

연구보고서 2000-09

치안정보의 효율적인 관리방안에 대한 연구

- 경찰의 정보관리에 대한 입법적 개선방안을 중심으로 -



〈 研 究 陣 〉

연 구 자 : 김 연 태 (고려대 교수)

비

명

목 차

약 어 표	9
제1장 도입부	11
I. 연구의 동기와 목적	11
II. 연구의 범위	12
III. 연구의 방법	15
제2장 경찰의 정보관리와 정보의 자기결정권	17
I. 독일 연방헌법재판소의 인구조사판결	17
1. 인구조사판결의 내용	17
2. 인구조사판결 이전의 연방헌법재판소의 판결	19
3. 인구조사판결의 의의	20
II. 정보의 자기결정권의 헌법적 근거	21
1. 일반적 인격권과 사생활의 비밀과 자유	21
2. 주거의 자유	23
3. 통신의 자유	24
4. 양심의 자유	25
5. 언론·출판의 자유	26
6. 집회·결사의 자유	27
III. 정보의 자기결정권의 내용	28
IV. 정보의 자기결정권의 한계	29
V. 강제적인 정보수집의 조건	30
VI. 인구조사판결의 경찰영역에의 적용	31

VII. 인구조사판결의 경찰 정보처리에 대한 귀결	33
제3장 독일에 있어서 경찰의 정보관리에 관한 법적 규율	37
I. 통일경찰법모범초안에 대한 개정초안	37
II. 정보보호법과 경찰의 정보관리	39
1. 수권규정으로서의 정보보호법	39
2. 정보보호법의 경찰영역에의 적용	40
III. 경찰의 정보관리에 관한 법적 규율	41
1. 경찰에 의한 정보수집	41
(1) 개념정의: 정보의 수집	41
(2) 개괄적 수권조항에 의한 정보수집	42
(3) 정보수집에 대한 법적 규율	44
2. 경찰에 의한 정보의 처리: 정보의 저장, 수정, 이용	55
(1) 정보의 저장	55
(2) 정보의 수정	57
(3) 정보의 이용	57
3. 정보의 제공	59
(1) 정보제공의 의의	59
(2) 법적 근거 및 목적구속의 원칙	60
(3) 온라인 연결	60
4. 정보의 정정, 삭제, 차단	61
5. 고지청구권	64
제4장 우리나라에서의 치안정보의 관리현황 및 문제점	66
I. 머리말	66
II. 경찰정보의 수집·처리 상황	67

1. 개념	67
(1) 정보의 개념	67
(2) 개인정보의 개념	69
(3) 수집·처리의 개념	69
2. 경찰정보 수집·처리의 기본유형	70
(1) 첩보수집	70
(2) 컴퓨터 입력자료의 수집	71
(3) 전산자료의 활용	73
(4) 기타 경찰조치	75
III. 경찰 정보수집·처리에 대한 법적 근거	75
1. 머리말	75
2. 법적 근거의 필요성	76
3. 현행법상 경찰정보 수집·처리의 법적 근거	76
(1) 경찰의 직무범위와 권한	76
(2) 경찰 정보수집·처리를 규율하는 법률규정	80
4. 소 결	84
IV. 경찰 정보처리와 개인정보보호	85
1. 개인정보보호의 의의	86
(1) 개인정보보호의 이념	86
(2) 개인정보보호의 헌법적 근거	87
2. 공적부문에서의 개인정보보호의 문제	88
(1) 주민등록증에 의한 개인정보의 문제	88
(2) 영상감시	90
(3) 통신감청	91
(4) 인구조사	92
(5) 출국자에 대한 신원조사	93

(6) 기 타	94
3. 외국의 개인정보보호법제	94
(1) 스웨덴	94
(2) 독 일	95
(3) 영 국	96
(4) 미 국	97
(5) 일 본	98
4. 개인정보보호법제의 국제적 동향	98
(1) OECD의 프라이버시 보호와 개인정보의 국제유통에 관한 가이드라인	98
(2) EU의 개인정보의 자동처리에 따른 개인의 보호에 관한 조약	100
5. 우리나라의 법제화 동향	100
(1) 법제의 특색	100
(2) ‘공공기관의 개인정보보호에 관한 법률’	101
(3) 개인정보보호지침	102
V. 경찰 정보처리활동의 변화 양태와 전망	104
1. 경찰 정보처리 영역의 확대	104
(1) 양적인 증가	104
(2) 질적인 변화	104
2. 새로운 과학적 수단의 등장	105
(1) 전자감시장치	105
(2) 유전자지문(DNA Fingerprint)	106
3. 시민저항운동의 확대	106
4. 소 결	107
제5장 결론 : 효율적인 치안정보 관리를 위한 입법적 제안	108
I. 정보처리에 관한 일반적인 규정	108

1. 경찰의 직무범위	108
2. 다른 행정기관과의 관계	109
3. 비례의 원칙	110
II. 개별적인 정보처리 시 준수해야 할 원칙	111
1. 정보수집	111
(1) 정보수집에 대한 수권조항	111
(2) 정보수집의 일반원칙	112
(3) 공개된 행사, 모임 및 집회에서의 정보수집	113
2. 정보의 처리	114
(1) 저장 및 목적구속의 원칙	114
(2) 아동에 대한 정보의 저장	115
3. 정보제공	116
4. 정보의 정정·삭제·차단	118
참 고 문 헌	119

비

면

약 어 표

Abs.	Absatz
Art.	Artikel
ASOG berl	Berliner Allgemeines Gesetz zum Schutz der öffentlichen Sicherheit und Ordnung
Aufl.	Auflage
BayPAG	Bayerisches Polizeiaufgabengesetz
BayVGH	Bayerischer Verwaltungsgerichtshof
BDSG	Bundesdatenschutzgesetz
Brbg	Brandenburg, brandenburgisch
BremPolG	Bremisches Polizeigesetz
BT-Drucks.	Bundestagsdrucksache
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BW	Baden-Württemberg, baden-württembergisch
BWPolG	Baden-Württembergisches Polizeigesetz
DSG	Datenschutzgesetz
DÖV	Die öffentliche Verwaltung
Einf.	Einführung
f.	folgende
ff.	fortfolgende
HambDVPolG	Hamburgische Durchführungsverordnung zum Polizeigesetz
HbgDSG	Hamburgisches Datenschutzgesetz
HDSG	Hessisches Datenschutzgesetz
Hrsg.	Herausgeber
HSOG	Hessisches Gesetz über die öffentliche Sicherheit und Ordnung
JZ	Juristenzeitung

MV	Mecklenburg-Vorpommern
NGefAG	Niedersächsisches Gefahrenabwehrgesetz
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NW	Nordrhein-Westfalen, nordrhein-westfälisch
PolG BW	Polizeigesetz von Baden-Württemberg
PolG NW	Polizeigesetz von Nordrhein-Westfalen
Rdn.	Randnummer(n)
S.	Seite, Satz
SächsPolG	Polizeigesetz des Freistaates Sachsen
SGB	Sozialgesetzbuch
SH	Schleswig-Holstein, schleswig-holsteinisch
SOG	Gesetz über die öffentliche Sicherheit und Ordnung
SOGMV	Gesetz über die öffentliche Sicherheit und Ordnung in Mecklenburg-Vorpommern
SPolG	Saarländisches Polizeigesetz
ThürPAG	Thüringer Gesetz über die Aufgaben und Befugnisse der Polizei
VE ME PolG	Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes
VerwArch	Verwaltungsarchiv
ZRP	Zeitschrift für Rechtspolitik

제1장 도입부

I. 연구의 동기와 목적

정보통신기술의 급속한 발전에 의한 새로운 정보처리기술의 도입은 국민의 생활관계에 지속적인 변화를 가져왔다. 행정기관에 의한 정보처리에 있어서 기술의 발전은 행정업무의 효율적인 수행을 위한 조건을 제공하는 반면에 감시·감독·통제의 가능성, 일차리의 축소 및 인간관계의 변질 등 부정적인 측면을 지니고 있다. 기술의 발전, 특히 새로운 정보처리기술의 도입은 인간의 삶의 질을 향상시키는 경우에만 의미가 있는 것이다. 그러나 종래 개인은 국가작용의 객체로서 개인에 대한 정보는 국가기관의 권력행사를 위한 기초로서 사용되었으며 국가에 의해 평가되고 이용되었을 뿐, 개인은 자기의 정보가 어떻게 이용되고 처리되는지에 대하여 알지 못하였다.

그러나 자기에 관한 정보가 어떻게 처리되고 또한 누구에게 전달될 수 있는지를 아는 것은 매우 중요하다. 개인이 자신의 정보처리에 대하여 알지 못한다거나 또는 국가기관의 정보처리의 불투명성은 국민의 불안을 야기한다. 이것은 행정기관에 의한 정보처리의 적법성이 보장됨으로써 해소될 수 있는 것이다. 적법한 정보처리를 요구하는 것은 정보처리의 제한과는 구별하여야 한다. 개인의 정보보호에 의하여 경찰의 직무수행에 지장을 가져올 것이라는 우려는 타당하지 않다. 정보수집 및 정보처리와 정보보호는 동전의 양면과 같은 것이다. 정보처리의 목적, 이유, 형태 등에 관계없이 정보를 처리하는 자는 항상 관련된 정보보호법상의 원칙을 준수하여야 한다. 오늘날의 정보사회에 있어서는 행정기관의 업무수행을 위하여 필요한 정보를 많은 경우 시민의 협력에 의하여 획득하게 되는데, 행정기관에 의한 적법한 정보처리는 시민의 참여를 위한 필수 불가결한 전제조건이라 할 수 있다.

행정기관의 각종 자료나 정보는 행정정책이나 조치의 기초가 된다. 정보사회에 있어서 행정기관이 그 상대방인 국민에 대하여 정보에 있어서 우월한 권한을 행사하게 된다면, 행정절차의 민주성 확보는 어려워질 것이다. 1960년대 후반부터 세계 각 국에서는

행정기관의 정보처리에 있어 적법성을 유지하는 것이 중요하다는 점을 자각하고 개인정보를 보호하는 법률을 제정하여 왔다. 특히 미국을 비롯하여 대부분의 서유럽 국가들은 1970년대부터 1980년대 사이에 개인정보보호법을 제정하여 시행하고 있다.¹⁾ 우리나라는 1994년도에 ‘공공기관의 개인정보보호에 관한 법률’을 제정하였으나, 아직까지 국민의 낮은 정보보호의식과 입법적인 지원의 부족으로 인하여 정보보호에 미흡한 편이며, 실제로 개별분야에서 적용하려고 할 때 적용범위와 규율내용의 모호성 등으로 인하여 실효성을 거두지 못하고 있다는 비판을 받고 있다.²⁾

경찰작용은 본래적인 특성상 다른 어떤 국가행정작용 보다도 개인의 정보에 관한 권리를 침해할 개연성이 높음에도 불구하고 이에 대하여 정보보호법의 일반규정을 제외하고는 거의 법적인 통제가 되고 있지 않다고 해도 과언이 아닐 것이다. 따라서 다른 나라의 법제와의 비교, 특히 우리나라와 법제가 유사하고 정보보호법에 관한 모범적인 국가로 보이는 독일의 경우와 비교하는 것은 매우 의미 있는 일이라고 생각한다.

II. 연구의 범위

경찰의 개념은 법적으로 정의되지 않고 있고, 제도적 내지 형식적 의미 또는 실질적 의미 등 다양한 의미로 사용되고 있다. 본 연구에서는 경찰개념을 제도적 의미로 사용하기로 한다. 따라서 경찰법이라 함은 실정법상 보통경찰기관이 담당하는 모든 작용에 관한 법을 의미한다.

1) 독일에서는 정보의 수집 및 처리가 기본권에 대한 침해를 가져올 수 있다는 인식 하에 1970년에 헤센 주가 처음으로 정보보호법을 제정하였고, 1977년에는 연방정보보호법이 제정되었다. 덴마크는 1978년에 공적 영역뿐만 아니라 사적 영역에서의 정보보호에 관한 법률을 제정하였다. 또한 스웨덴은 1973년, 프랑스는 1978년, 노르웨이는 1978년, 오스트리아는 1978년, 룩셈부르크는 1979년부터 정보보호에 관한 법률을 제정·시행하고 있다. 영국은 1984년, 핀란드는 1987년, 네덜란드는 1988년, 포르투갈은 1991년부터 정보보호에 관한 법률을 제정·시행하고 있다.

2) 김일환, 개인정보보호법제의 정비방안에 관한 연구, 한국법제연구원, 1997, 16쪽 아래.

제도적 또는 형식적 의미의 경찰의 범위를 어떻게 정할 것인지는 전적으로 그 나라의 입법정책에 속하는 문제라고 하겠다. 경찰관직무집행법 제2조에서는 ① 범죄의 예방·진압 및 수사, ② 경비·요인경호 및 대간첩 작전수행, ③ 치안정보의 수집·작성 및 배포, ④ 교통의 단속과 위해의 방지, ⑤ 기타 공공의 안녕과 질서유지를 경찰관의 직무범위로 규정하고 있다. 또한 경찰법 제3조는 “경찰은 국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압 및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 임무로 한다”라고 규정하고 있다.

현재 경찰은 기본적인 업무를 수행하며 범죄, 사회문제, 민심동향 등 치안유지에 관련된 사항에 대한 내용을 접할 경우 이를 보고하여 업무수행에 반영토록 하고 있다. 경찰관직무집행법 제2조 3호는 치안정보의 수집·작성 및 배포가 경찰의 직무범위에 해당함을 명시하고 있는데, ‘치안정보’란 치안목적용 위해서 사용되는 모든 정보를 뜻하는 것으로 그 대상을 한정 지을 수 없어 법률상 특별한 의미가 없다.

그밖에 외근경찰관 근무규칙(경찰청 훈령 제10호) 제59조는 외근경찰관은 근무 중 다음 각호에 정하는 사항을 수집하여 경찰서장에게 보고하여야 한다고 규정하고 있다.

1. 각종 범죄와 방법에 관한 사항
2. 다중 범죄와 관련된 사항
3. 국가의 존립과 안정을 해하는 공산계열에 관한 사항
4. 경제·사회·문화 등 사회문제에 관한 사항
5. 공안·풍속·영업 기타 민심동향에 관한 사항
6. 기타 경찰업무 수행상 필요하다고 인정되는 사항

또한 경찰은 정보생산의 기초가 되는 사항을 수집하여 제출하여야 하는데, 이러한 첩보수집의 대상을 보면 다음과 같다.³⁾

1. 국가안전을 위태롭게 하는 요소
2. 사회불안요인

3) 경찰대학, 경찰실무전서, 1999, 1031-1032쪽.

3. 노사분규의 원인 및 노사협조의 저해요인
4. 사회 저변 시민들의 정보에 대한 요구
5. 시중에 유포되는 유언비어
6. 정부 주요시책의 시행과정상 문제점 또는 제언
7. 국민의 결속력을 저해하는 요소
8. 경제침체의 원인과 활성화를 위한 시책
9. 시민생활과 사회공공질서를 해치는 요소
10. 관내 주민의 고충사항
11. 국내외의 불순분자나 불순자금의 침투 동향
12. 국가정책 발표시 각계 반응 및 정책제언
13. 각종 법령·제도개선이 요구되는 사항
14. 기타 국가기관 및 자치단체에서 시책에 반영할 사항 등

이와 같이 경찰이 수집하는 첩보 또는 정보의 대상은 범죄에 관한 사항에 한정하지 않고 사회 제반 문제에 관한 사항 및 국가정책, 법령, 제도 등 각종 사안에 대한 민심동향 등 그 대상이 되지 않는 영역이 없을 정도로 우리 사회의 모든 분야를 포괄하고 있다.

결국 본 연구에서는 논의의 대상이 되는 정보의 범위를 한정할 필요가 있다. 경찰이 정보를 수집하는 과정 중의 많은 부분은, 예를 들면 파출소 경찰관이 순찰시 알게된 가정집 대문의 시정상태, 공개된 시위군중의 규모에 관한 사실처럼 업무의 성격에 비추어 자연스럽게 이루어지는 사실행위에 불과하므로 법적인 관심의 대상이 되지 않는다. 법적인 논의의 대상이 되는 것은 개인의 권리에 대한 침해의 소지가 있는 개인에 관한 정보의 수집·처리인 것이다. 즉 경찰의 정보관리와 관련하여 법적인 관심의 대상이 되는 것은 개인에 관련된 정보이므로 아래에서는 개인정보에 한정하여 경찰의 정보활동에 대한 법적 고찰을 하기로 한다.

III. 연구의 방법

경찰이 발생된 문제를 분석하고 사안을 해결하기 위하여서는 자세한 정보가 필수적이다. 정보수집과 처리는 경찰영역에서 전혀 새로운 것이 아니다. 경찰작용은 지금까지 계속해서 정보와 밀접한 관련을 맺어 왔다. 위험방지 또는 범죄수사를 위한 조치를 함에 있어서 개인관련 정보가 없다면 직무수행은 불가능할 것이다. 즉 정보수집과 처리는 경찰작용의 핵심이라고 할 수 있다. 그러나 경찰의 정보수집과 처리가 학문적 관심의 대상이 된 것은 그리 오래되지 않는다. 과거에는 국가가 필요한 정보를 수집하는 것은 국가의 당연한 권리로 여겨졌던 것이다. 그러다가 최근에 이르러서 위험방지를 위한 정보의 수집과 처리에 대하여 법적인 관점에서 관심을 기울이기 시작하였다. 이러한 상황은 독일의 경우도 마찬가지이다. 물론 이전에 경찰의 정보처리에 대한 연구가 있었지만,⁴⁾ 본격적인 논의의 출발점이 되고 일련의 법제정과 개정을 촉발한 것은 1983년의 독일 연방헌법재판소의 인구조사판결이라 할 수 있다. 인구조사판결은 경찰에 직접 관련되는 것은 아니지만, 경찰 직무수행의 핵심영역에 중대한 영향을 미치는 내용을 담고 있다. 독일 연방헌법재판소에 의하여 제시된 원칙들은 국가의 정보수집 및 처리 영역을 넘어서 모든 공행정 분야에서 준수되어야 하지만,⁵⁾ 특히 경찰영역에서 중요한 의미가 있다.⁶⁾

독일에 있어서는 오래 전부터 학설, 판례 및 입법에서 정보보호의 문제에 대처해 왔는데 비하여 우리나라의 경우 이에 대하여 지금까지 충분한 논의가 진행되어 왔다고 할 수 없다. 독일의 연방정보보호법(Bundesdatenschutzgesetz)에 대응하는 ‘공공기관의 개인정보보호에 관한 법률’이 1994년에 비로소 제정되어 1995년 1월 8일부터 시행되고 있을 뿐이다. 독일에서는 모든 주의 경찰법에서 개인관련 정보의 수집 및 처리에 관한 권한규정을 두고 있는데, 우리의 경찰관련 법률에 정보보호에 관한 규정은 아직까지 결여

4) 이에 대하여는 Schatzschneider, Ermittlungstätigkeit der Ämter für Verfassungsschutz und Grundrechte, 1979, S. 5 ff. 참조.

5) Hufen, JZ 1984, 1072 참조.

6) 이에 대하여는 Kowalczyk, Datenschutz im Polizeirecht, 1989, S. 1 참조.

되어 있다. 법률유보원칙에 따라 위험방지를 위한 정보적 활동에 의해 개인의 권리가 침해되는 경우에는 그에 대한 법적 근거가 필요하다. 따라서 우리나라의 경우 경찰의 정보 수집과 처리를 위한 법적 근거의 정비가 시급히 필요한 상태이다. 이에 대한 경찰관련 법률의 제정에 있어서 독일에서의 논의와 입법은 우리에게 중요한 참고가 될 수 있을 것이다.

아래에서는 우선 독일 연방헌법재판소의 인구조사판결과 관련하여 정보의 자기결정권에 대하여 살펴보고 경찰의 정보관리에 있어서 지켜야 할 원칙들을 제시하고자 한다. 그 다음에 독일에서의 경찰 정보관리에 관한 법제 및 이론을 고찰한 뒤, 우리나라에서의 치안정보의 관리현황과 경찰의 정보관리에 대한 입법적 개선방안을 모색해 보기로 한다.

제2장 경찰의 정보관리와 정보의 자기결정권

I. 독일 연방헌법재판소의 인구조사판결

1. 인구조사판결의 내용

독일 연방의회는 1982년 3월 25일 인구조사법(Volkszählungsgesetz)을 통과시켰다. 인구조사법의 내용을 보면 제1조에서 제8조까지는 인구조사의 계획과 수행에 관한 내용을 담고 있으며,⁷⁾ 제9조는 인구조사계획에 따라 조사된 정보의 사용과 제공에 관한 규정이다.⁸⁾ 이 법에 따라 인구조사는 1983년 4월 27일에 하기로 확정되었다. 그런데 국민

7) 이 법에 따라 개인은 성, 생년월일, 가족상황, 어떤 종교단체에 속하는지 여부, 국적, 주거상황 등 6 가지 질문에 답해야 했다.

8) [제9조 1항]: “법 제2조 1호 및 2호의 인구조사사항은 신고기록부와 비교되고 그의 정정을 위하여 사용될 수 있다. 인구조사사항으로부터 알게 된 사실은 정보제공의무자에게 부담이 되는 조치를 위하여 사용될 수 없다.”

[제9조 2항]: “법 제2조 내지 제4조에 따라 조사된 사항은 이름을 제외하고는 1980. 3. 14.의 연방통계법 제11조 3항에 의하여 연방과 주의 통계청으로부터 전문적 권한있는 연방과 주의 상급 행정관청에게 그의 권한에 속하는 업무를 수행하기 위하여 필요하는 한 제공될 수 있다. 법 제2조 1호의 종교단체에 대한 법적 소속 또는 무소속에 대한 징표와 법 제4조 1호 c목과 법 제4조 3호 c목의 조사사항을 제외하고, 제1문은 전문적 권한있는 연방과 주의 상급 행정관청으로부터 다른 행정관청, 그 밖의 공공단체 또는 비공공단체가 위임받은 업무를 수행하기 위하여 필요한 경우 그 기관이 상급 행정관청으로부터 제공받는 경우에도 적용된다. 제1항 2문은 여기에도 적용된다.”

[제9조 3항]: “지역계획, 측량, 지역공동체의 계획 및 환경보전의 목적을 위하여 필요한 경우, 법 제2조 1호의 종교단체에 대한 법적 소속 또는 무소속에 대한 징표와 법 제4조 1호 c목과 법 제4조 3호 c목의 조사사항을 제외하고 법 제2조 내지 제4조에 따른 정보제공의무자의 이름을 뺀 조사사항을 주의 통계관청으로부터 게마인데와 게마인데 조합은 제공받을 수 있다. 게마인데와 게마인데 조합은 법 제2조 내지 제4조에 따라 조사된 사항에 대하여 독자적인 통계처리를 할 수 있다. 제1항 2문은 여기에도 적용된다.”

[제9조 4항]: “학문적 목적을 위하여 필요한 경우, 법 제2조 1호의 종교단체에 대한 법적 소속 또는 무소속에 대한 징표와 법 제4조 1호 c목과 법 제4조 3호 c목의 조사사항을 제외하고 법 제2조 내지 제4조에 따른 조사사항(이름과 주소 제외)을 연방과 주의 통계관청은 다른 직무담당자 또는 공무수탁사인에게 제공할 수 있다.”

들이 인구조사법이 인격권을 충분히 존중하지 않는다고 하여 격렬하게 반대하였고, 결국 이 법에 대한 헌법소원이 제기되었던 것이다.⁹⁾

이에 대하여 1983년 12월 15일 독일 연방헌법재판소가 인구조사법에 대하여 내린 결정(인구조사판결: Volkszählungsurteil)의 요지를 살펴보면 다음과 같다.¹⁰⁾

1. 현대적 정보처리의 조건 하에 무제한적인 개인관련 정보의 수집·저장·사용 및 제공으로부터 개인을 보호하는 것은 기본법 제1조 1항과 결합하여 기본법 제2조 1항의 일반적 인격권에 포함된다. 일반적 인격권은 개인에게 원칙적으로 자신에 관한 정보의 공개 및 사용에 대하여 스스로 결정할 권한이 있음을 보장한다.
2. 이러한 정보의 자기결정권에 대한 제한은 중대한 공익이 있는 경우에만 허용된다. 정보의 자기결정권에 대한 제한을 위하여서는 규범의 명확성에 관한 법치국가적 요청에 부합하는 헌법합치적인 법적 근거가 필요하다. 그와 같은 규율을 함에 있어서 입법자는 비례의 원칙을 준수해야 한다. 또한 입법자는 인격권 침해의 위험을 방지할 수 있는 조직법적이고 절차법적인 장치를 마련하여야 한다.
3. 정보의 자기결정권의 제한에 대한 헌법적 요구에 있어서 익명의 형태가 아닌 개인을 식별할 수 있는 방법으로 수집되고 처리된 개인관련 정보와 통계의 목적으로 수집된 정보를 구별하여야 한다. 통계의 목적으로 정보를 수집하는 경우에는 엄격하고 구체적인 정보의 목적구속성을 요구하지 않을 수 있다.
4. 1983년의 인구조사법의 수집에 관한 규정(제2조 1호 내지 7호, 제3조 내지 제5조)은 개인을 등록화 및 목록화하여 인간의 존엄에 반하는 결과를 가져오는 것은 아니다. 인구조사법은 규범명확성의 원칙 및 비례의 원칙에 위반되지도 않는다. 그러나 정보의 자기결정권을 보장하기 위하여 정보수집의 실행과 조직에 대한 보충적인 절차법적 조치가 필요하다.

[제9조 5항]: “제2항 내지 제4항에 의하여 제공받은 조사사항은 그것이 제공된 목적을 위하여만 사용할 수 있다.”

9) 인구조사판결의 경위에 대하여는 김일환, 개인정보보호법제의 정비방안에 관한 연구, 한국법제연구원, 1997, 78쪽 아래.

10) BVerfGE 65, 1 ff. 인구조사판결 이후의 구체적인 입법조치에 대하여는 김일환, 개인정보보호법제의 정비방안에 관한 연구, 한국법제연구원, 1997, 79쪽 아래 참조.

5. 1983년의 인구조사법 제9조 1항 내지 3항의 제공에 관한 규정(특히 신고기록조정: Melderegisterabgleich)은 일반적 인격권에 반하는 것이다. 학문적 목적으로 제공하는 것(1983년의 인구조사법 제9조 4항)은 기본법에 합치한다.

2. 인구조사판결 이전의 연방헌법재판소의 판결

정보의 자기결정권(Recht auf informationelle Selbstbestimmung)이란 표현은 연방헌법재판소의 인구조사판결 이전에도 전자정보처리가 도입된 이후에 정보처리로부터 개인을 보호하기 위한 맥락에서 이미 여러 문헌에서 사용되고 있었다. 즉 슈타인뮐러(Steinmüller)¹¹⁾가 처음으로 ‘정보의 자기결정’이란 표현을 사용한 이후에 이러한 표현을 학자들이 받아들여서 사용하기 시작하였다.¹²⁾

연방헌법재판소도 인구조사판결에서 처음으로 정보의 자기결정권을 일반적 인격권의 한 부분으로 인정하였지만, 일반적 인격권에 대한 결정에서 이미 인구조사판결의 기초를 논증적으로 제시하고 있었다.¹³⁾ 즉 ‘자기결정’(Selbstbestimmung)이란 개념을 연방헌법재판소는 이미 다른 판결에서 정보와 관련 없이 사용하였는데 중요한 판결을 살펴보면 다음과 같다.

- ① 1969년 7월 16일의 마이크로센서스(Mikrozensus) 결정에서 연방헌법재판소는 개인에 대한 통계목적의 설문조사의 한계를 설정하였는데, 사생활의 불가침 영역(unantastbaren Bereich privater Lebensgestaltung)에 해당하는 사항은 통계조사의 대상이 될 수 없다고 하였다.¹⁴⁾ 이 결정에 의하여 사생활의 내부영역에 대한 개인의 자기결정권이 인정되었다.
- ② 이혼절차상의 서류를 당사자의 동의 없이 징계절차를 위하여 전달하는 것이 허용되는지가 문제된 이혼서류(Scheidungsakten) 결정에서 연방헌법재판소는 개인정

11) Steinmüller, Grundfragen des Datenschutzes, BT-Drucks. VI/3826, 88.

12) Schwan, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, VerwArch 1975, S. 120 ff.; Mallmann, Datenschutz in Verwaltungs und Informationssystemen, 1976, S. 47 ff.

13) BVerfGE 54, 148 (155); 65, 37 (41 ff.); 63, 131 (142 f.).

14) BVerfGE 27, 1 (6).

보의 목적 외 사용은 원칙적으로 기본권의 침해를 가져온다는 점을 명백히 하였다.¹⁵⁾

- ③ 다른 사람의 생활모습을 공개적으로 나타내는 것이 허용되는지 여부와 범위가 문제된 레바흐(Lebach) 결정에서 연방헌법재판소는 개인의 생활모습이 전체적으로 또는 특정부분이 공개적으로 표현되는 것이 허용되는지 여부와 그 범위에 대하여 모든 사람은 원칙적으로 스스로 결정해야 한다고 하여 자기결정권을 구체화하였다.¹⁶⁾
- ④ 에플러(Eppler) 결정에서는 자기가 하지도 않은 말을 했다고 주장하는 것으로부터 개인을 보호하는 것은 일반적 인격권에 포함된다고 하면서, 이것은 일반적 인격권의 기초가 되는 자기결정권으로부터 나온다고 하였다.¹⁷⁾

3. 인구조사판결의 의의

연방헌법재판소는 이른바 ‘정보의 자기결정권’을 일반적 인격권의 구체화로 인정함으로써 정보의 자기결정권과 정보보호에 헌법적 가치를 부여하였다. 그러나 위에서 살펴본 바와 같이 정보의 자기결정권은 인구조사판결에 의하여 새로이 형성된 개념은 아니다. 다만 이 판결에서 처음으로 현대적 정보처리의 위험성을 지적하고 정보보호에 관한 전문적인 용어를 사용하면서 정보의 자기결정권을 자세히 근거 지웠으며 그의 효력에 대하여 구체적으로 살펴보았다는 데 의의가 있다.

이 판결의 중요한 판시사항은 그 후 연방헌법재판소에 의하여 재차 확인되어,¹⁸⁾ 이제 는 확고한 연방헌법재판소의 입장이 되었다. 인구조사판결은 정보의 자기결정권의 내용과 제한가능성에 대한 일반적인 사항 및 정보수집에 관한 법률이 지켜야 할 조건들에 대한 내용을 포함하고 있다. 개인정보의 무제한적인 수집, 저장, 사용 및 전달로부터 개인의 사적 영역을 보호하기 위한 기본원칙을 제시하였다.

인구조사판결은 직접적으로 경찰에 관련된 것은 아니지만, 그 판결은 경찰직무수행의

15) BVerfGE 27, 344 (350 f.).

16) BVerfGE 35, 202 (220).

17) BVerfGE 54, 148 (153 ff.).

18) BVerfGE 69, 315 ff.; 78, 77 ff.; 67, 100 (144).

핵심영역에 영향을 미치는 내용을 포함하고 있다. 인구조사판결은 통계목적의 정보수집과 정보처리의 영역을 넘어서 모든 공행정 영역에서 고려해야 할 원칙들을 내포하고 있다.¹⁹⁾ 특히 인구조사판결은 공공의 안녕과 질서유지와 관련하여, 즉 경찰영역에서 중요한 의미를 갖는 원칙들을 포함하고 있다.²⁰⁾

II. 정보의 자기결정권의 헌법적 근거

1. 일반적 인격권과 사생활의 비밀과 자유

독일의 경우 연방차원에서 정보보호권 내지 정보의 자기결정권을 명문으로 인정한 기본권 조항은 없다.²¹⁾ 독일의 연방헌법재판소는 정보의 자기결정권의 근거를 기본법 제1조 1항과 결합하여 기본법 제2조 1항의 일반적 인격권에서 찾고 있다. 즉 일반적 인격권은 개인에게 원칙적으로 자신에 관한 정보의 공개 및 사용에 대하여 스스로 결정할 권한이 있음을 보장한다고 한다.

우리나라의 경우 일반적 인격권은 헌법 제10조의 행복추구권에 포함되는 것으로 볼 수 있으며, 이로부터 정보의 자기결정권을 도출할 수 있을 것이다. 그러나 우리의 경우 독일과 달리 사생활의 비밀과 자유, 다시 말하면 프라이버시권을 헌법에 명시적으로 규정하고 있으며(제17조),²²⁾ 이 권리가 소극적으로 사생활비밀의 불가침, 사생활자유

19) Hufen, JZ 1984, 1072 (1075).

20) Kowalczyk, Datenschutz im Polizeirecht, 1989. S. 1.

21) 그러나 몇몇 주의 헌법에서는 정보보호권에 대한 규정을 두고 있다. 예를 들면 베를린 헌법 제21b조, 브란덴부르크 헌법 제11조, 니더작센 헌법 제64a조, 노르트라인-베스트팔렌 헌법 제4조 2항, 자르란트 헌법 제2조 2항·3항, 작센 헌법 제33조, 튀링엔 헌법 제6조 등. 특히 노르트라인-베스트팔렌은 연방헌법재판소가 인구조사판결을 하기 5년 전인 1978년 12월 19일의 헌법개정에 의하여 주의 헌법으로는 처음으로 정보보호에 관한 기본권을 명문으로 규정하였다. 즉 제4조 2항에서 “모든 사람은 자기관련 정보의 보호에 대한 권리를 갖는다. 이에 대한 침해는 법률에 근거한 중대한 공공의 이익이 존재하는 경우에만 허용된다”고 규정하였는데, 이 조항은 그 후 다른 주 헌법규정의 모델이 되었다.

가침을 내용으로 할 뿐만 아니라 적극적으로 자기정보통제권을 보장하는 것으로 이해할 때,²³⁾ 개인의 정보적 자기결정권의 직접적 근거는 우선적으로 헌법 제17조에서 찾아야 할 것이다. 사생활의 비밀과 자유로부터 개인정보의 보호에 대한 직접적인 근거를 찾을 수 있는 한 개인의 정보적 자기결정권의 직접적 근거로서 일반적 인격권을 언급할 필요는 없을 것이다.²⁴⁾

대법원은 군 정보기관이 법령에 규정된 직무범위를 벗어나 민간인에 대한 정보를 비밀리에 수집·관리한 것이 문제된 사건에서 헌법 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.”고 규정하고, 헌법 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.”라고 규정하고 있는바, 이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다고 판시하여, 자기정보통제권 또는 정보의 자기결정권을 헌법적 권리로 인정하면서 그의 근거를 헌법 제10조 및 제17조에서 찾고 있다.²⁵⁾

그러나 위에서 언급한 바와 같이 헌법 제10조의 행복추구권의 내용으로서 일반적 인격권을 들 수 있고, 이로부터 정보의 자기결정권을 도출하는 것이 가능하다고 할지라도, 행복추구권은 포괄적인 기본권으로서 개별 기본권의 보호영역에 의하여 포섭되지 않는 경우에만 적용되는 것이다. 즉 사생활의 비밀과 자유로부터 정보의 자기결정권이 보장된다면 특별법우선의 원칙에 따라 개별 기본권이 적용되고 일반적 인격권, 즉 행복추구권은 적용되지 않는다고 보아야 할 것이다.²⁶⁾

22) 독일은 프라이버시의 권리를 헌법에 명시적으로 규정하고 있지 않지만, 인간의 존엄성과 연결하여 인격의 자유로운 발현권(기본법 제2조 1항)을 주된 근거로 들고 있다. 그밖에 주거의 자유(기본법 제13조), 통신의 자유(기본법 제10조), 종교·양심의 자유(기본법 제4조 1항과 3항), 혼인과 가족(기본법 제6조 1항) 등도 그 근거규정으로 보고 있다[이에 대하여는 제 회열, 헌법학(중), 2000, 343쪽 참조].

23) 홍성방, 헌법 II, 현암사, 2000, 102쪽.

24) 그러나 김철수 교수는 사생활의 비밀과 자유권을 소극적 권리로 보고, 정보에 대한 자기결정권은 헌법 제10조에서 보장된다고 한다[김철수, 헌법학개론, 1999, 523-524쪽].

25) 대판 1998. 7. 24, 96다42789.

그밖에 경찰상의 정보수집은 다양한 방법과 수단에 의하여 행해지므로 사생활의 비밀과 자유 이외에 다른 기본권이 관련될 수 있다. 부분적으로 정보의 자기결정권과 관련될 수 있는 헌법적 조항으로는 주거의 자유를 규정한 제16조(주거 안에서의 사생활 영역을 보호), 통신의 비밀을 보호하는 제18조, 양심의 자유를 보호하는 제19조, 종교의 자유를 규정한 제20조, 표현의 자유, 집회·결사의 자유를 규정한 제21조 등을 들 수 있다.

2. 주거의 자유

주거의 자유에 대한 불가침은 인간의 존엄과 가치 및 행복추구권을 보장하는 헌법 제10조와 밀접한 관련이 있다. 모든 사람은 자신의 주거공간에서 아무런 방해도 받지 않고 평온하게 지낼 수 있는 권리가 있다. 주거의 개념은 넓게 해석하여 모든 공간적인 사적 영역을 의미하는 것으로 이해해야 한다. 가택은 국가의 침해로부터 보호되는 가장 전형적인 주거공간에 해당한다. 그밖에 사무소, 공장, 학교, 호텔방, 창고 및 잠시 사람이 머무를 수 있는 자유스러운 공간은 모두 주거의 개념에 포함된다.²⁶⁾

주거의 자유에 대한 압수·수색 및 그 밖의 침해는 특별한 법적 요건을 충족한 경우에만 허용된다. 주거에 대한 압수·수색은 검사의 신청에 의하여 법관이 발부한 영장을 제시하며 공개적으로 행해져야 한다.

주거의 자유는 법적 근거 없이 감청하거나 사진촬영에 의하여 주거로부터 정보를 수집하는 것을 금지한다. 주거의 자유는 주거에 출입하는 것에 의해서 뿐만 아니라 특별한 기계시설에 의하여 주거 안을 감시하거나 관찰하는 것에 의하여도 침해될 수 있다. 주거 안 또는 주거 밖에서 은밀한 수단에 의하여 정보를 수집하는 것은 주거의 자유에 대한 중대한 침해에 해당한다. 독일 각주의 경찰법에서 주거에의 출입·수색 및 주거에서의 정보수집에 대하여 규율하고 있는 것은 바로 이러한 이유 때문이다.

26) 홍성방, 헌법 II, 현암사, 2000, 41-42쪽 참조.

27) 이에 대하여는 Vahle, Datenschutz und Datensicherheit, 1995, 388(391 f.) 참조.

3. 통신의 자유

헌법 제18조는 편지를 쓰거나 전화를 걸며 E 메일 등 통신매체를 이용하는 경우 국가로부터 방해받지 않고 자신을 표현할 수 있도록 보호해 준다. 즉 제18조는 제17조의 사생활의 비밀과 자유 및 제21조의 표현의 자유를 보충하여, 보호되는 사적 영역을 공간적으로 확장하며 개인의 인격의 자유로운 발현에 기여한다.

우편물의 검열이나 전기통신의 감청 등은 기본권에 대한 침해로서 형식적 법률의 근거가 있는 경우에만 허용된다.²⁸⁾ 경찰법상의 개괄적 수권조항은 원칙적으로 충분한 법적 근거가 될 수 없고 개별적인 법적 근거가 필요하다. 통신비밀보호법 제5조·제6조·제7조·제8조 및 제14조 등은 우편물검열, 전기통신감청, 대화를 녹음·청취할 수 있는 요건과 절차에 대하여 규정하고 있다. 그에 의하면 제5조에서 정하는 범죄²⁹⁾를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있

28) 통신비밀보호법 제3조 참조.

29) 통신비밀보호법 제5조에서 정하는 범죄는 다음과 같다:

1. 형법 제2편 중 제1장 내란의 죄, 제2장 외환의 죄, 제4장 국교에 관한 죄, 제5장 공안을 해하는 죄, 제6장 폭발물에 관한 죄, 제7장 공무원의 직무에 관한 죄, 제9장 도주와 범인 은닉의 죄, 제13장 방화와 실화의 죄 중 제164조 내지 제167조·제172조 내지 제175조의 죄, 제14장 일수와 수리에 관한 죄 중 제177조 내지 제180조·제182조·제183조의 죄, 제15장 교통방해의 죄 중 제185조 내지 제188조·제190조의 죄, 제16장 음용수에 관한 죄, 제17장 아편에 관한 죄, 제18장 통화에 관한 죄, 제19장 유가증권, 우표와 인지에 관한 죄, 제24장 살인의 죄, 제29장 체포와 감금의 죄, 제30장 협박의 죄, 제31장 약취와 유인의 죄, 제32장 강간과 추행의 죄, 제37장 권리행사를 방해하는 죄, 제38장 절도와 강도의 죄, 제39장 사기와 공갈의 죄 중 제350조의 죄
2. 군형법 제2편 중 제1장 반란의 죄, 제2장 이적의 죄, 제3장 지휘권 남용의 죄, 제4장 지휘관의 항복과 도피의 죄, 제5장 수소이탈의 죄, 제7장 군무태만의 죄 중 제42조의 죄, 제8장 항명의 죄, 제9장 폭행·협박·상해와 살인의 죄, 제11장 군용물에 관한 죄, 제12장 위령의 죄 중 제78조·제80조·제81조의 죄
3. 국가보안법에 규정된 범죄
4. 군사기밀보호법에 규정된 범죄
5. 군사시설보호법에 규정된 범죄
6. 마약법에 규정된 범죄
7. 향정신성의약품관리법에 규정된 범죄
8. 대마관리법에 규정된 범죄

고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 우편물검열, 전기통신감청, 대화의 녹음·청취를 허가할 수 있는데, 이 경우에 필요한 조치의 종류·그 목적·대상·범위·기간 및 허가요건 충족 사유 등의 청구이유를 기재하여 검사는 법원에 대하여 허가를 청구하고, 사법경찰관은 검사에 대하여 허가를 신청하고 검사가 법원에 대하여 그 허가를 청구하여야 한다. 또한 대통령령이 정하는 정보수사기관의 장은 국가안전보장에 대한 위해를 방지하기 위하여 이에 관한 정보수집이 필요한 경우에는 우편물검열, 전기통신감청, 대화의 녹음·청취를 할 수 있도록 규정하고 있다(제7조). 통신비밀보호법은 이러한 통신제한조치 등으로 취득한 내용을 사용할 수 있는 경우를 제한적으로 열거하고 있으며(제12조),³⁰⁾ 그 이외의 경우에는 이를 다른 기관 또는 외부에 공개하거나 누설할 수 없도록 하고 있다(제11조).

4. 양심의 자유

헌법 제19조는 특정한 활동을 보호하는 것이 아니라 개인의 생각, 신념, 확신 등 국가가 간섭할 수 없는 개인의 내부적 영역을 보호하는 것이다. 개인의 내부적 사고의 형성, 확신 등에 대하여 국가는 어떠한 영향도 미칠 수 없다. 양심의 자유는 자신의 사고 내지 신념을 적극적으로 나타낼 자유를 포함할 뿐만 아니라,³¹⁾ 소극적으로 자신의 신념과 확신에 대하여 침묵할 권리도 포함한다. 따라서 특정 종교에의 소속에 대한 질문은 그것

9. 특정범죄가중처벌등에관한법률에 규정된 범죄

10. 특정경제범죄가중처벌등에관한법률에 규정된 범죄

11. 제1호와 제2호의 죄에 대한 가중처벌을 규정하는 법률에 위반하는 범죄.

30) 통신제한조치 등으로 취득한 자료 또는 그 내용은 다음 각호의 경우 외에는 사용할 수 없다:

1. 통신제한조치의 목적이 된 제5조 제1항의 규정된 범죄나 이와 관련되는 범죄를 수사·소추하거나 그 범죄를 예방하기 위하여 사용하는 경우
2. 제1호의 범죄로 인한 징계절차에 사용하는 경우
3. 통신의 당사자가 제기하는 손해배상소송에서 사용하는 경우
4. 기타 다른 법률의 규정에 의하여 사용하는 경우.

31) 양심의 자유에 양심표현의 자유가 포함되는지 여부에 대한 논의에 대하여는 홍성방, 헌법Ⅱ, 현암사, 2000, 116쪽 참조.

이 법률에 규정된 통계 목적의 정보수집을 위하여 필요한 경우에 한하여 허용된다고 보아야 할 것이다.

5. 언론·출판의 자유

헌법 제21조의 언론·출판의 자유 또는 표현의 자유는 사상 또는 의견의 자유로운 표명의 자유와 전달의 자유뿐만 아니라 정보의 자유도 보장한다.³²⁾ 여기서 정보의 자유란 단순한 정보의 수집뿐만 아니라 적극적으로 정보를 창출하고 선택하는 것도 포함한다. 정보의 자유에 의해 국가는 정보원에의 접근을 어렵게 하거나 불가능하게 하여서는 안 된다. 그러나 정보의 자유는 본질적으로 침해배제청구권이므로,³³⁾ 그에 의해 국가 또는 공공기관에게 일반적으로 접근 가능한 정보원으로 만들어 달라고 요구할 수는 없다. 물론

32) 헌법재판소도 정보에의 접근·수집·처리의 자유는 표현의 자유에 당연히 포함된다고 한다(헌재 1989. 9. 4, 88헌마22; 헌재 1991. 5. 13, 90헌마133; 헌재 1992. 2. 25, 89헌가104).

33) 우리나라에서의 학계의 다수견해[계희열, 헌법학(중), 박영사, 2000, 385-386쪽; 홍성방, 헌법Ⅱ, 현암사, 2000, 128쪽; 허영, 한국헌법론, 박영사, 1997, 517쪽]과 헌법재판소[헌재 1991. 5. 13, 90헌마133; 헌재 1994. 8. 31, 93헌마174]의 입장은 알권리 또는 정보의 자유를 정보의 수집 내지 취재활동에 대한 침해배제권과 정보공개청구권을 구체적 내용으로 하는 권리로 보면서, 그의 법적 근거를 헌법 제21조에서 찾고 있다. 그러나 개인적으로 포괄적인 내용을 가진 정보공개청구권의 근거를 헌법 제21조의 언론·출판의 자유에서 찾는 것은 지나친 확장해석이라고 생각한다. 헌법 제21조의 언론·출판의 자유는 의사표명의 자유, 전달의 자유, 정보의 자유 및 언론매체에 대한 자유를 내용으로 하는데, 여기서 정보의 자유란 정부가 보유하고 있는 정보에 대한 국민의 알권리, 즉 국민의 정보에 대한 일반적 정보공개를 구할 권리[헌재 1989. 9. 4, 88헌마22 참조]라는 의미로 파악해서는 안 되고, 단지 일반적으로 접근 가능한 정보원으로부터 의사형성에 필요한 정보를 자유롭게 수집하고 수집된 정보를 선택할 수 있는 권리로 이해해야 한다. 공공기관이 보유하고 있는 정보는 공개적으로 접근할 수 있는 문서 또는 목록에 편입되어 있지 않는 한, 여기서 말하는 접근 가능한 정보원에 해당하지 않는다. 따라서 공공기관이 보유하고 있는 정보에 대한 열람 내지 공개청구는 헌법 제21조를 근거로 할 것이 아니라, 개인의 사적 영역에 관한 정보가 문제되는 한 헌법 제17조에 의하여 보장되는 정보의 자기결정권을 근거로 하여야 하며, 그 이외의 정보의 경우에는 헌법 제10조와 헌법 제37조 1항의 결합에 의한 일반적 인격권에 의하여 보장되는 것으로 보아야 할 것이다. 다만 후자의 경우 일반적 인격권에 근거하여 모든 경우에 공공기관에게 정보 공개를 청구할 수 있는 것은 아니며, 공개의 기관, 대상, 범위, 절차 등에 있어서 광범위한 입법재량이 인정된다고 보아야 할 것이다.

그렇다 하더라도 일반인이 접근 가능한 정보원에 해당하는지 여부가 국가의 자의적인 판단에 맡겨져서는 안 된다. 정보의 자유에 의해 개인은 일반적으로 접근 가능한 정보원으로부터 정보를 얻을 수 있는 권리가 보장된다. 따라서 정보의 제공을 방해하거나 금지함으로써 개인의 정보의 자유를 제한하는 조치는 기본권에 대한 침해가 될 수 있는 것이다.

6. 집회·결사의 자유

헌법 제21조의 표현의 자유와 밀접한 관련이 있는 집회의 자유는 집단적인 의견의 표명을 보호한다. 집회의 자유는 국가의 침해로부터 집회의 개최를 보호할 뿐만 아니라 국가에게 집회의 진행이 가능하도록 배려할 의무를 부여한다.

시위란 공개적인 의견표명을 의미하는 데, 이로부터 또는 시위의 참가자로부터 정보를 수집하는 것은 통상적으로 별 어려움이 없이 행해진다. 시위를 신고함에 있어서 이미 주최자, 연락책임자, 질서유지인, 연사 및 참가예정단체 등에 대한 정보가 알려진다. 신고서의 접수관청은 통상적으로 관할 경찰서장이 된다.

결사의 자유는 오랜 역사를 가진 기본권으로서 자유로이 선택된 특정한 목적을 가진 지속적이고 조직화된 결합체를 공권력의 침해로부터 보호한다.³⁴⁾ 결사의 자유는 자유로운 사회적 집단의 형성을 보호하고 개인의 자유의 실현에 기여한다. 표현의 자유와 함께 집회·결사의 자유는 의사소통의 기회를 보장하는 기본권으로서 민주주의의 실현을 위하여 없어서는 안될 기본권에 해당한다.

표현의 자유와 집회의 자유는 과도한 관찰 및 기록화로부터 개인을 보호한다.³⁵⁾ 어떠한 집회 또는 시위에 참가하는 것이 행정기관에 의하여 기록되고 그에 의하여 위협한 상태에 놓일지도 모른다는 생각이 들면 사람들은 집회·시위의 자유를 포기하려 할 것이다. 따라서 경찰에 의한 정보수집 활동(예컨대 관찰, 감청, 비디오촬영 등)은 정보의 자기결정권에 대한 침해에 해당하는 것이다. 집회의 자유는 집회의 준비 및 개최에 있어서 방해받지 않을 자유와 집회에서의 자유로운 의사소통을 보장한다. 즉 집회의 자유는

34) Badura, Staatsrecht, 1986, S. 117 f. 참조.

35) BVerfGE 69, 315 (349); Knisel/Tegtmeyer/Vahle, Handbuch des Datenschutzes für Sicherheitsbehörden, 1986, Rdn. 702 참조.

집회 및 시위의 준비단계 및 진행 중에 국가기관에 의한 관찰, 사진촬영, 녹음 및 참가자의 리스트 작성 등으로부터 개인을 보호한다. 결국 집회에서 또는 집회와 관련하여 사진촬영 하거나 녹음을 하는 것은 정보의 자기결정권에 대한 침해인 동시에 집회의 자유에 대한 침해에 해당한다.

더 나아가 비디오촬영에 의한 모든 시위참가자의 파악은 집회의 자유의 본질적인 내용에 대한 침해에 해당하기 때문에 법률에 의하여도 허용될 수 없다. 집회의 자유에 대한 침해는 공동의 의사형성 또는 의사표현을 완전히 불가능하게 하는 정도가 아닌 단지 어렵게 하는 경우에만 허용될 수 있다. 그러한 침해를 정당화하기 위하여서는 명백한 권한규범이 필요한 것은 물론이다.

III. 정보의 자기결정권의 내용

독일 연방헌법재판소의 견해에 의하면 정보의 자기결정권은 “개인은 원칙적으로 자기 개인정보의 제공과 이용에 대하여 스스로 결정할 권한이 있다”는 것을 내용으로 한다.³⁶⁾ 자유로운 사회의 구성원으로서 개인은 자유롭게 자기 결정할 권리가 보장된다. 여기에는 개인이 다른 사람에게 어떻게 행동할 것인지에 대하여 결정할 자유가 포함된다. 이것은 다시 다른 사람이 자기를 어떻게 인식하고 있는지를 어느 정도 확실하게 파악할 수 있는 것을 전제로 한다. 대화 상대방의 인식을 제대로 파악할 수 없는 사람은 독자적인 자기결정을 계획하고 결정하며 그에 따라 행동할 자유를 침해받게 되기 때문이다.³⁷⁾ 누가, 무엇을, 언제, 왜 자기에 대하여 알고 있는지를 개인이 알 수 없는 사회는 정보의 자기결정권과 조화될 수 없다.³⁸⁾ 즉 언제, 어떠한 한계 내에서 개인의 신상에 관한 사항이 공개될 것인지에 대하여 스스로 결정할 수 있어야 한다. 따라서 제한 없는 개인정보의 수집·저장·이용·제공으로부터 개인을 보호하는 것은 현대적 정보처리의 조건에

36) BVerfGE 65, 1 (42).

37) BVerfGE 61, 1 (43).

38) BVerfGE 65, 1 (43).

포함되는 것이다.³⁹⁾

현대적 정보처리는 더 이상 이전처럼 수작업으로 이루어진 카드나 서류에 의하여 행해지지 않고 개인정보가 컴퓨터에 의하여 저장되며 거리에 상관없이 신속하게 불러낼 수 있게 되었다. 따라서 오늘날에는 자동화된 정보처리로부터 개인을 보호하는 것이 특히 문제된다. 이러한 상황 하에서는 개인정보를 일반이 열람하고 영향을 미칠 위험이 증가하게 되는데, 이것은 자기의 정보가 공중에 개방되어 있다는 심리적 압박에 의하여 그의 행동에 영향을 미칠 수 있게 된다. 따라서 자신에 관한 개인정보의 이용과 제공에 대하여 스스로 결정할 개인의 권리는 자동화된 정보처리에 있어서 특별한 보호를 필요로 하게 된다.

IV. 정보의 자기결정권의 한계

정보의 자기결정권은 아무런 제한 없이 보장되는 것은 아니다. 자기 자신의 정보에 대한 절대적이고 무제한적인 지배권은 개인의 공동체 관련성과 구속성 때문에 인정될 수 없다. 개인은 독립적 존재로서가 아니라 사회의 구성원으로 존재하는 것이다. 헌법은 공동체에 관련되고 그에 구속된 개인을 전제로 한다(개인의 공동체 관련성과 구속성). 헌법은 폐쇄된 개인이 아니라 공동체에서 성장하고 다른 사람과 어울리는 인격체를 대상으로 한다. 즉 개인은 사회적 공동체의 구성원으로서 서로 의사소통하며 발전하는 인격체이다. 따라서 개인은 자신의 정보에 대하여 절대적이고 무제한적인 지배권을 가질 수는 없으며, 중대한 공공의 이익을 위하여 정보의 자기결정권에 대한 제한을 받아 들여야 한다.⁴⁰⁾

이러한 내용은 인구조사판결의 핵심적 내용으로 당연한 것으로 인식되고 있는데, 중요한 것은 정보의 자기결정권을 제한할 수 있는 조건과 그의 법적 근거이다. 정보의 자기

39) BVerfGE 65, 1 (42 f.).

40) BVerfGE 65, 1 (42 f.).

결정권에 대한 제한은 헌법에 적합하며 규범명확성의 원칙에 부합하는 법률의 근거가 있어야 한다.⁴¹⁾ 이 경우에 법률에 근거가 있어야 한다는 점과 그 법률은 헌법에 적합하여야 한다는 점, 특히 비례의 원칙에 위반되어서는 안되기 때문에 중대한 공익을 위하여 필요한 한도를 넘어서 제한되어서는 안 된다는 것 등은 그리 문제되지 않는다. 또한 명확성의 원칙에 따라 법률규정은 명확하여야 한다. 법규명령에 위임함에 있어서는 그 범위를 명확히 하여야 하며, 시민에게 의무를 부과함에 있어서는 법률로부터 그 의무가 도출될 수 있어야 한다. 규범명확성의 원칙은 관련자가 자기에 관한 정보가 어떤 구체적인 목적을 위하여 필요한지를 명확하게 인식할 수 있어야 한다는 것을 뜻한다. 따라서 개인 정보를 이용하는 목적이 구체적이고 정확하게 법률상 규정될 것을 요구한다. 즉 정보의 자기결정권에 대한 제한의 조건과 범위가 명확하여야 한다.

V. 강제적인 정보수집의 조건

국가가 시민에게 개인정보의 제출을 요구하는 경우처럼, 정보의 수집이 강제적으로 행해지는 경우에는 특별한 요건을 갖추어야 한다. 여기서 '강제'의 개념은 정보보호법 분야에서 특별한 의미로 사용되는 것으로, 전통적인 경찰법상의 침해권한에 있어서의 직접적 강제를 의미하는 것은 아니다. 정보보호법 영역에서는 개인정보가 관련자로부터 자발적으로 제출되지 않는 한 모두 강제적으로 수집되는 것이라 할 수 있다. 예컨대 설문조사에 응하지 않는 것에 대하여 과태료가 부과된다면 강제적인 정보수집에 해당한다고 볼 수 있다.

개인정보의 제출을 강제하기 위하여서는 법률에 사용목적이 분야별로 구체적으로 규정되어 있을 것이 전제되어야 한다.⁴²⁾ 또한 정보가 이러한 목적에 적합하고 필요하여야 한다. 다시 말하면 정보처리는 목적을 달성하기 위하여 필요한 최소한으로 제한되어야

41) Riegel, Datenschutz bei den Sicherheitsbehörden, 2. Aufl., 1992, S. 8.

42) BVerfGE 65. 1 (46).

한다. 중대한 공익은 통상적으로 사회적 관련성 있는 정보에만 존재하게 된다. 기대할 수 없는 내적인 사항과 자기부죄 자료를 요구해서는 안 된다. 사용목적에 대한 분야별로 자세한 규율을 요구하는데, 이에 의하여 익명이 아닌, 즉 특정인에게 관련되거나 또는 관련 지을 수 있는 정보를 불확정적이거나 또는 아직 확정되지 않은 목적에 사용하기 위하여 미리 수집하는 것은 배제된다. 정보는 개별적인 법적 근거에서 특정된 목적을 위해서만 사용되어야 한다(목적 구속성의 원칙). 자동화된 정보처리의 위험과 관련하여 특히 다른 기관에의 제공 및 사용을 금지함으로써 목적 외 사용에 대한 보호장치가 마련되어야 한다.

VI. 인구조사판결의 경찰영역에의 적용

독일 연방헌법재판소의 인구조사판결의 대상은 1983년의 인구조사법이다. 경찰영역에서의 정보처리는 이 판결의 직접적인 대상은 아니다. 그러나 판결이유에서 정보처리에 대한 일반적인 내용을 담고 있는 한, 그 한도 내에서 경찰의 정보처리에도 간접적으로 관련이 된다고 볼 수 있다. 이러한 점에서 인구조사판결이 담고 있는 정보처리에 대한 요구가 경찰영역에도 적용될 수 있는지가 밝혀져야 한다.

연방 헌법재판소법 제31조 1항에 의하면 연방 헌법재판소의 결정은 연방 및 주의 헌법기관, 모든 법원 및 행정청을 기속한다. 결정의 주문과 주된 이유⁴³⁾는 기속력을 발휘한다. 인구조사판결에서는 다음과 같은 문구가 빈번히 사용되는 것을 발견할 수 있는데, 그에 대하여는 아무런 의문이 제기될 수 없을 정도로 당연한 것이라 할 수 있다: “개인은 자기에 대하여 누가 무엇을 언제 어떠한 이유로 알고 있는지를 알고 있어야 한다. 자기의 일탈된 행위가 언제나 기록되고 저장되며 사용되거나 다른 기관 등에 제공될지 모른다는 것에 대하여 불안해하는 사람은 순응된 행위를 하려고 노력할 것이다. 그것은

43) 주된 이유란 그것을 간과하였을 때 결정의 의미가 상실될 정도의 가치를 지니는 이유를 말한다.

개인의 권리를 축소시킬 뿐 아니라 구성원의 행위가능성과 협력가능성에 의존하고 있는 자유민주적 기본질서에 대한 위협을 의미한다.”⁴⁴⁾ 이러한 내용은 특히 경찰행정청과 관련하여 의미가 있다. 경찰행정청에 의한 정보처리는 인격의 자유로운 발현과 능동적인 기본권실현을 위축시키는 효과를 가져올 수 있기 때문에 경찰행정청은 정보의 자기결정권을 특히 준수해야 한다. 이른바 Brokdorf-결정에서 연방헌법재판소는, 인구조사판결을 참조하면서 그에 보충적으로 ‘과도한 관찰과 기록’은 집회의 자유에 위반된다는 것을 분명히 하였다. 예컨대 집회 또는 시민의 모임에 참가한 사실이 공적으로 기록되며, 따라서 그로 인하여 어떠한 위협이 발생할 수 있다는 것을 우려하는 자는 집회·결사의 자유의 행사를 포기하게 될 것이다.⁴⁵⁾ 따라서 정보의 자기결정권은 아무런 제한 없이 경찰영역에 적용된다고 보아야 한다.⁴⁶⁾

경찰의 정보수집은 강제적으로, 다시 말하면 관계자의 의사에 반하여 또는 관계자 모르게 행해지는 경우가 많다. 이것은 예컨대 정보의 획득을 목적으로 - 긴급한 경우에는 관계자의 의사에 반하여 - 행해지는 주거수색, 압수, 검문 또는 수색 등과 같이 형사소송법의 전통적인 침해권한을 행사하는 경우에 명백해 진다. 강제적인 정보수집에 관한 특별요건은 정보가 비밀리에 수집되는 경우, 예컨대 관찰, 경찰의 감시, 컴퓨터에 의한 범죄혐의자의 검색·조사에 의하여 또는 신분위장자의 배치에 의하여 관계자 모르게 수집되는 경우에도 준수되어야 한다. 이러한 경우에 관계자는 자기의 정보결정권의 행사를 방해받게 되는 것이다. 은밀한 정보수집은 단지 인구조사판결에서의 ‘강제적인’ 정보수집을 의미하는 것이 아니라, 그것보다 더 문제가 되는 것이다. 왜냐하면 비밀리에 이루어지는 정보수집은 누가 어떠한 이유로 자기에 대한 정보를 수집하는지를 알 수 있어야 한다는 관계자의 권리에 정면으로 배치되는 것이기 때문이다.⁴⁷⁾ 따라서 인구조사판결은 완전한 범위에서 경찰의 정보처리에 적용되며, 강제적인 정보수집의 경우에는 더욱 엄격한 요건을 요구한다.

44) BVerfGE 65, 1 (43).

45) BVerfGE 69, 315 ff. 이에 대하여는 Bäumlner, JZ 1986, 469 ff. 참조.

46) Knemeyer, NVwZ 1988, 193 (196).

47) Rogall, JZ 1987, 847 (851). 그러나 다른 생각으로는 Rebmann, NJW 1985, 1 (4).

VII. 인구조사판결의 경찰 정보처리에 대한 귀결

인구조사판결로부터 정보의 자기결정권을 준수해야 하는 입법자 및 경찰행정청에게 다음과 같은 결론을 도출할 수 있다. 정보의 자기결정권에 대한 제한은 중대한 공익이 존재하는 경우에만 허용되고, 정보처리가 목적달성을 위하여 적합하고 필요한 경우이어야 한다. 개인은 자기에 관한 정보의 공개에 대하여 결정할 권한을 가지고 있는 반면에, 공동체의 구성원으로서 자기의 정보에 대한 절대적이고 무제한적인 지배권을 가지는 것은 아니다. 양자의 조정, 즉 기본권 보장과 질서유지 사이의 조정은 입법자에 의하여 행해져야 한다. 정보처리의 투명성은 정보의 자기결정권의 본질적 구성요소이므로, 정보의 자기결정권에 대한 제한은 법률에서 명확히 규정하여 개인은 자기의 정보결정권에 대한 제한을 예측할 수 있어야 한다.

입법자는 정보처리를 위하여 필요한 조치를 개별 영역별로 명확하게 규율해야 한다. 경찰영역에 있어서는 경찰의 직무수행, 즉 위협방지, 범죄예방, 범죄수사에 있어서의 정보처리를 위하여 그에 대한 개별적인 수권이 필요하다.⁴⁸⁾ 필요성의 원칙을 엄격히 적용할 때, 예방과 진압의 경우를 비교해 보면 명확해 지듯이 직무영역별로 상이한 정보처리의 수권을 요구하게 된다.

때때로 직무영역 사이의 구별의 어려움이 지적되지만, 그것은 크게 문제되지 않는다. 예방은 공공의 안녕·질서에 대한 장애를 방지하는 것이며, 범죄수사는 이미 행해진 범죄행위의 진상을 규명하고 그에 대하여 벌을 과하는 것을 목적으로 한다. 위협방지에 있어서 경찰은 경찰법을 근거로 하여 자율적으로 활동하는 데 대하여, 범죄수사에 있어서는 형사소송법을 근거로 하고 검사의 지휘를 받는다. 예방을 독자적인 제3의 직무영역으로 따로 구분하여 취급할 것인지에 대하여는 논란이 있지만,⁴⁹⁾ 여하튼 예방이라는 직무수행을 위하여서는 그것이 위협방지 또는 범죄수사에 관련된 것인지, 아니면 독자적인 영역에 관한 것인지를 불문하고 그를 위해 필요한 정보처

48) 다른 생각으로는 Götz, NVwZ 1987, 858 ff.

49) 이에 대하여는 Bäumlér, in: Liskén/Denninger, Handbuch des Polizeirechts, 2. Aufl., 1996 J. Rdn. 524 ff.

리에 관한 자세한 규율이 있어야 한다.

예컨대 이미 행해진 범죄행위 이후에 계속되는 다른 범죄행위를 저지하거나 또는 추가적인 손해의 발생을 방지하여야 하는 경우, 위협방지와 범죄수사의 관점에서 동일한 사실관계가 경찰로부터 병렬적으로 처리될 수 있다. 그러나 개별적인 경찰조치는 구체적인 경우에 양 업무영역 중 어느 하나에 귀속되어야 하며 법적으로 명확하게 확정되어야 한다. 정보수집에서부터 삭제에 이르기까지 정보처리를 위한 조치를 위하여 양자는 명확히 구별되어야 한다.

특정한 목적을 위하여 수집한 정보를 다른 목적으로 사용할 수 있는 요건이 무엇인지 또한 밝혀져야 할 문제이다. 이에 대하여는 입법자가 명확히 규율해야 한다. 관련된 정보의 종류와 정보획득을 위하여 사용된 방법상의 차이를 고려하지 않고 일괄하여 동일하게 취급하는 것은 잘못이다.

규범명확성의 원칙에 따라 침해의 수권규범은 가능한 한 자세하게 규정되어야 한다. 일반조항의 사용이 완전히 배제되는 것은 아니지만, 그렇다고 입법자의 자의에 맡겨져 있는 것은 아니다. 입법자는 가능한 한 자세하게 규율하려고 노력하여야 한다. 이것이 사실상 불가능한 경우에 한하여 일반조항의 사용이 허용된다. 물론 너무 자세하게 규정하는 것이 오히려 규범명확성의 목적에 반하는 경우가 있을 수 있음을 주의해야 한다.

불특정한 목적 또는 아직 확정할 수 없는 목적을 위하여 익명으로 되어 있지 않은 정보를 미리 수집하는 것은 금지된다. 정보의 저장은 그 개념상 장래의 사용을 위하여 미리 준비해 놓는다는 의미가 내포되어 있으므로, 미리 정보를 수집하는 것 자체가 금지되는 것은 아니다. 사용목적이 명백히 확정되어 있지 않다는 점이 문제가 되는 것이다.

입법에 의하여 사용목적이 구체적으로 특정되고 정보의 사용이 그에 한정된다면, 장래의 목적을 위한 정보의 저장도 허용될 수 있다. 이것은 결국 규범명확성의 요구를 강조하는 것과 다르지 않다.

입법자는 특히 은밀한 정보의 수집을 허용할 것인지, 허용하는 경우 그 범위에 대하여 신중하게 판단하여야 한다. 은밀한 정보수집은 정보의 자기결정권에 정면으로 배치되는 것이므로, 공개된 정보수집에 의하여서는 중대한 공적 업무의 수행이 불가능하거나 거의 가능성이 없는 경우에 한하여 고려될 수 있는 것이다. 단순히 편리하다거나 관행이라든가 또는 합리성이라는 측면은 중대한 공익을 근거 지우는 데 충분하지 않다. 또한

적법하게 은밀한 조사가 행해진 경우에도, 예를 들면 사후에 이를 관계자에게 알리는 등 최소한의 조정이 행해져야 한다.⁵⁰⁾

그밖에 입법자는 기대불가능한 내적 사항을 제공하도록 요구하거나 또는 자기의 죄를 스스로 인정할 것을 요구해서는 안 된다는 점을 유의해야 한다. 범죄수사에 있어서 스스로 죄를 인정할 것인지에 대하여는 관계자의 자유의사에 맡겨져 있다. 입법자는 자기의 죄를 스스로 인정하는 것과 마찬가지로의 정보수집 형식을 허용해서는 안 된다. 그러나 경찰이 범죄를 수사함에 있어서 관계자 스스로 남겨 놓은 단서를 수집하고 사안해결을 위하여 사용하는 것은 당연히 허용되는 것이기 때문에, 이에 관한 명확한 경계를 지우는 것은 쉽지 않다. 더 어려운 문제는 무엇이 '기대불가능한 내적 사항'(unzumutbare intime Angaben)에 해당하느냐를 밝히는 것이다. 기대불가능한 내적 사항에 관한 정보의 수집이 예외적으로 불가피한 경우에도, 입법자는 다른 목적으로 그 정보를 이용하는 것을 허용해서는 안 된다. 입법자는 그 정보를 포기할 수 없는 예외적인 경우에 극히 제한적으로만 그 사용을 허용해야 한다.

여러 가지 자료의 집적에 의하여 자동으로 처리되는 개인신상정보의 경우 특별한 주의가 필요하다. 이와 같은 업무처리의 경우에 있어서는 실수의 가능성이 높을 뿐 아니라, 정보의 왜곡, 축소, 도식화 및 목록화의 위험이 있는데, 이는 헌법상의 인간존엄의 원칙에 부합하지 않는 것이다. 따라서 입법자는 경찰에게 상이한 생활영역에서 나오는 정보를 자동장치에 의하여 결합하고 관련자의 신상에 대하여 포괄적으로 하나의 형상으로 나타내는 것을 허용해서는 안 된다.

입법자는 침해의 수권규정과 함께 설명의무(Aufklärungspflicht), 교시의무(Auskunftspflicht) 및 삭제의무(Löschungspflicht) 등 절차법적 보호조치를 마련해야 한다. 삭제의무와 관련하여 볼 때, 정보는 언젠가는 삭제되어야 한다는 것은 정보처리 그 자체를 위하여도 당연한 것이다. 수집된 정보를 활용하고 관리하는 것은 많은 비용과 노력을 필요로 하며, 설문조사와 탐구조사의 경우 중요하지 않은 정보도 많이 제공되기 때문에, 지나치게 광범위하게 정보를 수집하는 것은 비생산적이다. 인구조사판결에서는 입

50) 경찰조사의 공개성에 대하여는 Deutsch, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1991, S. 28 ff. 참조.

법자가 관계자의 이익을 위하여 준수해야 할 것으로 삭제의 의무를 특별한 보호장치의 하나로 언급하고 있는데, 이로부터 삭제의무는 정보를 저장하는 기관의 이익을 고려하는 것 이상의 의미를 가지는 것으로 이해해야 한다. 가능한 한 장기의 저장을 원하는 정보 저장기관의 이익과 부담적 정보의 경우 가능한 한 조속한 삭제를 원하는 관계자의 이익 사이에 조정이 문제된다. 입법자 스스로 얼마동안 정보가 저장되어야 하는지를 결정해야 한다. 그것은 일률적으로 결정될 문제가 아니고, 필요성의 원칙에 따라 혐의의 정도, 수집방법 및 저장된 정보의 내용에 따라 유형별로 삭제기간을 상이하게 정해야 한다. 정보를 수집함에 있어서 경찰이 관련자에게 법적 근거를 알려주도록 하는 것은 설명의무에 해당한다. 비밀에 의한 정보수집에 대하여 사후에 통지하는 것도 정보의 자기결정권에 대한 침해를 완화시킬 수 있는 방법이 될 것이다.

제3장 독일에 있어서 경찰의 정보관리에 관한 법적 규율

I. 통일경찰법모범초안에 대한 개정초안

1983년의 인구조사판결 이전에 독일 연방헌법재판소는 개인정보의 수집·처리를 침해적 활동이 아닌 것으로 보았었다. 그러나 현재 행정기관에 의한 개인정보의 처리에 의해 기본권에 의하여 보호된 법익이 침해될 수 있다는 것은 일반적으로 받아들이고 있다.⁵¹⁾ 즉 독일 연방헌법재판소의 인구조사판결에서 확인된 것처럼 개인정보에 대한 국가의 모든 수집·처리활동은 정보적 자기결정권에 대한 침해를 가져오며, 그에 대하여는 형식적 법률에 의한 특별한 법적 근거가 마련되어야 한다. 이와 같은 인구조사판결에서의 연방헌법재판소의 요구에 따라 독일에서는 개별적인 영역에서 정보보호에 관한 규정을 두고 있으며, 경찰관련 법률에서도 정보수집과 처리에 관하여 포괄적인 규율을 하고 있다. 주의 새로운 경찰법이나 입법을 위한 제안들은 대부분 통일경찰법모범초안의 개정을 위한 초안(VE ME PolG: 아래에서는 '통일경찰법모범초안에 대한 개정초안')에 따르고 있으므로, 독일에서의 경찰의 정보관리에 대한 분석 및 평가를 위하여서는 그 내용에 대하여 살펴볼 필요가 있다.

'통일경찰법모범초안에 대한 개정초안'을 내놓게 된 동기는 1984년 10월 31일의 첫 번째 초안에서 밝힌 바와 같이, 1983년의 인구조사법에 대한 연방헌법재판소의 판결에 있다. 연방헌법재판소의 인구조사판결은 국가의 정보수집 및 처리에 대한 법률규정의 허용성에 관하여 많은 헌법적 요구를 내포하고 있는데, 그에 의하면 그때까지의 경찰법상의 일반조항은 경찰의 정보관리에 대한 근거규정으로 불충분하고 따라서 법률에서 침해의 요건에 대하여 가능한 한 구체적이고 자세한 규정을 두는 것이 필요하게 되었다. '통

51) 이에 대하여는 Kowalczyk, Datenschutz im Polizeirecht, 1989, S. 65 f.; Götz, Allgemeines Polizei- und Ordnungsrecht, 12. Aufl., 1995, S. 72 참조.

일경찰법모범초안에 대한 개정초안'은 그때까지 경찰업무의 수행을 위하여 행해져온 정보관리활동의 필요성을 전제로 하고, 그 법적 근거로서 그때까지는 대부분 행정규칙에서 규율되었던 것을 법률에서 명확하게 규정하는 것을 그 내용으로 한다.⁵²⁾

'통일경찰법모범초안에 대한 개정초안'은 "경찰은 공공의 안녕·질서에 대한 위험을 방지함을 직무로 한다"고 규정한 통일경찰법모범초안 제1조 1항의 전통적인 실질적 의미의 경찰개념을 보충하여, 경찰은 이러한 직무의 범위 내에서 범죄수사에 대비하거나 범죄행위를 저지하기 위한 예방적 범죄투쟁(Vorbeugende Bekämpfung von Straftaten)과 장래의 위험을 방지하기 위한 준비행위(Vorbereitung auf die Gefahrenabwehr)를 할 수 있음을 명문으로 규정하였다. 이와 같은 직무범위의 확장에 대한 제안이유에 의하면 예방적 범죄투쟁은 전통적으로 위험방지에 속하는 것이라고 한다. 그러나 '구체적 위험'이나 '경찰책임자'(Störer)와 같은 전통적인 개념은 여기에 적용되지 않으며, 장래 범죄행위가 행해질 것이라는 의심이 있으면 예방적 범죄투쟁의 권한이 행사될 수 있다고 한다.⁵³⁾ 이와 관련하여 과연 예방적 범죄투쟁이 전통적인 위험방지 영역에 속하는 것인지는 의문이다. '통일경찰법모범초안에 대한 개정초안' 스스로 전통적인 위험방지와 예방적 범죄투쟁이 일치하지 않는다는 것을 전제로 하고 있음은 통일경찰법모범초안 제8조 1항을 개정한 내용으로부터 도출할 수 있다. 그에 의하면 제8a조 내지 제24조에서 경찰의 권한에 대하여 특별히 규정하고 있지 않는 한, 경찰은 공공의 안녕·질서에 대하여 존재하는 구체적인 위험을 방지하기 위하여 필요한 조치를 취할 수 있다고 한다. 이 규정은 일반적인 위험방지권한과 특별한 권한의 분리를 전제로 한다. 새로운 직무범위가 주어진 것이라는 측면에서 볼 때, 이 규정에 의하여 위험개념과 결합하지 않고 경찰활동이 행해질 수 있는 가능성이 열려진 것이다. 이러한 확장된 경찰의 직무범위에 상응하여 '통일경찰법모범초안에 대한 개정초안'에서는 전통적인 위험방지의 원칙을 넘어서 경찰의 정보수집이 행해지는 데 대한 수권규정을 명문으로 두고 있다(§§ 8a-d VE ME PolG 참조).

'통일경찰법모범초안에 대한 개정초안'에는 기존의 표준적인 직무조치(신원확인, 감식

52) Neumann, Vorsorge und Verhältnismässigkeit, 1994, S. 35.

53) Neumann, Vorsorge und Verhältnismässigkeit, 1994, S. 36.

조치, 소환)를 넘어서는 광범위한 정보의 수집과 처리에 관한 법률 규정을 매우 상세하게 규율하고 있다.⁵⁴⁾ 위의 기존의 표준적인 직무조치는 해당규정에 의하여 또는 직무범위 내에서 비권력적인 사실행위로써 언제나 허용될 수 있는 정도의 것으로 정보보호의 필요성 범위 내에 있지 않은 것으로 볼 것이며, 형사소송절차로써 이루어지는 모든 작용들은 별도의 형사소송법의 규율을 받는다는 차원에서 정보보호적 차원에서 규제의 대상이 되는 것은 위의 영역 사이에 존재하는 것들에 관한 것이라고 할 것이다.

II. 정보보호법과 경찰의 정보관리

1. 수권규정으로서의 정보보호법

경찰영역에서의 정보는 대부분 강제적으로 또는 비밀리에 수집되기 때문에 그를 위하여서는 특별하고 자세한 법적 근거가 있어야 한다. 이에 대한 충분한 법적 근거가 마련되어 있지 않은 상황에서는 일반적인 정보보호법이 그에 대한 법적 근거가 될 수 있는지를 살펴보아야 한다.

연방과 주의 정보보호법은 자연인의 개인관련 정보만을 보호한다. 연방정보보호법은 연방의 다른 법규정이 개인정보와 그의 공개에 적용되지 않는 한(법 제1조 4항 1문), 연방의 공공기관에 의한 개인정보의 수집, 처리 및 이용에 적용된다(법 제1조 2항 1호). 이전에 정보저장과 정보제공에 대한 정보보호법상의 일반조항(예컨대 연방정보보호법 제14조, 제15조)에서 개인의 법적 지위에 대한 제약(Eingriff)의 근거를 도출할 수 있다는 주장이 있었으나,⁵⁵⁾ 타당하지 않다. 정보와 관련하여 개인의 이익을 보호하려는 정보 '보호법'으로부터 모든 경우에 적용 가능한 침해의 수권규정을 도출할 수 있다는 전제부

54) 당초의 통일경찰법모범초안에서는 정보수집, 정보처리 및 정보이용 등에 대한 특별규정을 두고 있지 않았다. 그러나 인구조사판결에 의하여 개인정보의 수집, 처리 및 이용이 정보의 자기결정권을 침해하는 것이 인정되어 그에 관하여 구체적이고 자세한 규정이 필요하게 되었다.

55) Auernhammer. BDSG-Kommentar, 2. Aufl., 1981, Einf. Rdn. 37, § 9 Rdn. 2.

터 잘못된 것이다. 연방정보보호법 제14조는 저장하고자 하는 기관의 권한에 속하는 직무수행을 위하여 필요한 경우에만 정보저장이 허용된다고 규정하고 있으므로, 우선 특별법에서 저장하려는 기관의 직무수행을 위하여 정보저장이 필요함을 규정하고 있어야 한다. 이러한 해석은 인구조사판결에서도 확인되었다. 따라서 경찰이 개인관련 정보를 저장·처리함에 있어서는 구체적이고 자세한 법적 근거가 있어야 한다는 것은 의문이 여지가 없게 되었다.

정보보호법의 일반조항에 포함되어 있는 필요성의 원칙은 새로운 경찰법에 마찬가지로 규정되어 있으며, 더욱이 법치국가원칙에서 도출되고 경찰법에 확고한 뿌리를 두고 있는 비례의 원칙의 한 내용으로서 개별적 규정이 없더라도 준수되어야 함은 당연하다. 정보보호법의 일반조항과 관련 없이 정보처리는 특별한 규정이 없더라도 적법한 직무수행을 위하여 필요한 범위 내에서만 허용되는 것이다. 정보저장에 대한 개별적인 근거규정이 없는 경우에 그의 법적 근거로서 일반적인 정보보호법이 고려되는 것은 배제된다.

2. 정보보호법의 경찰영역에의 적용

연방정보보호법 제1조 4항과 그와 동일한 주법상의 규정은 일반적인 정보보호법과 개별적인 정보보호법 사이의 적용우위에 대하여 규율하고 있다. 그에 의하면 공개를 포함하여 개인정보에 대한 적용이 문제되는 한 특별법 규정이 우선하도록 되어 있다. 헌법합치적 해석에 의하면, 적어도 강제적으로 수집된 정보에 있어서는 충분한 정보보호조치를 마련하고 있어 정보처리에 적용할 수 있는 규정에만 우위가 인정되어야 한다. 경찰정보처리에 관한 특별법 규정이 증가함에 따라 개별적인 정보보호법이 일반적인 정보보호법에 우선하는 경우가 많아 졌다. 일반적인 정보보호법은 특별법에 흠결이 있거나 공백이 있는 경우에는 여전히 의미를 가진다.

경찰법에서 정보보호에 관련된 용어의 정의규정을 두고 있지 않은 경우에 일반적인 정보보호법상의 개념정의를 경찰영역에서도 그대로 적용될 수 있을 것이다. 예컨대 수집, 저장, 제공, 수정, 삭제 등의 의미, 누가 저장기관이며 제3자에 해당하는지 등에 대하여 경찰영역에서 그에 대한 특별한 규정을 두고 있지 않는 한, 일반적인 정보보호법에서 지속적으로 규정하고 있다고 보아야 한다.

III. 경찰의 정보관리에 관한 법적 규율

‘통일경찰법모범초안에 대한 개정초안’에는 경찰의 정보수집·처리와 관련하여 정보의 저장, 수정, 이용, 제공과 자동화된 검색절차, 정보의 조정 그리고 정보의 정정, 삭제, 차단 등에 대하여 규정하고 있다. 이들 개념에 대하여는 경찰영역에서 특별한 규정을 두고 있지 않는 한 일반적인 정보보호법상의 개념정의가 그대로 여기에도 적용된다.

아래에서는 정보보호와 관련하여 중요한 경찰의 정보활동을 ① 정보의 수집, ② 정보의 처리(저장, 수정, 이용), ③ 정보의 제공, ④ 정보의 정정, 삭제, 차단 그리고 ⑤ 관련자의 고지청구권 등 구분하여 살펴보기로 한다.

1. 경찰에 의한 정보수집

(1) 개념정의: 정보의 수집

경찰의 정보수집이란 경찰이 경찰목적에 위하여 특정한 자연인에 대한 개인관련 정보를 획득하는 모든 활동을 말한다. 획득된 정보의 고정화 작업(Fixierung)은 수집의 단계에 속하는 것이 아니라 그 다음의 편입(Erfassung)에 해당하는 것이다. 수집에 해당하는지를 판단함에 있어서는 경찰조사활동의 목적이 중요한 기준이 된다. 계속 사용하기 위한 의도로 행해진 모든 의식적인 개인정보의 인지와 기록화(Registrierung)는 수집에 해당한다. 경계의 눈을 가지고 거리를 걷어가는 경찰공무원은 그가 인지하는 모든 정보를 수집하는 것이 아니라, 계속사용의 목적으로 의식적으로 인지하는 정보만을 수집하는 것이다. 수집은 직무수행을 위하여 필요한 경우에만 허용된다. 일상적인 실무에서 정보수집이 존재하느냐의 여부는 보통 문제되지 않는다. 관계자의 보호할 가치 있는 이익에 대한 위협은 수집된 정보를 편입하고 저장하는 단계에서 비로소 제기된다. 그러나 이것이 수집이 정보보호에 있어서 중요한 과정의 하나라는 사실을 부인하는 것은 아니다. 수집에 있어서의 법적 하자는 그 이후의 정보처리 단계의 적법성에 영향을 미칠 수 있는 것이다.

(2) 개괄적 수권조항에 의한 정보수집

주의 경찰법에 규정되어 있는 '표준권한'(Standardbefugnisse)은 대부분 개인정보의 수집을 목적으로 한다.⁵⁶⁾ 그 이외에 개괄적 수권조항(Generalklausel)에 근거하여 어느 정도로 정보수집이 행해질 수 있는지가 문제될 수 있다. 적어도 표준권한에 규정되어 있는 방법은 단지 그에 근거하여서만 가능한 것이고 개괄적 수권조항을 근거로 실행될 수 없다는 점에 대하여는 의견의 일치를 보고 있다. 예컨대 감식사무의 처리(Erkennungsdienstliche Behandlung) 또는 신원확인 심사는 전적으로 특별권한에 근거하여 행해져야 하며 개괄적 수권조항을 근거로 할 수 없다.

경찰상의 개괄적 수권조항은 현존하는 구체적 위험을 방지하기 위하여 경찰책임자 - 예외적으로 비책임자 - 에 대한 권리제한의 권한을 부여한다. 이것은 경우에 따라서는 정보의 수집보다 강력한 조치에 대한 수권도 포함한다. 따라서 제한의 정도에 있어서 정보수집은 개괄적 수권조항에 근거하여 행해질 수 있는 조치의 범위 내에 있는 것이다.⁵⁷⁾ 그러나 정보의 자기결정권에 대한 제한은 규범적으로 명확한 법적 근거를 요한다. 그렇다고 하여 개괄적 수권조항의 적용이 원칙적으로 배제되는 것은 아니다. 경찰상의 개괄적 수권조항은 오랜 동안의 판례와 실무에서 구체화되었고 시민의 법의식에 굳게 자리잡고 있는 것이다. 시민들은 경찰에게 허용되는 것과 허용되지 않는 것이 무엇인지를 알고 있다. 그로부터 정보의 자기결정권에 대한 제한의 한계가 도출될 수 있는 것이다.

그러나 경찰법에서 공공의 질서유지를 경찰의 직무에 속하는 것으로 규정하고 있는 한 의문이 제기될 수 있다. 공공의 질서가 무엇인지는 그 당시의 사회관·윤리관에 따라 상이하게 나타난다. 따라서 시민들은 어떠한 조건 하에 경찰이 공공의 질서유지를 위하여 정보를 수집할 수 있는지를 명확하게 예견할 수 없다. 그러한 한도 내에서 개괄적 수권조항은 법적 근거에 대한 명확성의 요구를 충족하지 못하는 것이 된다.⁵⁸⁾ 다만 그

56) 이에 대하여는 Rchor, in: Lisken/Denninger, Handbuch des Polizeirechts, 2. Aufl., 1996, F. Rdn. 1 ff. 참조.

57) 외관상 위험(Anscheinsgefahr)과 위험의 의심(Gefahrenverdacht)의 경우에 있어서 정보수집에 대하여는 Deutsch, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1991, S. 210 f. 참조.

58) Knemeyer, NVwZ 1988, 193 (195); Kowalczyk, Datenschutz im Polizeirecht, 1989, S. 77;

에 대한 명확한 법적 규정이 마련될 때까지는 헌법에 더욱 합치되지 않는 상황이 발생하는 것을 피하기 위하여 개괄적 수권조항을 과도기적으로 법적 근거로 볼 수 있다고 해야 할 것이다. 그러나 그러는 사이에 몇몇 주에서 공공의 질서유지를 경찰의 직무범위에서 완전히 삭제해 버렸기 때문에 그와 같은 주장을 하는 것도 어렵게 되었다. 따라서 개괄적 수권조항에 근거하여 공공의 질서유지의 목적으로 개인관련 정보를 수집하는 것은 - 과도기적으로도 - 허용되지 않는다.

공공의 안전에 대한 구체적이고 직접적인 위험이 존재하는 경우에는 개괄적 수권조항에 근거하여 정보수집이 행해질 수 있다. 위와 같은 경우에 위험방지를 위하여 필요한 경찰책임자에 대한 개인정보가 수집될 수 있는 것이다. 비책임자에 대한 정보수집은 더 엄격한 요건 하에 허용될 수 있다.⁵⁹⁾ 따라서 제3자에 대한 정보의 수집, 예컨대 부상자, 의지할 데 없는 자 또는 행방불명된 자와 그의 가족, 법정대리인 또는 상담역, 위험에 처한 자, 증인 또는 참고인 등에 대한 정보수집은 비책임자에 대한 경찰권 발동의 요건이 충족되지 않는 한 배제된다. 마찬가지로 위험방지에 대한 특별한 능력과 지식을 갖고 있는 사람들에 대한 정보수집, 그로부터 중대한 위험이 발생하는 시설의 책임자 및 위험이 이미 발생한 시설의 책임자로부터 정보를 수집하는 것은 그들의 동의가 없는 한 허용되지 않는다.

개괄적 수권조항에 근거하여서는 단지 구체적 위험의 제거를 위한 권리제한만이 허용되므로, 예방목적을 위한 정보수집은 고려될 수 없다. 그러나 독일에 있어서 개괄적 수권조항이 경찰의 정보처리에 관한 조치의 법적 근거로서 인정될 수 있는지에 대하여는 더 이상 논의의 실익이 없다. 모든 주의 경찰법에서 정보수집에 대한 일반적인 수권규정을 두고 있기 때문이다.

Lisken, ZRP 1990, 17. 다른 생각으로는 Drews/Wacke/Volgel/Martens, Gefahrenabwehr, 9. Aufl., 1986, 245 ff. 참조.

59) 그 요건에 대하여는 Knemeyer, NVwZ 1988, 193 (195) 참조. 다른 생각으로는 Krüger, DÖV 1990, 641 (645).

(3) 정보수집에 대한 법적 규율

(가) 일반적인 수집권한

독일의 모든 주의 경찰법은 정보수집에 대한 일반적인 수권규정을 두고 있다. 일반적인 정보수집의 권한과 정보수집에 대한 특별권한 사이의 관계는 일반적 수권조항과 특별 수권조항에서처럼 특별법 우선의 원칙에 의하여 해결하면 된다. 일반적인 정보수집의 권한에 있어서 범죄와 관련이 없는 단순한 위험방지의 목적을 위한 정보수집과 위험방지의 특별한 형태로서 범죄예방을 위한 정보수집을 구별하여야 한다.⁶⁰⁾

위험방지를 위한 정보수집에 있어서 공공의 안녕·질서에 대한 구체적인 위험이 존재하여야 하는가에 대하여 독일의 입법은 두 가지 규율형태로 나눌 수 있다. 바이에른, 브란덴부르크, 튀링엔 경찰법은 경찰의 직무범위에 속하는 한 정보수집을 할 수 있다고 규정하고 있다. 이들 주에서는 조직적 의미의 경찰과 탈경찰화된 질서행정청을 구분하는 체계를 취하고 있는데, 경찰법은 집행경찰(Vollzugspolizei)에게만 적용된다. 여기서는 위험방지와 범죄예방(또는 예방적 범죄투쟁)을 구별하지 않고 있다. 이것은 범죄예방을 전통적인 경찰의 위험방지 업무로 파악하는 한 당연한 것이다. 위험개념을 개별적인 경우에 존재하는 위험, 즉 '구체적 위험'(konkrete Gefahr)으로 파악하지 않고, '추상적 위험'(abstrakte Gefahr)의 존재만으로 충분한 것으로 보고 있다. 노르트라인-베스트팔렌의 경찰법도 두 그룹의 행정청을 구분하는 법체계에 속한다. 노르트라인-베스트팔렌 경찰법 제9조 1항, 2항에 의하면 일반적인 정보수집의 권한에 대하여 규정하고 있지 않지만, 구체적 위험을 요구하지 않으며 모든 사람에게 조치를 취할 수 있다는 점에서 여기에 포함시킬 수 있다.

이러한 규율형태와 달리 바덴-뷔르템베르크, 브레멘, 베를린, 함부르크, 헤센, 작센-안할트, 메클렌부르크-포아폼메른, 자르란트, 슐레스비히-홀슈타인 등의 경찰법에서는 위험방지를 위한 정보수집과 범죄예방을 위한 정보수집을 구별하고 있다. 이들 주에서는 경찰행정청과 질서행정청을 구분하지 않는 통합체계를 취하고 있는데, 범죄예방은 오직

60) 물론 이러한 구별이 정보수집에 한정되는 것은 아니고 원칙적으로 정보처리에 관한 모든 권한에 적용된다.

집행경찰의 직무영역에만 속하게 되며, 그에 따라 그에 대한 특별규정을 두고 있다. 이들 주의 경찰법에서는 경찰행정청과 질서행정청에게 위험방지를 위한 정보수집의 권한을 부여하고 있는데, 정보수집을 위하여서는 '구체적 위험'이 존재하여야 하며, 원칙적으로 경찰책임자만을 대상으로 할 수 있고 예외적으로 특별한 요건을 충족한 경우에는 비책임자를 대상으로 할 수 있도록 규정하고 있다.

그에 대하여 범죄예방을 위한 정보수집에 대하여는 다른 요건을 요구한다. 이들 주에서는 범죄행위가 아직 종료되지 않았거나 범죄행위의 준비단계에 있는 경우에는 아직 공공의 안전에 대한 경찰상의 위험이 존재하지 않고 또한 형사소송법 제163조의 직무범위에 속하지 않는다는 생각을 밑바탕에 깔고 있다. 그러나 오늘날의 이른바 조직범죄에 효과적으로 대처하기 위하여서는 이미 이 단계에서 어떠한 대응방안이 강구되어야 한다는 점을 고려하여, 새로운 경찰법에서는 '잠재적' 범죄자, 그와의 접촉인물, 희생자 및 증인에 대한 정보수집의 권한을 부여하고 있다. 이와 같은 정보수집을 위하여서는 범죄행위가 행해질 것이라는 생각을 정당화 할 수 있는 사실관계가 존재하여야 한다.⁶¹⁾

(나) 위험방지를 위한 정보수집

(a) 정보수집의 대상

'통일경찰법모범초안에 대한 개정초안'과 새로운 주의 경찰법에서는 위험방지를 위하여 필요한 경우에는 경찰책임자, 일정한 조건 하에 비책임자, 부상자, 의지할 데 없는 자, 행방불명된 자 및 그의 가족, 법정대리인 또는 상담역, 위험에 처한 자, 증인 또는 참고인에 대한 개인관련 정보를 수집할 수 있다고 규정하고 있다.⁶²⁾ 경찰은 경찰책임자, 비책임자 및 제3자에 대한 정보를 수집할 수 있다고 규정하고 있는 헤센과 바이에른의 경찰법은 너무 포괄적이다.⁶³⁾ 이것은 모든 사람에 대한 정보를 수집할 수 있다는 것과

61) § 20 Abs. 3 Nr. 1 BWPolG, § 28 Abs. 1 Nr. 2 BremPG, § 6 Nr. 6 HambDVPolG, § 13 Abs. 2 Nr. 1 HSOg, § 26 Abs. 2 Nr. 1 SPolG 등 참조.

62) 예를 들면 § 26 Abs. 1 SPolG.

63) § 13 Abs. 1 Nr. 3 HSOg, Art. 28b Abs. 1 BayPAG 참조. § 28 BremPolG은 위험방지의

다르지 않다.⁶⁴⁾

물론 이러한 포괄적인 규정으로부터 누구에 대하여 정보를 수집할 것인지가 경찰의 자의에 맡겨져 있다는 결론을 도출할 수 있는 것은 아니다. 위협의 원인자가 우선적으로 위협의 제거에 대한 책임을 부담해야 한다는 위협방지법의 기본원칙은 그에 대한 특별한 규정이 없더라도 정보처리의 영역에서도 적용된다. 따라서 경찰은 위협방지 영역에서 정보수집을 함에 있어서 우선적으로 경찰책임자를 대상으로 해야 한다. 즉 경찰책임자에 대한 정보는 바로 그로부터 수집해야 한다. 이것이 불가능할 경우에 그에 대한 정보를 제3자로부터 수집할 수 있는 것이다. 그 다음에 제3자에 대한 정보수집이 고려되고 그 뒤로 제3자에 대한 정보를 제3자로부터 수집하는 것이 고려된다.

정보수집에 있어서 위와 같은 단계를 지키는 것은 연방헌법재판소의 인구조사판결의 요구에 부합하는 것이다. 경찰이 위협을 제거하기 위하여 누구든지에 대하여 정보를 자의적으로 수집할 수 있다고 한다면, 시민은 어떠한 요건 하에 자신의 정보적 자기결정권이 제한될 수 있는지를 알 수 없게 된다.

여하튼 정보수집, 처리 및 이용에 대한 경찰의 권한은 행위 또는 상태책임자와 일정한 조건 하에 비책임자를 대상으로 할 뿐만 아니라, 지금까지 경찰상의 수범자의 범위에 포함되지 않았던 다른 여러 관련자들에게까지 미친다. 즉 정보의 수집에 있어서 전통적인 경찰책임의 원칙은 수정을 받게 되었다. 이와 같이 정보수집의 대상자의 범위가 포괄적이라 하더라도, 정보수집은 경찰의 직무수행을 위하여 필요한 경우에만 허용된다는 제한을 받는다. 불특정한 또는 아직 확정되지 않은 목적을 위한 정보의 수집은 허용되지 않는다.⁶⁵⁾

목적을 위하여 어떠한 사람에 대한 정보를 수집할 수 있는지에 대하여 아무런 규정을 두고 있지 않다.

64) 이와 유사한 규정을 갖고 있는 것으로는 노르트라인-베스트팔렌의 경찰법을 들 수 있다. § 9 Abs. 1 PolG NW은 일반적인 질문권(Befragungsrecht)에 대하여 규정하면서, 경찰은 직무수행, 즉 위협방지를 위하여 도움이 되는 진술을 할 수 있는 '모든 사람'에게 질문을 할 수 있다고 규정하고 있다. 이 규정으로부터는 누구에 대한 정보를 수집할 수 있는지에 대하여 알 수 없지만, § 9 Abs. 3에 의하여 그것은 질문자 자체에 대한 정보가 된다.

65) § 13 Abs. 5 HSOG 참조.

(b) 정보수집의 요건

정보수집을 위하여서는 경찰상의 '위험'이 존재하여야 한다. 다만 노르트라인-베스트팔렌⁶⁶⁾과 자르란트⁶⁷⁾에서는 공공의 안전에 대한 위험만을 의미하는 데 대하여, 헤센⁶⁸⁾과 다른 주⁶⁹⁾에서는 그 이외에 공공의 질서에 대한 위험까지 포함한다는 점에서 차이가 있다. 더 나아가 기본권에 의하여 보호되는 법적 지위에 대한 침해가 있는 경우에는 '구체적 위험'이 존재해야 한다.

(c) 정보수집의 범위

수집될 정보의 범위와 관련하여 위험을 방지하기 위하여 필요한 한도 내에서만 정보수집이 허용된다. 따라서 통상적으로 경찰책임자의 신원을 확인할 수 있으며 위험과 관련된 정보가 수집될 수 있는 것이다.⁷⁰⁾ 그 이외에 노르트라인-베스트팔렌에서는 관련자를 보호하기 위하여 필요한 경우에는 질병 및 특별한 행동양식에 대한 정보를 수집할 수 있다고 규정하고 있다.⁷¹⁾ 통상적인 경우에 투입된 경찰관 또는 제3자를 보호하기 위하여 질병에 관한 정보를 획득하는 것은 필요하지도 않고 가능하지도 않다. 이와 같은 정보수집은 질병이 전염되지 않는 방법으로 위험이 제거될 수 있는 경우에는 처음부터 배제된다. 질병이 전염될 가능성이 있는데, 위험이 급박한 경우에는 신뢰할 만한 정보수집의 시간과 가능성이 없게 되는 것이 보통이다. 치료한 의사로부터 정보를 수집하는 것은 의사의 비밀준수의무 때문에 그 의무의 면제를 인정하는 명문규정이 없는 한 허용되지 않는다. 제3자에게서 질병에 대한 정보를 수집하는 것은 부정확한 정보의 위험이 있다. 많은 경우에 부정확한 전문정보에 의하여 관련 공무원, 제3자 또는 관련자 자신은 더 큰 위험에 직면하게 될 수 있다. 결국 질병에 대한 정보의 수집·저장에 있어서는 신중하게 접근하여야 할 것이다. 그밖에 경찰은 위험의 제거를 위하여 합리적 예측을 함

66) § 1 Abs. 1 PolG NW.

67) § 1 Abs. 2 SPolG.

68) § 1 Abs. 1 HSOG.

69) 예를 들면 § 1 PolG BW.

70) § 9 Abs. 5 PolG NW 참조.

71) § 9 Abs. 5 S. 2 PolG NW 참조.

에 있어서 필요한 정보를 수집할 수 있다. 정보의 이용에 대한 특별법적 규정을 준수해야 함은 당연하다.⁷²⁾

(다) 범죄예방을 위한 정보수집

경찰상의 구체적인 위협에 대한 효과적인 방지를 위하여서는 관련된 개인정보의 수집, 처리 및 이용이 전제되어야 한다. 따라서 경찰의 정보수집은 구체적인 위협이 발생하기 전에, 즉 위험배려(Gefahrenvorsorge)의 단계에서 행해져야 한다. 이를 위하여 '통일경찰법모범초안에 대한 개정초안'에서는 경찰에게 경험측상 사실상의 관점에 비추어 볼 때 예방적 범죄투쟁(위험배려의 영역)을 위하여 필요한 경우에는 특정인(예상되는 장래의 범죄자와 그와의 접촉자 또는 동반자, 범죄의 피해자가 될 것이 예상되는 자 및 증인 또는 참고인)에 대한 정보의 수집권한을 부여하고 있다.⁷³⁾

(라) 공개된 행사, 모임 및 집회에서의 정보수집

경찰이 공개된 행사, 모임 또는 집회를 단순한 관찰자로서, 망원경에 의하여 또는 사진촬영이나 녹음에 의하여 감시하는 것은 단순한 사실행위로서 침해에 해당하지 않는다. 그러나 그에 의하여 특정인의 신원을 확인하게 된다면 특별한 법적 근거가 필요한 침해에 해당한다. 즉 인구조사판결에 따라 이러한 정보수집에는 법적 근거가 있어야 하는데, 기본법 및 집회법상의 집회에서의 정보수집에 대하여는 집회법(Versammlungsgesetz) 제12a조 및 제19a조에서 근거규정을 두고 있으나, 그 이외의 경우에는 법적 근거가 없었다. 따라서 집회법 제12a조 및 제19a조에 의한 집회에서의 정보수집권한을 보충하여 주의 경찰법에서 공개된 행사와 모임에서의 정보수집에 대하여 규정하게 되었다.⁷⁴⁾ 이러한 수권규정의 목적은 한편으로는 구체적 위협의 전 단계에서의 위험방지와 개인의

72) 예를 들면 § 68, § 71 SGB X.

73) § 8a Abs. 2 VE ME PolG.

74) § 21 Abs. 1 BWPoIG, § 24 Abs. 1 ASOG Bln, § 34 BrbgPolG, Art. 32 Abs. 1 BayPAG, § 30 BremPG, § 8 HambDVPolG, § 14 HSOG, § 32 Abs. 1 SOGMV, § 16 Abs. 1 LSASOG, § 15 NWPoIG, § 27 SPoIG, § 184 Abs. 1 SHLVwG, § 33 Abs. 1 ThürPAG 등 참조.

권리보호이며, 다른 한편으로는 범죄의 예방을 위함이다.

주의 경찰법 규정은 수집권한을 확장하기도 하고 반대로 제한하는 측면도 있다. 수집권한을 확장하는 것으로는 공개된 행사 및 모임에서의 정보수집은 처음부터 경찰책임자에 한정되지 않는다거나,⁷⁵⁾ 제3자가 불가피하게 관련되는 한 정보수집이 허용된다거나,⁷⁶⁾ 또는 제3자에 대한 정보수집을 명문으로 허용하는 것⁷⁷⁾ 등을 들 수 있다.

제한하는 측면으로는 급박한 범죄행위⁷⁸⁾ 또는 질서위반⁷⁹⁾의 경우에만 정보가 수집될 수 있고 그 밖의 공공의 안전에 대한 위협의 경우에는 수집될 수 없다는 규정을 들 수 있다.⁸⁰⁾ 이와 같은 규정에 의하여 공개된 행사와 모임의 특별한 보호의 필요성이 고려되어야 한다.⁸¹⁾ 그 밖의 정보처리의 제한으로는 수집된 정보는 일반적인 위험방지의 목적이 아닌, 관찰된 행사에서 또는 그를 계기로 발생된 질서위반행위의 추적을 위하여 또는 범죄수사를 위한 목적에만 사용될 수 있다는 것을 들 수 있다.⁸²⁾ 또한 수집된 정보는 위의 목적을 위하여 필요하지 않는 한, 행사 또는 모임이 끝난 뒤 일정기간 내(1개월 내지 2개월 이내)에 삭제되어야 하는 것도 그에 해당한다. 공개된 행사 및 모임의 연장선상에서 위험방지의 목적으로 경찰이 정보를 수집하고 처리하는 것은 특별한 규정에 의하여 규율되고 있다.

이러한 규정을 됴으로써 경찰의 감시활동에 의하여 시민이 어떠한 행사나 모임에 참

75) § 27 SPolG. 그러나 § 32 Abs. 1 S. 3 SOGMV와 § 184 Abs. 1 S. 2 SHLVwG는 행위책임자와 상태책임자에 대한 정보수집에 한정하고 있다.

76) § 15 Abs. 1 S. 2 PolG NW, § 8 Abs. 1 HmbDVPolG, Art. 28c Abs. 1 BayPAG.

77) § 14 Abs. 1 HSOG.

78) § 24 ASOG Berl, § 16 SOG LSA.

79) § 14 Abs. 1 HSOG 및 § 32 NGefAG('nicht geringfügige'); Art. 28c Abs. 1 BayPAG('von erheblicher Bedeutung'), 유사한 규정으로는 § 21 PolG BW, § 33 ThürPAG.

80) 작센에서는 그 밖의 공공의 안녕에 대한 현저한 위협이 존재하는 경우에도 정보수집을 허용하고 있으며, 더 나아가 튀링엔에서는 일반적으로 공공의 안녕 또는 질서에 대한 위협의 경우에 허용하고 있다(§ 33 ThürPAG).

81) 이러한 측면에서 공공의 안녕에 대한 위험방지를 위하여 정보수집을 일반적으로 허용하고 있는 § 27 SPolG은 문제가 있다.

82) 그러나 § 27 SPolG는 예방적 범죄투쟁의 목적으로도 사용될 수 있다고 규정하고 있다. § 38 Abs. 3 SächsPolG는 공적 또는 사적 청구권의 주장을 위하여도 사용될 수 있다고 하는데 받아들이기 곤란하다.

여하는 것을 주저하게 될지도 모른다는 우려를 불식시켜야 한다. 즉 의도된 경찰의 감시 활동은 질서위반행위에 대한 책임자에 한정하여야 하고 모든 평화적인 집회 및 시위는 경찰의 정보수집에서 배제되어야 한다. 또한 은밀한 사진촬영이나 감청이 허용되어서는 안 된다.⁸³⁾

(마) 정보수집의 특별한 수단

‘통일경찰법모범초안에 대한 개정초안’은 경찰에게 정보수집을 위하여 특별한 수단을 사용할 수 있는 권한을 부여하였다.⁸⁴⁾ 예를 들면 숨겨진 기계시설의 설치(verdeckter Einsatz technischer Mittel), 신분을 위장한 경찰관(verdeckte Ermittler)의 배치, 경찰에 협조하는 것이 알려지지 않은 신뢰할 수 있는 사람(V-Leute)의 배치 등이 그에 해당한다. 숨겨진 기계시설의 설치란 비디오카메라 또는 마이크 등의 설치에 의하여 관계인이 모르게 사진촬영, 비디오녹화 또는 녹음을 하는 것을 말한다. 신분을 위장한 경찰관이란 가명을 가지고 범죄수사 또는 위협방지를 위하여 투입된 경찰공무원을 말한다. 신뢰할 수 있는 사람이란 경찰이 아니면서 여러 동기에 의하여 경찰이 범죄를 수사함에 있어서 도움을 주는 사람으로 그 신원이 경찰행정청에 의하여 비밀로 유지된다.⁸⁵⁾

이러한 정보수집의 특별한 수단은 통상적으로 중대한 기본권 침해를 가져올 수 있기 때문에 특히 엄격한 요건 하에서만 허용된다. 법에 열거되어 있는 중대한 범죄의 예방을 위하여 또는 중대한 위협의 방지를 위하여 필요한 경우에 한하여 허용될 수 있다. 주의 경찰법에 의하면 정보수집의 특별한 수단은 공공의 안전에 대한 직접적인 위협이 이미 발생한 경우에만 사용될 수 있는 것은 아니다. 사실상의 관점에서 범죄의 발생이 예견되는 것만으로 충분하다. 범죄의 발생이 목전에 급박해 있을 필요는 없다. 일반적으로 정보수집의 특별한 수단은 직접적인 위협발생의 방지를 위하여 사용될 수 있다고 볼 수 있다.

83) § 24 Abs. 1 ASOG Berl 참조.

84) § 8c VE ME PolG.

85) BVerfGE 57, 250 (284). 신뢰할 수 있는 사람은 경찰법상의 권한 및 다른 공권력을 행사할 수 없다. 이러한 이유로 바덴-뷔르템베르크와 바이에른에서는 이러한 사람의 투입에 대하여 규정하고 있지 않다.

그러나 이것이 위험방지를 위하여 정보수집의 특별한 수단을 일반적으로 사용할 수 있다는 것을 의미하는 것은 아니다. 개별적인 수권규정에 열거되어 있는 범죄행위가 발생할 위험이 존재해야만 한다. 이러한 정도를 넘지 않는 범죄행위 내지 그 밖의 위험을 방지하기 위하여서는 특별한 정보수집의 수단을 사용할 수 없다.

많은 주의 경찰법에서는 위험방지의 목적을 위하여 특별한 정보수집 수단의 사용을 명문으로 규율하고 있다. 예를 들면 노르트라인-베스트팔렌에서는 생명·신체 또는 자유에 대한 현존하는 위험의 방지를 위하여 필요한 경우에는 관찰,⁸⁶⁾ 사진촬영과 비디오 녹화를 위한 숨겨진 기계시설의 설치,⁸⁷⁾ 감청과 녹음을 위한 숨겨진 기계시설의 설치,⁸⁸⁾ 경찰에 협조하는 것이 알려지지 않은 사람의 배치⁸⁹⁾ 및 신분을 위장한 경찰관의 배치⁹⁰⁾에 의한 경찰책임자와 비책임자에 대한 정보수집을 허용하고 있다. 다른 주의 경찰법에서는 정보수집을 위한 특별한 수단의 투입을 단지 생명·신체 또는 건강에 대한 직접적인 위험을 방지하기 위한 경우에만 허용하고, 일반적으로 범죄예방의 목적으로는 허용하지 않고 있다. 이것은 특히 주거로부터 정보를 수집하는 경우에 적용된다. 자르란트에서는 주거, 일자리, 영업소, 사무소 또는 다른 평온한 소유물 안에서 또는 그러한 공간으로부터 특별한 수단에 의하여 정보를 수집하는 것은 생명·신체에 대한 현존하는 위험이 존재하고 그러한 수단의 투입이 필수 불가결한 경우에만 허용하고 있다.⁹¹⁾

경찰의 직무수행이 다른 방법으로는 위험하게 되거나 현저히 곤란해지는 경우에는 장기간의 관찰, 기계시설의 설치 등을 허용하는 튀링엔의 경찰법 규정⁹²⁾은 너무 광범위하게 특별한 수단의 사용을 수권하는 것으로 문제가 있다. 이와 같은 광범위한 수권규정은 개별적인 구성요건의 확인가능성을 필요 없게 만든다. 기본권에 대한 중대한 침해가 문제됨에도 연방헌법재판소가 요구하는 규범의 명확성을 충족하지 못하는 것이다.

86) 관찰은 계획적이고 의도적으로 특정인을 오랜 기간 동안 감시하는 것을 말하는데, 그것이 공개적이든 비밀스럽게 행해지든 관계없다. 이에 대하여는 § 16 Abs. 1 Nr. 1 PolG NW 및 § 9 Abs. 1 HmbDVPolG 참조.

87) § 17 Abs. 1 Nr. 1 PolG NW. 유사한 규정으로는 § 10 Abs. 1 HmbDVPolG 참조.

88) § 18 Abs. 1 Nr. 1 PolG NW. 유사한 규정으로는 § 10 Abs. 1 HmbDVPolG 참조.

89) § 19 Abs. 1 Nr. 1 PolG NW. 유사한 규정으로는 § 11 Abs. 1 HmbDVPolG 참조.

90) § 20 Abs. 1 Nr. 1 PolG NW, § 12 Abs. 1 HmbDVPolG.

91) § 28 Abs. 4 S. 1 SPolG.

92) § 34 Abs. 2 ThürPAG.

(바) 컴퓨터에 의한 인적 자료의 검색·조사

‘통일경찰법모범초안에 대한 개정초안’과 마찬가지로 주의 새로운 경찰법에서는 위험 방지의 목적을 위한 컴퓨터에 의한 인적 자료의 검색·조사(Rasterfahndung)⁹³⁾에 대하여 규정하고 있다.⁹⁴⁾ 그에 의하면 컴퓨터에 의한 인적 자료의 검색·조사는 연방과 주의 존립 또는 안전, 사람의 생명·신체 또는 자유에 대한 현존하는 위험을 방지하기 위하여서만 허용된다. ‘현존하는 위험’(gegenwärtige Gefahr)이란 관련된 법익에 대한 위험이 이미 발생한 것을 의미한다. 신체에 대한 중대한 위험이 존재하여야 하고, 약간의 신체에 대한 손상이 예견되는 것으로는 충분하지 않다.

컴퓨터에 의한 인적 자료의 검색·조사는 그 자체가 적합한 수단인 경우에만 위험방지를 위한 조치로서 고려될 수 있다. 따라서 현존하는 위험이 존재하는 경우에 있어서도 특별히 예외적인 경우에만 생각해 볼 수 있다. 정보를 조달하고 그를 활용하는 것은 현대적 정보처리기술을 사용한다고 하더라도 시간을 요하는 것이다. 극히 예외적인 경우에만 컴퓨터에 의한 인적 자료의 검색·조사는 해석의 필요 없이 바로 활용할 수 있는 결과물, 예컨대 경찰책임자에 대한 정보를 제공한다. 통상적으로 컴퓨터에 의한 인적 자료의 검색·조사에 의한 정보는 또 다른 조사를 필요로 하게 된다. 결국 실제에 있어서 컴퓨터에 의한 인적 자료의 검색·조사가 위에 언급한 법익에 대한 현존하는 위험을 방지하기 위한 적합한 수단인 경우란 극히 제한적일 것이다. 예컨대 인질극과 같이 위험이 장시간 계속되는 경우를 생각해 볼 수 있을 것이나, 이러한 경우에는 이미 범죄수사가 시작될 것이다.

여하튼 요건을 충족하는 경우 사법경찰은 다른 정보와 비교·조사하기 위하여 공적 또는 사적 기관, 즉 모든 저장기관에게 일정한 인적 그룹의 개인관련 정보의 제공을 요구할 수 있다. 정보파일 내지 모든 정보자료의 제공을 요구하는 것이 아니라 특정한 인적 그룹에 대한 정보를 요구하는 것이다. 예를 들면 일정한 징표에 의하여 그룹 지워지는 사람들에 대한 정보를 요구하는 것이다. 이 경우 징표는 정보를 요구하는 측에서 제

93) 컴퓨터에 의한 인적 자료의 검색·조사에 대하여는 Siebrecht, Rasterfahndung, 1997 참조.

94) § 10f VE ME PolG, § 31 PolG NW, § 26 HSOG, § 37 SPolG, § 44 ThürPAG, § 47 SächsPolG, § 40 PolG BW, § 23 HmbDVPolG 등 참조.

시하여야 한다.⁹⁵⁾

그에 따라 정보를 요구받은 기관은 제공할 자료를 추려내야 한다. 이를 위하여 제공하는 기관은 경찰에게 컴퓨터에 의한 인적 자료의 검색·조사를 위하여 필요한 범위를 넘어서 정보가 제공되는 것을 막기 위하여 필요하다면 독자적인 평가를 해야 한다. 기술적인 어려움 때문에 적정한 시간·비용으로는 그것이 불가능한 예외적인 경우에는 요청 받은 정보보다 많은 것을 제공하는 것이 허용된다. 전자정보처리기술의 발전 및 편리함과 관련하여 저장기관은 통상적으로 경찰에게 필요한 정보를 발췌할 수 있는 프로그램을 사용할 수 있을 것이다. 이렇게 하여 제공된 정보는 다른 정보자료와 비교하는 데 사용하는 것이 허용된다. 비교할 정보자료가 수작업에 의하여 이루어진 경우에는 비교·조사가 반드시 자동장치에 의하여 행해져야 하는 것은 아니다.

컴퓨터에 의한 인적 자료의 검색·조사의 목적은 위험방지이다. 위험방지의 목적이 달성되었거나 달성될 수 없음이 밝혀진 경우에는 제공된 정보와 컴퓨터에 의한 검색·조사에 의하여 획득된 정보는 삭제되어야 한다. 몇몇 주의 경찰법에서는 사안과 관련하여 필요하지 않은 자료(Unterlage)는 반환하거나 파기하여야 한다고 규정하고 있다.⁹⁶⁾ 여기서 '자료'라고 함은 통상적으로 정보가 저장되어 있는 정보함(Datenträger)일 것이다. 삭제의무는 우선 제공된 정보가 저장되어 있는 정보함을 대상으로 할 것이다. 그밖에 컴퓨터에 의한 검색·조사에 의하여 생성된 정보함도 '자료'로서 반환되거나 파기되어야 한다. 그러나 컴퓨터에 의한 검색·조사에 의하여 생성된 정보자료가 포함된 정보함을 반환하는 것은 생성된 정보가 완전히 삭제된 후에야 생각해 볼 수 있는 것이다. 그렇지 않다면 저장기관에게 허용되지 않는 정보제공이 행해지는 결과가 되기 때문이다.

'자료'의 파기는 그것이 사안과 관련된 다른 절차를 위하여 필요한 경우에는 행해지지 않을 수 있다. 그러나 이 경우에 당초의 사안과 내용적 관련성이 있어야 한다. 단지 외형상의 관련성만으로 정보를 다른 절차를 위하여 사용하는 것은 배제된다. 컴퓨터에 의한 검색·조사를 하게된 당초의 사안과 관련된 형사절차의 경우가 그에 해당하는 가장 전형적인 예일 것이다.⁹⁷⁾ 당초의 사안과 아무런 관련이 없는 형사절차는 내용적 관련성

95) § 37 Abs. 2 SPolG, § 26 Abs. 2 HSOG, § 23 Abs. 2 HmbDVPolG, Art. 28p Abs. 1 BayPAG 참조.

96) 예를 들면 § 26 Abs. 3 HSOG 참조.

이 없는 것이다.

(사) 위험방지에 대비하기 위한 정보수집

몇몇 주의 경찰법에서는 위험방지의 경우에 대비하기 위하여 정보를 수집할 수 있음을 규정하고 있다.⁹⁸⁾ 이러한 경우 정보수집의 시점에 구체적인 위험이 존재해야 하는 것은 아니다.⁹⁹⁾ 이 규정으로부터 그의 적용영역 이외에서는 구체적인 위험이 존재하지 않는 한 정보수집이 허용되지 않는다는 결론을 도출할 수 있다.

위험방지에 대비하기 위하여 우선 위험방지를 위하여 특별한 지식과 능력을 가지고 있는 사람에 대한 정보가 수집될 수 있다. 경찰 스스로 가지고 있지 않거나 또는 교육 및 장비에 의하여 갖추어 줄 수 없는 지식과 능력만이 고려될 수 있다. 그밖에 합리적인 평가 및 신중한 예측에 의할 때 위험방지를 위한 경찰작용을 위하여 필요한 것으로 판단되는 지식과 능력이어야 한다. 예를 들면 경찰은 외과의사 또는 다른 전문가에 대한 정보가 필요한 것은 아니다. 그것은 전문의를 보유하고 있는 병원의 일인 것이다.

그 이외에 중대한 위험이 발생할 수 있는 시설의 책임자 및 위험에 처한 시설의 책임자에 대한 정보가 수집될 수 있다. 위험이 발생한 경우에 직접적인 책임자와의 협력이 필요한 것이기 때문에 그에 대한 정보의 수집만이 고려된다.¹⁰⁰⁾ 옥외집회 또는 시위의 주최자에 대한 정보도 포함될 수 있다. 그러나 이러한 사람에 대한 정보는 늦어도 수집의 필요가 없어진 후 1달 이내에 삭제되어야 한다. 그러한 정보는 표현의 자유와 집회의 자유에 관련되기 때문에 특히 민감한 정보에 해당한다.¹⁰¹⁾ 그러한 정보를 다른 기관에 제공하는 것, 예를 들면 다른 정보기관에 제공하는 것은 배제된다.¹⁰²⁾

이름, 주소 등 개인신상명세에 관한 정보, 연락처 및 위에 언급한 인적 그룹에 속하는 것에 대한 자세한 사항 등이 수집된다. 정보는 행정기관으로부터 수집되거나, 관련자 또

97) Art. 28p BayPAG는 명문으로 모든 형사절차를 위하여 정보의 사용을 허용하고 있다.

98) 예를 들면 § 11 PolG NW.

99) 이에 대하여 비판적인 생각으로는 Liskén, ZRP 1990, 15 (17) 참조.

100) § 26 Abs. 3 SPolG 참조.

101) Bäumlér, JZ 1986, 469 ff.

102) 자르란트에서는 § 26 Abs. 3 S. 1 SPolG의 규정으로부터 그러한 결론이 도출될 수 있다. 그러나 지금까지 경찰의 실무는 이에 따르지 않고 있다.

는 제3자로부터 자유로운 진술에 의하는 등 일반적으로 접근 가능한 정보원으로부터 수집되어야 한다. 은밀한 정보수집 또는 특별한 수단의 사용에 의한 정보수집은 배제된다.¹⁰³⁾ 수집의 목적은 위험방지에 대비하기 위함이다. 따라서 정보의 사용은 그러한 목적에 한정된다.

2. 경찰에 의한 정보의 처리: 정보의 저장, 수정, 이용

경찰은 경찰목적에 위하여 수집한 정보가 경찰직무의 수행을 위하여 필요한 경우에만 저장하고 수정하고 이용할 수 있다. 이 경우에 적법하게 수집된 정보만이 문제됨은 당연하다.

(1) 정보의 저장

(가) 개념정의

정보저장이란 계속적인 사용을 목적으로 정보함(Datenträger)에 정보를 편입, 복사하거나 보관하는 것을 말한다. 정보함은 메모지, 문서, 디스켓, 테이프 등 그 형태를 불문한다. 저장된 정보에의 접근이 용이하나 또는 어려우냐는 중요하지 않다. 입법자는 경찰이 정보를 저장하기 위한 조건을 규율하여야 하는데, 그 경우에 있어서 저장된 정보에의 접근가능성 및 이용가능성에 따라 규율밀도를 달리하여야 한다. 정보가 전통적인 방법에 의하여 저장되는지 또는 자동화 절차에 의하여 저장되는지는 중요한 의미를 가진다. 컴퓨터 기술의 발전은 정보의 전달가능성을 확대하였다. 자동화는 단지 지금까지의 현대적 수단에 의한 정보처리기술의 발전을 의미하는 것이 아니라, 완전히 새롭고 특별한 정보의 이용가능성·사용가능성을 가져왔다. 이것은 정보의 자기결정권에 대한 새로운 위협을 의미하므로, 입법자는 이에 대한 법적 조치를 마련하여야 한다. 새로운 기술의 도입은 보호조치와 함께 고려되어야 한다.

103) 이를 명문으로 규정한 것으로는 § 31 Abs. 3 NGefAG.

(나) 법적 근거로서의 개괄적 수권조항

경찰법상 개괄적 수권조항은 위협방지 영역에서 개인정보의 저장에 대한 보충적인 법적 근거로서 고려될 수 있다. 경찰책임자에 대한 정보만이 대상이 되고, 비책임자의 경우에는 일반 경찰법상 비책임자에게 경찰권을 발동하기 위한 요건과 동일한 요건을 충족한 경우에만 허용될 수 있다.¹⁰⁴⁾ 그 이외에 공공의 안전에 대한 구체적인 위협이 존재해야 한다. 위협이 제거되었다면 개괄적 수권조항은 정보의 저장과 같은 그 밖의 조치에 대한 법적 근거가 될 수 없다. 따라서 개괄적 수권조항은 위협이 존재하는 동안, 즉 일시적인 정보저장의 법적 근거가 될 수 있을 뿐이다.

(다) 특별한 법적 근거

‘통일경찰법모범초안에 대한 개정초안’과 주의 새로운 경찰법은 경찰에게 직무의 수행을 위하여 필요한 경우에 개인정보의 저장·수정·이용에 관한 권한을 일반조항의 형식으로 수권하고 있다.¹⁰⁵⁾ 그에 의하면 경찰은 직무수행을 위하여 필요한 경우에는 개인정보를 서류 또는 정보파일에 저장하거나 수정 또는 이용할 수 있다. 위협방지 영역에서 그 조항에 의하여 일반적인 개괄적 수권조항에서 보다 더 광범위한 권한이 부여되는 것은 아니다. 위협이 제거되었고 새로운 구체적인 위협이 아직 발생하지 않은 경우에는 위협방지의 목적을 위한 저장의 필요성은 부인된다. 그와 같은 경우 저장을 계속 유지할 권한은 존재하지 않게 된다. 경찰법에서 규정하고 있는 심사기간(통상적으로 10년)은 그 만료 후 정보저장을 심사해야 하는 시간적 한계를 의미한다. 경찰법은 필요성에 대하여 개념정의를 하고 있지 않다. 정보가 더 이상 필요하지 않다면 심사기간이 만료하기 전이라도 정보는 삭제되어야 한다.¹⁰⁶⁾

104) 경찰법상 비책임자에게 경찰권을 발동하기 위한 요건에 대하여는 서정범 역, 독일경찰법론, 1998, 173쪽 아래 참조.

105) § 10a Abs. 1 VE Me PolG, § 30 Abs. 1 SPolG, § 24 Abs. 1, Abs. 2 S. 1 PolG NW, § 20 Abs. 1 HSOG, § 16 Abs. 1 HmbDVPolG, Art. 28i Abs. 1 BayPAG 참조.

106) 예를 들면 § 38 Abs. 2 Nr. 2 SPolG, § 27 Abs. 2 Nr. 2 HSOG 참조.

(2) 정보의 수정

정보의 수정이란 저장된 정보를 내용적으로 재구성하는 것을 의미한다.¹⁰⁷⁾ 정보의 내용을 수정하는 것이 중요하다. 단지 표현방식을 바꾸는 것은 수정에 해당하지 않는다. 저장된 정보를 재구성하는 것뿐만 아니라 정보에 새로운 의미가 부여되는 것도 수정에 해당한다. 예를 들면 행정목적으로 저장되었는데 그 후 혐의정보로 사용되는 경우에 개별적인 정보상의 문장은 바뀌지 않았을지라도 정보보호법상 중요한 수정에 해당하는 것이다. 또한 수합된 정보의 표제어를 바꾸는 것 자체가 수정에 해당할 수도 있는 것이다.

일반적인 정보보호법에 의하면 수정은 정보보호법 또는 다른 법규정에서 허용하고 있거나 관련자가 동의하는 경우에만 가능하다.¹⁰⁸⁾ 따라서 저장된 정보의 수정요건에 대하여 경찰법에서 규율하고 있는지가 중요하다.¹⁰⁹⁾

(3) 정보의 이용

정보의 이용은 전통적인 정보처리의 단계(수집, 저장, 수정 등) 이외의 개인정보의 모든 사용을 말한다. 정보보호법에 수집에 대한 규정이 포함됨으로써 이용에 해당하는 영역은 더 좁아졌다. 여기에 덧붙여 새로운 주의 경찰법은 정보의 비교조사(Datenabgleich)와 같은 정보이용의 중요한 형태를 명문으로 규율하고 있다. 이용 또한 적법한 직무수행을 위하여서만 허용된다.

(가) 정보이용과 목적 구속성

‘통일경찰법모범초안에 대한 개정초안’과 주의 경찰법에는 목적구속에 관한 규정을 두고 있다. 목적구속의 원칙에 의하면 개인정보는 그것이 수집된 목적으로만 이용되거나 사용되어야 한다. 개인의 자유로운 인격의 발현을 위하여서는 자신으로부터 수집된 개인

107) 연방정보보호법 제3조 5항 2호 참조.

108) 연방정보보호법 제4조, 제14조 참조.

109) 이에 대하여는 § 30 Abs. 1 SPolG, § 20 Abs. 1 HSOG, § 24 Abs. 1 PolGNW, Art. 28i Abs. 1 BayPAG 참조.

정보가 어떠한 목적으로 사용되는지에 대하여 알 수 있어야 하는데, 이것은 수집목적과 사용목적이 동일한 경우에만 가능하게 된다.

그러나 목적구속의 원칙은 광범위한 예외의 인정에 의하여 그의 본질적인 효력이 많이 상실되고 있다.¹¹⁰⁾ 위험방지를 위하여 수집된 정보는 그 정보가 경찰의 다른 직무를 위하여 수집될 수 있었던 것이라면 그 직무수행을 위하여 사용될 수 있다. 이와 관련하여 각각 특별한 요건을 충족하고 있는 한, 위험방지를 위하여 수집한 정보를 범죄수사 또는 예방적 범죄투쟁의 목적으로 사용하는 것을 우선적으로 생각해 볼 수 있다.

(나) 정보의 비교조사

정보의 비교조사(Datenabgleich)란 특정인에 대한 개인관련 사항이 경찰의 정보파일¹¹¹⁾에 저장되어 있는지를 다른 정보파일에서 특정인의 징표를 가지고 찾는 것을 말한다. '통일경찰법모범초안에 대한 개정초안' 및 모든 주의 경찰법은 정보의 비교조사에 대하여 규정하고 있는데, 그에 의하면 경찰은 다른 기관(또는 제3자)에게 정보를 요구하고 이들 정보 사이에 또는 자신이 갖고 있는 정보와 예컨대 나이, 국적, 거주지 등의 검색어에 따라 비교조사 할 수 있다. 이러한 조치에 의하여 아무런 혐의가 없는 사람의 정보에도 관련되게 되는데, 이것은 정보의 자기결정권에 대한 중대한 침해를 의미하므로 정보의 비교조사는 법에 규정된 요건¹¹²⁾이 충족되는 경우에만 허용될 수 있는 것이다.

정보의 비교조사에 관한 통일경찰법모범초안에 대한 개정초안' 및 주의 경찰법 규정에서는 그 목적에 대하여 특별히 규율하고 있지 않다. 따라서 일반적인 목적구속에 관한 조항이 그대로 적용된다. 그에 따라 위험방지 영역에서 수집되고 저장된 정보는 위험방지의 목적을 위하여서만 정보의 비교조사의 대상이 될 수 있다. 범죄수사 또는 예방적 범죄투쟁을 위한 정보의 비교조사는 정보가 이러한 목적을 위하여 수집될 수 있었을 경우에만 허용된다. 여러 종류의 정보가 모여 있는 경우에 저장된 개별 정보 각각에 대하

110) § 10a Abs. 2 S. 2, Abs. 3, Abs. 4 und § 10b VE ME PolG.

111) 정보파일이란 특별한 징표에 의하여 자동화된 절차에 의하여 이용될 수 있는 개인정보의 모음을 말한다. 수작업에 의한 정보파일은 동종으로 분류되고 특별한 징표에 의하여 정리되고 재편되며 이용될 수 있는 그 밖의 모든 개인정보의 모음을 말한다.

112) 정보의 비교조사의 요건에 대하여는 § 10f VE ME PolG.

여 위의 요건이 충족되어 있지 않다면, 범죄수사의 목적을 위하여 위험방지의 목적으로 모아진 정보의 묶음과 비교조사 하는 것은 배제된다.

3. 정보의 제공

(1) 정보제공의 의의

정보제공이란 저장되거나 정보처리에 의하여 직접적으로 얻어진 정보를 제3자에게 저장기관이 제공하거나 열람할 수 있도록 함으로써 알려주는 것을 말한다. 정보제공의 형태는 불문한다. 구두로 알려주거나 문서에 의하여 제공하는 것 그리고 전자장치에 의하여 알리는 것 등은 모두 정보제공에 해당한다. 중요한 것은 저장기관이 아닌 제3자에게 새로운 문맥으로(in einen neuen Kontext) 정보가 알려진다는 데 있다.

누가 제3자에 해당하는지의 문제는 저장기관과의 구별에 의하여 결정된다. 정보제공의 여부를 판단함에 있어서는 제공자와 제공받는 자가 수행하는 직무가 중요한 기준이 되며, 보충적으로 조직법적 요소를 고려하여야 한다. 우선 하나의 행정청 내에서 상이한 직무를 수행하는 기관 사이에 정보를 교환하는 것은 정보제공에 해당한다. 또한 각각 저장기관이 되는 독립된 행정청 사이에 정보를 제공하는 경우에는 각 기관이 동일한 직무를 수행한다 하더라도 정보제공에 해당한다고 보아야 한다.

그렇다면 우선 경찰과 관련하여 직무의 동일성과 상이성에 대한 판단이 문제되는데, 경찰이 사법기관으로서 활동하는 범죄수사와 경찰의 고유한 업무인 위험방지 사이에는 직무의 상이성이 존재하는 데에 의문의 여지가 없다. 그밖에 정보가 각각의 업무분야 내에서 부분영역으로 나누어 특별한 법적 규정에 의하여 처리되는지에 따라 직무를 나눌 수 있을 것이다. 예를 들면 특별히 중대한 위험을 방지하기 위하여 특별한 정보수집 방법이 허용되는 경우, 저장기관이 획득된 정보를 다른 기관(동일한 행정청 내도 포함)에 일반적 위험방지의 목적으로 제공하는 것도 정보제공이라고 볼 수 있다.

범죄수사에 있어서도 동일한 내용이 적용된다. 즉 특별한 범죄행위를 밝혀내기 위하여 특별한 정보처리 권한이 수권되어 있는 경우, 그에 의하여 획득된 정보를 다른 기관에 일반적인 범죄수사를 위하여 제공하는 것은 정보제공에 해당한다고 볼 수 있다.

(2) 법적 근거 및 목적구속의 원칙

정보제공은 수집되거나 저장된 정보를 다른 공적 기관 또는 제3자에게 전달하는 것을 말하므로, 이에 의하여 정보수집에 의한 침해는 더욱 심화될 것이다.¹¹³⁾ 직무원조에 관한 규정은 경찰상의 정보를 다른 기관에 제공함에 있어서 발생하는 정보의 자기결정권에 대한 침해의 법적 근거가 될 수 없기 때문에,¹¹⁴⁾ '통일경찰법모범초안에 대한 개정초안'과 주의 경찰법에서는 정보제공에 관한 권한을 명문으로 수권하고 있다.

정보제공에 있어서도 정보보호법상의 목적구속의 원칙이 적용된다. 그에 따라 개인정보는 제공기관의 측면에서 볼 때 그것이 수집되거나 저장된 목적을 위하여만 제공되어야 하며, 제공받는 자 또한 그에게 제공된 목적을 위하여만 제공된 개인정보를 이용하여야 한다. 이러한 정보의 제공과 관련된 목적구속의 원칙은 '통일경찰법모범초안에 대한 개정초안' 제10c조 1항 2문, 제5항 1문 및 제9항에 규정되어 있다. 그러나 이 원칙 또한 조기의 그리고 효과적인 위협방지를 보장하기 위하여 많은 예외가 인정되고 있다. 그밖에 경찰행정청에 저장되어 있는 정보에 다른 행정청이나 제3자가 접근하는 경우에 있어서는 다른 경찰행정청이 접근하는 경우에 비하여 더욱 엄격한 요건을 충족하여야 할 것이다.

(3) 온라인 연결

'통일경찰법모범초안에 대한 개정초안' 제10d조는 자동화된 검색절차(Abrufverfahren)의 도입, 즉 온라인 연결의 법적 근거가 된다. 그에 의하면 경찰행정청 또는 사법경찰기관 사이에 내무부의 승인을 얻어 온라인 연결이 허용된다. 온라인 연결은 제공기관의 책임이 완전히 배제되고 다른 기관이 정보를 아무 제한 없이 접근할 수 있다는 점에서 정보의 제공과 차이가 있다. 이러한 점에서 자동화된 검색절차의 허용을 위하여서는 엄격한 요건이 필요하게 된다.¹¹⁵⁾

113) 정보제공에 있어서 기본권 보호에 대하여는 Scholler/Schloer, Grundzüge des Polizei- und Ordnungsrechts in der Bundesrepublik Deutschland, 4. Aufl., 1993, S. 194 ff.

114) 이에 대하여는 Schenke, Polizei- und Ordnungsrecht, in: Steiner(Hrsg.), Besonderes Verwaltungsrecht, 6. Aufl., 1999, Rdn. 129; Siebrecht, JZ 1996, 711 ff. 참조.

몇몇 새로운 주의 경찰법은 개괄적·일반적 조항의 형식으로 자동화된 검색절차의 도입에 관한 규정을 두고 있는데, 자르란트와 헤센의 경찰법에는 경찰상 정보의 온라인에 의한 제공에 대하여 규정하고 있을 뿐이다. 또한 바이에른의 경우에도 단지 관련자의 보호가치 있는 이익을 고려하고 경찰직무의 수행을 위하여 적합하다면 자동화된 절차를 도입할 수 있다고 규정하고 있을 뿐이다. 다른 행정관청에 저장되어 있는 정보를 경찰이 온라인에 의하여 검색할 수 있는 방법을 도입하는 것은 그에 대한 구체적인 법적 근거가 있는 경우에만 허용된다. 그렇지 않다면 개인은 자기에 관한 정보가 어디로 흘러들어 가게 되는지를 추적할 수 없게 되기 때문이다.

경찰관청 사이에 자동화된 검색절차를 도입하는 것은 동일한 직무의 경우에 고려될 수 있다. 물론 직무의 동일성이 인정된다고 하여 바로 그 절차의 도입이 적합하다고 할 수는 없다. 자동화된 검색절차에 있어서는 검색의 시점에 정보제공의 요건이 충족되어 있는지가 심사될 수 없다는 점이 고려되어야 한다. 따라서 검색절차에 올려진 모든 정보는 제공에 적합하여야 하고,¹¹⁵⁾ 제공을 위한 요건을 충족하여야만 한다.

4. 정보의 정정, 삭제, 차단

정보보호법과 새로운 주의 경찰법에서는 개인정보가 잘못 저장되어 있는 경우에 관련자에게 정보의 정정청구권을 부여하고 있으며, 차단과 삭제의 요건이 충족되는 경우에 차단 및 삭제청구권을 인정하고 있다.¹¹⁷⁾ 이러한 권리는 소송상 주장할 수 있다.

115) 이에 대하여 비판적인 견해로는 Riegel, DÖV 1994, 814 (818).

116) 적합성에 대한 판단기준으로는 ① 단지 혐의가 있다는 정도의 정보에 해당하느냐 또는 확증된 정보에 해당하느냐의 문제, ② 혐의자에 관한 정보인지 또는 그 이외의 사람에 관한 정보인지의 문제(후자의 경우 더 엄격한 기준이 적용되어야 한다), ③ 단순한 신상명세에 관한 정보인지 또는 개인의 사생활에 관한 정보인지의 문제, ④ 정보의 내용에 의할 때 정보를 제공받은 자가 다른 보충적인 정보 없이도 제공된 정보에 기초하여 결정을 내릴 수 있는 위험이 존재하는지 여부, ⑤ 중대하지 않은 범죄에 관련되고 그에 대하여 초지역적이고 전국적인 접근이 적절하지 않다고 판단되는지 여부, ⑥ 검색 및 그 밖의 정보사용을 사후에 충분히 심사할 수 있는지 여부 및 ⑦ 권한 없는 자에 의한 접근이 배제되는지 여부 등이 고려될 수 있다(이에 대하여는 § 24 Abs. 3 HSOG 참조).

117) 연방정보보호법 제6조, 제20조 참조.

차단이란 저장된 정보의 처리를 저지하는 것을 말한다. 연방정보보호법 제3조 5항 4호에서는 차단이란 저장된 개인정보에 대하여 그의 처리 또는 이용을 제한하기 위한 표시를 말한다고 규정하고 있다. 개인정보는 특히 관련자로부터 그의 정확성에 대한 이의제기가 있고 그의 정확성 내지 부정확성에 대하여 확정할 수 없는 경우에 차단되어야 한다.¹¹⁸⁾

새로운 주의 경찰법에서는 보호할 가치 있는 개인의 이익을 위하여 삭제될 수 없는 경우, 입증의 어려움을 해소하기 위하여 정보가 필요하기 때문에 또는 학술적 목적을 위하여 정보가 이용되어야 하기 때문에 삭제될 수 없는 경우에만 차단이 고려된다고 규정하고 있다.¹¹⁹⁾ 그렇다면 일반적인 정보보호법상의 차단사유, 즉 정보의 정확성에 대하여 관련자가 이의제기를 하고 그의 정확성 내지 부정확성에 대하여 확정할 수 없다는 요건은 경찰영역에서 배제되는지는 의문이다. 새로운 주의 경찰법은 차단을 단지 삭제에 대한 대안으로서 고려하는 것을 규정하고 있을 뿐이므로 그러한 해석은 타당하지 않다.

이와 관련하여 범죄행위의 예방적 투쟁을 위하여 정보를 저장함에 있어서 어려운 문제가 나타난다. 예컨대 혐의자가 자신의 행위와 혐의정보의 정확성에 대하여 이의를 제기하고 그것이 증명될 수 없는 경우에, 그 정보가 차단되어야 하는지 의문이다. 일반적으로 조사가 진행 중인 경우에는 혐의자가 그 사실에 대하여 교지 받지 못하므로 저장된 정보의 정확성에 대하여 이의를 제기할 수 없다. 정보의 정확성에 대하여 이의를 제기한다고 하더라도, 그에 대하여는 조사가 종결된 후에야 비로소 판단될 수 있는 것이다. 조사가 종결된 후에 관련자의 혐의가 벗겨지지도 않고 그렇다고 그의 행위를 입증할 수도 없는 경우에는 차단의 청구권이 발생할 수 있을 것이다. 이것은 관련 정보가 더 이상 제공되어서는 안 된다는 것을 의미한다.

연방정보보호법과 주의 법률에서 규정하고 있는 또 다른 차단사유는 정보가 직무수행을 위하여 더 이상 필요 없게 된 경우이다. 이는 경찰은 - 그것이 차단되었든 차단되지 않았든 관계없이 - 적법한 직무수행을 위하여 필요한 정보만을 저장하여야 한다는 원칙과 일맥상통하는 것이다. 정보를 계속 저장하면서 차단하는 것이 관련자의 이익을 위한 것이 아니라면, 경찰의 직무수행을 위하여 더 이상 필요 없게 된 정보는 삭제되어야 한다.

118) 연방정보보호법 제20조 4항 참조.

119) § 38 Abs. 4 SPolG, § 32 Abs. 5 PolG NW, § 27 Abs. 6 HSOG.

삭제는 저장된 정보를 알아볼 수 없도록 만드는 것이다.¹²⁰⁾ 삭제는 정보함을 파기하거나 또는 개별적인 경우 연결을 끊는 것에 의하여 행해질 수 있다. 중요한 것은 저장기관이 정보의 내용을 더 이상 인식할 수 없게 된다는 데 있다. 단지 정보에의 접근이 '통상적인 경우' 더 이상 행해질 수 없다거나 또는 극히 제한적으로 가능하게 된 것만으로는 충분하지 않다. 새로운 인식가능성이 완전히 배제되어야 한다.

정보삭제의 경우 삭제된 정보의 기초가 된 자료들도 함께 파기하여야 한다. 이와 관련하여 여러 사람의 자료가 모여 이루어진 서류에 있어서 정보가 삭제되는 자 이외의 다른 사람에 대한 정보가 삭제되지 않는 경우에 어떻게 처리할 것인가가 실무상 문제된다. 다른 사람의 정보와 구분하기 곤란하거나 또는 먹칠 등의 방법에 의하여 알아볼 수 없도록 하기 어려운 경우에는 정보가 삭제된 자의 인격권에 대한 침해를 방지하기 위하여 서류상으로 그에 대한 정보를 차단하거나 특별한 표기를 하여 계속적인 사용을 금지시켜야 한다.

정정과 차단은 경찰 정보처리의 실무상 그다지 큰 의미를 갖지 못한다. 동일인 여부를 확인하는 데 사용하는 개인정보에 있어서 정정청구는 저장기관 자신의 이해에 속하는 것으로 따로 보장될 필요는 없다. 부담적인 물적 정보가 잘못된 경우, 그것은 신청에 의하여 삭제될 수 있다. 관련자의 신청에 의한 물적 정보의 정정은 극히 제한적인 경우에만 고려될 것이다. 실제에 있어서 의미 있는 것은, 경찰이 범죄예방을 위하여 유죄판결이 아닌 무죄판결 또는 공소기각의 재판에 의하여 종결된 조사절차에 의하여 획득한 정보를 법원으로부터 넘겨받아 저장하려는 경우에 있어서 차단을 청구하는 것이다. 새로운 정보보호법에 의하면 이러한 경우, 특히 법원에 의한 조사과정에서 관련자가 자기의 혐의를 다투는 경우에 정보는 관련자의 신청이 있어야만 비로소 차단되는 것이 아니라, 직권에 의하여 차단되어야 한다.¹²¹⁾ 삭제의 경우도 마찬가지이다. 관련자의 신청이 없더라도 삭제의 요건이 충족되는 경우에 정보는 삭제되어야 한다. 언제 정보가 삭제되어야 하는가는 개별 영역별로 특별법에 의하여 정해진다. 적법한 직무수행을 위하여 정보가 더 이상 필요하지 않게 되는 경우에 대하여 모든 분야를 총괄하여 규정할 수는 없다.

120) 연방정보보호법 제3조 5항 5호 참조.

121) 연방정보보호법 제20조 4항 참조.

개별영역별로 규정되어야 하며, 구체적인 결정에 의하여 확정되어야 한다.

5. 고지청구권

고지청구권 또는 정보제공청구권(Auskunftsanspruch)은 내용적으로 정보의 저장 여부뿐만 아니라 어떠한 정보가, 어떠한 물적 관련성으로, 어떠한 목적으로 저장되는지에 대하여도 알려줄 것을 요구하는 것이다.¹²²⁾ 그밖에 정보의 출처 및 제공받는 자에 대한 고지도 포함한다.

고지의 신청에 있어서 특별한 이유를 제시해야 하는 것은 아니다. 통상적으로 관련 행정기관이 정보의 모음에서 쉽게 찾을 수 있도록 보충적인 정보를 주는 것은 고지를 받음에 있어서 도움을 줄 것이다. 그러나 그를 위하여 제시된 내용은 전적으로 고지청구에 대한 처리의 목적으로만 사용되어야 한다. 고지청구에 있어서 주장된 내용이 경찰정보에 저장된다고 한다면, 그것은 고지청구를 주저하게 되는 결과를 가져올 것이다.

새로운 경찰법¹²³⁾ 및 정보보호법에 의하면 경찰행정청은 더 이상 고지의무로부터 일반적으로 면제되지 않는다. 개별적인 경우에 있어서 거부요건이 존재하는 경우에 한하여 고지를 거부할 수 있다. 고지에 의하여 적법한 직무수행이 곤란해질 경우에는 고지를 거부할 수 있다. 그러나 고지의 신청이 너무 많다는 것만으로는 거부할 수 없다. 예를 들면 고지함으로써 진행중인 조사의 상황이 공개되고 그로 말미암아 증거인멸의 위험이 발생하게 된다면 고지가 거부될 수 있다. 또한 공공의 안전에 대한 위험 또는 연방·주의 복리에 대한 위험이 존재하는 경우에 고지가 거부될 수 있는데, 위험의 존재 여부는 헌법 합치적이고 제한적인 해석을 요한다. 개별적인 경우 위험이 발생할 것이라는 구체

122) § 40 Abs. 1 SPolG, § 29 Abs. 1 HSOG, § 18 Abs. 1 PolG NW 참조.

123) 몇몇 주의 새로운 경찰법(§ 29 HSOG, Art. 28t BayPAG 등)에서는 관련자의 고지청구권에 대하여 규정하고 있다. 다만 그 내용은 일반적인 정보보호법의 규정과 크게 다르지 않다. § 25 HmbDVPolG은 명문으로 § 18 HbgDSG의 일반적인 고지청구권이 적용된다고 밝히고 있다. 따라서 경찰법에서 고지에 관한 특별규정을 두고 있지 않더라도 결과에 있어서 차이가 있는 것은 아니다. 이에 대하여는 Knemeyer, Polizei- und Ordnungsrecht, 7. Aufl., S. 110 참조. '통일경찰법 모범초안에 대한 개정초안' 및 노르트라인-베스트팔렌과 니더작센의 경찰법은 고지에 관한 규정을 두고 있지 않다. 이러한 경우 일반적인 정보보호법의 규정이 적용될 것이다.

적인 사실이 존재해야 한다.

실제에 있어서 중요한 의미가 있는 것은 정보가 법령에 따라 또는 그 본질에 있어서 제3자의 이익을 위하여 비밀 유지되어야 하기 때문에 고지가 거부되는 경우이다.¹²⁴⁾ 예를 들면 고발자, 정보제공자 또는 증인에 대한 정보가 문제되는 경우, 그에 대한 고지는 그들의 권리를 위협하게 할 수 있는 것이다.¹²⁵⁾ 이와 같은 경우에 고지청구자의 이익과 비교형량이 필요하다.¹²⁶⁾

고지청구에 대한 결정은 통상적으로 전부 긍정 또는 전부 부정과 같이 일도양단적이지 않다. 고지는 비밀 유지에 대한 이익을 위하여 필요한 범위 내에서만 거부될 수 있는 것이다. 고지를 할 것인지 또는 거부할 것인지에 대한 결정은 개별적인 경우 저장된 정보의 내용에 따라 다르게 내려질 수 있고 또한 경우에 따라서는 그것이 요구된다.

고지를 거부하는 경우에는 그 이유를 제시하는 것이 고지거부의 목적을 달성을 할 수 없게 만드는 것이 아닌 한,¹²⁷⁾ 그 이유를 제시하여야 한다.¹²⁸⁾ 고지가 거부된 경우에 관련자는 정보보호관리인¹²⁹⁾에게 요청하여 정보저장의 적법성에 대하여 심사하게 할 수 있다.¹³⁰⁾

124) 예를 들면 § 29 Abs. 3 HSOG.

125) 예를 들면 § 19 Abs. 4 BDSG, § 40 Abs. 2 SPolG, Art. 28t Abs. 2 BayPAG 참조.

126) 이에 대하여는 BayVGH, DuD 1988, 581 ff. 참조.

127) § 29 Abs. 4 HSOG, § 40 Abs. 3 S. 1 SPolG.

128) 경찰에게 이유제시의무로부터 일반적 면제를 허용하고 있는 Art. 28t Abs. 3 S. 1 BayPAG는 기본법 제19조 4항에 반하는 것이다. 공권력 주체의 이유제시의무에 대하여는 BVerfGE 6, 32 (44) 참조.

129) 공적 영역에서의 정보보호관리인(Datenschutzbeauftragter)은 공공기관이 정보보호법상의 규정을 준수하는지에 대하여 감독하는 것을 주 임무로 한다. 정보보호관리인은 감독을 받는 기관에 대하여 법적인 구속력 있는 지시를 발할 권한은 없고, 단지 정보보호법상의 규정 위반에 대하여 이의를 제기할 수 있다. 법적 구속력 있는 지시의 권한이 없기 때문에 정보보호관리인의 감독기관으로서의 기능에 대하여 특히 경찰영역에서 비판이 제기되기도 하지만, 그의 이의제기는 일반적으로 존중되며 장기적인 관점에서 효과를 발휘하고 있는 것으로 평가된다 [이에 대하여는 Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, 3. Aufl., 1998, S. 340 ff. 참조].

130) § 19 Abs. 5 BDSG, § 18 Abs. 5 HDSG, § 18 Abs. 4, Abs. 6 DSG NW 참조. 바이에른에서는 구체적인 경우에 고지에 의하여 연방 또는 주의 이익이 침해된다고 판단되면 주의 정보보호관리인에게도 고지가 거부될 수 있다.

제4장 우리나라에서의 치안정보의 관리현황 및 문제점

I. 머리말

우리나라에서 경찰은 범죄의 예방·진압과 수사, 교통의 단속을 비롯한 다양한 분야의 공공의 안녕과 질서의 유지업무를 수행하고 있으므로, 국민 개개인에 관한 사소한 일상 사로부터 민감한 개인정보에 이르기까지 방대한 양의 정보를 수집·처리하고 있다. 경찰청에 정보국, 지방경찰청에 정보과(서울특별시 지방경찰청은 정보관리부), 전국 경찰서에 정보 또는 보안과를 두어 범죄정보 외에 정치·경제·노동·사회·학원·종교·문화 등 각 분야에 대한 사회일반 정보를 수집·처리하고 있는데, 치안유지의 목적 범위를 벗어나 국가권력의 유지에 필요한 정보를 수집하고 있다는 의혹과 비난을 받고 있는 것은 매우 오래된 일이다.¹³¹⁾

한편 경찰의 정보관리 업무는 1972년 경찰청(당시 치안본부)에서 UNIVAC9400이라는 대형 컴퓨터를 도입하여 공안관련 자료의 전산화 작업을 시작한 이래, 1983년 정부 주도의 국가 기간전산망 구성계획에 의한 공안전산망의 구성을 비롯하여 '경찰종합정보 체계'를 근간으로 한 경찰내부 업무 및 개인정보의 수집·관리에 대한 전산화를 비롯하여 과학적인 수단에 의한 정보수집, 처리 영역의 급격한 확대가 이루어지고 있다.

경찰정보관리 행태는 종래에도 종종 비난의 대상이 되어 왔으나 개인정보에 대한 각계의 인식의 변화와 정보보호에 관한 법·이론의 발전으로 본격적인 저항에 직면하게 되었다. 또한 경찰 정보처리에 있어서 새로운 과학적인 수단의 등장으로 인하여 야기되는 많은 문제들은 경찰의 직무범위와 권한, 한계의 문제와 더불어 경찰업무에 있어서 새로운 양상을 보이게 될 것이다.

131) 경찰내부에서도 이러한 비판에 대하여 경찰정보활동(직제상 정보관련 부서의 활동)에 변화가 있어야 한다는 주장이 있다(이동권, "효율적인 첩보수집활동 개선방안", 치안정책연구, 1999. 12, 치안연구소, 294쪽 아래).

II. 경찰정보의 수집·처리 상황

1. 개념

(1) 정보의 개념

정보란 최광의로 인간사회의 제 현상을 말하지만, 정보가 갖는 성질·기능·과정·조정 및 한계에 이르는 모든 것을 규정함으로써 비로소 얻어지는 개념이기 때문에 이에 대해 정확하고 완전하게 정의 내릴 수 없는 개념이다.

정보란 원래 '적국의 동정에 관하여 알림'이라는 의미의 군사용어로 사용되었던 것이 사회가 발전되면서 일상용어로 확대되어 쓰여지고 있는데, 보는 관점에 따라 다양하게 정의 내리고 있다. 정보기관에서는 정보란 "국가의 정책결정을 위하여 수집된 첩보를 평가, 분석, 종합 및 해석한 결과로 얻은 지식"이라고 정의하여 첩보와 정보를 구분하고 있다.¹³²⁾ "특정한 목적에 의해 평가되어 있지 않은 단순한 여러 사실이나 기호"를 자료라고 하는데, 이에는 각종 신문자료, 서적, 광고, 개개인의 신상자료 등 모든 것이 자료에 포함되며 특정한 목적이나 처리과정을 거치지 않은 채 산재해 있는 것을 말한다. 첩보란 "목적성을 가지고 의도적으로 수집한 데이터"로서 의식적으로 수집하여야 하나, 아직 분석이나 평가 등의 정보처리과정을 거치지 않은 것을 의미한다. 그에 대하여 정보란 "특정한 상황에서 가치가 평가되고 체계화된 지식"으로서, 입수된 첩보를 필요성에 맞추어 처리 및 가공함으로써 이용가치를 부가시킨 것을 말한다.

현대사회를 정보사회라고 부르는 것은 현대사회에는 많은 정보가 유통되고 있고 다른 재화나 서비스와 마찬가지로 정보가 가치를 지니고 있다는 것을 의미한다. 이렇게 볼 때 정보란 그것을 받는 사람에게 의미가 있고, 현재 또는 앞으로의 행동이나 의사 결정하는데 도움이 될 형태로 처리된 자료라고 정의 내릴 수 있다.¹³³⁾

그러나 국가기관에 있어서 정보는 반드시 평가·해석된 것이라고 볼 수 없으며, 넓게

132) 경찰대학, 경찰정보론, 1999, 11쪽.

133) 노화준, 정보관리론, 경찰대학, 5쪽.

볼 때 국가기관이 그 업무에 기하여 지득하여 저장하고 있는 모든 정보체계의 집합체라고 할 수 있다. 참고로 국가정보자료관리규정(대통령령 제16211호)에서는 ‘국가정보자료’를 국가정보정책의 수립에 기여할 수 있는 국내외 정치·경제·사회·문화·군사·과학·지리·통신 등 각 분야별 기본정보와 각 분야에 영향을 미칠 수 있는 인적·물적 정보 등의 내용이 수록된 자료를 말한다고 정의하고 있다.

경찰법과 경찰관직무집행법에서는 ‘치안정보’라는 용어를 사용하고 있는데, 치안정보란 치안의 목적을 위해서 사용되는 모든 정보를 뜻하는 것으로, 치안의 목적을 위해 의도적으로 수집된 것인 한 평가·해석 등의 처리과정을 거치지 않은 첩보도 포함하는 넓은 의미로 해석하여야 할 것이다.

경찰목적의 달성을 위하여 사용되는 정보를 경찰의 업무에 따라 구분하면 다음과 같다:¹³⁴⁾

- ① 보안정보: 국가의 안전보장과 관련된 정보수집활동으로, 예컨대 북한의 이념에 동조하고 국익을 해하는 세력에 대한 활동상황이나 단체, 개인에 대한 정보수집, 국내에서의 간첩활동을 차단하기 위한 정보활동 등을 말한다.
- ② 범죄정보: 범죄의 예방과 진압, 그리고 공공의 안녕과 질서유지를 위하여 범죄의 대한 각종의 정보수집활동으로, 경찰정보활동의 핵심적인 영역에 해당한다.
- ③ 의사정보: 국내에 주재하는 외국인 또는 외국기관과 해외에 거주하는 동포로서 국내 제반정세에 미치는 영향력 및 취약성에 관한 지식을 말한다.
- ④ 일반정보: 국가의 안전을 위태롭게 하는 개인이나 단체의 모든 불법행위를 예방·수사하는 경찰, 즉 정보경찰이 수집하는 정보를 말한다. 일반적으로 정치, 경제, 사회, 문화 등의 제반 분야의 흐름과 문제점, 그리고 관련 국가정책 결정을 위한 정보 및 문제점 등을 수집한다.
- ⑤ 교통정보: 각종 교통수단의 발달과 이에 따른 다양한 교통문제, 즉 차량소통, 제반 신호기 설치문제, 교통법규 등 각종 교통문제에 대한 사전진단의 필요에 대응하는 정보활동을 말한다.

134) 이에 대하여는 경찰대학, 경찰정보론, 1999, 47-48쪽.

(2) 개인정보의 개념

위에서 살펴본 바와 같이 경찰의 정보활동은 다양한 영역에서 광범위하게 행해지고 있는데, 경찰의 정보 수집·처리활동과 관련하여 법률상 주된 논의의 대상이 되는 것은 개인관련 정보이다. 따라서 본 연구에서는 경찰의 개인정보의 수집·처리에 한정하여 논의를 전개하고 있음을 밝힌다.

‘공공기관의 개인정보보호에 관한 법률’에서는 ‘개인정보’를 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)라고 정의 내리고 있다(제2조 제2호).¹³⁵⁾ 즉 개인정보란 개인의 정신, 신체, 재산, 사회적 지위, 신분 등에 관한 사실·판단·평가를 나타내는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보를 말한다.

개인정보에 대한 구체적인 예는 다음과 같다:

- 내면의 비밀: 사상, 신조, 종교, 가치관, 양심 등
- 심신의 상태: 체력, 건강상태, 신체적 특징, 병력(病歷) 등
- 사회경력: 학력, 범죄경력, 직업, 자격, 소속정당·단체 등
- 경제관계: 재산상황, 소득, 채권채무관계 등
- 생활·가정·신분관계: 성명, 주소, 본적, 가족관계, 출생지, 본관 등

(3) 수집·처리의 개념

정보의 관리는 자료를 수집하여 정보를 추출하고 저장하며 이것을 필요한 때에 필요로 하는 사람에게 제공하는 일체의 업무를 지칭한다.¹³⁶⁾ ‘수집’은 정보를 취득하는 과정으로 단일의 절차인데 대하여, ‘처리’는 정보를 저장, 수정, 이용과 다른 기관에의 제공의

135) 참고로 독일 연방정보보호법 제3조 1항에서는 개인관련 정보를 “특정된 또는 특정할 수 있는 자연인의 인적·물적 관계에 관한 개별적 사항”이라고 규정하고 있다.

136) 노화준, 정보관리론, 경찰대학, 5쪽.

형태로 행해지는 일련의 절차를 포함하는 복합적인 개념으로 이해할 수 있다. 그 이외에도 국가기관의 정보취급과정에 정보의 열람, 정정, 삭제와 타인에 대한 열람제한 등의 관념들이 다루어져야 할 것이나, 이는 국가기관의 정보취급과정에 대한 통제적인 측면에서 사용되는 관념들로서 위의 국가기관의 목적달성을 위해 정보를 '처리'하는 과정과는 별도로 논의해야 할 것이다.

정보의 수집이란 특정인에 대한 정보를 획득하려는 목적을 가진 모든 활동을 말한다. 계속 사용을 목적으로 한 모든 의식적인 개인정보의 인지와 기록은 수집에 해당한다. 정보저장이란 계속적인 사용을 목적으로 정보파일에 정보를 보관하는 것을 말한다. 정보의 수정이란 저장된 정보를 내용적으로 재구성하는 것을 말한다. 단지 표현방식을 바꾸는 것은 수정에 해당하지 않고 정보의 내용을 바꾸는 것이 중요하다. 정보의 이용이란 전통적인 정보처리의 단계(수집, 저장, 수정 등) 이외의 개인정보의 모든 사용을 말한다. 정보의 비교·조사도 정보이용에 해당한다. 정보제공이란 저장되거나 정보처리에 의하여 직접적으로 얻어진 정보를 제3자에게 저장기관이 제공하거나 열람할 수 있도록 함으로써 알려주는 것을 말한다. 그 경우 정보제공의 형태는 불문한다. 구두로 알려주거나 문서에 의하여 제공하는 것 및 전자장치에 의하여 알려주는 것 등 모두 정보제공에 해당한다.

그밖에 삭제는 저장된 정보를 알아볼 수 없도록 만드는 것을 말한다. 정보파일을 파괴하거나 연결을 끊는 것에 의하여 행해질 수 있다. 중요한 것은 저장기관이 정보의 내용을 더 이상 인식할 수 없게 된다는 데 있다. 정정이란 개인정보가 잘못 저장되어 있는 경우에 그를 올바르게 고치는 것을 말한다. 개인은 자기에 관한 정보가 잘못 저장되어 있을 때 그의 정정을 청구할 수 있어야 한다. 열람제한 또는 차단이란 저장된 정보의 처리를 저지하는 것을 말한다. 저장된 개인정보의 처리 또는 이용을 제한하기 위한 표시를 하는 것이 그에 해당한다.

2. 경찰정보 수집·처리의 기본유형

(1) 첩보수집

견문수집 및 처리규칙(경찰청예규 제157호), 수사첩보활동규칙(경찰청예규 제167호)에

의하여 모든 경찰관은 아래의 기준에 의하여 자신이 지득한 첩보를 제출토록 하고 있다.

월간 첩보수집 기준량:

1. 정보외근요원: 30건
2. 외근형사 및 강력: 범죄관련 4건
3. 외근보안 및 의사: 4건
4. 내근수사, 형사, 강력: 범죄관련 2건
5. 내근 기타: 2건
6. 파출소직원: 4건(일반건문 2건, 범죄관련 2건)

위에서 살펴본 바와 같이 기능적으로 경찰의 정보는 보안정보, 범죄정보, 의사정보, 일반정보, 교통정보로 구분하고 있는데,¹³⁷⁾ 이러한 정보들은 경찰의 각종 업무수행에 있어 기본자료로 활용되고 있으나, 문서로 제출되는 이러한 정보들은 전산화되어 있지 않다. 경찰관의 첩보수집 활동에 대한 법적 근거로는 경찰관직무집행법 제2조 제3호를 들고 있다.¹³⁸⁾

(2) 컴퓨터 입력자료의 수집

각종의 경찰전산망에서 사용되는 기초자료는 다양한 경로를 통하여 다양한 방법으로 수집되고 있는데, 이를 수집방법별로 구분하면 다른 기관에서 제공받는 방법, 업무처리의 일환으로 수집하는 방법, 자체적으로 수집하는 방법 등으로 구분할 수 있다.

(가) 다른 기관에서 제공받는 방법

경찰전산망 자료 중에서 다른 기관에서 제공받는 가장 중요한 자료는 전 국민에 대한 기초자료인 주민등록 자료이다. 이는 국가기간전산망체제에서 정보의 연동의 기초가 되

137) 경찰대학, 경찰정보론, 1999, 47-48쪽.

138) 이동권, "효율적인 첩보수집활동 개선방안", 치안정책연구, 1999. 12, 치안연구소, 294쪽.

는 필수적인 역할을 담당하고 있는 것으로, 경찰공안전산망은 행정자치부가 관리하는 행정전산망과 연동되어 주민등록번호 등 주요 주민자료를 활용하고 있다. 이와는 별도로 주민등록법 제17조의 8에 의하여 주민카드를 작성하면서 열손가락의 지문을 날인하고 있는바, 주민등록발급신청서는 일괄하여 경찰청에 이송되어 공안전산망과는 별도로 독립된 데이터베이스인 지문검색 시스템에 입력되어 활용되고 있다. 이와 같은 경우는 행정기관으로부터 자료를 넘겨받아 경찰청 전산망에 입력·활용하고 있는 것이고, 출입국 관련사항 데이터베이스는 법무부에서 관리하면서 경찰에서는 터미널을 이용하여 조회할 수 있는 시스템을 갖추고 있다. 또한 범죄경력, 수사자료에서 처분의 결과 등은 '형의 실효등에 관한 법률'에 의하여 검찰청에서 자료를 넘겨받아 전산관리하고 있으며, 차적 정보 또한 행정기관에서 이관받아 활용하고 있다.

(나) 업무처리의 일환으로 수집하는 방법

상당량의 전산자료는 범죄수사 등 업무의 처리과정에서 법령에 의하여 또는 경찰청 훈령·예규 등 행정규칙에 의하여 수집되고 있다. 그밖에 도난차량, 가출인, 행정전산망에 있어서 운전면허발급 신청과 같이 당사자 등의 신고에 의하여 수집되는 정보가 있다.

범죄수사과정에서 전산입력의 기초가 되는 자료로 작성되는 문서는 범죄통계작성을 위한 발생·검거·피의자통계원표, 주요 장물수배를 위한 피해통보표, 수법자료입력을 위한 수법원지, 절도수법피의자관리를 위한 지문표, 지명수배를 위한 지명수배전산입력요구서 등 각종 수배요구서, 범죄경력관리의 기본이 되는 수사자료표, 유치인 명부, 수사서류, 즉결심판자료 등이 있고, 특이한 경우로 112신고 위치정보 시스템, 공중전화 발신지 추적시스템과 같이 통신회사의 통신망에 연결하여 실시간으로 정보를 조회하는 경우도 있다. 신고에 의해 수집되는 정보는 행정전산망에 있어서 면허자 정보, 미아·가출인 정보, 도난차량, 유실물 정보 등이 있다.

(다) 자체적으로 수집하는 방법

경찰에서 다른 자료를 참고하거나 단독으로 정보를 생산하여 입력하는 경우는 조직폭력배, 마약사범, 운전자 벌점관리 등이 있다.

(3) 전산자료의 활용

(가) 조 회

경찰이 보유한 정보의 단순한 조회는 목적구속의 원칙에 위배되지 않는 한 매우 일상적이며 광범위하게 활용되고 있다.¹³⁹⁾ 수사자료의 조회에 대하여 ‘형의 실효등에 관한 법률’에 의하여 조회에 제한이 가해지는 이외에 ‘공공기관의 개인정보보호에 관한 법률’에 의한 제한을 받게 되며, 경찰 자체적으로는 경찰컴퓨터 온라인 운영규칙(1987. 9. 14), 경찰 전산업무 보안관리 세부지침(1988. 10), 전산처리 되는 개인정보보호를 위한 세부지침(1991. 5. 27) 등에 의하여 조회의 요건 등을 규정하여 관리하고 있다.

(나) 데이터의 검색

데이터의 검색 또는 전산자료검색이란 수사기관이 자체적으로 정보를 수집하여 전산 보관 하거나 별도로 분류하는 것이 아니라, 다른 기관이나 범죄와 무관한 전산자료로부터 특정한 범죄적인 징표를 찾아내기 위해서 사용하는 수사기법이다.

독일 형사소송법은 제98a조에서는 컴퓨터에 의한 인적 자료의 검색·조사(Rasterfahndung)에 대하여 명시적으로 규정하고 있다. 이에는 일정한 제한이 있는데, 첫째는 범위에 있어서는 조직 범죄 및 국가안보의 영역에 한하여 허용되고, 어느 한 사람에 대한 자료가 다른 특정한 행위자와 관련되었다고 추정되는 특정한 수색의 징표를 찾을 수 있게 하는 자료 등에 한하며, 무관한 개인의 자료가 직접 검토되는 것을 금지하고 있다. 또한 보충성의 원칙에 의하여 전산자료의 조회는 다른 수사기법의 제한 등으로 인하여 범죄에 대한 소추가 어려운 경우 제한적으로 허용되고 있다.¹⁴⁰⁾ 경찰법 영역에서는 연방과 주의 존립 또는 안전, 사람의 생명·신체 또는 자유에 대한 현존하는 위협을 방지하기 위하여서만 허용된다. 요건을 충족하는 경우 사법경찰은 다른 정보와 비교·조사하기

139) 1992년의 경우 연 1억여 건의 컴퓨터 조회가 이루어지고 있다고 한다(이에 대하여는 채한수, 정보화사회에 있어서 한국경찰의 컴퓨터 활용성 제고방안에 관한 연구, 고려대 석사학위논문, 1994 참조).

140) 조두영, 독일사법경찰관의 지위 및 몇 가지 문제점, 독일연방법무부 연수보고서, 1996. 12.

위하여 공적 또는 사적 기관에게 일정한 인적 그룹의 개인관련 정보의 제공을 요구할 수 있다. 정보파일 또는 모든 정보자료의 제공을 요구하는 것이 아니라 특정 인적 그룹에 대한 정보를 요구하는 것이다. 예를 들면 일정한 징표에 의하여 그룹 지워지는 사람들에 대한 정보를 요구하는 것이다.

기술적으로 보면 전향의 조회는 컴퓨터신원조회(computer screening)¹⁴¹⁾, 프론트엔딩(front-ending)¹⁴²⁾, 프론트엔딩 감사(front-ending audit)¹⁴³⁾에 불과한 것이며, 데이터 검색은 컴퓨터 매칭(computer matching)¹⁴⁴⁾을 활용하는 것이라고 볼 수 있다. 이와 관련하여 행정자치부에서 보유한 주민등록자료를 바탕으로 각 기관에서 업무상 입력한 데이터와 통합하는 경우와 같이 중복되는 전산자료의 통합을 위한 조직내부 또는 국가기관간의 기록통합(record intergration)을 컴퓨터 매칭과 혼동하여 비판하는 경우도 있는데,¹⁴⁵⁾ 위와 같은 기록통합은 컴퓨터 매칭의 문제가 아니라 개별적인 정보가 수집권한 범위 내에 있고 필요한 정보가 목적제한의 원칙에 따라 사용되는 등 제반 정보보호의 원칙 하에 있으면 족하고 별도의 수권이 필요하지 않은 사실적 행위에 불과하다고 보아야 할 것이다.

그런데 독일 형사소송법에 있어서는 컴퓨터에 의한 인적 자료의 검색·조사를 하는 경우에 정보를 요구받은 기관은 필요한 데이터를 기억장치로부터 선별·정리하여 범죄 수사기관에 송부하도록 하고 검사의 요구가 있을 경우 데이터의 비교·조사를 보조할 의무를 부과하고 있음에 반하여, 우리나라의 경우 이러한 명문 규정이 없고 수사기관에 이러한 조치를 할만한 기술적 준비가 되어 있지 않기 때문에 실무상 컴퓨터 매칭을 통한 수사는 거의 이루어지고 있지 않다.

141) 마스터파일에서 개인의 정보를 조회하는 것을 말한다.

142) 컴퓨터 조회를 보다 발전시킨 것으로, 통신회선을 통한 원거리에서의 마스터파일 조회를 뜻한다.

143) 예컨대 교통위반으로 단속되었을 때, 차적조회, 도난차량조회, 운전자의 수배조회 등을 하는 것과 같이 특정한 정보를 기준으로 다른 마스터파일을 조회하는 것을 뜻한다.

144) 분리되어 있는 두 개 이상의 개인데이터 시스템의 정보를 결합하는 것을 말한다.

145) 예컨대 홍석만/이준구, 역감시의 권리로서 프라이버시권에 대한 재구성, 민주사회를 위한 변호사 모임, 1998. 7. 59쪽.

(4) 기타 경찰조치

독일 형사소송법에서 규정하고 있는 신원확인조치(제163조의 b, 제163조의 c), 전산망 입력(Schleppnetzfahndung: 제163조의 d), 경찰감시를 위한 등록(제163조의 e), 과학적 수사장비 투입에 의한 사진촬영 및 녹화, 기타 관측장비의 사용(제100조의 c), 신분위장 수사관의 투입(제110조의 a-e)¹⁴⁶⁾ 등과 경찰법 분야에서 통일경찰법모범초안에 대한 개정초안의 공개된 행사, 모임 및 집회에서의 정보수집(제8조의 b), 정보수집의 특별한 수단(제8조의 c), 경찰감시(제8조의 d), 신원확인 및 신분증명서의 심사(제9조), 감식조치(제10조), 정보제공(제10조의 c)¹⁴⁷⁾ 등은 우리나라 경찰에서 제도적으로 보장되어 있지 않으나, 일상적으로 행해지고 있거나 개인정보 침해의 문제 때문에 비공개로 행해지고 있는 부분이 많다.

Ⅲ. 경찰 정보수집·처리에 대한 법적 근거

1. 머리말

국가기관이 그 업무를 효율적으로 수행하기 위해서는 국민 개개인에 관한 많은 정보를 필요로 함에는 의문의 여지가 있을 수 없다. 특히 경찰작용은 성질상 국민의 개인생활과 밀접한 관련이 있으므로 다른 국가기관에 비해 그 필요성이 더욱 크다고 할 수 있다. 정보처리기술의 발전은 국가기관이 필요로 하는 개인에 관한 정보를 수집·처리하는 데 있어 매우 획기적인 변화를 가져 왔으나, 반면에 이로 인한 개인의 사생활 침해 등 국민의 권리침해의 위험성 또한 더욱 높아졌다고 할 수 있다. 개인의 사생활 보호, 개인 정보 보호의 필요성에 대한 논란이 제기되어 세계 각 국에서는 개인정보를 보호하기 위

146) 이들 조항의 내용에 대하여는 법무부, 독일형사소송법, 1998 참조.

147) 이들 조항의 내용에 대하여는 홍준형, 경찰통합법에 관한 연구, 치안연구소, 1997, 208쪽 아래 및 서정범 역, 독일경찰법론, 세창출판사, 1998, 314쪽 아래 참조.

한 법률이 다양한 형태로 제정되었는데, 이에 발맞추어 우리나라에서도 1995년 1월 8일부터 '공공기관의 개인정보보호에 관한 법률'을 시행하고 있다. 경찰작용은 주로 권력적·침익적 작용인 점에서 다른 어떤 국가기관보다도 정보에 대한 개인의 권리를 침해할 우려가 높아 그에 대한 법적 규제의 필요성이 이미 오래 전부터 인식되었음에도 불구하고 우리나라에서 그에 대한 본격적인 법적 측면에서의 논의나 입법적 조치는 상당히 미흡한 상태에 있다고 볼 수 있다. 아래에서는 우선 경찰이 국민의 정보를 수집·처리할 수 있는 법적 근거의 필요성 여부와 그에 관한 현행법 체계를 살펴보고자 한다.

2. 법적 근거의 필요성

법률유보원칙에 따라 개인의 자유와 권리에 대한 국가의 침해에는 법적 근거가 있어야 한다. 현대사회에 있어서 정보수집 및 처리는 행정업무의 원활한 수행을 위하여 필수 불가결하다. 따라서 경찰업무의 수행을 위하여 다양한 정보적 침해활동이 수반되는 것은 당연하다. 그러나 독일 연방헌법재판소의 인구조사판결에서 확인된 것처럼 개인정보에 대한 국가의 모든 수집·처리활동은 정보적 자기결정권에 대한 침해를 가져오므로,¹⁴⁸⁾ 그에 대하여는 형식적 법률에 의한 특별한 법적 근거가 마련되어야 한다.

3. 현행법상 경찰정보 수집·처리의 법적 근거

(1) 경찰의 직무범위와 권한

(가) 경찰의 직무범위

우리나라에서 조직적인 의미의 경찰은 경찰법 제2조에 의해 규율되는 것을 말하고,

148) 1983년의 인구조사판결 이전에 독일 연방헌법재판소는 개인정보의 수집·처리를 침해적 활동이 아닌 것으로 보았었다. 그러나 현재 공행정기관에 의한 개인정보의 처리에 의해 기본권에 의하여 보호된 법익이 침해될 수 있다는 것은 일반적으로 받아들이고 있다. 이에 대하여는 Kowalczyk, Datenschutz im Polizeirecht, 1989, S. 65 f.; Götz, Allgemeines Polizei- und Ordnungsrecht, 12. Aufl., 1995, S. 72 참조.

형식적 의미의 경찰은 경찰법 제3조와 경찰관직무집행법 제2조에 의해 수행되는 직무활동을 뜻한다. 경찰관계법은 크게 경찰조직법, 경찰공무원법, 경찰작용법 등으로 구분하는 것이 일반적인데, 현행법에서는 경찰조직법은 ‘경찰법’이, 경찰공무원법은 ‘경찰공무원법’이 제정되어 있으나, 경찰작용법에 대하여는 ‘경찰관직무집행법’이 일반법적인 기능을 수행하고 있고, 그밖에 ‘집회 및 시위에 관한 법률’, ‘사격 및 사격장 단속법’, ‘총포·도검 및 화약류등 단속법’, ‘도로교통법’ 등 다수의 개별법이 경찰작용을 규율하고 있다.

경찰관직무집행법 제2조에 의하면 조직적인 의미의 경찰은 범죄의 예방·진압 및 수사, 경비·요인경호 및 대간첩작전수행, 치안정보의 수집·작성 및 배포, 교통의 단속과 위해의 방지, 기타 공공의 안녕과 질서유지라는 형식적 의미의 경찰활동을 직무범위로 한다. 따라서 경찰은 행정경찰 뿐만 아니라 사법경찰로서의 직무도 수행하고 있는데, 형사소송법 제196조에 의하여 사법경찰관은 검사의 지휘를 받아 수사하고, 사법경찰리는 검사 또는 사법경찰관의 지휘를 받아 수사를 보조하도록 되어 있다.

(나) 직무규범과 권한규범

경찰권의 행사와 관련되는 규범은 그 직무에 관한 규범(직무규범 또는 임무규범: Aufgabennorm)과 구체적인 행위에 관한 권한규범(Befugnisnorm)으로 구분할 수 있는데, 경찰이 경찰권을 발동하기 위하여서는 직무규범으로 충분한 것인지, 아니면 직무규범 이외에 별도의 권한규범이 필요한 것이냐가 문제된다. 이와 관련하여 우리의 경찰관 직무집행법 제2조 5호의 ‘공공의 안녕과 질서유지’에 관한 조항을 개괄적 수권조항으로 보아, 개별적인 근거규정이 없을 때에는 이 조항에 의거하여 경찰권을 발동할 수 있다고 보는 견해가 있다.¹⁴⁹⁾

149) 김남진, 행정법 II, 법문사, 2000, 263쪽; 김남진, 행정법의 기본문제, 법문사, 1994, 698쪽; 김남진, 경찰상의 개괄적 수권조항, 고시연구, 1994. 7, 175쪽; 서원우, 경찰법상의 개괄조항, 월간고시, 1980. 6, 62쪽; 이명구, 경찰작용과 공공질서, 고시연구, 1984, 1. 58쪽 아래; 신보성, 경찰권의 근거와 한계, 월간고시, 1987. 12, 162쪽; 이순용, 경찰의 부작위와 개입청구권, 사법행정, 1990. 10, 40쪽; 강구철, 경찰권의 근거와 한계, 고시연구, 1991. 9, 80쪽; 서정범, 경찰권발동에 관한 연구, 고려대 박사학위논문, 1992, 26쪽; 남승길, 경찰관직무집행법, 공법연구, 제25집 제3호, 1997, 91쪽 아래; 오병주, 경찰권의 근거와 한계, 법조, 1998. 2, 73쪽 아래; 김해룡, 경찰권발동과 행정상 손실보상, 고시계, 1998. 4, 64쪽 아래; 김재호, 경찰권의 근거, 저스티스, 제32권 제2호, 6쪽 아래.

대법원은 1986.1.28, 85도2448사건에서 “청원경찰법 제3조는 청원경찰은 청원주와 배치된 기관, 시설 또는 사업장 등의 구역을 관할하는 경찰서장의 감독을 받아 그 경비구역 내에 한하여 경찰관직무집행법에 의한 직무를 행한다고 정하고 있고, 한편 경찰관직무집행법 제2조에 의하면 경찰관은 범죄의 예방·진압 및 수사, 경비·요인경호 및 대간첩작전수행, 치안정보의 수집·작성 및 배포, 교통의 단속과 위해의 방지, 기타 공공의 안녕과 질서유지 등을 그 직무로 하고 있는 터이므로 경상남도 양산군 도시과 단속계 요원으로 근무하고 있는 청원경찰관인 공소 외 김창성 및 이성주가 ……허가 없이 창고를 주택으로 개축하는 것을 단속한 것은 그들의 정당한 공무집행에 속한다고 할 것이므로 이를 폭력으로 방해한 판시 소위를 공무집행방해죄로 다스린 원심조치는 정당하고, 이에 소론과 같은 위법이 있다고 할 수 없다”라고 판시하고 있다. 이 판결이 직무규정인 경찰관직무집행법 제2조를 경찰권행사의 일반적 수권조항으로 보는 것인지¹⁵⁰⁾ 또는 경찰관직무집행법 제2조를 권한규범으로서의 성격을 아울러 가지는 것으로 보는 것인지는 명백하지 않으나,¹⁵¹⁾ 적어도 경찰관직무집행법 제2조가 경찰권 발동의 근거가 되는 것으로 본 것만은 분명하다. 즉 경찰관직무집행법에 경찰관이 불법적인 건축행위를 단속할 수 있다는 규정이 없음에도 불구하고 공공의 안녕과 질서유지를 규정하고 있는 경찰관직무집행법 제2조 5호를 우리나라의 실정법상의 경찰에 대한 개괄적 수권조항으로 해석하고 있다.

그러나 동 조항은 경찰관의 직무를 정하는 규범일 뿐이지 구체적인 경우에 경찰이 직무수행을 위하여 개인의 권리·이익에 대한 침해까지 가능하게 하는 규정으로 볼 수 없다. 경찰법에 있어서 위험방지임무와 위험방지를 위한 개인의 권리에 대한 침해의 권한과는 구별하여야 한다. 위험방지를 위하여 개인의 권리를 침해하는 것은 위험방지임무의 수행에 해당한다. 그러나 개인의 권리침해는 특별한 조건을 갖춘 경우에만 허용되는 것이다. 즉 침해에 대한 특별한 수권이 있거나 또는 개괄조항에 의한 수권이 있어야 한다. 위험방지를 위한 경찰의 직무에 해당하더라도 이러한 수권이 없으면 개인의 권리를 침해할 수는 없는 것이다.

150) 김재호, 경찰권의 근거, 저스티스 제32권 제2호, 18쪽.

151) 김남진, 경찰상의 개괄적 수권조항, 고시연구, 1994.7, 175쪽; 김남진, 행정법 II, 2000, 263쪽, 각 주 2) 참조.

법률유보의 원칙은 경찰이 공공의 안녕과 질서유지를 위하여 개인의 권리를 침해하게 되는 경우, 침해의 근거로서 권한규범에 의한 수권을 요구한다. 경찰권 발동의 법적 근거로서 개괄조항을 인정할 때, 여기서 개괄조항이란 단순히 경찰의 임무규정을 말하는 것이 아니고 권한규정을 말하는 것이다. 이러한 의미에서의 개괄조항의 입법례로는 1931년의 프로이센 경찰행정법 제14조 1항을 들 수 있다. 동조는 “경찰행정청은 공공의 안녕 또는 질서를 위협하는 위험(Gefahren)으로부터 공중 또는 개인을 보호하기 위하여 실정법의 범위 안에서 의무에 적합한 재량에 따라 필요한 조치(die nach pflichtmäßigen Ermessen notwendigen Maßnahmen)를 취하지 않으면 안 된다”고 규정하여 위험방지에 대한 개괄적 수권조항(Generalklausel)을 채택하였다. 이 규정과 우리나라의 경찰관직무집행법 제2조 또는 경찰법 제3조¹⁵²⁾의 경찰관의 직무에 관한 규정을 비교할 필요가 있다. 결국 우리나라의 경우에도 권한규범의 성격을 갖는 일반적 조항을 두어 개괄적 수권조항이 필요한 현실에 입법적으로 대응하는 것이 요청된다.

(다) 개괄적 수권조항의 보충성

개괄적 수권조항의 존재가 인정되는 경우에 개괄적 수권조항은 경찰법상의 개별적 수권조항 및 경찰관계법 이외의 다른 법률상의 개별적 수권조항이 존재하지 않을 때

152) 우리 문헌의 일부에서는 경찰법 제3조도 경찰권 행사에 관한 개괄적 수권조항에 해당한다는 주장을 발견할 수 있다[석종현, 일반행정법(하), 279쪽; 강구철, 경찰권의 근거와 한계, 고시연구, 1991. 9, 80쪽]. 이에 대하여 헌법재판소는 1991년 5월 10일 국회 본회의에서 통과되고 같은 달 31일 공포된 경찰법에 대한 위헌심사에서 “‘경찰법’은 경찰의 기본조직 및 직무범위 등을 규정한 전형적인 조직법으로서 원칙으로 그 조직의 구성원이나 구성원이 되려는 자 등 외에 일반국민을 수범자로 하지 아니한다. 그러므로 일반국민인 청구인들은 위 경찰법의 공포로써 자기의 헌법에 보장된 기본권이 현재 직접적으로 침해되었다고 할 수 없다. 청구인들은 위 법률에 의하여 설치된 경찰기관의 경찰권 행사로 인하여 언제든지 기본권을 침해받을 가능성이 있다고 주장하나, 그러한 기본권 침해는 경찰관직무집행법이나 형사소송법 등에 따라 행해지는 경찰권 행사라는 별도의 공권력의 행사에 의한 것이지 조직법인 위 법률에 의하여 직접 이루어지는 것이라고 할 수 없고, 또 청구인들이 주장하는 기본권 침해의 가능성은 잠재적인 우려에 불과한 것이다”라고 판시하였다[헌재 1994. 6. 30, 91헌마162]. 이로써 헌법재판소는 조직법으로서의 경찰법 제3조가 경찰권 발동의 개괄적 수권조항이 될 수 없음을 분명히 하고 있다. 그밖에 경찰관직무집행법 제2조 5호가 개괄적 수권조항에 해당하는지에 대하여는 언급하고 있지 않지만, 작용법인 경찰관직무집행법과 조직법인 경찰법은 경찰권 행사에 있어서 다르게 취급하여야 한다는 점을 전제하고 있다.

에만 보충적으로 적용되는 것이다. 즉 이들이 경합할 때에는 언제나 개별적 수권조항이 우선적으로 적용되는 것이다. 위의 대법원 판례의 경우 구 건축법 제42조 1항(1998.12.31 폐지됨, 현행 건축법 제69조 1항)에 의하여 위법한 건축행위에 대하여 단속할 권한은 시장 또는 군수에게 있는 것이다. 이 사안에서 불법적인 건축행위를 단속한 청원경찰은 경상남도 양산군 도시과 단속계 요원으로 근무하고 있었으므로 당해 청원경찰이 시장·군수의 단속권한을 행사한 것이라면 정당한 직무집행에 해당하는 것으로 볼 수 있을 것이다. 그러나 이 경우에도 단속의 법적 근거는 구 건축법 제42조 1항이 되므로 경찰관직무집행법 제2조를 근거로 보는 것은 개괄적 수권조항의 보충성에 반하는 것이다.

(2) 경찰 정보수집·처리를 규율하는 법률규정

경찰의 정보활동에 있어서 정보의 자기결정권에 대한 침해가 있는 경우에는 그에 대한 법적 근거가 있어야 함은 이미 살펴보았다. 즉 경찰영역에서의 개인정보가 강제적으로 또는 비밀리에 수집되는 경우에 그를 위하여서는 특별하고 자세한 법적 근거가 있어야 한다. 아래에서는 경찰의 정보수집·처리의 법적 근거로서 논의될 수 있는 법률규정을 살펴보기로 한다.

(가) 경찰작용법

(a) 경찰관직무집행법 제2조 3호: 정보수집·처리의 법적 근거?

경찰관직무집행법 제2조에서는 경찰의 직무범위를 범죄의 예방·진압 및 수사, 경비·요인경호 및 대간첩작전수행, 치안정보의 수집·작성 및 배포, 교통의 단속과 위해의 방지, 기타 공공의 안녕과 질서유지 등으로 정하고 있다. 여기에서 '치안정보의 수집·작성 및 배포'가 경찰이 직무를 수행함에 있어서 정보수집·처리의 근거규정으로서 역할을 하는 것이 아니라, 이는 정보기관으로서 경찰의 직무범위를 정하는 것이 목적이며, 직무수행을 위하여 필요한 정보의 수집 및 처리는 당해 직무에 대한 규정에 내재한 것으로 보는 것이 일반적이다. 따라서 경찰관직무집행법 제2조 3호는 정보기관으로서 경찰의 정보

활동에 대한 법적 근거로서 논의될 뿐이다.

그 동안 무리한 수사와 권한남용 등으로 끊임없이 인권침해의 논란을 빚어 온 이른바 '사직동팀'(경찰청 조사과)¹⁵³은 대통령 친인척 및 고위공직자 관련 비위에 대한 내사와 첩보수집 등의 업무를 맡아 왔는데, 이 기관의 법적 근거가 경찰관직무집행법 제2조 3호의 치안정보의 수집·작성 및 배포에 대한 규정에 있다고 한다.

그러나 이 규정이 정보기관으로서 경찰이 '개인정보'를 수집·처리하는 데 대한 법적 근거가 될 수 있는지는 의문이다. 경찰관직무집행법 제2조 3호에서는 치안정보의 수집·작성 및 배포가 경찰관의 직무범위에 속함을 명시하고 있을 뿐이다. 이 규정은 단지 직무규정으로서 직무수행을 통한 개인의 권리에 대한 제한 내지 침해의 근거규정이 될 수 없다. 치안정보의 수집 등에 의하여 개인의 권리에 대한 침해를 가져오는 경우에는 권리 침해에 대한 수권규정이 있어야 한다. 결국 경찰관직무집행법 제2조 3호의 규정은 단지 치안정보의 수집 등이 경찰의 직무범위에 속함을 규정한 포괄적인 직무규정으로서 개인의 정보적 자기결정권에 대한 제약을 가져오는 구체적인 개인정보의 수집·처리에 대한 근거가 될 수 없다고 하겠다.

결국 우리나라에서 경찰작용에 관한 일반법으로서 기능하는 경찰관직무집행법은 개인정보의 수집·처리에 관한 법적 근거규정을 결여하고 있다고 보아야 한다.

(b) 그 밖의 경찰관직무집행법 규정

경찰관직무집행법에서는 위험방지를 위한 구체적인 조치에 대한 근거규정을 두고 있다. 예컨대 제3조의 불심검문, 제4조의 보호조치, 제5조의 위험발생의 방지조치, 제6조의 범죄의 예방과 제지, 제7조의 위험방지를 위한 출입, 제8조의 사실의 확인 등을 규정하고 있는데, 이러한 경찰작용과 관련하여 정보의 수집·처리가 행해질 수 있으나, 그에 대하여는 명확한 규율을 하고 있지 않다. 따라서 이에 대한 입법적 조치가 마련되어야 하며, 법적 규율을 함에 있어서는 정보의 수집·처리에 관한 일반원칙이 중요하게 고려되어야 할 것이다. 예를 들면 정보의 수집은 관계인으로부터 행해져야 하며, 법률에 다른 규정이 없는 한 공개적으로 행해져야 하고, 관계인에게 정보수집의 법적 근거 및 정

153) 사직동팀(경찰청 조사과)는 2000년 10월 24일 경찰청 직제에서 폐지되었다.

보제공의무 또는 거절의 자유 등을 적당한 방법으로 알려주는 것이 특히 중요한 의미를 가진다.

(c) 개별적인 경찰작용법

경찰작용법은 경찰관직무집행법 이외에 많은 개별법의 집합체라고 할 수 있다. 사법경찰 분야에서 수사활동에는 형사소송법 규정이 적용됨에 반하여, 행정경찰 분야에서는 실질적인 의미의 경찰활동을 규율하는 모든 법률이 경찰작용법에 포함될 수 있는데, 이는 다시 직접 경찰이 관할권을 가지고 경찰작용을 행하는 근거가 되는 경찰작용관련 법률과 일반 행정기관에게 다른 행정작용과 관련하여 발생하는 사회공공의 안녕·질서에 대한 위험을 방지하도록 수권하는 개별법으로 구분할 수 있다. 경찰작용관련 법률에는 예컨대 집회 및 시위에 관한 법률, 용역경비업법, 청원경찰법, 청소년보호법, 사격 및 사격장 단속법, 총포·도검·화약류 등 단속법, 사행행위 등 규제법, 사행행위 등 규제 및 처벌 특례법, 도로교통법, 풍속영업의 규제에 관한 법률 등이 있다. 이들 법률에서 경찰의 정보수집·처리에 관한 규정을 두고 있으면 그에 따르면 되는데, 대부분 그에 관한 규정을 두고 있지 않은 상태이다.

(나) 경찰작용법 이외의 법률

(a) 공공기관의 개인정보보호에 관한 법률

1994년에 제정되고 1999년 일부 개정된 ‘공공기관의 개인정보보호에 관한 법률’은 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정하고 있다. 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 동법이 우선 적용되므로(제3조 1항), 행정기관의 컴퓨터에 의한 정보처리 부분에 있어서 일반법의 위치에 있다. 동법은 제2장에서 개인정보의 수집·처리에 관하여, 제3장에서 처리정보의 열람·정정 등에 관한 규율을 하고 있다.

경찰작용에 관하여도 컴퓨터로 처리되는 개인정보에 관하여는 동법의 적용을 받게 된다. 다만 동법은 제3조 2항에서 국가안전보장과 관련된 정보분석을 목적으로 수집 또는

제공요청되는 개인정보의 보호에 관하여는 이 법을 적용하지 아니한다고 하여 오히려 개인의 정보에 관한 기본권 침해의 우려가 가장 큰 국가정보기관의 정보수집·처리에 대해 동법의 적용을 배제하였고, 제6조 1항에서 공공기관이 개인정보파일을 보유하고자 하는 경우에 행정자치부 장관에 대한 사전통보 의무를 규정하면서 제2항에서 ① 국가의 안전 및 외교상의 비밀 기타 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일 및 ② 범죄의 수사, 공소의 제기 및 유지, 형의 집행, 교정처분, 보안처분과 출입국관리에 관한 사항을 기록한 개인정보파일의 경우는 그 적용을 배제함으로써, 결국 경찰작용 분야에서는 교통행정 등 순수 행정작용만이 동법에 의한 완전한 통제가 가능할 뿐이고, 국가정보기관으로서의 작용과 범죄수사 분야에 대하여는 통제영역 밖에 놓이게 되는 문제가 있다.¹⁵⁴⁾

(b) 공공기관의 정보공개에 관한 법률

1996년에 제정된 ‘공공기관의 정보공개에 관한 법률’은 헌법상 권리인 국민의 알권리를 보장하고자 공공기관이 보유·관리하는 정보의 공개의무 및 국민의 정보공개청구에 관하여 필요한 사항을 정하고자 하는 데 목적이 있다. 이 법은 공공기관의 정보공개에 대한 일반법의 위치에 있다. 동법에 의하여 경찰이 보유한 정보는 원칙적으로 공개되어야 하며, 이를 통하여 국민의 알권리를 충족함과 동시에 부적절한 행정작용에 대한 통제장치적 역할을 수행하게 된다.

(c) 형사절차법과의 관계

우리나라 경찰은 행정경찰작용과 사법경찰작용 양자를 아울러 관장함으로써 형사소송법 등 수사절차에 관한 법률이 경찰의 정보수집·처리에 관한 근거법이 될 수 있다. 주로 문제되는 컴퓨터데이터에 있어서 실제로 경찰전산망에 의하여 운영되는 상당부분의 데이터는 범죄의 예방, 진압, 수사라는 범죄투쟁을 위해 수집되었거나 그 과정에서 수

154) ‘공공기관의 개인정보보호에 관한 법률’ 제7조에 의하여 행정자치부 장관이 1998. 11. 공고한 개인정보파일 목록집에 의하면 경찰청 소관업무에 대하여 행정자치부 장관에게 통보한 개인정보파일은 운전면허 결격자 관리, 운전면허 대장관리, 자동차운전 기능검정원·강사자격증 관리, 병원관리 프로그램에 불과하다.

집된 자료가 많다. 그런데 경찰이 가지고 있는 방대한 데이터들이 행정경찰작용에 의해 처리되는 것인지 또는 사법경찰작용에 의해서 처리되는 것인지는 명백하지 않은 경우가 많다.

독일의 경우 연방헌법재판소의 인구조사판결의 영향을 받아 형사소송법에서도 일련의 조문들을 마련하였는데, 예를 들면 전산망입력(독일 형사소송법 제163조의 d), 전산망검색(제98조의 a 및 b), 정보의 비교조사(제98조의 c)에 관한 상세한 규정들이 그에 해당한다. 이에 비하여 우리나라 형사절차법에서는 임의수사의 원칙과 강제수사법정주의에 의하여 개인의 기본권을 제한하는 처분은 강제처분이라고 하여 법률에 특별한 규정이 있는 경우에 예외적으로 인정하고, 임의수사에 관하여는 구체적인 방법은 수사기관에서 결정하도록 하되, 다만 형사소송법은 이중에 공무소 등에의 조회(형사소송법 제199조 2항), 피의자심문(제200조, 제241조 아래), 참고인조사(제221조 전문), 감정·통역·번역의 위촉(제221조 후문) 등에 관해서만 특별한 규정을 통하여 그 절차적 규율을 하고 있을 따름이다.¹⁵⁵⁾ 문제점은 수사기관의 정보처리에 관하여 고유한 특별한 규정을 두고 있지 않고 있을 뿐 아니라 국민의 정보적 기본권을 제한하는 효과를 가져올 수 있는 전산망검색 등 정보처리에 대하여 입법의 공백을 두고 있기 때문에 기본권침해에 대한 시비의 우려가 상존하는 상태이다.

4. 소 결

경찰은 업무의 특성상 개인정보를 비롯한 많은 정보를 필요로 하게 되며, 정보통신의 발전과 사회의 다원화에 따른 정보의 컴퓨터를 통한 처리가 경찰목적 달성을 위해 많이 활용되게 되었으며 이와 함께 이에 의한 국민의 정보적 기본권 침해의 우려도 확대되었다.

경찰의 정보수집·처리는 경찰작용에 내재된 것으로 별도의 절차를 규정하지 않는 것은 우리나라가 계수한 독일법의 경우도 마찬가지였으나 정보의 자기결정권에 관한 독일 연방헌법재판소의 인구조사판결을 계기로 독일의 경찰법 및 형사소송법이 정보수집·처리에 관한 상세한 별도의 규정을 두게 되었음에 반하여, 우리나라의 경찰관련법에서는 여전히 입법상 공백을 두고 있다.

155) 배종대/이상돈, 형사소송법, 1997, 200쪽 아래.

경찰의 임무규범은 국민에 불이익을 주지 않는 범위 내에서 경찰작용의 근거가 될 뿐
이므로 국민의 정보적 기본권을 제한하는 경우에는 별도의 수권규정을 필요로 한다.

경찰관직무집행법에서는 제2조의 임무규정을 두고 있을 뿐 정보수집·처리에 관하여
전체 경찰작용을 규율하는 조문은 두고 있지 않다. 경찰관직무집행법을 비롯한 개별적인
경찰작용법에서 근거규정을 찾을 수 있으나, 이 경우에도 정보처리에 관하여 별도의 자
세한 규정을 두고 있지 않은 상태이다. 사법경찰 분야에 적용되는 형사소송법의 경우에
도 사정은 다르지 않다.

‘공공기관의 개인정보보호에 관한 법률’, ‘공공기관의 정보공개에 관한 법률’ 등은 부분
적으로 국민의 정보적 기본권을 보장하는 측면에서 경찰의 정보수집·처리 내지 그에
대한 통제에 관한 규율을 하고 있으나, 적용배제조항에 의하여 통제영역 밖에 놓이는 경
우가 많다.

IV. 경찰 정보처리와 개인정보보호

오늘날 컴퓨터산업의 발달에 따라 도래한 고도 정보화사회는 국민생활의 향상과 편리
를 제공해 주는 반면에 여러 문제도 가져왔다. 정보화시대의 여러 국가에서는 개인의 정
보가 공적·사적 부분으로 수집·축적되어 이용되고 그 결과 컴퓨터시스템에 의해 인간
상이 여러 가지 모양으로 노출되고 있다.¹⁵⁶⁾ 그에 따라 날로 발전하는 기술로부터 개인

156) 최근 미국에서는 교통량 등을 정확히 측정하기 위한 첨단 기술과 장치들이 본래의 취지와
는 달리 운전자의 사생활을 침해할 우려가 있다는 지적이 제기돼 논란을 빚고 있다. 뉴욕의
고속도로 당국은 차량들의 속도와 교통체증을 파악하기 위해 유료 고속도로와 교량, 터널
등을 통과할 때 현금 대신에 사용하는 이제트(E-Z) 전자 패스가 있는 차량의 운행상황을
모니터하고 있다. 버지니아 주와 메릴랜드 주는 워싱턴 외곽의 순환도로로 상습정체 도로인
495 벨트웨이를 주행하는 운전자들의 휴대폰 통화상황을 모니터, 교통체증의 정도를 파악하
는 프로그램을 개발중이다. 또한 도로에 설치된 카메라는 기술의 발달에 힘입어 어떤 차량
이 신호위반을 하는지 여부는 물론 신호위반 운전자의 얼굴이 차량 소유주의 운전면허 사
진과 일치하는지를 대조할 수 있는 기능까지 갖추게 될 전망이다. 이에 따라 운전자들은 크
레디트 카드나 인터넷을 사용하는 것처럼 자동차로 언제 어느 곳을 어떻게 다녔는지에 관

의 기본적인 인권을 보호할 수 있는 법적 통제장치를 마련하는 것, 특히 개인정보보호의 문제가 중요한 법적 문제로 등장한다.

아래에서는 먼저 개인정보보호의 의의를 살펴보고, 공적부문에서의 개인정보의 침해에 관한 개별적인 문제를 검토한 후, 개인정보보호법제에 대한 외국의 입법례와 국제적 동향과 우리나라의 법제화 동향을 살펴보기로 한다.

1. 개인정보보호의 의의

(1) 개인정보보호의 이념

개인정보는 개인에 전속하며 개인의 권익과 밀접한 관련이 있기 때문에, 업무처리과정에서 필수적으로 개인의 정보를 보유하게 되는 국가기관 등은 그에 대한 처리에 있어서 신중하여야 하며, 개인정보의 보호에 특히 유념하여야 한다.

개인정보보호에 있어서 보호의 기본적인 이념은 프라이버시권을 들 수 있다. 이 권리는 19세기 말 「혼자 있을 권리」(right to be let alone), 즉 황색 저널리즘(yellow journalism)에 의한 사생활 폭로로부터 보호라는 소극적인 권리에서 오늘날에는 「자기 정보를 관리할 권리 또는 정보의 자기결정권」이라는 보다 적극적인 성격을 띤 권리로 발전되었다. '자기정보'나 '관리'의 의미가 반드시 명확하지는 않다는 문제는 있지만, 그 배경에 자신에 관한 정보가 타인에 의해 임의로 이용되지 않는 것이 개인의 행복추구를 위해 필수 불가결하다는 인식이 있으며, 또한 그것이 현대의 정보사회에서 많은 사람들의 의식 속에 받아들여지고 있는 점은 부인할 수 없을 것이다.

개인정보의 보호는 개인에 관한 정보가 외부로 누설되는 것을 방지한다는 점에서는 정보를 가능한 한 널리 알리고자 하는 정보공개제도의 사고방식과 일견 대립적인 것처럼 보이지만, 이들 제도의 기초에는 정보에 대한 개인의 지배권을 강화한다고 하는 공통된 발상이 있는 점에 주의할 필요가 있다.

한 기록이 일종의 '전자 족적'으로 남게 되는 것을 우려하고 있는데, 이와 같은 첨단 교통량 측정장치의 사용기준을 법제화하는 것이 필요할 것이다.

정보의 자기결정권은 소극적인 사생활보호의 측면뿐만 아니라 정보공개요구권(또는 열람청구권)을 포함하는 개념인데, 여기서 정보공개요구권은 자신의 정보에 대한 국가기관의 무단한 이용을 막기 위한 소극적인 목적을 지닌다는 점에서 용어상의 혼란은 있으나 일반적인 정보공개청구권과는 구별되는 개념이다.

(2) 개인정보보호의 헌법적 근거

개인정보의 보호에 대한 현행 헌법상 근거는 제17조에서 찾을 수 있는데, 헌법 제17조는 「모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다」라고 규정하고 있다. 사생활의 보호조항은 제5공화국 헌법 개정시 신설된 조항으로 종래 개인의 인격과 관련된 정신적·물질적 피해를 입히는 일이 없도록 개별적인 통신의 자유·주거의 불가침 등 규정이 있었으나 사생활보호에 대한 일반적·포괄적 규정은 미비하여 신설되었다고 입법취지를 밝히고 있다.¹⁵⁷⁾

이러한 프라이버시권은 사생활 비밀과 자유의 불가침이라는 소극적인 내용에 한정되는 것이 아니라 ‘자신에 관한 정보를 관리·통제할 수 있는 권리’라는 적극적인 내용을 포함한다. 대법원은 헌법 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.”고 규정하고, 헌법 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”라고 규정하고 있는바, 이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다고 판시하고 있다.¹⁵⁸⁾

157) 법제처, 개정헌법의 주요내용(법제 No. 46, 1980. 9. 10.) 참조.

158) 대판 1998. 7. 24, 96다42789. 이 판결에 대하여는 제2장 II. 1. 일반적 인격권과 사생활의 비밀과 자유 참조.

2. 공적부문에서의 개인정보보호의 문제

(1) 주민등록증에 의한 개인정보의 문제

(가) 표준통일식별표(Standard Universal Identifier)

컴퓨터에 의한 인적 정보의 자동처리 및 데이터뱅크(Data Bank)간의 자료교환을 위한 연결망이 기술적으로 가능하기 위하여서는 그 정보주체인 개인은 다른 모든 사람과 구별되는 고유번호 또는 기호로써 특정되어야 한다. 수억, 수천만의 인구 중에는 동명이인이나 생년월일이 같은 자도 많으므로 사람을 특정할 수 있는 방법은 일련번호를 붙이는 방법이 가장 손쉬운 방법일 것이다.

표준통일식별표는 개인정보의 처리에 있어 정확성을 기하고 오류를 없애는 장점이 있으나 다른 면에서 개인을 효율적으로 감시하고, 개인의 프라이버시의 추적·탐색을 용이하게 한다는 큰 문제점이 있다. 만약 법에 의해 이 표의 휴대 및 제시가 강요된다면, 스스로를 노출시키고 다닌다고 할 수 있다. 출생과 동시에 부여되는 이 심벌은 사람을 평생동안 추적·기록하여 기록의 감옥에서 헤어날 수 없게 할 수 있다.

실제로 유럽에서는 사회보장의 증진의 차원에서 표준통일식별표가 있으나, 일본에서는 행정사무처리가 전산화함으로써 능률향상·사무처리의 정확·신속, 각종 자료의 종합적 이용, 각종 신고서의 간소화 등을 이유로 행정관리청이 중심이 되어 '사무처리용 통일개인코드'제의 실시를 계획하였다가 국민의 반대로 좌절되었고, 미국에서는 당초 사회보장 행정에 사용하기 위해 개인에게 사회보장번호를 부여하였으나 법적 근거도 없이 납세·운전면허·은행거래·외국인등록·학생등록 등에 광범하게 사용되어 신원을 증명하는 표준통일식별표의 역할을 하고 있으며 사생활보호에 우려의 요소가 되고 있는 실정이다.¹⁵⁹⁾

(나) 우리나라의 주민등록번호

1968년 121사태 이후 간첩색출을 목적으로 도입된 우리나라의 주민등록제도는 우리나라 국민 각 개인별로 주민등록번호를 부여하는데, 인구가 천만 단위인 우리나라에서 8자

159) 변재욱, 정보화사회의 프라이버시와 표현의 자유, 커뮤니케이션북스, 1996. 6. 160-162쪽.

리면 모든 사람에게 고유번호를 부여할 수 있으나 그 번호 속에 생년월일·최초 주민등록지·성별에 관한 정보를 수록하고자 하는 욕심에서 13자리로 길어졌다. 이러한 주민등록번호는 표준통일식별표로서의 기능을 하고 있다고 볼 수 있다.

대부분의 국가에서 신분증명서의 발급이 선택적으로 이루어지고 있는 데 대하여, 우리나라의 주민등록제도는 주민등록을 하지 않으면 법에 의해 처벌받는 강제등록원칙이다. 오로지 신분증명의 목적을 위하여 만들어진 우리의 주민등록증은 서비스제공을 주목적으로 만들어져 부수적으로 신분증명 기능을 갖는 미국이나 오스트레일리아의 의료보험증(Medicare Card)과 사회보장증(Social Security Card)과는 다르다고 할 수 있다.

또한 우리의 주민등록제도는 지나치게 많은 개인자료들을 요구하는데, 주민등록증에는 사진, 주민등록번호, 주소지, 거주지 변경사항, 지문 등이 실리며, 17세가 되어 처음 주민등록을 할 때 주민등록표상의 수록항목은 무려 141가지나 된다.¹⁶⁰⁾

주민등록번호는 행정기관에 제출하는 각종 신청서·신고서 등 모든 서류에 필수적으로 기재되며, 모든 증명서에 주민등록번호가 명시된다. 공공부문 뿐 아니라 학교·기업체·노동조합 등 사적부문에서도 널리 쓰인다. 우리들은 우리의 모든 정보를 강제 또는 반강제로 부지불식간에 공·사의 각종 데이터베이스(data base)에 쏟아 붓고 있는 것이다.

(다) 통합전자주민카드화 사업

정부는 1995년 행정의 효율화, 국민의 편의도모, 정보산업의 육성 등을 목적으로 현행의 주민등록증을 IC카드로 바꾸고 거기에 주민등록증, 의료보험증, 운전면허증, 국민연금, 주민등록초본, 인감증명, 지문의 7가지를 수록하는 다기능의 전자주민카드를 새로이 발급할 계획으로 사업을 추진했던 사실이 있다.¹⁶¹⁾

행정자치부가 추진하는 주민등록관리 입력항목을 보면 기본사항 23항목, 병력사항 16항목, 예비군 5항목, 인력동원 12항목, 자격면허 4항목, 생활보호 4항목, 의료보장 2항목 등 모두 78개 항목으로서 상당히 상세하게 구성되어 있어 만약 관계 공무원이 마음만

160) 전자주민카드 시행반대와 프라이버시권 보호를 위한 시민사회단체 공동대책위원회 홈페이지, <http://kpd.sing-kr.org/idcard>

161) 1999년 10월부터 전면 실시기로 계획되었던 이 사업은 특별한 이유 없이 행정자치부에서 주민등록증을 플라스틱으로 바꾸는 소규모사업으로 축소 실시하였다.

먹는다면 이것이 쉽게 외부에 유출되어 특정 개인의 신상이 광범위하게 공개될 우려가 없지 않다.¹⁶²⁾ 3천 4백만 명에 이르는 17세 이상의 모든 국민에게 중복이 없는 오직 한 사람에게만 있는 주민등록번호를 부여하고 많은 정보를 IC카드에 수록해서 국민에게 휴대·제시의 의무를 부과하는 전자주민카드제는 세계에서 처음 있는 일이다. 이 제도가 미래사회에 comtputopia를 실현한다고 하더라도 몇 가지의 개인정보가 한 기관에 집중돼 심각한 프라이버시 침해로 가져올 것은 분명하다고 생각된다.

(2) 영상감시

오웰(G. Orwell)의 소설 '1984년'의 'Big Brother'는 영상감시를 통해 사회 내 모든 개인을 통제하는 것으로 묘사되는데, CCTV(closed circuit television)를 이용한 감시는 범죄의 전자적 억제와 그 적발을 위한 것으로 우리나라에서도 은행, 지하철, 백화점, 도로, 교도소 등 수용시설 등에 활용되고 있다.

영상감시에 대해 그 효율성이 매우 높다고 하는 견해가 있는 반면 비판론자들은 CCTV에 의한 감시효과가 지나치게 강력하여 매우 위험스러우며 범죄예방을 목적으로 하여 개인의 프라이버시를 무제한적으로 침해하고 사회의 구석구석을 경찰이 감시하는 파놉티콘(Panopticon)¹⁶³⁾적 경찰만능의 사태를 낳을 수 있다고 한다.

은행이나 백화점에 설치된 CCTV는 범죄와는 아무런 관계도 없는 사람들까지 녹화하여 그 정보를 반영구적으로 저장·보관하고, 도로에 설치된 과속차량 단속카메라는 과속차량과 교통체증을 감시하는데 효과가 있을 수 있지만 운전자와 함께 동승한 사람의 얼굴까지 찍을 수 있으며, 작업장에 설치된 카메라는 작업현장을 파악하는데 도움이 되나 직원들은 자신들이 감시되고 있다고 생각하게 된다. 또한 영상감시와는 조금 개념이 다르지만 미국이나 영국에서는 수형의 한 방법으로서 전자감시제도¹⁶⁴⁾의 도입으로 Big

162) 변재욱, 정보화사회의 프라이버시와 표현의 자유, 커뮤니케이션북스, 1996. 6, 157쪽.

163) 파놉티콘은 1787년 Jeremy Bentham이 고안한 통제적 건축양식을 말하는 것으로 중앙에 원형의 탑이 있고 피수용자가 거주하는 방으로 구성된 링(ring) 모양의 건물이 탑을 둘러싸고 있는 모양인데, '보이지 않는 눈'이 언제나 재소자를 감시한다고 생각하기 때문에 통제가 유지된다. 이에 대하여는 정진수, CCTV에 의한 감시와 사회통제, 형사정책연구 제10권 제3호, 1999, 99쪽 참조.

Brother가 등장한 것이 아닌가 하는 우려를 낳고 있다.

그러나 현재 공공부문과 민간부문에서 폭넓게 사용 중인 CCTV에 의해 수집되는 개인정보에 대해서 아무런 법적 근거와 규제책이 없기 때문에 CCTV에 의해 개인의 권리가 침해되거나 재산적·정신적 피해를 받은 사람은 적절한 보상을 받을 수 없게 된다. 그러므로 CCTV의 설치·정보수집·이용·삭제 등 구체적인 절차에 대해 입법을 통해 적절한 법적인 규제를 하고, 이에 대한 감독기관을 지정하여 신고 또는 허가를 받은 후 정보수집 하도록 하는 것이 바람직하다고 보여진다.¹⁶⁵⁾

(3) 통신감청

감청은 수사기관이 타인의 대화를 본인 몰래 청취하는 것을 말하며, 물리적 강제력을 사용하지는 않지만 사생활의 비밀(헌법 제17조)이나 통신의 자유(헌법 제18조) 등의 기본권을 침해하는 강제수사로 공적부문에서의 개인정보 침해의 대표적인 유형이다. 감청 절차에 대해 규정하고 있는 통신비밀보호법은 통신 및 대화의 비밀과 자유에 대한 제한 대상을 한정하고, 엄격한 법적 절차를 거치도록 함으로써 통신의 비밀을 보호하는 데 그 목적이 있으며 보호의 대상이 되는 통신은 우편물과 전기통신을 말한다. ‘우편물’이라 함은 우편법에 의한 통상우편물과 소포우편물을 말하며, ‘전기통신’이라 함은 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음성·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다. 이와 관련하여 E 메일 등 컴퓨터통신이 전기통신에 포함되는지가 명확하지 않다는 이유로 수사기관은 E 메일 등 컴퓨터통신 감청의 경우 감청 영장과 압수수색영장 중 선택하여 청구할 수 있다고 보고, 수사편의를 내세워 대상범죄

164) 전자감시(electronic monitoring)란 범죄자의 행동을 특정 장소와 특정 지역 내로 제한하는 것으로 교도소에 수감해야 할 수형자를 재택구금하는 형식의 새로운 구금제도를 말한다. 현재 전자감시제도는 미국, 영국, 스코틀랜드, 프랑스, 이탈리아, 오스트레일리아, 캐나다, 이스라엘 등에서 채택되었다.

165) CCTV 등 영상감시의 문제는 오히려 민간영역에서의 소위 ‘몰래카메라’를 이용하여 개인의 사생활을 침해하는 것이 더 큰 문제라고 할 수 있는데, 이에 대해 1998년 12월 28일 ‘성폭력범죄의 처벌 및 피해자보호 등에 관한 법률’을 개정하여 의사에 반한 촬영행위에 대해 5년 이하의 징역 또는 1천만원 이하의 벌금형에 처하도록 하였다(제14조의 2).

등 허가요건이 상대적으로 엄격히 제한된 감청영장 대신에 일반 압수수색영장을 청구하는 경우가 많았던 것이 사실이다. 그러나 사이버 공간에서의 통신의 비밀도 보호되어야 함은 당연하다. 따라서 당사자의 동의 없이 컴퓨터통신 내용을 취득하는 것은 통신비밀보호법상의 전기통신 감청에 해당하는 것으로서 이를 위하여서는 반드시 법원의 감청영장을 발부 받아야 하는 것으로 보아야 할 것이다.¹⁶⁶⁾

통신비밀보호법의 제정으로 통신정보보호는 다른 영역에 비해 상대적으로 충실하게 될 수 있는 법적 토대가 마련되었다고 할 수 있다. 그러나 1994년부터 시행하고 있는 통신비밀보호법이 오히려 통신의 자유와 비밀을 합법적으로 침해하는 수단으로 역기능하고 있다는 비판이 있다.¹⁶⁷⁾ 현재의 통신비밀보호법은 범죄의 수사뿐만 아니라 범죄의 예방활동을 위해서도 감청을 허용하고 있으며, 허용이 되는 대상범죄가 너무 광범위하게 규정된 문제점이 있고, 감청을 당한 사람에게 사후에 그 제한사실과 근거 등을 통지하는 제도가 마련되어 있지 않아 정보의 자기결정권을 보호하지 못한다는 문제점이 있다.

(4) 인구조사

근대적인 기법을 갖춘 인구조사는 1925년부터 실시되었으나, 당시의 조사는 일제가 조선에서 노동력 착취 및 경제수탈을 위한 것이었다. 1948년 정부수립 후 정부는 각종 경제정책 수립을 위해 인구통계가 시급히 요구되어 1949년에 제1회 총인구조사를 실시하였고, 1966년에는 주택 총조사가 처음으로 병행 실시되는 등 매 5년마다 인구주택 총조사(소위 인구센서스)를 시행하여 왔고, 2000년 11월 1일부터 11월 10일까지 제11차 조사가 시행되었다.

2000년 인구주택 총조사는 인구 및 주택의 규모와 분포, 사회 경제적 특성을 파악하여 인구·주택에 관한 정책수립 뿐만 아니라 교통·환경·교육·에너지·지역경제의 개

166) 대법원이 이러한 취지에서 E 메일 등 컴퓨터통신 감청에 대한 법원의 심사를 강화하는 예규를 마련해 2000년 11월부터 시행에 들어갔음은 다행이라고 생각된다.

167) 수사기관의 감청허가 청구건수가 매년 500건을 넘고 있으며, 검찰의 감청허가 청구에 대해서 법원이 허가를 해준 비율이 지난 3년 동안 99.1%에 달하고 있는 것으로 볼 때, 수사기관이 수사의 편의만을 고려하여 감청허가 청구를 남발하고 있는 것은 아닌지, 또한 법원이 과연 엄격한 요건 하에 예외적인 경우에 한하여 감청허가를 해주고 있는 것인지 의문이 든다.

발 등 당면한 우리 사회의 제반 문제와 21세기의 지식정보화 및 복지사회 건설을 위한 국가정책 수립에 필요한 자료를 얻기 위함이라 한다. 2000년 인구주택 총조사에서는 인구나 주택의 기본사항 외에 시대상황 변화에 따라 총 50개 항목에 걸쳐 조사를 실시하였다.¹⁶⁸⁾

이 조사는 통계법 제4조 및 제8조의 지정통계에 관한 일반적 조항과 인구주택 총조사 규칙(부령 제143호, 2000.7.1)을 법적 근거로 하고 있으나 국민에게 수인의무를 부과하기 위하여서는 구체적인 근거법률을 제정하는 것이 바람직하다고 생각된다.

또한 개인별 조사내용은 통계법 제13조(비밀의 보호 등) 및 동법 제14조(통계작성사무종사자 등의 의무)의 규정을 통해 그 비밀이 엄격히 보호된다고 하나, 비밀에 속하지 않는 사항이라도 개인에 관한 정보가 아무런 제한 없이 통계작성 목적 이외의 용도로 사용되는 데 대한 법적 통제장치가 마련되어야 할 것이다.

(5) 출국자에 대한 신원조사

1970년 제정된 보안업무규정에 따르면 입국하는 교포를 포함하여 해외여행을 하는 자는 국가보안을 위한 신원조사의 대상이 되며, 신원조사는 '국가에 대한 충성심, 성실성 및 신뢰성'을 조사하기 위해 국가정보원장이 직권 또는 관계기관의 장의 요청에 의해 실시하는데, 신원조사사항에는 성명, 생년월일, 본적, 주소, 호주와의 관계, 본인 및 배우자사상관계, 보증인, 접촉인물, 정당, 사회단체 관계, 종교관계, 학력 및 경력, 가족관계, 재산관계, 상벌관계, 인품 및 소행, 병역관계, 해외여행 및 거주사실 등이 포함되어야 한다고 규정되어 있다.¹⁶⁹⁾

이 같은 신원조사제도는 그 정보수집의 목적이 매우 추상적이고 자의적이어서 목적명확성의 원칙에 어긋날 뿐 아니라 대상범위 또한 매우 광범위하고 개인의 기본권 인권을 침해하는 정보수집을 통해 출입국 사항을 실질적으로 통제한다는 문제점이 있다.

168) 2000년 인구주택 총조사의 조사내용은 인구에 관한 사항은 29개(전수조사 8개, 표본조사 21개), 가구에 관한 사항은 16개(전수조사 7개, 표본조사 9개), 주택에 관한 사항은 5개(전수조사 5개)이다.

169) 보안업무규정시행규칙 제56조.

(6) 기타

그밖에 공적부문의 개인정보 수집이 문제될 분야에는 경찰청에서 보관하는 17세 이상 전 국민의 지문자료, 범죄경력자료, 국세청의 수입품목자료, 외환거래자료, 외교통상부의 여권자료, 국민건강보험공단의 건강보험 관련자료, 노동부가 운영중인 고용관리시스템 등이 있다.

3. 외국의 개인정보보호법제

컴퓨터기술이 발달하고 정보통신이 발전함에 따라 유통되는 개인정보에 전 세계는 촉각을 곤두세우고 국가별로 규제정책을 마련하고 시행하고 있다. 미국, 캐나다를 중심으로 하는 자율규제 국가와 영국, 프랑스를 중심으로 하는 정부규제 중심의 국가가 서로 입장을 달리하고 있으나, 지금 세계 각 국의 개인정보보호 규제정책은 정부규제의 기본법을 토대로 민간주도의 자율규제를 시행시키는 방향으로 흘러가고 있다고 볼 수 있다.

(1) 스웨덴

스웨덴을 비롯한 북유럽 국가는 컴퓨터의 이용기술 및 보급이 미국과 서유럽 지역 국가 등에 비해 뒤늦게 발전하였으나 프라이버시 보호에 관한 입법조치는 이들 국가보다 앞서고 있다. 미국 등 주요 선진국이 대부분 1970년대에 들어 프라이버시에 대한 보호 논의가 있었으나 스웨덴은 1960년대부터 법적 보호논의가 있었고, 세계 최초로 1973년에 정보법(Data Act)이 제정되었다.

이 법의 특징은 국가기관으로서 옴부즈만적 성격을 가진 정보검사원(The Data Inspection Board)을 두어 프라이버시보호에 대한 사항을 결정하도록 하고 있는데 개인정보를 취급하는 공적·사적부문 모두가 이 법의 적용을 받도록 하고 있어, 많은 국가가 현재 까지도 공적부문만을 규제하는 점에 비추어 보면 매우 혁신적이라고 할 수 있다.

이 법의 주요 내용을 살펴보면

- ① 컴퓨터에 의해 처리되는 개인정보만을 규제대상으로 하고,

- ② 대부분의 개인정보 수집·처리에 정보검사원의 허가를 필요로 하고, 정보검사원은 불법행위자에 대해 공소제기를 할 수 있고,
- ③ 개인에 대한 열람청구권을 1년에 1회씩 무료로 인정할 책무와 잘못된 정보를 정정하고 그 결과를 개인에게 통지할 의무가 있으며,
- ④ 원칙적으로 개인정보의 개시·대출은 금지되고 국외전송이나 대출은 정보검사원의 허가가 있어야 하고,
- ⑤ 정보관리 업무종사자는 비밀준수의무가 있고 의무위반시 손해배상 및 형사처벌의 책임을 진다.

정보법은 시행초기의 문제점을 보완하여 1979년과 1981년에 개정이 되었으며, 그 운용실태는 정보검사원에서 국가의 중요 정보기관과 국방성까지도 상세하게 감사하는 등 그 실효를 거두고 있으나, 현행 정보법은 수작업에 의한 개인정보의 처리는 규제대상에서 제외된 문제점을 안고 있어 이를 포함하는 일반 프라이버시법(General Privacy Act)의 도입이 필요하다는 논의가 되고 있다.

(2) 독 일

독일은 개인 정보보호를 중요한 국가적 이슈로 인식하고 개인정보보호 지침을 공공부문과 민간부문에 걸쳐 적용하면서 급변하는 정보사회 속에서 개인정보보호를 위해 국가 주도로 철저한 노력을 기울이고 있다. 반인륜적인 유대인 학살이라는 쓰라린 역사를 가지고 있는 독일은 개인정보보호의 중요성을 일찍부터 깨닫고 1970년에 주정부 차원의 정보보호법을 제정·시행하였으나 국가차원의 연방법으로서는 1977년 「정보처리에 있어 개인에 관한 정보 남용방지에 관한 법률」을 마련함으로써 개인정보보호에 관한 포괄적인 법적 근거를 마련하였으나 이 법의 시행상 문제점¹⁷⁰⁾으로 인해 1991년 「연방개인정보보호법」(Bundesdatenschutzgesetz)을 제정하였다.

170) 이 법은 공적부문에 대한 개인정보보호를 그 대상으로 하여, 날로 늘어가는 민간부문의 개인정보처리에 대한 규제의 필요성이 크게 대두되었다.

이 법의 특징은 ① 법률의 적용범위에 있어 공공기관의 수작업자료를 포함한 개인에 관한 모든 정보를 적용대상으로 규정하고, ② 개인의 자기 정보에 대한 청구권, 정정권, 차단권, 삭제권 등의 권리를 보장하고 있으며 연방기관을 통한 권리구제절차를 규정하고, ③ 필요하다고 인정하는 범위에 한하여 개인정보를 수집하고 사용하도록 하는 목적 구속성의 원칙을 규정하고 있다.

독일의 개인정보보호법제의 특징은 정부가 개인정보보호의 중요성을 일찍부터 깨닫고 급변하는 정보사회의 물결에 순항하기 위해 여러 가지 지침 및 법안을 마련하여 정부의 적극적인 주도로 법제를 선도하고 있다는 점이다.

(3) 영 국

1960년대부터 프라이버시권의 보호를 위한 태동이 시작된 영국은 다른 선진국들보다는 비교적 늦은 1984년 「정보보호법」을 제정하게 되었다. 이 법은 공공·민간부문의 컴퓨터에 의해 처리되는 개인정보보호를 위한 법으로서 개인정보의 보호범위, 정보보호의 기본원칙, 정보보호 등록소 및 심판소의 설치, 개인정보처리의 등록 및 감독, 정보 주체로서의 정보정정권, 삭제권 행사의 한계 등을 규정하고 있다.

그러나 적용대상에서 컴퓨터에 의해 처리되는 개인정보만을 규정하고 실제 업무에 사용되는 수많은 수작업 개인정보를 제외시켜, 정부는 개인정보보호에 많은 어려움을 겪게 되었다. 이에 영국 정부는 1987년 컴퓨터에 의해 처리되는 개인정보는 물론 마이크로필름, 정보카드, 정보인덱스 등 수기처리정보도 적용대상에 포함하는 「개인정보접근법」(Access to Personal Files Act)을 제정하게 되었다.

그 후 기존의 정보보호법의 내용을 계승하면서 OECD의 「프라이버시 보호와 개인정보의 국제유통에 대한 가이드라인에 관한 이사회 권고」의 8개 원칙과 EU의 「개인정보의 자동처리에 따른 개인의 보호에 관한 조약」의 내용을 수용하여 정보처리에 보다 엄격한 「개인정보보호법」을 1998년 제정하였다.

이 법에서는 EU 회원국들간에 시행하고 있는 '정보보호등록관'(Data Protection Registrar)¹⁷¹⁾제도를 시행하고 있는데 개인정보를 수집·이용하고자 하는 업체나 개인은 정보등록소에 소유정보의 내용과 이용목적 등을 미리 신고하도록 하고 있고, 등록되

지 않은 개인정보는 결코 소유하거나 이용할 수 없도록 규정하고 있다. 또한 정보사용시 발생 가능한 분쟁의 중재역할을 담당하는 '정보보호심판소'(Data Protection Tribunal)¹⁷²⁾를 설치하도록 하고 있다.

영국의 개인정보 보호법제의 특징은 비록 법제화는 늦었으나 국제적으로 거의 공통적인 표준지침을 국내실정에 맞게 구체화하였다는 것이다.

(4) 미 국

정보보안에 어느 나라보다도 많은 관심을 갖고 정보보호관련 정책과 기술분야에 많은 투자를 해온 미국에서는 1970년대에 정보의 자유로운 흐름을 보장하는 취지의 정보자유법(The Freedom of Information Act)과 개인의 정보보호를 포괄적으로 규정하는 프라이버시법이 제정되었다. 그 이전의 개인정보보호법제는 공공부문과 민간부문을 포괄하는 법안을 제정하기보다는 필요에 따라 부분적이고 개별적인 입법조치를 취해 왔다.

1972년 Washington D.C.에 있는 민주당 본부 건물에 도청 장치를 해 정치적으로 커다란 문제를 야기 시켰던 워터게이트(Water Gate)사건 이후 미국 의회와 컴퓨터업계의 노력으로 연방행정기관의 개인정보 취급원칙을 규정하는 「1974년 프라이버시법」(Privacy Act of 1974)을 제정하게 되었다. 이 법에서는 기본적으로 헌법에서 보장하고 있는 사상, 종교, 표현의 자유와 같은 개인의 민감한 정보는 명확한 법률에 근거하거나 법집행 활동에 반드시 필요한 경우를 제외하고는 정보를 수집, 처리, 보관해서는 안 된다고 명시하고 있다.

그 후에도 정치, 경제, 의료, 통신 분야 등 각 분야별로 필요한 사항을 규정하는 「전자통신프라이버시법」(1986)과 산재해 있는 단편적인 개인정보를 보호하기 위한 「컴퓨터자료의 상호비교 및 프라이버시보호법」(1988), 전화나 팩스를 통한 불요청 광고메시지를 금지하는 「전화소비자보호법」(1991년) 등 필요에 따라 각 분야별 법제정으로 개인정보를 보호하고 있다. 즉 미국에서는 공적 영역을 규율하는 일반적인 개인정보보호법을 제

171) 정보보호등록관은 영국 여왕이 직접 임명하는 공무원으로 임기는 5년이다.

172) 정보보호심판소는 검찰총장과 협의 후 대법관이 임명한 의장과 주무장관이 임명하는 위원들로 구성된다.

정하지 않고 분야별로 규율하는 방식을 채택하고 있다.

(5) 일 본

일본은 1976년 정보보호 차원에서 「전자계산기처리 정보보호관리준칙」을 제정하면서부터 개인정보보호에 관심을 갖게 되었다. 그 후 공공기관의 개인정보 침해가 문제시되면서 행정기관의 컴퓨터를 통해 처리되는 개인정보에 관한 기본원칙과 개인의 접근권 및 통제권에 대해 규정한 「행정기관이 보유하는 전자계산기처리에 관한 개인정보의 보호에 관한 법률」을 1988년에 제정하게 되었다. 이 법에 열거된 개인정보보호에 관한 일반원칙은 자료수집제한의 원칙, 이용제한의 원칙, 개인참여의 원칙, 적정관리의 원칙, 책임의 원칙 등이다. 다만 이 법은 공공기관의 컴퓨터에 의해 처리되는 개인정보만을 보호 대상으로 규정하고 있어 아직 민간부문의 개인정보보호는 미비한 상태이다.

4. 개인정보보호법제의 국제적 동향

(1) OECD의 프라이버시 보호와 개인정보의 국제유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)

경제협력과 함께 국제적으로 유통되는 정보에 관심을 갖고 있던 OECD는 일찍부터 프라이버시 보호에 관한 지침 마련에 들어갔다. 1977년에는 비엔나에서 정보의 국제유통과 프라이버시 보호에 관한 회의를 개최하여 민간·공공부문을 망라한 개인정보의 유통실태와 문제점들을 파악하고 개인정보보호지침을 제정하였다.

그러나 많은 나라가 모인 협력기구인 만큼 각 나라 사정은 상이했고 정보보호 관련법 규도 미흡할 뿐 아니라 분야별로 필요에 따라 산발적으로 이루어지는 등 각 나라의 정보보호정책간 통일성이 결여된 상황이었다.

그 후 OECD는 산발적으로 이루어지는 정보보호정책을 통합하고 국가적, 지역적, 국제적인 정보유통질서를 확립하고자 1980년에 「프라이버시 보호와 개인정보의 국제유통에 대한 가이드라인에 관한 이사회 권고안」(Recommendation of the Council

concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data)을 제정하였는데, OECD의 개인정보보호 지침의 주요 내용을 살펴보면 다음과 같다:

- ① 수집제한의 원칙: 정보는 정보주체에게 알리거나 동의를 얻은 후에 수집하여야 하며, 합법적이고 공정한 절차에 따라 수집하여야 한다.
- ② 목적명확성의 원칙: 개인정보의 수집목적은 수집시 명확하게 밝혀져야 한다. 이후의 이용은 구체화된 수집목적과 일치하여야 하며, 목적 변경시 마다 명확한 목적을 명시하여야 한다.
- ③ 정보내용 정확성의 원칙: 개인정보는 그 이용목적에 부합하는 것이어야 하며, 정확하고 완전하며 최신의 것이어야 한다.
- ④ 이용제한의 원칙: 정보주체의 동의가 있거나 법률의 규정에 의한 경우를 제외하고는 목적명확성의 원칙에 따라 명확히 된 목적 이외의 다른 목적을 위하여 이용에 제공되어서는 안 된다.
- ⑤ 안전보호의 원칙: 개인정보는 분실, 부당한 접근·파괴·변형·공개 등의 위험으로부터 합리적인 안전조치에 의하여 보호되어야 한다.
- ⑥ 공개의 원칙: 개인정보의 존재 여부, 내용, 주된 이용목적, 정보관리자 등을 공개하여야 한다.
- ⑦ 개인참가의 원칙: 정보주체는 본인과 관련되는 정보의 존재 여부에 대한 확인, 열람, 정정, 삭제 등의 청구권을 가진다.
- ⑧ 책임의 원칙: 정보관리자는 위의 제 원칙의 원활한 준수를 위하여 각종 조치를 취해야 한다.

이 지침은 프라이버시 보호뿐 아니라 정보의 자유로운 흐름도 막지 않을 것을 목적으로 적용대상을 공공·민간부문을 초월한 특정 개인과 관련된 모든 정보로 규정하고 있다. 그리고 여기에서 밝힌 개인정보보호에 관한 8원칙은 OECD 회원 국가뿐만 아니라 우리나라, 일본을 비롯한 세계 각국의 개인정보보호법 제정에 중요한 모델이 되었다.

(2) EU의 개인정보의 자동처리에 따른 개인의 보호에 관한 조약(Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)

유럽연합 산하 단체인 각료회의 이사회(European Council)는 1995년 개인의 권리와 자유 및 프라이버시권의 보호원칙을 포함하는 개인정보의 자동처리에 따른 개인의 보호에 관한 조약을 체결하였다. 동 조약은 프라이버시의 보호와 유럽연합 국가 내에 정보의 자유로운 흐름을 지향하고 있다. 그리고 제정된 목적은 온라인 네트워크상의 개인정보보호만을 위해 제정된 것이 아니라 정치, 경제, 행정 등 개인정보가 수집, 처리되는 모든 영역을 규정하기 위해 제정되었다. EU의 개인정보보호에 관한 일반원칙을 살펴보면 우선 정보는 공정하고 합법적인 방법으로 수집되어야 하며, 구체적이고 정당한 목적을 위하여서만 저장되고, 이러한 목적과 양립될 수 없는 방법으로 사용되어서는 안되며, 저장 목적과 정보간에 적절한 관련성이 있어야 한다. 개인정보는 정확하고 최신의 것이어야 하며, 부정확하거나 불충분한 정보는 삭제되거나 수정되어야 한다. 정보는 저장되는 목적을 위하여 필요한 기간만큼만 보존되어야 한다. 그리고 정보주체의 명백한 동의가 있는 경우와 개인정보 처리가 계약 또는 법률상의 의무에 포함되는 경우 또는 정보주체의 기본적인 자유와 권리가 정보수집자의 법적 이익보다 중요하지 않으며 개인정보 처리가 이러한 법적 이익의 추구에 필수적인 경우에 한하여 개인정보의 처리가 가능하도록 규정하고 있다. 그밖에 대외적으로는 개인정보 보호대책이 기준 이상으로 충분히 정립되지 않은 제3국에는 정보주체의 명확한 사전동의를 있는 경우를 제외하고 모든 개인정보의 이전을 금지하고 있다.

5. 우리나라의 법제화 동향

(1) 법제의 특색

우리나라에서 개인정보에 대해 규정한 최초의 법률은 1994년 제정된 '공공기관의 개인정보보호에 관한 법률'이라고 볼 수 있는데, 이 법률은 국가 및 공공기관에 의해 처리

되는 개인정보를 그 대상으로 하여 범위가 제한적이라고 할 수 있어 그때 그때의 필요에 의해 개별 법규에 보호대상 정보를 규정하였는데, '신용정보의 이용 및 보호에 관한 법률',¹⁷³⁾ '금융실명거래 및 비밀보장에 관한 법률',¹⁷⁴⁾ '전기통신사업법', '통신비밀보호법', '전자서명법', '전자거래기본법', '의료법', '전산망보급확장과 이용촉진에 관한 법률'¹⁷⁵⁾ 등에 개인 관련정보의 보호에 대한 개별규정이 산재되어 있다.

(2) '공공기관의 개인정보보호에 관한 법률'

헌법상의 프라이버시권을 보장하기 위하여 각 국에서 개별입법을 하는 바와 같이 우리나라도 뒤늦게 공공기관의 개인정보보호에 관한 법률을 1994년 1월 7일 공포하여 1995년 1월 8일부터 시행하고 있다. 그 주요 내용을 살펴보면, 공공기관의 개인정보보호에 관한 법률은 공공기관에서 컴퓨터에 의하여 처리되는 개인정보를 대상으로 한다(법 제1조). 개인정보 중 사상, 신조 등 개인의 기본적 인권을 침해할 우려가 있는 정보에 대해서는 수집을 제한하고 있다(법 제4조). 국가기관은 기관의 업무를 수행하기 위하여 필요한 범위 내에서만 개인정보파일을 보유할 수 있도록 하였으며(법 제5조), 개인정보의 부당한 유출, 변조나 부정확한 정보로 인한 개인의 사생활침해를 예방하기 위하여 공공기관에 개인정보의 정확성과 안정성을 확보할 수 있는 대책을 수립하도록 하였다(법 제9조). 이 법에 따라 관련 개인은 자신의 정보에 관하여 열람을 청구할 수 있으며 잘못된 정보에 대한 정정을 청구할 수 있으며, 이러한 요구가 받아들여지지 않을 경우에 행정심판을 청구할 수 있다(법 제12조 아래).

1998년 12월 23일 공공기관의 개인정보보호에 관한 법률은 제1차 개정을 하였는데, 주요 내용은 정보를 제공하는 경우 그 요건을 강화하고, 개인정보 열람청구시 처리기간을 단축하고, 본인에 관한 정보열람을 용이하게 하는 등 개인의 권리를 일부 강화하는 것이었다.

173) 소비자의 개인정보 중 주로 신용과 관련된 정보에 대한 보호를 그 내용으로 한다.

174) 금융거래의 내용에 대한 정보 및 자료보호를 그 내용으로 한다.

175) 1999년 2월 개정된 이 법은 정보통신서비스 사업자에 의한 이용자의 개인정보 보호제도를 마련하였는데, 이 법 제4장에서 정보수집·취급·이용·제공 등을 규율하고, 정보주체의 자기정보 통제권을 강화하였다.

(3) 개인정보보호지침

정부에서는 정보통신 서비스 제공자와 정보통신 서비스 이용자의 개인정보를 적절히 보호를 목적으로 하는 개인정보보호지침을 마련하고 2000년 5월 1일 확정 공포하고, 한 달 동안의 준비기간을 고려하여 6월 1일부터 시행하고 있다.

이 지침에 따르면 서비스 제공자는 서비스 계약의 성립 및 이행에 필요한 최소한의 개인정보를 이용자의 동의 하에 수집해야 하고, 인종·민족, 사상·신조, 출신지·본적지, 정치적 성향·범죄기록, 건강상태·성생활 등 이용자의 기본적인 인권을 침해할 우려가 있는 개인정보를 수집해서는 안되며, 수집정보의 종류를 기본적인 필수항목과 부가적인 선택항목으로 구분해 필수항목 외에는 이용자가 정보수집에 선택적으로 응할 수 있도록 해야 하며, 사전에 ① 개인정보 관리책임자의 소속·성명·전화번호·기타 연락처, ② 정보의 수집·이용목적, ③ 정보를 제3자에게 제공하는 경우 제공받는 자와 제공목적 및 제공할 정보의 내용, ④ 동의·철회·열람·정정 요구 등 이용자의 권리 및 그 행사 방법, ⑤ 수집하고자 하는 개인정보항목 및 ⑥ 수집된 정보의 보유 및 이용기간을 고지해야 한다.

또한 이용자의 사전 동의를 받지 않으면 수집목적을 초과하여 개인정보를 이용하거나 제3자에게 제공할 수 없고, 개인정보가 분실, 도난, 누출, 변조 또는 훼손되지 아니하도록 안전성 확보를 위해 ① 비밀번호 등을 이용한 보안장치, ② 백신 프로그램을 이용한 컴퓨터바이러스 방지장치, ③ 암호알고리즘 등을 이용하여 네트워크상에 개인정보를 안전하게 전송할 수 있는 보안장치, ④ 침입차단시스템 등을 이용한 접근통제장치, ⑤ 기타 안전성 확보를 위하여 필요한 기술적 장치를 해야 하며, 정보의 수집목적은 달성한 때에는 종이에 출력된 개인정보는 분쇄기로 분쇄하거나 소각하고, 전자적 파일 형태로 저장된 개인정보는 기록을 재생할 수 없는 기술적 방법을 사용하여 삭제하는 등 지체 없이 파기하여야 한다.

서비스 제공자는 이용자가 자신의 정보에 대한 열람·정정을 요구하는 경우 필요한 조치를 취한 후 통보해야 하고, 상담창구를 통하여 이용자의 불만사항을 접수, 처리하고, 자체적으로 개인정보보호방침을 정하여 공개, 실행함과 아울러 관련 직원에 대한 교육 및 내부감사를 해야 하고, 개인정보 관리책임자를 지정 및 개인정보를 취급할 수 있는

자를 최소한의 인원으로 제한하여 지정하여야 한다.

또한 만 14세 미만의 아동으로부터 개인정보를 수집하는 경우는 법정대리인의 동의를 받아야 하고, 법정대리인은 정보제공자와 같은 권리가 있으며, 서비스 제공자 뿐 아니라 적법하게 서비스 제공자로부터 개인정보를 제공받은 2차 수집자나 위탁받아 개인정보를 관리하는 자, 대리점의 경우에도 위와 같은 절차를 준수해야 하며, 개인정보에 관한 분쟁이 있는 경우 한국정보보호센터 내 개인정보 분쟁조정위원회에 처리를 의뢰할 수 있다.

V. 경찰 정보처리활동의 변화 양태와 전망

1. 경찰 정보처리 영역의 확대

(1) 양적인 증가

경찰의 자체적인 정보기반의 확대는 경찰업무의 효율성을 획기적으로 개선하여 경찰 목적 달성에 크게 기여할 것이 분명한 반면에 개인정보의 침해 우려 또한 그에 따라 증가할 것이므로 양자의 적절한 조화가 주요한 과제가 될 것이다. 경찰은 1994년 이래로 계속되어온 경찰종합정보체제를 통하여 전 업무부서의 주요 업무에 대한 통합전산화 작업을 하였고, 특히 범죄수사 영역에서 사건수사활동의 상당부분을 일선 수사관의 개인컴퓨터에 연결된 전산망을 통하여 가능하도록 하는 등의 이용범위를 확대하고 있고, 공안 전산망과 행정전산망을 일부 통합하는 등 보유자료의 효율성을 향상시키기 위해 노력하고 있다. 경찰종합정보체제에서 나아가 개별적으로 이루어지던 경찰업무 정보화를 효율적으로 추진하기 위하여 2000. 4. 주요 정보화 작업의 비용절감을 위하여 통합을 주요 내용으로 하는 개선방안을 마련하는 등 일련의 작업을 통하여 정보처리의 양이 급격히 증가할 것이다.

또한 업무처리에 있어서도 정보화를 통해 사회활동이 점차 비대면적인 관계에 있게 됨으로써 경찰의 활동 또한 개인을 대면하지 않고 각종 데이터를 수집, 조회하는 등 처리업무가 급격하게 증가하게 될 것으로 예상된다.

(2) 질적인 변화

공공부문의 정보망의 연동은 비용절감과 행정의 효율성을 제고하기 위한 필수적인 과정이기도 하나 대부분의 정보가 '이차적 자료'(second-hand date)의 성격을 띠게 됨으로써 새로운 정보를 창출하는 효과를 발생시키기도 한다. 위에서 언급한 컴퓨터에 의한 인적 자료의 검색·조사의 경우가 대표적인 예라고 할 수 있다. 정보처리기술의 발전으로 대용량 자료의 효과적인 검색작업이 가능해 짐으로써 이를 통하여 종래의 단편적이

고 폐쇄적인 전산망의 단순한 조희에서 나아가 컴퓨터 매칭 등 기술을 활용한 새로운 정보처리 방법의 사용이 증가할 것으로 보인다.

위와 같은 컴퓨터를 이용한 정보의 처리는 경찰업무의 효율성을 높이지만 개인의 정보에 대한 권리를 침해할 우려를 증가시키기도 한다. 반면에 역감시적 절차로써 컴퓨터 기록의 관리를 통하여 경찰활동에 대한 감시를 가능하게 하고 이것은 경찰활동의 적법성을 담보하는 장치로써 작용할 수 있다.

2. 새로운 과학적 수단의 등장

컴퓨터 등 자동화된 정보처리 장치를 이용한 새로운 과학적 경찰수단은 급격한 발전 과정 중에 있다. 예컨대 자동지문검색시스템(AFIS)과 같은 새로운 경찰의 수단은 대부분 정보처리장치의 발전과 함께 하고 있다고 볼 수 있다. 이러한 새로운 과학적 수단의 예는 상당히 많은데 새로운 정보수집장치로서 전자감시장치, 유전자지문은 대표적인 논란의 대상이라 할 수 있다.

(1) 전자감시장치

국내에서 이미 활용하고 있거나 활용되고 있지 않지만 논의의 대상이 되고 있는 전자감시장치로는 기능별로 사람의 위치를 확인하거나 행동을 추적하는 장치, 전화번호의 다이얼링 추적이나 자동기록 등의 감시장치, 음성통신의 도청이나 디지털통신의 도청, 시각 감시장치 등으로 구별할 수 있다.¹⁷⁶⁾ 구체적인 예로는 CCTV, 야간감시기구와 영상강화장치, 전기스펙트럼 진동장치를 이용한 극대확성장치, 신호발신장치, 전화 도청 및 녹음장치, 발신자 식별장치, 컴퓨터 통신 감시기, 무선도청기, 위성전파 감시기, 표적 감지 시스템, 진동·초음파·적외선을 이용한 검파기 등이 있다. CCTV를 예로 볼 때, 프라이버시에 대한 합리적 기대가 있는 장소를 제외한 공공장소의 경우, 상호교환적 행위의 일방 당사자의 동의가 있는 경우 특별한 영장 없이 영상감시를 할 수 있다고 해석하

176) 최영호, 컴퓨터와 범죄현상, 컴퓨터출판, 1995. 7, 153쪽.

고, 그렇지 않은 경우에 이를 CCTV의 활용을 형사소송법상의 검증으로 보아 법관의 검증영장을 필요로 한다는 학설이 지배적이다. 그러나 이에 대한 현행법상의 규율은 충분하지 않으며, 대부분의 다른 수단들은 그러한 법적인 논의의 대상조차 되지 못하고 있는 형편이므로 이를 통제할 수 있는 새로운 형태의 입법적 변화를 필요로 한다.

(2) 유전자지문(DNA Fingerprint)

유전자지문은 사람의 혈흔, 혈액, 정액 및 정액반, 모발, 기타 장기조직편 등에서 검출이 가능한 사람의 유전자 정보에 대하여 유전자 감식기법(Deoxyribo Nucleic Acid Method)을 통하여 사람의 동일성을 식별하는 것을 가능케 한다.

경찰청의 지문검색시스템이 ‘형의 실효등에 관한 법률’ 및 ‘지문을 채취할 형사피의자의 범위에 관한 규칙’에서 정한 형사피의자에 대하여 작성된 범죄피의자 지문을 대상으로 동일인의 판단을 위한 대조뿐 아니라 일반적인 검색까지 가능토록 하여 범죄수사 및 사망자의 신원확인 등에 활용되고 있음에 반하여 유전자지문은 위와 같이 사람의 신체조직을 대상으로 하므로 현재 국립과학수사연구소와 대검찰청 유전자 감식실에서 동일인 대조로만 활용하고 있다. 범죄자를 대상으로 한 유전자 지문 작성을 위한 강제채혈의 허용 여부 등에 대하여 새로운 논란이 제기되고 있다.

3. 시민저항운동의 확대

경찰 등 국가기관의 정보화를 기반으로 한 전자감시활동 등 정보처리 영역의 확대를 우려하는 것은 학계나 개별적인 당사자의 문제를 벗어나 적극적인 시민저항운동의 형태로 확대되고 있다. 정보의 자기결정권 또는 자기정보통제권을 개인정보에 대한 ‘유통’을 통제하는 것에서 개인정보의 ‘수집(생산) 자체’에 대한 통제의 권리로 재구성하고 그 대상을 ‘자기와 관련되는 모든 정보’로까지 확대하는 것 등을 주요 내용으로 하는 ‘역감시의 권리’에 대한 주장,¹⁷⁷⁾ 시민단체가 주도하여 주민등록법에 근거한 지문날인 제도에

177) 홍석만, 자기정보통제권에서 역감시의 권리로, 동아일보, 2000. 6. 4.

대하여 반대하면서 제기한 주민등록법 제17조의 8 등에 대한 헌법소원,¹⁷⁸⁾ 새로운 주민등록증을 발급 받기를 포기하면서 지문날인거부운동을 벌이는 사람들의 연대¹⁷⁹⁾ 및 관련 시민단체들의 홈페이지 운영 등 다양한 방법의 시민저항운동 형태로 새로운 정보처리 수단에 대하여 비판하고 있으며, 제도적인 정비가 이루어지지 않는 한 이러한 경향은 점차 확대될 것으로 생각된다.

4. 소 결

경찰의 컴퓨터 등 정보처리장치를 활용한 정보처리는 양적·질적인 급속한 팽창의 단계에 있고, 새로운 과학적 경찰수단의 발달과 함께 경찰목적 달성을 위한 적극적인 활용이 예상된다. 새로운 정보처리 활동은 공공의 안녕과 질서를 유지하기 위한 경찰목적 달성을 위하여 필수적인 반면에 개인의 정보적 자기결정권에 대한 침해의 우려를 내재하고 있는 양면성이 있으므로 양자간의 조화가 필요하다. 그러나 새로운 정보처리 방법의 규율은 일부 법규에서만 규정되어 있을 뿐, 대부분은 경찰의 자체적인 행정규칙에¹⁸⁰⁾ 의하여 관리되고 있는 등 미비한 점이 많아 이에 대한 정비가 시급하게 요구된다.

경찰의 정보처리 활동의 강화에 반대하는 시민의 적극적인 저항운동이 확대되고 있고, 새로운 사회문제로 제기되고 있는 바, 위와 같은 새로운 정보처리 활동에 대한 입법적인 흠결은 논란을 야기하는 근본적인 원인중의 하나라고 생각된다.

178) 인권실천시민연대 사무국장 오창익과 사회진보연대의 홍석만은 1999. 9. 28. 주민등록법 제 17조의 8 등 위헌확인청구 헌법소원심판을 청구하였다.

179) 이와 관련된 신문기사로는 '국민의 손가락을 탐하지 말라' 주민증 지문찍기 첫 거부운동(한겨레신문, 1999. 7. 13.), '주민감시 주민증은 싫어'(한겨레신문, 2000. 6. 3.) 등이 있다.

180) 예컨대 경찰청 소관 전담관리 대상자료의 수집, 정리, 보존, 관리 및 지원에 관하여 필요한 사항을 규정하고 있는 국가정보자료관리규정시행규칙(1995. 10. 2, 경찰청 예규 제151호)와 기록정리의 세부절차를 규정하고 있는 국가정보자료관리규정시행정리규칙(1995. 12. 21, 경찰청 예규 제161호) 등을 들 수 있다.

제5장 결론 : 효율적인 치안정보 관리를 위한 입법적 제안

경찰작용은 그 자체 개인에 관한 정보를 수집하기 위한 것이거나 또는 그 작용을 위한 준비수단으로써 개인에 관한 정보를 수집하게 되는 경우가 대부분이다. 예를 들어 일반적인 순찰활동은 위험발생의 예방차원에서 거리에서 개인 등의 정보를 수집하는 과정이고, 불심검문은 좀 더 구체적인 범죄와 관련된 정보를 얻기 위한 것이며, 불심검문을 통하여 범죄혐의가 있는 자를 발견하게 되면 범죄수사를 개시하게 되는데 그야말로 범죄수사는 범죄혐의자에 대한 개인정보를 수집하는 것 자체라고 할 수 있을 정도로 정보와 밀접한 관련이 있다. 그러나 우리나라의 정보보호법은 컴퓨터로 처리되는 공공기관 등의 개인정보에 관한 사항만을 규율하고 있으므로 경찰의 정보처리의 극히 제한적인 부분만을 이 법을 통하여 규율할 수 있을 따름이다. 물론 입법정책적인 관점에서 정보처리에 관하여 일반적인 규정을 두지 않고도 다른 경찰작용과 중첩되는 개별적인 영역에 관하여 규율하면서 정보보호적인 내용을 포함시키고 해석하는 방법을 취하는 것도 가능하며, 현재 우리나라의 법제도 그러한 방향으로 되어 있다고 볼 것이나 정보보호의 필요성이 매우 강조되는 추세이고, 개별적인 영역에서의 규율은 명백한 한계를 지니고 있다는 점, 개별영역으로 규율되지 않은 부분에 관한 논란을 제공할 소지가 있다는 점에서 바람직하지 않은 것으로 보인다. 따라서 우리나라에서도 독일의 경우처럼 경찰의 정보처리에 대한 자세하고 구체적인 규율을 두는 것이 필요할 것이다. 아래에서는 경찰의 정보처리에 대한 입법에 있어서 고려해야 할 사항을 살펴보기로 한다.

I. 정보처리에 관한 일반적인 규정

1. 경찰의 직무범위

경찰의 직무에 대하여는 경찰관직무집행법 제2조 및 경찰법 제3조에 규정하고 있다

즉 경찰관직무집행법 제2조에서는 ① 범죄의 예방·진압 및 수사, ② 경비·요인경호 및 대간첩작전수행, ③ 치안정보의 수집·작성 및 배포, ④ 교통의 단속과 위해의 방지, ⑤ 기타 공공의 안녕과 질서유지를 경찰관의 직무범위로 규정하고 있다. 또한 경찰법 제3조는 “경찰은 국민의 생명·신체 및 재산의 보호와 범죄의 예방·진압 및 수사, 치안정보의 수집, 교통의 단속 기타 공공의 안녕과 질서유지를 그 임무로 한다”라고 규정하고 있다.

그러나 이 조항은 너무나 일반적으로 규정되어 있어 이를 구체적으로 명확하게 규정할 필요가 있다. 참고로 독일의 ‘통일경찰법모범초안에 대한 개정초안’ 제1조 1항에서는 경찰은 공공의 안녕·질서에 대한 위협방지 업무를 수행한다고 하면서, 이 범위 내에서 범죄행위가 발생한 경우에 형사소추에 대비하고 범죄행위의 발생을 예방하며(이른바 ‘예방적 범죄투쟁’) 및 장래의 위협을 방지하기 위하여 준비하여야 한다고 규정하여 경찰의 직무범위를 명확하게 규정하고 있다. 이 규정에 의하여 범죄행위를 범할 우려가 있는 자에 대한 정보와 장래의 범죄행위의 발생을 방지하기 위한 정보를 수집하며, 또한 장래의 위협발생에 대비하기 위하여 정보를 수집하는 것이 경찰의 직무범위에 속함이 명확해 진다.

그러나 이러한 규정은 경찰의 직무범위를 확정하는 것으로 그러한 직무수행에 의한 기본권의 침해는 정당화해 주는 것은 아니다. 즉 법률유보원칙에서 요구하는 침해의 수권규정은 아닌 것이다. 기본권 침해의 수권규정은 따로 규정하여야 한다. 독일의 ‘통일경찰법모범초안에 대한 개정초안’에서는 제8조 이하에서 수권규정을 두고 있다.

우리나라의 경우 지금까지 경찰은 경찰법 제3조 및 경찰관직무집행법 제2조의 ‘치안정보의 수집’ 규정에 의하여 또는 정보수집이 경찰의 직무수행에 당연히 내재하는 것으로 보아 직무에 대한 규정을 근거로 여러 가지 정보수집활동을 수행해 왔는데, 경찰 정보수집의 범위를 명확히 할 필요가 있으며, 그로 인한 개인의 권리 제한 및 침해에 대한 수권 규정을 두는 것이 개인의 기본권보장과 법치주의원칙, 특히 법률 명확성의 원칙 및 법률유보원칙에 부합하는 것이 될 것이다.

2. 다른 행정기관과의 관계

공공의 안녕·질서의 유지작용 모두가 경찰의 직무범위에 속하는 것은 아니다. 예컨대 위생·건축·산업 등과 관련하여 발생하는 공공의 안녕·질서에 대한 위협의 경우처

럼 다른 행정작용에 관련해서 일어나는 위험을 방지하는 것은 경찰기관이 아닌 다른 행정기관의 권한으로 규정되어 있다. 그런데 해당 행정기관이 적시에 위험방지업무를 수행하지 못하는 경우에 그러한 위험상태를 방치할 수도 없는 긴급한 경우에는 보충적으로 경찰이 위험방지업무를 수행할 수 있어야 할 것이다. 이에 대한 명문 규정이 필요하며, 또한 이와 관련된 정보수집 및 처리에 대하여도 명확한 규정을 두어야 할 것이다.

참고로 독일의 '통일경찰법모범초안에 대한 개정초안' 제1a조에서는 경찰과 다른 행정기관의 관계에 대하여 규정하고 있다. 이에 의하면 경찰은 다른 행정기관의 직무에 속하는 위험방지가 적시에 행해지기 어렵고 위험방지를 위한 조치가 불가피한 경우에는 그 방지활동을 할 수 있으며, 이러한 경우 경찰은 즉시 다른 행정기관에게 그 기관의 업무수행을 위하여 중요한 의미가 있는 모든 과정을 보고하도록 되어 있다. 다만 위험방지 업무수행을 통해 경찰이 획득한 개인관련 정보가 있는 경우에 이를 다른 행정기관에 전달하기 위하여서는 정보제공의 요건을 충족하여야만 한다.

3. 비례의 원칙

경찰법상 명문규정이 없더라도 비례의 원칙은 법치국가원리의 한 구성부분으로서 헌법적 지위를 갖고 모든 국가작용에 적용된다. 경찰작용은 주로 개인의 자유의 제한을 내용으로 하기 때문에 비례의 원칙은 경찰권의 발동에 있어서 특히 중요한 의미를 갖는다. 그러한 이유로 경찰관직무집행법 제1조 2항은 「경찰관의 직권은 그 직무수행에 필요한 최소한도 내에서 행사되어야 하며 이를 남용하여서는 아니 된다」고 하여, 경찰권발동에 있어서의 비례원칙을 명시적으로 규정하고 있다. 그러나 더 나아가 비례원칙의 구성요소인 수단의 적합성의 원칙, 필요성의 원칙(또는 최소침해의 원칙), 좁은 의미의 비례원칙(또는 상당성의 원칙)을 구체적으로 표현하는 것이 명확성의 관점에서 바람직 할 것이다.

비례의 원칙이 경찰의 정보처리에 있어서 적용되어야 함은 당연하다. 비례의 원칙은 정보처리에 관한 법률규정의 해석과 구체적 적용에 있어서 그 의미를 가진다. 그러나 비례의 원칙이 중대한 의미를 가지는 것은 오히려 정보처리에 관한 규정에 흠결이 있는 경우일 것이다. 예를 들면 어떠한 정보가 수집될 수 있는지에 대하여 아무런 법규정을 두고 있지 않은 경우에, 비례의 원칙이 적용되는 결과 부담적이거나 개인의 사생활에 속

하는 정보는 자의적으로 수집되어서는 안 되고 개별적인 경우에 그에 대한 필요성의 심사 후에 수집될 수 있는 것이다. 다시 말하면 필요성의 원칙에 따라 정보처리는 특별한 규정이 없더라도 적법한 직무수행을 위하여 필요한 범위 내에서만 허용된다.

수단에 의하여 달성하려는 목적보다 그로 인한 불이익이 더 커서는 안 된다는 좁은 의미의 비례원칙으로부터 저장의 필요성이 크지 않거나 경찰책임자 또는 혐의자가 아닌 일반인에 대한 정보의 저장이 문제되는 경우에, 개인의 인격을 나타내거나 개인의 사생활에 속하는 정보는 저장되어서는 안 된다는 결론이 도출된다.

자동화 장치에 의하여 저장된 정보의 경우 수작업에 의하거나 서류의 형태로 저장된 정보보다 이용될 가능성이 높고 그에 따라 위협에 노출될 가능성이 많기 때문에 저장의 형태를 선택하거나 서류형태를 자동화된 데이터로 저장방식을 바꿈에 있어서 그에 대한 판단이 저장기관의 자의에 맡겨져서는 안 된다. 정보처리의 자동화는 수행해야 할 직무와 관련자의 보호법익을 고려할 때 그것이 적합한 경우에만 고려될 수 있는 것이다.

II. 개별적인 정보처리 시 준수해야 할 원칙

1. 정보수집

(1) 정보수집에 대한 수권조항

정보수집에 대한 명확한 수권규정을 둘 필요가 있다. 경찰은 직무수행을 위하여 필요한 경우에는 개인정보를 수집할 수 있다고 일반적인 수권조항의 형식으로 규정하고, 정보수집의 대상자 및 정보수집의 종류·형태에 대한 자세한 규정은 하위 법령에 위임하면 될 것이다. 정보수집의 범위와 관련하여 경찰은 목적달성을 위하여 필요한 범위 내에서 개인정보를 수집할 수 있음은 비례의 원칙이 적용되는 결과 당연한 것이다.

관련자의 자유로운 진술에 의하여 정보를 수집하는 것은 침해에 해당하지 않으므로 이를 위하여 수권규정이 필요하지는 않다. 그러나 관련자에 대한 정보를 제3자로부터 수집하는 것은 정보의 자기결정권에 대한 침해에 해당하므로 수권규정이 있어야 한다.

정보수집의 권한규정으로부터 당사자의 정보제출의무가 도출되는지에 대하여는 논란의 여지가 있으므로 법적 명확성의 관점에서 정보제출의무의 요건에 대하여 규정할 필요성이 있다.

(2) 정보수집의 일반원칙

개인정보는 원칙적으로 공개적이며 관련자로부터 수집되어야 한다는 정보수집의 원칙이 규정되어야 한다.¹⁸¹⁾ 다만 예외적으로 관련자로부터 수집하는 것이 불가능하거나 또는 과도한 비용이 요구되는 경우와 다른 방법으로는 경찰의 직무수행이 현저히 곤란하게 되는 경우에 한하여 개인정보를 다른 행정기관, 공공단체 또는 제3자로부터 수집하거나 또는 은밀한 방법으로 수집할 수 있다는 규정을 두어야 한다.

정보의 자기결정권은 모든 사람에게 자신에 대한 정보제공에 대하여 스스로 결정할 권리를 부여한다. 제3자로부터의 정보수집은 특별히 중요한 사유가 존재하는 경우에만 고려될 수 있다. 간편함 또는 행정의 간소화 등의 사유만으로는 기본권 침해가 정당화시킬 수 없다. 구체적인 경우에 일반적인 비례원칙의 적용이 고려되어야 한다. 제3자로부터 정보수집의 허용 여부는 정보의 종류·내용에 따라 달리 판단하여야 한다. 예컨대 위험상황에 대비하기 위하여 수집되는 정보와 같이 비교적 무해한 정보의 경우에 있어서는 질병, 특별한 행동양식 또는 사생활에 관한 정보와 같은 민감한 정보의 경우보다 제3자로부터 수집되는 것에 대한 허용가능성이 크다고 할 것이다.

원칙적으로 정보수집은 공개적으로 행해져야 한다. 공개적이라 함은 자기에 대한 정보수집에 관하여 관련자가 알고 있어야 함을 의미한다. 정보수집 시에 관련자는 정보제공의 의무가 있는지 또는 정보수집에 자발적으로 응할 수 있는 것인지에 대하여 알고 있어야 한다. 정보수집에 동의하는 경우 공개성의 요구는 충족되는데, 동의를 하기 위하

181) 대법원도 군 정보기관이 법령에 규정된 직무범위를 벗어나 민간인을 대상으로 평소의 동향을 감시·파악할 목적으로 지속적으로 개인의 집회·결사에 관한 활동이나 사생활에 관한 정보를 미행, 망원 활용, 탐문채집 등의 방법으로 비밀리에 수집·관리하였다면, 이는 헌법에 의하여 보장된 기본권을 침해한 것으로서 불법행위를 구성한다고 판시하고 있다[대판 1998. 7. 24. 96다42789].

여서는 관련자가 자기에 대한 정보수집의 목적과 범위에 대하여 알고 있는 것을 전제로 하여야 한다.

공개적인 정보수집의 원칙은 개인의 정보적 자기결정권과 관련하여 중요한 의미를 갖는다. 은밀한 정보수집은 정보의 자기결정권에 완전 배치되는 것이다. 은밀한 정보수집이 아니라면 경찰의 직무수행이 곤란해진다라는 단순한 사실만으로는 그를 허용하는 충분한 근거가 될 수 없다. 경찰직무의 수행이 거의 불가능해 진다거나 비공개에 의한 정보수집이 예외적으로 관련자의 이익에 합치되는 경우에만 고려될 수 있을 뿐이다. 그러나 이로부터 은밀한 정보수집에 대한 명확한 한계를 도출할 수 있을지는 의문이다. 개별적인 경우 비공개에 의한 정보수집을 필요로 하는 직무의 중요성과 관련자의 이익이 비교형량 되어야 한다. 비교형량 함에 있어서는 정보의 종류가 중요한 의미를 갖는다. 또한 형량에서는 은밀한 정보수집이 장기적으로 시민과 경찰의 관계에 어떠한 영향을 미칠 것인지가 고려되어야 한다. 경찰에 대한 신뢰는 경찰의 원칙적인 공개성을 전제로 한다. 공개는 민주국가의 본질적인 요소이다.

정보의 자기결정권에 대한 침해를 완화하고 권리보호를 위한 방안으로 저장기간이 3년을 넘게 되면 관련자에게 그 사실을 통지하도록 하는 것을 고려해 볼 수 있다.¹⁸²⁾ 그 밖의 경우에는 은밀한 수집의 사유가 소멸된 이후에 비례의 원칙에 따라 관련자에게 사후에 통지하는 것이 필요한지 여부가 심사되어야 한다. 비공개 수집이 관련자의 이익을 위하여 행해진 경우에는 그에게 통지될 수 있는 것이다.

(3) 공개된 행사, 모임 및 집회에서의 정보수집

평화적인 집회·시위도 경우에 따라서는 감정의 자극 등에 의하여 폭력적인 집회·시위로 발전되는 경우가 많다. 이러한 경우에 경찰은 비디오 카메라 등을 사용하여 그 현장을 촬영하고 그에 의하여 폭력행위자 등을 선별하게 되며 이후 형사소추에 있어서 증거자료로 활용하게 된다.

182) 이러한 입법례로는 헤센의 경찰법 제20조 9항 참조. 슬레스비히-홀슈타인에서는 정보가 공개적으로 수집되지 않은 경우에 그 저장에 대하여 관련자에게 알려주도록 하고 있다(§ 178 Abs. 2 SHLVerwG 참조).

경찰이 공개된 행사, 모임 또는 집회를 단순한 관찰자의 눈으로, 망원경에 의하여 또는 사진촬영이나 녹음에 의하여 감시하는 것은 단순한 사실행위로서 침해에 해당하지 않는다. 그러나 그에 의하여 특정인의 신원을 확인할 수 있게 된다면 특별한 법적 근거가 필요한 침해에 해당한다. 따라서 이에 대한 법적 근거로서 경찰은 공개된 행사, 모임 및 집회에서 또는 그와 연장선상에서 주위의 사정을 합리적으로 판단하여 범죄행위 또는 중대한 질서위반행위를 하려 하고 있다고 의심할 만한 상당한 이유가 있는 자에 대하여 사진촬영, 비디오녹화 또는 녹음을 할 수 있다는 규정을 두어야 한다. 또한 그에 의한 필름 및 녹화·녹음테이프와 그로부터 수집한 개인정보는 형사소추 또는 질서위반행위의 조사를 위하여 필요한 경우와 법적 분쟁의 대상이 되는 경우를 제외하고는 늦어도 2개월이 지난 후에는 삭제되어야 한다는 점이 규정되어야 한다. 공공의 안녕·질서에 대한 위험이 발생하지 않은 경우에 행사, 모임 및 집회에서 수집된 자료는 삭제되어야 할 것이다.

2. 정보의 처리

(1) 저장 및 목적구속의 원칙

개인정보의 저장과 이용은 수집목적에 위하여만 허용됨을 분명히 하여야 한다. 개별적인 경우에 있어서 목적이 무엇인지가 밝혀져야 한다. 경찰의 일반적인 직무영역인 위험방지, 범죄수사 및 예방의 영역에서 그 목적이 자세하게 구체화되어야 한다. 예를 들면 위험방지영역에서 '증인'으로서 어떠한 사람에 대한 정보가 수집된 경우, 비록 위험방지의 목적을 위한 것이라 하더라도 '경찰책임자'로서의 정보로 저장되어서는 안 된다. 마찬가지로 범죄수사의 영역에 속하지만, 접촉한 사람으로서의 정보를 범죄혐의자의 정보로 이용하여서는 안 된다.

다만 정보가 다른 목적으로도 수집될 수 있었던 것이라면 다른 목적으로 저장되는 것이 허용될 수 있어야 할 것이다.¹⁸³⁾ 정보가 다른 목적으로 수집될 수 있었으나, 즉 수집

183) 이러한 독일의 입법례로는 § 20 Abs. 3 S. 2 HSOG, § 22 Abs. 1 SOG LSA, § 37 Abs. 2 PolG BW, § 42 Abs. 2 ASOG Berl 참조.

당시의 시점을 기준으로 허용성 여부를 판단하여야 할 것이다. 그밖에 ‘동일한 수집방법’으로 수집할 수 있었느냐도 허용성을 판단함에 있어서 고려하여야 한다.

정보의 저장과 관련하여 목적구속의 원칙 이외에 비례의 원칙도 중요한 의미를 갖는다. 즉 비례의 원칙에 따라 정보의 저장기간은 필요한 범위로 제한되어야 한다. 이를 위하여 정보의 저장이 계속해서 필요한지 여부에 대하여 정기적으로 심사해야 한다. 저장의 필요성에 대한 심사결과에 따라 정보를 계속 저장할 것인지 또는 삭제할 것인지가 결정되어야 한다.

(2) 아동에 대한 정보의 저장

아동¹⁸⁴⁾에 대한 정보의 저장에 대하여는 특별규정을 둘 필요가 있다. 저장기간을 제한한다거나,¹⁸⁵⁾ 고지에 의하여 직무수행이 현저히 곤란해지는 경우가 아니거나 또는 고지가 해당 아동에게 중대한 불이익을 가져다주는 것이 아닌 한, 보호자 또는 후견인은 아동정보의 저장에 대하여 고지를 받아야 한다는 등의 규정을 두는 것을 생각해 볼 수 있다.

이러한 규정을 두는 것이 오히려 경찰은 일정한 유보 하에 아동에 대한 정보를 아무 어려움 없이 저장할 수 있다고 생각을 야기할 수도 있을 것이다. 그러나 아동에 대한 정보의 저장을 위한 요건이 충족되는 경우는 극히 드물 것이다. 아동이 경찰법상의 원인자가 될 수 있지만, 그에 대한 정보의 저장은 위험방지를 위하여 통상적으로 필요하지 않을 것이다. 예외적으로 저장이 필요한 경우에도 비례의 원칙에 대한 합치 여부를 신중하게 심사해야 할 것이다. 형사소추와 관련하여서는 사실관계를 규명하기 위하여 아동에 대한 정보가 수집될 수 있고 검사에게 전달될 수 있다. 범죄의 예방을 위하여 아동에 대한 정보를 수집·저장하는 것은 단지 제한된 범위 내에서만 고려될 수 있다. 아동은 형사미성년자이기 때문에 장래 범죄의 ‘행위자’로서 중요한 의미를 가지고 고려되는 경

184) 여기서 ‘아동’이라 함은 만 14세 미만의 자를 말한다.

185) 독일에 있어서 아동에 대한 정보의 저장기간은 통상적으로 2년을 넘을 수 없도록 되어 있다. 이에 대하여는 § 38 Abs. 2 Nr. 2c SPolG, § 22 S. 5 PolG NW, § 27 Abs. 4c HSOG Art. 28i Abs. 2 S. 3 BayPAG 참조.

우는 극히 드물 것이다. 물론 범죄예방의 범위 내에서 행위자 이외의 '제3자'로서 아동에 대한 정보가 저장되는 것이 극히 엄격한 조건 하에서 또한 저장된 정보의 사용을 위한 요건을 갖춘 경우에 한하여 고려될 수 있을 것이다. 비례의 원칙에 따라 아동의 정보를 저장하는 것은, 예를 들면 장래의 중대한 '범죄자'에 접근할 다른 가능성이 없는 경우와 같이 최후의 수단으로 고려될 수 있을 것이다.

3. 정보제공

정보제공은 두 가지 측면에서의 고찰이 필요하다. 우선 정보제공기관의 입장에서 정보제공은 저장된 정보의 이용에 해당하고, 제공받는 기관에게는 정보수집의 형태에 해당한다. 따라서 정보제공의 경우에도 목적구속의 원칙이 적용되어야 함을 분명히 하여야 한다. 다만 정보가 '위험'방지를 위하여 없어서는 안 되며, 다른 방법으로는 전혀 또는 적시에 얻을 수 없거나 막대한 비용·노력에 의하여만 얻을 수 있는 경우에 한하여 예외가 인정될 수 있을 것이다. 그러한 경우에도 비례의 원칙에 따라 방지되어야 할 위험과 제공된 정보의 내용이 비교형량 되어야 한다. 직업상 또는 특별한 직무상의 비밀에 속하는 정보의 경우, 직업상 또는 직무상 비밀준수의무가 있는 자로부터 경찰에 제공된 것이라면, 경찰이 그 정보를 입수한 목적과 동일한 목적을 위하여 필요한 경우에만 경찰은 다시 정보를 다른 기관에 제공할 수 있다고 보아야 한다.¹⁸⁶⁾ 제공받는 자는 제공자가 정보를 수집한 방법과 동일한 방법으로 그 정보를 수집할 수 있어야 하며, 또한 제공받은 목적에만 사용할 수 있다는 규정을 두어야 한다.

정보제공의 적법성에 대한 책임은 제공기관이 부담한다. 정보제공의 요청이 있는 경우에 요청을 받은 기관은 요청의 이유에 대하여 문의하는 등 정보제공 여부에 대하여 심사하여야 한다. 정보제공은 개인의 권리에 대한 제약을 의미하므로 개별적인 경우마다 그 요건의 충족 여부를 판단하여야 한다. 경찰 또는 다른 행정관청에 정보를 제공하는 경우에는 정보를 요청하는 것이 요청기관의 직무범위에 속하는지 여부에 대한 심사로

186) 공적 기관 이외의 기관에 제공하는 경우에는 부가적으로 비밀준수의무 있는 자 또는 기관의 동의가 있어야 할 것이다.

충분할 것이다.

경찰관청 사이에는 직무수행을 위하여 필요하다면 정보가 제공될 수 있다. 정보제공에 대한 일반적인 원칙은 이 경우에도 적용됨은 당연하다. 정보를 경찰의 통합정보처리 시스템에 저장하는 것은 개념적으로 제공에 해당하는 것은 아니지만, 제공받는 기관이 정보를 사실상 불러내는 시점에 그에 대한 통제의 가능성이 없으므로 통합시스템에 정보를 저장할 때에 미리 통상적인 정보제공에 있어서 심사되어야 할 사항을 심사하여야 할 것이다.

경찰이 직무수행을 위하여 필요한 경우이거나, 제공받는 기관이 위험방지의 직무를 수행하기 위하여 필요한 경우에는 다른 행정관청 또는 공공단체에 정보를 제공할 수 있다는 규정을 두어야 한다.

외국기관, 특히 외국의 경찰기관에 정보를 제공하는 것은 경찰업무와 관련한 국제적 협력이 필요하다는 측면에서 점점 그 의미가 증대되고 있다. 그에 따라 제공받는 자의 고유한 직무수행을 위하여 필요하거나 또는 중대한 위험을 방지하기 위하여 외국기관에 정보를 제공할 수 있음을 규정하여야 한다. 다만 외국기관에 대한 정보제공에 의하여 국내법에 반하는 결과를 가져오거나 관련자의 보호할 가치 있는 이익이 침해된다고 판단되는 경우에 제공이 허용되어서는 안될 것이다. 정보의 자기결정권은 이 경우에도 보호되어야 한다.¹⁸⁷⁾

그밖에 경찰이 사인에게 정보를 제공하는 경우를 생각해 볼 수 있다. 독일의 경찰법에 의하면 경찰은 직무수행을 위해서나 공공복리에 대한 현저한 장애를 방지하기 위하여 또는 개인의 권리에 대한 중대한 침해를 방지하기 위하여 필요한 경우에는 사인에게 정보를 제공할 수 있다고 한다.¹⁸⁸⁾ 이러한 경우에는 경찰이 직권으로 정보제공을 하는 것인데, 그 이외에 경찰은 사인의 신청에 의하여도 정보를 제공할 수 있다고 한다. 즉

187) 참고로 독일의 경찰법에서는 정보의 자기결정권에 대한 침해가 문제될 수 있는 경우로 ① 제공받는 국가에 정보보호법이 존재하지 않는 경우, ② 정보보호법이 있지만 법규정이 제공받는 기관에는 적용되지 않는 경우, ③ 관련규정에 의한 보호 정도가 독일법규정에 비해 현저히 낮은 경우, ④ 제공받는 자에 의한 정보처리에 대하여 효과적이고 독립된 통제장치가 마련되어 있지 않은 경우 및 ⑤ 관련자에게 교시, 정정 및 삭제청구권이 인정되지 않는 경우 등을 들고 있다.

188) 예를 들면 § 23 HSOG, Art. 28m Abs. 1 BayPAG 참조.

경찰은 제공받는 자에게 정보제공에 대한 법률상 이익이 있으며 비밀유지에 관한 관련자의 이익이 더 크지 않는 경우와 제공이 오히려 관련자에게 이익이 되고 그가 알았다면 그에 대하여 동의하였을 경우에는 사인의 신청에 의하여 정보를 제공할 수 있다고 규정하고 있다.¹⁸⁹⁾ 이와 관련하여 관련자의 동의를 받을 수 있는 경우에는 동의를 받도록 하는 것이 해석상의 어려움을 해결하는 방법이 될 것이다. 독일의 헤센 주에서는 정보제공에 대하여 기록하여야 하며, 관련자가 제공에 동의하지 않은 경우에는 사후에 정보제공에 대하여 알려주도록 하고 있는데,¹⁹⁰⁾ 우리의 입법시에 참고가 될 수 있을 것이다.

4. 정보의 정정 · 삭제 · 차단

개인정보의 정정 · 삭제 · 차단에 대하여 구체적인 규정을 두어야 한다. 부정확한 정보는 더 이상 이용되지 않아야 한다. 그를 위해 저장된 개인정보가 정확한 것이 아니라면 정정되어야 한다. 또한 정보저장이 허용되지 않는 경우이거나 저장기관의 직무수행을 위하여 더 이상 필요하지 않게 된 경우에는 저장된 정보는 삭제 · 파기되어야 한다. 그러나 삭제 또는 파기가 관련자의 보호가치 있는 이익에 대한 침해를 가져오거나 정보가 현재의 입증의 곤란을 해소하기 위하여 없어서는 안 되는 경우이거나 또는 학술적인 목적으로 정보의 이용이 필요한 경우에는 예외적으로 삭제 · 파기되지 않는다. 이러한 경우에 해당 정보는 차단되어야 하며, 정보의 이용이 예외가 인정된 목적에 한정되어야 할 것이다.

189) § 29 Abs. 2 PolG NW, Art. 28m Abs. 2 BayPAG, § 44 Abs. 2 PolG BW 참조.

190) § 23 Abs. 4, § 22 Abs. 2 S. 2 HSOG 참조.

참 고 문 헌

[국내 문헌]

- 강구철, 경찰권의 근거와 한계, 고시연구, 1991. 9.
- 경찰대학, 경찰정보론, 1999.
- 계희열, 헌법학(중), 박영사, 2000.
- 고진영, 정보의 개념과 범죄정보의 수집방법 및 기술, 검찰 105, 1994. 7.
- 권영성, 헌법학원론, 법문사, 2000.
- 김남진, 행정법 II, 법문사, 2000.
- _____, 행정법의 기본문제, 법문사, 1994.
- _____, 경찰상의 개괄적 수권조항, 고시연구, 1994. 7.
- _____, 개인정보의 수집관리와 사생활보호, 충북대학교 법학연구, 1990.
- 김영수/김일환, 독일연방헌법법원의 인구조사판결, 김계환교수회갑기념논문집, 1996.
- 김일환, 개인정보보호법제의 정비방안에 관한 연구, 한국법제연구원, 1997.
- _____, 독일기본법상 정보자기결정권, 김운용교수회갑기념논문집, 1997.
- _____, 개인정보보호법의 개정필요성과 내용에 관한 연구, 공법연구 제26집 제2호 1998.
- 김재호, 경찰권의 근거, 저스티스 제32권 제2호.
- 김중겸/하옥현, 각국 경찰의 정보수집에 관한 입법례 분석, 1998.
- 김철수, 헌법학개론, 박영사, 1999.
- 남승길, 경찰관직무집행법, 공법연구, 제25집 제3호.
- 노화준, 정보관리론, 경찰대학.
- 류지태, 행정법신론, 신영사, 2000.
- 박상희/서정범, 경찰작용법제의 개선방안, 한국법제연구원, 1996.

- 배종대/이상돈, 형사소송법, 홍문사, 1997.
- 변재옥, 정보화사회의 프라이버시와 표현의 자유, 커뮤니케이션북스, 1996. 6.
- 서정범 역, 독일경찰법론, 세창출판사, 1998.
- _____, 경찰권발동에 관한 연구, 고려대 박사학위논문, 1992.
- 석종현, 일반행정법(하), 삼영사, 1997.
- 신동운, 독일의 수사구조와 사법경찰제도, 치안연구소, 1996.
- 심의기, 과학적 수사방법과 그 한계, 한국형사정책연구원, 1994.
- 이동권, 효율적인 첩보수집활동 개선방안, 치안정책연구, 1999. 12, 치안연구소, 1999.
- 이상돈, 형사절차와 정보보호, 한국형사정책연구원, 1996.
- 이윤식, 정보관리론, 경찰대학, 1998.
- 이준현, 수사절차에 있어서의 개인정보보호, 고려대 석사학위논문, 1997.
- 정준현, 서독 경찰법상 자료수집과 자료처리, 법제 236, 1988. 7.
- 정진수, 형사사법분야에서 영상매체의 활용, 한국형사정책연구원, 1999.
- _____, CCTV에 의한 감시와 사회통제, 형사정책연구 제10권 제3호, 1999.
- 정진환, 주요국가간 경찰의 임무 및 치안상태의 비교연구, 치안연구소, 1998.
- 조두영, 독일사법경찰관의 지위 및 몇 가지 문제점, 독일연방법무부 연수보고서, 1996. 12.
- 채한수, 정보화사회에 있어서 한국경찰의 컴퓨터 활용성 제고방안에 관한 연구, 고려대 석사학위논문, 1994.
- 최영호, 컴퓨터와 범죄현상, 컴퓨터출판, 1995.
- 허영, 한국헌법론, 박영사, 1997.
- 홍석만/이준구, 역감시의 권리로서 프라이버시권에 대한 재구성, 민주사회를 위한 변호사 모임, 1998.
- 홍성방, 헌법 II, 현암사, 2000.
- 홍준형, 경찰통합법에 관한 연구, 치안연구소, 1997.

[국외 문헌]

- Alexander, Rechtsfragen der Polizeilichen Datenverarbeitung, Jura 1993, 571 ff.
- Auernhammer, Bundesdatenschutzgesetz, 2. Aufl., 1981.
- Aulehner, Polizeiliche Gefahren- und Informationsvorsorge, 1998.
- Badura, Staatsrecht, 1986.
- Bäumler, Versammlungsfreiheit und Verfassungsschutz, JZ 1986, 469 ff.
- Deutsch, Die heimliche Erhebung von Informationen und deren Aufbewahrung durch die Polizei, 1991.
- Drews/Wacke/Vogel/Martens, Gefahrenabwehr, 9. Aufl., 1986.
- Gola/Schomerus, Bundesdatenschutzgesetz, 6. Aufl., 1997.
- Götz, Allgemeines Polizei- und Ordnungsrecht, 12. Aufl., 1995.
- _____, Die Entwicklung des allgemeinen Polizei- und Ordnungsrechts, NVwZ 1987, 858 ff.
- Gusy, Polizeirecht, 3. Aufl., 1996.
- Heckmann, Polizeiliche Datenerhebung und -verarbeitung, VBIBW 1992, 164 ff., 203 ff.
- Henninger, Observation im Versammlungsgeschehen, DÖV 1998, 713 ff.
- Honnacker/Beinhofer, Polizeiaufgabengesetz, 17. Aufl., 1999.
- Hornmann, Hessisches Gesetz über die öffentliche Sicherheit und Ordnung, 1997.
- Hufen, Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbstbestimmung - eine juristische Antwort auf „1984“?, JZ 1984, 1072 ff.
- Knemeyer, Polizei- und Ordnungsrecht, 7. Aufl., 1998.
- _____, Datenerhebung und Datenverarbeitung im Polizeirecht, NVwZ 1988, 193 ff.
- Kniesel/Tegtmeyer/Vahle, Handbuch des Datenschutzes für Sicherheitsbehörden,

1986.

Kniesel/Vahle, Polizeiliche Informationsverarbeitung und Datenschutz im künftigen Polizeirecht, 1990.

Kowalczyk, Datenschutz im Polizeirecht, 1989.

Krüger, Informationelle Selbstbestimmung und Kriminalaktenführung, DÖV 1990, 641 ff.

Lisken, Über Aufgaben und Befugnisse der Polizei im Staat des Grundgesetzes, ZRP 1990, 15 ff.

Lisken/Denninger, Handbuch des Polizeirechts, 2. Aufl., 1996.

Mallmann, Datenschutz in Verwaltungs- und Informationssystemen, 1976.

Monika, Rechtliche Probleme des Einsatzes verdeckter Ermittler, 1996.

Müller, Polizeiliche Datenerhebung durch Befragung, 1997.

Neumann, Vorsorge und Verhältnismässigkeit, 1994.

Peitsch, Die Informationsbeschaffung im neuen Polizeirecht, ZRP 1992, 127 ff.

Rebmann, Der Einsatz verdeckt ermittelnder Polizeibeamter im Bereich der Strafverfolgung, NJW 1985, 1 ff.

Riegel, Datenschutz bei den Sicherheitsbehörden, 2. Aufl., 1992.

_____, Zu Stand und Entwicklungstendenzen des informationellen Befugnisrechts zur polizeilichen Aufgabenerfüllung, DÖV 1994, 814 ff.

Rogall, Strafprozessuale Grundlagen und legislative Probleme des Einsatzes verdeckter Ermittler im Strafverfahren, JZ 1987, 847 ff.

Schatzschneider, Ermittlungstätigkeit der Ämter für Verfassungsschutz und Grundrechte, 1979.

Schenke, Polizei- und Ordnungsrecht, in: Steiner(Hrsg.), Besonderes Verwaltungsrecht, 6. Aufl., 1999.

Schmidbauer/Steiner/Roese, Bayerisches Polizeiaufgabengesetz und Bayerisches Polizeiorganisationsgesetz, 1999.

Scholler/Schloer, Grundzüge des Polizei- und Ordnungsrechts in der Bundes-

- republik Deutschland, 4. Aufl., 1993.
- Schwann, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, VerwArch 1975, 120 ff.
- Siebrecht, Rasterfahndung, 1997.
- _____, Die polizeiliche Datenverarbeitung im Kompetenzstreit zwischen Polizei- und Prozeßrecht, JZ 1996, 711 ff.
- Steinmüller, Grundfragen des Datenschutzes, BT-Drucks. VI/3826, 88 ff.
- Tinnefeld/Ehmann, Einführung in das Datenschutzrecht, 3. Aufl., 1998.
- Vahle, Staatliche Eingriffe in die durch das Wohnungsrecht (Art. 13 GG) geschützte Privatsphäre, Datenschutz und Datensicherheit, 1995, 388 ff.
- _____, Zum Stand der polizeilichen Datenverarbeitung, Datenschutz und Datensicherheit, 1996, 267 ff.
- Württemberg/Heckmann/Riggert, Polizeirecht in Baden-Württemberg, 3. Aufl., 1997.
- Württemberg/Schenke, Der Schutz von Amts- und Berufsgeheimnissen im Recht der polizeilichen Informationserhebung, JZ 1999, 548 ff.