법 학 석 사 학 위 논 문

지능정보화사회에서의 개인정보자기결정권에 관한 연구

2023년 2월

부 경 대 학 교 대 학 원

법 학 과

허 미 래

법 학 석 사 학 위 논 문

지능정보화사회에서의 개인정보자기결정권에 관한 연구

지도교수 지 규 철

이 논문을 법학석사 학위논문으로 제출함.

2023년 2월

부 경 대 학 교 대 학 원

법 학 과

허 미 래

허미래의 법학석사 학위논문을 인준함

2023년 2월 17일

위 원 장 법학박사 박 종 원 (인)

위 원 법학박사 김 혁 (인)

위 원 법학박사 지 규 철 (인)

≪목차≫

【표 목차】

지능정보화사회에서의 개인정보자기결정권에 관한 연구

허 미 래

부경대학교 대학원 법학과

【국 문 요 약】

이 연구는 전 세계적으로 직면한 지능정보화사회에서 정보통신기술의 발전에 따라 개인정보가 위협받는 새로운 정보환경에 처하게 되었고, 개인정보를 보호하고 정보주체의 권리를 헌법상 적극적으로 보호하기 위하여 개인정보자기결정권을 강화하기 위한 방향을 제시하는 데 목적이 있다. 이를 위하여 연구의 배경환경인 지능정보화사회의 특징과 개인정보의 침해유형을 분석하여 개인정보 보호의 중요성을 선제적으로연구한다. 그리고 자기 자신의 정보를 정보주체가 스스로 결정하고 통제할 수 있는 권리인 개인정보자기결정권을 살펴보고, 적극적 청구권으로서의 개인정보자기결정권의 기능을 중점으로 보호의 필요성을 강조하고 있다.

지능정보화사회에서 선제적으로 개인정보를 보호하고 정보주체의 권리를 강화하고 있는 해외 주요국들의 개인정보 보호법제를 유럽연합(EU)의 GDPR(General Data Protection Regulation), 독일, 프랑스, 영국, 미국, 일본 순으로 소개하고, 해외 개인정보 보호법제의 시사점으로 대두된 '잊힐 권리'의 동향을 살펴 개인정보자기결정권을 헌법상 새로운 기본권으로 정립해야 할 필요성을 찾고자 한다.

개인정보자기결정권을 구체적 제도로서 구현한 국내의 개인정보 보호법제를 법제의 제정 배경, 2016년 정부의 개인정보 비식별조치 가이드라인, 최근 개정된 현행 개인정보 보호법제와 같이 시대적 흐름으로 연구한다. 이후 현행 개인정보 보호법제의 문제점을 1)정보주체의 동의제도에 의존하고 있으나, 사실상 실효적이지 않고 무책임하여 개인정보자기결정권을 실질적으로 보장하지 못하는 문제점, 2)가명정보의 도입에 따라, 가명정보의 범주 및 활용범위가 불명확하여 개인정보 결정권과 통제권 또한 설정이 명확하지 않다는 문제점, 3)정보통신서비스제공자에 대한 특례조항에서 동의를 받을 때 고지사항 중 동의거부권을 제외하여 일반조항과 규제수준을 달리할 뿐만 아니라, 동의거부권은 정보주체의 중요한 권리 중 하나임에도 고지의무를 제외한 문제점, 4)개인정보보호 감독기구인 개인정보보위원회의 완전하지 않은 독립성의 문제점을 지적하며 법적 개선방향을 모색하고 있다.

주제어 : 개인정보자기결정권, 지능정보화사회, 정보주체의 권리, 개인정보 보호, 개인정보 보호법제, GDPR, 잊힐 권리, 동의제도, 가명정보, 동의거부권, 개인보보호위원회

제1장 서론

제1절 연구의 목적

우리 사회는 과거 산업화 사회와 정보화 사회를 거쳐 4차 산업혁명의 주도적 영향으로 지능정보화사회에 이르게 되었다. 지능정보화사회는 3차 산업혁명이 산출한 지식정보사회에 대응하는 개념으로 지식정보사회가 새롭게 진화한 시대이다. 정보기술(IT)의 등장으로 가시화된 3차 산업혁명의 산물인 지식정보사회가 인터넷을 통해 축적된 지식과 정보가 사회의 중요하고 핵심적인 자원이 되었다는 것을 보여주었다면, 4차 산업혁명의 산물인 지능정보화사회는 초고속 연결망을 통해 축적되는 빅데이터가 단순히 자원의 성격을 넘어 인공지능과 같은 새로운 지능체계가 공존하는 새로운 사회의 모습을 보여 주고 있다.

지능정보화사회의 도래는 경제와 사회구조 등 전반에서 근본적 변화를 가져오고 있다. 뿐만 아니라 지능정보기술의 발전은 다양한 헌법적, 사회적 문제를 야기하고 있고 이러한 새로운 시대에서 개인정보는 핵심자원이라고 할 수 있다. 이에 과거와는 비교할 수 없을 정도로 방대한 개인정보가 생산·수집·유통되고 있다. 개인정보의 수집부터 활용까지의 각각의 과정에서 개인정보는 무차별적으로 침해받고 있고, 지능정보화가 가속화 될수록 개인정보의 집적과 무작위한 오남용도 가속화 되고 있다.

이러한 시대에서 개인정보의 주체가 되는 정보주체는 자신에 관한 정보의 전파에 대하여 통제력을 행사하지 못함에 따라 인간으로서 존엄과 가치를 존중받지 못하는 문제가 발생하고 있고, 정보주체의 권리는 헌법상 보호할 필요성이 있는 대상이 되었다. 정보기술의 발달이 주는 위험성으로부터 개인정보를 보호함으로써 궁극적으로 개인의 결정의 자유를 보호하고 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여[1] 최

소한의 헌법적 보장장치로서 개인정보자기결정권은 그 의의가 있다.

정보주체의 동의권, 개인정보의 열람청구권, 개인정보 정정청구권과 삭제 및 차단청구권, 개인정보의 처리정지 요구권, 손해배상권 등과 같은 내용으로 개인정보와 정보주체의 권리보호를 강화하고 있는 개인정보자기결정권을 소극적인 방어권이 아닌 적극적 청구권으로 해석하여 권리 행사를 위한 조직과 절차라는 규범적 형성으로 그 실효성을 강조하고자 한다.

지능정보화사회의 개인정보 보호 정책으로 유럽연합(EU)은 GDPR(General Data Protection Regulation)을 제정하여 선제적으로 개인정보를 보호하고자 하였다. EU의 GDPR을 반영하여 정보주체의 권리를 강화하고 있는 해외 주요국의 개인정보 보호법제들을 통해 이들이 시사하는 점을 '잊힐 권리'를 중점으로 연구하여, 개인정보자기결정권의 새로운 기본권으로서의 헌법적 근거를 찾고자 한다.

새로운 환경변화에 직면하면 개인정보 보호에 관한 인식도 새롭게 개선되어야 한다. 우리나라도 지능정보화사회의 시대적 흐름에 상응하는 개인정보 보호정책으로 2020년 4월 「개인정보 보호법」을 개정하였다. 개정 「개인정보 보호법」에서도 정보주체에게 자신의 개인정보 처리에 관한 권리를 보장하고 있으며, 정보주체인 개인의 정보에 대한 통제권을 강력하게 행사할 수 있다는 의미에서 개인정보 보호법제를 선제적으로 연구한다.

이후 본 연구는, 개정된 현행 개인정보 보호법제의 정보주체의 동의권에 관하여 사실상 실효적이지 않고 무책임하여 개인정보자기결정권을 실질적으로 보장하지 못하는 문제점, 가명정보의 범주 및 활용범위가 명확하지 않아 정보의 결정권과 통제권 설정 또한 명확하지 않은 문제점, 정보통신서비스제공자에 대한 특례조항에서 동의를 받을 때 고지사항 중 동의거부권을 제외하여 일반조항과 규제수준을 달리할 뿐만 아니라, 정보주체의 중요한 권리임에도 고지의무를 제외한 문제점, 개인정보보호 감독기구인 개인정보보호위원회의 실질적 독립성 보장이 어려운 문제점들을 지적하여, 합리적이고 실현가능한 개선방향을 제안함으로써 보다 적극적으로 정보주

1) 헌재 2005. 5. 26. 99헌마513 등

체의 권리를 보호하고 개인정보자기결정권을 강화하기 위한 방향을 제시하고자 한다.

제2절 연구의 범위와 방법

제1장에서는 연구의 목적과 연구의 범위 및 방법을 제시하며 연구를 시작한다.

본격적으로 연구에 착수하기 전에 선행되어야 할 것은 지능정보화사회에 대한 이해이다. 제2장에서는 직면하고 있는 사회의 올바른 이해를 위하여 지능정보화사회의 개념을 명확히 하고자 한다. 지능정보화사회는 여러 가지 특징을 가지고 있으나 가장 뚜렷하게 나타나는 인공지능(AI)의 발전, 빅데이터 시대인 데이터 기반 사회, 인간과 인간, 인간과 사물, 사물과 사물이 네트워크로 연결된 사회인 초연결 사회로 나누어 살펴본다. 정보통신기술의 발전으로 개인정보를 광범위한 범위와 목적으로 이용하는 것이 가능해 졌고, 정보주체의 권리를 침해할 수 있는 개인정보의 이용에 대처하기 위하여 개인정보의 개념을 정확히 알아본다. 개인정보의 개념요소를 법률상 개인정보와 헌법상 개인정보의 개념으로 구분하여 정리하고, 지능정보화사회에서 개인정보가 침해되고 있는 심각성을 유형별로 검토하여 개인정보 보호의 중요성을 강조한다. 또한 과거의 개인정보 보호의 의미와 현재 지능정보사회에서의 개인정보 보호의 의미를 국가의 기능과 같은 헌법적 시각으로 정리하고, 개인정보 보호의 필요성 또한 헌법적 근거로 찾고자 한다.

제3장에서는 자기 자신의 정보를 정보주체가 스스로 결정하고 통제할 수 있는 권리인 개인정보자기결정권을 연구한다. 개인정보자기결정권의 내용을 정보주체의 동의권, 개인정보의 열람청구권, 개인정보 정정청구권과 삭제 및 차단청구권, 개인정보의 처리정지 요구권, 손해배상청구권을 주요내

용으로 정리한다. 개인정보자기결정권을 방어권으로서의 법적 성격과 적극적 청구권으로서의 법적 성격으로 구분하여 논하고, 적극적 청구권으로서 개인정보자기결정권의 기능을 중점으로 하여 그 필요성을 강조한다.

또한 개인정보자기결정권에 대한 3가지 주요이론을 정리하여, 헌법적 근거를 헌법 제10조 및 제17조, 헌법재판소의 결정에서 찾으며, 개인정보자기결정권의 보장과 헌법적으로 보호할 필요성의 의의를 넓히고자 한다.

제4장에서는 선제적으로 개인정보를 보호하고 정보주체의 권리를 강화하고 있는 해외의 개인정보 보호법제에 대하여 연구한다. 유럽연합(EU), 독일, 프랑스, 영국, 미국, 일본 순으로 정리하고, 특히 새롭게 직면한 사회의 정보기술 발전에 대응하기 위하여 새로운 개인정보보호 관련 규범을 대표적으로 마련한 EU의 GDPR에 대하여 깊이 있게 살펴본다. 이후 해외 주요국들의 개인정보 보호법제가 시사하는 다양한 논제들을 정리하고, 주요 시사점인 '잊힐 권리'의 동향을 살펴 개인정보자기결정권을 새로운 기본권으로서 정립할 헌법적 근거를 찾고자 한다.

제5장에서는 국내의 개인정보 보호법제를 연구한다. 개인정보자기결정권을 구체적 제도로 구현한 국내 개인정보 보호법제의 역사, 2016년 정부의 개인정보 비식별조치 가이드라인 정책, 최근 개정된 현행 개인정보 보호법제를 시대적 흐름으로 연구한다. 특히, 현행 개인정보 보호법제의 범위를 데이터 3법이라 불리는 개인정보보호법, 정보통신망법, 신용정보법의 주요 내용으로 정리한다.

제6장에서는 제5장에서 살펴본 현행 개인정보 보호법제의 문제점을 1)정보주체의 동의제도에 의존하고 있으나, 사실상 실효적이지 않고 무책임하여 개인정보자기결정권을 실질적으로 보장하지 못하는 문제점, 2)가명정보의 도입에 따라, 가명정보의 범주 및 활용범위가 불명확하여 개인정보 결정권과 통제권 또한 설정이 명확하지 않다는 문제점, 3)정보통신서비스제공자에 대한 특례조항에서 동의를 받을 때 고지사항 중 동의거부권을 제외하여 일반조항과 규제수준을 달리할 뿐만 아니라, 동의거부권은 정보주체의 중요한 권리 중 하나임에도 고지의무를 제외한 문제점, 4)개인정보보호 감독기구인 개인

정보보위원회의 완전하지 않은 독립성의 문제점과 같이 지적하며, 법적 개선 방향을 모색한다.

마지막으로 세계적으로 이행중인 지능정보화사회에서 정보주체의 권리인 개인정보자기결정권의 보장과 중요성을 재차 강조하며, 철저한 입법적 대처가 필요함을 언급하며 연구를 맺는다.

제2장 지능정보화사회와 개인정보의 보호

제1절 지능정보화사회의 의의

Ⅰ. 지능정보화사회의 개념

과거 산업화 사회와 정보화 사회를 넘어서 4차 산업혁명의 영향으로 지능정보화사회가 점차 확대되어 가고 있다. 이는 국가정보화 기본법이 지능정보화 기본법으로 전부개정되면서 밝힌 개정이유나 지능정보화 기본법 제1조에서 인공지능, 데이터, 5G 등 첨단기술의 혁신적 발전으로 초연결·초지능 기반의 4차 산업혁명 패러다임에 접어들고 있는바, 4차 산업혁명에 따른 사회적, 경제적 변화에 선제적으로 대응하기 위해 범국가적인 추진체계 구축과 기술혁신을 위한 정비가 필요하다는 점을 명시함으로써 지능정보사회에 직면하게 되었음을 알 수 있다.[2)]

지능정보사회의 도래를 촉진하는 밑바탕은 지능정보 기술로서, 데이터 활용기술과 인공지능 기술의 유기적인 결합을 통해 인간의 지적활동 능력을 기계에 구현하는 것이다. 즉, 인지, 학습, 추론 등을 비롯한 인간의 지적인 정보처리 활동을 분석하는 인공지능 기술 그리고 데이터를 실시간으로 수집, 전달, 저장, 분석하는 데이터 활용기술 간 접목이 바로 지능정보 기술이다.[3)]

---

2) 「지능정보화 기본법」 [시행 2021.6.10.] [법률 제17344호, 2020.6.9., 전부개정] 본문 및 제정·개정 이유 참고. 동 법률 제2조 제5호에서 지능정보화를 "정보의 생산·유통 또는 활용을 기반으로 지능정보기술이나 그 밖의 다른 기술을 적용·융합하여 사회 각 분야의 활동을 가능하게 하거나 그러한 활동을 효율화·고도화하는 것"이라 정의하였고, 제6호에서 지능정보사회를 "지능정보화를 통하여 산업·경제, 사회·문화, 행정 등 모든 분야에서 가치를 창출하고 발전을 이끌어가는 사회"라고 정의하였다.

3) 김민우·김일환, "지능정보사회에서 민감정보의 보호와 이용을 위한 법제 정비방안 연구", 「서울법학」 제29권 제2호, 2021.8.31., 81면.

지능정보사회는 지능정보기술(고도화된 정보통신기술 인프라를 통해 생성, 수집, 축적된 데이터와 인공지능이 결합한 기술)이 경제, 사회, 삶 모든 분야에 보편적으로 활용됨으로써 새로운 가치가 창출되고 발전하는 사회를 말한다. 지능정보사회의 전 단계를 이루는 정보사회는 후기 산업사회 또는 탈공업사회로도 불리며 산업사회에서의 자본과 동력 대신에 지식과 정보가 전략적으로 중요시되고 사회의 자본으로 변화되는 사회인데, 정보사회의 기반을 마련한 것은 정보통신기술의 발전이었다.[4] 정보사회와 지능정보사회를 비교해볼 때, 정보사회가 인터넷 네트워크를 바탕으로 한 자동화와 기계화가 시작된 시기였다면, 지능정보사회는 더 진보한 기술을 바탕으로 더 긴밀한 연결, 더 방대한 데이터 분석으로 성과·확산이 현실화되는 시기이며, 지능정보사회는 인공지능(AI)을 장착한 지능화된 기계가 일정한 영역에 있어서 인간처럼 생각하고 판단한다는 점에서 정보사회와 구별된다.[5] 이에 따라 지능정보사회는 기존의 정보사회와 비교할 때 다음과 같은 차이와 특징을 가진다.[6]

우선, 지능정보사회에서는 인터넷을 기반으로 하던 정보화 혁명 대신, 사물인터넷을 기반으로 하는 초연결 혁명이 사회의 근저를 이루고, 초연결사회에서 수집, 분석, 처리되는 데이터가 중심이 된다. 따라서 다양한 경제주체들이 인터넷을 통해 경제활동을 하던 네트워크 경제에서 모든 만물이 사물인터넷상에서 연결·융합되어 새로운 가치를 창출하는 인터넷 융합경제가 도래하게 될 것이다.

그리고, 모든 영역의 경계가 파괴됨으로써 혁신을 가져오게 될 것이다. 정보사회에서는 기업과 국민, 정부가 서로의 영역에서 생산성을 증진시킨 반면, 지능정보사회에서는 이들 모두가 협업을 통해 어느 영역과도 결합이

---

4) Daniel Bell, “Communication Technology – For Better or For Worse?”, Jerry L. Salvaggio,Telecommunications: Issues and Choices for Society (New York and London: Longman, 1983), at 34-50.

5) 김민호·이규정·김현경, “지능정보사회의 규범설정 기본원칙에 대한 고찰”, 성균관법학 제28권 제3호, 2016. 9., 285면.

6) 이원태·문정욱·류현숙, “지능정보사회의 공공정보화 패러다임 변화와 미래정책 연구”, KISDI(정보통신정책연구원) 기본연구 17-01, 2017. 10., 30-31면.

가능한 융합서비스를 추구하면서 더 큰 효용가치와 사회적 파급효과를 가져올 것으로 기대된다. 이는 빅데이터와 인공지능 기술이 방대한 데이터를 분석하여 판단함으로써 그 활용범위와 영역 간 경계를 허물기 때문이다.[7)]

Ⅱ. 지능정보화사회의 특징

1. 인공지능(AI)의 발전

인공지능 기술은 대체로 세 시기를 거치며 확산·발전하였다. 제1차 인공지능시대(1950~1960)는 '추론·탐색의 시대'이며, 제2차 인공지능시대(1980~1995)는 '지식의 기술, 관리의 시대'이고, 현재의 제3차 인공지능시대(2000~)는 딥 러닝(Deep Learning)을 필두로 알고리즘의 개선, 빅 데이터와 컴퓨팅 파워의 발전과 함께 비약적으로 발전하고 있다.[8)] 미국의 미래학자 레이 커즈와일(Ray Kurzweil)은 2045년에는 인공지능이 인간지성을 추월한다고 예측하기도 하였다.[9)]

이렇게 인공지능의 역사가 60여년을 넘는 동안에도 인공지능에 대한 정의는 아직 명확하게 내려지지 못하고 있다. 그것은 '지능'에 대한 개념 정의가 쉽지 않고, 인공지능에 대한 철학적 논쟁과 함께 법률적·윤리적 문제와 결부되면서 더욱 복잡한 양상이 전개되고 있기 때문이다.[10)]

이러한 가운데에서도 기술적·시스템적 측면에서 볼 때, 인공지능이란 인간의 학습능력과 추론능력, 지각능력, 자연언어의 이해능력 등을 컴퓨터 프로그램으로 실현한 기술이며, 인간의 지능으로 할 수 있는 사고, 학습, 자기개발 등을 컴퓨터가 할 수 있도록 하는 방법을 연구하는 컴퓨터 공학 및

---

7) 김배원, "지능정보사회와 헌법 - 인공지능(AI)의 발전과 헌법적 접근-", 「공법학연구」 제21권 제3호, 비교공법학회, 2020.8., 70-71면.
8) 고선규, "인공지능과 어떻게 공존할 것인가?", 타커스, 2019. 26면.
9) Ray Kurzweil, The Singularity is Near, 2005.
10) 고선규, 위의 책(註 8), 26-27면.

정보기술의 한 분야로서, 컴퓨터가 인간의 지능적인 행동을 모방할 수 있도록 하는 것을 말한다고 할 것이다.[11]

인공지능은 일종의 소프트웨어 또는 프로그램으로서 스스로 학습하고 결과물을 산출해 내는 알고리즘에 의해 구성된다. 알고리즘이란 "컴퓨터 혹은 디지털 대상이 과업을 수행하는 방법에 대한 설명으로 명확히 정의된 한정된 개수의 규제나 명령의 집합을 말하는데,[12] 이러한 알고리즘은 학습 결과에 따라 그 자체를 수정하고 재생산해 내기도 한다.[13]

알고리즘으로 구성된 인공지능의 사회·경제적 활용이 급증하고 있지만, 과연 알고리즘이 공정하고 중립적이며 객관적인가에 대한 문제들이 지속적으로 제기되고 있다. 알고리즘이 내리는 자동화된 의사결정에는 우선순위 결정, 분류, 관련짓기, 필터링이라는 과정이 존재하는데, 이 과정이 인간 개입에 따른 오류와 편향성, 검열의 가능성 등 본질적으로 차별적인 성격을 내포하기 때문이다. 알고리즘은 정의된 명령에 따라서만 작동하는 것이 아니라 이용하는 사람 혹은 객체와의 상호작용 속에서 끊임없이 수정 및 조정되므로 인간(소프트웨어 개발자)의 편견이나 선입견이 반영될 가능성이 상존한다. 특히, 알고리즘은 과거로부터 쌓여온 데이터를 학습하면서 인종 차별, 성차별 등 역사적 편향성을 반영할 가능성도 매우 높다.[14]

2. 데이터 기반사회

지능정보사회는 데이터 기반사회 또는 데이터 경제시대라는 말로 표현되기도 한다. 종래 데이터의 개념은 단순히 저장이나 수집된 정보 그 자체만을 의미하였으나 오늘날의 빅데이터는 기존 데이터의 수집·저장·관리·

---

11) 김배원, 앞의 논문(註 7), 73면.
12) 이원태, "EU의 알고리즘 규제 이슈와 정책적 시사점", KISDI16-12 Premium Report, 2016. 12. 26., 4면.
13) 심우민, "인공지능의 발전과 알고리즘의 규제적 속성", 법과 사회 53호, 2016. 12., 56면.
14) 이원태, 위의 논문(註 12), 4-5면.

분석의 역량을 넘어서는 대량의 정형 또는 비정형의 데이터세트 및 이러한 데이터로부터 가치를 추출하고 결과를 분석하는 기술을 말한다.[15]

이러한 빅데이터는 민간분야에서 기업들이 광범위하게 활용하고 있으며, 공공분야에서도 국가안보, 재난대응(자연재해・전염병감염 예방 등), 범죄예방, 교통체계 개선이나 교통사고 감소, 맞춤형 복지행정 등에서 활용되고 있다.[16]

기업들은 그들이 보유하고 있는 방대한 고객자료를 이용해 고객분석을 하고 다양한 마케팅에 활용한다. 외국의 대표적인 빅데이터 활용의 경우 구글의 자동번역 시스템, IBM의 슈퍼컴퓨터 왓슨, 아마존의 도서 추천 시스템 등이 대표적인 사례이고, 국내의 대표적인 빅데이터 활용의 경우는 카드사의 업종별 구매 분석을 활용한 마케팅, 보험사의 보험사건 이력분석을 통한 보험사기 사건 발견에 이용되는 것 등이 예이다.[17]

공공분야에서도 위험 예측을 활용한 위험 관리시스템, 공공기관 서비스 개선 프로젝트, 탈세 등 부정행위방지 시스템, 공공데이터 공개 시스템 등 다양한 분야에서 빅데이터를 활용하기 시작하고 있는데, 국내에서는 의료정보 데이터 자료를 활용하여 맞춤형 건강관리 서비스를 국민건강 보험공단에서 실시하고 있는 것이 예가 된다.[18]

이와 같이 빅데이터가 지능정보사회의 총아로서 민간・공공분야를 가릴 것 없이 널리 활용되고 있음에도 불구하고, 빅데이터에 개인정보가 포함되어 있다는 점에서 빅데이터의 활용은 개인정보보호의 문제를 야기한다. 따라서 지능정보기술의 발전으로 인한 경제・사회구조의 변화 속에서 빅데이터의 활용과 개인정보보호법제의 충돌과 그에 대한 조화방안이 문제로 대두하게 된다.[19]

---

15) 성준호, “빅데이터 환경에서 개인정보보호에 관한 법적 검토”, 법제연구 제21권 제2호, 2013, 310면.

16) 정부 관계부처 합동, “제4차 산업혁명에 대응한 「지능정보사회 중장기 종합대책」”, 2016. 12. 27., 8-9면.

17) 김상범·김효관, “4차 산업혁명과 빅데이터 기반 기술. 전자공학회지”, 제46권 제11호, 2019. 11., 19면.

18) 정부 관계부처 합동, 앞의 보고서(註 16), 22면.

3. 초연결사회

지능정보기술을 바탕으로 하는 지능정보사회의 또 다른 특징은 초연결사회이다. 초연결사회는 인간과 인간, 인간과 사물, 사물과 사물이 네트워크로 연결된 사회를 말한다. 이 용어는 제4차 산업혁명 시대의 특징 중 하나를 설명하는 것으로서 모든 사물들이 마치 거미줄처럼 촘촘하게 사람과 연결되는 사회를 일컫는다. 초연결사회는 사물인터넷(Internet of Things: IoT)을 기반으로 구현되며, 소셜 네트워킹 서비스(SNS), 증강 현실(AR)같은 서비스로 이어진다. 초연결사회의 기반을 이루는 사물인터넷은 사람과 사물, 공간의 모든 것들(Things)이 인터넷으로 연결되어 모든 것들에 대한 정보가 수집・생성되고 활용되는 것을 의미하며, 초연결사회에서 사물인터넷 기술은 이미 일상생활 속에서 구현되고 있다.[20]

스마트 폰과 연동되는 스마트 워치(Smart Watch), 블루투스로 통신되는 블루투스 스피커(Bluetooth Speaker), 가정 내 에너지와 조명・보안・건강 등을 통합적으로 관리하는 스마트 홈(Smart Home), 건강상태를 실시간으로 진단해 주는 스마트 헬스케어(Smart Healthcare), 스마트 폰을 통해서 비닐하우스를 원격으로 제어하는 스마트 팜(SmartFarm) 등이 그 예이다.[21]

그러나 초연결사회에서 생산 및 유통되는 정보에는 수많은 개인정보가 포함되어 있어 개인의 권리 침해와 사회의 불안을 야기할 수 있는 가능성도 내포되어 있다. 초연결사회의 도래로 예측되는 개인정보의 주요한 침해 유형은, 개인정보에 대한 자기통제가 어려워지는 사물인터넷 환경에서 나타나는 개인정보자기결정권의 침해가능성, 보안성이 담보되지 않은 IT기기를 통해 저장・전송되는 개인정보에 대한 침해위험성의 증가, 그리고 데이터 처리과정에서 행해지는 익명화 조치의 적절성 여부, 다른 정보와의 결합을 통

19) 박노형·정명현, “빅데이터 분석기술 활성화를 위한 개인정보보호법의 개선방안 -EU GDPR과의 비교분석을 중심으로-”, 고려법학 제85호, 2017, 3-4면.
20) 김배원, 앞의 논문(註 7), 78-79면.
21) 백제현, “사물인터넷(IoT) 환경에서 전자적 증거의 증거능력 제고방안에 관한 연구”, 성균관대학교 법학전문대학원 박사학위논문, 2019, 22면.

한 재식별 가능성 등으로 인한 침해 가능성 등으로 나타난다.[22]

제2절 개인정보의 개념과 침해유형

Ⅰ. 개인정보의 개념

앞서 살펴본 지능정보호사회의 특징에 따르면, 개인정보가 이용되는 유형과 범위는 정보통신기술의 발전에 따라 현저히 넓어지고 있다. 개인정보를 수집할 수 있는 경로의 확대, 개인정보를 저장할 수 있는 저장장치의 증대, 개인정보를 자동으로 분석할 수 있는 연산장치의 발달, 개인정보 분석을 위한 알고리즘의 개발 등을 통하여 새로운 범위와 목적으로 개인정보를 이용하는 것이 가능해지고 있다.

이러한 정보통신기술은 급속도로 발전하면서 더욱 더 예측할 수 없는 광범위한 범위에서 개인정보를 이용하는 것이 가능하게 함으로써 개인정보에 대한 유례없는 위협이 될 것이다. 개인정보의 이용에는 정보주체의 권리를 침해하는 측면이 존재하므로 이에 대처하기 위해서는 개인정보의 의미와 범위를 명확히 이해하는 것이 중요하다.

개인정보를 보호하고 있는 법률의 보호대상인 개인의 정보는 정보주체에게 정보와 관련된 각종 권리를 부여하거나, 정보의 수집·이용 등 각종 처리행위와 관련된 규제를 통해 보호되고, 정보의 무단 수집·이용·공개·누설과 같은 침해행위에 대해 민·형사 상의 책임 또는 행정 상의 책임여부를 결정하는 기준이 된다. 이와 같이 개인과 관련된 정보의 보호와 관련하여 보호 대상의 정보가 무엇인지를 정확히 알아야 관련된 각종 권리·의무·책임이 발생하는지 여부를 결정할 수 있으므로, 개인정보의 개념을 정확히 이해하는 것이 개인정보와 관련된 문제를 해결해 나가는 출발점[23]이라고

22) 선원진·김두현, “초연결사회로의 변화와 개인정보 보호, 한국통신학회지(정보와 통신)”, 제31권제4호, 2014, 53-54면.

할 수 있다. 이러한 의미에서 법률상 개인정보의 개념과 헌법상 개인정보의 개념을 정확히 알아보고자 한다.

1. 헌법상 개인정보의 개념

헌법에 '개인정보'라는 독립된 낱말이 등장하지는 않지만, '개인'과 '정보' 각각은 모두 헌법에 명시적으로 등장하는 헌법상 개념이다. 국가나 사회, 단체를 구성하는 낱낱의 사람을 의미하는 개인을 우리 헌법은 제10조 제2문, 제36조 제1항, 제119조 제1항에서 명시하고 있다.[24] 일반적으로 관찰이나 측정을 통하여 수집한 자료를 실제 문제에 도움이 될 수 있도록 정리한 지식 또는 그 자료(data)를 의미하는 '정보' 또한 헌법 제127조 제1항[25]에서 명시적으로 언급하고 있다.[26]

2005년 주민등록법 제17조의8 등 위헌확인 사건에서 헌법재판소가 "헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간으로서의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의 원리 등"을 이념적 기초로 거론하면서 헌법에 명시되지 아니한 독자적 기본권으로서 '개인정보자기결정권'을 도출시킨 후부터,[27] 개인과 정보가 결

---

23) 고학수, 「개인정보 보호의 법과정책」, 박영사, 2016, 97-98면.

24) 헌법 제10조 제2문 '국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다', 헌법 제36조 제1항 '혼인과 가족생활은 개인의 존엄과 양성의 평등을 기초로 성립되고 유지되어야 하며, 국가는 이를 보장한다', 헌법 제119조 제1항 '대한민국의 경제질서는 개인과 기업의 경제상의 자유와 창의를 존중함을 기본으로 한다'

25) 헌법 제127조 제1항 '국가는 과학기술의 혁신과 정보 및 인력의 개발을 통하여 국민경제의 발전에 노력하여야 한다'

26) 헌법상 개인과 정보의 의미는 헌법문헌에서 내용을 확인할 수 있지만, 지능정보화사회의 도래에 대응하는 헌법적 차원에서의 다각도적 의미를 연구할 필요가 있을 것이다.

27) 헌재 2005. 5. 26. 99헌마513 등, 판례집 17-1, 683쪽: "개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들

합된 합성명사인 '개인정보'의 헌법적 개념에 대한 관심이 본격화되었다고 할 수 있다. 개인정보의 개념은 독자적인 헌법적 차원의 권리, 즉 기본권인 개인정보자기결정권의 보호대상의 범위를 획정하고, 나아가 개인정보보호를 위한 입법에 있어서 구체적인 규율의 범위를 설정하는 지침·적용대상·내용 등에 대한 해석의 기준으로 작용할 수 있다.[28]

또한, 헌법상 개인정보의 개념을 설정하는 것은 기본권인 개인정보자기결정권의 보호범위 안에 있는 정보와 그 밖에 있는 정보를 구별하는 일이다. 헌법상 기본권의 보호범위는 헌법 내에서 그에게 부여된 고유한 의미와 기능에 의해서 결정되므로[29], 개인정보의 헌법상 개념 및 보호범위는 결국 개인정보자기결정권의 가치와 기능에서 찾아야 한다.

개인정보자기결정권은 정보가 컴퓨터에 저장되고 자동분류되면서 발생하는 새로운 유형의 프라이버시 침해, 즉 정보 프라이버시 침해에 대처하기 위하여 생성된 개념으로, 헌법재판소는 개인정보자기결정권을 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리"라고 설명한다. 헌법재판소에 따르면, 개인정보자기결정권의 보호대상이 되는 개인정보는 "개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보"이며, 이러한 개인정보는 반드시 개인의 내밀한 영역이나 사적 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함된다고 한다.[30]

과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다."

28) 권건보, "개인정보자기결정권의 보호범위에 대한 분석 - 개인정보의 개념을 중심으로 -", 공법학연구 18-3(한국비교공법학회), 2017, 200면.

29) 한수웅, "헌법학", 법문사, 2013, 434면.

하지만 법률에서 개인정보를 정의할 때 개인정보의 헌법상 개념을 그대로 수용하여야 하는 것은 아니다. 개별법상 개인정보의 정의는 개인정보의 헌법상 개념과 모순될 수는 없지만, 그 이상을 포괄하는 것은 가능하다. 정보통신기술의 발전으로 비식별정보가 다른 정보와 결합하여 식별성을 갖추게 되고, 인격주체성을 나타내지 않는 정보도 다른 정보와 결합하여 정보주체의 인격주체성을 침해할 가능성이 있으므로 이를 우려하여 개인정보의 범위를 확대하는 것은 필요한 일이다. 실제로 헌법재판소가 판시한 개인정보의 범위는 개인정보보호법이 정의하는 개인정보보다 좁다. 「개인정보보호법」에서는 개인에 관한 일체의 정보를 개인정보라고 하는데 반해 헌법재판소는 개인에 관한 정보 중 개인의 인격주체성을 특징짓는 사항을 개인정보로 한정하고 있기 때문이다.[31] 식별가능한 개인을 전제로 하는 것은 동일하다.[32]

2. 법률상 개인정보의 개념

개인정보의 보호를 위해 제정된 일반법이라 할 수 있는 「개인정보보호법」에서 법률상 개인정보란 '살아 있는 개인에 관한 정보'로서 다음 세가지 유형에 해당하는 정보를 말한다. 첫째, '성명, 주민등록번호, 영상 등을 통하여 개인을 알아볼 수 있는 정보'이다. 둘째, '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보'이다. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성

30) 헌재 2005. 5. 26. 99헌마513 등

31) 예컨대, '주민등록번호와 전화번호'로 구성된 정보(A)가 있다고 하자. 정보 A는 개인정보보호법에 따르면 개인정보이지만, 헌법재판소 판례에 따르면 개인정보가 아니다. 주민등록번호는 개인식별을 가능하게 하므로 전화번호의 정보주체 a가 특정되어, 개인정보보호법에 따르면 정보 A는 개인정보다. 하지만 전화번호가 인격주체성을 특징짓는다고 볼 수 없으므로 헌법재판소 판례에 따르면 정보 A는 개인정보가 아니다.

32) 문재완, "개인정보의 개념에 관한 연구", 공법연구 제42집 제3호, 한국공법학회, 2014.2., 70-71면.

등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다. 셋째, 위의 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(가명정보)이다.

법률상 개인정보의 정의에 따라 개인정보의 개념은 다음과 같이 다섯 가지 요소로 구성된다. 첫째, 개인정보는 '살아 있는' 개인에 관한 정보이고, 둘째, 개인정보는 '개인에 관한' 정보이고, 셋째, 개인정보는 내용·형태 등 제한이 없는 '정보'이고, 넷째, 개인정보는 개인을 '알아볼 수 있는' 정보이고, 다섯째, 개인정보는 '가명정보'도 포함한다.

1) '살아 있는' 개인에 관한 정보

개인정보 보호 법령상 개인정보는 '살아 있는' 자연인에 관한 정보이므로 사망했거나 실종선고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 개인정보로 볼 수 없다. 다만, 사망자의 정보라고 하더라도 유족과의 관계를 알 수 있는 정보는 유족의 개인정보에 해당한다.[33]

2) '개인에 관한' 정보

개인정보의 주체는 자연인이어야 하며, 법인 또는 단체에 관한 정보는 개인정보에 해당하지 않는다. 따라서 법인 또는 단체의 이름, 소재지 주소, 대표 연락처(이메일 주소 또는 전화번호), 업무별 연락처, 영업실적 등은 개인정보에 해당하지 않는다. 또한, 개인사업자의 상호명, 사업장 주소, 전화번호, 사업자등록번호, 매출액, 납세액 등은 사업체의 운영과 관련한 정보로서 원칙적으로 개인정보에 해당하지 않는다. 그러나 법인 또는 단체에 관한 정보이면서 동시에 개인에 관한 정보인 대표자를 포함한 임원진과 업무 담당자의 이름·주민등록번호·자택주소 및 개인 연락처, 사진 등 그 자체로 개인을 식별할 수 있는 정보는 개별 상황에 따라 법인 등의 정보에 그치지 않고 개인정보로 취급될 수 있다. 사람이 아닌 사물에 관한 정보는

33) 개인정보보호위원회,「개인정보 보호 법령 및 지침·고시 해설」, 2020.12., 10면.

원칙적으로 개인정보에 해당하지 않는다. 그러나 해당 사물 등의 제조자 또는 소유자 등을 나타내는 정보는 개인정보에 해당한다. 예를 들어, 특정 건물이나 아파트의 소유자가 자연인인 경우, 그 건물이나 아파트의 주소가 특정 소유자를 알아보는데 이용 된다면 개인정보에 해당한다. '개인에 관한 정보'는 반드시 특정 1인에 관한 정보이어야 한다는 의미가 아니며, 직·간접적으로 2인 이상에 관한 정보는 각자의 정보에 해당한다. SNS에 단체사진을 올린다면 사진의 영상정보는 사진에 있는 인물 모두의 개인정보에 해당하며, 의사가 특정 아동의 심리치료를 위해 진료 기록을 작성하면서 아동의 부모 행태 등을 포함하였다면 그 진료기록은 아동과 부모 모두의 개인정보에 해당한다. 다만, 특정 개인에 관한 정보임을 알아볼 수 없도록 통계적으로 변환된 '○○기업 평균연봉', '○○대학 졸업생 취업률'등은 개인정보에 해당하지 않는다. 이처럼 개인정보 해당하는지 여부는 구체적 상황에 따라 다르게 평가될 수 있다. 예를 들어 '휴대전화번호 뒤 4자리'를 개인정보라고 본 판례[34]가 있으나, 이는 다른 정보와의 결합가능성 등을 고려하여 개인 식별가능성이 있으므로 개인정보로 본 것이다. 만약 다른 결합 가능 정보가 일체 없이 오로지 휴대전화번호 뒤 4자리만 있는 경우에는 개인정보에 해당하지 않는다고 보아야 할 것이다.[35]

3) 내용·형태 등 제한이 없는 '정보'

정보의 내용·형태 등은 특별한 제한이 없어서 개인을 알아볼 수 있는 모든 정보가 개인정보가 될 수 있다. 즉, 디지털 형태나 수기 형태, 자동 처

---

34) '휴대전화번호 뒷자리 4자'에 대하여, "휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더더욱 그러할 가능성이 높으며, 설령 휴대전화번호 뒷자리 4자만으로는 그 전화번호 사용자를 식별하지 못한다 하더라도 그 뒷자리 번호 4자와 관련성이 있는 다른 정보(생일, 기념일, 집 전화번호, 가족 전화번호, 기존 통화내역 등)와 쉽게 결합하여 그 전화번호 사용자가 누구인지를 알아볼 수도 있다"고 하여 「개인정보 보호법」 제2조제1호에 규정된 개인정보에 해당된다고 판시하고 있다. 대전지법 논산지원 2013.8.9. 2013고단17 판결.

35) 개인정보보호위원회, 앞의 책(註 24), 10-11면.

리나 수동 처리 등 그 형태 또는 처리방식과 관계없이 모두 개인정보에 해당할 수 있다. 정보주체와 관련되어 있으면 키, 나이, 몸무게 등 '객관적 사실'에 관한 정보나 그 사람에 대한 제3자의 의견 등 '주관적 평가' 정보 모두 개인정보가 될 수 있다. 또한, 그 정보가 반드시 '사실'이거나 '증명된 것'이 아닌 부정확한 정보 또는 허위의 정보라도 특정한 개인에 관한 정보이면 개인정보가 될 수 있다.[36]

4) 개인을 '알아볼 수 있는' 정보

성명, 주민등록번호 및 영상 등을 통하여 개인을 '알아볼 수 있는' 정보도 개인정보에 해당한다. '알아볼 수 있는'의 의미는 해당 정보를 '처리하는 자'의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다면 개인정보에 해당한다. 현재 '처리하는 자' 외에도 제공 등에 따라 '향후 처리가 예정된 자'도 포함된다. 여기서 '처리'란 개인정보 보호법 제2조 제2호에 따른 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다. 한편, 주민등록번호와 같은 고유식별정보는 해당 정보만으로도 정보주체인 개인을 알아볼 수 있지만, 생년월일의 경우에는 같은 날 태어난 사람이 여러 사람일 수 있으므로 다른 정보 없이 생년월일 그 자체만으로는 개인을 알아볼 수 있다고 볼 수 없다. 또한, 위의 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 '쉽게 결합'하여 특정 개인을 알아볼 수 있으면 개인정보에 해당한다. 여기서 '입수 가능성'은 두 개 이상의 정보를 결합하기 위해 그 결합에 필요한 다른 정보에 합법적으로 접근하여 이에 대한 지배력을 확보할 수 있어야 하며 해킹·절취(切取) 등 불법적인 방법으로 취득한 정보까지 포함한

---

36) 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 인격주체성을 특징짓는 사항으로서 개인의 동일성을 식별할 수 있게 하는 일체의 정보를 의미하며, 반드시 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지도 포함한다고 판시하고 있다. 대법원 2016.03.10. 선고 2012다105482 판결.

다고 볼 수 없다. 아울러, 다른 정보와 쉽게 결합할 수 있는지 여부는 입수 가능성 외에 현재의 기술 수준이나 충분히 예견될 수 있는 기술 발전 등을 고려하여 시간이나 비용, 노력이 비합리적으로 과다하게 수반되지 않아야 한다.[37]

5) 가명정보

가명정보란 「개인정보보호법」 제2조 제1호 가목 또는 나목[38]에 따른 '개인정보를 가명처리[39]를 하여 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보'로서 이러한 가명정보도 개인정보에 해당한다. 가명정보는 데이터의 안전한 활용을 위해 도입된 개념으로 기본적으로 개인정보에 해당한다는 점에서 동법 제58조의2에 규정된 "시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보"와 다르다. 또한, 가명정보와 동법 제2조 제1호 나목의 개인정보는 모두 해당 정보만으로는 특정 개인을 알아볼 수 없지만, 가명정보는 추가 정보의 사용·결합을 통해 특정 개인을 알아볼 수 있는 정보라는 점에서 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보인 제2조 제1호 나목의 개인정보와 구분된다. 추가 정보란 가명처리 과정에서 개인정보의 전부 또는 일부를 대체하는데 이용된 수단이나 방식(알고리즘 등), 가명정보와의 비교·대조 등을 통해 삭제 또는 대체된 개인정보 부분을 복원할 수 있는 정보를 말한다. 동법 제2조 제1호 나

---

37) 개인정보보호위원회, 앞의 책(註 24), 11-12면.

38) 개인정보보호법 제2조(정의) 제1호 "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.

39) 개인정보보호법 제2조(정의) 제1의2 "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

목의 다른 정보와 추가 정보는 해당 정보와 결합하여 특정 개인을 알아볼 수 있도록 하는 정보에 해당한다. 하지만, 다른 정보는 해당 정보와 결합하여 특정 개인을 알아볼 수 있도록 하는 정보라면 처리하는 자가 보유하고 있거나 합법적으로 접근·입수할 수 있는 정보 모두가 다른 정보가 될 수 있지만, 추가 정보는 가명처리 과정에서 생성·사용된 정보로 제한된다. 또한, 추가 정보는 해당 정보를 가명처리 전 정보로 되돌릴 수 있는 정보(복원(復元)할 수 있는 정보)인 점에서 특정 개인을 식별 가능하게 하는 다른 정보와 구분된다.[40]

Ⅱ. 지능정보화사회에서 개인정보 침해 유형

1. 수집·저장단계에서의 침해

단일데이터 또는 집합데이터를 단순히 수집하여 저장하는 것은 인격권의 침해를 일으킬 가능성이 없다. 비록 동 데이터가 개인을 식별할 '가능성'이 있는 것이기 때문에 개인정보라고 분류된다고 하더라도 단순히 저장매체에 저장되는 것으로는 정보주체의 사생활의 비밀이 타인에게 인지될 수 없고 정보주체가 형성하고자 했던 인격에 대한 부정적인 효과를 일으킬 적극적 행동이 일어나지도 않기 때문이다. 만약 인지의 노력 없이 모아두는 것이 인격권의 침해로 구성된다면 해당 개인정보는 인터넷이라는 오픈 플랫폼에 존재하는 것 자체로 이미 인격권의 침해라는 결과가 된다. 수집은 단순히 정보의 좌표를 옮길 뿐이기 때문이다. 데이터의 수집이 경제적 이익을 가져오는지 여부는 두 가지 차원에서 생각해야 한다. 하나는 경제재가 아닌 데이터가 경제적 가치가 있는 경제재로 변모하게 된 경우를 생각할 수 있고 다른 하나는 해당 데이터가 경제재이기 때문에 이를 복제하여 저장하는

40) 개인정보보호위원회, 앞의 책(註 24), 12-13면.

것이 경제적 이익을 가져 오는 경우이다. 전자의 경우를 생각해보면, 단순한 수집으로는 데이터로부터 새로운 경제적 가치를 창출할 수 없으므로 경제적 이익은 발생하지 않는다고 할 수 있다. 후자의 경우는 타인의 권리 또는 이익을 침해하여 손해를 유발하는 것이지 새로운 경제적 이익을 창출하는 것이 아니므로 빅데이터 활용이 상정하는 경제적 이익 '창출'의 전형은 아니다. 이는 타인의 권리를 보호하고 있는 법의 적용을 받아야 한다. 예를 들어, 집합단계의 데이터 중 데이터베이스(DB)나 컴퓨터프로그램저작물은 저작권법에 의해 보호받는 경제재이므로 이를 수집하는 것은 저작권법상의 복제권의 침해를 구성할 수 있다. 그러나 이는 적극적인 이익발생을 유발하지는 않는다. 저작권의 침해를 논외로 하고, 단순한 데이터의 수집은 인격권의 침해도 없고 새로운 경제적 이익도 만들지 않는다. 수집이 해킹과 같이 공격적이고 위법한 방식으로 일어날 경우라고 하더라도 기계적·불규칙한 수집자체로는 인격권의 침해도, 새로운 경제적 이익 창출도 일어나지 않는다고 볼 수 있다. 물론, 기술적보호조치를 무력화한 행위는 별도로 제재 받게 될 것이다.[41]

2. 가공·분석단계에서의 침해

수집된 데이터를 가공하고 분석하는 단계에서는 인격권의 침해와 경제적 이익이 발생할 가능성이 있다. 빅데이터 기술은 개인정보의 수집과 배열을 더욱 용이하게 함으로써 개인을 기준으로 프로파일링 같은 집합정보까지도 만들 수 있기 때문에 개인의 사생활의 비밀과 자유를 침해할 가능성이 높다. 그러나 한편으로는 아직 분석정보를 공개·유통하지 않은 상태에서 해당 정보를 개인정보처리자가 알 가능성이 있다는 사실자체가 정보주체의 인격권의 침해를 바로 구성할 수 있는지는 논란의 여지가 있을 수 있다. 한편, 가공과 분석과정에서는 단일데이터가 집합데이터로서 데이터베이스

41) 고수윤, "빅데이터의 개인정보 이용으로 인한 법익침해의 私法적 해석", 강원법학 제52권, 2017.10., 533-534면.

(DB)나 저작물이 될 수 있고 데이터베이스(DB)가 저작물로, 또는 원저작물에서 2차적 저작물이 생성될 수 있다. 저작물이 되지 않더라도 데이터 가공 및 분석은 영업비밀과 같은 경제적 이익이 있는 가치를 생성할 수 있다. 그런데 빅데이터 분석을 통해 만들어진 결과물이 저작물로 인정된다면 새로운 권리가 생성될 수 있겠고, 저작재산권을 통한 경제적 이익도 발생할 수 있을 것이다. 물론 이러한 경제적 가치는 시장에서 매매될 때 실체화 될 것이다.[42]

3. 유통·활용단계에서의 침해

개인정보처리자는 빅데이터 처리로 개인정보를 유통 또는 활용할 수 있는데 이는 인격권의 침해를 일으키기도 하고 경제적 이익의 창출을 발생시키기도 한다. 분석에 기초가 된 개인정보 주체에게 있어서는 해당 정보 공개로 인격적 법익 또는 경제적 이익이 침해될 수 있다. 국내에서는 변호사들의 개인신상정보를 기반으로 '인맥지수'를 산출하여 공개했던 웹사이트 서비스는 변호사들의 개인정보에 관한 인격권을 침해하여 위법하다 판결되었었고[43], 해외에서는 대형마트가 빅데이터 분석으로 고등학생의 임신을 예측하고 유아용품 쿠폰을 발송한 것은 프라이버시 침해에 대한 논란을 일으켰다.[44] 반면, 빅데이터는 데이터베이스(DB)를 형성하여 검색의 용이성 등의 이점으로 경제적 가치를 얻게 하기도 하고 집합된 데이터의 분석을 통

---

42) 고수윤, 앞의 논문(註 39), 534-535면.

43) 대법원 2011. 9. 2. 선고 2008다42430

44) 2012년 뉴욕타임즈에서 "기업은 당신의 비밀을 어떻게 알고있는가"라는 기사를 통해 빅데이터 기술이 개인의 사생활을 침해할 수 있다는 경고들이 여기저기 나타나기 시작하였다. 이 기사에서는 미국의 대형마트에서 빅데이터 분석을 통해 '첫20주 동안 임산부는 칼슘, 마그네슘, 아연과 같은 영양보충제를 먹는다. 일반적으로 쇼핑객들은 비누와 면봉을 사지만 갑자기 손소독제와 수건을 포함해 무향의 비누나 면봉을 사기시작하면 출산일이 가까운 것이다.'라는 메타데이터를 생산하여 한 고등학생에게 육아용품 쿠폰을 발행하였는데 이로 인해 가족이 몰랐던 딸의 임신사실이 밝혀졌던 사건을 다루었다.(The New York Times Magazine, "How Companies Learn Your Secrets, FEB.16,2012.)

해 새로운 명제를 창출함으로써 가치를 얻게 하기도 한다. 데이터과학자(Data Scientist)는 분석의 틀을 마련하고, 분석할 데이터의 선별, 분석에 대한 해석을 통해 새로운 명제를 발견하며 이에 대한 활용을 통하여 경제적 가치를 만들어 내게 된다. 데이터베이스(DB)는 저작권법상 편집저작물로 인정받아 데이터베이스(DB)를 만든 자에게 권리가 주어질 수도 있고 데이터의 분석을 거쳐 시각화된 결과물이 저작물로 인정받아 데이터과학자에게 권리가 주어질 수도 있다. 이러한 빅데이터 결과물은 유통·활용되면서 실제적인 이익을 창출하게 된다.[45]

제3절 지능정보화사회에서 개인정보 보호의 의미

Ⅰ. 개인정보 보호의 헌법적 의의

1. 과거 개인정보 보호의 의미

역사상 국가는 오래전부터 국민의 통치에 필요한 자료를 확보하기 위하여 국민의 수많은 정보들을 파악하고자 노력해 왔으며, 그렇게 해서 수집된 국민 개개인의 정보들을 체계적으로 분류하여 관리하고 이를 다양한 목적으로 활용해 왔다. 어쩌면 국가를 효과적으로 통치하기 위한 행정기관의 정보활동은 국가의 성립과 함께 시작되었다고 할 수 있을 것이다. 고대국가에 있어서도 국가의 유지와 존속을 위해서 국민에게 국방과 조세의 의무를 부과할 필요가 있었고, 그러한 의무의 부과는 국민의 인구변동이나 재산상황 등에 대한 개략적 파악을 전제로 하는 것이었다.

근대국가에 이르러 국민들의 일상생활에 관한 다양한 정보의 조사는 더욱 중요한 의미를 갖게 되었다. 기든스(Anthony Giddens)는 “근대사회는 우리

45) 고수윤, 앞의 논문(註 39), 535-536면.

가 일반적으로 생각하는 것보다는 더 오래전부터 '전자사회'의 성격을 가지고 있었으며, 전자사회의 시작에서부터 정보사회로 접어들게 되었다. 이러한 사실은 근본적인 의미에서 '모든' 국가가 '정보사회'에 해당된다."고 주장하였다. 실제로 시민계급을 주권자로 하는 국민국가(nation state)의 확립에 있어서 시민의 자격요건을 객관적으로 확정하는 것은 무엇보다도 중요하였다. 또한 국민국가의 대외적인 독립과 대내적인 평화를 확보하고 개인의 자유와 권리를 합리적으로 보장하기 위해서는 강력한 상비군과 전문성을 갖춘 관료집단이 요구되었다. 그런데 그러한 상비군과 관료제의 유지에 필요한 국가재정의 안정성은 공정한 조세제도의 정착을 통해 확보되어야 했다. 이러한 연유로 근대국가의 새로운 통치수단은 시민 개개인의 수많은 정보들이 확보되지 않으면 제대로 작동되기 어려운 것이었다. 결국 자율적인 존재로서 개인의 지위를 확보하기 위한 근대국가의 성립은 역설적으로 개인의 정보에 대한 국가의 통제력을 강화하는 방향으로 진행되었다고 할 수 있다.[46]

현대로 오면서 사회국가원리 내지 복지주의의 이념 아래 국가의 기능은 점차 확대되어왔고, 그에 따라 국가에 의한 개인정보의 수집과 처리의 필요성은 더욱 증대되었다. 국민의 인간다운 생존을 보장해주기 위해 때때로 개인의 일상생활에 대한 정부의 충분한 이해와 관심이 요구되고, 그러한 정부의 이해와 관심은 국가의 개인에 대한 정보적 통제력의 확대로 이어질 수밖에 없다. 복지국가는 개인의 후견인으로서의 국가의 위상을 보편화시켰으며, 후견적 역할의 효율적 수행을 위해 국가는 개인의 생활을 총체적으로 감시하는 체제의 성격을 가지게 되었다고 할 수 있다.[47]

2. 지능정보화사회에서 개인정보 보호의 의미

---

46) 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론", 인터넷법률 제4호, 2001, 26-27면.

47) 고영삼, "전자감시사회와 프라이버시", 한울 아카데미, 1998, 66-68면.

현대에 들어서는 정보통신기술(ICT)의 발달로 정보의 수집 및 전파가 보다 신속하고 편리하게 되면서, 개인정보에 관한 국가와 시장의 수요가 더욱 증가하게 되었다. 하지만 정보의 주체가 자신에 관한 정보의 전파에 대한 통제력을 행사하지 못함에 따라 인간으로서의 존엄과 가치를 존중받지 못하는 문제가 발생하고 있다. 가령 타인에 의해 처리되는 개인정보가 객관적 사실에 부합하지 않는 내용을 포함하고 있는 경우에는 개인의 정체성에 혼란을 야기할 수 있다. 설령 그 개인정보가 정확성에 있어서는 문제가 없으나 그 자체로 지극히 민감하고 개인적인 성질을 가진 것이어서 부주의하게 유포되거나 관리된다면 개인의 인격적 가치에 커다란 손상을 초래할 수 있다.

과거에 국가는 자신이 독점하고 있는 공권력을 행사하거나 행사할 수 있다는 가능성을 통하여 국민들을 효율적으로 통치할 수 있었다. 하지만 오늘날에는 첨단 정보통신기술을 이용하여 과거보다 훨씬 용이하고 교묘한 방식으로 국민에 대한 관리와 통제를 실시하고 있다. 특히 각종의 개인정보들이 데이터베이스에 집적되고, 정보통신망을 통해 또 다른 데이터베이스와 용이하게 연동될 수 있게 되면서, 개인정보의 처리와 이용은 시간과 장소에 구애됨이 없이 신속하게 이루어질 수 있게 되었다.

이러한 정보처리과정에서 정보주체의 의사가 반영될 기회가 보장되지 않을 경우 개인은 은밀한 개인정보의 수집이나 부정확한 개인정보의 축적과 유통에 대해서까지도 그저 지켜만 보아야 하는 신세가 될 것이다. 자신의 인적 사항이나 생활상의 각종 정보가 자신의 의사와는 전혀 무관하게 집적되고 이용 또는 유통되는 상황에서 자신에 관한 정보에 있어서조차 자율적 결정이나 통제의 가능성을 봉쇄당한다면 개인의 자유로운 인격의 발현이나 사생활의 형성은 기대하기 어렵게 된다.[48]

이와 같은 문제는 비단 공적 기관에 의한 정보활동에만 국한되는 것이 아니다. 오늘날 민간기업체 직원의 채용 또는 인사 관련 정보, 금융기관의 고객정보, 의료기관의 환자에 대한 기록 등이 데이터베이스화되어 있을 뿐만

48) 권건보,「개인정보보호와 자기정보통제권」, 경인문화사, 2005, 2-3면.

아니라, 민간에서 CCTV나 GPS, 차량용 블랙박스 등을 통하여 개인의 행태나 위치에 관한 정보를 무분별하게 수집·이용하는 사례도 급증하고 있다. 최근에는 스마트폰이나 소셜 네트워킹 서비스(SNS), 클라우드 컴퓨팅(Cloud Computing) 등을 통하여 수집된 막대한 양의 개인정보들이 프로파일링을 거쳐 상업적으로 활용하려는 움직임이 가시화되고 있다. 대규모(Volume), 다양성(Variety), 광속도(Velocity) 등을 특징으로 하는 소위 빅데이터(BIg Data)의 시대에 우리는 언제 어디서 태어나고, 부모는 누구이고, 가족은 몇 명인지, 어떠한 직종에 종사하는지, 현재의 재산상태는 어떠한지, 어떤 상품을 자주 구매하는지, 무슨 질병을 앓았는지, 어떤 웹페이지를 얼마동안 읽었는지, 어떤 사람의 페이스북을 방문하고 누구와 트위트를 주고받았는지 등에 대해 속속들이 분석되고 있는 세상에 살고 있는 것이다. 이러한 사이버감시(cyber-surveillance)는 개인에 관한 모든 데이터를 개인별로 분류하여 영구적으로 관리할 수 있게 해줄 뿐만 아니라, 국가나 시장의 요구에 따라 막대한 개인정보의 개방과 공유를 부추길 수 있다. 그런데도 정보주체가 개인정보 처리의 상황이나 내용에 대해 전혀 인식하지 못하게 된다면, 그는 자신에 관한 정보로부터도 소외되는 인격적 손상을 입게 될 것이다. 설령 짐작하거나 인식한다고 하더라도 그 처리과정에 관여하거나 통제할 가능성이 차단되어 있는 경우 정보주체는 한없는 무기력증에 빠지고 말 것이다.[49]

한편, 개인정보의 수집과 처리에 있어서의 국가적 역량이 현격히 강화되었다는 것은 국민 개개인에 대한 감시능력이 무한히 증대되고 있음을 의미한다. 개인의 일상적 생활상이 국가에 의해 낱낱이 파악될 수 있음에도 불구하고 은밀하고 교묘하게 이루어지는 정보의 처리로 말미암아 국민들 개개인으로서는 좀처럼 자신이 감시를 받고 있다거나 통제되고 있다는 것을 인식할 수 없다. 이러한 상태에서 개인은 혹시 자신이 감시당하고 있을지 모른다는 막연한 두려움을 느끼게 되고, 그러한 심리상태는 개인의 자유로

49) 권건보, “개인정보보호의 헌법적 기초와 과제”, 저스티스 통권 제144호, 2014.10., 10-12면

운 일상생활을 위축시키는 결과를 가져올 수 있다. 이러한 감시의 내면화는 공동체생활에 있어서 개인이 공적 의사형성 과정에 자유로이 참여하지 못하도록 하여 민주적 의견형성을 저해하거나 의사를 왜곡하는 결과를 초래할 수도 있다.[50]

개인정보는 개별 소비자 맞춤형 마케팅 및 금융상품의 제공 등 상업적 목적 외에 교육, 사회복지, 조세 등 공공 분야에서도 행정서비스의 효율화를 위한 목적으로 널리 이용되고 있다. 또한 모바일 헬스케어, 원격의료 등 신산업이 부상함에 따라 수집되어 활용되는 개인정보의 범위는 점점 확대되고 있는 실정이다. 개인정보의 이용을 통해 얻는 편익을 무시할 수는 없지만, 이에 대하여 정보주체의 사생활과 인격적 이익 등 기본권의 보장에 관한 측면도 반드시 고려되어야 한다. 따라서 지능정보사회에서 개인정보의 의미는 혁신적 서비스와 상품 개발을 위한 핵심적 자원인 동시에 헌법상 보호할 필요성이 있는 대상이라는 양면성을 갖고 있다.[51]

Ⅱ. 개인정보 보호의 필요성

공공부문에서의 개인정보 처리는 국가의 존재가치를 발현하는 데 있어서 필수적 요소라 할 수 있다. 가령 수사나 재판, 선거제도, 조세제도, 징병제도, 교육제도 등의 운용을 위하여 국가는 국민들의 일상을 가능하면 소상하게 파악할 필요가 있다. 특히 오늘날 복지국가의 이념과 전자정부의 구현에 있어서는 효과적인 개인정보의 처리가 불가피하다. 하지만 무분별한 개인정보의 수집이나 활용은 국민의 인격권 내지 프라이버시권, 초상권, 재산권, 교육권, 사회보장수급권 등과 같은 기본권의 침해로까지 이어질 수 있다는 점에서 문제가 있다.

---

50) 권건보, “자기정보통제권에 관한 연구”, 서울대학교 법학박사학위논문, 2004, 13면.

51) 김민우·김일환, 앞의 논문(註 3), 82면.

정보화 사회에서 개인은 자신의 실존인격 외에 사이버스페이스에 또 하나의 가상인격을 가지게 된다. 그런데 가상인격이 실존인격을 규정짓게 될 경우에 개인의 사회적 정체성은 자칫 디지털화된 개인정보에 의해 좌우될 위험에 처하게 되었다. 예를 들어 잘못된 개인정보에 의하여 개인의 사회적 정체성이 왜곡되는 경우에는 그 개인이 입게 되는 피해는 예측할 수 없을 정도로 그 파장이 크다. 범죄자로 오인되어 체포된다거나 신용거래 불량자명단에 이름이 잘못 기록된다거나 하는 경우 신체의 자유의 침해나 경제생활상의 피해는 말할 것도 없고 고용에 있어서의 차별, 복지수혜의 기회상실, 공동체생활에 있어서 명예의 손상 등 그 피해는 지대한 것이다.[52]

이러한 점에서 오늘날 개인정보의 처리상황은 단순한 명예훼손이나 재산적 피해와 같은 법률상의 이익을 침해를 가져오는 정도에 그치지 아니하고 인격권 내지 프라이버시권, 재산권, 교육권, 사회보장수급권 등과 같은 기본권의 침해로까지 이어진다고 할 수 있다. 따라서 오늘날 개인에 관한 정보의 대량적 수집과 보유 및 용이한 결합을 적절하게 억제함으로써 막강한 정보권력의 남용에 따른 개인의 비인격화 내지 소외화를 막아야 할 필요가 있다. 이를 위하여 오늘날 개인정보보호의 과제는 기본적 인권의 보장이라는 관점에서 파악되고 있다.[53]

'개인정보보호'라는 용어는 개인정보를 둘러싼 법질서를 설계하고 집행하는 국가 또는 개인정보를 처리하는 자의 관점에 입각한 것이라 할 수 있다. 개인정보보호를 '하는 쪽'과 '받는 쪽'을 생각해보면, 개인정보는 보호를 '해주는' 혹은 '해주어야 하는' 대상이 되고, 개인정보보호의 이니셔티브는 개인정보정책에 관여하는 국가기관이나 공공기관 혹은 개인정보를 수집·이용하는 자에게 주어질 수밖에 없다. 그런데 오늘날 자신에 관한 정보를 통제할 수 있는 법적 지위를 우리 헌법상 인격권, 사생활권 등의 기본권을 통하여 보호할 필요성이 있다. 그렇다면 개인정보의 보호를 위한 정보주체

52) 성낙인 외, "개인정보보호를 위한 정책방안 연구", 정보통신산업진흥원, 1999, 27면.
53) 권건보, 앞의 논문(註 47), 13면.

의 자율적 관여는 단순히 법률적 권리의 차원에서 파악되기보다 헌법상 보장되는 기본권의 차원에서 논의될 필요가 있다고 본다.[54] 이와 관련하여 우리 헌법재판소도, 정보사회로의 급격한 진입으로 야기된 개인정보의 수집·처리와 관련한 사생활보호의 문제에 대처하기 위하여 새로운 독자적 기본권으로서의 '개인정보자기결정권'을 헌법적으로 승인할 필요가 있다고 판시하였다.[55]

다른 한편으로 개인의 의사소통의 과정이 상시적으로 기록되고 다양한 용도로 활용될지 모른다고 여길 경우 개인은 자신의 의견이나 태도를 함부로 드러내지 않으려고 할 것이다. 자신에 관한 정보가 어떤 사회적 영역에 알려질지 충분히 알 수 없거나 의사소통의 상대방이 무엇을 알고 있는지 예측할 수 없는 사람은 자율적 인격체로서 자신의 결정에 따라 계획하고 결정할 자유를 본질적으로 침해받게 된다. 이러한 점에서 볼 때 개인정보의 기본권적 보호는 궁극적으로 개인의 의사소통능력을 보장함을 목적으로 한다고 할 수 있다. 나아가 개인정보에 대한 자율적 통제권은 "자유민주주의적 공동체의 기초적 기능조건"으로서도 기능한다. 즉 개인이 자율적으로 의사소통에 참여하는 과정을 통하여 자신의 사회적 그리고 정치적 환경에도 영향을 미칠 수 있는 것이다. 물론 개인은 자신의 개인적인 자기결정을 단지 그가 그 속에서 움직이는 법질서와 사회질서가 이것을 허용하는 정도에서만 실현할 수 있다.[56]

54) 권건보, 앞의 책(註 46), 87-88면.
55) 헌법재판소 2005. 5. 26. 선고 99헌마513 결정, 판례집 17-1, 668, 682-683.
56) 권건보, 앞의 논문(註 47), 12-14면.

제3장 개인정보자기결정권의 의의와 근거 및 법적 성격

제1절 개인정보자기결정권의 의의

오늘날 현대사회는 개인의 인적사항과 관련한 각종 정보가 정보주체의 의사와는 상관없이 타인에 의해 온·오프라인에서 무한대로 집적되고 활용될 수 있는 새로운 정보환경에 처해 있다. 이와 같은 지능정보화사회에서 정보통신기술의 발달에 내재된 위험 요소로부터 개인정보를 보호함으로써 궁극적으로 개인의 결정의 자유를 보호하고 나아가 자유민주체제의 근간이 총체적으로 훼손될 가능성을 차단하기 위하여 최소한의 헌법적 보장장치로서[57] 개인정보자기결정권은 그 의의가 있다.

개인정보자기결정권은 기본권 영역에서 매우 빠르게 그 세력을 넓혀 가고 있다. 이는 거의 모든 생활영역이 컴퓨터와 스마트폰, 인터넷을 통해 지능적으로 정보화됨에 따라 개인정보의 이용과 보호가 문제시되는 영역 자체가 넓어지고 있기 때문이다.

Ⅰ. 개인정보자기결정권의 개념

자신의 개인정보에 대한 통제권, 즉 '개인정보자기결정권'[58]은 자기 자신에 대한 정보가 언제, 누구에게, 어느 범위까지 알려지고 이용되도록 할 것

57) 헌재 2005. 5. 26. 99헌마513 등

58) 개인정보자기결정권에 해당하는 독일 용례로 "Recht auf informationelle Selbstbestimmung"이라는 표현은 '개인이 어떤 개인정보를 어떠한 상황에서 누구에게 전달할 것인가에 대한 개인의 자기결정권'이라는 개념을 표기하기 위해. Wilhelm Steinmüller/Bernd Lutterbeck/Christoph Mallmann/Uwe Harbort/Gerhard Kolb/Jochen Schneider, Grundfragen des Datenschutzes,-Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs., Drucksache VI/3826, 1971, S.88f. S.93, S.104에서 처음 고안된 것으로 알려져 있다. 독일에서는 이 용례의 사용이 일반적이다.

인지를 그 정보주체가 스스로 결정하고 통제할 권리를 말한다.[59] 즉 정보의 조사·수집·취급의 형태, 정보의 내용 등을 불문하고 자신에 관해 무엇인가를 말해주는 정보를 수집·처리해도 되는지 여부, 그 범위 및 목적에 관해 정보주체 스스로 결정함으로써 개인이 자신에 관한 정보의 흐름을 파악하여 통제할 수 있는 권능에 대한 법적 보호를 말한다.[60]

개인정보자기결정권의 개념은 독일의 '정보자기결정권(Informationelle Selbstbestimmung)'[61]에서 비롯된 것으로서 1983년 독일연방헌법재판소의 인구조사판결[62]에서 인정된 이후, 우리나라 헌법재판소도 2005년 5월 25일 결정(이른바 지문날인사건)[63]에서 명시적으로 도입하여 개인정보관련 판례에서 헌법상의 기본권으로서 인용되고 있다.

개인정보자기결정권은 정보주체가 '자신에 관한 개인정보의 공개와 이용에 관해 스스로 결정하고 통제할 권리'이므로, 자신에 관한 정보를 누가 어떤 목적으로 보유하고 있고 누구에게 정보를 제공했으며 그 정보가 정확하고 적절한 것인지 등을 통제할 권리를 내용으로 한다. 따라서 개인정보를

---

59) 헌재 2005. 5. 26. 99헌마513 등, 판례집 17-1, 668, 682; 성낙인, 「헌법학」, 제20판, 법문사, 2020, 1346면.

60) 정태호, "개인정보자기결정권의 헌법적 근거 및 구조에 대한 고찰-동시에 교육행정정보시스템(NEIS)의 위헌여부의 판단에의 그 응용-", 헌법논총, 제14집, 헌법재판소, 2003, 407면; 김하열, 헌법강의, 제2판, 박영사, 2020, 527면. 개인정보의 공개와 이용에 관해 스스로 결정함으로써 궁극적으로 '누가 자신에 관하여 어떠한 사회적 인격상을 형성해도 되는지'에 관해 결정할 수 있는 권리로 개인정보자기결정권의 개념을 정의하는 견해로는, 한수웅, 헌법학, 제9판, 법문사, 2019, 572면.

61) 1971년 Steinmüller가 처음으로 '정보자기결정권'이란 표현을 사용하였는데, '개인이 어떠한 개인정보를 그리고 어떠한 상황에서 누구에게 전달할 것인지에 관한 개인의 자기결정권'으로 이해하였고, 이후 여러 학자들에 의해 학설로서 인정되기 시작하였다고 한다. 권헌영 외, "4차 산업혁명시대 개인정보권의 법리적재검토", 「저스티스」 제158-1호, 2017, 17면.

62) 정태호, "현행 인구주택 총조사의 위헌성 - 독일의 인구조사판결(BVerGE 65,1)의 법리분석과 우리의 관련법제에 대한 반성", 「법률행정논총」 제20집, 2000, 199-245면. 김태오, "데이터 주도 혁신 시대의 개인정보자기결정권 -정보통신망법과 EU GDPR의 동의 제도 비교를 통한 규제 개선방향을 중심으로-", 「행정법연구」 제55호, 2018, 38-39면.

63) 헌재 2005. 5. 26. 99헌마513 등

제공하도록 강요당하는 것뿐만 아니라 그 개인정보가 타인에 의해 사용되는 것도 이 권리에 대한 제한을 의미한다.[64]

개인정보자기결정권이 지칭하는 개념에 대한 용례가 학계에서는 아직 통일되어 있지 않다.[65] 이러한 다양한 용례는 개인정보와 관련된 '자기결정'의 측면을 주목할 것인지 아니면 개인정보의 '흐름에 대한 통제'를 강조할 것인지에 따라 크게 두 분류로 구분될 수 있다.[66] '자기결정'의 측면에 주목한다는 것은 자신에 관한 정보를 타인에게 알릴 것인지 여부, 알린다면 언제·누구에게·어떻게 전달할 것인지에 관해 스스로 결정할 수 있는 권리를 보호함으로써 자신에 관한 사항이 본인 의사와는 무관하게 타인에 의해 결정됨으로써 그 개인정보주체의 인격적 가치가 형해화되는 것을 방어한다는 것을 말한다. 반면에 개인정보의 '흐름에 대한 통제'를 강조한다는 것은 개인정보주체가 정보시스템 안에 보관되어 있는 자기의 개인정보에 접근해 그 정보를 열람하고 정보보유·처리기관에게 자신에 관한 정보의 정정·삭제·차단 등을 요구함으로써 자신에 관한 정보에 통제력을 행사할 수 있도록 한다는 것을 말한다. 그러나 이 기본권의 기저에는 자신의 삶에 관한 기획과 형성에 대한 근본적인 자기결정권이 깔려있다는 점, 자신에 관한 개인정보의 흐름을 통제하기 위해 상대방에게 적극적으로 청구를 한다는 측면은 그 통제내용과 방향에 대해 자기 스스로 결정할 자유에 대한 방어권을 논리적으로 전제한다는 점, 자기결정권의 대상이 자기 자신의 개인정

64) 정태호, 앞의 논문(註 58), 408면은 개인정보자기결정권이 '언제 누구에게 무엇을 알릴 것인지를 자유롭게 결정할 자유'뿐만 아니라 '그 후의 - 자신과 관련된 - 정보의 운명을 추적하여 통제할 수 있는 권리'도 보호하기 때문이라고 서술하고 있다.

65) '자기정보통제권'(홍성방, 헌법학개론, 박영사, 2017, 188면; 최대권, 헌법학강의, 증보판, 박영사, 2001, 266-267면), '정보자기결정권'(김학성/최희수, 헌법학원론, 전정4판, 피앤씨미디어, 2020, 566면; 김승환, 정보자기결정권, 헌법학연구, 제9권 제3호, 한국헌법학회, 2003, 149면), '개인정보결정권'(강경근, 헌법, 법문사, 2002, 496면), '자기정보관리통제권'(권영성, 헌법학원론, 법문사, 2003, 427면), '개인정보통제권'(김용섭, 정보공개와 개인정보보호의 충돌과 조화, 공법연구, 제29집 제3호, 한국공법학회, 2001, 181면), '정보상 자기결정권'(홍정선, 행정법원론(상), 제23판, 박영사, 2015, 590면) 등 다양한 용례가 사용되고 있다.

66) 권건보, 앞의 책(註 46), 89면.

보라는 점을 모두 명징하게 보여줄 수 있는 용어는 '개인정보자기결정권'이라고 할 수 있다.[67]

Ⅱ. 개인정보자기결정권의 주요내용

1. 정보주체의 동의권

개인정보자기결정권의 핵심은 자신에 관한 정보의 수집·이용·제공 등을 원칙적으로 정보주체의 의사에 따르도록 하는 것이라고 할 수 있다. 정보주체는 자신에 관한 정보를 자발적으로 타인에게 알리거나 이용하게 할 수 있고, 자신이 원할 경우 그 정보에 대한 타인의 접근이나 이용을 제한할 수 있다. 즉, 정보주체는 자신에 관한 정보에 대한 처분권을 가지고 있다. 이러한 정보주체의 권능은 일차적으로 개인정보 처리에 대한 동의권으로 발현된다.[68]

정보주체의 동의는 정보주체의 자유로운 결정에 기초해야 한다. 이를 위해서 정보주체는 정보의 수집에 따라 발생할 수 있는 여러 가지 문제점들을 충분히 이해해야 한다. 그러므로 개인정보의 수집에 있어서는 충분한 설명에 기초한 동의가 요구된다. 수집에 앞서 수집사실의 고지와 명시적인 수집목적의 제시가 필요하고, 수집된 개인정보의 처리와 이용 등에 대한 구체적인 안내가 있어야 한다. 아울러 정보처리의 목적, 정보관리자의 정보수집자의 신원, 수집거부에 따른 피해, 향후 정보처리과정에 있어서 정보주체의 관여권 등에 대해서도 충분한 고지와 설명이 요구된다.[69]

---

67) 권건보, 앞의 책(註 46), 91-93면은 개인정보와 관련된 헌법적 보호의 초점은 개인정보에 대한 '자율적 통제'에 있고 이것은 곧 정보의 '흐름'을 자율적으로 통제하여 자신에 관한 정보의 처리과정에 사전적으로나 사후적으로 정보주체가 주체적으로 관여할 수 있게 한다는 것을 말하므로, 정보주체가 가지는 이러한 적극적 권리의 측면을 효과적으로 설명할 수 있도록 "자기정보통제권"이라는 용어를 사용하는 것이 적합하다는 의견도 있다.

68) 신종철, 「개인정보보호법 해설」, 진한엠앤비, 2020, 22면.

2. 개인정보의 열람청구권

「개인정보보호법」은 정보주체가 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 개인정보처리자에게 요구할 수 있도록 규정하고 있다.[70] 이 규정은 정보주체가 자신에 관한 어떠한 개인정보를 개인정보처리자가 어떻게 활용하고 있으며, 동 정보가 정확한지 여부 등을 확인하도록 하기 위한 것으로써 이러한 개인정보열람권은 개인정보자기결정권의 전제조건으로 이해된다. 열람청구권은 정보주체로 하여금 자신에 관한 정보가 어떤 내용으로 기록·보유되고 있는지, 어떠한 목적을 위해 이용되고 있는지, 그 관리상의 안전상태는 어떠한지 등에 대해 확인할 수 있게 한다. 이를 위해 정보주체의 요청이 있는 경우 개인정보처리자는 그 정보의 내용이나 안전성에 대해 충분한 설명을 해 주어야 한다. 이러한 요청이 거부된 경우에는 그 이유를 제시하도록 하고, 나아가 그러한 거부에 대하여 이의를 제기할 수 있는 권리도 보장되어야 할 것이다. 그리고 이러한 열람청구권은 가급적 저렴한 비용으로 용이하게 행사될 수 있어야 한다.[71]

3. 개인정보 정정청구권과 삭제 및 차단청구권

「개인정보보호법」은 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있으나 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다고 규정하고 있다.[72] 허위 또는 부정확한 정보로부터 정보주체의 권리를 보호하기 위하여 잘못된 개인정보에 대한 정정 또는 삭제를 요구할 수 있는 권리를 정보주체에게 부여하고 있다. 그러나 개인정보를 일

---

69) 권건보, 「정보주체의 개인정보자기결정권」 (개정판 개인정보보호의 법과 정책), 박영사, 2016, 62-63면.
70) 개인정보보호법 제35조
71) 신종철, 앞의 책(註 66), 198면.
72) 개인정보보호법 제36조.

방적으로 삭제할 경우 국가안전보장, 거래기록보전을 통한 상거래 상 분쟁해결 등에 장애요인이 될 수 있으므로 이를 방지하기 위하여 제한을 두고 있다.[73]

정보주체는 자신의 개인정보에 부정확하거나 불완전한 부분이 있음을 인식하게 된 때에는 언제든지 개인정보처리자에게 오류사항을 지적하고, 정정할 것을 요구할 수 있는 권리를 가진다. 이러한 정정요구가 있는 경우, 개인정보처리자는 법률이 허용하는 특별한 사정이 없는 한 그 부분을 정정하여야 하며, 그 정정사실을 정보주체에게 통지하여야 한다. 개인정보의 저장이나 보유가 허용되지 않거나 정보보유자의 직무수행에 더 이상 필요하지 않게 되는 경우에는 정보주체는 개인정보처리자에 대하여 자신에 관한 정보를 삭제할 것을 청구할 수 있다. 정보주체의 삭제청구가 있는 경우에는, 개인정보처리자는 그에 따라 삭제를 하여야 하나 법적으로 혹은 현실적으로 삭제가 불가능하거나 곤란한 사정이 있는 경우에는 개인정보처리자는 그 정보의 이용을 차단하는 조치를 취하는 것으로 삭제에 갈음할 수 있다. 정보주체가 보유하고 있는 개인정보에 대해 정확성 여부에 관하여 이의를 제기하고 그것이 정확한지 여부를 확인할 수 없는 경우에도 그 정보는 차단되어야 할 것이다.[74]

개인정보처리자는 정보주체가 요구한 개인정보의 정정 또는 삭제에 관하여 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.[75] 개인정보처리자는 정보주체로부터 개인정보 정정·삭제 요구를 받은 날부터 10일 이내에 해당 개인정보의 정정·삭제 등의 조치를 한 경우에는 그 조치를 한 사실을, 정보주체의 요구가 다른 법령에서 그 개인정보가 수집대상으로 명시되어 있어 삭제요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 보호위원회가 정하여 고시하는 개인정보 정정·삭제 결과 통지서로 해당 정보주

73) 신종철, 앞의 책(註 66), 202면.
74) 권건보, 앞의 책(註 67), 64면.
75) 개인정보보호법 제36조 제5항.

체에게 알려야 한다.[76]

개인정보 삭제·차단청구권과 관련하여 쟁점이 되는 것이 잊혀질 권리이다. 잊혀질 권리(Right to be forgotten) 또는 개인정보삭제권(Right to erasure)은 개인의 선택에 따라 다른 사람의 관심으로부터 멀어질 권리를 뜻한다. 사이버공간에서 검색당하지 않을 권리 혹은 본인의 게시물이나 콘텐츠의 파기 또는 삭제를 요청할 수 있는 권리를 의미한다. 컴퓨터, 인터넷, SNS의 발달을 통하여 기록화된 개인정보들이 인터넷 또는 이를 매개로 한 주변 기술에 의해 사실상 영구적으로 보존되고 유통되게 되었다. 이와 더불어 프라이버시 침해 대상이 사회적 영향력을 행사하는 공인(public figure)에 한정된 것이 아니라 우리 사회의 모든 구성원들에게 해당하게 되었다. 기술발전으로 인하여 개인정보가 대규모로 집적되고 인터넷을 통해 개인정보가 대량으로 배포되고 있는 현실로 인해 중요성과 논란이 증대되고 있는 정보주체의 권리이다.[77]

잊혀질 권리가 최초로 인정된 것은 Google Spain SL v. AEPD판결[78]이다. 스페인 변호사인 Costeja González가 사회보장연금 체납으로 인한 재산강제경매가 게재된 신문기사의 삭제를 신문사인 La Vanguardia에게 요구하였으나, La Vanguardia는 이 기사가 스페인 노동복지부의 행정명령에 따른 것이므로 이를 삭제할 수 없다는 입장을 밝혔다. 그 후 Costeja González는 Google Spain에 대하여 동 기사의 삭제를 요청하였다. 이러한 요청에 대하여 기사의 내용이 모두 사실이므로 삭제할 수 없다고 하였다. 이에 Costeja González는 스페인 개인정보보호 규제기관인 AEPD에게 신문사인 La Vanguardia와 Google Spain 모두에 대하여 위 기사를 삭제할 것을 요청하였다. AEPD는 신문사인 La Vanguardia에 대한 요청을 기각하였으나, Google Spain에 대한 요청은 인용하였다. 이 결정에 불복하여 Google Spain은 소송을 스페인 법원에 제기하였다. 스페인 법원은 이에 대

76) 개인정보보호법 시행령 제43조 제3항.
77) 김주영·손형섭, 「개인정보보호법의 이해」, 법문사, 2012, 205면
78) Google Spain v AEPD, Case C-131/12, ECLI:EU:C:2014:317, ILEC 060 (CJEU 2014), 13. 2014.

한 법률적 판단을 EU사법법원에 의뢰하면서 잊혀질 권리가 국제적으로 이슈화되었다. EU사법법원은 2014년 4월 1995년 개인정보보호지침을 근거로 기사에 관한 검색엔진의 링크와 검색결과를 삭제하도록 하였다.[79]

이 문제와 관련하여 개인정보 보호법은 제36조에서 자신의 개인정보를 열람한 정보주체에게 그 개인정보의 삭제를 요구할 수 있는 권리를 부여하고, 동법 제37조 제4항은 개인정보처리자는 정보주체에게 요구에 따라 처리가 정지된 개인정보에 대하여 지체없이 해당 개인정보의 파기 등 필요한 조치를 취할 의무를 부과하고 있으며, 동법 제21조는 개인정보처리자는 보유기간의 경과, 개인정보의 처리목적 달성 등 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하도록 하고 있다.[80] 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의 2 제1항은 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우에 그 침해를 받은 자는 해당 정보를 처리한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재를 요청할 수 있다고 규정하고 있다.

4. 개인정보의 처리정지 요구권

정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다.[81] 처리정지의 요구는 정보처리자가 당해 개인정보의 지속적 활용을 중단해 줄 것을 청구하는 것으로 개인정보자기결정권의 실질적 보장을 위해 중요한 역할을 한다. 이러한 처리정지의 요구는 특별한 이유의 제시가 없이도 언제든지 행할 수 있는 정보주체의 권리이다.

개인정보가 수집 당시 예정되었던 기간을 경과하여 이용되고 있거나 지속

79) 함인선, 「개정판 EU개인정보판례」, 전남대학교 출판문화원, 2018, 321면.
80) EU GDPR은 제17조에게 잊혀질 권리를 규정하고 있는데, 우리나라 개인정보보호법과 달리 개인정보처리자 뿐만 아니라 개인정보를 제공받은 제3자에 대한 개인정보의 파기ㆍ삭제 등의 조치의무에 관한 규정을 두고 있다.
81) 개인정보보호법 제37조

적 처리가 업무상 불필요하게 된 경우, 혹은 원래의 목적 외의 용도로 처리되고 있는 경우에 정보주체는 언제든지 개인정보처리자에게 개인정보처리의 정지를 청구할 수 있다. 또한 개인정보의 처리가 자신이나 타인에게 부당하고 실질적인 손해나 고통을 초래하고 있거나 가능성이 있는 경우에도 정보주체는 개인정보처리자에게 즉시 혹은 상당한 기간의 경과 후에 그 처리의 정지를 청구할 수 있다. 경우에 따라서는 처리정지는 삭제나 차단을 위한 사전조치로서의 의미를 가질 수 있다. 이러한 경우 정보주체는 일단 처리정지를 요구하고 추가로 차단 또는 청구를 정지할 수도 있다.[82]

5. 손해배상청구권

현행의 개인정보보호 규제시스템에 따르면 개인정보 유출과 오남용에 대한 손해배상과 징벌적 손해배상(Punitive damages) 및 법정 손해배상을 규정하고 있다. 「개인정보보호법」은 개인정보 유출과 오남용에 대한 손해배상에 대하여 정보주체는 개인정보처리자가 이 법에 위반행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다고 규정하면서, 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다고 한다.[83] 동법은 징벌적 손해배상에 대하여 별도의 규정을 두고있다. 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실ㆍ도난ㆍ유출ㆍ위조ㆍ변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다고 규정하고 있다. 이와 같은 경우에도 개인정보처리자에게 고의 또는 중대한 과실에 관한 입증책임을 부과하고 있다.[84]

이 밖에도 피해자의 피해를 기준으로 손해배상을 산정하는 것이 아니라 법률에 정한 액수로 손해배상을 하는 법정 손해배상을 규정하고 있다.

---

82) 권건보, 앞의 책(註 67), 64면.
83) 개인정보보호법 제39조
84) 개인정보보호법 제39조 제3항

「개인정보보호법은」 정보주체는 개인정보처리자의 고의 또는 과실로 인하여 개인정보가 분실 · 도난 · 유출 · 위조 · 변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다고 규정하고 있다. 이 경우에도 해당 개인정보처리자에게 고의 또는 과실의 입증책임을 부과하고 있다.[85] 개인정보관리에 관하여 강화된 형태의 다중적인 손해배상시스템을 규정한 것은 개인정보 유출과 오남용을 방지하고 정보주체의 권리보호를 강화하기 위한 것으로 해석된다.[86]

제2절 개인정보자기결정권의 주요이론과 헌법적 근거

헌법이 규정하고 있지 않은 자유와 권리를 기본권으로 인정하는 것은 가장 중요한 헌법해석 문제 중 하나이다.[87] 우리 헌법은 제37조 제1항에서 “국민의 자유와 권리는 헌법에 열거되지 아니한 이유로 경시되지 아니한다.”고 하여 헌법이 규정하고 있지 않은 자유나 권리도 기본권으로 보호될 가능성을 인정하고 있다.[88] 다만, 이 조항은 헌법이 규정하지 않은 자유와 권리에 대해서도 기본권으로 승인 또는 확인하는 것에 대한 헌법적 정당성을 부여할 뿐, 헌법에 열거되지 않은 개별 기본권들의 직접적인 근거가 될 수는 없다.[89] 따라서 개인정보자기결정권과 같이 헌법에 열거되지 않은 권리를 기본권으로 인정하기 위해서는 그 권리를 기본권으로 인정할 수 있는 헌법상 근거가 제시되어야 한다. 한편 기본권의 보호영역은 그 기본권의

85) 개인정보보호법 제39조의2
86) 김창조, “정보주체의 개인정보자기결정권 보장과 개인정보의 활용”, 경북대학교 법학연구원 법학논고 제75집, 2021, 61-62면.
87) 미국헌법에서 헌법의 해석을 통해 헌법에 명시되지 않은 기본권을 발견 또는 확인하는 것을 “Invisible Constitution”이라는 비유로 설명하고 있는 것으로는, Laurence H. Tribe, The InvisibleConstitution, Oxford University Press, 2008.
88) 한수웅, “헌법상의 인격권”, 헌법논총, 제13집, 헌법재판소(2002), 635면.
89) Erwin Chemerinsky, Constitutional Law -Principles and Policies -, (3rd ed.), Aspen Publishers, 2006, p. 794.

헌법적 근거에 의해 결정된다. 개인정보자기결정권에 의해 보호되는 대상과 보호의 목적은 개인정보자기결정권의 헌법적 근거가 무엇인지에 달려 있다. 개인정보자기결정권이 보호하고자 하는 정보의 범위는 어디까지인지, 개인정보자기결정권을 통해 보호하려는 개인의 행위 또는 상태는 무엇인지, 다른 기본권들에 의한 보호와 개인정보자기결정권에 의한 보호는 어떻게 다른지 등에 관한 문제들은 개인정보자기결정권의 헌법적 근거가 무엇인지에 따라 달리 정해질 수 있는 것이다. 개인정보자기결정권의 헌법상 근거를 분명히 하는 것은 개인정보자기결정권의 보호영역을 확정하기 위한 전제이기도 하다. 요컨대 헌법에 열거되지 않은 개인정보자기결정권을 헌법상 보장되는 기본권으로 인정하기 위해서는 개인정보자기결정권의 헌법상 근거가 무엇인지에 대해 설득력 있는 논증이 제시되어야 한다.[90] 따라서 개인정보자기결정권의 헌법상 근거에 관하여 학설 및 결정례를 중심으로 연구해 보고자 한다.

개인정보자기결정권의 헌법적 근거에 대한 논의들은 “인간으로서의 존엄과 가치 및 행복추구권”을 규정하고 있는 제10조만을 근거로 보는 견해, “사생활의 비밀과 자유”를 규정하고 있는 제17조만을 근거로 보는 견해, 그리고 헌법 제10조와 제17조가 모두 근거가 되어야 한다는 견해로 나누어진다.[91]

Ⅰ. 개인정보자기결정권의 주요이론

90) 알렉시(Alexy)의 표현에 따른다면 “정확한 기본권적 논증(korrekte grundrechtliche begründung)”이 요구되는 것이다. 알렉시는 기본권규정에 표현되지 않은 권리는 “정확한 기본권적 논증”이 가능한 경우에만 기본권규범이 될 수 있다고 하였다. Robert Alexy, Theorie der Grundrechte, 이준일, 「기본권이론」, 한길사, 2007, 96-97면.

91) 개인정보자기결정권의 헌법적 근거에 대한 학설의 논의상황에 대한 소개와 검토로는, 정태호, 앞의 논문(註 58), 414-431면; 권건보,“자기정보통제권에 관한 연구 : 공공부문에서의 개인정보보호를 중심으로”, 서울대학교 법학박사학위논문, 2004, 84-89면; 권건보, 앞의 책(註 46), 99-115면.

1. 알란 웨스틴(Alan Westin)의 프라이버시와 자유론

개인정보자기결정권 즉, 정보 주체가 자신에 대한 정보에 대해 통제권을 가져야 한다는 주장은 1967년 알란 웨스틴(Alan Westin)의 「프라이버시와 자유(Privacy and Freedom)」[92]라는 책을 통해 처음 제시되었다. 그는 전화 등의 통신기기가 발달한 사회에서는 정보프라이버시 침해가 일어나며 이는 크게 감청, 심문, 정보의 대량수집 및 처리에서 발생하게 된다고 하였다. 특히 세 번째인 정보의 대량수집 및 처리에서는 개인이 스스로 공개한 정보라 하더라도 원래 합의한 공개 목적과 범위를 넘어서 이용됨으로써 개인이 원하지 않는 정보공개가 일어날 수 있으며 이는 '정보감시(Data Surveillance)'로 이어진다고 하였다. 즉, 개인들이 내용도 존재도 모르는 파일이 집적되고 유통되면 이러한 잠재적인 '기록-감옥'이 수백만 미국인들의 과거의 실수, 누락, 오해를 향후 수십 년 동안 통제할 수 있는 영구적인 증거가 될 수 있기에 이러한 정보는 언제 자신에게 '해롭게' 이용될지 어떤 목적으로 이용될지 모르는 '정보감시' 상태를 형성한다는 것이다.[93]

여기서 웨스틴은 정보감시를 막기 위한 방편으로 개인정보를 수집할 때 정보제공자가 정보제공의 조건으로 제시한 이용목적과 제3자 제공범위를 준수하도록 함으로써 자신이 제공한 정보의 축적과 이용은 자신이 동의한 범위 내에서만 이루어지게 하는 개인정보자기결정권을 주장하였던 것이다.[94]

2. 서독연방헌법재판소의 인구조사결정론

대륙법계에서는 1983년 서독연방헌법재판소의 인구조사결정(Volkszählungsurteil)[95]

---

92) Westin, A., *Privacy and Freedom*, New York: Atheneum, 1967.
93) 고수윤, 앞의 논문(註 39), 523면.
94) 박경신, ""구글 스페인" 유럽사법재판소 판결 평석-개인정보자기결정권의 유래를 중심으로-", 세계헌법연구 제20권 3호, 2014, 38-47면.
95) BVerGE 65,1

에서 개인정보자기결정권을 최초로 인정한다. 독일연방헌법재판소는 인구조사법에 따른 인구조사가 개인의 습관, 출근 교통수단, 부업 내역, 학력 등 매우 자세한 정보를 국민들에게 요청하며 해당 정보가 원활한 지방행정을 목적으로 지방정부들과 공유될 수 있도록 한 것에 대하여 위헌결정을 내렸다. 이는 자신에 대하여 국가가 수집한 많은 정보들을 조합하여 개인의 "인격" 전체를 구성해 낼 가능성을 그 개인이 통제할 수 있어야 한다고 결정한 것이었다. 이 판결에 따르면, 정보자기결정권(die Recht auf informationelle Selbstbestimmung)이란 개인이 자신의 개인정보의 공개 및 제공(Preisgabe)과 사용에 관하여 스스로 결정할 권한을 말한다. 그리고 이는 독일 기본법(Grundgesetz) 제1조 제1항의 인간의 존엄과 이와 연계된 제2조 제1항의 인격의 자유발현권에 기초를 둔 일반적 인격권에 근거한다.[96] 여기서 독일의 인격권은 인간의 존엄을 보장하기 위한 개인의 명예, 인격권, 사적 영역(Privatsphaere)을 포괄하는 것으로 미국의 프라이버시권에 해당하는 개념과 그 맥을 같이 한다.[97]

---

96) 정보처리기술의 발전에 따라 개인에 관한 정보들이 무한히 저장 가능해졌고, 정보를 신속하게 불러올 수 있게 되었으며, 정보주체가 그 정확성과 사용목적을 충분히 통제할 수 없는 상태에서 서로 다른 정보집합물이 결합됨으로써 개인에 대한 새로운 상(이른바 '프로파일')을 조합해 낼 수 있게 되었다. 그런데 자기에 대하여 누가 무엇을 얼마나 알고 있는지 알 수 없는 사람은, 자신의 의사소통 상대방의 지식을 공정하게 평가할 수 없으므로 앞서 살펴본 자기결정의 자유를 중대하게 제한 당한다. 또한, 자신의 행동이 누구에 의하여 어떻게 관찰되고 감시되는지 알 수 없으므로 그로 인한 불이익을 두려워하게 될 것이다. 그 결과 집회·결사의 자유를 포함한 기본권 행사가 저해되는 것은 물론 개인의 개성의 발현 기회를 박탈하는 결과가 야기될 것이며 이는 민주적 질서 또한 위협하게 될 것이다. 민주적 공동체는 시민의 자유로운 행위 및 참여에 의하여 비로소 존속 가능하기 때문이다. 그러므로 현대의 정보처리 상황 하에서는 개인정보에 대한 무제한적인 수집, 저장, 사용, 전송 등으로부터 개인을 보호하여야만 비로소 인격의 자유로운 발현이 가능할 수 있다. 정보자기결정권은 바로 이러한 맥락 하에서 도출되는 권리이다.(채성희, "개인정보자기결정권과 잊혀진 헌법재판소 결정들을 위한 변명", 정보법학, 제20권 제3호, 2016, 303-304면.)

97) 문재완, "프라이버시 보호: 신화에서 규범으로", 개인정보보호법제 개선을 위한 정책연구보고서, 2013.2., 4면

3. 주요 국제조약의 흐름

개인정보 보호의 목적이 프라이버시를 보호하기 위함임은 국제조약의 목적에도 고스란히 담겨 있다. 1980년 제정된 OECD가이드라인[98]과 1981년 1월 28일 유럽평의회(Council of Europe)가 체결한 개인정보의 자동처리와 관련한 개인의 보호를 위한 조약 (Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data)[99], 그리고 동 조약을 모델로 제정된 EU의 1995년 개인정보보호 지침(Data Protection Directive 95/46/EC)[100]과 2016년 EU의 일반정보보호규칙(GDPR)에서 이를 발견할 수 있다.

우선, OECD가이드라인의 제정 배경은 크게 두 가지로 제시되는데, 첫째, 컴퓨터가 보급되기 시작함으로써 순식간에 대량의 정보가 국경을 넘어 전달될 수 있는 자동정보처리가 발달되었고, 이로 인해 개인정보와 관련된 프라이버시 보호의 필요성이 인정되었다는 점이다. 둘째는, 각국의 개인정보보호입법의 부정합성이 국경을 넘는 개인정보의 자유로운 유통을 저해할 수 있다는 우려가 제기되었다는 점이었다. 이러한 이유로 OECD 회원국들은 프라이버시와 관련된 각국의 상이한 입법에 있어 조화를 이루고 개인의 프라이버시를 보호하면서 동시에 개인정보의 국경을 넘는 유통에 지장을 초래하지 않도록 하기 위하여 가이드라인을 제정하게 되었다.[101]

또한 유럽평의회(Council of Europe)가 체결한 개인정보의 자동처리와 관

---

98) Organization for Co-Operation and Economic Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, (http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html)

99) Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108, Strasbourg, 1981.

100) EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, (http://europa.eu/legislation_summaries/information_society/data_protection/l14012_en.htm)

101) 고수윤, 앞의 논문(註 39), 525-526면.

련한 개인의 보호를 위한 조약의 서문(Preamble)에서는 유럽평의회의 목적에 대하여 명시하고 있다. 서문에 따르면 법의 지배와 인권 및 기본적 자유에 대한 존중에 근거하여 회원국 간의 통일을 획득함에 있다는 점, 모든 사람의 권리와 기본적 자유, 특히 프라이버시를 존중할 권리와 함께 인권과 기본적 자유에 대한 보호장치를 확장하는 것이 바람직하다는 점, 자동처리되는 개인정보의 국경을 넘는 유통이 증가하고 있음을 고려하여 이것이 국경을 넘는 정보의 자유에 기여함을 재확인함과 동시에, 프라이버시에 대한 존중과 사람들 간의 정보의 자유로운 유통이라는 기본적인 가치의 조정이 필요하다는 점을 선언하고 있다.[102]

1995년 정보보호지침 제1조에서는 회원국은 자연인의 기본적 권리와 자유, 특히 개인정보의 처리와 관련하여 프라이버시권을 보호하여야 함과 함께, 그러나 이러한 보호와 관련되었다는 이유로 회원국 간의 개인정보의 자유로운 유통을 제한하거나 금지하여서는 아니 된다고 입법목적을 밝혔다.[103] 이는 2016년 EU의 일반정보보호규칙(GDPR)으로 이어졌다.

Ⅱ. 개인정보자기결정권의 헌법적 근거

1. 헌법 제10조를 근거로 보는 견해

개인정보자기결정권의 근거를 헌법 제10조에 찾는 견해들도 그 이유에 대해서는 견해가 나누어진다. 먼저, 헌법 제17조는 '사생활 보호'라는 인격권의 한 부분만을 보호하는 조항임에 반해 헌법 제10조는 사생활 보호를 포함하여 사회적 인격상에 관한 자기결정과 같이 인격의 자유로운 발현을 위한 조건을 포괄적으로 보호하는 조항이므로, 자유로운 인격발현의 조건이라고 할 수 있는 개인정보자기결정권은 일반적 인격권에 속하는 것이라는

102) 고수윤, 앞의 논문(註 39), 525-526면.
103) 함인선, "EU개인정보보호법", 마로니에, 2016, 25-47면.

견해가 있다.[104]

한편, 개인정보자기결정권의 대상이 되는 정보는 사생활 영역에 국한되지 않고 공적 생활영역에서 형성되는 정보나 이미 공개된 정보도 포함되므로 사생활의 비밀과 자유 조항으로는 개인정보자기결정권을 포섭할 수 없으므로 헌법 제10조에 의해 인정되는 일반적 인격권이 근거가 되어야 한다고 설명하는 견해도 있다.[105]

그런가 하면, 개인정보자기결정권은 사적인 생활영역에 속하는 사항이 아니라 사회생활의 영역에서 형성되는 인격상을 보호하기 위한 것이므로 제17조는 근거가 될 수 없고 제10조의 일반적 인격권이 근거가 되어야 한다는 주장도 있다[106]. 그러나 개인정보자기결정권이 사생활 영역 이외의 정보도 보호한다고 주장할 수는 있지만 사생활 영역에 속하는 사항은 보호하지 않는다는 주장은 이해하기 쉽지 않다. 개인정보자기결정권이 적극적인 청구권적 성격을 갖는다는 점에서 사생활의 비밀과 자유를 규정한 제17조가 아니라 헌법 제10조가 근거가 되어야 한다는 주장도 제기되고 있다.[107]

2. 헌법 제17조를 근거로 보는 견해

헌법 제17조가 개인정보자기결정권의 근거가 되어야 한다는 견해로는, 개인정보자기결정권을 궁극적으로는 인격의 자유로운 발현에 관한 것으로 보면서도 헌법 제17조가 규정한 사생활의 비밀과 자유에 대한 보장의 일환이라고 설명하거나,[108] 사생활의 비밀과 자유를 명시적으로 규정하고 있는 제17조와의 관계에서 헌법 제10조는 보충적인 의미를 가지므로 헌법 제17조를 근거로 삼아야 한다는 주장,[109] 또는 여기서 한발 더 나아가, 개인정

104) 한수웅, 앞의 책(註 114), 649면.
105) 정태호, 앞의 논문(註 58), 423-431면.
106) 문재완, “개인정보 보호법제의 헌법적 고찰”, 세계헌법연구 제19권 2호, 2013, 280-281면.
107) 양 건, 앞의 책(註 91), 554면.
108) 권영성, 「헌법학원론」, 법문사, 2010, 458면.
109) 성낙인, 「헌법학」, 법문사, 1272-1273면.

보자기결정권의 일반적 근거조항은 제17조이지만 사생활의 비밀과 자유에 관하여 보다 구체적으로 규정하고 있는 제16조(주거의 자유)와 제18조(통신의 비밀)와의 관계에서는 제17조가 보충적으로 적용된다는 주장,[110] 그리고 사생활의 비밀과 자유 이외의 개별 기본권들에 의한 보호 가능성을 인정하면서도, 자신에 관한 정보에 대한 통제는 사생활의 자유에서 나오는 것이므로 헌법 제17조가 근거가 되어야 한다는 주장[111] 등이 제기되고 있다.

3. 헌법 제10조, 제17조를 근거로 보는 견해

제10조와 제17조를 함께 근거로 제시하는 입장은 개인정보자기결정권의 보호대상이 되는 정보가 개인의 사생활에 관한 정보에 국한되지 않고 공적, 사회적 영역에서 생성된 정보도 보호대상으로 한다는 점을 강조한다. 개인정보자기결정권의 소극적 자유로서의 측면은 헌법 제17조에서 찾고, 정보의 통제에 관한 적극적인 청구권적 측면은 헌법 제10조에서 근거를 찾는 견해도 있다.[112] 이 밖에도, 개인정보자기결정권이 자유로운 인격의 보장과 함께 권력에 대한 민주적 통제와 감시 기능도 갖는다는 점을 강조하면서, 자유로운 인격의 보장과 관련해서는 헌법 제10조가, 민주적 통제와 감시 기능과 관련해서는 국민주권의 원리와 민주주의 원칙을 개인정보자기결정권의 근거로 제시하는 견해도 있다.[113] 다만, 이러한 주장에 대해서는, 권력통제 기능은 모든 기본권에 내재하는 속성으로서 다른 기본권들 역시 민주적 정치기능을 보장하는 기능을 수행한다고 지적하면서, 국민주권의 원리나 민주주의를 개인정보자기결정권의 근거로 드는 것은 기본권의 기능 문제와 기본권의 헌법상 근거 문제를 혼동한 것이라는 비판이 있다.[114]

---

110) 김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 공법연구 제29집 제3호, 한국공법학회, 2001, 100-102면.
111) 권건보, 앞의 논문(註 48), 91-93면.
112) 김철수, 「헌법학개론」, 박영사, 2010, 667면.
113) 김종철, 앞의 논문(註 44), 43면.

4. 헌법재판소의 결정례

개인정보자기결정권을 처음으로 인정한 결정에서 헌법재판소는 제17조와 제10조를 근거로 제시하는 한편 “동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의원리 등을 고려할 수 있으나, 개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다”고 하면서 “헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다.”라고 판시하였다.[115]

헌법재판소는 개인정보자기결정권이 독자적 기본권이라는 이유로 그 헌법적 근거를 한두 개에 국한시키는 것이 바람직하지 않다고 하였으나, 독자적인 기본권이라고 해서 헌법적 근거가 한두 개에 국한될 수 없는 것은 아니다. 다만 위 결정 직후의 판결에서는 개인정보자기결정권의 근거를 헌법 제10조의 일반적 인격권과 헌법 제17조로 국한하였다.[116] 그 후로는 “자유민주적 기본질서”, “국민주권원리”, “민주주의원리” 등에 대해서는 언급하지 않고 “헌법 제10조 제1문에서 도출되는 일반적 인격권”과 “제17조”만을 개인정보자결정권의 헌법적 근거로 제시하고 있다.[117] 그러나 헌법재판소는 개인정보자기결정권의 헌법상 근거가 제10조와 제17조인 이유에 대해서는 구체적으로 설명하거나 제대로 논증하지 못하였다.

제3절 개인정보자기결정권의 법적성격

---

114) 정태호, 앞의 논문(註 131), 421면.
115) 헌재 2005. 5. 26. 99헌마513 등, 판례집 17-1, 668, 683.
116) 헌재 2005. 7. 21. 2003헌마282 등, 판례집 17-2, 81, 90.
117) 헌재 2009. 10. 29. 2008헌마257, 판례집 21-2하, 372, 384, 385(수사경력자료의 보존); 헌재 2010. 5. 27. 2008헌마663, 판례집 22-1하, 323, 334(채무불이행자명부의 공개)

Ⅰ.방어권으로서의 개인정보자기결정권

개인정보자기결정권, 즉 자신의 개인정보에 대한 자기결정권은 개인정보의 공개와 사용에 관해 개인정보주체 스스로 결정할 수 있는 권리로서 누가, 무엇을, 언제, 어떠한 경우, 어느 범위에서 자신에 관한 개인정보를 수집·관리·처리할 수 있도록 할 것인가를 결정하는 것을 내용으로 한다.[118] '언제 그리고 어떠한 범위에서 누구에게 자신의 개인적인 정보를 공개하고 수집·처리할 수 있도록 할 것인지를 원칙적으로 스스로 결정할 수 있는 개인의 권능'을 헌법적으로 보호한다는 것은 자신의 의사에 반하는 자신에 대한 공개적인 표현과 자신을 은밀히 탐지하는 것에 대해 방어할 수 있는 권리를 보장하는 것을 말한다.[119] 따라서 개인정보자기결정권은 본질적으로 방어권의 성격을 가진다.[120] 어떤 개인정보를 어떠한 경우에 어떠한 범위에서 누구에게 공개하고 처리할 수 있도록 할 것인지의 적극적 측면과 공개·처리하지 못하도록 할 것인지의 소극적 측면 모두에 대한 결정의 자유를 가지며, 이 결정은 개인정보처리의 모든 국면을 대상으로 한다.[121] 따

---

118) Carl-Eugen Eberle, Datenschutz durch Meinungsfreiheit, DÖV, Vol.30, 1977. 9., S.306ff.; 김학성/최희수, 헌법학원론, 전정4판, 피앤씨미디어, 2020, 569면.

119) 계희열, 헌법학(중), 신정2판, 박영사, 2007, 219-220면; 정태호, 앞의 논문(註 58), 407면; 김하열, 헌법강의, 제2판, 박영사, 2020, 527면.

120) Andreas Geiger, Die Einwilligung in die Verarbeitung von persönlichen Daten als Ausübung des Rechts auf informationelle Selbstbestimmung, N eue Zeitschrift für Verwalgungsrecht, 1989, S.36; Spiros Simitis, Die informationelle Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung, Neue Juristische Wochenschrift, Vol.37 No.8, 1984, S.400; Adalbert Podlech, Individualdatenschutz -Systemdatenschutz, in: K. Brückner/G. Dalichau(Hrsg.), Beiträge zum Sozialrecht, Festgabe für Hans Grüner, Percha, 1982, S.451f.; 계희열, 헌법학(중), 신정2판, 박영사, 2007, 399면; 정태호, 앞의 논문(註 58), 415면, 431면; 김하열, 개인정보수집 등 위헌확인-교육정보시스템(Neis)의 위헌 여부-, 결정해설집, 제4집, 헌법재판소, 2005, 458면. 소극적 방어권과 청구권적 성격을 동시에 갖는다고 보는 견해로는, 신우철, 헌법(기본권), 문우사, 2018, 364면.

라서 개인정보주체의 자기결정 없이 그의 개인정보를 대상으로 하는 조사·수집·보관·처리·이용 등의 행위는 모두 자기정보결정권에 대한 제한이 된다.[122]

개인정보자기결정권의 방어권적 기능으로부터 개인은 국가에 대해 자신에 관한 개인정보의 수집·보관·처리 등의 금지를 요구할 수 있는 부작위청구권과 함께 이미 발생한 침해에 대한 침해중지·방해배제 내지 결과제거청구권을 가지게 된다.[123]

Ⅱ. 적극적 청구권으로서의 개인정보자기결정권

자기정보를 공개당하지 않을 권리는 사생활의 비밀을 침해받지 않을 권리와 마찬가지로 본래 소극적 자유권이지만, 개인정보자기결정권은 자기정보의 통제를 위한 적극적 청구권이라고 볼 수도 있다.[124] 자신에 관한 정보의 열람·정정·삭제·사용중지를 요구하고 그 피해를 구제받을 권리가 바로 개인정보자기결정권이며, 개인정보자기결정권의 특별한 의미는 적극적인 청구권의 측면에 있다.[125] 그 외에도 개인정보자기결정권을 정보자기결정

121) Konferenz der Datenschutzbeauftragten, DÖV, 1984, S.505; Spiros Simitis, Die informationelle Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung, Neue Juristische Wochenschrift, Vol.37 No.8, 1984, S.399; Helmut Bäumler, Datenschutz beim Verfassungsschutz, AöR, Vol.110 No.1, Mohr Siebeck GmbH & Co. KG 1985, S.33.

122) 헌재 2005. 5. 26. 99헌마513 등, 판례집 17-1, 668, 682.

123) Jellinek, System der subjectiven öffentlichen Rechte, 2.Aufl., 1863, S.10; 이준일, 헌법학강의, 제6판, 홍문사, 2015, 308면; 정태호, 앞의 논문(註 58), 432면.

124) 양건, 「헌법강의」, 제8판, 법문사, 2019, 563-564면. 이와는 달리 홍성방, 헌법학개론, 박영사, 2017, 188면은 자기정보열람청구권, 자기정보정정청구권, 개인정보사용중지·삭제청구권 등의 청구권이 개인정보자기결정권의 보호내용에 '포함'된다는 서술을 통해 개인정보자기결정권이 오로지 적극적 청구권에 국한된 보호내용을 가지지 않음을 보여주고 있다.

125) 양건, 위의 책(註 91), 565면.

권이라고 하면서, 자기정보결정권과 자기정보통제권으로 구성하는 견해도 있다. 자기정보결정권은 자신에 관한 정보가 언제, 누구에게, 어느 범위까지 알려지고 이용되도록 할 것인가를 정보주체 스스로 결정할 수 있는 권리이고, 자기정보통제권은 자신의 정보를 열람, 정정, 이용중지, 삭제 등을 요구할 수 있는 권리라고 한다.[126]

그러나 자신의 개인정보의 정정·이용중지·삭제 등의 청구권은 이미 발생한 개인정보 침해에 대한 침해중지·방해배제·결과제거청구권이라는 개인정보자기결정권의 방어권적 측면의 효과를 부분적으로 집약해 표현한 것으로 볼 수 있다.[127] 다만, 이러한 방어권적 측면의 효과는 그 개인정보주체가 자신의 개인정보가 국가에 의해 수집·보관·처리되고 있음을 인지하여야 비로소 의미를 가질 수 있는 것이고 개인정보의 정정·이용중지·삭제 등의 청구권은 그 권리 행사를 위한 조직과 절차에 관한 규범적 형성이 있어야 실효성을 담보할 수 있다.

따라서 개인정보자기결정권은 자신에 관한 개인정보의 공개·이용·처리에 대한 자기결정적 통제권의 자유로운 행사와 그 방해배제청구라는 자유권을 본체로 하지만, 개인정보에 대한 이러한 주체적 통제력을 확보하기 위해 필요한 경우에는 국가에 대해 일정한 내용의 작위·부작위를 청구할 수 있는 법적 지위를 인정함으로써 이 자유권에 '보호막'[128]을 부여하고 있는 것으로 개인정보자기결정권의 보호내용을 구체화하는 것이 타당하다.[129] 즉

---

126) 김학성/최희수, 헌법학원론, 전정4판, 피앤씨미디어, 2020, 568면.

127) 정태호, 앞의 논문(註 58), 432면. 자유권과 청구권의 관계에 대한 호펠트(W. N. Hohfeld)의 설명으로는, 김도균, 권리의 문법-도덕적 권리·인권·법적 권리-, 박영사, 2008, 13-17면. '자유권'이란 권리주체가 상대방에 대해 특정한 행위를 하거나 하지 않아야 할 의무를 지지 않는 상태의 권리유형을 말하고, '청구권'이란 권리주체가 상대방에 대해 작위/부작위를 요구하고 상대방은 요구된 작위/부작위를 해야 할 의무를 지는 권리유형을 말한다. 김도균, 같은 책, 6-8면, 10-11면.

128) 소위 '보호막이 부여된 자유권'(vested liberty rights), '청구권의 보호울타리'(protecitve perimeter of claim-rights)의 개념에 관해서는, John Bowring(ed.), Jeremy Bentham, The Works of Jeremy Bentham, Vol.Ⅲ, William Tait, 1962, p.218; H. L. A. Hart, Essays on Bentham: Jurisprudence and Political Philosophy, Oxford University Press, 1982, p.171.

129) 개인정보자기결정권은 자신의 개인정보에 대한 정보주체의 열람, 정정, 삭제,

개인정보주체가 자신의 개인정보에 대해 열람 및 정정·이용중지·삭제 등 필요한 조치를 요구할 권리들은 개인정보자기결정권의 실질적 행사가 가능하기 위한 전제조건이자 스스로를 관철하기 위한 절차형성적 요소가 내재된 청구권이라고 평가할 수 있다.[130] 입법자에게는 개인정보자기결정권에 내재된 이러한 청구권적 요소가 실현될 수 있도록 법률로 구체적인 절차를 형성해야 할 의무가 있다.[131]

「개인정보 보호법」은 개인정보의 처리 여부를 확인하고 그 열람 및 사본의 발급을 요구할 권리, 개인정보의 처리정지·정정·삭제·파기를 요구할 권리, 개인정보의 처리로 인해 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 정보주체의 권리[132]를 명시적으로 규정하고 있다(제4조 제3호 내

기타 필요한 조치의 요구권을 포함할 수 있는데, 이러한 요구권은 적극적 청구권의 외형을 띠지만 자유의 방해배제를 구하는 수단이라는 점에서 역시 자유권적 성격을 유지하는 것이라고 분석하는 견해로는, 김하열, 헌법강의, 제2판, 박영사, 2020, 529면. 방어권으로서의 개인정보자기결정권의 실질적 보장을 위해 '자기관련 개인정보에 접근할 수 있는 권리(자기정보공개청구권)'의 보완이 필요하고, 개인정보정정·삭제청구권은 자기정보공개청구권의 부수적 권리라고 분석하는 견해로는, 한수웅, 헌법학, 제9판, 법문사, 2019, 574-575면. 헌법재판소는 개인정보를 제공한 주체가 그 정보의 수집·이용·제공의 각 단계에서 그 정보에 대한 통제권을 가지고 있어야 하고, 해당 정보에의 자유로운 접근권, 정정청구권 등이 보장되어야 한다고 판시하였다. 이에 따라 개인정보가 기재된 주민등록표를 열람하거나 그 등본이나 초본을 교부받으려고 하는 정보주체에게 수수료를 부과하는 것은 개인정보자기결정권의 제한이라고 보았다. 헌재 2013. 7. 25. 2011헌마364, 판례집 25-2상, 259, 262-263.

130) 한수웅, 「헌법학」, 제9판, 법문사, 2019, 574면.

131) 한수웅, 위의 책(註 98), 2574면. 이준일 교수는 개인정보자기결정권 자체를 사생활의 비밀과 자유에 포함된 특수한 '절차권'으로 이해하면서 사생활 가운데 개인정보의 공개에 관한 자율성이 충분히 보장될 수 있도록 하는 기능을 수행하는 것으로 기본권체계를 구성하고 있다. 헌법재판소처럼 개인정보자기결정권을 헌법에 열거되지 않은 독자적인 개별 기본권으로 인정하면서 그 헌법적 근거를 사생활의 비밀과 자유 외에도 일반적 인격권과 자유민주적 기본질서, 국민주권원리, 민주주의원리 등으로까지 확대하게 되면, 개인정보의 비밀이 개인정보자기결정권의 핵심적 구성요건임을 나타내 주는 사생활의 비밀에 관한 기본권의 독자적인 의미가 사라질 수밖에 없다고 우려한다. 이준일, 헌법학강의, 제6판, 홍문사, 2015, 582-583면.

132) 개인정보주체는 자신의 개인정보처리와 관련하여, ①개인정보 처리에 관한 정보를 제공받을 권리, ②개인정보의 처리에 관한 동의 여부·동의 범위 등을

지 제5호).[133] 한편, 「개인정보 보호법」은 개인정보의 수집·이용(제15조 제1항 제1호), 국내외 제3자 제공(제17조 제1항 제1호 및 제3항), 목적 외의 이용 및 제3자 제공(제18조 제2항 제1호), 민감정보의 처리(제23조 제1항 제1호), 고유식별정보의 처리(제24조 제1항 제1호), 정보통신서비스제공자의 개인정보 수집·이용(제39조의3 제1항), 정보통신서비스제공자 등의 국외 제공·처리위탁·보관(제39조의12 제2항) 등에 있어서 정보주체의 동의를 정당화 요건으로 규정하고 있다.[134] 그런데 개인정보자기결정권이라는 권리개념의 요체는 자기정보에 대한 자기결정권 행사라는 통제권 보장에 있다. 정보주체의 '동의권'은 자신의 개인정보에 대한 원칙적인 처분의 자유

선택하고 결정할 권리, ③개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람·사본발급을 요구할 권리, ④개인정보의 처리 정지·정정·삭제·파기를 요구할 권리, ⑤개인정보의 처리로 인해 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리를 가진다(개인정보보호법 제4조).

133) 누구든지 채무불이행자명부나 그 부본을 열람하거나 복사를 신청할 수 있도록 한 민사집행법 규정이 개인정보자기결정권을 과잉금지원칙에 위배되게 침해하고 있는 것은 아니라는 것이 헌법재판소의 법정의견이었다. 헌재 2010. 5. 27. 2008헌마663, 판례집 22-1하, 323, 334-336. 반면에 재판관 5인의 반대의견은 개인정보자기결정권 침해를 인정하였는데, 채무자의 채무불이행 사실이 알려지는 것이 간접강제의 효과를 나타내는 경우는 채무자가 경제활동 내지 거래관계 형성 상황에 직면한 때이므로 그러한 단계에 나아갔음을 소명한 자에게만 채무불이행자명부나 그 부본의 열람·복사를 허용하더라도 거래안전이라는 입법목적을 달성할 수 있어서 최소침해성 원칙과 법익균형성 원칙에 반한다고 보았기 때문이었다. 헌재 2010. 5. 27. 2008헌마663, 판례집 22-1하, 323, 337.

134) 이미 공개된 개인정보를 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 수집·이용·제공 등의 처리를 할 때에는 별도의 동의가 불필요하다고 보는 견해로는, 김하열, 헌법강의, 제2판, 박영사, 2020, 529면. 같은 취지에서 대법원은 법률정보제공사이트를 운영하는 회사가 공립대학교 법과대학 법학과 교수로 재직 중인 자의 사진, 성명, 성별, 출생연도, 직업, 직장, 학력, 경력 등의 개인정보를 위 법학과 홈페이지 등을 통해 수집해 자신의 사이트 내 '법조인' 항목에 유료로 제공한 것은 개인정보보호법 제15조나 제17조 위반으로 볼 수 없다고 판시하였다. 대법원 2016. 8. 17. 선고 2014다235080 판결. 이 판결에서 대법원은 '정보주체의 동의가 있었다고 인정되는 범위 내인지 여부'는 공개된 개인정보의 성격, 공개의 형태와 대상 범위, 그로부터 추단되는 정보주체의 공개 의도 내지 목적뿐만 아니라 정보처리자의 정보제공 등 처리의 형태와 정보제공으로 공개의 대상 범위가 원래의 것과 달라졌는지, 정보제공이 정보주체의 원래의 공개 목적과 상당한 관련성이 있는지 등을 검토해 객관적으로 판단해야 한다고 설시하였다.

를 확보하게 해 준다. 따라서 개인정보주체의 '동의권'은 개인정보자기결정권의 핵심[135]이며, 그 동의로 이루어지는 개인정보의 수집·보관·처리는 개인정보자기결정권의 제한이 아니라 개인정보주체에 의한 기본권 행사라고 보아야 한다.[136] 다만 정보주체의 동의권 행사가 개인정보자기결정권의 실질적 행사로 인정되려면 사전에 개인정보 수집·처리 등에 관련된 정보가 충분히 제공되는 등 동의의 진정성이 담보될 수 있는 제도적·절차적 장치가 마련되어야 할 것이다.

Ⅲ. 개인정보자기결정권의 행사를 위한 법질서 형성의 의무

앞서 설명한 것처럼, 개인정보자기결정권은 자기 개인정보의 공개·이용·보관·처리 등에 대한 자기결정적 통제권의 자유로운 행사를 본체로 하고, 개인정보자기결정권의 실질적 행사가 가능하기 위한 전제조건이자 스스로를 관철하기 위한 절차형성적 요소로서 국가에 대해 일정한 내용의 작위·부작위를 청구할 수 있는 권리를 포괄한다. 이에 대응하여 국가는 개인정보자기결정권이 실질적으로 보장될 수 있도록 다양한 내용의 절차적·조직적 의무를 부담하는데, 이것은 개인정보자기결정권의 객관적 법질서성에서 그 이론적 근거를 구하기도 한다.[137]

개인정보자기결정권은 입법형성의 지침으로 작용하여 입법자에게 개인정보자기결정권의 실효적인 보호와 행사를 위해 절차와 조직을 마련하고 그에 따른 구체적인 권리·의무를 법률로 형성할 의무를 부과한다. 또한 국가는 개인정보를 수집·보관·처리할 때 그 개인정보의 관리주체, 수집·처리의 목적, 개인정보제공시 그 수령인과 그 범위, 동의 혹은 거부의 효과, 그 밖

135) 김하열, 「헌법강의」, 제2판, 박영사, 2020, 529면.
136) 김하열, 위의 책(註 102), 532면.
137) Hans-Heinrich Trute, öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL, Vol.57, 1998, S.216, S.258; 정태호, 앞의 논문(註58), 434-437면.

에 절차적 권리들에 관해 고지하고 설명[138]해야 하며, 개인정보처리에 관한 기술적·물리적·관리적 조치의 안전성과 투명성을 확보하기 위한 정책을 수립하여 시행하여야 한다. 개인정보가 유통되는 네트워크의 보안성을 확보하고 개인정보데이터베이스에 대한 침입이나 무단이용을 방지하기 위한 물리적 장치와 기술적 대책을 마련해야 한다. 개인정보자기결정권의 실효적 보장을 위한 독립된 기관과 조직을 설치하여 개인정보 보호를 위한 통제·감독기구[139]의 역할을 하는 권리옹호 기능을 수행해야 한다.[140]

조직과 절차를 통한 기본권의 성격은 국가의 부작위를 통해 실현하는 자유권의 성격이 아니라, 국가의 작위를 요구하는 적극적 청구권(급부권)의 성격에 가깝다.[141] 급부 기능으로 칭하는 국가의 작위는 제3자의 위해로부터의 보호일 수도 있고, 법질서의 구체적 형성을 위한 법적 조건의 조성일 수 있다.[142]다만 국가에 요구하는 적극적 행위가 규범적 행위라는 점에서 금전이나 현물 지급 등 사실적 행위를 대상으로 하는 사회적 기본권과는 구별된다.[143] 사회적 기본권의 경우 헌법이 스스로 보장 내용을 구체화하

138) BVerfGE 65, 1, 46, 59.

139) 「유럽연합기본권헌장」(Charter of Fundamental Rights of the European Union) 제8조는 개인정보자기결정권을 명시적으로 규정하고 있다. 동조 제1항은 모든 사람은 자신에 관한 개인정보를 보호받을 권리가 있다고 명시하고 있고, 제2항은 개인정보는 관련된 개인의 동의를 기초로 또는 법률에 따른 정당한 근거에 기초해 특정한 목적을 위해 정당하게 처리되어야 하며, 모든 개인은 자신에 관해 수집된 정보에 접근하고 이를 수정할 권리를 가진다고 규정하고 있다. 동조 제3항에서는 이러한 규정의 준수가 독립된 기관에 의해 통제되어야 함을 밝히고 있다.

140) BVerfGE 65, 1, 60; Reinhard Riegel, Rechtsgrundlagen für die informationelle Tätigkeit der Verfassungsschutzbehörden und datenschutzrechtliche Konsequenzen auf dem Volkszählungsurteil des Bundesverfassungsgerichts, DVBI, 765, 1985, S.765-769; 정태호, 앞의 논문(註58), 439면.

141) 국가에 소극적 행위, 즉 부작위를 청구하는 것을 방어권(Abwehrrecht)이라 하고, 국가의 적극적 행위를 요하는 기본권을 급부권(Leistungsrecht)이라 한다. 광의의 급부권에는 사회적 기본권,보호권, 조직과 절차에 관한 기본권이 포함된다. R. Alexy, Theorieder Grundrechte, 402면.

142) 정태호, 「독일기본권론 제33판 (Kingrenn/Poscher, Grundrechte Staatsrecht Ⅱ 33. Aufl.)」, 박영사, 2021, 57-58면

143) 로베르트 알렉시, 「기본권 이론」, 한길사, 2007, 507면

는 명시적 지침을 제시하지 않았을 뿐 아니라, 헌법 해석을 통해서도 보장 내용이 구체화될 수 없다는 점에서 그 내용을 밝히기는 어렵다.[144] 결국 사회적 기본권의 경우 국가에 최선을 요구할 수 없기 때문에 과소보호금지원칙을 기준으로 판단하게 된다. 그러므로 이를 적극적으로 보장하기는 쉽지 않다. 다만, 사회적 기본권의 경우 사법적 심사를 위한 규범적 기준이 존재하지 않기 때문에 그것을 사법적으로 관철할 수 있는 가능성이 제한적인 반면,[145] 조직과 절차를 통한 기본권의 경우 사법적 관철 가능성의 정도와 기준 설정이 가능할 것이다. 조직과 절차를 통한 기본권은 방어권과 비례 원칙을 결합하여 기본권에 대한 제한이 발생하는 경우 국가에 행위의무를 부과한 것으로 보고,[146] 개인정보보호 문제에 있어서 독자적 기본권으로 인정한 헌법재판소의 개인정보자기결정권의 내용, 해외 판례, 법률로 집적된 정보보호원칙이 그 기준이 될 수 있을 것이다. 방어권적 성격의 개인정보자기결정권은 계획적, 관리적, 기술적 보호 조치 또는 관련 정보의 상황 등에 대해 정보를 제공 받을 권리를 보장할 의무로 확장된다.[147] 지능정보사회의 토대를 이루는 지능정보기술의 안전성, 보안성, 정보통신 기반에 대한 국가 책임 등도 인공지능의 발전에 따르는 국가의 기본권의 보호 의무와 밀접한 관련을 가진 헌법적 과제들이다. 따라서 과소보호금지원칙의 최소 기준이 아니라, 지능정보기술 수준을 고려한 심사 밀도 강화가 필요하다.[148] 헌법 개정 시 정보통신 시스템의 안전성과 비밀 보장, 열람청구 및 정정권을 포함한 개인정보자기결정권, 독립된 통제기구 등으로 구성된 개인정보보호권을 명문 규정으로 두어 보장하는 것을 제안하는 의견도 존재한다.[149] 이 역시 개인정보자기결정권만으로 개인정보보호를 포섭하는 데는 한계가 있음을 인지하고 시스템의 보안과 조직과 절차를 통한

144) 한수웅, 「헌법학」 , 제7판, 법문사, 2017, 961면.
145) 한수웅, 위의 책(註 144), 957면.
146) 정태호, 앞의 책(註 142), 61면.
147) 김태오, “사이버안전의 공법적 기초”, 행정법 연구 제45호, 2016, 117면.
148) 김배원, 앞의 논문(註 7), 85-86면.
149) 김배원, “정보기본권의 독자성과 타당 범위에 대한 고찰”, 헌법학연구 제12권 제2호, 2006, 199면

통제장치를 필요로 하는 것으로 해석할 수 있다.

유럽인권재판소는 개인정보보호를 위하여 사생활을 제한하는 통신 감청의 남용방지를 위한 감시 기간의 한정, 수집 정보의 처리・사용・저장에 대한 절차 규정 마련 및 정보 이전에 대한 규정, 정보 삭제 규정을 두도록 최소한의 보호 조치를 요구한 바 있다.[150] 독일연방헌법재판소 역시 독일연방정보원법의 위헌 심사에서 정보기관의 해외 통신 정보 활동에 대한 법치국가적 한계를 제시하면서, 절차적 측면에서 헌법적 요건을 자세히 설시하였다. 수집 정보의 제한, 복합적 감시 목적의 확정, 감시 조치의 근거와 요건, 통신 정보 저장량의 양적 측면에서의 제한, 저장 기간, 신뢰 관계 보호를 위한 조치들과 삭제 의무 등이 필수적임을 확인하였다. 정보의 수집 및 이용과 활용의 가능성을 열어두되, 사전 또는 사후적으로 통제될 수 있도록 절차규정에 더 구속되어야 한다. 따라서 국가의 정보 수집을 포함한 기업의 정보 이용 역시 남용되지 않도록 수집 단계와 정보 이전 단계를 구별하고 각 단계마다 비례원칙에 맞는 기본권 제한과 형식적 절차(목적, 삭제 의무 등)에 강하게 구속될 것을 요구하였다. 또한 독립적인 통제기관이 엄격하게 감시하도록 하였으며, 전략적 해외 통신 감시에 대한 새로운 심사 기준으로서 독립성이 보장된 기관에서의 통제를 요청하였다.[151] 절차와 조직에 의한 자유권 보장이 적용되는 주된 영역은 실체적 규범의 불명확성 또는 실체적 규범을 기준으로 하는 실체적 심사의 불충분함으로 인하여 효과적인 기본권 보장을 위해 절차에 의한 보완과 통제를 필요로 하는 영역이다. 결정의 내용적 타당성에 대한 실체적 심사가 제한적인 경우, 절차에 대한 통제가 사법적 통제의 한계를 보완할 수 있다.[152]

특히 사인에 의한 개인정보의 부당한 수집·보관·처리 등에 대해 개인정보

150) EGMR 13.9.2019, Big Brother Watch u.a. v. U.K. Nr. 58170/13 Rn. 307

151) EGMR 13.9.2019, Big Brother Watch u.a. v. U.K. Nr. 58170/13 결정 요지 5. 본 판결에 대한 자세한 내용 및 분석은 정문식・정호경, “정보기관의 해외 통신정보 활동에 대한 헌법적 한계- 독일연방정보원법(BNDG)의 위헌 결정에 나타난 위헌 심사 기준과 내용을 중심으로”, 공법연구 제49집 제3호, 2021, 137면.

152) 한수웅, 앞의 책(註 144), 440면.

주체를 보호해야 할 국가의 기본권보호의무는 오늘날의 정보통신환경에서 개인정보자기결정권이 실질적으로 보장되는 데 있어 핵심이 된다.[153] 오늘날 정보통신매체와 기술서비스를 제공하는 주도권이 공권력주체로부터 사기업으로 넘어갔고 정보화 사회에서 개인정보를 담은 데이터베이스가 점차 더 고도의 경제적 가치를 가지게 됨에 따라 사인에 의한 개인정보의 수집·보관·처리는 국가 못지않게 개인정보자기결정권을 위협하고 있다. 따라서 국가는 1차적으로 입법을 통해 개인정보자기결정권을 보호하기 위한 대책을 강구[154]해야 하고, 개인정보자기결정권과 관련된 사적 분쟁시 기본권의 대사인효를 고려한 사법작용을 통해 권리구제를 도모해야 한다.[155] 예를 들어, 개인정보주체가 국가공권력에 대해 가지는 각종 청구권 및 절차적 권리의 상당수가 사적 정보보유자를 비롯한 모든 개인정보처리자에게도 인

153) 국가의 기본권보호의무의 실정헌법적 근거에 대해서는 대체로 헌법 제10조 제2문을 들고 있다. 예를 들어, 김하열, 앞의 책(註 102), 241면. 반면에 국가의 기본권보호의무 사안을 기본권의 기능 중 '보호권'의 문제로 보아 '제3자의 기본권침해로부터 보호하는 입법을 국가에 대해 요구하는 권리'로 구성하는 견해로는, 이준일, 「헌법학강의」, 제6판, 홍문사, 2015, 309면.

154) 1994년 제정된 「공공기관의 개인정보 보호에 관한 법률」은 공공기관의 컴퓨터에 의해 처리되는 개인정보의 보호를 위해 그 취급시 준수해야 할 사항들을 정하고, 공공기관외의 개인·단체에 대해서도 공공기관에 준하는 개인정보보호 조치를 강구할 것으로 요구하였다. 그러나 사인에 의한 개인정보 침해 문제가 심각함에도 불구하고 이를 체계적으로 규율하는 입법이 미흡한 문제가 있었다. 이에 따라 공공부문과 민간부문을 망라하여 국제적인 수준에 부합하는 개인정보처리원칙 등을 규정하고 개인정보 침해로 인한 피해 구제를 강화함으로써 개인정보에 대한 권리와 이익을 보장하기 위해 2011년 개인정보 보호에 관한 일반법으로서 「개인정보 보호법」을 제정하여 시행하고 있다.

155) 대법원은 사생활의 비밀 침해에 대해 기본권의 대사인효를 인정한 바 있다. 대법원은 본인의 승낙을 받고 승낙의 범위 내에서 그의 사생활에 관한 사항을 공개할 경우 이것은 위법한 것이라 할 수 없지만, 본인의 승낙을 받은 경우에도 승낙의 범위를 초과하여 승낙 당시의 예상과는 다른 목적이나 방법으로 이러한 사항을 공개할 경우에는 위법하다고 판시하였다. 이 판결에서 대법원은 피해자가 자신을 알아볼 수 없도록 해 달라는 조건하에 사생활에 관한 방송을 승낙하였는데, 방영 당시 피해자의 모습이 그림자처리 되기는 하였으나 그림자 옆모습의 윤곽이 그대로 나타나고 음성이 변조되지 않는 등 방송기술상 적절한 조치를 취하지 않음으로써 피해자의 신분이 주변 사람들에게 노출된 경우 사생활의 비밀을 공개하였다고 하여 불법행위에 의한 손해배상책임을 인정하였다. 대법원 1998. 9. 4. 선고 96다11327 판결.

정되어야 한다. 인터넷과 스마트기기의 보편적 보급에 맞춰 이를 활용하는 개인의 정보활동이 부지불식간에 포괄적으로 조사·수집되거나 기록되지 않도록 하는 보호조치가 강구되어야 한다.[156] 개인정보 보호를 위한 국가의 중앙집중적 감독수단들은 분산된 네트워크 구조 속에서 국경을 초월하는 실시간 정보유통이 무제한적으로 확장되어가는 현실태에 비추어 적정한 효과를 확보키 어렵기 때문에, 정보의 암호화·개인정보의 익명 내지 가명처리·네트워크 보안·해킹방지 등의 다양한 기술적 수단들이 개발되어 활용될 수 있도록 촉진하여야 한다. 정보통신기술의 개발 단계부터 관련 정책과 사업의 수행 그리고 물리적 인프라 구축에 이르기까지 '개인정보보호에 기초한 설계'(design by privacy)가 이루어질 수 있도록 제도적·법적인 정비를 이루어나가야 한다.[157]

제4절 지능정보화사회에서 개인정보자기결정권의 의미

Ⅰ. 개인정보자기결정권의 헌법적 보호의 필요성

오늘날 정보통신기술의 비약적인 발전으로 다양한 개인정보가 국가기관뿐만 아니라 민간부문에 의해서도 광범위하게 수집·처리되고 있고, 특히

---

156) Hans-Heinrich Trute, öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL, Vol.57, 1998, S.261f.; 정태호, 앞의 논문(註 58), 442면.

157) David Krebs, "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law?, JIPITEC, Vol.4, 2013, pp.3-4(https://www.jipitec.eu/issues/jipitec-4-1-2013/jipitec4krebs/jipitec-4-1-2013- 2-krebs.pdf, 2020. 10. 18. 최종방문). 개인정보보호 필요성만을 일방적으로 강조할 수는 없으며 정보인프라의 이용보장이라는 측면도 함께 고려되어야 한다는 견해로는, Hans-Heinrich Trute, öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL, Vol.57, 1998, S.265f.; 정태호, 앞의 논문(註 58), 443면.

대규모 데이터베이스의 구축과 자동화된 전산시스템의 활용은 개인정보에의 무단접근·정보결합·정보공유 등이 그 대상을 가리지 않고 빠른 속도로 더욱 간편하고 손쉽게 일어나고 있다. 분산되어 있던 단편적인 개인정보들은 통합정보체계를 통해 간편하게 결합되어 무제한적으로 저장·집적되고 검색·추출됨으로써 인간은 '어항 속의 금붕어'와 같은 존재로 전락할 수도 있다.[158] 자신도 인지하지 못하고 있는 사이 그 의사에 반해 개인정보가 수집·축적·유통·이용되는 경우 개인은 자신의 인격적 정체성이나 사회적 인격상에 대한 자율적 결정권이나 통제력을 상실하게 되고[159] 인격의 자유로운 발현이나 사생활의 자유로운 형성을 기대할 수 없게 된다.[160] 개인정보의 정확성 여부를 떠나 그 유통 자체로 입게 되는 손해는 비단 인격침해에 국한되지 않으며 유무형의 재산적·비재산적 피해로까지 확대될 수 있다. 따라서 개인정보가 국가를 비롯한 타자[161]에 의해 전방위적으로 노출되고 활용되는 상황에서 개인은 안전하고 평온한 존립과 자율성의 기초를 잃게 되며 헌법은 자신이 기반하고 있는 자유롭고 민주적인 체제를 더 이상 유지할 수 없게 된다.[162]

---

158) 정태호, 앞의 논문(註 58), 411면.

159) BVerfGE 65, 1, 43.

160) 김하열, 앞의 책(註 102), 527면. 잘 알지 못하고 통제할 수도 없는 전자적 기계의 고도 기술에 대한 시원적 불안으로 인해 자기 자신이 무장해제된 채 정보의 지배자에게 내맡겨져 있는 것 같은 두려움이 강화된다는 서술로는, Ernst Benda, Privatsphäre und Persönlichkeitsprofil-Ein Beitrag zur Datenschutzdiskussion, in: Festschrift für Willi Geiger zum 65. Geburstag, Menschenwürde und freiheitliche Rechtsordnung, Mohr Siebeck, 1974, S.27.

161) 개인정보자기결정권의 경우 국가공권력에 의한 침해 못지않게 사적 영역에서의 침해가 오늘날과 같은 정보화사회에서는 특히 문제된다. '정보'라는 자원의 일방적 이용가능성은 사인 사이에서도 '새로운 권력적 상황'을 조성하고 있으며, 경제와 정치 영역에서 개인의 자유로운 의사형성과 결정을 위협적으로 축소시키는 상황이다. 정태호, 앞의 논문 58), 413면; Otto Mallmann, Zielfunktionen des Datenschutzes: Schutz der Privatsphäre, korrekte Information, Metzner, 1977, S.66; Carl-Eugen Eberle, Datenschutz durch Meinungsfreiheit, DÖV, 1977. 9., S.309.

162) 개인은 국가나 타인이 자신도 모르는 사이에 자신에 관한 정보를 집적하고 관리함으로써 자신을 속속들이 들여다보고 있을지도 모른다는 심리적 압박을 받게 되고 그러한 개인정보를 집적·관리하는 자는 그 정보에 기초해 개인의 행

예를 들어, 국가가 단지 개인의 행위를 파악하고 그에 관한 정보를 수집하여 축적한다는 것 자체만으로도 그 개인은 심리적 압박을 받고 그의 의사 작용에 영향을 받으며 더 나아가 자유로운 기본권 행사를 저해하게 된다.[163] 자신에 관한 정보 중 어떠한 것이 외부에 알려지는지 파악하여 통제할 수 없거나 상대방이 자신에 관해 무엇을 알고 있는지 전혀 예측할 수 없는 상태에서는 자신의 결정을 토대로 인생을 기획하고 자유롭게 인격을 발현하며 행동하는 데 큰 제약을 받지 않을 수 없다.[164] 현대의 정보처리 기술은 그 자체로는 특별한 의미를 가지지 않고 널리 분산된 정보의 조각들을 무제한적으로 저장해 언제든지 효과적으로 서로 결합함으로써 개인에 관한 전체적 혹은 부분적인 인격상을 거의 완벽하게 형성해 낼 수 있는 반면, 당사자인 정보주체는 그 정확성이나 사용의 타당성을 충분히 통제할 수 없게 만들고 있다. 누가 자신에 관해 어떤 개인정보로 어떠한 사회적 인격상을 형성할 것인지의 문제는 자주적 인격의 자유로운 생존과 인격발현의 근본조건에 관한 문제이기 때문에, 자신에 관한 개인정보에 관한 자기결정권의 보장은 그 정보에 대한 타인의 조사·수집·보관·처리에 앞서 헌법적으로 보호할 필요가 있고[165] 자유의 행사를 실질적으로 가능하게 하는

태를 용이하게 조정할 수도 있게 되므로, 개인의 자유로운 결정을 바탕으로 한 국민의 행위능력과 참여능력에 토대를 둔 자유민주적 기본질서의 기본조건은 위험에 처해질 수 있다. 같은 취지의 독일연방헌법재판소 설시로는, BVerfGE 65, 1, 42f. 개인정보자기결정권을 헌법적으로 보호해야 하는 근거로 자유민주적 기본질서의 유지를 위한 필요성, 다른 기본권을 보장하기 위한 수단성을 들고 있는 견해로는, 이인호, 정보사회와 개인정보자기결정권, 중앙법학, 창간호, 중앙법학회, 1999, 62면.

163) 독일연방헌법재판소는 국가가 정보의 수집·처리와 관련된 실무에서 신뢰구축을 위해 노력하지 않으면 장기적으로는 이에 대한 불신이 생겨 국민의 협조 자세가 사라질 위험이 있다고 설시하였다. BVerfGE 65, 1, 50. 사회학적 개념인 '신뢰'의 문제를 사생활의 기초이자 목적으로 삼아 법적 보호대상으로서의 사적 관계는 주어진 것이 아니라 신뢰에 기초한 자기결정을 통해 비로소 형성된다고 이론구성하는 견해로는, 박종보, 4차 산업혁명과 사생활보호의 변화, 박종보 외, 4차 산업혁명과 인문적 소프트파워, 학고방, 50-55면.

164) 한수웅, 앞의 책(註 97), 571면.

165) BVerfGE 65, 1, 42; Rupert Scholz/Rainer Pitschas, Informationelles Selbstbestimmungsrecht und staatliche Informationsverantwortung, Aufl.1, Duncker & Humbolt, 1984, S.12f.; Spiros Simitis, Die informationelle

상황의 유지로까지 그 헌법적 의의를 확장할 필요가 있다.[166] 결국 개인정보자기결정권을 헌법상의 기본권으로 보호하는 근거이자 목표는 '자신에 관한 정보에 대한 개인의 결정의 자유'를 유지하고 보호하기 위함이다.[167]

Ⅱ. 개인정보자기결정권의 한계

개인정보자기결정권은 「개인정보보호법」의 헌법적 기초로서, 기본적으로 국가 등 공권력에 의한 개인정보의 광범위한 수집과 그로 인한 국민의 감시, 통제로부터 국민을 보호하기 위한 기본권이다.[168] 개인정보자기결정권의 핵심은 정보의 수집·이용에 대한 동의 및 활용에 대한 결정권인데, 비약적인 정보통신과학기술 발전 상황에서 개인정보자기결정권 또는 개인정보자기통제권으로 불리우는 개인정보보호를 위한 독자적 기본권으로 정말 개인정보보호가 실현되는가에 대해 회의적이다. 우리는 서비스 뒤편에서 자신의 개인 데이터가 수집, 처리되고 있음을 거의 인식하지 못한다. 하지만 기업들은 소비자에 대해 더 정교하게 분석하여 마케팅 전략을 수립하거나 타깃광고를 하기 위해 데이터를 수집한다. 더 많은 데이터는 나를 더 잘 통제할 수 있다는 것을 의미하고, 이런 상황에서 역으로 나의 선택권과 자율성은 상실되는 결과에 이른다. 대부분의 사람들은 자신의 정보와 관련하여 인터넷에 연결되어 있으면 어떤 가능성이 존재하는지, 이것이 어떠한 위험이나 기회를 야기하는지, 언제 그리고 어디서 특정 정보가 중요하게 되는지를 제대로 알 수 없다. 이렇게 정보가 수집되고 이동되는 상황과 시

Selbstbestimmung-Grundbedingung einer verfassungskonformen Informationsordnung, Neue Juristische Wochenschrift, Vol.37 No.8, 1984, S.398f.

166) 한수웅, 앞의 책(註 97), 572면.

167) 최규환, "가명정보와 개인정보자기결정권", 헌법재판소 헌법재판연구원, 2021. 28-30면.

168) 이해원, "데이터 경제 시대의 개인정보 보호와 사적 자치", 정보법학 제24권 제2호, 2020.8., 100면.

스템에 대한 이해도 없이 자기와 관련된 모든 정보의 공개, 수집, 관리 기타 처리를 스스로 결정하고 통제할 수 없다. 국가를 포함한 제3자가 은밀히 개인정보에 대해 접근할 수 있는 기술적. 법적 상황에서는 개인정보자기결정권 행사 자체가 무력화될 가능성이 크다. 이처럼 개인의 결정 권능에 초점을 두고 있는 개인정보자기결정권은 은밀한 IT 시스템에 대해 접근이 용이한 오늘날의 환경에서 그 보호범위가 너무 좁음을 분명히 드러낸다.[169]

게다가 개인정보자기결정권은 4차산업사회가 진전됨에 따라 AI의 활용이 더욱 광범위하게 이루어지고, 그로 인해 인간의 개입이 배제된 채로 개인에게 중요한 결정이 이루어지는 상황마저 발생했다.[170] 그렇다고 국민들이 자기에 관한 정보를 엄격히 통제하며 정보 회피 또는 정보 최소화가 개인정보보호의 핵심도 아니다. 국가에 의한 개인정보의 수집이나 활용은 국민 개개인에게 자신의 일상을 감시하는 억압적 기제로 느껴질 수 있겠지만, 전체 국가의 차원에서는 보다 많은 사람들의 자유와 편리를 보장하는 데 기여한다.[171] 물론 개인정보보호를 위한 접근권 등의 권리나 보호 체계 전체로 개인정보자기결정권의 내용을 구성하는 것도 가능할 것이나, 시스템 자체의 무결성과 사이버 보안 및 독립적 기관을 통한 통제 등을 포괄하는 개인정보보호의 내용이 자기 '결정' 또는 '통제'의 문언상 해석의 한계를 넘어서는 것으로 판단된다. 개인정보보호의 문제를 국가로부터의 자유인 방어권적 측면에서만 접근할 경우 충분한 보장이 어렵다. 정보보호는 그 정보 자체에 대한 보호가 본질이라기보다 당사자와 정보 처리자 간의 신뢰를 구축하는 일이다. 그렇다면 어떠한 대상 혹은 행위에 보호받을 만한 정당한 신뢰가 부여될지 고려해야 한다. 그런 다음 보호받을만한 신뢰가 생성되는 개별 관계들을 구별해야 한다. 인터넷 상에서 정보 주체는 스스로 자기 관련 정보에의 접근을 막을 능력도, 권한도 없는 상태에 놓여 있다. 그

169) 김태오, 앞의 논문(註 147), 112-118면.
170) 권건보・김일환, "지능정보시대에 대응한 개인정보자기결정권의 실효적 보장 방안", 미국헌법연구 제30권 제2호, 2019, 4면.
171) 권건보, 앞의 논문(註 47), 10면.

러므로 당사자는 그저 의사 소통의 상대방 또는 인터넷 서버 또는 검색 엔진 관리자 등의 제3자가 법을 통해 합법의 경계를 넘어서지 않을 것이라 믿는 것뿐이다.[172] 이러한 신뢰에는 사람과의 관계를 넘어서 어떠한 기술이나 시스템이 투명하고 안전하게 그 기능을 제대로 발휘할 것이라는 믿음이 포함된다. 그러므로 디지털 시대의 사생활 보호를 위해 사생활 보호 또는 (보호받을 만한) 신뢰에 대한 기대에 기반하여 적극적으로 권리 보장에 힘써야 하며, 사생활 침해 위험에 대한 적극적인 보호 가능성과 권한 범위 내에서 객관적 정보보호법을 관철해야 한다. 개인의 사생활 보호가 쉽고 효과적으로 보장될 수 있는 적절한 요청 규범과 절차가 형성되어야 한다. 개인정보보호는 개인과 관련된 정보의 수집과 유통에 대해 결정할 권리를 보장함으로써 실현되는 것이 아닌, 데이터의 자유로운 활용을 가능하게 하되 개인정보 처리에 오·남용을 막기 위한 적법한 활용 기준과 방법을 모색하는 것으로 접근해야 한다. 이러한 접근 방식에서 본다면 개인정보 처리의 오·남용의 위험을 막아 정보 주체의 신뢰를 구축하기 위해서 어떤 요건을 갖추어야 할지, 어떠한 절차와 통제가 적법한 정보 처리의 기준이 되는가를 고민해보아야 할 것이다.[173]

---

172) 정애령, “사생활보호와 개인정보보호의 관계에 관한 연구”, 공법학연구 제17권 제3호, 2016, 74면.

173) 정애령, “지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호”, 공법학연구 제23권 제1호, 2022. 39-41면.

제4장 해외의 개인정보 보호법제 현황

제1절 해외의 개인정보 보호법제

지능정보화사회의 개인정보 보호 정책으로 유럽연합(EU)은 GDPR(General Data Protection Regulation)을 제정하여 선제적으로 개인정보를 보호하고자 하였다. GDPR은 개인정보 처리에 대한 정보주체의 동의 요건을 강화하고, 정보주체에게 삭제권과 처리제한권·정보이동권을 부여하며, 자동화된 의사결정과 프로파일링에 관한 권리 등 여러 권리를 보장하고 있다. 데이터 처리가 개인정보에 고위험을 초래할 가능성이 있는 경우에는 개인정보 영향평가(DPIA)를 하도록 의무화하고, 대규모 정보처리나 민감정보 처리 등의 경우에는 정보보호관(data protection officer)을 의무적으로 지정해 이들이 독립적으로 업무를 수행하도록 규정하고 있다. GDPR은 EU 회원국뿐만 아니라 EU에 거주하는 정보주체의 개인정보를 취급·처리하는 비회원국에도 적용되는 국제적 기준으로 작용하고 있다.[174]

EU의 GDPR을 반영하고 정보주체의 권리를 강화하고 있는 해외 주요국의 개인정보 보호법제를 EU, 독일, 프랑스, 영국, 미국, 일본 국가 순으로 알아보고, 해외 개인정보 보호법제가 시사하는 점을 '잊힐 권리'를 중점으로 논하고자 한다.

Ⅰ. EU

1. EU의 개인정보보호지침(Directive 95/46/EC, 1995)

174) 최규환, 앞의 논문(註 153), 21면.

유럽연합(EU)은 1995년 10월 “개인데이터의 처리와 개인데이터의 자유로운 유통에 관련된 개인정보보호지침”[175](Directive 95/46/EC, 이하 ‘1995년 지침’이라 한다)을 채택하였다.

1995년 지침은 1980년 OECD의 프라이버시 가이드라인[176]과 1981년 유럽평의회(Council of Europe, CoE)[177] 협약 108(Convention 108)[178]에 기초하여 만들어졌다. 특히 OECD가 제시한 개인정보 보호 8개 원칙은 정보보호 지침에 큰 영향을 미쳤다.[179] 또한 협약 108은 법적 구속력을 가진 규범으로서 유럽 역사상 처음으로 개인정보 보호를 개인의 권리로 인정하였다는 점에 그 의의가 있다.[180]

1995년 지침은 개인정보의 처리와 관련하여 개인의 기본권과 자유를 보호하고, EU 회원국 간의 개인정보 이동의 단일한 기준을 제시하여 EU 회원국 간의 개인정보의 자유로운 이동을 보장하려는 것이었다. 동 지침은 개

---

175) Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281 , 23/11/1995 P. 0031 - 0050

176) OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, Paris, 23 September 1980.

177) 유럽평의회(Council of Europe)는 유럽 정상회의, EU이사회와 달리 회원국은 47개국이며, 이 중 28개국이 EU 회원국이다. 유럽평의회는 회원국을 구속하는 입법을 할 수 있는 권한이 없다. CoE의 기관으로 유럽인권재판소(ECtHR)가 있다.

178) Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, ETS 108, https://www.privacycommission.be/sites/privacycommission/files/documents/convention_108_en.pdf. 협약 108의 비준국은 총 48개국으로, EU 회원국 모두와 CoE 회원국 대부분이 비준하였다.

179) OECD의 개인정보 보호 8원칙은 ① 수집제한(Collection Limitation) 원칙, ② 정보 정확성(Data Quality) 원칙, ③ 목적 특정(Purpose Specification) 원칙, ④ 이용제한(Use Limitation) 원칙, ⑤ 안전성 확보(Security Safeguards) 원칙, ⑥ 공개(Openness) 원칙, ⑦ 개인 참가(Individual Participation) 원칙, ⑧ 책임(Accountability) 원칙이다.

180) 문재완, “유럽연합(EU) 개인정보보호법의 특징과 최근 발전”, 외법논집 제40권 제1호, 2016.2. 3면.

인정보의 처리와 관련하여 개인의 프라이버시 보호와 EU 회원국들 간의 개인정보 보호 기준의 조화를 위한 단일한 기준으로서, EU 각 회원국의 국내 규정에 대한 방향성을 제시하였다. 따라서 동 지침의 제정을 계기로 EU 회원국 국민들에 대하여 동일한 수준의 개인정보 보호가 적용되게 되었다는 데에 중요한 의의가 있다. 1995년 지침 제정 이후 유럽 국가들은 이에 영향을 받아 개인정보보호법을 제·개정하였는데, 독일은 연방정보보호법(Bundesdatenschutzgesetz, BDSG)을 2001년 개정하였고, 프랑스는 개인정보보호법(Loi n° 78-17 du 6 janvier 1978)을 2004년 개정했으며, 영국은 1998년 개인정보보호법(Data Protection Act 1998)을 제정하였다.[181]

2. EU의 GDPR(General Data Protection Regulation, 2018)

1) GDPR의 제정과정

1995년 지침은 그 법형식이 '지침'(Directive)이라는 점 때문에 회원국의 이행을 이끌어내는 데는 한계를 보일 수밖에 없었다. 그에 따라 EU 전역에 걸쳐 개인정보의 보호에 관한 규율체계가 통일성을 갖지 못하게 되어 개인정보의 처리에 있어서 법적 불확실성이 존재하는 상황이 지속되었다. 이에 따라 1995년 지침의 한계를 극복할 수 있는 구속적 규범체계의 확립을 요구하는 목소리가 높아졌다. 이는 EU의 전체 회원국에 통일적으로 적용될 개인정보보호법의 제정을 위한 움직임으로 가시화되었다. EU 집행위원회(European Commission)는 2009년 7월부터 회원국들의 의견을 수렴하는 절차에 돌입하여, 마침내 2012년 1월 25일에 개인정보의 처리와 관련한 개인의 보호 및 개인정보의 자유로운 이동에 관한 규정, 즉 일반개인정보보호규정(General Data Protection Regulation) 초안을 공표하기에 이르렀다. 동 규정안은 2012년 1월 27일에 EU의 입법기관인 유럽의회(European Parliament)와 EU 이사회(Council of the European Union)에 제출되었다.

181) 권건보, 이한주, 김일환, "EU GDPR 제정 과정 및 그 이후 입법동향에 관한 연구", 미국헌법연구 제29권 제1호, 2018.4., 3-4면.

유럽의회는 2014년 3월 12일에 그에 대한 제1독회(1st reading)의 입법적 결의(7427/14)를 하였고, 2015년 6월 24일부터 유럽의회, 유럽이사회, 유럽위원회의 3자간 협의를 시작하여 2015년 12월 15일에 최종합의안을 공표하기에 이르렀다. 2016년 4월 8일에 유럽이사회가, 그리고 2016년 4월 14일에 유럽의회가 각각 최종법안을 채택하였으며, 2016년 5월 4일에 EU공보에 공포되었다.[182] 이로써 "일반개인정보보호규정(General Data Protection Regulation, 이하 'GDPR'이라 한다)"이 공식적으로 성립되었고, 같은 해 5월 24일부터 발효되었다. GDPR은 기존의 EU 개인정보보호지침을 대체하는 법규적 효력을 가지게 되었으며, 2년의 유예기간을 거쳐 2018년 5월 25일 각 회원국에 발효되었다.[183]

GDPR의 기본적인 목적과 원칙은 1995년 지침과 동일하지만, 지능정보화사회에 정보통신기술(ICT)의 발전에 따라 새로이 등장한 개인정보보호 쟁점에 가이드라인을 제공하여 보다 강력하고 통일적인 법제도 체계로서 작용하며, EU 회원국들 뿐만 아니라 EU 회원국들의 개인정보를 취급하고 처리하는 비유럽 국가들에도 의무적으로 적용되는 국제적 기준으로 역할을 하는 중요한 역할을 하고 있다.[184]

GDPR은 유럽연합의 입법형식 가운데 Regulation의 형식을 취하고 있기 때문에, 모든 회원국에 직접 적용된다. 따라서 GDPR은 회원국의 국내법으로의 변형이 없이 직접 적용 된다. 비단 EU 뿐만 아니라 EU 비회원국의 기업이라도 개인정보와 조금이라도 관련되는 한 EU 회원국 시민 대상으로 서비스를 제공하거나 모니터링 할 경우 GDPR이 적용된다[185].

2) GDPR의 구성

182) 함인선, "EU의 2016년 일반정보보호규칙(GDPR)의 제정과 그 시사점", 법학논총 제36권 제3호, 전남대학교 법학연구소, 2016.9, 414-415면.
183) 이한주 외, "지능정보화사회에서 개인정보 법제정비에 관한 비교법적 검토", 성균관법학 제30권 제1호, 2018. 3., 7-8면.
184) 권건보, 이한주, 김일환, 앞의 논문(註 167), 5-6면.
185) 홍선기, 고영미, "개인정보보호법의 GDPR 및 4차산업혁명에 대한 대응방안 연구", 법학논총 제43권 제1호, 2019, 315-316면,

GDPR은 총 11장, 173개 전문, 99개 본문으로 구성된다. 총7장, 72개 전문, 34개 본문으로 구성된 1995년 지침에 비교하면 규정은 대폭 확장되었다[186].

GDPR은 EU시민과 기업들의 개인정보 보호체계를 구축하고 정보친화적인 법률제정을 통하여 EU에서의 개인정보처리(Data processing) 및 사용(Use of personal data)을 규정하여 EU시민과 기업의 경제적 이익(economic interests)과 혁신(Innovation)을 보호하는 것을 목표로 하고 있다. GDPR은 한편에서는 활용에 대해서도 규정하고 있지만 다른 한편에서는 엄격한 동의요건, 개인정보보호책임관 도입, 개인정보보호영향평가제 도입 등 기업의 책임과 의무를 강화하는 등 기존의 1995년 지침보다 더욱 강화된 보호체계를 두고 있다. 특히 4차 산업혁명과 관련하여 GDPR은 정보주체의 권리 면에서 기존의 지침보다 강화된 모습을 보이고 있다. 대표적으로 잊힐 권리(Right to be forgotten)[187], 정보이동권(Right to data portablility)[188] 및 프로파일링(profiling) 처리 제한권[189] 등이 그것이다.[190]

3) GDPR의 주요개념[191]

186) https://gdpr.kisa.or.kr/index.do "GDPR 대응지원센터" 홈페이지 참고.

187) 잊힐 권리(Right to be forgotten)란 정보주체가 원할시 본인 정보로의 링크 또는 복제의 삭제를 청구할 수 있으며, 사업자는 이에 대한 조치를 취할 의무가 있다. 한편 잊힐 권리에 대해서는 알 권리 등과 충돌하여 구글(Google) 사례 등에서 논쟁이 있어 왔었고, 구글은 EU 시민권자(Citizen)에 한하여 검색결과 삭제 요청 페이지를 만들기도 한바 있다.

188) 정보주체는 사업자에게 제공하였던 개인정보를 본인이 돌려받거나 제3자에게로 전송하여 관리토록 할 수 있는 권리를 가진다.

189) 프로파일링(profiling)이란 자동화된 개인정보의 처리 방법으로 이를테면 웹사이트에 접속했을 때 어떠한 정보를 입력하지 않아도 자동으로 위치나 IP등 정보를 수집하여 활용하는 것을 말한다. GDPR에서는 이러한 자동화 처리를 정보주체가 거부할 수 있도록 하였고 정보관리자는 이에 따른 조치를 하여야 한다.

190) 홍선기, 고영미, 앞의 논문(註 171), 316면.

191) GDPR의 주요개념에 관하여는 박노형, "한국 개인정보보호법과의 비교를 통한 EU GDPR의 이해", 언론중재 147, 2018; "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.

(1) 개인정보

GDPR은 개인정보를 정보주체와 관련된 모든 정보라고 정의하면서, 식별가능한 자연인을 '직접적 또는 간접적으로, 특히 이름, 식별번호, 위치 정보 등 온라인 식별자를 참조하거나, 그 자연인의 신체적, 생리적, 유전적, 정신적, 경제적, 문화적 또는 사회적 정체성에 특유한 하나 이상의 요소를 참조하여 식별될 수 있는 자'라고 명시하여, 개인정보를 보다 명확하게 규정한다.[192] 특히 온라인 식별자가 개인정보의 예로써 명시되어서 GDPR 제3조의 역외적용에 따라 인터넷 등에 의하여 EU시장에 진입하는 EU 역외에 설립된 기업 등도 GDPR의 적용을 받게 된다.[193]

(2) 민감정보

GDPR은 특수한 범주의 개인정보, 즉 민감정보의 처리를 원칙적으로 금지한다. GDPR은 제9조에서 일반적인 민감정보를, 제10조에서 범죄경력과 범죄행위에 관련된 개인정보를 별도로 규정한다. 또한, GDPR은 '인종이나 민족 기원'을 드러내는 개인정보와 '자연인을 고유하게 식별할 목적의 바이오인식정보'를 민감정보로서 명시하고 있다.

(3) 정보주체

GDPR은 정보주체를 별도로 정의하지 않고, 개인정보에 관한 정의에서 '식별된 또는 식별가능한 자연인'이라고 확인한다. 1995년 지침과 달리 GDPR은 '죽은 사람(deceased person)'의 개인정보에 적용되지 않는다고 명시한다[194].

(4) 컨트롤러(controller)

GDPR의 컨트롤러는 개인정보 처리의 목적과 수단을 결정하는 자연인이나 법인, 공공당국, 에이전시 또는 다른 기구를 가리킨다.[195] 컨트롤러는 스스로 개인정보를 처리할 필요가 없다. 컨트롤러는 직접 또는 제3자, 즉

0001.01.ENG&toc=OJ:L

192) GDPR Article 4 Definitions (1) (GDPR 제4조 제1호)

193) 박노형, 위의 논문(註 177), 66면.

194) GDPR 전문 제27항

195) GDPR Article 4 Definitions (7) (GDPR 제4조 제7호)

프로세서를 활용하여 개인정보를 처리할 수 있는데, 개인정보 처리에 관련된 원칙에 대한 책임을 지고, 이의 준수를 증명할 수 있어야 한다.[196] 또한, 컨트롤러는 개인정보 처리가 GDPR에 따라 수행되는 것을 보장하고 이를 증명할 수 있는 적절한 기술적 및 관리적 조치를 이행하여야 한다.[197]

(5) 프로세서(processor)

GDPR의 프로세서는 컨트롤러를 대신하여 개인정보를 처리하는 자연인이나 법인이다.[198] 컨트롤러는 GDPR 요건을 충족하고 적절한 기술적 및 관리적 조치를 이행한다는 충분한 보증을 제공하는 프로세서만 이용해야 한다.[199] 컨트롤러를 대신하여 개인정보를 처리하는 점에서 프로세서는 컨트롤러의 이익을 위하여 컨트롤러와 위탁에 관한 계약 등이 필요하다.[200] 프로세서의 개인정보 처리에 대하여 컨트롤러가 일체의 책임을 지는 점에서 컨트롤러는 프로세서의 개인정보법령 준수를 감독하여야 한다[201]. 프로세서는 컨트롤러의 사전 허가를 받아 다른 프로세서에게 개인정보 처리를 재위탁할 수 있다.[202] GDPR의 위반에 대한 과징금은 컨트롤러와 프러세서가 이행한 기술적, 관리적 조치를 고려하여 각자의 책임 정도에 따라 부과된다.[203]

(6) 처리

GDPR의 처리는 자동화된 수단이나 비자동화된 수단, 즉 수기 여부를 불문한다. 수기 처리에 해당하는 파일링시스템(filing system)을 별도로 정의하는데[204], 한국 「개인정보보호법」의 개인정보파일과 유사하다고 볼 수

196) GDPR Article 5 Principles relating to processing of personal data 2. (GDPR 제5조 제2항)
197) GDPR Article 24 Responsibility of the controller 1. (GDPR 제24조 제1항)
198) GDPR Article 4 Definitions (8) (GDPR 제4조 제8호)
199) GDPR Article 28 Processor 1. (GDPR 제28조 제1항)
200) GDPR Article 28 Processor 3. (GDPR 제28조 제3항)
201) GDPR Article 28 Processor 3.(h) (GDPR 제28조 제3항(h))
202) GDPR Article 28 Processor 2. (GDPR 제28조 제2항)
203) GDPR Article 83 Processor 2.(d) (GDPR 제83조 제2항(d))
204) GDPR Article 4 Definitions (6) (GDPR 제4조 제6호)

있다. GDPR의 처리는 수집부터 파기까지 다양한 처리 유형을 예로써 명시한다.[205] GDPR은 처리를 '개인정보 또는 개인정보의 집합물에 대하여 수행되는 모든 작업 또는 일련의 작업'을 의미한다고 규정하여, 개인정보에 대한 작업은 포괄적 처리로서 인정된다.

(7) 개인정보보호책임자(data protection officer)

GDPR의 컨트롤러와 프로세서는 다음의 경우에는 필수적으로 개인정보보호책임자를 지정해야 한다.[206] 첫째, 처리가 공공당국 또는 기관에 의해 수행되는 경우인데, 사법적 지위에 따른 법원의 경우는 예외로 한다. 둘째, 컨트롤러 또는 프로세서의 핵심적 활동이 그 성격, 범위, 목적에서 대규모로 정보주체에 대해 정기적이고 조직적인 감시를 요구하는 처리작업으로 구성되는 경우이다. 셋째, 컨트롤러 또는 프로세서의 핵심적 활동이 특수한 범주의 정보 및 범죄경력과 범죄행위에 관련된 개인정보 즉, 민감정보의 대규모 처리로 구성되는 경우이다. 넷째, EU 또는 회원국법이 요구하는 경우이다. GDPR의 개인정보보호책임자는 전문적 자질, 특히 개인정보보호법과 실무에 대한 전문적 지식 및 개인정보보호책임자의 직무를 완수할 능력에 근거하여 지정되어야 한다.[207] 개인정보보호책임자는 컨트롤러 또는 프로세서의 직원일 수 있고, 서비스계약에 근거하여 직무를 완수할 수 있는 자로 볼 수 있다.[208]

(8) 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적의 추가적 처리

GDPR은 '목적제한 원칙'에 따라 수집된 목적에 따른 처리를 요구한다. 이러한 원칙에도 불구하고 공익적 기록보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적의 추가적 처리는 '최초의 목적'과 양립할 수 있다고

---

205) GDPR Article 4 Definitions (2) (GDPR 제4조 제2호)
206) GDPR Article 37 Designation of the data protection officer 1.,4. (GDPR 제37조 제1항 및 제4항)
207) GDPR Article 37 Designation of the data protection officer 5. (GDPR 제37조 제5항)
208) GDPR Article 37 Designation of the data protection officer 6. (GDPR 제37조 제6항)

하여 그 예외가 허용된다.[209] '공익을 위한 기록보존 목적'과 관련하여, 공익적 가치를 지닌 기록물을 보유하고 있는 공공당국 또는 공공, 민간기관이 수행하는 기록물의 획득, 보존, 평가, 편찬, 기술, 교환, 홍보, 배포, 제공은 목적 외 추가처리로서 허용된다.[210] '과학적 연구 목적'의 개인정보 처리는 폭 넓게 해석되어야 하는데, 기술의 발전과 실현, 기초연구, 응용연구 및 민간투자연구, 공중보건 분야에서 시행된 공공보건연구를 포함한다[211]. 따라서 민간부분의 R&D의 목적으로 원래의 수집된 목적과 다른 처리가 가능할 것이다. '역사적 연구'에는 족보나 인명기록부 등 혈연관계나 계보를 밝히는 계보적 연구가 포함된다.[212] 이러한 세 가지 목적의 처리는 정보주체의 권리와 자유를 위하여 적절한 안전장치의 적용을 받아야 하는데, 그 안전장치들은 가명처리 등 기술적, 관리적 조치가 구비되는 것을 보장해야 한다.[213]

(9) 가명처리(pseudonymisation)

GDPR에서 처음 도입된 가명처리는 추가정보의 이용 없이 개인정보가 더 이상 특정 정보주체에게 귀속될 수 없는 방식으로 개인정보를 처리하는 것을 말한다.[214] 가명처리를 통하여 개인정보 처리에서의 정보주체에 대한 위험이 저감될 수 있다.[215] 개인정보의 유용성을 유지하면서 프라이버시를 제고하는 기법인 가명처리는 개인정보 처리의 암호화와 함께 '적절한 안전장치'의 예가 된다.[216] 따라서 가명처리를 활용하는 컨트롤러에게 상당한 부담이 감경된다. 한편, 가명처리는 다른 개인정보보호 조치를 배제하는 것

---

209) GDPR Article 5 Principles relating to processing of personal data 1.(b) (GDPR 제5조 제1항(b))
210) GDPR 전문 제158항
211) GDPR 전문 제159항
212) GDPR 전문 제160항
213)GDPR Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes 1. (GDPR 제89조 제1항)
214) GDPR Article 4 Definitions (5) (GDPR 제4조 제5호)
215) GDPR 전문 제28항
216) GDPR Article 6 Lawfulness of processing 4.(e) (GDPR 제6조 제4항(e))

은 아니다.[217] 가명처리된 개인정보, 즉 가명정보는 여전히 GDPR의 적용을 받으므로, 가명정보의 처리도 GDPR의 요건을 충족해야 한다.

(10) 과징금(administrative fines)

GDRP은 위반된 규정의 중요도에 따라 최대 1천만 유로(사업자의 경우 이 금액과 전년도 세계매출액의 2% 중 더 큰 금액), 또는 최대 2천만 유로(사업자의 경우 이 금액과 전년도 세계매출액의 4% 중 더 큰 금액)의 과징금을 부과할 수 있도록 규정하고 있다.[218]

Ⅱ. 독일

헌법에 구체적으로 명시되어 있지는 않으나, 1983년 독일 연방헌법법원은 독일 헌법 제1조 제1항의 “인간의 존엄성”과 “국가의 인간 존엄성 보호 의무”, 제2조 제1항에 명시된 “인격자유”를 “개인의 정보 자기결정권리(Recht auf informationelle Selbstbestimmung)”라는 권리로 해석하고 있다.[219]

독일의 개인정보보호 관련 법률은 사실상 기본법으로서 연방개인정보보호법(Bundesdatenschutzgesetz, 이하 BDSG)와 개인정보를 다루는 특수한 국가기관들에 관한 법률들이다. 예를 들어 연방헌법수호청법, 군사정보보호청법, 해외정보기관법 등이 그것이다. 따라서 BDSG가 개정되면 다른 법률들도 이에 부수하여 같이 개정된다. 2017년 개정된 연방개인정보보호법(BDSG)은 전체 4부, 19장, 2절, 85조문으로 구성되어 있다. 제1부는 일반규정, 제2부는 GDPR의 이행 규정들, 제3부는 형사사법지침 2016/680/EU의 이행 규정들, 제4부는 GDPR과 형사사법지침 2016/680/EU가 적용되지 않는 영역에서의 처리를 위한 특별 규정들로 이루어져 있다. 이를 통해 확인할 수 있듯이 BDSG는 처음부터 GDPR을 반영하기 위해서 개정되었다는

217) GDPR 전문 제28항
218) GDPR Article 83 Processor (GDPR 제83조)
219) 한국인터넷진흥원, “독일 개인정보보호 법 행정 체계 현황 및 주요 위반사례 (’21.11월 기준)”, 2021.11.

점이다. 따라서 양자를 철저히 반영하고 있다. 독일의 경우 개인정보처리의 국제적 기준에 최대한 부합한 국내법을 마련함으로써 자국민과 자국기업이 국제규범의 위반으로 발생할 수 있는 불이익의 최대한 방지하고자 하고 있다.[220]

GDPR은 EU 일반법으로서 독일 국내법인 BDSG보다 상위법에 위치해 두 법이 직접적으로 충돌할 경우 GDPR을 따르도록 규정하고 있다. BDSG은 제1조제5항에서 GDPR이 직접 적용되는 법률적 상황에서 BDSG은 효력을 갖지 않는다고 명시하여, 사실 상 GDPR이 제시하는 바를 거의 대부분 수용하고 직접 적용하여 받아들이고 있는 것을 의미한다. GDPR의 지침을 따른 독일 국내법 BDSG은 구체적 법률 시행과 GDPR에서 다루어지지 않은 사항들을 보충하고 있다고 볼 수 있다.[221]

4차 산업혁명이 도래하면 대부분의 산업은 사실상 빅데이터에 의존하고 있고, 이러한 경우 개인정보의 활용과 남용은 피할 수 없는 사실이다. 이러한 상황에서 중요한 것은 결국 정보주체의 권리를 얼마나 잘 보호함으로써 그 남용의 폐해를 막아내는가 인데, 이를 반영하여 BDSG에서도 정보주체의 권한을 상당히 강화하고 있다. 그 중에서 특히 민감정보에 관한 규정을 많이 두고 있음으로써 그 남용을 막기 위해서 노력하고 있다. 이처럼 BDSG의 가장 큰 특색은 바로 민감정보에 관한 규정이다. GDPR에서 입법재량으로 남긴 기존의 다른 분야는 거의 그대로 직접적용 방식을 채택함으로써 제2부인 GDPR 이행규정인 제22조에서 제44조에는 거의 관련 내용을 규정하지 않은 반면에 민감정보의 경우 제22조부터 28조에 이르기까지 관련내용을 담고 있다. 뿐만 아니라 제3부의 형사사법지침 이행 규정 파트에서도 제46조의 개념규정에서 재차 민감정보에 대한 정의 규정을 두고 있고 제48조에서는 민감정보의 처리에 관해 규정하고 있다. BDSG에 이렇게 많은 민감정보 규정을 둔 이유는 GDPR이 민감정보 처리와 관련해서는 상당히 많은 입법재량을 회원국에 부여하고 있기 때문이라 볼 수 있다. 또한,

220) 홍선기, 고영미, 앞의 논문(註 171), 320-321면.
221) 한국인터넷진흥원, 앞의 보고서(註 205).

삭제권(잊힐권리)도 우리보다는 더 폭넓게 인정하고 있으며, 우리에게는 인정되고 있지 않은 반대권이나 정보이전권 등도 인정된다.[222]

Ⅲ. 프랑스

프랑스는 개인정보보호에 대한 헌법상 근거는 없으나 1970년 7월 개정된 민법(Code civil) 제9조에서 개인의 사생활(vie privée)의 자유권을 보장한 것이 가장 근접한 근거라고 볼 수 있다. 최초의 개인정보보호 기본법은 1978년 1월 6일 제정된 개인정보보호법(Loi informatique et libertés, 이하 LIL)으로, 공공과 민간부문의 개인정보보호를 통합적으로 규율하고 있다.

프랑스 정부는 1970년대 초부터 사회보장번호에 전 국민의 모든 행정문서를 연계해 데이터 베이스화하기 위한 계획(SAFARI)[223]을 추진하였고, 1974년 3월 르 몽드(Le Monde)지가 이 계획에 대한 고발 기사 '사파리, 또는 프랑스인 사냥(SAFARI, ou la chasse aux Français)'을 게재하면서 대중에게 알려졌다. 공권력에 의한 감시와 사생활 침해를 우려한 시민의 거센 반발에 부딪혀 SAFARI 계획이 무산되었고 동 사건을 계기로 개인정보보호제도 도입 논의가 활발해지면서 프랑스 정부는 가칭 '정보처리 및 자유 위원회(commission dite Informatique et libertés)'를 구성해 정책 수립을 논의하였다. 이후 1975년 동 위원회는 개인정보보호법 제정 및 법 이행과 감독을 위한 독립기구 설립 등을 제언하는 보고서를 정부에 제출하였고, 1978년 1월 6일 LIL을 제정하고 이를 근거로 프랑스 개인정보 감독기구(Commission Nationale de l'Informatique et des Libertés, 이하 CNIL)가 정식 출범하였다.[224]

---

222) 홍선기, 고영미, 앞의 논문(註 171), 321-323면.

223) 행정문서 및 개인정보 목록 자동화 시스템 계획(projet SAFARI, Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus)

224) 한국인터넷진흥원, "프랑스 개인정보보호 법 행정 체계 현황 및 주요 위반사

프랑스 개인정보보호법 제1조는 공·사 영역에 대한 구별 없이 법이 적용될 수 있는 길을 열어놓았고, 동법 제11조에서는 위원회의 행정관청으로서의 권한을 상세하게 명시하는 수권규정을 두고 있다. 1978년 개인정보보호법 제정 이래 프랑스에서는 일관되게 독립행정기관인 CNIL에 의해 그 정책과 집행이 이루어지고 있다. CNIL은 개인정보에 관해서 공공 부문과 민간 부문을 구별하지 않고 통합하여 관리하기 때문에 사실상 거의 모든 분야의 개인정보를 포괄하여 관장한다. 18인의 위원 구성에 있어서 법관과 감사위원 자격 보유자를 포함하고 있는 점과 성비가 고려되고 있다. CNIL은 정책제안, 심의, 허가와 신고에 관한 규제권, 감독권과 제재권 등 개인정보보호에 관한 종합적 기능을 행사하며 사무처에는 법률전문직의 비중이 높아 이러한 기능을 수행하는 데 적절하다. 유럽연합의 규범에 맞춘 개정 중 특히 1995년의 EU 개인정보지침(Directive 95/46/EC)의 국내법화를 위한 2004년 8월의 개정으로 내용이 대폭 수정됨에 따라 개인정보의 개념에 대한 표현을 종전의 기명정보(information nominative)에서 인적특성정보(donnée à caractère personnel)로 변경하였다. 이 법은 개인정보 여부를 식별가능성을 기준으로 판단하고 있으며 정보처리의 개념도 상세하게 규정하고 있는데, 판례에 의해 확장되고 있다.[225]

2016년에 디지털공화국법, 보건시스템현대화법, 사법 현대화에 관한 법률에 의해 개인정보보호법을 위시한 관련법을 개정하였는데, 개인정보보호 자체에 관한 사항뿐만 아니라 타법과의 관계를 정비하기 위한 입법으로 볼 수 있다.[226] 개인정보 보호의 강화와 개인정보 이용의 가능성 확대라는 두 가지 모순을 조화를 이루고자 한 노력이라 볼 수 있다.

특히 디지털공화국법은 고지의무를 강화하고 잊힐 권리(삭제권)를 신설하는 등 정보보호를 강화하면서도 공공데이터의 개방 확대와 더불어 익명화 처리를 이용한 이용가능성을 확대한 점이 특징이다. 보건시스템현대화법은

례('21.11월 기준)", 2021.11.

225) 홍선기, 고영미, 앞의 논문(註 171), 326-327면.

226) 홍선기, 고영미, 앞의 논문(註 171), 326-327면.

연구 목적의 건강정보 이용가능성을 확대하였고 사법 현대화에 관한 법률은 정보침해에 대한 권리구제를 용이하게 하기 위한 집단소송을 도입하였다.[227]

EU의 GDPR 제정 이후, 프랑스는 CNIL을 중심으로 GDPR 전면 시행에 대응하여 LIL를 개정하고 있다. 2018년 6월, CNIL 직원이 조사 가능한 시설 및 건물 확대하고, 지자체· 협회· 기업에 벌금 및 과징금 제재를 가할 수 있도록 CNIL의 조사 및 제재 권한을 강화하였다. 그리고 생체정보 및 유전정보, 성적취향 정보를 민감 정보에 포함하여 민감정보 범위 또한 확대하였다. 2018년 12월에는 규정에 대한 개정이 아닌 LIL의 가독성 제고를 위한 구성 재편 및 'EU 형사사법 개인정보보호지침((EU)2016/680)'을 국내법에 반영하여 보완하였는데 이 점이 특히 주목적이다[228].

Ⅳ. 영국

영국은 다른 국가와 달리 성문 헌법이 없으므로 개인의 프라이버시권을 부여하는 헌법이 없으며, 그 대신 개인정보보호 일반법에 해당하는 영국 일반 개인정보보호법(UK General Data Protection Regulation, UK GDPR) 및 개인정보보호법 2018(Data Protection Act 2018, DPA)을 필두로 각 영역별 필요에 따라 도입된 개별 법률 등으로 개인정보보호 법제가 구성되어 있다. 개별 법률에는 공공기관이 다루는 개인정보에 대한 영국 국민들의 알권리를 보장하는 정보자유법, 정보통신 분야의 개인정보보호를 특별히 다루는 프라이버시 전자통신규정, 의료·보건 분야의 건강기록에 대한 열람권을 규율하는 건강기록접근법 등이 있다.[229]

---

227) 홍선기, 고영미, 앞의 논문(註 171), 326-327면.
228) 한국인터넷진흥원, 앞의 보고서(註 210).
229) 한국인터넷진흥원, "영국 개인정보보호 법 행정 체계 현황 및 주요 위반사례 ('21.11월 기준)", 2021.11.

1. 개인정보보호법(Data Protection Act, DPA)

1984년 최초 제정되어 한 차례 개정을 거쳐 오늘날에 이른 개인정보보호법(Data Protection Act, 이하 DPA)은 EU GDPR 시행에 따라 동 법의 영국 내 적용을 위해 2018년 개정 발효되었다. EU 회원국 내 동일한 법률을 적용하기 위해 제정된 EU GDPR은 일부 조항에 대해 회원국별 상황을 반영할 수 있도록 재량권을 부여하였고, 이에 영국은 DPA를 통해 아동 연령 및 개인정보 식별자에 대한 범위 등을 영국 상황에 맞게 2018년 5월 25일 제정·발효하였다. 현재 시행 중인 DPA는 영국의 유럽연합 탈퇴로 인해 개인정보보호, 프라이버시, 전자 커뮤니케이션 수정법 제정을 계기로 한 차례 더 수정을 거쳤다. EU GDPR과 마찬가지로, UK GDPR은 전체적으로 같은 맥락을 유지하고 있으며 UK GDPR이 규정하지 않는 범위에서는 재량에 따라 확대하여 규정하고 있다.

DPA는 총 7장 215개 조항으로 이루어져 있고, UK GDPR 등에 따른 개인정보 처리(제2장), 사법 당국의 법 집행을 위한 개인정보 처리(제3장), 정보기관(Intelligence services)에 의한 개인정보 처리(제4장), 정보커미셔너(ICO 커미셔너)의 역할(제5장), 법 집행절차(제6장) 등으로 구성되어 있고, 제5장을 통해 UK GDPR과 DPA를 집행하는 ICO의 집행 권한을 명명하고 있다.[230]

DPA는 사람들이 자신의 개인정보를 더욱 강력하게 통제할 수 있도록 하고, 디지털 시대의 데이터 보호 프레임워크를 보장하기 위해 마련되었다. 그 구체적인 내용을 살펴보면 사람들이 자신의 개인정보를 보다 안전하게 통제하고, 소위 잊힐 권리(right to be forgotten) 등을 통하여 개인정보를 보다 더 강력하게 관리하며, 소셜 미디어 플랫폼에 대해 아동용 또는 성인용 정보를 삭제하도록 요구할 수 있도록 하고 있다.[231] 나아가 기업, 공공

230) 한국인터넷진흥원, 위의 보고서(註 215).

231) '개인 데이터(personal data)'의 개념을 보다 명확히 하며, 그 개념에 IP 주소, 인터넷 쿠키, DNA도 포함시키고, 일반 개인들은 관련 사업자들이 자신의 개인정보를 보유하고 있는지 여부에 대한 공개를 보다 쉽게 요구할 수 있도록 하였다.

기관 등에 대해서는 개인정보를 보다 적합하게 관리하고 보안을 유지할 의무를 부과하고, 이를 위반한 경우 엄격하게 제재를 가할 수 있는 권한[232]을 정보위원회(Information Commissioner's Office, ICO)에 부여하고 있다.

2. 일반 개인정보보호법(UK General Data Protection Regulation, UK GDPR)

영국의 유럽연합 탈퇴(브렉시트) 선언 이후 2019년 2월 제정된 개인정보보호, 프라이버시, 전자 커뮤니케이션 수정법[233]을 근거로 EU GDPR을 UK GDPR로 명명하였고 이를 2021년 1월 발효하였다. 2018년 5월부터 EU의 GDPR이 영국에서도 직접 적용되고 있었으나, 영국의 유럽연합 탈퇴로 인해 유럽연합 법률이 더 이상 영국 내에 적용되지 않는 법적 공백을 야기하였다. 영국은 유럽연합 탈퇴법(European Union (Withdrawal) Act 2018)을 제정하여 EU 법령이 그대로 영국 국내법으로서 기능할 수 있도록 노력[234]하였고 그 과정에서 이전대로 EU GDPR과 영국 개인정보보호법(DPA)이 그대로 적용될 경우 변화한 법적 상황을 반영하지 못하게 되는 것을 이유로, 영국은 개인정보보호, 프라이버시, 전자 커뮤니케이션 수정법을 제정하여 개인정보 관련 법률에 수정을 가하는 등 개인정보보호 법제 전반을 정비하였다. UK GDPR은 실질적으로 EU GDPR과 동일한 내용을 담고 있고 단지 일부 조문이나 단어를 대체, 추가, 제거하는 등 최소한의 변경만을 가한 것으로, 개인정보보호법(DPA)과 더불어 영국 개인정보보호 법제를 이루는 큰 축 중 하나이다.[235]

---

232) 사업자들이 익명화된 데이터에서 고의적으로 개인들을 식별할 수 있는 환경을 조작하는 행위를 금지하기 위하여 새로운 형사상 범죄유형들을 적시하였다.

233) The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations

234) 유럽연합 탈퇴법(European Union (Withdrawal) Act 2018) 제3조에서는 영국에 직접 적용되어 오던 EU 법령(regulation)·결정(dicision)·하위입법(tertiary legislation)의 경우, 영국이 유럽연합을 탈퇴하더라도 그대로 영국의 국내법을 이룬다고 규정하고 있다.

Ⅴ. 미국

미국에서 빅데이터의 활용 또는 활성화에 거대한 걸림돌로 작용하는 것이 개인정보 보호법제이지만, 미국은 영국, 독일, 이탈리아, 스페인, 핀란드 등 유럽국가들이나 호주 및 뉴질랜드와는 달리 정보통신분야의 개인정보보호에 관한 법률을 기본법으로 마련하고 있는 나라는 아니다. 이와 같이 미국에서는 개인정보의 보호와 관련하여 포괄적인 입법을 지양하고 개별 분야별로 규율하는 단행법을 제정하여 시행하고 있다.[236] 미국에서 개인정보 보호는 공공부문과 민간부문으로 나누어지며, 법은 공공부문에만 적용하고, 민간부문에 대해서는 원칙적으로 윤리적 통제만 가능하도록 하고 있다. 즉, 원칙적으로 연방정부가 보유하고 있는 정보를 공개하기는 하지만, 프라이버시법에 의한 정부 규제가 이루어지고, 민간부문에서는 원칙적으로 정보의 자유로운 유통을 보장하면서 개별 분야에서의 개인정보 보호를 목적으로 영역별로 법제를 가지고 있는 점을 특징으로 들 수 있다. 이러한 개별법 체계는 장점과 함께 단점을 가지는데, 장점은 보호가 특히 필요한 개인정보 취급영역에 한정해 법적 규제를 가하는 점이며, 단점은 개별영역별로 법률을 제정함으로써 관련 업계 혹은 이익단체의 영향을 받을 우려가 높다는 점이다.[237]

현재 연방 차원의 개인정보 보호법제로는 정보자유법(Freedom of Information Act of 1966), 공정신용조사법(Fair Credit Reporting Act of 1970), 프라이버시법(Privacy Act of 1974), 금융프라이버시권법(Right to Financial Privacy Act of 1978), 프라이버시보호법(Privacy Protection Act of 1980), 전자통신프라이버시법(Electronic Communication Privacy Act of 1986) 등을 들 수 있다. 그리고 인터넷상의 개인정보 보호를 위해 '소비자

235) 한국인터넷진흥원, 위의 보고서(註 215).
236) 최경진 외 5인,□빅데이터 환경에서 개인정보호 강화를 위한 법·제도적 대책 방안 연구", 개인정보 보호위원회, 2012.12. 43면.
237) 김상겸 외 5인, "개인정보보호법 정비방안 연구", 한국인터넷법학회, 2012, 25-26면.

온라인 프라이버시 공개법'(Consumer Online Privacy and Disclosure Act)과 '소비자 인터넷 프라이버시 증진법'(Consumer Internet Privacy Enhancement Act) 등의 법안이 의회에 제출된 바 있다. 또한 빅데이터 정보환경에 개인정보를 보호하기 위한 최근의 법률로는 미국 의회 제113회기인 2013년부터 2014년 사이에 제출된 '전자 통신 프라이버시법 개정안'(Electronic Communications Privacy Act Amendments Act of 2013) 등을 들 수 있다. 또한, 미국의 경우 이러한 개인정보 보호법제에 의한 법적 규율 외에도 자율적 규제의 움직임도 있었다. 기업에 의한 자율적 규제의 대표적인 예로는 1999년 11월 네트워크 광고 이니셔티브(Network Advertising Initiative, NAI)의 창설과 NAI 원칙(The NAI Principles)의 제안 등을 들 수 있다. 이에 따라 Google과 Amazon 등 온라인 사업자도 약관과 내부규칙을 통하여 개인정보를 보호하고 있으며, NAI는 소속 회원사를 위한 자율규제규칙을 제정·운영하고 있다. 또한 2002년 12월 공포된 '전자정부법'(E-Government Act of 2002)에서는 국민 중심의 전자정부를 구현하는 과정에서 개인정보와 프라이버시가 충분히 보호되도록 프라이버시 영향평가(Privacy Impact Assessment)를 실시하도록 명문화하였다(제28조).[238]

그럼에도 불구하고, 2013년 대형 소매점 타깃(Target)사건[239]을 비롯하여, 대기업에 의한 개인정보 유출이 빈번하게 발생되었고,[240] 대규모 소셜 네

238) 최경진 외 5인, 위의 논문(註 222), 2012.12. 44면.

239) Target은 현재 1,829개소의 점포를 가지고 있는 대형소매점으로서, 2019년 미국 소매업 매출랭킹 8위를 차지하고 있다("Stores Top Retailers 2019", STORES NRF'S MAGAZINE, https://store.org/stores-top-retailers-2019). 이러한 대형소매점에서 발생된 정보유출사건은 당시까지 미국 소매업 역사상 찾아볼 수 없는 대규모 정보유출사건이라고 일컬어지고 있다(In re Target Corporation Customer Data Security Breach Litigation, Relates to Consumer Cases, MDL No,14-2522, PAM/JJK, Signed Dec. 18, 2014, p.1157), 김창화, "미국에서의 개인정보 유출 관련 소송에 대한 연구", 「정보법학」 제19권 제3호, 한국정보법학회, 2015, 12, 39면.

240) Miles Parks, Target Offers $10 Million Settlement in Data Breach Lawsuit, NPR(Mar. 19, 2015); Maggie McGrath, "Target Data Breach Spilled Info On As Many As 70 Million Customers", Forbes(January 10, 2014);

트워크(Social Networks) 기업이 그 이용자의 개인정보를 다른 기업으로 유출한 것이 발각되어 전 세계에 큰 화제가 되기도 하였다.[241] 이같이 미국 전역에서 데이터 유출(data breach)이 지속적으로 증가하고 미국 내 거대 디지털 기업이 소비자의 정보를 무단 이용하는 사례가 알려지면서 미국 소비자들의 데이터와 프라이버시 보호에 대한 요구가 확산되었다.[242] 특히 2017년 7월에 신용조사기관인 이퀴팩스(Equifax)에서 발생한 1.46억 소비자의 개인정보 유출사건과 2018년 3월의 페이스북(Facebook) 이용자 정보가 미 대선 맞춤형 광고에 활용된 사례 등은 미국사회에 큰 반향을 일으켰고, 소비자들은 개인정보보호에 대한 법적 보호 장치 마련을 요구하였다.[243]

더불어 소비자 개인정보 보호, 정보보안 및 아동 온라인 개인정보 보호 등에 대한 감독과 규제의 기능을 수행하는 연방거래위원회(Federal Trade Commission, 이하 FTC)의 권한과 역량 부족에 대한 문제점도 제기되었다. FTC는 소비자 정보를 활용하는 기업에 대하여 벌금 부과 권한을 가지고 있지만 집행력을 강제하기에는 벌금 수준이 낮았고, 미국 전역의 디지털 혁신기업과 금융, 신용 기관을 감독하고 소비자 정보의 침해 여부를 판단할 만한 숙련된 전문가 등 인력이 부족하였다.

이에 대응하여 최근 2022년 6월 3일 미국 의회의 양당 의원들은 연방 개인정보보호법안(American Data Privacy and Protection Act, 이하 ADPPA)을 발의하였고, 6월 23일 공개수정을 거쳐 하원 전원위원회에 회부되었다.

Liana B. Baker & Jim Finkle, Sony Playstation suffers massive data breach, REUTERS(Apr. 27, 2011); John Kell, Home Depot facing dozens of data breach lawsuits, FORTUNE(November 25, 2014).

241) Cecilia Kang and Sheera Frenkel, “Facebook Says Cambridge Analytica Harvested Data of Up to 87 Million Users”, New York Times(April 4, 2018).

242) Risk Based Security의 통계에 의하면, 미국에서는 2017년에만 약 78억 9천만건의 정보유출 사건이 발생하였다고 한다(Risk Placement Services, Inc., Data Powered by Risk Basad Security, Data Breach QuickView Report, Year End 2017).

243) 김용일, 김유정, “우리나라 개인정보보호 법제의 개선방안에 관한 연구”, 법과 정책 제27권 제1호, 2021.3.30., 88-89면.

ADPPA는 실제 제정까지는 여러번의 개정작업을 거칠 가능성이 높지만, 미국 연방 일반법으로 적용범위가 넓어 큰 영향력을 발휘할 수 있을 것이고 새로운 변화와 방향이므로 내용을 살펴보고 대비해야 할 필요가 있을 것이다.[244]

Ⅵ. 일본

일본은 '개인정보보호법'과 '개인정보보호 기본방침'을 토대로 공공 분야와 민간 분야를 대상으로 한 개인정보보호 법률과 가이드라인이 제정되어 있다. 민간 분야에는 금융, 의료, 정보통신 각 분야별 가이드라인을 통해 법령 준수 가이드를 제공하고 있고, 공공 분야에는 행정기관, 독립행정법인[245] 및 공공단체 등 각각을 대상으로 한 행정기관 개인정보 보호법, 독립 행정법인 개인정보 보호법, 개인정보 보호조례 등이 있다.[246]

일본은 개인정보보호를 위한 최초의 법제로서 1988년 '행정기관이 보유한 전자계산기처리와 관련된 개인정보보호에 관한 법률'을 마련했으며, 2003년 5월 민간 영역을 규제대상에 포함시킨 '개인정보보호법'이 최초 제정되어 2005년부터 전면 시행되었다.

이후 기술 발전에 비해 개인정보의 보호를 위한 법제도의 준비가 미비하였고, 새로운 기술에 맞는 새로운 법제도의 도입이 필요하게 되었다. 이에 기업과 정부의 ICT 이용을 높이고 동시에 개인정보 보호를 강화시키기 위한 목적으로 개인정보보호법 개정을 추진하였고, 2015년 9월 3일 중의원

---

244) 한국인터넷진흥원, "개인정보보호 월간동향분석(미국 연방 개인정보보호법안(ADPPA) 주요 내용과 시사점)", 2022.5., 3-4면.

245) 법인 설립체 중 국민생활 및 사회경제 안정 등의 공적인 관점에서 제공될 필요성이 명확한 사무 및 사업을 담당하는 법인을 말한다. 내각부 산하의 국립공문서관과 일본의료연구개발기구 총무성 산하의 정보통신연구기구와 통계센터 등이 이에 해당된다.

246) 한국인터넷진흥원, "일본 개인정보보호 법 행정 체계 현황 및 주요 위반사례('21.11월 기준)", 2021.11.

본회의 가결을 거쳐 2017년 5월부터 전면 시행되었다. IT 기술의 진보에 따라 '개인정보보호법'이 제정될 당시에 상정하지 못한 데이터가 '개인정보'에 해당하는지의 여부가 애매한 영역에 해당하는 것이 증가했기 때문에 이번 개정에 의해 개인정보의 정의가 명확해지게 되었다. 예를 들면 안면인식 데이터나 지문데이터 등의 '신체적 특징'이나 개인번호, 운전면허증번호, 여권번호 등이 '개인 식별 부호'로 추가되었다. 개인정보의 이용과 전 세계에서 취급되는 개인정보의 증가로 인해 국제적으로 개인정보 보호가 중요 관심사로 부각하였고 그러한 분위기를 반영하여 범죄이력이나 병력 등 부당한 차별이나 편견을 받을 가능성이 있는 정보를 '배려를 요하는 개인정보'로 규정하고 취득할 경우는 원칙적으로 본인의 동의가 필요하도록 하였다. 또한, 개인정보를 제3자에게 제공할 때의 기록 작성을 의무화하며, 개인정보취급사업자가 부당하게 이익을 얻을 목적으로 정보를 제공하거나 취득하면 처벌되도록 하는 규정 등이 있다. 또한, '익명가공정보'가 신설되었는데, 일정한 조건 하에서 특정 개인을 식별하지 못하도록 가공된 정보는 본인의 동이 없이 제3자에게 제공하는 것이 가능하도록 하였다.[247]

EU의 GDPR에 대응하여 최근 2020년 6월에는 지능정보화사회에 따른 혁신 기술을 기반으로 한 개인정보를 활용할 수 있는 조건을 명확히 하고 기업이 개인의 인터넷 열람 이력을 제3자에게 제공하는 행위를 규제하기 위해 또 한 차례의 개인정보보호법 개정안이 가결되어 2022년 4월 시행되었다. 최근 개정 주요 내용으로는 첫째, 개인정보가 포함된 기술(記述)을 일부 삭제하여 다른 정보와 대조하지 않는 한 특정 개인을 식별할 수 없도록 가공된 개인정보로서 개인정보에 대한 자체 분석은 허용하되 익명가공된 정보와는 달리 제3자 제공이 불가하다(제2조제9항)는 가명정보 개념을 추가하였다. 둘째, 쿠키 등 개인과 연관되어 사용하는 데이터 제공 시 본인동의를 의무화하고, 원치 않는 개인정보 이용을 중지할 수 있도록 기업에 요구할 수 있는 권리를 보장(제16조 외)하여 정보주체의 권리보호를 강화하였다. 셋째, 개인정보보호법을 위반한 법인에 대해 최대 1억엔까지 벌금을

247) 이한주 외, 앞의 논문(註 169), 29-31면.

상향조정하며(제87조제1항제1호), 일본 국내 체재자의 개인정보를 취하는 해외 기업에도 징수 및 명령을 확대(제75조외)하여 법집행을 강화하였다. 마지막으로, 정보를 제공하는 외국의 개인정보보호 제도나 해외 제3자가 강구하는 개인정보보호를 위한 조치를 포함하여 개인정보를 제공한 정보주체에게 개인정보 이전에 대한 고지를 행할 것(제24조제2항 및 제3항)이라고 하여 개인정보 국외 이전과 관련된 규제를 강화하였다.[248]

Ⅷ. 해외 개인정보 보호법제의 시사점

GDPR의 시행으로 개인정보의 보호와 이용 사이에서 균형을 유지할 수 있는 규정을 정비하는 것이 많은 국가들의 공통적인 고민이다.

특히 EU는 1995년 지침 이후로 개인정보 보호와 관련해서 오랜 기간 중요한 역할을 해왔고 2016년 GDPR 제정 이후 현재까지도 마찬가지이다. EU 회원국들은 2018년 5월 GDPR 시행에 따라 GDPR의 규정에 부합하도록 각 국가내의 개인정보보호법을 개정하거나 개인정보보호 담당기관을 통한 GDPR 시행 가이드라인과 참고자료(탬플릿과 각종 툴 포함) 등을 제공하면서 조금이라도 시행착오를 줄이려는 모습을 보이고 있다.[249]

이를 가장 먼저 이를 반영한 국가는 독일이었다. 독일은 세계에서 가장 먼저 GDPR 반영한 자국의 개인정보보호법제를 2017년에 통과시켰다. 이처럼 독일의 개인정보보호법제는 처음부터 GDPR을 반영하기 위해서 개정되었다. 이를 통해 독일의 경우 개인정보처리의 국제적 기준에 최대한 부합한 국내법을 마련함으로써 자국민과 자국기업이 법위반으로 발생할 수 있는 불이익의 최대한 방지하고자 하고 있다. 2017년 개정된 독일의 BDSG에서는 정보주체의 권한을 상당히 강화하고 있다. 그 중에서 특히 민감정보에 관한 규정을 상당히 많이 두고 있음으로써 민감정보의 남용을

248) 한국인터넷진흥원, 위의 보고서(註 232).
249) 권건보, 이한주, 김일환, 앞의 논문(註 167), 34면.

막기 위해서 노력하고 있다.[250] 또한 잊힐 권리 즉, 삭제권도 폭넓게 인정하고 있으며, 우리나라에서 인정되지 않는 반대권이나 정보이전권 등도 인정하고 있다.

프랑스도 CNIL이 중심이 되어 GDPR 전면 시행에 대해 준비해 왔다. 프랑스 또한 민감정보에 대해서는 GDPR보다 오히려 더 적극적으로 규정하고 있었다. 특히 디지털공화국법은 고지의무를 강화하고 잊힐 권리를 신설하는 등 정보보호와 정보주체의 권리를 강화하고 있는 점이 특징이다.[251]

영국도 정보위원회사무국(ICO)이 WP29의 가이드라인 작성에 주도적으로 참여하여 영향력을 행사하고 있으며, GDPR을 수용하고 세계적 수준의 입법을 위한 선도적인 역할을 담당하고 있다.[252] 또한 영국은 4차 산업혁명 시대는 빅데이터를 기반으로 한 인공지능, 프로파일링이나 머신러닝에 개인정보가 사용되어야 함을 전제로 정보수집과 이용의 공정성, 투명성에 초점을 맞춘 정책을 제시하고 있다. 특히 DPA는 잊힐 권리 등을 통하여 개인정보를 보다 더 강력하게 관리하고 있으며, 소셜 미디어 플랫폼에 대한 정보 삭제를 요구할 수 있도록 하고 있다.

미국에서 최근에 이루어지고 있는 미 연방 차원의 개인정보보호법안(ADPPA)의 논의는 우리나라가 개인정보보호 관련법을 지속적으로 정비해 나가는 데 중요한 참고자료가 될 수 있을 것이다.[253]

위에서 살펴본 바와 같이, 해외 주요국들의 개인정보보호법제에서 공통적으로 강조되고 있는 것이 '잊힐 권리'이다. 지능정화사회의 특성상, 인터넷 공간에 저장되고 유통되는 정보 가운데 특히 현재의 상태와 부합하지 않는 정보, 개인의 사생활과 밀접하게 관련된 정보, 전과자의 사회복귀를 위해 지우고 싶은 정보 등이 검색기술의 도움으로 지속적으로 반복하여 대중에게 노출됨으로써 정보주체가 현재 겪고 있는 고통 내지 괴로움을 해소하며 나아가 인격적 이익이 손상당하지 않도록 할 필요성이 대두되었다[254]. 이

250) 홍선기, 고영미, 앞의 논문(註 171), 329면.
251) 홍선기, 고영미, 앞의 논문(註 171), 329면.
252) 홍선기, 고영미, 앞의 논문(註 171), 329-330면.
253) 김용일, 김유정, 앞의 논문(註 229), 86면.

와 같은 동향으로 아래에서 ‘잊힐 권리’에 대해서 자세히 연구해 보고자 한다.

제2절 잊힐 권리

Ⅰ. 잊힐 권리의 의의

빅토르 마이어 쇤베르거(Viktor Mayer-Schönberger)에 의하면 인터넷이 인간의 삶 속으로 도입되기 이전, 인간의 정신작용에서는 망각이 기본이었고 기억과 기록이 예외적이었다. 그러나 정보통신망을 통해 전 세계에 존재하는 다양한 정보들에 손쉽고 빠르게 접근할 수 있게 되면서, 우리 삶에서 망각은 예외가 되고 기억과 기록은 오히려 기본이 되었다. 이처럼 망각과 기억의 기본적 구조가 역전현상이 심화됨에 따라 인간은 망각을 위한 인위적 시스템을 도입하는 문제에 대하여까지 고민해야 하는 처지가 되었다.[255] 이러한 상황에서 대두된 것이 ‘잊힐 권리’(right to be forgotten)이다. 이는 1970년대 프랑스에서 과거 범죄사실의 삭제를 요구할 수 있는 망각권에서 그 기원을 찾을 수 있다.[256] 하지만 최근에는 범죄인뿐만 아니라 모든 사람의 개인정보에 대해서까지 그 적용 범위가 확대된 개념으로 인정되고 있다. 이에 따라 잊힐 권리는 오늘날 인터넷상에서 잠재적으로 나타나 있는 자신과 관련된 정보를 포함하는 각종 자료의 삭제를 요구하여 해당 자료로부터 자유로워질 수 있는 권리라고 볼 수 있다.[257] 즉, 인터넷상

---

254) 문재완, “잊혀질 권리(이상과 실현)”, 집문당, 2016, 14-18면.
255) Viktor Mayer-Schönberger, 구본권 옮김, 「잊혀질 권리」, 지식의 날개, 2011, 18면.
256) 박정훈, “잊혀질 권리와 표현의 자유, 그리고 정보프라이버시”, 공법학연구 제14권 제2호, 한국비교공법학회, 2013, 573면.
257) 홍명신, “정보의 웰다잉을 향한 시도”, 언론중재 제31권 제2호, 언론중재위원회, 2011, 23-24면.

에서 지속적으로 검색되는 자신과 관련된 정보를 삭제하거나 검색을 차단할 수 있고, 정보제공 서비스와 관련하여 권한 있는 자에 대하여 정보의 삭제나 검색차단, 변경된 정보의 공시와 같은 조치를 요구할 수 있는 권리이다.[258]

Ⅱ. 잊힐 권리의 규범화

잊힐 권리를 입법에 의해 뒷받침하려는 논의는 2010년대에 들어서 인간의 존엄성과 사생활의 보호를 강조하는 유럽에서 본격화되었다. 유럽연합 집행위원회의 부위원장인 비비안 레딩(Viviane Redding)은 “정보를 수집할 당시의 목적이 더 이상 필요치 않게 되었을 경우, 당해 정보의 완전한 삭제를 청구할 개인의 권리”를 의미하는 잊힐 권리를 공식적으로 입법화할 필요가 있다고 선언한 바 있다.[259]

이에 EU는 GDPR을 마련하면서 잊힐 권리를 구체화 하였다. EU의 GDPR은 제17조에 삭제권(잊힐 권리)이라는 제목 하에 정보주체의 삭제요구권 및 정보관리자의 삭제의무에 대해 규정하였다. 이에 따라 유럽연합에서 잊힐 권리는 하나의 독자적인 권리로 성문법에 자리매김하게 되었다.[260]

EU GDPR 제17조 제1항은 잊힐 권리가 인정되는 경우를 6가지로 규정하고 있다.

첫 번째 경우는 개인정보가 수집된 목적 또는 달리 처리된 목적과 관련하여 더이상 필요하지 않은 경우이다. 여기에는 정보처리의 목적과 관련되며, 비례성 원칙을 준수하면서 정해진 정보처리의 기간이 만료된 경우가 해당된다(GDPR 제5조 제1항 (e)).[261]

---

258) 조소영, “잊혀질 권리”, 공법연구 제41집 제2호, 한국공법학회, 2012, 437면.
259) 박정훈, 위의 논문(註 242), 576-577면.
260) 이인호, “정보통신기술의 발전과 기본권에 관한 연구”, 헌법재판연구 제25권, 헌법재판소, 2014, 377면.

두 번째 경우는 정보처리의 법적 근거가 되는 동의를 철회한 경우이다. 여기에서의 동의는 일반적 동의인 GDPR 제6조 제1항 (a)와 민감한 정보 분야의 특별한 동의인 GDPR 제9조 제2항 (a)가 해당된다. 정보주체는 정보가 처리되는 동안 언제든지 동의의 철회를 결정할 수 있으며, 정보처리자는 다른 법적 근거로 대체함으로써 자신의 정보처리를 수행할 수 있다.[262]

세 번째 경우는 정보주체가 GDPR 제21조에 근거한 반대권(droit d'oppsition)을 성공적으로 행사한 경우이다.[263]

네 번째 경우는 불법적 정보처리의 경우이다. 이는 GDPR 제6조 제1항[264]

---

261) 한동훈, "유럽연합의 잊힐 권리에 관한 연구:프랑수의 경우를 중심으로", 헌법재판소 헌법재판연구원, 2021, 22면.

262) 한동훈, 위의 논문(註 247), 22면.

263) 반대권과 관련하여, GDPR 제21조는 "1. 정보주체는 자신의 특별한 상황에 관한 사유로 제6조 제1항 (e) 또는 (f)를 근거로 한 프로파일링을 포함하여 이들 규정에 근거한 자신에 관한 개인정보의 처리에 대해 언제든지 반대할 권리를 가져야 한다. 컨트롤러는 정보주체의 이익, 권리 및 자유에 우선하는 처리 또는 법적 청구권의 설정, 행사 또는 방어를 위한 납득할만한 정당한 근거를 입증하지 않는 한 더 이상 개인정보를 처리해서는 아니 된다. 2. 직접 마케팅을 목적으로 개인정보가 처리되는 경우, 정보주체는 언제든지 이러한 마케팅을 위한 자신에 관한 개인정보 처리에 반대할 권리를 가져야 하고, 이러한 직접 마케팅과 관련되는 한도 내에서 프로파일링을 포함한다. ……"라고 규정하고 있다. (박노형 외 8인 저, EU 개인정보보호법 -GDPR을 중심으로-, 박영사, 2017, 159면.)

264) GDPR 제6조 처리 적법성 "1. 처리는 다음 중 어느 하나에 해당하는 경우에만 적법하다: (a) 정보주체가 하나 이상의 특정한 목적을 위해 자신의 개인정보 처리에 동의한 경우; (b) 정보주체가 당사자인 계약의 이행을 위하여 또는 계약 체결 전에 정보주체의 요청에 따른 조치를 취하기 위하여 처리가 필요한 경우; (c) 컨트롤러에게 적용되는 법적 의무의 준수를 위하여 처리가 필요한 경우; (d) 정보주체 또는 다른 자연인의 중대한 이익을 보호하기 위하여 처리가 필요한 경우; (e) 공익을 위하여 수행되는 직무의 실행을 위하여 또는 컨트롤러에게 부여된 공적 권한의 행사에 처리가 필요한 경우; (f) 컨트롤러나 제3자가 추구하는 정당한 이익의 목적을 위하여 처리가 필요한 경우로서, 다만, 특히 정보주체가 아동인 경우와 같이 개인정보 보호를 요구하는 정보주체의 이익이나 기본권과 자유가 해당 이익에 우선하는 경우에는 그러하지 아니하다. 제1항(f)는 공공당국이 자신의 직무수행을 위하여 실행하는 처리에 적용되지 아니한다." (박노형 외 8인 저, EU 개인정보보호법 -GDPR을 중심으로-, 박영사, 2017, 85-86면.)

이 규정하는 바와 같은 정보처리의 유효한 법적 근거가 없는 경우를 의미하며, 삭제권이 행사되는 상당한 경우가 이에 해당된다.

다섯 번째 경우는 정보처리자가 법적 의무를 준수해야 하는 경우이다. 이는 유럽법 또는 개별 국내법이 정보처리자로 하여금 일정한 정보의 삭제를 하도록 명하는 경우이다. 프랑스의 경우 "우편 및 전자통신법전"(Code des postes et des communications électroniques) 제L.34-1조에 따라 일정한 경우 보존기간을 넘은 거래에 관한 일체의 정보에 대한 삭제나 익명화가 전자통신사업자에게 명해질 수 있다.[265]

여섯 번째 경우는 미성년자에 대해 인터넷 상에서 정보가 수집된 경우이다. 이는 정보주체가 미성년 시기에 자신의 동의에 근거하여 정보사회서비스의 제공과 관련하여 정보가 수집된 경우를 의미한다.[266]

GDPR 제17조 제3항은 정보주체의 삭제 요구에 대해 5가지 목적의 보유가 불가피한 사유를 규정하고 있다. 즉 ⅰ) 표현 및 정보의 자유권 행사, ⅱ) 정보처리자를 수범자로 하는 유럽연합이나 회원국의 법률에 의해 처리가 요구되는 그러한 법적 의무를 준수하기 위하여, 또는 공익을 위한 직무를 수행하기 위하여, 또는 정보처리자에게 부여된 공적 권한을 행사, ⅲ) 제9조 제2항 (h)와 (ⅰ)[267] 및 제9조 제3항[268]에 따른 공중보건 영역에서

265) 한동훈, 앞의 논문(註 247), 22-23면.

266) Mattieu Bourgeois, Droit de la donnée : Principes théoriques et approche pratique, LexisNexis, 2017, pp. 232-233.

267) GDPR 제9조 특수한 범주의 개인정보 처리 "2. 다음의 하나에 해당하면 제1항은 적용되지 아니한다. …… (h) 예방의학이나 직업병의학의 목적으로 처리가 필요한 경우 및 근로자의 업무능력 평가, 의학적 진단, 건강이나 사회복지나 치료의 제공, 또는 EU 또는 회원국 법에 근거하거나 건강전문가와의 계약에 따르고 제3항에서 언급된 조건과 안전장치를 조건으로 건강이나 사회복지 시스템과 서비스의 관리를 위하여 처리가 필요한 경우, (ⅰ) 정보주체의 권리와 자유, 특히 직업상 비밀을 보호하기 위한 적당하고 특정된 조치를 규정하는 EU 또는 회원국법에 근거하여 건강에 대한 심각한 초국경 위협으로부터 보호하거나 건강관리 및 의약품 또는 의료장비의 높은 수준의 품질 및 안전을 보장하는 것과 같이 공중보건 영역에서 공익을 이유로 처리가 필요한 경우 ……" (박노형 외 8인 저, EU 개인정보보호법 - GDPR을 중심으로 -, 박영사, 2017, 99-101면.)

268) GDPR 제9조 특수한 범주의 개인정보 처리 "3. 제1항에서 언급된 개인정보는, EU 또는 회원국 법이나 회원국 소관 기관이 확정한 규정에 따른 직업상

공익,ⅳ) 제89조 제1항[269]에 따라서 공익을 위한 자료보존 목적, 학술적 혹은 역사적 연구 목적, 또는 통계적 목적을 달성하기 위한 경우로서, 제1항에서 규정하는 권리가 위 처리의 목적을 달성하는 것을 불가능하게 하거나 또는 심각하게 방해할 위험이 있는 경우, ⅴ)법적 권리의 설정, 행사 및 방어를 위하여 필요한 정보처리에 대해서는 잊힐 삭제청구가 인정되지 않는다. 따라서 GDPR 제17조의 잊힐 권리는 절대적인 권리로 설정되지 않았으며, 다른 우월적 이익이 존재하는 경우 제한될 수 있는 세부적인 사유를 명문으로 규정함으로써 이익의 균형을 꾀하고 있다.[270]

비밀 유지의무에 따르는 전문가 또는 그의 책임으로 또는 EU 또는 회원국 법이나 회원국 소관 기관이 확정한 규정에 따른 비밀 유지 의무에 따르는 다른 자의 책임 하에 그에 의하여 처리되는 경우, 제2항 (h)호에서 언급된 목적을 위하여 처리될 수 있다." (박노형 외 8인 저, EU 개인정보보호법 - GDPR을 중심으로 - , 박영사, 2017, 99-102면.)

269) GDPR 제89조 공익을 위한 문서보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적을 위한 처리에 관련되는 안전장치와 일탈 "1. 공익을 위한 문서보존 목적, 과학적 또는 역사적 연구 목적 또는 통계적 목적을 위한 처리는, 본 규칙에 따라, 정보주체의 권리와 자유를 위하여 적절한 안전장치의 적용을 받아야 한다. 그 안전장치들은 특히 개인정보 최소화 원칙의 존중을 보장하기 위하여 기술적 및 관리적 조치가 구비되는 것을 보장하여야 한다. 그 목적을 그 방식으로 충족될 수 있다면 그 조치들은 가명처리를 포함할 수 있다. 정보주체의 식별을 허용하지 않거나 더 이상 허용하지 않는 추가적 처리에 의하여 그 목적들이 충족될 수 있는 경우, 그 목적들은 그 방식으로 충족되어야 한다. 2. 개인정보가 과학적 또는 역사적 연구 목적 또는 통계적 목적을 위해 처리되는 경우, EU 또는 회원국 법원, 제15조, 제16조, 제18조 및 제21조에 언급된 권리가 특정한 목적의 달성을 불가능하게 또는 심각하게 저해할 것 같고 이들 권리의 일탈이 그 목적들의 충족에 필요한 한, 본조 제1항에 언급된 조건과 안전장치를 조건으로 이들 권리로부터 일탈을 규정할 수 있다. 3. 개인정보가 공익을 위한 문서보존 목적으로 처리되는 경우, EU 또는 회원국 법원, 제15조, 제16조, 제18조 및 제21조에 언급된 권리가 특정한 목적의 달성을 불가능하게 또는 심각하게 저해할 것 같고 이들 권리의 일탈이 그 목적들의 충족에 필요한 한, 본조 제1항에 언급된 조건과 안전장치를 조건으로 이들 권리로부터 일탈을 규정할 수 있다. 4. 제2항과 제3항에 언급된 처리가 동시에 다른 목적을 위하는 경우, 일탈은 그들 항에 명시된 목적을 위한 처리에만 적용되어야 한다." (박노형 외 8인 저, EU 개인정보보호법 - GDPR을 중심으로 - , 박영사, 2017, 435-436면.)

270) 최경진, "'잊혀질 권리'에 관한 유럽사법재판소(ECJ) 판결의 유럽 법제상 의미와 우리 법제에 대한 시사점", 법학논총, 제38권 제3호, 단국대학교 법학연구소, 2014, 82면.

GDPR 제17조의 잊힐 권리는 우리의 개인정보보호법제와 구별되는 다음과 같은 특징이 있다. 첫째로, 잊힐 권리를 행사할 수 있는 요건과 더불어 정보처리자가 그러한 권리의 행사에 대하여 거부할 근거를 담고 있다. 특히 잊힐 권리의 행사로 이루어지는 정보 유통의 차단이나 억제, 즉 표현의 자유 혹은 정보의 자유와의 갈등을 조정할 기준이 제시되어 있다. 이에 반해 우리의 「개인정보 보호법」 제36조 제1항[271]은 권리행사 요건이 없으면서, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우를 제외하고는 정보주체가 삭제를 요구할 수 있도록 규정하고 있다. 따라서 정보처리가 필요한 경우나 합법적인 처리인 경우에도 삭제권이 행사될 수 있으며, 심지어 정보주체가 막연히 싫은 경우에도 삭제권을 행사할 수 있다. 둘째로, GDPR은 공익을 위한 기록보존 목적의 달성을 불가능하게 하거나 심각하게 방해할 위험성이 있는 경우를 거부사유로 확실히 규정하고 있는데 이는 우리의 개인정보보호법제에서 찾아보기 힘든 공익이다.[272] (「개인정보 보호법」 제58조, 「도서관법」 제20조의2[273])

Ⅲ. 잊힐 권리에 관한 주요판례 (2014년 Google v. Spain 판결)

1. 사건 개요

스페인에 거주하는 변호사 마리오 코스테하 곤잘레스(Mario Costeja González)는 구글(Google)에서 자신의 이름을 검색하면, 과거의 사회보장 분담금 채무로 인해 압류된 부동산의 경매를 공고하는 '라 방과르디아'(La

271) 개인정보 보호법 제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

272) 한동훈, 앞의 논문(註 247), 23-25면.

273) 개인정보 보호법 제58조(적용의 일부 제외) 및 도서관법 제20조의2(온라인 자료의 수집)

Vanguardia)의 1998. 1. 19.자 및 3. 9.자 기사 페이지를 연결하는 2개의 링크가 검색결과로 나타나는 것을 발견하였다. 곤잘레스는 위에서 언급된 사회보장 분담금 채무는 이미 청산되었고, 현재의 자신에 관한 적절한 정보가 아니라고 주장하면서, 2010. 3. 5. 스페인 개인정보보호원(Agencia Española de Protección de Datos, AEPD)에 '라 방과르디아' 및 구글 스페인(Google Spain EL)과 구글(Google Inc.)을 상대로 구제 신청을 하였다. 구체적으로 이 스페인의 변호사는 첫째, 부채로 인해 자신의 주택에 대한 경매를 알리는 공고문이 실린 16년 전의 신문기사에 대해, 신문에 실린 과거의 경매정보는 더이상 현재의 자신을 제대로 반영하지 못한다는 이유로 그 기사의 삭제를 해당 신문사에 요구하였고, 둘째, 구글(google)의 검색창에 자신의 이름을 넣고 검색하면, 위 신문기사에 실린 자신의 이름과 함께 그 기사에 바로 접근할 수 있는 링크가 담긴 검색결과가 나타나는데, 이 검색결과가 자신에 관한 적절한 정보가 아니라는 이유로 구글에 검색결과의 삭제를 요청하였다.[274]

이 구제신청에 대해 스페인 개인정보보호원(Agencia Española de Protección de Datos, AEPD)은 '라 방과르디아'에 대한 구제신청은 기각하였지만, 구글에 대해서는 검색결과 화면에서 관련 링크를 삭제하라는 결정을 내렸다. 이에 구글은 스페인 고등법원에 제소하였고, 스페인 고등법원은 위 결정의 법적 근거가 된 지침 95/46의 관련 규정들이 그 이후 등장한 인터넷 검색엔진에도 적용될 수 있는지 등에 대한 해석을 유럽사법재판소에 선결문제로 제기하였다.[275]

스페인 고등법원은 ⅰ) 구글의 정보처리서버가 미국에 있는 경우에도 유럽연합의 개인정보보호지침이 구글 스페인에 적용되는지 여부, ⅱ) 개인정보보호지침이 인터넷 검색엔진에도 적용되는지 여부, ⅲ) 개인정보보호지침이 개인(정보주체)에게 웹에 공표된 자신에 관한 정보가 검색엔진을 통해 접근이 되지 않도록 요구할 권리('잊힐 권리')를 부여하고 있는지의 문

274) 한동훈, 앞의 논문(註 247), 8면.
275) 한동훈, 앞의 논문(註 247), 8면.

제를 유럽사법재판소에 제기하였다.[276]

2. 판결 요지

유럽사법재판소는 제기된 세 가지 쟁점에 대해서 다음과 같이 판시하였다. 첫 번째 쟁점에 대해서, 유럽사법재판소는 정보를 처리하는 물리적 서버가 유럽 밖에 위치하고 있다고 하더라도 검색엔진 운영자가 회원국의 영토 내에 지사를 두고서 검색엔진이 제공하는 광고공간을 판매하는 활동을 하고 있다면 유럽연합의 규범은 이와 같은 검색엔진 운영자에게 적용된다고 판시하였다.[277]

두 번째 쟁점에 대해서, 유럽사법재판소는 ⅰ) 인터넷에 공표된 정보를 찾아서 인터넷을 자동적이고 지속적이며 체계적으로 탐색하는 가운데, 검색엔진 운영자는 검색엔진을 통해 그 자체의 색인프로그램 체계 내에서 나중에 '검색하고'(retrieve), '기록하며'(record), '편성하게'(organize) 되는 정보를 '수집한'(collect) 것이고, 그 정보를 자신의 서버에 저장하여, 필요한 때에 검색결과의 목록(lists of search results)이라는 행태로 자신의 이용자들에게 제공하고 이용하게 하였으며, 이와 같은 활동은 지침 제2조 (b)항이 규정하는 '처리'(processing)에 해당되며, ⅱ) 지침 제2조 (d)항은 개인정보처리자의 개념을 넓게 정의해서 정보주체를 효과적이고, 충실하게 보호하려는 입법취지를 반영한 것이며, 검색엔진이 수행하는 개인정보의 처리와 관련해서 그 활동의 목적과 수단을 결정하는 것은 바로 검색엔진 운영자이고, 따라서 지침 제2조 (d) 항에서 말하는 '개인정보처리자'(controller)에 해당한다고 판단하였다.[278]

세 번째 쟁점은 제3자의 웹페이지에 공표된 정보주체의 개인적인 정보가 설령 합법적으로 공표된 것이고 또한 정보주체에 관한 진실된 정보라고 하

276) 이인호, 앞의 논문(註 246), 385-386면.
277) 이인호, 앞의 논문(註 246), 386면.
278) 이인호, 앞의 논문(註 246), 386-391면.

더라도, 정보주체가 생각하기에 그 정보는 자신에게 해로울지 모른다거나(might be prejudicial) 또는 일정한 시간이 지나면 망각(oblivion) 속으로 사라지기를 원할 때 그 정보가 인터넷 이용자들에게 더 이상 알려져서는 안 된다고 주장하면서, 그 정보를 검색엔진이 색인하지 못하도록(또는 이름으로 검색된 결과의 목록에서 그 웹페이지로 연결되는 링크를 삭제하도록) 요구할 수 있는 권리('잊힐 권리')가 지침상의 삭제청구권이나 처리거부권에 포함되어 있다고 볼 수 있는지 여부에 관한 문제이다.[279]

이에 대해 유럽사법재판소는 '유럽연합 기본권헌장'(Charter of Fundamental Rights of the European Union) 제7조의 사생활 및 가족생활의 존중[280]과 제8조의 개인정보의 보호[281]가 각각 보장하는 정보주체의 사생활권(right to privacy)과 개인정보보호권(right to the protection of personal data)이 가지는 중요성과 오늘날의 검색엔진이 수행하는 기능으로 인해 이들 권리가 침해될 수 있는 위험이 크다는 점을 강조하면서, 웹사이트 발행자를 문제 삼지 않고 바로 검색엔진 운영자에게 검색결과를 제거하라는 명령을 내릴 수 있다고 판단하였다. 즉 유럽사법재판소는, 검색결과의 링크 정보가 "처리의 목적에 적합하지 않거나(inadequate), 연관성이 없거나(irrelevant) 또는 과도한(excessive) 때"에는 정보주체는 검색결과의 링크삭제를 요구할 수 있는 권리('잊힐 권리')가 인정된다고 판단하였다.[282]

다만, 유럽사법재판소는 잊힐 권리는 원칙적으로 검색엔진 운영자의 경제

279) 한동훈, 앞의 논문(註 247), 9-10면.

280) 유럽연합 기본권헌장 제7조 사생활 및 가족생활의 존중 "모든 사람은 사생활 및 가족생활, 주거와 통신을 존중받을 권리를 갖는다." 국회도서관 역, 유럽연합 기본권 헌장, 2014, 5면.

281) 유럽연합 기본권헌장 제8조 개인정보의 보호 "1. 모든 사람은 자신에 관한 개인정보에 대한 권리를 갖는다. 2. 개인정보는 규정된 목적을 위하여 당사자의 동의 또는 법률이 정하는 기타 적법한 근거에 기초하여 공정하게 취급하여야 한다. 모든 사람은 자신에 관하여 수집된 정보에 접근하고 그 정보의 정정을 요구할 권리를 갖는다. 3. 이러한 규칙의 준수는 독립적인 기관에 의한 통제를 받는다." 국회도서관 역, 유럽연합 기본권 헌장, 2014, 5면.

282) 이인호, "'잊힐 권리' 관련 최근 소송 동향 및 이슈", 언론중재, 2020년 가을호, 21-23면.

적 이익 뿐만 아니라, 대중의 정보의 이익보다 우월하지만, 이와 같은 일반적 원칙에 대한 예외 또한 인정하였다. 유럽사법재판소는 당사자가 정계에서 수행하는 역할과 같이 특별한 이유가 있는 경우에는 이와 같은 당사자에 대한 기본적 권리에 대한 제한이 대중의 문제되는 정보에 대한 접근할 이익의 우월성에 의해 정당화된다고 판시하였다.[283]

따라서 유럽사법재판소는 잊힐 권리는 절대적인 권리가 아니며, 인터넷 이용자들의 정당한 이익과 정보주체의 기본권 사이에서 공정한 균형이 추구되어야 한다고 보았다. 그리고 유럽사법재판소는 이러한 균형은 정보주체의 사생활에 대해 가지는 민감성과 그 정보를 알고자 하는 대중의 관심과 같은 문제가 된 정보의 성격과 문제가 된 사람의 특성에 달려있다는 입장을 전개하였다.[284]

Ⅳ. 소결

사람은 누구나 자기 스스로의 뜻에 따라 삶을 영위해 나가면서 개성을 신장시키기를 바라기 때문에 사생활 내용에 대한 외부적인 간섭을 원치 않을 뿐만 아니라, 다른 사람에게 알리고 싶지 않은 '나만의 영역'을 혼자 소중히 간직하고자 하므로 나만의 영역이 자신의 의사에 반해서 남에게 알려지는 것을 원치 않는다.[285] 그리고 이러한 사생활의 비밀과 자유는 인간 행복의 최소한의 조건이라 할 수 있다. 따라서 사생활의 내용에 대해서 스스로 원치 않았음에도 불구하고 외부적인 간섭을 받게 되고, 나만의 영역이 타의에 의해서 외부에 공표되었을 때 사람은 누구나 인간의 존엄성에 대한 침해나 인격적인 수모를 느끼게 된다. 사생활의 비밀과 자유를 지키는 것은 인간으로서의 존엄성을 지키는 것과 동일한 것으로 볼 수 있다. 그리고

283) CJUE 13 mai 2014, aff. C 131/12, point 99.
284) 이인호, 앞의 논문(註 246), 394-395면.
285) 허영, 「한국헌법론」, 박영사, 2012, 397면.

이러한 개인의 영역을 보장하는 것과 그로 인해 지켜지는 헌법적 가치는 지능정보화사회에서도 여전히 동일한 헌법적 의미를 유지한다.

잊혀질 권리에 대한 논의는 헌법 제17조의 사생활의 비밀과 자유권 보장 규정을 넘어선 새로운 권리로서 인정되고 보장되어야 하는 이유는 다른 차원에서 고민되어야 한다. 왜냐하면 잊혀질 권리가 문제시되는 영역은 더 많은 경우에 권리주체 스스로가 생성하고 공개했던 정보가 문제될 수 있다는 점에서, 그 정보의 현실적 유동성과 잠재적 유동성이 정도와 범위에 있어서 계산될 수 없다는 점에서, 권리주체의 미래의 삶이 과거와 현재의 정보로 인해 치유될 수 없는 치명적 상황에 이르게 될 수도 있다는 점에서, 잊혀질 권리는 개인정보자기결정권의 문제를 초월하는 또 하나의 새로운 기본권으로 정립되어야 할 필요성이 있다고 생각하기 때문이다.[286]

그렇다면 새로운 기본권으로서의 잊혀질 권리의 헌법적 근거는 헌법 제17조가 아니라 우선적으로 헌법 제10조 인간의 존엄성과 그 수단적 규정으로서의 제37조 제1항 규정이어야 한다. 인간의 존엄성은 인간이 이성을 통한 도덕적 자기결정을 할 수 있다는 것과 밀접한 관련성을 갖는다. 즉 인간의 존엄성과 자기결정권은 밀접한 상관관계를 가질 뿐만 아니라 내용적으로도 중첩되는 측면을 갖는다.[287] 인간은 존엄하기 때문에 자기결정권을 갖는 것이며, 역으로 자기결정권을 갖기 때문에 존엄한 존재가 될 수 있다. 헌법상 사생활권을 보호받고 있는 기본권주체가 단순히 사생활을 영위하면서 살아간다는 차원을 넘어 스스로 존엄하다고 생각하는 대로 자신의 삶을 설계하고 실천해 갈 수 있어야만 헌법적으로 존엄한 인간의 존엄성이 실현될 것이다. 존엄한 존재로서 자신의 삶을 영위해 가는데 있어서 자신과 관련된 정보들을 일시적이건 영구적이건 삭제하거나 변경함으로써 자신의 인간으로서의 존엄성을 회복하거나 유지할 수 있도록, 잊혀질 권리는 지능정보화사회에서 디지털 기억에 의한 존엄성에 대한 희화화나 저하 혹은 침해를

286) 김송옥, “잊혀질 권리에 대한 비판적 고찰”, 언론과법 제14권 제1호, 2015, 258면.

287) R. Dworkin, LIFE'S DOMAIN: AN ARGUMENT ABOUT ABORTION AND EUTHANASIA, Hart Publishing, 1993, p. 166

방지할 수 있는 권리로서의 존재의의와 가치가 인정되어야 할 것이다. 따라서 현대 인터넷 사회 속에서 법제화되어야 하는 잊혀질 권리는 사생활 보호 권리의 한 내용인 개인정보 자기결정권의 의미를 넘어 인간의 존엄성을 지키기 위한 권리로서 또 하나의 헌법상의 새로운 권리로 인식되고 구체화되어야 할 것이다.

제5장 국내의 개인정보 보호법제 현황

헌법재판소가 2005년 5월 이른바 지문날인사건에서 개인정보자기결정권을 도입한 이후, 개인정보자기결정권의 개념은 개인정보와 관련한 헌법상의 기본권으로서의 위치를 확고히 구축하였다. 이는 인격권 또는 프라이버시권의 성격을 가진 것으로서, 2011년에 제정·시행된 「개인정보보호법」은 개인정보의 처리를 위해서는 정보주체의 동의를 얻을 것을 원칙으로 규정한 것이 이러한 개인정보자기결정권이 실정법에서 반영된 단적인 예라고 할 수 있을 것이다.[288]

개인정보자기결정권은 「개인정보보호법」 등에서 구체적 제도로서 구현되어 있다고 할 수 있다. 「개인정보보호법」은 정보주체에게 자신의 개인정보처리와 관련하여, ①개인정보의 처리에 관한 정보를 제공받을 권리, ②개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리, ③개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람을 요구할 권리, ④개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리, ⑤개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리 등을 보장하고 있다. 이 가운데에서도 특히 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 동의권(②)은 개인정보 처리를 사전에 통제한다는 의미에서 사전적 통제권의 성격을 가지며[289], 따라서 우리 개인정보 보호법에서 개인(정보주체)이 자신의 정보에 대한 통제권을 강력하게 행사할 수 있다는 의미에서 개인정보자기결정권이 실체적으로 가장 잘 구현되어 있는 정보주체 권리 가운데 하나라고 할 수 있다.

이와 같은 맥락에서 국내의 개인정보 보호법의 현황을 다음과 같이 살펴

---

288) 함인선, “AI시대에서의 개인정보자기결정권의 재검토:EU 개인정보보호법을 소재로 하여”, 전남대학교 법학연구소 공익인권법센터, 인권법평론 제26호, 2021.2., 125-126면.

289) 권영준, “개인정보 자기결정권과 동의 제도에 대한 고찰”, 「법학논총」 제36권 제1호, 2016, 685면.

보고자 한다. 개인정보 보호법제의 역사를 시작으로, 2016년 정부에서 시행한 개인정보활용에 관한 정책인 개인정보 비식별조치 가이드라인의 제시 내용, 이후 개정된 현행 개인정보 보호법제에 대하여 검토해 보고자 한다.

제1절 국내 개인정보 보호법제의 연혁

Ⅰ. 개인정보 보호법제의 역사

개인정보보호의 역사는 역설적이게도 개인정보침해로부터 시작되었다. 개인정보보호에 관한 전문가들은 2008년 오픈마켓 옥션의 해킹이 개인정보보호 강화의 시발점이라고 말한다. 2008년 1월 옥션은 해킹으로 인해 1800만 명의 개인정보가 유출되는 사태가 발생했다. 당시 2008년만 하더라도 주민등록번호는 암호화 대상이 아니었다. 따라서 옥션 해킹 사건 당시 1000만 건 이상의 암호화되지 않은 주민등록번호가 유출됐으나, '주민등록번호를 암호화해 저장할 의무가 없다'는 판결[290]이 나왔다. 이후 정보통신망법에서 주민등록번호를 암호화 대상에 포함했다.[291]

이처럼 정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있었나, 국가사회 전반을 규율하는 개인정보 보호원칙과 개인정보 처리기준이 마련되지 못해 개인정보 보호의 사각지대가 발생할 뿐만 아니라, 개인정보의 유출·오용·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 초래하고 있는 바, 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화

290) 대법원 2015. 2. 12. 선고 2013다43994, 44003 판결
291) 이양복, "데이터 3법의 분석과 향후과제", 비교사법 제27권 2호(통권 제89호), 2020.5. 435면.

하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장하기 위하여 개인정보 보호에 관한 일반법으로 2011년 3월 29일 「개인정보보호법」을 제정하였다.[292]

하지만 「개인정보보호법」이 제정된 2011년 발생한 사고는 옥션 때 피해의 2배에 달했다. 네이트와 싸이월드를 운영했던 SK컴즈의 데이터베이스가 해킹되면서 3500만명의 개인정보가 유출되는 사태가 발생했다. 이런 잇단 개인정보 유출과 언론 및 기업을 대상으로 한 대규모 해킹 사건으로 인해 '망분리'가 대두되었다. 이후 '망분리'는 정보통신망법의 항목으로 법제화됐다. 지속되는 보안 사고로 인해 개인정보보호의 목소리가 커지던 중 2014년 대형 보안 사고가 연달아 터졌다. KB국민·NH농협·롯데카드 3사 개인정보 유출 사고가 그것이다. 이 사건은 특히 보안의 중요성이 높은 금융사에서 발생한 개인정보유출이라 더 주목받았다. 당시 카드 3사에서 유출된 개인정보는 약 1억 400만건에 달했다. 해당 사건은 해킹이 아니라 카드사의 시스템 개발을 하던 외부 용역 직원이 악의적으로 유출했다는 점에서 해킹으로 인한 유출과는 성격이 달랐다. 유출자가 외부자에게 더미 데이터가 아닌 중요한 데이터 원본을 준 것과 더불어 그 과정에서 접근 제어조차 되지 않았으며 인가되지 않은 USB로 개인 정보를 빼냈다는 점이 국민에게 충격을 안겨줬다. 계속되는 개인정보 유출로 개인정보보호 필요성의 목소리가 커지면서 결국 2016년 보호에 초점을 둔 개인정보보호 관련법 개정이 진행되었다. 금융권의 개인정보를 총괄하는 신용정보법과 일반 상거래회사의 개인정보를 맡는 개인정보보호법, 정보통신망법이 바로 그것이다. 동법들은 징벌적 손해배상제도 도입과 처벌 조항으로 형사처벌을 두는 등 개인정보처리자에 대한 규제를 대폭 강화하였다.[293] 또한, 개인정보처리자가 정보주체 이외로부터 개인정보를 수집·처리하는 경우 정보주체에게 수집 출처와 처리목적 등을 고지하도록 함으로써 정보주체의 개인정보

292) 이상윤 외, "빅데이터 관련 개인정보 보호법제 개선방안 연구", 법제처 한국법제연구원, 2017.10. 39면.
293) 이양복, 위의 논문(註 277), 435-436면.

자기결정권을 보다 두텁게 보호하는 방향으로 개정되었다.[294]

Ⅱ. 개인정보 보호법제에 관한 정책
- 2016년 개인정보 비식별조치 가이드라인 제시(개인정보활용에 관한 정책)

2016년 5월 18일 대통령 주재로 열린 제5차 규제개혁 장관회의 및 민관합동 규제개혁 점검회의(이하 2016년 5차 회의)에서는 4차 산업혁명을 주도하는 클라우드, 빅데이터 등 정보통신기술 융합 신산업에 대한 규제 완화를 목적으로 개인정보 활용과 관련된 가이드라인이 마련되어야 한다는 필요성과 함께 개인정보의 활용을 위하여 정보주체의 사전 동의가 완화될 수 있도록 관련 법률의 개정이 추진되어야 한다는 내용이 발표되었다.[295]

정부가 2016년 5차 회의에서 발표한 내용을 토대로 2016년 6월 당시 국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부 등 여섯 관계부처는 개인정보 비식별조치 가이드라인 (이하 2016년 가이드라인)을 발표하였다. 2016년 가이드라인은 “빅데이터, 사물인터넷 등 새로운 기술과 융합산업의 출현은 세계적 IT강국으로 자리매김한 우리나라에 도약의 기회를 제공하고 있지만, 해당 기술을 활용하는 가운데 발생 가능한 개인정보 침해를 방지하여 신산업 발전과 개인정보의 보호를 조화롭게 모색하여야 한다는 점을 강조하면서, 현행 개인정보보호 법령의 틀 내에서 빅데이터가 안전하게 활용될 수 있도록 개인정보의 비식별조치 기준과 비식별정보의 활용범위 등을 제시하여 기업의 불확실성을 제거하며 기업투자와 산업 발전을 도모하는 한편, 국민의 개인정보인권도 보호하고

294) 주승희, “데이터 3법의 주요 개정 내용 및 형사법적 의의에 관한 소고”, 숭실대학교 법학논총 제49집, 2021.1.. 271면.
295) 대한민국 정책브리핑, “대통령 제5차 규제개혁 장관회의 개최”, 2016. 5. 19, 국무조정실.
https://www.korea.kr/news/pressReleaseView.do?newsId=156130013

자 한다"는 점을 밝히고 있다.[296]

하지만 2016년 가이드라인은 그 내용이 어떠하든지 법률의 형식을 띠는 것이 아니기 때문에 법적 효력을 발휘할 수 없다. 따라서 정부가 가이드라인을 통하여 비식별조치된 비식별정보는 개인정보가 아니라고 추정하여 정보주체의 동의 없이 활용할 수 있다고 해석하더라도, 이러한 행위가 개인정보 보호와 관련된 법률을 위반한 것으로 판단된다면 위반자에게 형사상 또는 행정상 제재를 가할 수 있다. 2016년 가이드라인은 개인정보의 활용을 확대하기 위한 목적에 치중한 나머지 명확한 법적 근거 없는 비식별조치로 획득된 개인정보를 무분별하게 수집하고 활용하여 정보주체의 개인정보를 오용·남용 또는 유출하는 행위를 허용하고 있지만, 결론적으로 이로부터 발생하는 불법한 결과에 대한 책임이 어떠한지는 전혀 밝히고 있지 않다. 결국 새로운 기술의 개발과 연구를 목적으로 하는 개인정보의 활용과 정보주체의 개인정보 보호에 관한 문제는 입법적으로 해결될 수밖에 없다는 측면에서 현행 개인정보보호법을 개정하여 관련 법적 근거가 체계적으로 구축되어야 한다는 주장이 상당한 설득력을 얻게 되었다.[297]

Ⅲ. EU GDPR의 영향과 지능정보화사회로의 전환에 따른 개인정보보호법제 개정

정보통신기술의 급속한 발달과 더불어 우리들은 인터넷과 스마트폰 등 각종 디지털 기술을 활용해 손쉽고 빠르게 필요한 정보를 얻고 있다. 페이스북이나 트위터 등 다수의 소셜 네트워킹 서비스에 하루에도 여러 차례 텍

296) 행정안전부 보도자료, "「개인정보 비식별 조치 가이드라인」 발간", 2016.6.30.
https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=55287

297) 이정념, "개인정보보호법의 개정 의의와 적용상 한계", 「저스티스」 통권 제179호, 2020.8. 244-246면.

스트나 영상, 사진, 웹문서를 올리고 서로간에 필요한 정보들을 활발히 교류하고 있다. 그런데 모바일 데이터의 양이 워낙 방대하고 축적된 양이 폭발적으로 증대하다 보니 이들 비정형화된 데이터의 새로운 가치와 활용 가능성이 각광을 받게 되었고, 이들 데이터를 사물인터넷이나 인공지능, 클라우드 등 신기술과 결합하여 적극적으로 활용하는 이른바 빅데이터 산업이 근래 들어 4차산업혁명시대의 핵심산업으로 부상하였다. 문제는 21세기 원유라고 지칭되는 이들 빅데이터가 개개인에 관한 정보의 집합물이기에 빅데이터의 활용 가능성을 높일수록 개인정보의 침해 위험성도 그만큼 높아진다는 것이다.[298]

국제사회에서도 4차 산업혁명시대로 전환되어 가는 가운데 새로운 기술의 개발과 연구를 위하여 다양한 데이터를 확보하기 위한 법적 기반이 갖추어져야 한다는 인식을 같이 하면서도 개인정보의 보호를 위한 측면 또한 함께 고려되어야 한다는 논의가 지속적으로 이루어졌는데, 2018년 유럽연합이 GDPR을 마련하여 선제적인 대응체계를 갖추면서 우리나라의 관련 논의에 있어서도 상당한 영향을 끼쳤다.

유럽연합이 GDPR을 제정하여 2018년 5월부터 시행하였고, 4차산업혁명이라는 시대적 흐름에 부응하여 디지털 경제 활성화와 개인정보 보호 사이의 균형을 맞춘 입법이기에 우리나라 개인정보보호법제의 대대적 수정 필요성을 더욱 부각시켰다. 우리나라 정부 역시 데이터 경제로의 전환이라는 전 세계적 환경변화를 적극적으로 수용하고, 데이터를 이용한 신산업의 육성을 범국가적 과제로 삼아 관련 법률의 정비에 노력을 기울였다.[299]

우리 사회가 지능정보화사회로의 성격을 띠며 발전해 나가는 가운데 개인정보가 지니는 경제적 가치에 대한 흥미가 높아지고 개인정보를 자원으로 하는 산업을 발전시키려는 요구 또한 커지면서, 개인정보를 활용하는 행위에 대한 새로운 접근이 필요하다는 주장이 제기되어 왔고, 4차 산업혁명시대로 전환되는 사회적 흐름을 반영하여 새로운 기술의 개발과 연구를 위한

298) 주승희, 앞의 논문(註 280), 268면.
299) 주승희, 앞의 논문(註 280), 269면.

개인정보의 활용범위를 특정하면서도 정보주체의 개인정보를 보호하기 위한 두 가지 목적이 조화될 수 있도록 개인정보보호법이 개정되어야 한다는 논의가 입법적으로 본격화 되었다.[300]

상황은 계속해서 변화하였고 데이터 활용에 대한 필요성이 크게 대두되어 분위기가 반전되었다. 특히 데이터 활용에 대한 선진국들의 법제 동향과 비교하여 더욱 부각되었다. 2009년만 하더라도 글로벌 시가총액 10위 내에 있던 석유, 금융, 유통, 자원 등 전통 기업들이 10년 후인 2019년에 데이터를 활용하는 IT기업들에게 밀려났다. 이에 따라 개인정보보호를 위해 데이터 활용을 지나치게 억제해서는 안 된다는 의견에 힘이 실렸고, 이에 2018년 개인정보보호법 개정법이 발의되었다. 입법적 노력의 결실이 2020년 1월 9일 국회 본회의를 통과한 일명 '데이터 3법'이다. 데이터 3법이 개정되었지만 개인정보보호와 데이터 활용의 균형은 계속해서 풀어나가야 할 사안이다. 시장 참여자 모두를 만족하는 '균형'을 달성하는 것은 사실상 불가능에 가깝겠지만, 우리는 전 세계적으로 빠르게 변화하는 흐름에 맞게 변화를 도모해야 한다.[301]

제2절 현행 국내의 개인정보 보호법제

4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 범국가적 과제로 대두되고 있고, 특히 신산업 육성을 위해서는 인공지능, 클라우드, 사물인터넷 등 신기술을 활용한 데이터 이용이 필요한 바, 안전한 데이터 이용을 위한 사회적 규범 정립이 시급한 상황이 도래하였다. 그러나 기존법상 개인정보 보호 감독기능은 행정안전부·방송통신위원회·개인정보보호위원회 등으로, 개인정보 보호 관련 법령은 「개인정보보호법」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」등

300) 이정념, 앞의 논문(註 283), 249면.
301) 이양복, 앞의 논문(註 277), 436면.

으로 각각 분산되어 있어 데이터 이용 활성화를 지원하고 데이터 이용으로부터 정보주체의 권리를 보호하는 데 한계가 있었다. 이를 보완하고자 「개인정보보호법」 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정 법률안이 2020년 1월 9일 국회 본회의를 통과하였고, 2020년 2월 4일 개정되었다. 이에 따라 정보주체의 동의 없이 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련하되, 관련하여 개인정보처리자의 책임성 강화 등 개인정보를 안전하게 보호하기 위한 제도적 장치를 마련하는 한편, 당초 수집 목적과 합리적으로 관련된 범위 내에서 개인정보의 추가적인 이용·제공이 가능하도록 할 여지가 마련되었다. 또한, 개인정보의 오용·남용 및 유출 등을 감독할 감독기구는 개인정보보호위원회로, 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」과의 유사·중복 규정은 「개인정보보호법」으로 일원화함으로써 개인정보의 보호와 관련 산업의 발전이 조화될 수 있도록 개인정보 보호 관련 법령이 체계적으로 정비되었다.[302]

또한, 이와 함께 신용정보 관련 산업에 관한 규제 정비와 신용정보 주체의 개인정보 자기 결정권을 강화한 「신용정보의 이용 및 보호에 관한 법률」 또한 함께 개정되었다.

지능정보화사회에서 개인정보보호에 관한 법제의 중심은 「개인정보보호법」이 분명하나, 지능정보화사회의 다양한 요소들은 대부분 디지털화된 개인정보를 활용하고 있으므로 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법') 및 「신용정보의 이용 및 보호에 관한 법률」 (이하 '신용정보법')도 개인정보보호에 관한 법제에 포함되므로 함께 연구해 보고자 한다.

Ⅰ. 「개인정보보호법」

302) 개인정보보호위원회, 앞의 책(註 24), 5-6면.

개인정보보호법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. 이에 따라 개인정보의 수집·이용, 제공 등 개인정보 처리 기본원칙, 개인정보의 처리 절차 및 방법, 개인정보 처리의 제한, 개인정보의 안전한 처리를 위한 관리·감독, 정보주체의 권리, 개인정보 권리 침해에 대한 구제 등에 대하여 규정하고 있다.[303]

개정된 「개인정보보호법」의 주요 내용은 개인정보의 개념을 명확히 하여 혼선을 줄이고, 안전하게 데이터를 활용하기 위한 방법과 기준 등을 새롭게 마련하여 데이터를 기반으로 한 새로운 기술·제품·서비스의 개발, 산업 목적을 포함하는 과학연구, 시장조사, 상업 목적의 통계작성, 공익 기록보존 등을 위해서 가명정보를 이용할 수 있도록 하였다. 가명정보의 개념과 활용 가능범위를 정의하여 가명정보를 통한 데이터 활용을 할 수 있게 되었다. 또한 정보처리자의 책임성을 강화시켜 각종 의무를 부과하고, 법 위반 시 과징금 부과 등 처벌도 강화하여 개인정보를 안전하게 보호하는 제도적 장치를 마련하였고, 개인정보의 오·남용과 유출 등을 감독할 감독기구는 개인정보보호위원회로, 관련 법률의 유사·중복 규정은 「개인정보보호법」으로 일원화하였다.[304]

1. 유사·중복된 관련 법제 정비하여 「개인정보보호법」으로 일원화

「개인정보보호법」·「정보통신망 이용촉진 및 정보보호 등에 관한 법률」·「신용정보의 이용 및 보호에 관한 법률」에서 일반법인 개인정보보호법과의 유사·중복 조항을 정비하는 등 데이터 경제 활성화를 위하여 개정되었고, 개인정보보호에 관한 법이 부처별로 나뉘어 있기 때문에 생긴 불필요한 중복을 해소하여 개인정보를 안전하게 보호할 수 있도록 제도적

303) 개인정보보호위원회, 앞의 책(註 24), 6면.
304) 이양복, 앞의 논문(註 277), 440면.

인 장치를 마련하였다[305].

2. 개인정보 정의 및 판단 기준의 명확화

개정 전 「개인정보보호법」은 개인정보를 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)'로 정의하였는데(제2조 제1호), 개정 「개인정보보호법」은 개인정보 개념을 아래와 같이 구체화 시키고 있다.

개정 「개인정보보호법」 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. "개인정보"란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
   가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
   나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
   다. 가목 또는 나목을 제1호의2에 따라 가명처리 함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 "가명정보"라 한다)

1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를

305) 이양복, 앞위 논문(註 277), 441면.

대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.[306]

특히, 개정 「개인정보보호법」은 특정 개인의 식별 가능 여부에 대한 기준을 제시하였다. 개정 전 「개인정보보호법」은 “해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는”이라는 정의와 관련하여 “쉽게 결합하여”의 범위가 어디까지인지 여부를 명확하지 않아 법 적용의 어려움 등 논란이 지속되어 왔었다. 개정 「개인정보보호법」에서는 “다른 정보의 입수 가능성” 등 기준을 제시하여 기업 등 이해관계자의 개인정보 처리에 기존보다 명확한 기준을 제시하였다(제2조 제1호). 아울러 “익명정보”라는 용어는 사용하지 않았으나, 익명정보는 개인정보보호법을 적용하지 않는다는 규정도 신설(제58조의2)하였다.[307]

3. 가명정보 개념 도입 및 가명정보 처리에 관한 특례 규정 신설

개정 「개인정보보호법」은 가명정보의 개념을 도입(제2조 1의2호)하고, 그 처리에 관한 특례 규정(제28조의2)을 신설하였다.

개정법 제2조 제1의2호에서, ‘개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리’하는 것이 가명처리이고, ‘가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보’가 ‘가명정보’에 해당한다(제2조 제1호 다목)고 정의하였다. 개정 「개인정보보호법」은 이와 같은 가명정보 역시 개인정보에 해당함을 분명히 하였고, 가명정보의 경우 정보 주체의 동의가 없더라도 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리할 수 있을 뿐만 아니라 전문기관에 의한 가명정보의 결합이 가능하도록 특례 규정을 신설하였다(제28조의2

306) 주승희, 앞의 논문(註 280), 272-273면.
307) 이양복, 앞의 논문(註 277), 441면.

이하). 가명정보에 대해서는 정보처리자가 기타 개인정보의 이용시 준수해야 할 제한 규정들의 적용을 제외시킴으로써 그 활용을 상대적으로 용이하게 하였다(제28조의7). 다만 가명정보의 공개만으로도 정보주체를 식별할 수 있는 가능성이 전혀 없지 않고, 기술적 조치를 통해 정보주체를 식별할 수 있는 가능성이 있으므로, 가명정보를 처리하는 경우 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 취할 의무가 있다(제28조의4).[308]

<표 1> 개인정보·가명정보·익명정보의 개념 및 활용가능 범위[309]

구 분	개 념	활용 가능 범위	법의 적용
개인정보	특정 개인에 관한 정보, 개인을 알아볼 수 있게 하는 정보	사전적이고 구체적인 동의를 받은 범위 內 활용 가능	개인정보보호법 규정 일반 적용
가명정보	추가정보의 사용 없이는 특정개인을 알아볼 수 없게 조치한 정보	다음 목적에 동의 없이 활용 가능 (EU GDPR 반영) ①통계작성(상업적 목적 포함) ②연구(산업적 연구 포함) ③공익적 기록보존 목적 등	개인정보보호법상 가명정보에 관한 특례 적용
익명정보	더 이상 개인을 알아볼 수 없게(복원 불가능할 정도로) 조치한 정보	개인정보가 아니기 때문에 제한 없이 자유롭게 활용	개인정보보호법 적용되지 않음

308) 주승희, 앞의 논문(註 280), 273-274면.

309) 이양복, 앞의 논문(註 277), 442면; 이소은, “개인정보 보호법의 주요 개정 내용과 그에 대한 평가”, 이화여자대학교 법학논집 제24권 제3호 통권 69호, 2020.3. 225면.

4. 개인정보 수집·이용의 편의성 확대(수집목적과 합리적 관련 범위 내)

개정 전 「개인정보보호법」은 법률에 명시된 경우 외에는 개인정보처리자가 정보주체로부터 별도의 동의 없이 당초 수집한 목적 이외의 용도로 정보를 이용하거나, 제3자에게 제공하는 것을 금지하였는데, 개정 「개인정보보호법」은 정보주체의 동의 없이도 당초 수집 목적과 '합리적으로 관련된 범위 내'에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 개인정보를 이용하거나 제3자에게 제공할 수 있도록 하였다(제15조 제3항, 제17조 제4항).

개정 전 법령에 따르면 정보수집 주체인 기업은 아주 사소한 변경사항이 발생해도 재동의를 받아야 했다. 고객들에게 더 좋은 서비스 구현을 위한 목적이라고 밝혀도 이용자들이 동의를 잘 해주지 않아, 기업으로선 수집단계에서 가능한 많은 동의를 받으려는 경향이 있었고, 고객의 경우에는 서비스 이용을 위해 기계적으로 동의하다 보니 엄격한 사전동의제도가 오히려 개인정보보호에 역행하고 관련 산업의 발전도 저해한다는 비판이 있었는데,[310] 개정을 통해 이를 개선하였다.

이 규정은 개인정보의 활용을 도모하기 위해 개인정보 목적 명확화 원칙을 완화한 것으로 볼 수 있는데, 새로 생긴 추가의 개인정보 이용 또는 제공 목적이 애초의 수집목적과 합리적으로 관련되었다면 안정성 확보를 전제로 하여 정보주체의 동의 없이 개인정보를 이용하거나 제공하는 것을 허용함으로써 개인정보 처리자의 입장에서는 개인정보 처리의 범위를 넓혀주는 효과를 기대할 수 있게 되었다.[311]

5. 개인정보처리자의 책임 강화

---

310) 심상현, "개인정보 관련 제재 및 피해구제 합리화 방안 연구", 한국인터넷진흥원, 2013, 75면 ; 원소연/심우현, "지능정보사회 촉진을 위한 데이터 및 정보 관련 규제 개선 방안 연구", 한국행정연구원, 2019, 308면

311) 이양복, 앞의 논문(註 277), 442-443면.

가명정보를 복원하기 위한 추가정보의 별도 분리 보관 및 제3자 제공금지, 데이터 활용 과정에서 개인 식별가능 정보가 생성된 경우 지체 없는 처리 중단 및 회수·파기 등 안전조치 의무의 내용을 구체적으로 규정(제28조의4 및 제28조의5)하여, 가명정보 처리나 데이터 결합 시 안전조치 의무를 부과하고 특정개인을 알아보는 행위를 금지하였다. 안전조치 의무 내용 위반 시 행정적인 과태료나 형사적 처벌 이외에 전체 매출액의 3% 이하에 해당하는 과징금 부과(제28조의5 및 제28조의6, 제39조의15 등)하여 개인정보처리자의 책임성을 강화함으로써 데이터 활용과 개인정보보호의 조화를 도모하고 있다.[312]

6. 개인정보보호위원회의 중앙행정기관화

개정 「개인정보보호법」은 대통령 소속의 개인정보보호위원회를 국무총리 소속의 중앙행정기관으로 하고, 독자적인 조직·인사·예산권 및 조사·처분 등 집행권과 의안제출 건의권 및 국회·국무회의 발언권을 부여하였다. 개인정보보호위원회의 위상에 절대적으로 요구되는 독립성 보장을 위해 국무총리 소속으로 하되 조사·처분 등 독립성이 요구되는 일부 기능에 대해서는 국무총리의 행정 감독권을 배제하였다(제7조 제1항, 제2항). 이로써 개정 전 행정안전부와 방송통신위원회가 수행했던 업무는 개정 후 모두 개인정보보호위원회로 이관되었다. 한편 개정 신용정보법은 개인신용정보와 관련하여 금융위원회의 감독을 받지 않는 신용정보회사 등 금융회사외의 '상거래 기업 및 법인'에 대해서는 금융위원회의 감독·검사 등을 대신하여 보호위원회에 대하여 자료 제출 요구·검사·출입권·시정명령·과징금·과태료 부과 등의 권한을 부여(제38조 제5항, 제42조의2, 제45조의3, 제45조의4 등)함으로써 현행의 개인정보보호 추진체제를 완전히 탈바꿈시켰다.[313] 또한, 형사제재와 관련해서도 「개인정보보호법」 위반 범죄행위에 대한 고발권

312) 이양복, 앞의 논문(註 277), 443면.
313) 이양복, 앞의 논문(註 277), 443-444면.

의 행사주체가 행정안전부장관에서 개인정보보호위원회로 변경되었다(제65조 제1항).

Ⅱ. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 정보통신망법)

개정 법률에는 정보통신망법 내 개인정보 관련 다른 법령과의 유사·중복 조항 정비와 협치(거버넌스) 개선하면서 정보통신망법에 규정된 개인정보 보호에 관한 사항을 「개인정보보호법」으로 이관하고 온라인상의 개인정보 보호와 관련된 규제와 감독의 주체를 방송통신위원회에서 개인정보보호위원회로 변경하였다.[314]

1. 「개인정보보호법」과 유사·중복 조항의 정비

정보통신망법은 개인정보보호에 관한 내용을 삭제하고 관련 내용을 「개인정보보호법」으로 이관하는 개정 작업이 이루어졌다. 정보통신망법은 「개인정보보호법」과 유사하고 중복되는 조항이 다수 규정되어 있는 문제점이 있었다. 개인신용정보의 처리, 그 업무의 위탁, 유통 및 관리와 신용정보주체의 보호에 관하여 일반법인 「개인정보보호법」의 일부 규정을 금융분야에 알맞게 특별법인 신용정보법에 수용하거나 일반법과 특별법의 적용관계를 보다 명확히 규정하였다. 또한 이 법에서 유사하거나 중복적으로 규정하고 있는 내용에 대해서는 「개인정보보호법」의 해당 조문을 적용하도록 하는 등 현행 개인정보 보호 체계를 보다 효율화 하였다.[315]

2. 일부 규정을 「개인정보보호법」 내 특례 규정으로 이관

314) 이양복, 앞의 논문(註 277), 444면.
315) 이양복, 앞의 논문(註 277), 444면.

개정 「개인정보보호법」은 제6장으로 “정보통신서비스 제공자 등의 개인정보 처리 등 특례”를 신설하고, 개정된 정보통신망법과 함께 기존에 「개인정보보호법」과 정보통신망법으로 분산되어 있던 개인정보 보호 관련 법률을 「개인정보보호법」으로 일원화하였다. 즉 개정 「개인정보보호법」은 기존 정보통신망법에 있던 개인정보에 관한 규정 중 「개인정보보호법」과 상이한 규정들을 정보통신서비스제공자 등에 대한 특례 규정으로 이관하고 있다. 예를 들어 개인정보의 수집 및 이용, 개인정보 유출 통지 및 신고, 서비스 미이용 이용자 개인정보의 파기, 개인정보 이용내역의 통지, 손해배상의 보장, 국내대리인의 지정, 국외 이전 개인정보의 보호, 과징금 등 규정이 이에 해당한다. 정보통신망법 개정은 필수적이었고, 개인정보보호 관련 사항은 「개인정보보호법」으로 이관하고, 온라인상 개인정보보호 관련 규제와 감독 주체를 방송통신위원회에서 개인정보보호위원회로 변경하였다. 즉, 정보통신망법 내 개인정보 관련 다른 법령과의 유사·중복조항에 대한 거버너스 정비가 이루어진 것이다.[316]

3. 정보통신망법에 존치하는 규정

정보통신망법의 단말기 접근 권한에 대한 동의, 주민등록번호 처리 관련 본인확인기관의 지정 등 규정은 삭제되지 않고 여전히 존치한다. 이들 조항이 존치하는 이유는 개인정보 보호와는 직접 관련은 없으며, 그 적용 대상이 통신사업자 등 방송통신위원회 사업자라는 특성을 반영하였기 때문이다.[317]

Ⅲ. 「신용정보의 이용 및 보호에 관한 법률」(이하 신용정보법)

316) 이양복, 앞의 논문(註 277), 444-445면.
317) 이양복, 앞의 논문(註 277), 445면.

우리 정부는 금융분야에서의 데이터 활용 신산업 육성을 목표로 하고 있다. 금융결제원은 데이터 경제활성화 정책에 부응하고 빅데이터 활용을 촉진하기 위해 금융데이터융합센터를 신설하였고, 금융위원회는 마이데이터 산업('본인 신용정보 관리업')을 적극 추진 중에 있다. 금융분야의 마이데이터 산업은 금융정보의 주체인 금융소비자가 자신의 신용정보를 체계적으로 관리할 수 있도록 지원하고 소비패턴 등의 분석을 통해 개인의 신용관리·자산관리 서비스를 제공하는 데이터 산업으로서 단순히 개인의 신용정보를 수집, 신용도 등 신용정보를 만들거나 이를 제공하는 신용조회업(Credit Bureau)과는 차이가 있다. 이미 미국이나 유럽연합의 경우 다양한 핀테크 기업이 출현하여 개인을 대상으로 하는 금융정보관리 지원서비스를 경쟁적으로 제공 중인데, 우리나라의 핀테크 기업들은 서비스 수준이 제한적이고 정보보호와 보안의 측면에서 우려도 제기되어 산업 성장에 어려움이 컸다. 특히 이전의 신용정보법은 신용정보의 효율적 이용 및 체계적 관리나 신용정보 주체의 보호에 기여하는 측면이 있으나, 데이터 산업의 발전을 저해하는 부정적 측면도 없지 않았다. 이에 개정 신용정보법은 마이데이터 산업을 도입, 금융분야의 빅데이터 활용을 촉진시키는 한편 그에 따른 부작용의 방지와 개인의 정보자기결정권의 보장을 주요 내용으로 담고 있으며, 「개인정보보호법」과의 유사·중복 조항 문제 등 종전부터 지적되어온 조항들을 정비하였고, 그 구체적 내용은 아래와 같다.[318]

1. 신용정보 등 주요 개념 정비 및 신설

개정 전 신용정보법은 '금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 다음 각 목의 정보로서 대통령령으로 정하는 정보'(제2조 제1호)로 규정하면서, 그 구체적 의미는 시행령을 참고해야만 비로소 파악할 수 있었다. 개정 신용정보법에서는 다음과 같이 식별가능한 개

318) 주승희, 앞의 논문(註 280), 276-277면.

인정보만이 신용정보에 해당함을 법률로 명시하였다.

개정 신용정보법 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “신용정보”란 금융거래 등 상거래에서 거래 상대방의 신용을 판단할 때 필요한 정보로서 다음 각 목의 정보를 말한다.
   가. 특정 신용정보주체를 식별할 수 있는 정보(나목부터 마목까지의 어느 하나에 해당하는 정보와 결합되는 경우만 신용정보에 해당한다)
   나. 신용정보주체의 거래내용을 판단할 수 있는 정보
   다. 신용정보주체의 신용도를 판단할 수 있는 정보
   라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보
   마. 가목부터 라목까지의 정보 외에 신용정보주체의 신용을 판단할 때 필요한 정보

이 외에도 「개인정보보호법」과 마찬가지로 가명처리와 가명정보 개념을 새롭게 도입하였고, 개인신용평가회사나 신용정보집중기관 등에 제공하거나 그로부터 제공받는 경우, 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우에는 신용정보주체의 동의 없이도 개인신용정보를 제공할 수 있도록 하였다(제2조 제15호, 제16호, 제32조 제6항 제9호의2, 제9호의4). 또한 개정 전 지나치게 포괄적으로 규정되어 있는 신용조회업무의 정의를 개정하여 개인신용평가업, 개인사업자신용평가업, 기업신용조회업, 신용조사업으로 세분화하여 정의하였다(제2조 제8호, 제2조 제8호의2, 제8호의3, 제9호). 신용정보주체인 개인의 신용관리를 지원하기 위하여 본인의 신용정보를 일정한 방식으로 통합하여 그 주체에게 제공하는 행위를 영업으로 하는 본인신용정보관리업 개념을 도입함으로써(제2조 제9호의2, 제9호의3), 마이데이터 산업의 근거규정을 마련하였다.[319]

2. 개인신용정보 전송요구권 도입 등 정보주체의 권리 강화

개정 신용정보법은 개인인 신용정보주체가 신용정보제공·이용자등에 대하여 그가 보유하고 있는 본인에 관한 개인신용정보를 본인이나 본인신용정보관리회사, 개인신용평가회사 등에 전송하여 줄 것을 요구할 수 있는 개인신용정보 전송요구권을 도입하였다(제33조의2). 이는 일차적으로 개인의 자기정보 통제권한의 강화를 의미하지만, 시장 경제적 측면에서 볼 때 고객 기반이 확립되지 않은 신규 데이터산업자의 진입장벽을 낮추고, 동종업체간의 경쟁을 유발함으로써 서비스 혁신을 통해 소비자 이익을 높일 뿐만 아니라, 기업이 사용하는 데이터가 증가함으로써 기업의 생산성이 향상되고 집적된 데이터를 통해 혁신적인 이익이 기업과 소비자에게 주어질 것이라는 긍정적 전망[320]이 반영된 것으로 보인다. 이 외에도 EU의 GDPR이 개인정보 보호의 강화를 위해 신설한 프로파일링(Profiling) 대응권이 금번 개정을 통해 국내에도 도입되었다. 이는 개인인 신용정보주체가 개인신용평가회사 등에 대하여 자동화평가(프로파일링)[321]를 하는지 여부 등에 대해 설명을 요구할 수 있고, 자동화평가 결과의 산출에 유리하다고 판단되는 정보를 제출하거나 기초정보의 정정·삭제를 요구할 수 있는 권리이다(제36조의2). 기타 신용정보주체가 자신의 정보활용의 동의여부를 결정할 때 관련 내용을 명확하게 이해할 수 있도록 '보다 쉬운 용어나 단순하고 시청각적인 전달 수단 등을 사용하여 신용정보주체가 정보활용 동의 사항을 이해할 수 있도록 할 것' 등 개인신용정보 등의 활용 관련 동의의 원칙에 관한 사항을 신설하였다(제34조의2). 또한 '정보활용 동의등급' 제도를 신설하여 신용정보주체가 자신의 정보활용 동의의 파급효과를 손쉽게 알

319) 주승희, 앞의 논문(註 280), 278면.

320) 정원준, "데이터 이동권 도입의 실익과 입법적 방안 모색", 성균관법학 제32권 제2호, 성균관대학교 법학연구원, 2020, 82면.

321) 프로파일링이란 통계모형, 머신러닝에 기초한 개인신용평가나 인공지능을 활용한 온라인 보험료 산정 결과 등을 의미한다 (유주선, "데이터 3법 개정과 보험업에 관한 법적 연구",「상사판례연구」제33편 제3권, 한국상사판례학회, 2020, 174면)

수 있도록 하였다(제34조의3).[322]

3. 마이데이터 산업 도입 및 신용정보 관련 산업의 규제 완화

개정 신용정보법은 마이데이터 산업의 활성화를 위해 자본금 요건이나 금융권 출자의무 등 진입장벽을 최소화하는 차원에서 최소 자본금 또는 기본재산의 요건을 처리대상 정보나 업무의 특성 등을 고려하여 20억원 또는 5억원으로 하고 있다(제6조 제2항). 또한 신용조회회사의 경우 종래 영리 목적으로 다른 업무를 겸업할 수 없도록 한 규제를 폐지하고 신용정보주체 보호 및 신용질서를 저해할 우려가 없는 업무에 대해서는 겸영을 허용하였고, 허가를 받은 업무에 부수하는 업무를 수행할 수 있도록 하였다(제11조, 제11조의2). 빅데이터 활용의 활성화를 위해 신용정보회사 등이 금융위원회가 지정한 데이터전문기관을 통해서 자기가 보유한 정보집합물을 제3자가 보유한 정보집합물과 결합할 수 있도록 하였는데, 정보집합물의 결합 목적으로 데이터전문 기관에게 개인신용정보를 제공하는 경우에는 신용정보주체의 동의 없이도 개인신용정보를 제공할 수 있도록 하였다(제17조의2, 제32조 제6항 제9호의3). 한편 개인정보의 대량 수집·관리 등에 따라 발생할 수 있는 정보 유출 및 피해를 막기 위해서 상시적 평가체제 구축(제20조 제6항, 제22조의2), 가명처리·익명처리에 관한 행위 규칙 신설(제40조의2), 배상책임보험의 가입 의무화(제43조의3), 등록제 대신 허가제 실시(제4조) 등도 새롭게 포함되었다(제26조의3).[323]

4. 유관 법령과의 관계 명확화 및 유사·중복 조항 등 정비

다른 법률과의 관계를 규정한 신용정보법 제3조의2는 제1항에서 '신용정보의 이용 및 보호에 관하여 다른 법률에 특별한 규정이 있는 경우를 제외

322) 주승희, 앞의 논문(註 280), 278-279면.
323) 주승희, 앞의 논문(註 280), 279-280면.

하고는 이 법에서 정하는 바에 따른다'고 하면서, 제2항에서는 '개인정보의 보호에 관하여 이 법에 특별한 규정이 있는 경우를 제외하고는 개인정보보호법에서 정하는 바에 따른다'고 규정하고 있다. 이는 신용정보에 대해서는 신용정보법이 일반법의 지위에 있고, 개인정보에 대해서는 신용정보법이 특별법의 지위에 있음을 선언하는 규정으로 해석될 수 있다. 관련하여 개정 전 신용정보법에 따르면 식별정보가 개인신용정보이면서 동시에 개인정보에 해당하는 것으로 해석될 여지가 있어서 신용정보법과 개인정보 보호법 모두를 적용하는 이중규제의 문제가 발생할 여지가 있었다. 이 문제는 전술한 바와 같이 신용 관련 정보와 결합한 식별정보만이 신용정보에 해당함을 법률로 명확히 함으로써 자연스럽게 해결되었다.

「개인정보보호법」과 중복되는 규정들도 다수 정비하였다. 개정법 제15조 제1항이 '이 법 및「개인정보보호법」제3조 제1항 및 제2항에 따라 그 목적 달성에 필요한 최소한의 범위에서 합리적이고 공정한 수단을 사용하여 신용정보를 수집 및 처리하여야 한다'라고 규정한 부분과 동조 제2항 제1호에서 '「개인정보보호법」 제15조 제1항 제2호부터 제6호까지의 어느 하나에 해당하는 경우' 신용정보주체의 동의를 받지 않도록 예외규정을 둔 것을 예로 들 수 있다. 그 외에도 제17조 제1항, 제6항, 제20조 제4항, 제5항, 제20조의2 제2항 등에서 관련 「개인정보보호법」 규정을 준용하도록 자구를 수정하였으며, 신용정보회사의 신용정보의 수집·조사 및 처리의 제한에 관한 규정인 제16조는 「개인정보보호법」과 중복되는 내용으로 삭제되었다.[324]

324) 주승희, 앞의 논문(註 280). 280-281면.

제6장 개인정보자기결정권을 위한 개인정보 보호법제의 개선방향

제1절 의존적인 동의제도의 문제점과 개선방향

Ⅰ. EU·영국·일본의 동의제도

한국의 개인정보보호법과 달리 EU의 GDPR은 수집, 이용, 저장, 제공, 파기 등 단계별로 적법성 요건을 규정하지 않고 '처리'라는 하나의 용어로 묶어 '동의'를 포함한 6개 적법성 요건(lawfulness of processing)을 규정하고 있다.[325] 즉, 정보주체의 사전동의는 개인정보 처리의 6개 적법성 요건 중의 하나일 뿐이다.[326] 특히 민간의 개인정보처리자들은 정보주체와의 계약의 이행을 위해 필요한 경우(제6조 제1항(b)), 또는 개인정보처리자(controller)나 제3자가 추구하는 정당한 이익(legitimate interests)을 달성하기 위하여 필요한 경우(정보처리의 이익이 정보주체의 보호이익보다 더 커야 함)에, 동의 없이 개인정보를 처리(수집·이용·제공)하는 것이 합법적

325) GDPR 제6조 제1항(처리의 적법성) 개인정보 처리는 다음 어느 하나의 각 호에 해당하는 경우에만 적법하다. (a) 정보주체의 동의, (b) 정보주체가 당사자인 계약의 이행 또는 계약 체결 전 정보주체의 요청에 따른 처리, (c) 컨트롤러의 법적 의무 준수, (d) 정보주체 또는 제3자의 생명에 관한 이익 보호, (e) 공익상 이유 또는 컨트롤러에게 부여된 공식권한의 행사를 위한 업무수행, (f)) 컨트롤러 또는 제3자의 정당한 이익추구

326) EU '제29조 작업반'은 "동의가 항상 개인정보 처리의 가장 적법한 근거는 아니다. … 원칙적으로 동의는 하나의 보호조치일 뿐, 다른 보호원칙의 예외로 간주되어서는 안 된다. 동의는 기본적으로(primarily) 적법성 근거이며, 다른 보호원칙의 적용을 배제하지 않는다."라고 한다[ARTICLE 29 DATA PROTECTION WORKING PARTY, 「Opinion 15/2011 on the definition of consent」, 2011.7.13., P.7; 「Guidelines on consent under Regulation 2016/679」, 2018.4.10., p.29(note 71)]

으로 가능하다.

이는 온라인에서도 동일하게 적용된다. 한편, GDPR은 민감정보(special categories of personal data)에 대해서는 다른 합법성 기준을 가지고 있다. 즉, 민감정보는 원칙적으로 처리를 금지한다. 그렇지만 여기에는 10가지 예외를 인정하고 있다.[327] 이 경우에도 동의는 10가지 예외 중의 하나이다. 다만, 유럽연합은 GDPR 외에 정보통신망의 통신비밀과 프라이버시를 보호하기 위한 「전기통신 프라이버시 지침」(e-Privacy Directive)을 가지고 있는데, 이 지침에서는 쿠키(cookie)와 위치데이터를 합법적으로 처리하기 위해서는 사전고지(notice)와 동의(consent)를 요구하고 있다. 요컨대, 유럽은 온라인을 비롯하여 민간의 개인정보처리자가 일반개인정보를 수집·이용·제공하는 경우에 정보주체의 사전동의를 원칙으로 요구하지 않는다. 단지 동의는 6가지 합법성의 근거 중 하나일 뿐이다. 그렇지만 기업들은 개인정보를 처리할 때 반드시 이들 6가지 중의 하나의 근거를 가지고 있어야 한다.

영국의 개인정보보호기관(DPA)인 정보보호청(Information Commissioner's Office; ICO)은 정보주체를 위한 웹페이지 안내문에서 '당신의 정보는 중요하다'(Your data matters)고 안내하면서, "기업은 나의 동의를 받아야 할까?(Dose an organisation need my consent?)"라는 질문을 던지고서는 이렇게 답변한다: "아니오. 기업은 당신의 개인정보를 사용하기 위해서 항상 당신의 동의를 받을 필요는 없다. 기업이 유효한 근거를 가지고 있다면, 동의 없이도 당신의 개인정보를 이용할 수 있다. 개인정보보호법에서는 그

327) GDPR 제9조(Processing of special categories of personal data; 특수유형의 개인정보의 처리). 민감정보의 처리가 허용되는 10가지 예외는 다음과 같다: (a) 정보주체가 명시적 동의(explicit consent)를 한 경우 (b) 고용관계 등에서 정보처리자나 정보주체의 의무이행 및 권리행사를 위해 필요한 경우 (c) 정보주체나 다른 개인(자연인)의 중대한 이익 보호를 위해 필요한 경우 (d) 비영리단체의 정당한 활동을 위한 경우 (e) 정보주체가 명백히 공개한 개인정보를 처리하는 경우 (f) 법적 권리의 설정, 행사, 방어를 위한 경우 및 법원의 사법권 행사를 위한 경우 (g) 공공의 이익을 위해 처리가 필요한 경우 (h) 예방의료, 피고용인의 업무평가, 의료진단, 보건복지서비스를 위한 경우 (i) 공중보건을 위한 경우 (j) 자료보존, 학술연구, 통계 목적을 위한 경우.

근거들을 '합법적 근거'(lawful basis)라고 하는데, 기업이 활용할 수 있는 합법적 근거는 6가지가 있다."[328] 영국의 개인정보보호법(DPA 2018)에서 6가지 합법적 근거는 ①동의(consent) ②계약(contract) ③법적 의무(legalobligation) ④중요한 이익(vital interests) ⑤공무수행(public task) ⑥정보처리자 혹은 제공을 받는 제3자의 정당한 이익(legitimate interests)이다. 정보주체의 동의는 정보처리가 합법적이기 위한 근거 중의 하나이다.

일본 개인정보보호법은 opt-in과 opt-out을 혼용하여 규정함으로써 개인정보 활용의 길을 폭넓게 인정하고 있으며, 개인정보를 수집·이용할 때 GDPR과 같은 합법성의 근거를 달리 요구하지 않는다. 즉 개인정보취급사업자[329]는 원칙적으로 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다. 그렇지만 수집할 때 그 이용목적을 분명하게 특정해야 하고, 그 목적 범위 안에서 이용해야 하며, 처음의 이용목적과 연관성이 있다고 합리적으로 인정되는 범위 안에서는 목적을 동의 없이 변경할 수 있다(제15조). 이러한 이용목적을 벗어난 이용에 대해서는 동의를 받아야 하고(제16조 제1항), 다만 ①법령의 근거 ②급박한 생명·신체·재산의 보호 ③급박한 공중위생·아동의 육성 ④공무수행에의 협조의 경우 예외를 인정한다(제16조 제3항). 그러나 민감정보('배려를 요하는 개인정보')를 취득할 때에는 동의를 원칙적으로 받아야 하고, 다만 6가지 예외를 인정하고 있다(제17조 제2항).[330]

---

328) https://ico.org.uk/your-data-matters/does-an-organisation-need-my-consent, (영국 정보보호청(Information Commissioner's Office; ICO, 2022.9.26. 기준)

329) 일본에서 보호의무를 지는 '개인정보취급사업자'란 개인정보데이터베이스 등을 사업용으로 이용하는 자를 말한다(개인정보보호법 제2조 제5항). 공공부문을 제외한 민간의 사업자만이 대상이다. 한국에서 보호의무를 지는 '개인정보처리자'란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다(개인정보보호법 제2조 제5호).

330) 동의 없이 민감정보를 취득할 수 있는 6가지 예외 : ① 법령의 근거 ② 급박한 생명·신체·재산의 보호 ③ 급박한 공중위생·아동의 육성 ④ 공무수행에의 협조 ⑤ 정보주체 혹은 국가기관에 의해 공개된 경우 ⑥ 기타 정령(政令)으로 정하는 경우.

한편, 일본의 경우 제3자 제공에 대해서는 합법성의 근거를 6가지 두고 있다(제23조). 즉, ①정보주체의 동의 ②법령의 근거 ③급박한 생명·신체·재산의 보호 ④급박한 공중위생·아동의 육성 ⑤공무수행에의 협조 ⑥정보주체의 사후적 처리거부(opt-out)를 전제로 하는 제공이 그것이다. 여기서 여섯 번째의 사후적 처리거부를 전제로 하는 제3자 제공이 적법하기 위해서는 다음의 3가지 요건이 충족되어야 한다(제23조 제2항). 즉, (ⅰ)제3자 제공 후 정보주체의 요청이 있으면 제3자제공을 정지해야 하고, (ⅱ)제공이 있기 전에 미리 안내사항 5가지[331]를 통지하거나 또는 쉽게 알 수 있도록 해야 하며, 그리고 (ⅲ)개인정보보호위원회에 신고를 해야 한다. 요컨대, 민간의 개인정보취급사업자는 정보주체의 동의가 없더라도 제3자 제공을 할 수 있고, 대신에 정보주체에게는 고지를 받을 권리와 사후거부권(right to object)을 주어 통제할 수 있도록 하고 있다. 다만, 민감정보('배려를 요하는 개인정보')는 사후거부권 인정 방식으로 제3자 제공을 할 수 없다.[332]

Ⅱ. 우리나라 동의제도의 문제점과 개선방향

국내 「개인정보보호법」은 개인정보의 수집·이용에 있어서 정보처리자를 규제하는 규제의 기본방향을 정보주체의 동의제도에 의존하고 있다. 정보주체의 동의제도를 개인정보처리의 기본적 요건으로 삼은 것은 정보주체의 개인정보자기결정권을 보장한다는 것에서 비롯된 것이다.

이러한 동의제도는 체크박스에 체크함으로써 동의를 표시하는데, 개인정보자기결정권을 실질적으로 보장하는 장치인지는 의문이다. 그 내용이 방대하고 깨알같이 표시되는 약관 형태이기 때문에 이용자에게 제대로 인식

331) ① 제3자 제공을 이용목적으로 한다는 점 ② 제3자에게 제공되는 개인데이터의 항목 ③ 제3자 제공의 방법 ④ 정보주체의 요청이 있는 때에 식별이 가능한 개인데이터의 제3자 제공을 정지한다는 점 ⑤ 정보주체의 요청을 접수하는 방법

332) 이인환, "지능정보사회에서 개인정보보호의 법과 정책의 패러다임 전환", 과학기술과 법 제11권 제2호, 2020.12., 272-275면.

되지도 않을뿐더러 정보처리자가 이미 준비한 내용의 정보처리 계획에 동의하는 것이므로 현실적으로 계약당사자로서의 동등한 지위로서 협의가 가능한 것이라고 볼 수 없다. 이러한 문제점들은 국내 개인정보보호 관련 법제가 지나치게 동의제도에만 의존하고 있는 것에서 비롯된다.[333]

또한, 위에서 살펴본 바와 같이 EU·영국·일본과 비교해 볼 때 한국은 과하다고 할 정도로 정보주체의 사전 동의를 중심으로 하는 엄격한 합법성 근거를 요구하고 있다. 일부 예외가 인정되지만 매우 제한적이다. 그리하여 기업 등 모든 민간의 개인정보처리자는 정보주체의 사전 동의를 얻지 못하면 자칫 불법적인 정보처리가 되고 무거운 과징금과 형사처벌의 위험에 놓이게 된다. 이하에서 이 점을 구체적으로 살핀다.

우선 온라인에 적용되는 개정 전 정보통신망법[334]에 의하면, 정보통신서비스제공자가 정보주체의 사전 동의 없이 개인정보를 수집·이용하면 매출액 3% 이내의 과징금 및 5년 이하의 징역에 처해질 수 있다. 다만, ①서비스제공계약의 이행 ②요금정산 ③다른 법률에 특별한 규정이 있는 경우에만 예외가 허용된다. 심지어 계약의 이행을 위해 필요한 경우라도 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우라야만 예외가 인정된다(제22조, 제64조의3, 제71조제1항제1호; 2020년의 개정 개인정보보호법에서도 동일). 수집 시 동의를 받을 때 고지했던 사항(이용목적, 개인정보 항목, 보유기간)을 변경할 때에도 다시 동의를 받아야 한다. 그리고 제3자에게 제공할 때에는 별도로 이에 대해 사전 동의를 받아야 하고 이를 위반하면 과징금과 5년 이하의 징역에 처해질 수 있다. 단지 ①요금정산 ②다른 법률에 특별한 규정이 있는 경우에만 예외가 허용된다(제24

333) 이희옥, “초연결사회를 위한 개인정보보호법제의 개선방향”, 법제논단 3월호, 2019.3., 88면.

334)「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제4장(개인정보의 보호). 제4장의 기본내용들은 2020. 2. 4. 개정된「개인정보 보호법」제6장(정보통신서비스 제공자 등의 개인정보 처리 등 특례)에 거의 그대로 편입되었다. 개정법은 2020. 8. 5. 시행되었다. 특별법의 내용이 일반법으로 이동되었으나, 그 내용은 기존 특별법과 동일하기 때문에, 2020. 8. 5. 이후에도 정보통신망에서의 개인정보 처리에 대해서는 이전과 같이 엄격한 규율이 그대로 적용되고 있다.

조의2, 제64조의3, 제71조제1항제3호; 개정 개인정보보호법에서도 동일).

요컨대, 인터넷이나 모바일에서 서비스를 제공하는 기업이나 개인은 자신 또는 제3자의 정당한 이익을 위한 경우라도 이용자나 소비자의 사전 동의를 받아야만 합법적으로 수집·이용하거나 제공할 수 있다. 온라인에서는 거의 동의만이 처리의 합법적 근거로 인정되고 있는 셈이다. 다른 법률에서 특별한 규정을 두어야만 그 예외가 인정될 수 있다. 유럽연합이나 일본의 경우 온라인이든 오프라인이든 기업 등 민간의 서비스제공자가 자신 또는 제3자의 정당한 업무수행을 위하여 또는 광고나 마케팅 목적을 위하여 동의 없이 수집·이용·제공할 수 있도록 허용하면서 대신에 정보주체에게는 고지를 받을 권리와 사후거부권을 주어 통제할 수 있도록 하는 것과 비교할 때, 한국은 온라인 영역에서 지나치게 동의에만 의존하는 형식을 취하고 있다. 심지어 서비스 이용계약의 이행을 위해 필요한 경우라 하더라도 수집·이용에 있어서는 원칙적으로 동의를 받아야 하고, 제3자 제공에 있어서는 예외 없이 동의를 받아야만 한다.

한편, 민간과 공공의 모든 개인정보처리에 적용되는 일반법인 「개인정보보호법」은 수집·이용에 있어서 합법적 근거로 GDPR과 유사하게 6가지를 인정하고 있다(제15조). 즉, ①정보주체의 동의를 받은 경우 ②법률의 특별규정이 있거나 법령상 의무 준수를 위해 불가피한 경우 ③공공기관의 법령상 업무 수행을 위해 불가피한 경우 ④정보주체와의 계약 체결 및 이행을 위해 불가피한 경우 ⑤급박한 생명·신체·재산의 이익을 위하여 필요한 경우 ⑥개인정보처리자의 정당한 이익을 위해 필요한 경우(단, 정보주체의 권리보다 명백하게 우선해야 함)가 그것이다. 이처럼 수집·이용에 있어서는 동의 외에도 계약 및 정당한 이익을 합법적 근거로 인정하고 있다.

그러나 민간의 개인정보처리자의 경우 제3자 제공에 있어서는 GDPR과 달리 계약 혹은 개인정보처리자나 제3자의 정당한 이익을 합법적인 근거로 인정하지 않는다(제17조, 제18조). 다만, 2020년의 개정법 이전에는 한 가지 예외를 두고 있었는데, '통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우'

에는 정보주체의 동의 없는 제3자 제공을 허용하였었다(제18조제2항제4호). 2020년의 개정법에서는 이 조항을 삭제하고, 대신 제3절(제28조의2-제28조의7)을 신설하여 가명정보의 처리에 관한 특례를 마련하고 있다. 즉, 가명처리한 정보는 '통계작성, 과학적 연구, 공익적 기록보존'의 목적으로는 정보주체의 동의 없이 처리할 수 있도록 허용한 것이다. 그나마 인공지능·빅데이터 환경에서 산업계의 요구를 반영한 개정이라고 평가될 수있다.

그렇지만 위 특례를 제외하고, 기업을 비롯한 민간의 모든 개인정보처리자는 여전히 자신의 정당한 업무수행을 위한 경우에도, 또 이용자나 소비자와의 계약을 이행하기 위한 경우에도 정보주체의 사전 동의를 받아야만 한다. 이를 위반하는 경우 무거운 과징금과 5년 이하의 징역을 각오해야 한다. 이는 정당한 기업활동의 자유, 정보유통의 자유, 혹은 때에 따라서는 재판청구권을 과도하게 제약하는 측면이 있다. 예를 들어, 환자와 의료분쟁을 겪고 있는 병원이 소송수행을 위해 변호사에게 그 환자의 의료기록을 제공하는 것은 개인정보처리자(병원)의 정당한 이익으로 인정되어야 하지만, 현행의 개인정보보호법에서는 5년 이하의 징역을 감수해야 할지 모른다. 그밖에 개인정보보호법은 민감정보와 고유식별정보의 경우 그 수집·이용·제공의 합법적 근거로 동의와 법령 두 가지만을 인정하고 있다(제23조, 제24조). GDPR이 민감정보의 경우 동의 외에 9가지 예외를 인정하고 있는 것이나, 일본이 동의 외에 6가지 합법적 근거를 인정하고 있는 것과 비교하면, 민감정보와 고유식별정보의 경우 정당한 처리의 필요성을 고려하지 못하고 있는 셈이다.

이처럼 한국의 개인정보보호법제는 지나칠 정도로 동의제도에 의존적인 형태을 취하고 있다. 이로 인해 국내 기업을 비롯한 민간의 모든 개인정보처리자는 정보주체의 동의를 사전에 필수적으로 받아야 하는 부담을 안지만, 한편으로는 동의만 받으면 마치 모든 보호의무가 면제되는 듯이 인식할 수 있다.[335] 정보주체인 개인은 동의를 하게 되면 마치 자신의 통제권

335) 김기창, "개인정보 수집, 이용 '동의'를 받아내면 그만인가?", 하버드 비즈니스 리뷰 코리아, 2019 1-2월호("이용자의 사전 '동의' 표시는 사업자를 우월한 지위

을 온전히 행사하는 것으로 착각할 수 있다. 규제당국은 정보주체가 동의했기 때문에 법적 보호가 다 이루어진 것처럼 쉽게 뒷짐을 질 수 있다.

그러나 실제 개인들은 여러 개로 나누어져 있는 동의 체크박스에 마지못해 체크를 하는 것으로 동의의사를 표시하고, 그러나 정작 자신이 무엇에 동의하는지를 정확히 알지 못하는 경우가 허다하다. 많은 개인들은 이해하려고도 하지 않는다. 더군다나, 이해하려고 해도 이해하기 어렵다.[336] 오늘날의 복잡한 기술발전 속에서 개인정보의 수집 및 활용은 소비자나 이용자가 쉽게 이해할 수 없는 기술적 기반과 비즈니스 모델에 기초하고 있기 때문이다. 이런 상황에서 정보주체의 동의라는 보호기제에 지나치게 의존하는 것은 실효적이지 않을 뿐만 아니라 무책임하다는 평가를 받기도 한다.[337] 이처럼 실효성이 의심되는 의존적인 동의제도의 문제점을 되돌아보

에 놓이게 하고 사업자에게 매우 강력한 면죄부로 작용한다. 이용자의 사전 동의가 있기 때문에 사후에 사업자의 배신 행위에 대한 책임을 추궁하기가 현실적으로 어려워지는 것이다.")

336) 김송옥, "유럽연합 GDPR의 동의제도 분석 및 우리 개인정보보호법제에 주는 시사점", 아주법학 제13권 제3호, 아주대학교 법학연구소, 2019, 166면("동의제도는 정보주체의 '동의'가 있었다는 이유로 사업자를 우월한 지위에 놓이게 하고 사업자에게 매우 강력한 면죄부로 작용함으로써 결국 본래의 목적과 달리 정보주체를 보호하지 못한다. 특히 동의권과 개인정보자기결정권을 동일시하는 인식으로 인하여, 동의제도는 자신에 관한 정보가 어떻게 처리되는지 미리 검토하고 결정해야 한다는 부담을 정보주체에게 지우는 반면, 개인정보 처리의 타당성 등을 사전에 검토하고 판단해야 하는 사업자의 부담을 덜어주는 방향으로 전개되어왔다. 사업자와 달리 정보주체는 그러한 결정에 필요한 지식과 정보가 없고, 특히 사업자는 자신의 개인정보처리 행위로 인하여 발생할 수 있는 피해를 막을 수 있는 지위에 있다는 점을 고려하면, 동의제도는 오히려 정보주체에게 불리한 제도이다."). 그 외 유사한 논지를 펼치고 있는 글로서는, 고학수, "개인정보보호의 법, 경제 및 이노베이션", 경제규제와 법 제5권 제2호, 서울대학교 공익산업법센터, 2012, 153면; 구태언, "개인정보보호법상 동의 관련 범죄의 비범죄화 및 대안에 관한 연구", 가천법학 제6권 제4호, 가천대학교 법학연구소, 2013, 73면; 문재완, "개인정보 보호법제의 헌법적 고찰", 세계헌법연구 제19권 제2호, 세계헌법학회 한국학회, 2013, 293면; 박웅신, "변화하는 환경에서 개인정보 보호의 문제점과 개선방안에 관한 검토", 법학연구 제24권 제3호, 경상대학교 법학연구소, 2016, 107면.

337) 미국 코넬 대학교 정보과학 교수인 헬렌 니센바움(Helen Nissenbaum)도 동의에 기반한 개인정보보호정책이 근본적 결함을 지니고 있다고 지적하면서, "동의는 이제 그만 생각해야 한다. 동의는 가능하지도 않고, 옳지도 않다(Stop

아야 할 것이다.

우선적으로 시급한 현실적인 개선방안은 EU의 GDPR과 같이 일반법인 개인정보보호법에 있는 수집·이용의 합법성 근거를 제3자 제공의 경우에도 동일하게 인정하고, 정보통신망의 영역에서도 원칙적으로 동일한 기준이 적용되도록 하는 것이다. 글로벌 기준이라고 할 수 있는 EU GDPR의 예를 따르는 것이 적절해 보인다.[338]

제2절 가명정보 활용범위의 문제점과 개선방향(가명정보 활용 범위의 구체화 필요)

개정 「개인정보보호법」의 가장 큰 변화 중 하나는 개인정보의 가명 처리를 전제로 일정한 활용 가능성을 열어 둔 것이다. 「개인정보보호법」 제28조의2[339]에서 가명정보는 세 가지 목적을 위해 이용될 수 있다. 공익적 기록보존 목적, 과학적 연구 목적, 통계 목적이 그것이다. 그런데 기록보존에 대해서는 '공익적'이란 단서가 명시적으로 나타나는데, 그 외의 두 가지 목적에 대해선 공익적 목적이 명시적으로 요구되지 않는다. 또한 「개인정보보호법」과 달리 신용정보법은 통계 목적에 상업적 목적이 포함되고, 연구에는 산업적 연구가 포함된다고 명시적으로 규정하고 있기도 하다. 개인정보 유형의 데이터에 대해 상업적 활용이 허용돼야 하는지는 사실 간단하지 않은 이슈다. 연구의 개념이나 범위를 어떻게 설정할지도 쉽지 않다. 이는 단순히 데이터의 활용 목적에 관한 문제에 그치는 것이 아

---

thinking about consent. it isn't possible and it isn't right)."고 강조한다. 하버드 비즈니스 리뷰 코리아 2019 1-2월호.

338) 이인환, 앞의 논문(註 318), 275-279면.

339) 개인정보보호법 제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

니라 데이터에 대한 접근 권한과 통제권을 어떻게 설정할 것인지의 문제와 직결된다.[340] 산업의 발전을 위해 필요한 부분이겠지만 과연 개인정보 보호가 어떻게 보호될지 신중한 접근이 필요하며 데이터의 어디까지를 개인정보로 볼 것인지 대한 명확한 정의와 범주 구분이 필요하다. 「개인정보보호법」 개정안에서는 과학적 연구를 '기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등'이라고 정의하고 있다. 그러나 이 정의만 봤을 때 기업이 상업적 목적으로 어디까지 써도 되는지가 불명확해 하위 법령인 시행령에서 보다 구체화 될 필요가 있다.[341]

뿐만 아니라, 가명정보가 재제공 될 경우 해당 과정에서 재식별된 결과에 대한 책임 부과, 가명정보 활용의 이후 삭제와 관련된 내용은 존재하지 않으므로 이와 관련한 문제에 대한 해결책 또한 필요가 있다.

제3절 정보통신서비스제공자에 대한 특례조항의 문제점과 개선방향

「개인정보보호법」 개정 이전에는, 개정 전 개인정보보호법과 개정 전 정보통신망법을 통해 규제 대상 및 소관부처를 온·오프라인으로 양분한 규제 체계를 유지해 왔다. 하지만, 이미 온라인 영업 또는 활동이 보편화된 O2O (on-line과 off-line 환경의 융합) 환경에서, 온라인 또는 오프라인 사업자를 구분하는 것은 실제로 매우 어렵다. 더욱이 지능정보화사회에 접어들면서 온라인을 이용한 기업경영이 보편화되면서 「개인정보보호법」의 '개인정보처리자'와 정보통신망법의 '정보통신서비스 제공자'의 구분이 더욱 모호해졌다. '정보통신서비스 제공자'에 해당하는 "영리를 목적으로 전기통

340) http://news.kmib.co.kr/article/view.asp?arcid=0924133985&code=11171313&cp=du (국민일보, [경제시평] 코로나19와 데이터3법, 2020.4.21.)

341) https://biz.chosun.com/site/data/html_dir/2020/01/13/2020011302674.html (조선비즈, 데이터 3법은 주춧돌, 이제 시작"… 풀어야 할 숙제들, 2020.1.13.)

신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자"(정보통신망법 제2조제1항제3호)는 그 정의가 개념적·포괄적이어서 규제 대상을 확정하기 어렵다. 따라서 전형적인 제조업자(전자, 자동차 등)등도 인터넷 등 전기통신역무를 이용하여 서비스 제공 및 개인정보를 취급하는 경우에는 정보통신서비스제공자에 해당한다고 해석될 수 있다. 특히 인터넷으로 단순히 광고 등 행위를 하지만 개인정보를 처리하지 않는 영세사업자의 경우에 자신이 정보통신서비스 제공자인지 여부도 혼란스러운 경우도 발생할 수 있다. 이와 같은 문제는 어떤 사업자에 대해 어느 법을 적용해야 할지 여부부터 혼란을 야기하고, 이러한 체계는 소관 부처 간 정책 및 법집행의 일관성 미흡, 법준수 관련 사업자의 혼란 등의 원인으로 작용했다. 그리고 동일한 개인정보 처리행위에 대해서도 합리적 차별의 사유가 없음에도 두 법 간의 제재수준의 상이함도 문제로 제기되어 왔다. 이러한 문제는 개정된 「개인정보보호법」에서도 해결되지 못하였다. 개정 정보통신망법에서 개인정보 관련 규정을 삭제하였지만, 개정 전 정보통신망법의 개인정보 관련 조항 중, ①「개인정보보호법」과 유사·중복되지만 정보통신서비스제공자 등에게만 특별히 적용할 필요가 있다고 판단되는 일부 조항과[342], ②「개인정보보호법」에는 규정이 없고 개정 전 정보통신망법에만 규정되어 있던 일부 조항을[343] 거의 그대로 「개인정보보호법」내의 '정보통신서비스 제공자 등의 개인정보 처리 등 특례' 조항으로 옮겨 왔다.[344]

그렇다면, 법리적으로도 '특례 조항'은 다른 일반 조항과 차별적 규제의 당위성이 인정되어야 한다. 하지만 개정법은 여전히 규제대상의 모호한 이

342) 개인정보의 수집·이용(제39조의3 제1항, 제22항), 법정대리인 동의(제39조의3 제4항~제6항, 개인정보 유출통지 신고의무(제39조의4), 개인정보 1년 유효기간제(제39조의6), 개인정보 이용내역의 통지(제39조의8), 국외이전 개인정보의 보호(제39조의12) 등.

343) 손해배상책임보험 의무가입(제39조의9), 국내대리인 지정(제39조의11), 상호주의(제39조의13) 등.

344) 강달천, "개인정보자기결정권 보호의 한계의 관점에서 본 「개인정보보호법」 개정의 문제점", 중앙법학 제22집 제3호, 2020.9., 38-39면.

원화, 영역 간 유사·중복 규제의 잔존 및 비합리적 규제수준의 상이함 등 논란을 남겨 놓고 있다. 예를 들면, 일반조항인 제15조는 동의받을 때에 고지사항을 4개(수집항목, 수집목적, 보유기간, 동의거부권)로 규정하지만, 특례조항인 제39조의3은 동의거부권을 제외한 3개로 규정하고 있다. 즉, 정보통신서비스제공자는 동의를 얻을 때에 '동의를 거부할 권리'가 있음을 고지할 필요가 없다. 이 동의거부권은 정보주체 또는 이용자에게 가장 중요한 권리 중의 하나임에도 정보통신서비스제공자에게만 고지의무를 면제해줄 상당한 이유를 찾기는 어렵다. 또한 제15조는 '동의'를 법률근거, 계약이행, 개인정보처리자의 정당한 이익 달성 등 6개 적법처리 요건 중의 하나로 규정하여 동의 이외에도 개인정보를 수집, 이용할 수 있는 길을 열어주고 있다. 하지만 특례조항 제39조의3은 원칙적으로 '동의'를 필수조건으로 할 뿐 아니라, 경제적·기술적 사유, 요금정산, 법률근거 등만을 예외로 인정하고 있다. 여기에서도 정보통신서비스제공자에게는 계약이행, 정당한 이익 달성 등의 경우에도 왜 동의를 필수요건으로 하는지에 대한 합리적 차별성을 찾아보기 어렵다. 결국, 이 특례조항은 일반조항과의 대표적인 유사·중복 규정 사례로서 동의의 합리적 규제를 통한 개인정보 이용활성화라는 개정 개인정보보호법의 취지와도 부합하지 않는 것이다. 위 규정과 관련한 또 다른 문제는, 위반 시의 제재수준 자체의 비형평성 뿐만 아니라, '정보통신서비스제공자'와 '개인정보처리자'와의 경계가 모호한 상황에서, 어디에 해당되는지에 따라 처벌조항도 다르게 적용된다는 것이다. 제15조의 동의없는 수집에 대해서는 위반 시 행정처분(5천만원 이하 과태료)만 부과되지만, 제39조3의 정보통신서비스제공자의 동의없는 수집 행위에 대해서는 그 자체만으로 과징금(위반행위 관련 매출액의 100분의3) 및 형사처벌(5년 이하의 징역 또는 5천만원 이하의 벌금) 등 제재를 받는다. 이러한 규제수준의 상이함은, 오프라인보다 온라인 환경에서의 개인정보 처리가 더 위험성이 크다는 점을 감안하더라도, 그 제재의 합리적 차별성과 규제수준의 형평성을 인정하기는 어렵다고 할 것이다.[345]

345) 강달천, 위의 논문(註 330), 39-40면.

결국, ‘특례조항’과 관련하여 ①정보통신서비스제공자자와 개인정보처리자라는 이분법에 따른 적용대상 구분의 모호함과 ②이들에 대한 규제수준의 상이함과 비형평성 논란, ③특례 규정에의 유사·중복 규정의 잔존 문제 등 정보통신서비스제공자에 대한 규제를 개인정보처리자의 그것과 달리하여 특별히 규제하여야 할 부분에 합리적으로 차별을 두고 있는지(차별의 당위성) 여부에 대해 다시한번 검토가 필요할 것이다.[346]

제4절 개인정보보호위원회 독립성 문제점과 개선방향

독립된 개인정보보호 감독기구는 개인정보보호법이 존재하기 위한 필수조건이며, 공공부문과 민간부문 모두를 아우르는 기구로서 정부 또는 여타 기관의 직·간접적 간섭을 받지 않는 완전히 독립된 기구여야 한다. 물론 독립성 자체가 목적이 될 수는 없다. 기관의 독립성은 공정하고 객관적인 결과를 얻기 위한 수단일 뿐이며 공정한 결과를 위한 한 축이다. 즉, 감독기구와 그 구성원의 직·간접적인 외부 영향으로부터의 독립은 개인정보 문제를 결정함에 있어서 완전한 공정성을 보장하기 위한 한 축이다.[347]

개정 「개인정보보호법」은 개인정보보호위원회를 국무총리 소속의 중앙행정기관으로 하고 독자적인 조직·인사·예산권 및 조사·처분 등 집행권과 의안제출 건의권 및 국회·국무회의 발언권을 부여하였다. 그리고 개인정보보호위원회를 국무총리 소속으로 하되 조사·처분 등 일부 기능에 대해서는 국무총리의 행정감독권을 배제하였다(제7조제2항)[348].이러한 보호위원회 규

346) 강달천, 위의 논문(註 330), 40-41면.
347) 강달천, 위의 논문(註 330), 41면.
348) 개인정보보호법 제7조제2항은, 보호위원회의 소관사무 중 법 제7조의8 제3호 및 제4호(정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항/개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁) 및 법 제7조의9 제1호(보호위원회 심의·의결 사항 중 개인정보 침해요인 평가에 관한 사항)에 관해서만 국무총리의 행정감독권의 적용을 배제한다고 규정한다.

정은 전반적으로 감독기구의 독립성 확보라는 면에 부합하는 것으로 보인다. 그러나 국무총리의 행정감독권을 개인정보보호위원회의 일부 업무만을 제외한 대부분의 업무에 대해 배제하지 않은 것에 대해서는 실질적 독립성 보장이 어렵다고 볼 수도 있다. 예를 들면, 개인정보보호위원회의 소관업무로 명시되어 있는 개인정보보호 관련 법령 개선에 관한 사항, 개인정보 보호 관련 정책·제도·계획수립·집행에 관한 사항, 개인정보보호위원회의 심의·의결 사항 중 개인정보 침해요인 평가에 관한 사항을 제외한 모든 심의·의결 사항은 국무총리의 행정감독권 하에 놓여 있다. 개인정보보호위원회가 대통령 소속에서 국무총리 소속으로 격하되었다는 사실만으로는 그 독립성이 훼손된다고 볼 수 없을지라도, 개인정보보호위원회의 많은 소관업무가 국무총리의 감독 하에 놓여 있는 한, 그 자체로 보호위원회는 직·간접적으로 영향을 받을 수 밖에 없는 지위에 놓이게 되어 독립성 요건을 충족하였다고 보기는 어렵다.[349]

특히 유럽사법재판소(CJEU)는 여러 판결을 통해 개인정보 감독기관의 '완전한 독립성'의 의미를 구체화하였다. 특히 독일 개인정보 감독기관에 대한 C-518/07 판결에서 개인정보 감독기관들이 지침에서 보장된 개인정보 처리와 관련된 권리의 '수호자'이며, 완전히 독립적인 감독기관의 설치는 "개인정보의 처리와 관련하여 개인을 보호하기 위한 필수적인 구성요소"라고 강조하였다. 개인정보 감독기관이 '완전한 독립성'을 가지고 기능하는 것에 대한 법적 요건은 피감독 기관들로부터의 영향만이 아니라 국가나 주의 직접 또는 간접적인 영향을 포함하여, 어떠한 외부의 영향력으로부터도 자유로운 의사결정 권한을 의미한다. 또한, C-614/10 판결에서는 오스트리아의 개인정보 보호 감독기관의 상임위원 및 사무처의 직제에 있어서 완전히 독립적이지 않다고 보았고, C-288/12 판결에서는 헝가리의 개인정보 보호 감독기관의 재직기간이 전 임기를 보장하고 있지 않다는 점에서 완전히 독립적이지 않다고 보았다.[350]

---

349) 강달천, 위의 논문(註 330), 41-42면.

350) AI 시대, 세계 각국의 개인정보 보호제도 (슬로우뉴스, 2021.1.12.,

EU의 GDPR에서도 '개인정보보호법에 규정된 업무'에 대해서는 감독기구가 독립적으로 업무를 수행하는 것을 보장하고 있다. "각 감독기구의 위원들은 본 규정(GDPR)에 따라 부여된 직무를 수행하고 권한을 행사하는 과정에서 외부의 직간접적인 영향을 받지 아니하고 다른 누구에게도 지시를 구하거나 받지 아니한다."고 규정하고 있으므로(제52조제2항), 적어도 국내의 개인정보보호법에 규정된 개인정보보호위원회의 소관업무에 한해서는 국무총리의 행정감독권 범위에 대한 합리적 개선이 필요하다.[351]

https://slownews.kr/79101)

351) 강달천, 위의 논문(註 330), 42면.

제7장 결론

오늘 날 우리는 과거 산업화 시대를 거쳐 과학기술과 정보통신의 발달로 고도로 발전된 지능정보화사회에서 살아가고 있다. 이러한 환경에서 방대하고 다양한 정보의 수집과 이용이 활발하게 이루어지고 있는데, 그 중 개인정보의 수집과 활용 또한 포함될 수 밖에 없었다. 이와 같은 변화는 정보주체의 권리를 위협하고 인간이 가지는 불가침의 기본적 인권을 침해하고 있었다. 이와 같은 문제를 해결하고자 개인정보자기결정권의 보장과 실효성을 강조하기 위하여 본 연구는 지금까지 지능정보화사회에서의 개인정보의 보호(제2장), 개인정보자기결정권(제3장), 해외의 개인정보 보호법제 현황(제4장), 국내의 개인정보 보호법제 현황(제5장), 개인정보자기결정권을 위한 개인정보 보호법제의 개선방향(제6장)에 관하여 살펴보았다.

요약하면, 지능정보화사회에서 헌법상 개인정보자기결정권에 관한 연구를 시작하기 위하여 먼저 정보주체의 기본권 보장이라는 헌법적 차원에서 개인정보의 의미를 살펴보고, 지능정보화사회에서 개인정보가 침해되고 있는 심각성을 유형별로 검토하여 지능정보화사회에서 개인정보 보호의 중요성을 깨닫고 개인정보 보호가 필요한 이유를 살펴보았다. 자기 자신의 정보를 스스로 통제할 수 있는 개인정보자기결정권을 적극적 청구권으로 해석하여 그 실효성을 강조하였다.

지능정보화사회에서 선제적으로 개인정보를 보호하고 정보주체의 권리를 보장하고 있는 해외 주요국들의 개인정보 보호법제를 살펴보았는데, 특히 EU에서는 EU회원국에 공통적으로 적용되고 법적 구속력을 갖춘 EU의 GDPR을 시행하고 있었다. EU의 GDPR은 회원국 뿐만 아니라 회원국의 개인정보를 취급하는 비유럽 국가들에도 의무적으로 적용되어 국제적 기준으로 중요한 역할을 하고 있었다. 이어서 독일, 프랑스, 영국, 미국, 일본의 개인정보 보호법제를 살펴보았고 이들이 시사하는 점을 '잊힐 권리'를 중점

으로 논의하였다. 잊힐 권리와 개인정보자기결정권의 관련성을 헌법적 근거에서 찾아 새로운 기본권으로 정립되어야 함을 제안하였다.

이에 우리나라도 새로운 시대에 상응하는 개인정보 보호정책으로 2020년 4월 개인정보 보호법을 개정하였다. 국내의 개인정보 보호법제를 시대의 흐름에 따라 정리하였고, 최근 개정된 현행 개인정보 보호법제의 주요 개정 내용 다양한 측면에서 연구해 보았다.

마지막으로 현행 개인정보 보호법제의 문제점을 1)정보주체의 동의제도에 의존하고 있으나, 사실상 실효적이지 않고 무책임하여 개인정보자기결정권을 실질적으로 보장하지 못하는 문제점, 2)가명정보의 도입에 따라, 가명정보의 범주 및 활용범위가 불명확하여 개인정보 결정권과 통제권 또한 설정이 명확하지 않다는 문제점, 3)정보통신서비스제공자에 대한 특례조항에서 동의를 받을 때 고지사항 중 동의거부권을 제외하여 일반조항과 규제수준을 달리할 뿐만 아니라, 동의거부권은 정보주체의 중요한 권리 중 하나임에도 고지의무를 제외한 문제점, 4)개인정보보호 감독기구인 개인정보보위원회의 완전하지 않은 독립성의 문제점과 같이 지적하며, 법적 개선방향을 모색하였다.

한편, 국가는 개인정보의 목적 외 수집, 오·남용 및 무분별한 감시·추적 등에 따른 폐해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구해야 한다. 이는 「개인정보 보호법」 제5조 제1항에서도 규정하고 있는 국가의 책무이다. 이러한 국가의 책무는 개인정보 처리에 있어서 정보주체의 보호라는 이 법의 목적을 실현하기 위한 것이다. 또한, 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련해야 한다. 이 또한 「개인정보 보호법」 제5조 제2항에서 규정하고 있다. 「개인정보보호법」 제4조는 개인정보 처리에 관한 정보를 제공받을 권리 등 정보주체의 원칙적인 다섯 가지 권리를 규정하고, 동 법 제5장은 정보주체의 권리 보장을 규율한다. 이러한 명시적인 규정에도 불구하고 국가는 보다 적극적으로 정보주체의 권리를 보호하기 위한 시책을 개발하여 시행해야 할 것이다.

지능정보화사회에서 정보와 데이터의 활용은 우리에게 수많은 기회를 안

겨주고 있고, 이에 대하여 생각하는 방식에 근본적인 변화를 가져오고 있다. 정보와 데이터는 곧 재산을 의미하고, 국가와 기업은 이를 활용하여 삶의 편의성과 생산성을 증대시키고 있으므로 빅데이터의 활용도 중요하다. 그렇다면 개인정보 보호와 빅데이터 활용의 조화가 적절히 이루어져야 할 것이며, 무엇보다 새로운 기술의 개발과 연구를 위한 목적이 개인의 권리 보호보다 우위에 설 수는 없을 것이다. 또한 개인정보의 활용이 악의적으로 악용되지 않고 개인의 삶의 질이 향상될 수 있는 방향으로 나아갈 수 있도록 철저한 입법적 대처가 필요할 것이다.

개인정보와 정보주체의 권리 보호를 위해 개인정보 침해 문제를 제대로 인식하고 이를 해결하기 위한 개인정보 보호 체계를 구축해 나가는 것은 지능정보화시대뿐만 아니라 이후에 다가오는 새로운 시대에도 끈임없이 연구해 나가야 하는 과제이다. 앞으로는 예측하지 못한 새로운 문제들이 발생 가능할 것이므로, 변화하는 디지털 산업을 예의주시하고 변화속도에 맞춰 발빠른 대응으로 개인정보 보호와 관련한 법제의 정비를 지속적으로 해 나가야 할 것이다.

【참고문헌】

1. 국내문헌

[단행본]

권영성, 「헌법학원론」, 법문사, 2010.
김철수, 「헌법학개론」, 박영사, 2010.
성낙인, 「헌법학」, 제20판, 법문사, 2020.
양 건, 「헌법강의」, 법문사, 2018.
한수웅, 「헌법학」, 법문사, 2013.
한수웅, 「헌법학」, 법문사, 2019.
허 영, 「한국헌법론」, 박영사, 2012.
이준일, 「기본권이론」, 한길사, 2007.

개인정보보호위원회, 「개인정보 보호 법령 및 지침·고시 해설」, 2020.12.
고선규, 「인공지능과 어떻게 공존할 것인가?」, 타커스, 2019.
고학수, 「개인정보 보호의 법과정책」, 박영사, 2016.
권건보, 「개인정보보호와 자기정보통제권」, 경인문화사, 2005.
권건보, 「정보주체의 개인정보자기결정권」(개정판 개인정보보호의 법과 정책), 박영사, 2016.
김재형, 「언론과 인격권」, 박영사, 2012.
김주영 · 손형섭, 「개인정보보호법의 이해」, 법문사, 2012.
신종철, 「개인정보보호법 해설」, 진한엠앤비, 2020.
이창범, 「개인정보보호법」, 법문사, 2012.
정태호, 「독일기본권론 제33판 (Kingrenn/Poscher, Grundrechte Staatsrecht Ⅱ 33. Aufl.)」, 박영사, 2021.
함인선, 「개정판 EU개인정보판례」, 전남대학교 출판문화원, 2018.

문재완, 「잊혀질 권리(이상과 실현)」, 집문당, 2016.
로베르트 알렉시, 「기본권 이론」, 한길사, 2007.
Viktor Mayer-Schönberger, 구본권 옮김, 「잊혀질 권리」, 지식의 날개, 2011.

[국내논문]

강달천, “개인정보자기결정권 보호의 한계의 관점에서 본 「개인정보보호법」 개정의 문제점”, 중앙법학 제22집 제3호, 2020.9.
강태욱, “데이터 3법 통과... 의료·AI 등 산업 탄력 전망”, KISO JOURNAL Vol.38, 2020.2.
고수윤, “빅데이터의 개인정보 이용으로 인한 법익침해의 私法적 해석”, 강원법학 제52권, 2017.10.
고영삼, “전자감시사회와 프라이버시”, 한울 아카데미, 1998.
권건보, “개인정보자기결정권의 보호범위에 대한 분석 - 개인정보의 개념을 중심으로 -”, 공법학연구 18-3(한국비교공법학회), 2017.
권건보, “자기정보통제권에 관한 연구”, 서울대학교 법학박사학위논문, 2004.
권건보, “개인정보보호의 헌법적 기초와 과제”, 저스티스 통권 제144호, 2014.
권건보・김일환, “지능정보시대에 대응한 개인정보자기결정권의 실효적 보장 방안”, 미국헌법연구 제30권 제2호, 2019.
권건보, 이한주, 김일환, “EU GDPR 제정 과정 및 그 이후 입법동향에 관한 연구”, 미국헌법연구 제29권 제1호, 2018.4.
권영준, “개인정보 자기결정권과 동의 제도에 대한 고찰”, 「법학논총」 제36권 제1호, 2016.
권헌영 외, “4차 산업혁명시대 개인정보권의 법리적재검토”, 「저스티스」 제158-1호, 2017.
김민호·이규정·김현경, “지능정보사회의 규범설정 기본원칙에 대한 고찰”, 성균관법학 제28권 제3호, 2016.9.
김배원, “지능정보사회와 헌법 - 인공지능(AI)의 발전과 헌법적 접근-”,

「공법학연구」 제21권 제3호, 비교공법학회, 2020.8.
김배원, “정보기본권의 독자성과 타당 범위에 대한 고찰”, 헌법학연구 제12권 제2호, 2006.
김상겸 외 5인, “개인정보보호법 정비방안 연구”, 한국인터넷법학회, 2012.
김상범·김효관, “4차 산업혁명과 빅데이터 기반 기술”, 전자공학회지 제46권 제11호, 2019.11.
김송옥, “잊혀질 권리에 대한 비판적 고찰”, 언론과법 제14권 제1호, 2015.
김일환, “정보자기결정권의 헌법상 근거와 보호에 관한 연구”, 공법연구 제29집 제3호, 한국공법학회, 2001.
김용일, 김유정, “우리나라 개인정보보호 법제의 개선방안에 관한 연구”, 법과 정책 제27권 제1호, 2021.3.
김종철, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 인터넷법률 제4호, 2001.
김태오, “사이버 안전의 공법적 기초”, 행정법연구 제45호, 2016.6.
김태오, “데이터 주도 혁신 시대의 개인정보자기결정권 -정보통신망법과 EU GDPR의 동의 제도 비교를 통한 규제 개선방향을 중심으로-”, 「행정법연구」 제55호, 2018.
김창조, “정보주체의 개인정보자기결정권 보장과 개인정보의 활용”, 경북대학교 법학연구원 법학논고 제75집, 2021.
문재완, “개인정보 보호법제의 헌법적 고찰”, 세계헌법연구 제19권 2호, 2013.
문재완, “개인정보의 개념에 관한 연구”, 공법연구 제42집 제3호, 한국공법학회, 2014.2.
문재완, “유럽연합(EU) 개인정보보호법의 특징과 최근 발전”, 외법논집 제40권 제1호, 2016.2.
문재완, “프라이버시 보호: 신화에서 규범으로”, 개인정보보호법제 개선을 위한 정책연구보고서, 2013.2.
박경신, ““구글 스페인” 유럽사법재판소 판결 평석-개인정보자기결정권의 유래를 중심으로-”, 세계헌법연구 제20권 3호, 2014.

박노형, “한국 개인정보보호법과의 비교를 통한 EU GDPR의 이해”, 언론중재 147, 2018.

박노형·정명현, “빅데이터 분석기술 활성화를 위한 개인정보보호법의 개선방안-EU GDPR과의 비교분석을 중심으로-”, 고려법학 제85호, 2017.

박정훈, “잊혀질 권리와 표현의 자유, 그리고 정보프라이버시”, 공법학연구 제14권 제2호, 한국비교공법학회, 2013.

백제현, “사물인터넷(IoT) 환경에서 전자적 증거의 증거능력 제고방안에 관한 연구”, 성균관대학교 법학전문대학원 박사학위논문, 2019.

선원진·김두현, “초연결사회로의 변화와 개인정보 보호”, 한국통신학회지(정보와 통신) 제31권 제4호, 2014.

성낙인 외, “개인정보보호를 위한 정책방안 연구”, 정보통신산업진흥원, 1999.

성준호, “빅데이터 환경에서 개인정보보호에 관한 법적 검토”, 법제연구 제21권 제2호, 2013.

심상현, “개인정보 관련 제재 및 피해구제 합리화 방안 연구”, 한국인터넷진흥원, 2013.

심우민, “인공지능의 발전과 알고리즘의 규제적 속성”, 법과 사회 53호, 2016.12

원소연·심우현, “지능정보사회 촉진을 위한 데이터 및 정보관련 규제 개선방안 연구”, 한국행정연구원, 2019.

이상윤 외, “빅데이터 관련 개인정보 보호법제 개선방안 연구”, 법제처 한국법제연구원, 2017.10.

이소은, “개인정보 보호법의 주요 개정 내용과 그에 대한 평가”, 이화여자대학교 법학논집 제24권 제3호 통권 69호, 2020.3.

이양복, “데이터 3법의 분석과 향후과제”, 비교사법 제27권 2호(통권 제89호), 2020.5.

이원태, “EU의 알고리즘 규제 이슈와 정책적 시사점”, KISDI16-12 Premium Report, 2016.12.

이원태·문정욱·류현숙, “지능정보사회의 공공정보화 패러다임 변화와 미래

정책연구", KISDI(정보통신정책연구원) 기본연구 17-01, 2017.10.
이인호, "'잊힐 권리' 관련 최근 소송 동향 및 이슈", 언론중재, 2020.
이인호, "정보통신기술의 발전과 기본권에 관한 연구", 헌법재판연구 제25권, 헌법재판소, 2014.
이인호, "지능정보사회에서 개인정보보호의 법과 정책의 패러다임 전환", 과학기술과 법 제11권 제2호, 2020.12.
이정념, "개인정보보호법의 개정 의의와 적용상 한계", 「저스티스」 통권 제179호, 2020.8.
이창범, "개인정보호보법제 관점에서 본 빅데이터 활용과 보호방안", 법학논총 제37권 제1호, 2013.
이한주 외, "지능정보화사회에서 개인정보 법제정비에 관한 비교법적 검토", 성균관법학 제30권 제1호, 2018.
이해원, "데이터 경제 시대의 개인정보 보호와 사적 자치", 정보법학 제24권 제2호, 2020.8.
이희옥, "초연결사회를 위한 개인정보보호법제의 개선방향", 법제논단 3월호, 2019.3.
전상현, "개인정보자기결정권의 헌법상 근거와 보호영역", 저스티스 통권 제169호, 2018.12.
정문식・정호경, "정보기관의 해외 통신 정보 활동에 대한 헌법적 한계- 독일연방정보원법(BNDG)의 위헌 결정에 나타난 위헌 심사 기준과 내용을 중심으로", 공법연구 제49집 제3호, 2021.
정애령, "사생활보호와 개인정보보호의 관계에 관한 연구", 공법학연구 제17권 제3호, 2016.
정애령, "지능정보사회 개인정보자기결정권을 보완하는 데이터 활용과 개인정보보호", 공법학연구 제23권 제1호, 2022.
정원준, "데이터 이동권 도입의 실익과 입법적 방안 모색", 성균관법학 제32권 제2호, 성균관대학교 법학연구원, 2020.
정종구, "인공지능 시대의 개인정보 개념에 대한 연구 -자연어 처리를 중

심으로-", 법학논총 제38집 제2호, 2021.6.
정태호, "개인정보자기결정권의 헌법적 근거 및 구조에 대한 고찰 -동시에 교육행정정보시스템(NEIS)의 위헌여부의 판단에의 그 응용-", 헌법논총, 제14집, 2003.
정태호, "현행 인구주택 총조사의 위헌성 - 독일의 인구조사판결(BVerGE 65,1)의 법리분석과 우리의 관련법제에 대한 반성", 법률행정논총 제20집, 2000.
조소영, "잊혀질 권리", 공법연구 제41집 제2호, 한국공법학회, 2012.
주승희, "데이터 3법의 주요 개정 내용 및 형사법적 의의에 관한 소고", 숭실대학교 법학논총 제49집, 2021.1.
채성희, "개인정보의 개념에 관한 연구 : 식별가능성에 관한 유럽 및 일본의 논의를 중심으로", 서울대학교 대학원 석사학위 논문, 2017.
채성희, "개인정보자기결정권과 잊혀진 헌법재판소 결정들을 위한 변명", 정보법학, 제20권 제3호, 2016.
최경진 외 5인,□빅데이터 환경에서 개인정보호 강화를 위한 법·제도적 대책방안 연구", 개인정보보호위원회, 2012.12.
최경진, "잊혀질 권리'에 관한 유럽사법재판소(ECJ) 판결의 유럽 법제상 의미와 우리 법제에 대한 시사점", 법학논총, 제38권 제3호, 단국대학교 법학연구소, 2014.
최규환, "가명정보와 개인정보자기결정권", 헌법재판소 헌법재판연구원, 2021.
한동훈, "유럽연합의 잊힐 권리에 관한 연구:프랑수의 경우를 중심으로", 헌법재판소 헌법재판연구원, 2021.
한수웅, "헌법상의 인격권", 헌법논총 제13집, 2002.
홍명신, "정보의 웰다잉을 향한 시도", 언론중재 제31권 제2호, 언론중재위원회, 2011.
홍선기, 고영미, "개인정보보호법의 GDPR 및 4차산업혁명에 대한 대응방안 연구", 법학논총 제43권 제1호, 2019.
한국인터넷진흥원, "개인정보보호 월간동향분석(미국 연방 개인정보보호법안

(ADPPA) 주요 내용과 시사점)", 2022.5.
한국인터넷진흥원, "독일 개인정보보호 법 행정 체계 현황 및 주요 위반사례('21.11월 기준)", 2021.11.
한국인터넷진흥원, "영국 개인정보보호 법 행정 체계 현황 및 주요 위반사례('21.11월 기준)", 2021.11.
한국인터넷진흥원, "일본 개인정보보호 법 행정 체계 현황 및 주요 위반사례('21.11월 기준)", 2021.11.
한국인터넷진흥원, "프랑스 개인정보보호 법 행정 체계 현황 및 주요 위반사례('21.11월 기준)", 2021.11.
함인선, "AI시대에서의 개인정보자기결정권의 재검토:EU 개인정보보호법을 소재로 하여", 전남대학교 법학연구소 공익인권법센터, 인권법평론 제26호, 2021.2.
함인선, "EU의 2016년 일반정보보호규칙(GDPR)의 제정과 그 시사점", 법학논총 제36권 제3호, 전남대학교 법학연구소, 2016.9.
함인선, "EU개인정보보호법", 마로니에, 2016.

2. 해외문헌

ARTICLE 29 DATA PROTECTION WORKING PARTY, 「Opinion 15/2011 on the definition of consent」, 2011.7.13.
ARTICLE 29 DATA PROTECTION WORKING PARTY, 「Guidelines on consent under Regulation 2016/679」, 2018.4.10.
Daniel Bell, "Communication Technology – For Better or For Worse?", Jerry L. Salvaggio,Telecommunications: Issues and Choices for Society (New York and London:Longman, 1983)
Erwin Chemerinsky, Constitutional Law -Principles and Policies -, (3rd ed.), Aspen Publishers, 2006.

Laurence H. Tribe, The InvisibleConstitution, Oxford University Press, 2008.
Mattieu Bourgeois, Droit de la donnée : Principes théoriques et approche pratique, LexisNexis, 2017.
Ray Kurzweil, The Singularity is Near, 2005.
R. Dworkin, LIFE'S DOMAIN: AN ARGUMENT ABOUT ABORTION AND EUTHANASIA, Hart Publishing, 1993.

3. 웹사이트

[국가법령정보센터] https://www.law.go.kr/
[법제처] https://www.moleg.go.kr/
[한국인터넷진흥원] https://www.kisa.or.kr/
[EU(유럽연합)] https://european-union.europa.eu/index_en
[GDPR 대응지원센터] https://gdpr.kisa.or.kr/index.do
[ICO(Information Commissioner's Office;영국 정보보호청)] https://ico.org.uk/
[OECD] http://www.oecd.org/

4. 언론보도

[대한민국 정책브리핑, 대통령 제5차 규제개혁 장관회의 개최(2016.5.19.)]
https://www.korea.kr/news/pressReleaseView.do?newsId=156130013
[행정안전부 보도자료,「개인정보 비식별 조치 가이드라인」발간, (2016.6.30.)]
https://www.mois.go.kr/frt/bbs/type010/commonSelectBoardArticle.do?bbsId=BBSMSTR_000000000008&nttId=55287

[국민일보, ‘경제시평’ 코로나19와 데이터3법, (2020.4.21.)]
http://news.kmib.co.kr/article/view.asp?arcid=0924133985&code=11171313&cp=du
[슬로우뉴스, AI 시대, 세계 각국의 개인정보 보호제도, (2021.1.12.)]
https://slownews.kr/79101
[조선비즈, 데이터 3법은 주춧돌, 이제 시작"… 풀어야 할 숙제들, (2020.1.13.)]
https://biz.chosun.com/site/data/html_dir/2020/01/13/2020011302674.html
[정부 관계부처 합동, “제4차 산업혁명에 대응한 「지능정보사회 중장기 종합대책」, (2016. 12. 27)]
https://www.korea.kr/archive/expDocView.do?docId=37384

A Study on the Right to Self-determination of Personal Information in an Intelligent Information Society

Mi-Rae Heo

Department of Law, The Graduate School,
Pukyong National University

【Abstract】

The purpose of this study is to suggest the direction to strengthen the right to self-determination of personal information in order to protect the personal information and to actively safeguard the right of the information subject under the Constitution while having come to face a new information environment where the personal information is threatened according to the development in information communication technology in an intelligent information society of having been confronted globally. To this end, the importance of personal information protection is preemptively studied by making an analysis on the characteristics of intelligent information society as the background environment of the research and on the infringement types in personal information. It examines the right to self-determination of personal information as the right that the data subject itself can determine and control his or her own information, and emphasizes the necessity of protection focusing on the function of the right to self-determination of personal information as an active claim right.

The aim is to seek the need to establish the right to self-determination of personal information as a new basic right under the Constitution by introducing the Personal Information Protection laws in major overseas countries, which are proactively safeguarding the personal information and are intensifying the right of the information subject in an intelligent information society, in order of EU's GDPR(General Data Protection Regulation), Germany, France, England, America and Japan, and by observing the trend of 'the Right to be Forgotten' that was issued as the implication of foreign Personal Information Protection Legislation.

The domestic Personal Information Protection Act, which realized the right

to self-determination of personal information as a specific system, is studied with the stream of times such as the background of enacting the law, the government's Guideline on De-identification of Personal Information in 2016, the Personal Information Protection Act of having been revised recently. And then, the legal improvements are being devised with pointing out the problems about the current Personal Information Protection Law. Those include 1) the problem of failing to substantially guarantee the right to self-determination of personal information because of being virtually ineffective and irresponsible even though relying on the consent system of the information subject, 2) the problem as saying that the establishment in the right to determine and control the personal information is also unclear because the category and the scope of use in pseudonymous information are vague in accordance with the introduction of pseudonymous information, 3) the problem of having excluded the obligation to notify despite what the right to refuse consent is an important right of the information subject, as well as differing a level of regulation from general provisions because of having excluded the right to refuse consent among the matters to be notified when receiving a consent in the special provisions for information and communication service providers, 4) the problem about incomplete independence of the Personal Information Security Committee, which is the Personal Information Protection Supervisory Organization.

Key Words : Right to self-determination of personal information, Intelligent information society, Information Subject's Rights, Personal Information Protection, Personal Information Protection Law, GDPR(General Data Protection Regulation), Right to be Forgotten, Consent System, Pseudonymous Information, Right to refuse consent, Personal Information Security Committee