개인정보 자기결정권에 관한 비판적 검토

A Critical Study on The Right to Information Self-determination

이 희 옥 (Heui-ok Lee)
한양대 대학원

논문접수 : 2016. 10. 31. 심사게시 : 2016. 11. 22. 게재확정 : 2016. 12. 6.

목 차

Ⅰ. 들어가며

Ⅱ. 개인정보 보호의 헌법적 근거 및 개인정보보호의 법체계
1. 개인정보 보호의 헌법적 근거
2. 외국의 법체계의 검토
3. 시사점

Ⅲ. 판례를 통해서 본 개인정보 자기결정권의 내용과 한계
1. 논의의 개요
2. 개인정보 자기결정권 침해에 대한 최근 판례 검토
3. 개인정보 자기결정권의 한계
4. 법정손해배상책임 인정 입법개정에 관한 검토

Ⅳ. 나가며

국문요약

일찍이 앨빈 토플러는 「미래의 쇼크」, 「제3의 물결」,「권력이동」등을 통해 현대사회의 정보사회로의 전환을 예견해온바, 정보사회란 정보력이 중요한 생산 요소로 등장하고 정보기술이 비약적으로 발달하여 인간 생활에서의 정보의 활용여부가 중요한 요소로 떠오르는 사회를 말한다. 즉 정보는 그 자체로 가치가 되지만 또 다른 새로운 가치를 창출하고 정보화는 기업과 시장을 변화시킨다. 인터넷과 정보통신기술로 정보의 유통이 신속한 사회 속에서 개인은 자기의 정보에 대한 공개와 이용에 관하여 스스로 결정할 권리인 개인정보 자기결정권을 갖는다. 그러면, 개인정보 결정권이라는 기본권은 어떻게 실현되고, 정보주체는 이를 통해 자유롭게 사회에 참여하는 권리를 행사할 수 있을까? 본고는 이에 대한 질문을 따라 논의를 해나간다.

현대의 개인정보 보호의 의미는 보호 자체라기보다는 이를 통해 궁극적으로 추구하는 보호법익에 대한 검토에서 시작되어야 할 것이다. 개인정보보호 법제의 보호법익은 헌법상의 개인정보 자기결정권과 정보주체의 사생활의 비밀과 자유가 대표적이다. 우리사회는 급작스런 IT 산업의 성장과 함께 잇따른 개인정보 유출 사건들로 개인정보의 보호 필요성이 대두되면서 보완책으로서의 법정책적 시도를 해왔다. 그런데 실제 개인정보침해로 인한 침해를 주장하는 소송에서는 그 침해가 인정되더라도 소액의 위자료가 인정되는 것에 그치고 마는 것을 보면 개인정보에 관한 정보주체의 권리는 여전히 형식적인 권리에 머무르고 있는 것으로 보인다. 이것은 개인정보 자기결정권이 공공의 이익이나 타인의 다른 기본권들과 충돌할 때 이익형량을 통해 침해 여부가 결정되는 것 이외에도 개인정보자기결정권의 침해가 인정되는 경우에도 정보주체의 어떤 실체적 권리의 침해로 인정될 수 없었던 그동안의 개인정보 법제의 한계에서도 기인한다.

개인정보 자기결정권 내지는 정보보호는 그것이 실제 소송에서 침해를 주장하고, 이의 손해가 전보될 때 비로소 실체적인 권리로서 인정된다고 할 것이다. 최근 우리의 개인정보 법제는 과거 피해자 보호 시스템의 맹점을 보완하고자 법정손해배상제도 및 징벌적 손해배상제도를 관련 법률에 도입하였다. 다만, 일련의 사건에서 개인정보 자기결정권 침해 기준을 보다 정교하게 제시해가는 최근의 판례의 경향을 보건대, 도입된 제도의 미흡한 점을 두더라도, 개별 법령에서의 보호법익과 권리의 구체화, 침해행위에 대한 위법성의 기준, 손해보전

에 대한 마련 없이 정보주체의 실체적 권리 보장이 충분히 해결될지는 의문이다. 가속화될 정보화 사회에서의 정보인권과 관련한 국가의 역할은 법정책적인 제도 보장을 통한 정보주체의 실체적 권리 실현이다. 이를 위한 국가의 모습은 보장국가 모델이다. 급격한 변화의 시대에 국가는 법정책적 구조를 설정하고, 정보주체의 정보 기본권의 행사가 가능하도록 해야 한다. 개인정보보호법이 마련된 초기의 시도에서 한발 나아간 일관된 자율규제 시스템을 유지하고, 기업들의 참여를 유인하는 적극 유도할 수 있어야 한다.

※ 주제어 : 정보사회, 개인정보 자기결정권, 보장국가, 개인정보, 자율규제

Ⅰ. 들어가며

디지털 정보혁명은 산업혁명 이후 가장 획기적인 과학기술 혁신과 함께 인류에게 놀라운 커뮤니케이션 혁명을 가져온 것으로 평가되고 있다. 디지털 정보사회에서는 누구나 많은 정보를 쉽게 생성・이용・가공할 수 있으며 이를 저장하고 전달할 수도 있다. 고도화된 정보사회에서 정보는 단순한 데이터에 이르지 않으며 정보에 대한 장악과 통제력은 기관과 개인의 권력이자 스스로의 자유를 결정하는 중요한 요소가 되었다.

정보사회에서 정보주체의 자기정보에 대한 지배는 개인의 인격권과 자유권을 행사하는데 근본 조건이 되며, 국가가 이를 지배하는 경우 이는 국민인 개인을 통제할 수 있는 권력의 근간이 된다. 또한 오늘날 시・공간의 구분이 없는 디지털 정보사회에서는 제3자로서 거대 기업들의 정보에 대한 독점적 지배는 그 기업의 경쟁력을 좌지우지하는 핵심적인 요소가 되기도 한다.

정보가 가지는 경제적 가치의 증대로 정보사회에서의 개인에 관한 정보의 활용은 인류의 삶을 윤택하게도 하지만, 개인정보 수집 및 처리 과정에서 정보주체에게 예측할 수 없던 피해를 남기기도 하였다. 무분별한 개인정보의 수집과 이용으로 인한 문제 해결을 위해 2011년 9월 30일부터 시행된 「개인정보보호법」은 공공영역과 민간영역 모두에 걸친 국제수준에 부합하는 개인정보 처리원칙을 규율하고 있다.

2001년부터 2012년까지 감시나 감청, 민감사실에 관한 유포, 과다한 개인정보의 수집 및 유출 등으로 국가인권위원회에 접수된 정보프라이버시와 관련한 민원은 3년간 총31,479건에 건에 달한다.[1] 개인정보 유출로 인한 피해들은 기업의 사이트가 해킹되거나 내부 직원이 대량의 개인정보를 유출한 경우로 알려지고 있지만, 원인파악이 안되는 경우도 허다하고 실제 소송에서는 피해자의 재산상 손해를 입증하거나 손해액을 산정하기가 어려워 소액의 위자료에 그치는 터라, 특히 기업들에게 개인정보 보호에 대한 경각심을 일깨우기에는 극히 미비하다는 비판과 우려가 있어왔다.

개인정보 유출로 인한 피해에 대한 대응책의 실효성이 의문시되는 시점에서, 올해 3월22일 공표되어 7월 25일 시행된 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법')은 개인정보의 분실・도난・유출・위조・변조 또는 훼손된 경우로서 이용자에

1) 정보인권 보고서, 국가인권위원회, 2015. 141면.

게 손해가 발생한 경우에 징벌적 손해배상제도를 도입하였다.

그런데, 이러한 입법 정책적 개선 노력과는 달리 최근 일련의 개인정보 침해로 인한 손해배상을 청구하는 소송들에서 개인정보결정권이라는 인격적 법익의 침해를 주장하는 원고들의 손해배상 청구는 쉽사리 받아들여지지 않고 있다. 정보주체의 인격권으로서 인정되는 개인정보 자기결정권[2]은 공공의 이익에 필요한 경우에는 정보의 처리 행위로 인하여 얻어지는 공중의 '알 권리' 와 '표현의 자유'를 비롯한 공동체의 이익, 경제적 효율성 등의 다른 가치들과 충돌되는 경우 제한될 수 있으며, 현실적으로 개인정보를 취급하는 사업자들은 최초 수집시 정보 주체의 동의를 득하고 있어 최소한의 절차상의 적법성은 갖추고 있는 것이 일반적이다. 사업자들의 정보 수집 과정에서의 동의 방법의 유효성에 관해서 논란이 있을 수 있지만, 스마트 폰의 보편화로 대다수의 서비스들이 모바일 기기 등을 통하여 제공, 이용이 이루어지는 상황에서 현재 약관 등으로 실행되는 방식들보다 효율적이면서 적법한 방식이 있을 것이라는 모호한 비판을 하는 것도 적절치 않다고 생각한다.

요컨대, 정보수집처리자의 정보 수집・처리 행위가 위법하다고 인정되기는 매우 어려운 실정을 고려해보면 관련 소송들에서 피해자의 실질적 손해의 배상이 합리적으로 이루어지지 않고 있다는 것은 그리 놀라온 일이 아니다.

이와 같이 개인정보 자기결정권과 관련된 현실적인 문제들에 대한 대안으로 법・제도적 노력이 모색되고 있으나, 아직까지 개인정보에 대한 권리는 실체적인 권리의 침해가 아니라 법정 위자료에 그치는 정도인 형식적인 권리에 머무르고 있다는 인상이다. 이것은 정보사회에서의 개인정보의 보호의 필요성이 시급하다는 국민적 요구에도 불구함에도 불구하고 헌법상 기본권인 '표현의 자유'와 공익으로 대변될 수 있는 국가차원에서 수사권・행정적 효율성 및 정보화 시대의 신사업의 발전 등의 가치와 '개인정보보호'의 충돌에 따르는 해결의 대안이 충분하지 않은데에 가장 큰 이유가 있다고 할 것이다.

그 동안의 개인정보 유출 사건들에 대한 대응책으로 국가차원에서의 시행되는 법제도의 개선 움직임은 환영할만하나, 지금까지 제시된 국가차원의 보장들은 한편으로는 국가와 민간 사업자들이 개인정보 처리자에 과도한 부담을 주면서 개인정보의 실질적 보호는 이루어지지 않는 맹점이 있다. 더욱이 모든 일상생활을 온라인상에서 해결하고 있는 스마트미디어

2) "개인정보 자기통제권" 또는 "개인정보 관리통제권"이라는 용어가 혼용되고 있으나 여기에서는 헌법재판소 결정에서 쓰이는 "개인정보 자기결정권"이라는 용어를 사용하기로 한다.

세대에서 한번 공개된 정보는 소셜네트워크서비스(SNS)의 위력으로 개인의 의지와 상관 없이 인터넷상에 쉽사리 퍼져나가기 일쑤인데, 이러한 문제까지 생각한다면 후속적인 법정책적 대응은 언제나 한계가 있을 것이다.

결국, 개인정보의 실질적인 보장은 국가의 최소한의 가이드라인 아래서 정보수집·활용을 하는 사업자들로부터의 자율적인 준수를 이끌어 낼 수 있을 때 비로소 보다 실질적이고 창의적인 방안들이 모색되면서 한계점이 보완될 수 있다고 하겠다.

본고에서는 논의의 기초로서 정보사회에서 필연적으로 대두되는 개인정보보호에 관한 근거를 헌법적 관점에서 파악하고, 국외의 개인정보보호법의 체계를 비교함으로써 우리의 개인정보보호 법제의 헌법적 근거와 한계를 논의한다(Ⅱ). 다음으로는 최근 일련의 판례에서 확인되는 개인정보보호의 법체계의 한계를 비판적으로 논의하고, 헌법상 개인정보 관리통제권이 내포한 보호법익에 부합하는 개인정보 보호를 위한 현재 도입된 법정손해배상책임제도의 실효성을 검토한다(Ⅲ). 마지막으로 현재까지 마련된 개인정보보호법 체계로부터의 개인정보 자기결정권의 보호법익의 보장 여부를 검토한고, 실체적 권리의 구제 문제에 확인하여 앞으로 정보화 사회의 발전에 따라 그 영역이 확대될 수밖에 없는 민간영역에서의 개선방안을 모색하며(Ⅳ) 이 글을 마치도록 한다.

Ⅱ. 개인정보 보호의 헌법적 근거 및 개인정보보호의 법체계

1. 개인정보 보호의 헌법적 검토

가. 프라이버시권에 대한 이해

정보를 정보주체의 의사에 반하여 수집되거나 이용당하지 아니할 소극적 자유 즉, 프라이버시권은 국가로부터 사생활을 '방해받지 아니할 권리'에서 비롯하여 현대에 와서는 Warren과 Brandies에 의해, 문명으로부터 "홀로 있을 수 있는 권리"로[3] 전개되었다. 현대사회에서는 국가의 역할의 증대와 행정의 거대화로 인하여 국가가 수집하고 축적하는 정보의 양이 비약적으로 증가하고 있으며, 마찬가지로 가속화되는 정보화 사회의 민간기업 역시 다량의 정보를 수집·축적·관리하고 있다.

정보의 컴퓨터관리체계가 가져온 정보처리의 경제적 효율성·합리성의 이면에는, 정보의

3) Samuel D.Warren & Louis D.Brandeis, The Right to Privacy, 4 Harv. L. REV. 193. 1890.

오남용과 개인정보에 해당하는 정보들의 누출에 관한 문제점들도 있다. 이러한 배경에서 정보사회에는 사적정보 보호를 통해 국민 개개인이 정보유통에 대한 통제력을 지니게 되는 권리로서 정보인권의 하나인 '정보 프라이버시권'으로 이해되기도 한다.[4)]

개인정보 자기결정권 내지는 개인정보 관리통제권이라는 개인정보와 관련된 법적 보호를 논하기 위해서 보호 대상이 되는 개인정보에 대한 의의를 먼저 규명하는 것이 출발점이 되어야 함에도 불구하고, 선행된 논의들은 개인정보의 개념을 확정짓기에 충분하지 않은 것으로 보인다. 지금까지 정리된 개인정보는 개인에 관한 사적인 정보에서 이미 알려진 정보까지도 인정하는 폭넓은 개념으로 이해된다.[5)] 개인정보를 '개인에 관한' 정보라고 이해하는 관점에서는 개인정보에 대한 기념을 개인의 자율성 내지는 인격권의 관점에서 접근하게 되어 개인정보에 관한 소극적인 방어권이 아니라 자기 정보에 대한 자율적 통제에 관한 개념으로 적극적인 성격을 갖는다고 볼 수 있다.[6)] 이러한 맥락에서 개인정보에 대한 헌법적 보호는 개인정보 그 자체보다는 정보가 갖는 사회적 의미에 걸맞게 정보주체의 의사에 반하여 유통되지 아니하도록 정보저리과정에 정보주체가 참여하는 데에 초점을 두어야 할 것이다.

나. 개인정보 보호의 헌법적 근거

(1) 프라이버시권과 헌법 제17조의 관계

외국 법제상 프라이버시권에 대응하는 우리 헌법적 근거로서 헌법 제17조의 '사생활의 비밀과 자유'에서 찾는 것이 많은 헌법학자들의 견해다. 그런데 헌법 제 17조의 사생활의 비밀과 자유를 협의 또는 광의로 보는지에 따라서 프라이버시권의 보호법익에서도 차이가 생긴다. 이하에서는 프라이버시의 헌법적 근거에 대한 학설들을 간략히 살펴보겠다.

먼저, 프라이버시권을 인간의 존엄과 가치 행복추구권에서 찾는 입장이다. 이 입장은 프라이버시의 헌법적 근거로서 헌법 제17조의 사생활의 비밀과 자유를 좁게 생각하고 헌법 제10

4) 이인호, "정보인권 논의가 시사하는 헌법학적 프레임: 디지털시대에 있어서 정보를 둘러싼 권력과 자유의 긴장과 조화", 법학연구 제3호, 가톨릭대학교 법학연구소, 2008. 48면.

5) 개인정보보호법[시행 2016.9.30. 법률 제14107호, 2016.3.29., 일부개정] 제2조 제1호에서는 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 규정하고 있다. 한편 판례는 온라인 게임서비스에 가입한 이용자의 아이디와 비밀번호는 당연히 개인정보로 전제하여 판단하면서도(서울중앙지방법원 2007. 1. 26. 선고 2006나12182 판결), 금융상품에 가입한 고객의 유출 판결에서는 이메일 주소만으로는 특정 개인임을 알 수 없더라도 다른 정보와 결합하여 추정이 가능한 개인정보로 판단하였다. 한편, 수사기관의 통신자료 요청에 관한 판결에서는 아이디에 포털의 이메일 계정이 붙어 있는 것이어서 개인정보라고 보지 않았다(대법원 2016.3.10. 선고 2012다105482 판결).

6) 김민섭, "개인정보의 보호와 이용의 조화에 관한 법제적 연구", 숭실대학교 대학원 박사학위논문, 2015. 18면.

조의 인간의 존엄과 가치에 프라이버시권의 근거를 찾는다. 이는 헌법 제17조의 사생활의 비밀과 자유를 넓게 보아 인격적 이익의 총체를 포함하는 것으로 보게 되면 이는 다른 기본권을 모두 포괄하는 기본권이 되기 때문에 헌법 제17조의 사생활의 비밀과 자유는 좁게 보아야 하며, 사생활의 비밀과 자유를 일반 자유권 조항에서 규정하고 있으므로, 사생활의 비밀과 자유를 자유권으로 본다고 하여 개인의 자기 정보를 통제하는 권리가 부정되는 것은 아니므로 자기 정보에 대한 통제권은 헌법 제17조에서 찾을 것이 아니라 헌법 제10조에서 보장된다고 하는 견해이다.[7)]

다음으로는 헌법 제17조의 사생활의 비밀과 자유권을 넓게 인정하여, 프라이버시권의 근거로 보는 입장이다. 즉 헌법 17조는 넓은 의미에서 인격권의 일부가 되는 권리로 이해하고 프라이버시권을 넓게 해석하여 프라이버시권을 적극적으로 정보주체가 자기의 정보를 관리, 통제할 수 있는 능력으로까지 이해하는 것이다. 이러한 해석을 바탕으로 할 경우 헌법 제17조의 사생활의 비밀과 자유는 프라이버시권을 의미한다고 할 수 있다. 또한 인격권은 인격적 이익인 생명, 신체, 건강, 명예, 정조, 성명 및 사생활의 비밀을 포섭하는 권리를 의미한다. 이에 따르면 프라이버시권은 넓은 의미에서의 인격권의 일부가 되는 권리라고 하겠다.[8)]

마지막으로 사생활의 보호와 인격권의 프라이버시권을 도출하는 것이 아니라 개인의 정보에 대한 통제권을 독자적인 기본권으로 인정하는 견해이다. 즉, 개인정보 통제권을 근대와 현대의 입헌민주국가론의 중요한 기본권으로 인정하고, 개인정보는 절대적으로 보호되는 것이 아니기 때문에 개인정보 통제권은 국가나 사회적 필요에 따라서 재조정 될 수 있으므로 개인정보의 수집에 있어서 적법한 절차에 의하여 허용되고, 수집된 정보가 오・남용되지 않도록 통제하는 개인정보에 대한 통제권을 부여하는 것이 필요하다는 것이다. 이에 따르면 개인정보통제권은 자유로운 인격성의 보장을 위한 측면과 권력통제권인 정치적 권리로서의 성격을 동시에 갖는 것으로 이해할 수 있다.[9)]

생각하건대, 프라이버시권은 혼자 있을 권리(right to be let alone)와 사생활에 관한 의사결정의 자유(decisional privacy) 이외에도 정보 프라이버시의 개념이 있으므로, 헌법 제17조의 사생활의 비밀과 자유는 특히 정보 프라이버시와는 다른 의미를 갖는다고 할 것이다. 우리는 헌법 제 10조에서 일반적 인격권을 도출할 수 있기 때문에 정보 프라이버시라는 개

7) 김철수, 헌법학개론, 2007, 620면.
8) 조인현, "헌법상 개인정보보호에 관한 연구", 명지대학교 대학원 박사학위논문, 2009, 43면.
9) 김종철, "헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론", 선진상사법률연구, 제4호, 2001. 26-29면.

인의 사적 생활이라기보다는 사회 · 정치적 생활 영역에서 보이는 모습과 관련되기 때문에 헌법 제10조의 일반적 인격권으로 이해하는 것이 보다 타당하다고 할 것이다.[10]

(2) 판례의 태도

자기결정권에 대한 법적근거에 대해서 대법원은 국군보안사의 민간인 사찰에 대한 손해배상청구 사건에서 "헌법 제10조는 '모든 인간은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 가진다.'고 규정하고, 헌법 제17조는 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다."고 규정하고 있는 바, 이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적 권리는 물론 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 통제할 수 있는 적극적인 권리까지 보장하려는 데에 그 취지가 있는 것으로 해석된다."라고 설시하여, 헌법 10조의 인간의 존엄과 행복추구권 및 제17조의 사생활의 비밀과 자유에서 찾고 있다.[11]

한편, 헌법재판소는 주민등록법 제17조의8 등 위헌 사건[12]에서 "개인정보자기결정권의 헌법상 근거로는 헌법 제17조의 사생활의 비밀과 자유, 헌법 제10조 제1문의 인간의 존엄과 가치 및 행복추구권에 근거를 둔 일반적 인격권 또는 위 조문들과 동시에 우리 헌법의 자유민주적 기본질서 규정 또는 국민주권원리와 민주주의 원리 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 개인정보 자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 할 것이다."라고 함으로써 개인정보 자기결정권의 헌법적 근거를 헌법 제37조 제1항에서 규정한 헌법에 열거되지 아니한 권리로 보는 듯하였다. 그러나 이 결정이 난 후 얼마 안 되어 소위 교육정보시스템(NEIS)의 위헌사건[13]에서는 "인간의 존엄과 인간의 존엄과 가치, 행복추구권을 규정한 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하

10) 한수웅, 헌법학, 법문사, 2013, 541면.
11) 대법원 1998. 7. 24. 선고 96다42789 판결.
12) 헌재 2005. 5. 26. 선고 99헌마513 결정.
13) 헌재 2005. 7. 21. 선고 2003헌마282 결정.

여 보장되는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다"라고 판시함으로써 개인정보자기결정권의 근거를 헌법 제10조와 제17조에서 동시에 찾기도 하였다. 이러한 판례의 경향은 민사집행법 제70조 등 위헌확인 사건에서는 독자적인 기본권으로서 헌법에 명시되지 아니한 기본권으로 판단하다가[14], 최근에 와서는 접견 녹음파일 송부 요청 취소 사건[15]에서 "개인정보 자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리로서, 헌법 제10조 제1문에서 도출되는 일반적 인격권 및 헌법 제17조의 사생활의 비밀과 자유에 의하여 보장된다."고 판시하여, 개인정보자기결정권에 관한 헌법적 근거에 대해서 일관된 제시를 하고 있지 않은 것으로 보인다.

정리하건대, 개인정보자기결정권은 정보화 시대에서의 정보주체인 개인이 사회에 참여하는 한 모습으로서, 사회에 참여하는 자신에 대한 인격적인 캐릭터를 형성하는 자기의 정보에 대한 통제권이라고 이해하는 것이 바람직하다. 즉, 일반적 인격권에서 개인정보의 공개와 이용에 대하여 정보주체가 스스로 결정할 수 있는 개인정보결정권 핵심적 내용이 도출된다고 보아야 할 것이다.[16]

2. 외국의 법체계의 검토

가. EU의 개인정보 보호 법체계

EU는 1980년 「OECD 개인정보 보호에 관한 가이드라인」[17]을 제정하고 개인정보 보호와 EU 역내에서의 정보의 자유라는 상충될 수 있는 가치의 조화를 도모하기 위한 노력으로써, 1995년 「EU 개인정보보호지침(EU Directive 95/46/EC,)」[18]을 채택한 이래, 이를 기초로 2012년에는 종래의 규정을 현실적으로 구체화하여 정비하여 EU 협력차원에서 적용될 수 있

14) 헌재 2010. 5. 27. 선고 2008헌마663 결정.
15) 헌법 2012. 12. 27. 선고 2010헌마153 결정.
16) 이와 같은 견해는 한수웅, 앞의 책, 542면 참조.
17) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, O.E.C.D. Dos. C 58 final(September 23, 1980). 이에 관하여는 http://www.oecd.org/internet /ieconomy/ oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm 2013.
18) European Parliament and Council Directive 95/46/EC 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, 이에 관하여는 http://ec.europa.eu/justice/policies/privacy/ docs /95-46-ce/dir1995-46_part1_en. pdf, Official Journal L 281 of 23.11.1995.

는 일반법으로서 「EU 개인정보보호규정안(General Data Protection Regulation, 이하 'GDPR')」을 발표하였고, 2016년 4월 8일 의회의 승인을 통해 EU 회원국들은 2년 내에는 자국의 국내법으로 적용해야 하는 실정이다.[19]

EU의 개인정보보호지침은 회원국이 인간의 기본적 권리와 자유를 인정하고, 인간이면 누구나 개인정보에 관한 처리에 관한 프라이버시를 보호받아야 하며, 궁극적으로는 그 목적의 실현을 위해 EU 역내의 개인정보의 자유로운 흐름을 도모하고 있다. 개인정보 보호에 관한 의무를 지는 자(Controller)는 자연인과 법인, 공공기관 및 기타의 자로서, 공공기관과 민간기관 내지는 영리, 비영리 나아가 온오프라인의 구분이 없다. EU는 회원국 간에 기본적 인권과 자유, 프라이버시를 동등한 수준으로 보장하고, 역내에서의 개인정보 데이터와 통신설비, 그리고 서비스의 자유로운 이동을 보장하여 회원국 들 간에 적용되는 각종 규정과 지침에 있어서 조화를 추구하고 있다.

나. 영국의 개인정보 보호 법체계

성문헌법이 없는 영국은 헌법적 규범을 오랜 투쟁의 역사 속에서 관습헌법을 통해 형성해 온바, 1215년 대헌장(Magna Carta)에서 시작하여 1628년 권리청원(Petition of Right), 1689년 권리장전(Bill of Rights)의 제정을 거치면서 기본적 인권의 토대가 마련되었다. 경제협력기구인 OECD와 EU의 회원국인 영국은 프라이버시와 개인정보 보호에 대한 국제사회의 관심에 따라, 1984년 「정보보호법(Data Protection Act of 1984)」을 제정하였다.[20] 동법에서는 독립된 법정기구인 정보보호감독관을 개인정보보호 전담기구로 두고, 정보처리와 관련된 내용을 처리하는 공공기관과 사업자 등을 등록하는 공공등록부를 유지하고 관리하는 것에 대한 내용이나 정보보호감독권이 개인정보침해사건이나 개인정보 처리에 대한 불만사항을 접수하고, 구제해주는 기능 등을 하는 것이 주요 내용이 된 것으로 보인다.[21]

---

19) REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 이에 관하여는 http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf, Official Journal L 119 of 4.5.2016.

20) 이러한 배경은 1980년 9월 23일 경제협력기구(Organization for Economic Cooperation and Development; OECD) 이사회는 '프라이버시 보호와 개인정보의 국제유통에 관한 가이드라인'(Guidelines on the protection of Privacy and Transborder Flows of Personal Information)을 채택하였고, 이듬해 1981년 2월 28일 EU의 평의회가 '개인정보의 자동처리에 관한 개인의 보호를 위한 유럽협약'(Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)에 서명한 데에 있다. 이에 관해서는 이민영, "정보인권의 규범구체화", 아산재단 연구총서 제341집, 집문당, 2013, 151-153면 참조.

21) Data Protection Act 1998, Part III, VI, Function of Commissioner legislation.gov.uk <http://www.legislation.gov.uk/ukpga/1998/29/contents>

영국은 EU지침의 제정으로 국내법을 전면 수정하게 되면서 1998년「데이터보호법(The Data Protection Act1998)」을 통해 개인과 관련한 정보의 처리에 대해서 규율하고 있다. 동법은 EU 정보지침의 개인정보보호원칙을 담고 있으며 개인정보의 역외 이전에 관한 사항도 규정하고 있다. 정보보호법은 공공영역과 민간영역을 따로 구분하고 있지 않으면서 영국의 개인정보보호의 기본원칙을 포괄적으로 담고 있되, 특정 영역에 대한 부분은 특별법 또는 하위법령에 위임하고 있는바, 이는 정보보호법이 정보통신산업의 발달에 대응하기 위한 것으로써 데이터 컨트롤러 등을 공공기관과 민간기관으로 구분하지 않을 뿐 아니라 정보통신서비스 제공여부, 영리목적 유무에 따른 구분을 하지 않은 것으로 보인다.[22)]

영국의 개인정보 보호에 제도운영은 CCTV 사용과 사생활 보호에 관한 사례에서 들여다 볼 수 있다. 거리 곳곳에 설치된 CCTV로 유명한 영국은 범죄예방과 사생활 노출이라는 CCTV의 양면성에 대해서 고민해왔다. 영국정부는 데이터보호법에 따라 CCTV 실행규약(CCTV Code Practice)을, 2014년에는 '감시 카메라 사용규정(Surveillance Camera Code of Practice)'을 CCTV의 사용, 운영의 기본지침으로 발표한바, 이는 카메라의 사용에 관한 오남용을 다투는 분쟁에서 사용의 적법성을 판단할 수 있는 구체적인 원칙이 된다고 한다. 또한 기관이 보유한 모든 정보는 데이터보호법령에 의해 통제되는데 이에 따르면 영상자료를 포함한 모든 자료에 대해서 특정기관이 임의로 정보를 수집할 수 없고, 개인의 정보에 대한 권리는 어디까지나 정보주체에게 있다는 것이다. 영국 내 한 조사에 따르면 대다수 시민들이 CCTV 및 감시 카메라가 시민의 사생활을 침해하는 것이 아니라 일상을 보호하고 지원한다는 것에 확신을 갖고 있다는 것이다.[23)] 공공의 안녕, 질서 유지라는 목적 뒤에 사생활침해와 감시에의 노출에 관한 우려는 한 발 물러서야 할 문제인지는 여전히 석연치 않은 구석이 있다. 그러나 여기서 주목하고 싶은 것은 논란의 여지가 높은 감시시스템을 유지하고 있는 정부의 모습이다. 법적 강제력이 없는 세이프가드의 제정이 침해 자체를 방지하기 위해서라기보다 공동체의 신뢰를 주는데 목적이 있다는 점과, 그 운영이 자율적으로 이행될 수 있도록 유인하여 프라이버시를 침해할 수도 있는 기술을 오히려 공동체의 신뢰를 기반으로 활용되고 있음이 인상적이다.

22) 이민영 외, "해외 개인정보보호 집행체계 및 개인정보보호 주요 동향조사", 개인정보보호위원회, 2012, 79면 참조.
23) 관련기사: http://www.cctvnews.co.kr/news/articleView.html?idxno=17712(2016.10.22.방문)

다. 독일의 개인정보 보호 법체계

독일은 개인정보 보호에 관한 일반법으로서 1997년 「연방정보보호법(Bundes datens chutzgesetz)」을 제정하고, 개인정보 및 그 공개에 관한 다른 연방 법률이 있으면 그 법률이 우선한다는 점을 법 제1조 제3항에서 명시하고 있다. 독일은 독일기본법(Grundgesetz)의 제1조 인간존엄성 조항과 제2조 인격의 자유로운 발현 조항에서 개인정보보호의 헌법적 근거를 찾을 수 있다.[24] 다만, 기본법 제1조 및 제2조를 바로 프라이버시권이라고 적용하는 것은 무리가 있는데, 독일헌법재판소는 1993년 헌법소원 판결에서 '정보자기결정권'을 선언하고, 정보자기결정권은 인격권의 불가침성을 규정한 기본법 제1조 및 제2조에서 직접적으로 파생되는 권리임을 확인하였다.[25]

연방국가인 독일은 연방 차원에서 연방정보보호법을 채택하고 이외에도 각각의 주에서는 주법에 의해 주차원에서의 개인정보보호법을 마련하여 그에 기반하여 개인정보기구들을 설치하고 있다. 연방 데이터보호법은 연방의 공공기관의 정보처리를 규율할 뿐 아니라, 주법에 의해 개인정보 보호가 이루어지지 않는 영역과 주가 연방법을 적용하는 영역, 주가 행정적인 문제를 관여하지 않은 영역으로서 주의 공공기과에 처리되는 개인정보의 수집・처리・이용에도 적용이 된다. 또한 민간기관이 개인정보처리시스템에서 개인정보를 수집・처리・이용하기 위하여 개인정보를 수집하는 경우에도 동법이 적용이 되는 것으로 규정하고 있는바[26], 다른 연방법률에 규정이 없는 이상 연방 데이터보호법은 공공부문과 민간부분을 구분하고 있지 않는 것으로 보여진다.

라. 미국의 개인정보 보호 법체계

미국은 개인의 자유와 개성을 중시하는 전통으로 개인정보 보호에 있어서 일찍이 프라이버시의 개념을 새롭게 인식하고 프라이버시에 대한 침해를 보통법에서의 불법행위에 대한

24) Article 1(Human Dignity) (1) Human dignity is inviolable. To respect and protect it is the duty of all state authority. (2) The German People therefore acknowledge inviolable and inalienable human rights as the basis of every human community, of peace, and of justice in the world. (3) The following basic rights are binding on legislature, executive, and judiciary as directly valid law. 이에 대해서는 법제처 독일 헌법 영문본 참조
Article 2(Liberty) (1) Everyone has the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or morality. (2) Everyone has the right to life and to physical integrity. The freedom of the person is invi olable. Intrusion on these rights may only be made pursuant to a statute. 이에 대해서는

25) 명재진, "IT(정보기술) 기본권의 체계화에 관한 연구", 헌법논총 20집, 헌법재판소, 2009, 289-290면.

26) Artcle 1.(Purpose and scope)(2)This Act shall apply to the collection, processing and use of personal data by 1. public bodies of the Federation, 2. public bodies of the Länder in so far as data protection is not governed by Land legislation and in so far as they a) execute federal law or b) act as bodies of the judicature and are not dealing, 이에 대해서는 법제처 독일 연방데이터 보호법 영문본 참조.

손해배상책임을 인정해왔다. 미국의 프라이버시권은 보통법상의 권리로 인정되어왔기 때문에 권리침해가 발생하는 경우에는 법원에 소송을 제기하면 구제받을 수 있는 구조이다.

EU, 영국, 독일과 같은 대륙법계 국가와는 달리 미국은 연방차원에서 규율하는 개인정보 보호에 관한 법체계가 따로 없으며 개인정보 보호가 특별히 필요한 경우나 연방기관 등에 관한 규제가 필요한 경우에 개별법 제정을 통하여 개인정보를 보호하고 있다. 미국은 개인정보 보호에 있어서 프라이버시법(Privacy Act of 1974)의 이행에 대한 감독을 대통령 산하 기관이 일부를 관할할 뿐이고, 민간 영역에 있어서는 연방거래위원회(Federal Trade Commission, FTC)가 공정경쟁에 관한 집행권을 행사하고 있다.[27)]

미국이 포괄적인 개인정보보호법을 가지고 있지 않다는 점 및 접근방법에 있어서 부문별 접근방식을 취하는 것은 무엇보다 사적 자치의 원칙을 중시하고 자유로운 시장경제질서를 유도하는 경제적 관점에서 비롯한다.[28)]

개인정보 보호를 인권의 일부로 인정하여 국가가 적극 관여하는 유럽과 비교하여, 미국의 개인정보 보호에서 주목할 만 한 점은 개인정보 보호의 문제에 있어서 민간영역에 대한 규제방식으로 '자율규제(Self Regulation)'접근방식을 취한다는 것이다. 이러한 방식의 핵심은 원칙적으로 업계가 자율적으로 개인정보보호를 위한 제도를 만들 수 있도록 유도하는 것을 정부의 역할로 여긴다는 관점에 있다.

한편, 미국에서의 개인정보보호를 위한 지침으로서 '세이프하버 원칙(Safe Harbor Principles)은 1998년 10월 25일 발효된 EU지침이 당해 지침의 수준의 개인정보 보호 체계를 갖추지 못한 제3국으로의 개인정보 국외 이전을 엄격히 제한한 바, 이에 대응하여 자국의 민간부문, 즉 다국적 기업들이 세이프하버 원칙에 참가하고, 개인정보 보호 수준의 적정성을 유럽위원회(European Commission)가 확인하여 EU회원국과 개별적으로 별도의 협의를 하지 않을 수 있도록 하였다.

2000년 6월 미국 상무부(U.S. Department of Commerce)와 유럽위원회(European Commission)가 체결한 세이프 하버 협정은 2015년 10월 유럽사법재판소가 '세이프 하버(Safe Harbor)'를 전면 무효화하기 전까지 미국 IT 기업들이 세이프하버에 등록하여 준수하는 것으로 유럽의 개인정보 보호 기준을 충족한 것으로 인정받을 수 있었기 때문에 유럽 시

27) 이민영 외 앞의 논문 16~17면.
28) 이창범 · 윤주연, "각국의 개인정보피해구제제도 비교연구", 개인정보분쟁조정위원회 연구보고서, 2003, 160면.

장에 진출에의 발판을 활로가 되어왔던 것으로 평가된다.[29]

3. 시사점

앞에서 제한적으로나마 외국의 개인정보 보호 법제 현황에 대해서 검토하였다. 미국을 제외한 대부분의 국가들은 포괄적으로 적용할 수 있는 일반법으로서의 개인정보 보호 법률을 제정하여 시행하고 있는 것으로 이해될 수 있으며, 유럽의 경우에는 단일화된 개인정보보호기구를 통하여 개인보호의 실제적 기능 수행을 도모하고 있음을 볼 수 있었다. 우리나라의 경우 개인정보보호법을 제정하고 있으므로 외견상으로는 유럽과 비슷한 법제를 갖고 있는 것처럼 보이지만, 관련 법률이 혼재되어 완전히 단일법 체계로 정리된 것은 아닌 것으로 보인다. 또한, 실질적 법해석과 적용을 위해서는 EU가 종전의 지침에 나아가 실질적 Regulation을 마련한 것에 시사점을 둘 수 있을 것이다. 또한 GDPR이 시행되는 2018년 이후의 개인정보 보호는 유럽수준으로 끌어올리면서도, 구체적이면서도 개인정보를 안전하게 활용하는 시각에서의 실효적인 대비가 필요할 것이다. EU의 경우 1995년 지침과 2012 EU 개인정보보호지침에서는 그 각각이 개인정보 처리에 관한 개인의 보호와 관련된 규범이자, 개인정보의 자유로운 이동에 관한 규범이라는 점을 명시하고 있다. 특히 개인정보 처리에 대한 개인의 보호와 관련되었다는 이유로 개인정보의 자유로운 이동이 제한되어서는 안 된다는 점을 분명히 하고 있는데 이는 정보로서의 자유로운 유통을 전제하는 정보의 보호가 개인정보 보호의 목적임을 확고히 하는 것이다.

개인정보의 법제를 보완해나감에 있어서도 보호와 활용의 양면적 측면을 이해하는 접근이 필요하다. 우리나라의 경우, IT 기업들의 경쟁력이 사회전반에 미치는 영향력을 무시할 수 없는 사회적 배경을 감안할 때 미국의 자율규제를 통한 개인정보 보호 방식에 착안점을 둘 필요가 있다. 최근의 세이프 하버 협정 무효판결은 미국과 EU간의 개인정보 보호 정책을 둘러싸고, 글로벌 인터넷 경제 상황에서의 개인정보의 보호와 그 합리적인 이용을 가능하게 하는 개인정보처리 기준에 대한 합의의 문제였음을 보게 된다. 앞으로의 개인정보 보호는 일반적이고 실효적인 법적 규율아래 정보의 보호와 활용에 대한 조화가 균형있게 이루어지는 방향으로 나아가야 할 필요가 있다.

29) 사건개요 및 유럽사법재판소의 판결의 요지에 대한 자세한 내용은 최경진, “유럽사법재판소 세이프 하버 협정 무효 판결과 개인정보 보호 정책의 변화”, 언론중재위원회, 2016, 봄호 참조.

Ⅲ. 판례를 통해서 본 개인정보 자기결정권의 내용과 한계

1. 논의의 개요

정보통신기술의 급격한 발전으로 개인정보의 수집·과 이용을 둘러싸고 개인정보를 폭넓게 이용하고자 하는 정부기관과 기업, 그리고 개인의 프라이버시(privacy)를 가능한 두텁게 보호받고자 하는 국민 또는 시민과 소비자의 입장이 대비되고 있다. 이러한 양상은 비단 우리나라만의 현상 아니라, 정보사회의 개인정보와 관련한 논쟁에 있어서 국제사회의 흐름이다. 표현의 자유 혹은 인격권 중 어느 가치를 중시하는 하느냐에 따른 각 국의 역사적 배경에 따른 문제도 있겠으나, 자국의 다국적 기업의 활로를 유념한 국가차원의 의사 결정에 따라서도 프라이버시에 관한 입장은 달라질 수 있다.

개인정보의 처리는 공공영역과 민간영역 양쪽에서 상상을 초월하는 수준으로 확대되고 있다. 특히 민간영역에서 상업적인 목적에서 광범위하게 수집되는 개인정보는 최초 동의 이후에는 정보주체의 인식 없이 상업적으로 무분별하게 사용될 수 있는 여지가 높아 그에 대한 대비가 필요하다.

우리나라의 경우, IT 과학기술의 발전이 급속도로 이루어지고, 개인정보에 관한 특별한 의식이 없다가 점차 개인정보 유출사고가 대형화 되면서 2011년「개인정보보호법」이 제정·시행되어 개인정보보호 제도 및 개인정보처리를 위한 기준 등이 글로벌 수준으로 정비되는 역할을 하고 있다. 그러나 이러한 노력에도 불구하고, 계속되는 통신사, 소셜커머스 등의 개인정보 유출사고는 공공기관과 기업 등을 망라하여 사회전반적인 개인정보 보호 시스템에 대한 대책마련을 요구되게 되었다. 이러한 배경에서 범정부 차원의 '개인정보 정상화 대책'으로 마련된 피해구제제도인 법정손해배상제가「정보통신망법」을 비롯하여「개인정보보호법」과「신용정보의 이용 및 정보보호 등에 관한 법률」(이하 '신용정보법')에, 징벌적 손해배상제도가 올해 7월「정보통신망법」에 도입되면서 상기 모든 법에 도입 되었다. 법정손해배상제도는 기업 입장에서는 비용 부담으로 인한 기업 활동 위축의 우려가 있으나 피해자의 입장에서는 손해액의 입증책임이 전환되어 개인정보 유출 등으로 인한 피해보상이 되면서 그동안의 형식적으로 행해진 개인정보 수집과 관리 실태가 개선될 것이라는 기대를 주고 있다.

한편, 최근의 판례를 살펴보면 개인정보 자기결정권의 침해는 최초 수집시의 정보주체의 동의가 인정되는 개인정보의 범위 판단의 구체적 기준에 따라 개인정보보호법 위반 여부를

판단하고 있는바, 실제 소송에서 개인정보 침해주장이 받아들여지기는 쉽지 않은 것으로 보인다. 이러한 경향은 정보화 사회의 진전에 따라 강화되는 법제도의 이면에 개인정보침해를 둘러싼 법원의 개인정보 자기결정권 침해행위에 관한 법적판단의 정교화, 기업들의 개인정보보호 관련 법령에서 요구되는 수집에의 있어서의 동의절차 확보 및 기술적 관리적 조치를 다하거나, 혹은 그와 같은 법상의 개인정보의 보호조치를 다하지 않더라도 누출 등의 침해가 인정되지 않는 등으로[30] 사업자들의 책임 면제 가능성이 높아져, 실제 사건에서 개인정보 자기결정권이 침해된 경우라도 손해배상인정이 오히려 어려워질 수도 있음을 시사하기도 한다. 개인정보 보호 법제가 형식적인 차원의 권리보호에 머무르지 않기 위해서는 실체적인 권리침해에 대한 배상제도의 강구 이외에도 절차상 보장으로 개인정보의 수집 동의에서의 적법성 여부 심사에 머무를 것이 아니라 정보처리 전 과정에서 투명성이 확보가 필요하다. 이를 위해서 기술적 발전에 관하여 예측함으로써 정보주체의 존엄성과 자율을 보호할 수 있는 보호조치가 마련되어야 할 것이다.[31]

이하에서는 최근의 개인정보 자기결정권의 침해 소송 판결례를 검토한 뒤 현행 법제에서 개인정보 자기결정권의 보장의 한계를 진단해보고, 헌법상 보장되는 개인정보 자기결정권으로부터 도출되는 권리로서의 구체화의 필요성을 논의한다. 나아가 개인정보 자기결정권의 실질적 보호의 방안의 필요성을 제언하며 글을 마치기로 한다.

2. 개인정보 자기결정권 침해에 대한 최근 판례 검토

가. 불법행위법상 위법성 판단의 근거로서의 개인정보 자기결정권과 개인정보

개인정보 침해와 관련하여 표면적으로 드러나는 문제들은 대게는 대량으로 수집된 개인정보가 유출되거나, 개인정보의 강화에 따른 정보주체의 적법한 동의 여부, 수집한 정보에 대한 처리 및 관리의 문제들이다.[32] 여기서 소개할 판례는 개인정보 침해와 관련하여 본질적인 문제로서 '개인정보 자기결정권'에 관련하여 개인정보 자기 결정권이 보호대상으로 하

30) 대전지방법원 2015.3.18. 선고 2014 고정1905 판결.

31) Klaus Vogelgesang, Grundrecht auf informationelle Selbstbestimmung?, Nomos Verlag, 1987, S. 37f.(이상명, "개인정보자기결정권의 헌법적 근거에 관한 고찰", 공법연구 제36집 제3호, 2008, 2면 (재인용))

32) 유형별 소송사례에 관해서는 1. 관리소홀(리니지 사건, 국민은행 사건, LG전자 사건, 다음 사건) 2. 목적범위 외 사용(하나로 텔레콤 사건) 3. 해킹에 의한 유출(옥션 사건, 농협사건, SK 커뮤니케이션 사건, KT 사건 등) 4. 범죄목적을 위한 유출(GS 칼텍스 사건) 진대화, "개인정보침해에 대한 손해배상의 근거와 피해구제제도", Internet & Security Focus 2014. 7월호. 7면 표 참조.

고 있는 법익과 무엇을 기준으로 이의 침해를 판단하는지에 대한 시사점을 준다.

국회의원 A가 국정감사 자료를 수집하는 과정에서 취득한 초·중등학교 교원의 노동조합 가입현황 실명자료를 인터넷 홈페이지를 통하여 공개한 사안이다.[33] 대법원은 "개인정보 자기결정권의 보호대상이 되는 개인정보란 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함하는 것으로 판단하였다. 이미 공개된 정보라고 할지라도 사생활의 비밀과 자유에 의하여 보장되는 개인정보 자기결정권의 범위에 속한다는 것이다.

개인정보는 정보주체의 동의 없이 공개되어서는 안되는 것이 원칙이지만, 예외적으로 정보주체의 동의 없이 개인정보를 공개하는 것이 허용되기 위해서는 "개인정보를 공개함으로써 표현행위로써 보호받을 수 있는 법적 이익과 개인정보에 관한 인격권 보호로 얻을 수 있는 이익을 구체적으로 비교 형량하여, 어느 쪽 이익이 더 우월한 것으로 평가될 수 있는지에 따라 침해행위의 위법성 여부를 판단할 수 있다"고 하였다.

이때 충돌하는 이익의 비교형량에는 여러 가지가 함께 고려되는데, 개인이 공적 인물인지 여부, 개인정보 이용의 필요성, 개인정보의 공공성과 공익성, 개인정보 수집의 목적·절차·이용형태의 상당성, 개인정보 이용으로 침해되는 이익의 성질과 내용 등이다. 나아가 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체·사회적 지위·신념·신분 등과 같이 인격권의 주체성을 특징짓는 사항과 개인의 동일성을 식별할 수 있는 정보라는 요건을 갖추어야 한다고 하였다. 이 사건은 현행 개인정보보호법 시행 이전의 판결이기는 하나, 불법행위법상 위법성 판단의 근거로서의 개인정보자기결정권과 개인정보의 의미를 밝히고 있다. 현행법상 개인정보는 생존하는 개인정보 중에서 개인을 식별할 수 있는 정보라고 정의하지만, 그렇다면 어느 정도가 되어야 개인을 식별할 수 있는지 그 식별 주체는 누구인지, 결합이 용이하다고 보는 근거가 무엇인지에 따른 법해석의 문제가 남아 있다. 현행 개인정보보호법 제39조 제1항의 개인정보 침해로 인한 손해배상책임의 입증책임 전환이나 동법 제39조의 2 제1항의 법정손해배상의 청구 등은 이 사건 위법성을 판단한 불법행위법의 특칙규정이라고 할 것이지만, 불법행위법에서 침해 대상으로 삼는 개인정보는 개인정보보호법상의 그것 보다 '식별성 또는 식별가능성'을 보다 넓게 인정하는 것으로 이해할 수 있다.[34]

33) 대법원 2014. 7. 24. 선고 2012다49933 판결.
34) 김민호, "개인정보의 의미", 정보법 판례백선, 한국정보법학회, 2016, 598면 참조.

나. 공개된 개인정보를 정보주체의 동의 없이 수집 · 제공한 행위의 위법성 판단

공개된 개인정보를 정보주체의 별도의 동의 없이 영리목적으로 수집하여 제3자에게 제공한 행위에 대하여 현행법상 개인정보보호법 위반 여부를 판단한 대법원의 첫 판결[35]이 있었다. 신문사로부터 제공받은 법조인 데이터베이스와 자체적으로 인터넷 포털 등으로부터 수집한 국내 법과대학 교수들의 개인정보를 제공하는 종합법률정보 제공 사이트를 운영하는 사업자 A가 이 사이트에서 B의 사진, 성명, 성별, 출생연도, 직업, 직장, 학력, 경력 등의 개인정보를 유료로 제공한 행위에 대하여 B에 대한 개인정보결정권침해 및 개인정보 자기결정권 침해를 다툰 사건이다.

대법원은 이 사건에서도 공개된 개인정보 자기결정권 침해여부를 판단함에 있어서 앞에 소개한 대법원 2014. 7. 24. 선고 2012다49933 판결과 동일하게 "정보주체가 공적인물인지, 개인정보의 공공성과 공익성, 원래 공개한 정보의 대상범위, 개인정보 처리의 목적 · 절차 · 이용형태의 상당성과 필요성, 개인정보 처리로 인하여 침해될 수 있는 이익과 성질과 내용 등을 종합적으로 고려하여 개인정보에 관한 인격권 보호에 의하여 얻을 수 있는 이익과 정보처리자의 알권리와 이를 기반으로 한 정보수용자의 알권리 및 표현의 자유, 정보처리자의 영업의 자유, 사회 전체의 경제적 효율성 등의 가치를 구체적으로 비교 형량하여 어느 쪽 이익을 우월한 것으로 평가할 수 있는지에 따라 행위의 최종적인 위법성 여부를 판단하여야 한다"며 개인정보 자기결정권의 침해의 판단기준을 제시하였다. 이 사건에서 대법원은 정보처리자와 이를 기반한 정보수용자의 알권리 및 표현의 자유, 정보처리자의 영업의 자유, 사회 전체의 경제적 효율성 등이 이 사건 정보처리를 막음으로써 얻을 수 있는 정보주체의 인격적 법익에 비하여 우월하다고 판단하여 A의 행위를 위법한 행위로 하지 않았다.

한편, 개인정보보호법의 위반여부에 대해서는 개인정보보호법상의 개인정보처리자의 개인정보 수집 · 이용(제15조)과 제3자 제공(제17조)의 정보주체의 동의 여부의 판단에 있어서는 정보주체가 직접 또는 제3자를 통하여 이미 공개한 개인정보는 그 공개 당시 정보주체가 자신의 개인정보에 대한 수집이나 제3자 제공 등의 처리에 대하여 일정한 범위 내에서 동의를 한 것으로 보았고, 정보주체가 동의한 범위 내인지에 대해서는 공개된 개인정보의 성격, 공개목적, 공개된 형태와 대상범위, 그로부터 추단되는 정보주체의 공개의도 내지는 목적, 정보처리자의 정보제공 등 처리의 형태와 그 정보제공으로 인하여 공개 대상범위를 원래

35) 대법원 2016. 8.17. 선고 2014다235080 판결.

의 것과 비교하는 등을 개인정보보호법 위반의 판단기준으로 제시하였다.

이 사건에서 법원은 공개된 개인정보 자기결정권의 침해여부에 있어서 판단기준을 보다 구체적으로 제시하여, 침해행위의 위법성을 섬세하게 판단하였고 개인정보보호법 위반여부에 판단하는 유효한 동의 범위에 있어서도 비교적 많은 사정 등을 고려하여 판단하였다. 다만, 본 판례의 사안은 공개된 정보가 민감정보가 아닌 직업적 정보인 점, 원래 제공 동의한 정보와 범위에서 특별한 차이가 없다는 점에서 유사한 사안에 동일한 결론을 적용하는 데에는 신중하여야 할 것으로 보인다.

다. 수사시관 등 제3자에게 제공한 '통신자료제공'과 관련한 판례

최근 포털사와 이동통신사에 제공된 통신자료가 수사기관에의 제공이 사회적으로 이슈가 되는 가운데, 정보주체와 수사기관, 전기통신사업자간의 개인정보 유통에 관한 자기 통제의 문제가 전면적으로 드러난 사건을 이하 소개하고자 한다.

먼저, 전기통신사업법상 부가통신 사업자이자 정보통신망법상의 정보통신서비스 제공자인 포털, 피고 다음커뮤니케이션(2014.10. 경 주식회사 카카오와 합병 후 현재는 '카카오'로 사명변경 함)에 대하여 피고가 운영하는 서비스인 '다음'에 가입한 회원인 원고들이 피고가 전기통신사업법에 의한 통신자료 제공 요청 내지 형사소송법에 의한 이메일에 대한 압수수색영장의 집행에 따라 수사기관 등 제3자에 제공한 현황을 요구하였으나, 피고가 요청을 거절하자 본 건 소송[36]에 이른 사안이다. 쟁점은 피고가 수집・보유하고 있는 원고들의 개인정보(이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디 가입일 또는 해지일, 이메일 주소)를 전기통신사업법에 의한 통신자료제공요청에 따라 제3자에게 제공한 현황 내지 형사소송법에 의한 이메일에 대한 압수수색연장의 집행에 따라 제3자에게 제공한 현황의 공개의무가 있는지 여부와 공개거절로 인한 손해배상 책임여부였다.

이 사건에서 대법원은 이메일 등에 대한 압수수색을 집행하면 수사기관이 이용자에게 이 사실을 통지하도록 통신비밀보호법에 규정되어 있기 때문에 인터넷 포털사이트와 같은 전기통신사업자는 이메일 압수수색 사항을 알려달라는 이용자의 요청을 들어줄 의무가 없다고 판시하고, 이에 이메일 압수수색 사항을 알려달라는 원고들의 요청을 거절한 것은 정당하여 피고들에게 위자료를 청구할 만큼의 정신적 손해가 발생했다고 볼 수 없다고 하였다.

36) 대법원 2015.2.12. 선고 2011다76617판결.

대법원은 손해배상책임으로서의 위자료 인정에 관해서 “피고의 수사기관 등에의 정보제공 사항 공개 거부로 인하여, 피고가 개인정보를 제3자에게 제공한 사실이 있는지를 확인할 수 없음으로 원고에게 발생한 막연한 ‘불안감’이나 ‘불쾌감’이 원고의 수인한도를 초과하여 금전으로 위자할 만한 구체적인 정신적 손해가 발생하였다고는 단정하기 어렵다”는 이유로 원고들의 위자료 청구를 인정하지 않았다.

본 판결은 개인정보의 유출로 인한 어떠한 구체적인 손해를 판단하지 않고, 소액의 위자료로 인정하는 형태의 과거의 판례의 경향에 비교했을 때 원고들이 주장하는 정신적 손해가 피고의 정보공개거부로 인한 합당한 수준의 것인지에 대해 판단함으로써, 위자료 인정판단에 대해서 나름의 근거를 제시했다는 점에서 의미가 있다. 다만, 그 동안의 정보 유출로 인한 개인정보자기결정권 침해를 인정하여 정신적 손해를 인정해온 것과의 어떤 차이점이 있었는지 살펴보면, 법원은 개인정보를 제공한 제3자의 대상이 국가기관이라는 점에서 판단을 달리한 것은 아닌가 하는 미심쩍은 생각을 지우기 어렵다.[37] 대법원이 위자료를 인정하지 않은 이유가 원용된 원심 고등법원의 판결과 같이 개인정보 제공 대상이 수사기관이거나 법원이라서 정보를 악용할 위험이 적다는 점에서 비롯한 것이라면, 그것은 국가기관으로서의 판단에 치우친 판단이 아닐까 한다. 일반 국민들은 어쩌면 국가권력에 대한 정보 유출에 오히려 신변에의 불안을 느낄 수 있는데도[38], 대법원은 정보주체의 신원정보 등이 제3자인 국가에게 제공되었는지에 대한 정보주체의 알권리를 단지, “막연한 불안감이나 불쾌감”이라고 표현하였다. 정보주체가 통신자료의 제공사실을 알고자 하는 것이야 말로 헌법정신이 인정하는 개인정보자기결정권의 내용은 아닌 것일까?[39]

근래 대법원은 인터넷 이용자의 개인정보 제공과 관련하여 전기통신사업자에게 구 전기통신사업법 제54조 제3항, 제4항[40]의 수사기관의 통신자료 제공요청에 대한 실질적 심사의 무가 있지 아니하고 따라서 그러한 의무위반에 대한 책임을 물을 수 없다고 판결한 바 있다.[41] 원심법원이 전기통신사업자는 이용자의 개인정보에 대한 실질적 보호에 필요한 역량을

37) 이희창, “[판결비평] 포털사의 네티즌 신상정보 수사기관 제공 미통지 손배불인정 판결”, 참여연대, 2015.5.21. http://www.peoplepower21.org/Judiciary/1333687 사이트 참조.

38) [칼럼] 포털사의 네티즌 신원정보 수사기관 제공 미통지 손배불인정 판결, 오마이 뉴스, 15.05.21. http://www.ohmynews.com/NWS_Web/View/at_pg.aspx?CNTN_CD=A0002110646 사이트 참조.

39) 최창수, “수사・정보기관의 통신이용 정보수집권에 관한 미국의 입법례와 그 함의”, 정보법학 제20권 제1호, 121면.

40) 현재는 전기통신사업법 제83조 제3항, 제4항

41) 대법원 2016.3.10. 선고 2012다105482 판결. 전기통신사업자피고가 운영하는 포털사이트의 카페 서비스의 회원인 원고가 2010년 당시 벤쿠버 동계올림픽 선수단의 귀국 당시 소외 1 장관이 금메달리스트인 소외 2 선수를 환영하며 어깨를 두드리자 소외2 선수가 이를 피하는 것 같은 장면을 편집한 사진을 인터넷 카페 게시판에 올리자, 소외 1장관이 원고들을 명예훼손을 이유로 고소하면서 수사기관

갖추어야 하고, 구체적으로는 침해되는 법익상호간의 이익 형량을 통한 위법상의 정도와 중대성과 긴급성 등을 종합적으로 고려하여 어느 정도까지 제공할 것인지에 관한 세부적 기준을 마련하는 등으로 이용자의 개인정보를 보호하기 위한 충분한 조치를 취할 의무가 있다고 판단한 것에 반해, 이 사건 대법원 판결은 수사기관의 요구에 따른 자료제공에 전기통신사업자에게 가능의 내부 판단기준을 두는 등의 조치 의무를 부과함 없이 일반 국민의 개인정보를 수사시관에 제공하게 둠으로써, 피고인 포털 사업자의 개인정보 제공 책임을 면제하는 데 비중을 둔 것은 아닌가 하다. 물론 사기업에 불과한 전기통신사업자에게 실질적 심사의무를 두는 것은 바람직하지 않은 면이 있다. 그러나, 다양한 인터넷매체서비스가 일상생활에 크게 자리매김하고 있는 현실에서 포털사업자가 수사기관 등에 법적 부담 없이 이용자의 정보를 제공하도록 하는 본 판결 결론은 최근 개인정보 보호와 관련한 국내 인터넷매체 서비스 기업의 글로벌 경쟁력에 있어서도 그리 긍정적인 방향은 아닐 것으로 보인다.[42] 나아가 이 사건 대법원은 통신자료는 이의 제공으로 범죄에 대한 신속한 대처 등 중요한 공익을 달성할 수 있음에 비하여, 통신자료가 제공됨으로써 제한되는 사익은 해당 이용자의 인적 사항에 한정된다고 판시하였다. 개인의 인적사항은 헌법상 인정되는 개인정보자기결정권의 구체적 대상이 됨에도 불구하고, 본 판결에서는 일반 국민의 개인정보에 대한 보호문제가 수사관행의 효율성을 넘어 간편성보다 소홀히 여기진 것은 아닌가 하다.

3. 개인정보 자기결정권의 한계

가. 개인정보 자기결정권의 개념과 보호범위

프라이버시권은 Warren과 Brandeis에 정의에 의해 “홀로 있을 수 있는 개인의 일반적인 권리(the more general right of individual to be let alone)”라는 소극적 의미로 시작되었지만, 오늘날 정보사회에 들어서서는 정보통신기술발달로 개인의 정보가 생각할 수 없을 만큼의 데이터로 축적되고 처리되어지는 가능성 때문에 개인의 자기정보 내지는 개인정보에 관한 통제권이라는 적극적인 지위에 이르게 되었다.[43]

개인에 관한 정보는 이렇게 확대되어 스스로의 정보의 유통을 통제하고, 언제 어떻게 공개할 것인지를 정보 주체가 스스로 정하는 권리로 정의되면서 자기정보 관리 통제권, 자기정보

이 통신자료 제공요청서만으로 피고에게 원고들의 인적사항을 요구한 사건이다.

42)

43) Alan F. Westin, Privacy and Freedom, Atheneum, 1967, pp.7-8.(이상명, 앞의 논문 재인용)

통제권, 개인정보자기 결정권 등의 용어로 불리어진다. 개인정보 자기결정권에 대한 배경이나 법적 근거에 대하여 많은 논의들이 있지만, 헌법재판소는 개인정보결정권을 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것이지를 그 정보주체가 스스로 결정할 수 있는 권리"라고 판시하였고, 개인정보자기결정권은 헌법 제10조에서 규정하는 인간의 존엄과 가치, 행복추구권, 제17조에서 규정하는 사생활의 비밀과 자유로부터 발생하는 인격권에서 비롯된다고 할 것이다.[44] 하지만, 프라이버시 혹은 헌법 제17조의 '사생활의 비밀과 자유'가 개인정보 자기결정권에 관한 권리와 반드시 일치하는 것은 아니라고 할 수 있다. 왜냐하면 개인정보 자기결정권이 헌법 제17조로부터 도출되는 개념이더라도 그 핵심은 자기의 정보를 국가나 타인으로부터의 무분별한 수집과 이용으로부터 통제하는 것이므로 개인의 내밀한 사적 영역을 보호하기 위한 것에 목적이 있는 사생활권과는 보호대상과 내용에 있어서 분명 차이가 있기 때문이다.

개인정보 자기결정권은 타인에 공개하기 꺼려지는 일정한 영역의 사적인 개인정보에 대하여 크게 ① 개인정보의 수집・취득, ②개인정보의 보유・이용, ③개인정보의 열람・제공의 과정에서 정보주체의 개인정보에 대한 통제권에 대한 보장을 요구한다고 하겠다. 나아가 개인정보자기결정권의 헌법상 확인되는 기본권으로 인정되기 위해서는, 이러한 기본권이 사인에 의하여 정당한 이유 없이 침해되지 않도록 하고, 침해가 발생할 때에는 실질적인 구제가 실현되는 것을 의미한다.

한편, 개인정보결정권은 개인정보 보호에 있어서 중요한 위치에는 있으나, 실제 사건에서는 개인정보 수집과 활용에 있어서 정보 주체의 동의 요건이 결여되거나 열람 및 정정 청구권이 침해되거나, 개인정보의 안전 관리 미흡에 따라 개인정보가 유출된 경우에 절차적・형식적 측면의 개인정보자기결정권이 침해된 것일 뿐, 그것만으로는 정보 주체의 실체적인 권리가 침해된 것이 아니라 위험규제 측면에서의 개인정보자기결정권이 침해되었다고 보는 것으로 이해되는 측면이 있다. 이에 사실상 개인정보 자기결정권을 실체적 권리로 보고 이를 통해 정보 주체의 개인정보 침해로 인한 손해를 전보하려는 것은 사실상 상당한 무리가 있다고 할 것이다.[45] 이러한 한계를 보완하고자 하는 맥락에서 개별법에서 개인정보의 보호법익과, 보호 대상 및 범위를 범주화하고, 개인에 관한 어떤 정보를 보호대상으로 할지부터 분명

44) 헌법재판소는 개인정보결정권의 헌법상 근거와 내용 등에 관하여 구체적으로 설명하고 있지는 않지만, 이 기본권은 인간의 존엄성을 존중하는 헌법정신으로부터 나오는 것은 분명하다.
45) 김진환, "개인정보 보호의 규범적 의의와 한계", 저스티스, 2014. 55-57면.

히 하여 개인정보의 침해에 관한 논의를 개진해 나가는 것이 바람직할 것이다.[46]

즉, 헌법상 인정되는 개인정보 자기결정권이 권리로 인정되는 것은 그 권리 침해에 대하여 법원에 소송으로 제기할 수 있고, 침해를 예방하거나 침해를 당했을 때에 구제를 요구할 수 있어야하는 것을 의미한다. 따라서 개인정보자기결정권의 실현을 위해 익명권, 개인정보 수집제한청구권, 정보처리금지청구권, 정보열람청구권, 정보정정청구권, 정보차단청구권, 정보분리청구권, 정보삭제청구권 등의 권리로의 구체화를 통해 보호법익에 따른 구제책 등을 보호법에서 마련하는 것이 필요하다.[47]

4. 법정손해배상책임 인정 입법개정에 관한 검토

2014년 카드사 개인정보 유출 사고 이후 우리 법제에서는 개인정보 보호의 법제 마련의 심각성을 깨닫고 보완책으로서 개인정보보호법, 정보통신망법, 신용정보법은 손해배상 제도를 개선하는 입법을 마련해온 바, 그 대표적인 내용이 법정 손해배상 제도와 징벌적 손해배상 제도, 손해액 입증의 경감 제도 등이 대표적 예이다. [48]먼저, 과거 개인정보 유출시 기술적・관리적 보호조치와 유출 사고와의 인과관계를 입증하여야만 1억원 이하의 과징금을 부과하도록 하는 규정이 인과관계 입증이 쉽지 않은 점, 제재수준이 약하다는 지적을 수렴해 개인정보 유출시 기술적・관리적 보호조치와 유출 사고와의 인과관계를 입증하지 않더라도 관련 매출액의 3% 이내의 과징금을 부과하도록 하며, 개인정보 유출 사고 발생한 경우에도 이용자가 손해배상을 청구하려면 직접 손해 규모를 증명해야 하는 데 따른 이용자 권리 구제의 부재를 해결하기 위해 손해에 대한 구체적인 입증 없이도 최대 300만원의 손해 배상액을

46) 이민영, 앞의 책, 245-248면.

47) 1. **인격권**: 정보주체가 국가·기업·사인 등의 제3자와 온라인교섭 또는 거래를 할 때 불필요하게 자신의 신원을 밝히지 않고 거래를 할 수 있는 권리로서 개인의 이름이나 개인을 식별할 수 있는 정보를 부분 또는 전부를 익명화 또는 가명화할 수 있다. 2. **수집제한청구권**: 정당한 수집목적을 위하여, 필요한 범위 내에서, 공정하고 합리적인 방식으로, 정보주체의 분명한 인식 또는 동의하에 수집되어야 하고, 일단 정보가 수집되면 사후에 이용, 유통, 통합처리 등에 대한 통제는 사실상 힘들어진다는 점에서 수집제한청구권의 중요성은 날로 커진다고 할 것이다. 3. **정보처리금지청구권**: 본적인 정보처리 원칙이 충족되지 않는 경우에는 개인정보의 이용·제공 등의 정보처리를 금지하도록 요구할 수 있는 권리를 말하며, 여기에는 이용제한요구권, 시스템공개요구권이 포함된다. 4. **정보열람청구권**: 타인에 의하여 처리되고 있는 개인정보의 내용에 대하여 정보주체가 자신에 관한 정보의 열람을 청구할 수 있는 권리이다(현행 개인정보보호법 제12조). 5. **정보정정청구권**: 정보주체가 자신에 관한 정보를 열람한 결과 정보내용이 부정확하거나 불완전한 것일 경우 이에 대한 정정을 요구할 수 있는 권리이며, 정보주체의 정정요구가 있을 경우 정보보유기관은 잘못된 부분을 정정하고 정보주체에게 그 사실을 통보해야 한다(개인정보보호법 제14조). 6. **정보차단청구권**: 개인정보 제공자가 정보보유기관에 대해 자신의 정보에 대한 일반인이나 그 밖에 권한 없는 자의 불법적인 접근을 지속적으로 막아줄 것을 요구할 수 있는 권리이다. 개인정보 자기결정권의 구체적 권리에 대해서는 이상명, 앞의 논문, 228~233면 참조.

48) 정보통신망법의 주요개정안에 대한 구체적인 내용은 : http://www.lawnb.com/lawinfo/contents_view.asp?CID=AFB7D5E53E544C7696E941 F9708439ED&BizLetr=Y 사이트 참조.

지급하는 법정 손해배상제도를 도입한 것이다.(32조의 2)[49] 도입된 법정손해배상은 개인정보 침해로 인한 입증 어려움이 있었던 이용자 구제에 도움이 될 것으로 보이지만, 다소 급박하게 추진된 사정으로 법정손해배상액의 하한 설정이 없는 점과, 증명책임의 전화에 있어서 해석에 따라 법 제32조의 2의 제1항 단서와 본문에서 본문에서는 "다음 각 호의 모두에 해당하는 경우에는 … 청구할 수 있다"고 규정하면서 제1호에서는 "정보통신서비스 제공자등이 고의 또는 과실로 이장의 규정을 위반한 경우"라고 하여, 마치 각 호의 요건사실에 대하여는 정보주체에게 여전히 주장・입증책임을 다 해야 하는 것으로 읽힐 수 있어 추후 법 해석에 문제가 있을 수 있어 관련하여 해석상 논의가 있다.[50] 도입된 법정손해배상제도의 취지가 정보주체의 권리구제에의 기여와 합리적이고 실질적인 개인정보 보호에 있음을 생각할 때에 과도한 손해배상으로 인하여 국가나 기업, 그리고 기업의 활동에 지장을 주지 않으면서도 안정적으로 정착되도록 개선해 나가야 할 것이다.

마찬가지로, 가장 최근에 정보통신망법 제32조 제2항에 신설되어 도입된 징벌적 손해배상은 피해자의 손해를 보상하는 것을 목적으로 하는 것이 아니라 가해자의 악의적 또는 의도적 고의에 대하여 징벌을 함으로써 가해자 및 제3자가 동일하거나 유사한 행위를 반복하지 않도록 예방하는 것을 목적으로 한다. 징벌적 손해배상은 모든 위법 행위에 대하여 징벌적 손해배상이 적용되는 것은 아니고, 고의 또는 중대한 과실로 인하여 개인정보가 분실・도난・유출・위조・변조 또는 훼손된 경우로서 이용자에게 손해가 발생한 때에만 청구할 수 있다. 이번에 정보통신망법에 도입된 징벌 손해배상제도는 다른 피해자 구제제도와 함께 피해자 구제를 위한 범정부적으로 마련된 제도이다.

그러나 근본적으로 동법 제1항에서의 입증책임 전환이 이루어지지 않아, 실제로는 여전히 피해자가 위반행위를 입증해야한다는 점에서 실제 소송에서 피해자의 입증 부담은 매우 큰 짐으로 남아 있는 것으로 보인다. 제도가 시행된 지는 얼마 되지 않은 상황이므로 향후의 추이를 살펴보아 제32조 제1항의 실체적・절차적 입증 문제를 해결하는 것이 필요하다.

49) 방송통신위원회, "개인정보 유출시 처벌 및 손해배상 대폭 강화" 2014.5.8.자 보도자료 참조.

50) 최경진, "새로 도입된 법정손해배상에 관하 비판적 검토 ; 개인정보보호 관련법에서의 법정손해배상을 중심으로", 성균관법학, 제27권 제호, 2015. 200면은 향후 개정을 통하여 정보통신망법 제32조의2 제1항 본문에 따르는 동항 제1호의 "고의 또는 과실"과 신용정보법 제43조의2 제1항 본문에 따르는 동항 제1호의 "고의 또는 과실"을 각각 삭제할 필요가 있다고 한다. 유사한 의견으로 고형석, "개인정보침해와 손해배상책임의 원칙", 「저스티스」, 통권 제145호.2014. 69면. 정보통신망법 제32조의2 제1항 제1호에 규정된 "고의 또는 과실로"라는 문구를 삭제할 필요가 있다는 견해가 있다.

Ⅳ. 나가며

정보기술발전이 근간이 되어 급변하는 정보화 사회에서는 정보를 통제하는 것은 그 자체로 권력일 수 있기에 개인정보를 둘러싼 정보주체의 인격권, 자유의 실현의 문제와 이의 수집・처리를 통한 정부와 사업자들 간의 이해충돌로 인한 긴장 관계는 갈수록 첨예해질 수밖에 없다. 다만, 정보 주체에게 정보에 대한 통제권이 주어지는 경우에도 개인정보는 이를 침해하는 행위로부터 보호되어야 한다고 할 것이지 그 이용을 일률적으로 금지한다거나 개인정보 그 자체로 보호되어야만 한다는 주장은 합리적이지 않다. 개인정보를 둘러싼 정보주체와 개인정보를 활용하고자 하는 자들의 긴장관계 속에서 개인정보의 보호와 이용이 균형 속에서 조화를 이루는 보완책이 필요하다.

그 동안 우리사회는 수많은 개인정보 유출 사건들을 경험하고, 그로 인한 경각심으로 개인정보 보호를 위한 법정책적 변화를 도모하여, 정보주체의 개인정보자기결정권의 존중을 위해 나름의 시도를 해왔다. 그럼에도 불구하고 수많은 정보유출 사건들로 인한 피해자에 대한 손해배상은 손해 입증의 어려움으로 소액의 위자료에 그쳐왔다. 이것은 개인정보자기결정권의 보호 법익이 권리로서 명확히 구체화되지 못한 상태에서 개인정보와 관련한 개별법에서의 규정을 들어 실제 사건에 해석 적용하는 것에 한계가 있었던 점에 기인한다. 1980년 OECD 가이드라인과 1995년 EU의 개인정보 보호지침 등 선진사회의 개인정보 보호 법제가 “개인정보의 보호와 정보의 자유”라는 두 가치의 조화를 표제에 내세우는 것과 비교했을 때, 개인정보보호와 관련한 법제가 정보의 보호 측면에서만 규정되어 왔음은 IT 산업의 급속한 발달과 함께 찾아온 정보화 사회에서 개인정보자기결정권의 내용이 무엇인지에 대한 사회적합의가 이루어지지 않았기 때문이라고도 할 수 있다.[51] 정보화 사회에서의 개인정보자기결정권의 내용은 정보주체가 정보처리여부를 통제할 수 있는 권리로 접근하기 보다는 정보의 유통에 대해서 통제하고 참여할 수 있는 권리로 보는 것이 타당하다. 아니면, 개인정보보호 법제하에서 개인정보자기결정권을 강조하면서도 실제 정보주체에게 권리행사로써 부여하는 것이 개인정보의 처리에 관한 동의 여부, 동의 범위에 대한 선택권을 개인정보보호법에서 명시하면서도 실제 일상생활에서 개인정보 수집과 처리에 관한 무의식적인 동의를 유효하게 볼 수 있는지를 생각해보면, 한편으로 개인정보보호 법제는 형식적이고 절차적인 위험

51) 문재완, “개인정보보호 법제의 헌법적 고찰”, 세계헌법연구 제19권 제2호, 2013, 288면.

규제로서의 역할로서의 기능이 적지 않다는 생각이 든다. 52)

현행법에서 명시한 개인정보보호법이 보호하고자 하는 것은 개인정보가 실제 오남용 되어 침해되는 사생활의 비밀과 자유와 인격권에 있다. 따라서 최근에 도입된 법정손해배상제도 및 징벌적손해배상제도 등 강화된 개인정보보호 법체계의 취지와 정보주체에게 개인정보 수집・처리 등에 대한 동의권한을 형식적으로 두는 것만으로는 개인정보자기결정권이라는 보호법익을 충분히 보호하면서, ICT 기술발달로 가속화 되는 정보화 사회에서 사인간의 개인정보의 유통측면에서 효율적인 정보의 유통이라는 두 마리 토끼를 잡기는 쉽지 않을 것으로 보인다. 이는 기업 또는 사적이익을 추구하는 사업자를 실제 법적 장치가 쉽사리 제한할 수 없는 사회적 환경도 한 몫 한다. 그렇다면, 국가는 헌법상의 기본권인 개인정보 자기결정권에 대해서 완전하고 포괄적인 보장을 할 수 없는 자기 한계에서 그쳐야 하는 것일까? 정보사회 발전은 국경을 허물고 시공간을 초월한 사회로의 전환을 가져왔지만, 오히려 변화된 정보사회에서 국가는 자국민의 정보에 대한 권리를 보호하여 정보에 대한 불평등을 해소하고 개인의 사생활을 두텁게 보호하여야 한다. 이의 해결을 위해 국가가 기본적으로 사회의 자율성을 존중하되, 민간에 의한 자율적 과제이행이 가능하도록 틀을 보장하는 방식으로의 보장국가로서의 기능에서 찾고자 한다.53) 개인정보에 대한 정보주체의 권리를 그 동안 마련된 법제 속에서 보호법익을 구체화하고 실체적 권리로서 마련하는 등 관련된 법적 구조를 사전에 설정하여 그 안에서 개인의 정보에 대한 권리에 근거하여 자유로운 활동을 보장하여만 한다. 즉, 정보와 관련한 통제는 ICT 산업 발전을 저해하는 것이 아닌 인간 우호적이고 정보주체가 통제가능한 정보망 구축이 궁극적이라는 공감대를 형성해야한다.54) 이를 위해 국가는 민간영역에서 특히 사인간의 규범구조를 마련하고, 전문가 단체와 경제단체, 기타 관련영역에서의 조직체를 통해서 그들 스스로가 개인정보보호에 관한 자율적인 규범을 정하도록 하여, 민간에서 자율적으로 합의된 기준을 마련하고, 인센티브를 주는 유인장치를 통해서 개인정보 유통의 투명성을 유인할 수 있을 것으로 기대해본다.

52) 개인정보보호 법제를 프라이버시 침해 위험을 구제하는 위험규제로 보는 견해에 관해서는 박경신, "개인정보의 정의와 위치정보보호법의 개선 방안", 법학연구 통권 제37집, 2013.198면.
53) 홍석한, "새로운 국가역할 모델로서 보장국가론의 의미와 가능성", 공법학연구 제17권 제2호, 2016, 76면.
54) 김일환・홍석한, "개인정보 자율규제영역에서 보장국가로서 국가의 역할에 관한 연구", 헌법학연구 제14권 제4호, 2008, 142면.

참고문헌

- 김철수, 헌법학개론(제19판), 박영사
- 한수웅, 헌법학, 법문사, 2013
- 김민호, “개인정보의 의미”, 정보법 판례백선, 한국정보법학회, 2016
- 이민영, “정보인권의 규범구체화”, 아산재단 연구총서 제341집, 집문당, 2013
- 정보인권 보고서, 국가인권위원회, 2015
- “개인정보 유출시 처벌 및 손해배상 대폭 강화” 방송통신위원회, 2014.5.8.자. 보도자료
- 이인호, “정보인권 논의가 시사하는 헌법학적 프레임: 디지털시대에 있어서 정보를 둘러싼 권력과 자유의 긴장과 조화”, 법학연구 제3호, 가톨릭대학교 법학연구소, 2008
- 김민섭, “개인정보의 보호와 이용의 조화에 관한 법제적 연구”, 숭실대학교 대학원 박사학위논문, 2015
- 조인현, “헌법상 개인정보보호에 관한 연구”, 명지대학교 대학원 박사학위논문, 2009
- 김종철, “헌법적 기본권으로서의 개인정보통제권의 재구성을 위한 시론”, 선진상사법률연구, 제4호, 2001
- 명재진, “IT(정보기술) 기본권의 체계화에 관한 연구”, 헌법논총 20집, 헌법재판소, 2009
- 이민영 외, “해외 개인정보보호 집행체계 및 개인정보보호 주요 동향조사”, 개인정보보호위원회, 2012
- 이창범 · 윤주연, “각국의 개인정보피해구제제도 비교연구”, 개인정보분쟁조정위원회 연구보고서, 2003
- 최경진, “유럽사법재판소 세이프 하버 협정 무효 판결과 개인정보보호 정책의 변화”, 언론중재위원회, 2016 봄호
- 문재완, “개인정보보호 법제의 헌법적 고찰”, 세계헌법연구 제19권 제2호, 2013
- 박경신, “개인정보의 정의와 위치정보보호법의 개선 방안”, 법학연구 통권 제37집, 2013
- 홍석한, “새로운 국가역할 모델로서 보장국가론의 의미와 가능성”, 공법학연구 제17권 제2호, 2016
- 김일환 · 홍석한, “개인정보 자율규제영역에서 보장국가로서 국가의 역할에 관한 연구”, 헌법학연구 제14권 제4호, 2008
- 진대화, “개인정보침해에 대한 손해배상의 근거와 피해구제제도”, Internet & Security Focus 2014
- 이상명, “개인정보자기결정권의 헌법적 근거에 관한 고찰”, 공법연구 제36집 제3호, 2008
- 최창수, “수사·정보기관의 통신이용 정보수집권에 관한 미국의 입법례와 그 함의”, 정보법학 제20권 제1호, 2016
- 김진환, “개인정보 보호의 규범적 의의와 한계”, 저스티스, 2014
- Samuel D.Warren & Louis D.Brandeis, The Right to Privacy, 4 Harv. L. REV. 193(1890)

Abstract

A Critical Study on The Right to Information Self-determination

Heui-ok Lee

In his books "Future Shock," "The Third Wave," and "Powershift," Alvin Toffler predicted the shift in modern society to the information age. "Information society" is a society where knowledge emerges as a principal force of production, and rapid advances in information technology make the use of information about people's everyday life as an integral part of our society. Not only is information valuable in and of itself, but it also creates new value and drives business and market changes. In a society where the rapid distribution of information is enabled by access to the Internet and information and communication technologies, individuals have the rights of self-determination regarding personal information, which means the rights to determine what sort of personal information will be disclosed and used. This article examines how the rights to informational self-determination are exercised and whether or not the data subject can exercise the rights to freely participate in society through their rights to informational self-determination.

In modern society, a discussion on personal information protection should begin with an examination of the protection and benefit of the law that such protection is ultimately pursuing, rather than the protection itself. The benefit and protection of the data protection laws are chiefly concerned with the data subject's right to informational self-determination and freedom of privacy protected by the

Constitution. In Korean society, rapid growth of the IT industry has led to a succession of data breaches, and rising importance of privacy protection and legal and policy efforts have been made to develop countermeasures. However, in actual legal claims for invasion of privacy, damages are only awarded in very modest amounts even if the court acknowledges the invasion of privacy, indicating that the data subject's right regarding personal information is still exercised in a perfunctory manner. This is because current privacy laws have limitations, in that an invasion of privacy is determined through balancing of interests when the data subject's right comes into conflict with the public interest or another person's fundamental rights, and that an acknowledgement of the invasion of privacy does not mean that an invasion of the data subject's substantial rights is acknowledged. The right to informational self-determination or privacy will not be deemed as a substantial right until such invasion is claimed in an actual lawsuit and damages are awarded for the invasion. Recently, statutory damages and punitive damages have been incorporated into the Korean privacy legislation to overcome the limitations of the existing victim protection system. However, a series of recent cases have shown a tendency to develop more elaborate criteria for determining violations of informational self-determination. Thus, aside from the limitations of the recently adopted programs, it is still open to discussion whether the benefit and protection of the law and rights can be made more specific under individual laws, and whether a data subject's substantial rights can be sufficiently guaranteed without having in place any criteria for determining the illegality of an invasion or any measures in awarding damages. In a society that is rapidly entering the information age, the state has a responsibility to guarantee substantial rights for data subjects by providing legal and policy programs. To that end, this article suggests the "guarantor state" model. In this rapidly changing society, the state should establish a legal and policy framework

and allow each data subject to exercise their fundamental rights regarding information. Moving beyond early efforts to put privacy laws in place, the state should maintain a uniformly self-regulation system and actively encourage corporate participation.

Key word: Information society, Informational self-determination, Guarantor state, Personal information, Self-regulation