서장은 해당 지역 주민들의 의견을 고려하여 CCTV를 통한 감시지속 여부를 결정해야 하며, 자신의 결정의 내용과 근거를 그들에게 공지・제시하여야 한다. 그리고 반년에 1회씩 주민회의에서 CCTV 감시의 최신현황을 보고하여야 하고, 매년 CCTV 감시체계 및 그 사용과 관련한 보고서를 제출하여야 한다. 법원의 허가를 받아 행한 감시의 경우 및 현안사건의 수사를 목적으로 행해진 경우에는 예외가 인정된다(권건보, 2009: 9).

하는 시설에 설치하는 폐쇄회로 텔레비전에 대하여는 안내판을 설치하지 아니할 수 있다. <개정 2008.9.22>
1. 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설
2. 「통합방위법」 제2조제13호에 따른 국가중요시설
3. 「보안업무규정」 제36조에 따른 보안목표시설

그러나 이 규정에서는 국가중요시설에 포괄적인 예외를 두었다. 그 결과 국가중요시설에 해당하는 정부중앙청사, 청와대, 국회, 대법원, 중앙행정기관 부·처 및 이에 준하는 기관, 중앙행정기관의 청 등 주요 공공기관에서 안내판을 설치하지 않아도 된다.[216]

### 2) CCTV 정보의 이용 및 제공

국가인권위원회에서는 CCTV의 이용 및 제공에 있어서 고려해야 할 점을 다음과 같이 지적하였다. 첫째, 목적 내 이용. 현재 우리나라에서 공공기관이 설치하고 있는 CCTV 등 무인단속장비의 용도는 크게 교통흐름 조사용, 교통법규위반차량 단속용, 방범용, 쓰레기무단 투기 단속용 등이 있다. CCTV 등 무인단속장비가 오용되는 것을 방지하기 위해서는 최초 설치된 목적 외 용도로 사용할 수 없도록 엄격히 규제해야 하며, 목적이 변경될 경우에는 새롭게 동의를 받는 등 오·남용의 가능성을 최소화해야 한다. 둘째, 임의의 조작 금지. 최근의 CCTV 등 무인단속장비는 상하좌우로 자유롭게 조작이 가능하며 가시거리가 몇 백미터에 이를 정도로 가시성능과 줌(Zoom)기능이 뛰

---

216) 국가중요시설 지정 및 방호 [제1057호, 국방부훈령, 2009.5.25]
제7조(국가중요시설의 분류기준)
① 국가 및 공공기관시설은 다음 각 호와 같이 분류한다.
1. 다음 각 목의 국가 및 공공기관시설은 "가"급으로 한다.
가. 청와대, 국회의사당, 대법원, 정부중앙청사
나. 국방부·국가정보원 청사
다. 한국은행 본점
2. 다음 각 목의 국가 및 공공기관시설은 "나"급으로 한다.
가. 중앙행정기관 각 부(部)·처(處) 및 이에 준하는 기관
나. 대검찰청·경찰청·기상청 청사
다. 한국산업은행·한국수출입은행 본점
3. 다음 각 목의 국가 및 공공기관시설은 "다"급으로 한다.
가. 중앙행정기관의 청사
나. 국가정보원 지부
다. 한국은행 각 지역본부
라. 다수의 정부기관이 입주한 남북출입관리 시설
마. 기타 중요 국·공립기관

어나다. 따라서 모니터링 과정에 범죄혐의가 있다고 의심할만한 상당한 이유가 있는 경우 외에는 화면에 잡힌 사람의 얼굴을 줌(Zoom) 기능을 이용하여 확대 촬영할 수 없도록 하거나, CCTV 등 무인단속장비가 공공 도로가 아닌 개인의 집안을 촬영할 수 없도록 회전 기능의 사용을 제한하는 규정을 둘 필요가 있다. 셋째, 제3자 제공 제한. CCTV 등 무인단속장비로 촬영된 녹화기록에는 개인의 초상 및 언제 어느 곳에 누구와 함께 있었는가에 관한 개인의 행적을 담고 있으며, 그 녹화기록물은 보유목적 외에 다른 행정목적이나 범죄 목적으로 사용될 가능성이 있으므로, 당사자의 동의나 적법한 근거에 따라서만 제3자에게 제공할 수 있도록 해야 한다. 넷째, 파기의 원칙. 보유기간에 대해서도 필요이상 오랜 기간 보유할 수 없도록 하고 수사나 재판자료로 사용되는 경우를 제외하고는 범죄예방이라는 목적과 무관함이 판명되는 대로 신속하게 정보를 파기하도록 해야 한다(국가인권위원회, 2004a).

「공공기관개인정보보호법」에서는 CCTV로 수집한 개인정보를 내부 또는 보유기관 외의 자에게 이용하게 하거나 제공하는 경우에도 법률에 근거하지 않고서는 보유목적 외의 목적으로 처리정보를 이용할 수 없다. 보유목적에 따라 이용·제공하는 경우에도 업무수행에 필요한 최소한의 범위로 그 이용 또는 제공을 제한해야 한다(동법 제10조). 폐쇄회로 텔레비전의 설치목적 범위를 넘어 카메라를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자와 거짓 그 밖의 부정한 방법으로 공공기관으로부터 처리정보를 열람 또는 제공받은 자는 2년 이하의 징역 또는 700만 원 이하의 벌금에 처한다(동법 제23조제3항).

「공공기관 CCTV 관리 가이드라인」에서는 개인화상정보를 이용하거나 제공하는 절차에 대하여 보다 상세하게 규정하였다. 즉, 화상정보를 이용하거나 제공받고자 하는 기관은 이용목적 및 이용하고자 하는 처리정보의 범위를 명시하여 보유기관의 장에게 문서로 요청하도록 하고, 보유기관의 장은 처리정보 이용·제공대장에 △개인정보파일의 명칭 △이용하거나 제공받는 기관의 명칭 △이용 또는 제공의 목적 △법령상 이용 또는 제공근거가 있는 경우 그 근거 △이용 또는 제공을 요청하는 정보의 항목 △이용 또는 제공의 주기 △이용 또는 제공의 형태 △이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간에 대해 기록하고 관리하도록 하였다(동가이드라인 제12조).[217]

---

217) 「공공기관 CCTV 관리 가이드라인」에서는 방송사에서 개인영상정보를 요청하는 경우에 대해서도 해설하고 있다(행정안전부, 2009a: 22). 「공공기관개인정보보호법」에서는 언론사에 개인영상정보를 제공하는 법적 근거를 찾을 수 없지만, 「방송심의에 관한 규정」에 의하여 일반인에 대한 방송은 당사자의 동의 없이 방송하여서는 아니된

서울 자치구들의 경우도 대개 이와 비슷한 내용의 CCTV 설치 및 운영 규정 혹은 지침을 인터넷 홈페이지를 통해 공개하고 있다.

<표 3-7> CCTV 설치 및 운영 규정 혹은 지침 인터넷 주소 (서울 자치구)
(2009년 10월 20일 기준)

| 자치구 | CCTV 설치 및 운영 규정 인터넷 주소 |
|---|---|
| 강남구 | http://www.gangnam.go.kr/global/sub01_01.jsp |
| 강동구 | http://www.gangdong.go.kr/pub/etc/etc01010101_protect.htm |
| 강북구 | http://www.gangbuk.seoul.kr/help/03/index.aspx |
| 강서구 | http://www.gangseo.seoul.kr/new_portal/mypage/main_14_1.jsp |
| 광진구 | http://www.gwangjin.go.kr/member/MMB_005.jsp |
| 구로구 | http://www.guro.go.kr/kor/page.jsp?code=heg020020000 |
| 금천구 | http://www.geumcheon.go.kr/main.do?pageKey=10020101#gc_080203 |
| 노원구 | http://www.nowon.kr/help/help.jsp?mid=101112 |
| 도봉구 | http://www.dobong.go.kr/07_site/sub04_01.asp |
| 동대문구 | http://ddm.go.kr/08util/sub07_01.html#03 |
| 동작구 | http://www.dongjak.go.kr/application/system/employer/content.wR?func=view&pid=72&idx=772 |
| 마포구 | http://www.mapo.go.kr/Design/html_cms/h_info/02_cctv.jsp |
| 서대문구 | http://www.sdm.go.kr/open_content/administrative/organization/status/cctvPolicy.jsp?mid=mn0604000000 |
| 서초구 | http://www.seocho.go.kr/site/sd/page.jsp?code=eta060030000 |
| 성동구 | http://www.sd.go.kr/main/main.do?op=mainSub&lay=5&mCode=1H010000000&displayId=010000 |
| 송파구 | http://www.songpa.go.kr/user.kdf?a=songpa.info.InformationPageApp&c=1006&tab=1&cate_id=BG0000000000 |
| 양천구 | http://www.yangcheon.go.kr/member/cctv_oper.asp |
| 영등포구 | http://ydp.go.kr/upload/etc/CCTV%EC%84%A4%EC%B9%98%EB%B0%8F%EC%9A%B4%EC%98%81%EC%A7%80%EC%B9%A8.pdf |
| 용산구 | http://www.yongsan.go.kr/pms/contents/contents.do?contseqn=927&decorator=pmsweb&menucdv=07010000 |
| 은평구 | http://www.eunpyeong.seoul.kr/cms.asp?code=M2000030 |
| 종로구 | http://www.jongno.go.kr/wcms4/page?pageId=564480867 |
| 중구 | http://www.junggu.seoul.kr/web/w06/w06080103.php |
| 중랑구 | http://jungnang.seoul.kr/html/help/kh02_0101.php |

다고 하였다. 피의자에 대한 개인영상정보를 제공하는 경우에는 개인정보 침해 가능성에 대해 충분한 논의를 거친 후에 제공여부를 결정하여야 한다.

그런데 동 법률이나 가이드라인에서는 CCTV가 표현의 자유에 대한 제한이나 차별적 목적으로 이용하는 것을 금지하는 아무런 규정을 두고 있지 않다. CCTV를 집회의 자유를 비롯한 헌법이 보장한 기본권을 행사하는 사람들을 위축시키기 위해 사용하거나 감시시스템 운영자가 선입견을 가지고 사회의 주변집단을 주된 감시대상으로 선정하는 등 차별적인 감시조치가 행해질 위험도 있다. 그러므로 감시시스템을 그와 같이 오남용하는 것을 금지하는 명문의 규정을 두는 것이 바람직하다(정태호, 2008: 178).[218]

더불어 자동정보처리장치를 통해 CCTV 영상을 판독하고 이용하는 것에 대해서도 한정하는 규정이 없다. 최근 여러 CCTV 관제센터에 영상을 자동으로 판독하는 시스템이 도입되고 있는데[219], 자동정보처리장치를 이용하는 것은 모니터 요원이 맨눈으로 영상정보를 판독하고 상황에 대응하기 위해 이용하는 경우에 비하여 위험도가 높기 때문에 별도의 규정을 두는 것이 바람직하다(정태호, 2008: 181)[220].

또한, 위 법률에서는 공공기관 간의 정보 제공에 대한 예외 규정을 두고 있다(동법 제10조제3항제2호). 공공기관개인정보보호심의위원회의 심의를 거친 경우 보유목적과 무관하게 이용하거나 제공할 수 있도록 허용한 것이다. 공공기관개인정보보호심의위원회가 실질적인 기능을 못하고 있는 현 실태를 감안할 때(제2장 제1절 참조),[221] 공공기관이 개인정보를 보유하는 목적과

---

218) 이와 관련하여 정태호(2008: 178-179)는 감시공간에서 집회가 개최되는 동안에는 CCTV 가동을 중단함으로써 집회참여자가 심리적 압박감 없이 자유롭게 집회에 참가할 수 있도록 해야 한다고 주장하였다. 폭력행위 가담자 색출을 위한 비디오촬영은 폭력집회의 구체적인 위험이 존재하는 경우에 예외적으로 정당화될 수 있다는 것이다. 미국 워싱턴 D.C. 콜럼비아 특별구 경찰의 CCTV 사용에 관한 자치령에서는 수정헌법 제1조의 표현의 자유의 보호를 받는 전단 배부 등에 초점을 맞추어 감시하는 것을 금지하고 있으며, 인종, 종족, 성별, 성적 취향, 장애, 여타의 차별기준에 근거한 차별적 감시도 금지하고 있다고 한다.

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

220) 관련하여 독일 연방개인정보보호법상 개인들의 영상을 확대하고 추출해내거나 생체인식기술을 이용하여 그 주체를 인식하거나 사진을 비교하거나 프로필을 만들어 내기 위하여 자동화된 데이터베이스를 사용하는 경우에는 개인의 보호가치가 있는 이익들에 중대한 영향을 미치기 때문에, 그러한 자동화된 데이터베이스의 사용은 예외적으로만 허용된다고 해석되고 있다고 한다. 정태호(2008: 181) 참조.

221) “‘공공기관개인정보보호심의위원회’의 위원장은 여전히 행정자치부[행정안전부]차관이라는 점에서, 행정자치부[행정안전부]장관의 정책결정을 집행하는 데 대하여 통제적 기능을 발휘하는 쉽지 않을 것으로 보인다. 위원회의 운용측면에서는 특히 제20조제2항제2호 소정의 ‘처리정보의 이용 및 제공에 대한 공공기관간의 의견조정’에 있어 거수기(a rubber stamp) 역할에 자족할 여지가 없진 않다고 할 것이다”(이민영. 2007:

무관하게 정보이용과 제공이 허술하게 이루어질 수 있는 것이다. 정보주체 또는 제3자의 권리와 이익을 부당하게 침해할 우려가 있는 경우는 그러하지 아니한다는 예외 규정을 두었지만, 침해 여부를 이용하거나 제공하는 측에서 이 조항에 대한 판단을 자체적으로 판단하도록 하였다. 관련 규정의 보완이 시급해 보인다.[222]

본 연구는 특히 자치구가 경찰관서에 위탁하여 관리하는 방범용 CCTV의 경우를 집중적으로 분석하였다.[223] 서울시 자치구의 경우 대개의 방범용 CCTV를 관할 경찰관서로 위탁관리하고 있었다. 이것은 경찰의 적극적인 요구에 따라 시작된 것으로, 경찰청은 이미 지난 2004년 9월 지자체와 협조해 CCTV 설치를 적극 추진할 것을 지방경찰청에 지시한 바 있다.[224]

자치구들은 방범용 CCTV의 구축 비용 및 공공요금이나 모니터요원 등 유지보수에 필요한 비용을 부담하고, 그 실제적인 운영에 대해서는 관할 지역 내 경찰관서와 협약을 맺어 위탁하고 있다. 이러한 위탁은 공공기관의 장이 CCTV의 설치 및 관리에 관한 사무를 위탁할 수 있도록 한 법률에 따른 것으로서(동법 제4조의3), 시행령에서는 그 수탁기관의 자격으로서 개인정보보호에 필요한 전문 장비 및 기술을 갖출 것과 수탁받은 업무를 수행하는데 필요한 전문 인력을 갖출 것을 명시하고 있다. 또한 위탁기관은 위탁대상이 되는 사무의 범위, 개인정보에 대한 접근제한 등 개인정보보호에 필요한 사항을 세부적으로 정한 후 이를 위탁계약서 등 관련 서류에 분명하게 기록하여야 한다고도 하였다(동시행령 제4조의3 제1항과 제2항).

---

40).

222) 관련하여 정태호(2008: 185)는 독일의 연방개인정보보호법의 경우 국가 및 공공의 안전에 대한 위험을 방지하기 위하여 필요하거나 범죄행위의 소추를 위하여 필요한 경우에만 목적외 사용을 허용함으로써 목적구속의 원칙을 엄격하게 관철하고 있고, 워싱턴 D.C. CCTV 자치령에서는 영상의 모니터링을 범죄의 탐지와 감시, 범죄나 범죄혐의의 증거 확보, 교통관리를 위해서만 할 수 있도록 하고, 그 정보를 기타의 목적으로 사용하는 것을 허용하지 않고 있다고 지적하였다.

223) 그밖에 서울 자치구의 방범용 CCTV는 각 자치구의 시설관리를 목적으로 자체적으로 설치 및 관리되는 경우도 있고 아동 보호를 목적으로 관내 초등학교에 설치되어 각 학교에 의해 관리되는 경우도 있다. 본 연구는 서울 각 자치구 자치행정관련부서에서 설치하고 관내경찰서에서 운영을 맡고 있는 방범용 CCTV를 분석 대상으로 삼았다.

224) 중앙일보. 2004.10.31. “전국에 `방범 CCTV` 추진”.

<그림 3-3> CCTV 위탁관리 프로세스


자료: 행정안전부(2009a: 24).

서울 각 자치구의 방범용 CCTV 위탁 운영 현황은 <표 3-8>과 같다.

<표 3-8> 방범용 CCTV에 대한 위탁 운영 현황 (서울 자치구)

(2009년 6월 말 현재)

| 자치구 | 위탁경찰서 | 대수 | 자치구 | 위탁경찰서 | 대수 |
|---|---|---|---|---|---|
| 강남구 | 강남·수서경찰서 | 522대 | 서대문구 | 서대문경찰서 | 54대 |
| 강동구 | 강동경찰서 | 61대 | 서초구 | 서초·방배경찰서 | 127대 |
| 강북구 | 강북경찰서 | 52대 | 성동구 | 성동경찰서 | 32대 |
| 강서구 | 강서경찰서 | 46대 | 성북구 | 종암·성북경찰서 | 62대 |
| 관악구 | 관악경찰서 | 40대 | 송파구 | 송파경찰서 | 133대 |
| 광진구 | 광진경찰서 | 178대 | 양천구 | 양천경찰서 | 70대 |
| 구로구 | 구로경찰서 | 53대 | 영등포구 | 영등포경찰서 | 124대 |
| 금천구 | 금천경찰서 | 70대 | 용산구 | 용산경찰서 | 180대 |
| 노원구 | 노원경찰서 | 72대 | 은평구 | 서부·은평경찰서 | 44대 |
| 도봉구 | 도봉경찰서 | 51대 | 종로구 | 종로·혜화경찰서 | 86대 |
| 동대문구 | 동대문경찰서 | 125대 | 중구 | 중부·남대문경찰서 | 170대 |
| 동작구 | 동작경찰서 | 67대 | 중랑구 | 중랑경찰서·초등학교 | 146대 |
| 마포구 | 마포경찰서 | 91대 | | | |

자료: 각 자치구.[225]

기본적으로 위탁기관은 개인정보가 오·남용 되지 않도록 수탁기관에 대하여 관리·감독할 책임을 가지고 있다. 그러나 본 연구의 조사 결과 경찰이

225) '방범용 CCTV에 대한 정보공개 청구'에 대한 서울 각 자치구의 정보(공개) 결정통지서(2009.10.22~2009.10.30).

운영하는 방범용 CCTV의 구체적인 실태에 대해서 위탁기관인 각 자치구가 파악하고 있지 못한 것으로 드러났다. 방범용 CCTV의 실태에 대하여 서울 각 자치구에 질의한 결과, △설치대수, △성능, △보유/삭제기간, △담당자 연락처, △사전 의견수렴 방법, △CCTV 설치 및 운영에 대한 규정 및 지침 등 방범용 CCTV의 기본적인 현황정보와 자치구에서 관여한 사항에 대해서는 각 자치구가 비교적 그 실태를 파악하고 있는 것으로 조사되었다. 그러나 △CCTV 설치장소 통제 현황, △기관내 열람(조회)권자 현황, △제3자 제공 현황, △정보주체 권리 행사 현황 등 구체적인 실태에 대해서는 질의대상 자치구 모두가 관할 경찰서 소관 업무라고 답변하였다.

특히 방범용 CCTV 영상 기록 관리와 관련해서 각 경찰관서가 운영하는 실태는 자치구가 파악하고 있는 바와 다른 것으로 드러났다. 대개의 자치구는 방범용 CCTV 영상 기록에 대하여 「공공기관 CCTV 관리 가이드라인」에 명시된 30일 이후 자동삭제한다고 답변하였으며, 별도의 사본을 보유한다고 밝힌 자치구는 없었다. 그러나 서울 경찰관서 31개 가운데 15개 관서는 CCTV 영상 기록 가운데 일부에 대하여 "필요한 경우 운용감독관이나 운용책임관의 건의로 경찰서장의 승인 받아 관련사건 종결시까지 보존기간을 연장하여 특별관리"한다고 밝혀 CCTV 영상 기록 원본의 삭제와 별도로 사본을 보유하고 있었다(<그림 3-4>).[226]

<그림 3-4> CCTV 영상 기록의 사본 보유 사례 (서울 경찰관서)

**4. 방범용 CCTV 영상의 보존에 대한 정보공개 청구입니다.**

1) 영상의 보존기간 : **최대 1개월**

2) 영상의 보존원칙

**자동녹화시스템(일정 자료가 저장되면 이전자료는 삭제되고 새로운 자료가 저장됨)**

3) 위 1)과 2)에 예외가 있는지

**필요한 경우 운용감독관의 건의로 경찰서장의 결정을 받아 관련사건 종결시까지 별도 보안저장장치 등에 복사하여 특별관리함**

경찰이 운영하는 방범용 CCTV 영상자료에 대해 이용하거나 제공받으려는

226) '방범용 CCTV에 대한 정보공개 청구'에 대한 서울 각 경찰관서의 정보(공개) 결정 통지서(2009.8.18~2009.8.21). 이 장에서 각 경찰관서의 현황에 대한 출처는 이하 같다.

자는 조회신청서를 서면으로 작성한 후 경찰서장의 승인을 얻어 운용감독관의 책임하에 이용하거나 제공할 수 있다. 서울 경찰관서가 운영하는 방범용 CCTV의 이용 및 제공 현황은 다음 <표 3-9>와 같았다.[227] '방범용' CCTV는 범죄예방을 위하여 설치된 만큼, 설치 목적과 법률에서 규정된 용도 외 제3자에게 제공되는 경우는 없어야 할 것이다.

<표 3-9> 방범용 CCTV 기록 조회 현황 (서울 자치구 수탁 경찰관서)

| | 자기관 조회 | 정보주체 조회 | 범죄수사목적 제3자조회 | 그외 목적 제3자조회 | 대상기간 | 월평균 조회 |
|---|---|---|---|---|---|---|
| 강남 | 748 | - | 28 | - | '04.8.1~'08.12.31 | 14.6 |
| 강동 | 74 | - | 2 | 1 | '05.2.1~'09.8.19 | 1.4 |
| 강북 | 39 | - | - | - | '09.1.1~'09.8.19 | 4.9 |
| 강서 | 28 | - | - | - | '08.1.1~'09.7.31 | 1.5 |
| 관악 | 13 | - | - | - | '08.1.1~'08.12.31 | 1.1 |
| 광진 | 266 | - | - | 1 | '08.1.1~'08.12.31 | 22.3 |
| 구로 | 70 | - | 1 | - | '07.3.1~'09.8.20 | 2.4 |
| 금천 | 91 | - | 7 | - | '06.5.15~'09.7.31 | 2.5 |
| 남대문 | 54 | - | - | 2 | '09.1.1~'09.8.19 | 7.0 |
| 노원 | 41 | - | 1 | - | '09.1.1~'09.7.31 | 6.0 |
| 도봉 | - | - | - | - | - | - |
| 동대문 | 108 | - | - | - | '06.12.1~'08.12.31 | 4.3 |
| 동작 | 17 | - | - | - | '09.1.1~'09.8.17 | 2.1 |
| 마포 | 78 | - | 3 | - | '09.1.1~'09.7.31 | 11.6 |
| 방배 | 36 | - | 1 | - | '09.1.1~'09.8.21 | 4.6 |
| 서대문 | 211 | - | - | - | '08.4.21~'09.7.31 | 13.2 |
| 서부 | 17 | - | - | - | '09.1.7~'09.7.31 | 2.4 |
| 서초 | 49 | - | - | - | '09.1.1~'09.7.31 | 7.0 |
| 성동 | 126 | - | 2 | - | '07.1.1~'09.7.31 | 4.1 |
| 성북 | 24 | - | - | - | '04.9.1~'09.8.19 | 0.4 |
| 송파 | 47 | - | - | - | '04.10.1~'09.7.31 | 0.8 |
| 수서 | 193 | - | 1 | - | '08.1.1~'08.12.31 | 16.2 |
| 양천 | 248 | - | - | - | '06.7.1~'09.7.31 | 6.7 |
| 영등포 | 90 | - | 1 | - | '06.5.1~'09.8.17 | 2.3 |

227) 여기서 경찰은 자치구로부터 위탁받아 운영하는 수탁기관이기 때문에 엄밀히 말해 타경찰관서 및 수사기관 역시 제3자이다.

| | | | | | | |
|---|---|---|---|---|---|---|
| 용산 | 66 | - | 3 | 26 | '09.1.1~'09.8.19 | 11.9 |
| 은평 | 39 | - | - | 2 | '09.1.7~'09.7.31 | 5.9 |
| 종로 | | | | 1 | '09.1.1~'09.8.21 | 0.1 |
| 종암 | 106 | - | 1 | 1 | '07.4.1~'09.8.20 | 3.7 |
| 중랑 | 221 | - | 9 | 2 | '08.1.8~'09.6.30 | 12.9 |
| 중부 | 129 | - | 5 | - | '08.5.13~'09.8.19 | 8.4 |
| 혜화 | 9 | - | - | - | '09.1.1~'09.8.19 | 1.1 |

자료: 각 경찰관서.

이처럼 자치구가 방범용 CCTV에 대한 관리를 전적으로 경찰에 일임하는 것은 방범용 CCTV의 운영을 수사 과정으로 이해하고 있기 때문인 것으로 보인다. 실제 각 경찰관서는 CCTV 모니터링 과정에서 현행범인 또는 준현행범인을 발견하거나 112신고사건 중 강력범죄 발생시 상황실과 무전교신을 통해 발생지 주변 5개 화면을 일시에 띄운 후 용의자 발견 및 도주로를 추적하는 방법(투망검색)을 사용하고 있었으며, 이 경우 관할지구대에 무전으로 통보하여 불심검문을 통한 범인 검거 및 피해품 회수를 하고 있다고 밝혔다.

여기서 문제는 수사의 한 과정으로 이루어지는 방범용 CCTV 모니터링을 민간인이 담당하고 있다는 사실이다.

서울 경찰관서 31개 가운데 12개 관서가 민간인 모니터 요원을 두고 있었으며, 일부 경찰서의 경우 모니터 요원 전원을 민간인 가운데 선발하는 등 그 실태가 심각하였다(<표 3-10>).

이에 관제센터에서 근무하는 민간인 모니터 요원들이 CCTV를 악용할 수 있다는 우려가 지적되고 있을 뿐 아니라,[228] 범죄의 예방 및 수사를 경찰관의 직무로 규정하고 있는 현행 법률에 저촉될 소지도 가지고 있다.

228) "용역업체에서 보낸 사람을 전과 조회만 하고 쓰다 보니 다양한 사람이 모니터요원으로 옵니다. 보통은 상황실에 경찰관과 함께 있지만 경찰이 순찰을 나가고 나면 그 사람이 혼자서 주택가 방범 폐쇄회로(CC)TV를 줌으로 당겨 유리창을 통해 가정집 내부를 볼 수도 있죠." 동아일보. 2008.11.26. "가정집 안방까지 볼 수있는 방범 CCTV 상황실".; "늘어나는 CCTV 촬영으로 인해 개인의 사생활이 낱낱이 파헤쳐져 감시되고 있는 것에 대해서 국민들의 불안이 가중되고 있는 상태에서 검증되지 않은 용역업체 파견직원의 잦은 교체는 심히 우려되지 않을 수 없습니다." 양천구의회 제179회 제2차 정례회 제2차본회의 최진표 의원 질의내용(2008.12.9). http://www.ycc.go.kr/qna/qna_view2.asp?qtag=QUE00179_001_000_003&keywords= 참고.

<표 3-10> 방범용 CCTV 모니터 요원 현황 (서울 자치구 수탁 경찰관서)

(2009년 8월 현재)

| 경찰서 | 경찰관 | 민간인 | 경찰서 | 경찰관 | 민간인 |
|---|---|---|---|---|---|
| 강남 | 0 | 14 | 서부 | 3 | 0 |
| 강동 | 4 | 0 | 서초 | 3 | 3 |
| 강북 | 3 | 0 | 성동 | 4 | 0 |
| 강서 | 3 | 3 | 성북 | 4 | 0 |
| 관악 | 3 | 0 | 송파 | 3 | 4 |
| 광진 | 3 | 3 | 수서 | 0 | 14 |
| 구로 | 3 | 0 | 양천 | 4 | 3 |
| 금천 | 4 | 0 | 영등포 | 4 | 3 |
| 남대문 | 3 | 3 | 용산 | 10 | 0 |
| 노원 | 4 | 0 | 은평 | 2 | 0 |
| 도봉 | - | 0 | 종로 | 7 | 0 |
| 동대문 | 8 | 0 | 종암 | 3 | 0 |
| 동작 | 3 | 0 | 중랑 | 3 | 6 |
| 마포 | 4 | 0 | 중부 | 4 | 6 |
| 방배 | 0 | 3 | 혜화 | 1 | 0 |
| 서대문 | 3 | 0 | | | |

자료: 각 경찰관서.

### 3) CCTV 정보의 삭제

「공공기관개인정보보호법」에 따르면, 보유기관의 장은 개인정보파일의 보유목적 달성 등 개인정보파일의 보유가 불필요하게 된 경우에는 당해 개인정보파일을 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 보존하여야 하는 경우에는 그러하지 아니하다(동법 제10조의2). CCTV에 의해 처리된 개인정보에 대한 삭제는 별도의 규정 없이 이 조항의 적용을 받는다. 그러나 CCTV의 경우 사생활 침해 소지가 크기 때문에 파기에 관한 사항이 보다 명확히 규정될 필요가 있다.

이 점과 관련하여, 과거 국회에서 공공기관 CCTV 관련 법률이 논의될 당시에는 CCTV의 파기 기간을 명시했다는 점을 상기할 필요가 있다. 2005년 4월 행정자치위원회에서 검토된 「공공기관의 개인정보보호에 관한 법률중 개정법률안(김재경의원 대표발의안, 의안번호 제171070호)」에서는 “보유기

관의 장은 개인정보파일 중 화상정보는 수집목적을 달성하거나 수집 후 30일이 경과한 경우에는 지체 없이 파기하여야 한다. 다만, 화상정보를 수사나 재판자료로 사용하는 경우에는 당해 사실을 정보주체에게 통보하고 수사나 재판이 종료될 때까지 보관할 수 있다."라고 하여 CCTV 처리정보의 파기를 명시하였었다. 또한 「공공기관의 폐쇄회로 텔레비전 설치 및 개인의 화상정보 보호에 관한 법률안(김충환의원 대표발의안, 의안번호 제171287호)」에서도 "공공기관의 장은 명백히 수집 목적과 관계없이 수집일 이후 30일이 경과한 화상정보를 즉시 파기하여야 한다. 다만, 당해 화상정보를 수사나 재판자료로 제공하는 경우는 그러하지 아니하다"고 하여 CCTV 처리정보의 파기를 보다 강력하게 의무화하였을 뿐더러, "화상정보를 수사나 재판자료로 제공하는 경우 그 사실을 당해 개인에게 알려 주어야 한다"라는 규정을 덧붙여 자신의 개인정보 처리 사실에 대한 정보주체의 알 권리를 보장하였다.

이러한 취지가 법률 개정 과정에서 반영되지 않았던 점은 아쉽지만, 「공공기관 CCTV 관리 가이드라인」에 일부 반영되었다. CCTV에 의하여 수집된 화상정보는 규정에 명시된 기간이 만료한 즉시 삭제하도록 하고, 다만 해당기관의 특정에 따라 보유목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보유기간을 화상정보의 수집 후 30일 이내로 한 것이다(동가이드라인 제16조).

그러나, 앞서 살펴본 바대로 자치구 방범용 CCTV가 위탁운영되는 과정에서 수탁기관인 경찰관서가 정해진 기간에 따라 삭제되는 영상기록 원본과 별도로 사본을 보유하는 것은 법률과 관련 가이드라인에 위배되는 것이다.

## 3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태

CCTV 등 무인단속장비에 의해서 영향을 받는 모든 개인은 그 운영에 관해 의견을 제시할 수 있는 권리를 보장받아야 한다. 기본적으로 자신과 관련된 정보의 존재 확인, 열람요구, 이유부기, 이의제기 및 정정·삭제·보완 청구권을 가지며, 열람요구나 정정 신청 등을 거부당할 경우 그에 대한 불복신청과 손해발생시 권리구제 절차가 규정되어야 한다(국가인권위원회, 2004a).

현재 CCTV에 대한 정보주체의 열람 및 정정·삭제 청구권은 「공공기관 개인정보보호법」에 따라 일반적으로 보장받고 있다. 다만 개인신상정보(주소, 전화번호 등)에 오류가 있는 경우와 달리 CCTV에 의해 촬영·저장된 개인영상정보에 대해서는 정보주체에게 정정권을 인정하는 경우가 드물다(정보

통신부, 2007: 58).[229]

그런데 법문대로라면 이러한 열람 및 정정·삭제 청구권은 개인정보파일대장에 기재된 범위 안에서 그 행사가 한정된다.[230] 개인정보파일대장은 법 제8조에 의해 개인정보 보유기관이 작성하여 일반인이 열람할 수 있도록 원칙적으로 공개하는데, 개인정보파일대장이 공개되지 않을 경우 정보주체의 열람 및 정정·삭제 청구권 또한 제한을 받는 결과로 이어질 수 있다.

2008년 행정안전부가 고시한 개인정보파일대장을 조사한 결과 CCTV를 운영하는 많은 자치구가 개인화상정보 파일을 공개하지 않았다. 서울의 경우 개인화상정보 파일을 보유하고 있음을 공개한 자치구가 전체 25개 구 중 동대문구, 동작구, 양천구, 중구 등 4개 구에 불과하였다.

<표 3-11> 개인정보파일대장에 CCTV 개인화상정보 파일을 공개한 서울 자치구 현황 (2008년)

| 자치구 | 공개된 개인화상정보파일 |
|---|---|
| 동대문구 | 화상화일(153, 방범용), CCTV관리(3340), CCTV 관리현황(336) |
| 동작구 | 무단투기단속 CCTV관리파일(169), 무단투기단속 CCTV관리파일(178), cctv 관리 현황(398) |
| 양천구 | 방범용 CCTV 화상정보관리(2), 방범용 CCTV 화상정보관리(69), 쓰레기무단투기방지 CCTV(131) |
| 중구 | 쓰레기무단투기감시 화상파일(37), 본청사관리 화상파일(38), 보건소청사관리 화상파일(182), 범죄예방 화상파일(308), 구민회관관리 화상파일(309), 의회청사관리 화상파일(310) |

물론 정보주체가 열람 청구권을 행사하려 할 때 각 자치구의 개인정보파일대장 공개 여부와 무관하게 열람이 가능할 수도 있다. 그러나 정보주체의 권리 행사를 위하여 개인정보파일대장에 대한 작성과 더불어 그 이용사실에 대한 공개가 보다 적극적으로 이루어질 필요가 있다. 정보주체가 자신의 개인

229) 그러나 2003년 3월 학내도난사건 관련하여 CCTV 작동시간이 실제 시간과 달라 범행 시간보다 10여 분 앞서 현금인출기를 사용한 윤모씨가 용의자로 지목하는 일이 벌어지기도 한 만큼 CCTV에 있어서도 정정 청구권 행사가 완전히 불가한 것은 아니라 하겠다(함께하는 시민행동, 2003b: 20).

230) 공공기관의 개인정보보호에 관한 법률
제12조 (처리정보의 열람) ①정보주체는 개인정보파일대장에 기재된 범위안에서 문서로 본인에 관한 처리정보의 열람(문서에 의한 사본의 수령을 포함한다. 이하 같다)을 보유기관의 장에게 청구할 수 있다. <개정 2007.5.17>

정보가 CCTV에 의해 처리·이용되는지 여부를 알기 어려우면 개인에게 보장된 자신의 열람 및 정정·삭제 청구권을 의미 있게 행사하기 어렵기 때문이다. 정보주체에 대한 영상정보이용사실의 통지제도의 도입을 고려해볼 만하다.[231]

또한, CCTV의 경우 그 설치를 정보주체가 쉽게 인식할 수 있도록 공개하는 것이 매우 중요하다. 이는 CCTV 설치에 대한 인식이 그 기록에 대한 열람 및 정정·삭제 등 정보주체의 권리 행사와 불가분의 관계가 있기 때문이다. 따라서 공공기관 CCTV는 몰래 운영되는 경우가 없으며 반드시 안내판 등 정보주체가 그 설치를 인식하는 데 필요한 조치를 취하도록 법률에 명시되어 있다. 서울 자치구들도 불법 주정차 단속용 CCTV나 쓰레기 무단투기 감시 카메라의 경우 홈페이지 등을 통해 그 위치를 공개하는 경우가 많았다.

그러나, 방범용 CCTV의 경우 범죄에 이용될 소지가 있다는 명분으로 공개하지 않는 경우가 많았다. 25개 자치구 가운데 홈페이지에 공개한 경우는 3개 뿐이고, 비공개한 경우는 14개로 전체의 56%에 달했다. 이는 방범용 CCTV 위치를 비공개 정보로 취급할 것을 권고한 서울시 방침에 따른 것으로 확인되었다.[232]

<표 3-12> 방범용 CCTV 위치 공개 여부 (서울 자치구)

| 구 분 | 자치구수 (총25개구 중) |
|---|---|
| 홈페이지에 공개 | 3 |
| 정보공개에 의한 공개[233] | 8 |
| 비공개 | 14 |

서울 자치구들의 경우 CCTV 설치 및 운영 규정 혹은 지침에서 법률상 정

231) 관련하여, 정태호(2008: 188)는 독일연방개인정보보호법처럼 비공개수사의 필요성, 국가안보를 위한 비밀유지의 필요성 등 특별한 사정이 없는 한 관련 개인에게 영상정보의 처리나 이용 사실을 통지하여야 한다고 보았다. 그래야 CCTV 감시를 통해 확보한 개인정보 이용의 투명성을 확보할 수 있고, 또 개인정보의 주체들에게 개인정보보호법이 보장하고 있는 절차적 권리들이 실효성 있게 행사될 수 있기 때문이다.

232) "방범용 CCTV의 경우 CCTV 위치정보를 손쉽게 얻을 수 있도록 홈페이지에 게시하는 것은 범죄에 악용될 소지가 있어 그 설치 목적에 반하는 것으로 판단되므로, 이를 비공개 정보로 취급하여 홈페이지 게재 및 외부기관 정보제공 등을 지양할 것을 권고하니 업무에 적극 반영하여 주시기 바랍니다". 서울시. CCTV 설치위치정보 취급 주의사항 시달(2008.6.4). 문서번호: 정보통신담당관-8650 (2008.06.04).

233) '지방자치단체 CCTV 관련 정보공개 청구'에 대한 서울 각 자치구의 정보(공개) 결정통지서(2009.7.20~2009.8.13).

보주체의 권리를 명시하고 있었다. 본 연구의 목적을 위하여 실제로 열람 청구권을 행사하여 본 결과 방범용 CCTV의 경우 CCTV를 수탁운영하고 있는 경찰관서를 통하여 정보주체의 열람권 행사가 이루어질 수 있었다(<그림 3-5>).

<그림 3-5> 정보주체 화상정보 열람결정통지

[redacted]

인쇄일자 : 2009.10.27

# 정보(공개)결정통지서

수 신 자 [redacted]

| | | | |
|---|---|---|---|
| 접 수 일 자 | 2009.08.10 | 접 수 번 호 | [redacted] |
| 청구정보내용 | 귀 기관에서 운영하고 있는 CCTV에 의해 촬영된 본인의 화상정보에 대한 열람을 요청합니다.<br><br>- CCTV 위치 : [redacted]학교([redacted]동 1-2) 앞 사거리에서 학교쪽 블록에 설치된 CCTV<br>- 촬영일시 : 8월 5일, 6일 10시경<br>- 열람목적 : 본인 촬영 정보에 대한 확인<br>- 열람방법 : 영상 파일을 제공받을 필요는 없으며, 열람할 수 있는 장소에 방문하여 열람할 수 있음.<br>- 열람희망시간대 : 오전 11시경. (방문일시는 협의 가능) | | |
| 공 개 내 용 | CCTV 공개요청 자료시간대인 8월 5일, 6일 09:40부터 10:10까지의 열람시간대를 열람실시함. | | |
| 공 개 방 법 | 공개형태 | 열람 · 시청 | |
| | 교부방법 | 직접방문 | |
| 공개일시 (기간) | 2009.08.14 19 시 | 공 개 장 소 | [redacted]정찰서 [redacted]지구대 |

| 수 수 료 (A) | 우 송 료 (B) | 수수료감면액 (C) | 계 (A+B-C) |
|---|---|---|---|
| 0원 | 0원 | 0원 | 0원 |
| 수수료산정내역 | | 수수료 납입계좌(입금시) | |

귀하의 정보공개 청구에 대한 결정내용을 공공기관의 정보공개에관한법률 제13조 제1항 및 제4항의 규정에 의거하여 위와 같이 통지합니다.

2009 년 08 월 14 일

경찰청장

| 처 리 과 명 | 생활안전과 | 문 서 번 호 | 생활안전과 -5419(2009.08.14) |
|---|---|---|---|

그러나 각 자치구는 방범용 CCTV의 경우 정보주체의 열람 청구조차 수사의 일환으로 간주하여 경찰서에 일임하는 경향이 있었으며,[234] 경찰서 역시 수사상 목적이 아닌 정보주체의 권리 행사로서의 열람에 대한 업무 처리가 원활치 않았다. 서울 각 경찰관서에서 정보주체의 열람권과 그에 따른 삭제권이 행사된 사례는 지금까지 한 건도 보고되지 않았으며(<표 3-9>), 이는 정보주체의 권리 행사가 거의 이루어지고 있지 않거나 그 현황이 제대로 관리되고 있지 않은 결과로 보인다.

## 4. 소결

2002년 12월 서울시 강남구에 범죄예방을 위한 CCTV가 시범설치된 후 방범용 CCTV를 비롯한 공공기관의 CCTV가 크게 증가하여왔다. 그러나 이를 규제하는 법률은 비교적 최근에야 제정되었으며, 그 구체적인 규정 및 실태가 법률의 제정 취지와 어긋나는 경우가 많았다.

CCTV는 매우 광범위한 규모로 다양한 개인정보를 수집하는 개인정보 자동수집장치이기 때문에 필요최소한으로 설치하도록 설치 시점부터 사전적으로 규제하는 것이 중요하다. 그러나 법률상 공공기관의 CCTV 설치가 매우 폭넓게 인정되고 있으며, 의견수렴은 형식적으로 이루어지고 있다. 법률상 CCTV 설치 목적을 명확히 한정하고, 주민 등 이해관계인에게 CCTV의 설치에 대한 동의 여부를 물을 때는 정보주체가 동의권을 충분히 행사할 수 있도록 상세한 정보제공과 함께 공청회 등 적극적인 의견수렴 형식을 갖추는 것이 바람직하다.

특히 공공기관의 CCTV 기록의 이용 및 제공에 대한 현행 규정이 그리 엄격하지 않은 상태에서, 각 자치구가 경찰관서에 위탁운영하고 있는 방범용 CCTV의 문제가 심각하였다. 위탁기관인 자치구가 수탁기관인 경찰관서에 일체의 운영을 일임한 채 그 구체적인 실태를 파악하고 있지 않았다. 특히 정해진 기간에 따라 삭제되는 CCTV 영상기록 원본과 별도로 경찰관서가 법률적 근거 없이 사본을 보유하는 관행은 시정되어야 한다.[235] 또한 수사의

---

234) "범죄 관련 요구일 경우 경찰 신고 후 정식으로 요청할 것을 권하고 있는데, 어떤 이들은 내 얼굴인데, 내 집 앞인데 왜 안 되느냐며 막무가내식으로 따지고 들어 곤혹스럽다." 방범용 CCTV의 경우에는 정보주체라 하더라도 경찰 신고 후에만 열람이 가능하도록 안내하는 지자체도 있었다. 부산일보. 2009.8.7. "누가 내차 긁고 갔는데 CCTV 좀…."

235) 일본의 경우 공권력이 설치한 범죄예방 목적의 TV 카메라는 녹화하지 않는 것이

한 과정으로 이루어지는 방범용 CCTV 모니터링을 많은 경우 민간인이 담당하는 것은 우려스런 일이다. 자치구와 경찰의 역할분담에 있어 편의적인 측면이 있는 것이 사실이라 하더라도, CCTV의 운영주체와 그에 따른 책임 관계를 명확히 할 필요가 있다.

또한 정보주체가 CCTV에 대한 권리를 행사하는 것도 여의치 않았다. CCTV를 운영하는 많은 자치구가 개인화상정보 파일을 공개하지 않았으며, 방범용 CCTV의 경우 그 위치를 공개하지 않는 경우가 대다수였다. 이러한 이유에서인지 사실상 열람과 삭제 등 정보주체의 권리 행사가 이루어진 경우는 거의 보고되지 않았다.

최근 목적별·지역별로 CCTV 통합관제센터가 주목을 받고 있다. 기관간 또는 자치단체간에 인력과 장비를 공유함으로써 적은 자원으로 효과적인 방범을 수행할 수 있는 역할분담 및 협력체계를 강구하자는 것이다(오영균, 2009). 행정안전부도 이러한 추세를 반영하여 2009년 9월에 「공공기관 CCTV 관리 가이드라인」을 갱신하면서 'CCTV 통합 관리'에 대한 규정을 신설하였다. 여기서 'CCTV 통합 관리'란 기관내 또는 기관간에 용도별·지역별 CCTV를 물리적·관리적으로 통합하여 모니터링 등을 수행하는 것을 말한다. 그러나 기관내 CCTV를 통합 관리하는 것은 방범용, 쓰레기 투기방지, 시설물 관리, 주차관리, 교통정보 수집 등 고유의 목적으로 설치된 CCTV를 다목적으로 사용하겠다는 것으로서, 개인정보 수집장치를 목적 외의 용도로 활용할 수 없도록 한 개인정보보호원칙과 현행 법률에 반하는 것이다.[236] 기관간 CCTV를 통합관리하는 것은 지역 주민 등 이해관계인으로부터 의견수렴 및 동의를 받고 설치된 CCTV의 이용 범위를 넘어선 것으로서 정보주체의 권리를 형해화할 위험이 있다. 개정되기 전의 「공공기관 CCTV 관리 가이드라인」에서도 CCTV를 여러 목적으로 사용하고자 하는 경우 사전의견수렴시 사용 목적을 나열하여 의견수렴을 하고 안내판 등 설치 사실 공지시 다목적용 CCTV임을 공지하도록 하며 다목적용 CCTV를 설치

---

원칙이다. 즉 녹화되지 않는 것을 전제로 하여 ① 실제로 범죄가 실행중이거나 실행직후인 경우로서 ② 증거보전의 필요성과 긴급성이 있고, ③ 그 촬영이 일반적으로 허용되는 한도를 넘지 않는 상당한 방법으로 이루어진다는 조건하에서 CCTV 설치가 허용될 수 있지만, 녹화되는 경우는 범죄예방을 목적으로 한다고 하더라도 CCTV 설치가 허용되지 않는다는 판결이 주목을 받고 있다(권건보, 2009: 10).

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

·운영할 경우 행정안전부와 사전협의를 하도록 하는 등 다목적 CCTV를 일반 CCTV보다 한층 엄격하게 규제 해 왔었다(행정안전부, 2008b). 이러한 점에서 최근 행정편의적인 수요에 초점을 두어 CCTV 통합 관리가 확대되는 추세는 상당히 우려스럽다 할 것이다.

권건보(2009: 27)는 CCTV 관련 법제의 개선 방향에 있어 적절한 감독기관이 수시로 감독을 실시함으로써 책임 있는 CCTV의 운영이 될 수 있도록 유도하여야 한다고 지적하였다. 현행 「공공기관의 개인정보 보호에 관한 법률」은 공공기관의 개인정보 이용에 대한 감독기능을 행정안전부에 부여하고 있는데, 행정안전부는 그 스스로가 개인정보를 업무에 이용하는 대표적인 공공기관의 하나이다. 따라서 다른 중앙부처의 개인정보 오남용을 역시 중앙부처중의 하나인 행정안전부가 효과적으로 감독할 수 있을지 의문이다. 이러한 점에 비추어볼 때 독립적인 개인정보보호기구를 두어서 CCTV의 설치와 운영을 감독하고, 그로 인한 피해의 예방이나 구제 등의 업무도 함께 담당하도록 하는 것이 바람직할 것이다.

# 제2절 위치정보

## 1. 개요

정보통신기술의 발전으로 사물의 위치를 파악하는 능력이 고도화되고 있다. 위치가 추적되는 사물이 그것을 보유하고 있는 사람과 결합될 때, 혹은 추적되는 대상 자체가 사람인 경우, 그것은 개인 위치정보가 된다. 개인 위치정보의 수집, 이용을 통해 정보주체의 이동 경로를 추적할 수 있고, 이를 기반으로 개인의 활동 패턴을 파악하거나 다른 개인정보와 결합하여 개인의 활동 내용까지 유추가능하다. 예를 들어, 어떤 개인의 이동 경로가 누적되면, 집이나 사무실의 위치, 통상적인 출퇴근 시간, 예외적 이동이나 만남이 발생한 경우 등이 파악될 수 있을 것이다. 특히, 모바일 기반의 위치 추적은 개인을 실시간으로 감시할 수 있는 수단이 될 수 있다.[237] 따라서 개인 위치정보는 극도로 민감한 개인정보라고 할 수 있다.

개인 위치정보는 우선 「위치정보의 보호 및 이용 등에 관한 법률」(이하 「위치정보법」)에 의해 규제된다. 「위치정보법」 제2조제1호는 위치정보를 "이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 전기통신기본법 제2조제2호 및 제3호의 규정에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것"이라 정의하고 있다. 개인위치정보는 "특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)"로 규정하고 있다.

「위치정보법」은 제1장 총칙, 제2장 위치정보사업의 허가 등, 제3장 위치정보의 보호, 제4장 긴급구조를 위한 개인위치정보의 이용, 제5장 위치정보의 이용기반 조성, 제6장 벌칙 등 총 6장으로 구성되어 있다.

'제3장 위치정보의 보호'는 제1절 통칙, 제2절 개인위치정보의 보호, 제3절 개인위치정보주체등의 권리 등으로 구성된다. 제3장의 개인정보 보호 관련 조항들은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 규정하고 있는 개인정보 보호를 위한 일반 원칙과 크게 다르지는 않다. 다만, 다음과 같이 위치정보의 특성을 고려한 내용이 존재한다.

---

237) 대표적인 것이 삼성SDI 전현직 노동자들에 대해 불법복제된 휴대전화를 통해 몇 개월 동안 위치추적을 통한 감시가 이루어진 사례이다. 한겨레신문. 2004.7.14. "'위치추적' 삼성SDI 고소."

- 타인의 정보통신기기를 복제하거나 도용하여 개인위치정보 수집 금지 (제15조제2항)
- 위치정보를 수집할 수 있는 장치가 부착된 물건을 대여하는 자는 그 사실을 대여받는 자에게 고지해야 함 (제15조제3항)
- 위치정보 수집·이용·제공사실 확인자료를 위치정보시스템에 자동 기록·보존 의무화 (제16조제2항)
- 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 경우에는 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보 (제19조제3항)
- 8세 이하의 아동 등의 보호를 위한 위치정보 이용 (제26조)
- 긴급구조를 위한 개인위치정보의 이용 (제4장)

그러나 위치정보를 수집하는 모든 기관 혹은 업체가 이 법률의 적용을 받는 것은 아니다. 동법에서 규정하고 있는 개인 위치정보 보호 의무나 정보주체의 권리를 보장하는 주체는 위치정보사업자 및 위치기반서비스사업자(이하 위치정보사업자등)로 규정이 되어 있기 때문이다. 다만, 제15조에서 '누구든지' 개인이나 소유자의 동의없이 위치정보를 수집·이용·제공할 수 없도록 하고 있다. 동법 제2조에서는 '위치정보사업'을 "위치정보를 수집하여 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 것"으로 규정하고 있다(제2조제6호). 그리고 '위치기반서비스사업'은 "위치정보를 이용한 서비스를 제공하는 것을 사업으로 영위하는 것"이라 규정하고 있다(제2조제7호). 따라서 위치정보를 수집하기는 하지만 위치기반서비스사업자에게 정보를 제공하지 않는 기관/업체의 경우 동법의 적용대상에서 제외된다.

예를 들어, 서울시의 '승용차 요일제' 정책에서는 위반 차량에 대한 감시를 목적으로 시내 곳곳에 전자태그 인식기를 설치하고 있다. 인식기는 차량에 부착된 전자태그의 고유번호를 읽어내며, 이를 매개로 승용차 요일제를 신청한 사람들을 관리하는 개인정보 데이터베이스와 연계된다. 인식기에서 수집한 정보만으로는 개인 위치정보를 알 수 없지만, 전자태그 고유번호를 매개로 개인정보 데이터베이스와 연동됨으로써, 특정 개인의 위치를 추적할 수 있게 된다. 즉, 승용차 요일제 정책 수행 과정에서 서울시는 「위치정보법」에서 규정하고 있는 '위치정보' 및 '개인위치정보'를 수집하고 있는 것이다.

한국도로공사에서 시행하는 '하이패스 카드' 역시 마찬가지이다. 고속도로의 하이패스 진·출입 요금소에서는 승용차에 부착된 단말기 번호나 카드번호 등을 인식한다. 이 정보를 매개로 하이패스 신청자의 고객 정보 데이터베이스와 연동이 되며, 이를 통해 개인의 고속도로 진·출입 위치와 시간 등

개인 위치정보를 파악할 수 있게 된다. 대중교통 이용을 위한 교통카드 역시 마찬가지다.

그러나 서울시, 한국도로공사, 그리고 서울 교통카드를 운영하고 있는 한국스마트카드는 동법의 적용을 받지 않는 것으로 보인다. 이 기관/업체들이 동법의 적용을 받는지를 묻는 질의에 대해, 방송통신위원회는 "한국스마트카드(전자금융업자)와 한국도로공사(전자금융보조업자)는 '전자금융거래법'에 따라 교통운임 정산, 카드 사용내역 확인을 위해 금융거래 내역 및 차량통행 정보 등을 수집하고 있고, 서울특별시는 승용차 요일제 위반 조사 목적으로 차량 통행정보를 확인하고 있으며, 위치정보를 이용자에게 부가적인 서비스 형태로 제공하는 것이 아니기 때문에 '위치정보의 보호 및 이용 등에 관한 법률' 제2조제6호 및 제7호에 따른 위치정보사업 및 위치기반서비스사업으로 영위하는 것으로 볼 수 없어 동법에 해당되지 않는 것으로 판단된다"고 밝혔다.[238]

즉, 현행 「위치정보법」은 위치정보를 수집하는 모든 기관/업체에 적용되는 것이 아니라, 수집된 위치정보를 기반으로 이용자에게 서비스를 제공하는 경우에 한하여 적용되는 것으로 판단된다. 그렇다면, 위치기반 서비스를 위한 목적은 아니지만, 위치정보를 수집하고 있는 경우 이렇게 수집된 위치정보에 대해서는 「위치정보법」에 근거한 특별한 보호의 필요성은 없는지에 대한 검토가 필요할 것이다. 「위치정보법」의 제정은 한편으로는 위치정보사업과 위치기반서비스사업의 활성화를 위한 것이기는 하지만, 민감한 개인정보로서 '위치정보'의 보호를 보다 강화하기 위한 것이므로, 수집된 위치정보가 위치기반 서비스를 목적으로 한 것이 아니라고 해서 그 보호의 필요성이 덜한 것으로 보기는 힘들다.

본 연구에서는 「위치정보법」 적용을 받는 위치정보사업에서의 개인정보 수집·유통 실태와 함께, 동법의 적용을 받지 않지만 위치정보라고 규정될 수 있는 교통 관련 위치정보의 실태에 대해서 검토하였다.

## 2. 위치정보사업에서의 개인정보 수집·유통 실태

### 1) 위치정보사업 현황

현재 국내에서는 191개 업체가 위치정보사업 혹은 위치기반서비스사업을

238) '위치정보에 대한 정보공개 청구'에 대한 방송통신위원회의 정보(공개) 결정통지서 (2009.10.29)

하고 있다. 「위치정보법」은 제5조에서 위치정보사업자는 허가를 받아야 함을, 제9조에서 위치기반서비스사업자는 신고해야 함을 규정하고 있다. 방송통신위원회에 대한 정보공개 청구 결과[239], 2009년 10월 현재, 방송통신위원회의 허가를 받거나 신고한 업체 현황은 다음과 같다.

<표 3-13> 위치정보서비스 업체 현황

(2009년 10월 현재)

| 구 분 | 위치정보사업 | 위치기반서비스사업 | 계 |
|---|---|---|---|
| 업체수 | 55 | 136 | 191 |

위치정보사업자 및 위치기반서비스 사업자의 세부 현황은 다음과 같다.

<표 3-14> 위치정보사업 허가 현황

(2009년 10월 현재)

| 구 분 | 허가사업자 (수집방법) (총 55개) |
|---|---|
| 1차('05.10) | SK에너지(GPS), KT파워텔(GPS, 기지국), 현대자동차(GPS), KT(GPS, 기지국), 온세텔레콤(GPS), 이룸지엔지(GPS), 비엔지로티스(기지국), 로티스(기지국), SKT(GPS, 기지국), 대신정보통신(GPS), 썸넷(GPS), 팅크웨어(GPS), LGT(GPS, 기지국), 트라텍정보통신(GPS), KT로지스(GPS), 동부NTS(GPS), 비앤비쏠루션(GPS), 시너소어(GPS, SK M&C(GPS) (19개) |
| 2차('06.1) | 한국위치정보(기지국), BH정보통신(GPS), 엘렉스테크(GPS), 마이텍코리아(GPS), 티온텔레콤(GPS), 백산모바일(GPS) (6개) |
| 3차('06.9) | 에브리웨어(GPS), 코리아오브컴(GPS), 리얼텔레콤(GPS), 넥스모어시스템즈(GPS) (4개) |
| 4차('07.4) | 이케이시스(GPS), 아이엔(GPS), 유비폴로(GPS), 블루칩인터넷(GPS) (4개) |
| 5차('07.8) | SK브로드밴드(RFID), 케이웍스(GPS), 아이원맥스(GPS) (3개) |
| 6차('08.2) | 신동디지텍(GPS), 선진LBS(GPS), 자티전자(GPS), 하나로스쿨네트웍스(RFID) (4개) |
| 7차('08.8) | 동부건설(GPS), 에어미디어(GPS), 외길기업(RFID), 엠앤소프트(GPS), 지센하이텍(GPS), 네오지앤피(GPS), 대진기술정보(GPS) (7개) |
| 8차('09.6) | 에온웨이브(GPS), 셀리지온(GPS), LBC소프트(GPS), 경봉T&C(GPS), 루키스(지그비), 엠투엠글로벌(GPS), 티모넷(USIM내위치), 트윈클리틀스타(GPS) (8개) |

239) '위치정보에 대한 정보공개 청구'에 대한 방송통신위원회의 정보(공개) 결정통지서 (2009.10.29)

<표 3-15> 위치기반서비스 현황

(2009년 10월 현재)

| 위치기반서비스사업자 | | 위치정보사업자 |
|---|---|---|
| 업 체 | 서비스 | |
| SK네트웍스㈜ | 긴급구난 및 물류차량 관제 | SKT |
| ㈜썸넷 | 화물, 택배 등의 차량 관제 | 위치정보사업자 |
| ㈜이룸지엔지 | 길안내, 교통정보 및 주변 생활정보 | 위치정보사업자 |
| 대신정보통신㈜ | 차량 및 개인의 위치조회 | 위치정보사업자 |
| 비앤비쏠루션㈜ | 차량 등 이동체의 위치조회 | 위치정보사업자 |
| ㈜폴리큐브 | 근거리에 있는 개인과 채팅 | SKT, KTF, LGT |
| 포스데이타㈜ | 화물차량 관제 | SKT, KTF |
| SKT㈜ | 친구찾기, 보행자길안내, 폰위치내비게이션, 가족안심, 안심레이더, 자녀안심 등 | 위치정보사업자 |
| 트라텍정보통신㈜ | 대인위치조회, 문자위치관제 | 위치정보사업자 |
| ㈜백산모바일 | 써치온(차량추적, 대리운전, 택시콜) | 위치정보사업자 |
| ㈜엠가온 | 교통정보, 생활정보, 모바일지도 | SKT, KTF, LGT |
| 대한통운㈜ | 차량위치 추적 | SKT, LGT |
| ㈜이직스네트웍스 | 콜8200(택시관제) 서비스 | SKT |
| 한국관광공사 | 여행, 관광정보 제공 | SKT, KTF, LGT |
| ㈜제이엠넷 | 대중교통 정보 제공 | SKT, KTF, LGT |
| ㈜버츄얼웨어 | 위치기반의 채팅, 폰팅 | SKT |
| ㈜로티스 | 차량관제 | 위치정보사업자 |
| ㈜LGT | 친구찾기, 자동위치찾기, 분실폰위치찾기, 알라딘, 2시간보디가드, 아이지킴이, 한눈에 서비스 | 위치정보사업자 |
| ㈜바로바로넷 | 화물차량 관제, 주변검색 | KTF |
| ㈜네오지앤피 | 차량 관제 | SKT, KTF, LGT |
| ㈜아로정보기술 | 지하철역, 버스정류장 검색 | SKT, LGT |
| 블루칩인터넷㈜ | 차량위치조회 | SKT, KTF, LGT |
| ㈜스피드엠 | 위치기반의 채팅 | SKT |
| 카인즈소프트㈜ | 한눈에, 파워트랙, 가족위치조회, 자녀발자취 | LGT, KTF |
| 현대자동차㈜ | 안전구난, 길안내, 교통정보 | 위치정보사업자 |
| ㈜사이넷 | 채팅, 폰팅, 미팅 회원의 위치조회 | SKT, KTF, LGT |
| ㈜마이텍코리아 | 자가용의 위치 및 차량긴급상황정보 제공 | 위치정보사업자 |
| ㈜케이티로지스 | 화물운송조회, 택시안심콜 | 위치정보사업자 |
| SK에너지㈜ | 일반차량관제(엔트랙), 텔레메틱스 | 위치정보사업자 |

| | | |
|---|---|---|
| 포인트아이㈜ | 친구찾기, 굿모닝교통정보 | KTF |
| 모빌토크㈜ | 안전운전지킴이 | SKT, KTF, LGT |
| 케이티하이텔㈜ | 친구찾기, 채팅, 블로그, 메신저 등 | KTF |
| ㈜열정컴퍼니 | 채팅, 폰팅 회원의 위치조회 | SKT, KTF, LGT |
| 유니콘전자통신㈜ | 차량의 위치조회, 이동경로 및 지역이탈 | LGT |
| 씨엔에스캠프㈜ | 법인차량 및 직원의 위치추적 | KTF |
| ㈜파네즈 | 채팅, 폰팅 회원의 위치조회 | SKT |
| ㈜한국데이타하우스 | 모바일미팅, 채팅, 회원의 위치조회 | KTF, LGT |
| ㈜엠프리아이 | 미팅회원간에 접속위치 조회 | SKT |
| ㈜극동네트워크 | 인근 모바일적립, 할인 가맹점 검색 | SKT |
| ㈜네멕스 | 위치기반의 채팅, 미팅 | SKT |
| 케이아이티㈜ | 법인의 차량 및 직원의 현재위치 및 이동경로 조회 | SKT, KTF, LGT |
| 팅크웨어㈜ | 모여라친구, 안심레이더, 신기한 일기 | 위치정보사업자 |
| KT파워텔㈜ | 친구찾기 | 위치정보사업자 |
| ㈜인포러스 | 위치정보포함 메일링서비스 | SKT |
| ㈜쏘바쥬 | 위치기반의 채팅, 미팅 | SKT |
| ㈜케이씨인벤티드 | 인접 대리운전, 퀵, 화물, 콜택시 | SKT, KTF |
| ㈜KT | 친구찾기, 자동위치, 안심귀가, 길안내, 아이서치, SEND위치, 모바일출동, 전국대표전화, 어린이안심, Logis(CVO), Wibro검색・교통・모바일광고, Myisafe 등 | 위치정보사업자 |
| ㈜메타미디어 | 회원간 대화방, 폰팅 | SKT, KTF, LGT |
| ㈜테크노코리아 | 차량관제 | SKT, KTF, LGT |
| ㈜로코모 | 최인접 로또판매점 조회, 길찾기 | SKT, KTF, LGT |
| ㈜제니큐 | 전국 주유소・주차장・세차장 조회 | SKT, KTF, LGT |
| ㈜모바일큐브 | 전화번호, 업종, 상호 검색 | SKT |
| ㈜메그 | 위치기반의 미팅, 채팅 | SKT |
| 야후코리아㈜ | 친구찾기, 한눈에, 자동위치찾기, 주변정보 | SKT, KTF, LGT |
| ㈜파스넷 | 유가 및 주유소 정보 제공 | SKT |
| ㈜ADT캡스 | 긴급출동 | 한국위치정보㈜ |
| 리얼텔레콤㈜ | 실시간 교통정보 | 위치정보사업자 |
| ㈜네모드림 | 커뮤니티 미팅(SMS전송) | SKT |
| ㈜모비오 | 위치기반 채팅 | SKT |
| ㈜알리트 | 개인위치정보 조회 | SKT |

| | | |
|---|---|---|
| ㈜크레디프 | 카드안심, 카드가맹점 조회 | SKT, KTF |
| 티온텔레콤㈜ | 차량 관제 | 위치정보사업자 |
| ㈜엘비에스플러스 | 위치그림친구, 위치기반 채팅 | SKT |
| ㈜지오텔 | 모바일택시캅(승객이 지정한 사람에게 택시정보 전송), 운세정보 | KTF |
| 케이웨더㈜ | 내위치기반 실시간 날씨 제공 | SKT, KTF, LGT |
| ㈜아이원맥스 | 대리운전, 퀵서비스, 물류관제 | 위치정보사업자, KTF |
| ㈜라이온로직스 | 위치기반의 채팅 | SKT |
| ㈜에브리웨어 | 차량관제 | 위치정보사업자 |
| ㈜배리스 | 안심맞춤 택시콜 | LGT |
| 아이넥스네트워크㈜ | 모바일미팅 | SKT |
| ㈜데이콤 | 전국대표번호서비스(발·착신자의 위치정보 활용 전화연결 및 위치안내) | SKT, KTF, LGT |
| ㈜아레오네트웍스 | 주변의 신용카드 할인율 및 포인트 적립 혜택 가맹점 조회 | SKT, KTF |
| SKCTA㈜ | 화물차량 위치관제, 긴급출동 | SKT, KTF, LGT |
| 한국위치정보㈜ | 대인 안심보호, 차량위치확인, 자산관리 | 위치정보사업자 |
| ㈜에스원 | 버스승차, 물류 및 폐기물 관리 | SKT |
| 동부NTS㈜ | 콜택시 관제 | 백산모바일, KTF, 리얼텔레콤 |
| 사이트온㈜ | 버스정류장, 지하철역 검색 | SKT, KTF, LGT |
| ㈜플레이에듀테인먼트 | 친구찾기, 주변정보, 긴급출동, 교통정보 | LGT |
| 스미스앤모바일㈜ | 운세(풍수지리)정보제공 | SKT, KTF, LGT |
| ㈜네비웍스 | 선박 위치조회 | 코리아오브컴 |
| ㈜유비플로 | 콜택시 | 위치정보사업자 |
| ㈜이케이시스 | 차량관제 | 위치정보사업자 |
| ㈜온세일육팔오 | 음성포털서비스(대리운전, 퀵, 주문배달) | SKT, KTF, LGT |
| ㈜한국스마트카드 | 교통정보, 콜택시 | SKT, KTF, LGT |
| ㈜야호커뮤니케이션 | 차량 관제(대리운전, 퀵, 콜택시, 화물차량) | SKT, KTF, LGT |
| SK브로드밴드㈜ | 브로드앤 스쿨케어, 대표번호 서비스 | SKT, KTF, LGT |
| ㈜투비플라자 | 긴급출동 | SKT, KTF, LGT |
| ㈜와이즌네트웍 | 장애인 등 이동경로 제공 | SKT |
| 인포뱅크㈜ | 위치기반의 MO(방송참여, 리서치)서비스 | SKT, KTF, LGT |
| ㈜아이엔 | 차량위치조회 및 도난방지 | 위치정보사업자 |

| | | |
|---|---|---|
| 시너소어㈜ | 차량관제, 교통정보 | 위치정보사업자 |
| 서울씨티콜㈜ | 차량관제 | SKT |
| ㈜엘비씨소프트 | 개인위치 및 이동경로 제공 | SKT, KTF, LGT |
| ㈜컴투스 | 골프캐디(골프장 홀컵까지 거리 측정) | SKT, KTF, LGT |
| ㈜이에스시미어 | 정보화마을 정보제공 | SKT |
| 동부익스프레스 | 택시콜관제 | ㈜백산ITS |
| ㈜선진엘비에스 | 차량관제 | 위치정보사업자 |
| ㈜비앤지로티스 | 실시간 교통정보, 차량관제 및 위치추적 | 위치정보사업자 |
| ㈜한국위치정보 래스큐 | 인터넷 위치조회, 긴급출동 | SKT |
| ㈜바인아이엔지 | 채팅, 미팅, 러브콜114, 내근처100m친구 | KTF, LGT |
| ㈜케이웍스 | ARS친구찾기, 휴대전화대표번호 | SKT, KTF, LGT |
| ㈜동일정보통신 | 위치기반의 대리운전 | KTF |
| ㈜인포렉스 | 모바일 위치조회 | SKT, KTF, LGT |
| (유)엔와이텔 | 위치조회 및 데이트 쪽지(SMS)전송 | SKT, KTF, LGT |
| 제주존 | 텔레가이드 | SKT |
| ㈜미투데이 | 미투데이블로그 입력시 위치표시 | KTF |
| ㈜애니와이드 | 모바일채팅회원에 대한 위치조회 | SKT |
| ㈜지센하이텍 | 차량관제, 대인 위치조회 | ㈜에브리웨어 |
| SK커뮤니케이션㈜ | 유·무선간 친구찾기서비스 | SKT, LGT, KTF |
| ㈜지로커뮤니케이션 | 대리운전, 콜택시, 이삿짐 배달, 택배, 퀵서비스 항공권 발권대행 | SKT, LGT, KTF |
| ㈜MSP테크놀로지 | 콜택시 및 대리운전기사 제공 | SKT |
| 삼성네트웍스㈜ | 차량의 위치확인 및 경로추적 | SKT, KTF, LGT |
| ㈜에어미디어 | 개인 및 대물의 위치확인, 이동경로, SOS, 안심존이탈알림 | 위치정보사업자 |
| ㈜텔넷웨어 | 특수직무종사자의 위치조회 | SKT, KTF, LGT |
| ㈜BH정보통신 | 차량의 위치확인 및 이동경로 확인 | 위치정보사업자 |
| SK마케팅&컴퍼니㈜ | 모바일LBS, 차량(버스, 택시 등)관제 | 위치정보사업자 |
| SK네트웍스㈜ | FMS(법인차량관리시스템)서비스 | SK마케팅&컴퍼니 |
| ㈜다우기술 | 위치조회, 자동위치알림, 이동경로 조회 | 이통3사 |
| 유빈스㈜ | 본인의 위치관할 지방자치단체의 홈페이지 제공 | 이통3사 |
| ㈜다음커뮤니케이션 | 친구찾기, 주변정보를 모바일로 제공 | SKT |
| ㈜네오펙스 | 모바일 상에서의 회원간 채팅서비스 | 이통3사 |
| ㈜지어소프트 | 본인인근의 교통정보, POI제공 | 이통3사 |

| | | |
|---|---|---|
| ㈜메트로이플로직스 | 회원 근거리의 콜택시, 대리운전기사 제공 | 이통3사 |
| ㈜티모넷 | 티머니가맹점, 인근 버스정류장, 지하철역 찾기, 안심알리미 | 이통3사 |
| ㈜오토라이프테크 | 인근 콜택시 제공 서비스 | 이통3사 |
| 나인타임즈㈜ | 퀵서비스 제공 | SKT |
| ㈜정진하이테크 | 차량위치, 이동경로 서비스 | KTF |
| ㈜유비홈스커무니케이션 | 차량관제, 물류관제, 위치확인 | KTF, 동부건설 |
| ㈜필링크 | 본인주변 생활정보 제공 | 이통3사 |
| ㈜코리아로지스 | 차량의 위치확인서비스 제공 | KIP(파워텔) |
| 동룡에이치엔케이㈜ | 차량의 위치확인 및 궤적서비스 제공 | SKT |
| ㈜엠앤소프트 | 웹사이트 회원 상호간의 위치조회 | 위치정보사업자 |
| 서울특별시 | 시민의 위치기반 생활정보 제공 | 이통3사 |
| ㈜이투엠커뮤니케이션 | 자기주변의 이벤트 등 광고성정보전달 | 이통3사 |
| ㈜네오넥스소프트 | 대인 및 대물 위치조회, 안심존이탈, 이동경로조회, SOS서비스제공 | SK M&C |
| 강원도청 | 본인 주변의 관광정보 제공 | 이통3사 |

※ 위치정보사업자 열의 '위치정보사업자'는 해당 위치기반서비스사업자가 위치정보사업자를 겸업하는 경우를 의미함.

위 표에서 볼 수 있다시피, 위치기반서비스사업자들은 대인, 차량, 물건 등에 대한 위치추적 등을 통해 다음과 같은 서비스를 주로 제공하고 있다.

- 아동, 치매노인 등에 대한 신변보호 서비스
- 화물, 택배 등 차량/선박 관제
- 교통정보 등 주변 생활정보, 혹은 여행이나 관광정보 제공
- 대리운전, 택시콜
- 친구찾기, 모바일 채팅, 폰팅, 미팅 등

### 2) 위치정보의 수집

위치정보는 위치정보사업자에 의해 수집되어, 위치기반서비스사업자에게 제공된다. 위치정보사업자가 위치기반서비스사업을 겸하는 경우도 많다. 위치기반서비스 현황에 따르면, 위치정보사업자가 직접 위치기반서비스사업을 하는 경우가 아닌 경우, 대부분의 위치기반서비스사업자가 3개 이동통신사로부터 위치정보를 제공받고 있다.

현재 국내에서는 위치정보의 파악을 위해 GPS 신호와 이동통신 기지국의 Cell-ID 정보가 주로 활용되고 있으며, 최근 구축되고 있는 와이브로(WiBro) 기지국의 위치정보도 일부 활용되고 있는 것으로 보인다(오상진, 2009:36). '위치정보사업 허가 현황'에서도 GPS와 기지국이 위치정보 수집방법으로 가장 광범위하게 이용되고 있는 것을 확인할 수 있다.

GPS 정보는 네비게이터(Navigator) 등에서 지금도 광범위하게 활용되고 있지만, 기존의 핸드폰에 GPS 수신기능을 추가하면 이전의 기지국(Cell-ID) 방식에 비하여 위치정보의 정확도가 월등히 높아진다. 방식에 따라 위치정보의 정확도가 다른데, GPS 방식이 기지국(Cell-ID) 방식보다 정확도가 월등히 높아서 위치기반 서비스의 발전에 따라 활용도가 높아질 것으로 보인다(오상진, 2009:36).

<표 3-16> 위치정보의 정확도 비교

| 구분 | 네트워크 기반 Cell-ID방식 | GPS 활용 방식 |
|---|---|---|
| 정확도 | 500m(도심) ~ 5Km(외곽) | 10m(개활지) ~ 150m(도심) |

자료: 오상진(2009: 36).

위 표에서 볼 수 있다시피, GPS 정보는 개인의 실제 위치를 특정할 수 있을 정도의 정확도를 갖고 있다. 방송통신위원회는 2008년 11월 28일 발의한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 현행 「위치정보법」을 통합하면서, 위치정보사업자가 긴급구조기관 또는 경찰관서에 제공하는 개인위치정보의 위치 정확도에 관한 기준을 정하여 고시할 수 있도록 하고 있다(안 제78조의 9항). 이는 위치정보의 정확도를 높일 수 있는 법적인 근거를 마련하기 위한 일환인데, 이는 신중하게 이루어질 필요가 있다. 정확한 위치정보의 수집은 양질의 서비스를 제공하기 위한 조건이 되기도 하지만, 위치정보의 정확도가 높아질수록 프라이버시 침해 위험도 높아질 수 밖에 없기 때문이다. 예를 들어, 이동통신 단말기에 GPS 수신 기능을 의무화한다면, 이는 위치기반 서비스를 원하지 않는 이용자의 위치정보까지 정확하게 수집될 위험이 있다. 따라서 양질의 위치기반 서비스를 위해 위치정보의 정확도를 높이려는 노력을 할 수는 있지만, 그러한 서비스를 원하지 않는 이용자의 선택권을 배제하지 않도록 할 필요가 있다.

각 위치정보사업자 및 위치기반서비스사업자의 가입자 규모의 전반적인 현황은 파악하기 힘들다. 다만, 방송통신위원회에서 공개한 아동위치추적 서비스 현황은 다음과 같다.

<표 3-17> 아동 위치추적 서비스 현황

| 업 체 | 서비스명 | 위치정보 보관기간 | 제공 주기 | 가입자 |
|---|---|---|---|---|
| SKT | **자녀안심 서비스** 내 아이발자취 | 24시간 | 1일 8회 (자유 설정) | 23만 명 |
| KTF | **아이서치 서비스** 내 아이발자취 | 48시간 | 매 1,2,3시간 단위 | 48만 명 |
| LGT | **아이지킴이 서비스** 내 아이발자취 | 48시간 | 매 1,2,3시간 단위 | 8만 명 |

자료: 아동 위치추적 서비스 현황, 방송통신위원회 네트워크 정책국 블로그, 2009년 4월 1일자 게시물. http://blog.daum.net/internetclub/44.

### 3) 개인위치정보의 제3자 제공

개인위치정보가 제3자에게 제공되는 경우는 크게 두 가지로 구분할 수 있을 것이다. 하나는 개인위치정보의 제3자 제공 자체가 위치기반서비스에 포함되는 경우, 다른 하나는 긴급구조기관 등 공공기관에 제공되는 경우이다.

위치정보사업자가 수집한 개인위치정보는 정보주체의 동의를 얻어 위치기반서비스사업자에게 제공된다. 「위치정보법」 제19조제1항은 위치기반서비스사업자가 개인의 동의를 얻을 때 △ 위치기반서비스사업자의 상호 및 연락처, △ 정보주체의 권리 및 행사방법, △ 위치기반서비스의 내용, △ 위치정보 이용·제공사실 확인자료의 보유근거 및 보유기간 등을 이용약관에 명시하도록 하고 있다. 위치기반서비스사업자가 개인위치정보를 제3자에게 제공할 경우에도 마찬가지이다.

그런데, 이와 같은 위치기반 서비스는 비록 적법하게 이루어진다고 하더라도, 프라이버시 침해 가능성이 존재한다. 자녀, 노인, 장애인 등에 대한 신변보호 서비스의 경우, 사회적 약자에 대한 보호라는 명분을 가지고 있지만, 경우에 따라 이들에 대한 감시로 기능할 수 있다. 차량 관제 서비스의 경우에도 물류 사업의 효율성을 높이기 위한 목적을 가지고 있지만, 동시에 차량을 운전하는 노동자 입장에서는 자신에 대한 감시로 인식될 수 있다.

개인위치정보주체의 보호를 위해 「위치정보법」 제19조제3항은 위치기반서비스제공자가 개인위치정보를 제3자에게 제공하는 서비스를 할 경우,[240] 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보

240) 예를 들어, 아동이나 치매노인 등에 대한 신변보호서비스, 친구찾기 서비스, 차량관제 서비스 등이 모두 이에 해당한다.

하도록 하고 있다.[241] 그러나 비록 정보주체의 동의가 있었다고 하더라도, 사회 관계에서 약자인 자녀, 노인, 장애인, 노동자 등이 현실적으로 이에 대한 동의를 거부하기 힘든 상황이라는 점을 고려하면, 이러한 위치기반 서비스가 약자에 대한 감시로 기능할 가능성을 배제하기 힘들다.

「위치정보법」 제29조는 긴급구조를 위해 긴급구조기관(「재난 및 안전관리 기본법」 제3조제7항에 따른 긴급구조기관으로, 소방방재청·소방본부 및 소방서를 말한다. 해양에서의 재난의 경우에는 해양경찰청·지방해양경찰청 및 해양경찰서를 말한다)이 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있도록 하고 있다. 소방방재청의 조사에 따르면 신고를 접수하여 사고현장으로 출동하기까지 소요되는 시간이 위치정보를 사용하기 이전보다 약 37분 정도 단축되었다고 한다(오상진, 2009: 37). 방송통신위원회에 대한 정보공개 청구 결과에 의하면, 긴급구조를 위한 위치정보 제공건수는 다음과 같다. 이를 보면, 매해 그 활용도가 증가하고 있음을 알 수 있다.

<표 3-18> 긴급구조를 위한 위치정보 조회수

| 구분 | | 07년 | 08년 | 09년 8월말 |
|---|---|---|---|---|
| SKT | 소방방재청 | 1,816,712 | 4,761,289 | 2,116,039 |
| | 해양경찰청 | 3,476 | 2,806 | 606 |
| | 소계 | 1,820,188 | 4,764,095 | 2,116,645 |
| KT(KTF) | 소방방재청 | 1,006,769 | 1,041,531 | 774,962 |
| | 해양경찰청 | 485 | 835 | 168 |
| | 소계 | 1,007,254 | 1,042,366 | 775,130 |
| LGT | 소방방재청 | 845,040 | 1,040,457 | 710,198 |
| | 해양경찰청 | 180 | 329 | 80 |
| | 소계 | 845,220 | 1,040,786 | 710,278 |
| 합계 | 소방방재청 | 3,668,521 | 6,843,277 | 3,601,199 |
| | 해양경찰청 | 4,141 | 3,970 | 854 |

「위치정보법」 제29조는 긴급구조를 위해 위치정보사업자에게 개인위치정보를 요청할 수 있는 기관을 소방방재청 및 해양경찰청 등 긴급구조기관에 한정하고 있으나, 이에 경찰관서를 포함시켜야 한다는 요구가 동법 제정 당시부터 존재했다. 2008년 11월 28일 정부가 발의하여 2009년 10월 현재 국

241) 이는 주로 이동통신 서비스에 기반한 서비스를 염두에 둔 조항으로 보인다.

회에 계류되어 있는 「정보통신망 이용촉진 및 정보보호에 관한 법률」 개정안(의안번호 제1802396호)은 「위치정보법」 전부를 이 법에 통합하면서 경찰관서에서도 위치정보사업자로부터 개인위치정보를 요청할 수 있도록 허용하고 있다. 애초에 「위치정보법」 제29조에서 경찰관서를 제외한 것은 수사기관에 의한 개인위치정보의 남용을 우려했기 때문이다.

그러나 경찰 등 수사기관은 이미 수사목적으로는 개인위치정보를 제공받아온 것으로 드러났다. 2009년 10월 22일 발표된 변재일 의원실 보도자료에 따르면, 수사기관은 관행상 '통화내역'이라는 명목으로 발신기지국기록(개인위치정보)를 포함시켜 제공받아왔고, 통신사실 확인자료 중 '발신기지국의 위치추적자료'(「통신비밀보호법」 제2조제11호바목)는 사실상 미래 감청(실시간 위치추적)의 용도로 사용해 왔다. 발신기지국 위치추적자료의 경우 법원의 허가서에 발급일로부터 언제까지 사용하라는 의미의 사용기한만 적시하여 발급되고 있으며, 허가서가 발급되면 허가서에 적힌 사용기한 동안, 통화가 발생하지 않더라도 매 10분 또는 30분 간격으로 자동으로 단말기의 위치를 확인하고, 기지국의 위치정보를 담당 수사관의 휴대폰 SMS로 발송하는 방식으로 이루어졌다. 사업자는 이러한 위치추적정보 데이터는 저장하지 않고 발송 즉시 삭제한다고 한다. 이렇게 통신사실 확인자료를 이용하여 휴대전화 실시간 위치추적을 한 건수가 2009년 상반기에만 9,647건에 이르며, 2년 반동안 4만 건이 넘었다(변재일, 2009). 통신사실 확인자료에 대한 규정을 신설할 당시 접수시점 이전의 자료에 한정되는 의미였다는 점에서, 이는 「통신비밀보호법」의 편법 적용으로 관련 규정의 보완이 필요하다(제3장 제4절 참조). 또한, 위치기반서비스 사업이 활성화로 개인위치정보의 수집이 증가할 경우, 개인위치정보가 수사기관에 더욱 쉽게 노출될 가능성을 보여준다.

### 4) 정보주체의 열람 및 정정·삭제 청구권

「위치정보법」 제24조[242]는 개인위치정보주체의 권리를 규정하고 있다.

---

242) 제24조 (개인위치정보주체의 권리 등) ①개인위치정보주체는 위치정보사업자등에 대하여 언제든지 제18조제1항 및 제19조제1항·제2항의 규정에 의한 동의의 전부 또는 일부를 철회할 수 있다.
②개인위치정보주체는 위치정보사업자등에 대하여 언제든지 개인위치정보의 수집, 이용 또는 제공의 일시적인 중지를 요구할 수 있다. 이 경우 위치정보사업자등은 요구를 거절하여서는 아니되며, 이를 위한 기술적 수단을 갖추어야 한다.
③개인위치정보주체는 위치정보사업자등에 대하여 다음 각호의 1의 자료 등의 열람 또는 고지를 요구할 수 있고, 당해 자료 등에 오류가 있는 경우에는 그 정정을 요구할 수 있다. 이 경우 위치정보사업자등은 정당한 사유없이 요구를 거절하여서는 아니된다.

이에는 △ 동의의 철회권, △ 개인위치정보의 수집, 이용 또는 제공의 일시적인 중지 요구권, △ 자기정보에 대한 열람권 등이 포함된다. 개인위치정보주체가 열람할 수 있는 정보는 △ 본인에 대한 위치정보 수집・이용・제공사실 확인자료, △ 본인의 개인위치정보가 제3자에게 제공된 이유 및 내용 등이다.

본 연구에서는 한 이동통신사에 대해 개인위치정보에 대한 열람청구를 해보았으나 거부당했다.[243] 우선 한 이동통신사의 대리점을 방문하여, 열람청구자의 과거 1개월 치에 대한 통화내역을 요청했으며, 통화내역의 출력본을 받을 수 있었다. 통화내역 출력본은 발신번호, 통화시각, 이용한 서비스(일반음성통화, 문자메시지), 사용시간, 통화량 도수(kb), 할인전금액, 할인금액, 청구금액, 할인내용 서비스설명 등의 정보를 담고 있었으나, 통화한 기지국 위치에 대한 정보는 없었다. 이에, '통화내역에 기지국 정보 자체가 없는 것인지, 아니면 기록은 되어 있지만 제공할 수 없는 것인지'에 대해서 재차 문의하였다. 그 결과 다음과 같은 답변을 받을 수 있었다.

> 위치정보법 제24조와 개인정보보호지침(방송통신위원회고시) 제21조에 의하면 이용자가 위치정보 또는 개인정보 등의 열람/제공 요구를 하더라도 회사는 정당한 사유가 있으면 이를 거절할 수 있는 부분입니다.
> 고객님께서 확인을 원하셨던 통화한 위치 즉 기지국 위치는 원칙적으로 제공되지 않는 정보입니다만, 고객님께서 위치정보가 필요한 사유를 입증자료와 함께 소명하면서 제공요청을 해주시면 그 필요성이 인정된 경우에 한해서 예외적으로 제공 가능한 점 양해 부탁드립니다.
> 보내주신 내용만으로는 어떠한 특별한 사유로 인해서 또는 개인적인 호기심으로 인해서 확인을 원하시는 것인지 파악이 어렵습니다만, "위치정보의 관리적/기술적 보호조치 가이드라인 해설서(방통위 작성)"에 따라 단순 개인정보 열람/제공을 제한 없이 허용하면서 이러한 요구를 하는 고객이 늘어나 회사의 업무에 현저한 지장을 미칠 우려가 있거나 고객의 과도한 요구로 판단되는 등의 특별한 사유 없이 단순한 호기심에 의해서는 제공이 어려운 점 다시 한번 양해 부탁드립니다.

---

1. 본인에 대한 위치정보 수집・이용・제공사실 확인자료
2. 본인의 개인위치정보가 이 법 또는 다른 법률의 규정에 의하여 제3자에게 제공된 이유 및 내용

④위치정보사업자등은 개인위치정보주체가 제1항의 규정에 의하여 동의의 전부 또는 일부를 철회한 경우에는 지체없이 수집된 개인위치정보 및 위치정보 수집・이용・제공사실 확인자료(동의의 일부를 철회하는 경우에는 철회하는 부분의 개인위치정보 및 위치정보 이용・제공사실 확인자료에 한한다)를 파기하여야 한다.

243) 이 열람청구는 이동통신사에 대한 개인정보 열람청구와 함께 이루어졌다. 제2장 제3절 참고.

그러나 「위치정보법」 제24조는 오히려 '위치정보사업자등은 정당한 사유 없이 요구를 거절하여서는 아니된다'고 규정하고 있다. 이에 근거하면 '기지국 위치는 원칙적으로 제공되지 않는 정보'이고, '그 필요성이 인정된 경우에 한해서 예외적으로 제공 가능'하다는 답변은 법에서 규정한 것과 맞지 않는다.

한편, <위치정보의 관리적·기술적 보호조치 가이드라인 해설서>에는 정보주체의 열람 요구를 거절할 수 있는 경우를 다음과 같이 제시하고 있다.

> 열람·고지 및 정정요구의 거절 : 위치정보사업자등이 열람 또는 정정요구를 거절할 수 있는"정당한 이유"로는 열람•정정요구를 한 개인위치정보주체가 본인이 정당한 권한 있는 자임을 입증할 수 있는 본인확인을 위한 자료를 제출하지 않은 경우, 지나치게 과도하고 반복적으로 열람요구를 하여 업무에 중대한 지장을 초래하는 경우, 본인이 아닌 제3자의 자료를 요구하는 경우 등이 해당될 수 있을 것이다.

그러나 열람청구자는 본인확인을 하였고, 개인위치정보 열람청구는 이번이 처음이었으며, 본인의 개인위치정보를 요구했다는 점에서 거절 사유에 해당하는 것이 없어 보인다. 이에 다시 한번 개인위치정보를 열람하게 해줄 것을 요청하였으나, 문의를 한 지 한 달이 넘어서야 다음과 같은 답변을 받을 수 있었다.

> 우선 고객이 열람, 제공을 요구한 통화내역과 기지국 위치정보는 통신비밀번호법 상의 통신사실 확인자료에 해당하므로(통화내역은 전기통신개시·종료시간, 착/발신통신번호 등 상대방의 가입자 번호, 사용도수에 해당하며, 기지국 위치정보는 발신기지국의 위치추적자료와 접속지의 추적자료임. 통신비밀보호법 제2조 11호 참조) 유권기관의 해석에 따라 고객님의 요구에 응해 드릴 수 없는 점 양해 부탁드립니다.
> 다만, 이는 9월 11일자 법제처의 유권해석에 따른 것으로서 그 이전에 고객께 제공된 통화내역은 어쩔 수 없더라도 앞으로는 통화내역 제공이 불가합니다.
>
> ★참고
> 제3조(통신 및 대화 비밀의 보호)
> 누구든지 이 법과 형사 소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열. 전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인과의 대화를 녹음 또는 청취하지 못한다.

오히려 통화내역 제공까지 불가능하다는 답변이 왔다. 그러나 해당 이동통신사 콜센터에서는 앞으로 통화내역이 제공되지 않는다는 공지가 난 바가 없다고 답변하였다. 정보주체가 본인의 통화내역을 열람할 권한이 있다면 기지국정보까지 제공하지 못할 이유가 없으며, 「통신비밀보호법」에 근거하여 통신사실 확인자료를 제공할 수 없다면, 여타 통화내역 정보까지 제공하지 않아야 일관성이 있을 것이다. 그러나 「통신비밀보호법」이 정보주체에 대한 통화내역 제공까지 금지하는 것이라고 해석해도 문제는 남는다. 수사기관에는 제공되는 통화내역을 제3자도 아닌 정보주체에게 제공하지 않는 것은 정보주체의 알 권리를 과도하게 제한하는 것이기 때문이다. 어쨌든 「위치정보법」 제24조에서 규정한 개인위치정보의 권리가 제대로 보장되지 않고 있는 것은 분명하다.

## 3. 교통 관련 위치정보의 수집·유통 실태

### 1) 승용차 요일제

'승용차 요일제'란 에너지 절약과 교통 체증 완화를 목표로 서울시에서 추진하고 있는 정책으로, 월~금요일 중 하루를 쉬는 날로 정해 해당 요일에는 차량을 운행하지 말자는 캠페인이다. 승용차 요일제 참여자에게는 자동차세나 공영주차장 요금 할인 등 혜택이 주어진다. 그러나 '시민실천운동'이라는 이름에 무색하게, 승용차 요일제의 실효성을 위해 위반 차량을 감시하는 시스템을 운영하고 있다. 승용차 요일제 참여 차량의 앞 유리면에 운휴일과 고유번호가 내장된 전자태그(RFID Tag)를 부착케 하고, 곳곳의 교통시설물에 전자태그를 읽을 수 있는 인식기를 설치하여 준수 여부를 확인하는 것이다.

서울 시내에 설치된 인식기를 통해 기록된 전자태그 정보는 그 자체로 개인정보는 아니지만, 전자태그 고유번호를 매개로 승용차 요일제 참여자 데이터베이스와 연계될 수 있어, 사실상 승용차 요일제 참여자의 운행 정보가 기록되는 것이나 다름없다. 이 때문에 승용차 요일제의 시행과 함께 프라이버시 침해 논란이 제기되었는데, 이는 국정감사에서도 지적된 바 있다. 2006년 한국정보보호진흥원에 대한 국정감사에서 류근찬 의원은 승용차 요일제가 RFID 프라이버시 보호 가이드라인(이하 RFID 가이드라인)[244]을 준수하지 않고 있다고 비판하였다.[245] 즉, 승용차 요일제 가입신청 시, 자신의 운행정보

244) RFID 프라이버시 보호 가이드라인은 (구)정보통신부와 한국정보보호진흥원이 2005년 처음 제정하였으며, 2007년 일부 개정되었다.

가 기록되는 등의 개인정보 유출 우려에 대한 경고문이 없어 가이드라인 제6조를 위반하고 있다는 것[246], 그리고 서울시가 불법 주정차 단속요원들에게 휴대 기기를 지급해 전자태그 미부착이나 요일제 위반 여부를 적발할 계획인데 이는 '리더기의 설치 사실을 이용자가 용이하게 인식할 수 있도록 표시하도록 한' 제10조[247]를 위반했다는 것이다.

승용차 요일제가 RFID 가이드라인을 준수하고 있는지에 대한 질의에 대해 서울시는 준수하고 있다고 답변하였다.[248] 그 적용방식에 대해서는 △ 제4조 제1항 (개인정보 기록의 금지 충족) : 전자(RFID)태그에 개인정보 기록하지 않음, △ 제4조제2항(개인정보의 기록목적 및 이용목적 등을 고지 충족) : 신청서에 수집정보 이용목적 명시, △ 제10조(RFID 리더기 설치의 표시 충족) : RFID 리더기(인식기) 설치 100m 전방에 안내 표지판(안내 표지판 문구 : 승용차요일제 검지장소) 설치, △ 제13조(개인정보관리책임자의 지정 요건 충족) : RFID시스템 운영 관련 개인정보 관리책임자 지정 운영 등을 적용하고 있다고 답했다. 그러나 제4조[249] 제2항은 RFID에 개인정보를 기록할 경우의 규정으로 승용차 요일제는 RFID에 개인정보를 기록하지 않기 때문에 관계가 없으며, 류근찬 의원이 지적한 제6조 위반에 대해서는 답변하지 않았다. 아래 '이용자 유의사항'에도 RFID 태그의 정보와 개인정보의 연계에 대해서 명확하게 설명하고 있지 않다. 제10조와 관련해서도 단속요원들에게 지

---

245) 아이뉴스24. 2006.7.3. "[국감] "RFID 승용차요일제, 프라이버시 침해""

246) RFID 프라이버시 보호 가이드라인 제6조제1항은 다음과 같다.

제6조(RFID태그의 물품정보 등과 개인정보의 연계) ①RFID 취급사업자는 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우에는 미리 그 사실을 당해 이용자에게 통지하거나 쉽게 알아볼 수 있는 방법으로 표시하여야 한다.

승용차 요일제 RFID의 경우에는 개인정보를 담고 있지는 않으며, 다만 개인정보와 연계될 수 있다.

247) 제10조(RFID 리더기 설치의 표시) 누구든지 RFID 태그가 부착 또는 내장되어 이용자에게 교부된 물품에 대한 정보 또는 RFID 태그에 기록된 개인정보를 판독할 수 있는 리더기를 설치한 경우에는 리더기가 설치되어 있다는 사실을 이용자가 용이하게 인식할 수 있도록 표시하여야 한다. 다만, 물류유통·내부 보안유지·재고 관리를 목적으로 리더기를 설치하거나 고정된 장소에 설치되지 않아 설치장소를 용이하게 표시하기 힘든 경우에는 그러하지 아니하다.

248) '승용차 요일제 관련 정보공개 청구'에 대한 서울특별시의 정보(공개) 결정통지서 (2009.11.05) : 문서번호 기후변화담당관-3860 (2009.11.05)

249) 제4조(개인정보 기록의 금지 등) ①RFID 취급사업자는 RFID 태그에 개인 정보를 기록하여서는 아니 된다. 다만, 법률에 정한 경우 또는 서면 등을 통한 이용자의 명시적인 동의가 있는 경우는 그러하지 아니하다.

②RFID 취급사업자는 제1항 규정에 의한 동의를 얻고자 하는 경우에는 당해 이용자에게 미리 개인정보의 기록목적 및 이용목적 등을 고지하여야 한다.

급되는 휴대기기에 대해서는 답변하지 않았다.

승용차 요일제는 서울시 혹은 승용차 요일제 전용 홈페이지(http://no-driving.seoul.go.kr)에서 신청할 수 있으며, 동사무소나 구청을 방문해서 신청해도 된다. 승용차 요일제 홈페이지의 가입신청 메뉴를 클릭하면, 먼저 '이용자 유의사항'에 동의하도록 하고 있다. 이용자 유의사항 중 전자태그와 인식기를 통한 개인정보 수집과 관련된 조항은 다음과 같다.

(7) 희망 운휴일에 운행하여 도로에 설치된 RFID인식기를 통해 미준수 정보가 확인되거나, 점검인력에 의하여 전자태그 미부착 및 훼손 등이 확인되는 경우에는 신청서에 기재된 안내사항 수신방법에 따라 통지해 드립니다.

(8) 전자태그에는 차량의 운휴일 정보와 전자태그의 고유번호가 입력되어 있고, 신청인 차량의 참여정보 및 운휴일 미준수 정보 등 RFID시스템에 저장·처리되는 모든 개인정보는 『공공기관의 개인정보보호에 관한 법률』에 의하여 안전하게 보관·관리되고 있으며, 이용기간 종료 시 지체없이 폐기되고 있습니다. 또한, 운휴일 준수확인을 통한 참여혜택 제공을 위하여 시설관리공단, 승용차요일제 할인 상품 보험사(해당상품 가입자정보에 한함) 등에 제공될 수 있으며, 그 이외의 목적으로는 사용되거나 제공되지 않습니다.
RFID 시스템 운영 관련 개인정보 관리책임자는 서울시 친환경교통담당관(02-2115-7735,7)입니다.

그러나 이용자 유의사항에는 승용차 요일제를 통해 개인위치정보가 수집된다는 사실을 명확하게 공지하고 있지는 않고 있다. 다만, 'RFID 인식기를 통해 미준수 정보가 확인'된다고 언급하고 있을 뿐이다. RFID 가이드라인 제16조[250]는 RFID 시스템을 통해 개인 위치정보가 수집되는 경우 「위치정보법」에 따른다고 규정하고 있다. 그러나 이용자 유의사항과 승용차 요일제 홈페이지에는 위치정보의 수집이나 「위치정보법」 적용 여부와 관련한 아무런 언급도 없다.

이용자 유의사항에 동의하면, 성명, 주민등록번호, 차량등록번호 등을 입력하게 하고 있다. 이렇게 수집된 개인정보는 서울시에서 보유하고 있는 '승용차 요일제 참여 준수차량 관리파일'로 집적된다.[251] 행정안전부가 2009년 4

250) 제16조(RFID 시스템을 통한 개인위치정보 수집 등) 이 가이드라인에서 정한 사항 외에 RFID 취급사업자가 RFID 시스템을 통해 개인의 위치정보를 수집·이용·제공하는 경우에는 개인위치정보 보호와 관련한 사항에 대해서「위치정보의 보호 및 이용 등에 관한 법률」에 따른다.

251) 승용차 요일제 신청을 동사무소나 구청 등에서도 받기 때문에, 각 구청에서도 승용

월 28일 공개한 ‘2008년 공공기관별 개인정보파일대장’을 보면, 서울시가 보유한 ‘승용차 요일제 참여 준수차량 관리파일’의 세부 내용은 다음과 같다.

<표 3-19> 승용차 요일제 참여 준수차량 관리파일 대장

| 개인정보파일명 | 승용차 요일제 참여 준수차량 관리파일 | | |
|---|---|---|---|
| 1. 업무분야 | 교통 | 2. 단위업무 | 교통 |
| 3. 보유목적 | 승용차요일제 참여,준수에 따른 인센티브제공을 위한 정보관리 | | |
| 4. 보유근거 | 도시교통정비촉진법, 시행령, 참여신청서 | | |
| 5. 수집방법 | ,시스템 연계를 통한 수집 | | |
| 6. 대상개인범위 | 전자태그 승용차요일제 참여신청자 | | |
| 7. 대상인원수 | 840000 | 8. 보유기간 | 업무목적 달성후 바로 삭제관리 |
| 9. 기록항목 | 주민등록번호,이메일 주소,휴대폰 번호,성명,전화번호,주소,금융정보(계좌번호, 예금주, 은행명) | | |
| 10. 사용부서 | 친환경교통담당관 | | |
| 11. 열람예정일 | ②수시열람 | | |
| 12. 열람청구부서 및 주소 | - | | |
| 13. 열람제한 (1)열람제한항목 | 없음 | | |
| 13. 열람제한 (2)열람제한사유 | 없음 | | |
| 14. 이용, 제공기관명 | 경기도청 | 15. 이용, 제공근거 | 동의서 |
| 16. 이용, 제공항목 | 주민등록번호,이메일 주소,휴대폰 번호,성명,전화번호,주소 | | |

이와 별개로 서울시에 정보공개 청구하여 받은 답변은 다음과 같다.

<표 3-20> 승용차 요일제 관련 정보공개 청구 답변(1)

| 수집하는 개인정보 항목 | 자동차 등록번호, 성명, 주민등록번호, 주소, 전화번호(휴대폰) |
|---|---|

차 요일제 관련 개인정보파일을 보유하고 있다. 그러나 행정안전부가 공개한 ‘2008 공공기관별 개인정보파일대장’에 의하면 각 구별로 승용차 요일제 개인정보파일대장을 공개한 경우도 있었고, 그렇지 않은 경우도 있었다. 예를 들어, 강남구, 관악구는 관련 파일 대장이 공개되어 있는 반면, 강북구, 강서구, 금천구 등은 그렇지 않았다. 또한, 강남구와 관악구의 경우 승용차 요일제 관련 개인정보파일의 보유기간이 ‘영구’라고 되어 있었다.

| | |
|---|---|
| 수집 방법 | 승용차요일제 전자태그 참여등록 신청시 |
| 개인정보 파일 보유기간 | 10년 |
| 개인정보 파일의 담당 부서 | 기후변화담당관 |
| 개인정보 파일에 수록된 입력 건수 (연도별) | - 2006년 : 653천 건<br>- 2007년 : 766천 건<br>- 2008년 : 877천 건<br>- 2009년 : 923천 건 |
| 개인정보 파일에 대한 열람 및 정정, 삭제청구 방법 | 개인정보 정정: 본인희망, 승용차요일제 홈페이지<br>개인정보 삭제청구: 본인희망, 승용차요일제 홈페이지 |
| 위 개인정보 파일에 포함된 개인정보의 제3자(수사기관, 법원 등) 제공 건수 | 없음 |

정보공개 청구에 대한 답변은 행정안전부가 공개한 2008년 '공공기관별 개인정보파일대장'의 내용과 약간 차이가 있다. 어쨌든 공통적으로 기록항목에 전자태그 고유번호를 포함하고 있지 않은데, 이것이 없으면 RFID 인식기에서 기록한 정보와 연계될 수가 없다. 이와 관련하여 전화로 질의한 결과, 위 개인정보파일에 전자태그 고유번호도 포함된다는 답변을 얻을 수 있었다.[252]

전자태그 및 인식기와 관련한 정보공개 청구 결과는 다음과 같다.

<표 3-21> 승용차 요일제 관련 정보공개 청구 답변(2)

| | |
|---|---|
| 신청자에게 제공되는 전자태그에 수록하는 정보 항목 | 전자태그고유번호(개인정보없음) |
| 전자태그의 기술적 사양 | ・전자태그 성능 검증을 위해 공인검증기관인 한국전자거래진흥원 부설 RFID/USN센터에서 성능시험실시<br>・저온/고온 온습도 충격시험 및 도로주행 테스트를 실시 |
| 인식기(리더기)의 설치 대수 및 위치 | 서울시 전체 14개소 |
| 인식기(리더기) 설치 담당 부서 | 기후변화 담당관 |
| 인식기(리더기)를 통해 수집하는 정보 항목 및 승용차 요일제 개인정보파일과의 연계 방식 | 전자태그고유번호(개인정보없음) 인식 하여 승용차요일제시스템 D/B와 연계 |

252) 이는 공공기관 개인정보파일대장의 관리나 정보공개 청구에 대한 답변이 부실하게 이루어지고 있음을 보여준다.

| | |
|---|---|
| 인식기(리더기)를 통해 파악된 위반 건수 | - 2009. 6<br>- 미준수 차량: 86,683<br>- 1회 적발건수: 52,615<br>- 2회 적발건수: 15,894<br>- 3회 적발건수[253]: 18,174 |
| 인식기(리더기)를 통해 수집된 정보의 보유 기간 | 10년 |
| 인식기(리더기)를 통해 수집되는 정보에 대한 정보주체(승용차 보유자)의 열람, 정정, 삭제청구 방법 | 본인희망, 승용차 요일제 홈페이지 |
| 인식기(리더기)를 통해 수집된 정보의 제3자(수사기관, 법원 등) 제공 건수 | 없음 |
| (승용차요일제 참여 준수차량 관리파일을 포함한) 이상에 대한 법적 근거 | 공공기관의 개인정보보호에 관한 법률 |

위 정보공개 청구에 대한 답변에 따르면, 2009년 7월 현재 총 2,408,413대의 대상 승용차 중 883,088대가 승용차 요일제에 참여하여, 36.7%의 참여율을 보이고 있다고 한다. 아직 서울시 전역에 설치된 인식기가 14대에 불과하고, 수사기관 등 제3자에 제공된 바 없다고 하지만, 추후 인식기가 확대될 경우 개인위치정보가 보다 세밀하게 수집되고 이용될 가능성이 높다. 더욱이 이용자 유의사항에는 '이용기간 종료 시 지체 없이 폐기'한다고 명시하고 있음에도 불구하고, 인식기를 통해 수집된 위치정보가 10년 동안이나 보관될 필요가 있는지 의문이다. 또한, 승용차 요일제 시행과 관련하여 참여시 혜택만 강조되고 있을 뿐, 참여 시민의 개인위치정보가 수집될 수 있다는 것과 이로 인한 프라이버시 침해 문제에 대해서는 시민들에게 제대로 알려지지 않고 있는 점이 가장 큰 문제라고 생각된다.

사실 승용차 요일제는 시행 방법에 따라 위치정보의 수집을 전혀 하지 않아도 가능한 정책이다. RFID 가이드라인 제12조[254]는 RFID 시스템에 대한 프라이버시 영향평가를 권고하고 있다. 정책의 실효성을 높이는 것도 중요하지만, 어떤 정책을 추진하면서 프라이버시를 침해하지 않는 다른 방법은 없는지 검토할 필요가 있다.

---

253) 3회 이상 위반하면, 승용차 요일제 혜택을 받지 못하게 된다.

254) 제12조(RFID 시스템에 대한 프라이버시 영향평가) RFID 취급사업자는 RFID 시스템을 이용하여 개인정보를 기록·수집하거나 RFID 태그의 물품정보 등과 개인정보를 연계하는 경우, RFID 시스템 이용에 따른 프라이버시 침해 요인 등을 당해 RFID 시스템 도입 시에 분석·평가하여 이용자의 프라이버시가 침해되지 않도록 노력하여야 한다.

### 2) 하이패스

하이패스는 고속도로 요금소에서 정차 후 통행료를 지급하는 것이 아니라, 서행으로 차가 이동하면서 무선통신을 이용하여 통행료를 지급하는 시스템을 말한다. 하이패스를 이용하기 위해서는 단말기(OBU)에 하이패스 카드를 삽입해야 하며, 하이패스 차로로 진입해야 한다. 카드에는 미리 금액을 충전하고 이용하는 선불카드와 신용카드사와 제휴한 후불카드가 있다. 단말기에는 단말기 제조번호, 발행ID, 발급일, 차종, 차량번호 등 기본 정보가 입력되며, 차량 1대에 단말기 1대가 발급된다. 발급되지 않은 단말기를 장착하고 이용한 경우 또는 단말기에 등록된 차종정보와 실제운행한 차종이 다른 경우는 위반 차량으로 처리된다.[255]

하이패스 정책을 통해서도 개인 위치정보가 기록된다. 고속도로 요금소 하이패스 차로에 설치된 인식기에서 무선통신으로 차량에 설치된 단말기 번호 및 카드번호를 인식하여 특정 요금소를 통과한 하이패스 차량이 기록되며, 단말기 번호를 매개로 고객정보와 결합된다. 즉, 특정 단말기를 보유한 차량 운전자의 운행 기록이 추적될 수 있는 것이다.

(1) 개인(위치)정보의 수집

행정안전부가 공개한 '2008년 공공기관별 개인정보파일대장'에 의하면, 한국도로공사가 하이패스와 관련하여 보유한 개인정보 파일은 다음과 같다.

<표 3-22> 한국도로공사가 공개한 하이패스플러스카드 고객파일 대장

| 개인정보파일명 | 하이패스플러스카드고객파일 | | |
|---|---|---|---|
| 1. 업무분야 | 도로영업 | 2. 단위업무 | 하이패스플러스카드 발급 업무 |
| 3. 보유목적 | 고속도로이용 전자카드 회원 부가서비스 제공 | | |
| 4. 보유근거 | 공공기관의개인정보보호에 관한법률(정보주체 동의) | | |
| 5. 수집방법 | 온라인 수집(홈페이지 회원신청, 전자접수 등) | | |
| 6. 대상개인범위 | 전자카드 회원 기본 식별 정보 | | |
| 7. 대상인원수 | 1500000 | 8. 보유기간 | ④ 업무목적달성시 바로삭제 관리 |
| 9. 기록항목 | 주민등록번호,성명,차량번호,미납금액 등 관련정보 | | |

255) 하이패스 및 단말기 이용약관, 하이패스 홈페이지(http://www.hipassplus.co.kr/).

| | | | | |
|---|---|---|---|---|
| 10. 사용부서 | | 영업처 영업계획팀 | | |
| 11. 열람예정일 | | ②수시열람 | | |
| 12. 열람청구부서 및 주소 | | 경기도 성남시 수정구 대왕판교로 430 한국도로공사 영업처 영업계획팀 | | |
| 13. 열람 제한 | (1)열람제한항목 | 없음 | | |
| | (2)열람제한사유 | 없음 | | |
| 14. 이용, 제공기관명 | | 없음 | 15. 이용, 제공근거 | 없음 |
| 16. 이용, 제공항목 | | 없음 | | |

<표 3-23> 한국도로공사가 공개한 OBU 고객파일 대장

| 개인정보파일명 | | OBU고객파일 | | |
|---|---|---|---|---|
| 1. 업무분야 | | 하이패스단말기(OBU) | 2. 단위업무 | OBU 고객관리 |
| 3. 보유목적 | | 통행료 미납차량 고지, 자료관리 및 OBU회원 부가서비스 제공 | | |
| 4. 보유근거 | | 유료도로법 제20조 및 동법시행령 제15조 및 정보주체 동의 | | |
| 5. 수집방법 | | 오프라인 수집(개인의 신청서를 통한 수집) | | |
| 6. 대상개인범위 | | 하이패스 단말기 소유자 | | |
| 7. 대상인원수 | | 1312000 | 8. 보유기간 | ⑤ 영구적으로 보관관리 |
| 9. 기록항목 | | 이메일 주소・휴대폰 번호・성명・전화번호・주소・차량번호・차량모델 | | |
| 10. 사용부서 | | 하이패스처 단말기팀 | | |
| 11. 열람예정일 | | ②수시열람 | | |
| 12. 열람청구부서 및 주소 | | 경기도 성남시 수정구 대왕판교로 430 한국도로공사 하이패스처 단말기팀 | | |
| 13. 열람 제한 | (1)열람제한항목 | 없음 | | |
| | (2)열람제한사유 | 없음 | | |
| 14. 이용, 제공기관명 | | 없음 | 15. 이용・제공근거 | 없음 |
| 16. 이용, 제공항목 | | 없음 | | |

이와 별개로 한국도로공사에 대한 정보공개 청구를 통해 받은 답변은 다음과 같다.

<표 3-24> 하이패스 이용 고객 관리를 위한 개인정보파일대장

| 구 분 | 내 용 |
|---|---|
| 개인정보파일 종류 | 단발기발급 S/W |
| 수집되는 개인정보의 종류 | 고객명, 주소, 연락처, 이메일, 차량번호, 차량명 |
| 개인정보 수집 방법 | 단말기 발급 시 고객정보 동의 |
| 보유기간 | 준영구 |
| 담당부서 | ITS처 |
| 입력건수 | 2004 : 35,933<br>2005 : 56,698<br>2006 : 105,834<br>2007 : 422,607<br>2008 : 928,870<br>2009.8 현재 : 777,717<br>계 : 2,327,659 |
| 열람, 정정, 삭제 청구방법 | 서식에 따른 청구 |

하이패스 진·출입 요금소에서 수집되는 정보를 관리하기 위한 데이터베이스 대장은 다음과 같다.

<표 3-25> 하이패스 진·출입 요금소 수집 정보 관리 데이터베이스

| 구 분 | 내 용 |
|---|---|
| 데이터베이스 명칭 | ITCS |
| 수집항목 | 단말기번호, 카드번호, 통과영업소명, 차로번호, 통행시각, 통행요금 |
| 보유기간 | 3년 |

하이패스 고객 데이터베이스와의 연계방식 방식을 묻는 질문에는 “차량이 통과 시에 수집되는 단말기 번호와 하이패스 단말기 등록 시 수집되는 고객정보를 결합하여 미납통행요금 산정 및 고객상담 자료로 활용”한다고 답변하였다.

개인위치정보는 카드 사용 거래기록과 함께 기록되기도 한다. 하이패스에서 이용되는 카드는 두 가지 종류가 있는데, 한국도로공사의 하이패스플러스 카드는 선불식 카드이고, 신용카드사에서 발급하는 하이패스 카드는 후불식 카드이다.

한국도로공사 하이패스플러스카드 이용약관[256] 제12조[257]제1항에 의하면, 카드 사용시 회사와 가맹점 간 카드 이용대금의 정산 및 배분을 위해 필요한 거래내용 정보(거래일시, 거래금액, 전자적 장치 정보, 카드식별번호, 입·출구 및 승하차 정보 등 광의의 위치정보) 및 신용카드 충전여부 등이 기록된다. 제3항에서는 거래내역이 개인신상정보와 결합되어 관리되지 않는다고 규정하고 있다. 그러나 카드식별번호를 매개로 개인신상정보와 연계될 수 있기 때문에, 하나의 개인정보파일로 통합되어 있지는 않더라도 연계 자체가 불가능한 것은 아니다. 한국도로공사 선불하이패스 홈페이지에서는 이용내역조회 서비스도 제공하고 있다.

후불 하이패스 카드는 신용카드사에서 발급한다. 2009년 10월 현재, 신한, BC, 삼성, 현대, 롯데, 국민, 외환, 하나카드 등 국내 전 신용카드사와 이들과 제휴관계에 있는 우리은행, SC제일은행, 농협, 기업은행, 대구은행, 부산은행, 경남은행, 씨티은행 카드 등도 모두 발급가능하다고 되어 있다.[258] 후불 하이패스 카드 홈페이지(http://www.excard.co.kr)를 통해 카드번호, 거래일자, 차종, 입구, 출구, 이용차로, 사업자명칭, 거래금액 등 이용내역을 열람할 수 있는 것으로 보아, 후불 하이패스 카드를 통해서도 개인위치정보가 거래내역과 함께 기록되고 있음을 확인할 수 있다.

(2) 개인(위치)정보의 활용 및 제3자 제공

'하이패스(Hi-pass) 및 단말기 이용약관' 제10조제3항은 수집된 회원의 개인정보를 수집 목적 외로 제공할 수 있는 경우를 다음과 같이 나열하고 있다.

1. 배송담당 업체 등에게 배송에 필요한 최소한의 회원 정보를 알려주는 경우

256) 한국도로공사 선불하이패스 홈페이지(http://www.hipassplus.co.kr)에 나와있다.

257) 제12조(거래내역의 수집)
① 회사는 회원이 카드로 재화나 용역을 제공받을 때 회사와 가맹점 간 카드 이용대금의 정산 및 배분을 위해 필요한 거래내용 정보(거래일시, 거래금액, 전자적 장치 정보, 카드식별번호, 입,출구 및 승하차 정보 등 광의의 위치정보) 및 신용카드 충전여부 등 최소한의 정보만을 수집합니다.
② 회원의 계속적인 카드 사용은 카드를 통해 수집된 거래내역 정보가 이용대금 정산의 목적 한도 내에서 수집되고 사용되는 것에 대하여 동의한 것으로 간주합니다.
③ 수집된 거래내역 정보는 회원의 카드 등록시 기입한 회원의 개인신상정보와 결합되어 관리되지 않습니다.

258) 후불 하이패스카드 홈페이지 내 '카드 신청절차' 메뉴.
http://www.excard.co.kr/info/info01.jsp.

2. 통계 작성, 학술 연구 또는 시장 조사를 위하여 필요한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우
3. 관계 법령에 의하여 수사상의 목적으로 관계기관으로부터 요구 받은 경우
4. 전자카드 및(또는) 단말기를 이용한 교통정보 수집·이용 등 서비스 향상을 위하여 도공이 필요한 경우
5. 고객관계관리(CRM) 관련 서비스 향상 또는 새로운 상품의 소개 등을 위하여 도공의 콜센터 고객응대시 필요한 경우
6. 기타 관계법령에 의한 경우

제4호는 개인위치정보를 '서비스 향상'이라는 포괄적인 목적으로 한국도로공사가 남용할 수 있는 위험성이 있다. 제5호의 경우 상품 홍보에 이용하는 것까지 약관을 통해 일괄 동의를 하도록 하는 것은 과도하며, 별도의 동의를 받는 식으로 개선될 필요가 있다.

'하이패스플러스카드 이용약관' 제16조제2항 역시 수집된 개인정보를 제3자에게 제공할 수 있는 경우가 나열되어 있는데, 단말기 이용약관의 규정과 유사하다. 다만, 제5호에서 '서비스의 제공에 필요한 범위 내에서 제휴기관에 제공하는 경우', 제6호에서 '회원과 가맹점이 카드 거래로 인하여 분쟁이 발생하여 가맹점에게 회원의 정보 제공이 필요한 경우'를 규정하고 있다. 그런데, 문제는 어느 업체/기관이 제휴기관 및 가맹점으로 등록되어 있는지, 이들에게 어떠한 개인정보가 제공되는 것인지 공개되어 있지 않아 구체적으로 알 수 없다는 점이다. 「정보통신망법」에서 위탁 및 제3자 제공시 제공되는 개인정보의 항목과 제공되는 업체를 모두 공개하도록 한 것과 비교해볼 때, 매우 포괄적으로 기술되어 있음을 알 수 있다.

한국도로공사가 보유하고 있는 개인정보의 제3자 제공과 관련하여 한국도로공사는 △ 「공공기관의 개인정보보호에 관한 법률」 제10조제3항제6호, △ 정보주체의 동의(하이패스 및 단말기 이용약관), △ 「형사소송법」 제199조제2항, △ 「경찰관직무집행법」 제8조제1항 등에 근거하여 범죄 수사 목적으로 경찰에 제공한다고 답변했다. 그러나 하이패스 고객 개인정보파일에 포함된 개인정보의 제3자 제공건수와 진출입 요금소에서 수집되는 정보의 제3자 제공건수는 공개하지 않았다.[259] 그러나 한 보도에 의하면, 개인위치

259) 한국도로공사는 다음과 같이 납득하기 힘든 근거를 대면서 비공개 답변을 하였다.
비공개 근거 : 공공기관의 정보공개에 관한 법률 제2조, 제3조
"정보"라 함은 직무상 작성 또는 취득하여 관리하고 있는 문서, 도면 등을 말하며, "공개"라 함은 정보를 열람하게 하거나 그 사본, 복제물을 교부하게 하는 것으로 개인정보의 제3자 제공건수는 우리 공사에서 직무상 작성한 문서가 또는 취득한 문서가 아니므로 공개할 수 없음을 알려드립니다.

정보가 영장도 없이 수사기관에 제공되고 있는 것으로 보인다.[260] 보도에 따르면, 수사기관의 하이패스 이용자료 요청건수는 2007년 0건, 2008년 8건, 2009년(10월 11일 현재) 228건으로 급증하고 있다. 「공공기관의 개인정보 보호에 관한 법률」 제10조제3항제6호는 '범죄의 수사와 공소의 제기 및 유지에 필요한 경우' 공공기관이 보유하고 있는 개인정보를 수사기관에게 제공할 수 있도록 허용하고 있다. 이 경우 개인위치정보 역시 일반적인 개인정보와 마찬가지로 법원이 발부한 영장 없이도 제공될 수 있다. 즉, 한국도로공사가 보유하고 있는 개인위치정보는 「위치정보법」이나 「통신비밀보호법」이 적용되는 개인위치정보보다 보호수준이 낮아지게 된다. 「위치정보법」이 개인위치정보에 대한 특수한 보호의 필요성에 따른 것이라면, 이와 같이 적용이 배제되는 개인위치정보의 보호에 까지 그 범위를 확대할 필요가 있다.

(3) 개인(위치)정보의 폐기

단말기 이용약관이나 하이플러스카드 이용약관에 개인정보의 보유기간이나 폐기에 대해 명확하게 규정되어 있지는 않다. 한국도로공사가 공개한 하이패스플러스카드 고객파일 대장에 의하면, 보유기간이 '업무목적 달성시 바로 삭제 관리'라고 규정되어 있고, OBU고객파일의 경우에는 '영구적으로 보관관리'라고 되어 있다.

정보공개 청구 결과에 의하면, 고속도로 진출입 기록의 경우에는 3년 동안 보관된다. 그러나 단말기(OBU) 이용약관에는 위치정보가 수집되는 지 여부, 수집될 경우 보관 기간, 보관 기간의 법적 근거 등이 전혀 명시되어 있지 않다. 고속도로 진출입 기록이 3년 동안 보관될 이유가 무엇인지 의문이다.

(4) 정보주체의 열람 및 정정・ 삭제 청구권

한국도로공사가 보유하고 있는 개인정보에 대해서는 「공공기관의 개인정보 보호에 관한 법률」에 근거하여 열람, 정정, 삭제를 청구할 수 있다.

하이패스플러스카드 이용약관 제13조[261]에 따르면, 카드 회원은 카드번호,

---

260) MBC 뉴스. 2009.10.11. "또 다른 감시의 눈 '하이패스'."

261) 제13조 (거래내역의 제공)

① 회사는 회원 본인에 의해 등록된 카드에 한하여 회원 본인의 신청에 따라 다음 각 호의 거래내역 조회서비스를 제공합니다. 다만, 카드의 위치정보는 관련법령(위치정보의 보호 및 이용 등에 관한 법률)에 의거 제공하지 않으며, 거래내역 조회서비스의 상세한 절차와 방법은 홈페이지 등을 통해 고지합니다.

1. 카드번호
2. 거래의 종류, 시간 및 거래금액

거래의 종류, 시간 및 거래금액, 가맹점정보, 기타 관련 법령에서 규정하는 정보 등 거래내역을 조회할 수 있으며, 선불하이패스 홈페이지에서도 지불내역 조회 서비스를 제공하고 있다. 그러나 카드의 위치정보는 제공하고 있지 않은데, 이는 「위치정보법」에 따른 것이라고 한다. 하지만 「위치정보법」 어느 조항에 근거한 것인지는 명확하게 규정되어 있지 않다. 오히려 동법 제24조제3항은 △ 본인에 대한 위치정보 수집·이용·제공사실 확인자료, △ 본인의 개인위치정보가 이 법 또는 다른 법률의 규정에 의하여 제3자에게 제공된 이유 및 내용의 열람을 정보주체가 열람할 수 있도록 허용하고 있다.

그림과 같이 후불하이패스카드의 경우에는 카드번호, 거래일자, 차종, 입구, 출구, 이용차로, 사업자명칭, 거래금액 등 상세한 이용내역을 열람할 수 있도록 허용하고 있다.

<그림 3-6> 후불하이패스카드 홈페이지, 사용내역 확인방법


3. 가맹점정보
4. 기타 관련 법령에서 규정하는 정보

### 3) 교통카드

이제 대다수의 사람들이 버스나 지하철 등 대중교통수단을 이용할 때 현금 대신 교통카드를 이용한다.[262] 국내에서는 최초로 서울시가 1996년 3월에 버스카드제를 도입하였으며 1998년 6월부터는 지하철카드제를 도입하여 운영하기 시작하였다.

교통카드란 교통수단 탑승 및 이용을 위해 사용되는 전자화폐의 하나로서 현금, 수표, 신용카드 등 기존의 화폐와 동일한 가치를 지니는 디지털 형태의 정보를 말한다. 일반적으로 정보는 디스크, IC칩과 같은 컴퓨터 기록매체를 이용하여 저장 및 관리되고 있다. 현재 국내에서 사용되고 있는 교통카드는 충전식 선불카드와 신용카드를 활용한 후불카드로 운영되고 있으며, '96년 7월 서울시내버스 교통카드제 실시 이후 각 지자체별(광역시, 시 군 단위)로 시행되고 있다.

국내에는 한국스마트카드(T-money), Mybi, K-Cash, V-Cash등 공식적인 5개의 IC카드형 전자화폐와 다수의 네트워크형 전자화폐가 도입·운영되고 있다. 서울시 버스 및 지하철의 통합형 교통카드의 운영은 한국스마트카드(T-money)[263]가 맡고 있는데, 본 연구에서는 한국스마트카드를 중심으로 분석하였다.

후불카드란 기존의 신용카드에 교통카드용 IC칩을 장착함으로서 교통카드 기능을 갖도록 하고 있는 것을 말한다. 즉 직접적으로 단말기 설치, 프로그램 개발 등 교통카드시스템을 구축하지 않고 교통카드사의 시스템으로 운영하면서 교통카드사에 일정수수료를 지불하고 있다(조규석, 2005).

(1) 개인(위치)정보의 수집

교통카드시스템은 기본적으로 교통요금 지불용 단말기, 교통카드 및 단말

---

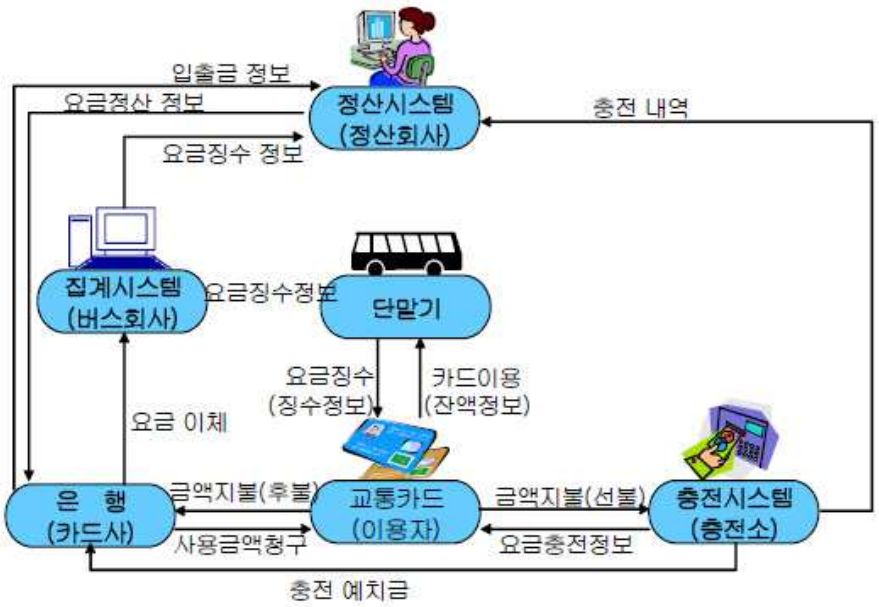
262) 전국에서 교통카드는 2004년 11월 기준으로 약 36,000천매가 보급되었으며, 단말기(판독기)는 약 3만 여대가 설치되어 운영 중에 있다(조규석, 2005: 19). 국내 교통카드 이용실적은 광역도시가 기타 지역에 비해 높은 이용률을 보였다. 전국적으로 이용률을 살펴보면 서울시의 경우, 2004년 12월말 기준으로 버스는 71%, 지하철은 52%로 나타났으며, 부산과 대구, 인천의 경우에도 약 50% 정도의 이용률을 보였다(박진영·김동준, 2006:40).

263) T-머니 교통카드는 기본적으로 비접촉식 통신 방식을 지원하는 스마트카드로 무선으로 데이터를 주고받게 되며, 기존 메모리카드와는 달리 CPU가 탑재되어 자체연산 작업이 가능하다. 손톱만한 칩 하나에 CPU와 메모리를 담아서 자체 연산과 많은 양의 정보를 저장할 수 있다. 비접촉식 무선인식 기능을 가능하게 하는 RFID 기술이 사용되며, 반경 수 미터까지 정확한 위치 정보를 제공하는 GPS 기술이 융합된 첨단 교통카드이다(박진영·김동준, 2006: 40).

기로부터 교통요금 지불거래기록을 수집하기 위한 집계시스템, 집계시스템으로부터 전송된 교통요금 지불거래를 인증하여 데이터베이스를 구성하고 정산하는 정산시스템, 각 시스템의 구성요소를 유기적으로 연결하는 네트워크 등으로 구성된다(조규석, 2005: 8).

대중교통 이용자들이 교통카드를 단말기에 접촉시키면, 사용한 교통카드의 식별 및 요금이 부과되고 거래 내용이 단말기와 카드에 기록된다. 지하철에서는 승·하차 정보가 모두 기록되지만, 버스의 경우에는 환승이 아닐 경우 하차할 때 단말기 접촉을 하지 않는 경우도 있으므로, 하차정보가 남지 않을 수도 있다. 단말기에 남은 기록은 즉시 중앙전산망으로 송신되어 최종 집계된다(박진영·김동준, 2006: 41).

<그림 3-7> 교통카드시스템의 주요 구성요소




자료: 조규석(2005: 8).

서울시 교통카드에 수록되는 정보는 아래 표와 같다.

<표 3-26> 서울시 교통카드 수록 정보

| 번호 | 수록내용 | 예시 | 내용 |
|---|---|---|---|
| 1 | 카드번호 | 1 | 개인정보 보호를 위해 부여한 가상 카드 번호 |
| 2 | 승차일시 | 20041027114320 | 2004년 10월 27일 11시 43분 20초 |
| 3 | 트랜잭션ID | 4 | 탑승 형태에 따른 구분 |
| 4 | 교통수단CD | 120 | 탑승 수단에 따른 구분 |
| 5 | 환승횟수 | 1 | 환승 횟수 |
| 6 | 버스노선ID | 41110044 | 버스 노선에 따라 부여되는 고유번호 |
| 7 | 버스노선명 | 1111번(군포 공영차고지~노량진) | 버스 노선 명 |
| 8 | 교통사업자ID | 111000600 | 운수 업체별로 부여되는 고유 번호 |
| 9 | 교통사업자명 | 가나교통(주) | 운수 업체 명 |
| 10 | 차량ID | 111746615 | 버스차량별 고유 번호 |
| 11 | 차량등록번호 | 서울74사6615 | 차량등록 번호 |
| 12 | 사용자구분코드 | 1 | 일반, 또는 학생, 무임승차 구분 |
| 13 | 사용자구분명 | 일반 | 사용자 구분 코드에 따른 내용 |
| 14 | 운행출발일시 | 20041027113424 | 탑승 차량이 차고지를 출발한 시각 |
| 15 | 승차정류장ID | 10029 | 승차한 버스 정류장의 고유 번호 |
| 16 | 승차정류장명 | 당동지하차도 | 승차 정류장 ID에 다른 정류장 명 |
| 17 | 하차일시 | 20041027121530 | 하차일시 (승차일시와 동일한 형태) |
| 18 | 하차정류장ID | 9699 | 하차한 버스 정류장의 부여된 고유 번호 |
| 19 | 하차정류장명 | 국립식물검역소 | 하차 정류장 ID에 다른 정류장 명 |
| 20 | 이용객수(다인승) | 1 | 하나의 교통카드로 승차한 이용객 수 |
| 21 | 승차금액 | 800 | 이용 금액 |
| 22 | 승차위반금액 | 0 | 승차위반 금액 |
| 23 | 하차금액 | 0 | 거리비례제에 따른 추가요금 |
| 24 | 하차위반금액 | 0 | 하차위반 금액 |
| 25 | 운행종료일시 | 20050909052349 | 운행을 종료한 시각 |

자료: 박진영・김동준(2006: 55).

위 표에서 볼 수 있는 바와 같이 교통카드에는 승하차 정보 뿐만 아니라, 환승 정보, 이용한 버스의 노선과 차량번호까지 세세하게 기록된다. 물론 위 이용기록 자체는 개인신상정보를 포함하고 있지 않다. 그러나 카드번호를 매

개로 개인신상정보와 연계될 수 있다.

선불 교통카드의 경우에는 기본적으로 개인신상정보를 수집하지 않기 때문에 위치정보가 신상정보와 결합되어 있지는 않다. 다만, 특정 개인이 보유하고 있는 선불 교통카드의 카드번호를 알고 있다면, 누적되어 있는 교통카드 이용기록을 통해 특정 개인의 이동 경로를 추적할 수 있을 것이다. 또한, 교통카드를 발급한 업체의 홈페이지에 회원 가입을 하고 카드번호를 등록하면 자신의 교통카드 이용내역을 조회할 수 있다. 예를 들어, 서울시 교통카드를 제공하고 있는 (주)한국스마트카드의 경우, T-money 홈페이지(http://www.t-money.co.kr)에 회원 가입을 하고 카드 번호를 등록하면 카드 등록일 이후의 거래내역을 조회할 수 있도록 하고 있는데, 거래종류(버스/지하철/충천 등), 거래일시, 충전금액, 거래금액, 미징수금액, 거래후잔액, 사용처(버스번호 및 업체명, 지하철노선번호, 충전업체 등) 등을 열람할 수 있다. 승하차 정보는 나오지 않는데, 이는 기록이 없어서가 아니라 열람을 제한한 것이다. (주)한국스마트카드의 이용약관 제10조[264]는 거래내역의 수집을 규정하고 있는데, 서비스 이용 및 물품 구매시 회사와 가맹점간 이용대금의 정산을 위해 카드번호, 거래일시, 거래금액, 단말기 및 가맹점정보, 승/하차정보 등 광의의 위치정보를 수집한다고 명시하고 있다.

신용카드와 결합된 후불 교통카드는 기본적으로 개인신상정보와 연계되어 개인위치정보가 기록된다. 서울지역의 경우 신용카드사는 (주)한국스마트카드(T-money)로부터 위치정보를 포함한 거래내역을 제공받는다. 해당 카드사의 홈페이지를 통해 교통카드 이용내역을 열람해볼 수 있는데, 이용일자, 이용수단(버스/지하철), 승차시각, 하차시각, 이용금액, 승차역, 하차역, 청구일자 등의 정보를 열람할 수 있다.

264) 제10조(거래내역의 수집) ① 회사는 고객이 T-money를 통해 서비스 이용 및 물품 구매시 회사와 가맹점간 이용대금의 정산을 위해 필요한 최소한의 거래내역 정보(카드번호, 거래일시, 거래금액, 단말기 및 가맹점정보, 승/하차정보 등 광의의 위치정보)를 수집합니다.

<그림 3-8> T-money 거래내역 조회 화면


(2) 개인(위치)정보의 활용 및 제3자 제공

교통카드 이용내역은 우선 버스 사업자를 통해 집계되고, 정산을 위해 정산회사의 정산시스템으로 보내진다. 서울시 교통카드의 경우 (주)한국스마트카드[265]가 정산 업무를 맡고 있다. (주)한국스마트카드 입장에서는 교통기관은 하나의 가맹점[266]이 되고, 교통카드 이용내역은 서비스 거래내역이 된다. (주)한국스마트카드에서 버스승하차정보, 버스운행기록, 버스정산금 업무를

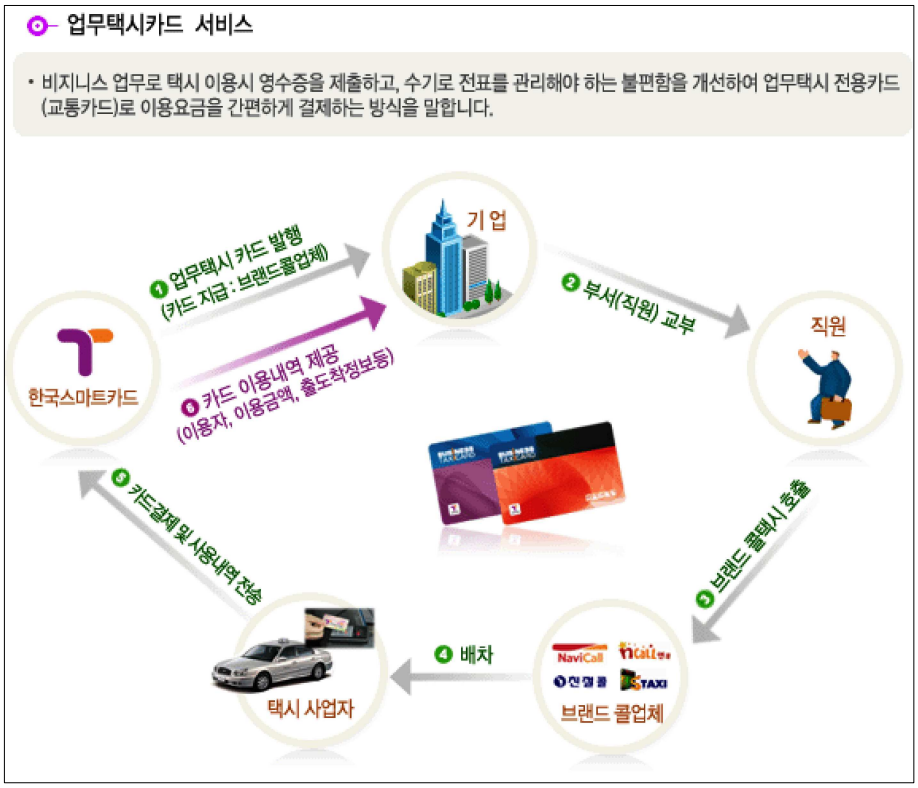
265) 서울시에서 사용되는 교통카드 T-money는 (주)한국스마트카드에서 발급하고 있다. (주)한국스마트카드는 서울시 신교통시스템 구축 및 운영을 위해 설립된 법인으로, T-money 카드 발급 및 제휴, 상품개발, 정산, 시스템운영개선 등을 주요 업무로 하고 있다(박진영・김동준, 2006: 42).

266) T-money 서비스 이용약관 제2조(용어의 정의)
⑤ "가맹점"이란 회사와 별도의 계약을 체결한 교통기관을 포함하여, T-money 가맹점약관에 따라 가맹점가입을 신청하고 회사로부터 가입을 승인 받은 업소, 시설 등을 말합니다.

담당하며, 추출된 버스관련 원자료(Raw Data)로부터 데이터 필터링을 통해 자료를 가공하고, 버스 각각의 운행정보(GPS)로부터 각 버스의 운행횟수(대-km) 자료를 제공하며, 개인별, 일별, 차량별, 정류장별, 카드별 승하차 정보를 취합한다(박진영・김동준, 2006: 42).

(주)한국스마트카드는 교통결제와 유통가맹점 결제가 가능한 기본 T-money 카드 외에 인터넷 T-money, 모바일 T-money, 업무택시카드, 법인 T-money 등 다양한 종류의 카드 서비스를 제공하고 있다. 그런데, 업무택시카드나 법인 T-money는 노동 감시에 활용될 수 있는 위험성이 존재한다.

<그림 3-9> T-money 업무택시카드 서비스




자료: T-money 홈페이지.

업무택시카드는 (주)한국스마트카드가 기업에 카드를 발행해주고 직원이 택시(브랜드 콜택시)를 이용한 내역(이용자, 이용금액, 출도착정보 등 카드이

용내역)을 기업에 제공한다. 법인 T-money 역시 마찬가지다. 법인 T-money를 이용하면, 부서별, 팀별, 개인별 거래내역이 기업에 제공된다. 대중교통 영수증 발급이 곤란하거나 택시 영수증 제출 등의 불편함을 개선하는 효과가 있을 수 있지만, 직원 입장에서는 회사 외부에서의 이동 내역(승하차 일시 및 장소, 이용한 교통수단 등)이 회사에 세세하게 드러나게 될 수밖에 없다. 위치기반서비스에서와 같이 업무택시카드나 법인 T-money 이용내역을 통해 실제 카드를 사용한 정보주체의 개인위치정보가 회사 등 제3자에게 제공되지만, 위치정보주체의 보호를 위한 「위치정보법」 규정은 이 경우에 제공되지 않는다. 이 역시 현행 「위치정보법」의 사각지대라고 볼 수 있다.

개인정보의 제3자 제공과 관련해서는, T-money 이용약관 제23조 및 제24조에서 규정하고 있다. 제23조제3항은 “회사는 양질의 서비스를 제공하기 위해 여러 비즈니스 파트너와 제휴를 맺거나 국가기관의 요구 등을 위해 개인정보를 위탁관리 하거나 개인정보를 제공할 수 있습니다. 그럴 경우 회사는 약관에 해당 목적, 내용 및 업체명을 밝혀 회원의 동의를 받습니다. 단, 고객의 소득공제 목적으로 국세청에 개인정보 및 T-money 사용내역을 제공하는 경우 등과 같이 고객의 요청에 의하는 경우는 예외로 합니다.”라고 규정하고 있다. 홈페이지 개인정보 취급방침에는 제3자 제공 업체와 취급위탁 업체가 공개되어 있다. 제24조[267]는 회원의 동의 없이 제공할 수 있는 경우를 나열하고 있는데, 위에서 살펴본 ‘하이패스 및 단말기 이용약관’과 유사하다. 제3자 제공과 관련하여 개인위치정보에 대해서 특별히 규정하고 있지 않다.

---

267) 제24조 (개인 정보 보호)
① 회사는 회원의 정보 수집 시 정상적인 서비스를 위한 최소한의 정보를 수집합니다.
② 회원이 제공한 개인정보는 회원의 동의 없이 제3자에게 누설하거나 제공하지 않습니다. 다만, 다음 각 호에 해당하는 경우에는 예외로 합니다.
1. 배송을 위해 배송담당 업체등에게 배송에 필요한 최소한의 회원 정보를 알려주는 경우
2. 통계 작성, 학술 연구 또는 시장 조사를 위하여 필요한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우
3. 관계 법령에 의하여 수사 상의 목적으로 관계기관으로부터 요구 받은 경우
4. 서비스의 이용에 따른 거래상 발생하는 요금정산
5. 서비스의 제공에 필요한 범위 내에서 제휴 회사와 공유해야 하는 경우
6. 기타 관계법령에 의한 경우

(3) 개인(위치)정보의 파기

T-money 이용약관 제21조는 회원탈퇴 및 자격상실을 규정하고 있는데, 여느 업체와 마찬가지로 회원탈퇴 시 개인정보가 삭제되지만, 탈퇴 후에도 1개월 동안은 보유한다. T-마일리지 거래내역이 있는 경우 5년 동안 보관된다. 개인위치정보에 대해서는 별도로 규정하고 있지 않지만, 카드업체 입장에서는 '거래내역'이기 때문에 「전자금융거래법」에 근거해서 보존될 것으로 보인다.

(4) 정보주체의 열람 및 정정·삭제 청구권

T-money 이용약관 제11조는 회원에 대한 거래내역 조회서비스를 규정하고 있다. 하이패스플러스카드 이용약관과 같이, 「위치정보법」에 의거 승·하차 위치정보는 제공하지 않고 있다. 그러나 법인 T-money와 같이, 오히려 제3자인 기업에게는 제공되는 개인위치정보가 왜 당사자에게는 제공되지 않는지, 그리고 「위치정보법」 어떤 조항에 근거한 것인지 의문이다. T-money 이용약관 제12조는 거래내역의 정정을 규정하고 있지만, 개인정보의 정정이나 삭제 청구와 관련해서는 특별한 규정이 없다.

## 4. 소 결

정보통신기술의 발전으로 사물의 위치를 파악하는 능력이 고도화되고 있으며, 수집된 사물의 위치정보가 개인정보 데이터베이스와 연계됨으로써 개인위치정보에 대한 접근이 가능해지게 된다. 개인 위치정보는 우선 「위치정보법」에 의해 규제되는데, 동법이 위치정보를 수집하는 모든 종류의 기관/업체에 적용되지는 않는다. 예를 들어, 본 연구에서 주로 다룬 승용차 요일제, 고속도로 하이패스, 교통 카드같은 경우 주 운영기관/업체의 관련 규정은 (일부 연관된 조항이 있기는 하지만) 동법에 근거하지 않고 있었다.

2009년 10월 현재, 191개의 사업자가 위치정보사업자 혹은 위치기반서비스사업자로 허가를 받거나 신고되어 있었다. 이와 같은 위치기반 서비스는 비록 적법하게 이루어진다고 하더라도, 위치가 수집되는 대상의 프라이버시 침해 가능성을 배제할 수 없다.

위치기반서비스사업자에게 위치정보를 제공하는 주요 위치정보사업자 이동통신사이다. 「위치정보법」 제24조는 본인에 대한 위치정보 수집·이용·제공사실 확인자료 및 제3자에게 제공된 이유 및 내용 등을 열람할 수 있는 정

보주체의 권리를 규정하고 있으나, 한 이동통신사에 대해 개인위치정보에 대한 열람청구를 해본 결과 이 권리가 제대로 보장되지 않고 있음을 확인할 수 있었다.

승용차 요일제의 경우, 서울 시내에 설치된 인식기를 통해 차량에 부착된 전자태그의 정보를 인식하여 위치정보를 수집하고 있으며, 전자태그 고유번호를 매개로 승용차 요일제 참여자 데이터베이스와 연계될 수 있어, 프라이버시 침해 논란이 제기되고 있다. 가입시 '이용자 유의사항'에는 개인 위치정보의 수집 사실이 공지되고 있지 않았으며, 인식기를 통해 수집되는 위치정보도 10년 동안이나 보관되고 있었다. RFID 가이드라인에서 규정하고 있듯이, 지금이라도 프라이버시 영향평가를 실시할 필요가 있다.

하이패스의 경우에도 차량 통과 시에 고속도로 요금소에서 단말기 및 카드정보가 수집되고, 이를 매개로 고객정보와 연계됨으로써 개인 위치정보를 수집하고 있다. 하이패스 이용자는 선불/후불하이패스 홈페이지를 통해 위치정보를 포함한 거래내역을 조회할 수 있다. 이렇게 수집된 개인(위치)정보는 수사기관 등에 제공되고 있는데, 수사상 목적을 위한 것일지라도 개인위치정보를 제공받기 위해서는 영장을 제시하도록 하는 등 제공 절차를 보다 엄격하게 할 필요가 있다.

버스, 지하철 등 대중교통 요금결제를 위한 교통카드 사용도 일반화되고 있다. 교통카드는 각 지자체별로 운영되고 있다. 서울시 교통카드의 경우 교통카드 이용시 카드 내에 25개 정보가 기록이 되는데, 카드번호를 매개로 개인신상정보와 연계되면 개인위치정보가 된다. 버스 등 단말기에 기록된 교통카드 이용내역은 정산회사의 시스템에 집적되게 된다. 신용카드와 결합된 후불 교통카드는 은행 홈페이지에서 승하차 정보를 포함한 이용내역을 열람할 수 있다. 선불 교통카드의 경우에도 카드회사의 홈페이지를 통해 이용내역을 열람할 수 있는데, 「위치정보법」을 근거로 승하차 정보는 제공하지 않고 있다. 그러나 기업 등을 대상으로 한 교통카드 상품의 경우에는 직원들의 교통카드 이용내역을 구매 기업에 제공하고 있었는데, 이는 자칫 노동감시의 수단이 될 수 있어 우려된다.

# 제3절 유전정보

## 1. 개요

유전정보란 유전자검사의 결과로 얻어진 정보를 말한다. 여기서 '유전자검사'라 함은 개인 식별을 목적으로 혈액·모발·타액 등의 검사대상물로부터 유전자를 분석하는 행위를 말한다.

일반적인 유전자검사와 유전정보 등의 보호 및 이용에 관한 사항, 유전자은행에 관한 사항은 2004년 1월 29일 제정된 「생명윤리 및 안전에 관한 법률」에서 규정하고 있다. 그러나 이 법률에서는 국가기관이 유전자검사를 하는 경우를 제외하고 있다.[268]

현재 국가기관이 구축·운영하는 유전정보 데이터베이스는 실종아동등에 대한 데이터베이스를 들 수 있다. 2005년 5월 31일 제정된 「실종아동등의 보호 및 지원에 관한 법률」은 보호시설의 입소자 중 보호자가 확인되지 아니한 아동등과 실종아동등을 찾고자 하는 가족으로부터 유전자검사대상물을 채취하여 유전자검사를 실시하고 그 결과를 데이터베이스로 구축·운영토록 하고 있다. 여기서 '아동등'은 실종신고 당시 14세 미만 아동이나 「장애인복지법」 제2조의 장애인 중 정신지체인·발달장애인·정신장애인을 의미한다. 유전자검사대상물의 채취는 경찰청장이 실시하고, 유전자검사를 실시하고 그 결과를 데이터베이스로 구축·운영하는 것은 국립과학수사연구소이다(동법 시행령 제5조).

보건복지가족부는 위 데이터베이스의 대상에 '치매노인'을 포함하기 위한 법률개정안을 2009년 3월 27일 입법예고하였다. 또한 법무부와 경찰청 등은 2009년 5월 26일자로 「디엔에이신원확인정보의 이용 및 보호에 관한 법률안」을 입법예고하였다. 디엔에이(DNA) 신원확인정보 데이터베이스 제도는 강력범죄를 저지른 자의 디엔에이신원확인정보를 미리 확보하여 관리하면서

---

268) 「생명윤리 및 안전에 관한 법률」
제24조 (유전자검사기관 등) ①유전자검사를 하고자 하는 자 또는 직접 검사대상물을 채취하여 유전자에 관한 연구를 하고자 하는 자는 유전자검사시설 또는 연구시설의 소재지, 기관장, 유전자검사 또는 연구항목 등의 사항에 대하여 보건복지가족부령이 정하는 바에 따라 보건복지가족부장관에게 신고하여야 한다. 다만, 국가기관이 유전자검사 또는 유전자에 관한 연구를 하는 경우에는 그러하지 아니하다. <개정 2008.2.29>
제32조 (유전자은행의 허가 및 신고) ①유전자은행을 개설하고자 하는 자는 대통령령이 정하는 바에 따라 보건복지가족부장관의 허가를 받아야 한다. 다만, 국가기관이 직접 유전자은행을 개설하고자 하는 경우를 제외한다. <개정 2008.2.29>

강력범죄가 다시 발생하였을 때 보관 중인 데이터와 현장에 남아 있는 디엔에이감식시료로부터 채취한 디엔에이신원확인정보를 비교하여 신속히 범인을 특정·검거할 수 있도록 하는 제도이다(입법예고안).

본 연구는 현재 국가가 법률에 의해 구축·운영하고 있는 실종아동등의 유전정보 데이터베이스를 일차적인 대상으로 한다.

「실종아동등의 보호 및 지원에 관한 법률안」이 제정되는 과정은 순탄치 않았다. 2004년 경찰이 '미아찾기 사업'의 일환으로 유전정보 데이터베이스를 구축하기 시작하자 인권단체들의 반대가 일었다.[269] 유전정보 데이터베이스가 이와 같은 논란을 가져온 것은 그 민감성 때문이다.

원안 중 하나였던 17대 국회 고경화 의원의 「실종아동의 보호 및 지원에 관한 특별법안」에 대한 국회 보건복지위원회 전문위원의 2004년 9월 검토보고서는 "본래 유전정보는 각 개인의 고유하고 다양한 정보들을 담고 있어서 실종아동을 찾기 위한 유용한 수단이 될 수 있지만 한편으로는 동 정보의 유용에 따른 인권침해의 우려가 있으므로, 이를 감안하여 신중히 접근할 필요가 있다고 생각됨"이라고 지적하였다.[270] 보다 구체적으로, 국가인권위원회는 「실종 아동 찾기 지원법 제정안」에 대한 의견에서 "유전자정보는 정보의 분석을 통해 개인 식별이 가능하고, 개인이 발현할 수 있는 성격상의 특징, 유전병과 관련한 정보 등을 알 수 있을 뿐 아니라 개인과 그 개인이 속한 가족구성원 전체의 유전적 질병에 대하여도 알 수 있는 정보로 오·남용의 경우 국민의 기본권을 침해할 소지가 있는 정보"라고 지적하였다.[271]

유전정보의 민감성이 거론되는 이유는 일차적으로 유전정보가 개인과 그

---

269) "미아찾기 사업은 지난 2001년부터 검찰이 해오던 사업으로 관련 법률이 없는 상태에서 진행돼 인권 사회단체들의 우려를 사왔던 사업이다. 그런데 경찰은 2004년 이 사업을 정치적인 이유로 검찰로부터 넘겨받아 법률적 기반도 없이 강행했다. 경찰은 '장기미아'에 대한 구체적인 정의가 무엇인지, 부모를 찾고자 하는 미아들이 얼마나 되는지 그리고 이들 중에서 인적정보가 없어 DNA 채취가 꼭 필요한 경우가 얼마나 되는지 등의 기본 개념 및 통계조자 밝히지 않고 우선 뽑고 보는 식으로 사업을 진행했다. 그러다 보니 부모가 명확한 위탁아동들에게 DNA 채취를 요구하거나 채취한 DNA를 외부로 넘길 수 있는 동의서를 받아 사회적 물의를 일으켰다. 또한 미아에 머무르지 않고 정신지체장애인, 치매 노인, 변사자로 그 대상을 확장했다. 그 동안 검경이 유전자 감식 정보를 이용한 신원확인 영역에서 보여준 모습은 각종 DB가 일부에 국한된 것이 아닌 또 다른 신원확인 시스템으로 발전할 수 있음을 보여준 것이다." 생명공학감시연대 등. 2005.11.14. "검경의 신원확인 유전자 DB 구축은 새로운 국가감시 시스템 도입의 서막이다".

270) 보건복지위원회 전문위원. 2004.9. 실종아동의보호및지원에관한특별법안(고경화의원) 검토보고서.

271) 국가인권위원회. 2004.9.6. 실종아동찾기지원법제정안에 대한 의견.

가족의 질병정보를 포함하고 있을 가능성 때문이다.[272] 사회적으로 유전정보의 이용이 확산될 경우 그에 따른 차별이 발생할 것을 우려하는 시각이 존재하고,[273] 유전자 검사 결과를 지나치게 과신하는 것이 위험하다는 지적도 있다.[274]

---

272) "개인의 유전체는 하나의 책과 같아서 5페이지에서 신원확인 정보를, 10페이지에서 질병정보를 뽑아낼 수 있다 … 실제로 영국 경찰은 유전자 감식 목적으로 추출한 혈액을 이용해 용의자의 인지나 동의 없이 HIV 검사와 같은 의료적 목적의 유전자 검사를 실시해 문제를 일으킨 바 있다"(김병수, 2005). "유전자 검사를 할 경우 민감한 개인의 질병정보 등이 분석될 수 있으므로, 지문의 채취나 혈액형의 확인을 위하거나, 혈중 알코올 농도의 측정을 위한 혈액의 채취에 비하여 훨씬 더 심각한 개인정보의 침해가 될 수 있다 … 유전자 정보는 기술이 계속 발전하면서 이미 가지고 있는 정보만으로도 새롭게 분석하는 것이 가능하므로 타 목적으로의 전용이나, 수집 당시에 알려진 것을 훨씬 뛰어넘는 정보분석을 할 수 있다. 이는 헌법상의 기본권인 사생활의 비밀과 자유, 양심의 자유를 훼손하는 문제가 있다"(이은우, 2009). "DNA 정보는 개인정보 중에서도 '사람의 육체적 상태에 관한 정보'로서 일종의 민감성 정보에 해당한다고 할 것이다. 따라서 그 보호의 정도는 여타의 개인정보보다 강하다고 보아야 한다 … 질병명은 내밀한 사적 영역에 근접하는 민감한 개인정보로서, 특별한 사정이 없는 한 타인의 지득, 외부에 대한 공개로부터 차단되어 개인의 내밀한 영역 내에 유보되어야 하는 정보이다. 이러한 성격의 개인정보를 공개함으로써 사생활의 비밀과 자유를 제한하는 국가적 조치는 엄격한 기준과 방법에 따라 섬세하게 행하여지지 않으면 아니된다(헌재 2007. 5. 31.)"(황성기, 2009). "유전정보는 개인마다 고유하고 다양한 정보들이 포함되어 있어 정보에 대한 기밀유지와 차별 금지가 요구되고 있다. 그리고 특정인의 유전자를 검사하면 가족의 유전적 상태까지 알 수 있어 특별한 주의가 필요하다. … 신원확인 목적으로 얻은 유전정보와 의료정보 같은 유전정보는 다르지만 유전자 DB 구축 과정에서도 식별 이외의 개인 유전정보를 얻을 수 있다. 신원확인에 사용되는 DNA와 다른 정보 분석에 사용되는 DNA는 그 부위만 다를 뿐 동일한 DNA 가닥 안에 존재하기 때문이다"(참여연대 등. 2004.4.20. "경찰의 유전자 DB구축에 대한 인권·사회단체 의견서"). "범죄자의 유전자 정보와 많은 부분 같을 수밖에 없는 가까운 친족들의 유전자 정보도 범죄자 유전자감식정보의 데이터베이스화를 통해 이들 친족들의 동의없이 공개되는 것이기 때문에, 범죄자의 가까운 친족들은 자기의 행위가 아닌 친족의 행위로 인하여 불이익한 처우를 받는 것이 된다. 연좌제 금지에 위배된다"(임지봉, 2005).

273) "개인의 유전정보는 매우 민감한 생체정보여서 활용에 따른 사회적 우려가 증가하고 있다. 유전정보는 각 개인마다 고유하고 가족과 공유하고 있으며, 미래의 상태까지 추측할 수 있는 예측력을 가지고 있다. 따라서 유전정보나 유전정보를 뽑아낼 수 있는 검체가 잘못 사용될 경우 사회적 차별과 불이익을 받을 가능성이 있다 … 2004년 7월 서울 남부지역에서 발생한 연쇄살인사건의 범인을 잡는다는 구실로 구체적 정황도 없이 수십 명 이상의 조선족 동포들의 유전자를 채취해 인권단체들로부터 비난을 받은 적이 있다"(김병수, 2005). "유전자 정보은행의 구축 대상자는 사회적 편견과 낙인이 강화되고, 비대상자와 차별되는 것이다. 이는 헌법상의 기본권인 평등의 원칙을 훼손하는 것이다"(이은우, 2009).

274) "오클라호마의 툴사에 거주하는 듀햄은 강간죄로 4년 동안 복역 후에 1997년 석방되었다. 그가 범죄시각에 다른 곳에 있었다는 7가지의 알리바이가 있었음에도 불구하고 그는 11살 소녀를 강간한 죄로 3000년 형을 선고받았는데, 이는 전적으로 DNA 테스트에 근거한 것이었다. 듀햄의 유전자형이 소녀의 몸에서 발견된 정액의 그것과 일

다른 한편으로 법률이 유전자검사의 대상으로 삼고 있는 아동등은 권리의 주체이자 보호의 대상이라 할 수 있는데, 보호라 할지라도 권리 존중이 선행되어야 하고 보호의 정도 또한 연령이나 성숙도 등에 따라 합리적으로 설정되어야 한다.[275] 이러한 취지에서 법률의 제정 목적에 부합하는 아동등에 한하여 유전자검사를 엄격히 실시하고, 보호자에게 복귀할 의사가 없거나 이미 복귀한 경우 등 그 목적에 더 이상 부합하지 않는 경우 그 유전정보를 즉각 폐기하는 것이 바람직하다. 그렇지 않으면 검사대상물이 오남용되거나, 대상이 한때 보호시설에 있었다는 이유로 평생 다양한 사유의 유전정보 검색 대상으로 편입될 가능성이 높기 때문이다.[276] 그러나 법률 제정 전후로 유전정보 데이터베이스의 관리감독이 엄격하고 투명하게 이루어지고 있는지에 대하여 사회적 우려가 존재해온 것이 사실이다.[277]

---

치했기 때문이다. 나중의 DNA 검사에서 듀햄은 용의자가 아님이 밝혀졌는데, 초기 테스트를 재분석한 결과 혼합된 샘플을 분리하는 어려움 때문에 해석을 잘못했음이 밝혀졌다 … 미국의 웨스트버지니아 주에서는 법의학 실험실에서 근무하는 법의학 기술자가 수년간 DNA 기록들을 변조한 사건이 있었다. 주 대법원은 이 기술자가 증언한 130건의 사례들을 검토한 결과 2001년까지 9명이 무죄로 석방되었다"(김병수, 2005). "2004년 미국 뉴저지검찰은 36년전 소녀를 강간살해한 혐의로 Bellamy를 체포하였다. 이때 유전자분석이 결정적인 역할을 하였다. 그러나 2년 후 체포된 Bellamy의 유전자가 오염되었다는 것이 드러나 풀려났고 이후 진범이 밝혀졌다 … 미국 FBI는 연방범이나 불법이민자들로부터 매년 130만명의 유전정보를 수집하려는 계획을 세우고 있다. 이에 대해 죄가 없으면 자신의 유전자가 보관된다는 것에 대해 전혀 두려워할 필요가 없다는 생각이 일반적이었으나 검사기관에서 검사오류가 발생한다는 것이 사실로 밝혀지면서 우려하는 분위기로 전환되고 있다"(남명진, 2009).

275) 국가인권위원회. 2009.6.4. 실종아동 등의 보호 및 지원에 관한 법률 일부개정법률안(김소남의원 대표발의)에 대한 의견표명.

276) "분석이 끝난 DNA는 일반적으로 차후의 검증 목적 등으로 보관하게 된다. 즉 DNA의 분석·이용·보관에 대한 관리 감독이 철저히 이루어지지 않는다면 잔여 DNA에서 식별이외의 유전정보가 분석 된 후 오·남용되어 인권을 침해할 가능성이 높다."(참여연대 등. 2004.4.20. 앞의 글); "DB에 입력된 개인은 감시를 의식하면서 살아야 할 것이다. 일순간의 잘못으로 죄를 저질러서 개인정보가 입력되면 평생을 압박감속에서 살아갈 것이다. 그것은 DB운명론으로 발전할 수 있다. 즉, 정직하게 살게 되기 보다는 감시를 피해 더욱 더 고도화된 범죄를 모색할 수 있다는 우려를 자아낸다."(남명진, 2009)

277) "불과 두달 사이에 3,143명의 18세 미만 무연고 아동과 5,672명의 무연고정신장애인의 유전자 샘플을 채취하였다 … 유전자 시료채취 및 활용 과정을 투명하게 하기로 하였음에도 불구하고 경찰청은 어떤 과정으로 시료채취와 활용이 이루어졌는지 전혀 공개하지 않고 있다." (참여연대 등. 2004.6.22. "미아찾기를 위한 근본적인 대책을 마련하라").

## 2. 유전정보의 수집·유통 실태

### 1) 유전정보의 수집 및 구축

「실종아동등의 보호 및 지원에 관한 법률」에 따르면 경찰청장은 보호시설의 입소자 중 보호자가 확인되지 아니한 아동등과 실종아동등을 찾고자 하는 가족으로부터 유전자검사대상물을 채취할 수 있고, 국립과학수사연구소장은 유전자검사를 실시하고 그 결과를 데이터베이스로 구축·운영할 수 있다.

2009년 7월까지 국립과학수사연구소가 보유중인 유전정보 현황은 다음과 같다.

<표 3-27> 국립과학수사연구소가 보유중인 연도별 유전정보 건수

| 연도 | 보유중인 유전자정보 건수 |
|---|---|
| 계 | 21,051 |
| 2004.05~2005.12 | 11,029 |
| 2006 | 4,406 |
| 2007 | 2,905 |
| 2008 | 1,296 |
| 2009.08.31 | 1,415 |

※ 요구입력 대상자수에서 폐기된 대상자수를 제외한 현보유 건수임.

자료: 국립과학수사연구소.[278]

법에서는 검사대상을 최소한으로 제한하기 위하여 검사대상물의 채취 및 유전자검사는 실종아동등의 여부를 확인한 후에 실시하도록 하였다(동법 제11조 및 동시행령 제5조). 여기서 실종아동등의 여부를 확인할 수 있는 신상정보 데이터베이스는 보건복지부의 위탁을 받은 실종아동전문기관에서 구축·운영하도록 되어 있어, 검사대상물을 채취하는 경찰청장과 유전자검사를 실시하는 국립과학수사연구소장의 업무와 분리되어 있다(동법 제8조). 검사대상물의 채취가 남발되지 않도록 사전에 실종아동등의 여부를 확인할 수 있으려면 서로 다른 기관간에 확인 및 협조 절차가 원활히 이루어질 필요가 있는 것이지만, 법률과 관련 시행령 및 규칙에서는 그 구체적인 절차에 대하여 규

278) '유전자 DB에 대한 추가 정보공개 청구'에 대한 국립과학수사연구소의 정보(부분공개) 결정통지서(2009.10.16). 문서번호: 유전자분석과-23261 (2009.10.15). 이 장에서 별도의 표시가 없으면 유전정보의 현황에 대한 출처는 이하 같다.

정하지 않았다. 또한 보호시설의 입소자 중 실종아동등의 여부가 확인되지 않은 경우 어떻게 처리할 지에 대한 사항은 경찰청장의 재량에 맡겨져 있다.

이에 대하여 경찰은 실종아동전문기관 및 경찰청 실종아동등찾기 시스템(프로파일링)상 실종아동등 여부를 조회 확인 후 검사대상물을 채취한다고 밝혔다.[279] 대상자의 인권침해를 방지하기 위하여서는 유전자검사 대상물의 채취와 검사의 목적을 명확히 하고 대상이 아닌 사람의 채취를 제한하는 절차가 매우 중요한 만큼, 경찰은 이러한 절차의 운용에 유념해야 할 것이다.

특히 정보주체의 유전자 검사 동의 여부는 민감한 개인정보 수집시 우선적으로 고려해야 할 중요한 사항 중의 하나이다. 법에서는 경찰청장이 검사대상물을 채취하고자 하는 때에는 미리 검사대상자의 서면동의를 얻도록 하였다(<그림 3-10>). 그리고 서면동의서를 10년간 보존하도록 하였다(동법 제11조 및 동시행령 제6조). 2009년 8월 현재 경찰이 보관중인 동의서는 21,577건이다.[280]

그러나 검사대상자가 미성년자・심신상실자 또는 심신미약자인 때에는 본인 외에 법정대리인의 동의를 얻도록 하여 보호시설 입소자가 대부분인 실종아동군의 검사대상자인 경우 본인의 동의 여부 의사가 반영될 수 없는 구조를 가지고 있다. 따라서 유전정보의 주체인 검사대상자가 성년에 도달하거나 심신미약상태를 벗어나는 경우 과거 검사에 대한 동의 철회 여부를 확인하고 그에 따른 조치를 취할 수 있는 절차가 구체적으로 마련될 필요가 있다.

### 2) 유전정보의 이용 및 제공

「실종아동등의 보호 및 지원에 관한 법률」 등에 의해 구체적으로 유전자검사 대상물이 채취되어 유전자검사가 이루어지고 그 결과를 관련 기관이 이용하고 제공하는 과정은 다음과 같다.[281]

먼저 경찰이 보호자가 확인되지 아니한 보호 아동등과 실종아동등을 찾고자 하는 가족으로부터 유전자검사대상물을 채취한 후, 해당 검사대상자의 신상을 기재한 서류와 채취한 검사대상물 및 서면동의서 사본을 같은 법률에 의해 설치된 실종아동전문기관 및 법인・단체의 장에게 송부한다.

---

279) '유전자DB 관련 추가 정보공개 청구'에 대한 경찰청의 정보(공개) 결정통지서 (2009.11.3). 문서번호: 여성청소년과-3544 (2009.11.03). 이 장에서 별도의 표시가 없으면 경찰의 업무와 관계된 내용의 충처는 이하 같다.

280) '유전자DB 관련 추가 정보공개 청구'에 대한 경찰청의 정보(공개) 결정통지서 (2009.11.3). 문서번호: 여성청소년과-3544 (2009.11.03).

281) 구체적인 절차 묘사는 국립과학수사연구소의 정보공개에 의함.

<그림 3-10> 유전자검사 동의서

## 유전자검사 동의서

| | | | | |
|---|---|---|---|---|
| 검사대상자 | 성 명 | | 생년월일 | |
| 법정대리인 | 성 명 | | 생년월일 | |
| 참 여 인 | 성 명 | | 생년월일 | |
| 동의서작성일자 | 년 월 일 | | | |

1. 유전자검사의 목적 : 유전자활용 실종아동등 찾기
2. 검사대상물의 처리 : 검사 후 즉시 폐기
3. 검사대상물은 본래 목적 외로 이용되거나 타인에게 제공되지 않음

※ 다음 각 항목에 대해서 상담자로부터 설명을 들은 후 본인이 충분하게 이해를 하였다고 판단하는 때에 □란 안에 √ 표를 하십시오.

1) 유전자검사의 이익과 위험에 대하여 관계자로부터 충분한 설명을 들었습니다. --□

2) 실종아동등이 보호자를 확인한 때, 검사대상자 또는 법정대리인이 요구하는 때 또는 유전자검사 작성일로부터 10년이 경과한 때는 유전정보를 폐기합니다. -----□

3) 동의권자가 상기 사항에 대하여 동의를 하였더라도 검사가 시작되기 이전에는 언제든지 동의를 철회할 수 있습니다. ---------- □

4) 실종아동전문기관 및 유전자검사기관은 동의권자의 개인정보 보호를 위하여 필요한 조치를 취하여야 할 의무가 있습니다. ----------□

※ 신상정보는 실종아동전문기관, 유전정보는 유전자검사기관(국립과학수사연구소)에서 분리 보관합니다

5) 유전자검사의 결과는 10년간 보존되며 언제든지 본인의 유전자검사 결과기록에 대하여 열람 또는 사본의 교부를 신청할 수 있습니다. ----------□

위의 사항에 대한 동의는 자발적 의사에 의한 것임을 밝히는 바입니다.

서명 검사대상자 _____

법정대리인 _____

참 여 인 _____

※ 구비서류 : 법정대리인임을 증명하는 서류(동의인이 법정대리인의 경우에 한합니다)

실종아동전문기관의 장은 받은 자료 중 검사대상물에 대하여 일련번호를 부여하여 이를 국립과학수사연구소장에게 송부한다. 국립과학수사연구소는 접수된 보호자군과 실종아동군의 검사대상물에 대한 유전자검사를 실시한 후 데이터베이스에 입력한다. 국립과학수사연구소의 유전자검사 결과 보호자를 확인한 건에 대해서는 감정서를 실종아동전문기관과 경찰청 여성청소년과에 회보한다. 또한 데이터베이스를 통하여 실종아동등이 보호자를 확인한 건과, 데이터베이스 조회와 관계없이 가족이 확인되어 실종아동전문기관에서 유전정보 폐기요청을 한 때에는 데이터베이스에서 유전정보를 폐기한다.[282]

이처럼 관련 법규에서 실종아동전문기관, 실종아동전문기관에 업무를 위탁한 보건복지부, 경찰청, 그리고 국립과학수사연구소의 업무가 상세하게 구분된 것은 민감한 유전정보의 목적 외 이용이나 제공을 엄격하게 제한하려는 취지에서이다.

「실종아동등의 보호 및 지원에 관한 법률」에 따르면 누구든지 실종아동등을 발견하기 위한 목적 외로 검사대상물의 채취 또는 유전자검사를 실시하거나 유전정보를 사용할 수 없다. 이 규정을 위반하여 목적 외로 검사대상물의 채취 또는 유전자검사를 실시하거나 유전정보를 사용한 자는 2년 이하의 징역 또는 1천만 원 이하의 벌금에 처한다. 또, 검사대상물의 채취, 유전자검사 또는 유전정보관리에 종사하거나 종사하였던 자는 채취한 검사대상물 또는 유전정보를 외부로 유출하여서는 아니되며, 이 규정을 위반한 자는 마찬가지의 형벌에 처해진다(동법 제12조 및 제18조).

### 3) 유전정보의 폐기

「실종아동등의 보호 및 지원에 관한 법률」에 따르면 검사기관이 유전자검사를 완료한 때에는 지체없이 검사대상을 폐기하도록 하여 오남용 소지를 방지하고자 하였다. 또한, 실종아동등이 보호자를 확인하였거나, 검사대상자 또는 법정대리인이 요구하였거나, 유전자검사일로부터 10년이 경과하는 때에는 해당유전정보를 지체없이 폐기하도록 하였다(동법 제13조).

282) 국립과학수사연구소는 매달 10일에 실종아동등이 보호자를 확인한 건, 실종아동기관에서 폐기 요청을 한 건에 대해 실종아동관련 데이터베이스에 접속하여 '삭제'한다고 밝혔다.

<표 3-28> 유전자 데이터베이스에서 폐기된 유전정보 건수

| 연 도 | 유전자검사 결과 보호자확인후 폐기된 건 | | 유전자검사 결과와 관계 없이 실종아동전문기관이 요청하여 폐기된 건 |
|---|---|---|---|
| | 보호자군과 실종아동군 합계 | 실종아동군 | |
| 계 | 276 | 132 | 77 |
| 2004.05~2005.12 | 71 | 34 | 15 |
| 2006 | 33 | 16 | 12 |
| 2007 | 50 | 23 | 4 |
| 2008 | 74 | 34 | 24 |
| 2009.08.31 기준 | 48 | 25 | 22 |

자료: 국립과학수사연구소.

국립과학수사연구소가 밝힌 바에 따르면, 유전정보 데이터베이스가 구축된 후 2009년 10월 16일 현재까지 폐기된 유전정보 건수는 353건이며 이는 실종아동등이 보호자를 확인하였거나 실종아동전문기관이 폐기를 요청한 데 따른 폐기이다. 이중 유전자검사를 통해 실종아동등이 보호자를 확인한 건수는 276건이다. 그밖에도 「실종아동등의 발견 및 유전자검사 등에 관한 규칙」에서는 유전정보의 폐기를 요구하는 검사대상자 또는 법정대리인이 사용할 수 있는 유전정보 폐기 신청서의 서식을 설명하고 있다. 이러한 규정에 따라 국립과학수사연구소장이 유전자검사대상물 또는 유전정보를 폐기하는 경우에는 서식에 의한 유전자검사대상물·유전정보 폐기대장을 작성하고, 5년간 보관하여야 한다(동규칙 제6조). 국립과학수사연구소는 2009년 10월 16일 현재까지 검사대상자 또는 법정대리인이 유전정보의 폐기를 요청하여 폐기가 이루어진 건수는 존재하지 않는다고 밝혔다.

그러나 보건복지부는 실종아동전문기관이 검사대상자의 요청에 따라 폐기를 요청한 건수가 2009년 8월 31일 현재 98건이라고 밝혔다. 또한 실종아동전문기관이 폐기를 요청한 전체 건수가 445건이라고 밝혀 국립과학수사연구소와 큰 차이를 보였다.

유전정보 관리 및 통계에 있어 국립과학수사연구소와 실종아동전문기관 간에 차이가 나는 것은, 유전정보 관리가 다소 허술하게 이루어지고 있다는 우려를 낳는다. 만약 검사대상자가 국립과학수사연구소에 직접 폐기를 요청하지 않고 실종아동전문기관을 통하여 폐기하는 것이 현실적이라고 하면, 그에 따른 폐기 신청서의 관리 등 관련 법령과 절차의 개선이 이루어질 필요가 있다.

<표 3-29> 실종아동전문기관이 폐기를 요청한 건수

| 연도별 | 가족관계 확인으로 인한 폐기 | 기타 | 계 |
|---|---|---|---|
| 2006년 | 54 | 16 | 70 |
| 2007년 | 102 | 23 | 125 |
| 2008년 | 129 | 34 | 163 |
| 2009년 8월 31일 | 62 | 25 | 87 |
| 계 | 347 | 98 | 445 |

※ 기타는 검사대상자의 요청에 의한 폐기등임.
자료: 보건복지가족부.[283]

이 법률에서는 법률에서 규정하고 있는 유전정보의 보유 목적이 다한 경우 적극적인 폐기 원칙을 규정하지 않았다. 즉 유전정보의 주체인 검사대상자가 성년에 도달하거나 심신미약상태를 벗어나는 경우 과거 검사에 대한 동의 철회 여부를 확인하고 그에 따른 조치를 취할 수 있는 절차가 구체적으로 마련되어 있지 않다. 다만 유전자검사일로부터 10년이 경과하는 때에는 해당유전정보를 지체 없이 폐기하도록 하였다. 2009년 10월 16일 현재 이 사유에 따른 폐기 건수는 존재하지 않는다.

## 3. 정보주체의 열람 및 정정·삭제 청구권 보장 실태

「실종아동등의 보호 및 지원에 관한 법률」에 따르면 검사기관은 검사대상자 또는 법정대리인이 유전자검사 결과기록의 열람 또는 사본의 교부를 요청하는 때에는 이에 따르도록 하였다(동법 제14조). 또 「실종아동등의 발견 및 유전자검사 등에 관한 규칙」에서는 검사대상자 또는 법정대리인이 유전자검사 결과기록의 열람 또는 사본의 교부를 요청할 때 사용할 수 있는 유전자검사 결과기록 열람·사본교부 신청서의 서식을 설명하고 있다. 이러한 규정에 따라 국립과학수사연구소장은 유전자검사 결과기록 열람·사본교부 신청서를 5년간 보관하여야 한다(동규칙 제7조).

국립과학수사연구소에서 밝힌 바에 따르면, 2009년 10월 16일 현재 유전자검사기록의 열람 또는 사본의 교부 건수는 존재하지 않는다.

283) '실종아동등의 보호 및 지원에 관한 법률 시행에 대한 정보공개 청구'에 대한 보건복지가족부의 정보(공개) 결정통지서(2009.11.02). 문서번호: 아동청소년안전과-3642 (2009.11.02). 이 장에서 보건복지가족부의 자료에 대한 출처는 이하 같다.

한편 유전정보는 그 특성상 정정 청구권이 인정되기는 어렵지만, 법률에서는 검사대상자 또는 법정대리인이 유전정보의 폐기를 요구하는 때에 해당정보를 지체없이 폐기하도록 하였다. 본 연구에서는 실종아동전문기관을 통해 검사대상자의 요청에 따른 유전정보의 폐기가 이루어져 온 것으로 확인되었다.

## 4. 소결

「실종아동등의 보호 및 지원에 관한 법률」은 보호자가 있는 곳으로 복귀하고 싶은 아동등에게 그럴 수 있는 지적능력이나 판단능력이 충분하지 않은 경우 그들의 조속한 발견과 복귀를 돕기 위한 법률인 만큼, 검사대상자이자 정보주체인 실종아동등의 의사를 계속적으로 확인하고 반영할 수 있는 구조가 필요하다. 또한 유전정보는 사회적 차별로 이어질 수 있는 매우 민감한 개인정보인 만큼 그 수집 및 이용과 제공을 엄격하게 제한하려는 법률의 제정 취지를 훼손하는 일이 없어야 할 것이다.

그러나 국가가 유전정보를 채취하고 데이터베이스를 구축 및 운영하는 과정에서 다소 미흡한 점이 발견되었다. 특히 검사 시점에 본인이 아닌 법정대리인의 동의 하에 채취가 이루어진 경우 이후 정보주체의 동의 철회 및 폐기 의사를 확인하여 반영할 수 있는 구조가 보장되어 있지 않았다.

한때 유전정보 데이터베이스에 그 유전정보가 편입되었다 하더라도, 유전정보의 주체인 시설 아동등이 성년에 도달하거나 심신미약상태를 벗어나는 경우 폐기되어야 한다. 따라서 검사대상자가 과거 검사에 대한 동의 철회 여부를 확인하고 그에 따른 폐기 조치를 취할 수 있는 절차가 구체적으로 마련되어야 법률상 취지와 목적에 부합한다 할 것이다.

또한 기본적인 유전정보 관리 및 통계에 있어 국립과학수사연구소와 실종아동전문기관 간에 차이가 있는 것으로 드러났다. 이는 유전정보 관리의 허술함으로 이어질 수 있기 때문에 개선될 필요가 있다.

# 제4절 통신 비밀

## 1. 개요

### 1) 통신의 비밀과 자유

헌법 제18조는 “모든 국민은 통신의 비밀을 침해받지 아니한다.”고 규정하고 있다. 통신의 비밀은 개인이 그 의사나 정보를 우편물이나 전기통신 등의 수단에 의하여 전달 또는 교환하는 경우에 그 내용 등이 본인의 의사에 반하여 공개되지 아니할 권리를 말하며 통신의 자유라고도 한다. 국가안보 및 범죄수사 등 공공의 안전을 위한 감청은 허용될 수 있으나 최후적 수단으로 사용되어야 하며, 그 내용과 절차에 엄격한 사전·사후 통제장치를 마련해 국민의 통신의 자유와 사생활의 비밀과 자유에 대한 제한을 최소화하는 것이 바람직하다(국가인권위원회, 2009).

통신의 자유는 오늘날과 같이 전자우편 또는 인터넷의 활용이 일상화되고 있는 상황에서 통신행위와 표현행위를 포괄하는 양면성을 가진 자유이다. 통신기술의 발달은 개인간 의사전달 수단을 다양화함으로써 통신 자유를 확장하는데 기여했지만, 그에 못지않게 아니 그 이상으로 개인의 통신 비밀을 광범위하게 침해할 수 있는 수단을 제공하고 있다. 오늘날 한 개인에게 통신활동이 차지하는 비중을 감안할 때 통신 감청에 의한 개인 통신 정보의 노출은 한 개인의 인격 전반의 노출은 물론 그에 따른 왜곡까지 우려된다는 점에서 더 심각한 문제를 야기한다. 신체 자유 제한은 외형적으로 드러나지만 통신 감청은 대상자가 의식할 수 없는 점에서 더 심각한 인권 침해를 초래한다.

따라서 통신 비밀의 최대한 보장원칙은 국가권력에 의한 최소한의 제한을 통해 그리고 통신사업자 등 사인에 의한 침해 보호를 통해 구현되어야 한다. 현행 「통신비밀보호법」에서는 동법에 의한 우편물의 검열 또는 전기통신의 감청이 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다는 점을 명시하고 있다(동법 제3조의 제2항). 또한, 사이버공간에서 표현행위는 일반적인 언론 자유보다 더 강하게 보장되어야 하므로 익명성의 보장과 접속에 있어서 추적당하지 않을 권리가 강하게 보장되어야 한다(오동석, 2007).

### 2) 법적 근거

국가안보 및 범죄수사 등의 목적으로 통신의 비밀을 제한하는 것과 관련한 현행 법률은 크게 「전기통신사업법」, 「통신비밀보호법」, 「형사소송법」으로 볼 수 있다.

먼저 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입 또는 해지일자 등 통신 이용자의 인적사항에 대한 자료는 「전기통신사업법」 제54조에 의해 이루어진다. 이 법에 따르면 일반수사기관이나 정보수사기관이 통신사업자에게 이용자의 성명 등에 대한 통신자료를 요청할 때 서면에 의하도록 하였다. 이 조항은 1991년 8월 「공중전기통신사업법」이 「전기통신사업법」으로 개정되면서 제54조에 '통신비밀의 보호'에 대한 규정을 신설하고 제3항에 "전기통신사업자 또는 … 전기통신사업의 일부를 수탁하여 취급하는 자는 수사상 필요에 의하여 관계기관으로부터 전기통신업무에 관한 서류의 열람이나 제출을 서면으로 요구받은 때에는 이에 응할 수 있다"고 규정한 것으로부터 유래했다. 그러나 수사기관이 '전기통신업무에 관한 서류의 열람이나 제출'을 요구할 수 있는 법률적 요건과 절차의 모호함에 대한 비판이 계속되었다.[284] 그로 인하여 2000년 1월 전기통신사업자에 대하여 전기통신업무에 관한 서류의 제출등을 요구할 수 있는 자를 검사 및 수사관서의 장등으로 제한하고, 그 제공되는 서류의 범위를 한정하는 등 절차를 강화하는 개정이 이루어져 오늘에 이른다.

하지만 현행 법률에 따르면 통신자료에 대한 수사기관의 서면 요청에 있어 범죄사실의 입증이나 법원의 영장이 불필요하며, 긴급한 사유가 있는 때에는 서면을 사후에 제출해도 된다. 그 긴급한 사유가 무엇인지에 대해서는 법률에 규정을 두고 있지 않다. 이로 인하여 통신자료의 제공에 있어 남용의 가능성이 크므로 적절한 제한이 필요하다는 지적이 일고 있다. 관련하여 2009년 5월 22일 이정현 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의

284) "통신비밀의 보호를 정한 54조의 예만 해도 사업자에 대해 … 통화내용의 유출통로를 크게 넓힘으로써, 기본권 제한의 과잉금지 원칙을 스스로 거스르고 있다." 문화일보. 1999.9.4. "<사설>전화걸기 무서운 세상".; "통신업체에서는 수사기관들이 문서를 제출하지 않고 전화로 가입자정보를 요구해도 바로 알려주는 것이 관행으로 돼 있다." 경향신문. 1999.9.14. "보호막 뚫린 私生活 - '통신가입자 정보제공' 문제점".; "여야는 전기통신사업법에서 대표적인 '독소조항'으로 지적받고 있는 통화정보제공 관련부분의 개정을 추진키로 했다. 이 조항은 그동안 수사기관이 통화상대방의 전화번호, 통화시간, 특정 전화번호의 주소지 등 통화정보를 무차별적으로 제공받을 수 있어 법 남용의 소지가 많다는 지적을 받아왔다." 동아일보. 1999.10.21. "여야, 전기통신사업법 개정 통화정보제공 제한."

안번호 제1804925호)」에서는 「전기통신사업법」에 규정된 가입자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입 또는 해지일자 등을 가입자정보로 정의하여 「통신비밀보호법」의 규정에 포함하고, 검사 또는 사법경찰관이 수사 또는 형의 집행을 위하여 필요한 경우 법원의 허가를 받아 전기통신사업자에게 가입자정보의 제공을 요청할 수 있도록 하여 통신자료의 제공과 관련한 절차 규정을 강화하였다.

「전기통신사업법」
제54조 (통신비밀의 보호)
③전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장으로부터 재판, 수사(「조세범처벌법」 제11조의2제1항, 제4항 및 제5항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청받은 때에 이에 응할 수 있다. <개정 2002.12.26, 2007.1.3>
1. 이용자의 성명
2. 이용자의 주민등록번호
3. 이용자의 주소
4. 이용자의 전화번호
5. 아이디(컴퓨터시스템이나 통신망의 정당한 이용자를 식별하기 위한 이용자 식별부호를 말한다)
6. 이용자의 가입 또는 해지 일자
④제3항의 규정에 의한 통신자료제공의 요청은 요청사유, 해당이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 "자료제공요청서"라 한다)으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있는 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 해소된 때에 지체없이 전기통신사업자에게 자료제공요청서를 제출하여야 한다. <신설 2000.1.28>

한편, 통신 이용자의 전기통신일시, 전기통신개시·종료시간, 발·착신 통신번호 등 상대방의 가입자번호, 사용도수, 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료, 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료, 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료 등 통신사실 확인자료는 「통신비밀보호법」에 의해 제공된다. 「통신비밀보호법」은 일반수사기관이나 정보수사기관이 통신사업자에게 통신사실

확인자료를 요청할 때 법원의 허가를 받도록 하였으며 사업자에 협조 의무를 규정하였다. 본래 「통신비밀보호법」이 제정되었을 당시에는 통신사실 확인자료 제공에 대한 아무런 조항이 없어 「전기통신사업법」에 의해 제공되어 오다가 2001년 12월 「통신비밀보호법」이 개정되면서 "검사 또는 사법경찰관이 … 통신사실 확인자료제공을 요청하는 경우에는 미리 서면 또는 이에 상당하는 방법으로 관할지방검찰청 검사장(검찰관 또는 군사법경찰관이 통신사실 확인자료 제공을 요청하는 경우에는 관할 보통검찰부장을 말한다)의 승인을 얻어야 한다"고 관련 규정을 두게 되었다.[285] 2003년부터 국가정보원과 국군기무사령부가 일간지 기자의 통화내역을 조회하는 등 통신사실 확인자료 제공의 오남용 문제가 사회적으로 불거지면서,[286] 2005년 5월 개정에서 일반수사기관과 정보수사기관이 통신사실 확인자료 제공을 요청할 경우 "요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다) 또는 지원의 허가를 받"도록 절차가 강화되었다.

그러나 현행 법률에 따르면 수사기관이 '수사 또는 형의 집행을 위하여 필요한 경우'만으로 통신사실 확인자료의 제공을 요청할 수 있도록 하여 범죄사실을 입증할 필요가 없다. 긴급한 사유가 있는 때는 법원의 허가를 사후에 받도록 하였고, 긴급한 사유가 무엇인지에 대해서는 법률에 규정을 두고 있지 않다. 이와 관련하여 2009년 5월 22일 변재일 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1803789호)」에서는 범죄수사를 위한 통신사실 확인자료 요청의 경우 예외 없이 법원의 허가를 먼저 얻은 후 하도록 절차를 강화하였다.

또한 현행 법률은 정보수사기관의 경우 '국가안전보장에 대한 위해를 방지

---

285) 이와 같은 사실은 통신사실 확인자료 규정 신설을 논의하였던 당시 국회 소관상임위원회 전문위원의 관련 법안 검토보고서에서도 확인할 수 있다. "1999년 12월 이전에는 전기통신사업법 제54조에서 통신자료제공이라는 용어를 사용하면서 '이용자인적자료'와 '통신사실확인자료'를 모두 포함하여 자료제공범위로 규정하고 있었으나, 1999년 12월 법제사법위원회의 전기통신사업법 및 통신비밀보호법 개정안 심사시 여야가 합의하여 전기통신사업법의 통신자료제공, 즉 '통신사실확인자료'를 통신비밀보호법으로 이관하기로 합의한 바가 있음." 과학기술정보통신위원회 수석전문위원. 2001.2. "통신비밀보호법중개정법률안에대한 의견제시의건 - 검토보고" 참조.

286) 한겨레신문. 2003.10.7. "[사설] 기자 '통화' 조회는 반언론적 발상"; 한겨레신문. 2003.10.8. "통화 멋대로 조회…"영장도입을""; 국민일보. 2004.1.30. "[사설] 정부가 아직도 이 수준인가"; 경향신문. 2004.1.30. "국정원, 靑요구로 기자 통화내역 조회"; 한국일보. 2004.2.18. "한국일보 기자 통화내역도 조회"; 국민일보. 2004.2.18. "기무사령부도 기자 통화내역 조회했다"; 한국일보. 2004.2.19. "'통화내역 조회' 가입자 33명중 1명꼴"; 서울신문. 2004.2.19. "[사설] 통화조회 남발 이대로 안된다" 등 참조.

하기 위하여 정보수집이 필요한 경우' 전기통신사업자에게 통신사실 확인자료 제공을 요청할 수 있도록 규정되어 있다(동법 제13조의4). 이와 관련하여 변재일 의원의 개정안에서는 현행 감청의 허가 요건과 동일하게 '국가안전보장에 대하여 상당한 위험이 현존하거나 예상되어 그 위해를 방지하기 위한 경우'로 그 요건을 강화하였다.

「통신비밀보호법」
제13조 (범죄수사를 위한 통신사실 확인자료제공의 절차 <개정 2005.5.26>) ① 검사 또는 사법경찰관은 수사 또는 형의 집행을 위하여 필요한 경우 전기통신사업법에 의한 전기통신사업자(이하 "전기통신사업자"라 한다)에게 통신사실 확인자료의 열람이나 제출(이하 "통신사실 확인자료제공"이라 한다)을 요청할 수 있다.
②제1항의 규정에 의한 통신사실 확인자료제공을 요청하는 경우에는 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(보통군사법원을 포함한다. 이하 같다) 또는 지원의 허가를 받아야 한다. 다만, 관할 지방법원 또는 지원의 허가를 받을 수 없는 긴급한 사유가 있는 때에는 통신사실 확인자료제공을 요청한 후 지체 없이 그 허가를 받아 전기통신사업자에게 송부하여야 한다. <개정 2005.5.26>

가장 민감하고 논란이 많이 되는 것은 전화 통화, 이메일 등 공개되지 않은 통신의 내용에 대하여 통신제한조치, 즉 감청을 실시하는 경우이다. 많은 논란을 거쳐 제정된 「통신비밀보호법」은 제정 당시부터 일반수사기관이나 정보수사기관이 통신 사업자에게 공개되지 않은 통신 내용에 대한 감청을 요청할 때 법원의 허가서, 즉 영장을 받도록 규정하였다. 이때 통신 감청은 헌법상의 기본권을 중대하게 제한하는 것이므로 법률에 규정된 대상 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가될 수 있다(동법 제5조). 또한 법률에서는 검사와 사법경찰관이 법원에 대하여 감청의 허가를 구하는 절차에 대하여 상당히 엄격하게 규정하였다(동법 제6조).

「통신비밀보호법」
제6조 (범죄수사를 위한 통신제한조치의 허가절차) ①검사(검찰관을 포함한다. 이하 같다) 는 제5조제1항의 요건이 구비된 경우에는 법원(군사법원을 포함한다. 이하 같다)에 대하여 각 피의자별 또는 각 피내사자별로 통신제한조치를 허가하여 줄 것을 청구할 수 있다. <개정 2001.12.29>

②사법경찰관(군사법경찰관을 포함한다. 이하 같다)은 제5조제1항의 요건이 구비된 경우에는 검사에 대하여 각 피의자별 또는 각 피내사자별로 통신제한조치에 대한 허가를 신청하고, 검사는 법원에 대하여 그 허가를 청구할 수 있다. <개정 2001.12.29>
③제1항 및 제2항의 통신제한조치 청구사건의 관할법원은 그 통신제한조치를 받을 통신당사자의 쌍방 또는 일방의 주소지·소재지, 범죄지 또는 통신당사자와 공범관계에 있는 자의 주소지·소재지를 관할하는 지방법원 또는 지원(보통군사법원을 포함한다)으로 한다. <개정 2001.12.29>
④제1항 및 제2항의 통신제한조치청구는 필요한 통신제한조치의 종류·그 목적·대상·범위·기간·집행장소·방법 및 당해 통신제한조치가 제5조제1항의 허가요건을 충족하는 사유등의 청구이유를 기재한 서면(이하 "청구서"라 한다)으로 하여야 하며, 청구이유에 대한 소명자료를 첨부하여야 한다. 이 경우 동일한 범죄사실에 대하여 그 피의자 또는 피내사자에 대하여 통신제한조치의 허가를 청구하였거나 허가받은 사실이 있는 때에는 다시 통신제한조치를 청구하는 취지 및 이유를 기재하여야 한다. <개정 2001.12.29>
⑤법원은 청구가 이유 있다고 인정하는 경우에는 각 피의자별 또는 각 피내사자별로 통신제한조치를 허가하고, 이를 증명하는 서류(이하 "허가서"라 한다)를 청구인에게 발부한다. <개정 2001.12.29>
⑥제5항의 허가서에는 통신제한조치의 종류·그 목적·대상·범위·기간 및 집행장소와 방법을 특정하여 기재하여야 한다. <개정 2001.12.29>
⑦통신제한조치의 기간은 2월을 초과하지 못하고, 그 기간중 통신제한조치의 목적이 달성되었을 경우에는 즉시 종료하여야 한다. 다만, 제5조제1항의 허가요건이 존속하는 경우에는 제1항 및 제2항의 절차에 따라 소명자료를 첨부하여 2월의 범위안에서 통신제한조치기간의 연장을 청구할 수 있다. <개정 2001.12.29>
⑧법원은 청구가 이유없다고 인정하는 경우에는 청구를 기각하고 이를 청구인에게 통지한다.

한편, 공개되지 않은 통신의 내용이라 하더라도 송수신이 완료된 과거의 통신 내용에 대한 제공은 「통신비밀보호법」의 감청 절차에 의하지 않고 「형사소송법」상 일반 압수·수색·검증 절차에 의해 이루어져 왔다. 이는 송수신이 완료된 경우에는 「통신비밀보호법」의 보호대상이 되지 않는다는 법원의 입장에 따른 것이다.[287] 그러나 2009년 4월 검찰이 주경복 전 서울

287) 대법원 2003.8.22. 2003도3344 판결. 그러나 이 판결 이후로도 과거의 통신 내용에 대한 압수수색 문제가 계속 불거져 왔다. 2004년에는 대학수학능력시험 부정 사건과 관련하여 당일 시험시간대의 전 국민 문자메시지 2억여 건 중 숫자로만 구성된 24만8천 건의 내역을 이동통신사들로부터 제출받아 경찰이 수사에 이용한 사건이 논란이 되었었다. 압수수색의 대상인 휴대전화 번호를 특정하지 않은 '투망식' 압수수색영장이 시민 전체를 잠재적 범죄자로 취급하였다는 비판이 제기되었다. 김두식. "누구에게도

시 교육감 후보의 선거법 위반 사건을 수사하면서 수사 대상자 100여 명의 최장 7년 치 이메일을 압수수색하고 당사자에게는 그 사실이 전혀 통지되지 않은 사건이 알려지면서 과거의 통신 내용 제공에 대한 규제 요구가 높아졌다.[288] 이어 6월에는 광우병 쇠고기 관련 MBC <PD수첩> 보도를 조사 중이던 검찰이 작가 등 7개월 치 이메일을 압수수색하고 그 내용의 일부를 공개한 사건이 큰 파장을 불러왔고, 7월에는 YTN 노조원 20여 명의 이메일을 압수수색한 사실이 밝혀졌다. 또 8월에는 경찰이 시국선언을 주도한 교사 25명의 이메일을 대대적으로 압수수색한 사실이 알려지는 등 관련 사건이 연이었다.[289]

이런 논란 속에 2009년 5월 수사기관이 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 당사자에게 통지하도록 하는 규정이 「통신비밀보호법」에 신설되었으나(동법 제9조의3), 그 구체적인 요건이나 절차는 규정하지 않았다. 현재 송·수신이 완료된 전기통신에 대한 압수·수색·검증은 「형사소송법」의 일반적인 압수 및 수색 관련 규정에 따라 이루어진다.

2009년 10월 현재 송·수신이 완료된 전기통신에 대한 압수·수색·검증 요건과 절차를 규정하는 법률 개정안 2건이 발의되어 있다. 먼저 박영선 의원이 대표발의한 「형사소송법 개정안(의안번호 제1805246호)」에서는 압수·수색할 물건이 우편물, 통신사업자의 서버에 저장된 이메일 내용, 휴대전화의 문자메시지, 음성사서함, 비공개 게시물 기타 이와 유사한 것으로서 대통령령으로 정하는 물건의 경우에는 피고인이 죄를 범하였다고 의심할만한 상당한 이유가 있고 특정한 사유가 있을 때 압수할 수 있도록 하고, 제출을 명하거나 압수할 물건이 이메일 등인 경우 송수신자에게 그 취지를 통지할 수

---

비밀은 없다." 한겨레신문. 2004.12.1.

288) 검찰은 2008년 7월에 치러진 서울시교육감 선거 과정상의 불법 선거운동에 대한 수사와 관련하여, 주경복 선거대책본부의 간부 및 실무자들과 전교조 서울지부 간부 및 조합원들 백여 명의 이메일계정에 대하여 압수수색하였다. 이 과정에서 압수된 이메일이 가입 당시부터 최장 7년 치에 해당하는 방대한 규모에 달하는 것으로 드러났다. 이에 2009년 4월 27일 전교조 활동가 21명과 주경복 당시 교육감후보자 및 주경복 선본 관계자 1명(총 23명)은 헌법소원 심판을 청구하였다. http://seoul.eduhope.net/bbs/view.php?board=seoul-210&id=1005&page=1 참고.

289) 한겨레. 2009.6.19. "사생활 엿보고 들추고…검찰 '이메일 공안통치'"; 프레시안. 2009.7.1. "YTN 노조원 20명 9개월치 이메일 압수 수색 당해"; 위클리경향 832호. 2009.7.7. "e메일 공개 적법성 검찰에 되묻다"; 미디어스. 2009.8.29. "사이버 망명 : 저항의 공간을 개시하는 작은 몸짓"; 내일신문. 2009.9.2. "메일 압수수색 등 무리한 수사 논란" 등.

있도록 하는 등 우체물 압수에 관한 규정을 준용하는 한편, 압수·수색할 물건이 이메일 등인 경우에는 압수·수색영장에 작성기간을 추가로 기재하도록 하였다. 이학재 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1805261호)」에서는 전기통신의 정의에 송수신이 완료된 전자우편을 포함하고, 송수신이 완료된 전자우편에 대한 수사 등에 대하여 「형사소송법」에 우선하여 「통신비밀보호법」을 적용하도록 함으로써 「통신비밀보호법」의 감청 요건과 절차를 따르도록 하였다.

<표 3-30> 통신 관련 자료 제공의 절차 현황 (2009년 10월)

| 제공 대상 | 적용법률 | 제공 절차 |
|---|---|---|
| 이용자 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입/해지일자 [통신자료] | 전기통신사업법 제54조 | 요청사유, 해당이용자와의 연관성, 필요한 자료의 범위를 기재한 서면으로 요청<br>※ 긴급한 사유가 있는 때에는 사후제출 |
| 가입자 전기통신일시, 전기통신개시·종료시간, 상대방 가입자번호, 사용도수, 인터넷 로그기록자료, 발신기지국의 위치추적자료, 정보통신기기 접속지 위치추적자료 [통신사실 확인자료] | 통신비밀보호법 제13조부터 제13조의5 | 요청사유, 해당 가입자와의 연관성 및 필요한 자료의 범위를 기록한 서면으로 관할 지방법원(군사법원 포함) 또는 지원의 허가를 받아 요청<br>※ 긴급한 사유가 있는 때에는 사후제출<br>※ 정보수사기관의 경우 별도 규정 |
| 발송·수취하거나 송·수신하는 특정한 우편물이나 전기통신 또는 대상자가 일정한 기간에 걸쳐 발송·수취하거나 송·수신하는 우편물이나 전기통신 [통신제한조치] | 통신비밀보호법 제5조부터 제9조의2 | 통신제한조치의 종류·그 목적·대상·범위·기간·집행장소·방법 및 당해 통신제한조치가 허가요건을 충족하는 사유 등의 청구이유를 기재한 서면 청구서와 청구이유에 대한 소명자료를 첨부하여 법원의 허가서를 발부받아 요청<br>※ 긴급한 사유가 있는 때에는 36시간 이내 사후제출<br>※ 정보수사기관의 경우 별도 규정 |
| 송·수신이 완료된 전기통신에 대한 압수·수색·검증 | 형사소송법 제215조 | 피고인의 성명, 죄명, 압수할 물건, 수색할 장소, 신체, 물건, 발부연월일, 유효기간 등을 기재하고 재판장 또는 수명법관이 서명날인한 압수·수색영장을 발부받아 요청 |

## 2. 개인정보의 수집・유통 실태

### 1) 통신자료

가입자 성명, 전화번호, 주민등록번호, 주소, 인터넷 아이디 등 이용자 인적사항에 대한 통신자료를 정보수사기관에 제공하는 건수는 해마다 급증하는 추세에 있다. 통신수단별로 살펴보았을 때 전반적으로 인터넷 관련 통신자료 제공건수의 증가치가 두드러지는 가운데, 2008년 전체적인 제공건수가 전화번호 혹은 아이디 건수를 기준으로 5백만 건을 넘어섰다. 통신자료 제공건수가 이처럼 높은 것은 현행 법률이 통신자료 제공을 요청할 때 필요한 절차를 엄격히 규정하지 않은데 따른 결과로서 오남용 논란이 끊이지 않고 있다.[290]

<표 3-31> 통신수단별 통신자료 제공 건수

(단위: 문서수)

| | 유선전화 | 이동전화 | 무선호출 | PC통신・인터넷 | 합계 |
|---|---|---|---|---|---|
| 2000 | 18,464 | 57,077 | 885 | 1,647 | 78,073 |
| 2001 | 22,665 | 85,390 | 158 | 5,209 | 113,422 |
| 2002 | 24,533 | 87,858 | 111 | 15,285 | 127,787 |
| 2003 | 39,460 | 119,360 | 70 | 30,302 | 189,192 |
| 2004 | 46,366 | 191,649 | 20 | 41,894 | 279,929 |
| 2005 | 56,614 | 244,976 | 23 | 41,158 | 342,771 |
| 2006 | 48,462 | 204,071 | 9 | 71,024 | 323,566 |
| 2007 | 57,375 | 275,338 | 4 | 93,691 | 426,408 |
| 2008 | 58,374 | 296,913 | 1 | 119,280 | 474,568 |

자료: (구)정보통신부와 방송통신위원회의 반기별 발표자료를 취합.[291]

290) 2008년 10월, 정부와 경찰이 인터넷 게시물을 상시적으로 사찰하고 그 게시자의 아이디 등 개인정보를 입수해온 사실이 언론과 국정감사를 통해 알려졌다. 위클리 경향 797호. 2008.10.28. “경찰 앞에 서면 ‘작아지는 포털’”.; 한겨레신문. 2008.10.5. “문화부 ‘비판댓글 사찰반’ 5개월째 운영”.

291) 이 장에서 별도의 표시가 없으면 통신자료/통신사실 확인자료/통신제한조치의 현황에 대한 출처는 이하 같다.

<표 3-32> 기관별 통신자료 제공 건수

(단위: 전화번호 혹은 아이디 건수)

| | 검찰 | 경찰 | 국정원 | 군수사기관 | 합계 |
|---|---|---|---|---|---|
| 2000 | 99,925 | 213,975 | 31,676 | 121,336 | 466,912 |
| 2001 | 122,651 | 380,480 | 64,348 | 140,478 | 707,957 |
| 2002 | 158,949 | 481,474 | 48,522 | 110,007 | 798,952 |
| 2003 | 271,488 | 697,621 | 79,988 | 107,944 | 1,157,041 |
| 2004 | 348,620 | 1,378,130 | 84,273 | 97,464 | 1,908,487 |
| 2005 | 881,954 | 2,103,661 | 58,976 | 145,320 | 3,189,911 |
| 2006 | 947,369 | 2,069,948 | 43,184 | 151,808 | 3,212,309 |
| 2007 | 873,423 | 3,257,258 | 49,995 | 143,730 | 4,324,406 |
| 2008 | 1,061,553 | 3,770,259 | 55,090 | 268,949 | 5,155,851 |

### 2) 통신사실 확인자료

통화내역, 위치정보, 인터넷 IP주소 등 통신사실 확인자료를 정보수사기관에 제공하는 건수 역시 해마다 증가하는 추세에 있다. 통신수단별로 살펴보았을 때 이동전화 관련 통신사실 확인자료 제공건수가 압도적이다.

<표 3-33> 통신수단별 통신사실 확인자료 제공 건수

(단위: 문서수)

| | 유선전화 | 이동전화 | 무선호출 | PC통신・인터넷 | 합계 |
|---|---|---|---|---|---|
| 2000 | 19,295 | 61,232 | 67 | 1,818 | 82,412 |
| 2001 | 25,438 | 122,459 | 195 | 9,070 | 157,162 |
| 2002 | 15,350 | 87,974 | 0 | 19,217 | 122,541 |
| 2003 | 21,306 | 111,924 | 21 | 33,790 | 167,041 |
| 2004 | 23,403 | 108,759 | 3 | 44,665 | 176,830 |
| 2005 | 21,636 | 118,930 | 10 | 54,793 | 195,369 |
| 2006 | 21,948 | 87,114 | 0 | 41,681 | 150,743 |
| 2007 | 31,337 | 110,738 | 0 | 41,584 | 183,659 |
| 2008 | 37,912 | 128,166 | 0 | 46,667 | 212,745 |

통신사실 확인자료 제공 요청시 법원의 허가를 받도록 한 2005년 5월 「통신비밀보호법」 개정 이후 제공 건수가 잠시 줄어드는 경향을 보이기도

하였으나, 최근 다시 증가 추세로 돌아 섰다. 통신사실 확인자료 제공건수가 이처럼 증가하는 것은 현행 법률이 통신사실 확인자료 제공을 요청할 때 범죄사실의 입증 등 필요한 절차를 엄격히 규정하지 않은 데 따른 결과이다.

<표 3-34> 기관별 통신사실 확인자료 제공 건수

(단위: 전화번호 혹은 아이디 건수)

| | 검찰 | 경찰 | 국정원 | 군수사기관 | 합계 |
|---|---|---|---|---|---|
| 2000 | 28,378 | 138,474 | 12,351 | 35,691 | 214,894 |
| 2001 | 45,118 | 304,131 | 33,353 | 40,233 | 422,835 |
| 2002 | 33,532 | 250,530 | 18,232 | 41,033 | 343,327 |
| 2003 | 68,258 | 360,363 | 40,283 | 39,773 | 508,677 |
| 2004 | 100,103 | 563,433 | 35,568 | 29,057 | 728,161 |
| 2005 | 127,070 | 623,162 | 35,467 | 31,086 | 816,785 |
| 2006 | 124,089 | 429,539 | 12,499 | 39,399 | 605,526 |
| 2007 | 91,708 | 660,830 | 10,480 | 28,216 | 791,234 |
| 2008 | 113,636 | 305,570 | 4,048 | 23,646 | 446,900 |

통신사실 확인자료 제공 요청에 대한 법률상 요건과 절차가 엄격하게 규정되어 있지 않기 때문에 이에 대한 법원의 허가 기각률 또한 매우 낮다. 통신사실 확인자료 요청 시에 법원의 허가를 받도록 함으로써 그 오남용 소지를 줄이고자 했던 법률의 개정 취지가 무색하다 할 것이다.

<표 3-35> 통신사실 확인자료 청구 및 기각률

| | 청구 | 기각 | 기각률 |
|---|---|---|---|
| 2006년 | 60,357 | 557 | 0.9% |
| 2007년 | 66,651 | 585 | 0.9% |
| 2008년 8월 | 47,280 | 579 | 1.2% |

자료: 국회 국정감사 법원행정처(2008); 오길영(2008)에서 재인용.

또한, 새로운 기술이 개발돼 입법자가 예상하지 못한 상황이 발생하면서 「통신비밀보호법」의 편법 적용 논란이 일고 있다. 그 대표적인 사례가 현재 통신사실 확인자료로서 규정되어 있는 '위치추적자료'이다. 휴대전화 발신기지국의 위치추적자료는 현행 「통신비밀보호법」에서 통신사실 확인자료로

규정되어 있고(동법 제2조제11호바목), 수사기관들은 이 조항과 통신사실 확인자료 제공에 대한 다른 조항들을 통해 대상자의 휴대전화에 대한 위치추적을 해 왔다. 그런데 휴대전화 발신기지국에 대한 위치추적자료는 과거에 이루어진 통신사실에 대한 자료가 있는가 하면, 장래에 이루어질 통신에 대한 자료가 있다. 「통신비밀보호법」에서는 과거와 장래의 자료를 명확히 구분하고 있지는 않지만 동 법률이 통신사실 확인자료에 대한 규정을 신설할 당시에는 접수시점 이전의 자료에 한정되는 의미였다.[292] 그러나 휴대전화 이용자가 증가함에 따라 그에 따른 수사기관들의 위치추적에 대한 요구가 늘어났고, 구 정보통신부의 관련 지침이 개정되면서 장래 발신(착신) 전화번호 추적이 통신사실 확인자료에 포함되기 시작하였다.[293] 장래의 휴대전화 위치추적에 대한 통신사실 확인자료 제공 허가서가 발급되면, 이동통신사업자는 허가서에 적힌 사용기간 동안 통화가 발생하지 않더라도 매 10분 또는 30분 간격으로 단말기와 통신하는 기지국의 위치정보를 담당 수사관의 휴대전화 SMS 문자메시지로 실시간 발송하고 있다. 이에 통신사실 확인자료를 이용하여 휴대전화 실시간 위치추적을 한 건수가 2009년 상반기에만 9,647건에 이르며, 2년 반 동안 4만 건이 넘었다(변재일, 2009). 통신사실 확인자료에 대한 허가가 감청에 대한 허가보다 완화된 절차로 이루어지는 것은, 이 자료가 과거에 이루어진 통신사실에 대한 확인자료이기 때문에 그 통신의 비밀에 대한 침해가 장래의 통신의 비밀에 대한 침해보다 덜하기 때문이다. 현재처럼 장래의 위치정보에 대하여 과거의 통신사실 확인자료에 대한 조항을 적용하여 완화된 절차로 그 제공이 이루어지는 것은, 해당 조항을 신설할 당시의 취지와 목적을 위배하는 것이기 때문에 관련 규정의 보완이 시급하다.

### 3) 통신 감청

이메일 등 공개되지 않은 통신의 내용을 감청하는 건수는 문서별로 살펴보았을 때 2002년부터 감소하는 추세를 보이고 있다. 이는 2001년 12월 「통신비밀보호법」이 통신 감청 사실을 당사자에게 서면통지하도록 개정된 데 따른 것으로 보인다. 그러나 전화번호 혹은 아이디 건수별로 상세히 살펴보

292) 2001년 통신사실 확인자료 관련 조항 신설 시점의 '정보통신부 통신업무처리지침'에서는 통신사실 확인자료를 "자료제공요청서 접수시점 이전의 자료에 한정"한다고 명시하고 있으며, 국회 소관 상임위원회 검토과정에서도 이를 인용하였다. 과학기술정보통신위원회 수석전문위원. 2001.2. 위 검토보고. p.6 참조.

293) 통신비밀 보호업무 처리지침(안). 2005.11. "통신사실확인자료제공업무 처리지침". p.29.

면 유독 국가정보원의 감청 건수가 압도적으로 증가해 왔다는 사실을 알 수 있다.

<표 3-36> 통신수단별 통신 감청 건수

(단위: 문서수)

| | 유선전화 | 이동전화 | 무선호출 | PC통신·인터넷 | 합계 |
|---|---|---|---|---|---|
| 2000 | 1,931 | 217 | 8 | 224 | 2,380 |
| 2001 | 2,107 | 366 | 1 | 410 | 2,884 |
| 2002 | 1,013 | 169 | 0 | 346 | 1,528 |
| 2003 | 1,097 | 216 | 0 | 383 | 1,696 |
| 2004 | 887 | 265 | 0 | 461 | 1,613 |
| 2005 | 621 | 1 | 0 | 355 | 977 |
| 2006 | 577 | 0 | 0 | 456 | 1,033 |
| 2007 | 503 | 0 | 0 | 646 | 1,149 |
| 2008 | 506 | 0 | 0 | 646 | 1,152 |

기관별로 살펴보면, 국가정보원의 감청 비율이 압도적으로 높다.

<표 3-37> 기관별 통신 감청 건수

(단위: 전화번호 혹은 아이디 건수)

| | 검찰 | 경찰 | 국정원 | 군수사기관 | 합계 |
|---|---|---|---|---|---|
| 2000 | 386 | 1,320 | 1,575 | 261 | 3,542 |
| 2001 | 362 | 1,289 | 2,412 | 308 | 4,371 |
| 2002 | 208 | 627 | 2,234 | 187 | 3,256 |
| 2003 | 165 | 648 | 5,424 | 203 | 6,440 |
| 2004 | 106 | 554 | 8,201 | 289 | 9,150 |
| 2005 | 100 | 241 | 8,082 | 112 | 8,535 |
| 2006 | 43 | 131 | 8,440 | 51 | 8,665 |
| 2007 | 41 | 95 | 8,628 | 39 | 8,803 |
| 2008 | 24 | 94 | 8,867 | 19 | 9,004 |

국가정보원의 감청 비율이 높은 것은 현행 법률상 정보수사기관의 감청에 대한 감독이 충분하지 못하기 때문이다. 통신 감청에 대한 감독이 부실한 것은 통신 감청이 보충적으로 이루어져야 한다는 현행 법률상의 원칙을 형해화하는 것이나 마찬가지이다. 실제로 국가정보원은 그 전신인 국가안전기획부 당시부터 직접 개발한 휴대전화 감청장비를 동원하여 방대한 규모로 불법적인 감청을 해왔음이 2005년 드러나 사회적으로 큰 충격을 주었다. 일반 범죄 수사와 관련이 없는 정보수사기관이 불법 감청을 실시하는 것은 정치적인 반대자들을 감시하고 억압하는 목적으로 사용될 수 있다는 점에서 매우 심각한 문제이다. 그러나 이 사건 이후로 현재까지 「통신비밀보호법」의 관련 조항들은 개선된 바가 없다. 탈법적이거나 불법적인 감청 문제가 또다시 불거질 수 있는 소지가 잠복해 있는 것이다.

현재 모든 감청이 법원의 영장 하에 적법하게 이루어지고 있다 하더라도 그 감독이 부실한 것은 사실이다. 영장 심사 과정을 통해 통신 감청의 실태를 감독해야 할 법원이 그 기능을 다하지 못하고 있기 때문이다.[294] 법원의 영장 기각률은 3%대에 그치고 있다. 이로 인하여 통신 감청에 대한 법원의 통제가 사문화된 상황이라는 비판이 제기되고 있다(오길영, 2008).

<표 3-38> 통신감청 영장 청구 및 기각률

| | 청구 | 기각 | 기각률 |
|---|---|---|---|
| 2003년 | 347 | 10 | 2.9% |
| 2004년 | 193 | 2 | 1.0% |
| 2005년 | 73 | 1 | 1.4% |
| 2006년 | 107 | 3 | 2.8% |
| 2007년 | 112 | 4 | 3.6% |
| 2008년 6월 | 35 | 1 | 2.9% |

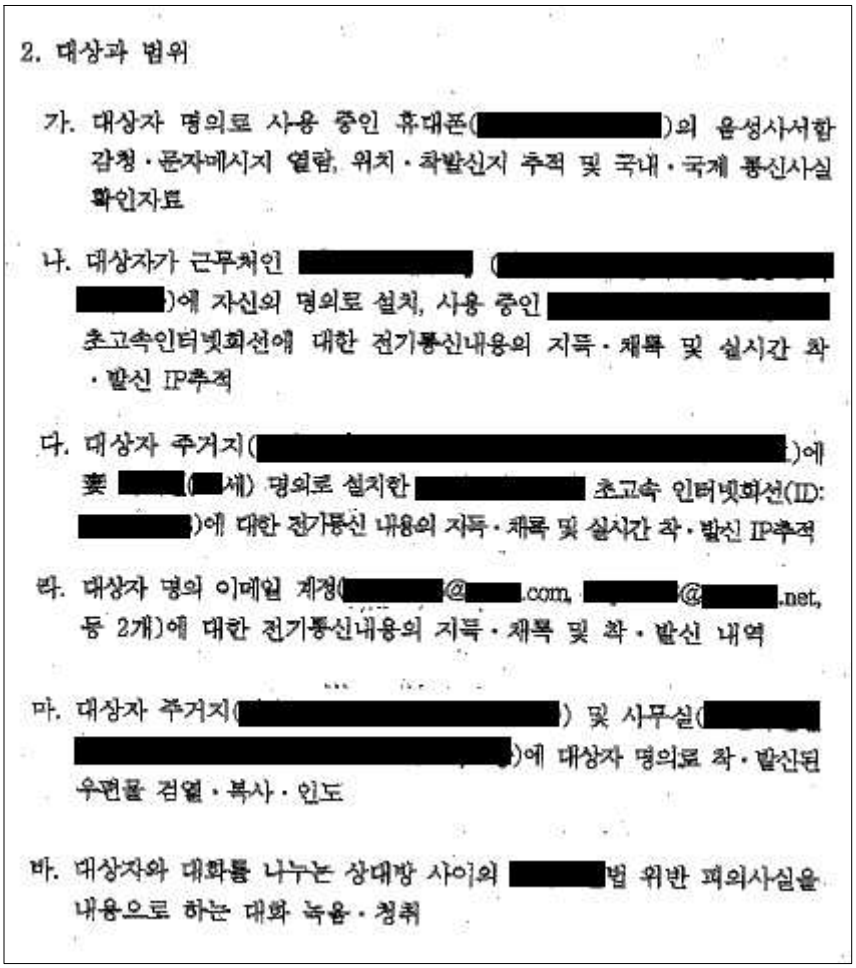
자료: 국회 국정감사 법원행정처(2008); 오길영(2008)에서 재인용.

실제 법원이 허가서 한 장으로 우편물 검열, 유선전화·휴대전화·인터넷 메일에 대한 감청은 물론 인터넷 회선 전체와 대화에 대한 감청까지 한번에 실시하는 저인망식 감청을 허용해 왔다는 사실이 드러났다(<그림 3-11>).

294) 한겨레21 보도에 따르면, 최초 발부된 감청 영장이 2개월씩 무려 14차례 연장되어 총 28개월간 감청이 이루어진 사례도 있었다. 한겨레21. 2009.9.4. “인터넷·전자우편 실시간 감청 시대”. 제776호.

또한 현행 「통신비밀보호법」에는 영장주의의 예외가 존재한다. 먼저 정보수사기관이 외국인을 감청할 때는 법원의 허가가 아닌 대통령 승인만으로 가능하도록 규정하였다(동법 제7조제1항). 또한 "국가안보를 위협하는 음모행위, 직접적인 사망이나 심각한 상해의 위험을 야기할 수 있는 범죄 또는 조직범죄등 중대한 범죄의 계획이나 실행 등 긴박한 상황에 있고 … 규정에 의한 절차를 거칠 수 없는 긴급한 사유가 있는 때"에는 법원의 허가 없이 통신제한조치, 즉 감청을 할 수 있다(동법 제8조제1항). 이러한 규정들은 영장주의를 우회할 수 있는 방법을 제공함으로써 편법적이거나 불법적인 통신 감청으로 이어질 수 있다는 우려를 낳고 있다.

<그림 3-11> 감청 허가서 (일부 예시)



2. 대상과 범위

가. 대상자 명의로 사용 중인 휴대폰([redacted])의 음성사서함 감청·문자메시지 열람, 위치·착발신지 추적 및 국내·국제 통신사실 확인자료

나. 대상자가 근무처인 [redacted] ([redacted])에 자신의 명의로 설치, 사용 중인 [redacted] 초고속인터넷회선에 대한 전기통신내용의 지득·채록 및 실시간 착·발신 IP추적

다. 대상자 주거지([redacted])에 妻 [redacted]([redacted]세) 명의로 설치한 [redacted] 초고속 인터넷회선(ID: [redacted])에 대한 전기통신 내용의 지득·채록 및 실시간 착·발신 IP추적

라. 대상자 명의 이메일 계정([redacted]@[redacted].com, [redacted]@[redacted].net, 등 2개)에 대한 전기통신내용의 지득·채록 및 착·발신 내역

마. 대상자 주거지([redacted]) 및 사무실([redacted])에 대상자 명의로 착·발신된 우편물 검열·복사·인도

바. 대상자와 대화를 나누는 상대방 사이의 [redacted]법 위반 피의사실을 내용으로 하는 대화 녹음·청취

더불어, 현행 법률이 법원의 영장 발부 후에는 사후 감독에 대한 규정을 전혀 명시하지 않고 감청 집행과 그 자료에 대한 사항을 감청을 집행하는 정보수사기관의 재량에 전적으로 맡기고 있는 점도 문제이다. 감청 집행 시 법원 등에서 입회를 하여 실제 감청이 발부된 영장대로 집행되도록 감독하고 감청 결과는 봉인하여 법원에서 관리하고 필요시 당사자 등이 청구하여 열람할 수 있도록 보장하는 방안이 강구될 필요가 있다.

한편, 인터넷 회선을 오가는 신호 전체에 대한 패킷 감청은 그 사생활 침해 정도가 매우 심각하다(<그림 3-11>의 '나'항과 '다'항). 인터넷을 통한 정보전달은 각각의 파일을 패킷(packet)이라는 단위로 잘게 쪼개어 송신한 뒤 이를 받아보는 컴퓨터가 해당 패킷을 재구성해 화면에 다시 구현하는 형태로 이루어진다. 패킷 감청이란 이용자가 인터넷을 이용하는 과정에서 인터넷 회선을 통해 전기신호 형태로 흐르는 패킷을 제3자가 실시간으로 가로챔으로써 같은 내용을 들여다보는 것이다. 따라서 패킷 감청을 이용하면 대상자가 인터넷을 통해 접속한 사이트 주소와 접속시간, 대상자가 입력하는 검색어, 전송하거나 수신한 게시물이나 파일의 내용을 모두 볼 수 있다. 이메일과 메신저의 발송 및 수신내역과 그 내용 등 통신내용 일체도 마찬가지로 볼 수 있다.

패킷의 내용을 검사하는 기술은 인터넷 초창기서부터 발달해왔다. 전통적인 패킷 검사들은 패킷 라우팅을 최적화하거나, 네트워크 남용을 탐지하거나, 통계 분석을 하는 등의 이유에서 이루어져 왔다. 이러한 패킷 검사들은 검사자에게 인터넷 트래픽에 대한 기초적인 정보를 제공하지만, 이용자의 이메일이나 웹서핑 내용을 보여주진 않는다. 반면 최근의 패킷 감청은 이용자가 보내고 받는 모든 비암호화된 인터넷 트래픽의 '내용'에 접근할 수 있도록 한다. 인터넷 초창기에는 컴퓨터 속도와 자원의 한계 때문에 규모가 큰 패킷 감청은 효과적으로 이루어질 수 없었다. 최근의 기술적 진보로 인하여 ISP와 정보수사기관들이 큰 규모로 패킷 감청을 하는 것이 가능해진 것이다.[295]

패킷 감청이 과연 현행 법률은 물론 기술적인 측면에서 허용될 수 있는지를 두고 최근 전세계적인 논쟁이 일고 있다. 특히 미국과 영국 등 다른 나라에서는 광고서비스업체들이 패킷 감청을 이용하여 이용자의 통신 내용을 실시간으로 보고 그에 맞춘 광고를 내보내는 소위 '관심기반 광고' 방법을 도입하는 것을 두고 정부와 의회에서 토론이 계속되고 있다.[296]

---

295) EPIC의 다음 자료 참고. http://epic.org/privacy/dpi/.

296) 영국에서는 2008년 BT가 광고서비스를 위하여 폼사의 패킷감청기술을 도입한 문제

한국에서는 남북공동선언실천연대 사건에 대한 재판과정에서 국가정보원이 패킷 감청을 실시한 사실이 드러났고, 지난 8월 31일 인권단체들이 이를 비판하는 기자회견을 개최함으로써 패킷 감청 문제가 처음 알려졌다.[297] 2009년 정기국회에서는 관련 법률의 보완이 이루어져야 한다는 지적이 여럿 이어졌다.

패킷 감청의 가장 큰 문제점은 감청 대상을 특정화하기 쉽지 않다는 점이다. 첫째, 보통의 가정이나 직장에서는 공유기 등을 통해 다수의 PC와 다수인이 해당 네트워크 서비스를 공동이용한다. 대상자의 PC를 임시적으로 다른 이가 사용할 수도 있다. 따라서 현재의 패킷 감청은 감청 대상자가 아닌 타인의 인터넷 통신 내용을 감청하게 되는 경우가 다수 있을 것이다. 그러나 외부에서 감청을 집행하는 입장에서는 지금 전송되는 패킷이 감청 대상자의 행위에 의해 송수신되는 것인지 알 수 없다. 따라서 감청 대상자를 특정할 수 없는 패킷 감청은 각 피의자별로 감청이 이루어지도록 한 현행 「통신비밀보호법」에 위배되고(동법 제6조제1항), 법정 증거로서의 효력도 없다. 둘째, 패킷 감청의 경우 특정 이메일이나 메신저에 대한 감청과 달리 서버로부터 대상자에게 전달되는 모든 통신내용을 대상으로 한다. 이 가운데에는 공개된 통신내용도 있을 수 있지만 비공개 통신내용도 있을 수 있는데, 비공개 통신내용은 단지 대상자가 이용하였다는 이유만으로 정보수사기관에게 제공된다. 이 과정에서 이용자의 비밀번호 등이 제공될 가능성도 있는데, 이는 감청을 집행하는 과정에서 비밀번호가 누설되어서는 안된다는 「통신비밀보호법」의 취지에 위배된다(동법 제9조제4호). 결국 패킷감청은 감청대상자와 무관한 제3자를 감청하는 결과를 낳을 수 있으며, 수사목적과 무관한 통신내

---

에 대하여 관련 업계, 정부와 시민단체 간에 많은 논쟁이 벌어졌으며, 이 문제로 EU에서 조사를 하고 있다. The Register. 2008.2.29. “How Phorm plans to tap your internet connection”; The NewYork Times. 2009.7.6. “BT Backs Off From Tracking Internet Customers”; The Guardian. 2009.10.30. “EU goes to next stage in privacy action against Britain” 참조, 미국에서는 역시 광고서비스를 위하여 초고속 인터넷서비스업체인 차터 커뮤니케이션에서 네뷰애드사의 패킷감청기술을 도입한 문제에 대하여, 2008년 7월 17일 하원 에너지 및 통상위원회 산하 통신 및 인터넷 소위원회에서 청문회가 개최되었다. http://energycommerce.house.gov/index.php?Itemid=58&catid=32&id=1400&layout=default&option=com_content&view=article&date=2009-11-01. 캐나다 프라이버시위원회에서는 패킷 감청에 대한 특집 사이트를 운영하고 있다. http://dpi.priv.gc.ca/.

297) 아이뉴스24. 2009.8.31. “국정원 인터넷회선 패킷 감청 의혹제기”; 오마이뉴스. 2009.8.31. “국정원, 인터넷 사용내역도 엿봤다”; 한겨레신문. 2009.8.31. “국정원, 우리집 인터넷 통째로 엿봤다”; 서울신문. 2009.9.1. “국정원, 인터넷회선 통째 감청 의혹” 등.

용까지 무제한적으로 포괄감청한다는 것이 가장 큰 문제점이다(오길영, 2009).

우리 「통신비밀보호법」 제3조제2항은 전기통신의 감청이 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다는 점을 명시하고 있다. 동법 제5조제1항에서도 감청은 대상 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 허가하도록 명시하였다. 패킷 감청은 그 범위가 너무 광범위하여 대상자와 대상 통신내용을 특정할 수 없다는 점에서 우리 「통신비밀보호법」이 허용하는 감청의 범위를 벗어난 위법한 감청이다(박영선, 2009). 더구나 패킷이란 목적을 가지고 이동하는 통신 과정상의 자료로서 수사에 필요한 자료는 해당 패킷이 목적지에 도달한 후 기존의 이메일 전달(forwarding) 방식의 감청이나 압수·수색으로도 충분히 입수가능하다. 여러모로 통신비밀보호법에 규정된 감청 방식으로 부적합한 패킷 감청이 굳이 인정될 필요가 없는 것이다. 결론적으로 통신 감청이 최소한으로, 보충적으로 이루어져야 한다는 「통신비밀보호법」의 제정 취지대로라면 현재와 같은 형태의 인터넷 회선 감청은 재고되어야 할 필요가 있다.

#### 4) 송·수신이 완료된 전기통신에 대한 압수·수색·검증

2009년 5월 수사기관이 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 당사자에게 통지하도록 하는 규정이 「통신비밀보호법」에 신설되었으나(동법 제9조의3), 압수·수색·검증의 집행 실태는 알려져 있지 않다. 다만 2008년 국정감사에서 상위 두 개 포털업체로부터 제출받은 자료에 따르면 해당년도 상반기에 두 개 업체의 메일에 대한 압수수색이 3,360건에 달했다고 한다(박영선, 2008). 2009년 국정감사 자료에 따르면 법무부는 압수수색검증 대비 통지 건수와 비율 산출을 위한 별도의 검찰 시스템을 개발 중이며, 현재는 통계산출이 불가능하다고 밝혔다.

### 3. 정보주체의 열람 및 통지에 대한 권리 보장 실태

「통신비밀보호법」은 2001년 12월 개정된 후로부터 통신제한조치, 즉 감청의 대상이 된 자의 알권리를 위하여 감청의 집행에 관한 통지제도를 두고

있다. 또한 2005년 5월 개정된 후에는 통신사실 확인자료 제공 요청의 당사자에게도 그 집행에 관한 통지제도를 두었다. 2009년 5월부터는 송수신이 완료된 통신에 대해서도 그 압수·수색·검증의 대상자에게 통지하도록 하였다.

「통신비밀보호법」
제9조의2 (통신제한조치의 집행에 관한 통지) ①검사는 제6조제1항 및 제8조제1항의 규정에 의한 통신제한조치를 집행한 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지 결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 우편물 검열의 경우에는 그 대상자에게, 감청의 경우에는 그 대상이 된 전기통신의 가입자에게 통신제한조치를 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 한다.
②사법경찰관은 제6조제1항 및 제8조제1항의 규정에 의한 통신제한조치를 집행한 사건에 관하여 검사로부터 공소를 제기하거나 제기하지 아니하는 처분(기소중지 결정을 제외한다)의 통보를 받거나 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그 날부터 30일 이내에 우편물 검열의 경우에는 그 대상자에게, 감청의 경우에는 그 대상이 된 전기통신의 가입자에게 통신제한조치를 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 한다.
③정보수사기관의 장은 제7조제1항제1호 본문 및 제8조제1항의 규정에 의한 통신제한조치를 종료한 날부터 30일 이내에 우편물 검열의 경우에는 그 대상자에게, 감청의 경우에는 그 대상이 된 전기통신의 가입자에게 통신제한조치를 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 한다.
④제1항 내지 제3항의 규정에 불구하고 다음 각호의 1에 해당하는 사유가 있는 때에는 그 사유가 해소될 때까지 통지를 유예할 수 있다.
1. 통신제한조치를 통지할 경우 국가의 안전보장·공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때
2. 통신제한조치를 통지할 경우 사람의 생명·신체에 중대한 위험을 초래할 염려가 현저한 때
⑤검사 또는 사법경찰관은 제4항의 규정에 의하여 통지를 유예하고자 하는 경우에는 소명자료를 첨부하여 미리 관할지방검찰청검사장의 승인을 얻어야 한다. 다만, 검찰관 및 군사법경찰관이 제4항의 규정에 의하여 통지를 유예하고자 하는 경우에는 소명자료를 첨부하여 미리 관할 보통검찰부장의 승인을 얻어야 한다.
⑥검사, 사법경찰관 또는 정보수사기관의 장은 제4항 각호의 사유가 해소된 때에는 그 사유가 해소된 날부터 30일 이내에 제1항 내지 제3항의 규정에 의한 통지를 하여야 한다.
[본조신설 2001.12.29]
제9조의3 (압수·수색·검증의 집행에 관한 통지) ① 검사는 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 공

소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 한다.
② 사법경찰관은 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 그 사건에 관하여 검사로부터 공소를 제기하거나 제기하지 아니하는 처분의 통보를 받거나 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그 날부터 30일 이내에 수사대상이 된 가입자에게 압수·수색·검증을 집행한 사실을 서면으로 통지하여야 한다.
[본조신설 2009.5.28]
제13조의3 (범죄수사를 위한 통신사실 확인자료제공의 통지) ①제13조의 규정에 의하여 통신사실 확인자료제공을 받은 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한 날부터 30일 이내에 통신사실 확인자료제공을 받은 사실과 제공요청기관 및 그 기간 등을 서면으로 통지하여야 한다.
②제1항에 규정된 사항 외에 통신사실 확인자료제공을 받은 사실 등에 관하여는 제9조의2(동조제3항을 제외한다)의 규정을 준용한다.
[본조신설 2005.5.26]

그러나 이러한 통지제도가 그 취지대로 정보주체의 권리를 보장하고 있는지는 미지수이다.

<표 3-39> 통신제한조치 통지 건수와 통지유예 건수 (검찰)

(단위: 건)

| 연도별 | 구분 | 합계(건) | 비율(%) |
|---|---|---|---|
| 2007 | 발부 | 17 | 100.0 |
| | 검사(통지) | 18 | 105.9 |
| | 통지유예 | 2 | 11.8 |
| 2008 | 발부 | 6 | 100.0 |
| | 검사(통지) | 11 | 183.3 |
| | 통지유예 | 0 | 0.0 |
| 2009 (1~8월) | 발부 | 6 | 100.0 |
| | 검사(통지) | 6 | 100.0 |
| | 통지유예 | 0 | 0.0 |

자료: 법무부. 2009 국정감사 자료.
※ 통지대상자는 통신제한조치의 대상인 피의자 혹은 내사자가 아닌 전기통신의 가입자에 대해 이루어지므로, 청구건수보다 통지 건수가 더 많을 수 있음.[298)]

감청에 대한 통지 관련 규정이 신설된 후 2004년 국정감사에서 노회찬 의원은 검찰이 통신 감청 결과를 당사자에게 통지하는 비율이 30%에도 미치지 못한다고 지적하였다.[299]

2009년 국정감사에서 법무부는 통신 감청에 대한 통지 비율이 100% 이상 이루어지고 있다고 답변하였다(<표 3-39>). 그러나 감청의 대부분을 집행하는 정보수사기관의 통지 건수는 알려져 있지 않다.

<그림 3-12> 감청에 대한 통지서 (일부 예시)

제목 통신제한조치 집행사실 통지

[redacted]법위반 [redacted] 피의사건과 관련하여 아래와 같은 내용의 통신제한조치를 집행하였으므로 통신비밀보호법 제9조의2 제2항의 규정에 따라 이를 통지합니다.

| | |
|---|---|
| 허가서번호 | 2009[redacted]지방법원) |
| 통신제한조치집행기관 | [redacted] |
| 전기통신의 가입자 | [redacted] |
| 통신제한조치의 대상과 범위 | o [redacted]에서 사용중인 [redacted] 인터넷 전용회선 및 인터넷전화[redacted], [redacted]에 대한 전기통신의 감청 및 출력·인도, 착·발신지 (IP로그기록) 추적 |
| 통신제한조치의 종류와 기간 | o 종류 : 【 전기통신 감청 】<br>o 기간 : 2009.[redacted] |

298) 통신제한조치 건수에 대한 법무부의 통계는 경찰과 검찰이 통신제한조치 허가를 청구한 문서에 따른 통계이므로, 사업자별로 이루어진 집행결과가 추산된 앞서 (구)정보통신부/방송통신위원회의 통계와 차이가 있음. 통신사실 확인자료 요청 건수에 대한 법무부 통계도 이하 같음.

299) 오마이뉴스. 2004.10.20. ""검찰, 감청 뒤 통지하지 않아"..."규정위반한 적 없다"".

법률에서는 국가의 안전보장·공공의 안녕질서를 위태롭게 할 현저한 우려가 있는 때 통지를 유예할 수 있도록 하였다(동법 제9조의2 제4항). 즉, 국가안보를 이유로 이루어지는 정부수사기관의 감청이 전체 감청 건수의 대부분을 차지하는 상황에서, 그 통지마저 국가의 안보라는 이유로 유예되는 것이다. 결국 전체 감청 대상자 가운데 실제 감청의 집행 통지를 받는 경우는 극히 미미한 것으로 추정된다. 또한 검사와 사법경찰관이 통지를 유예하고자 하는 경우 소명자료를 첨부하여 관할지방검찰청 검사장의 승인(제4항의 규정에 의하는 경우 관할 보통검찰부장의 승인)을 얻도록 한 데 비해(동법 제9조의2 제5항), 정보수사기관은 통지유예에 대한 감독 규정을 두고 있지 않다.

통신사실 확인자료에 대한 통지 역시 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 날부터 30일 이내에 통신사실 확인자료제공을 받은 사실과 제공요청기관 및 그 기간 등을 서면으로 통지하여야 하지만(동법 제13조의3), 감청의 경우와 마찬가지로 통지 유예가 인정되어 왔다.

<표 3-40> 통신사실 확인자료요청 통지 건수와 통지유예 건수 (검찰)

(단위: 건)

| 연도별 | 구분 | 합계(건) | 비율(%) |
|---|---|---|---|
| 2007 | 발부 | 8,616 | 100.0 |
| | 검사(통지) | 9,394 | 109.0 |
| | 통지유예 | 5 | 0.1 |
| 2008 | 발부 | 10,634 | 100.0 |
| | 검사(통지) | 13,665 | 128.5 |
| | 통지유예 | 57 | 0.5 |
| 2009 (1~8월) | 발부 | 7,147 | 100.0 |
| | 검사(통지) | 10.587 | 148.1 |
| | 통지유예 | 317 | 4.4 |

※ 통지대상자는 통신제한조치의 대상인 피의자 혹은 내사자가 아닌 전기통신의 가입자에 대해 이루어지므로, 청구건수보다 통지 건수가 더 많을 수 있음.

그러나 통신사실 확인자료는 통신을 이용한 과거 사실에 대한 확인 자료로서 범죄가 발생했을 경우 그것을 입증하기 위한 용도로 제공되는 것이다. 자신의 통신 기록이 수사기관에 제공되었다는 사실에 대하여 당사자가 알게 된다고 하여 실제 수사에 방해가 될 것인지 의문이다. 따라서 통신사실 확인자

료의 통지가 수사기관의 수사 진행 여부에 따라 지연되거나 유예될 것이 아니라, 그 제공이 이루어진 즉시 이루어지는 것이 마땅하다. 그 통지 주체 역시 제공을 허가한 법원으로 하여금 통지하도록 하는 것이 바람직할 것이다.

통신사실 확인자료의 구체적인 통지 실태에 대하여 법무부는 통지 비율이 100% 이상 이루어지고 있다고 답변하였지만(<표 3-40>), 정보수사기관을 비롯하여 다른 기관에 의한 통지 건수는 알려져 있지 않다.

실제 수사기관의 통지서를 검토해 보면, 요청 기관과 방식, 기간 등만 적혀 있을 뿐, 구체적인 혐의와 사유를 알려주지 않는다(<그림 3-13> 참조). 그러나 현행 통신비밀보호법의 입법 취지를 볼 때 본인에게 최대한 자세하게 통신사실 확인자료의 제공 사유를 통지해야 한다는 지적이 있다.[300]

<그림 3-13> 통신사실 확인자료 제공에 대한 통지서 (일부 예시)

| 제 목 | 통신사실 확인자료제공 요청 집행사건 처리결과통보 | | |
|---|---|---|---|
| 귀서에서 통신사실 확인자료제공 요청을 집행한 후 송치한 당청 제 2009 형제 [redacted] 피의사건의 처리결과를 아래와 같이 통보합니다. | | | |
| ① 허가서번호 | 서울중앙지방법원 2009 - [redacted] | ② 청구부 진행번호 | 2009 - [redacted] |
| ③통신사실 확인자료 제공 요청 기관 | 서울[redacted]경찰서 | ④ 처리자 소속,계급,성명 | [redacted] |
| ⑤ 전기통신가입자 (통지대상자) | [redacted] | | |
| ⑥ 전기통신사업자 | | | |
| ⑦통신사실 확인자료 제공 요청의 대상과 종류 | 010[redacted] | 발신기지국위치추적 | |
| ⑧통신사실 확인자료 제공 요청의 기간 | 2009.[redacted] ~ 2009.[redacted] | | |

300) 한겨레신문. 2009.1.15. “경찰 ‘묻지마 감청’ /사후통보도 시늉만.”

통신사실 확인자료에 대한 통지가 수사기관의 수사 진행 여부에 따라 지연되거나 유예되는 일이 생기면서 정보주체가 자신의 통신사실 확인자료의 제공 여부를 통신사업자에게 문의하는 경우가 있다. 여기서 오래도록 논란이 되고 있는 문제는 통신사업자가 통신사실 확인자료 제공 내역을 이용자에게 공개하지 않는다는 것이다.[301] 자신의 통화내역 등 통신사실 확인자료가 수사기관에게 제공된 바를 확인 및 열람케 해달라는 정보주체의 요구에 대하여, 통신사업자들은 수사에 방해가 될 수 있고 관련 규정이 명확하지 않다는 이유에서 줄곧 그 공개를 거부해 왔다. 본 연구의 목적을 위하여 통신사업자에 대해 열람 청구권을 행사하여 본 결과에서도 수사기관에 제공된 사실에 대해서는 그 열람이 제한되었다(제2장 제3절 참조). 법원에서도 현행 「통신비밀보호법」에는 당사자가 검찰이 조회한 통신기록을 열람할 수 있는 근거 규정이 없다면서 수사기관이 조회한 통화기록을 본인에게 공개할 수 없다는 판결을 내렸다.[302]

그러나 구체적인 규정이 없다는 이유로 자신의 개인정보에 대한 제3자 제공 현황을 열람할 수 없다는 것은 정보주체의 열람 및 정정·삭제 청구권에 대한 중대한 제약이다. 결국 현 실태는 법률의 제정 취지와 다르게 당사자의 알 권리가 어느 곳에서도 보장받고 있지 못한 것이다.

「전기통신사업법」상 통신자료 제공에 대해서는 아예 당사자에 대한 통지 제도를 두고 있지 않다. 통신사업자에게 요청하여도 정보주체에게 그 사실에 대한 공개를 하지 않는 것이 현실이고, 2009년 국정감사에서는 정보주체 역시 열람권을 행사하는 경우가 적은 것으로 드러났다(김창수, 2009). 결국 자신의 통신자료가 수사기관에게 제공된 내역을 열람할 수 있는 정보주체의 권리가 사실상 형해화하고 있는 것은 아닌지 우려스럽다 할 것이다.

<표 3-41> 주요포털사 정보주체 열람권 행사 현황

| | A사 | B사 | C사 | D사 | E사 |
|---|---|---|---|---|---|
| 요청건수 | 1 | 2 | 1 | 1 | 2 |
| 발급건수 | 1 | 2 | 1 | 1 | 2 |

자료: 김창수(2009).

301) YTN. 2003.10.21. “통화내역 조회 거부…인권침해.”

302) “서울중앙지법 민사합의18부(부장판사 이병로)는 김모씨가 SK텔레콤을 상대로 낸 열람·등사 청구 소송에서 원고 패소 판결을 내렸다고 18일 밝혔다.” 국민일보. 2009.10.18. “수사기관 ‘통화조회’ 본인도 열람 안돼.”

2008년 12월 11일 최문순 의원이 대표발의한 「통신비밀보호법 일부개정법률안(의안번호 제1802973호)」에서는 통신자료제공을 받은 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분을 한 날로부터 30일 이내에, 정보수사기관의 장은 통신자료제공을 받은 날로부터 30일 이내에 그 대상이 된 전기통신의 가입자에게 통신자료 제공을 받은 사실을 통지하도록 하였다. 이 개정안은 통신자료의 제공에 있어서도 통지제도를 둔 점에서 진일보한 측면이 있으나, 정보주체에게 자신에 대한 인적 사항인 통신자료가 수사기관에 제공되었다는 사실을 즉시 알린다고 하여 수사의 기밀성이 훼손되지 않는다. 따라서 개정안에서 나아가 그 제공 사실을 즉시 통지하도록 하는 것이 바람직할 것이다.

한편, 현행 「통신비밀보호법」에서는 송·수신이 완료된 전기통신에 대하여 압수·수색·검증을 집행한 경우 당사자에게 통지하도록 하였으나(동법 제9조의3), 사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 날부터 30일 이내에 통지하도록 하였다. 하지만 「형사소송법」에서는 일반 증거물에 대한 압수·수색의 경우 그 영장이 집행될 때 영장을 처분을 받는 자에게 제시하도록 하였고(동법 제118조) 영장 집행에 있어 피고인의 참여권을 인정하고 있으며(동법 제121조) 미리 집행의 일시와 장소를 당사자에 통지하도록 하였다(동법 제122조). 다만 통신의 경우 집행의 편의상 영장을 제시받고 참여하는 것이 해당 정보주체가 아니라 통신사업자로 인정되어 왔을 따름이다. 「형사소송법」의 취지대로라면 당사자인 정보주체에게는 사후적인 통지에서 더 나아가 압수·수색 영장이 집행되는 시점에 즉시 그 집행 사실에 대한 통지와 참여권이 보장될 수 있도록 관련 규정이 개선되는 것이 마땅하다.

## 4. 소결

「통신비밀보호법」과 「전기통신사업법」 등 국가안보 및 범죄수사 등의 목적으로 통신의 비밀을 제한하는 현행 법률들은 통신 및 대화의 비밀과 자유에 대한 제한에 있어 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다. 그러나 그 실제 집행 실태를 검토하여 보면, 이 목적에 맞게 현행 법률이 정비되어 있고 그에 따른 집행이 이루어지고 있는지 의구심이 들지 않을 수가 없다.

먼저 「전기통신사업법」에 의해 가입자 성명, 전화번호, 주민등록번호, 주

소, 인터넷 아이디 등 이용자 인적사항에 대한 통신자료가 수사기관 등에 제공되는 건수는 해마다 급증하여 한해 제공건수 5백만 건을 넘어섰다. 통신자료 제공건수가 이처럼 높은 것은 현행 법률이 통신자료 제공을 요청할 때 필요한 절차를 엄격히 규정하지 않은데 따른 결과로서 오남용 논란이 끊이지 않고 있다.

통화내역, 위치정보, 인터넷 IP주소 등 통신사실 확인자료를 정보수사기관에 제공하는 건수 역시 해마다 증가하는 추세에 있다. 이 역시 현행 법률이 통신사실 확인자료 제공을 요청할 때 범죄사실의 입증 등 필요한 절차를 엄격히 규정하지 않은 데 따른 결과이다. 특히 장래의 위치정보에 대하여 과거의 통신사실 확인자료에 대한 조항을 적용하여 완화된 절차로 그 제공이 이루어지는 것은, 통신사실 확인자료를 과거의 통신사실에 대한 자료로서 규정하였던 법률 개정 취지와 목적을 위배하는 것이다.

이메일 등 공개되지 않은 통신의 내용에 대한 감청은 대부분 국가정보원에 의해 집행되고 있었다. 이는 법원의 영장 심사 등 정보수사기관에 대한 감독이 제대로 이루어지지 못한 데 따른 것으로서, 허가서 한 장으로 우편물 검열과, 유선전화·휴대전화·인터넷 메일에 대한 감청은 물론 인터넷 회선 전체와 대화에 대한 감청까지 한번에 모두 실시하는 저인망식 감청이 이루어지고 있었다. 또한 현행 법률이 영장주의의 예외를 인정함으로써 편법·불법 감청으로 이어질 수 있다는 우려를 낳고 있고, 반면 영장 발부 후 감청을 실제 집행하는 과정에서는 아무런 사후 감독 규정을 두고 있지 않은 점은 큰 문제이다. 더불어 인터넷 회선을 오가는 신호 전체에 대한 패킷 감청은 그 사생활 침해 정도가 매우 심각하고, 대상자와 대상 통신내용을 특정할 수 없다는 점에서 재고되어야 할 필요가 있다.

한편 「통신비밀보호법」은 대상자의 알권리를 위하여 감청과 통신사실 확인자료 제공 및 송수신이 완료된 통신에 대한 압수·수색·검증의 대상자에게 그 집행을 통지하는 제도를 규정하고 있다. 그러나 수사기관의 수사 진행 여부에 따라 이러한 통지가 지연되거나 유예되고 있고, 「전기통신사업법」에 따른 통신자료의 경우에는 통지에 대한 규정 자체가 없기 때문에 실제 통지에 대한 권리는 충분히 보장되고 있지 않다.

# 제4장 설문조사 결과 분석

개인정보 수집·유통의 구체적인 실태를 파악하기 위해 일반 시민과 개인정보보호 책임자를 대상으로 설문조사를 실시하였다. 일반 시민 대상 설문조사는 개인정보 수집·유통 실태와 개인정보 열람 및 정정·삭제 청구권 보장 실태에 관한 시민의식을 측정하기 위해 전화면접조사를 하였으며, 개인정보보호 책임자 대상 설문조사는 공공 및 민간의 주요 기관에서의 개인정보 수집·유통 현황을 조사·분석하기 위해 각 기관에서 개인정보 수집·유통 실태를 가장 잘 알고 있고, 가장 많이 다루고 있는 공공기관 및 민간기업의 개인정보보호 책임자들을 대상으로 온라인 설문을 하였다.

## 제1절 일반 시민 대상 설문조사 결과 분석

### 1. 조사 개요

여기서는 자신들의 개인정보가 수집되고 유통되는 시민들을 대상으로 부록에 첨부된 설문조사를 통해 개인정보 수집·유통 실태와 개인정보 열람 및 정정·삭제 청구권 보장 실태에 관한 시민의식을 측정하여 우리나라 개인정보 보호와 권리에 관한 법제도 현황과 그 보장 등 실태분석을 위한 기초자료로 활용하고자 하였다. 설문대상은 전국 19세 이상 성인남녀 500명이며, 조사기간은 2009년 7월 18일 하루에 진행하였다. 총 13개의 선택형 설문문항으로 구성된 구조화된 질문지를 가지고 전화면접조사를 하였으며, 최대 허용오차는 95% 신뢰수준 하에서 ±4.4%이다.

보다 구체적으로 살펴보면, 설문분석을 통해 시민들이 개인정보 유출과 같은 프라이버시 침해 문제에 대해 심각성을 느끼고 있음을 알 수 있었으며, 개인정보 관리의 안전성과 함께 개인정보 관련 인지도를 파악할 수 있었다. 또한 개인정보 확인을 위해 개인정보 열람을 청구한 경험 및 개인정보 열람 후 정정·삭제를 청구한 경험이 어느 정도 있는지를 파악하여 열람 및 정정·삭제 청구의 실태를 알 수 있었으며, 개인정보를 다른 기관과 공유/제공하는 사실에 대한 인지도와 어떤 기관에 어떤 개인정보를 제공하는지에 대한 인지도를 파악하여 개인정보 수집·유통에 대한 실태 분석에 시사점을 얻을 수 있었다. 그리고 이와 함께 날로 확대보급되고 있는 CCTV에 대한 인식을

살펴봄으로써 이에 대한 정책적 함의를 이끌어낼 수 있었다.

이번 설문조사는 개인정보 보호실태에 대한 일반 시민의 전반적 인식과 정보주체의 권리에 대한 인지정도에 초점을 맞추었기 때문에 개별 사회 영역에서의 문제나 영역별 차이점은 검토할 수 없었다는 데 한계가 있다. 개인정보 수집·유통 및 열람·정정청구에 대한 인식을 솔직하게 드러냈다는 점에 이 시민인식 조사의 의의가 있다 하겠다.

## 2. 종합결과

전반적으로 시민들은 개인정보 관리에 대한 인식에 있어 그 심각성을 절감하고 있다. 우선 개인정보 유출과 같은 프라이버시 침해가 심각하다고 보는 사람이 대다수(82.2%)이고, 심각하지 않다고 보는 사람은 별로 되지 않는다(4.8%). 이와 관련하여 공공기관이나 민간기업의 개인정보 관리의 안전성에 대해서도 부정적인 인식을 보였다. 안전하지 않다고 보는 사람이 과반수 가까이 되었기 때문이다(48.4%, 47.6%). 이는 우리 사회의 개인정보 관리 양태에 대한 전반적인 불신을 보여준다. 시민들은 주민번호를 다른 번호로 대체하는 것에 대해 동의한다는 의견(65.8%)이 많았는데, 이는 주민번호가 개인 식별자로 사용되는 것에 대한 거부감이 많음을 보여준다.

한편 개인정보 취급 방침을 공개해야 한다는 사실을 '알고 있는' 응답자(20.6%)보다는 '모르고 있는' 응답자(79.4%)가 압도적으로 많았고, 개인정보 열람을 청구할 수 있다는 사실을 '알고 있는' 응답자(24.2%)보다 '모르고 있는' 응답자(75.8%)가 압도적으로 많은 것으로 조사되어 개인정보 관련 인지도는 낮은 편으로 나타났다. 그 연장선에서 개인정보 확인을 위해 개인정보 열람을 청구한 경험이 있는 사람(5.6%)이나 개인정보 열람 후, 정정/삭제를 청구한 경험이 있는 사람(10.7%)이 소수인 것은 당연하다.

하지만 자신의 개인정보를 가지고 있는 기관이 개인정보를 다른 기관과 공유하거나 제공하는 경우가 있다는 것에 대한 인지도는 과반수를 넘어서(53.6%) 제3자 제공에 대해 알고 있음을 보여주고 있으나, 인지자 중에서 구체적으로 알고 있는 이는 4분의 1이 채 되지 않았다(22.8%).

이상의 설문과는 별개로 CCTV에 대한 인식을 물었는데, 공공기관에서 CCTV를 설치하는 경우 이를 쉽게 인식할 수 있도록 해야 한다는 사실을 몰랐던 경우가 과반수를 넘었으며(55.8%), 알고 있다고 응답한 경우는 22.6%에 불과하였다. 그리고 CCTV가 설치된 것을 보면 안심이 되는 사람이 과반

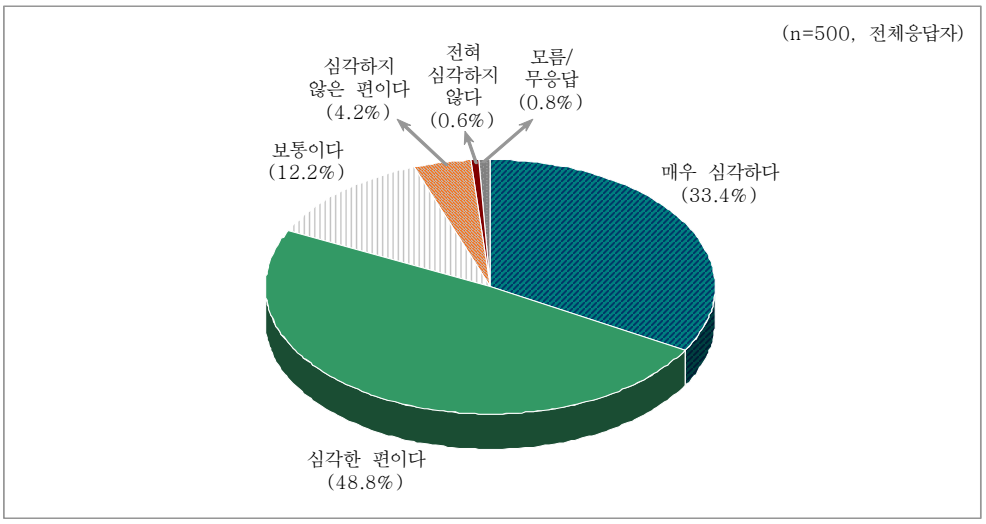
수를 넘고(50.2%), CCTV에 찍히더라도 이에 위축되지 않는다는 사람이 과반수를 넘어(54.8%) CCTV의 프라이버시 침해 가능성에 대해서는 크게 개의치 않는 모습을 보여주었다.

## 3. 설문별 분석 결과

설문별 분석의 자세한 결과는 다음과 같다.

우리 사회에서 개인정보 유출과 같은 프라이버시 침해가 얼마나 심각한지를 묻는 질문에 대해 시민들은 '매우 심각하다' 33.4%, '심각한 편이다' 48.8%로 전체 응답자의 82.2%가 '심각하다'고 답하여 대부분을 차지했으며, '심각하지 않다'는 응답은 4.8%에 불과한 것으로 드러났다.

<그림 4-1> 개인정보 유출과 같은 프라이버시 침해의 심각성




이를 성별로 보면 여성의 '심각하다'는 응답이 85.3%로 남성의 79.0%에 비해 높게 나타났다. 여성이 남성보다 프라이버시 침해의 심각성에 더 많이 공감하고 있는 것이다.

<표 4-1> 성별 개인정보 유출과 같은 프라이버시 침해의 심각성

| 구분 | 사례 수 | 매우 심각하다 | 심각한 편이다 | 보통이다 | 심각하지 않은 편이다 | 전혀 심각하지 않다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 심각하다 | 심각하지 않다 |
| 전체 | (500) | 33.4 | 48.8 | 12.2 | 4.2 | 0.6 | 0.8 | 82.2 | 4.8 |
| 남성 | (248) | 33.5 | 45.6 | 15.3 | 4.4 | 0.4 | 0.8 | 79.0 | 4.8 |
| 여성 | (252) | 33.3 | 52.0 | 9.1 | 4.0 | 0.8 | 0.8 | 85.3 | 4.8 |

‘심각하다’ 응답률을 연령별로 살펴보면, 40대 이하 연령층의 응답률(29세 이하: 83.5%, 30대: 87.5%, 40대: 86.1%)이 50대 이상 연령층의 응답률(50대: 70.9%, 60세 이상: 79.1%)에 비해 상대적으로 높게 나타났는데, 이는 사회활동의 정도와 관련이 있는 것으로 보인다. 즉 적극적인 사회활동을 하는 경우일수록 자신의 개인정보가 유출될 가능성이 높고, 이로 인해 프라이버시 침해의 심각성을 더 강하게 느끼는 것이다. 나아가 50대 이상 연령층에서 전형적으로 나타나는 프라이버시 인식에 대한 부재도 드러내고 있다고 본다.

<표 4-2> 연령별 개인정보 유출과 같은 프라이버시 침해의 심각성

| 구분 | 사례 수 | 매우 심각하다 | 심각한 편이다 | 보통이다 | 심각하지 않은 편이다 | 전혀 심각하지 않다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 심각하다 | 심각하지 않다 |
| 전체 | (500) | 33.4 | 48.8 | 12.2 | 4.2 | 0.6 | 0.8 | 82.2 | 4.8 |
| 29세이하 | (103) | 33.0 | 50.5 | 14.6 | 1.9 | 0.0 | 0.0 | 83.5 | 1.9 |
| 30대 | (112) | 34.8 | 52.7 | 6.3 | 6.3 | 0.0 | 0.0 | 87.5 | 6.3 |
| 40대 | (115) | 40.9 | 45.2 | 11.3 | 1.7 | 0.0 | 0.9 | 86.1 | 1.7 |
| 50대 | (79) | 31.6 | 39.2 | 20.3 | 6.3 | 1.3 | 1.3 | 70.9 | 7.6 |
| 60세이상 | (91) | 24.2 | 54.9 | 11.0 | 5.5 | 2.2 | 2.2 | 79.1 | 7.7 |

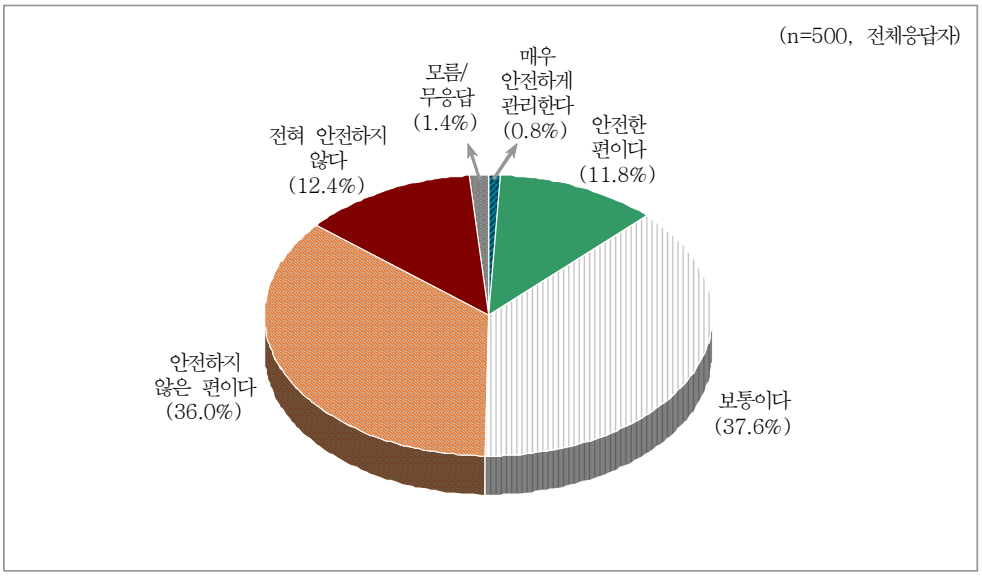
시민들은 공공기관이나 민간기업이나 공통적으로 개인정보 관리의 안전성에 대해서 부정적인 인식을 보였다. 우선 중앙행정기관이나 지방자치단체와 같은 공공기관이 국민의 개인정보를 얼마나 안전하게 관리한다고 생각하는지에 대해 과반수 가량인 48.4%(전혀 안전하지 않다: 12.4%, 안전하지 않은 편이다: 36.0%)가 ‘안전하지 않다’라고 응답하여 ‘안전하다’ 12.6%에 비해 35%p 이상 높게 나타났다.

한편 은행 등 금융기관이나 인터넷 포털과 같은 민간기업이 고객의 개인정보를 얼마나 안전하게 관리한다고 생각하는지에 대한 질문에 대해서는 ‘안전

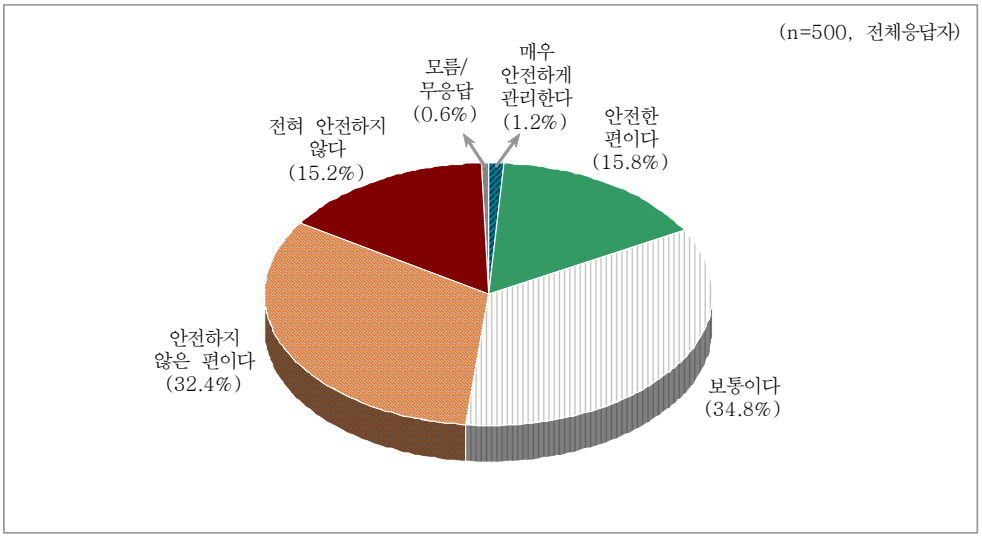
하지 않다'는 응답은 '전혀 안전하지 않다' 15.2%, '안전하지 않은 편이다' 32.4% 등 47.6%인 반면, '안전하다'는 응답은 17.0%('매우 안전하게 관리한다' 1.2%, '안전한 편이다' 15.8%)로 나타났다. 즉 공공기관이나 민간기관의 개인정보 관리의 안전성에 대해 불신하는 비율이 과반수 가까이에 육박하여 우리 사회의 개인정보 관리 양태에 대한 전반적인 불신을 보여주었다.

그 가운데에서도 공공기관의 국민 개인정보 관리가 안전하다는 응답의 비율(12.6%)보다는 민간기업의 고객 개인정보 관리가 안전하다는 응답의 비율(17.0%)이 더 높게 나타났다.

<그림 4-2> 공공기관의 국민 개인정보 관리의 안전성



<그림 4-3> 민간기업의 고객 개인정보 관리의 안전성




그리고 공공기관과 민간기업 모두 남성이 여성보다 개인정보 관리의 안전성에 대해 상대적으로 긍정적이었는데, 공공기관의 경우 '안전하다'는 평가는 남성 13.7%, 여성 11.5%로, 민간기업의 경우 남성 19.8%, 여성 14.3%로 나타났다. 이는 여성이 남성보다 프라이버시 침해의 심각성을 더 강하게 느끼는 것과 일치하는 결과이다.

<표 4-3> 성별 공공기관의 국민 개인정보 관리의 안전성

| 구분 | 사례 수 | 매우 안전하게 관리한다 | 안전한 편이다 | 보통이다 | 안전하지 않은 편이다 | 전혀 안전하지 않다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 안전하다 | 안전하지 않다 |
| 전체 | (500) | 0.8 | 11.8 | 37.6 | 36.0 | 12.4 | 1.4 | 12.6 | 48.4 |
| 남성 | (248) | 1.2 | 12.5 | 37.9 | 33.5 | 13.3 | 1.6 | 13.7 | 46.8 |
| 여성 | (252) | 0.4 | 11.1 | 37.3 | 38.5 | 11.5 | 1.2 | 11.5 | 50.0 |

<표 4-4> 성별 민간기업의 고객 개인정보 관리의 안전성

| 구분 | 사례 수 | 매우 안전하게 관리한다 | 안전한 편이다 | 보통이다 | 안전하지 않은 편이다 | 전혀 안전하지 않다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 안전하다 | 안전하지 않다 |
| 전체 | (500) | 1.2 | 15.8 | 34.8 | 32.4 | 15.2 | 0.6 | 17.0 | 47.6 |
| 남성 | (248) | 1.6 | 18.1 | 34.3 | 31.0 | 14.9 | 0.0 | 19.8 | 46.0 |
| 여성 | (252) | 0.8 | 13.5 | 35.3 | 33.7 | 15.5 | 1.2 | 14.3 | 49.2 |

연령별 개인정보 관리의 안전성 평가의 비율을 보면, 다른 연령층에서 안전성에 대한 긍정적인 평가율이 10%대인 반면, 60세 이상 연령층만이 공공기관 22.0%, 민간기업 29.7%로 20%가 넘게 개인정보 관리가 안전하다고 보고 있었다. 이것은 각 기관의 활용도와 관련이 있을 것이며, 앞서 보았던 개인정보 침해에 대한 민감도와도 관련이 있는 듯하다.

<표 4-5> 연령별 공공기관의 국민 개인정보 관리의 안전성

| 구분 | 사례수 | 매우 안전하게 관리한다 | 안전한 편이다 | 보통이다 | 안전하지 않은 편이다 | 전혀 안전하지 않다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 안전하다 | 안전하지 않다 |
| 전체 | (500) | 0.8 | 11.8 | 37.6 | 36.0 | 12.4 | 1.4 | 12.6 | 48.4 |
| 29세이하 | (103) | 0.0 | 8.7 | 48.5 | 30.1 | 12.6 | 0.0 | 8.7 | 42.7 |
| 30대 | (112) | 0.9 | 10.7 | 37.5 | 33.9 | 16.1 | 0.9 | 11.6 | 50.0 |
| 40대 | (115) | 0.0 | 10.4 | 35.7 | 38.3 | 14.8 | 0.9 | 10.4 | 53.0 |
| 50대 | (79) | 1.3 | 10.1 | 32.9 | 40.5 | 13.9 | 1.3 | 11.4 | 54.4 |
| 60세이상 | (91) | 2.2 | 19.8 | 31.9 | 38.5 | 3.3 | 4.4 | 22.0 | 41.8 |

<표 4-6> 연령별 민간기업의 고객 개인정보 관리의 안전성

| 구분 | 사례수 | 매우 안전하게 관리한다 | 안전한 편이다 | 보통이다 | 안전하지 않은 편이다 | 전혀 안전하지 않다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 안전하다 | 안전하지 않다 |
| 전체 | (500) | 1.2 | 15.8 | 34.8 | 32.4 | 15.2 | 0.6 | 17.0 | 47.6 |
| 29세이하 | (103) | 0.0 | 17.5 | 41.7 | 31.1 | 9.7 | 0.0 | 17.5 | 40.8 |
| 30대 | (112) | 0.0 | 12.5 | 40.2 | 26.8 | 20.5 | 0.0 | 12.5 | 47.3 |
| 40대 | (115) | 1.7 | 9.6 | 27.0 | 39.1 | 22.6 | 0.0 | 11.3 | 61.7 |
| 50대 | (79) | 1.3 | 15.2 | 32.9 | 34.2 | 15.2 | 1.3 | 16.5 | 49.4 |
| 60세이상 | (91) | 3.3 | 26.4 | 31.9 | 30.8 | 5.5 | 2.2 | 29.7 | 36.3 |

최근 주민등록번호를 식별키로 사용하는 것에 대한 비판이 높아지고 있고, 행정안전부도 관리대책을 내놓은 바 있다. 이에 다소 불편하더라도 개인정보 보호를 위해서 주민번호 대신 여권이나 운전면허증, 의료보험증 번호와 같은 것으로 대체해야 한다는 주장에 대해 시민들의 의견을 물은 결과, 주민번호를 다른 번호로 대체하는 것에 대해 '동의한다'는 응답률이 65.8%로 '동의하지 않는다' 응답률 31.6%에 비해 높게 나타났다.

<표 4-7> 성별 주민번호를 다른 번호로 대체하는 것에 대한 의견

| 구분 | 사례수 | 동의한다 | 동의하지 않는다 | 모름/ 무응답 |
|---|---|---|---|---|
| 전체 | (500) | 65.8 | 31.6 | 2.6 |
| 남성 | (248) | 61.3 | 37.1 | 1.6 |
| 여성 | (252) | 70.2 | 26.2 | 3.6 |

이 설문에서도 여성의 경우 주민번호를 다른 번호로 대체하는 것에 '동의한다'는 응답이 70.2%로 남성 61.3%에 비해 상대적으로 높게 나타났으며, 연령별 의견의 경우에는 '동의한다'는 응답률이 비슷한 것으로 나타났다.

<표 4-8> 연령별 주민번호를 다른 번호로 대체하는 것에 대한 의견

| 구분 | 사례수 | 동의한다 | 동의하지 않는다 | 모름/ 무응답 |
|---|---|---|---|---|
| 전체 | (500) | 65.8 | 31.6 | 2.6 |
| 29세 이하 | (103) | 65.0 | 34.0 | 1.0 |
| 30대 | (112) | 64.3 | 33.9 | 1.8 |
| 40대 | (115) | 66.1 | 32.2 | 1.7 |
| 50대 | (79) | 67.1 | 31.6 | 1.3 |
| 60세 이상 | (91) | 67.0 | 25.3 | 7.7 |

개인정보 취급 방침을 공개해야 한다는 사실을 인지하고 있는지 여부는 개인정보 열람 및 정정 청구의 전제가 되기 때문에 의미가 있는 설문이다. 공공기관이나 민간기업이 개인정보를 수집/이용하는 경우, 개인정보를 취급하는 방침을 정하고 일반에 공개해야 한다는 사실을 알고 있는지 여부를 조사한 결과, 전체 응답자들 중 개인정보 취급 방침을 공개해야 한다는 사실을 '알고 있는' 응답자는 전체의 1/5 수준인 20.6%이며, 79.4%는 '모르고 있는' 것으로 나타났다.

성별로 보면 개인정보 취급 방침을 공개해야 한다는 사실을 '알고 있는' 응답자의 비율은 여성(17.9%)보다 남성(23.4%)이 더 높았는데, 이는 개인정보 취급 방침 공개 사실 인지 여부와 같은 개인정보 실태조사 항목과 인식조사 항목이 일치하지 않음을 보여준다. 앞의 인식조사를 묻는 설문에서는 여성의 응답율이 더 높았기 때문이다.

<표 4-9> 개인정보 취급 방침을 공개해야 한다는 사실의 인지 여부

| 구 분 | 사례수 | 예(알고 있다) | 아니오(모르고 있다) |
|---|---|---|---|
| 전 체 | (500) | 20.6 | 79.4 |
| 남 성 | (248) | 23.4 | 76.6 |
| 여 성 | (252) | 17.9 | 82.1 |

한편 연령별로는 저연령층일수록(29세 이하: 28.2%, 30대: 19.6%, 40대: 20.9%, 50대: 19.0%, 60세 이상 14.3%) '알고 있다'는 응답자의 비율이 높은 경향을 보였다.

본인의 개인정보를 보유하고 있는 공공기관이나 민간기업에 본인의 개인정보 열람을 청구할 수 있다는 사실을 알고 있는지 여부를 묻는 설문에 대해서는 개인정보 취급 방침 공개 사실 인지 여부 설문과 비슷하게 '아니다(모르고 있다)' 응답률이 75.8%로 '예(알고 있다)' 응답률 24.2%에 비해 3배 이상 높게 나타났다. 하지만, 남성과 여성의 응답률은 각각 24.6%, 23.8%로 크게 차이가 나지 않았다.

<표 4-10> 성별 개인정보 열람을 청구할 수 있다는 사실의 인지 여부

| 구 분 | 사례수 | 예(알고 있다) | 아니오(모르고 있다) |
|---|---|---|---|
| 전 체 | (500) | 24.2 | 75.8 |
| 남 성 | (248) | 24.6 | 75.4 |
| 여 성 | (252) | 23.8 | 76.2 |

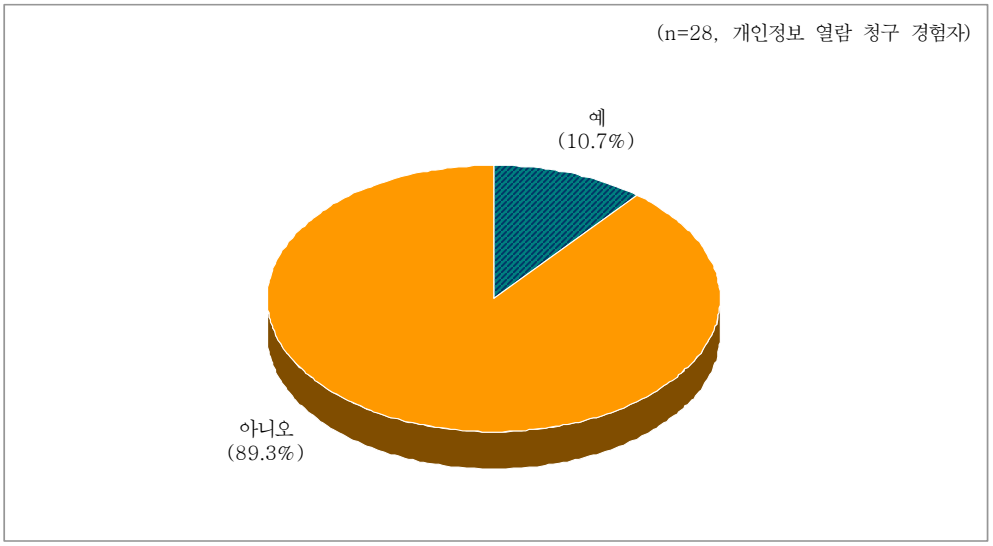
다음으로, 열람 및 정정 청구에 대한 실태조사 항목으로, 주민등록 등초본 등 일반 민원서류를 발급받는 것을 제외하고 본인의 개인정보를 확인하기 위해 개인정보 열람을 청구하신 경험이 있는지 여부를 조사하였다. 그 결과는 개인정보 확인을 위해 개인정보 열람을 청구한 '경험이 없는' 응답자가 94.4%로 대부분을 차지했으며, '경험이 있는' 응답자는 5.6%에 불과하였고 남녀간에 큰 차이가 나지 않았다(개인정보 열람을 청구한 '경험이 있다'는 응답이 남성 5.2%, 여성 6.0%). 그리고 연령별로는 저연령층일수록 '경험이 있다' 응답률은 높은 경향(29세 이하: 7.8%, 30대: 6.3%, 40대: 5.2%, 50대: 3.8%, 60세 이상: 4.4%)을 보였다.

<표 4-11> 성별 개인정보 확인을 위해 개인정보 열람을 청구한 경험 여부

| 구 분 | 사례수(%) | 예(경험이 있다) | 아니오(경험이 없다) |
|---|---|---|---|
| 전 체 | 500 (100) | 28 (5.6) | 472 (94.4) |
| 남 성 | 248 (49.6) | 13 (5.2) | 235 (94.8) |
| 여 성 | 252 (50.4) | 15 (6.0) | 237 (94.0) |

개인정보 열람 청구 경험자 28명을 대상으로 개인정보 열람 후에 개인정보의 정정이나 삭제를 청구한 경험이 있는지 여부에 대해 물어본 결과 경험이 있는 사람은 3명(10.7%)이었고, 나머지 25명(89.3%)는 정정/삭제 청구 경험이 없었다. 이러한 설문결과는 법령에서 보장하고 있는 정보주체의 권리에 대해 일반 시민들의 인지 정도가 매우 낮으며, 이에 대한 정부의 홍보 및 교육 노력이 미흡한 현실을 보여준다. 따라서 일반 시민을 대상으로 정보주체의 권리에 대해 적극적으로 홍보하고 교육할 필요가 있다고 본다.

<그림 4-4> 개인정보 열람 후, 정정/삭제를 청구한 경험 여부




한편 본인의 개인정보를 가지고 있는 기관이 개인정보를 다른 기관과 공유하거나 제공하는 경우가 있다는 사실을 알고 있는지를 묻는 설문에는 '알고 있다'는 응답자가 268명(53.6%)이었고, '모르고 있다'는 응답자가 232명(46.4%)으로 나타났으며, 남녀간에 응답율의 차이는 없었다.

<표 4-12> 개인정보를 다른 기관과 공유/제공하는 사실의 인지 여부

| 구 분 | 사례수 (%) | 예(알고 있다) | 아니오(모르고 있다) |
|---|---|---|---|
| 전 체 | 500 (100) | 268 (53.6) | 232 (46.4) |
| 남 성 | 248 (49.6) | 133 (53.6) | 115 (46.4) |
| 여 성 | 252 (50.4) | 135 (53.6) | 117 (46.4) |

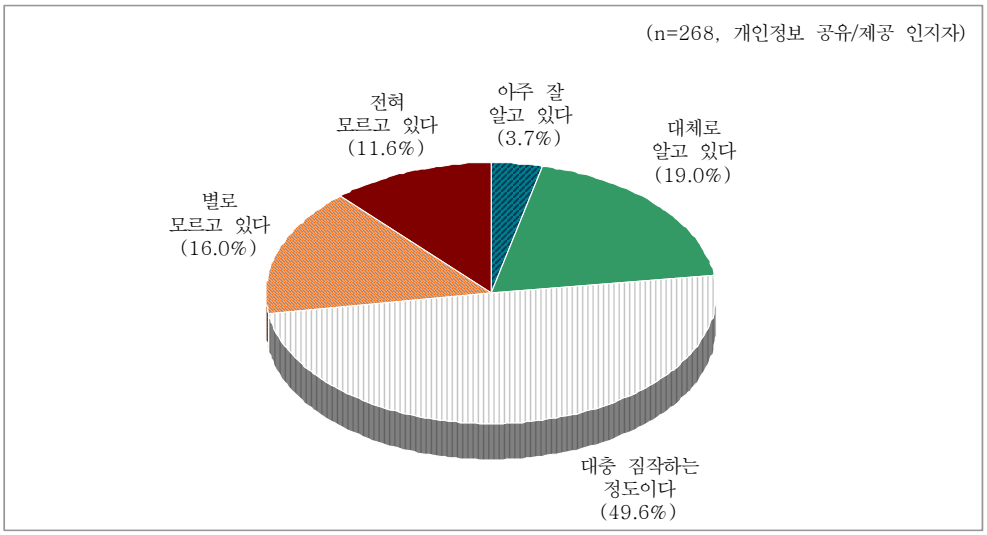
연령별로 보면 60세 이상 연령층의 개인정보의 타 기관 공유/제공 사실 인지도가 29.7%로 50대 이하 연령층(29세 이하: 55.3%, 30대: 59.8%, 40대: 65.2%, 50대: 53.2%)에 비해 매우 낮게 조사되었다. 이러한 조사결과를 통해 앞에서 50대 이상 연령층에서 개인정보 침해에 대한 우려가 낮게 나타난 것도 개인정보의 활용 사실에 대한 인지 부족 때문일 개연성이 높다고 생각해볼 수 있다.

<표 4-13> 연령별 개인정보를 다른 기관과 공유/제공하는 사실의 인지 여부

| 구분 | 사례수 (%) | 예(알고 있다) | 아니오(모르고 있다) |
|---|---|---|---|
| 전체 | 500 (100) | 268 (53.6) | 232 (46.4) |
| 29세 이하 | 103 (20.6) | 57 (55.3) | 46 (44.7) |
| 30대 | 112 (22.4) | 67 (59.8) | 45 (40.2) |
| 40대 | 115 (23.0) | 75 (65.2) | 40 (34.8) |
| 50대 | 79 (15.8) | 42 (53.2) | 37 (46.8) |
| 60세 이상 | 91 (18.2) | 27 (29.7) | 64 (70.3) |

위의 설문과 관련하여 본인의 개인정보를 다른 기관과 공유/제공하는 경우가 있다는 사실을 알고 있는 268명에게 본인의 개인정보를 가지고 있는 기관이 외부의 어떤 기관에 어떤 정보를 제공하는지를 알고 있는지 여부를 질문한 결과, '대충 짐작하는 정도이다'라는 응답이 49.6%로 절반 가까이 차지한 가운데, '모르고 있다'는 응답이 27.6%(전혀 모르고 있다: 11.6%, 별로 모르고 있다: 16.0%)로, '알고 있다'는 응답 22.8%(아주 잘 알고 있다: 3.7%, 대체로 알고 있다: 19.0%)에 비해 다소 높게 나타났다. 구체적으로 외부의 어떠한 기관에 자신의 어떠한 정보가 공유되거나 제공되고 있는지를 정확하게 아는 이가 1/4 정도에 불과한 셈이다.

<그림 4-5> 어떤 기관에 어떤 개인정보를 제공하는지에 대한 인지 여부

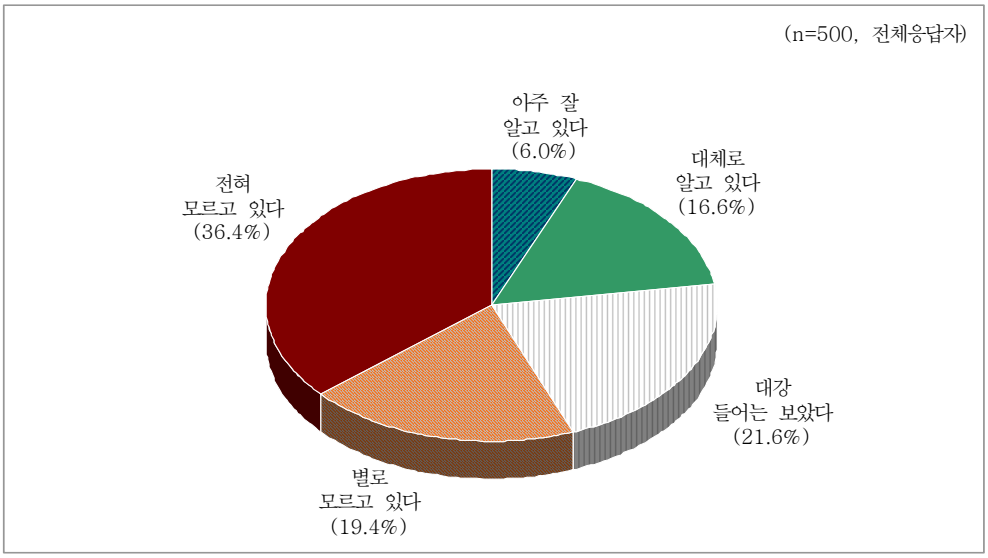



성별 인지도는 '알고 있다'는 응답이 남성은 24.1%, 여성 21.5%로 크게 차이가 나지 않았으며, 연령별 인지도는 유의미한 결과가 나오지 않았다.

시민 인식조사의 마지막은 CCTV에 관한 것이었다. 우선 공공기관에서 CCTV를 설치하는 경우, 이를 쉽게 인식할 수 있도록 조치를 취해야 한다는 사실을 알고 있는지 설문한 결과, '아주 잘 알고 있다' 6.0%, '대체로 알고 있다' 16.6%로 22.6%가 '알고 있다'고 응답했으며, '모르고 있다'는 응답('전혀 모르고 있다' 36.4%, '별로 모르고 있다' 19.4%)은 55.8%로 나타났다.

성별 인지도 여부는 '알고 있다' 응답률이 남성 24.2%, 여성 21.0%로 나타나 큰 차이가 없었으며, 연령별 인지도는 50대 연령층의 인지도가 31.6%로 다른 연령층(29세 이하: 18.4%, 30대: 23.2%, 40대: 23.5%, 60세 이상: 17.6%)에 비해 높게 나타났다. 20대 이하와 60대 이상에 비해, 가정 및 사회생활에서 중심적 역할을 하는 30대~50대 연령층의 CCTV에 대한 관심이 상대적으로 높음을 짐작할 수 있다.

<그림 4-6> CCTV를 인식할 수 있도록 해야 한다는 사실의 인지 여부



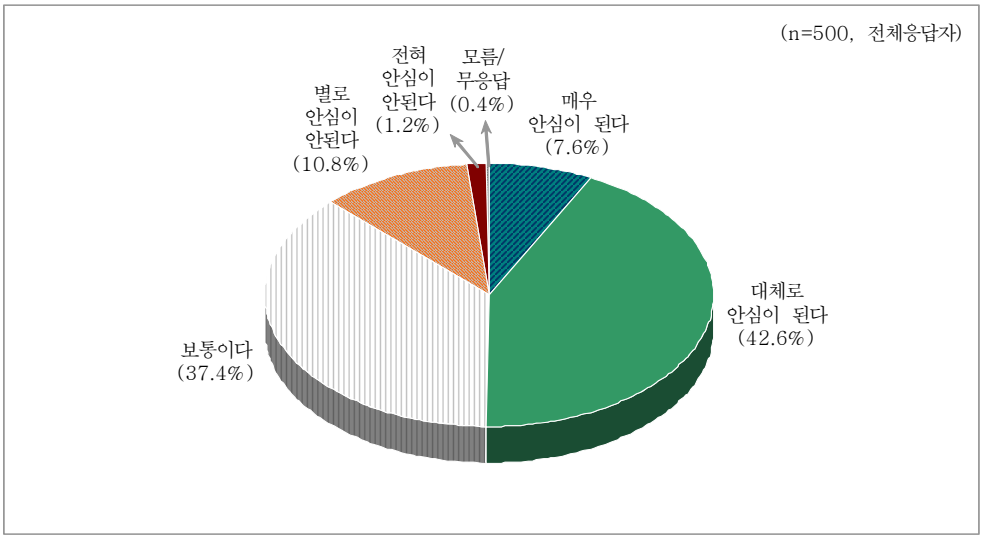

<표 4-14> 연령별 CCTV를 인식할 수 있도록 해야 한다는 사실의 인지 여부

| 구 분 | 사례수 | 아주 잘 알고 있다 | 대체로 알고 있다 | 대강 들어는 보았다 | 별로 모르고 있다 | 전혀 모르고 있다 | 종합 | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | 알고 있다 | 모르고 있다 |
| 전체 | (500) | 6.0 | 16.6 | 21.6 | 19.4 | 36.4 | 22.6 | 55.8 |
| 29세이하 | (103) | 4.9 | 13.6 | 22.3 | 21.4 | 37.9 | 18.4 | 59.2 |
| 30대 | (112) | 5.4 | 17.9 | 20.5 | 19.6 | 36.6 | 23.2 | 56.3 |
| 40대 | (115) | 6.1 | 17.4 | 21.7 | 22.6 | 32.2 | 23.5 | 54.8 |
| 50대 | (79) | 8.9 | 22.8 | 21.5 | 16.5 | 30.4 | 31.6 | 46.8 |
| 60세이상 | (91) | 5.5 | 12.1 | 22.0 | 15.4 | 45.1 | 17.6 | 60.4 |

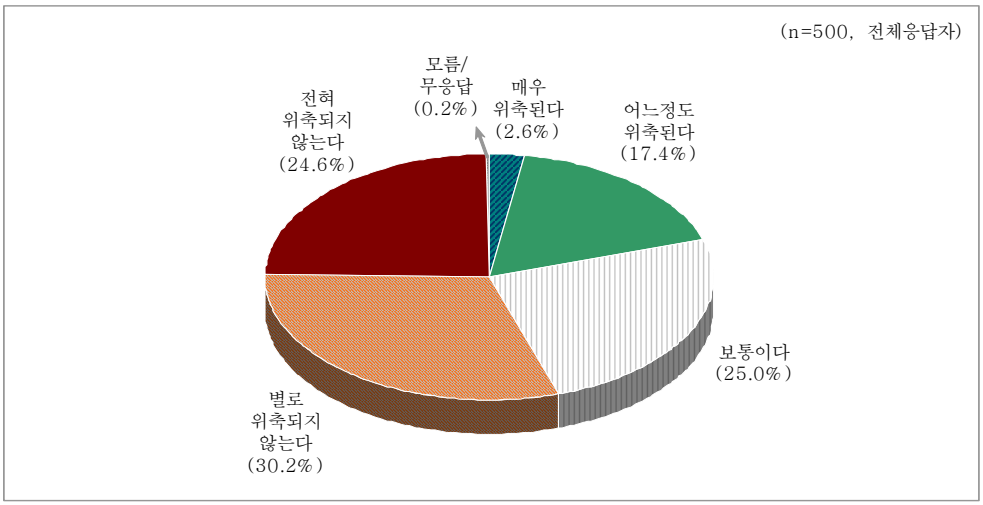
CCTV의 설치 효과를 살펴보기 위해 CCTV가 설치된 것을 보면 안심되는지, 그리고 CCTV에 찍힌다는 사실에 위축되는지 여부를 조사하였다. 우선 CCTV가 설치된 것을 보았을 때 안심되는 정도에 대해서는 '안심이 된다'는 응답이 50.2%(매우 안심이 된다: 7.6%, 대체로 안심이 된다: 42.6%)로 '안심이 안된다'는 응답 12.0%(전혀 안심이 안된다: 1.2%, 별로 안심이 안된다: 10.8%)에 비해 높게 나타났다. 이러한 결과는 어느 정도 예상된 것이었다. 그러나 곳곳에 설치되어 있는 CCTV를 보았을 때 내가 CCTV에 찍힌다는 사실에 위축될 것이라는 가정으로 설문한 문항에 대해서, CCTV에 찍힌다는 사실에 '위축된다'는 응답('매우 위축된다' 2.6%, '어느정도 위축된다' 17.4%)

이 20.0%밖에 되지 않는 반면, '위축되지 않는다'는 응답은 54.8%('전혀 위축되지 않는다' 24.6%, '별로 위축되지 않는다' 30.2%)로 조사되어 예상과 어긋나는 결과를 보였다. 이는 시민들이 CCTV의 부작용에 대해 아직까지 많이 접하지 못한 결과로 보이며, 또한, 우리사회에서 CCTV 도입에 대한 대중적 관심이 범죄예방 효과에만 맞추어져 있어서, 일반 시민들의 경우 CCTV로 인한 인권침해에 대한 인식은 높지 않다는 것을 보여준다.

<그림 4-7> CCTV가 설치된 것을 보았을 때 안심되는 정도




<그림 4-8> CCTV에 찍힌다는 사실에 위축되는 정도



여성의 경우 CCTV가 설치된 것을 보면 안심이 된다고 응답한 비율이 남성의 46.4%보다 높은 54.0%로 나타나 여성에게 특히 CCTV의 심리적 효과가 큰 것으로 조사되었다. CCTV에 찍힌다는 사실에 위축되는지 여부에 대해서는 남녀간에 큰 차이가 나지 않았다.

<표 4-15> 성별 CCTV가 설치된 것을 보면 안심되는 정도

| 구분 | 사례 수 | 매우 안심이 된다 | 대체로 안심이 된다 | 보통이다 | 별로 안심이 안된다 | 전혀 안심이 안된다 | 모름/무응답 | 종 합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 안심이 된다 | 안심이 안된다 |
| 전체 | (500) | 7.6 | 42.6 | 37.4 | 10.8 | 1.2 | 0.4 | 50.2 | 12.0 |
| 남성 | (248) | 6.5 | 39.9 | 38.7 | 12.9 | 1.6 | 0.4 | 46.4 | 14.5 |
| 여성 | (252) | 8.7 | 45.2 | 36.1 | 8.7 | 0.8 | 0.4 | 54.0 | 9.5 |

연령별로는 고연령층일수록(29세 이하: 39.8%, 30대: 46.4%, 40대: 48.7%, 50대: 60.8%, 60세 이상: 59.3%) CCTV가 설치된 것을 보면 '안심이 된다'는데 높은 응답률을 보였으며, CCTV 노출 시 위축 여부에 대해서는 29세 이하: 20.4%, 30대: 18.8%, 40대: 21.7%, 50대: 19.0%, 60세 이상: 19.9%로 나타나 뚜렷한 경향이 보이지는 않았다.

<표 4-16> 연령별 CCTV가 설치된 것을 보면 안심되는 정도

| 구 분 | 사례 수 | 매우 안심이 된다 | 대체로 안심이 된다 | 보통이다 | 별로 안심이 안된다 | 전혀 안심이 안된다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 안심이 된다 | 안심이 안된다 |
| 전체 | (500) | 7.6 | 42.6 | 37.4 | 10.8 | 1.2 | 0.4 | 50.2 | 12.0 |
| 29세이하 | (103) | 3.9 | 35.9 | 43.7 | 15.5 | 1.0 | 0.0 | 39.8 | 16.5 |
| 30대 | (112) | 8.9 | 37.5 | 45.5 | 7.1 | 0.9 | 0.0 | 46.4 | 8.0 |
| 40대 | (115) | 7.0 | 41.7 | 36.5 | 13.0 | 1.7 | 0.0 | 48.7 | 14.8 |
| 50대 | (79) | 12.7 | 48.1 | 27.8 | 8.9 | 1.3 | 1.3 | 60.8 | 10.1 |
| 60세이상 | (91) | 6.6 | 52.7 | 29.7 | 8.8 | 1.1 | 1.1 | 59.3 | 9.9 |

<표 4-17> 연령별 CCTV에 찍힌다는 사실에 위축되는 정도

| 구 분 | 사례 수 | 매우 위축된다 | 어느정도 위축된다 | 보통이다 | 별로 위축되지 않는다 | 전혀 위축되지 않는다 | 모름/무응답 | 종합 | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | 위축된다 | 위축되지 않는다 |
| 전체 | (500) | 2.6 | 17.4 | 25.0 | 30.2 | 24.6 | 0.2 | 20.0 | 54.8 |
| 29세이하 | (103) | 2.9 | 17.5 | 28.2 | 35.9 | 15.5 | 0.0 | 20.4 | 51.5 |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 30대 | (112) | 1.8 | 17.0 | 32.1 | 26.8 | 22.3 | 0.0 | 18.8 | 49.1 |
| 40대 | (115) | 2.6 | 19.1 | 20.0 | 33.0 | 24.3 | 0.9 | 21.7 | 57.4 |
| 50대 | (79) | 1.3 | 17.7 | 17.7 | 29.1 | 34.2 | 0.0 | 19.0 | 63.3 |
| 60세이상 | (91) | 4.4 | 15.4 | 25.3 | 25.3 | 29.7 | 0.0 | 19.8 | 54.9 |

CCTV의 설치 효과와 관련하여 CCTV가 설치된 것을 보면 안심되는지 여부와 CCTV에 찍힌다는 사실에 위축되는지 여부 사이에 상관관계가 존재하는지를 측정하기 위해 상관분석을 하였다. 즉, CCTV가 설치된 것을 보면 안심된다는 사람은 CCTV에 찍히는 것에 상대적으로 덜 위축되고, 그 반대도 성립하는지 알아보고자 한 것이다. 하지만 실제 CCTV가 설치된 것을 보면 안심이 된다고 응답한 사람의 경우에도 자신이 CCTV에 찍힌다는 사실을 알게 된 경우 위축된다는 사람은 251명 중 43명으로 17.1%로 전체 평균인 20.0%보다 약간 낮긴 했지만, 그렇게 큰 차이를 보이지는 않았다.

<표 4-18> CCTV에 위축되는 정도와 안심되는 정도 사이의 상관관계

| 구 분 | | | CCTV에 찍힌다는 사실에 위축되는 정도 | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | 매우 위축된다 | 어느정도 위축된다 | 보통이다 | 별로 위축되지 않는다 | 전혀 위축되지 않는다 | 모름/무응답 | 전체 |
| CCTV가 설치된 것을 보면 안심되는 정도 | 매우 안심이 된다 | 빈도 | 2 | 2 | 3 | 13 | 18 | 0 | 38 |
| | | % | 5.3 | 5.3 | 7.9 | 34.2 | 47.4 | 0 | 100 |
| | 대체로 안심이 된다 | 빈도 | 4 | 35 | 49 | 67 | 57 | 1 | 213 |
| | | % | 1.9 | 16.4 | 23.0 | 31.5 | 26.8 | 0.5 | 100 |
| | 보통이다 | 빈도 | 6 | 35 | 66 | 47 | 33 | 0 | 187 |
| | | % | 3.2 | 18.7 | 35.3 | 25.1 | 17.6 | 0 | 100 |
| | 별로 안심이 안된다 | 빈도 | 1 | 14 | 6 | 21 | 12 | 0 | 54 |
| | | % | 1.9 | 25.9 | 11.1 | 38.9 | 22.2 | 0 | 100 |
| | 전혀 안심이 안된다 | 빈도 | 0 | 1 | 1 | 2 | 2 | 0 | 6 |
| | | % | 0 | 16.7 | 16.7 | 33.3 | 33.3 | 0 | 100 |
| | 모름/무응답 | 빈도 | 0 | 0 | 0 | 1 | 1 | 0 | 2 |
| | | % | 0 | 0 | 0 | 50 | 50 | 0 | 100 |
| | 전체 | 빈도 | 13 | 87 | 125 | 151 | 123 | 1 | 500 |
| | | % | 2.6 | 17.4 | 25.0 | 30.2 | 24.6 | 0.2 | 100 |

피어슨(Pearson) 상관계수 값은 완벽한 정의 상관관계가 있을 경우를 1로,

그 반대의 경우를 -1로 나타나는데, 그 절대값이 작으면 두 변수 간의 관련성이 낮음을 의미한다. 이에 따라 상관관계를 분석한 결과 두 응답들은 미약한 음(-0.096)의 상관계수를 보여주어 CCTV가 설치된 것을 보면 안심되는지 여부와 CCTV에 찍힌다는 사실에 위축되는지 여부 사이에 별 상관이 없음을 보여주었다.

<표 4-19> CCTV 설치 관련 위축과 안심 정도 간의 상관계수(n=500)

| | CCTV가 설치된 것을 보면 안심되는 정도 |
|---|---|
| CCTV에 찍힌다는 사실에 위축되는 정도 | -.096* |

*p<0.05

# 제2절 개인정보보호 책임자 대상 설문조사 결과 분석

## I. 조사 개요

여기서는 공공 및 민간의 주요 기관에서의 개인정보 수집·유통 현황을 조사·분석하기 위해 각 기관에서 개인정보 수집·유통 실태를 가장 잘 알고 있고, 가장 많이 다루고 있는 공공기관 및 민간기업의 개인정보보호 책임자들을 대상으로 부록에 첨부된 설문조사를 하였다.

설문대상 선정을 위해 공공기관의 경우 국가인권위원회를 통해 총 88곳의 공공기관에 공문서를 보내 협조를 구했고, 민간기관의 경우 정보통신서비스 제공자 66, 준용사업자 41, 기타사업자 30, 총 137곳을 선정하여 설문지를 보냈다[303]. 그 결과 2009.8.20 - 9.10에 공공기관 45곳, 민간업체 31곳, 총 76곳의 개인정보보호 책임자가 답변을 하였다.

<표 4-20> 설문 개인정보보호 책임자들의 소속기관

| 소속기관 | 정부중앙부처 | 지방자치단체 | 교육기관 | 공기업 및 준정부기관 | 보건의료기관 | 금융권 | 통신사 | 포털 등 | 준용사업자 | 전체 |
|---|---|---|---|---|---|---|---|---|---|---|
| 공공기관 | 22 | 13 | 9 | 1 | 0 | 0 | 0 | 0 | 0 | 45 |
| 민간기업 | 0 | 0 | 2 | 0 | 2 | 4 | 2 | 14 | 7 | 31 |
| 전체 | 22 | 13 | 11 | 1 | 2 | 4 | 2 | 14 | 7 | 76 |

※ 금융권은 신용정보회사를 포함하며, 통신사는 이동통신사를 포함하며, 포털 등은 부가통신서비스 사업자, 준용사업자는 「정보통신망법」 상 준용사업자이다.

303) "정보통신서비스제공자"란 초고속인터넷 등 유·무선 통신망을 통하거나 컴퓨터 및 컴퓨터 이용기술을 활용하여 정보를 제공하거나 정보의 제공을 매개하는 서비스로써 이동통신서비스, 초고속통신서비스, 인터넷 포털 사이트, 쇼핑몰 등의 서비스를 말하며, 준용사업자는 정보통신서비스제공자이외에 오프라인을 통해 개인정보를 수집하는 아래적시한 사업자로, 정보통신망법의 개인정보보호 규정에 적용되어 이와 관련한 개인정보보호의무 조치를 이행한다. 법률 적용시에는 법률조문의 '정보통신서비스'는 준용사업자의 '서비스'에 해당된다(행정안전부·한국정보보호진흥원, 2008).
- 여행 서비스 제공을 위해 고객의 개인정보를 수집하는 여행업자,
- 피트니스 센터 등 멤버십 클럽 운영 및 객실 예약·이용 등을 위해 개인정보를 수집하는 호텔업자,
- 마일리지 서비스 제공 등 회원제 서비스를 제공하는 항공운송사업자, 휴양콘도미니엄업자, 할인점·백화점·쇼핑센터 운영사업자, 체인사업자
- 수강 신청 및 등록을 위해 수강생 정보를 수집하는 학원 또는 교습소 운영자

<표 4-21> 성별 및 공사 구분

| 구 분 | | | 성 별 | | 전체 |
|---|---|---|---|---|---|
| | | | 남성 | 여성 | |
| 공사 | 공공기관 | 빈도 | 31 | 14 | 45 |
| | | % | 68.9% | 31.1% | 100.0% |
| | 민간기업 | 빈도 | 25 | 6 | 31 |
| | | % | 80.6% | 19.4% | 100.0% |
| 전체 | | 빈도 | 56 | 20 | 76 |
| | | % | 73.7% | 26.3% | 100.0% |

설문문항은 개인정보의 수집·유통 실태를 6개의 영역으로 나누어 각 영역에 대해 3개에서 7개 정도의 선택 문항으로 구성하였으며, 그 외에 총 3개의 오픈 문항을 두었다. 대략적인 조사내용은 다음과 같다. 이러한 조사내용은 정보통신부와 한국정보보호진흥원이 2005년 12월에 발간한 「기업의 개인정보 영향평가 수행을 위한 가이드」에서 개인정보 영향평가 기준(점검표)로 제시된 사항 중에서 본 조사를 위해 적절한 항목들을 선별하여 재구성한 것이다.

(1) 개인정보 침해 위험 및 개인정보보호 체계와 관련한 사항
- 개인정보 침해사고 발생 여부
- 개인정보 침해신고 접수 여부
- 개인정보 영향평가 수행 여부
- 개인정보관리 책임자 및 담당자의 지정 여부
- 개인정보관리담당자의 개인정보 보호업무외 업무수행 여부
- 개인정보관리담당자가 개인정보 보호업무를 주된 업무로 하는지 여부
- 개인정보관리담당자가 개인정보 보호 등 담당 업무를 맡은 기간
- 개인정보보호 관련 교육이수 여부
- 정보보호 교육을 실시한 기관
- 개인정보 보호교육의 효과성
- 개인정보 보호교육 미이수시 그 이유
- 개인정보 보호규정의 공개 여부
- 개인정보 보호 관련 규정 등의 충실한 반영 여부
- 개인정보 보호정책이 수시로 변경·공개되는지 여부

(2) 개인정보 수집단계에서 발생할 수 있는 개인정보 침해 문제와 관련한

사항
- 최소한의 개인정보만 수집 여부
- 정보주체의 민감한 개인정보 수집 여부
- 정보주체의 주민등록번호 수집 여부
- 개인정보 수집항목을 구분하는 절차·시스템의 구성 여부

(3) 개인정보의 이용·제공·공유, 보유 및 파기 등과 관련한 사항
- 개인정보의 목적 외 이용이나 제3자 제공시 동의 절차·방법 마련 여부
- 제3자제공 정보의 폐기관리
- 제3자 제공내역이 대장 등에 기록·보관되고 있는지 여부
- 개인정보 열람·출력기록의 저장·보관 여부
- 목적 달성 시 해당 개인정보의 파기 여부

(4) 개인정보 처리의 위탁 등과 관련한 사항
- 수탁기관에 대한 적절한 관리·통제시스템의 구축 여부
- 위탁관리자 등에 대한 개인정보 보호 관련 교육 시행 여부
- 위탁관리자 등에게 교육을 하지 않는 이유
- 수탁기관 등의 접근가능 개인정보 설정 여부
- 위탁 종료 시 수탁기관의 개인정보 회수·파기 절차 수립·적용 여부
- 수탁기관의 개인정보 처리과정에 대한 정기 감사 실시 여부

(5) 정보주체의 권리보장 조치와 관련한 사항
- 개인정보취급방침 변경의 통지 여부
- 정보주체의 개인정보 열람·정정절차 수립 여부
- 정보주체의 제3자제공 내역요청 절차 마련 여부
- 개인정보 열람청구 처리 경험 여부
- 열람청구 후 정정·삭제청구받은 경험 유무
- 정보주체의 개인정보 정정요구 후 정보 이용방지 절차 마련 여부
- 정보주체의 동의철회에 대한 제약 유무
- 동의철회 제약의 고지 및 약관 명시 여부

(6) 개인정보 보호를 위한 인적 통제와 관련한 사항
- 전산담당자에 대한 개인정보보호 교육 프로그램 유무

- 각 직무별로 특화된 교육시스템 마련 여부
- 내부직원의 개인정보 접근권한 및 권한별 직무범위의 차등설정 여부
- 접근권한별 직무범위 차등 미설정시 그 이유

이러한 개인정보보호 책임자들에 대한 설문조사는 개인정보 수집·유통에 대한 구체적인 실태를 파악하는데 초점을 두었으나, 실제 예상되었던 분석결과를 얻었다고 하기엔 무리가 있다. 개인정보 수집·유통 실태에 대한 개인정보보호 책임자들의 설문이 객관적인 실태를 나타내기보다 실태에 대한 책임자들의 주관적인 인식을 반영한 경우가 많았기 때문이다. 따라서 아래의 개인정보보호 책임자에 대한 설문조사를 통해 각 기관/업체의 개인정보보호 실태에 대한 담당자의 인식을 파악했다는 점에 의의가 있다고 하겠다. 또한 총 응답자 수가 100명이 되지 않아 이 결과를 일반화하는데는 한계가 있으며, 특히 민간업체의 개인정보보호 책임자들의 경우 31곳 정도에 불과하여 공공기관과 민간기업을 비교하는 것 또한 어느 정도 무리가 있다는 점도 감안해야 한다.

공공기관 및 민간기업의 개인정보 보호에 대한 객관적인 실태를 정확하게 파악하기 위해서는 설문조사의 방식보다는 실제 운영 실태에 대한 점검이 이루어질 필요가 있다. 설문조사는 그 자체로 한계가 있다. 설문조사의 특성상 응답자의 주관이 반영될 수 있고, 특히 개인정보보호책임자로서 자신이 책임지고 있는 부분에 대해서, 그리고 각 기관/업체의 평가에 부정적으로 작용할 수 있는 답변을 회피할 가능성이 높기 때문이다. 객관적인 실태점검과 개인정보보호책임자에 대한 설문조사가 병행해서 이루어진다면, 개인정보보호책임자가 느끼는 실태와 실제와의 괴리에 대해서도 판단해볼 수 있을 것이다. 실제로 이번 설문 응답을 보면, 본 연구의 실태조사 결과와 일정하게 괴리가 있는 응답 결과가 나온 경우도 있었다.

## II. 설문별 분석 결과

설문별 분석의 자세한 결과는 다음과 같다.

## 1. 개인정보 침해 위험 및 개인정보보호 체계와 관련한 사항

정보통신부・한국정보보호진흥원(2005)의 「기업의 개인정보 영향평가 수행을 위한 가이드」에서는 개인정보 영향평가의 사전분석으로서 개인정보보호 체계를 검토하고 있다. 이번 개인정보보호 책임자들에 대한 설문조사에서도 개인정보 침해 위험 및 개인정보보호 체계와 관련한 사항을 조사하였다.

우선 과거 개인정보 침해 사고가 발생한 적이 있는지를 조사한 결과 개인정보 침해 사고가 발생하지 않았다고 응답한 경우가 76명 중 69명(90.8%)으로 나타났다. 그리고 공사기관을 비교한 결과 공공기관의 개인정보 침해사고 발생 비율은 45명 중 1명으로 2.2%, 민간기업은 31명 중 6명으로 19.4%로 나타났다.

개인정보 침해사고는 일상적으로 발생하면 당연히 안되는 것이기 때문에 민간기업의 침해사고 발생비율 19.4%는 심각한 수준이라고 할 수 있다. 개인정보 침해사고가 사실상 발생하지 말아야 할 일이고, 개인정보보호 책임자들의 답변이 보수적으로 이루어질 가능성까지 고려하면, 전체적으로 거의 10%에 가까운 기관/기업에서 개인정보 침해사고가 발생한 적이 있다는 사실은 개인정보 침해사고가 빈발하고 있음을 말해준다. 특히, 민간기업의 경우 5개 중 1개에서 개인정보 침해사고가 발생한 것으로 나타난 것은 매우 심각한 상황임을 의미한다.

<표 4-22> 개인정보 침해사고의 발생 여부

| 개인정보 침해사고 발생 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 1 | 44 | 45 |
| | % | 2.2% | 97.8% | 100.0% |
| 민간기업 | 빈도 | 6 | 25 | 31 |
| | % | 19.4% | 80.6% | 100.0% |
| 전체 | 빈도 | 7 | 69 | 76 |
| | % | 9.2% | 90.8% | 100.0% |

정보주체로부터 개인정보 침해신고를 받은 적이 있는지에 대해서는 '아니다'라는 응답이 82.9%로 압도적이었다. 이에 대해 공사기관을 비교하면 공공기관에서는 단지 6.7% 정도만 침해신고가 접수된데 비해, 민간기업의 경우에는 31명 중 10명, 즉 1/3 가량인 32.1%가 개인정보 침해신고를 받은 적이

있다고 대답하여 상대적으로 민간기업에서 개인정보 침해사례가 많은 것으로 나타났다. 이는 아무래도 일반 시민들이 민간기업과 일상적인 관계를 가지는 경우가 많기 때문인 것으로 추측할 수 있다.

<표 4-23> 개인정보 침해신고 접수 여부

| 개인정보 침해신고 접수 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 3 | 42 | 45 |
| | % | 6.7% | 93.3% | 100.0% |
| 민간기업 | 빈도 | 10 | 21 | 31 |
| | % | 32.3% | 67.7% | 100.0% |
| 전체 | 빈도 | 13 | 63 | 76 |
| | % | 17.1% | 82.9% | 100.0% |

개인정보 영향평가를 수행하고 있는지 여부에 대해서는 75개 기관 중 40개 기관이 영향평가를 수행하고 있지 않다고 응답하여 과반수를 넘었다(53.3%). 하지만 개인정보 영향평가를 수행하고 있다는 응답이 46.7%나 되어 예상보다 매우 높게 나왔다. 여기에서 응답자들이 답변한 '개인정보 영향평가'가 어느 수준에서 이루어지는 것인지에 대해 좀 더 세부적인 평가가 필요할 듯하다. 즉, 영향평가의 대상은 무엇인지, 누가 영향평가를 수행하는지, 어떠한 단계에서 영향평가를 하는지, 영향평가의 방식은 무엇인지, 그 결과는 어떻게 반영되고 있는지 등에 대해 면밀한 조사가 요구된다는 것이다.

<표 4-24> 개인정보 영향평가 수행 여부

| 개인정보 영향평가 수행 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 19 | 26 | 45 |
| | % | 42.2% | 57.8% | 100.0% |
| 민간기업 | 빈도 | 16 | 14 | 30 |
| | % | 53.3% | 46.7% | 100.0% |
| 전체 | 빈도 | 35 | 40 | 75 |
| | % | 46.7% | 53.3% | 100.0% |

공사기관을 비교한 결과에서는 커다란 차이는 나지 않았지만, 민간기업의 경우 공공기관보다 개인정보 영향평가를 수행한다고 응답한 비율이 높았다

(공공기관 42.2%, 민간기업 53.3%). 이는 정보통신부가 2005년에 「기업의 개인정보 영향평가 수행을 위한 가이드」를 배포하여 대량의 개인정보를 수집·이용하는 기업에 대해 개인정보 영향평가를 하도록 권하고 있었던 것도 영향을 미쳤다고 볼 수 있다.

개인정보관리 책임자 및 개인정보관리 담당자는 응답한 76개 기관 모두 가지정되어 있었다. 개인정보관리 담당자는 실제 개인정보 보호 업무를 담당하는 사람을 말하는데, 이들 개인정보관리 담당자가 실제 역할을 제대로 하고 있는지 여부를 살펴보기 위해 개인정보관리담당자의 경우 개인정보 보호에 관한 업무 이외에 하는 별도의 업무가 있는지를 조사하였다. 그 결과 89.5%가 '그렇다'고 응답하여 개인정보관리 담당자의 대부분이 개인정보 보호업무와 함께 별도의 업무를 함께 수행하고 있는 것으로 나타났다. 공사기관을 비교해보면 공공기관의 겸업 비율이 93.3%로 민간기업의 겸업 비율 83.9%보다 더 높아서, 공공기관의 경우에 개인정보 보호업무가 독자적인 업무로 취급되는 경우가 더 적은 것으로 나타났다. 한편 개인정보관리 책임자나 담당자가 개인정보 보호업무만을 독자적으로 수행하는 기관을 살펴보면 정부중앙부처가 22곳 중 1곳, 교육기관이 11곳 중 2곳, 금융권이 4곳 중 1곳, 포털 등의 부가통신서비스 사업자가 14곳 중 3명, 준용사업자가 7곳 중 1곳으로 나타났다. 교육기관, 금융권, 포털 등에서 개인정보 보호업무를 독자적으로 수행하는 비율이 높은 것은 업무의 성격이 영향을 미친 것으로 보인다.

<표 4-25> 개인정보 보호업무 이외의 별도 업무수행 여부

| 개인정보관리 담당자의 개인정보 보호업무 이외의 별도 업무수행 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 42 | 3 | 45 |
| | % | 93.3% | 6.7% | 100.0% |
| 민간기업 | 빈도 | 26 | 5 | 31 |
| | % | 83.9% | 16.1% | 100.0% |
| 전체 | 빈도 | 68 | 8 | 76 |
| | % | 89.5% | 10.5% | 100.0% |

그렇다면 개인정보관리 담당자가 개인정보 보호에 관한 업무와 별도의 업무를 모두 하고 있는 경우 두 업무 중에서 주된 업무가 무엇인지를 살펴볼 필요가 있었다. 그래서 이를 조사한 결과, 개인정보 보호에 관한 업무가 주된

업무라고 답한 사람은 68명 중에서 22명으로 32.4%였다.[304] 특히 민간기업에서 개인정보관리 담당자의 주된 업무가 개인정보 보호인 경우는 26명 중 6명으로 23.1%에 불과하였다. 이는 그 만큼 민간기업에서 개인정보 보호에 대한 관심이 낮음을 반증하는 것이다. 공공기관의 경우에도 42명 중 16명으로 40%가 되지 않았다.

<표 4-26> 개인정보 담당자의 주된 업무가 개인정보 보호업무인지 여부

| 개인정보관리 담당자의 주된 업무가 개인정보 보호업무인지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 16 | 26 | 42 |
| | % | 38.1% | 61.9% | 100.0% |
| 민간기업 | 빈도 | 6 | 20 | 26 |
| | % | 23.1% | 76.9% | 100.0% |
| 전체 | 빈도 | 22 | 46 | 68 |
| | % | 32.4% | 67.6% | 100.0% |

이를 소속기관별로 살펴보면 개인정보관리 담당자가 개인정보 보호업무를 포함하여 업무를 겸하는 경우 개인정보보호업무를 주된 업무로 하는 경우는 지방자치단체(13곳 중 6곳)와 교육기관(9곳 중 5곳)에서 그 비율이 높았을 뿐 나머지 기관들은 30%를 밑돌았다. 비록 소규모 기관이나 업체의 경우 겸업이 불가피하다고 하더라도, 전반적으로 개인정보 보호 업무를 부차적으로 취급하고 있는 것은 아닌지 우려된다.

<표 4-27> 소속기관별 개인정보보호업무의 주된 업무 정도

| 개인정보관리 담당자의 소속기관별 개인정보 보호업무의 주된 업무 정도 | 그렇다 | 아니다 | 전체 |
|---|---|---|---|
| 정부중앙부처 | 6 | 15 | 21 |
| 지방자치단체 | 6 | 7 | 13 |
| 교육기관 | 5 | 4 | 9 |
| 공기업 및 준정부기관 | 0 | 1 | 1 |
| 보건의료기관 | 0 | 2 | 2 |

304) 설문결과에서는 70명이었으나, 이 중 2명은 개인정보관리담당자가 개인정보 보호에 관한 업무 이외에 하는 별도의 업무가 없는 경우라서 분석에서 제외하였다.

| | | | |
|---|---|---|---|
| 금융권 | 1 | 2 | 3 |
| 통신사 | 0 | 2 | 2 |
| 포털등 부가통신서비스 사업자 | 3 | 8 | 11 |
| 준용사업자 | 1 | 5 | 6 |
| 전 체 | 22 | 46 | 68 |

개인정보관리담당자가 개인정보 보호 등 담당 업무를 맡은 기간을 물어본 결과 1.84년으로 조사되었다. 공공기관의 경우 평균 담당기간은 1.36년, 담당기간이 가장 긴 사람이 3년인데 반해, 민간기업의 경우 평균 담당기간이 2.64년, 담당기간이 가장 긴 사람이 6년으로 나타나 정보보호업무 수행을 위한 전문성 제고 면에서 상대적으로 민간기업이 더 나은 것으로 조사되었다. 하지만 앞선 설문에서 개인정보관리 담당자의 겸직이 광범위하게 행해지고 여기에서 개인정보 보호업무가 주된 업무인 비율이 낮음을 감안한다면, 각 기관/기업에서 개인정보 담당업무의 경우에는 상대적으로 전문적인 영역으로 자리잡지 못하고 부차적인 업무로 취급되고 있다고 말할 수 있겠다.

개인정보관리담당자가 개인정보 보호 등 담당 업무와 관련한 교육을 받았는지에 대해서는 '그렇다'는 응답이 73명 중 62명(84.9%)으로 나타났고, '아니다'라는 답변은 11명(15.1%)에 불과했다. 공사기관 비교에서는 공공기관이 45명 중 41명(91.1%)으로 민간기업의 경우 응답한 28명 중 21명(75.0%)보다 그 이수 정도가 더 높은 것으로 조사되었다.

<표 4-28> 개인정보관리 담당자의 개인정보 보호 관련 교육 이수 여부

| 개인정보관리 담당자의 개인정보 보호 관련 교육 이수 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 41 | 4 | 45 |
| | % | 91.1% | 8.9% | 100.0% |
| 민간기업 | 빈도 | 21 | 7 | 28 |
| | % | 75.0% | 25.0% | 100.0% |
| 전체 | 빈도 | 62 | 11 | 73 |
| | % | 84.9% | 15.1% | 100.0% |

개인정보 보호 등 담당 업무와 관련된 교육을 이수한 경우 그 회수를 물은 결과 1회에서 10회까지 다양하게 나타났는데, 공공기관은 4회를 이수했다고

답한 경우가 10명으로 가장 많았고, 그 다음은 1회 이수로 8명이었다. 민간기업은 2회 이수가 6명으로 가장 많았고, 3회 이수가 5명으로 그 다음이었다.

개인정보 보호 등 담당 업무와 관련한 정보보호 교육을 실시한 기관을 모두 적시하도록 한 결과 공공기관과 민간기업이 다르게 나타났다. 공공기관의 경우에는 많은 사람들이 행정안전부나 한국정보보호진흥원을 교육기관으로 적시하였으며, 민간기업의 경우에는 한국정보보호진흥원을 적시한 경우가 가장 많았으며, 사내교육을 언급한 경우도 4곳이 있었다. 2009년 3월의 정부조직개편 결과 한국정보보호진흥원이 행정안전부의 소속기관이 되었고, 2009. 7월에 한국인터넷진흥원으로 통합 출범한 만큼 개인정보담당자들에 대해 개인정보 보호 등 담당 업무와 관련한 정보보호 교육을 실시한 기관은 행정안전부 한국인터넷진흥원으로 거의 일원화되었다고 할 수 있다.

이러한 개인정보 보호 등 담당 업무와 관련한 교육이 법적·기술적 전문성 확보에 도움을 주었는지 여부에 대해서는 그렇다는 응답이 61명 중 56명(91.8%), 아니라는 응답이 5명(8.2%)으로 나타났다. 이는 공공기관과 민간기업 사이에 별 차이가 나지 않았다.

<표 4-29> 개인정보 보호 관련 교육의 효과성

| 개인정보 보호 등 업무 관련 교육이 전문성 확보에 도움을 주었는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 37 | 3 | 40 |
| | % | 92.5% | 7.5% | 100.0% |
| 민간기업 | 빈도 | 19 | 2 | 21 |
| | % | 90.5% | 9.5% | 100.0% |
| 전체 | 빈도 | 56 | 5 | 61 |
| | % | 91.8% | 8.2% | 100.0% |

개인정보 보호교육을 받지 않은 개인정보보호 책임자들을 대상으로 이를 이수하지 않은 이유를 물은 결과 이 문항의 설문에 응한 6명은 '개인정보 보호교육이 있는 줄 몰라서', '개인정보 보호에 대해 잘 알고 있어서', '개인정보 보호교육이 필요하지 않다고 생각해서'에 각각 2명씩 응답하였다.

한편, 개인정보 보호에 관한 기관내 정책이나 규정 등을 직원들이 인지할 수 있도록 공개하고 있는지 여부에 대해서는 공공기관의 경우 전부 그렇다고 답하였고, 민간기업의 경우에는 31명 중 28명이 그렇다고 답하여, 전체적으

로 76명 중 73명(96.1%)이 긍정하였고, 공개하지 않고 있다고 답한 경우는 총 3명으로 3.9%에 불과했다.

<표 4-30> 개인정보 보호규정의 공개 여부

| 개인정보 보호에 관한 기관내 정책이나 규정 등을 직원들이 인지할 수 있도록 공개하고 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 전체 | 빈도 | 73 | 3 | 76 |
| | % | 96.1% | 3.9% | 100.0% |

기관의 전체적인 사업 계획 및 내용이 개인정보 보호 관련 법률·지침·가이드라인 및 내부 규정 등을 충실하게 반영하고 있는지 여부에 대해서도 76명 중 72명이 그렇다고 응답하여 대부분의 기관에서 개인정보보호 관련 법률·지침·가이드라인 등을 반영하여 소속기관의 사업 계획 및 내용이 수립된다고 하였다.

<표 4-31> 개인정보 보호 관련 규정의 충실한 반영 여부

| 기관 사업 계획 및 내용에 개인정보 보호 관련 규정 등의 충실한 반영 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 43 | 2 | 45 |
| | % | 95.6% | 4.4% | 100.0% |
| 민간기업 | 빈도 | 29 | 2 | 31 |
| | % | 93.5% | 6.5% | 100.0% |
| 전체 | 빈도 | 72 | 4 | 76 |
| | % | 94.7% | 5.3% | 100.0% |

조직 내 개인정보 보호정책이 개인정보보호 관련 법령의 제·개정, 보안기술의 발전 등에 따라 수시로 변경되고 공개되는지 여부에 대해서도 긍정하는 비율이 높았는데, 76명 중 68명이 '그렇다'고 답변하였고(89.5%), 8명이 '아니다'라고 답변하였다(10.5%). 그리고 공사기관을 비교한 결과 공공기관의 긍정 비율이 93.3%로 민간기업의 83.9%보다 높게 나타났다. 이를 공공기관의 개인정보 보호정책이 대외적으로 영향력을 미치기 때문에 수시로 변경·공개할 필요성이 그 만큼 크게 나타난 결과라고 볼 수도 있겠지만, 민간기업의 경우에도 정부의 법적 규제를 받기 때문에 민감하게 반응할 수 있다는 점

에서, 이러한 설문조사 결과는 앞 장들에서 수행한 실태조사와는 다소 괴리가 있다고 본다. 물론 실태조사 대상 기관과 설문 응답자의 소속 기관이 다르다는 점을 고려해야겠지만, 이번 실태조사의 대상이 되었던 지방자치단체나 공공병원 등의 경우 개인정보파일대장과 홈페이지의 개인정보보호정책에서 법령의 제·개정 상황을 제때 반영하지 않은 기관이 많았기 때문이다. 이 점에서 설문조사 응답자들이 '그래야 한다'는 당위론적 인식이 '그렇다'라는 답변으로 표출되었을 가능성도 염두에 둘 필요가 있다.

<표 4-32> 개인정보 보호정책이 수시로 변경·공개되는지 여부

| 개인정보 보호정책이 수시로 변경·공개되는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 42 | 3 | 45 |
| | % | 93.3% | 6.7% | 100.0% |
| 민간기업 | 빈도 | 26 | 5 | 31 |
| | % | 83.9% | 16.1% | 100.0% |
| 전체 | 빈도 | 68 | 8 | 76 |
| | % | 89.5% | 10.5% | 100.0% |

## 2. 개인정보 수집단계에서 발생할 수 있는 개인정보 침해 문제와 관련한 사항

정보통신부·한국정보보호진흥원(2005)의 「기업의 개인정보 영향평가 수행을 위한 가이드」는 개인정보 영향평가 기준(점검표)에서 개인정보의 수집과 관련하여 다음의 원칙을 피력하면서 이에 따른 평가 항목을 제시하고 있다.

- 개인정보의 수집은 사업목적을 달성하는데 필요한 최소한의 범위 내로 제한되어야 한다.
- 개인정보는 공정하고 합법적인 방법으로 수집되어야 한다.
- 개인정보를 수집할 때에는 반드시 정보주체의 동의를 얻어야 한다. 그러나, 정보주체가 만14세 미만 아동인 경우에는 부모 등 법정대리인의 동의를 얻어야 한다.
- 개인정보 수집에 대한 동의를 얻을 때에는 미리 개인정보의 수집·이용목적, 제3자 제공에 관한 사항 등 법률의 규정에 의한 의무고지사항을

당해 정보주체에게 명확히 고지하여야 한다. 이러한, 고지의무는 개인정보보호를 위한 가장 기본적인 사항이므로 반드시 준수되어야 한다.

- 개인정보의 처리(수집・이용・제공・보관 및 파기 등에 관한 사항을 포함한다)에 관한 기업 내부 방침을 정보주체에게 알리기 위해 『개인정보보호방침』을 공개하여야 한다. 『개인정보보호방침』은 기업이 「정보통신망법」에서 규정하고 있는 의무고지사항 외에(또는 고지사항을 포함하여) 개인정보의 처리에 대한 자사의 전반적인 방침을 알리기 위해 스스로 마련한 규정을 말한다.

개인정보 수집・유통 실태 파악을 위해 개인정보보호 책임자를 대상으로 한 이번 설문조사에서는 이러한 개인정보 수집의 원칙과 평가 항목을 반영하여 설문문항을 작성하였다.

우선 소속기관이 '사업목적 달성에 필요한 최소한의 개인정보만을 수집하는지 여부'에 대해 조사한 결과 76명 중 74명이 '그렇다'고 하여 대부분의 기관에서 최소한의 개인정보만을 수집하고 있다고 답변하였다. 이것이 개인정보 수집・유통의 실태를 정확하게 반영한다면 바람직한 일이나, 이러한 결과가 개인정보보호 책임자들의 개인정보 수집에 대한 실태가 아니라 인식을 반영한 것일 가능성이 높고, 나아가 기관에 개인정보를 제공한 정보주체가 그러하다고 인식하고 있는지는 별개라는 점에 유의할 필요가 있다. 실제로 앞 장들에서 나타난 바와 같이 실태조사 결과 서비스 제공에 필요한 정도 이상의 개인정보를 수집하는 기관・기업들이 많았다.

<표 4-33> 최소한의 개인정보만 수집 여부

| 사업목적 달성에 필요한 최소한의 개인정보만 수집 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 45 | 0 | 45 |
| | % | 100.0% | 0.0% | 100.0% |
| 민간기업 | 빈도 | 29 | 2 | 31 |
| | % | 93.5% | 6.5% | 100.0% |
| 전체 | 빈도 | 74 | 2 | 76 |
| | % | 97.4% | 2.6% | 100.0% |

이에 구체적으로 'CCTV, 지문·홍채·유전정보 등 생체정보, 병력, 종교·정당 가입 여부 등 정보주체의 민감한 개인정보가 수집'되고 있는지를 조사하였다. 조사 결과 민감정보를 수집한다는 응답이 76명 중 19명(25.0%), 민감정보를 수집하지 않는다는 응답이 57명(75.0%)로 나타나, 정보주체의 민감한 개인정보가 수집되는 비율이 1/4에 이르렀다. 특히 민간기업은 민감정보의 수집 비율이 9.7%인데 비해, 공공기관은 45명 중 16명(35.6%)이 민감정보를 수집하고 있다고 응답하여 공공기관의 민감정보 수집 비율이 더 높았다. 민간기업보다는 공공기관에서 정보주체의 민감한 개인정보 수집이 불가피한 경우가 더 많을 수도 있고, 특히 공공기관의 경우 CCTV 영상정보나 의료정보를 수집하고 있을 가능성이 높기 때문에 민감정보 수집 비율이 높게 나온 것으로 짐작할 수 있다.

<표 4-34> 정보주체의 민감한 개인정보 수집 여부

| 정보주체의 민감한 개인정보 수집 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 16 | 29 | 45 |
| | % | 35.6% | 64.4% | 100.0% |
| 민간기업 | 빈도 | 3 | 28 | 31 |
| | % | 9.7% | 90.3% | 100.0% |
| 전체 | 빈도 | 19 | 57 | 76 |
| | % | 25.0% | 75.0% | 100.0% |

민감한 개인정보의 대표적인 예로서 '정보주체의 주민등록번호를 수집하고 있다'고 응답한 경우는 76명 중 62명(81.6%)이었고, 수집하고 있지 않다고 응답한 경우는 14명(18.4%)이었다. 주민등록번호 수집 비율은 공공기관이 75.6%, 민간기업이 90.3%로 공공기관보다 민간기업에서 더 높은 것으로 나타났다. 이는 민간영역에서 주민등록번호의 이용을 제한하려는 노력이 있기는 하지만, 여전히 대부분의 민간기업에서 주민등록번호를 수집하고 있음을 보여준다.

<표 4-35> 정보주체의 주민등록번호 수집 여부

| 정보주체의 주민등록번호 수집 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 34 | 11 | 45 |
| | % | 75.6% | 24.4% | 100.0% |
| 민간기업 | 빈도 | 28 | 3 | 31 |
| | % | 90.3% | 9.7% | 100.0% |
| 전체 | 빈도 | 62 | 14 | 76 |
| | % | 81.6% | 18.4% | 100.0% |

‘개인정보 수집항목을 정보주체가 필수사항과 선택사항으로 구분하여 기재할 수 있도록 절차나 시스템이 구성되어 있는지 여부’에 대해서는 76명 중 60명이 ‘그렇다’고 응답하였고(78.9%), 16명이 ‘아니다’고 응답하였다(21.1%). 특히 민간기업의 경우 31명 중 28명(90.3%)이 개인정보 수집항목을 구분하고 있다고 하여 정보주체의 개인정보 수집을 최소화하는데 있어서 공공기관보다 더 노력하고 있다고 답변했다. 이러한 결과는 공공기관의 경우 특정 사업에 필요하다고 기관이 인식하는 정보들을 모두 필수사항에 포함시키는 반면, 민간기업의 경우에는 법적 규제로 인해 필수사항에 포함시킬 수 있는 개인정보에 한계가 있기는 하지만, 기업 활동을 위해 가능한 많은 개인정보를 필요로 하므로 선택사항으로라도 개인정보를 수집하려고 노력하고 있기 때문이라고 짐작할 수 있다.

<표 4-36> 개인정보 수집항목을 구분하는 절차·시스템의 구성 여부

| 개인정보 수집항목을 정보주체가 구분하여 기재하는 절차·시스템의 구성 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 32 | 13 | 45 |
| | % | 71.1% | 28.9% | 100.0% |
| 민간기업 | 빈도 | 28 | 3 | 31 |
| | % | 90.3% | 9.7% | 100.0% |
| 전체 | 빈도 | 60 | 16 | 76 |
| | % | 78.9% | 21.1% | 100.0% |

## 3. 개인정보의 이용・제공・공유, 보유 및 파기 등과 관련한 사항

개인정보는 정보주체의 동의가 있거나 법률의 규정에 의한 경우를 제외하고는 사전에 정보주체에게 고지한 수집・이용목적 외의 다른 목적으로 사용되거나 타인에게 제공・공유・판매되어서는 아니 된다. 개인정보의 이용 및 제공 등에 대해 정보주체의 추가적인 동의가 필요한 수집・이용목적의 변경인지 여부를 판단할 경우에는 정보주체의 합리적인 기대감이 고려되어야 한다. 예를 들면, 정보주체는 물품배송을 위해 제공한 전화번호가 신상품 광고를 위한 마케팅 목적으로 이용될 것이라고는 기대하지 않을 것이기 때문이다(정보통신부・한국정보보호진흥원, 2005: 40). 「공공기관의 개인정보보호에 관한 법률」 제10조제1항도 개인정보파일은 다른 '법률'에 따라 보유기관 내부 또는 보유기관 외의 자에 대하여 이용하게 하거나 제공하는 경우를 제외하고는 당해 개인정보파일의 보유목적 외의 목적으로 처리정보가 이용되거나 제공되어서는 아니 된다고 규정하고 있다. 보유정보를 다른 기관에 제공하고자 할 때에는 문서를 통해 보유목적, 범위 등을 확인하여야 하는데, 최소한의 범위로 제한하여 제공하고, 보유기관의 동의 없이 제3자에게 이용・제공할 수 없도록 조치해야 한다(행정안전부, 2009d: 5-6).

이와 관련하여 '개인정보 수집 시 고지하거나 이용약관에 명시한 목적 범위를 넘어 개인정보를 이용하거나 제3자에게 제공하는 경우 정보주체로부터 추가적인 동의를 받는 절차와 방법이 마련되어 있는지 여부'를 조사한 결과 '그렇다'는 응답은 73명 중 65명(89.0%), '아니다'라는 응답은 8명(11.0%)으로 나타났다. 특히 공공기관에서는 '그렇다'는 응답이 44명 중 37명으로 84.1%인 반면, 민간기업의 경우에는 응답자 29명 중 1명을 제외하고 28명이 개인정보의 목적 외 이용이나 제3자 제공시 추가적인 동의 절차・방법을 마련하고 있다고 답변하였다(96.6%). 이러한 결과는 공공기관의 경우 정보주체의 동의보다는 법적 근거에 의해 개인정보의 수집・제3자 제공이 이루어지기 때문에 민간기업보다 상대적으로 그 비율이 낮게 나온 것이라고 볼 수 있으며, 또한 민간기업의 경우 개인정보의 목적 외 이용이나 제3자 제공 문제로 인해 논란이 된 경우가 많았기 때문에 그 만큼 신경쓰고 있음을 보여주는 것이지만, 제2, 3장에서 분석했던 것처럼 개인정보의 목적 외 이용이나 제3자 제공의 범위를 축소하여 파악한 결과일 수도 있다는 점을 유의해야 한다.

<표 4-37> 개인정보의 목적외이용이나 제3자제공시 동의절차·방법 마련여부

| 개인정보의 목적 범위를 넘는 이용이나 제3자 제공시 정보주체로부터 추가적인 동의를 받는 절차·방법 마련 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 37 | 7 | 44 |
| | % | 84.1% | 15.9% | 100.0% |
| 민간기업 | 빈도 | 28 | 1 | 29 |
| | % | 96.6% | 3.4% | 100.0% |
| 전체 | 빈도 | 65 | 8 | 73 |
| | % | 89.0% | 11.0% | 100.0% |

개인정보의 수집목적 또는 제공받은 목적을 달성하여 해당 개인정보의 보유가 불필요하게 된 경우에는 당해 개인정보를 지체 없이 파기하여야 한다. 다만, 법률에 보존해야 할 정보나 보유기간을 정하고 있는 경우에는 예외가 인정된다(정보통신부·한국정보보호진흥원, 2005: 43). 공공기관의 경우 개인정보처리부서의 장은 해당 파기사항에 대해 입출력자료관리대장에 개인정보파일명과 주요기록항목, 폐기일, 처리담당자성명, 처리부서장을 기재하여 관리해야 한다. 다만, 다른 법령에 따라 보존이 필요한 경우 파기하지 않을 수 있다.

이에 '개인정보를 타기관에 제공할 경우에는 사용목적이 다했을 때 즉시 폐기토록 하고 있는지 여부'에 대해 조사하였는데, 73명 중 72명(98.6%)이 '그렇다'고 하여 제3자 제공 정보의 폐기 관리에 대해서는 대부분이 폐기하고 있다고 답변하였다.

<표 4-38> 제3자 제공 정보의 폐기관리

| 개인정보의 타기관 제공시 사용목적이 다했을 때 즉시 폐기토록 하고 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 전체 | 빈도 | 72 | 1 | 73 |
| | % | 98.6% | 1.4% | 100.0% |

그리고 '제3자 제공내역이 대장 등에 기록·보관되고 있는지 여부'에 대해서도 71명 중 68명이 '그렇다'(95.8%)고 응답하여 대부분의 기관이 제3자 제공내용을 기록·보관하고 있는 것으로 나타났다.

<표 4-39> 제3자 제공내역이 대장 등에 기록·보관되고 있는지 여부

| 제3자 제공내역이 대장 등에 기록·보관되고 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 43 | 1 | 44 |
| | % | 97.7% | 2.3% | 100.0% |
| 민간기업 | 빈도 | 25 | 2 | 27 |
| | % | 92.6% | 7.4% | 100.0% |
| 전체 | 빈도 | 68 | 3 | 71 |
| | % | 95.8% | 4.2% | 100.0% |

‘개인정보의 열람·출력에 대한 기록이 시스템에 자동 저장되거나 수기로 대장에 기록·보관되고 있는지 여부’는 75명 중 60명이 ‘그렇다’고 응답한 반면(80.0%), ‘아니다’라고 응답한 경우는 15명으로 20.0%였다. 공사기관을 비교해보면, 민간기업의 경우 개인정보 열람·출력기록이 저장·보관되고 있는 비율이 30명 중 20명으로 66.7%로 나타나, 공공기관의 88.9%에 비해 낮았다. 이는 공공기관의 경우 법령이나 지침으로 개인정보 열람·출력기록의 저장·보관을 규정하고 있기 때문으로 보인다. 그러나 개인정보에 대한 무단 열람이나 불법 열람이 사회적으로 이슈화되고 있는 상황이기 때문에, 향후에 민간기업에서도 이러한 무단 열람을 방지하기 위한 장치를 마련해나가야 할 것이다.

<표 4-40> 개인정보 열람·출력기록의 저장·보관 여부

| 개인정보의 열람·출력에 대한 기록이 시스템에 자동 저장되거나 수기로 대장에 기록·보관되고 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 40 | 5 | 45 |
| | % | 88.9% | 11.1% | 100.0% |
| 민간기업 | 빈도 | 20 | 10 | 30 |
| | % | 66.7% | 33.3% | 100.0% |
| 전체 | 빈도 | 60 | 15 | 75 |
| | % | 80.0% | 20.0% | 100.0% |

‘회원탈퇴, 서비스기간 종료, 본인정보 삭제 요청 등이 있는 때에 관련법령에 의해 보유해야 하는 경우를 제외하고는 지체 없이 해당 개인정보를 파기하고 있는지’에 대해서도 1곳을 제외한 모든 기관에서 지켜지고 있다고 답변하였다. 하지만 이 역시 앞 장에서 보고된 실태조사 결과와는 약간 괴리가 있다. 지난 2008년 상당수의 포털, 초고속인터넷업체, 이동통신사 등이 해지정보의 미파기로 인해 방송통신위원회의 시정조치를 받은 바 있다. 물론 본 설문조사는 그 이후에 이루어졌기 때문에 어느 정도 시정이 이루어진 상황을 반영하였다고 볼 수는 있으나, 해지자의 정보 파기가 개인정보보호 책임자들의 설문 응답과 같이 이루어지고 있는지는 의문이다. 어느 정도는 답변 속에 응답자의 당위론적 인식이 반영된 것으로 보인다.

<표 4-41> 목적 달성 시 해당 개인정보의 파기 여부

| 목적 달성 시 해당 개인정보의 파기 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 전체 | 빈도 | 75 | 1 | 76 |
| | % | 98.7% | 1.3% | 100.0% |

## 4. 개인정보 처리의 위탁 등과 관련한 사항

개인정보의 처리 등을 직접 수행하지 않고 외부 업체의 위탁을 통해 수행하는 경우에는 이러한 사실을 정보주체에게 미리 고지하여야 한다. 여기에서 ‘위탁’이란 계약의 형태와 종류를 불문하고 기업이 타인에게 개인정보 취급의 전부 또는 일부를 대행하게 하는 것을 내용으로 하는 계약을 말하며, 위탁의 예로는 대리점, 콜센터, AS센터 등이 있다. 위탁계약의 내용은 개인정보의 유출 방지를 비롯하여 개인정보 보호조치가 확보되도록 정함과 동시에 개인정보 침해사고 발생 시 책임관계를 명확하게 규정하여야 한다(정보통신부·한국정보보호진흥원, 2005: 41-42).

이에 개인정보의 처리 등을 직접 수행하지 않고 외부 업체의 위탁을 통해 수행하는 경우 ‘위탁 처리되는 개인정보가 안전하게 관리될 수 있도록 위탁업무의 범위 내에서 개인정보 보호 교육 등 수탁기관에 대한 적절한 관리·통제시스템이 구축되어 있는지 여부’를 조사한 결과 응답한 32명 중에서 26명이 ‘그렇다’고 응답하여 81.3%가 수탁기관에 대한 적절한 관리·통제시스템이 구축되어 있다고 하였고, ‘아니다’라고 응답한 경우는 6명(18.7%)이었다.

<표 4-42> 수탁기관에 대한 적절한 관리·통제시스템의 구축 여부

| 위탁 처리되는 개인정보가 안전하게 관리될 수 있도록 위탁 업무의 범위 내에서 수탁기관에 대한 적절한 관리·통제시스템의 구축 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 12 | 3 | 15 |
| | % | 80.0% | 20.0% | 100.0% |
| 민간기업 | 빈도 | 14 | 3 | 17 |
| | % | 82.4% | 17.6% | 100.0% |
| 전체 | 빈도 | 26 | 6 | 32 |
| | % | 81.3% | 18.7% | 100.0% |

‘위탁관리자 및 운영자 등에 대해 정기적으로 개인정보보호 관련 교육을 시행하고 있는지’에 대해서는 32명 중 22명이 ‘그렇다’(68.8%)고 응답한 반면, 10명은 ‘아니다’(31.2%)라고 응답하였다. 특히 위탁관리자 및 운영자 등에 대한 정기적인 개인정보보호 관련 교육은 민간기업에서 시행되는 비율(58.8%)보다 공공기관에서 시행되는 비율이 80.0%로 더 높았다. 이는 행정안전부 등 상급부처에서 공공기관에서 개인정보보호 관련 교육이 정기적으로 시행되는지를 점검하고 있기 때문인 것으로 짐작된다.

<표 4-43> 위탁관리자 등에 대한 개인정보 보호 관련 교육 시행 여부

| 위탁관리자 등에 대한 정기적인 개인정보 보호 관련 교육 시행 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 12 | 3 | 15 |
| | % | 80.0% | 20.0% | 100.0% |
| 민간기업 | 빈도 | 10 | 7 | 17 |
| | % | 58.8% | 41.2% | 100.0% |
| 전체 | 빈도 | 22 | 10 | 32 |
| | % | 68.8% | 31.2% | 100.0% |

위의 설문에서 위탁관리자 등에게 개인정보 보호 관련 교육을 실시하지 않고 있는 기관의 개인정보보호 책임자 10명에게 ‘위탁관리자 등에게 교육을 하지 않는 이유’를 질문한 결과, 공공기관의 경우 ‘수탁기관 직원에 대한 보안교육 사항이 마련되어 있어서’가 1명, ‘현재의 관리적·기술적 보호조치로 충분해서’가 1명, ‘행정안전부 또는 자체적으로 수시교육을 실시하고 있어서’

가 1명으로 나타났다. 민간기업의 경우에는 '수탁기관이 기본적인 사항을 파악하고 있어서'가 3명으로 가장 많았고, '수탁기관 직원에 대한 보안교육 사항이 마련되어 있어서'가 1명, '현재의 관리적·기술적 보호조치로 충분해서'가 2명으로 파악되었으며, '위탁사업자에게 교육하는 것에 대한 사항 자체를 인지하지 못하고 있다'는 응답도 1명 있었다. 한편, '수탁기관 또는 협력기관 등에서 접근할 수 있는 개인정보의 범위가 명확하게 정의되고 문서화되어 있는지 여부'를 묻는 질문에 대해서는 '그렇다'는 응답이 32명 중 28명으로 87.5%, '아니다'라는 응답이 4명(12.5%)으로 나타났다.

<표 4-44> 수탁기관 등의 접근가능 개인정보 설정 여부

| 수탁기관 등에서 접근할 수 있는 개인정보 범위의 명확한 정의·문서화되어 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 13 | 2 | 15 |
| | % | 86.7% | 13.3% | 100.0% |
| 민간기업 | 빈도 | 15 | 2 | 17 |
| | % | 88.2% | 11.8% | 100.0% |
| 전체 | 빈도 | 28 | 4 | 32 |
| | % | 87.5% | 12.5% | 100.0% |

'개인정보 처리의 위탁 종료 시 수탁기관으로부터 개인정보를 회수·파기하는 절차를 수립하여 적용하고 있는지 여부' 또한 이와 비슷한 답변 결과가 나왔다. 32명 중 29명(90.6%)이 그렇다고 답한 것이다.

<표 4-45> 위탁 종료 시 수탁기관의 개인정보 회수·파기 절차 수립 여부

| 개인정보 처리의 위탁 종료 시 수탁기관의 개인정보 회수·파기 절차 수립·적용 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 13 | 2 | 15 |
| | % | 86.7% | 13.3% | 100.0% |
| 민간기업 | 빈도 | 16 | 1 | 17 |
| | % | 94.1% | 5.9% | 100.0% |
| 전체 | 빈도 | 29 | 3 | 32 |
| | % | 90.6% | 9.4% | 100.0% |

‘개인정보관리 위탁시 수탁기관의 개인정보 처리과정에 대한 정기 감사를 실시하고 있는지 여부’에 대해서는 32명 중 22명이 ‘그렇다’(68.8%)고 응답한 반면, 10명은 ‘아니다’(31.2%)라고 응답하였다. 특히 수탁기관의 개인정보 처리과정에 대한 정기 감사는 민간기업에서 실시되는 비율(58.8%)보다 공공기관에서 실시되는 비율이 80.0%로 더 높았다. 이는 공공기관의 경우 수탁기관의 개인정보 처리과정에 대한 정기 감사 실시를 법령 등에서 규정하고 있기 때문인 것으로 생각된다.

<표 4-46> 수탁기관의 개인정보 처리과정에 대한 정기 감사 실시 여부

| 개인정보관리 위탁 시 수탁기관의 개인정보 처리과정에 대한 정기 감사 실시 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 12 | 3 | 15 |
| | % | 80.0% | 20.0% | 100.0% |
| 민간기업 | 빈도 | 10 | 7 | 17 |
| | % | 58.8% | 41.2% | 100.0% |
| 전체 | 빈도 | 22 | 10 | 32 |
| | % | 68.8% | 31.2% | 100.0% |

## 5. 정보주체의 권리보장 조치와 관련한 사항

정보주체에게는 자신의 개인정보를 열람하거나 잘못된 정보를 정정할 수 있는 권리가 보장되어야 한다.

‘개인정보취급방침을 변경할 경우 미리 전자우편으로 통지하거나 웹사이트 공지사항 등을 통해 정보주체가 개인정보보호방침의 변경을 알 수 있도록 조치를 취하고 있는지’에 대해 조사한 결과 민간기업의 개인정보보호 책임자들은 모두 ‘그렇다’고 응답한 반면, 공공기관의 개인정보보호 책임자들은 45명 중 35명(77.8%)이 ‘그렇다’고 응답하고, 10명(22.2%)은 ‘아니다’라고 응답하였다. 이는 개인정보취급방침의 변경 통지 대상에서 공사기관 사이에 차이가 있기 때문인 것으로 보인다. 즉 민간기업의 경우에는 방침이 변경될 경우 통지해야 할 대상 회원이 있지만, 공공기관의 경우에는 특정 사업대상 집단이 있는 것이 아니라 전체 국민을 대상으로 하고 있기 때문이다. 공공기관에서 ‘그렇다’라고 답변을 한 것은 관련된 조치를 홈페이지를 통한 공지로 파악하고 답변했을 것으로 보인다.

<표 4-47> 개인정보취급방침 변경의 통지 여부

| 개인정보취급방침 변경 시 정보주체가 이를 알 수 있도록 조치를 취하고 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 35 | 10 | 45 |
| | % | 77.8% | 22.2% | 100.0% |
| 민간기업 | 빈도 | 31 | 0 | 31 |
| | % | 100.0% | 0.0% | 100.0% |
| 전체 | 빈도 | 66 | 10 | 76 |
| | % | 86.8% | 13.2% | 100.0% |

‘정보주체가 자신의 개인정보를 스스로 열람·정정할 수 있는 절차’는 민간기업의 1명을 제외하고 75명 중 74명(공공기관 44명, 민간기업 30명)이 마련되어 있다고 응답하였다(98.7%).

<표 4-48> 정보주체의 개인정보 열람·정정절차 수립 여부

| 정보주체의 개인정보 열람·정정 절차 수립 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 전체 | 빈도 | 74 | 1 | 75 |
| | % | 98.7% | 1.3% | 100.0% |

한편, 수집한 개인정보의 이용 및 제3자 제공 등에 대한 투명성 확보를 위해, 정보주체가 개인정보를 이용하거나 제3자에게 제공한 내역을 요구할 수 있는 절차가 마련되어야 한다. ‘정보주체가 자신의 개인정보에 대한 제3자 제공 내역을 요청할 수 있는 절차가 마련되어 있는지 여부’를 조사한 결과 73명 중 57명(78.1%)이 마련되어 있다고 응답하였고, 16명(21.9%)이 마련되어 있지 않다고 응답하였다. 하지만 이러한 설문조사 결과 역시 앞 장에서 행한 실태조사 결과와 괴리가 있다. 이번 실태조사에서 정보주체의 제3자 제공 내역에 대한 열람권은 전반적으로 제한이 되고 있는 것으로 나타났다. 예를 들어, 통신업체를 대상으로 한 열람청구에서도 상당수의 업체들이 제공을 거부하거나 개인정보취급방침을 확인하라고 답변하였던 것이다. 따라서 이 설문문항에서 개인정보보호 책임자들의 답변은 각 기관/업체의 개인정보보호정책이나 취급방침 등을 통해 개인정보 제3자 제공과 관련한 내용을 공개하고 있는 현실을 반영한 것으로 보인다.

<표 4-49> 정보주체의 제3자 제공 내역요청 절차 마련 여부

| 정보주체의 자신의 개인정보에 대한 제3자 제공 내역요청 절차 마련 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 36 | 8 | 44 |
| | % | 81.8% | 18.2% | 100.0% |
| 민간기업 | 빈도 | 21 | 8 | 29 |
| | % | 72.4% | 27.6% | 100.0% |
| 전체 | 빈도 | 57 | 16 | 73 |
| | % | 78.1% | 21.9% | 100.0% |

개인정보보호 책임자에게 '개인정보의 열람절차에 따른 개인정보 열람 청구를 처리한 경험이 있는지'를 조사한 결과 75명 중 18명만이 개인정보 열람 청구 처리 경험이 있다고 하였고(24.0%), 57명은 그런 경험이 없다고 하였다(76.0%). 특히 공공기관은 44명 중에 단지 2명만이 그렇다고 응답하여 개인정보 열람 청구 처리 경험이 별로 없는 것으로 나타난 반면(4.5%), 민간기업은 31명 중 16명(51.6%)이 개인정보 열람 청구 처리 경험이 있다고 응답하여 과반수가 넘었다.

앞의 일반 시민을 대상으로 한 설문조사에서도 개인정보 열람청구 경험이 있는 경우는 5.6%로 그다지 높지 않은 것으로 나왔다. 민간기업에서 개인정보 열람청구 처리 경험이 있는 경우가 51.6%로 나왔지만, 이는 그리 높은 수치가 아니다. 왜냐하면, 각 기업은 수많은 고객들을 상대하고 있기 때문에, 개인 고객 입장에서는 그러한 경험이 거의 없거나 낮을지라도, 기업 입장에서 보면 최소한 1번 이상은 열람청구 처리 경험을 할 수 있을 것이기 때문이다. 따라서 오히려 48.4%의 기업에서 개인정보보호 책임자가 열람청구 처리 경험이 없다는 것 자체에 초점을 둘 필요가 있다. 이는 개인정보 열람청구권이 일반 시민들에게 제대로 인식되지 않아 의미가 없는 상태에 있다는 것을 보여주고 있기 때문이다.

<표 4-50> 개인정보 열람청구 처리 경험 유무

| 개인정보 열람청구 처리 경험 유무 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 2 | 42 | 44 |
| | % | 4.5% | 95.5% | 100.0% |

| | | | | |
|---|---|---|---|---|
| 민간기업 | 빈도 | 16 | 15 | 31 |
| | % | 51.6% | 48.4% | 100.0% |
| 전체 | 빈도 | 18 | 57 | 75 |
| | % | 24.0% | 76.0% | 100.0% |

이와 관련하여 개인정보 열람청구 처리 경험이 있는 18명을 대상으로 '열람 청구를 처리한 후에 정보에 잘못이 있다 하여 정정·삭제청구를 받은 경험이 있는지 여부'를 조사하고자 했는데, 민간기업의 경우 개인정보 열람청구 처리 경험은 없으나 정정·삭제청구를 받은 경험이 있는 사람이 3명이 추가되었고, 개인정보 열람청구 처리 경험은 있으나 정정·삭제요청 경험 유무에는 답하지 않은 1명을 제외하여, 19명을 대상으로 검토하였다. 그 결과 19명 중에서 9명(47.4%)이 정정·삭제요청 경험이 있었고, 10명(52.6%)이 경험이 없었다.

<표 4-51> 열람청구 후 정정·삭제청구받은 경험 유무

| 열람 청구 처리 후 정보에 잘못이 있다 하여 정정·삭제청구를 받은 경험이 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 1 | 1 | 2 |
| | % | 50.0% | 50.0% | 100.0% |
| 민간기업 | 빈도 | 8 | 9 | 17 |
| | % | 47.1% | 52.9% | 100.0% |
| 전체 | 빈도 | 9 | 10 | 19 |
| | % | 47.4% | 52.6% | 100.0% |

'정보주체가 자신의 개인정보에 대한 정정을 요구하는 경우 이를 확인하고 당해 정보를 정정하기 전까지 개인정보가 이용되지 않도록 하는 절차의 마련'과 관련하여 73명 중 49명이 마련되어 있다고 응답하였고(67.1%), 24명이 마련되어 있지 않다고 응답하였다(32.9%). 이는 공공기관과 민간기업 사이에 큰 차이가 없었다.

<표 4-52> 정보주체의 개인정보 정정요구 후 정보 이용방지 절차 마련 여부

| 정보주체가 자신의 개인정보에 대한 정정 요구 시 이를 확인하고 당해 정보 정정 전까지 개인정보 이용방지 절차 마련 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 29 | 15 | 44 |
| | % | 65.9% | 34.1% | 100.0% |
| 민간기업 | 빈도 | 20 | 9 | 29 |
| | % | 69.0% | 31.0% | 100.0% |
| 전체 | 빈도 | 49 | 24 | 73 |
| | % | 67.1% | 32.9% | 100.0% |

한편, 민간기관을 대상으로 '정보주체가 동의철회(회원탈퇴, 서비스 이용계약 해지 등)를 하는데 관련 법령 또는 계약상에 일정한 제약이 있는지 여부'를 조사한 결과, 응답자 26명 중 제약이 있다는 응답이 7명(26.9%), 제약이 없다는 응답이 19명(73.1%)으로 나타나, 정보주체의 동의철회에 대한 제약은 별로 없다고 답변한 경우가 많았다. 하지만 실제 살펴보면 대부분의 기관과 업체들이 동의 철회에 제약이 있다. 이를테면 이용자가 대금을 미납한 경우 해지처리가 바로 되지 않을 텐데, 이러한 경우에도 제약이 없다고 답변했을 가능성이 높다는 것이다. 이 점에서 설문 구성 시 '제약'을 좀더 구체적으로 명확하게 했어야 한다는 아쉬움이 남는다.

<표 4-53> 정보주체의 동의철회에 대한 제약 유무

| 정보주체가 동의철회를 하는데 관련 법령 또는 계약상에 일정한 제약이 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 민간기업 | 빈도 | 7 | 19 | 26 |
| | % | 26.9% | 73.1% | 100.0% |

그리고 정보주체의 동의철회에 대한 제약이 있다고 응답한 경우, 이를 정보주체에게 미리 고지하거나 서비스 이용약관 등에 명시하고 있는지를 질문한 결과 7명 모두 다 그렇다고 답변하였다.

## 6. 개인정보 보호를 위한 인적 통제

개인정보보호를 위해서는 인적·물리적 보안 조치가 필요한데, 여기에서는 인적 통제를 중심으로 설문문항을 구성하였다.

우선 '정보시스템 설계부터 운영에 이르기까지 시스템 구축의 전 과정에 관련된 전산담당자에 대한 개인정보보호 교육 프로그램이 있는지 여부'에 대해 조사하였다. 이에 대해 '그렇다'고 응답한 사람이 76명 중 32명(42.1%)이었고, '아니다'라고 응답한 사람이 44명(57.9%)이었다. 공사기관을 비교해보면 공공기관의 경우 전산담당자에 대한 개인정보보호 교육 프로그램이 있다고 응답한 비율이 30%가 조금 넘는 수준인데 비해 민간기업의 경우에는 교육 프로그램이 있다고 응답한 비율이 60%가량 되었다. 그 만큼 민간기업에서 전산담당자에 대한 개인정보보호 교육에 관심을 보이고 있다고 해석할 수 있다.

<표 4-54> 전산담당자에 대한 개인정보보호 교육 프로그램 유무

| 시스템 구축 전 과정상의 전산담당자에 대한 개인정보보호 교육 프로그램이 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 14 | 31 | 45 |
| | % | 31.1% | 68.9% | 100.0% |
| 민간기업 | 빈도 | 18 | 13 | 31 |
| | % | 58.1% | 41.9% | 100.0% |
| 전체 | 빈도 | 32 | 44 | 76 |
| | % | 42.1% | 57.9% | 100.0% |

'정보주체의 개인정보를 다루고 있는 모든 직원에게 각 직무별로 특화된 교육시스템이 상세하게 마련되어 있는지 여부'에 대한 조사결과 또한 위의 조사 결과와 유사하게 나왔는데, 76명 중 24명(31.6%)만 각 직무별 특화된 교육시스템이 마련되어 있다고 응답하였다. 그리고 공사기관 비교에 있어서도 민간기업의 비율이 48.4%로 공공기관의 비율 20.0%보다 배가 넘었다.

<표 4-55> 각 직무별로 특화된 교육시스템 마련 여부

| 정보주체의 개인정보를 다루고 있는 모든 직원에게 각 직무별로 특화된 교육시스템이 상세하게 마련되어 있는지 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 9 | 36 | 45 |
| | % | 20.0% | 80.0% | 100.0% |
| 민간기업 | 빈도 | 15 | 16 | 31 |
| | % | 48.4% | 51.6% | 100.0% |
| 전체 | 빈도 | 24 | 52 | 76 |
| | % | 31.6% | 68.4% | 100.0% |

한편 76명 중 69명이 '정보주체의 개인정보에 대한 내부직원들의 접근 권한은 권한별 직무 범위에 차등을 두거나 데이터의 중요도 별로 각각 다른 ID/PW를 부여하는 등 구체적으로 설정되어 있다'고 하여(90.8%), 대부분의 기관에 접근권한별 차등 설정이 이루어지고 있었으며, 특히 공공기관의 경우 45명 중 2명(4.4%)을 제외한 43명(95.6%)이 '그렇다'고 응답하였다.

<표 4-56> 내부직원의 개인정보 접근권한 및 권한별 직무범위의 차등설정 여부

| 내부직원의 개인정보 접근권한 및 권한별 직무범위의 차등 설정 여부 | | 그렇다 | 아니다 | 전체 |
|---|---|---|---|---|
| 공공기관 | 빈도 | 43 | 2 | 45 |
| | % | 95.6% | 4.4% | 100.0% |
| 민간기업 | 빈도 | 26 | 5 | 31 |
| | % | 83.9% | 16.1% | 100.0% |
| 전체 | 빈도 | 69 | 7 | 76 |
| | % | 90.8% | 9.2% | 100.0% |

내부직원의 개인정보에 대한 접근권한 및 권한별 직무범위가 차등 설정되어 있지 않은 경우, 내부직원들의 개인정보 접근권한 및 권한별 직무 범위에 차등을 두지 않는 이유에 대해 '내부직원이 많지 않기 때문'이라는 응답이 1명, '개인정보 접근권한에 차등을 둘 만큼 많은 정보를 수집·이용하지 않기 때문'이라는 응답이 3명, 그리고 그밖에 개인정보를 직접 받고 있지 않기 때문이라거나, 업무의 효율성이 떨어진다는 이유를 제시하는 경우가 있었다.

# 제5장 결 론

## 제1절 연구결과

본 연구는 행정정보공동이용 및 수사/범죄경력 등 공공영역, 포털, 이동통신사, 초고속인터넷업체 등 통신 영역, 금융 영역, 보건의료 영역, 교육 영역 등 사회 주요영역에서의 개인정보 수집·유통실태를 조사하였다. CCTV, 위치정보, 유전정보, 통신비밀 등 특수한 개인정보에 대한 수집·유통실태도 별도로 다루었다. 또한, 이번 연구에서는 수집·유통실태에 대한 조사와 함께, 정보주체의 열람 및 정정·삭제 청구권이 어느 정도로 보장되고 있는지를 파악하고자 하였다. 각 개인정보 영역에서 드러난 문제점 및 개선방안은 각 절의 '소결'을 통해 정리하였기 때문에, 본 절에서는 이번 연구를 통해 드러난 개인정보 수집·유통의 전반적인 실태를 간단히 정리해 보고자 한다.

첫째, 공공 및 민간영역에서 보유하고 있는 개인정보의 제3자 제공 규모가 방대하다는 것을 확인할 수 있었다. 우선 공공영역의 경우, 2009년 9월 현재 75종이 행정정보 공동이용 대상정보로 지정되어 있었으며, 379개 기관이 공동이용을 하고 있었다. 국민건강보험공단은 각 의료기관에서 제공하는 의료정보뿐만 아니라, 행정안전부, 국세청 등으로부터 시스템 연계를 통해 개인정보를 제공받아 방대한 개인정보 데이터베이스를 구축하고 있었다. 이는 다시 각 기관의 요청에 의해 보유목적 외로 활용되고 있었으며 그 규모는 2008년부터 2년 동안 총 733회, 1억 건이 넘는 것으로 나타났다. 민간영역 역시 마찬가지이다. 예컨대, 각 이동통신사가 업무 제휴나 취급위탁 계약을 통해 개인정보를 제공하는 업체의 수는 1000~2000개에 달한다. 또한, 고객 유치를 위해 만 여개가 넘는 판매점과도 관계를 맺고 있었다. 각 금융기관에서 생성된 신용정보와 공공기관이 보유하고 있는 개인정보는 신용정보집중기관 및 신용조회회사로 집적되며, 다시 각 금융기관과 공공기관에 제공된다. 금융지주회사 내에서는 금융거래정보 및 신용정보가 공유된다. 이러한 현상은 공공영역에서는 '공공적 목적'과 '효율성'을 이유로, 그리고 민간영역에서는 서로 다른 서비스 간의 '제휴'나 '융합'에 따라 강화되고 있다. 물론 이는 정보주체의 동의 혹은 법률에 근거한 것으로 그 자체로는 불법이 아니지만, 개인정보의 제3자 제공과 공유가 증가하면 할수록 정보주체의 자기정보에 대한 통제력은 약화될 수밖에 없다. 국민건강보험공단의 사례에서 볼 수 있다시피, 한

번 집적된 개인정보는 '효율성' 등의 이유로 애초 수집목적 외로 활용될 수 있는 다양한 유인을 갖게 마련이다. 또한, 아무리 법제를 강화하고 보안 시스템을 갖춘다고 해도 제3자 제공이나 시스템 연계를 통해 개인정보에 접근할 수 있는 사람들이 많아지게 되면, 무단/불법 열람이나 유출의 위험 역시 커질 수밖에 없다.

따라서 개인정보 보호법제는 앞으로 개인정보의 수집 목적 외 제3자 제공을 제한하는 것에 초점을 맞출 필요가 있다. 현재「공공기관의 개인정보보호에 관한 법률」 등 개인정보 보호와 관련된 주요 법률에서는 정보주체의 열람·정정·삭제권을 보장하고 있다. 이번 연구에서 각 기관/업체에 대한 열람청구를 진행해본 결과, 각 기관/업체가 보유하고 있는 개인정보에 대해서는 대체적으로 열람이 허용되었다. 그러나 내 개인정보의 제3자 제공 내역에 대해서는 대부분의 기관/업체에서 제공을 거부하였다. 「공공기관의 개인정보보호에 관한 법률」에서는 제공 내역에 대한 열람권 자체가 규정되어 있지 않으며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 제3자 제공 내역에 대한 열람권을 규정하고 있으나 실제로는 제대로 보장되지 않는 경우가 많았다. 그러나 개인정보의 제3자 제공이 방대하게 이루어지는 현실에서, 정보주체의 개인정보자기결정권을 효과적으로 보장하기 위해서는 제3자 제공 내역에 대한 열람권의 보장이 더욱 중요해진다. 내 개인정보가 누구에게 제공되는지 알 수 없는데, 어떻게 결정권을 행사할 수 있겠는가? 정보주체의 동의를 받고 제3자에게 제공하는 경우는 그나마 나은 편이다.[305] 법에 근거해서 개인정보가 제공되는 경우는 더욱 정보주체가 인지하기 힘들다. 애초 수집목적 외로 개인정보를 활용할 수 있도록 하는 것은 최소한으로 제한하도록 관련 법제가 개선될 필요가 있다.[306] 또한, 불가피하게 개인정보를 제공하는 경우라면 정보주체에게 통지를 의무화할 필요가 있다. 더불어 개인정보를 취득한 기관에 대해서는 정보주체가 자기 정보의 취득경위를 요구할 수 있도록 법적 근거를 마련할 필요도 있다.

둘째, 개인정보 보유의 법적 근거가 모호하거나, 개인정보 보호를 위한 법적 체계가 미진한 영역이 여전히 존재하고 있다. 예를 들어, 범죄정보관리시스템의 경우 방대한 양의 개인정보의 수집과 관리를 하면서도 엄밀한 법률적 근거를 갖추지 않은 채 운영되고 있었다. 국민건강보험공단 등이 수집하는

305) 물론 이 경우에도 정보주체가 자신이 동의한 사실을 일일히 기억할 수 없기 때문에 언제든 자신의 동의 내역을 확인하고 동의를 철회할 수 있도록 보장되어야 한다.

306) 예를 들어, 국민건강보험공단에 개인정보 제공을 요청할 수 있도록 규정하고 있는 법제들부터 재검토될 필요가 있다.

개인정보의 경우에도, 수집의 근거를 추상적으로 규정하고 있어 업무상 필요한 정보를 자체적으로 판단하여 수집하고 있는 실정이다. 특히, 의료 영역의 경우 여타 사회 영역과 달리 개인 의료정보의 보호를 위한 법제가 아직 마련되어 있지 않아 개인정보 보호의 사각지대로 남아있는 것은 심각한 문제이다. 방대한 개인정보를 보유하고 있는 기관에 대해서 개인정보 수집의 범위와 근거, 활용 및 제3자 제공의 근거와 한계, 정보주체의 권리 보호 등에 대한 명확하고 상세한 규정을 포함한 법제 정비가 시급히 필요하다.

셋째, 공공기관에서 추진하고 있는 정보화 사업들이 국민의 프라이버시권을 침해할 우려가 있음에도 불구하고, 정보인권의 관점에서 이를 견제할만한 제도적 장치가 마련되어 있지 않다. 교육행정정보시스템은 지난 2003년 많은 사회적 갈등을 겪으며 도입되었음에도 불구하고, 주무부처의 자체적인 판단에 의해 다시 원점으로 회귀하려 하고 있다. 행정정보 공동이용 시스템은 개인정보에 접근할 수 있는 범위를 확대시키고 있음에도 불구하고, 주로 '효율성'의 관점에서 추진되고 있다. 공공기관 CCTV는 설치되기 시작한 지 몇 년이 지나서야 법적 근거가 마련되었다. 범죄정보관리시스템은 법적 근거도 모호한 상태에서 추진이 되었으며, 행정안전부를 통해 공개되는 '공공기관 개인정보파일목록'에도 포함되지 않는 등 운영실태가 잘 드러나지 않고 있다. 현재 형사사법정보시스템의 구축이 추진[307]되고 있는데, 이 역시 프라이버시 침해 논란을 불러일으키고 있다. 이번 연구에서 다룬 승용차 요일제나 고속도로 하이패스 등 공공기관이 추진하는 정책에서 위치정보를 수집하고 있지만, 시행 및 운영 과정에서 위치정보의 보호 문제는 거의 고려되지 않고 있다. 이와 같이 공공기관이 추진하고 있는 사업에 프라이버시 문제가 제대로 검토되지 않는 이유는 '공공기관 개인정보보호심의위원회'가 거의 유명무실하기 때문이다. 이런 점에서 독립적이고 실효성 있는 '개인정보 감독기구' 설립의 필요성을 다시한번 절감할 수 있다. 더불어, 공공기관이 정보화와 관련된 사업을 추진할 경우, 사업을 추진하기 전에 '프라이버시 영향평가'를 반드시 거치도록 제도화할 필요가 있겠다.

넷째, 법률에서 개인정보주체의 열람 및 정정·삭제 청구권을 보장하고 있음에도 불구하고, 이에 대한 정보주체의 인식은 매우 부족한 것으로 드러났다. 본 연구에서 수행한 설문조사 결과, 시민들의 대다수는 우리 사회 프라이버시 침해가 심각하다고 느끼고 있었고, 공공기관이나 민간기업의 개인정보

307) 형사사법정보시스템의 경우는 현재 시행하고 있는 것은 아니기 때문에, 이번 조사에서는 제외하였다.

관리 실태에 대해서도 부정적인 인식을 보였으나, 정작 개인정보 취급방침을 공개해야 한다는 사실이나 정보주체가 열람 및 정정·삭제 청구권을 보장받고 있다는 사실에 대해서는 모르고 있는 경우가 압도적으로 많았다. 즉, 언론 등을 통해 터져 나오는 숱한 개인정보 유출 사고 등을 접하면서 프라이버시 침해에 대한 우려는 높아졌지만, 실제 개인정보 보호를 위한 정책이나 자신의 권리를 보장받기 위한 방법 등에 대해 교육받을 기회는 별로 없었기 때문인 것으로 판단된다. 정규교육이나 언론 등 다각적인 경로를 통해 일반 시민을 대상으로 한 정보인권 교육이 절실하게 필요한 상황이다. 한편, 개인정보보호책임자(담당자)에 대한 설문조사 결과를 보면, 각 기관/업체의 개인정보보호책임자는 자 기관/업체의 개인정보 보호 체계가 전반적으로 큰 문제가 없는 것으로 답변하여, 본 연구에서 드러난 실태와 일정한 간극을 보였다. 반면, 각 기관/업체의 개인정보보호책임자가 해당 업무를 맡은 기간은 평균 1.84년으로 별로 길지 않았고, 별도의 업무와 함께 수행하면서 부차적으로 개인정보 업무를 맡고 있는 경우가 많아 오히려 각 기관/업체에서 개인정보보호업무는 부차적으로 취급되고 있었다.

## 제2절 연구의 한계 및 향후 과제

본 연구는 법제에 대한 고찰 보다는 사회 주요영역의 개인정보 수집·유통 실태와 정보주체의 열람 및 정정·삭제 청구권이 실제 보장되고 있는지를 파악하고자 노력하였다. 그러나 다루고자 했던 영역이 광범위했던 것에 비해, 7개월이라는 한정된 시간과 연구자 역량의 부족으로 각 영역의 조사에서 미진한 부분이 있을 수밖에 없었다는 점은 아쉬움으로 남는다. 이번 조사를 기반으로 향후에는 각 개인정보 영역에 대해 보다 면밀한 실태 조사가 시행될 수 있기를 기대한다.

이번 연구에서 많은 사회 영역, 혹은 특수한 개인정보 영역을 다루기는 했으나, 중요하지만 이번 연구에서는 빠진 사회 영역이 당연하게도 많이 존재한다. 예컨대, 형사·사법 영역, 사회복지 영역, 세무 영역 등이나 생체정보, 노동감시, 주민등록제도 등의 주제가 포함될 수 있을 것이다.

정보주체의 열람 및 정정·삭제 청구권 보장 실태 조사의 경우에는 해당 영역에 관련된 당사자를 섭외하는데 어려움이 있었다. 특히, 보건의료 영역이나 유전정보 등이 그러한 경우이다. 또한, 특정 영역의 관련 업체나 기관이 많기 때문에 특정 영역 내에서 각 기관/업체별 차이나 전반적인 실태를 보다

정확히 분석하기 위해서는 더 많은 기관/업체에 대한 열람청구가 이루어질 필요가 있겠다. 이번 조사에서는 포털 영역에 대해서는 대다수의 포털을 대상으로 열람청구를 하였으나, 타 영역에서는 소수의 기관/업체만을 선정해서 진행할 수밖에 없었다.

정확한 실태조사를 위해 필요한 정보 접근의 한계도 존재했다. 공공영역의 경우 여타 문헌이나 국회 등을 통한 정보 접근 외에 각 기관에 대한 정보공개 청구를 통해 정보를 얻고자 했으나, 아예 답변을 하지 않거나 부실한 답변을 제공하는 경우가 많았다. 그나마 공공기관은 정보공개라는 수단이라도 존재하지만, 민간 업체의 경우에는 자기정보에 대한 열람청구 외에는 각 업체의 내부 실태와 관련된 정보에 접근하는데 한계가 많았다. 정보를 제공할 의무도 없고, 영업상 비밀이라는 이유로 제공하지 않으려 하기 때문이다. 따라서 민간 영역의 개인정보 보호 실태를 파악하기 위해서는 개인정보 보호와 관련된 각 기업의 정책이나 실태의 일정한 공개를 법에서 규정[308]하거나 개인정보 감독기구와 같은 권한있는 기관에서 각 영역의 주요 기관이나 업체의 협조를 얻어 실태조사를 수행할 필요가 있다.

그런 점에서 (구)한국정보보호진흥원(KISA)에서 발간하던 개인정보보호백서가 2002년과 2003년을 끝으로 중단된 것은 아쉬움이 크다. 국가적 차원에서 개인정보보호백서를 매년 발간해왔다면, 사회 각 영역의 개인정보 보호 실태를 파악하는데 큰 도움이 되었을 것이다. 물론 사회 각 영역에서 개인정보 보호에 대한 비판적 관점의 연구는 자율적으로 이루어질 필요가 있으며, 백서의 발간은 그러한 연구를 심화하는데 기여할 수 있을 것이다.

개인정보보호백서의 발간이 중단된 구체적인 사유는 알 수 없지만, 국가적 차원에서 '국가정보화백서'(구 정보사회진흥원에서 발행)나 '국가정보보호백서'(국가정보원에서 발행)가 매년 나오는 것과 달리, 개인정보보호백서의 형태로는 정리되지 않고 있는 것이 어쩌면 우리나라 정보화의 기본 방향을 보여주는 것일지도 모른다. 국가정보화백서나 국가정보보호백서 역시 개인정보 문제를 다루고 있기는 하지만, 간략하고 부차적인 것에 머물고 있다. 향후에 개인정보 감독기구가 설립이 되어, 매해 사회 각 영역의 개인정보 보호 실태를 종합한 개인정보보호백서를 발간하기를 기대해본다.

---

308) 예를 들어, 개인정보 취급방침이나 신용정보 활용체계의 공개가 그러한 예가 될 것이다.

## 참고문헌


감사원. 2008. 감사결과 처분요구서: 행정정보 공유 및 관리실태. 2008.5.

강기정. 2009. “CCTV 설치·운영 지역별 편차 커, 정작 범죄취약지역, 범죄다발지역은 외면당해”. 강기정 의원 보도자료. 2009.9.15.

강창동. 2005. 교육행정정보시스템(NEIS) 도입 과정에서 표출된 사회적 갈등에 관한 연구. 「교육사회학연구」 15(1): 1-22.

건강보험심사평가원·대한의료정보학회. 2005. 요양기관 정보화 실태조사 보고서.

공정거래위원회. 2008. 의결서 제2008-260호. 2008.9.8.

교육과학기술부. 2009. “교육행정정보시스템(NEIS) 시·도교육청 단위로 통합.” 교육과학기술부 정보화담당관실 보도자료. 2009.8.6.

교육인적자원부. 2003. 교육행정정보시스템(NEIS) 관련 자료집.

국가인권위원회. 2003. 교육행정정보시스템(NEIS) 관련 권고. 2003.5.17.

국가인권위원회. 2004a. 공공기관의 CCTV 등 무인단속장비의 설치·운영 관련 정책 권고. 2004.4.19.

국가인권위원회. 2004b. 구금시설 수용거실 내 CCTV 설치·운영 등 인권침해. 03진인971, 03진인833, 03진인5806(병합) 결정 2004.10.

국가인권위원회. 2008. “재학생에게 NEIS 본인정보 열람·정정청구권 보장돼야.” 국가인권위원회 보도자료. 2008.12.15.

국가인권위원회. 2009. 「통신비밀보호법 일부개정법률안(이한성 의원 대표발의)」에 대한 의견표명. 2009.2.27.

국가정보원·방송통신위원회·행정안전부·지식경제부. 2009. 2009 국가정보보호백서.

국민건강보험공단. 2009. 8대 중점목표 추진계획. 2009.7.

권건보. 2009. 지방자치단체의 CCTV 설치·운영과 프라이버시. (사)유럽헌법학회 및 국가인권위원회 공동학술발표회 <유럽인권협약과 기본권>. 2009.5.29.

권영성. 1998. 『헌법학원론』. 서울: 법문사.

권해수. 2006. 행정정보 공유 추진과정의 갈등관리에 관한 연구. 행정정보공유추진위원회.

김덕근. 2006a. 교육정책형성과정에서 나타난 이익집단의 활동전략 분석: 전국교직원노동조합과 한국교원단체총연합회의 이익표출활동을 중심으

로. 「교육사회학연구」 15(2): 1-36.
김덕근. 2006b. 교육정책참여자들의 이슈네트워크 분석. 「교육행정학연구」 24(2): 81-102.
김민호. 2007. 공공부문 개인정보보호법제의 현황과 과제. 「토지공법연구」. 37(1): 207-223.
김병수. 2005. 유전자감식기술의 사회윤리적 쟁점. <한국생명윤리학회 2005년 봄철 학술대회> 자료집.
김유정. 2009. “개인정보 4,417만건이 저장된 CIMS, 관리는 느슨”. 경찰청 국정감사 보도자료. 2009.10.12.
김주한. 2008. 개인 건강정보 보호법안에 대한 검토의견. <개인건강정보 보호법안 전문가 간담회> 자료집. 전현희 의원 주최. 2008.8.22.
김창수. 2009. “‘나 모르는 통신 수사 비일비재’…본인확인은 7건?” 김창수 의원 보도자료. 2009.10.7.
김춘진. 2009. “교육행정정보시스템(NEIS) 학부모이용률, 100명 중 6명에 불과, 시도별 격차 최대 10배”. 김춘진 의원 보도자료. 2009.10.12.
김태우. 2006. 정책결정 딜레마 상황에서의 정부의 대응행동에 관한 연구: 교육행정정보시스템(NEIS)정책을 중심으로. 서울대학교 석사학위논문.
김해석. 2005. 교육행정정보시스템(NEIS)의 도입이 교육행정 효율성에 미치는 효과에 대한 비교 연구. 석사학위논문. 인천대학교 교육대학원.
나태준. 2006. 정책 인식 프레이밍 접근방식에 따른 갈등의 분석: 교육행정정보시스템 도입 사례를 중심으로. 「한국정책과학학회보」, 10(4): 297-325.
남명진. 2009. 신원확인을 위한 유전정보이용법에 관한 제언. <살인・강간 등 흉악범죄 어떻게 대처할 것인가> 정부공청회 자료집. 2009.4.29.
NEIS 반대와 정보인권 수호를 위한 공동대책위원회. 2003. NEIS 문제해결과 올바른 교육정보화를 위한 공대위의 정책 대안. 2003.11.27.
민주노총 공공연맹 의료연대노동조합. 2006. 보건의료정보화와 EMR(전자의무기록). 2006.12.
박상준・임정빈. 2004. 교육행정정보시스템(NEIS) 정책갈등에 관한 연구. 「한국거버넌스학회보」 11(2): 111-146.
박영선. 2008. “압수수색・통신감청・통신사실확인자료제공 등 올 상반기에만 33만 7천여 건”. 박영선 의원 보도자료. 2008.10.9.

박영선. 2009. “법원, 인터넷 회선 감청(패킷감청) 허가에 신중해야”. 박영선 의원 보도자료. 2009.10.9.
박정주. 2007. 학교 조직의 교육행정정보시스템(NEIS) 수용 요인에 관한 구조적 분석. 「교육행정학연구」 25(4): 215-236.
박진영・김동준. 2006. 대중교통정책 수립에 있어서 교통카드 자료 활용방안 연구. 한국교통연구원.
방송통신위원회. 2008a. “방송통신위원회, 하나로텔레콤에게 초고속인터넷서비스 신규가입자 모집정지 40일 부과”. 방송통신위원회 보도자료. 2008.6.24.
방송통신위원회. 2008b “하나로텔레콤, ´08. 7. 1 ~ 8. 9일까지(40일간) 신규가입자 모집정지.” 방송통신위원회 보도자료. 2008.6.30.
방송통신위원회. 2008c. “방송통신위원회, 8월 30일 부터 KT・LG파워콤 초고속인터넷서비스 신규가입자 모집정지”. 방송통신위원회 보도자료. 2008.8.28.
방송통신위원회. 2008d. “방통위, 8개 MSO・포털사업자의 개인정보 유용행위에 대해 과태료 부과.” 방송통신위원회 보도자료. 2008.11.14.
방송통신위원회. 2008e. “방통위, 3개 이동전화사업자의 개인정보 유용행위에 대해 과태료 부과.” 방송통신위원회 보도자료. 2008.12.30.
방송통신위원회. 2009. “이통사, 판매점 개인정보관리 대폭 개선.” 방송통신위원회 보도자료. 2009.5.1.
변미리. 2004. 서울시 전자정부의 개인정보보호에 관한 연구. 서울시정개발연구원.
변웅전. 2009. “건강보험・국민연금 관계기관의 개인정보 불법유출 여전해 / 건보공단, 최근 2년간 개인정보 관련 33명, 연금공단 12명 징계.” 변웅전 의원 보도자료. 2009.10.12.
변재일. 2009. “09년 상반기 휴대전화 위치추적 허가 일평균 53건”. 변재일 의원 보도자료. 2009.10.22.
서상기. 2009. “국가 핵심연구정보 노린다, 교육기관(대학, 교육청)에서 개인정보 줄줄 샌다.” 서상기 의원 2009년 국정감사 보도자료. 2009.9.17.
서울지방경찰청. 2007. “인터넷 초고속망 가입 주의보”. 서울지방경찰청 보도자료. 2007.8.9.
서울지방경찰청. 2008a. “이동통신사 고객정보 실시간으로 누출”. 서울지방

경찰청 보도자료. 2008.4.21.
서울지방경찰청. 2008b. “「통신업체의 도를 넘는 고객정보 불법이용」“이용자 주의보”.” 서울지방경찰청 보도자료. 2008.4.22.
서울지방경찰청. 2008c. 2008년도 행정안전위원회 국정감사요구자료 제1권.
서울지방경찰청. 2009. “뻥 뚫린 금융기관 고객정보, 불법거래 심각”. 서울지방경찰청 보도자료. 2009.5.18.
성낙인・이인호・김수용・권건보・김삼용・이지은・김주영・손형섭・박진우・김송옥. 2008. 개인정보보호법제에 관한 입법평가. 현안분석 2008-45. 한국법제연구원.
손승식. 2008. 개인건강정보의 보안(Security)체계. <EHR핵심공통기술 심포지엄> 발표자료. 2008.12.11.
송광용・김수윤. 2004. 교육행정정보시스템 도입과정에서 교육부와 전교조의 갈등 상황 분석. 「교육행정학연구」 22: 193-212.
송희준. 2008. 정보화와 전자정부: 비판적 성찰과 향후 과제. 「한국행정학회 세미나」 발표자료.
송희준・권효진・김상운・유효정. 2008. 교육행정정보화사업의 성과분석. <한국행정학회 2008년도 하계학술대회> 발표논문집.
신영진. 2008. 미래사회에서 정보보호 발전방안에 관한 연구. 「한국행정학회학술논문집」.
신영진・강원영. 2008. 우리나라의 개인정보보호수준 향상 및 개선을 위한 연구. <한국행정학회 2008년도 추계학술대회> 발표논문집. 2008.10.16.
심재철. 2009. “건강보험공단, 개인정보 불법열람 및 유출 여전.” 심재철 의원 보도자료. 2009.10.8.
오길영. 2008. 통신비밀보호법 개정안 비판. 국회 이춘석 의원・민주당 정책위원회 주최 <수사・정보기관의 통신감청, 국민은 안전한가?> 토론회 자료집. 2008.12.11.
오길영. 2009. 인터넷 감청과 DPI(Deep Packet Inspection). 「민주법학」 41호. 2009. 11. 391-426.
오동석. 2007. 통신비밀보호법 개정안에 대한 반대의견. 국회 문병호 의원 등 주최 <통신비밀보호법의 올바른 개정을 위한 토론회> 자료집. 2007.6.5.
오상진. 2009. 위치정보서비스, 진흥과 규제 이슈. *TTA Journal No.123.*

오영균. 2009. 공공부문 CCTV 통합활용에 관한 사례연구. <한국행정학회 2009년도 하계학술대회> 발표논문집.
원유철. 2008. “개인정보보호, 정부는‘나 몰라라’”. 원유철 의원 보도자료. 2008.9.9.
유정현. 2008. 제278회 국회(정기회) 행정안전위원회 국정감사 행정안전부 질의서. 2008.10.7.
윤영민. 2004. 개인정보화 사생활의 비밀과 자유 보호를 위한 정책 연구. 국가인권위원회 연구용역 보고서.
이건・이현희・정초영. 2005. 범죄정보관리시스템(CIMS)활용방안 연구. 치안정책연구소 연구보고서 2005-11.
이대식・정주영. 2006. 교육행정정보시스템의 운영실태분석. 「인터넷정보학회논문지」 7(4): 115-122.
이동원・박준・강민형・채승병・최홍. 2009. 사회적 자본 확충을 위한 정책과제. 「CEO 인포메이션」 제722호. 2009.09.16. 삼성경제연구소.
이미정. 2008. 의료기관 내에서의 개인정보 보호대책. <EHR핵심공통기술 심포지엄> 발표자료. 2008.12.11.
이민영. 2007. 공공기관의 개인정보보호에 관한 법적 쟁점. 「정보통신정책」 19(10) 통권 417호.
이보영. 2005. 교육행정정보시스템(NEIS)의 정책집행과정에서 나타난 쟁점분석. 중앙대학교 석사학위논문.
이상명. 2008. 개인정보자기결정권의 헌법적 근거에 관한 고찰. 「공법연구」 36(3): 225-248.
이성호. 2007. 부상하는 위치기반서비스(LBS). 삼성경제연구소. *CEO Information* 제615호. 2007.8.
이은우. 2009. 디엔에이신원확인정보의 이용 및 보호에 관한 법률안에 대한 의견. <살인・강간 등 흉악범죄 어떻게 대처할 것인가> 정부공청회 자료집. 2009.4.29.
이인호. 2001. 개인정보자기결정권의 한계와 제한에 관한 연구. 「개인정보연구」 01-01. 한국정보보호진흥원.
이향수. 2009. 개인정보 보호에의 관심과 대응. 「정책분석평가학회보」 18(2).
임지봉. 2005. 유전자 감식정보의 수집 및 관리에 관한 법률안의 위헌성과 기타의 문제점 및 그 대안. <유전자감식정보의 수집 및 관리에 관한

법률(안) 입법공청회> 자료집. 2005.10.27.
임지봉. 2007. CCTV 개인영상정보 보호를 위한 개별 입법의 필요성 및 당위성. 한국정보보호진흥원 개인정보보호기획팀 편. 「신규IT 서비스의 프라이버시 이슈리포트」. 2007.6.
전현희. 2008. “(건보공단) 업무외 목적 부당이용, 무작위 무단조회 여전, (연금공단) 공단에 있는 개인정보, 지인찾기 검색창? ⇒ 봐주기식 징계 일관, 보호관리 허점 투성이.” 전현희 의원 보도자료. 2008.7.22.
정보통신부. 2005. “이동통신사 개인정보보호 지침 마련”. 정보통신부 보도자료. 2005.09.29.
정보통신부. 2007. CCTV 개인영상정보보호 가이드라인. 2007.11.
정보통신부・한국정보보호진흥원. 2005. 기업의 개인정보 영향평가 수행을 위한 가이드.
정부혁신지방분권위원회. 2005. 행정정보 공유현황 및 개선방안. <제63회 국정과제회의> 발표자료. 2005.7.20.
정연수. 2004. 민간분야 개인정보관리 현황조사 연구. 한국전산원.
정연수・김동우・고재종. 2005. 2005년 민간부문 개인정보보호 관리현황 및 보호방안에 관한 연구. 한국정보보호진흥원.
정준현. 2007. CCTV 개인영상정보보호와 규제수단. 한국정보보호진흥원 개인정보보호기획팀 편. 「신규IT 서비스의 프라이버시 이슈리포트」. 2007.6.
정책기획위원회. 2008. 교육행정정보시스템 (NEIS): 갈등을 넘어 교육정보화의 새로운 총아로. 참여정부 정책보고서 2-37.
정충식. 2009. 『2009 전자정부론』. 서울: 서울경제경영.
정태호. 2008. CCTV 감시에 대한 개인정보보호법의 규율에 대한 헌법적 평가. 「헌법학연구」, 14(1).
정혜정・김남현. 2009a. u-Health 시대의 개인건강정보 보호를 위한 법제 고찰. 「정보보호학회지」, 19(1): 115-124.
정혜정・김남현. 2009b. 보건의료의 정보화와 정보보호관리 체계. 「정보보호학회지」, 19(1): 125-133.
조규석. 2005. 교통카드 전국호환시스템 도입에 관한 연구. 한국운수산업연구원. 「KRITI 정책연구」 05-1.
하연섭・주재현・강민아・나태준・장지호. 2006. 사회의사결정구조의 개선: 담론구조와 틀 짓기 개념을 중심으로. <2006년도 한국행정학회 동계

학술대회> 발표논문집.
한국소프트웨어진흥원. 2008. 국내 소프트웨어 시장 2008년 회고와 2009년 전망. 2008.12.
한국인터넷진흥원. 2009. 2009년 인터넷이용실태조사결과 요약보고서.
한국정보화진흥원. 2009. 2009 국가정보화백서.
한국정보보호진흥원. 2003. 2002 개인정보보호백서. 2003.2.
한국정보보호진흥원. 2004. 2003 개인정보보호백서.
한국정보보호진흥원. 2008a. 2008년도 문화체육관광방송통신위원회 국정감사요구자료.
한국정보보호진흥원. 2008b. 2008 정보보호 실태조사: 개인편.
한국행정연구원. 2007. 개인정보보호와 행정정보공유의 조화방안에 관한 연구. 행정정보공유추진위원회 보고서.
한정미. 2007. 신용정보의 이용 및 보호에 관한 법제연구: 금융기관의 구조변화에 따른 대응을 중심으로. 한국법제연구원. 2007.9.
함께하는 시민행동. 2003a. 금융기관과 인터넷에서의 개인정보 공유현황 실태조사. 국가인권위원회 인권상황실태조사 연구용역 보고서.
함께하는 시민행동. 2003b. 공공기관의 감시카메라 운영 실태 보고서.
행정안전부. 2008a. 공공기관 개인정보관리 업무 매뉴얼. 2008.4.
행정안전부. 2008b. 공공기관 CCTV 관리 가이드라인. 2008.4.
행정안전부. 2008c. 제278회 국회(정기회) 행안위 국정감사 서면답변. 2008.10.16.
행정안전부. 2008d. 제278회 국회(정기회) 행안위 국정감사 서면답변. 2008.10.31.
행정안전부. 2008e. '08년 개인정보파일 전수조사 결과 보고. 2008.12.
행정안전부. 2009a. 공공기관 CCTV 관리 가이드라인. 2009.9.
행정안전부. 2009b. “구비서류 제출 부담을 덜어주는, 행정정보 공동이용 실적 전년대비 81% 증가.” 행정안전부 보도자료. 2009.9.9.
행정안전부. 2009c. “행안부, CCTV 통합관제센터 및 네트워크 카메라 관리기준 마련.” 행정안전부 보도자료. 2009.9.28.
행정안전부. 2009d. 공공기관의 개인정보파일 관리지침.
행정안전부 개인정보보호팀. 2008. 공공기관 CCTV 관리실태 현장조사 결과. 2008.2.
행정안전부・한국정보보호진흥원. 2008. 민간기업 개인정보보호 매뉴얼.

행정자치부. 2007. "'공공기관 개인정보보호', 대폭 강화됩니다!". 행정자치부 보도자료. 2007.5.25.
행정자치부. 2008. 2007 전자정부법의 이해와 해설. 2008.2.
행정정보공유추진단. 2009. 행정정보공동이용 실태점검 결과.
행정정보공유추진위원회. 2007. 2007 행정정보공동이용 백서.
허진회. 2006. 교육행정정보시스템(NEIS) 도입에 관한 일선 교사들의 인식 조사. 숙명여자대학교 교육대학원 석사학위논문.
황성기. 2009. 범죄수사시 DNA 정보의 활용에 있어서의 문제점. <살인·강간 등 흉악범죄 어떻게 대처할 것인가> 정부공청회 자료집. 2009.4.29.

## <부록 1> 시민인식조사 설문지

| **2009** 개인정보 보호 및 정보주체의 개인정보 접근권에 대한 시민 인식조사 | | | |
|---|---|---|---|
| • 안녕하십니까? 저는 여론조사 전문기관인 리서치플러스의 면접원 ○○○입니다.<br>• 저희는 지금 국가인권위원회 연구용역사업의 일환으로서 우리나라 개인정보 보호와 권리에 관한 법제도 현황과 그 보장 등 실태 분석을 위해 시민들을 대상으로 설문조사를 실시하고 있습니다.<br>• 바쁘실 줄 아오나 개인정보와 관련된 대안을 제시하는 데에 도움이 될 수 있도록 협조를 부탁드리겠습니다. 귀하의 응답 내용은 통계처리를 위한 목적으로만 사용되며 절대 비밀이 보장됨을 알려드립니다. 감사합니다. | | | |

Sq1. 지역

01. 서울 02. 부산 03. 대구 04. 인천
05. 광주 06. 대전 07. 울산 08. 경기
09. 강원 10. 충북 11. 충남 12. 전북
13. 전남 14. 경북 15. 경남 16. 제주

Sq2. 실례지만 귀하께선 지금 특별시, 광역시, 중소도시, 군/읍 지역 중 어디에 거주하고 계십니까?

1. 대도시(특별시/광역시) 2. 중소도시 3. 군/읍/면지역

Sq3. 나이 : 실례지만 ○○님의 연세는.. 만_____세
1990년 7월이전 출생자_만 19세이상만 조사 진행

Sq4. 성별 : 1. 남 2. 여

### Ⅰ. 일반시민의 개인정보 접근권

Q 1) ○○님께서는 우리 사회에서 개인정보 유출과 같은 프라이버시 침해가 얼마나 심각하다고 생각하십니까?

① 아주 심각하다

② 심각한 편이다
③ 보통이다
④ 심각하지 않은 편이다
⑤ 전혀 심각하지 않다

Q 2. ○○님께서는 중앙행정기관이나 지자체와 같은 공공기관이 국민의 개인정보를 얼마나 안전하게 관리한다고 생각하십니까?

① 매우 안전하게 관리한다
② 안전한 편이다
③ 보통이다
④ 안전하지 않은 편이다
⑤ 전혀 안전하지 않다

Q 3. 그럼, 은행 등 금융기관이나 인터넷 포털과 같은 민간기업이 고객의 개인정보를 얼마나 안전하게 관리한다고 생각하십니까?

① 매우 안전하게 관리한다
② 안전한 편이다
③ 보통이다
④ 안전하지 않은 편이다
⑤ 전혀 안전하지 않다

Q 4. 다소 불편하더라도 개인정보 보호를 위해서 주민번호 대신 여권이나 운전면허증, 의료보험증 번호와 같은 것으로 대체해야 한다는 의견에 대해서는 어떻게 생각하십니까?
① 동의한다 ② 동의하지 않는다

Q 5. ○○님께서는 공공기관이나 민간기업이 개인정보를 수집·이용하는 경우, 개인정보를 취급하는 방침을 정하고 일반에 공개해야 한다는 사실을 알고 계십니까?
① 예 ② 아니오

Q 6. ○○님께서는 ○○님 본인의 개인정보를 보유하고 있는 공공기관이나 민간기업에 본인의 개인정보 열람을 청구할 수 있다는 사실을 알고 계십니까?
① 예 ② 아니오

Q 7. 주민등록 등초본 등 일반 민원서류를 발급받는 것을 제외하고 본인의 개인정보를 확인하기 위해 개인정보 열람을 청구하신 경험이 있으십니까?
① 예 ② 아니오--> Q8로 가시오.

Q7-1. ([Q 7]에서 '① 예' 응답자만 답해주십시오) 그럼, 개인정보 열람 후에 개인정보의 정정이나 삭제를 청구한 경험이 있으십니까?
① 예 ② 아니오

Q 8. ○○님의 개인정보를 가지고 있는 기관이 개인정보를 다른 기관과 공유하거나 제공하는 경우가 있다는 것을 알고 계십니까?
① 예 ② 아니오 --> Q9로 가시오.

Q8-1. ([Q 8]에서 '① 예' 응답자만 답해주십시오) ○○님의 개인정보를 가지고 있는 기관이 외부의 어떤 기관에 어떠한 정보를 제공하고 있는지 알고 계십니까?

① 아주 잘 알고 있다
② 대체로 알고 있다
③ 대충 짐작하는 정도이다
④ 별로 모르고 있다
⑤ 전혀 모르고 있다

Q 9. 공공기관에서 CCTV를 설치하는 경우 이를 쉽게 인식할 수 있도록 안내판 설치 등 필요한 조치를 취해야 한다는 사실을 알고 계셨습니까?

① 아주 잘 알고 있다
② 대체로 알고 있다
③ 대강 들어는 보았다
④ 별로 모르는 사실이다
⑤ 전혀 모르는 사실이다

Q10. ○○님께서는 CCTV가 설치된 것을 보면 안심이 되십니까? 그렇지 않습니까?

① 매우 안심이 된다
② 대체로 안심이 된다

③ 보통이다
④ 별로 안심이 안된다
⑤ 전혀 안심이 안된다

Q11. 그럼, ○○님께서는 곳곳에 설치되어 있는 CCTV를 보면 내가 CCTV에 찍힌다는 사실에 위축되십니까? 그렇지 않습니까?

① 매우 위축되는 느낌이다
② 어느정도 위축되는 느낌이다
③ 보통이다
④ 별로 위축되는 느낌은 없다
⑤ 전혀 위축되는 느낌이 없다

## Ⅱ. 응답자 배경 변인

DQ1) ○○님의 직업은 무엇입니까?

① 농업/임업/어업
② 자영업(상업,소규모장사,개인택시 등)
③ 판매/서비스직(상점점원,세일즈맨 등)
④ 기능/숙련공(운전사,선반,목공 등)
⑤ 일반작업직(현장직업,청소관리,경비원 등)
⑥ 사무기술직(차장이하 사무직,기술직,교사 등)
⑦ 경영/관리직(5급이상 공무원,기업체 부장이상)
⑧ 전문/자유직(변호사,의사,건축사,교수 등)
⑨ 가정주부
⑩ 학생
⑪ 무직/기타

| | |
|---|---|
| **응답자명 :** | **전화번호 :** |
| **조사원명 :** | |

<부록 2> 개인정보 보유기관 담당자 대상 실태조사 설문지

# 2009 개인정보 수집 · 유통 실태 파악을 위한 개인정보 보유기관 담당자 대상 실태조사

| | | | | |
|---|---|---|---|---|
| | | | | |

안녕하십니까?

진보네트워크센터에서는 국가인권위원회의 연구용역 의뢰를 받아 우리나라 개인정보 보호 및 정보주체의 개인정보 열람 · 정정 · 삭제 등의 접근권과 관련한 법제도 현황파악과 접근권 보장 절차, 실태 분석을 통해 공공 및 민간의 각 영역에서의 개인정보 수집 · 유통의 대안을 제시하기 위해 개인정보 보유기관 담당자들을 대상으로 실태조사를 실시하고 있습니다.

바쁘실 줄 아오나 개인정보 수집 · 유통 대안 제시에 도움이 될 수 있도록 적극적인 협조를 부탁드리겠습니다. 귀하의 응답 내용은 통계처리를 위한 목적으로만 사용되며 절대 비밀이 보장됨을 알려드립니다.

설문조사에 응해 주셔서 감사드리며, 귀하의 평안과 번창하심을 기원합니다. 고맙습니다.

2009년 8월

조사기관 : 진보네트워크센터
(연구책임자 : 오병일, 02-774-4551)

※ 주관식 질문의 경우 해당 공란에 입력을 해주시고, 객관식 질문의 경우 해당 예시에 V 표시를 해주시면 됩니다.

## 먼저, 자료 분류를 위한 기초 질문입니다

1. 귀하의 나이는 만으로 어떻게 되십니까? 만 (_____) 세
2. 귀하의 성별은 어떻게 되십니까? ① 남성( ) ② 여성( )
3. 귀하의 소속기관은 어떻게 되십니까?
   ① 정부중앙부처( ) ② 지방자치단체( )
   ③ 교육기관( ) ④ 공공기관(공기업,준정부기관,기타)( )
   ⑤ 보건의료기관( ) ⑥ 금융권(신용정보회사 포함)( )
   ⑦ 통신사(이동통신사 포함) ( ) ⑧ 포털 등 부가통신서비스 사업자( )
   ⑨ 정보통신망법 상 준용사업자( ) ⑩ 기타( )

## 다음은 개인정보의 수집·유통 실태에 대한 질문입니다

**[문 1] 개인정보 침해 위험 및 개인정보보호 체계와 관련된 다음 질문에 답해주십시오.**

1. 과거 개인정보 침해 사고가 발생한 적이 있다.
   ① 그렇다( ) ② 아니다( )
2. 정보주체로부터 개인정보 침해신고를 받은 적이 있다.
   ① 그렇다( ) ② 아니다( )
3. 우리 기관은 개인정보 영향평가를 수행하고 있다.
   ① 그렇다( ) ② 아니다( )
4. 개인정보관리책임자 및 담당자가 지정되어 있다.
   ① 그렇다( ) ② 아니다( )(☞ 5.로)
   ※ 담당자는 실제 개인정보 보호 업무를 담당하는 사람을 말합니다.
   4-1. (4.에서 ①에 답한 경우만) 개인정보관리담당자는 개인정보 보호에 관한 업무 이외에 하는 별도의 업무가 있다.
   ① 그렇다( ) ② 아니다( )
   4-1-1. (4-1.에서 ①에 답한 경우만) 개인정보 보호에 관한 업무와 별도의 업무 중에서 주된 업무는 개인정보 보호에 관한 업무이다.

① 그렇다( )　　② 아니다( )

4-2. (4.에서 ①에 답한 경우만) 개인정보관리담당자가 개인정보 보호 등 담당 업무를 맡은 기간은 얼마입니까? _____년

4-3. (4.에서 ①에 답한 경우만) 개인정보관리담당자는 개인정보 보호 등 담당 업무와 관련한 교육을 받았다.

① 그렇다( )　　② 아니다( )

4-3-1. (4-3.에서 ①에 답한 경우만) 개인정보 보호 등 담당 업무와 관련한 교육을 받은 회수는 총 몇 회입니까? _____회

4-3-2. (4-3.에서 ①에 답한 경우만) 개인정보 보호 등 담당 업무와 관련한 정보보호 교육을 실시한 기관을 모두 써주십시오. _____

4-3-3. (4-3.에서 ①에 답한 경우만) 개인정보 보호 등 담당 업무와 관련한 교육은 법적·기술적 전문성 확보에 도움을 주었다.

① 그렇다( )　　② 아니다( )

4-3-4. (4-3.에서 ②에 답한 경우만) 개인정보 보호교육을 받지 않은 이유는 무엇입니까?

① 개인정보 보호교육을 받기 귀찮아서( )
② 개인정보 보호교육이 있는 줄 몰라서( )
③ 개인정보 보호에 대해 잘 알고 있어서( )
④ 개인정보 보호교육이 필요하지 않다고 생각해서( )
⑤ 개인정보 보호교육이 부실할 것 같아서( )

5. 개인정보 보호에 관한 기관내 정책이나 규정 등을 직원들이 인지할 수 있도록 공개하고 있다.

① 그렇다( )　　② 아니다( )

6. 기관의 전체적인 사업 계획 및 내용은 개인정보보호 관련 법률·지침·가이드라인 및 내부 규정 등을 충실하게 반영하고 있다.

① 그렇다( )　　② 아니다( )

7. 조직 내 개인정보보호정책은 개인정보보호 관련 법령의 제·개정, 보안기술의 발전 등에 따라 수시로 변경되고 공개된다.

① 그렇다( )　　② 아니다( )

**[문 2] 개인정보 수집단계에서 발생할 수 있는 개인정보 침해 문제와 관련되는 다음 질문에 답해주십시오.**

1. 사업목적 달성에 필요한 최소한의 개인정보만을 수집한다.

① 그렇다( )　　② 아니다( )

2. CCTV, 지문・홍채・유전정보 등 생체정보, 병력, 종교・정당 가입 여부 등 정보주체의 민감한 개인정보가 수집된다.
   ① 그렇다( )　　② 아니다( )
3. 정보주체의 주민등록번호를 수집하고 있다.
   ① 그렇다( )　　② 아니다( )
4. 개인정보 수집항목을 정보주체가 필수사항과 선택사항으로 구분하여 기재할 수 있도록 절차나 시스템이 구성되어 있다.
   ① 그렇다( )　　② 아니다( )

**[문 3] 개인정보의 이용・제공・공유, 보유 및 파기 등에 관한 다음 질문에 답해주십시오.**

1. 개인정보 수집 시 고지하거나 이용약관에 명시한 목적 범위를 넘어 개인정보를 이용하거나 제3자에게 제공하는 경우 정보주체로부터 추가적인 동의를 받는 절차와 방법이 마련되어 있다.
   ① 그렇다( )　　② 아니다( )
2. 개인정보를 타기관에 제공할 경우에는 사용목적이 다했을 때 즉시 폐기토록 하고 있다.
   ① 그렇다( )　　② 아니다( )
3. 제3자 제공내역이 대장 등에 기록・보관되고 있다.
   ① 그렇다( )　　② 아니다( )
4. 개인정보의 열람・출력에 대한 기록이 시스템에 자동 저장되거나 수기로 대장에 기록・보관되고 있다.
   ① 그렇다( )　　② 아니다( )
5. 회원탈퇴, 서비스기간 종료, 본인정보 삭제 요청 등이 있는 때에는 관련법령에 의해 보유해야 하는 경우를 제외하고는 지체없이 해당 개인정보를 파기한다.
   ① 그렇다( )　　② 아니다( )

**[문 4] 다음은 개인정보 처리의 위탁 등에 관한 질문입니다. 해당사항이 있는 경우에만 답해주십시오.**

1. 위탁 처리되는 개인정보가 안전하게 관리될 수 있도록 위탁 업무의 범위 내에서 개인정보 보호 교육 등 수탁기관에 대한 적절한 관리・통제시스템이 구축되어 있다.
   ① 그렇다( )　　② 아니다( )

2. 위탁관리자 및 운영자 등에 대해 정기적으로 개인정보보호 관련 교육을 시행하고 있다.

① 그렇다( ) ② 아니다( )

2-1. (2.에서 ② 응답자만) 위탁관리자 등에게 교육을 하지 않는 이유는 무엇입니까?

① 교육의 필요성을 느끼지 않아서( )

② 교육에 따른 비용이 많이 들어서( )

③ 수탁기관이 기본적인 사항을 파악하고 있어서( )

④ 수탁기관 직원에 대한 보안교육 사항이 마련되어 있어서( )

⑤ 현재의 관리적·기술적 보호조치로 충분해서( )

⑥ 기타 (적어주세요 :_____)

3. 수탁기관 또는 협력기관 등에서 접근할 수 있는 개인정보의 범위가 명확하게 정의되고 문서화되어 있다.

① 그렇다( ) ② 아니다( )

4. 개인정보 처리의 위탁 종료 시 수탁기관으로부터 개인정보를 회수·파기하는 절차를 수립하여 적용하고 있다.

① 그렇다( ) ② 아니다( )

5. 개인정보관리 위탁시 수탁기관의 개인정보처리과정에 대한 정기 감사를 실시하고 있다.

① 그렇다( ) ② 아니다( )

**[문 5] 정보주체의 권리보장 조치에 관한 다음 질문에 대해 어떻게 생각하십니까?**

1. 개인정보취급방침을 변경할 경우 미리 전자우편으로 통지하거나 웹사이트 공지사항 등을 통해 정보주체가 개인정보보호방침의 변경을 알 수 있도록 조치를 취하고 있다.

① 그렇다( ) ② 아니다( )

2. 정보주체가 자신의 개인정보를 스스로 열람·정정할 수 있는 절차가 마련되어 있다.

① 그렇다( ) ② 아니다( )

3. 정보주체가 자신의 개인정보에 대한 제3자 제공 내역을 요청할 수 있는 절차가 마련되어 있다.

① 그렇다( ) ② 아니다( )

4. 개인정보의 열람절차에 따른 개인정보 열람 청구를 처리한 경험이 있다.

① 그렇다( ) ② 아니다( )

4-1. (4.에서 ① 응답자만) 열람 청구를 처리한 후에 정보에 잘못이 있다 하여 정정·삭제청구를 받은 경험이 있다.

① 그렇다( ) ② 아니다( )

5. 정보주체가 자신의 개인정보에 대한 정정을 요구하는 경우 이를 확인하고 당해 정보를 정정하기 전까지 개인정보가 이용되지 않도록 하는 절차가 마련되어 있다.

① 그렇다( ) ② 아니다( )

**※ 아래 질문은 민간기관만 답해주십시오.**

6. 정보주체가 동의철회(회원탈퇴, 서비스 이용계약 해지 등)를 하는데 관련 법령 또는 계약상에 일정한 제약이 있다.

① 그렇다( ) ② 아니다( )

6-1. (6.에서 ① 응답자만) 만약 그렇다면, 이를 정보주체에게 미리 고지하거나 서비스 이용약관 등에 명시하고 있다.

① 그렇다( ) ② 아니다( )

**[문 6] 개인정보 보호를 위한 인적 통제에 관한 다음 질문에 대해 어떻게 생각하십니까?**

1. 정보시스템 설계부터 운영에 이르기까지 시스템 구축의 전 과정에 관련된 전산담당자에 대한 개인정보보호 교육 프로그램이 있다.

① 그렇다( ) ② 아니다( )

2. 정보주체의 개인정보를 다루고 있는 모든 직원에게 각 직무별로 특화된 교육시스템이 상세하게 마련되어 있다.

① 그렇다( ) ② 아니다( )

3. 정보주체의 개인정보에 대한 내부직원들의 접근 권한 및 권한별 직무 범위에 차등을 두거나 데이터의 중요도 별로 각각 다른 ID/PW를 부여하는 등 구체적으로 설정되어 있다.

① 그렇다( ) ② 아니다( )

3-1. (3.에서 ④,⑤ 응답자만) 내부직원들의 개인정보 접근권한 및 권한별 직무 범위에 차등을 두지 않는 이유는 무엇입니까?

① 내부직원이 많지 않기 때문에 ( )

② 개인정보 접근권한에 차등을 둘 만큼 많은 정보를 수집·이용하지 않기 때문에( )

③ 개인정보 접근권한에 차등을 둘 필요성을 느끼지 않기 때문에( )

④ 내부직원들도 개인정보 취급방침을 잘 숙달하고 있기 때문에( )

⑤ 기타 (적어주세요 :_____)

## <부록 3> 행정정보공유추진위원회 소위원회 회의록 중 개인정보 보호 관련 내용

### □ 2차 소위원회 (2006. 1. 12)

○ 행정정보공유체계 종합계획 및 추진전략 측면

- 행정정보의 공유도 중요하나, 공유의 필요성을 줄일 수 있는 방안 중요
  - ·행정정보공유를 통한 문서 감축 및 진위여부 확인 등 프로세스 혁신 방안이 가능하도록 해야 함
  - ·공공기관·금융 등 민간 부분의 접근방법은 서비스 종류와 정보 범위에 따라 프로세스를 재설계하고, 정보의 접근권한도 4단계가 아니라 정보특성이나 이용목적에 따라 차별화할 수 있어야 함.
- 공유추진이 금융기관까지 확대할 때 정부와 민간 간 책임소재 문제도 명확히 검토하여 마련할 필요 있음

○ 행정정보공유관련 법·제도 측면

- 제도적 측면으로 개인정보보호 관련 법안 비교 분석 및 개인정보보호 영향평가제의 현실가능성 타진할 것

### □ 5차 소위원회 (2006. 3. 23)

○ 국민의식조사 보고 회의결과 주요내용

- 국민의식조사 결과가 공유 찬성 등 우리가 고려한 방향으로 동일하나,
- 금융기관과의 공유가 행정·공공기관과의 공유보다 민감하다는 의견이 있으므로 방안 고려할 것
- 본 조사시에는 행정정보공유에 대한 향후 2년간의 로드맵을 보다 명확히 하여 체계적으로 추진한다는 인상을 줄 것
- 시민단체의 경우, 여론을 조성하는데 많은 영향성이 있으므로 추가로 조사 필요
  ·추가 조사 시, 공유의 필요성에 대해 설명할 수 있는 기회로 활용
- 국민의식조사에 대한 타이틀을 거부감이 없는 제목으로 변경했으면 함(국민인식조사 등)
- 국민의식조사 자체는 홍보성 및 교육성 효과가 크기 때문에 그에 따라 수행할 것

### □ 7차 소위원회 (2006. 6. 1)

○ 행정정보공동이용법 관련, 공동이용법은 대상범위를 행정정보에서 정책정보까지 확대하여 종합적인 정보공동이용법으로 제정해야 됨

※ 행정정보공동이용법(안) 제5조3항을 신설하여 정책정보 등을 공동이용할 수 있도록 규정

○ 법인 및 개인 처벌 조항

- 정보의 오·남용 등의 우려가 크므로 다른 법률보다 처벌조항을 강화하고, 특히 법인의 경우 개인보다 처벌조항을 강화해야 됨
- 그러나 개인과 법인의 처벌조항을 달리하는 경우가 없고, 법제처·국회 등에서 형평성 문제를 제기할 수 있음
- 따라서, 행정정보 공동이용은 국민들의 개인정보보호와 직접 관련이 있는 만큼 처벌조항을 강화하는 등 차별화할 수 있도록 추진 필요

**□ 8차 소위원회 (2006. 6. 29)**

○ 5개 공공기관 시범운영계획 보고 중 개인정보보호 측면

- 보안 및 개인정보보호에 대한 구체적인 방안 필요
  - 시스템상의 정보유출, 데이터 복호화시 정보유출, 인적보안에 의한 정보유출 등 단계적 요소별 보안대책 수립
  - 사전에 시스템이 공격받을 수 있는 상황을 예견하여 구체적인 대응체계 마련
- 감독기관 요청 시 수시로 이용기관에서 정보이용상황 점검결과 보고서를 제출할 수 있는 체계 필요
- 프로세스 보안 검토팀을 구성하여 내용 검토 추진 필요

**□ 9차 소위원회 (2006. 8. 4)**

○ 행정정보공동이용법 제정 측면

- 새로 제정하는 행정정보공동이용법과 전자정부법과의 관계를 명확히 하여야 할 것임
- 정책정보와 관련하여 정보의 생성제공에 대한 법조항을 넣는데 정책정보에 대한 조금은 부족한 부분이 있는 것 같아서 보완해야 함
- 벌칙조항에서 예외적으로 위법으로 금전적 이득이 있을 시 50배라는 규정은 50배가 5,000만 원 한도에서 50배라면 50배를 넣을 필요가 없을 것임
- 정보를 보유한 기관은 소관행정정보의 공동이용에 있어서 사고가 발생했을 경우에는 중단 또는 승인철회를 할 수 있다 라는 규정을 강화했으면 좋겠음
- 공동이용에 대한 개념을 “행정기관의 보유하고 있는 개인정보를 이용기관이 활용할 수 있도록 그 정보소유자의 동의하에 제공기관에 정보제공을 하는 행위”로 규정하는 것을 검토

○ 5개 공공기관 정보이용승인 추진 측면
- 공공기관은 행정정보 공동이용을 하고 싶다 안 하고 싶다 그런 차원이 아니라 대민서비스 차원에서 국민한테 더 좋은 서비스를 하기위한 것이므로 꼭해야 될 것임
- 불필요한 서류 요청에 대한 서류감축이 선결되어야 하고 정보보유기관 쪽에서 정보제공을 거부하는 것에 대한 타당성에 대하여 면밀히 검토해야 함
- 공동이용정보 70여종에 대하여 이용기관에서 필요하다고 하는 각각의 정보에 대하여 필요성에 대한 연구가 있어야 함
- 금번 시범사업기관에서 필요로 하는 11종의 서류는 서류감축차원을 넘어서 꼭 필요한 것으로 보임
- 4대 기관의 경우에 정보축적을 해야 된다고 하니까 클러스터링을 하면 기관마다 특성이 나오고 그 특성에 따라 축적필요여부 등의 연구가 진행되었으면 좋겠음

□ 10차 소위원회 (2006. 8. 24)
○ 행정정보 공유확대 홍보 측면
- 실제로 이용해 본 국민들의 사례 등 기획 프로그램을 활용하는 홍보방안 활용이 효율적임
- 홍보 브로슈어 등은 홍보차원에서 좋은 수단이 되나 제작비용이 낭비되지 않도록 적절한 수준에서 제작해야 함
- 행정정보공유의 변화하는 모습 등에 대해 호감이 가는 긍정적인 기사를 조금씩 게재하는 것도 훌륭한 홍보방안임

○ 범정부 정책정보공유 방안 측면
- 정책정보공유는 장기플랜을 기반으로 추진 필요
  · 기반조성을 위해 30년 이상의 시간과 노력을 투자하고 있는 핀란드 등의 해외 사례에서처럼, 우리도 장기적인 계획을 수립하여 추진하여야 함
  · 현 정부에서 할 수 있는 일과 차기정부에서 할 수 있는 일을 구분하고 정책의 연속성을 유지하면서 추진해야 함
- 정책정보공유는 민원서류를 공유하는 서비스보다 행정효율을 극대화할 수 있는 방안임
- 행정정보공동이용법에는 정책정보공유를 시작할 수 있는 여지를 두고, 정책정보공유의 대상과 내용이 구체화되면 별도법으로 분리하여 추진하는 것이 바람직할 것임
- 정책정보공유 시 개인정보보호 문제는 중요하게 다루어야 함

・정책정보 이용자는 행정기관의 의사결정자이므로 개인정보보호 문제보다는 누가 주관하여 추진하는가가 중요함
・다른 관점에서 정부가 개인정보를 수집하는 자체를 반대하는 의견도 있으므로 개인정보보호 문제는 중요하게 다루어야 함

□ 12차 소위원회 (2007. 2. 15)

○ 호적・제적정보 공동이용 측면
- 호적정보 공동이용은 대법원의 의견대로 이용범위를 행정기관 민원사무에 한정하면 행정정보공동이용서비스 효과가 줄 것임
・호적은 개인의 모든 신상정보를 포함하므로 여성시민단체에서 정보공유에 대해 부정적인 입장이며, 향후 변경되는 제도에서는 용도별로 나누어 증명서를 발급할 것임
- 대법원 의견은 관련 법 마련에 따라 호적정보의 정보공유 범위를 확대할 수 있으며, 제적은 2008년부터 제도가 변경되므로 행정정보공동이용법의 별첨 목록에서 삭제하기를 요청함
- 대법원 호적과와 의견을 계속적으로 조율할 것

○ NGO에서 개인정보보호법에 관심이 많으므로 개인정보보호 기본법의 추진에도 주시를 해야함
- 개인정보보호기본법이 국회에서 진척이 없어 공공기관의개인정보보호에관한법률의 주요내용을 행정정보공동이용법이 포함되도록 추진

□ 14차 소위원회 (2007. 3. 21)

○ 미 제공 행정정보 보유기관과 협의 추진 관련
- 현재까지 정보제공기관에 1,505건을 요청했는데 608건(40%)을 승인받았고, 국세청, 법무부 등에서 승인을 거부하고 있어 승인률이 매우 저조한 실정임
- 정보제공에 관한 법적근거가 미약하여 국세청 등 행정정보 보유기관이 공공・금융기관의 오・남용에 대한 불안감으로 제공을 꺼리고 있으므로, 정보공유과정에서 절차상의 문제가 없을시 제공기관 담당자는 법적책임이 없다는 근거가 있어야 안심하고 제공 승인을 할 것임

○ 행정정보 보유기관의 미 제공 사유 설명 및 토론 내용
- 보건복지부 : 공공기관의 경우에는 장애인증명서를 활용하고자하는 목적이 분명하고 구체적으로 명시가 되어 있어 승인을 하였으나, 금융기관은 이용사무의 목적이 분명하지 못할 뿐 아니라 정보의 주체인 장애인들이 정보가 노출되는 것을 꺼려

하고 있어 승인을 보류하였음

· 행정정보공유 추진단에서 장애인 단체와 만나 개인정보 노출에 문제가 없음 등을 설명하고 설득하여 동의를 얻었을 수 있도록 보건복지부에서 준비하여 주시면 좋겠음

- 대법원 : 제도적, 기술적으로 미비점이 있는 상태에서 개인의 프라이버시에 관해 본질적인 내용을 이루고 있는 호적·제적정보를 공공·금융기관에까지 제공하는 것은 원칙적으로 제외하는 것이 타당하다는 의견임

· 기술적인 측면은 이용기관 담당자가 자기인증서를 이용해서 담당자만이 접근할 수 있도록 하였으며, 인터넷 망에서 해킹을 방지할 수 있는 강한 암호화와 증적관리시스템을 구축하는 등 현재의 기술 중에서 가장 완벽한 기술을 사용하여 오남용의 우려는 크지 않을 것임

· 개인정보 보호의 원칙 중에는 공공기관의 개인정보보호에 관한법률에 정보주체가 자기정보를 스스로 통제할 수 있는 권리가 있으므로 본인동의라는 절차 하에 호적정보를 제공하는 것은 문제가 없음

· 호적정보를 항목마다 코드를 정하여 데이터 레벨링하여 제공하고 있으므로 종이문서보다 개인정보가 보호되고 있음

· 전자정부 추진사업이 효율성만 강조하면서 다른 가치를 희생시키는 것이 아니고, 효율성도 높이고 프라이버시 보호라는 가치도 올릴 수 있다는 마인드로 접근해야 함

· 보안상의 기술적인 문제가 보장이 되어야 하고, 법률적으로도 현재 전자정부법의 근거규정 조항 내용으로 정보제공이 충분한 것인지 대법원에서 검토해주시고 불충분하다면 보완 의견도 제시해 주시기 바람

· 오프라인상의 종이문서에서 생기는 여러 가지 불필요하고 민감한 정보들이 행정정보공유시스템이 보완해주는 수단이 됨

· 종이문서는 제출 후 악용을 확인이 안 되지만 행정정보공유시스템은 증적관리가 되기 때문에 이런 문제가 해결될 것임

- 법무부 : 공동이용의 법적근거, 오남용시 제공기관의 책임소재, 일반사무에 대한 정형화 문제 등이 있는 상황에서 공공·금융기관에까지 확대하는 것은 곤란하다는 의견임

· 현재의 법적인 환경에서 최소한 제공기관이 적법한 절차에 따라서 정보제공을 할 수 있는 법적환경은 갖추어 졌다고 봄

· 법도 시대 상황에 따라 변천·발전되어 온 것이기 때문에 완벽한 법제도에 맞추어 시행하여야 한다는 마인드를 버리고 문제가 생기면 보완·발전시키는 방향으

로 추진하여야 할 것임

- 행정정보공유시스템 자체가 현재의 문제점 등을 보완할 수 있는 보완 시스템의 역할을 할 수 있다는 점과 법적근거는 상세하고, 구체적인 근거 외에 포괄적인 근거로 크게 보아 접근할 수도 있을 것임

- 보건복지부 : 34개 공공기관에 대하여는 모두다 승인 예정이나, 금융기관은 정보주체의 금융거래제한 등 권익침해 목적에도 사용할 우려가 있고, 오남용을 제어할 충분한 장치가 없다고 판단하여 정보제공이 곤란함
  - 실제적으로 현재의 종이문서가 오남용을 오히려 제어할 수 없음
  - 종이문서는 오남용을 통제할 수 없으나 공유시스템은 통제가 가능하고 정보공유는 정보공개가 아닌 최소한의 미니멈적 정보공유 개념임
- 국세청 : 국세기본법 제81조의 10 비밀유지조항에서 국세정보제공을 기본적으로 금지하고 있어 행정정보공동이용법이 통과된다 하더라도 공공·금융기관에 정보를 제공하는 것은 곤란하다는 것이 현재 국세청의 입장임
  - 법리적인 문제라면 국세청과 추진단이 법제처와 협의를 해서유권해석을 받아 해결하면 될 것임

□ 20차 소위원회 (2008. 5. 15)

○ 행정정보공동이용 확대대상기관(공공·금융기관) 선정 건

- 공동이용 시 출력사례의 최소화
  - 행정정보공동이용 시 국회나 감사원 등 외부기관에 증빙자료로 제출하기 위한 사유 등으로 출력하는 경우 제도개선 등을 통하여 출력하는 사례가 최소화되도록 해야 함
  - 종이문서 출력을 제한적으로 허용하는 문제는 현행 출력 실태조사 결과를 토대로 다음에 별도 안건으로 상정하여 검토하되, 구비서류 원본과 공동이용 출력물을 비교할 수 있도록 준비 필요
- 대상기관(공공·금융) 확대의 속도조절이 필요함
  - 아직 행정정보공동이용법 등 제도적 장치가 완비되지 않은 상태에서 공동이용 활성화의 당위성에만 초점을 맞추어 확산에 너무 치중할 필요는 없을 것임
  - 무조건적으로 확산에 치중하기보다는 전략적 차원으로 접근하여 어느 정도의 속도조절과 선별적인 대상선정이 필요함
  - 확대 대상기관 선정기준에 시스템적 보안보다는 그것을 관리하는 사람의 관리자세와, 기관의 사회적 평판도가 매우 중요하고, 특히 외국계 은행은 전략적 차원에서 검토해 볼 필요가 있음

- 보안성 검토결과를 기준으로 확대 대상기관 조건부 선정
  - 수요조사(서면조사) 및 현장실사, 보안성검토 등 결과를 재검토하여, 특히 보안성 검토결과가 우수로 판정받은 기관은 확대 대상기관에 포함하고,
  - 행정정보 공동이용 확대 구축사업의 추진일정('08.8월말 종료)을 감안, 협약체결 이전까지 보완조치하여 우수로 판정받은 기관에 대해서는 추가로 확대 대상기관에 포함하고, 최종 선정 이전에 전산 프로그램 개발 등을 우선 진행
  - 보완조치 후에도 우수상태에 미달되는 되는 것으로 판정된 기관에 대해서는 재점검 후 우수상태가 되기 전까지는 서비스 개시를 보류하고 보완 이후 대상기관으로 추가 선정

## 개인정보 수집 • 유통 실태조사


(100-842) 서울시 중구 무교동길 41 금세기 빌딩 (을지로 1가 16)
발 행 일 : 2009. 12
발 행 인 : 현 병 철
발 행 처 : 국가인권위원회
전　　화 : 02) 2125-9759　　FAX : 02) 2125-9733
U R L　: http://www.humanrights.go.kr

ISBN 978-89-6114-181-9 93330

# 개인정보 수집 • 유통 실태조사

국가인권위원회

인 쇄 일 : 2009년 12월
발 행 일 : 2009년 12월
발 행 인 : 현 병 철
발 행 처 : 국가인권위원회
주　　소 : (100-842) 서울시 중구 무교동길 41 금세기 빌딩
전　　화 : 02) 2125-9759
F A X : 02) 2125-9733
U R L : http://www.humanrights.go.kr
인 쇄 처 : 한길문화사