연구보고 97-5

個人情報保護法制의 整備方案에 관한 硏究

硏究者 : 金日煥(先任硏究員)

한국법제연구원

發刊辭

情報社會란 情報 그 자체의 중요성이 엄청나게 증대하고 이를 바탕으로 하여 情報의 생산, 유통 및 이용이 기존사회를 새롭게 바꾸는 그러한 사회를 말합니다. 그렇기 때문에 情報社會에서는 중요한 情報와 중요하지 아니한 情報간에 구별의 의미가 없어졌으며, 컴퓨터의 연결을 통하여 참으로 엄청난 情報들을 처리, 결합함으로써 순식간에 질적으로 전혀 다른 情報들을 만들어낼 수 있는 사회입니다.

이제 우리는 '情報秩序'란 개념에 대하여 생각하여 보아야 합니다. 情報秩序란 개념은 전반적이고 구체적으로 이미 확정된 개념이 아니라 經濟秩序와 아주 유사하게 한 사회내에서 情報調査나 處理 등에 관하여 나름대로의 原則과 基準을 제시하는 모델개념입니다.

그리고 궁극적으로 우리가 지향하여야 하는 情報秩序는 인간지향적 情報秩序이어야 합니다. 곧 인간우호적이고 인간이 통제할 수 있는 情報시스템이어야 한다는 것입니다. 이는 法이 달라진 사회환경에 어떻게 반응하여야만 하는가를 연구하는 것이 아니라 社會秩序를 유지하고 憲法에 규정된 목표를 구체화하기 위하여 이러한 科學技術시스템에 法이 어떻게 대처하여야 하는지에 관한 것입니다. 과학기술의 적용은 무엇보다도 憲法에 바탕을 두고 민주적으로 조정되어야 합니다.

또한 個人關聯情報가 매우 간편하고 순식간에, 그리고 전체적으로 조합·연결될 수 있는 이러한 상황하에서 憲法과 조화되는 情報社會란 국가행정의 투명성을 확보하여 情報의 흐름과 처리를 국민들이 충분히 파악할 수 있는 사회이어야 합니다. 그리고 국민 모두가 알아야 하는 그러한 情報는 가능한 한 모든 국민이 손쉽게 공유할 수 있도록 공개되어야 합니다. 이와 더불어 국가는 필요한 최소한도의 목적을 위해서 個人關聯情報를 조사, 저장, 전달하여야 합니다.

情報社會에서 個人의 자유와 권리가 침해될 수 있는 새로운 가능성을 인식한다면 個人의 사생활자유는 "情報自己決定權"을 통하여 적극적으로 保護되어야 합니다. 여기서 情報自己決定權이란 個人관련情報의 사용과 공개에 대하여 원칙적으로 個人 스스로 결정할 권리를 말하는 것으로서 이러한 情報自己決定權의 목표는 단순히 個人의 權利保護에만 있는 것이 아니라 사회 속에서 個人의 의사소통능력을 보장함으로써 個個人이 자율적으로 자기의 삶을 꾸려나갈 수 있는 사회를 실현하는 데에 있습니다.

많은 국가들이 1960년대 후반부터 情報社會에서 個人의 사생활을 保護하는 法律을 제정하였거나 立法중에 있으며 특히 영국을 비롯한 대부분의 서유럽국가들은 1970년대부터 80년대 중반 사이에 個人情報保護法을 제정하였습니다. 우리 나라에서는 1980년대 이후에 국가가 행정전산망사업 등 국가와 사회의 情報化에 주력하면서 1980년대말에 個人의 사생활보장에 관한 立法을 추진하였으며, 이에 따라 1994년 "公共機關의個人情報保護에관한法律"이 제정, 공포되었습니다. 우리 나라의 個人情報保護法은 국제적으로 본다면 1980년대에 만들어진 가장 최근의 個人情報保護法이지만 그 내용에 있어 일부 개선되어야 할 부분이 있습니다. 더욱이 국민의 낮은 個人情報保護意識, 個人情報를 保護하기 위한 효율적인 통제방안의 결여, 個人情報의 저장과 처리 기술의 급속한 발전으로 우리 나라에서 "個人情報"의 효과적 保護는 더욱 중요한 사안이 되어 있습니다.

이 연구보고서는 다른 나라들에서 個人情報保護法의 제정 및 시행을 통하여 발견한 문제점들을 우리 나라의 '個人情報保護法'의 개선을 위해 반영할 수 있는 자료가 될 것입니다.

끝으로 본 연구과제를 수행하는데에 많은 수고를 한 金日煥 선임연구원의 노고를 치하하는 바입니다.

1997. 12.

韓國法制硏究院長
法學博士 朴 松 圭

發刊辭

情報社會란 情報 그 자체의 중요성이 엄청나게 증대하고 이를 바탕으로 하여 情報의 생산, 유통 및 이용이 기존사회를 새롭게 바꾸는 그러한 사회를 말합니다. 그렇기 때문에 情報社會에서는 중요한 情報와 중요하지 아니한 情報간에 구별의 의미가 없어졌으며, 컴퓨터의 연결을 통하여 참으로 엄청난 情報들을 처리, 결합함으로써 순식간에 질적으로 전혀 다른 情報들을 만들어낼 수 있는 사회입니다.

이제 우리는 '情報秩序'란 개념에 대하여 생각하여 보아야 합니다. 情報秩序란 개념은 전반적이고 구체적으로 이미 확정된 개념이 아니라 經濟秩序와 아주 유사하게 한 사회내에서 情報調査나 處理 등에 관하여 나름대로의 原則과 基準을 제시하는 모델개념입니다.

그리고 궁극적으로 우리가 지향하여야 하는 情報秩序는 인간지향적 情報秩序이어야 합니다. 곧 인간우호적이고 인간이 통제할 수 있는 情報시스템이어야 한다는 것입니다. 이는 法이 달라진 사회환경에 어떻게 반응하여야만 하는가를 연구하는 것이 아니라 社會秩序를 유지하고 憲法에 규정된 목표를 구체화하기 위하여 이러한 科學技術시스템에 法이 어떻게 대처하여야 하는지에 관한 것입니다. 과학기술의 적용은 무엇보다도 憲法에 바탕을 두고 민주적으로 조정되어야 합니다.

또한 個人關聯情報가 매우 간편하고 순식간에, 그리고 전체적으로 조합·연결될 수 있는 이러한 상황하에서 憲法과 조화되는 情報社會란 국가행정의 투명성을 확보하여 情報의 흐름과 처리를 국민들이 충분히 파악할 수 있는 사회이어야 합니다. 그리고 국민 모두가 알아야 하는 그러한 情報는 가능한 한 모든 국민이 손쉽게 공유할 수 있도록 공개되어야 합니다. 이와 더불어 국가는 필요한 최소한도의 목적을 위해서 個人關聯情報를 조사, 저장, 전달하여야 합니다.

情報社會에서 個人의 자유와 권리가 침해될 수 있는 새로운 가능성을 인식한다면 個人의 사생활자유는 "情報自己決定權"을 통하여 적극적으로 保護되어야 합니다. 여기서 情報自己決定權이란 個人관련情報의 사용과 공개에 대하여 원칙적으로 個人 스스로 결정할 권리를 말하는 것으로서 이러한 情報自己決定權의 목표는 단순히 個人의 權利保護에만 있는 것이 아니라 사회 속에서 個人의 의사소통능력을 보장함으로써 個個人이 자율적으로 자기의 삶을 꾸려나갈 수 있는 사회를 실현하는 데에 있습니다.

많은 국가들이 1960년대 후반부터 情報社會에서 個人의 사생활을 保護하는 法律을 제정하였거나 立法중에 있으며 특히 영국을 비롯한 대부분의 서유럽국가들은 1970년대부터 80년대 중반 사이에 個人情報保護法을 제정하였습니다. 우리 나라에서는 1980년대 이후에 국가가 행정전산망사업 등 국가와 사회의 情報化에 주력하면서 1980년대말에 個人의 사생활보장에 관한 立法을 추진하였으며, 이에 따라 1994년 "公共機關의個人情報保護에관한法律"이 제정, 공포되었습니다. 우리 나라의 個人情報保護法은 국제적으로 본다면 1980년대에 만들어진 가장 최근의 個人情報保護法이지만 그 내용에 있어 일부 개선되어야 할 부분이 있습니다. 더욱이 국민의 낮은 個人情報保護意識, 個人情報를 保護하기 위한 효율적인 통제방안의 결여, 個人情報의 저장과 처리 기술의 급숙한 발전으로 우리 나라에서 "個人情報"의 효과적 保護는 더욱 중요한 사안이 되어 있습니다.

이 연구보고서는 다른 나라들에서 個人情報保護法의 제정 및 시행을 통하여 발견한 문제점들을 우리 나라의 '個人情報保護法'의 개선을 위해 반영할 수 있는 자료가 될 것입니다.

끝으로 본 연구과제를 수행하는데에 많은 수고를 한 金日煥 선임연구원의 노고를 치하하는 바입니다.

1997. 12.

韓國法制硏究院長
法學博士 朴 松 圭

차 례

第1章 序 論

第1節 問題提起

情報社會란 무엇일까? 情報社會란 情報 그 자체의 중요성이 엄청나게 증대하고 이를 바탕으로 하여 情報의 생산, 유통 및 이용이 기존사회를 새롭게 바꾸는 그러한 사회를 말한다. 물론 과거에도 情報는 중요하였다. 예전부터 생산수단이나 무기 등을 가진 사람이 그에 필요한 情報를 가짐으로써 그들의 권력이나 富가 증대되었다. 그러나 過去에는 사람들이 주로 각자의 고유한 경험에 바탕을 두고 어떤 決定을 내렸던 반면에 오늘날에는 사람들이 중요한 결정을 내릴 때 자신의 경험보다는 구체적이고 확실한 情報에 근거한다. 다시 말하자면 과거에는 물질적이고 유형적인 것이 無形的인 情報보다 중요하였다. 하지만 情報社會에서는 情報가 유일하거나 가장 중요한 富의 원천[1]이자 權力의 중심[2]에 있다. 물론 정보란 무엇인지에 대하여 지금까지 많은 토론은 있었으나[3] 일반적으로 받아들여지는 개념은 없다. 그렇다면 정보란 이것으로부터 합리적 결정이 행해질 수 있고 이것의 도움을 받아서 문제를 해결할 수 있는 의미내용을 가진 기호라고 개념정의할 수 있다. 결국 情報 그 자체가 價値를 가질 뿐더러 또 다른 새로운 價値를 만들어내는 사회, 그래서 情報化 내지는 컴퓨터화를 통하여 근본적인 변화를 받고 있는 사회가 바로 情報社會인 것이다.

여기서 우리는 다음과 같은 토플러의 말을 들어보자 : "어떤 어머니가 마가린 및 TV가이드란 잡지를 산 경우 이론적으로 그 여자는 이때 상점 컴퓨터에서 다음과 같은 내용을 알려준 셈이다. ① 자기가 사용하는 제품의 종류, ② 그 상표, ③ 그 규격 또는 양, ④ 자기가 소금을 치지 않은 마가린을 좋아한다는 사실, ⑤ 구매시간, ⑥ 자기가 동시에 구입한 다른 품목들과 그 상표·규격 등, ⑦ 구매총액, ⑧ 광고주가 자기에게 알리기 위해 이용해야 할 잡지의 종류, ⑨ 이제 진열장의 어느 곳에 빈자리가 생겼느냐에 관한 정보 등등. …이 모든 자료를 짜 맞추면 개개인의 운전습관, 여행, 좋아하는 오락 및 독서, 외식의 빈도, 알코올음료와 콘돔 등 피임기구의 구매상황, 호감을 갖는 자선단체의 이름 등 개개인의 생활양식에 관한 놀랄

1) 이에 관해서는 예를 들어 데이비스, 데이빗슨/한성호, 하헌식 번역, 「경제이동」, 知識工作所, 1993 참조.

2) 토플러/이규행 번역, 「권력이동」, 韓國經濟新聞社, 1990 참조.

3) 정보화촉진기본법 제2조제1호에 따르면 "정보"란 "자연인 또는 법인이 특정 목적을 위하여 광(光) 또는 전자적(電磁的) 방식으로 처리하여 부호·문자·음성·음향 및 영상 등으로 표현한 모든 종류의 자료 또는 지식"이다.

만큼 상세한 모습을 파악할 수 있다."[4] 결국 情報社會에서 중요한 정보와 중요하지 않은 정보간 구별이 의미 없어졌고, 컴퓨터의 연결을 통하여 참으로 엄청난 정보들을 처리, 결합함으로써 순식간에 質的으로 전혀 다른 情報들을 만들어낼 수 있는 시대에 우리가 살고 있다는 아주 평범한 사례를 토플러는 설명하고 있다.

이에 따라서 결국 情報社會에서 거대한 情報結合網들을 통하여 國家行政과 經濟活動의 효율성이 과거와는 비교할 수 없을 정도로 향상될 수 있기 때문에 오늘날 모든 經濟主體와 國家機關들은 현대적인 情報通信技術을 사용하지 않고서는 그들의 다양한 과제와 기능을 수행하지 못한다.[5] 그러나 다양한 情報通信技術의 이러한 발전이 사회에 어떤 영향을 미치는지는 情報의 특성 및 情報通信技術은 물론 이를 사용하려는 主體의 認識 또한 고려해야만 한다. 여기서 새로운 情報通信技術이 사회에 미치는 영향은 ① 새로운 技術을 적용할 때 언제나 나타나는 영향과 ② 컴퓨터를 이용하는 情報通信技術의 발전으로 인하여 특별하게 나타나는 영향[6]으로 나누어 볼 수 있다. 우선 컴퓨터의 발전이 사회전체에 미치는 영향을 요약하면 다음과 같다 : ① 컴퓨터와 通信技術은 다른 科學技術 등과 결합하여 과거와는 비교할 수 없을 정도로 강력한 情報網을 구성한다. 그리고 이러한 시스템통합을 통하여 또 다시 새로운 技術이 발전된다. ② 이를 통하여 모든 경제적, 사회적, 정치적 영역에서 새롭게 情報를 소유하거나 처분권한을 갖는 자에게 권력이 집중되거나 그쪽으로 권력이 이동한다. 따라서 國家는 우월한 情報獲得地位에 근거하여 그들의 권력을 강화하고 직접적이고 물리적인 억지력을 행사하기 보다는 情報統制를 통하여 이미 그들이 원하는 바를 이룰 수 있으며 예를 들어 또한 勤勞關係에서 고용주만을 위한 정보시스템이 발전될 가능성도 있다. ③ 결국 이에 따라서 과거에 대규모산업의 발전을 통하여 환경오염 등이 문제되었던 것처럼 情報社會에서는 情報技術의 이용에 따른 個人統制라는 새로운 문제가 등장한다.[7] 이제 이러한 설명을 통하여 새로운 情報通信技術의 社會的 中立性이란 처음부터 존재하지 않는다는 것을 우리는 알 수 있다. 곧 이러한 技術의 개발자나 이용자 또는 그 통제자의 價値判斷이 언제나 이러한 기술발전에서 중요한 역할을 하게 된다는 것을 언제나 인식해야만 한다.

그렇다면 이제 우리는 "情報秩序"란 개념에 대하여 생각해 보아야만 한다. 여기서

---

4) 엘빈 토플러/이규행번역, '권력이동', 한국경제신문사, 137면 이하.

5) Karl Steinbuch, *Der Mensch - Objekt oder Subjekt der Informationsverarbeitung?*, RDV 1988, S. 1.

6) 여기서 情報通信技術이 원자력발전소에 관한 기술과 같은 개별기술이 아니라 여러 다양한 과제들이 모여서 발전된 기술집합체에 관한 것임을 인식해야만 한다.

7) Wilhelm Steinmüller, *Die Zweite industrielle Revolution. Techmische und sozialökonomische Bedingungen der Informationstechnologiepolitik*, DVR, 1981, S. 53.

情報秩序란 개념은 전반적이고 구체적으로 이미 확정된 개념이 아니라 經濟秩序와 아주 유사하게 한 사회내에서 情報調査나 處理 등에 관하여 나름대로의 原則과 基準을 제시하는 모델개념이다.[8] 결국 이러한 情報秩序를 통하여 구체적으로 情報處理 및 傳達과 관련되는 모든 규정들에 관하여 상세하게 그 내용을 알 수는 없지만 한 사회의 全體情報秩序를 이끄는 原則이나 基準을 추상적이고 일반적으로 제시해야만 하는 바로 그러한 것들을 얻을 수 있다. 왜냐하면 情報秩序에 관한 이러한 원칙적인 논의와 事前理解가 우선 선행되어야 개개 분야에서 이러한 원칙과 기준이 어떻게 적용되어야만 하는지를 제대로 살펴볼 수 있기 때문이다. 따라서 情報秩序에 관한 논의나 개개 분야에서 구체적으로 어떤 결과가 도출되어야만 하는가는 情報通信技術의 적용에 따른 현실적, 실제적 문제가 아니라 우리가 規範的으로 근거하고 있는 原則 및 基準에 따라 판단해야만 하는 當爲的 問題이다. 결국 情報處理의 이용가능성, 위험성여부, 효율성 등에 관한 판단은 새로운 情報通信技術을 적용함으로써 얻게 되는 것이 아니라 이에 관한 組織的, 法的, 社會的 前提條件에 따라서 행해진다.[9]

뒤에서 자세히 설명되겠지만 궁극적으로 결국 우리가 지향해야만 하는 情報秩序는 人間指向的 情報秩序이어야만 한다.[10] 곧 인간우호적이고 인간이 통제할 수 있는 정보시스템이어야만 한다는 것이다. 이러한 정보시스템을 구축하기 위하여 事後的으로 개인의 권리를 보호할 뿐만 아니라 이러한 시스템을 계획하고 구축할 때부터 關聯者의 포괄적 참여와 협조가 필요하다.[11] 따라서 情報技術을 통제하고자 하는 것은 새로운 정보통신기술의 발전을 방해하려는게 아니라는 것을 반드시 기억해야만 한다. 물론 개개 경우에 이러한 統制가 어느 정도 행해져야만 하는지는 통제되어야만 하는 情報技術의 危險性에 우선 달려있다. 이러한 情報技術의 危險性에 관한 일차적인 판단은 먼저 立法者가 해야만 한다. 결국 이는 情報技術의 발전과 정보흐름의 사회적응성과 바람직함에 대하여 결정할 임무를 立法者가 일차적으로 부담해야만 함을 뜻한다. 이러한 立法者의 지침속에 情報秩序의 원칙과 기준에 관한 중요한 내용들이 존재해야만 한다.[12] 立法者가 인간우호적인 정보질서의 구축

---

8) Wolfgang Zöllner, *Informationsordnung und Recht*, Walter de Gruyter, 1990, S.11.

9) Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch, *Digitalisierung der Grundrechte?*, Westdeutscher Verlag, 1990, S. 36.

10) 미국이나 독일·한국 모두가 오늘날 이러한 情報社會라는 일반적 특징을 공통적으로 갖고 있다 하여도, 개개 국가의 상황에 따라서 강조점이 다를 수 있다는 것 또한 인식해야만 한다. 예를 들어 미국, 독일보다는 한국에서 정보의 자유로운 흐름이나 정보사회에서 새로운 종속성 등에 관하여 더 심각하게 논의될 수 있는 것이 이러한 사례중 하나에 속한다.

11) Wilhelm Steinmüller, a.a.O., S.66.

을 위하여 필요한 法律을 제정함으로써 일차적인 임무를 이행한 경우에는 그 다음으로 法律이 존재하는가가 아니라 이미 존재하는 法律이 제대로 지켜지는가를 분석해야만 한다. 이러한 검토와 분석을 거쳐서 비로소 情報秩序의 원칙과 기준이 개개 영역에서 어떻게 구체화되어야 하는지가 심도깊게 다루어질 수 있다. 결국 법제정과 법적용에서 이러한 토론과 분석을 통하여 法이 學問的, 技術的 發展에 적응하도록 할뿐만 아니라 이를 넘어서서 새로운 정보기술을 도입하려고 하는 社會와 國家에게 이에 관하여 다시 한번 생각하고 결정할 수 있는 기회를 제공하게 되는 것이다.[13] 학문적, 기술적 발전이 가질 수 있는 위험에 관한 이러한 警告는 이러한 警告가 정보기술의 적용보다 앞서거나 최소한 동시에 이루어지는 경우에만 비로소 의미를 가질 수 있다. 결과적으로 나중에 이러한 警告가 미리 사서 하는 걱정이었다면 오히려 다행일 것이다. 그러나 이미 새로운 정보통신기술의 적용을 통하여 이미 예상되었던 위험한 결과가 발생한다면 나중에 이러한 警告를 고려한다는 것은 이미 때늦은 自責에 불과할 뿐이다.

따라서 궁극적으로 個人關聯情報가 매우 간편하고 순식간에, 그리고 전체적으로 조합, 연결될 수 있는 이러한 상황하에서 (憲)法과 조화되는 情報社會란 다음과 같은 사회이어야만 한다 : 우선 國家行政의 투명성을 확보하여 정보의 흐름과 처리를 國民들이 충분히 파악할 수 있어야 한다. 이에 따라서 국민 모두가 알아야만 하는 그러한 情報는 가능한 한 모든 국민이 손쉽게 공유할 수 있도록 공개되어야만 한다.[14] 이와 더불어 國家는 필요한 최소한도의 목적을 위해서만 個人關聯情報를 조사, 저장, 전달하여야 한다. 이러한 전제조건 없이 國家가 일방적으로 국민에 관한 무수한 정보들을 저장, 전달, 처리하는 경우에 우리는 결국 자기에 관한 정보를 國家에 제공하는 客體로 떨어질 뿐이다. 결국 情報社會에서 국민의 私生活保護와 국가의 情報公開란 서로 모순되는 명제들이 아니라, 自由民主主義란 헌법상 토대를 굳건하게 하는 상호 보충적 작용을 한다.[15]

---

12) Bernhard Schlink, *Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht*, VVDStRL 48, 1990, S. 250.

13) Bernhard Schlink, a.a.O., S. 260.

14) 그 구체적인 보기로서 김일환, '법령정보의 생활화', 시민과 변호사 통권 37호, 1997년 2월, 20면 이하 참조.

15) 예를 들어 김석준·강경근·홍준형의 '열린 사회 열린 정보'(비봉출판사, 1993)의 32면 이하에서 언급하는 것처럼 情報公開를 個人情報의 保護보다 우선시하는 주장은 매우 위험하다.

第2節 研究目的과 內容

1. 研究目的

1) 科學技術의 發展과 法

國家와 經濟의 발전을 이룩하며 국제사회에서 국가경쟁력을 확보하기 위해서는 國家, 특히 行政은 科學技術을 발전시키고 촉진시키고자 노력하게 된다. 學問的, 技術的 發展의 성취는 중요한 국가과제로서 이러한 임무는 정치적, 경제적 이유에 근거하여 주장될 뿐만 아니라 憲法 自體에서도 도출되는 명령이기도 하다.[16] 따라서 民主法治國家에서 行政法 및 國家機關은 과학기술정책을 집행할 때 과학기술의 발명자나 이용자가 선택한 기술을 가능한한 존중하고 사회내에서 자유스러운 연구분위기가 조성될 수 있는 환경을 만들어 주어야만 한다. 그러나 동시에 이러한 科學技術 및 학문의 발전으로부터 어떤 위험이 초래될 수 있는 한 이를 막을 책임 또한 국가에게 있다. 다시 말하면 憲法上 法治國家原則 및 國家의 基本權保護義務에 근거하여 당연히 통제되지 못하거나 통제할 수 없는 技術이나 실험으로부터 나오는 위험으로부터 시민과 사회를 보호할 책임을 國家는 지고 있다.[17] 예를 들어 國家는 과학기술의 위험으로부터 시민의 생명, 건강, 소유, 그 외 다른 基本權을 보호할 책임을 갖고 있다.[18] 이에 따라서 國家는 다양한 실체법규정과 절차법상 예방조치를 통하여 과학기술로부터 나올 수 있는 위험을 인식하고 이를 예방할 과제를 수행해야만 한다.[19] 이렇게 國民의 基本權을 보호해야만 하는 憲法上 義務 때문에 제3자를 통한 과학기술발전과 이용을 國家가 책임질 수 없다고 주장해서는 안된다.

科學技術의 발전이 개인과 사회를 과거의 억압과 굴레로부터 해방시킬 수도 있으나 오히려 이러한 발전을 막을 수도 있고 새로운 위협을 만들 수도 있다. 그렇다면 결국 憲法은 이러한 사회변화에 탄력적으로 대응할 수 있어야만 한다. 여기서 科學

16) BVerfGE 49, 89/141f. ; BVerfGE 53, 30/57. 한국헌법 제127조 참조.

17) 科學技術의 특징은 본질합치적으로 어떤 법학적-규범적 당위척도를 제기하는 것이 아니라 우선 인과관계지향적 관계를 제시한다는 데에 있다. 따라서 이러한 과학기술이 법학적-법률적 명령과 결합하는 경우에만 비로소 규범적 당위척도가 된다. 또한 法과 技術間 긴장관계는 법제정측면에서 뿐만 아니라 법적용측면에서도 나타난다. 이에 관해서는 Rupert Scholz, Technik und Recht, Dieter Wilke (Hrsg.), *Festschrift zur 125jährigen Bestehen der Juristischen Gesellschaft zu Berlin*, Walter de Gruyter, 1984, S. 696 참조.

18) BVerfGE 49, 89/140 ff. ; BVerfGE 53. 30/57 ff. ; BVerfGE 56, 54/73 ff.

19) Josef Isensee, *Widerstand gegen den technischen Fortschritt*, DÖV, 1983, S. 569.

技術의 憲法調和性이 새롭게 대두된다. 여기서 憲法調和性이란 현행 憲法이 규정하고 있는 척도에 따라서 미래에 나타날 수 있는 과학기술의 발전을 평가, 판단하는 것을 가능하게 하는 規範的 槪念을 말한다. 憲法이 구체적 국가질서와 사회적, 정치적 과정의 발전을 위한 규범적 틀이라고 할 때 결국 憲法調和性이란 科學技術의 발전을 통한 사회의 변화가 憲法에 규정된 목표와 조화되어야만 한다는 것을 말한다. 따라서 이러한 憲法調和性基準은 法秩序의 변경가능성을 함께 고려하는 것이기 때문에 법정책적인 토론을 동시에 그 대상으로 한다. 그렇다면 憲法調和性을 심사할 수 있기 위한 척도가 우선 제시되어야만 하는데 이러한 척도로는 個人의 自由保障, 國民의 民主的 參與, 社會的, 政治的 權力의 統制 등이 언급될 수 있다. 따라서 미래의 과학기술발전이 개인의 기본권발현 및 憲法에 규정된 목표실현을 가능하게 하면 할수록 더욱 더 憲法調和的이다.[20] 그렇다면 科學技術의 憲法調和性이란 미래를 단순히 예측하는 것에 관한 것이 아니라 현재의 관점에서 미래를 비판적으로 검토하는 것이다. 미래는 어떨가라는 상상과 어떤 미래를 우리가 원해야만 하는가에 관한 생각이 동시에 행해져야만 한다는 것이다. 그러므로 憲法調和性審査는 일반적이고 추상적인 자연과학적, 기술적 시스템이 아니라 언제나 사회에 구체적으로 적용되는 과학기술시스템을 대상으로 한다는 것을 인식해야만 한다. 곧 이는 法이 달라진 사회환경에 어떻게 반응해야만 하는가를 연구하는 게 아니라 사회질서를 유지하고 憲法에 규정된 목표를 구체화하기 위하여 이러한 과학기술시스템에 法이 어떻게 대처해야만 하는지에 관한 것이다. 따라서 검증되지 않은 과학기술의 성급한 적용보다는 사회, 연구단체, 국가기관을 통한 조심스러운 검토 및 이를 거친 기술발전이 요구되며[21] 과학기술의 적용은 무엇보다도 憲法優越思想에 따라 民主的으로 조정되어야 한다. 그렇다면 결국 이에 관한 법적 전제조건을 만들고 여러 이해관계를 형량할 일차적 과제가 立法者에게 속한다. 일차적으로 立法者가 모든 法的, 技術的, 經濟的, 環境的 狀況을 고려하여 어떤 위험이 불가피하며 국민이 이를 受忍할 수 있는 것인지를 결정하고 그 안전기준을 확인해야만 한다.[22] 다만 科學技術이 본래 갖고 있는 특성상 憲法調和性基準을 가능한한 이미 기술연구와 그 발전단계에서부터 미리 검토하는 것이 좋다. 왜냐하면 科學技術이란 급격하게 변하고

---

20) Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch, a.a.O., S. 11.

21) 獨逸의 聯邦憲法法院은 과학기술의 가능한 위험을 초기에 인식하고 그에 필요하고 헌법합치적인 수단으로 대처할 의무를 국가기관에 지웠다. BVerfGE 49, 89/132.

22) 물론 議會留保와 本質性理論을 통하여 얼마만큼 구체적으로 立法府가 구체적으로 활동해야만 하는지는 또다른 문제이다. 곧 議會留保를 통하여 과학기술의 발전에 따른 국가책임이 의회책임으로 바뀌는지 또는 언제 바뀌는지 등의 문제를 검토해야만 한다.

그 영향을 쉽게 파악할 수 없기에 立法者를 통한 예방적 기술형성, 과학기술시스템의 法制化, 사회적, 법적 영향의 사전적 검토가 거의 통제할 수 없는 사후의 이용금지보다 훨씬 더 효과적이기 때문이다. 따라서 立法者를 통한 憲法調和的 技術形成은 무엇보다도 과학기술의 발전과 이용에 관한 윤곽조건을 설정하는 것을 목표로 해야 한다. 이는 개인의 자유영역 및 민주적 참여기회를 확대하고 국가 및 사회권력의 제한과 통제를 효율화하기 위하여 情報通信技術이 사용되어야만 하는 것을 뜻한다.[23] 따라서 새로운 과학기술의 적용이 국민의 基本權實現을 위협한다면 國家는 이를 허용할 것이 아니라 간섭하면서 통제해야만 한다.

2) 情報技術의 危險性

(1) 自動情報處理의 위험성

과거에 國家는 자신이 독점하고 있는 물리적 폭력을 행사하거나 행사할 수 있다는 가능성을 통하여 國家權力을 효율적으로 행사할 수 있었다. 그러나 오늘날 국가는 이러한 물리적 폭력대신에 승인과 거부, 급부제공 및 정보조사와 처리라는 새로운 수단을 더 애용하고 있다. 바로 여기에서 情報通信技術의 위험성이 존재한다. 왜냐하면 물리적 폭력과는 달리 情報通信技術을 사용하는 경우에는 개인은 그들이 감시받고 있다거나 통제되고 있다는 것을 쉽게 또는 전혀 인식할 수 없기 때문이다.

따라서 우선 오웰이 언급하였던 빅 브라더(Big Brother)형태, 곧 國家가 國民을 완전히 감시하고 통제하는 사회는 의심할 바 없이 처음부터 허용될 수 없다. 이는 또한 私的 領域에서 개인을 통한 다른 개인의 완전한 감시의 경우에서도 마찬가지이다. 그 다음으로 문제가 되는 自動情報處理의 구체적 위험성에 대하여 대하여 명확하게 인식해야만 한다 : 먼저 自動情報處理는 엄청난 처리속도 및 상상할 수 없는 연결가능성을 특징으로 한다. 이에 따라서 自動情報處理는 개인의 자유를 보장하던 전통적인 보호장벽들을 사실상 손쉽게 부술 가능성을 제공하였다. 예를 들어 自動化된 情報處理를 통하여 공간적으로 떨어져 있는 다른 정보에 순식간에 접근할 수 있으며 이것으로부터 情報가 원래 저장되었던 목적과는 다른 목적으로 이용될 위험성 및 자동화된 정보결합가능성 등이 새롭게 등장하였다.

(2) 情報連結의 危險性

발전된 情報通信技術을 國家, 특히 行政이 이용하려는 이유는 무엇보다도 한 기관에서 다른 기관에 정보가 손쉽게 전달될 수 있다는 것이다. 따라서 自動情報處理

23) Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch, a.a.O., S. 276.

의 技術的 問題보다는 정보처리기관이나 저장기관이 파악하고 있는 정보의 끈임없는 연결이 公的 領域에서 특히 심각한 문제로 대두된다. 한 기관의 컴퓨터에 저장된 정보의 새로운 결합과 연결을 통하여 추가적으로 아주 새로운 정보를 만들 수 있게 된다.[24] 이에 따라서 정보의 연결로부터 개인의 私生活保護는 현재는 물론 미래에서도 심도깊게 다루어져야만 하는 중요한 문제영역을 형성한다.

(3) 情報自己決定權의 內容

이미 위에서 설명한 것처럼 발전된 정보처리과정은 언제나 급격한 정도로 우리 사회의 사회적, 정치적 구조를 변화시키는바 특히 이러한 변화속에는 개인의 私生活과 民主主義를 위협할 수 있는 잠재성 또한 내재해 있다. 예를 들어 개인행동에 대한 컴퓨터감시를 통하여 이러한 개인의 정치적 의사형성과 선택기회를 억압함으로써 공동체생활의 건전한 발전에 심각한 영향을 줄 수도 있다. 이를 통하여 결국 自由民主主義秩序의 기본적 전제조건인 개인적, 사회적 자율이 상실될 위험을 낳을 수도 있는 것이다.[25] 왜냐하면 개인이 민주적, 정치적 결정과정에 적극적으로 참여하기 위해서는 누가, 무엇을 언제 그리고 어떤 맥락에서 자기에 관하여 얼마만큼 알고 있는지를 인식해야만 하기 때문이다. 관련자가 모르는 기록화, 목록화는 그 개인을 관찰대상으로 만들며 다른 목적을 위하여 이용, 조종할 수 있게 된다. 이러한 정보처리과정을 통하여 한 개인이 투명해질 정도로 노출된다면 그 개인의 의사소통관계를 파괴하게 되고 이에 따라서 나타나는 필연적 결과는 개인적 불안정과 사회에 대한 불신이다. 상대방이 자기에 대하여 얼마만큼 아는지를 모르면서 개인이 자신의 결정을 자율적으로 행사한다는 것은 상상하기가 매우 힘들다.[26] 따라서 이러한 권리는 私生活의 제한된 물리적, 공간적 영역뿐만 아니라 다양한 사회생활 속에서 방해받지 않고 의사소통을 할 개인의 결정자유 또한 보호한다.[27] 그러므로 이러한 권리의 보호는 외부로부터 개인의 私生活公開를 방어할 뿐만 아니라 또한 이를 넘어서서 사회내에서 개인의 自己決定 또한 보장한다. 이는 개인의 私生活自由가 폐쇄된 공간적 영역으로 한정되는게 아니라 개인적 동일성형성의 기본적 전제조건으로서 이러한 영역밖의 私的 交涉도 포함한다는 것을 뜻한다.[28]

---

24) Rupert Scholz/Rainer Pitschas, *Informationelle Selbstbestimmung und staatliche Informationsverantwortung*, Duncker & Humblot , 1984, S. 20.

25) Marie-Theres Tinnefeld/Eugen Ehmann, *Einführung in das Datenschutzrecht*, Oldenbourg Verlag, 1992, S. 1.

26) BVerfGE 65, 1/43.

27) Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch, a.a.O., S. 208.

이를 요약한다면 정보사회에서 컴퓨터를 통한 무제한적 처리능력과 저장능력이 순식간에 엄청난 정보를 파악할 수 있는 가능성과 결합함으로써 관련자가 자기에 관한 정보의 처리와 결합이 정당한지를 충분히 통제할 수 없는 상황이 발생할 수 있게 되며 이를 통하여 지금까지는 인식되지 못하였던 새로운 통제수단이 등장한 것이다. 따라서 情報社會에서 개인의 私生活自由는 情報自己決定權을 통하여 적극적으로 보호되어야만 한다. 여기서 情報自己決定權이란 개인관련정보의 사용과 공개에 대하여 원칙적으로 개인 스스로 결정할 권리이다. 결국 이러한 권리는 원칙적으로 그 자신이 스스로 개인관련정보의 공개와 이용에 대하여 결정할 권한을 보장하기 때문에[29] 누가, 무엇을, 언제 그리고 어떠한 경우에 자기에 관하여 아는지를 시민들이 더 이상 알 수 없는 사회질서 및 이를 가능하게 하는 법질서는 情報自己決定權과 조화되지 못한다.[30] 그러므로 情報自己決定權의 목표는 개인의 의사소통능력을 보장하는데에 있다. 물론 이러한 기본권을 보장하기 위하여 어떠한 예방조치가 행해져야만 하는지는 이러한 현실을 충분히 인식해야만 비로소 도출될 수 있다.[31] 결국 이러한 情報自己決定權을 바탕으로 하여 개인은 국가가 자기자신에 관한 어떤 정보를 조사, 처리해도 되는지를 결정, 통제할 수 있는 권리를 갖고 있다. 따라서 국가를 통한 개인관련정보의 모든 조사, 저장, 전달은 情報自己決定權의 제한이므로 이에 관한 法的 授權을 필요로 하는 것이다.[32] 그래서 情報調査와 모든 정보처리는 관련자가 명시적으로 목적이 구체화된 정보처리에 동의하거나 중요한 公共福利에 따라 제정된 法律에 근거한 경우에만 허용된다.

2. 研究內容과 方法

아래에서 설명되는 것처럼 많은 國家들이 1960년대 후반부터 情報社會에서 개인

28) 獨逸의 聯邦憲法法院 또한 개개인을 사회공동체내에서 발현하는 의사소통에 의존하는 인격체로 보았다. BVerfGE 65, 1/44.

29) BVerfGE 65, 1 (Leitsatz 1).

30) 獨逸의 聯邦憲法法院이 이렇게 개인정보의 보호를 강조하게 된 배경에는 바로 電子情報處理라는 조건하에서 개개인이 특별한 보호를 필요로 한다는 인식이 깔려 있었다. 다시 말하면 "자기와 관련된 정보들중 어떤 것이 특정한 사회영역 속에서 알려지는지를 충분할 정도로 확실하게 알 수 없는 사람, 의사소통상대방이 무엇을 알고 있는지를 충분히 판단할 수 없는 사람은 독자적인 자기결정에 따라서 계획하고 결정할 그의 자유가 결정적으로 억제될 수 있다." (BVerfGE 65, 1/42)

31) Spiros Simitis, Informationelle Selbstbestimmung und Informationsfreiheit als Verfassungsprinzipien, Thomas Kreuder (Hrsg.), *Der orientierungslose Leviathan*, 1992, S. 143.

32) Adalbert Podlech, Das Recht auf Privatheit : Joachim Perels (Hrsg.), *Grundrechte als Fundament der Demokratie*, Suhrkamp, 1979, S. 55.

의 私生活을 보호하는 法律을 제정하였거나 立法中에 있다. 물론 개개 국가의 역사적, 정치적, 법적 전통이 다르기에 이에 대처하는 방법도 다양하다. 예를 들어 美國은 프라이버시법 및 개개 분야에서 個人情報를 보호하는 복잡하면서도 체계적이지 않은 접근방식을 채택하는 반면에 서유럽국가들과 최근에 법률을 제정한 국가들은 "個人情報保護法"을 제정하여 情報社會에서 개인의 私生活을 보호하고자 하는 방식을 채택하였다. 다만 後者에 속하는 나라들이라 하더라도 개인의 私生活이 누구로부터 더 많이 침해될 수 있는지에 관하여 관점이 다르기에 個人情報保護法의 적용범위나 규율대상이 약간씩 다르다. 게다가 어느 나라든지 나름대로 독특한 행정적, 정치적, 법적 전통이 있기 때문에 個人情報를 보호하기 위하여 國家機關 등을 감독하고 통제하는 기관의 설치여부, 그 권한 등에 관해서는 참으로 다양할 정도로 많은 유형들이 있다. 결국 여기서 우리는 各國의 個人情報保護法이 우선 情報社會에서 개인의 私生活, 個人關聯情報가 보호되어야만 한다는 공통된 인식과 목표하에서 個人情報保護에 관한 일반적인 원칙 및 이러한 원칙들의 실현에 관한 여러 일반적인 기준들을 대체로 비슷하게 담고 있다는 것을 알 수 있다. 그러나 이러한 일반적 원칙들과 기준들을 구체적으로 적용할 때 바로 해당 국가의 정치, 사회, 문화, 법체계 등이 나름대로 작용하게 된다.

특히 美國을 비롯한 대부분의 서유럽국가들은 1970년대부터 80년대중반사이에 "1세대" 個人情報保護法을 제정하였으며 그 뒤 급격하게 발전되는 정보통신기술에 발맞추어 1980년대후반부터 "2세대" 개인정보보호법률로 개정하거나 새롭게 제정하고 있다.[33] 이에 반하여 우리 나라는 1980년대이후에 정력적으로 國家가 行政電算網事業 등 국가와 사회의 情報化에 주력하면서 개인의 私生活侵害가 우려된다는 비판이 강하게 제기되자 1980년대말에 비로소 개인의 私生活保護에 관한 입법을 추진하였다. 이에 따라서 마침내 1994년 "공공기관의개인정보보호에관한법률"이 제정, 공포되었다. 그런데 유감스럽게도 우리 나라의 個人情報保護法은 국제적으로 본다면 1990년대에 만들어진 가장 최근의 개인정보보호법임에도 불구하고 그 내용은 서유럽국가 등에서 수십년전에 만들어진 "1세대" 個人情報保護法에 가깝다는 것이었다. 게다가 국민의 낮은 개인정보보호의식, 個人情報를 보호하기 위한 효율적인 統制方案의 缺如, 국가기관을 통한 개인정보의 무차별적 저장과 처리 등을 통하여 우리 나라에서는 "個人情報保護法"은 있되 정작 "個人情報"는 보호되지 못하고 있는 실정이다. 결국 이에 따라서 다른 나라들에서 個人情報保護法을 제정과 시행을 통하여 문제점을 발견하고 이를 다시 법개정을 통하여 반영하는 법실무와는 달리

33) 여기서 "1세대", "2세대" 개인정보보호법과 같은 표현은 筆者가 개인정보보호법을 그 내용에 따라서 구별하기 위하여 임의로 만든 단어이다.

우리 나라는 "個人情報保護法"을 제정하였다는데에 만족하고 있음을 알 수 있다.

이러한 우리 나라의 상황은 立法者가 필요한 法律을 제정함으로써 그 일차적인 임무를 이행했다면 法律이 존재하는가가 아니라 이미 존재하는 法律이 제대로 지켜지는가를 분석해야만 한다는 사실을 다시 한번 일깨워준다. 따라서 이 硏究에서는 우리 나라에서 제정된 個人情報保護法이 어떤 문제점을 갖고 있는지를 살펴보기 위하여 우선 外國의 個人情報保護法制를 분석한다. 외국의 이러한 個人情報保護法制 分析은 단순히 어떤 한 나라의 法律을 소개하거나 언급하는 수준에 그치는 것이 아니라 그 나라에서 왜 個人情報保護法이 제정되었으며 이러한 법의 적용과정에서 어떤 문제점을 갖고 있었으며, 어떻게 개정되었는지를 자세히 살펴보고자 한다. 바로 이러한 분석을 바탕으로 하여야 비로소 우리 나라에서 個人情報保護法은 제정되었으나 왜 이 法律이 실효성이 없는지를 이해하기 위한 틀이 만들어질 수 있다. 이러한 일차적인 분석을 근거로 하여 그 다음으로 우리 나라의 個人情報保護法이 과연 어떤 문제들을 갖고 있으며, 어떻게 개정되어야만 하는지를 검토한다. 따라서 본 연구는 ①比較法的 分析, ②現行 個人情報保護法體系에 관한 분석을 거친 이후에 ③법정책적 고려하에서 시급히 개정되어야만 하거나 설치가 필요한 기관 등에 관하여 논의하고자 한다. 그러므로 이 연구는 個人情報保護法制의 개선방안에 관한 完結論的 硏究가 아니라 무수히 많은 個人情報保護法制의 制定 및 改正을 위한 일반론적이고 원칙론적인 연구라는 것을 기억해야만 한다.

第2章 各國의 個人情報保護法制分析

第1節 個人情報保護에 관한 國際的 基準

1. 國際聯合(UN)

UN총회는 1946년 12월 14일 결의에서 "情報自由는 UN이 기초하고 있는 모든 自由들의 초석이며 이는 基本的 人權이다. 情報自由는 情報를 모으고 구속없이 언제나 어느 곳에나 情報를 전하고 출판할 권리를 포함한다."고 결정하였다. 결국 이는 UN이 초창기에는 人權으로써 情報自由, 情報의 자유로운 흐름을 강조하였다는 것을 지적한다. 그러나 1960년대 후반에서 70년대 초반부터 차츰 自動化된 情報處理가 私生活保護權(프라이버시권)에 미칠 수 있는 영향에 관하여 국제적 차원에서 관심을 갖게 되었다. 특히 유네스코(UNESCO)는 1970년부터 프라이버시 및 個人情報保護領域에 관심을 기울이기 시작하였다.[1] 물론 국제적인 모든 인권목록들중에서도 프라이버시를 개념 정의하려는 노력이 가장 어려울지도 모른다. 특히 이러한 어려움은 프라이버시를 개념정의하려는 무수한 이론적인 시도들이 지금도 계속 행해지고 있으며 이에 관한 새로운 법규정들이 끊임없이 제정되고 있다는 것을 통하여 더욱 더 커진다. 어쨌든 프라이버시권은 國際法上 人權目錄속에 보호되어야 할 근본적인 권리로서 명확하게 확립되기는 하였으나 프라이버시권에 관한 이러한 국제적인 보호규정들은 일반적이고 추상적이었다.[2] 1948년 世界人權宣言(Universal Declaration of Human Rights) 제12조는 프라이버시가 보호되어야만 한다고 규정하고 있을 뿐만 아니라 더나아가 이 人權宣言 제12조에서 정교화된 프라이버시권은 그 보호에 관한 구체적인 규정들을 포함하고 있다. 그래서 예를 들어 개인의 프라이버시권은 가족영역에서 프라이버시보호로 확대된다. 이에 따라서 프라이버시보호는 가정, 다른 사람과 의사소통도 포함하는 쪽으로 그 보호범위가 넓어지게 되었다.[3]

어쨌든 個人情報의 保護에 관해서는 1990년 12월 14일 UN총회의 결의로 채택된[4] 컴퓨터화된 개인정보파일의 규율에 관한 지침(Guidelines for the regula-

1) James Michael, *Privacy and Human Rights*, Dartmouth, 1994, 서문
2) James Michael, ibid., p. 1.
3) James Michael, ibid., p. 19.
4) Resolution 45/95.

tion of computerized personal data files)을 주목해야만 한다.

이 指針은 個人情報를 보호하기 위하여 다음과 같은 원칙들을 담고 있다 : 1) 合法性과 公定性原則(Principle of Lawfulness and Fairness) : 個人에 관한 情報는 합법적인 방법으로 수집, 처리되어야만 하고 UN헌장에 명시된 목적과 원칙에 반해서는 안된다. 2) 正確性原則(Principle of Accuracy) : 情報를 수집하거나 저장하는 사람 및 이에 관하여 책임있는 담당자는 個人情報를 정기적으로 검사하여 수록된 정보가 정확한 정보인지를 검토해야만 한다. 3) 目的具體性原則(Principle of the Purpose-specification) : 個人情報를 수집하고 처리는 목적이 구체적이고 정당해야만 한다. a) 이에 따라서 수집, 저장되는 이러한 모든 個人情報는 구체화된 목적과 관련되며 필요한 것이어야만 한다. b) 이러한 個人情報는 관련개인의 동의가 없는 한 사용되거나 공개되어서는 안된다. c) 수집된 個人情報의 저장은 구체화된 목적을 위하여 필요한 기간을 넘어서는 안된다. 4) 關聯個人에 의한 接近原則(Principle of Interested-person Access) : 情報가 수집되거나 저장된 해당 개인은 이러한 情報가 어떻게 처리되며 사용되는지에 관하여 알 권리를 갖고 있으며 잘못되거나 정확하지 못한 정보의 삭제권 등 여러 보호권리들이 이러한 개인들을 위하여 제공되어야만 한다. 5) 非差別原則(Principle of Non-discrimination) : 個人關聯情報의 주체들은 宗教的, 人種的, 性的 差異나 政治的 見解 등을 이유로 不當하거나 恣意的인 差別을 받아서는 안된다. 6) 例外에 관하여 결정할 수 있는 機關(Power to make Exceptions) : 위에서 열거된 원칙으로부터 예외가 인정되는 경우로는 國家安全保障, 秩序維持, 他人의 自由와 權利保護 및 反人類的 犯罪를 범한 犯人追跡처럼 그 목적과 근거가 국내법절차에 따라서 정당하게 제정된 법규정에 구체화된 경우에 인정될 수 있다. 7) 安全(保安)原則(Principle of Security) : 자연재앙이나 컴퓨터바이러스, 권한없는 접근 등으로부터 이러한 개인정보파일을 보호하기 위한 적절한 조치들이 행해져야만 한다. 8) 監督과 制裁(Supervision and Sanctions) : 모든 國家들은 열거된 원칙들의 준수를 감시할 독립된 기관을 설치해야만 하고 이러한 원칙들을 위반한 경우에 대비하는 처벌규정 및 개인보호규정들도 만들어야만 한다. 9) 국경 없는 정보흐름(Transborder Data Flows) : 個人情報가 한 국가에서 다른 국가로 전달될 때 해당 국가들에 私生活保護에 관한 충분한 보호대책들이 마련되어 있다면 情報는 관련 국가들 내에서 가능한 한 자유롭게 전달, 처리될 수 있어야만 한다. 10) 適用範圍(Field of Application) : 이러한 원칙들은 모든 公的, 私的 機關들에 적용되어야만 하고 컴퓨터파일뿐만 아니라 手作業파일도 적용대상에 포함된다.

2. 유럽연합(EU)

1) 개인정보보호협정의 성립과 내용

먼저 Gaskin v. United Kingdom사건[5]에서 유럽人權法院은 유럽인권협약 8조에 규정된 프라이버시권은 정부가 갖고 있는 情報에 관한 일반적이고 적극적인 접근권은 포함하고 있지는 않으나 어린 시절에 公的 機關들의 보호를 받은 것과 같은 특정정보에 접근할 권리를 해당 개인은 갖고 있다고 결정하였다. 그 다음으로 英國의 人口調査計劃에 관하여 유럽인권위원회는 인구조사가 언뜻 보기에는 프라이버시를 제한하는 것처럼 보이기는 하나 이러한 계획은 法律을 준수하였으며 국가의 경제적 발전을 위하여 필요하다고 결정하였다.[6]

情報의 국제적인 이동이나 흐름을 규제하는 효과적인 유일한 조치는 國際協約을 통한 경우이다.[7] 이에 관한 중요한 국제협약은 1) OECD위원회가 1980년 9월 23일 채택한 프라이버시의 보호 및 個人情報의 국경 없는 흐름에 관한 指針(Guidelines on the Protection of Privacy and Transborder Flows of Personal Information) 및 2) 유럽연합이 1981년 2월 28일 서명하고 1993년에 개정한 個人情報의 自動處理에 관한 個人保護를 위한 協定(Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)이 있다. 결국 국제적 차원에서 이러한 발전은 국내적으로는 물론 국제적으로도 個人情報에 관한 保護規定의 필요성 - 특히 구체적으로 국경을 넘는 정보흐름에 대한 규정필요성 - 이 증가하고 있음을 나타내는 것이다.

유럽연합(EU)의 차원에서 個人關聯情報의 처리에 관한 일반원칙을 확정적이고 구체적으로 열거하기는 힘들다. 왜냐하면 개개 국가의 다양한 상황, 상이한 法秩序, 충돌하는 보호이익들이 모두 고려되어야만 하기 때문이다.[8] 다만 1993년초반까지 유럽연합의 단일시장완성으로 인하여 EU내 기업간에 그리고 국제적 차원에서 個人情報를 다루고 교환할 가능성이 더욱 더 커지고 있다는 것만은 확실하다. 이에 따라서 1980년 제정되고 1993년에 개정된 유럽연합의 個人情報保護協定은 개개 국가의 다양한 個人情報保護法律들을 근거로 하여 자유로운 정보교환의 부당한 제한

---

5) Judgment of 7 July 1989, Series A No. 160

6) 유럽인권위원회와 유럽인권법원은 性轉換에 따른 출생증명서의 개정을 인정하지 않았으며 모든 동성애금지법률은 유럽인권협약 제8조를 위반했다고 결정하였다.

7) *Raymond Wacks*, Personal Information, Clarendon Press, 1989, p. 205.

8) *Ferdinand Kopp*, Das EG-Richtlinienvorhaben zum Datenschutz, RDV 1993, S. 1.

을 제거하고자 했다. 다시 말하자면 EU내에서 한 국가는 다른 국가(情報를 받는 나라)가 충분한 個人情報保護法制를 갖추고 있지 않다는 이유를 들어 국가간 정보교환을 방해해서는 안된다는 것이다. 이 협정은 1981년부터 비준되기 시작하여 1985년에 효력을 발생하여 이제 서명국들에게 법적인 구속력을 갖는다. 유럽연합의 개정된 個人情報保護에 관한 협정은 유럽연합에 속하는 국가들에게 個人情報保護에 관한 최소한도의 기준을 준수하는 法律을 제정하도록 요구한다. 이를 통하여 유럽연합내에서 情報의 자유로운 이동에 관한 제한들을 금지시키기는 하나 유럽연합이 제시하는 個人情報保護에 상응하는 個人情報保護法律을 갖고 있지 않은 國家들로 情報의 이동은 제한된다.[9] 따라서 이 협정은 다음과 같은 세 가지 주요기능들을 갖고 있다 : 1) 이는 개개 署名國家들에 의하여 국내적으로 채택될 수 있는 個人情報保護에 관한 基本原則들을 확정한다. 2) 국경 없는 정보흐름들에 관한 특별규정들을 만든다. 3) 이러한 조치들을 이행하기 힘든 상황이 발생한다면 이에 관한 협의장치를 확립한다.

이 협정의 내용을 살펴보면 다음과 같다. 우선 협정 제1조에 규정된 目的에 따르면 加入國家들은 파일에 담긴 個人情報의 처리, 전달로부터 개인의 私生活을 보호해야만 한다. 결국 이는 협정의 보호대상이 個人의 自由와 權利 특히 自然人의 私的 領域保護라는 것을 나타낸다.[10] 협정 제2조에서 個人情報란 확인되거나 확인할 수 있는 개인과 관련되는 情報라고 하였다. 그리고 협정 3조에서 협정의 適用範圍는 公的, 私的 領域 모두를 포함한다고 규정하였다. 결국 개정된 협정에서는 私的 領域과 公的 領域의 형식적 분리가 포기되었다. 獨逸처럼 個人情報保護法의 적용범위를 公的 領域으로 한정하는 나라의 시각과는 달리 유럽의회 및 가입국의 많은 대표자들은 公的 機關을 통한 정보처리가 私的 領域에서 情報處理보다 작은 위험성을 갖고 있다고 생각하였다. 왜냐하면 行政府는 결국 議會에 책임을 지고 議會가 충분히 行政府를 통제할 수 있다고 생각하였기 때문이다. 이에 따라서 公的 領域을 위한 특별규정은 필요한 경우에만 삽입되었다. 따라서 이러한 특별규정이 없는 한 公的 領域과 私的 領域에 동일한 규정이 원칙적으로 적용된다.[11] 또한 첩보기관의 활동처럼 EU법하에 있지 않은 영역은 개개 협정에서 이에 관한 규정을 마련하도록 하였다.

특히 유럽협약 5조와 16조에 個人情報保護에 관한 기본원칙들이 규정되어 있다

9) Henry H. Perrit Jr., *Law and the Information Superhighway*, Wiley Law Publications, 1996, p. 139.
10) *Ferdinand Kopp*, a. a. O., S. 3.
11) *Ferdinand Kopp*, a. a. O., S. 4.

: 情報가 자동적으로 처리된다면 이들은 a) 공정하고 합법적으로 획득되어야 하고, b) 구체적이고 정당한 목적을 위해서만 저장되어야 하며 이러한 목적들과 양립할 수 없는 방법으로 사용되어서는 안되고, c) 저장목적과 해당 정보간에 적절한 관련성이 있어야 하며, 이를 넘어서는 저장은 허용되지 않으며, d) 個人情報는 올바르고 필요한 경우에는 최신의 것이어야만 하며 부정확하거나 불충분한 정보는 삭제되거나 수정되어야만 하고, e) 情報는 저장되는 목적을 위하여 필요한 시간만큼 보존되어야만 한다.

이 협약은 個人情報가 어떤 목적으로 저장될 수 있는지에 관하여 설명하지는 않으나, 최소한 구체화되지 않은 目的을 위한 個人情報의 수집을 금지한다. 특히 협약 제17조에는 人種, 政治的 見解, 宗教的·哲學的 信念이나 勞動組合加入與否, 健康情報나 性生活情報와 같은 個人情報는 국내법이 적절한 보호를 제공하지 않는 한 자동적으로 처리될 수 없다고 규정되어 있다. 이러한 목록은 EU에 속하는 유럽국가들의 대표들에 의하여 특별히 민감한 것으로 생각되는 개인정보의 보호에 관한 광범위한 합의를 나타낸다. 그러나 이는 최소한도의 목록으로서 협약 제11조하에서 다른 종류의 個人情報들에게도 이와 유사한 특별한 보호를 제공할 수 있는 길을 가입국들에게 열어놓는다. 협약 제7조는 가입국들에게 公的 分野에서 個人情報의 보호를 監督할 기관의 설치 및 적절한 保安措置들을 요구한다. 그리고 협약 제12조 이하는 정보주체들의 권리들에 관한 것이다. 이 조항들에서 자신들에 관한 자동화된 정보파일들이 있는지를 알 권리, 이에 관한 열람권, 삭제권이나 수정권 등이 정보주체에게 인정된다. 그러나 이러한 情報保護原則들도 절대적이지는 않다. 예를 들어 협정 제15조에서 a) 정보주체의 私生活을 침해할 위험이 전혀 없는 統計나 學問硏究를 위하여 사용되는 개인정보파일, b) 國家安保, 公共安全, 국가의 財政·金融問題나 刑事犯罪의 訴追, b) 情報主體나 다른 사람의 자유보호를 위한 경우에는 해당 개인의 권리들이 제한될 수 있다. 그리고 협약 제21조 이하는 정보저장기관의 책임 및 처벌규정을, 협정 제24조는 제3국에 個人情報를 전달하는 것에 관하여 규정하고 있는데 국제적인 개인정보의 이동은 해당국가에 個人情報에 관한 적절한 보호대책이나 보호규정이 있는 경우에 가능하도록 하였다.

2) 유럽안보와 個人情報間 關係

유럽이 통합되면서 특히 유럽 刑法과 刑事訴訟法이 필요한지 그리고 필요하다면 그 권한은 가입국가의 수사기관과 어떤 관계에 있어야만 하는가 등이 논의되기 시작하였다. 왜냐하면 우선 유럽의 統合에 따라 犯罪(특히 경제범죄, 마약, 신용거래

범죄 등)가 국제화되었고 두 번째로 EU내에서 居住移轉의 自由가 보장되기 때문에 시민들을 국경에서 검사하고 통제하기가 매우 어려워졌기 때문이다.[12] 이에 따라서 국경을 감시·통제하고 국가간 효율적인 경찰협력문제를 해결하기 위한 논의가 시작되었다. 그리하여 가입국간 범죄극복을 위하여 국경에 제한없이 정보를 교환할 수 있도록 규정하고 슈트라스부르크에 이에 관한 중앙컴퓨터를 설치하도록 하는 유럽정보협정(Schengen Ⅱ)이 체결되었다. 이 협정에 따라서 EU내에서 공통적으로 사용할 수 있는 자동화된 추적시스템(SIS, Schengerer Informationssystem)의 설치 및 SIS에서 개인정보보호와 안전에 관한 상세한 규정을 마련하였다. 특히 이 정보시스템에서는 범인인도, 마약수색과 불법적인 마약거래, 무기거래에 대한 정보교환이 행해지고 있다.[13]

3. 經濟協力開發機構(OECD)

個人情報의 보호에 관한 또다른 국제협약으로는 OECD위원회가 1980년 9월 23일 채택한 私生活保護 및 個人情報의 국경 없는 흐름에 관한 지침(Guidelines on the Protection of Privacy and Transborder Flows of Personal Information)이 있다. 이 지침은 다음과 같은 네 가지 중요 목적들을 달성하려고 한다 : ① 個人情報를 보호하고, ② 情報의 자유로운 흐름을 촉진하며, ③ 情報의 이러한 자유로운 흐름을 개개 국가의 私生活保護法律에 의하여 부당하게 억제하는 것을 제한하고, ④ 여러 국가들의 關聯法律規定들을 조화시킨다.[14] 영국을 비롯한 대부분의 선진국가들에서 제정된 個人情報保護法律들은 유럽연합과 OECD지침들에 담긴 중요 원칙들을 대부분 반영하고 있다.

이 지침은 제1부 총칙, 제2부 국내적으로 적용되는 개인정보보호에 관한 원칙, 제3부 국제적으로 적용되는 개인정보보호원칙, 제4부 국내적 실현, 제5부 국제적 협력으로 구성되어 있다. 이 지침은 공적, 사적 영역에서 개인관련정보호를 그 목적으로 하고 있다.

OECD지침의 중요내용을 살펴보면 다음과 같다 : ①蒐集制限原則(Collection limitation principle) : 개인정보수집에 관하여 일정한 제한이 있다. 곧 個人情報

12) Manfred Schreiber, Europäische Einigung und Innere Sicherheit : Peter Badura /Rupert Scholz (Hrsg.), *Festschrift für Peter Lerche*, 1993, S. 529.

13) 결국 유럽의 통합으로 인하여 1. 유럽경찰중앙기구 2. 조사를 위한 정보교환과 이용 3. 경찰간 정보공유 4. 범죄극복과 예방프로그램에 관한 공통전략이 앞으로 연구대상이라고 한다. 이에 관하여 자세한 것은 Manfred Schreiber, a. a. O., S. 534 이하 참조.

14) Raymond Wacks, ibid., p.207.

는 情報主體가 인식하거나 동의한 후에 합법적이고 공정한 방법들에 의하여 수집되어야만 한다. ②情報內容原則(Data quality principle) : 個人情報는 이들이 사용되는(또는 될 수 있는) 목적들과 관련되어야만 하며, 이러한 목적들을 위하여 필요한 만큼 정확하고 완전하며 최신의 것이어야만 한다. ③目的具體化原則(Purpose specification principle) : 個人情報의 수집목적은 사전에 구체화되어야만 하지 정보수집이후에 구체화되어서는 안되고, 계속적인 사용은 이러한 목적들과 양립할 수 있어야만 한다. 목적의 변경은 개개 경우에 구체화되는 목적들의 이행으로 제한되어야만 한다. ④利用制限原則(Use limitation principle) : 정보주체의 동의가 있거나, 법에 근거한 경우를 제외하고 個人關聯情報는 사전에 구체화된 목적들과는 다른 목적으로 사용, 이용되거나 공개되어서는 안된다. ⑤安全保護原則(Security safeguards principle) : 個人情報는 정보의 손실이나 권한 없는 접근, 파괴, 변형과 같은 그러한 위험으로부터 합리적인 보안장치에 의하여 보호되어야만 한다. ⑥公開原則(Openness principle) : 個人情報에 관한 개발; 운용, 정책들에 관하여 일반적인 공개정책이 택해져야만 한다. 개인정보의 존재와 내용, 이러한 정보사용의 주요목적은 물론 정보관리자의 신원 및 통상적인 거주지는 즉시 이용·확인할 수 있어야만 한다. ⑦個人參加原則(Individual participation principle) : 관련개인은 ⓐ 정보관리자가 본인과 관련되는 정보를 갖고 있는지 여부를 확인할 권리를 갖고 있어야만 하고 ⓑ 필요하다면 과도하지 않은 비용 내에서 합리적 시간 내에서 적당한 방법으로 본인과 관련되는 정보에 관하여 개인에게 즉시 알려질 수 있는 있어야만 하고 ⓒ ⓐ와 ⓑ가 거부된다면 이에 대한 이유제시 및 이러한 거부에 대하여 이의를 제기할 수 있어야만 하고 異議提起가 받아들여진다면 그에 관한 정보는 삭제, 개정, 보충 또는 수정되어야만 한다. ⑧責任原則(Accountability principle) : 정보관리자는 위에서 설명된 원칙들에 영향을 주는 조치들에 뒤따르는 책임을 진다.

유럽연합의 개인정보보호협약과 OECD의 지침은 1980년에 제정되었다. 그런데 유럽연합의 협약이 1981년부터 비준되기 시작하여 1985년에 서명국가들에게 법적인 구속력을 가지기 시작하였으나 OECD의 지침은 법적인 구속력을 갖고 있지는 않다. OECD지침은 법적 구속력을 갖지 않는 권고형태로 되어 있으며 캐나다, 미국, 호주와 같은 연방국가들의 특수성을 인정하는 특별규정들을 갖고 있다. 따라서 OECD지침의 기본원칙들은 EU협약의 기본원칙들과 유사하기는 하나 더 추상적인 용어로 규정되어 있다.[15]

OECD지침이 自然人과 法人의 情報保護問題를 언급하고 있지는 않지만 확인되

15) James Michael, ibid., p. 40.

거나 확인할 수 있는 개인에 관한 정보라고 개인정보를 개념정의하는 것은 오로지 自然人만을 보호하려는 의도를 드러낸다. 어쨌든 이렇게 법적 구속력이 없는 OECD의 지침이 중요한 역할을 할 수 있다는 것은 다음 사례를 통하여 알 수 있다. 예를 들어 1978년 스웨덴의 정보보호기관은 스웨덴에서 영국으로 개인정보의 이동에 반대하였다. 왜냐하면 영국에는 그당시 個人情報保護法이 없었기 때문이었다. 또 1990년 12월 영국의 정보보호관은 영국에서 미국으로 個人情報의 이동을 금지시켰다. 왜냐하면 私的 領域에서 美國의 個人情報保護法律들이 이에 관한 적절한 보호를 제공하지 않았기 때문이었다. 아래에서 설명되는 것처럼 個人情報保護에 관하여 광범위하게 다른 접근들이 있다. 예를 들어 私的 領域 또한 公的 領域처럼 규율해야만 하는지에 관하여 두 가지 전혀 다른 입장들이 있다 : 곧 일반적으로 이에 찬성하여 입법하는 유럽국가들과 캐나다, 미국, 일본처럼 구별하여 私的 領域을 다르게 취급하는 나라들. 이러한 경우에 私的 領域을 公的 領域과 달리 취급하고 있는 비유럽국가들에게 OECD지침들은 公的 領域과 私的 領域의 포괄적인 규제방향으로 나아가게 한다. 비록 이 OECD지침이 EU협약만큼 구체적이고 구속력이 있지 않다 할지라도 말이다.[16]

第2節 個人情報保護法 및 情報公開法을 制定한 國家들[17]

個人情報를 보호하는 法律을 제정한 國家들을 다음과 같이 유형별로 나누어 볼 수 있다. 우선 ① 個人情報保護法과 情報公開法을 모두 제정한 나라로는 스웨덴, 덴마크, 노르웨이, 핀란드, 네덜란드, 프랑스, 뉴질랜드, 캐나다, 미국, 오스트렐리아 등이 있고, ② 個人情報保護法만을 제정한 나라로는 독일, 룩셈부르크, 영국, 아일랜드, 오스트리아, 아이슬랜드, 이스라엘, 포르투갈, 일본 등이 있으며, ③ 情報公開法만을 제정한 나라로는 그리스가 있다.[18]

스웨덴은 가장 먼저 個人情報保護에 관한 法律을 제정한 나라로서, 컴퓨터와 私

16) 이를 아주 잘 보여주는 다음과 같은 사례가 있다. 캐나다가 1984년 OECD지침에 동의한 이후에 외무부장관은 약 150여개에 달하는 캐나다기업들에게 이 OECD지침에 따르도록 촉구하는 서한을 보냈다 : "캐나다에서 사적 영역의 개인정보보호기준이 OECD지침에 따르지 않는다면 다른 OECD국가들이 캐나다로 개인정보의 이동을 제한하거나 금지할 수 있는 위험이 있다. 이는 분명히 캐나다경제에 반대되는 경제적 결과를 가져올 것이다."

17) 이 장에서는 개인정보보호법을 제정한 나라들에 관한 개략적인 소개에 그친다. 개인정보보호법을 제정한 나라들 중에서 중요한 국가의 개인정보보호법률은 아래에서 자세히 설명된다.

18) 스페인은 현재 個人情報保護에 관한 법률제정을 서두르고 있으며 憲法上 私生活保護에 관하여 규정되어 있다.

生活保護問題를 다룰 때 유럽 및 다른 나라들의 일차적인 연구대상이었다. 스웨덴은 美國과 거의 동시인 1960년대 중반에 情報社會에서 개인의 프라이버시보호에 관한 논쟁이 시작되었으나, 특히 1970년에 행해지기로 계획되었던 人口調査가 국민을 정부가 지나치게 통제할 수 있는 새로운 가능성을 갖고 있다는 우려속에서 많은 비판과 항의를 시민들로부터 받게 되었다. 이에 따라서 결국 公的 記錄들의 공개와 비밀에 관한 의회위원회가 1969년 처음으로 만들어졌으며 1972년 "컴퓨터와 프라이버시"에 관한 보고서에서 個人情報保護에 관한 特別立法이 제안되었다. 이에 따라서 1973년에 情報法이 제정되었고 이 情報法은 公的 領域이든, 私的 領域이든 간에 컴퓨터로 처리되어 확인할 수 있는 個人情報의 수집, 저장, 유통을 규율하는 情報監督委員會(Data Inspection Board)를 만들었다. 그럼에도 불구하고 이미 스웨덴이 200년전부터 정부문서에 관한 일반적인 접근권을 제공하는 法律을 만든 첫 번째 국가라는 것은 덜 알려져 있다.[19] 어쨌든 개인의 私生活保護에 관하여 오래전부터 확립된 원칙 및 전세계적으로 가장 먼저 個人情報保護法을 제정한 선구자적인 위치에 있음에도 불구하고 스웨덴은 개인의 프라이버시권을 보호하는 일반적 법률을 제정하지는 않았다. 어쨌든 스웨덴에서 個人情報를 보호하기 위하여 제정된 情報法에 따르면 情報監督委員會(DIB)는 個人情報를 보호하기 위한 집행기구로 설치되었다. DIB는 私的 領域에서 개인정보파일의 설치를 허가하고 심사한다. 個人情報가 민감한 것에 속한다면 이러한 정보파일의 설치에 관하여 DIB의 공식적인 허가가 필요하다. 또한 DIB는 公的 領域에서 個人情報의 수집을 규율한다. 더나아가 DIB의 권한은 個人情報保護法으로 한정되지 않는다. 그래서 이 위원회는 私生活保護를 위하여 필요하다고 인정된 다른 法律들의 집행을 감독하고 이에 관하여 허가한다.[20] 1990년 8월 스웨덴의 情報立法委員會는 情報法에 관한 改正案을 제출하였으며 이에 따라서 새로 개정된 法律은 1993년부터 시행되었다.

---

19) 다만 정부기록들에 관한 公的 接近權을 포함하는 出版自由法은 접근으로부터 기록을 면제하는 대단히 일반적인 7가지 원칙들을 규정하고 있는데, 이러한 원칙들은 비밀법(the Secrecy Act)에서 더 상세하게 정교화되었다. 이러한 구체적인 면책조항중 하나가 어떤 사람의 개인적인 상황들을 보호하는 것이다. 그러나 이는 다른 사람들에 관한 정보를 담고 있는 서류가 아니라 자기자신에 관한 정보를 담고 있는 기록들에 대한 개인들의 접근권을 금지하고 있는 것은 아니다.

20) 이러한 법률로는 1974년에 제정된 信用情報法(the Credit Information Act)과 債務救濟法(the Debt Recovery Act)이 있다. 그 이행방법이 다르다 할지라도 스웨덴의 신용정보법은 미국의 1970년 공정신용기록법(the Fair Credit Reporting Act) 및 영국의 1974년 소비자신용법(the Consumer Credit Act)과 비슷하다. 스웨덴의 신용정보법은 신용정보사업 - 자동정보처리와 수작업파일을 포함하는 - 을 위한 허가를 요구하고 개인의 주관적 접근권을 확립하였다. 이는 미국법보다 영국법에 더 유사하고 채무구제법 또한 미국보다는 영국시스템에 더 가깝다.

덴마크는 國家가 보관하고 있는 情報에 접근 및 個人情報保護에 관한 立法에서 스웨덴방식을 따랐다. 따라서 덴마크는 公的 領域과 私的 領域에서 個人情報保護를 규율하는 두 개의 독립된 法律들을 제정하였다. 私的 領域을 규율하는 法律은 자동화된 개인정보와 몇몇 수작업파일들을 포함하는 반면에 公的 領域을 규율하는 法律의 適用對象에는 자동화된 個人情報만이 포함된다. 公的 領域에서는 情報監督機關(the Data Surveillance Authority)이 개인기록파일을 설치할 때 諮問役割을 하며 개인의 主觀的인 接近權, 잘못되거나 불충분한 정보의 수정이나 삭제에 관하여 통제한다. 私的 領域에서는 이와 유사한 일반적인 접근권은 없으나, 그 대신에 특정 유형의 정보에 관한 주관적 접근권이 있으며, 민감한 개인정보의 처리는 관련개인에게 통지되고 그 개인이 동의한 후에만 행해질 수 있다.

노르웨이는 1970년에 政府記錄에 관한 公的 接近權을 확립하는 法律을 만들었고 1978년에 個人情報保護法律을 제정하였는데, 이 두 法律 모두 기록들에 관한 일반적인 접근권을 규정하였다. 우선 노르웨이의 個人情報保護法은 自然人과 法人의 프라이버시를 보호한다. 그리고 이 法律은 자동화된 기록과 手作業記錄들 모두에 적용되며 또한 公的 領域과 私的 領域 모두에 적용된다. 이 法律은 민감한 개인정보의 처리를 위한 특별규정들을 포함하고 있으며 信用調査, 輿論調査 등과 같은 몇몇 정보산업분야들의 규제를 위한 특별규정들도 있다.

핀란드는 1987년 개인정보파일법(Personal Data Files Act)을 제정하였으며 이 法律은 1988년 1월 1일부터 시행되었다. 이 法律은 자동화된 기록들과 手作業記錄들 모두를 포함하고, 公的 領域과 私的 領域 모두를 포함한다. 이 法律은 自然人의 個人情報를 보호하며 個人情報保護法律을 제정하지 않은 나라들로 민감한 개인정보의 이동에 관하여 허가할 수 있는 등의 권한을 갖고 있는 情報保護委員會를 만들었다. 또한 私的 領域에서 민감한 개인정보유형을 전산처리한다면 이 위원회에게 통지해야만 한다. 핀란드는 1991년 4월 10일 유럽연합의 個人情報保護協約에 서명하였다.

個人情報의 保護에 관하여 네덜란드인들이 관심을 갖는 첫 번째 이유는 2차대전 동안에 나치(Nazi)가 네덜란드국민중 유태인들을 확인하기 위하여 人口調査記錄을 사용했다는 역사적 사실 때문이었다. 그리고 1980년대에 네덜란드정부가 새로운 개인신원확인카드를 도입하려 한 것에 대하여 국민들이 반대하면서 個人情報保護에 관하여 새롭게 주목하게 되었다. 네덜란드에서는 이미 대부분의 사람들을 위한 個人確認番號(Personal Identification Numbers, PINs)가 존재하기는 하였으나 원래 이러한 번호는 오로지 행정부내에서 사용할 목적으로만 이용되었다.[21] 네덜

란드정부는 두 가지 개인확인번호시스템도입 - 하나는 이미 내부적으로 사용되고 있는 個人確認番號에 바탕을 두고 있는 시스템이고, 다른 하나는 租稅와 社會保障 目的을 위해서만 사용되는 시스템 - 을 계획하였다. 네덜란드정부는 1986년부터 個人情報를 보호하는 法案을 준비하면서 동시에 위 시스템을 추진하였다. 그런데 이러한 개인번호확인시스템은 채택되지 않았고 個人情報保護法을 제정하는 계획만이 받아들여졌다.[22] 情報接近法은 1970년부터 토론되기 시작하여 1978년 草案이 채택되고, 1980년부터 시행되었다. 情報接近法은 자동화된 기록들을 포함하고, 중앙정부와 지방자치단체에 의하여 보관되는 公的인 記錄들을 포함한다. 이러한 접근권의 보장은 네덜란드시민으로만 한정되지 않는다.[23] 그러나 이러한 접근권은 기록들의 열람 및 복사에 관한 권리가 아니라, 기록내용들의 요약이 公務員에 의하여 제공될 수 있는 그러한 권리이다. 물론 개인의 私生活과 관련되는 情報 - 특히 치료정보와 정신병에 관한 정보 - 는 정보공개의 대상에서 면제된다. 이에 반하여 네덜란드의 個人情報保護法은 1989년 1월 1일 시행되었다. 이 법은 手作業記錄은 물론 컴퓨터화된 기록들에게도 적용된다. 이 법은 公的, 私的 領域 모두에 적용되나 개인적으로나 내부적인 사용을 위해서만 처리되는 個人情報는 保護對象에서 제외한다. 이 법은 言論에 의하여 일반대중에게 정보의 제공을 위한 목적으로만 사용되는 정보파일들에게는 적용되지 않는다. 그리고 경찰과 첩보기관은 이 법의 적용을 받지 않으나, 독립된 法律에 의하여 규율된다.

프랑스는 가장 일찍, 그리고 정열적으로 情報社會에 진입하고자 노력한 국가에 속한다. 그래서 프랑스국민들은 새로운 技術의 적용으로 인하여 개인의 自由, 특히 私生活保護에 미칠 수 있는 위협을 재빨리 인식할 수 있게 되었다. 1975년 個人確認番號를 통하여 모든 개인기록들을 연결하려는 행정부계획을 언론이 보도하였던 사파리(Safari)사건은 엄청난 파문을 불러 일으켰고 이에 따라서 사파리계획은 취소되었다. 결국 公的, 私的 領域에서 私生活自由, 個人自由 등을 존중하는 정보처리의 발전을 보장하기 위한 立法委員會를 法務部는 설치하였다. 이를 바탕으로 하여 1978년 情報保護法이 시행되고, 같은 해에 행정서류들에 관하여 일반적인 접근권을 보장하는 法律 또한 制定하였다. 이 情報保護法은 다음과 같은 중요 내용들로

---

21) 1985년 여론조사에 의하면 응답자의 65%는 이러한 개인확인번호(주민등록번호)를 갖는 것에는 반대하지 않았으나, 응답자의 47%는 이러한 번호가 컴퓨터에 의하여 처리되지 않기를 희망하였다.

22) 여론은 정보프라이버시에 관하여 관심이 있고 잘 알고 있는 것처럼 보였다. 1979년 한 조사에 따르면 57%는 자신에 관한 정보를 스스로 결정할 일반적인 권리에 찬성하였고, 51%는 정보보호에 관한 입법을 지지하였고, 47%는 기록연결을 위한 PINs의 사용에 반대하였다.

23) 정보접근법 제1조제1항

구성되어 있다 : 첫 번째로 설치하고자 하는 정보처리시스템에 관하여 諮問하고, 기존시스템을 감독하고 조사하는 임무를 갖고 있는 독립기관인 國家情報處理自由委員會(CNIL)를 만들었다. 두 번째로 정보처리시스템들의 허가나 기록방법을 확정하였다. 세 번째로 個人情報에 관한 주관적 접근권 및 수정권을 보장하였다. 네 번째로 개인이름과 연결되는 개인정보들의 처리를 특별히 규율하도록 하였다. 그런데 그당시 국회에서 정보보호법안에 관하여 행해졌던 토론중 대부분은 CNIL의 구성과 독립에 관한 것이었다.[24] 이 CNIL은 여러 다양한 단체들의 대표 - 下院, 上院, Conseil d'Etat, 勞動組合, 情報處理專門家 등 - 로 구성되는 독립된 정부기관으로 탄생하였다. 情報保護法은 公的 領域과 私的 領域 모두에 적용되고, 手作業記錄은 물론 자동화된 파일 또한 포함하는 것으로 해석된다. 다만 그 보호주체는 自然人으로 한정된다. 기본적인 규제시스템은 대부분의 유럽국가들이 갖고 있는 개인정보보호시스템과 비슷하다. 예를 들어 개인이름과 연결하여 個人情報를 처리하는 정보처리시스템은 기록해야만 하며 이러한 기록은 다른 시스템과 상호 연결되는지, 얼마만큼의 정보가 보관되는지, 이에 관하여 어떤 보안조치들이 행해지고 있는지, 누가 이러한 情報에 접근하는지, 다른 나라들로 이러한 情報가 전달되는지에 관한 규정들을 이 법은 담고 있다. 이에 반하여 행정서류들에 접근하는 경우를 다루는 法律은 情報保護法制定時 國民이 자신의 情報를 보호하고자 강력하게 요구하는 것과 같은 것의 산물이 아니었고 私生活保護措置로서 의도되지 않았다. 오히려 이는 일련의 행정개혁의 일부로서 만들어진 法律이었다. 이 法律은 행정서류에 접근에 관한 위원회(CADA)의 감독과 자문을 받는다. 이 위원회(CADA, Commission d'Accès aux Documents Administratifs)의 위원은 議會, 司法府, 行政府, 大學 등으로부터 임명된다. 이들은 기록의 공개를 명령할 권한을 갖고 있는 게 아니라, 이에 관하여 권고만 할 수 있을 뿐이다. 포함되는 서류들은 일반적으로 행정부의 통제하에 있는 모든 서류들이나 法院의 기록들은 법률의 적용대상에서 제외된다.

뉴질랜드국민의 프라이버시는 普通法原則, 1976년 人權委員會法, 1976년 Wanganvi Computer Centre Act, 1982년의 公的 情報法 4장을 통하여 보호된다. 우선 1976년에 제정된 Wanganvi Computer Centre Act 15조에 근거하여 구성되는 프라이버시위원은 임기가 5년이며 정부에 의하여 下院에 추천되고, 신분상 독립성을 보장받는다. 그의 임무는 컴퓨터시스템에 기록된 情報가 부정확하거나 잘못 기록되어서 그릇된 인상을 준다고 믿을만한 이유를 갖고 있는 사람으로부터 불평을 접수하고 이에 관하여 조사하는 것이다. 이 프라이버시위원은 의회에 매년 이

24) James Michael, ibid., p. 65.

에 관한 보고서를 제출한다. 그 다음으로 어떤 강제력을 갖고 있는 것은 아니라 할지라도 추가적인 프라이버시보호조치는 1977년 人權委員會法을 통하여 행해진다. 人權委員會는 公的, 私的 領域에서 프라이버시를 침해하는 어떤 문제에 관한 조사기능을 갖고 있다. 人權委員會는 이에 관한 정보를 모으고, 해당 대표들을 초청하여 의견을 듣고, 이에 관하여 수상에게 보고할 수 있다. 그러나 이 委員會는 개인의 프라이버시가 침해되었다는 구체적 불평을 조사할 권한을 갖고 있지는 않다. 그 다음으로 1982년의 公的 情報法은 일단 프라이버시를 보호하기 위해서가 아니라, 더 열려진 정부를 확립하기 위하여 제정되었다: 물론 이에 따라서 이 法律은 앞의 두 法律보다는 잠재적으로 덜 효율적인 것처럼 보이나, 최소한 公的 領域에서 저장되는 개인정보에 관하여 해당개인의 접근권을 인정하고 있다는 점에서 어느 정도는 개인의 私生活保護에 기여한다. 뉴질랜드는 1990년에 個人情報保護法을 제정하였는데, 이 법은 두 단계로 나뉘어 시행되었다. 우선 1991년의 첫 번째 단계에서는 정보연결프로그램을 감독하기 위한 프라이버시위원에 관한 규정을 삽입하였고, 1992년의 두 번째 단계에서는 개인의 주관적 접근권을 인정하는 규정을 만들었다. 두 번째 단계의 法律시행으로 인하여 Wanganvi Computer Centre Act는 폐지되었다.

1973년의 캐나다 프라이버시보호법은 그 적용대상이 電話盜聽 및 電子監視의 규제로만 한정되었다. 연방차원에서 캐나다는 우선 1977년에 제정된 캐나다人權法 4章에서 個人情報를 보호하고자 하였다. 이 법은 1974년에 제정된 미국의 프라이버시법과 유사하였다. 이 법은 자동화된 시스템이든 手作業파일이든 구별하지 않고서, 연방정부에 의하여 저장되는 自然人에 관한 정보를 보호하고, 個人情報保護에 관하여 관련성, 정확성, 공정성이라는 기본원칙들을 확립하였다. 그러나 개인의 불평을 접수하고 이에 관하여 활동하는 프라이버시위원을 만듦으로써 統制機關의 경우에는 유럽의 입법례를 따랐다. 1982년 캐나다는 다시 개인의 프라이버시보호에 관한 法律을 만들었는데, 이 법률의 제정으로 인하여 캐나다는 政府情報에 접근과 프라이버시보호를 單一法律에 규정한 첫 번째 국가가 되었다. 그러나 사실상 캐나다의 프라이버시법을 유럽적 시각에서 본다면 個人情報를 보호하는 法律은 아니다. 왜냐하면 동일한 이름의 美國의 法律처럼 이 法律은 私的 領域에서 情報處理를 전혀 규율하지 않고 있기 때문이다. 어쨌든 캐나다의 1982년 프라이버시법은 연방정부의 통제 밑에 있는 手作業情報와 자동처리되는 정보 모두에 적용된다. 개인의 주관적인 접근권과는 별도로 이 법은 국가에 의한 개인정보의 수집 및 저장을 지배하는 원칙들을 제공한다.[25] 公的 情報에 관한 일반적인 권리처럼 개인의 주관적인

접근권은 캐나다시민과 거주민에게만 인정된다. 또한 이 法律에는 개인의 주관적인 접근권외에 잘못된 정보를 교정할 修正權 등 이 규정되어 있다. 다만 이 법에 규정된 프라이버시위원에 불평접수절차, 조사절차, 법원에 항소절차는 정보접근법에 규정된 절차들과 매우 비슷하다.

美國은 스웨덴과 더불어 國家情報에 관한 接近法을 국가적 차원에서 제정한 첫번째 나라에 속한다(1966년). 스웨덴에서처럼 미국의 情報自由法 또한 우선적으로 개인의 프라이버시를 보호하고자 제정되지는 않았다. 미국에서 情報自由法의 制定目的은 먼저 국가행정의 투명성을 높힘으로써 연방행정부를 개혁하고자 한 것이다. 워터게이트사건이후 1974년에 情報自由法이 개정되었고, 그 뒤 다시 프라이버시법이 제정되었다. 두 法律은 연방행정부가 갖고 있는 기록들에 적용될 뿐, 私的 領域을 규제하지는 않으며[26] 두 法律 모두 手作業記錄과 자동적으로 처리되는 기록들 모두에 적용된다. 그러나 프라이버시법은 情報自由法下에서는 이용할 수 없는 個人情報의 삭제권과 수정권을 포함한다. 어느 법에 의해서든 정보의 공개가 가능하면 해당 기관은 보통 그 기록을 공개할 것이다. 다만 이를 허용되는 절차에서 두 법률은 차이가 난다. 우선 情報自由法下에서 인정되는 정부기록에 접근권은 모든 사람으로 확대되는 반면에, 프라이버시법에 따르면 이러한 접근권은 미국시민이나 영주권자에게만 인정된다.[27] 프라이버시법은 연방기관들에 의한 개인정보수집을 제한하고, 이들이 처리하는 個人情報의 유형에 관하여 일반시민에게 통지하도록 요구한다. 다만 미국에서는 公的 領域을 규율하는 일반적인 個人情報保護法을 制定할 可能性보다는 분야별로 규율하는 방식이 聯邦과 州次元에서 채택되고 있다. 결국 미국의 경우에는 지금까지 완결된 개인정보보호시스템은 존재하지 않고 情報處理를 규제하는 범위구체적인 法律들이 존재한다는 것을 확인할 수 있다.[28] 게다가 法院의 判例에서 시민의 프라이버시권은 지금까지 전적으로 國家의 제한으로부터 보호받아야만 되는 權利로 이해되었지 다른 私人으로부터 보호되어야만 하는 것으로는

---

25) section 5, 6, 7, 8.

26) 私的 領域들의 규율은 부분적으로 다음 법률들에 의해서 행해진다. 예를 들어 이에 관한 법으로는 1970년 공정신용기록법(Fair Credit Reporting Act), 1974년 공정신용경리법(Fair Credit Billing Act, 1976년 개정), 1974년 가족교육권 및 프라이버시법(the Family Educational Rights and Privacy Act, 1976년개정), 1977년 공정한 채무수집실행법(the Fair Debt Collection Practices Act), 1978년 금융프라이버시권에 관한 법(the Right to Financial Privacy Act), 1988년 컴퓨터연결과 프라이버시보호법(the Computer Matching and Privacy Protection Act) 등이 있다.

27) 5 USC 552 a (a) 2.

28) Marie-Theres Tinnefeld, Der Datenschutz in den Vereinigten Staaten, RDV 1992, S. 216.

이해되지 않는다. 따라서 私的 領域에서 個人情報를 보호하고자 하는 일반적 형태의 연방법은 지금까지 제정되지 않았고 개별영역을 위한 法律들이 부분적으로 있을 뿐이다.[29] 결론적으로 미국의 개인관련정보보호시스템을 유럽의 시스템과 비교한다면 우선 美國法律의 適用範圍는 매우 제한되어 있으며 聯邦의 次元에서 본다면 個人情報를 보호하기 위한 法律들이 다수 있기는 하나 이는 언제나 다소 제한된 일부영역만을 규율대상으로 하고 있기 때문에 개인정보보호에 관한 일관성있는 시스템은 확인되지 못한다고 말할 수 있다.[30]

오스트레일리아의 프라이버시보호法律들은 영국의 法律들과 매우 비슷하다. 聯邦次元에서 濠洲는 프라이버시문제연구에 상당한 주의를 기울였다. 1973년 정부는 법개혁위원회를 만들었고 이 委員會는 1976년 프라이버시보호에 관한 회의를 열고 프라이버시보호에 관한 입법 및 이에 관한 다른 조치들을 제안하였다. 특히 이당시에 컴퓨터를 통한 정보저장시스템들에 많이 주목하기 시작하였다. 1983년 12월 聯邦의 法改革委員會는 개인의 불평을 조사할 권한을 갖고 있는 연방프라이버시위원의 창설을 권고하였다. 연방프라이버시법은 1986년 당시의 法律草案을 강화하여 1988년에 제정되었다. 1986년 法案은 국가적인 개인신원카드(오스트레일리아카드)를 도입하고자 하는 法案과 함께 제출되었으나, 국민들의 격렬한 반대로 인하여 개인신원카드를 도입하고자 하는 계획은 취소되었던 반면에 프라이버시법규정은 더욱 더 엄격해졌다.[31] 그럼에도 불구하고 호주의 프라이버시법은 여전히 유럽의 個人情報保護法보다는 미국의 프라이버시법과 유사하였다. 이 법은 公的 領域만을 포함할 뿐이었다. 어쨌든 이 법에 담긴 11가지 기본원칙들은 본질적으로 OECD지침이나 유럽연합의 개인정보보호협약에 담긴 원칙들과 동일하였다. 1982년에 호주에서 제정된 情報自由法은 聯邦政府가 보관하는 공적인 기록들에 시민들의 일반적인 접근권을 확립하였다. 오스트레일리아의 프라이버시법에서 개인의 프라이버시를 보호하기 위하여 가장 중요한 것은 자동화되었든 手作業이든간에 개인파일에 접근할 권리 및 이를 수정할 권리를 개인에게 인정하였다는 것이다.

第3節 個人情報保護法만을 制定한 國家들

獨逸은 情報社會에서 個人의 私生活을 보호하고자 가장 먼저 個人情報保護法律을 제정한 나라들중 하나에 속한다. 聯邦次元에서 이미 1977년에 個人情報保護法을 제정하였으며 1983년 獨逸聯邦憲法法院의 人口調査判決은 그 당시 獨逸聯邦政府가

29) Stephan Wilske, Datenschutz in den USA, CR , 1993, S. 299.
30) Stephan Wilske, a.a.O., S. 307.
31) James Michael, ibid., p. 90.

계획하고 있었던 人口調査를 연기시키고, 人口調査法의 개정을 불러왔을 뿐만 아니라, 컴퓨터가 읽을 수 있는 개인확인카드시스템의 도입 또한 취소시켰다.[32] 그러나 獨逸은 컴퓨터의 사용으로 인하여 個人의 私生活이 침해되는 위험성을 막고자 하는 法律을 제정하는데에 대부분의 노력을 기울였을뿐 정부가 보관하는 情報에 市民이 일반적으로 접근하는 권리를 보장하는 法律을 제정하고자 하는 노력은 聯邦이나 州 次元에서 거의 행해지지 않았다. 1970년대 후반에 聯邦個人情報保護法에 관한 草案을 만들 때 연방정부는 국가정보처리의 효율성을 높이기 위하여 국가적인 個人確認番號(개인확인카드시템)를 도입하고자 하였다. 그러나 다른 나라에서처럼 컴퓨터를 통한 개인기록의 사용 및 컴퓨터로 확인할 수 있는 개인신원번호의 도입에 관한 法律案들은 채택되지 않은 반면에 個人情報를 보호하는 法案은 받아들여졌다. 그러나 독일에서 私的 領域의 規制는 스칸디나비아국가들이나 영국과 같은 나라들의 시스템과는 아주 다르다. 곧 獨逸의 개인정보보호시스템상 私的 領域에서 個人情報를 처리할 때 私的 情報處理機關은 이에 관하여 일반적으로 기록할 의무를 갖고 있지 않다. 다만 獨逸의 個人情報保護法에 따르면 公的, 私的 領域에서 관련개인에게 자신의 기록에 접근할 권리 및 이에 관한 수정권과 삭제권이 보장된다. 그러나 이러한 권리들은 절대적으로 보호되는게 아니라 경우에 따라서 제한될 수 있었다. 어쨌든 聯邦憲法法院의 人口調査判決이후에 獨逸에서 個人情報保護法이 1990년에 크게 개정되었을 뿐만 아니라 公的, 私的 領域에서 個人情報를 보호하고자 하는 많은 特別法들이 제정되었다.

룩셈부르크는 1979년에 個人情報保護法을 제정하였다. 그리고 같은 해에 政府情報에 接近法이 제정되었다. 그러나 이 法은 정부가 보관하고 있는 기록이나 정보에 시민들이 일반적으로 접근할 권리를 보장한다기 보다는 법적 이해관계를 갖는 사람들이 해당 기록들에 접근할 권리만을 부여하므로 일반적으로 情報自由法으로 언급되는 法律에 포함시켜서는 안된다.

英國에서는 法院이나 議會 모두 개인의 프라이버시를 보호하기 위한 法律을 만드는 데에 특별히 적극적이지 않았다.[33] 그럼에도 불구하고 많은 논란 끝에 1984년 個人情報保護法이 제정되었는데 이 법은 自動的으로 처리되는 個人情報만을 규제대상으로 삼는다. 그리고 영국에서도 또한 情報自由法이 제정되어야만 한다고 野黨, 市民團體 등이 강력하게 주장하였지만 與黨과 政府의 반대로 인하여 결국 情報自由法은 제정되지 못하였다.

1988년에 제정된 아일랜드의 個人情報保護法은 자동화된 기록들만을 규제대상으

32) James Michael, ibid., p.93.
33) James Michael, ibid., p.100.

로 하며 公的, 私的 領域 모두를 포함하나 민감한 개인정보를 저장하는 기관들중에서 특정 기관들에게만 이에 관하여 기록하도록 요구함으로써 해당 기관의 自己規制를 강조하였다.

오스트리아의 個人情報保護法에 따르면 해당 개인은 자신의 情報가 비밀로 지켜지는 것을 요구할 권리를 갖고 있다.[34] 이 법의 草案은 1971년 나왔으나 1978년까지는 제정되지 않았다. 우선 이 법은 公的, 私的 領域 情報處理 모두를 포함하며 手作業記錄은 물론 자동처리되는 기록들에게도 적용된다. 公的 領域에서 규제는 情報保護委員會가 담당하며, 公的 領域에서 개인정보의 수집과 처리는 명시적인 제정법상 권한에 근거해야만 한다. 私的 領域에서 정보처리의 규제는 개인정보의 처리를 위한 어떤 정당한 목적 - 保護價値있는 정보주체의 이익에 대하여 형량되어야만 하는 - 을 요구한다. 자신의 정보가 자동적으로 처리되는 관련 개인들은 정보처리에 관하여 알 권리가 인정됨으로써 그 보호가 시작된다. 다시 말하면 公的 領域과 私的 領域 모두에서 이러한 情報處理가 公的으로 記錄됨으로써 관련개인은 자신의 정보가 어떻게 처리되는지를 알 수 있게 된다. 추가로 정보주체는 누가 정보처리담당자인지, 어디로부터 情報를 획득하였는지, 무엇을 처리하였는지, 무엇을 위하여 사용되었는지 등을 알 권리를 갖게 된다. 다만 公的 領域과 私的 領域들간에 구별되는 중요한 것은 公的 領域에서 개인의 주관적인 접근권은 위 法律에서 인정되는 중요한 公益을 바탕으로 하여 거부될 수 있는 반면에, 私的 領域에서 이러한 접근의 거부는 책임 있는 사람이나 제3자의 중요한 정당한 이익들에 바탕을 둘 수 있다는 것이다. 情報保護委員會는 公的 領域에서 일반적인 조사와 권고권한을 갖고 있으며 해당부서는 위원회의 이러한 권고를 받아들이지 않은 이유를 위원회에 제시해야만 한다. 더 나아가서 이 법에 따르면 市民에게 본인의 기록에 관한 접근권과 교정권 및 추가적으로 민사법원을 통한 損害賠償請求權이 인정된다. 情報保護委員會는 5년의 임기로 임명되는 4명의 위원들로 구성되어 있다. 이러한 委員會는 규제기관과 行政法院을 결합한 형태의 구조를 갖고 있다. 그 규제기능들은 대부분 私的 領域에 집중되어 있으며 公的 領域에서 委員會가 행하게 되는 주요 기능중 하나는 개인의 권리가 침해되었다는 불평을 접수하고 검토하는 것이다.

1981년에 제정된 아이슬랜드의 個人情報保護法은 1982년부터 시행되었는데 이 법은 덴마크법의 個人情報保護法과 거의 비슷하였다. 1986년에 이 법은 다시 개정된 후에 결국 1990년에 제정된 個人情報의 記錄 및 處理에 관한 법(Act Concerning the Registration and Handling of Personal Data)에 의하여 대체되었다.

---

34) 개인정보보호법 제1조제1항.

특히 새로 제정된 이 법은 輿論調査 및 市場調査에 관한 특별규정들을 갖고 있다. 곧 이 법에 따르면 輿論調査에 의하여 획득된 개인관련정보는 즉시 삭제되거나 개인의 身元確認을 불가능하게 만드는 방법으로 저장되어야만 한다고 규정하였다. 또한 이 법은 公的 領域과 私的 領域 모두를 규율하며 개인의 財政問題나 信用等級에 관한 정보처리, 컴퓨터서비스제공, 외국으로 제공되는 情報處理와 같은 활동들에 관하여 委員會의 허가를 받도록 규정하였다. 그리고 이 법에 따라서 人種, 政治的 또는 宗教的 信念, 刑事記錄, 性行爲, 健康記錄, 알코올중독에 관한 개인정보를 처리하기 위해서는 이에 관한 제정법상 근거 및 이러한 정보처리가 필요하다는 입증이 요구된다. 마지막으로 이 法은 독립된 3명의 情報委員會 - 허가를 부여하고 분쟁을 해결하는 - 에 의하여 집행된다.

1981년에 제정된 이스라엘의 프라이버시법은 개인의 프라이버시를 일반적으로 보호하는 것에 관한 법으로서 個人情報保護에 관한 규정들이 이 속에 담겨있다. 이 법의 첫 번째 章은 非公的 機關에 의하여 행해지는 프라이버시권의 侵害行爲를 상세하게 열거한다. 예를 들어 盜聽, 사진이나 비디오촬영, 秘密情報의 出版 등이 이러한 침해행위에 포함된다. 이 法의 두 번째 章은 개인정보보호조치에 관한 것이다. 예를 들어 이 章에는 개인의 주관적인 접근권 및 잘못된 정보의 수정권이 규정되어 있으며 분쟁은 거의 대부분 法院을 통하여 해결된다. 계속해서 이 두 번째 章은 개인의 지위, 비밀정보, 건강상태, 경제상황, 개인에 관한 의견이나 평가를 언급하는 정보를 처리하는 데이터베이스에 관한 책임을 지고 있는 사람들에 관한 여러 규정들을 두고 있다.

1975년의 포르투칼헌법은 제33, 34조에서 프라이버시에 관한 권리를 규정하고 있다. 특히 憲法 제35조는 개인정보처리에 관한 규정을 담고 있다 : "1. 모든 시민들은 자기에 관한 情報銀行의 내용 및 사용목적에 관한 정보권을 가져야만 한다. 이들 시민들은 자신의 정보에 관한 삭제권 및 수정권을 가져야만 한다. 2. 情報處理는 統計目的을 위하여 확인할 수 없는 정보의 경우를 제외하고는 개인의 정치적 신념, 종교적 믿음이나 私生活에 관한 정보를 다루어서는 안된다. 3. 시민들은 모든 목적의 국가적인 확인번호를 가져서는 안된다." 또한 1989년에 改正된 憲法 제35조는 다시 "① 國家秘密과 司法秘密에 관한 法律을 제외하고는 모든 시민들은 자기에 관한 情報銀行의 내용 및 使用目的에 관한 정보권을 가져야만 한다. 이들 시민들은 자신의 정보에 관한 삭제권 및 수정권을 가져야만 한다. ② 개인정보나 파일에 접근은 法律에 규정된 예외적인 경우를 제외하고는 금지되어야 하고, 특히 이러한 파일들의 內的 連結은 물론 제3자에 대한 정보획득의 목적을 위한 접근은 금지되어야

한다. ③ 統計目的을 위하여 확인할 수 없는 정보를 다루는 경우를 제외하고는 개인의 철학적이거나 정치적 신념, 종교적 믿음, 政黨과 勞動組合에 가입여부, 私生活에 관한 情報가 다루어져서는 안된다. ④ 法律은 公的, 私的 領域에서 情報銀行과 데이터베이스를 만들 조건과 활용 및 접근조건은 물론 정보저장목적을 위하여 個人情報의 개념을 규정해야만 한다. ⑤ 시민들은 모든 목적의 국가적인 확인번호를 가져서는 안된다. ⑥ 法律은 국경 없는 정보흐름에서 국가이익상 그 보호가 정당화되는 다른 정보와 個人情報의 보호에 관하여 적절한 규정을 만들어야만 한다."고 규정하고 있다. 이에 따라서 마침내 1991년 個人情報保護法이 제정되었다. 이 법은 公的 領域과 私的 領域에서 自然人들에 관하여 自動的으로 처리되는 기록들에 적용된다. 그리고 이 法律은 자동화된 개인기록들의 보호를 위하여 國家委員會를 만들었는데, 이 위원회는 個人의 주관적인 접근권과 수정권의 보호에 관하여 감독하고 통제한다. 또한 이 委員會는 자동화된 파일들의 내부적 연결을 금지하고, 민감한 정보들을 서로 연결하기 위한 個人確認番號의 사용을 금지하며, 더 이상 필요하지 않는 정보의 삭제를 요구할 권한을 갖고 있다. 그리고 권한 없이 파일을 삭제하는 것은 물론, 권한 없이 파일을 만드는 것도 이 법에 따라서 처벌된다.

日本은 1988년 個人情報保護法을 제정하였다. 이 법은 公的 領域에서 국가행정기관을 통한 정보처리에만 적용된다. 이 法에서 개인의 주관적인 접근권과 수정권은 규정되었으나 이에 관한 몇몇 제외사유가 있다.

그리스는 1986년 행정서류에 관한 접근법을 제정하였고, 1991년 이를 다시 개정하였다. 이 법은 프랑스法律과 매우 유사한 것으로서, 제3자의 私生活이나 家族生活과 관련되지 않는 한, 정부기록을 열람하고 복사할 시민의 일반적인 권리를 확립한다. 그러나 시민과 국가간 관계에서 신원(확인)카드와 연결되어 프라이버시를 보호하는 法律이 있다.[35] 이 法律은 인구기록, 선거기록, 조세기록, 사회보장기록, 운전면허기록과 같은 다양한 데이터베이스들간 정보연결을 금지하며 이러한 연결목적을 위한 개인확인번호의 사용을 금지하고 있다.

第4節 小 結

1. 國際的 情報秩序

위에서 설명한 것처럼 "情報秩序"란 개념은 전반적이고 구체적으로 이미 확정된 개념이 아니라 經濟秩序와 아주 유사하게 한 사회내에서 情報調査나 處理 등에 관

35) Law No. 1599/1986.

하여 나름대로의 原則과 基準을 제시하는 모델개념이다. 결국 이러한 情報秩序를 통하여 구체적으로 情報處理 및 傳達과 관련되는 모든 규정들에 관하여 상세하게 그 내용을 알 수는 없지만 한 사회의 全體情報秩序를 이끄는 原則이나 基準을 추상적이고 일반적으로 제시해야만 하는 바로 그러한 것들을 얻을 수 있다. 왜냐하면 情報秩序에 관한 이러한 원칙적인 논의와 事前理解가 우선 선행되어야 개개 분야에서 이러한 원칙과 기준이 어떻게 적용되어야만 하는지를 제대로 살펴볼 수 있기 때문이다. 따라서 情報秩序에 관한 논의나 개개 분야에서 구체적으로 어떤 결과가 도출되어야만 하는가는 情報通信技術의 적용에 따른 현실적, 실제적 문제가 아니라 우리가 規範的으로 근거하고 있는 原則 및 基準에 따라 판단해야만 하는 當爲的 問題이다. 결국 情報處理의 이용가능성, 위험성여부, 효율성 등에 관한 판단은 새로운 情報通信技術을 적용함으로써 얻게 되는 것이 아니라 이에 관한 組織的, 法的, 社會的 前提條件에 따라서 행해진다.

그런데 이러한 情報秩序는 國際的 情報秩序와 國內的 情報秩序로 나누어 파악할 수 있다. 우선 국제적 차원에서 世界情報秩序가 어떻게 형성되어야만 하는지를 살펴본다면 무수한 토론에도 불구하고 아직까지 전체가 합의하는 世界情報秩序에 관한 정확한 윤곽을 그려낼 수는 없다.

우선 UN총회는 1946년 12월 14일 결의에서 "情報自由는 UN이 기초하고 있는 모든 自由들의 초석이며 이는 基本的 人權이다. 情報自由는 情報를 모으고 구속없이 언제나 어느 곳에나 정보를 전하고 출판할 권리를 포함한다."고 결정하였다. 1949년의 普遍的 人權宣言은 제19조에서 意思와 情報自由를 규정하고 있으며 市民權과 政治的 權利에 관한 1966년 人權規約 제19조제2항에서 다시금 자유로운 意思表現權이 보장되고 있다. 이러한 權利는 국경을 고려하지 않고 單語, 文字, 印刷 또는 다른 수단으로 된 모든 종류의 情報와 생각들을 형성하거나 받고 전달할 자유를 포함한다. 그리고 유럽인권선언 또한 제10조제1항제1절에서 情報自由를 보장하고 있다.

그런데 國際的인 情報秩序를 형성하고자 할 때 先進國에서는 "정보의 자유로운 흐름"을 주장하는 반면에 開發途上國들은 이러한 情報의 자유로은 흐름을 통하여 그들의 文化的 同一性이 상실되고, 이에 따라서 결국에는 先進國에 커다랗게 의존할 수밖에 없는 상황이 벌어지는 소위 "文化帝國主義"를 두려워한다. 위에서 설명한 것처럼 현행 國際法原則이 우선 意思自由와 情報自由를 지향하고 있기 때문에 어떠한 규제없이 情報가 자유롭게 유통되어야만 한다는 것이 先進國의 주장이다.[36] 이

36) 이미 60, 70년대에 정보의 자유로운 흐름에 관하여 서구민주주의국가들과 사회주의국가들 간에 대립이 있었다.

에 반하여 거의 모든 정보영역에서 외국, 특히 先進國으로부터 제공되는 서비스에 의존하는 開發途上國은 情報通信技術分野에서 국가운영상 중요한 社會間接資本의 기반이 외국에 있다는 것을 특히 민감하게 받아들이고 있기 때문에 이러한 영역에서 어느 정도 독립성을 한 국가의 主權保護와 동일시하는 경향이 매우 강하다.[37] 결국 새로운 世界情報秩序에 관한 開發途上國들의 요구는 한편으로 先進國과 開發途上國間 자유로운 정보흐름을 필요하다고 생각하는 경우에 차단할 수 있어야만 한다는 것이고 또다른 한편으로 國際的으로 開發途上國에 대한 정보의 통제와 왜곡을 철폐하자는 것으로 요약된다.[38]

위에서 설명한 것처럼 어쨌든 情報自由는 國際法上 人權으로 보장되고 있으나 이러한 자유로운 정보흐름이 현실화된 결과로서 나타나는 "情報多元主義"는 오늘날 상이한 역사적, 경제적, 사회적, 법적 전통을 근거로 하여 많은 반대에 부딪히고 있다. 그럼에도 불구하고 처음부터 정보의 자유로운 흐름, 또는 情報多元主義와 文化的, 個人的 同一性保護 또는 私生活保護間에 일차원적이고 평면적인 대립관계를 설정하는 것은 문제가 있다. 결국 情報多元主義란 국경을 넘는 정보흐름이 개개 국가의 법규정을 통하여 제한받아서는 안된다는 원칙으로 이해된다.[39] 이러한 의미에서 情報多元主義는 지금까지 대개 西歐-民主主義國家들을 지탱하는 문화의 구성적 요인으로 파악되었다. 여기서 정보의 자유로운 흐름과 文化的, 個人的 同一性保護間 關係設定問題는 국경을 넘는 정보의 자유로운 흐름을 원천적으로 봉쇄하는 것이 아니라 그 "限界"와 "拘束"을 설정하자는 문제임을 인식해야만 한다.[40] 따라서 예를 들어 開發途上國이 국제통신에 평등하게 참여함으로써 개개 통신담당자의 권리를 제한할 수도 있으나 이러한 제한은 오히려 사실상 情報多元主義의 창출에 따르는 부수적 효과일 수도 있다. 그렇다면 文化的, 個人的 同一性保護와 정보의 자유로운 흐름은 동시에 모두 保障되어야만 하는 것으로서 어느 한쪽이 다른 한쪽보다 우월할 수 없는 것이다.[41]

이와 더불어 國際法的으로 또한 個人情報保護와 국경을 넘는 자유로운 정보흐름

---

37) Dietrich Rauschning, Der Zugang zu dem internationalen Informationsverteilungssytem als Forderung des Völkerrechts?, Wolfrum, Rüdiger (Hrsg.), *Recht auf Information Schutz vor Information*, Duncker & Humblot, 1986, S. 133.

38) Dietrich Rauschning, a.a.O., S. 136.

39) Jost Delbrück, Die kulturelle und individuelle Identität als Grenzen des Informationspluralismus?, Wolfrum,Rüdiger (Hrsg.), *Recht auf Information Schutz vor Information*, Duncker & Humblot, 1986, S. 185.

40) Jost Delbrück, a.a.O., S. 186.

41) Jost Delbrück, a.a.O., S. 193.

간 관계가 토론되고 있다. 情報의 자유로운 흐름과 個人情報保護는 情報社會에서 모두 다 보호되어야만 하는 중요한 기본적인 가치들이기만 하지만, 이들은 때때로 상호 충돌할 수 있으며 특히 個人情報의 보호를 통하여 보장하려는 個人의 私生活은 정보의 자유로운 흐름에 관한 제한들 속에 반영되어 있다. 다만 위에서 설명된 관점에 따라서 個人情報保護와 정보의 자유로운 흐름간 관계도 해결되어야만 한다. 곧 個人情報保護와 정보의 자유로운 흐름중 어느 한쪽이 다른 한쪽에 비하여 언제나 절대적으로 우월하다고는 말할 수 없다. 오히려 인간지향적인 情報社會를 지향하기 위해서는 兩者가 조화될 수 있도록 해야만 한다. 따라서 정보의 자유로운 흐름은 그 제한을 정당화할 수 있는 구체적 권리 - 個人情報保護, 個人의 私生活 - 가 인식되어야만 하며 이러한 개인의 私生活權과 정보의 자유로운 흐름간 충돌을 해결하기 위한 법적 장치가 구체적으로 마련되어야만 한다. 따라서 여러 國際條約 등은 우선 정보의 자유로운 흐름을 보장하는 틀 내에서 個人情報保護에 관한 일반적 기준을 확립하고자 노력한다.[42] 결국 1960년대 후반에서 70년대 초반에 차츰 자동화된 정보처리가 개인의 私生活權에 대하여 미칠 수 있는 영향에 관하여 국제적 차원에서 관심을 갖게 되었다.[43] 먼저 1948년 世界人權宣言(Universal Declaration of Human Rights) 12조는 프라이버시가 보호되어야만 한다고 규정하고 있을 뿐만 아니라 더 나아가 이 人權宣言 12조에서 정교화된 프라이버시권은 人權宣言의 다른 조항들에서 더 구체적으로 보호되고 있다. 특히 個人情報의 보호에 관해서는 1990년 12월 14일 UN총회의 결의로 채택된[44] 컴퓨터화된 개인정보파일의 규율에 관한 지침(Guidelines for the regulation of computerized personal data files)을 주목해야만 한다.

2. 個人情報保護에 관한 國際的, 國內的 基準

個人情報保護에 관한 國際的, 國內的 基準들을 살펴보면 이미 설명된 것처럼 개개 국가의 政治的, 行政的, 法的 傳統이나 法體系의 상이함 때문에 구체적인 법규정이나 統制機關의 權限 등에 관하여 많은 차이를 보이고 있다. 그럼에도 불구하고 情報社會에서 個人情報가 보호되어야만 한다는 공통되는 인식과 더불어 그 보호에 관한 공통되는 기준이나 원칙들이 나름대로 확립되어 있음을 파악할 수 있다. 이에 따라서 國際的, 國內的으로 個人情報保護에 관한 일반적 기준들을 요약하여 설명하

42) James Michael, ibid., p.47.
43) James Michael, ibid., p.32.
44) Resolution 45/95.

고자 한다. 이러한 설명은 과연 우리 나라의 個人情報保護法制가 이러한 國際的, 國內的 基準에 부합되는지를 살펴볼 수 있는 중요한 척도를 제공한다는 점에서 중요한 의미를 갖는다.

1) 國際的 基準

(1) 國際聯合(UN)

情報社會에서 個人情報를 보호하기 위한 1990년 12월 14일 UN총회의 결의로 채택된[45] 컴퓨터화된 개인정보파일의 규율에 관한 지침(Guidelines for the regulation of computerized personal data files)은 個人情報保護를 위하여 다음과 같은 원칙들을 담고 있다 : 1) 合法性과 公正性原則(Principle of Lawfulness and Fairness) : 個人에 관한 情報는 합법적인 방법으로 수집, 처리되어야만 하고 UN헌장에 명시된 목적과 원칙에 반해서는 안된다. 2) 正確性原則(Principle of Accuracy) : 情報를 수집하거나 저장하는 사람 및 이에 관하여 책임있는 담당자는 個人情報를 정기적으로 검사하여 수록된 정보가 정확한 정보인지를 검토해야만 한다. 3) 目的具體性原則(Principle of the Purpose-specification) : 個人情報를 수집하고 처리는 목적이 구체적이고 정당해야만 한다. a) 이에 따라서 수집, 저장되는 이러한 모든 個人情報는 구체화된 목적과 관련되며 필요한 것이어야만 한다. b) 이러한 個人情報는 관련개인의 同意가 없는 한 사용되거나 공개되어서는 안된다. c) 수집된 個人情報의 저장은 구체화된 목적을 위하여 필요한 기간을 넘어서는 안된다. 4) 관련개인에 의한 접근원칙(Principle of Interested-person Access) : 정보가 수집되거나 저장된 해당 개인은 이러한 정보가 어떻게 처리되며 사용되는지에 관하여 알 權利를 갖고 있으며 잘못되거나 정확하지 못한 정보의 삭제권 등 여러 권리들이 이러한 개인들을 위하여 제공되어야만 한다. 5) 非差別原則(Principle of Non-discrimination) : 해당 정보의 주체들은 그 宗教的, 人種的, 性的 差異나 政治的 見解 등을 이유로 부당하거나 자의적인 차별을 받아서는 안된다. 6) 예외에 관하여 결정할 수 있는 기관(Power to make Exceptions) : 위에서 열거된 원칙으로부터 예외가 인정되는 경우로는 國家安全保障, 秩序維持, 他人의 自由와 權利保護 및 反人類的 犯罪를 범한 범인추적처럼 그 목적과 근거가 국내법절차에 따라서 정당하게 제정된 법규정에 구체화된 경우에 인정될 수 있다. 7) 安全(保安)原則(Principle of Security) : 자연재앙이나 컴퓨터바이러스, 권한없는 접근 등으로부터 이러한 개인정보파일을 보호하기 위한 적절한 조치들이 행해져야만 한다. 8) 監督과 制裁(Supervision and Sanctions) : 모든 國家들은 열

45) Resolution 45/95.

거된 원칙들의 준수를 감시할 독립된 기관을 설치해야만 하고 이러한 원칙들을 위반한 경우에 대비하는 처벌규정 및 개인보호규정들도 만들어야만 한다. 9) 국경 없는 정보흐름(Transborder Data Flows) : 個人情報가 한 국가에서 다른 국가로 전달될 때 이러한 정보를 전달받는 國家들에서 개인의 私生活保護에 관한 충분한 보호대책들이 마련되어 있다면 정보는 관련 국가들 내에서 가능한 한 자유롭게 전달, 처리될 수 있어야만 한다. 10) 適用範圍(Field of Application) : 이러한 원칙들은 모든 公的, 私的 機關들에 적용되어야만 하고 컴퓨터파일뿐만 아니라 수작업파일도 적용대상에 포함된다.

(2) 유럽연합(EU)

유럽내에서 個人情報의 保護에 관한 것으로는 유럽연합이 1981년 2월 28일 서명하고 1993년에 개정한 個人情報의 自動處理에 관한 個人保護를 위한 協定(Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)이 있다. 특히 유럽협약 제5조와 제16조에 個人情報保護에 관한 기본원칙들이 규정되어 있다 : 情報가 자동적으로 처리된다면 이들은 ⓐ공정하고 합법적으로 획득되어야 하고, ⓑ구체적이고 정당한 목적을 위해서만 저장되어야 하며 이러한 목적들과 양립할 수 없는 방법으로 사용되어서는 안되고, ⓒ 저장목적과 해당 정보간에 적절한 관련성이 있어야 하며, 이를 넘어서는 저장은 허용되지 않으며, ⓓ個人情報는 올바르고 필요한 경우에는 최신의 것이어야만 하며 부정확하거나 불충분한 정보는 삭제되거나 수정되어야만 하고, ⓔ 情報는 저장되는 목적을 위하여 필요한 시간만큼 보존되어야만 한다. 이 협약은 個人情報가 어떤 목적으로 저장될 수 있는지에 관하여 설명하지는 않으나, 최소한 구체화되지 않은 목적을 위한 個人情報의 수집을 금지한다. 특히 협약 제17조에는 人種, 政治的 見解, 宗教的·哲學的 信念이나 勞動組合加入與否, 健康情報나 性生活情報와 같은 個人情報는 國內法이 적절한 보호를 제공하지 않는 한 자동적으로 처리될 수 없다고 규정되어 있다. 협약 제7조는 가입국들에게 公的 分野에서 個人情報의 保護를 감독할 기관의 설치 및 적절한 보안조치들을 요구한다. 협약 제12조 이하는 정보주체들의 권리들에 관한 것이다. 이 조항들에서 자신들에 관한 자동화된 정보파일들이 있는지를 알 권리, 내용열람권, 삭제권이나 수정권 등이 정보주체에게 인정된다.

(3) 經濟協力開發機構(OECD)

個人情報의 保護에 관한 또다른 국제적 협정으로는 OECD위원회가 1980년 9월 23일 채택한 私生活保護 및 個人情報의 국경 없는 흐름에 관한 지침(Guidelines

on the Protection of Privacy and Transborder Flows of Personal Information)이 있다. OECD지침의 중요내용을 살펴보면 다음과 같다 : 1) 蒐集制限原則(Collection limitation principle) : 個人情報蒐集에 관하여 다음과 같은 제한이 있다. 곧 個人情報는 정보주체가 인식하거나 同意한 후에 합법적이고 공정한 방법들에 의하여 蒐集되어야만 한다. 2) 情報內容原則(Data quality principle) : 個人情報는 이들이 사용되는(또는 될 수 있는) 목적들과 관련되어야만 하며, 이러한 목적들을 위하여 필요한 만큼 정확하고 완전(충분)하며 최신의 것이어야만 한다. 3) 目的具體化原則(Purpose specification principle) : 個人情報의 수집목적은 사전에 구체화되어야만 하지 정보수집이후에 구체화되어서는 안되고, 개인정보의 계속적인 사용은 이러한 목적들과 양립할 수 있어야만 한다. 목적의 변경은 개개 경우에 구체화되는 목적들의 이행을 위한 경우로 제한되어야만 한다. 4) 利用制限原則(Use limitation principle) : 정보주체의 동의가 있거나, 법에 근거한 경우를 제외하고 個人關聯情報는 사전에 구체화된 목적들과는 다른 목적으로 사용, 이용되거나 공개되어서는 안된다. 5) 安全保護原則(Security safeguards principle) : 個人情報는 정보의 손실이나 권한 없는 접근, 파괴, 사용, 변형이나 공개와 같은 그러한 위험으로부터 합리적인 보안장치에 의하여 보호되어야만 한다. 6) 公開原則(Openness principle) : 個人情報에 관한 개발, 운용, 정책들에 관해서는 일반적인 공개정책이 택해져야만 한다. 個人情報의 존재와 내용, 이러한 정보사용의 주요목적은 물론 정보관리자의 신원 및 통상적인 거주지는 즉시 이용·확인할 수 있어야만 한다. 7) 個人參加原則(Individual participation principle) : 관련 개인은 a) 정보관리자가 본인과 관련되는 정보를 갖고 있는지 여부를 확인할 권리를 갖고 있어야만 하고 b) 필요하다면 과도하지 않은 비용 내에서 합리적 시간 내에서 적당한 방법으로 본인과 관련되는 정보에 관하여 개인에게 즉시 알려질 수 있는 있어야만 하고 c) a)와 b)가 거부된다면 이에 대한 이유제시 및 이러한 거부에 대하여 異議를 제기할 수 있어야만 하고 이의제기가 받아들여진다면 그에 관한 情報는 삭제, 개정, 보충 또는 수정되어야만 한다. 8) 責任原則(Accountability principle) : 정보관리자는 위에서 설명된 원칙들에 영향을 주는 조치들에 따르는 책임을 진다.

2) 國內的 基準

(1) 플래허티의 기준

個人情報保護法에 규정되어야 할 기본원칙으로 플래허티는 다음과 같은 것을 언

급하고 있다 : ①國家의 개인정보시스템들에 관하여 公開性과 透明性原則 ②個人情報의 수집과 저장시 해당 정보의 必要性과 關聯性原則 ③가능한 한 최대한의 정도로 個人關聯情報의 수집, 사용, 저장을 줄이는 원칙 ④사전에 확립된 목적에 따라 個人情報를 처리, 이용하라는 最終性原則 ⑤개인정보시스템들에 관하여 책임질 사람들을 확정하라는 원칙 ⑥個人情報의 연결, 전달, 결합을 통제해야만 한다는 원칙 ⑦個人情報의 수집을 위하여 個人의 同意를 요구하는 원칙 ⑧개인정보시스템들에서 個人關聯情報의 正確性과 完全性을 명령하는 원칙 ⑨個人情報의 不法濫用에 대한 민·형사처벌을 포함하여 個人情報에 違法한 侵入禁止의 原則 ⑩민감한 個人情報의 특별한 보호명령 ⑪개인정보를 저장하거나 처리하는 정보시스템에 해당 개인의 접근권과 수정권 ⑫거의 모든 個人情報의 궁극적인 匿名化나 삭제를 포함하여 잊혀질 권리의 규정요구.[46]

(2) 페리트기준

페리트는 個人情報보호에 관한 기준으로 다음과 같은 것을 제시하였다 : ①어떤 개인정보시스템도 비밀리에 유지되어서는 안된다. ②個人은 자신에 관한 어떤 정보가 기록되고 어떻게 사용되는지를 알 수 있는 수단을 갖고 있어야만 한다. ③하나의 목적을 위하여 획득된 個人情報를 이들의 동의 없이 다른 목적을 위하여 사용하지 못하도록 금지시킬 수 있는 手段을 개인은 갖고 있어야만 한다. ④個人에게 자신에 관한 잘못된 정보를 수정하거나 고칠 수 있는 수단이 보장되어야만 한다. ⑤제3자에게 특정한 個人情報를 공개하는 것에 관하여 제한이 가해져야만 한다. ⑥자신의 정보에 관한 수정이나 삭제요구가 거절된 개인은 해당 기록 속에 포함되고 나중에 함께 공개되어야만 하는 不一致陳述을 할 수 있어야만 한다. ⑦어떤 개인을 확인할 수 있는 情報記錄을 만들고, 이를 유지하고, 사용하거나 유통시키는 기관들은 해당 個人情報의 신뢰성을 보장하고 정보의 濫用을 막기 위한 합리적인 예방책들을 마련해야만 한다. ⑧해당 개인은 위와 같은 자신의 요구가 받아들여지지 않거나 情報記錄機關의 義務違反審査를 제기할 수 있는 手段을 갖고 있어야만 한다.[47]

(3) David F. Linowes의 기준

美國에서 1991년에 共和黨 議員 Wise가 個人情報保護法案을 제출하였는데, 이 法案에 관한 聽聞會에서 1977년 미국프라이버시보호연구위원회의 議長이었던 David

46) David H. Flaherty, *Protecting Privacy in Surveillance Societies*, The University of North Carolina Press, 1989, p.380.

47) Henry H. Perrit Jr., *Law and the Information Superhighway*, Wiley Law Publications, 1996, p.91.

F. Linowes는 個人情報를 보호하기 위하여 다음과 같은 原則들을 강조하였다 : ① 구체적 결정들과 관련되는 情報만이 수집되어야만 하고 수집된 정보는 이러한 목적을 위해서만 사용되어야 한다. ② 관련개인의 同意나 최소한 해당 개인에게 통지 없이 제3자에게 어떠한 個人情報도 전달되어서는 안된다. ③ 國家가 어떻게 이러한 정보를 수집하고 사용하였으며 누구에게 공개하는지를 해당 개인에게 통지해야만 한다. ④ 관련개인은 자신에 관한 기록들을 열람하고 복사할 권리를 가져야만 한다. ⑤ 관련개인은 기록의 정확성에 관하여 질문하고 이를 修正할 권한을 가져야만 한다. 記錄의 眞否에 관하여 논란이 있다면 이에 관한 해당 개인의 언급은 이러한 기록파일의 일부분으로 삽입되어야만 한다. ⑥ 개인기록들에 접근하고자 하는 公務員은 이러한 정보에 접근할 수 있는 적절한 권한을 갖고 있어야만 한다. 그리고 해당 개인에게 이러한 접근에 관하여 통지되어야만 한다. 그러나 Linowes는 個人情報保護에 관하여 통제하고 감독하는 機關을 만들 것을 제안하는 것 대신에 관련개인의 損害賠償請求에 의하여 個人情報를 보호하는 방법을 주장하였다.[48]

(4) 英國法上 基準

英國의 個人情報保護法은 다음과 같은 情報保護原則들을 담고 있다 : a) 저장되는 個人情報는 공정하고 합법적으로 획득되고 처리되어야만 한다. b) 個人情報는 구체화된 합법적 목적을 위해서만 저장되어야 한다. c) 어떤 목적을 위하여 획득된 정보는 이러한 목적과 양립할 수 없는 방법으로 사용되거나 공개되어서는 안된다. d) 어떤 목적을 위하여 획득된 個人情報는 적절하고 관련되며 이러한 목적을 벗어나는 것이어서는 안된다. e) 個人情報는 정확하고, 필요한 곳에서는 최신정보이어야만 한다. f) 어떤 목적을 위하여 저장된 個人情報는 이러한 목적을 위하여 필요한 범위를 넘어서서 저장되어서는 안된다. g) 지나치게 지연되거나 비용이 들지 않으면서 ① 자신에 관한 정보를 어떤 정보사용자가 갖고 있는지를 통지받고, ② 어떤 정보사용자가 저장한 이러한 정보에 해당 개인이 접근할 수 있고, ③ 적절한 경우에 이러한 정보를 수정하거나 삭제할 권리를 해당 개인이 갖고 있어야만 한다.

결국 지금까지 위에서 설명된 個人情報保護에 관한 國際的 基準이나 國內的 基準을 살펴보면 구체적으로 그 내용이 약간씩 다르다 하더라도 본질적인 내용에서는 별 차이가 없다는 것을 알 수 있다. 이러한 일반적인 기준을 간단히 요약하면 다음과 같다 : 우선 個人情報를 조사, 처리, 저장하는 기관은 事前에 구체적으로 결정된 목적을 위해서만 이러한 個人情報를 처리해야 한다. 그리고 이러한 個人情報를 조사, 처리할 때는 해당 개인의 事前同意가 있거나 이에 관한 範圍具體的인 法律上

48) Henry H. Perrit Jr., ibid., p.148.

根據가 있어야만 한다. 세 번째로 情報가 조사, 처리, 저장되는 해당 개인은 자신에 관한 情報에 접근하여 잘못된 정보를 수정하거나 삭제하는 등의 권리를 갖고 있어야만 한다. 네 번째로 個人情報를 처리하는 機關에게 情報의 무단유출 등에 관한 民·刑事處罰規定 등이 있어야만 하고, 마지막으로 이러한 情報處理를 감독, 통제할 統制機關이 있어야만 한다.

3. 情報公開와 個人情報保護間 關係

우리 나라처럼 情報公開法과 個人情報保護法을 모두 갖고 있는 경우에 두 法律間에 충돌문제가 발생할 수 있다. 이를 논하기 이전에 우선 다음을 인식해야만 한다. 우선 어떤 기록들에 主觀的인 接近權이 허용되는 한, 두 制定法의 適用範圍가 겹칠 수 있다는 것이다. 어느 法에 의해서든 公開가 가능하면 해당 機關은 보통 그 기록을 공개해야만 한다. 이러한 의미에서 情報公開法은 두 가지 측면에서 個人情報를 보호하는 기능을 갖고 있다. 곧 한편으로 情報公開法은 國家가 갖고 있는 기록들이나 서류들에서 자신에 관한 정보에 주관적으로 접근할 권리를 보장한다. 그리고 다른 한편으로 이 法은 어떤 정보의 공개로 인하여 개인의 私生活이 침해될지도 모른다면 이러한 情報의 公開를 허용하지 않음으로써 제3자의 私生活을 보호한다. 그럼에도 불구하고 情報公開法은 개인의 주관적인 권리침해여부와는 상관없이 모든 국민들에게 國家가 갖고 있는 서류나 기록 등에 일반적으로 접근할 권리를 보장하는 반면에 個人情報保護法은 해당 개인에게만 本人의 個人情報에 접근할 권리를 인정한다. 곧 前者는 國家行政의 透明性을 확보함으로써 국민들의 정치적 참여기회를 넓히고, 민주주의의 실현을 강화하고자 하는데에 그 목표가 있기 때문에 해당 개인의 주관적인 권리가 침해되는지와는 상관없이, 따라서 일반적으로 국민들이 국가가 갖고 있는 서류나 기록에 접근할 권리를 보장하는 것이다. 이에 반하여 後者는 개인에게 自己情報에 관한 決定權과 統制權을 보장하기 위하여 국가가 처리, 저장하고 있는 本人에 관한 情報를 열람하고 잘못된 정보를 수정하거나 삭제할 것을 요구할 수 있는 권리를 해당 개인에게 부여하고 있다. 결국 두 法律 모두 해당 개인이 자신의 정보에 접근하는 경우를 보장하기는 하나 그 목표와 절차가 다르다는 것을 기억해야만 한다.[49]

그렇다면 情報公開와 個人情報間 關係를 이제 살펴보아야만 한다. 우선 市民의 적극적인 참여가 없다면 民主的 意思形成을 통하여 國家를 조정, 안내, 통제하려는 어떤 노력도 의미없을 것이다. 결국 國民이 그들에게 부여된 政治的 自由 등을 적

49) 따라서 만약 個人情報保護法이 제정되어 있지는 않으나 情報公開法은 제정되었다면 관련 개인은 情報公開法에 규정된 接近權을 통하여 일정부분 자신에 관한 정보를 열람할 수 있다.

극적으로 행사하기 위해서는 정당, 여론매체, 시민단체 등을 통하여 언론, 출판의 자유가 보장됨과 동시에 國家가 행하고 있거나, 행하고자 하는 일들에 대하여 잘 알고 있어야만 한다. 그 목표는 行政의 公開와 透明性을 높힘으로써 國民들이 현실문제에 관한 독자적 판단을 가능하게 하며 政治生活에 능동적이고 책임감있게 참여하는 것이다. 결국 이렇게 國家行政의 透明性을 보장함으로써 진정한 의미의 國民主權을 실현하고 民主主義가 꽃피울 수 있도록 하고자 하는 것이 情報公開法의 기본취지이다. 이에 따라서 國民의 情報公開權이란 國家機關이 갖고 있는 情報에 일반적으로 국민이 접근할 수 있는 권리를 뜻한다. 그래서 얼핏 보기에 개인의 情報自己決定權과 情報公開權을 동시에 보장하는 것이 모순된 것처럼 보일지도 모른다. 그러나 個人情報保護와 情報公開는 결코 서로 분리되거나 상호 대립되는 것이 아니라 市民의 意思疏通能力과 民主社會의 기능을 촉진하기 위하여 모두 필요한 것이다.[50] 따라서 兩者間 충돌이 발생했을 경우에 둘중 하나를 위하여 성급하게 결정하는 것이 필요한 것이 아니라 양자 모두를 존중하고 구체적으로 고려하고 조정해야만 한다.[51] 이는 결국 이러한 긴장관계는 個人情報保護나 情報公開中 어느 것을 더 우선시할 것인지라는 이념적 논쟁을 통하여 해결되는 것이 아니라 관련영역의 명확한 구분 및 구체적인 해결시도를 통하여 해결하려고 노력해야만 한다는 것을 뜻한다. 다시 말하자면 결국 情報自己決定權과 情報自由, 研究自由 및 環境情報들에 관한 접근간에 갈등이 있음은 물론 부인될 수는 없다. 그럼에도 불구하고 가능한 한 양자 모두 그 작용을 발현하고 한 권리가 다른 권리를 통하여 절대적으로 차단되지 않을 것이 요구된다.[52] 다시 말하자면 情報自己決定權과 몇몇 基本權들 속에 담겨 있는 情報接近權은 行政의 公開와 透明性을 요구하기 때문에 양자는 서로 전제로 하고 보충한다. 따라서 양자 모두 民主的 社會秩序 속에서 개인의 意思疏通을 위하여 포기할 수 없는 전제조건인 것이다.[53] 따라서 이 양자간에 존재하는 이러한 긴장관계를 조정하는 것은 우선적으로 立法者의 課題이다. 그리고 立法者가 이러한 과제를 충실히 수행한 경우에 개개 경우에 구체적으로 個人情報保護가 우선되는지 아니면 情報公開가 중요시되는지를 판단해야만 하는 것이다.[54]

---

50) Spiros Simitis, Informationelle Selbstbestimmung und Informationsfreiheit als Verfassungsprinzipien, Thomas Kreuder(Hrsg.), *Der orientierungslose Leviathan*, 1992, S. 145.

51) *Spiros Simitis*, a.a.O., S. 146.

52) Marie-Theres Tinnefeld / Eugen Ehmann, a.a.O., S. 22면 이하 ; Thilo Weichert, Neue Verfassungsregelungen zur informationellen Selbstbestimmung, CR 1992, S. 743.

53) Spiros Simitis, a.a.O., S. 145.

54) 예를 들어 연방정보보호법 40조 이하 참조.

第3章 公共機關의 個人情報保護에 관한 法律의 改正必要性과 그 內容

第1節 主要國家의 個人情報保護法律

1. 스웨덴

1) 個人情報保護法의 연혁과 내용

美國에서와 비슷한 시기인 1960년대 중반에 프라이버시와 컴퓨터에 관한 논쟁이 스웨덴에서도 시작되기는 하였으나, 1970년 스웨덴의 人口調査計劃이 비로소 個人情報를 保護해야만 한다는 의식을 스웨덴 국민들이 갖도록 하였다. 이에 따라서 議會는 1972년 "컴퓨터와 프라이버시"에 관한 보고서에서 個人情報保護에 관한 立法을 提案하였다.

이러한 立法案을 바탕으로 하여 1973년에 제정된 情報法(Data Act)은 세계적으로 個人情報保護에 관한 첫 번째 國家法으로서 다른 서유럽국가들에서 個人情報保護法을 제정할 때 상당한 영향을 끼쳤던 선구자적인 법률이었다. 우선 이 법의 목표는 개인프라이버시에 대한 부당한 침해를 방지하는 것이다. 따라서 1973년 情報法은 公的 領域이든, 私的 領域이든 간에 컴퓨터로 처리하여 확인할 수 있는 個人情報의 수집, 저장, 유통을 규율하는 情報監督委員會(Data Inspection Board)를 만들었다.[1] 이 委員會(Data Inspection Board DIB)는 수집되는 個人情報의 내용과 특성, 個人情報의 획득방법에 관하여 파악해야만 한다. 그래서 情報法의 適用範圍는 자동화되고 확인할 수 있는 형태로 기록되는 파일, 메모 등으로 한정되고 수작업파일은 규율되지 않는다. 그리고 정보법 제5조에 따르면 정보처리기관이 개인정보파일을 설치하거나 보존하고자 하는 경우를 위하여 DIB는 파일의 목적과 관련되는 규정을 만들어야만 한다. 여기서 책임 있는 정보저장자가 특정 시스템의 목적을 확인해야만 하므로 "目的"의 의미를 개념 정의하는 것이 위 법적용시 발생되는 핵심문제중 하나이다. 그런데 기록되는 사람의 프라이버시에 대한 부당한 침해의 발생을 방지하는 것이 情報法의 일차적인 관심사라고 언급하고 있음에도 불구하고[2] 이 법은 "개인프라이버시" 또는 개인프라이버시의 부당한 침해수단을 개념 정

1) 1973년에 제정된 情報法은 그 동안 여러 번 개정되었다. 1990년 8월에 의회의 정보입법위원회는 정보법개정안을 다시 제출하였고, 개정된 법률은 1993년에 효력을 발생하였다.

의하는데에는 다소 인색하였으며 1982년 개정법에도 프라이버시란 단어가 적절하게 개념 정의되고 있지는 않다.

이에 반하여 情報法은 情報處理에 관하여 아주 상세한 규정을 갖고 있다. 따라서 DIB는 기록될 個人情報의 내용과 양, 어떻게 그리고 누구로부터 정보가 수집되어야 하는지 등을 심사할 수 있다. 프랑스법에서처럼 情報法은 人種, 性生活, 犯罪情報, 健康情報, 精神病記錄이나 社會福祉記錄, 政治的, 宗敎的 信念들과 같은 정보를 특별히 민감한 것으로 개념정의한다. 특별히 예외적인 경우에 한하여 公的 機關만이 이러한 정보를 기록, 저장할 수 있다. 그리고 情報監督委員會는 私的 領域에서 개인정보파일의 설치를 허가하는데 個人情報가 민감한 것이라면 이에 관한 공식적인 허가가 필요하다. 또한 이 委員會는 公的 領域에서 個人情報의 수집을 규율한다. 따라서 이 委員會는 個人情報의 수집과 전달을 통제하고, 기록들의 사용을 규율하고, 정보은행에 관한 책임있는 관리체계를 집행한다. 이 법 자체가 이러한 관리자들의 상세한 의무들을 확정하였기 때문에 이에 관한 여러 民·刑事處罰規定들 또한 두고 있다. 그러나 이 委員會(DIB)의 權限은 情報法의 집행을 위한 것만으로 한정되지는 않는다. 이에 따라서 情報監督委員會는 개인의 프라이버시를 보호하기 위하여 제정되었다고 생각될 수 있는 다른 두 가지 法律 - 1974년에 제정된 信用情報法(the Credit Information Act)과 1974년에 제정된 債務救濟法(the Debt Recovery Act) - 의 집행을 감독하고 필요한 사항에 관하여 허가한다.[3]

그러나 이 情報法은 다시 1983년에 대폭적으로 개정되었다. 우선 그동안 情報監督委員會에게 너무 많은 업무부담을 지웠다는 인식하에서 모든 개인정보시스템에 관한 一般的인 事前許可로부터 기록시스템으로 바뀌었다. 이제 한 사람의 평가기록에 관한 것처럼 민감한 기록이나 정보보유자와 관련 없는 사람에 대한 정보를 담고 있는 파일에 관해서만 DIB의 명시적인 허가를 필요로 하도록 법은 요구하였다.[4] 또한 문제가 되는 기록파일의 내용이 어떤 다른 개인파일들로부터 받아오는 것이라면 이에 관한 許可를 필요로 한다. 그러나 委員會의 이러한 許可와 監督權限은 정부나 의회에 의하여 만들어진 개인파일은 委員會의 허가를 필요로 하지 않는다는 정보법규정에 의하여 심각하게 제한된다. 예를 들어 스웨덴에서 행정부나 의회는 약 600개 정도의 정보은행을 갖고 있다고 한다. 결국 이는 DIB의 감독으로부터 면제될 정보은행을 만들 궁극적인 권한을 의회와 정부가 갖고 있다는 것을 뜻한다.

---

2) 情報法 제3조.

3) 스웨덴의 신용정보법은 미국의 1970년 공정신용기록법(the Fair Credit Reporting Act) 및 영국의 1974년 소비자신용법(the Consumer Credit Act)과 비슷하다.

4) 情報法 제3조.

다만 면제되는 정보은행을 만들 國家의 권한에 관한 중요한 한 가지 통제는 情報法 2조가 포함하는 민감한 個人情報를 처리하는 경우에 미리 DIB와 상담해야만 한다는 명령이다. 그런데 1982년 개정에 따라서 許可(license)와 承認(permission)간에 구별되었다. 이에 따라서 모든 책임 있는 기록자는 형식적으로는 여전히 개인파일의 설치에 관한 許可를 필요로 하나 실질적으로는 보통 이에 관한 申請을 함으로써 자동적으로 허용된다. 게다가 DIB는 이러한 기록파일을 허가할 때 申請內容의 정확성을 상세하게 심사하지 않는다. 다만 健康, 前科, 宗教, 政治的 見解와 같은 민감한 정보를 사용하고자 하는 경우에만 시스템설치이전에 이에 관한 허가를 받도록 요구할 뿐이다. 그리고 情報法下에서 책임 있는 個人情報保有者란 그의 처분 하에 있는 개인파일들을 어떤 목적을 위하여 저장하는 자를 말한다. 이러한 책임 있는 보유자는 情報法의 규정이 준수된다는 것을 입증해야만 한다. 그리고 책임 있는 보유자는 이러한 정보시스템의 감독를 위하여 委員會(DIB)가 요구하는 자동정보처리와 관련되는 정보를 DIB에 전달해야만 한다.[5] 결국 이는 立法府는 감독을 할 아주 강력한 권한들을 DIB에게 부여하였다는 것을 뜻한다. 이에 따라서 委員會는 자동정보처리와 관련된 기록들에 접근할 권리를 갖고 있으며 컴퓨터작동에 관하여 지시를 내릴 수도 있다.[6] 그러나 獨逸에서와는 달리 DIB는 보통 구체적인 개인정보파일이나 그 처리에 관하여 심사하려고 하지 시간이 허락하지 않는 한 전반적인 검사는 거의 하지 않는다. 이에 따라서 情報法은 명확히 개념정의되는 중요한 원칙들을 열거하기보다는 정보처리 등에 관한 실무와 절차들을 상세하게 설명하는 데에 더 많은 공간을 할애한다는 것을 알 수 있다. 더군다나 DIB가 우선적으로 정보처리의 구체적인 경우들에 대하여 許可決定들을 내리므로 광범위한 일반원칙들 - 특히 公的 領域과 관련되는 - 에 많은 신경을 쓰지 못하는 실정이다.

또한 情報法은 관련개인에게 여러 권리들은 인정하고 있다. 우선 情報法 10조하에서 기록보유자에게 書面質疑를 한 사람은 기록보유자부터 자신에 관한 情報를 받을 권리를 갖고 있다. 이러한 정보제공시 특별한 이유가 있다고 DIB가 인정하지 않은 한, 해당개인에게 정보제공은 無料이다. 또한 情報法은 잘못된 정보를 수정할 權利를 개인에게 부여하였다. 그러나 개인의 이러한 接近權은 경찰기록처럼 秘密法(Secrecy Act)이 다루는 사항이나 治療記錄, 社會保障記錄과 같은 非公開記錄들에서는 허용되지 않는다.[7] 그러나 일반적으로 대부분의 개인들은 이러한 접근권의 존재를 잘 모르거나 매우 드물게 행사한다. 따라서 이러한 경우에 대비하여 情報法

5) 情報法 제17조.
6) 情報法 제16조.
7) 情報法 제10조제3항.

은 個人情報의 主體가 정보처리에 관하여 DIB에 불평할 수 있도록 규정하였다. 그러므로 이러한 경우 情報監督委員會(DIB)는 "정보옴부즈만"으로서 활동하게 된다.[8] 그리고 情報法 제23조는 책임 있는 기록자가 부정확한 정보를 저장한 경우에 해당 개인이 民事上 損害賠償을 청구할 수 있도록 규정하였다.

스웨덴은 公的, 私的 領域에서 많은 정보은행들이 존재할 뿐만 아니라 개개 시민들에게 個人確認番號(PINs)가 부여 되어 있기 때문에 크고 작은 형태들의 감시를 위한 기록연결들이 빈번하게 행해지고 있다. 우선 스웨덴에서는 개인관련정보가 구체적인 制定法이나 DIB의 결정, 기록되는 사람의 허가에 의하여 저장, 연결되지 않는 한, 정보시스템간 연결을 통한 個人情報의 결합은 이에 관한 특별한 허가를 DIB로부터 받아야만 한다. 여기서 情報監督委員會(DIB)가 모든 형태의 기록연결에 반대하려는 것은 아니나 정보이용자가 個人情報를 왜 수집하였는지를 모르거나 또는 매우 심각한 정보를 연결하려고 하는 연결들에는 반대한다는 것에 주목해야만 한다. 결국 이러한 문제에서 주요 관심사는 기록의 연결을 통하여 전달·이용되는 정보가 個人情報라는데에 있다. 어떤 기록연결이 허용되어야만 하는지를 검토하기 이전에 언제, 왜 그리고 어떻게 정보가 수집되었는지를 사람들이 우선 알아야만 한다. 情報監督委員會(DIB)는 더 많은 기록연결을 위한 압력들이 정보처리전문가로부터가 아니라 行政府로부터 나온다고 지적한다. 어쨌든 거의 모든 個人情報의 연결들이 情報監督委員會(DIB)에 의한 규제밑에 있다는 것이 중요한 점이다. 예를 들어 社會福祉機關들은 기록연결을 강력하게 주장하나 DIB는 이러한 기록연결이 사회적으로 유용할 수 있다는 것을 인정하면서도 이러한 두 파일(租稅目的으로 신고된 所得과 복지혜택자격)간 비교에 반대한다.

위에서 언급한 것처럼 스웨덴에서는 개개 시민들에게 個人確認番號(PINs)가 부여되어 있다. 1978년 情報法改正에 관한 議會委員會는 이러한 개인확인번호가 처음에는 한 가지 목적을 위하여 수집되었으나, 그후에 계획되지 않았던 다른 목적들을 위하여 사용되는 것을 통하여 개인의 私生活을 부당하게 침해할 가능성이 있다는 것에 초점을 맞추었다. 결국 이 議會委員會는 실제로 個人確認番號(PINs)가 없어진다면 나타날 현실적인 어려움들과 이에 따르는 막대한 비용을 강조하면서 이러한 번호의 사용이 금지되어야만 한다는 견해를 거부하였다. 그러면서도 또한 이 委員會는 이러한 個人確認番號가 개인의 私生活에 미칠 수 있는 위험성을 언급하였다. 따라서 議會委員會는 이러한 個人確認番號가 요구되어야만 하는 상황을 제한하도록 제안하였다. 또한 議會委員會는 충돌하는 이익들의 최종적인 형량이 오로지

8) David H. Flaherty, ibid., p.135 이하.

情報法上 規定을 통해서만 확정될 수는 없다고 결정하였다. 결국 이는 개인들에 대한 통제유형들을 궁극적으로 情報監督委員會(DIB)가 아니라 議會가 결정해야만 한다는 것을 뜻하였다. 어쨌든 스웨덴에서 일단 個人確認番號가 존재하게 된 이후로 예를 들어 운전면허증에 이러한 번호를 기입하도록 명령되는 것처럼 이러한 個人確認番號는 언제나 계속적으로 원래 목적과는 다른 경우들을 위하여 사용되고 전달된다. 그러나 情報法이 이러한 個人確認番號의 사용에 관하여 규율하지 않는 반면에 DIB는 이러한 번호의 사용에 관한 시민의 불평을 계속해서 받고 있다. 어쨌든 이러한 個人確認番號가 일단 사회에 존재하는 한 이러한 번호의 사용을 情報監督委員會가 제한하려고 노력한다는 것은 매우 어렵다.

스웨덴에서 個人情報보호에 관하여 가장 독특한 영향을 미친 것중 하나가 情報監督委員會(DIB)가 지원하고 議會가 1976년 만든 SPAR(National Register of Names and Addresses)라고 알려진 정보시스템이다. 이 정보시스템의 설치에 따라서 개인이름과 住所를 국가적으로 기록하게 되었다. 본래 이러한 정보시스템은 企業이나 信用調査機關 등 私的 領域에서 국민전체에 관하여 조사하고 기록할 위험성을 통제함으로써 개인의 私生活을 보호하고자 한 것이었다. 그러나 역설적으로 이러한 정보시스템은 실제로 단일한 國家情報銀行이기 때문에 거꾸로 국민을 감시할 능력을 확대해 버렸다. 이에 따라서 개정된 情報法은 이 정보시스템(SPAR)에 관한 규정을 두고 있다.[9] 이 情報法規定에 따라 정당한 목적들을 위하여 특정한 個人情報를 구하는 사람들은 다른 곳에서보다는 SPAR에서 이러한 정보를 우선 획득하여야만 한다. 이 정보시스템(SPAR)에 담긴 情報는 이제 스웨덴에서는 은밀한 것으로 여겨지지 않는 개인이름, 個人確認番號, 國籍, 婚姻與否, 推定所得, 租稅能力, 不動産所有 등이다. 그래서 예를 들어 私人들은 이 정보시스템으로부터 그들이 원하는 거의 모든 個人情報를 획득할 수 있다. 그러다보니 실제로 이러한 정보시스템은 다른 나라들에서 오래전부터 두려워했던 國民을 감시하는 정보은행이 되어버렸다. 결국 이에 따라서 원래 국민의 私生活을 보호하기 위하여 계획되었던 이 정보시스템(SPAR)이 역설적으로 다른 서구국가들이 피하고자 했던 감시형태의 상징이 되어버렸다.[10]

2) 小 結

(1) 스웨덴정부의 빅브라더경향에 대한 저항형태로서 1980년대(1983년 人口調査와 1986년 대도시계획에 대한 시민들의 반대)에 발생하였던 프라이버시에 관한

9) 情報法 제26조~제28조.

10) David H. Flaherty, ibid., p.150 이하.

두 번의 대규모토론들 때문에 특히 이 시기에 個人情報를 보호하고자 하는 스웨덴 국민의 인식이 높아졌다. 결국 스웨덴처럼 급격하게 情報化되는 사회, 보편적인 個人確認番號의 존재, 情報公開를 통한 개방성원칙은 이와 더불어 동시에 엄격한 個人情報保護原則 또한 확립되어 있어야 비로소 정보사회에 살고 있는 개인의 사생활이 보호될 수 있다. 그럼에도 불구하고 시민들이 이런 개인기록들을 사용하는 것에 저항할 수 없을 때 나타나는 감시사회의 유형이 바로 스웨덴이다.

(2) 비록 스웨덴식 개인정보보호모델이 광범위하게 모방되지는 않았다 할지라도 이러한 스웨덴식 모델은 서유럽국가들에서 個人情報保護法制의 발전에 직접적인 영향을 미쳤다. 예를 들어 1978년 프랑스 個人情報保護法은 스웨덴식 모델을 채택한 가장 명확한 사례일지도 모른다. 또한 영국의 情報保護法(1984)은 이 스웨덴식 모델에 의하여 크게 영향을 받았다. 왜냐하면 公的 領域과 私的 領域에서 個人情報를 처리하는 컴퓨터를 위한 일반적 기록체계를 채택하였기 때문이다.[11]

(3) 위에서 설명한 것처럼 스웨덴은 西歐國家中에서 감시사회의 전형적인 모델이다. 왜냐하면 매우 높은 정도로 個人情報가 자동처리되고, 기록연결을 촉진하는 個人確認番號가 존재한다. 그리고 私的 領域과 公的 領域間에 정보이동이 매우 빈번히 이루어지고 있기 때문이다. 더군다나 유명한 言論自由法 속에 표현된 公開原則 때문에 다른 국가들에서 보통 비밀인 個人情報들을 스웨덴에서는 제3자가 손쉽게 이용할 수 있다. 게다가 스웨덴은 선구자적인 情報保護法律에 의하여 전세계에 많은 영향을 주었다 할지라도, 일반적인 프라이버시보호법률을 제정하지는 않았다. 이러한 점에서 영국이 스웨덴과 유사하다.[12] 실제로 스웨덴에서는 정부나 다른 개인들로부터 비밀로 할 수 있는 個人情報가 상대적으로 별로 없다. 이를 통하여 국가의 여러 행정부처들은 시민의 私生活에 관하여 많이 알고 있다. 특히 이러한 상황은 개인들에 관한 결정 - 복지혜택 등 - 을 내리기 위하여 사용되는 행정정보에서 가장 강하게 나타난다. 결국 결정적인 문제는 個人情報의 수집과 그 사용목적인데 租稅回避 등을 막기 위한 광범위한 기록 및 기록연결을 시행하기로 스웨덴정부와 입법부는 결정하였다. 그렇다면 결국 스웨덴은 情報公開와 개인의 私生活 또는 효율적인 국가업무수행이라는 충돌하는 가치들과 목표들의 세심한 형량에 바탕을 둔 정책을 선택한 것이 아니라, 개인의 프라이버시을 충분히 고려하지 않고서 성급하게 정보기술을 사회에 적용하고 있다고 말할 수 있다.

(4) 어쨌든 情報法上 統制機關으로 만들어진 情報監督委員會(DIB)는 나름대로 그들의 임무를 효과적으로 이행하고 있다고 말할 수 있다. 예를 들어 DIB는 기록

11) David H. Flaherty, ibid., p.94 이하.
12) James Michael, ibid., p.56.

연결에 적극적으로 영향을 미쳤고 위원회의 허가활동을 통하여 주요한 공공행정시스템들에 적극적으로 영향을 주었다. 情報法의 1979년 일부 개정, 1982년 대폭적인 개정, 1993년 개정은 個人情報保護法의 실험적인 성격 및 情報技術이 사회에 미치는 영향때문에 이러한 法律이 주기적으로 개정될 필요성을 나타낸다. 그리고 최근에 스웨덴에서는 기록연결들의 규제 및 민감한 個人情報에 관한 특별입법의 필요성 등에 관하여 많이 토론되고 있다.

(5) 다른 나라들과 비교하여 스웨덴은 비교적 작은 840만명이라는 인구를 갖고 있다. 결국 매우 높은 생활수준과 결합하여 이렇게 작은 규모의 인구라는 사회적, 지리적 조건은 스웨덴이 일찍부터 국가사회의 정보화를 통하여 국가행정의 효율성을 높힐 수 있는 토대가 되었다. 그래서 스웨덴은 전세계에서 가장 情報化된 국가들 - 특히 公共行政에서 - 중 하나에 속한다. 그리고 이러한 높은 정도의 自動化는 스웨덴에서 일반적으로 문제없이 받아들여지고 있다. 그러다보니 결과적으로 스웨덴은 "기록의 천국"이라고 일컬어지고 있는데 예를 들어 情報監督委員會(DIB)는 5만개가 넘는 개인정보시스템의 존재를 확인하였다. 그래서 情報社會에서 일반적인 個人情報保護라는 원칙은 스웨덴에서는 비교적 새로운 것으로서 열린 정부라는 오래전부터 확립된 원칙과 명백히 충돌한다. 특히 言論自由法은 情報自由나 公開原則을 구체화한다. 이를 통하여 公的 機關들에 의하여 수집된 모든 정보들은 원칙적으로 모든 사람에게 개방된다. 따라서 대부분의 다른 국가들과는 대조적으로 정부가 보관하고 있는 대부분의 정보들 - 컴퓨터화된 정보를 포함하여 - 은 모든 시민들이 즉시 이용할 수 있다. 그래서 스웨덴에서는 일반시민이 정부정보에 접근할 수 있다는 情報公開原則이 個人私生活保護原則보다 우월하다고 말할 수 있다.[13]

2. 프랑스

1) 정보보호법의 연혁과 내용

프랑스는 가장 일찍, 그리고 정열적으로 情報社會에 진입하고자 노력한 국가에 속하였다. 그래서 프랑스사람들은 재빨리 새로운 情報通信技術이 개인의 자유 및 私生活에 미칠 수 있는 위험을 인식하였다. 특히 모든 개인기록들을 연결하려는 행정부계획을 언론이 보도하였던 1975년 사파리(Safari)사건으로 인하여 公的, 私的 領域에서 시민의 私生活自由, 다른 個人自由 등을 존중하는 정보처리발전을 보장하기 위한 위원회를 法務部가 설치하게 되었다.[14] 그런데 財經部(the Ministry of

13) David H. Flaherty, ibid., p.135.
14) James Michael, ibid., p.65.

Economy and Finance)管轄下에 있는 統計와 經濟에 관한 國家調査廳(the National Institute of Statistics and Economic Studies)은 약 5000만명에 달하는 인구에 관한 정보를 담고 있는 국가적인 身分記錄(National Identification Register, NIR)을 갖고 있었다. 1973년 낭트에 설치된 이 자동화된 국가신분(확인)기록(NIR)은 국민들에 관한 기록을 저장하는 國家記錄所 - 選擧人名簿로도 작용하는 - 로서 기능하기 시작하였다. 모든 새로 태어난 아동들에게 배정되는 13자리숫자는 결국 국가적인 個人確認番號였다. 1970년대말까지 이런 個人確認番號(NIR)는 다양하게 행정적으로 사용되었다. 1982년에 정부는 이러한 기록(NIR)에 개인이름, 출생일과 출생장소, 性, 個人確認番號만을 포함하도록 하였을 뿐 주소, 婚姻與否, 자녀의 이름 등은 제외시켰다. 그래서 法에 의하여 명시적으로 허용되지 않는 한, 이러한 기록(NIR)은 개인을 찾기 위하여 사용될 수 없었다. 그럼에도 불구하고 이러한 기록(NIR)이 어떤 다른 감시목적들을 위하여 사용될 수 있는지가 불확실하게 남아 있었다.

1974년 프랑스정부는 새로운 個人確認番號를 도입하려고 하면서 1960년대 중반에 미국에서 국가정보은행설립에 관하여 벌어졌던 것에 비유할만한 論爭에 휩싸였다. 프랑스정부의 원래 계획에 따르면 프랑스거주민들은 종이로 만들어졌고 위조되기 쉬운 국가적 확인(신분)카드를 휴대해야만 했다. 1979년말 內務部(Ministry of the Interior)는 컴퓨터가 읽을 수 있는 새로운 형태의 개인확인카드도입을 발표하였다. 그 주요 목표는 더 신뢰할 수 있는 신분증을 만드는 것이었다. 이 계획은 약 5000만명 정도 되는 사람 개개인에게 컴퓨터가 읽을 수 있는 카드를 발급하는 것이었다. 이러한 카드의 수령자들은 연결된 6개의 컴퓨터센터에 기록되고 이 카드 속에는 서명, 사진 등이 들어가도록 하였다. 外國人과 內國人의 카드는 그 색깔을 달리해서 구별할 수 있도록 하였다. 다만 이 身分證은 명백히 이름과 출생일을 바탕으로 해서만 개인을 확인할 수 있었지, 어떠한 個人確認番號도 사용하려고 하지 않았다. 이러한 새로운 身分證은 情報貯藏能力을 포함하여 신용카드의 모든 특징들을 가졌다. 그러다보니 우선 다른 정보시스템들과 연결가능성 때문에 이러한 身分證에 대하여 비판되었다. 內務部는 정보에 담긴 카드가 이러한 정보를 체크하는 과정에서 사용되거나 연결될 수 없다고 하였으나 컴퓨터가 읽을 수 있다는 가능성은 새로운 카드가 또 다른 목적을 위하여 사용될 수 있다는 우려를 불러 일으켰다. 새로운 국가적 신원확인카드가 바람직한지에 관한 言論의 論爭은 1980년 초반에 심화되었다.[15] 결국 1980년대 초반에 정부는 국가적인 개인확인카드를 만들려

15) 1980년 6월 국가적 신원카드에 관한 國家情報處理自由委員會가 제시한 해결책은 사람이 아니라 카드에 번호를 붙여서 카드를 잃어버린다면 개인은 새로운 번호를 받는다는 것이었다. 그

고 노력하였지만 이에 國民들이 격렬하게 반대하였다. 그래서 1981년 9월 정부는 새로운 개인확인카드의 도입을 포기한다고 공식적으로 발표하였다. 國民들의 격렬한 반대를 겪은 이후에 정부는 새로운 委員會를 만들었는데 이 위원회는 개인의 私生活이나 다른 自由 등을 존중하는 정보처리의 발전을 확보하는 방법들을 제안하였다. 이 委員會의 가장 일반적인 결론은 컴퓨터를 통한 情報處理를 통하여 생길지도 모르는 잠재적 위험성을 줄이기 위하여 이에 관한 豫防行爲가 필요하다는 것이었다. 결국 국가적인 개인확인카드의 도입에 관한 계획과 더불어 個人情報保護法律에 관하여 1974년부터 토론되다가 1978년 1월 6일 마침내 법률이 제정되었다. 이에 따라서 1978년 情報保護法을 만들 때 立法府는 법이 公的 領域과 私的 領域 모두에 적용되어야만 한다고 결정하였다.

프랑스에서 제정된 "情報處理·파일 및 自由에 관한 法律"은 우선 그 適用範圍가 대단히 넓고 法律內容이 혁신적이라는데에 그 특징이 있다. 특히 이는 英美法系 國家들의 시각에서 본다면 개인의 私生活保護나 감시통제를 훨씬 넘어서는 대단히 광범위한 사회문제들을 다루는 법이라는 점에서 그렇다.[16] 처음 보기에 프랑스의 이 法律은 情報處理의 규제에 직접적으로 관심을 갖는다. 예를 들어 情報處理法 14조는 이 법이 公的 또는 私的 領域에서 個人情報의 自動處理를 규율한다고 규정하였으며 이 법이 우선적으로 자동화된 情報處理에 적용된다 할지라도 위 법 제25조에서 제33조까지 규정들은 자동처리되지 않는 파일들에도 적용된다. 물론 개인의 住所錄처럼 아주 일상적인 手作業記錄들은 법률의 적용대상에 속하지 않는다. 그럼에도 불구하고 手作業으로 처리되는 個人情報의 경우에도 不法的인 情報蒐集이 금지되고 왜 이러한 個人情報들이 수집되는지가 개인들에게 통지되어야만 한다고 요구함으로써 위 법에서 열거된 일반원칙들의 적용을 받는다. 이 법 전체를 살펴본다면 情報處理法을 만든 立法者가 公的 領域에서 사용되는 개인정보시스템들의 규제에 우선적으로 관심을 가졌다는 것을 알 수 있다. 그럼에도 불구하고 이 법은 단순히 자동정보처리로부터 個人情報를 보호한다는 측면을 넘어서서 더 많은 사항을 다룬다는 점에서 다른 나라의 법률과는 다른 독특한 특징을 갖고 있다. 예를 들어 이러한 특징은 情報處理의 목적을 규정한 법 제1조를 살펴보면 알 수 있다. 위 법 제1조에 따르면 "情報處理는 국민각자에게 도움이 되어야 하고 그 개발은 國際協力의

래서 이러한 카드는 시민의 지위를 입증하기 위해서만 사용될 수 있지, 카드 그 자체나 숫자에 의하여 또다른 확인이 가능할 수 없도록 하자고 주장하였다.

16) 프랑스시민들이 때때로 프라이버시를 언급한다 할지라도 프랑스언어에서는 프라이버시란 단어가 일반적으로 알려져 있지 않다. 물론 많은 언어들이 영미권의 프라이버시에 해당하는 것을 갖고 있지 않다는 것은 사실이다.

범위내에서 이를 행하여야 한다. 정보처리에 의하여 인간존엄, 인권, 사생활, 개인적 또는 公的 自由가 침해해서는 안된다." 계속해서 情報處理法 제2조는 개인에 대한 평가나 판단을 자동화된 정보처리에만 근거하지 못하도록 하였고 제3조에 따르면 특정개인에 관하여 자동정보처리에 근거하여 결정될 때 그 개인은 사용된 정보 및 해당 컴퓨터프로그램 등에 관하여 알 권리를 갖는다고 규정하였다. 이 법 자체는 公的 領域과 私的 領域을 포함하고, 手作業記錄은 물론 자동화된 파일 또한 포함하는 것으로 해석된다. 다만 그 보호주체는 自然人으로 한정된다. 기본적인 규제시스템은 다른 유럽국가들에서 제정된 개인정보보호법률상 규제시스템과 비슷하다. 예를 들어 개인이름과 연결되는 정보를 다루는 정보처리시스템은 이러한 연결을 기록해야만 하며 이러한 기록은 다른 시스템과 연결되는지, 어떤 정보가 얼마만큼 저장되는지, 이에 관하여 어떤 保安措置들이 행해지고 있는지, 누가 情報에 접근하는지, 다른 나라들로 이러한 기록이 전달되는지에 관한 정보들을 공개해야만 한다. 그리고 이러한 경우에 해당하는 개인에게 이러한 기록 등에 관하여 通知될 권리 및 자신의 정보에 접근할 권리와 잘못된 정보에 관한 교정권 등이 인정된다. 그래서 情報가 해당개인로부터 수집될 때 情報處理法 제27조 이하에 근거하여 정보수집자들은 관련개인에게 어떠한 權利들이 인정되는에 관하여 通知해야만 한다. 또한 정보주체의 명시적인 同意 없이 人種, 政治的·哲學的 또는 宗敎的 見解나 勞動組合 所屬與否에 관한 정보수집은 명백히 금지된다. 프랑스의 情報處理法은 情報處理에 관한 통제수단으로서 個人情報에 관하여 해당 시민의 接近權을 강조한다. 따라서 부정확하거나 애매하고 오래되었거나 획득, 사용이나 저장이 금지된 개인관련정보의 수정, 명확화, 추가, 최신화 등을 개인은 요구할 수 있다. 다만 情報處理法 제34조에서 제37조까지는 전적으로 자동화된 個人情報에 접근할 수 있는 權利의 行使와만 관련된다. 관련개인에게 제공되는 정보는 명확해야만 하고 기록내용과 일치해야만 한다. 또한 情報處理法 제39조와 제40조는 國防, 國家安保나 公共安全과 관련되는 정보시스템에 간접적으로 접근할 권리를 개인에게 인정한다. 國際的 基準에서 본다면 민감한 정보파일에 시민이 간접적으로나마 접근할 수 있도록 보장한 것은 시민의 權利保護를 위하여 매우 높이 평가할만한 것이다. 일반적으로 정보파일들에 관하여 알고자 하는 정보주체들은 國家情報處理自由委員會(CNIL)에 의하여 유지되는 기록을 열람하고 이 委員會와 이에 관하여 상담할 수 있다. 그러나 國家安保, 公共安全과 관련되는 기록은 이러한 요구로부터 면제된다. 國家情報處理自由委員會(CNIL)는 광범위한 감독 및 감시권한을 갖고 있으나, 위 法律의 違反與否判斷은 檢察의 管轄事項이다.[17]

여기서 프랑스의 情報處理法에서 중요한 부분을 차지하는 國家情報處理自由委員會(the National Commission on Informatics and Freedom, CNIL)에 주목해야만 한다. 이 법에 따라서 어떤 기관이 정보처리시스템을 설치하고자 하는 경우에 이에 관하여 諮問하고, 기존 정보처리시스템을 감독하고, 조사하는 임무를 갖는 독립기관인 國家情報處理自由委員會(CNIL)가 설치되었다.[18] CNIL은 독립된 行政機關으로서 스웨덴에서처럼 이 委員會도 公的, 私的 領域들에서 제기되는 요구에 응답하고, 특정한 정보시스템들의 許可與否에 관한 결정을 내린다. 이러한 의미에서 CNIL은 충돌하는 이익들 자체를 형량하고 어려운 사건들을 결정하려고 노력한다. 情報處理法 15조하에서 CNIL은 상당한 정도의 간섭권한을 획득하였다. 왜냐하면 公的 領域에서 個人情報의 自動處理는 이 CNIL의 찬성의견을 바탕으로 해서만 행해질 수 있기 때문이다. 그래서 CNIL은 개인정보시스템을 통제할 상당한 권한을 갖고 있다. 그런데 委員會의 活動에 관한 첫 번째 報告書에서 이 위원회(CNIL)는 委員會의 목적이 단순히 個人情報의 保護에만 있는 것이 아니라 情報處理와 情報自由間 關係에 대해서도 검토하는 임무 또한 갖고 있다고 설명하였다. 그래서 이 委員會는 모든 유형의 새로운 情報技術과 관련되어 발생되는 情報處理와 表現의 自由에 관한 小委員會를 만들었다. 또한 프랑스의 情報處理法은 일련의 정보처리활동들을 시민들이 파악할 수 있도록 하기 위하여 정보시스템의 이름과 목적을 구체화하거나, 기록되는 個人情報範疇를 구체화하거나 이러한 정보를 받도록 허가된 사용자나 그 사용자범주를 구체화할 임무를 國家情報處理自由委員會(CNIL)에게 부여하였다.[19] 이 위원회는 자동화된 개인정보시스템에 관한 기록을 갖고 있는데 이러한 기록은 명백히 모든 사람이 이용할 수 있는 것이다. 公的 領域에서 情報處理에 관한 의견을 제시할 때 CNIL의 가장 기본적인 관심사는 정보의 계속적인 전달이나 연결은 물론 특정 시스템에서 수집되는 個人情報의 궁극적인 사용을 事前에 확립한다는 것을 뜻하는 "公正性"이나 最終使用原則이다. 또한 CNIL은 情報處理의 透明性이나 開放性增進이라는 중요원칙의 의미를 계속해서 명확히 요구한다. 비록 이 委員會가 法院이 아니라 할지라도, 諮問要求에 대한 의견제시형태로 결정을 내린다. 그리고 諜報機關과 軍事機關들은 정보시스템설치시 CNIL의 의견을 구해야만 하고, 이에 관한 최소한도의 정보를 위원회에게 제공해야만 한다. 安保領域과 軍事領域에서 중요한 문제들중 하나는 특정 유형의 정보저장을 제한하는 情報處理法 제31조 이하에 따라서 어떠한 종류의 민감한 정보들이 수집될 수 있는지를

17) James Michael, ibid., p.66.
18) 국회에서 法案에 관한 토론은 대부분 CNIL의 구성과 독립에 관한 것이었다.
19) 정보처리법 제22조.

이 國家情報處理自由委員會가 결정한다는 것속에 있다. 실제로 1981년 CNIL은 國防部의 정보시스템에서 몇몇 항목들 - 개인들은 잊혀질 권리를 갖고 있으며, 16세이전 개인에 관한 그 어떤 정보도 저장되어서는 안되고, 저장기간도 사전에 결정되어야만 한다는 것을 근거로 하여 - 은 削除되어야만 한다고 결정하였다.

2) 小 結

프랑스행정부는 매우 官僚化되었고 더군다나 中央集權國家이기 때문에 국가의 정보시스템들에 의한 감시를 통제한다는 것을 매우 어렵게 만든다. 1978년에 제정되어서 그 후 몇 차례 개정된[20] 情報處理法은 비교적 잘 만들어진 법이었으나 문제는 이 法律이 제대로 적용되지 못한다는데에 있다. 특히 行政府를 통제해야만 하는 國家情報處理自由委員會의 활동은 아주 실망스러웠다.[21] 이렇게 國家情報處理自由委員會가 제대로 기능하지 못하게 된 몇가지 요인들을 열거하면 다음과 같다 : 우선 이 委員會에 부여된 권한의 범위가 너무 넓다는 것이다. 情報處理法에 의하여 명령되는 CNIL의 과제는 최소한 13가지 의무나 과제들을 포함한다 : 정보시스템을 검토하고, 法, 命令이나 判斷의 형태로 公的 領域에서 권고하고, 諮問해주며 감독하고, 시스템사용자들에게 경고하고, 벌금을 부과한다. 실제로 설립이후 처음 5년동안에 CNIL은 새로운 정보시스템들을 설치하고자 하는 정부의 요청에 응답하여 사례별로 처리하는 방식을 채택하였다. 이를 통하여 이 委員會의 중요한 임무인 個人情報保護에는 제대로 신경을 쓸 수 없었다. 그리고 두 번째로 委員會의 구성원들이 여러 다양한 정치적 성향을 갖는 인사들이었기 때문에 위원회의 결정이 다른 나라의 統制機關과 비교한다면 더 정치적이었다는 것이다. 실제로 위원회의 위원중 그 누구도 그들의 시간을 전적으로 個人情報保護에만 쏟지 않기에 스탭들과 협조 및 효율적인 감독문제가 제기되었다. 결국 이는 현재와 같은 조직하에서는 CNIL에게 부여된 기본적 임무들을 이행하지 못한다는 것을 뜻한다.[22]

3. 英 國

英國에서 法院이나 議會는 개인의 프라이버시를 보호하기 위한 法律을 만드는 데에 특별히 적극적이지 않았다. 예를 들어 영국의 立法府는 1969년에 "모든 상황에 적용할 수 있는 일반적인 프라이버시권"을 규정한 "프라이버시법"을 제정하려고 하

20) 1988년과 1994년 두 차례 개정되었다.
21) David H. Flaherty, ibid., p.233.
22) David H. Flaherty, ibid., p.199.

였으나 이에 대하여 많은 비판이 제기되었다.[23] 이에 따라서 결국 프라이버시법안에 관한 심사위원회는 일반적인 프라이버시권을 보호하는 法律을 제정하기 보다는 프라이버시보호를 해당 분야별로 나누어 검토하고 접근하는 방식을 채택하였다.[24] 그럼에도 불구하고 많은 논란 끝에 1984년 個人情報保護法이 제정되었는데 특히 이 법은 스웨덴의 個人情報保護法으로부터 많은 영향을 받았다.[25]

英國의 個人情報保護法은 다음과 같은 情報保護原則들을 담고 있다[26] : a) 수집, 처리의 適法性原則 : 저장되는 個人情報는 공정하고 合法的으로 획득되고 처리되어야만 한다. b) 目的明確性原則 : 個人情報는 구체화된 합법적 목적을 위해서만 저장되어야 한다. c) 目的外 使用禁止原則 : 어떤 목적을 위하여 획득된 정보는 이러한 목적과 양립할 수 없는 방법으로 사용되거나 공개되어서는 안된다. d) 蒐集, 保有制限의 原則 : 어떤 목적을 위하여 획득된 個人情報는 적절하고 관련되며 이러한 목적과 관련되지 않는 것이어서는 안된다. e) 正確性維持의 原則 : 個人情報는 정확하고, 필요한 곳에서는 최신정보이어야 한다. f) 無期限保有禁止의 原則 : 어떤 목적을 위하여 저장된 個人情報는 이러한 목적을 위하여 필요한 것을 넘어서는 안된다. g) 個人參與의 原則 : 부당하게 지연되거나 지나친 비용이 들지 않으면서 ① 관련개인의 정보를 어떤 정보사용자가 갖고 있는지를 통지 받고, ②어떤 정보사용자가 저장하고 있는 이러한 정보에 접근할 수 있고, ③적절한 경우에 이러한 정보를 수정하거나 삭제할 권리를 관련 개인은 갖고 있어야 한다.

이러한 情報保護原則을 바탕으로 하여 우선 英國의 個人情報保護法은 公的 機關에서 自動情報處理에만 적용된다. 이 법에 따르면 정보이용자는 해당 정보의 상세한 내용을 등록부에 기록해야만 한다. 이러한 등록부에는 정보이용자의 이름과 주소, 個人情報保有目的, 정보제공자 등이 기록되어야 한다.[27] 그리고 등록인이 위에서 설명된 情報保護原則을 위반하였다고 판단되면 정보보호등록관은 해당 등록인에게 등록부에 포함된 등록사항의 전부 또는 일부를 삭제하도록 요구할 수 있으며[28] 삭제할 때까지 該當 個人情報의 이용이나 전달을 금지시킬 수 있다.[29]

그리고 個人情報保護法에 따르면 해당 개인은 자신에 관한 정보이용을 통지받고,

---

23) 이에 관해서는 James Michael, ibid., p.40 이하 참조.
24) Raymond Wacks, Personal Information, Clarendon Press, 1989, p.41.
25) 영국에서도 정보자유법의 제정이 야당 등으로부터 강력하게 주장되기는 하였지만 결국 제정되지 못하였다.
26) Data Protection Act Schedule 1. Part Ⅰ. The Principles, Part Ⅱ.
27) 개인정보보호법 제4조.
28) 개인정보보호법 제11조.
29) 개인정보보호법 제12조.

그 사용내용을 제공받을 權利를 갖고 있으며[30] 부정확한 정보 등으로 인하여 손해를 입은 경우에는 賠償을 받을 권리[31] 및 부정확한 정보에 관한 수정권과 삭제권을 갖고 있다.[32]

英國의 個人情報保護法에서 個人情報란 어떤 個人에 관한 의견의 표현을 포함한 情報로부터 同一性을 인식할 수 있는 自然人에 관한 情報이다.[33] 그런데 英國의 個人情報保護法은 일정한 유형의 情報들에게 특별한 성격을 인정하고 이러한 민감한 정보는 추가적인 보호를 받는다고 규정하였다.[34] 이는 위 個人情報保護法에서 개념정의된 個人情報가 반드시 민감한 정보일 필요는 없다는 것을 인정한 반면에, 민감한 個人情報는 특별히 취급해야만 한다는 것을 뜻한다. 마지막으로 영국의 個人情報保護法은 個人情報의 保護를 위하여 정보보호등록관과 情報保護法院을 설치하도록 하였다.[35]

4. 美 國

1) 問題提起

美國의 聯邦大法院은 헌법상 명시적으로 규정되지 않은 개인의 프라이버시를 判例를 통하여 적극적으로 보호하였다. 그러나 이렇게 普通法과 聯邦大法院의 判例를 통한 개인의 프라이버시보호는 한편으로는 포괄적이고 탄력적이라는 장점을 갖고 있으나, 다른 한편으로는 바로 이러한 점 때문에 개인의 프라이버시권이 어느 경우에 보호되는지가 불확실하다는 단점을 갖고 있으며 특히 憲法을 통한 프라이버시보장은 國家行爲로부터 보호로만 한정된다. 다만 여기서 개념상 다른 두 가지 유형의 프라이버시가 있다는 것을 기억하여야 한다. 곧 첫 번째 측면은 프라이버시보호에 관한 개인의 기대와 관련된다. 두 번째 측면은 개인프라이버시에 침입의 허용성판단과 관련된다. 첫 번째 유형의 프라이버시는 個人情報的인 것으로서 이는 자기자신에 관한 私的인 情報를 보호하려는 개인의 욕구와 관련된다. 두 번째 유형의 프라이버시는 개인의 自律과 관련된다. 곧 이는 스스로 자기 자신에 관하여 자율적으로 독립된 결정을 내릴 개인의 욕구를 보호하고자 하는 것이다.[36] 이에 따라서 개

30) 개인정보보호법 제21조.
31) 개인정보보호법 제22조.
32) 개인정보보호법 제23조.
33) 개인정보보호법 제1조.
34) 개인정보보호법 제2조제3항.
35) 개인정보보호법 제3조.
36) Henry H. Perrit Jr., ibid., p.89.

인의 프라이버시보호는 충돌하는 네 가지 이익들과 관련된다 : 곧 ①情報主體의 권리, ②개인에 관한 情報를 저장, 처리하는 사람의 이해관계, ③개인에 관한 정보를 획득하고, 규제나 起訴目的 등으로 사용하려는 國家의 이해관계, ④다른 사람에 관한 情報를 얻고자 하는 私企業이나 개인들의 이해관계. 英美法系에서 이에 관한 기본적인 법적 구조는 다음과 같다 : 普通法은 정보의 획득 및 그 공개를 제한하는 의무들을 개인에게 부과하고 이러한 의무를 위반했을 경우로부터 損害賠償을 받을 권리를 관련개인에게 보장한다. 그리고 憲法은 情報의 공개를 명령하는 특별한 경우를 제외하고는 자신에 관한 情報를 정부에 제공하지 않아도 되는 권리를 개인에게 인정한다.

그런데 情報社會에서는 상호연결되는 컴퓨터망들을 통하여 개인의 私生活이 침해될 수 있다는 문제가 강하게 제기된다. 왜냐하면 電算網이 연결되면 될수록 개인에 관한 情報를 서로 연결하는 것이 더 쉬워지기 때문이다. 특히 美國은 전세계에서 가장 먼저 情報社會에서 개인의 私生活이 심각하게 침해될 수 있다는 것을 인식한 나라중 하나에 속한다. 그럼에도 불구하고 미국은 개인관련정보를 포괄적으로 보호하는 法律을 제정하지 않았다. 오히려 구체적이고 개별적인 정보를 보호하며, 信用記錄機關처럼 특정 유형의 情報調査 및 사용기관을 규율하는 다양한 法律들이 聯邦이나 州에서 제정되고 있다.[37] 우선 이렇게 부분적 입법을 채택하게 된 첫 번째 이유는 美國의 聯邦大法院이 개인의 프라이버시를 헌법상 권리로 인정함으로써 이미 普通法과 憲法을 통하여 상당한 정도의 個人情報가 보호되고 있기 때문이다. 다만 普通法을 통한 보호는 포괄적이기는 하나 그 적용이 불확실하고 憲法을 통한 보호는 國家가 개인의 프라이버시를 제한하는 경우로만 한정된다. 결국 憲法에 따르면 개인은 法律에 규정된 경우처럼 특별한 경우를 제외하고는 개인이 자기에 관한 정보를 정부에 공개하지 않을 권리를 해당개인에게 인정한다. 통일적인 個人情報保護法이 미국에서 제정되지 않고 있는 또다른 이유는 美國의 지리적, 역사적 상황 때문이기도 하다. 결국 國家를 통한 시민의 감시문제는 그 나라의 크기에 비례할 수 있다는 것에 관하여는 더 이상의 설명이 필요없을 것이다. 미국이라는 나라의 크기와 복잡성, 많은 인구를 생각한다면 컴퓨터를 통한 정부감시는 물론 이러한 정부감시를 제한하고 個人情報를 보호할 조직모델의 채택 또한 그리 단순한 문제가 아니라는 것을 인식하게 된다. 오히려 역설적으로 매우 非中央化된 聯邦國家라는 시스템이 특히 정부기관들간 정보전달과 관련하여 個人情報를 보호하는 역할을 맡기도 한다.[38] 어쨌든 이에 반하여 미국인들이 그들의 프라이버시보호에 지속적으

37) Henry H. Perrit Jr., ibid., p.88.

38) 미국에서 情報保護委員會가 없음에도 불구하고 정부안팎에서 감독기능을 수행하려고 시도하

로 관심을 갖고 있다는 것은 그동안의 設問調査를 통하여 입증되고 있다.[39]

2) 프라이버시법

많은 논의와 토론을 거친 후에 마침내 포드대통령은 1974년 12월 31일 연방프라이버시법에 서명하고 이 법은 1975년 9월 27일부터 시행되었다. 이 법은 聯邦機關으로부터 개인의 私生活을 보호하고 聯邦機關이 갖고 있는 본인에 관한 기록에 접근할 권리를 해당 개인에게 부여한다.

우선 연방프라이버시법은 聯邦機關들이 보유하고 있는 기록들에 적용된다. 따라서 프라이버시법의 適用範圍는 "記錄(record)"의 개념정의에 의하여 결정되는 바, 프라이버시법에 따르면 記錄이란 "개인의 敎育, 財政, 病歷, 前科나 履歷을 포함하나 이것으로 제한되지는 않는 기관에 의하여 보유되는 이름, 개인확인번호, 상징, 지문이나 목소리, 사진처럼 개인을 구체적으로 확인할 수 있는 어떤 다른 것을 담고 있는 개인에 관한 정보, 정보의 수집이나 목록화(grouping)"이다.[40] 이러한 기록들은 구체적인 확인요소를 포함하는 경우에만 프라이버시법이 적용되는 기록으로 인정되기 때문에 실질적으로 개인을 확인할 수 있다 할지라도 거래나 기타 다른 환경조건 등에 관한 정보의 단순한 수집은 이러한 기록에 포함되지 않는다. 개인프라이버시의 침해로부터 시민을 보호하기 위해서는 결국 ① 聯邦機關에 의하여 유지되는 기록속에 개인에 관한 구체적인 정보가 담겨 있어야만 하고, ② 이러한 기록이 개인의 이름이나 어떤 다른 확인방법에 의하여 이러한 정보가 쉽게 검색될 수 있는 기록시스템 속에 담겨 있어야만 한다.[41]

비록 프라이버시법이 개인의 프라이버시를 보호함으로써 일정부분 個人情報를 보호한다 할지라도, 이 법은 프라이버시나 프라이버시이익들을 개념정의하고 있지 않다. 그래서 聯邦法院이 대부분 헌법상 보장되고 있는 프라이버시권 및 프라이버시법에 근거하여 개개 경우들에서 개인의 정보를 보호하고는 있으나, 이러한 보호가

는 기구들이 있다. 예를 들어 하원의 "정부정보, 正義(justice), 농업에 관한 소위원회"가 프라이버시법 및 정보자유법의 수행에 관하여 지속적으로 신경을 쓴다. 그리고 개인의 프라이버시를 보호하기 위하여 연방정부에 많은 압력을 여러 그룹들 - 정보보호전문가들, 기자들, 언론들, 시민단체 등 - 이 행사한다. 그리고 연방프라이버시법상 중요한 부분들을 이행하기 위하여 소송에 의존하는 것은 미국사회의 소송선호를 반영한다. 개인은 프라이버시법하에서 인정되는 권리들을 이행하기 위하여 연방법원에 소송을 제기해야만 한다.

39) 예를 들어 1979년의 설문조사에 따르면 미국시민 90%가 개인정보의 수집이 문제가 있다고 생각하였으며 79%가 개인관련정보의 지나친 이용을 우려하였으며 71%가 개인정보의 이용과 처리에 대한 통제가 어려울 것이라고 보았다.

40) 5 U. S. C. § 552 a (a) (4).

41) David H. Flaherty, ibid.; p.321.

체계적이고 일관적으로 행해지지는 못하고 있다. 어쨌든 프라이버시법은 個人情報의 수집과 전달에 관하여 명확하게 규정하고 있다. 곧 프라이버시법 제2항(b)에 담긴 目的拘束에 따르면 확인할 수 있는 個人情報를 수집, 저장, 사용 또는 전달하는 행위는 필요하고 합법적인 목적을 위한 것이어야 하며, 그 의도되는 사용을 위하여 해당 정보는 최신의 것으로서 정확하며 그 남용을 막기 위한 적절한 보호책들이 제공되는 방법으로 수집, 저장, 사용 또는 전달하도록 聯邦機關들에게 요구된다. 또한 개인의 프라이버시를 보호하기 위하여 프라이버시법은 법에 규정되어 있는 특별한 경우를 제외하고는 자신에 관한 기록이 수집, 저장, 사용 또는 전달되는지를 개인이 알거나 이에 관하여 동의할 수도 있도록 조치할 것을 聯邦機關에게 요구하였다.

프라이버시법은 수집목적과 양립할 수 있는 目的을 위한 경우를 제외하고 개인의 書面同意가 없이는 어떤 기록의 공개도 금지한다.[42] 그리고 이 법은 개인의 요구에 따라 기록된 자신에 관한 정보를 本人에게 공개할 것을 명령한다.[43] 또한 이 법은 모든 공개와 교정을 정확하게 기록할 것을 명령하고[44] 저장된 정보가 정확하지 않다는 주장이 거부당한 사람의 不一致陳述을 해당기관이 동시에 기록하도록 명령한다.[45] 그래서 制定法이나 大統領의 行政命令(executive order)에 의하여 수행되도록 명령된 기관의 목적수행을 위하여 필요하고 관련되는 것과는 다른 기록들을 해당 기관이 보관하는 것을 이 법은 또한 금지한다.[46] 그리고 이 법은 기관들이 이러한 기록들에 근거하여 결정을 내릴 때 이러한 결정의 合理性을 보장하기 위하여 정확하고 관련성이 있으며, 시의적절하고 완전한 기록의 유지를 명령한다.[47] 예를 들어 强制的 命令節次에 따라 개인에 관한 기록들이 공개될 때 기관들은 해당 관련자에게 이에 관하여 통지할 합리적인 노력을 기울여야만 한다.[48] 마지막으로 기관들은 기록의 安全性 및 信賴性을 확보하고, 이러한 기록을 보호하기 위하여 적절한 행정적, 기술적, 물리적 보호대책들을 확립해야만 한다.[49] 결국 부주의한 정보처리나 잘못된 정보의 저장은 특히 해당개인에게 해로울 수 있기 때문에 정당화할 수 없다. 또한 어떤 개인에 관한 정보에 근거하여 기관이 반대되는 결정을 내릴 때 이를 주체에게 통지하지 않는 것도 정당화될 수 없다. 그리고 획득된 목적과 일

42) 5 U.S.C. §552a(b).
43) 552a(d).
44) 552a(c).
45) 552a(d)(2)~(4).
46) 552a(e)(1).
47) 552a(e)(5).
48) 552a(e)(8).
49) 552a(e)(10).

치하지 않는 정보의 사용을 금지하는 것은 원래목적과는 다른 목적을 위한 사용으로 인하여 해당개인의 정당한 이익들을 해칠 수 있기 때문이다.

聯邦機關들이 저장, 처리하는 기록시스템에 관하여 다음과 같은 두 가지 방법으로 그 공개를 프라이버시법은 요구한다. 우선 첫 번째로 기존의 기록시스템이나 바뀐 시스템의 존재와 특징에 관하여 개개 기관이 공개하도록 하였다.[50] 그리고 두 번째로 개개 기록시스템들에 개인이 접근할 수 있도록 하기 위한 규정들을 만들도록 개개 기관에게 요구한다.[51] 더 나아가서 외부자들이 연방기관의 정보처리실무를 열람할 수 있는 또다른 방법은 연방기관들이 OMB와 의회에 제출하도록 요구되는 새롭게 실질적으로 바뀐 정보시스템들에 관한 보고서를 보거나 프라이버시법규정에 따른 機關의 通知 및 개인의 접근규정을 요약형태로 연방기록소에서 출간하는 인쇄물을 보는 경우이다. 이처럼 연방기록소는 매년 기록시스템에 관한 聯邦機關의 通知와 이에 관한 개인의 접근규정들을 모아서 출간한다. 그리고 연방기관의 부당한 정보처리로부터 개인을 보호하기 위하여 프라이버시법은 연방기관이 저장, 처리하고 있는 기록에 담긴 個人情報에 관련개인이 접근, 복사, 수정할 수 있도록 규정하고 있다.[52]

그럼에도 불구하고 개인기록의 濫用與否나 어떤 정보가 저장되고, 사용되는지에 관하여 개인이 안다는 것은 현실적으로 매우 힘들다. 그런데 美國에서 개인권리의 침해라고 인식되는 정보처리에 관해서는 개인 스스로 法院에 訴를 제기하는 것 이외에 또다른 특별한 장치가 프라이버시법하에서는 없을 뿐더러 개개 기관들에 의하여 받아들여진 정보처리에 관한 불평의 건수나 내용에 관해서도 알려진 것이 별로 없다는 것이 개인의 권리보호측면에서 본다면 아주 커다란 문제점이다.[53] 현재 OMB 스스로가 개인의 이의제기를 접수하기는 하나 이러한 이의제기가 대단히 드물 뿐만 아니라 국가기관 자체에 제기된 이의제기 및 그 처리에 관해서는 보고된 어떤 자료도 없다. 결국 현실적으로 이러한 정보처리를 감독하는 外部統制機關이 없기 때문에 프라이버시법에 규정된 기준들이 현실적으로 어떻게 적용되었는지를 안다는 것은 불가능하다.[54] 물론 개개 시민들이 그들의 권리를 보호받기 위하여

---

50) 552a(e)(4)

51) 552a(f)

52) 552 2(b)(3), 3(d)(f).

53) David H. Flaherty, ibid., p.339.

54) 연방프라이버시법에 근거하여 연방기관들이 소유하고 있는 기록시스템에 관한 공개명령에 따라서 연방기관이 제출한 정보처리자료를 OMB가 다른 국가기관이나 일반시민이 열람할 수 있도록 회람시킨다. 이러한 회람은 해당 기관의 과제수행을 위하여 필요한 정보만을 수집하고 처리, 전달, 사용, 저장하도록 함으로써 정보처리에 관한 통제를 강화하려는 의도를 갖고 있었

프라이버시법에 근거하여 訴를 제기한다는 것이 대단히 유용하다고 생각할 수 있을지도 모르나 현실을 살펴보면 그렇지 않을 수도 있다. 왜냐하면 프라이버시법에 따른 보호를 개인이 받기 위해서는 연방기관이 故意를 갖고서 행동하였다는 것을 原告가 立證해야만 할 뿐만 아니라, 프라이버시법에 규정된 정보처리기관에 관한 免責條項이 대단히 광범위하기 때문이다. 이에 따라서 결국 개인기록의 남용여부, 어떤 個人情報가 저장되고 사용되는지에 관하여 개개인 스스로가 알아내야만 한다는 것은 국가정보처리에 관하여 감독하고 통제하고자 할 때 특히 중대한 결함을 드러낸다.

프라이버시법이 제정된 이후에 프라이버시보호연구위원회가 만들어졌고 이 위원회는 1977년 이에 관한 보고서를 작성하였다. 이 위원회는 그당시 우선적으로 私的 領域에서 個人情報保護問題에 관심을 가졌었다. 불행히도 프라이버시보호연구위원회의 보고서는 公的 領域이나 私的 領域에서 個人情報保護에 관하여 직접적인 영향을 주지는 못하였다. 그 뒤 1983년 6월에 프라이버시법 전반에 관한 청문회가 처음으로 개최되었고 1991년에 다시 공화당의원 Wise가 個人情報保護法安을 제출하였다. 그 당시에 공화당의원 Wiese가 이렇게 立法案을 제출하게된 동기는 물론 일차적으로는 情報社會에서 개인의 私生活保護必要性에 있었지만, 유럽연합의 個人情報指針이 미국에서 유럽으로 그리고 유럽으로부터 미국으로 個人情報를 전달할 필요가 있는 美國會社들의 활동을 저해할 수도 있기에 이에 대비하고자 하는 데에 있었다. 이 법안은 일반적으로 프라이버시보다는 個人情報保護 - 특히 個人情報의 수집, 사용, 전달의 통제 - 에 더 많이 초점을 맞추었다. 이에 따라서 이 법안은 情報保護委員會(Data Protection Board)를 설치하려고 하였다. 물론 이 위원회에게는 어떤 규제권한을 부여하는 게 아니라, 個人情報의 保護를 촉진할 역할만을 맡기고자 하였다. 1977년 미국프라이버시보호연구위원회의 의장이었던 David F. Linowes는 이 법안에 관한 청문회에서 프라이버시보호입법을 위하여 다음과 같은 원칙들을 강조하였다 : ① 구체적 결정들과 관련되는 정보만이 수집되어야만 한다. 수집된 정보는 이러한 목적을 위해서만 사용되어야 한다. ② 개인의 同意나 최소한 개인에게 통지 없이 제3자에게 어떤 정보도 전달되어서는 안된다. ③ 정부가 어떻게 個人情報를 수집, 사용하며 누구에게 공개하였는지를 해당개인에게 통지해야만 한다. ④ 개인은 자신에 관한 기록들을 열람하고 복사할 권리를 가져야만 한다. ⑤ 개인은 기록의 正確性에 관하여 질문하고 수정할 권한을 가져야만 한다. 이러한 개인진술의 진위여부가 논란이 된다면 이러한 개인의 진술은 영구적으로 저장되는 파일

다. 따라서 연방기관들이 OMB의 이러한 의도와 지시들에 따른다면 이러한 회람은 나름대로 프라이버시보호를 위하여 의미가 있을 수 있다. 그러나 실제적으로 이러한 회람은 오로지 연방기관의 정보처리행위를 정당화하기 위한 근거만을 만들어 주었을 뿐이다.

의 일부분이어야만 한다. ⑥ 개인기록들에 접근하고자 하는 공무원은 정보에 접근이 허용되기 이전에 이에 관한 적절한 권한을 갖고 있어야만 한다. 그리고 해당개인에게 이러한 접근에 관하여 통지되어야만 한다.[55]

3) ECPA법

전자통신프라이버시법(Electronic Communications Privacy Act ECPA)[56]은 정보서비스제공자 및 관리인에게 개인의 프라이버시보호에 관한 義務를 부과함은 물론 침입자 및 盜聽者에 관한 처벌규정 또한 두고 있는 법이다. 전자통신프라이버시법은 電子通信을 통하여 저장된 전자메시지들에 담긴 개인의 프라이버시를 보호하고자 제정된 법으로서 電子通信을 도청하기 위해서는 令狀을 받도록 규정하고 있다. ECPA의 Title 1[57]은 通信內容의 획득과 공개에 관한 것이다. Title 2[58]는 저장된 정보의 획득과 공개를 포함한다. 이 법 Title 1, 2는 인간의 音聲 및 電子通信에 적용된다.[59] Title 3[60]은 거래되는 정보의 획득 및 공개를 다룬다. 위 법률의 개정으로 인하여 비디오테이프임대기록의 보호가 추가되었고[61], 이통통신수단(transponder, mobile tracking devices)을 통한 개인의 프라이버시도 보호된다.[62] 그래서 이 법은 공중통신기기(common carriage)에서 개인의 프라이버시보호로만 한정되는 게 아니라, 私的인 네트워크에서 개인의 프라이버시보호 또한 포함하도록 의도되었다. 그래서 ECPA는 人工衛星을 통한 권한 없는 盜聽도 포함한다. ECPA의 Title 1은 전달중인 意思疏通(communications streams), 그래서 사람의 목소리와 情報 모두를 보호한다. 有線通信에서 개인의 프라이버시보호는 국내 또는 외국과 통신을 위한 시설을 제공하거나 이러한 시설의 작동업무에 종사하는 사람들에 의하여 유지되는 電線이나 이와 유사한 전송매개체를 통하여 행해지는 聽覺的 傳達로 제한된다.[63] 그래서 결국 ECPA법의 Title 1은 電子通信을 보호한

55) Henry H. Perrit, ibid., p.148 이하.
56) 18 U.S.C. §§2510~2522, 2701~2711.
57) 18 U.S.C. §§2510~2521.
58) 18 U.S.C. §§2701~2710.
59) 여기서 전자통신(electronic communication)은 전자우편, 디지털화된 전송, 비디오화상회의처럼 정보로만 구성된 의사소통을 뜻한다.
60) 18 U.S.C. §§3121~3126. 이 Title 3은 합헌으로 결정되었다. United States v. Cafero, 473 F. 2d 489, 501 & n. 9 (3d Cir. 1973).
61) 18 U.S.C. §2710.
62) §3117.
63) 18. U.S.C. §2510(1). 텔렉스(Telex)통신의 획득은 청각적 획득에 속하지 않는다. 왜냐하면 이것은 목소리의 청취를 동반하지 않기 때문이다. United States v. Gregg, 829 F. 2d 1430, 1433 (8th Cir. 1987).

다. 여기서 電子通信(Electronic communication)이란 "國內的 通商 또는 外國과 通商에 영향을 주는 電線, 無線通信, electromagnetic, photo electronic, photo optical system에 의하여 전체적으로 또는 부분적으로 전달되는 신호, signs, 이미지, 소리, 문자, 정보나 소식의 이동을 뜻한다."[64] 有線(wire)通信과 電子通信間 구별은 有線通信은 聽覺的 傳達로 제한되고 다른 無線에 의한 전달을 포함하지 않는다는 것이다. Title 1은 이 법에 포함되는 통신유형의 盜聽, 盜聽된 通信의 공개, 盜聽된 내용의 사용, 盜聽裝置의 계획적 사용을 금지한다.[65] 이 법은 공적 전자통신서비스업자가 受信人이나 전달하고자 하는 受領人이 아닌 어떤 다른 사람에게도 이러한 通信內容을 故意로 누설하지 못하도록 금지한다.[66] 그러나 ECPA는 서비스제공자의 재산이나 權利를 보호하기 위한 경우나 통신서비스에 필연적으로 부수되는 활동들과 연결되어 시스템작용자가 통신을 盜聽, 공개, 사용하는 것은 허용한다.[67] 그리고 전자감시에 종사하거나 통신을 盜聽하려는 법집행기관 및 이 법하에서 이에 관한 권한이 있는 다른 기관을 원조할 가능성이 통신시스템의 작용자에게 인정된다.[68] 이에 따라서 위 법 Title 1은 서비스제공자의 財産이나 權利保護, 통신서비스의 작동을 위하여 필요한 경우에 受信人이나 發信者의 동의를 얻어서 또는 서비스제공자에 의하여 우연히 획득된 통신내용이나, 법집행기관에게 행해지는 내용공개가 刑事訴追에 관한 것인 통신내용들을 공개할 권한을 공공통신서비스업자에게 인정한다.[69] 동의된 도청의 목적이 聯邦이나 州의 憲法이나 法律들에 위반하여 犯罪나 不法行爲를 행할 목적이 아닌 한, 관련당사자가 盜聽에 동의하였을 때 有線通信의 盜聽에 대한 금지규정은 적용되지 않는다. 여기서 Title 1의 適用範圍는 "有線, 口述 또는 電子通信"[70]이란 문구에 의하여 결정된다. 有線通信(wire communication)이란 발신점과 수신점간에 有線, 케이블, 기타 다른 통신전달을 위한 시설들의 사용을 통하여 전체적으로나 부분적으로 행해지는 어떤 聽覺的인 傳達"을 포함하는 것으로 개념정의된다.[71] 따라서 有線通信은 공중통신업자(common carrier)에 의하여 처리되는 통신들로 제한되지 않는다. 私的인 네트워크와 회사내 통신시스템도 이 법의 적용범위에 속하나, 미국영토밖에서 행해지는 도청은 포함되

64) 18 U.S.C. §2510(12).
65) 18 U.S.C. §2511(1)(a)~(d).
66) §2511(3)(a).
67) 18 U.S.C. §2511(2)(a)(i).
68) §2511(2)(a)(ii).
69) §2511(3).
70) §2510(1)(a).
71) §2510(1).

지 않는다. 이러한 개념정의는 聽覺的으로 傳達되는 通信內容이 통신시스템에 딸려 있는 장치에 저장된다면 이러한 통신의 電子的 情報도 포함한다. 특히 음성사서함(voice mail)이 이에 포함되나 無線電話通信은 명백히 배제된다.[72] 따라서 有線通信은 전자장치수단들에 의하여 확대되는 통신을 포함하지 않고, 녹음기에 의하여 기록되는 口述通信도 포함하지 않는다. ECPA의 Title 1은 有線, 口述 또는 電子通信을 盜聽하기 위하여 우선 사용될 수 있도록 고안된 기구들의 생산, 유통, 소유, 광고를 금지한다.[73] 이러한 "기구들"에는 하드웨어뿐만 아니라 情報通信을 검색하기 위하여 만들어진 컴퓨터프로그램도 속한다. 그러나 가입자의 전화이용상황기록장치(pen registers), trap, trace devices 등은 ECPA Title 1의 적용범위로부터 명백히 배제되는 대신에 Title 3의 적용을 받는다. ECPA의 Title 2는 저장된 有線 및 電子通信과 거래기록(transactional records)에서 개인의 프라이버시를 보호한다.[74] 여기서 전자통신서비스가 제공되는 시설에 권한 없이 접근하거나, 이러한 有線通信施設이나 電子通信施設에 접근을 막는 불법적인 접근금지는 수단적 요인과 결과적 요인을 동반한다. 手段的 要因이란 전자통신서비스가 제공되는 시설에 권한 없이 접근하거나 권한을 넘어서서 의도적으로 접근하는 경우를 말한다.[75] ECPA Title 1의 §2510(15)은 전자통신서비스를 전화회사, 전자우편회사, 원거리컴퓨터서비스를 포함하는 것으로 개념 정의한다. 結果的 要因이란 電子的으로 저장된 有線通信이나 전자통신내용에 접근하거나 이를 임의로 바꾸거나, 권한 있는 접근을 막는 것이다.[76] 여기서 불법적인 접근금지란 제3자만을 향하고 서비스제공자나 사용자에는 적용되지 않는다.[77] 추가로 공적 전자통신서비스와 공적 원거리컴퓨터서비스의 제공자는 제공된 서비스가 단순히 저장목적을 위한 경우이거나, 컴퓨터로 처리하는 서비스인 경우에는 가입자나 소비자로부터 電子的으로 받아서 저장된 통신내용을 누설할 수 없다.[78] 다만 ECPA Title 2의 §2702에 규정된 비공개의무가 전자통신서비스제공자 및 공중에 대한 원거리컴퓨터서비스에만 부과되기 때문에 私的인 通信이나 컴퓨터서비스의 운용자에 의한 공개를 금지하지 않으

72) §2510(1).
73) §2512.
74) 18 U.S.C. §§2701~2710. 18 U.S.C. Title 1의 §2510(17)의 전자저장(electronic storage)이란 컴퓨터, 마그네틱 테이프, 디스크, 다른 마그네틱 매개체 - 광학적 매개체의 random access memory를 포함하는 - 를 통한 저장을 말한다. 저장은 전자적 전달에 뒤따르는 일시적인 저장도 포함한다. 18 U.S.C. §2510(17)(A).
75) §2701(a)(1).
76) §2701(a).
77) §2701(c).
78) §2702.

며, 순수하게 內的인 통신시스템으로부터 메시지나 파일의 공개를 금지하지도 않는다.[79] 그러나 ECPA법 Title 1은 有線通信이나 電子通信의 내용을 공개하여 법집행기관을 돕도록 지시하는 法院이나 法務部長官에 의한 명령에 의하여 유선통신서비스제공자, 전자통신서비스제공자, 그 직원, 고용인, 대리인 등에 관한 免責規定을 두고 있다.

4) 私的 情報處理

지금까지 설명을 통하여 알 수 있는 것처럼 美國의 聯邦憲法을 통하여 보장되는 개인의 프라이버시는 지금까지 전적으로 國家의 제한으로부터 보호로만 이해되고 있지 私人으로부터 보호로 이해되고 있지 않다. 이에 따라서 私的 部門에서 개인관련정보보호를 위한 일반적인 聯邦法은 지금까지 통과되지 않았으며 다만 개별영역을 위한 규정들이 여러 法律들에 부분적으로 있을 뿐이다.[80]

5) 小 結

(1) 美國에서는 지금까지 완결된 개인정보보호시스템은 존재하지 않는다.[81] 다시 말하면 美國에서 個人關聯情報가 보호되는 범위가 유럽과 비교하면 매우 한정되어 있다는 것이다. 우선 聯邦次元에서 個人情報를 보호하고자 하는 法律들이 다수 있기는 하나 이는 언제나 다소 제한된 일부영역만을 위한 法律들이다. 결국 그렇다면 美國에서는 個人情報保護에 관한 일관성있는 시스템이 확인되지 못한다고 말할 수 있다.[82] 앞으로도 미국에서 公的 領域을 규율하는 일반적인 個人情報保護法의 제정가능성이 희박하여 보인다 할지라도, 분야별로 규율하는 制定法들이 聯邦과 州 차원에서 제정되고 있으며 제정될 것이다.[83] 이러한 상황하에서도 美國은 특정영역에서 個人情報를 보호하는 法律들을 제정하는 데에서는 상당한 진보를 이뤄냈는바,

---

79) 보기 : 전자게시판에 의한 공고.

80) Stephan Wilske, Datenschutz in den USA, CR 1993, S. 299. 州憲法에 개인의 프라이버시권이 규정되어 있는 경우도 있으나 私人으로부터 보호를 규정하는 헌법규정은 없다. 私的 領域에서 중요한 법률로는 1970년 공정신용기록법(Fair Credit Reporting Act), 1974년 공정신용경리법(Fair Credit Billing Act, 1976년 개정), 1974년 가족교육권 및 프라이버시법(the Family Educational Rights and Privacy Act, 1976년개정), 1977년 공정한 채무수집실행법(the Fair Debt Collection Practices Act), 1978년 재정적 프라이버시권에 관한 법(the Right to Financial Privacy Act), 1988년 컴퓨터연결과 프라이버시보호법(the Computer Matching and Privacy Protection Act) 등이 있다.

81) Marie-Theres Tinnefeld, Der Datenschutz in den Vereinigten Staaten, RDV 1992, S. 21 이하.

82) Stephan Wilske, a.a.O., S. 307.

83) James Michael, ibid., p.89.

이에 관한 가장 좋은 사례가 1988년에 제정된 "컴퓨터연결과 프라이버시보호법"이다.

(2) 美國의 프라이버시법이 제정당시에는 매우 혁신적이었고 다른 나라에 미치는 영향력 또한 매우 컸다 할지라도 다른 나라에서와는 달리 실제로 이러한 제정법이 잘 작용하는지를 統制할 책임은 대단히 광범위하게 분산되어 있다. 예를 들어 이 법은 聯邦政府에 의한 個人情報의 수집과 처리에 관한 규정들을 담고 있으나 정보감시문제들을 검토하거나 個人情報保護問題를 파악하기에는 미국의 정부조직구조가 너무 복잡하다. 이에 따라서 개인의 프라이버시를 침해할 수 있는 행위들이 동시에 여러 곳에서 발생할 수 있다. 그럼에도 불구하고 다른 나라들에서처럼 國家의 情報處理를 통제할 外部監督機關을 설치하는 것 대신에 미국에서는 制定法이 잘 작용되는지를 보장할 책임을 해당 國家機關 자체에게 넘기고 있다. 그리고 이러한 內部的인 統制와는 별도로 프라이버시법의 이행에 관한 監督은 대통령관할하에 있는 管理豫算室(Offiece of Management and Budget, OMB)이 부분적으로 담당한다. 결국 이를 분석하여 본다면 기본적으로 美國의 정보보호시스템은 外部的 統制機關의 직접적인 개입 없이 해당 행정기관들이 자체적으로 해결하는 방식을 택하였다는 것을 알 수 있다. 이러한 시스템에는 개개 국가기관 스스로가 정보처리 및 프라이버시문제들을 다루어야만 한다는 생각이 바탕에 깔려있는 것이다. 이에 따라서 OMB와 議會의 所管委員會, 法院에게는 이러한 행정기관의 실무를 事後的이고 制限的으로 감독하는 역할만이 기대된다. 특히 美國에서 프라이버시법의 이행에 관한 감독은 대통령관할하에 있는 管理豫算室(Offiece of Management and Budget, OMB)이 담당한 것은 聯邦政府의 情報處理를 통제하는 데에는 현명하지 않은 선택으로 입증되었다. 왜냐하면 OMB 스스로가 프라이버시법의 집행에 관한 감독권한만을 갖고 있을 뿐인데다 실제로 OMB는 유럽이나 캐나다의 情報保護委員會와 비교한다면 집행과정에서 상대적으로 약한 지도력을 행사하고 있기 때문이다. 따라서 美國에서는 個人情報保護를 위한 효율적인 統制機關이 없기 때문에 OMB와 개개 정부기관들의 실제작업을 분석하고, 분야별로 접근하여 검토해야만 한다. 그렇다면 個人情報保護를 위한 현재의 미국시스템은 심각한 문제점을 갖고 있다고 말할 수 있다. 왜냐하면 1974년에 제정된 프라이버시법이 적절히 시행되고 개인의 프라이버시권이 보호되고 있는지를 감독할 적절한 統制機關을 갖고 있지 않기 때문이다. 물론 情報社會에서 國家의 정보처리보다 개인의 프라이버시권이 언제나 우월해야만 한다고 주장할 수는 없으나 이러한 권리가 입법과 행정실무에서 언제나 고려되어야만 한다는 것을 잊어서는 안된다.

3) 情報社會에서 개인의 私生活保護에 관하여 많은 연구를 하고 있는 플래허티는

美國의 프라이버시법이 대폭적으로 개정될 필요가 있다고 주장한다. 곧 그는 프라이버시법제정이후에 새롭게 등장한 情報通信技術의 적용에 의하여 개인의 프라이버시를 침해할지도 모르는 위험성을 방지할 수 있도록 美國의 현행 프라이버시법은 개정되어야만 한다고 주장한다.[84] 먼저 플래허티는 美國에서 현재 개인정보보호시스템이 만족스럽게 작동하고 있지 않으므로 프라이버시법이란 法律 이름 자체를 바꾸어야만 한다고 주장한다. 곧 "프라이버시"법이란 이름 자체에 문제가 있다는 것이다. 이러한 法律 이름은 개인의 모든 프라이버시문제들이 이 법을 통하여 적절히 다루어지고 있다는 잘못된 인식을 많은 사람들에게 심어준다는 것이다. 그러나 실제로 현행 프라이버시법은 1970년대 이후에 등장하였던 개인프라이버시의 보호에 관한 가장 근본적인 문제들중 많은 것에 대처하지 못하고 있기 때문에 프라이버시법은 새로운 형태의 情報技術에 의하여 제기되었던 많은 문제들을 더 충분하게 반영해야만 한다는 것이다. 결국 여기서 가장 중요한 문제는 프라이버시법이 제정된 이후에 國家에 의한 情報處理技術에 급격한 변화가 발생하였음에도 불구하고 이러한 정보통신기술의 적용을 통제하는데에 실패했다는 것이다.[85] 따라서 프라이버시법은 오늘날 정보통신기술의 발전에 맞추어서 대폭적으로 개정되어야만 한다는 것이다. 계속해서 플래허티는 서유럽국가들에서처럼 個人情報保護에 관한 일반적인 統制機關을 만드는 것이 현재 美國에서 어렵다면 OIRA내에 프라이버시정책국을 만드는 것이 바람직할지도 모른다고 언급하고 있다. 물론 프라이버시법의 遵守與否를 개개 국가기관이 책임지는 모델이 꼭 잘못되었다고 말할 수는 없으나 外部機關이나 議會를 통한 統制를 강화할 필요성이 강하게 요구된다는 것이다.

어쨌든 플래허티는 美國에서 個人情報를 보호하기 위하여 프라이버시보호위원회를 설치하는 것이 가장 바람직하다고 주장한다. 그리고 이러한 프라이버시위원회는 다음과 같은 책임과 권한들을 가져야만 한다고 역설하고 있다[86] : ① 우선 이러한 委員會는 個人情報保護와 관련되는 모든 상황에서 이러한 個人情報가 保護되고 있는지를 세밀하게 검토하고, 특히 個人情報를 보호하기 위한 경보시스템으로서 기능해야만 한다. ② 이 위원회는 연방기관의 모든 情報處理過程에서 개인의 프라이버시가 보호되는지를 監督해야만 한다. ③ 프라이버시법에 규정된 연방기관의 義務遂行與否를 감독하고, ④ 프라이버시법규정의 준수여부를 감독하기 위하여 연방기관의 정보처리시스템을 조사, 열람, 감독하고, ⑤ 연방차원에서 個人情報保護를 위한 적절한 안전지침과 실무지침을 발전시키며 ⑥ 특정유형의 개인정보시스템들에 관하

84) David H. Flaherty, ibid., p.368.
85) David H. Flaherty, ibid., p.367.
86) David H. Flaherty, ibid., p.365 이하 참조.

여 필요하다고 생각하는 적절한 규정들을 권고하고, ⑦ 개인프라이버시를 위하여 情報通信技術의 발전을 평가하며 ⑧ 美國에서 모든 유형의 프라이버시문제들에 관하여 연구를 하고 기록한다. 이러한 委員會는 가능한 정도로 立法府와 行政府만큼 독립되어야만 하며 委員會는 그들의 과제수행을 위하여 연방기관들과 합의, 조정, 협조할 수 있는 권한을 가져야만 한다.

5. 캐나다

캐나다에서 개인의 私生活保護法制에 관하여 살펴보면 우선 盜聽을 규제하는 1974년 프라이버시법이 이 부문에서 중요한 법률로 부각된다. 왜냐하면 이 법이 캐나다에서 개인의 프라이버시권을 연방법률중에서 인정한 첫 번째 법률이었기 때문이다. 먼저 1970년대에 캐나다에서는 일반시민이든 의회든 간에 새로운 기술에 의한 개인의 프라이버시침해가능성을 별로 인식하지 않고 있었다. 그 뒤 1982년에 연방프라이버시법이 제정되어서 1983년 7월 1일 효력을 발생하였다. 캐나다의 연방프라이버시법은 聯邦政府에 의한 個人情報의 수집과 사용에 관하여 다룬다. 이 법은 캐나다인권법 4장의 프라이버시규정들을 보충하였고 聯邦次元에서 공정한 정보실무원칙을 도입하였으며 프라이버시위원을 설치함으로써 個人情報를 보다 더 확실하게 보호하고자 하였다. 특히 1982년 연방프라이버시법은 프라이버시위원을 독립된 기관으로 만들고 그 감독 및 감사권한을 상당히 강화하였다.

우선 1974년에 제정된 캐나다의 프라이버시보호법은 電話盜聽 및 電子監視의 규제로만 한정되었다. 이에 따라서 연방차원에서 캐나다는 1977년 캐나다인권법 4章에서 정보프라이버시를 보호하는 규정을 보충하였다. 이 법은 1974년에 제정된 美國의 프라이버시법률과 유사하였다. 우선 이 법은 자동화된 시스템이든 수작업파일이든 구별하지 않고서 적용되며, 여기서 個人情報란 연방정부에 의하여 저장되는 自然人에 관한 정보를 뜻하며, 이 법에서 情報運用과 使用에 관하여 관련성, 정확성, 공정성이라는 기본원칙들을 확립하였다. 그러나 캐나다가 이 법률을 제정할 때 많은 부분에서 미국의 立法例를 따랐지만 개개인으로부터 불평을 들을 프라이버시위원을 만든 점에서는 유럽국가들의 立法例에 따랐다.

1982년 캐나다는 다시 프라이버시에 관한 法律을 제정하였는데, 이 법률에는 정부가 갖고 있는 정보에 접근할 시민의 권리와 개인의 프라이버시권이 동시에 규정되어 있다. 이처럼 情報公開와 個人情報保護를 하나의 法律에 모아서 규정하는 立法例는 전세계적으로 캐나다에서 처음으로 채택되었다.[87] 議會는 가능한 한 조화

87) 지금까지도 이러한 입법례에 따른 國家는 아직 없다.

되는 방법으로 情報自由와 個人情報保護 모두가 실현될 수 있도록 하기 위하여 이러한 法律을 제정한 것이다. 그래서 個人情報란 단어는 두 법영역들에서 모두 동일한 의미를 갖는다. 특히 이 法律의 草案者들은 프라이버시법규정의 적용을 피하기 위하여 情報自由法이 사용될 수 있었던 美國의 경험을 의식하였던 것이다. 1982년 연방프라이버시법은 聯邦政府의 統制 밑에 있는 手作業情報와 自動處理되는 情報 모두에 적용된다. 주관적인 접근권과는 별도로 이 법은 국가기관에 의한 個人情報의 수집 및 저장에 관한 원칙들을 규정하고 있다.[88] 이들 조항에 규정된 원칙들은 다음과 같다 : 수집, 처리되는 情報는 정확하고 최신의 것이어야만 하고, 수집되었던 목적과 일치하지 않는 목적을 위하여 사용되어서는 안되며, 관련개인에게 정보수집의 목적에 관하여 통지되어야만 하며 예외적인 경우가 아닌 한 정보는 관련개인의 同意 없이는 공개되어서는 안된다. 이러한 원칙들은 다른 國家들의 個人情報保護法에서 열거되고 있는 기본적인 情報保護原則들과 매우 유사하다. 그리고 연방프라이버시법하에서 자신의 권리를 행사하고자 하는 사람들을 돕는 것이 매년 출판되는 個人情報目錄(index)인데 이 목록에는 정부의 모든 個人情報銀行目錄과 개인의 접근이 제한되는 정보가 어떤 것인지에 관한 내용이 담겨 있다. 다만 국가가 갖고 있는 공적 정보에 관한 시민의 일반적인 권리처럼 자신의 정보에 관한 주관적인 접근권 또한 캐나다시민과 거주민으로 한정된다.[89] 그리고 관련개인이 프라이버시위원에게 불평하거나 이 위원이 조사할 수 있는 절차, 法院에 抗訴節次 등은 國家情報에 접근하는 경우를 위한 절차들과 거의 비슷하다. 이제 캐나다의 모든 개인들은 個人情報銀行에 있는 자기자신에 관한 情報뿐만 아니라 國家의 統制下에 있는 본인에 대한 정보에 대해서도 접근권을 갖고 있다.[90] 이러한 접근권을 개인에게 허용하지 않는 國家의 결정에 대해서는 聯邦法院이 審査하는데[91] 이에 관한 立證負擔은 申請人이 아니라 政府에게 있다. 그리고 法院이 이러한 경우를 심사하기 위한 유일한 전제조건은 접근이 거부되었다는 사람의 불평을 프라이버시위원이 첫 번째로 심사해야만 한다는 것 뿐이다. 프하이버시위원이 국가의 견해에 동의한다 할지라도 法院의 審査는 행해질 수 있다. 그러나 연방프라이버시법은 특정한 정보은행들을 개인의 접근으로부터 배제하고 프라이버시위원이 이에 관한 분쟁을 조정하도록 규정하고 있다. 이에 따라서 프라이버시위원은 이러한 情報銀行들을 감사하고 어떤 개인파일은 이러한 정보파일속에 담겨서는 안된다고 該當 國家機關의 長에게

88) section 5, 6, 7, 8.
89) James Michael, ibid., p.75.
90) 연방프라이버시법 제12조.
91) 연방프라이버시법 제41조.

권고한다. 이러한 권고에 대한 該當 國家機關의 응답이 부적절하거나 응답이 합리적 시간 내에 이루어지지 않았다고 프라이버시위원이 결정한다면 관련개인은 聯邦法院에 이에 관한 審査를 신청할 수 있다.[92]

聯邦政府는 個人情報를 보호하기 위하여 의회, 프라이버시위원, 캐나다연방법원 간에 역할을 나누는 복잡한 시스템을 채택하였다. 우선 일차적으로 개개 國家機關의 長이 그 조직 내에서 프라이버시법의 집행에 관하여 책임을 진다. 그 다음으로 法務部는 個人情報를 보호하기 위한 정책개발 및 法的 紛爭에 대하여 책임을 지고 法律의 解釋과 이에 관하여 諮問한다. 또한 프라이버시위원은 개인정보시스템들을 許可하거나 기록하지는 않으나 다양한 國家機關들에서 정보처리를 기록하고 조사할 권한을 가진다는 점에서는 유럽의 정보보호기관에 가깝다. 1982년 연방프라이버시법은 자동화된 情報處理로만 한정되는 게 아니라, 모든 個人情報에 적용된다. 이에 따라서 실제로 현재의 프라이버시법은 個人情報保護法이 되어버렸다. 본래 立法目的은 國家機關에 의하여 보유되는 個人情報에 관하여 규율함으로써 개인의 프라이버시를 보호하고자 하는 것이었다.[93] 그러나 이 법에서 프라이버시란 단어는 유감스럽지만 더 이상 개념 정의되고 있지 않다. 위에서 설명한 것처럼 연방프라이버시법은 個人情報의 수집, 삭제, 보호와 관련되는 공정한 정보실무를 포괄적으로 담고 있는 바, 가장 중요한 새로운 규정중 하나는 연방기관의 활동이나 운용과 직접적으로 관련되는 경우를 제외하고 어떤 個人情報도 國家機關에 의해서 수집되어서는 안된다는 규정이다. 따라서 가능한 한 이러한 정보는 개인들로부터 직접 수집되어야만 하고 수집되는 목적에 관하여 해당 개인에게 통지되어야만 한다.[94] 그리고 위 법 제8조는 상당히 자세하게 國家機關이 그 통제하에 있는 個人情報를 공개할 수 있는 13가지 조건들을 확정하였다. 따라서 예를 들어 개인이 이러한 공개에 同意하거나 연방기관에 의하여 수집된 情報가 사용목적과 일치하는 경우에 해당 정보를 공개할 수 있다.

1982년 연방프라이버시법에서 가장 중요한 내용은 프라이버시위원에게 더 적극적인 역할을 맡도록 그 법률상 지위를 바꾼 것이었다. 우선 프라이버시위원은 개인으로부터 불평에 의존하기보다는 독립적으로 조사할 권한을 갖게 되었다. 프라이버시위원이 이러한 감독능력을 적극적으로 사용함으로써 國家의 情報處理를 성공적으로 통제하고 개인의 私生活을 보호할 수 있게 된다. 추가로 프라이버시법은 프라이버시위원이 國家機關들의 불평을 조사할 수 있도록 규정하였다. 더나아가 프라이버

92) 연방프라이버시법 제36조 1.
93) 연방프라이버시법 제2조.
94) 연방프라이버시법 제4조, 제5조.

시위원들은 여러 다른 상황들에도 간섭할 수 있다. 예를 들어 개인은 프라이버시위원에 직접적으로 불평함으로써 자신의 기록들에 접근이 거부된 경우로부터 구제받을 수 있다. 캐나다의 프라이버시위원은 議會의 승인을 받아서 임명되며 임기는 7년이다. 곧 캐나다의 프라이버시위원은 정부에 의하여 직접 임명되지 않으며 의회에 속한다.[95] 이 위원은 개인의 불평을 조사하고, 司法審査에 참여하며 의회에 매년 보고서를 제출한다. 개인의 불평들은 1년 이내에 서면으로 프라이버시위원에게 제출되어야만 하나 프라이버시위원은 이러한 불평접수없이도 조사를 시작할 수 있다. 그러나 프라이버시위원은 광범위한 조사권한 및 免責權限을 갖고 있기는 하지만 해당 정보의 공개를 명령할 권한이 아니라 諮問할 권한만을 갖고 있을 뿐이다.[96] 프라이버시위원의 權限은 勸告的인 것으로서 국가기관에 명령하지는 못한다. 그러나 연방정부의 個人情報實務를 감독하기 위하여 이 위원은 이러한 諮問權限에 크게 의존한다. 또한 프라이버시위원은 법규정에 의해서든 개인의 요구에 의해서든 간에 어떤 민감한 정보의 공개기록들을 검토할 수 있는 권한을 갖고 있다.[97]

6. 獨 逸

1) 問題提起

1970년대에 독일의 聯邦政府는 모든 거주민에게 12자리숫자로 구성된 個人確認番號를 도입하려고 하였으나 비판가들은 이러한 個人確認番號가 헌법상 존재하는 개인의 人格權을 근본적으로 위협한다고 주장하였다. 결국 이에 따라서 이러한 個人確認番號에 근거한 어떤 정보처리시스템도 이에 대응하는 정보보호체계없이는 만들어져서는 안된다는 것에 의회도 동의하였다. 이후 독일에서는 이러한 個人確認番號를 도입하려는 생각은 다시 제기되지 않았다. 왜냐하면 1976년에 다시 立法府가 이러한 個人確認番號의 도입에 반대하였기 때문이다. 1980년 연방의회는 地方自治團體의 인구를 기록하기 위한 규정을 담고 있는 기록법을 통과시켰으나 이 법에도 個人確認番號에 관한 규정들이 들어가 있지는 않다. 이 법에 따라서 해당 기록기관들은 개인의 거주장소 및 그 身元을 확인하고 입증할 수 있기 위하여 그 관할영역내에 있는 거주자들에 관하여 기록하였다. 다만 개인에 관하여 기록하는 기관들은 選擧人名簿作成, 身分證明書, 旅券發給, 兵役義務 등을 위하여 이러한 정보들을 사용할 수 있도록 허용하였다. 그리고 국가기관들이 이러한 의무들을 수행하기 위하

95) 연방프라이버시법 제53조 1.
96) James Michael, ibid., p.81.
97) 연방프라이버시법 제8조제4항, 제8조제5항, 제9조제3항, 제37조제1항.

여 인구기록소는 19가지 종류의 정보들을 공유하도록 허용하였다. 따라서 오늘날 독일에서 사용되는 개인확인시스템은 해당 국가기관들이 수행하고자 하는 구체적인 목적들을 위하여 그들 자신의 시스템을 발전시키고 이를 위해서만 사용한다. 예를 들어 社會保障目的을 위한 年金保險番號가 있으나 이는 美國의 社會保障番號와는 달리 일반적으로 개인을 확인하기 위하여 사용되지는 않는다. 이러한 번호는 고령보험 등 社會保險目的을 위해서만 사용될 수 있다. 1980년대 초반에 연방의회는 컴퓨터가 읽을 수 있는 개인확인카드를 또다시 도입하려고 하였으나 1983년 聯邦憲法法院의 人口調査決定 때문에 이러한 카드의 도입이 또다시 무기한 연기되었다.[98]

2) 人口調査判決

이미 1970년대 말에 人口調査法草案이 의회에서 자세히 검토되었으나 3억 7천만 마르크에 달하는 엄청난 비용 때문에 통과되지 못하였다. 1981년초에 당시 與黨이었던 CDU가 그 내용이 본질적으로 크게 달라지지 않은 人口調査法을 다시 연방의회에 상정하였다.[99] 연방의회는 결국 1982년 3월 25일 人口調査法(Volkszählungsgesetz 1983)을 통과시켰다.[100] 이 법에 따라 人口調査는 1983년 4월 27일 하기로 확정되었다. 그러나 몇 주만에 상황이 급격하게 변하였다. 곧 위 인구조사법은 연방의회에서 여당이나 야당 모두에게 전혀 정치적인 이슈가 아니었던데 반하여, 바로 국민들이 밑에서부터 격렬하게 이 법에 반대하기 시작하였다. 왜냐하면 이 인구조사법이 그들의 人格權을 충분히 존중하지 않는다고 많은 국민들이 생

98) 정보보호수임인들은 내무부에 이러한 전자카드 - 특히 개인프로필을 만들기 위한 정보저장 및 다목적 사용의 위험 때문에 - 의 도입필요성을 설명하도록 요구하였다. 이 문제는 대단히 정치적이었다. 綠色黨은 어떠한 신원확인카드의 도입에도 반대하였고, 사민당은 전자카드에 반대하였고, 보수적인 연합정부는 이를 받아들이고자 하였다.

99) 연방정부와 여당이 이 立法案을 상정하면서 人口調査가 불가피하다고 제시한 사유는 다음과 같다 : a) 국민의 인구적·사회적 특징을 아는 것은 연방과 州가 여러 가지 사회적·경제적·정치적 결정을 내리기 위한 불가피한 토대이다. b) 그밖에 정당, 경제단체, 직업단체처럼 공적 생활과 관련하여 중요한 의미를 가지는 단체들도 그들의 활동을 위하여 이러한 인구조사결과에 의존한다. c) 게다가 이 시점에서 가장 최근의 情報들을 조사하지 않는 한 잘못된 투자와 계획이 넓은 범위에서 나타날 것으로 우려된다. d) 따라서 가장 현대화되고 기술적인 절차에 따라 원하는 情報들을 가능한 한 빨리 모으고 이를 이용할 수 있다면 이를 이용하지 않았을 경우보다 시간과 비용을 많이 절약한다. 자세한 것은 Otwin Massing, Von der Volkszählungsbewegung zur Verrechtlichung oder : Ôffentlichkeit, Herrschaftsrationalisierung und Verfahren, Harald Hohmann (Hrsg.), *Freiheitssichrung durch Datenschutz*, Suhrkamp, 1987, S. 94.

100) 이 법률의 원래 이름은 "das Gesetz über eine Volks-, Berufs-, Wohnungs-, und Arbeitsstättenzählung"이다.

각하였기 때문이다. 이렇게 주목을 받으면서 제기된 인구조사법에 대한 憲法訴願에 관하여 드디어 聯邦憲法法院은 판결을 내렸다. 이 인구조사판결에서 연방헌법법원은 우선 인구조사법에 규정된 조사계획이 憲法에 合致되지 않는다고는 볼 수 없다고 확정하였다. 하지만 이 인구조사법 제9조제1항과 제3항은 一般的 人格權(기본법 제1조제1항과 결합한 제2조제1항)을 침해하였기 때문에 違憲이라고 하였다. 곧 統計目的을 위한 人口調査와 申告記錄(Melderegisterabgleich)의 결합은 憲法이 요구하는 명령들에 일치하지 않는다는 것이다. 그 다음으로 상급연방관청이나 州官廳에 개인관련정보들을 전달하도록 규정한 제9조제2항 또한 違憲이라고 결정하였다. 그리고 마지막으로 지방자치단체영역에서 조사된 개인관련정보를 특정한 行政目的을 위하여 처분할 수 있도록 규정한 이 인구조사법 제9조제3항도 違憲으로 결정되었다.[101] 이 인구조사판결은 情報社會에서 시민의 私的 領域保護, 특히 情報自己決定權의 보호를 일깨우는 출발로서 의의를 가지는 결정이었다.[102] 많은 문헌들에서 지적되는 것처럼 聯邦憲法法院의 인구조사판결은 情報社會, 高度技術社會에서 점점 더 많은 情報를 필요로 할 수밖에 없는 국가와 이로부터 자기의 私的 領域을 보호하고자 하는 시민간에 갈등 속에서 탄생하였다. 그렇다면 위 설명에서 이미 나타나는 것처럼 국가나 시민 어느 한쪽을 일방적으로 편드는 결정을 聯邦憲法法院이 내린 것이 아니라 "憲法"과 조화하는 기술채택, 憲法이 정하고 있는 테두리 내에서 정보사회건설을 그 해결방안으로 제시한 것이다. 그래서 이 인구조사결정은 단순히 人口調査에 관한 것만을 담고 있는 것이 아니라 이를 넘어서서 오늘날까지도 유효한 국가정보처리의 전제조건들에 관한 여러 중요한 언급들을 담고 있다.

3) 人口調査判決以後 重要法律의 改正

우선 聯邦憲法法院의 人口調査判決以後에 노르트라인-베스트팔렌, 자르란트, 베를린헌법, 브란덴부르크와 작센州의 憲法에 情報自己決定權이 基本權으로 추가되었다.[103] 그러나 聯邦憲法이 개정될 때 이에 관한 많은 贊反論議가 있었으나 결국 州憲法에서와는 달리 情報自己決定權은 기본권으로 규정되지 못하였다.[104]

---

101) BVerfGE 65, 1/62면 이하.

102) Scholz/Pitschas, a.a.O., S. 12.

103) 이에 관하여 자세한 것은 Alfred Einwag, Die neuen Bundesländer und das neue Bundesdatenschutzgesetz, RDV 1992, S. 1 이하 ; Philip Kunig, Der Grundsatz informationeller Selbstbestimmung, Jura 1993, S. 597 ; Thilo Weichert, Neue Verfassungsregelungen zur informationellen Selbstbestimmung, CR 1992, S. 738면 이하 참조.

104) Peter Gola, Zwei Jahre neues Bundesdatenschutzgesetz, NJW 1993, S. 3109 이하 참조. 오스트리아헌법, 스페인헌법, 네델란드헌법, 포르투칼헌법 등이 개인관련정보이용

인구조사판결 이후에 먼저 미크로젠주스법, 旅券法, 身分證明書法[105], 統計法[106] 등이 개정되었다. 安保領域에서도 이 인구조사판결 이후에 憲法保護廳法[107]이 개정되고 聯邦諜報機關法(Bundesnachrichtendienst)[108]과 軍防諜機關法(der Militärische Abschirmdienst)[109]이 제정되었다. 學問의 自由나 情報의 自由와 情報自己決定權이 충돌하는 영역에서 聯邦文書保管法(Bundesdatenarchivgesetz)[110], 슈타지서류법(Stasi-Unterlagen Gesetz)[111] 등이 제정되었다.

그 다음으로 聯邦憲法法院의 인구조사판결 이후에 人口調査法이 1987년 11월 8일 개정되었다. 먼저 이 법의 통계조사대상은 1983년 人口調査法과 동일하였다. 개정된 법에는 개인관련정보의 삭제와 분리에 관한 규정이 삽입되었고, 시민의 情報自己決定權保護를 위하여 인구조사담당자의 엄격한 비밀유지의무 등이 추가되었다. 또한 인구조사를 통하여 획득된 情報들이 다른 절차나 다른 목적들을 위하여 사용되는 것이 명시적으로 금지되었다. 결국 이 法律에 따라 행정집행목적을 위한 정보전달은 더 이상 가능하지 않게 되었으며 오로지 통계목적를 위한 정보전달만이 허용된다.[112] 지금까지 聯邦憲法法院은 이 개정된 人口調査法의 違憲與否를 다투는 憲法訴願을 받아들인 적이 없다.[113]

구체적인 분야에서 個人情報를 保護하는 또다른 立法例로는 聯邦文書保管法(Bundesdatenarchivgesetz)을 들 수 있다. 이 법률은 硏究目的을 위하여 국가가 보관하고 있는 문서이용에 관한 규정을 담고 있다. 이는 국가가 문서보관소에 개인관련정보가 담긴 서류를 넘기는 것을 통하여 발생할 수 있는 위험에 대비하여 節次法的이고 組織法的 豫防措置를 만들어야만 한다라는 인식하에서 특별히 제정된 법

에 관하여 규정하고 있다.

105) Reinhold Baumann, Datenschutz drei Jahre nach dem Volkszählungsurteil, RDV 1987, S. 118.

106) 이에 관하여는 Otto Ziegler, *Statistikgeheimnis und Datenschutz*, VVF 1990 참조.

107) BGBl. I, 2970(1990.12.29).

108) BGBl. I, 2979.

109) BGBl. I, 2977.

110) 이 법은 1988년 1월 15일 시행되었다. 자세한 것은 Dieter Wyduckel, Archivgesetzgebung im Spannungsfeld von informationeller Selbstbestimmung und Forschungsfreiheit, DVBl, S. 1989, 327 이하 참조.

111) 이 법은 1991년 12월 20일 시행되었다. 이에 관해서는 Klaus Stoltenberg, Die historische Entscheidung für die öffnung der Stasi-Akten - Anmerkungen zum Stasi- Unterlagen-Gesetz, DtZ 1992, S. 65면 이하 참조.

112) Gerhard Groß, Das Recht auf informationelle Selbstbestimmung mit Blick auf die Volkszählung 1987, das neue Bundesstatistikgesetz und die Amtshilfe, AÖR, 1988, S. 178면 이하.

113) Gerhard Groß, a.a.O., S. 183.

이다. 연방기관은 그들의 관할에 있는 서류가 더 이상 필요하지 않은 경우에 연방문서보관소에 이 문서들을 넘겨준다. 그런데 國家機關이 이러한 서류들이나 문서를 문서보관소에 전달함으로써 다른 法律에서 특별하게 보호되는 個人關聯情報가 침해될 수 있다. 이러한 경우에 관련자의 보호할 가치있는 이익을 연방문서보관소는 고려해야만 한다. 따라서 관련자가 문서보관소에 자기에 관한 정보를 전달하는 것을 受忍할 수 있기 위해서는 우선 이에 관한 특별한 법규정을 통해서 넘겨진 서류가 보호되어야만 한다. 그러나 모든 서류가 아니라 문서로 보존할만한 가치가 있다고 판단된 경우에만 보관하거나 저장하고 넘겨준 行政機關과 문서보관소는 이 문서가 또 다른 行政目的에 쓰이지 않도록 하기 위한 예방책을 강구하고 제 3자나 관련자의 보호할만한 가치있는 이익이 침해되지 않는 경우에만 문서열람을 통한 개인관련정보의 결합이 허용된다. 이 문서보관소법에 따라서 관련자는 자신의 기록에 관한 설명권과 열람권, 교정권과 반론권을 가진다. 個人關聯情報는 관련자가 사망한 이후 30년이 지나면 이용할 수 있으나 예외적인 경우에는 관련자가 사망한 이후 보호기간이 60년 또는 80년으로 늘어난다. 그러나 관련자 스스로 또는 사망후 그 후손이 이용에 동의하면 법적 보호기간은 짧아진다.

그리고 통일이후에 獨逸에서 새롭게 個人情報保護問題가 제기된 분야가 바로 슈타지가 보관하고 있던 각종 서류였다. 곧 과거 東獨에서 비밀첩보기관인 슈타지가 여러 가지 다양한 방법으로 동독국민들을 감시하였는 바, 통일이후에 슈타지건물에서 이에 관한 엄청난 서류가 발견되었다. 이에 따라서 의회는 슈타지서류법(Stasi-Unterlagen Gesetz)[114]을 제정하였는데, 이 법에는 동독의 과거를 歷史的, 法律的, 政治的으로 종합적으로 관찰하려는 연구단체나 언론에게 이러한 서류에 접근을 보장하는 규정 또한 만들었다. 곧 이 法律은 이러한 연구단체나 언론에게 단계화된 접근권을 인정하였다 : 곧 ① 전혀 개인관련성이 없는 슈타지의 서류, ② 슈타지가 보관하던 서류중 匿名化된 個人關聯情報, ③ 보관서류중 공개할 경우 문제가 될 수 있는 슈타지직원, 슈타지협조자, 슈타지특혜자에 관한 개인관련정보로 나누어 서류열람권을 인정한 것이다.

4) 개인정보보호법

먼저 독일에서 個人情報保護法制의 발전에 관하여 시대적으로 구별한다면 ⓐ 1977년 1월 27일 聯邦情報保護法과 州의 情報保護法制定을 통하여 제 1단계가 시작되었고 ⓑ 情報自己決定權을 憲法上 基本權으로 인정한 聯邦憲法法院의 人口調査

114) BGBl 1991 I, S. 2272 ff.

判決이 두 번째 단계를 형성하고 ⓒ 세 번째 단계는 1990년 12월 20일 제정되어 1991년 6월 1일부터 시행된 새로운 聯邦情報保護法의 적용에서부터 시작된다.

聯邦憲法法院의 人口調査判決 以後에 제정되거나 개정된 法律中 가장 중요한 法律이 바로 聯邦情報保護法(Bundesdatenschutzgesetz)이다. 독일에서는 1977년 1월 27일 제정된 연방정보보호법이 처음으로 개인관련정보처리에 관한 포괄적인 법적 근거를 만들었는데 ① 연방헌법법원의 인구조사판결, ② 정보와 통신기술발달 및 ③ 연방정보보호법의 적용을 통하여 드러난 문제점 등 때문에 개정필요성이 강하게 제기되었다.[115] 원래 聯邦議會는 1982년에 聯邦情報保護法을 개정하려고 하였으나 정권교체 및 특히 聯邦憲法法院의 人口調査判決때문에 의회에 상정된 情報保護法草案이 통과되지 않았다. 많은 논란과 토의 끝에 마침내 1990년 聯邦情報保護法이 개정, 통과되었다. 이러한 聯邦情報保護法과 州情報保護法은 個人情報保護에 관한 범위구체적인 法律들에 대하여 보충적으로 작용하는 一般的인 個人情報保護法이다.

우선 개정된 聯邦情報保護法 제1조제1항은 이 法律의 保護利益이 一般的 人格權임을 분명하게 규정하였다. 따라서 이 법은 더 이상 예전처럼 個人關聯情報의 濫用으로부터 시민을 보호하는 것에 관한 것이 아니라 濫用與否와는 상관없이 개인관련정보의 調査로부터 貯藏·使用·傳達에 관하여 규율한다.[116] 이는 개정된 情報保護法이 情報濫用으로부터 개인을 보호하는 것에만 제한되지 않음을 명백히 하면서 그 보호목적을 확대하고 구체화한 것이다.

그 다음으로 聯邦情報保護法의 適用範圍가 확대되었다. 그래서 개인관련정보는 情報의 調査로부터 處理(저장, 변경, 전달, 삭제, 이용)를 거쳐 匿名化될 때까지 보호된다. 개정된 법률에 情報의 調査와 利用이 포함됨으로써 情報處理 이외의 모든 개인관련정보의 사용이 情報利用을 뜻하게 되었다. 그리고 聯邦情報保護法은 자동화된 정보처리뿐만 아니라 서류들도 그 適用範圍에 포함시켰다.[117] 다만 聯邦情報保護法의 適用範圍에 서류가 포함되는지 여부는 公的 領域과 非公的 領域에서 다르게 규정되었다. 公的 領域에서는 원칙적으로 個人情報의 保護가 또한 書類 속의 개인관련정보로까지 확대되는 반면에 非公的 領域에서는 서류속의 개인관련정보는 위

115) Alfred Büllesbach, Das neue Bundesdatenschutzgesetz, NJW 1991, S. 2593. 연방정보보호법의 개정이 늦은 이유 : ① 정치적으로 문제되는 안보기관법률과 관계 ② 개인관련정보의 조사를 포함할지 여부 ③ 서류를 통한 정보처리문제 ④ 비공적기관의 정보처리에 대한 규정필요성 ⑤ 정보보호수임인의 통제권한범위 ⑥ 정보처리에서 관련자동의의 의미 등에 관하여 논란이 있었기 때문이다.

116) Alfred Büllesbach, a.a.O., S. 2595.

117) 연방정보보호법 제3조제3항, 제27조제2항.

법률의 適用範圍에 속하지 않는다. 여기서 書類라는 개념은 州情報保護法에 이미 규정되어 있던 개념에 의존하였는데 이는 모든 公的 目的 또는 業務目的을 위하여 사용되는 書類를 말한다.[118]

세 번째로 情報自己決定權을 보호하기 위하여 개인관련정보를 처리하고 이용할 때 目的拘束原則이 舊法보다 新法에 엄격하게 규정되었다.[119] 이에 따라서 公的 領域에서는 물론 非公的 領域에서도 개인관련정보의 처리와 이용의 목적구속강화가 특별히 강조될 수 있다. 따라서 과제수행을 위하여 필요하고 처리목적을 위하여 행해지고 조사되는 경우에만 개인관련정보의 저장, 변경, 이용이 허용된다. 또한 聯邦情報保護法 제16조제4항에 따라 受信人은 전달받은 목적을 위해서만 그 정보를 처리하거나 이용하여야 한다.

네 번째로 개인정보관련자의 權利가 여러 측면에서 향상되었다.[120] 특히 본인에 대한 정보를 받을 때 이러한 정보제공은 원칙적으로 무료로 행해져야 한다는 立法者의 결정이 개인의 정보보호를 위하여 중요한 의미를 갖는다.[121] 자기에 관한 정보처리와 저장기관을 통한 이용에 관하여 알 수 있기 위하여 관련개인에게 인정되는 說明權은 個人情報를 보호하기 위해서는 매우 중요한 統制權이다. 이러한 정보에 관한 설명과 동의요구를 통하여 자신에 관하여 저장된 情報를 교정하거나 統制할 기회가 관련자에게 보장된다. 계속해서 이러한 權利는 누가 저장기관인지 알 수 없는 파일결합과 電算網에서 정보처리로까지 확대된다. 또한 연방기관의 개인관련정보조사, 처리, 이용을 통하여 자기의 權利가 침해되었다고 생각하는 모든 사람들은 이에 대하여 聯邦情報保護受任人에게 호소할 수 있는 權利를 갖고 있다.[122] 또한 개정법 제28조제3항에 따라 廣告 또는 市場調査과 輿論調査目的을 위하여 개인관련정보를 이용하거나 전달하는 것에 대한 항변권이 관련개인에게 인정된다. 관련개인이 이에 관하여 항변하면 해당 정보는 이러한 목적으로 이용되지 못한다.[123]

다섯 번째로 자동화된 呼出節次(automatisierte Abrufverfahren)로부터 個人情報를 보호하는 규정이 도입되었다.[124] 컴퓨터연결을 통한 직접호출절차는 정보가 교환되는 관련자의 이익이 고려되고 해당기관의 과제측면에서 필요한 경우에만 허용된다. 따라서 개정법에 따르면 전체적인 온라인연결을 통한 個人情報傳達은 허용

118) Alfred Büllesbach, a.a.O., S. 2595.
119) 연방정보보호법 제14조제1항.
120) 연방정보보호법 제16조제3항.
121) 연방정보보호법 제19조, 제34조.
122) 연방정보보호법 제21조.
123) 자세한 것은 연방정보보호법 제6조, 제7조를 참조.
124) 연방정보보호법 제10조를 참조.

되지 않는다. 오히려 정보를 받는 기관이 저장한 기관에게 정보를 사실상 호출한 경우에 비로소 전달이 존재한다.[125] 이에 따라서 聯邦情報保護法 제10조에 근거하여 온라인연결을 통한 정보전달의 原因, 目的, 情報受信人, 種類 등이 문서로 확인되어야만 한다.

여섯 번째로 1977년 情報保護法은 責任問題를 다루지 않았던 반면에 개정법은 제7조에서 公的 領域을 위한 특별한 책임구성요건을 만들었다. 公的 機關이 이 法律規定이나 個人情報保護에 관한 다른 규정에 반하여 허용되지 않거나 정당하지 않은 방법으로 관련자의 개인관련정보를 처리한다면 해당 기관은 관련자에게 損害賠償責任이 있다.

그 밖에 聯邦情報保護受任人의 法的 地位를 강화하였는 바 의회를 통한 聯邦情報保護受任人의 선출을 결정하였다. 그리고 聯邦情報保護法 제22조에서 제26조까지 公的 機關을 위한 聯邦情報保護受任人의 선출, 법적 지위, 통제, 그외 다른 과제가 규정되어 있다. 이 법규정에 따라서 聯邦情報保護受任人의 우선적인 임무는 個人情報를 保護하기 위하여 公的 領域에서 情報處理의 발전을 감독하는 것이다. 그러나 이러한 과제수행을 하기 위한 聯邦情報保護受任人의 역할은 우선적으로 勸告的인 것으로서 그는 조사하고 설득할 권한은 갖고 있으나, 구속력 있는 지시를 내릴 권한을 갖고 있지는 않다. 다만 聯邦情報保護法이나 다른 情報保護法들을 위반하는 사례를 발견했을 때 해당 기관에 공식적으로 불평할 권한이 그에게 부여되어 있다.[126] 결국 聯邦情報保護受任人은 個人情報를 보호하기 위하여 활동하는 옴부즈만으로서 기능한다.

5) 小 結

獨逸聯邦憲法法院의 人口調査判決은 人口調査法을 개정하도록 했을 뿐만 아니라 컴퓨터가 읽을 수 있는 개인확인카드시스템의 도입 또한 취소시켰다.[127] 情報公開에 많은 노력을 기울였던 美國과 달리 獨逸은 대부분 컴퓨터이용을 통하여 나타날 수 있는 위험성으로부터 개인의 私生活을 保護하는 立法에 집중하였다. 그리고 個人情報를 다루는 私的 領域의 規制는 스칸디나비아국가들이나 영국과 같은 나라의 시스템과는 아주 다르다. 곧 私的 領域의 情報處理 또한 公的 領域에서 情報處理에 요구되는 기준을 따라야만 하는 후자의 시스템과는 달리 獨逸에서 非公的 情報處理機關은 情報處理에 관한 一般的인 記錄義務도 없고 公的 機關에서 보다는 여러 측

125) 연방정보보호법 제3조제5항.
126) 연방정보보호법 제20조제1항.
127) James Michael, ibid., p.93 이하.

면에서 자유롭게 個人情報를 調査, 處理할 수 있다. 어쨌든 獨逸은 포괄적인 個人情報保護法律들을 제정한 국가로서 1969년 이후로 잘 발전된 개인정보보호시스템을 갖춘 매우 중요한 모델중 하나라고 말할 수 있다.[128]

7. 日 本

日本의 경우에는 中央政府에서 個人情報保護法를 제정하기 이전에 地方自治團體에서 條例로서 個人情報를 보호해왔다. 地方自治團體의 이러한 條例들은 電算處理되는 個人情報만을 규율대상으로 하며 個人情報保護法에서 규정하고 있지 않은 내용을 보완하는 역할을 담당하고 있다고 한다.[129]

일본은 마침내 1988년 行政機關이 보유하는 전자계산처리에 관계된 個人情報保護에 관한 法律을 제정하였다. 이 法律에 열거된 個人情報保護에 관한 基本原則을 살펴보면 다음과 같다 : 1) 資料蒐集制限의 原則 - 個人情報를 수집할 때 수집목적을 밝혀야 하며 수집되는 情報도 이러한 목적을 위하여 필요한 최소한도의 범위로 한정되어야만 한다. 2) 利用制限의 原則 - 수집된 情報는 事前에 구체화된 목적을 위해서만 이용되어야 한다. 3) 個人參與의 原則 - 자신에 관한 情報가 저장, 처리되는 개인은 이러한 내용에 관하여 알고 있어야만 하고, 이를 위하여 본인의 정보에 관한 접근권과 수정권을 갖고 있어야만 한다. 4) 適正管理의 原則 - 수집된 정보는 정확하고 최신의 것이어야만 한다. 5) 責任原則 - 個人情報를 관리하는 機關은 情報管理에 관한 責任을 져야만 한다.[130]

1988년에 제정된 日本의 個人情報保護法은 國家機關에게만 적용된다.[131] 그리고 이 법에서 "個人情報"란 생존하는 개인에 관한 정보로서 당해 정보에 포함되는 姓名, 生年月日, 기타 記述이나 개인별로 붙여진 번호, 기호 기타 부호에 따라 당해 개인을 식별할 수 있는 것을 말한다고 규정하였다.[132] 또한 이 法律에 의하면 행정기관은 法律에 정해진 사무를 수행하는데에 필요한 경우에 한하여 개인정보파일을 보유할 수 있으며 이러한 파일도 필요한 범위를 초과해서는 안된다.[133] 그리고 行政機關은 電算處理過程에서 個人情報의 누설, 손상방지 등 여러 안전조치들을 취해

128) David H. Flaherty, ibid., p.21.

129) 일본의 지방자치단체 510여개가 개인정보보호에 관한 조례를 갖고 있다고 한다. 임재홍, 개인정보보호법과 개인정보보호조례, 민주법학 9호, 민주주의법학연구회, 1995, 293면 이하 참조.

130) 안문석, 정보체계론, 학현사, 1995, 499면 이하 참조.

131) 개인정보보호법 제1조.

132) 개인정보보호법 제2조 2.

133) 개인정보보호법 제4조.

야만 하며[134] 해당 行政機關의 長은 總務廳長官에게 해당기관이 보유하는 개인정보파일에 관한 사항을 통지하여야 한다.[135] 해당 행정기관이 보유하는 個人情報는 機關內에서만 이용되어야만 하고 파일보유목적 이외의 목적으로 이용해서는 안된다.[136] 그리고 누구라도 본인에 관한 정보의 처리를 공개하도록 書面으로 청구할 수 있고 예외적인 경우를 제외하고 行政機關은 이를 공개하여야 한다.[137] 또한 이러한 정보가 잘못되었을 경우에 해당 개인은 訂正을 청구할 수 있으며 해당 행정기관은 이를 조사하고 그 결과를 請求者에게 통지하여야 한다.[138]

第2節 公共機關의 個人情報保護에 관한 法律의 制定背景과 그 內容

1980년대부터 우리 나라는 行政電算網을 포함하여 國家基幹電算網事業을 추진하였다. 이는 결국 국가가 선도적으로 情報化를 추진함으로써 情報通信技術分野에서 만큼은 先進國에게 뒤지지 않겠다는 강한 의지를 갖고 있었음을 나타낸다. 그리고 이러한 國家基幹電算網事業의 추진을 통하여 민원처리시간이 단축되고, 행정서비스가 질적으로 개선되는 등의 많은 효과를 본 것 또한 사실이다. 그러나 이와 동시에 국가기관내에서 個人情報의 電算化가 확대됨으로써 잘못된 정보의 입력, 電算情報의 유출 등으로 인한 개인의 私生活侵害可能性이 증대하였다. 이에 대하여 종전의 法律들로는 충분히 대처하기가 곤란하였기 때문에 학계와 언론 등에서 個人情報保護에 관한 法律의 제정을 촉구하였고 이에 따라서 마침내 1994년 1월 7일 '공공기관의개인정보보호에관한법률'이 제정되어 1995년 1월 8일부터 시행되었다.

우선 個人情報保護法은 公共機關에서 컴퓨터로 처리하는 個人情報를 대상으로 한다.[139] 이 법에 따르면 個人情報中 思想, 信條 등 개인의 基本的 人權을 침해할 우려가 있는 정보에 대해서는 수집을 제한하고 있다.[140] 그리고 국가기관은 기관의 업무를 수행하기 위하여 필요한 범위내에서만 개인정보파일을 보유할 수 있도록 하였으며[141] 個人情報의 부당한 유출, 변조나 부정확한 정보로 인한 개인의 私生活侵

134) 개인정보보호법 제5조.
135) 개인정보보호법 제6조.
136) 개인정보보호법 제9조.
137) 개인정보보호법 제13조 이하.
138) 개인정보보호법 제17조.
139) 개인정보보호법 제1조.
140) 개인정보보호법 제4조.
141) 개인정보보호법 제5조.

害를 예방하기 위하여 공공기관에 個人情報의 정확성과 안정성을 확보할 수 있는 대책을 수립하도록 하였다.[142] 이 법에 따라 관련개인은 자신의 정보에 관하여 열람을 청구할 수 있으며 잘못된 정보에 대한 정정을 청구할 수 있으며, 이러한 요구가 받아들여지지 않을 경우에 行政審判을 청구할 수 있다.[143]

이 個人情報保護法은 1995년 1월 8일부터 시행에 들어갔으며 현재 약 29, 000개의 기관에 적용되고 있다. 총무처는 위 법 시행이후에 1995년 4월 30일까지 公共機關이 보유하고 있는 파일에 대해 개인정보파일의 명칭, 보유목적, 보유근거, 기록대상자의 범위, 기록항목의 범위 등 처리현황을 통보하도록 하였다. 그 결과 전체 4,791개 기관에서 332종 10,579개의 파일을 보유하고 있으며 총 기록건수는 10억 2천만건에 달하는 것으로 나타났다. 그리고 1996년 10월에는 공공기관에서 보유하고 있는 개인정보파일현황을 종합한 공공기관의 개인정보파일목록집을 발간하였다.[144]

第3節 公共機關의 個人情報保護에 관한 法律中 改正되어야 할 內容

1. 改正必要性

1) 內 容

이미 위에서 설명한 것처럼 각국의 個人情報保護法에는 우선 情報社會에서 개인의 私生活, 個人情報가 보호되어야만 한다는 공통된 인식과 목표하에서 個人情報保護에 관한 중요한 원칙 및 이러한 원칙들의 실현에 관한 여러 일반적인 기준들이 대체로 비슷하게 담겨 있다는 것을 파악할 수 있다. 그러나 이러한 一般的 原則들과 基準들을 한 국가와 사회 속에서 구체적으로 적용할 때 바로 해당 국가의 정치, 사회, 문화, 법체계 등이 나름대로 작용하게 된다. 따라서 일반적으로 어떤 국가나 사회가 "情報社會"인가라는 토론과 더불어 구체적으로 정보사회에 속하는 "特定" 國家와 社會는 어떠한 문제점과 특징을 갖고 있는지라는 논의를 동시에 진행해야만 한다는 것이다.

먼저 美國을 비롯한 대부분의 서유럽국가들은 1970년대부터 80년대 중반사이에 "1세대" 個人情報保護法을 제정하였다. 그 뒤 서유럽국가들과 다른 많은 나라들은 급격하게 발전되는 정보통신기술에 발맞추어 1980년대 후반부터 "2세대" 個人情報

142) 개인정보보호법 제9조.
143) 개인정보보호법 제12조 이하.
144) 한국전산원, 1997 국가정보화백서, 668면 이하 참조.

保護法律로 개정하고나 새롭게 제정하고 있다. 이에 반하여 우리 나라는 1980년대 이후에 정력적으로 국가가 行政電算網事業 등 國家와 社會의 情報化에 주력하면서 개인의 私生活侵害가 우려된다는 비판이 강하게 제기되자 個人情報保護에 관한 立法을 추진하였다. 이에 따라서 마침내 1994년 "공공기관의개인정보보호에관한법률"이 제정, 공포되었다. 그런데 유감스럽게도 우리 나라의 個人情報保護法은 國際的으로 본다면 1990년대에 만들어진 가장 최근의 個人情報保護法임에도 불구하고 그 내용은 서유럽국가 등에서 수십년전에 만들어진 "1세대" 個人情報保護法에 가깝다는 것이었다. 게다가 국민의 낮은 個人情報保護意識, 個人情報保護를 위한 효율적인 統制方案의 缺如, 國家機關이나 私的 情報處理機關을 통한 個人情報의 무차별적 저장과 전달 등을 통하여 우리 나라에서는 "個人情報保護法"은 있으되 정작 "個人情報"는 보호되지 못하고 있는 실정이다.

결국 이는 다른 나라들에서 個人情報保護法을 만들었을 뿐만 아니라 이러한 法律의 施行을 통하여 문제점을 발견하고 이를 다시 法改正을 통하여 반영하는 법실무와는 달리 우리 나라는 "個人情報保護法"을 제정하였다는데에 만족하고 있는 현실을 드러내고 있는 것이다. 이러한 사실은 立法者가 필요한 法律을 제정함으로써 그 일차적인 임무를 이행했다면 法律이 존재하는가가 아니라 이미 존재하는 法律이 제대로 지켜지는가를 분석해야만 한다는 것을 일깨워준다. 國家나 社會의 情報調査나 處理로부터 개인의 私生活을 보호하기 위하여 個人情報保護法律을 제정하는 것만으로는 충분하지 않고, 국가나 사회에서 이러한 法律이 실제로 준수될 수 있도록 노력해야만 한다. 그러기 위해서는 우선 國家機關의 엄격한 법집행, 국민들의 私生活保護意識 등을 살피는 法政策的 分析도 중요한 몫을 차지한다. 하지만 과연 우리 나라의 個人情報保護法 자체가 이미 처음부터 문제점을 갖고 있기에 個人情報가 충분하게 보호되지 못하고 있는 것은 아닌가 하는 것을 法解釋的, 立法論的으로 따져보아야만 한다. 따라서 이 章에서는 우리 나라의 個人情報保護法이 정말로 개인의 私生活을 보호할 수 있기 위하여 과연 어떤 부분들이 문제를 갖고 있으며 어떻게 改正되어야만 하는지를 검토하고자 한다.

여기서 個人情報를 保護하기 위하여 분명히 인식해야만 하는 전제조건은 우리 나라의 個人情報保護法은 다른 나라의 "1세대" 個人情報保護法처럼 個人關聯情報의 濫用으로부터만 市民을 보호하는 것이 아니라 그 濫用與否와는 상관없이 개인관련정보의 조사로부터 저장·사용·전달로부터 보호해야만 한다는 것이다.[145] 따라서 이는 個人情報保護法이 정보의 남용으로부터 개개인을 보호하는 것에만 제한되지 않음을 명백히 하면서 그 保護目的을 확대해야만 한다는 것을 뜻한다.

---

145) Alfred Büllesbach, a.a.O., S. 2595.

2) 個人情報保護法의 목적

독일연방헌법법원이 人口調査判決에서 인정한 情報自己決定權에 따르면 개개인의 情報自己決定權行使가 아니라 국가를 통한 개인관련정보의 파악이 正當化를 필요로 한다는 결과를 갖는다. 정보기술과 정보처리의 발전 때문에 바로 個人情報保護와 情報安全이 과거보다 더 큰 의미를 갖는다. 왜냐하면 컴퓨터와 電子情報處理가 도입된 이후에 지금까지는 인식되지 못했던 정도로 개개인의 基本權들을 제한할 수 있는 새로운 가능성들이 생겨났기 때문이다. 그래서 누가, 언제 그리고 어떤 경우에 자기의 어떤 정보를 이용하고 전달하는지를 개개인이 더 이상 알지 못할 수도 있다. 그러므로 情報社會에서 개인의 자기결정자유를 보호해야할 특별한 필요성이 더욱 더 존재하는 것이다.[146] 따라서 당사자의 동의가 없거나, 이에 반하는 정보조사와 처리는 情報自己決定權과 곧장 조화할 수 없으며 正當化를 필요로 하는 自己決定權의 制限이다.[147] 따라서 情報自己決定權은 個人情報를 恣意的으로 처리, 전달하는 것으로부터 뿐만이 아니라, 개인관련정보의 처리(회전)를 통한 위험으로부터도 보호되어야만 한다. 그리고 個人情報들은 구체적이고 事前에 정당한 것으로 언급된 목적들을 위해서만 조사되어도 된다. 個人情報의 처리가 自動的으로 행해지든, 아니든 상관없이 이러한 정보처리는 基本權制限을 위한 法律上 根據命令을 만족시켜야만 한다. 이는 개인관련정보의 처리를 통하여 그의 情報自己決定權이 제한되는 것으로부터 개인의 보호를 지향한다. 따라서 個人情報保護의 대상은 악의적인 잘못된 행위의 억제만이 아니라 이를 넘어서서 개인관련정보의 합법적 처리를 지향한다. 따라서 관련자의 情報自己決定權이 부당하게 제한되지 않는 경우에만 이러한 개인관련정보의 처리는 허용된다. 이렇게 개인이 자기의 정보처리에 관하여 결정할 권리는 개인관련정보가 어떤 방법으로 처리되어도 되는지를 원칙적으로 스스로 결정할 권리를 포함한다. 예를 들어 정보조사에 관한 허용이 다른 것 - 정보처리 - 에 관한 허용을 곧장 의미하는 것은 아니다. 결국 이는 개인관련정보의 모든 처리가 정당화를 필요로 하는 제한이라는 것을 뜻한다. 그러한 제한은 개인관련정보의 조사와 이용에서만 존재하는 것이 아니라 동시에 個人情報 저장 그 자체가 제한이다.[148] 따라서 정보이용과 처리는 분리되어 파악되고 판단되어야만 한다. 예를 들

146) BVerfGE 65, 1/42.

147) Hans-Ulrich Gallwas, Zum Prinzip der Erforderlichkeit im Datenschutzrecht, *Festschrift für Arthur Kaufmann zum 70. Geburtstag*, C. F. Müller, 1993, S. 823면 이하.

148) Hans-Ulrich Gallwas, a.a.O., S. 825.

어 특정한 목적으로 정보를 조사하는 것이 허용되기는 하나 그 기관이 정보처리프로그램이나 개인의 접근권을 충분히 보장하지 않는다면 이러한 個人情報는 저장되어서는 안된다.[149]

1977년 독일에서 제정된 聯邦情報保護法은 정보처리시 남용으로부터 관련자의 보호가치있는 이익침해를 억제하려는 과제만을 명시적으로 규정하였다.[150] 따라서 舊情報保護法(1977)에서 관련자의 보호가치이익은 결국 정보처리남용으로부터만 보호되었다. 결국 舊情報保護法이 정보처리의 남용금지를 목표로 하면서 정보처리의 "합법적인 이용"과 남용인 "예외적으로 금지되는 이용"을 구별해야만 했다. 그러나 새로 개정된 聯邦情報保護法은 개인관련정보의 회전을 통한 情報自己決定權의 侵害로부터 개인을 보호하는 것이 정보보호법의 목적임을 분명히 하였다. 이는 立法者가 결국 개인관련정보처리가 원칙적으로는 금지되고 예외적인 경우에 허용될 수 있다는 정보보호법의 기본원칙을 받아들였다는 것을 의미한다.[151] 따라서 정보처리를 통한 情報自己決定權의 침해가 합법적인지 위법적인지는 결국 정보처리의 목적, 종류 등에 달려 있다. 이것으로부터 정보처리로부터 관련자의 권리에 대한 제한이 존재하는지 그리고 얼마만큼 존재하는지가 결정되어야만 한다. 이 두 가지 문제가 해명되어야만 비로소 정보처리의 목적적합성명령과 정보처리중 가장 온화한 수단을 택하라는 명령 곧 수단적합성명령이 작용할 수 있다.

그런데 우리 나라의 個人情報保護法 제1조에 "이 법은 공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다"고 규정되어 있다. 위에서 설명된 獨逸의 聯邦情報保護法이 개정될 때 분명히 하였던 것처럼 個人情報의 保護를 통하여 情報社會에서 개인의 私生活을 보호하고자 함을 좀 더 확실하게 밝힐 뿐만 아니라 국가를 통한 個人情報의 濫用으로부터만 개인을 보호하는 게 아니라 국가의 個人情報處理 그 자체가 合法的이어야만 한다는 것 또한 인식할 수 있도록 우리 나라의 個人情報保護法에도 명시되어야만 한다.

2. 情報社會에서 保護되어야 할 個人情報의 意味

1) 問題提起

"個人情報"란 단어에서 우선 어떤 것이 "개인적"인 것으로 이해될 수 있는가? 그

149) Hans-Ulrich Gallwas, a.a.O., S. 826.
150) 1977년 연방정보보호법 제1조제1항.
151) Hans-Ulrich Gallwas, a.a.O., S. 822.

리고 어떠한 상황하에서 한 사항이 "개인적"인 것으로 생각될 수 있는가라는 문제가 제기된다. 또는 이러한 질문은 "個人的인" 것과 "私的인" 것간에 구별할 수 있을까라는 매우 철학적이면서 어려운 문제로 바꾸어서 생각해 볼 수 있다. 電子情報處理에서 다루어지는 "個人情報"는 다음과 같은 "개인적"이란 단어와 연결된다 : a) 共同體에 영향을 주지 않거나 관심사가 아닌(관련되지 않는) 문제를 뜻할 수 있다. 예를 들어 "個人的"이라는 이유로 질문에 대답을 개인은 거절할 수 있다. b) 어떤 활동들을 떠맡는 것을 거절할 수 있기 위하여 이에 반대되어 私的이거나 個人的인 것으로 설명되는 어떤 행동들이 있을 수 있다. c) 어떤 對話들은 私的이거나 個人的인 것으로 설명될 수 있다. 동일한 정보가 한 문맥에서는 대단히 私的인 것이나, 다른 문맥에서는 그렇지 않은 것으로 생각될 수도 있다. 그러므로 "個人情報"라는 개념은 다음과 같은 두 가지 요소들을 포함한다. 곧 개인정보란 개념속에서는 정보의 특성 및 이러한 정보의 사용에 관한 개인의 합리적인 기대 모두가 언급되어야만 한다. 다른 말로 하면 어떤 정보가 "개인적", "사적", "민감하다"고 단순히 주장함으로써 자동적으로 이를 그렇게 만들지는 않는다는 것이다. 그래서 "個人情報"란 어떤 개인과 관련되고 그가 내적이거나 민감한 것으로 생각하는 것을 기대하는 게 합리적일지도 모르고, 그래서 이러한 정보를 모으고, 사용하거나 유통하는 것을 허락하지 않거나 최소한 제한하려고 하는 그러한 사실, 대화 또는 의견들로 구성된다고 말할 수 있다.

그렇다면 왜 英美法系에서 프라이버시보호나 신뢰관계보호를 위하여 그동안 발전되었던 基準들이 情報社會에서 個人情報保護를 위한 기준으로서 적합하지 않은지가 우선 설명되어야만 한다. 英美法系의 法院들은 지금까지 많은 判例들을 통하여 개인간 신뢰관계를 위반한 경우로부터 개인의 프라이버시를 보호하고자 노력하였다. 이러한 신뢰관계의 위반으로부터 프라이버시의 침해가 성립되기 위해서는 ① 공개되는 情報 자체가 信賴(秘密)性을 가져야만 한다. 보통 이러한 요구는 공개되는 情報가 公的 財産이나, 公的 知識에 속하지 않는다는 立證에 의하여 만족된다. ② 情報는 信賴義務를 부과하는 상황들 속에서 전달되어야만 한다. 명시적이든 묵시적이든 情報가 제한된 목적을 위하여 믿을만한 사람에게 전달되고 이 사람이 이러한 신뢰를 위반하여 관련정보를 제3자에게 공개했을 때 보통 이러한 權利義務關係가 발생할 것이다. ③ 신뢰의무밑에 있었던 사람에 의하여 권한 없는(또는 권한 밖의) 정보사용이 있어야만 한다. 이러한 신뢰관계를 위반으로 한 訴訟은 주로 營業機密과 관련되나 예술적, 문학적 신뢰관계에 속하는 個人情報도 이러한 범주에 속할 수 있다. 그러나 신뢰관계보호를 위하여 발전된 이러한 기준을 個人情報保護分野에 직

접 적용할 수 없는 첫 번째 이유는 위와 같은 信賴關係違反訴訟이 보통 營業秘密과 같은 상업적이고 경제적인 이익에 초점을 맞추고 있는 반면에 情報社會에서 보호하고자 하는 個人情報는 이러한 情報公開로 인하여 침해되는 것이 관련개인의 人格(또는 私生活)이라는 것이다. 더 나아가서 信賴關係違反을 근거로 한 訴訟에서 제기되는 것처럼 어떤 個人情報가 商業的 性格을 갖는지 또는 단순히 個人的(또는 私的) 性格을 갖는지를 기반으로 하여 정보를 구별하려는 시도는 많은 어려움들을 갖고 있다.[152] 예를 들어 신뢰의무위반여부의 판단은 情報受領人의 입장에 있는 합리적인 사람이 해당정보가 신뢰 속에서 그에게 제공된 것임을 인식하였는지에 따라 판단된다. 이는 營業秘密侵害與否에 관한 판단과 관련해서는 별다른 어려움이 없다.[153] 그러나 個人情報와 관련해서는 어떤 관계(예를 들어 婚姻)속에 있다 할지라도 신뢰의무가 덜 적용될 수 있으며 더 나아가 도대체 어떤 신뢰관계가 전혀 존재하지 않는 곳에서는 私的 事實의 공개를 막을 어떤 수단이 아마도 없을지도 모른다는데에 위 기준을 적용하기 어려운 측면이 있는 것이다.

그렇다면 情報社會에서 個人情報를 보호해야 할 필요성은 바로 情報通信技術의 발달에 따른 위험성으로부터 個人情報를 보호하고자 하는 것임을 인식하고 이에 관한 새로운 기준을 제시해야만 할 것이다.

2) 情報社會에서 個人情報保護의 强化必要性

人口調査判決에서 獨逸의 聯邦憲法法院이 언급한 바에 따르면 情報自己決定權은 개인관련정보의 사용과 공개에 대하여 원칙적으로 개인 스스로 결정할 권리라고 하였다. 결국 이러한 權利는 원칙적으로 그 자신이 스스로 개인관련정보의 공개와 이용에 대하여 결정할 권한을 보장한다고[154] 하면서 누가, 무엇을, 언제 그리고 어떠한 경우에 자기에 관하여 아는지를 시민들이 더 이상 알 수 없는 사회질서 및 이를 가능하게 하는 법질서는 情報自己決定權과 조화되지 못한다고 聯邦憲法法院은 위 판결에서 결정하였다.[155] 이렇게 獨逸의 聯邦憲法法院이 個人情報保護를 강조하게 된 배경에는 바로 電子情報處理라는 조건하에서 개인의 私生活을 특별히 보호해야만 한다는 인식이 깔려 있었다. 다시 말하면 "자기와 관련된 정보들중 어떤 것이 특정한 사회영역 속에서 알려지는지를 충분할 정도로 확실하게 알 수 없는 사람, 의사소통상대방이 무엇을 알고 있는지를 충분히 판단할 수 없는 사람은 독자적인 자기결정

152) Raymond Wacks, ibid., p.106.
153) Raymond Wacks, ibid., p.107.
154) BVerfGE 65, 1(Leitsatz 1).
155) BVerfGE 65, 1/42.

에 따라서 계획하고 결정할 그의 자유가 결정적으로 억제(방해)될 수 있다."[156]는 것이다. 더나아가 聯邦憲法法院은 허용할 수 없는 정보처리를 통한 이러한 情報自己決定權의 침해는 개개인의 개인적인 발현기회뿐만 아니라 公共福利 또한 약화시킬지도 모른다고 언급한다. 왜냐하면 이러한 自己決定은 그 시민들의 행동능력과 협력능력에 바탕을 두고 있는 자유민주적 공동체가 기능할 수 있도록 하는 기본적인 조건이기 때문이라는 것이다.[157] 따라서 獨逸의 聯邦憲法法院에 따르면 정보의 종류가 아니라 그 이용가능성이 결정적이고 自動情報處理라는 조건하에서 중요하지 않은 정보란 더 이상 없다고 확정하였다.[158]

이에 따라서 情報社會에서 개인의 私生活自由는 自己情報에 관한 統制權이라는 情報自己決定權으로 강화되어야만 하는 것이다. 허용되지 않는 정보처리를 통한 情報自己決定權의 侵害는 시민의 개인적 발현기회들을 제한할 뿐만 아니라 公共福利 또한 제한할지도 모른다. 왜냐하면 정치적 의사형성절차에 적극적으로 참여하기 위해서는 모든 市民들이 이러한 절차에 참여할지, 어떻게 그리고 언제 참여할 지에 관하여 스스로 결정할 權利를 갖고 있어야만 하는데 국가의 국민관찰이나 기록(목록)화는 자발적으로 기본권의 행사를 포기하도록 하는 결과를 낳을 수도 있기 때문이다.[159]

3) 個人과 관련되는 모든 情報로 保護의 擴大

그렇다면 여기서 個人關聯情報란 구체적인 사람에 관한 정보를 포함할 뿐만 아니라, 명확히 한 사람에게 귀속시킬 수는 없으나, 다른 정보들의 도움을 받아서 그 동일성을 확인할 수 있는 모든 개개 정보들 또한 포함한다.[160] 예를 들어 단지 개인이름만 생략한 경우(形式的 匿名情報)에 다른 정보를 통하여 한 개인을 여전히 확인할 수 있다면 이러한 정보는 누구에 관한 정보인지를 전혀 알 수 없게 만든 匿名情報가 아니다.[161] 여기서 구체화될 수 있는 個人情報와 匿名情報間 區別이 쉽지 않다는 것을 알 수 있다. 왜냐하면 어떤 하나의 개인정보를 匿名化하더라도 다른 정보의 도움을 받아서 그 개인이 확인될 수 있다면 이러한 과정을 거쳐서 어떤 개인에 관한 정보인지를 구체화할 수 있기 때문이다. 이에 따라서 獨逸의 聯邦憲法法

156) BVerfGE 65, 1/42.
157) BVerfGE 65, 1/43.
158) BVerfGE 65, 1/45.
159) BVerfGE 65, 1/42.
160) BVerfGE 67, 100/144 ; BVerfGE 77, 1/46.
161) Johann Bizer, Forschungsfreiheit und Informationelle Selbstbestimmung, Nomos, 1992, S. 151.

院은 "憲法으로부터 다만 정보의 事實上 匿名化가 요구된다면 이는 情報受信人이나 제3자가 얻고자 하는 정보가치와 관계에서 受忍할 수 없는 정도로 커다란 시간, 돈, 작업과 그외 다른 인력을 쓰는 비용하에서만 재식별할 수 있는 경우로 이해된다."[162]고 결정하였다. 그렇다면 한 개인이 밝혀질지도 모르는 구체화위험성이 組織的이고 技術的인 보호조치를 통하여 광범위하게 줄어들어서 위에서 언급한 요인들의 고려하에서 재식별위험이 관련자에게 기대되어질 수 있는 개인화될 수 있는 (개인과 관련될 수 있는) 정보가 "事實上 匿名化된 情報"이다. 個人化될 수 있는 情報와 事實上 匿名化된 情報 사이의 한계는 따라서 유동적이고 예를 들어 얻고자 하는 정보의 가치 및 受信人 또는 잠재적 침입자의 처분하에 있는 자원을 고려하여서 개개 경우에 구체화될 수 있는 것이다. 그렇다면 충분한 匿名化가 되었는지를 평가할 수 있는 그러한 기준들은 무수히 많으며 완결된 것이 아니다. 예를 들어 이에 관한 판단기준으로는 정보의 形式的인 匿名化, 정보처리기관과 다른 기관간 분리, 조직적 삭제 등이 이에 속하고[163] 또한 事實上 匿名化된 情報의 전달시 逆匿名化에 대한 효과적 예방조치가 행해져야 한다.[164] 또한 재식별위험성을 줄이기 위하여 "事實上 匿名化槪念"은 예를 들어 개인정보의 분리조치와 결합되어야 한다. 그리고 정보를 처리하는 기관의 내부에서 사실상 익명화는 이용목적이 도달된 후에 조사되고 처리된 정보를 삭제하라는 명령을 바꾸지 못한다. 결국 그렇기 때문에 事實上 匿名化된 情報는 언제나 개인관련성의 테두리내에서 움직인다. 다시 말하자면 이는 단지 저장기관으로부터 뿐만이 아니라 또한 受信人 또는 잠재적 침입자에 달려있는 달라진 환경하에서 事實上 匿名化된 情報는 언제든지 다시 개인관련정보가 될 수 있다는 것을 뜻한다. 따라서 立法者는 필요한 보호조치를 명령하는 법규정에서 정보처리기관이 추가적인 組織的이고 技術的인 豫防措置를 취하도록 의무화함으로써 재식별위험을 줄이는 소위 事實上 匿名化된 情報處理를 확보하여야 한다.

4) 絶對的으로 保護되어야만 하는 個人情報의 認定與否

위에서 설명한 것처럼 個人情報란 보통 확인할 수 있는 개인에 관한 정보를 뜻한다. 그러나 이렇게 個人情報란 개념을 넓게 인정함으로써 모든 개인관련정보가 보호될 수 있다는 장점을 갖고 있는 반면에 다른 한편으로는 민감하거나 內的인 정보범주의 특수한 취급을 소홀하게 할 수 있는 가능성이 있을 수 있다. 그렇다면 어떤 정보를 민감하다든지, 기록되어서는 안된다든지 또는 특별한 보호를 받아야 하는

162) BVerfG NJW 1987, S. 2805/2807 ; NJW 1988, S. 962/963..
163) Johann Bizer, a.a.O., S. 154.
164) BVerfGE 65, 1/49.

個人情報로 분류할 필요성이 있는가를 검토한 다음에 이의 필요성이 인정된다면 과연 민감한 정보를 구별할 수 있는 기준을 제시할 수 있는지를 살펴보아야만 한다.

(1) 獨逸의 領域理論

獨逸의 聯邦憲法法院은 "領域理論"에 근거하여 一般的 人格權을 보호하고자 하였다. 그런데 情報自己決定權을 보장하기 위하여 聯邦憲法法院이 情報制限에 관한 한 聯邦憲法法院이 이 領域理論을 포기하였는지에 관하여 그동안 文獻에서 상당히 많이 토론되었다. 먼저 이 문제에 관한 聯邦憲法法院의 입장은 명확하지 않다. 한편으로 聯邦憲法法院은 人口調査判決에서 다음과 같이 결정하였다 : "따라서 진술(언급)의 종류만을 목표로 할 수는 없다. 결정적인 것은 그 利用可能性이다. 이것은 한편으로 조사가 기여하는 목적에 달려있고 또다른 한편으로는 독자적인 처리가능성 및 連結(結合)可能性이라는 情報技術에 달려있다. 이를 통하여 중요하지 않은 정보가 새로운 가치를 가질 수 있다. 그러한 한 自動情報處理라는 조건 하에서는 더 이상 "중요하지 않은" 情報란 없다."[165] 그러나 다른 결정에서 聯邦憲法法院은 이와는 약간 다르게 설명하고 있다 : "다른 사람의 인격영역과 관련된다는 것이 이미 어떤 행위나 정보에 법규정의 접근을 가능하게 하는 사회적 의미를 부여한다. … 따라서 한 事案이 침해할 수 없는 私的 生活形成領域에 속하는지, 또는 구체적인 전제조건 하에서 국가간섭이 가능한 私生活領域에 속하는지는 사회적 의미나 관계가 도대체 존재한다는 것이 아니라 이들이 어떤 종류이며, 얼마만큼 중요한지에 달려있다."[166] 文獻上 多數說은 위 人口調査判決에서 언급된 내용 - ① 더 이상 중요하지 않은 정보는 없다. ② 결정적인 것은 이용가능성이다 - 을 바탕으로 하여 정보와 관련되는 한 聯邦憲法法院이 領域理論으로부터 떠났다고 주장하나 少數說은 여전히 聯邦憲法法院이 領域理論을 고수하고 있다고 주장하면서 위 多數說에 반대한다.[167]

獨逸聯邦憲法法院의 人口調査判決 및 후속판례들을 종합해 볼 때 聯邦憲法法院은 부분적으로는 領域理論을 떠났으나 부분적으로는 이 理論을 고수한다고 말할 수 있다. 우선 聯邦憲法法院에 따르면 어떤 상황이 不可侵의 私生活領域에 속하는지 여부는 그러한 상황이 갖고 있는 사회적 의미나 관계가 도대체 존재하는지에 달려있는 것이 아니라 오히려 그 상황이 내용에 따라 매우 인격적인 성격이며 이것으로부

165) BVerfGE 65, 1/45.

166) BVerfGE 80, 367/374.

167) 이에 관하여 자세한 것은 Max-Emanuel Geis, Der Kernbereich des Persönlichkeitsrechts, JZ 1991, S. 112 이하 ; Rainer Störmer, Zur Verwertbarkeit tagebuchartiger Aufzeichnungen, Jura 1991, S. 17 이하 참조.

터 이 상황이 다른 이의 영역이나 공동체이익에 관련되는 종류와 정도에 달려있다고 하였다.[168] 결국 이러한 판례를 분석해 보면 시민의 어떠한 정보나 행위가 公共領域(Öffentlichkeitssphäre)에 속한다는 이유로 이 영역에서 행해지는 국가의 각종 정보활동으로부터 이들 정보나 행위가 보호받지 못한다는 생각은 人口調査判決에 따라서 더 이상 인정할 수 없으나 절대로 침해할 수 없는 核心領域(Kernbereich)은 계속해서 남아있다는 것을 알 수 있다. 따라서 구체적으로 정보의 조사와 처리가 관련자의 情報自己決定權에 어떤 영향을 가지는지는 정보의 이용맥락을 고려해야만 판단할 수 있다.

(2) 왁스의 기준

왁스는 個人情報를 넓게 개념정의하는 것에 찬성하면서도 더 나아가서 민감한 개인정보의 특별한 보호를 강하게 주장한다. 그러면서 왁스는 個人情報의 민감성을 판단하는 여섯 가지 요소들을 다음과 같이 열거한다 : ①情報主體의 합리적인 기대(예를 들어 性生活情報와 자동차번호간 輕重比較), ②情報受領者(치료정보를 의사에게 주는지, 사용자에게 주는지), ③공개의 범위, ④情報의 壽命, ⑤情報의 수집·사용이나 공개되는 문맥, ⑥情報의 수집·사용이나 공개의 목적.

이러한 요소들에 따라 왁스는 個人情報를 上級의 민감성, 中級의 민감성, 下級의 민감성을 갖는 것으로 나눈다. 여기서 上級의 민감성을 갖는 정보는 일반적으로 病歷이나 性生活과 같이 구체적으로 어떤 사실과 관련되어 개인에 관한 內的인 情報들이다. 이러한 정보에서 개인의 私生活保護論據가 가장 강하게 제기된다고 한다. 그리고 中級의 민감성을 갖는 정보는 이러한 정보가 남용될 때 해악의 잠재성이 매우 높다는 의미에서 상당히 민감한 정보라고 한다. 그리고 마지막으로 下級의 민감성을 갖는 情報는 개인에 관한 傳記的 情報라고 한다.[169] 위에서 행해진 個人情報의 세 가지 분류는 정보의 수집과 사용이 주체에게 주는 중대한 해악의 잠재성정도에 근거한 것으로서 그 민감성에 따라서 보호정도가 달라져야만 한다고 주장한다.

(3) 各國 法律上 個人情報概念

1978년에 제정된 덴마크의 個人情報保護法은 個人情報란 一般人에게 제공하는 것을 허락하지 않는 것이 합리적으로 요구되어질 수 있는 어떤 개인적 정보나 개인, 단체, 결사나 기업에 관한 私的이거나 財政的인 情報라고 규정하면서 더 나아가 여러 상세한 정보형태들을 민감한 것으로 인정하였다. 그래서 個人情報를 사소한

168) BVerfGE 80, 367/374.
169) Raymond Wacks, ibid., p.229.

정보(trivial data), 私的 情報(private data), 민감한 정보(sensitive information)로 구분하여 더 특별한 보호를 받아야 하는 민감한 정보에는 前科記錄, 人種, 宗教, 政治的, 性的 問題가 속한다고 규정하였다.[170] 그리고 1982년에 만들어진 캐나다의 연방프라이버시법 제3조는 個人情報를 "ⓐ 개인의 人種, 國家的 또는 民族的 血統, 피부색, 연령 또는 婚姻與否, ⓑ 개인의 病歷, 前科 또는 雇用前歷에 관한 정보 또는 한 개인과 관련되는 金融去來에 관한 정보, ⓒ 개인에게 부여된 어떤 확인할 수 있는 번호(식별번호), 상징이나 기타, ⓓ 개인의 주소, 지문, 혈액형, ⓔ 개인의 私的 見解와 觀點의 기록, ⓕ 명시적, 묵시적으로 私的이거나 비밀스런 성격을 갖는 書信 및 이에 대한 答信, ⓖ 한 개인과 관련되는 다른 個人情報에서 나타나거나 이름공개 그 자체가 개인에 관한 정보를 공개하게 되는 다른 개인의 관점이나 의견들"이라고 상세하게 규정하였다. 또한 1974년에 제정된 美國의 연방프라이버시법은 個人情報란 "教育, 金融去來, 病歷, 前科나 雇用前歷에 한정되는 게 아니라, 지문이나 음성, 사진처럼 개인에게 속하는 이름, 식별번호나 상징, 기타 다른 확인특징을 포함하는 개인에 관한 정보의 어떤 항목, 수집이나 목록(범주)화"를 포함한다."[171]고 규정하였다.

특히 1984년에 제정된 英國의 情報保護法은 일정한 유형의 정보에 특별한 성격을 인정하고 위 법 제2조제3항 이하에서 이러한 민감한 정보에 따르는 추가적인 보호를 규정하였다. 이는 위 정보보호법을 통하여 보호되는 個人情報가 반드시 민감한 정보일 필요는 없는 반면에, 민감한 정보는 일반 개인정보와는 달리 특별한 취급을 필요로 한다고 규정한 것이다. 그럼에도 불구하고 왁스는 위 情報保護法의 個人情報分類基準에 관하여 다음과 같이 강하게 비판하였다 : 왁스에 따르면 英國의 個人情報保護法은 민감한 個人情報를 적절히 보호하지 못한다는 것이다. 그 첫번째 이유로 왁스는 민감한 정보들의 분류기준에 일관성이 없다는 것이다.[172] 두번째로 위 情報保護法은 手作業으로 처리되는 個人情報를 특별한 보호를 받는 정보범위로부터 배제함으로써 個人情報를 적절히 보호하는 데에 실패하였으며 세 번째로 위 情報保護法에 따르면 國家安保에 관한 정보파일에 의하여 個人情報蒐集이 면책될 수 있다는 것이다. 그렇다면 이는 위 법 제2조제3항 자체에 의하여 가장 민감한 정보로 분류된 個人情報가 國家安保目的으로 수집되고 기록된다며 이에 관한 감독, 접근으로부터 免責될 수 있다는 것을 뜻한다. 게다가 이렇게 免責됨으로써 개

170) 개인기록 등에 관한 법률(The Private Registers, Etc. Act) 1978 제1조제1항.
171) 5 USC 552a(a)(4).
172) Raymond Wacks, ibid., p.239.

인의 접근이 허용되지 않는 정보에 정보보호통제관에 의한 조사나 감독도 허용되지 않기에 더욱 더 문제가 있다는 것이다.[173]

5) 小 結

우리 나라의 個人情報保護法은 個人情報를 보호하고자 한다고 규정하였고 個人情報를 "생존하는 개인에 관한 정보로서 당해정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보를 말한다"고 하였으며 다시 공공기관은 개인의 思想, 信條 등 개인의 基本的 人權을 현저하게 우려할 침해가 있는 個人情報를 수집하여서는 아니된다고 규정하고 있다. 이를 보면 우리 나라의 個人情報保護法이 나름대로 個人情報를 폭넓게 보호하려고 한다는 것을 알 수 있다. 다만 다음과 같이 개정한다면 더욱 더 바람직할 것이라고 보여진다 : 이미 위에서 언급한 것처럼 개인정보보호법의 목적에서 個人情報의 保護를 통하여 "개인의 私生活"을 보호하고자 한다는 것을 구체화할 필요가 있을 것이다. 그리고 두 번째로 개인과 관련되는 그리고 개인을 식별할 수 있는 모든 정보를 個人情報라고 폭넓게 개념정의한 것은 바람직하지만 이러한 個人情報가 필요하지 않은 경우 삭제하거나 가능한 한 초기에 익명화하는 등의 보호조치에 관한 규정이 신설되어야만 한다. 마지막으로 모든 개인관련정보가 보호된다면 그중에서 특히 민감한 정보는 처음부터 蒐集되어서는 안되도록 명시하거나 이를 統制하는 규정을 만들어야만 한다. 특히 우리 나라처럼 지역감정이나 사상시비가 심각한 문제가 될 수 있는 곳에서는 민감한 정보의 조금 더 구체적인 재분류가 필요하며 이에 관하여 더 엄격한 보호조치가 뒤따라야만 한다. 특히 이러한 민감한 정보의 조사나 저장여부는 統制機關을 통하여 감독되어야만 하는 중요한 사항으로 외국에서는 다루어지고 있다. 유감스럽게도 우리 나라의 個人情報保護法에는 이러한 統制機關이 없기 때문에 바로 이러한 민감한 個人情報의 조사와 처리를 감독, 통제한다는 것이 매우 어려운 것이다. 따라서 특히 더 보호되어야만 하는 정보의 재분류 및 이에 관한 통제대책을 수립해야만 한다.

3. 關聯個人의 同意問題

1) 同意의 法的 性格

위에서 설명한 것처럼 情報自己決定權은 자신에 관한 情報의 전달과 이용에 대하

173) Raymond Wacks, ibid., p.240.

여 결정할 권리를 개개인에게 부여한다. 따라서 결국 개인정보의 조사나 처리는 이에 관한 法的 根據가 있는 경우나 관련개인의 同意를 얻은 경우에만 허용된다. 여기서 관련개인의 동의란 情報自己決定權을 침해할지도 모르는 행위를 제3자가 행해도 되는지에 대한 관련자의 결정을 뜻한다.[174] 관련자가 그의 정보처리에 동의하는 한 그는 그의 정보처리와 이용에 관하여 결정한 것이다. 이러한 결과는 情報自己決定權의 내용 및 그 제한에 관하여 중요한 의미를 갖는다 : ①우선 이는 관련자의 意思에 반하거나 意思없이 행해진 情報處理로부터만 해당개인이 보호될 수 있다는 것을 뜻한다. ②결국 관련자의 意思에 반하거나 없는 경우의 정보처리로부터 보호만이 보장된다면 이러한 정보처리에 관한 관련개인의 동의가 존재하는 경우 이미 情報自己決定權의 보호범위와는 관련되지 않는다는 결론이 나온다. 그렇다면 個人情報處理에서 관련자의 同意는 중요한 의미를 갖는다. 왜냐하면 國家는 이미 관련자의 동의를 받음으로써 個人情報處理를 위한 法的 授權을 필요로 하지 않을 수도 있기 때문이다. 따라서 개개인에게 구체적 목적을 위하여 정보처리가 행해진다는 것을 알려야 할 뿐만 아니라, 이에 관한 그의 同意를 필요로 한다. 곧 관련자의 意思에 반하거나 관련자가 모르는 情報處理는 개인의 情報自己決定權을 제한하는 것으로서 이에 관한 正當化를 필요로 하는 制限이다.

2) 同意成立의 條件

위에서 설명한 것처럼 관련개인이 同意하는 경우에 국가의 個人關聯情報處理는 허용된다. 그럼에도 불구하고 이러한 동의가 형식적으로 행해지는 경우에 오히려 개인정보의 無制限的 利用이나 傳達可能性은 더욱 더 커지는 반면에 그 표면적인 合法性은 갖추고 있는 것처럼 보이기에 관련개인의 同意問題는 세심하게 검토해야만 한다. 이에 따라서 情報處理에 관한 개인의 同意가 유효하게 성립하기 위해서는 우선 관련자 스스로가 자신이 행하는 同意의 본질, 의미, 범위에 관하여 인식하고 있어야만 한다. 이는 구체적으로 情報處理의 어떤 단계가 관련되고 어떤 종류의 정보가 어떤 목적으로 처리되고 이용되는지를 관련자가 인식해야만 한다는 것을 말한다. 특히 관련개인의 同意는 원칙적으로 정보처리기간 동안에만 유효하다는 것을 확인할 수 있다.

또한 관련개인의 同意는 언제나 구체적인 情報處理行爲와 통지된 정보처리목적에서만 유효하다는 것에 주의해야 한다.[175] 예를 들어 어떤 연구계획을 위하여 그의

174) Andreas Geiger, Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, NVwZ, 1989, S. 36.

정보가 이용될지를 관련자가 알 수 없는 동의는 유효하게 성립된 것이 아니다. 왜냐하면 이렇게 불충분한 동의를 통하여 본래의 정보처리목적을 벗어난 정보처리가 가능해질 수 있기 때문이다. 이에 따라서 관련자에게 情報處理의 범위, 정보를 받는 受信人의 숫자, 정보처리목적 등이 구체적으로 통지되어야만 한다. 따라서 관련개인이 이러한 情報處理에 효과적으로 동의할 수 있기 위해서는 事前에 그 處理目的에 관하여 통지받아야만 한다. 그런데 관련자가 同意를 부여하거나 거절하기 위해서는 情報處理에 대하여 관련자가 포괄적으로 설명을 들어야만 한다. 왜냐하면 이미 설명된 것처럼 情報自己決定權은 자신의 정보에 관한 처리나 이용을 개인 스스로 인식하고서 統制할 수 있도록 인정하기 때문에 관련자가 同意하기 이전에 이러한 情報處理에 관하여 해당개인이 충분히 설명을 듣고, 납득해야만 하기 때문이다. 그리고 관련자의 同意는 自發的이어야만 한다. 예를 들어 강제나 사기에 의한 同意는 情報自己決定權에 반하며 관련자는 불이익을 두려워할 필요없이 同意를 거절할 수 있어야만 한다. 이에 따라서 國家는 특히 私的 領域에서 형식적인 개인의 同意를 통한 정보처리와 이용의 남용가능성을 방지해야만 한다. 물론 관련개인의 同意는 書面은 물론 口述로도 행사할 수 있다. 다만 書面을 통한 동의요구는 성급한 동의로부터 개개인을 보호하는 기능을 가질 수 있으며 또한 동시에 同意의 書面性을 통하여 정보처리의 필요한 투명성이 보장될 수도 있다.

獨逸의 聯邦情報保護法 제4조제1항에 따르면 同意는 구체적인 정보처리목적에 관해서만 할 수 있으며 목적변경시에는 원래 同意가 유효하지 않다.[176] 게다가 聯邦情報保護法은 同意를 위한 포괄적인 事前說明必要性을 규정하였다.[177] 따라서 個人情報貯藏機關은 관련자에게 어떤 목적으로 정보를 저장하고 그리고 경우에 따라서 제3자에게 정보가 전달될 수 있다는 것에 관하여 관련자에게 설명해야만 한다. 또한 이를 넘어서서 저장기관은 관련자의 요구에 따라 정보제공이 거부된 결과를 통지해 줄 의무를 갖고 있다. 이에 따라서 관련자의 同意는 정보처리 전체가 아니라 개개 경우에 관해서만 허용된다. 예를 들어 이용되는 정보범위가 처리자의 판단에 맡겨지는 白紙委任同意는 허용되지 않는다.[178]

---

175) Christian Rosenbaum, Der grundrechtliche Schutz vor Informationseingriffen, Jura 1988, S. 181.

176) BDSG 제14조제2항, 제28조제2항.

177) BDSG 제4조제2항 1.

178) BDSG 제4조제2항 2에 따르면 동의는 보통 서면(Schriftform)형태를 필요로 한다.

4. 適用範圍의 問題

1) 個人情報保護法과 다른 법률간 관계

憲法上 보장되는 情報自己決定權은 個人情報保護法의 그때 그때 適用範圍로 제한되는 것이 아니라 個人關聯情報에 관한 국가의 정보조사와 처리로부터 일반적으로 보호된다(憲法優位思想).[179] 이에 따라서 個人情報保護法은 그 기능과 본질상 個人情報保護에 관한 範圍具體的인 法律들에 대해서 보충적으로 작용하는 一般的인 個人情報保護法이다.

2) 獨逸에서 情報保護法改正前 論議

인구조사판결 이후에 情報自己決定權이 얼마만큼 적용되어야만 하는지에 관하여 문헌상 토론되었다.

(1) 情報調査의 포함여부

少數說에 의하면 情報調査는 情報自己決定權의 제한으로 판단될 수 없고 따라서 法律상 근거를 필요로 하지 않는다고 한다.[180] 이에 대하여 聯邦憲法法院은 情報自己決定權이 개인관련정보를 조사하는 경우에도 보호됨을 강조한다.[181] 문헌상 通說 또한 情報는 구체적이고 사전에 정당한 것으로 증명된 목적을 위해서만 調査되어야 하며, 그러므로 이러한 개인관련 정보조사도 法律상 근거가 있어야만 허용된다고 주장한다.[182]

(2) 自動化되지 않은 情報處理의 포함여부

少數說에 따르면 情報自己決定權의 보호범위는 自動化된 情報處理로만 제한된다고 한다.[183] 그러나 聯邦憲法法院은 서류 속에 있는 개인관련정보 또는 구체적인 저장수단과는 독립적으로 개인생활사정의 공개에 관한 事案에도 情報自己決定權을 적용한다.[184] 문헌상 통설 또한 情報處理가 自動的이든, 非自動的이든간에 정보처

---

179) BVerfGE 78, 77/84.

180) Scholz/Pitschas, a.a.O., S. 115.

181) BVerfGE 65, 1/43 이하 ; BVerfGE 67, 100/143 ; BVerfGE 77, 1/46 ; BVerfGE 78, 77/84.

182) 예를 들어 *Hans-Ulrich Gallwas*, Verfassungsrechtliche Grundlagen des Datenschutzes, Der Staat 1979, S. 517.

183) *Horst Ehmann*, Zur Zweckbindung privater Datennutzung, RDV 1988, S. 171, 178면.

리는 情報自己決定權을 제한하는 경우에 法律상 근거를 필요로 한다고 주장한다.[185]

(3) 强制的인 調査로 限定與否

少數說은 人口調査判決이 統計目的을 위하여 국가가 시민의 대답을 강제하는 경우에만 적용된다고 주장한다.[186] 그러나 연방헌법법원은 다른 결정에서 情報自己決定權이 강제적인 조사로부터 보호만을 포함하는 것이 아니라고 언급하였으며[187] 문헌상 통설 또한 이러한 입장에 찬성한다.[188]

이러한 논란은 새로 개정된 聯邦情報保護法 및 聯邦憲法法院의 후속판례들을 통하여 다음을 확인할 수 있다 : ① 情報自己決定權은 정보조사로부터 처리를 거쳐 삭제될 때까지 보장된다. ② 이 권리는 自動化되지 않는 정보처리로 확대된다. ③ 이 권리는 강제적이지 않은 조사로부터도 보호된다.

3) 情報調査

情報社會에서 國家를 통한 시민의 감시는 우선 情報調査와 蒐集을 전제로 한다.[189] 발달된 情報通信技術에 근거하여 國家는 광범위하면서도 손쉽게 개인정보를 조사하고 수집할 뿐만 아니라 이러한 정보에 관한 검색이 가능하게 됨으로써 거의 모든 사람에 관하여 아주 자세하고 폭넓게 안다는 것이 가능할 수 있게 된다. 그렇다면 情報社會에서 個人情報保護에 관한 출발점이 바로 情報調査라는 것부터 인식해야만 한다.

獨逸의 聯邦憲法法院 또한 情報社會에서 개인의 情報自己決定權이 情報調査로부터 보호되어야만 한다는 것을 강조하였다.[190] 여기서 情報調査란 어떤 개인에 관한 정보획득을 뜻한다. 情報가 관련자로부터 직접적으로 획득되든 제3자로부터 획득되든 상관없다. 이렇게 情報調査로부터 개인을 보호해야만 한다는 근거는 情報自己決定權으로부터 누가 자기에 관한 個人情報를 획득해도 될지를 스스로 결정할 개개인의 권한이 나온다는 것이다. 그래서 獨逸의 聯邦憲法法院은 情報自己決定權을 强制

184) BVerfGE 67, 100/142 이하 ; BVerfGE 77, 1/46 이하 ; BVerfGE 78, 77/84 이하.
185) Jost-Dietrich Busch, Anmerkung zu BVerfG, DVBl 1984, S. 386. ; Gerhard Groß, a.a.O., S. 166.
186) Uwe Hartleb, a.a.O., S. 105.
187) BVerfGE 67, 100/142 이하.
188) Gerhard Groß, a.a.O., S. 167 ; Scholz/Pitschas, a.a.O., S. 28.
189) James Michael, ibid., p.8.
190) BVerfGE 65, 1/43, 45, 47 ; BVerfGE 67, 100/143 ; BVerfGE 77, 1/46 ; BVerfGE 78, 77/84.

調査로부터만 보호하는 것으로 한정하는 것에 반대하였다.[191] 그렇다면 個人情報를 보호하기 위하여 個人情報保護法의 適用範圍에 情報調査를 포함하는 것은 당연하다. 왜냐하면 정보자기결정권의 보호문제는 이미 情報調査로부터 시작되기 때문이다. 그 다음으로 情報調査는 다음 세 가지 유형으로 나눌 수 있다 : ① 관련자를 통한 調査와 제3자를 통한 조사, ② 공개된 조사와 은밀한 조사, ③ 강제적 조사와 자발적 조사. 우선 强制的 情報調査가 公的 領域에서 특별히 중요한 역할을 맡는다. 예를 들어 刑事訴訟法 등에 따라서 관련자는 이러한 强制的 情報調査를 受忍할 의무를 갖기도 하며 더 나아가서 租稅法領域에서처럼 情報調査에 관련자가 협력해야 할 의무를 갖는 경우도 있다.

獨逸의 聯邦情報保護法에 따르면[192] 情報調査란 어떤 개인에 관한 정보를 획득하는 것이다. 따라서 관련자를 목표로 하는 획득만이 여기서 情報調査라 할 수 있다. 따라서 우연한 획득이나 다른 행동과 결합한 인식은 위 法律의 의미에서 조사가 아니다. 따라서 관련자가 처음부터 匿名인채로 남아있는 그러한 의도된 관찰은 위 법에 규정된 調査槪念에 해당되지 않는다. 따라서 정보획득이란 언제나 개인관련정보의 획득을 목표로 하는 적극적 행위를 전제로 한다.[193] 獨逸의 聯邦情報保護法에 따르면 情報調査는 정보저장기관이 조사하는 個人情報를 필요로 하는 경우에 허용된다.[194] 따라서 情報調査가 해당국가기관의 목적달성을 위하여 객관적으로 적합하고 필요하다는 것이 언제나 입증되어야 한다. 위 법의 다른 규정에 따르면[195] 개인관련정보는 원칙적으로 관련자의 調査를 통하여 획득하여야 한다. 이는 국가기관이 해당개인의 협력을 받아 공개적으로 조사해야 한다는 것을 말한다. 개인의 협력을 받지 않는 조사나 은밀한 조사 또는 제3자를 통한 조사는 다음과 같은 엄격한 전제조건하에서만 허용된다. : ① 관련자의 협력없는 조사는 해당 法律에서 명시적으로 허용되어야만 한다.[196] ② 관련자의 협력없는 조사를 强制的으로 행하는 경우에 또한 해당 法律에 이에 관한 명시적 허용규정이 있어야만 한다[197]. ③ 관련자의 협력없는 조사가 해당기관의 행정과제 때문에 필요한 경우에도 法律에 명시적 허용규정이 있어야만 한다.[198] ④ 이미 한번 조사된 경우나 사소한 질문을 다수에게 하

191) BVerfGE 67, 100/142 ; BVerfGE 67, 157/169.
192) BDSG 제3조제4항
193) BDSG 제3조제4항.
194) BDSG 제13조제1항.
195) BDSG 제13조제2항 1.
196) BDSG 제13조제2항 2.
197) BDSG 제13조제2항 2.
198) BDSG 제13조제2항 2.

는 경우처럼 관련자를 직접 조사하는 비용이 너무 클 경우에 관련자의 협력없는 조사가 허용될 수 있다.[199]. 그리고 관련자의 인식하에서 조사된다면 調査目的을 관련자에게 말해야만 한다.[200] 따라서 관련자의 인식하에서 행해진 情報調査는 해당 개인에게 조사목적이라고 말한 것이 결정적이고, 관련자에게 설명의무가 있는 强制調査의 경우에는 관련자에게 조사목적근거로 언급된 법규정내에서 행해져야만 한다. 이에 반하여 관련자가 情報調査에 관하여 알지 못하는 경우의 調査目的은 公的機關이 情報調査時 근거하는 법규정에 반드시 구체적으로 언급되어 있어야만 한다. 그런데 情報調査時 이에 관한 특별한 법규정이 없는 경우에는 聯邦情報保護法 제13조제1항에 따라서 해당 機關의 행정업무와 사항적 관련성이 있어야만 한다.

결국 이를 요약하면 다음과 같다. 獨逸의 舊聯邦情報保護法(1977)에는 情報調査에 관한 어떤 규정도 두고 있지 않았던 반면에 새로운 聯邦情報保護法(1990)에서 立法者는 저장기관의 情報調査에 관한 法的 根據를 처음으로 만들었다. 그러나 情報調査가 公的 領域 또는 私的 領域에서 행해지느냐에 따라 그 규정의 적용이 다르다. 우선 公的 領域에서 行政機關은 정보처리와 이용뿐만 아니라 또한 情報調査에서도 情報自己決定權을 통하여 제한된다. 이에 따라서 情報調査와 획득은 관련자가 同意하거나 법규정이 허용하는 경우에만 허용된다.[201] 그러므로 情報調査는 연방의 公共機關이 과제이행을 위하여 필요한 경우에만 허용된다.[202] 조사대상이 정당한 과제이행을 위한 경우가 아니라면 情報調査는 허용되지 않는다. 이에 반하여 私的 領域에서는 상황이 다르다. 公的 領域에서와는 달리 私的 領域에서 私人은 법에 반하지 않는한 자기의 목적을 위하여 많은 個人情報를 조사, 수집할 수 있는 권리를 갖고 있다고 말할 수 있다. 따라서 聯邦情報保護法 제28조제1항 2에 따르면 私的 領域에서는 情報는 信義誠實原則에 따라 그리고 법합치적 방법으로 조사되어야만 한다고만 규정함으로써 사인간에는 情報調査가 원칙적으로 禁止되지 않는다는 것을 알 수 있다. 결국 私人은 국가와는 다른 방법으로 基本權에 구속되므로 聯邦情報保護法은 私的 領域에서 情報調査를 위한 비교적 열려진 형성을 獨逸의 聯邦情報保護法은 선택하였던 것이다.

4) 情報의 貯藏, 傳達, 利用

獨逸의 聯邦情報保護法上 情報處理는 다섯 단계 - 貯藏, 變更, 傳達, 削除, 遮斷

199) BDSG 제13조제2항.
200) 제3자를 통한 정보조사 : BDSG 제13조제4항.
201) BDSG 제13조.
202) BDSG 제13조제1항.

- 의 상위개념이다. 情報處理의 가장 일반적인 형태가 情報貯藏이고[203] 情報의 矯正이나 僞造 등으로부터 情報의 추출, 다른 곳에 정보의 삽입을 통하여 새로운 진술이 획득된다면 정보변경이 존재한다.[204] 그리고 情報의 削除는 저장된 개인관련정보를 더이상 재구성하지 못하도록 만드는 것이다.[205] 情報削除의 방법에는 ① 情報나 파일을 파기하거나 ② 해당하는 개인관련정보를 더 이상 재구성할 수 없도록 만드는 것이 있다.

또한 聯邦情報保護法上 傳達槪念[206]은 特定受信人에게 개인관련정보를 알리는 것뿐만 아니라 불특정다수에게 행하는 公的 公示 또는 公告도 포함한다. 왜냐하면 情報自己決定權의 保護는 저장기관으로부터 제3자에게 개인정보를 넘기는 모든 정보전달형태로까지 확대되기 때문에 특정개인에게 하든 公告을 통해서하든 이는 중요하지 않다. 그런데 이러한 情報傳達은 다음과 같은 세 가지 요소로 구성되어 있다 : ① 公告事實, ② 公告對象, ③ 公告의 受信人. 公告對象은 컴퓨터에 저장되었거나 서류 또는 파일에 담긴 정보의 처리를 통하여 획득된 개인관련정보이다. 여기서 公告의 受信人은 해당 정보의 주체가 아니라 언제나 단지 제3자를 말한다.[207] 그러나 公的 機關內에서 情報傳達은 위에서 언급한 情報傳達이 아니라 情報利用의 또 다른 경우이다.[208] 그래서 이러한 公的 機關內에서 情報傳達은 聯邦情報保護法의 정보전달규정의 적용을 받는 게 아니라 情報利用에 속한다. 왜냐하면 前者에 속하는 情報傳達이란 제3자에게 정보를 공개하는 것을 전제로 하기 때문이다. 이러한 제3자는 정보저장기관 밖의 개인이나 機關일 수 있다. 그런데 저장기관내에서 情報傳達의 경우에 유효한 目的拘束原則은 다른 기관에 정보를 전달하는 경우에도 유효해야만 한다. 그 다음으로 情報受信人이 저장기관의 個人情報를 요구함으로써 정보가 전달되는 보통의 경우에는 이러한 정보가 정보수신인의 과제에 속하는지를 검토해야만 한다.[209]

獨逸의 聯邦情報保護法에 따르면[210] 情報利用은 개인관련정보의 변경, 저장, 전달, 삭제를 포함한다. 따라서 정보이용(Verwendung bzw. Nutzung)은 정보의 저장, 변경, 전달, 삭제를 통하여 이미 개념정의되지 못하는 모든 나머지 처리단계

203) "개념정의" BDSG 제3조제5항 1.
204) BDSG 제3조제5항 2.
205) BDSG 제3조제5항 5.
206) BDSG 제3조제5항 3.
207) BDSG 제3조제5항 3.
208) BDSG 제14조제2항.
209) BDSG 제15조제2항 1.
210) BDSG 제3조제5항 1.

를 포함하기 때문에 나머지 처리단계에 대하여 補充的으로 작용하는 기능을 가진다. 이는 저장된 개인관련정보의 내용변경 및 그에 따른 정보의 문맥상실로서 변경뿐만 아니라 모든 다른 형태의 이용과도 관련된다. 따라서 이러한 情報利用槪念에는 정보의 조사, 저장, 전달외에 모든 다른 정보처리단계를 위한 補充機能이 속하게 된다. 그런데 獨逸의 聯邦情報保護法上 利用槪念[211]에 따르면 公的 領域에서는 저장기관내부에서 서류와 파일을 통한 개인관련정보의 모든 다른 이용이 이러한 개념에 속하게 된다. 이러한 정보이용의 사례를 들면 ①처리되는 정보의 評價, ②결정을 위하여 처리되는 정보의 이용, ③저장기관내에서 전달 등이 있다. 따라서 公的 領域에서 제3자를 통한 개인관련정보의 열람은 정보이용이 아니라 정보전달에 속한다. 저장기관과 다른 기관간 구별은 누가 관련자에 대하여 情報保護法上 責任을 지며 언제 정보전달규정이 적용되는지를 결정하기 위하여 중요한 의미를 갖는다.

5) 書類에 適用與否

獨逸의 聯邦憲法法院은 個人情報가 서류속에 담겨 있는지, 個人情報를 어떻게 저장하는지 등과는 상관없이 일반적으로 개인적 생활사정의 공개와 관련되는 경우에 情報自己決定權을 적용하였다.[212] 情報自己決定權의 保護目的이 저장수단의 종류와는 상관없이 자기정보에 대한 개개인의 결정자유를 보호하는데에 있으므로 이러한 넓은 適用範圍는 정당화된다. 여기서 獨逸의 聯邦情報保護法은 파일을 자동화된 파일과 비자동화된 파일로 구별한다.[213] 예를 들어 비디오녹음테이프와 마이크로필름은 서류로 다루어지고 원칙적으로 파일개념에 속하지 않는다. 그러나 사진이나 음성이 디지탈화된 형태로 존재하고 이 속에 개인관련정보가 담겨 있으면 파일개념에 속하게 된다.[214]

6) 適用機關

獨逸의 聯邦情報保護法은 公的 機關과 非公的 機關을 명백히 구별하고 있다. 그래서 公的 機關에서는 파일과 서류에서 정보처리가, 私的 機關에서는 파일합치적 정보처리만이 규제된다. 그리고 聯邦情報保護法 제2조에서 公的, 非公的 機關에 관하여 개념정의하고 있다. 이에 따르면 機關(Behörde)槪念은 행정절차법 1조 4항

211) BDSG 제3조제6항.
212) BVerfGE 67, 100/142 ; BVerfGE 72, 155/170 ; BVerfGE 77, 1/46 ; BVerfGE 78, 77/84 ; BVerfGE 80, 367/373.
213) BDSG 제3조제2항.
214) BDSG 제3조제2항 2, 제3조제3항.

의 개념에 따른 이른바 조직적 기관개념과 연결되어있다. 따라서 機關이란 비독자적인 하부기관이 아니라 국가행정의 독자적 부분을 말한다. 그래서 예를 들어 연방내무성내에서 정보전달은 위 정보보호법 의미에서 다양한 기관간 정보전달이 아니라 정보이용에 관한 것이다. 그런데 獨逸의 聯邦情報保護法에 따르면 국내에서 개인관련정보를 이용하는 모든 非公的 機關[215] 또한 이 法律의 適用範圍下에 있다. 이 聯邦情報保護法上 私的 機關에 관한 규정은 非公的 機關과 公法上 企業이 파일속에서 정보를 처리하거나 그리고 업무나 직업 또는 영업목적을 위하여 처리 또는 이용한다는 전제조건하에서 이런 기관을 통한 개인관련정보의 조사, 처리, 이용으로 확대된다. 다만 立法者는 私的 領域에서 個人情報保護를 원칙적으로 파일관련처리와 이용의 경우로 제한하였다.[216] 또한 聯邦情報保護法에서는 헌법상 보장되는 출판자유와 자유로운 방송의 보도자유를 근거로 輿論媒體에 특별한 지위를 인정하였다. 따라서 聯邦情報保護法 제41조제1항 1에 따라 언론, 영화기업에서 저널리즘이나 출판목적으로 개인관련정보가 처리, 이용되는 경우에는 BDSG 규정중 제5조, 제9조, 제41조제4항만이 적용된다. 다만 이러한 개인관련정보가 언론, 방송문서에서 다른 목적 - 예를 들어 근로자정보 등 - 으로 처리, 이용되는 경우에는 이러한 여론매체의 특권을 누리지 못한다.

7) 小 結

(1) 위에서 설명한 것처럼 個人情報를 보호하기 위해서는 우선 이에 관한 일반적인 원칙과 기준 및 개인의 권리 등을 규정하는 일반적인 個人情報保護法이 정보사회에서 개인정보를 보호하기 위하여 일단 필요하기는 하나 충분한 것은 아니다. 왜냐하면 이러한 法律은 개개 구체적인 분야에 적용하기에는 너무 추상적이고 일반적이기 때문이다.[217] 따라서 일반적인 개인정보보호법의 제정과 더불어 개개 분야별로 특수하게 個人情報를 보호하는 특별한 個人情報保護法들이 동시에 제정되어야만 한다. 바로 이러한 특별법들이 일반적인 個人情報保護法에 규정된 원칙들을 개개 분야에서 구체화시키는 아주 중요한 역할을 하게 된다. 다시 말하면 결국 이러한 특별법을 통하여 일반적인 정보보호원칙들이 개개 분야에서 정확하게 구체화되며 특정 유형의 문제들에 적용되며 개인들이 구체적으로 보호를 받을 수 있게 되는 것이다.[218]

---

215) BDSG 제2조제4항.
216) BDSG 제1조제2항 3, 제21조제1항 2.
217) 이상돈, 형사절차와 정보보호, 한국형사정책연구원, 1996, 91면 이하 참조.
218) 우리나라 개인정보보호법 제3조 : "공공기관의 컴퓨터에 의하여 처리되는 개인정보의 보호

(2) 우리 나라 個人情報保護法에 따르면 個人情報의 "처리"란 "컴퓨터를 사용하여 정보의 입력, 저장, 편집, 검색, 삭제 및 출력 기타 이와 유사한 행위를 하는 것을 말한다."고 하였으며 個人情報의 "보유"란 "개인정보화일을 작성 또는 취득하거나 유지, 관리하는 것을 말한다"고 규정하였다.[219] 그리고 다시 個人情報의 수집에 관한 규정을 두고 있으며[220] 處理情報의 이용 및 제공에 관한 규정을 갖고 있다.[221]

방금 설명한 것처럼 우리 나라 個人情報保護法이 個人情報 및 個人의 私生活을 보호하기 위하여 나름대로 위와 같은 규정들을 두고 있지만 그래도 여전히 정보사회에서 개인정보를 보호하기에는 많은 문제점을 갖고 있다. 이미 언급한 것처럼 우선 情報社會에서 국가를 통한 시민의 감시는 우선 情報調査와 수집을 전제로 한다.[222] 그래서 정보사회에서 個人情報保護에 관한 출발점이 바로 情報調査라는 것을 인식해야만 한다. 여기서 情報調査란 관련자에 대한 정보획득이라고 이해된다. 이는 관련자로부터 직접적으로 획득되든 제3자로부터 획득되든 상관없다. 그렇다면 個人情報를 보호하기 위해서는 個人情報保護法의 適用範圍에 情報調査를 포함하는 것은 당연하다. 따라서 1990년에 개정된 獨逸의 聯邦情報保護法은 情報調査에 관한 규정을 신설하였던 것이다. 이 규정에 따르면[223] 情報調査란 관련자에 관한 정보를 획득하는 것이다. 따라서 관련자를 목표로 하는 획득만이 여기서 情報調査라 할 수 있다. 따라서 우연한 획득이나 다른 행동과 결합한 인식은 위 法律의 의미에서 조사가 아니다. 그러므로 정보획득은 언제나 개인관련정보의 획득을 목표로 하는 적극적 행위를 전제로 한다.[224] 따라서 관련자인식하에서 행해진 情報調査는 해당 개인에게 조사목적이라고 말한 것이 목적으로 결정적이고 설명의무가 있는 强制調査는 관련자에게 조사목적의 근거로 언급된 법규정틀내에서 행해져야만 한다. 이에 반하여 관련자가 알지 못하는 경우 다시 말해서 情報調査에 관하여 알지 못하는 경우의 조사목적은 公的 機關이 情報調査時 근거하는 법규정으로부터만 나오게 된다. 또한 個人情報는 情報調査를 넘어서서 이러한 정보가 저장, 변경, 전달, 이용을 거쳐 삭제될 때까지 보호되어야만 한다. 그래서 개인관련정보는 情報의 調査로부터 처리(저장, 변경, 전달, 삭제, 이용)를 거쳐 익명화될 때까지 보호되도록 개정되어야만 한다. 그리고 우리 나라 個人情報保護法은 公共機關에서 "자동정보처리"로부터

에 관하여는 다른 법률의 특별한 규정이 있는 경우를 제외하고는 이 법이 정한 바에 의한다."

219) 개인정보보호법 제2조.

220) 개인정보보호법 제4조.

221) 개인정보보호법 제10조.

222) James Michael, ibid., p.8.

223) BDSG 제3조제4항

224) BDSG 제3조제4항.

個人情報를 보호하고자 하나 개인의 私生活을 정보사회에서 효율적으로 보호하기 위해서는 자동화된 정보처리뿐만 아니라 서류들도 그 適用範圍에 포함시켜야야만 한다.[225] 따라서 공공기관의 경우에는 원칙적으로 個人情報의 보호가 또한 서류 속의 개인관련정보에까지 확대되도록 개정되어야만 한다. 왜냐하면 정보자기결정권의 보호목적이 저장수단의 종류와는 상관없이 자신의 정보에 관한 개개인의 결정자유를 보호하는데에 있으므로 이러한 넓은 適用範圍는 정당화된다.

5. 規範明確性의 原則

1) 規範明確性의 意味

(1) 人口調査判決에서 規範明確性原則의 강조

法律上 根據는 法治國家的 要求인 "規範明確性"과 "具體性"에 일치해야만 한다.[226] 이것은 관련자가 자기의 개인관련정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 명확하게 인식할 수 있어야만 한다는 것을 뜻한다.[227] 따라서 法律의 規範明確性, 조직적이고 절차법적인 예방책들, 관할기관들의 설명, 관련자의 포괄적인 說明請求權 등을 통하여 누가, 언제, 어디에서 어떤 경우에 자기에 관하여 아는지를 관련 시민이 알 수 있도록 보장되어야 한다. 聯邦憲法法院은 위에서 설명된 人口調査判決에서 이 規範明確性(Normenklarheit)原則을 자세히 설명하였다 : 결국 이러한 規範明確性原則은 개인관련정보를 이용하는 목적이 범위 구체적이고 정확하게 法律上 규정될 것을 요구한다. 그래서 첫 번째로 情報自己決定權의 制限은 (憲法合致的인) 法律上 根據를 필요로 하는데 이러한 제한들은 그 전제조건들과 제한범위가 명확하며, 이를 시민들이 인식할 수 있어야 한다는 法治國家命令에서 나오는 規範明確性을 따라야만 한다.[228] 두 번째로 개인관련정보를 강제로 대답하도록 하기 위해서는 立法者가 이러한 정보의 이용목적을 범위 구체적이고 정확하게 규정하고 이들 정보가 法律에 규정된 목적을 위하여 필요하고 적합하다는 것을 전제로 해야만 한다.[229] 세 번째로 시민은 자기의 정보가 통계목적을 위해서만 사용되지 않을 경우에 구체적으로 어떤 행정집행목적을 위하여 필요로 하는지를 法律規定으로부터 인식할 수 있어야만 한다.[230] 이러한 規範明確性原則을 바탕으로 聯邦

225) 연방정보보호법 제3조제3항, 제27조제2항.
226) Philip Kunig, *Das Rechtsstaatsprinzip*, J.C.B. Mohr, 1986, S. 200 이하.
227) BVerfGE 65, 1/62.
228) BVerfGE 65, 1/44.
229) BVerfGE 65, 1/46.

憲法法院이 구체적으로 人口調査法을 심사하여 다음과 같은 결론에 도달하였다 : a) 원래 통계목적상 필요하다고 하여 시민들이 언급한 개인관련정보들이 申告法(Melderecht)規定에 따라서 광범위하게 관청과 공공기관에 전달될 수 있다는 것을 이 시민들은 인식할 수 없다. 그러므로 이 규정은 規範明確性原則을 침해한다.[231] b) 이러한 개인관련정보가 다른 행정목적들을 위하여 전달될 수 있는지가 人口調査法 제9조제2항으로부터 명확하지도 않을 뿐만 아니라 어떤 구체적이고 명확한 목적들을 위하여 이러한 정보가 필요한지도 인식할 수 없기 때문에 이 제9조 제2항 또한 情報自己決定權을 侵害하였다.[232]

(2) 規範明確性原則의 內容

獨逸의 聯邦憲法法院에 따르면 規範明確性命令은 어떤 법규정으로부터 관련자가 법적 상황을 인식하고 이에 따라 자기의 행동을 준비할 수 있도록 하기 위한 법적 근거를 마련하라는 立法者에 대한 요구로서 표현되었다.[233] 특히 관련자가 법규정으로부터 그의 개인관련정보가 어떤 구체적인 행정목적을 위하여 필요한지를 명백히 인식할 수 있는 것이 포함되어야 한다.[234] 따라서 두개의 서로 다른 목적결합을 통하여 個人情報의 연결을 허용하는 법규정은 관련자의 권리보호를 불확실한 쪽으로 이끌 수 있다.[235] 그렇다면 이러한 규범명확성원칙은 관련자에게 국가정보처리의 투명성을 확실한 정도로 보장한다. 왜냐하면 자신에 관한 정보가 관련자의 同意와 인식없이 처리된다면 국가가 어떠한 목적으로 자신에 관한 정보를 제3자에게 전달하고 처리하여도 되는지를 이 개인은 최소한 법규정에서 추측할 수 있어야 하기 때문이다. 그밖에 법규정을 통하여 관련자가 명확하게 인식할 수 없다면 이 관련자는 자신의 統制權과 說明權을 주장할 수 없다. 또한 規範明確性原則은 규범적용시 행정부가 준수해야만 하는 기준을 형성한다. 行政府에 法的 授權은 그 내용, 목적, 정도가 구체적이어서 개개인이 행정행위의 결과를 예상할 수 있고 계산할 수 있어야만 한다.[236] 따라서 이러한 規範明確性原則은 관련자가 본인의 권리에 관한 어떠한 기본권제한을 참아야만 하는지를 인식하게 한다. 그렇다면 規範明確性과 具體性命令을 실현하는 법규정이란 정보처리 및 이용목적을 정확하게 표현하는 것을 말한

230) BVerfGE 65, 1/62면 이하.
231) BVerfGE 65, 1/65.
232) BVerfGE 65, 1/66.
233) BVerfGE 31, 255/264 ; BVerfGE 45, 400/420 ; BVerfGE 65, 1/64.
234) BVerfGE 65, 1/62.
235) BVerfGE 65, 1/62.
236) BVerfGE 56, 1/12.

다. 곧 비구체적이거나 계속해서 구체화될 수 없는 목적을 위한 개인관련정보의 준비행위는 금지된다.[237] 또한 구체적인 처리목적을 위하여 필요한 이상의 개인관련정보가 처리되어서는 안된다.

결국 이와 같은 설명을 통하여 국가의 정보처리와 이용에 대하여 規範明確性原則이 강조되는 이유를 요약하면 다음과 같다 : ① 자신의 情報自己決定權이 제한되는 관련자에게 법규정 자체에 이용목적의 구체화를 명령하는 바로 규범명확성과 구체성원칙을 통하여 관련자의 동의없이 어떤 목적으로 본인에 관한 정보가 처리되어도 되는지가 투명해진다. ② 立法者가 범위구체적으로 情報利用目的을 규정함으로써 立法者는 법의 목적과 이 법규정을 적용하는 행정의 활동영역을 결정한다. ③ 범위구체적인 규정과 목적구속원칙에 立法者가 구속됨으로써 立法者는 그 내용, 목적, 정도에 따라 법규정을 충분히 구체화해야만 한다. ④ 情報自己決定權의 제한목적이 확정되고 정보이용목적이 인식되는 경우에만 기본권제한에 관한 비례성심사가 비로소 가능해진다.

2) 目的拘束

(1) 槪 念

컴퓨터의 엄청난 저장가능성과 처리능력을 통하여 시민의 완전한 파악과 기록화로 이끌 수 있는 오늘날 정보기술의 위험성을 우리가 파악한다면 개인관련정보의 目的拘束的인 使用과 傳達을 보장하는 것만이 이러한 위험의 실현을 막을 수 있다.[238] 이렇게 요구되는 정보처리의 目的拘束은 한편으로는 處理目標를 확정하고 다른 한편으로는 處理範圍를 한정한다. 이에 따라서 처음부터 명확하게 개념 정의할 수 있는 목적을 위하여 필요한 최소한도의 정보처리만이 허용된다. 이러한 目的拘束要求는 원래 比例性原則으로부터 파생된다.[239] 따라서 이미 法律上 決定된 目的을 위해서만 개인정보는 이용되어도 되며, 목적과는 다른 정보이용 및 처리는 매우 제한된 범위 내에서만 인정되고 法律上 根據를 필요로 하는 새로운 基本權制限이다.[240] 결국 이는 목적구속을 보장하기 위하여 국가기관간 정보전달과 이용에 관한 엄격한 대비책을 필요로 한다는 것을 뜻한다.[241]

---

237) BVerfGE 65, 1/46.

238) Bernhard Hoffmann, *Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes*, Nomos, 1991, S. 21.

239) Philip Kunig, a.a.O., S. 195 이하 참조.

240) Spiros Simitis, Von der Amtshilfe zur Informationshilfe, NJW 1986, S. 2796.

241) BVerfGE 65, 1/46.

(2) 內 容

개인의 情報自己決定權은 개인에 관한 정보가 존재한다는 사실을 통해서가 아니라 통제되지 못하는 정보전달과 원래 조사와 이용목적으로부터 떨어져 나가는 것을 통하여 발생된다. 따라서 정확한 目的決定과 목적구체적인 개인관련정보의 이용 및 전달을 통하여 이러한 위험에 효과적으로 대처할 수 있다. 여기서 우선 정확한 목적설정 및 조사된 개인관련정보의 범위내에 있도록 유지시키는 目的拘束이 모든 합법적 정보처리과정을 위하여 중요한 기준으로 작용하는 원칙이다.[242] 따라서 情報處理의 합법성을 확정지을 수 있기 위해서는 먼저 어떤 목적을 위하여 個人情報가 조사되는 지에 대한 인식을 필요로 한다. 왜냐하면 個人情報가 처리되어도 되는지 여부는 정보처리목적과 情報調査目的이 동일한지라는 판단에 달려있다.[243] 따라서 충분할 정도로 정확하지 않은 그러한 목적을 위해서는 어떤 개인관련정보도 조사, 수집되어서는 안된다. 目的拘束이란 원래 情報調査를 통하여 수집된 個人情報들이 법규정에 따라서 규정된 목적을 위하여 집행된다는 것을 보장하기 위한 것이다. 따라서 정확한 목적결정은 목적구속을 위한 필요한 전제조건으로서 제시된다. 정확한 목적없는 目的拘束이란 공허한 것이다.[244]

3) 委任의 限界

獨逸의 聯邦憲法法院은 人口調査判決에서 규범명확성원칙을 강조하였는 바, 이 원칙은 자신에 대하여 누가 어떤 정보를 처리해도 되는지를 시민이 명백하고 확실하게 인식할 수 있어야만 한다는 것을 뜻한다.[245] 따라서 이는 정보자기결정권의 제한 및 이에 관한 전제조건이 法律 自體로부터 명확하고 시민이 인식할 수 있어야만 한다는 것을 뜻한다. 결국 그렇다면 행정이 개인의 권리를 얼마만큼 제한해도 되는지를 立法者 스스로 규정해야만 한다.[246] 그러나 立法者가 행정과 관련하여 중요한 것을 스스로 결정해야 한다는 것만으로는 충분하지 않고 오히려 추가적으로 해당법규정으로부터 어떤 목적으로 정보가 이용되고 어떤 목적으로 정보가 제3자에게 전달되어도 되는지를 시민들이 명확하게 인식할 수 있어야 한다는 것이 결정적이다. 그렇다면 결국 規範明確性原則은 立法者에게 지속적이고 중요한 요구로 남아

242) Bernhard Hoffmann, a.a.O., S. 26.
243) Bernhard Hoffmann, a.a.O., S. 110.
244) Bernhard Hoffmann, a.a.O., S. 127.
245) Helmut Bäumler, Normenklarheit als Instrument der Transparenz, JZ 1984, S. 361.
246) Helmut Bäumler, a.a.O., S. 363.

있을 것이다. 예를 들어 정보처리에 관한 법규정에서도 一般條項이나 불명확한 법개념이 이용될 수 있는 분야가 언제나 존재할 것이다. 그럼에도 불구하고 이는 사항적으로 가능한 경우 구체적이고 정확한 규정들이 언제나 우선되어야만 한다는 원칙에 반해서는 안된다.[247] 그렇다면 국가정보처리에 관한 法的 根據는 충분히 구체적이어야만 한다. 그리고 이러한 具體性原則은 규범적용시 행정부가 준수해야만 하는 법규정에 반영되어야만 한다. 獨逸聯邦憲法法院의 判例에 따르면 情報自己決定權의 제한은 정당한 공공복리를 지향하는 규범명확성과 구체성원칙요구에 일치하며 범위구체적인 법적 근거를 필요로 한다.[248] 곧 이는 情報自己決定權을 제한하기 위해서는 충분한 법적 근거를 필요로 한다는 것을 뜻한다.[249] 어쨌든 이러한 聯邦憲法法院의 명령은 법규명령의 제정시 고려되어야만 한다. 따라서 立法者는 基本權制限에 관한 권한을 임의대로 법규명령제정자에게 위임하지 못한다.[250] 따라서 ① 문제로 제기된 個人情報의 종류와 범위 ② 처리종류와 특히 貯藏期間의 程度 ③ 생각할 수 있는 이용목적 ④ 구체적인 남용위험 등에 근거하여 立法者가 스스로 결정해야만 하는 사항을 行政府에 위임해서는 안된다.[251]

4) 小 結

個人情報保護에 관한 국제적, 국내적 기준에서 반드시 강조되는 원칙이 바로 規範明確性原則과 目的拘束原則이다. 위에서 이미 설명된 것처럼 規範明確性原則이란 자신에 관한 정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 해당 개인이 명확하게 인식할 수 있어야만 한다는 것을 뜻한다.[252] 따라서 法律의 規範明確性, 조직적이고 절차법적인 예방책들, 관할기관들의 통지의무, 관련자의 포괄적인 說明請求權 등을 통하여 누가, 언제, 어디에서 어떤 경우에 자기에 관하여 아는지를 관련 시민이 알 수 있도록 보장되어야 한다. 특히 관련자가 법규정으로부터 그의 개인관련정보가 어떤 구체적인 행정목적을 위하여 필요한지를 명백히 인식할 수 있어야만 한다.[253] 또한 정보처리의 目的拘束은 한편으로는 처리목표를 확정하고 다른

247) Helmut Bäumler, a.a.O., S. 364.
248) BVerfGE 65, 1/44, 46 ; BVerfGE 67, 100/143 ; BVerfGE 77, 1/46 ; BVerfGE 78, 77/85.
249) BVerfGE 65, 1/44, 46 ; BVerfGE 67, 100/143 ; BVerfGE 77, 1/46 ; BVerfGE 78, 77/85.
250) Christian Rosenbaum, Der grundrechtliche Schutz vor Informationseingriffen, Jura 1988, S. 181.
251) Christian Rosenbaum, a.a.O., S. 182.
252) BVerfGE 65, 1/62.
253) BVerfGE 65, 1/62.

한편으로는 처리범위를 한정한다. 처음부터 명확하게 개념정의할 수 있는 목적을 위하여 필요한 최소한도의 정보처리만이 허용된다. 따라서 이미 法律上 決定된 目的을 위해서만 개인정보는 이용되어도 된다. 목적과는 다른 정보이용 및 처리는 매우 제한된 범위 내에서만 인정되고 法律上 根據를 필요로 하는 새로운 基本權制限이다.[254] 결국 이는 목적구속을 보장하기 위하여 국가기관간 정보전달과 이용에 관한 엄격한 대비책을 필요로 한다는 것을 뜻한다.[255]

우리 나라 個人情報保護法 또한 나름대로 이러한 規範明確性原則과 目的拘束原則을 반영하고 있다. 우선 公共機關은 소관업무를 수행하기 위하여 필요한 범위안에서 個人情報화일을 보유할 수 있으며[256] 보유기관의 長은 당해 개인정보화일의 보유목적이외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니된다고 규정하고 있다.[257]

그러나 우리 나라 個人情報保護法은 지나치게 많은 사항을 대통령령 등에 위임함으로써 바로 규범명확성원칙과 목적구속원칙을 위협하고 있다. 위에서 설명한 것처럼 결국 이러한 規範明確性原則은 개인관련정보를 이용하는 목적이 범위 구체적이고 정확하게 法律上 규정될 것을 요구한다. 그래서 첫 번째로 情報自己決定權의 制限은 (憲法合致的인) 法律上 根據를 필요로 하는데 이러한 제한들은 그 전제조건들과 제한범위가 명확하며, 이를 시민들이 인식할 수 있어야 한다는 法治國家命令에서 나오는 規範明確性을 따라야만 한다.[258] 두 번째로 개인관련정보를 강제로 대답하도록 하기 위해서는 立法者가 이러한 정보의 이용목적을 범위 구체적이고 정확하게 규정하고 이들 정보가 法律에 규정된 목적을 위하여 필요하고 적합하다는 것을 전제로 해야만 한다.[259] 또한 이러한 규범명확성원칙은 규범적용시 行政府가 준수해야만 하는 기준을 형성한다. 行政府에 法的 授權은 그 내용, 목적, 정도가 구체적이어서 개개인이 행정행위의 결과를 예상할 수 있고 계산할 수 있어야만 한다.[260] 이러한 기준에서 볼 때 우리 나라 個人情報保護法이 많은 문제점을 갖고 있음은 다른 나라의 個人情報保護法과 비교하여 명백하게 드러난다. 우선 個人情報保護法의 적용을 배제하는 규정이 너무 많다. 예를 들어 國家安全保障을 목적으로 하여 수집되는 정보에 관해서는 個人情報保護法의 적용을 배제하고 있다. 또한 개인정보화일

254) Spiros Simitis, Von der Amtshilfe zur Informationshilfe, NJW 1986, S. 2796.
255) BVerfGE 65, 1/46.
256) 개인정보보호법 제5조
257) 개인정보보호법 제10조
258) BVerfGE 65, 1/44.
259) BVerfGE 65, 1/46.
260) BVerfGE 56, 1/12.

을 보유하고자 하는 기관은 이를 반드시 총무처장관 등에게 사전통지해야만 한다고 규정하고 있으나 다시 제2항에서 그 적용배제사유를 광범위하게 규정하고 있을 뿐만 아니라 다시 제2항제7에서 적용이 배제되는 사항을 대통령령으로 정할 수 있도록 하였다. 그리고 처리정보의 이용 및 제한이나 처리정보의 열람제한 등에 관한 규정에서도 대통령령에 위임하고 있다. 결국 이렇게 지나친 委任 때문에 시민들은 도대체 본인의 어떤 정보에 관하여 어떤 국가기관이 처리, 저장하고 있는지를 파악하기가 매우 힘들다. 게다가 위 법의 적용이 배제됨으로써 발생할 수 있는 위험성에 관한 별도의 보호대책없이 국가안전보장 등 매우 막연한 사유를 근거로 한 위 법의 적용을 배제하는 것은 個人情報保護를 포기하는 것과 다름없다. 어떤 국가기관에게 위 법이 적용되며, 어떤 사유로 위 법의 적용이 배제되며 그러한 경우에 어떤 보호대책이 확립되어 있는지는 立法者 스스로가 반드시 法律에 규정해야만 하는 사항인데도 이에 관한 규정이 전혀 없거나 이를 行政府에 委任한다는 것은 規範明確性原則에 반한다. 이에 따라서 규범명확성원칙에 근거하여 우리 나라 個人情報保護法의 개정이 매우 시급하다.

6. 關聯個人의 權利保護問題

美國의 프라이버시법에 따르면 해당 개인은 자신에 관한 기록에 접근할 권리 및 잘못된 정보에 대한 수정권을 갖고 있다.[261] 그리고 이러한 요구가 받아들여지지 않았을 경우에 행정기관을 상대로 訴를 제기할 수 있다.[262] 英國의 정보보호법에 따르면 개인은 본인에 관한 자료에 접근하고 이에 관하여 설명을 들을 권리를 갖고 있으며[263] 부정확한 정보를 정정하거나 삭제하도록 요구할 권리를 갖는다.[264] 그리고 부정확한 자료의 공개 등으로 인하여 損害를 입은 경우에 賠償을 받을 권리[265] 및 이러한 요구가 받아들여지지 않을 경우에 法院에 裁判을 청구할 권리가 인정된다.[266] 프랑스의 情報保護法에 따르면 개인은 본인에 관한 정보에 접근할 권리 및 이에 관하여 설명을 들을 권리를 갖고 있으며[267] 본인에 관한 정보가 잘못되었을 경우에 이를 수정하거나 보완, 말소할 것을 요구할 권리를 갖고 있다.[268]

261) 5 U.S.C. 552a(d)
262) 5 U.S.C. 552a(g)
263) 개인정보보호법 제21조
264) 개인정보보호법 제24조
265) 개인정보보호법 제22조, 제23조
266) 개인정보보호법 제25조
267) 개인정보보호법 제35조
268) 개인정보보호법 제36조

獨逸의 정보보호법에 따르면 원칙적으로 관련자는 公的 機關 및 非公的 機關에 대하여 다음과 같은 권리를 가지고 있다 : ① 자신의 정보에 관하여 설명을 요구하는 권리,[269] ② 情報處理에 관하여 통지받을 권리,[270] ③ 잘못된 정보 등에 관하여 삭제를 요구하는 권리,[271] ④ 한 기관이 저장한 정보를 다른 목적을 위하여 전달하는 것을 차단하는 권리.[272] 公的 領域에서 인정되는 이러한 권리는 非公的 領域에서 인정되는 권리와는 많이 다르며 이는 특히 설명청구에서 그렇다. 非公的 領域에서 인정되는 관련자에 대한 通知義務[273]는 公的 機關에서는 존재하지 않으며 公的 機關에서는 관련자를 위한 情報調査와 처리의 투명성이 다르게 보장된다. 곧 公的 機關에서는 연방정보보호법 제13조의 조사규정을 통하여 보통 관련자에게 직접 조사하고 그 관련자에게 조사근거가 통지된다. 따라서 이러한 정보의 저장이나 전달에 대한 추가적 통지를 개인에게 할 필요가 없다. 그리고 公的 領域에서 특별히 인정되는 것은 연방정보보호수임인에게 호소할 관련자의 권리[274]이다. 이러한 권리는 관련자가 주관적으로 자기의 권리가 제한되었다고 생각하는 것만으로도 관련자에게 인정되나 非公的 領域에서는 관련자는 公的 領域에서와 마찬가지로 감독기관에 호소할 수는 있으나 그 권리충돌을 입증해야 하므로 더 높은 설명책임하에 있다. 관련자에게 公的 機關이 보고하도록 하는 목적은 관련자가 자기에 관한 정보처리를 인식한다는데에 있다. 이러한 보고를 통하여 관련자가 정보처기기관에 대하여 항변권을 주장할 수 있다.

그런데 자신에 관한 정보처리부터 개인의 私生活을 보호하고자 한다면 해당 개인에게 이러한 정보처리를 통제할 수 있는 가능성이 인정되어야만 한다. 따라서 우선 관련자의 설명청구[275]를 통하여 자기정보가 어떻게 이용, 처리, 전달되고 있는지를 알 수 있어야만 한다, 그래야만 관련개인은 잘못된 정보처리에 대항할 수 있는 것이다. 따라서 개인의 설명청구는 情報自己決定權을 위한 확대된 권리보호수단이다. 국가기관은 해당 개인에게 본인에 관하여 저장한 정보, 정보처리의 목적, 처리의 법적 근거, 정보출처, 정보수신인 등을 설명해야만 한다.[276] 이에 따라서 정보처리기관이 설명을 부여할 수 있기 위해서는 필요한 정보를 처리할 것을 설명권은 전제

269) BDSG 제19조, 제34조.
270) BDSG 제20조, 제35조.
271) BDSG 제20조, 제35조.
272) BDSG 제20조, 제35조.
273) BDSG 제33조.
274) BDSG 제21조.
275) BDSG 제19조, 제34조.
276) BDSG 제19조.

로 하기 때문에 정보처리를 기록하는 것이 법적으로 의무화되어야만 한다. 그럼에도 불구하고 관련자에게 설명이 거부되는 경우에 그 거부사유가 통지되어야만 하고 이에 대하여 그 개인이 정보보호수임인에게 호소할 수 있는 권리가 정보보호법에 규정되어 있으며 校正權(자기정보에 관한 교정권)과 反論權(자기정보에 관련개인의 의견을 첨부하는 권한) 또한 인정되어야만 한다.[277] 이러한 설명청구는 아직도 모르고 있는 것을 알고자 하는 목적에 기여하는 것으로서 情報保護法上 說明請求는 節次法上 說明請求가 아니라 개인관련정보처리에 대한 독자적이고 實體法的 請求를 뜻한다.[278]

그런데 우리 나라 個人情報保護法에 따르면 관련개인은 본인에 관한 처리정보의 열람을 청구할 수 있고[279] 잘못된 정보에 관하여 정정을 요구할 수 있으며[280] 이러한 요구가 받아들여지지 않을 경우에 行政審判을 청구할 수 있다.[281] 그러나 우리 나라 個人情報保護法은 위에서 설명한 것처럼 개인에게 열람권과 정정권을 인정하기는 하나 이러한 권리를 인정하는 것만으로는 個人情報가 충분히 보장된다고 볼 수 없다. 우선 단순한 열람권만이 아니라 왜 자신에 관한 정보를 조사, 처리, 이용하였는지, 누구에게 어떻게 전달하였는지에 관하여 설명을 들을 권리가 관련개인에게 인정되어야만 한다. 그리고 잘못된 정보에 관하여 정정할 권리뿐만이 아니라 삭제권과 보충권이 인정되어야만 하며 해당 정보의 내용에 관하여 국가기관과 해당 개인간에 의견차이가 있는 경우에 해당 개인의 진술이 이러한 기록에 첨부될 수 있는 기록도 인정되어야만 한다. 그리고 個人情報를 처리하는 기관은 관련자를 위해서뿐만 아니라 통제기관을 위해서도 어떤 방법으로든 이를 기록해야만 한다. 이러한 기록화는 관련자에게 정보처리의 필요한 투명성을 보장하는데 특히 이는 삭제청구와 損害賠償請求時 의미를 가질 수 있다.

물론 자신에 관한 정보에 해당 개인의 접근권이나 설명권은 언제나 절대적으로 보호될 수는 없다. 우리 나라 個人情報保護法도 개인의 학교성적, 치료기록 등의 경우에는 열람을 제한할 수 있도록 규정하고 있다. 또한 우리 나라 법에 의하면 國家安全保障과 관련되는 개인정보파일에는 個人情報保護法의 적용이 배제되며, 그외에도 여러 가지 다양한 사유로 개인의 접근권이 인정되지 않는다. 외국의 경우에도 자신의 정보에 접근할 권리를 인정하지 않는 예외사유를 인정하기는 하지만 이러한

277) BDSG 제19조제6항 이하 참조.
278) Peter M. Huber, Der datenschutzrechtliche Auskunftsanspruch, ThürVBl 1992, S. 121.
279) 개인정보보호법 제12조
280) 개인정보보호법 제14조
281) 개인정보보호법 제15조

경우에 개인의 권리보호를 위한 절차를 규정하거나 統制機關을 통하여 보호되도록 하였다. 그러나 이와는 다르게 우리 나라 법에서는 개인의 설명권이나 접근권이 처음부터 불충분하게 보장되고 있을 뿐만 아니라 이러한 권리가 인정되지 않을 경우에 대비하는 규정이 전혀 없다. 물론 法院을 통하여 해결할 수도 있지만 적어도 정보보호위원회나 統制機關이 이러한 분쟁을 조정하도록 규정하는 것이 바람직하다. 따라서 해당 개인의 권리는 일반적으로가 아니라 구체적이고 매우 한정되어 제한되어야만 하며 개인의 설명권제한이 불가피하다면 이러한 제한이 통제기관의 권한을 통하여 감독되는 것이 요구된다.[282]

7. 自動呼出節次에 관한 問題

1) 問題提起

발전된 現代情報技術을 행정조직이 이용하는 利點으로 무엇보다도 한 기관에서 다른 기관에로 정보의 막히지 않는 흐름을 들 수 있다. 그런데 情報社會에서 個人情報를 보호해야만 한다는 관점에서 본다면 公共行政에서 자동정보처리의 적용못지 않게 정보소지자가 파악하고 있는 정보의 순환이 문제이다. 특히 公的 領域에서 個人情報保護問題가 심각하게 토론되는 것은 특히 컴퓨터연결이나 기록결합을 통하여 행정이 서로 정보를 공유하기 시작하면서부터였다. 컴퓨터연결이나 기록결합시 行政府의 주요 관심사는 個人情報의 보호가 아니라 행정작용의 효율성인 반면에, 시민은 이러한 정보집중이 촉진하는 불필요한 감시를 두려워하게 된다. 따라서 정보사회의 미래를 부정적으로 예견하는 사람들이 가장 우려하는 것중 하나가 바로 보편적인 개인확인번호를 통하여 무수한 個人情報를 통합할 수 있는 中央情報銀行의 출현이다. 실제로 이러한 정보처리가 일반시민들이 거의 인식하지 못하면서 행해지고 있다는데에 가장 큰 위험성이 있는 것이다.

다시 말하면 情報通信技術은 무엇보다도 비용인하, 신속한 결정보장, 행정절차의 합리화에 기여하나 바로 동시에 이러한 기술들이 個人情報의 보호에는 부정적으로 작용할 수도 있는 것이다. 계속해서 발전되는 情報技術로 인하여 시민에 대한 국가의 정보획득은 증가하고 이에 따라서 시민은 국가에 대하여 더욱 더 투명해지는 반면에 반대로 국가의 정보활동은 시민에게 더욱 더 불투명해진다. 게다가 國防이나 外交와 같은 전통적인 과제외에 경제적, 사회적, 환경적 위험과 위기에 대처하기

282) Hermann Heußner, Zur Funktion des Datenschutzes und zur Notwendigkeit bereichsspezifischer Regelungen, Wolfgang Gitter (Hrsg.), *Festschrift für Georg Wannagat*, 1981, S. 189.

위하여 국가는 교육, 환경, 사회, 안보영역에서 새로운 과제들에 부딪히고 있다. 따라서 행정은 그 효율성을 높이기 위하여 모든 가능성을 이용하려고 하는데 특히 情報通信技術의 발전덕분에 행정은 지금까지 분리되었던 많은 작업들을 통합하고 간편하게 정보를 교환하게 된다. 그런데 이러한 행정정보시스템구축은 지금까지 행정시스템과는 전혀 다르다. 왜냐하면 이러한 새로운 행정시스템에서는 서류전달이 아니라 온라인연결을 통하여 정보교환이 행해지고 있기 때문이다. 그렇다면 국가기관 상호간에 과제를 구분하거나 정보협조를 특별히 구할 필요성도 줄어들 것이다. 물론 情報通信技術의 이용을 통하여 국가행정은 많은 과정을 합리화하고 자동화의 도움을 받아 행정은 시민에 봉사하고 처리시간을 줄일 수도 있다. 그러나 이렇게 기대되는 행정자동화를 통하여 국가가 시민을 돕고 지원할 수 있을 뿐만 아니라 시민을 통제하고 조종할 수 있는 가능성 또한 갖게 된다. 예를 들어 통합된 행정시스템에서 기관은 필요한 정보를 언제든 다른 기관이나 중앙컴퓨터로부터 직접 호출할 수 있다. 결국 이렇게 되면 정보처리의 투명성이 보장되기 힘드므로 다시 개인은 정보처리에 관한 설명, 통지, 삭제, 차단에 관한 권리를 주장하기가 힘들어진다. 왜냐하면 정보망형성과 다양한 행정영역통합이 個人情報保護의 기술적, 조직적 보장을 어렵게 하고 통합된 시스템에서 個人情報를 기술적으로 보장하는 어떤 효율적인 안전절차가 여태까지 확인된 적이 없기 때문이다. 결국 이는 발전된 情報通信技術의 투입을 통하여 국가의 의사를 다른 사람에게 강요할 가능성이 높아지는 권력강화적 결과를 낳게 된다. 왜냐하면 정보는 계획, 조정, 통제를 허용하며 다른 사람에게 영향을 주고 자기 목적을 관철할 가능성을 또한 만들기 때문이다. 예를 들어 어떤 사람이 상대방에 관하여 충분한 정보를 가지고 있다면 그는 상대방을 더 잘 감시할 수 있고 그 반응을 더 쉽게 예상할 수 있을 것이다. 그러다보면 그는 상대방을 지배할 수 있게 되며 결국 정보획득 및 사용은 언제나 잠재적 권력행사일 수도 있는 것이다.

그렇다면 이렇게 情報社會의 발달로 인하여 혜택을 누려야만 하는 사람들이 고통을 받지 않도록 하기 위해서는 새로운 기술변화와 발전방향을 한 국가의 기본원칙을 정하여 놓은 헌법과 조화되는 방향으로 이끌어야만 한다. 따라서 새로운 기술시스템이 국민의 基本權을 그 밑바닥에서부터 위협한다면 국가는 이를 허용할 것이 아니라 조정하면서 간섭해야만 하고 基本權의 효력을 미래에서도 보장하기 위하여 기본권에 위협이 될 수 있는 기술발전에 관한 연구가 또한 필요하다.

2) 美國의 컴퓨터연결법[283]

美國에서는 기록연결을 컴퓨터매칭(연결)이라고 한다. 이러한 연결계획은 카터행정부시대에 健康, 敎育, 福祉를 담당하는 부처가 1977년에 만들어지면서 수립되었다. 이러한 카터행정부의 계획을 레이건 행정부가 이어받음으로써 국가의 복지프로그램에서 사기, 낭비, 남용의 소지를 없애려는 구체적인 목표들을 두 行政府는 공유하게 되었다. 그리고 레이건행정부시대에 정부의 통합과 효율성에 관한 대통령자문위원회는 이를 실현하기 위한 운영수단으로서 컴퓨터연결을 강력하게 주장하였다. 그래서 이러한 주장은 레이건행정부시대에 상당한 정도로 반영되었다.[284] 그런데 특히 1980년대 초반에 컴퓨터연결을 통하여 복지수혜에 관한 사기나 낭비를 줄이고자 한 것은 자동적으로 개인의 프라이버시보호를 침해할 수 있다는 측면을 갖고 있었다.

우선 美國의 프라이버시법에 따르면 특정 목적을 위하여 제공된 정보는 관련개인의 同意 없이 다른 목적으로 이용되거나 사용될 수 없다. 그래서 기관간 情報共有는 당사자에 게 이에 관한 通知없이 정보를 공유하는 것을 허용함으로써 개인의 프라이버시를 침해한다. 그런데 1988년까지 이러한 기록연결을 규율하는 법규정은 완비되지 못하였다. 이에 따라서 분야별로 필요한 法律을 만드는 전통에 따라서 의회는 컴퓨터연결을 위한 제정법을 만들고자 하였고, 마침내 1988년 10월 18일 컴퓨터연결과 프라이버시보호법이 제정, 공포되었다. 이 컴퓨터연결과 프라이버시보호법은 제한된 범위, 곧 ① 연방복지계획의 혜택을 받을 수 있는 자격을 확정, 확인하거나, ② 이러한 프로그램 하에서 이미 지불되었거나 만기일이 지난 債務를 공제할 목적으로 전산화된 기록들을 비교하는 데에만 적용되었다. 그래서 위 법은 통계, 검색, 법집행, 외국의 첩보기관, 사회보장목적, 조세목적을 위하여 행해지는 정보연결에는 적용되지 않는다. 다만 새롭게 제정된 이 법은 개인의 프라이버시보호와 정보감시문제에 초점을 맞추기보다는 적정한 行政節次, 행정비용과 복지혜택의 분석을 포함하여 행정부가 실현하려는 목표들을 강조한다. 그러나 어쨌든 이 컴퓨터연결법은 개인의 프라이버시보호를 위하여 관련기관들이 연결기록들을 사용하기 위해서는 해당 기관들의 書面同意를 요구하고, 제안된 연결들에 관하여 연방기록소(Federal Register)에 기록함으로써 시민들에게 事前通知되어야만 한다. 그리고 연결프로그램이나 기록시스템들 속에서 중대한 변화를 확정하거나 만드는 어떤 제

283) 이에 관해서는 卞在玉, 立法紹介 : 1988年의 컴퓨터連結 및 프라이버시保護法, 美國憲法研究 第1號, 1990, 33면 이하 참조.

284) David H. Flaherty, ibid., p.344.

안을 하는 國家機關들은 대통령관할하에 있는 OMB와 상원 및 하원의 감독위원회에 적절한 시간내에 이에 관하여 사전에 통지해야만 한다.[285] 또한 행정기관들은 반대정보들이 그들의 정확성을 유효한 것으로 입증하고 개인들에게 이에 관하여 항변할 기회를 제공하지 않는 한 이러한 반대정보들에 근거하여 어떤 사람에게 수혜를 줄이거나 거절하는 조치를 취할 수 없다.

컴퓨터연결과 프라이버시보호법은 컴퓨터연결프로그램들을 규율하고 통제하려고 하며, 연결프로그램들이 잘 행해진다는 것을 확실히 하기 위하여 컴퓨터연결을 하거나 이에 참여하는 기관들에게 컴퓨터연결을 감독하고 이를 승인하기 위하여 해당기관의 상급관청들로 구성된 情報完全性委員會(Data Integrity Boards)를 만들도록 요구한다. 이러한 개개 위원회는 모든 관련제정법이나 지침의 준수여부를 확실히 감독해야만 하고 비용 - 수혜분석을 행하고, 연결행위들에 관한 연례보고서를 제출해야만 한다.[286] 그런데 1982년 5월 11일 만들어진 컴퓨터연결에 관한 OMB의 지침은 프라이버시법의 이행에 관한 1975년 지침처럼 컴퓨터연결과 프라이버시보호법의 시행을 위하여 만들어진 것이다. 이러한 지침은 프라이버시법상 "일상적인 사용"규정에 근거하여 한 기관으로부터 다른 기관으로 컴퓨터연결을 통하여 個人情報의 전달을 정당화하는 것을 목표로 한다.[287] 그런데 1979년 컴퓨터연결프로그램에 관한 OMB의 지침은 이러한 연결프로그램에 개인의 프라이버시를 침해할 수 있는 위험성이 내재해 있음을 인정하였다. 그러나 이러한 OMB의 지침은 勸告的일뿐 제정법 자체에 따르도록 하는 拘束力을 갖고 있지는 않다. 게다가 이에 관한 1978년 OMB지침은 프라이버시보호를 위하여 컴퓨터연결프로그램이 확인할 수 있는 개인들에 관하여 담고 있는 情報의 내용과 양을 최소해야만 하며 연결프로그램에 따라 허용되는 모든 일상적인 사용들이 가능한 한 구체적이고 제한되어야만 한다는 몇몇 유용한 통제들을 포함하고 있었는데 불행히도 이러한 내용이 1979년 지침에서는 삭제되고 말았다. 더군다나 1982년 만들어진 OMB의 새로운 지침들은 OMB의 감독역할을 축소시키고 말았다. 그럼에도 불구하고 OMB의 이러한 지침 및 프라이버시법상 규정들에 근거하여 국가기관간에 컴퓨터연결이 행해졌다. 결국 이런 현실 속에서 컴퓨터연결을 통하여 어떤 기관이 다른 기관들에게 정보를 제공하면서 여전히 프라이버시법을 준수하는지를 통제한다는 것은 불가능하다. 왜냐하면 프라이버시법의 준수여부를 감독할 어떤 聯邦機關도 존재하지 않기 때문이다.

285) 5 U.S.C. 552a, section 2, 3.
286) 5 U.S.C. 552a, section 2, 3.
287) David H. Flaherty, ibid., p.346.

물론 컴퓨터연결에 관한 1982년 OMB지침은 개인의 프라이버시를 보호하기 위하여 예를 들어서 컴퓨터연결을 통하여 필요한 최소한도의 정보만이 공개되어야 하고, 정보사용에 관한 개인의 서면동의가 있어야만 하고, 기록의 처분과 반환에 관한 통제가 있어야만 하고, 새로운 기록시스템의 설치에 관하여 의회와 OMB에게 통지되어야만 한다는 몇몇 현실적인 대책들을 제시하였다. 문제는 프라이버시법과 OMB의 지침에 규정된 "일상적 사용"이란 규정을 통하여 컴퓨터연결프로그램이 정당화된다는 것이다. 결국 현재 컴퓨터연결프로그램과 이에 관한 통제실무가 부적절하다는 것은 이러한 컴퓨터연결에 내재해 있는 충돌하는 이해관계들을 토론하고 형량할 수 있는 확립된 기구나 광장이 없다는 데에 있다. 컴퓨터연결에 관한 기관내부의 심사나 기준들이 존재하지 않을 뿐만 아니라 프라이버시법하에서 컴퓨터연결에 관하여 OMB에게 공식적으로 통지해야만 하는 시스템이 제대로 작동하고 있지도 않다.[288] 물론 이러한 컴퓨터연결법은 美國에서 현실적으로 수집되는 個人情報의 양을 줄이고 수집되는 정보의 정확성을 확실하게 높이는 좋은 결과도 낳았다. 특히 기록연결에 관한 1982년 OMB지침은 개인프라이버시를 위하여 몇몇 현실적인 보호책들, 예를 들어서 기록연결을 위하여 필요한 최소한도의 정보만이 공개되어야만 하고, 정보사용에 관한 書面同意가 있어야만 하며, 기록의 처분과 반환에 관한 통제가 있어야만 하고, 새로운 기록시스템의 설치에 관하여 의회와 OMB에게 통지되어야만 한다는 요구 등을 포함하고 있다. 그러나 個人情報를 보호하기 위해서는 행정부가 연결하여 검색할 수 있는 데이터베이스의 범위를 통제해야만 하는데 현재 OMB의 지침은 기관내부에서 연결이 아니라 機關間 連結만을 그 대상으로 할 뿐이라는 데에 문제가 있다. 게다가 OMB의 지침은 勸告的일 뿐 제정법 자체에 따르도록 구속할 수 없을 뿐만 아니라 OMB 자체가 충돌하는 이익들을 형량할 수 있는 機關이 아니라는 점이다.[289] 또한 특히 프라이버시법하에서 공적 통지시스템은 대단히 빈약하게 작동하고 있는데다가 컴퓨터연결에 관해서도 機關內部의 審査가 행해지지 않으며 이에 관한 판단기준들이 존재하지도 않는다. 그리고 外部的으로 이러한 기록연결이 프라이버시법과 일치하는지 여부를 판단할 聯邦機關도 없다.[290] 결국 이러한 상황은 프라이버시법 자체의 준수를 감독할 기관이 없다는 결과를 명백하게 지적하는 것이다.

---

288) David H. Flaherty, ibid., p.351.
289) David H. Flaherty, ibid., p.349.
290) David H. Flaherty, ibid., p.348.

3) 獨逸의 法規定

(1) 機關協助와 情報協助

獨逸 基本法 제35조제1항에 따라 聯邦과 州의 모든 機關은 상호간에 法協助와 機關協助下에 있다. 機關協助에서 協助란 찾는 기관의 과제수행을 가능하게 하거나 쉽게 하기 위하여 다른 국가기관에게 문의하고 찾아주는 국가기관의 활동을 말한다. 이에 따라서 獨逸 基本法 제35조제1항은 이에 관한 전제조건을 상세히 규정하지 않고서 원칙적으로만 機關協助義務를 규정한다. 이러한 機關協助制度는 行政節次法, 社會法 등을 통하여 구체화된다.[291] 基本法에 규정된 제35조제1항의 機關協助는 한편으로 聯邦과 州間 國家權力分立이라는 문제에 관한 대답이며[292] 또 다른 한편으로는 聯邦과 州間 關係를 넘어서서 行政機關과 法院間 協助 및 원조권 및 그 의무의 최소정도를 모든 국가기관 상호관계에서 확보하려는 것이다.[293] 따라서 基本法 제35조제1항은 聯邦과 州間 相互援助義務原則만을 표현할 뿐 이를 넘어서서 다른 기관간에 이러한 협조의 전제조건, 범위, 내용, 한계, 수행과 비용 등을 스스로 규정하지 않고 이를 實定法을 통하여 구체화하도록 하였다. 이에 관하여는 行政節次法 제4조에서 제8조까지에 규정되어 있다. 따라서 機關協助는 이를 구하거나 제공하는 기관에게 그 관할이나 권한의 확대나 이동을 뜻하지는 않는다. 그러므로 機關協助는 行政節次法 제4조 이하에 따라 결정된 전제조건과 한계하에서만 적용된다. 그래서 도움요청이 없는 자발적인 機關協助는 법에 특별히 규정되어 있지 않는 한 허용되지 않으며 기관내에서 지원행위는 원칙적으로 機關協助가 아니다. 그러나 한 기관내에서 기관내부간 협조가 무제한적으로 허용되는 것이 아니라 업무에 필요하고 사항적 관할영역속에 있으며 사항결정을 위하여 필요한 경우에 허용된다.[294] 이러한 機關協助는 현존하는 관할과 권한내에서만 보충기능을 가진 것으로서 그 내용에 따라 情報協助뿐만 아니라 다양한 事實行爲 또는 그외 다른 행위도 포함한다. 機關協助는 원칙적으로 개개 경우 청구하고 요청하며 허용되어야만 한다. 따라서 장기간 또는 지속적인 협력이나 공동의 전자정보처리시스템운영은 더이상 기관협조로 표현될 수 없다. 그러한 협력형태를 위해서는 이에 관한 또다른 法的 根據를 필

291) Christian Peter Wilde, Amtshilfe und Datenschutz im Lichte des Volkszählungsurteils des Bundesverfassungsgerichts, BayVBl 1986, S. 230.
292) BVerfGE 7, 183/190 ; BVerfGE 31, 43/46 ; BVerfGE 42, 91/95.
293) BVerfGE 31, 43/46 ; BVerfGE 42, 91/95.
294) Paul Stelkens/H. J. Bonk/Michael Sachs, *Verwaltungsverfahrensgesetz*, C.H. Beck, 1993, S. 242.

요로 한다.[295] 그런데 基本法에 규정된 이러한 機關協助를 통하여 정보를 교환하는 것이 얼마만큼 허용되어야만 하는지가 독일에서 많이 논의되고 있다. 우선 개인의 情報自己決定權保護가 機關協助의 限界를 형성한다. 그래서 聯邦情報保護法 제1조 제5항에서 개인관련정보전달의 경우에는 이 법이 行政節次法보다 우선한다고 규정하였다.

(2) 聯邦情報保護法

1990년에 개정된 獨逸의 聯邦情報保護法은 특히 公的, 非公的 領域에서 自動化된 呼出節次制度에 관한 규정을 도입하였다.[296] 이러한 自動呼出節次에 근거한 전달의 실질적 허용성은 범위구체적인 다른 법규정이나 聯邦情報保護法規定[297]에 따라서 결정된다. 먼저 온라인절차의 작동전에 관련기관은 이러한 절차가 합당한지를 검토해야만 한다. 그리고 이러한 절차에 참여한 기관의 이익을 관련자이익과 형량해야만 한다. 예를 들어 특별히 빠른 안내의 필요성이나 대량전달의 필요성이 존재한다면 절차는 적합하다고 할 수 있다. 온라인호출을 위한 정보준비는 더 이상 전달로 구분되지 않는다. 정보전달은 구체적인 호출 또는 구체적인 열람을 위하여 호출하는 경우에 파악할 수 있다. 개개 호출에 관한 책임은 정보의 受信人에게 있다.[298] 따라서 그는 온라인연결을 통하여 정보를 파악할 정당한 이익을 가지고 있는지를 개개 경우에 검토해야만 한다. 정보전달목적으로 情報를 저장하는 기관은 이에 관한 또 다른 추가의무가 있다.[299] 또한 形式的 節次를 통하여 호출절차의 허용성이 전체적으로 보장되어야만 한다. 이에 따라서 온라인호출제도의 운용전에 구체적인 개별성이 書面으로 확정되어야 한다.[300] : 곧 ① 呼出節次의 원인과 목적, ② 情報受信人, ③ 전달되는 情報의 종류, ④ 情報安全에 관한 技術的·組織的 措置가 확인되어야만 한다. 첩보기관이나 檢察과 같은 영역에서는 해당 관청이 事前에 동의한 경우에만 호출절차제도가 허용된다.[301] 그런데 온라인연결을 통하여 정보를 검색, 저장할 수 있는 자는 저장기관에 그 허가를 물어보는 일없이 언제든지 원하는 정보를 호출할 수 있다. 따라서 그는 스스로 호출필요성을 검사해야만 한다. 이는 매우 위험하므로 이에 관한 방어조치로써 저장기관이 이를 검토할 의무가

295) Paul Stelkens/H. J. Bonk/Michael Sachs, a.a.O., S. 248.
296) BDSG 제10조.
297) BDSG 제4조제2항, 제15조, 제16조, 제17조, 제28조, 제29조.
298) BDSG 제10조제4항 1.
299) BDSG 제28조제2항 4.
300) BDSG 제10조제2항 2.
301) BDSG 제10조제3항.

있다. 예를 들어 이는 호출기록 등을 통하여 실현될 수 있다. 그런데 여기서 自動呼出節次를 통한 개개 호출의 허용성통제는 단지 事後的으로만 가능하며 연결된 기관은 이러한 정보가 필요한지 여부와는 상관없이 파악할 수 있는 모든 정보에 관하여 사실상 영구적으로 처분할 수 있다는 데에 문제가 있다. 따라서 自動呼出節次의 설치가 아니라 개개 경우 구체적인 호출에서 비로소 情報傳達이 파악된다.

4) 우리 나라의 實態와 問題點

모든 國家機關은 그들이 갖고 있는 자료나 정보를 갖고서 그들의 과제를 처리하기에 충분하지 않다면 기관 상호간에 그들의 과제를 이행할 수 있도록 원조해야만 한다. 문제는 이러한 국가기관 상호간 기관협조가 電子情報處理時代에서도 헌법합치적으로 존재할 수 있도록 해야만 한다는 것이다. 결국 정보처리시 요구되는 目的拘束은 한편으로 정보처리목적를 확정하고 다른 한편는 정보처리의 범위를 한정한다. 이에 따라서 필요한 최소한도로 사전에 명백하게 규정된 목적을 위한 정보처리만이 허용된다. 그렇다면 특정기관이 저장하고 있는 정보가 동시에 모든 다른 행정기관의 공통된 정보를 뜻하는 情報統一體란 존재해서는 안된다. 결국 국가기관 상호간에 정보가 전달되는 한 이러한 정보권력분립과 목적구속을 통하여 시민이 이러한 정보전달을 알 수 있도록 그 정보이동과정이 공개되어야 한다. 그렇다면 個人情報保護와 機關協助는 헌법상 충돌관계에 있는 것이 아니라 상호보충한다.[302] 個人情報保護는 광범위하면서 정확한 法律上 根據없는 정보와 자료교환으로부터 시민을 보호한다. 이는 행정이 그 정당한 과제수행을 위하여 필요로 하는 것보다 더 많은 정보교환을 가능하도록 하는 그러한 法律로부터 시민을 보호한다. 그러나 여기서 인식해야 하는 것은 個人情報保護가 국가기관간 정보교환을 전면적으로 금지시키는 것이 아니라 이러한 정보교환이 규정된 범위내에서 필요한만큼만 행해질것을 요구한다는 것이다.

그런데 위에서 언급한 것처럼 우리 나라의 個人情報保護法이 規範明確性原則에서 비추어볼 때 커다란 문제점을 갖고 있는 것처럼 바로 이 자동호출절차부분에서도 그에 못지 않은 문제점을 갖고 있다. 예를 들어 한 新聞記事에 의하면 경찰전산망에 등록된 個人情報가 안기부, 청와대 등과 연결된 단말기를 통해 지난 3년간 1천5백만건이나 조회된 것으로 드러났다고 한다. 특히 안기부, 청와대 등 8개 기관이 자체 단말기를 통해 범죄경력과는 상관없이 주민자료를 조회한 것도 6백10여만건에 이르러 이들 기관이 경찰청 단말기를 다른 목적으로 사용했을 가능성도 크다고

302) Bernhard Schlink, Datenschutz und Amtshilfe, NVwZ 1986, S. 249.

한다.[303] 결국 우리 나라의 個人情報保護法이 1990년대에 제정된 법임에도 불구하고 다른 나라의 "1세대" 法律과 비슷한 이유중 하나가 바로 이렇게 自動呼出節次에 관한 보호규정이 전혀 없다는데에 있다. 이렇게 컴퓨터전산망을 통하여 행정기관들이 원하는 정보를 마음대로 처리, 이용할 경우에 우리 나라 個人情報保護法을 포함하여 정보보호법상 일반적 원칙중 하나인 목적구속원칙과 규범명확성원칙을 준수한다는 것은 처음부터 불가능하다. 왜냐하면 결국 이러한 온라인연결을 통하여 개인이 한 行政機關에게 자신에 관한 정보를 제공하는 것은 모든 국가기관들에게 자신에 관한 정보를 제공하는 것과 똑같기 때문이다. 이렇게 되면 관련개인은 자신의 정보를 누가, 어떤 목적으로, 얼마만큼 처리, 이용, 전달하는지를 파악하고 통제한다는 것은 처음부터 불가능하다. 따라서 個人情報를 保護하기 위하여 가장 시급한 것이 바로 이렇게 컴퓨터의 연결을 통하여 자동적으로 정보를 조회, 처리하는 것을 통제하는 규정을 두어야만 한다는 것이다. 이러한 自動呼出節次로부터 個人情報를 얼마만큼 보호하느냐에 따라서 바로 個人情報保護法의 효율성여부를 판단할 수 있다고 해도 지나친 말이 아니다. 따라서 美國의 경우처럼 자동호출절차에 관한 특별법을 제정하든지, 독일처럼 個人情報保護法內에 이에 관한 규정을 신설해야만 한다. 특히 이러한 自動呼出節次에 관한 규정에서는 呼出節次의 사유와 목적, 情報受領人, 전달되는 정보의 종류 등에 관하여 해당 기관은 書面으로 이를 기록하고 이러한 기록을 정보보호위원회와 같은 통제기관이 감독할 수 있어야만 한다는 내용이 포함되어야만 한다.

第4節 私的 領域에서 個人情報保護

1. 問題提起

오늘날 예를 들어 신용카드회사는 무수한 카드사용자들의 매일 매일 활동들을 파악할 수 있을 뿐만 아니라, 또한 예를 들어 온라인카드를 통하여 특정 시점에서 그들의 위치파악을 가능하게 하는 온라인데이터베이스들을 설치할 수도 있다. 또한 아주 많은 사람들이 물건을 사고 수표나 신용카드로 지불한다. 그런데 現金을 지불하는 경우와는 달리 신용카드를 이용할 경우에는 개인관련정보가 컴퓨터에 저장되며 이러한 정보의 도움을 받아서 신용카드회사는 한편으로 顧客의 信用狀態를 검토할 수 있고 또다른 한편으로 消費者에 관하여 지나칠 정도로 상세하게 파악할 수 있게 된다. 또 작업장에서 증가하는 자동화는 특히 조직되지 않고, 임시직이거나

303) 세계일보 1997.10.16. 30면.

파트타임으로 일하는 노동자들이나 구직자들을 효율적으로 감시할 수 있도록 만든다. 그러나 다른 측면에서 본다면 經營者나 使用者 등이 정보사회에서 올바른 결정과 판단을 내리기 위해서는 많은 정보를 필요로 한다는 것은 더 이상의 설명이 필요없을 것이다. 그렇다면 기업의 효율적인 경영과 운용을 위하여 작업장에 전자정보처리기술을 도입하는 경우에, 이를 근로자의 입장에서 본다면 근로자를 감시하는 것으로 판단되나 기업주의 입장에서 본다면 작업과정을 합리화하기 위하여 불가피한 것으로 생각할 것이다. 또 職員의 전화사용을 컴퓨터를 통하여 기록한다든가, 직원채용시 應募者에게 과연 어떤 질문을 하여서는 안된다거나 어떤 個人情報를 수집해서는 안되는지에 관해서도 많은 논란이 되고 있다. 어쨌든 私的 領域에서 個人情報保護問題는 公的 領域에서 國家를 규율하는 것과 동일한 방법으로 처리하기 힘든 측면들이 많다. 왜냐하면 私人들은 원칙적으로 자유로이 정보를 수집할 권리 및 契約自由에 관한 권리 등을 갖고 있기 때문이다.

2. 私的 情報處理에 관한 論爭

1) 全面的 適用見解

獨逸에서 聯邦憲法法院이 人口調査判決에서 제시한 個人情報保護에 관한 원칙들이 私的 領域에 얼마만큼 적용될 수 있느냐에 관하여 많이 토론되었다. 우선 한편에서는 聯邦憲法法院의 人口調査判決에서 언급된 個人情報保護에 관한 원칙이 처음부터 무차별적으로 私人關係에 적용될 수 있지 않다는 것이 인정된다고 하면서 예를 들어 保險, 勤勞, 信用部門과 같은 私的 領域에서 개개인에 대한 경제적, 사회적 힘의 행사가 문제인한 이러한 영역에서도 情報自己決定權이 보호되어야만 한다고 주장된다.[304] 私的 領域에서 정보를 처리하는 기업에게 헌법상 보장되는 자유와 基本權을 존중해야만 하나 情報處理가 경제적, 사회적 힘의 행사와 관련되면 될수록 개개인을 위한 국가보호의무가 더욱 더 현실적으로 제기된다는 것이다. 따라서 私的 領域에서 個人情報의 남용위험성을 인식한다면 聯邦情報保護法이 公的 領域과 私的 領域을 분리하여 규정할 어떤 근본적인 차이도 존재하지 않는다는 것이다. 다시 말하면 公的 情報處理와 私的 情報處理間 分離는 個人情報保護에 관하여 분열된 모습만을 보일 뿐이라는 것이다. 따라서 오히려 聯邦情報保護法이 公的 領域과 私的 領域을 분리한 것이 비판되기까지 한다. 결국 個人情報를 보호하기 위하여 私的 情報調査에도 위 情報保護法이 적용되어야만 할 뿐만 아니라 情報處理의 目的拘束

304) Otto Mallmann, Zweitgeteilter Datenschutz?, CR 1988, S. 94.

原則은 私的 領域에서도 동일하게 유효해야만 한다는 것이다.[305]

2) 制限的 適用見解

이에 대하여 獨逸의 聯邦憲法法院이 人口調査判決에서 언급한 기본원칙들을 公的 領域에서와 동일한 방법으로 私的 情報處理에도 적용하려는 위와 같은 견해에 대하여 강하게 비판하는 입장 또한 있다. 우선 憲法으로부터 個人情報處理에 관하여 제시되는 원칙을 私法에 그대로 적용하려는 것은 고유한 私法體系를 무시한 것이라는 비판이 제시된다. 公的 領域과 私的 領域에 관하여 제시되는 헌법상 기준이 많이 다르기 때문에 情報自己決定權이 私法關係에서는 변형되어 제한적으로만 적용되어야 한다는 것이다. 예를 들어 현실적으로 私法領域에서 目的拘束原則의 적용은 公法領域에서와 똑같이 강도있게 구체화되지 못하며 모든 이용목적을 정확하게 결정한다는 것도 현실적일 수 없다고 주장한다. 그래서 오히려 위 주장과는 반대로 情報保護法에 公的 領域과 私的 領域이 분리되어 규정되어야 한다고 주장된다.[306] 두번째로 公的 領域에서 요구되는 정보이용의 目的拘束原則을 私的 領域으로까지 확대하는 것은 公的 領域과 私的 領域에서 정보이용의 본질적 차이를 이해하지 못한 것이라고 비판된다. 國家機關이 특정 목적을 수행하기 위하여 권한을 행사할 수 있는 公的 領域에서와는 달리 私的 領域의 경우에는 개개 시민이 반드시 따라야만 하는 목적을 확정하거나 자신의 과제를 제한할 수 있는 그러한 권한의 틀이 존재하지 않는다는 것이다. 다시 말하면 개인은 자기의 생활을 유지하고 권리를 행사하기 위하여 가능한 한 많은 정보를 수집하려 할 것이고 이러한 행동은 헌법상 여러 기본권들(예를 들어 意思의 自由, 職業의 自由, 所有權)을 통하여 보호된다는 것이다.[307] 公的 領域에서 정보이용이 구속되어야만 한다는 目的의 확정은 원칙적으로 해당 국가기관의 과제를 통하여 나오기 때문에 이에 관한 통제가 가능한 반면에 私的 領域에서는 보통 목적의 확정은 契約이나 계약과 유사한 신뢰관계의 공통되는 합의된 목적을 통하여 나오는 바 이러한 계약목적은 여전히 客觀的으로 확정할 수 있는 통일된 목적이 아니라 契約當事者를 통하여 원칙적으로 자유롭게 행해진다.

---

305) Otto Mallmann, a.a.O., S. 97.

306) Wolfgang Zöllner, Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV, 1985, S. 16.

307) Josef Brossette, *Der Wert der Wahrheit im Schatten des Rechts auf informationelle Selbstbestimmung*, Duncker & Humblot, 1991, S. 192.

3. 主要國家의 法制分析

예를 들어 스웨덴이나 프랑스, 영국의 情報保護法은 公的 領域과 私的 領域을 구별하지 않고 情報保護法의 원칙과 규정들이 일반적으로 私的 領域에서도 유효한 것으로 인정하고 있으며 특히 스웨덴의 情報監督委員會와 프랑스의 國家情報處理自由委員會는 私的 領域에서 개인정보파일의 설치에 관하여 허가나 승인을 할 권한을 갖고 있기도 하다. 여기서는 公的 領域과 私的 領域을 분리하여 다루고 있는 美國과 獨逸의 경우를 살펴보기로 한다.

1) 美 國

美國은 전세계에서 가장 먼저 情報社會에서 개인의 私生活이 심각하게 침해될 수 있다는 것을 인식한 나라중 하나에 속한다. 그럼에도 불구하고 美國의 立法府는 개인관련정보를 포괄적으로 보호하는 法律을 제정하지 않았다. 오히려 특정 유형의 정보를 보호하고 신용기록산업과 같은 구체적인 정보집중산업을 규율하는 다양한 法律들이 聯邦이나 州에서 제정되고 있다.[308] 이에 따라서 일반적 형태로 私人의 개인관련정보를 보호하기 위한 聯邦法律은 지금까지 통과되지 않았으며 개별영역을 위한 규정들이 여러 법규정들에 부분적으로 있다.[309]

이에 관한 미국의 法律들을 대략적으로 개괄한다면 먼저 公正信用記錄法(Fair Credit Reporting Act FCRA)[310]은 개인의 信用情報를 다루고 保險 및 健康情報法(the insurance and health information statutes)은 개인의 保險 및 健康情報에 관하여 규율한다. 公正信用記錄法은 통상적으로 제3자에게 消費者에 관한 기록들을 제공할 목적으로 消費者信用에 관한 정보를 수집하거나 평가하는 일에 종사하는 소비자기록기관들에게 여러 가지 의무들을 부과한다.[311] 우선 이러한 개인기록에는 營業的 信用記錄도 포함되지 않고, 조사기관의 요구들에 의하여 준비되는 보험기록에 관한 요구들도 포함되지 않는다. 그리고 위 信用記錄法은 정보주체들에게 정보를 공개할 넓은 의무들을 부과하며 소비자기록기관들은 다음과 같은 요구에 대하여 그 기록을 공개해야만 한다 : ① 이러한 機關이 보유하고 있는 파일들 속에 있는 모든 정보의 내용, ② 訴訟이 관련되지 않는 한 조사기록들의 출처를 제외한 정보에 관한 그외 다른 출처, ③ 6개월 이내 소비자기록을 획득한 사람의 명단[312]

308) Henry H. Perrit Jr., ibid., p.88.
309) Stephan Wilske, Datenschutz in den USA, CR 1993, S. 299.
310) 15 U. S. C. §§ 1681, 1681 a - 1681 t
311) 15 U.S.C. §1681a(f)

이 信用記錄法은 또한 관련자들에게 해당 정보가 정확하지 않다는 이의제기를 허용한다.[313] 이러한 이의제기에 대하여 소비자기록기관은 재조사하고 이의제기된 정보의 현재 상황을 기록하고 이러한 정보가 더 이상 유효하지 않거나 부정확하다면 해당 기관은 정보를 삭제해야만 한다. 정보가 삭제되지 않는다면 관련자에게 100단어를 넘지 않는 한도 내에서 이에 관하여 진술할 권한이 부여되고, 이러한 소비자의 진술은 미래의 보고서에 기록되어야만 한다.[314] 이러한 信用記錄의 사용자들은 위 기록기관의 정보에 근거하여 반대되는 결정을 내릴 때 이러한 기록관련자에게 이를 통지해야만 한다. 관련자의 요구에 따라 위 기록들의 使用者는 신용기록들에 동반되지 않은 반대되는 결정들을 내렸을 때 이에 관한 근거를 관련자에게 公開해야만 한다.[315] 그리고 이 신용기록법은 情報를 받을 권한이 없는 사람이 정보를 받는 경우에 관하여 처벌규정을 두고 있다.[316]

금융기록프라이버시법(Financial Records Privacy Act)은 법에 규정된 경우를 제외하고는 行政機關이 金融記錄들을 획득하는 것을 금지한다.[317] 예외가 인정되는 기관들은 은행을 감독하는 기관, 내국세수입국(Internal Revenue Service) 등이다. 金融記錄들은 금융기관과 소비자간 관계를 담고 있는 금융기관에 의하여 보관되는 기록정보로 개념정의된다. 이러한 기록에는 個人消費者에 관한 기록만이 포함된다. 금융기관이란 은행, 저축은행(savings banks), 受與信組合(savings and loan associations), 信用組合(credit unions), 소비자금융기관, 신용카드발급업자를 포함하는 것으로 개념정의된다.[318] 政府機關은 국가기관이나 공무원, 그 雇傭人을 뜻한다.[319] 消費者는 이러한 정보의 공개에 동의할 수는 있으나, 이러한 정보가 이러한 금융기관의 업무활동조건으로서 공개하도록 요구될 수는 없다.[320] 다만 이러한 기록들이 정당한 법집행을 위하여 구해진다고 믿을 만한 이유가 있거나 이러한 기록의 복사가 소비자를 위한 것이거나 금융기관에 봉사하는 경우에만 행정상 명령이나 소환장에 따라서 이러한 기록들은 공개될 수 있다.[321] 또한 聯邦刑事節次規則에 따른 영장발부를 위하여 이러한 기록들이 획득될 수 있다.[322] 그래서 이러

312) 15 U.S.C. §1681g.
313) §1681i.
314) §1681i(b), (c).
315) §1681m.
316) §1681q, r.
317) 12 U.S.C. §3402.
318) §3401(1).
319) §3401(3).
320) §3401(a), 3404(b).
321) §3405.

한 기록들의 공개는 令狀이나 다른 합법적으로 요구되는 범위를 넘어서는 안된다.

그리고 보험회사나 보험정보의 수집기관들은 이들이 소유하거나 통제하는 保險去來를 위하여 기록한 個人情報를 해당 개인이 이용할 수 있도록 해야만 한다. 이에 따라서 관련개인은 保險會社나 다른 보험정보수집기관들이 갖고 있는 자신에 관한 情報의 公開를 書面으로 요구할 수 있다. 이렇게 關聯個人이 요구하는 경우에 해당 보험회사나 다른 보험정보수집기관들은 보통 30일 이내에 이러한 요구에 응답해야만 한다. 관련개인이 個人情報를 요구할 때 신청자와 보험계약자는 보험회사나 다른 보험정보수집기관들의 기록으로부터 본인에 관한 정보를 수정, 개정, 삭제하도록 요구할 수 있으며 보험회사나 다른 보험정보수집기관들은 30일 이내에 이러한 개인의 요구에 응답해야만 한다. 또한 보험회사나 다른 보험정보수집기관들이 個人情報를 수정, 개정 또는 삭제한다면 해당 개인에게 이에 관하여 書面으로 통지해야만 한다. 보험회사나 다른 보험정보수집기관들이 위에서 언급된 개인의 요구를 거절한다면 개인에게 거절, 거절이유, 이에 관한 개인의 진술권, 심사를 요구할 개인의 권리를 통지해야만 한다. 이러한 陳述權은 개인이 동의하지 않는 정보에 관한 것으로서 보험회사나 다른 보험정보수집기관들은 이를 정리해야만 한다. 이들 會社나 기관이 일단 개인으로부터 진술을 받은 한, 개인자신의 기록들 속에 이렇게 논란이 되는 個人情報에 관한 진술을 기록, 정리하고 이러한 자료를 나중에 살펴보고 접근할 수 있도록 해야만 한다. 논란이 되는 情報를 계속적으로 공개할 때 保險會社나 다른 보험정보수집기관은 논쟁이 되는 문제를 분명하게 확인하고, 이러한 개인의 진술을 공개되는 정보와 함께 제공해야만 한다. 추가로 이들 회사나 기관들은 과거에 이들로부터 해당개인에 관하여 정보를 받은 기관이나 회사들에게 이러한 새로운 陳述을 제공해야만 한다. 일반적으로 保險會社나 다른 보험정보수집기관들은 보험거래와 연결되어 수집되거나 접수된 개인에 관한 정보를 공개할 수 없다. 그러나 이러한 규정은 아주 많은 예외들 밑에 있기 때문에 이러한 예외가 허용되려면 정보의 가능한 受領者 및 어떤 목적으로 정보들이 공개될 수 있는지를 구체화한다. 그리고 정보가 제공되고 어떤 상황에서 정보가 제공되는지를 개인에게 일반적으로 통지해야만 한다. 그리고 공개에 관한 또다른 제한은 해당개인에 의한 승인이다. 일반적으로 保險會社나 보험정보수집기관은 개인에 의하여 공개가 승인된 정보만을 공개할 수 있다.

그외 公正信用請求法(Fair Credit Billing Act 1974), 公正債務徵收法(Fair Debt Collection Practices Act of 1977), 公正信用機會法(Equal Credit Op-

322) §3406.

portunities Act of 1974)은 性, 人種, 年齡 등에 관하여 알 수 있는 어떤 個人情報도 信用情報提供會社는 요구하지 못하도록 규정하고 있고, 電子基金移替法(Electronic Fund Transfer Act of 1978), 金融機關規制 및 利子統制法(Financial Institutions Regulatory and Interest Rate Control Act of 1978), 전자통신프라이버시법(Electronic Communications Privacy Act of 1986)은 원칙적으로 기록과 盜聽으로부터 비공식적 대화내용을 보호한다. 가족교육권 및 프라이버시법(Family Educational Rights and Privacy Act of 1974)은 부모, 成年이 된 학생과 대학생에게 본인에 관한 서류열람권을 부여하고 사전에 관련개인의 書面同意없이는 제3자가 이러한 정보에 접근하지 못하도록 규정하였다.

2) 獨 逸

(1) 聯邦情報保護法

독일에서 1990년에 聯邦情報保護法이 개정된 이후에 非公的 分野에서도 많은 변화가 있었다.[323] 우선 舊聯邦情報保護法(1977)에는 情報調査에 관한 어떤 규정도 없었던 반면에 새로운 聯邦情報保護法(1990)에서 立法者는 저장기관의 情報調査에 관한 法的 根據를 처음으로 만들었다. 그러나 情報調査가 公的 領域 또는 私的 領域에서 행해지느냐에 따라 그 적용이 다르다. 公的 領域에서 情報調査는 연방의 公共機關이 그 과제이행을 위하여 필요한 경우에만 허용된다.[324] 이에 반하여 私的 領域에서 情報調査는 상황이 다르다. 公的 領域에서와는 달리 私人은 법에 반하지 않는 한 자신의 목적을 위하여 많은 個人情報를 조사, 수집할 수 있는 권리를 갖고 있다고 말할 수 있다. 따라서 聯邦情報保護法 제28조제1항 2는 私的 領域에서는 정보는 信義誠實에 따라 그리고 법합치적 방법으로 조사되어야만 한다고 함으로써 私人間에는 情報調査가 원칙적으로 금지되지 않는다고 규정하였다. 非公的 領域에서는 情報調査로부터 저장 또는 이용사이에 目的拘束原則이 적용되지 않는다. 단지 情報를 받은 사람이 정보전달목적에 구속된다.[325] 非公的 機關은 관련자에게 個人情報를 첫번째로 저장[326]할 때 또는 첫번째로 전달[327]하는 경우에 해당 개인에게 통지할 의무를 갖고 있다. 그러나 개인관련정보의 파일합치적 정보처리와 이용에서

---

323) Stefan Walz, Das neue Bundesdatenschutzgesetz, CR 1991, S. 364. 私的 領域이란 개념은 불명확해서 BDSG의 법적 개념으로 사용되지 않았다.
324) BDSG 제13조제1항.
325) BDSG 제28조제4항.
326) BDSG 제33조제1항 1.
327) BDSG 제33조제1항 2.

個人情報가 직업비밀이나 특별한 기관의무 때문에 보호를 받는 경우나[328] 硏究機關을 통하여 처리 또는 이용되거나[329] 오로지 統制目的으로 저장된다면[330] 목적구속에 따라야만 한다. 따라서 이러한 범위내에서는 私的 領域에서도 엄격한 목적구속이 적용된다.

聯邦情報保護法 제1조제2항 2에 따라 非公的 領域에서 個人情報는 파일합치적 저장목적으로 조사되거나 파일속에서 또는 파일로부터 처리되거나 이용되는 경우에만 원칙적으로 보호된다. 따라서 聯邦情報保護法에 따르면 파일합치적으로 이용되는 개인관련정보만이 非公的 領域에서 보호된다. 非公的 領域에서 개인관련정보가 업무합치적으로 처리 또는 이용될 뿐만 아니라 직업적 또는 산업적 목적으로 행해지는 경우에도 聯邦情報保護法이 적용된다. 그래서 業務合致的, 職業的, 産業的이란 개념은 상호보충적으로 작용하며 個人情報의 처리를 규율한다. 聯邦情報保護法은 고유한 업무목적의 이행을 위한 수단으로서 정보이용[331]과 정보전달목적을 위한 업무합치적 정보저장이나 변경[332]을 구별한다. 두 활동간에 구별을 위하여 결정적인 것은 情報處理의 목적결정이다. 요약하면 ① 聯邦情報保護法 제28조의 情報處理와 利用은 병원이나 기업에서처럼 그 정보이용이 고유한 업무목적이행을 위한 수단으로 쓰이는 경우에 적용된다. ② 이에 반하여 聯邦情報保護法 제29조의 情報處理와 이용은 주소록출판처럼 그 이용이 자기 목적을 위하여 행사된다면 적용된다.

그리고 非公的 領域에서는 관련자의 權利를 保護하기 위하여 다층적 통제시스템을 두었다. 이는 ① 內部統制機關인 經營情報保護受任人, ② 集團的 統制機關으로서 經營協議會, ③ 外部統制機關인 國家機關으로 구성되어 있다.[333] 여기서 經營協議會는 勤勞者의 이익을 대표하는 기관으로서 從業員을 보호해야만 하는 과제를 맡는다. 經營組織法(BetrVG)은 우선적으로 근로자 전체이익을 보호하고자 하는 것인 반면에 聯邦情報保護法은 정보처리과정에서 관련개인의 이익을 보호하려고 한다.[334] 그리고 私的 領域에서 활동하는 情報保護受任人은 사용자편도 아니고 경영협의회쪽도 아닌 중립적인 기관으로서 활동한다. 그는 ① 個人情報를 보호하기 위

328) BDSG 제39조.
329) BDSG 제40조.
330) BDSG 제31조.
331) BDSG 제28조
332) BDSG 제29조.
333) BDSG개정시 입법자의 중요한 목적중의 하나가 통제기관지위를 강화하고 그 권한을 확대하는 것이었다(BDSG 제36조, 제38조).
334) Gerhard F. Müller/Michael Wächter, Der Datenschutzbeauftragte(2. Auflage), C.H. Beck, 1991, S. 35.

한 統制를 행할 수 있고, 개선점을 제안하며 관련개인의 설명요구를 지원하기 위하여 정보처리의 범위와 관할에 대하여 검토해야만 한다. ② 또한 그는 개인관련정보처리와 이용의 허용조건에 관하여 검토해야만 한다. 이에 따라서 이러한 情報保護受任人은 情報處理의 담당자와 보관자에게 권고하고 근로자정보에 관한 경영협의시 이에 관하여 협조하기 위하여 정보처리의 적용내용과 이용관계를 파악하고 있어야만 한다. ③ 그리고 個人關聯情報의 처리가 個人情報를 보호하는 쪽으로 개선되도록 해야만 한다. 따라서 예를 들어 情報安全指針을 정하고 법규정에 따른 프로그램 적용을 감독하기 위하여 情報保護受任人은 情報安全技術에 관하여 이해하고 있어야만 한다. 그리고 個人情報를 보호해야만 하는 임무를 情報保護受任人은 위임할 수 없다. 이에 반하여 個人情報를 보호하기 위한 國家機關의 활동영역은 私的 領域 전체와 관련된다.[335] 여기서 국가기관을 통한 감독은 부차적 통제기능을 가질 뿐이고 개인정보보호에 관한 우선적 통제는 저장기관과 情報保護受任人의 과제이다. 이에 따라서 國家機關을 통한 外部統制는 효과적인 自己統制를 대체할 수 없다. 정보저장기관과 정보보호수임인이 충분한 정도로 個人情報를 보호하기 위하여 애쓰는 경우에는 저장기관을 통한 自己統制가 國家機關을 통한 外部統制보다 많은 장점을 갖고 있다 : ① 개개 기업상황의 고려하에서 관련자의 권리에 관한 위험이 인식되고 이에 대한 올바른 예방책이 행해질 수 있으며 ② 통일적인 情報安全槪念이 저장기관의 전체정보처리를 위하여 형성될 수 있다. 이를 통하여 절차투명성, 전체정보처리의 통제가능성이 높아진다. ③ 마지막으로 自己統制를 통하여 個人情報保護의 효율성이 높아진다. 따라서 포괄적일 수 없는 國家機關을 통한 外部統制는 보충적, 엄호적 통제이다.

(2) 遺傳子情報保護問題

個人情報保護에 관한 토론중에서 오늘날 특히 治療情報와 遺傳子情報가 시민들로부터 커다란 주목을 받고 있다. 특히 遺傳子情報는 다음과 같은 두 가지 구체적인 특징을 갖는다 : 우선 첫 번째로 이러한 遺傳子情報는 한 개인 뿐만 아니라 그 가족, 자손과도 관련된다. 두 번째로 遺傳子情報의 사용가능성이 미래에 예측하기 힘들 정도로 확대된다는데에 있다. 따라서 遺傳子情報의 수집, 저장 및 처리는 情報自己決定權을 보호하기 위하여 중요한 많은 문제를 제기한다. 이미 人間遺傳子에 관한 분석절차는 ① 胎兒의 疾病認識, ② 勞動關係의 시작과 종료, ③ 個人疾病에 관한 健康保險 및 生命保險締結, ④ 刑事節次에서 犯人確認, ⑤ 親父確認訴訟 등에서 이용되고 있다. 그런데 이렇게 遺傳子分析이 빈번히 행해짐으로써 개인의 情報

335) 감독기관의 통제권한은 BDSG 38조에 상세하게 규정되어 있다.

自己決定權에 야기하는 특별한 위험성은 우선 이러한 遺傳子情報 자체에 있다. 다시 말하면 遺傳子情報는 개인의 생물학적 생존조건과 관련되며 한 개인에 관하여 더할나위없이 중요한 정보이다. 더나아가서 이러한 遺傳子情報의 인식과 이용을 통하여 관련자에게 심각한 결과를 가져올 수도 있다.[336] 특히 개인의 고유한 遺傳子情報 및 잠재적 건강위험에 관한 인식은 관련자의 심리와 생활형성에 심각한 영향을 줄 수도 있다. 결국 이러한 遺傳子情報는 한 개인의 현재 건강상태뿐만 아니라 미래의 건강상태에 관한 설명도 제공한다. 따라서 遺傳子情報의 이용은 勞動領域에서 雇傭契約을 체결할 때 커다란 의미를 가질 수 있다. 예를 들어 특정한 재료나 원료를 다루는 직장에서 이러한 재료나 원료에 부정적으로 반응하는 應募者를 遺傳子檢査를 통하여 탈락시킬 수도 있다. 遺傳子分析이 갖고 있는 위험성은 개인의 職業選擇自由와만 관련된 것이 아니라 遺傳子分析이 개인의 직업과 관계없이 勤勞者의 일반적인 건강위험상태를 파악할 경우에도 존재한다. 예를 들어 保險會社가 遺傳子分析을 통하여 특정인과 보험계약을 체결하려 하지 않으려는 경우도 생길 수 있다. 遺傳子分析을 통하여 "알 권리(Recht auf Wissen)" 뿐만 아니라 이와는 전혀 다른 새로운 문제제기가 발생한다. 곧 미래에 발생할지도 모르는 질병을 초기에 알아야 할지에 대하여 본인이 스스로 결정할 가능성을 개개인에게 인정하는 "모를 권리(Recht auf Nichtwissen)" 문제가 바로 제기되는 것이다. 이미 여러번 설명한 것처럼 情報社會에서 개인의 私生活自由는 자신의 情報에 관한 處分權을 해당 개인이 행사할 수 있는지에 달려있다. 따라서 遺傳子分析問題는 개인의 情報自己決定權을 보호하기 위하여 새롭게 대두되는 분야이다. 왜냐하면 遺傳子分析은 새롭고 특별히 민감한 정보의 처리에 관한 것이기 때문이며 遺傳子分析은 개인관련정보의 조사 및 이용과 불가분적으로 결합되어 있기 때문이다. 어쨌든 앞으로 刑事節次, 勞動關係, 保險分野 등에서 遺傳子分析이 더욱 더 활발해질 것은 분명하다. 이에 따라서 憲法上 保障되는 情報自己決定權이 침해되거나 높은 정도로 위협받게 된다는 것 또한 확실하다.[337] 따라서 遺傳子分析을 통하여 情報自己決定權이 침해되지 않도록 보호해야만 한다. 곧 어떤 전제조건과 목적하에서 遺傳子情報가 처리되어야만 하며 누가 이를 다루어도 되는지, 遺傳子情報의 이러한 목적구속이 보장될 수 있는지에 대하여 가능한 한 초기에 대응하는 것이 필요하다. 일단 遺傳子分析을 통하여 획득된 정보는 개인관련정보이며 파일로 처리되는 한 聯邦과 州의 情報保護法이 이에 적용된다.[338] 또한 勤勞者에 관한 健康診斷은 현재 건강진단으로 한정되어

336) 고용거부, 직업상실, 계약체결부인 등.

337) Rita Wellbrock, Genomanalysen und das informationelle Selbstbestimmungsrecht, CR 1989, S. 204.

야지 미래질병의 진단으로까지 확대되어서는 안된다.[339]

(3) 勤勞者의 情報保護

오늘날 전자정보처리를 설치하지 않은 企業은 없다. 이들은 事務自動化뿐만 아니라 개인정보시스템과 경영정보시스템도 설치운영하고 있다. 그런데 이러한 정보시스템을 통하여 使用者는 ① 從業員을 효율적으로 관리할 수 있으며, ② 다른 종업원과 비교가 매우 쉬워지며, ③ 종업원의 성취도에 관한 기준 및 판단설정이 매우 쉬워지게 된다. 또한 이러한 인사정보시스템은 人事行政, 人事指導, 人事計劃을 위하여 설치되는데 이 시스템속에는 구체적 작업장소와 관련된 요구사항과 노동기준 등이 포함된다. 결국 이는 근로자의 행동과 성취도를 능력별로 평가한다는 적극적 의미를 갖기도 하지만 결국 근로자를 감시한다는 부정적 의미 또한 갖고 있음을 부인할 수 없다. 더군다나 모든 영역으로부터 저장된 근로자정보의 연결이 가능해짐으로써 後者의 可能性은 더욱 더 커진다.

獨逸에서 勤勞者情報는 두 가지 방법으로 보호된다. ① 使用者가 勤勞者와 관계에서 준수해야만 하는 聯邦情報保護法規定을 통하여 ② 賃金契約, 雇傭協商 등에서 근로자의 정보처리에 관한 허용규정[340]과 경영협의회 및 인사협의회(Betriebsrat und Personalrat)을 통하여.

a) 聯邦情報保護法을 통한 保護

勤勞者의 個人情報가 보호받기 위해서는 우선 이러한 정보가 다른 근로자 및 會社의 외부자들로부터 차단되어 처리되어야만 한다는 것에 우선 중요한 의미가 속한다. 聯邦情報保護法이 구체적으로 근로자의 個人情報를 보호하기 위하여 제정되지는 않았다 할지라도 오늘날 이 法은 근로관계에서도 중요한 역할을 한다. 따라서 여러 법들에서 근로자에게 인정되는 권리외에도 聯邦情報保護法에 따른 권리들이 이들에게 추가된다. 우선 公的 機關에 근로자에 관한 정보를 전달하는 것은 명확한 법규정을 근거로 해서만 허용된다. 그러나 勤勞者情報를 經營協議會에 전달하는 것은 저장기관내에서 전달로써 聯邦情報保護法上 제3자에게 전달이 아니다. 다만 勞動組合員의 情報를 제3자에게 전달하는 것은 이에 관한 法的 根據를 필요로 하고 關聯組合員의 書面同意를 필요로 한다. 그리고 經營協議會도 聯邦情報保護法 제5조에 따르는 情報秘密義務를 갖고 있다. 勤勞者는 聯邦情報保護法 제34조에 근거하여 雇用主에 대하여 본인에 관한 정보와 그 정보의 또 다른 운명에 관하여 통지할 것

338) Rita Wellbrock, a.a.O., S. 205.
339) Rita Wellbrock, a.a.O., S. 208.
340) BDSG 제4조제1항.

을 요구할 수 있다. 이러한 설명요구의 대상으로는 정보출처, 情報受信人, 입력목적 등이 있다. 여기서 정보출처란 정보를 제공한 사람이나 기관을 말한다. 情報受信人은 과거에 정보가 전달된 모든 사람과 기관을 말한다. 저장목적에는 일반적인 이용맥락뿐만 아니라 이용프로그램도 속한다. 그런데 經營組織法 제83조제1항에 따르면 從業員은 그에 관한 인사서류를 열람할 권리를 갖고 있다. 이 규정이 충분한한 聯邦情報保護法規定에 우선한다.[341] 여기서 인사서류에는 근로관계에 잠재적으로 영향을 미칠 수 있는 개별근로자와 관련된 모든 정보가 속한다.[342]

b) 經營組織法을 통한 보호

經營組織法(BetrVG) 제80조제2항 1에 따르면 經營協議會는 雇用主에게 勤勞者의 개인관련정보의 모든 처리형태에 대하여 적절하고 포괄적으로 설명해 줄 것을 요구할 권리를 가진다.[343] 또한 個人情報를 보호하기 위하여 經營協議會가 영향을 줄 수 있는 가능성은 새로운 정보기술계획수립 및 도입시 使用者가 經營協議會에 통지하도록 규정한 經營組織法(BetrVG) 제90조로부터 나온다. 이 규정에 관한 聯邦勞動法院의 判例에 따르면 雇用主가 이러한 정보기술계획을 수립할 때 감시를 의도했는지에 달려있는 게 아니라 새로 도입한 정보기술이 勤勞者를 감시하기에 적당하다는 것으로 충분하다고 결정하였다. 따라서 勤勞者에 대한 감시위험만으로 충분하며 情報調査나 처리중 어느 한 단계가 자동적으로 행해지면 족하다는 것이다.

經營組織法에 관한 聯邦勞動法院의 判例를 근로자의 정보보호에 관한 관점에서 본다면 이는 넓은 의미의 정보보호에 관한 것이다. 우선 이러한 判例는 연방정보보호법규정의 적용과 해석에 관한 것이 아니라 종업원정보를 雇用主가 정보기술을 통하여 처리할 때 이에 관여하는 經營協議會의 參與權에 관한 것이다. 따라서 이에 관한 聯邦勞動法院의 判例에서는 經營協議會가 소위 정보기술적 감시에 관하여 공동결정해야만 하는 經營組織法(BetrVG) 제87조제1항 Nr. 6의 해석과 적용이 그 핵심을 이룬다. 그리고 또한 經營組織法 제80조제1항이 근로자의 정보보호와 관련되어 언급될 수 있다. 왜냐하면 1987년 3월 17일 결정에서 聯邦勞動法院은[344] 연방정보보호법이 또한 근로자정보에 관한 보호법이라고 명시적으로 강조했기 때문이다. 이 判例에서 聯邦勞動法院은 계속해서 經營組織法 제80조제2항제1절에 따라 雇用主는 勤勞者의 개인관련정보를 처리하는 모든 형태에 관하여 經營協議會에게

341) BDSG 제1조제4항 1.

342) 응모서류, 월급계산 등. 열람이란 근로자가 받은 정보를 사실상 이해할 수 있는 것만을 말할 수 있다. 따라서 컴퓨터용어 등과 같은 전문용어는 설명되어야만 한다.

343) BAG, BB 1987, S. 1807.

344) BB 1987, 1806 ff.

포괄적으로 통지해야 할 의무가 있다고 결정하였다.

이에 따라서 使用者는 근로자의 사생활을 침해해서는 안되는 것으로까지 확대된다. 그래서 예를 들어 應募者에 대한 使用者의 質問權은 고용관계와 정당한 목적관련속에 있는 그러한 情報調査로 한정되어야만 한다. 따라서 근로관계에서 근로자의 個人情報保護는 구체적인 勞動保護權으로서 기능한다. 다만 聯邦情報保護法은 私的領域에서 근로자의 개인권리를 보호하고자 하는 반면에 經營組織法(BetrVG)은 근로자의 이익을 사용자의 이익과 동등하게 고려하도록 요구하기 위하여 근로자에게 일정부분 경영에 참여하거나 통제하는 것에 관하여 규정한 법이라는 것을 인식해야만 한다. 따라서 예를 들어 經營協議會는 근로자의 권리보호측면에서 감독기능을 행사하는 반면에 情報保護受任人은 정보보호법규정의 준수를 근로자측면에서뿐만 아니라 또한 다른 관련자와도 관련해서 통제할 의무를 가지고 있다. 이러한 의미에서 聯邦情報保護法과 經營組織法間에 그 지향점이 다르다는 것을 알 수 있다. 곧 聯邦情報保護法은 勤勞者의 개인적 정보보호에 초점을 맞추고 있는데 대하여 經營組織法은 勤勞者의 단체적 권리보호를 목표로 한다. 따라서 聯邦情報保護法은 관련자의 개인관련정보를 보호하고자 하지만 특히 經營組織法 제87조제1항 Nr. 6을 통하여 분명히 나타나는 經營組織法의 立法目的은 經營協議會의 共同決定을 통하여 근로자에 대한 정보기술의 감시를 통제하는데에 있다.

4. 私的 部門에서 個人關聯情報保護의 原則과 그 基準

市場經濟가 작용하기 위해서는 우선 경쟁을 가능하게 하고 개인간 契約締結을 가능하게 하고 그 준수를 보장하며 빠르면서도 확실한 교환을 가능하게 하는 法秩序를 필요로 한다. 따라서 한편으로는 시장경제시스템이 제대로 작동하기 위해서는 個人情報를 보호해야만 하는 필요성이 있다. 예를 들어 업무를 위임받은 代理人의 비밀유지나 침묵의무, 은행의 고객비밀보호의무, 雇用主와 근로자 또는 계약상대방간에도 당연히 상호간에 정보를 보호하려고 노력한다. 그러나 또다른 한편으로 시장경제 속에서 활동하는 사람들은 올바른 결정과 판단을 내리기 위하여 불확실성은 가능한한 줄이고 필요한 정보에 관하여 가능한한 많이 획득하려고 한다. 따라서 이를 위하여 개인관련정보가 필요함은 너무도 당연하다.[345] 결국 필요한 정보에 근거하지 않은 합리적인 결정이란 가능하지 않다. 왜냐하면 행동대안이 전혀 또는 완전히 인식될 수 없기 때문이다. 물론 자유로운 결정이 언제나 올바른 결정을 보장하

345) Wolfgang Zöllner, Datenschutz in einer freiheitlichen marktwirtschaftlichen Ordnung, RDV 1991, S. 3.

지는 않으나 올바른 결정의 개연성을 높인다는 것만은 확실하다. 法秩序 또한 이러한 위험부담을 줄이기 위하여 여러 가지 방법으로 시민들이 경제활동영위시 올바른 결정을 내릴 수 있도록 도와주려고 한다.[346] 하지만 더욱 더 중요한 것은 이러한 경제활동의 주체인 개인 스스로가 적극적으로 개인관련정보를 조사, 수집, 처리하려 한다는데에 있다. 결국 요약하면 시장경제가 제대로 기능하기 위해서는 부분적으로 또는 분야별로 個人情報保護가 요구되기도 하나 이와 동시에 개인관련정보의 가능한한 방해받지 않는 접근과 광범위한 저장 및 이용자유를 전제로 한다고 확인할 수 있다. 결국 市場經濟에서만이 개인의 소유권, 직업자유, 사적 자치가 발현될 수 있는 것이다.

그렇다면 個人情報保護命令과 시장경제간에 일정부분 갈등관계가 성립됨을 부인할 수는 없다. 곧 국가는 法律의 根據없이 정보를 조사, 처리할 수 없는 반면에 시민은 원칙적으로 자유롭게 개인관련정보를 처리하고 교환할 수 있다. 양자간 필요한 조정은 우선 立法者의 과제이다. 이러한 이익형량시 立法者는 일방적으로 특정 이해관계에 따라서만 결정해서는 안된다.[347] 물론 私的 領域에서 情報自己決定權에 관한 보호의무를 이행할 때 立法者는 어느 정도의 형성영역을 가지고 있기는 하나[348] 이러한 形成領域은 比例性原則을 통하여 제한된다. 왜냐하면 보호목적을 달성하기 위하여 立法者가 필요한 보호조치를 하지 않거나 행해진 조치가 전혀 적합하지 않거나 완전히 도달할 수 없는 것이어서는 안되기 때문이다.[349]

그렇다면 한편으로 私的 情報處理가 情報社會에서 한계를 가져야만 한다는 것과 그럼에도 불구하고 또 다른 한편으로는 情報處理의 自由가 私法領域에서 중요한 구조적 가치를 가진다는 것을 인식한다면 私法領域에서 모든 정보처리를 관련자의 情報自己決定權을 제한하는 것으로 보는 것은 정확하지 않다. 따라서 먼저 私人間 情報處理領域에서 특히 개인의 情報自己決定權保護가 필요한 경우에 立法者가 간섭하여 이에 관한 法律을 만들어야만 한다. 이러한 法律에는 최소한 규범명확성원칙, 관련자의 동의원칙, 목적구속이 포함되어야만 한다. 또한 이러한 法律은 정보처리는 물론 情報調査도 포함해야만 한다.

---

346) 예를 들어 상업등기, 채무자열람이나 공고 등.

347) Jürgen Wente, Informationelles Selbstbestimmungsrecht und absolute Drittwirkung der Grundrechte, NJW 1984, S. 1447.

348) BVerfGE 56, 54/73 ; BVerfGE 77, 170/214 ; BVerfGE 79, 174/202.

349) BVerfGE 56, 54/81 ; BVerfGE 77, 170/215 ; BVerfGE 79, 174/202.

5. 現行 法律들의 內容과 批判的 檢討

우리 나라에서 個人情報保護法을 제정할 때 법집행의 실효성확보와 私的 部門의 自律性保障이라는 측면에서 私的 部門을 정보보호법의 적용대상에는 포함시키지 않았다.[350] 그러나 국가, 사회의 정보화가 진전되면 될수록 개인에 관한 금융정보, 신용정보 등의 이용이 활성화됨에 따라서 私的 部門에서도 個人情報保護의 필요성이 높아졌다. 이에 따라서 금융실명거래및비밀보장에 관한 대통령긴급명령, 신용정보의 이용 및 보호에 관한 法律 등 정보의 종류에 따라 분야별로 法律을 제정하여 個人情報를 보호하고 있다.

우선 이 부문에서 신용정보의이용및보호에관한법률에 주목해야 한다. 이 法律은 信用情報의 효율적 이용과 체계적 관리를 통해 신용정보의 오용과 남용으로부터 個人私生活의 秘密을 보호하는 목적을 갖고 있다. 이 법에 따라서 신용정보업자는 신용정보를 수집, 조사할 때 업무범위안에서 수집, 조사의 목적을 명확히 하고 그 목적달성에 필요한 범위안에서 합리적이고 공정한 수단을 사용해야만 한다.[351] 다만 신용정보업자는 ① 개인의 정치적 사상, 종교적 신념 기타 신용정보와 무관한 사생활에 관한 정보 ② 불확실한 개인신용정보를 수집, 조사하는 것이 금지된다.[352] 그리고 신용정보업자는 관리정보의 종류, 이용목적, 제공대상 및 신용정보주체의 권리 등에 관하여 공시하여야 하고[353] 이러한 개인신용정보는 당해 신용정보주체와 신용거래관계의 설정 및 유지여부 등을 판단하기 위해서만 제공, 이용되어야만 한다.[354] 신용정보업자는 허위사실을 의뢰인에게 알리거나 신용거래관계 이외 사생활을 조사하는 것이 금지된다.[355] 다만 이 法律은 신용정보의 효율적 관리와 활용을 통하여 신용사회의 구축에 기여하고자 하는 법으로서 私的 部門에서 일반적인 個人情報保護法이 아니라는 것을 알 수 있다.

그외 금융실명거래및비밀보장에관한긴급재정명령 등을 통하여 특정인의 금융정보가 보호되도록 규정하고 있으나 私的 部門에서 개인의 私生活이 침해될 수 있으며, 침해되는 경우 그 강도가 가장 심한 부문이 바로 금융정보부문이다. 특히 우리 나

350) 다만 개인정보보호법 제22조는 공공기관외의 개인 또는 단체는 공공기관의 예에 준하여 개인정보의 보호를 위한 조치를 강구하여야 하며, 관계 중앙행정기관의 장은 이들에게 개인정보의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다.

351) 신용정보의이용및보호에관한법률 제13조.

352) 同法 제15조.

353) 同法 제22조.

354) 同法 제24조.

355) 同法 제26조.

라처럼 금융정보의 전산화와 금융기관의 전산망연결을 통한 個人情報의 유출가능성이 엄청난만큼 은행은 물론, 보험업계 등 금융권전체적으로 이에 관한 전반적인 법제도적 개선책이 시급히 마련될 수 있어야만 한다. 그리고 위에서 설명한 것처럼 私的 部門에서 個人情報保護와 관련하여 앞으로 진지하게 논의되어야만 하는 분야는 勤勞者의 個人情報保護, 遺傳子情報의 處理, 治療記錄 등이다.

第4章 個人情報의 效率的 保護를 위한 外部的 統制의 必要性

第1節 問題提起

이미 언급된 것처럼 情報社會에서는 컴퓨터를 통하여 권력의 집중화가 가능해지며 또한 컴퓨터는 새로운 통제기술로 이용될 수 있다. 따라서 컴퓨터와 다른 정보기술의 결합은 조직의 효율성 및 통제가능성을 거의 상상할 수 없을만큼 높혀 놓았다. 특히 컴퓨터와 通信技術은 따로 존재하는 정보시스템을 상호결합하여 정보망을 구성한다. 그렇다면 원칙적으로 새로운 情報技術의 中立性이란 존재하지 않는다. 결국 이는 정보이용자의 판단과 시각에 달려 있음을 뜻한다. 정보기술의 도움으로 情報는 사회에서 가장 중요한 지배수단이 되었기 때문에 정보우월적 지위를 통하여 國家는 직접적으로 그 권력을 강화하고 시민의 私的 領域喪失 및 지나치게 강화된 국가통제가능성이 나타날 수도 있다.

이미 우리들이 알고 있는 것처럼 정보처리 특히 자동정보처리가 전적으로 시민을 위한 방향으로만 발전될 수 없다는 것이 확인되었다. 技術發展은 한편으로 커다란 사회적 유용성을 갖기도 하지만 다른 한편으로 이는 시민을 보다 효율적으로 통제하도록 이끌 수도 있다. 따라서 개인관련정보처리와 자동정보처리가 행해지는 곳에서는 처음부터 이러한 발전에 情報保護가 동반되어야 한다. 반복해서 언급하고 있지만 國家나 개인을 통한 모든 情報調査와 획득이 이들의 지식과 권력을 증대시킨다는 것을 결코 잊어서는 아니된다. 정보의 조사와 처리를 통하여 나오는 권력의 확대는 헌법이 보호하려는 원칙과 국민의 기본권에 위협적일 수 있다. 특히 國家權力統一體나 機關協助에 무차별적으로 근거하여 국가기관간 방해받지 않는 정보교환을 정당화하려는 것에 특히 주의해야 한다. 행정이 자동화되어야 하는 곳에서 또한 시민을 위한 자유가 같이 계획되어야 하고 기본권 - 情報自己決定權 - 으로부터 구체화된 개인보호임무가 수행되어야 한다. 특히 情報社會에서 立法府, 行政府, 司法府間 權力分立原則의 유지도 진지하게 검토되어야 한다. 왜냐하면 情報社會에서 行政府가 정보를 거의 독점하기 때문에 立法者가 적절한 판단척도를 발전시키고, 명확한 예측들을 제시하고, 상응하는 입법조치들을 통하여 정보사회에 대처할 능력을 갖기가 매우 힘들기 때문이다. 결국 정보 및 통신기술과 이에 관한 법적 대응방안 간에 괴리가 크면 클수록 立法府는 더욱 더 무력해진다. 이렇게 달라진 상황하에서

국가적인 (정보)권력분배, 입법부와 행정부간 관계, 정보권력분립이 새롭게 논의된다.[1]

문제는 국가의 個人情報侵害를 발견하기가 매우 어렵다는 것이다. 왜냐하면 과거에 행해졌던 개인에 대한 물리적이고 신체적인 직접적 피해와는 달리 情報社會에서 발전된 情報通信技術을 통한 국민의 사생활감시를 국민들이 현실적으로 인식한다는 것이 매우 어렵기 때문이다. 各國의 個人情報保護法에 규정된 個人權利 - 설명권이나 교정권 등 - 또한 이러한 個人情報侵害를 인식해야 비로소 작용할 수 있는 것이다. 그래서 各國에서 情報保護法의 제정 및 개인권리보호가 논의된 이후에 진지하게 논의되고 있는 문제가 바로 個人情報保護를 위한 統制이다. 특히 이 부문에서는 統制機關들의 기능과 조직, 역할, 통제정책의 형성, 통제실무, 국가기관내 편입문제 등이 연구되고 있다. 여기서는 이미 이러한 통제기관을 두고 있는 중요국가들의 통제실무를 살펴보고 우리 나라에서 이러한 통제제도의 도입이 시급함을 설명하고자 한다.

第2節 個人情報의 保護를 위한 組織的, 節次法的 保護

1. 一般的 節次保護의 意味

오늘날 基本權의 발전은 基本權保護의 강한 확대를 통하여 특징 지워진다. 이러한 경향중 하나가 바로 基本權을 節次保障으로 파악하는 것이다. 따라서 기본권과 조직, 절차를 연결하는 것이 基本權의 실현과 보장을 위하여 아주 중요한 일반적 의미를 갖는다.[2] 따라서 모든 관련자들이 자기의 견해와 법적 관점을 피력할 수 있는 공정한 기회들이 절차 속에서 보장되어야 한다. 그런데 節次들을 통한 基本權保護의 확대는 두 가지 방향 속에서 행하여진다. 곧 확대된 制限槪念의 채택을 통하여, 그리고 客觀法的 側面으로서 基本權의 이해를 통하여. 이에 따라서 實體的인 基本權이나 一般的 原則들로 되돌아가기 이전에, 언제나 節次的 基本權이 해당하는지가 우선 심사되어야 한다. 이것이 해당하지 않는 경우에만 절차법적 요구들이 實體的 基本權들로부터 발전될 수 있다. 獨逸의 聯邦憲法法院에 따르면 절차규정들 또한 基本權制限을 표현할 수 있다.[3] 따라서 예를 들어 主觀的 權利들의 고려없이

1) Evangelia Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes, Nomos, 1993, S. 20.

2) Herbert Bethge, Grundrechtsverwirklichung und Grundrechtssicherung durch Organisation und Verfahren, NJW 1982, S. 1.

행하여진 原子力發電所의 承認節次는 이미 違憲일 수 있다.[4] 또한 節次權들은 實體的인 基本權들로부터 파생될 수 있다.[5] 결국 그 효율적인 보장을 위하여 基本權들은 우선 행정조직 및 그 절차들 영역에서 보장되어야만 한다. 이를 넘어서서 새롭게 인식되는 基本權들의 客觀法的 側面을 통하여 국가기구가 基本權實現을 위하여 중요한 그러한 영역들에서 절차들과 조직들을 규정해야 한다는 것이 또한 요구된다. 물론 해당하는 절차규정들을 통하여 基本權을 실현할 이러한 명령은 우선 立法者를 향한다.[6]

2. 個人情報保護를 위한 節次의 重要性

1) 內 容

個人情報를 효율적으로 보호하기 위해서는 정보와 통신기술시스템을 계획하고 결정하는 과정에서 이미 이러한 것이 고려되어야만 한다. 이러한 事前的 節次統制가 이루어지지 않는다면 정보통신기술이 설치되고 작동된 후에 통제기관과 개인의 몇몇 사후적 권리를 통하여 이러한 정보처리에 효과적으로 대응한다는 것은 거의 불가능하다. 技術에 관한 統制가 事前的이고 豫防的으로 행해져야만 情報自己決定權이 이미 기술적 시스템설치시 영향를 주고 보호될 수 있는 것이다. 따라서 事後的 個人情報保護는 예방적 시스템정보보호를 통하여 보충되어야만 한다. 個人情報處理를 법적으로 제한하고, 개인이 설명을 요구하고, 차단, 삭제를 요구하는 등의 개인권리를 통해서 情報自己決定權이 충분히 보호될 수 있다고 더 이상 생각해서는 안된다. 情報調査와 處理는 개개 경우 관련자이익이 관련되는지, 제한되는지와는 독립적으로 사회에 해로운 결과를 끼치지 않도록 구조적으로 명령되어야 한다. 따라서 이러한 법적 요구는 정보보호합치적인 시스템의 형성을 통하여 확인되어야 한다. 투명성, 엄격한 목적구속, 정보흐름의 운하화에 따른 정보보호법요구를 구조적으로 이행하기 위하여 정보와 통신기술시스템의 다른 특성옆에 허용절차가 보장되어야 한다. 그래서 統制機關이 그들의 과제를 인식하고 수행하기 위하여 중요한 시스템의 기능과 운영을 통제자가 개관할 수 있을 만큼 시스템은 투명해야만 한다. 이는 복잡한 시스템허용을 배제하며 정보의 목적에 반하는 이용과 전달은 기술적으로 배제되도록 정보와 통신기술이 형성되어야 한다는 것을 뜻한다.

---

3) BVerfGE 20, 144/148 이하.
4) BVerfGE 53, 30/65이하.
5) BVerfGE 24, 367/401 ; BVerfGE 46, 325/334.
6) BVerfGE 83, 130/152.

이미 설명한 것처럼 情報保護法은 個人情報의 보호를 목표로 하는 바 이는 시스템정보보호를 통하여 보충되어야만 한다.[7] 이러한 시스템정보보호란 개개 경우에 관련자의 권리와 관련되는지, 안되는지와는 독립적으로 情報調査나 處理過程이 법으로 규율되어서 법에 규정된 정보과정전체가 사회에 해로운 결과를 초래하지 않도록 통제하는 것을 뜻한다. 어떤 정보행위가 사회에 해로운가는 우선 立法者가 정치적으로 헌법질서의 틀내에서 결정해야 한다.[8] 이러한 시스템정보보호의 원칙들을 열거하면 다음과 같다 : ① 시스템정보보호는 첫 번째 원칙으로 정보처리의 투명성을 요구한다. 곧 누가 시스템관리자이며 이 시스템에서 어떤 목적으로 관련정보가 이용되며 어떤 정보가 어떤 목적으로 다른 기관에 넘겨지는지를 시민이 확인할 수 있는 경우에만 컴퓨터가 지원하는 정보시스템은 설치되거나 계속 운영되어질 수 있다. ② 그 다음으로 정보처리의 필요성이 제시된다. 이러한 필요성은 정보처리과정과 과제이행간 관계를 말한다. 따라서 관련정보시스템의 설치시 이러한 필요성이 제시되는 경우에만 컴퓨터에 근거한 정보시스템이 설치되고 계속 유지되어도 된다. ③ 또한 시스템정보보호원칙으로부터 지나치게 복잡한 행정활동이 금지될 수 있다. ④ 그 다음으로 妥當性命令과 문맥변경금지원칙이 있다. 節次의 妥當性이란 이용되는 관련절차가 정확히 이를 위하여 필요하다는 것을 확인하는 확실성의 정도를 말한다. 이러한 절차의 타당성은 관련자보호, 과제이행, 정보시스템평가를 위해서 중요하다. 또한 문맥변경을 금지하는 원칙에 따라 정보시스템에서 個人情報에 관한 문맥이 보호되는 경우에만 컴퓨터지원정보시스템에 개인관련정보는 저장되어도 된다. 곧 컴퓨터지원정보시스템은 관련자의 法的 狀況을 변경하지 않으면서 행해질 수 있도록 설치되어야만 한다. ⑤ 마지막으로 관련자의 法的 地位를 보호해야만 한다. 곧 시민이 제때에 자기의 권리를 인식할 수 있고 그 법적 지위가 약화되지 않도록 하는 경우에만 컴퓨터지원정보시스템은 설치되어도 된다.[9]

2) 立法者의 基本權保護義務

民主法治國家에서 모든 본질적인 결정은 의회로부터 그 본질적 부분이 결정되어야만 한다. 의회가 국가의 주요정책결정시 중요한 역할을 하고 議會制定法律이 정치적으로 중요한 의미를 갖는 경우에만 민주주의원칙이 충분하게 효력을 주장할 수

---

7) Adalbert Podlech, Individualdatenschutz - Systemdatenschutz, Klaus Brückner/ Gerhard Dalichau(Hrsg.), *Beiträge zum Sozialrecht, Festgabe für Hans Grüner*, 1982, S. 451.

8) Adalbert Podlech, a.a.O., S. 452.

9) Adalbert Podlech, a.a.O., S. 460.

있다. 곧 의회는 국가행동의 모든 영역을 위한 프로그램형성자이어야 한다. 이를 獨逸의 聯邦憲法法院이 人口調査判決에서 명확히 밝혔다. 곧 情報自己決定權을 보호하기 위하여 情報調査와 처리에 관한 예방조치들을 절차법적으로 규정해야 한다고 결정하였다.[10] 이러한 결정 자체가 새로운 것이 아니라 오히려 새로운 것은 立法者가 情報自己決定權을 보호하는 절차를 만들도록 구속된다는 것이다. 곧 법원이 언급한 것처럼[11] 立法者는 조사계획에 관하여 관심을 갖는 것으로 만족할 것이 아니라 情報調査와 처리절차에 영향을 주어야만 하고 이에 관하여 규정해야만 한다. 이를 통하여 입법계획과 그에 따르는 입법절차뿐만 아니라 지금까지 행정의 권한으로 인식되었던 계획수행 및 전환까지도 이제는 立法者의 헌법적 판단과 책임밑에 있게 되었다.(立法者의 執行 또는 結課責任) 이에 따라서 立法者는 法律內容에 일치하는 전제조건과 계획을 확정할 의무를 가지고 있다. 法律制定後 행정행위를 통하여 전환되어야만 하는 것에 관하여 立法者가 부담하는 이러한 결과책임은 聯邦憲法法院의 절차적 보호개념으로부터 나온다. 지금까지는 立法이란 언제나 절차의 마지막 단계로 간주되었으나 이를 통하여 立法者의 憲法上 權限은 이를 넘어서게 된 것이다. 이에 따라서 정보이용목적과 처리조건이 立法者로부터 정확히 표현되고 관련개인이 추가적인 절차법적, 조직적 규정을 통하여 보호된다면 개인은 情報自己決定權의 제한을 受忍할 수 있다. 이러한 組織的이고 節次法的인 規定은 獨逸 聯邦憲法法院의 人口調査判決을 통하여 비로소 의미를 획득한 것이 아니라 이미 聯邦憲法法院의 과거결정에서 효과적이고 가장 가능한 기본권보호를 위한 조직적이고 절차법적 규정들의 기능이 강조되었다.[12] 이에 따라서 節次에 基本權이 영향을 준다는 것은 組織的이고 節次法的 規定을 통하여 개인의 기본권행사를 가능하게 한다는 것을 뜻한다. 이는 개개 경우에 다양하게 근거되나 일차적으로 立法者에 대한 명령으로서 客觀法的 保護義務로부터 나온다.[13]

3) 個人情報保護에 관한 구체적 보기

獨逸의 聯邦憲法法院은 人口調査判決에서 情報自己決定權의 保護를 위하여 組織的이고 節次法的인 豫防策들을 다음과 같이 강조하였다 : "더욱이 情報自己決定權을 보호하기 위하여 情報調査 및 처리의 수행과 조직을 위한 특별한 예방책들을 필

10) BVerfGE 65, 1/59
11) BVerfGE 65, 1/58
12) BVerfGE 52, 391/408 ; BVerfGE 53, 30/65 ; BVerfGE 63,131/143 ; BVerfGE 73, 118/201
13) BVerfGE 53, 30/65

요로 한다. 왜냐하면 情報는 조사단계는 물론 부분적으로는 저장단계에서도 여전히 개인화할 수 있기 때문이다."[14] 그러므로 개인관련정보의 보호는 이미 情報體系의 계획단계와 결정단계에서 특히 고려되어야만 한다. 따라서 事後的인 個人情報保護는 事前的인 體系的 情報保護를 통하여 보충해야 한다.[15] 물론 개개인은 구체적 예방책의 채택에 관한 어떤 主觀的 權利請求를 갖고 있지는 않다. 하지만 受忍할 수 없는 국가의 制限에 대한 防禦請求가 개개인의 基本權으로부터 나온다.[16] 특히 익명화되지 않은 정보의 전달이나 행정기관의 설명청구거부가 正當化를 필요로 한다. 이를 바탕으로 하여 聯邦憲法法院은 人口調査判決에서 몇몇 예방책들을 구체적으로 열거하고 있다. 첫 번째로 관련자의 情報自己決定權을 위하여 개인관련정보는 가능한 한 빨리 匿名化되어야만 한다고 강조한다.[17] 두 번째로 필요 없는 개인관련정보 또한 가능한 한 빨리 삭제되어야만 한다.[18] 세 번째로 외부에 대한 차단규정들을 통하여 정보처리기관과 다른 기관간에 기능상 분리가 확보되어야만 한다.[19] 네 번째로 개인관련정보를 연방이나 州의 다른 통계담당 공무원에게 전달하는 경우에 이를 기록하도록 聯邦憲法法院은 요구한다.[20]

결국 獨逸 聯邦憲法法院의 人口調査判決에서 조직적이고 절차법적 규정은 다른 의미를 담고 있다. 곧 이는 立法者가 公共福利를 위하여 개인의 情報自己決定權을 제한하는 곳에서 조직적이고 절차법적 규정은 국가의 제한으로부터 관련기본권의 보호를 위한 보장을 뜻한다. 우선 개인관련정보가 제3자에게 넘겨질 경우 情報受信人은 이러한 정보를 가능한한 초기에 사실상 익명화하고 再匿名化에 대한 필요한 예방조치를 행해야만 한다.[21] 이에 따라서 獨逸의 聯邦情報保護法[22]에 따르면 개인관련정보는 연구목적을 위하여 개인관련정보가 처리되려면 먼저 匿名化되어야 한다. 그 다음으로 개인관련정보가 저장된다면 특정인을 식별할 수 있는 정보는 이 개인에 관한 그외 나머지 정보로부터 분리되어 특별히 보호되어야만 한다. 여기서 특정인을 식별할 수 있는 정보란 구체화되거나 구체화될 수 있는 개인적 또는 사항적 관계에 대한 개개 정보라고 이해할 수 있다.[23] 이러한 보호조치를 통하여 권한

14) BVerfGE 65, 1/49.
15) Adalbert Podlech, a.a.O., S. 458 ; Alexander Roßnagel/Peter Wedde/Volker Hammer/Ulrich Pordesch, a.a.O., S. 290.
16) Johann Bizer, 주 107) 216면.
17) BVerfGE 65, 1/49.
18) BVerfGE 65, 1/59.
19) BVerfGE 65, 1/49면 이하.
20) BVerfGE 65, 1/70.
21) BVerfGE 65, 1/49 ; BVerfGE 51, 59, 62
22) BDSG 제40조제3항 1.

없는 사람의 우연한 침입 뿐만 아니라 기관내에서 정보남용의 위험도 줄어든다. 세 번째로 기관의 외부로부터 기관이 저장하고 있는 個人情報를 차단하고 분리해야 한다. 이러한 分離와 遮斷原則은 정보의 필요성 원칙뿐만 아니라 목적구속원칙을 구체화한 것으로써 개인관련정보가 전혀 다른 목적으로 이용될 위험성을 줄인다. 이러한 分離原則은 또한 제3자에게 개인관련정보를 전달하는 경우에도 작용한다. 결국 이는 정보를 조사한 정보보유기관으로부터 개인관련정보가 전달되어야 한다는 생각에 근거한다. 이러한 방법으로 관련자는 그의 정보를 조사한 기관이 갖고 있는 자기정보에 관한 이용을 통제할 수 있다. 또한 遮斷과 分離原則은 個人情報를 보호하기 위한 예방조치의 하나로서 온라인연결을 통한 정보전달의 경우에 전달기관이 개개 경우에 受信人이 이러한 정보를 받아도 되는지를 검토할 권한을 갖고 있도록 요구한다. 그리고 관련자는 자기에 관한 정보이용에 대하여 설명을 받아야 하고 관련자는 자기에 관한 정보처리에 대하여 처리기관으로부터 통지받아야 한다. 그 다음으로 情報受信人은 필요없는 개인관련정보를 가능한한 초기에 삭제해야 한다.[24] 이러한 삭제요구는 전달된 정보의 目的拘束을 지향한다. 필요없는 개인관련정보의 삭제는 情報自己決定權에 관한 침해를 배제할 수 있는 가장 커다란 보호조치이다. 필요없는 個人情報의 삭제를 통하여 구체적인 계획없는 준비목적으로 個人情報를 수집하거나, 목적에서 벗어나는 정보처리, 전혀 다른 목적을 위한 정보전달로부터 개인관련정보는 보호된다.

4) 統計目的을 위한 個人關聯情報

국가가 변화하는 경제적, 사회적 상황에 계획적으로 대응하려면 많은 통계정보를 필요로 할 수 밖에 없다는 것은 당연하다. 獨逸의 聯邦憲法法院 또한 情報社會에서 國家가 활동을 효과적으로 하기 위하여 많은 情報를 필요로 한다는 것을 또한 人口調査判決에서 인정하였다 : "기본법상 원칙들과 지침들을 실현할 의무를 지고 있는 국가에게 統計란 중요한 의미가 있다. 경제적·사회적 발전이 바꿀 수 없는 운명으로 받아들여지는 게 아니라 영구적인 과제로 이해되어야 한다면 경제적·환경적·사회적 관계들에 대하여 포괄적이고 지속적으로 현실화되는 情報를 필요로 한다. 社會國家原則을 지향하는 국가에게 관련정보들의 인식이 비로소 불가피한 행동기반을 제공한다."[25] 그러면서 國家가 개인관련정보를 조사할 경우에 범위 구체적인 규정들을 요구하나 統計目的을 위한 경우에는 그 예외를 인정한다 : "統計目的을 위

23) BDSG 제40조제3항 2.
24) BVerfGE 65, 1/59
25) BVerfGE 65, 1/47.

한 情報調査의 경우에는 정보의 좁고 구체적인 목적구속이 요구될 수 없다. 그 통계처리후에 정보들이 처음부터 구체화되지 않은 아주 다양한 과제들을 위하여 사용되어야만 한다는 것이 통계의 본질이다. 국가가 산업사회의 발전에 준비없이 대처해야 한다면 인구조사는 多目的調査와 多目的處理(준비목적으로 정보를 수집, 저장하는 것)이어야 한다."[26] 결국 통계정보가 갖고 있는 특성 때문에 다른 個人情報보호에서와는 달리 통계정보분야에서는 個人情報의 구체적이고 제한적인 목적구속이란 엄격하게 유지되기 힘들다. 따라서 獨逸의 聯邦憲法法院은 통계조사가 구체적 목적에 속하지도 않으며 처음부터 그런 구체적 목적에 구속되지도 않는다고 인정하였던 것이다. 그럼에도 통계정보에서도 자동정보처리를 통한 情報自己決定權의 침해위험성이 존재한다. 우선 통계목적을 위하여 조사된 정보는 다양한 목적으로 이용될 수 있다. 이는 여러 행정기관에서 개인에게 적대적인 기록화와 목록화위험을 불러일으키기 때문에 통계정보의 다기능적 이용과 개인관련정보보호간 갈등은 행정내부에서 정보처리에 관한 규정을 통하여 해결해야만 한다. 그래서 통계목적을 위한 情報調査와 처리시에 모든 통계의 과제구속원칙이 확정되어야만 한다. 이는 통계정보가 행정기관의 공적인 과제수행을 위해서만 봉사해야 한다는 것을 말한다.[27] 또 통계를 통한 조사목표가 개인에 관하여 익명화된 조사를 통하여 달성될 수 없는지를 언제나 물어봐야 한다. 그리고 統計目的을 위한 정보의 조사와 처리에서 특히 통계와 행정간 분리원칙이 고려되어야 한다.[28] 따라서 통계목적을 위한 情報調査와 處理時 이에 관한 특별한 예방조치가 전제로 되어야 한다. 먼저 개개인을 식별할 수 있는 정보를 통계정보로부터 삭제하는 규정이 있어야만 한다. 두 번째로 외부에 대한 효과적인 차단규정을 필요로 한다. 그 다음으로 통계목적으로 조사된 개인관련정보의 내용들이 엄격한 비밀유지(통계비밀)의무밑에 있어야 한다. 마지막으로 이러한 개인관련정보는 가능한 한 이른 시기에 匿名化되어야만 한다.[29]

第3節 정보시스템안전 및 그 保安對策

정보시스템의 안전 및 보안대책에 관하여 살펴보기 위해서는 우선 情報保護와 情報安全간에 구별하여야 한다. 우선 情報保護에 관한 규정이란 個人情報의 획득 및 처리와 관련되어서 존재하거나 규정되어야 하는 법규정으로 이해되어야 한다. 이에

---

26) BVerfGE 65, 1/47.
27) BVerfGE 65, 1/48
28) BVerfGE 65, 1/50
29) BVerfGE 65, 1/49.

대하여 情報安全은 個人情報를 보호하기 위한 法律들에 기여하기 위하여 결정되고 이러한 法律들의 준수와 유지를 확보, 보장해야 하며 個人情報의 남용이나 위조방지에 기여하는 技術的, 組織的, 節次合致的 保護豫防措置라고 이해된다. 따라서 個人情報保護와 관련되어 情報安全은 個人情報保護에 기여하는 기능을 갖고 있다. 그렇다면 우선 어떤 사람이 특정정보에 관하여 통제할 권한을 갖고 있는지에 대하여 우선 법규정으로부터 확인되어야 한다. 이것이 法律에서 충분히 보호된다는 것이 확인된 다음에 비로소 논리적으로 個人情報에 권한없는 침입으로부터 보호하는 技術的, 組織的, 節次合致的 情報安全이 언급될 수 있다. 따라서 情報安全과 情報保護間 關係는 手段과 目的間 關係이다.[30] 그러므로 情報安全은 개인관련정보를 보장하기 위한 본질적인 전제조건으로서 이를 통하여 보호되는 정보에는 개인관련정보뿐만 아니라 사항관련정보도 속하게 된다. 다시 말하자면 個人情報保護는 개인에 관한 정보처리시 개인의 情報自己決定權制限으로부터 개개인의 보호를 뜻하는 반면에 情報安全은 個人情報를 처분할 개인의 능력보호, 이러한 정보에 권한없는 인식과 접근으로부터 보호, 정보처리시스템내에서 이러한 정보의 권한없는 변경으로부터 보호을 보장해야만 하는 組織的, 技術的 措置라고 이해된다. 따라서 個人情報保護란 個人情報를 보호하기 위하여 무엇이 행해져야만 하는 가에 관한 것이고 情報安全은 이러한 정보보호가 어떻게 실현되어야 하는가에 관한 것이다. 따라서 개인의 情報自己決定權을 침해할 수도 있는 어떤 절차나 기술도 투입되어서는 아니된다. 獨逸에서는 정보안전에 관한 규정은 個人情報保護에 관하여 규정한 특별법규정에서 우선 발견되나 이러한 특별법에서 관련규정이 없는 경우에는 언제나 聯邦情報保護法 제9조가 적용된다고 규정하고 있다. 聯邦情報保護法 제9조에 따라 私的, 公的 領域에서 個人情報를 保護하기 위하여 적합한 기술적이고 조직적 조치를 취할 의무가 정보이용자에게 있다. 이 정보보호규정은 연방정보보호법 전체에 적용된다. 특히 個人情報를 저장하는 기관은 특히 민감한 개인관련정보에 관하여 적절한 정보안전조치를 취해야 한다.

우리 나라의 個人情報保護法 또한 공공기관은 個人情報가 분실, 도난, 변조 또는 훼손되지 아니하도록 안전성확보에 필요한 조치를 강구하도록 규정하였으며[31] 이 法律의 시행규칙에서 전산실 등의 관리, 입출력자료의 관리, 단말기의 설치, 관리에 관하여 규정하고 있다.[32] 그리고 국가기간전산망보호를 포함한 종합적인 정보보안

30) Eggert Schwan, Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, Verwaltungsarchiv 1975, S. 125.

31) 개인정보보호법 제9조

32) 개인정보보호법 제4조, 제5조, 제6조

대책을 강구하기 위해 정보보안전담기관의 설치가 요구되었던 바, 1996년 4월 10일 한국정보보호센터가 설립되었다. 이 한국정보보호센터가 중심적으로 추진할 업무는 ① 초고속정보통신망 보안대책연구, ② 정보보호시스템개발 및 보급활성화, ③ 컴퓨터해킹방지시스템연구개발, ④ 정보보호시스템의 안전과 신뢰성에 관한 기준을 제정하고 공표하는 것 등이다.[33]

第4節 主要國家의 統制機關分析

1. 問題提起

정보시스템 및 통신시스템이 제공하는 새롭게 달라진 조건들하에서 國家的인 (情報)權力分立, 立法府와 行政府間 關係, 새로운 권력강화 및 이동의 문제가 심각하게 제기된다.[34] 특히 立法府와 행정부간 권력균형이 심각하게 위협받을 가능성이 많이 지적되고 있다 : ① 그 작업형태상 情報通信技術은 무엇보다도 行政府의 활동을 위하여 우선 활용된다. 또한 行政府가 담당하고 있는 과제에 비추어볼 때 행정이 의회나 법원보다 정보수집, 처리 등에서 비교할 수 없을만큼 더 유리하다. 이에 반하여 立法者에게는 情報社會의 발전에 관한 적절한 판단척도를 발전시키고, 명확한 예측들을 제시하며, 상응하는 입법조치들을 통하여 이에 반응할 능력이 결여되어 있다. 특히 情報通信技術의 발전과 법규정간 괴리가 크면 클수록 前者에 대처하려는 立法府의 능력은 더욱 더 작아질 수 밖에 없다. ② 게다가 이러한 상황하에서 의회, 특히 野黨은 행정부가 가지고 있는 정보에 접근하기가 더욱 더 어려워진다. ③ 마지막으로 個人情報를 보호하기 위한 통제방안이나 제도를 확보한다는 것이 매우 어렵다. 왜냐하면 法院이나 의회가 행정부의 정보처리행위를 검토, 통제하기 위해서는 行政府의 모든 행위가 반드시 기록되어야 하나 이 또한 여태까지 해결되지 못하고 있을 뿐만 아니라 확실하게 효율적인 통제방안조차 논란이 되고 있기 때문이다.

따라서 개인의 情報自己決定權을 보호하기 위하여 情報保護法을 제정하고 이 법속에 개인의 각종 권리보호조항을 신설하며, 情報保護에 관한 조직적, 절차법적 규정을 두는 것과 동시에 個人情報保護에 관하여 통제하는 機關을 만드는 것에 관하여 진지하게 토론하여야 한다 : 통제기관들의 기능과 조직, 통제정책의 형성과 권한, 통제실무 등. 그렇다고 전세계 모든 국가의 統制機關들을 검토대상으로 삼을 수는 없다. 따라서 이러한 통제기관을 크게 유형화시켜 고찰할 필요가 있다. 따라서 이러한 統制機關은 우선 外部的인 統制類型과 內部的 統制類型으로 나눌 수 있

33) 김홍근, 선진국의 정보보호전담기관현황, 정보화로 가는 길, 1997.10, 110면 이하.
34) Evangelia Mitrou, a.a.O., S. 20.

다. 먼저 外部的 統制類型은 ① 相談시스템 : 公的 領域에 관해서만 統制權限이 있을 뿐만 아니라 事後統制와 助言(相談)機能만을 갖고 있는 것으로 특징 지워지는 獨逸式 情報保護機關類型과 ② 許可시스템 : 정보파일의 설치에 관하여 승인하고 公的 領域은 물론 私的 領域을 위한 통제권한 및 결정권한, 간섭권한들을 統制機關에게 부여하는 프랑스식 정보보호기관유형으로 나눌 수 있다. 그리고 內部的 統制類型이란 個人情報를 다루는 개개 國家機關 스스로 이러한 정보처리에 관하여 통제하는 방식으로서 美國이 이러한 유형에 속한다.

이러한 상이한 정보보호시스템에는 당연히 서로 다른 統制機關의 役割이 반영되어 있다. 우선 情報社會에서 개인의 私生活을 보호해야 한다는 인식은 이러한 두 시스템 모두에서 공유된다. 그리고 이렇게 다른 시스템을 갖고 있다 하더라도 이러한 나라들의 情報保護法規定 또한 많은 부분 유사할 뿐만 아니라 상호간에 비교함으로써 보충하고 수정하기도 한다. 그럼에도 불구하고 개개 나라의 정치적, 법적 시스템의 차이나 통제방안을 강구하는 시각의 차이 때문에 統制機關의 설치 및 統制機關의 권한에서 많은 차이를 보이고 있는 것이다. 따라서 情報保護를 위한 統制機關의 조직 및 그 운용을 이해하기 위해서는 우선 일반적이고 특별한 정보보호법규정은 물론 개개 사회의 사회적, 정치적, 역사적 상황 또한 살펴보아야만 한다. 왜냐하면 개개 국가의 구체적인 정치적, 역사적 상황 및 法的, 行政的 傳統이 통제기관의 법적인 권한은 물론 그 정책 및 행동방법에도 영향을 주고 있기 때문이다. 따라서 統制機關의 권한 등이 개개 국가 立法者의 구체적인 생각들, 목표들, 기대들을 표현하고 있기 때문에 단순한 比較法的 檢討를 거쳐서 임의로 바꿀 수는 없다 할지라도 상이한 통제모델이 개개 국가의 다른 상황들 속에서 어떻게 발현, 전개, 작용할지를 확인할 수 있는 경우에만 우리 나라에서 바람직한 통제방안을 강구하는 데에 도움이 될 것이다.

결국 個人情報를 보호하기 위하여 어느 統制機關이 더 효율적인지를 판단하기 위한 척도는 궁극적으로 두 모델중 어떤 것이 시민들에게 더 포괄적인 情報保護를 보장하는가이다. 이러한 분석을 위하여 한편으로는 해당 모델을 채택한 국가의 情報保護法制를 분석해야 한다. 예를 들어 우선 법규정속에 담긴 統制機關의 조직과 과제 및 권한들에 관하여 살펴보아야 한다. 그러나 다른 한편으로는 統制機關을 효율적으로 분석, 검토하기 위해서는 이러한 統制機關에 관한 법규정들의 자세한 설명을 넘어서서 한 국가내에서 통제가 실제로 어떻게 행해지고 있는지를 파악하여야 한다. 왜냐하면 個人情報保護에 관하여 제기되는 많은 문제들 중에서 특히 情報保護法規定의 一般條項的 性格과 해결해야 하는 事案이 情報社會에서 새롭게 제기되는 것이기 때문에 個人情報保護는 이에 관한 실무 속에서 비로소 그 윤곽을 획득하

고, 정보보호우호적이거나 적대적으로 해석되고 판단되기 때문이다. 결국 이는 어떤 통제모델이 적합한지는 통제기관의 실무를 파악해야만 확인된다는 것을 뜻한다. 물론 어떤 기준들에 따라서 통제기관들이 판단되고 어떤 척도에 따라서 그 효율성이 평가되어야 하는지는 어려운 문제에 속할지도 모르나 특히 統制機關의 독립성보장 및 그 충분한 法的 權限保障은 개개 통제모델를 평가하기 위하여 작용하는 중요한 기준들이다.

중요한 국가들의 統制機關을 살펴보기 이전에 이러한 통제기관을 설치한 각국의 법규정을 개략적으로 살펴보면 다음과 같다. 덴마크는 公的 領域과 私的 領域에서 個人情報保護를 규율하는 두 개의 독립된 法律들을 갖고 있다. 私的 領域을 규율하는 法律은 자동화된 個人情報와 몇몇 수작업파일들을 포함하는 반면에 公的 領域을 규율하는 法律은 자동화된 정보에만 적용된다. 公的 領域에서는 監督機關이 개인기록들을 처리하는 機關들에게 자문을 하며 개인의 주관적인 접근권이 보장되고, 잘못되거나 불충분한 정보가 수정되거나 삭제되도록 돕는다. 연방차원에서 오스트레일리아는 私生活保護問題에 관하여 상당한 주의를 기울였다. 1973년에 연방정부는 法改革委員會를 만들었고 이 委員會는 1976년에 私生活保護에 관한 회의를 개최하였으며 私生活保護에 관한 입법 및 이에 관한 다른 조치들을 제안하였다. 1983년 12월에 연방법개혁위원회는 다시 불평을 조사할 권한을 갖고 있는 연방프라이버시위원의 창설을 권고하였다. 마침내 1988년에 제정된 연방프라이버시법은 이 법을 침해하는 활동에 대하여 조사하고 금지를 요구할 수 있으며 불평을 접수하는 권한을 프라이버시위원에게 인정하였다. 1978년에 제정된 오스트리아의 情報保護法에 따르면 公的 領域에서 個人情報保護에 관한 統制를 情報保護委員會가 담당한다. 이 情報保護委員會는 5년의 임기로 임명되는 4명의 위원들로 구성되어 있는데 이 委員會의 주요 기능중 하나가 바로 자신의 권리가 침해되었다는 개인의 불평들에 관하여 검토하는 것이다. 이 위원회의 권한은 諮問的인 것으로 한정되나 重要法律에 관한 개정안을 제시할 수는 있다.

2. 外部統制型 시스템

1) 許可시스템

(1) 스웨덴

a) 序

이미 언급한 것처럼 스웨덴은 전세계에서 가장 먼저 個人情報保護에 관한 法律을

제정한 나라로서 컴퓨터와 私生活保護問題를 다룰 때 유럽 및 다른 나라들을 위한 모델로서 언급된다.[35] 비록 스웨덴식 모델의 정확한 내용들이 광범위하게 모방되지는 않았다 할지라도 정보보호에 관한 이러한 스웨덴식 모델은 서유럽국가들에서 정보보호의 발전에 막대하고 직접적인 영향을 미쳤다.[36] 스웨덴에서는 公的 記錄들의 공개와 비밀에 관한 議會委員會가 1969년에 처음으로 만들어졌고, 1972년 "컴퓨터와 프라이버시"에 관한 보고서에서 情報保護에 관한 특별입법을 제안하였다. 1973년에 제정된 스웨덴의 情報法(Data Act)은 個人情報保護에 관한 첫 번째 국가법으로서 다른 서유럽국가들에서 個人情報保護에 관한 法律을 제정할 때 상당한 영향을 주었다. 이런 과정을 거쳐서 제정된 스웨덴의 情報保護法은 개인의 私生活에 관한 부당한 침해를 방지하는 것을 목표로 하였다. 1973년 情報法은 公的 領域이든, 私的 領域이든 간에 컴퓨터화된 형태에 의하여 확인할 수 있는 個人情報의 수집, 저장, 유통을 규율하는 情報監督委員會(Data Inspection Board)를 만들었다. 위 법을 제정할 때 가장 주목할만한 부분은 정부와 의회의 명령에 의하여 만들어진 정보시스템을 제외하고서 모든 다른 정보시스템들이 이 DIB의 허가를 받도록 하는 시스템(許可시스템)을 확립하였다는 것이다. 결국 DIB는 개인의 私生活에 관한 위험여부를 판단하기 위하여 수집되는 個人情報의 특성과 내용, 어떤 개인의 정보가 어떻게 획득되는지를 관찰할 권한을 갖고 있다. 그리고 이 情報監督委員會는 個人情報의 수집과 전달을 통제하고, 정보사용을 규율하며, 컴퓨터화된 정보은행에 관한 관리체계를 통제한다.[37]

b) 組 織

스웨덴의 情報監督委員會는 다양한 정당들과 이익단체들을 대표하는 기관으로서 확정된 임기를 갖고 임명되는 事務局長을 갖는 독립된 기관이다. 이 情報監督委員會는 個人情報保護에 관한 기본정책을 확립하나 대부분의 결정들은 위 위원회의 일원인 事務局長이 이끄는 전문스탭들에 의하여 내려진다. 이 정보감독위원회는 정보법하에서 다양한 決定權限을 갖고 있는 機關으로서 사무국장을 제외하고서 4년임기로 정부에 의하여 선출된다. 이 위원회의 委員들은 立法府, 勞動組合, 산업체, 行政府, 연구기관들을 대표한다. 이를 자세히 설명하면 스웨덴의 정보감독위원회 위원 중 4명은 의회의 중요정당들을 대표한다. 그외 사무직노조, 생산직노조, 정보처리 산업계의 대표들 및 한 명의 언론인, 한 명의 교수가 포함된다.[38] 이 위원회에 立

35) James Michael, ibid., p.53.
36) 1978년에 제정된 프랑스의 법률이 스웨덴방식을 채택한 가장 명확한 사례일지도 모른다.
37) David H. Flaherty, ibid., p.93.
38) 위원회의 위원 중에는 장기간 위원으로 있는 사람이 있는데 이들은 단순히 이 주제에 관심

法府의 대표들이 존재한다는 것은 이 위원회를 한 정당이 지배하지 않으며 이에 따라서 광범위하게 다양한 여론을 반영하려 한다는 것을 뜻한다. 따라서 실무상으로 보면 이러한 議會의 대표자가 위원회의 구성원이라는 사실이 情報監督委員會가 작은 의회로서 기능 하도록 한다. 설치된 후 처음 10년 동안에 이 情報監督委員會는 許可問題와 監督問題를 각각 따로 담당하는 두 부서를 두었으나, 1983년 법개정으로 인하여 이 위원회는 세 부서로 개편되었다. 곧 公的 機關들과 私的 領域을 담당하는 부서들이 각기 그 영역에서 허가기능과 감독기능을 맡고 세 번째 부서는 私的 領域의 일부인 信用領域과 債務領域에서 활동한다.[39]

c) 權 限

1973년에 제정된 스웨덴의 情報法은 公的 領域이든, 私的 領域이든 간에 컴퓨터화된 형태에 의하여 확인할 수 있는 個人情報의 수집, 저장, 유통을 규제하는 情報監督委員會를 만들었으며 1982년 법개정으로 인하여 이 위원회는 정보법의 執行機構로 그 권한이 부분적으로 확대되었다.

우선 스웨덴의 情報法은 정보처리에 관하여 아주 상세한 규정을 갖고 있다.[40] 이에 따라서 情報監督委員會는 기록될 個人情報의 내용과 양, 어떠한 방법으로 그리고 누구로부터 이러한 정보가 수집되어야 하는지 등을 심사할 수 있다. 예외를 인정할 특별한 이유가 존재하지 않는 한, 책임 있는 파일관리자와 관계되는 직원, 고용인 또는 소비자에 관해서만 개인파일이 설치될 수 있다.[41] 情報法 제5조에 따라 情報監督委員會는 파일설치목적에 일치하는 개인파일의 설치와 보존에 관한 규정을 공포해야만 한다. 그 다음으로 情報監督委員會는 私的 領域에서 개인정보파일의 설치에 관하여 許可한다. 그리고 자동처리되는 個人情報가 민감하다면 이 委員會의 公式的인 許可를 필요로 한다. 또한 이 委員會는 또한 公的 領域에서 個人情報의 수집을 규율한다. 그러나 이 委員會의 권한은 情報保護法으로 한정되지 않는다. 따라서 이 委員會는 개인의 私生活保護와 관련되는 다른 두 가지 法律을 감독

을 갖고 있기에 기꺼이 이 일을 하려고 한다. 이러한 공적 서비스의식이 스웨덴의 엘리트들 가운데에 높게 발전되어 있다.

39) David H. Flaherty, ibid., p.101.

40) 정보법은 명확히 개념 정의되는 중요한 원칙들을 열거하기보다는 자세한 실무들과 절차들을 상세하게 설명하는 데에 더 많은 공간을 할애한다. 더군다나 DIB가 우선적으로 구체적인 적용들에 대하여 허가결정들을 내리므로 광범위한 일반원칙들 - 특히 공적 영역과 관련하여 - 에 많은 신경을 쓰지 못하였다.

41) 프랑스 정보보호법에서처럼 스웨덴정보법은 어떤 정보 - 인종, 성생활, 형사, 건강, 정신병 기록이나 사회복지기록들, 정치적, 종교적 신념들 - 를 특별히 민감한 것으로 개념 정의한다. 이에 따라서 특별히 예외적인 경우에만 공적 기관만이 이들 정보를 기록, 저장할 수 있다.

하고 이 부문에서 필요한 경우에 이에 관한 허가권한을 갖고 있다. 이러한 法律로는 1974년에 제정된 信用情報法(the Credit Information Act)과 債務救濟法(the Debt Recovery Act)이 있다.

1973년에 제정된 情報法에 관한 改正(1981년과 1982년)을 통하여 개인파일설치시 情報監督委員會의 허가를 받도록 요구하던 시스템으로부터 이 委員會에 단순히 신고(기록)하는 것으로 충분한 시스템으로 바뀌었다. 다시 말하면 과거에는 개인정보파일설치에 관한 許可는 전통적으로 情報監督委員會의 주요활동이었다. 그래서 그전에는 모든 주요한 정보시스템들이 규제되었으나 情報法이 개정됨으로써 모든 책임 있는 기록자는 여전히 許可를 필요로 하기는 하나 이러한 허가는 보통 해당 기관의 개인파일신청을 통하여 자동적으로 행해진다.[42] 따라서 이러한 법개정을 통하여 모든 개인정보시스템에 관한 一般的인 事前許可로부터 우선적인 記錄(申告)시스템으로 바뀌었다. 이제 情報監督委員會는 事前에 이러한 개인정보파일의 설치에 관하여 상세하게 그 정확성을 심사하지 않는다. 이제 어떤 사람에 관한 평가나 건강, 前科, 宗教, 政治的 見解와 같은 민감한 정보에 관한 개인정보파일설치에 관해서만 시스템설치이전에 情報監督委員會로부터 명시적으로 허가를 받도록 정보법은 요구한다.[43] 그래서 예를 들어 문제가 되는 파일이 어떤 다른 개인파일들로부터 나온다면 許可를 필요로 한다. 그러나 실제로는 私的 領域과 公的 領域에서 個人情報를 처리, 저장하는 대부분의 기관들은 개인파일을 저장하려고 하기 전에 情報監督委員會에 그들의 계획을 단순히 표명하면 된다. 여기서 주목할 것은 情報監督委員會의 許可는 실제로는 또한 개인정보파일설치에 관한 承認으로서 기능한다는 것이다. 이러한 의미에서 情報監督委員會의 許可는 새로운 기술도입 및 정보사용을 정당화하고 촉진하는 간접적인 효과를 갖는다. 예를 들어 警察은 새로운 정보시스템설치에 관한 계획들을 情報監督委員會와 토론한다. 그리고 이러한 許可를 받기 위하여 경찰들은 실제로 그들 자신의 정보시스템을 검토하고 수정해야만 했다.

그런데 行政府나 議會에 의하여 만들어진 개인파일은 이에 관한 許可를 필요로 하지 않는다는 정보법규정에 의하여 情報監督委員會의 이러한 허가와 감독권한은 심각하게 제한된다. 따라서 정보감독위원회의 統制로부터 면제될 정보은행을 만들 궁극적인 권한을 의회와 행정부는 갖고 있는 것이다. 다만 감독으로부터 면제되는 정보은행을 만들 정부권한에 대한 중요한 統制는 情報法 제2조가 포함하는 민감한

42) 따라서 위 법개정을 통하여 허가(license)와 승인(permission)간에 구별된 것이 큰 변화중 하나이다. 특히 1982년에 개정된 정보법은 종전에 정보감독위원회가 짊어졌던 많은 과제와 이에 관한 비용들을 줄이고 선택적인 허가시스템을 만드는 것을 목표로 가졌다.

43) 情報法 제3조

個人情報를 수반하는 경우에 事前에 情報監督委員會와 상담해야만 한다는 것을 통하여 이루어진다. 이러한 조항하에서 情報監督委員會는 면제되는 個人情報銀行을 바꾸거나 새롭게 지정할 권한을 갖고 있다.[44] 情報監督委員會의 統制權限에 관한 또 다른 제한은 情報法 제25조 이하에 근거하여 구체적인 경우에 공익보호를 위하여 法務部長官이 정보감독위원회의 결정들에 반대하는 것이다. 法務部長官의 이러한 반대는 정보보호원칙들의 과도한 적용을 제한하는 기능을 갖고 있다.

위에서 이미 설명한 것처럼 스웨덴 情報法의 우선적인 목표는 기록되는 사람의 私生活이 부당하게 침해되는 것을 방지하는 것이다.[45] 그러나 유감스럽게도 이 情報法은 情報監督委員會가 "개인의 프라이버시"나 이에 관한 부당한 침해조치를 어떻게 개념 정의해야만 하는지에 관하여 단지 제한적으로만 언급하고 있을 뿐이다. 이에 따라서 개인의 프라이버시에 관한 부당한 침해와 연결되어 결국 이에 관하여 결정을 내리는 情報監督委員會에 커다란 裁量權限이 부여되어 있다. 따라서 情報監督委員會는 충돌하는 이해관계를 형량할 책임을 갖고 있으나 情報監督委員會에 의한 통제가 필요한 정도를 넘어서서 더 많은 비용이나 불편함을 불러일으키지 않을 만큼만 행사되어야 한다.[46]

또한 DIB의 통제권한과 관련하여 情報法은 이에 관한 일련의 벌칙들 및 제정법 위반에 대한 벌금규정을 담고 있다. 情報法 제23조에 따르면 책임 있는 기록자가 부정확한 정보를 저장하는 것에 대하여 관련개인이 民事上 損害賠償을 청구할 수 있다고 규정하였다. 情報法에서 책임 있는 보유자란 그의 처분 하에 있는 개인정보 파일들을 어떤 목적을 위하여 저장하는 사람(기관)이다. 그리고 이러한 책임 있는 보유자는 情報法의 규정 및 그 許可事項을 준수한다는 것을 입증해야만 한다. 또한 이러한 보유자는 정보저장을 중단한다면 이에 관하여 情報監督委員會에 신고할 의무가 있다. 그래서 책임 있는 보유자는 감독을 위하여 情報監督委員會가 요구하는 자동정보처리와 관련되는 정보를 이 위원회에 제공해야만 한다.[47] 결국 立法府는 個人情報를 효율적으로 保護하기 위하여 대단히 강력한 권한들을 情報監督委員會에 부여하였던 것이다. 이에 따라서 위원회는 자동정보처리와 관련된 기록들에 접근할 권리를 갖고 있으며 컴퓨터운용에 관하여 지시할 수도 있다.

또한 개인관련정보가 제정법, 정보감독위원회의 결정이나 기록되는 사람의 동의를 받아서 기록되거나 처리되지 않는 한, 어떤 다른 개인파일로부터 획득된 個人情

44) 情報法 제18조
45) 情報法 제3조
46) 情報法 제6조
47) 情報法 제17조

報를 연결하려면 이에 관한 구체적인 許可를 情報監督委員會로부터 받아야 한다. 물론 情報監督委員會가 모든 형태의 기록연결에 반대하려는 것은 아니나 정보사용자가 個人情報가 왜 수집되었는지를 모르거나 또는 매우 민감한 정보를 연결하려고 하는 경우에는 반대한다. 왜냐하면 기록연결을 통하여 국민을 감시하려고 하거나 개인들로부터 정보를 직접적으로 수집하는 것을 피하고자 하는 이러한 행위는 위험한 것으로 생각되기 때문이다. 어떤 기록연결이 시도되기 이전에 언제, 왜 그리고 어떻게 정보가 수집되었는지를 사람들이 우선 알아야 한다는 것이다. 어쨌든 스웨덴에서는 거의 모든 기록연결들이 情報監督委員會의 규제밑에 있다는 사실이 個人情報保護側面에서 중요하다. 예를 들어 사회복지기관들은 기록연결을 강력하게 주장하나 情報監督委員會는 이러한 기록연결이 사회적으로 유용하다는 것을 인정하면서도 이러한 두 파일(조세목적으로 신고된 소득과 복지혜택자격)간 비교에 반대한다.

기록보유자에게 書面質疑를 한 사람은 情報法 제10조 이하에 근거하여 이들로부터 본인에 관한 정보를 받을 권리를 갖고 있다. 情報監督委員會가 특별한 이유가 있다고 인정하지 않은 한, 관련개인에게 이러한 정보제공은 무료이다. 그리고 관련개인의 이러한 권리가 인정되지 않는 한 그는 情報監督委員會에 이러한 정보처리에 관하여 불평할 수 있다. 그래서 情報監督委員會는 이러한 경우에 "정보옴부즈만"으로서 활동하게 된다.[48]

d) 評 價

다른 나라들과 비교하여 스웨덴은 840만명이라는 비교적 작은 인구를 갖고 있는 단일국가로서 個人情報保護를 위하여 만들어진 통제시스템이 비교적 단순하다. 따라서 스웨덴의 情報監督委員會와 같은 통제기관유형은 실제로 정책을 입안하거나 집행하는 부서들의 규모가 아주 작고 행정기관들이 많은 정부활동을 수행하는 전통적인 정부모델에 적합하다.[49] 문제는 이러한 統制機關이 國家機關들을 효율적으로 통제하기 위해서는 情報保護機關이 독립되어 있으며 이러한 기관이 감독권한을 사용하려는 의지를 갖고 있어야 한다는 것이다. 이는 개인정보보호를 적대시하거나 반대하는 정치적 분위기 속에서 기록연결을 통제하려는 경우에 특히 그렇다. 그런데 스웨덴에서 情報監督委員會의 독립은 情報法의 구체적인 규정에 근거해서라기보다는 이에 관한 憲法慣行에 의하여 확립되었다. 이러한 憲法慣行에 따르면 정부가 情報監督委員會의 일상적인 업무에 간섭하는 것이 금지된다. 그러나 이는 스웨덴에서 情報監督委員會의 활동이 언제나 성공적이었다는 것을 뜻하지는 않는다. 예

48) David H. Flaherty, ibid., p.136.
49) David H. Flaherty, ibid., p.96.

를 들어 한편에서는 情報監督委員會가 너무 강력한 권한을 갖고 있으며 私的, 公的 領域의 정보처리에 자주 간섭한다고 주장하는 반면에 오히려 이 委員會가 그 諮問機能 및 정부가 허용하는 程度를 넘어서는 권한을 갖고 있지 않다는 견해도 또한 있다. 일반적인 시각에서 보면 스웨덴의 정보감독위원회는 강력하고 영향력이 큰 편이다. 많은 다른 나라들처럼 스웨덴의 情報監督委員會는 모든 공공행정부문과 관련되어 있으며 이러한 위원회를 통제하려는 정부의 노력 또한 다행스럽게도 그리 크지 않았다. 문제는 변화하는 정치적 상황이 情報監督委員會에 의한 권한행사에 영향을 준다는 것이다. 예를 들어 1970년대에는 모든 政黨들이 個人情報의 保護를 지지하였으나, 그 뒤 경제불황으로 이러한 합의는 깨지고 말았고 1980년대 이후에는 비규제, 비중앙화 등이 더 많이 언급되고 있다. 그렇다면 이제 문제는 情報監督委員會가 이렇게 변화하는 정치적 상황에 적응해야 하는 지이다. 곧 情報監督委員會는 국가가 인정하는 권한만을 가져야 하는가? 또는 행정부와 입법부가 위원회의 활동을 강하게 지지할 때에만 그 권한이 강화될 수 있는가? 어쨌든 情報監督委員會의 반관료주의적 경향은 1982년의 情報法改正에서 명백하였다. 법개정당시에 情報監督委員會는 형식적인 허가의 양을 줄일 것을 주장하였는데, 이는 개인기록들의 보편적인 허가시스템운용을 통하여 이러한 시스템이 위원회에 엄청난 업무부담을 지운다는 것이 입증되었기 때문이다. 스웨덴에서 개인정보를 보호하기 위한 統制機關으로서 情報監督委員會가 얼마만큼 현실적으로 유용한지를 평가하기가 매우 어렵다. 우선 스웨덴에서 情報監督委員會의 활동은 나름대로 성공적이라고 말할 수 있다. 이는 情報監督委員會가 맡은 바 직무를 잘 수행하였다는 것을 뜻한다. 예를 들어 情報監督委員會는 기록연결에 적극적으로 영향을 미쳤고 그 허가활동들을 통하여 주요한 공공행정의 정보시스템들에 커다란 영향을 주었다. 그러나 스웨덴의 情報法은 명확히 개념 정의되는 중요한 원칙들을 열거하기보다는 자세한 실무들과 절차들을 상세하게 설명하는 데에 더 많은 공간을 할애한다. 더군다나 情報監督委員會가 구체적인 개인정보파일의 설치와 그 적용에 대하여 허가하므로 특히 公的 領域에 적용되어야만 하는 중요한 일반원칙들의 확정 및 그 집행에 관하여 많은 신경을 쓰지 못하였다. 또한 불행히도 DIB는 많은 정보처리기관들을 적절히 감독하지 못하였다. 이는 個人情報를 보호해야 한다는 측면에서는 중대한 결함으로 드러난다. 왜냐하면 이러한 감독활동은 감시통제를 위한 장치들이 실제로 작용되도록 하는 주요한 수단이기 때문이다. 그렇다면 스웨덴에서 情報監督委員會의 존재는 감시사회의 출현을 막지는 못하였지만 이를 제한하거나 억제하기는 하였다고 말할 수 있다. 결국 스웨덴에서 몇 차례에 걸친 情報法의 개정은 情報保護法의 실험적인 성

격과 변화, 발전하는 정보통신기술의 적용에 법이 어떻게 대처하여야 하는지를 잘 드러낸다.

(2) 프랑스의 情報保護機關

a) 序

프랑스는 가장 일찍, 그리고 정열적으로 정보처리를 시작한 情報國家에 속한다. 그래서 프랑스국민들은 일찍 새로운 情報技術이 개인의 자유와 프라이버시에 미칠 수 있는 위험을 인식하였다. 1975년 사파리(Safari)사건이 언론에 보도된 이후에 公的, 私的 領域에서 私生活自由, 개인적 자유, 공적 자유들을 존중하는 정보처리발전을 검토하기 위한 위원회를 法務部는 설치하였다. 이에 따라서 1978년에 情報保護法이 시행되었고, 같은 해에 다른 法律에 의하여 행정서류들에 관한 일반적인 접근권이 확립되었다. 1978년에 情報保護法을 만들 때 議會는 법이 公的 領域과 私的 領域 모두를 포함하여야 한다고 결정하였다. 또 立法者는 개인정보처리시스템에 관하여 諮問하고, 기존시스템을 감독하고, 조사하는 임무를 갖고 있는 독립기관인 國家情報處理自由委員會(Commission Nationale de l'Informatigue et des Libertés, CNIL)를 설치하였다.[50]

b) 組 織

프랑스의 國家情報處理自由委員會는 5년의 임기로 임명되는 17명의 위원들로 구성된다. 또 이 위원들 중에서 1명의 議長, 2명의 副議長, 다른 한 CNIL위원으로 구성되는 執行委員會가 구성되며 執行委員會에는 전문스탭들이 있다. 전문스탭들은 ① 法的 問題, ② 情報處理技術, ③ 行政的이고 財政的인 서비스를 담당하는 세 가지 주요부서로 구성되어 있다. 게다가 이 執行委員會는 議長이나 副議長에게 권한을 위임할 수도 있다.[51] 실제로 특정정보시스템에 관한 의견을 얻기 위하여 國家情報處理自由委員會에 諮問한다면 여러 스탭들이 해당주제에 관하여 대답한다. 國家情報處理自由委員會는 연구, 통계, 자치단체, 기술과 안전에 관한 소위원회들로 구성되었으며 委員會의 위원들은 해당 소위원회에서 근무한다. 이중 최소한 한 명은 가장 주요한 諮問領域을 위한 報告者로 임명된다. 그래서 이들은 健康, 경찰, 사회복지기록과 같은 여러 분야들을 담당한다.[52] 첫 번째 보고서에서 國家情報處理

50) James Michael, ibid., p.65. 의회는 독립된 행정기관을 만들었는데, 이는 프랑스가 처음이었다. 이러한 위원회를 채택할 때 입법부는 스웨덴식 정보감독위원회에 의하여 크게 영향을 받았으며, 한 사람이 혼자 기능 하는 것보다 위원회를 선호하였다.

51) David H. Flaherty, ibid., p.172.

52) David H. Flaherty, ibid., p.173.

自由委員會는 委員會의 목적이 個人情報에 관하여 규율하는 것만이 아니라 정보처리와 다른 자유간 관계들에 대하여 조화시키는 것이라고 설명하였다.

c) CNIL의 地位와 活動條件

프랑스의 통제기관은 合議制機關이면서도 독립적인 行政機關으로 설립되었다. 立法者는 상호통제를 통한 기관의 獨立性 및 기관의 지위강화를 목표로 하였다. 情報保護機關이 도대체 존재의미를 가져야 한다면 이는 독립되었다는 전제조건하에서만 그렇다. 그러나 이러한 獨立性 자체가 자기목적적인 것이 아니라 효율적인 統制機關을 保障하기 위한 구체적인 한 가지 조건에 불과하므로 CNIL의 조직이 기능합치적인지는 여러 측면에서 판단되어야 한다. 처음에 政府는 委員會의 역할을 法院의 기능과 行政府의 기능을 모두 갖는 기관으로 만들려고 하였으나 議會는 이러한 정부의 생각에 반대하고 의회의 대표들이 이 기관에 참여하기를 원하였고 결국 國會議員들이 이 위원회의 구성원이 되는 것을 통하여 위원회가 강력해져야 한다고 생각하였다. 이에 따라서 만들어진 법규정은 여러 意思들간에 타협이었으나, 어쨌든 의회가 원하는대로 규정되었을 뿐만 아니라 이를 넘어서서 개개 구성원의 임명형태에 관한 議會의 견해 또한 관철되었다.[53] 이미 설명한 것처럼 CNIL은 여러 국가기관들을 대표하는 17명의 구성원들로 구성되며 위원회에서 일하는 위원의 다수는 해당 기관의 총회로부터 선출되고 行政府는 단지 3명의 구성원만을 직접 임명할 뿐이다.[54] 따라서 CNIL에 영향을 줄 행정부의 가능성은 제한되어 있다. 이들 위원들의 신분은 法律에 규정되어 있으며 겸직금지조항은 위원회의 독립성강화를 목표로 하였다. 立法者는 CNIL의 자율을 인정하여 위원의 적격여부를 개개 경우에 결정할 가능성을 이 委員會에게 부여하였다.[55] 그리고 行政府는 이 위원회에 정부공무원을 파견한다. 수상이 지명하여 파견한 공무원은 CNIL내에서 정부를 대표한다. 이러한 공무원은 CNIL에 접수된 이의나 신고를 CNIL과 상담할 임무를 갖고 있다. 그러나 그는 어떤 拒否權을 갖고 있지 않기 때문에 그는 이 위원회에 파견된 정부의 대표에 불과하다. CNIL의 機能上 獨立은 法律的으로 보장되어 있다. 이에 따라서 委員會는 그 활동과 관련하여 어떤 지시도 받지 않는다. 그리고 委員會의 특수성을 인식한 立法者는 어떤 國家機關으로부터 지시를 받지 않는다는 것뿐만 아니라 CNIL의 구성원들은 그를 임명하고 선출한 기관으로부터도 지시를 받지 않는

53) Evangelia Mitrou, a.a.O., S. 203.

54) 위원회의 위원은 하원(2명), 상원(2명), Wirtschafts- und Sozialrat(2명), Staatsrat(2명), Kassationshof(2명), 감사원(2명)으로 구성되어 있는 바, 이러한 구성원들은 해당기관의 총회에서 선출된다.

55) Evangelia Mitrou, a.a.O., S. 205.

다는 것을 확정하였다.[56] 立法者에 따르면 委員會의 구성원은 결코 특수한 이해관계나 그를 임명하거나 선출한 기관의 대표로 인식해서는 안된다는 것이다. 그러나 立法者는 委員會를 法院의 통제밑에는 있도록 하였다. 따라서 이렇게 독립된 기관이 모든 법적 통제를 벗어나려고 하는 곳에서 行政法院은 시민의 보호자로서 그리고 CNIL과 충돌할 수 있는 이익의 보호자로서 역할을 맡아야 한다.[57]

國家情報處理自由委員會의 독립성을 보장하기 위한 조건으로서 立法者가 이러한 위원회를 合議制機關으로 형성하였다는 것과는 별도로 이러한 구조가 과연 효율적인가는 그 활동과 관련하여 판단해야 한다.[58] 우선 合議制機關이 어떤 결정을 내리는 것과 관련하여 특히 많은 문제점들이 나타난다. 공동상담, 공동결정, 공동책임은 충돌하는 견해들간 타협을 모색하도록 하는 결과를 갖고 있기 때문에 결국 抽象的으로 合議制構造에 찬성하거나 반대하는 게 아니라 合議制的 情報保護機關으로서 CNIL이 어떠한지를 분석해야 한다. 機關의 獨立性에 관한 한 CNIL은 선출단체의 지시에 따를 위험을 막을 수는 있으나 개개 구성원의 직업적, 정치적 성향 때문에 이러한 단체들로부터 절대적으로 영향을 받지 않는다고는 말할 수 없다. 이러한 의미에서 CNIL은 영향을 받지 않는 게 아니라, 절대적이지 않은 다양한 영향을 받는다고 말할 수 있다. 이에 따라서 個人情報를 보호하기 위하여 合議制構造가 적합한지를 평가하기 위해서는 일반적으로 사회에서 統制機關을 어떻게 인식하는지에 특별한 의미가 속한다. 統制機關이 그 활동의 受信人과 여론으로부터 독립되고 효율적인 기관으로 파악된다면 비로소 統制機關은 그 정당성을 획득한다. 그러나 CNIL의 구성이 個人情報를 보호할 수 있는지는 여러 측면에서 의심된다. 우선 이렇게 큰 위원회가 비관료적으로 활동할 수 있다는 것이 의심된다. 두 번째로 專門家의 시각에서 볼 때 委員會의 구성이 결코 최상의 해결책이 아니라는 것이다.[59] 그 다음으로 국회의원의 포함을 언제나 긍정적으로 평가할 수만은 없다. 물론 CNIL에 國會議員이 포함된다는 것의 의미를 과소평가해서는 안된다. 확실히 民主國家에서

---

56) 정보보호법 제13조.

57) 또 다른 중요한 문제는 法官이 효율적 정보보호시각으로부터 정보통신정책영역으로까지 그 심사를 확대해야만 하는가? 아니면 합법성 및 裁量을 넘어섰는지라는 심사로 한정되어야 하는지이다. 이와 관련하여 우선 법관이 정보처리와 같은 특수하고 새로운 문제들을 처리할 수 있는지, 이러한 문제를 충분하게 파악하고 평가할 수 있는지에 문제가 있으며 게다가 재판이란 절차가 이렇게 급속도로 발전하는 기술에 관하여 부적합한 방법일 수 있다는데에 문제가 있는 것이다.

58) 합의제구조의 장점으로는 ① 영향을 받기 어렵거나 힘들다. ② 이에 따라서 공정성확보, ③ 구성원의 다양한 경력 때문에 다양한 문제의 해결이 가능하다는 것을 들 수 있으며 단점으로는 ① 덜 신속하고 비용이 많이 든다. ② 작업과정이 길어짐으로 덜 탄력적이라는 것을 꼽을 수 있다.

59) 예를 들어 정보처리전문가의 숫자가 너무 적으며 구성원의 3/1 이상을 법관이 차지한다.

議會는 정보통신정책에 관한 계획을 수립할 때 중요한 역할을 한다. 그럼에도 불구하고 CNIL과 입법부간에 이러한 연결이 CNIL의 과제수행에 적극적으로 작용하는지는 의문시된다. 다시 말하자면 이를 통하여 오히려 위원회가 정치화될 위험성이 존재한다는 것이다.[60] 결국 이는 個人情報를 보호하기 위한 기관의 통제효율성을 떨어뜨리는 쪽으로 이끈다. 곧 마찰 없는 활동과 委員會의 권위를 보장하기 위하여 내적으로 타협할 경향이 나타나게 되고 자연적으로 갈등들은 내면화된다. 獨立性의 또다른 중요한 측면인 재정적인 면을 살펴본다면 CNIL이 이러한 측면에서 자율성을 누린다는 것은 사실이다. 물론 CNIL은 예산에 관하여 監査院의 통제 밑에 있기는 하다. 그러나 위원회의 과제이행을 위하여 필요한 예산은 현실적이고 행정적 이유들 때문에 法務部의 豫算으로부터 나온다. 그런데 현실적으로 委員會는 財務部와 그 豫算을 상담하고 예산액에 관하여는 예산의 틀 속에서 議會가 결정한다. 어쨌든 委員會의 자치행정에도 불구하고 CNIL은 재정문제에 관한 한 국가로부터 영향을 받을 수 있다.[61]

d) CNIL의 機能과 權限

프랑스에서 個人情報保護法을 만든 立法者는 公的 領域에서 사용되는 주요한 개인정보시스템들의 규제에 우선적으로 관심을 가졌다. 그래서 國家情報處理自由委員會의 기본적인 목적은 個人情報에 관한 情報處理를 감독하는 것이었다. 그러나 프랑스에서 國家情報處理自由委員會는 이를 넘어서서 法律上 독립된 行政機關으로서 法規命令制定權限, 干涉權限, 統制權限을 갖고 중개, 조정, 공동작업을 한다. 따라서 이 위원회의 권한과 조직구조는 고전적인 국가기관인 立法府, 司法府, 行政府로부터 구별되는 뚜렷한 특징을 갖고 있다. 이 委員會의 조직은 이 위원회가 갖고 있는 다양하고 광범위한 권한들속에서 이해가 가능하다. 우선 프랑스의 統制機關은 정보시스템의 설치에 관하여 허가하는 권한을 갖고 있다. 이에 따라서 公的 領域에서 이러한 정보시스템의 설치는 法律에 근거한 경우에만 허용된다. 國家情報處理自由委員會(CNIL)의 공식입장에 따르면 公的 機關에서 정보사용은 法律이나 法規命令을 통하여 승인된다. 그런데 公的 領域에서 행해지는 정보처리에 관한 의견을 제시할 때 CNIL의 가장 기본적인 관심사는 "公正性" 또는 정보의 전달은 물론 특정 시스템에서 수집되는 個人情報의 사용을 사전에 확립한다는 것을 뜻하는 "最終使用原則"이다. 다만 非公的 領域에서 행해지는 정보처리에 관해서는 형식적인 신고만을

60) Evangelia Mitrou, a.a.O., S. 214.

61) 다른 나라들에서처럼 CNIL의 예산을 확보하는 방법은 그 독립에 관하여 중요한 것이다. 실제로 CNIL은 Ministry of Finance와 그 예산을 협상한다.

규정하고 있다.[62] 이는 스칸디나비아국가들의 경험을 고려하여 명백히 개인의 私的 領域이나 基本權을 침해하지 않는 情報處理는 엄격한 許可시스템의 적용을 받지 않도록 하였다는 것을 뜻한다. CNIL은 이러한 범주들을 결정하기 위하여 이에 관한 단순규정들을 만들었는 바, 해당 정보처리기관의 의무는 이 속에 담겨 있다.[63]

결국 許可시스템과 申告시스템의 채택, 자세한 실체법규정과 범위 구체적인 규정들의 缺如 그리고 마지막으로 公的 領域과 私的 領域 전체에서 정보처리의 통제를 통하여 이 國家情報處理自由委員會가 프랑스 情報保護法의 중심축이라는 것을 알 수 있다. 더 나아가서 立法者는 CNIL에게 전산자료에 관한 기록자와 통제자의 역할만이 아니라 법적용역할 또한 인정하였다. 이에 따라서 CNIL은 法規命令制定權限을 통하여 이 분야의 법적 발전에 참여하게 된다. 그런데 CNIL에 法規命令制定權限의 부여는 CNIL의 가장 본래적인 특징중 하나를 설명한다. 委員會의 이러한 권한이 행정부의 법규명령제정권한을 보충하는 것이 아니라 대체한다는 것 속에 어떤 새로움이 존재한다. 따라서 法律에 이미 규정된 경우에는 行政府의 法規命令制定權限이 배제된다. 또한 CNIL의 자율성을 보장하면서 동시에 이를 확실하게 하기 위하여 CNIL에게 해당직무규정을 스스로 만들 가능성을 情報保護法은 인정하였다. 이러한 內部規則制定權限과는 별도로 시스템안전영역에서 CNIL은 폭넓은 간섭권한들을 행사하면서 정보처리시설의 안전보장에 관한 모범규정들을 만들고 이에 관한 안전조치들을 규정할 수 있다. 특히 이에 따라서 명백히 개인의 私的 領域이나 基本權을 침해하지 않는 아주 일상적인 정보처리에 관한 단순규정들을 만들 과제와 권한이 CNIL에게 부여되었다는 것에 주목해야 한다.[64] 이에 따라서 立法者는 표준화된 절차 및 이에 해당하는 규정들을 事前에 제정하는 것 대신에 명백히 관련자에게 위험하지 않은 정보처리에 관한 규칙을 확정할 책임을 CNIL에게 부여하였던 것이다. 그럼에도 불구하고 이러한 權限은 과대 평가되어서는 안된다. 오히려 다른 관점에서 본다면 입장표명을 통하여 法律制定節次에 CNIL이 참여하는 것이 규범제정에 관한 이 위원회의 권한보다는 더 큰 영향력을 갖고 있다. 公的 領域에서 정보시스템설치에 관한 계획을 수립할 때 委員會가 포함된다는 것은 적절한 상담의 제도화 또는 정보처리계획 및 정보처리의 합법성을 사전적으로 보장한다는 것을 의미할 뿐만 아니라 이에 관한 CNIL의 입장표명 또한 국가정보정책을 함께 형성하는 중요한 작용을 하는 것이다. CNIL의 이러한 입장표명을 통하여 委員會는 정보처리목적의 정당성 및 정보처리기관의 과제에 관하여 심사한다. 물론 위원회의 이

62) 정보보호법 제16조.
63) 정보보호법 제17조.
64) 정보보호법 제17조.

러한 입장표명은 法的 拘束力을 갖고 있지 않기 때문에 무시될 수 있음에도 불구하고 구속력이 없는 이러한 입장표명을 행정부가 대체로 존중한다는 것을 기억해야 한다. 또한 CNIL은 의회의 立法節次에 참여한다. 곧 法律에 근거하여 정보처리시스템이 설치되려면 事前에 CNIL과 상담해야만 한다. 이 상담이 끝난 후에 CNIL의 입장표명이 붙여진 法律草案이 의회에 제출된다.

그리고 프랑스의 情報保護法上 人種과 같은 민감한 個人情報를 수집하고 저장하는 것은 일반적으로 금지되고 이러한 정보수집을 위해서는 사전에 통지된 관련개인의 同意를 필요로 하며 특히 宗教, 정치적 신념 등에 관한 정보수집은 그 사람의 명시적인 書面同意를 필요로 한다. 그리고 관련개인으로부터 이러한 同意를 받기 위해서는 어떤 個人情報를 원하는지와 응답자들이 자신의 정보에 관한 접근권과 교정권을 갖고 있다는 것 등을 이들에게 말해주어야만 한다. 또한 安保領域과 軍事領域에서 CNIL이 담당했던 중요한 문제들중 하나는 어떠한 종류의 민감한 個人情報들이 수집될 수 있는지를 결정하는 것이었다. 1981년에 CNIL은 國防部의 정보시스템을 분석한 다음에 개인들은 잊혀질 권리를 갖고 있으며, 16세 이하의 個人에 관한 情報는 어떤 情報이든간에 저장되어서는 안되고, 저장기간도 事前에 결정되어야만 한다는 것을 근거로 하여 일부 항목들은 삭제되어야 한다고 결정하였다.[65] 이에 따라서 민감한 것으로 분류되는 개인관련정보는 보통의 개인관련정보보다 더 특별하고 강력한 보호를 누린다. 예를 들어 범죄행위, 前科 등에 관한 개인관련정보는 제한된 범위의 公的 機關이나 CNIL의 동의를 얻어서 公的 課題를 담당하는 機關만이 처리하여도 된다.[66] 또한 민감한 個人情報를 특별하고 강력하게 보호하기 위하여 情報保護法에는 이러한 정보처리의 금지에 관하여 예외를 인정하는 CNIL의 동의입장표명을 필요로 한다고 규정되어 있다.[67] 이러한 경우에 관하여 판단하는 委員會에게 중요한 권한이 부여되어 있음은 당연하다. 行政府는 CNIL의 입장표명을 요청하여야 할 뿐만 아니라 계획된 정보처리를 포기하거나 새로운 협상을 요청하지 않는 한 行政府는 CNIL의 이러한 견해표명에 따라야 한다. 결국 정보보호법을 살펴보면 프랑스의 立法者는 CNIL을 통제기관으로 인식하였을 뿐만 아니라 이익형량을 하는 기관으로 또한 인식하였다는 것을 알 수 있다. 더 나아가서 CNIL은 독자적으로 민감한 個人情報의 처리금지에 관한 예외를 제안할 수 있으며 CNIL의 판단에 따라 자동화되지 않은 개인자료가 개인의 권리보호를 위협한다면

65) David H. Flaherty, ibid., p.219.

66) 직간접적으로 인종, 정치적, 종교적 신념이나 노동조합소속여부를 인식하게 하는 개인관련정보의 경우에는 저장금지명령이 유효하다.

67) 정보보호법 제31조제1항.

이러한 기록에 법규정들의 확대적용을 제안할 권한을 갖고 있기까지 하다. 이러한 경우에 CNIL은 수작업처리정보에 위 정보보호법규정의 확대적용여부를 결정하는 유일한 기관이다. 그리고 국경을 넘는 정보전달의 경우에 CNIL이 또한 이에 관한 제안권을 가질 수 있으며 국제간 정보흐름을 승인하거나 이에 관한 특별규정을 제안할 수 있다.[68] 그럼에도 불구하고 정부는 CNIL의 제안에 반드시 따라야 하는 것은 아니다. 다만 個人情報를 보호하기 위하여 이 國家情報處理自由委員會가 개입할 수 있는 이러한 제안권은 오히려 상담기능에 속한다는 것을 인식하여야 한다. 따라서 이는 法的으로 拘束力 있는 상담이 아니라 법규정들의 해석 및 구체화, 그리고 지침들의 확정에 관한 것이다.

결국 이러한 설명을 통하여 프랑스의 정보통제시스템이 사전통제시스템이라는 것을 알 수 있다. 그래서 프랑스의 情報保護法은 CNIL에게 매우 폭넓고 법적으로 거의 제한되지 않는 통제권한을 부여하였다. 이에 따라서 公的 領域은 물론 私的 領域에서도 통제를 수행할 권한을 CNIL은 갖고 있다. 이러한 권한을 수행하기 위하여 CNIL은 광범위한 설명권과 열람권을 갖고 있으며 CNIL의 작업을 돕기 위한 모든 조치를 취할 의무가 정보처리기관에게 부과되어 있다. 또한 프랑스의 立法者는 개인관련정보를 처리하는 기관으로부터 시민을 보호하기 위하여 CNIL이 개개 시민이나 시민단체로부터 이의를 접수하고 시민의 설명요구가 부당하게 제한되지 않도록 CNIL이 감독하도록 하였다.[69] 또한 정보처리활동을 시민이 파악할 수 있도록 하기 위하여 CNIL은 자동화된 개인정보시스템에 관한 기록을 갖고 있으며 이러한 기록은 모든 사람들이 이용할 수 있는 것이다.[70] 신청인이 이러한 기록에 접근하는 것이 부인되는 경우에 CNIL의 委員長은 이에 관하여 심사하도록 위원중 한 명을 선발한다.[71] 이 위원은 개인에게 무엇이 전해질 수 있는지를 결정할 권한을 갖고 있다. 이렇게 개인의 권리를 보호하는 것이 CNIL이 履行해야만 하는 중요한 영역중 하나에 속한다.

프랑스 통제시스템의 또 다른 특징은 情報處理와 관련된 결정들에 통제기관이 참여한다는 것이다. 이를 위하여 우선적으로 CNIL에게 고전적인 간섭권한과 결정권한들이 부여되어 있다. 그 다음으로 CNIL은 연례활동보고서를 대통령과 의회에 제출해야만 한다.[72] 이러한 연례보고서는 다양한 목적들을 갖고 있다. 일반적으로 이

68) 정보보호법 제24조제1항.
69) 정보보호법 제35조. 입법자에 따르면 CNIL은 시민의 변호사가 아니라 충돌하는 이해관계의 조정자로 이해된다.
70) David H. Flaherty, ibid., p.204.
71) 정보보호법 제39조.
72) 정보보호법 제23조.

러한 활동보고가 정보통제 및 간접적인 압력수단으로서 작용하는데 반하여, 프랑스의 情報保護法은 CNIL의 이러한 보고서를 CNIL가 담당하는 과제의 수행에 관한 보고서로 이해하고 있다. 이러한 법규정에 따라서 立法者가 이 위원회의 작업형태 및 조직의 투명성에 중점을 두고 있다는 것을 알 수 있다.[73] 다른 나라들처럼 CNIL 또한 정보보호문제에서 경종을 울리기 위하여 여론매체에 특히 의존한다. 따라서 여론매체 등을 통한 여론과 접촉이 CNIL에게 원조수단으로 봉사해야만 한다. 예를 들어 CNIL이 보기에 어떤 國家機關의 法律違反이 존재하는 경우에 이러한 정보처리기관에게 CNIL이 발할 수 있는 경고는 刑事法的 意味에서 制裁가 아니라 오히려 도덕적 종류의 제재성격을 갖는다. 이러한 경고는 정보처리기관의 違法을 지적하고 정보처리기관에게 이를 제거하도록 공식적이고 확정적으로 요구하는 것이다.[74]

e) CNIL의 統制政策

결국 CNIL은 情報社會에서 궁극적으로 국가의 과제수행과 시민의 권리간 조화를 목표로 한다. 그래서 CNIL은 우선적으로 타협책을 모색하게 되고 그러다 보니 이 위원회가 결정한 대부분의 결정은 행정부의 시스템설치계획에 찬성하였다.[75] 이러한 것을 통하여 이 위원회가 個人情報의 處理를 제한하려는 게 아니라 人權, 私的 領域, 개인적 자유 또는 공적 자유를 제한하지 않는 정보통신기술의 발전에 관한 틀을 제시하려 하였다는 것이 명백하게 나타난다. CNIL이 행정부의 시스템설치에 반대하는 입장표명을 한 경우는 드물었다. 반대하는 입장표명중 많은 경우는 특히 安全規定의 缺如 또는 保障의 缺如에 근거하였다. 또 저장기간의 불명확, 전달되어도 되는 정보의 불명확성이 반대입장표명의 또 다른 이유였다. 계속해서 위원회는 서로 관련이 없는 정보의 연결을 금지시켰다. 또한 정보처리의 필요성과 목적합치성이라는 관점에서 정보처리계획을 금지시킨 CNIL의 몇몇 결정이 이러한 측면에서 중요한 의미를 갖는다.[76] 이와 같은 결정을 내릴 때 CNIL은 이익형량을 抽象的으로 하지 않는다. 곧 CNIL은 현행법규정에 근거하기는 하나 현행법을 技術的, 經濟的, 社會的 文脈 속에서 적용한다. 여기서 社會的, 經濟的, 技術的 文脈을

73) Evangelia Mitrou, a.a.O., S. 199.

74) 경고(Warnung)는 어떤 행정결정을 형성하지는 않는다. 이러한 경고는 어떤 직접적인 법작용을 발현하지는 않으나, 해당기관에게 법률 및 CNIL의 결정들을 준수하도록 유도한다.

75) 거부하는 입장표명은 아주 작았다. 예를 들어 1990년 한해에 전체 입장표명(7716)중 28건에서만 반대의견을 표명하였다.

76) 몇몇 경우들에서 계획된 정보처리에 동의하지 않았다. 계획된 정보처리의 합법성을 판단할 때 CNIL은 법률뿐만 아니라 행정법원칙들, 개인정보보호에 관한 EU지침, 평등원칙과 같은 기본권들도 고려한다.

함께 고려한다는 것은 제기되는 정보처리의 필요성 또한 고려하고 검토한다는 것을 뜻한다.

그런데 입장표명이든 권고든 간에 CNIL이 내리는 결정은 일방적이고 권위적인 절차의 결과가 아니라 대부분 CNIL과 이해관계기관간 협상의 결과이다. 우선 CNIL은 行政과 私的 領域에서 정보처리기관을 대표하는 그룹이나 단체와 접촉한다. 그리고 CNIL은 위원회의 입장표명이나 권고를 하기 이전에 또는 情報保護法 제17조에 따른 단순규정을 결정하고 이를 공표하기 이전에 이해당사자와 협의한다. 이러한 협의방식은 프랑스 정보보호모델의 특징이다. 이러한 작업방식은 탄력적이지 않은 法律을 구체적인 상황과 필요성에 적응시킴으로써 국가의 간섭을 최소화하려는 의도 또한 갖고 있는 것이다. 이해관계가 충돌하는 경우에 CNIL이 택하는 결정들을 보면 이러한 결정들에서는 특히 융화적 입장이 두드러진다. 결국 이는 CNIL이 대립되는 이해관계들간에 조정을 하려고 노력한다는 것을 뜻한다. 그렇다면 委員會의 과제의 성격, 그 작업방식에 근거하여 CNIL의 행동방법이 억제가 아니라 예방을 지향한다는 것을 알 수 있다. 따라서 委員會는 강요하기보다는 설득하려고 하며 예외적인 경우에만 극단적인 관철수단과 간섭권한을 행사하려고 하였다. CNIL 스스로가 法的으로 拘束力 있는 제한권한들의 투입보다는 경고, 협의, 권고라는 非法的이고 온화한 수단이 더 커다란 영향을 행사할 수 있다고 주장하였다. 위원회가 억제대신에 예방을 선호하는 것은 특히 검찰에 신고하는 것과 관련된 CNIL의 방침에서 관찰할 수 있다. 곧 검찰에 신고하는 방법을 CNIL은 아주 드물게 사용한다.[77] 스스로를 調停者로 생각하고 협상하려고 하는 기관이 억제적 수단의 투입을 꺼릴 수 밖에 없다는 것은 이해할만하다. 그럼에도 불구하고 이러한 CNIL의 정책은 많은 비판에 부딪혔다.[78] 어쨌든 1984년이후에 CNIL은 계속해서 이러한 방법을 사용하였는 바, 특히 이는 민감한 정보의 위법한 저장, 法律上 要求되는 형식과 目的拘束의 非遵守와 관련되는 분야들에서 그랬다. 그런데 정보처리기관이 CNIL에 협조해야만 한다는 것은 委員會의 활동을 위하여 중요한 역할을 맡는다. 우선 情報處理가 違法일 경우에 관련자에게 경고할 권한이 법에 따라서 CNIL에게 인정된다. 委員會로부터 특정 정보처리가 違法行爲라고 公的으로 언급되는 한 이러한 경고는 하나의 制裁일 수 있으며 여론매체 등에 法律違反事項이 보도된다면 이러한 경고는

77) 매우 드문 경우에만 형사제재를 가하고자 하였다. 위원회의 초창기에는 아예 이러한 수단의 사용이 포기되었다.

78) 이러한 신고를 하나의 가능성으로만 생각하는 위원회에 대하여 신고가 법적 의무라는 견해가 강력하게 대립된다. 법률에 대한 위반의 양적, 질적 증가와 CNIL의 소극성에 대한 비판이 CNIL이 더 강하게 행동하도록 요구하고 있는 실정이다.

관련자에게 심각한 영향을 줄 수도 있다. 이러한 이유 때문에 CNIL은 이러한 수단의 사용에 소극적이거나 조심스럽게 사용하였다. 1983년 이후로 相談과 勸告를 통하여 만족할만한 해결책이 나오지 않는다면 CNIL은 책임자에게 경고를 하였다. CNIL이 이러한 경고를 발하는 가장 흔한 사례는 어떤 기관의 情報處理가 원래 목적으로부터 벗어나는 경우이다. 이를 넘어서서 CNIL의 반대입장표명이 받아들여지지 않았을 때 委員會는 또한 警告手段을 사용한다.

그리고 이 위원회가 수상과 의회에게 매년 제출하여야 하는 活動報告書는 다음과 같은 두 가지 역할을 갖는다. 한편으로 이 活動報告書는 CNIL에게 立法府와 行政府 그리고 시민에게 CNIL의 활동결과와 정보기술 및 정보보호의 발전에 관하여 보고할 수 있는 정보통로를 제공한다. 다른 한편으로 이 報告書를 통하여 CNIL활동의 투명성이 보장된다. CNIL의 활동에서 간섭권한의 행사보다 상담과 설득이 더 큰 의미를 갖는다는 것으로부터 출발한다면 이러한 活動報告書의 가치를 과소평가해서는 아니된다. 발생된 문제들 및 관련되는 입장들의 설명을 통하여 이미 國家機關이나 私的 領域에서 이에 관한 토론의식이나 문제의식이 발전된다. 이러한 報告書에서 委員會는 보고연도의 중점사항을 제시한다. 그리고 위원회는 이 報告書에서 통제되는 정보시스템들의 주요특징과 문제점을 설명한다. 또한 이러한 活動報告書에는 委員會의 모든 결정들, 처리과정 및 방법에 관한 자세한 설명들이 있는데 이들이 중요한 정보가치를 갖는다. 위원회의 활동에 관한 자세한 설명과 다양한 사례설명을 통하여 CNIL은 주로 다음과 같은 기능을 하고자 노력한다 : 곧 법을 적용하고 정보시스템을 구축할 때 문제에 관한 자세한 보고를 통하여 情報處理機關에게 동일하거나 유사한 事案에 관한 정보를 제공하려고 위원회는 노력한다.

마지막으로 CNIL은 壓力團體나 情報處理에 관한 항의나 반대를 주도하는 단체로서가 아니라 정보처리에 관한 경고장치와 자극장치로서 이해된다. 따라서 CNIL은 특히 여론매체와 협력을 강조한다. 그리고 委員會의 활동을 언론에 알리고 대학, 학회와 같은 단체와 함께 세미나, 학술대회를 개최하며 강연회 등에서 위원회의 활동을 홍보하고 個人情報保護의 중요성을 강조하며 委員會와 情報保護에 관한 소개책자와 안내책자를 만든다.

f) CNIL에 관한 評價

프랑스의 통제모델에 관한 판단은 결국 CNIL의 효율성문제에 관한 것이다. 일단 행정부가 시민의 이익들을 고려하도록 하는 데에 CNIL이 성공했다는 것은 확인된다. 그리고 개인의 자유를 보호하는 법규정들을 만들려는 CNIL의 노력은 커다란 정도로 성공적이었고 특히 個人情報를 보호하도록 法律들이 개정되었고 구체화되었

다는 것 또한 확실하다. 그러나 CNIL의 주장들이 대립되는 정치적 이익들과 충돌한다면 CNIL은 많은 경우에 좌절을 경험하였다. 예를 들어 身分證明書의 자동화에 CNIL이 반대하지 못하였고 시민들에게 포괄적인 설명권을 보장하려는 CNIL의 노력 또한 실패하였다. 특히 國家安保나 公共安全과 같은 영역에서 CNIL은 그 역할 및 효율성에 관하여 많은 비판에 부딪쳤다. 어쨌든 CNIL의 다양한 활동이 목표로 하였던 가장 중요한 목표는 정보처리시스템의 투명성형성을 꼽을 수 있다.

프랑스에서 CNIL은 個人情報保護機關으로 개념정의되지 않았으며 위원회의 임무는 단순히 시민의 보호나 事前的, 事後的인 情報保護로 축소되지 않는다. 오히려 이 위원회는 여러 이해관계들간 조정 및 사회적 합의산출에 노력하여야 했다.[79] 따라서 CNIL은 個人情報에 관한 보호를 法的으로 統制하기 보다는 이를 정치적으로 해결하기 위하여 만들어진 政治的 機關이다. 따라서 CNIL은 결정을 내리기 보다는 타협과 절충을 모색한다. 결국 CNIL과 같은 合議制機關은 다양한 견해들간에 대립을 조정하고 일치시킬 그러한 능력에 결정적인 정도로 그 효율성이 의존한다. 그러다보니 個人情報保護問題를 판단할 때 合議制機關으로서 CNIL은 어느 한쪽에 손을 들어주기 보다는 양자의 입장을 조정하고 교정하는 것으로 그 역할을 이해하였다. 그렇다면 CNIL은 이미 처음부터 調停機構로 개념정의되었던 것이다. 그렇다면 CNIL의 制度的 役割은 우선적으로 시민과 국가권력간 조정 속에 있다.

CNIL 스스로는 그들의 과제수행에 관하여 전체적이고 전반적으로 만족스러운 것으로 평가하나 CNIL의 활동과 정책을 전체적으로 판단한다는 것은 어려운 과제에 속한다.[80] 왜냐하면 이 위원회의 효율성은 여러 측면들로부터 판단될 수 있기 때문이다. 우선 CNIL에게 포괄적이면서 어려운 여러 다양한 과제들이 부여되어 있다. 예를 들어 統制機關과 電算情報記錄機關의 역할을 넘어서서 CNIL에게 정보기술적용의 결과를 관찰하고 이러한 기술발전이 법에 적응하도록 하기 위하여 해당하는 조치들을 제안하는 기능이 언급된다. 그런데 情報處理의 적용을 위한 이러한 事前的인 統制權限이나 상담과제 옆에 더 나아가서 위원회에게 準立法的 役割[81] 또한 부여되어 있다. 이를 통하여 한편으로 CNIL은 그들의 과제를 아주 넓게 파악한다. 그럼에도 불구하고 이 위원회가 맡고 있는 이렇게 방대한 양의 과제들이 오히려 CNIL가 수행하는 과제의 질과 효율성을 떨어뜨린다는데에 문제점이 있다. 결국

79) 정보, 정보은행, 자유에 관한 1978년 1월 6일의 프랑스법은 넓고 혁신적이다. 특히 이는 영미법계국가들의 시각으로부터 본다면 개인의 프라이버시보호나 감시통제를 훨씬 넘어서는 대단히 광범위한 사회문제들을 규율하도록 하는 내용을 담고 있다.

80) 실제로 처음 5년 동안에 CNIL은 새로운 정보시스템들을 위한 정부요구들에 응답하여 케이스 바이 케이스로 일하는 방식을 채택하였다.

81) 정보보호법 제17조.

CNIL의 정보보호정책과는 상관없이 정보처리의 전체영역을 담당하는 CNIL의 폭넓은 권한에 의하여 도대체 CNIL이 이러한 범위 전체를 통제할 수 있는지가 의심스러운 것이다.

그 다음으로 프랑스의 情報保護法을 제정한 立法者는 개인의 자유를 보호하기 위해서만 CNIL을 만들지는 않았다. 위원회는 다기능적 기관으로서 정보처리의 합법성을 통제하고 결정과 상담을 통하여 정보정책의 형성에 함께 참여하고 정보전달을 규율하고 국가권력들간 균형을 유지하도록 하며 시민과 국가간에 중재자로서 충돌을 극복해야만 했다. CNIL이 이러한 요구들을 현실적으로 만족시킬 수 없었다는 의미에서 CNIL의 폭넓은 권한들이 우선 단점으로 나타난다는 것은 명백하다. 왜냐하면 이러한 통제모델은 내재적으로 상호 대립하는 기능들을 갖고 있기 때문이다. 곧 決定機能은 정보제공기능 및 제안기능과 모순된다. 그런데 決定權限은 프랑스 통제모델의 주요특징인 바, 결국 이 위원회는 이러한 결정권한을 가짐으로써 行政府의 한 기관처럼 되어버린다. 이에 따라서 위원회는 個人情報保護라는 척도옆에 經濟的, 政治的, 行政的 必要性을 함께 고려하여야 한다. 이처럼 결국 CNIL이 조정기구의 역할을 맡는다면 도대체 프랑스에서 어떤 기관이 個人情報保護役割을 담당하여야 하는지를 묻게 된다.

게다가 이러한 CNIL은 대부분의 경우에 정부와 충돌하는 것을 원하지 않는다. 프랑스는 매우 관료화된 중앙국가로서 이러한 중앙화와 관료화는 정부가 보유하는 정보시스템들에 의한 감시를 통제하는 데에 심각한 장애요인이다.[82] 문제는 委員會가 개인의 私生活을 보호하는 데에 집중하기 보다는 정치적 견해들이 다루어지고 토론되며 이에 관한 합의를 도출하는 작은 의회형태로 기능한다는 것이다.[83] 스웨덴이나 캐나다와 같은 나라들은 情報保護委員會가 정치화되는 것을 피하기 위하여 이익형량의무를 立法府에 넘기는 반면에 프랑스의 情報保護法은 어려운 사건들에서 충돌하는 이익들을 형량하기 위한 책임을 CNIL에 부과한다. 그래서 CNIL의 문제별 접근방식은 국가정보실무의 체계적인 검토를 어렵게 만든다.

결국 법에 의하여 부과되는 대단히 넓은 제정법상 命令 및 許可制度, 위원회에 정치적 대표들의 존재 때문에 특히 개인의 권리보호에 관한 한 CNIL의 효율성은 크게 떨어진다. 그렇다면 프랑스의 情報保護法은 비교적 잘 정비된 것이나 문제는 이러한 법의 執行機關이 부적절하다고 말할 수 있다.[84]

---

82) David H. Flaherty, ibid., p.170.
83) 1986년말까지 정부에 반대하는 단지 7개의 부정적 결정들만이 행해졌을 뿐이다.
84) David H. Flaherty, ibid., p.237.

2) 相談시스템

(1) 캐나다

a) 組 織

1982년에 제정된 연방프라이버시법은 1983년 7월 1일 효력을 발생하였다. 이 법은 캐나다인권법 4장의 프라이버시규정들을 보충하고 公的 領域에서 공정한 정보실무원칙을 도입하였으며 프라이버시위원을 규정하였다. 캐나다의 연방프라이버시법은 연방정부에 의한 個人情報의 수집과 사용을 규율한다. 특히 이 법은 프라이버시위원을 독립된 機關으로 만들고 그 감독 및 감사권한을 상당히 강화하였다. 다만 프라이버시위원의 활동이 個人情報保護에 관한 것이라 할지라도 그 역할은 諮問的일 뿐이고, 감독권한은 2차적이다. 따라서 정부의 情報處理에 관하여 충돌하는 이익들간 형량임무는 캐나다에서 議會가 담당한다.

위에서 설명된 것처럼 캐나다의 연방프라이버시법은 프라이버시위원의 독립을 크게 강화하였다. 캐나다인권법하에서 人權委員會의 모든 구성원들은 정부에 의하여 임명된다. 이 委員會議長의 추천에 의하여 法務部長官이 이 구성원들중 한 명을 프라이버시위원으로 지명한다. 그런데 프라이버시위원은 의회가 선출하지 정부에 의하여 직접 임명되지 않는다.[85] 따라서 프라이버시위원은 議會에게만 책임을 진다. 프라이버시위원의 임기는 7년이고 連任할 수 있다.[86]

b) 權 限

우선 프라이버시위원은 개개 시민의 불평을 조사하고, 司法審査에 참여하며, 議會에 활동상황에 관하여 보고한다. 결국 情報通信技術의 계속적 발전에 대응하여 個人情報를 보호하기 위하여 감독하는 것이 프라이버시위원의 주요 임무이다. 다만 연방프라이버시법은 國家機關들의 정보처리를 열람하고 조사하도록 위원의 權限을 확대하였으나 프라이버시위원의 권한은 勸告的일 뿐이다. 따라서 프라이버시위원은 國家機關에게 어떤 것을 명령하지 못하고 설득에 의존하여야 한다. 그리고 프라이버시위원은 개인정보시스템들을 허가하거나 기록하지 않는다. 그러나 프라이버시위원은 個人情報의 수집 및 사용을 다루는 연방프라이버시법규정들의 위반여부을 조사할 때 이에 관한 주도권을 가질 수 있다. 추가로 警察의 개인정보시스템은 프라이버시위원으로부터 특별한 통제를 받는다. 그래서 個人情報의 어떤 민감한 사용에

85) 연방프라이버시법 제53조 1.
86) 연방프라이버시법 제54조 2 참조.

관하여 프라이버시위원에게 통지하도록 규정한 중요한 제정법규정들이 있다. 이러한 특별법규정은 個人情報의 합법적인 사용을 프라이버시위원이 심사하도록 허용한다. 이에 따라서 법규정에 의해서 자동적으로든 또는 개인의 요구에 의해서든 프라이버시위원은 어떤 민감한 個人情報公開를 검토할 수 있다.[87] 그리고 프라이버시위원은 이러한 경우에 정보가 관련되는 개인에게 통지할 재량을 갖고 있다.[88]

연방프라이버시법 제60조에 따르면 개인의 프라이버시보호와 관련되어 프라이버시위원은 특별한 조사, 감독을 위하여 우선 法務部와 협의해야만 하며 이에 관하여 나중에 의회에 보고하여야 한다. 게다가 프라이버시위원은 개인정보시스템들을 감사할 수 있다. 실제로 1985년에 개인의 접근이 배제되었던 대규모 정보은행중 몇몇에 대하여 프라이버시위원이 감사하였는데 이러한 감사판단의 기준은 저장된 個人情報의 量과 非中央化與否였다.

그리고 情報銀行 속에 저장되거나 획득되는 個人情報의 목적과 이러한 정보의 사용이 일치하여야 한다는 설명을 기록목록이 담고 있어야 하고 프라이버시위원은 이러한 목록의 정확성과 범위를 감독하고 목록상 결함에 대한 불평을 조사한다. 프라이버시위원의 이러한 활동들은 더욱이 안보기관의 민감한 기록들도 포함하였다.

그런데 캐나다의 연방프라이버시법에 의하면 자신의 권리가 보호받지 못하였다는 個人의 이의제기는 원칙적으로 1년 이내에 서면으로 제출되어야 한다. 그러나 위원은 이러한 불평의 접수없이도 調査를 시작할 수 있다. 따라서 이는 개인의 불평에 의존하기보다는 위원들에게 독립적으로 조사할 권한이 부여되어 있다는 것을 뜻한다.[89] 이러한 監督能力의 적극적인 사용은 國家에 대한 성공적인 통제를 확보하기 위하여 매우 중요하다. 추가로 연방프라이버시법은 프라이버시위원이 國家機關들의 불평을 조사하도록 허용한다. 그런데 1977년부터 연방프라이버시법은 개인에게 자신의 정보에 접근할 권리를 인정하였으며 1982년에 개정된 연방프라이버시법은 個人情報를 관련개인에게 제공하지 않는 國家機關의 결정을 聯邦法院이 심사하는 것을 허용하였다.[90] 더군다나 이에 관한 立證負擔은 신청인이 아니라 國家에게 있다. 다만 개인의 접근권에 관한 法院의 審査를 허용하기 위한 유일한 전제조건은 이러한 개인의 접근이 거부되었다는 한 사람의 불평을 프라이버시위원이 첫 번째로 심사해야 한다는 것 뿐이다. 따라서 프라이버시위원이 정부의 입장에 동의한다 할지라도 法院의 審査는 행해질 수 있는 것이다. 또한 연방프라이버시법은 특정한 個人

87) 연방프라이버시법 제8조제4항, 제8조제5항, 제9조제3항, 제37조제1항.
88) 연방프라이버시법 제8조제5항.
89) 연방프라이버시법 제31조~제37조.
90) 연방프라이버시법 제41조.

情報銀行을 개인의 접근으로부터 배제하고 이에 관하여 프라이버시위원이 분쟁을 조정하도록 규정한다. 그래서 이 법은 접근이 배제되는 정보은행속에 저장된 논란이 되는 個人情報에 관하여 프라이버시위원과 聯邦法院이 심사하도록 하였다. 프라이버시위원은 접근이 배제되는 은행들을 감사하고 어떤 개인파일은 이 속에 담겨서는 안된다고 정부기관의 長에게 보고할 수 있다. 프라이버시위원의 이러한 권고에 해당 機關의 응답이 부적절하거나 합리적 시간 내에 이루어지지 않는다고 위원이 결정한다면 그는 聯邦法院에 司法審査를 신청할 수 있다.

그리고 프라이버시위원이 議會에 제출하는 年例報告書는 정부의 정보처리에 관한 報告書이다. 더욱이 연방프라이버시법은 언제든지 위원의 권한, 의무, 기능들의 범위 내에서 어떤 긴급하거나 중요한 문제를 언급하거나 논평하는 특별보고서를 제출할 수 있도록 규정하였다.[91] 모든 國家機關의 長 또한 議會에게 보고하기 위하여 연방프라이버시법의 집행에 관한 年例報告書를 준비하여야 한다. 다만 유감스럽게도 이러한 보고서들에 우선적으로 특성상 통계적인 경향이 있다는 것에 주목하여야 한다.

(2) 독일의 情報保護機關

a) 組 織

獨逸 情報保護機關의 組織을 간단히 살펴보면 다음과 같다. 個人의 情報自己決定權을 보호하기 위하여 情報保護受任人이 중요한 의미를 갖는다는 것은 人口調査判決 以後에 聯邦憲法法院의 결정에서 반복적으로 언급되었다.[92] 이에 따라서 獨逸에서 情報保護受任人을 통한 統制는 연방의 모든 공공기관으로까지 확대되었으며 聯邦情報保護受任人은 그 권한행사시 독립적이고 法律에만 따른다.[93] 그러한 그의 지위는 法官과 비슷하다. 또한 聯邦情報保護受任人의 이러한 독립성은 국가기관의 어떤 지시로부터 자유를 뜻하는 바 이는 聯邦情報保護受任人이 어떤 職務監督下에 있지 않다는 것을 뜻한다. 聯邦情報保護受任人은 원래 議會에 속하는 統制機關으로 규정되어야 했으나 이는 憲法改正을 필요로 하는 사항이므로 聯邦政府에 속하도록 규정하였다.[94] 따라서 聯邦情報保護受任人은 聯邦內務省에 속한다. 그러나 이러한 소속이 그가 이 聯邦內務省의 한 부서이어야만 함을 뜻하지는 않는다. 연방내무성의 監督은 결코 受任人活動의 내용적 정당성이나 정치적 목적합치성을 검토할 가능

91) 연방프라이버시법 제38조, 제39조.
92) 예를 들어 BVerfGE 67, 185.
93) BDSG 제17조제4항제2절.
94) BDSG 제17조제4항제3절

성까지 포함하지는 않는다. 이 연방내무성의 監督은 聯邦情報保護受任人의 활동이 허용되는지, 그가 서류내용을 검토할 권한을 가지고 있는지와 관련된다. 聯邦情報保護受任人의 任期는 5년이다.[95]

b) 人口調査判決前 統制機關의 機能

1977년 독일에서 연방정보보호법을 제정할 때 행정부로부터 독립된 외부통제기관의 설치가 그 당시에 강하게 요구되었다. 왜냐하면 전통적인 법적, 정치적 통제 시스템의 기능상 한계, 국가활동의 질적인 변화 및 정보실무의 변화로 인하여 기존의 제도들을 통해서는 個人情報保護分野에서 등장하는 문제들을 극복할 수 없다는 인식이 매우 강하였기 때문이다.[96] 獨逸 聯邦憲法法院의 人口調査判決이 나오기전 정보보호법들(제1세대法律들)의 공통적인 특징은 간섭 및 명령권한들을 갖는 統制機關을 포기하였다는 것이다.[97] 왜냐하면 行政府에 대하여 지시권한들을 갖는 統制機關이 정부의 지시권한 및 의회에 대한 책임을 제한할지도 모른다고 우려하였기 때문이다. 이에 따라서 立法者는 설명, 추천, 상담, 제안을 통하여 여러 위험들을 분석하고 이를 제거하는데에 기여하여야 했던 독립된 상담기관의 설치에 찬성하였다. 이렇게 직접적인 간섭권한을 갖는 것을 포기하는 통제모델은 결국 統制機關이 민주적인 토론절차와 결정절차의 실현에 기여함으로써 행정관청을 통한 정보보호규정들의 준수여부를 통제하거나 감독한다. 이러한 과제의 효율적인 이행을 위하여 立法者는 統制機關들에게 그들의 과제를 이행할 때 이들에게 협조할 행정관청의 일반적인 의무를 넘어서서 정보보호수임인에게 설명, 열람 등을 제공할 의무를 부여하였다. 따라서 情報保護機關들의 통제과제는 情報處理가 잘못된 상황에 있는지, 잘못 발전되고 있는지를 관찰하는 것뿐만이 아니라, 정보보호법규정 및 실무가 情報保護法의 목표들을 충실히 따르고 있는지에 관한 심사 또한 포함한다. 이러한 審査權限은 저장된 정보와 정보처리계획은 물론 모든 서류들을 포함하였다. 이러한 統制機關은 個人情報保護에 관하여 勸告(諮問)하고 個人情報保護에 관한 문제를 立法府 또는 行政府와 상담하였다. 물론 이러한 상담은 法的 問題나 전문분야의 문제로 축소되지는 않았다. 1세대 情報保護法에 따르면 統制機關의 통제기능과 상담기능은 통제기관이 독자적으로 하거나 의회, 의회의 위원회, 정부의 요청에 따라서 행해질 수도 있었다. 이를 통하여 統制機關에게 시민의 변호사로서 가능한 한 비관료적이고 시민 우호적인 방법으로 도움을 제공하는 옴부즈만역할이 부여되었던 것

95) BDSG 제18조제1항 1, 2.

96) Evangelia Mitrou, a.a.O., S. 46.

97) 의회책임 밖에 있는 행정권한들의 인식은 독일헌법에 따라서 원칙적으로 금지된다(헌법 제80조).

이다. 情報保護機關은 이러한 경우들에 관하여 심사하고 관련자에게 그 결과를 통지해야만 했다. 또한 1세대 法律의 統制機關은 매년 활동보고서를 제출해야 하였다. 이러한 보고서제출은 통제기관활동의 종류와 범위를 설명할 뿐만 아니라 個人情報를 보호하기 위한 개선책들을 제공하는 임무의 성격을 갖고 있었다. 그리고 1세대 法律에는 명시적으로 규정되어 있지 않다 할지라도 統制機關은 여론매체와 공동작업을 통하여 관련 문제들을 해명하고 그들의 생각들을 설명, 비판하며 그들의 제안과 목표들을 공개적으로 제시하였다.

그러나 이러한 1세대 法律에 규정된 統制機關의 권한에는 몇 가지 문제들이 있었다. 우선 개인관련정보의 조사, 수집은 모든 후속적인 정보처리에 관한 기본적인 전제조건으로서 그 자체가 情報自己決定權의 제한을 설명한다. 그런데 1세대 法律에서 정보보호기관을 통한 통제에서 특히 情報調査領域이 배제되었다. 그 다음으로 統制機關이 자신의 과제를 인식해야만 한다면 이에 상응하는 설명권과 조사권을 필요로 한다. 이미 설명된 것처럼 법률상 통제기관들에게 行政機關으로부터 설명을 받은 권한이 인정되었다. 그런데 1세대의 모든 情報保護法들은 개개 경우에 서류열람이 國家安保上 許容되지 않는다고 상급관청이 확인하는 한, 이들 수임인들의 서류열람이나 이들에게 설명을 제공할 의무로부터 첩보기관들을 제외시켰다. 결국 통제되는 기관이 拒否權을 갖는 통제는 통제되지 않는 것과 마찬가지이다. 비록 이러한 결정이 직접적으로 통제되는 첩보기관으로부터가 아니라 관할 부처로부터 행해진다 할지라도 말이다.

그리고 個人情報保護統制에 관한 1세대 정보보호법규정들을 살펴보면 個人情報保護機關이 상담 및 제안기구로 개념정의되었음에도 불구하고 이 당시 立法者는 個人情報保護法의 목표를 개인관련정보처리의 濫用을 막는 좁게 개념정의되는 정보보호개념을 갖고 있었다. 그러나 이는 情報保護受任人이 個人情報의 보호에 기여하기 위해서는 法律을 제정할 때 상담(자문)기관의 적절한 포함이 이미 전제로 된다는 것을 이해하지 못한 것이다. 결국 聯邦憲法法院의 人口調査判決以前 個人情報保護法들에서는 정보처리시스템의 설치계획과 법제정과정에 統制機關의 개입을 法律上 명시적으로 규정하지 않았다. 결국 이는 개인정보보호개념과 관련하여 情報保護機關의 과제와 권한들이 불충분하였다는 것을 입증하였다. 정보처리의 "濫用으로부터 保護"로 統制機關들의 과제를 한정하는 것은 통제기관이 情報調査와 처리를 관찰하고 분석해야만 한다는 요구들을 충족하지 못한다. 이를 다른 말로 하면 個人情報를 보호하기 위한 통제는 情報調査와 處理, 利用의 모든 측면들을 포함되어야 한다는 것을 말한다.

c) 情報保護受任人에 관한 人口調査判決의 영향

聯邦憲法法院은 人口調査判決에서 情報保護受任人의 중요성을 다음과 같이 강조하였다 : "자동정보처리라는 조건하에서 정보의 이용과 저장을 시민이 파악할 수 없다는 것과 적절한 예방책들을 통하여 행하여지는 권리보호라는 측면에서 독립된 情報保護受任人의 참여는 情報自己決定權의 효율적인 보호를 위하여 중요한 의미를 갖는다."[98] 또한 그 뒤 다른 판결들에서 관련자의 情報自己決定權을 보호하기 위하여 情報保護受任人이 중요함을 聯邦憲法法院은 강조하였다.[99] 人口調査判決에서 聯邦憲法法院은 情報自己決定權 및 民主法治國家的 情報秩序의 효율적인 보장를 위하여 포괄적이고, 흠결없으며, 독립적인 정보통제기관을 강조한 것이다. 이러한 기준들에 따라서 獨逸의 立法者들로부터 만들어진 통제모델이 평가되고, 통제실무가 심사되고, 個人情報保護法이 판단되어야만 한다.

여기서 우선 人口調査判決에서 聯邦憲法法院의 統制機關에 관한 설명이 직접적으로 유효하고 구속력있는 법원의 결정을 의미하는지 또는 立法者에 대한 단순한 법정책적인 요구들에 관한 것인가라는 문제가 제기된다. 聯邦憲法法院은 人口調査判決에서 어떤 새로운 통제기관을 만들도록 요구하지는 않았다. 그러나 聯邦憲法法院은 情報社會에서 개인의 情報自己決定權을 보호하기 위하여 규범명확성과 비례성원칙의 준수뿐만 아니라, 조직적이고 절차법적인 조치들도 필요한 것으로 생각하였다. 정보사회에서 행정의 情報處理가 매우 복잡해짐에 따라서 이러한 정보처리과정을 개개 시민이 파악할 수 없기 때문에 시민의 권리를 보호하기 위한 제도적인 통제가 필요하다는 것이다.[100] 이미 聯邦憲法法院이 밝힌 것처럼[101] "적절한 예방책들을 통하여" 개인의 권리를 앞서서 보호한다는 표현을 통하여 情報保護受任人에게 이에 관한 통제기능이 부여될 뿐만 아니라, 법규정들을 준비하고, 새로운 시스템들을 계획할 때 이미 이러한 기관들이 참여해야만 한다는 명령이 제기된다. 또한 聯邦憲法法院은 통제의 효율성을 보장하기 위하여 통제기관의 독립성을 강조하였다. 어쨌든 聯邦憲法法院의 설명들로부터 통제기관의 권한과 조직에 관한 구체적이고 상세한 지침들이 나오지는 않는다. 그러나 이는 정보보호기관들이 立法者의 처분밑에 있다는 것을 뜻하지는 않는다. 立法者의 形成自由는 통제기관의 독립 또는 헌법상 명령되는 통제의 보장에서 그 한계를 발견한다. 특히 개인의 情報自己決定權이 제한되고 설명권을 통한 개인적 통제가 행해지지 않는다면, 統制機關을 통한 제

98) BVerfGE 65, 1/46.
99) BVerfGE 67, 157/185.
100) BVerfGE 65, 44.
101) BVerfGE 65, 44.

도적 통제는 個人情報를 보호하기 위하여 포기할 수 없는 핵심으로 입증된다. 왜냐하면 이러한 통제만이 정보처리의 合憲性을 심사할 수 있는 유일한 수단이기 때문이다.

d) 統制機關의 地位와 獨立性

위에서 이미 설명된 것처럼 情報保護機關의 활동 그리고 결국에는 전체적인 情報保護統制政策이 효율적인가를 판단하는 척도는 결국 정보보호수임인의 활동이 성공적이었느냐에 달려있다. 물론 이에 관한 기준을 확정적으로 事前에 결정한다는 것은 어렵다. 또한 통제실무를 전체적으로 판단하기 위해서는 현행 法律들뿐만 아니라 이를 넘어서서 개개 나라들의 구체적인 역사적, 법적, 정치적, 사회적 배경들과 전통들에 관한 인식 또한 전제로 되어야 한다. 결국 그러한 한 法典 속에 統制機關의 統制權限들이 확정되는 것만이 결정적인 의미를 갖는 게 아니다. 오히려 獨逸의 경우처럼 강제적인 명령권한이나 간섭권한을 갖고 있지 않은 통제기관을 통하여 수행되는 情報保護統制의 효력은 통제되는 公的 機關이 이러한 통제기관에 얼마만큼 협조하는지에 결정적인 정도로 의존한다.

그런데 獨逸의 聯邦憲法法院은 統制機關의 독립을 個人情報保護에 관한 制度的 統制의 핵심사항으로 제시하였다. 따라서 統制機關의 獨立性은 個人情報保護를 위한 통제의 기본조건이면서 동시에 이러한 통제의 효율성에 관한 척도를 나타낸다. 우선 통제개념의 구성요소로서 統制者와 통제되는 사람간 非同一性이라는 기본명제는 독립성개념의 구체화를 위한 판단근거로서 봉사한다. 그리고 外部統制-自己統制라는 단순한 2분법적 구별을 넘어서서 統制機關의 과제, 활동, 기능들과 관련하여 獨立性槪念을 발전시켜야 한다. 그밖에 제시된 과제들의 종류와 범위 및 정보보호통제 속에 설정된 목표들로부터 獨立性槪念이 도출되어야만 한다. 여기서 이러한 統制機關의 獨立性은 그 자체가 어떤 가치를 형성하거나 독립적 목표를 형성하지 않는다는 것을 기억해야만 한다. 따라서 獨立性이란 기능관련적이고 기능지향적으로 구체화되어야 한다.

獨逸에서 統制機關은 세 가지 다른 모델들로 나뉜다. 우선 첫 번째로 統制機關을 가능한 한 통제할 수 있는 기관들에 가깝게 놓는 모델, 곧 行政府에 편입시키는 모델과 두 번째로 헤센(Hessen)州와 라인란트-팔쯔(Rheinland-Pfalz)州처럼 統制機關을 議會에 귀속시키는 모델, 세 번째로 베를린처럼 정보보호수임인을 監査院과 같은 최고의 州官廳으로 설치하는 모델이다.

우선 統制機關을 行政府에 편입시키는 모델은 특히 立法府에 소속한 통제기관모델에 반대하는 생각에 근거한다. 그런데 이렇게 行政府에 편입모델은 그 자체가 모

순을 갖고 있다. 그런데 이러한 모델에 따르면 統制者가 통제되는 기관의 일부분을 형성하게 되나 行政府와 정보보호통제기관간에는 너무 많은 충돌요소들이 있다. 왜냐하면 行政府는 個人情報保護에 관하여 다툼이 있는 경우에 行政府의 시각에서만 결정하려고 하기 때문이다. 이에 따라서 통제기관의 과제이행이 상당히 어려워질 수도 있다. 결국 그렇다면 行政府에 조직적인 편입에 대하여 다음 논거를 갖고서 반대할 수 있다 : 곧 機關의 獨立은 어떤 추상적이고 절대적이며 확정된 기준들에 따라서 판단할 수 있는 가치가 아니다. 그렇다면 機關의 獨立이란 情報保護機關이 한편으로는 통제되는 行政府와 다른 政治機關들로부터, 또 다른 한편으로는 市民으로부터 독립된다는 것을 뜻한다. 統制機關이 통제되는 기관의 일부분으로 국민들에게 파악된다면 시민 쪽에서 統制機關을 불신할 수 있고 이러한 불신은 다시 정보보호기관의 작용기반을 해칠 수도 있다. 따라서 統制者와 統制되는 기관간 명확한 분리가 이러한 신뢰관계의 구축을 위한 최소한의 토대이다. 다음으로 行政府에 편입이 法律에 규정된 統制機關槪念에 일치하는 지라는 문제가 제기된다. 예를 들어 行政이 정보보호기관의 비판과 제안들을 받아들이지 않을 수도 있다. 정보보호수임인이 이를 통제할 수 없다면 결국 統制機關은 여론에 호소하고 의회의 개입을 요구할 수밖에 없는데 統制機關이 바로 비판하는 기관들과 통제기관의 예산 및 인사에 관하여 상담하여야 하는 현실이 이러한 통제를 어렵게 만든다는 것은 더 이상의 설명이 필요없을 것이다.

그런데 獨逸에서 統制機關은 상담, 경고, 이의제기기관으로 개념 정의된다. 당연히 이러한 모든 기능들은 행정 및 일상적인 정보처리실무와 관련된다. 바로 독일의 정보보호기관이 어떤 법적 관철수단을 갖고 있지 않기 때문에 상담과 제안을 통하여 결정들이 내려져야 한다. 따라서 法律適用에 관한 해석상 차이와 토론에서는 물론 統制機關의 권한에 관한 시각에서도 立法府는 중요한 대화상대방이며 立法者에게 통제기관의 경험들을 직접 보고하는 것은 법제정이나 개정시 이러한 의견이 반영되도록 할 가능성을 높인다. 다시 말하면 議會에서 언제나 個人情報保護에 관한 우호적인 결론이 나온다고 할 수는 없지만 의회내 토론은 어쨌든 규범제정절차의 투명성을 보장한다. 정보처리 및 정보보호와 관련하여 이러한 투명성을 극대화하려는 노력 속에서 바로 情報統制機關을 의회와 결합하려는 중요한 이유가 존재한다. 따라서 헤센(Hessen), 라인란트-팔쯔(Rheinland-Palz), 베를린과 같은 州들에서 統制機關을 의회에 귀속시키거나 의회감독하에 있는 최고의 州官廳으로 설치하는 것이 정보통제기관모델은 물론 聯邦憲法法院의 결정에서 제시된 기준들에도 일치한다.[102]

統制機關의 獨立은 또한 統制機關의 영역에 속하는 決定節次들의 독자적인 운용을 전제로 한다. 이러한 의미에서 이러한 獨立性은 필연적으로 제3자의 통제나 외부통제로부터 자유, 또는 이를 적극적으로 표현한다면 전적으로 자기 스스로 통제하는 결정의 자유를 뜻한다. 情報保護法에 따라 정보보호수임인들은 獨立的이며 法律에만 구속된다. 이에 따라서 統制機關들은 準法官的 獨立을 누린다. 따라서 모든 정보보호기관들은 그 기관활동과 관련하여 어떤 지시도 받지 않으며 어떤 職務監督 밑에 있지도 아니한다. 그러나 이러한 機關의 獨立은 行政府로부터 自由를 의미하지 議會로부터 자유를 말하는 것은 아니다.

그런데 한 기관의 實質的인 獨立性保障은 그 機關이 효율적으로 활동할 수 있는 결정적인 요인이다. 法的으로 독립된 구조와 권한들이 보장되어 있음에도 불구하고 이러한 기관이 財政的인 면에서 從屬的이라는 것을 통하여 이미 정보보호기관들의 독립은 제한될 수 밖에 없다. 해당법규정이 의회 및 행정부를 구속하기는 하나, 豫算立案者는 불명확한 개념을 해석하고 구체화할 때 필연적으로 매우 커다란 활동영역을 갖고 있다.[103] 어쨌든 豫算을 통하여 거꾸로 정부나 여당 쪽에서 統制機關에 대한 통제수단과 압력수단으로서 활용될 수 있다는 것은 언제나 인식해야만 한다.[104]

---

102) 라인란트-팔쯔는 州議會에 연결되는 조직구조를 결정하였다. 그러한 한 이러한 통제기관은 독일에서 유일한 것으로서 그 통제권한은 법률에만 따르고 명령이나 지시로부터 자유롭다. 한 명의 정보보호수임인이나 그 당시 새롭게 설치되던 옴부즈만기관의 정보보호통제대신에 5명의 합의제기관이 통제기관으로 만들어졌다. 정보보호위원회는 3명의 의원, 州의 두 명의 공무원이나 판사로 구성되었다. 베를린의 통제기관은 최고의 州관청으로 설치된 독일의 유일한 지역이다. 베를린의 입법자는 감사원과는 달리 정보보호수임인을 의회의장의 감독 하에 두었다. 왜냐하면 이는 한편으로는 이러한 기관에게 상당한 정도의 행위(동)자율을 부여하고 다른 한편으로 의회의장밑에 둠으로써 입법부와 연결이 보장되기 때문에 이러한 구성은 많은 장점들을 제공한다. 이와는 달리 바이에른州는 11명의 위원중 7명은 의회가 선발하고, 나머지 4명은 행정부와 지방자치단체를 대표한다. 이러한 Beirat에게는 원칙적으로 자문과제들이 부여된다. 특히 이 Beirat는 활동보고서의 준비, 정보보호조치들의 채택에 관하여 행정에 요구할 입장을 제시하는 등의 과제를 수행한다.

103) 예를 들어 베를린의 경우 40만 마르크의 예산이 배정되나, 바덴-뷔르텐베르크의 경우 베를린의 4분의 1수준의 예산이 배정되어 있다. 개개 州의 다소 빡빡한 재정상황이 개개 통제기관에 작용하는 예산의 높음에 관하여 결정적으로 작용한다는 것은 이해할만 하다. 이러한 상황은 정보보호수임인이 요구할 때 고려해야만 하는 상황이다.

104) 재정문제는 정보보호수임인이 그 직원들을 선발할 때 부딪히게 되는 유일한 문제는 아니다. 어느 정도 자격이 있는 사람을 받는 어려움은 아주 작은 직원의 숫자에서 법-조직적 문제들을 위하여 자격 있는 사람들은 물론 정보전문가 - 법적 문제의 중요성 때문에 법률가들이 우세한 곳에서 - 도 뽑아야만 한다는 것을 통하여 강화된다. 교육 및 자격을 넘어서서 선발기준들은 개개 통제기관의 작업방식에 따라서 다르다. 예를 들어 실무상 교육받은 합의제구조를 갖고 있는 헤센주의 정보보호수임인은 그 직원을 뽑을 때 합의제운영가능성에 중점을 두는 반면에 바이에른주의 정보보호수임인은 정보보호통제의 행정영역에 관하여 어느 정도의 실무경험이

그 다음으로 統制機關의 구성과 관련하여 獨逸의 立法者는 合議制機構보다는 한 사람의 情報保護受任人에게 여러 권한들을 주는 제도를 선호하였다. 문제를 여러 관점 하에서 판단하고 정치적으로 결정하고 처리할 수 있을지도 모르는 合議制機構보다는 비관료적이고 신속하며 탄력적이고 시민에 우호적인 형태를 지향하면서 立法者는 한 사람의 受任人制度를 결정하였다.[105] 어쨌든 情報保護受任人을 行政府가 아니라 議會가 선출하는 것은 확실히 이러한 기관의 正當性을 커다란 정도로 높인다. 이에 따라서 議會를 통한 임명은 行政府로부터 통제기관의 독립을 입증하여야 한다. 물론 정치현실상 與黨이 이러한 受任人을 결정하거나 선택한다 할지라도 후보자에 관한 토의나 협상이 정부를 통한 지명보다는 더 나은 선택을 기대할 수 있게 한다. 따라서 이러한 임명형태에서는 후보자에 관한 공적인 토론이 선행되어야만 한다.

e) 情報保護受任人의 統制政策

정보보호정책의 내용이 어느 정도 法律에 규정된 과제들과 수단들에 의하여 결정된다는 것은 당연하다. 그럼에도 불구하고 情報保護受任人이 그들의 과제를 이행하기 위하여 상담, 설명, 공개적 비판이라는 비전통적인 수단을 사용할 수 있으므로 나름대로 고유한 통제방법을 발전시킬 비교적 넓은 활동영역을 처분할 수 있다. 전통적인 行政機關과는 달리 개인적 입장, 정보보호수임인의 개성이 결국에는 직무수행시 주요역할을 행사한다. 이에 따라서 우선 情報保護受任人 스스로가 자기의 기능과 과제를 어떻게 이해하고 인식하는지가 결정적이다. 獨逸에서 情報保護受任人의 역할은 근본적으로 個人情報保護와 행정기관의 이익간 목표충돌의 조정에 있다. 그러므로 정보보호수임인의 역할에 관하여 공통되는 인식은 情報保護受任人이 우선 시민의 辯護士라는 것이다. 그럼에도 불구하고 情報保護受任人은 대립되는 하나의 이해관계를 위하여 성급하게 판단을 내리려고 하지 않고 언제나 행정기관의 이익과 個人情報保護가 절대적으로 상호 대립되지는 않는다는 생각으로부터 출발한다.[106] 따라서 獨逸統制機關의 통제실무 및 통제전략에 관하여 판단할 때 특히 立法者가 채택한 통제모델이 유효한지, 얼마만큼 유효한지라는 문제에 주의를 기울이고 그 다음에 개개 분야에서 행해지는 통제가 위 통제모델에 일치하는지라는 문제를 다룬

있고 정보처리에 관하여 잘 알고 있는 사람을 선발의 결정적인 기준으로 생각한다. 어쨌든 일반적으로 직원을 행정부출신의 사람들로 편성한다는 경향을 확인할 수 있다. 그래도 이들이 과거에 익숙한 행정활동으로부터 벗어나서 새로운 기관에서 일을 하고 정보보호적이고 시민이익지향적인 자리에 있어야만 한다는 어려움은 이해할만한 문제이다.

105) 다만 일원론적 모델에서는 능동적이지 못하거나 기회주의적 인물이 임명되어서 따라서 전체적인 통제가 약해질 위험성이 어느 정도는 있다.

106) Evangelia Mitrou, a.a.O., S. 120.

다. 그러다보니 통제기관에게 상호 긴장관계 속에 있는 많은 기능들이 위임되었다, 곧 統制機關이 상담자와 경고자로서 등장하고 충돌문제들을 정리, 분석하며 설득작업을 통하여 예방적으로 정보처리실무에 관여하고 個人情報에 관한 위험을 事前에 방지하려고 노력한다. 여기서 독일의 統制機關들에게 法律上 간섭권한과 명령권한이 결여되어 있기 때문에 통제되는 기관의 정보준비와 협조준비에 크게 의존한다는 것을 잊어서는 안된다.[107] 個人情報를 보호하기 위하여 공격적이고 엄격한 통제는 심지어 행정부와 비공식적으로 타협하고 조정하는 통로마저 배제하는 결과를 가질 수도 있다. 그럼에도 불구하고 충돌하는 이해관계들의 조정을 통하여 合意를 도출하려는 이러한 통제모델이 갖고 있는 위험성 또한 언제나 기억해야만 한다. 이를 구체적으로 말하면 이러한 통제모델이 개인의 情報保護가 아니라 오로지 행정정보처리만을 정당화하는 기능만을 가질 위험성을 갖게 될지도 모른다는 것이다. 따라서 統制機關은 行政府나 立法府와 대화할 수 있는 통제전략들과 이행전략들을 갖고 있어야만 한다. 결국 행정내부적 통제가 정보보호에 관한 통제기관으로부터 구별되는 것은 특히 후자가 정보처리의 투명성에 기여하고 관할기관으로서 이러한 문제들에 관하여 여론에 호소하고 사회적으로 토론될 수 있도록 자극하는 것에 있다. 따라서 統制機關들은 공식적인 이의신청이란 수단을 보통 매우 소극적으로 사용하였다. 이러한 이의신청의 제기여부가 情報保護受任人의 재량에 속한다 할지라도 정보보호수임인은 이러한 이의제기를 최후통첩으로 파악하였다. 그래서 이러한 이의신청은 상담과 권고를 책임 있는 기관을 어떤 방향으로 유도하려는 노력이 성과 없게 된 이후에 비로소 선택된다.

統制機關의 작업과 정책을 파악하기 위하여 가장 좋은 자료가 바로 기관의 活動報告書이다. 情報保護法은 어떤 내용을 담아야만 하는지에 관한 언급없이 활동보고서의 제출을 정보보호수임인에게 의무 지우고 있다. 이미 설명된 것처럼 이러한 活動報告書는 처음부터 여러 기능을 갖고 있다. 우선 個人情報保護와 관련되는 문제들 및 이에 관한 해결책들을 의회에 제출하는 것을 통하여 活動報告書는 실제로 統制機關의 활동매개체역할을 맡는다. 따라서 통제기관이 통제를 수행할 때 확인된 문제들과 미해결인 채로 남아있는 문제들이 주로 報告書에 기록된다. 따라서 이러한 報告書를 통하여 한편으로 行政府의 統制者로서 의회에게 문제점을 보고하고 다른 한편으로는 충돌하는 이해관계가 제기되거나 이에 관한 대안들이 설명된다. 어

107) 정보보호수임인들은 그들의 관심사가 정보보호스캔들의 폭로에 있는 게 아니라 행정과 시민간 지속적인 대화 속에 있다고 언제나 다시 강조한다는 것은 우연이 아니다. 정보보호수임인이 행정과 공공에 공격적으로 다가간다면 한편으로 특히 예방적으로 작용하는 상담기능에서 신뢰기반이 없어지고 다른 한편으로 행정공무원들의 협조준비도 눈에 띄게 축소될 것이다.

쨌든 이러한 報告書들에 담기는 내용들은 個人情報保護 등과 관련하여 행정기관들을 자극하고 정보보호법규정을 적용할 때 나타나는 구체적인 문제에 관한 해결책들이다. 이에 따라서 많은 報告書들이 풍부한 사례설명들을 담고 있다. 그리고 이러한 活動報告書는 행정에게 입문서와 보조자료로서 활용되는 것을 목표로 한다. 이를 넘어서서 이러한 종류의 報告書는 또한 의회와 일반 국민들이 정보보호법상 문제점을 파악할 수 있도록 하기 위하여 이에 관한 統制機關의 견해를 제시한다. 결국 통제기관의 이러한 보고서가 갖고 있는 또 다른 특징은 情報保護關聯法律들을 심도있게 분석하고 광범위하게 설명하는 것 속에 있다. 특히 獨逸 聯邦憲法法院의 人口調査判決以後에 이러한 보고서들의 많은 부분은 法律上 결함 및 이에 상응하는 제안설명에 할애된다. 그리고 統制機關의 이러한 活動報告書는 주로 公的 領域에서 통제기능의 효율성 및 정보처리의 투명성을 확보하기 위하여 노력한다.[108]

그리고 이와 더불어 情報保護受任人은 정보보호통제의 효율성을 높이기 위하여 일반시민의 정보보호의식을 강화하고 계속 발전시키는 작업을 펼친다. 이러한 情報保護受任人의 활동은 다양한 형태를 취한다. 우선 정보보호나 통제에 관한 안내책자의 출간은 시민에게 정보보호와 개인의 권리보호에 관하여 알리는 첫 번째 시도였다. 그리고 정당, 단체, 학교 등에서 정보보호수임인들이 갖게 되는 많은 강연기회도 비슷한 기능을 갖고 있다. 특히 情報保護受任人들은 이러한 활동을 하기 위하여 여론매체를 적극적으로 활용하려고 노력한다.[109]

f) 情報保護受任人에 관한 評價

1969년 聯邦과 州에서 個人情報保護法을 제정한 이후로 獨逸은 잘 발전된 정보보호시스템을 갖춘 국가로서 다른 나라에서 검토대상으로 삼는 매우 중요한 모델이었다.[110] 그런데 독일의 통제기관은 제한적 권한과 일원론적 구조를 갖고 있기 때문에 統制機關의 效率性은 누가 情報保護受任人이냐에 따라 약간씩 달라진다. 왜냐하면 情報保護受任人이 사회적 진공체 속에서 활동하는 게 아니라, 시대적, 장소적,

108) 그럼에도 불구하고 이러한 보고서의 운명에 관하여 토론해야만 한다. 우선 의회에서 다루어지는 것과 관련하여 몇몇 문제들이 나오게 된다. 심각한 문제는 많은 경우에 활동보고가 너무 늦게 다루어진다는 것속에 있다. 보기 : 의회에서 연방정보보호수임인의 6, 7번째 보고서가 다루어지고 있을 때 이 수임인은 10번째 보고서를 준비하고 있었다.

109) 정보보호문제와 정보보호자들에 대한 여론매체의 태도가 결코 통일적이지 않다는 것은 당연하다. 이는 개개 신문이나 잡지의 정치적 성향은 물론 개개 기관의 정보보호정책과 연결된다. 이를 일반화하여 인식할 수 있는 것은 보수적 신문(예를 들어 die Frankfurter Allgemeine Zeitung)은 정보보호문제 - 특히 안보와 관련된 -에 관한 토론에서 매우 소극적이라는 것이다. 위 설명으로부터 여론매체와 협조가 문제없지는 않다는 것을 쉽게 파악할 수 있다.

110) David H. Flaherty, ibid., p.21.

역사적으로 구체화된 특정 사회적, 정치적 문맥 속에서 활동하기 때문이다. 결국 情報保護受任人이 의회를 통하여 임명되는지 또는 행정부를 통하여 임명되는 지와는 상관없이 정치적인 고려가 情報保護受任人의 임명에 작용한다는 것은 의심의 여지가 없다.[111] 그러나 이는 임명된 情報保護受任人이 언제나 좁고 단편적인 당파적인 기준들에 따라서 선출된다는 것을 뜻하지는 않는다. 결국 獨逸의 통제기관은 이러한 기관에게 강제적인 명령권한이 없다는 것 뿐만 아니라 또한 이러한 기관이 독립된 일원론적 형태라는 특징을 갖고 있다는 것 때문에 情報保護受任人의 개성과 견해가 중요한 요소로 작용한다. 몇몇 예외를 제외하고는 압도적인 다수의 정보보호수임인들이 행정부출신이었고 심지어는 정보보호에 반대하는 것처럼 보이는 기관에서 근무했던 사람도 있었다. 이에 관한 찬반논쟁이 있으나 그 동안의 경험으로 볼 때 과거의 이력과 사회정치적인 견해들이 통제기관의 활동에 관하여 중요한 의미를 갖기는 하지만 결정적인 요소로는 표시될 수 없다고 한다.

결국 시민과 많은 정보보호단체들은 情報保護受任人이 시민의 자유를 보호하기 위하여 적극적으로 또는 공격적으로 활동하기를 기대하지만 통제기관에게 강제적인 명령권한이 결여되어 있으며 통제활동시 통제되는 기관의 협조하려는 태도에도 어느 정도 의존할 수밖에 없는 현실을 또한 인식하여야 한다.[112]

그런데 獨逸에서 한편으로는 정보보호법상 요구들이 얼마만큼 실현되었는지를 비교, 판단할 수 있는 統制機關들의 활동에 관한 통계자료가 없다. 다른 한편으로 이렇게 여러 기능을 갖고 있는 기관의 효율성이 하나의 관점에서 충분하게 판단되지 않는다는 것이다. 이에 따라서 결국 情報保護受任人의 통제활동에 관한 전반적으로 조망하고 판단한다는 것이 결코 쉽지 않다. 그렇다면 정보보호통제에 관한 기대수준과는 상관없이 정보보호통제의 효율성을 평가할 수 있는 관점이 우선 개념 정의되어야 한다. 여기서 그러한 관점들로는 個人情報保護에 관한 시각과 더불어 통제되는 기관의 시각을 지적할 수 있다. 그렇다면 결국 統制機關의 활동과 그 효율성은 기관이 담당하는 직무수행의 결과들에 따라서 판단된다는 것은 불가피하다. 이를 자세히 설명하면 行政府가 필요한 만큼만 개인정보를 처리하도록 情報保護受任人이 이끌었는가? 행정부의 계속적인 자동화가 기본권합치적인 방법으로 이루어지

111) 또한 정부가 바뀌는 것이 종종 연방내무성의 정치적 경향을 결정하며 계속해서 이는 연방정보보호수임인의 선발에 영향을 줄 수 있다. 예를 들어 Bull이 수임인이었는데 선거를 통하여 여당이 SPD에서 CDU로 바뀌고 새로 임명된 Friedrich Zimmermann은 Bull이 국가안보이익보다는 개인정보보호에만 관심을 갖고 있다고 생각하여서 임기가 끝난 Bull을 재임명하지 않았다.

112) 이러한 의존성은 통제기관이 제도적으로 의회에 직접 속하는 게 아니라 행정부에 속하는 경우들에서 극단적으로 명확하게 표현된다.

도록 하는 데에 受任人이 성공하였으며 정보처리기관의 개인관련정보의 남용을 얼마만큼 막았는가? 통제기관들이 행정부의 주장에 대하여 그들의 입장과 방침을 얼마만큼 관철시켰는가? 등이다.

우선 개개 시민을 보호하기 위한 분야에서 정보보호수임인이 거둔 성과는 논란이 되지 않는다. 곧 情報保護受任人의 옴부즈만기능은 성공적인 것으로 표시할 수 있다.[113] 또한 많은 영역들에서 실제로 통제기관들이 나름대로 성과를 올렸다.[114] 통제기관들의 논거가 설득력 있게 시민과 여러 정치세력들에게 작용하는 한, 行政府는 통제기관들의 견해를 완전히 무시할 수는 없었다. 특히 情報保護受任人은 정보처리의 헌법합치적인 근거를 法治國家原則에서 찾았다. 곧 統制機關은 法治國家原則에서 파생되는 규범명확성원칙, 과잉금지원칙 및 다른 헌법원칙 및 행정법원칙들을 바탕으로 하여 국가의 정보처리를 평가하고 판단하였다.[115]

이미 이러한 설명으로부터 情報保護受任人의 임무가 단순히 個人情報統制로 한정되지 않는다는 것을 알 수 있다. 이들이 담당하는 또 다른 기능은 立法者를 批判하고 立法案에 관하여 의견을 표명하는 것 속에 있다. 이를 구체적으로 말하면 情報保護受任人은 技術的으로 가능한 것이 또한 헌법적으로 또는 법정책적으로도 받아들일 수 있는지에 관하여 의견표시를 할 수 있다. 다만 情報處理가 국가가 수행하려는 목적을 위하여 필요한지라는 일차적 판단은 정치적 판단사항으로서 정보보호수임인이 이에 관하여 결정할 수 있는 위치에 있지 않다. 어쨌든 정보보호기관의 제안들중 얼마나 많은 것이 이행되었는지와는 상관없이 情報處理의 투명성을 확보하기 위하여 애쓴 정보보호수임인들의 활동이 가장 중요한 업적에 속한다.[116] 정보보호수임인이 국가의 정보처리행위를 투명하게 하거나 이러한 투명성의 한계를 명백하게 함으로써 국가의 정보처리가 개인의 권리보호 및 민주사회발전에 기여하는지를 판단하기 위한 근거를 형성하였던 것이다.

더군다나 1990년에 개정된 聯邦情報保護法은 情報保護受任人의 地位와 獨立性에

113) David H. Flaherty, ibid., p.61.

114) 보기 : 사회법영역, 안보관련법규정들의 개정, 안보기관의 컴퓨터에 저장된 불필요한 몇백만 개인정보들의 삭제, 연방경찰청(Bundeskriminalamt)에 설치하려는 포괄적인 중앙개인전산자료계획의 저지, 정보통신영역입법에 참여. 또한 행정부초안에 대하여 해당 부처나 의회위원회에서 새로운 초안의 발전에 기여하는 경우와 각종 법률에서 정보보호를 위한 규정의 삽입들을 위하여 노력한 경우를 들 수 있다.

115) 이들은 헌법상 분리명령을 언급하면서 첩보기관과 경찰간 정보교환을 비판하였다. 이들은 정부가 추진하였던 기계가 읽을 수 있는 새로운 신분증명서나 여권의 허용성에 직접적으로 의문을 제기하지는 않았으나, 그럼에도 정부가 제시한 도입근거가 충분하지 않다는 전문가들의 견해를 지적하기는 하였다.

116) Evangelia Mitrou, a.a.O., S. 155.

관하여 개선된 조항들을 담고 있다. 특히 政府草案에는 원래 규정되어 있지 않았으나 연방정보보호법개정에 관한 聯邦議會의 토론에서 채택되었던 議會를 통한 선출은 확실히 연방정보보호수임인의 지위를 강화한 것으로서 확실히 환영할만한 것이다. 임명하고자 하는 사람에 관한 투명하고 진지한 토론이 전제로 된다는 것은 정보보호수임인의 正當性에 관하여 의회가 기여하고 정부로부터 독립을 상징하는 것이다. 그럼에도 불구하고 다른 한편으로는 聯邦情報保護法의 개정과정에서 聯邦情報保護受任人의 통제권한들을 새롭게 규정할 때 정보보호통제권한을 강화하는 게 아니라, 오히려 이를 제한하고 축소하려는 쪽으로 규정되었다고 비판된다. 예를 들어 통제기관의 상담기능은 법개정이후에도 중요성이 강화되지 않았고 자동화된 호출절차의 설치를 정보처리기관에 통지해야만 하는 의무[117]와는 별도로 새로운 시스템의 설치나 기존의 자동화된 정보시스템들의 구축에 관한 계획들을 포괄적으로 聯邦情報保護受任人에게 통지할 法律上 義務가 해당 기관에게 부과되지 않았다. 다만 聯邦情報保護受任人의 통제대상에 서류의 포함은 오랜 다툼 끝에 해결되었다. 곧 聯邦情報保護受任人은 오로지 서류 속에서만 처리되거나 이용되는 개인관련정보를 자유로운 재량에 의해서가 아니라 관련자권리의 침해에 관한 충분한 근거들이 존재하는 경우에만 통제할 수 있다.

3. 內部統制型 시스템

이미 여러번 언급된 것처럼 美國에서는 지금까지 완결된 개인정보보호시스템은 존재하지 않는다.[118] 따라서 美國에서 個人關聯情報의 保護를 유럽과 비교한다면 매우 한정되어 있다고 말할 수 있다. 연방차원에서 個人情報를 보호하고자 하는 法律들이 다수 있기는 하나 이는 언제나 다소 제한된 일부영역만을 위한 법규정들이다. 그렇다면 결국 美國에서는 個人情報保護에 관한 일관성있고 체계적인 시스템은 확인되지 못한다.[119] 다만 公的 領域을 규율하는 一般的인 情報保護法을 제정할 가능성이 없어 보인다 할지라도, 분야별로 규율하는 제정법들이 聯邦과 州에서 제정되고 있다.

美國의 프라이버시법이 제정당시에는 혁신적이었고 다른 나라에 미치는 영향력 또한 매우 컸다 할지라도 다른 나라에서와는 달리 실제로 이러한 제정법이 잘 적용되는지를 통제할 책임은 대단히 광범위하게 분산되어 있다. 우선 이 법은 聯邦政府

117) BDSG 제10조제3항.

118) Marie-Theres Tinnefeld, Der Datenschutz in den Vereinigten Staaten, RDV 1992, S. 216 이하.

119) Stephan Wilske, Datenschutz in den USA, CR 1993, S. 307.

에 의한 個人情報의 수집과 처리에 관한 규정들을 담고 있다. 그러나 美國의 통치기구는 전체로서 정보감시문제들을 검토하거나 個人情報保護問題를 파악하기에는 너무 복잡하다. 이는 개인의 프라이버시를 침해할 수 있는 행위들이 동시에 여러 곳에서 발생할 수 있다는 것을 뜻한다. 그럼에도 불구하고 다른 나라들에서처럼 국가의 정보처리를 통제할 監督機關을 설치하는 것 대신에 실제로 制定法이 잘 작용하는 것을 보장할 책임이 대단히 광범위하게 분산되어 있다. 그렇다면 왜 연방차원에서 프라이버시보호위원회가 설치되지 않았는지를 이해하는 게 중요하다. 프라이버시법제정 당시에 프라이버시보호위원회를 설치하고자 한 上院의 최종계획 또한 下院의 초안처럼 이 위원회가 규제권한이나 옴부즈만권한을 갖도록 규정하지는 않았다.[120] 한편에서는 이러한 권한을 갖는 委員會의 설치가 강력하게 주장되었지만 이러한 委員會의 설치로 인한 비용증가 및 위원회의 관료화위험성, 위원회활동을 통하여 오히려 시민권리의 구제가 침해될 가능성이 있다는 주장이 더 설득력있게 받아들여져서 프라이시버시보호위원회를 만드는 계획은 결국 부결되었다.[121] 그러나 個人情報保護法을 제정하고 시행한 경험을 갖고 있는 국가들에 관한 설명에서 이미 지적된 것처럼 行政機關 스스로 자율적으로 프라이버시法律에 명시된 기준을 이행하도록 기대한다는 것은 힘들다. 왜냐하면 결국 국가를 통한 情報調査, 처리욕구와 個人情報保護는 자주 충돌할 가능성을 처음부터 갖고 있기 때문이다. 個人情報保護에 관한 美國 연방시스템은 두 가지 중요한 속성들을 갖고 있다. 우선 첫 번째로 연방차원에서 情報保護委員會가 없음에도 불구하고 정부 안팎에서 情報保護委員會와 유사한 감독기능들을 수행하려고 노력하는 사람과 조직들이 있다는 것이다. 예를 들어 하원의 "政府情報, 正義(justice), 農業에 관한 小委員會"가 프라이버시법 및 정보공개법의 이행에 관하여 많은 관심을 갖고 이에 관하여 검토한다. 이에 따라서 1983년 6월 7일, 8일 양일간 프라이버시법에 관한 전반적인 聽聞會가 처음으로 개최되었다. 또 의회 상임위원회에 소속된 전문가들이 행정부내에서 정보처리에 관하여 살펴봄으로써 情報保護委員會가 담당해야만 하는 임무중 일부를 수행한다. 다만 이렇게 의회의 常任委員會를 통한 프라이버시법의 감독은 제한되고 비정기적이라는 단점을 갖고 있다. 그 다음으로 정보보호전문가들, 언론, 시민단체 등이 프라이버시보호를 위하여 연방정부에 많은 압력을 행사한다. 그런데 개개인의 訴提起 및 法院의 裁判을 통하여 프라이버시법규정의 위반을 통제하려는 것은 美國社會의 소송선호경향을 반영한다. 결국 미국의 현실에 따르면 프라이버시법에 규정된 권리들을 國家가 인정하지 않을 경우에 개인이 聯邦法院에 訴를 제기하여 문제

120) David H. Flaherty, ibid., p.11.
121) David H. Flaherty, ibid., p.313.

를 해결할 수밖에 없다. 그러나 이러한 訴訟節次는 비용과 시간이 많이 들뿐만 아니라 재판절차나 입증부담책임 등에서 매우 복잡하고 어려운 문제들이 많이 깔려있다. 그렇다면 美國의 개인정보보호시스템에서 가장 중요한 특징은 위에서 설명한 것처럼 정보보호기관가 없다는 것이다. 이에 따라서 개개 정부기관의 長이 프라이버시법의 집행에 관하여 책임을 진다. 다만 프라이버시법의 이행에 관한 감독은 대통령관할하에 있는 管理豫算室(Offiece of Management and Budget, OMB)이 부분적으로 담당한다. 결국 기본적으로 美國의 정보보호시스템은 통제기관의 직접적인 개입 없이 行政機關들이 스스로 해결하는 방식을 택한 것이다. 이러한 시스템에는 개개 국가기관 스스로가 정보처리 및 프라이버시문제들을 다루어야만 한다는 생각이 바탕에 깔려있다. 이에 따라서 OMB와 의회의 상임위원회들, 法院에게는 이러한 행정기관의 실무를 事後的이고 制限的으로 감독하는 역할만이 기대된다. 이렇게 美國에서 프라이버시법 이행에 관한 감독은 대통령관할하에 있는 관리예산실이 맡았는데 뒤에서 설명하는 것처럼 결국 이러한 시스템은 연방정부의 정보처리를 통제하는 데에는 현명하지 않은 선택으로 입증되었다. 왜냐하면 OMB 스스로가 프라이버시법의 집행에 관한 감독권한만을 갖고 있을 뿐인데다 실제로 OMB는 유럽이나 캐나다의 정보보호위원회와 비교한다면 집행과정에서 상대적으로 약한 지도력을 행사하였기 때문이다. 그렇다면 美國에는 個人情報를 보호하기 위한 통제기관이 없기 때문에 OMB와 개개 정부기관들의 실제작업을 분석하고, 분야별로 접근하여 검토해야만 한다.

우선 연방프라이버시법은 個人情報의 수집과 유통에 관하여 엄격하게 규정하고 있다. 프라이버시법 제2항(b)에 담긴 목적구속원칙에 따르면 확인할 수 있는 個人情報를 수집, 저장, 사용 또는 전달하는 행위는 필요하고 합법적인 목적을 위한 것이어야 하며, 그 의도되는 사용을 위하여 해당 정보는 최신의 것으로서 정확하며 그 남용을 막기 위한 적절한 보호책들이 제공되는 방법으로 수집, 저장, 사용 또는 전달하도록 연방기관들에게 요구된다. 또한 개인프라이버시가 침해되는 것을 방지하기 위하여 연방프라이버시법은 법에 다르게 규정되어 있는 경우를 제외하고는 國家機關들에 의하여 개인정보가 수집되고, 저장되고, 사용 또는 전달되는지를 관련 개인이 알거나 동의할 수도 있도록 조치할 것을 연방기관에게 요구하였다. 그런데 聯邦機關들이 소유하고 있는 이러한 기록시스템에 관하여 두 가지 유형의 공개를 연방프라이버시법은 요구한다. 우선 위 법은 기존의 기록시스템이나 바뀐 시스템의 존재와 그 내용에 관하여 개개 機關이 공개하도록 요구한다. 그리고 또한 위 법은 개개 기록시스템들에 개인의 접근을 보장하는 규정들을 공포하도록 개개 기관에게

요구한다. 더 나아가서 외부자들이 聯邦機關의 정보처리실무를 열람할 수 있는 또 다른 방법은 연방기관들이 OMB와 의회에 제출하도록 요구되는 새롭게 실질적으로 바뀐 정보시스템들에 관한 보고서를 보거나 연방프라이버시법의 규정에 따른 기관의 통지와 접근규정을 요약형태로 연방기록소에서 출판하는 인쇄물을 통한 경우이다. 이처럼 연방기록소는 매년 기록시스템에 관한 기관의 통지와 개인의 접근규정들을 모아서 출판한다. 그리고 부당한 정보처리실무로부터 개인을 보호하기 위하여 프라이버시법은 해당 개인이 연방기관의 기록에 담긴 個人情報에 접근, 복사, 수정할 수 있도록 규정하고 있다.[122] 그러나 여기서 중요한 것은 이러한 법규정들을 통하여 개인이 정부의 감시 밑에 있다고 믿을 이유를 갖고 있을 때 관련개인이 이에 관한 접근권을 행사하려고 할 때 美國의 정보보호시스템은 이를 제대로 보호하지 못한다는 것이다. 곧 개인기록의 남용, 어떤 個人情報가 저장되고 어떻게 사용되는지에 관하여 개개인 스스로가 알아내서 통제하라는 것은 國家情報處理를 감독하고 통제하려는 관점에서 본다면 특히 중대한 瑕疵를 드러낸다. 게다가 개인권리를 침해한다고 생각되는 정보실무에 관하여 개인이 불평할 수 있는 특별한 장치가 프라이버시법하에서는 없고 개개 기관들에 의하여 받아들여진 이의제기의 숫자나 그 처리내용에 관해서도 알려진 것이 별로 없다.[123] 현재 OMB 스스로가 이러한 이의제기를 접수하기는 하나 이러한 이의제기가 대단히 드물 뿐만 아니라 國家機關 自體에 제기된 이의제기에 관해서는 아무 것도 모른다. 결국 현실적으로 이러한 情報處理를 감독하는 외부통제기관이 없기 때문에 연방프라이버시법상 기준들이 현실적으로 어떻게 적용되었는지를 안다는 것은 불가능하다.[124] 그런데 연방프라이버시법에 따르면 연방기관들이 소유하고 있는 기록시스템에 관한 공개명령이 있는 바, 이러한 정보처리에 관하여 聯邦機關이 제출한 자료를 OMB가 회람시킨다. 이러한 회람은 해당 기관의 과제수행을 위하여 필요한 정보만을 수집하고 처리, 전달, 사용, 저장하도록 함으로써 국가의 정보처리에 관한 통제를 강화하려는 의도를 갖고 있었다. 따라서 연방기관들이 OMB의 이러한 의도와 지시들에 따른다면 이러한 회람은 나름대로 개인의 프라이버시를 보호하는 의미를 가질 수도 있다. 그러나 현실적으로 이러한 회람은 오로지 聯邦機關의 정보처리행위를 정당화하기 위한 근거만을 만들어 주었을 뿐이다.

이제 미국에서 연방프라이버시법의 이행에 관한 監督을 맡고 있는 管理豫算室(Offiece of Management and Budget, OMB)에 관하여 살펴보아야만 한다. 비

122) 5 U.S.C. §552a2(b)(3), 3(d)·(f).
123) David H. Flaherty, ibid., p.339.
124) David H. Flaherty, ibid., p.322.

록 OMB가 연방프라이버시법하에서 統制를 담당하고 있다 할지라도 美國의 정보보호시스템에서 우선적으로 강조되어야 하는 것은 국가의 정보처리실무를 制限하고 統制하는 실무의 평가와 판단을 위해서는 단순히 한 기관에 초점을 맞추어서는 안된다는 것이다. 그래서 미국에서 개인정보를 보호하기 위한 통제정책을 槪觀하려면 개개 聯邦機關들에 의한 법의 준수여부 및 의회에 의하여 행사되는 통제를 함께 검토하는 것이 필요하다. 우선 1980년까지 管理豫算室(OMB)은 단지 국가의 정보처리에 관한 諮問役割만 담당했을 뿐이고, 그나마 이러한 諮問은 國家機關들을 구속하지도 않았다. 따라서 OMB가 담당하는 주요 기능은 연방프라이버시법에 관한 年例報告書를 만드는 것이었다. 우선 OMB가 그 동안 이루어낸 주요한 업적은 聯邦機關들에게 연방프라이버시법에 관한 정책지침들을 내리는 것이었다. 비록 이러한 지침이 구속력을 갖고 있지 않다 할지라도, 보통 聯邦機關들이 OMB와 충돌하기를 원하지 않으므로 가능한 한 OMB의 지침을 존중하려고 노력하였다. 그러나 위에서 이미 언급된 것처럼 OMB가 1975년 프라이버시법의 집행에 관하여 만든 이러한 지침이 중요한 역할을 하기는 했지만 이는 결코 구속력있는 法律이나 法規命令은 아니었다. 그 뒤 OMB는 연방프라이버시법하에서 그들이 담당하고 있는 몇몇 과제들을 다른 機關들에게 위임하였다. 특히 그 중에서 人事運營室(the Office of Personnel Management, OPM)은 중앙통제하에 있는 정부기록시스템들을 감독한다. 이러한 시스템은 약 700만명이 넘는 개인기록을 담고 있는 9개의 개인기록시스템들이다. 그러나 불행히도 이러한 공무원기록시스템이 엄격한 통제하에 있는지를 판단할만한 충분한 자료들이 아직까지는 없다. 어쨌든 1980년에 다시 카터행정부는 OMB내에 OIRA라는 기관을 만들었다. OIRA는 기록시스템들을 具體的으로 監督하기 위하여 국가기관을 통한 個人情報의 수집이 명확성원칙에 근거하고 있는지와 새로운 정보시스템들에 관한 보고서의 검토에 종사한다. 그래서 매년 OIRA는 개개 연방기관으로부터 프라이버시보호에 관한 보고서를 받고 연방프라이버시법에 관한 대통령의 보고서를 준비한다. 그리고 OIRA는 제안된 法律草案에 관하여 논평하기도 한다. 따라서 새롭게 제안되거나 바뀐 기록시스템들에 관하여 聯邦機關들이 OIRA에 해야만 하는 事前通知는 연방프라이버시법의 준수여부를 확보하기 위하여 OIRA가 사용할 수 있는 가장 중요한 수단중 하나이다. 그리고 OIRA는 새로운 시스템에 관한 기관의 보고서를 OMB가 검토하기 위하여 이에 관한 18가지 질문들을 던지고 시스템의 요약평가 및 이에 관한 논평을 준비하는 형태로 기입할 것을 요구한다. 그 다음으로 OIRA가 활동하는 주요한 두 번째 영역은 "日常的인 情報使用"의 경우에 연방프라이버시법의 적용을 배제하는 규정[125]의 적용을 받으려는 聯

邦機關의 주장을 심사하는 것이다. 그런데 1975년 OMB지침에 따르면 "日常的인 情報使用"은 聯邦機關의 기록이 저장되는 목적과 양립할 수 있어야 할 뿐만 아니라 이러한 기록이 저장목적과 관련되어야만 한다고 결정하였다. 새로운 정보시스템이나 바뀐 정보시스템에 관하여 개개 機關은 그들이 제안하는 日常的인 情報使用이 연방프라이버시법 (a)(7)에 규정된 요구를 어떻게 준수하는지를 OIRA에게 설명해야만 한다. 여기서 정보처리의 일상적 사용을 정당화하기 위한 척도로는 "기능적으로 동등한 사용"과 "적절하고 필요한 다른 사용"들간에 비교하는 것이라고 OMB는 강조한다. 이에 따라서 OIRA는 정기적으로 일상적인 정보사용실무를 심사하고 이를 벗어난다고 판단되는 정보처리를 못하도록 가끔 요구한다. 그럼에도 불구하고 聯邦機關의 情報處理에 관하여 統制해야만 하는 OIRA 또한 여전히 情報處理에 관한 통제와 책임을 일차적으로 연방 기관 스스로에게 맡긴다는 것이다. 따라서 "日常的인 情報使用"에 관하여 의견이 서로 충돌할 경우에 연방프라이버시법하에서 최종적으로 결정을 내릴 권한을 갖고 있는 기관들을 OMB가 설득하려고 노력할 수 있을 뿐이라는 데에 문제가 있다. 게다가 현재로서는 聯邦機關들이 이에 관하여 필요한 通知를 제출할지를 확실하게 알아낼 수 있는 어떤 수단도 OMB는 확보하고 있지를 않다. 결국 OMB 스스로가 연방프라이버시법하에서 맡고 있는 役割을 개인의 프라이버시이익과 정부의 정보처리필요성간의 형량으로 보는데 이는 개인의 프라이버시를 보호해야만 한다는 시각으로부터 본다면 OMB의 役割을 처음부터 대단히 제한적인 것으로 본다는 것을 의미한다. 결국 OMB는 어떤 독립된 行政機關도 아니고, 독립된 行政委員會도 아니다. OMB에 따르면 연방프라이버시법을 준수할 궁극적인 책임은 개개 연방기관들에게 있다는 것이다. 그래서 전체적으로 본다면 개인의 프라이버시를 보호해야할 과제는 OMB가 담당하는 여러 활동중 아주 작은 부분에 불과할 뿐이고 이에 따라서 나타나는 결과는 國家의 情報處理를 충분히 감독, 통제하지 못한다는 것이다.

그리고 美國에서 개인정보보호의 통제와 관련되는 중요한 문제로 기록연결문제가 있다. 위에서 설명한 것처럼 美國에서는 기록연결을 컴퓨터매칭(연결)이라고 한다. 이러한 연결계획은 우선 카터행정부시대에 건강, 교육, 복지를 담당하는 부처가 1977년에 만들었다. 이러한 카터행정부의 계획을 레이건 행정부가 이어받음으로써 국가복지프로그램에서 사기, 낭비, 남용의 소지를 없애려는 구체적인 목표들을 두 행정부는 공유하였다. 마침내 1988년 10월 18일 컴퓨터연결과 프라이버시보호법이 제정, 공포되었다. 이 컴퓨터연결과 프라이버시보호법은 제한된 범위, 곧 ① 연

125) §552a(b)(3).

방수혜프로그램을 위한 資格을 확정, 확인하거나 ② 이러한 프로그램 하에서 이미 지불되었거나 만기일이 넘은 債務를 공제할 목적으로 전산화된 기록들을 비교하는 데에만 적용되었다. 컴퓨터연결과 프라이버시보호법은 컴퓨터연결프로그램들을 규율하고 통제하려고 하며, 연결프로그램들이 잘 행해진다는 것을 확실히 하기 위하여 컴퓨터연결을 하거나 이에 참여하는 기관들에게 컴퓨터연결을 감독하고 이를 승인하기 위하여 해당기관의 상급관청들로 구성된 情報完全性委員會(Data Integrity Boards)를 만들도록 요구한다. 또한 연결프로그램이나 기록시스템들 속에서 중대한 변화가 계획되거나 이에 관한 새로운 제안을 하는 聯邦機關들은 OMB와 상원 및 하원의 감독위원회에 이에 관하여 적절히 사전에 통지해야만 한다.[126] 그런데 1982년 5월 11일 만들어진 컴퓨터연결에 관한 OMB의 지침은 연방프라이버시법의 이행에 관한 1975년 지침처럼 컴퓨터연결과 프라이버시보호법의 시행을 위하여 만들어진 것이다. 이러한 지침은 연방프라이버시법상 "日常的인 情報使用"規定에 근거하여 한 기관으로부터 다른 기관으로 컴퓨터연결을 통하여 個人情報의 전달을 정당화하는 것을 컴퓨터연결에 관한 지침이 목표로 하였다. 1979년 컴퓨터연결프로그램에 관한 OMB의 지침 또한 연결프로그램에 내재해 있는 개인프라이버시를 침해할 수 있는 위험성을 인정하였다. 그러나 이러한 OMB의 지침은 勸告的 效力을 갖고 있을 뿐 제정법 자체에 따르도록 하는 拘束力을 갖고 있지는 않다. 게다가 개인의 프라이버시를 보호하기 위하여 컴퓨터연결프로그램이 확인할 수 있는 개인정보의 내용과 양을 최소해야만 하며 연결프로그램에 따라 허용되는 모든 일상적인 정보사용들이 가능한 한 구체적이고 제한되어야만 한다는 몇몇 유용한 통제들을 포함하였던 1978년 OMB지침내용이 불행히도 1979년 지침에서는 삭제되고 말았다. 게다가 1982년에 만들어진 OMB의 새로운 지침들은 OMB의 감독역할을 축소시키고 말았다. 결국 컴퓨터를 통한 기록연결이 OMB의 이러한 지침 및 연방프라이버시법상 규정들에 근거하여 행해지는 바, 컴퓨터연결을 통하여 어떤 기관이 다른 기관들에게 정보를 제공하면서 계속해서 연방프라이버시법을 준수하는지를 통제한다는 것은 불가능하다. 왜냐하면 연방프라이버시법의 준수여부를 감독할 어떤 聯邦機關도 존재하지 않기 때문이다. 물론 컴퓨터연결에 관한 1982년 OMB지침은 개인의 프라이버시를 보호하기 위하여 예를 들어서 컴퓨터연결을 통하여 필요한 최소한도의 정보만이 공개되어야 하고, 정보사용에 관한 개인의 書面同意가 있어야만 하고, 기록의 처분과 반환에 관한 통제가 있어야 하며, 새로운 기록시스템의 설치에 관하여 의회와 OMB에게 통지되어야 한다는 몇몇 현실적인 대책들을 제시하였

126) 5 U.S.C. 552 a, section 2, 3

다. 문제는 연방프라이버시법과 OMB의 지침에 규정된 "日常的인 情報使用"이란 규정을 통하여 컴퓨터연결프로그램을 정당화한다는 것이다. 결국 현재 미국에서 행해지고 있는 정보연결프로그램과 연결실무가 부적절하다는 것은 이러한 컴퓨터연결활동들에 내재하여 있는 충돌하는 이해관계들을 토론하고 형량할 수 있는 확립된 기구나 광장이 없다는 데에 있다. 컴퓨터연결에 관한 기관내부의 심사나 기준들이 존재하지 않을 뿐만 아니라 연방프라이버시법하에서 컴퓨터연결에 관하여 OMB에게 공식적으로 통지하여야 하는 시스템이 제대로 작동하고 있지도 않다.

그러다 보니 情報社會에서 개인의 私生活保護에 관하여 많은 연구를 하고 있는 플래허티는 美國의 프라이버시법이 대폭적으로 개정될 필요가 있다고 주장한다. 곧 그는 프라이버시법제정 이후에 새롭게 등장한 情報通信技術의 적용에 의하여 개인의 프라이버시를 침해할지도 모르는 위험성을 방지할 수 있도록 美國의 현행 프라이버시법은 개정되어야만 한다고 주장한다.[127] 특히 그는 연방프라이버시법이 제정된 이후에 國家에 의한 情報處理技術에 급격한 변화가 발생하였음에도 불구하고 이러한 정보통신기술의 적용을 통제하는데에 실패하였다는 것을 강조한다.[128] 따라서 서유럽국가들에서처럼 個人情報保護에 관한 일반적인 統制機關을 만드는 것이 현재 美國에서 어렵다면 OIRA내에 프라이버시정책국을 만드는 것이 바람직할지도 모른다고 그는 언급하고 있다. 물론 프라이버시법의 遵守與否를 개개 국가기관이 책임지는 모델이 꼭 잘못되었다고 말할 수는 없으나 外部機關이나 議會를 통한 統制를 강화할 필요성이 강하게 요구된다는 것이다.

어쨌든 플래허티는 美國에서 個人情報를 보호하기 위하여 프라이버시보호위원회를 설치하는 것이 가장 바람직하다고 주장한다. 그리고 이러한 프라이버시위원회는 다음과 같은 책임과 권한들을 가져야 한다고 역설하고 있다[129] : ① 우선 이러한 委員會는 個人情報保護와 관련되는 모든 상황에서 이러한 個人情報가 保護되고 있는지를 세밀하게 검토하고, 특히 個人情報를 보호하기 위한 경보시스템으로서 기능해야만 한다. ② 이 위원회는 연방기관의 모든 情報處理過程에서 개인의 프라이버시가 보호되는지를 監督해야 한다. ③ 프라이버시법에 규정된 연방기관의 義務遂行與否를 감독하고, ④ 프라이버시법규정의 준수여부를 감독하기 위하여 연방기관의 정보처리시스템을 조사, 열람, 감독하고, ⑤ 연방차원에서 個人情報保護를 위한 적절한 안전지침과 실무지침을 발전시키며 ⑥ 특정유형의 개인정보시스템들에 관하여 필요하다고 생각하는 적절한 규정들을 권고하고, ⑦ 개인프라이버시를 위하여 情報

127) David H. Flaherty, ibid., p.368.
128) David H. Flaherty, ibid., p.367.
129) David H. Flaherty, ibid., p.365 이하 참조.

通信技術의 발전을 평가하며 ⑧ 美國에서 모든 유형의 프라이버시문제들에 관하여 연구를 하고 기록한다. 이러한 委員會는 가능한 정도로 立法府와 行政府만큼 독립되어야 하며 委員會는 그들의 과제수행을 위하여 연방기관들과 합의, 조정, 협조할 수 있는 권한을 가져야 한다.

第5節 個人情報保護를 위한 統制機關의 必要性

1. 統制機關의 地位와 權限

個人情報保護法의 制定目的은 새로운 情報通信技術의 발전에 발맞추어 효율적이고 헌법합치적인 調定規定과 個人情報保護規定들을 사전에 또는 동시에 준비하도록 하는 것이다. 그러나 情報社會에서 국민의 私生活을 보호하기 위하여 個人情報保護法을 제정하는 것만으로는 충분하지 않다. 왜냐하면 오늘날 새로운 기술들의 발전 및 적용가능성이라는 점에서 볼 때 法律家 또는 立法者는 그전보다 더 불리한 위치에 놓여 있을 뿐만 아니라 더 이상 개인 스스로 자신의 정보를 보호하고 통제할 수 없기 때문이다. 따라서 個人情報保護法 制定 그 자체도 중요하지만 시민을 효율적으로 보호하기 위해서는 국가나 사회의 情報處理를 통제하는 統制機關의 설치 및 활동이 절대적으로 요구된다. 결국 公的 領域에서 이러한 統制機構를 설치하는 근본적인 임무는 國家의 지나친 情報調査와 處理로부터 시민들을 보호하는 데에 있다. 이러한 통제장치가 없다면 國家機關에 의한 제한되지 않는 個人情報의 수집과 전달, 個人私生活의 지나친 감시를 방지한다는 것이 불가능하다. 특히 이는 個人情報保護에 관한 미국시스템을 본다면 쉽게 이해할 수 있다. 우선 美國의 연방프라이버시법하에서 制定法의 遵守與否를 판단하는 일차적 기관은 法院인 바, 이미 法院이 이러한 분야에서 효율적인 統制機關으로서 불충분하다는 것은 미국에서 그 동안의 실무와 경험을 통하여 입증된다. 게다가 통상적인 公務員에 의한 內部監督이란 너무 약하고 형식적인 통제가 되어버린다.[130] 더 나아가서 個人情報保護에 관한 統制機關의 必要性은 國際的인 側面에서도 강조되고 있다 : 국경을 넘는 정보흐름, 증가하는 국제적 국가간 정보교환을 배경으로 하여 계속해서 국제적 통제기관확립의 필요성 및 한편으로는 國際機關과 國家機關間에 또 다른 한편으로는 國家機關相互間에 긴밀하고 수평적이거나 수직적으로 제도화된 공동작업의 필요성이 최근에

130) 미국에서 레이건정부 시대에 OMB의 경우에서처럼 이러한 기관이 정치적 고려 하에 있으므로 연방정보보호위원회가 미국에서 만들어지지 않는 한, 개인의 프라이버시를 보호하는 연방시스템은 부적절하다고 말할 수 있다. 특히 개인정보보호에 대한 관료적 저항을 예상할 수 있기 때문에 정보보호기관은 필수적으로 필요하다.

등장하고 있다.

궁극적으로 情報保護委員會와 같은 統制機關은 개인의 私生活을 보호하기 위한 경보시스템으로 작용한다. 이들은 國家의 情報處理를 지속적으로 監督하고 法律에 규정된 목표를 준수하는지를 검토한다. 그리고 이들은 구체적인 국가정보시스템들의 작용을 규율하고 情報通信技術의 새로운 적용을 감독, 평가한다. 이러한 統制機關은 모든 國家機關을 감독해야만 하며 특히 경찰과 첩보기관을 효율적으로 감독할 수 있는 방안을 강구해야만 한다. 결국 이러한 임무를 수행하기 위해서는 立法府, 司法府, 行政府 어느 하나에 속하지 않는 통제기관을 만들어야만 한다. 왜냐하면 이러한 統制機關은 충돌하는 여러 이해관계들을 형량해야 하기 때문이다.

그럼에도 불구하고 統制機關은 우선적으로 그들의 활동과 정책을 국가와 사회의 情報調査와 處理를 통제하기 위한 것으로 한정해야만 한다. 곧 統制機關은 개인의 情報保護를 우선적인 목표로 하여 情報社會에서 개인의 여러 권리들을 보장하고 강화하도록 노력해야만 한다. 결국 국가나 사회 전체를 위한 情報政策을 발전시키는 것은 바람직하기는 하나 統制機關은 個人情報保護에 집중해야만 한다. 統制機關은 情報政策의 형성과 집행에 관하여 책임을 지는 國家機關들이 관련정책을 만들고 효율적으로 집행하는데에 기여할 수는 있으나 주도할 수는 없다.

이에 따라서 個人情報를 보호하기 위한 통제기관의 임무를 열거하면 다음과 같다 : 물론 個人情報保護에 집중되는 情報保護委員會의 활동이 국가적인 정보정책 전체를 이루는 것은 아니라 할지라도 國家의 부당한 정보처리를 제한하려고 노력하는 것 자체가 國家의 일관된 정보정책형성에 지속적으로 기여하는 것이기도 하다. 이에 따라서 個人情報保護委員會는 부당한 감시를 받고 있다고 느끼는 시민들의 권리보호를 위하여 노력하는 것이 이러한 위원회의 일차적인 중요임무이다. 그러나 이 委員會의 役割은 이것으로 한정되지 않는다. 個人情報保護委員會는 여러 가지 방법으로 국가의 정보처리과정에서 個人情報가 보호될 수 있도록 일반적이고 체계적으로 統制하며 이에 관한 代案提示를 하기 위하여 노력해야만 한다. 그렇다면 국가의 정보처리에 관한 監督이 바로 統制機關에게 부과되는 중요한 임무이다. 個人情報保護法이 반드시 새로운 정보기술의 도입에 적대적이지도 않고, 統制機關이 국가의 정당한 정보처리활동들을 불필요하게 방해하려고 해서도 안된다. 새로운 정보통신기술의 도입이 국가와 사회 속에서 개인의 自律을 희생시키면서 더욱 더 정교하고 통합된 개인정보시스템을 만들 위험성을 막는 것이 個人情報保護法의 일차적인 목적이다. 따라서 情報保護委員會의 또 다른 역할은 새로운 정보기술형태의 잠재적 영향력과 효과를 판단하여서 이러한 정보통신기술의 적용이 계획단계에서부터 個人

情報를 보호하는 방향으로 전개될 수 있도록 노력하는 것이다. 그러기 때문에 이러한 역할을 담당하기 위하여 情報保護委員會에 상담과 조정기능 외에 위험예방기능이 요구된다.[131] 급속하게 발전하는 情報通信技術, 거대한 정보처리시스템의 엄청난 복잡성 등 때문에 統制機關이 계획과 절차단계에서부터 참여하고 個人情報保護觀點에서 토론해야만 한다. 따라서 이러한 統制機關에서 일하는 사람들이 情報通信技術에 관하여 어느 정도 이해하고 있어야만 한다. 그리고 情報保護委員會는 個人情報를 다루는 모든 구체적 法律과 규정들에 담긴 情報保護原則들을 國家機關들이 준수하는지를 감독해야만 한다. 統制機關은 구체적인 法律들에서 一般的인 情報保護原則들이 실현될 수 있도록 노력해야만 하며 구체적인 法律들에서 일반적인 정보보호원칙들을 실현하는 해결책들을 도출해야만 한다. 마지막으로 컴퓨터연결을 통한 個人情報의 결합을 통제하는 것이 현재 個人情報保護에 관한 중심문제로서 바로 情報保護委員會가 해결하려고 노력해야만 하는 분야이기도 하다.

이제 개개 國家의 憲法的, 法的, 行政的 傳統들이 다름에도 불구하고 情報保護委員會의 權限과 運用에 관한 이상적인 모델을 발전시키기 위한 논의를 시작하여야 한다. 우선 여기서 인식하여야 하는 것은 어떤 통제모델이 個人情報를 보호하는데 가장 좋은지는 아직 확정적으로 논의가 끝나지 않았다는 것이다. 왜냐하면 그 동안 기능해온 그 어떤 모델도 완전히 만족스럽게 기능하지는 않았기 때문이고, 또한 채택된 모델들이 理論的, 學問的 論議에 바탕을 두었다기 보다는 개개 나라의 政治的, 憲法的 傳統에 많이 의존하는 것처럼 보였기 때문이다. 그럼에도 불구하고 그 동안 여러 나라의 많은 통제모델들을 살펴 본 결과 다음과 같은 결론을 도출할 수 있다 : 우선 정보사회에서 보호되어야 하는 개인의 권리들을 立法府가 해당 법률들에서 충분히 구체화하였다면 執行機關이나 統制機關은 해당 법률을 적용하고 그 원칙들을 해석할 때 지나치게 넓은 裁量權을 행사해서는 안된다.[132] 특히 일반적으로 중요한 사회적 가치들의 형량에 관해서는 다른 國家機關 - 특히 立法府 - 이 이러한 情報保護委員會보다 더 나은 입장에 있다. 다시 말하자면 해결하기 어려운 이해관계가 충돌하는 경우나 情報保護委員會와 國家機關間 衝突境遇는 대부분 立法府가 원칙적으로 法律을 통하여 해결하도록 노력해야만 한다. 그리고 個人의 私生活과 다른 충돌하는 가치들을 형량할 때 個人情報保護委員會의 우선적인 역할은 보호를 필요로 하는 개인의 權利들을 위하여 지속적으로 감독, 조사하는 데에 있다. 위에서 이미 설명된 것처럼 스웨덴과 프랑스의 통제모델 - 許可시스템 - 은 많은 문

131) 사전적인 위험분석과 평가를 통하여 정보시스템들의 성립절차 속에서 이미 규범적인 요구들을 받아들일 수 있다.

132) 스웨덴과 프랑스가 바로 이러한 유형에 속한다.

제를 갖고 있는 통제모델이다. 왜냐하면 이러한 통제방식은 統制機關에 너무 많은 부담을 지우기 때문에 결국 統制機關의 作業方式이 결국에는 너무 관료적이고 형식적인 것처럼 되어 버리기 때문이다. 모든 것을 통제한다는 것이 처음부터 불가능하며 그러다보니 나중에는 정작 중요한 과제들마저도 제대로 수행하지 못하게 되는 결과를 낳는다.

따라서 우선 公的 領域에서 개인정보시스템의 작동에 관하여 諮問權限을 갖는 獨逸이나 캐나다의 정보보호위원회시스템이 더 효율적이라고 말할 수 있다. 이러한 諮問(相談)시스템은 統制機關의 許可를 行政府가 저항하거나 무시할 수 있는 위험성을 극복할 수 있는 장점을 갖고 있으며 이러한 통제기관 또한 탄력적이면서 실용적인 방법으로 행동할 수 있다. 다만 情報保護委員會들이 法律上 그들에게 부여된 목적들을 달성하기 위하여 이러한 설득 및 상담권한들에 계속해서 의존해야만 하는지는 앞으로 더 연구를 해야만 하는 문제이다. 어쨌든 이러한 統制機關은 다양한 이해관계자간에 독립적이고 신뢰받을만한 조정자로 등장한다. 특히 이러한 統制機關에게는 技術的 專門知識의 缺如와 直接的인 民主的 正當性의 缺如 때문에 立法府나 行政府 대신에 統制機關이 정보정책에 관한 결정들을 내리는 것은 정당하지도 않고 적합하지도 않다. 특히 프랑스나 스웨덴에서처럼 승인절차제도 자체속에 정보보호기능의 비탄력성과 관료화라는 피할 수 없는 위험성이 존재하며 더욱이 이를 통하여 統制機關이 行政機關으로 바뀔 위험성마저 갖고 있다.[133]

또한 情報保護委員會의 구성과 관련하여 초기의 프랑스에서처럼 情報保護委員會의 長에 政治家를 임명하는 것은 덜 성공적인 모델이다. 統制機關이 個人情報를 효율적으로 보호하기 위해서는 상당한 정도의 리더십을 갖고 있는 常勤職 委員長이 있어야 한다. 또한 個人情報保護의 성공적인 수행은 적극적이고, 열성적이며 능력있고 헌신적인 스탭을 필요로 한다. 그리고 이미 설명된 것처럼 情報保護委員會는 그들에게 부여된 과제를 효율적으로 수행하기 위하여 獨立性이 보장되고 신분이 法官에 해당하는 정도는 보장되어야 한다. 다만 실제로 정부의 豫算統制가 情報保護委員會의 활동을 상당히 위협할 수 있다는 것을 기억하여야 한다.

2. 우리 나라의 現行法內容 및 改正必要性

우리 나라 個人情報保護法上 監督機關은 總務處로 되어 있다. 위 법에 따르면 總務處長官은 公共機關의 長에게 個人情報의 처리에 관한 자료의 제출을 요구할 수

133) 프랑스모델의 분석에서 강조되었던 것처럼 간섭권한은 시민권리의 보호와 제도적 통제의 효력 그 자체를 확실하게 할 수 있을지도 모르는 만병통치약을 설명하지는 않는다.

있으며[134] 관계기관의 장에게 個人情報의 보호에 관하여 의견을 제시하거나 권고를 할 수 있다.[135] 그리고 중앙행정기관이외의 공공기관에 대해서는 총무처 이외에도 관련중앙행정기관으로 하여금 지도, 감독하도록 하고 있다. 아울러 국무총리소속하에 個人情報保護審議委員會를 설치하도록 하였다.[136] 이 委員會는 위원장 1인을 포함한 10인 이내의 위원으로 구성하고 위원은 공공기관의 소속직원과 個人情報에 관한 학식과 경험이 풍부한 자중에서 위원장의 추천으로 국무총리가 임명 또는 위촉하도록 하였다.[137] 이 위원회는 個人情報保護에 관한 정책이나 제도의 개선에 관한 사항이나 個人情報의 이용과 제공에 관한 공공기관간 이견조정 등에 관한 사항을 심의하도록 하고 있다.[138] 이에 따라서 個人情報保護審議委員會는 현재 총무처차관을 위원장으로 하여 學界, 法曹界, 言論界, 女性界 및 관련기관의 공무원 등이 참여할 수 있도록 관련기관, 단체의 추천을 거쳐 민간인 5명, 총무처, 법무부, 정보통신부 등 관련기관 공무원 4명으로 구성하였다.[139]

위에서 이미 설명한 것처럼 우리 나라 個人情報保護法은 많은 문제점을 갖고 있는데, 그중 가장 커다란 문제는 바로 統制機關의 缺如이다. 個人情報保護法의 목적은 새로운 정보통신기술의 발전에 대응하여 효율적이고 헌법합치적인 조정규정과 개인보호규정들을 事前에 또는 적어도 동시에 준비하도록 하는 것이다. 그러나 情報社會에서 국민의 私生活을 보호하기 위하여 個人情報保護法을 제정하는 것만으로는 충분하지 않다. 왜냐하면 오늘날 새로운 기술들의 발전과 그 적용가능성에 비추어 볼 때 法律家 또는 立法者는 그전보다 더 불리한 위치에 놓여 있을 뿐만 아니라 개인 스스로가 이를 통제할 수 있는 능력이나 기회를 가질 수 없는 불리한 위치에 놓여 있기 때문이다. 따라서 個人情報保護法 制定 그 자체도 중요하지만 시민을 효율적으로 보호하기 위해서는 국가나 사회의 정보처리를 통제하는 統制機關의 설치 및 활동이 절대적으로 요구된다. 결국 公的 領域에서 이러한 統制機構를 설치하는 근본적인 임무는 國家의 지나친 情報調査와 처리로부터 시민들을 보호하는데에 있다. 이러한 통제장치가 없다면 국가기관에 의한 제한되지 않는 個人情報의 수집과 전달, 個人私生活의 지나친 감시를 방지한다는 것이 불가능하다. 그런 의미에서 본다면 우리 나라 個人情報保護法은 결국 統制機關을 통한 감독없이 개개 국가기관에게 個人情報를 보호하도록 맡기고 있으며 이를 개개인이 자신에 관한 기록을 열람

134) 개인정보보호법 제18조.
135) 同法 제19조.
136) 同法 제20조.
137) 同法 시행령 제27조.
138) 同法 제20조.
139) 한국전산원, 1997 국가정보화백서, 668면.

하는 것 등을 통하여 통제하는 아주 제한적이고 비효율적인 방식을 채택하고 있다. 결국 우리 나라 個人情報保護法의 가장 취약한 점은 바로 개개 국가기관이 제대로 個人情報를 보호하고자 하는지를 통제할 권한을 가진 기관이 전혀 없기 때문에 個人情報가 제대로 보호되지 못하고 있다는 데에 있다. 표면상으로는 總務處가 이러한 임무를 담당하고 있는 것처럼 보이나 이는 美國의 사례를 보아도 실패할 수밖에 없다. 이미 法院이 이러한 분야에서 효율적인 통제기관으로서 불충분하다는 것은 美國에서 그 동안의 경험을 통하여 입증되었다. 게다가 통상적인 공무원에 의한 內部監督이란 너무 약하고 형식적인 통제가 되어버린다. 이는 그나마 우리 나라에서는 그동안 국가기관을 통한 개인정보의 처리와 연결에 관하여 통제되어서 시정된 사례가 전혀 보고되거나 기록되고 있지 않다는 것이 이를 명확하게 드러내고 있다.

그렇다면 우선 우리 나라의 현행 個人情報保護法처럼 統制機關의 권한이나 지위, 조직에 관한 사항을 下位法規에 위임하는 것 자체에 문제가 있다. 個人情報를 보호하기 위하여 활동하는 統制機關은 매우 중요하므로 立法者가 직접 이에 관한 사항을 法律로 자세히 규정해야만 한다. 그 다음으로 우리 나라에서도 개인의 私生活保護를 위한 경보시스템으로서 情報保護委員會와 같은 통제기관을 설치하여야 한다. 이러한 統制機關은 우선 국가의 정보처리를 지속적으로 감독하고 法律에 규정된 목표를 준수하는지를 검토하여야 한다. 그리고 이들은 구체적인 국가정보시스템들의 작용을 규율하고 정보통신기술의 새로운 적용을 감독, 평가하여야 한다. 특히 統制機關은 모든 國家機關을 감독하여야 하며 특히 경찰과 첩보기관을 효율적으로 감독할 수 있는 방안을 강구해야만 한다. 결국 이러한 임무를 수행하기 위해서는 立法府, 司法府, 行政府중 하나에 속하는 국가기관이 아닌 統制機關을 만들어야 하는 것이다. 왜냐하면 이러한 統制機關은 충돌하는 여러 이해관계들을 형량하여야 하기 때문이다. 그럼에도 불구하고 이러한 統制機關은 그들의 활동과 정책을 국가와 사회의 情報調査와 처리를 통제하는 것에 집중해야 한다. 곧 統制機關은 個人의 情報保護를 우선적 목표로 하여 情報社會에서 개인의 여러 권리들을 보장하고 강화하도록 노력하여야 한다. 그렇다면 위에서 이미 설명된 것처럼 스웨덴과 프랑스의 통제모델 - 허가시스템 - 은 문제가 있는 통제모델이다. 왜냐하면 이러한 통제방식은 統制機關에게 너무 많은 부담을 지우기 때문에 통제기관의 작업방식이 결국에는 너무 관료적이고 형식적인 것으로 되어 버리기 때문이다. 이러한 통제시스템 속에서 모든 것을 통제한다는 것은 불가능하게 되고 그러다보니 나중에는 정작 중요한 과제들마저도 제대로 수행하지 못하게 되는 결과를 낳는다. 따라서 우선 公的 領域에서 개인정보시스템의 작동에 관하여 諮問權限을 갖는 독일이나 캐나다의 정보보호시스템이 더 효율적이다. 이러한 자문(상담)시스템은 통제기관의 허가에 대하여 행

정부가 저항하거나 무시할 수 있는 위험성을 극복할 수 있는 장점을 갖고 있으며 자문(상담)권한을 갖는 통제기관 또한 유연하며 실용적인 방법으로 행동할 수 있다.

그 다음으로 統制機關은 부당한 감시를 받고 있다고 느끼는 시민들의 권리보호를 위하여 노력하는 것이 이러한 위원회의 또다른 중요기능에 속한다. 이를 넘어서서 統制機關은 다양한 방법을 통하여 국가의 정보처리과정에서 個人情報가 보호될 수 있도록 일반적이고 체계적인 감독과 대안제시를 하기 위하여 노력하여야 한다. 이러한 국가정보처리의 감독행위가 바로 統制機關에게 새롭게 부과되는 중요한 임무이다. 이를 통하여 새로운 정보통신기술의 도입이 개인의 자율을 희생시키면서 더욱 더 정교하고 통합된 개인정보시스템을 만들 위험성을 막아야만 한다. 따라서 個人情報保護委員會는 새로운 정보기술형태의 잠재적 영향력과 효과를 판단하여서 이러한 정보통신기술의 적용이 계획단계에서부터 個人情報保護와 조화될 수 있도록 노력하여야 한다. 이에 따라서 情報保護委員會에 상담과 조정기능외에 위험예방기능이 요구된다.[140] 그리고 統制機關은 個人情報處理와 관계되는 중요사항에 대하여 매년 의회에 年例報告書를 제출하고 個人情報保護와 관련되는 事案에 대하여 여론매체 등을 이용하여 널리 알리고 시민에게 홍보하여야 한다. 마지막으로 컴퓨터연결을 통한 個人情報의 결합을 통제하는 것이 현재 個人情報保護의 중심문제로서 바로 情報保護委員會가 해결하려고 노력하여야 하는 분야이기도 하다. 이러한 많은 일들을 하기 위하여 한 사람의 통제관을 두든, 情報保護委員會를 만들든간에 이러한 統制機關은 직접 議會가 선출하여야 하고 그 신분은 法官에 준할만큼 獨立性이 보장되고 豫算도 직접 편성할 수 있어야만 한다.

---

140) 사전적인 위험분석과 평가(판단)를 통하여 정보시스템들의 성립절차(과정) 속에서 이미 규범적인 요구들을 받아들일 수 있다. 자유공동체 속에서 통제는 합리적인 결정절차, 민주적으로 정당화되는 국가활동, 정보통신기술의 사회적 일치(조화)성 및 헌법일치(조화)성의 필요한 구성부분을 표현한다.

第5章 結 論

1. 情報秩序란 개념은 통일적으로 이미 확정된 개념이 아니라 경제질서와 아주 유사하게 情報調査나 처리 등에 관한 모델개념이다. 결국 여기서 구체적으로 정보처리 및 전달과 관련되는 모든 규정들에 관하여 상세하게 그 내용을 지시할 수는 없지만 全體情報秩序를 지도하는 이념을 추상적이고 일반적으로 제시하여야 하는 바로 그러한 질서개념이다. 이러한 논의가 우선 선행되어야 개개 분야에서 이러한 원칙과 이념이 어떻게 적용되어야 하는지를 제대로 살펴볼 수 있는 것이다. 그렇다면 궁극적으로 우리가 지향하여야 하는 情報秩序는 人間指向的 情報秩序이다. 곧 인간우호적이고 인간이 통제할 수 있는 정보시스템구조이어야 한다는 것이다. 이러한 목적달성을 위하여 事後的으로 개인의 권리를 보호할 뿐만 아니라 계획, 집행시 관련자의 포괄적 참여와 협조가 필요한 것이다. 그렇다면 情報技術을 통제하고자 하는 것은 새로운 정보통신기술의 발전을 방해하려는게 아니라 바로 이러한 발전이 인간우호적이도록 조화시려는 것임을 반드시 기억하여야 한다. 개개 경우에 이러한 통제가 어느 정도 행하여져야 하는지는 통제되어야 하는 情報技術의 위험성에 우선 달려있다. 이러한 情報技術에 관한 판단은 먼저 立法者가 해야만 한다. 결국 이는 정보흐름의 사회적응성과 바람직함에 대하여 결정할 임무를 立法者가 일차적으로 부담하여야 함을 뜻한다. 이러한 立法者의 지침속에 情報秩序의 원칙과 기준에 관한 중요한 내용들이 존재한다. 立法者가 필요한 法律을 제정함으로써 일차적인 임무를 이행한 경우에는 그 다음으로 法律이 존재하는가가 아니라 이미 존재하는 法律이 제대로 지켜지는가를 분석해야 한다. 이러한 검토와 분석을 거쳐서 비로소 情報秩序의 원칙과 기준이 개개 영역에서 어떻게 구체화되어야 하는지가 심도깊게 다루어질 수 있다. 결국 법제정과 법적용에서 이러한 토론과 분석을 통하여 법이 학문적, 기술적 발전에 적응하도록 할뿐만 아니라 이를 넘어서서 새로운 情報技術을 도입하려고 하는 사회와 정치에게 이에 관하여 다시 한번 생각하고 결정할 수 있는 기회를 제공하게 되는 것이다.

2. 컴퓨터를 통한 무제한적 처리능력과 저장능력이 순식간에 엄청난 정보를 파악할 수 있는 가능성과 결합함으로써 관련자가 자기에 관한 정보의 처리와 결합이 정당한지를 충분히 통제할 수 없는 상황이 발생할 수 있게 되며 이를 통하여 지금까지는 인식되지 못하였던 개인에 관한 새로운 통제수단이 등장한 것이다. 따라서 情報社會에서 개인의 私生活自由는 情報自己決定權을 통하여 적극적으로 보호되어야

한다. 여기서 情報自己決定權이란 개인관련정보의 사용과 공개에 대하여 원칙적으로 개인 스스로 결정할 권리이다. 결국 이러한 권리는 원칙적으로 그 자신이 스스로 개인관련정보의 공개와 이용에 대하여 결정할 권한을 보장하기 때문에 누가, 무엇을, 언제 그리고 어떠한 경우에 자기에 관하여 아는지를 시민들이 더 이상 알 수 없는 사회질서 및 이를 가능하게 하는 법질서는 情報自己決定權과 조화되지 못한다. 그러므로 情報自己決定權의 목표는 개인의 교섭능력을 보장하는 데에 있다. 결국 이러한 情報自己決定權을 바탕으로 하여 개인은 국가권력에 대하여 자기 자신에 대한 어떤 정보를 조사, 처리해도 되는지를 결정, 통제할 수 있는 권리를 갖고 있다.

3. 個人情報보호에 관한 국제적 기준이나 국내적 기준이 구체적으로 그 내용이 약간씩 다르다 하더라도 본질적인 내용에서는 별 차이가 없음을 알 수 있다. 이러한 법률들 속에서 담겨 있는 일반적인 기준을 간단히 요약하면 다음과 같다 : 우선 個人情報를 조사, 처리, 저장하는 기관은 事前에 구체적으로 결정된 목적을 위해서만 이러한 個人情報를 처리해야 한다. 그리고 이러한 個人情報를 조사, 처리할 때는 해당 개인의 事前同意가 있거나 이에 관한 범위구체적인 法律上 根據가 있어야만 한다. 세 번째로 정보가 조사, 처리, 저장되는 해당 개인은 자신에 관한 정보에 접근하여 잘못된 정보를 수정하거나 삭제하는 등의 권리를 갖고 있어야만 한다. 네 번째로 個人情報를 처리하는 기관에게 정보의 무단유출 등에 관한 민형사처벌 규정 등이 있어야만 하고, 마지막으로 이러한 정보처리를 감독, 통제할 統制機關이 있어야만 한다.

4. 1980년대부터 우리 나라는 行政電算網을 포함하여 國家基幹電算網事業을 추진하였는 바, 이를 통하여 국가기관내에서 個人情報의 電算化가 확대됨으로써 잘못된 정보의 입력, 전산정보의 유출 등으로 인한 개인의 私生活侵害可能性이 증대하였다. 이에 따라서 마침내 1994년 1월 7일 '공공기관의개인정보보호에관한법률'이 제정되어 1995년 1월 8일부터 시행되었다. 이 個人情報保護法은 공공기관에서 컴퓨터로 처리하는 個人情報를 대상으로 한다. 이 법에 따르면 個人情報中 思想, 信條 등 개인의 基本的 人權을 침해할 우려가 있는 정보에 대해서는 수집을 제한하고 있다. 그리고 國家機關은 기관의 업무를 수행하기 위하여 필요한 범위내에서만 개인정보파일을 보유할 수 있도록 하였으며 個人情報의 부당한 유출, 변조나 부정확한 정보로 인한 개인의 私生活侵害를 예방하기 위하여 公共機關에 個人情報의 정확성과 안정성을 확보할 수 있는 대책을 수립하도록 하였다. 이 법에 따라 관련개인은 자신의 정보에 관하여 열람을 청구할 수 있으며 잘못된 정보에 대한 정정을 청

구할 있으며, 이러한 요구가 받아들여지지 않을 경우에 행정심판을 청구할 수 있다. 그런데 美國을 비롯한 대부분의 서유럽국가들은 1970년대부터 80년대중반사이에 "1세대" 個人情報保護法을 제정하였다. 그 뒤 서유럽국가들과 다른 많은 나라들은 급격하게 발전되는 정보통신기술에 발맞추어 1980년대후반부터 "2세대" 個人情報保護法律로 개정하고나 새롭게 제정하고 있다. 이에 반하여 우리 나라는 1980년대이후에 정력적으로 국가가 행정전산망사업 등 국가와 사회의 情報化에 주력하면서 개인의 私生活侵害가 우려된다는 비판이 강하게 제기되자 개인의 私生活을 보호하는 입법을 추진하였다. 이에 따라서 마침내 1994년 "공공기관의개인정보보호에 관한법률"이 제정, 공포되었다. 그런데 유감스럽게도 우리 나라의 個人情報保護法은 국제적으로 본다면 1990년대에 만들어진 가장 최근의 個人情報保護法임에도 불구하고 그 내용은 서유럽국가 등에서 수십년전에 만들어진 "1세대" 個人情報保護法에 가깝다는 것이었다. 게다가 국민의 낮은 個人情報保護意識, 個人情報保護를 위한 효율적인 통제방안의 결여, 국가기관을 통한 個人情報의 무차별적 저장과 처리 등을 통하여 우리 나라에서는 "個人情報保護法"은 있으되 정작 "個人情報"는 보호되지 못하고 있는 실정이다. 이에 따라서 과연 우리 나라의 個人情報保護法 자체가 이미 처음부터 문제점을 갖고 있기에 個人情報보호가 충분하게 확보되지 못하고 있는 것은 아닌가 하는 것을 법해석적, 입법론적으로 따져보아만 한다.

우선 個人情報를 보호하기 위하여 분명히 인식해야만 하는 전제조건은 우리 나라의 個人情報保護法은 다른 나라의 "1세대" 個人情報保護法처럼 개인관련정보의 남용으로부터만 시민을 보호하는 것이 아니라 그 남용 여부와는 상관없이 개인관련정보의 조사로부터 저장·사용·전달로부터 삭제될 때까지 보호해야만 한다는 것이다. 따라서 이는 個人情報保護法이 정보남용으로부터 개개인을 보호하는 것에만 제한되지 않음을 명백히 하면서 그 보호목적을 확대해야만 한다는 것을 뜻한다. 따라서 情報自己決定權은 個人情報를 恣意的으로 처리, 전달하는 것으로부터 뿐만이 아니라, 개인관련정보의 처리(회전)를 통한 위험으로부터도 보호되어야 한다. 그리고 個人情報들은 구체적이고 사전에 정당한 것으로 입증(언급)된 목적들을 위해서만 조사되어도 된다. 또한 個人情報의 처리가 自動的으로 행해지든, 아니든 상관없이 이러한 정보처리는 제한을 위한 法律上 根據命令을 만족시켜야 한다. 이는 개인관련정보의 처리를 통하여 그의 情報自己決定權이 제한되는 것으로부터 개인의 보호를 지향한다는 것을 뜻한다. 따라서 個人情報保護의 대상은 악의적인 잘못된 행위의 억제만이 아니라 이를 넘어서서 개인관련정보의 합법적 처리를 지향한다. 따라서 관련자의 情報自己決定權이 부당하게 제한되지 않는 경우에만 이러한 개인관련

정보의 처리는 허용된다.

그렇다면 우리 나라 個人情報保護法에서 개정되어야만 하는 내용을 간략하게 요약하면 다음과 같다.

1) 위에서 설명한 것처럼 個人情報를 보호하기 위해서는 우선 이에 관한 일반적인 원칙, 기준, 개인의 권리 등을 규정하는 일반적인 個人情報保護法이 필요하기는 하나 충분한 것은 아니다. 왜냐하면 이러한 法律은 개개 구체적인 분야에 적용하기에는 너무 추상적이고 일반적이기 때문이다. 따라서 개개 분야별로 특수하게 個人情報를 보호하는 특별한 個人情報保護法들이 제정되어야만 한다. 바로 이러한 특별법들이 일반적인 個人情報保護法에 규정된 원칙들을 개개 분야에서 구체화시키는 아주 중요한 역할을 한다. 결국 이러한 특별법을 통하여 일반적인 정보보호원칙들이 정확하게 구체화되며 특정 유형의 문제들에 적용되며 개인들이 구체적으로 보호를 받을 수 있게 된다.

2) 우리 나라 個人情報保護法은 個人情報를 보호하고자 한다고 규정하였고 個人情報를 "생존하는 개인에 관한 정보로서 당해정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보를 말한다"고 하였으며 다시 공공기관은 개인의 사상, 신조 등 개인의 기본적 인권을 현저하게 우려할 침해가 있는 個人情報를 수집하여서는 아니된다고 규정하고 있다. 이를 보면 우리 나라의 個人情報保護法이 나름대로 個人情報를 폭넓게 보호하려고 한다는 것을 알 수 있다. 다만 다음과 같이 개정한다면 더욱 더 바람직할 것이라고 보여진다 : 우선 위 법의 목적에서 個人情報의 보호를 통하여 "個人의 私生活"을 보호하고자 한다는 것을 구체화할 필요가 있을 것이다. 그리고 두 번째로 개인과 관련되는 그리고 개인을 식별할 수 있는 모든 정보를 個人情報라고 폭넓게 개념정의한 것은 바람직하지만 이러한 個人情報가 필요하지 않은 경우 삭제하거나 가능한 한 초기에 익명화하는 등의 보호조치에 관한 규정이 신설되어야만 한다. 마지막으로 모든 개인관련 정보가 보호된다면 그중에서 특히 민감한 정보는 처음부터 수집되어서는 안되도록 명시하거나 이를 통제해야만 한다. 특히 우리 나라와 같이 지역감정이나 사상시비가 문제가 될 수 있는 경우에는 민감한 정보의 조금 더 구체적인 재분류가 필요하며 이에 관하여 더 엄격한 보호조치가 뒤따라야만 한다. 특히 이러한 민감한 정보의 조사나 저장여부는 統制機關을 통하여 감독되어야만 하는 중요한 사항으로 외국에서는 다루어지고 있다. 특히 우리 나라 個人情報保護法에는 統制機關이 없기 때문에 바로 이러한 민감한 個人情報의 조사와 처리를 감독, 통제한다는 것이 매우

어려운 것이다. 따라서 특히 더 보호되어야만 하는 정보의 재분류 및 이에 관한 통제대책을 수립해야만 한다.

3) 우리 나라 個人情報保護法이 個人情報 및 개인의 私生活保護를 위하여 나름대로 위와 같은 많은 규정들을 두고 있지만 그래도 여전히 여러 문제점들을 갖고 있다. 우선 情報社會에서 국가를 통한 시민의 감시는 우선 情報調査와 蒐集을 전제로 한다. 그래서 情報社會에서 個人情報保護에 관한 출발점이 바로 情報調査라는 것을 인식해야만 한다. 따라서 관련자의 인식하에서 행해진 情報調査는 해당 개인에게 조사목적이라고 말한 것이 목적으로 결정적이고 설명의무가 있는 강제조사의 경우에는 관련자에게 조사목적근거로 언급된 법규정틀내에서 행해져야만 한다. 그래서 개인관련정보는 정보의 조사로부터 처리(저장, 변경, 전달, 삭제, 이용)를 거쳐 익명화될 때까지 보호되도록 개정되어야 한다. 그리고 우리 나라 個人情報保護法은 公共機關에서 자동정보처리로부터 個人情報를 보호하고자 하나 개인의 私生活을 효율적으로 보호하기 위해서는 자동화된 정보처리뿐만 아니라 서류들도 그 適用範圍에 포함시켜야야 한다. 따라서 공공기관의 경우에는 원칙적으로 個人情報의 보호가 또한 서류 속의 개인관련정보에까지 확대되도록 개정되어야 한다.

4) 個人情報保護에 관한 국제적, 국내적 기준에서 반드시 강조되는 원칙이 바로 規範明確性原則과 目的拘束原則이다. 規範明確性原則이란 관련자가 자기의 개인관련정보가 어떤 구체적인 처리목적들을 위하여 필요한지를 명확하게 인식할 수 있어야 한다는 것을 뜻한다. 따라서 法律의 規範明確性, 조직적이고 절차법적인 예방책들, 관할기관들의 설명, 관련자의 포괄적인 說明請求權 등을 통하여 누가, 언제, 어디에서 어떤 경우에 자기에 관하여 아는지를 관련 시민이 알 수 있도록 보장되어야 한다. 특히 관련자가 법규정으로부터 그의 개인관련정보가 어떤 구체적인 행정목적을 위하여 필요한지를 명백히 인식할 수 있어야만 한다. 또한 정보처리의 目的拘束은 한편으로는 처리목표를 확정하고 다른 한편으로는 처리범위를 한정한다. 처음부터 명확하게 개념 정의할 수 있는 목적을 위하여 필요한 최소한도의 정보처리만이 허용된다. 따라서 이미 法律上 決定된 目的을 위해서만 개인정보는 이용되어도 된다. 그리고 원래 목적과는 다른 정보이용 및 처리는 매우 제한된 범위 내에서만 인정되고 法律上 根據를 필요로 하는 새로운 基本權制限이다. 결국 이는 목적구속을 보장하기 위하여 국가기관간 정보전달과 이용에 관한 엄격한 대비책을 필요로 한다는 것을 뜻한다.

우리 나라 個人情報保護法 또한 나름대로 이러한 규범명확성원칙과 목적구속원칙

을 반영하고 있다. 우선 공공기관은 소관업무를 수행하기 위하여 필요한 범위안에서 개인정보화일을 보유할 수 있으며 보유기관의 장은 당해 개인정보화일의 보유목적이외의 목적으로 처리정보를 이용하거나 다른 기관에 제공하여서는 아니된다고 규정하고 있다.

그럼에도 불구하고 우리 나라 個人情報保護法이 많은 문제점을 갖고 있음은 다른 나라의 個人情報保護法과 비교하여 명백하게 드러난다. 우선 個人情報保護法의 적용을 배제하는 규정이 너무 많다. 예를 들어 國家安全保障을 목적으로 하여 수집되는 정보에 관하여 個人情報保護法의 적용을 배제하고 있다. 또한 개인정보화일을 보유하고자 하는 기관은 이를 반드시 총무처장관 등에게 사전통지해야만 한다고 규정하고 있으나 다시 제2항에서 그 적용배제사유를 광범위하게 규정하고 있을 뿐만 아니라 다시 제2항 7에서 적용이 배제되는 사항을 대통령령으로 정할 수 있도록 하였다. 그리고 처리정보의 이용 및 제한이나 처리정보의 열람제한 등에 관한 규정에서도 대통령령에 위임하고 있다. 결국 이렇게 지나친 위임 때문에 시민들은 도대체 본인의 어떤 정보에 관하여 어떤 국가기관이 처리, 저장하고 있는지를 파악하기가 매우 힘들다. 게다가 위 법의 적용이 배제됨으로써 발생할 수 있는 위험성에 관한 별도의 보호대책없이 국가안전보장 등 매우 막연한 사유를 근거로 한 위 법의 적용을 배제하는 것은 個人情報保護를 포기하는 것과 다름없다. 어떤 국가기관에게 위 법이 적용되며, 어떤 사유로 위 법의 적용이 배제되며 그러한 경우에 어떤 보호대책이 확립되어 있는지는 立法者 스스로가 반드시 法律에 규정하여야 하는 사항인데도 이에 관한 규정이 전혀 없거나 이를 행정부에 위임한다는 것은 규범명확성원칙에 반한다. 이에 따라서 규범명확성원칙에 근거하여 우리 나라 個人情報保護法의 개정이 매우 시급하다.

5) 자신에 관한 정보처리부터 개인의 私生活을 보호하고자 한다면 해당 개인에게 이러한 정보처리를 통제할 수 있는 가능성이 인정되어야만 한다. 따라서 우선 관련자의 설명청구를 통하여 자기정보가 어떻게 이용, 처리, 전달되고 있는지를 알 수 있어야만 한다. 그래야만 관련개인은 잘못된 정보처리에 대항할 수 있는 것이다. 우리 나라 個人情報保護法은 위에서 설명한 것처럼 개인에게 열람권과 정정권을 인정하기는 하나 이러한 권리들만으로는 個人情報를 보호하기에는 불충분하다. 우선 단순한 열람권만이 아니라 왜 자신에 관한 정보를 조사, 처리, 이용하였는지, 누구에게 어떻게 전달하였는지에 관하여 설명을 들을 권리가 관련개인에게 인정되어야만 한다. 그리고 잘못된 정보에 관하여 정정할 권리뿐만이 아니라 삭제권과 보충권이 인정되어야만 하며 해당 정보의 내용에 관하여 국가기관과 해당 개인간에 의견

차이가 있는 경우에 해당 개인의 진술이 이러한 기록에 첨부될 수 있는 기록도 인정되어야 한다. 그리고 個人情報를 처리하는 기관은 관련자를 위해서 뿐만 아니라 統制機關을 위해서도 어떤 방법으로든 이를 기록하여야 한다. 이러한 기록화는 관련자에게 정보처리의 필요한 투명성을 보장하는데 특히 이는 삭제청구와 손해배상 청구시 의미를 가질 수 있다. 물론 자신에 관한 情報에 해당 개인이 접근할 수 있는 권리나 설명을 요구할 수 있는 권리가 언제나 절대적으로 보호될 수는 없다. 우리 나라 個人情報保護法도 개인의 학교성적, 치료기록 등의 경우에는 열람을 제한할 수 있도록 규정하고 있다. 그러나 우리 나라 법에 의하면 국가안전보장과 관련되는 개인정보파일에는 個人情報保護法의 적용이 배제되며 또 여러 가지 다양한 사유로 개인의 접근권이 인정되지 않는다. 외국의 경우에도 자신의 정보에 접근할 권리를 인정하지 않는 예외사유를 인정하기는 하지만 이러한 경우에 개인의 권리보호를 위한 특별절차를 규정하거나 統制機關을 설치하였다. 그럼에도 불구하고 우리 나라 법에서는 개인의 설명권이나 접근권이 처음부터 불충분하게 보장되어 있을 뿐만 아니라 이러한 권리가 인정되지 않을 경우에 대비하는 규정이 전혀 없다. 물론 이러한 다툼이 法院을 통하여 해결될 수도 있지만 적어도 정보보호위원회나 統制機關이 이러한 분쟁을 조정하도록 규정하는 것이 바람직하다. 따라서 해당 개인의 권리는 일반적으로가 아니라 구체적이고 매우 한정되어 제한되어야 하며 개인의 설명권제한이 불가피하다면 이러한 제한이 統制機關을 통하여 감독되는 것이 요구된다.

6) 모든 國家機關은 그들이 갖고 있는 자료나 정보를 갖고서 그들의 과제를 처리하기에 충분하지 않다면 기관 상호간에 이러한 과제를 이행할 수 있도록 원조해야 한다. 문제는 이러한 국가기관 상호간 機關協助가 전자정보처리시대에서도 헌법합치적으로 존재할 수 있도록 하여야 한다는 것이다. 결국 정보처리시 요구되는 目的拘束은 한편으로 정보처리목적를 확정하고 다른 한편는 정보처리의 범위를 한정한다. 이에 따라서 필요한 최소한도로 事前에 명백하게 규정된 목적을 위한 정보처리만이 허용된다. 그렇다면 특정기관이 저장하고 있는 정보가 동시에 모든 다른 행정기관의 공통된 정보를 뜻하는 情報統一體란 존재해서는 안된다. 우리 나라 個人情報保護法이 규범명확성원칙에서 커다란 문제점을 갖고 있는 것처럼 바로 이 자동호출절차부분에서도 그에 못지 않은 문제점을 갖고 있다. 결국 우리 나라 個人情報保護法이 1990년대에 제정된 법임에도 불구하고 다른 나라의 "1세대" 法律과 비슷한 이유중 하나가 바로 이렇게 자동호출절차에 관한 보호규정이 전혀 없다는데에 있다. 이렇게 컴퓨터전산망을 통하여 행정기관들이 원하는 정보를 마음대로 처리, 이용할 경우에 우리 나라 個人情報保護法을 포함하여 정보보호법상 일반적 원칙중 하

나인 목적구속원칙과 규범명확성원칙을 준수한다는 것은 처음부터 불가능하다. 왜냐하면 결국 이러한 온라인연결을 통하여 어떤 개인이 한 行政機關에게 자신에 관한 정보를 제공하는 것은 모든 國家機關들에게 자신에 관한 정보를 제공하는 것과 동일하기 때문이다. 이렇게 되면 관련개인은 자신의 정보를 누가, 어떤 목적으로, 얼마만큼 처리, 이용, 전달하는지를 파악하고 통제한다는 것은 처음부터 불가능하다. 따라서 個人情報를 보호하기 위하여 가장 시급한 것이 바로 이렇게 컴퓨터의 연결을 통하여 자동적으로 정보를 조회, 처리하는 것을 통제하는 규정을 두어야 한다는 것이다. 이러한 자동호출절차로부터 個人情報를 얼마만큼 보호하느냐에 따라서 바로 個人情報保護法의 효율성여부를 판단할 수 있다고 해도 지나친 말이 아니다. 따라서 美國의 경우처럼 자동호출절차에 관한 특별법을 제정하든지, 독일처럼 個人情報保護法內에 이에 관한 규정을 신설하여야 한다. 특히 이러한 자동호출절차에 관한 규정에서는 호출절차의 사유와 목적, 정보수령인, 전달되는 정보의 종류 등에 관하여 해당 기관은 書面으로 이를 기록하고 이러한 기록을 정보보호위원회와 같은 統制機關이 감독할 수 있어야 한다는 내용이 포함되어야만 한다.

7) 우리 나라 個人情報保護法상 감독기관은 總務處이다. 아울러 국무총리소속하에 個人情報보호심의위원회를 설치하도록 하였으며 이 위원회는 個人情報保護에 관한 정책이나 제도의 개선에 관한 사항이나 個人情報의 이용과 제공에 관한 공공기관간 이견조정 등에 관한 사항을 심의하도록 하고 있다.

위에서 이미 설명한 것처럼 우리 나라 個人情報保護法은 많은 문제점을 갖고 있는데, 그중 가장 커다란 문제는 바로 統制機關의 缺如이다. 個人情報保護法의 목표는 새로운 정보통신기술의 적용을 위하여 효율적이고 헌법합치적인 조정규정과 보호규정들을 사전에 또는 동시에 준비하도록 하는 것이다. 그렇기 때문에 情報社會에서 국민의 私生活을 보호하기 위하여 個人情報保護法을 제정하는 것만으로는 충분하지 않다. 왜냐하면 오늘날 새로운 기술들의 발전 및 적용가능성이라는 관점에서 볼 때 法律家 또는 立法者는 그전보다 더 불리한 위치에 놓여 있고 더 이상 개인 스스로 이를 통제할 수 없기 때문이다. 따라서 個人情報保護法 制定 그 자체도 중요하지만 시민을 효율적으로 보호하기 위해서는 국가나 사회의 정보처리를 통제하는 統制機關의 설치 및 활동이 절대적으로 요구된다. 결국 公的 領域에서 이러한 통제기구를 설치하는 근본적인 임무는 國家의 지나친 情報調査와 처리로부터 시민들을 보호하는데에 있다. 이러한 통제장치가 없다면 국가기관에 의한 제한되지 않는 個人情報의 수집과 전달, 개인사생활의 지나친 감시를 방지한다는 것이 불가능하다. 그런 의미에서 본다면 우리 나라 個人情報保護法은 결국 統制機關을 통한 감

독없이 개개 國家機關에게 個人情報를 보호하도록 맡기고 있으며 이를 개개인이 자신에 관한 기록열람 등을 통하여 통제하는 아주 제한적이고 비효율적인 방식을 채택하고 있다. 결국 우리 나라 個人情報保護法의 가장 취약한 점은 바로 개개 국가기관이 제대로 個人情報를 보호하고자 하는지를 통제할 권한을 가진 기관이 전혀 없기 때문에 바로 오늘날 우리 나라에서 個人情報가 제대로 보호되지 못하고 있는 것이다. 표면상으로는 總務處가 이러한 임무를 담당하고 있는 것처럼 보이나 이는 美國의 사례를 보아도 실패할 수 밖에 없다. 왜냐하면 法院이 이러한 분야에서 효율적인 통제기관으로서 불충분하다는 것은 美國에서 그 동안의 경험을 통하여 입증되었기 때문이다. 게다가 통상적인 공무원에 의한 내부감독이란 너무 약하고 형식적인 통제가 되어버린다. 그나마 우리 나라에서는 國家의 정보조사나 처리가 통제되어서 시정된 사례가 전혀 보고되거나 기록되고 있지 않다. 그렇다면 우리 나라의 현행 個人情報保護法처럼 통제기관의 권한이나 지위, 조직에 관한 사항을 하위법규에 위임하는 것은 문제가 있다. 이러한 통제기관은 個人情報를 보호하기 위하여 매우 중요하므로 立法者가 직접 이에 관한 사항을 法律로 자세히 규정해야만 한다.

그렇다면 우리 나라에서도 개인의 私生活保護를 위한 경보시스템으로서 정보보호위원회와 같은 統制機關을 설치해야 한다. 이러한 통제기관은 우선 국가의 정보처리를 지속적으로 감독하고 法律에 규정된 목표를 준수하는지를 검토하여야 한다. 그리고 이들은 구체적인 국가정보시스템들의 작용을 규율하고 정보통신기술의 새로운 적용을 감독, 평가해야만 한다. 특히 統制機關은 모든 정부기관을 감독하여야 하며 특히 경찰과 첩보기관을 효율적으로 감독할 수 있는 방안을 강구하여야 한다. 결국 이러한 임무를 수행하기 위해서는 立法府, 司法府, 行政府에 속하는 국가기관이 아닌 統制機關을 만들어야 하는 것이다. 왜냐하면 이러한 통제기관은 충돌하는 여러 이해관계들을 형량하여야 하기 때문이다. 그러나 이러한 통제기관은 그들의 활동과 정책을 국가와 사회의 情報調査와 處理를 통제하는 것에 집중하여야 한다. 곧 통제기관은 개인의 정보보호를 우선적으로 목표로 하여 情報社會에서 개인의 여러 권리들을 보장하고 강화하도록 노력하여야 한다. 위에서 이미 설명된 것처럼 스웨덴과 프랑스의 통제모델 - 허가시스템 - 은 문제가 있는 통제모델이다. 왜냐하면 이러한 통제방식은 통제기관에 너무 많은 부담을 지우기 때문에 통제기관의 작업방식이 결국에는 너무 관료적, 형식적인 것처럼 되어 버리기 때문이다. 그래서 모든 것을 통제한다는 것은 불가능하게 되고 그러다보니 나중에는 정작 중요한 과제들마저도 제대로 수행하지 못하게 되는 결과를 낳는다. 따라서 우선 公的 領域에서 개인정보시스템의 작동에 관하여 諮問權限을 갖는 독일이나 캐나다의 정보보호위원회

시스템이 더 효율적이다. 이러한 자문(상담)시스템은 통제기관의 허가를 행정부가 저항하거나 무시할 수 있는 위험성을 극복할 수 있는 장점을 갖고 있으며 자문(상담)권한을 갖는 統制機關 또한 유연하며 실용적인 방법으로 행동할 수 있다.

그 다음으로 統制機關은 부당한 감시를 받고 있다고 느끼는 시민들의 권리를 보호하기 위하여 노력하는 것이 이러한 위원회의 또 다른 중요기능에 속한다. 이를 넘어서서 통제기관은 다양한 방법을 통하여 국가의 정보처리과정에서 個人情報가 보호될 수 있도록 일반적이고 체계적인 감독과 대안제시를 위하여 노력하여야 한다. 이러한 국가정보처리의 감독행위가 바로 통제기관에게 새롭게 부과되는 중요한 임무이다. 이를 통하여 새로운 정보통신기술의 도입이 개인의 자율을 희생시키면서 더욱 더 정교하고 통합된 개인정보시스템을 만들 위험성을 막아야 한다. 따라서 個人情報保護委員會는 새로운 정보기술형태의 잠재적 영향력과 효과를 판단하여서 이러한 정보통신기술의 적용이 계획단계에서부터 個人情報保護와 조화될 수 있도록 노력하여야 한다. 이에 따라서 情報保護委員會에 상담과 조정기능외에 위험예방기능이 요구된다. 그리고 統制機關은 個人情報處理와 관계되는 중요사항에 대하여 매년 의회에 年例報告書를 제출하고 個人情報保護와 관련되는 事案에 대하여 여론매체 등을 이용하여 널리 알리고 시민에게 홍보하여야 한다. 마지막으로 컴퓨터연결을 통한 個人情報의 결합을 통제하는 것이 현재 個人情報보호의 중심문제로서 바로 정보보호위원회가 해결하려고 노력해야 하는 분야이기도 하다. 이러한 많은 일들을 하기 위하여 한 사람의 통제관을 두든, 정보보호위원회를 만들든간에 이러한 統制機關은 직접 議會가 선출하여야 하고 그 신분은 法官에 준할만큼 獨立性이 보장되고 豫算도 직접 편성할 수 있어야 한다.

參考文獻

〈國內文獻〉

金南辰, 情報化社會에서의 法治行政體系의 法制度的 再構成 : 國家社會의 情報化와 公法體系의 再構成, 53~69, 전기통신학술연구과제, 1990.

_____, 行政調査와 個人情報保護 : 情報의 蒐集 管理와 私生活保護, 165~178, 전기통신학술연구과제, 1989.

김석준/강경근/홍준형, 열린 사회 열린 정보 : 비봉출판사, 1993.

金善旭, 西獨에 있어서의 情報公開와 私生活保護 : 未來情報化社會의 公法的 對應, 49~66, 1989.

金哲洙, 情報公開法과 私生活秘密保護法 序說 : 情報의 蒐集 管理와 私生活保護, 13~71, 전기통신학술연구과제, 1989.

김홍근, 선진국의 정보보호전담기관현황 : 정보화로 가는 길, 1997,10.

文光三, 情報主權體系의 法理論的 構成 : 國家社會의 情報化와 公法體系의 再構成, 27~51, 전기통신학술연구과제, 1990.

박영도외, 情報化社會의 展開와 立法的 對應 : 한국법제연구원, 1992.

法制處, 各國의 個人情報保護關係法 : 法制資料 第150輯, 1989.

卞在玉, 立法紹介 : 1988年의 컴퓨터連結 및 프라이버시保護法 : 美國憲法硏究 第1號, 33~58, 1990.

_____, 美國에서의 私生活保護法制 : 情報의 蒐集 管理와 私生活保護, 72~114, 전기통신학술연구과제, 1989.

成樂寅, 프랑스에서의 私生活保護法制 : 情報의 蒐集 管理와 私生活保護, 115~164, 전기통신학술연구과제, 1989.

_____, 自動化社會와 프라이버시保護 : 법제연구 1996, 8-36.

안문석, 정보체계론 : 학현사, 1995.

이상돈, 형사절차와 정보보호 : 한국형사정책연구원, 1996

임재홍, 개인정보보호법과 개인정보보호조례 : 민주법학 9호, 1995.

전석호, 정보사회론 : 나남, 1993.

千炳泰, 國際間情報流通에 따른 프라이버시 保護 : 情報의 蒐集 管理와 私生活保護, 199~220, 전기통신학술연구과제, 1989.

한국언론연구원, 세계언론법(상) : 1995.

한국전산원, 1997 국가정보화백서.

黃祐呂, 美國에 있어서의 情報公開法과 私生活保護法 : 未來情報化社會의 公法的 對應, 27~48, 1989.

Davis, Stan/Davidson, Bill - 2020 Vision : Simon & Schuster, 1991 (한성호/하헌식역(譯) - 경제이동 : 지식공작소, 1993.

Toffler, Alvin - Powershift : Bantam, 1990(이규행(李揆行) 감역(監譯), 권력이동 : 韓國經濟新聞社, 1990).

〈外國文獻〉

Aulehner, Josef. 10 Jahre "Volkszählungs"-Urteil : CR, 1993, 446~ 455.

Baumann, Reinhold. Stellungnahme zu den Auswirkungen des Urteils des Bundesverfassungsgerichts vom 15.12. 1983 zum Volkszählungsgesetz 1983 : DBVl, 1984 , 612~619.

Bäumler, Helmut. Normenklarheit als Instrument der Transparenz : JR, 1984, 361~366.

Bethge, Herbert. Grundrechtsverwirklichung und Grundrechtssiche rung durch Organisation und Verfahren : NJW, 1982, 1~7.

Bizer, Johann.Forschungsfreiheit und Informationelle Selbstbestimmung : Nomos, 1992.

Brossette, Josef. Der Wert der Wahrheit im Schatten des Rechts auf informationelle Selbstbestimmung : Duncker & Humblot,. 1991.

Büllesbach, Alfred. Das neue Bundesdatenschutzgesetz : NJW 1991, 2593~2600.

Busch, Jost-Dietrich. Anmerkung zu BVerfG : DVBl, 1984, 384~389.

Dammann, Ulrich.Das neue Bundesdatenschutzgesetz : NVwZ, 1991, 640~643.

Däubler, Wolfgang. Individualrechte des Arbeitsnehmers nach dem neuen BDSG : CR, 1991, 475~482.

Delbrück, Jost. Die kulturelle und individuelle Identität als Grenzen des Informationspluralismus? : Wolfrum,Rüdiger(Hrsg.), Recht auf Information Schutz vor Information, 181~200, Duncker & Humblot, 1986.

Eberle, Carl-Eugen. Die öffentliche Verwaltung vor den Herausforderungen der Informationsgesellschaft : Die Verwaltung, 1987, Bd. 20, 459~476.

Egloff, Willi. Information und Grundrechte : DVR, 1978, 115~140.

Ehmann, Horst. Zur Zweckbindung privater Datennutzung : RDV, 1988, 169~180, 221~247.

Einwag, Alfred. Die neuen Bundesländer und das neue Bundesdatenschutzgesetz : RDV, 1992, 1~8.

Gallwas, Hans-Ulrich. Verfassungsrechtliche Grundlagen des Datenschutzes : Der Staat, 1979, 507~520.

_____, Zum Prinzip der Erforderlichkeit im Datenschutzrecht : Festschrift für Arthur Kaufmann zum 70. Geburtstag, 819 ~ 829, C. F. Müller, 1993.

Geiger, Andreas. Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung : NVwZ 1989 , 35~38.

Geis, Max-Emanuel. Der Kernbereich des Persönlichkeitsrechts : JZ 1991, 112~117.

Groß , Gerhard. Das Recht auf informationelle Selbstbestimmung mit Blick auf die Volkszählung 1987, das neue Bundesstatistikgesetz und die Amtshilfe : AÖR, 1988, 162~213.

Flaherty, David H. Protecting Privacy in Surveillance Societies : The University of North Carolina Press, 1989.

Heußner, Hermann. Datenverarbeitung und Grundrechtsschutz : Hohmann, Harald(Hrsg.), Freiheitssichrung durch Datenschutz, 110~126, Suhrkamp, 1987.

_____, Zur Funktion des Datenschutzes und zur Notwendigkeit bereichsspezifischer Regelungen : Wolfgang Gitter (Hrsg.), Festschrift für Georg Wannagat zum 65. Geburtstag, 173~200, Carl Heymanns Verlag, 1981.

Hoffmann , Bernhard. Zweckbindung als Kernpunkt eines prozeduralen Datenschutzansatzes : Nomos Verlag, 1991.

Hohmann , Harald. Freiheitssicherung durch Datenschutz : Suhrkamp,

1987.

Huber, Peter M. Der datenschutzrechtliche Auskunftsanspruch : ThürVBl, 1992, 121~133.

Isensee, Josef. Widerstand gegen den technischen Fortschritt : DÖV, 1983, 565~575.

Kloepfer, Michael. Datenschutz als Grundrecht : Athenäum, 1980.

Kopp , Ferdinand - Das EG-Richtlinienvorhaben zum Datenschutz : RDV, 1993, 1~10.

Krause , Peter. Das Recht auf informationelle Selbstbestimmung - BVerfGE 65,1 : JuS, 1984, 268~275.

Kunig, Philip. Der Grundsatz informationeller Selbstbestimmung : Jura, 1993, 595~604.

_____, Das Rechtsstaatsprinzip : J.C.B. Mohr, 1986.

Langer, Margit. Informationsfreiheit als Grenze informationeller Selbstbestimmung : Duncker & Humblot, 1992.

Linnenkohl, Karl. Arbeitsnehmerdatenschutz und BAG-Rechtsprechung : RDV, 1990, 61~68.

Mallmann, Otto. Zweigeteilter Datenschutz? Auswirkungen desVolkszählungsurteils auf die Privatwirtschaft : CR, 1988, 93~98.

_____, Volkszählung und Grundgesetz : JZ, 1983, 651~659.

Massing, Otwin. Von der Volkszählungsbewegung zur Verrechtlichung oder : Öffentlichkeit, Herrschaftsrationalisierung und Verfahren : Hohmann, Harald(Hrsg.), Freiheitssichrung durch Datenschutz, 85~109, Suhrkamp, 1987.

Michael, James. Privacy and Human Rights : Dartmouth, 1994.

Murswiek, Dietrich. Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht : VVDStRL 48, 208~234, 1990.

Müller, Gerhard F./Wächter, Michael. Der Datenschutzbeauftragte(2. Auflage) : C.H. Beck, 1991.

von Münch, Ingo(Hrsg.). Grundgesetz - Kommentar Bd. 1 (4. Auflage) : C.H. Beck, 1992.

Perrit Jr., Henry H. Law and the Information Superhighway : Wiley Law Publications, 1996.

Podlech , Adalbert. Individualdatenschutz - Systemdatenschutz : Brückner, Klaus/Dalichau,Gerhard(Hrsg.), Beiträge zum Sozialrecht : Festgabe für Hans Grüner, 451~462, Verlag R. S. Schulz, 1982.

_____, Das Recht auf Privatheit : Joachim Perels(Hrsg.), Grundrechte als Fundament der Demokratie, 50~68, Suhrkamp, 1979.

Rauschning, Dietrich-Der Zugang zu dem internationalen Informationsverteilungssytem als Forderung des Völkerrechts? : Wolfrum, Rüdiger(Hrsg.), Recht auf Information Schutz vor Information, 129~147, Duncker & Humblot, 1986.

Rosenbaum, Christian. Der grundrechtliche Schutz vor Informationseingriffen : Jura, 1988, 178~184.

Roßnagel, Alexander/Wedde, Peter/Hammer, Volker/Pordesch, Ulrich. Digitalisierung der Grundrechte? : Westdeutscher Verlag, 1990.

Schlink, Bernhard. Datenschutz und Amtshilfe : NVwZ, 1986, 249~256.

_____, Das Recht der Informationellen Selbstbestimmung : Der Staat, 1986, Bd. 25, 233~250.

_____, Die Bewältigung der wissenschaftlichen und technischen Entwicklungen durch das Verwaltungsrecht : VVDStRL 48, 236~264, 1990.

Scholz, Rupert. Technik und Recht : Dieter Wilke (Hrsg.), Festschrift zur 125 jährigen Bestehen der Juristischen Gesellschaft zu Berlin, 691~714, Walter de Gruyter, 1984.

_____/Pitschas, Rainer. Informationelle Selbstbestimmung und staatliche Informationsverantwortung : Duncker & Humblot, 1984.

Schreiber, Manfred. Europäische Einigung und Innere Sicherheit : Peter Badura, Rupert Scholz (Hrsg.), Festschrift für Peter Lerche zum 65. Geburtstag, 529~543, 1993, C.H. Beck.

Schwan, Eggert. Datenschutz , Vorbehalt des Gesetzes und Freiheitsgrundrechte : Verwaltungsarchiv, Bd. 66, 120~150, 1975.

Stelkens, Paul / Bonk , H. J. / Sachs , Michael. Verwaltungsverfahrensgesetz : C.H. Beck, 1993.

Simitis, Spiros. Von der Amtshilfe zur Informationshilfe : NJW 1986, 2795~2805.

_____, Zur Aufnahme der informationelle Selbstbestimmung in das Grundgesetz : KritV, 1993, 46~52.

_____, Informationelle Selbstbestimmung und Informationsfreiheit als Verfas-sungsprinzipien : Kreuder, Thomas(Hrsg.), Der orientierungslose Leviathan, 141~151, Schüren, 1992.

_____, Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung : NJW, 1984, 398~405.

Steinbuch, Karl. Der Mensch - Objekt oder Subjekt der Informationsverarbeitung? : RDV, 1988, 1~7.

Steinmüller,Wilhelm. Die Zweite industrielle Revolution. Techmische und sozialökonomische Bedingungen der Informationstechnologiepolitik : DVR, 1981, 37~70.

Stoltenberg, Klaus. Die historische Entscheidung für die öffnung der Stasi-Akten- Anmerkungen zum Stasi-Unterlagen-Gesetz : DtZ, 1992, 65~72.

Störmer, Rainer. Zur Verwertbarkeit tagebuchartiger Aufzeichnungen : Jura, 1991, 17~24.

Tinnefeld, Marie. Theres-Der Datenschutz in den Vereinigten Staaten - Die gegenwärtige Situation : RDV, 1992, 216~221.

_____/Ehmann, Eugen. Einführung in das Datenschutzrecht : Oldenbourg, 1992.

Vogelgesang, Klaus. Grundrecht auf informationelle Selbstbestimmung? : Nomos Verlag, 1987.

Wacks, Raymond. Personal Information, Clarendon Press, 1989.

Walz, Stefan. Das neue Bundesdatenschutzgesetz : CR, 1991, 364~369.

Weichert,Thilo. Neue Verfassungsregelungen zur informationellen Selbstbestimmung : CR, 1992, 738~745.

Wellbrock, Rita. Genomanalysen und das informationelle Selbstbestimmungsrecht : CR, 1989, 204~210.

Wente, Jürgen. Informationelles Selbstbestimmungsrecht und absolute

Drittwirkung der Grundrechte : NJW, 1984, 1446~1447.

Wohlgemuth , Hans H. Neuere Entwicklungen im Arbeitnehmerdatenschutz : BB, 1992, 281~285.

Wolfrum, Rüdiger. Recht auf Information Schutz vor Information : Duncker & Humblot, 1986.

Wyduckel, Dieter.Archivgesetzgebung im Spannungsfeld von informationeller Selbstbestimmung und Forschungsfreiheit : DVBl, 1989, 327~337.

Ziegler, Otto. Statistikgeheimnis und Datenschutz : VVF, 1990.

Zöllner, Wolfgang. Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung : RDV, 1985, 3~16.

_____. Datenschutz in einer freiheitlichen marktwirtschaftlichen Ordnung : RDV, 1991, 1~11.

_____. Informationsordnung und Recht : Walter de Gruyter, 1990.

연구보고 97-5
個人情報保護法制의 整備方案에 관한 연구

1997년 12월 25일 印刷
1997년 12월 30일 發行

發行人 朴 松 圭
發行處 한국법제연구원
印刷處 東 洋 商 社

서울특별시 종로구 신문로 2가 1-103
전화:(02)722-2901, FAX:(02)722-2900
등록번호 : 1981. 8.11. 제1-190호

값 8,000 원

ISBN 89-8323-039-8 93360