法 學 碩 士 學 位 論 文

電子去來와 個人情報保護에 관한 硏究

2009年 8月

釜 慶 大 學 校 大 學 院

法 學 科

權 聖 弼

法 學 碩 士 學 位 論 文

電子去來와 個人情報保護에 관한 硏究

指導敎授 崔 明 龜

이 論文을 碩士 學位 論文으로 提出함

2009年 8月

釜 慶 大 學 校 大 學 院

法 學 科

權 聖 弼

權聖弼의 法學碩士 學位論文을 認准함

2009年 8月 日

主 審 法學博士 高 明 植 印

委 員 法學博士 金 斗 鎭 印

委 員 法學博士 崔 明 龜 印

목 차

제1장 서 론

제2장 전자거래 일반론

제3장 개인정보보호에 관한 국내·외 동향

제4장 전자거래에서의 개인정보 침해 및 구제

표 목 차

Abstract

A Study on the Electronic Transaction and the Protection of Personal Information Data

Kwon, Seong Pil

Department of Law, The Graduate School,

Pukyong National University

The purpose of this writing is to review the issue of protecting the personal information data in the electronic transaction field.

Rapid development of modern science and technology has brought many changes, which we haven't expected, to politics, economy, society, culture and so on. Especially the development of worldwide network through the Internet in the area of information and communication technology has been as innovative as the other areas. It has affected the lives of people in great quantity. The advancement of the Internet has rapidly developed in the electronic transaction field.

As the electronic transaction field is developed, the issues of protecting personal data have newly appeared. The issues include preventing

online fraud and deceit and protecting personal information data that is collected in the course of electronic transaction. Individual person hesitates to use electronic transaction, as his personal information data and trade information could be secretly collected and used in the process of electronic transaction infringing their private lives.

As long as electronic transaction is developed and advanced rapidly, it could infringe private information more frequently. So the importance of protection individual information will be more strongly argued afterward.

keywords: electronic transaction, personal information data, modern science, modern technology

제1장 서 론

제1절 연구의 목적

현대사회를 정보화 사회라고 한다. 정보화 사회라 함은 정보가치의 생산을 중심으로 경제·사회구조가 변화·발전되어 가는 사회를 말한다. 정보화 사회가 발전함으로써 정보가 주요 자원이 되면 개인에 관한 정보까지도 당연히 수집·정리·보관 및 전파의 대상이 된다.

이러한 과정에서 개인이 공개를 꺼리는 자기만의 사적 영역의 정보도 부득이 타인에 의하여 수집·관리되는 경우가 있게 마련인 바, 이에 따라 기본권 보호를 위하여 등장한 것이 바로 프라이버시권(또는 개인정보보호권)이다. 이러한 프라이버시권은 일반적으로 사생활을 함부로 공개당하지 아니하고 사생활의 평온과 비밀을 요구할 수 있는 권리(홀로 남을 권리, 소극적 개념의 프라이버시권)와 함께 자신에 관한 정보를 관리·통제할 수 있는 권리까지를 의미(정보주체의 자기결정권)하는 넓은 개념이다.

이렇듯 프라이버시권 또는 개인정보보호권은 현대사회에 있어서 더욱 중요하게 그 보호가치를 인정받고 있다. 특히나 정보화 사회의 발달로 인한 전자거래의 비약적인 성장은 개인의 프라이버시권에 대한 침해를 야기하게 되었고, 이에 대한 대책 마련이 시급한 사회 문제 대두되었다. 2008년 초 발생한 대형 온라인 쇼핑몰의 해킹 사건[1]은 전자거래에 있어서 개인정보보호가 얼마나 중요한 문제이며, 시급히 해결해야할 문제인가를 보여준 한 예라 하겠다.

---

1) http://www.ytn.co.kr/_ln/0102_200802051535087083 참조.

이처럼 대량거래가 가능한 전자거래는 그 피해범위가 광범위하다는 점에서 기존의 거래에서의 피해양상과는 다른 측면을 가지며, 그에 대한 피해예방 및 구제가 중요한 사회문제로 부각되는 것이다. 이에 따른 해결방안으로 전자거래에 있어 대체적 신분확인제도(i-PIN : Internet Personal Identification Number) 등이 논의되고 있으나, 개인정보의 범위가 과연 신분확인에 그치는지, 어떤 제도적 도입이 개인정보보호에 실효성이 있는지 등에 대해서는 여러 가지로 의견이 나뉘고 있다.

따라서 이와 같은 현실상황을 고려해볼 때, 전자거래에 있어서 개인정보보호에 관한 논의는 결코 적지 않은 중요성과 의미를 가진다고 할 것이다.

제2절 연구의 범위와 방법

이하에서는 전자거래 분야에 있어서 개인정보보호와 관련한 논의를 설명하기 위한 방법으로 전자거래에 관한 일반론을 언급한 후, 개인정보보호제도와 관련한 국내·외 동향을 살펴보고, 마지막으로 전자거래 분야에서 개인정보 침해유형과 그에 따른 구제제도 및 우리나라에 있어서 전자거래 개인정보 침해구제제도의 개선점을 알아보기로 한다.

제1장에서는 본 연구의 필요성에 대해서 언급하고, 본 연구의 범위와 방법에 대한 안내를 한다.

제2장에서는 전자거래와 관련하여 전자거래의 인접 개념들을 살펴본

후, 이를 통해서 전자거래의 정의를 도출해 낸다. 그리고 이를 바탕으로 현재 국제기구 및 주요국가에서 정의하고 있는 전자거래의 의미를 알아본다. 아울러 일반적으로 논의되고 있는 전자거래의 특성 및 유형에 대해서 간략히 소개하기로 한다.

제3장에서는 개인정보의 연혁적 발전 과정 및 그 정의에 대해서 알아본 후, 개인정보보호의 필요성에 대해서 살펴본다. 그리고 개인정보보호제도에 관한 일반적인 논의를 한 후, 이를 바탕으로 개인정보보호와 관련한 우리나라의 법제도와 일반적인 국제적 동향을 소개하기로 한다.

제4장에서는 제3장에서의 논의를 더욱 깊게 하여, 전자거래 분야에서의 개인정보침해 유형을 살펴본 후, 그 구제방법에 관하여 알아보기로 한다. 그리고 마지막으로 이러한 논의를 전제로, 우리나라 전자거래 분야에 있어서 개인정보보호와 관련한 현실적인 문제점을 제시하고, 이에 대한 개선방안을 모색하기로 한다.

마지막으로 제5장에서는 앞서의 논의를 정리하고 전자거래와 개인정보보호에 관한 본 연구를 마무리하도록 한다.

제2장 전자거래 일반론

제1절 전자거래의 의의

Ⅰ. 전자거래 인접 개념들

일반적으로 '전자거래'라는 용어가 본격적으로 사용되기 이전에 '전자상거래'라는 용어가 먼저 사용되기 시작하였다. 전자상거래라는 용어가 사용되기 시작한 것은 인터넷이 전문가들은 물론 일반인에 의해서도 본격적으로 이용되기 시작하던 무렵인 1980년대부터이다. 그리고 이러한 전자상거래라는 용어의 등장 이전에는 '광속거래(CALS)', '전자문서교환(EDI)' 등과 같은 개념들이 전자적 의사전달 수단을 이용한 거래 분야에서 널리 쓰이고 있었다. 따라서 전자거래의 개념을 정확히 이해하기 위해서는 이러한 개념들의 연혁적인 측면을 우선적으로 검토하는 것이 필요하다.[2)]

1. 전자상거래 (EC : Electronic Commerce)

전자상거래에 관하여는 종래 법학, 경영학, 경제학, 전자공학 등 관련 분야마다 제각기 나름대로의 개념 정의를 시도하여 왔는데, 그 분야에 따라 각기 약간씩의 차이를 보이고 있다. 이는 전자상거래가 현실에서 어떠한 기능을 담당하고 있는 것인가에 따른 것으로 각각의 분야마다 강조하는 관점을 달리하기 때문이다.

예컨대, 전자상거래에 관하여는 "재화와 용역의 매매 뿐만 아니라, 이

2) 사법연수원, 「전자거래법」, 사법연수원편집부, 2006, 13면 이하.

에 더하여 그 재화와 용역의 수요를 창출하거나 판매지원 및 고객에 대한 서비스를 제안하고 거래당사자간의 의사소통을 원활히 하기 위한 것과 같은 부수적인 행위를 포함한 하나의 체계", "재화와 용역의 품질을 향상시키고, 그 전달과정의 속도를 향상시킴으로써 기업과 상인 그리고 소비자로 하여금 비용을 절감하고자 하는 욕구를 충족시켜주는 현대 비즈니스의 방법론", "전자문서교환, 전자우편 등과 같이 전자적, 과학적 또는 이와 유사한 방법에 의하여 생성, 저장되거나 소통되는 정보의 교환을 통하여 이루어지는 상거래 행위", "전자적 방식을 이용하여 전자공간 상에서 이루어지는 상거래 및 이에 필요한 제반정보를 교환하는 방식", "상업적인 거래의 당사자 간에 정보기술을 활용하여 거래를 보다 효율적이며 효과적으로 수행하기 위한 제반행동"이라는 다양한 정의가 논의되고 있다.[3)]

결국 위와 같은 정의들 대부분이 포함하고 있는 공통점만을 뽑아보면, '전자적인 수단을 통한', '상거래'라는 점에 일치하는 것을 발견할 수 있다. 따라서 법률적 의미에 있어서의 전자상거래를 "인터넷과 같은 개방형 시스템 하에서 컴퓨터 등 연산 작용에 의한 정보처리장치를 통하여 이루어지는 상거래 또는 상행위"라고 정의하여도 무방하다할 것이다.

다만 전자상거래라는 용어는 Electronic Commerce라는 영어의 번역으로서 초기부터 사용되어 온 바 있으나, 최근 들어서는 '상거래'라는 용어 자체가 마치 상법상의 상행위에 한정된 것으로 오인될 여지가 있고, 그 규율대상으로 상사적인 범주뿐만 아니라 인터넷을 이용한 일반 사인간의 거래관계를 당연히 포함할 수 있어야 한다는 논의에 따라 적어도 법률 분야에 있어서만큼은 이를 '전자거래'라는 용어로 대체함이 타당하다는 쪽으

3) 사법연수원, 전게서, 14면 이하.

로 의견의 일치를 보고 있다.[4)5)]

2. 광속거래 (CALS : Commerce At Light Speed)

광속거래(CALS)는 처음에는 1985년경 미국에서 군수지원의 컴퓨터화(Computer Aided Logistics Support)라는 개념으로서 군업무 수행을 위하여 시작되었다. 이 후 1988년경 군과 방위사업체간에 정보를 공유하고 무기를 비롯한 각종 군수 물자의 조달을 위한 무기 체계의 획득 및 군수지원의 컴퓨터화(Computer-aided Aquisition and Logistics Support)라는 개념을 거쳐, 1994년경에는 군업무 수행을 위한 애초의 목적에서 벗어나 일반 기업체 내·외의 정보공유 및 제조업 분야의 산업 정보화에 이어 모든 산업분야에 적용되는 물류 생산·조달·운영지원의 전자화(Continuous Acquisition and Life-cycle Support)의 개념으로 발전하였다. 그리고 1995년경 그 최종단계로서 광속거래(Commerce At Light Speed)라는 개념에 이르게 되었다.

이처럼 광속거래는 "정보의 공유화 등에 의해 경영효율을 증진시키는 세계 공통의 새로운 비즈니스 시스템으로서, 표준화 및 정보통합화 기술을 이용하여 원재료의 조달에서 설계·개발·생산·조달·관리·유통·유지라는 제품의 전 라이프사이클(life-cycle)에 관한 정보를 전자화한 통합

---

4) 「전자거래기본법」이 제정된 우리나라에서는 상거래를 포함하는 일반적인 개념으로서 '전자거래'라는 용어를 사용하는 것이 타당하다. 최근 미국에서도 National Conference of Commissioners on Uniform State Laws(NCCUSL)와 American Law Institute(ALI)에서 제안한 Uniform Electronic Transaction Act(UETA)의 1999년 4월 초안에서 Electronic Transaction이라는 표현을 사용하고 있다. (사법연수원, 전게서, 15면 이하 참조.)

5) 이와 같은 의견 일치는 우리나라 「전자상거래등에서의소비자보호에관한법률」(법률 제8635호)에서 잘 나타나고 있다. 동법 제2조 제1항은 다음과 같이 규정을 하고 있다. "전자상거래라 함은 전자거래(전자거래기본법 제2조 제5호의 규정에 의한 전자거래를 말한다. 이하 같다)의 방법으로 상행위를 하는 것을 말한다."

정보시스템으로의 전략적 접근"[6]이라는 매우 방대한 부문에 걸친 개념으로 발전하였다. 이러한 광속거래가 도입됨으로써 종이 없는 업무환경을 구축하고 이에 기하여 신속한 정보서비스를 제공하며, 그에 따라 생산 제품의 품질향상, 인력 및 비용절감을 달성하고, 나아가 경영환경에 대한 각종 변화에 대하여 유연한 대처가 가능하게 되었다.

이와 같은 광속거래는 어떠한 고정된 개념으로 설명할 수 있기보다는 산업시스템에 있어서 관련 데이터베이스를 근간으로 한 과정(process), 방법(method) 또는 전략(strategy)으로서의 성격이 강하며, 'CALS 운용', 'CALS에 이용되는 정보기술', '도구·기술 관리'의 3가지 영역에 관한 정보시스템의 구축을 기본적 요소로 하고 있다.

이러한 점에 비추어 볼 때, 광속거래와 전자거래는 기본적으로 컴퓨터 등을 그 수단으로 사용한다는 점에서 공통점이 있으나, 전자거래는 소비자거래와 같이 CALS가 포괄하지 못하고 있는 분야를 포함하는 더욱 광범위한 개념임을 알 수 있다. 그리고 전자거래와 광속거래는 개념적으로 상호 포섭 관계에 있다고 하기보다 각기 스스로의 고유 영역을 가진 채 컴퓨터 등을 수단으로 한다는 점에서 공통점을 갖는 관계라 할 것이다.

3. 전자문서교환 (EDI : Electronic Data Interchange)

전자문서교환은 "컴퓨터를 통하여 표준화된 전자문서를 교환하는 방식"을 말한다.[7] 즉 한 컴퓨터에서 다른 컴퓨터로 EDI 네트워크를 통하여 표준화된 양식의 데이터를 전송하여 직접 업무에 활용할 수 있도록 하는

---

6) 최경진, 「전자상거래와 법」, 현실과 미래, 1998, 7면 이하.
7) 정쾌영, 「전자거래법」, 무역경영사, 2001, 33면 이하.

새로운 정보전달체계를 일컫는 것이다.[8)]

전자문서교환은 미국 운송업계의 운송문서조정위원회(TDCC)가 1975년에 최초로 그 표준을 마련한 이후 다른 업종에서도 EDI 표준을 개발, 그 사용이 점차 확산되었으며, 미국은 국가차원의 EDI 표준을 마련하기 위하여 1978년 X.12위원회를 설립하였으며, 이 위원회는 1981년 최초의 EDI 표준을 제정하여 발표하였다. 국제적으로는 1979년 이후 UN산하 유럽경제위원회와 국제거래법위원회가 각국에 대해 국제무역에 있어서 EDI를 이용할 수 있도록 법률을 개정할 것을 권고하였으며, 국제상업회의소(ICC)는 1990년 Incoterms를 개정, EDI를 정규의 해상운송서류로 취급하고 선하증권과 동일한 효력을 인정하였다.

이처럼 전자문서교환은 종이문서의 전자화라는 점에서 일정한 법률효과를 원하는 의사표시를 요소로 하는 전자거래와 구분된다. 또한 전자문서교환은 포맷으로 코드화된 표준양식을 이용한다는 점에서 반드시 표준화된 양식을 필요로 하지 않는 전자거래와 다르다고 할 수 있다. 그러나 그렇다고 하여 전자문서교환이 전자거래와 전혀 다른 별개의 것이라고 할 수는 없다. 전자문서교환은 본질적으로 전자거래의 핵심적 요소라고 할 수 있는 컴퓨터 등을 이용한 전자적 방식의 데이터 교환을 수행한다는 점에서 전자거래와 공통점을 갖고, 또한 전자문서교환이 대부분 기업 간 거래에 이용된다는 점에서 전자거래의 한 범주에 속한다고 할 것이다.

한편 종래의 전자문서교환은 그 시스템 구축에 과다한 비용이 소요되고, 설정된 표준을 지원하지 못하는 각종 데이터를 이용하지 못할 뿐만

8) 홍준형, “인터넷 사회에 있어서의 EDI 및 전자거래 기능”, 「전자거래 및 EDI관련법 제도 정비방향」, 한국전산원, 1996, 16면.

아니라, 이미지, 사운드, 비디오 파일 등의 새로운 멀티미디어 데이터를 수용하지 못하는 단점을 가지고 있음으로 말미암아 기존에 EDI 네트워크를 구축하였거나 부가가치 통신망에 가입한 일정 규모 이상의 기업들에 의하여만 이용될 수 있다는 단점을 지니고 있었는데, 최근 전 세계적으로 인터넷을 이용한 기업 간 거래의 중요성이 고조됨에 따라 Open EDI 혹은 Internet EDI라는 인터넷을 이용한 전자문서교환 방식이 새로이 모색되고 있어 주목된다.

Ⅱ. 전자거래의 정의

앞서 살펴본 바와 같이 전자거래는 그 인접 개념들과의 구별을 통해 그 뜻을 명확히 할 수 있으며, 이를 토대로 전자거래란, "인터넷과 같은 개방형 시스템 하에서 컴퓨터 등 정보처리장치를 통하여 이루어지는 거래[9]"로 정의할 수 있다.

전자거래는 그 개념적 징표로 기업 간, 또는 기업과 소비자 간에 이루어지는 민간부문의 거래를 1차적으로 지칭하고 있으나, 정부와 기업, 또는 정부와 소비자 간에 이루어지는 공공부문의 거래를 포함하는 넓은 개념으로도 볼 여지가 있다. 왜냐하면 정보화의 발달로 인해 전자거래는 비단 민간부문에만 국한되지 않고 공공부문에까지 광범위하게 나타나고 있기 때문이다.[10]

이러한 전자거래의 정의에 대하여 국제사회에서 아직까지 확실히 합의된 것은 없다고 할 수 있다. 즉 국가마다 또는 기관마다 서로 다른 정의

9) 사법연수원, 전게서, 17면.
10) 제2장 제3절 전자거래의 유형에서 상술한다.

를 내리고 있다. 우리나라는 「전자거래기본법」(법률 제9504호)에서 전자거래의 정의를 “재화나 용역을 거래함에 있어서 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래”라고 규정하고 있다.[11] 이하 국제기구 및 주요국가에서 규정하고 있는 전자거래의 정의를 살펴보기로 한다.

Ⅲ. 국제기구 및 주요국가에서의 전자거래 정의

1. OECD

현재 국제기구 중에서 전자거래에 대하여 가장 다양한 논의를 벌이고 있는 국제기구는 OECD라 할 수 있다.[12] OECD는 다른 어느 국제기구보다 먼저 전자거래에 관한 논의를 시작하였으며, 산하 각 위원회를 통하여 조세, 소비자보호 및 개인정보보호, 암호, 인증 등 전자거래에 관한 주요 이슈에 대한 포괄적인 논의를 수행하여 왔다.

이를 통해 OECD는 1997년, “일반적으로 개인과 조직을 모두 포함해서 텍스트, 음성, 화상을 포함한 디지털화된 데이터의 처리와 전송에 바탕을 두고 있는 상업적인 활동과 관련된 모든 종류의 거래형태”라고 전자거래를 정의[13]하고 있다.

---

11) 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. “전자문서”라 함은 정보처리시스템에 의하여 전자적 형태로 작성, 송신·수신 또는 저장된 정보를 말한다.
2. “정보처리시스템”이라 함은 전자문서의 작성, 송신·수신 또는 저장을 위하여 이용되는 정보처리능력을 가진 전자적 장치 또는 체계를 말한다.
5. “전자거래”라 함은 재화나 용역을 거래함에 있어서 그 전부 또는 일부가 전자문서에 의하여 처리되는 거래를 말한다.

12) 이정원, “전자거래와 개인정보보호에 관한 연구”, 고려대학교 대학원 석사학위 논문, 고려대학교, 2002, 12면 이하.

13) http://www.oecd.org 참조.

2. EU

EU에서 전자거래의 일반적인 정의는 1997년 유럽위원회가 발표한 보고서인 '전자거래 서론(Introduction to Electronic Commerce)'에서 살펴볼 수 있다. 즉 전자거래는 "물리적인 교환 또는 직접적인 물리적 접촉에 의한 것보다는 당사자들이 전자적으로 상호 작용함으로써 이루어지는 모든 형태의 거래"로 정의하고 있다.[14]

한편, 유럽위원회는 1997년 '전자거래의 유럽 이니셔티브(European Initiative in Electronic Commerce)'에서 전자거래를 "텍스트, 음성, 화상 등을 포함한 데이터의 전자적인 처리와 전송을 기반으로 기업의 업무를 전자적으로 수행하는 방식"이라고도 정의함[15]으로써, 전자거래가 상품 및 서비스의 전자적인 무역, 상업적인 경매, 공동구매 등 많은 다양한 행동들을 포괄한다고 하였다.[16]

3. 미국

미국에서의 전자거래의 모습은 1997년 7월 Clinton 대통령이 발표한 '세계전자거래골격(Framework for Global Electronic Commerce)'[17]에서 간접적으로 찾을 수 있다. 1997년 세계전자거래골격은 미국의 전자거래 정책의 핵심적인 시각과 리더십을 천명하는 중요한 내용을 담고 있다. 1997년 세계전자거래골격에 따르면 "인터넷은 소매 및 직접 마케팅의 방식 역시 개혁할 것이다. 소비자들은 가정에서 전 세계의 제조업체와 소매

14) European Commission, *An Introduction to Electronic Commerce*, 1997.
15) European Commission, *An European Initiative in Electronic Commerce*, 1997.
16) *Id.*
17) The White House, *A Framework for Global Electronic Commerce*, 1997.

업체로부터 다양한 제품을 구매할 수 있게 될 것이다. 소비자들은 거실에 앉아서 이러한 상품을 그들의 컴퓨터나 TV로 보고, 상품에 대한 정보를 얻고, 제품이 얼마나 서로 잘 어울리는지를 보고, 선택한 제품을 주문하고, 대금을 지불할 수 있게 될 것이다"라고 언급하여 전자거래의 실제적인 형태를 설명하고 있다.[18]

또한 미국에서의 일반적인 전자거래의 정의는 1999년 미국 상무부가 발표한 보고서인 '떠오르는 디지털경제 Ⅱ(Emerging Digital Economy Ⅱ)에서 찾을 수 있다. 동 보고서는 전자거래를 "인터넷 또는 웹을 기반으로 한 시스템에서 거래가 이루어지는 영업방식"으로 정의하고 있다. 또한 미 상무부 상하 통계국(U.S. Census Bureau)[19]은 "상품이나 서비스의 소유권 또는 권리의 이전을 포함하는 컴퓨터를 매개로 한 네트워크상에서 완료되는 거래"로 정의하고 있다.

4. 일본

일본에서의 전자거래 정의는 1998년 3월 「민간부문의전자상거래개인정보보호지침」에서 찾을 수 있다. 동 지침 제2조에 의하면 전자거래란 "전자적 네트워크상에서 상거래 및 이것을 유인하기 위한 선전 광고의 일부 또는 전부를 행하는 것"이라고 규정되어 있다. 그리고 1996년 일본전자성거래추진협의회는 "다양한 종류의 컴퓨터 네트워크를 이용하여 상품 디자인, 제조, 광고활동, 상거래, 계좌결제 등 전반적인 활동을 지원하는 것"이라고 정의한 바 있다.

---

18) 최석범, 엄광열, "미국의 통일전자거래법과 한국의 전자거래기본법에 관한 연구", 「국제상학 16권 2호」, 2001. 11, 4면 이하.

19) http://www.census.gov 참조.

제2절 전자거래의 특성

Ⅰ. 의사전달의 호환성

전자거래에 있어서의 가장 큰 특징은 양 당사자 간의 의사전달의 호환성 문제이다.[20] 기존의 거래방식은 자연적인 방법과 수단을 이용하므로 의사전달의 호환성은 거의 문제가 되지 않으나 컴퓨터를 이용한 전자거래에 있어서는 하드웨어와 소프트웨어의 호환성에 따라 계약체결의 여부가 달려있게 된다. 즉 컴퓨터라는 하드웨어와 소프트웨어를 이용하는 것은 호환성의 필요조건에 불과하고, 그 외에도 그것들의 기술적인 호환성의 존재가 충분조건이라고 할 것이다. 구체적으로는 컴퓨터 간의 전자데이터 전달을 위한 프로토콜의 설정에 있어서도 불일치가 발생하게 되면 호환성이 결여되게 된다. 이러한 호환성 불일치 문제는 계약체결과정의 의사전달에 있어서만이 아니라 전자적 이행에 있어서도 발생하는 광범위한 문제이다.

Ⅱ. 의사표시의 기술화

전자거래의 또 다른 특징으로는 의사표시의 기술화를 들 수 있다. 즉 의사전달을 위해 기술적 수단이 이용되며 표의자는 그러한 기술적 수단에 대한 이해가 부족한 것이 통상이다. 이로 인해 의사전달과정에 있어서 제3자의 개입을 필요로 하게 되고 그에 따라 법률관계도 중첩적으로 구성될 가능성이 있다. 즉 일방의 의사표시의 전달을 위해서 제3자의 개입이 존

20) 사법연수원, 전게서, 24면 이하.

재하므로, 그 제3자의 영향에 따라 전달위험을 발생영역이 확대된다는 점이다. 이는 이행과정에서도 대부분의 경우에 전산망의 소유자나 운영자 등의 이행보조자를 필요로 하게 되는 양상으로 나타나며, 그에 따라 법률관계도 매우 복잡하게 된다.

Ⅲ. 의사결정의 자동화

전자거래의 특성 중 현실적인 장점은 재산법적 거래에 있어서 컴퓨터라는 새로운 의사결정 수단을 이용하여 인간의 의사결정기능을 대체시킬 수 있다는 것이다. 기존의 거래과정에 있어서 의사결정이란 전적으로 행위자인 인간의 유일한 능력이었지만, 전자거래에 있어서는 행위자 내지는 다른 전문가의 도움을 받아 컴퓨터에게 그 기능을 맡길 수 있게 된다. 즉 컴퓨터는 인간이 사전에 입력한 프로그램에 종속되어, 프로그램에 따른 수치적 판단을 하여 일정한 결정을 하게 된다. 이러한 컴퓨터의 결정프로세스는 전적으로 비인간적인 전자적 작동과정이며, 인간이 구체적이고 개별적인 프로세스 과정을 자연적인 방법으로 인식할 수 없다는 점이 그 특징이다.

Ⅳ. 전자적 이행방법의 도입

전자거래에 있어서는 전자적인 방법을 이용해서 목적물의 이행이 가능하다는 점도 중요한 특징 중의 하나이다. 즉 전자거래의 목적물의 이행과정도 체결과정과 같이 컴퓨터와 컴퓨터망을 이용하여 행해지게 되는 특징이 나타난다. 이것은 전자거래가 기존의 거래와 구별되는 매우 중요한 특성이며, 이로 인해 사이버스페이스에서 계약체결과 이행까지 거래의 전

과정이 완결될 수 있게 된다. 이러한 특성에 따라 경제적인 측면에서는 대량거래가 이루어질 수 있게 되며 나아가 자동화된 대량거래 또한 가능하게 된다.

Ⅴ. 방식의 정형화

전자거래의 체결과정에 있어서는 법률행위 방식의 정형화가 이루어지게 되어 마치 고대의 방식주의로의 회귀가 이루어지는 것과 같은 결과를 초래하게 된다. 따라서 의사표시이론에 있어서도 무방식주의에 따른 기존의 해석론에 변화가 초래될 여지가 있다. 그러므로 당사자로서는 입력할 공간이 주어지지 않는 경우에는 계약의 내용에 삽입하고자 하는 조항을 포함시킬 수 없게 되고, 따라서 기존의 별도의 특약이 존재할 가능성이 없어지게 됨으로써 예기치 못한 불이익을 받을 가능성이 커질 수 있다.

제3절 전자거래의 유형

전자거래의 분류방법 중 현실적으로 가장 의미 있는 방법은 거래주체에 따른 분류방법이라고 할 수 있다.[21][22][23]

---

21) 사법연수원, 전게서, 41면.

22) 전자거래의 유형은 학자에 따라 다양한 기준을 제시하여 분류한다.
"거래주체에 따라서 기업과 소비자 간의 전자상거래, 기업과 기업 간 전자상거래, 기업과 정부 간 전자상거래, 소비자와 소비자 간의 전자상거래로, 거래유형에 따라서 인터넷 포털 서비스업, 인터넷 콘텐츠 서비스업, 인터넷 전자상거래업, 인터넷 중개업으로, 기술유형에 따라서 EDI 전자상거래(폐쇄형 전자상거래), 인터넷 전자상거래(개방형 전자상거래)로 분류한다." (정완용, 「전자상거래법」, 법영사, 2002, 24면 참조.)
"디지털화에 따라 자연적 방법의 계약체결, 전자적 방법의 계약체결, 자연적 방법의 이행, 전자적 방법의 이행으로 구분한 후 이러한 유형의 전자거래를 다시 협의의 전자거래, 광의의 전자거래로 분류하고, 거래주체에 따라 기업 간의 전자상거래, 기업과 개인 간의 전자상거래, 개인 간의 전자상거래, 기업과 공공기관의 전자거래로 분류하고, 자동화에 따라 수동적 전자거래, 자동화된 전자거래로 분류한다." (오병철, 「전자거래법」, 법원사, 2000. 73면 참조.)
"거래주체, 표준화 여부, 자동화 여부에 따라 분류한다." (정쾌영, 전게서, 37면 참조.)

첫째, 개인을 거래의 한 축으로 삼아 P(person) to P, P to B(Business), P to G(Government)로 분류해 볼 수 있다.[24]

전자문서를 이용하거나 이행행위가 전자적인 방법으로 이루어지는 경우를 전자거래로 보게 되면 상인이 아닌 일반 개인의 법률행위도 전자거래가 된다. P to P의 가장 일반적인 경우는 경매나 벼룩시장을 통한 개인간의 매매이다. 경매는 판매자가 경매사이트에 판매할 물품의 목록, 성능, 가격 등을 올려놓으면 구매자가 경매절차를 거쳐 구입하는 방식이다. 벼룩시장은 판매자가 자신이 사용하던 상품을 일정한 비용을 주고 벼룩시장 웹사이트에 광고하면 구매자가 필요한 상품을 구입하거나 특정한 상품을 구입하기를 원하는 구매자가 구매 정보를 올려놓으면 그것을 본 판매자가 상품을 제공하는 방식으로 이루어지는 전자거래행위이다.

P to B는 가장 일반적인 전자거래의 한 형태이다. 일반적으로 판매자는 사이버몰이나 기업의 웹사이트를 통해 상품의 목록, 성능, 가격, A/S 조건 등을 제시해놓고 구매자를 기다린다. 구매자들은 이러한 정보를 보고 자신이 필요로 하는 물건의 신분을 확인하는 내용을 기재하고 대금을 지급한 후 구입하게 된다.

P to G의 경우는 공공기관의 대민 서비스라는 차원뿐만 아니라 행정업무의 전자화라는 측면에서 아주 중요한 문제이다. 공공기관에서 발급하는 각종 민원서류를 정보처리시스템을 통해 발급받을 수 있고, 각종 신고

23) 이윤선, “전자거래에 관한 연구”, 「민사법연구 11집 2호」, 2003. 12, 7면 이하.
24) 장은상, “전자거래에있어서 개인정보의 보호”, 호남대학교 대학원 석사학위 논문, 호남대학교, 2006, 16면 이하.

를 전자문서를 사용해서 할 수 있고, 공공기관에서 발급하는 각종 통지를 이메일로 받아볼 수 있는 제도이다. 이러한 P to G의 경우는 공공기관이나 개인 모두에게 중요한 사항일 가능성이 많으므로 특히 전송되는 정보의 정확성과 보안성이 중요시된다.

둘째, 기업을 전자거래의 한 축으로 보면 B to P, B to B, B to G로 구분해 볼 수 있다.

기업과 기업 간의 거래는 특정 기업과의 거래와 불특정 기업과의 거래로 구분해 볼 수 있다. 특정기업 간의 거래는 미리 합의된 표준화된 전자문서를 사용하여 상거래를 체결하고 대금을 결제하고 급부를 이행할 가능성이 많다. 그러나 불특정 기업과의 거래는 새로운 납품입찰에 응찰하거나 구매 계약을 통해서 이루어진다.

그리고 B to G의 경우는 크게 공공기관의 사경제 주체로서 기업과 경제활동을 하는 경우와 공공기관이 기업과 관련된 민원업무를 정보처리시스템을 사용하여 처리할 수 있게 하는 경우이다. 전자의 경우에는 기업은 공공기관이 필요로 하는 상품의 구매입찰에 응찰하거나 수의계약을 통해 판매하게 된다. 물론 입찰이나 계약이 전자문서를 사용하여 이루어진 경우에 「전자거래기본법」이 적용될 여지가 있다. 후자의 경우에는 공공기관이 기업에 세금고지서나 민원서류를 전자문서를 사용하여 발급하고 기업은 각종 등록과 신고를 전자문서를 사용하여 하게 된다. 공공기관과 기업 간의 이러한 민원 업무는 정확성과 보안성을 요구하는 경우가 많아 전자서명이나 전자인증제도의 사용이 필요하게 된다.

셋째, 공공기관을 전자거래의 한 축으로 삼으면 G to P, G to B, G to G로 구분할 수 있다. 특히 공공기관 간 업무결제, 의사전달, 정보교환은 보안을 요구하는 중요한 사항이 많으며, 공공기관 내부나 공공기관 간의 업무결제는 표준화되고 전자서명이 필수적 요소가 된다.

제3장 개인정보보호에 관한 국내·외 동향

제1절 개인정보의 의의와 개인정보보호의 필요성

Ⅰ. 개인정보의 의의

1. 개인정보 개념의 연혁

개인정보를 지칭하는 용어로는 전통적으로 '비밀' 또는 '프라이버시'라는 용어가 사용되어 왔다. 비밀이란 '일반적으로 알려지지 않은 사실 또는 일정한 범위 내의 사람에게만 알려진 사실로서 이를 타인에게 알리지 않음으로써 본인에게 이익이 있는 사실'을 말한다. 이러한 비밀에 대하여 보호받을 권리는 개인이 가지는 프라이버시권의 내용 중 하나라고 할 수 있다.

프라이버시라는 용어가 사용되기 시작한 것은 Samuel D. Warren과 Louis D. Brandeis가 1890년 발표한 'The Right to Privacy'[25]라는 논문에서부터였다. 위 두 사람은 프라이버시를 "홀로 있을 권리(the right to be let alone)"라고 정의하면서 당시의 과학기술의 진보와 사회 환경의 변화에 따라 이와 같은 새로운 유형의 권리를 인식할 필요성을 강조하였는데, 그 후 1903년 뉴욕 주에서 최초로 「프라이버시법」을 제정하였고 1965년 Griswold v. Connecticut (381 U.S. 479) 판결에서 프라이버시권은 법원에서 헌법상 권리로까지 인정되었다. 한편 1960년 미국의 민법학자인

25) S.D. Warren & L.D. Brandeis, *The Right to Privacy*, Harv. Law Rev., 1890. (양창수, "정보화 사회와 프라이버시의 보호", 「인권과 정의」, 1991. 3, 73면 이하 참조.)

Prosser가 프라이버시권에 대한 침해를 사사(私事)에 대한 침입(intrusion), 공개(public disclosure), 오인(false light in the public eye), 도용(appropriation) 등 4가지 민사법상의 불법행위 유형으로 분류하여 널리 학계와 법원의 지지를 받게 되었다.[26]

그러나, 1960년대 말 이후 컴퓨터와 정보통신기술의 발달로 인하여 개인정보의 대량 수집·축적·처리·이용이 가능해지면서 개인의 프라이버시가 침해될 가능성이 커지고 특히 인터넷이라는 범세계적인 네트워크를 통한 정보의 광범위한 유통으로 인하여 프라이버시 문제가 크게 부각되었다. 그리고 국가 및 공공기관 뿐만 아니라 민간기관이나 기업 등에 의한 개인정보의 대량수집·이용이 활발해지면서, '홀로 있을 권리' 또는 '사사에 대한 침입과 공개 등에서 오는 피해의 보호'라는 소극적 측면에서의 전통적인 프라이버시의 개념을 통한 민사적 구제만으로는 개인의 프라이버시를 충분히 보호하기 어렵게 되었다.

이에 따라 오늘날의 정보처리기술의 발달에 부응하는 보다 동적이고 다양한 내용을 포섭할 수 있는 개념의 프라이버시권을 주장하는 경향이 대두되어, 최근에는 '적극적으로 자신에 관한 정보의 유통을 통제하는 권리[27]' 또는 '자신의 정보를 언제 어떻게 어느 정도로 타인에게 알릴 것인가를 결정하는 배타적인 권리[28]' 등을 의미하는 정보프라이버시(Information Privacy)권[29]이라는 개념이 나타나게 되었다. 즉, 정보프라이

---

26) 헌법재판소는 프라이버시를 사생활 은폐권이라고 하였다. (헌법재판소 1990. 9. 10. 선고 89헌마82 결정)

27) 판례도 "헌법 제17조는 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.'라고 규정하고 있는바, 이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다"라고 하여 같은 견해를 취하고 있다(대법원 1998. 7. 24. 선고 96다42789 판결).

28) Alan F. Westin, *Privacy and Rreedom*, N.Y. Ateneum, 1967, p.32.

버시권은 개인이 자신에 관한 정보가 어디까지 이용되는가를 결정하고 그 정보에 대하여 자신이 자유롭게 통제할 수 있는 자기결정권[30]을 의미하는 적극적이고 능동적인 권리를 의미하는 것이다.[31]

그리고 개인정보(personal data)라는 표현은 독일의 1997년 「연방데이터보호법」에서 사용된 개인관련 정보(Personbezogenes Datum)에서 비롯된 것으로 보는 것이 일반적인데, 이는 '프라이버시'나 '개인의 비밀'이라는 표현의 외연이 불분명하여 가벌성의 범위를 확정하기 어려웠던 데서 나온 해결책이다.[32] 이러한 의미에서 개인정보는 정보주체의 자기결정권에 의한 통제 하에서 수집·저장·관리·유통될 수 있는 개인에 관련된 자료 및 정보라고 할 수 있고, 그 보호법익은 '정보의 자기결정권 내지 자기통제권'이라고 할 수 있다.[33][34][35]

---

29) 정보프라이버시권의 구체적인 내용으로는 개인정보의 존재를 알 권리, 정보수집에 대한 동의권, 정보에 대한 열람권, 정보처리의 용도와 공개의 범위 및 변경 사항에 대하여 통지를 받을 권리, 잘못된 개인정보에 대한 정정청구권, 반대권, 삭제권 및 이용금지권 등이 논의되고 있다.

30) 이를 자기정보콘트롤권이라고도 한다. (大澤秀介, "個人情報の 保護", 「法學敎室」, 1996. 3, 36면 이하 참조.)

31) 김영철, "프라이버시권의 보호법익과 법적 성격", 「언론중재」, 1999년 여름호, 10면. 이와 관련하여, 종래 일컬어졌던 Privacy(정보내용의 비밀성 보호) 뿐만 아니라 Security(정보보안, 특히 정보의 완전성을 포함하는 안정성과 무결성)를 포함하는 개념으로서 개인의 정보보안권이 기본권으로 새롭게 인식되어야 한다는 견해도 있다. (강경근, "인터넷 사회에서의 개인정보보안과 정보기반보호, 「인터넷 법률」, 2000. 7, 37면 참조.)

32) 개인정보에 관한 용어는 미국의 '프라이버시' 이외에도, 뉴질랜드에서는 '데이터'로 표현하고, 중국에서는 '隱私'라고 표현하는 등으로 각국마다 그 용어가 조금씩 다르게 사용되고 있다. (장영민, "정보통신망발전에 따른 개인정보보호", 「형사정책 연구 7권 2호」, 1996, 8면 참조.)

33) 프라이버시와 개인정보에 관하여는, 프라이버시(privacy)는 내심의 정신활동의 자유를 포함하여 행동이나 환경면에서 사적 영역에의 간섭과 침해를 배제하는 것으로서의 장소적·공간적 영역 개념이고, 개인정보(personal data)는 개인에 관련된 개별적인 정보로서 개인의 프라이버시가 기록되고 관리되는 형태로 나타난 것이므로 프라이버시 보호는 장소적·공간적 영역에 대한 침해를 규제하여 직접적으로 프라이버시를 보호하는 측면에서, 개인정보보호는 관리되는 개인데이터를 보호하기 위하여 그 관리자를 규제하는 측면에서 양자를 구분하여 논의하여야 한다는 견해도 있다. (牧野二郎, "プライバシとはなにか", 「プライバシ保護と個人情報保護の關する考察」, 1999. 8, 28면 이하 참조.)

34) 이와 관련하여, 프라이버시의 정의는 불분명하고 매우 상대적이므로 프라이버시권을 특히 사법상의 개인정보에 관한 권리의 보호근거로 삼기는 어렵고 개인정보에 관한 자기주장과 정보제공에 대한 자기결정권을 하나의 독립한 인격권으로 보아 개인정보권을 하나의 권리로 인정함이 상당하다는 견해도 있다. (임건면, "민사법상의 개인정보보호", 「비교사법 3권 1호」, 1996. 6, 155

2. 개인정보의 정의

개인정보의 정의와 관련하여 「공공기관의개인정보보호에관한법률」은 “개인정보라 함은 생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명·주민등록번호 및 화상 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)를 말한다”[36]라고 정의를 내리고 있다.

또한 이와 유사하게 「정보통신망이용촉진및정보보호등에관한법률」은 “개인정보란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등의 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한

면 이하 참조.)

35) 프라이버시는 특정개인을 식별할 수 있는 개인정보를 보호함으로써 보호될 수 있을 것이다. 즉 개인정보보호는 개인정보의 수집·처리·이용에 의한 프라이버시 침해를 예방하거나 구제하는 것으로 프라이버시보호의 한 부분이라 할 수 있다. 왜냐하면 정보화 사회에서 프라이버시의 침해는 전통적인 의미의 프라이버시 보호의 관점보다 개인정보보호의 관점으로 옮아가고 있는데, 이는 프라이버시 문제를 개인정보보호의 문제로 보는 경우 더욱 효과적인 법적 해결책을 발견할 수 있기 때문이다. 이 같은 프라이버시권의 보호법익은 크게 3가지 측면에서 살펴볼 수 있다. 첫째, 사법상의 견지로부터의 프라이버시권의 보호법익은 성명권의 침해, 초상권의 침해, 과거의 경력· 병력 등의 폭로, 전신·전화의 도청, 미행, 엿보기, 가족관계의 폭로나 비방 또는 중상 등으로부터의 보호이다. 둘째, 공법상의 견리로부터의 프라이버시권의 보호법익은 전신·전화의 도청, 사상조사로서의 부당한 가택수사나 지문채취, 미행, 경찰관의 직무집행에 의한 불필요한 입회조사, 적법절차에 위반된 인신자유의 침해 및 불법 주거침입, 압수수색, 불이익한 진술의 강요 등으로부터의 보호이다. 셋째, 행정기관의 개인정보 수집·이용 등에 관한 보호법익은 어떠한 개인정보를 입력하여 보유하고 있는가, 보유하는 정보를 어느 정도까지 공개하는가, 행정기관 상호간의 정보제공의 정도, 개인정보의 열람과 정정, 삭제권, 불복신청제도의 인정여부 등을 들 수 있다. (최상호, “전자거래에 있어서의 소비자보호 -특히 프라이버시 및 개인정보보호를 중심으로”, 「비교사법 8권 1호」, 2001, 4면 이하.)

36) 「공공기관의개인정보보호에관한법률」(1994. 1. 7. 제정 법률 제4734호, 2008. 2. 29. 제5차 개정 법률 제8871호) 제2조 제2호.

다"[37]라고 정의 내리고 있다.[38]

이들 법은 인격주체성의 유지라는 측면에서가 아니라 그 인격주체성을 현출할 수 있는 정보라고 정의하기 때문에 적극적인 프라이버시개념을 정의하고 있는 것으로 볼 수 있다. 즉 개인정보의 범위는 전통적인 인격권적 프라이버시 개념을 넘어 재산상황, 소득, 채권채무관계 등의 경제관계에 관한 정보 내지 기업주의 당해 사업에 관한 정보까지 포함하는 적극적인 의미를 지니고 있는 것이다.[39] 또한 전통적 프라이버시 개념을 넘어 그 범주가 정보 내지 자료까지 포함할 수 있는 내용을 지님으로써 개인정보를 그 핵심적 요소로 하는 정보프라이버시(Information Privacy)의 개념까지 포함하는 정의를 하고 있는 것이다.

이러한 개념이야말로 인터넷과 같은 통신망을 기초로 하는 사이버스페이스에서의 프라이버시(Cyberspace Privacy)에 적합한 개념이라 볼 수 있다. 이 때 개인정보의 개념은 자기결정권으로서의 프라이버시권이라는 '위치적' 성격으로부터, 정보생산자와 소비자 사이의 '유통적' 측면이 중요시되는 '정보프라이버시'의 성격을 나타내고 있는 것이다.

즉 요약하자면 개인정보란 '개인의 신념, 신체, 재산, 사회적 지위, 신분 등에 관한 사실 판단·평가를 나타내는 일체의 정보'라 할 수 있다. 이

37) 「정보통신망이용촉진및정보보호등에관한법률」(1986. 5. 12. 제정 법률 제3848호, 2008. 6. 13. 제26차 개정 법률 제9119호) 제2조 제6호.

38) 이러한 정의는 OECD의 개인정보보호지침의 내용과 유사한데, EU지침 역시 개인정보보호에 관한 회원국 간의 국내법규범의 차이를 제거하고 공통된 법원칙을 마련하기 위하여 발표한 「개인정보의 처리 및 자유로운 이전에 관한 개인보호지침(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data on the free Movement of such Date)」에서의 개인정보의 정의인 '자연인을 식별하거나 식별시킬 수 있는 모든 정보'와 그 내용이 유사하다고 할 수 있다.

39) 총무처, 「축조해설 개인정보보호법」, 총무처, 1994, 31면 이하.

러한 개인정보는 다음과 같은 2가지 점에서 그 개념적 한계를 설정할 수 있다.

1) 생존하는 개인에 관한 정보

개인정보는 자연인으로서 현재 생존하고 있는 개인에 관한 정보만을 말한다. 따라서 이미 사망하였거나 사망으로 추정되는 자 또는 법인 기타 단체에 관한 정보는 개인정보의 보호대상에서 제외된다고 할 수 있다.[40] 다만, 사망자의 정보 중 사망자와 유족 간의 관계를 나타내는 정보는 사망자의 정보인 동시에 관계되는 유족의 정보이기도 하므로 유족이 생존하고 있는 경우에는 개인에 관한 정보가 된다.

2) 개인 식별이 가능한 정보

개인정보는 당해 정보에 포함된 사항에 의하여 당해 개인을 식별할 수 있는 정보를 말한다. 당해 특정 정보만을 가지고는 식별할 수 없으나 다른 정보와 쉽게 결합하여 당해 개인을 식별할 수 있는 경우에는 그것도 해당된다. 예컨대 주소와 본적만을 가지고는 당해 개인을 식별할 수 없으나, 성명 및 주민등록번호 등과 조합할 경우 특정인을 식별할 수 있기 때문에 주소와 본적 등도 개인정보에 해당된다고 볼 수 있다.

개인 식별이 가능한 정보에는 당해 개인정보에 대하여 특별한 정보를 가지지 못한 제3자가 보더라도 당해 개인을 식별할 수 있는 정보를 포함

40) 개인정보보호의 기초가 되는 프라이버시권은 흔히 인격권으로서 사망과 더불어 소멸되는 일신전속권을 가지는 것으로 보고 있으며, 사자 및 법인에게는 인정되지 않는 것으로 보는 것이 일반적이다.

한다. 예컨대 성명없이 특수한 직함이나 직명 등을 포함하고 있는 경우를 들 수 있다. 따라서 이용자 개인의 기호도 식별성이 있는 경우에는 개인정보에 해당할 수 있다.

3. 개인정보의 종류

개인정보는 그 영역에 따라 '공공부문의 개인정보'와 '민간부문의 개인정보'로 나누어 볼 수 있다. 종래 프라이버시보호의 개념이 공공기관의 개인에 대한 프라이버시 침해 위주로 논의되어 온 관계로 공공부문의 개인정보보호에 관하여는 그 동안 각국에서 입법에 의한 보호 노력이 이어져 왔으나, 민간부문에 대한 개인정보보호 문제는 개인정보의 소유자와 취급자 사이의 개별적인 관계로 한정되어 취급되어 오다가, 최근 정보통신기술의 발달과 함께 전 세계적인 네트워크가 구성되고 개인에 의한 프라이버시 침해가 사회적 문제로 부각되면서 그 규제 문제가 초점의 대상이 되고 있다.[41]

또한 개인정보의 구체적인 내용에 따라 성명, 주민등록번호, 생년월일, 출생지, 성별, 국적 등의 일반정보와 가족정보, 교육 및 훈련정보, 병역정보, 부동산 및 동산정보, 소득 및 기타 수익정보, 신용정보, 고용정보, 법적정보(형사처벌기록, 소송기록, 이혼기륵 등), 의료정보, 조직정보, 습관 및 취미정보 등으로 나누어 볼 수 있다.

한편 개인정보를 인적 요소가 강한 정보와 재산적 요소가 강한 정보로 나누어 볼 수도 있다. 전자는 앞서 본 일반정보, 가족정보, 교육 및 훈련

41) 백충길, 정회근, "전자상거래와 개인정보보호", 「토지공법연구」, 2002, 650면 이하.

정보, 병역 정보 등이 그 대상이 되고, 후자는 부동산 및 동산정보, 소득 및 기타 수익정보, 신용정보 등이 그 대상이 될 것이나, 하나의 정보가 인적 요소와 재산적 요소를 모두 가지는 것도 있으므로 그 구분이 반드시 명확한 것은 아니다.

Ⅱ. 개인정보보호의 필요성

개인정보가 본인이 알지도 못하는 사이에 축적되거나 사업자가 목적을 밝히지 않고 또는 허위의 목적으로 정보를 수집하는 경우, 소비자가 사업자에게 맡긴 개인정보의 관리나 보안을 소홀히 하여 사업자가 분실하거나 외부로 유출하게 되는 경우, 개인정보가 원래의 목적 이외의 목적으로 부당하게 이용되거나 제3자에게 판매 등으로 유출되는 경우[42], 과거의 정보 내지 잘못된 정보가 유통되어 개인정보의 진실성 및 최신성을 침해하는 경우 등으로 인하여 정보주체에게 직접적인 경제적 피해뿐만 아니라 정신적 피해도 입히는 경우가 날이 갈수록 많이 발생하고 있다.

42) 개인정보의 누출 경로를 보면, 내부자 정보 오·남용과 외부자에 의한 해킹 등을 들 수 있다. 먼저 시청, 동사무소 등 행정관청이나 경찰청, 검찰청 등 국가 공공기관에서뿐만 아니라, 전화국, 보험회사, 대학교 등 민간의 고객정보가 유출되는 사례가 빈번히 일어나고 있으나 주로 내부자에 의한 개인정보 유출이 주를 이루고 있다. 그리고 내부자에 의한 정보 오·남용은 특히 금융기관을 중심으로 외부인과 결탁하여 내부직원의 전산단말기의 조작을 통한 한탕주의식 범죄 형태로 이루어지는 경우도 많다. 이와 같이 기업 내지 관공서 내부에서 나타나고 있는 내부자 정보 오·남용 현상은 주로 임직원, 퇴직자 또는 협력관계의 직원에 의해 발생하므로 방지와 적발에 어려움이 많다. 그리고 과학기술의 발달과 정보통신의 발전으로 정보수집 장비와 기법 등이 발전하고 기업환경이 국경 없는 무한경쟁시대로 급변함에 따라 국내·외 기업에서의 주요 산업기밀유출이 증가하고 있어 국가 간의 분쟁의 소지에 대한 우려가 많다. 그리고 정보시스템에 대한 사이버 테러는 국가 주요업무의 마비와 사회전체의 혼란을 초래한다. 해킹사고 유형은 해킹 대상을 데이터, 시스템 프로그램, 네트워크로 분류하여 해커들이 저지를 수 있는 해킹 행위를 불법삽입, 불법유출, 불법변조, 파괴·거부 등의 행위로 구분할 수 있다. 사업자 시스템에 대한 해킹은 주로 관리자 권한을 부당 획득하는 방법 등을 이용하면 개인정보 등 유출이 가능하며, 특히 사용자ID, 비밀번호 파일 등이 유출되고 있는 실정이다. (사법연수원, 전게서, 97면 이하 참조.)

그리고 하루가 다르게 발전해 가고 있는 컴퓨터 기술은 정치, 경제, 사회, 문화, 군사 등 모든 분야에 걸쳐 엄청난 영향력을 행사하고 있는 바, 특히 컴퓨터를 이용한 정보처리기술의 획기적인 발달은 개인에 관한 정보를 대량으로 수집하고 분석하는 것을 용이하게 함으로써, 개인정보에 관한 상업적 이용가능성이 높아졌다. 이러한 개인정보에 관한 상업적 이용은 개인정보 침해·유출, 근본적으로는 프라이버시권 침해라는 우려를 증폭시키고 있으며, 나아가 개인정보의 유출과 오·남용의 문제가 심각한 사회문제로까지 이어질 수 있을 것이다.

왜냐하면 정보화 사회에 있어서 개인정보를 소유하는 자는 그 사람의 사회적, 경제적 지위와 기호 및 선호하는 상품의 양상까지도 파악할 수 있게 되어 그 개인정보가 그 사람의 모든 것을 판단할 수 있는 중요한 척도가 되어 있으므로, 만일 개인정보의 침해가 발생한다면 개인의 프라이버시를 침해하는 것은 물론 개인 권익의 손실을 유발할 수 있고 궁극적으로는 인간의 존엄성 침해를 가져올 수도 있기 때문이다.[43]

그러므로 사생활의 비밀과 자유의 불가침은 사생활의 내용을 공개당하지 않을 권리, 자신에 관한 정보를 스스로 관리·통제할 수 있는 권리 등을 내용으로 하는 인격권으로서 오늘날 정보화 사회가 급속히 진행되면서 그 호보가 절실히 필요한 권리가 되었다. 일반적으로 기본권의 보호법익은 생명권, 인격권이 가장 우선한다고 보여지는 점에서 국민의 기본권에 속하지만 공공기관의 정보에 대한 공개청구권을 의미하는 한 청구권적·간접적 성격을 가진다고 보여지는 국민의 알 권리보다는 개인의 사생활의 비밀과 자유가 더 보호해야할 우선적인 가치라고 할 것이다.[44]

---

43) 유황빈, "디지털시대의 개인정보보호 기술", 「인터넷 법률」, 2001, 63면.
44) 서울고법 1995. 8. 24. 선고 94구39262 판결.

이처럼 개인정보의 유출은 결국 개인의 인격형성을 저해하고 사적 자유영역을 심각하게 위협함으로써 개인의 인간존엄을 핵심요소로 하는 자유민주체제의 그간을 흔들 가능성을 지니고 있다고 볼 수 있기 때문에 개인정보보호는 절실하다고 하겠다.[45] 다만 이러한 견해는 헌법재판소가 "기본권이 충돌하는 경우에는 헌법의 통일성을 유지하기 위하여 상충되는 기본권 모두가 최대한으로 그 기능과 효력을 나타낼 수 있도록 조화로운 방법을 모색하여야 할 것[46]"이라고 보고 있는 태도와는 다소 다르다고 볼 여지는 있다.

물론 인격권으로서의 개인의 명예의 보호와 표현의 자유의 보장이라는 두 법익이 충돌하였을 때, 그 조정을 어떻게 할지의 문제는 구체적인 경우에 사회적인 여러 가지 이익을 비교하여 표현의 자유로 얻어지는 이익 및 가치와 인격권의 보호에 의하여 달성되는 가치를 형량하여 그 규제의 폭과 방법을 정해야 하겠지만[47], 프라이버시권의 보호를 통한 개인의 사적 생활영역의 확보는 정보화 사회가 더욱 진전됨에 따라 그 중요성은 배가된다고 볼 수 있으며, 가능하다면 개인정보의 보호에 더 큰 비중을 두어야 할 것이다.

제2절 개인정보보호제도 개관

현재, 개인정보의 부당한 유출을 막고 이를 보호하기 위한 여러 가지 제도적 장치가 있다. 먼저 개인정보보호법의 제정을 통한 방법이 있으며,

45) 한국정보보호센터, 「정보화 역기능 사례집(보고서)」, 2006, 59면.
46) 헌법재판소 1991. 9. 16. 선고 89헌마165 결정.
47) 대법원 1988. 10. 11. 선고 85다카29 판결.

이를 근거로 설립한 개인정보보호기구를 통한 방법이 있다. 물론 어느 한 가지 방법만 사용하는 것은 아니며, 이 둘을 적절히 조화롭게 사용하는 것이 보다 효율적으로 개인정보를 보호하는 것이라 하겠다.

Ⅰ. 개인정보보호법

오늘날 세계 각국의 개인정보보호법은 법률의 적용범위나 영역이 특정 부문에 한정되어 있는지 아니면 개인정보보호를 위한 기본적인 사항을 규정하여 포괄적인 적용범위를 가지고 있는지에 따라, 통합형 입법주의와 구분형 입법주의로 나누어 볼 수 있다.[48]

1. 통합형 입법주의

통합형 개인정보보호법이란 공공부문과 민간부분을 포괄적으로 규율하는 개인정보보호기본법을 의미한다. 그러나 통합형 입법주의라고 하여 개별 영역별 개인정보 법률이 전혀 없는 것은 아니다. 공공부문과 민간부문을 아우르는 기본법은 모든 영역에 적용될 수 있는 기본원칙과 같은 일반적인 사항을 규정하고 있고 세부적인 내용을 규정하지 않는 경우가 많다. 그렇기 때문에 개인정보의 유형의 다양성, 정보처리기술의 복잡성, 개인정보처리 영역의 광범위성 등으로 인하여 새롭고 특수한 분야의 경우에는 별도의 개인정보 관련 특별법이 제정되어 시행되고 있는 경우가 많다. 또한 기본법에서 모두 포함될 수 없는 부분을 특별법 또는 하위법령으로 제정하는 형식 외에도, 개인정보 커미셔너와 같은 개인정보보호기구에게 실

48) 이러한 '입법의 존재형식에 따른 비교' 외에도 적용범위에 따라 '개인정보의 자동처리 유무에 따른 비교', '정보주체의 성질에 따른 비교'가 가능하다. (개인정보분쟁조정위원회, 전게서, 235면 참조.)

행규약의 승인이나 제정을 통해 통합형 개인정보보호법에서 제시하고 있는 기본원칙의 적용범위를 영역별 특성에 적합하게 확대 또는 축소할 수 있도록 상당한 재량권을 부여하는 경우도 많다.

[표3-1] 공공·민간 통합형 입법주의

국가	법률
영국	정보보호법 (Data Protection Act, 1998)
프랑스	정보처리파일및자유에관한법률 (Loi 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux livertes, 1978)
독일	연방정보호보법 (Bundesdatenschutsgesetz, 1974)
스웨덴	개인정보법 (Personal Data Act, 1998)
스페인	개인정보보호기본법 (Organic Law on the Protection of Personal Data, 1999)
네덜란드	개인정보보호법 (Personal Data Protection Act, 1999)
오스트리아	연방개인정보보호법 (Datenschutzgesetz, 1978)
벨기에	개인정보처리에관한프라이버시보호법 (Law of December 8, 1992 on Privacy Protection in Relation to the Processing of Personal Data, 1992)
덴마크	개인정보처리에관한법 (The Act on Processing of Personal Data, 2000)
핀란드	개인정보법 (Personal Data Act, 1999)
그리스	개인정보처리에서의개인의보호에관한법 (Law on the Protection of Individuals with Regard to the Processing of Personal Data, 1997)
아일랜드	정보보호법 (Data Protection Act, 1988)
이탈리아	개인정보처리에서의개인및기타주체의보호에관한법 (Law on the Protection of Individuals and Other Subject with Regard to the Processing of Personal Data, 1996)
룩셈부르크	개인정보처리에서의개인의보호에관한법 (Law of 2 August 2002

	on the Protection of Persons with Regard to the Processing of Personal Data, 2002)
포르투갈	개인정보보호법 (Act on the Protection of Personal Data, 1998)
노르웨이	개인정보법 (Personal Data Act, 2000)
아이슬란드	개인정보처리및보호에관한법 (Act on the Pretection and Processing of Personal Data, 2000)
스위스	연방정보보호법 (Federal Act on Data Protection, 1992)
호주	프라이버시법 (Privacy Act, 1998)
뉴질랜드	프라이버시법 (Privacy Act, 1993)
홍콩	개인정보법 (Personal Data(Privacy) Ordinance, 1996)
일본	개인정보보호에관한법률 (2003)

이처럼 유럽을 비롯하여 많은 국가들이 통합형 입법주의 형식의 개인정보보호법을 가지고 있다. 그러나 통합형 입법주의를 취하고 있다고 하더라고 실제로는 국가별로 상당히 다양한 유형을 보이고 있다. 예를 들어 독일은 「연방정보보호법」이라는 개인정보보호기본법을 가지고 있지만, 동법은 공공영역과 민간영역을 구분하여 각기 다른 규정을 두고 있다. 또한 호주의 개인정보보호기본법인 「프라이버시법」도 공공과 민간에 적용되는 개인정보보호원칙을 달리 규정하고 있다.

2. 구분형 입법주의

통합형과는 달리 구분형 입법주의는 개인정보보호법의 적용을 받는 영역을 공공부문과 민간부문 또는 각 영역별로 구분하여 개별적으로 입법하는 방식이다. 이러한 구분형 입법주의를 취하고 있는 대표적인 국가는 캐

나다와 미국이다.

캐나다는 공공부문(「프라이버시법」, Privacy Act, 1980)과 민간부문(「개인정보보호및전자문서에관한법률」, Personal Information Protection and Electronic Document Act, 2000)에 적용되는 법률이 명확하게 구분되어 별도로 제정되어 있다. 반면 미국은 건강정보, 교육정보, 비디오감시, 신용정보, 금융정보, 전자통신분야, 공공분야 등 개개 영역별로 입법이 산재되어 있다.

한편 우리나라 개인정보보호법도 이러한 구분형 입법주의 형식을 취하고 있다고 할 수 있다. 특히 구분형 중에서도 캐나다와 같이 공공부문과 민간부분에서 각각 대표적인 기본법적 성격을 가진 형식이라기보다는 오히려 미국과 같이 개별입법을 가지고 있다고 보는 쪽에 더욱 가깝다. 「공공기관의개인정보보호에관한법률」과 「정보통신망이용촉진및정보보호등에관한법률」이 어느 정도 공공부문과 민간부분에서 기본법적인 역할을 하고 있기는 하지만[49], 양자 모두 적용범위에 있어서는 다소 한계가 있기 때문이다. 「공공기관의개인정보보호에관한법률」은 적용범위가 컴퓨터에 의해 전산처리되는 개인정보에 한정되고 있으며, 민간분야의 「정보통신망이용촉진및정보보호등에관한법률」도 원칙적으로 정보통신망을 통해 영리목적으로 개인정보를 처리하는 사업자에게만 적용된다는 점에서 그 규제대상이 한정적이기 때문에 각 분야를 대표하는 기본법적인 성격을 가지고 있다고 보기 어렵다.

---

49) 물론 공공기관 등은 행정업무 등을 함에 있어 대부분의 개인정보를 컴퓨터에 의해 전산처리하고 있기 때문에 사실상 그 적용범위가 포괄적이라고 볼 수 있고, 민간부문에서도 정보보호법 제53조가 일부 개인정보를 많이 수집하고 이용하는 오프라인사업자에게도 적용하고 있다는 점에서 각각 공공부문과 민간부문의 기본법적 역할을 하고 있다고도 볼 수 있다.

Ⅱ. 개인정보보호기구

개인정보보호를 위한 각국의 노력은 실체법적 측면에서 개인정보 관련 법령을 정비하는 것에 그치지는 않고, 많은 국가들이 이러한 개인정보 관련 법령이 제대로 정립되고 이행될 수 있도록 제도적인 측면에서 개인정보보호기구를 설치하여 운영하고 있다. 특히 영국, 프랑스, 캐나다, 호주 등과 같은 국가들은 개인정보보호 전담기구를 통해 보다 효과적으로 개인정보보호 기능을 수행하고 있다. 이러한 개인정보보호 전담기구는 정보주체의 법적 권익을 보고하고 불법적인 개인정보침해행위를 보다 효과적으로 방지하여 올바른 정보처리관행을 확립하는 데 기여할 수 있다는 점에서 세계적인 추세가 되고 있다. 그러나 각국의 개인정보보호기구는 기능, 역할, 소속, 유형 등의 측면에서 그 나라의 법적 환경이나 사회·경제적 특성, 정보화 발달여부 등에 따라 각기 다른 모습을 보이고 있는 것 또한 사실이다. 예를 들어 미국은 별도의 전담기구를 설치하지 않고 독립규제기관인 '연방거래위원회(FTC)'가 소비자 프라이버시 및 개인정보보호의 역할도 함께 담당하고 있다.

각국의 개인정보보호기관이 어떠한 형태로 구성·운영되고 있는지를 구분해보면,[50] 크게 법원형태의 '사법기구형'과 '전문적인 독립기구형', '행정부 지원형', '행정부 소속형', '민간단체형'의 5가지로 나누어 볼 수 있다. 이 중 그 성격이 다른 사법기구형과 민간단체형을 제외한 전문독립기구형, 행정부 지원형, 행정부 소속형을 구분하는 중요한 요소는 기관장의 임명권자, 위원회의 경우 위원의 자격 및 임명·위촉권자, 사무국의 자체운영여부, 업무활동을 보고하는 기관이 누구인지 여부, 명시적인 법률상의

50) 이와 같은 형태에 따른 비교 외에도 개인정보보호기구의 기능 및 권한에 따른 비교도 가능하다. (개인정보분쟁조정위원회, 전게서, 283면 이하 참조.)

소속 규정 등이다. 물론 각각의 유형을 선을 긋듯이 명확하게 구분한다는 것은 사실상 불가능하며 국가별로 다양한 형태의 기구들이 있어 한 유형에 꼭 들어맞는다고 보기도 어렵지만, 위에서 본 중요요소들을 중심으로 그 행정체계를 구분해보는 것도 의미 있을 것이다.

1. 사법기구형

사법기구형은 고도의 독립성이 유지되는 사법기구인 법원이 다른 개인정보보호기구와 연계하여 개인정보침해 및 법위반에 관한 사건을 처리하는 형태의 기관이다. 법원은 모든 국가에서 개인정보피해구제의 역할을 담당하는 대표적인 사후적 피해구제기관이다. 그럼에도 불구하고 사법기구형을 별도로 구분한 것은 일반 민사·형사·행정 법원을 통해서가 아니라 별도로 개인정보와 관련된 사건을 처리하는 특별법원의 한 형태로 운영되는 경우가 있기 때문이다. 즉 이러한 사법기구형 개인정보보호기구는 법원의 일종이나 개인정보 또는 인권, 프라이버시 등에 관한 사건을 개인정보(프라이버시) 보호기관으로부터 직접 이관 받아 심사하고 처리한다는 점에서 특색이 있다. 여기에는 개인정보와 정보고개 등의 사안을 심사하는 영국의 '정보법원(Information Tribunal)'과 개인정보 또는 프라이버시 침해를 포함하여 제반인권문제에 대하여 모두 심사하는 '인권법원(Human Right Review Tribunal)'이 이에 해당된다.

2. 전문독립기구형

세계 각국의 개인정보보호기구가 참여하는 '국제정보보호기구회의(The International Conference of Data Protection Commissioners)'에서는 '효

율적인 개인정보보호의 역할을 담당하고 있는 개인정보보호기구'를 승인하고 있는데, 그 승인 요건 중 하나가 바로 '독립성'과 '자율성'이다.[51] 전문독립기구형 개인정보보호기구는 바로 이러한 독립성과 자율성, 그리고 전문성을 담보할 수 있다는 점에서 그 의의가 있다. 즉 앞서 살펴본 바와 같이 전문독립기구형 개인정보보호기구는 ① 한 국가 내에서 개인정보보호에 관한 모든 전반적인 업무를 처리한다는 점에서 전문성을 갖추고 있으며, ② 개별 행정부처가 아닌 국왕, 대통령, 수상, 의회 등에 소속된 기구로서 의회가 수상에게 기관의 업무결과나 실적과 같은 제반사항을 직접 보고한다는 점에서 독립성을 확보하고 있다. 또한 ③ 업무를 수행하는 사무국의 운영을 자체적으로 하고 있기 때문에 일반 행정기관의 간섭을 배제하고 독자적으로 활동해나갈 수 있다는 점에서 자율성을 갖추고 있다.

전문독립기구형은 다시 '합의제형', '독임제형', '별도기구형'의 3가지 유형으로 나누어 볼 수 있다. 먼저 합의제형은 위원회 형태의 전문·독립기구로서 대표적인 예는 프랑스의 '정보자유위원회(CNIL)'이다. 정보자유위원회는 입법부, 사법부, 행정부 등에서 선출된 위원들로 구성된다는 점에서 각각의 위원들은 직무수행에 있어 독립성과 자율성을 보장받고 있다.[52] 특히 정보자유위원회는 3권 중 어느 권력에도 속하지 않으며 기관장인 위원장도 대통령이나 의회 등에서 임명하는 것이 아니라 위원 중에서 호선한다는 점에서 다른 어떠한 형태의 기구들보다도 높은 독립성을 가졌다고 볼 수 있다.

---

51) 2001년 파리에서 개최된 정보보호기관회의에서는 법적 근거, 자율성과 독립성, 다양한 국제협약이나 가이드라인의 준수 등을 개인정보보호기관의 승인기준으로 삼고 있다. (Blair Stewart, *International Accreditation of Privacy and data Protection Authorities*, APEC Data Privacy Workshop, 2003.)

52) 「정보처리파일및자유에관한법률」 제13조에 의하면, 정보자유위원회는 권한의 행사에 있어 다른 어떠한 기관의 지시·감독도 받지 않는 고도의 독립성을 가진다.

한편 전문·독립기구형의 대표적인 형태는 독임제형이다. 이는 1人의 커미셔너(Commissioner)가 개인정보보호를 책임질 단독기구로 임명되고 이를 지원하는 사무국이 운영되는 형태이다. 현재 영국, 캐나다, 호주, 뉴질랜드, 홍콩에서 이와 같은 형태의 개인정보보호기구를 운영하고 있는데, 커미셔너는 주로 국왕이나 대통령 등 최고통수권자에 의해 임명되며 개인정보보호법에서 규정한 역할과 기능을 수행할 수 있도록 폭넓은 권한을 부여받고 있다. 커미셔너는 개인정보 처리행위의 감독과 실행규약과 같은 각종 지침의 제정, 상담 및 피해구제 등 개인정보보호를 위한 업무를 전담하여 수행하고 있기 때문에 대표적인 전문독립기구로 볼 수 있다. 그러나 독임제형의 경우도 대부분 커미셔너의 전문성을 보강하는 한편 커미셔너의 독주를 견제하기 위해 일반적으로 각종 자문위원회, 전문위원회 등이 설치·운영되고 있다.

이 밖에도 커미셔너나 위원회 형태가 아닌 별도의 독립기관이 개인정보보호를 위한 전담 역할을 맡는 예가 있다. 대표적으로 스페인의 '개인정보보호원(Agencia de Proteccion de Datos)'이 이에 해당된다. 개인정보보호원의 기관장은 국왕에 의해 개인정보보호자문위원회(Consulative Council) 구성원 중에서 임명되는데, 자문위원회는 입법부와 행정부, 학계, 소비자·사업자 단체 대표들로 구성된다. 스페인의 「개인정보보호기본법(Orsanic Law 15/1999 of 13 December on the Protection of Persona Data)」 제36조에 의하면 개인정보보호원은 독립적이고 객관적으로 직무를 수행하며 다른 어떠한 기관의 지시도 받지 않는다. 단 기관의 실적이나 상황에 대해서는 직접 의회에 보고하여야 한다.

3. 행정부 지원형

많은 국가들이 개인정보보호와 관련된 업무를 전문적으로 행하는 법정기구를 운영하고 있지만 사실 이러한 개인정보보호기구는 법률에서 규정한 역할과 임무를 원활히 수행하기 위한 예산이나 인력 면에서 행정부의 지원을 받는 경우가 많다. 즉 행정부 지원형은 전문·독립기구형과 비교해 볼 때, 기관장의 임명권자나 구성원의 지워, 기능, 역할, 권한 등의 측면에서 그리 큰 차이는 없지만 사무국의 운영을 행정부로부터 지원받고 있다는 점에서 양자의 차이가 있다고 하겠다. 행정부 지원형도 역시 '합의체형', '독임제형(옴브즈만형)', '별도기구형'으로 나눠 볼 수 있다.

먼저, 합의제형에는 대표적으로 오스트리아의 '정보보호위원회'와 '정보보호자문위원회(Data Protection Council)'를 들 수 있다. 정보보호위원회의 위원은 사법부와 행정부, 지방자치단체, 정당대표 등으로 각각 구성되고 있고, 연방정부의 제청을 받아 연방수상이 후보자 중 선정하여 연방대통령이 직접 임명한다. 또한 자문위원회의 위원들도 정당대표, 연방정부 대표, 지방정부 대표 등으로 구성되며 각각의 소속기관으로부터 직접 임명되기 때문에 기관장의 임명이나 위원회의 구성인원의 자격 면에 있어서 높은 독립성을 가지고 있다. 다만 정보보호위원회와 자문위원회는 합의제형태의 기구이기 때문에 별도의 사무국이 운영되고 있는데, 이 사무국은 연방수상관청 소속이며 연방정부로부터 예산을 지원받고 있다.[53] 또한 정보보호위원회는 연방정부에 대하여 연 2회 업무활동을 보고하여야 한다.

또한 네덜란드의 '정보보호위원회(College Bescherming Persoonsgege

53) 프랑스의 CNIL과 오스트리아의 정보보호위원회 및 정보보호자문위원회는 모두 합의제형의 개인정보보호기구라는 점에서는 유사하나, 위원회의 활동을 지원하고 실질적으로 업무를 수행하고 있는 사무국이 연방수상관청 소속이라는 점에서 프랑스의 그것과는 다소 구분된다.

vens)'와 핀란드의 '정보보호위원회(Data Protection Board)'도 이와 유사한 형태이다. 네덜란드의 경우 위원장과 위원은 법무부장관의 제청으로 국왕이 임명하며 특히 위원장은 법관의 자격을 갖춘 자 중에서 임명되나, 사무국의 직원과 자문이사회의 구성원은 위원장의 제청으로 법무부가 임명하고 있다. 핀란드의 정보보호위원회 역시 개인정보처리의 허가 및 기타 중대한 사안을 심의하여 결정하는 기구로서 국무회의에서 위원을 임명하고 있으나, 위원회는 별도 사무국을 운영하지 않으며 법무부로부터 바로 행정적 지원을 받고 있다.

한편 핀란드는 독임제형 개인정보보호기구로서 '정보보호옴브즈만(The Data Protection Ombudsman)'을 설치하고 있다. 핀란드에서는 전통적으로 다양한 분야에서 옴브즈만 제도가 발달한 영향으로 개인정보와 관련하여서도 조사·감독 등 다양한 기능을 수행하고 있는 옴브즈만이 활동하고 있는 것이다. 옴브즈만은 독립적인 임무를 수행할 수 있는 개인이 임명된다는 점에서 커미셔너와 유사하나, 핀란드의 개인정보 옴브즈만은 법무부에서 옴브즈만의 활동을 지원하는 사무국 인력과 예산을 지원하고 있다는 점에서 차이가 있다.[54]

이외에도 행정부로부터 지원을 받고 있는 별도기구형의 개인정보보호기구가 있다. 대표적인 예가 독일의 '연방정보보호청'이다. 연방정보보호청의 기관장은 연방정부의 제청을 받아 의회가 선출한 자를 대통령이 임명

54) 핀란드의 정보보호옴브즈만은 1988년 설립된 기구로 5년 임기로 국무회의(Council of State)에 의해 임명되어 활동하고 있는 개인정보보호기구이다. 옴브즈만의 주요기능은 정보처리자와 정보주체에게 상담이나 안내를 통해 정보를 제공하고, 정보처리자가 자발적인 실행규약을 제정할 수 있도록 자문을 해주거나 동 규약을 심사해주는 것이다. 또한 정보주체의 요청이 있을 경우 정보처리자가 올바르게 법규를 준수하였는지, 정보주체의 권리를 침해하지 않았는지를 심사하여 결정한다. 정보처리실태에 관하여 조사하고 감독하는 것도 역시 옴브즈만의 주된 기능 중 하나이다. (개인정보분쟁조정위원회, 전게서, 259 이하 참조.)

하나, 연방내무부로부터 인력과 예산을 지원받으며 연방정부와 의회에 업무활동을 보고하도록 되어 있다.

4. 행정부 소속형

행정부로부터 독립된 형태의 개인정보보호기구와는 달리 행정기관이나 행정부 내 설치된 부속기관이 개인정보보호의 역할을 담당하는 경우도 있는데, 이는 행정부 소속형 개인정보보호기구로 분류할 수 있다. 여기에는 '엄격한 의미의 행정부 소속형'과 '다소 포괄적인 의미의 행정부 소속형'이 있다. 전자에는 개인정보보호기구가 개별 정부부터의 내청 또는 외청이나 그 산하기관으로 되어 있는 경우이고, 후자는 행정부에 의해 설립되고 운영지원을 받는 개인정보보호기구와 기관장을 각 정부부처가 임명 또는 위촉하는 경우를 포함한다.[55]

행정부에 의해 설립되고 예산을 지원받으며 행정부처와 여러 가지 운영상 관계를 유지하고 있는 형태의 행정부 소속형 기구로 합의제 형태로 운영되고 있는 예는 아이슬란드의 '정보보호위원회'이다. 아이슬란드의 정보보호위원회는 법무부가 위원 및 사무국장을 임명 또는 위촉하여 설치된다.[56] 이러한 합의제형 개인정보보호기구는 법률로서 기구의 설치 및 구성이 보장되며 법률가나 교수 등이 각계 전문가로 구성된다는 점에서 개별 정부부처나 그 산하기관보다는 독립성과 전문성이 높은 편이라고 할 수 있다. 그러나 개별 행정부처의 행정적 지원을 받을 뿐 아니라 위원회

55) 오늘날 개인정보보호기구들은 직무수행에 있어 독립성과 자율성이 요구되는 경우가 많기 때문에 대부분 법정기구에 해당되며, 명시적으로 어느 행정부처 소속으로 법률상 규정되어 있는 경우는 거의 없다. 따라서 법률상으로는 개인정보보호기구를 행정부 소속형으로 보기 어려운 경우가 많다.

56) 아이슬란드의 정보보호위원회는 총 5인으로 구성되는 이사회 형태로 운영되며, 이사회의 의장과 부의장은 대법원과 아이슬란드 정보처리협의회에서 각각 추천한 자를 법무부가 임명한다.

의 구성과 설립도 행정부처에 의해 이루어진다는 점에서, 각 삼권에서 위원이 선출되는 프랑스의 정보자유위원회 및 국왕이나 국무회의에서 위원이 임명되는 네덜란드나 핀란드의 '정보보호위원회'와는 차이가 있다. 우리나라의 '개인정보분쟁조정위원회'도 아이슬란드와 유사한 형태의 개인정보보호기구로 볼 수 있다. 「정보통신망이용촉진및정보보호등에관한법률」[57]에 의해서 설립된 법정기구이고 법조계와 학계, 시민단체 등의 전문가가 위원으로 활동하고 있기 때문에 그 독립성과 자율성이 보장되기는 하나, 행정안전부 장관에 의해 분쟁조정위원이 위촉 또는 임명된다는 점과 행정안전부 산하기관인 '한국정보보호진흥원' 내에 사무국을 두어 그 운영상 필요한 인력과 예산을 지원받고 있다는 점에서 행정부 소속형 합의제 기구로 볼 수 있을 것이다.

이러한 합의제형이 아닌 일반 행정기관 또는 그 소속기관이 개인정보보호의 역할을 맡는 경우가 있다. 대표적인 예가 바로 일본의 경우이다.

---

57) 제33조(개인정보분쟁조정위원회의 설치 및 구성)
① 개인정보에 관한 분쟁을 조정하기 위하여 개인정보분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.
② 분쟁조정위원회는 위원장 1명을 포함한 15명 이내의 위원으로 구성하며, 그중 1명은 상임으로 한다.
③ 위원은 다음 각 호의 어느 하나에 해당하는 자 중에서 대통령령으로 정하는 바에 따라 행정안전부장관이 임명하거나 위촉한다. 이 경우 다음 각 호의 어느 하나에 해당하는 자가 1명 이상 포함되어야 한다.
1. 대학이나 공인된 연구기관에서 부교수급 이상 또는 이에 상당하는 직에 있거나 있었던 자로서 개인정보보호 관련 분야를 전공한 자
2. 4급 이상 공무원(고위공무원단에 속하는 일반직공무원을 포함한다) 또는 이에 상당하는 공공기관의 직에 있거나 있었던 자로서 개인정보보호 업무에 관한 경험이 있는 자
3. 판사·검사 또는 변호사의 자격이 있는 자
4. 정보통신서비스 이용자단체의 임원직에 있거나 있었던 자
5. 정보통신서비스 제공자 또는 정보통신서비스 제공자단체의 임원직에 있거나 있었던 자
6. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체에서 추천한 자
④ 위원의 임기는 3년으로 하고, 연임할 수 있다.
⑤ 위원장은 위원 중에서 행정안전부장관이 임명한다.
⑥ 분쟁조정위원회의 업무를 지원하기 위하여 제52조에 따른 한국정보보호진흥원(이하 제46조의2, 제47조, 제48조의2, 제48조의3 및 제49조의2에서 "보호진흥원"이라 한다)에 사무국을 둔다.

일본은 별도의 개인정보보호기구를 두지 않고 각 주무 행정부처에서 개별적으로 개인정보보호의 업무를 처리하고 있다. 우리나라의 경우도 '개인정보분쟁조정위원회'가 설립되어 개인정보피해구제의 측면에서 활발히 운영되고 있다는 점을 제외하고는 기본적으로 일본과 유사하다. 즉 행정안정부, 방송통신위원회, 지식경제부, 교육과학기술부 등 각 주무부처가 해당 영역의 개인정보에 관련된 법률 규정을 마련하고 집행할 책임과 권한을 가지고 있다. 그러나 엄밀히 말해서 이런 형태의 정부부처는 본래적 의미의 개인정보보호기구라고는 볼 수 없다.

또한 스웨덴, 덴마크, 그리스, 노르웨이와 같은 유럽 일부 국가의 경우도 행정부처에 소속된 행정기관이 개인정보보호기구로서 활동하고 있다. 스웨덴의 '정보조사원'은 중요사안을 결정하는 이사회의 구성원이 사무국장을 제외하고는 모두 현직 국회의원이라는 점에서 독립성을 가지나, 이사회의 활동을 지원하는 사무국은 재정부(Ministry of Finance)로부터 인력과 예산을 지원받으며 매년 정부에 보고를 할 뿐 아니라 사무국장과 이사회의 구성원은 모두 재정부가 임명 또는 위촉하고 있다. 덴마크의 '정보보호원(Datatilsynet)'도 정보이사회와 사무국으로 구성되어 운영되고 있는데, 운영을 위한 예산 지원과 관련하여서는 법무부의 지원을 받으며, 정보보호원장과 이사회의 구성원은 법무부장관에 의해 임명 또는 위촉된다.[58] 또한 노르웨이의 '정보보호원(Datatilsynet)'의 기관장은 국왕이 임명하나 노동내무부(Ministry of Labour and Government Administration) 소속기관으로 설치되어 운영되고 있으며, 그리스 '정보보호원(Hellenic Data Protection Authority)'의 기관장은 현직 법관 또는 법관에 준하는 자로서 내각의 제청을 받아 대통령이 임명하나 동 기관은 법무부에 소속되어 있

58) 사무국은 주로 일상적인 업무를 하며, 이사회는 공공·민간기구에 중대한 영향을 끼칠 수 있는 사건을 처리한다.

다.

지금까지 살펴본 기구들은 모두 행정부처 또는 그 소속기관이라는 점에서 행정부 소속형 기구라고 부를 수 있다. 그러나 엄격한 의미에서 유럽의 기구와 일본 및 우리나라의 경우는 다소 차이가 있다. 일본과 우리나라의 경우 각 행정부처가 소관 관할업무 내에서만 개인정보보호의 기능을 수행하나, 스웨덴 등 유럽의 기구들은 비록 특정 부처 소속하에 있기는 하지만 모든 영역에 걸쳐 개인정보보호 전담기구로서의 기능을 수행한다.

5. 민간단체형

민간단체형은 국가가 아닌 일반 비영리 민간단체에서 개인정보보호의 역할을 담당하는 경우이다. 따라서 성격상 다른 유형의 기구들과는 차이가 있으나, 미국이나 일본에서는 이러한 민간단체형의 개인정보보호기구들이 중요한 역할을 담당하고 있다. 이러한 민간단체형의 개인정보보호기구들은 특히 민간 영역에서 사업자들의 자율규제 차원에서 활동하고 있는 경우가 많으며, 미국의 'BBBOnLine'과 같은 프라이버시보호단체 및 일본의 '인정개인정보보호단체'가 여기에 해당된다.

제3절 우리나라 개인정보보호제도

우리나라는 20여년 전부터 새로운 국가발전 동력으로 정보화를 선택하여 세계의 IT 혁명에 능동적으로 대처하기 위한 노력을 꾸준히 펼쳐 왔다. 그 결과 오늘날 전 세계로부터 정보통신 선도국가라는 평가를 받고

있다. 초고속 정보통신망이 2008년 9월 기준으로 이미 2,100만 가구에 보급되어 인구의 75%가 넘는 3,520만명이 인터넷을 이용하고 있을 뿐 아니라, 이동통신 가입자 역시 4,100만명을 넘어서는 등 세계 어디에서도 찾아볼 수 없는 정보통신 환경을 구축하였다.[59] 또한 우리나라의 IT 산업은 한국경제의 핵심 축을 정보통신기반산업으로 이동시켜 경제구조에 근본적인 변화를 가져오기도 하였다.

그러나 이러한 정보화의 진전과 발달로 인한 우리 삶의 변화는 항상 긍정적인 면만 있는 것은 아니었다. 우리나라에서는 특히 고도화된 정보통신망을 이용하는 사람들이 증가하면서 개인프라이버시의 침해 문제도 함께 대두되기 시작하였고, 이에 개인정보보호에 대한 국민적 관심도 높아지고 있다. 이러한 경향은 개인정보보호에 대한 법체계의 정립과 개인정보보호기구의 설립에 대한 관심과 논의로 이어지고 있다.

Ⅰ. 우리나라 개인정보보호법

우리 헌법 제10조는 “모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적인 인권을 확인하고 이를 보장할 의무를 진다”고 하고, 헌법 제17조는 “모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다”고 규정하여, 개인의 사생활의 비밀과 자유의 불가침성을 선언하고 있다.

하지만 우리나라는 이러한 헌법원칙을 구현하기 위한 일반적인 개인정보보호법이 제정되어 있지는 않고 각 영역별로 개개 법률규정이 있는데,

59) 방송통신위원회, 「정보통신백서」, 2008, 1면.

개인정보와 관련한 대표적인 법률로는 「공공기관의개인정보보호에관한법률」, 「정보통신망이용촉진및정보보호등에관한법률」, 「신용정보의이용및보호에관한법률」 등이 있다. 이외 「통신비밀보호법」[60]은 도·감청 금지 및 개인의 통신비밀의 자유 보장에 관한 내용을, 「형법」은 개인의 비밀침해금지 및 업무상 취득한 비밀의 누설금지 규정을, 「의료법」은 의사·간호사·조무사 등이 의료행위 과정에서 취득한 환자의 비밀을 누설하는 것을 금지하는 내용을 각각 규정하고 있다.

[표3-2] 우리나라 개인정보관련 입법 현황

구분	법률	
공공부문	• 공공기관의개인정보보호에관한법률(1994) • 전자정부구현을위한행정업무등의전자화촉진에관한법률(2001) • 주민등록법(1962) • 국가공무원법(1949) • 공직자윤리법(1981) • 민원사무처리에관한법률(1997)	
민간부문	정보통신분야	• 정보통신망이용촉진및정보보호등에관한법률(1999) • 정보화촉진기본법(1999) • 전기통신사업법(1961) • 정보통신기반보호법(2001) • 통신비밀보호법(1993)
	상거래분야	• 전자거래기본법(1999) • 전자서명법(1999) • 전자상거래등에서의소비자보호에관한법률(2002)
	금융·신용분야	• 신용정보의이용및보호에관한법률(1995) • 금융실명거래및비밀보장에관한법률(1997) • 증권거래법(1962) • 증권투자신탁업법(1969)
	의료분야	• 의료법(1962) • 약사법(1953) • 국민건강보험법(1999)

60) 1993. 12. 27. 제정 (법률 제4650호), 2008.2.29 제14차 개정 (법률 제8867호)

기타	• 형법 제127조, 제316조제2항, 제317조 • 공증인법(1961) • 변호사법(1949) • 법무사법(1990)

이렇듯 우리나라는 다양한 개인정보 관련 규정이 여러 법률에 산재되어 있다. 이 중 「공공기관의개인정보보호에관한법률」은 공공부문에서의 개인정보 처리절차 및 그 과정에서 준수하여야 할 사항 등을 규정하고 있고, 「정보통신망이용촉진및정보보호등에관한법률」은 정보통신사업자 및 일부 오프라인 사업자가 개인정보를 처리할 때 고객의 개인정보를 어떻게 관리하고 보호하여야 하는지를 규정하고 있는 바, 각각 공공부문과 민간부문을 대표하는 개인정보보호법이라 할 수 있을 것이다.

1. 공공기관의개인정보보호에관한법률[61]

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

61) 1994. 1. 7. 제정 (법률 제4734호), 2008. 2. 29. 제5차 개정 (법률 제8871호)

작용을 효과적으로 예방하고 대처하는 데 한계가 있었다.[62]

이에 「공공기관의개인정보보호에관한법률」은 전통적으로 개인정보 보호요청의 대상이 되었던 공공기관에서의 개인정보보호를 규정함으로써 공공기관의 업무수행 중 발생할 수 있는 개인정보 누출 피해를 방지하고자 제정되었다.[63] 비록 조항의 수는 타법에 비해 상대적으로 적지만, 공공기관의 업무 중 개인정보 보호업무에 특화된 법규정을 가지는 것이 가장 큰 특징이라 할 수 있다. 따라서 동법은 법률 전반에 걸쳐서 개인정보의 수집 및 취급에 대하여 포괄적인 규정을 하고 있으며, 특히 제3차 개정시(2007년 5월 17일 일부개정) 공공기관이 준수해야할 개인정보보호원칙[64]을 추가하여 공공기관의 개인정보 보호의무를 더욱 강화하고 있다.

2. 정보통신망이용촉진및정보보호등에관한법률[65]

민간부문에서 개인정보침해 문제가 심각하게 대두된 이유는 역시 정보통신망을 통한 개인정보의 수집・이용・처리 행위가 증가되었기 때문이다. 이에 1999년 「정보통신망이용촉진및정보보호등에관한법률」이 시행

62) 행정자치부, 「공공기관의 개인정보보호제도 이해와 해설」, 2003. 5면 이하.

63) 제1조(목적) 이 법은 공공기관의 컴퓨터·폐쇄회로 텔레비전 등 정보의 처리 또는 송·수신 기능을 가진 장치에 의하여 처리되는 개인정보의 보호를 위하여 그 취급에 관하여 필요한 사항을 정함으로써 공공업무의 적정한 수행을 도모함과 아울러 국민의 권리와 이익을 보호함을 목적으로 한다.

64) 제3조의2(개인정보보호의 원칙)
① 공공기관의 장은 개인정보를 수집하는 경우 그 목적을 명확히 하여야 하고, 목적에 필요한 최소한의 범위 안에서 적법하고 정당하게 수집하여야 하며, 목적 외의 용도로 활용하여서는 아니 된다.
② 공공기관의 장은 처리정보의 정확성 및 최신성을 보장하고, 그 보호의 안전성을 확보하여야 한다.
③ 공공기관의 장은 개인정보관리의 책임관계를 명확히 하여야 한다.
④ 공공기관의 장은 개인정보의 수집·활용 등 개인정보의 취급에 관한 사항을 공개하여야 하며, 개인정보처리에 있어서 처리정보의 열람청구권 등 정보주체의 권리를 보장하여야 한다.

65) 1986. 5. 12. 제정 (법률 제3848호), 2008. 6. 13. 제26차 개정 (법률 제9119호)

되었다. 동법은 본래 1986년 제정된 「전산망보급확장과이용촉진에관한법률」의 전문을 개정, 개인정보보호 부분을 추가한 것이다. 법령명과 입법연혁을 통해서도 알 수 있듯이 동법은 정보통신망의 이용촉진과 개인정보의 보호라는 2가지 목적을 함께 담고 있다.[66]

「정보통신망이용촉진및정보보호등에관한법률」은 이러한 목적을 바탕으로 하여 제정되었기 때문에, 주로 민간영역에서의 정보통신망을 통한 개인정보의 수집・이용・제공 등의 행위를 규율하고 있다. 그러나 동법은 정보통신망에 한하지 않고 일부 오프라인 사업자에 의한 개인정보 처리도 함께 규율함으로써 민간부문을 대표하는 개인정보보호법의 역할을 담당하고 있다. 또한 동법은 개인정보보호에 대한 국제규범 및 국제표준이라 할 수 있는 OECD 프라이버시 8원칙을 충실히 반영하고 있다.[67]

동법은 그 주요내용으로 정보통신사업자 뿐만 아니라, 그 대리점이 개인정보를 유출하는 행위에 대해서도 규제하도록 하고(제71조), 개인정보를 매매하는 행위에 대하여 형사 처벌하는 외에 과징금을 부과하도록 하여 개인정보취급자의 책임을 강화하고(제64조의3) 이들이 개인정보를 외부에 유출하는 경우에는 가중 처벌하도록 규정하고 있다(제75조).

또한 합병 또는 영업양수 등으로 개인정보가 합병회사 등에 이전되는 경우에 당사자에게 그 사실을 알리도록 의무화하고, 개인정보침해로 인한 분쟁을 신속・간편하게 해결하기 위해 '개인정보분쟁조정위원회'를 법정기구화하여 동위원회의 조정결과에 민법상 화해와 같은 효력을 부여하도록

66) 제1조(목적) 이 법은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

67) 동법 제4장 '개인정보의 보호', 제22조부터 제40조까지에서 규율하고 있다.

규정하고 있다.[68]

그리고 국가 간 개인정보 유통과 관련해서는 동법 제8장 제62조에서 “정부는 개인정보의 국가 간 이전 및 개인정보보호에 관련된 업무 등을 추진함에 있어 다른 국가 또는 국제기구와 상호협력하여야 한다”고 규정하고 있다[69]. 또한 제54조에 “정보통신서비스제공자는 이용자의 개인정보에 관한 동법의 규정을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니된다”고 규정하고 있다.[70] 이는 국가 간 개인정보 유통과 관련한 국제 협력 및 국제 계약의 제한 규정을 둠으로써 최소한의 법적 규제의 필요성을 인정하였다는 측면에서는 그 의미가 있다 할 것이다.

---

68) 제38조(조정의 효력) ① 분쟁조정위원회는 제36조제2항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.
② 제1항에 따라 조정안을 제시받은 당사자는 제시받은 날부터 15일 이내에 조정안의 수락 여부를 분쟁조정위원회에 통보하여야 한다.
③ 당사자가 조정안을 수락하면 분쟁조정위원회는 즉시 조정서를 작성하여야 하며, 위원장 및 각 당사자는 그 조정서에 기명날인하여야 한다.
④ 당사자가 제3항에 따라 조정안을 수락하고 조정서에 기명날인을 하면 당사자 간에 조정서와 같은 내용의 합의가 성립된 것으로 본다.

69) 제62조(국제협력) 정부는 다음 각 호의 사항을 추진할 때 다른 국가 또는 국제기구와 상호 협력하여야 한다.
1. 개인정보의 국가간 이전 및 개인정보의 보호에 관련된 업무
2. 정보통신망에서의 청소년 보호를 위한 업무
3. 정보통신망의 안전성을 침해하는 행위를 방지하기 위한 업무
4. 그 밖에 정보통신서비스의 건전하고 안전한 이용에 관한 업무

70) 제63조(국외 이전 개인정보의 보호)
① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하여서는 아니된다.
② 정보통신서비스 제공자등은 이용자의 개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다.
③ 정보통신서비스 제공자등은 제2항에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.
1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간
④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

3. 신용정보의이용및보호에관한법률[71]

「신용정보의이용및보호에관한법률」은 신용정보업의 건전한 육성과 신용정보의 오용·남용으로부터 프라이버시의 비밀을 보호하고자 제정된 법률이다.[72] 신용정보업의 경우 그 업무의 특성상 개인정보 취급이 필수 요건이므로 동법은 신용정보과 관련한 업무에 그 적용범위를 한정시켜, 신용정보업과 관련하여 발생할 수 있는 개인정보침해를 방지하고자 한다.

동법은 신용정보란 "금융거래 등 상거래에 있어서 거래 상대방의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보"로 규정하고, 개인신용정보란 "신용정보 중 개인의 신용도와 신용거래능력 등을 판단할 때 필요한 정보로서 대통령령으로 정하는 정보"로 정의하고 있다.[73]

---

71) 1995. 1. 5. 제정 (법률 제4866호), 2009. 4. 1. 제20차 개정 (법률 제9617호 시행일 2009. 10. 2.)

72) 제1조(목적) 이 법은 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 도모하며 신용정보의 오용·남용으로부터 사생활의 비밀 등을 적절히 보호함으로써 건전한 신용질서의 확립에 이바지함을 목적으로 한다.

73) 제2조(정의)

① 법 제2조제1호에서 "대통령령이 정하는 정보"라 함은 다음 각호의 1에 해당하는 정보를 말한다. 다만, 법 제2조제8호·제9호 및 제11호의 업무와 관련하여서는 다른 법령의 규정에 의하여 공시 또는 공개되거나 다른 법령에 위반됨이 없이 출판물·방송 등의 공공매체 등을 통하여 공시 또는 공개된 정보 등은 제외한다.

1. 개인의 성명·주소·주민등록번호(외국인의 경우 외국인등록번호 또는 여권번호)·성별·국적 및 직업등과 기업 및 법인의 상호·법인등록번호·사업자등록번호·본점 및 영업소의 소재지·설립연월일·목적 및 임원에 관한 사항 등 특정 신용정보주체를 식별할 수 있는 정보(제2호 내지 제6호의 1에 해당하는 정보와 결합되는 경우에 한한다)

2. 대출·보증·담보제공·가계당좌예금 또는 당좌예금·신용카드·할부금융·시설대여 등의 금융거래 등 상거래와 관련하여 신용정보주체의 거래내용을 판단할 수 있는 정보로서 총리령이 정하는 정보

3. 금융거래 등 상거래와 관련하여 발생한 연체·부도·대지급 또는 허위 기타 부정한 방법에 의한 신용질서 문란행위 등 신용정보주체(신용정보주체가 회사인 경우에는 다음 각목의 자를 포함한다)의 신용도를 판단할 수 있는 정보로서 총리령이 정하는 정보

가. 「국세기본법」 제39조제2항의 규정에 의한 과점주주로서 최다출자자인 자

나. 「국세기본법」 제39조제2항의 규정에 의한 과점주주인 동시에 당해 회사의 이사 또는 감사

아울러 제3장 ‘신용정보의 수집·조사 및 처리’ 및 제4장 ‘신용정보의 유통·이용 및 관리’를 통해 신용정보를 취급함에 있어서 필요한 사항을 규정하고 있다.

4. 전자거래기본법[74]

「전자거래기본법」은 우리나라 전자거래에 있어서의 기본법으로 전자거래에 관한 사항을 총괄적으로 규정[75]하고 있다. 물론 동법은 ‘전자거래’에 관한 사항을 중점적으로 관리하고 있으나, 제12조[76]에서 ‘개인정보보호’를 위한 정부와 전자거래사업자의 의무 및 준수사항을 규정함으로써 개인정보보호를 위한 포괄적인 규정을 마련하고 있다.

로서 당해 회사의 채무에 연대보증을 한 자
다. 당해 회사의 발행주식 총수 또는 지분총액의 100분의 30이상을 소유하고 있는 자로서 최다출자자인 자
라. 당해 회사의 무한책임사원
4. 금융거래등 상거래에 있어서 신용도등의 판단을 위하여 필요한 개인의 재산·채무·소득의 총액, 납세실적등과 기업 및 법인의 연혁·주식 또는 지분보유현황 등 회사의 개황, 판매내역·수주실적·경영상의 주요계약등 사업의 내용, 재무제표 등 재무에 관한 사항, 「주식회사의외부감사에관한법률」의 규정에 의한 감사인의 감사의견 및 납세실적 등 신용정보주체의 신용거래능력을 판단할 수 있는 정보
5. 금융거래등 상거래에 있어서 신용정보주체의 식별·신용도 및 신용거래능력을 판단할 수 있는 법원의 심판·결정정보, 조세 또는 공공요금 등의 체납정보, 주민등록 및 법인등록에 관한 정보 및 기타 공공기관이 보유하는 정보로서 총리령이 정하는 정보
6. 제2호 내지 제5호와 유사한 신용정보로서 총리령이 정하는 「정보금융투자업에관한법률」 제4조제3항에 따른 특수채증권·사채권 또는 기업어음증권으로서 다음 각 호의 금융기관이 인수[「자본시장과금융투자업에관한법률」 제9조제11항에 따른 인수(모집·사모·매출의 중개·주선 또는 대리업무를 포함한다)를 말한다]·매매중개 또는 매매하는 증권을 말한다.

74) 1999. 2. 8. 제정 (법률 제5834호), 2009. 3. 18. 제16차 개정 (법률 제9504호)

75) 제1조(목적) 이 법은 전자거래의 법률관계를 명확히 하고 전자거래의 안전성과 신뢰성을 확보하며 전자거래의 촉진을 위한 기반을 조성함으로써 국민경제의 발전에 이바지함을 목적으로 한다.

76) 제12조(개인정보보호)
① 정부는 전자거래의 안전성 및 신뢰성을 확보하기 위하여 전자거래이용자의 개인정보를 보호하기 위한 시책을 수립·시행하여야 한다.
② 전자거래사업자는 전자거래이용자의 개인정보를 수집·이용·제공 및 관리함에 있어서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등 관련 규정을 준수하여야 한다.

5. 전자서명법[77]

「전자서명법」은 전자문서와 관련한 전자서명에 있어서 공인인증에 대한 규율을 하기 위하여 제정[78]된 법이다. 동법은 공인인증을 위한 전자서명생성정보에 대한 보호[79] 및 공인인증기관의 개인정보 보호[80]의무를 규정하고 있다.

Ⅱ. 우리나라 개인정보보호기구

우리나라는 개인정보 관련 법률의 제정·시행과 함께 개인정보보호를 위한 환경을 조성하고 피해구제제도를 정착시킬 필요성이 꾸준히 제기되어 왔다. 특히 민간 사업자나 공공기관 등의 개인정보를 처리하는 자가 국내 개인정보 관련 법령의 규정에 맞게 개인정보를 처리하고 보호하고 있는지를 관리·감독하고, 정보주체가 부당한 개인정보 침해로 인하여 입

77) 1999. 2. 5. 제정 (법률 제5792호), 2008. 12. 26. 제6차 개정 (법률 제9208호)

78) 제1조(목적) 이 법은 전자문서의 안전성과 신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명에 관한 기본적인 사항을 정함으로써 국가사회의 정보화를 촉진하고 국민생활의 편익을 증진함을 목적으로 한다.

79) 제23조(전자서명생성정보의 보호 등)
① 누구든지 타인의 전자서명생성정보를 도용 또는 누설하여서는 아니된다.
② 누구든지 타인의 명의로 공인인증서를 발급받거나 발급받을 수 있도록 하여서는 아니된다.
③ 누구든지 공인인증서가 아닌 인증서 등을 공인인증서로 혼동하게 하거나 혼동할 우려가 있는 유사한 표시를 사용하거나 허위로 공인인증서의 사용을 표시하여서는 아니된다.
④ 누구든지 공인인증서를 이용범위 또는 용도에서 벗어나 부정하게 사용하여서는 아니된다.
⑤ 누구든지 행사하게 할 목적으로 다른 사람에게 공인인증서를 양도 또는 대여하거나 행사할 목적으로 다른 사람의 공인인증서를 양도 또는 대여 받아서는 아니된다.

80) 제24조(개인정보의 보호)
① 공인인증기관은 인증업무 수행과 관련하여 개인정보를 보호하여야 한다.
② 제1항의 개인정보보호에 관하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제22조 내지 제32조, 제36조제1항, 제54조, 제55조, 제62조, 제66조 및 제67조의 개인정보에 관한 규정을 준용한다. 이 경우 "정보통신서비스제공자"는 "공인인증기관"으로, "이용자"는 "가입자"로 본다.

은 피해를 구제받을 수 있도록 지원하는 개인정보보호기구의 설치는 그 핵심내용이라 할 수 있다. 그러나 국내에는 개인정보에 관한 종합적 기능을 담당하는 개인정보보호기구는 없다고 볼 수 있는 상태이다. 개인정보 관련 법규정이 산재해 있는 만큼, 개개 법령을 집행하고 관리·감독할 담당 행정부터 또는 동 법령에 의해 설립된 기구 등이 부분적으로 해당 분야의 개인정보보호 역할을 맡고 있을 뿐이다.

그러나 이러한 행정부처나 공공기관들을 모두 본래의 의미의 개인정보보호기구라고 확정짓기는 다소 어려움이 있다. 예를 들어, 「신용정보의이용및보호에관한법률」을 구체적으로 시행하고 신용정보 처리업자의 행위를 규율함으로써 일반 시민들의 개인신용정보를 보호하고 있는 역할을 하고 있는 것은 금융감독위원회(금융위원회)와 금융분쟁조정위원회이나 이들 기구의 주된 활동목적은 은행, 보험, 증권 등 금융 전반의 업무관행을 관리·감독하는 것이어서 개인정보보호는 그 중 극히 일부를 차지하고 있을 뿐이기 때문이다. 따라서 보다 정확한 의미에서 개인정보보호기구라고 함은 '법률에 의해 명시적으로 개인정보보호기구로 지정된 기관'만을 의미할 것이다. 이를 '협의의 개인정보보호기구'로 볼 수 있다. 그러나 우리나라의 현실은 이러한 협의의 개인정보보호기구가 개인정보와 관련한 모든 역할을 수행하는 것이 아니라 상당부분 다른 기구에 그 역할이 분산되어 있다는 것이다.

[표3-3] 우리나라 개인정보보호기구 현황

구분	기관명	관할범위
공공부문	개인정보보호심의위원회	공공기관이 보유하는 개인정보
	행정안전부	

	국민권익위원회	행정기관에 의한 민원사무처리로 인한 고충
민간부문	개인정보분쟁조정위원회	개인정보침해 일반
	한국정보보호진흥원	「정보통신망이용촉진및정보보호 등에관한법률」적용을 받는 자에 의한 개인정보 침해
	방송통신위원회	
	금융감독위원회	신용정보기관 등에 의한 신용정보처리 과정에서의 침해
	금융위원회	
	금융분쟁조정위원회	
	전자거래분쟁조정위원회	전자거래에서의 개인정보침해
	한국소비자원	소비자거래에서의 개임정보침해
	소비자분쟁조정위원회	
기타	국가인권위원회	인권침해 일반
	경찰청	처벌 대상이 되는 개인정보침해

제4절 국제기구 및 각국의 개인정보보호제도

개인정보보호의 문제가 국제적으로 논의되기 시작한 시기는 불과 20여 년전이다. 1970년대 선진국에서는 과학기술의 발달, 특히 컴퓨터의 보급과 개인정보의 자동처리기술의 발달이 개인의 프라이버시에 미치는 영향에 대한 관심과 우려가 증대하였고, 이에 대한 대처방안을 입법·정책적으로 모색하기 위한 활발한 논의가 이루어졌다. 실제로 이러한 논의는 자국 내에서 개인정보의 자동처리를 규율하기 위한 법제도를 확립하는 방향으로 진행되었다. 이와 같은 개인정보보호를 위한 개별 국가차원의 논의는 1980년대 들어 국제적 차원의 논의와 국제규범의 정립으로 이어졌다. 특히 경제협력개발기구(OECD)는 각국의 입법현환을 전문가그룹(Group of Experts)으로 하여금 조사·연구토록 하여, 그 결과를 바탕으로 1980년

「개인정보의 국경 간 이동과 프라이버시보호에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)」을 제정하였다.[81]

정보화 사회로의 급속한 진입으로 인해 개인정보보호에 대한 국제사회의 관심은 더욱 증대되었다. UN은 1970년대부터 개인정보와 프라이버시 영역에 관심을 가지고 활동하기 시작하여, 1990년 12월 14일 총회 결의로 「컴퓨터화된 개인정보파일의 규제를 위한 가이드라인(Guidelines for the Regulation of Computerized Personal Data Files)」을 채택한 바 있다. 또한 EU도 1995년 10월 24일 「개인정보의 보호 및 자유로운 이전에 관한 유럽의회와 이사회 지침(DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of such data)」을 마련한 데 이어, 1997년에는 「통신부문의 개인정보처리 및 프라이버시 보호에 관한 유럽의회와 이사회 지침(DIRECTIVE 97/66/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector)」으로 대체하였다.[82]

Ⅰ. 국제기구의 개인정보보호제도

1. OECD 프라이버시 가이드라인

81) 개인정보분쟁조정위원회, 「각국의 개인정보피해구제제도 비교연구」, 개인정보분쟁조정위원회, 2007, 278면 이하.
82) 손경한, "전자상거래 입법의 국제적 동향", 「저스티스 통권68호」, 2002, 8면 이하.

1980년 제정된 「OECD 프라이버시 가이드라인」(이하 '「OECD 가이드라인」'이라 한다)의 주된 목적은 각 국가별로 제정·논의되고 있는 개별적이고 상이한 프라이버시보호법을 조화시킴으로써, 국가 간 정보의 자유로운 이동을 활성화하고 개인정보처리로 인한 프라이버시 침해를 방지하는 것이다. 이와 같은 「OECD 가이드라인」은 회원국의 개인정보와 프라이버시의 보호 및 개인의 자유보호를 위한 최소한의 기준을 제시할 필요성은 물론, 국가 간 개인정보 이동이 지속적으로 이루어지고 과도하게 방해받지 않도록 할 필요성과 정보의 경제적 가치 및 공정경쟁원칙에 따른 정보교역의 중요성 등을 염두에 두고 마련된 것으로 볼 수 있다.[83]

「OECD 가이드라인」은 회원국에 강제적으로 적용되는 규범이 아니라 '가이드라인'이라는 이름 그대로 일종의 기준을 제공하는 역할을 한다. 따라서 동 가이드라인을 어떻게 이행할 것인지는 각 회원국에 일임되어 있다. 다만, 「OECD 가이드라인」 제4장 제19조는 회원국이 동 가이드라인을 국내 차원에서 이행할 때 참고할 수 있는 전반적인 틀을 제공하고 있다. 이에 의하면, 회원국은 ① 적절한 국내 입법을 채택하고, ② 실행규약(Code of Conduct)이나 기타의 형식으로 자율규제를 장려하여야 하며, ③ 개인의 권리행사를 도울 수 있는 적절한 방법을 제공하여야 한다. 또한 ④ 개인정보보호원칙을 따르지 않는 경우 적절한 제재조치를 취하고 이로 인한 피해에 대한 구제수단을 마련하여야 하며, ⑤ 정보주체에 대한 불공정한 차별이 없도록 보장하여야 한다.

「OECD 가이드라인」은 자동처리되는 개인정보에 한정하지 않고 모든 개인정보를 그 대상으로 삼고 있다. 따라서 개인정보가 다루어지는 방

83) 김재두, "전자상거래의 입법동향에 관한 법률", 「경영법률」, 2008, 9면 이하.

법이나 수단에 관계없이 프라이버시와 개인의 자유에 위협을 가할 수 있는 모든 개인정보의 처리에 적용된다. 또한 여기서 말하는 개인정보란 식별되는 또는 식별가능한 개인에 관한 정보 일체를 뜻하기 때문에, 직접 또는 간접적으로 특정 자연인과 관련되는 모든 정보를 의미한다. 그 외에도 「OECD 가이드라인」은 정보관리자, 개인정보의 처리, 개인정보의 국외 이전 등의 개념에 대하여 정의하고 있다. 특히 동 가이드라인은 8가지 개인정보보호 기본원칙을 천명하고 있는데, 이러한 개인정보보호원칙은 「UN 개인정보 가이드라인」이나 「EU 개인정보보호지침」을 비롯하여 각국의 개인정보보호법에 큰 영향을 끼쳤다. 「OECD 가이드라인」 역시 회원국 내에서 준수되어야 할 개인정보처리에 관한 최소한의 기준을 제시한 것이라고 밝히고 있고, 세계적으로도 개인정보보보를 위한 기본원칙과 기준으로서 인정받고 있다. 구체적인 「OECD 가이드라인」 8원칙의 내용을 살펴보면 다음과 같다.

[표3-4] 「OECD 가이드라인」 프라이버시 8원칙[84)]

원칙		내용
제1원칙	수집제한의 원칙	• 적법하고 공정한 방법을 통한 개인정보의 수집 • 정보주체의 동의를 얻어 개인정보 수집 • 민감한 개인정보의 수집 제한
제2원칙	정확성확보의 원칙	• 이용목적과의 관련성 요구 • 이용목적상 필요한 범위 내에서 개인정보의 정확성, 완전성, 최신성 확보
제3원칙	목적명시의 원칙	• 수집 이전 또는 당시의 개인정보 수집목적 명시 • 명시된 목적에 적합한 개인정보의 이용
제4원칙	이용제한의 원칙	• 정보주체의 동의가 있거나 법규정이 있는 경우를 제외하고는 목적 외 이용 및 공개 금지

84) http://www.oecd.org 참조.

제5원칙	안전성확보의 원칙	• 개인정보의 침해, 누설, 도용 등을 방지하기 위한 물리적·조직적·기술적 안전조치 확보
제6원칙	공개의 원칙	• 개인정보의 처리 및 보호를 위한 정책의 공개 • 개인정보관리자의 신원 및 연락처, 개인정보의 존재사실, 이용목적 등에 대한 접근 용이성 확보
제7원칙	개인참여의 원칙	• 개인정보 열람·정정·삭제청구권 보장 • 정보주체가 합리적 시간과 방법에 의해 개인정보에 접근할 수 있도록 보장
제8원칙	책임의 원칙	• 개인정보관리자에게 원칙준수의무 및 책임 부과

2. UN 개인정보 가이드라인

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

[표3-5] 「UN 가이드라인」 개인정보 6원칙[85)]

원칙		내용
제1원칙	합법성과 공정성 원칙	• 공정하고 합법적인 방법에 의한 개인정보 수집・처리 • UN헌장 목적과 원칙에 합치되는 개인정보 처리
제2원칙	정확성 원칙	• 정확성과 관련성 확보를 위한 정기적 확인절차 • 정보의 완전성과 최신성 확보를 위한 노력
제3원칙	목적구체화 원칙	• 목적과 이용에 관한 사항에 대한 구체적 명시 및 정당성 확보 • 명시된 목적과의 적절성과 관련성 유지 • 동의가 있는 경우를 제외한 목적 외 이용 및 공개 금지 • 목적달성에 필요한 기간 이상으로의 정보 보유금지
제4원칙	개인접근의 원칙	• 정보의 이용 또는 처리방법에 대한 정보주체의 알 권리 • 부정확한 정보에 대한 정정 또는 삭제 요구권
제5원칙	차별금지 원칙	• 종교, 인종, 정치적 견해 등을 이유로 한 자의적이고 부당한 차별 금지
제6원칙	안정성 원칙	• 사고로 인한 정보의 손실이나 파괴 또는 정보의 남용, 권한 없는 접근, 컴퓨터 바이러스 오염 등으로부터 정보를 안전하게 보호하기 위한 적절한 조치 필요

한편 「UN 가이드라인」은 제6조에서 개인정보보호원칙의 적용으로부터 배제되는 경우를 규정하고 있는데, 이에 의하면 국가안보・공공질서・공중보건 또는 공중도덕과 관련된 정보처리는 제1원칙부터 제4원칙의 적용을 받지 않는다고 한다. 단, 이 경우에도 회원국에서 이러한 적용 제

85) http://www.un.org 참조.

외에 대한 사항을 법률로 명시하고 있고 필요 최소한의 수준으로 적용배제의 범위를 제한하고 있는 경우에만 가능하다. 또한 차별금지원칙의 적용 제외는 오직 인권보호와 차별방지를 위한 국제인권법의 한계 내에서만 허용된다. 이 외에도 동 가이드라인은 프라이버시 보호에 관한 충분한 보호대책이 구비된 국가들 간의 자유로운 정보의 이동 및 상기 원칙의 준수 여부를 감독할 독립기구의 설치 등에 대하여 규정하고 있다.

3. EU 개인정보보호지침

「EU 개인정보보호지침(95/46/EC 지침)」(이하 '「EU 지침」'이라 한다)은 EU 회원국 시민들의 기본권과 자유를 보호하고 개인정보처리와 관련된 개인의 프라이버시를 보호하기 위한 일반적인 개인정보보호지침이다.[86] 동 지침은 상이한 개인정보보호 수준을 가진 회원국의 개인정보보호 법체계를 통일하여, EU 내에서는 모든 회원국 시민들의 개인정보가 동일한 수준으로 보호될 것을 보장함을 목표로 하고 있다.

구체적으로는 EU 회원국 내에서 ① 개인정보 처리에 관한 의무와 책임을 확립하고, ② 개인정보처리의 투명성이 유지되도록 보장하며, ③ 민감한 정보에 대한 특별한 보호기준을 설정하고, ④ 개인정보처리에 대한 효과적인 감독권과 집행권을 확보하는 것이 그 목표이다. 「EU 지침」은 유럽연합 의회와 이사회에 의해 채택된 지침이므로, 회원국은 동 지침의 이행을 위하여 새롭게 개인정보보호법을 제정하거나 기존의 법률을 개정할 필요가 있었다. 이에 EU 회원국이 모두 EU 지침에 맞추어 자국의 개인정보보호법을 완비한 상태이다.

---

86) 개인정보분쟁조정위원회, 전게서, 87면 이하.

동 지침은 「OECD 가이드라인」과는 달리, 기본적으로 자동화된 수단에 의한 개인정보의 처리에 적용된다. 물론 전적으로 자동화된 수단에 의할 것을 요구하지는 않으며 부분적으로 자동화된 수단에 의할 경우에도 적용될 수 있고, 더 나아가 자동화된 수단이 아닌 다른 방법에 의한다 하더라도 개인정보가 파일링시스템[87]의 일부를 구성하거나 그러한 의도로 처리되는 경우에도 적용된다.[88] 즉 「EU 지침」은 모든 개인정보의 자동화된 처리 및 구조화된 수기파일(structured manual files)에 적용되는 것으로 볼 수 있다. 또한 동 지침은 기본적으로 자연인의 개인정보보호를 위한 것이므로, 법인의 정보는 보호대상이 아니다. 다만, 회원국이 법인의 정보를 보호하는 내용의 규정을 두는 것은 가능하다.

한편 「EU 지침」은 적용범위를 제외하고는 「OECD 가이드라인」의 개인정보보호 8원칙의 내용을 대부분 수용하고 있다. 다소 구분되는 점이 있다면, 「EU 지침」은 원칙적으로 민감한 개인정보의 수집을 금지하고 있어 민감한 개인정보에 대한 더욱 강력한 개인정보보호의 입장을 취하고 있다는 점이다. 또한 수집된 개인정보를 제3자에게 제공하거나 공개하는 행위에 대해서 「OECD 가이드라인」과는 달리 상세한 규정을 두어 수집·이용목적 고지 시, 개인정보 제3자 제공에 대한 점도 함께 고지하도록 하고 있다. 그 외에도 필요 이상으로 정보주체가 식별되지 않도록 하고, 장기간의 저장이 필요한 개인정보에 대해서는 적절한 보호 기준을 설정하도록 규정하고 있다.

---

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

88) 「EU 지침」의 적용범위는 「UN 가이드라인」과 기본적으로 유사하다.

그러나 무엇보다도 「EU 지침」의 가장 두드러진 특징은 바로 독립적인 개인정보보호기구의 설립을 통한 개인정보처리의 관리·감독 및 개인정보의 제3국으로의 이전에 대한 엄격한 제한이다. 「EU 지침」은 개인정보처리자로 하여금 회원국 내 독립적인 개인정보보호기구에 개인정보처리행위에 대해 고지하도록 하고 있는데, 이는 개인정보보호기구가 고지받은 개인정보처리행위가 정보주체의 권리와 자유에 위협이 될 수 있는지 여부를 사전심사할 수 있도록 하기 위함이다. 또한 「EU 지침」은 제25조에서 회원국 외 제3국이 동 지침에서 밝히고 있는 개인정보보호의 적절한 수준을 갖추고 있지 아니한 경우에는 개인정보를 해당 국가에 이전하지 못하도록 하고 있는데, 이 규정은 일명 '프라이버시 라운드(Privacy Round)'라 불리는 사실상의 새로운 무역장벽으로 떠오르고 있다.[89]

[표3-6] 「EU 지침」의 주요내용[90]

구분	내용
적용범위	• 물적 범위 : 자동처리되는 개인정보 및 구조화된 파일링시스템에 포함되는 개인정보 • 인적 범위 : 자연인의 개인정보
적용제외 영역	• 국가안보, 공공의 안정 및 방위를 위한 개인정보 처리 • 형사법 영역에서의 개인정보 처리 • 지극히 개인적이고 사적인 목적의 개인정보 처리 • 언론보도, 문학, 예술적 표현을 위한 개인정보 처리
정보처리자의 의무	• 공정하고 적법한 개인정보의 처리 • 정보처리목적의 명시

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

90) http://www.europa.eu 참조.

	• 정보처리목적과의 적절성과 관련성, 비례성 유지 • 개인정보의 정확성과 최신성 확보 • 기술적, 조직적 보안조치 확보 • 감독기구에 정보처리에 대하여 고지
정보주체의 권리	• 정보처리의 전반적인 사항에 대하여 통지받을 권리 • 정보처리에 대하여 협의할 권리 • 자신의 개인정보에 대해 수정을 요구할 권리 • 특정 상황에서의 개인정보 처리에 대하여 반대할 권리
제3국으로의 정보이전금지	• 적절한 보호수준을 갖추지 않은 제3국으로의 개인정보 이전 금지
독립기구의 설치	• 회원국 내 독립적인 개인정보보호기구의 설치

EU는 또한 지난 2002년, 「전자통신부문에서의 개인정보처리 및 프라이버시 보호에 관한 지침」을 마련하였다. 동 지침은 지난 1995년 EU지침에 규정된 기본원칙을 통신부문에 대한 세부규칙으로 전환하고 통신 영역에서의 개인정보와 프라이버시를 보호하기 위하여 마련된 지침 97/66/EC을 폐기하고 대체하는 새로운 지침이다. 동 지침은 1997년 이후 새롭게 변화된 정보통신서비스 시장과 기술의 발전상황을 반영하고 통신서비스 사용자에게 사용기술과 관계없이 동일한 수준의 개인정보와 프라이버시 보호를 제공하기 위한 목적으로 개정되었다.

동 지침의 기본목적은 전자통신 분야의 개인정보 처리와 관련하여 EU 회원국의 기본권과 자유, 특히 프라이버시의 보호수준을 동등하게 맞추고 EU 회원국 내에서 전자통신 장치와 서비스 및 개인정보가 자유롭게 이전될 수 있도록 보장하는 것이다. 따라서 1995년 「EU 지침」에서 규정한 개인정보보호를 위한 기본사항을 바탕으로, 전자통신과 관련한 이용자의 전송정보(traffic data)·위치정보·통신비밀의 보호, 쿠키사용에 대한 이

용자의 거부기회 보장, 옵트인(opt-in)제도[91] 도입을 통한 스팸메일 등 원치 않는 통신으로부터의 이용자 보호, 전자통신서비스의 기술적·조직적 보안조치, 발신자번호·접속자번호의 표시 제한 등에 관한 사항을 규정하고 있다.

이와 같이 동 지침은 기술 발달의 영향을 가장 빨리 그리고 가장 밀접하게 받고 있는 전자통신 및 전자거래 분야에서 이용·전송되고 있는 개인정보를 어떻게 보호할 것인가에 대한 문제를 다루고 있을 뿐 아니라, 위치정보와 발신자번호 표시, 스팸메일과 같은 최근 급격히 문제가 되고 있는 사안들에 대해 구체적으로 규율하고 있다는 점에서 의미가 있다. 동 지침은 2002년 7월부터 시행되었으며, EU 회원국들은 2003년 10월 31일까지 지침의 내용을 반영하는 법체계를 마련하였다.

Ⅱ. 주요국가의 개인정보보호제도

1. 영국

1) 개인정보보호법

성문헌법이 없는 영국은 당연히 프라이버시권 또는 개인정보자기결정권에 대한 명시적·묵시적인 헌법상의 근거를 가지고 있지 않다. 그러나 영국은 1215년 마그나카르타(Magna Carta)에서 시작하여 인권선언의 의미를 가지는 권리청원(Petition of Rights)과 권리장전(Bill of Rights)의 제정을 거치면서, 시민들의 사적 자유와 인권을 존중하는 법제도 도입에

91) 옵트인(opt-in)은 광고 메시지 등을 전송할 때, 그 수신자가 이를 허용했을 경우이고, 그렇지 않다면 옵트아웃(opt-out)이다.

선구적인 역할을 해왔다. 이러한 인권존중의 법적 전통은 당연히 프라이버시 및 개인정보에 법적 보호로 이어지게 되어, 「1984년 정보보호법(The Data Protection Act 1984)」을 제정하여 시행하게 되었다. 또한 유럽인권협약을 이행하고자 제정한 「1998년 인권법(The Human Rights Act 1998)」에서는 동법 제 8조에서 프라이버시와 가정생활, 주거 및 통신의 자유와 권리를 규정함으로써, 명시적으로 프라이버시 보호의 필요성과 권리를 인정하고 있다.

영국은 「1984년 정보보호법(The Data Protection Act 1984)」을 제정함으로써 개인정보보호를 위한 첫 번째 발판을 마련하였다고 볼 수 있다. 그러나 동법은 개인정보보호를 위한 일반원칙을 모두 아우르고 있다기보다는 개인정보를 처리하는 공공기관이나 사업자 등을 등록하여 '정보처리자 등록부'를 유지·관리하는 것에 더 큰 초점이 맞추어져 있었다. 그러던 중 1995년 「EU 지침」이 제정되면서, 영국도 동 지침의 내용에 맞추어 국내법을 전면 수정할 필요가 생겼다. 이런 이유에서 제정된 법률이 바로 「1998년 정보보호법(The Data Protection Act 1998)」이다. 동법은 공공과 민간부문의 구분 없이 영국에서 이루어지는 모든 개인정보 처리에 적용되는 개인정보보호 기본법의 역할을 하고 있다.[92]

이렇듯 「정보보호법」은 영국의 개인정보보호 기본법으로서 적용 범위가 광대함은 물론, 개인정보보호 기본원칙을 비롯한 개인정보와 관련된 사항을 포괄적으로 규정하고 있다. 그러나 기본법의 특성상 「정보보호법」은 각 개별 영역의 특수한 개인정보 처리상황을 모두 규정하고 있지는 않고, 특정 영역에 관하여는 다른 특별법이나 하위법령에 위임하고 있

92) 개인정보분쟁조정위원회, 전게서, 125면 이하.

다. 대표적인 것이 전자통신 분야에서의 개인정보보호와 관련하여, 1997년 「EU 지침」의 내용을 보충하고 구체화하기 위해 제정된 「1999년 전자통신(정보보호 및 프라이버시)규칙(The Telecommunications(Data Protection and Privacy) Regulations 1999(1999/2093)」, 「2000년 조사권에 관한 법률규칙(RIPA 2000 : The Regulations of Investigatory Powers Act 2000)」, 「2000년 전자통신규칙(합법적인 사업관행)(통신차단)(The Telecommunications(Lawful Business Practice)(Interception of Communication) Regulations 2000 (2000/2699)」이 있다. 이 중 「1999년 전자통신규칙」은 종합정보통신망(ISDN), 공공디지털모바일네트워크(public digital mobile network), 주문형 비디오(VOD), 쌍방향 TV 등 새로운 전자통신분야에서의 개인정보보호를 위해 제정된 것으로, 원하지 않는 팩스나 전화와 같은 스팸통신에 대하여 규제하고 있다.[93]

또한 「2000년 조사권에 관한 법률 규칙」은 「EU 전자통신 분야에서의 정보보호지침」 제5조의 내용을 시행하는 별도의 입법으로 공공·민간 네트워크를 통한 전자통신의 비밀을 보호하기 위해 제정된 것이다.[94] 이 외에도 정보주체가 신용정보회사 등 평가기관에서 보유하고 있는 각종 개인정보에 대하여 접근권을 행사할 수 있도록 규정한 「1974년 소비자신용법(The Consumer Credit Act 1974)」, 자신의 건강정보 또는 치료기록에 대한 접근을 요청할 수 있도록 한 「1988년 의료기록 접근에 관한 법률(The Access to Medical Reports Act 1988)」, 「1990년 건강기록 접근에 관한 법률(The Access to Health Records Act 1990)」 등의 법률이

93) 동법은 2003년 12월 11일부로 「2003 프라이버시 전자상거래 규칙(EC 지침)(The Privacy and Electronic Communication (EC Directive) Regulation 2003」으로 대체되었다. 새롭게 제정된 규칙은 전자상거래의 발달상황에 따른 규율을 위해 1999년 규칙보다 기술과 프라이버시에 관한 사항을 더욱 많이 포함하고 있다. (http://www.dca.gov.uk 참조.)

94) Gerald Spindler, *E-Commerce Law in Europe and the USA*, Springer, 2002, p.298.

있다. 이와 더불어 「1998년 정보보호법」은 하위법령으로 국가안보, 형사, 세금, 의료, 교육, 사회사업, 언론 등 특정 영역을 규율하는 규칙을 제정하여 시행하고 있다.

[표3-7] 영국의 개인정보관련 법제 현황

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

2) 개인정보보호기구

영국은 1984년부터 '정보보호등록관(Data Protection Register)'을 설치

하여 자국 내에서 이루어지는 모든 개인정보 처리행위를 사전 등록함으로써 개인정보를 보호하여 왔다. 이러한 정보보호등록관은 그 역할과 위상이 점차 증대하여, 1998년 전면 수정된 「정보보호법」에 따라 정보보호커미셔너(Data Protection Commissioner)로 개칭되었고, 2000년에는 「정보공개법」에 따라 '정보커미셔너(Information Commissioner)'로 변천되어 오늘날에 이르고 있다.

정보커미셔너는 「정보보호법」과 「정보공개법」에 근거하여 설립된 개인정보보호를 위한 독립법정기구이다. 커미셔너는 여왕의 특허장에 의해 임명되며 5년의 임기가 보장되고 두 차례에 걸쳐 재임이 가능하다. 영국의 정보커미셔너는 독립성과 자율성은 무엇보다도 행정부의 지시·감독을 받지 않고 독자적으로 운영된다는 점을 통해 확인할 수 있다. 즉 커미셔너의 임금과 연금은 하원의 결의를 통해 결정되고 별도 조성된 통합기금에서 지급받으며 기관의 운영예산도 직접 의회의 결의를 통해 지원받고 있기 때문에, 내무부로부터 행정적 지원이나 협조 외의 간섭을 받지 않는다. 또한 정보커미셔너는 기관의 각종 활동상황에 대해 의회에 직접 보고한다.

이러한 정보커미셔너는 민간과 공공부문의 모든 개인정보처리를 관할대상으로 삼고 있다. 따라서 온라인·오프라인을 구분하지 않고 일반 사업자에 의한 개인정보처리나 정부부처 등 공공기관에 의한 개인정보처리가 올바르게 이루어지고 있는지 감시하고 규율하는 역할을 하고 있다. 이와 더불어 특수한 영역별로는 의료정보, 신용정보, 교육정보, 정보통신분야에서 취급되는 개인정보, 근로자 정보 및 CCTV와 프라이버시 문제, 다이렉트 마케팅 문제 등에 대해서도 각종 규칙이나 지침 등의 법규를 통해

규율하고 있다.

따라서 정보커미셔너는 개인정보를 취급하는 개인이나 단체의 이름과 주소 등 연락처, 정보처리목적, 수집·보유하고 있는 개인정보항목 등 정보처리와 관련된 소정의 내용을 고지받아 기록하는 공공등록부(public register)를 유지·관리할 책임을 진다. 아울러 이러한 정보보호등록부(The Data Protection Register)는 인터넷 웹사이트를 통해 공개됨으로써 일반 국민들이 쉽게 접근하여 확인할 수 있도록 하고 있다.[95]

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

2. 프랑스

1) 개인정보보호법

프랑스에서 일반 국민들의 개인정보에 관한 관심이 증대된 계기는

95) http://www.privacyinternational.org 참조.

1974년 프랑스 정부가 모든 행정기관이 개인신원확인대장을 검색·이용하도록 하겠다는 내용의 사파리(Project SAFARI en 1974(Systéme autoinatisé pour les fichiers administratifs et le répertoire des individu)) 법안을 발표하면서부터이다. 프랑스에서는 1960년대부터 산업화와 정보화의 진전, 특히 컴퓨터 등 정보처리 기술의 발달에 대응하기 위한 새로운 법질서 확립에 대한 논의가 시작되었다. 이에 프랑스 최고행정법원(국참사원, Conseil d'Etat)에서는 '공적·사적 자유 및 행정결정에서의 정보처리발달의 결과'라는 연구보고서를 발간하였고, 여기서 언급된 해결방안이 위 입법안으로 구체화된 것이다. 그러나 이러한 정부의 계획은 개인정보를 보호하기 위한 제도적 장치가 마련되지 않은 상태에서 행정기관이 자신들의 개인정보를 아무런 제한 없이 사용할 수 있도록 하는 것은 개인정보침해와 남용의 우려가 크다는 여론에 따라 보류될 수밖에 없었다. 일명 '사파리(SAFARI) 사건'이라고 불리는 이러한 일련의 과정을 겪으면서 프랑스에서는 체계적인 개인정보보호의 필요성이 제기되었고, 이는 1978년 「정보처리축적및자유에관한법률」의 제정으로 이어지게 되었다. 동법은 프랑스에서 이루어지는 모든 정보처리에 관한 사항을 규율하는 포괄적이고도 가장 기본적인 원칙을 확립함과 아울러, 의료정보를 비롯한 다양한 영역의 개인정보를 보호하기 위한 세부 시행규칙을 포함하고 있다.[96]

[표3-8] 정보처리축적및자유에관한법률 및 하위법령

구분	법규
기본규정	정보처리축적및자유에관한법률 (Loi n° 78-17 do 6 janvier 1978, Loi relative

96) 정재황, "프랑스법에서의 개인정보의 보호에 관한 연구", 「공법연구 34집 4호 1권」, 2006. 6, 12면 이하.

	à l'informatique, aux fichiers et aux libertés)
형사제재에 관한 규정	동법 제41조～제44조
	형법 제226-16조～제24조(Code Pénal Article 226-16 à 24)
	시행령 81-1142(Décret 81-1142 du 23 décembre 1981)
세부적용에 관한 규정	법적용에 관한 시행령(Décret 78-774 du 17 juillet 1978)
	국가안보를 위한 개인정보처리에 관한 시행령 (Décret 79-1160 du 28 decémbre 1979)
	접근권행사시 부과금에 관한 시행령 (Décret 79-1160 du 28 juin 1982)
	의료정보에 관한 시행령(Décret 95-682)
	개인건강정보의 처리에 관한 시행령 (Décret 99-919 du 27 octobre 1999)
	부과금 계산에 관한 시행규칙 (Arrêté du 23 septembre 1980)
	공공부문에서의 법적용에 관한 행정동첩 (Circulaire du 23 mars 1993)

2) 개인정보보호기구

1974년 사파리(SAFARI) 사건을 계기로, 프랑스 정부는 '공공·준공공·민간부문에서 이루어지는 정보처리의 발달에 대비하여 개인의 사생활과 개인적 자유 및 공적 자유를 존중하고 보장하는 방안'을 마련하여 이를 담당하는 위원회를 법무부 소속 하에 설치하였다. 당시 위원회의 대표자였던 버나드 쉐노(Bernard Chenot)는 수많은 자문과 논쟁을 거쳐 개인정보보호기본법의 제정 및 동법의 적용을 감독하는 임무를 맡는 독립적인 기구의 설치를 주장하였는데, 이는 1969년 최고행정법원(국참사원)에서 수

행한 연구를 구체화한 것이었다. 이 보고서를 기초로 하여 제정된 법률이 바로 1978년 「정보처리축적및자유에관한법률」이며, 동법 제6조를 근거로 하여 '정보자유위원회(CNIL : Commission nationale de l'informatique et des libertes)'가 설립되었다. 프랑스의 정보자유위원회는 프랑스 내에서 이루어지는 모든 개인정보 처리행위를 규율함으로써, 부당한 개인정보의 처리로 국민들의 개인정보가 침해되는 것을 방지하기 위해 설립된 대표적인 개인정보보호기구이다.

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

[표3-9] CNIL의 주요기능

구분	법규
정보처리 등록・신고	• 정보처리에 대해 의견제시 및 신고접수 • 정보등록부 관리 및 공개
법규준수 조사・감독	• 자료제출요구 및 직권조사 • 법위반자에 대한 경고조치 및 형사고발
각종 규칙(지침) 제정	• 보편적인 정보처리에 대한 규준 제정
접근권・정정권 보장	• 정보주체의 권리행사방법의 용이성 확보 • 공공기록에 대한 간접적 접근권 행사
고충처리 및 피해구제	• 각종 이의제기・신고・신청사항 등 민원처리 • 사전 사실조사 실시 및 당사자 합의유도

	• 경고, 제소, 기각 등의 결정
자문・상담 등 정보제공	• 당사자의 권리・의무에 대한 정보제공 • 의회에 연차보고서 제출 • 정부에 대하여 정책자문 및 입법절차 참여

3. 독일

1) 개인정보보호법

독일은 유럽 내에서도 가장 엄격한 정보보호법을 가지고 있는 국가 중 하나이다. 세계 최초의 정보보호법이 1970년 독일 헤센(Hessen)州에서 제정된 것을 보더라도, 독일인들의 개인정보보호에 대한 관심을 짐작할 수 있다. 독일에서는 1960년대 후반부터 정보전자화의 급속한 진행에 따른 개인정보침해 위험에 대비하여 개인정보보호 입법안을 마련하여야 한다는 학계의 주장이 대두되었고, 이러한 개인정보보호의 필요성에 대한 자각과 인식은 헤센주의 정보보호법을 시작으로 각 주와 연방차원에서 개인정보보호법의 제정으로 이어지게 되었다.[97]

독일에서 개인정보보호법제의 헌법적 근거는 바로 독일기본법(Grundgesetz) 제1조 인간존엄성 조항과 제2조 인격의 자유로운 발현조항을 들 수 있을 것이다.[98] 물론 독일 기본법상 프라이버시권에 관한 명시

97) 개인정보분쟁조정위원회, 전게서, 96면 이하.

98) 제1조(인간존엄의보호)
①인간의 존엄은 불가침이다. 이를 존중하고 보호하는 것은 모든 국가권력의 의무이다.
② 독일 국민은 불가침・불가양의 인권을 세계의 모든 인간 공동체, 평화 그리고 정의를 기초로서 인정한다.
③ 기본권은 직접 효력을 갖는 권리로서 입법권, 집행권, 사법권을 구속한다.
제2조(일반적 인격권)
① 누구든지 타인의 권리를 침해하지 아니하고 헌법질서나 도덕률에 위반하지 않는 한, 자신의

적인 규정은 없으나, 기본법 제1조와 제2조를 프라이버시권에 대한 일차적인 근거조항으로 보기에 무리가 없을 것이다. 독일 헌법재판소 역시 1983년 헌법소원 판결을 통해 '명확한 공공의 이익에 의해서만 제한받을 수 있는 정보자기결정권'을 선언하였는데, 특히 이러한 정보자기결정권은 인격권(Personlichkeitsrecht)의 불가침성을 규정한 기본법 제1조 제1항과 제2조 제1항에서 직접적으로 파생되는 권리임을 명확히 하였다. 이외에도 기본법 제10조는 서신, 우편, 통신 등의 비밀과 프라이버시가 보호되어야 할 대상임을 밝히고, 이에 대한 제한은 반드시 법률로서 하여야 한다고 규정하고 있다.

이러한 헌법상의 근거를 바탕으로 독일 시민들의 개인정보를 보호하기 위한 기본법이 1977년 연방차원에서 제정되었는데, 「연방정보보호법(BDSG : Bundesdatenschutzgesetz)」이 바로 그것이다. 동법은 2002년 개정을 통해 「EU 지침」의 내용을 반영한 바 있다.

이러한 「연방정보보호법」 외에도 독일은 연방 차원에서 개인정보 관련 개별법을 제정하여 시행하고 있다. 대표적인 것이 정보통신 분야에서의 정보보호에 관하여 규율하고 있는 1997년 「정보통신서비스정보보호법(TDDSG : Teledinenstdatenschutzgesetz)」으로, 동법은 「연방정보보호법」에 우선하여 적용된다. 특히 동법은 전자서비스 이용관계에서의 개인정보 이용에 대하여 규율하기 때문에, 인터넷포탈사이트, 이메일서비스제공자, 게임서비스제공자 등의 통신서비스제공자에 대해 직접 적용된다. 이외에도 「우편법(Postgesetz)」, 「사회보장법(Sozialgesetzbuch)」, 「조

인격을 자유로이 발현할 권리를 가진다.
② 누구든지 생명권과 신체를 훼손당하지 않을 권리를 가진다. 신체의 자유는 불가침이다. 이 권리들은 법률에 근거해서만 침해될 수 있다.

세법(Abgabenordnung)」, 「소득세법(Einkommensteurgesetz)」 등의 법률에 개인정보관련 규정이 포함되어 있다.

2) 개인정보보호기구

연방국가인 독일은 현재 연방 차원의 개인정보보호법인 「연방정보보호법」외에도 주 차원에서 각각 개인정보보호법이 마련되어 있고, 이를 바탕으로 개인정보보호기구들이 설치되어 활동 중이다.[99] 따라서 연방에서는 '연방정보보호청(BfD : Bundesbeauftragter für den Datenshutz)이 주로 연방공공기관을 중심으로 규율하고 있으며, 현재 주 단위의 개인정보보호기구는 주 공공기관의 정보처리에 대해 규율하고 있다. 또한 독일에서는 일부 영역을 제외한 대부분의 민간부문에 대해서는 민간 감독기구를 각 주마다 설치하여 사적 영역의 개인정보 처리에 대해 관리·감독하게 하고 있다. 그러나 베를린(Berlin), 브레멘(Bremen), 함브르쿠(Hamburg), 남부작센(Lower Saxony), 쉴러버그-홀슈타인(Schlerwig-Holstein)과 같은 주에서는 주 개인정보보호기구가 민간부문에 대해서도 함께 규율하고 있다.

연방정보보호청은 개인정보의 수집, 처리, 사용과 관련하여 「연방정보보호법」이 적용되는 범위 내에서 활동하나, 주의 개인정보보호기구와 각 주에서 설립한 민간 정보보호감독기구의 업무범위를 제외한 범위에서 활동한다. 따라서 실질적으로 연방정부와 공공기관, 연방정부 산하단체, 연방법원, 여러 주에 걸쳐 사업하는 우편이나 통신사업자 등에 대해서만 관할하는 것으로 볼 수 있다. 그러나 최근에는 사회정보의 보호와 관련해서

99) 「연방정보보호법」 제4d조 제4항.

도 연방정보보호청이 개업하고 있고, 환자, 사고, 연금보험, 실직보험과 관련된 정보영역에 대해서도 관할하는 등 점차 그 업무범위가 확장되어가고 있다. 즉 독일에서는 연방과 주의 업무영역이 구분되어 각자 독립적으로 활동하고 있으며, 특히 「연방정보보호법」은 공공과 민간부문 모두에 적용되는 기본법이나 개인정보보호기구는 공공부문과 민간부문이 분리되어 설치·운영되고 있다는 점에서 다른 유럽 국가들의 개인정보보호기구와는 다소 차이가 있다.

4. 미국

1) 개인정보보호법

개인의 자유와 개성을 중시해 온 미국은 일찍부터 프라이버시의 개념을 새롭게 인식하고 프라이버시 침해를 보통법상의 불법행위로 보아 손해배상책임을 인정해 온 법적 전통을 가지고 있다. 이렇듯 판례법 국가인 미국은 프라이버시권도 법원에서 보통법상 권리로 인정하여 왔기 때문에, 대륙법계 국가인 프랑스, 독일 등 다른 유럽 국가들과는 달리 포괄적이고 체계적인 개인정보 관련 법체계를 가지고 있지는 않다. 그래서 프라이버시보호 및 개인정보보호를 위해 영역별 접근방식을 택하여 세부적으로 개별 입법을 제정·시행하고 있다.

입법 체계상으로 포괄적인 개인정보보호법을 가지고 있지 않다는 점 외에도 미국은 개인정보에 대한 접근방식에 있어서도 다른 유럽 국가들과는 달리 경제적·기술적 측면에서 바라보는 경향이 있다. 이는 특히 민간부문에서 두드러지는데, 그 이유는 사적 자치의 원칙을 중시하여 정부의

간섭을 초소화한 자유로운 시장경제질서의 유지를 무엇보다도 중시하는 경제적 관점을 가지고 있기 때문이다. 따라서 민간부문에 대해서는 특별히 규제할 필요성이 인정되는 경우에만 법률을 제정할 뿐, 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 마련하도록 유도하는 것이 정부가 담당할 부분으로 여기고 있다. 흔히 '자율규제(Self Regulation)'라고 부르는 이러한 접근방식은 개인정보를 인권의 하나로 인정하여 국가가 적극 관여하여 보호하여야한다고 보는 유럽의 입장과는 다른 태도이다.

앞서 밝힌 바와 같이 미국은 헌법상 명시적인 프라이버시권 규정을 가지고 있지는 않다. 그러나 미연방대법원(U.S. Supreme Court)은 사적 통신의 자유가 있음을 확고히 한 Katz v. U.S. 판결에서 제1차, 제3차, 제4차, 제5차 수정헌법을 간접적인 의미에서의 프라이버시권 조항으로 해석할 수 있다고 밝힌 바 있다. 특히 미연방대법원은 제4차 수정헌법(Fourth Amendment)[100]을 함축적인 의미의 프라이버시권 규정으로 볼 수 있다고 하면서, 개인이 '프라이버시에 대한 합리적 기대(reasonable expectation of privacy)'를 가진 영역에 있어서는 정부의 감시나 간섭으로부터 자유로울 권리를 가진다고 하였다.[101] 이로 인해 미국에서는 헌법상 명시적인 개인의 프라이버시권에 대한 규정은 없지만, 다른 헌법상의 조항들을 통해 개인의 사적 자유가 존중되어야 할 프라이버시권을 가지는 것을 해석되고 있다.[102]

---

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

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

102) 그러나 이러한 헌법상 근거는 기본적으로 국가, 즉 행정부 등 공권력에 대한 개인의 프라이버시 및 사적 자유의 보장을 의미하는 것으로 보아야 한다. 즉 민간 기업이나 단체의 개인정보 침

한편 미연방대법원은 일반적인 프라이버시권 외 개인정보와 관련한 정보프라이버시에 대해서는 명확한 언급을 하고 있지는 않다.[103] 다만, 법원은 Roe v. Wade 판결[104]에서 "프라이버시에 대한 독립적인 권리나 영역은 존재한다. 이는 아이를 낳을 것인지에 대한 결정 또는 낙태를 할 것인지에 대한 결정과 같이 한 개인에게 중요한 영향을 끼치는 문제에 대하여 스스로 결정할 권리를 포함하는 개념이다"라고 하였고, Whalen v. Roe 판결[105]에서는 "프라이버시 영역은 두 가지 유영의 이익을 포함한다. 첫 번째는 자신의 사적인 사항들이 공개되는 것을 회피할 수 있는 사적 이익이고, 두 번째는 특정한 중요 결정을 내리는데 있어 독립성을 가지고 행할 수 있는 이익이다"라고 하여, 개인이 자신의 개인정보를 다른 간섭으로부터 자유로이 사적으로 관리하고 결정할 권리를 가지고 있음을 밝힌 바 있다.

이렇듯 미국은 판례법상 프라이버시권을 대체적으로 인정하고 있다. 즉 미국은 판례법 외에는 개인정보보호를 위한 포괄적이고도 체계적인 기본법을 가지고 있지도 않고, 되도록이면 시장경제질서에 개입하는 제재조항을 담은 내용을 입법화하지 않으려는 것이 일반적이다. 그러나 미국에

해행위로부터 개인의 자유를 보장하기 위한 헌법상 근거를 동 조항으로부터 바로 도출하기에는 다소 무리가 있다. (Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Indiana Law Review 174, 1999.)

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

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

105) Whalen v. Roe, 429 U.S. 589 (1977). 또한 동 법원은 Whalen v. Roe 판결 방론에서 "개인을 직접 식별할 수 있는 번호나 식별인자를 컴퓨터 데이터베이스로 수집하는 것은 개인의 자유나 권리를 침해할 위험이 함축되어 있다"고 밝히고 있다.

개인정보 또는 프라이버시 관련 법률이 전혀 없는 것은 아니며, 오히려 기본법이 부재한 상황이기 때문에, 사회적 변화나 기술발달에 맞춰 공공·통신·금융·온라인·전자거래 등 각 영역별로 많은 개인정보 관련 법률을 마련해 두고 있다.

[표3-10] 미국의 개인정보관련 법제 현황

구분	개인정보 관련법
공공부문	· 프라이버시법(Privacy Act, 1974) · 정보공개법(Freedom of Information Act, 1974) · 프라이버시보호법(Privacy Protection Act, 1980) · 컴퓨터에의한정보조합과프라이버시보호에관한법률 (Compute Matching and Privacy Protection, 1988) · 전자정부법(E-Government Act, 2002)
금융부문	· 공정신용평가법(Fair Credit Reportion Act, 1970) · 금융프라이버시에관한법률 (Right to Financial Privacy Act, 1978) · 금융현대화법(The Financial Modernization Act, 1999)
통신부문	· 케이블통신정책법 (Cable Communications Policy Act, 1984) · 전자통신프라이버시법 (Electronic Communication Privacy Act, 1986) · 전기통신법(Telecommunications Act, 1996)
교육부문	· 가족의교육권및프라이버시에관한법률 (Family Educational Rights and Privacy Act, 1974)
의료부문	· 건강보험책임법 (HIPPA) (Health Insurance Portability and Account뮤ility Act)
비디오감시	· 비디오프라이버시보호법 (Video Privacy Protection Act, 1988)
근로자정보	· 근로자기록보호법

	(Employee Polygraph Protection Act, 1988)
아동의 개인정보	• 아동온라인프라이버시보호법 (Child Online Privacy Protection Act, 1998)
기타	• 운전자프라이버시보호법 (Driver's Privacy Protection Act, 1994)

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

세이프하버 원칙은 기본적으로 EU 회원국과의 국제교류와 관련하여 유럽 시민들의 개인정보를 전달받아 처리하는 미국 기업이 「EU 지침」에서 규정한 '적정성(adequacy)'을 갖추고 있는지 여부를 판단하기 위한 기준이다. 이처럼 동 원칙은 국제조약의 성격을 가진 것이 아니고 개인정보 취급의 적정성 여부를 판단한다는 특정한 목적을 위해 합의된 사항이기 때문에, 미국에서 법적 효력을 가지고 전면적으로 시행되는 것은 아니다. 따라서 세이프하버 원칙에 참가할 것인지 여부는 전적으로 미국기업의 자발적 의사에 달려 있다.

그러나 실질적으로 동 원칙에 참가할 경우 유럽위원회(European Commission)가 개인정보취급의 적정성을 확인하여 주는 효과를 가지므로 EU 회원국과 개별적으로 별도 협의와 논의를 하여야 할 필요가 없고, 적

정성이 추정되기 때문에 특별한 사한이 없는 한 계속해서 개인정보를 교류할 수 있다. 따라서 현재 미국에서는 이러한 세이프하버 원칙의 장점과 이점으로 인해 다수의 기업체가 참여하고 있다.[106] 세이프하버 원칙에 참여하려는 기업은 반드시 동 원칙의 내용을 준수할 것임을 공표하여야 한다. 공표방법은 미국의 상무부(Department of Commerce)에 서면확인서를 제출하고 자사의 프라이버시정책에 위와 같은 사실을 공개하는 것이다.[107]

[표3-11] 세이프하버 7원칙

구분	원칙의 내용
고지 (Notice)	개인정보의 수집・이용목적, 용도, 정보를 제공하는 제3자의 유형, 문제제기 또는 권리행사시 접근방법 등에 대하여 고지
선택 (Choice)	개인정보가 제3자에게 제공되는지 여부 및 최초의 수집 목적과 양립할 수 없는 다른 목적으로 정보가 사용될 것인지 여부에 대해 옵트 아웃 방식의 선택권을 제공 (민감한 정보에 대해서는 옵트 인 방식의 선택권 제공)
제공 (Onward Transfer)	개인정보의 위탁처리 등과 같이 제3자에게 개인정보를 제공할 경우, 당사자에게 고지함은 물론 선택권을 부여하여야 함
접근 (Access)	정보주체의 접근권과 정정요구권을 보장
안전성 (Security)	개인정보의 손실, 오용, 권한 없는 접근, 변경, 파기로부터 보호하기 위한 합리적 예방조치를 취하여야 함

106) 2009년 현재 1786개의 기업이 세이프하버 원칙에 자발적으로 참여하고 있다. 이는 5년여 전인 2003년 12월, 433개의 기업이 참여했음을 감안하면 상당한 성과를 보인 것으로 판단된다. (http://www.export.gov/safeharbor 참조.)

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

정보 무결성 (Data Integration)	당초의 수집 및 이용 목적에 부합한 개인정보의 이용, 정확성・완전성・최신성의 확보
이행 (Enforcement)	원칙의 준수를 담보할 수 있는 구제수단과 분쟁해결절차, 제재수단이 확보되어야 함

세이프하버 원칙에 참여한 기업은 의무사항 중 하나로, 소비자의 이의제기와 분쟁을 적절히 해결하고 자사의 원칙 준수를 담보할 수 있는 대안적인 분쟁해결제도를 갖추어야 한다. 따라서 이러한 대안적 분쟁해결절차와 방법을 통해 소비자는 사업자의 원칙 불이행으로부터 입은 피해를 구제받을 수 있다. 그러나 민간차원의 자율규제 프로그램을 통해서도 해결되지 않은 경우에는 연방거래위원회와 미국 교통부(Department of Transportation)가 개입하여 위반 사업자에게 보다 강력한 제재를 부과할 수 있다. 또한 지속적으로 원칙을 위반하는 사업자의 경우에는 상무부의 세이프하버 참여기업 목록에서 삭제될 수도 있다.[108]

(2) 개인정보보호기구

미국은 개인정보보호를 위한 별도의 전담기구는 없다. 다만 공공부문과 민간부문에서 예산관리국(OMB : The Office of Management and Budget)과 연방거래위원회(FTC : The Federal Trade Commission)가 각각 개인정보보호기구로서의 역할을 담당하고 있을 뿐이다. 먼저 공공부문에 있어서는 예산관리국이 「1974년 프라이버시법」에 따라 연방정부의 프라이버시 또는 개인정보보호 정책을 정립하는 역할을 맡고 있다. 그러

108) 유럽연합은 연방거래위원회와 교통부를 사업자의 불공정 사기행위를 제재하고 사업자가 세이프하버 원칙을 이행하지 않아 피해를 입은 소비자의 이의제기를 조사하여 구제할 수 있는 권한이 있는 기관으로 인정하고 있다. (Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000. 개인정보분쟁조정위원회, 전게서, 175면 이하 참조.)

나 예산관리국은 예산편성과 운용 등 국가재정운영 전반에 관한 정책을 수립하고 집행하는 역항을 하는 기구인 바, 프라이버시 보호와 관련하여서도 예산관리차원에서만 제한적인 역할을 맡고 있을 뿐이다. 한편 민간부문에 있어서는 연방거래위원회가 아동의 온라인프라이버시, 소비자신용정보, 공정한 거래 관행과 관련하여 개인정보 또는 프라이버시를 보호하는 법률을 집행하고 준수 여부를 감독할 권한을 부여받아 행사하고 있다.

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

연방거래위원회는 1914년에 설립된 기구로서 자유롭고 공정한 거래의 확보를 위해 활동하는 독립기구이다. 연방거래위원회는 주로 대통령 또는 의회에 대하여 관련 입법에 관한 자문을 행하고 소비자에게 필요한 다양한 정보를 제공하려는 목적에서 설립된 기구이나, 점차 공정한 사업관행의 확보와 실행에 초점을 맞추어 활동하게 되면서 그 권한이 더욱 확대되었다.

동 위원회의 주요 임무는 과도한 제한을 가하지 않은 상태에서 시장기능이 효율적으로 작동되고 적절한 경쟁관계를 유지하도록 함으로써 불공정한 사업관행으로부터 자국의 소비자를 보호하는 것이다. 이는 개인정보와 관련해서도 마찬가지이다. 따라서 연방거래위원회는 개인정보 및 프라이버시의 중요성을 사업자와 소비자에게 알리는 역할을 하고 있다, 더 나아가 법위반행위나 불공정한 사업관행에 대해 모니터링을 하거나 조사권을 행사한다. 또한 BBBOnline이나 TRUSTe와 같은 자율규제 차원의

민간 프라이버시 단체[109]로부터 법률이나 가이드라인을 준수하지 않는 사업자에 대한 보고(referral)를 받아 실질적인 제재조치를 취하기도 한다.[110]

5. 일본

1) 개인정보보호법

일본헌법 제21조는 표현의 자유와 통신비밀 보장에 관하여, 제35조는 주거 불가침 등을 규정하고 있어 간접적인 의미에서 프라이버시권을 보호하고 있다.[111] 그러나 헌법 제21조는 프라이버시의 측면에서 통신비밀의 보호라는 부분이 강조되고 있기는 하지만 전반적으로는 언론·출판 등 표현의 자유에 좀 더 비중이 있는 것으로 보인다.[112] 또한 제35조 역시 소

---

109) BBBOnline은 미국의 대표적인 소송외 분쟁해결단체인 'The Council of Better Business Bureaus(CBBB)'의 분야별 산하조직 중 하나인데, CBBB는 1912년 설립되어 오늘날에 이른 미국의 대표적인 소송외적 분쟁해결단체이다. 현재 전미 지역에 약 300,000여개의 사업자들이 회원으로 가입하고 있는데, CBBB는 각 지역별로 'Better Business Bureau(BBB)'를 설립하여 네트워크화함으로써 전국적인 BBB 시스템을 구축하고 있다. 한편 BBBOnline 외 TRUSTe도 민간단체로서 프라이버시에 대한 신뢰마크를 부여하고 필요한 경우 분쟁조정을 해주는 구조를 갖추고 있으나, 개인정보와 관련한 분쟁의 해결은 BBBOnline의 역할이 더 크다. (이은선, "온라인을 통한 소송외적 분쟁해결에 관한 고찰", 「개인정보연구 2권 1호」,2003 .7, 291면 이하 참조.) (http://www.bbbonline.org 참조.)

110) 문성제, "온라인상에서의 개인정보보호에 관한 국제 동향 -미국의 제도를 중심으로", 「비교법학연구 3집」, 2004. 2, 14면 이하.

111) 제21조(집회·결사·표현의 자유와 통신비밀)
① 집회·결사 및 언론·출판 기타 모든 표현의 자유는 보장되어야 한다.
② 어떠한 검열도 행해져서는 안 되며 모든 통신비밀도 침해되어서는 안 된다.
제35조(주거불가침)
① 주거, 서류 및 소지품에 대한 침입 및 압수·수색을 받지 않을 권리는 제33조의 경우를 제외하고는 정당한 이유가 있는 경우에만 침해될 수 있을 뿐이고 수색장소 및 압수물건을 명시한 영장이 없는 한 침해되어서는 안 된다.
② 각각의 수색 또는 압수는 권한 있는 사법 관헌이 발행한 별도의 영장에 의하여 행해져야 한다.

112) 실제로 표현의 자유는 일본 헌법상에서 다른 기본권보다 우월적 지위를 인정받고 있다고 한다. (한영학, "일본의 개인정보보호 법제", 「세계언론법제동향」, 2000. 12, 1면 참조.)

극적인 의미의 주거불가침을 선언하고 이를 침해할 시에는 적정한 절차에 의하여야 한다는 원칙을 천명하는 수준이다. 따라서 적극적인 의미의 프라이버시권의 보장이나 또는 개인정보자기결정권에 대한 명시적인 헌법적 근거는 없는 것으로 보인다.

그러나 일본은 1970년대부터 개인정보보호를 위한 법체계를 도입하기 시작한 세계적인 흐름에 맞춰 공공부문을 중심으로 개인정보보호법 제정에 대한 논의를 본격적으로 시작하였고 2003년에는 민간부문에 적용되는 개인정보보호법을 비롯하여 총 5개의 개인정보 관련 법령을 새롭게 정비하였다. 이렇듯 일본이 민간과 공공부문에서 '개인정보보호법'이라 불릴만한 법제도를 정비한 것은 아주 최근의 일이다. 그 이전에는 미국과 유사한 개인정보보호 법제를 유지하고 있었기 때문에, 개인정보보호에 관한 기본법이라고 할 수 있는 법이 없었고, 전문적인 개인정보보호기구도 없었다. 다만 각 개별 법률을 관장하는 주무 행정부처가 부분적으로 개인정보보호의 역할을 담당하였을 뿐이다. 따라서 개인정보피해구제의 역할은 민간단체의 소송외적 분쟁해결제도나 법원의 소송에 의하는 것이 대부분이었다.

일본은 1970년대 들어 전산화된 개인정보 처리가 활발히 진행되면서 공공부문을 중심으로 전산화된 방법을 통한 개인정보처리를 규율할 필요성이 제기되기 시작하였다. 이러한 움직임은 1975년 쿠니타치(國立)市가 최초로 「개인정보보호조례」를 제정하는 것으로 시작[113]되어, 1976년 공공부문의 컴퓨터로 처리되는 개인정보처리에 적용되는 「전자계산기처리

113) 현재 일본에서는 지방자체단체가 보유하고 있는 개인정보의 처리는 대부분 해당 지방자치단체가 제정한 조례, 규칙 또는 규정에 의해 규율되고 있다. (김현수, "일본의 개인정보 관련 법제 동향과 법률 분석", 「IT법 연구」, 2007. 8, 1면.)

정보보호관리준칙」의 제정으로 이어졌다. 1970년대 중반을 전후로 하여 지방자치단체와 통상산업성(通商産業省) 및 기타 행정부처를 중심으로 시작된 정부 차원에서의 개인정보보호 문제에 대한 논의는 1980년대 들어 「OECD 가이드라인」의 영향으로 더욱 가속화되어, 1988년 「행정기관이보유하는전자계산기처리에의한개인정보보호에관한법률」의 제정에 많은 영향을 끼쳤다. 동법은 행정기관이 보유하고 있는 개인정보를 컴퓨터 등 전자화된 방법에 의해 처리하는 경우 개인정보의 적정한 취급방법에 대해 규정하고 있다.

반면 민간분야에서는 개인정보보호법이라 불릴 만한 법규범은 없었다. 1988년 공공부문에 적용되는 개인정보보호법 제정 당시 민간부문의 개인정보도 포함할 것인지에 대한 논의가 있기는 하였으나, 행정부처 간의 권한 분배 문제로 인한 갈등과 자유로운 기업 활동에 지장을 줄 우려가 있다는 주장으로 인하여 민간부문에 대한 개인정보 규정은 포함되지 못하였다. 따라서 민간부문에서는 개인정보보호를 위해 적용할 수 있는 일반적인 법률은 없었으며 대부분 정부의 지침이나 민간 자율단체의 가이드라인이 그 역할을 대신하여 왔다.[114] 따라서 일부 개별 법률에서 개인정보보호를 위한 관련 규정들[115]이 있어 개인정보침해에 대한 규제를 가할 수

114) 1989년 일본 통산성은 컴퓨터와 인터넷이 빠르게 보급됨에 따라 민간부문에서의 개인정보 침해가능성이 증가하자, 이에 대비하여 「개인정보보호가이드라인」을 제정한 바 있다. 또한 1998년 10월에는 「민간부문에서의전자계산기처리에관한개인정보보호가이드라인」을 제정하여 고시하였다. 한편 많은 사업자단체도 이러한 통산성의 가이드라인에 맞춰 업계의 자율적인 가이드라인을 마련하여 실행하였는데, 그 대표적인 예가 B2C 전자상거래 활성화를 위해 활동하고 있는 ECOM이 1998년 3월 마련한 「민간부문의전자상거래에서의개인정보보호에관한ECOM가이드라인」이다. 동 가이드라인은 전자상거래 산업체가 준수하여야 할 적정한 개인정보취급관행을 규정하고 있다.

115) 전기통신분야의 통신비밀보호에 관한 규정으로 「전기통신사업법」 제4조 제1항 및 제2항 등이 있으며, 개인 신용분야에서는 「개인신용부정경쟁방지법」, 「할부판매법」, 「대금업의규제에관한법률」 등이 있다. 또한 의료분야에서는 「형법」 제134조의 비밀누설금지의무 규정, 「의료방사선기사법」 제29조의 비밀준수의무 규정, 「의료법」 제21조 등이 있다.

있었지만, 대부분의 경우 개인정보침해는 민법에 기초한 불법행위 책임의 문제로 다루어져 프라이버시 침해에 대한 손해배상청구만 가능하였을 뿐이다.

이렇듯 일본은 공공부문에 한정되어 적용되는 개인정보보호법만을 두고 있고 민간부문에 대해서는 특정 영역을 제외하고는 별도의 법적 규제를 가하지는 않았다. 그러나 1990년대 후반 들어 인터넷의 보급과 이용증대로 인한 개인정보침해의 증가는 일본 정부로 하여금 업계의 자율적인 노력만으로 민간 부분에서 충분한 개인정보보호 체계를 확보하는 것은 한계가 있다는 판단을 하도록 하였다. 실제로 일본은 침체되어 있는 일본 경제를 되살릴 수 있는 전략의 한 방안으로 전자상거래를 비롯한 정보통신기반산업의 육성을 정책으로 삼고 1994년 8월 내각에 총리대신을 본부장으로 하는 '고도정보통신사회추진전략본부(IT 전략본부)'를 설치하는 등 많은 노력을 기울인 결과, 정보화가 빠르게 진행되었다.

그러나 이러한 정보화의 급격한 진행은 공공부문은 물론이고 민간부문에서도 개인정보침해가 심각한 문제로 야기되는 결과를 초래하였다.[116] 이에 일본 정부는 2000년 '개인정보보호법제화전문위원회'를 설치하여 새로운 개인정보보호법제 마련을 위한 검토 작업에 착수하게 되었고, 같은 해 10월 '개인정보보호기본법에관한대강'을 마련하였다. 일본 정부는 이를 바탕으로 2001년 3월 국회에 '개인정보보호에관한법률(안)'을 제출하였으나 2년이 넘게 논의를 거듭하다 결국 언론과 시민단체의 강력한 반대에 부딪쳐 2002년 12월 폐기되었다. 동 법안은 ① 이용목적에 의한 제한, ②

116) 일본 내각부가 실행한 설문조사에 의하면, 일본 국민의 69%는 행정기관과 민간영역의 사업자가 관리하는 개인정보가 '본인 승낙 없이 외부에 유출되고 있다고 느낀다'고 답하였고, 78.4%는 '프라이버시 침해가 증가한 것 같다'고 응답하였다. (개인정보분쟁조정위원회, 전게서, 265면 이하 참조.)

적정한 방법에 의한 취득, ③내용의 정확성 확보, ④ 안정보호조치의 실시, ⑤ 투명성의 확보라는 개인정보보호 기본 5원칙을 제시하였는데, 언론단체 및 야권과 시민단체는 동 원칙의 내용이 지나치게 포괄적이어서 헌법상 보장되는 언론의 취재보도의 자유를 침해할 가능성이 높다고 하여 반대의사를 밝혔었다. 이에 일본 정부는 당초의 입장에서 다소 후퇴하여 가장 논란이 되었던 5가지 기본원칙을 삭제하고 적용범위를 다소 변경한 새로운 법률을 마련하여 의회에 제출하였다.[117] 이 법안은 2003년 5월 23일 참의원을 통과한 뒤 법률로 성립되어 5월 30일 공포되었다.

이 때 새롭게 정비된 법률로는 「개인정보보호에관한법률(個人情報の保護に關する法律)」(이하 '개인정보보호법'이라 한다), 「행정기관이보유하는개인정보보호에관한법률(行政機關の保有する個人情報の保護に關する法律)」(이하 '행정기관개인정보보호법'이라 한다), 「독립행정법인등이보유하는개인정보보호에관한법률(獨立行政法人等の保有する個人情報の保護に關する法律)」(이하 '독립행정법인개인정보보호법'이라 한다), 「정보공개・개인정보보호심사회설치법(情報公開・個人情報保護審査會設置法)」(이하 '심사회설치법'이라 한다), 「행정기관이보유하는개인정보보호에관한법률등의시행에따른관계법률의정비등에관한법률(行政機關の保有する個人情報の保護に關する法律の施行に關係法律の整備等に關する法律)」(이하 '관계법률정비법'이라 한다) 등이 있다.

117) 새롭게 제출된 법안은 기존 법안과는 달리 ① 개인정보보호 기본 5원칙을 삭제하였고, ② 법적용 제외대상으로 보도기관, 학술연구기관, 종교단체, 정치단체 외 '저술업을 행하는 자'를 추가하였으며, ③ 적용제외대상 기관에 대해서는 개인정보보호주무장관이 권한을 행사하지 않는다는 것을 명문화하였다. 즉, 새 법안은 기존 법안에 대한 비판을 반영하여 개인의 표현의 자유와 언론보도의 자유를 최대한 보장하고 이에 대한 정부의 간섭을 최소화하고 있다.

[표3-12] 일본의 개인정보관련 법제 현황

법률명	적용범위	내용
개인정보보호법	민간부문 공공부문	• 개인정보의 적정한 취급에 관한 기본원칙 규정 • 국가, 지방자체단체의 책무 규정 • 민간 개인정보취급사업자의 의무 규정 • 사업자 및 인정개인정보보호단체에 의한 자율적인 피해구제제도 규정
행정기관개인정보보호법	공공부문	• 일반 행정기관이 보유하는 행정문서에 기록된 개인정보의 적정한 취급 원칙 • 이용목적 달성에 필요한 범위 내에서 개인정보 보유 • 개인정보 목적 외 이용 및 제공 금지 • 정보주체의 열람, 정정, 이용정지청구권 인정
독립행정법인개인정보보호법	공공부문	• 독립행정법인, 행정목적 수행을 위한 특수법인, 인가법인은 대상개인정보, 개인정보 취급규모, 관리규칙, 정보주체의 권리, 피해구제제도 등에 있어서 일반 행정기관과 동일하게 취급함
심사회설치법	공공부문	• 정보공개심사회의 설립에 관한 규정 • 개인정보의 열람, 정정, 이용정지신청에 대한 행정기관 등의 결정에 대한 불복신청과 관련하여 자문을 행함
관계법률정비법	공공부문	• 등기, 형사소송, 특허 등과 관련된 정보에는 행정기관개인정보보호법 등 적용제외

2) 개인정보보호기구

2003년 제정된 일본의 「개인정보보호법」, 「행정기관개인정보보호법」 등은 개인정보보호를 위한 특별 전담기구의 설치에 대해서 별도의 규정을 두고 있지 않다. 따라서 일본에서는 지금까지 개인정보보호기구라

고 부를 만한 전문적인 기구가 없었기 때문에 개인정보보호기구를 통한 피해구제의 역할도 소극적일 수밖에 없었다. 즉 정부 차원에서는 개별 영역을 담당하는 소관 주무부처가 개인정보보호의 역항을 부수적으로 수행하여 왔을 뿐 당사자 간 분쟁해결 등을 통한 피해구제의 역할을 담당하지 않았다. 따라서 개인정보피해는 순수하게 법원 또는 사업자의 자율적인 소비자 불만해소 절차를 통하여 이루어지는 것이 대부분이었다. 그러나 「개인정보보호법」은 국가, 지방자치단체, 사업자에게 각각 정보주체의 불만해소를 위한 고충처리제도를 마련하도록 규정함으로써, 신속하고 적절한 개인정보피해구제를 강조하고 있다.

정부차원에서는 각 개별법률 또는 해당 영역을 관장하는 소관 주무부처가 개인정보보호의 역할을 맡고 있단. 「개인정보보호법」도 주무대신에게 이러한 의미에서 개인정보보호를 위한 권한을 부여하고 있는데, 동법 제32조～제34조에서 규정하고 있는 주무대신의 권한을 살펴보면, ① 개인정보취급사업자 및 인정개인정보보호단체로부터 필요한 경우 개인정보 추급 등에 대한 보고를 받을 수 있으며, ② 사업자에게 필요한 사항을 조언할 수 있고, ③ 개인정보취급사업자가 의무규정을 위반하였을 경우 그러한 행위의 중지 또는 시정의 권고를 할 수 있다. 아울러 ④ 사업자가 정당한 이유 없이 권고를 무시하여 개인의 중대한 권리・이익이 침해될 위험이 있을 경우에는 권고 이행 명령을 내릴 수 있으며, 긴급한 조치가 필요하다고 인정될 때에는 사업자에게 의무위반행위의 중지명령 및 시정명령을 내릴 수 있다.

민간차원에서는 신뢰마크 제도를 바탕으로 자율적인 분쟁해결을 하고 있는데, 통산성 산하 '일본정보처리개발센터(JIPDEC : Japan Information

Processing Development Center)'가 운영하는 것과 우정성 산하 일본 '데이터통신협회'가 운영하는 제도가 있다. JIPDEC의 경우 전자상거래 활성화 차원에서 개인정보보호 가이드라인을 설정하고 인터넷에서의 개인정보보호 관련 연구를 수행하는 기관으로 프라이버시마크제도의 운영도 책임지고 있다. 그리고 우정성 산하 일본데이터통신협회는 '개인정보보호등록센터'를 개설하여 1998년부터 개인정보보호마크제도를 시행하고 있다.[118]

6. 홍콩

1) 개인정보보호법

홍콩은 영국의 영향을 많이 받은 역사적 특수성으로 인하여, 아시아권에서는 비교적 빨리 개인정보보호를 위한 법제를 도입·운영하고 있다. 홍콩에서 개인정보보호를 위한 법제도의 도입에 대한 논의가 본격적으로 시작된 것은 1994년 법률개혁위원회(LRC : Law Reform Commission) 산하 프라이버시소위원회가 정보보호를 위한 법제 도입에 관한 보고서를 제출하면서부터이다. 법률개혁위원회는 동 보고서에서 다른 국가의 프라이버시보호제도를 조사·분석한 내용을 바탕으로 각국이 개인정보보호를 위해 취하는 접근방법을 크게 3가지로 구분하였는데, ① 개인정보 관련 법률을 제정하고 전담규제기구를 설치하는 방안, ② 프라이버시 침해에 대한 불법행위를 인정하여 민사소송을 허용하는 방안, ③ 자발적인 실행 규약이나 자율적인 시장 감시 등 자율규제를 촉진하는 방안이 그것이다. 법률개혁위원회는 이러한 3가지 방안 중 명확한 개인정보관련 제정법의 마련을 통한 법적 규율체계를 구비하고 이를 시행할 규제기구를 설치하는

118) 강신원, "B2C 활성화를 위한 개인정보보호제도와 정책 방향", 「개인정보연구 2권 1호」, 2003. 7, 194면.

접근방법을 채택하는 것이 홍콩의 이익에 가장 부합한다고 결론지었다.[119]

홍콩은 법률개혁위원회의 최종 보고서에 따라, 1995년 8월 3일 「개인정보법(Personal Data Ordinance)」을 제정하였으며, 동법에 근거하여 개인정보보호를 위한 프라이버시 감독기구로서 '개인정보(프라이버시)커미셔너(PCO : Privacy Commissioner for Personal Data)'를 설치하여 개인정보보호를 위한 제도를 정비하였다. 특히 홍콩은 개인정보보호법과 개인정보보호기구를 도입함에 있어 영국은 물론 호주나 뉴질랜드, 캐나다의 모델을 많이 참조하여 체계를 갖추었다.

1995년 제정된 「개인정보법」은 1996년 12월 20일 발효되어 시행되고 있다. 동법은 생존하고 있는 개인과 직·간접적으로 관련 있는 모든 개인정보에 적용되며, 개인정보를 수집·보유·처리·이용하는 모든 자에게 적용된다. 따라서 기업, 비영리단체, 행정부처, 기타 공공기관 등 모든 정보이용자의 개인정보 처리행위를 규율하고 있다. 또한 동법 부칙은 국제적 표준에 맞춘 6가지 기본적인 정보보호원칙(DPP : Data Protection Principles)을 규정하고 있는데, 동 원칙은 개인정보의 수집방법과 목적, 보유한 정보의 정확성 확보 및 보유기간, 개인정보의 이용 및 보호를 위한 안전조치 확보, 일반적으로 이용 가능한 정보, 개인정보 접근에 관한 내용을 담고 있다.

119) Raymond Tang, *Remedies for Personal Data Infringements under the Personal Data(Privacy) Ordinance*, International Conference on Personal Data Protection 2002 in Seoul, 2002, p.1.

[표3-13] 홍콩의 정보보호 6원칙

구분	내용
개인정보의 수집	• 불공정하고 불법적인 방법에 의한 개인정보 수집금지 • 개인정보의 수집목적 고지
개인정보의 보유	• 보유하고 있는 개인정보의 정확성, 최신성, 완전성 확보 • 목적달성 이후 개인정보 파기
개인정보의 안전	• 개인정보의 손실 등으로부터의 안전조치 확보
일반적으로 제공되어야 할 정보	• 정보이용자의 개인정보보호방침에 대한 고지 • 정보이용자가 보유하는 개인정보를 정보주체에게 고지 • 정보이용자의 개인정보 이용목적을 정보주체에게 고지
개인정보 접근	• 정보주체의 개인정보 열람·정정권 보장

이러한 정보보호원칙을 비롯하여 정보주체는 「개인정보법」에 의해 많은 권리를 향유하고 있다. 즉 정보주체는 ① 개인정보가 공정한 방법에 의해 수집될 권리, ② 이용목적에 대하여 고지 받을 권리, ③ 오직 필요한 정보만을 제공할 권리, ④ 이용목적 변경 등에 대하여 기존의 동의를 보류할 권리, ⑤ 정확하고 안전하게 개인정보가 보유되고 관리될 권리, ⑥ 개인정보 열람권, ⑦ 개인정보 정정권, ⑧ 공개요구권 등의 권리를 보장받고 있다. 이 외에도 동법은 개인정보보호기구인 홍콩의 '개인정보커미셔너'의 설립, 권한, 기능에 대한 규정과 정보조합프로그램의 사용규제, 실행규약의 제정 및 고시, 정보이용자의 등록 및 그 관리 등에 관한 규정을 함께 포함하고 있다.

2) 개인정보보호기구

홍콩의 개인정보커미셔너는 정보처리자의 「개인정보법」 이행을 확보하고 개인의 프라이버시를 보호하는 임무의 실현을 위해, 1996년 8월 1일 설립된 독립법정기구이다. 개인정보커미셔너는 홍콩 행정특별구역 장관(Governor)에 의해 직접 임명되며, 법률에 의해 설립된 독립기구로서 예산지원은 재무부에서 받으나 인사권 행사나 각종 활동을 독자적으로 수행한다.

커미셔너는 홍콩 내에서 이루어지는 모든 개인정보의 처리행위, 즉 민간부문과 공공부문 모두에서의 개인정보 수집・이용・제공・저장 등에 대하여 조사하고 감독한다. 또한 커미셔너는 각 분야별로도 특별한 관심을 보이고 있어 의료정보, CCTV를 통한 프라이버시 침해, 신용정보보호, 정보통신분야에서의 개인정보보호, 근로자정보의 보호, 다이렉트 마케팅과 개인정보보호 등에 관하여 각종 지침이나 프라이버시규약을 제정・고시하는 등 프라이버시와 관련된 모든 분야를 다루고 있다.

이러한 커미셔너의 주된 임무는 효율적이고 효과적인 방법을 통해 홍콩 개인정보법의 준수여부를 조사・감독하고 법규에 적합하게 개인정보를 취급하는 관행을 장려함으로써, 개인정보를 보호하고 개인의 프라이버시를 지키는 것이다. 이를 위한 홍콩 개인정보커미셔너의 주된 기능을 살펴보면, ① 의견제시 및 분쟁조정을 통한 개인정보 피해구제, ② 정보보호원칙 등 법규준수여부 및 침해행위에 대한 개인정보보호 실태조사 및 감독・규제, ③ 실행규약 제정 등을 통한 자율규제활동의 지원, ④ 각종 법령 질의처리 및 정보제공, ⑤ 정책자문 및 입법안 검토 및 심의, ⑥ 개인정보관련 조사・연구, ⑦ 개인정보보호를 위한 교육 및 홍보, ⑧ 국・내외 유관기관 협력 등이 있다.

제4장 전자거래에서의 개인정보보호 침해 및 구제

제1절 전자거래에서의 개인정보 침해유형

Ⅰ. 개인정보의 수집

전자거래에 있어서 개인에 관한 정보를 해당 개인의 승낙이나 동의 없이 수집·저장하는 것은 프라이버시의 침해에 해당한다.[120] 누구나 자유롭게 접근할 수 있는 개인정보란 존재하지 않기 때문에 개인정보 수집·저장의 단계에서부터 보호되어야 한다. 개인정보의 수집은 그 자체만으로도 타인의 정보를 이용하는 것이므로 개인정보의 비밀적인 수집은 자신의 개인정보처리를 자신만이 결정할 수 있는 자기결정권을 침해하는 것이다.[121] 따라서 전자거래 분야에 있어서 개인정보는 해당 개인에 대한 사전고지 및 그로부터의 동의 및 승낙을 전제로 하여 수집되어야 하고, 개인정보가 수집되는 목적은 정보의 수집과 동시에 공개되어야 한다.

또한 개인정보는 수집 목적에 필요한 범위 내에서만 최소한으로 수집되어야 한다. 합리적인 범위를 넘어서는 불필요한 정보의 수집 및 과다한 정보의 수집은 그 자체로 정보프라이버시권을 침해할 가능성이 크고 정보유통과정에서 다른 목적으로 사용될 위험성이 있으므로 원칙적으로 제한되어야 한다.

---

120) 사법연수원, 전게서, 43면 이하.

121) 쿠키(cookies)를 통한 자동정보 수집 프로그램에 의한 개인정보 수집은 승낙 없이 이용자의 개인정보를 수집하는 대표적인 예이다. 이에 대한 자율적 규율의 방안으로 ① 웹서비스상 이용약관의 쿠키에 대한 보호에 관한 내용 삽입, ② 보안확보, ③ 가이드라인의 설정 등의 방법이 논의되고 있다. (최명구, "디지털 사회의 개인정보보호 -쿠키(Cookie)를 중심으로", 「인문사회과학연구 4권」, 부경대학교 인문사회과학연구소, 2004, 89면 이하 참조.)

Ⅱ. 개인정보의 2차적인 사용 (secondary use)

1. 개인정보의 가공 및 결합

전자거래 분야에 있어서 개인의 동의 및 승낙 하에 수집·저장한 개인정보라 하더라도 해당 정보의 가공 및 결합[122] 단계에서의 잘못된 편집 또는 고의적 변조, 조작의 위험성이 있으므로 이러한 단계에서 해당 개인의 사전 동의와 승낙이 있어야 한다.

해당 개인과 체결한 계약의 목적을 달성하기 위한 경우나 계약과 유사한 신뢰관계에 기초한 목적의 범위 내 또는 정보처리자의 정당한 이익을 유지하기 위하여 필요한 경우에는 어느 정도의 임의적 가공이 허용될 수 있으나, 이러한 경우에도 당해 개인의 정보프라이버시권의 본질적인 내용을 침해하여서는 안 된다.

2. 개인정보의 유통

전자거래에 있어서 개인정보의 유통은 수집, 저장 또는 가공된 개인정보를 제3자에게 이전하거나 이를 열람할 수 있도록 하는 방법으로 제공하는 것을 말한다. 최근에는 대가를 지불하고 개인정보를 매수하여 이를 제3자에게 판매 또는 대여하는 정보중개업을 전문적으로 하는 기업까지 생

122) 최근 정보통신기술의 발달에 따라 특정 목적을 위하여 수집한 개인정보들을 서로 결합하고 조작하여 2차, 3차 정보를 생성하는 사례가 많아지고 있을 뿐만 아니라, 전자거래의 활성화와 더불어 개인정보는 기업 경영의 중요한 자원으로서 상업 목적에 전략적으로 이용되고 있고, 나아가 개인정보 자체가 경제적 가치가 있는 상품으로 무단 거래되는 경향이 증가하고 있어 이로 인한 개인정보 침해의 우려가 더욱 높아지고 있다.

겨나고 있는데다가 인터넷의 발달로 인하여 개인정보의 국가 간 이동(Transborder Data Flow)에 의한 프라이버시 침해 문제가 크게 대두되고 있다.[123]

개인정보의 제3자에 대한 노출은 정보주체의 이익을 가장 크게 침해할 가능성이 있으므로 해당 개인의 동의 또는 승낙이 없는 개인정보의 임의적 유통은 엄격히 제한되어야 하고, 정보처리자에게는 강력한 비밀유지의 무가 부과되어야 한다.

Ⅲ. 개인정보의 오류 (error)

전자거래 시 개인에 대한 정보는 수집 과정에서 개인이 스스로 신고하거나 제공하는 것도 있지만 해당 개인 모르게 작성되는 것도 적지 않아 개인에 대한 정보가 잘못 입력될 가능성이 있다. 또한 고의적이거나 우발적 사고로 인한 정보데이터에 오류가 발생할 수도 있다. 오류가 있는 개인정보의 이용은 기업 측에는 잘못된 정보에 기한 마케팅으로 거래에서 커다란 손실을 초래할 수 있고, 이용자(소비자) 측에서는 심각한 프라이버시 침해를 가져올 수 있다. 특히 잘못된 개인정보의 제3자에의 유통은 더욱 큰 피해를 가져오게 된다.

따라서 정보관리자는 개인정보를 정확하게 수집・보존・관리하여야 하고, 해당 개인에게는 자신의 개인정보가 관리되고 있다는 것이 알려져야 할 뿐 아니라 자신의 정보에 대한 열람권 및 정정권을 보장하여 정보의 오류를 시정할 기회를 주어야 한다.[124]

---

123) 작년 대형 정유사 직원이 고객정보 1000만여 건을 유출한 사건은 사회적으로 큰 파장을 불러왔다. (http://www.ytn.co.kr/_ln/0103_200809090535058777 참조.)

Ⅳ. 개인정보에의 부당한 접근 (improper access)

전자거래 분야에서 개인정보를 처리할 정당한 권한을 가진 자 이외의 자가 저장, 수집, 관리되는 타인의 개인정보에 부당하게 접근하여 이를 남용하는 경우 정보프라이버시 침해가 발생한다. 이에는 해킹과 같이 정보관리시스템에 무단으로 침입하여 타인의 개인정보에 접근하거나 이를 조작·파괴하는 경우뿐만 아니라[125], 정보관리 조직 내의 관계자 및 관련자가 관리되는 개인정보를 처리할 정당한 권한이 없음에도 불구하고 이를 함부로 조작·유출하는 경우가 있을 수 있다.

특히 무단침입과 개인정보의 무단 변경과 파괴 등은 그 결과가 확인되지 않는 경우에는 더욱 심각한 프라이버시의 침해 문제를 야기한다. 따라서 정보관리자에게는 보유 개인정보의 안전을 도모하는 기술적 조치를 취한 의무가 부과되어야 한다.

제2절 전자거래에서의 개인정보 침해에 대한 구제

Ⅰ. 손해배상의 청구

전자거래에서의 개인정보 침해에 대한 손해배상 청구는 해당 개인과 침해자 사이에 일정한 정보통신서비스 이용계약과 같은 법률상의 관계가

124) 이외에도 이용자에게 자신에 관한 정보가 저장되었는지 여부, 정보의 출처와 수령자 및 저장목적 등에 관하여 알려줄 것을 요구하는 '통지청구권', 잘못된 정보의 '사용중지청구권' 및 '삭제청구권', 잘못된 정보를 처리하지 않도록 요구하는 '부작위청구권' 등의 권리가 보장되어야 한다는 주장도 있다. (사법연수원, 전게서, 190면 이하 참조.)

125) 최근 빈번히 발생하는 중국발 해킹의 피해는 큰 사회적인 문제로 부각되고 있다. (http://www.ytn.co.kr/_ln/0102_200904162057426711 참조.)

있는 경우와 그렇지 않은 경우로 나누어 볼 수 있다.[126]

1. 계약위반으로 인한 손해배상청구

개인정보 침해자에게 정보통신서비스 이용계약 등 계약에 기초하여 손해배상을 구하는 경우에는 약관 및 계약 등에서 정보통신서비스제공자에게 이용자 개인정보 처리에 있어서의 주의의무 등을 구체적으로 명시한 경우뿐만 아니라, 침해자가 계약상의 부수적 의무 즉 신의칙상 침해자에게 일반적으로 요구되는 계약 이행 과정에서의 개인정보보호에 관한 주의깊은 처리의무를 위반하였는지 여부가 문제가 된다. 계약 이행과정에서 요구되는 신의칙상 주의의무는 구체적 사정에 따라 다를 것이나, 개인정보보호 관련 법규에서 규정하고 있는 내용들은 침해자에게 요구되는 개인정보보호에 있어서의 주의의무의 기준이 될 수 있다.[127]

그러한 주의의무 위반으로 인하여 이용자에게 재산적 손해 또는 정신적 손해가 발생하였을 경우에는 그 배상책임이 인정될 것이다. 그러나 개인정보의 소재 및 그 구체적인 정보처리과정은 일반적으로 이용자에게 잘 알려져 있지 않은데다가 발생한 손해의 원인도 확정하기가 매우 어려운 점이 있어 개인정보 침해행위에 대한 실질적인 피해구제가 이루어지기는 쉽지 않다.[128]

---

126) 손해배상청구 이외에 일반적으로 명예훼손과 같은 인격권 침해의 사후적 구제방법에 관하여는 민법 제764조에 규정된 명예회복에 적당한 처분으로서 사죄광고와 같은 원상회복 방법이 논의되고 있으나, 이는 개인정보의 침해에 있어서는 그 성격상 적용되기 어려운 점이 있다. (임건면, “개인정보침해에 대한 민사법적 대응”, 「비교사법 8권 1호」, 2000, 89면 이하 참조.)

127) 지원림, “전자거래와 계약법”, 「법학논총 24집」, 2000, 3면 이하.

128) 이러한 점에서 개인정보에 대한 침해의 구제는 손해배상청구라는 사후적 구제보다는 개인정보의 수집, 저장, 관리, 유통 단계에서 해당 개인에 대한 통지 및 관여가 보장되도록 하는 사전적 규제가 더욱 중요한 것이다.

2. 불법행위로 인한 손해배상청구

개인정보의 침해행위로 인하여 불법행위가 성립하기 위한 요건은 일반 불법행위와 다를 바 없다. 즉 고의 또는 과실에 의한 위법행위로 이용자의 개인정보에 관한 권리를 침해하여 손해를 발생하게 한 경우에는 민법 제750조 및 제751조에 의한 손해배상책임이 인정된다. 구체적으로는 개인정보의 관리자가 개인정보의 수집, 저장, 유통의 전 과정에서 개인정보를 위법하게 처리하여 해당 개인에게 손해를 발생시킨 때에는 손해배상책임이 인정되는 것이다.

개인정보 침해행위의 위법성 여부는 그 행위의 구체적인 태양에 따라 다소 다를 수 있으나 일반적으로는 개인정보보호 관련 제반 법규에 규정된 이용자의 개인정보보호 의무를 위반하는 행위로 위법성이 쉽게 인정될 것이지만, 개인정보 침해행위에 대하여 불법행위에 기한 손해배상청구를 하는 경우 침해자의 고의 또는 과실을 입증하는 것은 쉬운 일이 아니다. 이용자가 일반적으로 자신에 관한 개인정보의 수집과 관리 및 유통이 구체적으로 어떻게 이루어지는가를 잘 알지 못하여 개인정보 침해행위에 대한 실질적인 피해 구제가 이루어지지 못할 가능성이 큰 것은 계약위반으로 인한 손해배상청구의 청구와 마찬가지이다.[129]

「정보통신망이용촉진및정보보호등에관한법률」은 제32조에서 정보통신서비스제공자 등의 개인정보의 수집·이용·제공 또는 위탁 등으로 인하여 손해를 입은 이용자는 그 정보통신서비스제공자등에 대하여 손해배상을 청구할 수 있다고 규정하여 개인정보 침해행위에 대한 손해배상청구

129) 이러한 점에서도 정보통신서비스 이용자가 자신과 관련한 개인정보의 소재와 그 처리 및 유통 상황을 정확하게 파악할 권리는 매우 중요하다.

권을 명문으로 규정하는 한편, 이용자의 정보통신서비스제공자 등에 대한 고의·과실에 대한 입증이 사실상 어려운 점을 고려하여 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 못하면 개인정보 침해행위에 책임을 면할 수 없도록 하는 내용의 입증책임의 전환 규정을 두어 이용자를 두텁게 보호하고 있다.[130][131]

Ⅱ. 사전적 예방 및 방해배제

일반적으로 프라이버시와 같은 인격권은 일단 권리가 침해된 경우에는 손해배상 또는 원상회복과 같은 사후적 구제수단만으로는 충분한 보호가 이루어지지 않는다. 프라이버시권과 밀접한 관련을 가지는 개인정보에 관한 권리 역시 사전적 예방 및 방해배제 등이 더 실효성 있는 구제수단이 될 수 있다.

---

130) 제32조(손해배상) 이용자는 정보통신서비스 제공자등이 이 장의 규정을 위반한 행위로 손해를 입으면 그 정보통신서비스 제공자등에게 손해배상을 청구할 수 있다. 이 경우 해당 정보통신서비스 제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

131) 「신용정보의이용및보호에관한법률」(1995. 1. 5. 제정 법률 제4866호, 2009. 4. 1. 제20차 개정 법률 제9617호 시행일 2009. 10. 22.) 제43조도 신용정보업자 또는 신용정보의 이용자가 이 법의 규정을 위반함으로써 신용정보주체에게 피해를 입힌 경우에는 손해배상의 책임을 지되, 다만 고의 과실이 없음을 입증한 경우에는 그렇지 않다고 규정하고 있다.

제43조(손해배상의 책임) ① 신용정보회사등과 그 밖의 신용정보 이용자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 손해배상의 책임을 진다. 다만, 신용정보회사등과 그 밖의 신용정보 이용자가 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

② 채권추심회사 또는 위임직채권추심인이 이 법을 위반하여 채무자 및 그 관계인에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다. 다만, 채권추심회사 또는 위임직채권추심인이 자신에게 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

③ 제4조제1항의 업무를 의뢰받은 신용정보회사가 자신에게 책임 있는 사유로 의뢰인에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다.

④ 제17조제2항에 따라 신용정보의 처리를 위탁받은 자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 위탁자는 수탁자와 연대하여 손해배상책임을 진다.

⑤ 위임직채권추심인이 이 법 또는 「채권의공정한추심에관한법률」을 위반하여 채무자나 채무자의 관계인에게 손해를 입힌 경우 채권추심회사는 위임직채권추심인과 연대하여 손해배상책임을 진다. 다만, 채권추심회사가 자신에게 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

따라서 침해자가 개인정보보호 관련 법규에서 정해진 정보통신망서비스 이용자의 권리 즉, 이용자에 대한 사전 고지권 및 통지권, 이용자의 동의권, 열람 및 정정청구권 등을 침해하여 이용자의 개인정보 수집 및 가공, 제3자에게 제공 등의 행위를 하는 경우 이러한 행위에 대한 사전억제, 즉 권리의 방해예방청구권과 이미 발생하여 계속되고 있는 침해행위의 제거, 정지 등의 금지청구권을 행사할 수 있는지 여부가 문제가 될 것이다.

정보프라이버시권등 개인정보에 대한 권리는 인격권의 일종으로 볼 수 있으므로 인격권 침해에 대한 방해배제 및 예방청구권 등의 인정 여부에 대한 논의[132] 및 판례[133]의 입장 등에 비추어 보면 개인정보의 침해행위에 관하여도 사전구제수단으로서 방해배제 및 예방청구권을 인정함이 타당할 것이다.[134]

제3절 전자거래에서의 개인정보 침해구제제도 개선방안

앞서 전자거래 시 발생하는 개인정보 침해에 해단 구제로서 손해배상의 청구와 침해의 사전적 예방과 배제를 알아보았다. 물론 이와 같은 침해구제방안은 민사적 해결방법으로서 상당한 효과를 가질 수 있다. 하지만 이와 더불어 제도적인 보완이 뒷받침되어야 더욱 효율적인 구제가 가

132) 대체로 이를 인정하는 견해가 다수이고, 다만 그 인정 근거로는 물권적 청구권 확대 적용설, 불법행위의 효과로 인정하는 설 및 고유의 인격권설 등 여러 가지 다양한 논의가 있다. (사법연수원, 전게서, 368면 이하 참조.)

133) 대법원 1996. 4. 1. 선고 93다 40614, 40621 판결은 “인격권은 그 성질상 일단 침해된 후의 구제수단(금전배상이나 명예회복 처분 등)만으로는 그 피해의 완전한 회복이 어렵고 손해전보의 실효성을 기대하기 어려우므로, 인격권 침해에 대하여는 사전(예방적) 구제수단으로 침해행위 정지·방지 등의 금지청구권이 인정된다”는 이유로 허위비방광고로 인한 인격권 침해에 대한 사전구제수단으로 원고의 광고 중지 청구를 인용하였다.

134) 구체적인 권리행사방법은 부작위청구의 소 또는 부작위청구의 가처분신청 등이 될 것이다.

능할 것이다. 이하에서는 제도적 관점에서 현행 전자거래 개인정보보호법제와 개인정보보호기구의 문제점을 알아보고 그에 대한 개선방안을 알아보기로 한다.

Ⅰ. 전자거래 개인정보보호법

1. 현행 전자거래 개인정보보호법제의 문제점

우리나라의 개인정보보호 법제도가 가지는 대표적인 특징은 각 영역별로 개별법에서 개인정보보호와 관련된 규정을 두고 있다는 것이다. 즉, 공공, 민간, 전자상거래, 통신, 의료, 금융 등 각 분야별로 개인정보에 관한 법률이 제정되어 있거나 관련 조항이 포함되어 있다.[135] 이 중 대표적인 전자거래 개인정보보호 관련 법률로 제시할 수 있는 것으로는 「전자거래기본법」, 「전자서명법」, 「공공기관의개인정보보호에관한법률」, 「정보통신망이용촉진및정보보호등에관한법률」, 「신용정보의이용및보호에관한법률」 등을 들 수 있으며, 관련 고시로 舊정보통신부가 제정한 「개인정보보호지침」을 들 수 있다. 또한 이 외에도 「금융실명거래및비밀보장

135) 이와 관련하여 총40여개 법령, 총150여개의 조문이 있다. 「건강검진기본법」, 「건축법」, 「결혼중개업의관리에관한법률」, 「공공기관의개인정보보호에관한법률」, 「공공기관의정보공개에관한법률」, 「공공기록물관리에관한법률」, 「공직자윤리법」, 「교육관련기관의정보공개에관한특례법」, 「국가공무원법」, 「국민의형사재판참여에관한법률」, 「근로자참여및협력증진에관한법률」, 「근로자퇴직급여보장법」, 「도로교통법」, 「도서관법」, 「보험업법」, 「복권및복권기금법」, 「생명윤리및안전에관한법률」, 「선원법」, 「소비자기본법」, 「수상레저안전법」, 「아동복지법」, 「암관리법」, 「여권법」, 「위치정보의보호및이용등에관한법률」, 「유비쿼터스도시의건설등에관한법률」, 「의료법」, 「인터넷주소자원에관한법률」, 「인터넷멀티미디어방송사업법」, 「자동차관리법」, 「장애인차별금지및권리구제등에관한법률」, 「전기통신사업법」, 「전자거래기본법」, 「전자상거래등에서의소비자보호에관한법률」, 「전자서명법」, 「전자정부법」, 「정보통신기반보호법」, 「정보통신망이용촉진및정보보호등에관한법률」, 「정보화촉진기본법」, 「채권의공정한추심에관한법률」, 「한국장학재단설립등에관한법률」, 「혈액관리법」, 「환경보건법」, 「6·25전사자유해의발굴등에관한법률」 등이다.
(국회법률지식정보시스템 참조 http://likms.assembly.go.kr)

에관한법률」을 비롯하여 「통신비밀보호법」, 「전자상거래등에서의소비자보호에관한법률」 등이 전자거래 개인정보보호와 관련된 법률로 인용되고 있다.

이처럼 우리나라의 경우 전자거래 개인정보와 관련된 법규정이 여러 법률에 산재되어 있는데, 이로 인해 통일적인 전자거래 개인정보보호원칙에 입각하여 국가적 차원에서 전자거래 개인정보정책을 수립·시행하기가 어려운 문제점을 안고 있다. 우리나라 전자거래 개인정보보호법제가 안고 있는 문제점은 다음과 같다.

우선, 우리나라는 통일적인 전자거래 개인정보보호원칙이나 법규범이 없기 때문에 개별적인 개인정보 관련 법률규정이 존재하지 않은 영역에서 수집·이용되는 개인정보는 법적으로 보호받을 수 없는 사각지대가 발생할 수 있다. 물론 「전자거래기본법」과 「전자서명법」 등 전자거래 관련 개인정보보호법이 마련되어 있기는 하나, 이는 각각의 법이 '전자거래에 있어서 개인정보보호'에 중점을 둔 것이 아닌 각각의 분야에서의 기본법적인 성격을 지니기 때문에, 전자거래 개인정보보호법에 국한되었다고 할 수가 없다. 그러므로 현재의 입법체계는 새로운 기술의 등장 또는 변화하는 사회상에 따라 갑자기 전자거래에 있어서 개인정보 침해 문제가 제기되는 경우에는 그에 해당하는 법률 규정을 포함시켜야만 보호대상으로 삼을 수 있게 되어 있는데, 법률의 제정이 사회의 변화를 항상 충실히 반영하고 있지는 못하기 때문에 법적 보호와 현실의 간격이 커질 수밖에 없는 한계가 있다.[136]

136) 성낙인 외, 「개인정보보호법제에 관한 입법평가」, 한국법제연구원, 2008, 370면 이하.

다음으로, 전자거래 개인정보보호법이라 일컬어지고 있는 법률들의 경우에도 실질적으로 관련되는 영역에 모두 적용되는 것이 아니고 그 중에서도 특정한 조건을 두어 적용범위를 한정시키고 있을 뿐만 아니라, 그와 같은 법률 상호간에도 일관성이 없다는 문제점이 있다. 예를 들어 「정보통신망이용촉진및정보보호등에관한법률」의 경우 비교적 OECD 가이드라인의 개인정보보호 8원칙 및 EU 지침의 여러 기본 원칙들을 잘 반영하고 있는 반면, 「전자거래기본법」과 「전자서명법」 등은 그렇지 못한 점이 많다. 예를 들어 수집된 개인정보의 제3자 제공에 대한 명확한 한계나 제한 규정을 두고 있지 않아 사실상 개인정보가 유통되거나 무제한 활용될 위험을 내포하고 있어 정보주체의 권리가 상당수 배제되는 결과를 낳고 있다.

2. 전자거래 개인정보보호기본법의 제정

우리나라 전자거래 개인정보보호법제가 가지는 문제점과 한계를 극복할 수 있는 방안으로 제시되고 있는 것이 바로 전자거래 개인정보보호기본법의 제정이다. 최근 국내에서는 학계와 시민단체를 중심으로 이에 대한 논의가 한창인데, 여기서 전자거래 개인정보보호기본법이란 세부적인 영역별로 개인정보 관련 규정을 두는 것이 아니라, 전자거래 개인정보보호에 관한 기본원칙, 정보주체의 권리 및 정보처리자의 의무에 관한 사항, 국가 등이 개인정보보호를 위해 하여야 할 의무, 전자거래 개인정보보호기구에 관한 사항 등 모든 영역에 적용될 수 있는 개인정보에 관한 일반적인 사항을 단일 법률을 통해 규정함으로써 하나의 일관성 있는 기준을 제시하는 의미로 이해된다.

아울러 전자거래 개인정보보호법이 그 법제정 실익을 가지기 위해서는 반드시 'OECD 프라이버시 8원칙' 및 'EU 개인정보보호지침'에서 규정하고 있는 내용을 반영하여야 할 것이다. 그러므로 무엇보다도 정보주체의 권리 및 정보처리자의 의무에 관한 사항을 명시적으로 규정하는 것이 필요하다. 이러한 내용은 일반적인 개인정보보호원칙의 형태로 규정되기도 하는데, 영국, 캐나다, 호주, 뉴질랜드, 홍콩, 스웨덴의 법이 그러하다. 이에 따라 개인정보보호 기본원칙을 규정하게 되면, 개인정보를 취급할 때 어떠한 목적 범위 안에서 무슨 방법으로 처리할 것인지를 보다 명확하게 제시할 수 있다는 장점이 있다. 또한 전자거래 개인정보보호법은 실질적으로 개인정보의 침해예방 및 피해구제를 위한 역할을 담당할 수 있는 개인정보보호기구의 설치 및 기능과 권한, 법위반시 처벌규정 등과 같은 절차적 보호규정을 포함하여 전자거래 개인정보보호법의 실현을 보장할 수 있어야 한다.

Ⅱ. 전자거래 개인정보보호기구

전자거래 개인정보보호기구가 실질적으로 전자거래 개인정보보호법을 집행하고 개인정보보호의 역할을 다하기 위해서는 전자거래 개인정보에 관한 전반적인 기능을 모두 수행할 수 있어야 하고, 이를 위한 권한이 확보되어야 한다.

1. 현행 전자거래 개인정보보호기구의 문제점

우리나라에서 전자거래 개인정보보호의 역할이 여러 기관에 분산되어 있다는 것은 일견 각각의 기구들이 통합적인 개인정보보호 기능을 수행하

고 있지 못하다는 것을 보여준다. 법률상 개인정보보호기구로 설립된 '개인정보보호심의위원회' 및 '개인정보분쟁조정위원회'도 기본적으로 그 기능이 각각 전자거래와 관련한 정책적 사안에 대하여 '심의'하는 역할과 개인정보에 관한 분쟁을 '조정'하는 역할로 한정되어 있다. 물론 '전자거래분쟁조정위원회'와 '방송통신위원회' 그리고 '한국정보보호진흥원(개인정보침해신고센터)'이 서로 유기적으로 협조하여 전자거래상 개인정보침해예방 및 피해구제 등의 기능을 수행하여 어느 정도 성과를 보여주고 있으나 그 한계가 있음은 부인할 수 없다. 또한 이렇게 기능이 분산되어 있다 보니 각각의 개인정보보호기구들이 행사할 수 있는 권한에도 제한이 따른다.[137]

우리나라의 경우 전자거래 개인정보보호 전담기구라 할 만한 개인정보보호기구가 없기 때문에 각각의 기관이 행사할 수 있는 권한도 다소 제한적이다. 방송통신위원회는 민간부문의 개인정보처리실태를 조사·감독하여 위법사항이 발견될 경우 시정권고, 시정명령, 과태로 등 행정적 제재조치를 취할 수 있으나 행정안전부는 기본적으로 공공부문의 개인정보처리 상황을 총괄할 뿐 직접적인 지도·감독은 각 관계행정기관의 장이 맡아하고 있다. 따라서 행정안전부는 필요한 경우 공공기관의 장에게 개인정보보호에 관한 의견을 제시하거나 권고하는 역할에 그칠 뿐이다.

또한 공공부문과 민간부문에 각각 설치된 법정 전자거래 개인정보보호기구인 '개인정보보호심의위원회' 및 '개인정보분쟁조정위원회'의 기능과 권한도 다소 제한적이다. 개인정보보호심의위원회는 공공부문의 개인정보처리에 관한 정책이나 제도개선, 공공기관 간 의견 조정 등에 관한 사항

137) 성낙인 외, 전게서, 374면 이하.

을 심의·의결하는 역할을 맡고 있을 뿐, 직접 전자거래상 개인정보침해 행위를 한 기관이나 당사자에게 시정을 권고하거나 의견을 제시하는 등 사후적 피해구제의 역할을 담당하지는 않고 있다. 또한 업무를 담당할 전문 인력이나 예산도 전무하여 위원회의 실질적인 운영을 지원하는 사무국도 없는 상태이다. '개인정보분쟁조정위원회' 역시 기능의 초점이 사후적 피해구제에 맞추어져 있어 전자거래 개인정보침해로 인한 피해를 접수받아 사실조사를 하고 분쟁조정을 함으로써 당사자 간 원만한 피해구제가 이루어지도록 하는 역할을 주로 담당하고 있을 뿐이며, 교육·홍보기능, 법률 및 기술자문, 정책연구 등은 'KISA(개인정보침해신고센터)'가 맡고 있다. 또한 KISA가 개인정보침해와 관련된 상담 및 고충처리를 개인정보분쟁조정위원회가 분쟁조정을 맡고 있어 개인정보피해구제기능도 중복되고 있다.

2. 전자거래 개인정보보호기구에 통합적 기능과 권한 부여

전문적으로 전자거래 개인정보보호 기능을 전담하여 수행하는 기구를 설립한다고 할 때, 이러한 기구가 본래의 목적을 원활히 달성할 수 있기 위해서는 무엇보다도 개인정보보호기구의 기능 및 권한에 지나친 제약이 있어서는 안 된다. 또한 공공부문과 민간부문의 개인정보처리를 각각 관할 할 수 있는 전자거래 개인정보보호 기구를 확립한다면, 각각의 기구는 해당 영역의 개인정보보호를 위한 사전 침해 예방적 기능부터 사후피해구제의 기능까지 총괄하여 담당할 수 있어야 한다. 물론 공공부문과 민간부문의 특징에 따라 개인정보보호기구의 세부적인 기능이나 권한 상의 차이는 있을 수 있지만, 기본적으로 현재 분산되어 있는 전자거래에 있어서 개인정보보호기능을 한 단계 높은 차원에서 통괄하여 시행할 수 있어야

할 것이다.

따라서 전자거래 개인정보보호기구는 우선 국민, 정부, 사업자, 의회 등을 대상으로 한 정보제공자의 역할을 충실히 담당하여야 한다. 또한 개인정보와 관련된 지침제정, 정보주체의 권리와 정보처리자의 의무에 대한 상담 및 교육, 개인정보와 관련된 지침제정, 정보주체의 권리와 정보처리자의 의무에 대한 상담 및 교육, 개인정보와 관련된 정책 및 법률 자문 등 총체적인 정보제공의 역할을 수행할 수 있어야 한다.

그리고 이러한 개인정보보호기구는 개인정보보호를 위한 기준을 정립하고 정보처리자의 자율적인 개인정보보호 환경이 정착되도록 도와주며, 이를 위해 필요한 교육·홍보활동을 실시하는 등 각종 침해예방활동을 펼칠 수 있는 기능이 부여되어야 한다. 특히 이러한 피해구제의 기능은 개인정보침해 피해자 또는 일반 국민 누구나 쉽게 접근하여 이용할 수 있도록 소송 외적 분쟁해결제도를 적극 활용함으로써 더욱 효과적으로 수행될 수 있을 것이다. 다만, 추가적으로 고려되어야 할 것은 분쟁조정제도가 신속하고 간편하게 분쟁을 해결할 수 있다는 장점이 있지만 강제력이나 구속력이 없어 당사자의 합의가 없는 경우에는 소송에 의하지 않고서는 실질적인 구제방법이 없다는 점이다. 따라서 이를 뒷받침할 수 있는 시정권고권이나 시정명령권 등 행정조치를 취할 수 있는 권한이 부여될 필요가 있다.[138] 그러나 개인정보보호기구의 법적 지위를 현재와 같이 반관반민(半官半民) 형태로 유지할 경우 현실적으로 시정명령권, 과태료 부과권 등

138) 외국의 전자거래 개인정보보호기구들도 대부분 개인정보 관련 민원이나 불만이 접수되면 당사자 간의 대화와 타협을 유도하고 알선함으로써 사전 합의가 되도록 하고 있는데, 개인정보처리 등록취소, 시정권고, 이행고지, 시정명령, 과태료 부과 등의 조치를 취할 수 있는 권한을 보유하고 있는 경우 당사자 간 합의에 도달할 수 있도록 사실상 강제할 수 있어서 더욱 효율적인 피해구제를 도모할 수 있다고 한다. (Douwe Korff, supra note 311, pp.207~208)

을 직접 부여하기는 어렵기 때문에, 그러한 권한을 가진 행정기관에 대하여 위법 사실을 통보하고 징벌을 요구할 수 있는 권한을 행사할 수 있도록 하는 것을 고려하여야 한다. 또한 형사고발조치나 소제기·소송지원의 역할을 적극적으로 담당하여 사후적 관리기능을 수행할 필요도 있다.

제5장 결 론

앞으로 과학기술의 발달 및 정보통신기술의 발달과 인터넷의 전 세계적인 보급으로 인해 전자거래는 우리 생활에서 점점 더 필수불가결한 요소가 될 것이다. 시간과 공간의 제약을 초월하는 이와 같은 전자거래는 기존의 국경이라는 개념을 무색하게 하고, 글로벌 시대에 걸맞게 더욱 활발하게 이루어질 것이다. 하지만 이러한 전자거래의 비약적인 발달에는 그에 따른 부작용도 함께 나타날 것이다. 현실적으로 이미 이러한 문제점들이 하나둘씩 나타나고 있으며, 이를 해결하기 위한 기술적·제도적·정책적 방안이 시급히 모색되고 있다.

본 연구는 전자거래에 있어서 발생할 수 있는 개인정보보호 측면에 초점을 맞추어, 전자거래의 개념적 정의와 그 특성 및 일반적인 유형을 살펴보았고, 개인정보보호제도와 관련하여 국내·외 동향을 살펴보았다. 그리고 전자거래에 있어서 개인정보침해 유형 및 그 구제방안을 모색하였고, 이를 통하여 전자거래에 있어서 개인정보침해구제 개선방안에 대한 논의를 마지막으로 본 연구를 마무리하였다.

전자거래에 있어서 개인정보보호는 전자거래 분야에서 국한된 문제이기보다는 우리나라가 가지고 있는 일반적인 개인정보보호체계와 맞물려 이에 관한 일반적인 문제점을 개선하는 것이 선결과제라 할 것이다. 즉 우리나라 법제에서는 '개인정보보호법'에 해당하는 개인정보보호 관련 기본법의 부재로 인해, 통일적이고 체계적인 개인정보보호가 효율적으로 이루어지지 않고 있다는 점이 가장 큰 문제점으로 지적되고 있다.

그리고 각각의 분야에 있어서 산재한 개인정보보호 관련 법률과 이를 근거규정으로 설립된 개인정보보호기구의 중첩적 존재는 개개의 개인정보보호기구의 기능 및 권한의 약화로 이어지며, 궁극적으로 신속하고 정확한 개인정보피해구제를 어렵게 하는 걸림돌이 되고 있다.

이와 같은 개인정보보호에 관한 근본 문제를 전제하여, 전자거래 분야에서의 개인정보보호 문제를 살펴보면 그 문제의 심각성은 더욱 커질 수밖에 없다. 이는 우리나라 개인정보보호체계가 갖는 위와 같은 한계가 전자거래에 그대로 드러나기 때문이다. 특히 전자거래의 특성상 법적인 분쟁이 발생했을 경우 사전예방보다는 사후구제에 초점을 맞출 수밖에 없어, 전자거래 분야에 있어서 개인정보보호는 법제의 정비가 잘 되어 있어야 효과적이고 신속한 피해구제가 가능하다. 하지만 현실적으로 이러한 효과적이고 신속한 피해구제는 앞서 밝힌 체계적 문제점으로 인해 불가능하다는 것이 밝혀졌다.

따라서 전자거래 분야에 있어서 개인정보보호를 위해서는 다음과 같은 법제도의 개선이 시급히 요구된다.

첫째, 전자거래 분야에 있어서 개인정보보호를 목적으로 하는 기본법의 제정이다. 물론 공공부문에서 「공공기관의개인정보보호에관한법률」과 민간부문에서 「정보통신망이용촉진및정보보호등에관한법률」이 해당 분야에서의 기본법 형태로 제정되어 시행되고 있지만, 해당 분야에 있어서 부차적인 과제로서 개인정보보호를 추가하여, 그 근본적인 한계를 벗어나지 못하고 있다. 따라서 전자거래 분야에 특화된 개인정보보호 기본법이 마련되어야 한다. 물론 이러한 기본법에는 「OECD 가이드라인」과

「EU 지침」 등에서 논의된 개인정보보호를 위한 기본 원칙들이 충실히 반영이 되어야 할 것이다.

둘째, 기본법 제정을 통한 단일 개인정보보호기구의 설립이다. 현재와 같이 산재한 전자거래 관련 개인정보보호기구가 아닌 전문 전자거래 관련 개인정보보호기구가 필요하다. 아울러 이렇게 설립된 개인정보보호기구에 그 기능 및 권한을 적절히 수여하여, 전자거래 분야에서 발생할 수 있는 개인정보피해의 사후구제에 더욱 효과적으로 대처할 수 있게 하고, 개인정보피해의 사전예방을 위한 제도적인 장치를 마련하게 하여야 할 것이다.

급속도로 발달하는 과학기술로 인해 현실과 법제도 사이의 괴리는 나날이 커지고 있다. 또한 법제도가 가지는 한계로 인해, 하루가 다르게 변화하는 현실을 법제도가 따라잡지 못하고 있는 것이 사실이다. 이렇다 하여 이러한 괴리를 방관하고 있을 수도 없는 일이며, 이를 방관하여서도 안 된다. 본 연구는 이러한 점에 기인하여, 오늘날 가장 빠른 속도로 발달해가고 있는 전자거래 분야와 인간으로서 기본적으로 가지는 개인정보보호에 관한 논의를 해 보았다. 전자거래에서 발생할 수 있는 개인정보피해를 방지하기 위해서는 제도적·정책적 변화와 함께 그에 대한 개선이 하루 빨리 이루어져야 한다는 점은 다시 한 번 강조하여도 지나친 점이 없을 것이다.

참고문헌

1. 단행본

개인정보분쟁조정위원회, 「각국의 개인정보피해구제제도 비교연구」, 개인정보분쟁조정위원회, 2007.

방송통신위원회, 「정보통신백서」, 2008.

사법연수원, 「전자거래법」, 사법연수원편집부, 2006.

성낙인 외, 「개인정보보호법제에 관한 입법평가」, 한국법제연구원, 2008.

오병철, 「전자거래법」, 법원사, 2000.

정완용, 「전자상거래법」, 법영사, 2002.

정쾌영, 「전자거래법」, 무역경영사, 2001.

총무처, 「축조해설 개인정보보호법」, 총무처, 1994.

최경진, 「전자상거래와 법」, 현실과 미래, 1998.

한국정보보호센터, 「정보화 역기능 사례집(보고서)」, 2006.

행정자치부, 「공공기관의 개인정보보호제도 이해와 해설」, 2003.

European Commission, *An European Initiative in Electronic Commerce*, 1997.

European Commission, *An Introduction to Electronic Commerce*, 1997.

The White House, *A Framework for Global Electronic Commerce*, 1997.

2. 논문

강경근, “인터넷 사회에서의 개인정보보안과 정보기반보호, 「인터넷 법률」, 2000.

강신원, “B2C 활성화를 위한 개인정보보호제도와 정책 방향”, 「개인정보연구 2권 1호」, 2003. 7.

김영철, “프라이버시권의 보호법익과 법적 성격”, 「언론중재」, 1999년 여름호.

김재두, “전자상거래의 입법동향에 관한 법률”, 「경영법률」, 2008.

김현수, “일본의 개인정보 관련 법제 동향과 법률 분석”, 「IT법 연구」, 2007. 8.

문성제, “온라인상에서의 개인정보보호에 관한 국제 동향 -미국의 제도를 중심으로”, 「비교법학연구 3집」, 2004. 2.

백충길, 정회근, “전자상거래와 개인정보보호”, 「토지공법연구」, 2002.

손경한, “전자상거래 입법의 국제적 동향”, 「저스티스 통권68호」, 2002.

유황빈, “디지털시대의 개인정보보호 기술”, 「인터넷 법률」, 2001.

양창수, “정보화사회와 프라이버시의 보호”, 「인권과 정의」, 1991. 3.

이윤선, “전자거래에 관한 연구”, 「민사법연구 11집 2호」, 2003. 12.

이은선, “온라인을 통한 소송외적 분쟁해결에 관한 고찰”, 「개인정보연구 2권 1호」, 2003. 7.

이정원, “전자거래와 개인정보보호에 관한 연구”, 고려대학교 대학원 석사학위 논문, 고려대학교, 2002.

임건면, “개인정보침해에 대한 민사법적 대응”, 「비교사법 8권 1호」, 2000.

임건면, “민사법상의 개인정보보호”, 「비교사법 3권 1호」, 1996 .6.

장영민, “정보통신망발전에 따른 개인정보보호”, 「형사정책 연구 7권 2호」, 1996.

장은상, “전자거래에있어서 개인정보의 보호”, 호남대학교 대학원 석사학위 논문, 호남대학교, 2006.

정재황, “프랑스법에서의 개인정보의 보호에 관한 연구”, 「공법연구 34집 4호 1권」, 2006. 6.

지원림, “전자거래와 계약법”, 「법학논총 24집」, 2000.

최명구, “디지털 사회의 개인정보보호 -쿠키(Cookie)를 중심으로”, 「인문사회과학연구 4권」, 부경대학교 인문사회과학연구소, 2004.

최상호, “전자거래에 있어서의 소비자보호 -특히 프라이버시 및 개인정보보호를 중심으로”, 「비교사법 8권 1호」, 2001.

최석범, 엄광열, “미국의 통일전자거래법과 한국의 전자거래기본법에 관한 연구”, 「국제상학 16권 2호」, 2001. 11.

한영학, “일본의 개인정보보호 법제”, 「세계언론법제동향」, 2000. 12.

홍준형, “인터넷 사회에 있어서의 EDI 및 전자거래 기능”, 「전자거래 및 EDI관련법 제도 정비방향」, 한국전산원, 1996.

大澤秀介, “個人情報の 保護”, 「法學教室」, 1996. 3.

牧野二郎, “プライバシとはなにか”, 「プライバシ保護と個人情報保護の關

する考察」, 1999. 8.

Alan F. *Westin, Privacy and Rreedom*, N.Y. Ateneum, 1967.

Blair Stewart, *International Accreditation of Privacy and data Protection Authorities*, APEC Data Privacy Workshop, 2003.

Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 Indiana Law Review 174, 1999.

Jonathan P. Cody, *Protecting Privacy Over the Internet : Has the Time Comer to Abandon Self-Regulation?*, 48 Catholic University Law Review 1183, 1999.

Domingo R. Tan, *Personal Privacy in the Information Age : Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 Loyola of Los Angeles Internet $ Comparative Law Journal 661, 1999.

Raymond Tang, *Remedies for Personal Data Infringements under the Personal Data(Privacy) Ordinance*, International Conference on Personal Data Protection 2002 in Seoul, 2002.

3. 기타

개인정보침해신고센터(개인정보분쟁조정위원회) : http://www.kopico.or.kr

공정거래위원회 홈페이지 : http://www.ftc.go.kr

국가법령정보센터 : http://www.law.go.kr

국민권익위원회 : http://www.acrc.go.kr

국회법률지식정보시스템 : http://likms.assembly.go.kr/law

금융위원회 : http://www.fsc.go.kr

미통계국 홈페이지 : http://www.census.gov

전자거래분쟁조정위원회 : http://www.ecmc.or.kr

한국소비자원 : http://www.kca.go.kr

한국정보보호진흥원 : http://www.kisa.or.kr

EU 홈페이지 : http://www.europa.eu

OECD 홈페이지 : http://www.oecd.org

UN 홈페이지 : http://www.un.org

YTN 홈페이지 : http://www.ytn.co.kr