

전문가가 진단한 정보화법제도 쟁점과 과제- 2009-⑧

개인정보보호의 법적 쟁점과 과제

이민영(카톨릭대학교 법학과 교수)

목 차

제 1 장 서론	1
제 2 장 개인정보영향평가의 쟁점과 과제	9
제 1 절 논의의 배경	9
제 2 절 입법적 현황	10
제 3 절 법제화 방향	37
제 3 장 개인정보보호기구의 쟁점과 과제	46
제 1 절 논의의 배경	46
제 2 절 입법적 현황	52
제 3 절 법제화 방향	80
제 4 장 개인정보피해구제의 쟁점과 과제	88
제 1 절 논의의 배경	88
제 2 절 입법적 현황	94
제 3 절 법제화 방향	121
제 5 장 결론	125
< 참고문헌 >	130

표 목차

[표 1] OMB 지침에 따른 PIA 평가대상	16
[표 2] 미국 OMB의 PIA 수행 절차	19
[표 3] 캐나다 공공기관의 PIA 수행 대상	23
[표 4] 캐나다 개인정보 영향평가 관련 지침	24
[표 5] 뉴질랜드의 주요 PIA 사례	28
[표 6] 법안별 개인정보 영향평가 규율내용	34
[표 7] 주요국의 PIA 실시 대상	37
[표 8] 국내 정보보호 관련 취약성 평가 및 진단 사례	43
[표 9] 국내 정보보호 관련 근거와 기준	44
[표10] 일본의 개인정보보호 법률체계	68

그림 목차

[그림 1] 국내 개인정보보호 관련 법률 체계	8
[그림 2] 캐나다 프라이버시 영향평가 절차도	25
[그림 3] 뉴질랜드 PIA 절차도	29

제1장 서론

바야흐로 지난 17대 국회부터 지금까지 개인정보보호에 관한 법률에 많은 논의가 있어왔다. 당시 우여곡절 끝에 민주노동당 노회찬의원이 대표발의한 ‘개인정보보호기본법(안)’과 열린우리당 이은영의원이 대표발의한 ‘개인정보보호법(안)’이 국회 상임위원회인 행정자치위원회에 회부되었고, 한나라당 이혜훈의원이 또 다른 「개인정보보호법(안)」을 대표발의하기도 했다. 이 같은 일련의 과정은 2003년 대통령 주재로 열린 국정과제회의에서 정부혁신지방분권위원회가 전자정부관련법제정비방안의 마련, 개인정보보호 기본원칙의 천명, 개인정보영향평가제도의 도입, 개인정보보호기구의 설치 등을 내용으로 하는 법제정 방침을 밝힌 지 만 2년만의 일이다. 하지만 이후 핵심쟁점으로 부각된 개인정보보호기구의 설치문제 및 개인정보영향평가제의 도입문제가 합의로 이어지지 못하고 결국 모두 임기만료 폐기되는 등 개인정보보호와 관련된 입법적 대응은 순조롭지 못했다.

이런 상황에서 이번 18대 국회 들어 2008년 8월 한나라당 이혜훈의원이 대표발의한 「개인정보보호법(안)」과 10월 민주당 변재일의원이 대표발의한 「개인정보보호법(안)」이 국회 행정안전위원회에 상정되었다. 이와 더불어 새 정부의 출범 이후 행정안전부가 개인정보보호에 관한 주무부처로 거듭나면서 행정안전부 공고 제2008-115호로 입법예고된 「개인정보보호법(안)」이 11월 제안되어 위 법안들과 함께 2009년 2월 23일 제281회 국회 제2차 법안심사소위에 상정된 상황이다. 이하 발의시기를 역순으로 하여 행정안전부안을 1안, 민주당안을 2안, 한나라당안을 3안이라 칭하여 법안의 주요내용 및 법제화 방향에 대하여 논의할 때에 이렇게 지목할 것인바, 이를 도식화하면 다음과 같다.

2 개인정보보호의 법적 쟁점과 과제

법안약칭	1안	2안	3안
의안명	개인정보 보호법안	개인정보보호법 안	개인정보보호법 안
발의주체	정부(행정안전부)	변재일의원(민주당)	이혜훈의원(한나라당)
의안번호	2369	1598	570
제안일자	2008.11.28	2008.10.27	2008. 8. 8
회부일자	2008.12. 1	2008.10.28	2008. 8.29

한때 2009년 상반기에 위 법안의 조율과 국회 본회의 통과가 유력시되기도 했지만 현재 개인정보보호 관련 법안논의는 다시 수면 아래에 있을 듯하다.

정보사회에서 개인정보의 지배는 그 정보주체에게는 인격의 존엄과 자유의 불가결한 조건이 되지만, 동시에 정부나 기업에 의한 개인정보의 지배는 정보주체를 통제할 수 있는 권력의 기초가 된다. 디지털 정보혁명으로 촉발된, 개인정보의 지배를 둘러싼 자유와 권력의 이항대립은 이미 우리 사회에 두드러진 현상이 되고 있다. 그런데 이러한 대립 속에는 결코 무시할 수 없는 개인정보처리의 이익과 가치가 그 위세를 떨치고 있음을 부인하기 어렵다.

현대의 정부는 단순히 물질적 생산조건의 확보라는 기능을 넘어서 복지나 사회정책 등 사회적 재생산조건을 보장하기 위한 기능을 담당하게 되었고, 이러한 기능을 효율적으로 수행하기 위해 개인정보의 수집과 처리는 불가피한 과정이 되고 있다. 이는 작고 효율적인 시민 중심의 행정

서비스를 제공하기 위해 전자정부의 개념이 구체화되는 현 상황으로도 잘 알 수 있다.

한편, 시장에 있어서도 기업에 의한 고객의 개인정보처리는 자원배분의 효율성을 극대화할 뿐만 아니라 소비자인 정보주체에게는 거부할 수 없을 정도의 달콤하고 편리한 이익을 안겨준다. 그러나 개인정보처리가 가져다 줄 이익과 가치 못지않게 그 위험성 또한 무시할 수 없을 정도로 커질 수 있다. 이른바 원형감옥(Panopticon), 즉 효과적이고 효율적인 감시체계의 등장은 큰 우려를 낳게 한다. 고도정보사회로 진입하는 길목에서 이러한 위험성을 최소화하면서 개인정보처리의 사회적 이익을 수용할 수 있는 규범적 척도를 찾아내는 것이 우리 사회의 시급하고도 절실한 과제인 셈이다.

인터넷을 위시하여 정보통신 및 첨단과학기술의 발달로 인해 각종 정보의 수집, 보유·관리, 처리·이용이 등이 확대된 오늘날에는 개인의 정보가 부당하게 노출되어 사생활이 침해되는 결과를 낳는 불법적 부작용이 방치될 수만은 없는 현실세계가 엄연히 공존한다. 특히 컴퓨터기술의 발전에 따라 개인에 관한 정보를 처리·배포하는 데 드는 비용은 지속적으로 감소하고 있기 때문에 사업적인 측면에서 개인정보의 수집은 비용 대비 효율적이라고 평가되고, 이와 같은 상황은 정보프라이버시에 대한 중대한 위협으로 작용하고 있다.

그럼에도 불구하고 현실적으로 개인정보의 취급에 따른 정보활용의 문제는 공공부문이든 민간부문이든 당위적 전제조건이 된다. 다만 공적 영역에 있어 개인정보의 활용은 원칙적으로 기본권의 제한을 가져오므로 기본권침해의 소지가 없는 한도 내에서 허용되는 반면, 사적 영역에 있어

4 개인정보보호의 법적 쟁점과 과제

개인정보의 활용은 원칙적으로 허용되는 것이다. 물론 영업의 자유 혹은 표현의 자유와 같은 다른 기본권과의 관계에서 이익 형량 여하에 따라 상호권익의 조율이 요구되며, 이에 따라 예외적인 제한에 대한 규제수준이 가늠될 수 있는 것이다.

결국, 현재 국회에 상정된 법안의 입법 취지는 이와 같은 활용, 침해, 허용, 규제를 위한 기준이 되는 것이다.

앞서 언급한 바와 같이, 국내 개인정보보호 체계는 공공·민간 분야별로 개별법에 근거하여 각 소관 부처가 규율하는 체계이다. 이러한 법제환경에서 개인정보보호 중요성에 대한 사회적 관심은 증가하고 있지만 사회 각 분야에 일반적으로 적용할 수 있는 법제는 존재하고 있지 않다. 현행 국내 개인정보보호 체계는 개별법에 근거한 다원화된 추진체계로 인하여 법 적용 사각지대를 발생시킬 뿐만 아니라 국민 혼란을 야기하고 있는 실정이다. 때문에 개인정보보호 추진체계를 재점검하고 법 적용의 사각지대를 방지할 수 있는 단일법인 개인정보보호법 제정은 필수적이라 할 수 있다. 이와 관련해 그동안 국회·시민단체 등에서 법제 일원화의 필요성을 지속적으로 요구해왔을 뿐만 아니라, 관련 전문가 및 학계에서도 연구결과를 토대로 공감하고 있다. 이에 따라 각 법안들은 공통적으로 다음과 같이 규율하고 있다.

첫째, OECD 8원칙을 위시하여 국제 사회가 요구하는 원칙을 최대한 반영하되 국내 환경을 고려한 보호원칙을 정립하고 있다. 이를 통해 공통적인 보호 및 처리 원칙, 보호 및 적용 대상의 범위를 최대한으로 반영하여 개별법 양산에 따른 혼란을 방지하는 데 주안점을 두고 있다.

둘째, 개인정보 이용에 대한 편익과 보호의 조화를 꾀하고 규제의 균형성을 증진하는 데 초점을 맞추고 있다. 그리하여 현행 「공공기관의 개인정보보호에 관한 법률(이하 '공공기관법'이라 한다)」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 한다)」 등 공공·민간 일반법을 포함한 개별법제 상호간 개인정보보호 및 제재 수준에 대하여 균형성을 확보하는 규율태도를 유지하고 있다.

셋째, 개인정보 처리 원칙의 명확화 및 이용자 권리 강화를 최우선으로 하고 있다. 이를 위하여 개인정보의 수집, 이용·제공, 파기 등 단계별 처리 기준을 일정하게 제시하고 있으며, 안내판설치·녹음금지 등 CCTV 설치 및 이용 기준을 반영하고 있을 뿐만 아니라, 국회·법원 등 헌법기관과 동호회·카페 등 비영리단체로 적용 대상을 확대하고 있다.

하지만 법률 취지와 내용에 대한 공감대는 형성과는 별개로 개인정보 보호 기구 창설과 관련된 논의가 아직까지 쟁점화 돼 합의에 이르지 못하고 있다. 기구창설에 대하여는 의견을 같이 하면서도 그 위상과 권한에 있어서는 차이가 있기 때문이다. 당초 17대 국회에서 제안된 민주노동당 안의 경우 시민사회단체의 의견을 수렴하여 독립된 위원회를 설립하여 개인정보보호에 관한 공공·민간예의 감독을 수행할 것을 논의하고 있었다. 이에 대응하여 당시 열린우리당안은 위원회를 설치하되, 여러 위원회가 난립하고 있는 사정을 감안해 이를 국가인권위원회 산하 위원회로 위상을 정립하려 했었으나 국가인권위원회가 이를 수용하지 않았었다. 18대 국회에 들어서도 국무총리 소속 위원회 혹은 대통령 소속 위원회로 그 위상 정립에 이견을 갖고 있으며, 특히 입법예고된 행정안전부안의 경우 행정안전부 소속 위원회로의 창설을 예정하고 있었으나 반대여론이 거세지자 국회 제출 당시 국무총리 소속 위원회로 변경하기도 하였다.

6 개인정보보호의 법적 쟁점과 과제

논란의 핵심은 바로 독립성에 있는데 개인정보보호를 위한 권한을 수행함에 있어 다른 국가기관의 간섭이나 개입을 받지 않고 독자적이고 독립적이며 공정하게 행할 수 있도록 함으로써 국민의 권익신장에 이바지해야 한다는 목소리인 것이다. 독립성의 견지가 필수적이라는 데 의견을 같이 하지만 위원회의 명칭이나 그 지향 그리고 위상과 권한이 제각기 다른 까닭에 위와 같이 법안의 내용구성도 달라져 있는 것이다. 현실적으로 개인정보보호법의 성안이 어려운 것은 물론, 정치적 현안에 따른 국회의 의사일정 탓인 때문도 분명 있지만, 법안 상호간 조율이 결국 위원회 문제에서 교착상태에 놓인 것이라고 할 수 있다.

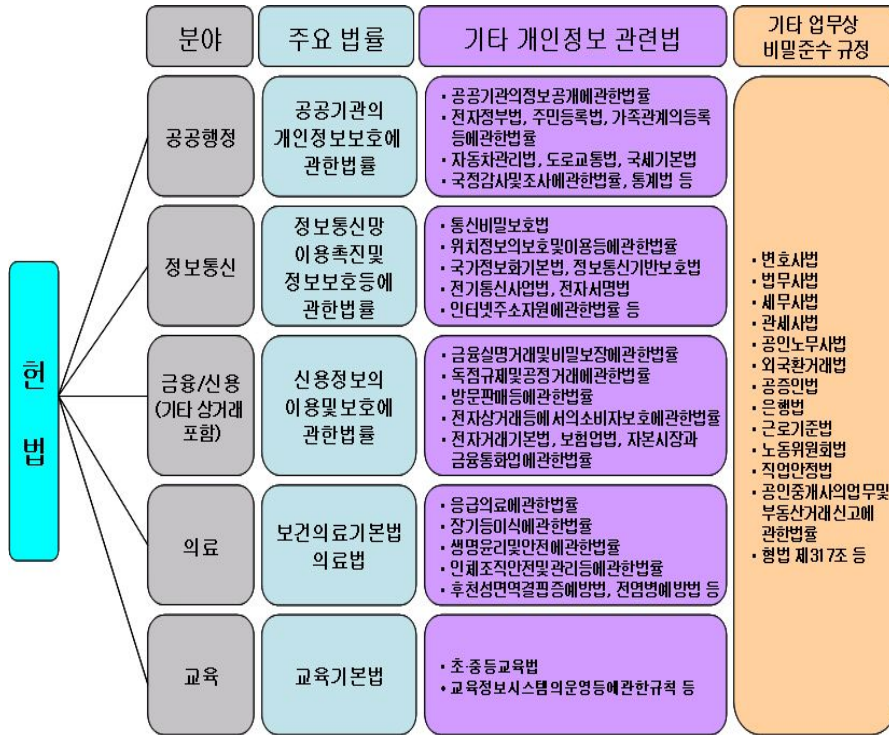
최근 한·EU FTA 협상 타결에 따라 국외 개인정보 이전과 관련하여 EU 등 국제사회는 적절한 수준의 개인정보보호 체계를 갖추지 않은 국가에 대해서는 자국민의 개인정보 제공을 원칙적 금지하고 있다는 점을 상기하여야 한다. EU의 경우 ‘개인정보의 자동처리에 관한 개인의 보호를 위한 유럽협약(Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)’에 따라 공공·민간 모든 부분에 포괄적으로 적용되며 개인정보처리자에 대한 감독 및 피해구제 체계가 실질적으로 이루어진 법제도의 실효성 있는 기준을 제시하고 있다.¹⁾ 이제 국제사회의 요청에 부합하면서 정보주체의 정보자기결정권을 보장할 뿐만 아니라 개인정보처리자의 합법적인 정보활용을 도모하여 정보사회의 균형점을 모색하기 위해서는 개인정보보호법의 제정과 독립된 위원회의 발족은 필수불가결한 요소이다. 대승적 차원에서 위원회의 위상과 권한에 관한 논의에 합의점을 도출하고 향후 위원회가 개인정보보호법의 입법목적을 순연하게 집행할 수 있도록 뜻을 모아야 할 시점

1) Ferdinand Kopp, Das EG-Richtlinenvorhaben zum Datenschutz, RDV, 1993, S. 4.

이라 하겠다. 그리고 이러한 조직적·구조적·형식적 프레임에 걸맞는 작용적·기능적·실질적 내구성이 개인정보보호법제에 반영될 수 있도록 사회적 합의를 도출하고 정치적·정략적 논의와 무관하게 민의를 수렴하는 절차가 조속히 이루어져야 할 것으로 본다.

이와 같은 관점에서 개인정보보호와 관련된 쟁점을 법이론적·법정책적 시각에서 재검토하고 법제도적 발전방향을 되짚어봄으로써 향후 법안의 조율과 대안의 제시에 있어서 단초가 될 수 있는 접점을 모색한다는 점이 본 연구의 의의이자 취지가 될 수 있다. 또한 아래와 같은 현행 법체제에서 입법공백이나 사각지대가 형성되는 부분을 메우기 위한 기본법제의 구축이 현실적으로 요청된다는 필요성은 본 연구의 배경이자 지향이라 할 수 있을 것이다.

8 개인정보보호의 법적 쟁점과 과제



<그림 1> 국내 개인정보보호 관련 법률 체계

제2장 개인정보영향평가의 쟁점과 과제

제1절 논의의 배경

지난 수년 간 개인정보보호법의 제정, 개인정보 관련 자율규제론, 개인정보보호 기술(Privacy Enhancing Technologies; PETs)의 개발, 개인정보보호에 대한 국제 기준의 제정 등 개인정보를 보호할 수 있는 다양한 방법들이 논의되어져 왔는데, 그 중 하나가 개인정보 혹은 프라이버시 영향평가(privacy impact assessment; PIA)라 할 수 있다. 어떤 기술이나 제도·상품이 인간이나 환경에 잠재적으로 위험성을 갖고 있다고 한다면, 설령 그 위험성이 분명하지 않다 하더라도 도입하려는 쪽에서 무해함을 입증하기 전까지는 예방 차원에서 도입을 금지할 수 있어야 한다는 것이다. 이러한 원칙이 제도화된 것이 환경영향평가를 비롯한 각종 사전영향평가제도이다.²⁾

개인정보 영향평가 제도는 ‘사후적인 치료보다는 사전적인 예방이 낫다’는 ‘사전예방의 원칙(precautionary principle)’으로부터 출발하는 제도이다.³⁾ 즉, 개인정보 영향평가 제도라 함은 새로운 정보시스템의 도입과

2) 한국전산원, 개인정보보호제도 시행을 위한 사례연구, 정부혁신지방분권위원회, 2005, 3쪽.

3) 지난 1992년 6월 브라질 리우에서 개최된 UN 인간환경회의에서는 ‘환경적으로 건전하고 지속가능한 개발(environmentally sound and sustainable development; ESSD)’을 실현하기 위하여 ‘리우선언’이 채택되었고 ESSD를 위한 전세계적인 규범이라 할 수 있는 리우선언에 제시된 27개 원칙 가운데 환경정책의 결정에 있어 ‘객관적이고 과학적인 사실’과 ‘정책결정자의 결단’ 사이의 절묘한 균형점을 시사하는 것이 바로 사전예방의 원칙(Precautionary Principle)이다. 환경보호를 위하여 각국은 능력에 따라 사전예방적 접근을 폭넓게 활용하여야 하며 심각하거나 비가역적인 피해의 위협이 있는 경우 충분

10 개인정보보호의 법적 쟁점과 과제

개인정보의 수집에 앞서 계획하고 있는 시스템이 구축·운영될 경우 프라이버시에 미칠 영향에 대하여 미리 조사·예측 및 검토하는 체계적인 절차를 의미한다. 일찍이 지난 1989년 David Flaherty의 “감시사회에서의 프라이버시보호(Protecting Privacy in Surveillance Societies)”란 저서에서 그 개념이 제시된 이후 1991년에 “개인정보영향평가를 위한 공식 가이드라인”이 미국 뉴욕주 공공서비스위원회(State of New York Public Service Commission)의 “통신상의 프라이버시에 대한 정책(Statement of Policy on Privacy in Telecommunications)”에서 제시되었고 1999년이 되어서야 비로소 캐나다를 비롯한 몇몇 국가에서 의무적으로 시행되었던 것이 PIA이다.⁴⁾

제2절 입법적 현황

1. 주요국가의 동향

(1) 미 국

한 과학적 확실성이 없다는 이유로 환경파괴를 방지하기 위한 비용-효과적 조치를 연기하여서는 아니 된다는 이 원칙은 어떠한 현상이 완벽하게 과학적으로 규명되지 않았다고 하더라도 정책결정자는 그 결단에 따라 필요한 조치를 강구할 수 있다는 그야말로 절묘한 원칙이고 정책결정이라는 것이 단순히 과학에 뒤따르는 것이 아니라 우리 사회가 필요로 하는 경우 과학을 앞서 갈 수도 있다는 원칙이면서 정책결정의 과학성을 동시에 유지하고 있는 원칙이다. 사전예방의 원칙 개념이 처음 적용된 것은 지난 1984년 북해 보호를 위한 제1차 국제회의로 알려져 있으며, 미국의 경우 오염예방법(Pollution Prevention Act of 1990)을 위시한 여러 환경관련법에 이 원칙을 도입하였다.

- 4) Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments: a guide*, Privacy Victoria - independent statutory office of Australia, 2004, p.3. available at <[http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/\\$FILE/OVPCPIA_GuideAugust2004.pdf](http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPCPIA_GuideAugust2004.pdf)>.

미국은 전자정부를 향한 노력의 일환으로 2002년 12월 17일 대통령이 서명하고 2003년 4월 17일부터 시행된 전자정부법을 제정한 바 있으며, 이 법에서는 국민 중심의 전자정부를 구현하는 과정에서 개인정보의 보호 및 프라이버시 보장이 충분히 이루어질 수 있도록 PIA(privacy impact assessment; 프라이버시영향평가 혹은 개인정보영향평가)의 실시를 명문화하였다.⁵⁾ 미국 전자정부법상 PIA는 법 제208조에 규정되어 있으며, 각종 전자정부 사업을 추진함에 있어 당해 사업이 프라이버시에 미치는 영향을 사전에 조사함으로써 전자정부 사업에 따른 국가기관에 의한 프라이버시 침해를 최소화하는 데 그 의의가 있다.⁶⁾

각 행정기관이 정보기술(information technology; IT)을 활용하여 새로운 정보를 수집하거나 개인 식별이 가능한 정보를 수집·처리하기 위하여 신규 IT시스템을 개발 또는 구매하는 경우 어떻게 개인정보를 보호할 것 인지를 반드시 사전 검토하도록 의무화하는 것으로 PIA의 법제화가 이루어졌으며, 이것이 바로 전자정부법 제208조의 핵심사항이라 할 수 있다. 이로 인하여 각 행정기관은 PIA 실시에 대한 법적 의무를 부담하게 된 것이다.⁷⁾ 한편, 미국 전자정부법은 이러한 PIA 수행을 위하여 미국

5) E-Government Act of 2002(Pub. L. No. 107-347, 116 Stat. 2899) §208(a), set out in a note under 44 U.S.C. §3501; The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

6) 구병문, 캐나다 및 미국의 프라이버시 영향평가 제도 분석과 국내 전자정부 법제도의 도입방향 검토, 정보화이슈분석 03-16, 한국전산원, 2003, 6쪽.

7) §208 of the E-Government Act.

B. Privacy Impact Assessments.

1. Responsibilities of Agencies.

a. In General—An agency shall take actions described under subparagraph (b) before—

i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

12 개인정보보호의 법적 쟁점과 과제

OMB(Office of Management and Budget; 관리예산처)가 구체적인 지침을 각 부처에 제공할 것을 규정하고 있는바,⁸⁾ 프라이버시 규정 이행을 위한 OMB 감독관(Director)의 책무로서 ① 각 부처가 PIA를 수행하는데 필요한 정책과 지침 개발, ② 정부 전체의 PIA 이행 상태 감독, ③ 각 부처가 기존 정보 시스템이나 국장이 적합하다고 인정한 식별 가능한 형태의 정보수집 활동에 대하여 PIA를 수행하도록 요청, ④ 각 정부기관의 웹사이트 운영과 관련하여 프라이버시 정책의 고지에 필요한 지침의 개발 등의 사항을 전자정부법 제208조에서는 열거하고 있다.⁹⁾ 이에 따라 OMB는 2003년 9월 26일 PIA를 포함한 전자정부법의 프라이버시 관련 규정을 각 부처가 이행하는 데 필요한 지침서를 발표하여 각 부처에 시달하였다. 다만, OMB 지침이 나오기 전까지는 IRS(Internal Revenue Services; 국세청)의 영향평가를 참고기준으로 제시하여 왔다.

전자정부법은 각 행정기관이 ① 신원확인이 가능한 정보를 수집·유지·관리 또는 배포하기 위해 IT를 개발하거나 조달하는 경우, ② IT를 활용

8) 미국 PIA 시행에 있어 전자정부법에서 OMB가 그 구체적 수행을 위한 지침을 마련하도록 하고 있다. 이에 따라 OMB는 각 행정기관에 PIA 수행 내용에 관한 지침을 시달하여야 한다. 이 지침에 반영될 내용으로 평가되는 정보시스템의 규모, 당해 시스템 상에서는 식별 가능한 정보의 민감성, 정보의 무단 유출 시의 위험성에 비례하여 이루어져야 하며, ① 수집대상 정보, ② 정보 수집의 목적, ③ 의도하는 정보의 사용처, ④ 정보 공유 대상, ⑤ 수집되는 정보의 내용과 이를 공유하는 방법과 관련하여 개인에게 통지하는 방식 및 동의 획득절차에 관한 방침, ⑥ 정보 보안의 방법, ⑦ 프라이버시법에 따른 기록시스템 실행 여부 등이 다루어져야 한다. <http://georgewbush-whitehouse.archives.gov/omb/memoranda/m03-22.html>

9) §208(b)(3)(C) of the E-Government Act; The Director shall—
a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
b. oversee the implementation of the privacy impact assessment process throughout the Government; and
c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

하여 수집·유지·관리 또는 배포될 정보를 새로이 수집하는 경우, ③ 연방정부기관, 그 대행기관 또는 직원을 제외한 10인 이상의 자에 대하여 신원확인에 관한 문제가 제기되거나 신원에 관한 보고의무가 부과되는 때에 특정 개인에 대하여 물리적 또는 온라인접속을 허용하는 신원확인 이 가능한 모든 정보 등을 새로이 수집하는 경우 등의 업무를 수행하기 이전에 PIA가 실시되어야 함을 규정하고 있다.¹⁰⁾

또한 전자정부법은 PIA의 필수내용을 지정해 OMB가 지침을 행정기관에 발행하도록 규정하고 있는데,¹¹⁾ 이러한 지침은 PIA가 평가대상인 정보시스템의 규모, 시스템상의 식별 형식에서의 정보의 민감도 및 해당 정보의 권한 없는 유출로 초래되는 위험 등에 대하여 이루어져야한다는 점을 명확히 하고 있다.¹²⁾¹³⁾

10) §208 of the E-Government Act.

B. Privacy Impact Assessments.

1. Responsibilities of Agencies.

a. In General—An agency shall take actions described under subparagraph (b) before—

ii. initiating a new collection of information that—

1. will be collected, maintained, or disseminated using information technology; and

2. includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

11) §208 of the E-Government Act.

B. Privacy Impact Assessments. 2. Contents of a Privacy Impact Assessment. a. In General—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

12) §208(b)(2)(B)(i) of the E-Government Act.

13) See generally Joshua B. Bolten, *E-Government Act Section 208 Implementation Guidance*, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, *Memorandum for Heads of Executive Departments and Agencies*, September 26, 2003.

14 개인정보보호의 법적 쟁점과 과제

한편, 전자정부 관련 사업을 수행하는 각 기관은 필요한 범위 내에서 PIA를 수행하여야 하고, 당해 기관장의 결정에 따라 정보화책임관 또는 그에 준하는 공무원이 프라이버시 영향평가서를 검토하여야 하며, 평가의 결과는 가능한 범위에서 공개하도록 되어 있다.¹⁴⁾ PIA 수행보고서는 가능한 범위에서 해당 기관의 웹사이트 또는 관보 게재를 포함한 그 밖에 가능한 수단으로 일반에게 공개하여야 하지만, 보안상의 이유로 또는 영향평가에 포함되어 있는 민감한 정보 또는 개인정보의 보호를 위하여 공개에 관한 사항을 변경하거나 공개 자체를 배제할 수 있다.¹⁵⁾ 전자정부기금의 출연이 필요한 시스템의 경우 당해 기관은 프라이버시 영향평가서 1부를 OMB에 제출하여야 한다.¹⁶⁾ 그 밖에 PIA의 평가 대상 및 절차 등은 「프라이버시 규정 이행에 대한 OMB 지침(OMB Guidance for

available at <<http://www.whitehouse.gov/omb/memoranda/m03-22.html#a>>

14) §208 of the E-Government Act.

B. Privacy Impact Assessments.

1. Responsibilities of Agencies.

b. Agency Activities.—To the extent required under subparagraph (a), each agency shall—

i. conduct a privacy impact assessment;

ii. ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and

iii. if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

15) §208 of the E-Government Act.

B. Privacy Impact Assessments.

1. Responsibilities of Agencies.

c. Sensitive Information.—Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.

16) §208 of the E-Government Act.

B. Privacy Impact Assessments.

1. Responsibilities of Agencies. d. Copy to Director.—Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.

Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22)」에 구체화되어 있다. 또한 「연방정보보안관리법(FISMA)¹⁷⁾」에서도 PIA를 포함한 프라이버시 및 보안관리 현황을 연간 의회에 보고토록 규정하고 있다.

PIA의 평가항목으로는 수집할 정보, 당해 정보를 수집하는 이유, 당해 정보의 용도, 정보 공유의 기관, 수집되는 정보 내용과 이를 공유하는 방식과 관련하여 개인의 동의를 얻기 위한 고지 등의 절차, 정보보호방안, 프라이버시법¹⁸⁾에 따른 기록시스템¹⁹⁾의 생성 여부 등에 관한 사항 등이 거론된다.²⁰⁾

17) The Federal of Information Security Management Act of 2002, 44 U.S.C. §3541, et seq.

18) 5 U.S.C. §552a, commonly referred to as Privacy Act of 1974; 미국은 스웨덴과 더불어 1966년에 ‘정보자유법(Freedom of Information Act; Public Information : agency rules, opinion, orders, records and proceedings, FOIA 1966)’을 제정함으로써 국가적 차원에서 입법조치를 단행한 첫 번째 나라에 속하지만 스웨덴에서처럼 우선적으로 개인의 프라이버시를 보호하고자 제정되지는 않았다. 미국에서 정보자유법의 제정목적은 먼저 국가행정의 투명성을 높힘으로써 연방행정부를 개혁하고자 한 것이다. 1972년 6월 발생한 Watergate 사건 이후 연방행정부가 갖고 있는 기록들에 적용될 뿐, 민간부문을 규제하지는 않는 정보자유법이 1974년에 개정되었고 그 뒤 연방기관들에 의한 개인정보의 수집을 제한하고 이들이 처리하는 개인정보의 유형에 관하여 일반시민에게 통지토록 요구하는 프라이버시법이 제정되었다.

19) 행정기관의 기록시스템에는 법률 또는 대통령의 집행명령에 의하여 달성하여야 할 당해 기관의 목적달성에 필요하고 이와 관련된 개인정보만을 관리하여야 한다; 5 U.S.C. 552a (e) (1) Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President.

20) §208(b)(2)(B)(ii) of the E-Government Act.

16 개인정보보호의 법적 쟁점과 과제

<표 1> OMB 지침에 따른 PIA 평가대상

구분	주요 내용
신규 시스템 구축 이전	<ul style="list-style-type: none"> ○ 국민의 개인정보를 수집, 관리, 배포하는 IT시스템이나 프로젝트의 개발 혹은 조달시 ○ 문서감축법에 따라 10명 이상의 개인정보를 온라인으로 수집하는 경우
절차 및 시스템 변경	<ul style="list-style-type: none"> ○ 종이문서 기반 기록을 전자시스템으로 변형하는 경우 ○ 기존 수집정보의 익명정보를 식별 가능한 형태의 정보로 변경하는 기능을 새로이 적용하는 경우 ○ 새로운 기술적용과 같은 기존 IT시스템의 신규 운용이 시스템 상의 식별 가능한 정보에 중대한 변화를 일으키는 경우 ○ 사용자 인증기술(예컨대, 패스워드, 전자인증서, 생체인식 등)이 공공 회원이 접근하는 전자정보시스템에 새로이 적용되는 경우 ○ 기관이 시스템적으로 상거래나 공공 자원으로부터 획득하거나 구매한 식별 가능한 형태의 정보 데이터베이스를 기존 정보시스템에 결합하는 경우 ○ 동시에 여러 기관이 유사한 전자정부 사업을 개시하거나 공동으로 IT투자 개발을 수행하는 경우에 식별 가능한 형태의 정보를 상호 교환하거나 신규로 정보를 사용하도록 하는 기능을 공유하는 경우 ○ 식별 가능한 형태로 시스템에 정보항목을 추가하거나 새롭게 정보를 사용 혹은 배포하는 결과를 유발하는 비즈니스 절차를 변경하는 경우 ○ 식별 가능한 형태의 정보 수집이 새로이 추가되어 개인 프라이버시에 위험을 야기하는 경우(예컨대, 건강정보 혹은 금융정보의 추가)
PIA 수행 예외 사항	<ul style="list-style-type: none"> ○ 일반 대중회원으로부터 식별 가능한 형태의 정보를 수집하거나 보관하는 IT시스템이 아닌 경우 ○ 피드백이나 추가정보 제공과 같은 제한적 목적만으로 사용자에게 접근하도록 선택사항을 지정한 경우(예컨대, 질의응답이나 코멘트) ○ 특정 국가보안시스템의 경우 ○ 모든 PIA 요소가 이미 프라이버시법의 컴퓨터 매칭 조항에 의해 결정되는 매칭 조약에 의해 처리되고 있는 경우 ○ 모든 PIA 요소가 엄격한 통계목적의 데이터 결합을 허용하는 기관간 조약에 의해 처리되고 있는 경우 ○ 해당 기관이 식별 가능한 형태의 정보를 생성하는 데이터베이스로부터 정보를 검색하거나 결합하지 않고, 개별 목적으로 식별 불가능한 정보만을 수집하거나 IT시스템을 개발하는 경우 ○ 새로운 프라이버시 위험을 발생시키지 않는 시스템의 작은 변경이나 수집의 경우

평가방법으로는 핵심정보시스템(Major information systems) 및 일반 DB시스템(Routine database systems)으로 구분하여, 핵심정보시스템의 경우 정보수집의 중대성, 정보흐름 분석, 계획 대비 정보수집과 처리의 변경사항, 적절한 위험절감 방법과 최종 디자인 설계, 비즈니스 프로세스의 선택의 이유에 대한 분석이 포함되어야 할 필요가 있는 것으로 규율되는 반면 일반DB시스템의 경우 사용과 접근이 제한되고 일상적인 정보를 포함하는 단순한 체크리스트나 템플릿을 이용한 보다 일반적인 PIA 평가가 적절한 것으로 규정되어 있다. 그리고 OMB 대상 예산 요청 여부와 상관없이 해당 기관에 대한 연간 보고서를 제출하되, ① PIA 수행 필요 정보 기술 시스템 혹은 PIA 수행결과 및 결과공개방법, ② 지속적인 추적 기술 사용 여부, ③ 자동화된 프라이버시 정책 적용 방법, ④ 연락처 정보 등의 사항이 포함되어야 한다.

FISMA의 경우 연방정부의 정보보안관리를 위해 프라이버시 및 보안 관리 현황을 매년 의회 및 OMB 매 예산 회기 시작 10월 1일까지에 보고서를 제출토록 의무화하고 있으며, 프라이버시 관련 일치된 견해를 도출토록 하기 위해 최고정보책임관(CIO; Chief Information Officers), 감독관(IG; Inspector General), 상위기관 프라이버시 감독관(SAOP; Senior Agency Official for Privacy)의 연간보고서 검토결과를 제출케 하고 있다.²¹⁾

21) 다만, 전자정부법과 OMB 지침에 의한 보고의무와 중복되므로 FISMA 보고로 전자정부법 보고의무를 대체할 수 있도록 'FISMA 보고 및 프라이버시 관리 보고 준비에 대한 지침(Instructions for Preparing the FISMA Report and Agency Privacy Management Report)'을 통해 제시하고 있으며, SAOP 검토 보고서 작성시 영향평가 및 기록통보시스템(SORN; A Systems of Record Notice) 의무 이행을 위한 시스템 목록 기재를 규정하고 있다. The Privacy Act of 1974는 제3절 제5편에서 신규 개인정보시스템이 구축되거나 변경될 때는 각 기록 시스템을 연방관보시스템에 발표하도록 요구하는 기록통보시스템(A Systems of Record Notice, SORN) 의무를 이행하도록 규정하고 있다. 지

18 개인정보보호의 법적 쟁점과 과제

한편, OMB 지침에서는 PIA 수행과정에서 분석되어야 할 주요 내용과 관련하여 다음과 같은 내용을 중심으로 순행되어야 하며, 이를 토대로 해당 부처는 IT 시스템이나 정보 수집에 어떤 선택적 조치를 취하였는지 밝혀야 함을 언급하고 있다.²²⁾

- 어떠한 정보가 수집되는가(정보의 성격 및 출처 등)
- 왜 그 정보가 왜 수집되어야 하는가(적격성의 결정 등)
- 정보의 이용목적(데이터 존재 여부의 확인 등)
- 누구와 수집된 정보를 공유하는가(특별히 계획된 목적으로 어떠한 부처와 개인정보를 공유하는가)
- 정보제공이 임의적인 경우에 개인이 정보제공을 거절해야만 하는 경우 또는 요청된 승인된 목적을 넘는 정보의 특정한 사용에 동의해야만 하는 경우가 어떤 경우인지 그리고 개인이 어떻게 동의를 표할 수 있는가
- 정보가 어떻게 보호되는가(관리적·기술적 조치)
- 프라이버시법에 의거하여 기록 시스템이 실행되는지 여부

또한 지침서에는 평가 대상의 특성·규모·복잡성 등에 따른 PIA 수행의 내용을 달리 언급하고 있다. 환원하자면, PIA를 수행함에 있어서 그 정도와 내용은 수집할 정보의 특성과 IT 시스템의 크기 및 복잡성에 적합하여야 함을 분명히 하고 있는 것이다.

난 3월 제출된 2008년 FISMA 보고에 대하여는 See <www.whitehouse.gov/omb/asset.aspx?AssetId=835>.

22) See Joshua B. Bolten, *supra* note 13, Attachment A of E-Government Act Section 208 Implementation Guidance, II. C.

<표 2> 미국 OMB의 PIA 수행 절차

IT 개발단계	<ul style="list-style-type: none"> ○ 시스템 개발과 관련된 문서(계획서 등)에는 개발 필요성에 대한 설명, 기능 요건 분석, 실현성 분석, 혜택/원가분석과 특히 초기 위험에 대한 평가 등의 프라이버시 내용이 포함되어야 함 ○ 개발 할 시스템이 개인의 프라이버시에 미치는 영향, 특히 PIA 수행시 분석하여야 할 내용의 각 항목과 관련된 잠재적인 위험을 규명하고 평가하는 내용을 개발 초기단계에 알고 있는 한 최대한 포함되어야 함 ○ 시스템 전개에 앞서 다음과 같은 사항을 위하여 반드시 PIA는 업데이트 되어야 함 <ul style="list-style-type: none"> - 정보의 보유 또는 처리 등 시스템 구상(계획) 단계에서 인지되지 못한 요소들을 고려하기 위하여 - 새로운 정보 수집 사항을 반영하기 위하여 - 분석 결과에 의거 시스템이나 정보 수집 설계 시 선택된 사항들을 다루기 위하여
통상적인 데이터 베이스 시스템	<ul style="list-style-type: none"> ○ 통상적인 정보를 다루는 시스템 또는 이용과 접근이 제한된 시스템에 대한 PIA 수행의 경우 체크리스트와 같은 표준화된 수단을 사용할 수 있음
주요 정보 시스템	<ul style="list-style-type: none"> ○ 다음과 같은 추가분석이 반영되어야 함 <ul style="list-style-type: none"> - 수집 결과 및 정보의 흐름 - 바람직한 수집 및 취급 대안 - 각 대안별로 확인된 위험의 경감 방안 - 설계와 업무 처리 절차의 최종 결정 방안에 대한 이론적 근거

한편 각 부처는 각 단계에서의 정보 취급이 개인의 프라이버시에 미치는 영향을 평가하는 경우 정보의 생애주기, 즉 개인정보의 수집·사용·보유·처리·공개 및 파괴 등 information life cycle을 고려하여야 하며, PIA가 포괄적이고 의미 있는 내용을 갖추기 위하여 IT 정보보안, 기록 관리

및 프라이버시 분야의 전문가 등의 협조체제가 필요함을 규정하고 있다.²³⁾

OMB 지침서는 PIA 수행 보고서의 검토 및 공개와 관련하여 각 행정기관은 PIA 문서와 요약서가 당해 부처의 검토 담당공무원에 의하여 승인되었는지 여부를 확인하여야 하며, 2005 회계 연도에 반영되고 OMB의 지침서에 적합한 각 IT 시스템의 PIA는 OMB에 제출되어야 한다고 하고 있다. 또한 가능한 한 요약서를 포함한 PIA 수행보고서는 예산이 지원되는 시스템의 정보 공개에 관한 행정부서의 정책에 따라 일반 대중에게 공개되어야 하며, 각 행정기관은 문서의 공개가 보안상 우려될 경우 공개하지 않거나, 예컨대 ① 국가보안관련 정보, ② 잠재적으로 국가의 이익을 손상하거나 법에 의거 그 공개가 금지된 정보, ③ 경쟁적인 기업 이익에 관한 정보 등과 같이 문서에 포함된 비밀정보에 대하여 일반 대중이 이용하지 못하도록 결정할 수 있으며 식별 가능한 형태의 정보를 PIA에 포함하는 것을 금지하고 있다.²⁴⁾

23) See Joshua B. Bolten, *supra* note 13, Attachment A of E-Government Act Section 208 Implementation Guidance, II. C. 2.

b. Information life cycle analysis/collaboration. Agencies must consider the information “life cycle” (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals’ privacy. To be comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.

24) See Joshua B. Bolten, *supra* note 13, Attachment A of E-Government Act Section 208 Implementation Guidance, II. C. 3.

Review and publication. a. Agencies must ensure that:

i. the PIA document and, if prepared, summary are approved by a “reviewing official” (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);

ii. for each covered IT system for which 2005 funding is requested, and

(2) 캐 나 다

캐나다의 경우 프라이버시감독관(privacy commissioner)²⁵⁾이 영향평가 제도를 도입할 것을 제안하였으며, 2002년 5월 프라이버시 영향평가 정책(Privacy Impact Assessment Policy)을 발표하여 연방정부에 프라이버시 영향평가(PIA) 도입을 의무화하고 같은 해 8월 이를 구체화한 PIA 지침(Guideline: A Framework to manage Privacy Risks)²⁶⁾이 재무부장관에 의해 고시되었다.²⁷⁾ 이에 따라 프라이버시감독관은 영향평가 결과에 따른

consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 3008); and
iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).

1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment⁹. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).

2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds

25) 캐나다 연방프라이버시법 제53조제1항(The Governor in Council shall, by commission under the Great Seal, appoint a Privacy Commissioner after consultation with the leader of every recognized party in the Senate and House of Commons and approval of the appointment by resolution of the Senate and House of Commons.)에 의해 의회 소속하에 설립된 프라이버시감독관은 상·하원에 직접 보고한다; Privacy Act (R.S., 1985, c. P-21) §38 (The Privacy Commissioner shall, within three months after the termination of each financial year, submit an annual report to Parliament on the activities of the office during that financial year.)

26) http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld-eng.asp

27) 캐나다 연방프라이버시법 제71조제1항제4호(the designated Minister shall

22 개인정보보호의 법적 쟁점과 과제

조언을 제공하도록 하고 있으며, 각 기관은 대국민 프로그램 및 서비스를 개발 및 시행함에 있어 PIA를 의무적으로 실시하여야 한다. 이를 통해 대국민 프로그램 및 서비스가 프라이버시 관련 법률을 준수하고 있는지를 판단하고, 관리책임자 또는 정책결정자로 하여금 프라이버시 침해 가능성을 해소하거나 경감할 수 있도록 지원하며, 철저한 검증을 거쳐 각종 정책이나 프로그램·시스템의 이용을 촉진할 수 있도록 지원하고 있다.²⁸⁾

캐나다에서는 법률내 영향평가 관련 사항을 규정하지 않고 2002년 중 연방정부가 프라이버시 영향평가 정책 및 이를 구체화한 지침 고시를 통해 공공기관의 자율 수행을 권고한 것인바, 그 밖에 Alberta, British Columbia, Ontario 등 3개 주(州)에서 영향평가 가이드 및 지침을 작성·배포한 바 있다. 또한 일부 주에서는 보건 의료 기관 등 일부 분야에 대한 영향평가 시행을 의무화하고 있는바, British Columbia의 경우 정보의 자유 및 프라이버시보호에 관한 법률(FOIPPA, Freedom of Information and Protection of Privacy Act)내 정부부처 및 공공기관이 법제·시스템·프로젝트 및 프로그램 신규 도입시 의무화를 규정하고 있고, Alberta의 경우 의료정보법(Health Information Act) 내 의료정보 보유기관의 경우 의료정보 수집·이용·공개, 데이터 비교작업(Data Matching) 시 PIA 수행토록 의무화하고 있으며, Ontario의 경우 개인 의료 정보 보호에 관한 법률(PHIPA, Personal Health Information Protection Act)내 의료정보네트

cause to be prepared and distributed to government institutions directives and guidelines concerning the operation of this Act and the regulations) 및 재무관리법 제7조에 따라 재무부장관은 연방프라이버시법의 시행에 관한 지침을 제정할 수 있다. 현재 캐나다는 프라이버시 및 개인정보 보호와 관련하여 공공부문을 규율하는 연방프라이버시법 이외에도 민간부문에 적용되는 「개인정보보호 및 전자문서에 관한 법률(Personnel Information and Electronic Documents Act)」가 존재한다.

28) <http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12450§ion=text>

워크 제공자에 한해 PIA를 수행토록 규율하고 있다.

캐나다에서 PIA는 공공기관에서의 프라이버시 침해가 예상되는 시스템, 프로그램, 프로젝트, 법제 등 추진 시를 대상으로 하는바, 그 절차적 내용은 다음과 같다.

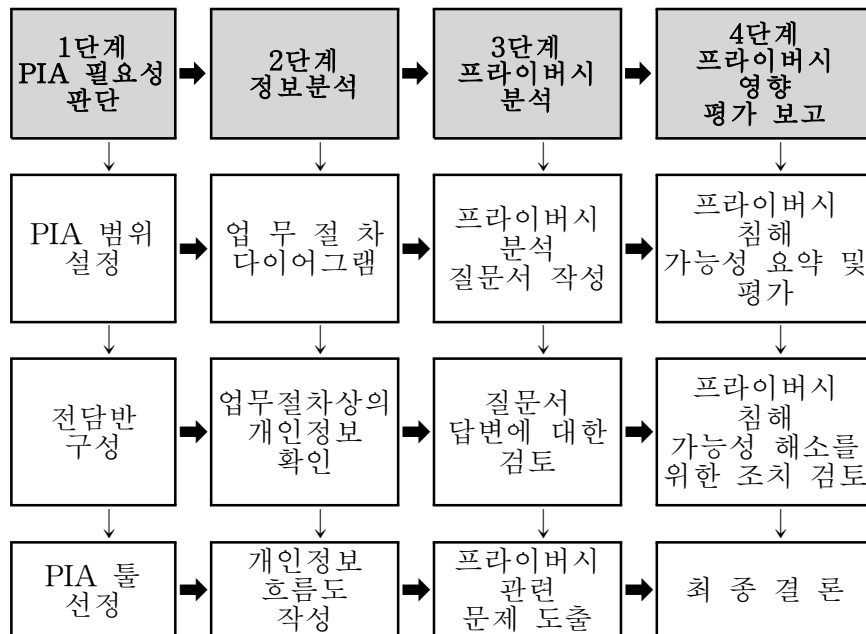
<표 3> 캐나다 공공기관의 PIA 수행 대상

신규 도입	<ul style="list-style-type: none"> ○ 개인의 동의여부와 상관없이 개인정보에 대한 신규 혹은 추가 수집, 이용, 공개되는 경우 ○ 수집 대상 인구가 확장되는 경우 ○ 개인정보 수집 방식이 직접 수집에서 간접 수집으로 바뀌는 경우 ○ 프로그램 통합 및 관리 목적으로 개인정보의 수집이 확대되는 경우 ○ 새로운 데이터 비교 작업이나 프로그램 간 혹은 조직, 관할권, 부서 간 추가적인 개인정보의 공유가 이루어지는 경우 ○ 개인정보의 물리적 혹은 논리적인 분할에 영향을 미치는 비즈니스 프로세스와 시스템에 중요한 변화가 있는 경우나 개인정보의 관리와 접근통제에 사용되는 정보보호 메커니즘에 중대한 변화가 발생한 경우 ○ 다른 수준의 정부기관이나 민간기관으로의 프로그램이나 서비스를 이관하는 계약을 한 경우 ○ 공통 개인 식별자들의 신규 이용 개발 및 확장 개발의 경우 ○ 대중들의 부정적인 반응이 예상되는 경우
기존 사업	<ul style="list-style-type: none"> ○ 서비스가 근본적으로 재설계될 경우 ○ 서비스 전송 채널이 근본적으로 재설계된 경우 ○ 서비스가 개인정보의 수집, 이용, 제공에 영향을 끼칠 수 있는 방식으로 전자전달수단으로 변경되었을 경우

24 개인정보보호의 법적 쟁점과 과제

<표 4> 캐나다 개인정보 영향평가 관련 지침

범 위	성 격	연 도	발 행 물 명	발 행 기 관
National Government	Process Overview	2002	Privacy Impact Assessment Policy	Treasury Board of Canada Secretariat
	Guide	2002	PIA Guidelines: A Framework to Manage Privacy Risks	
	Supplement	2003	Report on PIA Best Practices	
	Audit Guide	2003	PIA e-learning tool	
	Background	2004	Privacy Impact Assessment Audit Guide	
British Columbia	Process Overview	2006	Privacy Impact Assessment Process	Ministry of Labour and Citizens' Services
	Supplement	-	Privacy Impact Assessment Form and Process	-
Ontario	Guide	2001	Privacy Impact Assessment: a User's Guide	Management Board Secretariat, IPO
	Guide	2005	Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act	Information and Privacy Commissioner/ Ontario



<그림 2> 캐나다 프라이버시 영향평가 절차도

(3) 뉴질랜드

원래 PIA 개념은 뉴질랜드에서부터 논의가 시작된 것이다. 뉴질랜드 Office of Privacy Commissioner의 Blair Stewart는 1996년 'Privacy Law and Policy Reporter'²⁹⁾에서 PIA 개념 및 필요성을 제기하였고 2003년에는 PIA를 국제적으로 확산하기 위하여 관련 워크숍을 개최하였다.³⁰⁾ 하지만 뉴질랜드의 개인정보보호 일반법인 1993년 Privacy Act에서는 명시

29) <http://austlii.law.uts.edu.au/au/journals/PLPR/1996/64.html>

30) 워크숍(International Workshop on Privacy Impact Assessment)의 관련자료 및 문헌목록 등에 대하여는 See Blair Stewart, *Privacy Impact Assessment On-Line Resources*, 2003. available at <www.foi.gov.uk/sharing/toolkit/pia_online_res.pdf>

적으로 PIA를 규정하고 있지 않다.

뉴질랜드는 공공·민간 분야를 구분하지 않고 기관의 개인정보보호와 신뢰 구축을 위해 자발적으로 영향평가를 수행하도록 권고하고 있으며, 1997년 이후 운전면허, 의료정보, 교육 등의 분야에서 실행 중에 있다. 한편, 평가 수행을 위하여 프라이버시감독관(privacy commissioner)³¹⁾이 프라이버시 핸드북을 마련하여 평가의 목적, 대상, 원칙, 보고서작성 등에 관한 지침을 마련하고 있는바, 다음과 같이 개인정보를 취급하는 모든 공공 및 민간 부문, 특히 중대형 기업 및 정부 기구와 신규 프로젝트 추진 시에 PIA 수행을 권고한다.

31) Privacy Act 1993 §12 (Privacy Commissioner) (1) There shall be a Commissioner called the Privacy Commissioner.

(2) The Commissioner shall be appointed by the Governor-General on the recommendation of the responsible Minister.

(3) The Commissioner shall be a corporation sole with perpetual succession and a seal of office, and shall have and may exercise all the rights, powers, and privileges, and may incur all the liabilities and obligations, of a natural person of full age and capacity.

(4) The Commissioner shall be a Crown entity for the purposes of the Public Finance Act 1989.

Privacy Act 1993 §14 (Commissioner to have regard to certain matters) In the performance of his or her functions, and the exercise of his or her powers, under this Act, the Commissioner shall---

(a) Have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the right of government and business to achieve their objectives in an efficient way; and

(b) Take account of international obligations accepted by New Zealand, including those concerning the international technology of communications; and

(c) Consider any developing general international guidelines relevant to the better protection of individual privacy; and

(d) Have due regard to the information privacy principles and the public register privacy principles.

- 뉴질랜드의 거의 모든 국민들의 개인정보를 가지고 있는 데이터 웨어하우스의 경우처럼 PIA의 필요성과 관련하여 눈에 띄는 규모와 특성을 가지고 있는 프로젝트
- 사람들에게 데이터 처리에 있어 그 효과가 그다지 널리 알려져 있지 못하거나 신뢰를 받지 못하고 있는 최신 기술이 적용된 애플리케이션
- 본질적으로 명백한 프라이버시 침해 위험을 가지고 있어 PIA 수행으로 인한 장점이 확실하게 예상되는 경우
- 접근 가능한 데이터베이스로 기밀정보가 수집되는 모든 프로젝트
- 새로운 형식의 고객 프로파일링이 가능하도록 내부 비즈니스 데이터베이스가 통합되는 경우
- 다국적 기업의 직원 기록이 집중화된 경우
- 정보가 수집되는 방식을 변경하는 경우
- 현존 기술들을 통합하거나 새로운 기술을 적용하는 경우
- 새로운 환경에서 이미 알려진 프라이버시 침해 기술이 사용 되는 경우

PIA는 영향평가의 필요성을 판단하기 위한 예비분석부터 준수방안 마련까지 일련의 과학적 평가 과정을 거쳐 이루어져야 한다. 프라이버시영향평가는 먼저, 프로젝트 수행을 위해 과연 영향평가가 필요한가의 여부를 판단하는 ‘예비 프라이버시 분석’을 시작하고 그에 따라 영향평가 수행을 확정하면 평가의 시기를 확정하여야 한다. 평가 시기가 확정되면 수행되는 프로젝트 계획에서 정보의 흐름을 파악하여 각 흐름에 따른 프라이버시 위험요소를 분석하여야 한다. 그리고 위험 요소에 대한 분석이 완료되면 분석 결과를 토대로 위험평가를 실시하여 개선 및 대응방안을 마

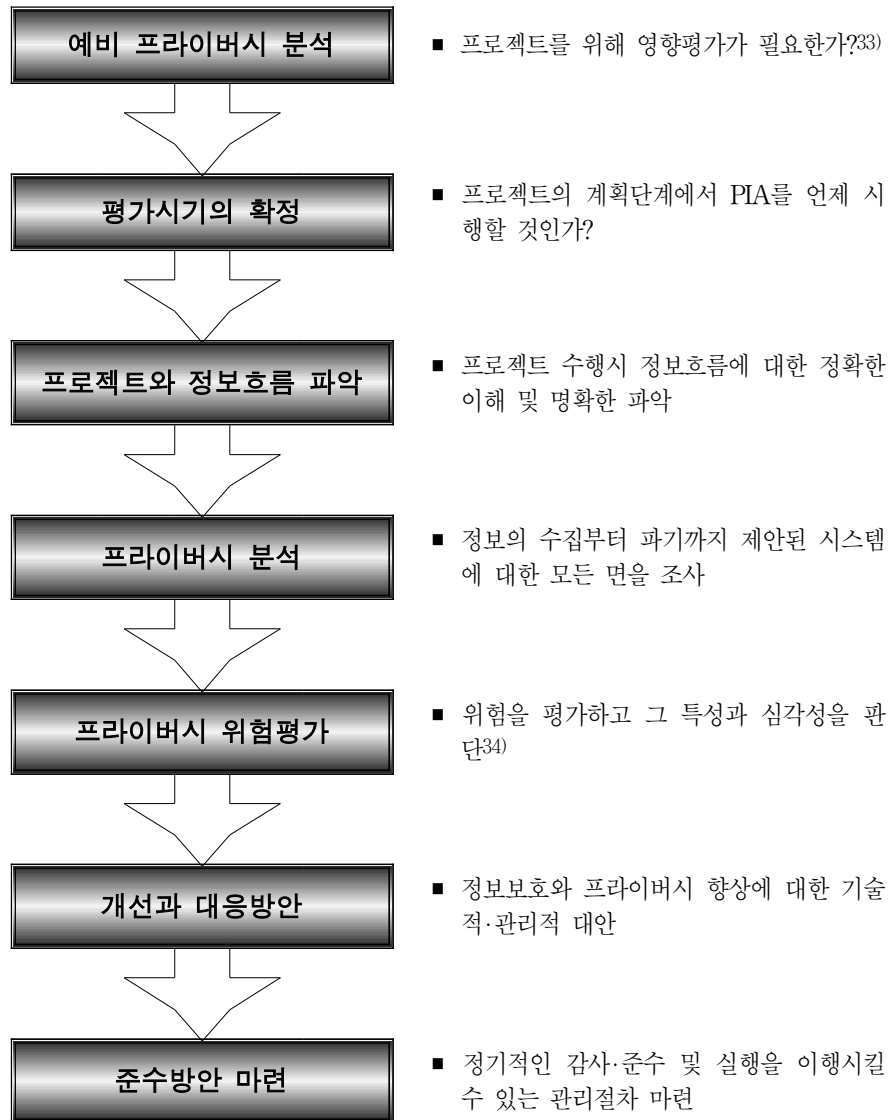
28 개인정보보호의 법적 쟁점과 과제

련하여야 한다. 최종적으로 프라이버시 사전 영향평가 수행을 완료하고 그에 따른 보고서를 작성하여 프라이버시 준수 방안을 마련하여 시행하여야 한다.³²⁾

<표 5> 뉴질랜드의 주요 PIA 사례

시행 년도	프로젝트명	수행 영역
1997	Driver Licensing : photo driver licence	정부
1998	Insurance Claims Register	업계
1998	Health Intranet	의료
1999	KidZnet Child Health Information	의료
2000	Diabetes Disease Management	의료
2000	National Student Index Number	교육
2001	Justice Sector Code for Infringement Information	정부
2001	Pharmacy Primary Integration Network	의료
2001	Transport Operator Safety Rating	정부
2002	Manukau City CRS	정부
2003	e-government on-line authentication project (1차)	정부
2004	e-government on-line authentication project (2차)	정부

32) 프라이버시 영향평가 보고서에 포함되어야 할 사항으로는 파악된 프라이버시 위험에 대한 설명 이러한 위험을 줄이거나 피하기 위해 고려해야 할 사항의 분석, 해결할 수 없는 잔여 위험의 목록과 개인, 일반대중, 주주반응과 프로젝트의 성공에 대해 이러한 위험의 가능한 관련의 분석 등이 반영되어야 한다. 프라이버시 영향평가 수행을 완료하였을 경우 예상되는 위험에 대하여 개선할 수 있는 대응방안을 마련하여야 한다. 이러한 대응 방안 중 보안 대응으로 프라이버시를 향상시키기 위해서는 정보의 민감도에 따른 보안장치와 특별한 정보처리 관행이 동시에 이루어져야 한다.



<그림 3> 뉴질랜드 PIA 절차도³⁵⁾

33) <http://www.e-government.govt.nz/docs/authent-pia-prelim/index.html>

34) 프라이버시영향평가지 어떤 위험이 심각하고 어떤 위험이 사소한가를 분류하

(4) 호 주

뉴질랜드와 인접국인 호주에서도 프라이버시기구(Privacy Agencies of New Zealand and Australia; PANZA) 회의³⁶⁾를 통해 PIA 개념을 정립하여 실시하고 있다. 호주 역시 PIA를 실시하도록 규정하고 있는 법률은 없으며, Privacy Commissioner는 자율적인 PIA 수행을 지원하기 위하여 2004년 11월에 'Managing Privacy Risk'라는 이름의 가이드라인(안)을 제시한 바 있으며,³⁷⁾ 연방정부 가이드라인보다 조금 앞선 같은 해 8월 빅토리아주에서도 주 정부기관 등이 참조할 수 있는 가이드라인³⁸⁾이 발간되었다.

호주의 PIA는 미국이나 캐나다와는 다르게 해당 기관에 의해 자율적

여야 하며, 프라이버시 영향 보고서는 피할 수 있는 위험을 파악하고, 위험을 적절한 수준으로 경감시킬 수 있는 비용 효율적인 대책을 제안하여야 한다. 한편 위험감소대책 마련시 고려사항으로는 위험으로 인해 발생하는 가장 최악의 결과는 무엇인지에 대한 사항, 보안이 침해되었거나, 절차를 준수하지 않았다면, 결과적으로 개인에게 어떤 영향을 미칠 것인가에 대한 사항, 일반 대중이나 고객이 제안된 시스템내의 개인정보에 대해 민감한 반응을 보이는가에 대한 사항, 정보가 국내에서 보유될 것인지, 국외로 전송될 것인가의 여부 등이 검토되어야 한다.

35) [http://www.e.govt.nz/policy/governance/business-case-07/chapter5.html/view?searchterm=Privacy Impact Assessment Process Flow](http://www.e.govt.nz/policy/governance/business-case-07/chapter5.html/view?searchterm=Privacy%20Impact%20Assessment%20Process%20Flow)

36) 뉴질랜드와 호주의 연방 및 각주 개인정보감독기구 상호간 정보교환을 위한 정기회의로서, 년 2회 개최된다. See generally Karen Curtis & Marie Shroff, *Memorandum of Understanding between the Office of the Australian Privacy Commissioner and the Office of the New Zealand Privacy Commissioner*, 2006, pp.4~6. available at <www.privacy.org.nz/assets/Files/2072970.doc>

37) Office of the Privacy Commissioner, *Managing Privacy Risk: An Introductory Privacy Impact Assessment for Australian Government and ACT Government Agencies*, Australian Government, 2004. available at <www.privacy.gov.au/publications/mprdraft.pdf>

38) [http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/\\$FILE/OVPC_PIA_Guide_August_2004.pdf](http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/FFC52F3B3A208C34CA256EF800819403/$FILE/OVPC_PIA_Guide_August_2004.pdf)

으로 실시되며, PIA 보고서도 Privacy Commissioner이나 예산편성 주관 부처에 제출할 의무를 가지지 않기 때문에 보고서가 공개되지 않는 경우가 많다. PIA 수행도 해당기관 자체 또는 외부 컨설팅기관에 의뢰하여 실시하고 있다. 호주의 Privacy Commissioner는 프라이버시 문제를 야기할 우려가 있는 프로젝트에 대해 PIA를 실시할 것을 권고하고 해당기관이 PIA를 실시함에 있어 자문을 요청하거나 공동 실시를 요청해 올 경우에 한하여 전문적인 도움을 주고 있을 뿐이다.

호주 PIA 가이드라인에서는 PIA를 실시하여 도움을 얻을 수 있는 경우를 다음과 같이 제시하고 있지만, 한편으로는 모든 새로운 프로젝트나 현존 시스템의 모든 분석에 PIA를 필요로 하지는 않을 것이며, PIA가 필요하다고 판단되거나 바람직한 곳에서 수행할 것을 권고하고 있다.

호주는 뉴질랜드에 비하여 상대적으로 PIA가 활발하게 수행되고 있지는 않다. 이는 호주의 경우 연방정부와 6개의 주 정부로 나뉘어져 있으므로 뉴질랜드보다는 PIA 시행을 위한 구심점이 분산되어 있기 때문으로 여겨진다. 통계청 인구조사시스템(Census Enhancement Proposal; CEP), 연방정부인증프로그램(Commonwealth Government Authentication Initiative) 등 소수의 연방차원 정부 프로젝트에서 PIA를 실시한 바 있으며, 지방정부에서는 시드니 교통 시스템 구축사업 등에서 실시한 사례가 있다. 민간차원에서는 호주의 대형 소매업체가 공공분야의 PIA 모델을 자사에 적용해 볼 의사를 개진하여 Privacy Commissioner의 도움을 받고 있는 정도가 알려져 있다. 그 가운데 통계청이 외부 컨설팅기관인 Pacific Privacy Consulting에 의뢰하여 수행한 CEP PIA의 경우 호주 연방 Privacy Commissioner가 제시한 PIA 가이드라인(안)을 평가기준으로 사용하였다. CEP PIA 수행자는 2006년 통계조사 방법이 권한 없는 자의

접근, 권한 있는 자의 오남용, 의도하는 바로부터 얻을 수 있는 이익을 초과하는 프라이버시 침해 요인이 있다고 평가하고 ① 이름과 주소를 연결하는 인구조사 강화방안은 2001년 방법으로의 복귀를 검토하는 것이 바람직하다는 점, ② 이름과 주소를 연결하는 계획안이 포기된다면 통계청은 인구조사 양식에서 이름 정보의 기입을 요구를 제한하는 개인정보보호법 개정을 고려해야 한다는 점, ③ 만일 계획안이 실행된다면 통계청은 인구조사 DB에 관련한 프라이버시와 기밀을 보호하기 위해 계획된 모든 관리적 대책을 적용해야 한다는 점, ④ 통계청은 통계목적에 특정 개인에 관련한 사항은 포함되지 않음을 관련 법률에 포함하는 것을 고려해야 하며 그러한 법률의 개정에는 Privacy Commissioner와의 협의가 이루어져야 할 것이라는 점 등과 같은 사항을 권고하였다. 이에 따라 호주 통계청은 PIA 결과를 공개하고 연방 및 각 주 Privacy Commissioner의 의견을 수렴하는 등 도출된 문제점을 보완하는 작업을 실시하였다.

2. 법안의 주요내용

이미 언급한 바와 마찬가지로 공공부문이나 민간영역을 막론하고 개인정보 수집·이용 등이 증대됨에 따라 개인정보의 대량 유출로 인한 피해 우려가 사회적 쟁점으로 제기되고 있을 뿐만 아니라 신규 정보시스템의 구축이나 개인정보의 취급에 앞서 사전에 국민의 프라이버시에 미칠 영향을 조사·검토하여 개인정보 권리침해의 위험성을 최소화하는 제도 도입의 요구가 증가하고 있다. 그리고 이미 선진 각국에서 일부분 의무화되어 시행되어 오고 있는 개인정보 영향평가를 적어도 공공기관에 대하여는 의무화하도록 하는 규정이 개인정보보호법(안)에 반영되어 있다. 개인정보의 수집·활용이 수반되는 사업 추진에 있어 개인정보의 유출·오남용으로 인한 프라이버시 침해가 없는지를 조사·예측·검토하여 개선하는 체

계적인 절차가 바로 개인정보 영향평가 제도이기 때문이다. 여기서는 2005년 이후 시범적으로 시행되어 온 개인정보 영향평가 사례³⁹⁾를 기반으로 공공기관 의무화 제도 도입을 위한 구체적인 방법 및 절차를 사전에 검토하여 국회 법안 심의과정 또는 대안 마련 과정에서 반영 가능성을 검토하는 한편, 하위법령의 구체화 방향을 짚어보기 위한 법안현황을 파악하기로 한다.

우선 1안은 평가 대상 및 방법 등은 하위 법령으로 위임하고, 개인정보 파일 등록시 평가 결과를 제출토록 하고 있으며, 영향평가 수행시 처리하는 개인정보의 수, 제3자 제공 여부, 정보 주체의 권리를 해할 가능성 및 그 위험 정도를 고려하도록 규정하고 있다. 한편, 2안과 3안은 개인정보 파일 신규 구축·확대·변경시 및 다른 개인정보 파일과 연동시를 의무대상으로 규정하고 확대·변경이 경미한 경우는 개인정보보호기구인 위원회에 대한 통지로 갈음토록 하고 있으며, 또한 지정된 요건의 평가·인증 기관에 의뢰하여 평가를 실시할 수 있도록 규정하고 있는 실정이다.

39) 시범사례로는 2005년 7월부터 8월까지 이동통신사 대리점·판매점 대상 시범평가가 실시된 것을 효시로 하여 같은 해 10월 주민등록번호 대체수단 관련 5개 본인확인기관에 대한 영향평가가 시행된 예를 꼽을 수 있다. 또한 같은 해 12월에는 이른바 ‘기업 개인정보 영향평가 수행 가이드’ 마련 및 보급 등이 이루어졌으며, 2006년 7월부터 8월까지 이동통신사 모바일 RFID 시범서비스로서 디지털콘텐츠 감상 및 정보 제공을 가능케 하는 SKT U-포털 서비스와 KTF 양주진품 정보제공 서비스를 대상으로 자체 영향평가가 실시된 바 있다. 한편 2007년 5월에는 서울시 승용차 요일제 시스템의 개인정보 관리 규정, 정보보호 조치, 연계 기관에 정보 제공 범위 및 관리 체계 등을 점검함으로써 서울시 RFID 승용차 요일제 영향평가 지원이 이루어졌으며, 같은 해 10월부터 12월까지 신여권통합정보관리시스템상에서의 개인정보 취급·관리 체계점검, 생활기록부 등 교육부 교무학사에서의 수집되는 정보의 수집방법 및 활용 현황, 관련기관에 제공되는 개인정보의 관리 등 점검함으로써 외교부 전자여권 및 교육부 NEIS 영향평가 지원이 행해졌다. 그밖에도 정보보호컨설턴트, 공공·민간 개인정보보호 담당자를 대상으로 한 ‘개인정보 영향평가 전문 교육과정’이 운영되었으며, u-IT 확산 사업 등 총 16개 공공분야 사업 대상 개인정보 영향평가를 실시하여 181건의 개선사항을 도출한 예가 있었다.

<표 6> 법안별 개인정보 영향평가 규율내용

1안	2안	3안
<p>제31조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 하고 그 결과를 행정안전부장관에게 제출하여야 한다.</p> <p>② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.</p> <p>1.처리하는 개인정보의 수</p> <p>2.개인정보의 제3자 제공 여부</p> <p>3.정보주체의 권리를 해할 가능성 및 그 위험 정도</p> <p>③ 행정안전부장관은 제1항에 따라 영향평가 결과를 받았을 때</p>	<p>제36조(영향평가의 실시) ① 개인정보처리자는 대량의 개인정보 또는 민감정보가 포함된 개인정보파일을 새로 구축하는 등으로 인하여 생활침해 위험이 크다고 판단하는 경우에는 다음 각 호의 사항을 고려하여 미리 그것이 개인정보보호에 미칠 영향을 평가(이하 “영향평가”라 한다)할 수 있다.</p> <p>1.취급·처리하게 될 개인정보의 양과 종류</p> <p>2.제3자에 대한 개인정보의 제공 여부</p> <p>3.정보주체의 권리를 침해할 가능성</p> <p>4.그 밖에 대통령령으로 정한 사항</p> <p>② 공공기관이 대통령령으로 정한 개인정보파일을 새로 구축하거나 확대 또는 변경하고자 하는 경우</p>	<p>제32조(개인정보 영향평가) ① 공공기관이 대통령령에서 정하는 개인정보파일을 새로 구축하거나 확대 또는 변경하고자 하는 경우 또는 다른 개인정보파일과 연계하거나 연동하고자 하는 경우에는 다음 각 호의 모든 사항을 고려하여 미리 그것이 개인정보에 미칠 영향을 평가(이하 “영향평가”라 한다)하여야 한다.</p> <p>1.취급하는 개인정보의 양과 내용</p> <p>2.개인정보의 제3자 제공 여부</p> <p>3.개인정보파일의 연동·연계 여부</p> <p>4.정보주체의 권리를 해할 가능성</p> <p>5.그 밖에 대통령령으로 정한 사항</p> <p>② 개인정보위원회는 다음 각 호의 어느</p>

<p>에는 그 평가 결과에 대하여 보호위원회의 심의를 거쳐 의견을 제시할 수 있다.</p> <p>④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제30조제1항에 따라 등록할 때에는 그 평가 결과를 함께 첨부하여야 한다.</p> <p>⑤ 행정안전부장관은 영향평가의 활성화를 위하여 관계 전문가의 육성, 평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.</p> <p>⑥ <u>영향평가의 방법 및 절차, 평가 기준 등에 관하여 필요한 사항은 대통령령으로 정한다.</u></p> <p>⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.</p>	<p>또는 다른 개인정보파일과 연계하거나 연동하고자 하는 경우에는 제1항 각 호의 사항을 고려하여 영향평가를 실시하여야 한다. 다만, 개인정보파일의 확대, 변경, 연계, 연동이 경미한 경우에는 그 사실을 개인정보보호위원회에 통지하고 영향평가를 생략할 수 있다.</p> <p>③ 개인정보보호위원회는 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 개인정보처리자로 하여금 영향평가를 실시하도록 권고할 수 있다.</p> <p>1.개인정보처리자가 운영하고 있는 개인정보파일과 관련하여 개인정보의 유출, 도용 등의 사례가 자주 발생하는 경우</p> <p>2.처리되는 개인정보의 양, 개인정보의 민감성, 처리목적, 처리방법 등을 고려하여 개인정보침해</p>	<p>하나에 해당하는 사유가 발생한 경우에는 해당 공공기관으로 하여금 영향평가를 실시하도록 권고할 수 있다.</p> <p>1.제1항의 사유가 발생하였음에도 해당 공공기관이 사전평가를 실시하지 아니한 경우</p> <p>2.해당 공공기관이 운영하고 있는 개인정보파일과 관련하여 개인정보 유출·도용·오남용 등의 사례가 자주 발생하는 경우</p> <p>3.해당 공공기관이 운영하거나 운영하고 있는 개인정보파일과 관련하여 개인정보의 유출·도용·오남용 위험이 현저히 우려되는 경우</p> <p>③ 제1항과 제2항에 따라 영향평가를 받은 공공기관은 평가결과를 대통령령으로 정하는 바에 따라 지체 없이 개인정보위원회에 제출하여야 하며 개인정보위원회</p>
---	---	--

<p>⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.</p>	<p>위험이 현저히 우려되는 경우</p> <p>④ 개인정보처리자는 영향평가를 제38조제1항에 따라 지정된 평가·인증기관에 의뢰하여 실시할 수 있다.</p> <p>⑤ 제1항에 따른 영향평가의 평가기준, 평가절차 등에 관하여 필요한 사항은 대통령령으로 정할 수 있다.</p> <p>제37조(영향평가 결과의 공개) 제36조제2항 및 제3항에 따라 영향평가를 받은 개인정보처리자는 평가결과를 대통령령으로 정하는 바에 따라 지체 없이 개인정보보호위원회에 제출하여야 하며 개인정보보호위원회는 이를 대통령령으로 정하는 방법에 따라 일반인에게 공개하여야 한다.</p>	<p>는 이를 대통령령으로 정하는 방법에 따라 일반인에게 공개하여야 한다.</p> <p>④ 공공기관은 영향평가를 제52조제1항에 따라 지정된 지정평가·인증기관에 의뢰하여 할 수 있다.</p> <p>⑤ 개인정보파일의 확대, 변경 등이 경미한 경우에는 그 사실을 개인정보위원회에 통지하고 제1항에 따른 영향평가를 생략할 수 있다.</p> <p>⑥ 영향평가의 방법 및 절차, 평가기준 등에 관하여 필요한 사항은 대통령령으로 정한다.</p>
--	---	--

제3절 법제화 방향

(1) 평가대상 기준

미국 전자정부법은 각 연방기관(Agency)이 ① 식별가능한 형태로 정보를 수집, 보관, 배포하는 정보 기술의 개발 혹은 구축 ② 새로운 정보 수집 이전으로 규정하고 있으며, OMB 지침에서는 신규 시스템 구축 이전과 절차 및 시스템 변경으로 구분하여 보다 구체적인 총 10개의 경우를 제시하고 있다. 특히 경미한 시스템 변경 등 PIA를 수행하지 않는 경우 또한 별도로 규정하고 있는 실정이다. 그리고 캐나다, 호주, 뉴질랜드의 경우 PIA는 자율시행이 원칙이며 개인정보의 양, 정보 민감도, 프라이버시에 미치는 영향 등을 고려하여 신규 사업 추진시나 기존 시스템을 대상으로 평가 수행토록 권고하고 있는 것이 현실이다. 다만, 캐나다의 경우 일부 주(州)에서 의료정보의 수집·이용시 영향평가를 의무화하고 있기도 하다.

<표 7> 주요국의 PIA 실시 대상

캐나다	신규 도입	<ul style="list-style-type: none"> • 개인의 동의여부와 상관없이 개인정보에 대한 신규 혹은 추가 수집, 이용, 공개되는 경우 • 수집 대상 인구가 확장되는 경우 • 개인정보 수집 방식이 직접 수집에서 간접 수집으로 바뀌는 경우 • 프로그램 통합 및 관리 목적으로 개인정보의 수집이 확대되는 경우 • 새로운 데이터 비교 작업이나 프로그램 간 혹은 조직, 관할권, 부서 간 추가적인 개인정보의 공유가 이루어지는 경우 • 개인정보의 물리적 혹은 논리적인 분할에 영향을 미치는 비즈니스 프로세스와 시스템에 중요한 변화가 있는 경우나 개인정보의 관리와 접근통제에 사용되는 정보보호 메커니즘에 중대한 변화가 발생한 경우 • 다른 수준의 정부기관이나 민간기관으로의 프로그램이나 서비스를 이관하는 계약을 한 경우 • 공통 개인 식별자들의 신규 이용 개발 및 확장 개발의 경우 • 대중들의 부정적인 반응이 예상되는 경우
-----	-------	--

38 개인정보보호의 법적 쟁점과 과제

캐나다	기 존 사 업	<ul style="list-style-type: none"> 서비스가 근본적으로 재설계될 경우 서비스 전송 채널이 근본적으로 재설계된 경우 서비스가 개인정보의 수집, 이용, 제공에 영향을 끼칠 수 있는 방식으로 전자 전달수단으로 변경되었을 경우
호주	신 규	<ul style="list-style-type: none"> 생체적 또는 유전적 요소를 가지는 정보를 다루는 경우 규모, 복잡성 또는 범위 등에서 중요한 프로젝트 개인정보 취급을 아웃소싱하는 경우 개인정보 취급과 관련된 새로운 법령, 기술이 출현하는 경우 데이터베이스에 많은 양의 개인정보를 보유하는 경우 기관이나 부서의 상호작용, 예를 들어 기관간의 데이터 연결에 의한 공유 또는 업무 관할이 공공 또는 사적 부분과 상호 연결되는 경우 프로젝트가 상당한 대중적 영향을 가지는 경우(예를 들어, 각 개인에 대한 많은 양의 개인정보를 다루거나, 많은 사람들의 개인정보를 다루는 곳) 새롭게 임무가 추가된 기관이 새롭게 개인정보의 수집과 취급하는 경우
뉴질랜드	기 존 사 업 및 신 규	<ul style="list-style-type: none"> 뉴질랜드의 거의 모든 국민들의 개인정보를 가지고 있는 데이터 웨어하우스의 경우처럼 PIA의 필요성과 관련하여 눈에 띄는 규모와 특성을 가지고 있는 프로젝트 사람들에게 데이터 처리에 있어 그 효과가 그다지 널리 알려져 있지 못하거나 신뢰를 받지 못하고 있는 최신 기술이 적용된 애플리케이션 본질적으로 명백한 프라이버시 침해 위험을 가지고 있어 PIA 수행으로 인한 장점이 확실하게 예상되는 경우 접근 가능한 데이터베이스로 기밀정보가 수집되는 모든 프로젝트 새로운 형식의 고객 프로파일링이 가능하도록 내부 비즈니스 데이터베이스가 통합되는 경우 다국적 기업의 직원 기록이 집중화된 경우 정보가 수집되는 방식을 변경하는 경우 현존 기술들을 통합하거나 새로운 기술을 적용하는 경우 새로운 환경에서 이미 알려진 프라이버시 침해 기술이 사용되는 경우

한편, '기업 개인정보 영향평가 수행 가이드'에서는 평가 대상 사업 범위를 ① 개인정보를 다량 보유·관리하는 정보시스템의 신규 구축 사업, ② 신기술 또는 기존 기술의 통합으로 프라이버시 침해 가능성이 우려되는 기술을 사용하는 사업, ③ 개인정보를 보유·관리하는 기존 정보시스템을 변경하는 사업, ④ 개인정보의 수집·이용·보관·파기 등 일련의 단계에서 중대한 개인정보 침해 위험이 발생할 가능성이 있는 사업 등에 한정하였다. 또한 민간부문 정보보호 분야 중 의무화제도는 주요 정보통신 기반 시설 지정, 정보보호 안전 진단 제도 등이 존재하며 일정 자격기준 이상 대상을 지정·진단하고 있는바, 주요 정보통신 기반 시설 지정 및 취약성 분석의 경우 중앙행정기관이 정하는 소관 분야의 정보통신기반시설을 주요대상으로 하는 반면 정보보호 안전진단의 경우 ① ISP 등 인터넷 접속서비스제공자, ② IDC 등 집적정보통신시설사업자, ③ 전년도 정보통신서비스 부문 매출액 100억 이상 또는 1일 이용자수 100만명 이상 정보통신서비스 제공자 등을 주요대상으로 삼고 있다.

생각건대, 개인정보 수집·활용이 수반되는 모든 사업을 대상으로 평가를 추진하는 경우 행정력 낭비 및 원활한 소관 업무의 추진이 저해될 우려가 있으므로 대상을 제한할 필요는 존재하며 국내외 사례를 종합하면 통상적인 평가 대상은 ① 개인정보 파일을 신규 구축하는 경우와 ② 개인정보 파일을 연계하거나 수집·이용 등이 변경·확대되는 경우라 할 수 있다. 이에 따라 신규 구축 및 변경·확대를 기반으로 1안 제31조제2항에서 평가시 고려사항으로 규정한 개인정보의 수, 제3자 제공 여부, 정보주체의 권리를 해할 가능성 및 그 위험 정도 등을 염두에 두어 평가대상을 구체화해야 할 것이다. 다만, 지난 2008년 행정안전부가 개최한 주민등록번호 클린캠페인을 위해 약 30만명의 참가자 개인정보를 수집·처리한 바 있지만 캠페인 종료 후에는 이용 및 보유 목적이 없어 파기하는 것이 적

합한 것이므로 이에 대한 영향평가는 의무적일 필요는 없다고 볼 것이기에, 상시업무가 아닌 이벤트 등 한시적 업무를 위한 경우나 경미한 사업에 대해서는 예외사항을 별도로 규정할 필요로 존재한다.

그렇다면 개인정보 수집·활용시 개인정보 침해 위험성이 상대적으로 높은 경우로 ① 유출시 피해 범위 및 사회적 파급 효과가 높은 대량의 개인정보 DB 보유, ② 해당 기관의 보호 체계를 벗어나 개인정보 취급자 확대 및 제공 과정에서의 안전성 미조치로 인한 유출 위험이 가중되는 개인정보 제3자 제공, ③ 개인정보 수집경로 및 이용범위 등 업무처리 절차가 신규로 추가되거나 변경되는 과정에서 개인정보가 유·누출되거나 오·남용될 우려가 존재하는 개인정보 취급 절차 확대·변경, 그 유·누출 및 오·남용시 부당한 차별 또는 명예훼손 등 2차적 피해 위험이 높은 민감정보 수집 등을 주요대상으로 삼아야 할 것이다. 그러므로 개인정보 파일 규모, 제3자 제공 여부, 개인정보취급절차 확대·변경, 민감정보 수집 여부 등을 기반으로 하위법령을 통해 평가 대상 세분화하여 규정하는 것이 바람직한 방향이 될 것으로 본다. 다만, 예컨대 공공기관 공모전, 캠페인, 이벤트 등 1년 이내 한시적으로 구축·운용되는 개인정보파일로서 영향평가 수행으로 인해 업무 추진이 현저히 저해되는 경우는 상시업무를 위한 파일에 비해 상대적으로 침해 위험성이 낮으며 평가수행으로 인해 오히려 본래의 업무추진에 지장을 초래할 수 있으므로 예외로 할 필요가 있을 것이다. 물론 예컨대, 홈페이지 회원 대상 고객 만족도 조사시 통계 활용을 위해 성별·연령 등의 통계정보 및 응답내역 등 추가 정보를 수집하는 것과 같이 기존 개인정보파일의 처리 절차에 변경 없이 해당 정보만으로는 정보주체의 식별이 불가능한 정보를 추가적으로 수집하는 경우 추가적인 개인정보가 수집되므로 개인정보파일이 확대되는 것으로 볼 수 있으나 해당 정보만으로는 개인식별이 불가하므로 위험성이 크다고 보기

어렵다는 점에서 영향평가의 대상에서 제외하는 것이 타당하다. 또한 1안 제48조제1항에서 법 적용에서 제외하는 경우 역시 영향평가가 면제되는 것이 논리적으로 타당하다.

(2) 평가기준

‘기업 개인정보 영향평가 수행 가이드’에서는 정통방법을 기준으로 수집·이용·제공·파기 등 생애주기(Life-Cycle)에 따른 보호조치 및 기술적·관리적 보호 조치 사항 등의 항목 제시하고 있는바, 예컨대 수집단계의 경우 개인정보 최소 수집 여부, 민감정보 수집 여부, 필수·선택 구분 여부, 이용자 대상 고지 및 동의 획득 여부, 개인정보 제공 거부권 부여 여부, 개인정보 DB화 필요성 여부 등이 거론되고 있다.

한편, 미국의 경우 OMB 지침에서는 수집 대상정보, 수집 목적, 이용 범위, 정보의 공유 및 연계 대상자, 정보 이용에 대한 동의 및 거부권 행사 절차, 동의 방법, 기술적·관리적 보호 조치 등을 규정하고 있고, 캐나다의 경우 연방정부 PIA 가이드를 통해 개인정보의 수집, 적절성, 동의, 이용, 공개, 정확성, 보안, 참가, 자기정보통제권 등 개인정보보호 관련 10대 원칙별 세부 질문항목을 제시하고 있으며, 호주의 경우 프라이버시 커미셔너 사무국 PIA 가이드를 통해 수집목적의 적정성, 제3자 제공 등 접근 통제에 관한 사항, 연계 방안의 적절성 평가항목이 제시되고 있는 형편이다.

판단컨대, 개인정보 영향평가는 OECD 8원칙을 기반으로 하는 프라이버시 보호의 관점에서 해당 사업을 평가가 이루어져야 하며, 더욱이 최근 들어 IT compliance(준수감사평가) 중요성이 대두됨에 따라 필요한 보호

42 개인정보보호의 법적 쟁점과 과제

조치 사항의 적법성 여부에 대한 평가 또한 필요할 뿐 아니라, 법적 준거성의 확보를 위해 공공분야 개인정보보호 관련 법령을 기반으로 평가기준을 규정할 필요가 있다고 하겠다. 그렇다면 1안 제15조에서 제30조까지 및 제32조에서 제36조까지의 준수를 위한 조치사항이 평가기준에 반영되도록 하위법령의 정비가 이루어져야 할 것이다.

(3) 평가 방법 및 절차

캐나다, 호주, 뉴질랜드 등에서는 기관내 사업담당자, 법률자문단, 기술전문가 및 외부전문가를 활용하여 전담반을 구성하거나 외부기관에 의뢰토록 가이드를 통해 권고하고 있다. 특히, 캐나다의 경우 도출된 개선방안이 반영될 수 있도록 내부적으로 책임과 권한을 갖는 내부 위원회 혹은 작업반 형태의 관리 구조를 갖출 것을 권고하고 있지만, 미국의 경우 OMB 지침 등에 수행주체에 관한 별도 규정은 없다.

한편, 국내에서는 정보보호 관련 취약성 평가 및 진단을 수행하는 경우 다음과 같이 외부 전문기관에 의뢰토록 법률을 통해 규정하고 있다.

또한 공공기관 정보시스템 감리의 경우 정보시스템의 효율적 도입 및 운영 등에 관한 법률을 통해 감리 절차, 감리 수행 기관·감리원 자격 기준 등을 상세히 규정하고 있는바, 영향평가를 통해 일정 수준 이상의 평가 품질이 담보될 수 있도록 영향평가 대상, 절차, 수행 인력 등을 하위법령을 통해 규정하고 세부기준에 대해서는 개인정보 영향평가 지침을 마련하여 상세화하는 방안을 고려할 수 있겠다. 덧붙여 영향평가 대상 범위, 평가시 주요 고려사항 등 원칙적인 사항에 대해서만 하위법령을 통해 규정하고 구체적인 수행방법은 각급 기관이 자율적으로 수행할 수

[표 8] 국내 정보보호 관련 취약성 평가 및 진단 사례

구 분	취약성 분석·평가	정보보호관리 체계 인증(ISMS)	정보보호 안전진단
시행일	2001년	2004년	2004년
주요 대상	정보통신기반시설	ISP, IDC 등	주요 ISP, IDC, 쇼핑몰 등
심사 분야	기반시설에 대한 취약점 분석·평가	정보보호정책/ 관리체계/위험관리	기술적·관리적·물리적 시스템 보안
법적 근거	정보통신기반보호법 제9조	정통방법 제47조	정통방법 제45조 및 제46조의3
인증 기관	<ul style="list-style-type: none"> ○ 한국정보보호진흥원 ○ 정보공유·분석센터 ○ 정보보호 컨설팅 전문 업체 ○ 전자통신연구원 	정보보호 관리체계 인증기관 ※ KISA 지정	안전진단 수행기관

있도록 유도하는 방향도 염두에 둘 수 있을 것인바, 전자(前者)이 경우 체계적이고 안정적인 평가 수행이 가능하며 최소한의 평가 품질이 담보되나 평가 대상 규모 등 특성에 맞는 탄력적 수행이 어려워 공공기관의 역량이 미비한 경우 제도 정착에 상당 기간이 소요되고 수행 업체 및 인력 관리 등에 따른 행정력 낭비가 우려되는 반면 후자(後者)의 경우 사업 특성에 맞는 탄력적 평가 수행이 가능하여 원활한 제도 정착이 기대되지만 최소한의 평가 품질이 저해될 우려 역시 병존하고 있으므로 조율이 필요하다. 그럼에도 불구하고 영향평가의 수행에 있어 평가 대상 사업의 규모, 해당 기관의 인력 역량, 예산 확보 여부 등 사업별 특성은 매우 다양하고 영향평가의 본질상 표준화된 세부 절차가 있는 것이 아니라 사업 특성에 맞는 탄력 운영이 필요하므로 평가 절차를 일괄적으로 법률

44 개인정보보호의 법적 쟁점과 과제

로써 규정함은 공공기관의 대규모 위법행위를 초래하거나 원활한 평가수행을 저해할 수 있음이 고려되어야만 할 것이다.

그리고 외부 전문업체 지정기준과 관련하여서는 외부 전문기관 자격기준을 법률을 통해 지정하고 있으며 보유 인력 및 정보보호 컨설팅 실적 등의 기준에 따라 관련 서류 제출, 현장 실사, 심의회 구성·운영 등의 절차를 거쳐 심사 후 인증서 교부토록 규정하고 있는 정보보호 관리체계 인증 등의 경우를 참조할 필요가 있다.

<표 9> 국내 정보보호 관련 근거와 기준

구분	정보보호컨설팅 전문업체	정보보호관리 체계 인증(ISMS) 기관	안전진단 수행 기관
근거 규정	정보통신기반보호법 제17조	정통방법 제47조 및 방통위 고시 제2008-11호	정통방법 제46조의3 제1항 및 시행령 제39조제2항, 제44조
지정 및 심사 기준	<ul style="list-style-type: none"> ○ 일반기술인력 10명 이상 및 고급 기술인력 5명 이상 ○ 납입자본금 20억원 이상 ○ 설비보유 여부 <ul style="list-style-type: none"> - 신원확인 및 출입통제 설비 등 	<ul style="list-style-type: none"> ○ 인증심사업무 전담 직원 10인 이상 보유할 것 ○ 방송통신위원회가 실시하는 업무수행 능력심사에서 적합하다고 인정받을 것 - 심사기준 : 3년간 정보보호 수행 실적 등 	<ul style="list-style-type: none"> ○ 15인 이상의 정보보호기술인력 ○ 최근 3년 이내 정보보호컨설팅 수행 실적이 있는 법인

생각건대, 정보보호 관련 인증·평가 기관이 다수 지정되어 있으므로 중복 제도의 운영 최소화 및 행정효율성 등을 고려하여 기존 평가기관을 활용하되, 개인정보 영향평가는 정보시스템 및 네트워크의 기술적 보호 뿐만 아니라 개인정보 오남용 방지 등 인적·관행적·법제도적 침해요소에 대한 접근방법 또한 요구되므로 기존 평가기관 대상 개인정보보호 소양 함양을 위한 추가적 자격 기준은 추후 별도 고시를 통해 규정함이 바람직할 것으로 여겨진다.

제3장 개인정보보호기구의 쟁점과 과제

제1절 논의의 배경

지난 2003년 대통령 주재로 열린 국정과제회의에서 정부혁신지방분권 위원회가 마련한 전자정부관련법제정비방안에는 “2004년까지 시민단체 등의 의견을 수렴하여 개인정보보호 기본원칙을 천명하고 개인정보영향 평가제를 도입하며 개인정보보호기구를 설치하는 것 등을 내용으로 하는 개인정보보호기본법의 제정에 대하여 검토하겠다”는 내용이 담겨 있다.⁴⁰⁾ 이 같은 사항은 초기의 선행연구 결과를 바탕으로 하는 것이기도 하지만 사회각계의 여론이 집합되는 논의과정에서 정책방안이 집결됨으로써 중국적으로 국정과제로 채택되기에 이른 것으로 여겨진다. 교육행정정보시스템(NEIS)의 도입에 있어 제기된 문제점 및 그에 따른 대응방안이 제시될 때에도 결국 총괄적으로 개인정보보호정책을 집행할 행정기구의 설치가 관건이 될 수밖에 없었던 예에서도 볼 수 있듯이, 보호가치 있는 정보주체의 권익보장을 제도화하는 데 중추적인 역할을 담당할 존재에 대한 갈망은 사회전반적인 인식의 근저에 녹아들어 있었다.

특히 이에 대하여는 시민사회단체의 노력이 간과되어서는 아니 될 중요한 견인차로 작용해왔음을 지적하지 않을 수 없다. 예컨대 지난 2004년 7월 프라이버시법제정을위한연석회의를 주축으로 하는 시민사회단체가 17대 국회가 주목하여야 할 ‘정보인권 보장을 위한 35대 과제’를 발표한

40) 다만 2003년에는 공공기관법과 정통방법을 개정하여, 정보자기결정권 및 심의 절차를 강화하고 적용범위를 확대할 것이라는 점이 적시되어 있다; 대통령비서실, 청와대 브리핑 제148호, 2003년 10월 2일자, 2~4쪽.

바 있다. 여기서 공공과 민간 그리고 온라인과 오프라인에 예외 없이 적용될 수 있는 국제적 수준의 개인정보보호기본법을 제정하고, 이에 따른 조치를 실질적으로 집행하기 위해 상시적인 사전 감독활동과 신속한 분쟁조정 활동을 일상적으로 수행할 수 있는 독립적인 개인정보보호위원회를 설치해야 한다는 주장이 재차 강조되었다. 그리고 이들은 개인정보보호위원회가 국가인권위원회의 위상에 준하는 독립적인 국가기구의 지위를 가져야 하고, 공공기관과 민간영역을 가리지 않고 사회 전체를 자신의 감독 및 분쟁조정 대상으로 삼아야 하며, 각종 법률제정에 있어 프라이버시보호에 관련된 권고권을 가져야 한다고 주장했다. 이어서 10월에는 프라이버시법제정을위한연석회의가 “개인정보보호위원회는 개인정보 현황에 대한 실태조사, 개인정보침해의 구제, 분쟁의 해결, 개인정보보호 관련 법령의 입안, 개인정보보호 교육 및 홍보, 개인정보를 침해할 수 있는 사업에 대한 사전영향평가 등의 업무를 담당함으로써 사회적 안전망의 역할을 해야 할 것이다. 개인정보보호위원회는 민간영역과 공공영역 모두를 포괄해야하며, 정부의 개인정보 수집 역시 감독해야 하기 때문에 정부로부터의 일정한 독립성이 보장되어야 한다.…”(中略)…신뢰성 있는 정보사회를 구축하기 위해서는 개인정보보호를 위한 사회적 시스템의 마련은 더 이상 늦출 수 없는 과제이다. 이번 정기국회에서 개인정보보호기본법 제정과 민간·공공 영역을 포괄하는 독립적인 개인정보보호위원회 설립이 반드시 통과되기를 촉구한다!”는 내용의 논평⁴¹⁾을 발표하여 기존의 입장을 재확인한 바 있다.⁴²⁾ 하지만 개인정보보호기구 설립의 정당성이 그

41) <http://networker.jinbo.net/maybbs/view.php?db=ektjtqud&code=policy&n=1085>

42) 문제는 그 당위론적 필연성을 검토하는 데 철저한 검증이 있었는지를 따져볼 필요가 있다. 다시 말해 개인정보보호를 위한 규제정책의 일원화에 대하여 정책방안을 수립하기 이전에는 그 목적 및 근거를 명확히 한 연후에 그에 따른 사회적 파장을 고려하여 타당성 있는 제안이 실효성을 발휘할 수 있는 논리적 기초를 제공해야 할 것인바, 이에 대하여 그동안 얼마나 실증적인 검토가 수반되었는지는 의구심이 전혀 없는 것이 아닐 뿐만 아니라 마땅히 행정통제와 행

설치방안의 타당성과 무관하지 않으며 이는 개인정보보호에 관한 정책 및 제도에 관한 사항이라는 점에서 입법논리적 검토와 함께 입법정책적 고려가 선행되어야 한다.

주지하는 바와 같이 사생활의 비밀과 자유의 불가침은 사생활의 내용을 공개당하지 않을 권리, 자신에 관한 정보를 스스로 관리·통제할 수 있는 권리 등을 내용으로 하는 인격권으로서 오늘날 정보사회가 급속히 진행되면서 그 보호가 절실한 권리이다.⁴³⁾ 참여로서의 개인정보에 대한 자기 결정과 통제권은 은둔으로서 사생활의 비밀과 자유의 권리와는 다른 측면이 있는 것이지만, 헌법에서 보장하는 기본권으로 인식되고 있기 때문이다.⁴⁴⁾ 명문으로 정해지지 않아 논란은 있지만, 일반적으로는 헌법 제17조에 의해 개인정보의 보호가 헌법적으로 인정된다고 한다. 그리고 여기서 자신에 관한 정보를 관리하고 통제할 수 있는 권리, 즉 자기 정보에 대한 정보주체의 자율적 결정권이 도출된다고 보고, 학자들은 이를 ‘자기정보통제권’, ‘개인정보자기결정권’ 등의 이름으로 부르고 있다. 이러한 용어의 연원은 일정한 범위 내에서 자기 자신에 관한 정보를 제공할 것인가를 자유로이 결정할 권한은 인간의 존중과 인격의 자유로운 전개에 해당하여 법적 보호를 필요로 하는 것으로 파악하여 독일 연방헌법재판소가 1984년에 결정한 인구조사판결(BVerfGE 65, 1)에서 인정한 ‘Recht auf informationelle Selbstbestimmung’에서 비롯된 것이다. 그리고 이는 미국에서 논의되는, 자신에 대한 정보가 언제·어떻게·어느 범위까지 타인에게 전달되고 이용될 수 있는지를 그 정보주체가 자율적으로

정규제를 포괄하여 개인정보보호기구의 소관업무가 갖춰져야 할 것인데 민간·공공 영역을 포괄하는 독립적인 기구의 설립을 촉구함에는 심리미진이 있다고 보이므로 이에 대해 전면적인 재검토를 시도해볼 필요성이 있다고 생각한다.

43) 서울고등법원 1995. 8.24 선고 94구39262 판결 [공 1998. 9. 1, (65), 2200] 참조.

44) 권영성, 헌법학원론, 법문사, 2005, 449쪽 이하 참조.

결정할 수 있는 개인정보보호의 적극적인 요소인 ‘information privacy’와 동일한 개념이라 하겠다. 결국 헌법이론상 미국과 독일에서는 기본권으로서 프라이버시 및 일반적 인격권으로부터 도출되어지는 정보자기결정권이라는 개념은 우리의 경우 헌법 제17조에서 규정하고 있는 사생활의 비밀과 자유에서 근원을 찾을 수 있으며,⁴⁵⁾ 이는 프라이버시⁴⁶⁾라는 용어로 준용되어 일반적으로 표현되고 있다.⁴⁷⁾ 프라이버시란 우리들에 관한 정보의 부재(不在)만을 의미하는 것이 아니라, 오히려 우리 자신에 관한 정보를 우리 스스로가 통제(統制)하는 것을 의미한다.⁴⁸⁾ 따라서 프라이버시는 이념적 가치이자 실천적 권리인 반면 개인정보는 프라이버시의 대상으로서 그 보호객체라는 점에서, 양자는 유기적인 관련성을 지니고 있다. 더욱이 인터넷활용의 증대로 인하여 개인에 관한 정보의 수집과 유출이 용이해지고 있으며 이로 인해 야기되는 개인정보에 관한 권리침해는 정보주체에게 정신적·물질적 손해를 야기할 뿐만 아니라 개인의 인격형성을 저해하고 인간의 존엄성을 파괴할 수 있으므로, 개인정보의 보호는 프라이버시 보장 차원에서 밀도 있게 구성되어져야 한다. 그럼에도

45) 학자들은 헌법 제10조에 관해 거론하는데, 기본적 인권으로서 인간의 존엄과 가치가 배제되는 것은 없다.

46) 프라이버시의 어원(語源)은 ‘사람의 눈을 피한다’는 의미의 라틴어인 *privatue*에서 유래한다. 그 사전적 의미는 “사생활에 대하여 타인의 눈길로부터 떨어져 있는 상태, 은거하는 장소, 타인으로부터 독립하여 사적 비밀(私的 秘密)이 보장된 분위기, 타인에게 알려지기를 꺼리는 사사(私事), 사적인 친척관계나 친밀한 관계와 같이 은밀한 관계 등을 뜻한다”고 기술되기도 하고(Merriam Webster, *Webster's new international dictionary of the English language unabridged*, Encyclopaedia Britannica, 1966, p.1804.), ‘사회·타인의 호기심 그리고 영향력으로부터 독립된 것으로서 규범적 요소를 포함한 개인적인 영역에 대한 접근의 배타적 통제력’으로 풀이할 수 있다(David L. Sills, *International Encyclopedia of the Social Science*, Vol.12, the MacMillan Press, 1976, p.480).

47) 넓은 의미에서는 권리로서 프라이버시의 개념 범주가 기본권으로서 사생활의 비밀과 자유를 포함하는 의미를 지닌다고 할 수 있지만, 분명 양자(兩者)는 중첩되는 영역을 지니고 있으므로 여기서도 이를 혼용하기로 한다.

48) Charles Fried, *Privacy*, 77 Yale L. J. 475, 482 (1968).

불구하고 나날이 발전하는 정보통신기술(ICT)은 법제현실을 뛰어넘어 전자적 감시의 역기능을 보유하고 있는 것이다.

그런데 자신의 개인정보에 대한 권리에 대하여 제대로 인식하지 못하면 소중한 정보가 유출되거나 하여 권리침해가 발생하였음을 깨닫지 못하기 때문에, 적절한 대응과 충분한 구제에 어려움이 있다. 이 권리가 해당 개인정보에 대하여 열람·정정·사용중지·삭제 등을 청구할 수 있는 능동적·적극적 권익으로 구성되는 까닭에 더욱 그러하다. 무엇보다 이는 보호법익으로서 개인정보를 보호가치의 영역 내로 끌어들이는 데 가장 기초적인 출발점이 될 수 있으며, 개인정보에 관한 권리가 구체적으로 실현되는지의 여부가 개인정보보호법제도 분석에 있어 하나의 중요한 기준으로 활용될 수 있기에 소홀히 다룰 수 없는 것이다. 따라서 개인의 정보자기결정권이 실현될 수 있도록 제도화된 개인정보보호정책을 수립하고 이를 집행하는 상설기구의 마련을 통해 권리침해를 사전적으로 예방하며 사후적으로 구제하는 일련의 과정이 형성되어야 하며, 이러한 점에서 개인정보보호기구의 설립은 그 정당성을 확보할 수 있다.⁴⁹⁾ 특히 시

49) 물론 지금까지 전통적인 기본권보호제도에서는 국가의 공권력작용으로 인하여 국민의 권리가 침해된 경우에 재산상 손해를 전보해 주거나 당해 행정작용을 취소, 변경해 주는 사후적 구제제도가 핵심이었다. 그러나 원자력발전소나 무수히 많은 사람들이 동시에 개인의 사적인 정보를 저장, 전달할 수 있는 정보처리기술이 등장하는 정보사회에서 이러한 전통적인 사후구제제도로는 개인의 권리를 충분히 보호할 수 없다. 오히려 정보사회에서는 국가의 공권력작용으로 인하여 국민의 권리침해가 발생하기 이전에 그러한 국가작용이 ‘기본권제한’에 해당하는지를 검토하고, 그렇다면 그러한 제한의 정당성 여부를 판단하는 작업이 필요한 것이다. 그리고 바로 이를 통하여 처음부터 위법하거나 부당한 공권력작용이 행하여지지 아니하도록 예방하는 사전절차적 제도를 통한 권리보호가 오늘날 훨씬 더 효율적임을 알 수 있다. 따라서 아직까지는 사전적 보호제도가 사후적 구제제도를 보충하는 역할을 맡고 있으나, 앞으로는 그 중요성이 사후적 구제제도에 준할 만큼 중요한 몫을 차지할 것이다. 오늘날 정보기술은 단시간에 전 세계적으로 엄청난 속도의 과급효과를 초래하는바, 이에 대한 사전적 절차통제가 이루어지지 않은 상황에서 이러한 기술들이 시행되고 작동된 후에 국가기관을 통한 사후통제나 몇몇 개인의 사후적 권리구제를 통하여 이

시각각 변모하는 기술동향에 대처하면서 개인정보에 관한 권리를 부당하게 제한하고 자기정보에 대한 통제를 무력화하는 감시기술에 역감시가 가능하도록 법제방안을 실현하는 기능을 담당할 개인정보보호기구의 창설은 시대적 요청이라 하겠다. 물론 여기에는 전자감시사회에 대한 자성적 호소가 짙게 배어있다.

그동안 개인정보보호기능이 분산되어 있는 것은 개인정보보호에 관하여 체계성 없이 개별법이 산재된 데 그 연유가 있다. 따라서 각 부문별로 일반법이 미완성된 채 보호의 집중·통합과는 거리를 두고 적용·집행되고 있을 뿐만 아니라, 이에 따라 개인정보보호정책을 주관하여 추진할 행정주체가 존재하지 않게 된 것이다. 이러한 미온적 보호체계로는 정보주체의 정보자기결정권을 확립하면서 전자정부시대에 걸맞은 개인정보보호수준의 수립이 어려울 것으로 전망되며, 전자정부의 집행기관인 행정자치부와 정보통신부가 상반된 가치인 개인정보보호기능을 수행하기는 사실상 어려울 것이라는 추측은 정책적 고려를 수반하는 부분이다. 더욱이 현행 법상 개인정보보호사무를 관장하는 기관으로 해석되는 개인정보보호심의위원회 및 개인정보분쟁조정위원회가 각기 부문별로 권리침해에 대한 사전예방 및 사후구제에 이르는 일련의 정책과정을 결정하고 추진할 만한 권한과 위상을 보유하지 못하고 있다는 점에서, 정보주체의 권리보장 기능을 전담할 독립적인 개인정보보호기구의 발족이 요청된다. 현행 개인정보보호기능만으로는 충실한 개인정보 권리침해의 예방 및 구제에 미비하므로 특단의 조치가 이루어져야 할 것이 때문이다.

에 효과적으로 대응한다는 것은 처음부터 불가능하다는 것이 바로 정보사회의 가장 핵심적인 특징이기 때문이다; 김일환, 개인정보보호감독기구의 설치에 관한 연구, 전자정부법제연구 창간호, 행정자치부, 2006, 156쪽.

제2절 입법적 현황

1. 주요국가의 동향

(1) 영 국

프라이버시 보호문제에 관한 국제적 관심이 증대되면서 OECD 이사회가 1980년 9월 23일 ‘프라이버시보호와 개인정보의 국제유통에 관한 가이드라인(Guidelines on the Protection of Privacy and Transborder Flows of Personal Information)’⁵⁰⁾을 채택하였고 다음해인 1981년 2월 28일 EU 평의회가 ‘개인정보의 자동처리에 관한 개인의 보호를 위한 유럽협약(Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)’에 서명하기에 이르자 이들 국제기구의 회원국인 영국으로서는 결국 1984년 정보보호법(Data Protection Act of 1984)의 제정이 불가피했었다.

영국의 정보보호법(Data Protection Act of 1998)은 공·사 부문을 구별하지 않고 개인정보보호에 관하여 규율하고 있으나, 동법에 대한 특별시행세칙으로 The Telecommunications Data Protection and Privacy Regulations of 1998(Direct Marketing Regulations; S.I. 1998 No.3170)이 있다. 1998년 법 개정에서 가장 흥미로운 점은 등록제에서 신고제로 바뀌었다는 점인데, 개인정보의 자동처리를 등록하는 제도는 당시 파탄지경에

50) 그 주요목적은 ① 공적·사적 영역에서 개인정보를 보호하고, ② 정보의 자유로운 흐름을 촉진하며, ③ 정보의 자유로운 흐름에 대한 개별 국가의 사생활 보호법률에 의한 억제를 제한하면서 ④ 여러 국가들의 관련 법규정을 조화시키는 데 있다; Raymond Wacks, *Personal Information*, Gloucestershire: Clarendon Press, 1989, p.205.

있어 완전히 폐기할 예정이었으나 EU지침(Directive 95/46/EC)에 따라 신고제를 채택하지 않을 수 없었던 것이다.⁵¹⁾

정보보호법은 개인과 관련된 정보인 데이터의 취득·유지·사용·공개 등의 활동을 포함한 새로운 처리 규범의 수립을 위하여 공공과 민간에 포괄하여 적용되는 영국의 개인정보보호에 관한 기본법이다. 따라서 이 법에는 개인정보보호 기본원칙을 비롯하여 정보주체의 권리와 정보처리자의 의무, 개인정보보호기구의 설립 및 운영, 정보법원(Information Tribunal)의 설치, 개인정보의 국외이전 등에 관한 사항을 포괄적으로 규정하고 있다. 또한 정보보호법은 주로 전자적인 형태로 처리되는 개인정보를 규율할 목적으로 제정된 것이나 그 후 적용범위가 더욱 확대되어 특정한 구조화된 수기파일링시스템(manual filing systems)은 물론, 의료기록이나 교육기록에 대해서는 순수하게 수기로 처리되는 개인정보까지도 동법의 규율대상으로 포함시키고 있는 한편, 생존하고 있는 개인에 관한 정보를 보호대상으로 함을 명시적으로 밝히고 있어 법인정보나 사자(死者)의 정보는 제외된다.⁵²⁾

정보보호법은 제1조에서 필요한 목적에 따라 자동으로 작동하는 장비

51) 1995년 10월 24일 제정된 EU지침은 EU가맹국으로 하여금 3년의 전환기간을 주어 EU지침에 따른 개인정보보호법을 정비하도록 하였으며(*EU directives are addressed to the member states, and aren't legally binding for citizens in principle. The member states must transpose the directive into internal law. Directive 95/46/EC on the protection of personal data had to be transposed by the end of 1998. All member states have enacted their own data protection legislation.*), 이에 이 전환기간을 지킨 나라는 이탈리아·그리스 및 영국, 스웨덴, 포르투갈 등이었다. 영국은 EU를 이끌어 가는 영국·독일·프랑스의 3국 중 유일하게 전환기내에 국내법을 제정한 나라이며, 또 영국의 정보보호법은 EU지침의 거의 모든 요구사항을 수용하고 있는 것이 특색이다.

52) Data Protection Act 1998 §5 (Application of Act) (3) (a) an individual who is ordinarily resident in the United Kingdom

에 의해 처리되는 정보, 이러한 장비로 처리하려는 목적으로 기록되는 정보, 관련 파일시스템의 일부로 기록되거나 이를 형성하려는 목적으로 기록되는 정보 그리고 이들 정보에 속하지는 않지만 제68조에서 정의된 접근가능기록의 일부가 되는 정보를 말한다고 하고 있다. 따라서 개정되기 전의 1984년 법이 자동처리형식으로 수집된 개인데이터만을 대상으로 하고 있었던데 비해, 새로운 정보보호법에서는 원칙적으로 수작업에 의한 정보까지도 적용대상으로 하고 있다. 한편 정보보호법 제2조에서는 민감한 개인데이터로 ① 데이터주체의 민족·인종적 출신사항, ② 정치적 견해, ③ 종교적 신앙이나 이와 유사한 성격의 믿음, ④ 노동조합의 가입여부, ⑤ 정신적·육체적 건강상태, ⑥ 성생활, ⑦ 법률위반사실 또는 추정된 위반, ⑧ ⑦에 대한 소송제기 여부 및 해당 소송의 재판결과로서의 판결 등에 관한 정보를 구성하는 개인데이터를 열거하고 있다.⁵³⁾

한편, 정보보호법 제5조에 따르면 제54조에 의해서 또는 그에 따라 달리 명시되지 않는 경우 동법은 데이터관리자가 영국에서 설립되고 데이터가 설립된 내용에 의해 처리된 경우나 영국 혹은 그 외의 유럽경제지역(EEA) 국가에서 설립되지 않은 데이터관리자지만 영국을 통해 전송하

53) Data Protection Act 1998 §2 (Sensitive personal data) In this Act "sensitive personal data" means personal data consisting of information as to-

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions,
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

는 목적 이외에 데이터를 달리 처리하기 위하여 영국에서 장비를 사용하는 경우의 모든 데이터에 대해 데이터관리자에게 적용된다. 따라서 그 적용범위에 있어 공공과 민간의 구별이 없다.⁵⁴⁾

정보보호법은 제14조에서 부정확한 정보주체의 개인정보에 대한 수정·삭제·파기를 명할 수 있는 권한을 부여하고 있으며,⁵⁵⁾ 개인은 언제라도 서면 통보에 의하여 데이터관리자에게 자신에게 중대한 영향을 미치는 결정도 데이터관리자나 그의 명령에 따라 개인데이터를 자동화기계로 처리하지 않았다는 것을 확인할 수 있는 권리가 있다고 정보보호법 제12조는 규정하고 있다.⁵⁶⁾

이러한 법규범 하에서 영국은 독임제 구조를 가진 독립된 법정기구인 정보보호감독관(Data Protection Commissioner)을 개인정보보호기구로

54) Data Protection Act 1998 §5 (Application of Act) (1) Except as otherwise provided by or under section 54, this Act applies to a data controller in respect of any data only if-

(a) the data controller is established in the United Kingdom and the data are processed in the context of that establishment, or

(b) the data controller is established neither in the United Kingdom nor in any other EEA State but uses equipment in the United Kingdom for processing the data otherwise than for the purposes of transit through the United Kingdom.

55) See Data Protection Act 1998 §14 (Rectification, blocking, erasure and destruction)

56) Data Protection Act 1998 §12 (Rights in relation to automated decision-taking) (1) An individual is entitled at any time, by notice in writing to any data controller, to require the data controller to ensure that no decision taken by or on behalf of the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data in respect of which that individual is the data subject for the purpose of evaluating matters relating to him such as, for example, his performance at work, his creditworthiness, his reliability or his conduct.

두고 있다. 정보보호감독관은 여왕이 임명하며,⁵⁷⁾ 그 임기는 5년으로 두 차례에 걸쳐 재임이 가능하다. 영국의 정보보호감독관은 행정부의 지시나 감독을 받지 않고 독자적으로 운영되는 행정청이므로 독립성과 자율성이 보장된다. 정보보호감독관은 공공등록부(public register)에서 정보처리와 관련된 소정의 내용을 고지 받아 기록하며 공공등록부를 유지·관리하는 기능을 담당한다.⁵⁸⁾ 또한 각종 개인정보침해사건이나 사업자 또는 공공기관 등의 개인정보처리행위에 대한 불만사항을 접수받아 사건을 조사·심사하여 당사자간 분쟁을 해결하고 피해자를 구제해주는 기능을 담당하는데,⁵⁹⁾ 침해사건의 접수 여부와는 관계없이 사회적으로 문제가 되

57) Data Protection Act 1998 (The Commissioner and the Tribunal) §6 (2) The Commissioner shall be appointed by Her Majesty by Letters Patent.

58) Data Protection Act 1998 §18 (Notification by data controllers) (1) Any data controller who wishes to be included in the register maintained under section 19 shall give a notification to the Commissioner under this section.

Data Protection Act 1998 §19 (Register of notifications) (1) The Commissioner shall –

(a) maintain a register of persons who have given notification under section 18, and

(b) make an entry in the register in pursuance of each notification received by him under that section from a person in respect of whom no entry as data controller was for the time being included in the register.

59) Data Protection Act 1998 §53 (Assistance by Commissioner in cases involving processing for the special purposes) (1) An individual who is an actual or prospective party to any proceedings under section 7(9), 10(4), 12(8) or 14 or by virtue of section 13 which relate to personal data processed for the special purposes may apply to the Commissioner for assistance in relation to those proceedings.

(2) The Commissioner shall, as soon as reasonably practicable after receiving an application under subsection (1), consider it and decide whether and to what extent to grant it, but he shall not grant the application unless, in his opinion, the case involves a matter of substantial public importance.

(3) If the Commissioner decides to provide assistance, he shall, as soon as reasonably practicable after making the decision, notify the applicant, stating the extent of the assistance to be provided.

(4) If the Commissioner decides not to provide assistance, he shall, as soon as reasonably practicable after making the decision, notify the applicant of

고 있어 자체 조사의 필요성이 있을 때에는 직권으로 개인정보보호 실태 조사를 실시할 수도 있다.⁶⁰⁾ 그밖에도 개인정보에 관한 각종 지침이나 규칙 제정,⁶¹⁾ 법률 및 기술자문, 사업자·소비자를 대상으로 한 정보제공, 교육·홍보, 개인정보보호를 위한 조사연구, 유관기관 협력, 법률위반행위에 대한 소송의 제기에 관여⁶²⁾ 등의 기능을 수행하고 있다.

정보보호법은 특히 정보보호감독관에 의한 예비평가에 대하여 규정하고 있는바,⁶³⁾ 여기서 평가대상이 되는 처리과정이라 함은 정보주체에게

his decision and, if he thinks fit, the reasons for it.

60) Data Protection Act 1998 §51 (General duties of Commissioner) (7) The Commissioner may, with the consent of the data controller, assess any processing of personal data for the following of good practice and shall inform the data controller of the results of the assessment.

61) 정보보호감독관은 민간과 공공부문의 모든 개인정보처리를 관할 대상으로 삼고 있으며, 의료정보, 신용정보, 교육정보, 정보통신분야에서 취급되는 개인정보, 근로자정보 및 폐쇄회로텔레비전(CCTV)와 프라이버시 문제, D.M.(Direct Marketing; 다이렉트마케팅) 문제 등에 대해서도 각종 규칙이나 지침 등의 법규를 통해 규율하고 있다;拙著, 개인정보법제론, 진한M&B, 2007, 76~77쪽.

62) Data Protection Act 1998 §60 (Prosecutions and Penalties) (1) No proceedings for an offence under this Act shall be instituted—

(a) in England or Wales, except by the Commissioner or by or with the consent of the Director of Public Prosecutions;

(b) in Northern Ireland, except by the Commissioner or by or with the consent of the Director of Public Prosecutions for Northern Ireland.

63) Data Protection Act 1998 §22 (Preliminary Assessment by Commissioner)

(1) In this section “assessable processing” means processing which is of a description specified in an order made by the Secretary of State as appearing to him to be particularly likely—

(a) to cause substantial damage or substantial distress to data subjects, or

(b) otherwise significantly to prejudice the rights and freedoms of data subjects.

(2) On receiving notification from any data controller under section 18 or under notification regulations made by virtue of section 20 the Commissioner shall consider—

(a) whether any of the processing to which the notification relates is assessable processing, and

(b) if so, whether the assessable processing is likely to comply with the

실질적인 피해나 고통을 야기하거나 그렇지 않더라도 정보주체의 자유와 권리를 중대하게 침해하는 것으로 국무장관이 판단하는 순서에 따라 특정한 처리과정을 말한다. 그리고 정보관리자로부터 혹은 통지의무규정에 의해 고지를 받은 즉시 정보보호감독관은 해당 고지와 관련된 처리과정이 평가대상인지 여부를 판단해야 하며, 평가대상이라면 평가대상 처리과정이 정보보호법에 부합하는지 여부를 검토해야 할 것이다. 또한 정보보호감독관은 통보를 접수한 날로부터 28일 이내에 정보관리자에게 해당처리과정이 정보보호법에 부합하는지 여부에 관한 정보보호감독관의 견해를 알려주어야 하며, 위 기간의 종료 이전에 정보보호감독관은 14일을 경과하지 않는 범위 내에서 1회에 한하여 통보로써 그 기간을 연장할

provisions of this Act.

- (3) Subject to subsection (4), the Commissioner shall, within the period of twenty-eight days beginning with the day on which he receives a notification which relates to assessable processing, give a notice to the data controller stating the extent to which the Commissioner is of the opinion that the processing is likely or unlikely to comply with the provisions of this Act.
- (4) Before the end of the period referred to in subsection (3) the Commissioner may, by reason of special circumstances, extend that period on one occasion only by notice to the data controller by such further period not exceeding fourteen days as the Commissioner may specify in the notice.
- (5) No assessable processing in respect of which a notification has been given to the Commissioner as mentioned in subsection (2) shall be carried on unless either—
 - (a) the period of twenty-eight days beginning with the day on which the notification is received by the Commissioner (or, in a case falling within subsection (4), that period as extended under that subsection) has elapsed, or
 - (b) before the end of that period (or that period as so extended) the data controller has received a notice from the Commissioner under subsection (3) in respect of the processing.
- (6) Where subsection (5) is contravened, the data controller is guilty of an offence.
- (7) The Secretary of State may by order amend subsections (3), (4) and (5) by substituting for the number of days for the time being specified there a different number specified in the order.

수 있다. 평가대상 처리과정은 정보보호감독관이 고지를 수신한 날로부터 28일이 지나야만 수행될 수 있으며, 이를 위반한 정보관리자는 처벌을 면치 못한다.

정보보호감독관은 민간과 공공부문의 모든 개인정보처리를 관할 대상으로 삼고 있으며, 의료정보, 신용정보, 교육정보, 정보통신분야에서 취급되는 개인정보, 근로자정보 및 폐쇄회로텔레비전(CCTV)와 프라이버시 문제, 다이렉트마케팅(direct marketing; D.M) 문제 등에 대해서도 각종 규칙이나 지침 등의 법규를 통해 규율하고 있었다. 하지만 종래의 정보보호감독관은 2000년 정보자유법(Freedom of Information Act)에 의하여 정보감독관(Information Commissioner)으로 대체되었다.⁶⁴⁾ 이에 따라 정보감독관은 1998년 정보보호법과 2000년 정보자유법을 집행하고 감독하며, 영국 의회에 직접 보고하는 독립된 감독관청으로서 임무를 수행한다.⁶⁵⁾

(2) 프랑스

1978년 제정된 프랑스의 「정보처리·축적 및 자유에 관한 법률(이하 여기서 ‘개인정보법’이라 함)」⁶⁶⁾은 이후 개인정보보호를 위한 국제규범들이

64) Freedom of Information Act 2000 §18 (The Information Commissioner and the Information Tribunal) (1) The Data Protection Commissioner shall be known instead as the Information Commissioner.

Freedom of Information Act 2000 Schedule 2. [The Commissioner and the Tribunal] Part I. [Provision consequential on s. 18(1) and (2)] (1) Any reference in any enactment, instrument or document to the Data Protection Commissioner or the Data Protection Registrar shall be construed, in relation to any time after the commencement of section 18(1), as a reference to the Information Commissioner.

65) http://www.ico.gov.uk/about_us/who_we_are/history_of_ico_page.aspx

66) Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et

공공부문과 민간부문을 구분하지 않고 모두 그 보호대상으로 규정하는 등 차츰 개인정보보호에 관한 법적 규율영역을 확대하는 것이 일반화됨에 따라 지난 2006년 1월의 것을 포함하여 아홉 차례 개정된 바 있다. 프랑스에서는 공·사 구분 없이 개인정보법이 통합법으로서 기본법이 되며, 이 원칙에 대한 특별법으로서 개별법이 존재한다.⁶⁷⁾ 개인정보법은 정보처리하는 국민 각자에게 도움이 되어야 하고, 그 개발은 국제협력의 범위 내에서 행해져야 하며, 정보처리에 의하여 신분·인권·사생활 및 개인적 또는 공적 자유가 침해되어서는 아니 된다는 점⁶⁸⁾을 그 입법취지로 하고 있다.

개인정보법에서 개인정보는 형식 여하에 관계없이 직접 또는 간접적으로 자연인의 신원을 확인할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보를 말하며,⁶⁹⁾ 사람의 혈통, 정치적·철학적 또는 종교적 견해, 조합의 소속이나 품행을 직·간접적으로 노출시키는 기명정보는 당사

aux libertés

67) Loi n° 78-17 §2 La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, lorsque leur responsable remplit les conditions prévues à l'article 5.

68) Loi n° 78-17 §1 L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

69) Loi n° 78-17 §2 Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

자의 명백한 동의 없이 정보시스템에 입력될 수 없다.⁷⁰⁾

개인정보법상 정보주체는 ① 자신에 관한 정보수집에 의하여 고지 받을 권리(제27조), ② 수집 이전 또는 이후 정보처리에 대해 반대할 권리(제26조), ③ 자기에 관한 정보에 대하여 열람, 정정, 삭제를 요구할 권리(제34~40조)를 행사할 수 있다. 한편, 개인정보법 제67조에서는 언론의 자유를 제한하는 것을 목적으로 하는 경우 언론기관에서 취급하는 개인정보에 일부규정을 준용하지 아니 하도록 하고 있다.⁷¹⁾

프랑스의 개인정보보호기구인 정보자유위원회(CNIL; Commission nationale de l'informatique et des libertés)는 17명의 위원으로 구성된 복수집단으로 합의제 기관이다. 특히 위원회를 구성하는 각각의 위원들은 그 자격이나 직위 면에서 볼 때 프랑스의 입법·사법·행정부를 대표하는 자로 이루어져 있어 강력한 권한과 위상을 가지고 있다. 정보자유위원회는 강한 독립성을 갖고 있는 합의제행정기관의 성격을 갖는다. 위원회를 구성하는 위원의 3분의 2가량이 의회나 법원에 의해 선출되고, 각각의 위원들의 독립성을 보장하기 위해 자신을 임명한 자 또는 소속기관의 지시 감독을 받지 않고 자유롭게 활동할 수 있도록 명시적으로 규정하고 있다.

70) Loi n° 78-17 §8 I. Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

71) Loi n° 78-17 §67 Le 5° de l'article 6, les articles 8, 9, 22, les 1° et 3° du I de l'article 25, les articles 32, 39, 40 et 68 à 70 ne s'appliquent pas aux traitements de données à caractère personnel mis en oeuvre aux seules fins:

1° D'expression littéraire et artistique;

2° D'exercice, à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession.

또한 정부의 장관이나 공공기관, 공기업, 사기업의 경영자 등은 여하한 이유로도 위원회의 활동을 방해할 수 없도록 규정함으로써, 위원회의 독립성을 더욱 강화하고 있다. 따라서 위원회는 임무수행에 대해서도 대통령과 의회에 직접 보고하며 직원의 임명도 위원장이 자유롭게 행한다. 또한 위원회는 행정기관의 성격을 갖기 때문에, 위원회의 결정은 행정행위로서의 성격을 띠며, 결정을 대상으로 콩세유데따(Conseil d'Etat)에 상소할 수 있다.

정보자유위원회는 정보처리 내지 정보의 축적에 관하여 확인하고 조사하는 기능을 수행하는데, 프랑스 안에서 이루어지는 모든 정보처리 및 축적에 대하여 등록 또는 신고접수를 통해 그 현황을 파악하고 이를 바탕으로 정보처리과정을 규제하고 있다. 또한 위원회는 정보관리자가 개인정보보호법규에 적합하게 개인정보를 처리하고 있는지 그 준수여부를 감독하는 기능을 수행하며, 정보처리에 관한 기준과 규범을 제시하는 규칙을 제정할 권한을 가진다. 이에 덧붙여 위원회는 정보주체의 접근권 및 정정요구권이 침해되지 않도록 보다 적극적인 역할뿐만 아니라 소송에 앞서 전문적이고 포괄적인 피해구제를 담당하고 있다. 아울러 위원회는 상담, 자문, 검토, 제안 등을 통한 정보제공의 역할도 담당하고 있다.⁷²⁾

(3) 독 일

독일은 연방정보보호법(Bundesdatenschutzgesetz; BDSG)이라는 통합법에서 공공부문과 민간부문을 별도 장(章)으로 구분하여 개인정보보호에 관하여 규율하고 있다. 기본법인 BDSG 소정의 개인정보란 특정한 또는

72) Voir Loi n° 78-17 Chapter III (The Commission Nationale De L'Informatique Et Des Libertés)

특정할 수 있는 일체의 개인의 인적 또는 물적 정보를 말하며, 자동화된 정보처리뿐만 아니라 서류들도 그 범주에 포함된다.⁷³⁾ 1977년에 제정된 BDSG은 이후 여러 차례에 걸쳐 개정되어왔고 현재 지난 2006년 8월 22일 개정된 것(BGBl. I S. 1970)이 현행법이다.

독일에는 개인정보보호에 관한 연방기본법인 BDSG 이외에도 주요한 개별법으로 ‘정보통신역무에 관한 기본조건의 규율에 관한 법률(Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste)’ 제2편으로 편입된 바 있는 통신역무정보보호법(Teledienstedatenschutzgesetz; TDDSG)이 존재한다.⁷⁴⁾ 한편 세계 최초로 제정되었던 멀티미디어법인 미디어서비스국가협약(Staatsvertrag über Mediendienste; MDStV)이 체결된 지 10년 만에 단일 법안으로 마련된 것으로 융합서비스의 경제적 활동 지원을 목적으로 하는 전자상거래단일화법(Elektronischer-Geschäftsverkehr- Vereinheitlichungsgesetz;

73) BDSG §3 (Weitere Begriffsbestimmungen) (1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder
2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, ungeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

74) 인터넷과 같은 새로운 정보통신수단의 급속한 확산으로 개인정보 관련 권리침해의 태양이 종전과 다른 형태로 전개되기에 이르자 정보통신서비스의 효율적 규율을 위한 특별법으로 제정된 것이 1997년 7월 22일 제정된 ‘전기통신서비스에 있어서의 정보보호에 관한 법률(Gesetz über den Datenschutz bei Telediensten)’이고 TDDSG는 그 약칭인바, 최종적으로 2007년 2월 26일 개정되어 오늘에 이르고 있다. 전기통신서비스 이용자의 개인정보를 보호하기 위해 전기통신서비스제공자가 개인정보를 취급하는 데 적용되는 TDDSG는 개인정보의 수집·처리가 오직 직업적으로나 서비스 목적으로만 이루어질 경우 해당 서비스관계와 근로관계에 적용되지 않는다.

ElGVG)의 세부법률인 텔레미디어법(Telemediengesetz; TMG)이 있다.⁷⁵⁾

연방정보보호법은 법의 보호법익이 일반적 인격권임을 분명하게 규정하였다. 법 제1조에서 이 법의 목적은 개인정보의 취급과정에서 개인의 인격권의 침해를 방지하는 데 있다고 규정하고 있기 때문이다.⁷⁶⁾ 이는 정보보호법이 정보남용으로부터 개인을 보호하는 것에만 제한되지 않음을 명백히 하면서 그 보호 목적을 확대하고 구체화한 것이다.

연방 및 주의 공공부문과 함께 개인정보의 수집·생산·이용이 다만 개인적이거나 가족적인 활동영역이 아니라는 전제로 민간부문에 있어 개인정보처리를 통해 개인정보를 생산·이용 또는 수집하는 경우나 비자동화된 개인정보모음집을 통해 개인정보를 생산·이용·수집하는 경우가 이 법의 적용영역이다.⁷⁷⁾ 후자의 민간부문 주체는 사법상 자연인과 법인 및 기업과 다른 사법상의 단체이다. 다만, 민간부문이 공행정의 주권적 임무를 수행하는 경우 이 법에 있어서는 공공부문에 속한다.⁷⁸⁾ 결국 독일 개

75) TMG 제1조제1항은 “이 법은 통신법 제3조제24항에 의해 통신으로, 방송국가협약 제2조에 의해 방송으로 규정하지 않은 모든 전자적 정보 및 커뮤니케이션서비스에 적용된다”고 범위를 정하고 있고 통신에는 방송망에서의 전송서비스를 포함하여 전통적인 음성전화처럼 신호 전송만을 하는 서비스들이 속하는 바, TMG는 정보보호와 관련하여 제11조부터 제15조에서 구체적으로 규정하고 있다.

76) BDSG §1 (Zweck und Anwendungsbereich des Gesetzes) (1) Zweck dieses Gesetzes ist es, den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

77) BDSG §1 (Zweck und Anwendungsbereich des Gesetzes) (2) 3. Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen, soweit sie die Daten in oder aus Dateien geschäftsmäßig oder für berufliche oder gewerbliche Zwecke verarbeiten oder nutzen.

78) BDSG §2 (Öffentliche und nicht-öffentliche Stellen) (4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere

인정보보호법체계의 특징은 일반법이 공공부문과 민간부문 모두를 포괄하고 있지만 해당영역에 따라 적용범위가 다르다는 것이다. 곧 공적 영역에서 개인정보를 다루고자 하는 경우에는 그 수집 및 처리방법과는 상관없이 포괄적으로 위 법에 구속되지만, 사적 영역의 경우 개인정보의 수집·처리·이용이 자동화되거나 서류모음을 통하여 개인을 식별할 수 있는 경우에 연방정보보호법이 적용된다.

연방정보보호법 제1조에 따르면 이 법은 개인정보의 수집·생산 및 이용이 된 경우 적용된다. 법의 적용범위를 개인정보는 정보의 조사로부터 처리(저장, 변경, 전달, 삭제, 이용)를 거쳐 익명화될 때까지로 규정하고 있어서, 개정된 법률에 정보의 조사와 이용이 포함됨으로써 정보처리 이외의 모든 개인정보의 사용이 정보이용을 뜻하게 되었다. 동의는 관련인의 자유결정에 의했을 경우에만 효력이 있다. 개별적 상황에 따라 필요하거나 요구에 따른 경우 동의의 거부에 따른 결과에 대하여 관련인에게 개인정보의 수집목적 및 생산 또는 이용에 관하여 설명해주어야 한다. 동의는 특별한 상황에 따른 다른 방법이 적절하지 않다면 서면 형식을 갖추어야 한다. 동의가 다른 설명과 함께 서면 형식으로 교부되어야 한다면 이 동의는 특별히 강조되어야 한다.⁷⁹⁾

독일에서 개인정보보호기구로 활동하는 연방개인정보보호관(Bundesbeauftragter für den Datenschutz)은 행정조직상으로는 연방내무부 소속으로 예산이나 인력자원과 같은 행정적 사안에 대해서는 연방내

Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

79) Vgl. BDSG §4a (Einwilligung)

무부장관으로부터 지원을 받으나, 직무수행에 있어서는 법률에 따라 독자적으로 활동할 수 있도록 보장받고 있다. 주로 연방정부와 공공기관, 연방정부 산하단체, 연방법원, 여러 주에 걸쳐 사업하는 우편이나 통신사업자 등에 대해서만 관할한다. 연방정보보호법은 공공부문과 민간부문 모두에 적용되는 기본법이지만 개인정보보호기구는 공공부문과 민간부문이 분리되어 설치·운영되고 있다는 점이 특징으로 한다. 연방개인정보보호관은 주로 개인정보를 취급하는 연방정부 및 연방공공기관에 대한 규제와 관리감독의 기능을 수행한다. 따라서 연방정부 등을 상대로 제기된 민원 신고를 접수하여 처리하고, 관할 영역에 해당되는 기관들의 개인정보처리 현황을 점검하고 조사 감독하는 기능을 수행하며, 관할범위에 해당되는 개인정보처리자를 등록하는 등록부를 유지 관리하고 의회 및 정부에 대한 법률정책자문을 기능을 수행한다.⁸⁰⁾

하지만 기존 연방개인정보보호관은 연방정보위원(Bundesbeauftragte für den Datenschutz und die Informationsfreiheit)으로 명칭이 변경되었으며, 정보자유에 관한 권한까지 담당하게 되었다.

한편, 개인정보보호와 정보보안을 개선하기 위해서는 정보처리시스템과 프로그램의 공급자와 정보처리를 실행하는 단체가 독립적이고 승인된 사정관이 시험하고 평가한 개인정보보호 계획안 및 기술적 설비를 보유할 수 있어야 할 뿐만 아니라 감사결과를 출간할 수 있어야 한다. 감사에 관한 상세한 필요조건과 평가, 사정관의 절차 및 선택 및 승인은 다른 법에 규정된다.⁸¹⁾

80) Vgl. BDSG §§22-26.

81) BDSG §9a (Datenschutzaudit) Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie

(4) 일 본

일본은 1970년대부터 세계적인 흐름에 맞추기 위해 개인정보보호를 위한 법체계를 도입하기 위한 논의를 진행시켜왔고, EU의 개인정보보호강화 요구에 대응하기 위해 개인정보보호법제의 정비를 추진하여 2003년 5월에 개인정보보호 관련 5개 법률을 제·개정하였다.⁸²⁾

여기에는 우선 공공부문과 민간부문에 공통으로 적용되는 기본법의 지위와 민간부문의 일반법의 지위를 갖고 있는 개인정보보호법(個人情報の保護に関する法律)이 있고, 개인정보보호법에 의해 공공부문에는 행정기관개인정보보호법(行政機関の保有する個人情報に関する法律)⁸³⁾이 존재한다.

개인정보보호법은 고도정보통신사회의 진전에 수반한 개인정보의 이용이 현저히 확대되고 있다는 것을 감안하고, 개인정보의 적정한 취급에 관하여 기본원칙 및 정부에 의한 기본방침의 작성 기타 개인정보의 보호에

ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

82) 이들 개인정보보호 관련 5개 법률은 「개인정보보호법(個人情報の保護に関する法律)」, 「행정기관보유개인정보보호법(行政機関の保有する個人情報に関する法律)」, 「독립행정법인보유개인정보보호법(獨立行政法人等の保有する個人情報に関する法律)」, 「정보공개·개인정보보호심사회설치법(情報公開・個人情報保護審査會設置法)」, 「행정기관보유개인정보보호법 등의 시행에 따른 관계법률의 정비 등에 관한 법률(行政機関の保有する個人情報に関する法律等の施行に伴う關係法の整備等に関する法律)」 등이 그것이다.

83) 이 법은 행정의 적정하고 원활한 운영을 도모하고 개인의 권리이익을 보호함을 목적으로 하는 공공부문의 일반법이다. 이 법은 행정기관에서의 개인정보취급, 개인정보과일, 본인의 권리와 불복청구 등을 규정하고 있다.

관한 시책의 기본이 되는 사항을 정하며, 국가 및 지방공공단체의 책무 등을 명확히 함과 개인정보를 취급하는 사업자가 준수하여야 할 의무 등을 정하는 것에 의하여 개인정보의 유용성에 배려하면서, 개인의 권리이익을 보호하는 것을 목적으로 한다.

<표 10> 일본의 개인정보보호 법률체계

구분	공공부문			민간부문
대상	국가행정기관	독립행정기관, 특수법인, 행정기관에 준하는 기관	지방자치단체	개인정보 취급사업자
기본법	<개인정보보호법> ○ 개인정보의 취급에 관한 기본원칙 ○ 국가, 지방자치단체의 책무 ○ 민간 개인정보취급자의 의무 ○ 사업자 및 인정개인정보보호단체에 의한 자율적 피해구제제도			
일반법	<행정기관보유 개인정보보호법> ○ 일반 행정기관 보유정보의 취급 원칙 ○ 이용목적 내 정보보유 ○ 목적 외 이용· 제공금지 ○ 정보주체의 열람· 정정청구권 인정	<독립행정법인 보유개인정보 보호법> ○ 일반 행정기관 과 동일하게 취급됨	<개인정보 보호조례>	개인정보보 호법으로 규율

개인정보보호법은 개인정보취급사업자에 대한 규율을 우선으로 하되 국가기관과 지방공공단체에 대하여 별도의 책무를 규정하고 있으므로 개인정보보호에 관한 기본법이자 민간부문개인정보보호에 있어 일반법의 기능을 담당한다고 하겠다. 따라서 공공부문에 대하여는 행정기관개인정보보호법이 일반법의 지위를 가지므로 개인정보보호법에서는 다만 그 기본이념으로 “개인정보는 개인의 인격존중의 이념 아래 신중하게 취급되어야 하며, 그의 적정한 취급을 도모하여야 한다”는 선언적 규정을 천명하고 있다.⁸⁴⁾ 생존하는 개인에 관한 정보로서, 다른 정보와 용이하게 대조할 수 있고 그에 의하여 특정의 개인을 식별할 수 있게 되는 것을 포함하여 당해정보에 포함된 성명·생년월일 기타 기술 등에 의하여 특정한 개인을 식별할 수 있는 것을 개인정보로 정의하고 있는 개인정보보호법에서는,⁸⁵⁾ 개인정보취급사업자가 개인정보를 취급함에 있어 그 이용목적 가능한 한 특정하여야 하고, 미리 본인의 동의를 얻지 아니하고 특정된 이용목적의 달성에 필요한 범위를 넘어 개인정보를 취급하여서는 아니 되며, 위계 기타 부정한 수단에 의하여 개인정보를 취득해서는 아니 된다.⁸⁶⁾ 그리고 정보주체에게 개인정보의 정정·추가·삭제·이용정지 또는 소거의 청구권한을 부여하고 있으며,⁸⁷⁾ 방송기관·신문사·통신사 등 보도용, 저술용, 학술연구용, 종교활동용 및 정치활동용의 제공목적에 대하여는 개인정보보호법 적용제외대상이 된다.⁸⁸⁾

84) 個人情報の保護に関する法律 第三條（基本理念）個人情報とは、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることにかんがみ、その適正な取扱いが図られなければならない。

85) 個人情報保護に関する法律 第二條（定義）1. この法律において「個人情報」とは、生存する個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）をいう。

86) 個人情報保護に関する法律 第四章 第一節（個人情報取扱事業者の義務）参照.

87) 個人情報保護に関する法律 第二十六 乃至 二十九條 参照.

공공부문에서는 2003년 5월 「정보공개·개인정보보호심사회설치법」을 제정하여 개인정보의 보호에 대한 행정기관의 자문과 개인정보보호 사무를 처리하는 정보공개·개인정보보호심사회가 설치되었다. 심사회는 행정기관이 보유하는 정보의 공개와 행정기관 등이 보유하는 개인정보보호에 관한 업무를 담당하는 기관으로 관계 행정기관 등의 자문에 응하고, 불복청구에 대한 조사심의를 담당하며, 행정기관의 장 등에게 답신을 한다. 이러한 업무를 수행하기 위해 심사회는 자문을 한 행정기관의 장 등에게 보유개인정보의 제시를 요구할 수 있다.⁸⁹⁾

88) 個人情報の保護に関する法律 第五十條（適用除外）1. 個人情報取扱事業者のうち次の各号に掲げる者については、その個人情報を取り扱う目的の全部又は一部がそれぞれ当該各号に規定する目的であるときは、前章の規定は、適用しない。

- 一. 放送機関、新聞社、通信社その他の報道機関(報道を業として行う個人を含む) 報道の用に供する目的
- 二. 著述を業として行う者 著述の用に供する目的
- 三. 大學その他の學術研究を目的とする機關若しくは団体又はそれらに屬する者 學術研究の用に供する目的
- 四. 宗教団体 宗教活動 (これに付隨する活動を含む) の用に供する目的
- 五. 政治団体 政治活動 (これに付隨する活動を含む) の用に供する目的

89) 情報公開・個人情報保護審査會設置法 第九條（審査會の調査權限）1. 審査會は、必要があると認めるときは、諮問廳に對し、行政文書等又は保有個人情報の提示を求めることができる。この場合においては、何人も、審査會に對し、その提示された行政文書等又は保有個人情報の開示を求めることができない。

2. 諮問廳は、審査會から前項の規定による求めがあったときは、これを拒んではならない。

3. 審査會は、必要があると認めるときは、諮問廳に對し、行政文書等に記録されている情報又は保有個人情報に含まれている情報の内容を審査會の指定する方法により分類又は整理した資料を作成し、審査會に提出するよう求めることができる。

4. 第一項及び前項に定めるもののほか、審査會は、不服申立てに係る事件に關し、不服申立人、參加人又は諮問廳（以下「不服申立人等」という。）に意見書又は資料の提出を求めること、適当と認める者にその知っている事實を陳述させ又は鑑定を求めることその他必要な調査をすることができる。

情報公開・個人情報保護審査會設置法 第十三條（提出資料の閲覽）1. 不服申立人等は、審査會に對し、審査會に提出された意見書又は資料の閲覽を求めることができる。この場合において、審査會は、第三者の利益を害するおそれがあると認めるとき、その他正当な理由があるときでなければ、その閲覽を拒むことができない。

한편, 민간부문에 대한 개인정보보호기구와 관련하여 일본은 미국과 마찬가지로 독자적인 국가차원의 개인정보보호기구가 존재하지 않는다. 다만, 각 개별법률 또는 해당영역을 관할하는 소관주무부처가 개인정보보호기관의 역할을 담당한다. 이와 관련하여 개인정보보호법 제32조 내지 제40조는 개인정보보호를 위한 주무대신의 권한을 규정하고 있다. 즉, 개인정보보호법이 규정하고 있는 주무대신의 권한은 ① 개인정보취급사업자 및 인정개인정보보호단체(認定個人情報保護団体)로부터 필요한 경우 개인정보 취급 등에 대한 보고를 받을 수 있고, ② 개인정보취급사업자에게 필요한 사항을 조언할 수 있으며, ③ 개인정보취급사업자가 의무규정을 위반하였을 경우 그러한 행위의 중지 또는 시정의 권고를 할 수 있을 뿐만 아니라, ④ 개인정보취급사업자가 정당한 이유 없이 권고를 무시하여 개인의 중대한 권익이 침해될 위험이 있는 경우 권고이행명령을 내릴 수 있고 긴급한 조치가 필요하다고 인정될 경우에는 사업자에게 의무위반행위의 중지명령 및 시정명령을 내릴 수 있다.

또한 인정개인정보보호단체는 개인정보보호지침을 작성·공표하고 대상사업자로 하여금 이를 준수토록 지도·권고 그밖에 조치를 취하여야 하는 바,⁹⁰⁾ 주무대신은 인정개인정보보호단체에 대하여 인정업무 실시방법의 개선 및 개인정보보호지침의 변경 그밖에 필요한 조치를 취하도록 명할 수 있다.⁹¹⁾ 민간차원의 개인정보보호기구로 개인정보피해구제의 역할을 담당하는 인정개인정보보호단체는 주무대신이 민간 개인정보보호단체에

2. 審査會は、前項の規定による閲覧について、日時及び場所を指定することができる。

90) 個人情報の保護に関する法律 第四十三條（個人情報保護指針）參照。

91) 個人情報の保護に関する法律 第四十七條（命令）主務大臣は、この節の規定の施行に必要な限度において、認定個人情報保護団体に對し、認定業務の實施の方法の改善、個人情報保護指針の変更その他の必要な措置をとるべき旨を命ずることができる。

대하여 적절한 역할을 담당하는 개인정보보호기구임을 인정해 줌으로써 민간의 자율규제와 정부의 적절한 감독을 함께 조화시킬 수 있다는 점에서 의미 있는 기관이다. 인정개인정보보호단체는 주로 개인정보취급사업자의 개인정보의 적절한 취급을 지원하고 확보할 목적으로 활동하는 단체로서, 사업자에게 필요한 정보를 제공하거나 사업자의 개인정보 취급 관행으로 인한 피해를 입은 소비자의 문제제기를 원만히 해결하고 피해 구제를 받을 수 있도록 지원하는 기능을 수행한다.⁹²⁾

2. 법안의 주요내용

(1) 1안

법안 제9조에서는 개인정보 보호위원회(이하 '위원회'라 한다)의 창설을 규정하고 있는바, 개인정보 보호에 관한 사항을 심의하기 위하여 국무총리 소속으로 위원회를 둔다는 점이 같은 조 제1항에 명시되어 있다. 국무총리 소속이라는 점에서 정부조직법에 따른 행정안전부의 정보보호에 관한 사무를 통할하는 국무총리의 사무 가운데 개인정보 보호에 관한 사항을 독립적으로 수행하는 합의제행정기관을 두고 있는 것이다. 다만, 위원회의 기능과 역할이 의결기관으로 수렴되는 측면에 있어서는 국무총리

92) 個人情報の保護に関する法律 第四十二條（苦情の處理）1. 認定個人情報保護団体は、本人等から対象事業者の個人情報の取扱いに関する苦情について解決の申出があったときは、その相談に応じ、申出人に必要な助言をし、その苦情に係る事情を調査するとともに、当該対象事業者に対し、その苦情の内容を通知してその迅速な解決を求めなければならない。
2. 認定個人情報保護団体は、前項の申出に係る苦情の解決について必要があると認めるときは、当該対象事業者に対し、文書若しくは口頭による説明を求め、又は資料の提出を求めることができる。
3. 対象事業者は、認定個人情報保護団体から前項の規定による求めがあったときは、正当な理由がないのに、これを拒んではならない。

소속이라는 위상과 결부하여 볼 때 개인정보 보호에 관한 실질적 집행력 부재라는 관점에서 논란이 가중될 여지가 있다. 여하튼 위원회는 위원장 1명을 포함한 15명 이내의 위원으로 구성되며, 위원장은 공무원이 아닌 사람으로서 개인정보 보호에 관하여 학식과 경험이 풍부한 사람 중에서 국무총리가 위촉하는 사람이 된다. 그리고 위원은 ① 대통령령으로 정하는 중앙행정기관의 고위공무원단에 속하는 공무원, ② 개인정보 보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람, ③ 개인정보처리자로 구성된 사업자단체로부터 추천을 받은 사람, ④ 그 밖에 개인정보에 관한 학식과 경험이 풍부한 사람 중 어느 하나에 해당하는 사람을 국무총리가 임명하거나 위촉한다. 위원장과 위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다. 다만, 제4항제1호에 따라 임명된 공무원인 위원은 그 직에 재직하는 동안 재임한다.

한편, 법안 제10조에서는 위원회의 기능과 역할에 대하여 규율하고 있는바, 위원회는 ① 기본계획 및 시행계획, ② 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항, ③ 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항, ④ 개인정보 보호에 관한 법령의 해석·운용에 관한 사항, ⑤ 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항, ⑥ 제31조제3항에 따른 영향평가 결과에 관한 사항, ⑦ 제51조제1항에 따른 의견제시에 관한 사항, ⑧ 제54조제4항에 따른 시정조치 권고에 관한 사항, ⑨ 제56조에 따른 처리 결과의 공표에 관한 사항, ⑩ 개인정보 보호와 관련하여 국무총리 또는 위원장이 회의에 부치는 사항, ⑪ 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의하는 사항 등을 심의한다. 위원회는 위 각 사항을 심의하기 위하여 필요하면 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회단체 및 관련 사업자로부터 의견을 들을 수 있다.

여기서 위원회의 기능과 관련된 심의사항을 구분해 풀어쓰면 다음과 같다.

우선 법안 제7조는 기본계획의 수립에 관한 것인바, 행정안전부장관은 개인정보의 보호와 정보주체의 권익 보장을 위하여 ① 개인정보 보호의 기본목표와 추진방향, ② 개인정보 보호와 관련된 제도 및 법령의 개선, ③ 개인정보 침해 방지를 위한 대책, ④ 개인정보 보호 자율규제의 활성화, ⑤ 개인정보 보호 교육·홍보의 활성화, ⑥ 개인정보 보호를 위한 전문인력의 양성, ⑦ 그 밖에 개인정보 보호를 위하여 필요한 사항 등이 포함된 3년 단위 개인정보 보호 기본계획을 수립·시행하여야 하는데 그 내용적 결정은 위원회의 심의에 구속된다. 즉, 기본계획에 대한 판단은 위원회가 심리·의결로 수행하고 이에 따라 행정안전부가 기본계획을 확정·수립하여 시행하는 구조이다. 또한 법안 제8조제1항에 따라 중앙행정기관의 장은 기본계획에 따라 매년 개인정보 보호를 위한 시행계획을 위원회의 심의를 거쳐 수립·시행하여야 한다.

다음으로 법안 제18조제1항은 개인정보처리자는 개인정보가 법정범위를 초과하여 이용하거나 제3자에게 제공해서는 아니 됨을 규정하고 있는 바, 그럼에도 불구하고 공공기관이 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 위원회의 심의를 거친 때에는 정보주체 또는 제3자의 이익을 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 개인정보의 목적 외 이용이나 제3자 제공이 적법하기 위한 요건으로 주체 측면에서는 공공기관에 한정하고 절차 측면에서는 위원회의 심의를 설정하면서 내용 측면에서는 업무수행의 법적 불가피성을 꼽고 있는 것인데, 그 중

하나가 위원회가 심리·의결하여 판단·결정하는 부분이라 하겠다.

그리고 법안 제31조는 이미 살펴본 개인정보 영향평가에 관한 사항인 바, 공공기관의 장은 법령상 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 권리침해가 우려되는 경우 ① 처리하는 개인정보의 수, ② 개인정보의 제3자 제공 여부, ③ 정보주체에의 권리침해 가능성 및 그 위험 정도를 고려하여 그 위험요인의 분석과 개선사항 도출을 위한 영향평가를 하고 그 결과를 행정안전부장관에게 제출하여야 하며, 영향평가 결과를 받은 행정안전부장관은 그 결과에 대하여 위원회의 심의를 거쳐 의견을 제시할 수 있다. 하지만 권고적 효력을 지니는 행정지도로서 비권력적 관계에 해당하는 행정안전부장관의 의견제시에 위원회의 심의가 절차적 관점에서의 신중한 판단을 도모하는 것 이외에 실질적인 개인정보 보호정책의 실효성 확보에 얼마나 조력할 수 있을지에 대하여는 의문스런 부분이 존재한다. 이는 법안 제51조제1항에서 행정안전부장관은 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 위원회의 심의를 거쳐 관계기관에 의견을 제시할 수 있다고 하여 의견제시 및 개선권고 관련 재량권이 부여된 상태에 위원회의 심의를 필수적 절차로 설정한 데서 동일하게 문제점으로 지적할 수 있는 대목이다.

(2) 2안

법안 제40조는 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 대통령 소속으로 개인정보보호위원회(이하 '위원회'라 한다)를 두도록 규정하고 있는바, 합의제행정기관임에는 차이가 없으나 대통령 소속이라는 위상적 측면과 이하 분석할 그 기능과 역할이 1안과 구별된다. 조직

적 구성에 있어 법안 제41조는 위원회가 위원장 1인과 상임위원 1인을 포함한 9인의 위원으로 구성되며, 위원은 개인정보보호에 관한 학식과 경험이 풍부한 자 중에서 국회가 선출한 3인(상임위원 1인을 포함한다), 대통령이 지명하는 3인, 대법원장이 지명하는 3인을 대통령이 임명하고, 위원장은 위원 중에서 대통령이 임명한다는 점을 명시하고 있다. 법안 제42조제3항에 따르면 위원장과 위원의 임기는 각각 3년으로 하되 연임할 수 있으며, 같은 조 제4항에서 같이 위원은 ① 「국가공무원법」 제33조 각 호의 어느 하나에 해당하는 때, ② 「공직선거법」에 따라 실시하는 선거에 후보자로 등록한 때, ③ 신체상 또는 정신상의 장애로 직무수행이 현저히 곤란한 때를 제외하고는 그 의사에 반하여 면직되지 아니한다는 점은 위원의 신분보장을 통한 위원회의 독립성을 위한 사항이라 할 수 있다. 법안 제44조는 위원회가 재적위원 과반수의 출석으로 개의하고 출석위원 과반수의 찬성으로 의결함을 명시하고 있다.

위원회의 업무와 권한에 있어 우선 법안 제47조는 위원회가 ① 개인정보 보호에 관한 중장기 계획 및 연차계획의 수립 및 시행, ② 개인정보처리의 실태, 관행 등에 관한 조사·연구 및 개선, ③ 개인정보의 처리 및 보호에 관련 법령·제도 등의 조사·연구 및 개선, ④ 개인정보보호기준의 제정·고시, ⑤ 개인정보 유출, 오남용 등의 사건에 대한 조사 및 고충·진정의 처리, ⑥ 개인정보처리로 인한 분쟁의 조정 및 피해구제, ⑦ 개인정보 보호에 관한 기술개발의 지원 및 보급, ⑧ 개인정보의 처리 및 보호에 관한 교육 및 홍보, ⑨ 개인정보보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력, ⑩ 이 법안 및 다른 법령에 따라 위원회의 소관으로 규정된 사항, ⑪ 그밖에 개인정보의 처리 및 보호를 위하여 필요하다고 인정되는 사항을 소관 업무로 수행한다고 규율하고 있다.

다음으로 법안 제48조제2항은 법령 또는 조례가 개인정보보호에 영향을 미칠 내용을 포함한 경우에는 위원회는 해당 행정기관, 국회, 지방자치단체, 지방의회 등에 의견을 제시할 수 있게 규정하고 있으며 법안 제49조제1항은 개인정보보호를 위하여 필요하다고 인정하는 때에는 위원회가 개인정보처리자에 대하여 정책·관행의 개선을 권고할 수 있도록 명시하고 있는바, 독립적 위상을 가진 위원회가 판단하여 수행하는 의견제시와 개선권고가 1안과 같이 심리·의결이라는 판단의 절차에 치중되어 있는 것이 아니라 공공·민간을 아울러 독립된 개인정보보호업무를 수행하는 측면에서 사실상 영향력은 차이를 가져올 수 있다고 여겨지는 대목이다. 특히 법안 제53조에 따르면 조사 등의 결과 정보주체의 권리가 침해되었거나 권리침해의 우려가 현저한 경우 개인정보처리자가 국가기관·지방자치단체인 때에는 당해 국가기관 또는 지방자치단체의 직근 상급기관으로 하여금 ① 개인정보처리 및 권리침해행위의 중지 및 ② 그 밖에 개인정보의 보호 및 침해방지를 위하여 필요한 조치에 관한 명령을 발하도록 권고할 수 있고, 이 경우 권고를 받은 기관은 그 범위 내에서 시정명령을 내릴 수 있으며, 권고를 받은 기관은 특별한 사유가 없는 한 위원회의 권고를 존중하여야 하며 그 처리결과를 위원회에 통보하여야 하기 때문에 실질적인 개인정보보호에 관한 법집행이 가능하다는 점에서 단순 비권력적 행정지도와는 차별성을 읽을 수 있다고 하겠다.

한편, 법안 제56조는 위원회가 개인정보보호기준의 제정·고시할 수 있음을 명시하고 있고 제58조제1항은 개인정보보호시책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출토록 하고 있는 까닭에, 개인정보보호에 관한 독립적 위상을 지닌 위원회가 의견수렴을 통해 협력적으로 개인정보보호기준을 제정하여 시행함으로써 법집행의 완결성을 높일 수 있고 입법기관에 대한 책임 강화로써 대국민적 법

집행이 권력분립원리 아래 적절히 통제될 수 있는 기제를 확보하고 있다고 하겠다.

(3) 3안

법안 제34조는 개인정보의 보호에 관한 업무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보위원회(이하 '위원회'라 한다)를 설치하도록 규정하고 있는바,⁹³⁾ 그 구성에 관하여 법안 제35조에서는 위원회는 위원장 1인과 상임위원 1인을 포함한 9인의 위원으로 구성되고, 위원장과 상임위원은 국무총리가 제정한 자를 대통령이 임명하며, 비상임위원은 위원장이 추천한 자 중에서 국무총리가 임명하도록 설정하고 있다. 위원의 신분보장은 2안과 유사하다.

위원회의 업무와 권한에 있어 우선 법안 제41조는 ① 개인정보의 보호 및 이용에 관한 시책의 수립 및 집행, ② 개인정보에 관한 법령·제도 및 관행의 조사·연구 및 개선, ③ 개인정보보호기준의 제정·고시, ④ 정보주체의 권리침해에 대한 조사, ⑤ 개인정보의 수집·처리와 관련한 고충처리·피해구제 및 분쟁조정, ⑥ 개인정보의 수집·처리 실태 등에 관한 조사·연구, ⑦ 개인정보보호에 관한 기술개발의 지원 및 보급, ⑧ 개인정보의 이용 및 보호에 관한 교육 및 홍보, ⑨ 개인정보보호단체의 지원 및 자율 규제활동의 촉진, ⑩ 개인정보보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력, ⑪ 이 법안 및 다른 법령에 따라 위원회의 소관

93) 개인정보의 수집·처리와 관련하여 개인의 자유와 권리를 보호하고 개인정보의 적정한 이용을 보장함으로써 정보사회의 균형 있는 발전에 이바지함을 목적으로 하는 이 법안에서 위원회의 임무가 개인정보의 보호와 이용의 균형적 발전에 있음을 명확히 하기 위하여 명칭을 '개인정보보호위원회'가 아닌 '개인정보위원회'로 한다는 점이 법안 제안이유에 명시되어 있다.

으로 규정된 사항, ⑫ 그 밖에 개인정보의 보호 및 이용을 위하여 필요하다고 인정하는 사항 등의 업무를 위원회가 수행한다고 규정하고 있다.

의견제시·개선권고 및 시정명령권고 등은 2안과 유사하며 위원회의 개인정보보호기준 제정·고시에 관한 권한과 국회에 대한 연차보고 역시 동일하지만, 법안 제52조에서 위원회가 개인정보의 안전하고 합법적인 처리를 지원하기 위하여 개인정보영향 평가 및 인증에 필요한 시설, 인력 및 기술 등을 갖춘 자를 평가·인증기관으로 지정하여 ① 개인정보 영향평가 및 인증표시의 부여, ② 개인정보 영향평가기법의 개발 및 보급, ③ 개인정보보호 및 영향평가와 관련한 전문인력의 양성, ④ 개인정보보호를 위한 교육 및 지도, ⑤ 개인정보보호기술의 개발 및 보급, ⑥ 그 밖에 개인정보의 안전한 처리를 지원하기 위하여 대통령령으로 정하는 사업 등의 업무를 수행하게 할 수 있다는 점은 특기할 만한 사항이다.

제3절 법제화 방향

1. 이론적 전제

현재 국회 계류중인 세 법안이 설정하고 있는 개인정보보호기구에 있어서는 조직상 국무총리 혹은 대통령 소속 합의제행정기관으로 작용상 심의 혹은 의결의 역할을 담당하는가 아니면 집행의 기능으로 행정청이 되는가가 교차적으로 논의되어야 하는 쟁점이 있다.⁹⁴⁾ 이른바 실질적 헌법에 해당하는 「정부조직법」은 제5조에서 “행정기관에는 그 소관사무의 일부를 독립하여 수행할 필요가 있는 때에는 법률이 정하는 바에 의하여 행정위원회 등 합의제행정기관을 둘 수 있다”고 명시하고 있는바, 위 개인정보보호기구는 모두 이에 해당한다. 합의체로서 개인정보보호기구, 즉 위원회는 법인격이 없는 행정주체의 기관(organ)에 해당한다. 그리고 권력분립원리(三權分立原理)를 실질적으로 이해할 경우 위원회는 입법적 혹은 사법적 작용을 담당하지 않으므로 당연히 행정기구의 위치를 점하는 것으로 봄이 타당하다.⁹⁵⁾ 반면, 행정에 관한 권리·의무의 귀속주체인 행정주체가 되기 위해서는, 자연인이나 사법상의 법인은 행정주체로부터 행정권을 위임받아 행사할 수는 있어도 그 자체가 본래적으로 행정권을

94) 국가의 표현기관을 행정관청이라고 하고 지방자치단체의 표현기관을 행정청이라 하는바, 흔히 행정관청과 행정청을 포괄하여 행정청이라 부르며 이를 광의의 행정청이라 한다.

95) 권력분립을 이해함에 있어 분화된 기관의 관점에서 권력을 나누는 형식적 기준이 우선적으로 고려되어야 할 것이다. 물론 국가의 권력을 분리하여서만은 안되고 상호간에 조화와 협동을 할 수 있는 연결이 필요하기 때문에 기능상의 권력분립 역시 필요하게 된 것이다. 따라서 규범의 정립권한을 의회에 맡기고, 그 집행을 행정권에 맡기며, 그 집행에 대한 판정권한을 사법부에 맡긴다고 하는 실질적 의미의 권력분립이 형식적 의미의 권력분립 위에 중첩되었을 뿐, 처음부터 국가권력이 성질상 구별되어 존재하였던 것은 아니다; 이광윤·김민호, 최신행정법론, 법문사, 2002, 17쪽.

가질 수는 없으므로 당연히 공법상의 법인이어야 한다.

한편 대통령령으로 제정된 「행정기관의 조직과 정원에 관한 통칙」은 제21조에서 “「정부조직법」 제5조의 규정에 의하여 행정기관에 그 소관사무의 일부를 독립하여 수행할 필요가 있을 때에는 법률이 정하는 바에 의하여 행정기능과 아울러 규칙을 제정할 수 있는 준입법적 기능 및 이의결정 등 재결을 행할 수 있는 준사법적 기능을 가지는 행정위원회 등 합의제행정기관을 둘 수 있다”고 규정하고 있는바, 여기서는 행정위원회에 관한 역할론적 정의만이 상세화되어 있을 뿐이고 합의제행정기관의 구체적 개념에 대하여는 언급이 되지 않고 있다.

일반적으로 한 사람의 공무원의 책임으로 행정을 처리하는 행정기관 형태인 독임제행정관청(獨任制行政官廳)과 구별되는 합의제행정기관(合議制行政機關)은 대통령·국무총리 및 행정각부에 소속되어 1973년 이래 설치되고 있는바, 역순으로 그 소속별 분류에 따라 기구현황을 살펴보면 다음과 같다.

우선 현재 행정각부에 부속되어 있는 「정부조직법」 제5조 소정의 합의제행정기관을 꼽아 보면, 부처별로 행정기관 소속 공무원의 징계처분 및 불이익처분 등에 대한 소청을 심사·결정하게 하기 위하여 「국가공무원법」 제9조제1항에 따라 행정안전부에 설치되는 소청심사위원회, 토지 등의 수용과 사용에 관한 재결을 하기 위하여 「공익사업을 위한 토지 등의 취득 및 보상에 관한 법률」 제49조에 따라 국토해양부에 설치되는 중앙토지수용위원회, 노동쟁의의 조정·중재 또는 해결지원 등을 위하여 「노동위원회법」 제2조제2항에 따라 노동부장관 소속하에 설치되는 중앙노동위원회 등이 존재한다.

다음으로 다른 법률의 특별한 규정에 의해 국무총리소속으로 설치되는 합의제행정기관을 살펴보면, 시장지배적지위의 남용과 과도한 경제력의 집중을 방지하고 부당공동행위 및 불공정거래행위를 규제하는 업무를 독립적으로 수행하기 위하여 「독점규제 및 공정거래에 관한 법률」 제35조 제1항에 따라 국무총리소속하에 설치되는 공정거래위원회, 외국환업무취급기관의 건전성 감독 및 금융정책·금융감독에 관한 업무를 수행하기 위하여 「금융위원회의 설치 등에 관한 법률」 제3조제1항에 따라 국무총리소속하에 설치되는 금융위원회, 고충민원의 처리와 불합리한 행정제도를 개선하고 부패의 발생을 예방하며 부패행위를 효율적으로 규제하기 위하여 「부패방지 및 국민권익위원회의 설치와 운영에 관한 법률」 제11조에 따라 국무총리소속으로 설치되는 국민권익위원회를 꼽을 수 있다.

마지막으로 대통령소속의 합의제행정기관으로는 현재 방송과 통신에 관한 업무를 수행하기 위해 「방송통신위원회의 설립 및 운영에 관한 법률」 제3조제1항에 따라 대통령 소속으로 설치되는 방송통신위원회만이 존재하고 있다.

주지하는 바와 같이 행정기관이란 조직적으로는 행정사무의 배분단위를 의미하며, 작용적으로는 행정의 주체인 국가 또는 공공단체의 행정사무를 담당하고 그 사무에 관하여 국가 또는 공공단체가 그 기관을 수족(手足)으로 삼아 활동하게 된다. 그리하여 일정한 권한의 귀속자인 행정청의 각종 행위의 효과는 궁극적으로 그 주체, 즉 공법상 법인인 국가 또는 공공단체에 귀속하게 되므로 기관 그 자체로는 법인격을 가지지 않는다.

그런데 국가행정사무의 체계적이고 능률적인 수행을 위하여 국가행정

기관의 설치·조직과 직무범위의 대강을 정함을 목적으로 하는 「정부조직법」은 제2조제2항에서 “중앙행정기관은 이 법과 다른 법률에 특별한 규정이 있는 경우를 제외하고는 부·처 및 청으로 한다”라고 규정하고 있다. 또한 대통령령 제21214호로 2008년 12월 31일 일부개정된 「행정기관의 조직과 정원에 관한 통칙」은 제1조에서 “이 영은 「정부조직법」과 다른 법령에 의하여 설치되는 국가행정기관의 조직 및 정원의 합리적인 책정과 관리를 위한 기준을 정함으로써 능률적인 행정조직의 운영을 기함을 목적으로 한다”고 하면서, 제2조제1호에서 “중앙행정기관이라 함은 국가의 행정사무를 담당하기 위하여 설치된 행정기관으로서 그 관할권의 범위가 전국에 미치는 행정기관을 말한다”고 규정하고 있다. 결국 「정부조직법」 및 「행정기관의 조직과 정원에 관한 통칙」에서 규정하고 있는 중앙행정기관은 대통령과 국무총리를 제외한 정부기관을 의미하게 된다. 그런데 관련규정에 비추어 보면 중앙행정기관은 최고감독기관인 대통령을 정점으로 하는 수직적 구조에 위치해 있으며⁹⁶⁾ 행정권이 대통령을 수반으로 하는 정부에 속함을 규정하고 있는 헌법 제66조제4항 및 「정부조직법」 제11조 소정의 정부를 구성하여 그 관할범위를 전국에 미치는 행정기관으로서, 여기에는 부·처·청 및 합의제행정기관이 포함된다고 할 수 있다.

2. 쟁점 재검토

결국 합의제행정기관인 개인정보보호기구의 쟁점은 그 독립적 기능 수행의 담보에 초점이 맞춰 있으며 이에 따라 그 소속과 작용적 권한이 논의의 핵심이 될 수밖에 없다.

96) 「정부조직법」 제11조 (대통령의 행정감독권) ① 대통령은 정부의 수반으로서 법령에 의하여 모든 중앙행정기관의 장을 지휘·감독한다.

앞에서 금융위원회·공정거래위원회 및 국민권익위원회의 법적 성격에 대하여 이를 국무총리소속으로 새기는 데는 의문의 여지가 있다. 금융위원회·공정거래위원회 및 국민권익위원회가 국무총리소속 합의제행정기관이라고 본다면 대통령을 수반으로 하는 정부에 속하는 행정권 가운데서도 ‘대통령을 보좌하며, 행정에 관하여 대통령의 명을 받아 행정각부를 통할’하는 행정기관인 국무총리의 소관사무 일부를 독립하여 수행할 필요가 있을 때 법률이 정하는 바에 따라 이들이 설치되어야 한다. 이렇게 합의제기관은 국무총리의 소관사무의 일부를 ‘독립’하여 수행하여야 하는 것인데, 여기서의 소관사무라 함은 국무총리가 통할하는 행정각부의 관장사무만이 해당되며 대통령을 보좌하는 직무는 배제될 수밖에 없다. 그러므로 금융·공정거래 및 부패방지 등에 관한 행정사무를 행정각부에서 관장하고 있지 아니한 현재의 정부조직법에 따르면 금융위원회·공정거래위원회 및 국민권익위원회는 국무총리소속하의 합의제행정기관이 될 수 없는 것이다. 따라서 직무범위를 볼 때 설치근거법의 규정이 어떠한 금융위원회·공정거래위원회 및 국민권익위원회는 대통령소속 합의제행정기관으로 해석하는 것이 논리상 타당할 것이다. 다만 이처럼 이들 기관을 국무총리소속 합의제행정기관으로 설정해 둔 것은 위원장의 예우 및 예산상·인사상 이유로 국무총리소속 합의제행정기관으로 편성해 둔 것으로 이해할 수 있을 것이지만, 부위원장을 두고 있는 점도 합의체의 본질에 어긋난다고 볼 것이다.⁹⁷⁾

97) 위와 같은 점을 방송통신위원회에 대입해보면, 정보통신산업에 관한 사무를 관장하는 지식경제부가 행정부로서 대통령과 직렬관계에서 계층적 감독을 받는 것이기에 통신분야에 관한 규율은 대통령소속 합의제행정기관으로서의 지위와 양립할 수 있지만 방송에 관한 사무를 관장하는 행정각부가 명시되지 아니한 정부조직법 아래서 방송분야에 관한 규율을 대통령소속 합의제행정기관으로 볼 수 있느냐에 대하여는 논란이 될 수 있다. 즉, 행정권이 속한 정부의 수반으로서 대통령에게는 행정각부를 통할하여 집행하는 행정권 이외에도 정부의 권한범위 내에 것이라면 행정권으로서 대통령이 총괄한다고 규율하고 있는 헌법 제66조제4항에 비추어 볼 때, 방송부문은 행정각부에 분배되어 있지는

결국 합의제행정기관으로서 위원회의 소속은 그것이 국무총리가 원행정기관이 되든 대통령이 원행정기관이 되든 위원회 자체의 법적 성질이 달라지는 것은 아니고 다만 위원장의 예우 및 예산상·인사상 이유로 해당 원행정기관을 구분함에 지나지 않다. 따라서 관건이 되는 것은 합의제행정기관이 원행정기관의 관여에서 얼마나 독립적이고 자율적으로 행정작용을 담당하느냐가 될 것이다. 그리고 개인정보보호를 위한 위원회의 업무가 적절한 권한행사에 해당하여 정보주체의 정보자기결정권을 보장하는 데 소홀함이 없도록 사무분장이 이루어지는지 여부에 관한 실질적 검토가 필요하다.

우선 「정부조직법」 제5조에 따라 행정기관의 소관사무 일부를 ‘독립’하여 수행할 필요가 있을 때 개별법에 의거하여 창설되는 합의제행정기관

않으나 대통령이 수반이 되는 정부의 권한 내에 있는 행정사무이고 이를 대통령소속 합의제행정기관인 방송통신위원회가 관장하며 통신부문에 있어서 특히 정보통신산업에 관한 사무만을 지식경제부가 관장하는 것으로 새길 수 있을 것이다. 하지만 대통령과 병렬관계에 놓여 있으면서도 행정부에 속하지 않는 영역을 점하고 있는 독립행정위원회를 해석론적으로 엄두에 두면 오히려 방송부문의 경우 공적 여론형성기능을 고려할 때 그 사무의 독립성을 관철하기 위해 무소속으로 설정해야 한다는 입법정책론적 논의와 연계해야 한다고 볼 수 있으며, 이 경우 방송통신위원회가 독립행정위원회이지만 위원장의 예우 및 예산상·인사상 이유로 대통령소속 기관이 된 것으로 여길 수 있게 된다. 여기서 독립행정위원회란 전통적 국가의 공평성과 독립성을 개선하기 위한 방안으로서 중재와 협상을 통한 객관적이고도 효율적인 해결책을 모색하는 과정에서 등장한 것으로, ① 계층적으로나 후견적으로도 감독기관이 없고, ② 정부조직법이 아닌 다른 법률에 의하여 독립성이 부여되기는 하지만 법인격이 없으며, ③ 부·처에 소속되지 않는 행정청을 말한다. 이러한 점에서 독립행정위원회는 중앙의 국가기관이기는 하나 계층적 감독을 받는 직접행정기관인 중앙행정기관이나 후견적 감독을 받는 간접행정기관인 공법상 특수법인과는 다르다. 중앙행정청이나 특수법인은 모두 대통령을 최고감독기관으로 하고 있으나, 독립행정위원회는 대통령의 감독도 받지 않는다는 점에서 대통령과도 병렬관계에 있다. 독립행정위원회는 공법상 행정기구로 법인격은 없으나, 국가행정기관에 속하므로 행정처분권·행정입법권·행정제재권을 보유하지만 예산에 있어서는 국무총리나 정부부처에 의존한다; 拙稿, 정보매체의 규제조직에 관한 법적 연구, 공법연구 제36집 제3호, 한국공법학회, 2008, 497~498쪽.

의 원행정기관과의 관계는 의사결정개입은 물론 지휘감독권도 행사할 수 없지만 인사권은 지니는 관계로서의 독립, 즉 소할(所轄)에 해당한다. 그러므로 대통령이나 국무총리가 원행정기관이 되어 인사권을 행사하는 것 이외에는 위원회에 대하여 의사결정개입은 물론 지휘감독권도 행사할 수 없는 것이다. 소할은 행정기관과 보조기관의 예처럼 인사권은 물론 의사결정과정까지 직접 개입이 가능한 관계인 직속(直屬)이나 대통령과 행정각부와 같이 인사권과 지휘감독권은 가지나 의사결정에 직접 개입 못하는 관계인 통할(統轄)과는 다르기 때문이다. 위원회 구성에서 대통령이 관여하는 것은 공무원임명에 있어서 대통령이 인사권자가 되는 원칙적인 측면을 고려하면 국무총리 소속의 개인정보보호기구보다는 대통령 소속의 개인정보보호기구가 보다 적합한 것이라 할 수 있다. 그렇다고 해서 위원회 자체의 성격이 소속에 따라 달라지는 것은 전혀 아니며, 그렇기 때문에 중국적으로는 위원회에 대한 사무분장에서 정보주체의 정보자기 결정권 보장이 실효성 있게 구조화되는 방안을 찾아야 할 것이다.

그렇다면 1안의 경우 심의기능에 국한된 의결기관으로 합의제행정기관을 설정한 것인데, 여기서 심의(審議; deliberation)는 법적 개념으로서 완전한 결정을 내리기 위하여 논리와 추론의 사용을 강조하는 의사소통방식으로서 법적 발견을 토론하는 과정이자 논쟁에 대한 결정을 말한다.⁹⁸⁾ 그리고 ‘자유로운 토론과 자유로운 투표’라는 원칙에 따라 이루어지는 것이라는 점에서 심의는 결국 심리(審理; hearing)와 의결(議決; resolution)의 합성개념이라 볼 수 있다.⁹⁹⁾ 여기서 심리라 하면 공정한 심의의 기초가 되는 사실관계 및 법률관계를 명확히 하기 위하여 조사하는 공식적

98) <http://en.wikipedia.org/wiki/deliberation>

99) 관련법령에서는 이를 ‘심의·의결’이란 용어를 사용하고 있지만, 여기서는 의사결정 이전의 심사절차를 뜻하는 ‘심리’와 중국적 판단으로서의 ‘의결’이 결합된 ‘심의’라는 용례를 취하기로 한다.

심사행위이며, 의결이라 하면 공정한 심의를 이끌어내기 위하여 심리한 사항에 대해 합의체에서 그 의사를 결정하는 종국적 행위라 할 수 있다. 심리와 의결의 연속적 결합행위인 심의는 의사결정 자체를 이루는 처분에 해당하고 이에 구속되어 법집행이 이어지는 구도를 예정한 것이기에, 행정안전부의 법집행기능에 반감이 없다면 실질적인 의사결정에 주안점을 두어 이를 실현하는 행정과정으로 개인정보의 보호가 이루어지게 하는 것이 법이론적으로 하자 있는 것은 결코 아니다. 하지만 독립성을 견지한 위원회의 법집행으로 완결된 개인정보보호사무를 수행하면서 준입법적·준사법적 기능까지 위원회의 권한으로 업무처리를 행하는 것이 정보주체의 정보자기결정권 보장에 있어 자족적 구성이 이루어진다는 측면에서 2안과 3안이 보다 바람직하다고 볼 수 있다. 결론적으로 대통령 소속 행정위원회로서 2안이 상대적으로 좋은 형식을 취한다고 할 수 있겠는데, 1안을 채택하더라도 위원회 구성에 있어 민주적 정당성을 확보하고 여론 수렴의 기제를 반영할 수 있는 방안을 택하고 심의권한이 발휘되어지는 사안을 확대하여 개인정보보호에 관한 의사결정에 구속되어 이루어지는 법집행은 단순한 개인정보실현작용에 지나지 않는 구조를 명확히 하는 방향에 접점을 둔다면 법현실적인 타협점은 모색될 수 있을 것이라 생각한다.

제4장 개인정보피해구제의 쟁점과 과제

제1절 논의의 배경

주지하는 바와 같이 우리 민법은 제750조에서 “고의 또는 과실로 인한 위법행위로 타인에게 손해를 가한 자는 그 손해를 배상할 책임이 있다”라고 규정함으로써 불법행위에 대한 손해배상책임을 제도화하고 있다. 여기서의 손해는 일정한 원인에 의하여 발생하는 가치·재화 등 이익의 상실을 뜻하며,¹⁰⁰⁾ 사실적 관점에서 고찰할 때 그 원인은 자연적인 것일 수도 인간의 행위에 의한 것일 수도 있다. 그리고 발생한 손해를 누가 부담해야 할 것인가 하는 문제는 발생한 손해와 원인 사이에 인간의 행위와의 관련성이 존재하지 않으면 아니 된다. 한편 불법행위법은 발생한 손해를 피해자 자신의 부담으로 하는 것을 원칙으로 하며, 피해자에게 타인에 대한 손해배상청구권이 주어지려면 발생한 손해에 대하여 가해자에게 책임을 지울 수 있는 법률상 특별한 원인인 귀책사유가 존재하여야 한다.

그런데 개인정보와 관련하여 일반적으로 정보주체는 자기에 관한 정보를 재산적 가치로 인식하기보다는 인격적 가치로 보는 반면, 그 취급자는 인격적 성격보다는 재산적 성격을 중시하게 된다. 따라서 이에 대한 권리 침해가 재산상의 손해로도 인정될 수 있으나, 그 재산적 가치를 산정하여 손해액수를 계산해내기가 곤란하고 또한 상당인과관계의 입증도 곤란한 경우가 많아 비재산적 손해의 배상에 해당하는 위자료 청구문제로 주로

100) Ernst Wolf, *Grundfragen des Schadensbegriffs und der Methode der Schadenserkenntnis*, Festschrift Schiedermair, 1976, S.545ff.

해결하고 있다. 여기서 위자료란 우리 민법 제751조가 제1항에서 “타인의 신체, 자유 또는 명예를 해하거나 기타 정신상 고통을 가한 자는 재산 이외의 손해에 대하여도 배상할 책임이 있다”라고 규정하고 있는 부분에서 재산적 손해에 대응하는 개념으로서의 ‘정신적 고통에 대한 배상’ 또는 ‘비재산적 손해에 대한 배상’으로 드러나며, “타인의 생명을 해한 자는 피해자의 직계존속, 직계비속 및 배우자에 대하여는 재산상의 손해 없는 경우에도 손해배상의 책임이 있다”라고 규정하고 있는 민법 제752조는 그 제명을 ‘생명침해로 인한 위자료’로 하고 있는 까닭에 여기서도 재산 이외의 손해에 대한 배상으로서 위자료 관념을 읽을 수 있다. 위자료 (Schmerzensgeld)란 그야말로 정신적 고통에 대한 배상(Entschädigung)으로서 지급되는 것으로 이해되어 왔다.¹⁰¹⁾

권리침해가 발생하면 그 불법행위로 인하여 발생한 손해를 보전하는 것이 권리구제의 핵심이 되는바, 개인정보에 관한 권리침해의 경우 정신적 손해에 대한 전보적 배상으로서 위자료가 민법상 불법행위에 따른 손해배상이라는 일반원칙에 따라 민사법원을 통해 민사소송으로 제기되어 집행되기에 이른다. 이는 “이용자는 정보통신서비스제공자 등이 이章의 규정을 위반한 행위로 손해를 입은 경우에는 그 정보통신서비스제공자 등에 대하여 손해배상을 청구할 수 있다. 이 경우 당해 정보통신서비스제공자 등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다”고 규정하고 있는 정통방법 제32조에서 확인할 수 있는 사항이다. 다만, 민법상 불법행위책임을 원용하고 있으면서도 정보주체의 권익보장 측면에서 그 입증책임을 전환하여 행위자에게 부담시키고 있음을 특색으로 한다. 원래 입증책임이란 민사소송에 있어서 당사자 사이에서의 증거

101) Karin Nehlsen, *Schmerzensgeld ohne Genugtuung*, in: Juristenzeitung, 1987, S.120ff.

의 배분을 뜻하는 것이 아니라, 입증불능의 경우에 누가 패소하느냐를 말하는 것으로서 권리를 주장하는 자가 부담하는 것이다. 그런데 예외적으로 ① 입증책임을 지는 당사자의 상대방이 원래 가능했던 증거제출을 불가능하게 만든 입증방해의 경우, ② 현저한 직무위반에 해당하는 경우, ③ 제조자책임의 경우, ④ 설명의무위반의 경우 등에서는 권리를 주장하는 자의 상대방으로 입증책임이 전환되며, 결국 이 모든 경우가 신의성실의 원칙으로 되돌아가는 것이다.¹⁰²⁾ 그러므로 위 법 소정의 입증책임 전환은 일종의 제조자책임으로 볼 수 있으며, 이렇게 하는 것이 정보통신서비스제공자 등이 사실상 점하게 되는 상대적 우위에서 정보주체의 권익을 보장함으로써 신의칙에 충실한 소송구조를 확보할 수 있게 하는 입법적 고려로 판단된다.

한편, 공공기관법은 개인정보권의 침해에 대한 구제방법으로 제15조에서 불복청구만을 규정하고 있는바, 즉 “제12조 제1항 및 제14조 제1항의 규정에 의한 청구에 대하여 공공기관의 장이 행한 처분 또는 부작위로 인하여 권리 또는 이익의 침해를 받은 자는 행정심판법이 정하는 바에 따라 행정심판을 청구할 수 있다. 이 경우 국가행정기관 및 지방자치단체 외의 공공기관의 장의 처분 또는 부작위에 대한 재결청은 관계중앙행정기관의 장으로 한다”고 하고 있다. 물론 이 규정이 없다고 해서 일반법인 행정심판법상의 행정심판이 개인정보에 관한 권리침해에 대하여 사후구제로서 이루어질 수 없는 것은 아니며, 다만 공공기관의 개인정보보호에 관하여는 행정심판의 청구를 수리하여 재결할 권한을 가진 행정기관으로 관계중앙행정기관의 장이 당해행정심판청구권에 대하여 법적 판단을 할 수 있는 권한을 보유하고 일정한 경우 신청 또는 직권으로 집행정지결정

102) Walter J. Habscheid 著/호문혁 譯, 입증책임과 입증의 정도, 법학 제32권 제1·2호, 서울대학교 법학연구소, 1991, 124~126쪽.

을 할 수 있도록 규정하고 있는 것이다. 그리하여 행정청이 행하는 구체적 사실에 관한 법집행으로서의 공권력의 행사 또는 거부와 그밖에 이에 준하는 행정작용으로서 처분 등에 관하여 그 공정력을 배제하거나 그 효력유무 또는 존재여부에 대한 확인을 구하거나 행정청의 위법·부당한 거부처분 또는 부작위에 대하여 그 이행을 구하는 객관적 심리·판단의 기회를 열어두고 있다. 하지만 개인정보에 관한 권리침해의 경우 처분의 취소 또는 무효확인이 원상회복이라는 측면에서는 그다지 실익이 없는 것이고 보면 권리구제의 실질적 확보가 요청된다. 환원하자면, 개인정보에 관한 권리침해의 경우 행정심판이 권리구제에 기여하는 것은 당해개인의 자기정보에 관한 권리로서 공공기관의 장이 개인정보를 권한 없이 처리하는 것에 대하여 집행정지를 신청할 수 있도록 하고 그러한 정보처리 공정력을 배제하는 것이나 자기정보의 열람제한 등에 대한 불복 등을 상정할 수 있다. 하지만 이 글에서 다루고자하는 것은 권익보장의 간접적 이행방식이 아니라 침해된 권익, 다시 말해서 정보주체의 정보자기결정권을 회복하여 주거나 그 피해에 대한 정당한 전보를 뜻하는 것이기에 이를 위해서는 사법적 확인을 위한 또 다른 행정상 법제도가 필요하다고 할 것이다.

여기서 공공기관법에 명시하고 있지 않지만 국가배상법 제2조에 따른 국가배상청구가 그 적격을 확보하면 공법상 당사자소송(公法上 當事者訴訟)으로 제기될 수 있다는 점¹⁰³⁾이 권익구제의 실효성에서 중요한 機制로 작용한다. 국가배상법은 행정상 손해배상에 관한 일반법으로서, 국가배상책임에 관하여 이 법의 규정에 의한 것을 제외하고는 민법을 따르지

103) 국가배상법을 공법(公法)으로 이해하는 통설적 견해에 따를 경우 행정법원이 제1심 법원이 되고 그 형식 또한 행정상 당사자소송이 되어야 할 것이다. 그러나 현재까지 실무에서는 관례의 태도에 따라 지방법원에서 민사소송절차에 따라 재판이 진행되고 있다.

만, 그밖에 법률에 다른 규정이 있을 때에는 그 규정에 의하기 때문에 공공기관법에서 규정되지 아니한 행정상 손해배상에 대하여는 국가배상법상의 관련규정이 적용되는 것이다. 위에서 살펴본 행정심판과 행정법 관계에서 당사자간의 법률관계에 관한 분쟁을 법원이 심리·판단하는 행정심판을 포괄하는 행정쟁송의 경우, 개인정보에 관한 권리보호라는 행위규범을 위반한 데 대하여 위법성(illegalis)이 있으므로 위법한 처분을 권한 있는 자가 취소하거나 그 처분의 효력이 없음을 인정토록 하는 것임에 반하여, 국가배상은 타인에게 법이 허용하지 않는 침해를 발생시킨 공행정작용(公行政作用)의 하자로서 권리침해의 불법성(illicitus)에 대하여 공법상의 전보적 손해배상을 부담지우는 것이다. 따라서 “국가 또는 지방자치단체는 공무원이 그 직무를 집행함에 당하여 고의 또는 과실로 법령에 위반하여 타인에게 손해를 가하는 때에는 이 법에 의하여 그 손해를 배상하여야 한다”는 국가배상법 제2조 제1항 본문상의 ‘법령위반’은 침해의 불법인 것이고 이에 따라 통설과 판례에 따라 행정주체로서 국가 또는 공공단체는 불법행위에 대한 自己責任을 지는 것이다.¹⁰⁴⁾ 즉, 직접

104) 다만 그 절차와 관련하여 국가배상법은 제10조 제1항 본문에서 “국가 또는 지방자치단체에 대한 배상신청사건을 심의하기 위하여 법무부에 본부심의회를 둔다”라고 하여 배상심의회의 설치에 대하여 근거를 두고 있다. 그리고 현행법에서는 제9조를 “이 법에 의한 손해배상의 소송은 배상심의회에 배상신청을 하지 아니하고도 이를 제기할 수 있다”라고 규정하고 있지만, 1997년 12월 13일 법률 5433호로 일부개정된 것까지는 “이 법에 의한 손해배상의 소송은 배상심의회의 배상금지급 또는 기각의 결정을 거친 후에 한하여 이를 제기할 수 있다”라고 규정하고 있었다. 그 까닭은 본조에 대한 違憲訴願(헌법재판소 2000. 2.24. 선고 99헌바17·18·19)이 제기되어 국민의 신속한 권리구제를 도모하는 데 대한 사회적 환기가 작용하였기 때문이다. 물론 전원재판부는 “국가배상법에 의한 손해배상청구에 관한 시간, 노력, 비용의 절감을 도모하여 배상사무의 원활을 기하며 피해자로서도 신속, 간편한 절차에 의하여 배상금을 지급받을 수 있도록 하는 한편, 국고손실을 절감하도록 하기 위한 이 사건 법률조항에 의해 달성되는 공익과, 배상절차의 합리성 및 적정성의 정도, 그리고 한편으로는 배상신청을 하는 국민이 감수해야 하는 수고나 시간의 소모를 비교하여볼 때, 이 사건 법률조항이 헌법 제37조의 기본권제한의 한계에 관한 규정을 위배하여 국민의 재판청구권을 침해하는 정도에는 이르지 않는다”라고 하면서 “국가 등의 사경제적 작용에 대해서는 국가배상법이 적용되지 않는 것으

불법행위를 행하는 공무원은 행정주체인 국가 또는 공공단체의 手足에 불과하며 스스로 대외적인 의사표현을 할 수 없고 공법상 법률관계인 권리의무의 귀속주체가 아닌 까닭에 행정주체가 직접 자기책임을 지는 반면,¹⁰⁵⁾ 다만 국가배상법 제2조 제2항의 규정에 의하여 공무원이 고의 또는 중대한 과실이 있는 때에는 그 공무원에게 구상할 수 있는 것이고 이는 국가와 공무원간의 내부적 문제로서 정책적 판단에 따른 것이지 배상책임의 본질과는 무관한 것이다. 결국 국가배상제도의 본질은 행정주체의 자기책임인 것이고, 이로써 정보주체의 권리구제에 실효성이 확보된다.

로 보는 것이 학설과 판례의 일치된 입장이고, 연혁적으로도 세계 각국에서 국가배상책임이 인정되게 된 것은 일반 민사상 손해배상책임이 인정된 것과 그 배경 및 시기를 달리하는 등 국가배상사건은 그 성격에 있어서 일반 민간인, 민간단체를 상대로 하는 손해배상청구사건과는 다르므로 이 사건 법률조항이 국가나 지방자치단체를 상대로 하는 국가배상법 제2조, 제5조에 의한 손해배상소송을 제기하기 위해서는 배상결정을 필요적으로 거치도록 규정하였다고 하더라도 이를 가리켜 본질적으로 같은 것을 자의적으로 다르게 취급함으로써 국민의 평등권을 침해하는 것이라고는 할 수 없다”라고 실시하였지만, 배상심의회에 배상신청을 하지 않고도 바로 국가배상청구소송을 제기할 수 있도록 2000년 12월 29일 법률 6310호로 일부개정하였던 것이다.

- 105) 이에 대하여 代位責任說은 過失責任主義의 논리귀결상 불법행위는 단체로서의 기관이 아닌 개인에 의해 발생할 수밖에 없으며, 위법행위는 이미 국가의 기관행위로서의 품격을 상실하였기 때문에 국가의 행위로 보기 어렵고 배상책임의 본질은 공무원 개인의 불법행위책임으로 보아야 한다고 주장한다. 다만 전보력이 부족한 공무원 개인에게 모든 책임을 부담지울 경우 피해자가 손해를 입증하고서도 배상을 받지 못하는 경우가 속출할 수 있으며 공무원 개인에게도 가혹하므로, 피해자인 국민을 두텁게 보호하기 위해 賠償資力이 있는 국가가 공무원 개인의 책임을 대위인수한 것으로 이해한다. 하지만 이는 우리 헌법 제29조 제1항이 “공무원의 직무상 불법행위로 손해를 받은 국민은 법률이 정하는 바에 의하여 국가 또는 공공단체에 정당한 배상을 청구할 수 있다”라고 규정하여 행정주체에 대한 배상책임을 헌법이념상 부과하고 있음을 부정하는 결과에 이르게 한다.

제2절 입법적 현황

1. 쟁점제도의 동향

(1) 집단소송의 제도적 법리와 검토

집단소송제도는 불특정다수인의 권리구제를 간이·신속한 집단적 소송 절차에 의하여 통일적으로 해결함으로써 집단민원을 사법적으로 처리하여 공익을 증진하는 것을 목적으로 하는 제도이다.¹⁰⁶⁾ 즉, 집단소송은 공통의 이익을 가진 집단의 구성원을 위하여 제소(提訴)하거나 피소(被訴)될 수 있는 소송형태로서, 미국의 경우에는 class action(대표당사자소송)이란 명칭으로, 독일의 경우에는 Verbandsklage(단체소송)이란 명칭으로 사용되고 있다. 집단소송은 다음과 같은 측면에서 그 장점을 보유하고 있다.

첫째, 원고의 입장에서는 다수의 소액피해자에 대한 유용한 구제수단이 된다는 점을 들 수 있다. 개별적으로 너무 소액이어서 소송수행의 경제성이 없는 경우나 피해를 입은 자가 정신적·육체적으로 무능력상태에 있거나 법적 권리에 대한 무지로 소송을 통한 권리주장이 막혀 있는 경우에 집단소송이 유용하기 때문이다.¹⁰⁷⁾ 집단소송에 있어서는 대표당사자가 개별소송에서의 당사자보다 더 강력한 지위를 확보할 가능성이 있어 피고로 하여금 화해나 합의에 이르도록 하여 조기에 분쟁해결이 가능

106) 김대휘, 집단적 소송에 관한 법률의 제정방향, 집단소송의 법리, 법무자료 제 149집, 법무부, 1991, 160쪽.

107) James D. Cox, *Making Securities Fraud Class Actions Virtuous*, 39 Arizona Law Review 497, 514-515 (1997).

하도록 하는 기능이 있고, 변호사로서는 개별소송보다 집단소송에서 보다 많은 수임료를 받을 수 있는 반면 집단구성원은 소송비용을 분산시킬 수 있으며,¹⁰⁸⁾ 주장내용을 입증할 증거의 폭이 개별소송에서보다 광범위하다고 할 수 있을 뿐만 아니라, 개별소송에서와 같이 청구가 구체적이지 않고 추상적이어서 기각되는 현상 및 소송중에 당사자적격(當事者適格)에 흠결이 발생하는 사정변경에 대해 충분히 대처할 수 있다는 장점이 있다.

둘째, 피고의 입장에서 집단소송에서는 개별소송에 대하여 각각 응소(應訴)하여야 하는 시간적·비용적 손실을 절감할 수 있고, 집단의 대표당사자와 단일 협상창구를 열어 화해나 합의를 성립시킬 수 있는 장점이 있다. 미국의 예를 보면, 손해배상을 청구하는 집단소송의 많은 경우에 대표당사자와 피고간 합의하에 금전배상에 대신하여 대물배상을 하거나, 채권증서로 환급하거나, 장래 구매시 할인쿠폰을 제공하거나 하는 등 집단소송의 장점을 활용하고 있다. 한편으로는 피고가 책임져야 할 전체금액을 산정할 수 있다는 점에서 여러 개별소송이 이루어지는 것보다 유용하다고 할 것이다.

셋째, 사회적인 관점에서 볼 때 집단소송은 중복적인 다수의 개별소송을 방지할 수 있고, 통일적 판결을 통하여 사법행정의 효율성을 제고할 수 있으며, 특히 장래에 있어 계쟁사건과 유사한 위법행위를 예방하는 효과를 갖는다는 장점을 지닌다. 또한 집단소송이 제기됨으로 인하여 일

108) 집단소송은 단순히 집단의 이익을 대변하여 대표자가 소송을 수행한다는 점뿐만 아니라 소송수행(litigation)의 핵심이 당사자가 아닌 유능한 변호사에게로 이전되고 손해배상의 액수보다는 변호사의 보수로 그리고 소송수행보다는 합의(settlement)로 그 중요성이 이전된다는 특성이 있다; Stephen C. Yeazell, *Civil Procedure*, Aspen Publishers Inc., 1996, p.966.

반대증의 관심이 집중되고 나아가 관련쟁점을 개선하기 위한 조직화된 시민단체의 출현을 기대할 수도 있을 것이다.

이와 같은 장점을 보유한 집단소송을 제도적으로 확립하고 있는 미국과 독일의 상황을 살펴보면 다음과 같다. 우선 미국의 대표당사자소송제도는 판결에 의하여 영향을 받는 자가 지나치게 많은 경우에 전원을 당사자로 하는 것이 불가능하거나 적어도 실제적이 아닌 경우에 판결에 영향을 받는 자의 모두를 하나의 집단에 속하게 하고, 신청된 구제절차에 이들이 공동의 이익을 가지거나 개개의 이익이 공통의 성질을 지닌 것이고 당사자로 된 자가 공동이익을 적절하게 대표하고 있는 경우에는 당사자 이외의 자를 소송절차에 참가시키지 아니하더라도 절차를 진행시킬 수 있도록 하여 당사자 이외의 자를 이 소송의 종국판결(終局判決)에 구속되도록 하는 제도이다.¹⁰⁹⁾ 이 제도는 당초 영국의 형평법(衡平法; equity)법원이 창설한 제도로서, 종래의 필요적 공동당사자의 원칙(a compulsory joinder rule)을 수정하여 소송경제의 추구라는 취지에서 중복된 분쟁을 단일소송으로 진행케 하는 집단적인 소송제도(group litigation)를 도입하여 뉴욕·캘리포니아 등 몇몇 주(州) 입법을 거쳐 1937년 연방민사소송규칙(聯邦民事訴訟規則; Federal Rules of Civil Procedure; FRCP) 제23조로 입법화함으로써 인정되기에 이르렀다. 미국의 연방민사소송규칙 제23조는 1966년 전면개정되어 그 요건을 상세히 규정하고 있으며, 대표당사자소송제도는 독점규제 내지 불공정거래에 관한 소송, 환경소송, 인종차별소송, 증권소송, 소비자보호와 관련 소송 등에서 널리 활용되고 있다.¹¹⁰⁾ 이는 대표당사자소송이 집단적인 손해배상

109) Jack H. Friedenthal et al., *Civil Procedure: Cases and Materials*, West Publishing Co., 2001, p.713.

110) 미국의 대표당사자소송에 관하여는 강태원, 미국 대표당사자소송의 최근동향에 대하여, 비교사법 제8권 제2호, 한국비교사법학회, 2001, 1007~1037쪽 참조.

청구에 적합하다는 기능적 장점에 기인한 것으로, 그 활용은 미국 민주주의발전에 크게 기여했다.¹¹¹⁾

한편 독일의 경우에는 1896년 부정경쟁방지법(Gesetz zur Bekämpfung des unlauteren Wettbewerbs: UWG)에서 일정단체에 유지소송(留止訴訟)을 제기할 수 있도록 한 것이 단체소송의 효시라고 할 수 있으며, 1965년 부정경쟁방지법(Gesetz gegen den unlauteren Wettbewerb)에서 소비자단체에도 제소권을 인정함으로써 이른바 사익적(私益的) 단체소송에서 공익적(公益的) 단체소송으로 전환하기에 이르렀다. 여기서 공익적 단체소송이라 함은 단체 자신 및 단체구성원의 이익을 보호하는 것을 목적으로 하는 사익적 단체소송과는 달리 소비자단체의 소비자보호와 같이 불특정 다수의 이익을 보호하는 것을 목적으로 하는 단체소송 형태를 의미한다.¹¹²⁾ 환원하자면, 구성원의 이익과 관계없이 공익의 실현을 위하여 단체에게 원고적격을 인정하는 것으로서 법적으로 보호되는 이익을 공동으로 보유하는 집단을 상정하고는 이러한 집단적 이익의 보호를 그 임무로 삼는 소비자단체 등은 그 이익이 침해되는 경우에 이익보호를 위하여 원고적격을 갖는 것이다. 이후 1976년에 개정된 보통거래약관규제법(Gesetz zur Regelung des Rechts der allgemeinen Geschäftsbedingungen: AGBG)에서는 이 법에 위배되는 거래약관의 사용금지청구권 및 해약청구권을 인정하는 반면 계약상대방 개개인의 제소권은 부인하는 규정이 추가되었다. 독일에서의 단체소송은 주로 불공정한 거래행위, 위협하거나

111) 박민영, 미국 Class Action제도의 현황과 문제점, 집단소송의 법리, 법무자료 제149집, 법무부, 1991, 227쪽.

112) 단체소송을 공법적 또는 사법적 영역으로 구분하는 견해는 단체소송의 성격 자체를 규명하기보다는 이 제도가 존재한다는 것을 간접적으로 설명해주는 이론이라 할 수 있으며, 단체소송을 경쟁법이 중시하는 공공복리의 측면을 중시하여 공법과 사법의 중간적 영역으로 분류하는 학설도 있다; Peter Reinel, *Die Verbandsklage nach dem AGBG*, Heymann, 1979, S.124.

불량한 제조물, 소비자에게 불리한 약관 등에 대하여 특정한 영업자단체나 소비자단체에게 원고적격을 인정하고 있는데, 금지청구의 형식을 주로 하여 인정된다고 할 수 있고¹¹³⁾ 어떤 범위의 단체에게 어떤 종류의 제소권을 인정할 것인지에 대해서는 개별특별법에서 규정하고 있다. 오늘날에 있어서는 미국과 마찬가지로 독일에서도 환경보호, 자연보호 등 공법적 분야에 있어서도 단체소송제도의 도입이 활발히 논의되고 있다.¹¹⁴⁾

미국의 대표당사자소송과 독일의 단체소송을 상호비교하면 다음과 같이 정리할 수 있다.

첫째, 법적 근거의 상이성을 들 수 있다. 다시 말해서 미국의 경우 연방민사소송규칙 제23조 및 각주(各州) 대표당사자소송규정과 같은 독립적이며 일반적인 법적 근거를 통해 집단적인 소송이 광범위하게 적용되고 있는 반면, 독일은 각 분야마다 실체법인 부정경쟁방지법 및 보통거래약관규제법 등 개별규칙으로 단체소송을 인정하고 있다는 점에서 근본적인 법리적 차이가 야기되는 것이다. 그러므로 독일의 경우에는 개별적 실체법에 단체소송을 인정하는 특별규칙이 존재하지 않는 한, 위와 같은 계쟁사건인 집단피해는 일반적인 민사소송절차를 통해 피해구제를 받아야 한다.

둘째, 절차적 집해과정에서의 차이점을 들 수 있다. 우선 미국에서는 사법적 정의의 실현을 위한 절차적 집행을 원칙적으로 법원에 일임하고

113) 1986년에 개정된 부정경쟁방지법에서는 소비자단체에게 제한된 범위 내에서 손해배상청구를 허용하고 있다.

114) Walther J. Habscheid, *Effektiver Rechtsschutz und verfassungsmäßige Ordnung*, Internationalen Kongreß für Prozeßrecht, Würzburg 1983, S.128.

있으며 법원에 의하여 해결되어야 할 분쟁과 그렇지 못한 분쟁에 대한 구별에 있어서도 법원의 개별적·구체적인 판단에 맡기고 있는 반면, 독일에서는 법원에 의하여 해결되어야 할 사건과 그렇지 못한 것으로 판단되어질만한 사건을 입법적으로 구별하고 있다. 또한 미국에서는 소송비용이나 변호사비용이 상당한 고액(高額)인 까닭에서 상당한 소제기(訴提起)의 제한이 사실상 이루어지고 있는 반면, 독일에서는 그와 같은 사실상의 제한이 없는 까닭에 먼저 제소권자(提訴權者)를 제한하여 남소(濫訴)를 방지하고 제소권(提訴權)이 부여된 자에 대하여는 경제적인 원조 등 절차적인 급부를 통하여 소송활동을 활발하게 진행시키려 한다.¹¹⁵⁾ 따라서 미국에서는 개인이 중심이 되어 개인의 이익실현을 주된 목적으로 하는 대표당사자소송이 발달하였으나, 독일에서는 공공의 이익실현을 주된 목적으로 하는 단체소송이 발달한 것이다.

셋째, 당사자적격에서 드러나는 구별징표가 있다. 즉 미국의 대표당사자소송은 동일한 이해관계를 가지고 있는 다수인이 존재하는 경우 그 중 1인 또는 수인이 대표자가 되어 그 집단의 구성원전원을 위하여 소송을 제기하는 데 반하여, 독일의 단체소송은 특정한 목적을 가지고 활동하는 단체가 그 구성원의 이익을 위해서 소송을 제기하는 것이 아니라 공공의 이익 또는 다른 사람의 이익을 위해 제소하는 것이다. 따라서 전자(前者)에서는 원칙적으로 개별적인 피해구제, 특히 소액다수피해자에게 제소권을 부여하고 있는 한편, 당사자적격에 있어서 법원의 자유재량이 주어져 사안에 따라 유연하게 대처할 수 있다. 그러나 후자(後者)에서는 소송법의 원리인 당사자처분주의와 변론주의를 유지하는 한 이를 기대하기 어렵

115) 이는 기본적으로 개인주의적이고 사법부중심의 법문화를 지닌 미국의 상황과 단체주의적이고 입법부중심의 법문화를 지닌 독일의 상황의 구별에서 비롯된 것이다; 권오승, 소비자보호와 단체소송, 인권과정의 통권 제179호, 대한변호사협회, 1991, 27쪽.

다.¹¹⁶⁾

넷째, 소송형식과 관련하여 양자의 구별이 뚜렷하다. 우선 미국의 대표 당사자소송은 소송형식에 대한 제한은 없으나 주로 소액다수의 손해배상 청구소송으로 개별적인 피해에 대하여 사후적인 구제를 주목적으로 하고 있음에 비하여, 소비자소송·환경소송을 포괄하는 독일의 단체소송은 주로 금지청구소송으로 부정경쟁행위의 방지나 무효인 약관의 사용금지 등에서 볼 수 있는 법규보호의 목적을 실현하기 위한 것으로 이해된다.¹¹⁷⁾ 따라서 전자가 주로 이미 발생한 손해에 대한 사후구제를 위해 활용되고 있는 것과 달리, 후자는 주로 위반행위의 방지를 통한 손해발생의 금지 또는 사전예방을 위해 활용되고 있는 실정에 있다.

다섯째, 손해배상금의 분배에 있어서의 이질적인 사항을 지적할 수 있다. 미국 대표당사자소송의 경우 대체로 통제를 두지 않는 사회적·법제적 구조에 비추어 그 제한방안을 모색하는 데 관심을 집중하는 경향을 보이는 반면, 독일 단체소송의 경우 계산서작성의무를 부과하고 이를 제대로 이행하지 않으면 제소능력을 박탈할 수 있기에 그 제한이 어렵지 않다.¹¹⁸⁾

우리나라에서 그 도입논의가 제기되어 온 집단소송에 대하여는 법무부

116) 다만 정관과 종래의 활동을 기초로 당사자적격을 심사하는 것은 수월하면서도 안전성이 보장된다는 장점이 있지만 이를 확보하는 대신 단체소송의 운영이 경직되고 획일화되는 문제점이 발생할 수 있다; 함영진, 집단소송에 관한 연구, 고려대학교 박사학위 청구논문, 1997, 104쪽.

117) 이시윤, 민사소송법, 박영사, 2000, 214~215쪽.

118) 따라서 독일에서는 단체소송의 예외적 측면을 중시하여 지나치게 이를 제한하고 있는 실정이며, 특히 소비자단체소송의 경우에는 그 활성화를 모색하여야 할 형편에 놓여 있다고 봄이 타당할 것이다.

에서 오랜 기간 동안 심혈을 기울여 1996년 집단분쟁을 처리하기 위한 시안을 마련한 바 있으나, 그 시행상의 문제점을 들어 입법을 중지한 예가 있다. 이후 시민사회단체가 연대하여 입법청원안으로 집단소송법안을 작성하여 이에 관한 토론회가 개최되었으나, 그마저도 전면적 도입에 대한 시기상조론 및 현행법체계와의 부조화설에 휩싸여 즉각적인 입법조치로 연결되지 못했었다. 여기서 제기된 문제점은 집단소송이 지닌 다음과 같은 일반적인 문제점에 연유하기도 한 것이다.¹¹⁹⁾

첫째, 원고측의 입장에서 제기되는 문제점이다. 이는 집단소송은 대표당사자가 집단전원의 이익보호를 최우선의 과제로 삼고 있기 때문에 개별소송에서 나타나는 소송중의 화해라든가 소장의 변경이 용이하지 않다는 점이 그것이다. 또한 집단소송의 당사자는 개인이 아닌 집단으로 이루어

119) 다만 법무부에서는 미국의 대표당사자소송과 독일의 단체소송을 우리 실정에 맞게 변형해 만든 증권관련집단소송법안을 국회에 상정하고 2001년 11월 7일 입법예고하였으며, 2004년 1월 20일 법률 제7074호로 제정하여 2005년 1월 1일부터 시행해오고 있다. ‘유가증권의 거래과정에서 발생한 집단적인 피해를 효율적으로 구제하고 이를 통하여 기업의 경영투명성을 높이기 위하여 증권관련 집단소송에 관하여 민사소송법에 대한 특례를 정하는 것을 목적으로’ 입안된 증권관련집단소송법안 소정의 증권관련집단소송이란 유가증권의 매매 그 밖의 거래과정에서 다수인에게 피해가 발생한 경우 그중의 1인 또는 수인이 법원의 허가를 받아 총원을 위하여 소송절차를 수행하는 구성원인 대표당사자가 되어 수행하는 손해배상청구소송을 말한다. 이 법은 제3조에서 그 적용범위를 명시하여 열거주의를 채택하고 있으며, 제6조에서는 이 법에 특별한 규정이 없는 경우에는 민사소송법을 적용하도록 규정함으로써 증권관련분쟁이라는 개별영역에 대한 민사소송법의 특별법임을 분명히 하고 있다. 그런데 집단소송은 당해구성원의 명시적인 위임 없이도 그 구성원을 위하여 소송을 제기하고 그가 소송결과에 구속되도록 한다는 점에서 개개인 구성원의 재판을 받을 권리를 침해하는 위헌소지를 갖고 있다고 보는 견해가 있으나, 다수인에게 피해가 발생한 경우 그 손해의 보전에 있어서 공통의 이해관계를 가지는 피해자 전원을 구성하는 각각의 피해자로서 구성원이 보장받아야 할 자기결정권과 절차참여권을 부여한다면 이러한 특질이 반드시 국민의 재판청구권을 침해하는 것으로 볼 수 없을 뿐만 아니라 통상적으로는 집단소송의 제기 前 당해판결주문의 기판력으로부터의 배제신청이 가능하므로 재판청구권을 침해하는 것으로 비판하는 것은 적절하지 못하다고 할 것이다.

여기 때문에 소송전략상의 공격·방어가 상대방에게 쉽게 노출될 가능성이 있다.

둘째, 피고측의 입장에서 제기되는 문제점이다. 이는 집단소송은 개별 소송에서는 큰 부담이 되지 않는 청구가 집단소송에서는 소액다수청구(少額多數請求)가 인정될 수 있기 때문에 이행 및 배상 등의 책임이 막대하다는 점이다.

셋째, 사회적 측면에서 제기되는 문제점이다. 주로 판결의 대세적 효력(對世的 效力)으로 인해 소송에서 패소(敗訴)한 자는 전멸하는 가혹한 결과가 발생하며, 경우에 따라서는 소액다수의 청구가 집단소송의 남발로 이어져 결국 상거래를 위축시키는 결과를 가져올 수도 있다는 점을 든다.¹²⁰⁾

그럼에도 불구하고 현행 민사소송법상으로도 각자가 개별적으로 제기한 소(訴)를 법원이 재량으로 병합심리할 수 있는 병합심리제도도 있고(법 제131조), 피해자가 공동으로 제소하여 하나의 절차로 권리를 실현할 수 있는 공동소송제도도 있으며(법 제61조), 공동의 이익을 가지는 피해자가 다수 있는 경우 다른 피해자로부터 수권(授權)을 받아 소송수행권이 주어진 자가 제소하여 그 판결의 효과가 수권한 다른 피해자에게 미치는 선정당사자제도(법 제49조)도 존재하는바, 이들 가운데 피해자 각자가 별도로 소를 제기하지 아니하고 선정된 피해자만이 당사자가 되어 하나의 소송에서 모든 피해자가 그 목적을 달성할 수 있는 선정당사자제도는 집단적 일괄처리에 적당하다고 할 수 있다는 점에 유념할 필요가 있다. 그

120) 하지만 집단소송의 경우 사전에 법원의 허가를 얻어야만 활용될 수 있는 제도이기에濫訴의 우려는 과장된 것으로 여겨진다.

리고 개별적인 수권을 필요로 한다는 점에서 연락이 닿는 범위내의 피해자에 한정되고 그렇지 않는 자를 위해서는 소송을 수행할 수 없으며 각 피해자가 선정자로 참여하여 소송비용을 분담하여야 하는 단점이 있으므로 선정당사자제도에 의해서는 가령 환경이나 제조물책임에 관한 분쟁 등 당사자의 수는 많지만 개별피해액은 소액인 경우가 많은 분쟁에 효과적으로 대처할 수 없지만, 정보사회에서 주목받고 있는 인터넷 등 정보기술(IT)을 활용하여 피해자들로부터 제소수권절차(提訴授權節次), 선정당사자선임절차(選定當事者選任節次) 그리고 제소후 참여요건(提訴後 參與要件) 및 절차 등을 보완할 경우 현대적 의미의 분쟁에 대응하는 빠르고 간편한 권리구제절차로 변모하도록 할 수 있을 것이란 지적은 주목할 필요가 있다.¹²¹⁾

앞서 살펴본 미국의 대표당사자소송제도와 독일의 단체소송제도를 통해 우리가 취해야 할 방향은 ① 집단소송의 형태를 독일식 제도와 미국식제도를 절충하여 장점을 살리고 단점을 보완하는 것, ② 우선 민사소송 분야 특히 소비자보호의 분야에서 집단소송을 인정하고 추후에 행정소송 분야에까지 확대하는 단계적 절차를 거치는 것, ③ 현행 민사소송법의 구조를 크게 벗어나지 않는 범위에서 특칙을 두어 집단소송이 지니는 공익적 측면을 살리는 것 등으로 압축할 수 있을 것이다. 이러한 설정은 위 요건을 모두 충족하는 범위에서 구체화되어야 할 것이고 증권관련집단소송법은 이들 제반사정을 고려하여 제정된 것으로 평가할 수 있을 것이다. 산업계의 저항에도 불구하고 개별영역에서 적용될 적절한 법리를 집대성하였기 때문이다.

121) 물론 이와 같은 논의는 디지털시대에 부합하는 電子的 司法行政 構築方案과 접목하여 다루어져야 할 것이다.

그렇다고 해서 집단소송에 관한 일반법의 제정을 선불리 찬성할 수만은 없는 게 현실이다. 증권관련집단소송법의 시행이 있기까지 불거졌던 논란 역시 이를 강변할 수 있는 것이지만, 무엇보다 위 요건을 충족하는 것은 개별영역보다 더 많은 변수가 존재하고 그 정합성을 따지기에 난점이 있는 손해배상청구소송의 일반론적 접근에서 더 어렵기 때문이다. 그러므로 미국식제도를 따를 것인지 아니면 독일식제도를 따를 것인지 그리고 이를 어떻게 다른 방식으로 보완하는 문제가 관건이 되며, 이는 오히려 이론적인 사안이라기보다는 정책적이면서도 법감정에 충실한 것이기 때문에 독일법을 계수한 우리 실정으로는 단체소송제도에 당연한 귀결을 내놓게 되는 우를 범할 수 있는 것이다. 개별영역에서 보면 소비자보호에 관한 것일 경우 집단소송은 무엇보다 소액소수의 피해자를 보호할 수 있도록 특정단체를 당사자로 허가할 수 있는 독일식 단체소송으로 갖추어지는 것이 중요하겠지만, 개인정보에 관한 손해배상청구의 경우에는 그것이 일의적으로 소비자보호에 관한 사항이라고 단언하기 어렵다. 물론 이것으로 개인정보보호와 소비자보호의 의미상 엄밀한 구별을 환기시키려는 의도는 아니지만,¹²²⁾ 국가배상청구소송이라는 공법상 당사자소송이 적용되는 부분과 민법상 불법행위책임으로서 손해배상청구소송이 상치하는 이 영역에서 소비자보호라는 축으로 인해 어느 하나, 즉 공법분야에 대한 논의를 불식시키는 것은 또 다른 문제를 야기한다. 개인정보권의 침해에 관한 국가배상청구소송의 경우 국가배상법 제2조 소정의 고의불법행위책임에 따른 손해배상 및 같은 법 제5조 소정의 영조물책임에 따른 손해배상이 모두 검토되어야 하며, 이에 대한 특례가 되는 집단소송 제도가 이루어져야 할 것이기 때문이다. 그러므로 이에 관한 문제는 개

122) 개인정보보호가 우리 헌법상 제10조 및 제17조 등을 통해 인정되는 정보자기 결정권의 표상임에 반하여, 소비자보호는 헌법의 일반원리에서 인정되는 계약상의 당사자권임을 고려할 때 개념적 구별은 존치하는 것이다.

인정보보호에 관한 총괄기구에서 행하는 절차와 상관성을 보유하도록 보호기구설립논의와 함께 이루어져야 한다.

개인정보에 관한 집단소송을 제도적으로 수용하기에는 민사소송법의 특례를 법상 규정할 여백이 충분하여야 할 것인바, 이를 위해서는 우선 개인정보보호에 관한 총괄기구를 설치하고 그 운영에 대하여 다루는 내용으로 관련법안을 조율하여 국회본회의를 거치게 하여 보호기구를 발족시킨 연후에 그 조사·연구·분석에 따른 전문화된 검증을 통해 분쟁조정 의 적정화 및 집단소송의 제도화를 개별법으로 구체화하는 과정을 밟게 하는 것이 타당할 것이라 생각한다. 기실 개인정보에 관한 집단소송이 수액다수피해자인 정보주체의 권리보장에 크게 이바지할 것이지만, 그 제도적 수용을 둘러싼 문제는 간단하지도 그렇다고 이론적인 법리공방으로만 치달지도 않는 사항이기 때문이다.

(2) 징벌적 손해배상의 법리와 검토

영미법상(英美法上) 불법행위로 인한 손해배상에 관한 체계는 크게 전보적 손해배상(填補的 損害賠償; compensatory damages), 명목적 손해배상(名目的 損害賠償; nominal damages), 징벌적 손해배상(懲罰的 損害賠償; punitive damages) 등으로 분류할 수 있는바,¹²³⁾ 징벌적 손해배상이란 가해자가 불법행위를 행함에 있어 악의적(惡意的)인 경우에 인정되는 배상제도이다.¹²⁴⁾ 이는 고의불법행위(故意不法行爲)를 범한 가해자를 처

123) 이는 실질적 손해배상(實質的 損害賠償; substantial or ordinary damages), 명목적 손해배상(名目的 損害賠償; nominal damages), 모욕적 손해배상(侮辱的 損害賠償; contemptuous damages), 징벌적 손해배상(懲罰的 損害賠償; exemplary or punitive or vindictive damages) 등으로 분류되기도 한다; James A. Henderson, Richard N. Pearson, & John A. Siliciano, *The Torts Process*, Aspen Publishers Inc., 2003, p.5

벌(處罰; punishment)하고 장래에 그와 유사한 행위를 못하게 억제(抑制; repression)하기 위하여 전보적 손해배상에 부과하는 손해배상으로서, 가해자의 비행(非行; wrongful act)으로 발생한 손실을 피해자에게 단지 전보(填補; recompense)할 뿐만 아니라 본보기로(in an exemplary) 가해자를 처벌하며 고의(故意)의 또는 과실(過失)의 가해자를 구별하기 위한 것이다. 미국의 불법행위법 재편찬(再編纂; Second Restatement of Torts) 제908조에서는 이에 대하여 ① 전보적 또는 명목적 손해배상과는 달리 무법행위(無法行爲; outrageous conduct)를 한 자를 처벌하고 장래에 당해 가해자 또는 다른 행위자가 그와 유사한 행위를 하지 못하도록 억제하기 위한, ② 타인의 권리에 대한 피고(defendant)의 악의(evil-motive) 또는 무모한 무관심(reckless indifference)을 이유로 무법행위에 대한 손해배상으로 정의하면서 ③ 징벌적 손해배상의 산정에 있어서 사실심리인(trier of fact)은 행위의 성격 및 원고(plaintiff)에게 생긴 손해 또는 원고에게 가하고자 의도되었던 손해의 성격과 범위 및 피고의 재산에 관하여 고려할 수 있도록 규정하고 있다.

이러한 징벌적 손해배상의 목적은 불법행위자의 처벌 내지 행위의 억제에 있으므로 단순히 처벌 내지 억제라는 측면에서 보면 형벌적 성격이 농후하다고 할 수 있겠으나, 징벌적 손해배상에 있어서는 가해자가 손해배상금을 국가에 지급하는 것이 아니라 피해자개인에게 지급하며 민사소송법에 의한 절차에 의하여 부과한다는 점에서 형벌과는 구별된다. 따라서 불법행위자가 동일한 행위로 인하여 형벌을 받았을 경우 손해배상금의 산정에 있어서 참작사유는 되겠지만 징벌적 손해배상의 인정 여부는 영향을 미치지 않으며, 징벌적 손해배상이 부과되었다고 하여 형벌이 면제되는 것도 아니다. 그 용법상 현재에는 징벌적(punitive) 또는 훈계적

124) Steven L. Emanuel, *Torts*, Aspen Publishers Inc., 2002, p.11.

(exemplary) 손해배상이라는 표현이 일반적으로 사용되고 있지만, 종래에는 복수적(復讐的; vindictive)·형벌적(刑罰的; penal)·가중적(加重的; aggravated)·응보적(報復的; retributory) 손해배상 또는 횡재금(橫財金; smart money)등의 용어가 혼용되었다고 한다.¹²⁵⁾

고대법(古代法)에서의 배수적 손해배상(倍數的 損害賠償; multiple damages)은 대다수의 법제도에서 찾아볼 수 있는 일반적인 특징이며, 이는 법으로 피해자가 실질적으로 입은 손해액의 몇 배를 배상받을 수 있게 인정하는 것이므로 일종의 징벌적 손해배상이라 할 수 있다.¹²⁶⁾ 이러한 규정은 기원전 2000년 함무라비법전(the code of Hammurabi)이 최초의 것으로 알려져 있으며, 특히 절도·간통 등의 경우에 이를 인정하는 모세율법의 헤브라이법전(the Hebrew Covenant Code of Mosaic Law)을 통해서 성서에도 인용되어 있다. 한편 로마에서는 고의행위 가운데 극히 악질이라고 여겨지는, 가령 강박(強迫; duress) 또는 準不法行爲(준불법행위; quasi ex delicto)의 경우 실제손해에 일정비율을 곱한 액수의 배상금이 부과되었다.

한편 영국에서도 일정배액의 배상이 13세기 이후 보통법(common law)상 인정되어 오고 있었지만, 징벌적 손해배상이 보통법에 수용된 것은 18세기 Wilkes v. Wood 사건판결¹²⁷⁾이 시초였고 이후 Huckle v. Money 사건판결¹²⁸⁾ 및 Benson V. Frederick 사건판결¹²⁹⁾에서 재확인되었다. 이렇게 하여 미국 수정헌법 제4조에도 영향을 미친 징벌적 손해배상제도는

125) Samuel Freifield, *The Rationale of punitive Damages*, 1 Ohio St. L. J. 5, 5-6 (1935).

126) Melvin M. Belli, *Punitive Damages; their history, their use and their worth in present-day society*, 49 UMCK. L. Rev. 1, 2-3 (1980).

127) (1763) Loff. 1, 98 Eng. Rep. 489.

128) (1763) 2 Wils. K. B. 205. 95 Eng. Rep. 768.

129) (1766) 3 Burr. 1845, 97 Eng. Rep. 1130.

1964년 *Rookes v. Barnard* 사건판결¹³⁰⁾을 계기로 오늘날과 같은 제도로 확립되었다. 하지만 이 사건에서 귀족원(House of Lords)은 징벌적 손해배상이 그 이론적 근거 자체에 문제가 있으므로 이는 극히 한정된 범위에서만 인정될 것이라고 판결하였다.¹³¹⁾ 이 사건에서 확립된 원칙은 이후 1972년의 *Cassell Co., Ltd. v. Broome* 사건판결에서 재확인되어 1982년의 *Taylor v. Beers* 사건판결 등 다른 사건에도 적용되어 오고 있다.

그리고 미국은 영국의 보통법상 판례를 도입하여 1784년에 징벌적 손해배상을 인정하는 판결¹³²⁾을 하였고, 이후 급속도로 확장되어 1852년에는 최초로 제조물책임에 대하여도 징벌적 손해배상을 인정하기에 이르렀다. 이후 1935년까지 징벌원리를 정당화시키는 선례에 구속되어 여러 형태의 징벌적 손해배상이 채택되었다.¹³³⁾ 그리고 징벌원리가 인정된 항소법원(court of appeal)의 판결이 있었는데, 대표적으로 *Ryder* 사건판결¹³⁴⁾ 및 *Settle* 사건판결¹³⁵⁾ 등이 거론된다.¹³⁶⁾

130) House of Lords (1964) A. C. 1129, 1 All E. R. 367.

131) *Rookes v. Barnard* 사건의 재판장 Devlin卿은 판결의견에서 “예외적으로 인정되는 징벌적 손해배상은 당연히 폐지되어야 할 것이지만, 판례법과 제정법에서 징벌적 손해배상을 인정하고 있으므로 이에 구속을 받지 않을 수 없다”라고 하였다. 그리하여 그는 결론적으로 징벌적 손해배상은 법적 집행력이 옹호되어야 할 경우와 논리상으로는 당연히 형벌에 의할 원칙을 민사법에 적용하는 것이 실제적으로 타당하다고 할 수 있는 경우에 한하여 한정적으로 인정된다고 주장하였다; See Tony Weir, *A Casebook on Tort*, Sweet & Maxwell, 2004, pp.295~299.

132) *Genay v. Norris*, 1s. C. L. (1 Bay.) 6. (1784).

133) 山口正久, 美國の製造物責任訴訟と懲罰的損害賠償(上), NBL 第281号, 1983, 15面.

134) *Loudon v. Ryder* (1953) 2 Q. B. 202.

135) *Williams v. Settle* (1960) 1 W. L. R. 1072.

136) 이들 판결의 사실관계 및 법적 판단에 대하여는 송홍섭, 미국의 징벌적 손해배상제도 개관, 재판자료 58집, 법원행정처, 1992, 515쪽 이하 참조.

징벌적 손해배상의 성립요건을 분설하면 다음과 같다.

첫째, 가해행위의 악성이 존재하여야 한다. 징벌적 손해배상의 주된 목적은 가해행위의 억제 및 가해행위에 대한 제재로 보는 것이 통설이며,¹³⁷⁾ 그 준형벌적(準刑罰的)인 성격으로 인해 단순히 가해자에게 과실이 있었다는 것만으로는 징벌적 손해배상을 부과할 수 없다. 따라서 일반적으로 범죄의 성립요건에서 요구하는 요소와 유사하게 무법(無法; outrageousness) 또는 타인의 권리에 대한 무모한 무배려(reckless indifference)에 따른 가해행위가 있었음을 요건으로 한다. 이러한 가해행위의 악성(惡性)은 사악한 동기(evil-motive), 악의에 찬(malicious) 혹은 의도적인 무법(intentional or willful wanton), 극악한(flagrant)·무신경적인(callous)·의식적인(conscious) 무시 등 여러 가지 용어로 사용되고 있다.¹³⁸⁾ 즉, 징벌적 손해배상의 부과에 있어서는 불법행위가 고의적이었던 것이 결정적인 요건이다. 이러한 고의는 행위의 동기, 불법행위의 본래적인 성질 및 결과를 악화시킨 행위의 강압성 등에 의해 나타나게 된다. 또한 사기적인 목적에서 행하였든지 다른 사람의 권리를 고의적으로 무시하였다고 할 정도의 방종이나 부주의가 있었던 경우에도 징벌적 손해배상은 인정될 것이다. 중과실(gross negligence)의 경우 행위의 결과에 대하여 고의적 무관심(conscious indifference)이 있는 때에 한하여 요건으로 인정될 수 있다.¹³⁹⁾ 가해행위의 실질적인 악성은 피해자가 입증하여야 하지만, 미국의 일부 주(州)에서는 ‘악성은 법에 내포되어 있는 것(implied in law)’으로 의제된다고 하여 악성의 입증을 요건으로 하지

137) 早川吉尙, 懲罰的損害賠償の本質, 民商法雜誌 第110卷 第6號, 有斐閣, 1995, 1036~1037面.

138) David L. Walther & Thomas A. Plein, *Punitive Damages: A Critical Analysis*, 49 Marquette L. Rev. 369, 372-373 (1965).

139) Illinois Cent. R. Co. V. Owens, 95 So. 833 (Miss. 1923); Reel v. Consolidated Inc. Co., 236 S. W. 43 (Mo. Sup. 1921).

않는다.¹⁴⁰⁾

둘째, 일반적 손해배상의 요건을 갖추어야 한다. 징벌적 손해배상은 예외적인 손해배상인 까닭에 피해자가 징벌적 손해배상을 받기 위해서는 일반적 손해배상을 받을 수 있는 요건을 갖추어야 하며, 징벌적 손해배상만을 청구하는 소송은 성립될 수 없다. 그러므로 징벌적 손해배상은 일반적인 불법행위소송에 부수되는 문제로 되며, 징벌적 손해배상의 전제조건으로 전보적 손해배상의 인정이 요구된다.¹⁴¹⁾ 한편, 불법행위에 대하여 징벌적 손해배상이 인정된다고 하여 불법행위의 일반적인 성립요건에 어떤 변화가 있는 것은 아니며, 가령 불법행위에서 실질적 손해의 발생이 전제되어야 하는데 징벌적 손해배상이 인정되었다고 하여 불법행위의 성립요건이 달라지는 것은 아니다.

징벌적 손해배상은 고의불법행위의 적용범위에서는 크게 개인의 불법행위와 단체에 의한 불법행위로 나누어 볼 수 있는바, 전자의 경우 특히 명예훼손과 같은 인격권침해에 대한 소송에 있어서는 예전부터 징벌적 손해배상이 인정되고 있어 오늘날에도 중요한 문제가 되고 있으며, 후자의 경우 영국에서는 특히 경찰공무원에 의한 강압적·자의적·위법적 행위에 대한 징벌적 손해배상이 인정되고 있고 미국에서는 정부기관과 같은 특정피고(特定被告)에 대하여 징벌적 손해배상의 부과를 금지하는 주(州)도 있으나 일반적으로 가해자가 누구든지 가해자의 악성이 존재하면 전보적 손해배상과 병행하여 배상을 명하고 있다.¹⁴²⁾ 한편, 일반적으로 계

140) 이에 대하여 의제된 악성이나 부주의를 인정하게 되면 징벌적 손해배상의 적용범위가 너무 확대될 가능성이 있기 때문에 이를 반대하는 견해도 있다; *Corrigan v. Bobbo-Merrill Co.*, 228 N. Y. 58, 126 N. E. 260, 10 A. L. R. 662 (1920); *Commercial Credit Corp. v. Blau*, 393 S. w. 2d 558 (Mo. 1965).

141) *Stacy v. Portland Pub. Co.*, 68 Me. 279, 287 (1878); *Long v. Davis*, 68 Mont. 85, 217 667 (1923).

약위반에 있어서는 징벌적 손해배상이 인정되지 않는 것이 원칙이다. 그 까닭은 ① 징벌적 손해배상은 항상 예외적으로 인정되는 것이므로 그 인정범위를 가능한 제한하려 하며, ② 계약위반에 따른 손해배상은 비교적 정확하게 예측하여 산정할 수 있으며 계약당사자들도 계약위반에 따른 실질손해만을 기대하는 것이 일반적이기 때문이다.¹⁴³⁾ 다만 ① 원고가 불법행위책임과 계약위반책임을 선택적으로 청구할 수 있는 경우¹⁴⁴⁾ 또는 ② 계약위반 그 자체가 악의적이므로 불법행위 내지 신뢰관계위반으로 된 경우¹⁴⁵⁾에는 예외적으로 징벌적 손해배상이 인정될 수 있다.

미국에서의 징벌적 손해배상은 원고의 권리에 기하여 인정되는 것이 아니라 배심의 재량에 의하여 그 인정여부가 정하여지는 일종의 횡재(橫財)로서의 성격이 있음은 부인할 수 없으며, 전보적 손해배상이 인정된 사건에서만 부과할 것을 전제조건으로 하면서 그 배상액은 실질적 손해배상의 합리적인 일정비율에 따라 산정되어야 한다고 판례 대부분에서 실시되고 있지만 사실상 그 산정기준은 명료하지 못한 실정이다. 예컨대, 제조물책임으로 한 피고에 대하여 대량적 소송이 제기된 경우 징벌적 손해배상금이 사건마다 제각기 다른 까닭도 그 배상액의 산정기준이 명료하지 못할 뿐 아니라 그 기준으로 제시되는 요인들이 추상적이기 때문이며, 따라서 많은 비판을 받고 있다. 다만, 적절한 배상액의 산정을 위해 고려할 요인으로 가해행위 및 가해행위로 피해자가 입은 손해의 성격·정도 그리고 가해자의 재력 등이 거론되고 있다.

142) 최근 새로운 영역으로 그 범위를 확대하여 제조물책임에 있어서 엄격책임을 적용한 경우에도 징벌적 손해배상을 부과하고 있으며, 이는 공해소송에도 인정되고 있다.

143) Hadley v Baxendale 9 Exch. 341, 156 Eng. Rep. 145 (Court of Exchequer, 1854).

144) Saberton v. Greenwald, 146 Ohio St. 414, 66 NE2d 224 (1946).

145) Hess v. Jarboe, 201 Kan. 705, 708, 443 P. 2d 294 (1968).

위와 같이 산정기준에 의하여 적절한 배상금이 결정될 수 있겠지만 그 자체로는 배상액이 과도하게 부과되는 것을 방지할 수 없다는 봄이 상당하며, 이에 따라 원고 한 사람에 대하여 지급할 배상액을 구체적으로 제한할 취지를 제안한 견해도 있다.¹⁴⁶⁾ 최근 미국 주법에서는 이를 실현할 것을 고려하여 Alabama주에서는 250,000 달러까지로 제한하는 것을 원칙으로 하고 있고, Virginia주는 350,000 달러까지로 제한하고 있으며, 또한 조지아주에서는 제조물책임에 의한 경우 그밖에 사건에서는 250,000 달러까지로 제한하고 있다.¹⁴⁷⁾ 또한 전보적 손해배상액에 비하여 극히 고액인 징벌적 손해배상액의 지급을 명하는 판결이 나오고 있으므로 양자간 적당한 균형을 요구하는 이른바, 합리적 관계기준(reasonable relation test)에 기할 것을 주장하며 전보적 손해배상액의 2배 또는 변호사비용에 10,000 달러를 합한 배상금액 중 선택적으로 결정하여야 할 것이라는 견해가 제기되기도 하였다.¹⁴⁸⁾ 하지만 여전히 배상액산정기준에 대하여 아무런 규정이 없고 집단소송에서 과다배상에 대한 제한이 없다는 점에서는 실질적으로 문제가 되고 있다고 하겠다.

미국에서 징벌적 손해배상의 정당성에 관한 최초의 논쟁으로는 Sedgwick와 Greenleaf사이의 논쟁이 유명하다.¹⁴⁹⁾ Sedgwick은 징벌적 손해배상을 전보적 손해배상의 한 유형으로 보고 그 정당성을 주장했던 반면, Greenleaf의 경우 Sedgwick의 결론을 비판하면서 징벌적 손해배상

146) 원고 1인당 100만 달러까지로 한정할 것을 제안한 것으로는 See David G. Owen, *Problems in Assessing Punitive Damages against Manufacturers of Defective Products*, 49 U. Chi. L. Rev. 1, 48 (1982).

147) Richard C. Ausness, *Retribution and Deterrence: The Role of Punitive Damages in Products Liability Litigation*, 74 Ky. L. J. 1, 124-125 (1985).

148) David G. Owen, *Civil Punishment and the Public Good*, 56 S. Cal. L. Rev. 103, 119 (1982).

149) David L. Walther & Thomas A. Plein, *op.cit.*, at 379.

에 관한 이론은 잘못된 것이라 지적하였다. 판례에서도 징벌적 손해배상에 대한 찬반론이 대립하고 있는데, 이러한 논쟁은 계속되어 오늘날 학자들에 의해서도 격론이 되고 있다.¹⁵⁰⁾

첫째, 징벌적 손해배상의 본질에 비추어 볼 때 이 제도에는 원천적인 문제점이 존재한다. 징벌적 손해배상은 사인(私人)이 소송을 제기하여 배상금을 취득케 하는 것으로, 가해자가 일정 이상의 악성이 강한 행위를 한 경우에만 실손해의 전보에 덧붙여 손해배상을 인정하며 배상액도 피해자측의 손해보다 가해자측의 사정을 중심으로 고려하여 산정하는 데 그 주요한 특징이 있는 것이다. 따라서 이 제도는 피해자에 대한 손해의 전보적 기능보다는 제재적 기능을 주된 목적으로 한 제도라고 할 것이다.¹⁵¹⁾ 환원하자면, 징벌적 손해배상은 제재를 주된 기능으로 하는 형사법적 기능과 전보를 부수적 기능으로 하는 민사법적 기능을 가지고 있는 것이다. 그리고 그 민사법적 기능 중에서 전보적 기능은 정신적 손해와 변호사비용 등 소송비용에 관한 입법적 불비(立法的 不備)의 경우에 이를 보충하기 위하여 부수적 작용해 온 것이다. 결국 징벌적 손해배상은 민사법적 작용을 행하는 경우가 있다고 해도 그 본질은 불법행위에 대한 처벌과 억제라고 하는 제재적 목적으로 하고 법을 준수시켜 질서를 유지하는 형사법적 기초에 근거하고 있다고 할 것이다. 따라서 징벌적 손해배상에서 가해자의 배상책임은 피해자가 아닌 사회일반에 향한 가해행위의 위법성에 근거하는 것으로 보아야 한다. 그럼에도 불구하고 징벌적

150) David G. Owen, *Punitive Damages in Products Liability Litigation*, 74 Mich. L. Rev. 1257, 1264 (1976).

151) 여기서 제재적 기능이라 함은 가해자를 처벌함으로써 그 불법행위를 예방하는 특별예방기능(punishment)과 함께 일반공중에 대하여 경각심을 불러일으켜 불법행위를 억제하는 일반예방기능(deterrence)이 포함되는 것으로 이해된다; Note, *Exemplary Damages in the Law of Torts*, 70 Harv. L. Rev. 517, 522-525 (1957).

손해배상제도는 일반공중(一般公衆)에 대한 공법적 위법성을 피해자에 대한 민사상 위법성과 분리하지 않음으로써 그 배상책임과 배상액의 귀속을 손해배상의 당사자간에 적용하는 오류에 놓인다. 그러므로 가해행위가 피해자에 대한 것인 동시에 사회일반에 대한 가해행위로 위법성을 가지는 것이라면 그 결과인 징벌적 손해배상은 공공적 귀속이어야 할 것이며, 이는 그것이 가해자에 대한 징벌 또는 가해자를 포함한 제3자에 대한 경고 등을 통하여 재발방지를 목적으로 한다는 자체가 그 배상액이 피해자에게 귀속되어야 할 법리적 근거가 될 수 없기 때문이다.¹⁵²⁾

둘째, 민사상 불법행위책임에 관한 이론적 논의선상에서는 징벌적 손해배상이 피해자에게 발생된 실질손해보다 현저하게 고액이라는 점을 설명할 수 없는 난점을 지니고 있다. 따라서 징벌적 손해배상제도는 사회적 손실에 대한 가해자의 배상액을 피해자에게 귀속시키는 법리로서 민사적으로는 피해자의 부담이득을 정당화시켜주는 제도로 전락할 수 있다. 징벌적 손해배상을 피해자에게 귀속시키는 것이 피해자가 가해자에 대한 소송을 통해 사악한 불법행위자를 현출함으로써 공익에 이바지하였다는 점에서 보상적 의미를 찾는다고 할지라도 그 보상은 국가가 행할 문제인 것이지 가해자에게 직접 부담시켜 피해자가 취득토록 해야 할 법리적 근거가 없기 때문이다. 뿐만 아니라 징벌적 손해배상이 사회적 가치의 실현을 위하여 필요한 것이라고 하더라도 당사자가 배상범위의 합의로 사건을 해결하는 경우에 그 공공적 가치가 당사자의 합의에 의존할 수 있는 것인지에 대한 의문도 남아있다.

셋째, 그밖에 여러 문제점이 지적될 수 있지만, 특히 개인정보권의 침

152) 同旨; 정해상, 손해배상의 법리와 징벌적 손해배상의 관계, 중앙법학 제6집 제4호, 중앙대학교 법학연구소, 2004, 249쪽.

해와 관련하여서는 ① 피해자인 원고가 복수이고 피고가 단수인 경우 빠른 소송을 제기한 원고가 유리하며 먼저 배상금을 획득했다면 다음 원고는 같은 배상액을 얻을 만한 보장이 없기 때문에 징벌적 손해배상이 피고간에 불공평을 초래할 수 있다는 점, ② 대위책임인 사용자책임의 경우 징벌해야 하는 가해자인 피용자의 행위에 대해서 왜 고용주인 사용자가 징벌적 손해배상책임을 지지 않으면 안 되는가를 설명하기 어렵다는 점, ③ 징벌적 손해배상액 지불 후의 형사법처벌(刑事罰處罰)은 동일범죄(同一犯罪)로 이중처벌금지(二重處罰禁止)의 이념에 위배될 수 있다는 점이 재고되어야 할 것이다.

여하튼 현행 제도에서 권리침해에 대한 구제방법이 적절치 못하다는 전제하에 정보주체의 권리보장 측면에서 징벌적 손해배상제를 도입하는 것이 법체계 혹은 법원리와의 충돌은 없는지 여부에 대하여 검토하면 다음과 같이 논의할 수 있다.

우선 원칙적 소극설로서 민사상의 손해배상은 근본적으로 형사벌과 구별된다는 점에서 권리침해행위에 대한 민사적 구제방법은 원칙적으로 전보적 손해배상으로 국한되어 있는 까닭에, 징벌적 손해배상을 현행 사법체계 내에서는 수용하기 어렵다는 입장이 있을 수 있겠다. 현행법상 손해의 배상이란 부족분을 메우는 전보에 국한되므로 발생한 손해의 전보를 위하여 산정된 금액은 침해자의 악의적 행위 또는 자력 유무와는 무관한 것이므로 징벌적 손해배상과는 이질적임을 그 논거로 한다. 곧 법이론적 관점에서는 민사적 구제방법인 손해배상법리가 전보배상에 따르므로 형사벌에 해당하는 징벌적 손해배상을 포섭하지 못하는 것으로 이해한다. 따라서 악의적 권리침해행위에 대한 예방적 효과를 확보하기 위하여 징벌적 손해배상을 제도적으로 도입하는 것은 현행 법체계에 합당하지 않

는다는 결론에 도달하게 된다. 이러한 견해를 따를 때 징벌적 손해배상이 지니는 제재적 기능을 보완하는 별도의 방안이 현실적으로 구체화될 필요가 있다. 한편 이에 대하여 그 현실적 필요성에도 불구하고 징벌적 손해배상제도를 수용하기에는 본질적인 법이론적 난점이 존재한다는 측면에서, 이중처벌금지원칙에 위배되지 않기 위하여는 개인정보보호법에서 규정하는 형사벌칙 규정을 없애야 한다는 논리귀결에 이르게 된다. 물론 이러한 견해에 찬동하기 어렵다는 측면에서 정책적 고려에 따라 징벌적 손해배상의 상한범위를 정하고 구체화된 산정기준에 따라 법관의 재량으로 부과하면서 관련 형사벌칙은 존치토록 하는 주장을 제시할 수 있겠으나, 법리적 논의에 비추어 볼 때 그 논거는 빈약하기만 하다고 할 것이다. 이런 주장은 제한적 수용설이라 부를 수 있을 것이다.

그렇다면 민법 그 자체에 일반원칙으로 징벌적 손해배상제도를 도입하는 것은 원론적으로 불가능할 것이지만, 공공기관법 및 정통방법에서 징벌적 손해배상을 제도적으로 수용하는 것이 가능할 것인가? 후자의 경우 일반법인 민법상의 손해배상과 달리 징벌적 손해배상을 제도화하고 특별한 정책적 고려를 반영하게 할 수 있겠지만 무엇보다 이중처벌금지원칙에 위배되지 않도록 현행 벌칙규정을 폐지하는 것이 선행되어야 할 것인데, 오히려 징벌적 손해배상의 대안으로서 벌금을 상향조정하는 방안이 보다 적절할 것으로 판단하는 관점이 유력할 것으로 보인다. 원래 징벌적 손해배상이 가지는 제재적 기능을 충실히 반영하면 될 것이고 이는 피해자가 획득할 부당이득의 문제에도 자유로울 수 있기 때문이다.

반면에, 전자의 경우 공법상의 당사자소송으로 제기되는 국가배상청구 소송에 대하여도 일반법으로 민법이 존재하는 것이고 다만 공공기관법이라는 행정특별법에서 징벌적 손해배상을 제도화하면 국가배상법과 충돌

하지 않고 그 제도의 제재적 기능을 발휘할 수 있도록 할 수 있으리라고 일견 상정할 수 있을 것이다. 이 경우 이중처벌금지원칙에 부합할 수 있도록 현존하는 벌칙규정을 폐지하는 수순을 밟아야 할 것이며 그렇지 않고 적절한 상한범위와 산정기준으로 제시한다면 그 제도화가 가능할 것으로 볼 수도 있다. 하지만 국가배상법에서 적용되는 자기책임법리와 모순되는 측면은 좀처럼 극복되기 어려운 난제로 남는다는 점을 간과해서는 아니 될 것이다. 왜냐하면, 가해자인 공무원 개인에 대한 불법행위책임을 민사법적 손해배상으로 보전하는 것을 넘어서 제재적 기능을 보유한 징벌적 손해배상으로 인정하게 된다면 이는 국가배상청구소송을 통한 행정책임과는 다른 것이 되기 때문이다. 그러므로 입법정책적으로 징벌적 손해배상을 관철하려 한다면 우선 공공부문과 민간부문을 구별하여 어느 영역에 국한시킬 것인지 아니면 兩者를 분리하더라도 그 수용을 대신할 만한 제도적 방안을 보충할 것인지를 결정하는 것이 선결과제가 될 것이다. 만일 후자의 방향으로 정리할 것이라면 민간부문에 대하여 과징금 또는 이행강제금의 도입 여부를 검토하고 공공부문과 함께 행정형벌로서 벌칙에 있어서의 양형수준을 상향조절하는 절차가 필요할 것으로 본다. 그리고 이와 같은 논의는 이른바 개인정보보호법을 제정하는 데에도 크게 다르지 않게 적용된다. 따라서 공공부문과 민간부문을 구분하여 규율하는 경우에는 그에 대한 천착(穿鑿)이 자연스럽게 이어질 수 있는 반면, 그렇지 않은 경우 순탄치만은 않은 과정이 될 것이다.¹⁵³⁾

2. 법안의 주요내용

2안의 경우 개인정보단체소송을 규정하고 있으며, 1안과 3안을 포함하

153) 공공부문과 민간부문의 구별논의에 대한 상세는 拙稿, 개인정보에 관한 법리의 재검토, 인터넷법률 통권 제30호, 법무부, 2005, 52~55쪽 참조.

여 법안 모두 징벌적 손해배상에 대하여는 규정하고 있질 않다. 개인정보 단체소송에 관한 2안의 내용을 조문별로 보면 다음과 같다.

제67조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인정보처리자가 위원회의 조정을 거부하거나 조정결과를 수락하지 아니한 경우에는 법원에 정보주체의 재산적 피해의 구제 및 권리침해행위의 금지·중지를 구하는 소송(이하 "단체소송"이라 한다)을 제기할 수 있다.

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록한 소비자 단체로서 다음 각 목의 요건을 모두 갖춘 단체

가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것

나. 단체의 정회원수가 1천명 이상일 것

다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것

2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체

가. 법률상 또는 사실상 동일한 침해를 입은 100인 이상의 정보주체로부터 단체소송의 제기를 요청받을 것

나. 정관에 개인정보보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동실적이 있을 것

다. 단체의 상시 구성원수가 5천명 이상일 것

라. 중앙행정기관에 등록되어 있을 것

제68조(전속관할) ① 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담

당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다.

② 제1항을 외국사업자에 적용하는 경우 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정한다.

제69조(소송대리인의 선임) 단체소송의 원고는 변호사를 소송대리인으로 선임하여야 한다.

제70조(소송허가신청) ① 단체소송을 제기하는 단체는 소장과 함께 다음 각 호의 사항을 기재한 소송허가신청서를 법원에 제출하여야 한다.

1. 원고 및 그 소송대리인
 2. 피고
 3. 손해배상액 또는 침해된 권리의 내용
- ② 제1항에 따른 소송허가신청서에는 다음 각 호의 자료를 첨부하여야 한다.
1. 소제기단체가 제67조 각 호의 어느 하나에 해당하는 요건을 갖추고 있음을 소명하는 자료
 2. 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류
 3. 개인정보처리자가 조정결과를 수락하지 아니한 경우에는 위원회의 조정결정서 정본

제71조 (소송허가요건 등) ① 법원은 다음 각 호의 요건을 모두 갖춘 경우에 한하여 결정으로 단체소송을 허가한다.

1. 개인정보처리자가 위원회의 조정을 거부하거나 조정결과를 수락하지 아니하였을 것
 2. 개인정보의 처리목적이 제27조제2호 및 제6호부터 제8호까지에 해당하지 아니할 것
 3. 재산적 손해
 4. 제70조에 따른 소송허가신청서의 기재사항에 흠결이 없을 것
- ② 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

제72조(확정판결의 효력) 원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 제67조에 따른 다른 단체는 단체소송을 제기할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체·수사기관 및 위원회에 의하여 새로운 증거가 나타난 경우
2. 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우

제73조(「민사소송법」의 적용 등) ① 단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다.

- ② 제71조에 따른 단체소송의 허가결정이 있는 경우에는 「민사집행법」 제4편의 규정에 따른 보전처분을 할 수 있다.
- ③ 단체소송의 절차에 관하여 필요한 사항은 대법원규칙으로 정한다.

제3절 법제화 방향

사법부를 통해 강제적으로 권리구제를 달성할 경우 현재의 미진함을 극복하는 방안으로 집단적 소송형식과 징벌적 손해배상이 제기되고 있는 바, 전자의 경우 그 도입으로 인해 야기되는 법적 문제보다는 현실적으로 책임을 질 당사자의 반대에 부딪혀 논란이 될 여지가 있는 반면에 후자의 경우 그 수용 자체가 법체계상 부조화를 낳을 수 있다.

다른 한편으로 전자의 경우 실정법으로 개별영역에서 이미 도입하고 있는 예가 있으므로 그 운영상 단점을 반면교사로 삼아 이를 극복하는 방안으로 사회적 합의를 이끄는 방향에서 오히려 그 도입이 용이할 수도 있는 반면, 후자의 경우 피해자의 부당이득귀속문제가 존재하지만 일반적 법감정으로는 가해자에 대한 비난가능성을 징벌적 책임의 가중으로 충족시킬 수 있다는 점만을 부각하고 부당이득에 관한 문제는 내면적으로만 주목토록 함으로써 그 제도적 수용을 보다 손쉽게 확보할 수도 있으리라 짐작되어진다. 그럼에도 불구하고 반대논거에 따라 그 도입에 소극적인 입장으로 정리할 경우에도, 개인정보보호법제의 개선을 위해 인터넷을 활용한 사법체계를 구축하거나 이 영역에 있어 처벌을 강화하고 과징금제도를 도입하는 등의 대안을 제시할 수도 있겠다.¹⁵⁴⁾ 하지만 이 또한 미

154) 정통망법의 경우 2008년 6월 13일 법률 제9119호로 제26차 일부개정에서 다음과 같이 과징금제도가 도입되었다.

정통망법 제64조의3(과징금의 부과 등) ① 방송통신위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 전기통신사업자에게 위반행위와 관련한 매출액의 100분의 1 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제6호에 해당하는 행위가 있는 경우에는 1억원 이하의 과징금을 부과할 수 있다.

1. 제22조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우
2. 제23조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인의 권리·이익

봉책에 불과하다는 점을 인식하여야 할 필요가 있다. 특히 과징금의 경우 정통망법과 같이 「전기통신사업법」 제2조제1항제1호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자인 정보통신서비스제공자에게 부과하는 것은 가능하지만 개인정보보호법의 수범대상으로서 개인정보처리자중 국가기관 또는 지방자치단체 등의 경우 그 대상이 되지 않기 때문이다. 즉, 공공기관에 대한 통제수단이 적절하게 마련되지 않는

이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집한 경우

3. 제24조를 위반하여 개인정보를 이용한 경우

4. 제24조의2를 위반하여 개인정보를 제3자에게 제공한 경우

5. 제25조제1항을 위반하여 이용자의 동의를 받지 아니하고 개인정보 취급위탁을 한 경우

6. 제28조제1항제2호부터 제5호까지의 조치를 하지 아니하여 이용자의 개인정보를 분실·도난·누출·변조 또는 훼손한 경우

7. 제31조제1항을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우

② 제1항에 따른 과징금을 부과하는 경우 전기통신사업자가 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 전기통신사업자와 비슷한 규모의 전기통신사업자의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억 원 이하의 과징금을 부과할 수 있다.

③ 방송통신위원회는 제1항에 따른 과징금을 부과하려면 다음 각 호의 사항을 고려하여야 한다.

1. 위반행위의 내용 및 정도

2. 위반행위의 기간 및 횟수

3. 위반행위로 인하여 취득한 이익의 규모

④ 제1항에 따른 과징금은 제3항을 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.

⑤ 방송통신위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다.

⑥ 방송통신위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니한 경우에는 기간을 정하여 독촉을 하고, 그 지정된 기간에 과징금과 제5항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

⑦ 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지 연 100분의 6에 해당하는 환급가산금을 지급하여야 한다.

한, 징벌적 손해배상의 도입은 이중처벌금지원칙의 위배 논란에도 불구하고 규율방향에서 논의가 이어질 쟁점이라고 할 수 있다.

한편, 전술(前述)한 바와 같이 다수당사자소송과 단체소송의 이원적으로 구분되는 가운데 집단소송의 법제화가 요청되는 현실에서는, 2안과 같이 정보주체의 재산적 피해의 구제 및 권리침해행위의 금지·중지를 구하는 단체소송을 제도화하는 시도는 논의의 가치가 충분하다. 특히 「소비자기본법」 제70조에서 규율하는 단체소송의 대상은 사업자가 「소비자기본법」 제20조¹⁵⁵⁾를 위반하여 소비자의 생명·신체 또는 재산에 대한 권익을 직접적으로 침해하고 그 침해가 계속되는 경우 법원에 소비자권익침해행위의 금지·중지를 구하는 단체소송을 제기할 수 있을 뿐이므로 재산적 피해의 구제를 소비자단체를 통하여 집단적으로 사법적 해소를 꾀할 수 있는 방안이 되기 때문에 더욱 그러하다. 하지만 이러한 사항은 국가나 지방자치단체에 의한 개인정보 권리침해에 따라 발생하는 재산적 피해의 구제에 대한 검토를 간과한 것으로 판단된다. 즉, 공무원이 직무를 집행하면서 고의 또는 과실로 법령을 위반하여 타인에게 손해를 입히거나 공공의 영조물(營造物)의 설치나 관리에 하자(瑕疵)가 있기 때문에 타인에게 손해를 발생하게 하였을 때 국가나 지방자치단체가 그 손해를 배상하는 「국가배상법」 제2조제1항 및 제5조제1항 적용영역에 있어서 집단적

155) 「소비자기본법」 제20조(소비자의 권익증진 관련 기준의 준수) ①사업자는 제8조제1항의 규정에 따라 국가가 정한 기준에 위반되는 물품등을 제조·수입·판매하거나 제공하여서는 아니 된다.

②사업자는 제10조의 규정에 따라 국가가 정한 표시기준을 위반하여서는 아니 된다.

③사업자는 제11조의 규정에 따라 국가가 정한 광고기준을 위반하여서는 아니 된다.

④사업자는 제12조제2항의 규정에 따라 국가가 지정·고시한 행위를 하여서는 아니 된다.

⑤사업자는 제15조제2항의 규정에 따라 국가가 정한 개인정보의 보호기준을 위반하여서는 아니 된다.

소송수행의 경우 2안은 “단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다”고 규정하여 국가배상청구에 대하여는 전혀 고려의 여지를 두고 있지 않으며, 이 경우 소비자단체에 의한 단체소송보다는 대표당사자소송에 의한 소송수행과 「국가배상법」의 준용으로 다루는 방안이 보다 실효성 있는 소송요건과 공법적 규율에 대한 적합한 절차이행을 이끌 수 있을 뿐만 아니라, 2안 제4절 개인정보단체소송에 규정된 제67에서 73조까지의 내용은 재산적 피해구제에 대한 침언과 개인정보보호에 관한 각색이 있을 뿐 「소비자기본법」 제70에서 76조까지의 규정을 가져온 데 지나지 않기 때문이다.

그러므로 징벌적 손해배상에 대한 개인정보보호법에의 수용은 적절한 입법방향으로 제시되기 어렵고 특히 개별분야에 대한 징벌적 손해배상의 도입보다는 일반적인 징벌적 손해배상에 대한 규정과 그 적용에 관한 기본법적 규율원칙을 정립하는 것이 바람직하다고 볼 수 있는 반면, 집단소송제도의 접목에 있어서는 개인정보보호법의 적용영역을 공적 부문과 사적 부문으로 이원화할 수 있다는 시각에서 절차법적 연계를 시도하는 방향에서 논의되어야 할 것으로 본다. 환원하자면, 이중처벌금지원칙에 위배될 여지가 있는 징벌적 손해배상은 관련 법제와 유관 기능의 보강으로 해소될 수 있는 쟁점이지만 집단소송제도의 경우 미국식 class action을 공공분야에 대한 국가배상청구소송과 결합하여 규율하면서 소비자단체의 소송참가를 예정하는 독일식 Verbandsklage의 유용성은 공행정 수행자가 아닌 민간분야의 사기업에 대항하여 불법적 손해에 대한 전보를 구하는 집단적 소송수행방식으로 자리매김하는 방안이 타당할 것이라는 관건이 논리적 설득력을 얻을 것으로 가늠된다.

제5장 결 론

개인정보보호라는 시대적 화두가 완결될 수 있기 위해서는 정보사회가 지향하는 정보질서¹⁵⁶⁾에 따라 균형 잡힌 정보가치관으로 정보환경을 구축하는 가운데 사회구성원의 권리를 상호 존중할 수 있어야 할 것으로 본다. 그 일환으로 개인정보취급자는 합법적이고 공정한 절차에 따라 정보주체가 인식할 수 있는 상태에서 개인정보를 수집·처리할 수 있도록 합리적인 입법적 조율이 선행되어야 할 것이다. 이러한 논급은 개인정보가 개인적·사회적 가치뿐만 아니라 엄연히 경제적 가치를 지니고 그 활용을 전제로 정보질서를 결정짓는 정보환경의 기본요소이기 때문이다. 이를 주장하는 것이 개인의 정보자기결정권을 보호하지 않고 이익을 구하려 하는 불법적이고 음성적인 정보시장의 수요를 대변하는 것도 아니며, 오히려 정보주체의 정보자기결정권을 보장하면서 합법적인 범위 내에서 합리적인 정보유통도 함께 가능하도록 하는 민주적인 정보질서의 정립에 대하여 참여적으로 논박하는 것이다.

물론 현재 개인정보보호법의 제정이 개인정보를 보호할 수 있는 체계적인 법제정비라는 측면에서 긍정적이지만, 그 파장으로서 경제적·사회적 효율성 하락에 대한 우려 역시 크다는 점은 일응 설득력을 지닌다. 하지만 공공부문에서의 행정정보공유나 민간부문에서의 개인정보활용에 대한 논리적 필연성은 헌법적 토양 위에 입법적 한계와 기술적 보완을 제도적으로 대응하지 않는다면 보호와 이용의 균형을 모색하는 것이 요원할 수

156) 법적으로 구성되는 정보질서는 현실적인 사회구조를 반영할 뿐만 아니라, 이들이 추구해야만 하는 ‘지침과 기준’을 제공해야 한다; Friedrich Schoch, *Öffentlichrechtliche Rahmenbedingungen einer Informationsordnung*, VVD StRL 57, Walter De Gruyter Inc., 1998, S.213.

밖에 없게 된다. 시대적 사명을 가지고 정보통신망을 통해 다루어지는 개인정보 관련 권리의 보호를 위해 일단의 행정적인 정책집행이 진행되고 있지만, 궁극적으로 법제도적인 정비에 맞물려 정보환경을 새롭게 다지지 않는다면 사상누각(砂上樓閣)이 될 수밖에 없을 것이다. 따라서 이를 위한 기반이 되는 개인정보보호법의 제정은 그로 인해 야기될 다양한 효과에 대하여 관련 이해관계인 및 전문가 등으로부터 광범위한 의견수렴과정을 거쳐 이를 사회적 합치로 이끌고 이에 따라 개인정보의 합법적 이용과 보호가 조화롭게 이루어질 수 있도록 논의되어야 할 것이다.

생각건대 국회에 계류중인 법안의 절충은 총괄적인 개인정보보호기구의 설립에 초점을 맞추고 그 설치 및 운영에 관한 내용만으로 된 법률을 공포하고 이에 따라 창설된 총괄기구가 개인정보보호를 위한 사무전반을 관장하면서 관련사항을 규범적·제도적으로 정립해 나가는 것이 더욱 중요하다고 할 것이다. 개인정보보호법제에 관하여 최근 몇 년간 천착해 온 결과물을 종합적으로 검토할 때에 현재의 상황에서 내릴 수 있는 잠정적인 결론은 어떠한 개인정보보호정책을 어떻게 집행할 것인가의 문제라기 보다는 의견수렴에 있어 어느 정도는 합치를 보이고 있는 개인정보보호기구의 발족에 따라 그 주요구성원인 위원(委員)들이 향후 방향성을 제시하고 보호의 사각지대를 메워나가며 필요한 제도를 도입·수용하여야 한다는 데 있기 때문이다.

그렇기 때문에 법정책적으로 개인정보보호법이 지니고 있는 정책법 부문에 있어서 요체는 바로 개인정보보호기구인 위원회의 창설이라 할 수 있다. 그런 만큼 그 법적 쟁점과 과제는 정치적·전략적 논의로부터 자유롭게 어려운 실정에서 거론될 수밖에 없으며, 위원회의 위원, 전문위원, 사무처 등의 자리다툼 역시 무시할 수 없는 현실적 장벽으로 작용하고

있다. 그럼에도 불구하고 개인정보보호법의 제정과 관련하여 영향평가의 제도적 도입과 피해구제의 실효성 있는 소송현실화를 논의하는 것은 모름지기 정보주체의 정보자기결정권 보장이라는 헌법적 요청에서 비롯된 것이다.

오늘날 개인정보는 개인이 사적 생활을 하는 데 필요한 것이라기보다는 단지 국가나 민간사업자 등이 업무나 영업활동을 수행하기 위하여 그 수행목적에 합치되는 대상자를 선별하기 위해 이용하는 것이 대부분이며, 이 경우 이용되는 개인정보는 정보 전부가 아니라 업무나 사업의 관점에서 다양한 정보군 가운데 필요한 정보를 분석하고 추출하여 재구성한 정보라 할 수 있다. 따라서 선별된 개인정보취급자는 개인정보를 기준으로 특정한 정보나 서비스를 제공하거나 또는 금전을 지급하고 징수하는 것이고, 그러므로 개인정보는 경제적 측면에서 대증을 통제하는 방법으로 활용되고 있는 것이며, 정보주체인 개인은 평등한 서비스를 향유한다는 측면에서 이익을 얻는 것임이 간과되어서는 아니 된다.¹⁵⁷⁾ 그러기에 개인정보의 보호 문제를 프라이버시권의 개념으로부터 도출하는 체계에서 벗어나 새로이 개인정보에 관한 권리의 개념을 재정립할 필요가 대두된다. 그 권리의 객체가 되는 개인정보를 범주화하고 이에 대응하는 권능을 세분화·체계화함으로써 보호와 이용의 조화로운 법률관계를 형성하도록 하는 적극적 의미로 해석될 수 있기 때문에, 우선 국가 또는 민간사업자 등 개인정보관리주체에 대한 부정과 불신의 관념에서 벗어나 정당한 권리·의무의 법률관계로 형성할 수 있도록 하는 것이 중요한 것이다. 결과적으로 보호할 것은 두텁게 보호하고 이용할 것은 합리적으로 보호할 수 있는 제도적 체계의 확립을 위해서 개인정보에 관한 권리의 재정

157) 황인호, 개인정보보호제도에서의 규제에 관한 연구, 건국대학교 박사학위 청구 논문, 2001, 88~90쪽.

립이 요구된다 할 것이다. 이를 바탕으로 하지 않는 한 개인정보보호기구의 창설은 유명무실해질 수밖에 없다. 따라서 한편으로 행정권한의 통제로서 또 다른 측면에서는 상충가치의 조율과 행정규제의 완화를 함께 추진해나갈 수 있는 조직으로 개인정보보호기구를 구성하여야 할 것이다.

이러한 측면에서 필자는 공공부문과 민간부문을 분리하여 단일법에 그 규율의 상이점을 포괄하고 이를 통합적으로 집행해나가는 개인정보보호기구의 정립을 주장해 왔다. 이는 정보주체의 입장에서 보면 자신의 개인정보가 공공부문이나 민간부문이나 그 어디에서 처리되고 있는 상관없이 단일의 통합기구에서 통일되게 보호기능이 이루어질 것이라는 믿음을 가질 수 있고 또 권리침해가 있는 경우에 통합기구라는 단일의 창구를 통해서 권리구제를 요청할 수 있다는 점에서, 국가적 차원에서는 개인정보 보호를 위한 종합적인 정책방향이 통합기구를 통해 수행될 수 있다는 점에서, 개인정보보호에 있어 국제협력의 모색을 위한 범세계적 차원의 원칙과 집행기준을 통합기구가 마련할 수 있다는 점에서 효과적이기 때문이다.¹⁵⁸⁾ 이를 위해서는 독임제의 폐단을 극복하고 신중한 결정을 신속하고 효율적으로 이루어질 수 있도록 구성원을 적정화하고 상임위원을 당해수행업무의 범위와 분량에 비추어 최적화하는 것도 필요하다.

개인정보보호기구의 권한은 정보주체의 권리를 실효성 있게 보장하면서 개인정보의 활용주체에 대해서는 적절한 통제와 정책적 대응으로 정보환경의 선진화를 유도하며 일반국민이 개인정보보호에 대하여 인식을 제고할 수 있도록 교육·홍보·연구하는 임무를 국제적 협력 아래 수행하는

158) 同旨; 이인호, 개인정보감독기구의 위상과 역할에 대한 비교법적 분석과 입법 방향, 중앙법학 제7집 제1호, 중앙법학회, 2005, 20쪽.

것으로 정리할 수 있겠지만, 현실적으로 대통령 소속 합의제행정기관으로서 구성하되 그 독립성과 정치적 중립성을 확보하는 방향으로 수립되어야 할 것으로 본다. 그리고 영향평가와 피해구제의 제도적 정립도 개인정보보호기구의 권한과 연계되어 개인정보보호법의 성안과 실행으로 이어지길 기대한다.

참고문헌

- 권영성, 헌법학원론, 법문사, 2005.
- 권오승, 소비자보호와 단체소송, 인권과정의 통권 제179호, 대한변호사협회, 1991.
- 구병문, 캐나다 및 미국의 프라이버시 영향평가 제도 분석과 국내 전자정부 법제로의 도입방향 검토, 정보화이슈분석 03-16, 한국전산원, 2003.
- 김용태·명형식·나용식, 한국법제사개요, 원광대학교출판부, 1981.
- 김일환, 개인정보보호감독기구의 설치에 관한 연구, 전자정부법제연구 창간호, 행정자치부, 2006.
- 배대현, 정보의 귀속·유통에 관한 민사법적 접근, 비교사법 통권 제15호, 한국비교사법학회, 2001.
- 법무부 編, 집단소송의 법리, 법무자료 제149집, 법무부, 1991.
- 서종표, 가상공간에서의 개인정보보호, 전남대학교 석사학위청구논문, 2005.
- 이광윤·김민호, 최신행정법론, 법문사, 2002.
- 이민영, 정보매체의 규제조직에 관한 법적 연구, 공법연구 제36집 제3호, 한국공법학회, 2008.
- 이민영, 개인정보법제론, 진한M&B, 2007.
- 이민영, 개인정보에 관한 법리의 재검토, 인터넷법률 통권 제30호, 법무부, 2005.
- 이시윤, 민사소송법, 박영사, 2000.
- 이인호, 개인정보감독기구의 위상과 역할에 대한 비교법적 분석과 입법방

- 향, 중앙법학 제7집 제1호, 중앙법학회, 2005.
- 이창범·김본미, 개인정보피해구제 및 배상기준에 관한 연구, 연구보고 04-02, 개인정보분쟁조정위원회, 2005.
- 정영화, 사이버스페이스와 프라이버시권, 헌법학연구 제6권 제3호, 한국헌법학회, 2001.
- 정해상, 손해배상의 법리와 징벌적 손해배상의 관계, 중앙법학 제6집 제4호, 중앙대학교 법학연구소, 2004.
- 한국전산원, 개인정보보호제도 시행을 위한 사례연구, 정부혁신지방분권위원회, 2005.
- 함영진, 집단소송에 관한 연구, 고려대학교 박사학위청구논문, 1997.
- 황인호, 개인정보보호제도에서의 규제에 관한 연구, 건국대학교 박사학위 청구논문, 2001.
- Walter J. Habscheid 著/호문혁 譯, 입증책임과 입증의 정도, 법학 제32권 제1·2호, 서울대학교 법학연구소, 1991.
- Ansley C. Tillman, *Unwarranted Entry: An Examination of the Supreme Court's Decision to Enter the Punitive Damages Arena*, 24 Rev. Litig. 473 (2005).
- Charles Fried, *Privacy*, 77 Yale L. J. 475 (1968).
- Daniel J. Solove & Marc Rotenberg, *Information Privacy Law*, Aspen Publishers Inc., 2003.
- David G. Owen, *Problems in Assessing Punitive Damages against Manufacturers of Defective Products*, 49 U. Chi. L. Rev. 1 (1982).
- David G. Owen, *Punitive Damages in Products Liability Litigation*, 74 Mich. L. Rev. 1257 (1976).

- Ernst Wolf, *Grundfragen des Schadensbegriffs und der Methode der Schadenserkennung*, Festschrift Schiedermair, 1976.
- Ferdinand Kopp, *Das EG-Richtlinenvorhaben zum Datenschutz*, RDV, 1993.
- Jack H. Friedenthal, Arthur R. Miller, John E. Sexton & John J. Cound, *Civil Procedure: Cases and Materials*, West Publishing Co., 2001.
- James A. Henderson, Richard N. Pearson, & John A. Siliciano, *The Torts Process*, Aspen Publishers Inc., 2003.
- James D. Cox, *Making Securities Fraud Class Actions Virtuous*, 39 Arizona Law Review 497 (1997).
- John Y. Gotanda, *Punitive Damages: A Comparative Analysis*, 42 Colum. J. Transnat'l L. 391 (2004).
- Kevin S. Marshall & Patrick Fitzgerald, *Punitive Damages and the Supreme Court's Reasonable Relationship Test: Ignoring the Economics of Deterrence*, 19 St. John's J. Legal Comment. 237 (2005).
- Melvin M. Belli, *Punitive Damages: their history, their use and their worth in present-day society*, 49 UMCK. L. Rev. 1 (1980).
- Office of the Privacy Commissioner, *Managing Privacy Risk: An Introductory Privacy Impact Assessment for Australian Government and ACT Government Agencies*, Australian Government, 2004.
- Office of the Victorian Privacy Commissioner, *Privacy Impact Assessments: a guide*, Privacy Victoria – independent statutory

- office of Australia, 2004.
- Paul M. Schwartz & Joel R. Reidenberg, *Data Privacy Law : A Study of United States Data Protection*, Michie Law Publishers, 1996.
- Raymond Wacks, *Personal Information*, Gloucestershire: Clarendon Press, 1989.
- Richard C. Ausness, *Retribution and Deterrence: The Role of Punitive Damages in Products Liability Litigation*, 74 Ky. L. J. 1 (1985).
- Samuel Freifield, *The Rationale of punitive Damages*, 1 Ohio St. L. J. 5 (1935).
- Steven A. Bibas, *A Contractual Approach to Data Privacy*, 17 Harv. J. L. & Pub. Pol'y 591, 1994.
- Steven L. Emanuel, *Torts: Keyed to Prosser, Wade, and Schwartz*, Aspen Publishers Inc., 2002.
- Tony Weir, *A Casebook on Tort*, Sweet & Maxwell, 2004.
- Walther J. Habscheid, *Effektiver Rechtsschutz und verfassungsmäßige Ordnung, Internationalen Kongreß für Prozeßrecht*, Würzburg 1983.
- W. V. H. Rogers, *Tort*, Sweet & Maxwell, 1998.
- 松井茂記, 個人情報保護基本法とプライバシーの權利, ジュリスト No.1190, 2000.
- 田島泰彦, 個人情報保護制度をどう構想するか, 法律時報 第72卷 第10號, 2000.
- 三宅 弘, 個人情報保護法制化の経緯と課題, 法律時報 第72卷 第10號, 2000.

134 개인정보보호의 법적 쟁점과 과제

早川吉尙, 懲罰的損害賠償の本質, 民商法雜誌 第110卷 第6號, 有斐閣, 1995.

山口正久, 美國の製造物責任訴訟と懲罰的損害賠償(上), NBL 第281号, 1983.

개인정보보호의 법적 쟁점과 과제

2009년 12월 인쇄

2009년 12월 발행

발행인 : 김 성 태

발행처 : 한국정보화진흥원

서울시 중구 무교동 77번지

전화 : (02) 2131-0114

인쇄처 : 호정씨앤피

전 화 : (02) 2277-4718

<비매품>

- 본 보고서의 내용은 한국정보화진흥원의 공식 견해와 다를 수 있습니다.
- 본 보고서 내용에 대해 무단전재(無斷轉載)를 금하며, 가공·인용할 때에는 반드시 「한국정보화진흥원」이라고 출처를 밝혀 주시기 바랍니다.