# 개인정보보호법제

## 개선을 위한

# 정책제안서







프라이버시 정책 연구 포럼

# 프라이버시 보호 : 신화에서 현실로

문재완, 한국외대 법학전문대학원 교수

# 프라이버시 보호 : 신화에서 현실로

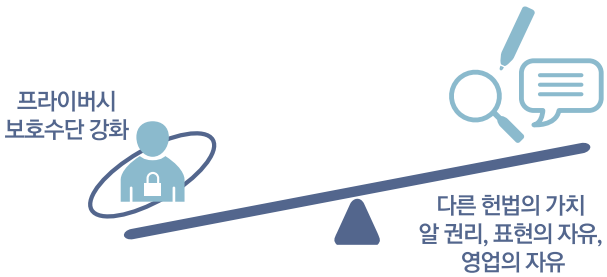
**문재완**
한국외대 법학전문대학원 교수

## 신화가 된 프라이버시 보호

- 프라이버시는 보호하면 할수록 좋고, 보호수단을 많이 마련할수록 좋고, 위반에 대해서 엄하게 다스릴수록 좋다는 막연한 믿음에 근거하여 개인정보 보호법제가 마련돼 시행 중
  - 개인정보 보호 강화는 다른 헌법적 가치, 즉 알 권리, 표현의 자유, 영업의 자유 등을 침해하는 결과가 될 수 있어 신중하게 접근하여야 함

## 프라이버시 보호에 있어서 공공부문과 민간부문의 구분 필요성

- 개인정보보호법은 공공부문과 민간부문을 통합하여 규제함으로서 프라이버시 침해의 주체가 공공부문에서 민간부문으로 이전하는 착시 효과가 발생함
  - 공공부문에서는 개인의 프라이버시를 최대한 보장하기 위하여 공권력 행사를 최대한 통제하여야 하지만, 민간부문에서는 대립되는 두 자유, 즉 한 쪽 사인의 프라이버시와 다른 한 쪽 사인의 표현의 자유 또는 영업의 자유 사이의 조화와 균형이 최우선되어야 함




## 프라이버시에 대한 올바른 이해

- 프라이버시는 공적 영역과 사적 영역의 구분을 전제로 해서 사적 영역을 보호하기 위해서 마련된 개념임. 최근 정보 프라이버시가 중시되면서 공사 구분론이 흔들리고 있지만 프라이버시의 핵심은 사적 영역의 보호에 있음

- 개인정보자기결정권은 개인이 사회생활 영역에서 다른 사람들에게 보이는 자기 모습과 관련된 인격권으로, 개인정보의 '공개'를 보호하고자 도입된 개념임
  - 사생활 영역이 아닌 공개된 영역에서 개인정보를 '수집'하는 것은 개인정보자기결정권을 침해하는 것이 아님

- 개인프라이버시 침해를 방지하고, 실효성 있는 구제방법을 찾기 위해서는 프라이버시를 총괄적으로 접근하는 태도를 버려야 함
  - 프라이버시의 내용을 하나씩 구분해서 그곳에서 발생하는 구체적인 해악을 발견하고 대책을 마련하는 것이 올바른 태도임
  - 공공부문과 민간부문의 구분, 사생활영역과 공개영역의 구분은 프라이버시 문제 해결의 전제임 정보통신기술의 발달로 구분이 불명확해지면 그 정도만큼 반영하여 입법하고 실행하는 것으로 보충할 수 있음

## 개인정보 보호와 다른 헌법적 가치의 조화

황성기, 한양대학교 법학전문대학원, 교수

## 개인정보보호의 법, 경제, 및 이노베이션

고학수, 서울대학교 법과대학 교수

## 현행 개인정보보호 법제상 개인정보 정의의 문제점

구태언, 테크앤로법률사무소 변호사

## 현행 개인정보처리의 법적 기준에 대한 타당성 분석

이인호, 중앙대학교 법학전문대학원 교수

## 정보 주체의 '동의' : 동의의 허구성과 해결방향

김기창, 고려대학교 법학전문대학원 교수

# 개인정보 보호와 다른 헌법적 가치의 조화

**황성기**
한양대학교 법학전문대학원 교수

## 개요 및 현황

- 개인정보와 관련하여서는 기존의 정책방향이나 시장에서의 관행이 '활용'에 치우쳤다고 한다면, 최근에는 「개인정보 보호법」의 시행을 계기로 유럽연합에서부터 촉발된 '보호' 쪽으로의 흐름이 강하게 존재

- 특히 유럽에서 형성된 '잊혀질 권리(right to be forgotten)'라는 개념이 이러한 '보호' 쪽으로의 정책 방향을 보여주는 대표적인 상징적 개념

- 개인정보 보호와 관련되어 있는 헌법상의 권리는 '개인정보자기결정권'임

- 개인정보자기결정권은 절대적인 권리는 아니며, 다른 기본권과의 조화 내지 다른 헌법적 가치와의 조화가 필요

## 주요 내용

- 개인정보 보호와 기타 헌법적 가치 간의 충돌을 조화시키기 위한 법익형량이 개별 사건에서의 법원의 판결을 통해서 이루어지겠지만, 입법적 차원에서도 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준이 제시될 필요

- 입법적 차원에서 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준을 모색함에 있어서는 다음과 같은 사항들을 고려

- 개인정보별 보호 정도의 차별화가 가능한지에 대한 검토가 필요

- 개인정보 보호와 충돌되는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화가 가능한지에 대한 검토가 필요

- 커뮤니케이션 및 통신기술의 변화 및 발전 정도도 고려할 필요

## 개선방안

- 민감 정보와 비민감 정보의 구분에 따른 보호정도의 차별화가 필요

- 공적 성격의 정보 v. 사적 성격의 정보 간의 구분

- 개인에 관한 정보(information about private person) v. 개인정보(personal data) 간의 구분


- 고유식별정보(개인정보 보호법 제24조, 동법 시행령 제19조. 주민등록법 제7조제3항에 따른 주민등록번호, 여권법 제7조제1항제1호에 따른 여권번호, 도로교통법 제80조에 따른 운전면허의 면허번호, 출입국관리법 제31조제4항에 따른 외국인등록번호) v. 개인식별정보(개인정보 보호법 제2조제1호의 개인정보 중 '개인을 알아볼 수 있는 정보') v. 개인식별가능정보(개인정보 보호법 제2조제1호의 개인정보 중 '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것' – 단편 정보 혹은 모자이크 정보) 간의 구분

- 충돌되는 다른 헌법적 가치의 중요도 및 보호정도의 차별화가 필요

- 표현의 자유가 가지는 중요도 및 보호정도를 고려해야 함. 비상업적 표현 v. 상업적 표현의 구분도 고려되어야 함

- 영업의 자유가 가지는 중요도 및 보호정도를 고려해야 함. 다만 이 경우 표현의 자유와 비교해보았을 때, 그 보호정도가 약하므로, 표현의 자유의 경우와는 그 방향성 및 기준이 달라질 수 있음

| 기본권의 종류 / 개인정보 유형 | | 표현의 자유 | | 영업의 자유 |
|---|---|---|---|---|
| | | 언론보도의 자유 | 사적 표현 및 광고 표현의 자유 | |
| 민감정보(고유식별정보 포함) | | 개인정보 보호가 우월 | 개인정보 보호가 우월 | 개인정보 보호가 우월 |
| 비민감성정보 | 개인식별정보 | 언론보도의 자유가 우월 | 사안에 따라 유동적 | 사안에 따라 유동적 |
| | 개인식별가능정보 | 언론보도의 자유가 우월 | 사적 표현 및 광고 표현의 자유가 우월 | 영업의 자유가 우월 |

# 개인정보보호의 법, 경제, 및 이노베이션

**고학수**
서울대학교 법학전문대학원 교수

## 개요

- 개인정보의 활용은 이노베이션을 촉진시키고, 이를 통해 사회와 경제에 도움이 되는 다른 많은 기능 또한 제공될 수 있음

- 따라서 개인정보의 수집과 이용에 대한 규제를 고려함에 있어, 개별 규제가 이노베이션 활동을 포함하여사회와 경제에 미치는 영향에 대한 엄밀하고 상세한 분석이 필요함

- 개인정보의 보호에 관한 논의에 있어 종종 발견되는 오류는, 개인정보의 보호와 개인정보의 수집·이용 사이에는 상충관계(trade-off)가 있어서, 개인정보의 보호수준을 높이기 위해서는 개인정보의 수집과 이용을 제한하는 것이 필수적이라는 일반적인 전제하에 논의를 진행하는 것임. 이러한 전제는 논리적으로나 실증적으로 근거가 없는 것임

- 실제로는 개인정보의 수집과 이용이 개인정보의 보호에 문제를 발생시키는 상황도 있고, 그렇지 않은 상황도 있음. 문제가 될 수 있는 '시장의 실패'(market failure) 상황이나 기타 구체적인 문제상황에 대한 과학적이고 실증적인 분석을 진행한 뒤에 그에 근거하여 정책적 판단을 해야 함. 그러한 문제의 가능성이 확인되지 않는 상황에 대해서는 시장의 기능이 충분히 발휘되어 새로운 기술이 계속 개발되고 활용될 수 있는 방향으로 규제의 틀을 정립해야 할 필요가 있음

## 주요 내용

- 개인정보의 수집과 이용에 대한 규제를 논의함에 있어 흔히 발견되는 오류는, 개인정보를 수집하고 이용하고자 하는 기업의 이익과 이용자의 이익이 일반적으로 서로 배치될 것이라고 전제하고 논의를 하는 것임

개인정보의 수집과 이용에 대한
규제논의의 흔한 오류


기업의 이익 개인의 이익

- 이러한 전제와는 달리, 실제로는 정보를 수집하고 이용하는 기업의 활동이 이용자의 이익에 부합되는 상황도 있고, 그 반대로 이용자의 이익에 저해되는 상황도 있을 것임. 규제의 문제는 기업활동이 이용자의 이익에 저해되는 경우를 선별하여, 그러한 상황이 발생되는 것을 방지하고 억제하는 것에 있는 것이지, 기업활동이 전반적으로 부정적인 효과를 가질 것이라고 전제하고 그러한 활동을 규제하는 것에 있지 않음을 항상 기억할 필요가 있음

- 개인정보의 활용에 대한 규제가 이노베이션에 영향을 미치는 상황에 대한 실증분석의 한 예로, 유럽에서의 온라인상거래에 대한 규제강화가 광고의 효과에 미친 영향에 대하여 분석한 사례를 들 수 있음(Goldfarb & Tucker, 2011). 이 연구는 규제강화가 광고의 효과를 65%나 저하시키는 결과를 초래하였음을 보여줌. 규제강화는 광고의 효과를 이처럼 매우 크게 떨어뜨리고 관련된 기술개발 시장을 위축시키는 결과를 가져왔는데, 다른 한편 이러한 규제의 강화를 통해 유럽 인터넷 이용자들의 개인정보보호가 실질적으로 강화되었다는 명확한 징후는 발견되지 않음

- 또한 웹사이트의 성격이나 광고의 성격 등에 따라서 규제의 변화로 인해 서로 크게 다른 차별적 영향을 받게 된다는 것도 확인됨. 예를 들어, 뉴스 사이트 등 특정 영역에 특화되지 않은 범용 사이트는 쇼핑 사이트나 여행 사이트 등 상품판매에 주력하는 사이트에 비해 그 영향을 훨씬 크게 받고, 또한 배너광고 등 정보제공을 위주로 하는 광고는 플래시 등을 적극 활용하는 화려하고 자극적인 형태의 광고보다 영향을 크게 받음

- 이와 같은 연구결과가 시사하는 바는, 새로운 규제의 도입이나 기존 규제의 수정에 있어, 그 전반적 영향이 어떠할 지에 대한 상세한 분석이 필요할뿐더러, 각기 다른 유형의 규제대상자들에 미칠 영향에 대한 미시적인 면밀한 분석 또한 요구된다는 것임. 표면적으로는 중립적인 형태의 규제도 규제로 인한 실제 영향을 살펴보면 매우 차별적인 결과를 가져올 수 있고, 나아가 언론의 자유나 영업의 자유 등 중요한 헌법적 가치에 대한 훼손이 초래될 수도 있음

- 흔히 개인정보의 보호는 개인정보에 대한 자기결정권을 기본전제로 하여, 그러한 자기결정권을 강화하는 방향으로 규제가 이루어지는 것이 당연히 바람직한 것으로 인식되는 경향이 있음

- 그런데 인터넷 이용자를 대상으로 한 정보의 노출 및 공개(disclosure)에 관한 연구결과에 따르면, 정보의 자기결정권을 강화하는 것이 이용자의 정보보호에 기여하지 못하는 역설적인 결과를 가져올 수도 있음이 확인됨.  즉, 이용자들에게 정보공개 여부에 대한 콘트롤(control)을 더 많이 부여할수록 이용자들은 더 많은 개인정보를 노출하는 경향을 보인다는 것임. 이를 '콘트롤 패러독스'(control paradox)라고 함 (Brandimarte, Acquisti & Lowenstein, 2010)


- 콘트롤 패러독스가 시사하는 것은, '잊혀질 권리'에 대한 논의를 포함하여 개인정보에 대한 자기 결정권을 확대하는 방향의 정책결정이 애초에 기대했던 개인정보보호의 강화라는 정책목적을 달성하는 데에 전혀 효과적이지 못할 가능성이 있고, 오히려 경우에 따라서는 정책을 통해 기대했던 것과는 다른 정반대의 결과를 초래할 수도 있다는 것임. 효과적인 정책수단의 개발을 위해서는, 개별 정책수단에 일반 이용자들이 구체적으로 어떻게 반응하는 지에 대한 행태자료에 기초한 엄밀한 실증적 연구가 전제되어야 할 것임

- 위에서 간단히 언급한 유형의 실증자료나 행태자료에 기초한 과학적 분석은 국내에서는 개인정보보호를 위한 법이나 정책에 대한 논의에 있어 지금까지 거의 활용된 적이 없는 것으로 보이는데, 이러한 태도에 대한 재검토가 필요함. 특히 국내자료에 기초한 검토와 분석이 시급히 요구됨. 실증적이고 과학적인 분석에 기초하지 않은 규제는 그 정책목표의 달성에 있어 어려움이 있을뿐더러 경우에 따라서는 부작용만을 불러일으킬 가능성도 높음

# 현행 개인정보보호 법제상 개인정보 정의의 문제점

**구태언**
테크앤로법률사무소 변호사

## 개요 및 현황

- 개인정보의 정의
  - 개인정보보호에 관한 기본법인 「개인정보 보호법」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)고 규정
  - 온라인상 개인정보보호에 관한 특별법인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보의 정의도 대동소이

- '개인식별정보'와 '사람관련정보(비식별인적정보)'의 구별
  - 관련 법령에서 규율하는 개인정보는 개인식별정보를 넘어서 사람관련정보도 포함하고 있음. 예를 들어, 개인정보 보호법은 개인정보라는 이름하에 개인정보 수집시 필수적 동의사항, 선택적 동의사항의 구분을 하도록 하고, 민감정보를 수집할 때에는 별도의 동의를 받도록 함

- 개인정보 운용 실태와 문제점
  - 실제 개인정보는 개인식별정보만 처리되거나, 개인식별정보와 사람관련정보가 결합되어 처리되어야 함
  - 사람관련정보는 개인식별정보가 제거되면 '개인정보성'을 상실하므로 별도로 동의의 대상으로 삼을 필요가 없음에도, 주요 법령상 사람관련정보의 수집이용도 그 대상으로 전제하고 규정하고 있음
  - 특히 우리나라 주요법령상 개인정보의 정의는 다른 주요나라의 개인정보의 정의에 비추어 지나치게 넓어 기업의 영업을 극도로 위축시키고 형벌을 지나치게 확장시키고 있음


## 주요 내용

- 개인식별정보와 사람관련정보의 혼동
  - 주요 법령이 개인정보라는 이름 하에 정의하고 있는 내용은 사실상 개인식별정보이며, 당사자를 식별할 수 있는 정보만을 개인정보라고 정의하고 있음
  - 그러나, 실제 개인정보의 이용실태는 개인을 식별할 수 있는 정보와 개인과 관련된 정보가 결합되어 이용되며 개인정보에서 개인식별정보를 제거할 경우에는 익명의 개인과 관련된 정보로 바뀌게 되므로 개인정보성을 상실하게 됨
  - 주요 법령이 개인식별정보와 사람관련정보를 구분하고 있지 않은 채 개인정보라는 이름으로 규율하고 있는 결과, 개념상 혼동을 초래하고 개인정보보호에 관한 규제의 실효성에도 의문이 제기되고 있음

- 개인식별정보(협의의 개인정보) 정의의 광범위성
  - 다른 주요 국가의 개인정보의 개념을 보더라도, '개인을 식별하거나 식별할수 있는 정보(PII, Personal Identified or identifiable Information)'를 개인정보[협의의 개인(식별)정보]라 정의하고 있는데 이는 우리나라 주요 법령상 개인정보 정의의 '본문'과 일치하는 것임
  - 그러나 우리나라 주요 법령은 개인정보의 정의에 '그 자체로는 아직 개인을 식별할 수 없는 정보라도 다른 정보와 쉽게 결합하여 개인을 식별할 수 있는 정보'[광의의 개인(식별)정보]도 개인정보로 본다고 정의하여 개인정보의 범위를 확대하고 있음(이는 형사처벌 조항과 연계되어 가벌성을 확장)

▶ 영국, 호주 등의 경우 법령명이 'Privacy Act'이나 내용은 개인식별정보에 기반한 개인정보 보호에 있는 반면, 우리나라는 개인정보 보호법의 목적 조항에 사생활 비밀의 보호를 포함시키고 개인정보의 범위를 극단적으로 확장함으로서 사실상 사생활(또는 비밀)보호법과 같이 운영되고 있음

| 법률 | 내용 |
|---|---|
| OECD 가이드라인<br>제1조 | 식별된 또는 식별가능한 개인에 관한 정보.<br>any information relating to an identified or identifiable individual ("data subject") |
| EU 지침<br>제2조 | 정보주체의 신원이 확인되었거나 확인 가능한 정보. any information relating to anidentified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;" (art. 2 a) |
| 캐나다 프라이버시법<br>제3조 | 신원을 확인할 수 있는 개인에 대한 정보 |
| 일본 개인정보보호에<br>관한 법률 제2조 | 생존하고 있는 개인에 관한 정보로서 당해 정보에 포함된 성명, 생년월일 기타 설명된 것에 의해 특정한 개인을 식별할 수 있는 것(다른 정보와 용이하게 조회할 수 있으며, 그렇게 함으로써 특정한 개인을 식별할 수 있게 되는 것을 포함한다) – 우리나라와 가장 유사함 – |
| 호주 프라이버시법<br>제6조 | 진실이든 아니든 물리적 형태에 기록되어 있든 아니든 간에 그의 신원이 명백하거나 합리적으로 판명될 수 있는 개인에 관한 정보 또는 의견 |
| 영국 개인정보보호법<br>제1조 | 신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터 또는 정보 관리자가 보유하고 있거나 앞으로 그러할 가능성이 높은 기타 정보 또는 데이터로부터 신원이 확인가능한 생존 개인과 관련된 데이터 |
| 프랑스 정보처리<br>축적 및 자유에 관한 법률<br>제4조 | 개인정보는 직접 또는 간접적으로 식별확인번호나 그를 확인하게 해주는 하나 이상의 요소를 참고함으로서 식별되거나 식별가능한 개인에 관한 정보로 구성된다. 개인이 식별가능한지를 결정하기 위해서는 신원확인을 이용가능하거나 정보처리의 책임자가 접근가능하거나 혹은 어떤 다른 사람이 소유할 수 있는 모든 수단을 고려할 것이 권고된다. |
| 독일 연방개인정보<br>보호법 제3조 | 신원이 확인되었거나 확인 가능한 정보주체의 인적·물적 환경에 관한 일체의 정보 |

- 기술이 발달한 결과, 통신사의 아이디(ID), 전화번호, 이동전화의 고유번호(IMEI), 랜카드의 맥(MAC)주소, IP주소, 쿠키(cookie)등 그 자체로 개인식별성이 떨어지는 정보도 개인정보로 보는 견해와 판결이 있음

- 개인정보 보호법의 괄호부분으로 인하여 어떠한 사람관련정보도 개인정보로 평가받을 수 있으므로 사실상 개인식별정보와 사람관련정보의 구별 실익이 없게 되어 '모든 정보는 개인식별정보'라는 비합리적인 결론에 도달

## 개선방안

○ 개인정보를 개인식별정보와 사람관련정보로 구별


- 개인정보를 현행처럼 개인을 식별할 수 있는 정보로만 정의한다면 오히려 개인의 식별성이 없는 정보자체의 수집 등 규제가 법적 효력의 흠결사유를 갖게 됨

- 개인식별정보와 사람관련정보를 구별하고, 개인식별정보를 제외한 사람관련정보의 수집에 있어서 원칙적으로 규제하지 않되 민감한 사람관련 정보 등 일정한 사람관련정보는 예외적으로 규율하는 체제로 정비

- 예를 들어, 사람관련정보 중 민감정보나 필수적이지 않은 정보의 수집을 규율하는 것이 타당하다면 이들은 개인(식별)정보와 함께 수집할 때에 의미가 있으므로 “개인(식별)정보와 함께 민감한 사람관련정보를 수집할 때”를 규율하는 것으로 법제를 정비할 필요 있음

○ 개인정보의 정의의 조정

- 광의의 개인(식별)정보를 미리 개인정보라 정의하는 것은 기업의 정보처리에 심각한 법적 위험을 야기하며, 실제 광의의 개인(식별)정보는 아직 개인식별성이 생기지 않은 정보이므로 선행적 법적 규제의 정당성도 미흡함

- 협의의 개인(식별)정보만 개인정보로 정의해도 법적 보호목적을 달성하기에 충분하며, 만약 개인정보 처리자가 광의의 개인(식별)정보에 다른 정보를 결합하여 협의의 개인(식별)정보를 만들게 되면 이는 이미 ‘개인정보’를 처리하는 것이므로 주요 법령상 개인정보보호에 관한 규제를 받게 되므로 광의의 개인(식별)정보를 개인(식별)정보의 개념에서 제외한다고 해도 처벌의 흠결도 전혀 생기지 아니함

# 현행 개인정보처리의 법적 기준에 대한 타당성 분석

**이인호**
중앙대학교 법학전문대학원 교수

## 개요 및 현황

- 지난 10년간 우리 사회는 개인정보보호를 절대화하는 경향을 보여 왔음
  - 정보주체의 동의없는 개인정보의 수집·이용·제공을 원칙적으로 불법으로 취급하려는 경향이 있음
  - 타인이 수집·처리하는 개인정보에 대해 그 정보의 주체에게 거의 절대적 통제권을 주고자 함. 이는 모든 개인정보를 '비밀정보'로 취급하려는 것임

- 개인정보자기결정권에 대한 오해
  - 헌법재판소가 2005년에 확인한 기본권으로서의 '개인정보자기결정권'은 '공공기관'의 개인정보처리(=수집·이용·공유)에 대한 개인의 통제권임. '민간'의 개인정보처리에도 무분별하게 헌법상의 개인정보자기결정권을 주장하는 것은 기본권과 사권을 구별하지 않는 오해에서 비롯됨
  - 개인정보자기결정권은 개인정보처리자가 행하는 개인정보처리의 전 과정(=수집·가공·이용·제공 등)을 정보주체가 직접 결정하거나 통제할 수 있는 권능이 아님. 개인정보의 '安全한 처리'를 보장하기 위하여 정보처리의 과정에 해당 정보주체가 참여할 수 있는 권능임(=참여해서 감시하는 권능)

- 개인정보보호법에 대한 오해
  - 법의 목적은 본래 '개인정보의 안전한 이용과 유통'에 있음. 무분별한 개인정보의 처리에 따르는 위험을 사전에 예방하기 위한 것임
  - 그런데 우리의 현행법은 '사생활비밀 보호'의 목적을 선언함으로써 입법목적을 처음부터 잘못 잡은 상태에서, 특히 민간부문을 겨냥하여 세계 유례가 없는 엄격한 처리기준을 설정해 놓고 사후 제재와 형사처벌 위주의 집행체계를 마련하고 있음. 사생활비밀보호법과 개인정보보호법을 혼동한 것임

- 개인정보보호법은 개인의 프로파일링(profiling)을 가능하게 하는 개인정보DB의 구축과 관련된 개인정보의 수집·이용·제공을 규율하는 것임

## 주요 내용

- 현행의 개인정보보호법들은 개인정보를 모두 '비밀정보'로 인식하는 잘못을 범함으로써, 개인정보의 '보호'의 가치에만 치우쳐 '안전한 이용과 유통'의 가치를 외면하고 있음. 그로 인해 민간의 영역에서 개인정보의 '안전한 활용' 자체를 거의 불가능하게 함으로써 자원배분의 효율성과 새롭고 창의적인 정보서비스의 창출을 가로막고 있음.


- 온라인 개인정보보호법인 2001년의 「정보통신망법」
  - 정보주체의 동의 없는 개인정보의 수집·이용·제공을 원칙적으로 不法으로 취급하여 강력한 행정제재 및 형사처벌을 가함
  - DB마케팅서비스 등 새로운 정보서비스가 생겨날 수 있는 가능성을 원천봉쇄하고 있음

- 공공과 민간을 아우르는 일반법인 2011년의 「개인정보보호법」
  - 민간부문에 있어 '일반개인정보'의 경우, '수집'에서부터 정보주체의 동의를 원칙으로 하면서 몇 가지 예외를 두고 있으며(§ 15, 16), '이용 및 제3자 제공'에 대해서는 동의의 원칙을 더욱 강화함(§ 17, 18) → 행정제재 및 형사처벌

- ‘민감개인정보’(건강정보 등)의 경우, 수집·이용·제공의 허용기준이 너무 엄격함(동의원칙의 절대화) → 강력한 행정제재 및 형사처벌
- 정보주체에게 ‘정정·삭제요구권’을 아무런 제약 없이 인정함(§36①)
- 유럽, 미국, 일본 등 외국의 개인정보보호법과 비교할 때 유례가 없음

## 개선방안

- 개인정보자기결정권과 개인정보보호법에 대한 오해를 불식시키는 노력을 지속적으로 강화

- 제3자 제공의 허용기준을 유럽이나 일본의 입법례를 참조하여 합리적으로 개선함
  - 유럽은 (ⅰ) 일반개인정보의 경우 개인정보처리자나 제3자의 정당한 이익을 달성하기 위한 경우에 정보주체의 동의 없는 제3자 제공을 넓게 허용하되, 대신 정보주체에게 사후에 그 제공을 거부할 수 있는 권리(right to object)를 줌 → opt-out 방식(사후거부방식). (ⅱ) 민감개인정보의 경우 제3자 제공을 원칙적으로 금지하되, 정보주체의 동의가 있거나 또는 기타 제3자 제공이 필요한 경우를 구체적으로 열거함
  - 일본도 제3자의 정당한 업무수행을 위하여 또는 광고나 마케팅 목적을 위하여 수집·처리한 개인정보를 정보주체의 동의 없이 제3자에게 제공하는 것을 합법적으로 허용하되, 대신 정보주체에게 사전 고지와 사후거부권을 주어 통제하게 함

# 정보 주체의 '동의' : 동의의 허구성과 해결방향

**김기창**
고려대학교 법학전문대학원 교수

## 개요 및 현황

- 개인정보 보호에 관한 법제는 정보주체의 '동의'를 핵심 개념으로 삼고 있음

- 예외적으로 동의가 필요 없는 경우를 법률로 정하고 있으나, 그 외의 경우에는 정보주체의 동의가 있으면 더 이상의 고려가 불필요 하다는 듯한 전제가 깔려있는 것으로 보임

- 그러나 '동의'의 법적 의미에 대하여는 상세한 논의가 없는 실정임. 그러나 '동의'는 적어도 다음과 같은 상이한 법적 의미를 가질 수 있음
  - 사법적 계약 관계에서 요구되는 '의사의 합치'
  - 형사 범죄행위 및 민사 불법행위에서 위법성을 조각하는 의미를 가지는 '피해자의 승락' (volenti non fit iniuria)
  - 헌법적 기본권 침해를 아예 성립시키지 않게 만드는 권리 주체의 자발적 요청, 승인

- 그러나, 이 세가지 경우 모두, 정보 주체의 '의사'만을 기준으로 동의/승락/승인의 법적 효력을 종국적으로 판단할 수 있는 것은 아님. 예를 들어,
  - 약관 규제 법리에 의할 경우, 사법적 계약 관계에서의 동의가 과연 '공정'하고 '신의칙'에 부합하는 것인지는 법원의 '사후적 통제'를 받음. 아무리 동의가 있었다 해도, 형평에 어긋나거나, 신의칙에 반하는 내용이라면 그러한 동의는 효력이 없음
  - 피해자의 승락 역시 공서양속에 반하는 것이라면 효력이 없음
  - 헌법적 가치 또한 당사자가 임의로 이를 포기할 수 있는지에 대하여는 논란의 여지가 있고, 아마도 승인되기 어려움

- 동의의 '방법'과 관련해서도 적지 않은 법적 문제가 있음
  - 사법적 의사의 합치, 또는 약관에 대한 동의는 일반적으로 어떠한 정해진 방식도 요구되지 않음. 약관에 대한 동의는 심지어 소비자가 약관의 존재 자체를 알지 못했더라도 일단은 '의제'됨
  - 형법적 맥락, 불법행위적 맥락에서의 '승락' 역시, 아무런 정해진 방식은 없음. 전후 사정을 고려하여 당연히 승락한 것으로 볼 여지가 있다면 명시적 의사 표시행위가 없었더라도 '묵시적 승락'을 충분히 인정할 수 있음. (예를 들어, 일상적 치료 행위에 필요한 한도의 신체 침해 행위에 대하여 환자가 별도의 '동의서'를 작성하지는 않지만, 이 경우에도 당연히 피해자의 승낙이 있는 것으로 해석)
  - 위 두가지와는 구분되는 헌법적 맥락에서의 동의는 아예 허용되기 어려울 것임

- 그러나, 개인정보보호법 제22조 및 동법 시행령 제17조는 '동의를 받는 방법'을 법령으로 특정하고 있음. 그러나 이런 방식의 규제는
  - 심각한 사업적, 기술적, 현실적 어려움을 초래하는 한편,
  - 규정된 '동의를 받는 방법'이 과연 실효성이 있는지도 불분명함. 유저 보호라는 명분은 실제로는 허구적
  - 설사 동의를 표시하는 유저의 행위가 있었다 하더라도, 그것이 적법한 효력을 지니는 것인지는 여전히 불분명함
  - 오히려 부당한 내용의 동의가 '표시'된 경우, 유저가 보호되기 어려운 결과를 초래함

## 개선 방안

- 동의 '방식'을 특정해둔 개인정보보호법 제22조 및 동법 시행령 제17조, 정보통신망법 제26조의2 및 동법 시행령 제12조, 위치정보법 제19조 등은 폐기

- 그러나, 개인정보보호법 제22조 및 동법 시행령 제17조는 '동의를 받는 방법'을 법령으로 특정하고 있음. 그러나 이런 방식의 규제는

  (1) 서비스 제공 용도를 넘어서 정보를 수집하거나,

  (2) 수집한 정보를, 당해 서비스와 관련하여 유저가 합리적으로 예측하는 범위를 넘어서 부당하게 사용하는 행위를 '사후적'으로 제재

  (3) 정보주체의 이익을 현저히 해할 우려가 있는 행위는 금지. (예를 들어, 개인정보 보호에 대한 적절한 보호가 제공되지 않는 나라로의 개인정보 이전은 유저가 동의하는지 여부와 무관하게 허용되어서는 안 될 것임)

# 클라우드 서비스와 개인정보 보호

**김기창**
고려대학교 법학전문대학원 교수

## 개요 및 현황

- 클라우드 컴퓨팅 기술은 가상화 기술, 그리드 컴퓨팅 기술, 고속 인터넷망등을 기반으로 하여 전산 자원을 지리적 위치에 구애받음이 없이 신축적, 효율적으로 이용할 수 있게 해주는 기술임
- 일반 이용자(end user)들이 이용하는 '개인용 클라우드' 서비스와 사업자들이 이용하는 '서비스 클라우드'는 여러 측면에서 차이가 있으므로, 개인정보 보호와 관련된 문제들도 이 두 가지 경우를 나누어 검토하고 대응해야 함
- '개인정보'는 개인을 식별하는데 사용되는 정보이며, '사적정보'와는 구분되어야 함. 개인에 관한 모든 정보가 개인정보는 아님. 개인이 지배하는 모든 정보가 개인정보인 것도 아님
  - 개인용 클라우드 서비스 이용자들이 자신의 계정에 저장하는 정보는 '사적정보'이지 '개인정보'가 아님. 설사 그 속에 개인정보에 해당하는 것이 포함되어 있을지라도 개인용 클라우드 서비스 제공자가 이를 파악하거나 분간하도록 의무를 지울 수는 없으므로, 이런 정보에 대하여 개인용 클라우드 서비스 제공자가 각종 보호조치를 취하도록 의무를 부과할 수는 없음
  - 개인용 클라우드 서비스 이용자의 계정정보(subscriber information) 자체는 개인정보이며, 이에 대하여 개인용 클라우드 서비스 제공자가 취해야할 보호조치 의무는 여느 다른 사업자가 부담하는 개인정보 보호조치 의무와 동일함

- 사업자들이 자신의 전산 자원을 서비스 클라우드 제공자로부터 확보하여 사업을 펼칠 경우, 그 사업자의 정보는 서비스 클라우드 제공자가 운용하는 데이터 센터에 저장되는데, 그 이유만으로
  - 해당 정보가 제3자(서비스 클라우드 제공자)에게 '제공'된다고 볼 수는 없음. 정보가 '제공'된다는 것은 일정한 용도로 그 정보를 '이용'할 수 있도록 해준다는 의미를 내포하는 것이지만, 서비스 클라우드 이용자가 저장하는 정보를 서비스 클라우드 제공자가 일반적으로 이용할 수 있는 것은 아님
  - 해당 정보의 처리가 제3자(서비스 클라우드 제공자)에게 '위탁'되는 것으로 볼 수도 없음. 서비스 클라우드 제공자는 하드웨어 및 플랫폼을 제공할 뿐, 해당 정보의 처리에 대하여는 어떠한 개입도 허용되지 않음. 서버룸을 청소하는 용역을 담당하는 업체가 그 서버에서 처리 되는 정보의 처리에 개입할 수 없는 것과 다르지 않음.

- 개인정보의 '국외 이전'은 개인정보의 '제3자 제공'과는 다른 개념임. 국내의 사업자가 국외에 위치한 서비스 클라우드 제공자가 운용하는 데이터 센터에 자신의 데이터를 저장할 경우, 비록 서비스 클라우드 제공자가 이 정보를 '이용'할 수는 없더라도(따라서 제3자 제공은 아니더라도), 그 정보가 국외로 이전되는 것은 분명함. 이 경우에도 유저의 '동의'를 받아야 하는지는 고민이 필요함

## 개선 방안

- 국내 사업자가 국외의 서비스 클라우드 제공자를 이용하여 그자의 저장 설비에 자신의 데이터를 저장할 경우, 양자간에 체결되는 서비스 수준 계약에서 어떤 점이 확보되어야 개인정보에 관한 국내법을 국내 사업자가 어기지 않게 되는지에 대한 명확하고 구체적인 지침이 마련될 필요가 있음

- 수사 및 증거 수집 목적으로 사법 당국이 서비스 클라우드 제공자를 상대로 자료 제출을 요구하거나 강제 처분으로 자료을 확보할 경우, 서비스 클라우드 이용자(사업자)나 그의 고객(최종 유저)는 그러한 사실을 통보받지도 못하게 될 위험이 있음. 이점에 대한 적절한 대응책 마련이 필요함

- 국내의 사법 당국이 국외에 위치한 서비스 클라우드 제공자를 상대로 수사나 증거 수집에 필요한 자료 제출을 요구하거나 강제 절차를 통하여 데이터를 확보하려 할 경우 적절한 국제사법 공조 체제가 마련될 필요가 있음

- 서비스 클라우드를 이용한다고 해서 개인정보의 제3자 '제공'이나, 제3자 '처리위탁'이 되는 것이 아니고, 서비스 클라우드의 데이터 센터가 국외에 있다는 이유만으로 '개인정보 국외 이전 동의'를 요한다고 해석되지 않도록 법령을 명확화 할 필요가 있음

- 적절한 개인정보 보호가 제공되는 나라의 서비스 클라우드 제공자를 이용할 경우, 유저의 동의는 애초에 불필요하고, 그렇지 않은 나라로 개인정보가 이전되는 것은 유저 동의와 무관하게 금지하는 것이 올바름

# 개인정보 국외이전의 실무적 문제와 개선방향

**박광배**
법무법인 광장 변호사

## 개요 및 현황

- 세계화의 진행에 따라 개인정보의 국외이동은 불가피함
  - 개인정보의 국외이전에 대한 입법태도는 나라별로 천차만별임
  - 미국 : 국외이전에 따른 추가적인 제한이 거의 없음 / EU : (정보주체의 동의없는 경우) 적절한 수준의 보호를 하는 국가로 이전하는 것만 허용함(예외 : 표준계약조항을 통해 수령인이 정보보호법규를 준수함을 정보통제자가 보증하는 경우, Safe Harbor scheme, Binding Corporate Rules 등)

- 현재 개인정보의 국외이전에 대해서는 통일적인 규제는 없으며, 개별 법률마다 상이하게 규제하고 있음
  - 개인정보의 국국외이전관련 엄격한 법적용 강요시 개인정보 국내외 이전을 통한 효율적, 통일적 개인정보의 관리가 제한되어 오히려 정보주체에 대한 편익이 제한됨

## 실무상 국외이전과 관련하여 문제되는 법적 이슈

- “제공”과 “위탁” 구분의 불명확성
  - 개인정보의 제3자 제공은 “제공받는 측의 사업목적”을 위하여, 위탁은 “제공하는 측의 사무처리”를 위한 경우로 구분(대법원 2011. 7. 14. 선고 2011도1960판결)
  - 현실에서는 제3자제공과 위탁의 구분이 어려움에도 불구하고, 서로 다른 법적의무를 부과시킴으로 인한 혼란이 초래됨
  - 특히 제3자제공 또는 위탁의 형태로 국외이전되는 경우 국내와는 다른 법체계하에 있는 외국사업자에게 국내법의 요건을 그대로 준수할 것을 요구함에 따라 현실성있는 법집행을 기대하기 어려움

- 특히 제3자제공 또는 위탁의 형태로 국외이전되는 경우 국내와는 다른 법체계하에 있는 외국사업자에게 국내법의 요건을 그대로 준수할 것을 요구함에 따라 현실성있는 법집행을 기대하기 어려움

- 개인정보 공유에 대한 예외가 인정되지 않음

  - 현행 규정에 따르면 개인정보 피제공자를 전부 list-up 해야 하고, 그 변동시 일일이 고지하고(해당 법률에 따라) 동의를 받아야 함

  - 예외없이 과도하고 형식적인 고지/동의항목을 요구함으로 인해, 정작 정보주체가 관심가져야 할 내용까지 매몰되어 고지/동의가 형식화, 왜곡화되는 현상이 심화됨

- 정보주체의 동의에만 지나치게 의존

  - 외국의 정보보호수준에 대한 판별능력이 없는 정보주체(개인)의 동의에만 의존하여 국외이전여부를 결정함. 국외이전대상 국가의 적정한 정보보호수준여부는 개인이 아닌 국가가 정책적으로 판단해야 함

  - 국외이전 관련 개인정보취급자의 정보보호조치에 대한 보증/책임부담여부 등의 보호조치 부재시 혹은 기타 심각한 피해가 있을 수 있는 항목의 개인정보유출 등에 대한 위험상황이 고지된 상태에서 해당 정보주체의 동의여부를 확인하는 실질적인 informed consent 절차가 이루어지지 못하고 있음

## 개선 방안

- 고지/동의 일변도의 규제정책에서 탈피하여, 정보주체에게 요구되는 고지/동의사항을 정보주체가 실질적으로 예측하기 어려운 경우로 한정하여, 정보주체가 실질적인 개인정보자기결정권을 행사할 수 있도록 개정할 필요가 있음

- Opt-out 원칙 : 업무위탁과 제3자 제공에 대한 고지/동의요건의 완화
  - 수집·이용에 대한 동의시 정보주체가 실질적으로 예측가능한 범위내에서라면, 업무위탁에 대해서 고지·동의, 공개도 불필요함 /제3자 제공의 경우에는 공개 혹은 고지로 충분함
  - 국외이전에 대해서는 따로 규제하지 않고, 국외이전의 성격에 따라 업무위탁 내지 제3자 제공의 법리를 적용
  - 정보주체는 언제든지 개인정보철회권 행사하여 동의 제공 거부

- Opt- in 예외 : ①(정보주체가 예측할수 없는) 통상적인 업무목적을 벗어나는 정보의 제공/위탁의 경우, ②재화나 서비스 홍보목적, ③개인정보보호가 취약한 국가로 이전하는 경우, ④주민번호와 같은 고유식별정보나 민감정보를 제공·위탁하는 경우
  - 이러한 예외적인 사유가 있는 경우, 정보주체의 보호필요성이 보다 강조되어야 하므로 업무위탁의 경우에는 공개(혹은 고지), 제3자 제공의 경우에는 동의를 얻도록 규정함.

- 효과 : 정보주체는 정보제공시 예측못한 상황(위험이 예상밖으로 증대될 수 있는 국외이전의 경우 포함)에 대해서만 고지/동의절차가 진행됨으로서 실질적인 개인정보 자기결정권 행사가 가능하고, 사업자는 과다한 고지/동의 요건으로 인한 업무상 부담 완화

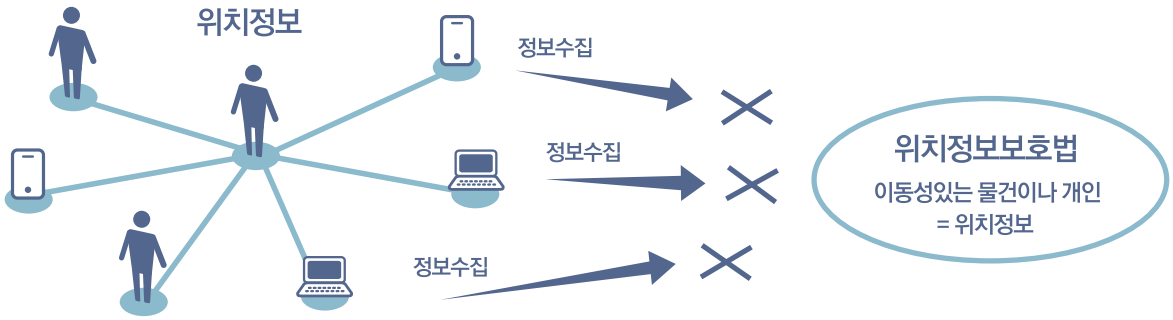
# ‘개인정보’의 정의와 위치정보보호법의 개정필요성

**박경신**
고려대학교 법학전문대학원 교수

## 개요 및 현황

- 위치정보보호법의 기본구조
  - 위치정보보호법은 개인의 위치정보의 남용이 그 사람의 사생활의 비밀을 침해할 수 있어 위치정보를 수집 및 이용할 경우 그 사람의 동의를 얻도록 하고 있음. 개인정보보호법이 일반적인 개인정보를 보호한다면 위치정보보호법은 그중에서 위치정보를 보호하는 특별법의 기능을 하고 있음
  - 또 개인의 위치정보를 생성하는 자를 ‘위치정보사업자’로, 그 위치정보를 제공받아 이용하는 업자를 ‘위치정보기반사업자’로 분류하고 전자는 허가제로 후자는 신고제로 규율하고 있음

- 현황과 문제점
  - 개인정보보호법제는 전세계적으로 사후규제를 원칙으로 하고 있음. 위치정보수집자(“위치정보사업자”)와 위치정보이용업자(“위치정보기반사업자”)를 허가제나 신고제와 같은 사전규제로 규율하는 것은 세계적으로 유례가 없어 산업발전을 억누르고 있음
  - 법 제15조는 ‘개인위치정보’와는 별도로 ‘이동성있는 물건이나 개인’의 위치를 ‘위치정보’로 정의한 후 “위치정보” 마저도 그 소유자나 그 개인의 동의 없이는 수집하지 못하도록 하고 있음
  - 이에 따라 업체들이 익명화된 위치정보 즉 위치정보의 주체를 파악할 수 없거나 파악하지 않는 상황에서 위치정보를 수집하여 이를 이용하는 방식의 서비스가 원천적으로 불가능함



## 주요 내용

- 허가제와 신고제의 폐지

  - 위치정보사업자를 허가제로 한 것은 이 법이 제정되었던 2005년 당시 (1) 민간기업이 다루는 개인정보를 규율하는 개인정보보호법이 존재하지 않았고 (2) 이동통신사업자만이 가입자 휴대폰의 접속 기지국 위치를 이용하여 가입자들의 위치정보를 수집할 수 있고 이들이 과점적인 지위를 남용할 가능성이 있었기 때문임

  - 그러나 (1) 현재 개인정보보호법이 시행되고 있고 (2) 휴대폰제조업체들이, 휴대폰사용자가 이통사들을 통하지 않고 스스로 자신의 위치정보를 파악할 수 있도록 하는 기능(예를 들어, 미군사위성의 GPS신호를 해독하는 방식)을 휴대폰에 탑재시키면서 훨씬 더 많은 업자들이 이 위치정보를 기반으로 하여 다양한 서비스를 제공할 수 있게 되어 위치정보의 과점 문제는 발생하지 않음

  - 또 실질적으로 위치정보는 스마트폰과 미국군사위성 사이에서 생성되므로 "위치정보사업자"는 존재하지 않는 것과 마찬가지. (법 실무상으로 단지 위치정보사업자-위치기반서비스업자 위계가 존재한다고 하여서 위치기반서비스업자에게 '위치정보사업자'의 지위를 부여하고 허가를 득하도록 하고있는 것은 위헌의 소지가 있음.)

  - 또 다른 개인정보의 수집과 이용에 대해서는 적용되지 않는 허가/신고제는, 위치정보의 수집 및 이용을 사전적으로 규제하여 위축시킴으로써 다양한 서비스의 제공과 비즈니스모델의 개발에 걸림돌이 되고 있음. 특히 누구나 위치정보를 이용한 다양한 앱을 만들어낼 수 있는 기술환경에서 신고를 사전에 해야 하는 것은 기술의 유출에 대한 위험 등으로 인해 기술개발을 위축시킴. 특히 위치기반서비스업자에게 강제로 위치정보사업자의 지위가 부여되는 경우 허가까지 득해야 함

- 위치정보보호법과 개인정보보호법의 규제평준화 : '위치정보' v. '개인위치정보'

  - 개인정보보호법이 정보주체를 식별해낼 수 있는 내용이 들어있는 정보 만(즉 "개인정보")을 보호대상으로 삼고 있는 것에 비하여, 위치정보보호법은 정보주체를 식별해낼 수 없는 위치정보 마저도 보호대상으로 삼고 있음.  예를 들어 "34, 위도 73에 있는 소유자불상의 휴대폰"처럼 실제로는 특정한 한 사람의 것이지만 그것이 누구인지 알 수 없는 정보도 모두 보호대상이 될 것임. 결국, 누구의 것인지 모르는 위치정보도, 위치정보의 주체를 색출해내어 동의를 얻을 것을 요구하고 있기 때문이며 동의를 얻는 과정에서 이미 위치정보의 주체가 파악될 수밖에 없고 결국 이 위치정보는 개인위치정보가 되어버림. 의료정보가 민감하다고 하여 누구의 것인지 모르는 의료정보를 수집하거나 처리하고자 한다면 해당 환자를 찾아내어 동의를 먼저 얻으라는 규제에 비교해볼 수 있음.

- 예를 들어, 캘리포니아 개인정보유출 통지법(SB1386)은 항상 (1)이름과 (2)고유식별정보 (예: 사회보장번호)의 “조합”을 보호대상으로 하고 있음. 이는 그 자체로 “John의 사회보장번호는 123-45-6789이다”라는 John에 대한 서술 또는 “사회보장번호 소유자 124-45-6789인 자의 이름은 John이다”라는 유의미한 “정보”를 유출하기 때문임

- 이를 차용하자면 개인정보의 의미는 그 정보를 여러 방식으로 서술하여 보았을 때 그 정보 자체로부터 특정한 개인을 우선 식별해낼 수 있는, 그 개인에 대한 정보를 의미하게 될 것임. 즉 개인정보는 “개인식별정보”와 “개인관련정보”의 조합. 개인정보보호법도 “(1)개인에 관한 정보로서 (2)성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말한다”고 하여 위와 같은 조합식 정의에 부합함

## 개선 방안

- 위치정보보호법의 제15조의 폐지 및 개인위치정보의 정의 수정 :

  - 위치정보보호법의 보호대상을 “(1) 개인의 위치에 관한 정보로서 (2) 그 개인을 알아볼 수 있는 정보(그 개인을 해당 정보만으로는 알아볼 수 없더라도 위치정보사업자나 위치정보기반사업자가 보유하고 있거나 일반적으로 공개되어 있는 정보와 쉽게 결합하여 알아볼 수 있는 정보)”로 정의되는 “개인위치정보”로 한정하고 “위치정보”라는 개념은 위치정보보호법에서 모두 삭제

- 위치정보보호법의 허가제와 신고제의 폐지 :

  - GPS방식으로 위치정보를 생성하는 한 ‘위치정보사업자’는 존재하지 않음. 기지국추적방식이 존재하더라도 GPS방식이 보편화되었으므로 과점의 위험이 없음. 허가제는 불필요. 신고제도 비즈니스모델의 공개를 강제하여 불필요하게 기술개발을 저해하고 있음

- 위치정보보호법의 제공 시마다 별도 동의 의무화 규정 폐지 :

  - 2002/58 유럽 Privacy and Electronic Communications Directive에 따라 도입되었으나 개별적 동의가 아니라 Opt-Out의 가능성만 제시하면 됨

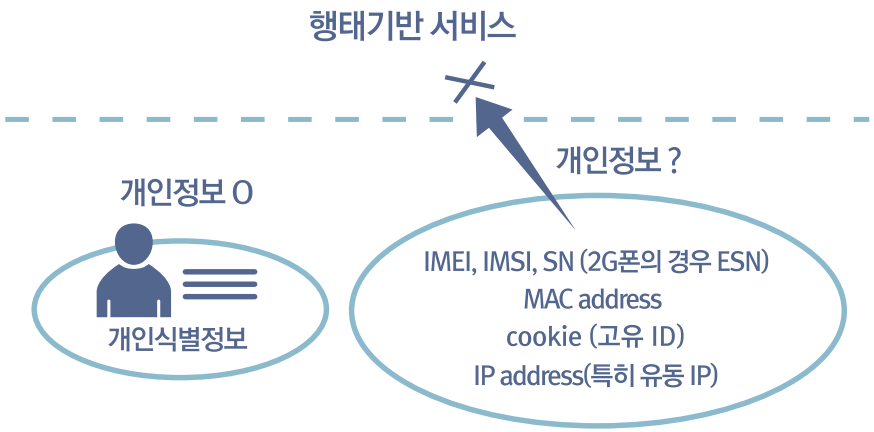
# 행태기반서비스(위치기반서비스 포함) 관련 법령 정비 방안

**박상철**
김·장 법률사무소 변호사

## 개요 및 현황

- 행태기반서비스(Behavior-Based Service; “BBS”)란 이용자의 온라인 이용 행태를 분석하여 이용자 관심에 맞춘 서비스를 제공하는 것이고, 온라인맞춤형광고(Online Behavioral Advertising; “OBA”)란 BBS 기반 광고이며, 위치기반서비스(Location-Based Service; “LBS”)란 위치정보 기반 BBS

- 개인식별정보(Personally Identifiable Information; “PII”)의 수집 없이 행태정보를 수집, 활용하기 위해서는 클라이언트 단말(PC, 스마트폰 등)에 할당 혹은 저장된 식별자(index)를 PII의 대체수단(proxy)으로 활용할 수밖에 없는바, 그 예는 다음과 같으며, 각 “개인정보” 해당 여부가 이슈임
  - 모바일 기기 정보 : IMEI, IMSI, SN 등 (2G폰의 경우 ESN)
  - PC 등 하드웨어 정보: MAC address
  - 쿠키(cookie)에 저장된 난수(random digit) 형태의 고유ID
  - IP address: 특히 유동 IP의 경우 이슈가 되고 있음



## 지금까지의 법적 논의 및 쟁점

- 관련 법령: 정보통신망법(온라인 BBS 전반에 적용), 위치정보법(LBS에 적용), 통신비밀보호법(IP address, log기록, 기지국 정보 등) 등

- 가이드라인: 방통위는 2010. 7. 1. “개인 식별성 행태정보”와“개인 비식별성 행태정보”로 구분하여 전자는 opt-in 규제를, 후자는 opt-out 규제를 하자는 취지의 가이드라인안을 마련하였으나 미시행되었고, 신경민 의원이 최근 이 내용을 반영하여 법률안으로 제출

- 가장 핵심적인 쟁점은 행태정보의 PII와의 결합의 용이성
  - 행태정보는 그 자체로 PII에는 해당하지 않으므로 “다른 정보와 쉽게 결합하여 알아볼 수 있는 경우”에만 정통망법상 개인정보나 위치정보법상 개인위치정보에 해당
  - 증권통 판결(서울중앙지법 2011. 2. 23. 선고 2010고단5343 판결) : 결합 용이성이란 “쉽게 다른 정보를 구한다”는 의미이기보다는 구하기 쉬운지 어려운지와는 상관없이 “해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것”을 의미한다고 보아 IMEI, USIM SN가 개인정보에 해당한다고 판시
  - 서울중앙지검 첨수부:  IP address의 경우, 같은 AP 사용 대역 내에서는 복수의 기기 이용자가 동일 IP주소로 접속할 수 있을 뿐 아니라 유동 IP address의 경우 시간별로 IP주소가 변동될 수 있으므로 “기술적 결합 가능성”이 없다고 판단

## “PII 결합 용이성”에 대한 기준 설정 및 이에 따른 법령 정비 방안

- 가능한 견해의 대립
  - 독립된 요건으로서의 무의미설 : “개인에 관한 정보”는 모두 개인정보
  - 객관적 결합 용이성설 : 행태정보는 다른 PII와 기술적으로 제약이나 어려움 없이 결합 가능할 경우 개인정보에 해당한다고 해석. 증권통 판결 및 서울중앙지검 첨수부가 취하는 견해
  - 주관적 결합 용이성설 : 행태정보의 보유자가 현재 보유 중인 PII를 결합해서 개인을 식별할 수 있을 경우 개인정보에 해당. 영국 Data Protection Act 1998이 취하고 있는 입장

- 증권통 판결은 행태정보가 해킹 등에 의해 유출되어 이통사가 관리하는 DB상의 PII와 결합될 막연한 가능성만으로 결합 용이성을 인정하였으나 프로그래밍 기술상 결합이 불가능한 경우는 사실상 존재하지 않는다는 점에서 지나친 확장 해석으로 보임. 막연한 유출 가능성만으로 결합 용이성을 인정하기보다는 현실적으로 결합되어 특정될 가능성에 따라 규제 여부를 결정하는 것이 타당하므로 주관적 결합 용이성설이 타당함

- 정보통신망법/위치정보법상 개인(위치)정보 정의 규정에 상기 요건이 명확하게 규정되지 않아, 규제 기관과 수사기관이 사실상 "독립된 요건으로서의 무의미설"을 채택하며 과잉규제, 과잉수사를 하는 폐단이 더 이상은 반복되지 않고, 예측가능성이 담보될 수 있도록, 정의 규정의 개정이 필요
  - 객관적 결합 용이성 개념에 따라 익명성 요건 충족시 개인정보 정의에 해당하지 않음을 명확히 하고
  - 주관적 결합 용이성 개념도 반영하여 PII의 경우 "현재 보유 중인 PII", "공지의 PII", "현재 적법하게 제공하고 있는 자가 보유 중인 PII"를 기준으로 하고, "당해 행태정보의 보유자"가 이러한 PII를 결합하여 개개인을 식별할 수 있는지 여부에 따라 결합 용이성 여부를 판단해야
  - 이 경우 기기정보 자체, 유동 IP address, 고유ID를 기준으로 수집된 행태정보는 결합 용이성이 인정되지 않아 개인정보에서 제외하여야 함

## 각 행태정보 유형별 처리에 대한 규제 정비 방안

- 식별 가능 행태정보의 처리에 대한 규제 방안
  - 현행 법령의 틀 내에서 개인정보에 준하는 규제를 할 수 있을 것이며 특별법 제정은 필요 없음

- 식별 불가능 행태정보의 처리에 대한 규제 방안
  - 이미 식별 불가능할 경우 프라이버시의 침해 우려가 없으므로 이에 대한 규제는 사업자 자율에 맡기도록 하는 것이 타당함

- 위치정보법 자체가 정보통신망법과 별도로 존립할 필요가 있는지 재검토가 필요하고, 존치하더라도 불합리한 세부 규정의 정비 필요

- 위치정보사업/LBS의 이원적 규제 폐지: 이통사가 수집한 CPS에 기반한 이원적 서비스 구조와 달리, 스마트 시대의 GPS 기반 서비스 구조 하에서는 app이 직접 개인의 위치정보를 수집하므로 양자가 분리되지 않음
- 허가/신고제 폐지 또는 완화
- 포괄적 제3자 제공 동의 허용 필요 : 현행 위치정보법은 각 제공시마다 동의를 미리 받도록 되어 있어, 제대로 된 LBS 기반 OBS가 불가능
- 스마트폰 환경에서의 불필요한 고지의무의 완화 필요 : 이용약관 등
- 취급위탁 규정의 신설 필요
- 영업양수인의 양수, 합병 후 통지 제도 개선 필요

- 통신비밀보호법의 정비 방안 : USIM 방식으로 전환되면서 사문화된 단말기기 고유번호 제공 금지 조항 폐지 필요

- 전기통신사업법 제83조 제1항, 제2항(“통신의 비밀”의 누설 금지), 정보통신망법 제49조(“타인의 비밀”의 침해, 도용, 누설 금지) 등 명확성이 결여되어 해당 정보의 식별 여부를 불문하고 무분별하게 적용될 수 있는 규정들을 정비하여야 함

# 개인정보 주체의 권리에 대한 조화로운 접근

**최경진**
가천대학교 법과대학 교수

## 개요 및 현황

### 현행법 상의 정보주체의 권리

- 개인정보보호법은 정보주체의 권리로서 개인정보의 열람청구권, 정정·삭제 요구권, 개인정보의 처리정지 요구권을 명문으로 규정하고 있음
- 정보통신망법은 이용자의 권리로서 열람 요구권, 정정 요구권, 동의철회권을 규정하고 있음
- 개인정보보호법 및 정보통신망법은 개인정보침해와 관련한 손해배상청구권에 대하여도 명문으로 규정하면서 입증책임을 전환하고 있음

### 현황과 문제점

- 개인정보주체 혹은 정보통신망에서의 이용자의 권리를 보장하기 위하여 각종 권리를 명시적으로 규정한 것은 바람직
- 개인정보는 보호만이 필요한 것이 아니라 일상생활이나 경제활동 등 다양한 영역에서 필수적으로 요구되는 것이고 안전한 활용이 함께 고려되어야 할 대상인데, 정보주체의 권리에 대응하는 개인정보를 활용하는 자의 이익이나 공익적 요청을 별로 고려하지 않고 극히 제한적인 예외만을 설정하는 문제가 있음
- 개인정보보호법 상의 손해배상책임 규정은 입증책임 전환과 함께 제한적인 책임감경규정을 두고 있는데, 사실상 면책이 불가능하게 되어 무과실책임과 다를 바 없게 규정하고 있음. 그런데 개인정보보호법 상의 모든 의무와 관련하여 너무 과도한 손해배상책임을 부담시킴으로써 오히려 법의 실효성을 약화시키고 경제활동에 악영향을 주거나 글로벌 스탠다드와 맞지 않는 과도한 규제로 인식될 우려도 존재함

## 주요 내용

- 개인정보주체와 관련한 최근 해외의 논의 동향
  - EU 일반개인정보규정(안) 및 개인정보보호지침(안)에 규정된 잊힐 권리(잊혀질 권리)를 포함한 정보주체의 권리나 손해배상책임과 우리의 개인정보 보호법령의 정보주체의 권리와의 입체적인 비교와 시사점 도출이 필요함

- 개인정보보호법과 정보통신망법 상의 정보주체의 권리에 대한 검토
  - 개인정보보호법은 정보주체의 권리로서 개인정보의 열람청구권, 정정·삭제 요구권, 개인정보의 처리정지 요구권을 명문으로 규정하고 있음. 개인정보보호법 상의 일반적 적용 예외 이외에 개인정보정정·삭제요구권에 대한 구체적인 예외로서는 다른 법령에서 예외를 인정하고 있는 경우에 한함
  - 정보통신망법은 이용자의 권리로서 열람 요구권, 정정 요구권, 동의철회권을 규정하고 있음. 이에 대한 구체적인 예외를 정하고 있지는 않음
  - 개인정보보호법 및 정보통신망법은 개인정보침해와 관련한 손해배상청구권에 대하여도 명문으로 규정하면서 입증책임을 전환하고 있음. 다만, 개인정보보호법은 동법을 준수하고 상당한 주의와 감독을 다한 경우에만 임의적으로 감경받을 수 있도록 규정함
  - 개인정보보호법의 광범위한 적용에 비추어 정보주체의 권리를 명시적으로 규정한 것은 정보주체의 권익보호에는 많은 기여를 하지만, 자칫 충돌될 수 있는 국가나 개인의 상충되는 다른 법익을 저해할 위험성도 상존함


상충되는 다른 법익을 저해할 위험성 상존

## 개선방안

- 정보주체의 권리에 관한 법적 기준을 일원화
  - 정보주체의 권리에 관하여 개인정보보호법과 정보통신망법 등에 중복하여 규정되고 있음
  - 정보주체의 권리에 대한 원칙적인 규정을 개인정보보호법에 두고, 정보통신망법과 같이 특별법 상 예외적인 사유를 규정하거나 권리보호를 강화하는 등의 사유가 존재할 때에 이를 개별법에서 규정하는 방식으로 일반법-특별법의 관계를 명확히 하는 것이 바람직

- 정보주체의 권리의 합리적 보장
  - 해외 입법사례와 우리 국민의 법감정을 고려하여 정보주체의 권리를 합리적인 범위에서 보호하는 방향으로 법을 개선하는 것이 필요함
  - 특히, 개인정보의 '보호'와 '안전한 활용의 보장'의 조화라는 관점에서 개인정보를 활용하는 자의 이익(예, 표현의 자유나 알권리) 중 보호되어야 하는 범위 내에서 정보주체의 권리(특히, 삭제 및 이용정지처리 요구권)를 제한하는 것이 필요함
  - 정보주체의 권리를 실제로 어떠한 내용과 방법, 절차에 의하여 실현할 수 있는지에 대하여 법령에 명확화하는 것이 필요함

- 손해배상책임의 명확화 및 실질화
  - 개인정보침해로 인한 손해배상책임을 실질적인 무과실책임으로 인정하는 개인정보보호법 상의 손해배상책임규정이 과연 현실적인지에 대한 정밀한 재검토가 요구됨
  - 개인정보침해 중 고의적인 유출이나 양도와 같이 무과실책임 혹은 무과실책임화가 필요하다고 인정되는 영역에 대하여도, 엄격한 요건 하에 무과실책임 혹은 입증책임전환을 규정하더라도 제한적인 범위에서 책임을 면책 받을 수 있는 길을 열어두는 것이 요구됨

# 잊혀질 권리와 알 권리의 조화

**구본권**
한겨레신문 온라인에디터

## 현황

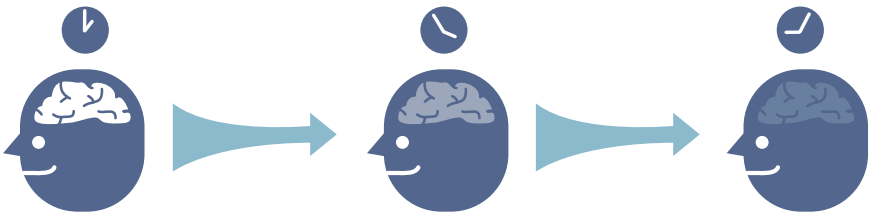
- 디지털화와 인터넷, 소셜네트워크서비스로 인터넷에 한번 등록된 개인적 정보가 지워지지 않고 지속 유통되며 사생활 침해를 일으키는 새로운 프라이버시 문제가 나타나고 있음

- 유럽연합 집행위원회는 2012년 초 인터넷 환경에 맞는 새로운 정보보호 법제인 Data Protection Regulation 개정안을 발표하고 27개 회원국에 입법화하도록 해, '잊혀질 권리'를 도입하기로 했음

- 국내에선 2011년 개인정보보호법에서 개인정보 삭제요구권을 규정해놓은 상태이고, 방송통신위원회는 2012년 9월에 "2013년중 잊혀질 권리 법안을 마련해 법제화 추진" 계획 밝힘

- 스페인, 프랑스, 독일 등 유럽 각국에서는 인터넷 검색 결과와 과거 기사의 인터넷 노출에 대한 관련자의 프라이버시 침해 주장으로 소송이 진행중임

- 구글 등 글로벌 검색사업자와 각국의 정보보호기관은 잊혀질 권리의 법적 권리로서의 타당성과 실효성, 산업적 영향 등을 놓고 첨예하게 대립하고 있음



잊혀질 권리 (right to be forgotten)

## 프라이버시권과 알 권리의 충돌

- ‘현재 통용될 수 없는 과거 기사’의 인터넷 유통

  - 기사의 작성 형태나 취재원이나 보도대상의 개인정보 등에 대한 언론계와 사회적 합의의 기준이 시대와 환경에 따라 달라지고 있음. 과거에는 공인 아닌 일반인이나 범죄 피해자까지 기사에서 실명과 나이, 주소 등을 상세히 기록해왔음. 1998년 대법원의 범죄 보도 실명요건 엄격화와 피의사실 공표 처벌 판결 이후 언론의 범죄 보도 기준이 달라짐. 최근 강력범죄 영향으로 강력범죄 피의자 신상공개 기준도 크게 확대됐음. 인터넷으로 과거 기사 서비스가 이뤄지면서 현재 시점에서는 통용될 수 없는 과거기사(일반인이나 범죄 피해자의 개인적 정보가 노출된 기사)가 손쉽게 검색되고 활용되고 있어 피해가 발생하고 있음. 수십년전 간통 사건에 연루된 사람이나 단순절도 등의 피해자도 인터넷 과거기사 검색에서 손쉽게 노출되어 피해가 발생하고 있으며 피해자의 기사 수정 삭제 요구에 언론사별로 다르게 대응하고 있음

  - 인터넷은 묵은 기사 찾기 같은 정보 검색 기능을 제한된 장소에서 전문가가 수행하던 것에서 만인의 일상생활 속으로 바꿔놓았음. 정보화는 그동안 일시적으로 활용된 이후 정보로서의 생명력을 상실하고 ‘실질적 비공개(practical obscurity)’ 상태가 되어 사실상 잊혀졌던 정보를 언제 어디서나 호출될 수 있는 ‘살아 있는 정보’로 바꿔놓았음


기사 영향력의 시공간적 제한이 사라짐, 피해 한계가 없어짐

- 언론사별 기준의 차이와 가이드라인의 부재

  - 언론 보도 기사는 일간·주간·월간 등 매체의 발행주기와 지역·전국 등 배포지역을 기반으로 특정한 시공간에서만 유효성을 지녔음. 뉴스가치가 특별한 사안이나 공적 인물이 아닌 경우에는 시간의 경과와 더불어 대중의 기억 속에서 자연스럽게 잊혀져 왔음. 인터넷으로 기사 영향력의 시공간적 제한이 사라지고 피해도 한계가 없어졌음. 하지만 관련 법제는 그대로인 까닭에 전에 없던 문제 발생. 회사별로 적용하고 있는 과거 기사나 오보에 대한 수정·삭제 처리 기준을 공론화해서 언론계 공통의 가이드라인 제정 필요

## 대안의 방향

- 표현 자유와 프라이버시 권리의 공존 모색

  - 디지털화 이전의 정보보호 법제로는 소셜네트워크 서비스 환경의 새로운 프라이버시 문제를 해결할 수 없음. 새로운 기술과 사용환경 반영해 프라이버시 개념과 권리를 업데이트하고, 저널리즘의 기능과 표현의 자유가 디지털 환경에 맞추어 새롭게 정의되어야 할 필요성. 정보주체의 권리에 관하여 개인정보보호법과 정보통신망법 등에 중복하여 규정되고 있음

- 입법적 접근 대신 이해주체들의 사회적 합의

  - 급변하는 정보기술은 그 변화가 현재에도 진행형이고 계속 발전해가고 있음. 디지털화 이후 생겨난 변화가 새로운 기기와 서비스 위주에서 앞으로는 문화와 가치체계, 인지구조 등 사회체계 전반의 변화로 확대될 것임. 기술과 서비스의 진화 과정에서 새로이 등장한 문제와 부작용에 대해 진지하게 검토해야 하지만, 성급하게 이를 입법 등으로 근원적으로 해결하겠다는 태도는 바람직하지 않음. 문화 지체 현상의 일종으로 보아 새로운 문제에 대해 포괄적이면서도 지속적이고 유연한 접근이 우선되어야 함. 이를 위해서 문제 해결식의 접근보다는 문제 보고와 그로 인한 개인적, 사회적 영향 위주로 파악이 우선될 필요성

  - 이는 입법보다는 관련 이해 주체들의 논의를 통한 자율적 해결책과 조정이라는 대안이 유연성 측면에서 효과적일 수 있음. 잊혀질 권리가 주로 문제되는 인터넷과 과거 기사의 유통에 대해 한국인터넷 자율정책기구와 한국기자협회, 언론중재위원회 등의 기구를 통해서 자율적 해법과 조정안을 모색하는 것이 요구됨

- 국내 고유 법제 아닌 글로벌 스탠더드와의 부합 모색

  - 잊혀질 권리 또한 인터넷에서의 문제인 만큼 국내에서만 적용되는 입법과 권리로서는 한계가 명확함. 인터넷이라는 글로벌 서비스에 맞게 프라이버시와 인터넷 법제에 관한 글로벌 스탠더드의 기준을 적용할 필요 요청됨

## 개인정보 손해배상소송에 있어서 과실 및 손해 판단기준

권영준, 서울대학교 법학전문대학원 부교수

## 개인정보침해에 대한 형사처벌의 적절성

전응준, 유미IP법률사무소 변호사

# 개인정보 손해배상소송에 있어서 과실 및 손해 판단기준

**권영준**
서울대학교 법학전문대학원 부교수

## 개요

- 대규모 개인정보유출사고들이 자주 발생하면서 개인정보처리자의 불법행위책임 역시 자주 문제되고 있음

- 이와 관련하여 어떤 경우에 개인정보처리자의 과실이 인정되는지, 또한 손해의 인정과 손해배상액의 산정은 어떻게 이루어져야 하는지가 중요한 법적 쟁점들로 부각됨

- 이러한 쟁점들에 대해서 입법으로 구체적인 판단기준을 제시하는 데에는 한계가 있을 수밖에 없음. 과실이나 손해에 대한 판단은 본래 사안중심적 성격이 강하기 때문임

- 그러므로 이는 재판례와 학술적 노력이 함께 축적되어 가면서 구체화해 나가야 할 문제임. 그러나 아직은 그러한 구체화의 노력이 충분히 진행되었다고 할 수 없음

## 주요 내용

- 현행법상 개인정보처리자의 불법행위책임은 과실책임임. 한편 관련 행위주체들의 예견가능성을 높여 최적의 행위를 유도하고 이를 통해 개인정보보호의 실효성을 높이기 위해서는 개인정보처리자의 주의의무를 구체화하는 작업이 필요함

  - 과실책임주의 하에서 주의의무는 그 이행에 대한 합리적 기대가능성을 전제로 함. 그러므로 무엇이 “합리적”인 이행인가에 대해 비용/편익 분석의 관점에서 접근할 필요가 있음

  - 개인정보처리자의 주의의무는 이론상 법령뿐만 아니라 조리나 신의칙 등 여러 가지 근거에 기하여 발생할 수 있음. 그러나 현행 개인정보보호법의 포괄성과 망라성에 비추어 볼 때 개인정보처리자의 주의의무는 특별한 사정이 없는 한 법령상 주의의무와 일치시키는 것이 타당함

- 개인정보유출과 관련된 개인정보처리자의 법령상 주의의무는 크게 안전조치의무와 사후조치의무로 구분할 수 있음. 한편 안전조치의무는 크게 기술적 조치의무와 관리적 조치의무로 구분할 수 있음

- 이러한 주의의무 위반 여부를 판단할 때 구체적으로 고려할 요소들로서는 내부적 고려요소(개인정보처리자의 통제영역 안의 고려요소), 외부적 고려요소(개인정보처리자의 통제영역 밖의 고려

- 요소), 기타 고려요소(개인정보 처리업무 위탁시의 고려요소)를 상정할 수 있음. 이러한 각 고려 요소와 주의의무 판단의 상관관계를 분석하여 가이드라인을 제공할 필요가 있음

○ 한편 개인정보처리자는 과실이 인정되는 등 불법행위 성립요건을 갖추게 되면 손해배상책임을 부담함 그런데 어느 정도에 이르러야 손해가 발생한다고 인정될 수 있는지, 그 손해액은 어떻게 산정하는지가 문제됨. 특히 개인정보유출사고에서는 대부분 위자료 배상과 관련하여 위와 같은 의문점들이 제시되고 있어 이에 대한 판단기준의 구체화 작업이 요구됨

- 우선 어느 정도의 단계에 이르러야 정신적 손해가 발생하였다고 볼 수 있는지가 불명확함. 우리나라는 일반적으로 정신적 손해를 넓게 인정하되 위자료 액수는 낮게 인정하는 경향을 보여 왔음. 이러한 입장이 타당한지, 특히 대규모 개인정보유출사고에 있어서 그대로 적용될 수 있는 것인지에 대한 재고가 필요함. 최근 우리나라 재판례들은 정신적 손해의 인정기준의 확립을 위한 의식적인 노력을 기울이고 있음

- 한편 일단 정신적 손해가 발생하였다고 인정되면 구체적인 위자료 산정작업이 진행됨. 위자료 산정에 있어서는 피해자측 요소(침해단계, 침해범위, 침해대상, 정보의 정확성, 개인식별가능성, 약용 여부, 재산적 손해의 입증 곤란정도, 피해자의 과실 등)와 가해자측 요소(침해태양, 가해자의 특성과 지위, 동기와 경위 정보의 필요성, 행위 이후의 사정)가 고려되어야 함

## 개선방안

- 표현 자유와 프라이버시 권리의 공존 모색
  - 본 주제의 특성상 입법을 통한 구체적인 기준 확립에는 한계가 있을 수밖에 없음. 과실과 손해판단의 구체적 기준에 대한 공감대가 형성된다면 이를 입법에 반영할 여지가 있겠으나 이러한 형성과정까지는 상당한 시간이 경과할 것으로 생각됨

- 재판례가 축적되면서 자연스럽게 판단기준이 형성되겠지만, 이를 위해서는 상당수의 분쟁이 일어나고 이에 대한 장기간의 재판이 진행되어 그 재판례들이 일정한 방향성을 획득하여야 하는 것임

- 그러므로 이에 앞서서 관련 분야 전문가들이 우리나라 개인정보보호의 현실과 관련된 분쟁사례, 외국의 입법례 등을 참조하여 과실과 손해 판단기준을 가급적 구체화함으로써 개인정보에 관련된 행위주체들, 나아가 법원에 일정한 가이드라인을 제공하기 위한 지속적인 시도가 있어야 함

# 개인정보침해에 대한 형사처벌의 적절성

**전응준**
유미IP법률사무소 변호사

## 개요 및 현황

- 우선 개인정보침해행위에 대하여 형사처벌이 반드시 필요한가에 대한 기본적인 고민이 필요함
  - 침해되는 개인의 권리가 무엇이고, 형벌의 보충성 원칙의 관점에서 이를 구제하기 위한 다른 민사적, 행정적 조치가 부재한 것인지, 그리고 이러한 형사적 제재에 의하여 일반예방적 및 특별예방적 효과가 달성되는 지 검토되어야 함

- 악의적이고 중대한 개인정보침해행위에 대하여 형사처벌이 필요하다고 하다면, 그 처벌의 범위와 정도가 문제됨
  - 현행 법령은 법위반행위의 거의 모든 행위에 대하여 형사처벌을 규정하고 처벌수준을 일반 형법상의 중요 범죄와 동일하게 취급하고 있음
  - 현개인정보에 관한 정의와 관련하여 범죄구성요건의 명확성원칙, 처벌의 비례성이 문제됨

- 개인정보보호 관련 법령 내에서도 처벌의 불균등성이 존재함
  - 동일 사안에 대하여 개인정보보호법, 정보통신망법, 위치정보법 간의 형사처벌의 내용이 다른 경우가 있음

## 주요 내용

- 먼저, 현행 법령에서 정의한 '개인정보'는 형사처벌의 관점에서 매우 불완전한 개념임
  - 개인에 대한 식별가능성을 개인정보의 지표로 삼은 것은 다른 입법례 등을 고려할 때 부당하다고 할 수 없으나 이를 범죄구성요건의 일부분으로 할 때에는 죄형법정주의의 명확성 원칙을 해친다고 할 수 있음

- 이러한 우려는 법원이 침해자가 수집한 IMEI, USIM 일련번호에 관하여 그 자체로는 개인을 식별하는 것이 아니나 이동통신사의 DB에 있는 다른 정보와 결합하면 개인을 특정할 수 있다는 이유를 들어 개인정보로 판시하고 이를 무단수집한 행위에 대하여 유죄를 인정하면서 현실화되었음

- 침해자가 현실적으로 타인이 보유한 DB정보를 취득할 수 있는 지 여부를 불문하고 추상적인 결합가능성만으로 개인정보임을 인정하는 것은 개인정보의 범위가 제한없이 확대되므로 부당함

○ 적어도, 범죄구성요건의 관점에서는 '개인정보'의 범위가 보다 명확하여야 하고 축소되어야 함

- 영국 데이터 보호법(1998)과 같이 '정보관리자가 보유하고 있거나 보유하게 될 가능성이 높은 데이터(those data and other information which is in the possession of, or is likely to come into the possession of, the data controller)'를 기준으로 개인에 대한 식별가능성을 판단하는 것이 바람직함

○ 현행 법령체계는 개인정보보호법(관련 정보통신망법 등 포함)을 위반한 거의 모든 행위에 대하여 형사처벌을 규정하고 있는바, 이러한 처벌범위는 다른 입법례에서 발견하기 어려움

- 처벌의 수준도 일반 형법의 그것에 비하여 결코 낮지 아니함. 정보주체의 동의없이 개인정보를 제3자에게 제공한 경우 5년이하의 징역 내지 5,000만원 이하의 벌금형에 처하게 되어 있는데, 이는 명예훼손죄, 업무상 비밀누설죄보다 높고 배임죄, 영업비밀누설죄와 유사한 정도임. 법정형의 관점에서 보면, 현행 개인정보침해죄는 개인정보를 영업비밀과 유사하게 보면서 개인정보처리자의 개인정보유출행위를 배임적 행위로 보는 것임


○ 동일한 행위에 대하여 법령에 따라 다르게 규율하거나, 다른 개인정보에 비하여 위치정보침해에 대하여 형사적으로 과잉보호하는 것이 발견됨

- 정보주체의 동의없이 개인정보를 수집하는 행위는 정보통신망법에서는 형벌의 대상이나 개인정보보호법에서 과태료의 대상임(정보통신망법 제71조 제1호, 개인정보보호법 제75조 제1호)

- 개인정보에 해당하지 않는 '물건 및 식별되지 않는 개인에 관한 위치정보'도 형사처벌의 대상으로 삼고 있음

- 단순히 기술적, 관리적 조치를 취하지 않는 행위는 개인정보보호법, 정보통신망법에서는 과태료 부과대상이나, 위치정보법에서는 형사처벌의 대상으로 되어 있음

## 개선방안

- 죄형법정주의 관점에서 '개인정보'의 범위를 명확히 하거나 축소하여야 함

  - 대부분의 입법례가 개인을 식별할 수 있는 일체의 정보를 개인정보로 보고 있으나, 개인정보침해를 형사처벌하는 관점에서는 개인을 구체적으로 식별하는 정보로 명확히 하여야 함

  - 죄형법정주의상 개인정보 정의의 문제점은 '다른 정보와 결합되어 개인을 식별할 수 있는 정보'의 범위가 불명확하다는 것에 있으므로, 특정 개인을 식별하는 자료의 범위를 당해 개인정보처리자가 보유하고 있거나 보유할 개연성이 높은 자료로 한정하고, 사업적 제휴관계, 정보시스템의 연결관계 등이 존재하지 않아 접근(보유)가능성이 없는 정보는 다른 정보와 결합가능성이 없다고 해석하는 것이 바람직함

- 범죄구성요건에 관하여, 일본, 영국과 같이 법위반시 시정조치를 명하고 이를 위반하는 행위에 대하여 형사적 제재를 가하는 방법을 제안함(일본 개인정보보호법은 시정조치 위반시 6월이하의 징역 또는 30만엔이하의 벌금)

  - 개인정보보호에 대한 의무위반행위는 그 범의의 정도, 행위의 내용, 피해의 수준 등이 매우 다양하므로 이를 일률적으로 직접 형사처벌하는 것보다 주무관청의 시정조치에 의하여 실질적인 피해회복을 꾀하도록 하고 이러한 시정조치를 위반하는 행위에 대하여 형사처벌을 가하는 것이 정책적으로 바람직하다고 판단됨

- 개인정보보호법, 정보통신망법, 위치정보법상의 법정형을 비례적으로 조정함

# 개인정보보호법이 의학 및 보건학 연구에 미치는 영향

박병주, 서울대학교 의과대학 예방의학교실 교수

# 개인정보보호법이 의학 및 보건학 연구에 미치는 영향

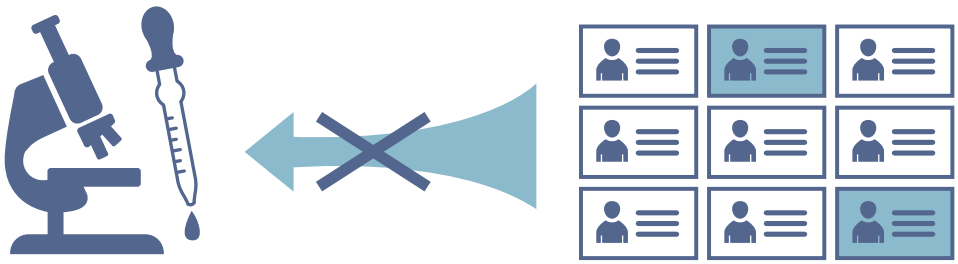
**박병주**
서울대학교 의과대학 예방의학교실 교수

## 배경 및 필요성

- 2008년 개정 헬싱키선언을 통하여 의학연구의 기반이 되는 윤리적 기준을 선언함
  - 개인식별이 가능한 자료를 이용한 연구를 수행할 경우 연구대상자의 동의가 필요함을 명시함
  - 동의획득이 불가능한 후향적 관찰연구 등은 연구윤리심의위원회(Institutional Review Board, IRB)의 검토 및 승인 후에만 연구수행이 가능하도록 규정하고 있음
  - 하지만 연구윤리심의위원회의 승인과 개인정보보호법의 법률적 책임은 다름

- 2011년 9월 개정 개인정보보호법이 발효되었으며, 이에 따라 의학연구를 수행할 경우 해당 법률의 내용을 준수하여야 함
  - 개인정보보호법의 제정에 따라 전향적 연구에 대하여는 예외조항이 적용되어 법률적 문제가 발생하지 않으나, 대규모 전산자료를 이용한 후향적 관찰연구 수행 시 연구에 제한이 발생함
  - 원칙적으로 후향적 관찰연구를 위한 자료의 제공이 금지되며, 익명화 처리되는 경우 예외가 인정되나, 이러한 익명화 자료를 이용할 경우 연구수행이 제한적이고 질적 수준이 낮음. 따라서 개인식별을 통한 자료연계를 이용한 질 높은 후향적 관찰연구의 경우 합법적 연구수행이 불가능함

- 국내외 개인정보보호법의 제정이 의학연구에 미치는 영향에 대한 문헌검토 및 고찰로 대응방안 모색이 필요함



개인식별 자료연계를 이용한 후향적 관찰연구의 경우 합법적 연구수행이 불가능

## 미국의 HIPAA법의 의학 및 보건학 연구에 미치는 영향과 국내 현황

- 20미국은 진료기록의 이전과 지속성을 개선하여 오남용을 방지하는 것을 목적으로 건강보험 이전과 책임에 관한 법률(Health Insurance Portability and Accountability Act, HIPAA)을 제정하였으며, 이에 따라 개인정보보호를 위하여 2003년 프라이버시 룰(Privacy Rule; Standard for Privacy of Individually Identifiable Health Information)을 발표함

- HIPPA법의 제정에 따라 의학연구수행에 많은 제한점이 발생한 것에 대한 미국 내 여러 역학연구 기관들의 조사결과가 발표됨
  - 개인식별자가 제거된 자료에 대한 접근의 어려움
  - 기관별 연구윤리심의위원회의 프라이버시 룰에 대한 견해 차이
  - 연구윤리심의위원회의 심의절차 및 소요시간 증가
  - 연구대상자 모집, 연구기간, 연구비용 증가, 연구오류 증가
  - 연구자의 연구수행 포기사례 증가

- 국내 연구자들을 대상으로 개인정보보호법이 연구에 미친 영향을 직접 조  사한 결과는 부재하나 국외에서 조사된 상황과 유사할 것으로 추정됨

- 국내 개인정보보호법(18조 4)의 익명화 처리 후 통계작성 및 연구 활용 허용의 문제점
  - 익명화 처리방법에 대한 구체적인 지침 부재
  - 공공기관자료간 연계를 통한 분석은 현실적으로 불가능

## 개선방안

- 2007년 미국 FDA법률개정안(FDA Amendments Act, FDAAA) ‘센티넬 이니셔티브(Sentinel initiative)’ 및 비교효과연구(Comparative Effectiveness Research, CER) 수행을 위한 제도적 지원

- 약화사고 예방과 건강증진과 같은 공익적 목적의 연구에 대한 특별법 제정
- 공공기관이 보유한 전산자료들의 통합을 위한 제도적 지원책 마련
- 약화대규모 전산데이터베이스를 활용한 대규모 관찰연구 활발히 수행

- 유럽 EMA에선 능동적 약물감시시스템인 엔셉 (European Network of Centres for Pharmacoepidemiology and Pharmacovigilance, ENCePP) 수행을 위한 제도적 지원
  - ENCePP은 27개 유럽연합 회원국의 89개 연구기관이 참여하는 범유럽연구 네트워크로 13개의 대규모 전산자료를 통합하는 연구를 수행하기 위해 유럽연합 차원의 법률 권고안을 고안하여 각국의 국내법에 적용함

- 개인식별정보 제거를 통한 익명화 시의 자료연계에 대한 제도적 보완
  - 미국의 경우 프라이버시 룰 제정 이전인 1988년 컴퓨터연계 및 프라이버시보호법(The Computer Matching and Privacy Protection Act)을 제정하여 자료연계와 관련된 이슈들에 대한 법률적 대책 마련
  - 미국 프라이버시 룰은 익명화 후에도 자료연계를 위하여 개인식별자를 보관할 수 있도록 허용
  - 개인정보보호법에서도 자료연계와 관련된 이슈들에 대한 법률적 대책과 구체적인 지침을 제시할 현 법령의 제도적 보완이 절실히 필요함

- 연구윤리심의위원회(IRB)의 역할 강화
  - 미국의 경우 대규모자료 연계연구에서 개인별 동의서를 받기 힘든 경우, IRB를 통해 연구의 과학적, 윤리적 타당성을 심의하고, 연구에 의한 공익성 여부, 이득과 위해의 균형을 따져 연구의 필요성을 평가하고 있음
  - 국내에서도 IRB에서 대규모자료의 연구필요성에 대한 평가와 심의가 가능하도록 명시하여야 함
  - 국가생명윤리정책연구원에서 IRB의 공정한 심의를 위한 지침서를 개발하여 제공하도록 함

- 개인정보보호법 개정등의 제도적 개선을 통하여 빅데이터를 활용한 과학적 근거창출을 활성화하여 이를 근거로 보건의료정책 수립 수준을 선진화하여 국민건강 증진에 기여하도록 함

## 개인정보보호법제 정책제안서 저자 프로필

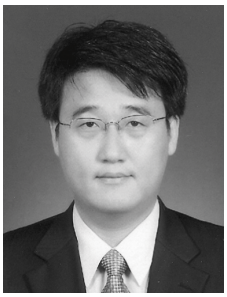
**문재완**

현직 : 한국외국어대 법학전문대학원 교수
전공 : 헌법
관련 : 언론법, 개인정보법, 정보통신법
저서 : 언론법-한국의 현실과 이론-(2008), 정치적 소통과 SNS(2012, 공저)
학력 : 서울대 법학사, 인디애나대 로스쿨(LL.M., SJD),
경력 : 사이버커뮤니케이션학회 회장, 미디어발전국민위원회 위원,
제19대 국회의원선거 선거방송심의위원회 부위원장
전자우편 : conlaw@hufs.ac.kr



**황성기**

현직 : 한양대 법학전문대학원 교수
전공 : 헌법
관련 : 언론법, 정보법
저서 : 인터넷은 자유공간인가?(2003, 공저)
학력 : 서울대 법학박사
경력 : 헌법재판소 헌법연구원
전자우편 : sghwang@hanyang.ac.kr


**고학수**

현직 : 서울대 법학전문대학원 교수
전공 : 법경제학
관련 : 과학기술과 방송통신의 법경제학, 공정거래
저서 : 경제적 효율성과 법의 지배(2009, 공편저)
학력 : 서울대 경제학사, 컬럼비아대 로스쿨(JD), 컬럼비아대 경제학과(PhD)
경력 : 방송통신위원회 자문위원, 법무부 자문위원
전자우편 : hsk@snu.ac.kr



**구태언**

현직 : 테크앤로 법률사무소 대표변호사
전공 : 법학, 정보보호
관련 : 전자거래법, 개인정보법, 정보통신법, 지식재산권법
저서 : 개인정보보호 실천가이드(2011)
학력 : 고려대 법학사, 동 정보보호대학원 석사수료
경력 : 국가정보화전략위원회 법제도 전문위원, 행정안전부 개인
정보보호법령 해석 자문위원, 개인정보보호위원회 자문변호사
전자우편 : taeeon.koo@teknlaw.com


## 이인호

현직 : 중앙대 법학전문대학원 교수
전공 : 헌법
관련 : 언론법, 개인정보법, 정보통신법
저서 : 사이버공간상의 표현의 자유(2002, 공저)
학력 : 중앙대 법학박사
경력 : 헌법재판소 헌법연구관보, 대법원 재판연구관(전문직),
국회입법지원위원, 중앙행정심판위원
전자우편 : inho61@cau.ac.kr

## 김기창

현직 : 고려대 법학전문대학원 교수
전공 : 민법, 로마법
관련 : 인터넷 정책, 보안 기술
저서 : 한국웹의 불편한 진실(2009)
학력 : 서울대 법학사, 시카고대 로스쿨(LL.M.), 캠브리지대(PhD)
경력 : 국회입법조사처 문화방송통신 자문위원, 인증방법평가위원회 위원
전자우편 : keechang@korea.ac.kr

## 박광배

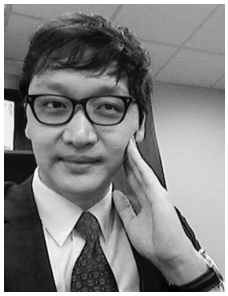
현직 : 법무법인 광장 파트너 변호사
전공 : 법학
관련 : 정보통신법, 개인정보법, 방송법
저서 : "The International Comparative Legal Guide to : Telecommunication Laws and Regulations 2011 Korea Chapter", co-author Yu Jin Kim, Global Legal Group "컴퓨터소프트웨어의 국제적 거래와 조세법규의 적용, 인권과 정의, 1994.4.(통권 212호)
학력 : 서울대 법학사, 조지타운대 로스쿨(LL.M.)
경력 : 방송통신위원회 고문변호사, 행정안전부 개인정보국제협력 자문위원,
대한상사중재원 중재인, 정보통신부 소프트웨어사업 분쟁조정위원회
조정위원
전자우편 : kwangbae.park@leeko.com

## 박경신

현직 : 고려대 법학전문대학원 교수
전공 : 헌법, 미국법
관련 : 국제계약, 저작권, 엔터테인먼트, 공정거래법
저서 : 논문집 〈표현의 자유, 통신의 자유〉(2013 예정), 〈진실유포죄〉(2012),
〈사진으로 보는 저작권, 초상권, 상표권 기타등등〉(2007),
〈영화, 드라마 뉴스 만들기 100문 100답〉(2007)
학력 : 하버드대 물리학사, UCLA로스쿨 (JD)
경력 : 방송통신심의위원회 위원, 서울시학생인권위원회 위원,
미디어국민위원회 위원
전자우편 : kyungsinpark@korea.ac.kr

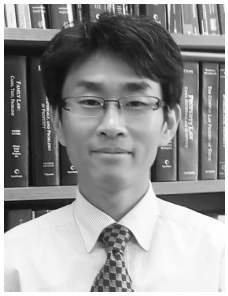
**박상철**

현직 : 김·장 법률사무소 변호사
관련 : 방송통신, 인터넷, 공정거래, 광고법
학력 : 서울대 법학사, 시카고대 로스쿨(LL.M.)
경력 : Associate, Herbert Smith LLP, London
전자우편 : scpark@kimchang.com


**최경진**

현직 : 가천대학교 법과대학 교수
전공 : 민사법
관련 : 전자거래법, 개인정보법, 방송통신법, 인터넷법
저서 : 로스쿨 민법사례연습I, II(2011, 공저), 전자상거래와 법(1998)
학력 : 성균관대학교 법학박사, 듀크대학교 로스쿨(LL.M.)
경력 : 가천대학교 법학연구소 소장, 국가정보화전략위원회 법제도 전문위원,
금융위원회 FTA에 따른 DATA 해외위탁 T/F 총괄반 위원,
행정안전부 개인정보보호 법령 해석 자문위원
전자우편 : kjchoi@gachon.ac.kr

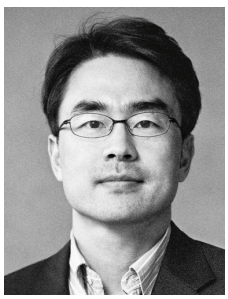

**구본권**

현직 : 한겨레신문 온라인에디터
전공 : 저널리즘
관련 : 저널리즘, 프라이버시
저서 : 인터넷에서는 무엇이 뉴스가 되나(2005), 잊혀질 권리(2011, 역)
학력 : 서울대학교 철학과, 한양대학교 박사수료(저널리즘)
경력 : 한겨레신문 기자, 한양대학교 신문방송학과 겸임교수, 경희사이버대 강사
전자우편 : starry9@hani.co.kr



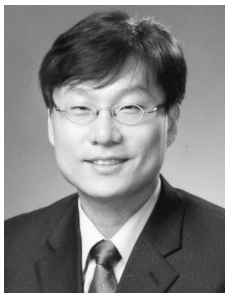
**권영준**

현직 : 서울대학교 법학전문대학원 교수
전공 : 민법
관련 : 민법이론, 지적재산권법
저서 : 저작권침해판단론(2007), 권리의 변동과 구제(2011,공저),
Law and Legal Institution in Asia (2012, 공저) 등
학력 : 서울대학교 법학사, 법학석사, 법학박사, 하버드대학교 로스쿨(LL.M.)
경력 : 판사, 법무부 법무자문위원, 민법개정위원, UNCITRAL 정부대표,
저작권위원회 위원, 서울대학교 기술과 법 센터장 등
전자우편 : youngjoon@snu.ac.kr

**전응준**

현직 : 유미IP법률사무소 대표변호사
전공 : 컴퓨터사이언스, 통계학
관련 : 지적재산권법, IT법, 개인정보법
저서 : Privacy Dictionary(2012, 공동저자)
학력 : 서울대학교 계산통계학과(이학사)
경력 : 유미특허법인 변리사, 중앙대학교 법과대학 겸임교수
전자우편 : ejjeon@youme.com



**박병주**

현직 : 서울대학교 의과대학 교수 / 한국의약품안전관리원 원장
전공 : 예방의학
세부전공 : 임상역학, 약물역학
저서 : 약물역학, 과학적 증거에 기반한 임상예방의료, 예방의학과 공중보건학
학력 : 서울대학교 의학사, 서울대학교 보건학 석사, 서울대학교 의학박사
경력 : 한국역학회 회장, 대한보건의료기술평가학회 회장, 서울의대/서울대병원 IRB위원장, 서울의대/서울대병원 의학연구협력센터 센터장, 대한민국 의학한림원 정회원, 복지부/식약청 중앙약사 심의위원회 위원
전자우편 : bjpark@snu.ac.kr

개인정보보호법제 개선을 위한

# 정책연구보고서

2013. 2

프라이버시 정책연구 포럼

# 〈목 차〉

# 프라이버시 보호: 신화에서 규범으로

한국외대 법학전문대학원 교수 문재완

## Ⅰ. 문제의 제기

정보화 시대가 되면서 프라이버시 침해를 우려하는 목소리가 점점 커지고 있다. 정보통신기술의 급속한 발전은 정치 경제 사회 문화 등 시민의 모든 생활을 혁명적으로 개선시켰지만, 부정적 측면도 나타난다. 평범한 사람의 일상적 움직임도 사회 곳곳에 설치된 정보통신기기에 기록되면서 시민은 프라이버시를 기대하기 어렵게 되었다. 세계 각국은 이러한 문제를 해결하기 위하여 법과 제도를 정비하고 있다. 우리나라 역시 개인정보를 보호하는 법제를 마련하였다. 특히 2011년 3월 29일 제정된 개인정보보호법은 개인정보의 수집 유출 오용 남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위한 목적으로 제정되었다.

하지만 우리나라에서 프라이버시 보호, 특히 개인정보 보호는 신화가 되었다. 프라이버시가 무엇을 의미하는지, 무엇을 보호하고자 하는 것인지, 어떻게 보호할 수 있는지에 대해서 충분히 논의하지 못한 채 법으로 강요되고 있다. 프라이버시는 보호하면 할수록 좋고, 보호수단을 많이 마련할수록 좋고, 위반에 대해서 엄하게 다스릴수록 좋다는 막연한 믿음, 즉 신화가 우리 사회를 지배한다. 개인정보보호법은 보호라는 명분 아래 개인과 기업의 활동을 과도하게 규제하고 있다. 개인정보 보호, 나아가 프라이버시 보호에 대한 냉철한 접근이 필요한 시점이다. 프라이버시를 보호하자는 이상을 추구하는 것은 바람직한 일이지만, 다른 가치에 대한 고려 없이 프라이버시는 보호하면 할수록 좋은 것이라는 맹목적인 태도는 지양하여야 한다.

신화가 아닌 현실의 프라이버시 보호라는 관점에서 살펴보면, 보호라는 명분으로 시행하는 법제 강화가 반드시 좋은 것만은 아니다. 그 이유는 첫째, 개인정보 보호 강화가 다른 헌법적 가치, 즉 알 권리, 표현의 자유, 영업의 자유 등에 대한 침해로 나타날 수 있기 때문이다. 개인정보 보호 입법에서는 서로 충돌하는 헌법적 가치들을 조화롭게 해결하는 방법을 찾는 일이 가장 중요하다. 조화로운 해결을 위해서는 개인정보 보호의 가치와 목적을 분명하게 성찰할 필요가 있다. 둘째, 개인정보 보호를 강화하는 법제는 자칫 잘못하면 개인정보 보호를 최고의 헌법적 가치로 오인하여 개인정보 보호라는 이름 아래 이루어지는 모든 조치를 정당한 것으로 간주하는 잘못으로 이어질 수 있다. 과연 이러한 과오가 실제로 발생하고 있는지 확인하기 위해서 개인정보 보호 법제에 수용된 각종 수단들이 얼마나 효율적으로 개인정보를 보호하는지 살펴볼 필요가 있다. 셋째, 개인정보 보호의 법제가 반드시 프라이버시 보호라는 현실적 결과로 이어지는 것도 아니다. 개인정보 보호라는 목표는 법으로만 달성할 수 있는 것이 아니라, 프라이버시를 존중하는 사회문화가 형성될 때 비로소 가능한 것이다. 일상생활에서 '다른 사람의' 프라이버시를 경시하는 사회에서, 개인정보 보호의 법제만 강화될 경우 '자신의' 개인정보만 중시하는 현상만 나타나고 한 사회 전체의 프라이버시 보호 수준은 향상되지 않을 수 있다.

중요한 것은 법제를 제대로 강화하는 것이다. 개인정보 보호, 나아가 프라이버시 보호는 공공부문과 민간부문을 구분하여 접근하는 것이 타당하다. 하지만 개인정보보호법은 두 부문을 동일하게 취급함으로써 개인정보 보호의 이슈가 공공부문에서 민간부문으로 이전하는 착시현상을 일으킨다. 공공부문은 공공기관과 사인간의 불균형적 권력관계에서 공권력에 의해 사인의 자유가 일방적으로 침해될 우려가 있는 영역이고, 민간부문은 사인과 사인의 대등한 관계

를 전제로 하지만 정보통신기술의 발전으로 자신도 모르는 새 또는 경제력 차이로 비자발적 동의 아래 사인의 자유가 침해될 수 있는 영역이다. 이 중 개인의 사생활 침해가 크게 우려되는 영역은 공공부문이다. 어느 나라에서나 개인정보 보호 법제는 기술 발달로 개인의 일거수일투족이 국가의 감시 하에 놓이면서 발생하는 개인의 자유 침해를 방지하기 위한 목적에서 시작되었다. 민간부문의 급속한 성장으로 인터넷서비스사업자 등 사기업에 의한 개인정보 침해 역시 심각해지고 있는 것은 사실이다. 그럼에도 불구하고 개인정보 보호 법제의 근간은 여전히 개인의 사생활 영역에서 공권력에 의한 자유 침해를 방지하고, 개인이 자유를 향유하도록 보장하는 데 있다.

공공부문과 민간부문을 구분해서 접근해야 하는 근본적인 이유는 영역별로 프라이버시 법제가 추구하는 목적과 수단이 다르기 때문이다. 공공부문에서는 개인의 프라이버시를 최대한 보장하기 위하여 공권력 행사를 최대한 통제하는 방향으로 법제가 마련되어야 한다. 즉 프라이버시의 최대 보장이 목적이고, 불가피한 사정으로 프라이버시를 제한하더라도 그 피해를 최소화하는 수단이 사용되어야 한다. 하지만, 민간부문에서는 대립되는 두 자유, 즉 한 쪽 사인의 프라이버시와 다른 한 쪽 사인의 표현의 자유 또는 영업의 자유 사이의 조화와 균형을 이루기 위해서 두 자유의 가치를 비교형량한 후  덜 중요한 자유를 제한하는 방법으로 법제화되어야 한다. 따라서 프라이버시의 최대 보장이 목적이 될 수 없으며, 프라이버시와 다른 자유의 조화와 균형이 목적이 되어야 한다.

문제는 표현의 자유, 영업의 자유와 같은 전통적 자유에 대해서는 그 헌법상 가치와 개념이 충분히 검토되었지만, 프라이버시와 같은 현대적 자유에 대해서는 그렇지 못하다는 데 있다. 프라이버시란 무엇인지, 프라이버시가 헌법상 권리인지, 프라이버시와 개인정보 보호와의 관계는 무엇인지, 개인정보자기결정권이 보호하고자 하는 것은 무엇인지, 개인정보의 헌법상 개념은 무엇인지 등에 대해서 사회 구성원 사이에 공감대를 형성하는 답은 현재 없다. 프라이버시 및 개인정보자기결정권의 성격에 대한 사회적 공감 없이 이루어지는 법제화는 프라이버시를 신화화하는 것이다. 프라이버시 보호가 제대로 이루어지기 위해서는 프라이버시와 개인정보자기결정권의 본질에 대한 연구가 선행되어야 한다.

# Ⅱ. 프라이버시에 대한 올바른 이해

## 1. 프라이버시를 보는 두 개의 시각

프라이버시를 바라보는 시각에 있어서 미국과 유럽의 차이는 크다. 예컨대 형사재판기록의 경우 미국에서는 공적 정보이기 때문에 프라이버시의 대상이 되지 않는다고 보고 있지만, 유럽에서는 그렇지 않다. 예컨대, 스위스 연방법원은 1983년 Société Suisse 사건에서 1939년 사형을 선고받고 집행된 한 범죄인의 사연을 TV 다큐멘터리로 방영하지 못한다고 선고한 적이 있다.[1] 다큐멘터리는 공문서와 생존자의 회고에 기초하여 제작되었지만, 법원은 범죄인의 신원에 관한 대중의 알 권리는 일정 시간이 흐르면 사라지고, 범죄인의 잊혀질 권리가 알 권리에 우선한다고 판단하였다.

유럽의 경우 프라이버시권의 보호이익은 개인의 인격권 보호에 있다고 본다. 인격권은 인간의 존엄성(human dignity)을 보호하는 데 있어서 필요한 '개인의 사생활영역' 및 '자유로운 인격발현의 기본여건'을 보장하는 것을 그 내용으로 한다.[2] 전자의 인격권이 '사생활의 보

1) X v. Société de Radio et de Télévison, BGE 109 Ⅱ 353 (1983).
2) 한수웅, 헌법학, 법문사, 2012년, 540~58쪽; 박용상, 명예훼손법, 현암사, 2008년, 388~89쪽.

호'이고, 후자의 인격권이 '사회적 인격상에 관한 결정권'(right to control one's public image)이다.[3] 사회적 인격상에 관한 결정권은 자유로운 인격발현의 기본여건으로 사회에서 다른 사람에게 비춰지는 자기 모습을 보장하는 권리다. 자신에 관한 정보를 자기가 결정할 수 있다는 개인정보자기결정권은 그 핵심내용이다. 결국 유럽이 보는 프라이버시권의 핵심은 개인정보자기결정권에 있으며, 원하지 않는 언론 보도로 인하여 일반인의 사회적 평가가 훼손되는 상황을 우려한다.

이에 반하여 미국에서는 공권력에 의하여 개인의 자유(liberty)가 침해되는 상황을 가장 우려한다. 프라이버시권의 핵심은 여전히 국가에 의하여 가정의 신성함(sanctity of home)이 침해받지 않도록 방어하는 데 있다. 가정 안에서 벌어지는 사안에 대해서는 개인 또는 가족의 자기결정권을 철저하게 보호하려고 한다. 유럽과 달리 언론에 의한 프라이버시 침해는 크게 우려하지 않는다. 언론의 자유를 절대적으로 보호하여야 한다는 인식이 더 강하기 때문이다. 결국 프라이버시의 가치를 미국에서는 자유에서 찾는 데 반하여, 유럽 국가들은 인간의 존엄성에서 찾고 있다고 하겠다.[4]

## 2. 미국 프라이버시법의 발전

미국에서 프라이버시법은 가정(home)이라는 사적 공간에 대한 보호에서 시작되어, 의사결정의 자율성 보장, 자기정보 결정권 등으로 발전하고 있는 중이다.[5]

### 가. 혼자 있을 권리(right to be let alone)

프라이버시권은 1890년 워렌(Samuel Warren)과 브랜다이스(Louis Brandeis)가 공동으로 작성한 논문, '프라이버시에 대한 권리'(The Right to Privacy)가 하버드대학 법률잡지에 게재되면서 주목받기 시작하였다.[6] 워렌과 브랜다이스는 위 논문에서 기술과 사업 모델의 발전으로 '혼자 있을 권리'(right to be let alone)를 보호하여야 할 필요성이 생겼다고 주장하였다.[7] '혼자 있을 권리'란 집과 같은 사적 공간의 보호를 의미하였다. 미 연방대법원이 음란물의 사적 소유를 형사처벌하는 법률을 위헌으로 선고하면서, "자기 집에 혼자 앉아 있는 사람이 어떤 책을 읽든, 어떤 영화를 보든 국가가 상관할 일이 아니다"라고 판시한 것은 이를 잘 설명하고 있다.[8]

### 나. 의사결정의 자유(decisional privacy)

사생활에 관한 의사결정의 자유가 주목받기 시작한 것은 인권운동이 한창이던 1960년대 중반이다. 사법적극주의자로 유명한 워렌(Earl Warren)이 대법원장이었던 1965년 미국 연

3) 한수웅, 위의 책, 541쪽.
4) Edward J. Eberle, DIGNITY AND LIBERTY: CONSTITUTIONAL VISIONS IN GERMANY AND THE UNITED STATES (2002); Robert C. Post, Three Concepts of Privacy, 89 Geo. L.J. (2001).
5) 프라이버시 개념 변화에 대해서는 노동일·정완, "사이버공간상 프라이버시 개념의 변화와 그에 대한 법적 대응방안", 「경희법학」 제45권 제4호, 2010 참고.
6) Samuel Warren & Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890).
7) 혼자 있을 권리는 쿨리(Thomas Cooley) 판사가 처음 만들어 낸 용어다. Thomas Cooley, LAW OF TORTS (2d ed. 1888).
8) Stanley v. Georgia, 394 U.S. 557 (1969) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.").

방대법원은 Griswold 사건에서 피임약의 사용을 금지한 코네티컷 주 법률을 위헌이라고 판시하면서 그 논거로 프라이버시 침해를 들었다.[9] 프라이버시권은 미국 헌법에 명시되어 있지 않지만, 연방대법원은 기본권 조항인 권리장전의 반영(penumbra)으로부터 도출된다고 판시하였다.[10] 그 후 프라이버시권은 낙태로 이어져, 1973년 미 연방대법원은 Roe 사건에서 여성의 프라이버시권을 헌법상 중대한 권리(fundamental right)로 인정하고, 여성의 낙태를 일률적으로 금지하는 법률이 위헌이라고 판시하였다.[11]

### 다. 자기정보 결정권(information privacy)

컴퓨터의 등장과 보급으로 개인정보를 대량으로 수집하여 보관하다 용도에 맞게 처리할 수 있게 되면서 새로운 법률문제가 발생하였고, 이를 해결하기 위하여 도입된 개념이 정보 프라이버시다. 개인정보는 낱개로 흩어져 있을 때는 가치가 없지만, 한 곳에 모이면 특정 개인이나 집단의 성향을 파악할 수 있는 자료로 가치를 생긴다. 컴퓨터를 이용하여 데이터베이스(DB)가 구축되면서 개인정보는 활용가치가 커졌다. 동시에 개인에 관한 정보를 그의 허락 없이 수집, 보관, 사용하는 것이 타당한지 의문을 품는 사람들도 늘어났다.

콜럼비아 대학의 웨스틴(Alan Westin) 교수는 1967년 프라이버시를 “개인, 집단 또는 기관이 자신에 관한 정보를 언제, 어떻게, 또 어느 범위에서 다른 사람에게 전달할 것인지 결정할 수 있는 요구”라고 정의하였다.[12] 즉 자기정보에 대한 관리, 편집 및 삭제의 권리를 프라이버시권이라 이해하였다. 웨스틴 교수의 자기정보 통제의 법리는 미국과 유럽의 프라이버시권 입법에 영향을 미쳤다.

## 3. 유럽의 인격권 법리[13][14]

### 가. 인격권의 근거

미국의 프라이버시권에 해당하는 독일의 법적 개념은 인격권이다. 독일 연방헌법재판소는 1954년 일반적 인격권을 사법상 권리로 인정한 이래 이 권리를 중심으로 프라이버시 침해 및 그 구제를 파악하고 있다. 독일에서 전개된 일반적 인격권의 법리에 의하면, 인격권은 1949년 독일 기본법(헌법)상 인간 존엄성 조항(제1조제1항)과 자유로운 인격발현 조항(제2조제1항)을 근거로 인정되었다.

### 나. 인격권의 내용

독일에서 일반적 인격권 내지 프라이버시권은 예로부터 법적으로 보호되어 오던 것은 물론이고 최근 새롭게 보호받게 된 것 등 다양한 인격 가치를 포괄하게 되었다. 즉 이 권리는 ‘고독에 관한 인간의 권리’ 또는 ‘자기 고유의 생활을 할 권리’라는 소극적 권리에서 출발하였지만 오늘날에는 ‘자유로운 자주결정권’ 또는 ‘개인정보에 관한 자주결정권’으로서 적극적 성격의 권리를 포함하고 있다.[15] 인격권은 생성 중인 권리이고, 그 내용과 한계가 확정되어 있는 권리

---

9) Griswold v. Connecticut, 381 U.S. 479 (1965).
10) Griswold 다수의견을 작성한 더글러스 대법관의 견해다.
11) Roe v. Wade, 410 U.S. 113 (1973).
12) Alan Westin, PRIVACY AND FREEDOM (1967).
13) 이하 내용은 박용상, 앞의 책, 389~96쪽 내용을 요약 소개한 것임.
14) 유럽의 인격권 법리 발전사에 대해서는 James Q. Whiteman, The Two Western Culture of Privacy: Dignity versus Liberty, 113 Yale. L.J. 1151 (2004) 참조.
15) Wenzel, a.a.O. 3 Aufl. S. 110; BVerGE 65, 1 (박용상, 앞의 책, 289쪽에서 재인용).

가 아니다. 즉 인격권에 대한 새로운 침해의 가능성은 항상 있으므로 일반적 인격권은 완결적 규율을 목표로 할 수 없다.

### 다. 인격권의 효력

인격권은 개인의 주관적 권리로서 국가권력에 대해서 뿐만 아니라 사인 간에도 통용될 수 있어야 하고, 따라서 대세적 효력이 인정된다는 것이 독일의 일반적 학설과 판례의 태도다. 따라서 인격권의 침해는 민사상 불법행위가 성립하며, 피해자에게 손해배상청구권은 물론 방해예방청구권과 방해배제청구권이 인정된다. 그런데 대세적 효력이 인정되는 다른 권리의 경우 그 내포와 외연이 근거법에 명시되어 있거나 확실히 뿌리내린 법 표상에 의해서 그 자체가 충분히 정해지만, 인격권은 그 내포와 외연이 불확정적이고 그 한계도 불명확하기 때문에 인격권 침해에 대해서는 신중한 법리가 적용되어야 한다.

### 라. 인격권의 한계

인간은 사회공동체 안에서 살아가는 존재이기 때문에 모든 권리는 '사회적 구속성'(Sozialgebundenheit)이 허용하는 범위 안에서만 인정된다. 인격권 역시 마찬가지다. 독일 판례와 학설은 정상적으로 사고하는 품위 있는 일반인의 인식을 기준으로 사회적 구속성을 수인할 수 있는 범위 내의 것인지 판단한다. 독일 연방헌법재판소는 사생활의 모든 영역이 절대적으로 보호받는 것이 아니며, 시민은 공공의 우월적 이익을 위해 엄격한 비례원칙의 준수 하에 내려진 국가의 조치가 사적 생활형성의 불가침영역을 침해하지 않는 한 이를 감내해야 한다고 한다.

## 4. 소결

프라이버시권의 발전과정에서 다음과 같은 몇 가지를 확인할 수 있다. 첫째, 프라이버시는 역사와 경험의 산물이다. 따라서 국가와 시대에 따라서 프라이버시 개념은 다를 수밖에 없다. 동양과 서양이 다르고, 같은 서양에서도 미국과 유럽이 다른 것이 프라이버시에 대한 인식이다. 프라이버시는 한 시대를 함께 살고 있는 공동체를 중심으로 생각할 수밖에 없다. 동일한 행위가 발생했을 때 사회마다, 시대마다 프라이버시 침해로 받아들이는지 여부가 다를 수 있다. 현실의 프라이버시 보호는 그 사회의 프라이버시 개념을 전제로 한다.

둘째, 프라이버시권의 개념은 일의적으로 정의내릴 수 없다. 프라이버시권은 시간이 흐르면서 그 내용이 확대되어왔다. 19세기 말 등장한 프라이버시권은 사적 공간에 대한 보호를 중시한 개념이어서, 오늘날 프라이버시권의 중심 내용이라고 할 수 있는 자기정보 결정권과는 다른 개념이다. 솔로브(Daniel J. Solove) 교수는 프라이버시의 모든 경우를 확인할 수 있는 공통분모를 찾는 방식으로 프라이버시 개념을 정립하는 방식은 실패했다고 주장한다.[16]

유럽은 인격권이라는 단일 개념으로 프라이버시권을 이해한다. 그러나 인격권 역시 그 내용을 살펴보면, 사생활 영역에서 자유를 인정하므로 은둔과 격리를 의미하는 혼자 있을 권리와 사회적 영역에서 자신의 인격상에 관한 결정권을 의미하므로 정보 프라이버시를 모두 포함하고 있다. 인격권 역시 성격이 다른 내용의 권리를 하나의 이름 아래 묶어 놓은데 불과하다. 여러 사람이 똑같이 프라이버시권이라고 이야기하더라도 각자 머릿속에 그리고 있는 개념이 서로 다를 수 있다.

16) Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002).

셋째, 프라이버시권은 기술 발전에 따른 사회 변화를 수용하여 형성된 권리다. 워렌과 브랜다이스가 처음 이 권리에 주목하여 논문을 발표하게 된 것은 19세기 말 급성장한 신문 산업과 보급형 사진기의 등장으로 인하여 사생활 침해의 우려가 커졌기 때문이다. 또 1960년대 정보 프라이버시 개념이 등장한 것은 컴퓨터의 발전으로 개인정보가 데이터베이스화되고, 이렇게 수집된 개인정보가 함부로 사용되는 일이 많아졌기 때문이다. 1990년대 중반 이후 인터넷 사용이 보편화되고, 정보통신기술이 급속도로 발전하면서 프라이버시 침해의 유형이 더욱 늘어나고 있는데, 이러한 변화가 새로운 프라이버시권의 탄생을 가져올지 주목되는 시점이다.

넷째, 프라이버시는 사적 영역과 공적 영역의 구분을 전제로 해서 사적 영역을 보호하기 위해서 마련된 개념이다. 인간은 혼자 살 수 없고, 다른 사람과 더불어 살기 때문에 공적 영역인 사회생활과 구분되는 사적 영역인 사생활을 보호할 필요가 생겼다. 미국의 경우 집(home)은 국가의 간섭에서 독립된 왕국처럼 보호된다. 독일 역시 사적 영역과 공적 영역을 구분해서 인격권의 보호정도를 달리한다. 영역이론은 개인의 생활영역을 내밀 영역, 비밀 영역, 사적 영역, 사회적 영역, 공개 영역 등 개방성에 따라 단계적으로 구분한 후 국가 개입의 한도 및 사생활에 관한 언론보도의 한계를 다르게 파악한다.

최근 정보 프라이버시가 중시되면서 사적 영역과 공적 영역의 구분론이 흔들리는 것은 사실이다. 정보통신기술의 발달로 개인정보가 광범위하고 무제한적으로 수집되고, 신속하고 종합적으로 처리되면서 공적 영역에서 수집된 개별적인 개인정보도 당사자의 사회적 인격상에 적지 않은 영향을 미칠 수 있게 되었기 때문이다. 그럼에도 불구하고 프라이버시의 핵심은 사적 영역의 보호에 있다.

# Ⅲ. 사생활의 비밀과 자유, 그리고 개인정보자기결정권

## 1. 프라이버시권과 헌법 제17조

미국의 프라이버시권에 대응하는 우리 법제상 개념은 사생활의 비밀과 자유라고 보는 것이 헌법학계의 다수 견해다. 하지만 양자를 동일시할 수는 없다. 첫째, 미국에서 프라이버시권은 헌법상 권리라고 단정할 수 없다. 미국 헌법은 프라이버시라는 용어를 담고 있지 않다. 수정헌법 제4조가 부당한 압수·수색(unreasonable searches and seizures)으로부터 신체, 가택, 서류 및 동산의 안전을 보장받는 권리를 규정하고 있어 혼자 있을 권리(right to be let alone)는 헌법상 권리로 이해할 수 있다. 미국 연방대법원은 1967년 Katz v. United States 사건[17]이후 프라이버시에 관한 합리적 기대를 보호하고 있으며, 그 근거를 수정헌법 제4조에서 찾고 있다. 연방대법원은 또 사생활에 관한 의사결정의 자유(decisional privacy)를 미국 헌법의 기본권 조항인 권리장전의 반영(penumbra)으로부터 도출된다고 판시한 바 있다. 그러나 자기정보 통제권(information privacy)은 미국에서 헌법상 권리로 인정되고 있지 않다.

둘째, 우리 헌법 제17조의 내용을 미국 프라이버시권 유형 분류를 그대로 수용하여 해석하는 것도 잘못이다. 우리는 헌법 제10조에서 일반적 인격권을 도출할 수 있으므로, 헌법 제17조는 다른 의미를 갖는 것으로 해석하는 것이 타당하다. 즉 헌법 제17조는 사생활 영역에서 비밀과 자유를 보장한 것으로, 미국식 분류에서 혼자 있을 권리(right to be let alone)와 사생활에 관한 의사결정의 자유(decisional privacy)가 여기에 해당된다. 하지만 개인이

17) 389 U.S. 347 (1967).

사회생활 영역에서 다른 사람들에게 보이는 모습과 관련된 내용은 헌법 제10조에서 도출되는 일반적 인격권의 내용으로 이해하는 것이 타당하다.[18]

## 2. 개인정보자기결정권

정보통신기술이 급속도로 발전하면서 정보 프라이버시(information privacy), 즉 자기정보 결정권이 더욱 중요해지고 있다. 하지만 자기정보 결정권의 성격이나 법적 근거에 대해서 미국과 유럽이 이해하는 바가 서로 다르다. 우리나라는 독일의 영향을 받아 인격권의 하나로 이해하고 있으며, 헌법상 권리로 수용한다. 다만, 헌법적 근거에 대해서는 견해가 갈린다. 헌법재판소는 이 권리를 개인정보자기결정권이라고 부른다.

### 가. 개인정보자기결정권의 법적 성격

개인정보자기결정권의 법적 성격을 인격권이라고 이해하는 유럽과 달리 미국에서는 재산권으로 이해하고자 하는 학자들이 상당수 있다. 이들은 개인정보를 재산권의 객체로 인정하게 되면 개인정보를 거래하는 시장에 의하여 투명하게 개인정보가 관리되고, 개인정보 주체들은 개인정보를 이용하고자 하는 기업들과 협상을 통하여 공개범위를 결정함으로써 자신의 개인정보를 완전히 통제할 수 있다고 본다.[19] 또 재산법은 집행에 관한 확립된 규범을 가지고 있기 때문에 현재 동의(consent)에 기초한 개인정보자기결정권 보호체제보다 우수하다고 판단한다.[20]

하지만 개인정보를 재산권으로 인정하게 되면 그 양도를 인정해야 하는데, 이는 개인의 독립성과 자율성을 보장하는 프라이버시 본래 취지에 반하게 되는 문제가 있다. 또 개인정보자기결정권을 보장하고자 한 취지가 개인정보의 공개에 있어서 개인의 이익을 인정하자는 데 있는 것이 아니라, 개인정보의 공개를 금지하는데 있기 때문에 재산권설은 정보 프라이버시의 본질에 반한다는 주장도 제기된다.

정보 프라이버시, 즉 개인정보자기결정권은 인간의 존엄성과 자율적 행동자유권을 보장하기 위한 여건을 마련하는 권리이기 때문에 의미가 있고, 따라서 그 법적 성격은 인격권이라고 보는 것이 맞다. 우리나라 판례와 학계 통설은 개인정보자기결정권의 법적 성격을 인격권으로 이해하는 데 일치한다.

### 나. 개인정보자기결정권의 헌법적 근거

앞에서 살펴본 바와 같이 미국 법조계는 개인정보자기결정권을 헌법상 권리가 아닌 법률상 권리로 이해한다. 이에 반하여 유럽 법조계는 개인정보자기결정권을 인격권에서 도출하고, 인격권의 근거를 최고의 헌법원리인 인간의 존엄성에서 찾고 있어 헌법상 권리로 파악한다.

우리나라에서는 개인정보자기결정권이 헌법상 권리라는 데 이견이 없다. 다만, 헌법상 근거에 대해서는 견해 차이가 크다. 인간의 존엄성과 행복추구권을 규정한 헌법 제10조에서 찾는

---

18) 한수웅 교수는 우리 헌법은 일반적 인격권의 보호범위 중 사생활의 보호에 관한 부분에 관하여는 개별적 기본권인 주거의 자유(제16조), 사생활의 비밀과 자유(제17조), 통신의 비밀(제18조)을 통하여 직접 구체적으로 규범화하였으며, 사회적 영역에서 인격발현의 기본조건의 보호(사회적 인격상에 관한 자기결정권)는 헌법에 명시적으로 규정되지 아니한 인격권을 보장하는 일반적 인격권에 의해서 이루어진다고 설명한다. 한수웅, 앞의 책, 541쪽.

19) 프라이버시의 경제적 분석에 대해서는 Richard A. Posner, The Right of Privacy, 12 Ga. L. Rev. 393 (1978), 정상조·권영준, "개인정보의 보호와 민사적 구제수단", 「법조」 제58권제3호 통권630호, 2009 참조.

20) Viktor Mayer-Schönberger, Beyond Privacy, Beyond Rights – Toward a "Systems" Theory of Information Governance, 98 Cal. L. Rev. 1853, 1860 (2010).

견해, 사생활의 비밀과 자유를 규정한 헌법 제17조에서 찾는 견해, 제10조와 제17조 모두에 근거가 있다는 견해, 민주주의 원리에서 찾는 견해 등 다양하다. 헌법재판소는 2005년 5월 지문날인 사건에서 개인정보자기결정권의 헌법적 근거를 굳이 어느 한두 개에 국한시키는 것은 바람직하지 않고, 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권이라고 보아야 한다고 판시하였다.[21]

생각건대, 우리 헌법은 일반적 인격권의 근거조항인 제10조 외에 제17조라는 독자적인 규정을 가지고 있기 때문에 개인정보자기결정권의 헌법적 근거는 제10조에서 찾는 것이 타당하다고 본다. 헌법 제17조는 사생활 영역의 권리를 보장한 것으로 이해되기 때문이다. 개인정보자기결정권은 사회로부터 은둔할 수 있는 사생활 영역의 권리가 아니고, 사회에 참여하는 데 필요한 사회적 영역의 권리다. 사회적 영역에서 인격권을 가진다는 것은 사회에 묘사되는 자신의 모습을 형성하는 개별정보에 대한 통제권을 가진다는 의미로 이해할 수 있다. 따라서 인격권보호의 핵심적 내용은 개인정보의 보호에 있고, 일반적 인격권으로부터 그 핵심적 보장내용으로서 개인정보의 공개와 사용에 관하여 스스로 결정할 수 있는 권리인 개인정보자기결정권이 도출된다고 보는 견해가 타당하다.[22]

## 3. 개인정보의 헌법상 개념

헌법재판소는 지문날인 사건에서 “개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보이며, 반드시 개인의 내밀한 영역이나 사적 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다.”고 판시한 이래 개인정보의 개념에 관하여 일관된 태도를 보이고 있다.

위 판시 내용은 개인정보자기결정권의 법적 성격을 인격권으로 파악하는 한 논리적이다. 헌법상 개인정보에 해당하는 정보는 개인에 관한 사회적 인격상에 영향을 미칠 수 있는 정보이기 때문에 사생활에 속하는 정보에 한정할 이유가 없고 공적 생활에서 형성되었거나 이미 공개된 정보도 여기에 포함되어야 한다. 또 정보처리 기술이 발전하면서 개인에 관한 사소한 개별정보라도 그러한 정보들이 결합되어 개인에 관한 사회적 인격상을 형성할 수 있기 때문에 헌법상 보호되는 개인정보는 그 가치의 경중을 따질 수 없다. 일체의 개인정보가 여기에 포함된다. 또한 정보처리 기술의 발전은 정보 그 자체로 정보주체를 식별할 수 없는 정보라고 하더라도 다른 정보와 결합하여 정보주체를 식별하는 일을 가능하게 한다. 따라서 개인의 동일성을 식별하는 정보(personally identified information)뿐 아니라 동일성을 식별할 수 있는 정보(personally identifiable information)까지 헌법상 개인정보의 개념에 포함되게 된다.

그런데 문제는 개인정보의 헌법상 개념을 이렇게 정의할 경우 개인이 사회생활을 하면서 남기는 모든 흔적이 개인정보자기결정권의 대상이 되어 프라이버시 내지 프라이버시권을 인정한 본래 의도에 반하게 된다는 데 있다. 프라이버시는 사회공동체에서 살아가는 개인을 전제로 사적 영역을 국가의 감시에서 벗어나 개인의 자율적 통제 아래 두겠다는 것이지, 모든 생활영역을 개인의 통제 아래 두겠다는 것이 아니다. 후자는 혼자 사는 사회에서나 가능한 것이다. 개인식별가능정보는 개념이 불명확하고, 사회 공동재산으로서의 정보를 과도하게 개인정보

21) 헌재 2005. 5. 26. 99헌마513, 판례집 제17권 1집, 681.
22) 한수웅, 앞의 책, 542쪽.

화하는 문제를 낳는다. 정보통신기술의 발달로 개인식별 불가능으로 분류됐던 정보도 개인식별가능정보로 바뀌고 있기 때문이다.

더구나 헌법재판소는 “개인정보를 대상으로 한 조사 수집 보관 처리 이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.”고 보고 있기 때문에 개인정보에 관련된 모든 사안은 위헌 시비가 놓이게 된다. 우리나라 헌법학계 통설은 일반적 인격권과 사생활 권리에 대해서 제3자적 효력을 인정하기 때문에 정부가 공권력 행사로 행하는 개인정보의 조사 수집 보관 처리 이용 등의 행위뿐 아니라 사인이 일상생활관계에서 행하는 개인정보의 조사 수집 보관 처리 이용 등의 행위도 정보주체의 개인정보자기결정권에 대한 제한이 된다. 개인정보보호법은 이러한 입장에서 공공부문과 민간부분을 구분하지 않고 법제화되었다.

그러나 개인정보자기결정권을 사회적 인격상에 관한 자기결정권의 핵심 내용으로 본다면, 개인정보자기결정권의 본질은 개인정보의 ‘공개’에 있는 것이지, 개인정보의 ‘수집’에 있는 것이 아니다. ‘수집’이 헌법적 문제를 일으키는 것은 헌법 제17조에 규정된 사생활의 비밀과 자유를 침해하는 방법으로 개인정보를 수집하는 경우다. 사생활 영역이 아닌 공적 영역에서 개인정보를 수집하는 것은 개인정보자기결정권을 침해하는 것이 아니다.

일부에서는 국가권력이 공적 영역에서 개인정보를 수집할 경우에도 수집한다는 사실이 개인의 자유로운 활동을 위축하기 때문에 개인정보의 ‘수집’도 개인정보자기결정권의 내용에 포함시켜야 한다고 주장한다. 그러나 공적 영역에서는 누구나 자기 행동을 누군가 보고 있다는 것을 의식하여야 하며, 그러한 의식이 책임 있는 사회 활동으로 이어질 수 있다고 본다. 물론 정보통신기술의 발전으로 개인의 모든 정보가 종합되어 모든 국민의 일거수일투족을 국가가 파악하는 감시국가는 바람직한 것은 아니다. 하지만 해악은 개별정보의 ‘수집’에 있지 않고, 수집된 정보를 종합하여 ‘사용’하는 데서 나온다. 감시정부의 위험은 ‘사용’의 해악을 처리하는 입법으로 해결하는 것이 올바른 접근이다.

모든 문제를 헌법 해석으로 일괄적으로 해결하는 것이 바람직한 것은 아니다. 헌법 해석으로 개인정보의 범위를 광범위하게 설정하고 개인정보자기결정권의 내용을 광범위하게 인정할 경우 개인정보는 보호되지만, 이와 상충하는 다른 사람의 자유와 권리는 보호되지 않을 수 있다. 개인의 사회활동을 하면서 남기는 정보를 다른 개인이 알 권리를 실현하기 위해서 또는 영업활동을 위하여 수집해서 내부에서 이용하는 행위를 ‘일반적으로’ 금지할 헌법적 타당성은 없다. 그렇지 않고 개인의 사생활 정보를 수집하여 이용한다면, 이는 개인정보자기결정권의 침해가 아니라 사생활의 비밀과 자유의 침해로 다루면 될 일이다.

## Ⅳ. 맺는 말

현대 사회에서 프라이버시는 중요하다. 중요한 만큼 누구나 공감하는 개념이어야 할 터인데, 실제로 그렇지 못해서 문제를 더욱 복잡하게 한다. 많은 사람들이 프라이버시를 이야기하지만, 서로 사용하는 의미가 같지 않다. 동양이 생각하는 프라이버시와 서양이 생각하는 프라이버시가 다르고, 미국인이 느끼는 프라이버시와 유럽인이 느끼는 프라이버시가 다르다. 프라이버시의 정의를 내리지 못하겠다는 학자들도 많다.

우리나라에서 프라이버시는 더욱 어려운 개념이다. 미국의 사생활 보호를 중심으로 하는 프라이버시 논의와 유럽의 인격권 중심의 개인정보자기결정권 논의가 혼재되어 있다. 프라이버시는 사회생활과 사생활의 구분을 전제로 하는 개념인데, 이를 제대로 인식하지 못한 채 법률이 만들어지는 경우도 많다. 또 공권력의 행사로 프라이버시가 침해되는 헌법 문제와 사인

간 불법행위가 성립하는지 살펴보는 민사 문제를 혼용하기도 한다.

프라이버시 침해를 방지하고, 실효성 있는 구제방법을 찾기 위해서는 프라이버시를 총괄적으로 접근하는 태도를 버려야 한다. 프라이버시를 총괄적으로 이해하려고 할수록 개념 혼동은 심화된다. 개인정보자기결정권이라는 포괄적 개념으로 모든 문제를 해결할 수 있다는 것은 근거 없는 신화일 뿐이다. 프라이버시의 내용을 하나씩 구분해서 그곳에서 발생하는 구체적인 해악을 발견하고 대책을 마련하는 것이 올바른 태도라고 본다. 공공부문과 민간부문의 구분, 사생활영역과 공개영역의 구분은 프라이버시 문제 해결의 전제다. 정보통신기술의 발달로 구분이 불명확해지면 그 정도만큼 반영하여 입법하고 실행하는 것으로 보충해야 할 것이다.

# 개인정보 보호와 다른 헌법적 가치의 조화

황성기(한양대 법학전문대학원 교수)

## Ⅰ. 들어가는 말

2011. 9. 30부터 시행된 「개인정보 보호법」(이하 '개인정보보호법'이라 함)에 대해서는 여러 가지 맥락에서 문제제기라든지 논란이 존재하고 있다. 예컨대 개인정보보호법에 대한 이해의 부족[1], 새로운 개인정보보호 처리 비용의 증가에 따란 부담감 등도 그 중의 하나이다.

그런데 개인정보와 관련된 법정책은 개인정보의 성격을 어떻게 파악하느냐에 따라 그 방향성이 달라질 수 있다. 즉 일반적으로 개인정보는 인격적 가치와 경제적·재산적 가치를 동시에 갖고 있는 것으로 평가되는바, 이 두 가지 가치 중에서 어느 부분에 초점을 맞추느냐에 따라 개인정보를 둘러싼 법정책의 방향성이 달라질 수 있다. 예컨대 개인정보의 인격적 가치에 방점을 두는 경우에는 개인정보의 보호에 초점을 맞추게 될 것인 반면에, 개인정보의 경제적·재산적 가치에 방점을 두는 경우에는 개인정보의 활용 내지 이용으로 무게중심이 옮겨지는 경향이 있다.

개인정보와 관련하여서는 기존의 정책방향이나 시장에서의 관행이 '활용'에 치우쳤다고 한다면, 최근에는 특히 개인정보보호법의 시행을 계기로 유럽연합에서부터 촉발된 '보호' 쪽으로의 흐름이 강하게 존재한다. 특히 유럽에서 형성된 '잊혀질 권리(right to be forgotten)'라는 개념이 이러한 '보호' 쪽으로의 정책방향을 보여주는 대표적인 상징적 개념이라고 할 수 있다.

현재 유럽을 중심으로[2] 논의되고 있는 '잊혀질 권리'[3]는 양면성을 갖고 있는 것으로 분석된다. 즉 잊혀질 권리는 두 가지 서로 다른 상황을 전제로 주장되고 있는바, 첫째는 개인정보처리자가 개인정보를 취득할 목적으로 정보주체로부터 개인정보를 수집·관리·이용·제공하고 있는 경우이고, 둘째는 개인정보를 직접적으로 수집·관리·이용할 목적이 아니었지만 인터넷 서비스를 제공하는 과정에서 부수적으로 개인에 관한 정보들이 모여지거나 검색·유통됨으로써 결과적으로 사생활이나 인격권 침해가 발생하는 경우[4]이다. 이 두 가지 경우를 전제로 해서 각각 정보주체 및 피해자의 권리구제 프로세스가 논의되거나 제도화되고 있는데, 이 두 가지 경우의 이념적 공통분모로 활용되고 있는 개념이 바로 잊혀질 권리이다. 하지만 여기에서 이

---

1) 특히 개인정보보호법에 대한 이해의 부족에 대해서는 손형섭, "개인정보 보호법의 특징과 앞으로의 방 - 업계의 반응에 대한 몇 가지 대안을 중심으로 -", 「언론과 법」 제11권 제1호, 2012. 6, 104-108면 참조.

2) 잊혀질 권리에 관한 간략한 국제적 동향은 홍명신, "정보의 웰다잉을 향한 시도 - '잊혀질 권리'를 둘러싼 국제동향", 「언론중재」 제119호(2011년 여름호), 2011. 6, 20-31면 참조.

3) 잊혀질 권리가 등장하게 된 여러 가지 배경 중의 하나는 디지털 및 커뮤니케이션 기술의 비약적인 발전으로 인해 개인에 관한 정보가 삭제불가능한 현실에 대한 인식이 존재한다. 예컨대 빅토어 마이어-쉔베르거는 정보의 디지털화, 정보저장의 저비용성, 정보검색의 용이성, 정보접근의 광범위성(글로벌 네트워크) 등으로 인해 과거와는 달리 기억이 표준이 되고 망각은 예외가 되었다고 한다. 빅토어 마이어 쉔베르거 저·구본권 역, 「잊혀질 권리」, 지식의 날개, 2011, 88-139면 참조.

4) 두 번째의 대표적인 경우가 바로 '묵은 기사'로 인한 사생활이나 인격권 침해를 주장하면서 과거의 기사에 대한 삭제·수정 요구를 하는 경우이다. 이러한 문제를 해결하는 방안으로 프라이버시 권리 개념에 잊혀질 권리 개념을 도입함과 동시에 언론중재법의 개정을 제안하면서, 언론사가 기록적 형태의 콘텐츠는 그대로 유지하되, 인터넷 검색을 통해 유통되는 과거 기사는 언론중재 조정의 대상이 되도록 해서 언론의 보도 매체로서의 기능과 개인의 프라이버시 보호 요청 간에 합의점을 찾을 수 있다는 견해가 있다. 이재진·구본권, "인터넷상의 지속적 기사 유통으로 인한 피해의 법적 쟁점 - '잊혀질 권리' 인정의 필요성에 대한 탐색적 연구 -", 「한국방송학보」 제22-3호, 한국방송학회, 2008. 5, 207면. 그리고 헌법적으로 보면 이러한 문제는 언론의 자유와 인격권 및 사생활의 자유의 충돌(기본권의 충돌)문제로 이해되고 있다. 지성우, "기본권 이론적 관점에서의 '잊혀질 권리(Right to be forgotten)'에 대한 시론적 고찰", 「언론중재」 제119호(2011년 여름호), 2011. 6, 38-39면.

념적 권리개념으로 활용되고 있는 잊혀질 권리는 그 법적 성격이 각각의 경우에 상이한데, 전자와 관련된 경우는 개인정보자기결정권으로 파악되고, 후자와 관련된 경우는 사회적 인격상에 관한 자기결정권으로 이해된다.[5] 여기서 개인정보자기결정권은 아래에서 상술하다시피, 이미 지문날인제도사건에서부터 우리 헌법재판소가 헌법상의 권리로 인정한 바 있다.[6] 그리고 사회적 인격상에 관한 자기결정권도 청소년성매수자 신상공개제도사건에서 그 개념의 단초가 제시된 적이 있으며[7], 지문날인제도사건에서는 개인정보자기결정권이 사회적 인격상에 대한 자기결정권을 내포한다고 판시한 적이 있다.[8]

이러한 맥락에서 잊혀질 권리는 그 용어에 있어서의 새로움과는 별개로, 내용적인 측면에 있어서는 새로운 것이라 보기 힘든 측면이 있다. 왜냐하면 내용적인 측면에서는 이미 우리 법제 하에서도 위에서 설명한 바와 같이 개인정보자기결정권 및 사회적 인격상에 관한 자기결정권이라는 개념하에 충분히 포섭될 수 있기 때문이다. 따라서 현재 유럽을 중심으로 논의되고 있는 잊혀질 권리 담론의 실질적 의의는 기존의 개인정보 '활용정책'에서 향후 개인정보 '보호정책'으로 그 트렌드를 전환시키기 위한 흐름에 있어서 추동력으로 작동되는 하나의 '레토릭'으로서의 의미를 가지는 것으로 이해된다.[9] 물론 레토릭으로서의 잊혀질 권리가 갖는 의미는 결코 과소평가되어서는 안된다. 하지만 잊혀질 권리 담론의 실천적 의미를 확보하기 위해서는, 궁극적으로는 개인정보 보호 v. 개인정보 활용 간의 구도에 있어서 어떻게 균형을 유지하고, 상호 대립되는 목표를 어떻게 조화시킬 것인가의 문제로 귀결되어야 할 것이고, 보다 구체적인 법제도 및 정책에 있어서 어떻게 반영시킬 것인가의 문제로 귀결되어야 한다.

이 글은 이러한 방향성을 전제로 하여, 일반론적이고도 추상적인 차원에서 개인정보 보호와 다른 헌법적 가치의 조화 문제를 검토하는 것을 목적으로 한다.

# Ⅱ. 개인정보 보호와 다른 헌법적 가치의 충돌

## 1. 개인정보 보호와 객관적 공익 목적과의 충돌

일반적으로 개인정보 보호와 관련되어 있는 헌법상의 권리는 '개인정보자기결정권'이다. 우

---

5) 문재완, "프라이버시 보호를 목적으로 하는 인터넷 규제의 의의와 한계 - '잊혀질 권리' 논의를 중심으로 -", 「언론과 법」 제10권 제2호, 한국언론법학회, 2011. 12, 32면.

6) 헌재 2005. 5. 26. 99헌마513, 주민등록법 제17조의8 등 위헌확인 등.

7) 헌재 2003. 6. 26. 2002헌가14, 청소년의성보호에관한법률 제20조 제2항 제1호 등 위헌제청. 청소년성매수자 신상공개제도사건에서는 위헌의견이 5이고 합헌의견이 4이어서 위헌의견이 많았지만, 정족수 미달로 합헌결정이 내려졌다. 이 사건에서 위헌의견은 다음과 같이 사회적 인격상에 관한 자기결정권을 설명하였다. "국가가 범죄사실과 같이 개인에 대한 사회적 평가에 중대한 영향을 미치는 정보자료를 함부로 일반에 공개할 경우, 그 개인의 긍정적인 면을 포함한 총체적인 인격이 묘사되는 것이 아니라 단지 부정적인 측면만이 세상에 크게 부각됨으로써 장차 그가 사회와 접촉·교류하며 자신의 인격을 자유롭게 발현하는 것을 심대하게 저해할 수 있다. 그러므로 사회활동을 통한 개인의 자유로운 인격발현을 위해서는, 타인의 눈에 비치는 자신의 모습을 형성하는 데 있어 결정적인 인자가 될 수 있는 각종 정보자료에 관하여 스스로 결정할 수 있는 권리, 다시 말하여 사회적 인격상에 관한 자기결정권이 보장되어야 하고, 국가는 이를 최대한 보장할 책무가 있다. 그러나 이 사건 신상공개제도는 본인이 밝히기를 꺼리는 치부를 세상에 공개하여 위와 같은 사회적 인격상에 관한 자기결정권을 현저하게 제한함으로써 범죄인의 인격권에 중대한 훼손을 초래한다고 볼 것이다."(밑줄 필자 강조)

8) "개인정보자기결정권은 정보주체로 하여금 개인정보의 공개와 이용을 스스로 통제하도록 함으로써 타인에게 형성될 정보주체의 사회적 인격상에 대한 결정권을 정보주체에게 유보시킨다는 의미를 갖고 있는바…"(헌재 2005. 5. 26. 99헌마513, 주민등록법 제17조의8 등 위헌확인 등).

9) 반면에 잊혀질 권리는 기존의 정보보호 관련 권리들이 정보의 정확한 처리 등 주로 정보의 저장과 기록, 수집 등의 행위에 초점을 맞춘 것에 반해, 정보의 삭제, 망각 등에 중점을 두는 패러다임 전환적인 권리라는 평가가 이루어지기도 한다. 즉 기존의 개인정보자기결정권의 내용에 더하여 잊혀질 권리의 고유한 부분은 '특정기간이 지났을 경우 자동적인 정보의 삭제'가 보장된다는 것이다. 민윤영, "인터넷 상에서 잊혀질 권리와 「개인정보보호법」에 대한 비교법적 고찰", 「고려법학」 제63호, 고려대학교 법학연구원, 2011. 12, 288-289면 및 299면.

리 헌법재판소는 일찍이 지문날인제도사건에서 “개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다.”[10]고 판시하면서, 개인정보자기결정권을 현대의 정보사회에서 새로운 독자적 기본권으로서 헌법에 명시되지 아니한 기본권으로 인정한 적이 있다.[11]

이러한 개인정보자기결정권은 그 보호법익과 한계의 설정에 있어서 강한 유동성을 지니는데, 그 이유는 개인정보자기결정권은 그 존재 및 의의, 내용이 판례에 의해 인정 및 형성되고 있을 뿐만 아니라, 유동적인 정보통신의 발달과 궤적을 같이 하고 있기 때문이다.[12]

한편 위와 같은 개인정보자기결정권은 결코 절대적인 권리는 아니다. 즉 일정한 경우에는 객관적 공익을 위해서 제한이 가능하다. 예컨대 우리 헌법재판소는 ‘범죄수사 목적’이라는 공익과 관련하여, 지문날인제도사건에서 개인의 지문정보에 대한 수집, 보관, 전산화 및 범죄수사 목적 이용행위에 대하여 그 합헌성을 인정한 적이 있고[13], 범죄혐의로 수사를 받은 피의자가 검사로부터 ‘혐의없음’의 불기소처분을 받은 경우 혐의범죄의 법정형에 따라 일정기간 피의자의 지문정보와 함께 인적사항·죄명·입건관서·입건일자·처분결과 등 수사경력자료에 관한 정보의 보존 및 범죄수사 등을 위한 이용에 대해서도 합헌성을 인정한 적이 있다.[14] 또한 졸업증명서 발급업무에 관한 ‘민원인의 편의 도모, 행정의 효율성 및 투명성의 제고’를 위하여, 서울특별시 교육감 등이 졸업생의 성명, 생년월일 및 졸업일자 정보를 교육정보시스템(NEIS)에 보유하는 행위에 대해서도 합헌성을 인정하였다.[15] 국민기초생활보장법상의 ‘수급자격 및 급여액의 객관성과 공정성 확보’를 위하여, 급여신청자에게 금융거래정보의 제출을 요구할 수 있도록 하는 것에 대해서도 합헌성을 인정한 바 있다.[16] 납세자의 편의 및 사회적 비용의 절감과 같은 ‘조세행정의 효율성 확보’와 부당공제 방지를 통한 ‘조세정의 및 형평의 실현’을 위하여, 의료기관에게 환자들의 의료비 내역에 관한 정보를 국세청에 제출하는 의무를 부과하는 것에 대해서도 합헌성을 인정하였다.[17] ‘의료이용자가 의료급여를 받을 적법한 수급자인지 여부 및 의료급여의

---

10) 헌재 2005. 5. 26. 99헌마513, 주민등록법 제17조의8 등 위헌확인 등.

11) 헌법재판소의 이러한 입장은 지문날인제도사건 이후에도 일련의 사건들에서 일관되게 유지되고 있다. 헌재 2005. 7. 21. 2003헌마282, 개인정보수집 등 위헌확인; 헌재 2005. 11. 24. 2005헌마112, 국민기초생활보장법 제23조 위헌확인; 헌재 2007. 5. 31. 2005헌마1139, 공직자등의병역사항신고및공개에관한법률 제3조 등 위헌확인; 헌재 2008. 10. 30. 2006헌마1401등(병합), 소득세법 제165조 제1항 등 위헌확인 등; 헌재 2009. 9. 24. 2007헌마1092, 의료급여법 시행령 별표 제1호 가목 등 위헌확인; 헌재 2009. 10. 29. 2008헌마257, 형의 실효 등에 관한 법률 제8조의2 위헌확인; 헌재 2010. 5. 27. 2008헌마663, 민사집행법 제70조 등 위헌확인; 헌재 2010. 9. 30. 2008헌바132, 민사소송법 제290조 등 위헌소원; 헌재 2011. 12. 29. 2010헌마293, 교육관련기관의 정보공개에 관한 특례법 제3조 제2항 등 위헌확인; 헌재 2012. 8. 23. 2010헌마47, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제44조의5 제1항 제2호 등 위헌확인.

12) 임규철, “국내외 개인정보 보호법제 현황 및 쟁점”, 「언론중재」 제124호(2012년 가을호), 2012. 9, 9면.

13) 헌재 2005. 5. 26. 99헌마513, 주민등록법 제17조의8 등 위헌확인 등.

14) 헌재 2009. 10. 29. 2008헌마257, 형의 실효 등에 관한 법률 제8조의2 위헌확인.

15) 헌재 2005. 7. 21. 2003헌마282, 개인정보수집 등 위헌확인.

16) 헌재 2005. 11. 24. 2005헌마112, 국민기초생활보장법 제23조 위헌확인.

범위 등의 정확성'을 담보하기 위하여, 개별 의료급여기관으로 하여금 수급권자의 진료정보를 국민건강보험공단에 알려줄 의무를 부과하는 것에 대해서도 합헌성을 인정하였다.[18] '채무이행의 간접강제 및 거래의 안전 도모'를 위하여, 채무자의 이름, 주소, 주민등록번호, 집행권원과 불이행한 채무액 및 그 등재 사유와 날짜를 기재한 채무불이행자 명부를 누구든지 열람·복사할 수 있도록 하는 것에 대해서도 합헌성을 인정하였다.[19] 마지막으로 '객관적인 증거에 의해 확인되는 실체적 진실에 따라 법적 분쟁을 공정하게 해결'하기 위하여, 법원의 제출명령이 있는 경우 금융기관이 특정인의 금융거래의 내용에 대한 정보 또는 자료를 본인의 동의 없이도 법원에 제공할 수 있도록 하는 것에 대해서도 합헌성을 인정하였다.[20]

## 2. 개인정보 보호와 표현의 자유의 충돌

개인정보 보호가 위와 같이 범죄수사 목적 등과 같은 공익적 목적뿐만 아니라 다른 기본권 주체의 기본권, 예컨대 의사표현의 자유라든지 알권리와 같은 여타의 헌법적 가치와 충돌하는 경우도 존재한다.

우선 의사표현의 자유와 개인정보자기결정권의 충돌과 관련하여, 대법원은 예컨대 '로마켓 사건'에서 "정보주체의 동의 없이 개인정보를 공개함으로써 침해되는 인격적 법익과 정보주체의 동의 없이 자유롭게 개인정보를 공개하는 표현행위로서 보호받을 수 있는 법적 이익이 하나의 법률관계를 둘러싸고 충돌하는 경우에는, 개인이 공적인 존재인지 여부, 개인정보의 공공성 및 공익성, 개인정보 수집의 목적·절차·이용형태의 상당성, 개인정보 이용의 필요성, 개인정보 이용으로 인해 침해되는 이익의 성질 및 내용 등의 여러 사정을 종합적으로 고려하여, 개인정보에 관한 인격권의 보호에 의하여 얻을 수 있는 이익(비공개 이익)과 표현행위에 의하여 얻을 수 있는 이익(공개 이익)을 구체적으로 비교 형량하여, 어느 쪽의 이익이 더욱 우월한 것으로 평가할 수 있는지에 따라 그 행위의 최종적인 위법성 여부를 판단하여야 한다"[21] 고 판시한 적이 있다. 또한 언론보도에 의해서 개인정보가 공표되는 경우라든지 언론에 의한 개인정보의 취급도 언론의 자유와 개인정보보호 사이의 조화적 해석이 필요한 경우라고 할 수 있는데, 예컨대 유명인의 동정에 관한 보도에 있어서 개인정보가 노출된다든지 혹은 범죄관련 보도에 있어서 범인이나 범죄피해자 등의 성명, 나이, 직업, 주소, 전과사실 등이 공개되는 사례가 대표적이다.[22]

그리고 알권리와 개인정보자기결정권의 충돌과 관련하여, 헌법재판소는 교원의 교원단체 및 노동조합 가입현황(인원 수)만 공시대상정보로 규정하고 개별 교원의 명단은 규정하지 아니한 것의 위헌 여부가 문제가 된 '교육관련기관의 정보공개에 관한 특례법사건'에서, "교원의 교원단체 및 노동조합 가입에 관한 정보의 공개를 요구하는 학부모들의 교육정보에 대한 알권리 및 그것을 통한 교육권과 그 정보의 비공개를 요청하는 정보주체인 교원의 사생활의 비밀과 자유 및 이를 구체화한 개인정보자기결정권이 충돌하는 문제상황"을 전제로 하여 사건을 해결하고 있다.[23] 법원도 이와 동일한 사안에서 "학부모의 알권리에 근거하여 교원의 노동조

17) 헌재 2008. 10. 30. 2006헌마1401등(병합), 소득세법 제165조 제1항 등 위헌확인 등.
18) 헌재 2009. 9. 24. 2007헌마1092, 의료급여법 시행령 별표 제1호 가목 등 위헌확인.
19) 헌재 2010. 5. 27. 2008헌마663, 민사집행법 제70조 등 위헌확인.
20) 헌재 2010. 9. 30. 2008헌바132, 민사소송법 제290조 등 위헌소원.
21) 대법원 2011. 9. 2. 선고 2008다42430 전원합의체 판결, 정보게시금지 등.
22) 권건보, "방송의 자유와 방송사업자의 개인정보 보호", 「공법학연구」 제11권 제2호, 한국비교공법학회, 2010. 5, 37-38면.
23) 헌재 2011. 12. 29. 2010헌마293, 교육관련기관의 정보공개에 관한 특례법 제3조 제2항 등 위헌확인.

합 가입 여부에 관한 정보를 공개하는 것은 교원의 인격권 및 사생활의 비밀과 자유에 의하여 보장되는 개인정보자기결정권의 침해에 해당하고, 이는 학부모의 알권리와 교원의 개인정보자기결정권의 충돌로 나타나게 된다"는 점을 전제하였다."[24]

위와 같이 개인정보 보호와 의사표현의 자유라든지 알권리가 충돌하는 경우에는, 결국 상충하는 헌법적 가치를 조화시키기 위한 규범조화적 해석 내지 법익형량이 개별 판결에서나 입법을 통해서 이루어져야 할 필요가 있을 것이다.

## 3. 개인정보 보호와 영업의 자유의 충돌

개인정보 보호가 다른 기본권 주체의 기본권과 충돌하는 양상과 관련하여, 영업의 자유와 충돌하는 경우도 존재한다.

우선 기업이나 개인이 영업활동의 일환으로 소비자의 개인정보를 수집·처리하여 이를 상품 또는 서비스의 생산이나 마케팅에 활용하는 것은 헌법이 보장하는 영업의 자유에 속하는바, 만약 기업이나 개인이 영업활동의 일환으로 소비자의 개인정보를 수집·처리·이용하는 것을 제한하거나 금지하는 경우에는 당해 기업이나 개인은 헌법상 보장받고 있는 자신의 영업의 자유를 제한받는 것이 된다.[25]

또한 개인정보 보호와 관련된 법정책이나 시스템의 설계에 있어서 일관성이 없거나 체계정당성이 확보되지 않는 경우에도, 사업자인 개인정보처리자의 영업의 자유에 대한 부정적 효과가 발생할 수 있다.

예컨대 동일한 수범자에 대해서 개인정보의 수집의무와 개인정보의 보호의무를 동시에 부과하는 경우를 볼 수 있다. 공직선거법 제82조의 6이 규정하고 있는 인터넷언론사 게시판·대화방 등의 실명확인제가 대표적인 경우이다. 공직선거법 제82조의 6 제1항은 인터넷언론사로 하여금 선거운동기간 중 당해 인터넷홈페이지의 게시판·대화방 등에 정당·후보자에 대한 지지·반대의 문자·음성·화상 또는 동영상 등의 정보(이하 '정보 등'이라 한다)를 게시할 수 있도록 하는 경우에는 행정자치부장관 또는 「신용정보의 이용 및 보호에 관한 법률」 제2조 제4호에 따른 신용정보업자가 제공하는 실명인증방법으로 실명을 확인받도록 하는 기술적 조치를 하도록 인터넷언론사에 대해 의무를 부과하고 있다. 다만, 인터넷언론사가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제44조의 5에 따른 본인확인조치를 한 경우에는 그 실명을 확인받도록 하는 기술적 조치를 한 것으로 보고 있다(동항 단서). 실명확인과정에서 인터넷언론사는 당해 인터넷홈페이지의 게시판·대화방 등에서 정보 등을 게시하고자 하는 자에게 주민등록번호를 기재할 것을 요구하여서는 아니된다(동조 제5항). 그런데 공직선거법 제82조의 6이 예정하고 있다시피, 인터넷언론사 게시판·대화방 등의 실명확인제가 운영되기 위해서는 개인정보의 수집 및 활용이 필수적이다. 즉 '본인인증시스템의 강제적 구축을 통한 의사표현의 통제'가 인터넷언론사 게시판、대화방 등의 실명확인제의 기본목적이라고 한다면, 본인인증시스템을 구축하기 위해서는 궁극적으로 개인정보를 활용할 수밖에 없다.[26] 따라서 주민등록번호를 직접적·간접적으로 활용하든 또는 주민등록번호 이외의 개인정보를 활용하든지간에, 본인인증 내지 실명인증절차는 개인정보의 활용이 반드시 전제될 수밖에 없게 되고, 따라서 공직선거법

24) 부산지방법원 2011. 2. 17 선고 2010가합10002 판결, 손해배상(기).
25) 김일환, "개인정보의 보호와 이용법제의 분석을 위한 헌법상 고찰", 「헌법학연구」 제17권 제2호, 한국헌법학회, 2011. 6, 363면.
26) 황성기, "인터넷 실명제에 관한 헌법학적 연구", 「법학논총」 제25집 제1호, 한양대학교 법학연구소, 2008. 3, 24면.

상의 실명확인제는 인터넷언론사에 대해서 사실상 개인정보의 수집의무를 부과하는 결과를 초래한다. 그런데 인터넷언론사가 공직선거법 제82조의 6에 따라 자신에게 부과된 의무를 수행하기 위해 개인정보를 수집, 활용할 수밖에 없다고 한다면, 문제는 인터넷언론사가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 함)상의 정보통신서비스제공자에 해당하는 경우에 발생한다. 왜냐하면 그 순간에 정보통신망법상의 개인정보 보호시스템이 동시에 적용되기 때문이다. 결국 인터넷언론사는 공직선거법상의 실명확인의무를 수행하기 위하여 동시에 정보통신망법상의 개인정보 보호의무도 부담할 수밖에 없는 모순적인 상황이 만들어질 수 있는 것이다.

위와 같은 현상은 동일한 법률 내에서도 발견되기도 한다. 예컨대 최근에 헌법재판소로부터 위헌결정된[27] 정보통신망법상의 제한적 본인확인제 등은 개인정보의 수집의무를 정보통신서비스제공자에 부과하였으면서도, 동일한 정보통신서비스제공자에 대해서는 동시에 정보통신망법상의 개인정보 보호관련 규정들도 동시에 적용되었던 것이다.

개인정보 보호와 영업의 자유가 실제로 충돌하는 상황도 볼 수 있다. 예컨대 사업자들은 개인정보보호법이나 정보통신망법상의 개인정보 보호관련 규정들에 근거해서 개인정보 보호를 위하여 인적·물적 비용 등을 투입하고 있다. 실제로 개인정보 보호를 위한 인적 비용으로 개인정보 보호책임자(Chief Privacy Officer: CPO)와 본부 단위의 팀이 투입되고 있으며, 개인정보보호법상의 기술적·관리적 및 물리적 보호조치의무에 따라 물적 비용으로 보안시스템 구축 및 유지 비용, 매년 이루어지는 실태조사에 따른 비용, 관제서비스 구축(시스템 공격에 대한 방어)에 따른 비용 등이 투입되고 있다. 더 나아가서 개별 사업자들은 개인정보보호법이나 정보통신망법상의 개인정보 보호관련 규정들이 너무 강력하여 고객관리 및 리스크관리에 어려움이 많을 뿐만 아니라, 비즈니스의 창의성이나 다양성을 확보하기 어렵다는 호소를 많이 한다.

결국 위에서 적시한 예들은, 개인정보보호법이나 정보통신망법상의 강력한 개인정보 보호시스템이 개인정보자기결정권의 보호라는 관점에서는 (+)의 효과를 야기시킬 수 있지만, 반면에 개인정보처리자가 되는 사업자의 영업의 자유의 보호라는 관점에서는 (-)의 효과를 야기시킬 수 있다는 것을 의미한다.

# Ⅲ. 개인정보 보호와 다른 헌법적 가치의 조화의 방향성 및 기준

## 1. 일반적 방향성 및 기준

일반적으로 개인정보 보호와 다른 헌법적 가치 간의 충돌을 조화시키기 위한 법익형량은 개별 사건에서의 법원의 판결을 통해서 이루어지겠지만, 입법적 차원에서도 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준이 제시될 필요가 있다고 생각한다. 이렇게 사법적 차원뿐만 아니라 입법적 차원에서 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준을 모색함에 있어서는 다음과 같은 사항들을 고려해야 한다고 본다.

첫째, 개인정보별 보호 정도의 차별화가 가능한지에 대한 검토가 필요하다. 예컨대 민감정보와 비민감정보의 구분에 따른 보호 정도의 차별화가 가능한지, 민감정보와 비민감정보 사이에 중간영역의 정보유형이 존재하는지 등에 대한 검토가 필요하다. 만약 개인정보별로 유형화

27) 헌재 2012. 8. 23. 2010헌마47등(병합), 정보통신망 이용촉진 및 정보보호 등 에 관한 법률 제44조의5 제1항 제2호 등 위헌확인.

가 가능하고, 그에 따른 보호 정도의 차별화가 가능하다면, 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준의 모색이 보다 수월해질 수 있을 것이다.

둘째, 개인정보 보호와 충돌되는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화가 가능한지에 대한 검토가 필요하다. 예컨대 표현의 자유가 가지는 중요도 및 보호 정도, 비상업적 표현 v. 상업적 표현의 구분, 영업의 자유의 중요도 및 보호 정도 등에 대한 검토가 필요하다.

셋째, 커뮤니케이션 및 통신기술의 변화 및 발전 정도도 고려해야 한다고 본다. 오늘날 커뮤니케이션 및 통신기술의 변화 및 발전을 고려한다면, 사실상 개인정보의 활용을 전제하지 않는 비즈니스는 거의 존재하기 어려울 것이다. 또한 개인정보가 전혀 노출되지 않은 채 삶을 살아가는 것은 거의 불가능하다. 즉 오늘날 커뮤니케이션 및 통신기술의 변화 및 발전을 고려한다면, 어느 정도의 개인정보의 노출은 불가피하다. 따라서 너무 개인정보의 '보호'에만 집착하는 경우에는 오히려 새로운 기술의 개발 및 발전을 저해할 위험성도 존재할 수 있다. 이러한 관점에서 개인정보보호법으로 대표되는 현재의 우리나라의 개인정보 보호법제가 '보호'에만 너무 무게중심을 두었다면, 앞으로는 '안전한 활용'으로 무게중심을 좀 옮길 필요가 있다. 이와 관련하여 우리가 교훈을 얻을 수 있는 유사한 예가 바로 공직선거법이다. 그동안 공직선거법은 '선거의 공정성'에 너무 갇혀 있어서 인터넷이라는 새로운 매체의 등장과 그 활용에 대해서 공직선거법이 전혀 수용을 하지 못하였다. 최근에 헌법재판소가 공직선거법상의 인터넷 이용 선거운동에 대해서 위헌결정[28]을 내리는 등 전향적인 흐름이 등장하고 있지만, 그동안 공직선거법상의 각종 규제장치는 인터넷이라는 매체의 특성을 전혀 고려하지 못한 채 오히려 인터넷을 이용한 커뮤니케이션 기술의 발전을 저해한 측면이 없지 않았다. 바로 여기서 새로운 커뮤니케이션 기술의 발전에 있어서 법제도가 어떠한 역할과 기능을 해야 하는가의 문제가 등장하게 된다.

결론적으로 우리의 개인정보 보호법제가 너무 개인정보의 '보호'라는 도그마에 갇혀, 새로운 커뮤니케이션 기술의 발전을 저해하는 일이 없도록 할 필요가 있고, 이러한 관점에서 우리나라의 개인정보 보호법제에 대한 면밀한 재검토가 필요하다고 본다.

## 2. 개인정보별 보호 정도의 차별화

현행 개인정보보호법은 '개인정보'를 "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 것 포함한다)"으로 정의하고 있고, 정보통신망법은 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)"로 정의내리고 있다. 이 두 가지 법률이 채택하고 있는 개인정보에 관한 개념정의의 기본틀은 개인정보간의 차별화 혹은 개인정보별 보호정도의 차별화는 전제하고 있지 않다. 왜냐하면 두 가지 법률상의 개인정보 개념정의의 핵심지표는 '개인의 동일성의 식별가능성' 그 자체이지, 그 활용시 개인의 존엄과 인격권, 사생활에 미치는 영향, 당해 개인정보의 형성 영역 등은 고려하지 않기 때문이다. 하지만 개인정보간의 차별화 혹은 개인정보별 보호정도의 차별화는 헌법적으로 정당화될 수 있다.[29]

---

28) 헌재 2011. 12. 29. 2007헌마1001, 공직선거법 제93조 제1항 등 위헌확인.

29) 개인정보를 보호가치 혹은 경제적 가치에 따라 유형별로 분류하고 인격적 속성과의 연관성에 비추어 개별적으

대표적인 것이 바로 민감정보와 비민감정보의 구분에 따른 보호정도의 차별화가 될 것이다. 우선 현행 개인정보보호법은 민감정보라는 개념을 분명히 전제하고 있다. 현행 개인정보보호법 제23조 본문은 "사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보"를 '민감정보'라고 개념정의를 내리고 있고, 동법 시행령 제18조는 '민감정보의 범위'라는 제하에 유전자검사 등의 결과로 얻어진 유전정보, 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보도 민감정보에 포함시키고 있다. 그리고 이러한 민감정보에 대해서는 '원칙적 처리 금지, 예외적 처리 허용'이라는 정책을 적용하고 있다. 민감정보는 오·남용의 경우 그 피해는 커지고 복구가 거의 불가능한 특징을 갖고 있으므로 민감정보는 상대적으로 활용보다는 보호에 더 치중해야 한다는 점에서[30], 민감정보에 대한 현행 개인정보보호법의 기본태도는 타당하다.

우리 헌법재판소도 '종교적 신조, 육체적·정신적 결함, 성생활에 대한 정보'와 같이 인간의 존엄성이나 인격의 내적 핵심, 내밀한 사적 영역에 근접하는 것은 민감정보로서 엄격히 보호되어야 하는 반면, '성명, 직명(職名)'과 같이 인간이 공동체에서 어울려 살아가는 한 다른 사람들과의 사이에서 식별되고 전달되는 것이 필요한 기초정보들은 그 자체로 언제나 엄격한 보호의 대상이 되기 어렵다고 보면서[31], 민감정보와 비민감정보의 구분에 따른 보호정도의 차별화가 가능하다는 것을 전제하고 있다. 이러한 맥락에서 헌법재판소는 '성명, 생년월일, 졸업일자'는 그 자체로 개인의 존엄과 인격권에 심대한 영향을 미칠 수 있는 민감정보라고 보기 어렵다고 보았다.[32] 그리고 지문정보에 대해서도 개인정보자기결정권의 한 내용인 사회적 인격상에 관한 자기결정권과의 고리가 약하다고 헌법재판소는 보았다.[33] 반면에 병역의무가 면제된 공무원의 경우 그 공개가 강제되는 면제사유 질병명이 그 공개 시 인격이나 사생활의 심각한 침해를 초래할 수 있는 질병이나 심신장애내용인 경우에 내밀한 사적 영역에 근접하는 민감한 개인정보에 해당한다고 보았다.[34] 이와 동일한 차원에서 '개인의 의료에 관한 정보(의료비내역에 관한 정보 및 병명이나 구체적인 진료내역에 관한 정보 포함)'는 개인의 인격 및 사생활의 핵심에 해당하는 민감한 정보 가운데 하나라고 보았다.[35]

개인정보간의 차별화 혹은 개인정보별 보호 정도의 차별화는 위와 같은 민감정보 v. 비민감정보 간의 구분의 경우에만 적용되는 것은 아니다. 기타 다른 기준이나 관점에 따라서도 개

---

로 논의하는 시도는, 개인정보에 관한 구조적 조망을 가능케 하는 법리적 논거를 제시할 뿐만 아니라, 적정 수준의 개인정보 유통을 유지할 수 있는 정책적 유인으로 작용한다는 점에서도 그 의의가 인정될 수 있다. 이민영, 「개인정보법제론」, 개정증보판, jinhan M&B, 2007, 40면.

30) 임규철, "교원정보 실명공개의 위법성 유무", 「공법학연구」 제11권 제3호, 한국비교공법학회, 2010. 8, 350면.

31) 헌재 2005. 7. 21. 2003헌마282, 개인정보수집 등 위헌확인.

32) 헌재 2005. 7. 21. 2003헌마282, 개인정보수집 등 위헌확인.

33) 헌재 2005. 5. 26. 99헌마513, 주민등록법 제17조의8 등 위헌확인 등.

34) 헌재 2007. 5. 31. 2005헌마1139, 공직자등의병역사항신고및공개에관한법률 제3조 등 위헌확인.

35) 헌재 2008. 10. 30. 2006헌마1401등(병합), 소득세법 제165조 제1항 등 위헌확인 등; 헌재 2009. 9. 24. 2007헌마1092, 의료급여법 시행령 별표 제1호 가목 등 위헌확인. 물론 개인의 의료에 관한 정보라고 할지라도 의료비내역에 관한 정보와 병명이나 구체적인 진료내역에 관한 정보 간에는 차별화될 수 있는 여지는 존재한다. "개인의 의료에 관한 정보는 개인의 인격 및 사생활의 핵심에 해당하는 민감한 정보 가운데 하나이다. 물론 이 사건 소득공제증빙서류에 기재될 내용은 누가, 언제, 어디서 진료를 받고 얼마를 지불했는가라는 의료비의 지급 및 영수(領收)에 관한 것으로 병명이나 구체적인 진료내역과 같은 인격의 내적 핵심에 근접하는 의료정보는 아니다. 그러나 누가, 언제, 어디서 진료를 받고 얼마를 지불했는가라는 사실은 그 자체만으로도 보호되어야 할 사생활의 비밀일 뿐 아니라, 이러한 정보를 통합하면 구체적인 신체적·정신적 결함이나 진료의 내용까지도 유추할 수 있게 되므로, 개인정보자기결정권에 의하여 보호되어야 할 의료정보라고 아니할 수 없다."(헌재 2008. 10. 30. 2006헌마1401등(병합), 소득세법 제165조 제1항 등 위헌확인 등)(밑줄 필자 강조).

인정보간의 차별화 혹은 개인정보별 보호 정도의 차별화는 가능하다.

예컨대 '성향중립 개인정보'[36]와 '성향기반 개인정보'[37]로 구분하고, 성향기반 개인정보는 그 자체의 유통이 국가나 사회가 존속하고 발전하는 데 필수적인 경우(예컨대 전과기록)와 그렇지 않은 경우(예컨대 개인이 핸드폰에 저장해 놓은 지인의 전화번호)로 구분하는 것도 가능하다.[38]

공적 성격의 정보 v. 사적 성격의 정보간의 구분도 개인정보별 보호 정도의 차별화를 가능하게 하는 기준이 될 수 있다. 공적 성격의 정보는 개인정보자기결정권의 보호대상이 되는 개인정보이기는 하지만, 또한 정보의 자유라고 하는 권리의 보호대상이 되기도 하다. 이러한 측면에서 공적 성격의 정보는 순수한 사적 성격의 정보보다는 그 보호의 정도가 약하다고 할 수 있을 것이다.[39]

개인에 관한 정보(information concerning a person) v. 개인정보(personal information) 간의 구분도 가능하다. 전자는 개인에 대한 묘사, 서술, 평가, 의견, 언론보도 등을 의미하는 것으로서 사회적 인격상에 관한 자기결정권의 보호대상이지만[40], 후자는 전형적인 개인정보자기결정권의 보호대상이라는 점에서, 그 보호의 방향성이나 방법, 정도가 차별화될 수 있는 여지가 존재한다. 즉 개인에 관한 정보의 경우에는 표현의 자유, 언론의 자유, 예술의 자유에 따른 그 활용 및 이용이 가능할 수 있다는 점에서, 전형적인 개인정보와 비교해 볼 때, 그 보호의 방향성이나 방법, 정도가 차별화될 수 있다.

마지막으로 현행 개인정보보호법이 예정하고 있는 개인정보 유형별 구분에 따른 보호 정도의 차별화도 고려할 수 있다. 예컨대 현행 개인정보보호법 제24조 및 동법 시행령 제19조는 '고유식별정보'라는 범주를 인정하고 있는데, 여기서 고유식별정보란 "법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보"를 의미하고, 이러한 고유식별정보에 해당하는 것으로는 주민등록법 제7조제3항에 따른 주민등록번호, 여권법 제7조제1항제1호에 따른 여권번호, 도로교통법 제80조에 따른 운전면허의 면허번호, 출입국관리법 제31조제4항에 따른 외국인등록번호를 들 수 있다.[41] 현행 개인정보보호법 제24조는 이러한 고유식별정보에 대해서도 민감정보와 마찬가지로 '원칙적 처리 금지, 예외적 처리 허용'이라는 정책을 적용하고 있다. 따라서 고유식별정보와 민감정보에 대해서는 동일한 정도의 보호수준을 적용하고 있는 것이다. 반면에 현행 개인정보보호법 제2조 제1호가 내리고 있는 개인정보의 개념정의에 따르면, 그

---

36) 개인을 식별하는 정보로서 그 자체로는 아무런 가치판단을 일으키지 않는 것. 성명, 주민등록번호, 운전면허번호, 여권번호, 외국인등록번호, 전화번호, 지문, 동공, 이메일 등.

37) 개인의 성향을 파악할 수 있는 개인정보. 전과기록, 구매기록, 방문기록, 검색기록, 위치정보 등.

38) 예컨대 문재완, 앞의 글, 14-16면.

39) 한편 개인정보보호법이나 정보통신망법이 보호하고자 하는 개인정보는 개인의 사생활비밀 등에 관련한 정보를 의미하고 사회적 소통의 수단으로서 그 공개성이 전제되어 있는 연락정보(이름, 전화번호)는 특별한 사유가 없는 한, 이들 법의 보호대상인 개인정보에 해당하지 않는다는 견해가 존재한다. 정준현, "개인정보의 이전형태에 따른 "정보통신망법" 등의 적용과 한계에 관한 검토", 「법학논총」 제36권 제1호, 단국대학교 법학연구소, 2012. 6, 49면; 이승길, "정보화 사회에서의 개인정보권의 침해와 그 구제", 「중앙법학」 제11집 제1호, 중앙법학회, 2009. 4, 54면.

40) 현행 개인정보보호법상의 개인정보 개념정의가 이러한 개인에 관한 정보(information concerning a person)까지 포괄하는 경우에는, 민주주의에서의 표현의 자유가 갖는 비판 감시기능이 제대로 작동될 수 없게 되는 위험성이 발생한다는 점에서, 현행 개인정보보호법상의 개인정보 개념범위의 확장을 비판하는 견해가 존재한다. 박경신, "사생활의 비밀의 절차적 보호규범으로서의 개인정보보호법리 - 개인정보보호법 및 위치정보보호법의 해석 및 적용의 헌법적 한계", 「공법연구」 제40집 제1호, 한국공법학회, 2011. 10, 130-133면.

41) 고유식별정보는 법령에 의해서 개인에게 부여된 것이므로, 기업, 학교 등이 소속 구성원에게 부여하는 사번, 학번 등은 고유식별정보가 아니며, 또한 법인이나 사업자에게 부여되는 법인등록번호, 사업자등록번호 등도 고유식별정보가 될 수 없다. 김재광, "개인정보보호법에 관한 새로운 법적 문제", 「강원법학」 제36권, 강원대학교 비교법학연구소, 2012. 6, 108-109면.

내용상 '개인식별정보'(개인정보보호법 제2조 제1호의 개인정보 중 '개인을 알아볼 수 있는 정보')와 '개인식별가능정보'(개인정보보호법 제2조 제1호의 개인정보 중 '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것'. 즉 단편 정보 혹은 모자이크 정보)[42] 간의 구분[43]이 가능하다.[44] 그런데 개인정보보호법상 개인정보 개념정의의 핵심지표가 '개인의 동일성의 식별가능성'이라는 점을 염두에 둔다면, 이러한 개인의 동일성의 식별가능성을 담보해 낼 수 있는 '정도'에 있어서는 개인식별정보와 개인식별가능정보 간에는 분명한 차이가 존재한다고 할 수 있다. 이러한 차원에서 개인식별정보와 개인식별가능정보 간의 보호 정도의 차별화는 어느 정도 가능할 것으로 판단된다.

## 3. 충돌되는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화

개인정보 보호와 다른 헌법적 가치의 조화의 방향성 및 기준을 제시하기 위해서는, 위에서 언급한 개인정보간의 차별화 혹은 개인정보별 보호 정도의 차별화뿐만 아니라, 개인정보 보호와 충돌되는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화도 고려될 필요가 있다. 즉 개인정보의 종류 및 성격, 수집목적, 이용형태, 정보처리방식 등에 따라 개인정보자기결정권의 제한이 인격권 또는 사생활의 자유에 미치는 영향이나 침해의 정도는 달라지므로, 개인정보자기결정권의 제한이 정당한지 여부를 판단함에 있어서는 위와 같은 요소들과 동시에 추구하는 공익의 중요성도 고려해야 한다.[45]

그런데 개인정보자기결정권의 제한을 통해서 추구하는 공익은, 우리 헌법재판소의 판례상에서 나타난 바와 같이, '범죄수사 목적', '민원인의 편의 도모, 행정의 효율성 및 투명성의 제고', '공적 급여의 수급자격 및 급여액의 객관성과 공정성 확보', '조세행정의 효율성 확보' 및 '조세정의 및 형평의 실현', '의료이용자의 의료급여 수급자 해당 여부 및 의료급여의 범위 등의 정확성', '채무이행의 간접강제 및 거래의 안전 도모', '법적 분쟁의 공정한 해결' 등과 같은 객관적 공익일 수도 있다. 하지만 타인의 표현의 자유나 언론의 자유, 예술의 자유, 혹은 타인의 영업의 자유도 개인정보자기결정권의 제한을 정당화할 수 있는 헌법적 가치가 될 수 있다.

따라서 개인정보 보호와 표현의 자유나 언론의 자유, 예술의 자유, 영업의 자유가 충돌하는 상황이 발생하는 경우에, 그 조화의 방향성 및 기준을 제시하기 위한 방법 중의 하나로, 개인정보 보호와 충돌하는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화도 하나의 중요한 고려요소로서 기능할 수 있다.

일반적으로 표현의 자유 내지 언론의 자유는 개인이 표현 내지 언론 활동을 통하여 자기의

---

42) 예컨대 인터넷 이용자가 인터넷 검색창에 검색어를 입력하는 경우, 이러한 검색어가 여기서 말하는 개인식별가능정보에 해당한다고 이해된다. 왜냐하면 검색어는 그 자체만으로는 특정한 개인을 알아볼 수 없지만, 예컨대 IP주소나 쿠키 등과 같은 다른 정보와 쉽게 결합하여 특정한 개인을 알아볼 수 있는 정보이기 때문이다. 허순철, "인터넷 검색과 개인정보자기결정권", 「공법학연구」 제10권 제2호, 한국비교공법학회, 2009. 5, 168-169면. 한편 개인정보를 암호화한 정보가 개인정보에 해당하느냐와 관련하여, 당해 암호의 발신자 및 수신자에 있어서는 용이하게 해당정보를 개인을 식별하는 정보로 복원할 수 있다면 개인정보에 해당하지만, 일반적으로 그 암호에 접근한 제3자에 의하여 당해 정보로부터 특정 개인을 식별할 수 없기 때문에 개인정보에 해당하지 않는다는 견해가 있다. 김주영·손형섭, 「개인정보 보호법의 이해 - 이론·판례와 해설 -」, 법문사, 2012, 162면.

43) '직접 식별 개인정보'와 '간접 식별 개인정보'의 구분으로 불리기도 한다. 이기혁·이강신·박진식·최일훈, 「알기 쉬운 개인정보보호의 이해와 활용」, 인포더북스, 2011, 19-20면.

44) 한편 현행 개인정보보호법 및 정보통신망법상의 개인정보 범위의 포괄성에 대해서는, 특정 개인과의 결합성이 일시적으로 결여되어 있거나 약한 단편(모자이크) 정보가 다른 특정성이 있는 정보와 융합(결합)될 가능성으로 인한 침해 위험의 증대를 방지하기 위해서 타당한 입법이라는 견해가 존재한다. 임규철, "개인정보의 보호범위", 「한독법학」 제17호, 한독법률학회, 2012. 2, 225면.

45) 헌재 2005. 7. 21. 2003헌마282, 개인정보수집 등 위헌확인.

인격을 형성하는 개인적 가치인 자기실현의 수단임과 동시에 사회 구성원으로서 정치적 의사결정에 참여하는 사회적 가치인 자기통치(self-government)를 실현하는 수단이다. 특히 다른 기본권과의 관계에서 표현의 자유 내지 언론의 자유가 가지는 우월적 지위를 고려할 때[46], 개인정보자기결정권과 표현의 자유 내지 언론의 자유가 충돌하는 경우에는, 사안마다 구체적인 조화 및 형량은 다를 수 있겠지만, 원칙적으로 표현의 자유 내지 언론의 자유가 우선되어야 한다. 예술의 자유도 표현의 자유 내지 언론의 자유와 마찬가지로 정신적 기본권의 범주에 해당한다는 점에서 마찬가지이다.

예컨대 2012. 1. 25 발표된 EU의 일반정보보호규정(General Data Protection Regulation)안[47] 제17조는 '잊혀질 권리 및 삭제할 권리(right to be forgotten and to erasure)'라는 제목하에 개인정보의 삭제 및 배포중지에 관한 사항을 규정하고 있다. 그런데 제17조 제3호는 개인정보의 삭제 및 배포중지에 관한 정보주체의 권리의 예외를 규정하고 있다.

우선 동조 제3(a)호는 개인정보의 보유가 제80조에 따라 표현의 자유에 관한 권리를 행사하기 위해 필요한 경우에는 삭제의 예외를 인정하고 있다. 그런데 보다 구체적으로 잊혀질 권리가 표현의 자유와 충돌하는 경우 어떻게 조화시킬 것인가에 대한 기준과 관련하여서는, 동 규정 제80조가 규정하고 있다. 동 규정 제80조는 '개인정보의 처리 및 표현의 자유'(processing of personal data and freedom of expression)라는 제목하에 회원국으로 하여금 순전히 보도 목적(journalistic purposes)이나 예술 또는 문학적 표현의 목적만을 위하여 개인정보가 처리되는 경우에는 동 규정이 제시하고 있는 개인정보 보호에 관한 일반원칙, 정보주체의 권리, 개인정보관리자 및 처리자에 관한 사항, 개인정보의 이전 등에 관한 사항의 예외로 설정해야 한다고 규정하고 있다. 따라서 정치·경제·사회·문화·시사 등에 관한 보도·논평·여론 및 정보 등을 전파할 목적으로 취재·편집·집필한 기사 등과 같이 언론이나 보도 기능을 수행하기 위한 표현이나 예술 또는 문학을 위한 표현의 경우에는 그 중에 개인정보가 포함된다고 하더라도 잊혀질 권리가 제한된다고 이해된다. 문제는 언론보도, 예술, 문학의 범주에 속하지 않는 표현에 대한 권리와 잊혀질 권리가 충돌하는 경우, 위 예외의 범주에 포함시키거나 유추적용할 수 있을 것인가가 논란이 될 수 있는데, 법에 명시적으로 규정되어 있지 않은 이상 확대하는 것은 어렵다는 지적이 있다.[48]

우리나라의 개인정보보호법도 제58조에서 '적용의 일부 제외'라는 제목하에 네 가지 종류의 개인정보에 대해서는 동법 제3장부터 제7장까지를 적용하지 아니한다고 규정함으로써(동조 제1항), 이들 개인정보에 대해서는 '일괄적 전부배제방식'을 적용하고 있다. 그러한 개인정보로는 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보(제1호), 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보(제2호), 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보(제3호), 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보(제4호)가 그것이다. 그리고 제58조 제3항에서는 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경

46) 헌재 1998. 4. 30. 95헌가16, 출판사및인쇄소의등록에관한법률 제5조의2 제5호 등 위헌제청.
47) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
48) 최경진, "잊혀질 권리 - 개인정보 관점에서", 「정보법학」 제16권 제2호, 한국정보법학회, 2012. 8, 108면.

우에는 개인정보 수집·이용조항(제15조), 개인정보 처리방침의 수립 및 공개조항(제30조), 개인정보 보호책임자의 지정조항(제31조)을 적용하지 아니한다고 규정함으로써, '개별적 일부 배제방식'도 또한 도입하고 있다.

한편 개인정보보호법 제58조 제1항 제4호가 규정하고 있는 언론의 취재·보도에서 '언론'의 범위가 어디까지인가가 문제될 수 있다. 이에 대한 단서가 될 수 있는 것이 바로 「언론중재 및 피해구제 등에 관한 법률」(이하 '언론중재법'이라 함) 제2조 제1호가 규정하고 있는 '언론'의 개념정의이다. 언론중재법 제2조 제1호는 언론을 '방송, 신문, 잡지 등 정기간행물, 뉴스통신 및 인터넷신문'이라고 개념정의내리고 있다. 하지만 개인정보보호법 제58조 제1항 제4호가 규정하고 있는 언론의 범위는 '방송, 신문, 잡지 등 정기간행물, 뉴스통신 및 인터넷신문'에 국한되지 않고, 공직선거법 제8조의5 제1항이 규정하고 있는 '인터넷언론'[49]까지 포괄하고 있는 것으로 해석되고 있다.[50] 개인정보자기결정권과 언론의 자유가 충돌하는 경우에, 원칙적으로 언론의 자유가 우선되어야 한다는 관점에서 본다면, 일괄적 전부배제의 대상에 전통적인 의미에서의 언론뿐만 아니라 새로운 형태의 언론인 인터넷언론까지 포함시키는 것은 바람직하다고 할 수 있다.

다만 여기서 비상업적 표현 v. 상업적 표현의 구분도 고려되어야 하는지가 문제될 수 있다. 특히 광고와 같은 상업적 표현의 자유 혹은 광고표현의 자유와 개인정보자기결정권이 충돌하는 경우에 어떻게 조화시키고 형량할 것인가가 문제될 수 있는 것이다. 일반적으로 광고가 단순히 상업적인 상품이나 서비스에 관한 사실을 알리는 경우에도 그 내용이 공익을 포함하는 때에는 헌법 제21조의 표현의 자유에 의하여 보호된다는 것이 우리 헌법재판소의 입장이다.[51] 그런데 상업광고는 표현의 자유의 보호영역에 속하지만 사상이나 지식에 관한 정치적, 시민적 표현행위와는 차이가 있기 때문에, 그 보호 정도에 있어서는 사상이나 지식에 관한 정치적, 시민적 표현행위보다 완화될 수 있다.[52] 이러한 측면에서 본다면, 광고표현의 자유와 개인정보자기결정권이 충돌하는 경우에는 개인정보자기결정권이 우월하거나 혹은 두 가지 기본권이 동일한 가치를 지닌다는 일응의 기준이 가능할 수 있다. 한편 상업광고는 직업수행의 자유 내지 영업의 자유의 보호영역에 속하기도 하므로[53], 영업의 자유와 개인정보자기결정권의 충돌시 그 조화의 방향성 내지 기준에 의해서 해결될 여지도 존재한다.

한편 개인정보자기결정권과 영업의 자유가 충돌하는 경우에, 영업의 자유가 특히 표현의 자유와 비교해 보았을 때 갖는 중요도 및 보호정도를 고려한다면, 개인정보자기결정권이 우월하거나 혹은 개인정보자기결정권과 영업의 자유라는 두 가지 기본권이 동일한 가치를 지닌다는 기준이 가능할 수 있다. 따라서 표현의 자유 내지 언론의 자유, 예술의 자유의 경우와는 달리 그 조화의 방향성 및 기준이 달라질 수 있다.

이와 같은 일반론적인 관점에서 본다면, EU의 일반정보보호규정(General Data Protection Regulation) 제80조의 규정 중에서, 언론보도, 예술, 문학의 범주에 속하지 않는 표현, 예컨대 광고와 같은 상업적 표현의 자유와 같이 상대적으로 보호의 가치가 낮은 표현의 자유에 대하여는 잊혀질 권리가 우선하여 적용된다는 논리가 가능하게 된다. 그리고 우

---

49) 공직선거법 제8조의5 제1항상의 '인터넷언론'개념은 "신문법상의 인터넷신문, 정치·경제·사회·문화·시사 등에 관한 보도·논평·여론 및 정보 등을 전파할 목적으로 취재·편집·집필한 기사를 인터넷을 통하여 보도·제공하거나 매개하는 인터넷 홈페이지, 이와 유사한 언론의 기능을 행하는 인터넷 홈페이지"로 정의된다.

50) 행정안전부, 「개인정보 보호법령 및 지침·고시 해설」, 2011. 12, 353-354면.

51) 헌재 2002. 12. 18. 2000헌마764, 옥외광고물등관리법 제3조 제1항 제6호 등 위헌확인.

52) 헌재 2005. 10. 27. 2003헌가3, 의료법 제69조 등 위헌제청.

53) 헌재 2000. 3. 30. 97헌마108, 식품위생법 제11조 위헌확인.

리 개인정보보호법도 제58조 제1항 제4호에서 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보를 일괄적 전부배제방식의 대상으로 삼고 있는 점에 비추어 볼 때, 언론의 자유, 종교의 자유, 정당의 자유보다는 영업의 자유의 보호정도를 완화시키는 것을 전제하고 있다고 해석할 수 있다. 물론 일반론적인 차원에서 영업의 자유의 보호정도가 언론의 자유, 예술의 자유, 종교의 자유, 정당의 자유보다 완화된다고 하더라도, 영업의 자유도 엄연한 헌법상의 권리이자 자유이므로, 영업의 자유를 형해화시킬 정도로 개인정보 보호를 강화할 수는 없을 것이다. 이러한 관점에서, 개인정보보호법에 삭제요구권이 포함된 것은 정보주체의 개인정보자기결정권을 두텁게 보호한다는 면에서 바람직하지만, 그로 인하여 정보처리자의 영업의 자유 등 다른 헌법적 가치가 훼손될 수 있기 때문에 신중하게 접근하였어야 할 과제였고, 개인정보자기결정권과 충돌되는 다른 헌법적 가치와의 비교형량이 충분히 이루어졌는지에 대해서는 의문을 제기하는 견해도 존재한다.[54] 따라서 개인정보자기결정권과 영업의 자유가 충돌하는 경우에는, 위에서 언급한 개인정보의 종류에 따른 개인정보별 보호 정도의 차별화원리를 적용하여 그 조화의 방향성과 기준을 다시 차별화하는 것도 고려할 수 있다.

## 4. 개인정보 보호와 표현 자유 및 영업 자유와의 조화의 방향성 및 기준

지금까지 필자는 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 기준을 모색함에 있어서는 개인정보별 보호 정도의 차별화가 가능한지에 대한 검토, 개인정보 보호와 충돌되는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화가 가능한지에 대한 검토를 원론적이고 추상적인 관점에서 행하였다.

지금까지의 원론적이고 추상적인 검토에 따르면, 개인정보 보호와 다른 헌법적 가치가 충돌하는 경우에 다음과 같은 방향성 및 추상적인 기준이 일응 도출될 수 있음을 알 수 있다.

| 기본권의 종류 / 개인정보 유형 | | 표현의 자유 | | 영업의 자유 |
|---|---|---|---|---|
| | | 언론보도의 자유 | 사적 표현 및 광고표현의 자유 | |
| 민감정보 (고유식별정보 포함) | | 개인정보 보호가 우월 | 개인정보 보호가 우월 | 개인정보 보호가 우월 |
| 비민감정보 | 개인식별정보 | 언론보도의 자유가 우월 | 사안에 따라 유동적 | 사안에 따라 유동적 |
| | 개인식별가능 정보 | 언론보도의 자유가 우월 | 사적 표현 및 광고표현의 자유가 우월 | 영업의 자유가 우월 |

위의 도표를 설명하면 다음과 같다.

우선 개인정보별 보호 정도의 차별화가 가능하다는 것을 전제로 하여, 민감정보와 비민감정보의 구분이 가능할 것이다. 위의 도표에서의 민감정보란 현행 '사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 유전자검사 등의 결과로 얻어진 유전

54) 문재완, "프라이버시 보호를 목적으로 하는 인터넷 규제의 의의와 한계 - '잊혀질 권리' 논의를 중심으로 -", 「언론과 법」 제10권 제2호, 한국언론법학회, 2011. 12, 23면.

정보, 범죄경력자료에 해당하는 정보'(개인정보보호법 제23조 및 동법 시행령 제18조)와 고유식별정보(개인정보보호법 제24조 및 동법 시행령 제19조)를 의미한다. 즉 현행 개인정보보호법상의 민감정보와 고유식별정보를 포괄하는 것을 의미한다. 이러한 민감정보에 대해서는 현행 개인정보보호법상 '원칙적 처리 금지, 예외적 처리 허용'이라는 정책을 적용하고 있을 뿐만 아니라, 그 활용 내지 이용시 인간의 존엄성, 인격권 또는 사생활의 자유에 미치는 영향이나 침해의 정도가 크다는 점에서, 그 보호가 표현의 자유 혹은 영업의 자유보다 원칙적으로 우월하다고 보아야 할 것이다. 물론 구체적인 사안에 따라서는 민감정보의 활용 내지 이용이 헌법적으로 정당화되는 경우가 존재할 수 있다는 점은, 이미 위에서 헌법재판소의 판례를 통해서 확인한 바 있다.

한편 위의 도표에서 비민감정보란 '민감정보를 제외한 모든 개인정보'라고 할 수 있다. 그런데 이러한 비민감정보는 '개인의 동일성의 식별가능성'이라는 관점에서 '개인식별정보'(개인정보보호법 제2조 제1호의 개인정보 중 '개인을 알아볼 수 있는 정보')와 '개인식별가능정보'(개인정보 보호법 제2조 제1호의 개인정보 중 '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것'. 즉 단편 정보 혹은 모자이크 정보)로 구분이 가능하다.

개인식별정보의 경우에는, 개인정보 보호와 표현의 자유 혹은 영업의 자유가 충돌할 때, 언론보도의 자유를 제외하고는, 사안에 따라 그 조화 및 형량의 결과는 달라질 수 있다. 즉 이러한 경우에는 당해 개인정보의 구체적인 종류 및 성격, 수집목적, 이용형태, 정보처리방식, 사적 표현 및 광고표현의 자유, 영업의 자유 등에 미치는 영향 등을 종합적으로 고려해서 판단해야 할 것이다.

하지만 개인식별가능정보의 경우에는, 그 자체만으로는 특정 개인을 알아볼 수 없는 정보이므로, 이러한 정보에 대한 보호와 표현의 자유 혹은 영업의 자유가 충돌하는 경우에는, 원칙적으로 표현의 자유 혹은 영업의 자유가 우선되어야 한다고 본다. 이러한 관점에서 본다면, 현행 개인정보보호법이 개인식별가능정보도 개인정보의 개념범위에 포섭시켜서 개인식별정보와 동일한 정도의 보호를 적용하는 것은 문제가 될 수 있다. 즉 개인식별가능정보의 경우에는, 개인정보자기결정권과 표현의 자유 혹은 영업의 자유 간의 충돌에 있어서 개인정보자기결정권을 지나치게 보호할 가능성이 높은 것이다.

결론적으로 지금까지의 논의를 입법론적으로 적용한다고 할 때, 개인식별정보와 개인식별가능정보를 구분해서, 그 보호 정도 및 방법의 차별화를 도모할 필요가 있다. 구체적인 입법방향과 관련하여서는 다음과 같은 두 가지 방안이 가능할 것이다.

첫째, 처음부터 개인정보에 관한 개념정의에서 개인식별가능정보를 배제하는 방법이다. 이 방법의 장점은 우선 입법기술적으로나 입법경제적으로 제일 수월하거나 효율적일 수 있다는 점이다. 왜냐하면 현행 개인정보보호법상의 개인정보의 개념정의에서 괄호 안의 내용을 삭제하면 되기 때문이다.[55] 그리고 현재의 개인정보보호법이 지나치게 개인정보의 '보호'에 치우쳐 있다는 비판을 상당 정도 불식시킬 수 있다는 점도 장점으로 지적될 수 있다. 왜냐하면 애초부터 보호의 대상이 되는 개인정보의 범위를 제한할 수 있고, 따라서 표현의 자유 혹은 영업의 자유와 충돌될 수 있는 경우의 수가 줄어들 수 있기 때문이다. 하지만 우리 헌법재판소가 개인정보의 개념정의 및 범위의 외연을 광범위하게 설정하고 있다는 점, 헌법상 명문으로 규

55) 이 방법을 채택하는 경우에는 현행 개인정보보호법상의 개인정보의 개념정의는 "살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보"로 재구성될 수 있을 것이다.

정되어 있지 않은 개인정보자기결정권이라는 기본권의 보호범위를 설정하는 것은 궁극적으로 헌법재판소의 역할이라는 점, 개인정보의 개념정의 및 범위의 외연에 관한 헌법재판소의 해석이 최종적인 유권해석이라는 점, 하위 입법인 법률에서 헌법재판소가 제시한 개인정보의 외연을 축소하기가 쉽지 않다는 점 등을 고려할 때, 채택되기 쉽지 않을 것으로 판단된다.

둘째, 현행과 같이 개인정보에 관한 개념정의에 개인식별가능정보를 포함시키되, 개인정보의 수집, 처리, 보관과 관련된 각종 규제장치나 규제방식, 기타 개인정보 보호관련 시스템을 개인식별가능정보에 대해서는 차별적으로 완화해서 적용하거나 아니면 아예 면제하는 방법이다. 이 방법은 헌법재판소가 제시한 개인정보의 개념정의 및 범위의 외연을 그대로 유지할 수 있다는 점에서 장점을 갖고 있다. 뿐만 아니라 이 방법도 위의 첫 번째 방법과 마찬가지로 현재의 개인정보보호법이 지나치게 개인정보의 '보호'에 치우쳐 있다는 비판을 상당 정도 불식시킬 수 있다는 점에서 장점을 갖고 있다고 볼 수 있다. 다만 이 방법이 현실성을 담보하고 개인정보의 보호와 활용 사이에서 균형을 유지하는 방법이 되기 위해서는, 개인정보의 수집, 처리, 보관과 관련된 각종 규제장치나 규제방식, 기타 개인정보 보호관련 시스템을 어떻게 구체적으로 유형화하고 차별화할 것인가가 제시되어야 한다. 이와 관련하여 현행 개인정보보호법 제58조 제3항에서 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 개인정보 수집·이용조항(제15조), 개인정보 처리방침의 수립 및 공개조항(제30조), 개인정보 보호책임자의 지정조항(제31조)을 적용하지 아니한다고 규정함으로써, 이미 '개별적 일부배제방식'을 채택하고 있는 것에 비추어 볼 때, 개인정보 보호관련 시스템 적용의 차별화가 입법론적으로 불가능한 것으로 보이지는 않는다.

# Ⅳ. 나오는 말

지금까지 필자는 일반적으로 개인정보 보호와 기타 헌법적 가치 간의 충돌을 조화시키기 위한 법익형량에 있어서, 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준을 제시하였다. 개인정보 보호와 다른 헌법적 가치 간의 조화를 위한 방향성 및 추상적인 기준을 모색함에 있어서는 다음과 같은 사항들을 고려하였다.

첫째, 개인정보별 보호 정도의 차별화가 가능한지에 대한 검토가 필요하다는 점이다.

둘째, 개인정보 보호와 충돌되는 다른 헌법적 가치의 중요도 및 보호 정도의 차별화가 가능한지에 대한 검토가 필요하다는 점이다.

위와 같은 두 가지 고려요소들을 전제로 하여, 필자는 개인정보 보호와 표현 자유 및 영업의 자유와의 조화의 방향성 및 기준을 추상적인 수준에서 제시하였다.

궁극적으로 이러한 작업이 의미있는 이유는, 개인정보 보호 v. 개인정보 활용 간의 구도에 있어서 어떻게 균형을 유지하고, 상호 대립되는 목표를 어떻게 조화시킬 것인가의 문제를 해결하기 위한 기본전제이기도 하고, 더 나아가서 보다 구체적인 법제도 및 정책을 설계하는데 있어서 주요한 지침이 될 수 있기 때문이다.

개인정보자기결정권과 표현의 자유 및 영업의 자유 간의 충돌에 있어서 '헌법적 균형'을 유지하는 것이 필요하고, 더 나아가서 '입법적·사법적 균형'도 유지될 필요가 있을 것이다. 이러한 맥락에서 이 글에서 제시하고 있는 방향성 및 기준이, 비록 원론적이고 추상적인 수준이지만, 그러한 균형을 유지하기 위한 하나의 방향타 내지 지침으로서 기능할 수 있기를 기원하면서 이 글을 마친다.

# 개인정보보호의 법, 경제, 및 이노베이션

서울대학교 법학전문대학원 교수 고학수

## Ⅰ. 들어가는 말

개인정보의 활용은 이노베이션을 촉진시키는 중요한 기능을 하고, 이를 통해 사회와 경제에 도움이 되는 다른 많은 기능 또한 제공될 수 있다. 따라서 개인정보의 수집과 이용에 대한 규제를 고려함에 있어, 개별 규제가 이노베이션 활동을 포함하여 사회와 경제에 미치는 영향에 대한 엄밀하고 상세한 분석을 할 필요가 있다. 이를 통해, 개인정보의 활용을 통해 발생할 수 있는 역기능은 최대한 억제하고, 반면에 순기능을 장려하는 방향의 정책설계를 할 필요가 있다.

규제나 정책에 관해 논의함에 있어, 개인정보의 수집과 이용은 일반적으로 문제를 발생시킬 가능성이 높을 것이라는 막연하고 피상적인 전제하에 정책을 수립하는 것은 매우 위험한 발상일 수 있다. 특히, 개인정보의 보호와 개인정보의 수집 및 이용 사이에는 항상 상충관계(trade-off)가 있어서, 개인정보의 보호수준을 높이기 위해서는 개인정보의 수집과 이용을 제한하는 것이 필수적이라고 전제하는 것은, 논리적으로나 실증적으로나 근거가 매우 미약한 것이고, 따라서 이에 기초하여 논의를 진행하는 것은 잘못된 결론을 도출하게 될 가능성이 높다. 실제로는 개인정보의 수집과 이용이 개인정보의 적절한 보호에 문제를 발생시키는 상황도 있고, 그렇지 않은 상황도 있을 것이다. 정책결정은, 문제가 될 수 있는 '시장의 실패'(market failure) 상황이나 기타 구체적인 문제상황에 대한 과학적이고 실증적인 분석을 진행한 뒤에 그에 근거하여 이루어져야 한다. 그리고 그러한 문제의 가능성이나 크기가 확인되지 않는 상황에 대해서는 시장의 기능이 충분히 발휘되어 새로운 기술이 계속 개발되고 시장에 도입되어 활용될 수 있는 방향으로 규제의 틀을 정립해야 할 필요가 있다.

다른 한편, 개인정보는 그 속성상 매우 쉽게 국경을 넘나들 수 있을 것인데, 규제기관은 국내기업이 해외에서 영업활동을 함에 있어 불이익을 받지 않도록 배려하고 이를 위해 필요한 조치를 해야 할 필요가 있다. 개인정보보호의 맥락에서는, 그 중에서도 해외정보의 국내이전이 중요한 이슈가 될 것인데, 이에 관해 규제기관이 어떠한 역할을 할 필요가 있을 것인지 적극적으로 생각해 보아야 한다.

이 글은 개인정보의 보호에 관하여 규제기관이 어떠한 원칙 하에서 규제의 틀을 마련해야 할 것인지에 대해 근본적인 차원의 문제제기를 하고, 그에 대해 몇 가지 해답이나 방향을 제시하고자 하는 글이다. 이하에서는 개인정보보호에 관한 규제에 있어 생각해야 하는 대원칙에 관해 우선 생각해 본다. 그리고, 개인정보보호의 법제가 이노베이션이나 기타 정보의 수집 및 활용 등을 함에 있어 미치는 영향이 어떠한지 또 그러한 영향에 관한 판단을 하기에 앞서 사전적으로 이루어져야 하는 분석은 어떤 것인지에 관해 살펴보도록 한다. 구체적으로는 규제가 온라인 광고 시장에서의 이노베이션에 미치는 영향에 관한 분석, 이용자들의 실제 행태에 기초한 정보보호의 필요성에 관한 분석, 정보의 수집과 이용 등에 대하여 이용자들로부터 동의를 구하는 것에 관한 분석 등으로부터 시사점을 얻도록 한다. 시사점을 제시하는 분석들은 모두 국내가 아닌 외국의 통계나 사례에 기초한 것인데, 이는 지금까지 국내의 통계나 국내 상황에 기초한 엄밀한 분석이 거의 이루어지지 않은 현실을 반영하는 것이기도 하고, 다른 한편

앞으로 국내 데이터에 기초한 과학적인 분석이 절실하게 필요하다는 것을 보여주는 것이기도 하다. 마지막으로 국내기업이 외국에서 영업활동을 하면서 외국에 있는 정보를 국내로 이전하는 것이 필요한 상황에 관해 살펴보고, 규제당국이 해야 할 역할에 대해 생각해 본다.

## Ⅱ. 개인정보보호의 법과 규제

개인정보의 수집과 이용에 대한 규제를 논의함에 있어 종종 발견되는 오류 중의 하나는, 개인정보를 이용하고자 하는 기업의 이익과 이용자의 이익이 일반적으로 서로 배치될 것이라고 전제하고 논의를 하는 것이다. 예를 들면, 정보의 광범위한 수집을 허용하면 이는 당연히 이용자의 이익에 반하는 결과가 초래될 것이라고 전제하는 것이다.

그런데 이러한 전제가 실제의 상황에 부합되는 것인지에 대해서는 명확한 근거가 없다. 오히려 이러한 전제와는 달리, 개인정보와 관련된 사항에 있어서도 다른 많은 경제활동의 경우와 마찬가지로 기업활동이 이용자의 이익에 부합되는 상황도 있고, 그 반대로 이용자의 이익에 저해되는 상황도 있을 것이다. 일반적으로 규제의 목적은, 기업활동이 이용자의 이익을 저해하는 경우를 정확히 파악하여, 그러한 상황이 발생하는 것을 방지하고 억제하는 것에 있는 것이지, 기업활동이 전반적으로 부정적인 효과를 가질 것이라고 전제하고 기업활동을 전반적으로 제약하는 것에 있지 않다.

새로운 기술이 시장에 도입될 때, 그로 인해 발생될 수 있는 문제점에 특히 주목하여 강력한 규제를 주장하는 경우를 종종 볼 수 있다. 하지만 문제를 정확히 파악하여 최적(optimal)의 규제를 하는 것이 중요한 것이고, 지나치게 광범위하거나 과다한 규제를 하는 것은 역효과를 가져올 수 있다. 개인정보보호와 관련된 맥락에서는, 개인정보의 수집과 이용 등에 있어 발생될 수 있는 문제가 어떤 것인지 명확하게 파악하고 체계화하여, 구체적으로 발생가능하고 중대한 문제에 대해 체계적인 해결책을 모색하는 정책적인 태도가 필요하다. 즉, 정책에 대한 논의에 앞서, 구체적으로 인터넷 등의 이용에 있어 개별 이용자에게 발생할 수 있는 개인정보관련 문제가 어떤 것인지에 관해 실제 데이터에 기초한 정확한 파악과 분석이 선행되어야 한다.

## Ⅲ. 개인정보의 활용에 대한 규제가 이노베이션에 미치는 영향

아래에서는 몇 가지 사례 및 연구결과를 통해 규제가 이노베이션에 미치는 영향에 대해 검토해 보고, 개인정보보호 법제에 관한 논의를 함에 있어 특히 유의해야 할 시사점에 대해 생각해 본다.

우선, 개인정보의 활용에 대한 규제가 이노베이션에 영향을 미치는 상황에 대한 실증분석의 한 예로, 유럽에서의 온라인상거래에 대한 규제강화가 광고의 효과에 미친 영향에 대하여 분석한 연구사례를 들 수 있다.[1] 이 연구는 유럽에서 e-Privacy Directive의 도입을 통한 규제의 강화가 광고의 효과를 65%나 저하시키는 결과를 초래하였음을 보여주었다.[2]

규제강화는 광고의 효과를 이처럼 매우 크게 떨어뜨리는 결과를 가져왔는데, 그와 동시에 웹사이트의 유형이나 광고의 성격 등에 따라서 그 영향에 있어 커다란 차이가 있다는 것 또한 이 연구를 통해 확인되었다. 첫째, 뉴스 사이트 등 특정 영역에 특화되지 않은 범용 사이트는

1) A. Goldfarb and C. Tucker (2011), "Privacy Regulation and Online Advertising", Management Science, 57(1), 57-71.

2) 통상 e-Privacy Directive라 지칭되는 이 지침(Directive 2002/58/EC)은 2002년에 제정된 것으로 공식적인 이름은 Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector 이다.

여행 사이트나 쇼핑 사이트 등 특정 영역에서의 상품판매에 주력하는 사이트에 비해 규제로 인해 훨씬 커다란 영향을 받게 된다는 것이다. 둘째, 배너광고 등 정보제공을 위주로 하는 유형의 광고는 플래시 등을 적극 활용하는 화려하고 자극적인 형태의 광고보다 영향을 크게 받는다는 것이다.

이와 같은 연구결과가 시사하는 바는, 새로운 규제의 도입이나 기존 규제의 수정에 있어, 그 전반적 영향이 어떠할지에 대한 상세한 분석이 필요할뿐더러, 각기 다른 유형의 규제대상자들에 미칠 영향에 대한 미시적인 면밀한 분석 또한 요구된다는 것이다. 예를 들어, 규제의 일괄적인 강화는 사이트의 유형이나 광고의 유형에 따라 차별적인 영향을 가져오게 될 것이므로 그에 관한 검토와 분석이 요구된다. 특히, 중립적인 형태의 규제일지라도 그 결과는 크게 차별적인 것으로 나타날 수 있고 그 중에서도 특정 규제가 언론 사이트 등 일부 유형의 사이트에 매우 중대하고도 차별적인 영향을 가져오게 되는 경우, 이는 온라인 '생태계'에 직접적인 영향을 미치는 것은 물론이고 이로 인해 언론 및 표현의 자유나 영업의 자유 등 헌법적 가치와 관련된 새로운 문제가 제기되면서 추가적인 파장이 발생될 수도 있다.

그런데 개인정보의 수집과 이용 등과 관련된 규제의 영향에 대하여, 국내자료를 이용한 체계적이고 실증적인 분석은 아직 본격적으로 이루어지지 않고 있는 것으로 보인다. 규제로 인해 발생된 효과나 영향에 대한 분석은 당연히 이루어져야 하는 꼭 필요한 것이고, 또한 향후 지속적으로 반복되어야 하는 작업이다. 더 기본적으로는, 국내 인터넷 환경에서 이용자에 대한 트래킹(tracking) 등 정보수집 활동이 어떤 방식으로, 얼마나 광범위하게 이루어지고 있는지에 대한 기초자료의 확보 및 그에 기초한 분석이 절실하게 필요하다.[3] 예를 들어, 국내 웹사이트들이 HTTP 쿠키, 플래시 쿠키(local shared objects), 웹버그(web bug), DPI(deep packet inspection) 등 트래킹 기술을 이용하여 정보를 수집하는 현황에 대해 파악하고, 그로부터 개별 기술의 활용도에 영향을 미치는 여러 요소들에 대한 상세한 분석을 하는 것이 필요하다. 트래킹 기술의 활용현황을 파악한 뒤, 그로부터 기술의 활용에 영향을 미치는 법적, 제도적 요소에 대한 분석, 이용자 행태에 대한 분석, 광고시장의 구조에 대한 분석, 소프트웨어 업계의 구조에 대한 분석 등 상세한 분석을 수행하는 것은 실효성 있는 규제의 틀을 짜기 위한 중요한 전제가 될 것이다.

# Ⅳ. 개인정보보호의 중요성에 대한 이용자의 인식

개인정보보호관련 규제는 개인정보보호의 중요성에 대한 인식을 전제로 한다. 규제체계를 설계함에 있어, 규제의 실효성을 확보하기 위해서는 실제 일반 이용자들이 보이는 개인정보보호나 프라이버시 관련 우려의 내용이나 그와 연관된 실제 행태가 어떤지에 대한 면밀한 분석이 선행되어야 한다. 예를 들어, 20대는 인터넷의 활용도가 특히 높은 한편 개인정보의 보호를 위해 의식적인 노력을 기울이지 않는 경우가 많다고 판단되면, 일정한 수준의 국가후견인적(paternalistic) 규제가 정당화될 수도 있을 것이다. 그런데 중요한 것은 이러한 규제체계를 구상하기에 앞서, 실제 이용자들의 행태가 어떠한지에 대한 조사가 선행되어야 한다는 것이다.

실제로 20대는 50대나 60대에 비해서 개인정보보호를 소홀히 한다거나 덜 중요하게 여긴

3) 미국에서의 쿠키 등 트래킹 기술의 활용현황에 대한 보고와 분석의 예로는, A. Soltani et al. (2009), "Flash Cookies and Privacy"; M. Aynson et al. (2011), "Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning"; A. McDonald and L. Cranor (2011), "A Survey of the Use of Adobe Flash Local Shared Objects to Respawn HTTP Cookies" 참조.

다는 판단을 하기 위해서는, 일반 상식에 기초해서 추단해서는 곤란하고 이용자들의 의식과 실제 행태에 대한 정확한 사실관계 파악에 기초한 엄밀한 분석이 필요하다. 실제로 미국에서 행해진 연구에 따르면 20대가 50대에 비해서 개인정보보호를 덜 중요하게 생각한다고 판단할 수 있는 징후를 찾기 어렵다고 한다.[4] 오히려 언론 등에서 종종 전제되는 것과는 달리, 20대 이용자가 그보다 나이 많은 다른 세대의 이용자보다 더욱 개인정보의 노출가능성에 민감하게 반응하는 행태를 보인다고 한다. 이와 같은 연구와 조사가 국내의 인터넷 이용자를 대상으로 해서도 행해질 필요가 있다.

이와 같은 실제 이용자의 행태에 대한 엄밀한 조사가 필요한 중요한 이유 하나는, 개인정보의 보호나 프라이버시와 관련된 맥락에서는 개별 이용자의 행태가 개별 사안이나 상황에 따라서는 합리적(rational)이지 않거나 일관적이지 않은(inconsistent) 경우를 적지 않게 볼 수 있기 때문이다. 따라서, 실제 행태에 기초한 자료나 통계자료에 기반을 둔 엄밀한 분석을 하지 않고 직관이나 상식에서 출발하여 규제의 틀을 마련할 경우, 애초에 의도했던 정책목표를 달성하지 못하게 되는 것은 물론, 예상하지 못했던 부작용을 초래할 가능성도 있다.

프라이버시와 관련하여 이용자들이 보이는 구체적인 행태에 대해서는 아직 국내에서는 본격적인 연구가 이루어지지 못하고 있는 한편, 외국에서는 현재 매우 활발한 연구가 진행되고 있다. 지금까지의 연구를 통해 밝혀진 연구결과 중에서도 중요한 것 하나는, '프라이버시 패러독스'(privacy paradox)라고 불리는 현상이다.[5] 이는 간단히 말하면, 개인정보에 관하여 서베이 참여 등을 통해 개인이 표현하는 선호의 내용과 실제상황에서 행동을 통해 표출되는 선호의 내용 사이에는 상당한 차이가 있을 수 있다는 것이다. 좀 더 구체적으로 간단히 정리하면 다음과 같다. 첫째, 개인들은 흔히 개인정보의 보호를 원한다거나 매우 중요하게 생각한다고 말한다. 다른 한편, 둘째, 개인들은 약간의 비용을 지불하면 개인정보가 잘 보호될 수 있는 상황에서도 비용지불을 거부하고 개인정보가 공개될 위험성을 감수하는 경우가 많다. 그리고 더 나아가, 셋째, 개인들은 매우 적은 액수의 보상만 제시하더라도 민감한 정보를 흔쾌히 제시하는 경우가 많다. 이는 경제학적인 개념으로는 지불의사금액(willingness to pay)과 수용의사금액(willingness to accept) 사이의 괴리의 한 형태인 것으로 해석될 수 있다. 즉, 이용자가 정보를 보호하고자 할 때 요구되는 지불의사와 정보의 공개 맥락에서 생각하게 되는 수용의사 사이에서 매우 비일관적인 의사결정을 하는 경우를 많이 볼 수 있은데, 개인정보보호의 맥락에서는 이러한 괴리가 특히 극명하게 나타난다는 것이다.[6]

국내의 인터넷 이용자들을 대상으로 이와 같은 프라이버시 패러독스의 존재여부나 그 크기를 확인하는 것은 정책적으로 매우 중요한 의미를 지닌다. 왜냐하면, 프라이버시 패러독스가 크게 나타날 경우, 어떤 판단기준에 근거하여 개인정보보호의 중요성을 파악하는지에 따라 정책적 판단 또한 크게 달라질 수 있기 때문이다. 즉, 일반 이용자의 선호도에 대한 서베이 조사를 통해, 개인정보보호가 매우 중요하고 규제를 더욱 강화해야 한다는 결론을 쉽게 얻을 수도 있지만, 다른 한편으로는, 이러한 이용자들이 실제로 개인정보보호를 위해 비용을 지불해야 하는 경우에는 개인정보보호를 실질적으로 거부하는 행태를 보일수도 있으므로 판단에 주의해야

4) C. Hoofnagle et al. (2010), "How Different are Young Adults from Older Adults when it Comes to Information Privacy Attitudes and Policies".

5) A. Acquisti and J. Grossklags (2007), "What can behavioral economics teach us about privacy?" In Alessandro Acquisti et al. (Ed.), Digital Privacy: Theory, Technologies and Practices, pp. 363-377. Auerbach Publications (Taylor and Francis Group).

6) L. John, A. Acquisti, and G. Lowenstein (2011) "Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information", Journal of Consumer Research, Vol 37.

한다는 것이다. 따라서, 이용자에 대한 서베이 결과에만 기초하여 개인정보보호의 중요성 정도를 파악하는 것은, 개인정보보호의 중요성을 과대평가하게 되는 오류를 초래할 가능성이 상당히 높다.

이용자들의 구체적인 행태에 기초한 연구를 통해 발견된 또 다른 패러독스는 '콘트롤 패러독스'(control paradox)라고 하는 것이다.[7] 이에 따르면, 인터넷 이용자들은 자신의 개인정보에 대한 통제권을 많이 가지고 있다고 인식하고 있는 경우에 개인정보를 상대적으로 많이 공개하고, 그 반대로 통제권을 적게 갖고 있다고 인식하는 경우에는 개인정보를 적게 공개한다고 한다. 이 연구결과는, '정보의 자기통제권'에 기초하여 규제체계를 생각하는 것에 대해 시사하는 바가 많다. 이용자들에게 소위 '잊혀질 권리'(right to be forgotten)를 부여하는 등 이용자들에게 통제권을 많이 부여하는 방식의 규제는, 역설적이게도 이용자들이 자신의 개인정보를 많이 노출하도록 유도하는 결과를 초래할 수 있다는 것이다. 이러한 결과는 기본적으로 이용자들이 일반적으로 보이는 인지심리학적 속성에 기인하는 것이기 때문에, 실제로 이용자들이 정보에 대한 통제권을 적극적으로 행사하게 될 것인지 여부와는 무관하게 결정되는 사항이 될 것이다. 따라서 개인정보의 자기통제권을 강화하는 것에 대한 논의를 하더라도, 어떤 경우에 어떤 맥락(context)에서 규제의 내용이 변화하게 될 것인지 그리고 그러한 변화에 반응하여 이용자들의 행태가 구체적으로 어떻게 변화하게 될 것인지에 관하여 엄밀한 실증적 분석을 먼저 해야 한다.

## Ⅴ. 정보의 수집·이용 등에 대한 이용자 동의의 문제

개인정보의 수집과 이용 등과 관련하여 이용자들로부터 동의를 받는 방식이나 그 구체적인 과정에 대해서도, 현재 시행되고 있는 방식이나 과정이 애초에 상정한 정책목표를 달성하는 데에 유효한 방법인지 여부에 대해 이용자들의 실제 행태에 대한 엄밀한 분석에 기초하여 재평가할 필요가 있다. 특히 개인정보보호법 제22조는 포괄동의를 금지하고 있기 때문에, 실질적으로는 약관으로 통칭되어 분류될 수 있는 성질의 문서를 여럿으로 나누어, 수집·이용 동의, 제3자 제공 동의, 국외 제3자 제공 동의, 마케팅 목적 처리 동의 등 여러 개의 개별 동의사항으로 나누어 동의를 받도록 하고 있고, 실제 이용자들은 하나의 웹사이트에 회원으로 가입하는 과정에서 수차례에 거쳐 '동의합니다' 창에 동의를 표시해야 하는 것이 보통이다.

그런데 이처럼 동의가 필요한 사항들을 나누어 개별 사항들에 대해 개별적인 동의를 받도록 하는 것이 바람직한 방법인지 여부는, 제시되는 동의사항들에 대해 이용자들이 그 내용을 파악하고 난 뒤 동의의사를 밝히도록(소위 'informed consent') 유도하기 위해서는 어떤 방법을 사용하는 것이 효과적일 것인지 판단하는 것과 직결된다. 만일 몇 차례 개별 동의를 하도록 의무화하는 것이 이용자의 실질적 동의를 유도하는 데에 있어 실제로 기여하는 바가 없다면, 이는 사실 불필요한 규제일 수 밖에 없다. 특히, 모바일 기기를 이용하는 상황에서는 작은 화면을 조작하여 동의를 표시하는 것 하나 하나가 이용자에게 불편을 초래하는 것일 가능성이 높으므로 규제의 구체적인 내용에 대해 신중하게 생각할 필요가 있다.

그런데 외국에서 진행된 지금까지의 연구결과는, 이용자들이 약관을 거의 읽지 않을 뿐더러 이용자들에게 약관을 읽도록 유도하는 것이 쉽지 않다는 것을 확인하게 해주는 것이 대부분이다. 더 나아가, 약관을 읽도록 유도하기 위해서 약관을 더 눈에 뜨이도록 하거나 클릭을

7) L. Brandimarte, A. Acquisti & G. Lowenstein (2010), "Misplaced Confidences: Privacy and the Control Paradox".

여러 번 하지 않고도 쉽게 찾아볼 수 있게 하는 방법을 생각해 볼 수 있지만, 이러한 방법을 사용하는 것 또한 효과가 없다고 한다.[8] 그리고, 약관을 읽는 경우에조차, 그 내용 중 본인에게 불리한 내용이 포함되어 있음을 파악하더라도 그와 무관하게 결국 동의를 하게 되는 것이 보통이라고 한다.[9]

이와 같은 연구가 시사하는 것은, 약관을 고지하고 동의를 받는 기존의 방식에 근본적인 한계가 있을 수 있다는 것이다. 이용자들이 거의 읽지 않을뿐더러 읽더라도 실질적인 내용과 무관하게 결국 동의하는 경우가 대부분이라면, 기존의 방식은 사후적으로 문제가 발생할 가능성에 대한 책임의 대부분을 이용자들이 부담하도록 유도하는 결과만을 초래할 것이다. 즉, 사후적으로 문제가 발생하게 되면, 기업들은 이용자들의 동의를 근거로 책임이 없음을 주장할 수도 있을 것인데, 이는 동의를 강제하여 이용자를 보호하고자 하는 애초의 취지에 정면으로 반하는 결과가 될 것이다.

더 나아가, 몇 개의 문서로 나누어 개별 사안별로 동의를 받는 과정에서, 선택적 동의사항까지 이용자에게 함께 제시되어 이용자의 동의를 구하게 되는 상황을 생각해 보자. 이 때, 이용자 입장에서는 개별적 동의대상 항목이 필수적 동의사항인지 선택적 동의사항인지 여부에 대하여 파악하려는 노력을 기울이지 않고 모든 제시된 동의대상 항목에 일괄적으로 동의를 표시하는 경우가 적지 않을 것이다. 그러한 경우에는, 사안별로 동의를 나누어서 받도록 하는 제도로 인해 이용자의 선호가 정확하게 반영되지 못하고 오히려 이를 왜곡하는 결과가 초래될 것이다. 즉, 필수적 동의사항이 아닌, 웹사이트 운영자 입장에서 유용한 정보수집과 활용에 관한 내용을 수 개의 동의사항 중 하나로 제시하면, 이용자들은 그 내용을 구체적으로 검토하지 않은 채 동의를 표시할 가능성이 높을 것이다. 그렇다면, 이 과정에서 이용자 입장에서는 본래의 의도와 달리 정보를 과다 노출하게 될 것이고, 반대로 웹사이트 운영자 입장에서는 이용자들의 이러한 태도를 이용하여 손쉽게 원하는 정보를 수집하게 되는 결과가 초래될 것이다.

물론 이상의 논의는 외국에서의 연구결과에 상당히 의존하는 것이고, 국내 이용자를 대상으로 하는 규제에 대한 논의를 본격적으로 하기 위해서는 당연히 국내 이용자들의 행태에 대한 별도의 독립된 연구와 분석이 필요하다. 특히 국내 이용자들이 동의를 제공하는 과정이 어떠한지, 선택적 동의사항이 제시되는 방식에 따라 이용자들의 선택이 바뀌게 되는지 여부 및 그 정도 등에 대한 정확한 파악과 분석이 필요할 것이다.

# Ⅵ. 해외 개인정보의 국내이전

개인정보의 국가간 이전에 관한 규제를 논의할 때 흔히 국내에 있는 개인정보의 국외이전을 주로 전제로 하여 논의하는 경우가 많다.[10] 그런데, 국내기업이 유럽 등지에서 영업활동을 하면서 외국에 위치한 개인정보를 국내의 서버에 보내야 하는 등 정보의 국내이전이 필요한 경우도 충분히 있을 수 있고 앞으로 그러한 정보이전이 필요한 상황이 늘어날 상당한 개연성이 있다. 예를 들어, 스마트TV를 해외에서 유통·판매하는 경우나 국내에서 많은 이용자를 확보한 SNS나 소셜게임을 외국에서도 제공하기 시작하는 경우를 생각해 보면 해외정보의 국내이전의 필요에 대해 어렵지 않게 생각할 수 있다.

---

8) F. Marotta-Wurgler (2012), "Does Contract Disclosure Matter?", Journal of Institutional and Theoretical Economics, 168: 94.

9) 같은 글.

10) 국내소재 개인정보의 국외이전에 관해서는 박광배(2012), "개인정보 국외이전의 실무적 문제와 개선방향" (이 보고서에 포함된 글) 참조.

그런데 이와 같은 해외정보의 국내이전에 대해, 해외에서의 규제로 인해 국내이전이 어려운 경우 어떻게 문제를 해결해야 할 것인가? 시장의 규모나 성숙도 등을 고려할 때, 해외정보의 국내이전과 관련하여 특히 중대한 문제가 될 수 있는 경우는 유럽에 소재한 정보의 국내이전이 필요한 경우이다. EU의 경우에는,[11] 개인정보에 대한 국내의 규제가 EU가 요구하는 소위 '적절한 보호'(adequate protection)의 기준을 충족함을 보여야 하는 문제가 있다.[12] 이는 국내 규제기관에서 적극적으로 나서서 해결해야 할 문제이다. 특히 우리나라와 같이 무역의존도가 높은 나라는 국내기업이 해외에서 영업활동을 하는 데에 불이익이 발생하지 않도록 규제기관이 제도적인 여건을 마련하는 데에 적극적 역할을 할 필요가 있다.[13]

## Ⅶ. 맺는말

이상에서 논의한 내용을 정리하면 다음과 같다.

1. 개인정보보호와 관련된 규제는, 이에 관한 구체적인 논의에 앞서 이용자들의 행태에 대한 엄밀한 파악과 분석을 전제로 해야 한다. 그런데 이용자들의 실제 행태나 통계에 기초한 실증적이고 과학적인 분석은 국내에서는 개인정보보호법제에 대한 논의에 있어 지금까지 심각하게 고려되거나 활용된 적이 거의 없었던 것으로 보인다. 이러한 태도에 대한 근본적인 재검토가 필요하다.

2. 구체적으로는 국내 인터넷 환경에서의 쿠키 등 트래킹 기술의 이용현황 및 그에 대한 분석, 규제의 변화에 따른 영향평가 등을 체계적으로 수행한 뒤, 정책적 방향에 대해 반복적으로 재검토할 필요가 있다. 또한 인터넷 이용환경의 변화와 이용자 행태의 변화 등을 고려하여, 이러한 분석은 정기적으로 반복하여 수행되어야 한다.

3. 규제에 따라서는, 중립적인 형태의 규제일지라도, 그 영향은 구체적인 웹사이트의 유형이나 광고의 성격 등 규제 대상의 특징에 따라 매우 다르게 차별적으로 나타날 수 있다. 그러한 차별적인 영향은 기업의 이노베이션 활동에도 크게 영향을 미칠 수 있을뿐더러, 더 나아가 우리나라 인터넷 '생태계'의 장래를 결정짓는 데에 중대한 영향을 미칠 수도 있으므로, 정책결정에 앞서 그 영향에 대한 엄밀한 분석이 필요하다.

4. 인터넷 이용자의 행태에 대해서도 엄밀한 파악과 분석이 필요하다. 예를 들면, 프라이버시 패러독스나 콘트롤 패러독스와 같은 현상이 국내 인터넷 이용자들 사이에서도 발견되는지, 그 경우 그 크기나 양태는 어떠한지에 대한 분석이 필요하다. 그러한 분석이 없이 이루어지는 규제는 경우에 따라서는 규제의 목적달성 자체를 어렵게 하거나 역효과를 가져올 수도

---

11) 좀 더 정확하게는 EEA(European Economic Association)이다. 이는 27개의 EU 국가들 및 비 EU 국가인 노르웨이, 아이스랜드, 리히텐스타인을 포함한다.

12) European Commission (Directorate General for Justice)이 이에 관해 EEA 전체에 유효한 판단을 할 수 있고("Commission Adequacy Finding" 이라 한다), EEA내 개별국가의 규제기관이 해당국가에서 유효한 독자적인 판단을 할 수도 있다. http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm 참조. 국가차원에서 EC나 개별국가의 규제기관으로부터 adequate protection에 관해 인정을 받지 못하고 있는 경우에는, 개별 기업차원에서 접근하여 "Binding Corporate Rules", "Standard Contractual Clauses" 등의 방법을 통해 문제를 해결해야 한다. 개별 기업의 차원에서 유럽의 규제를 충족시키면서 문제를 해결하는 것은 매우 부담스러운 것이 될 것이다.

13) 더 나아가 개인정보보호와 관련된 규제의 국제적 조화(international harmonization)를 도모하면서 국제적 논의를 주도하는 것이 필요할 수도 있다. 장기적으로는 정보의 국외이전에 대한 규제가 실질적인 무역규제의 한 형태로 논의될 가능성도 있어서 그에 대한 적극적 준비가 필요하다. Haksoo Ko (2012 forthcoming), "Law and Technology of Data Privacy: A Case for International Harmonization", Journal of Asian Law and Economics 참조.

있다.

5. 정보의 수집, 이용 등과 관련하여 이용자의 동의를 획득하는 과정에 대한 규제에 있어서도 이용자의 실제 행태에 대한 엄밀한 분석이 필요하다. 이용자가 동의 여부를 결정함에 있어, 동의대상 내용에 대하여 이해를 하고 동의(informed consent)하도록 유도하는 데에 어떤 방법이 더욱 유효한지에 관해서는, 이용자들의 실제 행태에 대한 체계적인 분석을 전제하지 않고는 실효성 있는 결론을 얻을 수 없다.

6. 규제기관이 적극적으로 관여해야 할 영역중 하나는 국내기업이 해외에서 영업활동을 함에 있어 불이익을 받지 않도록 도움을 주는 것이다. 그런 맥락에서, 국내기업이 외국에서 기업활동을 하면서 수집하게 되는 개인정보를 국내로 이전하는 경우에 발생할 수 있는 법적 문제에 관하여 규제기관이 적극적인 관심을 가질 필요가 있다. 특히, 유럽에서는 유럽연합 집행위원회(European Commission)에 국내 규제가 적절한 수준의 개인정보에 대한 보호('adequate protection')를 제공함을 보여야 하는데, 이에 관해 국내의 규제기관이 중요한 역할을 할 필요가 있다.

# 현행 개인정보보호 법제상 '개인정보' 정의의 문제점

구태언(변호사, 테크앤로 법률사무소)

## Ⅰ. 정보의 집합체

사람은 정보의 집합체이다. 정보화 사회[1]를 살아가는 사람들은 원하던 원하지 않던 자신에 관한 정보를 생성하거나 부여받고 다른 존재와 교환하면서 정치·경제·사회·문화적 네트워크 속에서 살아간다. 사람은 '정보'로 기억되고 기록되며 평가된다. 사람이 태어나는 순간부터 그 사람에게 각종 정보가 부여되기 시작한다. 그 사람을 특정하거나 기억하거나 다른 사람과 구분하기 위함이다. 태어난 일시, 몸무게, 성별, 혈액형, 질병 유무부터 곧이어 이름, 주민등록번호, 신용정보 등 다양한 정보가 부여된다. 그런데 이러한 정보만 '개인에 관한 정보'가 아니다. 얼굴 어디에 점이 있는지, 눈 모양이 어떤지, 목소리는 어떤지, 안경을 꼈는지, 걸음거리가 어떤지 등도 개인에 관한 정보이다. 개인과 관련된 정보는 무궁무진할 뿐 아니라 죽을 때까지 새롭게 생성된다. 집단에서 유일한 여자라면 그 사람은 그 정보만으로 특정이 가능하게 될 것이고, 유일한 빨강 머리 친구가 있다면 구성원들은 시간이 흐른 후 그 사람의 이름은 기억을 하지 못하더라도 머리색으로 기억될 수 있는데, 그렇다면 성별이나 머리색도 개인에 관한 정보라 할 것이다. 앞서 말한 바와 같이 사람은 다른 사람과의 관계를 맺고 유지하기 위하여, 상대방이 제공하는 서비스를 이용하기 위하여 상대방과 계약을 맺기 위하여 의도적으로 자신에 관한 정보를 남기고 교환하며 살아간다. 수많은 정보 중 그 자체로 유의미한 정보도 있고, 그렇지 못한 정보도 있다. 어떤 정보는 그 사람을 특정할 수 있는 힘을 갖기도 하고 어떤 정보는 그렇지 못하기도 한다. 기술의 발달로 무의미한 정보로 보였던 것들을 모아 분석함으로서 유의미한 정보를 추출하기도 한다.

이러한 정보를 보호해야 한다는 것은 누구나 공감하는 것이지만, 어디까지 보호할 것이냐는 매우 어려운 문제이다. 개인정보는 홀로(solus) 의미가 있는 것이 아니라 외부의 어떤 존재와 관계를 맺을 때 비로소 의미가 있기 때문에 이해당사자도 많고 그들의 기본권과도 조화를 이루어야 하는데 그 접점을 찾는 것이 이론적으로나 입법기술적으로나 매우 어렵기 때문이다. 일례로, 영업은 영업재산을 토대로 지속적인 수익활동을 통해 이루어지며 그러한 과정에서 영업의 가치는 영업재산가치 뿐만 아니라 그 이상의 가치가 추가되며, 이러한 '그 이상의 가치'의 보존이 필요한데, 상법은 이러한 영업상 무형의 가치를 보존하기 위하여 영업 그 자체의 양도를 인정하고 있다.[2] 고객이 없으면 계속적 영업행위가 이루어 질 수 없기 때문에 전통적으로 고객은 영업재산의 중요한 요소로 간주되어 왔다. 영업재산을 이루는 고객관계의 기본은 고객정보이며 이는 당연히 개인정보이다.[3] 개인정보 보호에 지나치게 치우칠 경우 '영업의 자유'가 제한되는 이유가 바로 여기에 있다.

아래에서는 우리나라의 개인정보와 관련된 법률들이 개인정보를 어떻게 정의하고 있는지와

---

1) 정보사회란 "정보 그 자체의 중요성이 엄청나게 증대하고 이를 바탕으로 하여 정보의 생산, 유통 및 이용이 기존 사회를 새롭게 바꾸는 사회"이다. 김일환, 정보자기결정권의 헌법상 근거와 보호에 관한 연구, 공법연구 제29집 제3호, 2001, 87쪽, 개인정보보호법의 내용과 체계에 관한 분석_정혜영_한국비교공법학회, 공법학연구, 제12권 제4호 2011.11, 410면.

2) 김현경, 「상법상 영업양도의 '영업재산'으로서 '개인정보' 법리에 관한 재검토」, 법학논고, 경북대학교 법학연구원, 38권, 2012, 288면.

3) 김현경, 앞의 논문, 301면.

이에 관한 해석론을 통해 현행 법률의 문제점을 파악한 뒤 외국의 입법례를 통해 개정방향의 시사점을 도출한 다음, 앞서 본 문제점의 해결방안을 살펴보도록 한다.

# Ⅱ. 개인정보 관련 국내 법령 및 해석론

## 1. 개론

우리나라의 개인정보에 관한 법령은 종전에 공공부분과 민간부분으로 구분되어 그 법체계 및 집행체계를 달리하여 왔다. 공공부분에서는 「공공기관의 개인정보 보호에 관한 법률」이 그 역할을 수행한 반면, 민간부분에서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라고만 한다)이나 「신용정보의 이용 및 보호에 관한 법률」(이하 '신용정보법'이라고만 한다) 등이 소관 분야를 규율하였다. 그러나 2011. 3. 29. 「개인정보 보호법」이 제정되어 2011. 9. 30. 시행됨에 따라 위와 같은 체계는 근본적인 변화를 맞이하였다.

「개인정보 보호법」이 시행됨에 따라 이제는 공공부분과 민간부분을 구분하지 않고 개인정보 보호법이 일반법으로 적용되고, 다만 특별법 우선의 원칙에 따라 개별 분야에 있어 해당 법령이 적용될 뿐이다.[4)]

〈표1〉 개인정보 보호 관련 법령 개관[5)]

| 분야 | 적용 법률 |
|---|---|
| 일반 | 개인정보 보호법 |
| 정보통신 | 정보통신망 이용촉진 정보보호 등에 관한 법률 |
| 개별분야 | 신용정보의 이용 및 보호에 관한 법률, 위치정보의 보호 및 이용에 관한 법률, 통신비밀보호법, 주민등록법(제31조), 금융실명거래 및 비밀보장에 관한 법률(제4조), 형법(제316, 제317조), 보건의료기본법(제13조) 등 |

아래에서는 우선 위 법률 중 개인정보 보호에 관한 대표법률인 「개인정보 보호법」, 「정보통신망법」, 「위치정보법」에서 규정하고 있는 '개인(위치)정보'의 개념을 살펴본 뒤, 문제점과 그 대안에 관하여 살펴보고자 한다.

## 2. 현행 법률상 '개인정보'의 정의

현행 개인정보 보호법은 개인정보에 관하여 ①'살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보' 외에 ②'해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것'도 포함하는 태도를

4) 입법론적으로는 유럽과 같이 일반법을 제정한 이상 개별법령을 폐지하거나 정비를 하였어야 함에도 불구하고 우리나라는 개별법령을 폐지하지 않고 병존시킴으로써 중복규제, 법령간의 충돌 등 심각한 문제가 발생하고 있다. 더욱이 사업자들이 온/오프라인 사업을 병행하고 있고 관련 법령들이 '형사처벌' 규정을 두고 있어서 국민들의 예측가능성과 법적안정성에 큰 위해를 가하고 있다.

5) 개별 법령 중 일부는 '개인정보'라기 보다는 '비밀'을 보호하기 위한 것도 있다.

취하고 있고, 이러한 입법태도는 정보통신망법이나 위치정보법에서도 찾아볼 수 있다.[6]

'개인정보'의 구성요소로는 ① 살아 있는 개인, ② 특정 개인과의 관련성, ③ 정보의 임의성, ④ 식별 가능성을 제시하고 있다.[7] 특히 '특정 개인과의 관련성'과 관련하여서는 일반적으로 특정 개인의 정체성(identity)을 구별하거나 밝혀낼 수 있는 정보(성명, 주민등록번호, 생일, 주소, 바이오정보 등) 및 특정 개인의 과거 및 현재의 상황이나 상태를 나타낼 수 있는 정보(교육상황, 재정상황, 진료 및 건강기록 등)가 이에 해당되는데, 특정 개인을 알아볼 수 없도록 가공되었거나 통계적으로 변환된 경우에는 특정 개인과의 관련성을 인정할 수 없고 식별이 어려우므로 개인정보에 해당하지 않는다고 설명한다. 한편 '식별 가능성'에 관하여 한 가지 정보만으로는 특정인을 알 수 없는 경우가 많은데 '개인정보의 식별성'은 정보의 결합 또는 조합을 통하여 특정 개인을 구분·구별 할 수 있다면 모두 개인정보에 포함될 수 있다는 의미이고, 개인정보 보호법 제2조 제1호에서 말하는 "쉽게 결합하여"는 각각의 정보 결합 수단·방법이 합리적으로 이루어 질 수 있다는 의미라고 설명하고 있다.[8]

〈표2〉 개별 법률상 '개인정보' 정의 규정

| 법령 | 규정 |
|---|---|
| **개인정보법** | "개인정보" 란 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)를 말한다. |
| **정보통신망법** | "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다. |
| **위치정보법** | "개인위치정보"라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다. |
| **신용정보법** | "신용정보"란 금융거래 등 상거래에 있어서 거래 상대방의 신용을 판단할 때 필요한 다음 각 목의 정보로서 대통령령으로 정하는 정보를 말한다.<br>가. 특정 신용정보주체를 식별할 수 있는 정보<br>나. 신용정보주체의 거래내용을 판단할 수 있는 정보<br>다. 신용정보주체의 신용도를 판단할 수 있는 정보 |

6) 연혁적으로 살펴보면 우리나라는 1999. 7. 1. 「전산망보급확장과이용촉진에관한법률」을 '정보통신망법'으로 전문개정하면서 개인정보에 관한 포괄적 정의 조항을 도입한 이후 '위치정보법'과 '개인정보 보호법'에도 동일한 입법태도를 취해왔다.

7) 행정안전부, 「개인정보 보호법령 및 지침·고시 해설」, 2011. 12., 제2조 해설 부분 ; 이창범, 「개인정보 보호법」, 법문사, 2012, 14면 이하 참조.

8) 행정안전부, 앞의 해설서, 제2조 해설 부분 ; 이창범, 앞의 책, 19면.

| | |
|---|---|
| | 라. 신용정보주체의 신용거래능력을 판단할 수 있는 정보<br>마. 그 밖에 가목부터 라목까지와 유사한 정보<br>〈시행령〉<br>1. 법 제2조제1호가목의 특정 신용정보주체를 식별할 수 있는 정보: 생존하는 개인의 성명, 주소, 주민등록번호, 외국인등록번호, 국내거소신고번호, 여권번호, 성별, 국적 및 직업 등 (후략) (**제2호부터 제5호까지의 어느 하나에 해당하는 정보와 결합되는 경우만 해당한다**)<br>2. 법 제2조제1호나목의 신용정보주체의 거래내용을 판단할 수 있는 정보: 대출, 보증, 담보제공, 당좌거래(가계당좌거래를 포함한다), 신용카드, 할부금융, 시설대여와 금융거래 등 상거래와 관련하여 그 거래의 종류, 기간, 금액 및 한도 등에 관한 사항<br>3. 법 제2조제1호다목의 신용정보주체의 신용도를 판단할 수 있는 정보: 금융거래 등 상거래와 관련하여 발생한 연체, 부도, 대위변제, 대지급과 거짓, 속임수, 그 밖의 부정한 방법에 의한 신용질서 문란행위와 관련된 금액 및 발생·해소의 시기 등에 관한 사항. 이 경우 신용정보주체가 기업인 경우에는 다음 각 목의 어느 하나에 해당하는 자를 포함한다.<br>4. 법 제2조제1호라목의 신용정보주체의 신용거래능력을 판단할 수 있는 정보: 금융거래 등 상거래에서 신용거래능력을 판단할 수 있는 다음 각 목의 어느 하나에 해당하는 정보〈각 목 생략〉<br>5. 법 제2조제1호마목에 따른 정보로서 다음 각 목의 어느 하나에 해당하는 정보 〈각 목 생략〉 |

위 표를 살펴보면 유일하게 「신용정보법」만 신용정보를 정의함에 있어 매우 다양한 식별자를 이용하여 한계를 명확히 하고 있다는 점이다. 개인정보 보호법의 괄호와 같은 확장이 아닌, 시행령 제2조 제1항 제1호와 같이 괄호를 통해 제한을 하고 있음을 볼 수 있다.

## 3. 신용정보법을 제외한 주요 법률상 '개인정보'의 해석론

신용정보법을 제외한 개인정보 보호법, 정보통신망법, 위치정보법이 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보'만 개인정보로 한정하지 않고, '해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것' 역시 개인정보로 포함시킴으로 인하여 개인정보의 구체적 범위에 관하여 견해가 대립할 수 있다.

가능한 견해 중 첫 번째는, 문언에 충실한 입장으로서 해당 정보만으로는 특정 개인을 알아 볼 수 없는 단순한 정보이더라도, 다른 정보와 쉽게 결합하여 알아 볼 수 있다면, 즉 특정 개인을 식별할 수 있는 가능성을 가지고 있기만 하다면, 현재로서는 식별성이 없다 하더라도

개인정보로 보아야 한다는 견해이다.[9]

두 번째 견해는, 첫 번째 견해와 같이 해석할 경우 개인정보의 범위가 무한정 확장되어 예측가능성이 보장되지 않는다는 문제의식에서 출발한 견해로서, 그 자체로는 식별성을 갖지 않지만 다른 정보와 쉽게 결합하여 식별성을 갖게 된다는 가능성만으로는 부족하고, '실제로 다른 정보와 결합하여 식별성을 가진 경우'에 한하여 그 정보를 개인정보로 보아야 한다는 견해이다.[10]

세 번째 견해는, 현행 법률을 문언 그대로 해석할 경우 개인정보의 범위가 무한히 확장되어 예측가능성이 매우 낮은 반면 현행 법률이 형사처벌·과징금에 관한 규정을 두고 있어서 다른 이의 기본권(특히 영업의 자유 등)을 지나치게 제한한다는 점에 관한 문제의식에는 두 번째 견해와 같은 입장이나, 식별성 없는 정보가 다른 정보와 결합되어 식별성을 갖춘 경우에 한하여 그 정보를 개인정보로 보는 것은 -개정의 필요성은 별론으로-'해석론'의 한계를 넘어선 것이라고 보는 점에서 차이가 있는바, 이 견해는 정의 조항 중 괄호 부분을 삭제할 필요가 있고 '사람관련정보'라는 개념을 도입할 필요가 있다는 견해이다.

## 4. 포괄적 정의조항에 따른 문제점

우리나라 주요법령상의 개인정보 정의조항은 그 범위가 지나치게 넓어 영업의 자유를 지나치게 제한할 뿐 아니라 빅데이터나 클라우드와 같이 새로운 산업의 발전을 저해한다.

현행 법체계를 옹호하는 입장에서는 개인정보 보호와 관련하여 헌법재판소가 1995년에 인정한 '개인정보 자기결정권'을 근거로 제시하고 있으나 이러한 입장은 동 권리가 기본적으로 '국가'에 대한 소극적 방어권으로서의 성격과 적극적 청구권의 성격을 가지는 것이라는 점을 간과하고 있다. 물론 정보화사회에서는 사인들 역시 타인의 개인정보를 수집·이용하고 그로 인하여 다양한 개인적·사회적·국가적 문제가 발생할 수 있으므로 국가는 보호의무에 입각하여 사인에 의한 개인정보 자기결정권의 침해를 예방할 입법적·행정적 조치를 취할 의무를 부담한다는 점에 관하여는 이견이 없을 것이다. 다만 사인간의 개인정보 수집·이용을 제한하고 경우에 따라서는 형사처벌까지 하는 것을 내용으로 법률을 제정함에 있어서는 다른 기본권과 조화를 이룰 수 있도록 세심한 배려를 할 필요가 있는데, 현행 주요 법률에서의 개인정보 개념은 이러한 점을 고려하지 않은채 개인정보 보호에 지나치게 치우친 것이라고 판단된다. 대표적으로 '빅데이터 산업'은 소비자에 관한 정보를 얼마나 많이 모아서 분석하느냐에 그 신뢰도의 수준을 비롯하여 사업 자체의 성패가 달려 있다 할 것인데, 최근의 데이터 분석 기법에 따르면 그 자체로는 식별성이 없는 정보들도 쉽게 정보주체를 식별할 수 있으므로 기업으로서는 형사처벌의 위험성을 안고 빅데이터를 수집·이용하려 하지 않는다. 이것이 기업 자체는 물론이고 빅데이터 분석을 통해 제공될 각종 서비스를 이용하지 못하는 고객에게도 불이익임은 다언을 요하지 않는다. 이러한 문제는 관련 서비스를 위하여 정보를 수집함에 있어서 '익명화'를 통해 해결할 문제이지, '개인정보'의 개념을 무한히 확대하여 해결할 문제가 아니다.

더 큰 문제는 현행 개인정보 보호에 관한 법령이 세계적으로 유래 없는 강력한 형사처벌 조항을 두고 있다는 점인데, 개인정보에 관한 포괄적 정의 조항과 맞물리면서 많은 위헌성을 띄게 된다. 구성요건이라 할 수 있는 '개인정보'의 개념 자체가 명확하지 않기 때문에 어느 정

9) 행정안전부와 방송통신위원회의 입장이기도 하다.
10) 방송통신위원회(정상조), 「비식별개인정보의 보호 및 활용에 관한 연구」, 2010. 8, 48~49면.

보를 수집하고 제공 등의 행위를 했을 때 형사처벌의 대상이 되는지 명확하지 않다. '다른 정보와 쉽게 결합'한다는 것이 무엇을 의미하는지, 판단하는 시점은 언제인지, 판단의 주체는 누구인지를 예측할 수 없다. 또한 법정형이 지나치게 높다. 형법이 비밀침해죄나 업무상비밀누설죄에 관하여 3년 이하의 징역에 처할 수 있다고 규정하고 있는데 반하여, 개인정보 보호법은 개인정보의 제3자 제공 규정 위반의 경우 5년 이하의 징역에 처할 수 있도록 규정하고 있다.[11] 비교법적으로 보더라도 일본의 개인정보 보호법은 시정명령이라는 완충장치를 마련하고, 시정명령에 위반할 경우에 6개월 이하의 징역 또는 50만 엔 이하의 벌금에, 보고를 하지 않거나 허위보고를 할 경우에 30만 엔 이하의 벌금에 각 처한다고 규정하고 있을 뿐이다(우리나라는 개별 의무 위반에 대한 직접적 형사처벌 규정과 시정명령 위반에 따른 형사처벌 규정을 병존적으로 마련하고 있다).[12]

## 5. 소결론

이상에서 본 바와 같이 현행 법률상 개인정보에 관한 정의 조항은 괄호부분으로 인하여 범위가 지나치게 넓어 개인정보의 범위가 무한히 확장되어 예측가능성이 매우 낮다는 문제가 있고, 이러한 포괄적 정의조항이 형사처벌 조항과 맞물려 심각한 문제를 야기하고 있다. 그러나 입법론은 별론으로, 현행법의 '해석'상 괄호 부분을 제2설과 같이 제한하여 해석하는 것도 무리다. 제2설을 지지하는 입장은 '결합하여' 특정한 개인을 '알아볼 수 있는 경우'라는 표현은 비식별정보가 실제로 다른 정보와 결합하여 특정 개인에 대한 식별성을 획득한 경우를 의미한다고 주장하나,[13] 문언의 해석상 비식별정보가 개인식별정보 또는 다른 비식별정보와 결합된 경우를 의미한다기 보다는 결합에 의한 식별가능성을 염두해 둔 것이라고 봄이 타당하다.[14]

따라서 현행 법률상 개인정보 정의에 관한 문제는 법개정을 통해 해결해야 하는 문제라고 보는 제3설이 타당한바, 아래에서는 외국 입법례를 간략히 살펴본 뒤 개선방안을 알아보도록 한다.

---

11) 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처할 수 있다.

12) 第六章　罰則
第五十六條　第三十四條第二項又は第三項の規定による命令に違反した者は、六月以下の懲役又は三十万円以下の罰金に處する。
第五十七條　第三十二條又は第四十六條の規定による報告をせず、又は虚僞の報告をした者は、三十万円以下の罰金に處する。
第五十八條　法人（法人でない団体で代表者又は管理人の定めのあるものを含む。以下この項において同じ。）の代表者又は法人若しくは人の代理人、使用人その他の從業者が、その法人又は人の業務に關して、前二條の違反行爲をしたときは、行爲者を罰するほか、その法人又は人に對しても、各本條の罰金刑を科する。
2 法人でない団体について前項の規定の適用がある場合には、その代表者又は管理人が、その訴訟行爲につき法人でない団体を代表するほか、法人を被告人又は被疑者とする場合の刑事訴訟に關する法律の規定を準用する。
第五十九條　次の各号のいずれかに該当する者は、十万円以下の過料に處する。
一　第四十條第一項の規定による届出をせず、又は虚僞の届出をした者
二　第四十五條の規定に違反した者

13) 방송통신위원회(정상조), 「비식별개인정보의 보호 및 활용에 관한 연구」, 2010. 8, 39면.

14) 수사기관은 지속적으로 결합가능성만으로 수사 및 기소를 하려고 하고 있고, 실제로 하급심 판결이기는 하나 IMEI 정보가 다른 정보와 결합할 경우 개인을 식별할 수 있다는 이유로 유죄판결을 한 경우도 있다.
만약 제2설과 같은 취지라면, 괄호부분은 "해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 (쉽게) 결합되어 알아볼 수 있게 된 것을 포함한다"라고 규정되었을 것이다.

# Ⅲ. '개인정보' 정의와 관련된 외국 입법례

## 1. 서론

EU나 OECD의 경우 오래전부터 개인정보 보호에 관한 일반적 지침을 마련해왔고, 미국 역시 「The Privacy Act of 1974」를 비롯하여 각종 개인정보에 관한 개별법을 제정·운영하여 왔으며 영국, 독일, 호주, 일본 등 개별 국가들도 관련 법률을 제정하여 시행하고 있다.[15] 여기서는 외국 입법례를 간략히 살펴봄으로써 현행 법률의 개인정보 정의 규정의 적정성을 비롯하여 개정 방향에 관한 시사점을 도출하고자 한다.

간략히 살펴보면 미국, 유럽의 개인정보보호 법제에서는 개인정보(personal information) 외에 추가적으로 '개인기록'과 '고유식별자'의 개념을 사용하고 있는데, 개인기록은 이름, 주민등록번호, 주소, 전화번호 등 개인에 관한 여러 가지 정보들을 묶은 것이고, 고유식별자는 이름, 주민등록번호, 사회보장번호 등 특정 개인의 신원을 식별할 수 있게 하는 식별자를 말한다.[16] 미국, 유럽의 개인정보관련 법제는 이와 같이 개인정보에 관한 개념을 세분화하여 사용함으로써 수범자의 예측가능성을 높이고 있다.

## 2. 유럽연합

유럽연합 회원국들의 개인정보 보호에 관한 연구와 입법에 관한 노력은 60년대에서 70년대 초까지 거슬러 올라가는데, 유럽연합 차원에서 개인정보 보호정책에 관한 공식적인 입장을 취한 것은 1981. 1. 28. 유럽연합 이사회가 채택한 '개인정보의 자동처리로부터 개인보호에 관한 협약'이라고 할 수 있다.[17] 그러나 동 협약은 협약에 서명한 가맹국에 대해서만 효력이 미치는 관계로 유럽연합은 개인의 권리와 자유 그리고 프라이버시 보호의 원칙을 확산시키기 위하여 노력하였고 그 결과 유럽의회와 이사회는 1995. 10. 24. '개인정보의 처리 및 자유로운 이전으로부터 개인보호를 위한 지침'(이하 '개인정보보호지침'이라 한다)을 제정하였다.[18]

개인정보보호지침은 "Personal data"라 함은 신원이 확인된(identified) 또는 신원 확인이 가능한(identifiable) 자연인(정보주체, data subject)에 관한 일체의 정보를 말하며, 신원확인이 가능한 개인(identifiable person)이란 직접 또는 간접적으로, 신원확인번호(an identification number)나 그의 신체적, 생리적, 정신적, 경제적, 문화적 또는 사회적 동일성을 고유하게 나타내는 하나 또는 그 이상의 요소를 참조하여 그 신원이 확인될 수 있는 사람이라고 정의하고 있다.[19]

---

15) 미국, 영구, 호주, 뉴질랜드 등의 경우 법령명이 'Privacy Act'이나 내용은 개인식별정보에 기반한 개인정보 보호에 있는 반면, 우리나라는 개인정보 보호법의 목적 조항에 사생활 비밀의 보호를 포함시키고 개인정보의 범위를 극단적으로 확장함으로서 사실상 사생활(또는 비밀)보호법과 같이 운영되고 있다는 점 역시 향후 정비가 필요한 부분이다.

16) 방송통신위원회(정상조), 「비식별개인정보의 보호 및 활용에 관한 연구」, 2010. 8, 46면.

17) 정식 명칭은 "Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data".

18) 정식명칭은 "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"

19) ′personal data′ shall mean any information relating to an identified or identifiable natural person (′data subject′); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
2012년 1월에 발표된 「General Data Protection Regulation」은 다음과 같이 규정하고 있다. : ′data subject′ means an identified natural person or a natural person who can be

## 3. 미국

미국의 공공부분에 관한 개인정보 보호에 관하여는 연방정부기관이 보유하고 있는 개인정보에 관한 「The Privacy Act of 1974」를 비롯하여 각 주 단위로 제정된 법률과 특정 영역에 적용되는 법률들이 제정되어 시행되고 있다.[20] 그러나 민간부분에 관하여는 개인정보 보호에 관한 일반법을 마련하지 않고 시장의 자율규제에 입각하여 소비자의 권리를 보호하는 것에 초점을 맞추고 있다.

「프라이버시법」에 따르면, 개인 기록(record)이란 "행정기관이 보유하는 개인에 관한 정보의 개개 항목 또는 그 집합을 말한다. 그 기록에는 당해 개인의 교육(education), 금전적 거래(financial transactions), 병력(medical history), 전과(criminal history), 취업경력(employment history)에 관한 정보가 담기지만 이에 한정되지 않는다. 그리고 그 기록에는 당해 개인의 이름 또는 식별번호나 식별부호 혹은 지문(finger print), 성문(voice print), 사진(photograph)과 같은 당해 개인에게 고유한 식별자(identifying particular)가 포함되어 있어야 한다"라고 규정하고 있다.[21]

미국의 프라이버시법은 규율대상인 "개인기록(record)" 안에 적어도 신원을 확인할 수 있는 식별자가 포함되어 있어야 하고, 그 식별자로 기능할 수 있는 것으로서 이름, 공적으로 부여한 식별번호나 식별부호, 기타 지문, 성문, 사진과 같은 생체식별정보를 명시하고 있다.[22]

## 4. 영국

영국의 개인정보 보호법(Data Protection Act of 1998)은 개인기록에 관하여 신원확인이 가능한 생존하는 개인에 관한 기록으로서 그 기록으로부터 또는 data controller(우리나라 개인정보 보호법상 '개인정보처리자')가 보유하고 있거나 또는 앞으로 보유하게 될 다른 정보로부터 신원확인이 가능한 것을 말하며, 이에는 당해 개인에 관한 의견표명 및 당해 개인과 관련해서 controller나 그 밖의 다른 사람이 드러낸 일체의 의견이 모두 포함된다고 규정하고 있다.[23]

---

identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifiers or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. 현재 EU의 개인정보 보호 관련 법규는 `지침(Directive)′으로 돼 있으나 집행위는 이번 개정안을 `규정(Regulation)′으로 내놓았다. 발효 목표 시기는 2014년이다.

20) 자세한 내용은 전은정, 김학범, 염흥열, 「미국의 개인정보보호 법·제도 동향」, 정보보호학회지, 제22권 제1호, 2012. 2., 48면. ; 이호용, 「각국의 개인정보호법제 동향」, 인터넷법률, 제8호, 153면 참조.

21) 5 U.S.C. §522a (a) (4) - the term ″record″ means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph ; 방송통신위원회(정상조), 앞의 연구보고서, 46면.

22) 방송통신위원회(정상조), 앞의 연구보고서, 46면.

23) data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller

## 5. 일본

일본 정부는 공공부문의 개인정보보호를 위해 1988년 12월「행정기관이 보유하는 전자계산기처리에 관한 개인정보의 보호에 관한 법률」을 제정·공포하였으나, 민간 부문과 관련하여서는 1990년대 후반 들어 인터넷의 보급과 이용증대로 인한 개인정보침해가 증가하면서 민간 부문 자율규제의 한계가 드러나자 2003년 5월 30일 'EU 개인정보보호지침'과 'OECD 프라이버시 가이드라인'을 참고하여 작성된「개인정보의 보호에 관한 법률(個人情報の保護うに關する法律)」(이하 개인정보보호법)을 제정·공포하였고, 2005년 4월 1일부터 전면 시행하게 되었다. 일본의 개인정보보호법은 개인식별정보 외에 다른 정보와 용이하게 조합 할 수 있어 그것에 의해 특정 개인을 식별 할 수 있게 되는 것을 포함한다고 규정하여 우리나라와 거의 동일한 것을 볼 수 있다.[24]

〈표〉 국제기구 및 국가별 개인정보 정의[25]

| 법률 | 내용 |
|---|---|
| OECD 가이드라인 제1조 | 식별된 또는 식별가능한 개인에 관한 정보. any information relating to an identified or identifiable individual (“data subject“) |
| EU 지침 제2조 | 정보주체의 신원이 확인되었거나 확인 가능한 정보. any information relating to an identified or identifiable natural person (“data subject“); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;“ (art. 2 a) |
| 캐나다 프라이버시법 제3조 | 신원을 확인할 수 있는 개인에 대한 정보 |
| 일본 개인정보보호에 관한 법률 제2조 | 생존하고 있는 개인에 관한 정보로서 당해 정보에 포함된 성명, 생년월일 기타 설명된 것에 의해 특정한 개인을 식별할 수 있는 것(다른 정보와 용이하게 조회할 수 있으며, 그렇게 함으로써 특정한 개인을 식별할 수 있게 되는 것을 포함한다) - 우리나라와 가장 유사함 |
| 호주 프라이버시 법 제6조 | 진실이든 아니든 물리적 형태에 기록되어 있든 아니든 간에 그의 신원이 명백하거나 합리적으로 판명될 수 있는 개인에 관한 정보 또는 의견 |
| 영국 개인정보보호법 제1조 | 신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터 또는 정보 관리자가 보유하고 있거나 앞으로 그러할 가능성이 높은 기타 정보 또는 데이터로부터 신원이 확인가능한 생존 |

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

| | |
|---|---|
| | 개인과 관련된 데이터 |
| 독일 연방개인정보 보호법 제3조 | 신원이 확인되었거나 확인 가능한 정보주체의 인적·물적 환경에 관한 일체의 정보 |

# Ⅳ. 개인식별정보와 사람관련정보의 구별 필요성

## 1. 개론

개인정보를 현행 개인정보 보호법이나 정보통신망법과 같이 포괄적으로 규정함으로써 생기는 문제점은 앞서 본 바와 같다. 그 자체로 예측가능성이 없어서 개인정보의 범위를 무한대로 확장시킬 뿐 아니라 높은 형량의 형사처벌규정과 결합하여 개인정보처리자와 정보통신서비스 제공자의 영업의 자유와 같은 기본권을 극도로 제약하고 있다. 즉, 개인식별정보와 식별성은 없으나 다른 정보와 결합될 경우 식별성을 가지는 정보를 모두 개인정보로 정의하는 것은 '모든 사람 관련 정보는 개인정보다'라는 결론으로 귀결되는바, 이는 기업의 정보처리 등에 심각한 법적 위험을 야기한다. 비식별정보는 아직 식별성을 가지지 않으므로 선행적 법적 규제의 정당성도 미흡하다. 앞서 본 외국 입법례를 보더라도 '개인을 식별하거나 식별 할 수 있는 정보(Personally Identified or Identifiable Information, PII)'를 개인정보〔협의의 개인(식별)정보〕라 정의하고 있는데 이는 우리나라 주요 법령상 개인정보 정의의 '본문'과 일치한다. 이러한 문제를 해결하는 방법은 현행 개인정보 보호법과 정보통신망법상 개인정보의 정의조항에서 괄호 부분을 삭제하고 사람관련정보[26]와 같은 개념을 도입하는 것이다.

## 2. 개인정보의 명확화

현행 개인정보 보호법, 정보통신망법, 위치정보법은 모두 개인정보에 관한 정의조항에서 괄호 부분을 두어 그 범위를 무한히 확장하고 있다. 개인정보의 충실한 보호를 통해 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하려는 입법취지에는 부합할지 몰라도 앞서 본 많은 문제점을 야기시키고 있다. 법 전체를 관통하는 중요 개념인 '개인정보'를 불명확하게 정의함으로써 개인정보의 수집·이용·제공 모든 영역에 있어서 예측가능성을 현저히 저해하고 있다.

이러한 문제를 해결하기 위한 방법으로 현행 정의조항 중 괄호 부분을 삭제하여 '개인식별정보'만 개인정보로 규율함으로서 예측가능성과 법적안정성을 확보함과 동시에 개인식별정보를 제외한 나머지 정보를 '사람관련정보'로 규율하는 방법을 검토할 필요가 있다. 즉, 개인식별자를 가지고 있는 '개인식별정보'를 제외한 '사람관련정보'의 수집에 관하여는 원칙적으로 규제하지 않음으로서 개인정보처리자나 정보통신서비스 제공자에게 보다 많은 자율을 부여하되, 사람관련정보는 개인식별정보와 함께 수집되고 이용될 때 비로소 의미를 가지는 것이므로 이 경우에 한하여 개인정보로서 규율하면 족하다.

본고의 첫 머리에 영업양도에 관한 예를 검토한바 있는데, 개인정보의 제3자 제공과 관련하여 현행 법률에 따르면 사실상 기업이 보유하고 있는 모든 정보가 개인정보가 된다. 그렇다면 개인정보처리자가 영업의 일부를 양도하거나 그 전제로 협의를 함에 있어서 고객관련 통계

25) 한국정보보호진흥원, 주요 국가의 개인정보보호 동향 조사, 2009.

26) 관련 법령상 '개인'이라는 말은 특정인을 의미하는 바, 용어에서 '개인'이라는 말을 쓰는 이상 특정인을 지칭하게 되어 부적절하다. 여기서 '사람'이란 특정인을 지칭하지 않는 일반적 의미의 자연인을 뜻하는 의미로 사용한다. 법인이나 사물에 대칭되는 의미이기도 하다.

를 제공하는 경우에 그 정보들이 분석기술의 발달로 어렵지 않게 식별성을 가질 수 있다는 가능성만으로 관련 당사자에게 서면으로 알리거나 홈페이지에 게재하여야 하는데, 이것은 개인정보 자기결정권과 영업의 자유의 조화로운 해결방법이라고 보기 어렵다. 영업양도인이 보유하고 있는 사람관련정보는 그 자체로 영업의 무형적 자산이므로 자유롭게 양도하도록 허용하되, 개인식별정보와 함께 제공하거나 다른 정보와 결합하여 식별성을 가진 경우에 한하여 규율하면 족하다 할 것이다.

〈개정안〉 "개인정보"란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 또는 그러한 정보와 결합된 사람관련정보를 말한다.

## 3. 개인정보가 아닌 민감정보의 처리

현행 개인정보 보호법은 민감정보에 관하여 제23조에서 별도로 규정하고 있다. 근본적으로 개인정보의 보호에 관한 법률에서 사생활 또는 비밀에 해당하는 정보까지 규율하는 것이 타당한 것인지에 관한 의문이 있을 뿐 아니라,[27] 민감정보 역시 '개인정보'로 규정하고 있는데, 정의조항에서 개인정보의 범위를 무한히 확대함으로서 사실상 민감정보의 수집·이용을 저해하고 있다. 이에 관하여 통계처리 등을 통하여 익명처리를 할 경우에는 개인식별성을 띄지 않으므로 개인정보가 아니므로 문제가 없다는 견해도 있으나, 이 견해는 이미 수집 및 익명·통계처리를 거친 후에 관한 것일 뿐 수집단계의 개인정보처리자에 대하여는 아무런 해결책을 제시하지 못하고 있다.

사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보는 그 자체로 개인정보가 아니라 그 사람에 관한 정보라고 봄이 타당하다. 따라서 개인식별정보와 결합하여 수집하지 않는 이상 이에 관한 자유로운 처리를 허용하고, 다른 개인식별자와 함께 수집할 때나 개인식별자와 함께 제3자에게 제공하는 경우에 정보주체의 동의를 얻도록 할 필요가 있다.

〈'민감정보'처리 금지 규정 개정안〉

개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 개인정보(괄호 부분이 삭제된 것을 의미)와 함께 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

## 4. 소결론

개인식별정보만 개인정보로 정의하더라도 개인정보 보호 법제가 추구하는 목적을 달성할 수 있으며, 만약 개인정보처리자 또는 정보통신서비스 제공자가 사람관련정보에 개인식별정보를 결합하거나 다른 정보를 결합하여 개인식별정보를 만들어 내면 그 자체로 '개인정보'를 처리하는 것이 되므로 개인정보 보호법이나 정보통신망법의 규율을 받게 될 것이기 때문이다.

27) 개인정보보호법의 내용과 체계에 관한 분석_정혜영_한국비교공법학회, 공법학연구, 제12권 제4호 2011.11, 415면 이하.

# Ⅴ. 결론

개인정보보호에 관한 기본법인 「개인정보 보호법」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)고 규정하고 있고, 온라인상 개인정보보호에 관한 특별법인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상 개인정보의 정의도 대동 소이하다.

사람관련정보는 개인식별정보가 제거되면 '개인정보성'을 상실하므로 별도로 동의의 대상으로 삼을 필요가 없음에도, 주요 법령상 사람관련정보의 수집이용도 그 대상으로 전제하고 규정하고 있고, 특히 우리나라 주요법령상 개인정보의 정의는 다른 주요나라의 개인정보의 정의에 비추어 지나치게 넓어 기업의 영업을 극도로 위축시키고 형벌을 지나치게 확장시키고 있다.

다른 주요 국가의 개인정보의 개념을 보더라도, '개인을 식별하거나 식별 할 수 있는 정보(PII, Personal Identified or identifiable Information)'를 개인정보라 정의하고 있는데 이는 우리나라 주요 법령상 개인정보 정의의 '본문'에 해당하는 것이다. 그러나 우리나라는 괄호부분을 통해 개인정보의 범위 및 가벌성의 범위를 무한히 확장하고 있다.

이러한 문제를 해결하기 위해서는 개인정보 정의 조항 중 괄호부분을 삭제할 필요가 있고, 개인식별정보와 사람관련정보를 구별하여 개인식별정보를 제외한 사람관련정보의 수집에 있어서 원칙적으로 규제하지 않되 민감한 사람관련 정보 등 일정한 사람관련정보는 예외적으로 규율하는 체제로 정비할 필요가 있다. 이렇게 하더라도 협의의 개인(식별)정보만 개인정보로 정의해도 법적 보호목적을 달성하기에 충분하고, 개인정보처리자나 정보통신서비스 제공자에게 보다 많은 자율을 부여할 수 있을 뿐 아니라 빅데이터 또는 클라우드와 같은 신산업의 발전을 도모할 수 있을 것이다.

정보화 사회를 살아가는 구성원으로서의 사람에 관한 정보의 흐름은 사회·문화적으로 타당한 것일 뿐 아니라 경제적으로도 필수불가결한 것이다. 개인정보 보호의 당위성은 누구나 인정하는 것이지만, 역효과를 우려하여 개인정보의 이용 및 활용을 지나치게 막거나 규제할 경우 새로운 서비스의 등장은 물론이고 새로운 산업의 탄생과 발전이 저해되어 결국 사회의 역동성이 저해받게 될 것이다. 조화로운 해결책을 모색해야 할 시점이다.

# 개인정보처리(수집·이용·제공)의 법적 기준에 대한 타당성 분석

중앙대학교 법학전문대학원 교수 이인호

## Ⅰ. 정보주체의 동의를 절대화하는 정보통신망법의 문제

최근 우리 사회에서 개인정보보호를 절대화하려는 경향은 개인정보자기결정권에 대한 오해를 낳았고, 공공부문과 민간부문을 포괄하여 규율하는 일반법인 「개인정보보호법」(2011. 9. 30. 시행)에서 구체화되었다. 그러나 이미 개인정보보호의 절대화경향은 2001년에 전문개정된 온라인 개인정보보호법인 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2001. 1. 16. 법률 제6360호. 이하 '정보통신망법')에서부터 시작되었다. 이 절대화경향에 의하면, 정보주체의 동의 없는 개인정보의 수집·이용·제공은 원칙적으로 불법으로 취급된다. 그러나 이는 개인정보자기결정권을 잘못 이해한 결과이다. 자칫 이러한 절대화경향은 우리 사회에서 필요로 하는 개인정보의 이용과 유통의 사회적 가치를 부정하고 모든 개인정보를 비밀정보로 취급하는 우를 범할 수 있다.

우리나라에서 정보주체의 동의를 개인정보처리(=수집·이용·제공)의 기본적인 요건으로 인식하게 된 것은 온라인 개인정보보호법인 정보통신망법에서 유래한다.

정보통신망법은 정보통신서비스제공자가 이용자의 개인정보를 수집하는 경우 ① 개인정보의 수집·이용목적 ② 수집하는 개인정보의 항목 ③ 개인정보의 보유·이용기간을 사전에 고지하고 정보주체의 동의를 받아야 한다고 규정하고 있다(제22조 제1항). 그리고 이를 위반한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하고 있다(제71조 제1호). 이용자의 동의 없는 개인정보의 수집 자체를 불법화하고 그것도 무거운 법정형의 형사처벌로 규율하고 있는 것이다. 물론 이에는 아주 제한적인 예외가 있다. 즉, ① 정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우 ② 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 ③ 이 법 또는 다른 법률에 특별한 규정이 있는 경우가 그것이다(제22조 제2항).

또한 정보통신망법은 정보통신서비스제공자가 이용자의 개인정보를 제3자에게 제공하려면 ① 개인정보를 제공받는 자 ② 개인정보를 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간을 사전에 고지하고 이용자의 동의를 받아야 한다고 규정하고 있다(제24조의2 제1항). 이를 위반한 경우에는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하여진다(제71조 제3호). 다만, ① 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우 ② 이 법 또는 다른 법률에 특별한 규정이 있는 경우에는 예외로 하고 있다. 이처럼 정보통신망법은 동의 요건을 온라인상에서의 모든 개인정보처리(=수집·이용·제공)가 합법적이기 위한 절대적인 기준으로 설정하고 그 위반에 대해 5년 이하의 징역에 처하고 있다.

그런데 정보통신망법이 이렇게 동의 요건을 절대적인 합법성 기준으로 설정한 것은 회원가입시 이용자가 직접 제공해주는 정보(이름, 주민등록번호, 전화번호, 이메일주소, 우편주소, 직업, 직장명, 학력, 결혼여부 등)를 수집하는 경우만을 상정한 때문인 것으로 보인다.

그러나 인터넷 이용과정에서는 실로 무수히 많은 개인정보가 자동으로 수집된다. 인터넷쇼핑몰의 경우 회원이 구매한 물건, 가격, 일시, 결제방법, 그리고 이를 분석하여 2차적으로 생성되는 회원의 소비성향과 구매패턴, 설령 구매하지 않았더라도 열어 본 웹페이지 등 실로 다양한 개인정보가 수집될 수 있다. 게임사이트에서는 회원의 게임머니, 즐기는 게임의 종류, 게임 중의 대화 등 모든 것이 기록된다. 포털사이트에는 실로 엄청난 개인정보가 매일 매일 기록되고 저장된다. 그렇다면 이러한 이용자의 동의 없는 수집을 전부 금지시켜야 하는가? 현행 우리의 정보통신망법에 의하면 모두 5년 이하의 징역에 해당하는 범죄행위이다.

우리의 현행 정보통신망법은 회원가입시 이용자가 제공하는 개인정보의 수집만을 상정해 놓고 그러한 수집에 대해서 이용자의 사전 동의를 받도록 규정해 놓은 것이다. 그러나 이는 인터넷에서의 개인정보의 처리에 대한 현실을 전혀 고려하지 않은 입법이 아닐 수 없다.

정보통신망에서의 일체의 개인정보의 수집에 대해 절대적인 동의 요건을 설정해 놓은 것은 아마도 세계 유례가 없는 것으로 보인다. 개인정보를 강하게 보호한다고 평가받는 유럽의 경우도 정보통신망에서의 모든 개인정보의 수집 · 이용 · 제공에 대해 동의 요건을 절대적인 합법성 기준으로 설정하고 있지 않다.

유럽연합의 온라인프라이버시보호지침이 특별히 규율하는 주요 내용은 통신비밀의 보장(제5조), 통신사실확인자료(traffic data)에 대한 보호(제6조), 위치정보에 대한 보호(제9조), 스팸메일에 대한 opt-in 방식의 채택(제13조) 등이다. 이에 의하면, 통신의 전송 목적을 위해 처리되는 통신사실확인자료(traffic data)는 정보주체의 동의를 얻어 정보통신서비스의 마케팅 목적으로 이용할 수 있도록 허용하고 있다. 그리고 위치정보는 익명 또는 정보주체의 동의에 의해서만 처리가 가능하도록 하고, 동의를 얻기 전에 사전고지(처리대상 위치정보의 종류, 처리의 목적 및 기간, 부가가치서비스의 제공목적에서 당해 위치정보를 제3자에게 제공하는지 여부)의 의무를 지우며, 정보주체는 언제든지 동의철회를 가능하게 하고 있다. 이처럼 유럽연합의 온라인프라이버시보호지침은 통신사실확인자료를 마케팅 목적으로 이용하는 경우와 위치정보의 처리에 대해서만 정보주체의 동의를 요건으로 하고 있을 뿐이다.

요컨대, 우리의 정보통신망법은 이용자의 사전 동의 없이는 일체의 개인정보를 수집 · 이용 · 제공하는 것을 금지시키고 있다. 이는 지나치게 동의 요건을 절대화하고 있는 것이다. 통신사실확인자료나 위치정보의 처리(=수집 · 이용 · 제공)의 경우에나 요구될 수 있는 동의 요건을 모든 개인정보의 처리에 요구하고 있는 것이다.

동의 없는 개인정보의 처리를 5년 이하의 징역에 처할 만큼 정보통신서비스제공자가 수집 · 이용 · 제공하는 모든 개인정보가 그 개인의 사생활비밀에 해당하는 것인가? 형법상의 비밀침해죄는 '비밀장치에 의해 보존되어 있는 정보'를 그 비밀장치를 깨고 열어 보는 행위를 3년 이하의 징역에 처하고 있다. 그런데 정보통신망법은 정보통신서비스를 제공하고 이용하는 관계에서 정보통신서비스제공자가 이용자의 사소한 개인정보라도 그 이용자의 동의 없이 수집했다면 그 행위를 5년 이하의 징역에 처하고 있다. 또 형법상의 업무상비밀누설죄는 의사 · 변호사 등의 전문가가 의뢰인과의 신뢰관계 속에서 주고받은 의뢰인의 비밀을 제3자에게 누설하는 행위를 3년 이하의 징역에 처하고 있다. 그런데 정보통신망법은 서비스제공이라는 상업적 이용관계에서 생성된 어떤 사소한 개인정보라도 그 이용자의 동의 없이 제3자에게 제공했다면 그 행위를 5년 이하의 징역에 처하고 있다. 과연 이렇게까지 온라인상의 이용관계에서 처리되는 개인정보를 보호해야 할 필요가 있는 것인가?

문제의 발단은 온라인의 서비스이용관계에서 수집 · 이용 · 제공되는 개인정보를 모두 "비밀"

로 잘못 이해하고 있는 데서부터 시작한다. 그리하여 현행 정보통신망법의 개인정보보호규정은 '개인정보보호법'이 아니라 '비밀보호법'으로 기능하고 있다. 개인정보의 이용과 보호의 균형을 현저히 상실한 법이라고 하지 않을 수 없다.

더 나아가, 문제는 정보통신망법에 그치지 않고 있다. 정보통신망법의 비밀보호법으로서의 성격과 내용이 일반법인 「개인정보보호법」에 거의 그대로 반영되어 있다는 점이다. 온라인을 규율하는 특별법도 아닌 일반법에서 정보주체의 동의 요건을 개인정보처리의 원칙적인 합법성 기준으로 설정하고 있는 것이다.

# Ⅱ. 「개인정보보호법」의 수집·이용·제공의 허용기준에 대한 평가

## 1. 종합적 평가

2011. 9. 30.부터 시행되고 있는 일반법인 「개인정보보호법」은 외국의 입법례와 비교해 볼 때 허용기준에 있어서 상당한 차이가 있고, 입법기준이 매우 거칠게 법제화되어 있다. 일반개인정보의 수집·이용의 허용기준은 유럽연합의 입법례와 유사하게 법제화하고 있으나, 일반개인정보의 제3자 제공에 대해서는 유럽이나 일본과는 달리 과도하게 제한하고 있을 뿐만 아니라, 민감개인정보의 수집·이용·제공의 허용기준이 너무 엄격하여 그 집행과정에서 심각한 사회적 혼란과 비용을 초래할 것으로 보인다.

이러한 「개인정보보호법」의 기저에는 여전히 개인정보를 '비밀'로 취급하는 그릇된 오해와 그에 따라 정보주체의 동의를 절대화하려는 잘못된 인식이 깔려 있는 것으로 분석된다. 보다 면밀하고 세밀한 분석을 통해 개인정보의 이용과 보호를 균형 있게 조화시키려는 노력이 절실히 필요하다.

우리의 「개인정보보호법」이 수집·이용·제공의 허용기준을 입법화하는 방식을 보면, 우선 공공부문과 민간부문을 장을 나누어 달리 규정하지 않고 동일 조항에서 함께 묶어 규정하고 있다. 이 점은 유럽연합과 영국의 입법례와 유사하다. 그러나 '자체 이용'과 '제3자 제공'을 분리하여 그 허용기준을 달리 입법화하고 있는 점에서는 일본의 입법방식에 유사하다. 또한 일반개인정보와 민감개인정보를 나누고 그 처리의 허용기준을 달리 정하고 있는 점에서는 유럽의 입법방식과 유사하다.

이하에서는 「개인정보보호법」의 허용기준에 대해 그 타당성과 적정성 여부를 평가하고 그 수정대안을 제시해본다.

## 2. 일반개인정보 수집·이용의 허용기준의 타당성

「개인정보보호법」 제15조 제1항은 일반개인정보의 수집·이용이 정당화되기 위한 실체적 요건을 6가지로 제시하고 있다.[1] 유럽연합, 영국, 독일의 개인정보보호법과 같이 정보주체의 동의를 여러 합법성 요건 중의 하나로 제시하면서, 정보주체의 동의가 없더라도 '정당한 업무수행에 필요한 범위 내에서' 개인정보의 수집·이용을 허용하고 있다. 이는 그나마 균형 잡힌 법적 기준이라고 할 수 있다.

---

1) 법 제15조는 "일반개인정보"라는 표현을 사용하고 있지는 않지만, 제23조에서 별도로 "민감정보"의 처리(수집·이용·제공)를 규율하고 있기 때문에, 이 제15조 제1항은 민감정보를 제외한 일반개인정보의 수집·이용에 관한 실체적 요건을 규정한 것이 된다.

제15조(개인정보의 수집 · 이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

다만, 다음의 몇 가지 점에서 유럽이나 일본의 법적 기준에 비하여 다소 더 강화되어 있다.

첫째, 「개인정보보호법」은 위 제3호에서 공공기관의 수집·이용의 허용요건을 소관 업무의 수행을 위하여 "불가피한 경우"로 설정하고 있는데, 이 "불가피한 경우"라는 개념이 "필요한 경우"라는 개념보다 우리의 언어사용례에서는 더 엄격하게 느껴진다. 과거의 「공공기관의 개인정보보호에 관한 법률」 제5조는 "공공기관은 소관업무를 수행하기 위하여 필요한 범위 안에서 개인정보파일을 보유할 수 있다."고 규정하고 있는 것과 굳이 비교한다면, 수집·이용의 정당성 요건을 좀 더 강화하고 있다는 느낌을 받는다. 물론 실제의 적용에 있어서는 별반 차이가 나지 않을 수도 있을 것으로 짐작된다.

둘째, 위 제6호는 민간의 개인정보처리자가 정보주체의 동의 없이 적법하게 수집·이용할 수 있는 실체적 요건을 설정한 조항인데, 정보주체의 권리보호의 이익과의 형량기준이 유럽의 경우보다 더 엄격하게 설정되어 있다. 즉, 제6호에 의하면 정보처리의 이익이 "명백하게 정보주체의 권리보다 우선하는 경우"에 한하여 그 수집·이용은 적법한 것이 된다. 이에 비해, 유럽연합 지침에서는 민간기관의 정보처리의 이익이 "정보주체의 기본적인 권리와 자유를 보호해야 하는 이익보다 더 클 때"에 그 수집·이용은 허용된다(제7조 f항). 또한 영국의 개인정보보호법은 수집·이용이 "구체적인 사안에서 정보주체의 권리와 자유 또는 정당한 이익을 침해하여 정당화될 수 없을 때" 그것은 금지된다. 그리고 독일 연방개인정보보호법의 형량기준은 두 가지 경우로 나누어 설정되어 있다. (i) "일반적으로 접근이 가능한 개인정보"(공개된 개인정보)의 경우에는 "그 수집·이용을 금지시켜야 할 정보주체의 정당한 이익이 개인정보처리자의 정당한 이익보다 명백히 우월한 때"에 한하여 금지된다. (ii) 그 외의 개인정보는 "그 수집·이용을 금지시켜야 할 압도적인 정당한 이익이 정보주체에게 있다고 볼 만한 근거가 있는 때"에는 그 수집·이용이 금지된다. 한편, 일본의 개인정보보호법에는 이러한 형량기준 자체가 없다. 그리하여 개인정보취급사업자는 스스로 특정하여 제시한 이용목적의 달성에 필요한 범위 내에서 자유로이 수집·이용할 수 있다.

또한, 우리 「개인정보보호법」의 문구 중 정보처리의 이익이 "명백하게 정보주체의 권리보다 우선하는 경우"라는 표현은 이익형량의 기준으로서는 다소 어색해 보인다. 정보주체의 "권리가 우선"한다고 하기보다는 "수집·이용을 금지시켜야 할 정보주체의 이익이 우선"한다고 규정하는 것이 타당해 보인다.

〔수정대안〕

**6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우. 다만, 수집·이용을 금지시켜야 할 정보주체의 이익이 더 우월한 때에는 그러하지 아니하다.**

## 3. 정보주체의 동의권 인정 조항의 문제점

「개인정보보호법」 제15조 제1항이 개인정보의 수집·이용에 있어서 정보주체의 동의 요건을 절대화하지 않고 정당한 업무수행을 위해 필요한 범위 내에서 동의 없이 수집·이용할 수 있다고 규정한 것은 타당한 것으로 평가되지만, 그런데 법 제4조 제2호의 규정내용은 이러한 제15조 제1항과 모순되고 상호 충돌한다.

제15조 제1항은 정보주체의 동의 없는 정당한 수집·이용을 허용하고 있는 반면, 제4조 제2호는 "정보주체의 권리"의 하나로서 "정보주체는 자신의 개인정보 처리와 관련하여 개인정보의 처리에 관한 동의, 동의범위 등을 선택하고 결정할 권리를 가진다."고 규정하고 있기 때문이다.

이 제4조 제2호의 의미가 정보주체에게 자신의 개인정보 처리(=수집·이용·제공)와 관련하여 동의권을 부여하는 것이라면, 그리하여 정보주체의 동의 없는 개인정보의 처리를 금지하는 것이라면, 이는 정면으로 제15조 제1항과 충돌하게 된다. 그러나 그것이 명백히 잘못된 입법방향임은 위에서 강조한 바 있다. 만약 그런 취지라면 제2호는 삭제되어야 마땅하다. 특히 「개인정보보호법」은 민간부문뿐만 아니라 공공부문에 공통적으로 적용되는 법률인데, 공공기관의 업무수행에 필요한 개인정보의 처리에 대하여 정보주체의 동의권을 인정한다면 공적 업무의 수행은 거의 불가능하게 될 것이다.

다만, 제4조 제2호의 의미가 '제15조 제1항 제1호에 해당하는 경우, 즉 개인정보처리자가 정보주체의 동의를 받아 수집·이용하려고 하는 경우에 정보주체는 동의를 할 것인지, 또 동의를 한다면 어느 범위까지 동의를 할 것인지에 관하여 자유롭게 결정할 권리가 있다'는 것이라면, 제15조 제1항과 특별히 충돌하는 것은 아니라고 하겠다. 그러나 이 같은 '자유롭게 동의를 할 수 있는 권리'는 너무나 당연한 것으로서 굳이 정보주체에게 개인정보보호법이 인정하는 특별한 권리로서 명문화할 필요가 없는 것이 아닌가 생각된다.

요컨대, 제4조 제2호는 자칫 오해를 일으킬 수 있는 규정이거나 아니면 굳이 명시할 필요가 없는 규정으로서 재검토를 요한다.

## 4. 일반개인정보 '제공'의 과도한 제한과 그 문제의 심각성

### 가. 분석의 관점 : 제3자 제공의 효용성과 위험성

개인정보를 수집하는 것은 크게 '자체 이용'을 위한 경우와 '제3자 제공'을 위한 경우로 나누어진다. 일반적으로는 주로 자체 이용을 위하여 개인정보가 수집된다. 공공기관이 법적으로 주어진 자신의 소관 업무를 수행하기 위하여 개인정보를 수집하거나 또는 민간기업이 고객관리나 자사제품의 홍보를 위하여 수집하기도 한다. 그리고 이러한 자체 이용이 주된 목적이지만, 부수적으로 제3자 제공이 이루어지는 경우가 있다. 예컨대, 판매계약에 따른 상품의 송달을 위해 제3자인 배송업자에게 주소정보를 제공하는 경우이다.

그러나 한편 처음부터 제3자 제공을 목적으로 수집되는 경우가 있다. 예컨대, 민간의 경우 정보판매업자(조선일보나 중앙일보의 인물정보서비스, 법조인대관 출판)나 신용정보업자는 제3자 제공을 목적으로 개인정보를 수집하고 이를 가공하여 그 정보를 원하는 고객이나 의뢰인

에게 제공한다. 또 기업의 홍보나 광고 또는 여론조사를 위한 목적에서 개인정보를 수집하여 제공하기도 한다. 이러한 개인정보의 유통은 업무제휴의 방식으로 이루어질 수도 있고 또는 수익을 위한 판매의 형태로 이루어지기도 한다.

어떤 방식이든지 간에 개인정보의 사회적 유통은 많은 사회적 효용을 가지고 있다. 예컨대, 마케팅(marketing)의 사회적 효용은 여기서 새삼 언급할 필요가 없을 정도로 지대하고, 이러한 마케팅 목적의 개인정보의 수집·이용과 그 유통 또한 사회적으로 필요할 뿐만 아니라 그 사회적 효용이 매우 크다. 오늘날의 마케팅에 있어서 고객의 개인정보의 수집·처리는 불가결의 필수조건이기 때문이다.

특히 직접 마케팅(direct marketing) 방식은 판매자(marketer)들에게는 매우 매력적이다. 왜냐하면 많은 경우에 그 긍정적 효과를 직접 측정할 수 있기 때문이다. 예컨대, 백만 건의 광고 메일을 보냈는데 거기에 만 명의 고객이 긍정적인 반응을 했다면 직접 그 효과를 측정할 수 있게 된다. 그러나 그 광고 메일을 불쾌하게 생각하는 고객의 부정적인 반응은 쉽게 측정되지 않는다. 최근 대량의 광고메일이 원치 않는 고객에게 무작위로 전달됨에 따라 또 다른 사회적 비용이 지불되고 있다. 원치 않는 광고메일(spam)에 의한 고객의 불쾌감이나 사생활의 평온 방해 외에도 그 처리에 드는 시간 낭비나 환경적 문제 등이 야기되고 있다.

이 경우 만일 고객에 관한 보다 정확하고 상세한 정보를 판매자가 가지고 있다면 그 고객에 대한 맞춤광고를 할 수 있을 것이고, 그 결과 스팸의 문제가 일정한 정도 해결될 수 있을 것이다. 이 부분은 개인정보처리의 긍정적 측면이다. 그러나 한편으로 고객에 관한 상세하고 정확한 개인정보의 보유와 유통은 고객의 사생활 침해의 문제를 야기할 수도 있다. 이 점은 마케팅에 있어서 개인정보처리의 부정적 측면이다.

이처럼 마케팅 목적의 개인정보처리(=수집·이용·제공)가 긍정적 측면과 부정적 측면을 동시에 가지고 있을 때 그 개인정보처리에 관하여 법적으로 어떻게 규율하는 것이 바람직한가 하는 문제가 제기된다.

여기에는 몇 가지 대안을 상정해 볼 수 있다.

첫째, 마케팅 목적의 개인정보처리(=수집·이용·제공)를 전면 금지시키는 방안이 있을 수 있지만, 그러나 이는 결코 바람직한 대안이라고 볼 수 없다. 마케팅 행위가 반사회적이거나 불법적인 행위가 아닌 한 그것을 위한 개인정보처리를 불법화할 수는 없다. 세계적으로도 그러한 사례는 찾아볼 수 없다.

둘째, 정보주체에게 일정한 통제권을 주는 방안을 고려할 수 있다. 이 경우 통제권을 주더라도, 사전 동의 없는 개인정보의 처리를 금지시킬 것인지(opt-in 방식), 아니면 사전 동의가 없더라도 개인정보의 처리(=수집·이용·제공)를 허용하되 사후적으로 그 처리를 거부할 수 있는 권리(거부권)를 줄 것인지(opt-out 방식)를 나누어 고려할 수 있다. 유럽과 일본은 후자의 방식을 채택하고 있다.

셋째, opt-out 방식을 채택한다 하더라도 마케팅 목적으로 처리되는 개인정보의 범위를 제한하는 방안을 고려할 수 있다. 특히 민감개인정보의 처리를 어느 정도 허용할 것인지가 검토되어야 한다.

넷째, 자신의 마케팅 목적을 위하여 개인정보를 수집·가공·이용하는 것과 타인의 마케팅 목적을 위하여 개인정보를 수집·가공·제공하는 것을 구별하여 달리 규율할 것인가 하는 문제가 있다.

이상의 평가요소와 관점을 전제로 개인정보의 제3자 제공 또는 공유의 문제를 법적으로 어

떻게 규율할 것인지, 제3자 제공의 허용 요건을 어떻게 설정할 것인지와 관련해서 현행의 「개인정보보호법」을 검토해 본다.

## 나. 현행 법률의 내용 분석과 비판

「개인정보보호법」은 일반개인정보와 민감개인정보를 나누어 허용기준을 정하고 있고, 일반개인정보는 다시 수집·이용의 허용 요건(제15조 및 제18조)과 제3자 제공의 허용 요건(제17조 및 제18조)을 나누어 달리 규정하고 있다. 한편, 민감개인정보의 처리(=수집·이용·제공)의 허용기준은 제23조에서 규정하고 있다.

그런데 법 제17조와 제18조는 제3자 제공을 유럽이나 일본의 개인정보보호법에 비교하여 지나치게 제한적으로 허용하고 있어서 사회적으로 필요한 개인정보의 유통을 막고 있는 것으로 평가된다. 그 사회적 파장은 매우 크고 심각할 것으로 보인다.

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.
1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.
1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

제18조(개인정보의 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.
1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인정보를 제공하는 경우

5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용목적(제공 시에는 제공받는 자의 이용목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용기간(제공 시에는 제공받는 자의 보유 및 이용기간을 말한다)
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 행정안전부령으로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.

이처럼 법은 일반개인정보를 제3자에게 제공할 수 있는 '일반적 허용기준'을 제17조 제1항에서 정하고, 제18조 제2항에서는 '예외적 허용기준'을 정하고 있다.

우선 일반적 허용기준을 보면, 제17조 제1항 제1호와 제2호는 공공이나 민간의 개인정보처리자가 개인정보를 제3자에게 제공(공유 포함)할 수 있는 경우를 다음의 4가지로 제한하고 있다: (i) 정보주체의 동의를 받은 경우(제1호); (ii) 제15조 제1항 제2호("법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우")에 따라 개인정보를 수집한 목적 범위에서 제공하는 경우(제2호); (iii) 제15조 제1항 제3호("공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우")에 따라 개인정보를 수집한 목적 범위에서 제공하는 경우(제2호); (iv) 제15조 제1항 제5호("정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체의 사전 동의를 받기 곤란한 경우")에 따라 개인정보를 수집한 목적 범위에서 제공하는 경우(제2호).

그러나 이 제17조의 규정내용은 몇 가지 심각한 문제점을 안고 있다.

**첫째, 제15조 제1항의 제2, 3, 5호와 연결하여 법률문장을 구성하고 있는데, 그 의미내용이나 취지가 애매할 뿐만 아니라 규정 상호간의 정합성이 결여되어 있다**. 제15조(개인정보의 수집·이용)는 제1항 제2, 3, 5호의 경우에 정보주체의 동의 없이 개인정보를 "수

집·이용"할 수 있다는 규정이다. 이 제15조는 문언표현상 개인정보처리자 내부의 자체적인 이용을 목적으로 하는 수집에 관한 규정이다. 그렇다면 제17조 제1항은 "내부이용을 전제로 수집한 개인정보를 그 내부이용 목적의 범위 안에서 제3자에게 제공할 수 있다"는 것이 되는데, 무슨 의미인지 이해하기 어렵다. 예컨대, 제15조 제1항 제3호의 경우 공공기관의 개인정보파일 보유목적은 자신의 소관 업무의 수행을 위한 것이다. 그런데 어떻게 그 보유목적의 범위 안에서 다른 공공기관에게 제공할 수 있는 것인지 의문이 생긴다.

다만, 제17조 제1항이 의미가 있으려면, 수집목적 안에 처음부터 제3자 제공을 예정한 것이 있을 수 있다는 것인데, 그렇다면 제15조의 제목이 "수집·이용"이라고 하는 것은 맞지 않다. 물론 자신의 소관 업무를 수행하기 위해서 제3자와의 업무제휴가 필요하고 그 한도에서 개인정보를 공유할 수는 있는데, 그것이 처음부터 예정되어 있고 그리하여 수집 당시 제3자 제공을 목적으로 하고 있었다면 그러한 목적 범위 안에서 제3자에게 제공할 수 있도록 허용한 것으로 이해될 수 있다. 사실 처음부터 제3자 제공 혹은 공유를 목적으로 수집되는 경우가 있다. 그렇다면 굳이 수집·이용에 관한 제15조 제1항 제2, 3, 5호와 연결하여 제3자 제공을 허용하는 기준을 정할 것이 아니라, 독자적으로 표현문구를 사용하는 것이 타당할 것이다.

**둘째, 더욱 심각한 문제는 민간의 개인정보처리자가 "자신이나 제3자의 정당한 업무수행을 위해서" 개인정보를 제공 혹은 공유할 수 있는 길을 원천봉쇄하고 있다는 점이다. 유일하게 정보주체의 사전 동의를 받아야만 제3자 제공이 가능하도록 하고 있다(opt-in 방식). 이는 세계 유례가 없는 입법이다. 그러면서도 공공기관의 제3자 제공은 아무런 제한 없이 허용하고 있다.**

제17조는 "민간의 개인정보처리자"가 정보주체의 동의 없이 제3자에게 개인정보를 제공할 수 있는 경우를 딱 두 가지 경우, 즉 ① 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우(제15조 제1항 제2호) ② 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(제15조 제1항 제5호)에 한정하고 있다. 그리고 제18조에서는 제3자 제공이 허용되는 예외적인 경우로서, ① 정보주체로부터 별도의 동의를 받은 경우(제2항 제1호) ② 다른 법률에 특별한 규정이 있는 경우(제2항 제2호)[2] ③ 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우(제2항 제3호) ④ 통계작성 및 학술연구 등의 목적을 위한 경우로서 특정 개인을 식별할 수 없는 형태로 제공하는 경우(제2항 제4호)에 한하여 제3자 제공을 예외적으로 허용하고 있다.

**이들 규정에 따른다면, 민간의 개인정보처리자가 "자신 또는 제3자의 정당한 업무수행을 위하여" 개인정보를 공유하거나 제3자에게 제공할 수 있는 경우는 유일하게 정보주체의 사전 동의를 받는 방법(opt-in 방식)뿐이다.** 정보판매업자(조선일보나 중앙일보의 인물정보서비스, 법조인정보서비스)나 신용정보업자는 제3자 제공을 목적으로 개인정보를 수집하고 이를 가공하여 그 정보를 원하는 고객이나 의뢰인에게 제공하게 되는데, 현행법에 의하면

2) 제17조에서 제3자 제공이 허용되는 경우로 "정보주체의 사전 동의"와 "법률의 규정"을 들고 있는데, 또 다시 제18조에서 이를 제시하는 것은 어떤 의미가 있는지 불명확하다.

정보주체의 사전 동의 없는 이러한 제3자 제공은 모두 불법이 된다. 또 기업의 홍보나 광고 또는 여론조사를 위한 목적에서 우편주소나 이메일주소를 수집하여 제공하는 행위도 정보주체의 사전 동의를 받지 않으면 모두 불법이 된다. 심지어 그 위반행위에 대해서는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하여진다(제71조 제1호 및 제2호). 심지어 현행법에 의하면, 판매계약에 따른 상품의 송달을 위해 제3자인 배송업자에게 주소정보를 제공하는 경우나 또는 마케팅 목적으로 고객의 이메일정보를 위탁업자에게 제공하는 경우도 사전 동의가 없다면 모두 불법이 될 수도 있다.

특별법인 「신용정보의 이용 및 보호에 관한 법률」에서 신용정보업자는 정보주체의 동의 없이 개인의 신용정보를 수집하여 의뢰인에게 제공하는 것을 허용하고 있는데, 일반법인 개인정보보호법에서 금지시킨다고 하는 것은 입법체계상으로도 전혀 균형이 맞지 않은 입법이다.

**실로 개인정보의 필요한 사회적 유통과 이용의 가치를 전혀 고려하지 않은 세계 유례가 없는 기형적인 법률이라고 평가할 수밖에 없다.**

### 다. 수정대안의 검토

제3자 제공의 허용기준에 관해서는 적어도 유럽의 입법례나 일본의 입법례를 참조할 필요가 있다.

유럽은 제3자 제공의 허용기준을 일반개인정보와 민감개인정보로 나누어서 규정하고 있는데, (i) 일반개인정보는 개인정보처리자나 제3자의 정당한 이익을 달성하기 위한 경우에 정보주체의 동의 없는 제3자 제공을 넓게 허용하되, 다만 정보주체에게 사후에 그 제공을 거부할 수 있는 권리(right to object)를 주고 있다. (ii) 그러나 민감개인정보는 제3자 제공을 원칙적으로 금지하면서, 정보주체의 동의가 있거나 또는 그 밖에 제3자 제공이 필요한 경우를 구체적으로 열거하고 있다. 일반개인정보에 관하여 좀 더 설명하면 다음과 같다.

유럽연합의 개인정보보호지침은 일반개인정보의 수집·이용 및 제3자 제공이나 공유가 허용되기 위한 법적 기준으로서, "개인정보처리자나 개인정보를 제공받는 제3자가 추구하는 정당한 이익(legitimate interests)을 달성하기 위하여 정보처리가 필요한 때. 다만, 그러한 이익보다 정보주체의 기본적인 권리와 자유(fundamental rights and freedoms)를 보호해야 하는 이익이 더 클 때에는 그러하지 아니하다."고 규정하고 있다(제7조 f항). 이처럼 유럽연합은 정보주체의 동의 없는 제3자 제공을 개인정보처리자 또는 제3자의 정당한 이익을 달성하기 위하여 필요한 범위 내에서 넓게 인정하고 있다. 다만, "opt-out 방식(사후거부방식)"에 의해 정보주체의 통제권을 인정하고 있다. 즉, 정보주체에게 다음과 같이 사후거부권(right to object)을 주고 있다. 그리고 이 경우에도 거부권의 행사요건을 일반적인 목적의 정보처리(=수집·이용·제공)의 경우와 직접마케팅 목적의 정보처리의 경우를 나누어 달리 규정하고 있다. 후자의 경우에는 조건 없는 거부권의 행사를 인정하고 있다.

> 제14조 (정보처리에 대한 거부권: right to object) 정보주체는
> (a) 적어도 〔공공기관이나 민간기관이 자신의 정당한 업무수행을 위하여 동의 없이 합법적으로 개인정보를 처리할 수 있는 경우에(제7조 e호 및 f호)〕, 언제든지 자신의 특별한 상황과 연관된 불가피한 정당한 사유를 제시하면서(at any time on compelling legitimate grounds relating to his particular situation) 자신에 관한 정보의 처리를 거부할 수 있는 권리를 가진다. 다만, 회원국이 국내법으로 이와 달리 규정할 수 있다. 정당한 거부(a justified objection)가 있는 경우에, 당해 개인정보처리기관이 하고

있는 정보처리에서 거부 요청된 정보가 더 이상 포함되어서는 안 된다.

(b) 직접마케팅(direct marketing) 목적으로 처리될 것이 예상되는 자신에 관한 정보의 처리를, 비용부담 없이 신청에 의하여, 거부할 권리를 가지거나, 아니면 직접마케팅(direct marketing) 목적으로 제3자에게 최초로 제공되기 전이나 자체적으로 이용하기 전에 그 사실을 통지받고 그 목적의 제공이나 이용을 비용부담 없이 거부할 권리를 가진다.

회원국은 위 (b)호 제1문 소정의 권리가 있음을 정보주체가 알 수 있도록 필요한 조치를 취하여야 한다.

또한 독일의 연방개인정보보호법은 민간의 개인정보처리자가 자신의 업무수행을 위한 제3자 제공의 경우와 처음부터 제3자 제공목적으로 수집하는 경우를 나누어 제공의 허용기준을 다르게 정하고 있다. 우선 다음의 경우에는 자신의 업무수행을 위한 제3자 제공이 정보주체의 동의 없이 일반적으로 허용된다(제28조 제1항 제1문).

1. 정보주체와의 계약 또는 준계약적 신뢰관계를 위한 목적인 때
2. 개인정보처리자의 정당한 이익을 보호하기 위하여 필요하고, 또한 그 처리나 이용을 하지 못하게 할 압도적인 정당한 이익이 정보주체에게 있다고 볼 만한 근거가 전혀 없는 때
3. 그 개인정보가 일반적으로 접근이 가능한 것인 때, 또는 개인정보처리자가 합법적으로 개인정보를 공표할 수 있는 때. 다만, 그 정보처리를 배제해야 할 정보주체의 정당한 이익이 당해 개인정보처리자의 정당한 이익보다 명백히 우월한 때에는 그러하지 아니하다.

그리고 자신의 업무수행을 위한 경우가 아니라도, (i) “제3자의 정당한 이익을 보호하기 위하여 필요한 때”(제28조 제3항 제1호), 또는 (ii) “광고, 시장조사 그리고 여론조사를 위한 목적인 때”(제28조 제3항 제3호)에는 수집·이용하고 있던 개인정보를 제3자에게 제공하는 것이 허용된다. 다만, 위 (ii)의 경우에는 다음의 조건 하에서만 가능하다.

이용 또는 제공되는 개인정보는 일정 범위의 사람들에 관한 명부형식으로 된 개인정보여야 하고, 그에 포함되는 개인정보는 (a) 당해 정보주체가 그 명부에 포함되는지 여부, (b) 직업, (c) 이름, (d) 직책, (e) 대학학위, (f) 주소, 그리고 (g) 출생연도에 한정되어야 하며, 그리고 당해 정보주체가 그 제공이나 이용을 못하게 할 정당한 이익을 가지고 있다고 믿을만한 근거가 일체 없어야 한다.

그리고 이 경우에 정보주체에게는 다음과 같은 거부권이 주어진다(제28조 제4항).

정보주체가 자신의 정보를 광고, 시장조사 또는 여론조사를 목적으로 이용 또는 제공하지 못하도록 개인정보처리자에게 이의를 제기하는 때에는, 그러한 목적의 이용 또는 제공은 허용되지 아니한다. 광고, 시장조사 또는 여론조사의 목적으로 연락을 받았을 때, 정보주체는 그 개인정보처리자의 신원과 자신의 거부권에 대하여 통지를 받아야 한다. 자신이 알지 못하는 개인정보처리자가 가지고 있던 개인정보를 이용하여 〔위 목적으로〕 연락을 취하는 자는 그 개인정보의 출처를 정보주체가 알 수 있도록 보장하여야 한다. 정보주체가 위 제3항에 의하여 개인정보를 제공받는 제3자에게 광고, 시장조사 또는 여론조사를 목적으로 하는 처리나 이용을 하지 못하도록 이의를 제기한 때에는, 그 수령인

은 그 제공받은 개인정보가 위 목적으로 처리 또는 이용되지 않도록 차단시켜야 한다.

더 나아가, 독일의 연방개인정보보호법은 민간의 기업이 광고, 정보제공서비스, 상업적인 주소목록작성, 시장조사나 여론조사를 위하여 처음부터 제3자에게 제공하기 위한 목적에서 개인정보를 수집·처리하는 것을 일정한 조건 하에 허용하고 있고(제29조 제1항), 이러한 목적을 위한 제3자 제공을 다음의 경우에 허용하고 있다(제29조 제2항). 물론 이렇게 제3자 제공이 허용된 경우 정보주체에게는 당연히 거부권이 인정된다(제29조 제4항).

1. (a) 개인정보를 제공받는 제3자가 그 개인정보를 알아야 할 정당한 이익을 확실하게 증명하거나 또는 (b) 제28조 제3항 제3호에 열거한 개인정보가 명부형식으로 편집되어 광고 또는 시장조사나 여론조사의 목적으로 제공되는 경우, 및
2. 자신의 개인정보가 제3자에게 제공되지 못하게 할 정당한 이익이 정보주체에게 있다고 볼만한 근거가 전혀 없는 때.

한편, 일본의 민간부문 일반법인 개인정보보호법도 유럽과 마찬가지로 민간의 개인정보처리자가 제3자의 정당한 업무수행을 위하여 또는 광고나 마케팅 목적을 위하여 수집·처리한 개인정보를 정보주체의 동의 없이 제3자에게 제공하는 것을 합법적으로 허용하고 있다. 다만, 이 때 정보주체에게는 사전 고지와 사후 거부권(right to object)을 주어 통제할 수 있도록 하고 있다. 즉, 사후에 정보주체의 요청이 있으면 제3자 제공을 정지한다는 조건 하에, 4가지 사항을 미리 통지 또는 쉽게 알 수 있도록 하고 있는 경우에는 정보주체의 사전 동의 없이도 제3자 제공이 가능하다.[3)]

또한 다음의 3가지 경우에는 제3자 제공으로 보지 않는다(제23조 제4항).

(i) 개인정보취급사업자가 이용목적의 달성에 필요한 범위 내에서 개인데이터의 취급의 전부 또는 일부를 위탁하는 경우
(ii) 합병 기타의 사유에 의한 사업의 승계에 수반하여 개인데이터가 제공되는 경우
(iii) 개인데이터를 특정의 자와의 사이에서 공동으로 이용하는 경우로서, 그 취지 및 공동으로 이용되는 개인데이터의 항목, 공동으로 이용하는 자의 범위, 이용하는 자의 이용목적 및 당해 개인데이터의 관리에 대해 책임을 지는 자의 성명 또는 명칭에 대하여 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두고 있는 때.

## 5. 민감개인정보에 대한 과도한 보호의 문제점

「개인정보보호법」 제23조는 민감개인정보의 처리(수집·이용·제공)에 대하여 일반개인정보와 달리 특별하게 규율하고 있다. 이는 유럽의 입법례를 따른 것으로서, 일본의 경우에는 민감개인정보에 대하여 달리 특별한 규율을 하고 있지 않다. 그런데 우리 법은 유럽의 입법례에 비하여 이용보다 보호 쪽으로 지나치게 기울어져 있다. 법은 민감개인정보의 수집·이용·제공을 원칙적으로 금지하면서 그 예외를 ① 정보주체의 사전 동의와 ② 법률의 규정이라는 두 가지 경우로 매우 좁게 설정하고 있어서 그 적용과정에서 심히 불합리한 결과가 예상된다.

---

3) 미리 알려 주어야 할 4가지 사항은 (i) 제3자 제공을 이용목적으로 한다는 점, (ii) 제3자에게 제공되는 개인데이터의 항목 (iii) 제3자 제공의 수단 또는 방법 (iv) 본인의 요청이 있는 때에 당해 본인의 식별이 가능한 개인데이터의 제3자 제공을 정지한다는 점이다(제23조 제2항). 그리고 위 (ii)와 (iii)의 사항을 변경하는 때에는 그 변경내용을 미리 본인에게 통지하거나 본인이 용이하게 알 수 있는 상태에 두어야 한다(제23조 제3항).

제23조(민감정보의 처리 제한) 개인정보처리자는 사상 · 신념, 노동조합 · 정당의 가입 · 탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 "민감정보"라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우

이처럼 민감개인정보의 수집·이용·제공을 원칙적으로 금지하는 입법태도는 과거의 「공공기관의 개인정보보호에 관한 법률」과 현행의 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서 비롯된 것으로 보인다. 구 「공공기관의 개인정보보호에 관한 법률」 제4조 제1항은 "공공기관의 장은 사상·신조 등 개인의 기본적 인권을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 정보주체의 동의가 있거나 다른 법률에 수집대상 개인정보가 명시되어 있는 경우에는 그러하지 아니하다."고 규정하고 있었다. 또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제23조 제1항은 "정보통신서비스제공자는 사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 그 개인정보를 수집할 수 있다."고 규정하고 있다.

이하에서는 민감정보의 개념정의의 문제와 민감정보의 과도한 보호문제를 짚어 본다.

### 가. 민감정보의 개념정의

우선, 민감정보의 개념을 정보통신망법에서는 "사상, 신념, 과거의 병력(病歷) 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보"라고 정의하고 있으나, 「개인정보보호법」은 이를 좀 더 구체적으로 정의하고 있다. 법 제23조는 민감정보의 개념을 "사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보"라고 정의하고 있다.

이러한 개념정의는 유럽연합 개인정보보호지침이나 독일 연방개인정보보호법의 그것과 유사하다. 유럽연합 지침은 특수개인기록을 "인종적 또는 민족적 출신(racial or ethnic origin), 정치적 견해(political opinions), 종교적 또는 철학적 신념(religious or philosophical beliefs), 노동조합 가입여부(trade union membership)를 드러내는 개인기록 및 건강이나 성생활(health or sex life)에 관한 기록"이라고 정의하고 있고, 독일의 법률은 "인종적 또는 민족적 출신, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 가입여부, 건강이나 성생활에 관한 기록"이라고 규정하고 있다.

그런데 「개인정보보호법」의 개념정의 중 막연히 '사상·신념'을 모두 민감정보로 분류하여 특별취급을 하는 것은 그 개념범위가 너무 넓어져서 타당하지 못한 것으로 평가된다. '종교적 신념' 정도로 축소하여 분명하게 명시하는 것이 적절해 보인다. 또한 법은 '정당의 가입·탈퇴 정보'를 민감정보로 분류하고 있는데, 이를 민감정보로 분류하여 특별히 보호해야 할 필요가

있는지는 의문이다.

## 나. 민감정보의 과도한 보호에 대한 수정대안의 검토

유럽의 개인정보보호법들은 정보주체의 동의 없는 민감개인정보의 처리(수집·이용·제공)를 원칙적으로 금지하고 있지만, 그에 대한 예외를 넓게 인정하고 있다. 예컨대, 독일 연방개인정보보호법상 민간기관이 정보주체의 동의 없이 민감개인정보를 처리할 수 있는 경우는 다음과 같다.

첫째, 다음의 4가지 경우에는 동의 없는 수집·이용·제공이 가능하다: ① 동의를 받는 것이 사실상 또는 법적으로 불가능하지만, 정보주체나 제3자의 중대한 이익을 보호하기 위하여 필요한 때 ② 정보주체가 스스로 명시적으로 공개한 때 ③ 법적 권리의 입증·행사·방어에 필요한 때. 다만 수집과 이용을 금지시켜야 할 압도적인 정보주체의 이익이 존재한다고 인정될 때에는 그러하지 아니하다. ④ 학문적 연구의 수행을 위하여 필요한 때. 다만, 그 학문적 이익이 수집을 금지시켜야 할 정보주체의 이익보다 월등히 우월해야 하고, 달리 다른 수단에 의해서는 그 연구의 목적을 달성하기 어려운 경우라야 한다(제28조 제6항).

둘째, 예방의학, 의학적 진단, 치료 또는 건강관리서비스의 제공 목적인 경우에는 정보주체의 동의 없이도 특수개인정보(주로 건강정보나 성생활정보)의 수집이 가능하다. 다만, 그 정보는 의료전문가 또는 그에 상응하는 비밀유지의무를 지는 자에 의하여 처리되어야 한다(제28조 제7항).

셋째, 위 첫째와 둘째의 요건이 충족되는 경우에는 처음에 수집된 목적과는 다른 목적을 위하여 정보주체의 동의 없이 이용되거나 제공될 수 있다. 또한 중대 범죄의 수사를 위해서 또는 국가안보나 공공의 안전에 대한 상당한 위험을 피하기 위하여 필요한 때에는 그 이용 또는 제공은 합법적이다(제28조 제8항).

넷째, 정치적, 학문적, 종교적 목적이나 노동조합의 목적을 가진 비영리단체는 그 단체의 활동을 위하여 필요한 때에는 정보주체의 동의 없이 특수개인정보를 수집·처리·이용할 수 있다. 다만, 그 단체 구성원들의 개인정보 또는 단체의 목적과 관련하여 정규적인 관계를 맺고 있는 사람들의 특수개인정보에 한정된다. 그러나 특수개인정보를 단체의 외부 사람이나 기관에게 제공하는 것은 오직 정보주체의 동의 요건 하에서만 합법적인 것이 된다(제28조 제9항).

그런데 우리의 현행법은 민감정보의 처리(수집·이용·제공)를 금지시키면서, 단 두 가지 예외만을 설정하고 있다. 즉 ① 정보주체의 사전 동의가 있는 경우와 ② 다른 법률에서 명시적으로 민감정보의 처리를 요구하거나 허용하는 경우가 그것이다. 이렇게 되면 다른 법률에서 명시적으로 허용하지 않는 한 동의 없는 민감정보의 처리는 모두 불법이 된다.

예컨대, 정당이 정당활동의 목적으로 동의 없이 당원들의 정치적 견해를 수집하는 것은 그 자체 불법이 될 것이다. 또는 학문적 연구를 수행하기 위하여 또는 제3자의 중대한 이익을 보호하기 위하여 정보주체의 동의 없이 건강정보를 수집하거나 제공하는 것도 불법이 된다. 또 학생의 건강정보를 학생생활기록부에 기록할 때마다 교사는 학생의 동의를 받아야 할 것이다. 또는 정부가 예방의학적 목적에서 개인의 건강정보를 관련 공공기관들 상호간에 주고받는 경우에 그에 대한 '명시적인' 법률규정이 없다면 일일이 그 정보주체의 동의를 받아야 할 것이다. 현행법은 정보주체의 동의를 받기 위한 절차적 요건으로 수집·이용목적, 이용기간, 제공받는 자, 제공하는 개인정보 항목 등 여러 사항을 사전에 고지하는 의무를 지우고 있다.

이러한 사전고지에 의한 동의와 법률의 명시적인 허용규정이 없는 한 일체의 민감정보의

수집·이용·제공을 불법화하는 것은 보호와 이용의 균형을 현저히 상실한 것으로 평가된다.

만일 개인의 민감정보가 '일반인에게 공표되거나' 또는 '민감정보의 공유를 통해 정보주체에게 수인할 수 없는 차별적 혹은 불리한 결정이 내려진다면' 그에 따르는 정보주체의 사생활 또는 인격적 이익의 침해나 불합리한 차별로 인한 정보주체의 불이익이 크다고 할 수 있다. 그러나 개인의 민감정보라도 정당한 업무수행을 목적으로 하는 수집·이용·제공이 있을 수 있고, 또 그것이 널리 공표되는 것이 아니라 비밀의무를 지는 한정된 소수의 사람들에 한정해서 이용된다는 안전장치가 있다면, 그리고 그러한 정보처리의 이익보다 정보처리를 금지시켜야 할 정보주체의 이익이 더 크지 않는 한, 민감정보 처리의 위험성은 그렇게 높지 않다고 보아야 할 것이다.

이처럼 민감정보 처리의 위험성이 그렇게 높지 않은 상황을 전제로 할 때 그럼에도 불구하고 사전고지에 의한 동의획득을 민감정보 처리의 허용요건으로 한다면, 보호하고자 하는 정보주체의 이익은 적은 반면 동의획득에 수반되는 상당한 사회적 비용을 요구하는 것이 된다. 다시 말해서, 지출되어야 할 사회적 비용은 상당히 높은 반면 그로 인한 긍정적 효과는 미약하다.

요컨대, 사전고지에 의한 정보주체의 동의획득이나 또는 일일이 처리를 허용하는 법률의 제정에 수반되는 상당한 사회적 비용을 감안할 때, 그 대신에 위험성을 줄일 수 있는 안전장치를 마련해 놓고 그 한도 내에서 정당한 수집·이용·제공을 허용하는 것이 입법정책상 비용·효과 면에서 바람직한 방안이라고 판단된다.

# 개인정보 주체의 '동의': 동의의 허구성과 해결방향

고려대학교 법학전문대학원 교수 김기창

## Ⅰ. '동의' 중심의 현행 법제

개인정보 보호법("개인정보법"), 정보통신망 이용촉진 및 정보보호 등에 관한 법률("정통망법") 그리고 위치정보의 보호 및 이용 등에 관한 법률("위치정보법")은 사업자가 고객의 개인정보를 수집, 처리, 이용, 제3자 제공 등을 하기 위해서는 정보 주체의 동의를 받도록 규정하고 있다. 물론, 동의 없이도 개인정보를 수집, 이용, 제3자 제공할 수 있는 경우를 예외적으로 규정하고 있기는 하지만(이들 예외에 대하여는 뒤에서 상세히 논한다), 동의 없이 개인정보를 수집, 처리, 이용하는 행위에 대하여는 형사처벌 또는 과징금 부과 규정을 두는 등 매우 강력한 제재를 가하고 있다(개인정보법 제71조, 정통망법 제64조의3, 위치정보법 제39조, 제40조).

정보 주체의 동의를 개인정보 보호 체제의 근간으로 삼는 듯한 입장은 유럽연합에서도 나타난다. 예를 들어, 최근에 채택된 쿠키(Cookie)사용에 관한 입법지침(Cookie Directive (2009/136/EC))은 종래 별다른 동의 절차 없이 이루어지던(그러나, 이용자 자신의 기기에 쿠키가 저장되는 것을 이용자가 명시적으로 거부함으로써 opt-out 할 수 있도록 하던) 쿠키 사용을, 앞으로는 이용자의 동의에 근거하여 사용하도록(즉, 쿠키가 자신의 기기에 저장되는 것에 이용자가 동의하고 opt-in해야 쿠키 사용이 적법하게 되도록) 변경하는 정책을 취하고 있다. 물론 모든 종류의 쿠키에 이런 제약이 있는 것은 아니지만, 이용자의 웹사이트 방문 내역을 토대로 이용자의 관심 영역을 판단하여 최적화된 선전(Online Behavioural Advertising)을 하는데 필요한 제3자 쿠키의 경우 변경된 정책의 적용을 받게 된다.

그러나 유럽연합의 입법지침은 각 나라 마다 약간씩 상이한 방법으로 입법화되고 있을 뿐 아니라, 이른바 유저의 '동의'가 어느 수준에서 어떤 방법으로 '표현'되면 족한지에 대하여는 매우 많은 논란이 있다. 그러나 어느 경우건 정보 주체의 '동의'가 규제 체제의 핵심에 놓여 있다는 점은 분명하다[1].

## Ⅱ. 동의 '방식'을 법령으로 특정

개인정보법 제22조는 "정보주체의 동의를 받는 세부적인 방법"까지 법령으로 정하고 있다. 정통망법 제26조의2 또한 같다. 정통망법 시행령 제22조는 동의를 얻는 방법을 열거하고 있는데, 이용자를 직접 대면하여 서면을 교부하거나, 우편, 팩스, 이메일 등으로 전달하여 이용자가 그 내용에 동의한다는 의사를 표시하여 그 결과를 사업자에게 우편, 팩스, 이메일 등으로 보내오도록 하는 방법은 인터넷상으로 이루어지는 서비스 이용 계약 체결이라는 맥락에서는 사실상 무의미하므로 논외로 한다면, 결국 다음과 같은 두가지 방법이 법령으로 특정되어 있는 셈이다:

---

1) Andrew McStay, 'I Consent: An Analysis of the Cookie Directive and Its Implications for UK Behavioral Advertising', New Media & Society (September 30, 2012); N. van Eijk et al., 'Online Tracking: Questioning the Power of Informed Consent', Info 14, no. 5 (2012): 57-73. M. S. Kirsch, 'Do-Not-Track: Revising the EU's Data Protection Framework to Require Meaningful Consent for Behavioral Advertising', Rich. JL & Tech. 18 (2011): 1.

· 인터넷 사이트에 동의 내용을 이용자가 명확하게 인지하고 확인할 수 있도록 표시하여 게재하고 이용자가 동의 여부를 표시하도록 하는 방법 (정통망법 시행령 제22조 제1항 제1호)
· 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우, 동의 내용을 확인할 수 있는 방법(인터넷주소 링크·사업장 전화번호 등)을 이용자에게 안내하고 동의를 얻는 방법(정통망법 시행령 제22조 제2항)

위치정보법 제19조 또한 동의 확보 방법을 규정하고 있다. 예를 들어 사업자의 주소, 위치기반 서비스의 내용 등 법규가 정하는 사항을 "이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다"고 규정하고 있는 부분이 그것이다. 개인위치정보가 이용자가 지정한 제3자에게 제공될 경우에는 "매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보"하여야 한다는 규정도 두고 있다.

이러한 법제도로 규제받고 있는 국내 사업자들은 거의 예외 없이 개인정보 수집, 처리, 이용 등에 대한 이용자의 '동의'를 구하고 있고, 이용자들은 이러한 요구에 대하여 체크 박스를 클릭함으로써 동의를 '표시'하는 행위에 매우 익숙한 실정이다. 또한, 얼마전 문제가 된 이토마토 '증권통' 앱 사건에서 보듯이, 규제 당국은 수집 정보의 내용을 분명하고 자세하게 설명하지 않은 사업자에게 개인정보를 '동의 없이' 수집했다는 이유를 들어 형사처벌을 가하고 있다[2].

그러나, 개인정보 수집, 이용, 처리, 제3자 제공 등과 관련된 여러 법적 쟁점들이 정보주체의 동의만으로, 또는 동의에 기하여 해결될 수 있다고 보기에는 여러 현실적, 법리적 어려움이 있다고 생각한다. 더욱이, 동의를 받는 세부적인 방법까지를 법령으로 특정하여 둔 것은 더 어려운 문제를 만들어 낸다고 볼 여지도 있다. 이들 쟁점에 대하여 논의하기 앞서 우선 '동의'의 법적 의미에 대하여 간략히 살펴볼 필요가 있다.

## Ⅲ. '동의'의 법적 의미

정보주체의 '동의'는 개인정보 보호 및 이용을 규율하는 법제도의 중요한 축을 이루는 것이기는 하지만, 이때 말하는 '동의'가 법적으로 어떤 의미를 가지는지에 대한 상세한 논의는 막상 찾아보기 힘든 실정이다. 일반적으로 '동의'는 다음과 같은 상이한 법적 의미를 가질 수 있다:

· 사법적 계약 관계에서 요구되는 '의사의 합치', '합의'
· 형사적 범죄행위 또는 민사적 불법행위를 구성하는 어떤 행위의 위법성을 조각하는 사유의 하나인 '피해자의 승락' (volenti non fit iniuria)
· 헌법적 기본권 침해를 성립시키지 않게 만드는 권리 주체의 자발적 요청, 승인

이하에서 이들 각각에 대하여 간략히 살펴본다.

### 1. '약관 내용'에 대한 동의가 필요한가?

사업자와 이용자 간에 해당 서비스 이용에 관한 의사 합치가 없다면 '계약 체결' 자체가 불가능할 것이다. 서비스 이용 계약이 체결되었다는 말은 곧 해당 서비스 제공 및 이용에 관한 의사 합치가 있었다는 말이다. 그러나 해당 서비스를 위하여 이용자로부터 어떤 정보(개인정

2) 서울중앙지방법원 2011. 2. 23. 선고 2010고단5343 판결

보를 포함해서)가 수집되고 어떻게 이용되는지는 서비스의 구체적 내용에 따라 다를 것이며, 그 상세한 내용은 서비스 이용 약관(terms of service)에 규정되는 것이 보통이다. 그러나 약관을 사용하여 정형적, 반복적으로 이루어지는 소비자 계약 관계에서 소비자가 약관 내용의 상세한 모든 부분을 실제로 인식하거나 이해하기를 기대할 수는 없다. 약관은 사업자가 일방적으로 마련하는 것이고, 약관 내용을 계약의 일부로 편입하기로 하는 합의가 있는 이상 비록 "계약자가 그 약관의 내용을 알지 못하더라도" 그 약관의 구속력을 배제할 수 없는 것이 원칙이다[3]. 그러나 약관 조항의 의미나 효력은 분쟁이 발생한 연후에 사후적으로 법원의 해석과 판단을 통하여 비로소 확정된다. 우리 대법원은 "약관의 내용은 개개 계약체결자의 의사나 구체적인 사정을 고려함이 없이 평균적 고객의 이해가능성을 기준으로 하여 객관적·획일적으로 해석하여야 하고, 고객보호의 측면에서 약관 내용이 명백하지 못하거나 의심스러운 때에는 고객에게 유리하게, 약관 작성자에게 불리하게 제한 해석하여야 한다"는 입장을 확고히 유지하고 있다(밑줄은 필자가 추가)[4].요컨대, 약관 내용을 계약의 일부로 편입하기로 합의한 이상, 약관 조항들은 '일단은' 구속력을 배제할 수 없고 이용자가 약관의 내용을 몰랐다거나 그 내용에 동의하지 않았다는 이유로 그 약관의 효력을 부인할 수는 없다.

반면에, 설사 이용자가 약관의 특정한 조항을 구체적으로 알고서 이에 동의하고 계약을 체결했다 하더라도 해당 조항이 신의칙에 반하여 공정성을 잃은 내용이라면 그런 조항은 효력이 없다. 약관의 규제에 관한 법률("약관규제법") 제6조는 다음과 같이 규정하고 있다.

> ① 신의성실의 원칙을 위반하여 공정성을 잃은 약관 조항은 무효이다.
> ② 약관의 내용 중 다음 각 호의 어느 하나에 해당하는 내용을 정하고 있는 조항은 공정성을 잃은 것으로 추정된다.
> 1. 고객에게 부당하게 불리한 조항
> 2. 고객이 계약의 거래형태 등 관련된 모든 사정에 비추어 예상하기 어려운 조항
> 3. 계약의 목적을 달성할 수 없을 정도로 계약에 따르는 본질적 권리를 제한하는 조항

당사자(이용자)가 해당 조항을 실제로 '알았는지', 해당 조항의 내용에 '동의'했는지 여부는 아예 고려 대상이 아니라는 점은 이 조항의 문언 자체에서도 명백할 뿐 아니라, 실제로 어느 이용자가 어느 정도까지 해당 약관 조항을 이해하고 동의했는지를 약관의 해석에 반영하려 시도한다면, 이는 "약관의 내용은 개개 계약체결자의 의사나 구체적인 사정을 고려함이 없이 … 객관적·획일적으로 해석"되어야 한다는 대법원의 확고한 입장에 반하는 것이다.

요컨대, 약관은 그 내용을 당사자가 몰랐다고 해서 적용이 배제되는 것이 아니고, 특정 당사자가 알고서 명시적으로 동의를 표시했다고 해서 언제나 효력이 있는 것도 아니다. 약관의 내용(그 내용을 알았건 몰랐건)을 계약의 일부로 하겠다는 점에 대하여 당사자들이 동의한 이상, 일방(이용자)이 약관 내용 자체를 알았건 몰랐건, 약관 내용에 대한 '동의'가 표시되었는지 아닌지를 전혀 고려하지 아니하고, 법원이 약관 조항의 공정성을 사후적으로 심사하여 그 효력을 객관적, 획일적으로 결정한다는 것이 약관의 효력에 대한 확립된 법리이다.

인터넷으로 체결되는 계약이라 해서 이러한 약관 법리가 수정되어야 할 이유는 없다. 문제는, 개인정보의 수집, 처리, 이용(제3자 제공 포함)에 관해서는 지금껏 유지되어 왔던 이러한

3) 대법원 1989.3.28. 선고 88다4645 판결, 대법원 1991.9.10. 선고 91다20432 판결 등
4) 대법원 1989.3.28. 선고 88다4645 판결, 대법원 1991.9.10. 선고 91다20432 판결 등

약관 법리를 적용하지 아니하고 다르게 규율할 이유가 있는지 여부이다. 앞서 소개한 개인정보법, 정통망법, 위치정보법은 전통적인 약관 법리를 다음과 같이 중대하게 수정하는 내용을 담고 있다.

- 첫째, 개인정보 수집 등에 관한 사항을 약관에 기재하고, 그러한 '약관 내용'에 대한 동의를 '특정한 방법으로' 얻어야 한다고 규정하고 있다. 그러나 기존의 약관 법리에 따르면, 약관을 계약에 편입할지 여부에 대한 동의만 요구될 뿐, 약관 내용(개인정보 처리에 관한 부분도 약관 내용의 일부임)에 대한 이용자의 동의가 필요한 것이 아니다. 그런 동의가 어떤 특정한 방식으로 '표시'되어야 하는 것은 더더욱 아니다.

- 둘째, 약관 내용(개인정보 수집 등에 관한 부분)에 대하여 법령이 정한 방식으로 '동의'를 얻기만 하면 해당 약관 조항의 효력에 대하여 법원이 사후적으로 판단할 여지가 아예 없어지는 듯 암시하고 있다. 개인정보법 제15조 제1항은 "다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다"고 규정하는데, 거기 나열된 경우 중 첫번째(제15조 제1항 제1호)가 바로 "정보주체의 동의를 받은 경우"이기 때문이다. 그러나 기존의 약관 법리에 따르자면, '약관 내용'에 대한 동의는 애초에 필요 없을 뿐 아니라, 설사 일부 이용자가 특정 약관 조항을 실제로 이해하고 그 내용에 명시적으로 동의하고, 그렇게 동의했다는 점을 '표시'까지 하고서 계약을 체결했더라도 그 조항이 신의칙에 반하여 공정성을 잃었다고 법원이 판단한다면 그런 조항의 효력은 획일적으로 부인되어야 한다(비록 일부 이용자가 그 내용을 이해하고 동의했어도 그런 이용자와의 관계에서도 효력이 없다). 그러나 현행 개인정보법은 오히려 이런 입장을 취하기 어렵게 만들고 있다.

온라인상으로 체결되는 각종 서비스 이용 계약에서 문제되는 개인정보의 수집 등에 관한 사항은 사법적 계약 관계(서비스 이용 계약)에 편입되는 약관 내용의 일부를 이루는 것임은 분명하다. 기존의 약관 법리에 의하자면 약관 내용을 이용자가 인식, 이해, 동의하였는지, 그러한 동의가 표시되었는지와는 전혀 무관하게 약관 조항의 효력이 결정되는데 반하여, 개인정보법 등 현행 법령들은 개인정보 수집 등에 관한 약관 '내용'을 이용자가 인식, 이해, 동의하였는지, 그리고 그 동의를 표시하였는지를 중요하게 고려하고 있으므로 약관 법리와는 근본적으로 다르다. 약관 내용 중 개인정보 수집 등에 관한 부분을 이처럼 기존의 약관 법리와는 다르게 취급하는 것이 과연 바람직한지는 뒤에서 논한다.

## 2. 피해자의 승낙

개인정보 수집 등에 관한 이용자의 '동의'를 '약관 내용에 대한 동의'라고 파악하지 않고, 형사상 범죄행위나 민사상 불법행위의 피해자가 하는 '승낙'이라고 파악하는 것은 법리적으로 가능할까?

피해자가 승낙하는 행위는, 그 승낙이 사회 상규에 반하지 않는 이상, 위법하지 않다. 치료행위가 그 대표적인 예이다. 치료 행위는 환자의 신체에 대한 침습을 수반하는 것이므로 만일 환자 또는 그 보호자의 승낙이 없다면 그러한 행위는 위법한 가해행위(형사상 상해죄 및 민사상 불법행위)가 될것이다. 의학 연구나 실험의 대상이 되고자 자원하는 행위도 법리적으로는

‘피해자의 승낙’으로 설명된다. 왜냐하면 연구나 실험 과정에서 신체의 침습 또는 사생활의 침해가 이루어질 것이지만, 당사자(동의가 없었더라면 ‘피해자’로 될 자)가 그러한 ‘침해’를 승낙함으로써 그자를 상대로 한 연구 및 실험행위 자체가 위법하지 않게 된다. 물론 승낙이 과연 적법, 유효, 적절한지에 대하여는 많은 복잡한 고려가 필요하다. 하지만, (i)연구나 실험의 내용을 충분히 이해하고, (ii)부당한 심리적 제도적 사회적 압박 없이 자유롭게 동의하였다면 대부분 유효한 동의로 평가되어 연구나 실험을 수행하는 자의 행위가 위법하지 않게 될 것이다.

치료, 연구, 실험 행위 자체가 자신을 대상으로 행해지는 것에 동의하는 것은 이처럼 ‘피해자의 승낙’으로 분석하는 것이 옳고, 이른바 ‘informed consent’라는 개념에 대한 여러 연구는 바로 치료, 연구, 실험 등에 대한 환자 또는 연구 객체의 동의에 관한 것이다. 그러나 개인정보의 수집이나 처리등에 대한 동의도 ‘피해자의 승락’이라고 파악하고, ‘informed consent’라는 개념을 여기에 동원, 적용하는 것이 옳은지는 의문이다. 치료, 연구, 실험 행위에 관하여 환자 또는 보호자의 ‘동의’가 필요한 이유는 치료 등의 행위 그 자체가 환자의 신체에 대한 침습을 수반하기 때문이고, 환자의 ‘동의’ 역시 그러한 치료 등 행위가 자신의 신체에 대하여 이루어지는데 대한 승낙을 말하는 것이다. 그러나 치료 등의 행위와 부수하여, 그 행위의 일부분으로서 또는 그 행위의 기회에 이루어지는 개인정보 수집에 대한 동의는 치료 등 행위 자체에 대한 승낙과는 구분되어야 한다. 당사자들 간의 관계, 당사자의 의도, 당사자들 간의 교섭의 맥락, 그리고 일반적으로 이런 상황에서 사람들이 기대하고 예상하는 것이 무엇인지 등을 고려한다면, (i)내 배를 가르고 내 몸에 약물을 주입하는데 동의하는 것(피해자의 승낙)과 (ii)‘그런 치료, 연구, 실험에 부수하여’ 내 개인정보를 수집하는데 동의하는 것을 같게 보고, 두 경우 동의의 법적 효력 등을 동일하게 분석해야 한다는 입장은 극단적인 형식논리(‘동의’는 모조리 동일하다는 지극히 피상적인 논리 조작)에 매몰된 궤변에 가깝다고 생각한다.

애초에 아무런 치료, 연구나 실험도 이루어지지 않고(따라서 어떠한 신체에 대한 침습이나 사적비밀에 대한 접근도 없고), 오로지 개인정보만 수집, 이용하겠다며 동의를 구하는 경우라면, 당사자가 개인정보 수집, 이용에 실제로 동의하였지 여부가 핵심적 중요성을 가질 것이다. 그러나 치료 행위 자체에 대한 승낙이 이루어졌다면, 그 기회에 그와 부수하여 개인정보가 수집, 이용될 경우 그에 관한 사항은 치료서비스 이용 조건을 규정한 약관으로 규율되면 족하고, 그 법적 효력에 대한 분석도 약관 법리에 따르는 것이 타당한 것이지, 그것을 치료 행위 자체에 대한 동의(‘피해자의 승낙’)와 동일시 해서는 안될 것이다.

일반적으로 인터넷 상에서 제공되는 여러 서비스의 경우도 마찬가지이다. 해당 서비스를 받겠다는 합의는 계약 성립의 핵심적 요소이므로 이용자와 사업자(서비스 제공자) 간의 동의(의사 합치)가 필요하다. 이 점에 대한 동의가 없다면 서비스 이용 계약 자체가 성립될 수 없을 것이다. 그러나 서비스를 받겠다고 합의한 이상, 그에 부수하여 그 서비스의 이용 및 제공과 관련하여 개인정보가 어떻게 수집, 이용되는지의 문제는 당사자의 합의나 동의가 아니라 서비스 이용 약관으로 규율되는 문제라고 생각한다. 요컨대, 이용자와 사업자 간에 (1)서비스 이용 자체에 대한 동의(의사 합치)는 있어야 하고, (2)이용 약관(개인정보 수집, 이용 등을 규정해둔 약관)을 서비스 이용 계약의 내용으로 편입할지 여부에 대한 합의 또한 반드시 있어야 하지만, (3)약관 내용에 대한 동의는 당사자 간의 계약관계를 규율하고 약관의 효력 여부를 판단하는데 고려되어서는 안되는 것이 원칙이라고 생각한다.

약관 법리는 애당초 약관 ‘내용’에 대한 이용자의 인식이나 동의를 요하는 것이 아니며, 피해자의 승낙이라는 개념과도 전혀 무관하다. 서비스 이용 계약 관계 성립 자체에 요구되는 ‘합

의'가 언제나 '피해자의 승낙'으로서의 성격을 가지는 것도 아니다. '피해자의 승낙'은 해당 서비스가 침해적 요소를 내포하고 있어서 당사자(환자 등)의 승낙이 없으면 위법하게 될 경우(예를 들어, 시술 행위 등), 해당 시술이나 서비스를 받겠다는 당사자의 승낙이 있었는지를 판단하는데 유용할 뿐이다. 일단 그 서비스(치료 등)를 받겠다는 당사자의 승낙이 있은 이상, 그에 부수하여 개인정보가 어떻게 수집, 이용되는지에 대한 문제까지도 '피해자의 승낙'이라는 개념으로 설명하려 시도하는 것은 피상적인 형식논리일 뿐 아니라 치료행위 자체와 그에 부수된 개인정보 수집, 수집 이용 행위를 혼동하는 것에 불과하다.

## 3. 헌법적 기본권을 포기하는 내용의 약정?

개인정보 수집, 이용에 관한 정보주체의 '동의'를 요구하는 현행 법제도는 기존의 약관 법리에도 어긋나고, 피해자의 승낙이라는 개념으로 설명하기도 어렵다면, 개인정보의 자기결정권 등 헌법적 기본권을 포기하는 내용의 약정으로 볼 여지는 없을까? 그러나 국가가 개인의 동의에 근거하여 헌법적 기본권을 박탈할 수 있다는 입장을 취하는 논자는 없어보인다. 예를 들어, 개인이 참정권을 포기하겠다고 정부를 상대로 약정한다고 해서 그 약정이 법률상 효력을 가지기는 어려울 것이다. 다른 예로서, 정부가 사회 단체에 예산을 지원하면서 정부에 대한 비판을 하지 않겠다는 약정(표현의 자유를 일부 포기하겠다는 약정)을 받아낸다고 해서 그런 약정이 법적으로 효력을 가질 수는 없을 것이다[5].

이렇게 본다면, 개인정보의 수집, 이용 등에 관한 '동의'를 헌법적 기본권의 일부를 포기하는 약정으로 분석할 수는 없다고 생각한다. 따라서 개인정보의 국외 이전 허용 여부를 오로지 이용자의 동의만을 기준으로 결정하도록 하고 있는 정통망법 제63조 제2항("개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다")은 개인의 기본권이 침해되는 한에서는 위헌적인 조항이라고 생각한다. 국내의 제3자라면 모두 정통망법 등 여러 관련 법제가 규정하는 개인정보 보호의무를 지고 있으므로 정보주체의 동의가 있으면 제3자 제공이 허용된다는 점은 쉽게 납득이 간다. 그러나 국외의 사업자들 중에는 한국법의 기준을 상회하는 정보보호 의무를 부담하는 자들도 있겠지만, 한국법의 기준으로 볼때 용납될 수 없는 수준의 사업자들도 있을 수 있다. 이점에 대한 고려나 고민이 없이 그저 '이용자의 동의'만 있으면 개인정보의 국외 이전이 가능하다고 규정하고 있는 정통망법은 기본권 포기 약정이 마치 유효한 약정인 것처럼 오해하고 있다는 비판이 가능하다.

> 그러나, 개인정보법 제17조 제3항은 다음과 같이 조금 다르게 규정되어 있다:
> 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

이용자가 '동의'하기만 하면 개인정보 보호와 관련하여 더 이상 아무런 고려가 필요없다는 듯한 입장은 기본권 보호의 근본 원리에 반할 뿐 아니라, 실제로 이용자의 '동의'가 있었다 하더라도 그 동의가 약관의 형태로 확보된 것이라면, 그런 약관 조항이 과연 유효한지는 이용자의 '동의'와는 무관하게 획일적, 객관적으로 판단하여야 한다는 확립된 법리에도 반하는 것이다.

---

5) P. Hamburger, 'Unconstitutional Conditions: The Irrelevance of Consent', Virginia Law Review 98 (2012): 107 ("Private or state consent cannot enlarge the government's constitutional power.")

## Ⅳ. '약관 법리'의 재평가

개인정보 수집, 처리, 이용 등에 관한 사항은 비록 약관의 일부를 이루는 것이긴 하지만, 약관의 다른 내용에 비하여 그 중요성과 이용자에게 미치게 될 잠재적 위험의 정도가 다르므로 약관 중 이 부분을 '분리'하여 기존의 약관 법리와는 달리 이용자의 명시적, 현실적 '동의'를 받도록 하겠다는 것이 아마도 개인정보 보호에 관한 현행 법제의 태도인 것 같다. 그러나, 의도야 비록 좋을지 몰라도 이런 입장은 종래 치료, 연구, 실험 등에 참여하는 '피해자의 승낙'으로서의 의미를 가지던 'informed consent'라는 개념을 개인정보 수집 등에 관하여 무비판적으로 확장하여 불필요한 혼동을 초래하고 있을 뿐 아니라, 이용자 행태의 실상을 간과한 무모한 입장이라고 생각한다. 그 이유는 다음과 같다:

· 첫째, 이용자의 '동의'를 요구하고, 그 동의를 '표시'하게 하면서, 명확하고 충분한 설명을 하도록 규정할 경우, 비록 이론적으로는 흠잡을 데 없는 '제대로 된 동의'가 있다고 볼 수 있겠지만, 현실적으로 과연 이용자가 약관의 해당 부분을 어느 정도 이해하고 동의하였는지를 확인할 방법은 없다. 이용자가 개인정보 처리와 관련된 약관 내용을 실제로 이해할 가능성을 높이기 위해서는 (뒤에서 설명하듯이) 사업자의 설명의무를 제대로 관철하는 방안을 모색해야 하는 것이지, 이용자가 약관 내용에 '동의'하도록 하거나, 그 동의를 '표시'하게 한다고 해결되는 문제가 아니다.

· 둘째, 이용자의 동의를 '표시'하게 함으로써, 법원이 불공정한 약관 조항에 대하여 사후적으로 개입하여 그 효력을 부인하는 것을 오히려 어렵게 만들게 되어 (동의를 '표시'하지 않아도 될 뿐 아니라, 아예 이용자의 동의에 기반 하지 않는 기존의 약관 법리에 비하여) 이용자에게 더 불리한 결과를 낳게 된다. 애초에 '약관 내용'에 대한 동의를 표시하지 않았을 경우, 이용자는 예측하지 못한 약관 조항의 효력을 다투기가 '현실적으로' 더 용이하게 되지만, 현행 법제는 이용자가 약관 내용 중 개인정보 처리 방침에 대하여 동의를 명시적으로 표시하게 만들고 있으므로, 그 약관 조항의 효력을 사후에 다투는 것이 '현실적으로는' 더 어렵게 된다(동의해 놓고 왜 시비를 거느냐? 는 반론이 가능해지기 때문). 특히, 약관 내용 중 개인정보 취급에 관한 사항을 실제로 이해했건 못했건 '동의'를 '표시'해야만 서비스 이용 계약 체결이 가능한 현실을 고려한다면, 현행 제도는 이용자의 불복을 사실상 불가능하게 만든다. "정보 주체의 동의를 받아 개인정보를 수집, 이용할 수 있다"는 명문의 법규정은 이용자에게 결코 유리하게 작용하지 않는다.

· 셋째, 이용자의 동의를 반드시 받도록 강요하는 현 체제는 사업자에게도 불편하게 작용한다. 해당 거래의 성격이나 맥락에 비추어 일반적으로 예상할 수 있는 한도에서라면 이용자의 동의와 무관하게 약관의 효력이 배제되지 않는다는 약관 법리가 관철되었더라면 대부분의 경우 사업자는 약관에 해당 내용을 규정하고 이용자가 알 수 있게 해둠으로써 이용자의 '동의'나 동의의 '표시'가 없이도 개인정보를 '해당 서비스 이용관계에서 일반적으로 예측가능한 한도에서는' 수집, 이용하며 사업을 적법하게 영위할 수 있을 것이지만, 현행 개인정보 보호 법제는 그러한 가능성을 대폭 축소하여 사실상 기계적으로 '동의'를 받도록 강요하고 이용자 역시 기계적으로 동의를 하고 있다.

실효성이 전혀 없는 요식행위를 반복, 누적함으로써 개인정보 보호가 될 것이라고 스스로를 기만하는 딱한 형국이라고 생각한다.

개인정보의 수집, 이용 등에 관하여는 약관 법리의 적용을 배제, 포기하고, 이용자의 '동의'를 구하도록 하는 현재의 제도가 과연 현명한지를 논하기에 앞서, 약관 법리를 조금 더 살펴볼 필요가 있다.

약관은 이용자의 주관적 '동의'가 필요한 것이 아니라 객관적으로 그 내용이 '공정성'과 '예측가능성'을 갖추어야 효력이 있고, 그렇지 못하면 효력이 없다는 것이 약관 법리의 핵심이다. 앞서 인용한 약관규제법 제6조는 "고객이 계약의 거래형태 등 관련된 모든 사정에 비추어 예상하기 어려운 조항"은 공정성을 잃은 것으로 추정되어 사업자가 그 조항이 그래도 공정하다는 점을 입증해야 비로소 효력이 유지될 수 있도록 하고 있다. 예를 들어, 해당 서비스 이용계약에서 일반적으로 예상할 수 있는 범위를 벗어나는 특이한 용도로 개인정보가 이용된다는 점을 약관에 규정해 둔 경우, 그 약관의 효력을 부인 당하지 않으려면 이용자의 '동의'를 받았다는 것으로는 안되고(어차피 약관 내용에 대한 '동의' 여부는 약관의 효력과는 무관하므로) 사업자가 적절한 방법으로 충분히 해당 내용을 설명하여 이용자들이 그 내용을 예상할 수 있도록 만들었는지가 관건이 된다. 즉, '동의'에 초점이 놓이는 것이 아니라 효과적이고 충분한 '설명'을 고객에게 하였는지에 초점이 놓이는 것이다.

일반적으로는 고객이 예상하기 어려운 내용이더라도, 해당 서비스 이용 계약을 체결하는 기회에 사업자가 '적절한 방법으로' 그 내용을 사전에 충분히 설명하였다면, "거래 형태 등 관련된 모든 사정"을 감안할 경우, 결국 그 내용도 예상할 수 있게 되었다고 평가될 여지도 있고, 예상하기는 여전히 어렵더라도 충분히 설명되었기 때문에 공정성을 잃은 조항은 아니라고 판단 받을 가능성이 높아질 것이다.

물론 약관 조항의 효력 여부가 이런 식으로 '사후(분쟁 발생 후)에' 비로소 판가름 나도록 되어 있기 때문에 해당 약관 조항의 효력에 대하여 불확실성이 존재하게 된다. 그러나 이런 '불확실성'은 사업자로 하여금 해당 조항을 더욱 분명하고 효과적으로 고객에게 설명하도록 유인을 제공하는 것이므로 이용자의 보호가 소홀히 되는 것은 아니다. 실제로 큰 액수의 경제적 이해관계가 걸려있는 보험 계약, 운송 계약 등에서 바로 이런 방식으로 고객과 사업자 간의 이해관계를 지금껏 조정해 왔음을 고려할 필요가 있다. 유독 개인정보 보호 분야에서는 이런 방법으로는 제대로 정보 주체의 보호가 이루어지지 못할 것이라고 전제할 근거는 없어 보인다.

현행 개인정보 보호 법제는 이용자의 '동의'를 받음으로써 해당 약관 조항의 효력에 관한 불확실성을 사전에 제거해주고 있다. 이러한 규제 전략이 과연 이용자에게 실제로 유리하게 작용하는지는 냉정하게 평가되어야 한다. 물론, 법령은 정보주체가 "명확하게 인지할 수 있도록 알리고" 동의를 받아야 한다고 규정하고 있지만(개인정보법 제22조 제1항, 정통망법 시행령 제22조 제1항 제1호 참조), 그런 규정을 둔다고 사업자가 이용자에 대한 설명에 실제로 노력을 기울일 가능성은 없다. 현재와 같이 약관 해당 부분을 무조건, 모조리 제시하고 거의 아무도 그 내용을 실제로는 읽지 않은 채 체크박스를 모조리 클릭하여 동의를 표시하는 엄연한 현실을 애써 외면하면서 "정보주체의 동의를 받게 했으니 개인정보 보호가 될 것"이라 자위하는 것은 무책임하며 안일한 태도라고 생각한다. 이용자의 '동의'가 표시되고 나면, 이용자가 내용을 알고 체크하였건 모르고 체크하였건, 이용자에게 "명확하게 알리지 않았다"는 이유로 이용자 동의의 효력이 부정될 가능성은 오히려 낮아진다. 반면에 약관 법리에 충실하게 이

용자 동의를 전혀 요하지 않을 경우, 사업자는 “예측하기 어려운 내용에 한하여” 현재 보다는 더 효과적인 방법으로 그 내용을 이용자에게 설명하려 진지하게 노력할 인센티브가 있게 된다. 그런 노력을 기울이지 않을 경우 해당 약관 조항은 사후에 효력을 부인당할 가능성이 크기 때문이다. 물론 이용자가 일반적으로 예측할 수 있는 내용이라면 사업자가 굳이 설명할 필요도 없을 것이다.

기존 약관 법리를 그대로 적용했더라면, 사업자는 ‘예측하기 어려운 약관 조항에 대하여’ 그 내용을 이용자에게 각별히 설명하기 위한 노력을 집중하게 되었겠지만, 정보주체의 ‘동의’를 받도록 해둔 현행 법제하에서는, 예측할 수 있는 내용인지 예측할 수 없는 내용인지를 가리지 아니하고 사업자는 무조건 이용자의 ‘동의’를 받고 말 뿐, 이용자에게 정작 필요한 ‘설명’을 효과적으로 제공하려는 노력을 기울일 인센티브는 상대적으로 줄어든다.

# Ⅴ. 개선 방안

개인정보 보호에 관한 현행 법령은 정보 주체의 동의 없이 개인정보를 수집, 이용할 수 있는 경우를 ‘예외적’인 것으로 규정하고 있다. 예를 들어, 개인정보법 제15조 제1항 제2호-제6호는 “법률에 특별한 규정이 있거나”, 법령상 의무를 준수하거나 업무를 수행하기 위하여 불가피한 경우, “정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우” 등에는 동의 없이 개인정보의 수집, 이용이 가능하도록 정하고 있다. 정통망법 제22조 제2항 제3호도 “이 법 또는 다른 법률에 특별한 규정이 있는 경우”에는 정보 주체의 동의 없이 개인정보를 수집, 이용할 수 있도록 규정하며, 위치정보법 제15조 제1항 제3호도 “다른 법률에 특별한 규정이 있는 경우”에는 당사자의 동의 없이 위치정보를 수집할 수 있도록 규정하고 있다.요컨대, 원칙적으로는 정보 주체의 동의를 받아야 하지만, 특별한 경우에 예외적으로는 동의 없이도 개인정보의 수집, 이용 등이 가능하다는 것이다.

그러나, 정보 주체의 ‘동의’를 원칙으로 삼는 현행 법제는 다음과 같은 문제점이 있다:

- 첫째, 서비스 제공 “목적에 필요한 범위에서 최소한의 개인정보만을 수집”해야 한다는 최소 수집 원칙(개인정보법 제3조 제1항)과의 관계를 분분명하게 만든다. 정보 주체의 ‘동의’가 있기만 하면 불필요한 정보를 마구 수집해도 “적법하고 정당하게” 된다는 뜻은 결코 아닐 것이다. 그러나 정보주체의 ‘동의’가 있을 경우, 동의 자체가 정보 수집, 이용의 적법성과 정당성의 근거로 작용할 위험이 생기게 되며, 최소 수집의 원칙을 관철하는 것이 현실적으로 매우 어렵게 된다.

- 둘째, 동의에 의존할 경우, 동의의 내용을 이용자가 현실적으로 이해하도록 확보할 방법이 없다. 더욱이, 동의가 일단 표시되고 나면 그 내용을 사후에 다투는 것이 현실적으로 오히려 더 어려워진다. 반면에, 약관 법리는 동의에 의존하지 않는 대신, 예측을 넘어서는 불공정한 약관 조항을 사후적으로 무효화함으로써, 사업자들이 해당 조항을 사전에 고객에게 충분히 설명하도록 실효성 있는 인센티브를 제공한다.

- 셋째, 해당 서비스 제공에 필수 불가결한 한도의 개인정보 수집, 이용 등의 경우 그에 대한 동의가 없으면 서비스 이용 계약 체결 자체가 불가능하게 되는데, 이런 경우 서비스 이용 계약 체결(의사 합치)과 구분하여 개인정보 수집 등에 대한 ‘동의’를 별도

로 표시하도록 하는 것은 법리적으로도 무의미하다. 해당 약관 내용에 대한 동의를 거부하면 계약 체결이 아예 불가능하다면 계약 체결에 필요한 합의가 곧 그런 약관이 계약에 편입되는 것에 대한 동의가 되기 때문이다. 물론, 해당 서비스 제공에 필수 불가결한 개인정보 수집, 이용이라고 해서 모두 예측 가능한 것은 아니다. 예측 가능하지 않은 내용의 개인정보 수집, 이용에 대해서는 충분한 '설명'이 제공되어야 하는 것이지 이용자의 '동의'가 필요한 것은 아니다. '동의'를 받도록 할 경우, 관심의 초점은 동의를 받았는지 여부에 놓이게 되는데 이는 무의미하고(약관 동의 없이는 계약 체결이 불가능하기 때문에 계약 체결이 이루어졌다면 해당 약관 조항에 대한 동의는 100% 이루어졌을 것임), 정작 '설명'이 충분하였는지에 대하여는 제대로 다투기 어렵게 된다.

개인정보의 보호는 정보 주체의 '동의'에 의존하여 해결될 수 있는 문제가 아니라, 사업자가 이용자에게 개인정보의 수집, 이용에 대하여 얼마나 효과적으로 '설명'하게 만들 것인가에 중점을 두고 풀어나가야 한다. 해당 서비스의 성격과 맥락을 전체적으로 판단하여 일반적인 이용자가 예상할 수 있는 내용이라면, 이에 대한 설명의 필요는 없을 것이고, 이런 뻔한 내용에 대하여 굳이 동의를 '표시'하도록 해서 얻을 것도 별반 없다고 생각한다. 반면에 일반적으로 이용자들이 예상하기 어려운 내용에 대해서 사업자들이 제대로 설명하도록 인센티브를 제공하기 위해서는 '이용자 동의'라는 쉬운 '탈출구'를 사업자에게 열어주기 보다는, 적절한 방법으로 충분히 설명하여 이용자로 하여금 해당 내용을 '예측'할 수 있도록 만들지 않으면 해당 약관 조항의 효력을 사후적으로 부인하겠다는 높은 관문을 유지하는 것이 옳다. 즉, 기존의 약관 법리를 그대로 유지하는 것이 개인정보 보호를 위한 올바른 규제 기법이라고 생각한다.

한편, 정보주체의 '동의'는, 이용자가 동의를 거부하고도 해당 서비스 이용 계약을 체결할 수 있을 선택가능 조항('optional' terms)에 한하여 의미를 가질 수 있다. 동의를 거부하면 서비스 이용 계약 체결이 아예 불가능한 당연 편입 조항이라면, 그런 조항의 존재와 내용을 안내하면 족할 뿐이고, 동의 여부를 표시(체크)하게 해서는 안된다. (물론 그 내용 중 일반적으로 예측 가능하지 않은 부분이 있다면 사업자는 해당 내용을 특별히 '설명'하여 예측 가능하게 만들어야 하고, 그렇게 하지 않을 경우 해당 약관 조항은 그 효력을 사후에 부인당할 것이다). 동의할지 말지를 이용자가 선택할 수 있는 (진정한 선택권을 가지는) 항목에 한해서만 사용자에게 동의할지 말지를 '선택'할 수 있도록 체크 박스를 제시하는 것이 사업자로서도 정직한 태도이다. 동의를 거부하는 것이 가능할 경우에만 체크박스가 제시되도록 하면, 동의 체크박스는 "체크할지 말지를 선택할 수 있는 것"이라는 사실을 이용자들이 쉽게 이해할 것이다.

이렇게 진정한 선택권이 부여된 경우, 이용자의 '동의'는 해당 조항을 계약 내용에 '추가로' (이미 계약 내용의 일부로 편입된 약관 조항에 더하여) 편입하겠다는 유효한 합의로서의 효력을 가질 것이다.

현재의 실상은, 동의를 거부할 수 있는지 없는지 구분하지 아니하고 이용자에게 모조리 동의를 표시하도록 사업자들이 요청하고 있다(그리고 이렇게 하도록 사업자들이 제도적으로 강제 당하고 있다). 해당 서비스 이용계약을 체결하고자 희망하는 이용자는 자신의 과거 경험에 비추어 보아, 동의를 하지 않으면 서비스 이용 계약 체결 자체가 불가능하다고 인식하고(이 인식이 틀리지도 않으므로) 사업자가 제시하는 동의 요청 항목 어느 것도 제대로 읽어보지 않고 '모조리' 동의를 표시하도록 '유도'되는 실정이다. 말이 '체크박스' 일뿐, 체크하지 않으면 안

되는 박스라는 인식이 자리하고 있기 때문에 그 내용을 읽어볼 이유조차 없는 것이다. 이런 상황을 초래해 놓고, 그 실상을 외면한 채로 “동의를 받게 했으므로 개인정보 보호가 잘 될 것이다”라는 환상에 머무르는 것은 규제자로서의 책임을 방치하는 것이다. 정보 주체의 ‘동의’를 받게 하면 개인정보 보호가 잘 될 것이라는 환상에서 벗어나는 것이야말로 개인정보 보호를 위한 첫걸음이 될 것이다.

# 클라우드 서비스와 개인정보보호

고려대학교 법학전문대학원 교수 김기창

## Ⅰ. 클라우드 서비스의 의미 및 유형

클라우드 컴퓨팅 기술은 (1)가상화(Virtualization) 기술과 (2)그리드 컴퓨팅(Grid computing) 기술, 그리고 (3)고속 데이터 전송을 가능하게 하는 네트워크 기반 구조를 사용하여 지리적, 물리적으로 분산되어 존재하는 컴퓨팅 자원을 마치 자신의 물리적 지배하에 놓여 있는 컴퓨팅 자원처럼 이용할 수 있도록 하는 기술을 의미한다[6]. 사업자건 최종 고객이건 하드웨어를 구입하거나 임대하여 컴퓨팅 자원을 자체적으로 확보하고 이것으로 작업을 수행하는 것이 종래의 모습이었다면, 클라우드 컴퓨팅 기술은 사업자나 최종 고객이 하드웨어를 확보할 필요가 없이 클라우드 서비스 제공자로부터 컴퓨팅 자원을 서비스로서 공급받아 이용할 수 있도록 하는 것이다[7].

클라우드 서비스는 흔히 세가지 유형으로 분류하여 설명되고 있다. 첫째, SaaS (Software as a Service)은 서비스 이용자가 자신의 PC에 소프트웨어를 설치할 필요 없이, 네트워크에 연결된 모든 디바이스에서 해당 소프트웨어를 서비스로서 공급받아 사용할 수 있게 해주는 것을 말한다. 예를 들어, 종래 이메일을 처리하는 소프트웨어(아웃룩, 유도라 등)는 유저가 자신의 컴퓨터에 설치하여 구동해야 했다. 그러나 클라우드 서비스 제공자가 이메일 처리 소프트웨어를 서버에서 구동하고 유저는 웹브라우저를 통하여 메일을 송신, 수신, 저장, 검색할 수 있게 되는 '웹메일'은 SaaS의 대표적인 사례이다. 둘째, PaaS (Platform as a service)는 클라우드를 통해 표준화된 개발 플랫폼을 제공하는 서비스이다. 2008년에 구글이 제공하기 시작한 Google App Engine 이 PaaS 의 일례가 된다[8]. 셋째, IaaS (Infrastructure as a service)는 서버, 스토리지, 네트워크와 같은 인프라 스트럭쳐를 클라우드 서비스의 형태로 제공하는 것이다. 이런 서비스를 HaaS (Hardware as a service)라고도 부른다. 서비스 이용자(전산자원이 필요한 사업자)는 자신이 필요로 하는 전산 자원 일체를 클라우드 서비스 제공자로부터 서비스로서 구매하여 공급받을 수 있다[9]. 이렇게 확보된 전산자원(서버)으로 자신의 서비스를 구성하고 자신이 이를 관리하며, 수요의 증감에 따라 전산 자원의 논리적인 확장 또는 감축이 가능하다. 아마존의 EC2(Elastic Compute Cloud), S3(Simple Storage Service), AWS(Amazon Web service), IBM의 Blue Cloud project 등이 대표적인 사례이다.

## Ⅱ. '서비스' 클라우드와 '개인용' 클라우드

그러나 이 글의 논지전개에 더 큰 의미를 가지는 구분은, 최종 유저를 상대로 제공되는 '개인용 클라우드' 서비스와, 서비스 제공자를 상대로 제공되는 '서비스 클라우드' 간의 구분이다.

---

6) M.D. Dikaiakos et al., 'Cloud Computing: Distributed Internet Computing for IT and Scientific Research', Internet Computing, IEEE 13, no. 5 (2009): 10; M. Cafaro and G. Aloisio, 'Grids, Clouds, and Virtualization', Grids, Clouds and Virtualization (2011): 10 - 12.

7) "Cloud computing is a style of computing where massively scalable IT-related capabilities are provided "as a service" across the Internet to multiple external customers " Cafaro and Aloisio, op. cit., 7.

8) T.F. Cotter, 'Pragmatism, Economics, and the Droit Moral', NCL Rev 76 (1997): 627.

9) Lizhe Wang et al., 'Cloud Computing: a Perspective Study', New Generation Computing 28, no. 2 (June 3, 2010): 139.

## 1. 서비스 클라우드

아마존은 무수히 많은 컴퓨터들로 구성된 데이터 센터를 여러 곳에 운영하면서, 그리드 컴퓨팅 기술을 이용하여 이들을 하나의 컴퓨팅 자원으로 취합(pooling) 함과 동시에, 가상화 기술을 사용하여 몇 십만명의 고객(서비스 제공자)들에게 각자 고유한 가상 하드웨어(Virtual machine)를 제공한다. 서비스 계약(Service Level Agreement)의 종류 및 가격대에 따라 고객에게 제공되는 가상 하드웨어의 처리 용량이나 사양(CPU 속도, RAM 크기 등), 네트워크 대역폭 등이 물론 다르다. 어느 데이터 센터에 위치한 어느 물리적 하드웨어가 데이터를 실제로 저장하고 있는지를 파악하는 것은 기술적으로 어려울 뿐 아니라 별 의미도 없다. 하드웨어와 소프트웨어 간에 논리적, 추상적 단계(hardware abstraction layer)가 개입되어 있고, 하드웨어 자원은 이 추상적 단계를 거쳐 소프트웨어와 연결되기 때문이다.

Netflix, Pinterest, Foursquare, Ericsson 등 세계 유수의 무수한 기업들은 아마존 EC2 로 알려진 서비스 클라우드를 사용하여 자신의 서비스를 제공하고 있다. 서비스 제공자가 HaaS 형태의 클라우드 서비스를 이용하여 자신의 서비스를 제공할 경우, 서버를 구성하는 하드웨어의 물리적 관리와 운영(전기 공급, 온도, 습도 관리, 접근 통제, 하드웨어 관리 등)은 클라우드 제공자가 전적으로 수행하는 반면, 서버에 응용프로그램을 설치하고 소프트웨어의 보안을 확보하고 보안 패치를 업데이트하는 일 등은 해당 사이트 운영자(서비스 클라우드 이용자)가 마치 자신의 하드웨어를 이용하여 웹사이트를 운영하는 경우처럼 자기 스스로 전적으로 관리하게 된다. 요컨대, 서비스 클라우드 제공자(예를 들어, 아마존)는 사업자들이 필요로 하는 전산 자원을 '서비스로서' 제공하고, 서비스 클라우드 이용자(예를 들어, 에릭슨)는 이렇게 확보된 전산 자원으로 자신의 고객들에게 각 해당 서비스를 제공한다.

## 2. 개인용 클라우드

이와는 달리, 최종 이용자가 자신의 문서, 사진, 동영상, 음악, 프로그램 파일, 사적 데이터 등 모든 형태의 정보를 자신이 가입한 '개인용 클라우드' 서비스의 계정에 업로드하여 저장하고 이렇게 저장된  파일을 해당 클라우드 계정과 동기화된 스마트폰, 태블렛PC 등 자신의 다른 디바이스에서도 접근, 이용하거나 다운로드 받을 수 있도록 하는 서비스가 매우 빠르게 성장하고 있는데, 이것을 '개인용 클라우드'라고 부른다[10]. 구글 독스(Google Docs)는 개인용 클라우드를 활용한 문서작성, 저장, 편집 서비스의 대표적 사례 중 하나이다. 최근의 진보된 클라우드 서비스에서는 업로드된 미디어 파일(음악, 영상, 사진 등)을 다운로드할 필요 없이 스트리밍 형태로 재생할 수 있도록 서비스를 제공하기도 한다. 요컨대, 개인용 클라우드는 이용자에게 소프트웨어를 서비스로 제공(SaaS)함과 동시에(Office Web Apps, Google docs 등), 저장 공간을 제공하며, 개인용 미디어 스트림 서버로서도 기능하는 것이다. 현재 널리 이용되는 N드라이브, 다음 클라우드, iCloud, Ubuntu One,  Amazon Cloud Drive, 구글의 뮤직베타등 개인용 클라우드 서비스들은 모두 그러하다.

물론 '개인용 클라우드' 서비스를 자신의 고객들에게 제공하려는 사업자는 그러한 서비스에 필요한 전산 자원(하드웨어/소프트웨어)을 구입, 임대하는 대신, '서비스 클라우드' 제공자와 이용계약을 체결하고 서비스로서(IaaS) 전산자원을 확보하여 자신의 고객에게 개인용 클

10) '개인용(personal)' 클라우드라는 표현은 '최종이용자를 상대로 제공되는 클라우드 서비스'라는 뜻이고, 자연인은 물론 회사나 기업 등도 이용약관에 따라 최종이용자로 이러한 '개인용' 클라우드 서비스를 사용할 수 있을 것이다.

라우드 서비스를 제공할 수도 있다. 예를 들어, 드롭박스(Dropbox)는 파일 저장 설비를 서비스의 형태로 유저들에게 제공하는 개인용 클라우드 서비스 사업자이다. 그러나 데이터를 저장하는데 실제로 필요한 물리적 설비를 드롭박스가 구입, 임대, 운용하는 것은 아니다. 서비스 클라우드 제공자인 아마존과 드롭박스가 계약을 체결하고 아마존으로부터 "서비스로서" 공급받는 가상의 하드웨어 자원(Amazon's Simple Storage Service)을 이용하여 드롭박스는 자신의 이용고객들에게 개인용 클라우드 서비스를 제공하고, 고객은 이렇게 마련된 자신의 계정(저장 공간)에 자기의 사적 데이터를 저장한다[11].

이하에서는 개인정보 보호와 관련된 주요한 논점들을 (1)최종 유저를 상대로한 개인용 클라우드 서비스와 (2)사업자를 상대로 한 서비스 클라우드로 나누어 살펴본다.

## Ⅲ. 私的정보와 개인정보의 차이

'私的정보'는 그 내용과는 무관하게 특정 개인/법인/단체의 지배 하에 있어 공중의 자유로운 열람이나 이용이 허용되지 않는 일체의 정보를 뜻한다. 유체물에 대한 지배와는 달리 정보에 대한 지배는 '인식' 여부에 따라 좌우되는 측면이 있으므로, 공중이 이미 알고 있는 정보라면 이를 어느 특정인이 '지배'하는 것이라고 할 수는 없을 것이다. 그러나 자신이 인식하는 정보라고 해서 자신이 자유로이 이용하거나 공표할 수 있는 것은 아니다. 예를 들어 비밀을 유지할 것을 조건으로 제공된 정보를 전달 받은 자가 그 정보를 함부로 공표하거나 제공자의 의사에 반하여 이용하는 것은 허용되지 않을 것이다.

반면에 '개인정보'는 해당 개인을 특정할 수 있는 정보를 말하며, 그 정보가 누구의 지배하에 있는지와는 무관하다. 개인정보 보호법 제2조 제1호는 개인정보를 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보(당해 정보만으로는 특정 개인을 식별할 수 없다 하더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)"라고 정의한다. 정보의 내용이 이러하다면, 그 정보가 누구의 지배하에 있건 이를 개인정보로 본다는 것이다.

따라서, 개인정보와 사적정보는 다르다. 예를 들어, 개인의 이름, 전화번호는 개인정보임이 분명하지만, 이러한 정보를 수록한 전화번호부를 사적정보라고 여길 수는 없다[12]. 개인에 '관한' 정보나 개인이 지배하는 정보(개인의 사적정보)는 위에 정의된 개인정보와는 구분되어야 할 것이다. 어느 개인의 행적에 대한 서술이나 그자에 대한 평가를 담은 評傳은 개인에 관한 정보임이 분명하지만, 이것을 개인정보라고 하기는 어려울 것이다. 어떤 자가 자신의 가계 지출과 수입을 정리해 둔 문서라던가, 습작으로 작성하여 발표하지 아니한 시, 수필이나 일기 등은 그 개인이 지배하는, 그 개인의 私的 정보임은 분명하지만, 이것을 모두 '개인정보'라고 하기는 어려울 것이다. 개인정보를 대단히 포괄적으로 파악하여 "개인의 정신, 신체, 자산, 사회적 지위, 신분 등에 관한 사실, 판단, 평가를 나타내는 개인에 관한 정보 및 당해 정보에 포함되어 있는 성명, 주민등록번호 등의 사항에 의하여 개인을 식별할 수 있는 정보의 총체"라고 하는 논자도 있긴 하나[13] 이렇게 넓게 개인정보의 개념을 규정하려 시도할 경우 과연 무슨 도움이 될지는 의문이다. '개인에 관한 정보'가 모두 개인정보는 아니라고 하는 것이 옳을 것이다.

---

11) https://www.dropbox.com/help/7/en

12) David L. Baumer, Julia B. Earp, and J.C. Poindexter, 'Internet Privacy Law: a Comparison Between the United States and the European Union', Computers & Security 23, no. 5 (July 2004): 403.

13) 이관기, "알권리와 프라이버시권의 관계에 관한 연구", 한양대학교 박사학위논문, 1999년, 99면.

# Ⅳ. 개인정보 보호에 관한 국내 법제

2011년 9월30일부터 시행된 개인정보 보호법(“개인정보법”)은 개인정보의 수집, 처리 및 보호에 대한 기본적 사항들을 종합적으로 규율하고 있다. 한편 정보통신서비스 제공자가 개인정보를 수집, 처리하는 경우에는 정통망법이 우선적으로 적용되며, 개인정보법은 정통망법이 규정하지 아니하는 사안에 대하여 보충적으로 적용된다. 개인정보 중 개인의 신용도와 신용거래능력을 판단하는데 필요한 정보(개인신용정보)에 대하여는 신용정보의 이용 및 보호에 관한 법률(“신용정보법”)이 우선적으로 적용될 것이며, 개인정보법은 보충적으로 적용된다(개인정보법 제6조). 개인의 위치정보에 대하여는 위치정보의 보호 및 이용 등에 관한 법률(“위치정보법”)이 규율한다.

클라우드 서비스와 관련하여 다음과 같은 논점들을 검토할 필요가 있다.

## 1. 개인정보에 대한 안전조치의무

서비스 제공자가 최종 유저로부터 유저의 이름, 주소, 이메일, 연령, 성별 등에 관한 정보를 수집한다면 이러한 정보가 ‘개인정보’에 해당하고, 이런 정보에 대하여 개인정보 처리에 관련된 규정들이 적용됨은 의문이 없다. 그러나 개인용 클라우드 서비스는 이용 고객의 私的 데이터(고객이 제작 또는 보유하게 된 업무용 문서 파일, 사진, 동영상 등)를 수령하여 저장하는 것 자체를 서비스의 핵심 내용으로 하고 있다. 고객의 이러한 사적 데이터는 이 법이 말하는 ‘개인정보’라고 할 수는 없을 것이다. 설사 그런 사적 데이터 중에 고객 자신이나 다른 사람의 이름, 주민등록번호, 질병 이력, 신용정보 등 개인정보가 수록되어 있다 하더라도(예를 들어, 어느 유저가 자신이 근무하는 회사의 인사 기록을 담은 파일을 개인용 클라우드에 저장하는 경우), 이것에 대하여 개인정보 보호법을 적용할 수는 없을 것이다. 왜냐하면 고객이 자신의 개인용 클라우드 계정에 저장하는 사적 데이터에 이런 내용이 포함되어 있는지를 클라우드 서비스 제공자가 가려낼 수도 없고 그것을 가려내려면 고객이 업로드하여 저장하는 고객의 모든 데이터를 클라우드 제공자가 일일이 열람하고 판단해야 한다는 말이 되는데, 이렇게 할 의무를 클라우드 서비스 제공자에게 지울 수는 없기 때문이다. 여러 사람이 열람할 수 있는 웹사이트 게시판에 유저가 게시물을 게시, 공표하는 상황이라면, 웹사이트 운영자도 물론 그 내용을 당연히 열람할 수 있겠지만, 개인용 클라우드 계정에 유저가 저장하는 유저의 사적 데이터는 이와는 근본적인 차이가 있다.

정통망법이나 개인정보법에 규정된 ‘개인정보’에 관한 여러 조항들은 정보의 내용이나 성격만을 판단하여 그것이 개인정보에 해당한다고 해서 언제나 적용될 수 있는 것이 아니다. 최종 유저가 자신의 개인용 클라우드 계정에 저장하는 데이터는 ‘私的정보’일 뿐, 이를 모두 ‘개인정보’라고 할 수는 없고, 그러한 私的정보 중 과연 어느 것이 개인정보인지를 클라우드 서비스 사업자가 가려낼 수도 없다. 따라서 유저가 저장해 둔 이러한 사적 데이터에 대하여 개인용 클라우드 사업자가 정통망법 제28조에 규정된 개인정보 보호조치 의무나, 개인정보법 제3조 제7항에 규정된 익명처리 의무를 지거나 개인정보법 제29조에 규정된 안전조치의무를 지는 것은 아니다.

유저가 자신이나 타인의 모습이 담긴 사진이나 동영상 파일을 개인용 클라우드 계정에 저장하는 경우도 위와 같은 이유로 ‘개인정보’에 관한 법령이 규정하는 각종 조치를 취해야 할 의무가 있고 볼 여지는 없다. 자신의 사적 데이터를 저장하는 공간에 유저가 임의로 저장하는 사진, 동영상 등의 데이터에 대하여 개인용 클라우드 사업자가 정통망법이나 개인정보법 상의

개인정보에 관한 각종 조치를 취해야 할 의무를 부담하는 것은 아니다.

이용자가 저장해둔 사진이나 동영상이 유출되거나 이용자의 동의 없이 제3자에게 제공되거나 공개될 경우 개인용 클라우드 서비스 이용계약 위반 여부가 문제로 되는 것은 당연하다. 그러나 그에 더하여 이것을 개인정보 유출이나 개인정보의 제3자 제공 문제로 파악할 수 있을까? 유저가 저장 해둔 정보 중, 개인을 식별하는데 사용될 수 있는 사진, 동영상, 인사 기록 파일 등의 정보를 사업자가 그 내용을 알면서 고의로 유출하거나 제3자에게 제공한 경우라면 이용 계약 위반은 물론이며, 개인정보 보호법 위반의 문제로도 될 것으로 생각한다. 고의로 이러한 정보를 유출시키거나 제3자에게 제공할 경우에는 적어도 행위 시점에 행위자는 자신이 유출, 제공하는 정보가 개인을 특정, 식별하는데 사용될 수 있는 정보라는 점을 인식하고 행위하는 것이기 때문이다. 반면에 개인용 클라우드 사업자가 해킹 공격을 당하여 유저들이 저장해둔 유저의 私的 데이터가 유출된 경우라면 비록 그 속에 개인정보에 해당하는 데이터가 포함되어 있었다 하더라도, 유저와 사업자 간의 서비스 이용 계약 위반이 문제될 여지는 있지만 개인정보의 보호와 관련된 법령 위반의 문제가 제기될 여지는 없을 것이다(유저의 계정 정보 자체는 침입되지 않았다고 전제할 때).

반면에, 회원 가입 정보의 일부로서 유저의 사진을 사업자가 수집, 보관한다면 이것은 정통망법이나 개인정보 보호법이 말하는 '개인정보'에 해당한다. 동일한 사진이더라도 어떤 맥락과 이유에서 제공되는지에 따라 그 법적 평가가 달라지는 것이다. 회원 가입 정보의 일부로서 수집한 고객과 관련된 일체의 정보(회원 계정 정보)는 개인정보임이 분명하므로 개인용 클라우드 사업자는 정통망법이나 개인정보 보호법의 규정에 따라 이 정보를 처리, 보호하여야 한다. 이점은 개인용 클라우드 사업자건 다른 여느 사업자건 차이가 없다.

## 2. 개인정보의 제3자 제공

개인정보법 제17조-제19조는 사업자가 고객의 개인정보를 제3자에게 제공하는 문제를 규율한다. 전산 자원을 서비스 클라우드 제공자로부터 (IaaS 형태로) 확보하고 사업을 펼치는 사업자는 자신의 모든 정보(고객의 개인정보까지 포함)를 클라우드 제공자가 운영하는 저장설비(데이터 센터)에 저장하게 될 것이다. 이것을 두고 개인정보를 제3자에게 '제공'하는 것이라고 할 수 있을까? 정보가 물리적으로 제3자의 지배하에 있는 저장 설비에 저장되면, 그 제3자는 적어도 '기술적'으로는 그 정보에 접근할 수 있게 된다. 그러나, 사업자와 서비스 클라우드 제공자 간의 계약 조항에 기하여 서비스 클라우드 제공자가 그 정보에 접근하는 것을 금하고 있다면, 이를 제3자에게 제공하는 것이라고 할 수 있을지는 선뜻 판단하기가 쉽지 않다. 정보를 제3자에게 '제공'한다는 의미는 그렇게 제공받은 정보를 제3자가 적어도 일정한 용도로는 사용할 수 있도록 제공한다는 것인데, 서비스 클라우드 제공자는 클라우드 이용자가 저장하는 정보를 사용할 수 없다는 내용이 서비스 수준 계약(Service Level Agreement)에 명시되어 있다면 비록 정보가 물리적으로 저장되는 저장설비 자체가 서비스 클라우드 제공자가 지배하는 데이터센터라고 하더라도 이를 "제3자 제공"이라고 파악하기는 어려울 것이다.

## 3. 개인정보의 국외 이전

한편, 정보의 '이전'과 정보의 '제공'은 그 의미가 다르다고 볼 여지가 없지 않다. 정보의 '이전'은 이전받는자가 그 정보를 사용할 수 있는지 여부와는 무관한 개념이라고도 할 수 있다. 이전 받는 자가 그 정보를 사용할 수 있는지 여부와는 무관하게 정보가 '이전'되기는 하였다고

볼 수 있기 때문이다. 국내법의 적용을 받는 국내 사업자가 외국에 데이터 센터를 건립, 운영하는 경우이거나, 외국에 데이터 센터를 운영하는 서비스 클라우드 제공자로부터 전산 자원을 확보하여 사업을 펼치는 국내 사업자의 경우 개인정보가 '제3자에게 제공'되는 것은 아니지만, '국외로 이전'되는 것은 분명하다고 생각한다.

정통망법 제63조 제2항은 "개인정보를 국외로 이전하려면 이용자의 동의를 받아야 한다"고 규정하고 있다. 그러나 이 조항이 과연 서비스 클라우드를 이용하여 전산 자원을 확보하고 사업을 펼치는 경우에도 적용되는지는 의문이 없지 않다. 제63조 제3항은 이용자의 동의를 구함에 있어서 고지되어야 할 사항을 열거하고 있는데, 거기에는 "개인정보를 이전받는 자의 개인정보 이용목적 및 보유, 이용 기간"을 고지하도록 되어 있다. 요컨대, 이 조항은 개인정보를 이전받는 자(국외에 위치한 자)가 그 정보를 이용할 수 있도록 이전받은 상황을 당연한 것으로 전제하고 있다. 그러나 서비스 클라우드 제공자는 그의 고객(서비스 클라우드를 이용하여 사업을 펼치는 사업자)이 저장하는 개인정보를 애초에 이용할 수가 없다는 점을 감안한다면, 외국에 위치한 데이터 센터에 개인정보가 저장된다는 이유만으로 정통망법 제63조가 언제나 적용된다고 보기는 어렵다. 정통법 제63조에서 말하는 "개인정보를 국외로 이전"하는 경우란, 국외에 위치한 제3자가 개인정보를 이용할 수 있도록 제공하는 경우라고 보아야 한다. 즉, 이 조항은 개인정보의 제3자 제공 중, 그 수령자가 국외에 위치한 자일 경우에 적용되는 조항이라고 생각한다. 서비스 클라우드 제공자가 (여러 나라에 분산되어) 운용하는 데이터 센터에 개인정보가 저장되는 경우는 애초에 제3자 제공이라고 볼 수조차 없으므로(비록 개인정보의 '국외 이전'임을 부인할 수는 없지만), 정통망법 제63조가 아예 적용될 여지가 없다고 생각한다. 그러나, 이점은 향후 해당 규정을 개정하여 입법적으로 명확히 할 필요가 분명히 있다.

한편, 개인정보법 제17조 제3항은 다음과 같이 조금 다르게 규정되어 있다:

개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

이 조항을 보면, 개인정보를 국외의 제3자에게 '제공'하는 경우에는 정보주체의 동의가 필요하다는 점이 분명하지만, 개인정보의 '국외 이전'의 경우에는 언제나 동의가 필요한 것이 아니다. 물론, '국외 이전' 중에는 국외의 제3자가 그 정보를 이용할 수 있도록 '제공'하는 경우도 있고, 국외의 제3자가 이용할 수는 없지만 정보가 국외로 이전되는 경우도 있다. 전자의 경우(국외의 제3자에게 정보가 제공되는 경우)에는 정보 주체의 동의가 필요할 뿐 아니라, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약이 체결되어서는 안된다는 요건이 모두 적용되는 반면, 후자의 경우(제3자 제공은 아니고 단순히 정보가 국외로 이전되는데 불과할 경우)에는 정보 주체의 동의가 필요한 것은 아니고, "이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다"는 요건만이 적용될 것이다.

"이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다"는 요건을 준수하려면, 사업자는 서비스 클라우드 제공자(데이터 센터 운영자) 와 체결하는 서비스 수준 계약이 개인정보 보호법에 규정된 사업자(서비스 클라우드 이용자)의 의무를 완수하는데 장애가 되지 않는지를 점검할 필요가 있게 된다. 이점을 구체적으로 살펴본다.

개인정보법 제24조 제3항은 이용 고객의 고유식별정보(주민등록번호, 여권번호, 운전면허번호, 외국인등록번호)를 사업자가 수집, 처리할 경우, 암호화 등 안전성 확보에 필요한 조치를 하도록 규정하고 있고, 제29조는 개인정보의 안전한 보호에 필요한 기술적, 관리적 및 물

리적 조치를 하도록 규정하고 있다. 2011년9월30일 행정안전부 장관이 고시한 “개인정보의 안전성 확보조치 기준”은 이러한 의무를 구체화한 것인데, 개인정보처리자의 접속권한 통제, 개인정보의 암호화 기준, 개인정보 처리에 관련된 접속기록의 보관, 보안프로그램 설치, 운영 그리고 물리적 접근 통제 등의 조치가 이루어져야 한다는 내용을 담고 있다[14].

저장설비, CPU, 접속 대역 등 인프라스트럭쳐 자체를 국외의 클라우드 서비스 제공자로부터 서비스로서(IaaS) 구매하여 확보하고 사업을 수행하는 국내 사업자의 경우에도 개인정보 보호에 관한 법령이나 고시가 요구하는 조치의 대부분은 국내 사업자 스스로가 수행할 수 있고, 수행해야 하는 내용이다. 예를 들어 고유식별정보의 암호화를 어떤 알고리즘으로 어떻게 할지는 전적으로 사업자 자신이 결정하고 실행해야 한다. 또한 개인정보처리 시스템에 대한 접속 기록의 안전한 보관이나 위, 변조 방지에 필요한 조치 역시 서비스 클라우드 제공자가 수행해야 하는 것이 아니라 그런 클라우드 서비스를 이용하여 사업을 펴는 국내 사업자가 수행해야 할 문제이다. 사업자는 자신의 고객과 관련된 개인 정보를 별도의 서버에(물리적으로 별개의 서버이건, 가상화를 통하여 확보되는 별개의 서버건 간에) 보관하고, 이 서버에 대한 접근을 통제하고 접근 기록(log)을 분산 저장하는 등의 조치를 취함으로써 접근 기록 위, 변조에 대처할 수 있게 된다.

하지만, 전산실 등에 대한 ‘물리적 출입 통제 절차’를 수립, 운영하는 문제는 국내의 사업자가 직접 수행할 수 있는 것이 아니라, 서비스 클라우드 제공자가 이행해야 하는 부분이다. 이 부분에 대하여 국내의 사업자가 행할 수 있고, 행해야 하는 조치는 외국의 서비스 클라우드 제공자와 자신이 체결하는 서비스 수준 계약(Service Level Agreement; 서비스 수준협약서) 조항에 클라우드 제공자가 자신의 데이터 센터에 대하여 적절한 수준의 물리적 출입 통제 절차를 도입하고 실행하도록 하는 내용의 계약상 의무를 규정하는 방식으로 이를 확보하는 것이다.

행정안전부 장관이 고시한 “개인정보의 안전성 확보조치 기준” 부칙 제3조는 “개인정보처리자가 전산센터 클라우드컴퓨팅센터 등에 계약을 통해 하드웨어 소프트웨어 등을 임차 또는 임대하여 개인정보를 처리하는 경우에는 계약서 또는 서비스수준협약서에 이 기준에 준하는 수준의 안전조치 내용이 포함되어 있으면 이 기준을 이행한 것으로 본다 ”고 규정하고 있다. 여기서 말하는 ‘안전조치’는 클라우드 제공자가 수행하는 물리적 출입 통제와 관련된 안전조치를 포함하는 것임은 물론이다. 그리고 데이터 센터 전체에 대한 낮은 수준의 네트워크 방화벽 설비 등도 여기에 포함될 여지가 있다. 사업자가 수집, 보관하는 개인정보에 대한 암호화나 개인정보처리 시스템 계정에 대한 접속 권한 통제 등 소프트웨어적 조치는 클라우드 제공자가 하는 것이 아니라 그를 이용하여 사업을 펴는 사업자가 스스로 구현해야 하는 것이지만, 클라우드 제공자가 담당해야 할 소프트웨어적 조치가 전혀 없지는 않고, 이러한 내용을 서비스 수준 협약으로 확보하는 일이 언제나 용이한 것은 아니다(당사자 간의 협상력의 차이 등).

따라서 국외에 위치한 데이터 센터를 이용하는 문제는 개인정보 보호와 관련하여 적지 않은 어려움이 있다. 유럽 연합의 개인정보 보호에 관한 입법지침 또한 개인정보의 역외 이전에 대하여 적지 않은 어려움을 야기하고 있으며 이런 이유로 유럽의 업체들이 미국에 위치한 클라우드 사업자를 이용하기를 꺼리는 문제가 발생하기도 한다. 이 문제를 해결하고자 미국 상무부는 데이터 안전지대 프로그램(Data Safe Harbor Program)을 시행하고 있다. 유럽연

14) ‘개인정보의 안전성 확보조치 기준 고시 및 해설서’
http://www.mopas.go.kr/gpms/ns/mogaha/user/userlayout/bulletin/userBtView.action?userBtBean.bbsSeq=1039198&userBtBean.ctxCd=1037&userBtBean.ctxType=21010005.

합 입법지침이 요구하는 “적정한 수준의 정보 보호 조치(adequate level of protection)” 요건을 준수하는 클라우드 사업자들은 이 프로그램에 등록하여 자신이 제공하는 서비스가 그런 요건을 충족한다는 점을 서약하도록 하는 것이다. 이런 업체들을 이용하여 전산 자원을 확보하고 사업하는 유럽 연합의 사업자(클라우드 이용자)들은 개인정보 보호 의무 준수가 한층 용이해 질 것이다[15].

## 4. 개인정보 취급, 처리 업무 위탁

정통망법 제25조는 제3자에게 “개인정보를 수집·보관·처리·이용·제공·관리·파기 등”을 할 수 있도록 업무를 위탁하는 경우에 사업자가 준수해야 할 사항을 정하고 있다. 개인정보법 제26조 역시 “개인정보의 처리 업무”를 제3자에게 위탁하는 경우에 준수되어야 할 사항을 정하고 있다. 개인정보법 제2조는 개인정보의 ‘처리’를 “개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위”라고 정의하고 있다. 서비스 클라우드를 이용하여 사업을 펼치는 자가 그가 수집하는 개인정보를 서비스 클라우드 제공자가 운영하는 데이터 센터에 보관하는 경우에 이를 개인정보 취급, 처리 업무의 위탁이라고 볼 수 있을까? 정통망법과 개인정보법은 개인정보의 “취급”과 “처리”를 매우 포괄적으로 규정하고 있고, ‘저장’, ‘관리’, ‘복구’, ‘파기’ 등도 개인정보의 취급이나 처리 개념에 포함되어 있긴하다. 하지만, 서비스 클라우드를 이용하여 자신의 사업을 펴는 사업자의 경우, 개인정보를 저장, 관리, 복구, 파기하는 주체는 오로지 사업자이지, 서비스 클라우드 제공자가 아니라고 보아야 한다. 데이터 센터를 운영하고, 그를 이용하는 모든 고객의 데이터 전체에 대한 backup 서비스를 제공하는 클라우드 사업자라고 해서 개인정보 취급 수탁을 받은 자라고 해석할 수는 없을 것이다. 클라우드 서비스 사업자는 자신의 고객들(인터넷 서비스 사업자들)이 최종 유저들로부터 수집하여 보관하거나, 폐기하는 개인 정보에 대하여 어떠한 형태로든 개입하는 것이 서비스 수준계약상 허용되지는 않기 때문이다(비록 기술적으로 ‘가능’은 하더라도, 만일 그렇게 한다면 서비스 수준 계약 위반 책임을 져야 할 것이다). 만일 이와 달리 해석한다면, 예를 들어 서버실의 청소를 용역 업체에 맡기는 경우에도 (그 청소 업체가 해당 서버의 하드웨어에 ‘물리적’으로는 접근할 수 있고, 그 하드웨어를 복제하는 것이 ‘기술적’으로는 불가능하지 않으므로) ‘개인정보 처리 업무’를 제3자에게 위탁한 것이라고 해석해야 한다는 터무니 없는 결론에 도달 할 것이다. 청소 업체가 ‘개인정보 처리’ 업무를 위탁받는 것이 아닌것과 마찬가지로, 서비스 클라우드 제공자가 전세계에서 사업을 펼치는 무수한 자신의 고객들(사업자들)의 개인정보 처리 업무를 위탁받는 것은 아니다.

## 5. 사법 목적의 고객정보 제공

사법이나 법 집행 목적상 고객 정보를 수사 기관 등에 제출 하는 문제는 개인용 클라우드의 경우와 서비스 클라우드의 경우를 나누어 생각해야 한다.

### 가. 개인용 클라우드의 경우

사법 당국이 적법한 절차에 따라 수사 목적이나 증거 수집 용도로 자료의 제출을 요구할

15)‘개인정보의 안전성 확보조치 기준 고시 및 해설서’
http://www.mopas.go.kr/gpms/ns/mogaha/user/userlayout/bulletin/userBtView.action?userBtBean.bbsSeq=1039198&userBtBean.ctxCd=1037&userBtBean.ctxType=21010005.

경우 개인용 클라우드 서비스 사업자가 이 요구에 응하여 개인의 사적 데이터(개인정보까지 포함)를 자발적으로 제출해도 무방한지는 좀더 신중한 논의가 필요하다. 우선, 법원의 영장이 있는 경우에는 해당 정보를 제공해야 한다는 점은 아무런 의문이 없다. 누구도 법원 명령을 어길 근거는 없다. 그러나, 수사 기관이나 행정 기관이 법원의 영장도 없이 수사 목적 등을 이유로 사적정보나 개인정보 제출을 요구할 경우에는 적지 않은 어려움이 있다. 개인정보의 경우에는 개인정보법 제18조가 명문의 근거를 제공하고 있으므로("범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우", "법원의 재판업무 수행을 위하여 필요한 경우"에는 "정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는" 해당 정보를 제공할 수 있다), 클라우드 사업자가 유저의 개인정보를 자발적으로 제출할 수 있음이 분명하다(그렇게 해야 할 '의무'는 없지만, 그렇게 하더라도 위법하지는 않다는 뜻). 그러나, 개인정보 외의 사적 정보 전반에 대하여도 클라우드 사업자가 수사기관의 요구만 있으면 영장에 의한 사법 당국의 강제 처분(영장)을 기다리지 않고 자발적으로 이를 제출하더라도 유저와의 서비스 이용 계약상의 책임을 지지는 않는다고 해석해야 할지는 뚜렷하지 않다.

애플 iCloud 서비스의 경우 애플사는 다음과 같은 약관 조항을 통하여 매우 광범한 자료 제출 권한(애플사의 권한)을 확보해 두고 있다:[16]

> 법령, 법적 절차, 소송, 국내 또는 국외의 공공기관이나 정부 기관의 요청에 의하여 애플사는 귀하의 사적 정보를 공개할 필요가 있을 수 있음. 또한 국가 안보, 법 집행, 기타 공공적인 중요성을 감안하여 귀하의 사적 정보의 공개가 필요하거나 적절하다고 우리가 결정할 경우 이를 공개할 수 있음[17].

이렇게 광범한 자료 공개 권한을 사업자에게 일괄 유보하는 내용의 약관 조항이 실제로 그 효력을 전부 인정받을 수 있을지, 아니면 해당 약관의 일부분은 무효로 선언되고 사업자가 이용 고객에 대하여 계약 위반 책임을 지게 될지 아직은 불분명하지만, 사업자가 수사 당국의 적법한 자료 제출 요청에 자발적으로 협력하지 않을 경우 압수, 수색을 당하게 될 가능성이 크고 이럴 경우 여러 현실적, 사업적 불편과 불이익을 감수해야 한다는 점도 고려에 넣는다면 이런 약관의 합리성을 인정해야 한다는 주장도 설득력이 없지는 않다.

정통망법 제24조의2는 이용자의 개인정보를 제3자에게 제공하려면 이용자에게 알리고 동의를 받아야 한다고 규정할 뿐, 수사나 증거 수집 용도로 사법 당국의 적법한 요청이 있을 경우에는 이용자의 동의 없이도 해당 정보를 사법 당국에게 제공할 수 있다는 명문의 규정은 없다. 한편, 정통망법 제44조의6 은 "특정한 이용자에 의한 정보의 게재나 유통으로 사생활 침해 또는 명예훼손 등 권리를 침해당하였다고 주장하는 자"의 신청이 있으면 명예 훼손 분쟁조정부의 결정으로 해당 게시자의 성명, 주소 등 대통령령이 정하는 정보를 신청자에게 제공하도록 규정하고 있고, 정통망법 제64조는 사법당국이 아니라 방송통신위원회가 일정한 경우에 "관계 물품, 서류 등"을 사업자들로 하여금 제출하도록 명할 수 있다고 규정하는데, 여기서 말하는 "관계 물품, 서류 등"은 같은 조 제3항, 제6항, 제9항, 제10항, 제11항 등에서는 "자료

16) Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent', SSRN eLibrary (March 8, 2011): 8, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067&rec=1&srcabs=1924240.
17) 'Apple - Apple Customer Privacy Policy', n.d., http://www.apple.com/privacy/.

등의 제출, 요구, 열람, 검사" 등이라고 표현되는 것으로 보아 정보의 제출까지를 포함하는 것으로 읽힌다. 다만, 방송통신위원회의 이러한 자료 제출 요구 권한은 법 위반 행위 전반에 대한 것은 아니고, 오로지 정통망법에 위반 되는 사항에 대한 조사나, 청소년 보호 시책 마련에 필요한 경우이거나, 청소년 보호업무 수행 여부를 확인하는데 필요하거나, 대형 해킹 사고 등의 발생과 관련하여 방송통신위원회의 역할이 필요한 범위 내에 국한되는 것으로 해석되어야 마땅하다. 만일 "이 법에 위반되는 사항"을 확대 해석하여 불법정보를 유통해서는 안된다는 정통망법 제44조의7에 위반되는 사항에 대하여까지 방송통신위원회가 자료 제출 요구 권한을 가지는 것으로 파악하고 이 제도를 운용한다면, 거의 모든 범죄와 관련된 정보에 대하여 방송통신위원회가 영장도 없이 정보 제출을 요구할 수 있게 되는데, 방송통신위원회는 수사 기관도 아닐 뿐 아니라, 이런 식으로 정통망법을 운용한다면 영장 주의의 근간을 뒤흔들게 될 것이다.

한편, 전기통신사업법 제83조 제3항은 "법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사... 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여" 이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디 등의 제공을 요청하면 전기통신사업자는 "그 요청에 따를 수 있다"고 규정한다. 그러나 최근의 판례는, 이런 규정이 있다고 해서 사업자가 함부로 수사기관의 요청에 응하여 이러한 개인정보를 자발적으로 제공하는 것이 정당화되지는 않는다고 보고있다. 해당 법령에서 수사기관의 요청이 있을 때 "그 요청에 따를 수 있다"고 규정하고, 이용약관에서도 "법령의 규정에 의거하거나 수사 목적으로 법령에 정해진 절차와 방법에 따라 수사기관의 요구가 있는 경우"에는 개인정보를 외부에 공개할 수 있다고 규정하고 있더라도, 그 의미는 전기통신사업자가 수사기관의 요청에 임하여 개인정보 보호의 필요와 수사의 필요를 비교검토하여 수사의 필요가 개인정보 보호의 필요를 능가한다고 평가될 경우에 한하여 그 요청에 자발적으로 응하여 개인정보를 제출할 수 있다는 뜻이라고 법원은 해석하였다. 수사기관이 혐의 내용을 구체적으로 명시하지 않은채, 그저 수사에 필요하다고만 하면서 개인정보 제공을 요청하였을 때, 이런 요청에 응하여 사업자가 이용자의 개인정보를 수사기관에 제공하는 것은 이용자에 대한 불법행위가 된다[18].

## 나. 서비스 클라우드의 경우

범죄 수사나 법집행에 필요한 범위 내에서 수사 기관 등의 적법한 요청에 기하여 고객의 사적 데이터(개인정보)를 제출하도록 요구받는 일차적 대상은 서비스 클라우드 제공자가 아니라, 사업자 자신일 것이다. 사업자가 이러한 요구에 대하여 어떻게 대응할 수 있을지에 대하여는 전 항에 이미 설명한 바와 같다. 하지만, 사업자에 대한 자료 제출 요구와는 별도로(또는 이와 병행하여) 그 사업자가 이용하는 서비스 클라우드 제공자에 대하여 수사 기관 등이 정보 제공을 요청할 경우, 서비스 클라우드 제공자가 이에 응해야 할 의무가 있는지, 또는 이에 자발적으로 응하여 자신의 이용 고객(서비스 클라우드를 이용하여 사업을 펴는 사업자)의 데이터를 제공해도 무방한지는 어려운 문제이다.

예를 들어, 개인용 클라우드 서비스를 제공하는 우분투 원(one.ubuntu.com)은 자신이 필요로 하는 전산 자원을 아마존 S3로부터 서비스 수준 계약을 체결하고 확보하여 사업을 수행하고 있다. 우분투 원을 이용하는 어떤 고객이 아동 학대 포르노 사진들을 자신의 우분투

18) 2012.10.18 선고, 2011나19012 판결.

원 계정에 저장하고 있다고 믿을 상당한 이유가 있을 경우, 수사 기관은 일차적으로 우분투 원에 대하여 해당 자료 일체(그 고객의 개인정보까지 포함)의 제출을 요구할 수 있음은 물론이고, 이때 우분투 원이 압수, 수색 영장을 제시받지 않았음에도 자발적으로 해당 자료를 수사 기관에 제공해도 무방한지에 대하여는 위에서 이미 논의하였다(물론 국제 사법 공조와 관련된 논점은 별도의 논의가 필요하지만). 문제는 아마존을 상대로 수사 기관이 해당 자료의 제출을 요구할 수 있는지이다. 우분투 원의 경우는, 자신의 데이터를 아마존에 저장하기 전에 각 고객에게 고유한 비밀키(그러나 그 비밀키는 고객이 아니라 우분투 원이 생성하여 보관한다)로 해당 고객의 사적 데이터를 암호화한 다음 아마존에 저장하므로, 사법 당국이 아마존 만을 상대로 자료 제출 요구를 하고, 자료를 제출받아 본들 우분투 원의 협력이 없다면 별 소용은 없을 것이다. 그러나, 서비스 클라우드를 이용하여 전산자원을 확보하고 사업을 수행하는 사업자 중에는 우분투 원과는 달리 자신의 데이터를 암호화하지 않은 상태로 서비스 클라우드 제공자가 운영하는 데이터 센터에 보관하는 경우가 많고 이럴 경우 사업자의 협력이 없더라도 서비스 클라우드 제공자가 그 사업자의 데이터에 접근하는 것이 '기술적으로는' 가능하므로 수사 기관의 자료 제출 요구가 서비스 클라우드 제공자를 상대로 행해 질 수 있는 것이다.

이럴 경우, 클라우드 제공자가 자료 제출 전이나 제출 후에 해당 사업자(서비스 클라우드 이용자)에게 그 사실을 고지해야 할 의무가 있는 것도 아니므로, 막상 서비스 제공자는 자신의 고객의 사적 데이터가 수사 기관에 제출되었는지 여부 조차를 알지 못하고, 해당 고객 역시 그런 사정을 전혀 모르게 되는 문제가 있다[19].

이 문제에 대하여는 앞으로 좀더 신중한 논의가 필요하다고 생각한다.

# Ⅴ. 결론 및 제안

클라우드 컴퓨팅 기술은 매우 큰 성장 잠재력을 가지고 있다. 이 기술은 일반 이용자(end user)들과 사업자들 모두에게 지금껏 경험하지 못했던 가능성들을 열어주고 있다. 클라우드 컴퓨팅 기술이 제기하는 여러 측면에 대한 검토는 인반 이용자들이 사용하는 개인용 클라우드 서비스와 사업자들이 이용하는 서비스 클라우드를 나누어 검토할 필요가 있다. 일반 유저들의 경우, 개인용 클라우드 서비스를 이용함으로써 다양한 디바이스에서 언제나 자신의 사적 데이터를 동기화(synchronised)된 상태에서 접근, 이용할 수 있게 되어 일상 생활에서의 이용 경험을 획기적으로 향상시키게 된다. 한편 서비스 클라우드는 무수한 사업자들이 자신의 사업 현황에 최적화된 전산 자원을 매우 신축적, 경제적으로 확보하여 기민하게 전산자원 수요변화에 대처할 수 있도록 해준다. 이러한 장점이 유인으로 작용하여 점점 많은 사적 데이터가 클라우드 서비스 제공자의 물리적 지배 영역하에 놓이게 된다.

그러나 개인정보의 보호와 관련해서는 개인용 클라우드 서비스가 새로운 법적 문제를 제기하는 것은 아니다. 이용자의 私的정보가 클라우드 서비스 제공자의 물리적 통제하에 놓인다고 해서, 유출의 위험이 커진다고 단정할 근거도 없고(오히려 이용자의 PC자체가 노출될 위험이 더 크다고 볼 여지도 있다), 그러한 사적 정보는 개인정보로 볼 수가 없기 때문이다. 물론 개인용 클라우드 이용 고객의 계정 정보(subscriber information)에는 개인정보에 해당 하겠지만, 이런 정보에 대한 보호 의무는 개인용 클라우드 서비스라고 해서 다른 여러 서비스와 달라져야 할 이유가 전혀 없다.

한편, 서비스 클라우드는 개인정보의 제3자 '제공'이나 '취급 위탁'의 문제를 야기하는 것은

19) Walden, 'Accessing Data in the Cloud', 3.

아니라는 점을 분명히 인식할 필요가 있다. 서비스 클라우드 제공자의 역할은 하드웨어 및 전산 인프라스트럭쳐를 '서비스로서 제공'하는 것이 그칠 뿐이고, 서비스 클라우드 이용자(최종 이용자를 상대로 서비스를 제공하는 사업자)가 전적으로 수행하는 개인정보의 수집, 처리, 이용에 개입할 여지가 전혀 없기 때문이다. 물리적으로 해당 개인정보가 서비스 클라우드 제공자의 지배하에 있고, 기술적으로 서비스 클라우드 사업자가 그 정보에 접근하는 것이 가능하다고 해서, 이를 개인정보의 제3자 제공이라고 보거나, 개인정보의 취급 위탁이라고 해석한다면, 아마존과 같은 업체는 전세계 사업자들이 보유하는 개인정보를 모조리 제공받은 제3자라거나 이들 모든 사업체들로부터 개인정보 취급 위탁을 받은 제3자라고 파악해야 할 터인데, 이런 해석은 서비스 클라우드가 운용되는 원리 자체에 대한 몰이해를 노정할 뿐이다.

그러나, 사법목적의 개인정보 제공 요청은 서비스 클라우드와 관련하여 적지 않은 어려운 문제를 불러일으키고 있고, 이점에 대해서는 앞으로 보다 정교한 법제도의 정비와 국제적 사법 공조의 필요가 있다.

# 개인정보 국외이전의 실무적 문제와 개선방향

법무법인 광장 변호사 박광배

## Ⅰ. 서론

경제적·사회적 생활 전반에 걸쳐 세계화가 진행되어 개인정보를 포함한 각종 정보의 이동은 불가피한 현실이 되고 있다. 특히 인터넷은 시·공간의 제약이 없기 때문에 국경의 제한없이 정보의 이동이 가능하여 그 흐름을 가속시키고 있다. 구글이나 애플과 같이 전세계적으로 동일한 플랫폼 하에서 동일한 서비스를 제공하는 글로벌 기업이 점점 늘어나고 있고 이러한 기업들은 글로벌 영업전략 차원에서 국내에서 수집한 개인정보를 국외에 위치한 본사나 계열사 내 전담주체에게 이를 전송하여 처리하려고 한다. 나아가 글로벌한 플랫폼을 통한 서비스를 제공하는 경우까지는 아니라 하더라도 한국을 포함한 세계 여러 지역에 자회사, 현지법인 등의 형태로 글로벌한 영업을 수행하는 외국계 회사들 대부분은 비용을 절감하고 효율적이고 통일적인 자원관리를 위하여 임직원, 고객의 개인정보를 국외에 위치한 본사로 보내어 처리하거나 관련 홈페이지 운영을 따로 본사나 전담 계열사 등에게 맡기는 형태로 업무를 수행하고 있다. 반대로 글로벌한 영업을 수행하는 한국기업이 해외자회사나 해외지점 임직원, 고객의 개인정보를 동일한 차원에서 공유하는 과정에서 개인정보가 국경을 넘나드는 경우도 있다. 예컨대, 한국회사가 해외진출하면서 해외 회사와 제휴하여 고객의 개인정보를 공유하거나, 현지에 자회사를 세우면서 국내 서비스를 포함한 서비스 전반을 아웃소싱하는 경우는 이제 쉽게 볼 수 있는 사례가 되었다. 더구나 글로벌 기업으로 성장한 국내기업들은 앞에서 언급한 구글, 애플과 같은 글로벌 기업과 같이 비용절감이나 통일적인 인사/고객 관리 등의 이유로 전세계적으로 수집한 개인정보를 국내로 들여오거나 혹은 국내에서 수집한 개인정보를 국외로 전송하여 처리하는 경우는 점점 더 많아 질 것이다.

한국법의 입장에서 보면, 한국에 진출한 자회사나 지점의 임직원이나 이들이 수집한 한국내 고객의 개인정보를 글로벌 본사로 옮기는 행위 혹은 국내 회사가 해외로 진출하면서 임직원의 개인정보를 해외 업체에 위탁하여 처리하거나 모든 고객 개인정보를 해외자회사에 이전하여 처리하는 것은 개인정보의 국외이전에 해당하게 될 것이다.

한편, 개인정보의 "국외이전"의 개념을 일반적으로 정의하고 있는 법률은 존재하지 않고, 국외이전을 개인정보의 제3자 제공의 일종으로 규정하거나(개인정보보호법 제17조 제3항), 실무적으로 어떠한 형태로든지 대한민국 국민의 개인정보가 물리적으로 국외로 이동한다면 국외이전에 해당한다고 해석하거나(정보통신망 이용촉진 및 정보보호 등에 관한 법률 제63조 참조), 아예 국외이전에 대한 규정 자체가 존재하지 않는 경우(신용정보의 이용 및 보호에 관한 법률 등) 등 법률에 따라 규율 방식이 상이한 상황이다.

국경이 없다는 인터넷의 특성에 충실하다면 개인정보가 국외로 이전하더라도 원칙적으로 국내에서 발생하는 개인정보의 제3자 제공이나 취급위탁의 경우와 달리 취급할 이유는 없다. 그러나 국가마다 상이한 개인정보 보호수준이나 규율을 감안할 때, 국외이전되는 개인정보에 대해 한국법의 적용만을 엄격하게 강요한다면, 국외이전은 거의 불가능해지게 되고, 이 때문에 개인정보의 원활한 이동이 제한된다면 국외이전을 통해 달성하려는 긍정적인 효과(비용절감, 자원의 효율적, 통일적 관리 등)를 얻을 수 없게 되어 궁극적으로 해당 개인정보의 정보주체에 대한 편익이 제한되는 결과가 초래될 수 있다. 더구나 이러한 결과는 해외에 진출하려는

국내기업의 입장에서는 해외 진출에 커다란 장애요소로 작용할 수 있다. 반면 국외이전을 전혀 규제하지 않는다면, 국민의 개인정보가 국외로 무분별하게 유출되어 범죄에 악용되는 등 심각한 부작용도 예상된다. 이하에서는 개인정보의 국외이전과 관련하여 민간분야에서 자주 문제되는 법적 이슈에 대해 살펴보고 그 개선방향을 실무적 관점에서 접근해 보려고 한다[1].

# Ⅱ. 개인정보의 국외이전에 대한 현행 법제도

## 1. 적용가능한 규범

①개인정보의 국외이전과 관련한 직접적으로 규정을 두고 있는 법령으로는 "개인정보보호법"(제17조 제3항), "정보통신망 이용촉진 및 정보보호 등에 관한 법률"(이하 "정보통신망법" 제63조)이 있고, ②국외이전과 관련한 직접적인 규정을 두고 있지는 않으나, 간접적으로 연관된 법령으로는 "전자금융거래법" 및 그 하부규정인 "전자금융감독규정"(제36조 제1항)이 있으며, ③개인정보와 관련한 법령이지만 국외이전과 관련한 언급이 전혀 없는 경우로는 "신용정보의 이용 및 보호에 관한 법률"(이하 신용정보법"), "금융실명거래 및 비밀 보장에 관한 법률"(이하 "금융실명법") 등이 있다.

## 2. 구체적인 규정내용

### 가. 정보통신망법 및 개인정보보호법의 규정

(1) 정보통신망법은 정보통신서비스 제공자 등이 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결하는 것을 금지하고(제63조 제1항), 이용자의 개인정보를 국외로 이전하려고 하는 경우 이용자에게 일정한 사항을 고지하고 동의를 받아야 한다고 규정하고 있다(제63조 제2항, 제3항). 그리고 이용자의 동의를 얻어 개인정보를 국외로 이전하는 경우 정보통신망법 제63조 제4항 및 동법 시행령 제67조 제1항[2]이 정한 일정한 보호조치를 하여야 한다(제63조 제4항).

(2) 또한 개인정보보호법은 개인정보를 국외의 제3자에게 제공할 때에는 국내 제3자에게 제공하는 경우와 마찬가지로 일정한 사항[3]을 정보주체에게 고지하고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하는 것을 금지하고 있다(제17조 제3항).

---

1) 다만 이용자가 스스로 해외사업자가 해외에서 개설한 사이트에 접속하여 회원가입을 하는 경우와 같이, 해외사업자가 국내 이용자의 개인정보를 직접 수집하는 경우도 개인정보가 물리적으로 국외로 이전하는 경우에 해당되나, 이하에서는 국내에 위치한 사업자가 수집한 개인정보를 그 사업자에 의하여 국외로 이전하는 경우만을 전제로 검토한다.

2) 정보통신망법 제63조 ④ 정보통신서비스 제공자등은 제2항에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.
정보통신망법 시행령 제67조 ① 법 제63조제4항에 따라 개인정보를 국외로 이전하는 경우에 하여야 하는 보호조치는 다음 각 호와 같다.
1. 제15조에 따른 개인정보보호를 위한 기술적·관리적 조치
2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항
3. 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치
② 정보통신서비스 제공자등은 제1항 각 호의 사항을 개인정보를 국외에서 이전받는 자와 미리 협의하고, 이를 계약내용 등에 반영하여야 한다.

3) 개인정보를 제공받는 자/개인정보를 제공받는 자의 개인정보 이용 목적/제공하는 개인정보의 항목/ 개인정보를 제공받는 자의 개인정보 보유 및 이용기간/동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 (개인정보보호법 제17조 제2항)

## 나. 전자금융거래법 및 전자금융감독규정

전자금융거래법상 금융기관과 전자금융업자[4]는 전자금융감독규정의 적용을 받게 되는데, 전자금융감독규정은, 금융기관과 전자금융업자가 (ⅰ)전산실을 신규로 설치, 이전하거나 재해복구센터를 구축하는 경우, (ⅱ)외국금융기관의 전산시설에 대한 해외설치, 이전 및 공동이용을 하는 경우, (ⅲ)전자금융업자 중에서 정보통신망을 이용하여 이용자를 대상으로 신규전자금융업무를 수행하는 경우 등에는 금융감독원장에게 보안성 심의를 요청하여야 한다고 규정하고 있다(제36조 제1항, 전자금융감독규정 시행세칙 제3조 제1항). 아울러 국내에 본점을 둔 금융기관의 전산실 및 재해복구센터는 국내에 설치해야 한다고 규정하고 있다(전자금융감독규정 제11조 제11호).

그런데, 전자금융업자가 외국 본사나 해외계열사에게 전자금융업무와 관련한 개인정보의 처리를 위탁함으로써 실질적으로 해외에 있는 전산실을 이용하게 되는 경우에는 전산실을 해외에 신규로 설치 또는 이전하는 경우에 해당하여 보안성 심의가 필요할 수 있다는 것이 현재 금융감독원의 비공식적인 입장이다.

## 다. 신용정보법의 규정

국외로 이전하는 정보가 상거래와 관련한 정보라면 신용정보법상 신용정보에 해당될 수 있는데(제2조 제1호, 제2호), 신용정보법은 개인신용정보의 국외이전에 대해 별도로 규율하고 있지 않다. 그러므로 개인신용정보의 국외이전의 경우도 개인신용정보의 제3자 제공의 경우와 마찬가지로, 개인신용정보를 제공받는 자 등 일정한 사항을 고지하고 신용정보주체의 동의를 받으면 가능한 것으로 해석될 수 있다(신용정보법 제32조 제1항, 동법 시행령 제28조 제2항[5]). 즉, 신용정보법의 일반법으로써 개인정보보호법이 제정되었고, 개인정보보호법 제6조는 "개인정보에 관하여는 정보통신망법, 신용정보법 등 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다"고 정하고 있는바, 신용정보법에 개인신용정보의 국외이전에 관한 규정이 없는 경우, 개인정보보호법 제6조에 따라 개인정보보호법의 국외 이

---

4) 전자금융거래법 제2조 제4호 "전자금융업자"라 함은 제28조의 규정에 따라 허가를 받거나 등록을 한 자(금융기관을 제외한다)를 말한다. 실무적으로 지마켓, 옥션 등의 사이트를 운영하면서 포인트(선불전자지급수단)을 발행하는 이베이코리아, NHN과 같은 사업자를 비롯하여, 다날, 페이케이트 등과 같은 PG업체 등 인터넷을 기반으로 한 전자결제관련 업무를 수행하는 기업들이 여기에 해당한다.

5) 신용정보법 제32조 ① 신용정보제공·이용자가 대출, 보증에 관한 정보 등 대통령령으로 정하는 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 개인으로부터 다음 각 호의 어느 하나에 해당하는 방식으로 미리 동의를 받아야 한다.
1. 서면
2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다)
3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식
4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보·유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다
5. 그 밖에 대통령령으로 정하는 방식

동법 시행령 제28조 ② 신용정보제공·이용자는 법 제32조제1항에 따라 해당 개인으로부터 동의를 받으려면 다음 각 호의 사항을 미리 알려야 한다. 다만, 동의 방식의 특성상 동의 내용을 전부 표시하거나 알리기 어려운 경우에는 해당 기관의 인터넷 홈페이지 주소나 사업장 전화번호 등 동의 내용을 확인할 수 있는 방법을 안내하고 동의를 받을 수 있다
1. 개인신용정보를 제공받는 자
2. 개인신용정보를 제공받는 자의 이용 목적
3. 제공하는 개인신용정보의 내용
4. 개인신용정보를 제공받는 자(신용조회회사 및 신용정보집중기관은 제외한다)의 정보 보유 기간 및 이용 기간

전에 관한 규정(제17조 제3항)이 보충적으로 적용된다고 보는 것이 타당할 것이다[6].

### 라. 금융실명법의 태도

금융실명법은 "금융회사 등에 종사하는 자는 명의인의 서면상의 요구나 동의를 받지 아니하고는 그 금융거래의 내용에 대한 정보 또는 자료(이하 "거래정보 등"이라 한다)를 타인에게 제공하거나 누설하여서는 아니 되며, 누구든지 금융회사 등에 종사하는 자에게 거래정보 등의 제공을 요구하여서는 아니 된다"(제4조 제1항)라고 규정하고, 일정한 경우에는 명의인의 요구나 동의를 받지 않고서도 거래정보 등을 타인에게 제공할 수 있다고 규정(동 조항 단서 각 호)하고 있을 뿐 별도로 국외이전에 대한 규정을 두고 있지 않다[7]. 만일 '금융회사 등'에서 고객의 거래정보 등을 국외의 제3자에게 이전한다면 위 제4조 제1항의 규정에 따라 명의인으로부터 서면상의 요구나 동의가 필요하다는 결론이 된다.

### 마. 해외 입법례

아래에서 보는 바와 같이 현재 개인정보의 국외이전에 대해서는 국제적으로 통일적인 규제는 존재하지 아니하며, 국가별로 입법태도는 다양하다.

#### (1)미국

미국의 경우, 공공부문과 민간부문을 아우르는 종합적인 입법 방식을 채택하지 않고, 민간부문에 있어서는 개별적인 단행법에 의하여 개인정보를 보호하는 접근방법을 채택하고 있다. 이와같이 개별적인 영역이나 개별 주(州)마다 개인정보에 대하여 각각 다른 규제방식을 채택하고 있는 관계로 개인정보의 국외이전에 대해서도 일률적으로 말할 수는 없다.

몇몇 주에서는 주정보기관이나 주와 계약한 상대방이 미국 국경 외부로 정보처리를 위탁하는 것을 제한하거나 금지하는 규제가 존재하는 것으로 알려져 있으나, 이러한 규제들도 적용대상을 주정부기관으로 하거나 주정부기관에게 서비스나 상품을 제공하는 계약을 체결한 계약상대방으로 한정되는 것들이다[8]. 다만, 미국 연방거래위원회(FTC) 및 기타 규제기관은 기본적으로 미국 국경을 떠난 후에도 그 정보에 대해서는 계속 미국법률이 적용될 수 있다는 입장이고, (개인정보를 국외로 이전한) 해당 미국회사에 대하여 "해외로 나간 정보, 하청업자에 의한 정보의 해외처리, 규제대상 정보에 대해 하청업자가 동일한 보호조치를 취할 것"에 대하여 책임을 진다는 입장을 보이고 있는 것으로 알려져 있다[9].

#### (2)EU

EU는 1995. 10. EU회원국을 위한 개인정보보호법의 기본원리에 관한 '개인데이터처리에 관

---

6) 다만, 현재 금융위원회와 금융감독원 실무부서는 개인신용정보를 해외에서 처리할 목적으로 개인신용정보를 국외로 제공하는 것은 신용정보법상 특별한 규정이 없어 허용되지 않는다는 해석을 취하고 있다. 강준모,우리나라 FTA와 전자금융법제, 한국법제연구원, (2010. 10. 27), 49페이지 참고

7) 참고로 금융실명법은 공공분야에 대해서는 국외이전과 관련한 근거규정을 두고 있다.
금융실명법 제4조 제1항 6. 금융위원회 및 금융감독원장이 그에 상응하는 업무를 수행하는 외국 금융감독기관(국제금융감독기구를 포함한다. 이하 같다)과 다음 각 목의 사항에 대한 업무협조를 위하여 필요로 하는 거래정보등의 제공
가. 금융회사등 및 금융회사등의 해외지점·현지법인 등에 대한 감독·검사
나. 「자본시장과 금융투자업에 관한 법률」 제437조에 따른 정보교환 및 조사 등의 협조.

8) http://uk.practicallaw.com/6-502-0467?source=relatedcontent#a285827 20.번 참조

9) 위 각주 9)번 링크 자료 참조

한 개인의 보호 및 해당 데이터의 자유로운 이동에 관한 1995년 10월 24일 유럽의회 및 이사회 95/46/EC 지침'(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of the personal data and on the free movement of such data)[10](이하 "EU개인정보 보호지침")을 배포한바 있다. 위 보호지침 제25조와 제26조는 개인정보를 제3국으로 이전할 때 제3국은 적절한 보안수준을 준수하여야 한다고 규정하고 있다. 이를 위해 유럽연합은 제3국에 대하여 개인정보 처리기한, 데이터 제공국가, 법률 환경 등 다양한 내용을 기준으로 하는 개인정보보호 수준을 평가하여 회원국에 통보하고 있으며, 유럽연합 수준으로 개인정보를 보호하지 않는 국가로는 자국민의 개인정보 이전을 금지하고 있다.

이러한 원칙에는 몇 가지 예외가 인정되고 있는데, 예를 들어 정보주체가 전송에 동의한 경우, 정보제공자와 관리자(Controller) 사이의 계약수행에 있어 전송이 필요한 경우, 관리자와 제3자 사이에 정보대상자의 이익을 위한 계약의 체결 또는 이행을 위해 필요한 전송인 경우, 중요한 공익적 근거에 기초하여 필요한 경우이거나 법적 의무사항 혹은 소송을 제기하여 이를 수행 또는 방어하기 위해 필요한 법적 의무 전송인 경우, 정보주체의 중대한 이익의 보호를 위하여 필요한 경우, 법 또는 명령에 의해 공중에 정보를 제공할 의도로 등록명부로부터 이루어진 전송 등이 있다[11].

### (3) 영국

영국은 개인정보보호를 위해 공공과 민간부문에 포괄적으로 적용되는 법으로 정보보호법(Data Protection Act)을 1998년에 제정·시행하고 있다. 영국의 정보보호법에서는 개인정보의 국외이전과 관련, 위 EU개인정보보호지침의 내용을 반영하여 "유럽 경제 구역 밖의 나라나 지역에서 개인정보의 처리에 정보주체의 권리와 자유를 적절한 수준으로 보장하지 않는다면 개인정보를 그 국가나 지역으로 이동시킬 수 없다"고 규정하고 있다. (반대로 유럽연합 지역 내에서는 개인정보의 이전과 관련한 특별한 제한은 없다). 만일 개인정보가 도착하는 국가가 이러한 수준을 구비하지 못한 경우라 하더라도 정보주체의 동의 등 일정한 예외[12]가 있다면 그 국가로 개인정보를 이전하는 것은 허용된다[13].

---

10) EU의 15개국 회원국 모두는 위 지침을 1998. 10.까지 국내법에 반영하도록 요구되어졌고, 결과적으로 EU 시민은 동일한 수준의 개인정보 보호를 받을 수 있게 되었다.

11) 이하 예외에 대한 내용은 개인정보보호위원회, 2012 개인정보보호 연차보고서, 303면 참조

12) - 정보주체가 이전에 동의한 경우
- 정보주체와 관리자 사이에 계약의 이행을 위해서 또는 데이터관리자와 그 계약을 체결시 정보주체의 요청에 의한 조치를 취하기 위하여 이전이 필요한 경우
- 데이터 관리자와 정보주체가 아닌 개인이 정보주체의 요청을 이행하는 계약 또는 정보주체의 이익을 반영하는 계약을 체결하거나 그 계약의 이행을 위해 이전이 필요할 때
- 이전이 중요한 공익을 위해 필요할 때, (그러나 내부장관은 명령으로 중요한 공익을 위해 이전을 하는 경우 필요한 조건이나 법령에서 요구하지 않는 이전을 하지 않을 조건을 명시할 수 있음)
- 이전이 법률적 소송을 위해 소송과 관련하여 법적 조언을 얻기 위해, 그 밖에 법적 권리를 확립·행사·수호하기 위해 필요한 때
- 이전이 정보주체의 중요한 이익을 보호하기 위하여 필요한 때
- 이전은 공적 기록상의 개인정보의 일부이며 그 기록이 일반에게 공개되는 조건은 그 이전 이후에 공개되거나 공개될 수 있는 모든 사람이 준수하여야 함
- 이전이 정보주체의 권리와 의무를 적절히 보장하는 감독관에 의해 승인받을 경우
- 이전을 시행할 자격은 개인의 권리와 의무를 적절히 보장하도록 하는 감독관에게 주어진 경우
(이상의 예외의 내용은 KISA〈 개인정보 국외이전 관련 국가간 협력방안 연구, 2006. 12, 78면 참고)

13) 참고로 세이프하버 원칙이란, 미국과 EU의 개인정보보호정책의 차이로 인해 통상마찰이나 개인정보의 국가간 유통을 방해할 수 있다는 우려에서 미국과 EU가 협상을 통해 수립한 원칙을 말한다. 즉, 미국의 기업이나 단체가 자발적으로 세이프 하버원칙을 준수하겠다고 미국 상무부에 신고할 경우, 충분한 개인정보보호 조치를 강

**(4)일본**

일본은 공공부문에서는 "행정기관이 보유한 개인정보에 관한 법률"(行政機關の保有する個人情報の保護に關する法律)이, 민간 부문에서는 2003. 5. 30. 제정된 "개인정보의 보호에 관한 법률"(個人情報の保護うに關する法律)이 각각 시행되고 있다. 민간부문에서 시행되는 개인정보의 보호에 관한 법률에서는 개인정보의 국외이전에 특별한 별도의 규정을 두고 있지 않으며, 일본 국외로 이전하는 것이 성격이 제3자 제공에 해당한다면, 본래 그 성격에 따라 사전 동의가 요구될 뿐이다[14].

# Ⅲ. 실무상 국외이전과 관련하여 자주 문제되는 법적 이슈

## 1. "개인정보"의 범위

### 가. 개인정보의 개념에 대한 실무의 입장

정보통신망법 및 개인정보보호법상 개인정보는 생존하는 개인에 관한 정보로서 특정 개인을 식별할 수 있는 부호, 문자, 음성, 음향 등 영상 등의 정보를 말하고, 해당 정보만으로는 특정개인을 알아볼 수 없어도 "다른 정보와 쉽게 결합하여 알아볼 수 있는 경우"라면 개인정보의 범주에 포함될 수 있다(정보통신망법 제2조 제1항 제6호, 개인정보보호법 제2조 제1호).

실무상 개인정보의 개념과 관련하여서는 "다른 정보와 쉽게 결합하여"의 의미가 주로 문제된다. 즉, 개인에 관한 정보라고 하더라도 특정 개인을 식별할 수 없다면 논리상 개인정보에 해당되지 않는다고 보아야 할 것이지만, 규제기관이 "다른정보와 쉽게 결합하여"의 범위를 지나치게 넓게 인정하고 있기 때문에 "개인정보"의 개념에 포섭되고 만다.

일례로 방송통신위원회가 발간한 "정보통신서비스 제공자를 위한 개인정보보호 가이드"에서도 "개인과 관련된 일반적인 정보들은 대부분 다른 정보와 결합하면 개인식별이 가능해지므로 정보통신망법의 적용을 받는 사업자들은 해당 서비스 이용자와 관련된 모든 정보를 개인정보로 간주하고, (이하 중략)"이라고 설명하고 있어, "개인에 관한 정보"라면 사실상 거의 예외없이 개인정보에 해당한다는 입장이다(정보통신서비스 제공자를 위한 개인정보보호 가이드, 15면). 또한 하급심 판례 중에는 스마트폰에서 증권시세를 검색하는 사용자의 앱을 개발하여 스마트폰의 IMEI(국제모바일 단말기 인증번호), USIM 일련번호를 사용자의 동의없이 수집한 사례에서 이용자의 동의를 받지 않고 개인정보를 수집하였다는 검찰 기소를 유죄로 인정하면서(서울중앙지방법원 2011. 2. 23. 선고 2010고단5343 판결 ; 이른바 e토마토 사건), "쉽게 결합하여 알아볼 수 있다"는 의미에 대하여, 당해 정보와 결합 가능한 다른 정보가 모두 동일인에게 보유되고 있는 것을 전제로 하고 있지 아니하고, 쉽게 다른 정보를 구한다는 의미가 아니라, 구하기 쉬운지 어려운 지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정개인을 알아볼 수 있게 되는 것을 말한다고 판시하였다. 즉, IMEI나

---

구하고 있는 것으로 간주하여 EU로부터 정보이전을 계속해서 받을 수 있다. 미국 상무부는 EU개인정보보호지침이 정하는 제3국으로의 정보이전에 관한 충분성 기준을 만족시키기 위해 EU에 이 원칙을 제안하였고, EU도 미국으로의 개인정보 이전이 금지되면 현실적으로 EU에 이익이 되지 않는다고 판단하여 2년여에 걸친 협상을 거쳐 2000. 7. 27. 유럽의회에서 심의되어 유럽연합 회원국에 승인되었다.
세이프하버 원칙에는 개인정보보호를 목적으로 고지(Notice : 수집되는 정보, 어떻게 쓰일 것인지에 대해 정보주체에게 알릴 의무), 선택(Choice:수집/이전에 대해 opt-out할 능력 부여), 제3자로의 이전(Onward transfer: 적절한 정보보호원칙을 따르는 기관에만 이전가능), 보안(Security : 분실을 막기 위한 합리적인 노력의무), 정보의 무결성(Data Integrity: 수집한 정보는 수집목적에 관련되고 신뢰할만한 것이어야 함), 접근(Access : 정보에 대한 접근권, 정정권, 삭제권), 집행(Enforcement : 규칙을 집행할 효과적인 수단이 있어야 함) 등의 준수사항이 정해져 있다.

14) http://uk.practicallaw.com/5-520-1289?source=relatedcontent#a629036 참조

USIM일련번호는  통신사의 데이터베이스에서 관리되어 있고, 그 시스템을 이용하면 누구인지 식별가능하다는 이유로 "쉽게 결합하여" 개인을 식별할 수 있으므로 개인정보에 해당한다는 입장이다.

### 나. 개인정보의 범위와 국외이전과 관련한 문제

이러한 개인정보의 범위에 대한 문제는 비단 국외이전에 국한된 이슈는 아니지만 위와 같은 실무 태도로 인해 개인정보의 국외이전과 관련하여 국내에서 수집된 개인에 관한 정보는 그 개인정보를 제공받는 국외자가 그 개인정보가 누구의 것인지 전혀 알 수 없는 경우에도 불구하고, 앞서 언급한 개인정보의 국외이전에 관한 규제가 적용될 수밖에 없는 상황이다.

예컨대 국내 소비자의 소비패턴 분석을 위하여 국내 자회사에서 수집한 국내 회원에 대한 정보를 해외 본사에서 취합하려고 할 경우 내지 국내 회사가 수집한 고객의 개인정보를 해외로 전송하여 위탁처리하는 경우, 설령 그 정보주체의 이름, 주소, 연락처, 주민등록번호 등과 같은 식별자가 전혀 포함되어 있지 않아 해외 본사가 해당 정보의 주체가 누구인지 전혀 알 수 없는 상황이라고 하더라도, 국내에서 다른 정보와 결합할 수 있는 이상, "개인정보"에 해당하고, 결국  앞서 언급한 개인정보의 국외이전에 대한 엄격한 규제가 적용되는 결과가 된다.

개인정보의 국외이전시 정보통신망법이나 개인정보보호법에서 정보주체로부터의 동의를 요구하는 것은 정보주체의 자기정보결정권을 보호한다는 취지이기는 하나, 국외에서 개인정보를 제공받는 자가 전혀 그 정보의 주체가 누구인지 식별할 수 없는 상태라면 개인정보로써 보호할 필요성이 크게 떨어지고, 실질적으로 개인을 식별할 수 없는 정보임에도 개인을 식별할 수 있는 정보와 아무런 구분 없이 동일한 규제를 적용하는 것은 지나친 규제가 아닐 수 없다[15].

## 2. "국외이전"의 범위 - "제공" 또는 "위탁"

### 가. "국외이전"의 의미

앞서 언급한 바와 같이 국외이전에 대하여 규정하고 있는 정보통신망 제63조와 개인정보보호법 제17조는 정보주체로부터 동의를 요구하고, 법령에 반하는 내용으로 계약을 체결할 수 없다는 등 유사한 방식으로 규정되어 있기는 하나, 다음과 같은 점에서 중대한 차이가 존재한다.

즉, 정보통신망법 제63조는 실무상 국외의 제3자에게 "제공"하는 경우와 "위탁"하는 경우 등 여하한 이유로든 개인정보가 국외로 이동하는 상황을 모두 포함하는 개념으로 해석된다. 따라서 정보통신서비스 제공자가 그 이용자의 개인정보를 국외의 제3자에게 제공하거나, 개인정보의 처리를 국외의 제3자에게 위탁하는 경우 혹은 어느 쪽에도 해당되는지 애매하지만 개인정보가 물리적으로 이동하는 경우에는 기본적으로 정보통신망법 제63조의 적용을 받게 된다.

반면, 개인정보보호법 제17조 제3항은 오로지 국외의 제3자에게 제공하는 경우를 상정하고 있다. 즉, 개인정보보호법은 국외이전에 대한 규정을 개인정보의 제3자 제공에 관한 규정안에 포함시키고 있기 때문에, 개인정보를 국외로 위탁하는 경우에 대해서는 개인정보보호법 제17조 제3항이 적용되지 않고, 일반적인 위탁에 준하여 개인정보보호법 제26조가 적용된다고 해

15) 물론 개인정보보호법은 개인정보를 특정 개인을 알아볼 수 없는 형태로 활용하는 경우에는 개인정보로써 적용되는 규제를 완화하는 취지의 예외규정(제18조 제2항 제4호)을 두고 있으나 이 규정이 적용되려면 제공되는 목적이 "통계처리 및 학술연구"로 제한되기 때문에 완전한 해결책은 되지 못한다. 향후 개인정보의 국외이전에 대해서도 이와 같이 식별성을 제거한 경우에는 기존 규제가 적용되지 않는다는 내용의 입법도 고려해 볼 필요가 있을 것이다.

석된다. 다시 말해, 개인정보를 국외의 제3자에게 "제공"하는 경우에는 정보주체에게 일정한 사항을 고지하고 동의를 받아야 하지만(제17조 제3항), 위탁하는 경우에는 위탁하는 업무의 내용과 수탁자를 정보주체가 언제든지 쉽게 확인할 수 있도록 공개하면 된다(제26조 제2항)

## 나. "제3자 제공"과 "위탁"의 구분

개인정보보호법이나 정보통신망법상 "제3자 제공"과 "위탁"의 의미는 통상 다음과 같이 설명하고 있다. 즉, "위탁"이란 자신의 업무와 직, 간접적으로 관련된 업무의 일부를 타인으로 하여금 그 책임과 권한으로 행하도록 하는 것을 말하고, "제공"이란 개인정보를 제공받는 자의 이익이나 업무를 위하여 개인정보의 이용권 혹은 관리권이 제공받는 자에게 이전되는 것을 말한다. 좀 더 쉽게 설명하면, 개인정보의 제3자 제공은 "제공받는 측의 사업목적"을 위하여 개인정보가 제공되는 것을 말하고, 위탁은 "제공하는 측의 사무처리"를 위한 경우를 말한다(대법원 2011. 7. 14. 선고 2011도1960판결[16]).

예컨대, 국내 회사가 수집한 이용자의 개인정보를 글로벌 마케팅 목적으로 국외의 자회사와 공유한다면 이는 "제공"에 해당할 수 있고, 국내 회사의 임직원에 대한 인사업무 전부를 국외의 자회사가 대신 수행한다면, 임직원의 개인정보가 "위탁"되는 경우로 볼 수 있다.

문제는 제3자 제공과 위탁의 구분이 실무상 항상 명확하지 않다는 점에 있다. 즉, 개인정보를 이전하는 이유가 제공하는 측인 국내업체와 제공받는 측인 국외 업체가 각자 자신의 사업목적을 위한 것이라면, 이를 개인정보의 제공인지 위탁인지 판단하기 어려운 측면이 있다. 이를테면, 일부 다국적 기업은 내부적으로 수립한 인력정책을 통해, 계열회사 임직원의 세세한 정보를 수집, 종합하여 인력배치나 평가업무를 통일적으로 수행하여 전체 관리비용을 절감하고 전 세계적으로 통일적 운영을 도모하려고 하는바, 국내 계열회사를 기준으로 보면 국외 본사의 업무목적이라는 점에서 이를 제3자 제공으로 보아야 할지, 아니면 국내 계열회사의 인사업무를 국외의 본사에서 수행한다는 측면에서 위탁으로 보아야 할지 명확한 판단이 어렵다. 앞서 언급한 바와 같이 개인정보보호법은 "제공"인지 혹은 "위탁"인지 여하에 따라서 정보주체의 동의를 받아야 하는지 여부가 결정된다는 점에서, 실무상 개인정보의 처리 위탁인지 제3자에 대한 제공인지 여부는 중요한 의미를 가질 수 있다.

또한 앞에서 본 바와 같이 설령 개인정보의 처리 위탁으로 보더라도, 개인정보의 처리위탁에서 위탁자는 정보주체의 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 하는바(개인정보보호법 제26조 제4항), 국내 위탁자가 국외 수탁자에 대해 이러한 감독책임을 수행할 수 있는지 의문이다. 즉, 위 규정에 의하면 국내 위탁자가 일단 국외사업자에게 개인정보의 처리업무를 위탁하면, 국내 위탁자가 국외 사업자를 교육한다거나 안전하게 처리하는지를 감독해야 할 것인데, 만일 현지자회사나 지점의 지위에 불과한 국내 위탁자라면 국외에 위치한 본사를 감독하는 것은 실무상 거의 불가능하다고 볼 수 있다[17]. 특히, 해외 본사

16) 대법원 2011. 7. 14. 선고 2011도1960판결은 정보통신서비스 제공자인 피고인 갑 주식회사의 임원 피고인 을이 이용자들의 동의를 받지 아니하고 개인정보를 제3자인 병 주식회사에 제공하였다고 하여 구 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반으로 기소된 사안인바, 원심은 위와 같은 전제를 설시하면서 병 회사가 갑 회사를 위하여 갑 회사 일부 업무를 위탁받아 수행하는 '수탁자' 지위에 있어 법 제24조에서 정한 제3자가 아니라는 판단하였고, 대법원은 그 판단에 동의하였다.

17) 만일 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 법을 위반하여 발생한 손해배상책임에 대해서는 수탁자가 위탁자의 소속직원으로 간주되어 결국 위탁자도 손해배상책임을 부담하게 되는바(개인정보보호법 제26조 제5항), 만일 수탁자인 해외 본사에서 개인정보가 유출되는 사고가 발생하는 경우, 위탁자인 국내 계열회사가 관리,감독에 관한 주의의무를 다하였다는 점을 입증하지 않는 이상(민법 제756조 참고), 국내 계열회

가 전 세계적으로 수집하여 통일적으로 처리하고 있는 임직원의 개인정보 중 한국 임직원의 개인정보만의 관리를 위하여 본사에게 (현지 법규에 따른 조치 외에 추가하여) 한국 내 법규에 따른 제반 조치(예: 기술적, 관리적 조치)를 별도로 준수하라고 요구하기도 어렵거니와, 그러한 한국 임직원의 개인정보만을 구분하여 본사의 개인정보 처리관련 업무를 교육, 감독하라고 요구하는 것도 현실적이지 못하다. 이에 대하여 행정안전부는 수탁자가 국외의 제3자라고 하더라도 이러한 교육이나 감독의무가 면제되는 것은 아니라고 하면서도, 정작 국내 위탁자가 이러한 의무를 이행할 수 있는 방법에 대해서는 뚜렷한 가이드를 제시하지 않고 있다.

## 3. 계열회사간 개인정보 공유

또한 개인정보와 관련한 정보통신망법이나 개인정보보호법은 동일 그룹의 계열회사나 제휴회사 간 정보공유나 이전에 대해서도 별도의 예외가 인정되지 않는다. 다시 말해 동일한 기업집단에 속해 있는 계열회사 간이라고 하더라도 임직원의 개인정보를 주고받을 경우에는 개인정보의 제3자 제공 또는 위탁의 법리가 그대로 적용된다. 이와 같이 계열회사 간에 개인정보를 서로 공유하기 위해서는 이용자 혹은 정보주체에게 개인정보를 제공받는 자의 명칭을 고지하고 동의를 받아야 하고(위탁의 경우 동의를 받지 않는다고 하더라도 제공받는 자의 명칭을 고지해야 한다는 점은 동일하다), 그 현황은 개인정보처리방침에 공개되어야 한다.

문제는 방송통신위원회나 행정안전부가 실무상 이러한 "개인정보를 제공받는 자의 명칭이나 상호" 혹은 "수탁자의 명칭이나 상호"를 구체적으로 명시할 것을 요구하고 있다는 점이다. 심지어 이러한 제공받는 자 혹은 수탁자가 수백에서 수천 개에 이르더라도 대표 업체명과 업체수를 기재하되, 웹사이트 링크 등을 통해 상세 내역을 이용자가 언제든지 확인할 수 있도록 조치하여야 한다[18]는 입장이고, 실제로 이를 위반한 사업자에게 개별적으로 시정명령을 내린 사례도 존재한다.

예컨대 글로벌 기업의 계열회사간에 임직원의 개인정보를 서로 공유하기 위해서는 해당 개인정보를 공유할 수 있는 모든 주체의 리스트를 정보주체에 일일이 알려야 하는 바, 이와 같은 리스트를 작성하는 것이 실무상 곤란한 경우가 많을 뿐만 아니라 과연 정보주체가 이러한 리스트의 내용을 관심을 가질지도 의문이다. 더구나 이렇게 개인정보를 공유하는 주체에 변동이 있으면, 그 변동 사항에 대해서도 일일이 고지하고 동의를 받아야 하는바(정보통신망법 제24조의2 제1항 후단, 개인정보보호법 제17조 제2항 후단 참고[19]), 국내 회사가 해외계열사의 변동 상황을 일일이 정보주체에게 알리고 동의를 준수하는 것은 실무적으로 매우 어려울 것이다. 물론 이용자 혹은 정보주체에게 그의 개인정보가 누구에게 제공 혹은 위탁 처리된다는 점을 알리는 것은 자기정보결정권의 보호를 위한 것이기는 하나, 이용자 혹은 정보주체가 자신의 개인정보가 누구에게 제공될 것인지 예측이 가능하거나 계열회사 간 개인정보를 공유하는 경우에는 일일이 개인정보를 공유하는 주체의 리스트를 열거할 필요가 없는 예외를 인정할 필요가 있다.

---

사가 손해배상책임을 부담하게 될 수 있다.

18) 예컨대, 방송통신위원회, 정보통신서비스 제공자를 위한 개인정보보호 가이드,45면 참고

19) 정보통신망법 제24조의2 ① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다

개인정보보호법 제17조 ② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

### 4. 국외이전에 대한 규정의 실효성

개인정보의 국외이전에 대해 규정하고 있는 정보통신망법 제63조와 개인정보보호법 제17조 제3항의 실효성에 대해서도 문제제기가 가능하다.

즉, 정보통신망법 제63조의 경우 위반시 형사처벌이나 과태료와 같은 별도의 제재규정이 없을 뿐만 아니라 그 위반자체가 문제시되는 경우도 드물어 실무상 거의 사문화된 규정으로 볼 수 있다. 또한 개인정보보호법 제17조 제3항은 개인정보의 제3자 제공을 전제로만 규정되어 있을 뿐만 아니라 그 제공의 목적이나 형태와는 상관없이 개인정보가 국외의 제3자에게 제공되면 동의를 구해야 하는 획일적인 결론이 도출될 수밖에 없으며, 그 규정의 반대해석상 이용자의 동의를 받으면 개인정보가 국외의 제3자에게 제공되는 것에 거의 아무런 제한이 없다는 결론이 되어, 과연 위 규정이 추구하려는 입법목적을 달성할 수 있을지 의문이다.

더구나 양 규정 모두 개인정보를 제공받는 자가 국외에 위치하고 있기 때문에 이러한 사업자들에 대해서는 국내 행정청이 행정력을 행사하기도 어렵다.

## Ⅳ. 현재 실무에 대한 평가 및 개선방향

### 1. 현재 실무에 대한 평가

개인정보 국외이전에서 정보주체의 동의제공을 전제로 하는 관련 국내 규정들은 지나치게 엄격하다. 국내에서 수집한 수천에서 수만 명에 이르는 고객의 개인정보를 위탁처리하기 위하여국외로 이전하는데 고객들로부터 일일이 동의를 받아야 한다면, 이를 준수할 수 있는 사업자는 많지 않을 것이다. 또한 국내회사의 서비스를 이용하려는 이용자나 국내 회사 임직원의 경우 자신의 개인정보가 국외로 이전될 수 있다는 점에 대하여 관심 자체를 두지 않는 경우가 많고, 관심이 있다고 하더라도, 별다른 대안이 없는 이상 무감각하게 동의할 가능성이 많은바, 현행 입법은 이용자에게 반드시 유익한 규정이라고 보기는 어렵다. 더구나 이용자의 동의를 제외하고는 다른 대안(예: Safe Harbor원칙, model clause, model contract, BCR 등)을 전혀 인정하고 있지 않기 때문에 정보주체의 동의이외에 사업자가 합리적으로 가능한 범위에서 준수할 수 있는 방안이 제시될 필요가 있다.

또한 이렇게 국외이전에 대해 이용자의 동의를 얻는 입법태도는 오히려 사업자에 의해 악용될 가능성이 있다. 즉, 정보주체의 "동의"를 받아야 국외이전을 할 수 있다는 것은 반대로 정보주체의 "동의"만 있으면 국외이전을 할 수 있다는 사업자의 "면책"규정으로 악용될 우려가 있다. 특히 개인정보가 이전되는 외국 국가의 정보보호수준에 대한 판별능력이 없는 정보주체의 동의에만 의존하여 국외이전 여부를 결정하는 것은, 설령 동의가 있는 경우라 하더라도 이를 실질적인 informed consent라고 단정하기 어렵다. 이러한 점에서 국외이전대상 국가의 적정한 정보보호 수준에 대해서는 공신력이 있는 국가기관이 판단하는 것이 타당할 것이다.

그와 더불어 국외이전과 관련하여 이전되는 개인정보의 정보주체의 자기정보결정권을 보호할 수 있는 실질적인 방안을 고려해야 할 것이다. 물론 현재 규정상 국외이전의 경우에도 보호조치를 규정하는 등의 보호 규정이 존재하지만, 사업자가 자발적으로 준수하지 않는 이상 이를 강제할 수단이 많지 않다는 점에서 실효성에 문제가 있다.

참고로, 한-미, 한-EU FTA 체결로 인하여 금융기관에서 보관하고 있는 금융정보에 대해서는 국외이전이 원칙적으로 허용되는 방향으로 국내 법률이 개정될 예정이다. 즉, 한-미, 한-EU FTA 협정에서는 해외금융기관들의 국내지점 내지 자회사가 국내에서 수집한 개인신용정보를 통상적인 업무수행과정의 일환이라면 해외에서 위탁 처리하는 것을 허용하는 취지의 합

의가 존재하는바, 이에 따른다면 적어도 금융기관에서 취급하는 금융정보에 대해서는 국외이전에 대한 규율이 신설되어야 한다. 물론 금융기관이 아닌 사업자가 보유한 개인정보의 국외이전에 대해서까지 언급된 것은 아니나, 금융정보가 상대적으로 엄격한 규제와 보호의 대상이 된다는 점을 감안하면, 금융정보와의 균형상 기존 개인정보의 국외이전에 대한 규제도 개정을 고려해 볼 수도 있을 것이다.

## 2. 개선방향

개인정보의 위탁과 제공에 있어서 기존의 고지와 동의 일변도의 규제정책에서 탈피하여 정보주체에게 요구되는 고지와 동의사항을 정보주체가 실질적으로 예측하기 어려운 경우로만 한정하는 방향으로 법률을 개정하는 방안을 고려할 필요가 있다.

예컨대, 글로벌 기업에 근무하는 직원의 경우, 직원으로서 자신의 개인정보를 본사나 다른 해외 계열회사 등에서 이를 관리하는 것이 통상적인 업무이고, 이는 충분히 예측이 가능한 것인데, 굳이 이에 대한 별도의 동의 내지 별도의 고지가 있어야 할 필요가 있을지 의문이다. 마찬가지로 해외에서 플랫폼을 운영하는 서비스를 이용하는 경우, 통상 그 이용자는 자신에게 서비스를 제공하는데 필요한 통상적인 업무가 해외에서 이루어 질 것을 예측하고 자신의 개인정보를 제공하였다고 볼 수 있을 것이다. 이러한 사용자에게 현행법령이 정하는 바와 같이 통상적으로 예측되는 개인정보의 위탁, 제공과 관련한 수많은 고지, 동의 절차까지 요구할 경우, 정작 관심을 가지고 보아야 할 내용, 고민후 내려야할 결정까지 이러한 수많은 고지, 동의 절차에 매몰되어 제대로 검토함이 없이 만연히 고지내용을 간과하거나 동의여부에 대한 결정을 성급하게 내리게 될 위험이 크다.

즉, 실무적으로 대부분의 개인정보의 정보주체는 자신이 제공하는 개인정보가 어떤 목적으로 이용되며 대체로 그 목적을 달성하기 위해 필요한 관련 업체에게 제공될 것임을 각오하고 개인정보를 제공함에도 형식적, 기계적인 절차로 개인정보의 수집이용, 제3자 제공, 취급위탁, 고유식별정보처리 동의 등 여러 단계의 동의서에 서명하거나 온라인상으로 click하는 경우가 대다수인바, (개인정보의 적법한 수집·이용을 전제로) 정보주체가 예측할 수 있는 범위 내에서 개인정보가 위탁 혹은 제3자 제공되는 경우라면 기존의 고지나 동의요건을 완화할 필요가 있다.

예컨대, 개인정보의 수집·이용시 정보주체가 실질적으로 개인정보가 위탁되거나 제3자에게 제공된다는 점을 예측할 수 있는 범위라면, 그 위탁에 대해 별도의 고지나 동의는 불필요하며, 제3자 제공에 대해서는 동의가 아니라 공개나 고지로 갈음하는 것이 가능할 것이다. 특히 위탁의 경우 해당 개인정보의 위탁자가 수탁자의 개인정보 처리업무에 대해 자신이 처리하는 것과 동일한 책임을 부담하고 있고, 정보통신망법 또는 개인정보보호법상 기술적·관리적 보호조치 등을 준수해야 하는 등 안전장치가 있다는 점을 고려하면 별도로 고지나 동의를 요구할 필요가 없다. 또한 제3자 제공의 경우에서도 앞서 언급한 것과 같이 그 제공목적, 제공을 받는 자가 사전에 충분히 예측될 수 있는 경우라면, 구태여 정보주체의 동의를 구하는 것은 요식절차에 불과할 수 있기 때문에, 정보주체에게 제공사실을 고지하거나 공개하는 것으로써 대체하는 것이 바람직할 것이다.

반면 정보주체가 예측할 수 있는 범위를 넘어서 통상적인 업무 목적을 벗어나는 개인정보의 제공이나 위탁의 경우나 주민등록번호와 같은 고유식별정보나 건강정보와 같은 민감정보를 국외로 이전하는 경우에는 정보주체의 자기정보결정권을 보호할 필요가 존재하므로, 이러한

경우에는 기존 규제와 유사하게 업무위탁은 “공개”(혹은 고지), 제3자 제공은 “동의”를 요구하는 것이 바람직할 것이다. 또한 개인정보처리자가 “개인정보를 재화나 서비스의 홍보목적으로 이용”한다거나 “개인정보 보호 수준이 적정하다고 평가되지 않는 국가로 이전하는 경우”에는 정보주체의 예측가능성 유무를 따지기에 앞서 개인정보의 남용과 취약한 관리가 우려되는 상황이므로, 정보주체가 예측할 수 있는 범위를 넘어서는 경우로 간주(혹은 추정)하는 방안도 고려해 볼 수 있을 것이다.

다만 이러한 예외상황에 대해서는 정보주체가 자신의 개인정보가 위탁 또는 제공되는 것을 원치 않는 경우가 있을 수 있으므로, 이러한 경우에는 정보주체가 개인정보처리자에게 개인정보의 처리정지나 동의철회권을 행사할 수 있도록 보장하는 것이 전제되어야 할 것이다(Opt-out방식).

위와 같은 개선이 이루어진다면 과다한 고지/동의 요건으로 인한 사업자의 업무부담은 완화될 수 있을 것이며, 정보주체도 예측하지 못한 개인정보의 위탁 혹은 제공에 대해서만 기존과 마찬가지로 고지나 동의절차가 진행되기 때문에 실질적으로 개인정보 자기결정권을 행사할 수 있게 할 수 있을 것이다. 이와 아울러 개인정보 보호수준이 상당한 수준이 이른 국가들과의 미국-EU간 Safe Harbor 와 유사한 협정의 체결노력, APEC의 CBPR(Cross Border Privacy Rules) system과 같은 개인정보의 원할한 국가간 이동을 도모할 수 있는 보호장치가 빨리 활성화 될 수 있도록 필요한 국제적 공조를 서둘러야 할 것이다.

# “개인정보”의 정의와 위치정보보호법의 개선 방안
## - 익명위치정보, 허가제 및 즉시동의요건을 중심으로

고려대학교 법학전문대학원 교수 박경신

## Ⅰ. 서론

위치기반서비스(LBS: Location-Based Service)는 무선통신망 및 GPS 등을 통해 파악된 위치정보를 바탕으로 인터넷 사용자에게 사용자가 변경되는 위치에 따른 특정 정보를 제공하는 무선 콘텐츠 서비스를 말한다.[1] 군사용으로 출발한 LBS는 그 효용성이 입증되면서 교통·치안 등 공공부문에서 널리 활용되고 있다.[2] 국내에는 1999년 이동통신사를 중심으로 위치정보를 이용한 서비스가 소개되었는데, 친구찾기 서비스, 내비게이션, 가족 안전 서비스, 주변 정보 제공 서비스 등이 대표적인 LBS이다. 이동성과 휴대성, 끊김 없는 정보를 제공하는 스마트폰에서 LBS는 소위 ‘킬러앱’으로 자리매김하고 있으며, ‘LBS +증강현실’, ‘LBS +SNS’ 등의 다양한 융합형 LBS가 등장하고 있다. 2009년 IT 시장조사 기관 가트너(Gartner)는 2012년 가장 주목받을 스마트폰 애플리케이션 중 하나로 LBS를 선정했고[3], 한국정보화진흥원도 2012년 10대 IT 트렌드 전망에 LBS를 포함시켰다.[4]

정보통신 기술의 눈부신 발달과 함께 LBS 산업은 급성장 중이다. 미 시장조사기관 피라미드 리서치(Pyramid Research)는 전 세계 LBS 시장 규모가 2010년 28억 달러에서 2015년에는 103억 달러 규모로 성장할 것으로 전망했으며, 이 중 전 세계 LBS 광고 시장이 GPS 탑재 단말 확산과 모바일 비즈니스 인프라 개선에 힘입어 2015년에는 62억 달러 규모에 달할 것으로 전망했다.[5] 가트너는 세계 LBS 시장이 2008년 19억 달러에서 연평균 성장률(CAGR) 27.3%씩 성장하여 2014년경에는 82.6억 달러 규모의 시장을 형성할 것으로 전망했다.[6] 그리고 전 세계 모바일 LBS 및 관련 앱 매출은 2014년경에는 127억 달러에 이를 것으로 전망했다.[7] 국내 LBS 시장도 스마트폰 열풍에 힘입어 빠르게 성장하면서 2012년까지 1조 6,000억 원 규모의 매출을 기록할 것으로 예상된다. 삼성경제연구소는 2013년경 스마트폰 이용자의 80%가 LBS를 이용할 것으로 전망하였다.[8]

이렇듯 LBS 산업이 급부상하는 현실에서 위치정보는 상업적 활용도가 매우 높은 정보사회의 중요한 자원임은 분명하다. 그러나 위치정보는 해당 개인의 활동반경이나 이동경로, 취미나 관심사까지도 예측할 수 있는 단서가 될 수도 있다는 점에서 개인 사생활과 직결되며, 오·남용 시 심각한 프라이버시 침해의 우려가 있는 것도 사실이다. 삼성그룹 노동자 위치추적 감시 사건(2004), 국가정보원 X파일 사건(2005), 여배우 휴대전화 위치추적·도청사건(2009년) 그리고 최근에는 아이폰 사용자 위치정보 수집 사건(2011) 등에서 위치정보의 오·남용 문제

---

1) 백인수 외, “2010년 IT 분야 10대 전략 이슈와 시사점”, IT 정책연구시리즈, 한국정보화진흥원, 2010
2) 이영일 외, “부상하는 위치기반서비스(LBS)”, CEO Information, 삼성경제연구소, 2007. 8. 1., 1쪽
3) 전황수, “LBS 시장 및 업체 동향”, 정보통신산업진흥원, 주간기술동향 2011. 1. 19., 1쪽
4) 주윤경 외, “2012년 IT 트렌드 전망 및 정책방향”, IT정책연구시리즈, 한국정보화진흥원, 제23호(2011. 12. 29.), 4쪽
5) Pyramid Research, “Location-Based Services: Market Forecast, 2011-2015”, 2011. 5.
6) Gartner, ″Forecast: Consumer LBS″ Worldwide, 2008-2014, 2010. 7.
7) (주)알앤디비즈, “국내외 LBS산업 현황 및 동향조사”, 한국인터넷진흥원, 2011. 12.
8) 전황수, 4쪽

가 부각되었다.[9] 이에 대한민국 정부는 “위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호”하고자[10] 세계 최초로 2005년 「위치정보의 보호 및 이용 등에 관한 법률(이하 ‘위치정보보호법’)」을 제정·시행하고 있다.

위치정보보호법이 제정될 당시에는 현재의 개인정보보호법이 존재하지 않았으며, 과점적 지위를 가진 이동통신사업자의 사생활의 비밀의 침해 방지 필요성에 규제의 초점이 맞추어졌다. 허가, 인가, 신고 등 진입규제가 도입되었으며, 강한 의무 내지 제재 규정들은 사업자가 위치정보를 수집하여 제3자에게 제공하는 서비스(소위 “위치정보사업”)를 대표적인 규제 대상으로 하고 있다.[11] 그리고 위치정보보호법은 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는지 여부에 따라 ‘위치정보’와 ‘개인위치정보’[12]를 구분하면서도, 제15조 제1항에서 “누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집、이용 또는 제공하여서는 아니 된다”[13]고 하여 특정되지 않는 ‘개인 또는 이동성 물건의 위치정보’도 보호대상으로 삼고 있다. 이는 개인정보보호법 상 보호되는 ‘개인정보’의 범위를 훨씬 넘는 것으로, ‘특정 개인의 것이 아닌 위치정보’ 즉 ‘익명인의 위치정보’의 경우에도 프라이버시 침해 문제가 발생할 수 있을지 의문이 발생한다.

이제는 이동통신사업자뿐만 아니라 위성신호 등을 이용해 자신을 측위할 수 있는 기술이 보편화되었고, 이용자의 위치공개 욕구를 반영한 서비스 또는 특정 개인을 식별할 수 없는 익명인의 위치정보를 사용한 서비스가 등장하는 등 LBS 산업 환경이 하루가 다르게 변화하고 있다. 특히 LBS 산업은 아직 성장단계로서 GPS 등 원천기술은 서구의 선진국들이 세계 시장을 선점하였으나, 세계 최고 수준의 IT 응용기술을 보유한 우리나라는 LBS 응용 분야에서 글로벌 기업들과 충분히 경쟁이 가능하다.[14] 또한 LBS는 단순한 하나의 사업 분야에 그치지 않으며 다양한 측면에서 국가 전반의 효율성을 높일 수 있는 전략적 자산으로, 지속적 육성이 필요한 미래형 산업이다. 이러한 LBS 산업을 기존의 규제 틀에 맞추어 제한해서는 안 되며, 규제를 재정비하여 LBS 산업 육성과 개인위치정보 보호의 균형을 찾는 정책적 노력이 시급한 상황이다.

이하 먼저 개인정보보호의 보편적 규범인 개인정보보호법에 비추어 위치정보보호법의 문제점을 지적하고 이에 대한 개선 방안을 제시해보도록 한다. 여기서 살펴볼 위치정보보호법의 주요 내용은 다음 세 가지이다.

---

9) 박정훈, “최근의 위치정보에 관한 논의, 그리고 그 평가와 시사 - 미국의 사례를 중심으로 -”, 경희법학 제46권 제4호, 2011, 112쪽

10) 위치정보의 보호 및 이용 등에 관한 법률 제1조(목적) 이 법은 위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호하고 위치정보의 안전한 이용환경을 조성하여 위치정보의 이용을 활성화함으로써 국민생활의 향상과 공공복리의 증진에 이바지함을 목적으로 한다.

11) 허은영, “위치정보 서비스 활성화와 사생활 보호를 위한 과제”, 통신연합 58호(2011 가을호), 42쪽

12) 위치정보보호법 제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. ″위치정보″라 함은 이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조 제2호 및 제3호에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것을 말한다.
2. ″개인위치정보″라 함은 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)를 말한다.

13) 위치정보보호법 제15조(위치정보의 수집 등의 금지) ①누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집、이용 또는 제공하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 제29조 제1항에 따른 긴급구조기관의 긴급구조요청 또는 같은 조 제7항에 따른 경보발송요청이 있는 경우
2. 제29조 제2항에 따른 경찰관서의 요청이 있는 경우
3. 다른 법률에 특별한 규정이 있는 경우

14) 전황수, 12쪽

첫째, 위치정보 수집 등의 금지를 규정하여 누구든지 개인 또는 이동성이 있는 물건의 소유자의 동의 없이는 당해 개인 또는 물건의 위치정보를 수집•이용 또는 제공할 수 없도록 하고, 위반시 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처하고 있다(법 제15조 및 제40조).

둘째, 위치정보사업의 허가제(법 제5조)와 위치기반서비스사업의 신고제(법 제9조)에 따라, 위치정보를 수집하여 위치기반서비스사업자에게 제공하는 위치정보사업을 하고자 하는 자는 방송통신위원회의 허가를 받도록 하고, 위치정보를 이용하여 서비스를 제공하는 위치기반서비스사업을 하고자 하는 자는 방송통신위원회에 신고를 하도록 하고 있다.

셋째, 개인위치정보의 제3자 제공시 통보의무를 규정하되 위치기반서비스제공자는 개인위치정보주체가 지정한 제3자에게 개인위치정보를 제공할 때에는 개인위치정보주체에게 제공사실을 매회 즉시 통보하여야 한다(법 제19조제3항).

# Ⅱ.위치정보보호법의 개요

## 1. 개인정보보호법제 개관

위치정보보호법제는 개인정보보호법제의 일종으로서 개인정보 중에서 위치정보를 특별히 보호하는 것이므로 양자는 특별법과 일반법의 관계라고 볼 수 있다. 이에 따라 위치정보보호법제를 평가하기 위해서는 우선 개인정보보호법제를 이해할 필요가 있다.

우리나라에서는 1990년대 중반부터 본격적으로 개인정보보호를 위한 법률들이 제정되기 시작했는데, 이들은 특수목적을 위한 법률이었으며 일반법에 해당하는 공공기관의 개인정보보호에 관한 법률은 오직 공공기관에만 적용되었기 때문에 민간기관에도 적용될 수 있는 통합적인 개인정보보호법 제정에 대한 요구가 많았다.[15] 이러한 요구를 수렴하여 제안된 여러 법안들이 국회에서 통과되지 못하고 폐기되었다가 2011년 3월 마침내 개인정보보호법안이 통과되어 같은 해 9월 30일부터 시행되고 있다.[16]

현행 개인정보보호법은 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보'를 '개인정보'라고 정하고 이 개인정보를 쉽게 검색할 수 있도록 체계적으로 배열 및 구성한 집합물을 '개인정보파일'이라고 하며 '개인정보파일'을 처리하는 기관, 법인, 단체 및 개인을 '개인정보처리자'라고 정의한다(법 제2조). 또한 개인정보의 대상이 되는 자를 '정보주체'라고 정의하고 있다(법 제2조). 개인정보보호법의 핵심은 정보주체는 개인정보처리자의 행위를 제한할 수 있는 권한을 가지게 된다는 점이다. 대표적으로 '개인정보처리자'는 원칙적으로 '정보주체'의 동의를 받은 경우에만 정보주체에 대한 정보를 수집할 수 있다(법 제15조). 뿐만 아니라 개인정보처리자는 이 동의를 얻을 때 수집목적을 정보주체에게 밝혀야 하고 그렇게 수집한 후에도 정보를 처리목적에 필요한 용도로만 사용해야 하며(법 제15조), 그 정보가 정확하도록 유지해야 하고 유출되지 않도록 관리해야 하며 정보주체가 그 개인정보를 열람할 수 있게 해야 함은 물론 개인정보 처리방침 등을 공개하고 최대한 익명처리해야 한다(법 제3조). 그리고 '정보주체'는 '개인정보처리에 대해 동의권, 정정 및 삭제권을 가지며 개인정보처리에 의해 피해가 발생할 경우 구제청구권도 가지게 된다(법 제4조).

그런데 위 법조문들을 실제로 적용해보면 개인정보보호법의 문제점을 금방 알 수 있다. 법상 정의에 따라 개인을 식별할 수 있는 정보를 모두 개인정보라고 하게 되면 실명을 거론하는 모든 말이 개인정보가 된다. 예를 들어 '박경신은 고려대학교 교수이다'라는 정보가 들어있는

15) 김상겸·김성준, "정보국가에 있어서 개인정보보호에 관한 연구", 세계헌법연구 제14권 제3호, 2008, 106쪽
16) 정혜영, "개인정보보호법의 내용과 체계에 관한 분석", 공법학연구 제12권 제4호, 2011, 407쪽

모든 문서들은 개인정보를 담지한 것이 된다. 그런데 개인정보보호법을 여기에도 적용한다면 정보주체인 박경신은 이 문장의 존재를 알아야 하고 이 문장이 어떻게 사용되는지를 알아야 하며 이 문장이 어떻게 이용될지도 통제할 수 있어야 할 것이다. 이것은 표현의 자유에 대한 심대한 침해를 발생시킬 것이 자명하다.[17] 어떻게 개인정보보호법제를 이해할 수 있을까?

세계적으로 개인정보보호법제는 정보기술이 발전하면서 여러 사람들에 대해 매우 민감한 정보가 한 매체에 집적되는 현상이 발생하기 시작하였고 이 매체에서 정보유출이 발생할 경우 수많은 사람들이 심대한 피해를 입을 수 있게 되었다는 자각에서 시작되었다. 이에 따라 프라이버시를 더욱 적극적으로 보호할 필요가 인식되기 시작한다. 1967년 Alan Westin이 「Privacy and Freedom」이라는 책을 통하여 대량정보의 수집 및 처리에 대한 연구결과를 발표하여 미국, 영국 등 각국의 정부들의 연구를 촉발시켰고,[18] 이는 소위 공정정보관행(Fair Information Practice 또는 FIPP)이라는 이름으로 각국의 법으로 또는 정책으로 퍼져나갔다. 미국에서는 1973년에 보건복지성의 자동화된 개인정보시스템에 관한 자문위원회가 보고서를 발간하였다.[19] 1977년의 미국연방정부는 영역별로 프라이버시 보호에 대한 연구를 진행하여 현황을 파악하였고 이 연구결과가 추후 입법과정에 도움을 주었다.[20] 이 움직임은 「1980년 OECD 프라이버시 보호 및 개인정보 국제유통 가이드라인(이하 'OECD 가이드라인')」[21]과 1981년의 EU자동처리개인정보협약[22]으로 이어졌고 이때 20여 개국이 정보보호법을 제정하였다. 10여년이 흐른 후 인터넷시대가 열리면서 「1995년 EU 개인정보 처리에 관한 개인의 보호 및 자유로운 정보유통에 대한 지침(이하 'EU 개인정보보호지침')」[23]이 발표되었다.[24] 독일을 비롯한 유럽의 여러 나라들이 EU 협약이나 EU 지침에 따라 우리나라와 비슷한 포괄적인 개인정보보호법을 제정하였다.

공정정보관행원리 또는 FIPP에 따르면 모든 정보가 잠재적으로 프라이버시를 침해할 수 있으므로 개인을 식별할 수 있는 모든 정보가 '개인정보'가 되고[25] 대량으로 그리고 자동화된 형태의 개인정보를 처리하는 경우의 수집, 유통 및 이용에 대해 정보주체가 통제권을 갖는 것을 기본으로 하고 있다.[26] 이렇게 되면 프라이버시권이 침해되기 전부터 이미 대량정보처리

---

17) 개인정보보호규범들이 표현의 자유를 침해할 가능성에 대해서는 파워블로거로 유명한 UCLA의 Eugene Volokh 교수의 논문이 있다. "FREEDOM OF SPEECH AND INFORMATION PRIVACY: THE TROUBLING IMPLICATIONS OF A RIGHT TO STOP PEOPLE FROM SPEAKING ABOUT YOU", 52 Stanford Law Review 1049 (2000). 프라이버시의 대가인 Paul Schwartz가 해당 저널의 같은 호에 반박글을 게재하였다.

18) G.B.F. Niblett, ed., Digital Information and the Privacy Problem (Paris: OECD Informatic Studies No. 2, 1971); Great Britain, Home Office, Report of the Committee on Privacy (London, 1972); Canada, Department of Communications and Department of Justice, Privacy and Computers: A Report of the Task Force (Ottawa, 1972); Sweden, Committee on Automated Personal Systems, Data and Privacy (Stockholm, 1972); United States, Department of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (Washington, D.C., 1973).

19) http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

20) U.S. Privacy Protection Study Commission, Personal Privacy in an Information Society Ch. 13 (1977) http://epic.org/privacy/ppsc1977report/ (2011년9월26일 방문)

21) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

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

23) DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

24) Sandra C. Henderson, Charles A. Snyder, "Personal information privacy: implications for MIS managers", Information & Management 36 (1999) 213-220쪽.

25) 개인을 식별하는 모든 정보를 개인정보로 정하는 정의조항이 우리나라의 정보통신망 이용촉진 및 정보보호에 관한 법률, (구)공공기관의 개인정보 보호에 관한 법률, 개인정보보호법에도 포함되어 있다.

26) 이와 같은 원리를 명시하지 않은 EU 지침에 대해서는 비판이 있다. 2001년 스웨덴정부는 95년 EU 지침에

자에게는 여러 의무가 주어진다. 예를 들어 정보가 정보주체의 허락 없이 유통된다면 프라이버시침해라고 볼 수 없겠지만 개인정보보호법리의 침해는 된다는 식이다.

FIPP는 정작 개인정보보호법제의 발원지인 영미계에서는 보편적인 형태로 법제화가 되지는 않았다. 미국은 Privacy Act of 1974를 통하여 우리나라의 공공기관의 개인정보보호에 관한 법률에 해당하는 법만을 제정하고 공공기관들 사이의 정보공유를 규제하는 Computer Matching and Privacy Act of 1988을 제정하고 국가정보기관들의 생체정보수집을 통제하는 Executive Order 12333을 제정한 후, 사기업이 다루는 정보들에 대해서는 Fair Credit Reporting Act를 포함하여 금융소비자들이 은행 및 금융기관에 제공하는 정보의 프라이버시를 보호하는 일련의 법들, 그리고 의료정보를 다루는 '건강보험 이전 및 책임에 관한 법(HIPAA: Health Insurance Portability and Accountability Act)'등과 같이 내밀한 것으로 인정되는 영역에 대해서만 공정정보처리원칙을 법제화하였다.[27]

결론적으로 개인정보 보호법제는 프라이버시를 침해하는 행위를 직접 규제하는 '행위규제'에 대비되는, 프라이버시의 침해 위험이 높은 행위 즉 자동화된 대량 개인정보의 처리에 대해 절차적 통제를 가함으로써 프라이버시침해의 위험을 구제하는 일종의 '위험규제'라고 볼 수 있다.

## 2. 각국의 위치정보보호법제 현황

위치정보는 다른 개인정보에 비해 유출 및 공개될 경우 프라이버시 침해가 더욱 심대하다는 자각 속에서 각국은 위치정보보호법제를 다음과 같이 마련하게 된다.

### 가. 유럽연합(EU)

EU 국가들 중에서 우리나라처럼 위치정보에 관한 별도의 법률을 제정한 사례는 없다. 대신 EU는 앞서 언급한 「EU 개인정보보호지침」을 통해 개인정보 및 프라이버시 보호의 일반원칙을 마련하고 각 회원국들이 동 지침에 맞게 개인정보보호법제를 정비하도록 강제하여 역내 개인정보보호 수준의 강화를 위해 노력하고 있다. 특히 1997년 동 지침을 보다 구체화한 「프라이버시 및 전자통신에 관한 지침」[28]을 제정하였고, 동 지침은 2002년 위치정보를 비롯한 새로운 전자통신 분야의 개인정보보호 문제들을 다루기 위해 전면개정되었다. 동 지침에 의하면, 위치정보(location data)는 "공개된 전자통신서비스 사용자의 단말기의 지리적 위치를 나타내는, 전자통신네트워크 또는 전자통신서비스에 의해 처리되는 정보"를 말한다.[29] 여기에는 단말기의 위도·경도 및 고도, 이동 방향, 위치정보(location information)의 정확

---

따라 개인정보보호법을 제정하여 시행해본 결과, 95년 지침이 '표현의 자유 및 정보의 자유를 과도하게 제약하며, 수집부터 삭제까지의 모든 단계를 규제하는 방식이 아니라 정보의 남용만을 규제하는 방식으로 규제모델을 바꿔야 한다'는 의견서를 제출하면서 그러한 방식으로 지침을 개정할 것을 요청하였다. Swedish Ministry of Justice, November 26, 2001, "Note in Preparation for the Internal Market Council Meeting on Directive 95/46/EC"

27) 미국의 영역별 개인정보보호법의 최근 현황에 대해서는 U.S. Federal Laws Regarding Privacy and Personal Data, and Applications to Biometrics, NBSP Publication 0105, March 2006. http://www.nationalbiometric.org/publications/US_FederalPrivacyReport0306.pdf (2011년9월26일 최종방문)

28) EU의 「전자통신 부문에서 개인정보의 처리와 프라이버시 보호에 관한 유럽연합 지침 2002/58/EC(프라이버시 및 전자통신에 관한 지침)」: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

29) Directive on privacy and electronic communications Article 2 (c) 'Location data' means any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

도, 일정 시점에 단말기가 위치한 망 셀(network cell)의 확인, 또는 위치정보(location information)가 기록된 시간 등이 포함된다.[30]

「프라이버시 및 전자통신에 관한 지침」 상 전송정보에 속하지 않는 위치정보는 해당 정보를 익명으로 처리하거나 부가서비스(value added service)를 제공하기 위한 목적이라면 부가서비스 제공에 필요한 한도 및 기간에 한해, 사용자 또는 가입자의 동의가 있는 경우에만 처리가 가능하다. 서비스제공자는 동의를 받기 전, 처리할 위치정보의 종류, 해당 처리의 목적과 기간 그리고 부가서비스 제공을 목적으로 그 정보를 제3자에게 전송할 것인지 여부를 사용자나 가입자에게 알려야 한다. 또한 사용자 내지 가입자는 언제든지 위치정보 처리에 대한 동의를 철회할 수 있어야 한다. 그리고 사용자나 가입자의 동의를 이미 받은 경우라도 사용자나 가입자는 네트워크 접속시마다 또는 통신 전송시마다 당해 정보의 처리를  간단한 방법과 무료로 일시적으로 거부할 수 있는 가능성을 계속 보유해야 한다.[31]

그 외에 「전자통신망 및 서비스에 관한 이용자의 권리와 보편적 서비스에 관한 유럽연합 지침 2002/22/EC(보편적 서비스 지침)」[32]은 유럽 공용의 응급전화번호인 112에 응답하는 긴급구조서비스센터에 통신사업자가 발신자의 위치정보를 제공하도록 하고 있다.[33] 이러한 지침들의 내용은 유럽 각국의 개인정보보호법이나 통신법 등에 반영되고 있으며, 개인정보 및 위치정보보호를 위한 기준이 되고 있다.

---

30) Directive on privacy and electronic communications (14) Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded.

31) Directive on privacy and electronic communications Article 9
Location data other than traffic data
1. Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data other than traffic data at any time. (이하 생략)
2. Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.
3. Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be restricted to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

32) Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

33) Universal Service Directive Article 26 paragraph 3. Member States shall ensure that undertakings which operate public telephone networks make caller location information available to authorities handling emergencies, to the extent technically feasible, for all calls to the single European emergency call number "112".

## 나. 미국

미국은 EU와 달리 일반적인 개인정보 보호법을 두지 않고 분야별 또는 특정 개인정보의 보호를 위한 개별법을 제정·시행하고 있다. 미 연방법률 중 우리나라의 위치정보보호법과 같이 위치정보의 수집·사용에 관한 보호 및 규제를 목적으로 한 직접적인 법률은 존재하지 않으며, 범죄 수사 등에 있어 영장 없는 위치정보의 수집·이용이 영장주의를 규정한 미 연방 수정헌법 제4조에 위반하지 않는지 여부가 주로 쟁점이 되어 왔다.[34] 민간영역에서의 위치정보 수집·활용에 대해서도 연방 차원의 규제는 거의 존재하지 않는 상황이다.

물론 미국에서도 위치정보의 보호를 위한 입법 시도가 여러 차례 있어 왔다. 특히 구글과 애플사의 스마트폰을 통한 위치정보 수집 등이 문제되자 미 연방의회는 2011년 5월 이들 회사를 상대로 청문회를 개최한 바 있다. 이를 계기로 미국에서 개인정보와 관련된 법제정비 노력이 본격화 되었는데, 107대 연방의회에 상정된 바 있는 「위치프라이버시보호법안(Location Privacy Protection Act of 2001)」은 수집된 위치정보를 제3자와 공유하기 이전에 사용자의 명시적 동의가 필요하다고 규정하였으나 법제정으로 이어지지는 못하였다.[35] 위치정보보호와 관련하여 제안된 가장 강력하고 포괄적인 법안으로는 「위치프라이버시 및 감시법안(Geolocation Privacy and Surveillance Act)」이라 부르는 연방형법개정안이 있으며, 이 외에도 다수의 위치정보 보호법안이 연방의회에 제안되어 있다.[36]

다만, 통신서비스 분야에서는 「1934년 통신법(Communications Act of 1934)」을 대대적으로 개정한 「1996년 전자통신법(Telecommunication Act of 1996)」이 통신서비스 사용자의 위치정보 보호에 대한 근거를 마련해놓고 있다.[37] 동 법은 전자통신사업자가 통신서비스 제공에 의해 취득한 식별 가능성 있는 "고객소유네트워크정보(CPNI: Customer Proprietary Network Information)"는, 법률에서 규정하거나 고객의 승인이 있는 경우가 아닌 한, 통신서비스를 제공하기 위한 목적에 한해서 이용·공개·제공할 수 있다고 규정하고 있는데(§222(c)(1)),[38] 「1999년 무선통신 및 공공안전법(Wireless Communications and Public Safety Act of 1999)」은 위치정보를 전자통신법에서 규정한 CPNI로 분류하고 있다. 그러나 전자통신법은 CPNI와 관련하여 고객의 승인을 받는 방식이나 시점에 대해서는 명확한 규정을 두고 있지 않음은 물론, CPNI에 해당하는 정보 자체가 매우 제한적이어서 동 법이 적용되는 경우는 많지 않을 것으로 생각된다.[39] 한편, 'E119 Act'라고도 불리는 무선통신과 공공안전법은 전자통신법 제222조를 개정하여, 공공구조기관이 무선사업자들에게 이동전화의 911 발신자 위치정보를 제공하도록 요구할 근거를 마련해두고 있다.

---

34) 박정훈, 123쪽
35) 위치정보의 보호 및 이용 등에 관한 법률 해설서, 방송통신위원회·한국인터넷진흥원, 2010. 1., 10쪽
36) 박정훈, 141쪽
37) 동 법은 이후 「2000년 전자통신법(The Telecommunication Act 2000)」에 의해 미세한 개정이 이루어졌다.
38) The Telecommunication Act 1996 §222 (c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION- (1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS- Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.
39) 박정훈, 125쪽

## 다. 일본

일본은 2005년 4월 1일부터 시행된「개인정보의 보호에 관한 법률(個人情報の保護に關する法律)」을 통해 개인정보 보호를 위한 기본원칙을 마련했다. 동법은 개인정보취급사업자가 개인정보를 전자적으로 처리할 경우 수집목적에 따른 개인정보 취급, 명시적 동의 없는 제3자 제공 금지 등의 의무를 준수토록 하고 있다. 한편 일본 총무성이 발표한「전기통신사업에서의 개인정보보호에 관한 가이드라인」[40]은, 전기통신사업자에게 통신비밀에 속하는 사항 및 기타 개인정보의 적정한 취급에 대하여 가능한 구체적인 지침을 제공하기 위해 제정되었다.

가이드라인은 "위치정보"를 "이동체단말(移動体端末)을 소지한 자의 위치를 나타내는 정보로서 발신자 정보가 아닌 것"이라고 정의하고 원칙적으로 위치정보를 타인에게 제공해서는 안 된다고 하고 있다. 다만 이용자의 동의가 있거나 법원이 발부한 영장에 따르는 경우, 범죄수사 등을 위한 역탐지의 일환으로 제공되는 경우 기타 위법성조각사유가 있는 경우는 제외된다. 그리고 전기통신사업자가 위치정보를 가입자 또는 그가 지시하는 자에게 통지하는 서비스를 제공하거나 제3자에게 제공케 하는 경우에는 이동체단말 소지자의 권리가 부당하게 침해되지 않도록 필요한 조치를 취해야 한다. 전기통신사업자가 보유하고 있는 위치정보는 그것이 개개의 통화와 관련있는 경우에는 통신의 구성요소가 되므로「전기통신사업법」제4조 제1항의 통신비밀로서 보호된다고 해석되고 있다.[41]

## 라. 한국

2004년 12월 29일 국회를 통과한 위치정보보호법은 2005년 1월 27일 공포되어 같은 해 7월 28일부터 시행되었다. 동법은 위에서 보았다시피 EU, 미국, 일본 등 선진국에서도 아직 위치정보에 관한 구체적인 법률이 없는 상황에서 제정된, 위치정보 보호에 관하여 전 세계적으로 유례가 없는 입법이라고 할 수 있다. 대부분의 외국 입법례들은 위치정보를 보호의 대상인 프라이버시의 일부로서 제한적으로 다루고 있으며, 예외적으로 공공구조를 위한 활용 가능성을 열어 두고 있다. 이에 비해 우리나라의 위치정보보호법은 프라이버시 보호 대상인 개인위치정보뿐만 아니라 '익명인의 위치정보' 역시 적용대상으로 하고 있으며, 통신사업자만를 대상으로 하고 있는 해외 입법례와 달리 통신사업자뿐만 아니라 폭넓게 위치정보를 상업적으로 수집·제공 또는 이용하는 기업을 규율하고 있다. 그리고 긴급구조는 물론 해외 입법선례가 없는 재난·재해에 대한 경보발송을 규정하고 있다.[42]

위치정보보호법은 총 6장 43조로 나뉘어 있으며, 법률명에서도 볼 수 있듯이 위치정보의 '보호'와 '이용'을 양축으로 하여 구성되어 있다. 동법은 위치정보의 보호를 위해 위치정보사업 허가제 및 위치기반서비스사업의 신고제 도입, 사업 허가취소·정지 등 행정처분 및 과징금 부과, 이용약관 신고제 도입 등 사업자에 대한 행정적 관리·규제제도를 규정(제2장)하는 한편, 개인위치정보의 수집·이용·제공 등 처리기준과 기술적·관리적 보호조치, 위치정보주체의 권리 등을 명시(제3장)하고 있다. 위치정보의 이용과 관련하여서는 긴급구조와 재해·재난 등의 경보발송 목적으로 위치정보를 이용할 수 있는 법적 근거 규정을 명시(제4장)하고, 위치정보 이용 활성화를 위한 연구·기술개발의 추진, 표준화 추진, 정책 심의 등을 위한 위치정보 심의위원회의 설립·운영 등을 규정(제5장)하고 있다.

---

40) 電氣通信事業における個人情報保護に關するガイドライン(平成 10年 12月 2日 郵政省 告示 第570)
41) 위치정보법 해설서, 12쪽
42) 국립목포대학교, "위치정보 관련 법·제도 개선방안", 한국정보보호진흥원, 2006. 11., 10쪽

### 마. 소결

위에서 보다시피 개인정보 중 위치정보에 대해서 특별법을 제정한 곳은 전 세계에서 우리나라 거의 유일하다. 미국 일본의 위치정보보호법제는 모든 개인위치정보의 처리에 적용되는 것이 아니고 주로 수사기관이 개인위치정보 수집을 하는 행위를 통제하는 법제이다. 유럽의 경우 위치정보도 개인정보보호법제에 의해 보호될 것을 요구하고 있으며 「프라이버시 및 전자통신에 관한 지침」은 기존 개인정보보호법제가 개인위치정보에 어떻게 적용될 것인가에 대한 해석적 지침을 제시하고 있다. 또, 우리나라 위치정보보호법은 개인위치정보가 아닌 새로운 개념인 '위치정보'(즉 익명의 위치정보)도 개인정보보호법제에 포함시키고 있다는 면에서 역시 유일하다. 내용에 있어서도 일반적으로 개인정보보호법제가 개인정보처리자에게 특정한 의무를 사후적으로 부과하는 형태를 띠는 반면, 위치정보보호법은 개인정보처리자에게 사전적인 신고 및 허가의무를 부과한다는 면에서 세계에서 유일하다.

## Ⅲ. 위치정보보호법의 적용범위

### 1. 위치정보보호법의 특수성

위치정보보호법은 위치에 대한 개인정보를 '개인위치정보'라고 정의하여 보호함으로써(제2조 제2호 및 제3장 제2절 전체) 개인정보보호법에 대해 특별법으로 기능한다. 보호방식도 개인위치정보에 대해서는 개인위치정보주체의 동의를 수집시(제18조 제1항), 그리고 이용 및 제공시(제19조) 반드시 얻도록 하고 있으며 정정 열람권 등의 개인위치정보주체의 권리 등도(제24조) 개인정보보호법과 거의 동일한 내용을 담고 있다. 구체적으로 위치정보보호법은 "누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니 된다(제15조)"[43]고 하여 '특정 개인의 위치정보'가 아니라 '특정되지 않은 개인의 위치정보'의 취득마저도 그 개인을 찾아서 그의 동의를 얻도록 요구하고 있다. 또한 '이동성이 있는 물건'의 경우에도 소유주를 찾아 그의 동의를 얻도록 요구하고 있다.

그런데 '특정되지 않은 개인의 위치정보'는 개인정보라고 보기 어렵다. 일반법인 개인정보보호법은 정보주체를 식별할 수 없는 정보 즉 익명화된 정보는 개인정보의 정의에서 배제하고 있는데,[44] 그렇다면 개인정보보호법제의 하나인 위치정보보호법은 개인정보보호법제가 보호하지 않는 정보를 보호하고 있는 것으로 보인다. 또한 '이동성이 있는 물건의 위치정보' 역시 그 소유주가 특정되어 있다면 그 소유주의 물건의 위치는 소유주 '개인에 대한 정보'이므로 개

---

43) 제15조(위치정보의 수집 등의 금지) ① 누구든지 개인 또는 소유자의 동의를 얻지 아니하고 당해 개인 또는 이동성이 있는 물건의 위치정보를 수집·이용 또는 제공하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 제29조제1항에 따른 긴급구조기관의 긴급구조요청 또는 같은 조 제7항에 따른 경보발송요청이 있는 경우
2. 제29조제2항에 따른 경찰관서의 요청이 있는 경우
3. 다른 법률에 특별한 규정이 있는 경우
② 누구든지 타인의 정보통신기기를 복제하거나 정보를 도용하는 등의 방법으로 위치정보사업자등을 속여 타인의 개인위치정보를 제공받아서는 아니 된다.
③ 위치정보를 수집할 수 있는 장치가 부착된 물건을 대여하는 자는 위치정보 수집장치가 부착된 사실을 대여받는 자에게 고지하여야 한다.

44) 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1. "개인정보"란 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)를 말한다.

인정보라고 볼 수 있다. 하지만 소유주가 특정되어 있지 않다면 개인정보라고 볼 수 없다. 그렇다면 특정물건의 소유자가 누구인지 식별하지 않고 그 위치를 추적하면 개인정보보호법 상으로는 개인정보취득에 포함되지 않지만 위치정보보호법은 그러한 위치추적에 있어서 동의를 얻도록 의무화하는 것이다.

위와 같은 조항이 발생시키는 문제는 쉽게 예측할 수 있다. 우리 중의 누군가가 길거리에서 매우 특이하게 주차된 차량을 발견했다고 가정하자. 차량은 이동성이 있는 물건이므로 그 차량이 발견된 위치 등의 정보를 스마트폰의 GPS기능을 통해 '수집'하여 그 정보와 함께 사진을 트위터나 페이스북 등에 올리는 행위는 위치정보보호법 제15조 위반이 되어 최고 3년 징역에 처해질 수 있다.[45] 차량번호판을 모자이크 처리하여 가렸다고 할지라도 그러하다. (위치정보사업자나 위치기반서비스사업자의 경우) 차량번호판을 그대로 보여줬다면 위 차량의 장소는 '개인위치정보'가 되어[46] 더욱 엄하게 처벌되겠지만,[47] 이를 보여주지 않고 익명화하더라도 위치정보보호법 제15조 위반에 해당한다. 또는 환경운동을 하는 사람이 우림지대의 벌목기계 위치를 측정하는 것 역시 '이동성있는 물건'의 위치를 측정하는 것이 되므로 벌목회사의 동의를 얻지 않으면 역시 제15조 위반에 해당한다.

결국 익명인의 (또는 익명인의 물건의) 위치정보를 보호하는 것이 과연 개인정보보호법제의 입법취지에 부합하는 것인가의 문제가 발생한다.

## 2. 개인정보보호법에 대한 해석

위치정보보호법이 보호대상인 위치정보를 이렇게 폭넓게 정의하게 된 것은 우연이나 착오에 의한 것이 아니다. 위치정보보호법은 외국에서는 보편화되기 시작했던 개인정보보호법이 국내에 도입되기 이전에 위치와 관련된 개인정보에 대해서만 우선적인 보호체제를 갖추기 위하여 제정된 일종의 특별법이다. 그런데 개인정보보호법제 내에서도 이미 국내와 국외를 가리지 않고 '개인정보'의 정의에 대해 엄청난 혼란이 존재하고 있었는바, 이 혼란이 위치정보보호법 내로 고스란히 옮겨온 것이라고 볼 수 있다.

### 가. 개인정보의 문언적 정의

누구에 대한 정보인지 모르는 정보들의 목록 그 자체는 개인정보보호법제의 보호대상인가

---

45) 제40조(벌칙) 다음 각 호의 1에 해당하는 자는 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처한다.
4. 제15조 제1항의 규정을 위반하여 개인의 동의를 얻지 아니하고 당해 개인의 위치정보를 수집·이용 또는 제공한 자

46) 제18조(개인위치정보의 수집) ① 위치정보사업자가 개인위치정보를 수집하고자 하는 경우에는 미리 다음 각 호의 내용을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다.
1. 위치정보사업자의 상호, 주소, 전화번호 그 밖의 연락처
2. 개인위치정보주체 및 법정대리인(제25조 제1항의 규정에 의하여 법정대리인의 동의를 얻어야 하는 경우에 한한다)의 권리와 그 행사방법
3. 위치정보사업자가 위치기반서비스사업자에게 제공하고자 하는 서비스의 내용
4. 위치정보 수집사실 확인자료의 보유근거 및 보유기간
5. 그 밖에 개인위치정보의 보호를 위하여 필요한 사항으로서 대통령령이 정하는 사항
② 개인위치정보주체는 제1항의 규정에 의한 동의를 하는 경우 개인위치정보의 수집의 범위 및 이용약관의 내용 중 일부에 대하여 동의를 유보할 수 있다.
③ 위치정보사업자가 개인위치정보를 수집하는 경우에는 수집목적을 달성하기 위하여 필요한 최소한의 정보를 수집하여야 한다.

47) 제39조(벌칙) 다음 각 호의 1에 해당하는 자는 5년 이하의 징역 또는 5천만 원 이하의 벌금에 처한다.
3. 제18조 제1항·제2항 또는 제19조 제1항·제2항·제4항의 규정을 위반하여 개인위치정보주체의 동의를 얻지 아니하거나 동의의 범위를 넘어 개인위치정보를 수집·이용 또는 제공한 자 및 그 정을 알고 영리 또는 부정한 목적으로 개인위치정보를 제공받은 자

아닌가? 위 질문에 대한 답이 '그렇다'라면 누구인지 모르는 사람의 위치와 누구의 것인지 모르는 물건의 위치도 당연히 개인정보보호법제의 대상이 되므로 위치정보보호법 제15조는 정당화된다. 그러나 답이 '아니다'라면 해당 조항은 악법이 된다. 그렇다면 개인정보보호법 스스로는 이에 대해 정확한 답을 제공하고 있는가? 우선 국내에서는 이에 대한 많은 혼란이 있는 것으로 보인다.

개인정보보호법은 개인정보의 정의를 "(b)살아 있는 개인에 관한 정보로서 (a)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)"라고 하여, 개인정보가 2가지 정보의 조합으로 이루어졌음을 알 수 있다. 첫째 위의 (b)에 해당하는 개인에 관한 정보이다. 그리고 위의 (a) 즉 "개인을 알아볼 수 있게 해주는 성명, 주민등록번호, 영상 등"에 해당하는, 위의 "개인에 관한 정보"에서 "개인"을 표창하는 정보 즉 식별자(identifier)이다. 그렇다면 개인정보는 당연히 (b) 개인에 관한 정보와 (a) 그 개인의 식별자의 조합으로 이루어져야 비로소 개인정보라고 할 수 있다.

이는 "정보"에 대한 일반적 통념과도 일치한다. 즉 정보는 어떤 의미를 가져야 하고 어떤 말이 의미를 가지기 위해서는 주어와 서술어가 있어야 한다. 시각적 정보 예를 들어 얼굴사진의 경우 얼굴의 소유자가 주어의 역할을 하고 얼굴의 사진이 서술어의 역할을 하게 된다. 위에서 해당 개인의 식별자가 "주어", 그리고 그 개인에 대한 정보가 "서술어" 역할을 하게 된다.

### 나. 개념적 혼돈

하지만 실무에서는 예를 들어 소유주의 이름이 나타나 있지 않은 전화번호 목록 등도 개인정보라는 인식이 존재한다. 즉 전화번호를 "개인에 관한 정보(b)"라고 했을 때 "그 개인이 누구인지 알아볼 수 있는 정보(a)"인 예를 들어 '성명'과 같은 식별자가 없어도 이를 개인정보라고 생각하는 것이다.

이런 인식은 개인정보보호법이 개인을 식별하는 매개인 정보들 중에서 주민등록번호 등과 같이 소위 "고유식별정보"에 대해 그 번호의 소유자에 대한 여타의 정보가 없이도 그대로 처리에 대해 제한을 두고 있다는 점[48]과 무관하지 않은 것으로 보인다. 즉 주민등록번호나 여권번호와 같이 "개인에 관한 정보"가 매칭되어 있지 않아도 법이 개인정보성을 부여한 것이다. 이에 따라 법은 주민등록번호 소유자에 관한 아무런 정보가 부기되지 않은 단순한 주민등록번호를 처리할 경우에도 번호 소유자를 찾아서 동의를 얻어야 할 의무를 부과한다. 다시 말하면, "개인정보 = (b) 개인에 관한 정보 + (a) 그 개인의 식별자"라는 등식의 유일성이 깨지고

---

48) 제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 "고유식별정보"라 한다)를 처리할 수 없다.
1. 정보주체에게 제15조 제2항 각 호 또는 제17조 제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우
2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우
시행령 제19조(고유식별정보의 범위) 법 제24조 제1항 각 호 외의 부분에서 "대통령령으로 정하는 정보"란 다음 각 호의 어느 하나에 해당하는 정보(이하 "고유식별정보"라 한다)를 말한다. 다만, 공공기관이 법 제18조 제2항 제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.
1. 「주민등록법」 제7조 제3항에 따른 주민등록번호
2. 「여권법」 제7조제1항 제1호에 따른 여권번호
3. 「도로교통법」 제80조에 따른 운전면허의 면허번호
4. 「출입국관리법」 제31조 제4항에 따른 외국인등록번호

단순히 “개인정보 = (a) 개인의 식별자”라는 등식도 가능해진 것이다.

그런데 재미있는 것은 주민등록번호는 “개인의 식별자”로 기능하기도 하지만 “그 개인에 관한 정보”로 기능할 수도 있다. 즉 주민번호가 성명과 조합된다면 성명이 “식별자”로 그리고 주민번호가 “그 식별자가 표창하는 개인에 관한 정보”로 기능할 수도 있는 것이다. 사실 주민등록번호만으로는 누구인지 알 수 있는 방법이 없지만 성명을 알면 전화번호부 등을 통해 해당 개인을 찾아낼 수 있으므로 성명이 “식별자” 역할을 하고 주민번호가 그 개인에 관한 정보로 기능하는 경우가 더 설득력이 있다고 하겠다.

그렇다면 위의 일반적인 인식을 통해 새로이 성립된 개인정보의 정의의 가능성은 두 가지가 된다. 즉 “개인정보 = (b)개인의 식별자” 또는 “개인정보 = (a) 개인에 관한 정보”이다. 여기서 위치정보보호법의 제15조는 바로 후자의 가능성에 대응됨을 알 수 있다. 즉 개인의 식별자가 없는 상황에서 그 개인에 관한 정보(위치정보)에게 개인정보성을 부여한 것이다. 그렇다면 위와 같은 새로운 개인정보의 정의는 타당한 것인가?

이와 같은 개념적 혼돈은 개인정보보호법제의 원산지인 미국 내에서도 나타난다. 우선 National Institute of Standards and Technology(NIST)의 개인식별정보보호지침(SP 800-122)[49]은 보호대상 정보를 personally identifiable information이라 하여 “홀로 또는 다른 정보와 결합하였을 때 사람의 신원을 식별해낼 수 있는 정보”라고 정의하고 있다. 반면 캘리포니아주의 개인정보유출통지법(SB 1386)[50]에서는 보호대상 정보를 personal data라 하여 “이름과 〔다른 개인고유번호〕의 조합”으로 정의하고 있다.

위키피디어에 따르면 이 2개의 정의는 완전히 다른 것이다.[51] 사람의 이름 자체도 실존인물의 것이라면 NIST 정의에 따르면 보호대상이 되지만 SB 1386 정의에 따르면 “맥락이 없는(lacks context)” 이름 자체는 아무런 “의미가 없어(has no meaning)” 보호대상정보가 되지 않는다. 즉 “홍길동”이라는 것은 사물의 표지일 뿐 그 자체가 정보일 수는 없는 것이다. “홍길동은 간염치료를 받았다”는 서술이 있어야 비로소 정보로 인정이 된다. 또 사회복지번호(Social Security Number) 역시 그 번호소유자의 이름이나 다른 신원정보와 조합되어 있지 않다면 그 자체로는 SB 1386 상의 보호대상정보가 되지 않지만 NIST 정의 상으로는 보호대상이 된다. 그러나 이름과 사회복지번호의 조합은 SB 1386 상의 보호대상정보가 된다. 그러한 조합은 “그 이름의 사람이 해당 사회복지번호를 가지고 있다“라는 의미를 가지게 되기 때문이다. HIPPA 역시 우선 건강정보(health information)에 식별자(identifier)가 존재하면 보호대상정보로 본다. 즉 ”사회보장번호 123-45-6789인 사람이 간염치료를 받았다“는 완성된 서술이 가능한 경우만을 보호대상정보로 본다.

그렇다면 SB 1386식의 접근법과 NIST접근법 중 어느 것이 개인정보보호법제의 취지에 충실한 것일까?

일견 우선 프라이버시 보호라는 원래의 측면에서 살펴보자면 SB 1386이 더욱 충실한 것으로 보인다. 프라이버시는 특정사람에 대한 정보에 의해 훼손되는 것이지 익명인의 프라이버시를 침해하는 것은 불가능하다. 결국 즉 주어와 서술어가 존재하는 명제만을 규제한다고 볼 수 있다. 그러나 문제는 그렇지 간단하지는 않다.

---

49) http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

50) http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html
이 법의 해설로는 http://www.oit.ucsb.edu/committees/itpg/sb1386.asp

51) http://en.wikipedia.org/wiki/Personally_identifiable_information

### 다. 개인정보보호법제의 목표[52]에 따른 해석

위에서 우리는 개인정보보호법제를 사생활의 비밀에 대한 위험규제라고 규정하였다. 개인정보보호법제의 위험규제로서의 성격은 개인정보보호법제의 적용범위를 축소시키는 해석과 확대시키는 해석 두 가지 모두를 가능하게 한다.

#### (1) 축소해석

우선 축소해석에 관하여 보자면, 우리나라 개인정보보호법 제정의 근간이 되었던 OECD 가이드라인[53]과 EU 개인정보보호지침[54] 모두 개인정보의 정의는 우리나라의 그것과 다르지 않아 식별가능한 개인에 대한 모든 정보'를 개인정보라고 정의하고 있다. 그런데 OECD가이드라인과 EU개인정보보호지침을 살펴보면 프라이버시침해의 개연성이 없는 개인정보에는 적용되지 않도록 하려는 노력이 엿보인다.

즉 1980년 OECD가이드라인은 개인정보를 개인을 식별할 수 있는 모든 정보로 정의하되, 개인정보처리자의 의무가 적용되는 개인정보처리의 범위를 '자동화된 처리'로 최소보호수준을 좁히고 있으며, 서문에서 개인정보의 범위도 '프라이버시 및 개인의 자유를 침해할 개연성이 있는 정보'만으로 한정하고 있다. 그리고 개인정보권의 내용에 있어서도 다른 차이도 있겠지만 가장 눈에 띄는 것은 개인정보의 수집에 있어서도 동의를 의무화하고 있지 않다. 프라이버시의 보호와 무관한 경우에는 동의를 얻을 필요 없다는 의미로 해석된다.

또 EU개인정보보호지침 역시 개인정보는 개인을 식별할 수 있는 모든 정보로 폭넓게 정의하되 서문에서 그 규제목표는 '프라이버시권'의 보호임을 천명한 후에 적용범위에 있어서 ① 자동화된 시스템이나 ② 자동화되어 있지 않다면 구조화된 파일링시스템에만 적용된다고 한정하고 있다. 즉 개인정보라고 할지라도 위와 같이 자동화 또는 구조화된 파일링시스템에 속한 개인정보에만 법이 적용된다고 하는 것이다. 또 개인정보의 수집에 있어서는 동의를 의무화하고 있지만 이익형량을 통해 "개인정보처리자의 이익이 정보주체의 이익보다 우선할 경우" 정보주체의 동의를 얻을 의무가 면제되며 해석상 이 이익형량에서 정보주체의 이익은 지침이 전문에서 그 중요성을 밝히고 있는 프라이버시권이 된다. 즉 모든 자동화된 시스템이나 구조화된 파일링시스템에서 처리되는 개인에 대한 정보의 경우 우선적으로 모두 개인정보보호권이 적용되기는 하나, 개인정보보호권의 가장 대표적인 의무인 수집동의권의 경우 정보주체의 프라이버시가 정보처리자의 이익(예를 들어, 표현의 자유)에 앞설 경우에만 적용된다. 그렇다면 역시 적어도 개인정보보호권의 가장 중요한 요소인 수집동의권은 프라이버시권의 침해 개연성이 있는 정보에만 적용된다고 보는 것이 합당하다.

위와 같은 축소해석의 입장에서는 위치정보보호법이 개인위치정보가 아닌 위치정보를 보호하는 것은 위의 개인정보보호법제들이 적용범위에서 배제하려고 노력하고 있는 '프라이버시 침해의 개연성이 없는 정보'를 보호하려는 것이 된다.

#### (2)확장해석

하지만 거꾸로 위험규제이기 때문에 입법자는 개인에 관련된 모든 정보를 개인정보라고 폭

---

52) 박경신, "사생활의 비밀의 절차적 보호규범으로서의 개인정보보호법리", 공법연구 제40집 제1호 (2011년 10월), 130-162쪽의 일부를 전재한 것임.

53) "personal data" means any information relating to an identified or identifiable individual (data subject)

54) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

넓게 정했을 수도 있다. 예를 들어, 서술어가 없이 단지 주어만 있다거나 주어가 없이 서술어만 있는 경우에도 결국 특정인과 대응만 된다면 보호대상으로 보는 것이다. 여타의 정보와 조합되지 않은 주민등록번호 자체도 추후에 사생활침해의 매개가 될 수 있으니 보호되어야 한다는 것이다. 이런 논리라면 개인위치정보가 아닌 위치정보 그 자체도 보호대상이 될 수 있다.

실제로 이름, 주민등록번호와 같이 그 자체로 고유한 사람을 지정하는 정보는 그 자체로 그러한 사람이 존재한다는 명제가 공개되는 것과 마찬가지가 될 수 있다. 즉 해당 정보의 수집과 동시에 우리는 그런 주민번호를 가진 사람이 존재한다는 개인에 관한 정보를 얻게 된다고 볼 수도 있다. 그리고 이름, 사회보장정보를 특정 사업자가 가지고 있다는 사실 자체도 "해당 사업자와 거래가 있었다"는 "개인에 관한 정보"가 될 수도 있다. 이렇게 생각한다면 사실 순수한 이름, 주민등록번호도 해당 사업자가 수집했다는 정보와 그런 사람이 존재한다는 정보를 담고 있다.

재미있는 것은 그러한 논리도 사실 개인정보는 (a)개인의 식별자 + (b)그 개인에 대한 정보로 구성된다는 정의에 대한 예외가 아니라 그 정의를 충족시킴으로써 '익명인에 대한 정보'에게 개인정보성을 부여한다. 그렇다면 같은 논리로 익명인의 위치정보 역시 개인정보보호법제의 보호대상이 될 수 있을까?

### 라. "익명인의 정보"의 개인정보성

실제로 NIST접근법에서도 주어가 없이 서술어만 있어도 맥락과 의미를 가질 수 있다. 예를 들어 "2010년 호프앤웰빙병원에서 AIDS치료를 받고 2011년에 다시 같은 병원에서 간염치료를 받은 사람"이라는 것은 어떤 사람의 표지라고 볼 수도 있지만 그런 사람이 존재한다면 "2010년에 호프앤웰빙병원에서 AIDS치료를 받은 사람이 2011년에 다시 같은 병원에서 간염치료를 받았다"는 서술과 등가가 된다. NIST접근법의 마지막 항목이 바로 이와 같은 정보들이다.[55] 이때 "2010년 호프앤웰빙병원에서 AIDS치료를 받은 사람"이 한 명 밖에 없다면 그 문구가 (b) 식별자가 되어 "2011년에 호프앤웰빙병원에서 치료를 받았다"는 (a) 개인에 관한 정보를 공개함으로써 프라이버시가 침해되는 것으로 인정될 수 있다.

NIST접근법의 다른 항목들은 어떠할까? 더욱 깊이 상상해보자면 "사회보장번호 123-45-6789" 역시 그 사람이 존재한다면 "사회보장번호의 앞 다섯자리가 123-45인 사람의 뒤의 네 자리가 6789이다"라는 식으로 쪼개어 생각해볼 수도 있다. 하지만 이렇게 쪼개면 사회보장번호의 앞 다섯자리가 123-45인 사람의 숫자가 많을 경우 해당 개인을 식별해낼 수가 없다. "2010년 호프앤웰빙병원에서 AIDS치료를 받은 사람"의 숫자가 많지 않아 그 사람에 대한 프라이버시를 침해하는 것과는 다른 것이다.

결국 어떤 정보가 개인정보가 되기 위해서는 정보가 주어와 서술어를 갖춘 구조를 갖추고 있는가가 중요하다기 보다는 어차피 주어-서술어 조합을 다양하게 구성할 수 있다는 전제 아래서 주어 부분 만으로 특정 개인을 식별할 있는 주어-서술어 조합이 있는가가 문제가 된다.

예를 들어 순수한 이름들의 목록의 경우를 생각해보자. "박"이라는 성을 가진 사람이 "경신"이라는 이름을 가지고 있다는 것은 하나의 주어-서술어조합이다. 그러나 "박"씨 성을 가진 사람이 우리나라에 수백만 명이 있는 상황에서 제대로 된 표지를 구성하지 못한다. 그렇다면

55) Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

이는 개인정보라고 볼 수 없다.

그렇다면 주민번호의 조합들은 어떠할까? 주민번호는 앞번호가 생년월일 그리고 뒷번호가 출생지와 관련된 번호로 이루어져있다. 그렇다면 쉽게 생각해볼 수 있는 주어-서술어 조합은 "1971년1월5일에 태어난 사람의 주소지가 1180176이다"라는 문장이다. 하지만 우리나라 인구 5천만 중에 해당 생년월일인 사람이 몇 천명은 될 것이므로 특정 자체가 불가능하다.

얼굴사진에 대해서 생각해보자. 우선 얼굴사진은 그 자체로 윤곽을 잡아 누구인지 식별할 수도 있지만 그 이후에도 얼굴의 디테일에 대한 정보를 얻을 수 있다. 생체측정정보(biometric data) 역시 마찬가지이다. 이에 대해서는 EU개인정보보호지침에 대한 실무그룹에서도 그 이중적 특성을 언급한 바 있다.[56] 사실 엄밀하게 말하면 얼굴도 생체측정정보 중의 하나이다. 우선 특정가능성있는 표지가 추출될 수 있고 그 나머지로도 그 표지의 대상에 대한 정보가 존재한다면 이는 개인정보에 해당되는 것이다.

현재의 개인정보보호법 상의 개인정보의 정의도 위와 '개인을 특정할 수 있는 정보'라 함은 정보를 주어-서술어의 다양한 조합으로 전환시켜보았을 때 주어 부분이 고유한 개인의 표지가 될 수 있고 나머지에 서술부분이 남아있는 경우에 개인정보라고 볼 수 있어야 한다. 그렇다면 여타의 정보가 매칭되어 있지 않은 전화번호의 목록이나 주민번호의 목록도 그것 자체로 개인정보라고 볼 수 없는 것은 아니고 누가 수집하였는가에 따라 수집자가 밝혀진 상황에서는 "해당 전화번호나 주민번호의 소유자가 해당 수집자와 거래를 했다"는 서술부가 구성이 된다.

## 3. 위치정보보호법 상의 '위치정보'

### 가. '위치정보'의 정의

그렇다면 위치정보보호법은 어떠한가. 개인위치정보와 달리 순수한 위치정보 자체가 그러한 위험이 있을까. 그러한 위험이 있을 수도 있고 없을 수도 있다. 예를 들어 며칠 간의 트래킹 데이터의 경우 저녁에 매일 같은 곳에 있다고 가정할 때 wifi access point방식이라면 그것은 주소를 알 수 있는 것과 마찬가지이고 그렇다면 그 주소로부터 개인을 확정할 가능성이 있다. 그렇다면 낮의 위치정보들은 그 주소에 있는 사람이 해당 장소에 다녔다는 '정보'가 될 수 있다.

결국 위치정보보호법 상 위치정보의 정의도 개인을 확정할 수 있는 표지가 추출되어야만 비로소 프라이버시 보호라는 개인정보보호법의 목적에 합당하다고 볼 수 있을 것이다. 현재의 위치정보보호법은 개인위치정보와 위치정보를 별도로 정의함으로서 위와 같은 고유표지추출 가능성이 있는 정보는 모두 '개인위치정보'의 범주에 넣기 때문에 나머지 '위치정보'는 그러한 고유표지추출 가능성이 없는 것만 남게 되며 법적 보호가 불필요해진다.

위치정보보호법의 '위치정보'의 개념적 문제는 기본적으로 주어-서술어 구조 또는 (a) 개인의 식별자 (b) 그 개인에 관한 정보의 구조를 가져야 하는 개인정보의 요건을 정면으로 부인하고 주어나 (a)개인의 식별자가 없는 상태임에도 불구하고 개인정보의 지위를 부여받는다는 것이다 이렇게 위치정보보호법상 위치정보의 정의 규정은 지나치게 광범위하고 포괄적이어서 제한이 필요하다.[57]

---

56) ARTICLE 29 DATA PROTECTION WORKING PARTY, 01248/07/EN WP 136, Opinion 4/2007 on the concept of personal data (June 20, 2007)

57) 같은 비판으로는 조용혁, "개인위치정보의 보호에 관한 법률적 고찰", 정보화정책 제12권 제2호, 2005, 136쪽

### 나. 개선방안

현재의 위치정보보호법에 의하면 업체들이 익명화된 위치정보 즉 위치정보의 주체를 파악할 수 없거나 파악하지 않는 상황에서 위치정보를 수집하는 방식의 서비스가 원천적으로 불가능하다. 즉 통신사의 아이디(ID), 전화번호, 이동전화의 고유번호(IMEI), 랜카드의 맥(MAC)주소, IP주소, 쿠키(cookie)등 개인식별성이 떨어지는 정보 만을 수집하는 위치기반서비스업이 불가능해진다. 왜냐하면 위치정보보호법은 위치정보의 주체를 색출해내어 동의를 얻을 것을 요구하고 있기 때문인데, 동의를 얻는 과정에서 이미 위치정보의 주체가 파악될 수 밖에 없고 결국 이 위치정보는 개인위치정보가 되어버린다. 예컨대 의료정보가 민감하다고 하여 누구의 것인지 모르는 의료정보를 수집하거나 처리하고자 할 때마다 해당 환자를 찾아내어 동의를 먼저 얻으라는 규제에 비교해볼 수 있다.

특히 법은 “위치정보사업자”나 “위치정보기반사업자”를 “개인위치정보”의 수집이나 이용을 업으로 하는 자나 “위치정보”의 수집을 업으로 하는 자로 정의하고 있다. 즉 “개인위치정보”가 아닌 “위치정보”만을 수집하더라도 허가나 신고의 의무를 갖게 된다. 이는 과도한 의무부과가 아닐 수 없다.

따라서 위치정보보호법의 보호대상은 개인정보보호법과의 대비선상에서 “(1)개인의 위치에 관한 정보로서 (2) 그 개인을 알아볼 수 있는 정보(그 개인을 해당 정보만으로는 알아볼 수 없더라도 위치정보사업자나 위치정보기반사업자가 보유하고 있거나 일반적으로 공개되어 있는 정보와 쉽게 결합하여 알아볼 수 있는 정보)”로 정의되어야 한다. 그리고 이는 입법취지상 “개인위치정보”에 대응하는 것이므로 “개인위치정보”의 정의를 위와 같이 바꾸고 “위치정보”라는 개념은 위치정보보호법에서 모두 삭제되거나 “개인위치정보”로 바뀌어야 한다.

## Ⅳ. 허가제/신고제 및 즉시통보의무

### 1. 허가제/신고제의 문제점

위치정보보호법은 개인의 위치정보가 그 사람의 사생활의 비밀을 침해할 수 있어 위치정보를 수집 및 이용하는 업자에게 허가제 및 신고제를 적용하고 있다. 이중에서 직접 위치정보를 수집하여 이를 제공하는 업자를 ‘위치정보사업자’로, 이렇게 제공받은 위치정보를 이용하는 업자를 ‘위치정보기반사업자’로 분류하고 전자는 허가제로 후자는 신고제로 규율하고 있다.

여기서 ‘위치정보사업’은 위치정보를 수집하여 위치정보기반사업자에게 제공하는 업을 말하는데 ‘위치정보’는 “이동성이 있는 물건 또는 개인이 특정한 시간에 존재하거나 존재하였던 장소에 관한 정보로서 「전기통신사업법」 제2조 제2호 및 제3호에 따른 전기통신설비 및 전기통신회선설비를 이용하여 수집된 것”을 말한다. 방송통신위원회는 “전기통신설비 및 전기통신회선설비를 이용하여 수집된 정보”에는 휴대전화, RFID, GPS 등 각종 전기통신설비 및 회선설비를 이용하여 수집된 정보가 포함되며, 대면상 구두로 수집하거나 사진촬영을 통해 수집한 정보 등은 제외된다고 하고 있다.[58]

그런데 GPS위치정보의 경우 전기통신설비나 전기통신회선설비를 통해 수집되지 않는다.[59] GPS위치정보는 미국군사위성이 송신하는 시간별 위성의 위치정보를 포착하여 위치정보와 그 위치정보가 도착하는 시간을 이용하여 자신의 위치를 계산하는 수신기와 간단한 소프

58) 위치정보법 해설서, 19쪽

59) EU개인정보보호실무위원회도 똑같은 의견이다. ARTICLE 29 Data Protection Working Party, 881/11/EN WP 185, Opinion 13/2011 on Geolocation services on smart mobile devices (16 May 2011)

트웨어만 있으면 충분히 수집가능하다. 물론 이와 같은 수신기와 소프트웨어는 전기통신설비라고 말할 수 없다. 이와 같은 일방적인 수신기가 전기통신설비라면 라디오 및 텔레비전 등도 모두 전기통신설비로 규정되어야 할 것이다. 그렇다면 사실 GPS기능이 있는 스마트폰을 이용해서 제공되는 위치기반서비스와 관련되어서는 위치정보사업자는 더 이상 존재하지 않는다. 물론 GPS만으로는 위치정보가 실내 등에서는 정확하지 않아 기지국추적과 wifi access point기법으로 보완하기는 한다.

위치정보사업을 허가제로 한 것은 (1) 이 법이 제정되었던 2005년 당시 민간기업이 다루는 개인정보를 규율하는 개인정보보호법이 존재하지 않는 상황에서, (2) 위치기반서비스를 제공하는 주요사업자는 이동통신사업자였고, 대부분의 위치기반서비스가 개인위치정보를 활용하고 있었기 때문이었다. 과점적 지위를 가진 이동통신사업자가 가입자 휴대폰의 접속 기지국 위치를 이용하여 가입자들의 개인위치정보를 광범위하게 수집할 수 있다는 사실은 규제의 초점이 국민의 사생활의 비밀에 대한 침해 방지에 맞추어지도록 하였다.

그러나 현재는 (1) 개인정보보호법이 시행되고 있고, (2) 또 휴대폰제조업체들이 휴대폰 사용자가 이통사들을 통하지 않고 스스로 자신의 위치정보를 파악할 수 있도록 하는 기능을 휴대폰에 탑재시키면서 훨씬 더 많은 업자들이 이 위치정보를 기반으로 하여 다양한 서비스를 제공할 수 있게 되어 위치정보의 과점 문제는 발생하지 않는다. 또한 버스 등 물건의 위치정보만을 활용하는 서비스도 증가하는 추세이다.

또한 다른 개인정보에 대해서는 적용되지 않는 허가제와 신고제는 규제 형평성에 있어 문제가 되고 있다. 특히 개인정보보호법 위반에 대해서는 형사처벌이 거의 없으나 위치정보를 다루는 업체들에 대한 형사처벌이 집중적으로 이루어지면서 IT업계가 위치정보 이용에 있어서 위축되어 있는 상황이다. 게다가 익명화된 위치정보를 다루고자 하는 업체들도 모두 허가 및 신고제의 질곡에서 자유롭지 못하다. 이렇듯 개인정보보호법이 정보주체를 식별해낼 수 있는 내용이 들어있는 정보(즉 “개인정보”)만을 보호대상으로 삼고 있는 것에 비하여, 위치정보보호법은 정보주체를 식별하지 않는 위치정보 마저도 보호대상으로 삼고 있음은 물론 허가제 및 신고제로 규율하고 있어 위치정보의 이용을 매우 다른 정보와 불균형하게 위축시키고 있다.

이에 따라 허가/신고제가 위치정보를 이용한 더욱 다양한 서비스의 제공과 비즈니스모델의 개발에 걸림돌이 되고 있는지 판단이 필요하다. 정부도 이러한 문제의식을 가지고 2011년 4월 제18대 국회에 위치정보법 개정안을 제출한 바 있으나 아쉽게도 폐기되었다. 동 개정안은 개인위치정보를 대상으로 하지 아니하는 사업으로서 방송통신위원회가 정하여 고시하는 기준에 해당하는 경우에는 허가 또는 신고 없이 위치정보사업 또는 위치기반서비스사업을 할 수 있도록 하였다. 국회문화체육관광방송통신위원회는 개인위치정보를 취급하지 않는 위치정보사업자 및 위치기반서비스사업자에 대해서도 일괄적으로 허가 및 신고제를 적용하여 국민의 사생활 침해와 무관한 사업자에 대해서까지 진입장벽을 두는 것은 다양한 응용서비스의 개발과 사업화에 악영향을 미칠 우려가 있음을 표명했다.[60]

## 2. 즉시통보의무의 문제점

위치정보보호법은 위치기반서비스사업자가 위치정보를 이용할 때 매회 위치정보주체에게 통지를 하도록 하고 있다.[61] 이와 같은 의무는 실제 위치정보서비스의 제공 시 서비스의 질

60) 위치정보의 보호 및 이용 등에 관한 법률 일부개정법률안 검토보고서, 국회문화체육관광방송통신위원회, 2011. 11., 9쪽
61) 제19조(개인위치정보의 이용 또는 제공) ① 위치기반서비스사업자가 개인위치정보를 이용하여 서비스를 제공하고

을 저하시킨다. 특히 위치의 변화에 따라 자동적으로 특정 정보가 제공되는 서비스의 경우 이용자가 매회 위치의 변화에 따른 동의를 해주지 않으면 서비스가 제대로 기능을 하지 않고 그 서비스의 시장에서의 경쟁력을 구성하는 자동성 자체가 없어지게 된다. 또 위치가 연속적으로 변하는 경우 '매회'를 어떻게 이해해야 하는지도 불분명하다.

이와 같은 규제는 EU의 「프라이버시 및 전자통신에 관한 지침」이 "사용자나 가입자의 동의를 이미 받은 경우라도 사용자나 가입자는 네트워크 접속시마다 또는 통신 전송시마다 당해 정보의 처리를  간단한 방법과 무료로 일시적으로 거부할 수 있는 가능성을 계속 보유해야 한다."는 내용에서 유래하는 것인데 "정보의 처리를 거부할 수 있는 가능성을 보유한다"는 것과 매회 정보처리에 대해 동의를 얻으라는 것은 문언적으로 차이가 있다. 「프라이버시 및 전자통신에 관한 지침」에 대한 실무위원회도 언제라도 이용자가 정보의 처리를 중단할 권한을 가지고 있어야 한다는 것이라고 설명하고 있다.[62]

위치정보보호법의 제정 당시부터 이러한 즉시통보의무에 대한 비판이 제기되었다.[63] 앞서 언급한 개정안 검토보고서는 "현행 법률에서는 개인위치정보를 제3자에게 제공하는 경우 매회 개인위치정보 주체에게 제공대상·일시·목적을 '즉시 통보'하도록 하고 있어, 이용자는 빈번한 즉시 통보로 서비스에 대한 불편함을 초래하고, 사업자는 잦은 문자메시지 방송으로 인하여 서비스 비용이 증가한다는 지적"이 있으며, 또한 "최근 스마트폰용 위치기반 애플리케이션에서 개인이 방문한 장소를 스스로 지인 등에게 공개할 수 있는 서비스(예시 서비스는 아래 표 참조)가 활성화되고 있으나, 현행 법률에서는 개인위치정보주체가 스스로 공개를 선택한 사항에 대해서까지 매회 즉시통보를 하도록 하고 있어 불필요한 통보로 인한 비용이 소모되고 있는 실정"이라고 하였다.[64]

이용자가 중단할 권한을 상시 갖도록 하기 위해서는 예컨대 위치기반서비스가 제공되는 동안에는 제공되고 있다는 사실을 지속적으로 표시하는 아이콘이 활성화되도록 하고 그 아이콘과 관련되어 버튼을 제공하여 이를 누르면 위치정보의 제공이 즉각 중단되는 형식을 취하는 정도면 충분하다고 보인다.

# Ⅴ. 결론

위치정보보호법은 다음과 같이 개정되어야 한다. 첫째, 법 제15조가 폐지되어 익명인의 위치정보는 보호대상에서 배제되어야 한다. 물론 익명인의 위치정보의 경우에도 그 양에 따라 식별성을 갖출 수도 있으나 이때는 이미 더 이상 익명인의 위치정보가 아니라 '개인위치정보'인 것이다. 그 시점에서는 개인위치정보와 관련된 조항으로 의율하면 된다. 둘째, 위치정보의 주종을 이루는 GPS정보는 더 이상 법해석상 위치정보의 개념에 포함되지 않으며 기지국추적방식이나 wifi access point방식에서 추출되는 정보를 감안하더라도 더 이상 이동통신사들이 과점하고 있지 않은 상황이라서 허가제를 할 필요가 없다. 신고제도 역시 규제의 형평성을

---

자 하는 경우에는 미리 다음 각호의 내용을 이용약관에 명시한 후 개인위치정보주체의 동의를 얻어야 한다.
② 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 서비스를 하고자 하는 경우에는 제1항 각호의 내용을 이용약관에 명시한 후 제공받는 자 및 제공목적을 개인위치정보주체에게 고지하고 동의를 얻어야 한다.
③ 제2항의 규정에 의하여 위치기반서비스사업자가 개인위치정보를 개인위치정보주체가 지정하는 제3자에게 제공하는 경우에는 매회 개인위치정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하여야 한다.

62) ARTICLE 29 Data Protection Working Party, 881/11/EN WP 185, Opinion 13/2011 on Geolocation services on smart mobile devices (16 May 2011), 14-15쪽.

63) 조용혁, "개인위치정보의 보호에 관한 법률적 고찰", 정보화정책 제12권 제2호, 2005, 139쪽 이하;

64) 검토보고서, 19쪽

고려할 때 폐지되는 것이 옳다. 셋째 법 제19조 제3항이 위치정보가 이용될 때마다 동의를 요구하는 것은 그 조항의 원전이었을 것으로 보이는 EU의 「프라이버시 및 전자통신에 관한 지침」이 요구하는 것이 아니다. 원활한 서비스개발을 위해서 이 역시 폐지하고 '서비스중단권'을 제공하는 방식으로 개정되어야 할 것이다.

# 참고문헌


조용혁, “개인위치정보의 보호에 관한 법률적 고찰”, 정보화정책 제12권 제2호, 2005

국립목포대학교, “위치정보 관련 법·제도 개선방안”, 한국정보보호진흥원, 2006. 11.

이영일 외, “부상하는 위치기반서비스(LBS)″, CEO Information, 삼성경제연구소, 2007. 8. 1.

김상겸·김성준, “정보국가에 있어서 개인정보보호에 관한 연구”, 세계헌법연구 제14권 제3호, 2008

백인수 외, “2010년 IT 분야 10대 전략 이슈와 시사점”, IT 정책연구시리즈, 한국정보화진흥원, 2010

위치정보의 보호 및 이용 등에 관한 법률 해설서, 방송통신위원회·한국인터넷진흥원, 2010. 1.

전황수, “LBS 시장 및 업체 동향”, 정보통신산업진흥원, 주간기술동향 2011. 1. 19.

허은영, “위치정보 서비스 활성화와 사생활 보호를 위한 과제”, 통신연합 58호(2011 가을호)

박정훈, “최근의 위치정보에 관한 논의, 그리고 그 평가와 시사 - 미국의 사례를 중심으로 -”, 경희법학 제46권 제4호, 2011

위치정보의 보호 및 이용 등에 관한 법률 일부개정법률안 검토보고서, 국회문화체육관광방송통신위원회, 2011. 11.

(주)알앤디비즈, “국내외 LBS산업 현황 및 동향조사”, 한국인터넷진흥원, 2011. 12.

주윤경 외, “2012년 IT 트렌드 전망 및 정책방향”, IT정책연구시리즈, 한국정보화진흥원, 제23호(2011. 12. 29.)

정혜영, “개인정보보호법의 내용과 체계에 관한 분석”, 공법학연구 제12권 제4호, 2011

Pyramid Research, “Location-Based Services: Market Forecast, 2011-2015”, 2011. 5.

Gartner, ″Forecast: Consumer LBS″ Worldwide, 2008-2014, 2010. 7.

# 국문요약

LBS 산업이 급부상하는 현실에서 위치정보는 상업적 활용도가 매우 높은 정보사회의 중요한 자원이다. 그러나 위치정보는 개인 사생활과 직결되며, 오·남용시 심각한 프라이버시 침해의 우려가 있는 것도 사실이다. 이에 대한민국 정부는 “위치정보의 유출·오용 및 남용으로부터 사생활의 비밀 등을 보호”하고자 세계 최초로 2005년 「위치정보의 보호 및 이용 등에 관한 법률(이하 ‘위치정보보호법’)」을 제정·시행하고 있다.

위치정보보호법이 제정될 당시에는 현재의 개인정보보호법이 존재하지 않았으며, 과점적 지위를 가진 이동통신사업자의 사생활의 비밀의 침해 방지 필요성에 규제의 초점이 맞추어졌다. 허가, 인가, 신고 등 진입규제와 강한 의무 내지 제재 규정들은 사업자가 위치정보를 수집하여 제3자에게 제공하는 서비스(소위 “위치정보사업”)를 대표적인 규제 대상으로 하고 있다. 그러나 LBS 산업을 기존의 규제 틀에 맞추어 제한해서는 안 되며, 규제를 재정비하여 LBS 산업 육성과 개인위치정보 보호의 균형을 찾는 정책적 노력이 시급한 상황이다.

본 논문에서는 위치정보보호법의 세 가지 주요 내용의 문제점을 지적하고 개선 방안을 제시하려 한다. 위치정보보호법은 먼저 프라이버시 침해의 우려가 없는 위치정보도 보호하고 있어 옳지 않다. 그리고 일률적으로 위치정보사업의 허가제(법 제5조)와 위치기반서비스사업의 신고제(법 제9조)를 규정해 기술의 발달과 함께 가능해진 다양한 LBS 서비스를 제공하는 데 걸림돌이 되고 있다. 마지막으로 위치기반서비스제공자의 즉시 통보 의무는 사업자들에게 과도한 부담을 안기고 있다.

# 행태기반서비스(위치기반서비스 포함) 관련 법령 정비 방안

박상철, 김·장 법률사무소 변호사

## Ⅰ. 서론

행태기반서비스(Behavior-Based Service; "BBS")는 기업 입장에서는 가장 고도화된 마케팅 기법 중의 하나인 고객관계관리(Customer Relation Management; "CRM")의 핵심적인 수단으로서 새로운 부가가치 창출의 기회이며, 소비자 입장에서도 맞춤형 서비스를 제공받는 편익을 누릴 수 있다는 점에서 각광을 받고 있다. 그러나 BBS의 과정에서 수집되는 행태정보가 일반적인 식별정보 이상으로 이용자의 프라이버시를 침해할 우려가 제기되고 있으며, 역으로 이러한 우려가 필요 이상의 과도한 규제로 이어짐으로써 BBS의 기반 자체가 위협을 받을 수 있는 위험 요소 또한 존재한다.

이하에서는 일단 BBS의 현황을 개괄한 후, 그간의 법적 논의를 살펴봄으로써 BBS 규제의 핵심이 "개인식별정보(Personally Identifiable Information;"PII")와의 결합의 용이성"에 있다는 점을 규명하기로 한다. 이에 대한 명확한 논의 없이 현 법령과 같은 포괄적인 정의를 방치할 경우, 우리 규제기관과 수사기관이 때때로 취할 수 있는 "최대한의 엄격 해석 원칙"에 따라 BBS의 기반 자체가 질식할 우려가 있으므로, 위 PII와의 결합의 용이성이라는 핵심 개념을 사업자의 영업의 자유와 소비자의 프라이버시 간에 조화를 추구할 수 있는 한에서 어떻게 구체화할 수 있는지를 살펴본 후, 이에 따른 세부적인 법령 정비 방안에 대해 논의하기로 한다.

## Ⅱ. BBS의 개념과 현황

### 1. BBS의 개념

BBS는 이용자의 온라인 이용 형태를 분석하여 이용자 관심에 맞추어진 서비스를 제공하는 것을 의미한다[1]. BBS를 대표하는 서비스 형태는 온라인맞춤형광고와 위치기반서비스이다. BBS를 PII의 수집 없이 제공하려면, 하드웨어 정보 혹은 식별자를 기준으로 행태정보를 프로파일링할 수밖에 없는데, 이에 대해서도 상세히 살펴보기로 한다.

### 2. 온라인맞춤형광고(Online Behavioral Advertising; "OBA")

OBA란 이용자의 온라인 이용 형태를 분석하여 이용자 관심에 맞추어진 광고를 제공하는 기법을 의미한다[2].

---

1) KISA 개인정보보호포털 (http://www.i-privacy.kr)
2) Ibid.

〈그림 1: OBA의 개념도[3]〉

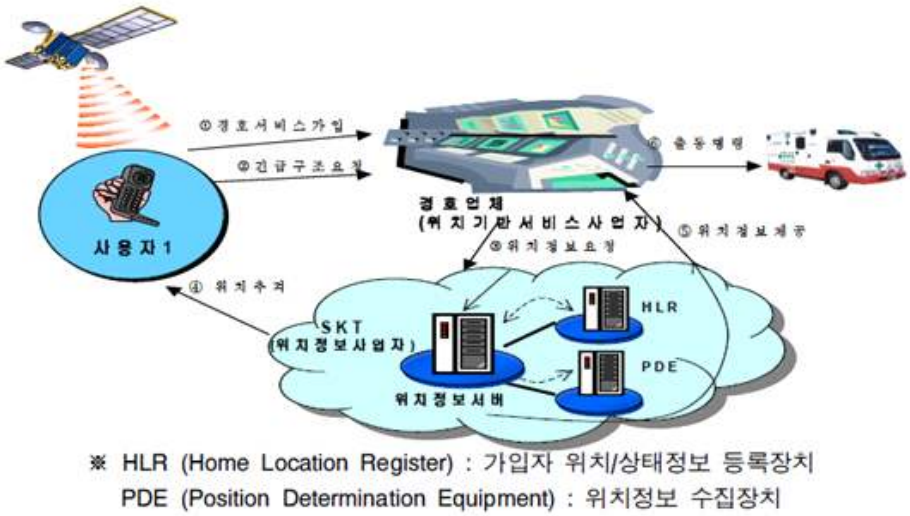

KISA[4]및 서울대 나종연 교수[5]에 따르면 OBA의 대표적인 유형은 다음과 같다.

| 구분 | 개념 | | 프라이버시 침해 여부에 대한 평가 |
|---|---|---|---|
| | KISA | 나종연 교수 | KISA |
| ① 사이트 정보를 이용한 맞춤형 광고 (Site Targeting) | 이용자가 방문한 웹사이트 정보만을 이용한 광고 | 이용자가 싱글 사이트나 싱글 앱과의 상호작용을 통해서 얻게 된 정보만을 이용한 광고 | 웹사이트에 종속된 형태이므로 프라이버시 침해 없음 |
| ② 문맥을 활용한 맞춤형 광고 (Contextual Targeting) | 이용자가 방문한 웹사이트에서 검색하는 검색어에 따른 광고 | 이용자가 읽은 콘텐츠의 내용 혹은 이용자가 검색한 내용을 이용한 광고 | 검색단어 기반이므로 프라이버시 침해 가능성이 거의 없음 |
| ③ 이용자의 행태정보를 활용한 맞춤형 광고 (Behavioral Targeting) | 이용자가 웹사이트에 방문하여 수행하는 행태 정보가 일정 기간 동안 수집 · 저장 · 축적 · 분석되고 이를 기반으로 이루어지는 광고 | 특정 이용자가 찾은 검색어, 방문한 웹페이지, 클릭한 링크, 이용자가 본 콘텐츠 등 이용자의 행동 양태에 대한 정보가 일정 기간 동안 수집, 저장, 축적, 분석되고 이를 기반으로 이루어지는 광고로 ad profile data가 구축됨 | Ad profile data가 구축된다는 점에서 프라이버시 침해 우려가 있음 |
| ④ 이용자 행태와 프로파일 정보를 결합 · 활용한 맞춤형 광고 (Profile Targeting) | ③ + 이용자 회원정보를 직접 활용 | 특정 이용자의 온라인 상에서의 행태에 대한 정보가 일정 기간 동안 수집, 저장, 축적, 분석된 자료를 이용하는 광고행위로 | ③ 이외에 이용자 정보를 직접 이용하므로 프라이버시 침해 우려가 높음 |
| ⑤ ISP 기반 맞춤형 광고 (ISP Behavioral Targeting) | ISP, 웹사이트, 광고 네트워크 간의 제휴를 통해 ISP에서 수집된 이용자 인터넷 행태 정보를 활용하여 광고 | ISP/웹사이트/광고네트워크 간의 제휴를 통해 ISP에서 수집된 데이터를 활용해서 이루어지는 광고행위 | ISP에 의한 인터넷 패킷 감청(deep packet inspection) 우려 |
| ⑥ 이용자 관심기반형 맞춤형 광고 | 회원가입/비가입시 선택하도록 되어있는 관심사항에 기반한 광고 | 키워드, 콘텐츠 외에 추가적인 정보를 활용하여 고객의 관심에 부합하는 광고를 제공. Ad preference manager를 활용하여 관심분야를 설정하면, 이에 따라 쿠키 설정. | 이용자 관심정보 활용이 가능하므로 프라이버시 침해 우려가 높음 |

3) Ibid.
4) Ibid.
5) 나종연, "U환경에서의 개인정보 보호 및 활용 방안: 온라인 행태정보 기반 광고" (2010. 7. 1. 방통위 온라인 행태정보 보호 및 이용에 관한 가이드라인 공청회 발표자료)

## 3. 위치기반서비스 (Location-Based Service; "LBS")

LBS란 위치정보사업자로부터 제공받은 위치정보를 이용하여, 고객에게 직접 위치정보를 기반으로 한 서비스를 제공하는 사업자를 의미한다(위치정보법 제2조 제7호에도 정의됨).




〈그림 2: LBS의 개념도[6]〉

2011. 2. 14. 현재 235개 사업자가 방통위에 LBS 신고를 하고 있는데, 주로 통신사, 포털, 앱개발사, 물류, 경비업체, 보험사 등이나 다양한 업계에 걸쳐 있다. 이동통신 단말기를 통한 위치정보의 경우 GPS (Global Positioning System), CPS (Cell Positioning System) 방식으로 주로 수집되고, 유선 인터넷의 경우 IP address로 GeoIP에 의한 대략적인 위치 확인이 가능한 것으로 알려져 있다. 최근 SNS의 geo-tagging 기능, 위치기반 맞춤형광고의 개발 등으로 서비스 저변이 확대되고 있고, 위치정보 활용 기술이 SDK, API 형태로 제공되어 초보자도 쉽게 프로그래밍하여 구현할 수 있게 되었다.

## 4. 하드웨어 정보 혹은 식별자를 기준으로 한 프로파일링 기법

상기 OBA와 LBS를 포함하여, 제반 BBS를 제공함에 있어, PII의 수집, 이용, 제공을 위한 관련 법령상의 고지, 동의를 거쳐 해당 PII를 기준으로 행태정보를 결합(associate)시켜 축적, 프로파일링하는 방법도 고려할 수 있다(앞서 살펴본 OBA의 유형 중 Profile Targeting이 그 전형적인 예이다). 그러나 BBS 제공자의 정책으로 인해, 혹은 사업모델상 PII의 수집이 불가능하여(검색사업자가 회원가입하지 않은 단순 방문자를 위한 OBA를 제공하는 경우 등) PII를 수집하여 활용할 수 없는 경우도 많은데, 이 경우 BBS를 제공하기 위해서는 클라이언트 단말(PC, 스마트폰 등)의 고유번호, 혹은 이러한 클라이언트 단말의 보조기억장치(HDD, Flash Memory, SSD 등)에 쿠키(cookie) 등의 형태로 저장된 식별자(index)를 PII의 대체수단(proxy)으로 활용하여 이를 기준으로 행태정보를 프로파일링할 수 밖에 없다.

---

6) 구 정보통신부 보도자료, "7. 28.부터 위치정보의 보호 및 이용 등에 관한 법률 시행" (2005. 7. 27.)

하드웨어 고유번호의 전형적인 예는 (1) 모바일 기기 정보(IMEI, IMSI, SN 등 (2G폰의 경우 ESN))와 (2) 하드웨어 일반의 MAC Address이다. 식별자의 전형적인 예는 OBA 중 Behavioral Targeting에 있어 광고플랫폼이 방문자의 PC에 쿠키(cookie) 파일을 생성한 후 해당 쿠키에 난수(random digit) 형태의 고유ID를 부여하고, 이 고유ID를 기준으로 방문 사이트 등 행태정보를 축적, 분석하여 이를 기반으로 맞춤형 광고를 제공하는 것이다. 아울러 IP Address의 경우에도 식별자의 역할을 하게 되는데, 특히 유동 IP의 경우 논란이 되고 있다. 이 모든 하드웨어 정보 및 식별자와 관련하여, 이들이 PII와 용이하게 결합됨으로써, 프로파일링된 전체 행태정보가 개인정보 법령상의 "개인정보"의 정의에 포섭되게 되는지 여부가 뜨거운 논란이 되고 있으며, 상세히 후술하기로 한다.

# Ⅱ. BBS와 관련된 지금까지의 법적 논의 및 쟁점

## 1. 관련 법령

### 가. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 ("정통망법")

BBS와 관련한 법적 문제의 핵심은 정통망법상 개인정보의 수집, 이용, 제공에 해당하는지 여부이다. 특히, 행태정보의 "개인정보" 해당 여부 및 행태정보주체의 "이용자" 해당 여부가 쟁점이 되고 있다.

개인정보는 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)로 정의(제2조 제6호)되어 있어 그 범위가 명확히 한정되어 있지 않아 행태정보가 이에 해당할 수 있는지 여부에 대한 결론이 내려져 있지 아니하다.

아울러, 정보주체 일반이 아닌 "이용자", 즉 "정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자"(제2조 제4호)로부터 수집된 개인정보의 처리에만 적용되고, 이외의 정보주체로부터 수집된 개인정보의 처리는 개인정보 보호법의 규제를 받게 된다.

### 나. LBS의 경우: 위치정보의 보호 및 이용 등에 관한 법률 ("위치정보법")

LBS에 대하여는 위치정보법이 규율하고 있다. 정통망법에 준하여 개인위치정보를 "특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합하여 특정 개인의 위치를 알 수 있는 것을 포함한다)"라고 정의하면서(제2조 제2호), 그 처리와 관련하여 동법에 준하는 고지/동의의무, 암호화의무 등을 부과하고 있다.

### 다. 통신비밀보호법 ("통비법")

그밖에 이용 일시, 개시/종료시간, 사용도수, log 기록, IP address, 기지국 정보는 통신비밀보호법상 "통신사실확인자료"에 해당(제2조 제11호)하여 수집, 이용에는 제한이 없으나(오히려 전기통신사업자에게 수사 협조를 위한 일정 기간 보존의무가 있음) 이를 제3자(일정 요건 하의 법원, 수사기관에 대한 제공 제외)에게 제공하는 것은 금지되어 있다(제3조 제1항). 단, 불법 감청과 달리 형사처벌 규정은 없다. 감청과 달리 당사자의 동의가 명시적인 허용 요건으로 규정되어 있지는 아니하나 당사자의 동의(정통망법과 달리 형식에 제한이 없음) 하에 제공이 가능하다고 보는 것이 합리적인 해석으로 보인다.

그밖에, 통비법은 단말기기 고유번호의 제공도 원칙적으로 금지하고 있다(제3조 제3항). 본래 단말기기 고유번호의 개인정보로서의 보호 측면보다는 휴대폰 복제를 금지하기 위한 조항이었으나 후술하듯이 확대 해석의 우려가 크다는 문제가 있다.

### 라. 신용정보의 이용 및 보호에 관한 법률 (“신용정보법”)

신용정보법은 “신용정보주체의 거래내용을 판단할 수 있는 정보” (대출, 보증, 담보제공, 당좌거래(가계당좌거래 포함), 신용카드, 할부금융, 시설대여와 금융거래 등 상거래와 관련하여 그 거래의 종류, 기간, 금액 및 한도 등에 관한 사항)을 개인신용정보에 포함시켜 규제하고 있다.

### 마. 전자상거래 등에서의 소비자보호에 관한 법률 (“전자상거래법”)

전자상거래법은 오히려 계약 또는 청약철회 등에 관한 기록, 대금결제 및 재화 등의 공급에 관한 기록을 수집하여 이를 5년간 보존할 의무를 부과하고 있다(제6조 제3항, 시행령 제6조 제1항 2호, 3호).

## 2. 가이드라인 및 법집행 사례

방통위는 2010. 7. 1. 행태정보를 “개인 식별성 행태정보”와 “개인 비식별성 행태정보”로 구분하여 전자는 정통망법에 기해 opt-in 규제를, 후자는 opt-out 규제를 하자는 취지의 “온라인 행태정보의 보호 및 이용에 관한 가이드라인(안)”을 마련하여 공청회를 열었으나, 시행하지는 않았다.  그러던 중 신경민 의원실에서 동 가이드라인을 바탕으로 동일한 내용으로 “온라인 행태정보 보호 및 이용에 관한 법률(안)”을 준비하여 화제가 되었다.

형사사법기관의 법집행 사례를 보면, 개인정보나 개인위치정보의 정의의 지나친 포괄성이 무리한 법집행으로 이어지고 있다. 구로경찰서는 2011. 1. “오빠 믿지” 등 모바일앱 제작 4개 업체 8명을 LBS 신고 미비를 이유로 입건하였고, 경찰청 사이버수사대는 2011. 4. 앱을 통해 GPS값, 휴대폰 식별번호, MAC address 등을 수집한 3개 모바일 광고 대행업체 및 대표자를 입건하였으며, 이후 모바일 광고 플랫폼에 대한 전방위 조사를 하였으나 방통위의 기존 해석에도 배치될 뿐 아니라 각계로부터 과잉 수사라는 비판을 받다가 서울중앙지검이 2011. 12. 모두 무혐의로 종결한 바 있다.

그밖에 서울중앙지법(형사11단독)은 2011. 2. 23. 증권정보앱 증권통을 개발, 로그인을 편하게 하기 위해 IMEI, USIM SN 등 스마트폰 기기정보를 수집한 이토마토 임원에 대해 정통망법 위반을 인정하여 벌금 700만원을 선고하였다(2010고단5343; 이하 “증권통 판결”). 동 판결은 본 논의에 있어 매우 중요한 의미가 있으므로 이하에서 좀더 상세히 살펴보도록 하겠다.

## 3. 해외의 규제 동향

미국의 경우 연방거래위원회(FTC)가 Self-Regulatory Principles for Online Behavioral Advertising (2009. 2.)을 발표하여 자율규제를 유도하고 있다.  (1) 투명성 및 고객 통제 원리, (2) 고객 데이터와 관련한, 합리적인 보안, 제한된 데이터 보유의 원리, (3) 현존하는 프라이버시 관련 약속에 중대한 변경시 명시적 동의 의무, (4) 행태광고를 위해 민감정보를 사용할 경우 명시적 동의 의무 등으로 나누어 자율적인 준수 원리를 규정하고 있다. 동 기준상의 논의는 우리 법 해석상으로도 상당한 참고 가치가 있으므로 후술하기로 한다.

EU의 경우 Article 29 Data Protection Working Party Opinion 1/2008 on data protection issues related to search engine (2008)을 발표하는 한편, 이를 Article 29 Data Protection Working Party Opinion 2/2010 on online behavioural advertising (2010. 6.)로 개정하였던바, 다양한 이해관계자들의 역할과 책무, informed consent의 필요성과 이를 확보하기 위한 방안, 아동소비자의 보호, OBA에 대한 정보제공 등의 내용을 포함하고 있다. 특히 2009. 4. 개최된 EC Summit에서 온라인 행태정보 이용 관련 roundtable을 개최하고 소비자 통제권을 강조하기 위한 방안의 필요성을 논의한 바 있다.

## 4. 지금까지의 주요 법리적 쟁점

### 가. PII와의 결합의 용이성

앞서 살펴보았듯이 정통망법상 개인정보든, 위치정보법상 개인위치정보든 "다른 정보와 쉽게 결합하여 알아볼 수 있는 경우"에만 이에 해당할 수 있다. 일반 개인정보의 경우 회원가입 등의 단계에서 PII와 결합되어 수집되는 것이 일반이라 동 요건이 큰 쟁점이 아니나 행태정보의 경우 그 자체만 떼어놓고 보면 대부분 비식별정보(non-PII)에 해당할 것이기에 위 "정보 결합의 용이성", 보다 구체적으로 "PII와의 결합의 용이성" 여부가 핵심적인 쟁점이 된다.

방통위, KISA 등의 경우 다수의 자료에서 위 범위를 최대한 넓게 해석해서 식별가능성을 폭넓게 인정하는 경향을 보이고 있으며, 경찰청 사이버수사대의 경우 가일층 넓은 정의를 취하여 식별가능성 요건을 무의미하다고 보고 사실상 "생존하고 있는 개인에 관한 정보"면 모두 개인정보에 해당한다는 입장을 취한 바 있다.

증권통 판결은 이에 대하여 "'쉽게 결합하여 알아 볼 수 있다'는 것은 쉽게 다른 정보를 구한다는 의미이기보다는 구하기 쉬운지 어려운지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합하여 특정 개인을 알아볼 수 있게 되는 것을 말한다"라는 기준을 제시하면서 IMEI, USIM SN 자체만으로는 사용자 정보를 확인할 수 없으나, 권한 있는 자가 정보를 조합하여 사용자 정보를 확인할 수 있어 개인정보에 해당한다고 판시하였다. 다만, 위 사례에서는 IMEI 또는 USIM SN을 알 경우 통신사DB를 통해 가입자의 구체적인 정보 확인이 가능했다는 사정이 있었다는 점에는 유의할 필요가 있다.

해외 사례를 보면, 앞서 살펴본 미국 FTC의 Self-Regulatory Principles 또한 III.A.1.에서 non-PII에 대한 자율규제의 적용 여부를 가장 중요한 법리적 쟁점으로 다루고 있다. 다양한 이해관계자의 의견을 취합하여 결론적으로 정보가 특정의 소비자나 기기에 "합리적으로 결합될 수 있는지(reasonably could be associated)"여부에 따라 자율규제 적용 여부가 결정된다고 보고 있다. 그러나 이 역시 "사실관계와 가능한 기술(factual circumstances and available technologies)"에 따라 판단하여야 한다고 결론내리고 있을 뿐 상세한 기준을 제시하고 있지는 않다.

"기준"의 가치가 있을 만큼 충분히 상세한 규정은 영국 Data Protection Act 1998에서 찾을 수 있는데, 동법상 개인정보는 "data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller"로 정의되어 있어, 당해 데이터 관리자가 소지하고 있거나, 소지할 개연성(likeliness)이 있는 PII와 결합 가능성이 있을 경우에만, non-PII의 개인정보성을 인정하고 있다.

앞서 살펴보았듯이, 결합 용이성은 하드웨어 정보 뿐 아니라 개인이 사용하는 기기를 식별

할 수 있는 정보(식별자 혹은 IP address)의 경우에도 쟁점이 되고 있다. 특히 IP address는 국내외 판결이 제각각으로 갈리고 있다. 스위스의 경우 개인정보에 해당한다고 판결하였으나, 프랑스의 경우 개인정보에 해당하지 않는다는 판결이 나왔다가(2007, 2009) 2010년 개인정보보호법 개정안에서는 "통신 네트워크 연결의 단말 장치를 판별하는 모든 주소나 번호를 개인정보로 규정한다"라고 명시하여 입법적으로 개인정보에 해당하도록 하였다. 미국도 주에 따라서 저작권 침해자 식별 목적의 RIAA의 IP주소 수집행위에 대해 합법 및 불법 결정이 엇갈리고 있다.

서울중앙지검 첨수부의 현재 입장은 같은 AP 사용 대역 내에서는 복수의 기기 이용자가 동일 IP주소로 접속할 수 있을 뿐 아니라 유동 IP address의 경우 시간별로 IP주소가 변동될 수 있으므로 "기술적 결합 가능성"이 없다는 것이다.

### 나. 서비스계약의 이행을 위한 필수성 여부

정통망법 제22조 제2항 제1호는 "정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적•기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우"에는 이용자에 대한 고지, 동의 절차 없이 개인정보를 수집•이용할 수 있다고 규정하고 있어, 이용자의 이용 과정에서 불가피하게 수집되는 온라인서비스 이용기록(로그)이 위 경우에 해당하는지 여부에 대하여 논란이 있다.

KISA의 2007. 7.자 "개인정보취급방침 작성 예시"는 이에 대해 "서비스 이용과정이나 사업자에 의한 처리과정에서 생성되는" 생성정보의 경우 자동으로 수집 또는 생성되어 이용자에게 매번 고지하고 동의를 받는 것이 경제적, 기술적 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우(구 정통망법 제22조 제2항 제1호)에 해당하므로 동의는 필요 없고 개인정보 취급방침에 공개만 하면 되나, 생성정보라 하더라도 마케팅 등을 목적으로 수집하려는 경우 또는 동의 획득시 미리 예상할 수 있는 정보의 수집, 생성에 관한 사항일 경우 고지, 동의가 필요하다고 해석하였으나, 방통위나 경찰 등에서는 보다 엄격한 해석을 내리는 경향이 있다. 증권통 판결에서도 쟁점이 되었으나, 해당 정보가 증권통 서비스를 위해 반드시 필요한 정보도 아니고, 동의를 받는 것이 뚜렷하게 곤란한 경우에 해당한다고 보기도 어렵다며 위 예외에 해당하지 않는다고 판시하였다.

### 다. 사이트내(intra-site) 이용의 경우 규제 필요성 여부

개인정보의 "이용"을 "제공" 못지않게 강하게 규제하고 있는 우리 법상으로는 논의의 큰 실익은 없지만, 앞서 살펴본 미국 FTC의 Self-Regulatory Principles은 본인(first party) 혹은 사이트내(intra-site) OBA의 경우 동 자율규제가 적용될지 여부에 대하여 논의하고 있다. 즉, 단일 사이트 내에서만, 당해 사이트에서 수집된 정보만을 가지고 OBA를 제공하는 경우는 프라이버시 침해 우려는 적으나 이용자의 니즈는 크다는 점에서 규제 대상이 될 필요가 없다는 논의를 소개하면서, 이에 찬동하고 있다. 만약 현행 규제에 덧붙여 비식별 행태정보에 대하여도 추가적인 규제를 하여야 한다는 입장이 입법화될 경우, 지나친 규제 가능성을 피하기 위하여 사이트내 이용의 경우 적용을 제외하는 등의 조치가 필요함을 시사하고 있다.

# III. 식별가능성에 대한 명확한 기준 설정을 위한 법령 정비 방안

## 1. 개인(위치)정보의 정의에 있어 “식별정보 결합 용이성” 요건 명확화

### 가. 가능한 견해의 대립

현행 법령 하에서의 PII와의“결합 용이성”의 의미와 관련하여서는 다음과 같은 견해가 나눠질 수 있다.

독립된 요건으로서의 무의미설: “정보 결합의 용이성”은 대체로 인정되므로, “개인에 관한 정보”는 대부분 개인정보로 보아야 한다는 시각. 경찰청에서 때때로 취해온 견해.

객관적 결합 용이성설: 해당 행태정보와 다른 PII가 기술적으로 제약이나 어려움 없이 결합 가능할 경우 개인정보에 해당한다고 해석. 증권통 판결  및 서울중앙지검 첨수부가 취하는 견해.

주관적 결합 용이성설: 해당 행태정보의 보유자가 자신이 보유하거나(혹은 보유하게 될 개연성이 있거나) 공지된 PII를 결합해서 개인을 식별할 수 있을 경우 개인정보에 해당한다고 해석. 앞서 살펴본 대로 영국 Data Protection Act 1998이 취하고 있는 입장(동법은 이하에서 “절충설1”에 가까울 것임). 구체적으로는 다음과 같은 스펙트럼으로 나눠질 수 있음

<table>
<tr><th></th><th>현재 보유 중인 PII + 공지의 PII</th><th>+ 사업자가 이미 제3자제공/위탁 고지/동의를 하여 원하면 언제든지 동 사업자로부터 가져올 수 있는 PII</th><th>+ 향후 PII의 보유자와의 협상을 통해 적법 제공받을 가능성이 있는 PII</th><th>+ 향후 위법하게 입수할 가능성이 있는 PII</th></tr>
<tr><td>해당 행태정보 보유자</td><td>협의의 주관적 결합 용이성설</td><td>절충설1</td><td rowspan="3">모든 PII 보유자는 개별 고지/동의를 받아 제공해줄 “가능성”이 있으므로 객관적 결합 용이성설과 달라질 것이 없음</td><td rowspan="3"></td></tr>
<tr><td>현재 적법하게 제공받고 있는 자</td><td>절충설2</td><td>절충설3</td></tr>
<tr><td>향후 적법하게 제공받을 가능성 있는 자</td><td>절충설4</td><td>절충설5</td></tr>
<tr><td>위법하게 입수할 가능성 있는 자</td><td colspan="4">객관적 결합 용이성설</td></tr>
</table>

특히 증권통 판결의 주요 근거는 (1) 당해 행태정보가 “제3자에 의하여 획득될 가능성이 없다고 할 수는 없다”는 점과 (2) PII를 보유한 통신사DB와 대조하여 개인 식별이 가능하다는 점이다. 위 표의 行에서는 “위법하게 입수할 가능성 있는 자”를 포함시키고, 列에서는 “향후 PII의 보유자와의 협상을 통해 적법 제공받을 가능성이 있는 PII”를 포함시켜 객관적 결합 용이성설을 도출했다고 할 수 있다.

### 나. 객관적 결합 용이성 개념에 따라 익명성 요건 충족시 개인정보 정의에 해당하지 않음을 명확화

판단컨대, 1차적으로는 과잉 규제와 수사의 위험을 완화하기 위해 객관적 결합 용이성 개념을 명확화, 익명성(anonymity)의 요건을 충족시켰을 경우 개인정보 정의에 해당하지 않음을 명확히 할 필요가 있다.

익명성이란 그 누구에게 유출되더라도 이미 익명화되어 PII와의 결합이 불가능해 졌다는 개념인바, 특히 개인의 특성을 완전히 제거한 하드웨어 고유번호(MAC Address 또는 이하 2항에서 논의하는 식별자에 저장된 고유ID를 포함)는 이를 보유자 혹은 제3자의 별도DB로써 PII와 1:1 매칭할 수 없는 경우 객관적 결합 용이성 요건에 해당하여 개인정보 규제에서 벗어한다고 보아야 할 것이다.

### 다. 주관적 결합 용이성 개념의 반영

2차적으로는 객관적 결합 용이성이 인정될 경우에도 향후 제3자의 DB를 통해 대조될 가능성을 배제할 수 없다는 막연한 가능성만으로는 결합 용이성을 인정하지 않는, 주관적 결합 용이성 개념을 도입하여야 할 것이다. 특히 과잉규제를 막기 위해서 상기 표 기준으로 "절충설 1" 정도의 타협이 필요할 것이다. 즉, PII의 경우 "현재 보유 중인 PII", "공지의 PII", "현재 적법하게 제공하고 있는 자가 보유 중인 PII"를 기준으로 하고, "당해 행태정보의 보유자"가 이러한 PII를 결합하여 개개인을 식별할 수 있는지 여부에 따라 결합 용이성 여부를 판단해야 할 것이다.

예컨대 IP address의 경우 객관적 결합 가능성설에만 충실하게 해석할 경우 유동IP의 경우 ISP의 DB를 통해 PII 대조가 가능하고 AP 공유의 경우 증언을 통한 입증이 가능하므로 개인정보에 해당한다고 주장하겠지만 이러한 지나치게 확장적인 해석은 비합리적이다. 앞서 살펴본 서울중앙지검 첨수부의 입장 또한 이러한 측면을 감안한 합리적인 해석이라고 볼 수 있다.

IMEI의 수집의 경우 증권통 판결은 통신사DB로 이용자 대조가 가능하므로 개인정보에 해당한다고 보았으나 현실적으로 통신사가 중소 앱사에 이용자 DB를 제공할 가능성은 희박하고, 해킹 사고 등의 경우 해당 사고에 대한 처벌 규정으로 단속할 수 있으므로, 이러한 막연한 가능성만으로 개인정보 규제를 적용하는 것은 불합리하다.

## 2. 적용사례 1: OBA의 경우

앞서 살펴본 서비스 구분에 따라 살펴보면, Site Targeting이나 Contextual Targeting의 경우 아무런 결합이 이루어지지 않으므로 개인정보 규제가 적용되지 않을 것이다. ISP Behavioral Targeting의 경우 해당 ISP의 개인정보 제3자 제공 혹은 위탁 관련 규제의 문제로 다뤄질 사항이고, Profile Targeting이나 이용자 관심기반형 맞춤형 광고의 경우 행태정보의 이슈라기보다는 PII와 명확히 결합되는 정보의 문제이므로, 기존의 개인정보 규제 틀에 따라 판단될 수 있다. 다만 가장 이슈가 될 수 있는 부분은 앞서 살펴보았듯이 Behavioral Targeting으로서, 광고 프로파일 데이터(ad profile data)의 축적이 어느 정도까지 허용될 수 있는지가 관건이다.

이와 관련하여, 결합 용이성에 대한 상기 논의의 결론은, 특히 OBA 사업자들이 개인의 식별정보와 용이하게 결합되지 않으면서도 이용자의 행태에 따른 맞춤형 서비스를 제공할 수 있는 기반이 되는 식별자를 운용해야 한다는 점을 시사하고 있다. 다시 말해, 각 개인의 PC에 쿠키 등의 형태로 랜덤한 고유ID("123456" 등의 일련번호)가 부여된 식별자를 저장시킨 후, 동 식별자를 기준으로 쿠키 등에 이용자의 방문 사이트, 검색어 등 광고 프로파일 데이터(즉, 행태정보)를 축적하도록 할 경우, 당해 사업자가 이러한 고유ID를 식별정보와 결합하려면 모든 이용자의 PC를 직접 뒤져야 하는데 이는 불가능하다는 점에서 객관적 결합 용이성이 인정

될 수 없는 경우라고 보아야 할 것이며, 개인정보 규제의 적용을 받을 필요가 없는 경우에 해당할 것이다.

여기서 한걸음 더 나아가 IP address나 기기정보(MAC address, IMEI, S/N 등)가 함께 수집되어 식별자와 결합될 경우에도, 앞서 논의한 대로 각각의 정보의 결합 용이성이 인정되지 않으므로 달리 PII와 결합되지 않는 이상 개인정보의 규제의 적용 대상이 아니라고 보아야 할 것이다.

### 3. 적용사례 2: LBS의 경우

위치정보법상 "위치정보"에 "이동성이 있는 물건"이 포함되어 있어, 비록 "개인위치정보"에서 결합 용이성을 요하고 있다 하더라도, 실무상 많은 혼선을 초래하고 있다. 그러나 "이동성이 있는 물건" 관련 정보일지라도 상기 객관적, 주관적 결합 용이성이 인정되지 않을 경우 개인위치정보에 해당할 수 없다는 점은 법문상 명확하다.

객관적 결합 용이성과 관련하여서는, 특히 위치정보를 활용한 모바일맵 서비스의 경우, 맵 서비스 서버가 익명화된 좌표값만을 모바일 기기로부터 받아 이에 해당하는 맵 타일 데이터를 1:1로 보내주는 것에 불과하다면 해당 좌표값만으로는 개인 식별이 불가능하므로 개인위치정보에 해당하지 않는다고 보아야 할 것이다.

주관적 결합 용이성과 관련하여서는, 모바일 앱 개발사가 모바일 OS로부터 단말기의 GPS 정보 값만을 전달받아 처리할 GPS 정보만으로는 특정 개인의 위치정보를 알 수 없어 규제의 필요성이 없는데도, 해당 모바일 OS사가 GPS 정보와 함께 해당 단말기의 OS, 기기 고유번호, ID를 수집한다는 이유로 이미 결합되었다며 모두 LBS 사업자에 해당한다고 보는 것은 불합리하며, 규제 대상에서 제외하여야 할 것이다. 주관적 결합 용이성과 관련하여 결합의 용이성을 해당 정보의 수수에 관여한 모든 사업자가 아닌 현재 해당 정보를 보유한 사업자를 기준으로 판단할 경우 당연한 결론이다.

## IV. 각 행태정보 유형별 처리에 대한 규제 정비 방안

### 1. 식별 가능 행태정보의 처리에 대한 규제 방안

일단 현행 법령의 틀 내에서는 위와 같은 해석의 결과 식별 가능하다고 판단될 경우 개인정보에 준하는 규제를 할 수 있을 것이다.

다만, 사문화되어 버린 정통망법 제22조 제2항 제1호의 고지/동의 면제 요건("정보통신서비스의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적•기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우")을 적극적으로 해석할 필요가 있고, 특히 동 면제요건을 무의미하게 하는 "뚜렷하게"라는 단어를 삭제할 필요가 있다. 해당 서비스의 이용 history에 대한 정보(로그정보)가 대표적인 경우라고 할 수 있고, 행태정보의 수집, 이용이 해당 서비스의 본원적 요소를 이룰 경우 해당 서비스에 대한 동의를 행태정보 수집, 이용에 대한 동의로 간주할 수 있으므로 위 규정을 적극적으로 적용할 수 있을 것이다.

다만 약관 형태의 고지 문구를 보여주고 이에 동의를 얻도록 하는 현행 개인정보 관련 법령의 규제는 (1) 사업자의 신규 서비스 개발에 의한 혁신과 가치창출을 저해, (2) 특히 국내 사업자들을 과잉규제함으로써 개인정보 기반 맞춤형 서비스를 제공하는 글로벌 사업자에 비해 글로벌 경쟁력을 떨어뜨림, (3) 역으로 이용자들이 잘 읽지도 않는 형식적 절차만 밟은 사업자들에게 면죄부를 부여, (4) 전세계적으로 긴 고지 문구를 보여주는 표시(labeling) 규제가

실효성이 없다는 실증연구 결과 축적, (5) 스마트, 모바일 시대의 화면 인터페이스에 맞지 않음 등 한계를 드러내고 있으며, 특히 행태정보와 관련하여 부작용이 더욱 첨예하게 도출되고 있으므로, 이에 대해 전반적으로 함께 논의를 할 필요는 있다. 이에 대하여는 본 포럼의 다른 연구들이 상세히 다루고 있으므로, 본 논문에서는 이를 생략하도록 하겠다.

## 2. 식별 불가능 행태정보의 처리에 대한 규제 방안

방통위의 "온라인 행태정보의 보호 및 이용에 관한 가이드라인(안)"과 이를 기초로 한 "온라인 행태정보 보호 및 이용에 관한 법률(안)"은 식별 불가능 행태정보의 경우 opt-out 규제를 권고하고 있으나, 이미 식별 불가능할 경우 프라이버시의 침해 우려가 없으므로 이에 대한 규제는 사업자 자율에 맡기도록 하는 것이 타당하다. 가사 규제를 추가하더라도, 앞서 살펴보았듯이 intra-site OBA의 경우 적용을 배제함이 합리적이다.

## 3. 위치정보법상 LBS에 대한 세부 규정들의 정비 방안

현재 위치정보법은 세계 어디에도 없는 독특한 법령으로서 지나치게 규제 일변도로 제정되어 많은 문제점을 내포하고 있다. 위치정보법의 문제점은 "오원춘 사건" 때 동법으로 인해 경찰서의 119 발신 휴대폰 위치추적이 불가하여 귀중한 생명이 처참히 희생됨으로써 가장 극단적인 형태로 현실화되기에 이른다[7]. 과연 위치정보법을 정보통신망법과 별도로 존립시켜 일반 개인정보보다 강력한 규제를 하는 것이 타당할지 평가가 필요할 것이며, 존치하더라도 이하와 같은 불합리한 세부 규정들을 정비할 필요가 있다.

### 가. 위치정보사업과 LBS의 이원적 규제 폐지

현행 위치정보법상 허가 대상인"위치정보사업"과 신고 대상인 LBS의 준별은 다분히 스마트 혁명 이전의 과거의 이동통신의 구조(이동통신사가 이동통신 기지국의 삼각측량 방식을 통해 CPS 정보를 수집하면, 각종 LBS사업자들이 이를 받아 서비스하는 구조)를 전제하고 있다. 그러나 스마트 혁명 이후 많은 앱 개발사들이 이용자의 단말로부터 직접 GPS 정보를 수집하여 다양한 서비스를 제공하고 있는바, 방통위는 실무적으로 모바일 OS /Open API 제공자를 위치정보사업자, app 운영자(app 자체에서 서버를 경유하지 않고 단말기 단에서 위치정보를 처리하는 경우 제외)를 위치기반서비스사업자로 보고 있으나, OS/API의 경우 실은 해당 OS/API 개발자가 (자신의 서버로 단말기단에서 수집된 GPS정보를 전송받지 않는 이상) 각 스마트폰에 이미 설치되어 클라이언트(단말기) 단에서 구동되는 OS/API를 운영하는 것이 아니어서(Microsoft가 Windows를 개발했다 하여, Windows가 설치된 각 PC를 운영하는 것이 아닌 것과 같은 이치), 기술적 특성에는 부합하지 않는 해석이다. 스마트 시대에 맞지 않게 되어 버린 이원적 규제를 폐지하는 것이 근본적인 해결 방안일 것이다.

### 나. 허가/신고제의 폐지 또는 완화

현재 LBS 서비스를 제공하려는 자는 예외 없이 방통위에 LBS 신고를 하도록 되어 있으며, 사업계획서(위치정보 보호조치에 대한 내용 기입), 사업용 주요 설비의 내역 및 설치장소 확인 서류, 위치정보의 보호조치 증명 서류 등을 제출하여야 하여 결코 간단한 양식이 아니다.

---

7) 위 사건을 계기로 뒤늦게 2012. 5. 14.자 개정을 통해 위치정보법 제15조 제1항 단서 2호에 "제29조제2항에 따른 경찰관서의 요청이 있는 경우"가 삽입되어 2012. 11. 15.부터 시행되고 있다.

현재 구글 맵스(Google Maps) 등 가장 발전된 형태의 온라인 지도 플랫폼들은 API(Application Programming Interface)를 공개함으로써 누구든지 구글 맵스의 기능을 자신이 개발하는 모바일 앱에 쉽게 이식할 수 있도록 하고 있다. 워낙 API의 기능이 강력하고 사용이 용이한 관계로 어린 학생들도 약간의 관심만 있으면 쉽게 구현할 수 있는 실정이라, 부지불식간에 미신고에 따른 형사처벌을 받아야 할 잠재적 전과자가 양산되고 있으며, "오빠 믿지" 사건도 그 와중에서 생긴 해프닝으로 이해된다. 2G 시대에 생긴 허가제와 신고제는 모바일 시대에 즈음하여 근본적인 재검토가 필요하다.

### 다. 포괄적인 제3자 제공 동의 허용 필요

위치정보법 제19조 제3항의 "매회"라는 단어 하나가 위치정보를 이용한 OBA 사업 자체를 불가능하게 만들고 있다. 동 조항은 LBS가 개인위치정보를 정보주체가 지정하는 제3자에게 제공하는 경우에는 "매회" 정보주체에게 제공받는 자, 제공일시 및 제공목적을 즉시 통보하도록 하고 있다. 이렇게 건건이 통보하는 것은 현실적으로 불가능하므로, 예컨대 포털이 광고 플랫폼에 입주한 모바일 광고주에게 개인위치정보를 전송하여 맞춤형 광고를 노출하는 것 자체가 불가능하다. 한번의 동의로 다채로운 서비스를 제공받고 싶은 이용자의 수요를 법이 나서서 부정할 필요는 없다고 생각되며, 개정이 필요하다.

### 라. 스마트 환경에 맞지 않는 고지의무의 완화

현 위치정보법상 이용약관 명시의무 조항(제18조 제1항, 제2항, 제19조 제1항, 2항)은 스마트폰 화면에 제대로 들어가기 어려운 지나치게 많은 항목의 명시를 요하고 있어 개선이 필요하다.

### 마. 취급위탁 규정의 신설 필요

여타 개인정보 관련 법령들은 해당 서비스 주체의 서비스 제공을 위한 정보 제공은 제3자 제공이 아닌 취급위탁으로 보아 고지, 동의 의무 등을 완화시키고 있다.  유독 위치정보법만 이러한 예외를 인정하지 않아 경직된 규제가 이루어지고 있으므로, 다른 개인정보 관련 법령 수준의 개정이 필요하다.

### 바. 영업양수인의 양수 후 통지 제도의 개선

영업양도시 정통망법 제26조와 개인정보보호법 제27조는 모두 영업양도인이 영업양도 전 통지하도록 규정하고 있는 반면, 어떤 경위에서인지 위치정보법 제7조는 영업양수인이 영업양도 후 통지하도록 규정하고 있다. 개인위치정보가 개인정보와 통상 함께 양도되는 상황에서, 두 번이나 거듭 통지를 받아야 하는 이용자의 불편도 고려해 주어야 할 것이다.

### 사. 보안 관련 규제의 개선

위치정보법상 명확한 근거 규정은 없으나 특히 외국 모바일OS사나 앱사의 경우 LBS 신고 과정에서 방통위가 국내 이용자 개인정보 보호 및 규제관할권 확보를 위해 서버의 국내 설치를 요하는 경향이 있다.  클라우드 컴퓨팅으로의 전환기에 이용자의 다채로운 이용권을 확보하기 위한 좀더 완화되고 탄력적 정책 운용이 가능하도록 설비 기준에 대한 명확한 규정이 필요할 것이다.

## 4. 통비법의 정비 방안

우선, USIM 방식으로 전환되면서 사문화된 단말기기 고유번호 제공 금지는 폐지할 필요가 있다. CDMA 단말기의 경우 이통사가 개통시 단말기기 자체에 부여하는 ESN가 복제폰 제조에 이용될 수 있어 동 규정의 실효성이 있었으나, 3G로 이행한 후 단말기기의 IMEI와 USIM의 IMSI가 분리되었고 IMEI만으로는 복제폰 제조가 불가능하여 사문화되었다. 결국 IMEI는 복제폰 제조에 사용될 수 없음에도 불구하고 "단말기기 고유번호"라는 이유만으로 처벌 가능성이 남아 있어 혼란을 주고 있다. 특히, 단말기 복제는 전파법 제84조 제6호(적합성 평가를 받은 기자재를 복제, 개조 또는 변조한 자를 3년 이하의 징역 또는 2천만원 이하의 벌금에 처함)로 처벌 가능하고 이에 대하여 단말기기 고유번호 제공을 "예비죄"로 처벌할 합리적인 근거가 없다는 점에서도 통비법에 존치될 이유가 없다.

한편, 통신사실 확인자료의 경우 감청과 마찬가지로 "당사자의 동의"가 있을 경우 제공이 가능하다는 점을 명확히 할 수 있도록 제3조 제1항을 개정할 필요가 있다.

## 5. "타인의 비밀", "통신의 비밀" 등 명확성을 결여한 금지, 처벌 규정의 정비

정통망법 제49조는 "누구든지 정보통신망법에 의하여 처리, 보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해, 도용 또는 누설하여서는 아니 된다"라고 규정하고 있는데(위반시 제71조 11호에 의하여 징역 또는 벌금형), 이는 "비밀"의 불명확성으로 인하여 다양한 형태의 행태정보 활용을"비밀"침해로 광범위하게 처벌할 근거가 될 수 있는 조항이다. 대법원은 "타인의 비밀"을 "일반적으로 알려져 있지 않은 사실로서 이를 다른 사람에게 알리지 않는 것이 본인에게 이익인 것"을 말한다고 보나(대법원 2012. 1. 12. 선고 2010도2212 판결), 이로써 충분히 특정 가능한지 의문이다.

이와 더불어 전기통신사업법 제83조 제1항은 "누구든지 전기통신사업자가 취급 중에 있는 통신의 비밀을 침해하거나 누설하여서는 아니 된다"라고 규정하고, 제2항은 "전기통신업무에 종사하는 자 또는 종사하였던 자는 그 재직 중에 통신에 관하여 알게 된 타인의 비밀을 누설하여서는 아니 된다"라고 규정하고 있는바(위반시 역시 제95조 7호, 제94조 4호에 의하여 징역 또는 벌금형), 대부분의 BBS 사업자가 전기통신사업자에 해당한다는 점, 그리고 "비밀"이라는 개념의 모호성과 광범위성으로 인해 BBS 사업자들에게 큰 리스크 요소로 작용하고 있다.

이러한 불명확한 규정이 둘이나 존재하는 상황에서는, 아무리 개인정보와 행태정보의 정의를 세련되게 개정하더라도 이에 대한 고민 없이 쉽게 "비밀"로 규정하여 규제하고 처벌하는 남용의 가능성이 남아 있다. 최근 경찰청의 PG업계 조사 또한 위 "비밀"이라는 개념의 모호성으로 인한 지나친 법집행의 예이다. 이들을 삭제하거나 명확하게 개정할 필요가 있을 것이다.

# 개인정보 주체의 권리에 대한 조화로운 접근
## - 잊힐 권리(잊혀질 권리)와 손해배상청구권의 합리적 보장을 중심으로 -

가천대학교 법과대학 교수 최경진

## Ⅰ. 머리말

사회가 복잡해지고 다변화되면서 개인에 관한 정보의 활용영역도 더욱 확대되고 있다. 기존에는 개인에 관한 정보를 수집하더라도 그 활용범위가 매우 협소하였고 그 오남용으로 인한 피해도 특정 개인에 한정되는 경우가 대부분이었지만, 스마트환경으로 전환되면서 개인정보의 집적이 쉬워지고 확산되는 속도도 매우 빨라졌다. 이러한 변화에 따라 동적이고 수동적 측면에서 타인의 사적 영역에 대한 침입이 일어날 때에 비로소 권리로서 보호하던 것에서 벗어나서 그 침해의 가능성을 높이게 되는 개인정보에 대한 법적 규율이 강화되기 시작하였고, 개인정보의 오남용에 따른 침해에 머무르지 않고 개인정보 그 자체를 법적 보호의 대상으로까지 삼게 되었다. 이처럼 현대 정보화시대에서 요구되는 개인정보주체의 보호를 위하여 개인정보보호법이 제정·시행되었다. 개인정보 보호법에 따르면 개인정보처리자에게 일정한 개인정보의 처리 기준을 제시하면서, 정보주체에게 적극적으로 개인정보자기통제권을 행사할 수 있는 길을 열어 놓고 있다. 즉, 개인정보자기통제권의 구체적 실현으로서 개인정보 열람 청구권, 개인정보 정정 청구권, 개인정보 삭제 청구권, 개인정보 처리정지 청구권이 개인정보 보호법에 의하여 보장된다. 기존에 명문으로 인정되지 않던 이런 권리들이 일반 규정으로서 도입됨에 따라 다른 권리와의 충돌 가능성이 야기된다. 특히, 최근 여러 언론보도를 통하여 잊힐 권리[1]가 강조되면서 개인정보 측면에서 잊힐 권리의 문제가 어떻게 다루어져야 하는가가 문제되고 있다.[2] 또한 개인정보 보호법에 의하면 개인정보처리자에게 개인정보침해에 따른 손해배상책임을 인정하면서, 그 입증책임을 전환하고 있다. 이는 기존의 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 함)에서도 동일하게 인정되던 것이다. 그런데 개인정보 보호법은 이에서 더 나아가서 개인정보의 분실·도난·유출·변조 또는 훼손에 따른 손해배상책임의 경우에는 개인정보 보호법을 준수하고 상당한 주의와 감독을 다한 경우에 감경 받을 수 있도록 규정하고 있다. 이로 인하여 실제 개인정보처리자의 주의의무의 수준이 매우 높아지게 되었다. 이는 개인정보주체의 권리보장 및 보호에는 충실한 것이지만, 한편으로는 개인정보처리자에게 과중한 의무를 부담시켜서 형평에 어긋날 가능성도 완전히 배제할 수 없다. 따라서 현행 개인정보 보호법에 따른 개인정보주체의 권리, 특히 삭제 및 처리정지 청구권과 손해배상청구권이 개인정보를 이용하고자 하는 자들의 합리적·합법적으로 보호받아야 할 권리들과의 충돌 속에서 어떻게 균형 있고 적절하게 보호되어야 하는가라는 문제를 진지하게 고민해 보아야 한다. 이러한 시각에서 이 글에서는 먼저 정보주체의 적극적 권리에 대한 해외의 동향을 살펴보고, 이와 관련한 국내법의 규정을 비교하여 검토한 후 바람직한 개선방향에 대한 시

1) 종래 용어법으로서 '잊혀질 권리'가 많이 사용되었지만, 이는 이중피동형으로서 한글 맞춤법에 맞지 않는다는 점을 고려할 때 용어례로는 '잊힐 권리'가 적절하다. 이 글에서는 '잊힐 권리'의 용어례의 사용을 권장하면서, 잊힐 권리로 통일하였다.

2) 잊힐 권리의 개인정보측면에 관한 상세한 논의는 최경진, "잊혀질 권리 - 개인정보 관점에서", 정보법학 제16권제2호, 97면 이하 참조.

사점을 제시하고자 한다.

# Ⅱ. 정보주체의 권리에 대한 해외 동향

## 1. OECD

개인정보에 대한 정보주체의 권리는 1980년 OECD의 “프라이버시 보호와 개인정보의 국제적 유통에 관한 지침(Guidelines Governing the Protection of Privacy & Transborder Flow of Personal Data)”에서 천명된 내용이 이후 여러 나라의 개인정보 관련 입법에 영향을 주었다. OECD 개인정보지침에 천명된 개인정보보호 8원칙 중 개인 참가의 원칙 (Indivisual Participation Principle)에 의하면, 개인은 자기에 관한 데이터의 소재를 확인할 권리를 가지며, 필요한 경우에는 자신에 관한 정보를 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 통지받을 권리를 가진다. 이러한 권리가 거부되는 경우에 개인은 그 이유를 구하고 거부에 대하여 이의를 제기하거나 데이터의 폐기·정정·보완을 청구할 권리를 가진다.

## 2. EU

최근 우리에게 소위 ‘잊힐 권리’의 논란을 야기한 진원지는 EU의 일반정보보호규정안(Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data)과 개인정보보호지침안(Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data)이다. 특히, 일반정보보호규정안에는 잊힐 권리가 명문으로 규정되어 있다.

일반정보보호규정안 제17조는 정보주체가 개인정보처리자(controller)를 상대로 그와 관련된 개인정보의 삭제권을 보유하여야 한다고 규정한다. 그리고 정보주체는 개인정보의 확산을 중지시킬 권리를 가진다. 특히, 아동인 정보주체의 개인정보에 대하여 그러한 권리가 보장되어야 한다. 다만, 이러한 잊힐 권리가 인정되기 위한 요건은 다음의 4가지 중의 한 경우이어야 한다. 즉, (1) 수집되거나 처리되는 목적에 정보가 더 이상 부합하지 않는 경우, (2) 정보를 처리할 수 있는 법적 근거가 없으면서 제6조(1)(a)에 따라 이루어지는 처리에 대한 동의를 철회하거나 동의한 보관 기간이 만료된 경우, (3) 정보주체가 제19조에 따라 개인정보의 처리에 반대하는 경우, (4) 정보의 처리 방식이 다른 이유로 인해 본 규정의 조건을 충족하지 못하는 경우이다.

개인정보처리자가 개인정보를 공개한 경우에 개인정보처리자는 공개에 대하여 책임있는 개인정보와 관련하여 기술적 조치를 포함하여 그 개인정보를 처리하는 제3자에게 정보주체가 그들에게 그 개인정보의 링크, 사본을 삭제할 것을 요청한다는 점을 알리기 위한 모든 합리적인 조치를 취하여야 한다. 개인정보처리자가 제3자에게 개인정보의 공개를 허용하였다면, 그 개인정보처리자는 그 공개에 대하여 책임있는 것으로 보아야 한다.

개인정보처리자는 개인정보의 보유가 필요한 다음의 경우를 제외하는 개인정보를 지체 없

이(without delay) 삭제하여야 한다. 즉, (1) 제80조에 따라 표현의 자유에 대한 권리를 행사하는 경우, (2) 제81조에 따라 공공 보건 부문에서 공익을 위한 경우, (3) 제83조에 따라 역사, 통계, 과학 연구 목적으로 필요한 경우, (4) 유럽연합 또는 개인정보처리자가 속한 회원국의 법률에 의해 개인정보를 보관해야 하는 법적 의무를 준수해야 하는 경우,[3] (5) 제4항에 따라 개인정보의 처리를 제한하여야 하는 경우에는 예외적으로 개인정보를 보유할 수 있다. 이러한 예외 중에서 특별히 논란이 되는 것은 잊힐 권리가 표현의 자유와 부딪히는 경우에 어떻게 균형을 이룰 것인가이다. 이에 대하여 일반정보보호규정안은 표현의 자유를 보호하기 위한 예외를 설정하였다. 즉, 비평 목적이나 예술 또는 문학적 목적만을 위하여 개인정보가 처리되는 경우에는 잊힐 권리보다 표현의 자유를 우선하여 보호하고 있다. 이에 따라 언론이나 보도와 같은 시사·비평 기능을 수행하기 위한 표현이나 예술이나 문학을 위한 표현의 경우에는 그 중에 개인정보가 포함된다고 하더라도 잊힐 권리가 제한된다. 또한 보건 부문에서의 공익 외에 일반적 공익을 목적으로 개인정보를 처리하는 경우에도 잊힐 권리를 제한할 수 있을 것인가가 문제된다. 이에 대하여는 각국의 사정과 국민의 법의식, 법체계 등 각국이 처한 환경에 따라 다양한 입장이 전개될 것이다. 독일의 Walter Sedlmayr 사건과 관련된 범죄자의 정보 삭제요청 사례에서 보이는 것처럼 잊힐 권리를 중시하는 입장을 취하면 일반적 공익보다 잊힐 권리의 보호를 강조하여 일반적 공익의 예외를 인정할 수 없을 것이다. 일반정보보호규정안은 그러한 입장에 따른 것으로 보인다.

이상과 같이 잊힐 권리에만 인정되는 예외와는 별도로 일반정보보호규정안의 적용이 배제되는 일반적 적용 예외 사유가 존재한다. 즉, (1) 유럽연합 법률의 범위 외의 활동 과정 중의 개인정보의 처리, 특히 국가 안보와 관련된 활동 과정에서의 개인정보의 처리, (2) 유럽연합 기관, 기구, 관청 등에 의한 처리, (3) 유럽연합조약(Treaty on European Union) 제2장의 범위 내의 활동을 실행하는 과정에서의 회원국의 개인정보의 처리, (4) 개인적 또는 가정 내의 그 자신의 배타적 활동 과정에서 영리 목적이 아닌 자연인에 의한 개인정보의 처리, (5) 범죄 행위의 예방, 조사, 수사, 기소 또는 형사 처벌의 집행을 위한 주무기관에 의한 개인정보의 처리에 대하여는 일반정보보호규정안이 적용되지 않기 때문에 이에 대하여는 잊힐 권리에 관한 규정도 적용되지 않는다.

개인정보처리자는 다음에 해당하는 경우에는 개인정보의 삭제 대신 개인정보의 처리를 제한하여야 한다. 즉, (1) 정보의 정확성을 개인정보처리자가 검증할 수 있는 기간 중 정보주체가 정보의 정확성에 대해 이의를 제기하는 경우, (2) 개인정보처리자의 업무 수행 중 개인정보가 더 이상 필요하지는 않지만, 증명 목적으로 보관해야 하는 경우, (3) 정보 처리가 불법이면서 정보주체가 정보 삭제에 반대하며 사용 제한을 요청하는 경우, (4) 정보주체가 제18조 (2)에 따라 다른 자동화된 처리 시스템으로 개인정보의 전송을 요청하는 경우에는 개인정보의 처리를 제한하여야 한다. 이상의 경우에 예외적으로 보관이 인정됨에 더하여 증명의 목적, 정보주체의 동의, 다른 자연인이나 법인의 권리의 보호를 위하거나 공적 이익의 목적을 위하여만 처리될 수 있다. 개인정보의 처리가 제한된 경우에 개인정보처리자는 처리에 대한 제한을 취소하기 전에 저보주체에게 이를 알려야 한다.

개인정보처리자는 개인정보의 삭제나 그 정보의 보관의 필요성에 대한 정기적 검토를 위하여 설정된 시간제한이 준수되도록 보장할 메카니즘을 구축하여야 한다. 삭제가 실행되는 경우

3) 이 경우에 회원국 법률은 공공의 이익을 위한 목적을 충족하고, 개인정보의 보호를 위한 권리를 존중하고, 추구하는 합법적 목적에 적합해야 한다.

에 개인정보처리자는 그 개인정보를 다르게 처리하여서는 안 된다.

한편, 개인정보보호지침안 제54조는 개인정보처리자의 손해배상책임을 규정하면서, 동조 제3항에서 입증책임의 전환을 규정하고 있다. 즉, 개인정보처리자는 손해를 야기한 사건에 대하여 책임이 없다는 것을 입증함으로써 손해배상책임의 전부 또는 일부를 면제받을 수 있다. 일반정보보호규정안 제77조도 개인정보보호지침안과 동일한 규정을 두어 입증책임전환을 규정하고 있다.

## 3. 미국

최근 미국에서도 오바마 대통령이 "네트워크세계에서의 소비자정보프라이버시: 글로벌 디지털경제에서의 프라이버시 보호 및 혁신 촉진을 위한 기본구상"을 발표하면서, 소비자프라이버시권리장전(A Consumer Privacy Bill of Rights)을 제시하였다. 이는 개인정보와 관련한 개인의 권리 및 그에 대응하는 기업의 의무를 설정하고자 의도하고 있으며, 개인의 권리는 미국 국내외에서 인정되는 공정한 정보실행원칙을 기초로 한다. 이 권리장전의 적용대상은 개인정보의 상업적 이용이며, 개인정보란 특정 개인과 관련 있는 모든 정보를 의미한다. 이에 의하면 소비자에게 보장되는 권리 중에서 특히, 목적 제한적 수집(focused collection)에 따라 기업은 개인정보를 폐기하지 말아야 할 의무가 없는 이상 개인정보가 더 이상 필요하지 않은 경우 확실히 폐기하거나 비식별 처리하여야 한다고 천명하였다.

아울러 백악관은 소비자프라이버시 강화를 위하여 의회에 입법을 촉구하였는데, 관련 법안으로서 캘리포니아주 하원의원인 Jackie Speier가 2011.2.11. 발의한 온라인추적방지법안(Do Not Track Me Online Act of 2011, H.R. 654)과 2011.4.12. 캘리포니아주 상원의원들이 발의한 온라인 프라이버시권 보호 법안(Commercial Privacy Bill of Rights Act of 2011, S.799)이 있다. 온라인추적방지법안에 의하면, 타겟광고를 위하여 이용되는 온라인 추적으로부터 소비자가 옵트아웃할 수 있도록 규정하고 있다. 그런데 어느 것에 의하더라도 아직 미국에서는 적극적으로 개인정보의 삭제청구권을 일반적으로 인정하는 입법은 추진되고 있지 않다. 이는 구글이나 애플과 같은 클라우드컴퓨팅서비스기업이나 세계적 금융기관 등 미국의 글로벌기업들이 전세계의 개인정보를 활용한 기업활동에서 많은 이익을 거두고 있기 때문에 자유로운 기업활동을 최대한 보장한다는 측면에서 그에 저해가 될 수 있는 개인정보의 보호보다는 개인정보의 활용에 보다 더 초점을 맞추고 있기 때문인 것으로 보인다.

한편, 개인정보침해로 인한 손해배상책임에 대하여 개인정보처리자의 책임을 강화하는 일반적 규정을 두는 입법적 시도는 찾아보기 어렵다.

## 4. 일본

일본의 개인정보의 보호에 관한 법률에 의하면, 정보주체에게 개인정보에 관한 일정한 권리가 명문으로 인정된다. 즉, (1) 이용목적의 통지 요구(제24조제2항), (2) 보유개인정보의 공개 요구(제25조제1항), (3) 보유개인정보의 정정 요구(제26조제1항), (4) 보유개인정보의 이용정지 요구(제27조제1항, 제2항)에 대한 권리가 인정된다. 이 중에서도 특히 잊힐 권리와 관련된 것은 보유개인정보의 이용정지 요구권이다. 즉, 개인정보취급사업자는, 본인으로부터 해당 본인의 식별이 가능한 보유개인데이터가 본래의 합법적인 이용목적에 위반하여 취급되고 있다는 이유 또는 허위 기타 부정한 수단에 의하여 개인정보를 취득되었던 것이라는 이유에 의하여 해당 보유개인데이터의 이용의 정지 또는 消去(이하 "이용정지 등")를 요청받은

경우에, 그 요청에 이유가 있다는 점이 판명된 때에는 위반을 시정하기 위하여 필요한 한도 내에서 지체 없이 당해 보유개인데이터의 이용정지 등을 행하여야 한다(제27조제1항). 다만, 해당 보유개인데이터의 이용정지 등에 다액의 비용을 요하는 경우 기타 이용정지 등을 행하는 것이 곤란한 경우에 본인의 권리이익을 보호하기 위하여 필요한 대신할만한 조치를 취한 때에는 예외이다(제27조제1항 단서).

개인정보취급사업자는, 본인으로부터 해당 본인의 식별이 가능한 보유개인데이터가 제23조 제1항(제3자 제공의 제한)의 규정에 위반하여 제3자에게 제공되고 있다는 이유에 의하여 해당 보유개인데이터의 제3자 제공의 정지를 요청받은 경우에, 그 요청에 이유가 있다는 점이 판명된 때에는 지체 없이 해당 보유개인데이터의 제3자 제공을 정지하여야 한다(제27조제2항). 다만, 해당 보유개인데이터의 제3자 제공의 정지에 다액의 비용을 요하는 경우 기타 제3자 제공을 정지하는 것이 곤란한 경우에 본인의 권리이익을 보호하기 위하여 필요한 대신할만한 조치를 취한 때에는 예외이다(제27조제2항 단서).

개인정보취급사업자는, 이용목적 위반이나 부정한 취득에 근거하여 요청된 보유개인데이터의 전부 혹은 일부에 대하여 이용정지 등을 행한 때 혹은 이용정지 등을 행하지 않는다는 취지의 결정을 한 때, 또는 제3자 제공 제한 규정 위반에 근거하여 요청된 보유개인데이터의 전부 혹은 일부에 대하여 제3자 제공을 정지한 때 혹은 제3자 제공을 정지하지 않는다는 취지의 결정을 한 때에는, 본인에 대하여 지체 없이 그 취지를 통지하여야 한다(제27조제3항).

이러한 개인정보 이용정지 요구권은 일반적 적용예외사유에 해당하는 경우에는 그 적용이 배제된다. 즉, 동법 제50조에 의하면, 보도, 저술, 학술연구, 종교활동, 정치활동을 각각의 목적으로 하는 보도기관, 저술업자, 학술연구기관·단체, 종교단체, 정치단체인 개인정보취급사업자는 그 개인정보를 취급하는 목적의 전부 또는 일부가 각 해당 목적인 때에는 개인정보취급사업자의 의무에 관한 제4장의 규정을 적용하지 않는다.

한편, 일본의 개인정보의 보호에 관한 법률에는 개인정보처리자의 손해배상책임이나 그 가중에 대한 규정은 두고 있지 않다.

# Ⅲ. 국내법에 규정된 정보주체의 권리

## 1. 잊힐 권리

개인정보 보호법에는 EU의 잊힐 권리에 대응하는 규정으로서 개인정보의 삭제 요구권과 처리정지 요구권을 두고 있다.

개인정보 보호법 제36조에 의하면 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.[4] 개인정보처리자는 정보주체의 정정 또는 삭제 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여[5] 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다. 개인정보를 삭제할 때에는 복구 또는 재생되지 않도록 조치하여야 한다.

개인정보 삭제 요구권과는 별개로 개인정보 보호법은 제37조에서 개인정보의 처리정지 요

4) 이 경우에 개인정보처리자는 지체 없이 그 내용을 정보주체에게 알려야 한다.
5) 개인정보처리자는 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

구권을 규정하고 있다. 즉, 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다(제37조제1항). 이 경우 공공기관에 대하여는 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다. 이러한 요구를 받은 개인정보처리자는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 개인정보처리자는 (1) 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우, (2) 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우, (3) 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우, (4) 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우에는 정보주체의 처리정지 요구를 거절할 수 있다. 다만, 개인정보처리자는 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다. 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.

이러한 개인정보 삭제 또는 처리정지 요구권에 대하여만 인정되는 예외와는 별도로 개인정보 보호법 제58조에 규정된 일반적 적용예외 사유에 의하여 다음과 같은 개인정보에 대하여는 개인정보의 정정·삭제 요구권이나 개인정보 처리정지 요구권이 허용되지 않는다. 이러한 예외에 해당하는 개인정보로는 (1) 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보, (2) 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보, (3) 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보, (4) 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보가 있다.

## 2. 손해배상청구권

개인정보 보호법은 개인정보의 침해에 대하여 정보주체가 공정하고 합리적으로 피해를 구제받을 수 있는 실체적 권리를 보장하기 위하여 제39조에서 손해배상책임과 관련하여 민법에 대한 특례를 규정하고 있다. 즉, 개인정보처리자는 고의나 과실이 없음을 입증하지 못하면 개인정보침해로 인한 손해배상책임을 지게 된다. 이는 개인정보에 대한 침해가 발생한다고 하더라도 개인정보처리자와 정보주체 사이에 현저한 정보의 불균형이 존재하고 정보주체는 상대적으로 기술에 대하여 비전문가이기 때문에 정보주체가 개인정보처리자의 고의나 과실을 입증하는 것은 사실상 불가능하다는 점과 이로 인하여 정보주체의 피해에 대한 구제가 어렵게 되어 궁극적으로는 정보주체의 개인정보에 대한 권리를 효과적으로 보호하기 어렵게 된다는 점을 고려하여 입증책임을 전환한 것이다. 이는 기존의 정보통신망법에도 있던 규정이다. 그런데 개인정보 보호법은 이보다 더 나아가서 일정한 개인정보침해로 인한 손해배상책임에 대하여 개인정보처리자가 개인정보 보호법에 따른 의무를 준수하고 상당한 주의와 감독을 게을리하지 않은 경우에는 개인정보의 분실·도난·유출·변조 또는 훼손으로 인한 손해배상책임을 감경받을 수 있도록 규정하였다. 이에 따라 법원은 개인정보처리자가 개인정보 보호법에 따른 의무를 준수한 사실과 상당한 주의와 감독을 게을리하지 않은 사실을 입증한 때에는 임의적으로 감경할 수 있다.

# Ⅳ. 정보주체의 권리에 대한 검토 및 개선방향

## 1. 잊힐 권리

최근 EU가 보다 향상된 개인정보보호입법안을 제시하면서 잊힐 권리를 강조하고 있지만, 우리의 개인정보 보호법에 의하더라도 개인정보와 관련한 개인정보의 정정 또는 삭제 요구권이 명시적으로 인정되고 있으며, 그에 대한 특정 예외는 EU보다 좁아서 다른 법령에서 그 개인정보가 수집대상으로 명시된 경우에만 삭제요구가 받아들여지지 않는다.

반면, EU 일반정보보호규정안에 따르면, (1) 제80조에 따라 표현의 자유에 대한 권리를 행사하는 경우, (2) 제81조에 따라 공공 보건 부문에서 공익을 위한 경우, (3) 제83조에 따라 역사, 통계, 과학 연구 목적으로 필요한 경우, (4) 유럽연합 또는 개인정보처리자가 속한 회원국의 법률에 의해 개인정보를 보관해야 하는 법적 의무를 준수해야 하는 경우,[6] (5) 제4항에 따라 개인정보의 처리를 제한하여야 하는 경우에는 예외적으로 개인정보를 보유할 수 있어서 보다 넓은 예외가 인정된다. 그러나 이에 대응하여 우리 개인정보 보호법도 일반적 적용예외규정에 의하여 (1) 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보, (2) 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보, (3) 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보, (4) 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보에 대하여는 정보주체의 권리에 관한 규정이 적용되지 않기 때문에 결과적으로 언론, 종교단체, 정당의 개인정보의 수집·이용, 공공보건, 공공기관의 통계 목적으로 수집하는 개인정보, 국가안전보장을 위하여 수집 또는 제공 요청되는 개인정보에 대하여는 공통적으로 예외가 허용된다고 할 수 있다. 그럼에도 불구하고 특히 개인정보의 보호와 대응관계에 있는 표현의 자유와의 관계에서는 EU가 더 폭넓은 예외를 인정한다고 할 수 있다.

EU 일반정보보호규정안은 (1) 정보의 정확성을 개인정보처리자가 검증할 수 있는 기간 중 정보주체가 정보의 정확성에 대해 이의를 제기하는 경우, (2) 개인정보처리자의 업무 수행 중 개인정보가 더 이상 필요하지는 않지만, 증명 목적으로 보관해야 하는 경우, (3) 정보 처리가 불법이면서 정보주체가 정보 삭제에 반대하며 사용 제한을 요청하는 경우, (4) 정보주체가 제18조 (2)에 따라 다른 자동화된 처리 시스템으로 개인정보의 전송을 요청하는 경우에는 개인정보를 삭제하는 대신 개인정보의 처리를 제한하도록 규정하고 있다. 한편, 우리의 개인정보보호법은 개인정보의 처리정지를 요구할 수 있도록 규정하여, 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하도록 규정하였다. 이에 의하면 파기나 또는 이에 갈음하는 조치로서 EU가 규정한 처리제한조치를 포함하는 것으로 해석될 수 있다. 그런데, 우리의 개인정보 보호법은 처리정지 청구에 대하여 다시 폭넓은 예외사유를 규정함으로써 EU보다 정보주체의 처리정지 청구권은 그 인정범위가 제한적이다.

여기에서 주의할 점은 EU 일반정보보호규정안은 개인정보의 범위를 매우 넓게 설정함에 반하여,[7] 우리는 개인정보의 범위를 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및

---

6) 이 경우에 회원국 법률은 공공의 이익을 위한 목적을 충족하고, 개인정보의 보호를 위한 권리를 존중하고, 추구하는 합법적 목적에 적합해야 한다.

7) EU의 일반정보보호규정안과 달리 우리의 개인정보 보호법은 강력하고 폭넓은 형사처벌 규정을 두고 있는 점을 함께 고려하여야 한다.

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 규정하여 식별성 요건을 통하여 제한하고 있다는 점이다. 반면, EU 일반정보보호규정안은 개인정보보호 강화를 꾀하면서도 개인정보의 자유로운 이동의 안전한 보장을 균형 있게 규율하고자 하였는데, 우리의 개인정보보호법은 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고 개인의 존엄과 가치를 구현하는 것을 목적으로 하여 개인정보의 보호에 초점이 맞춰져 있는 점에서 미묘한 차이가 발생한다.

이상을 살펴보면, 적용되는 개인정보의 범위는 우리 개인정보보호법이 다소 좁을지 모르지만, 개인정보의 삭제요구권이나 처리제한 요구권에 관한 규정을 보면, 우리의 법제도 이미 상당부분 잊힐 권리에 관한 규정을 두고 있다고 할 수 있다. 특히, 개인정보의 삭제요구권의 경우에는 EU보다 상대적으로 좁은 예외를 설정함으로써 정보주체의 보호가 더욱 강조되는 면이 있다.

잊힐 권리를 별도의 권리로서 인정하건 개인정보자기결정권에 포섭하여 논의하건 관계없이, 이들 권리가 헌법상 보장되는 기본권이라고 하더라도 헌법상 기본권에 인정되는 제한은 잊힐 권리나 개인정보자기결정권에도 그대로 유효하다. 해외 입법사례와 우리 국민의 법감정을 고려하여 정보주체의 권리를 합리적인 범위에서 보호하는 것이 요구된다. 따라서 개인정보보호법 상의 잊힐 권리 혹은 개인정보자기결정권과 관련된 규정의 해석에 있어서도 다른 권리와의 비교 형량을 통하여 그 보호범위를 설정하여야 할 것이다. 특히, 개인정보의 보호와 안전한 활용의 보장의 조화라는 관점에서 개인정보를 활용하는 자의 이익 중 반드시 보호되어야 하는 범위를 한도로 하여 정보주체의 권리를 제한하는 것이 필요하다. 개인정보 삭제요구권의 예외사유로서 표현의 자유의 예외를 설정하는 것도 하나의 예이다. 이와 함께 정보주체의 권리를 실제로 어떠한 내용과 방법, 절차에 의하여 실현할 수 있는지에 대하여 법령에 명확히 규정하는 것이 필요하다. 현행 법령에 의하면, 구체적으로 어떠한 절차에 따라서 정보주체가 자신의 권리를 행사할 수 있는지에 대한 명확한 기준이 제시되고 있지 않다. 자칫 권리행사의 남용으로 인하여 개인정보처리자에게 심각한 피해를 줄 우려도 있기 때문이다. 또한 개인정보 삭제요구권이나 처리정지요구권 등 정보주체의 권리에 대하여 원칙적인 규정을 개인정보 보호법에 두고, 정보통신망에서의 개인정보, 금융정보 또는 의료와 같이 특별법상 예외적인 사유를 규정하거나 권리보호를 강화할 필요가 있다는 등의 사유가 존재할 때에 이를 개별법에서 규정하는 방식으로 일반법-특별법 관계를 명확히 하는 방향으로 일원화하는 것이 바람직하다.

## 2. 손해배상청구권

개인정보 보호법 제39조 제1항은 고의 또는 과실의 입증책임을 법률상 전환하는 규정형식을 취함으로써 기본적으로 과실책임의 원칙을 지지하면서 입증책임을 전환하는 중간책임의 성질을 규정하고 있다. 또한 동법 제39조 제2항은 개인정보 보호법에 따른 의무를 준수하고 상당한 주의와 감독을 게을리하지 아니한 경우에는 손해배상책임을 감경받을 수 있도록 규정하고 있다. 제39조 제1항 및 제2항을 모두 검토하면, 개인정보 보호법은 기본적으로 무과실책임의 원칙을 정립하고자 의도한 것은 아니라고 생각한다. 제1항에서 입증책임을 전환시키고는 있지만 책임성립에 고의나 과실을 요구하고 있기 때문이다. 반면, 제2항에서 일정범위의 손해배상책임에 대하여 상당한 주의와 감독을 게을리 하지 않은 경우에는 감경을 인정하고 있어서 이론상으로는 '상당한 주의와 감독 이상의 주의와 감독'을 하면 책임을 감면받을 수도 있도록

규정하여 기존의 민법상 중간책임과 유사한 것처럼 보인다. 그러나 실제에 있어서는 상당한 주의와 감독을 게을리 하지 않더라도 임의적으로 감경할 수 있을 뿐이지 면책을 인정하지도 않고 필수적으로 감경하여야 하는 것도 아니기 때문에 기존의 중간책임보다 훨씬 손해배상책임을 강화하고 있음을 알 수 있다. 더욱이 '상당한 주의와 감독 이상의 주의와 감독'을 했다는 것의 입증이 사실상 불가능하기 때문에 무과실에 거의 근접한 책임이라고 할 수 있다. 결국 제1항에서는 고의나 과실이 없음을 입증하면 책임을 면할 수 있는 것으로 규정했지만, 일정 범위에서는 제2항에 따라 '상당한 주의와 감독'을 다하였더라도 책임이 임의적으로 감경될 뿐이기 때문에 제1항의 과실의 의미에 대하여 모순이 발생한다. 개인정보침해로 인한 손해에 대하여 피해자인 정보주체의 구제의 실효성을 증진시킨다는 측면에서는 효과적일지 모르지만, 개인정보처리자에게 일정한 책임에 대하여는 어떠한 경우에도 책임을 질 수밖에 없다는 두려움을 심어주게 된다면 개인정보 보호법의 준수에 대한 유인이 감소할 수도 있다. 개인정보처리자에게 과중한 책임을 부과할 필요성이 있다고 하더라도 엄격한 요건을 충족하면 책임을 감면받을 수 있다는 가능성 혹은 책임에 대한 예측가능성을 주어서 국가나 민간의 각종 활동에 대한 불필요한 제약이 발생하지 않도록 하는 것이 타당하다.

결과적으로 국민의 법감정, 글로벌 스탠다드와의 조화, 개인정보 침해로 인한 구제의 실효성 확보, 개인정보의 활용성 등을 종합적으로 고려하여, 개인정보침해로 인한 손해에 대한 배상책임을 무과실책임으로 규정할 필요성이 있다면 오해의 소지 없이 명문으로 무과실책임을 선언하는 것이 타당하다. 그러나 개인정보는 보호와 활용을 적정한 선에서 조화시키는 것이 중요하며 개인정보 활용의 중요성이 나날이 증가하고 있는 시점에서 너무 과중한 책임을 지우는 것은 경제활동 전체에 엄청난 역효과를 발생시킬 수 있기 때문에 무과실책임의 위험을 사회에 분산시키는 "책임보험제도"의 지원 없이 무과실책임을 전면적으로 선언하는 것은 바람직하지 못하다. 따라서 (1) 손해배상책임을 발생시키는 불법행위의 유형에 따라 책임의 정도를 차별화하거나 (2) 과실책임을 유지하는 방향으로 제2항을 필요적 면책 규정으로 전환하거나 (3) 국민의 법의식이나 사회에 미치는 효과 등을 종합적으로 고려하여 무과실책임이 명백히 필요하다면 안전망으로서 책임보험제도를 도입하는 전제 하에 무과실책임을 선언하는 방안 등 가능한 방안을 모두 검토하여 바람직한 방향으로 법령을 개선하여야 한다.

# Ⅴ. 맺음말

개인정보는 인격적 이익의 발로로서 보호되어야 할 대상임에는 분명하지만, 현대 사회에서 그 경제적 가치를 무시할 수 없으며, 개인정보의 안전한 활용을 꾀하여 개인정보를 보호하고 나아가 개인의 인격적 가치를 보장하는 방향으로 입법과 법의 적용이 이루어져야 한다. 아울러 우리 경제가 세계 시장과 매우 긴밀한 관계를 맺고 있다는 점을 고려할 때 글로벌 스탠다드와도 가능하다면 부합하는 방향으로 나아가야 한다. 이러한 측면에서, 현행 개인정보보호법이 규정하고 있는 잊힐 권리와 관련된 개인정보주체의 자기결정권에 대한 규정이나 손해배상책임에 관한 규정을 개인정보의 보호와 안전한 활용의 조화라는 측면에서 보다 정밀히 검토하여 지속적으로 개선해 나가야 할 것이다.

# 잊혀질 권리와 알 권리 : 저널리즘적 관점에서

한겨레신문 온라인에디터 구본권

## Ⅰ. 현황 : '잊혀질 권리'의 등장

인터넷에서 불법적이지 않은 정보에 대해 이해관계자가 삭제를 요청할 수 있는 '잊혀질 권리(Right to be Forgotten)'에 대한 논의가 나라 안팎에서 본격적으로 이뤄지고 있다.

방송통신위원회는 2012년 9월25일 '제2차 방송통신 정책 고객 대표자 회의'를 열어서 2013년 잊혀질 권리에 관한 법안을 마련해 법제화를 추진하겠다고 밝혔다. 인터넷에서 유통되고 있는 개인정보에 대해 당사자가 삭제를 요청할 수 있는 권리를 부여하겠다는 게 방송통신위원회의 입법 추진 방향이다. 2011년 시행된 개인정보보호법에서 개인정보의 정정과 삭제에 대한 정보주체의 권리를 규정하고 있지만, 이 법에는 개인정보 삭제요구권의 행사 요건이 구체적으로 명시돼 있지 않다.

유럽에서는 잊혀질 권리의 입법 움직임이 이미 구체화했다. 2010년 프랑스 사르코지 대통령이 '잊혀질 권리'의 도입 필요성을 언급한 이후 2011년 유럽연합(EU) 집행위원회 비비안 레딩(Vivian Redding) 부위원장이 관련한 입법화에 나서면서 본격화했다. 2012년 초 비비안 레딩은 1995년 만들어진 유럽연합의 데이터보호지침(Data Protection Directive)은 인터넷 이전의 법제로 인터넷 환경에 맞는 새로운 법제가 필요함을 강조하고, 기존의 디렉티브(지침)를 구속력이 더 높은 레귤레이션(규정) 개정안으로 제시했다.

2012년 초 유럽연합 집행위원회에서 제시한 데이터보호규정(Data Protection Regualation) 개정안에서 '잊혀질 권리'는 정보 주체가 자발적으로 제공한 개인정보에 대해 '삭제할 권리(Right to delete)'로 구체화했다. 잊혀질 권리란 인터넷 사용자들이 자신의 개인정보에 대해 이를 관리하고 있는 정보처리 사업자에게 삭제를 요청해 서버에서 이를 지우도록 하는 것을 지칭한 것이기 때문에 실질적으로는 정보를 삭제할 권리다. 이 규정 개정안은 2014년을 목표로 유럽연합 각 회원국에서 입법화가 진행중이다. 유럽연합 법 체계상 레귤레이션은 회원국의 정부와 개인·법인 모두에 적용되는 강력한 규범이다. 유럽연합의 규정은 동일 사안에 관한 회원국 법률에 우선하기 때문에 27개 회원국들은 이 규정에 맞게 국내법을 제·개정해야 한다.

잊혀질 권리가 나라 안팎에서 새로운 프라이버시 권리로 주목받는 까닭은 디지털 정보혁명으로 정보의 생산과 전달·보존 방법이 근본적으로 변화한 게 배경이다. 생산된 뒤에 유통 단계를 거칠수록 품질이 떨어지고 시간이 지나면서 자연스럽게 망각되거나 낡아가던 아날로그 시대의 미디어 콘텐츠가 디지털로 바뀌면서 일어난 현상이다. 0과 1로 된 디지털 정보는 거듭된 복제와 전송에도 원형 그대로 보존이 가능하고 시간의 흐름에도 영향을 받지 않는 보존성을 갖고 있다. 내구성과 원본 복원력을 지닌 디지털 정보가 인터넷이라는 글로벌 네트워크를 통해 실시간으로 유통되고 복제되어 국경과 언어권을 넘어 활용되고 있다. 그동안 종이나 필름 등 미디어에 아날로그 형태로 기록돼 유통돼 왔던 콘텐츠가 가상 재화(virtual goods)로 바뀌면서 이제까지의 물리적 제약을 넘어서고 있다.

"세상의 정보를 수집하고 조직화해서 누구나 접근 가능하고 유용하게 만드는 것"을 목표로 하는 구글과 같은 검색엔진을 통해 전세계의 정보는 인터넷을 통해 손쉽게 접근할 수 있다. 또한 사용자가 목적을 갖고 디지털 형태로 만든 텍스트 정보만이 아니라, 이미지와 동영상 등 다양한 포맷의 정보도 검색이 손쉽다. 인터넷이 등장하기 이전에 만들어져 검색엔진이 도달할

수 없던 아날로그 정보의 영역까지도 디지타이제이션(Digitization) 기술을 동원해 디지털화된 데이터베이스로 변모시키고 있다. 페이스북이나 트위터처럼 이용자들간에 직접적 소통이 이뤄지는 소셜네트워크 서비스들의 이용이 늘어나고 소셜네트워크에서는 개인정보에 해당하는 내용들이 여과없이 유통되고 있다. 인터넷 검색엔진은 소셜네트워크 등으로 지인들끼리 순간적으로 주고받았던 개인적 정보나 한때의 감상 토로도 손쉽게 찾아낸다.

한번 생성된 정보가 인터넷에서 망각되지 않는 현실은 특히 개인적 정보와 프라이버시에 관련되어 지대한 영향을 끼치고 있다. 인터넷의 서비스가 다양해지고 사용 범위와 용도가 늘어나면서 개인적 정보와 프라이버시에 관련된 내용이 유통되고 있는데 사용자들이 인터넷에 한번 올라간 정보를 삭제하기 매우 어렵다는 현실에 직면하고 있다. 특별히 중대한 기록이거나 공적 정보가 아니라면 자연히 세월의 흐름에 따라 망각되는 인간과 사회의 기억체계에 익숙한 사용자들로서는 곤혹스러운 현실이다. 인터넷과 디지털 기기의 보급과 함께 인터넷에서 지워지지 않는 개인정보와 관련된 기록들로 인해 다양한 유형의 피해 보고가 갈수록 늘어나고 있다.

마이어쇤베르거(Mayer-Schönberger 2009)는 정보의 디지털화, 인터넷과 같은 전지구적 네트워크, 인터넷 검색엔진, 디지털 저장장치의 저렴화 등의 요인으로 인해 기억과 망각에 관한 인류의 인지 구조가 역전됐다고 주장했다. 유사 이래로 인류에게는 망각이 일반적이어서 그림이나 문자 등 각종 보조적 장치를 통해서 기억을 보존해오려고 노력했지만 디지털 환경에서는 망각과 기억의 관계가 역전돼, 특별한 노력을 기울이지 않으면 인터넷에 한번 기록된 것이 사라지지 않는다는 것이다.

오래되어 어디에 있는지 모르고 사실상 '잊혀진' 정보를 인터넷에서 순식간에 검색해 찾아주는 편리한 정보 생활의 도구인 검색엔진이 가져온 부작용으로 인해 이미 마찰은 시작됐다.

2009년 말 독일에서는 독일 위키피디아를 상대로 유명배우 살해에 연루되어 복역한 이들이 정보 삭제를 요구해 삭제한 바 있다.[1] 스페인에서 한 성형의사는 자신의 이름을 구글에서 검색하면 20년 전의 성형수술 실패에 관한 정보가 맨 먼저 노출돼 의사로서의 평판을 해친다는 이유로 구글을 상대로 검색 결과의 수정을 요청하는 소송을 벌였다.[2] 원고는 문제가 된 기사가 게재된 엘 파이스(El Pais) 신문사 웹사이트의 인터넷 기사에 대해서는 삭제요청을 하지 않았다. 스페인 데이터보호위원회는 스페인에서 언론의 표현자유 영역은 보장되어 있지만 인터넷 검색결과에서는 아니라고 주장했으며, 스페인 법원은 유럽연합의 최고법원인 유럽 사법재판소(European Court of Justice)의 판단을 받아보겠다고 의뢰한 상태다.

아르헨티나에서는 유명가수(Virginia Da Cunha)가 구글과 야후를 상대로 자신이 과거에 촬영한 야한 사진이 검색에 노출되어 명예훼손을 일으킨다고 삭제를 요구해 1심에서 승소했다. 2006년부터 시작되어 130여건의 유사한 케이스로 확대된 이 소송에서 2심 재판부는 2010년 8월 원고 패소 판결을 내렸다. 항소심 재판부는 구글과 야후는 해당 콘텐츠가 명백히 불법적 콘텐츠라는 점을 인지하고, 삭제를 게을리 했을 경우에만 명예훼손 책임이 있다고

1) 1990년 독일에서 발터 제들마이어(Walter Sedlmayr)라는 배우가 살해된 사건이 발생했다. 볼프강 베를레(Wolfgang Werle)와 만프레트 라우버가 범인으로 밝혀져 15년을 교도소에서 보냈다. 이들은 출소 뒤 위키피디아에 이 사건과 관련된 항목에서 자신들의 이름을 지워줄 것을 요구했다. 독일 법정은 2008년 1월 이들의 손을 들어줬고, 위키피디아 독일어판에서 이들의 이름은 사라졌다. 그러나 미국에서 운영되는 위키피디아 영어판은 표현의 자유를 규정한 미국 수정헌법 1조를 들어 요구를 거절했다.

2) 1991년 스페인 일간신문 EL Pais에 실린 Dr. Hugo Guidotti Russo와 환자와의 분쟁을 다룬 기사가 대상이다. 스페인 데이터보호위원회는 구글이 단지 엘 파이스의 인터넷 뉴스를 검색을 통해 연결시킨 중개행위 이상의 적극적인 행위를 했다고 구글의 책임을 주장했다. 구글은 원활한 서비스를 위해서 자체 서버에 검색대상 기사를 일시저장(캐시)하고 인덱싱을 통해 서열을 매겨 서비스하는 등 중개 이상의 행위를 했다는 것이다.

판결했다.[3]

'잊혀질 권리'를 인정하고 있지 않은 미국에서는 유사한 사안에 대한 법원의 판단이 다르다. 캘리포니아의 한 대학에서 운동선수로 활동하다가 2010년 사망한 한 학생의 아버지가 아들이 4년 전 술집에서 벌인 소동을 다룬 과거 기사를 온라인 데이터베이스에서 삭제해달라고 언론사에 요청한 뒤 거부당하자 이에 대해 손해배상 청구소송을 낸 바 있다.[4] 소 제기자는 패소했다.

2010년 미국 펜실베이니아주에서 두 대학신문을 상대로 제기된 과거 기사 삭제 요청도 해당 신문사들의 거부로 받아들여지지 않았다. 펜실베이니아의 더 센터 데일리 타임스(The Centre Daily Times)와 더 데일리 컬리지언(The Daily Collegian)은 센터 카운티의 판사로부터 경미한 범죄를 저지른 두 사람에 관한 기사 삭제 요청을 받았으나, 이를 묵살했다. 기사 삭제를 요청한 쪽은 법원으로부터 전과 기록 말소 명령을 받아 법적 기록을 삭제했지만 이에 관한 과거 기사가 검색되면 소용이 없다며 법원에 신문사 기사의 삭제 명령을 요청했다. 하지만 신문사쪽 변호사는 보도될 당시에 정확한 기사라면 불법이 아니며 이는 헌법의 보호를 받는 발언이라며 삭제를 거부했다. 결국 해당 법원 판사는 신문사에 기사 삭제를 요청한 애초의 명령을 번복하고 해당 기사로 연결되는 참조 링크를 삭제하라는 새로운 전과기록 말소 명령을 발부했다.

국내에서도 과거 기사 삭제, 수정과 관련한 이해 당사자들의 요구가 생겨나고 있는 상황이다. 특히 NHN의 네이버가 운영하는 과거 신문 보기 서비스인 뉴스 라이브러리가 2009년 4월30일부터 '옛날 신문보기'라는 서비스로 제공되기 시작하면서 과거 기사에 대한 접근성이 크게 높아졌다. 하루 방문자가 1700만여 명인 네이버 사이트에서 검색 결과 안에 포함되어 노출되기 때문에 접근성과 파급력이 뛰어나다.[5]

국내에서는 과거 기사를 온라인에서 삭제해달라는 주장이 법정에서 소송을 통해 제기되지 않았지만, 일부 언론사와 포털에 등재된 과거기사에 대한 삭제 요청이 간헐적으로 제기돼 왔으며 일부 기사는 당사자의 요청으로 인해 과거 데이터베이스에서 수정되거나 삭제된 경우가 있다. 1975년 한 인기가수의 피소와 관련해 3개 신문사에 실린 기사는 37년이 경과한 2012년 온라인에서 그 서비스 형태가 차이난다.[6] 신문사에 따라 당사자의 기사 수정 요청을 수용한 정도가 달라서 기사의 수정 여부와 수정 범위가 다르다.

---

3) 판결 이후 구글과 야후는 서로 다른 방식으로 대응했다. 구글은 법원의 삭제 명령을 광범하게 적용하는 것은 불가능하다는 태도를 고수했고, 야후는 원고들이 언급된 모든 사이트를 차단하고 해당 주소의 사이트에 법원의 명령을 게시했다.

4) 2010년 말 UC버클리대학의 풋볼팀 선수였던 Chris Purtz의 아버지 Harvey Purtz가 미국 Daily Californian Newspaper의 편집장인 Rajesh Srinivasan을 상대로 소송을 제기한 사건이다. Chris Purtz는 4년 전에 샌프란시스코 스트립클럽에서 말썽을 부린 게 이 신문에 보도됐고 문제가 되어 이후 팀을 떠나 2010년 6월 죽었다. Harvey Purts는 아들 사망 한달 뒤 Daily Californian Newspaper 상대로 온라인에서 4년 전 기사의 삭제를 요청했으나 거부당했다. 이에 Harvey Purts가 7500달러의 손해배상 청구소송을 냈으나 패소했다.

5) 네이버 뉴스라이브러리는 1920년부터 발행되기 시작한 동아일보를 비롯해 경향신문(1946년 창간)과 매일경제신문(1966년 창간)에 대해 1999년까지 80년치의 신문 전체 분량을 제공한다. 무료로 제공되고 있으며, PDF 지면 형태와 더불어 한자가 한글로 변환되어서 텍스트로도 서비스된다.

6) "가수 태진아 피소 간통혐의로(〔경향신문〕 1975년 1월29일 7면) 서울 서부서는 29일 모건설회사 사장부인 김**씨(47 서울**********)와 74년도 모방송국 신인가수상을 받은 가수 태진아씨(본명 조방헌 21)를 간통혐의로 구속했다. 김 여인은 2남2녀의 어머니로 지난 74년 5월부터 지난 27일 사이 10여 차례 자기보다 26살이나 나이가 적은 조씨와 놀아났는데 돈이 많은 김 여인은 조씨와 만날 때마다 80만~100만원씩의 용돈을 주기도 했다는 것." 이 기사는 네이버 뉴스라이브러리에서 볼 수 있는 3개 신문(경향신문, 동아일보, 매일경제신문)에서 실려 있다. 하지만, 언론사에 따라서, 기사의 서비스 상태가 다르다. 경향신문과 매일경제신문에서는 위와 같이 해당 사건 관련자의 실명과 주소가 지워진 채 서비스되고 있지만 동아일보는 두 신문과 달리, 사건 당사자의 실명과 주소를 지우지 않은 채 과거 발행당시 그대로 서비스하고 있다.

## Ⅱ. 프라이버시권과 알 권리의 충돌

보도될 당시에 문제 되지 않던 '진실 보도'의 기사가 오랜 시간이 지난 뒤 관련자에게 권리 침해를 이유로 삭제 요구를 받는 상황은 디지털 문명이 인류에게 부과한 풀기 어려운 과제다. 사실 보도와 역사적 기록의 보존, 프라이버시와 인격권, 언론과 표현의 자유, 전과 기록과 행복추구권 등 다양한 권리가 충돌하는 복합적 문제다. 디지털 기술과 환경의 도래로 기사 자체의 영향력 범위와 구조가 과거와 크게 달라진 것이 한 이유이고, 또 하나의 이유는 시대에 따른 변화로 기사에 대한 기준이 달라진 일종의 문화지체(cultural lag) 현상을 들 수 있다.

과거의 기사가 현재에 유통되면서 생겨나는 프라이버시 문제는 언론의 보도 내용과 보도 기준이 당대의 사회적 필요와 합의에 따라서 형성되었다는 특성을 배경으로 하고 있다. 보도될 시점에는 당시의 사회적 필요와 합의에 따라서 문제가 없는 보도였지만, 기술적 발전에 따라 보도 당시가 아닌 다른 시점에서 기사가 유통되면서 달라진 보도 기준과 사회적 필요와 충돌하는 현상이 생겨났기 때문이다. 또한 수십년전 기사에 관련된 당사자가 생존해 있는 시점에 과거의 시점과 사회환경에서 주로 통용되던 형식의 기사가 그 맥락을 잃어버린 채 유통되는 문제가 일어나고 있다. 더욱이 그 당사자가 공인이 아니거나 어느 시점 이후 공인의 지위를 잃어버린 평범한 개인으로의 삶을 살고 있는 경우라면 그 침해는 더 심각해진다.

공적 관심사에 대한 사실을 취재해 보도하는 언론의 본업이 시대에 따라 크게 달라지지 않지만 기사의 형태로 전달하는 정보의 내용과 형식은 시대적, 사회적 합의의 기준에 따라 변화한다. 네이버 뉴스라이브러리와 언론진흥재단의 과거 기사 검색서비스 미디어가온, 조선일보, 중앙일보의 검색 데이터베이스, 국사편찬위원회가 구축한 한국역사정보 통합시스템 등의 데이터베이스를 통해 과거의 신문 기사를 인터넷으로 검색할 수 있는데 시대별로 기사의 표현 방식과 취재대상의 개인정보 노출 정도가 다르다.

언론의 범죄 보도에서 프라이버시 노출 정도가 달라지는 주된 계기는 언론계 내부의 윤리 기준이나 자율적 합의와 법원의 판결이다.

인터넷으로 검색되는 국내 과거 신문기사에서 개인정보의 노출 정도는 앞서 살펴본 1975년의 한 가수 간통 피소 기사의 수준과 크게 다르지 않다. 수사나 체포 단계에서 혐의자와 범죄 피해자, 사건 관련자의 실명과 나이, 집 주소, 직업 등이 그대로 나타난다.[7] 언론의 범죄 보도 기사에서 개인정보 노출 관행이 바뀌게 된 계기는 1998년 대법원의 판결 이후다. 대법원은 이혼소송을 제기한 원고 아내가 남편에게 청부 폭력을 행사했다는 내용의 언론 오보사건에 대한 판결에서 범죄 보도의 실명 요건을 엄격하게 제한했다. 대법원은 범죄보도는 공익에 속하지만 범죄 보도를 위해서 범인이나 범죄 혐의자의 신원을 밝힐 필요가 있는 것은 아니기 때문에 범인과 혐의자에 대한 보도가 공익성을 지니지 않는다고 판결했고 이후 언론의 기사 작성 관행은 크게 달라졌다.

검찰, 경찰, 국세청 등 국가 기관이 발표하는 범죄 혐의 피의자에 대한 언론 보도의 관행도 1998년 이른바 '진모양 사건'에 대한 대법원의 판결로 기존의 관행이 달라지게 된다. 언론의 보도 관행은 사회적 합의와 이에 따른 법률에 따라 달라지게 된다. 잇단 강력범죄의 대책의 일환으로 강력범죄 피의자에 대한 신상 공개 원칙이 최근 다시 바뀌었고 대부분의 언론은 특

---

7) '가전제품 상습절도'〔한국일보, 1991년 1월13일 22면〕 서울시경 특수대는 12일 김대선씨(35·전과4범·서울 영등포구 대림1동 856) 등 2명을 상습특수절도혐의로 구속영장을 신청하고 박길진씨(26) 등 2명을 수배했다. 경찰에 의하면 고향 선후배 사이인 이들은 지난 7일 상오 10시께 경기 부천시 중구 중동 769 강중선씨(30) 집의 잠긴 문을 절단기로 끊고 들어가 안방에 있던 VTR 1대를 훔치는 등 지난해 6월부터 지금까지 14차례에 걸쳐 8백여만 원 상당의 가전제품을 훔친 혐의다.

정강력범죄의 처벌에 관한 특례법 개정에 따라 해당 범죄 피의자의 얼굴과 이름을 공개하고 있다. 모든 언론사가 기사에서 범죄자와 용의자의 신원 공개 기준을 동일하게 적용하지는 않고 있으며 구속과 재판 등 혐의 확정 이후의 단계부터 신원을 보도하는 언론사가 있는가 하면 혐의자 지목 초기 단계에서부터 실명과 사진 보도를 하는 경우도 있다.

언론의 보도 관행이 법률 제정 등 외부의 요인에 의해서만 달라지는 것은 아니다. 현재 대부분이 신문이 채택하고 있는 기사 실명제는 언론계의 암묵적 합의에 따른 변화다. 과거에는 사건사고를 보도하는 이른바 '스트레이트 기사'의 경우, 기자의 주관이나 가공, 해석이 개입될 수 없는 객관 보도의 영역이라 여겨 취재기자의 이름을 명기하지 않았으나, 1993년 4월1일 〈조선일보〉가 사고를 통해 기사실명제를 표방한 이후 기사 실명제는 언론계에 정착했다.

기사의 작성 형태나 취재원이나 보도대상의 개인정보 등에 대한 언론계와 사회적 합의의 기준이 시대와 환경에 따라 달라지고 있다. 하지만 인터넷의 과거 기사 서비스는 보도 당시 사회적으로 수용되었던 기사의 형식과 관행이 상당한 시간이 흘러 적절하지 않은 형태로 유통되게 하면서 새로운 프라이버시 문제를 만들어내고 있다.

기사가 유통되는 환경과 그로 인한 영향력이 달라졌는데, 관련한 법제는 그대로인 까닭에 전에 없던 문제가 생겨나고 있다. 대부분의 언론 보도 기사는 일간, 주간, 월간 등 매체의 발행주기에 따라서 발행 당시에 주로 읽히고 뉴스가치가 높은 사안이나 공적 인물이 아닌 경우에는 시간의 경과와 더불어 대중의 기억 속에서 자연스럽게 잊혀져 왔다.

언론의 기사가 특정한 기간 동안 통용되는 한시적 유효성을 갖는다는 인식은 언론중재 및 피해구제 등에 관한 법률(언론중재법)의 정정보도 청구 요건 규정에도 반영돼 있다. 언론중재법은 언론 보도로 인한 피해에 대해 정정보도 청구 기한을 보도 이후 6개월 이내로 한정하고 있다. 정정보도 청구 요건을 규정한 언론중재법의 제14조는 2009년 2월 언론중재 대상에 인터넷언론사를 포함시키며 달라진 언론 환경을 반영하는 내용으로 개정이 이뤄졌지만, 보도가 있은 지 6개월이 지난 경우에는 정정보도를 청구할 수 없다는 조항은 개정되지 않았다. 이러한 조항은 기사가 보도된 지 6개월이면 관련자에게 충분한 이의 제기기간을 제공한 셈이 되고 6개월이라는 기간이 지나면 기사로서의 사회적 영향력 등 실질적 효과와 그로 인한 관련자의 이익 침해가 상당부분 줄어들 것이라는 판단이 입법 의도에 반영돼 있는 것으로 해석된다. 인터넷언론을 중재대상으로 포함시키면서도 기존에 신문과 방송을 염두에 두고 제정된 정정보도 청구 시한에서 보도된 지 6개월 이내라는 이의제기 요건이 달라지지 않은 데에는 기사의 실질적 영향력과 관련한 판단으로 볼 수 있다.

인터넷은 묵은 기사 찾기 같은 정보 검색 기능을 제한된 장소에서 전문가가 수행하던 것에서 만인의 일상생활 속으로 바꿔놓았다. 스마트폰과 같은 모바일 인터넷 기기의 사용은 이동하면서도 인터넷에 접속해 방대한 정보를 찾아낼 수 있는 환경을 만들어냈다. 정보의 디지털화와 검색 기능의 발전, 모바일 기기 등 유비쿼터스 컴퓨팅 등 환경 변화는 그동안 분류되지 않은 종이더미에 쌓여 정보로서의 생명력을 상실한 '실질적 모호성(practical obscurity)' 상태의 사실상 잊혀진 정보를 언제 어디서나 호출될 수 있는 '살아 있는 정보'로 바꿔놓았다.[8]

유럽연합은 언론보도, 예술, 문학은 잊혀질 권리가 적용되지 않는 영역이라고 밝혔지만, 인터넷상에서 게재 당시 문제가 없던 정보를 삭제하는 것은 현실적으로 어려운 일이다. 구글, 페

8) 미국 연방대법원은 1989년 기록의 전산화를 반영해 그 이전 시기에 제정된 정보공개법(FOIA)에 기반해 접근가능한 정부의 정보를 모아놓은 데이터베이스에 대한 접근권을 제공해달라는 언론의 요구에 대해 '실질적 보호성(practical obscurity)' 논리를 제시하며 거부했다. U.S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U.S. 749 (1989)

이스북 등 글로벌 인터넷 기업은 공개적으로 '잊혀질 권리'에 반대한다고 밝히고 있다. 하지만 구글은 유럽연합이 '개인정보 삭제 요청권'으로 구체화한 부분에 대해서는 일부 수용할 방침을 밝혔다. 유럽연합의 데이터보호 레귤레이션이 공표된 직후인 2012년 2월 구글은 자사의 공식 블로그에 '잊혀질 권리에 대한 구글의 생각'이란 글을 올려 이에 관한 입장을 공개했다. 구글은 이용자가 구글 플랫폼에 올린 자신의 글에 대해 삭제 요청을 할 경우 삭제할 권리를 원칙적으로 허용하지만, 플랫폼의 특성에 따라 이 삭제권이 현실적으로 제한될 수밖에 없다는 한계를 밝혔다. 구글 서비스의 이용자로 구글이 관리하는 영역에 콘텐츠를 올린 사용자가 해당 콘텐츠에 대해 삭제를 요청할 경우 이에 대한 삭제권은 허용된다. 하지만, 이 콘텐츠를 제3의 사용자가 복제하거나 가져가 자신의 블로그 등 애초 글 게시자의 관리권한 밖에 있는 영역에서 다시 발행할 경우 애초 게시자의 삭제권은 적용되지 않는다. 구글은 또 콘텐츠 삭제권으로 인해 구글 서비스의 안전현실적해치거나 사기 등 범죄에 취약하게 될 현실적해치글 작성자의 삭제권실적의무화범죄에 취약고 밝혔다. 1명의 사용자가 아닌 다수의 사용자가 협업을 통해 만든 콘텐츠에 대해 1명의 참여자가 삭제를 요청할 경우, 구글은 이에 대해 삭제 기준이 없다고 밝혔다. 콘텐츠 전체에 대한 공동 작성자일 경우와 게시글와 댓글의 관계에서처럼 1차적인 작성자와 부수적인 작성자의 관계로 구분된다. 구글은 자사의 플랫폼 안에 등록된 콘텐츠에 대해서만 제한적으로 작성자에게 삭제권을 제공할 뿐, 제3자에 의해 발행된 콘텐츠는 모니터하거나 삭제할 수 없다고 밝혔다.

하지만 현재 유럽연합의 데이터보호규정 개정안이 요구하는 잊혀질 권리는 그 이상이다. 잊혀질 권리의 실행안은 표현 자유를 침해하지 않는 한 개인은 웹사이트에서 자신의 개인정보에 대해 삭제 요청을 갖고, 웹사이트 운영자는 사용자로부터 삭제요청을 받은 개인정보를 자신의 서버와 함께 제3자의 서버에서도 지워지도록 노력해야 한다고 되어 있다.

인터넷 통신규약인 TCP/IP를 개발한 빈트 서프는 온라인에서 잊혀질 권리는 달성될 수 없기 때문에 전혀 현실적인 방안이 될 수 없다고 반대했다. 누군가 온라인에 정보를 공표한 뒤에 삭제해서 잊혀질 권리를 보장하겠다는 것은 마치 책을 출판한 뒤에 구매자가 보유하고 있는 모든 책을 수거해서 없애버리겠다는 의도와 같은 비현실적인 제안이라는 것이다. 인터넷에서는 정보를 내려받고 공유하는 과정이 매우 간편하기 때문에, 정보가 일단 공표되어 다른 사람의 수중에 넘어가버리면 그를 삭제한다는 것이 현실적으로 불가능에 가깝다는 주장이다.

인터넷이 있기 전부터 사회는 인위적 망각체계를 법으로 도입해왔다. 신용정보 삭제와 전과기록 삭제가 대표적인 사회적 망각 시스템이다. 과거 한때 잘못을 저지른 사회 구성원들에게 과거로부터 단절해 새 출발을 할 수 있는 기회를 제공하는 제도다. 어느 나라에서나 청소년 보호를 위해 성장과정에 있는 청소년의 범죄에 대해서는 그 기록의 보존과 공표를 엄격히 통제하고 있다. 특정한 기록과 사실을 사회가 제도를 통해 의도적으로 기억하지 않거나 기록 삭제를 통해 망각하려고 하는 것은 기억과 망각이 자연스러운 현상만이 아니라, 의도적인 현상의 측면이 있다는 것을 보여준다. 블랑셰트와 존슨(Blanchette & Johnson 2002)은 사회적 망각을 통한 프라이버시 보호가 개인적으로 유익할뿐 아니라 사회적으로 가치가 크다는 점을 지적했다.

우리나라에서도 일정 시간이 지난 뒤에는 전과 기록과 신용정보 기록을 공식적으로 삭제해 더 이상 활용하지 못하도록 법률로 정해, 사회적 망각을 적용하고 있다.  형법과 형 실효에 관한 법률은 범죄자가 형을 선고받고 집행을 마치면 법정 최고형의 경우에도 형 집행 종료 10년 뒤에는 형이 실효된 것을 규정하고 있다. 형이 실효되면, 전과기록에 해당하는 수형인명부

의 기록을 삭제하고 수형인명표를 폐기하고 있다. 신용정보 이용과 보호에 관한 법률은 신용정보 ü마치게 불리한 정보에 대해 그 사유가 사라지면 5년 부의  대해 것을 규정하고 있다. 청소년 범죄를 다루고 있는 소년법은 기록의 열람과 유통에 대해 더 엄격한 기준을 적용하고 있다.

그러나 어떤 정보를 제도화된 망각 시스템으로 포함시킬 것인지, 또 특정 정보에 얼마나 오랜 시간이 경과한 이후에 망각에 포함시킬지 여부에 대해서는 국가별로 상당한 차이를 보인다. 미국에서는 범죄 기록을 삭제하는 형 실효에 관한 법률과 같은 제도가 없다. 주별로 법률에 따라서 경범죄의 경우에 처벌을 받고 일정 시간이 경과한 이후 당사자가 개별적으로 전과 기록 삭제 요청 재판을 청구할 수 있도록 돼 있다. 미국에서는 오히려 재판 기록 공개나 현행법 체포 사진 등의 인터넷 공개가 국민의 알 권리 차원에서 이뤄지고 있지만, 개인의 신용정보나 파산기록과 같은 금융 정보에 대해서는 이와 다른 기준을 적용한다.

## Ⅲ. 제언 : 잊혀질 권리와 알 권리의 공존

프라이버시권과 표현의 자유는 한쪽의 권리 보장이 다른 쪽의 침해를 가져오는 관계이기 때문에 법 제정을 통한 일괄적 조정안 시도보다 사안별로 접근해 구체적 상황에서 현실적 조화를 추구하는 게 바람직하다.

프라이버시는 국가별로 개념과 보호 내용이 차이나고 사회와 문화에 따라 고유한 역사적 산물이다. 또한 소셜네트워크 환경과 잊혀질 권리의 등장처럼 새로운 기술적 환경의 영향을 받는다. 성급하고 강제적인 해결책보다 현존하는 문제를 다룰 수 있는 유연한 형태의 이해 조정방안이 업계와 전문가 위주로 논의되고 모색되어야 할 이유다.

잊혀질 권리 도입을 추진하는 유럽연합에서도 언론 보도는 문학, 예술과 함께 예외대상으로 명시하고 국내에서도 기사는 개인정보보호법상 삭제 대상이 아니다. 하지만 오래된 기사의 인터넷 노출로 인한 피해 호소와 그 처리는 법률을 뛰어넘는 해결책을 요구하고 있어 이를 계기로 오래된 정보의 인터넷 유통에 관한 논의와 사회적 합의를 모색해볼 수 있다.

국내외 일부 언론사가 오래된 기사로 인한 피해를 처리하기 위한 내부 기준을 만들어 적용하고 있는 것은 참고할 만한 사례다. 미국 〈패서디나 위클리(Pasadena Weekly)〉는 2006년 종이신문에 기사가 게재된 지 6개월 뒤에는 온라인 아카이브에 저장된 기사에서 피의자 이름을 삭제하기로 결정한 바 있다. 〈한겨레신문〉은 2006년 과거 기사에 대한 수정, 삭제요구가 있을 경우에 1) 최종심에서 무죄나 무혐의임이 확인된 경우 2) 오보 3) 불필요하게 개인정보가 노출된 경우에 한해 이를 반영한다고 지면을 통해 밝혔다. 〈뉴욕타임스〉는 과거 기사 수정을 역사 지우기로 인식해 수정을 허용하지 않는다. 오보나 표절도 삭제나 수정을 하지 않고 대신 문제가 된 과거기사에 '편집자 주(edtor's note)'를 첨부하는 방식을 사용한다. 표절로 문제가 된 제이슨 블레어의 뉴욕타임스 기사도 아카이브에 그대로 남아 있으며, 편집자 주를 첨부해 표절 확인 사실 등을 밝히고 있다. 하지만 국내에서 범죄 피해자와 일반인의 신상정보가 고스란히 노출된 과거 기사에 대한 언론사별 수정 정도 차이에서 확인되는 것처럼, 언론사 공통의 기준이나 합의는 없는 상태다.

디지털화 이전의 정보보호 법제로는 소셜네트워크 서비스 환경의 새로운 프라이버시 문제를 해결할 수 없는 게 현실이다. 새로운 기술과 사용환경을 반영해 프라이버시 개념과 권리를 업데이트하되, 저널리즘의 기능과 표현의 자유가 디지털 환경에 맞추어 새롭게 정의되어야 할 필요성이 높다.

급변하는 정보기술은 그 변화가 현재에도 진행형이고 계속 발전해가고 있어 기술과 서비스의 진화 과정에서 과거 기사로 인한 프라이버시 침해 및 명예훼손과 같은 새로운 문제와 부작용도 나타난다. 섣부른 입법을 통한 해결책보다는 문화 지체 현상의 일종으로 보아 포괄적이면서도 지속적이고 유연한 접근이 우선될 필요가 있다. 입법에 앞서 관련 이해 주체들의 논의를 통한 자율적 해결책과 조정이라는 대안이 실효성과 유연성 측면에서 바람직할 수 있다. 공인이 아닌 일반인의 과거 기사로 인한 프라이버시 침해와 명예훼손의 경우 언론 관련 단체와 언론피해 중재기구의 자율적 기준과 조정안을 통한 모색이 우선되어야 한다.

언론계가 합의한 공통의 기준 없이 회사별로 적용하고 있는 과거 기사나 오보에 대한 수정·삭제 처리 기준을 공론화해서 일종의 가이드라인을 제정할 필요가 있다. 시대와 법률에 따라 기사의 개인정보 노출 수준이 변화해온 만큼, 현재 시점에서 통용될 수 없는 과거의 기준에 따라 보도된 기사로 인한 개인정보 침해에 대해서는 언론계의 적극적인 해결책 마련이 요구된다. 언론계가 기자협회나 신문협회 등의 기구를 통해서 보도윤리강령을 비롯해 자살 보도나 범죄 보도에 관한 내부적 기준을 만들어 회원사들이 이를 적용하도록 해온 것처럼 인터넷으로 서비스되는 과거 기사에 대한 수정·삭제 기준의 필요성이 있다. 언론 보도로 인한 피해 구제요구를 중재하는 기관인 언론중재위원회에서도 인터넷 환경에서 새로운 언론 피해 유형이 된 과거 기사로 인한 문제에 대한 가이드라인 연구에 나서는 방법이 있다. 언론계의 논의를 통해 디지털 환경에 적합한 취재 보도 윤리강령을 만들고, 새로운 환경에서 언론의 기능과 프라이버시 관련 기준을 전면적으로 검토해야 할 필요성이 높다.

이 가운데는 법률에 규정돼 있는 추후보도 청구권을 시대에 맞게 정비해, 범죄나 판결을 다룬 신문 기사의 경우 최종심의 결과를 과거 기사의 인터넷 서비스에 반영할 수 있는 방법도 모색되어야 한다. 특정한 시간대와 공간에서 맥락을 지닌 채 제한적으로 유통되다 그 영향력이 점차 사라져가던 과거 종이신문 시절의 보도와 달리 인터넷 환경에서는 맥락과 무관하게 기사가 무제한적 유통되는 상황으로 인한 피해 구제 절차의 마련이 필요하기 때문이다. 언론의 자율성과 표현 자유를 침해하지 않으면서도 기사의 정확성을 제고하고 관련자의 권익 보호를 반영할 수 있는 방안에 대한 모색이 요구된다. 공적 관심사를 보도하는 언론의 기능이 디지털 환경의 프라이버시 요구로 위축되지 않도록, 공인과 공적 관심사에 대한 언론 보도를 적극적으로 보호하되 공익과 무관한 개인들의 프라이버시는 최대한 보호되는 가이드라인이 필요하다.

개인정보가 과다 노출된 과거 기사에 대한 잊혀질 권리의 모색은 나아가 인터넷상의 다양한 서비스에 사용자들이 자발적·비자발적으로 제공한 개인정보의 수정·삭제 요구에 대한 논의와 사회적 합의 추구에서 주요한 기능을 할 수 있다. 인터넷 공간에서는 개인들도 블로그나 소셜네트워크를 통해 콘텐츠의 발행과 배포를 자유롭게 할 수 있는 표현 주체이기 때문에 과거의 언론사들이 지녔던 영향력을 공유하고 있다. 과거 기사에 대해 '잊혀질 권리'를 적용해 수정·삭제를 하는 것은 블로그나 소셜네트워크 등에서 개인의 프라이버시와 표현 자유를 공존시키는 데 주요한 참고 기준이 될 수 있다. 국내에서도 한국인터넷자율정책기구를 통해서 인터넷상의 표현 자유 범위에 대한 인터넷 업계가 자율적 기준을 마련하고 콘텐츠 자율규제를 추진하고 있다.

또한 인터넷 서비스의 특성상 사용자가 국내외 서비스를 자유롭게 이용할 수 있는 만큼, 국내 고유의 기준보다는 프라이버시와 표현 자유에 관한 국제적 기준과의 부합을 고려해야 한다.

# 개인정보 관련 소송에 있어서 과실 및 손해판단

서울대학교 법학전문대학원 부교수 권영준

## Ⅰ. 서론

개인정보 유출사고가 빈번하게 발생하고 있다. 이는 종종 손해배상소송으로 연결된다. 개인정보 유출은 많게는 수천만명이 연관될 정도로 사건 규모가 크다. 따라서 청구되는 손해배상액도 천문학적 규모이다. 그 청구가 모두 받아들여지면 웬만한 기업은 도산할 정도이다. 그런데 이처럼 수천만명의 개인과 한 기업의 흥망성쇠를 좌우하는 손해배상책임 판단기준이 꼭 명확한 것은 아니다. 이러한 불명확성은 주로 과실과 손해의 판단과 관련하여 존재한다.

법률(가령 개인정보보호법)이 세세하게 과실 및 손해판단기준을 정해주면 이상적일 것이다 그러나 이는 비현실적인 방안이다. 이러한 판단은 구체적 사안이 주어지지 않으면 미리 할 수 없기 때문이다. 따라서 모든 사안에 두루 적용되어야 하는 일반성을 요건으로 하는 법률에서는 이러한 기준의 제시에 한계가 있다. 오히려 손해배상소송의 결과는 재판이 끝나야 알 수 있다. 이는 구체적 타당성을 꾀하는 데에는 요긴하지만 법적 안정성 확보의 측면에서는 문제이다.

특히 개인정보 관련 소송에 대한 재판례는 아직 충분히 축적되었다고 하기 어렵다. 그러므로 법관의 판단재량을 부당하게 옥죄지 않는 범위 내에서 과실판단기준을 사전(事前)에 구체화하려는 학술적·실무적 노력이 필요하다. 이러한 지속적 노력과 재판례의 축적이 결합되어 그 기준이 구체화되고 이에 대한 공감대가 서서히 형성되어 가면 사회적 비용이 감소되고 법의 실효성이 제고된다.

이러한 점을 염두에 두고 이 글에서는 최근 제정된 개인정보보호법을 중심으로 하여 개인정보유출에 대한 개인정보처리자의 과실과 손해의 판단기준에 관하여 간략하게 검토한다. 이 보고서의 다른 주제들과는 달리 이 글은 입법부 내지 행정부보다는 사법부와 더 깊은 관련이 있다.

## Ⅱ. 과실판단기준

### 1. 과실책임주의

개인정보처리자가 부담하는 책임의 법적 성격은 불법행위책임이다. 따라서 법률에서 별도로 정하지 않는 한 불법행위법의 일반원리가 적용된다. 한편 이러한 일반원리에 따르면 불법행위책임은 원칙적으로 과실책임이다. 개인정보처리자의 불법행위책임에 관해 규정하는 개인정보보호법 제39조도 이 점을 분명히 하고 있다. 따라서 이 점에 대해서는 더 이상 논의의 필요성도 없다고 할지도 모른다.

그런데 실상은 그렇지 않다. 과실은 대표적인 불확정개념이다. 따라서 과실판단에는 판단주체의 재량이 광범위하게 개입된다. 이러한 판단재량의 행사를 통해 과실책임이 실질적으로는 무과실책임에 가깝게 운용되기도 한다. 이는 일종의 부진정과실책임이라고 말할 수 있다. 예컨대 법원은 과실책임의 일종인 사용자책임(민법 제756조 제1항)에 있어서 면책사유를 인정하지 않음으로써 이를 실질적인 무과실책임처럼 운용한다. 또한 법원은 환경침해사건에서 일단

수인한도를 넘어 위법성이 인정되는 경우에는 과실 여부에 대해서는 판단을 생략함으로써 실질적으로 과실 요건을 무색하게 만드는 경향을 보인다. 이처럼 과실판단에 관한 광범위한 재량 때문에 법원이 과실판단에 관하여 어떠한 방향성을 취하는가에 따라 구체적 사건의 결론은 상당한 영향을 받을 수 있다. 그러므로 과실판단의 구체적인 기준을 논하기에 앞서 과실판단의 거시적인 방향성을 설정하는 것 - 구체적으로 말하자면 개인정보처리자의 책임이 부진정 과실책임의 성격을 가지는지에 대한 입장 정립 - 은 유의미한 일이다.

결론부터 말하자면 개인정보처리자의 불법행위책임은 위와 같은 의미의 부진정과실책임으로 파악할 수 없다. 우선 개인정보보호법 제39조 제1항은 과실의 입증책임을 개인정보처리자에게 전환할 뿐 무과실책임까지 인정하지는 않는다. 이는 개인정보의 보호와 이용을 조화시키려는 입법적 결단으로서 존중되어야 한다. 한편 위와 같은 입법적 결단에도 불구하고 법원이 이를 해석, 적용하는 과정에서 무과실의 입증가능성을 사실상 봉쇄하거나 좁힘으로써 무과실책임에 가깝게 운용하는 것도 가능하긴 하다. 그러나 이러한 운용을 정당화할 근거를 찾기는 어렵다. 공작물 소유자나 자동차 운행자, 사용자 등에게 무과실책임 또는 이에 가까운 책임을 부담시킬 수 있는 이유는 자신의 이익이나 행동의 자유를 극대화하는 과정에서 수반되는 위험은 그들에게 귀속시키는 것이 위험책임 또는 보상책임의 원리에 부합하기 때문이다. 하지만 공작물 소유나 자동차 운행, 피용자 사용 등의 활동이 대체로 공작물 소유자 등의 배타적 이익으로 귀속되는 것과 달리 개인정보의 수집과 활용은 개인정보처리자와 정보주체의 상호 이익, 나아가 공동체의 이익으로 귀착되는 측면도 강하다. 개인정보의 수집과 활용을 통해 사회적 비용이 현저하게 감소되고 이로 인한 편익을 일반 국민들도 누리기 때문이다. 그러므로 개인정보처리자의 과실 없이 발생한 위험을 개인정보처리자에게만 전가하는 것은 타당하지 않다. 만약 이를 관철시키려면 강제보험제도나 보상기금제도 등 위험을 분산하는 별도의 장치가 필요하다. 그러한 법적 장치도 마련되지 않은 상태에서 개인정보처리자에게 실질적인 무과실책임을 부과하는 방향은 타당하다고 할 수 없다.

## 2. 개인정보처리자의 주의의무 내용

### 가. 주의의무 일반론

과실은 사회생활상 요구되는 주의를 게을리 하여 일정한 결과가 발생하리라는 것을 인식하지 못하는 것이다. 따라서 과실의 본질적 내용은 주의의무 위반이다. 그렇다면 누구를 기준으로 주의의무 위반을 결정하는가? 또한 주의의무 위반의 정도가 어떠해야 하는가? 이에 관해 지배적인 견해는 추상적 경과실의 개념을 채택하여 이러한 의문에 답한다. “추상적”이라는 것은 통상인 또는 평균인을 기준으로 한다는 의미이다. “경과실”은 주의의무를 게을리 하였으나 현저하게 게을리 한 데에는 이르지 않은 과실을 의미한다.

이러한 과실이 있는지의 판단은 ① 판단대상인 행위와 관련된 사실관계를 확정하고, ② 그 행위에 적용되어야 할 주의의무의 내용을 확정하며, ③ 확정된 주의의무를 문제되는 행위에 적용하여 그 행위가 주의의무를 다하지 못한 것인지를 판단하는 순서로 이루어진다.[1] 그 중 ①과 ③의 단계는 구체적인 사안이 주어지지 않으면 미리 정할 수 없다. 그러나 ②의 단계는 사안이 주어지지 않더라도 미리 일정 부분 구체화할 수 있다. 그러므로 과실판단에 관하

1) Gert Brüggemeier, Common Principles of Tort Law, British Institute of International and Comparative Law, 2004, pp. 66-69 참조. 독일 문헌에서는 이처럼 주의의무에 따라 이루어져야 마땅할 행위를 Soll-Verhalten, 실제로 이루어졌던 행위를 Ist-Verhalten이라고 명명하고 과실판단에 있어서 양자를 비교한다. Kötz/Wagner, Deliktsrecht, 9. Aufl. 2001, Rn. 106.

여 학술적 논의가치가 큰 것은 ②의 단계, 즉 주의의무 내용의 확정단계이다.

한편 주의의무의 내용은 주의의무의 발생근거가 정하는 바에 따라 결정된다. 주의의무는 단순한 도의적 의무가 아니라 법적 의무이다. 이러한 법적 의무는 법령이나 계약에 의해 정해지는 것이 원칙이다. 그러나 법령에서 늘 주의의무를 빠짐없이 열거할 수 있는 것은 아니다. 또한 모든 사람이 장차 발생할 수 있을 불법행위를 염두에 두고 미리 계약을 체결해 놓기도 어렵고, 설령 그런 계약이 가능하더라도 그 계약에서 모든 주의의무를 빠짐없이 열거하기도 어렵다. 이러한 불완전성 때문에 주의의무는 법령과 계약 이외에도 선행행위나 조리(條理), 신의칙 등 보충적인 근거에 의해 발생할 여지도 있다. 이들도 넓게 보면 법질서의 한 내용을 구성하므로 이 역시 법적 근거의 하나라고 할 수 있다. 다만 조리나 신의칙 등 무정형한 속성을 가지는 근거에 의해 주의의무를 인정하는 것은 신중해야 한다. 특히 법령이 주의의무를 포괄적이고 망라적으로 제시하고 있다면 주의의무의 내용은 별도로 계약에서 정함이 없는 이상 법령에 의해 정해진다.

## 나. 개인정보처리자의 주의의무

### (1) 주의의무의 발생근거 - 법령

개인정보처리자의 주의의무 역시 주로 법령과 계약(대체로 약관)에 따라 결정된다. 계약에 따른 주의의무는 개별적 계약내용에 따라 달라지는 것이므로 논의범위에서 제외한다. 한편 우리나라 개인정보보호법과 이에 기초한 하위 규범들은 상당히 포괄적이고 체계적인 방식으로 개인정보처리자의 주의의무를 규정하고 있다.

이와 관련하여 개인정보보호법에서 제시하는 주의의무가 민사분쟁에서 사인 간에 적용되는 주의의무와 일치하는가에 관한 의문이 제기될 수 있다. 원론적으로만 말하자면 개인정보처리자가 개인정보보호법상 기준을 준수하였다고 하여 반드시 민사책임을 면하게 된다고 단정할 수는 없다. 그런데 개인정보보호법은 개인정보보호를 위한 정책적, 행정적 얼개를 짜는 것에 그치지 않고, 더 나아가 개인정보처리자와 정보주체 사이의 사법(私法)상 권리의무관계를 규율할 의도로 만들어진 규범이다. 따라서 개인정보보호법을 건축법과 같은 일반적인 행정법규와 동일하게 취급할 수는 없다. 더구나 개인정보보호법과 그 하위 규범들이 제시하는 주의의무는 개인정보보호의 포괄적이고 체계적인 규율을 위해 매우 촘촘하게 구성되어 있다.

그렇다면 계약에서 달리 정하지 않는 이상 개인정보보호법령에 상세하게 규정된 주의의무 이외에 추가적인 주의의무를 인정할 여지는 크지 않고, 그러한 인정이 바람직하지도 않다. 이는 특히 개인정보보호법상 과실 인정은 비단 민사책임뿐만 아니라 형사책임으로도 이어진다는 점에서도 그러하다. 따라서 원칙적으로 개인정보처리자는 개인정보보호법령에 규정된 주의의무를 준수한 이상 민형사상 책임을 지지 않는다고 하여야 한다. 이처럼 공시된 규범상의 주의의무 기준과 법원이 적용하는 주의의무 기준을 가급적 합치시키는 것이 예측가능성의 증대라는 과실책임주의의 기능과도 부합한다.

### (2) 주의의무의 전제 - 합리적 기대가능성

위와 같은 내용의 주의의무는 합리적 기대가능성이라는 테두리 안에서 인정된다. 법은 합리적으로 기대할 수 없는 행위를 강제할 수 없기 때문이다. 가령 개인정보처리자가 어떠한 보안조치를 취하지 않았다는 것이 문제되면 우선 그러한 보안조치를 취하는 것이 합리적으로 기대가능한지 살펴보아야 한다.

인터넷 보안을 강화하는 것은 마치 양날의 검과 같다. 이는 한편으로는 개인정보유출의 가능성을 줄이지만, 다른 한편으로는 인터넷과 관련된 비용을 높여 인터넷 사업체에 부담을 줄 수 있다. 이러한 부담은 궁극적으로 인터넷 이용자에게 전가될 가능성이 높다. 따라서 인터넷 보안 강화를 법적으로 강제하는 것은 인터넷에 일종의 간접세를 부과하는 것과 마찬가지이다. 결국 그 명암을 따져보아 어느 정도까지 이러한 간접세 부과가 정당화되는지를 고민해야 한다. 바꾸어 말하면 법령에 정해진 주의의무의 외연을 끝없이 확장하여 나가는 것만이 능사가 아니라 일종의 비용/편익 분석(cost-benefit analysis)의 사고에 기초하여 합리적으로 기대할 수 있는 범위 내에서 주의의무의 외부 경계선을 그을 필요가 있다.

### (3) 개인정보보안과 관련된 주의의무의 내용

개인정보보호법에서는 개인정보처리자의 주의의무를 열거하고 있다. 이는 개인정보의 수집단계부터 파기단계에 이르기까지 매우 다양한 모습으로 나타난다. 그런데 개인정보 유출은 주로 개인정보보안과 관련된다. 그러므로 지면관계상 아래에서는 개인정보보안과 관련된 주의의무만 소개한다.

#### (가) 안전조치의무

개인정보보호법 제29조는 안전조치의무라는 표제 하에 "개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다."라고 규정함으로써 개인정보처리자의 주의의무를 기술적 조치의무, 관리적 조치의무, 물리적 조치의무로 구분한다. 다만 이 중 물리적 조치의무는 넓게 보면 관리적 조치의무의 범주에 포함시킬 수 있으므로,[2] 개인정보처리자는 크게 보면 기술적 조치의무와 관리적 조치의무를 부담한다고 할 수 있다. 이러한 토대 위에 개인정보보호법상 개인정보처리자의 안전조치의무를 표로 정리하면 다음과 같다.

〈표 1〉 개인정보처리자의 안전조치의무

| 대분류 | 소분류 | 내용의 요지 | 관련 조항 |
|---|---|---|---|
| 기술적 조치의무 | 접근통제 | 접근권한 제한,<br>접근통제 시스템<br>설치 및 운영 | 법 제29조<br>고시 제4, 6조 |
| | 암호화 | 일정한 정보를<br>암호화하여 저장 | 법 제29조<br>영 제21조. 제30조 제1항<br>제3호<br>고시 제7조 |
| | 접속기록의 보관<br>및 위·변조<br>방지조치 | 개인정보처리시스템<br>접속기록을<br>안전하게 보관·관리 | 법 제29조<br>영 제30조 제1항 제4호<br>고시 제8조 |

2) 정보통신망법 제28조와 신용정보법 제18조, 개인정보보호법 제26조 제1항 제2호도 "기술적·관리적 보호조치"라는 개념을 사용하고 있다.

| | | | |
|---|---|---|---|
| | 보안프로그램 설치와 갱신 | 백신 소프트웨어 등 보안프로그램 설치와 업데이트 | 법 제29조<br>영 제30조 제1항 제5호<br>고시 제9조 |
| 관리적 조치의무 | 내부관리계획 | 개인정보의 안전한 처리를 위한 내부관리계획 수립 | 법 제28, 29, 31조<br>고시 제3, 5조 |
| | 물리적 조치 | 개인정보의 안전한 보관 및 출입통제절차 | 법 제29조<br>영 제30조 제1항 제6호<br>고시 제10조 |

**(나) 사후조치의무**

개인정보처리자는 위와 같이 개인정보가 유출되지 않도록 안전성을 확보하여야 할 사전적인 조치의무를 부담하는 이외에도 개인정보보호법 제34조에 따라 일단 개인정보가 유출된 후에도 사후적인 조치의무를 부담한다. 이 조항에 따르면 개인정보처리자는 유출 후 지체 없이 해당 정보주체에게 그 사실을 알리고(제1항), 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 하며(제2항), 일정 규모 이상[3]의 개인정보 유출시에는 제1, 2항에 따른 통지 및 조치결과를 지체 없이 대통령령이 정하는 전문기관[4]에 신고하여야 한다(제3항).

## 3. 주의의무 판단시 고려요소

위와 같이 법령상 주의의무의 내용을 확정하였더라도 구체적인 사안에서 주의의무 위반 여부를 판단하는 것은 쉬운 일이 아니다. 또한 사안의 개별성을 뛰어넘는 획일적인 판단기준을 제시하는 것도 불가능하다. 결국 법원은 위와 같은 주의의무의 틀 안에서 여러 가지 세부 요소들을 고려하여 규범적·총체적인 관점에서 과실판단을 하게 된다.

그렇다면 법원은 어떤 요소들을 고려하여 주의의무 위반 여부를 판단하게 되는가? 아래에서는 위와 같은 하급심 판결과 관련 법령의 태도를 참조하여 법원이 구체적 사건에서 주의의무 위반 여부를 판단함에 있어서 고려하여야 할 요소와 그 방향에 대해 정리해 보았다. 여기에서는 고려요소를 ① 내부적 고려요소(개인정보처리자의 통제영역 안의 고려요소) ② 외부적 고려요소(개인정보처리자의 통제영역 밖의 고려요소) ③ 기타 고려요소(개인정보 처리업무 위탁시의 고려요소)로 분류하였다. 이를 표로 정리하면 다음과 같다.

〈표 2〉 개인정보처리자의 주의의무 판단에 고려할 요소들

| 대분류 | 소분류 | 고려 요소 | 주의의무 판단에 미치는 영향 |
|---|---|---|---|
| 내부적 고려요소 | 정보 관련 | 정보의 민감성과 위험성 | 민감정보 +<br>위험정보 + |
| | | 정보의 양 | 대량정보 + |
| | | 정보의 필요성 | 불필요하거나 필요성이 적은 정보 + |

3) 시행령 제39조 제1항은 1만 명 이상의 정보주체에 관한 개인정보 유출시신고의무를 부과한다.
4) 시행령 제39조 제2항은 한국정보화진흥원과 한국인터넷진흥원이 그 전문기관이라고 규정한다.

| | | | |
|---|---|---|---|
| | 개인정보처리자 관련 | 특성 | 영리기관 +<br>개인정보처리 자체가 주된 업무 내용인 기관(관련 정부기관, 신용정보기관 등)++<br>민감정보 내지 위험정보를 주로 다루는 기관(관련 정부기관, 금융기관 등) ++ |
| | | 규모 | 대규모기관 + |
| | | 해커와의 관계 | 내부자인 해커 ++<br>내부자의 조력을 받은 해커 + |
| | 사전징후 및 사후 조치 | 사전징후 | 사전징후(해킹피해전력 포함) 유 + |
| | | 사후조치 | 지연된 사후조치 +<br>비자발적 사후조치 +<br>부적절한 사후조치 + |
| 외부적 고려요소 | 보편적인 기술수준 및 관행 관련 | 보편적인 기술수준 | 보편적인 기술수준 미달 +<br>(기술수준의 준거집단 확정 및 사후편견 유의) |
| | | 관행 | 관행 미달 +<br>(관행은 하위 고려요소에 불과) |
| | 외부기관 안전평가 관련 | 외부기관 안전평가의 내용과 결과 | 안전평가상 취약점 지적 +<br>취약점에 대한 사후조치 미이행 + |
| 기타 고려요소 | 업무위탁 관련 | 개인정보업무처리수탁자의 선정과 관리·감독 | 선정과 관리감독상 문제 + |

※ +는 과실인정가능성이 상대적으로 높아짐을 의미함.

# Ⅲ. 손해판단기준

## 1. 손해의 발생여부

과실판단결과 과실이 인정되더라도 손해배상청구권이 발생하려면 손해가 실제로 발생하여야 한다. 그런데 개인정보와 관련된 손해배상소송은 대부분 비재산적 손해배상, 즉 위자료의 배상을 구하는 것들이다. 그러므로 정신적 손해가 과연 발생하였는지를 확정할 필요가 있다. 그런데 본래 손해의 개념 자체가 늘 확실성을 가지는 것이 아닌데다가 정신적 손해의 개념은 더욱 그러하다. 따라서 개인정보 관련소송에 있어서 정신적 손해의 발생 여부는 중요한 쟁점이 되는 경우가 많다. 한편 이러한 손해의 발생여부를 판단함에 있어서는 손해의 개념에 관한 다음 두 가지 점을 염두에 둘 필요가 있다.

## 가. 손해 개념

### (1) 법적 개념으로서의 손해

손해는 어디까지나 법적 개념이다. 따라서 이 세상에 존재하는 모든 불이익을 손해의 개념 안에 끌어들일 수는 없다. 예를 들어 여행 중 행인에게 길을 물어보았는데 잘못된 정보를 제공하여 목적지에 5분 늦게 도착하게 된 것도 일종의 불이익이다. 하지만 이러한 불이익은 법적인 의미의 손해에는 해당하지 않는다. 한강을 조망할 수 있던 아파트 앞에 다른 아파트가 들어섬으로써 그 아파트의 시가가 하락하는 것도 분명히 불이익이다. 하지만 이러한 조망이익이 반사적 이익에 불과하다고 보면 그 이익의 박탈을 배상하여야 할 손해로 인정할 수 없는 경우가 많다. 만약 손해 개념을 모든 유형의 불이익에 무분별하게 확장한다면, 거의 매순간 세상 곳곳에서 끊임없이 손해배상청구권이 발생할 것이다. 그리고 이 세상에 존재하던 단순한 불운(不運)의 영역이 순식간에 불법(不法)의 영역으로 뒤덮일 것이다. 이는 바람직하지 않다.

이와 같이 불법행위로 인한 손해배상청구권은 법률상 보호받아야 마땅한 이익에 관하여 현실적으로 손해가 발생한 때 비로소 성립한다. 그리고 손해의 발생 여부는 사회통념에 비추어 규범적으로 판단할 수 밖에 없다. 이러한 판단에 있어서는 손해의 직접성, 구체성, 특정성, 법익과의 거리, 법익에 야기된 불이익에 대한 법적 가치판단 등 여러 가지 요소들을 고려하여야 한다. 손해배상제도와 다른 구제수단 사이의 기능적 연관성도 고려할 수 있다. 예를 들어 손해배상 이외의 다른 구제수단이 충실히 기능하고 있는가 여부가 손해배상의 범위를 확정하는 데에 영향을 미칠 수 있다.

### (2) 침해와 손해의 구별

대법원은 소유권의 방해와 손해가 구별되는 개념임을 명확하게 하고 있다.[5] 현재 지속되는 권리침해상태는 방해로, 그 결과제거만 문제되는 상태는 손해로 관념함으로써 "지속성"이라는 구분표지를 사용한다. 이러한 구분은 권리침해자가 반드시 손해배상책임을 지는 것은 아니라는 점을 의미한다. 가령 대법원은 부정경쟁행위에 있어서 침해자라고 하여 반드시 손해배상책임을 지는 것이 아니라는 점을 명확하게 한다.[6]

인격권에 있어서도 인격권의 침해와 이로 인한 손해는 구별된다. 이러한 구별은 중요한 의미를 가진다. 인격권의 침해는 침해금지청구권을, 이로 인한 손해는 손해배상청구권을 발생시킨다. 침해금지청구권의 상대방은 현재 침해상태를 지배하는 자이지만, 손해배상청구권의 상대방은 과거에 손해를 야기한 자이다. 따라서 침해금지청구권에 있어서는 그 상대방이 직접 침해상태를 야기하였는가는 본질적으로 중요하지 않다. 침해금지청구권의 발생에는 고의 내지 과실과 같은 귀책사유가 요구되지 않지만, 손해배상청구권의 발생에는 원칙적으로 위와 같은 귀책사유가 요구된다. 둘 다 위법성이 요구되지만, 그 위법성의 정도는 손해배상청구보다 침해금지청구에서 더 높게 파악하여야 한다는 견해도 주장되고 있다.[7]

이처럼 양자의 차이점에 주목한다면 인격권의 일종인 개인정보자기결정권이 침해되었다고 하여 논리필연적으로 정신적 손해가 곧바로 발생하는 것은 아니다. 일반적으로 말하자면 개인정보권의 침해는 사회통념상 정신적 손해를 발생시킬 개연성이 크다. 하지만 "개인정보권이 침해되었지만 정신적 손해는 발생하지 않는다"는 명제가 적용되는 사례도 있을 수 있다. 따라

---

5) 대판 2003. 3. 28, 2003다5917.
6) 대판 2008. 11. 13, 2006다22722; 대판 2004. 7. 22, 2003다62910.
7) 郭潤直編, 民法注解(Ⅴ), 1992, 311면(柳元奎 執筆部分)에서는 임미시온에 관하여 일본에서 주장되는 위법성의 2단계설을 소개하고 있다. 또한 대판(전) 2008. 4. 17, 2006다35865의 다수의견도 이를 전제하고 있다.

서 개인정보자기결정권에 있어서도 개념적으로나 실제적으로 침해와 손해를 구분할 실익이 있다. 개인정보자기결정권의 침해와 손해 사이의 상관관계에 관하여 비교법적으로 검토하면 독일이나 미국은 이를 엄격하게 구분하는 경향을 보이는 반면, 일본이나 우리나라는 양자의 연계성을 확대하는 경향을 보인다.

## 나. 정신적 손해발생의 판단기준

손해가 발생하였다면 그것은 재산적 손해이건 정신적 손해이건 배상되어야 한다. 그런데 정신적 손해는 재산적 손해와 비교할 때 무정형하고 객관화하기 어려워 이를 느슨하게 인정하기 시작하면 법관의 자의적 재량에 의하여 범위가 끝없이 확장될 위험이 있다.

이러한 위험에 대한 경계는 외국에서도 여러 가지 모습으로 나타난다. 독일에서는 민법을 제정하면서 이러한 위험을 염두에 두고 법률의 근거가 있는 경우에 한하여 정신적 손해배상을 인정하였다.[8] 같은 이유로 미국에서도 20세기 초에서부터 비로소 정신적 고통에 대한 불법행위책임이 인정하기 시작하였고, 아직도 위자료인정을 위한 소인(cause of action)은 제한적이다. 반면 우리나라는 민법 제751조에서 포괄적인 정신적 손해배상을 규정하고 있어 이 점에서 위자료의 폭넓은 인정이 가능하다. 실제 재판실무도 폭넓게(하지만 얕게) 위자료를 인정해 주는 입장을 취한다고 보인다.

그런데 이러한 차이에도 불구하고 법계를 불문하고 공통적으로 직면하는 과제가 있다. 그것은 두 가지 요청의 조화이다. 하나는 정신적 손해의 범위 확정문제는 정신적인 고통도 배상대상이 되어야 한다는 요청이다. 다른 하나는 정신적 손해의 범위가 비합리적으로 확장되어서는 안 된다는 요청이다. 이러한 요청들의 조화를 통하여 일상 속에서 경험하는 단순한 불쾌감 또는 불안감으로부터 정신질환을 야기할 정도의 충격 사이 어딘가에 손해와 비손해의 경계선이 설정된다.

이러한 경계선을 설정하는 데에 있어서는 손해배상제도가 사회 전체에서 차지하는 위치와 기능에 대한 숙고가 수반되어야 한다. 예컨대 개인정보침해라는 현상을 방지하거나 그 침해결과를 제거하기 위하여 행정규제, 자율규제, 기술적 접근, 형사시스템, 보험, 손해배상 등 다양한 제도들이 존재한다. 이러한 제도들은 현실 속에서 강한 연관성을 가지고 유기적으로 작동한다. 따라서 손해배상제도를 어떻게 운영할 것인가를 고민함에 있어서는 다른 제도들과의 역할분담을 고려하여야 한다. 손해배상제도는 기본적으로 손해전보를 주된 기능으로 하는 제도이다. 그리고 전보되어야 할 손해는 '확정적이고 현실적인' 손해이다.[9] 만약 이러한 요건을 갖추지 못한 덜 익은(unripe) 불이익에 대하여 자유롭게 손해배상을 명할 수 있게 된다면, 민주적 정당성이 결여된 법원에 의하여 단순한 교정을 넘어서서 부의 재분배가 초래될 수 있어 타당하지 않다. 또한 손해배상제도에 과도한 부하(負荷)가 걸리면서 제도의 비용이 그 편익을 초과하는 상황이 발생한다. 따라서 이러한 확정성을 갖추지 못한 불이익이나 위험은 손해전보의 대상으로 삼기보다는 그러한 불이익 등을 초래한 행위 자체에 대한 예방이나 제재(특히 행정규제나 형사처벌 등)의 몫으로 남겨놓는 것이 전체적인 유기성의 차원에서 더 바람직하다. 특히 영미법과 같이 손해가 없더라도 불법행위임을 선언하는 의미의 명목적 손해배상(nominal damages)

8) 독일 민법 제253조 제1항은 비재산적 손해는 법률이 정한 경우에만 금전에 의한 배상을 청구할 수 있다고 규정한다. 한편 같은 조 제2항은 신체, 건강, 자유 또는 성적 자기결정의 침해를, 제1300조는 약혼의 부당파기를 그 사유로 들고 있다. 일반적 인격권 침해에 관하여는 명문 규정이 없지만 1958. 2. 1. 연방대법원이 이를 자유침해에 해당한다고 판시한 이래 위자료배상이 인정되고 있다.

9) 대판 2007. 6. 28, 2006다52259; 대판 2004. 11. 26, 2003다58959 등.

이나 실손해를 초과하는 제재적 배상을 명하는 징벌적 손해배상(punitive damages)을 인정하지 않는 우리나라 법제 하에서 제재 또는 예방의 목적을 전면에 내세워 손해배상의 범위를 지나치게 확장하는 것은 경계해야 할 것으로 생각한다.

그렇다면 개인정보와 관련하여서는 어떤 경우에 정신적 손해가 발생하였다고 할 수 있을까? 이에 대하여 일률적인 기준을 제시하기는 어렵다. 다만 그 판단기준을 좀더 구체화하면 다음과 같다.

① 개인정보 수집단계에서는 그것이 민감한 정보일수록 정신적 손해발생가능성이 커지는 반면, 민감하지 않은 정보라면 사생활침해 등 또다른 법익을 침해하는 방법으로 수집하지 않는 한 그 정보의 수집에 의한 정신적 손해발생가능성은 낮아진다.
② 일단 적법하게 수집된 개인정보를 보유한 주체가 이를 허술하게 관리한다는 점만으로 곧바로 정신적 손해가 발생한다고 할 수는 없고 오직 관련 성문법상의 행정제재의 대상이 될 수 있을 뿐이다.
③ 개인정보 유출단계에서는 그것이 불특정 또는 다수인이 접근할 수 있는 상태로 공개되었는지 또는 이들에게 적극적으로 배포되었는지 여부에 따라 정신적 손해발생가능성이 좌우된다. 다만 이 때에도 개인정보의 민감성이나 유출의 범위를 추가적으로 고려하여야 한다.
④ 유출과 유사한 문제로 개인정보의 양도/위탁의 경우에는 마케팅회사 등 개인정보를 업무로 활용하는 기업에의 양도/위탁이 그 개인의 의사에 반하여 이루어진 것인지 여부에 따라서 정신적 손해발생가능성이 좌우된다.
⑤ 개인정보의 유출에 이어 실제 그 개인정보가 악용되어 2차 피해가 발생했는지 여부도 정신적 손해발생가능성에 영향을 미친다.

## 2. 손해배상액의 산정

한편 위자료를 어떻게 산정할 것인가? 이에 대해 구체적인 기준을 제시하는 것은 시기상조이다. 다만 개인정보침해사건에 관한 개별적 고려요소들을 유형화, 체계화하는 작업은 가능할 것이다. 위자료를 구체적으로 산정할 때 고려하여야 할 요소는 무엇인가? 이와 관련하여 다음 두 가지 사항을 언급하고자 한다.

우선 불법행위법의 목적은 손해전보에 초점이 맞추어지지만 위자료의 속성상 손해예방과도 적지 않은 관련이 있다. 특히 손해전보는 대체로 “피해자”가 어느 정도의 피해를 입었고 어떻게 그 피해를 회복할 수 있는가에 초점을 맞춘다. 하지만 손해예방은 대체로 “가해자” 또는 사회의 잠재적 가해자에게 어떤 메시지를 던질 것인가에 초점을 맞춘다. 그러므로 가해자측 요소 가운데에는 예방적 성격을 가지는 것들이 많다.

아래에서는 각종 요소들을 피해자측 요소와 가해자측 요소로 나누어 도표로 표시하였다. 피해자측 요소는 불법행위법의 목적 중 손해전보와 관련성이 크다. 가해자측 요소는 불법행위법의 목적 중 손해예방 내지 제재와 관련성이 크다. 이 도표는 이해의 편의를 도모하기 위하여 위자료산정의 방향성을 도식화한 것으로서 획일적인 기준으로 제시한 것은 아니다. 따라서 개별적 사안에 따라 유연하게 변형되거나 배제될 수 있다. “+”와 “+ +” 표시 등은 같은 요소 안에서의 상대적 관계를 나타낸 것일 뿐 절대적인 증감관계를 표시한 것이 아니다.

## 가. 피해자측 요소

【표3】 위자료산정시 고려할 피해자측 요소

| 요소 | 분류 | 위자료 반영정도 | 설명 |
|---|---|---|---|
| 침해 단계 | 무단수집 | + | 밑의 단계로 갈수록 위자료 증액 |
| | 무단이용 | + + | |
| | 무단유출 | + + + | |
| 침해 범위 | 좁은 범위 | + | 이는 특히 무단유출과 관련있음. 유출범위가 넓을수록 위자료 증액 |
| | 넓은 범위 | + + | |
| 침해 대상 | 비민감정보 | + | 민감정보일수록 위자료 증액 |
| | 민감정보 | + + | |
| 정보의 정확성 | 정확한 정보 | + | 일반적으로 부정확한 정보(특히 의도적으로 왜곡된 정보)일수록 위자료 증액 |
| | 부정확한 정보 | + + | |
| 정보의 식별가능성 | 식별가능성이 낮은 정보 | + | 개인식별가능성이 높을수록 위자료 증액 |
| | 식별가능성이 높은 정보 | + + | |
| 악용 여부 | 불특정 또는 다수인에 대한 정보유출 | + | 신분 도용이나 금전 인출 등 개인정보의 실제 악용이 일어난 경우에는 위자료 증액 |
| | 불특정 또는 다수인에 대한 정보유출 악용 | + + | |
| 재산적 손해 | 재산적 손해 미발생 | + | 개인정보침해가 재산적 손해로 이어졌으나 구체적 입증이 어려운 경우 위자료의 보완적 기능에 따라 위자료 증액 |
| | 재산적 손해 발생 (입증곤란) | + + | |
| 피해자의 과실 | 과실 ○ | - | 피해자의 과실이 있는 경우에는 위자료 감액 위자료 감액 |
| | 과실 × | 0 | |

## 나. 가해자측 요소

【표4】 위자료산정시 고려할 가해자측 요소

| 요소 | 분류 | 위자료 반영정도 | 설명 |
|---|---|---|---|
| 침해 태양 | 경과실 | + | 경과실에 의한 침해보다 고의 또는 중과실에 의한 침해의 경우 위자료 증액 |
| | 고의 또는 중과실 | ++ | |
| 가해자의 지위 | 일반적인 경우 | 0 | 공공기관이나 정보통신서비스제공자와 같이 조직적으로 대량의 개인정보를 수집, 취급하면서 이로부터 유무형의 이익을 많이 얻고, 동시에 개인정보남용의 높은 위험을 수반하는 주체일수록 더욱 높은 주의의무를 부담하고, 이는 위자료산정에도 영향을 미침 |
| | 공공기관, 정보통신서비스 제공자 등 | + | |
| 동기 | 비영리적 동기 | 0 | 영리적 동기 또는 범죄에 활용할 동기가 있었던 경우는 학술, 언론, 종교 등 그렇지 않은 경우보다 위자료 증액 |
| | 영리적 동기 또는 범죄 관련 동기 | + | |
| 정보 필요성 | 필요성 ↑ | + | 문제된 개인정보의 필요성이 크지 않음에도 불구하고 굳이 이를 과도하게 수집, 보관, 활용하는 과정에서 생긴 사고에 대하여는 위자료 증액 |
| | 필요성 ↓ | ++ | |
| 행위 이후의 사정 | 피해확대방지 또는 회복을 위한 적극적 노력 ○ | - | 피해회복을 위한 적극적 노력은 정신적 손해의 폭을 줄일 뿐만 아니라 예방이나 제재의 측면에서도 책임의 폭을 줄일 요인임. 아무런 조치를 취하지 않는 것 자체가 위자료 증액요소가 될 수는 없지만, 행위 이후 오히려 피해자의 정신적 손해를 가중시키는 언동이 있었다면 위자료 증액 |
| | 피해확대방지 또는 회복을 위한 적극적 노력 × | 0 또는 + | |

## 다. 기타 요소

### (1) 피해자의 재산상태

피해자의 재산상태는 일반적으로 위자료액수에 영향을 미치지 않는다.[10] 따라서 피해자가 재산이 많고 적음이 위자료의 증감요소로 작동하지는 않는다.[11] 가령 동일한 정도의 개인정보 관련 피해를 입었더라도 동일한 정도의 전보 내지 만족기능을 수행하기 위하여 부자의 경우 더 큰 위자료를 받아야 한다는 논리는 타당하지 않다.[12] 다만 사건의 성격에 따라서 피해자의 재산상태가 참작되어야 하는 경우도 있을 것이다.[13] 예컨대 개인정보침해로 인하여 2차적인 재산상 손해가 발생하였는데, 이로 인하여 피해자가 파산에 이르렀다면 개인정보침해가 가져온 정신적 손해는 매우 크다고 할 수 있다. 그런데 이러한 경우에도 이는 특별한 사정에 해당하여 예견가능성이 있는 때에만 배상가능하다(민법 제763조, 제393조 제2항).

### (2) 피해자가 실제로 침해행위를 인식하였는지 여부

피해자가 자신의 개인정보자기결정권을 침해당하였다는 사실 자체를 인식하는 경우도 많다. 법리상으로는 불법행위는 침해 당시에 성립하는 것인데 그 당시에 피해자가 이를 인식하지도 못하였다면 정신적 고통은 발생하지 않은 것이 아닌가 하는 의문이 든다.

하지만 실제 인식 여부가 위자료청구권의 발생 여부를 좌우하는 것은 아니다. 위자료청구권의 발생원인인 정신적 고통은 다분히 규범적인 것이다. 따라서 주관적인 감정에 대한 배상이라기보다는 객관적인 비재산적 이익상실에 대한 배상의 본질을 가진다. 이러한 이유 때문에 실제 정신적 고통을 느끼지 못하는 의식불명자, 유아 또는 태아[14]에게도 위자료청구권이 인정된다. 따라서 개인정보자기결정권의 침해사실을 구체적으로 인식하지 못하였던 개인에 대하여도 다른 요건이 갖추어진다면 위자료청구권이 발생한다. 인식 여부는 위자료액에 영향을 미치는 변수가 될 뿐이다.

### (3) 가해자의 재산상태 내지 피해자의 숫자

개인정보침해사건은 일반적으로 피해자의 숫자가 매우 많아지기 쉽다. 물론 이러한 사건이 모두 손해배상청구소송으로 이어지지는 않는다. 또한 손해배상청구소송으로 이어지더라도 모든 피해자들이 모두 원고가 되는 것은 아니다. 그러나 현실적으로 원고들의 숫자가 매우 많아지는 경우 지급하여야 할 위자료의 총액도 천문학적인 액수에 이를 수 있다. 이 때 가해자의 재산상태에 따라서는 이러한 책임을 부담하게 됨으로써 파산에 이르는 경우도 쉽게 상정할 수 있다.

이때 가해자의 재산상태 내지 피해자의 숫자를 위자료 산정에 감안할 수 있는가? 가령 원고들의 숫자가 많거나 향후 추가소송이 예견되는 경우 가해자의 자력을 감안한 손해배상액산정이 타당한가? 이는 위자료의 전보적 기능과 제재적 기능 중 어느 것을 중시할 것인가와 관련있다. 전보적 기능은 피해자에게, 제재적 기능은 가해자에게 초점을 맞춘다. 따라서 전보적

---

10) Huber in Anwaltkommentar, 2005, §253 Rn. 81; Heinrich in Palandt, Bürgerliches Gesetzbuch, Kommentar, 64. Aufl. 2005, §253 Rn. 19; MünchKomm/Oekter, 5.Aufl. 2006, §253 Rn. 38.

11) MünchKomm/Oekter, 5.Aufl. 2006, §253 Rn. 38.

12) Huber in Anwaltkommentar, 2005, §253 Rn. 81.

13) 이혼으로 인한 위자료가 그 대표적인 예이다. 현실적으로 우리나라에서는 이혼당사자들의 재산상태가 위자료 액수에 영향을 주고 있다. 재산분할청구제도가 생긴 이후에도 위자료 청구권은 이혼 후 부양적 의미를 가지는 이혼급부로서의 보충적 의미를 완전히 상실하지 않고 있기 때문이다. 趙恩嬉, "離婚後 配偶者 扶養에 관한 우리나라와 獨逸法의 比較法적인 考察", 法制硏究 통권 제23호, 2002. 12. 196면.

14) 태아의 위자료청구권을 인정한 판결로서 대판 1993. 4. 27, 93다4663 참조.

기능을 강조한다면 가해자의 재산상태가 전보액에 영향을 미치는 것은 수긍하기 어렵다. 중요한 것은 피해자의 피해전보이지 가해자에 대한 적정한 제재가 아니기 때문이다. 반면 제재적 기능을 강조한다면 가해자의 재산상태에 따른 적합화(customize)된 제재부과 차원에서 이를 충분히 고려할 수 있다. 제재의 정도는 가해자의 악행에 못 미쳐서도 안 되지만 넘쳐서도 안 되기 때문이다. 따라서 잘못의 크기와 관계없이 피해의 정도가 매우 광범위할 수 밖에 없는 사건에서는 이러한 적정제재의 필요성이 발동할 여지가 크다.

앞서 살펴본 것처럼 위자료에 있어서는 제재와 관련이 있는 예방 패러다임이 일정한 역할을 수행하는 것은 사실이다. 그러나 우리 법은 근본적으로 회복 패러다임에 기반하고 있고, 위자료산정에 있어서도 그러한 큰 틀을 넘어서는 것은 곤란하다. 따라서 피해자에게 본래 지급되어야 할 위자료 액수가 산정될 수 있음에도 불구하고, 가해자의 재산상태를 이유로 위자료를 감액하는 것은 원칙적으로 허용되어서는 안 된다. 같은 취지에서 가해자의 부(富)가 많다는 이유만으로 이를 증액하는 것도 허용될 수 없다. 하지만 법원이 위자료산정에 관한 폭넓은 재량을 가지고 이에 관하여 별다른 제어수단도 없는 것이 현실이다. 따라서 법원이 내부적으로 이를 고려할 가능성도 있다. 가해자가 고액의 손해배상책임을 부담함으로써 지급불능상태에 이르는 것보다는 저액의 손해배상책임을 부담함으로써 현실적으로 지급이 이루어지게 하는 것이 더 타당하다고 생각할 수도 있기 때문이다. 하지만 가해자의 자력을 고려하여 손해배상액을 산정하는 것은 법률의 뒷받침이 있을 때 비로소 타당성을 획득한다.

이와 관련하여 민법 제765조를 활용하는 방안을 생각해 볼 수 있다. 민법 제765조는 고의, 중과실에 의하지 않은 불법행위에 있어서 배상으로 인하여 배상자의 생계에 중대한 영향을 미칠 경우 그 배상의무자는 법원에 배상액의 경감을 청구할 수 있게 하고, 법원은 채권자 및 채무자의 경제상태와 손해의 원인 등을 참작하여 배상액을 경감할 수 있게 한다. 그러나 이에 관한 대법원 판례는 거의 없고, 그나마 모두 배상액 경감청구를 부정한 사례들이다.[15] 이러한 이유 때문인지 이 조항은 실무에서 거의 활용되지 않고 있는 듯 하다. 그러나 손해배상제도의 지도원리를 손해의 공평·타당한 분담으로 이해하는 대법원 판례의 태도에 비추어 볼 때, 민법 제765조의 손해배상 조정기능은 간과할 수 없다. 그러므로 위와 같은 지도원리를 염두에 둘 때 가해자에게 모든 책임을 부과하는 것이 오히려 부정의한 결과를 가져오는 예외적인 사안에서는 민법 제765조를 원용할 수 있을 것이다.

이러한 해석론만으로도 '잘못의 크기에 비하여 과다한 책임'의 문제를 온전히 극복할 수 없다면, 이는 궁극적으로 손해배상액의 감경이나 상한선 설정 등에 관한 입법조치를 통하여 풀 수 밖에 없다. 참고로 독일에서는 연방정보보호법 제8조 제3항에서 개인정보침해로 인한 손해배상액의 상한선을 130,000유로로 설정하고 있다.

해석론이건 입법론이건 손해배상책임의 경감을 일반적으로 허용할 것인지에 관하여는 추가적인 논의가 필요하다. 다만 이러한 조치가 손해전보기능을 본질적으로 훼손한다고 볼 수는 없다. 위법한 행위로 손해를 입은 자가 그 손해를 전보받아야 한다는 기본명제는 당연하다. 그러나 문제는 전보받아야 할 "손해"는 사실상 발생한 모든 손해가 아니라 규범적으로 평가된 손해이다. 위와 같은 조치들은 넓게 보면 그러한 규범적 평가과정의 일환이다.

15) 대판 1962. 9. 20, 62다428; 대판 1963. 6. 20, 63다242; 대판 1966. 3. 15, 65다2637; 대판 1970. 4. 14, 69다1580; 대판 1995. 2. 17, 84다34234.

# Ⅳ. 결론

많은 불법행위 사건들이 그러하듯이 개인정보침해사건에서도 결국 개인정보의 활용으로 인한 위험을 관련 주체들 사이에 어떻게 배분할 것인가의 문제로 귀착된다. 이러한 위험배분체계(또는 책임배분체계)는 관련 주체들의 행동에 영향을 미친다. 따라서 그 배분이 정교하게 이루어지는 것이 중요하다. 과실과 손해 판단은 이러한 위험배분에 큰 영향을 미친다. 그러한 점에서 이러한 판단기준에 관한 논의는 단지 법조인들에게만 국한되는 성격의 것은 아니다. 즉 개인정보 관련소송은 개인정보보호체계 전반에 파급효과를 미친다.

물론 이러한 소송이 개인정보보호체계를 좌우하는 유일한 요소는 아니다. 따라서 손해배상법제가 안전(security)과 자유(liberty)를 균형 있게 도모하기 위한 전체 사회시스템의 구조 속에서 어떻게 자리매김해야 하는가에 대한 고민이 필요하다. 그러므로 행정지도나 과징금 부과 등의 행정규제, 자율적 규제, 형사처벌, 평판과 신뢰도에 기초한 시장원리 등 다른 예방 내지 제재의 메커니즘들이 어떻게 개인정보보호에 기여할 것인지, 손해배상법은 그 안에서 어떻게 이들과 유기적인 관계를 구축해 나가면서 그 기능을 수행할 것인지에 대한 논의가 지속되어야 할 것이다.

# 개인정보침해행위에 대한 형사처벌의 적절성

전응준, 유미IP법률사무소, 변호사

## Ⅰ. 개인정보보호와 형사처벌

개인정보, 프라이버시에 대한 위협은 정보화사회에서 불가피한 항시적인 문제이다. 이러한 위험상황에 대응하여 우리의 개인정보보호법, 정보통신망법, 위치정보법에서는 사업자의 거의 모든 위반행위에 대하여 형사처벌 규정을 둠으로써, 행정안전부, 방송통신위원회 등의 관할 행정청의 행정조치 외에도 수사기관 등의 사법당국의 관여를 허용하고 있다. 위 법률에서 규정한 형사처벌의 법정형은 일반 형법에 비하여 결코 낮지 않기 때문에 수사기관의 공권력 행사도 소극적이지 않은 것으로 보인다.

이러한 형벌규정은 개인정보침해행위에 대하여 민사상의 구제가 부족하였던 우리의 현실에서 어느 정도 순기능을 가지는 측면도 있다. 법원에서 인정된 손해배상이 그리 만족스럽지 못한 상황에서 피해자들을 대변하면서 공권력에 의한 강제력을 발휘하는 것은 피해자들에 대한 심리적인 보상을 줌과 동시에 사후적인 예방효과를 가질 수 있는 것이다.

한편, 현행법상 개인정보의 정의는 개인에 대한 식별가능성에 의존하고 있고 특별히 이를 한정하는 개념도구도 없기 때문에 그 범위가 광범위하고 불명확한 것이 사실이다. 이러한 상황에서 개인정보처리자는 어떠한 정보가 법률상 개인정보인지 의문이 들 수 있다. 법률적으로 개인정보인 것을 개인정보가 아닌 것으로 오인하여 정보주체의 동의를 받지 않는다면 이는 곧 형사처벌로 이어지게 되기 때문에 개인정보처리자는 항상 긴장할 수 밖에 없다. 현행 '개인정보'의 정의가 죄형법정주의의 명확성의 원칙에 부합하는 지 문제되는 지점이다.

또한 정보주체가 행하는 '동의'의 의미에 대하여도 생각해 볼 필요가 있다. 개인정보를 개인정보자기결정권이라는 헌법상 기본권의 객체로 본다면, 정보주체의 동의는 이러한 기본권을 행사하는 개인의 의사표시라고 할 수 있다. 형법적으로 보면 동의는 구성요건해당성을 조각하는 양해에 해당한다. 의사표시 내지 양해의 일반이론에 따르면, 정보주체의 동의는 묵시적으로도 가능하고 표현방법에 제한이 없다. 그러나 우리의 개인정보보호 실무는 정보주체의 동의를 명시적인 것으로 한정하고 동의가 명시적이지 않은 경우는 아예 동의를 받지 않은 것으로 처리하는 경향이 있다. 이러한 실무의 태도는 행정감독의 관점에서는 타당할 수 있어도 형사처벌의 관점에서는 매우 의문이다.

비교법적 관점에서 보면, 현행 법령체계는 개인정보보호법(관련 정보통신망법 등 포함)을 위반한 거의 모든 행위에 대하여 형사처벌을 규정하고 있는데, 이러한 처벌범위는 다른 입법례에서 발견하기 어려운 것이다. 처벌의 수준도 일반 형법에 비하여 결코 낮지 않고 다른 입법례를 비교하여도 높은 수준으로 되어 있다. 개인정보보호는 세계 각국이 공통적으로 직면하고 있는 문제이고 특히 개인정보의 국제적 유통을 위하여 국제기준에 부합하는 법령체계를 완비할 필요가 있으므로 비교법적 관점에서 우리의 형사처벌 규정을 검토해 보아야 한다.

## Ⅱ. 죄형법정주의의 관점에서 본 '개인정보'의 정의규정

### 1. '개인정보'의 정의에 따른 형사처벌의 문제점

원칙적인 관점에서 보면, 개인정보를 보호객체로 하는 형사처벌규정은 명확성에 한계가 있

다. 우리의 개인정보보호 법령체계에서 정의하고 있는 개인정보라고 함은 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아 볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함)'를 말한다. 이러한 개념정의는 개인에 대한 식별가능성 여부에 의존하고 있는데, 문제는 이러한 식별가능성이 과학기술의 발전, 개인정보 관련 DB의 집적에 의하여 나날이 높아지고 있다는 점에 있다. 예컨대 단독으로는 개인정보로 평가될 수 없는 정보도 다른 DB와 결합하였을 때는 특정 개인을 식별할 수 있는 개인정보가 될 수 있다.

애초 법적으로 보호받는 개인정보의 범위가 공적/사적의 모든 영역을 포함하고 있어 그 범위에 제한이 없는 데다가, '다른 정보와 용이하게 결합'하여 특정 개인이 식별될 수 있는 경우도 개인정보로 보고 있음에 따라, 법률상 개인정보로 볼 수 있는 대상이 시간이 갈수록 확대되고 있다. 바로 이 지점에서 법적 안정성, 예측가능성의 문제가 발생하는데, 이를 형사법의 관점에서 보면 죄형법정주의의 문제가 된다. 예컨대, 개인정보보호에 관한 법률이 제정된 초기에는 별 다른 문제제기가 없었던 IP주소, MAC주소는 현재 논의의 흐름을 보면 대체로 개인정보로 인정되고 있다. 스마트폰 GPS정보도 그 자체로는 개인(위치)정보로 보기 어렵지만 MAC주소, 단말기 번호와 결합하여 개인(위치)정보가 될 수 있다.

현행법상 개인정보의 인정여부는 위 개인정보 정의조항의 해석에 따라 또는 정보를 처리한 사업자의 사정(예컨대 이동통신사와의 사업적 제휴관계, 사업자가 보유한 정보의 내용)에 따라 그 범위가 달라진다. 이는 형사법적 관점에서 죄형법정주의(명확성의 원칙) 위반의 소지가 있고 수사기관의 광범위한 개입을 허용하는 근거가 된다. 법원은 스마트폰 앱의 로그인 절차를 간편하게 하기 위하여 수집된 국제단말기인증번호(IMEI), 범용가입자식별모듈(USIM) 일련번호를 다른 정보와 결합하여 개인을 식별할 수 있는 개인정보로 인정하고 벌금형을 선고하면서, "당해 정보와 결합 가능한 다른 정보는 모두 동일인에게 보유되는 것을 전제로 하지 않고 '쉽게 결합하여 알아 볼 수 있다'는 것은 쉽게 다른 정보를 구한다는 의미이기 보다는 구하기 쉬운지 어려운지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움이 없이 쉽게 결합하여 특정 개인을 알아 볼 수 있게 되는 것을 말한다"라고 판시한바 있다(서울중앙지법 2011. 2. 23.선고 2010고단5343판결). 이러한 논리에 따르면 A라는 사업자의 DB에 있는 정보만으로는 개인이 식별되지 않지만 특별한 사업적 제휴관계가 없는 B라는 사업자의 DB에 있는 정보를 결합시키면 개인이 식별되는 경우에도 A가 보유한 정보는 개인정보로 평가될 수 있다. 이러한 문제를 해결하기 위하여는 '다른 정보와 쉽게 결합'이라는 구성요건에 관한 보다 구체적인 해석론이 필요하다.

## 2. '개인정보'의 정의에 관한 입법례

'개인정보'의 정의에 관한 외국의 입법례는 아래와 같다. 개인정보의 개념은 대체로 국내외 모두 특정 개인을 식별하거나 식별할 수 있는 정보로 정의되고 있음을 알 수 있다. 다만, 식별가능성의 기준에 관하여 EU 지침, 미국, 프랑스의 입법에서는 고유한 식별자를 예시하면서 이들과 결합 내지 참조되어야 함을 규정하고 있고, 개인정보의 범위에 있어서 영국, 호주 등은 다른 나라와 달리 개인에 관한 의견도 개인정보로 포함시키고 있다. 일본 개인정보보호법이 표현하고 있는 개인정보의 정의는 우리나라의 규정과 매우 유사하다.

국내외를 막론하고 개인정보의 개념은 결국 식별가능성의 의미에 의존한다고 할 수 있다. 식별가능성을 판단하기 위하여 일부 입법례는 고유식별자들을 예시하면서 이들의 결합, 참조

에 의하여 개인신원이 확인될 수 있음을 명시하고 있는데, 후술하거니와 개인을 식별하기 위하여 결합, 참조될 수 있는 자료의 범위, 자료를 보유하는 주체 등이 개인정보의 범위를 좌우한다고 볼 수 있다.

이러한 식별가능성의 기준에 관하여 EU 95년 지침은 식별가능성을 판단하기 위해서 정보처리자나 그 밖의 자가 합리적으로 사용할 가능성이 있는 모든 수단을 고려해야 한다고 밝힌 바 있다(whereas to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person)[1]. EU 제29조 정보보호 작업반의 설명에 의하면, 위 기준은 개인을 식별하기 위해 소요되는 비용, 정보처리의 목적, 정보처리의 방식, 정보처리자가 예상하는 이점, 개인과 관련된 이익, 비밀유지의무 위반 등으로 조직내의 부작용이 발생할 위험, 기술적 실패 등의 요소를 고려하는 것이며 다른 측면으로는 정보처리 시점의 기술, 향후 정보가 처리되는 시점에서의 기술의 발전가능성을 고려하는 것이다.[2]

< 해외 입법례에서의 '개인정보'의 정의 >

| 국 가 | 내 용 |
|---|---|
| OECD 가이드라인 | 식별되거나 식별될 수 있는 개인에 관한 모든 정보[3] |
| EU지침 | 식별되거나 식별될 수 있는 자연인에 관한 모든 정보 ; 식별될 수 있는 자란 신원확인번호나 개인이 가지는 고유한 신체적·생리적·정신적·경제적·문화적·사회적 특질 중 하나 이상의 요소 등을 참고(reference)함으로써 직·간접적으로 신원이 확인될 수 있는 사람을 말한다.[4] |
| 독일 | 식별되거나 식별될 수 있는 개인의 인적, 물적 환경에 관한 일체의 정보[5] |
| 영국 | 다음으로부터 식별할 수 있는 생존하는 개인에 관한 데이터<br>· 당해 정보 ; 또는<br>· 정보관리자(data controller)가 보유하고 있거나 보유할 가능성이 있는 기타 데이터나 정보(information). 그리고 해당 개인에 대한 견해의 표시나 해당 개인에 대한 정보관리자 또는 기타 사람들의 의도를 드러내는 모든 표시를 포함하는 데이터나 정보[6] |
| 일본 | 생존하는 개인에 관한 정보로서, 당해 정보에 포함되는 성명, 생년월일 기타 서술 등에 의해 특정한 개인을 식별하는 일이 가능한 것(다른 정보와 용이하게 조합되어, 그에 의해 특정한 개인을 식별하는 일이 가능하게 되는 것을 포함한다)을 말함[7] |
| 미국 | (Privacy Act 1974)행정기관이 보유하는 개인에 관한 정보의 개개 항목 또는 그 집합을 말한다. 그 기록(record)에는 당해 개인의 교육, 금전적 거래, 병력, 전과, 취업경력에 관한 정보가 담기지만 이에 한정되지 않는다. 그리고 그 기록에는 당해 개인의 이름 또는 식별번호나 식별부호 혹은 지문, 성문, 사진과 같은 당해 개인에게 고유한 식별자가 포함되어 있어야 한다[8] |
| 프랑스 | 직·간접적으로 식별확인번호나 특정인을 확인하게 해주는 하나 이상의 요소를 참고함으로써 식별되거나 식별가능한 개인에 관한 정보. 개인이 식별가능한지 여부를 결정하기 위해서는 신원확인을 위해 정보처리의 책임자가 접근가능하거나 이용할 수 있는 모든 수단 또는 기타의 자가 가질 수 있는 모든 수단을 고려할 것이 권고된다. |
| 스웨덴 | 직·간접적으로 생존하는 자연인을 언급할 수 있는 모든 유형의 정보 |
| 핀란드 | 사람 또는 사람의 가족 구성원이나 세대에 관한 것으로서 이들을 식별할 수 있는 사적 개인에 관한 모든 정보 및 당해 개인의 사적인 특징이나 상황에 관한 모든 정보 |
| 캐나다 | 식별할 수 있는 개인에 대한 정보. 단, 정보처리단체(organization)의 직원들의 이름, 직위, 직장 주소, 전화번호는 포함되지 아니한다. |
| 호주 | 당해 정보 또는 의견으로부터 신원이 명백하거나 확실시될 수 있는 개인에 관한 정보 또는 의견을 의미하는 것으로, 데이터베이스에 포함된 정보 또는 의견을 포함하며 해당 정 |

1) EU 95년 지침 전문 제26호
2) ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 4/2007 on the concept of personal data, 15면

| 국 가 | 내 용 |
|---|---|
| | 보가 진실인지 여부 및 물리적인 형태로 기록되어 있는지 여부와는 관계없음 |
| 뉴질랜드 | 식별가능한 개인에 관한 정보로서 「출생사망신고법 1951」에 의해 보관되는 사망자등록부에 포함된 정보를 포함 |

## 3. '개인정보'의 정의에 관한 해석론

전술한 바와 같이, 유럽 여러 나라의 입법의 기초가 된 EU 95년 지침은 식별가능성의 기준에 대하여 정보처리자나 그 밖의 자가 합리적으로 사용할 가능성이 있는 모든 수단을 고려하여야 한다고 보고 있다. 그리고 29조 정보보호 작업반은 개인의 식별가능성 여부를 결정하기 위하여 고려되는 요소로서 비용, 의도, 경제적 이점, 현재 및 장래의 기술수준 등을 들고 있다. 이러한 견해를 종합하면, 개인을 식별하는 개인정보는 단독으로 개인을 식별하는 정보뿐만 아니라 다른 정보와 결합하여 개인을 식별하고자 하는 의도가 담긴 정보, 지금 당장은 아니지만 향후 기술발전에 의하여 개인을 식별할 수 있을 가능성이 있는 정보등도 포함하게 된다. 즉 개인을 식별할 가능성이 있는 정보인지 여부는 시간적, 공간적으로 유연하게 고려되어야 하는 것이다.

이와 같은 개인정보의 개념은 우리나라 법률에서는 "해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다"는 표현으로 포섭되었다. 이는 정보주체의 권리를 보호한다는 측면에서는 매우 당연한 입법이었을 것이라고 생각된다. 그러나 우리나라의 경우에는 개인정보침해행위를 직접적으로 형사처벌함으로써(독일과 같은 친고죄도 아님), 개인정보의 개념에 관하여 죄형법정주의에 따른 형법적 관점도 필요하게 되었다. 이에 따라 개인정보의 개념은 정보주체의 권리보호에 도움이 되어야 할 뿐만 아니라 개인정보처리자에게 범죄와 형벌이 어떠한 것인지 예견하여 주어야 하고 이로써 개인정보처리자에게 적절한 행위기준을 시사해 주어야 한다.

"해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다"는 표현과 관련하여 개인정보의 범위로 제시될 수 있는 견해는 크게 보아 다음의 2가지로 보인다.[9]

A설 : 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보라면, 실제로 다른 정보와 결합하여 특정 개인을 식별한 바 없더라도, 특정 개인을 식별할 수 있는 잠재적 가능성이 있

3) any information relating to an identified or identifiable individual
4) any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
5) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).
6) data which relates to a living individual who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller
7) この法律において「個人情報」とは、生存する個人に關する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む）をいう
8) 5 U.S.C. §552a (a) (4) - the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph
9) 정상조, 비식별개인정보의 보호 및 활용에 관한 연구, 39면

는 이상 그 정보를 개인정보로 보아야 한다

B설 : 다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보가, 실제로 다른 정보와 결합하여 특정 개인을 식별할 수 있게 된 경우에 한하여, 그 정보를 개인정보로 보아야 한다. 이와 달리, 다른 정보와 결합함이 없이 익명으로 처리되어 특정 개인을 식별할 수 없는 상태에서 이용된 비식별개인정보는 동법상의 개인정보로 볼 수 없다.

B설은 해당 정보가 다른 정보와 결합하여 실제로 특정 개인을 식별할 수 있게 된 상태에 놓여야 개인정보로 인정한다. 그에 반하여 A설은 다른 정보와 결합하여 특정 개인을 식별할 수 있는 가능성만 있어도 개인정보로 인정한다. B설은 실제로 정보들이 결합하여 특정 개인을 식별할 수 있게 되어야 개인정보로 인정하기 때문에 어떠한 정보가 개인정보가 되는 지 비교적 명확하게 알 수 있다. 이러한 점은 죄형법정주의의 관점에서도 크게 환영할 수 있는 견해이다. 그러나 B설은 OECD 가이드라인, EU 지침 등에서 수용된 개인정보의 개념과는 다소 거리가 있다고 생각된다. 위 가이드라인 등은 개인을 식별할 수 있는 일체의 정보를 개인정보로 보기 때문에 실제로 결합되지는 않았지만 향후 결합될 가능성이 있는 다른 정보를 참고하여 특정 개인이 식별될 수 있는 정보도 개인정보로 포함한다고 해석한다. 위 정보보호 작업반이 개인정보의 예로 든 향후 기술발전에 의하여 특정 개인을 식별할 수 있는 가능성이 높은 정보는 B설에 의하여 설명되기 어렵다.

그러므로, 개인정보의 개념은 기본적으로 A설이 타당하다고 생각한다. 다만, A설이 말하는 특정 개인을 식별할 수 있는 '잠재적 가능성'이 무엇인지 더 구체적으로 해석되어야 할 것이다. 이 점에 관하여 EU 95년 지침을 수용하여 제정된 영국 데이터보호법을 참고하는 것이 도움이 된다. 영국 데이터보호법은 '정보관리자가 보유하고 있거나 보유하게 될 가능성이 높은 데이터(those data and other information which is in the possession of, or is likely to come into the possession of, the data controller)'를 기준으로 개인에 대한 식별가능성을 판단하고 있다. 영국의 가이드라인은 '보유'의 의미를 '통제'로 해석하고 있다. 즉 정보관리자가 해당 정보를 '실제적으로 통제'(physical control)하거나 통제할 것 같으면 개인정보가 될 수 있다는 것이다.[10]

이러한 영국의 실무에서 시사받을 수 있는 것은 2가지라고 생각된다. 첫 번째, 우리나라 법률에서 규정한 '다른 정보와 쉽게 결합'한다는 것의 기준은 개인정보처리자가 되어야 한다. 개인정보처리자의 입장에서 해당 정보가 다른 정보와 쉽게 결합되어야 한다는 것이다. 개인정보처리자에 의하여 실제로 결합될 가능성이 거의 없고 이론상으로만 결합될 가능성이 있는 정보는 개인정보를 여부를 결정하는 자료로 볼 수 없다. 두 번째, 개인정보처리자는 다른 정보를 현실적으로 통제하고 있거나 지금은 통제하지 않더라도 현실적으로 통제할 수 있는 가능성이 상당히 높은 경우이어야 한다. 다른 정보를 사용할 수 있는 특별한 계약관계 내지 정보시스템의 연결관계가 없는 경우라면 그 다른 정보는 '쉽게 결합'할 수 있는 정보가 아니라고 하여야 한다. 이 점에서 위 우리나라 하급심 판결이 앱서비스 제공자(피고인)가 이동통신사의 DB정보를 사용할 수 있는 법적, 사실적 관계가 있는지 여부를 가리지 않고 단지 이동통신사의 DB정보가 제3자에 의하여 획득될 가능성이 없는 것으로 보이지 않는다는 추상적인 가능성만으로 이동통신사의 정보를 '쉽게 결합될 수 있는 다른 정보'로 인정한 것은 비판의 소지가 많다고 생각한다.

10) 박노형, EU 및 영국의 개인정보보호법제연구, 56면

결론적으로, '다른 정보와 쉽게 결합하여 특정 개인을 식별할 수 있는 정보'의 범위는 개인정보처리자의 입장에서 해당 정보를 현실적으로 통제하는 지 여부 또는 현재는 통제하지 않더라도 계약관계, 사실상의 관계에서 해당 정보를 통제할 가능성이 상당히 높은 지 여부에 따라 판단되어야 한다. 여기에는 결합에 소요되는 비용, 기간, 노력도 중요한 판단요소가 되지만 무엇보다 개인정보처리자의 의도가 중요하다고 생각된다. 개인정보처리자에게 향후 다른 정보와 결합하여 특정 개인을 식별하려는 의도가 있다면 개인정보처리자는 해당 정보를 개인정보보호법에 따른 개인정보로 취급하여야 할 것이다.

# Ⅲ. 범죄구성요건을 배제하는 정보주체의 '동의'

## 1. '동의'의 형법적 의미

정보주체의 개인정보를 무단으로 수집, 이용등을 하는 개인정보침해행위는 정보주체의 동의에 반할 것을 그 전제로 하고 있으므로, 형법이론상 정보주체의 동의는 위법성조각사유라기보다는 구성요건해당성을 배제하는 양해로 평가된다. 즉 정보주체의 동의가 있으면 처음부터 범죄구성요건에 해당하지 않는다.[11] 이는 주거침입죄, 절도죄 등에서 주거권자, 점유자의 동의가 있으면 주거침입행위, 절취행위가 성립하지 않는 것과 같은 이치이다.

대체로, 법익주체의 동의가 구성요건을 조각시키는 범죄유형으로는 자연적인 행동의 자유, 의사결정의 자유, 사실상의 지배관계의 침해와 관련된 범죄를 들고 있는데, 정보주체의 동의없이 개인정보를 무단으로 수집, 이용하는 개인정보침해행위도 이러한 범주에 속한다고 할 수 있다. 정보주체의 동의는 개인정보에 대한 사실상 지배권을 이전하는 의사표시라고 해석되기 때문이다.

일반적으로, 구성요건을 배제하는 양해는 순수하게 사실적인 성격을 가지기 때문에 ① 양해자의 내심에 존재하는 내부적 동의로도 족하며 반드시 외부적으로 표시될 필요가 없고[12] ② 따라서 상대방이 양해가 있다는 사실을 인식할 필요도 없으며 ③양해가 착오로 표시된 경우에도 유효하고 ④ 사실상의 양해로 충분하기 때문에 양해자는 자연적 의사능력을 가지고 있으면 되고, 훼손당하는 법익의 의미를 이해한다든가 판단능력이 필요한 것은 아니라고 설명된다.[13][14]

타인에게 자신의 개인정보를 제공하려는 정보주체의 동의 역시 행위의 법률적 성격을 파악하는 판단능력이나 거래능력을 요구하는 것이 아니라 수집,이용행위 자체의 자연적 의미만을 파악하면 가능하다. 즉 자신의 개인정보에 관한 사실상의 지배관계를 타인에게 넘겨주어 이를 이용하게 한다는 자연적인 의사능력만 있으면 정보주체의 동의로서 충분하고 이로써 범죄구성요건은 배제된다.

정보주체의 동의를 피해자의 승낙이 아닌 양해로 이해한다면, 행위시에 양해가 존재하였다는 사실이 중요하기 때문에 이러한 양해는 반드시 명시적으로 표현될 필요가 없다. 다만, 개인정보보호법은 고지된 동의(informed consent)를 요구하므로(제22조), 비명시적 동의, 묵시적 동의인 경우에도 정보주체에게 수집목적이나 범위등에 관하여 충분히 설명하고 이를 명확하게 인지하도록 하여야 한다.

---

11) 이정원, 형사법상의 개인정보보호, 경남법학 제111집, 273면, 정혜욱, 개인정보보호법상의 형사처벌규정에 관한 연구, 법학논문집 제35집 제3호, 중앙대학교 법학연구원, 124면

12) 묵시적으로도 표시될 필요가 없다고 한다.

13) 임웅, 형법총론, 법문사, 1999, 228면

14) 이에 대하여 구성요건의 성격(의료적 침해, 모욕 등)에 따라서 자연적인 의사능력을 넘어서는 법률상 판단능력 내지 행위능력을 요구하는 견해도 있다.

## 2. 묵시적 동의도 포함하는 지 여부

위와 같이, 형법의 일반이론에 따르면, 정보주체의 동의는 순수한 사실적 행위인 양해에 해당하여 명시적, 묵시적 동의에 의하여도 유효한 양해가 되며 외부에 표현될 필요도 없게 된다.

그러나 우리나라의 수사실무나 행정실무는 정보주체의 동의를 엄격하게 파악하여 거래관계에 따른 묵시적 동의 내지 추정적 승낙을 이에 포함시키지 않는 것으로 보인다. 즉, 현행 개인정보보호법 해설서는 정보주체의 명시적인 동의를 얻어야 개인정보를 처리할 수 있다고 표현하고 있으며[15], 경찰 등의 수사기관에서도 정보주체의 동의가 명시되어야 개인정보보호법/정보통신망법위반이 아니라는 태도를 보이고 있다. 이에 따라 특히 수사실무에서는 정보주체의 명확한 동의를 보여주는 자료가 없는 경우 일단 개인정보보호법위반의 강한 혐의를 두는 경향이 보이고 있다.

그러나 법리적으로 볼 때 정보주체가 개인정보자기결정권을 행사함에 있어 그 의사표시인 동의를 반드시 명시적인 형태로만 할 필요는 없다. 이는 정보주체의 자유와 편의의 문제인 것이다. 어느 경우에나 명시적인 동의를 요구한다면 일상적인 거래관계가 어려워질 수 있다. 위 해설서에서도 예를 든 것처럼, 인터넷 중고거래사이트에서 상품을 팔기 위하여 정보주체가 판매물품에 대한 설명과 자신의 전화번호를 기재한 경우, 이는 해당 상품의 거래목적으로 전화번호를 이용해도 된다는 동의의 의사표시를 한 것으로 보아야 하고 묵시적 동의에 해당한다.[16]

현행 개인정보보호법, 정보통신망법, 위치정보법, 신용정보법 등은 정보주체의 동의를 반드시 명시적으로 받으라고 규정하고 있지 않다. 위 법률은 해당 정보주체에게 수집목적, 항목, 기간 등을 명확하게 인지할 수 있도록 알리고 동의를 받으라고 하고 있을 뿐이다(개인정보보호법 제22조). 다만, 하위 시행령에서 동의받는 방법을 한정하여 개인정보처리자에게 전화, 우편, 팩스, 인터넷 홈페이지 등을 통하여 동의의 의사표시를 확인할 것을 요구하고 있다(개인정보보호법 시행령 제17조, 정보통신망법 시행령 제12조)[17]. 그러나 위 시행령 규정이 정보주체가 행할 수 있는 동의의 형식을 제한하는 것으로 해석되어서는 곤란하다. 위 규정은 개인정보처리자의 정보주체에 대한 고지방법을 특정한 것이며 이를 어기고 동의를 받더라도 동의 자체가 없는 것은 아니다. 정보주체에게 명확하게 알리지 않고 동의를 받는 행위는 동의를 전혀 받지 않는 행위와 구분되며 이는 별도로 과태료라는 행정질서벌로 규제되고 있다(개인정보보호법 제75조 제3항 제2호[18]).

물론 정보주체의 권익을 보호하기 위하여 정보주체의 동의는 반드시 명시적인 동의이어야 한다고 해석할 수도 있다. EU 1995년 지침도 전문 (33), 제7조에서 정보주체의 명시적 동

---

15) '이 법에서 정보주체의 동의는 명시적 동의를 의미한다', 행정안전부, 개인정보보호법령 및 지침고시 해설서, 73면

16) 행정안전부, 개인정보보호법령 및 지침고시 해설서, 82면

17) 해외 입법례

- EU 개인정보보호지침 제2조제h항 : "정보주체의 동의"라 함은 정보주체가 그 자신과 관련된 개인정보가 처리되도록 하는 합의를 표시함으로써 자유롭게 표명된, 특정의 통지된 의사표시를 말한다.
- 독일 연방데이터보호법 제4a조제(1)항 : 동의는 관련인의 자유결정에 의했을 경우에만 효력이 있다. 개별적 상황에 따라 필요하거나 요구를 받은 경우 관련인에게 개인정보의 수집목적, 생산 또는 이용, 동의거부에 따른 결과에 대하여 설명해 주어야 한다. 동의는 특별한 상황에 따른 다른 방법이 적절치 않다면 서면의 형식을 갖추어야 한다. 동의가 다른 설명과 함께 서면의 형식으로 교부되어야 한다면 이 동의는 특별히 강조되어야 한다.
- 영국「데이터보호법 해설서(Data Protection Act 1998, Legal Guidance)」3.1.5 동의 : "정보주체는 반드시 그의 동의를 "표시"하여야 한다는 사실은 당사자간에 활발한 의사소통이 있어야 한다는 것을 의미한다. 정보주체는 주로 서면으로 동의를 표시할 것이다. 정보관리자는 고객이 리플렛에 응답하지 않거나 또는 되돌려보내지 않는 의사소통에 대한 무응답으로부터 동의를 추론할 수 없다. (이하 생략)"

18) 개인정보보호법 제75조 제3항 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.
2. 제22조제1항부터 제3항까지의 규정을 위반하여 동의를 받은 자

의(explicit consent, unambiguously given his consent)가 필요함을 규정하고 있다. 그러나 이러한 해석은 경우에 따라 오히려 정보주체의 의사표시 방법을 제한하고 불필요한 거래비용을 증가시킬 우려가 있으므로, 이러한 원칙은 실정법의 세계에서 탄력적으로 적용될 필요가 있다. 실제로 영국 데이터보호법, 독일연방데이터보호법, 일본 개인정보보호법에서 정보주체의 동의를 반드시 명시적인 것으로 제한하는 규정은 없는 것으로 보인다.[19] 나아가 동의가 범죄구성요건의 성부를 좌우한다는 점에서 보면, 정보주체가 어떠한 방법으로든 적법하게 처분한 보호법익에 대하여 처분의 의사표시가 명시적이지 않다고 하여 형사처벌을 가하는 것은 매우 부당하다고 생각한다. 이 점에서 정보통신망법 시행령 제12조 소정의 동의받는 방법을 준수하지 않은 경우 동의 자체를 받지 않은 것으로 보아 정보통신망법 제71조 제1호 내지 4호 소정의 5년 이하의 징역 또는 5천만원 이하의 형사처벌을 할 수 있다는 견해[20]에는 큰 의문이 있다.

## 3. 동의의 예외요건에 관한 검토

현행 우리나라 법률은 개인정보의 모든 처리과정에서 정보주체의 동의가 원칙적으로 필요하다는 관점에 서 있다. 이는 기본적으로 타당한 관점이라고 할 수 있다. 그러나 원칙에 대응하는 예외를 적절히 규정하지 않으면 이는 일종의 도그마로 변질될 가능성이 높고 국제기준에도 부합되지 않을 공산이 크다. 개인정보의 수집, 이용, 저장, 제공, 파기에 이르는 생명주기의 전 과정에서 정보주체의 동의를 한결같이 요구하는 것은 불필요한 거래비용을 증가시킬 뿐 정보주체의 인격권 보호에는 큰 도움이 되지 못한다. 경우와 상황에 따른 동의 조건의 완화 내지 예외는 당연히 필요하다.

각국을 입법례를 보아도 동의를 요하는 요건이 동일하지 않음을 알 수 있다. 일본 개인정보보호법은 개인정보의 수집단계에서는 정보주체의 동의를 반드시 요구하지 않고 그 이용목적을 정보주체에게 통지하면 족하도록 하고 있으며, 제3자 제공에서도 옵트아웃(opt-out)방식의 동의를 허용하고 있다. EU 1995년 지침은 계약이행에 필요한 경우, 정보주체의 중대한 이익을 보호하기 위한 경우, 개인정보처리자의 정당한 이익을 위한 것으로서 정보주체의 권리보다 우선하는 경우 등과 같이 개인정보의 수집, 이용, 제공 시 정보주체의 동의없이 이를 처리할 수 있는 통일적인 예외요건을 규정하고 있다.

반면, 우리나라의 개인정보보호법은 개인정보의 수집, 이용 단계(제15조)에서는 EU 1995년 지침과 유사한 동의의 예외요건을 두고 있지만 제3자 제공(제17조), 목적외이용·제공(제18조)에서는 동의를 요하지 않는 예외요건을 축소하여 타 입법례에 비하여 보다 엄격하게 개인정보의 처리를 허용하고 있다. 예컨대, 현행 개인정보보호법에 의하면 계약의 체결 및 이행을 위하여 불가피한 경우 개인정보의 수집·이용은 가능하지만, 제3자 제공, 목적외이용·제공은 불가능하다.

동의획득의무는 기본권의 보호와 사회의 편익이 형량되어야 하는바, 일반법으로 개인정보보호법이 시행된 지 얼마 되지 않은 상황에서 타 입법례보다 정보주체의 동의를 엄격하게 요구하는 것은 과도한 컴플라이언스 비용을 유발하여 무리라고 보인다. 나아가 형사정책의 관점에서 보면, 불필요하거나 불가능한 동의획득요구는 수범자로 하여금 법규준수의무를 쉽게 포기하게 만들어 범죄자를 양산할 우려가 크다. 우리나라의 개인정보보호법도 EU지침과 같이

19) 독일연방데이터보호법, 영국 데이터보호법은 민감정보의 처리에 관하여 정보주체의 명시적 동의를 요구한다.
20) 방송통신위원회, 정보통신서비스제공자를 위한 개인정보보호 법령 해설서, 64면

개인정보처리원칙을 통일하여 무분별한 개인정보의 처리는 금지하되, 불필요하거나 현실적으로 불가능한 동의획득의무는 면제하여 사회경제적 비용을 경감시킬 필요가 있다.[21]

# Ⅳ. 형사처벌규정의 개선

## 1. 입법형식 및 법정형의 개선

현행 우리나라의 개인정보보호관련 법률은 거의 모든 법률위반행위를 형벌 또는 과태료의 대상으로 하고[22], 범죄구성요건의 주요표지인 '개인정보'의미를 결국 법관의 보충적 해석에 의하여 보완하도록 하고 있는바, 이러한 체계로는 죄형법정주의에서 요구하는 명확성의 원칙 내지 개인정보의 범위에 관한 예측가능성이 떨어지게 되고 과잉형사처벌을 막을 수 없으므로 마땅히 입법적 개선이 필요하다고 생각한다. 광범위하고 과도한 형사처벌규정은 수범자에게 법규준수의 의지를 저하시키고 오히려 사법기관도 형벌집행에 소극적으로 나서게 되는 원인이 된다.

개인정보침해행위에 대한 형사처벌의 필요성은 해외 각국도 크지 다르지 않을 것이므로, 형사처벌규정의 개선사항은 비교법적 관점에서 논의하여도 좋을 것이다. 이하에서 각국의 형사처벌규정을 살펴본다.

일본 개인정보보호법은 법률위반행위에 대하여 직접적으로 형벌을 가하지는 않고 주무장관이 명령한 시정권고조치/시정조치에 응하지 않을 경우에만 6월 이하의 징역 또는 30만엔 이하의 벌금에 처하도록 하고 있다(제56조).[23]

영국 데이터보호법의 형사처벌규정은 일본과 유사한데, 집행통지(enforcement notice), 정보통지(information notice), 특별정보통지(special information notice)를 이행하지 않을 경우 벌금을 부과한다(제47조, 제60조 제2항),

독일연방데이터보호법은 권한없이 일반적으로 접근할 수 없는 개인정보를 수집 또는 생산한 경우 등에 최고 30만유로의 과태료(Bußgeld)를 부과하고(제43조 제2항), 자기 또는 타인의 이익을 위한 목적에서 또는 타인을 해할 목적에서 의도적으로 제43조 제2항에 열거된 행위를 한 자를 최고 2년 이하의 징역 또는 벌금에 처한다. 위 범죄는 친고죄인데 고소는 정보주체이외에도 개인정보처리자, 연방개인정보보호청, 주의 정보감독청에 의하여도 가능하다. 독일연방데이터보호법은 사회적으로 비난가능한 행위에 대하여 행정질서벌인 과태료를 부과하고, 위 행위에 행위자의 악의적인 목적이 있는 경우 형사처벌을 과하고 있다. 개별 법률위반행위에 대하여 형사적 제재가 있다는 점에서 우리나라의 경우와 유사하나 그 종류가 우리나라에 비하여 상당히 적고 법정형도 낮다.

미국은 프라이버시보호를 아우르는 일반법을 제정하지 않고 개별 영역에 관한 특별법을 제정하여 이에 대처하고 있다. 그 중 공적영역에서의 대표적인 개별연방입법인 1974년 프라이버시법(Privacy Act, 1974), 사적영역에서의 대표적인 개별연방입법인 1986년 전자통신 프라이버시법(Electronic Communications Privacy Act, 1986)의 형사처벌규정을 살

---

21) 이창범, 비교법적 관점에서 본 개인정보보호법의 문제점과 개정방향, Internet and Information Security 제3권 제2호, 93면

22) 법률위반행위에 대하여 상한이 10년에서 2년까지의 징역 또는 1억에서 1천만원의 벌금에 처하거나 5천만원에서 1천만원에 이르는 과태료를 부과함

23) 주무장관은 당해 위반행위의 중지 등을 위하여 필요한 조치를 취할 것을 권고할 수 있고, 위 권고를 받은 개인정보처리자가 정당한 이유없이 권고에 상응한 조치를 취하지 않고 개인의 권리침해가 임박하다고 인정될 때는 위 권고에 관한 조치를 행하도록 명령할 수 있으며, 개인의 중요한 권리를 침해하여 긴급한 조치를 취할 필요가 있다고 인정되는 때에는 바로 당해 위반행위를 시정하기 위하여 필요한 조치를 명령할 수 있다(일본 개인정보보호법 제34조).

펴본다. 프라이버시법은 연방기관의 공무원등이 개인을 식별할 수 있는 연방기관의 기록(record)를 악의적으로 공개하는 행위를 경범죄(misdemeanor)로 규정하고 $5,000 이하의 벌금에 처하고 있고[24], 전자통신프라이버시법은 제3자가 유선통신, 구술통신, 전자통신의 내용을 악의적으로 획득, 사용, 공개하는 행위에 대하여 5년이하의 징역 또는 $250,000 이하의 벌금에 처하도록 규정하고 있다.[25] 전자통신프라이버시법은 통신상의 프라이버시를 보호하는 법률이기 때문에 형사처벌의 성격이 우리나라 개인정보보호법과 다른 것으로 보인다.

정리하여 보면, 해외 주요국가 개인정보보호법률의 형사처벌규정은 대체로 개별 법률위반행위에 대한 직접적인 제제 대신에 행정청의 시정조치를 매개로 하여 이를 위반하는 경우 비로소 형사처벌을 하거나(일본, 영국), 개별 법률위반행위에 대하여 직접 형사적 제재를 가하더라도 규제행위의 수가 적고 그 법정형도 우리나라의 경우보다 현저히 낮다(독일).

이러한 입법례를 고찰하여 볼 때, 현행 우리나라 개인정보보호법률의 형사처벌 규정은 상당히 엄격하고 높은 수준으로 규율되고 있음을 알 수 있다. 특히 법률위반행위에 대하여 높은 수준의 직접적인 형사처벌을 규정하고 있기 때문에 관할 행정청과 별도로 수사기관이 사법적 조치를 취할 개연성이 높다. '개인정보'의 정의 및 범위에 관하여 아직 법원의 해석이 확립되지 않은 상황에서, 수사기관은 개인과 관계된 새로운 유형의 정보가 등장할 때마다 이를 법률상 '개인정보'로 취급하여 동의확보 여부를 조사하는 경향이 있는 것으로 보인다.

형사처벌은 형벌의 보충성 원리에 따라 피해를 구제하기 위한 다른 민사적, 행정적 조치가 부재할 때 비로소 이루어져야 하는 것이므로, '개인정보'의 의미, 보호 및 활용에 관한 전문적이고 국제적인 고려가 부족한 현 시점에서 강제수사에 입각한 공권력행사가 우선적으로 행하여지는 것은 바람직하지 않다고 생각된다. 원래 개인정보보호법 초안은 개인정보보호 원칙이 발전과정에 있고 개인정보보호법이 일반법이라는 점을 고려하여 처벌규정이나 수준을 최소화하고자 하였다고 한다. 즉 개인정보처리자가 의도적으로 특정 목적을 위하여 불법을 저지르는 파렴치하고 비난 가능성이 높은 목적범에 대해서만 형사처벌을 하고, 단순한 법 위반행위에 대해서는 시정권고나 시정명령을 할 수 있게 하였다고 한다.[26]

개인정보는 보호의 대상이기도 하지만 활용의 대상이기도 하다. 개인정보의 보호와 활용은 동시적으로 고려되어야 한다는 점에서 보호와 활용은 어느 선에서 적절히 타협하여야 한다. 이러한 경계선의 획정은 개인정보보호에 관한 전문적인 능력과 책임이 있는 기관에서 다루어야 한다. 또한 개인정보침해를 당한 피해자 구제를 위하여는 감독기관의 즉각적이고 실효적인 조치, 실질적인 손해배상이 우선적으로 고려되어야 하고 형사처벌은 보충적인 수단임은 분명하다. 이러한 관점에서 형사책임의 입법형식에 관하여 다음과 같은 방안을 제안한다.

O 감독기관의 시정명령권을 활성화하고 이를 위반하는 경우에 형사적 제재를 가하는 방법. 이는 감독기관에게 당해 위반행위의 사회적인 의미를 평가할 수 있는 1차적 권한을 부여하고, 종합적인 사정을 고려하여 적절한 시정조치를 명령할 수 있도록 하면서 시정조치의 이행을 형사적으로 강제하는 방법이다.

O 개개의 의무사항에 대한 단순 위반행위에 형사처벌을 가하는 방식을 지양하고, 위반의 고의

---

24) 5 USC §552a (i) (1)
25) 18 U.S.C. 2511 (4)(a). felony에 대한 벌금은 $250,000이하이다.
26) 이창범, 비교법적 관점에서 본 개인정보보호법의 문제점과 개정방향, Internet and Information Security 제3권 제2호, 72면

외 목적범, 영업범 등의 특별한 신분표지를 갖춘 경우에 형사책임을 부담시키는 방법. 각국의 입법례를 볼 때 우리나라와 같이 법률에서 정한 수십 개의 의무사항을 단순 위반한 경우에도 형사처벌을 하는 예는 드문 것으로 평가된다. 법위반행위가 일상화되면 효율적인 형법집행은 오히려 어려워진다. 독일의 예와 같이, 대가를 받거나 자신/타인의 이익을 목적 또는 타인에게 손해를 가할 목적이 있는 경우 등에 형사처벌을 가하고 그 외의 경우에는 행정질서벌인 과태료를 부과하는 방법이다.

O 형사처벌형식에 관하여 어느 방식을 택하더라도, 현행 법정형은 다소 낮출 필요가 있다고 생각된다. 정보통신망법은 2008. 6. 13. 개정으로 기존 과태료 중심이던 벌칙규정을 형사처벌규정으로 상향한 바 있고 개인정보보호법은 그와 상응하게 법정형을 규정하였다.

그러나 동의 없는 단순 수집, 제공 등의 행위에 대하여 5년 이하의 징역 내지 5,000만원 이하의 벌금형에 처하게 하는 것은 전체적인 형벌체계를 고려할 때 상당히 무거운 형벌이라고 생각된다(개인정보법 제71조, 정보통신망법 제71조). 이는 형법상 명예훼손죄, 업무상 비밀누설죄보다 높고 배임죄, 영업비밀누설죄와 유사한 정도인데, 법정형의 관점에서 보면, 현행 개인정보침해죄는 개인정보를 영업비밀과 유사하게 보면서 개인정보처리자의 개인정보침해행위를 배임적 행위로 보는 것과 같다.

또한 동일한 행위에 대하여 법률에 따라 다르게 규율하거나, 다른 개인정보에 비하여 위치정보침해에 대하여 형사적으로 과잉보호하는 것이 발견된다. 예컨대, 정보주체의 동의없이 개인정보를 수집하는 행위는 정보통신망법에서는 형벌의 대상이나 개인정보보호법에서 과태료의 대상이다(정보통신망법 제71조 제1호, 개인정보보호법 제75조 제1호) 위치정보법의 경우, 개인정보에 해당하지 않는 '이동성 물건 및 식별되지 않는 개인에 관한 위치정보'도 형사처벌의 대상으로 삼고 있다(위치정보법 제40조 제4호). 또한 단순히 기술적, 관리적 조치를 취하지 않는 행위는 개인정보보호법, 정보통신망법에서는 과태료부과대상이나, 위치정보법에서는 형사처벌의 대상으로 되어 있다(위치정보법 제41조 제4호)

전체적인 관점에서 개인정보보호 관련 법률들의 법정형 수준을 검토할 필요가 있으며, 개인정보보호법, 정보통신망법, 위치정보법 등의 관련 법률들 간의 형사처벌 규정도 일관성있게 조정되어야 한다고 판단된다.

# 개인정보보호법이 의학 및 보건학 연구에 미치는 영향

서울대학교 의과대학 예방의학교실 박병주

## Ⅰ. 연구배경 및 필요성

개인정보보호법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리를 보호하고 이익을 증진시키며, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정하는 것을 목적으로 제정되었다. 개정된 개인정보보호법이 2011년 9월부터 발효됨에 따라 공공과 민간에서 개인정보를 수집, 저장, 가공, 제공, 공개, 파기할 때 법에서 규정한 절차를 위반하게 되는 경우 처벌이 따르게 되었다. 이 법률은 직접 의학연구를 관리하기 위하여 제정된 법률은 아니지만 개인정보보호에 관한 일반법으로서 의학연구를 수행하고자 하는 모든 연구자들은 이 법률의 내용을 준수하여야 한다.

하지만 굳이 법률까지 적용하지 않더라도 연구자가 연구참여자를 존중하고, 연구참여자의 권익과 건강을 보호하기 위한 노력을 기울이는 것은 의학연구가 윤리적으로 수행되었다는 평가를 받기 위한 필수적인 전제조건이다. 연구자는 항상 연구대상자의 입장에서 생각하여야 하며 특히 연구참여에 대한 결정을 스스로 내릴 수 없거나 거부할 수 없는 경우에는 더욱 특별한 주의를 기울여야 함을 윤리적인 이유로 강조하고 있다.(1) 이러한 연구대상자의 자기결정권 존중은 연구내용에 대한 충분한 설명 후 동의를 얻는 과정을 통하여 실현되는데 이는 이미 우리나라 의학연구 현장에서 당연하고 필수적인 과정으로 자리잡고 있다. 2008년 서울에서 개최된 제 59차 세계의사총회에서 개정된 헬싱키선언은 제 25조에 개인 식별이 가능한 인체유래물이나 자료를 이용한 의학연구의 경우, 의사는 통상적으로 수집, 분석, 보관 및 재사용에 관한 동의를 구하여야 한다는 항목이 추가되었다. 기존 선언문이 의학연구에서 사생활과 비밀보호를 연구자에게 요구하고 있었음에도 개인 식별이 가능한 인체유래물과 자료를 이용한 연구에 한정하여 충분한 설명에 의한 동의가 필요하다는 점을 강조한 것은 현재 빠르게 증가하고 있는 대규모 코호트연구에서 수집하고 있는 생체시료에 대한 적절한 관리문제와 보건의료기관에 축적되고 있는 대용량 자료를 활용한 연구가 가까운 미래에 폭발적으로 늘어갈 것을 고려할 때 시급히 대응방안을 마련하여야 한다는 점에서 시의적절한 조치임을 알 수 있다.

모든 의학연구가 연구대상자들에게 충분한 설명을 한 후 자유의지에 의한 동의를 받은 후에 수행할 수 있는 것은 아니다. 지역사회 또는 국가 구성원 전체를 대상으로 하지 않으면 그 의미가 축소되거나 연구결과의 비뚤림이 발생할 수 있는 단면조사연구, 특정 노출과 질병발생 사이의 인과관계를 파악하기 위하여 장기간 지속되는 추적조사연구, 드물게 발생하여 탐색과 인과성 평가가 매우 어려운 약물의 부작용에 대한 연구 등은 연구의 성격상 연구대상자 전체로부터 설명 후 동의를 구하는 것은 현실적으로 불가능하다. 이에 개정 헬싱키선언에서는 연구에서 동의를 획득하는 것이 불가능하거나 비현실적인 상황, 또는 동의를 구하는 것이 연구의 타당성을 위협하는 상황에서는 연구윤리심의위원회(Institutional Review Board, IRB)가 검토하여 승인한 후에만 연구를 수행할 수 있도록 규정하고 있다. 하지만, 연구윤리심의위원회가 내리는 판단은 연구윤리지침에 근거한 연구기관의 판단으로 법률적 책임을 면할 수는 없다. 연구윤리심의위원회의 승인을 득한 후에 수행되는 연구라 하여도 개인정보보호법에 비추어 불법적인 요소가 있다면 이는 처벌조항에 따른 조치가 불가피하여 결국 연구자와 연구기관은 보호받지 못하며 연구수행은 중단될 수 밖에 없게 된다. 정보주체의 동의를 구하

여 수행되는 대부분의 전향적 연구에 있어서는 기존 자료와 연계를 통한 분석을 수행하여도 개인정보보호법 제 18조에 제시된 정보이용과 제공의 금지 예외가 되어 법적으로 큰 문제가 없으나, 대규모 전산자료를 이용한 대부분의 후향적 관찰연구들은 통계작성 및 학술연구를 목적으로 특정 개인을 알아볼 수 없는 형태로 익명화 처리하여 제공되는 경우를 제외하고는 원칙적으로 자료제공을 금지하고 있다. 일견 연구가 가능할 것으로 생각될 수도 있지만, 개인을 알아볼 수 없는 형태로 익명화된 자료로 수행할 수 있는 연구는 매우 제한적이며, 개인식별이 연구수행을 위하여 필수적인 요소라면 이러한 개인정보보호법이 적용되는 여건에서는 합법적으로 연구를 수행하는 것은 불가능하다는 것을 의미한다. 미국에서는 우리의 개인정보보호법과 유사한 영향력을 지닌 '건강보험 이전과 책임에 관한 법률(Health Insurance Portability and Accountability Act ; 이하 HIPAA법)' 때문에 장기간에 걸친 추적관찰 연구와 대규모 전산자료를 활용한 연구에 장애가 발생하는 사례가 보고되고 있다(2, 3). 국내에서는 이와 같은 사례가 보고되는 경우는 매우 드물었지만, 의학연구자들 사이에서는 이와 관련된 우려가 크다. 왜냐하면 이러한 연구들이 우리나라 국민들의 건강증진 및 질병발생과 관련된 요인들을 가장 효율적으로 파악해내는 방법이고 동시에 사회 전체의 이익과 직결되는 정책적 결정을 내리는데 필요한 과학적 근거를 제공할 수 있음에도 불구하고 개인정보보호법 때문에 연구수행 자체가 제한을 받을 수 있기 때문이다. 이에 국내외에서 출판된 개인정보보호법이 의학연구에 미친 영향과 관련된 문헌을 검토하고 고찰하여 바람직한 대응방안을 모색하는 것은 대단히 의미있는 일이다.

## Ⅱ. HIPAA법이 의학 및 보건학 연구에 미치는 영향

미국의 HIPAA법은 의료보험 시장에서 진료기록의 이전과 지속성을 개선하여 낭비와 사기, 오남용을 방지하는 것을 목적으로 제정되었다. 이 법의 신설로 인하여 자료의 이전에 따르는 보안의 유지와 사생활 보호를 구체화하는 규칙의 제정이 필요해졌고, 이러한 규칙은 미국 의회가 건강자료의 프라이버시 보호에 관한 추가적인 법안을 제정하거나, 미보건성이 제정할 수 있었다. 당시 의회가 연구에 대한 법안들을 통과시키는데 실패함에 따라 미보건성이 프라이버시 룰(Privacy Rule; Standard for Privacy of Individually Identifiable Health Information)을 제정하여 2003년부터 발효시켰다. 이 규정은 사생활보호를 강화하여 진료자료 활용을 제한하고, 자료주체가 진료 이외의 상황에서 자신에 관한 정보의 활용여부를 결정할 수 있는 권리를 보장한다. 프라이버시 룰은 익명화된 자료는 자유롭게 공개되고 사용될 수 있도록 규정하고 있다. 프라이버시 룰이 정의하는 '익명화'는 개인식별의 가능성이 있는 18개 항목을 제거한다는 뜻으로, 여기에는 이름, 주소, 날짜, 전화번호, 팩스번호, 이메일, 사회보장번호, 의무기록번호, 계좌번호, 보험등록번호, 면허증번호, 자동차등록번호, 장치식별자 및 일련번호, 웹의 URL, 인터넷 접속 IP, 지문 성문 등의 생물학적 식별자, 얼굴사진, 기타 고유 식별번호가 속한다. 연구에 자료를 활용하기 위해서는 이들 모두를 제거하거나 이들 중 일부를 유지하면서 통계적 보완책을 사용하여 개인식별을 할 수 없도록 만들어야 한다. HIPAA법의 시행은 연구자들의 연구수행에 지대한 영향을 미쳤는데, 미국 내 여러 역학연구기관은 그 영향의 크기를 파악하기 위하여 내부 연구자 및 전문가들을 대상으로 설문조사를 수행하였다〔표1〕.

표 1. 설문조사 결과 요약

| 연구 수행 기관 | 년도 | 설문 참여자 | 설문 참여율[1] |
|---|---|---|---|
| Association of American Medical College (AAMC) | 2003 | 연구자, 연구책임자, Institutional review board (IRB) 직원, 공무원 | 331명[2] |
| National Cancer Advisory Board (NCAB) | 2003 | 암센터장, 임상협력그룹의 장, 연구프로그램의 대표연구자에 의해 추천된 구성원 | 39% (89/226) |
| Agency for Healthcare Research and Quality (AHRQ) | 2004 | 16명의 보건서비스 연구자, 17명의 IRB 센터장, 연구감사책임자 | 77% (33/43) |
| National Survey of Epidemiologists | 2007 | 13개 역학분야 단체의 전문가 | 1,527명[3] |
| HMO Research Network (HMORN): survey of investigators | 2008 | 15개 HMORN 연구센터의 과학자 | 43% (89/235) |
| HMORN: survey of IRB administrators | 2008 | 15개 HMORN 연구센터의 IRB 센터장 | 73% (11/15) |
| AcademyHealth | 2007 | AcademyHealth 의 전문가 | 396명[4] |
| American Heart Association/American College of Cardiology (AHA/ACC) | 2007 | American Heart Association 과 American College of Cardiology 의 전문가 | 656명[5] |
| North American Association of Central Cancer Registries | 2006 | The North American Association of Central Cancer Registries 의 구성원 | 66% (47/77) |
| American Society for Clinical Oncology (ASCO) | 2008 | 13개 기관의 감사 종사자 27명 | 27명 |
| Association of Academic Health Centers (AAHC) | 2007 | 5개 기관의 연구자 및 감사책임자 | 5개 기관 |
| 모든 설문 참여자 총 수 | | | 3,211명 |

1. 설문 참여율은 자료의 접근이 가능한 경우 설문을 보낸 총 수를 대답을 한 수로 나누어 제시함.
2. 설문을 보낸 총 수가 몇 명인지 제시되지 않음.
3. 역학분야 단체에서 10,347개의 e-mail 주소로 설문을 전송하였으나, 한 역학자가 여러 단체에 소속된 경우가 있어 정확한 응답률을 계산할 수 없음.
4. 총 3,461명의 AcademyHealth 구성원에게 설문이 발송되었으나 선임연구원의 응답만을 분석하여 정확한 분석자 수를 알 수 없음.
5. 총 18,261명의 American Heart Association과 American College of Cardiology 구성원에게 설문조사를 수행하였으나 그 중 다수는 연구자가 아닌 임상만을 수행하는 경우로 그런 경

우를 제외한 후의 정확한 분석대상자 수를 알 수 없음.

## 1. 미국의과대학협의회(Association of American Medical Colleges, AAMC) 조사

미국의과대학협의회(AAMC)는 2003년 HIPAA 법에 의한 프라이버시 룰이 제정된 후 연구기관, IRB 직원, 및 공무원들을 대상으로 프라이버시 룰에 의한 연구환경의 변화에 대한 설문조사를 시행하였고, 그 결과에 따라 331명의 응답 내용을 바탕으로 연구 기능의 변화에 대한 자료를 만들었다.

자료를 분석한 후, AAMC는 프라이버시 룰은 임상진료, 건강서비스, 역학, 의학, 보건경제학적으로 보건관련 연구의 수행에 다양한 종류의 영향을 미쳤다는 결론을 내렸다. 보고서에 의하면 프라이버시 룰에 의한 가장 보편적인 변화는 환자모집의 어려움, 선택비뚤림 발생가능성 증가, 더 많은 서류작업의 필요, 복잡해진 IRB 승인절차에 따른 연구비용의 증가, 연구대상자의 개인식별자 제거에 따른 연구오류의 증가, 기관별 IRB의 프라이버시 룰에 대한 해석 차이에 의한 다기관연구 수행의 어려움, 연구수행에 관련된 규칙의 증가로 인한 연구자의 연구수행 포기사례 증가 등이 있었다(4).

## 2. 국가암자문위원회(National Cancer Advisory Board, NCAB) 조사

국가암자문위원회(NCAB)는 2003년 프라이버시 룰과 관련된 보건연구자들의 경험을 설문조사하였다. 설문조사를 위하여 암센터의 이사, 임상연구협력센터의 기관장, Special Programs of Research Excellence의 선임연구자들에게 프라이버시 룰과 관련된 전문가의 명단을 요청하였다. 이를 통하여 총 226명의 전문가를 확인하여 설문조사에 응해줄 것을 오청하였다. 해당 전문가들은 설문 웹사이트를 통해 프라이버시 룰과 관련된 공개의견을 제출하였다. 해당 설문조사는 총 89명(39%)으로부터 의견을 제출받았다.

제출된 의견의 주요 내용은 프라이버시 룰은 이전에 비해 환자들을 더 혼란스럽게 만들었고, 프라이버시 룰이 요구하는 복잡한 서류는 연구의 진행을 지연시켰으며, 각 기관의 프라이버시 룰에 대한 서로 다른 해석은 다기관공동연구를 더욱 어렵게 만들었고, 연구목적을 달성하기 위하여 임상시험 중 수집한 환자의 검체를 사용하는 것을 더욱 어렵게 만들었다 등이었다(5).

## 3. 보건의료연구및질평가원(Agency for Healthcare Research and Quality, AHRQ) 조사

미국 보건의료연구및질평가원(AHRQ)은 2004년에 미국의 모든 지역을 대표하며, 다양한 연구환경을 반영할 수 있는 18개 기관에 근무하고 있는 33명의 선임연구원, IRB 위원장, 연구감사책임자들을 대상으로 면접조사를 수행하였다. 전체 대상자 중 77%가 면접조사에 참여하였는데 그 중 92%가 프라이버시 룰이 보건의료분야 연구에 유의한 영향을 미친다고 답하였다.

여러 보고서에서 다수의 기관에서 많은 환자정보를 수집해야 하는 다기관공동연구에서 나타나는 문제점들을 보고하였다. 많은 연구자들은 여러 연구기관들에 속한 IRB들간 의사결정의 불일치, 개인식별자가 제거된 자료에 대한 접근의 어려움, 연구에 소요되는 비용과 시간의 증가, 자원의 부족으로 인한 소규모 기관들의 연구참여가 어려워짐 등의 문제점들을 호소하였다. 절반 이상의 보고자는 프라이버시 룰에 대한 보수적인 해석과 잘못된 해석에 의해 이러한

문제점이 발생하고 있는 것으로 인식하고 있었다(6).

## 4. 전국 역학자 조사(National Survey of Epidemiologists)

미국 의학한림원(Institute of Medicine, IOM)에서 2004년 피츠버그대학의 Roberta Ness에 의뢰하여, 프라이버시 룰을 제정한 후 사람을 대상으로 하는 의학연구에 대한 IRB 업무에 종사하는 1,527명의 역학자들에게 설문조사를 시행하였다. 설문문항은 5점척도(1점＝없음, 5점＝매우 그러함)로 구성되었다.

84% 이상의 응답자가 '프라이버시 룰을 제정한 후 연구수행이 편리해졌는가?'라는 질문에 1점 혹은 2점으로 대답하였으며, 반대로 68%의 응답자가 '프라이버시 룰은 연구수행을 어렵게 만드는가?'라는 질문에 4점 혹은 5점으로 대답하였다. 또한 11%만이 프라이버시 룰에 의해서 연구에서의 공공의 선이 강화되었다고 응답하였으며, 26%만이 연구참여자의 기밀보호와 개인정보 보호를 향상시켰다고 응답하였다. 또한 설문조사 항목 중 프라이버시 룰의 제정에 따른 연구경험을 작성할 수 있는 항목에서 총 427개의 응답이 보고되었으며, 그 중 90% 이상에서 부정적인 응답을, 5%에서 중립적인 의견을, 5%에서 긍정적인 응답을 서술하였다. 가장 많이 보고된 의견으로는 프라이버시 룰은 개인정보보호와 관계없는 환자의 부담을 증가시킨다, 프라이버시 룰의 해석에 대한 기관 간의 차이가 크게 나타난다, 다수의 정부기관에서 프라이버시 룰에서 예외가 인정되는 공중보건조사와 의학연구의 경계에 대한 혼동을 보인다, 프라이버시 룰에 의해 연구가 지연됨에 따라 연구비용이 추가로 소요되며, 연구참여자를 모집하기가 더욱 어려워졌다 등을 보고하였다(7).

## 5. HMO Research Network Survey

IOM 위원회는 프라이버시 룰 하에서 HMO 연구네트워크(HMORN)의 연구자료 수집 노력 및 IRB 위원의 경험에 대하여 2008년 조사를 의뢰하였다. HMORN는 15개 연구센터에서 일하고 있는 250명 이상의 과학자로 구성된 컨소시엄이다. 자료수집은 암연구네트워크의 웹 기반 설문조사로 수행되었고, 설문조사에서 프라이버시 룰에 의해 영향을 받았다고 보고한 조사자들은 추가로 전화면접조사가 이루어졌다. 그리고 15개 HMORN 사이트의 IRB 관리자에게는 메일 설문조사를 추가로 실시하였다. 235명을 설문조사에 참여하도록 초대하였으나, 그 중 89 명이 응답하여 조사의 응답율은 43% 였다. 응답자들은 대부분 박사급이었고, 그 중 72 %는 10 년 이상의 연구경력이 있었다. 12명의 응답자가 전화면접조사를 완료하였고, IRB 관리자의 설문조사에 대한 참여율은 73%였다.

응답자들은 프라이버시 룰의 실시 이후 연구수행에 필요한 시간의 증가를 포함하여, IRB 승인의 문제점, 다기관공동연구 수행의 장애, 연구승인과정에서의 혼란, 그리고 익명화 데이터 사용의 문제 등 수많은 어려움을 보고하였다. 응답조사자 중 74 %가 연구하는데 프라이버시 룰에 의해 영향을 받았다고 보고하였는데 이 중 61%가 연구에 한 번 이상 영향을 받았다고 보고하였다. 또한, 조사자의 60%가 프라이버시 룰의 요구에 따라 연구를 수행하는데 어려움이 있음을 보고했다. 한편, 조사자의 59 %가 프라이버시 룰은 환자 개인정보보호를 강화했다고 보고했다.

IRB관리자는 프라이버시 룰에 관하여 연구자 응답자들보다 더 긍정적이었다. IRB관리자의 90%는 프라이버시 룰은 환자 개인정보보호를 강화했다고 보고했다. 또한, IRB관리자 46%가 규정 내에서 일하기가 쉬웠다고 말한 반면, IRB 관리자의 36%는 규정 내에서 일하기가

쉽지 않았다고 답했다. 그럼에도 불구하고, IRB관리자의 63 %는 프라이버시 룰은 연구 수행을 더 어렵게 만든다고 보고했다. IRB관리자의 72% 이상이 연방정부가 IRB에 프라이버시 룰을 해석하고 구현하는 방법에 대한 더 많은 지침을 제공할 필요가 있다고 보고하였다(8).

## 6. AcademyHealth Survey

IOM으로부터 연구를 의뢰받아 AcademyHealth는 프라이버시 룰에 따라 연구를 수행한 경험에 대하여 연구자들에게 2007년 설문조사를 실시하였다. AcademyHealth는 건강서비스 연구 및 보건 정책분석가들을 위한 전문가집단이다. AcademyHealth의 사명은 연구인프라의 강화, 활용 가능한 연구적용 홍보, 주요 건강문제 해결을 위한 보건정책 수립 및 실행을 지원하는 것이다. AcademyHealth는 주요 연구자에게 웹 기반 설문조사를 실시하였다. 총 3,461명 회원이 전자우편으로 설문조사에 참여하도록 초대되었고, 이 중 696명(20.1%)이 응답했다. 이 중 396명(59.6%) 회원은 책임연구자들로서 설문조사 분석의 포함기준에 적합하였다.

응답자의 75%가 프라이버시 룰에 대한 경험이 부정적이었다고 보고하였고 불과 6%만이 긍정적인 경험이라고 보고하였다. 거의 절반인 48%의 기관이 HIPPA 준수 및 IRB 문제에 대해서 연구자에게 지원을 제공하고 있었고, 이 기관의 연구자 중 77 %가 이러한 지원을 활용하는 것으로 나타났다. 프라이버시 룰이 개별 개인정보보호와 연구수행을 가능하게 하는 것 사이에서 올바른 균형을 유지하고 있는 지에 대한 질문에 대하여 63% 응답자들은 연구수행보다는 개인정보보호에 치중되어 있다고 응답하였고, 28%는 올바른 균형을 유지한다고 응답하였으며, 단 1 %가 개인정보보호 보다 연구수행에 치중되어 있다고 응답하였다(9).

## 7. 미국심장협회(American Heart Association, AHA)/ 미국심장학회(American College of Cardiology, ACC) 조사

미국심장협회(The American Heart Association, AHA))와 미국심장학회(the American College of Cardiology, ACC)도 2007년에 설문조사를 실시하였다. AHA와 ACC에 속한 18,261명의 전문회원은 전자우편으로 설문지를 작성하도록 초대되었고, 656명의 회원이 설문조사에 참여하였다. 그러나 AHA와 ACC의 많은 전문가회원은 연구자가 아닌 병원에서 일하고 있는 임상의사로서 설문조사의 잠재적인 대상은 아니었다는 점을 참고해야 한다.

설문조사를 완료한 61%는 프라이버시 룰이 시행된 후 IRB에 연구계획서를 제출하였다고 보고했다. 프라이버시 룰은 연구수행에 부정적인 영향을 주었고 환자의 개인정보보호를 향상시키지 않았다고 응답자는 대답했다. 응답자의 22%만이 프라이버시 룰이 연구결과에 대한 대중의 신뢰를 증가시켰다고 응답하였고, 44%는 기밀유지가 더 잘되었다고 보고하였다. 9%가 개인정보보호를 위반하는 사례가 감소하였다고 보고하였고, 14%는 프라이버시 룰 이전보다 환자의 개인정보보호가 더 잘 되고 있다고 응답했다. 많은 응답자들은 프라이버시 룰이 연구대상자의 모집, IRB 승인과정, 연구비용 및 연구수행시간, 다기관공동연구 및 개인정보비공개처리정보 사용에 부정적인 영향이 있다고 지적하였다(10).

## 8. 북미중앙암등록협회(North American Association of Central Cancer Registries, NAACCR) 조사

2006 년 북미 중앙암등록협회 (NAACCR)는 프라이버시 룰과 관련하여 회원들의 경험에 대한 설문 조사를 실시하였다. NAACCR 회원은 캐나다, 미국 북부 지역의 암등록을 수행하고, 공공연구 목적을 위하여 암등록자료를 제공한다. NAACCR의 모든 71개 회원이 설문 조사에 참여하도록 초대되었고 55개 회원의 응답을 받았다. 그러나, 회원의 대부분은 HIPAA 법률이 적용되는 대상 기관이 아니었다. 응답자들은 프라이버시 룰이 기본적인 암 발생감시 및 암등록사업 기반의 연구 모두를 방해했다고 지적했다(11).

## 9. 미국임상종양학회(American Society of Clinical Oncology, ASCO) 조사

미국임상종양학회(ASCO)는 2008년 초에 구조화된 인터뷰를 통해 질적 정보를 수집하였다. 27명의 기관연구윤리심의위원회의 순응도평가위원들과 13개 기관 연구자들로부터 프라이버시 룰에 대한 견해를 수집하였다. 참가자들은 인터뷰에 앞서 암 생존자의 가족들과 소통하여 '가족 암 증후군' 조사에 대한 유전자연구 참여에 대한 동의를 구하는 것, 민감정보를 포함한 조직은행과 자료은행 구축연구, 장기 생존연구에 참여하기 위한 암 생존자 추적조사에 대한 설명 후 연구참여에 대한 동의를 획득하는 3가지 연구 시나리오를 제시받았다.

이런 시나리오들은 개인정보보호법이 다양한 연구기관들에서 어떻게 해석되는 지를 확인하고 기관연구윤리심의위원회의 순응도평가위원들과 연구자들이 개인정보보호법을 해석하는데 어떤 차이를 보이는지 확인하기 위한 방편으로 개발되었다. 다른 설문조사와는 다르게 ASCO의 다수 면접조사 참여자들은 프라이버시 룰이 민감정보가 연구에서 어떻게 다루어져야 하는지에 대한 재고를 촉진함으로써 개인정보보호에 긍정적인 영향을 준다고 답하였다. 하지만 기관연구윤리심의위원회가 개인정보보호법 준수에 대하여 매우 엄격한 견해를 취하고 있어 중요한 연구를 지연시킬 수 있다는 지적도 있었다. 면접조사 대상자들은 프라이버시 룰을 준수하는 것이 연구승인과정에 중요한 과제임을 지적하였다. 특히 생체시료와 데이터베이스에 의존하는 미래의 연구에 있어서 그 중요성은 더욱 두드러졌다. 개인정보보호법에 대한 교육 부족과 유용한 지침서의 부재, 연구 데이터베이스의 보안에 대한 우려 등이 또 다른 문제로 지적되었다(12).

## 10. Association of Academic Health Centers Focus Groups

Association of Academic Health Centers Focus Groups (AHCC)는 2007년 가을에 5개의 기관에서 HIPAA법 하에서 연구자들의 경험을 조사하였다. 각각의 포커스그룹은 연구자와 기관으로부터 연구윤리심의위원회의 순응도평가위원들을 포함하였고 동일한 내용의 질문지 셋으로 질문하였다. 포커스그룹은 HIPAA법의 적용으로 인하여 개인정보보호가 필요 이상으로 강조되어 연구참가자들을 모으기 힘들며 저장된 조직과 유전자 데이터에 접근하는데 장애가 되고, 연구의 시간과 비용을 증가시키고, IRB 심의절차의 복잡성을 증가시킨다는 문제점을 지적하였다. 참가자들은 어떤 병원과 지역 의사들은 개인정보보호법을 준수하지 않고 독자적인 연구를 진행하기도 한다는 것을 지적하였다(13).

## Ⅲ. 개인정보보호법이 국내 의학 및 보건학 연구에 미치는 영향과 이에 대한 대응

지금까지의 연구결과를 요약하면 개인정보보호 강화라는 긍정적인 영향이 없는 것은 아니지만 HIPAA법에 의하여 연구의 시작에서 종료까지의 시간과 비용이 증가하였고, 기관 간의 자료연계를 어렵게 만들고 있다는 문제점이 공통적으로 지적되고 있다. 또한 연구대상자를 확보하기가 더 힘들어졌으며, 선택비뚤림이 발생할 위험이 커졌고, 기관연구윤리심의위원회, 연구자, 및 연구대상자가 피험자의 권익보호에 대해 혼란을 느끼는 일이 더 많아졌다. 환자의 개인식별자 제거로 인하여 연구자가 효과적으로 자료를 수집하는 것이 어려워졌으며, 임상시험 수행 과정에 모은 환자의 검체를 연구에 사용하기도 어려워졌다. 결과적으로 이러한 어려움들로 인하여 연구자들이 연구를 포기하게 만든 경우도 많았다. 우리나라의 경우 연구자들을 대상으로 개인정보보호법이 연구에 미친 영향을 직접 조사한 결과가 부재하나 국외에서 조사된 상황과 크게 다르지 않을 것으로 추정되며, 익명화 후에만 제공될 수 있는 공공자료의 특성으로 인하여 자료간의 연계를 통한 분석은 현실적으로 불가능하여 많은 연구자들이 포기하고 있는 상태이다.

미국의 경우 HIPAA법의 세부항목으로 의학연구에 사용할 수 있는 자료의 형태를 규정하고 있다. 개인식별자 18개 항목을 제거한 익명화 자료 외에 통계적 방법 등을 적용하여 개인을 식별할 수 없는 형태로 가공된 자료는 연구자가 자료를 단독 사용하거나 다른 자료와 연계하여 분석하더라도 환자의 개인정보 노출위험이 매우 적은 경우에는 사용할 수 있음을 명시하고 있다. 연구참여에 대한 환자동의의 경우에도 예외규정을 제시하여 익명화 자료, IRB가 환자동의에 대한 면제를 승인한 경우, 예비조사 및 사망자의 의료정보 등은 환자의 동의가 없더라도 보건의료정보를 사용할 수 있도록 허용하고 있다. 1988년 컴퓨터연결 및 프라이버시보호법(The Computer Matching and Privacy Protection Act of 1988)을 제정하여 자료연계와 관련된 구체적인 항목 및 이슈들에 대하여 법률적 대책을 마련하였다. 하지만 미국에 비하여 아무런 준비가 되어있지 않은 우리나라의 경우 연구자들이 개인정보보호법의 제정으로 인하여 향후 연구수행에 더 큰 어려움을 겪게 될 것으로 우려된다. 개인정보보호법이 특정 개인을 알아볼 수 없는 형태로 익명화 처리한 후에 통계작성 및 학술연구에 활용할 수 있도록 허용하고 있으나(18조 4), 현재까지 익명화 처리에 관한 구체적인 지침이 제시되지 않고 있다. 개인식별정보들을 모두 배제한다면 개인의 사생활에 대한 침해는 거의 없어지겠지만, 역으로 이러한 정보를 모두 배제하였을 때에는 의미있는 의학연구의 수행도 불가능해진다. 하지만, 개인식별자가 있는 상태에서 연구자료로서 완전한 가공을 한 후에 익명화를 시행하게 되면 활용도가 높으면서도 안전한 자료를 만들 수 있다. 국내에서도 지난한 노력으로 의료정보를 국제적 기준에 비추어 문제가 없을 정도로 익명화하여 공개한 사례가 있다(14). 이 연구에서 대부분의 개인식별정보는 배제되었고 날짜정보는 개인의 진료일에 대하여 -90일에서 +90일 사이의 난수를 발생시켜 더하여 줌으로써 개인의 진료 및 입원일을 알 수 없게 만드는 방법을 적용하였다.

우리나라는 국제적으로 정보기술 선진국으로서 보건의료정보의 전산화를 빠른 시간 안에 이루어냈다. 개별 병원의 의무기록뿐만 아니라 건강보험심사평가원 청구자료, 통계청 생정통계자료, 국립암센터의 중앙암등록자료 등 건강관련 데이터베이스들이 구축되어 있으며 이를 연계, 활용한 연구를 수행할 수 있는 가능한 자원을 갖추고 있다. 하지만, 이러한 자료를 활용하는 연구에 있어서 가장 큰 걸림돌은 제도이다. 건강정보의 적극적 활용은 예기치 않은 정보의

누출과 공개의 위험성이 높아짐을 의미하며 경우에 따라서는 건강정보 유출로 인하여 개인에게 치명적인 사회적, 정신적, 심리적 피해가 발생할 수 있다. 하지만 이를 자료에 대한 접근과 자료사용을 금지하여 원천적으로 예방하는 것만이 국민들을 보호하고 국민들에게 도움을 줄 수 있는 유일하고 옳은 선택인 지에 대하여는 다시 한 번 생각해볼 필요가 있다. 즉 철저하게 개인정보를 보호할 수 있는 시스템을 구축하면서 동시에 보건의료와 관련한 정보를 공익적 목적으로 활용하여 과학적 근거를 생성함으로써 보건의료정책 수립과 의사결정의 근거로 활용하게 되면 국민들에게 더 많은 유익을 제공할 수 있기 때문이다. 이 경우 비록 개인정보를 공익적 연구 목적의 자료사용에 동의하지 않는 국민이라 할지라도 공익적 목적의 연구를 통하여 생성한 과학적 근거를 활용한 보건의료정책의 수립으로 인한 이익의 수혜자가 될 수 있다.

우리나라 보다 개인정보보호제도를 일찍 정비한 미국과 유럽연합에서도 공익적 목적의 연구를 수행하는데 대규모 전산자료를 활용하는 시스템 구축을 적극적으로 추진하고 있다. 미국의 경우 FDA법률 개정안(FDA Amendments Act, FDAAA)이 2007년 제정되었다. FDAAA는 미국내 모든 환자들의 건강정보를 통합한 능동적 약물감시시스템의 구축책임을 FDA에 부여하고, '센티넬이니셔티브(Sentinel initiative)'라는 선제적 약물감시체계 구축프로젝트를 2008년 출범시켰다. 즉, 미국은 HIPPA법을 통한 개인정보보호조치가 여전히 유효한 상황에서 약화사고 예방과 건강의 증진이라는 공공선을 위하여 특별법을 제정하여 공공기관이 보유한 전산자료들의 통합을 위한 제도적 지원책을 마련한 것이다. 이는 미국 오바마대통령이 급증하고 있는 과다한 의료비 지출을 줄이고 의료개혁의 일환으로 추진하기 시작한 사업의 일환이다. 고비용 저효율적인 임상시험을 수행하는 대신에 대규모 전산데이터베이스를 활용한 대규모 관찰연구의 활발한 수행으로 동일한 질병에 대한 여러 치료법 간 안전성과 유효성 및 경제성을 평가하는 비교효과연구(Comparative Effectiveness Research, CER)를 활발히 수행함으로써 저비용 고효율적인 근거생성을 추진하도록 정부에서 적극 지원하기 시작한 것이다. 한편, 유럽연합도 회원국들의 건강데이터베이스를 통합한 능동적 약물감시시스템인 엔셉(European Network of Centres for Pharmacoepidemiology and Pharmacovigilance, ENCePP)을 2006년에 구성하였다. ENCePP은 27개 회원국의 89개 연구기관이 참여하는 범유럽연구네트워크로서 13개의 대규모 전산자료를 통합하는 프로젝트로 유럽연합이 각 회원국의 법률을 고려하여 해당 ENCePP 구현에 필요한 법률조항을 개발하여 각 회원국에 전달한 후 이를 각국의 여건에 맞도록 적절히 국내법에 반영한 후 ENCePP에 참여할 수 있도록 조치하였다. 하지만 미국과 유럽연합의 각국의 자료는 표준화 및 전산화 정도가 낮고 대표성도 결여되어 있어 우리나라의 자료에 비하여 많은 한계점을 가지고 있다. 정작 더 질 좋은 자료를 보유하고 있는 우리나라에서는 개인정보보호법으로 인해 대규모 전산자료를 활용하는 의미있는 의학연구의 수행에 심대한 제한을 받고 있어 현 법령의 제도적 보완이 절실히 필요하다(15).

우리나라는 2013년 2월부터 생명과학, 의과학 분야는 물론 사회과학분야까지 확대하여 인간 대상 연구를 수행하는 모든 기관에 IRB 설치를 의무화함으로써 연구의 윤리적 기준이 국제기준에 부합될 정도로 높아질 것으로 기대하고 있다. 1995년 이후 의료기관에서 운영하고 있는 IRB의 역할은 윤리성 및 과학성을 근거로 연구의 타당성과 적합성을 평가 심의하여 궁극적으로 연구대상자의 안전을 보장하고 권익과 개인정보를 보호하고자 하는 것이며 이와 같은 역할을 수행하는 IRB 위원회의 구성기준에 해당 기관과 관련이 없는 외부위원을 반드시 포함하는 등 공정성 측면에서도 역할을 공고히 하고 있다. 미국에서는 개인별 동의서를 받을 수 없는 대규모자료를 연계한 연구의 경우 IRB를 통해 연구의 과학적, 윤리적 타당성을 심의

하고, 공익적 목적 여부 및 연구의 이득과 위해의 균형을 평가하고 있다. 국내 연구기관의 IRB 확대 설치 및 역할강화를 지원하기 위하여 2012년 4월 국가생명윤리정책연구원이 출범하였다. 국가생명윤리정책연구원은 개인정보보호법과 정보공개법 및 생명윤리법의 차이점과 합의점을 파악하여 대규모 전산자료를 연계하는 공익적 목적의 의학 및 보건학 연구수행의 활성화를 위한 방안을 강구하여야 한다. 의학과 보건학 연구만을 심의하는 독립기관으로서 공동 IRB의 구성 및 도입에 관해 논의하여 합의점을 도출하여야 하고, 이러한 IRB의 업무수행에 대한 감시 기능에 대한 의견을 수렴할 필요성이 있다. 이를 바탕으로 공익적 목적의 의학연구에 대한 사회적 정의 및 범위를 명시하고 실현가능한 조항을 제시할 뿐 아니라 공익적 목적의 연구에 대한 IRB의 공정한 심의를 위하여 필요한 규정 및 지침서 등을 개발하여 제공할 것을 제안한다.

축적된 개인건강정보를 부정하게 사용하면 사회적으로 혼란을 야기할 수도 있고 심지어는 개인을 추적하여 피해를 줄 수도 있으나, 우리나라의 경우 축적된 개인건강정보를 사회적으로 유익하도록 활용할 수 있는 시스템을 갖추고 있다. 개인정보보호 강화를 위하여 위축된 대규모 전산자료의 활용을 촉진할 수 있는 적극적 제도적 개선을 통하여 빅데이터를 활용한 과학적 근거창출을 활성화하여 이를 근거로 보건의료정책 수립과 의사결정 수준을 선진화하여 국민 건강증진에 기여할 수 있도록 만들어야 한다.

# 참고문헌


Schmidt H, Mehring S, McMillan J. Interpreting the declaration of Helsinki (2008): "must", "should" and different kinds of obligation. Med Law 2010;29(4):565-91.

Kaiser J. Patient records. Privacy rule creates bottleneck for U.S. biomedical researchers. Science 2004;305(5681):168-9.

Kaiser J. Patient privacy. Rule to protect records may doom long-term heart study. Science 2006;311(5767):1547-8.

NCVHS. National Committee on Vital and Health Statistics, Subcommittee on Privacy and Confidentiality. Susan Ehringhaus's testimony on behalf of the Association of American Medical CollegesColleges; 2003.

Ramirez AG, J. E. Niederhuber. Letter to the Honorable Tommy G. Thompson, Secretary of the Department of Health and Human Services.; 2003.

Walker DK. Impact of the HIPAA Privacy Rule on health services research. In. Philadelphia, PA: Abt Associates, Inc.; 2005.

Ness RB. Influence of the HIPAA Privacy Rule on health research. JAMA 2007;298(18):2164-70.

Greene SM, S. Bennett, B. Kirlin, K. R. Oliver, R. Pardee, E. Wagner. Impact of the HIPAA Privacy Rule in the HMO Research Network. In. Seattle, WA: Group Health Cooperative Center for Health Studies; 2008.

Helms D. PowerPoint presentation to the Institute of Medicine Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule, on the Academy Health survey results.; 2008.

Ring J. PowerPoint presentation to the Institute of Medicine Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule, on the American Heart Association survey results; 2007.

Deapen D. Negative impact of HIPAA on population-based cancer registry research: A brief survey. . Springfield, IL; 2006.

ASCO. The impact of the Privacy Rule on cancer research: Variations in attitudes and application of regulatory standards. Alexandria, VA.; 2008.

AAHC. HIPAA creating barriers to research and discovery: HIPAA problems widespread and unresolved since 2003. In: Association of Academic Health Centers; 2008.

Park MY, Yoon D, Choi NK, Lee J, Lee K, Lim HS, et al. Construction of an Open-Access QT Database for Detecting the Proarrhythmia Potential of Marketed Drugs: ECG-ViEW. Clin Pharmacol Ther 2012;92(3):393-6.

한국보건의료연구원. 공익적 보건의료연구 자료 활용을 위한 Round-table Conference 보고서; 2011.