



개인정보 보호제도 개관

개/인/정/보/보/호/관/리/사

www.lawnb.com

I. 개인정보 보호의 의의

1. 프라이버시 권리와 개인정보 자기결정권

가. 개인정보 자기결정권의 보장

사람은 누구나 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가지고 있다. 또 인간은 자아를 둘러싼 비밀을 가지고 있으며, 자기만의 영역에서 평온을 누리면서 자유롭게 살아가길 원한다. 이처럼 인간 내면의 비밀과 평온을 보호하고자 우리 헌법은 모든 국민에게 프라이버시 권리(privacy right) 즉, '사생활의 비밀과 자유'(제17조)를 보장하고 있다. '사생활의 비밀과 자유'는 인간의 존엄을 실현하고 인격의 자유로운 발전을 포괄적으로 뒷받침하는 불가침의 인격권이라 할 수 있다.

프라이버시 권리는 원래 소극적 의미의 '홀로 있을 권리'(a right to be let alone)로 이해되었으며, 1890년 미국의 Warren과 Brandeis의 논문¹⁾에서 하나의 독립된 권리로 주창되어 20세기 초 미국에서 판례를 통하여 법적 권리로 인정되었다. 이러한 '홀로 있을 권리'로는 '사생활의 자유의 불가침', '사생활 비밀의 불가침' 등이 있다. 이 중 '사생활의 자유의 불가침'은 결혼, 임신, 피임, 낙태, 자녀양육, 교육, 용모, 성생활의 자유 등 사생활의 자율을 침해받지 아니하는 것을 말한다. 그리고 '사생활 비밀의 불가침'은 개인의 사사(私事)에의 침입, 개인의 난처한 사사의 공개, 공중에게 오해를 낳게 할 사사의 공표, 성명·

1) Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", 4 Harvard L. Rev. 193 (1890).



초상 등 사사의 영리적 이용 등으로부터 보호받는 것을 뜻한다.²⁾

현대에 들어와 정보기술의 발전과 정보화의 진전에 따라 개인에 관한 온갖 정보가 다양한 방식으로 수집·이용·제공·축적되어 개인의 사생활을 더욱 위협하게 되었다. 이처럼 정보사회에 있어서 정보화의 부작용으로 나타나는 사적 영역의 침해에 대응한 ‘정보 프라이버시’(informational privacy)는 중요한 권리로 인식되고 있다.

‘정보 프라이버시 권리’는 주로 개인이 자신에 관한 정보의 수집·공표·이용·유통을 결정하고 통제할 수 있는 ‘개인정보 자기결정권’의 형태로 구체화된다. 자기정보의 무단 수집·이용·제공의 금지, 자기정보의 열람 및 정정·보완 요구 뿐만 아니라 CCTV, 통신 도·감청, 직장에서의 이메일 감청 등을 통한 노동감시, 스마트폰 등 첨단 미디어를 이용한 위치추적 및 개인행동양식 탐지, 생체정보의 수집·이용 증가, 스팸메일, 인터넷상의 신상털기 등 정보처리기술의 고도화·지능화 및 이용·남용의 증대로부터의 사생활 보호 등 오늘날 사회문제화 되고 있는 다양한 이슈가 ‘개인정보 자기결정권’과 관련되어 있다. 전통적인 프라이버시 권리인 ‘홀로 있을 권리’는 소극적 권리의 성격이 강한 반면에, ‘정보프라이버시 권리’ 또는 ‘개인정보 자기결정권’은 소극적으로 ‘자기에 관한 정보가 없을 것’을 요구하는 권리에 머물지 않고 정보주체가 보다 적극적으로 ‘자기정보를 통제할 수 있는 권리’까지 내포하고 있다.

‘개인정보 자기결정권’은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보 자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보 자기결정권에 대한 제한에 해당한다.³⁾

2) 이상, 윤명선·김병목, 헌법체계론(I), 법률계, 520면.

나. 정보사회와 개인정보 보호의 중요성

정보사회에 있어서 개인정보는 유용한 수단·가치로서의 빛이자 다른 한편으로는 다양한 역기능을 내포하는 그림자라고 할 수 있다. 전 사회적인 정보화 진전과 정보기술에 대한 의존도가 커짐에 따라 개인정보는 기업의 영업활동과 수입창출을 뒷받침하는 영업자산이고, 공공·민간부문에 있어서 다양한 서비스 제공과 사회적 기능을 뒷받침하는 기반으로써 개인정보의 비즈니스 가치가 크게 증대되었다. 최근 스마트폰 등 정보기술의 발달로 새롭게 등장하는 많은 서비스는 대부분 개인정보의 활용에 기반한다.

한편 정보기술의 발달로 개인정보 수집경로의 다양화, 디지털 개인정보의 무한복제와 빠른 전파성으로 인해 개인정보의 유출과 침해 위험은 더욱 커지고 있다. 언제·어디서나 개인정보의 수집·편집·생성·복구·제공 등이 가능하게 되어 정보주체의 의지 또는 인지 여부와 관계없이 외부로 노출 또는 침해될 가능성이 있다. 이러한 침해사고의 원인으로는 개인정보의 고의적인 오·남용, 내부자 관리 부실로 인한 유출, 개인정보의 불법적 매매(제공), 개인정보 과다보유, 해킹 등 외부공격에 의한 유출, 업무위탁시 수탁자에 의한 유출 등 매우 다양하다.

개인정보 유출·침해의 심각성은 유출·침해된 개인정보를 이용·악용한 2차 피해에 있다. 유출·침해된 개인정보를 이용한 스팸메일 발송, 명예훼손, 해킹, 회원가입, 대포폰·대포통장 가입·신용카드발급·보이스피싱 등 신분증 위조, 명의도용과 경제적 손실 등의 피해 뿐만 아니라 심하면 사람의 납치·유인·살인 등 사람의 생명·신체에 대한 위해로까지 피해를 줄 수 있다. 단순 유출의 1차 피해는 정보주체 등의 심리적 측면에 피해를 주지만, 2차 피해는 정보주체의 경제적·사회적 생활영역에 실질적인 피해를 준다는 점에서 더욱 심각하다.

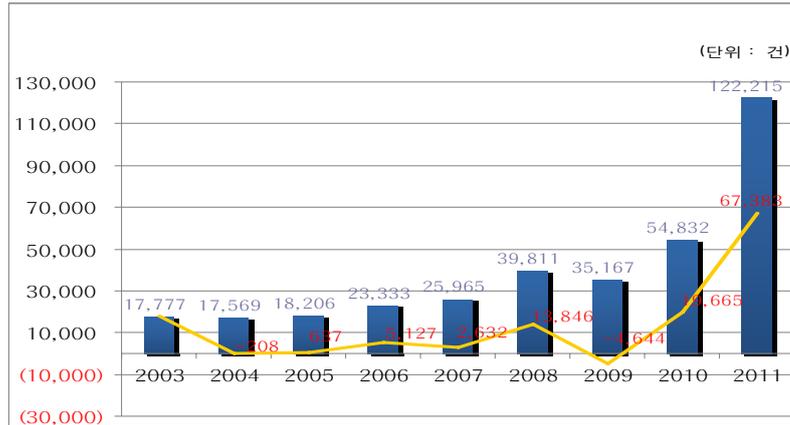
3) 헌법재판소 2005.5.26. 선고, 99헌마513 결정.



다. 개인정보의 유출 등에 따른 피해 현황

개인정보분쟁조정위원회와 개인정보침해센터에 접수된 개인정보 피해구제 신청 건수는 2003년 이후 매년 증가하고 있다. 특히 2011년 신청건수는 122,215건으로 2010년의 54,832건보다 약 223% 증가된 것으로 나타났다.

〈그림 1〉 연도별 (2003-2011) 개인정보 침해 상담 신청 건수



* 출처 : 인터넷통계정보 검색시스템(<http://isis.kisa.or.kr/>)

그리고 2007년 이후 개인정보 침해신고는 개인정보의 수집·이용·제공·파기 등 개인정보 처리의 전 과정에 걸쳐 이루어지고 있으며, 그 중에서 특히 ‘주민등록번호 등 타인 정보의 훼손·침해·도용’과 ‘기술적·관리적 조치 미비로 인한 개인정보누출’을 이유로 한 상담 신청이 큰 부분을 차지하고 있다.

〈표 1〉 연도별 개인정보 침해 상담 사유별 신청 건수

(단위 : 건, %)

항목	연도	2007	2008	2009	2010	2011
	건수	건수	건수	건수	건수	건수
	비율	(비율)	(비율)	(비율)	(비율)	(비율)
이용자의 동의 없는 개인정보수집	건수	1,166	1,129	1,075	1,267	1,623
	비율	(4.4)	(2.8)	(3.06)	(2.31)	(1.33)
개인정보 수집시 고지 또는 명시 의무 불이행	건수	7	6	15	75	53
	비율	(0.0)	(0.0)	(0.04)	(0.14)	(0.04)

과도한 개인정보 수집	51 (0.2)	87 (0.2)	115 (0.33)	146 (0.27)	379 (0.31)
고시·명시한 범위를 넘어선 이용 또는 제3자 제공	1,001 (3.9)	1,037 (2.6)	1,171 (3.33)	1,202 (2.19)	1,499 (1.23)
개인정보 취급자에 의한 훼손·침해 또는 누설	123 (0.5)	125 (0.3)	158 (0.45)	158 (0.29)	278 (0.23)
개인정보 처리 위탁시 고지의무 불이행	2 (0.0)	6 (0.0)	6 (0.02)	25 (0.05)	36 (0.03)
영업의 양수 등의 통지의무 불이행	14 (0.1)	9 (0.0)	6 (0.02)	22 (0.04)	64 (0.05)
개인정보관리책임자 미지정	10 (0.0)	26 (0.1)	10 (0.03)	21 (0.04)	38 (0.03)
기술적·관리적 조치 미비로 인한 개인정보누출 등	522 (2.0)	1,321 (3.3)	819 (2.33)	1,551 (2.83)	10,958 (8.97)
수집 또는 제공받은 목적 달성 후 개인정보 미파기	146 (0.6)	294 (0.7)	294 (0.84)	323 (0.59)	488 (0.40)
동의철회·열람 또는 정정 요구 불응	865 (3.3)	949 (2.4)	680 (1.93)	826 (1.51)	662 (0.54)
동의철회, 열람·정정을 수집보다 쉽게 해야 할 조치 미이행	461 (1.8)	503 (1.3)	603 (1.71)	630 (1.15)	800 (0.65)
법정대리인의 동의 없는 아동의 개인정보 수집	14 (0.1)	27 (0.1)	19 (0.05)	35 (0.06)	71 (0.06)
주민등록번호 등 타인정보의 훼손·침해·도용	9,086 (35.0)	10,148 (25.5)	6,303 (17.92)	13,137 (18.49)	67,094 (54.90)
「정보통신망법」 적용대상 이외의 개인정보침해(신용정보침해 등)	12,497 (48.1)	24,144 (60.7)	23,893 (67.94)	38,414 (70.06)	38,172 (31.23)
합계	25,965 (100)	24,144 (100)	35,167 (100)	54,832 (100)	122,215 (100)

* 출처 : 인터넷통계정보 검색시스템(<http://isis.kisa.or.kr>)



그동안 공공부문·민간부분에 있어서 크고 작은 개인정보 피해사고가 많이 발생하였으며, 유출된 개인정보의 규모가 상당한 수준에 이르고 있다. <표 2>는 2005년 이후 민간부분에서 발생한 주요 개인정보 유출사례를 정리한 것이다.

<표 2> 민간부분의 주요 개인정보 유출사례

날 짜	업 체	피해 내용(출처)	법적 책임
2005.5	엔씨소프트	게임서버 업데이트시 이용자 개인정보파일을 암호화하지 않아 ID와 비밀번호 노출(2005.5.18, 연합뉴스)	1심: 50만원, 2·3심: 10만원 배상 판결
2006.2	엔씨소프트	온라인게임 '리니지'불법 명의도용에 의한 대 규모 계정 개설(2006.2.13, 매일경제)	
2006.3	국민은행	직원의 부주의로 인터넷 복권 구매 안내메일에 32,277명의 발송대상 고객명단을 파일첨부하여 발송(2006.3.16, 한국일보)	1심: 이름·이메일 유출 7만원, 주민번호 포함시 10만원 2심: 각 10만원, 20만원 배상판결
2006.9	LG전자	홈페이지 해킹으로 입사지원서의 개인정보 유출(2006.9.27, 아이뉴스24)	70만원 배상판결
2008.2	옥션	1,081만여 명의 개인정보 해킹, 이 중 900여 만명의 이름, 주민번호, 환불정보, 은행계좌 번호 등 유출(2008.2.5, 머니투데이)	무혐의
2008.4	하나로텔레콤	전·현직 임직원이 51만여 고객의 이름·주민번호·주소·전화번호 등 개인정보 8,500만여 건을 텔레마케팅업체에 불법으로 제공(2008.4.24, 전자신문)	동의없이 수집·이용 20만원, 무단 제공 10만원 배상판결. 회사 등 벌금형
2008.7	LG유플러스	벨소리 다운로드 서비스시 주민번호, 핸드폰 기종, 가입일 등 노출(279명 소송)(2009.11.6, 보안뉴스)	1심: 5만원 배상 판결, 2심 원고패소
2008.9	GS칼텍스	GS칼텍스 보너스 회원 1,100만 명의 개인정보가 CD와 DVD에 담겨 유출(2008.9.5, 이데일리)	
2010.3	신세계몰 등 25개 업체	중국 해커가 국내의 유명 백화점, 도박 사이트, 골프용품 판매사 등 25개 업체 홈페이지를 해킹하여 개인정보 2,000만건 유출	

		(2010.3.12, 스포츠경향)	
2011.4	현대캐피탈 (2011.4.10, MK뉴스)	회원 수 175만 명의 현대캐피탈 고객 중 23%인 42만 명의 이름과 이메일 주소, 주민등록번호, 휴대전화 번호, 신용등급 등 유출	
2011.5	세티즌	휴대폰사이트 '세티즌' 해킹으로 140만명의 개인정보 유출(2011.5.21, 아시아투데이)	
2011.6	대부업체, 저축은행, 채팅사이트 등	중국인 해커와 공모하여 3,000만건의 개인정보 해킹 후 인터넷에서 거래(2011.6.24, 동아일보)	
2011.7	SK컴즈	SK컴즈의 자회사인 네이트와 싸이월드 가입자 3,560만 명의 개인정보 유출(2011.7.28, 디지털데일리)	100만원 지급명령(소송 중)
2011.8	삼성카드	직원이 서버를 해킹하여 고객정보 192만건 조회, 47만건 유출(2011.9.5, 이데일리)	
2011.11	넥슨	해킹으로 게임 이용자 정보 1,320만건 유출(2011.11.27, 전자신문)	
2012.4	대리운전업체 등	대리운전 운행정보 관리업체를 해킹해 빼낸 운행정보(고객 전화번호, 행선지, 요금, 대리운전기사 정보 등) 2,600여만건을 구입해 1,300만원에 판매한 혐의(2012.4.4, 뉴스스)	

2. 개인정보 보호의 국제적 동향

1970년대 이후 컴퓨터에 의한 정보처리가 확대됨에 따라 스웨덴, 미국 등 선진각국과 국제기구에서는 정보 프라이버시 권리 또는 개인정보 자기결정권의 보호를 위한 법·제도 마련 등 구체적인 논의가 폭넓게 진행되었다. 개인정보 보호 논의의 초기에는 정부기록에 있어서의 개인비밀 보호가 주된 이슈이었으나, 차츰 통신비밀, 의료기록, 재산·신용정보, 소비정보 등으로 그 보호범위가 확대되어 왔다.

스웨덴이 1973년 세계 최초로 개인정보보호를 위해 데이터법(Data Act)을



제정하였다. 이 법은 공공·민간부문 모두에 있어서 컴퓨터로 처리되는 개인데이터를 규제하며, 이를 위해 개인데이터시스템의 설치·보유시 특별감독기관(데이터검사원)의 허가를 얻도록 하고, 특정 종류의 데이터의 입력금지, 개인의 자기기록 열람권, 부정확한 데이터에 의한 손해배상청구권을 인정하였다. 이 법은 EU 지침(1995)에 따라 새롭게 제정된 개인정보법(Personal Information Act, 1998)에 의해 대체되었다.

이후 1974년 미국의 프라이버시법(Privacy Act), 1977년 독일의 연방데이터보호법, 1978년 프랑스의 '정보처리·축적 및 자유에 관한 법률', 1983년 캐나다의 공공부문 프라이버시법, 1984년 영국의 데이터보호법, 1988년 일본의 '행정기관이 보유하는 전자계산기처리에 따른 개인정보의 보호에 관한 법률' 등 많은 나라가 개인정보 보호를 위한 법체계를 마련하였다.⁴⁾

미국의 경우에는 1974년 프라이버시법 제정 이후에도 통신, 의료, 소비자 등 각 분야별로 다양한 프라이버시 보호법을 제정하였고, 2002년에 제정된 전자정부법에서는 프라이버시 영향평가제도를 도입하였다. 캐나다도 2001년 '민간부문 개인정보보호·전자문서법'을 제정하고, 2002년 프라이버시 영향평가 의무시행 제도를 도입하였다. 그리고 일본은 2003년 5월 '개인정보의 보호에 관한 법률' 등 5개의 법률을 제정하여 개인정보 보호법제를 정비하였다.⁵⁾

1980년대 들어 정보통신기술의 발전으로 개인정보의 보호 필요성이 더욱 강하게 대두되었고, 이에 국제기구들도 이를 위한 여러 지침을 제시하기 시작하였다. 가장 먼저 OECD는 1980년 '프라이버시 보호와 개인정보의 국제유통에 관한 지침'을 통하여 각국의 개인정보 보호를 위한 노력과 국내 입법의 제정을 권고하면서 유명한 8개의 국내적용 기본원칙(Basic Principles of National Application)을 제시하였다. 그리고 UN은 1990년 '전산처리된 개인정보파일의 규제 지침'(Guideline for the Regulation of Computerized Personal Data

4) 2000년 이전까지 주요국가의 입법동향은 이규정, 주요국의 정보화 법·제도 개선 동향(한국정보화진흥원, 1999), 28-38면 참조.

5) 5개 제정법률은 1) 개인정보의 보호에 관한 법률, 2) 행정기관이 보유한 개인정보의 보호에 관한 법률, 3) 독립행정법인등이 보유한 개인정보의 보유에 관한 법률, 4) 정보공개·개인정보보호심사회설치법, 5) 행정기관이 보유한 개인정보의 보호에 관한 법률 등의 시행에 따른 관계법률의 정비 등에 관한 법률이다.

Files)에서 개인정보파일을 규율하는 6개 원칙을 제시하여 회원국이 개인정보에 관한 입법이나 규율시 참고하도록 하였으며,⁶⁾ APEC도 2005년 Working Group 활동을 통해 9개의 프라이버시 보호원칙을 제시하였다.

〈표 3〉 국제기구의 개인정보 보호 원칙 비교

OECD	UN	APEC
수집제한의 원칙	합법성과 공정성의 원칙	수집제한의 원칙
정보내용 정확성의 원칙	정확성 원칙	정확성의 원칙
목적 명확성의 원칙	목적구체화의 원칙	
이용제한의 원칙	-	이용제한의 원칙
안전성 확보의 원칙	안전성의 원칙	안전성의 원칙
-	-	침해방지의 원칙
공개성의 원칙	-	
개인 참여의 원칙	개인접근의 원칙	선택권 보장의 원칙
-	비차별 원칙	고지의 원칙
-	-	정보접근권의 원칙
책임의 원칙	-	책임의 원칙

또한 유럽연합(EU)은 회원국 국민의 기본권과 자유를 보호하고 개인정보처리와 관련한 프라이버시권을 보호하며 EU 국가간의 개인정보의 자유로운 유통을 촉진하기 위하여 1995년10월 ‘개인데이터의 처리와 개인데이터의 자유로운 유통에 관련된 개인정보 지침’을 채택하고, 1997년 12월에는 ‘정보통신부문에 서의 개인정보 처리 및 프라이버시보호에 관한 지침’, 1999년 2월에는 ‘정보고속도로에서 신상정보의 수집처리와 관련한 개인의 보호를 위한 지침’ 등을 채택하였다.

한편 개인정보의 보호를 위한 각국의 개인정보 보호기구(Data Protection

6) 6개 원칙은 ① 합법성과 공정성의 원칙(Principle of Lawfulness and Fairness), ② 정확성의 원칙(Principle of Accuracy), ③ 목적구체화의 원칙(Principle of the Purpose-specification), ④ 개인접근의 원칙(Principle of Interested-person Access), ⑤ 비차별 원칙(Principle of Non-discrimination), ⑥ 안전성 원칙(Principle of Security)을 말한다.



Authority) 연합체로서 각 국가의 개인정보 보호현황을 모니터하고 정보보호를 위한 국제적 협력을 위하여 조직된 국제기구로 국제개인정보보호기구회의(ICDPPC: International Conference of Data Protection and Privacy Commissioners)가 2001년 발족되었다. ICDPPC는 당초 EU 개인정보보호기구간의 정보교류를 위한 회의(Conference)로 출발하였으나, 2001년 2월부터 참여범위를 EU 외로 확대하면서 국제기구(협의체) 성격으로 변화하였다. 현재 영국, 호주, 캐나다 등 47개국 77개 개인정보보호기구가 회원으로 등록되어 있다.

3. 우리나라 개인정보 보호제도의 발전

가. 개인정보 보호법제의 연혁

1970~80년대 미국, 스웨덴, 독일, 프랑스, 일본 등 각국의 정보 프라이버시 권리 강화를 위한 입법 노력과 여러 국제기구의 개인정보보호 움직임은 우리나라의 개인정보보호법 제정에 영향을 미쳤다. 또 1980년대 중반부터 시작된 국가기간전산망사업으로 인한 개인정보의 광범위한 수집·보관·이용으로부터 개인의 사생활 보호를 위한 제도적 장치 마련 요구도 컸었다.

그리하여 정부는 외국의 입법례와 학계의 연구성과 등을 반영하여 1994년 1월 7일 「공공기관의 개인정보보호에 관한 법률」(법률 제4743호)을 제정하였다. 전체 5개 장 25개 조 및 부칙으로 구성된 이 법은 정부 등 공공기관을 적용대상으로 하였으며, 1995년 1월 8일 시행되었다. 한편 국민의 통신 및 대화의 비밀과 자유를 보장하기 위하여 전기통신의 감청과 우편물 검열 등의 대상을 한정하고 엄격한 법적 절차를 거치게 함으로써 사생활의 비밀과 통신의 자유를 구현하고자 1993년 12월 27일 「통신비밀보호법」(법률 제4650호, 1994.6.28 시행)이 제정되었다.

1995년 1월 5일에는 신용정보업을 건전하게 육성하고 신용정보의 효율적 이용과 체계적 관리를 기하는 한편, 신용정보의 오·남용으로부터 사생활의 비밀등을 적절히 보호함으로써 건전한 신용질서를 확립하기 위하여 「신용정보의 이용 및 보호에 관한 법률」(법률 제4866호, 1995.7.6 시행)이 제정되었다.