

개인정보 보호법제의 개선과 이용 활성화

구태연*

1. 들어가는 글

IT 강국이라고 하는 우리나라는 개인정보에 대한 IT 규제 역시 강국이라 해도 과언이 아니다. 1995년부터 보급된 인터넷이 국민의 속성과 맞물려 수많은 인터넷 역기능 현상을 보이자 정부는 2001년 1월 16일 '정보통신망 이용촉진 등에 관한 법률'을 전면 개정(같은 해 7월 1일 시행)해 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(이하 '정보통신망법'이라고 한다)로 바꾸고, 정보통신망에서 개인정보보호와 관련한 규제와 인터넷 명예훼손, 음란물 전송 등 인터넷 역기능에 대한 처벌을 전면 도입했다. 2005년 1월 27일에는 '위치정보의 보호 및 이용에 관한 법률'(이하 '위치정보법'이라고 한다)을 제정해 위치정보사업 허가제 및 위치기반서비스 사업 신고제를 도입하고, 개인의 위치정보를 함부로 수집·이용하는 행위에 대해 처벌을 도입했다(같은 해 7월 27일 시행). 오랜 논의 끝에 2011년 3월 30일에는 개인정보에 관한 기본규제법인 '개인정보보호법'을 제정하고 같은 해 9월 30일 시행하기에 이른다.

개인정보를 보호하는 것은 당연히 바람직한 일이다. 과거 왕조시대,

일제시대, 권위주의 정부 시대를 거쳐 민주주의 정부를 갖게 된 지 불과 20여 년이 되지 않은 우리 사회에는 아직도 정부에 의한 민간사찰 의혹 사건이 남아 있으며¹⁾, 민간 서비스에 의한 과도한 정보수집이 소위 '빅 데이터(Big Data)'²⁾ 처리기술에 의해 개인의 프라이버시를 과도하게 침해하지 않을까라는 우려가 점점 커지고 있다.

다만, 우리나라는 2001년 정보통신망법의 전면 개정과 2005년 위치정보법의 제정, 그리고 2011년 개인정보보호법의 제정을 통해 개인정보의 보호에 있어서는 세계 최고 수준의 규제 법체계를 갖고 있어 오히려 개인들이 갖는 개인정보자기결정권의 과도한 행사가 우려되는 상황이다. 이는 필연적으로 경제활동의 자유, 표현과 창작의 자유 등 헌법상 다른 기본권과 가치들에 대한 우월적 지배 현상으로 연결되어 기본권 간 가치 충돌 현상이 빈번해질 것으로 예상되며, 개인정보자기결정권과 다른 헌법적 가치들의 합리적 해석과 조화가 안정화될 때까지 이러한 혼란은 피하기 어려울 것이다.

세계적인 온라인서비스업체인 구글, 애플, 페이스북, 트위터가 개인정보보호법제가 가장 완비되어 있지 않은 미국의 기업들이라는 것은 필자가 보기에는 우연이 아니다. 초국가적인 산업진흥정책과 막강한 기업 육성펀드들의 활약도 크겠지만, 이들 서비스업체들의 활동을 가로막는 일체의 규제를 과감하게 면제해 주는 법정책도 그들의 성장에 소리 없는 기여를 한 것이다. 하물며 우리는 온라인을 넘어 생활의 모든 면에서 개인정보의 동의 없는 이용을 처벌하는 법까지 도입했다. 국민들이 개인정보보호법의 위력에 익숙해진 순간, 기업 마케팅의 전면적 위축은 불을 보듯 뻔한 상황이며, 이는 생산원가의 증가로 이어져 우리나라 기업들의 경쟁력 약화로 연결될 것이다.

이 글에서는 현행 개인정보보호 법제가 갖는 개인정보보호의 문제점

* 변호사, 법률사무소 형법이루

과 그 해결방안을 살펴보고, 개인정보 이용의 합리적 조정과 활성화를 통한 기업 경쟁력의 강화 방안을 생각해 보고자 한다.

2. 우리나라 개인정보 보호법제 개관

개관

2001년 정보통신망법 전면 개정 이후 우리나라의 개인정보보호는 정보통신망법이 일익을 담당해 왔다. 그러나 영리 목적의 정보통신서비스 제공자가 다루는 개인정보 중심으로만 규율되는 한계가 있어 그 밖의 영역을 다루기 위해 2011년 3월 30일 개인정보보호법이 제정·공포되었다. 그 밖에 위치정보법 등도 개인정보 보호법제의 근간을 이루고 있다.

개인정보보호법

개인정보보호법은 업무를 목적으로 개인정보파일을 운용하기 위해 스스로 또는 다른 사람을 통해 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등에게 적용되는 법이다. 개인정보 파일이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다. 종래 정보통신망법이 공공기관 등 비영리적 목적의 이용에 적용되지 않는 점을 보완하기 위해 도입되었다.

정보통신망법

정보통신서비스제공자가 개인정보를 수집·이용할 때는 정보통신망법이 적용된다. 정보통신망법은 온라인에 있어 영리 목적의 개인정보 수

집·이용 행위에 대한 기본 규제법이다. IT 기술의 발달로 기업서비스가 점점 정보통신서비스로 변화하거나 정보통신서비스를 위주로 하는 기업의 비중이 높아지고 있어 정보통신망법의 적용 영역은 지속적으로 증가해 왔다. 개인정보보호법이 제정되었음에도 대부분 개인정보보호의 문제는 대규모 고객정보를 보유하고 있는 인터넷기업에서 발생하고 있는 원인도 그 때문이다.

위치정보법

2005년 위치정보법이 제정되었을 때는 소위 아이폰을 필두로 한 스마트폰이 도입되기 이전이었다. 무선통신망을 갖고 있는 이동통신사(위치정보사업자)들이 사람이나 물건의 위치정보를 수집해 제공하면, 위치정보를 기반으로 서비스를 제공하는 사업자(위치기반서비스사업자)들이 고객들에게 사람이나 물건의 위치정보를 제공하는 것이 위치정보법의 규제 모델이다. 그러나 2007년 미국에서 아이폰이 발표되고 2009년 11월 우리나라에 아이폰이 도입되어 대부분의 사람들이 스마트폰을 사용하고 스마트폰 애플리케이션을 사용하게 되자 위치정보를 이용하는 스마트폰 애플리케이션들의 위치정보법 위반 문제가 대두되었다. 스마트폰의 애플리케이션이 위치정보를 이용하는 모델은 위치정보사업자와 위치기반서비스사업자의 모델과 중복되기 때문에 이 법률은 변화된 상황에 맞추어 개정 필요성이 높게 제기되고 있다.

3. 우리나라 개인정보 보호법제의 주요 문제점

광범위한 개인정보의 정의

우리 개인정보 보호법제의 가장 큰 문제점은 개인정보의 정의가 광범

위하다는 데 있다. 정보통신망법은 ‘개인정보’란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의해 특정할 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합해 알아볼 수 있는 경우에는 그 정보를 포함한 다)를 말한다고 정의하고 있다.(제2조 제1항 제6호) 개인정보보호법도 ‘개인 정보’란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통해 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합해 알아볼 수 있는 것을 포함한다)를 말한다고 정의해 동일하게 정의하고 있다.(제2조 제1호)

이러한 법률들의 개인정보에 대한 정의를 잘 살펴보면 개인의 식별성을 기준으로 개인정보를 정의하고 있음을 알 수 있다. 다만, 그 자체로 개인을 식별할 수 있는 정보만 개인정보로 정의하지 않고 아직 개인을 식별할 수 있지 않더라도 나중에 다른 정보와 결합해 개인을 식별할 수 있는 정보 역시 개인정보로 정의하고 있다. 필자는 그 자체로 개인을 식별할 수 있는 정보를 진정 개인정보라고 부르고, 그 자체로는 개인을 식별할 수 없으나 다른 정보와 결합해 개인을 식별할 수 있는 정보를 비진정 개인정보라고 부른다.

개인정보의 정의는 개인정보 보호법제의 출발점이므로 무척 중요한 의미를 갖는다. 개인정보나 아니냐에 따라 정보통신망법과 개인정보보호법 규제 조항들의 적용을 받을지 여부가 결정되고 그 위반 여부에 따라 과징금·과태료와 같은 행정처분이나 징역형·벌금형과 같은 형사처벌도 받게 된다. 어떠한 정보가 개인정보인지를 판단할 때는 진정 개인정보인지에 대한 판단만으로는 부족하고, 그 정보가 비진정 개인정보인지 여부도 고려해야 한다. 실제로 구체적인 정보를 앞에 두고 이러한 판단을 해 보면 쉽게 판단할 수 없는 경우가 많다.

비진정 개인정보를 문제 삼은 대표적 예로는 휴대전화의 국제 단말기

인증번호(IMEI: International Mobile Equipment Identity)와 범용 가입자 인증 모듈(USIM: Universal Subscriber Identity Module)을 개인정보로 보고 처벌한 사례다.³⁾

과중한 형사처벌 규정

정보통신망법은 정보통신서비스제공자가 개인정보를 수집·이용·제공하려고 할 때는 일정한 사항을 이용자에게 알려주고 그의 동의를 받을 것을 원칙으로 하면서 이러한 알림과 동의를 제대로 확보하지 않은 채 개인정보를 처리하는 정보통신서비스제공자에 대한 형사처벌을 규정하고 있다. 이러한 형사처벌은 5년 이하의 징역에서 1년 이하의 징역 또는 벌금에 이른다. 개인정보를 동의 없이 수집하는 행위도 5년 이하의 징역 또는 5천만원 이하의 벌금형이 규정되어 있다.⁴⁾

이러한 개인정보 오남용에 대한 형사처벌 조항은 법집행의 실효성을 담보하는 데는 아주 효과적이겠지만, 세계 어느 나라에도 유례가 없는 강력한 법제도로써 개인정보보호를 다른 법제도나 기본권보다 우위에 놓는 결과를 초래한다. 실제 인간 생활에서 개인정보의 수수를 목적으로 거래가 이루어지는 경우는 예외적이고⁵⁾, 재화와 용역을 거래하기 위해 이루어진 활동에 개인정보가 부수적으로 거래되는 것이 일반적이기 때문이다.

옴트인 원칙에 의한 마케팅의 위축

‘고지와 동의 원칙’은 일견 정보주체의 개인정보자기결정권을 보장하기 위해서는 불가결한 원칙으로 여겨진다. 이를 ‘원칙(principle)’의 수준에서 정의하고 있을 때는 아무런 문제가 없으나, ‘법규(regulation)’로서 규정해 이를 위반할 때 불법행위로 평가하게 되면 문제가 달라진다. 개인의 선택에 의해 그의 개인정보를 이용할 수 있다는 의미에서 ‘옴트인

(opt-in) 원칙'이라고도 부를 수 있다.

옵트인 원칙은 동의를 얻지 못하면 그의 개인정보를 활용하지 못한다는 것으로 일견 합당한 원칙처럼 보인다. 그러나 기업의 입장에서 보면 자신의 잠재적 고객에게 광고를 전달하기 위해 연락을 취하기가 어렵게 된다. 잠재적 고객의 동의를 받아 연락을 하면 되지 않느냐는 생각을 할 수 있으나, 잠재적 고객에게 광고성 정보의 전달을 위한 개인정보 이용의 동의를 받기 위해 연락을 취하는 행위 자체가 '동의 없는 개인정보의 이용'에 해당하는 불법행위가 되므로 곤란하다. 결국 옵트인 원칙은 기업에는 정상적인 마케팅 활동의 중단으로 연결되는 것이다.

기업이 정상적으로 '동의를 얻은' 고객에게 연락하는 방법은 누군가 사람이 많이 모이는 곳에서 고객들로부터 동의를 받고 개인정보를 수집해 기업에 제공하고 기업은 '동의를 얻은 개인정보'를 이용해 마케팅 활동을 하는 것이다. 따라서 이러한 개인정보 수집·제공기업들이 새롭게 생겨나고 있다.⁶⁾

개인정보보호법에 의한 민사법상 원칙의 변경

한편 재화와 용역의 거래 이면에 있는 개인정보의 수집·이용·제공의 측면을 개인정보보호법이 강력하게 규제하는 결과, 개인정보보호법에 의해 민사법 원칙의 변경이 이루어지고 있는 현상도 발생하고 있다.

예를 들어, 채권양도의 경우 양도인인 채권자가 채무자에 대한 채권을 양수인에게 양도하게 되는데 이때 양도인이 채무자의 개인정보를 양수인에게 제공하게 되는 것이다. 이러한 경우 채무자의 개인정보를 양수인에게 제공할 수 있는 채무자의 동의를 채권자가 미리 획득했느냐의 문제가 발생한다.⁷⁾ 채권자와 채무자 사이에 계약을 체결할 때 후일 있을지 모를 채권양도의 경우를 예상해 미리 개인정보 제공에 관한 동의를 받아두지 않는 경우가 대부분이므로 채권자는 채권양도를 할 때 채무자

의 동의 없이 개인정보를 양수인에게 제공할 수 없게 된다. 채무자의 개인정보가 포함되지 않은 채권양도는 그 중요한 내용을 누락한 채권양도로서 민사상 채권양도의 효력을 인정받을지 의문이다. 결국 채권자는 채권의 양도에 대해 채무자의 동의를 받아야 적절한 채권의 양도를 할 수 있게 되므로, 개인정보보호법에 의해 민법상 채권양도의 원칙(양도성의 원칙)⁸⁾이 변경되는 것이다.⁹⁾

이와 같이 재화와 용역의 거래 이면에 부수적이고 필연적으로 발생하는 관계자의 개인정보 이전을 규율함으로써 거래와 관련된 법률이 변경되는 것은 바람직하지 않다. 개인정보보호법의 예외사유의 해석에 있어 법률조화적인 해석이 중요한 이유가 바로 그 점에 있다.

4. 개인정보보호법과 정보통신망법의 관계

인터넷 서비스는 사실상 대부분 기업이 제공

정보통신망법의 적용 대상자인 정보통신서비스제공자는 '전기통신사업법' 제2조 제8호에 따른 전기통신사업자뿐만 아니라 영리를 목적으로 전기통신사업자의 전기통신역무를 이용해 정보를 제공하거나 정보의 제공을 매개하는 자를 포함한다.¹⁰⁾ 영리를 목적으로 한 기업이 인터넷을 통해 어떤 서비스를 제공하면 정보통신서비스제공자에 해당한다.

인터넷의 발달로 모든 기업이 인터넷을 통해 일정한 서비스를 제공하고 있다. 인터넷을 기업 활동의 본무대로 삼는 인터넷기업뿐 아니고 전통적인 제조업체들도 인터넷 홈페이지를 만들어 고객들을 위해 일정한 서비스를 제공한다. 오프라인 산업의 대표적인 예로 일컬어지는 금융산업이 대표적이다. 우리나라는 전자금융이 발전되어 웬만한 금융거래는 인터넷 금융서비스를 통해 거의 이루어진다. 인터넷 금융서비스는 바로

정보통신서비스다. 결국 인터넷 홈페이지를 갖추고 기업활동을 하면 정보통신망법의 적용 대상이 된다.

정보통신망법과 개인정보보호법의 이중적 적용

영리 기업이 인터넷 홈페이지를 통해 수집한 개인정보는 정보통신망법이 적용되고, 비영리단체의 인터넷 홈페이지를 통해 수집된 개인정보 및 공공기관·법인·단체·개인이 오프라인을 통해 수집한 개인정보는 개인정보보호법이 적용된다. 한편, 정보통신망법이 적용되더라도 개인정보보호법에 특별한 규정이 있으면 그 규정은 추가로 적용된다는 것이 행정안전부의 입장이다.

이렇다 보니, 경제활동의 대부분을 수행하고 있는 영리 기업으로서는 정보통신망법과 개인정보보호법의 이중적 적용상태로 무척 혼란스럽다. 두 법은 유사하면서도 서로 다른 부분이 있고, 용어도 구별되고 있으며¹¹⁾ 무엇보다도 아래에서 기술할 ‘처벌 수준의 차이’로 인한 혼란과 규범력의 저하가 가장 큰 문제다.

처벌 수준의 상이가 가져오는 의외의 인식처

동일한 행위에 대해 정보통신망법은 형사처벌, 개인정보보호법은 과태료로 규정되어 처벌의 차이를 보이는 경우가 많다. 예를 들어, 동의 없는 수집·이용의 경우 정보통신망법은 형사처벌¹²⁾, 개인정보보호법은 과태료¹³⁾로 처벌한다.

인터넷기업이 아닌 대부분의 기업은 오프라인에서 재화와 용역의 공급을 하므로 개인정보 역시 오프라인에서 수집한다. 그와 같은 기업이 인터넷 홈페이지를 열고 오프라인 고객의 등록을 받아 일정한 서비스를 제공하는 경우가 많다. 이러한 경우에 그 고객의 개인정보는 정보통신망법이 적용될 것인지, 개인정보보호법이 적용될 것인지 모호하다. 온라인

으로 수집된 개인정보라는 점을 강조하면 정보통신망법이 적용될 것이고, 오프라인에서 이미 수집된 개인정보를 온라인에서 다시 확인한 것에 불과하다는 입장에 서면 개인정보보호법이 적용될 것이다.

형사처벌의 경우에 해석상 양 법이 모두 적용될 수 있다면 ‘의심스러울 때는 피고인의 이익으로’ 원칙에 의해 가벼운 처벌규정을 적용해야 한다. 정보통신망법의 적용으로 형사처벌을 받아야 할 대부분의 경우에 개인정보보호법의 동일한 내용을 담고 있는 규정을 들어 과태료 사안임을 주장할 경우 어떻게 할 것인가? 동일한 행위에는 동일한 규제를 도입함이 바람직하다. 어느 법을 적용하느냐에 따라 처벌 수준이 상이하다면 가급적 경한 규제를 갖고 있는 법으로 끌림현상이 발생할 것이고, 이는 준법의식의 저하로 연결된다.

5. 이용활성화를 위한 개인정보 보호법제의 개선방향

개인정보 정의의 수정 및 개인정보 생성 개념의 도입

앞에서 말한 진정 개인정보와 비진정 개인정보를 구분하는 견지에 설 때, 비진정 개인정보는 지나치게 넓은 개념으로서 개인정보의 정의에서 삭제하는 것이 바람직하다. 장래에 개인을 식별할 수 있는 상태에 불과한 ‘쪽정보’를 규율하기 위한 개념이 비진정 개인정보다.

이러한 비진정 개인정보 개념은 형사처벌로 이어지므로 죄형법정주의 원칙에 비추어 정당한지 의문이다. 데이터베이스 기술의 발달로 세상의 모든 정보가 특정 개인과 연결될 수 있으므로 자칫 어떤 정보든 수집하면 모두 개인정보라는 식으로 처벌이 확대될 수 있다.

비진정 개인정보는 개인정보의 정의에서 삭제되는 것이 옳다고 본다. 이러한 경우, 기업이 사실 빅 데이터(Big Data)를 수집하고 있는 현실에

서 쉽게 쪽정보들을 결합해 개인정보를 생성할 수 있으므로 개인정보보호에 대해 결정적 흠결이 발생한다는 반론이 있을 수 있다. 이러한 지적도 일리가 있으므로 바로 그러한 쪽정보의 결합을 통해 개인정보를 생성해 내는 행위를 '개인정보의 생성'으로 정의하고, 동의 없이 개인정보를 생성하는 행위는 현행 법상 동의 없는 개인정보의 수집과 동일하게 규율하면 될 것이다.

정보통신망법의 예를 들어 보면, 정보통신망법 제2조 제1항 제6호에서 비진정 개인정보 정의를 삭제해 진정 개인정보만 개인정보로 정의하고, 같은 항 제6의 1호에 "개인정보의 생성이란 해당 정보만으로는 특정 개인을 알아볼 수 없는 정보를 다른 정보와 결합해 특정 개인을 알아볼 수 있게 하는 것을 말한다"라고 신설하고, 정보통신망법 제22조 제3항에 "개인정보의 생성의 경우에도 제1항의 규정을 준용한다"를 신설하고, 정보통신망법 제71조 제1호를 "제22조 제1항(제67조에 따라 준용되는 경우를 포함한다) 및 제3항을 위반해 이용자의 동의를 받지 아니하고 개인정보를 수집하거나 생성한 자"로 개정해야 한다.

법령 간 처벌 수준의 일치화

정보통신망법과 개인정보보호법상 동일한 행위에 대해서는 서로 동일한 행정벌, 형사처벌을 규정할 필요가 있다. 두 법에 적용되는 사실관계가 동전의 양면 내지는 필연적인 관계에 있으므로 처벌 수준의 차이는 법집행상 심각한 문제점을 야기한다.

필자는 우리나라 개인정보 보호법제가 과도하게 형사처벌을 하고 있으므로 개인정보보호법의 규제 수준에 맞추어, 정보통신망법을 개정하는 것이 바람직하다고 생각한다. 즉, 동의 없는 제3자 제공의 경우와 이에 준하는 정도만 형사처벌을 존치하고 나머지 위반행위에 대해서는 과태료로 변경하는 것이다.

개인정보 침해행위 처벌에 피해자의 처분권 허용

개인정보 보호법제의 이론적 출발점이 헌법상 프라이버시권, 행복추구권이라고 본다면 개인정보 침해에 대한 처벌도 개인의 의사를 존중해야 할 것이다. 명예훼손과 같이 개인의 명예감정을 침해하는 범죄, 강간죄와 같이 개인의 성적 자기결정권을 침해하는 범죄도 친고죄 내지 반의사불벌죄로 규정해 개인의 의사에 따라 처벌하고 있다. 개인정보의 정의가 상당히 모호하고 경우에 따라 지나치게 확장될 수 있으며, 모든 인간의 활동에 필연적으로 수반되는 것이 개인정보임을 감안하면 개인의 의사를 묻지 않고 국가가 나서서 개인정보를 처벌하는 것은 국가권력이 지나치게 개인의 사생활 영역에 개입하는 것이다.

필자는 동의 없이 개인정보를 처리하는 행위 중 형사처벌 규정은 반의사불벌죄로 규정하는 것이 바람직하다고 본다. 현행법은 피해자인 정보주체 내지 이용자의 의사를 묻지 않고 위반행위를 처벌하고 있어 가해자가 피해자와 합의에 관심을 기울이지 않는 부작용이 있다.

개인식별력이 적은 행태정보 수집·이용 시 옵트아웃 허용

행태정보(behavioral information)란 개인의 행태에 관한 정보를 말한다. 온라인 서비스 이용자에 대해서는 웹사이트의 어떠한 정보를 이용했는지 웹서버가 파악할 수 있으므로 그가 관심을 기울이는 정보에 대해 기록·수집이 가능하다. 기업들은 이렇게 파악한 행태정보를 이용해 이용자의 관심을 파악하고 이용자에게 맞춤형 광고를 보내는 플랫폼을 구축하고 싶어 한다. 이러한 행태정보를 활용해 광고비로 막대한 돈을 벌고 있는 기업들이 미국의 온라인 서비스 기업들이다. 이에 비해 우리나라 인터넷 기업들은 개인정보 보호법제 때문에 개인의 동의를 얻지 않고서는 이러한 행태정보를 활용한 마케팅을 할 수 없으므로 맞춤형 광고서비스가 활성화되고 있지 않다.

개인정보의 보호에만 치중하면 이와 같은 행태정보도 개인을 식별할 가능성이 있는 비진정 개인정보이거나, 이미 그 자체에 개인을 식별할 수 있는 정보를 포함하고 있는 진정 개인정보이므로 엄격하게 사전 고지와 사전 동의 원칙을 적용하는 것이 바람직하다. 그러나 경제활동의 자유라는 측면을 조화시켜 해석하는 입장에서는 행태정보의 활용의 길을 열어줌으로써 얻는 기업경쟁력의 강화를 고려하지 않을 수 없다. 기업의 경쟁력은 비용의 절감에서도 높일 수 있는데, 행태기반 광고는 마케팅 비용을 절감해 기업의 경쟁력을 높여 준다.

개인식별정보를 갖고 있는 행태정보를 이용함에는 현행법과 같이 사전 동의를 원칙을 준수하도록 하고, 개인식별정보가 포함되지 않은 행태정보는 정보주체 내지 이용자의 반대 의사표시가 없다면 행태정보를 수집해 이용하는 것을 허용하는 방향으로 법을 개정하는 것이 바람직하다.

광고성 정보전송 시 옵트아웃 허용

전기통신을 이용한 광고성 정보의 전송은 현재 정보통신망법 제50조(영리 목적의 광고성 정보전송 제한)가 규율하고 있다. 이 조항은 의무 주체를 정보통신서비스제공자에 국한하지 않고 '누구든지'로 규율함으로써 온라인 사업자뿐만 아니라 오프라인 사업자도 규율대상이다. 한편, 영리 목적의 광고성 정보를 전달하려면 필연적으로 수신자의 연락처 등 개인정보를 이용해야 하므로, 이 조항의 이면에는 개인정보의 동의 없는 이용 이슈가 포함되어 있다. 만약 영리 목적의 광고성 정보를 전달하는 것이 동의 없이 수신자의 개인정보를 수집한 것으로 평가되면 위 조항 소정의 과태료 이외에 동법 제22조 제1항 위반이 되어 동법 제71조 제1호의 형사처벌(5년 이하의 징역 또는 5천만원 이하의 벌금)을 받게 될 것이다. 나아가 개인정보보호법도 개인정보를 이용할 때는 동의나 기타 법률적 근거 등을 요하고 있어 사실상 기업이 개인에게 광고활동을 하기 어렵다.

동의를 받기 위해 연락하는 것도 동의 없는 이용이기 때문이다.

이와 같은 처벌이 다소 지나치다는 점에는 이론이 없을 것이다. 개인 정보는 안전하게 활용되어 기업의 활동을 원활히 해 경제발전에 긍정적 영향을 미치게 할 수 있는 자연자원이다. 기업이 개인정보를 광고성 활동을 위해 이용할 때는 당사자의 명시적인 거부 의사에 반해 이용하지 않도록 하는 규제가 적절할 것이다.

8. 미치는 글

이제 2001년 이후 10여 년에 걸친 노력으로 우리나라는 세계 어느 나라보다도 강력한 개인정보 보호법제를 갖게 되었다. 그러나 실제 현실에서 개인정보 보호와 관련한 법제를 제대로 준수하고 있는지에 대해 살펴보면, 과거보다는 많이 발전한 것은 사실이나 아직도 제대로 법규를 준수하고 있다고 말하기는 어려운 상황이다. 한편, 개인정보 보호법규가 형사처벌을 수반한 강력한 의무규정들을 많이 도입하고 있어 신규 기업에는 상당한 진입장벽으로 작용하고 있다. 정보통신망법상 기술적·관리적 보호조치를 다하기 위해서는 보안시스템 투자를 상당히 해야 하며, 보안인력과 관리에 소요되는 비용을 부담해야 한다. 이러한 많은 부담들은 신규 기업으로서는 감당하기 어려운 부담이다.

개인정보를 보호하기 위해 도입된 여러 제도들은 이제 법률로서 기능하고 있으나, 다른 헌법적 가치와 법제도 사이에서 발생하는 문제점들을 제대로 살펴볼 필요가 있는 시점이 되었다. 본고에서 제안한 아이디어들은 사실 많은 단점도 갖고 있을 터이나 개인정보 보호법제가 기업활동과 국가경쟁력을 강화하는 제도로서도 작용하기 위해 필요한 방안이라고 생각한다.

- 1) 위키피디아, “국무총리실의 민간인 사찰 사건”, http://ko.wikipedia.org/wiki/국무총리실의_민간인_사찰_사건, 2012. 5.
- 2) 위키피디아, “빅 데이터(Big Data)”, http://ko.wikipedia.org/wiki/빅_데이터, 2012. 5.
- 3) <http://www.boan.com/news/articleView.html?idxno=4116>
개인에 대한 정보가 아닌 물건에 대한 고유번호도 다른 정보와 쉽게 결합되어 개인을 식별할 수 있는 정보이므로(비진정 개인정보) 개인정보로 보아 처벌했다.
- 4) 정보통신망법 제71조 제1호, 제22조 제1항
- 5) 마케팅을 위한 개인정보의 제3자 제공이 대표적이다.
- 6) 2012년 6월 14일 방송통신위원회는 인터넷 개인정보 수집·제공업체 (주)열심 커뮤니케이션즈에 대해 203만원의 과징금 및 1500만원의 과태료 부과와 함께 동의 없이 수집한 개인정보에 대해 별도 동의를 받거나 파기하도록 하는 등의 시정명령을 내립.
- 7) 개인정보 보호법 제17조(개인정보의 제공) ①개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유)을 포함한다. 이하 같다)할 수 있다.
 1. 정보주체의 동의를 받은 경우
 2. 제15조 제1항 제2호·제3호 및 제5호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우
- 8) 민법 제449조 (채권의 양도성) ①채권은 양도할 수 있다. 그러나 채권의 성질이 양도를 허용하지 아니하는 때는 그러하지 아니하다.
②채권은 당사자가 반대의 의사를 표시한 경우에는 양도하지 못한다. 그러나 그 의사표시로써 선의의 제3자에게 대항하지 못한다.
제450조 (지명채권양도의 대항요건) ①지명채권의 양도는 양도인이 채무자에게 통지하거나 채무자가 승낙하지 아니하면 채무자 기타 제3자에게 대항하지 못한다.
- 9) 개인정보 보호법 제17조 제1항 제2호는 법 제15조 제1항 제2호(법률에 특별한

규정이 있는 경우)에 해당할 경우에 개인정보를 제3자에게 제공할 수 있다고 규정하고 있다. 민법 제449조 제1항을 이 특별한 규정으로 해석할 수 있는지의 문제가 있다.

- 10) 정보통신망법 제2조 제1항 제3호
- 11) 예를 들어, 개인정보보호책임자(개인정보보호법)와 개인정보관리책임자(정보통신망법), 누출(정보통신망법)과 유출(개인정보보호법), 기술적·관리적 보호조치(정보통신망법)와 안전성 확보에 관한 기술적·관리적 및 물리적 조치(개인정보보호법)
- 12) 정보통신망법 제71조 제1호, 제22조 제1항
- 13) 개인정보 보호법 제75조 제1항 제1호, 제15조 제1항

참고 문헌

- 윤광석, 『민간기업 보유 개인정보의 보호를 위한 정부의 기능개선 연구』, 한국행정연구원, 2011.
- 김범수 외 14인, 『디지털 프라이버시와 법률』, 한국학술정보, 2009.
- 이원태 외 3인, 『방통융합 환경에서 정보의 자유와 개인의 프라이버시 보호방안 연구』, 정보통신정책연구원, 2010. 12.
- 손규식, 『U-사회와 프라이버시』, 조명문화사, 2008.
- 이진우, 『프라이버시의 철학』, 돌베개, 2009.
- 김주영·손형섭, 『개인정보 보호법의 이해』, 법문사, 2012.
- 박우성 외 11인, 『개인정보보호-의료기관 개인건강정보보호』, Pacific Books, 2010.
- 이창범, 『개인정보 보호법』, 법문사, 2012.

위치정보서비스의 법적 쟁점 —위치정보의 보호와 이용 활성화의 관점에서

전용준*

1. 들어가는 글

위치정보, 그중에서 개인위치정보는 특정 개인이 과거 및 현재에 어디에 있었는지를 나타내는 정보로서 그 추세 및 존재 지역을 분석해 미래의 위치를 예상하고 해당 개인의 취향 및 행태를 분석할 수 있는 민감한 자료다. 이러한 특성으로 인해 사업자는 이를 프로파일링해 사업적으로 활용하고자 하고 해당 개인은 최대한 자신의 정보를 보호하고자 한다. 반면 어떤 사업자는 기업의 이미지 제고를 위해 사업적 활용보다는 정보보호활동을 선전하기도 하고 어떤 개인은 기꺼이 자신의 개인정보를 유통시켜 그에 상응하는 경제적 이익을 취하기도 한다. 위치정보법은 이러한 양 세력 간의 적절한 균형을 찾아 정보보호와 이용활성화라는 목적을 동시에 추구하는 법률이라고 할 수 있다.

최근 몇 년 사이에 진행된 스마트폰 위치정보기술의 발전, 특히 앱에 의해 제공되는 다양한 위치기반서비스는 위치정보의 중요성을 여실히 보여주고 있다. 우리나라를 비롯한 세계 각국은 스마트폰, 태블릿 컴퓨터 등 스마트 모바일 기기에 의한 위치정보의 적절한 처리에 관심을 집

* 변호사, 유미법률사무소

중하고 있다. 스마트 모바일 기기를 활용한 측위기술이 계속 발전하고 위치정보와 결합할 수 있는 다른 개인정보들이 스마트 모바일 기기를 중심으로 광범위하게 집적됨에 따라 위치정보의 유출, 오남용에 따른 피해가 다른 개인정보에 비교할 수 없을 정도로 심각해졌지만, 반면 개인 위치정보를 활용한 공적·사적인 이익도 그 피해를 상쇄할 만큼 막대해졌기 때문이다.

2005년 1월 제정된 현행 위치정보의 보호 및 이용 등에 관한 법률(이하 '위치정보법'이라 한다)은 이른바 피쳐폰 시대에 이동통신사 기지국 기반으로 수집된 위치정보를 염두에 둔 것이다. 그에 따라 현재의 스마트폰 시대에 제기되는 다양한 현상(위치기반서비스)을 적절히 포섭하지 못하는 단점이 있다. 본고는 현행 법률에서 제기된 법적 쟁점을 개인정보보호와 이용활성화 측면에서 고찰하기로 한다.

2. 우리나라 및 외국의 위치정보보호 법제 현황

우리나라 법상의 위치정보보호

위치정보법은 2005년 1월에 제정되었다. 종래 우리나라 정보통신서비스에서 발생하는 개인정보보호의 문제는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 한다)에서 규율되었으나, 그 중 위치정보 특히 개인위치정보에 관해 별도의 입법이 이루어진 것이다. 여기에는 위치정보에 대한 침해가 심각해짐에 따라 그에 대한 규제 의 필요성이 부각된 까닭도 있겠으나, 위치정보법의 명칭에서 보다시피 위치정보의 활용가능성이 높아짐에 따라 정보보호만을 규정하는 정보통신망법에서 위치정보를 분리해 그 이용과 보호를 모두 규율하고자 한

것으로 보인다. 이와 같이 위치정보를 개인정보에서 분리해 독립적으로 입법한 예는 우리나라가 최초이며, 대부분의 주요 국가는 개인위치정보를 통합적인 개인정보의 범주에서 규율한다.

우리나라의 위치정보법은 보호와 이용 모두를 규율하고 있으나, 개인 위치정보가 생명·신체에 대한 즉각적인 침해를 유발할 수 있는 민감정보라는 점에서 이용보다 보호 측면에 더 초점이 맞추어져 있다고 볼 수 있다. 법체계로 보면 위치정보를 보호하기 위해 사업자를 규제하는 조항이 많으며 이용활성화에 관해서는 긴급구조를 위한 개인위치정보 이용 및 위치정보의 이용기반 조성에 관한 몇 개의 조문이 있다. 보호와 이용의 균형점에서 가장 중요한 역할을 하는 것은 사업자에 대한 허가·신고 제도라고 여겨진다. 개인위치정보보호를 위한 이용자의 사전 동의 및 개인위치정보의 보호조치는 필수적이므로 결국 사업자에 대한 감독기관의 진입규제가 우리나라 위치정보법의 성향을 좌우하고 있는 것이다. 후술하겠거니와 위치정보사업·위치기반서비스사업의 발전은 이러한 진입규제의 타당성에 대해 강한 논란을 발생시킨다.

개인위치정보보호의 핵심은 개인위치정보의 라이프사이클 각 단계에서 개인위치정보 주체로부터의 사전 동의를 얻고, 처리된 개인위치정보를 안전하게 보호하는 것이다. 여기에 더해 우리나라 위치정보법은 거의 모든 법률 위반행위에 대해 형사처벌 및 양벌규정을 규정함으로써 형사제재에 의한 일반 예방적 효과를 달성하려고 한다. 다만, 개인위치정보의 범위가 다른 정보와 결합되어 특정 개인의 위치를 식별할 수 있는 경우에까지 확대되어 있는 까닭에 형사법적으로는 죄형법정주의 문제가 발생하고 있다.

현재 개인위치정보를 규율할 수 있는 법률은 위치정보법, 정보통신망법, 개인정보보호법이 있다. 위치정보법 제4조, 정보통신망법 제5조, 개

인정보보호법 제6조를 종합적으로 해석하면, 위치정보에 관해서는 위치 정보법이 특별법으로 우선 적용되고 정보통신망법 및 개인정보보호법은 정보주체의 권익보호 측면에서 보충적으로 적용된다고 판단된다.

유럽과 미국의 위치정보 법제의 현황

1) 유럽

EU는 개인정보를 인권(human right) 차원에서 보호하며 자율규제보다는 법률에 의한 규제를 선호한다. 이러한 관점은 미국이 개인정보보호를 소비자보호의 문제로 파악하면서 시장의 자율적인 조치를 중요시하는 것과 대비된다.

EU에서 위치정보보호는 1995년 개인정보보호지침(Directive 95/46/EC), 1997년 전자통신분야 개인정보지침(Directive 97/66/EC), 2002년 지침(Directive 2002/58/EC), 2009년 지침(Directive 2009/136/EC)에 채택된 일련의 e-privacy 지침에 의해 규율된다. 위 지침에서 '위치정보(location data)'는 "공중이용 전자통신서비스 이용자의 단말장치의 지리적 위치를 표시하는 전자통신망에서 또는 전자통신서비스로 처리되는 정보"로 정의되며, 가입자 보호를 위해 ①가입자의 위치정보를 처리하는 경우 그 동의를 받거나 익명으로 처리해야 하고 ②사업자는 사전 동의를 얻기 전에 가입자에게 처리되는 위치정보의 유형, 처리의 목적, 기간, 부가서비스를 위해 제3자에게 전송되는지 여부를 고지해야 하고 ③가입자는 언제든지 위 동의를 철회할 수 있으며, 위 동의를 한 경우에도 무료의 간편한 수단을 사용해 위치정보의 처리를 일시적 거부할 수 있고 ④ 위치정보의 처리는 공공통신망이나 전자통신서비스 제공자 또는 부가서비스를 제공하는 제3자의 권한하에 활동하는 자만으로 제한되며 부가서비스의 경우에는 그 제공 목적에 필요한 범위로 위치정보의 처리가 제한됨을 규정하고 있다.¹⁾

위 지침들은 종래 이동통신사의 기지국 기반의 위치정보를 염두에 둔 것이었는바, 스마트폰의 GPS, WiFi AP 등에 처리되는 위치정보를 보호하기 위해 EU 정보보호작업반(Data Protection Working Party)은 2011년 5월 16일 GPS수신정보, 인터넷접속정보 등을 처리하는 스마트 모바일 기기(smart mobile devices)의 위치정보 서비스에 관한 의견서를 발표했다. 위 작업반은 1995년 지침 제29조에 따라 EU 회원국 정보보호기관의 대표들과 유럽정보보호감독관으로 구성된 독립적인 자문기구다. 위 작업반의 의견은 그 자체로서는 법적 구속력이 없으나 실제에 있어서는 EU의 프라이버시법 운용과정에서 큰 영향력을 발휘하므로 주목할 필요가 있다.

위 의견서의 주요 내용은 다음과 같다. ①스마트 모바일 기기에서 수집된 위치정보는 개인정보이고, MAC(Media Access Control) 주소와 WiFi AP(Access Point)의 결합에 의해 취합된 정보도 개인정보로 취급되어야 한다. ②스마트 모바일 기기에서 수집된 위치정보는 사전 고지된 동의(prior informed consent), 즉 옵트인(opt-in)에 의한 것이어야 한다. ③동의는 위치정보 처리의 목적들에 따라 개별적으로 얻어져야 한다. ④위치정보서비스는 디폴트 값으로 부동의로 설정되어야 한다. ⑤동의의 유효기간은 제한되는 것이 바람직하며, 적어도 1년에 한 번씩 옵트아웃(opt-out)할 수 있는 쉬운 수단을 제공하면서 이러한 사실을 이용자들에게 환기시키는 것이 바람직하다. ⑥정보주체는 아무런 불이익 없이 매우 쉬운 방법에 의해 동의철회를 할 수 있어야 한다. ⑦종업원에 대한 위치정보는 적법한 목적하에 필요최소한의 경우로 제한되어야 한다. ⑧부모는 어린이의 위치정보처리행위가 정당한지 판단할 수 있고 그에 대한 동의권이 있다. 다만 이러한 부모의 권리는 어린이의 자율성을 침해해서는 아니 된다. ⑨정보주체는 수집된 위치정보를 접속·수정·삭제할 권리가 있다. ⑩위치정보서비스 및 앱 사업자는 위치정보 보유기간에 관

한 정책을 수립하고 보유기간이 지나면 해당 정보를 삭제해야 한다. 운영체제 사업자 내지 위치정보 기반시설 관리자가 처리한 MAC 주소나 UDID(Unique Device Identifier) 등의 고유식별번호는 24시간 내에 삭제되어야 한다.

위 의견서는 사업자의 유형을 위치정보 기반시설 관리자(controller of geolocation infrastructure), 위치정보 앱 및 서비스 사업자(provider of geolocation application and services), 운영체제 사업자(developer of the operating system of smart mobile devices)로 분류하면서 위치정보보호를 위한 구체적인 사항을 기술하고 있는바, 이러한 기술방식은 우리나라 위치정보보호 실무에도 참고할 만하다고 판단된다.

2) 미국

미국은 유럽과 같은 개인정보보호를 위한 일반법을 두지 않고 분야별 내지 특정 개인정보의 보호를 위한 개별법을 시행해 왔다. 또한, 법률 내지 정부의 관여를 최소화해 이용자에게 보다 큰 편익을 제공하는 데 역점을 두고 있다. 미국의 개인정보보호법제에서는 개인정보의 사업적 이용, 타겟 마케팅이 비교적 용이하고 같은 맥락에서 사업자의 자율적인 프라이버시 준수를 강조하며, 개인정보보호에 관해 독립적인 감독기구 없이 개별 행정부처가 이를 담당하고 있다. 이는 사후적이지만 소송에 의한 사법적 구제가 비교적 용이한 미국의 문화에 기인한 것으로 보인다.

현재 개인위치정보를 규율하는 제정법으로는 통신서비스 분야에 서 '1996년 전자통신법(The Telecommunication Act 1996)'-1934년 통신법(Communications Act of 1934)을 대폭 개정한 법률-이 존재한다. 위 법률 제222조는 '소비자 정보의 프라이버시(Privacy of Consumer Information)'

라는 제목으로 유무선 통신서비스 이용자의 프라이버시 보호를 위한 몇 가지 사항을 규정하고 있는데, 특히 고객의 위치정보를 '고객소유통신망 정보(Customer Proprietary Network Information: CPNI)에 포함시키면서 법률의 규정 내지 이용자의 승인(approval)이 있는 경우를 제외하고는 오로지 통신서비스 제공 목적으로만 CPNI를 이용·제공할 수 있도록 엄격히 제한하고 있다.

그러므로 통신사업자는 이용자의 위치정보를 통신서비스 제공을 위한 목적이 아닌 마케팅 등 다른 목적을 위해 제3자와 공유하기 위해서는 서비스 이용자의 승인을 받아야 한다. 다만, 위 법률은 이용자의 승인을 받는 방식이나 시점에 대해 명확한 규정을 두고 있지 않기 때문에 '승인(approval)'이 옵트인(opt-in) 내지 명시적(express) 동의를 의미하는지, 아니면 옵트아웃(opt-out) 방식의 동의도 포함하는 것인지 논란이 있다.²⁾ 이에 대해 연방통신위원회(Federal Communications commission: FCC)는 법원의 U.S. West, Inc. v. FCC 사건의 판결취지에 따라 CPNI를 제3자에게 제공하는 경우에는 옵트인 방식의 승인이 필요하나 제휴회사 간 정보공유의 경우에는 옵트아웃 방식의 승인도 가능하다는 의견을 밝혔다.

이와 같이 통신서비스 분야에는 개인위치정보를 보호하는 법률이 제정된 상황이나, 공적·사적 영역을 전반적으로 규율하는 위치정보보호 법률은 존재하지 아니한다. 이러한 상황에서 상원의원 알 프랭크(Al Franken), 리처드 블루멘탈(Richard Blumenthal)은 2011년 6월 16일 스마트폰 등 모바일 기기의 위치정보보호에 관해 'Location Privacy Act of 2011(S.1223)'을 발의한 바 있다. 이는 애플 아이폰 및 구글의 위치정보 캐시 저장 및 전송에 관한 문제가 불거진 상황에서 제출된 것으로, 기존의 개별적인 연방법 체계하에서 많은 사업자들이 고객의 동의 없이 고객의 위치정보를 제3자에게 제공할 수 있는 현재의 상황을 반성하고 있다. 위 법안의 중요한 내용은 ①스마트폰 등 모바일 기기에서 고객의 위

치정보를 수집하는 모든 사업자(any company that may obtain a customer's location information from his or her smartphone or other mobile device)는 고객으로부터 위치정보를 수집하기 전에 고객의 명백한 동의(express consent)를 얻어야 하고, ②위치정보를 제3자와 공유하기 전에 고객의 명백한 동의를 받아야 한다는 것이다.³⁾

또한 제이 록펠러(Jay Rockefeller) 상원의원에 의해 2011년 5월 9일 'Do-Not-Track Online Act of 2011'이 발의되었다. 이 법안은 FTC(Federal Trade Commission)에 이용자가 개인정보 수집에 대한 동의 여부를 표시하는 방법에 관한 기준 및 개인정보 수집을 거부하는 이용자에 대한 개인정보 수집행위를 금지하는 규정을 제정할 수 있는 권한을 부여하고 있다.⁴⁾

3. 위치정보의 보호와 관련된 법적 쟁점

개인위치정보의 범위

현행법은 개인위치정보를 특정 개인의 위치정보(위치정보만으로는 특정 개인의 위치를 알 수 없는 경우에도 다른 정보와 용이하게 결합해 특정 개인의 위치를 알 수 있는 것을 포함)라고 정의하고 있다. 이러한 개념정의는 개인정보보호법상의 개인정보와 마찬가지로 특정 개인의 식별 가능성에 의존하고 있는데, 문제는 이러한 식별 가능성이 과학기술의 발전, 개인정보 관련 DB의 집적에 의해 나날이 높아지고 있다는 점에 있다. 예컨대 단독으로는(단순)위치정보로 평가될 수 있는 정보도 다른 DB와 결합했을 때는 특정 개인을 식별할 수 있는 위치정보가 될 수 있다.

이는 크게 보아 두 가지 측면에서 문제가 된다. 첫 번째는 동의를 받

아야 하는 개인위치정보 범위의 문제이다. 사업자 입장에서는 특정 정보가 특정 개인의 위치를 알 수 있는 개인위치정보인지 불분명한 경우가 있다. 예컨대 스마트폰의 GPS정보, 기지국 위치정보(Cell ID), WiFi AP 정보는 특정 개인을 식별할 수 있는 이동전화번호, USIM 정보, ISP 가입 정보 등의 다른 정보와 결합하지 않는다면 단독으로 개인위치정보가 된다고 보기 어렵다. 같은 이유로 앱서비스사업자와 같은 위치기반서비스 사업자는 다른 정보가 없다면 위 GPS정보 등을 처리한다 해도 개인위치정보 주체를 식별할 수는 없다. 그러나 이동통신사, ISP, 스마트폰 제조사, OS사업자 등이 보유하고 있는 다른 개인정보 DB와의 결합 가능성을 적극적으로 고려해 특정 개인의 식별 가능성을 인정한다면, 위 앱서비스사업자는 위 GPS 등의 정보를 개인위치정보로 보아 개인위치정보 주체에게 위치정보법 제18조에 따른 동의를 구해야 한다. 여기서 하나의 논리적 모순이 발생하는데, 결합할 수 있는 다른 개인정보를 실제로 확보할 수 없어 특정 개인(개인위치정보 주체)을 '현실적'으로 알 수 없는 앱서비스사업자도 위 개인위치정보 주체에게 동의를 얻어야 한다는 점이다. 물론 이 문제는 위치정보법 제18조의 동의가 아니라 제15조의 동의, 즉 스마트폰에 동의화면을 띄워 물건(스마트폰) 소유자의 동의를 얻는 것으로 현실적으로 해결될 수 있으나, 제15조와 제18조는 규범의 수범자가 다르고 벌칙도 달라(제15조 물건 소유자의 동의 확보 위반은 과태료, 제18조 개인위치정보 주체의 동의 확보 위반은 형벌) 이론상 구분해야 한다.

두 번째는, 우리나라 형사사법체계의 특성에서 발생하는 형사처벌의 문제다. 현행법상 개인위치정보의 인정여부는 위 정의조항의 해석에 따라 또는 위치정보를 처리한 사업자의 사정(예컨대 이동통신사와의 사업적 제휴관계, 위치정보사업자가 보유한 정보의 내용)에 따라 그 범위가 달라진다. 이는 형사법적 관점에서 죄형법정주의(명확성의 원칙) 위반 소지가 있고 수사기관의 광범위한 개입을 허용하는 근거가 된다. 작년 법원은 스마트

폰 앱의 로그인 절차를 간편하게 하기 위해 수집된 국제단말기인증번호(IMEI), 범용가입자식별모듈(USIM) 일련번호를 다른 정보와 결합해 개인을 식별할 수 있는 개인정보로 인정하고 벌금형을 선고하면서, “당해 정보와 결합 가능한 다른 정보는 모두 동일인에게 보유되는 것을 전제로 하지 않고 ‘쉽게 결합해 알아 볼 수 있다’는 것은 쉽게 다른 정보를 구한다는 의미이기보다는 구하기 쉬운지 어려운지와는 상관없이 해당 정보와 다른 정보가 특별한 어려움 없이 쉽게 결합해 특정 개인을 알아 볼 수 있게 되는 것을 말한다”라고 판시한 바 있다(서울중앙지법 2011. 2. 23. 선고 2010고단5343판결). 이러한 논리는 개인위치정보에도 그대로 적용된다고 보이는데, 이에 따르면 이동통신사의 개인정보 DB를 이용하거나 접근하지 않는 스마트폰 앱서비스사업자가 수집한 (단순)위치정보도 모두 개인위치정보로 평가될 수 있다. 사건으로는, 결합 가능한 다른 정보는 동일인의 보유일 것으로 제한되지는 않지만 적어도 사업적 제휴관계, 정보시스템의 연결관계 등이 존재해 접근 가능성이 있는 정보로 제한되어야 한다고 본다. 이러한 문제를 해결하기 위해서는 ‘다른 정보와 쉽게 결합’이라는 구성요건을 보다 구체적으로 해석하고 나아가 제18조 위반의 유형을 분류해 일부 위반행위를 비범죄화하는 것이 필요하다고 판단된다.

참고로, 일본 개인정보보호법에서 규정한 개인정보의 정의도 다른 정보와 용이하게 조합할 수 있고 그것에 의해 특정 개인이 식별될 수 있는 정보도 포함하고 있다는 점에서 우리 법제상의 개인정보의 정의와 동일하지만, 일본 개인정보보호법은 사업자의 의무위반행위를 직접 처벌하는 규정은 없고 의무위반행위에 대해 일차적으로 주무대신이 시정권고 내지 시정명령을 하고 이러한 시정명령조치를 위반한 자에 대해 6월 이하의 징역 또는 30만 엔 이하의 벌금에 처하도록 하고 있다(일본 개인정보

보호법 제56조). 이러한 법제에서는 주무관청이 해당 개인정보의 성질, 중요도, 위반행위의 유형을 고려해 시정명령권을 발동할 수 있는 장점이 있고 죄형법정주의 문제도 비교적 적다.

법적으로 보호해야 하는 위치정보의 종류

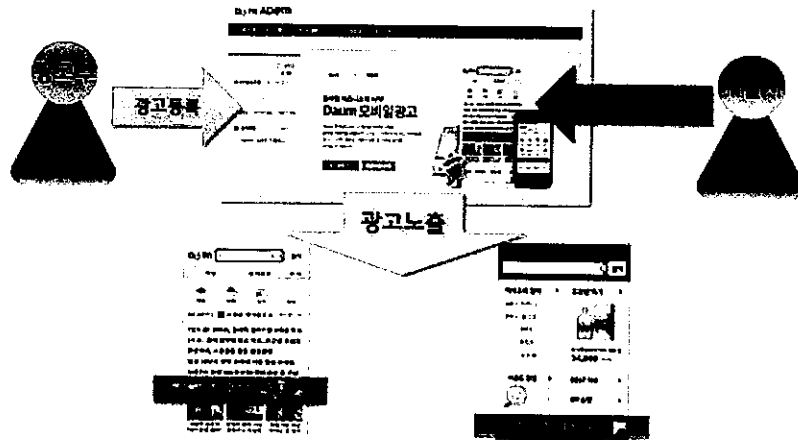
우리나라 위치정보법은 세 가지 유형의 위치정보를 규정하고 있다. 즉 ①개인이 식별되거나 식별될 가능성이 있는 개인위치정보, ②이동성이 있는 물건의 위치정보, ③식별되지 않는 개인에 관한 위치정보를 말한다(위치정보법 제2조. 본고에서는 ②, ③ 유형의 위치정보를 단순위치정보라고 부르기로 한다). 개인위치정보의 수집 등은 개인위치정보 주체의 동의를 받아야 하고(위치정보법 제18조, 제19조), 이동성이 있는 물건 내지 개인에 대한 위치정보의 수집 등은 해당 물건의 소유자 내지 개인의 동의를 받도록 되어 있다(위치정보법 제15조). 그리고 위 세 가지 유형의 위치정보 모두 기술적·관리적 보호조치의 대상이 되고(위치정보법 제16조), 기술적·관리적 조치를 취하지 않는 경우 1년 이하의 징역 또는 2천만원 이하의 벌금에 처해진다.

전체적으로 보면, 우리나라 위치정보법은 개인이 식별되는 개인위치정보뿐만 아니라 개인의 식별 가능성과 무관한 단순위치정보까지 동의 및 기술적·관리적 보호조치의 대상으로 하고 있다. 개인이 식별되지 않는 위치정보에 대해 해당 개인의 동의를 받게 하는 것은 논리적으로 모순이거나 정보 주체의 보호와 관계없는 단순위치정보를 개인위치정보와 동일한 수준으로 보호하는 것은 타당하지 아니하다고 판단된다. 단순위치정보는 개인정보보호법상의 개인정보가 아니므로 위치정보법이 없다면 동의 및 보호조치를 할 근거가 없다. 나아가 단순위치정보를 처리하는 사업자에 대해 허가·신고 등의 진입규제를 하는 것도 재고할 필요가 있다.

모바일 광고의 경우 동의의 문제

1) 모바일 광고서비스의 주체

스마트폰의 위치정보를 활용해 스마트폰 앱 내지 모바일 웹에서 개인 맞춤형 광고를 제공하는 서비스가 날로 증가하고 있다. 이러한 광고서비스는 앱에서 광고를 게재하려는 광고주, 앱에서 광고를 보여주는 앱서비스사업자, 광고주와 앱서비스사업자를 연결해 주는 광고플랫폼사업자들이 각자 가지고 있는 개인정보 DB와 스마트폰에서 제공하는 위치정보를 결합해 개인의 현재 위치에 부합하는 맞춤형 광고를 제공한다.



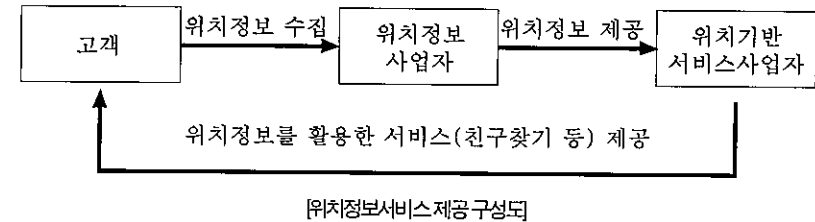
[다음이 운영하는 모바일 광고플랫폼AD@m]⁹⁾

종래의 광고서비스는 광고주와 매체로 이루어졌으나, 스마트폰에서는 각각의 앱이 매체 역할을 함에 따라 별도의 광고플랫폼사업자가 등장하게 되었다. 광고플랫폼사업자는 광고주와 앱서비스사업자(개발자)를 유치해 앱에 광고를 노출해 주는 역할을 수행하는데, 구글의 애드몹(AdMob), 다음의 AD@m, 퓨처스트림네트웍스의 카울리(Cauly) 등이 이

에 해당한다.

2) 모바일 광고에서 위치정보서비스사업자, 위치기반서비스사업자의 구분

위치정보사업자는 위치정보를 수집해 위치기반서비스사업자에게 제공하는 것을 사업으로 영위하는 자를 말하고, 위치기반서비스사업자는 위치정보사업자로부터 위치정보를 받아 이를 이용한 서비스를 제공하는 것을 사업으로 영위하는 자를 말한다.



모바일광고서비스에서는, 스마트폰의 GPS정보를 수집하는 OS사업자인 구글·애플·MS가 위치정보사업자에 해당하고, 위치정보를 활용해 광고를 앱에 제공하는 광고플랫폼 사업자, 앱에서 광고를 보여주는 앱서비스사업자, 광고주(위치정보를 이용하는 경우)들이 위치기반서비스사업자에 해당한다.

이와 같이 위치정보를 이용한 모바일광고서비스에서는 위치정보 및 개인정보를 활용하는 복수의 사업자가 존재하게 되는데, 각 사업자의 동의 획득의 필요성 및 동의 방식을 검토해야 한다.

보 취급방침의 내용과 유사하므로, 이를 개인정보 취급방침에 반영해 고지하는 것으로 대체하자는 견해가 있다.⁹⁾

개인위치정보 제3자 제공 시 매회 즉시 통보

위치정보법 제19조 제3항은, 위치기반서비스사업자가 개인위치정보를 개인위치정보 주체가 지정하는 제3자에게 제공하는 경우 매회 개인위치정보 주체에게 제공받는 자, 제공일시 및 제공목적 등을 즉시 통보해야 한다고 규정하고 있다. 통보방법으로는 원칙적으로 위치정보사업자가 개인위치정보를 수집한 당해 단말장치를 통해 통보해야 하지만, 예외적으로 당해 단말장치가 문자·음성 또는 영상수신 기능을 갖추지 않았거나 개인위치정보 주체가 다른 통신단말장치 또는 전자우편으로 통보할 것을 미리 요청한 경우, 미리 개인위치정보 주체가 지정한 다른 통신단말장치나 전자우편주소로 통보할 수 있다(시행령 제24조¹⁰⁾).

위 조항은 개인위치정보가 생명·신체에 대해 즉각적인 위험을 초래할 수 있는 민감정보라는 측면을 고려해 제정된 규정으로 보이나, 매회 즉시 통보하도록 하는 것은 이용자 및 사업자 모두에게 불편과 부담을 줄 수 있다.

또한 다음 마이피플, 페이스북 등의 위치기반 앱에서는 개인이 방문한 장소를 스스로 지인 등에게 공개하는 서비스가 활성화되고 있으나, 위 규정에 의하면 지인인 제3자에게 개인위치정보가 공개될 때도 해당 개인에게 매번 즉시 통보를 해야 하는 문제가 발생한다. 개인위치정보 주체가 스스로 자신의 개인위치정보를 공개하는 서비스를 이용하는 경우에는 해당 개인정보 주체에게 통보할 필요가 없으므로, 매회 즉시 통보 의무에 예외를 두어야 할 것이다. 위와 같은 즉시 통보 의무의 예외는 정부가 2011년 4월경에 제출한 위치정보법 개정안에 수용된 바 있다.

제16조 제1항을 위반해 기술적, 관리적 조치를 하지 않은 경우

위치정보법 제16조는 사업자가 위치정보의 누출·변조·훼손을 방지하기 위해 기술적·관리적 조치를 취할 것을 의무화하고 있고, 구체적인 기술적·관리적 조치의 내용은 동법 시행령 제20조에 위임하고 있다. 위 제16조의 기술적·관리적 조치 의무를 위반하는 경우 제41조에 의해 1년 이하의 징역 또는 2천만원 이하의 벌금에 처하게 된다.

이와 관련해, 최근 방송통신위원회는 애플과 구글이 스마트폰의 위치정보 캐쉬¹¹⁾를 암호화하지 않은 행위에 대해 이를 위 시행령 제20조 제2항 제2호의 '위치정보시스템에의 권한 없는 접근을 차단하기 위한 암호화' 조치 의무 위반으로 판단하고 이를 시정할 것을 권고한 바 있다(현행 위치정보법은 시정명령권을 규정하고 있지 않아 행정지도 성격의 시정권고를 한 것으로 보임).

그러나 위치정보 캐쉬 암호화는 위 시행령 제20조 제2항 제2호에 명백히 포섭된다고 단정하기 어렵다. 위 시행령 제20조 제2항 제2호는 법 제16조 제1항의 기술적 조치의 하나로 '위치정보시스템에의 권한 없는 접근을 차단하기 위한 암호화, 방화벽 설치 등의 조치'를 규정하고 있는데, 여기에서 말하는 암호화 조치는 위치정보시스템에 대한 권한 없는, 즉 불법적인 접근을 차단하기 위한 암호화 조치이므로 문언해석상 '위치정보' 자체를 암호화하는 것과 구분되기 때문이다. 이는 위치정보법의 일반법인 정보통신망법에서 규정하고 있는 기술적·관리적 보호조치의 내용을 보아도 분명하다. 정보통신망법 제28조 제1항에서 규정하는 기술적·관리적 조치는 '개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영(제2호)'과 '개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치(제4호)'를 구분하면서 동법 시행령 제15조 제4항에서 '주민등록번호 및 계좌번호 등 금융정보의 암호화 저장'을 위 '개인정보를 안전하게 저장·

전송할 수 있는 암호화기술 등을 이용한 보안조치(4호)'에 포함시키고 있다. 즉 주민등록번호 등의 개인정보 자체를 암호화하는 것은 불법적인 접근을 차단하기 위한 암호화조치와는 구별되는 것이다.

다만, 방송통신위원회가 정한 '위치정보보호를 위한 기술적, 관리적 보호조치 권고' 제8조는 '위치정보에 대한 권한 없는 접근을 차단하기 위한 조치' 중 하나로 '위치정보를 안전하게 저장할 수 있는 암호화기술 등을 이용한 보안조치'를 들고 있으나, 위 권고는 고시가 아니라 모법의 위임근거가 없는 행정지도적 성격의 가이드라인에 불과하므로 이를 법적인 근거로 제시하기는 무리라고 판단된다.

또한, 개인위치정보뿐만 아니라 단순위치정보까지 기술적·관리적 보호조치를 취하도록 되어 있는 것도 현실과 부합되지 않는다고 보인다. 단순위치정보는 특정 개인이 식별되지 않는 위치정보이므로 굳이 이러한 정보의 유출 등을 방지하기 위해 기술적·관리적 보호조치를 취할 필요는 없다고 판단된다. 개인정보에 해당하는 개인위치정보에 대해서만 기술적·관리적 보호조치를 하는 것이 개인정보 보호법률의 체계에 부합한다.

정보통신망법의 기술적·관리적 조치는 해당 법률 및 시행령 조항, 관련 고시들이 여러 번 개정되면서 어느 정도 체계적으로 정비된 반면, 위치정보법의 기술적·관리적 조치 관련 내용은 제정 후 지금까지 개정된 것이 없었다. 현재 새롭게 요청되는 여러 가지 기술적·관리적 보호조치에 능동적으로 대처하기 위해서는 차제에 위 보호조치의 내용 및 법적 지위에 대해 체계적인 정비를 할 필요가 있다.

한편 기술적·관리적 보호조치 미이행에 대한 벌칙의 비례성도 한번 생각할 필요가 있다. 전술한 바와 같이 위치정보법 제16조 제1항을 위반해 기술적·관리적 조치를 하지 않은 경우 1년 이하의 징역 또는 2천만

원 이하의 벌금에 처하게 되어 있다(제41조). 반면 이에 대응하는 정보통신망법 제28조 제1항을 위반해 기술적, 관리적 조치를 하지 않은 행위는 3천만원 이하의 과태료 부과 대상이다(정보통신망법 제76조). 정책적인 판단하에 위치정보에 대한 기술적·관리적 조치 미이행을 더 크게 제재하는 것으로 이해할 수도 있으나, 정보통신망법 및 개인정보보호법 모두 기술적·관리적 조치를 하지 아니해 개인정보가 유출된 경우에만 형사처벌을 가하고 단순히 기술적·관리적 조치를 하지 않은 경우에는 과태료 부과로 그치는 것을 고려해 보면, 개인위치정보 유출에 관계없이 기술적·관리적 조치 미이행 행위에 형사처벌을 가하는 것은 입법적 검토가 필요하다고 생각된다.

4. 이용 활성화에 관련된 법적 쟁점

위치정보사업 등의 허가·신고

현행법은 위치정보사업자에 대해 방송통신위원회의 허가를 받도록 규정하고 있으며(법 제5조 제1항), 위치기반서비스사업자에 대해서는 방송통신위원회에 신고하도록 규정하고 있다(법제 9조 제1항). 위치정보사업자는 개인 사생활을 직접적으로 침해할 위험성이 높은 개인위치정보를 광범위하게 수집·제공하기 때문에 위치정보의 정확성과 안정성, 국민의 사생활 보호를 위해 위치정보사업에 대해서는 일정한 자격을 요구하는 허가제를 규정하고, 위치기반서비스사업자는 단순히 위치정보사업자로부터 취득한 위치정보를 이용해 서비스를 제공하는 것에 불과하므로 다양한 서비스 개발을 유도한다는 차원에서 위치기반서비스사업에 대해서는 신고제를 규정한 것이다. 이러한 허가·신고 없이 위치정보사업, 위치기반서비스사업을 하는 자는 5년 이하의 징역 또는 5천만원 이하의

벌금 내지 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하게 된다(위치정보법 제39조 제1항, 제40조 제2항).

그러나 이러한 허가제·신고제에 대해서는 많은 비판이 있다. 근본적으로는 허가·신고제를 두더라도 개인정보를 보호하지 않는 사업자의 출현을 막을 수 없고 오히려 개인정보를 제대로 보호하는 앱서비스사업자에 대해 신고를 하지 않았다는 이유로 형사처벌을 가하는 수단이 된다고 비판한다. 또한 일본일초가 중요한 인터넷 시대에 허가·신고 서류 제출로 인해 사업을 1~2개월 지체하는 것도 큰 문제가 된다고 한다. 한편에서는 허가·신고 없이 국내로 진출한 외국의 위치기반 앱의 경우와 비교해 국내 사업자에 대한 역차별 규정이라고 비판한다. 반대로 외국인 이 개발한 앱서비스는 국내에 거소가 없고 주민등록번호가 존재하지 아니하므로 사업자등록이 불가능해 합법적으로 국내에 유통될 수 없다는 주장도 있다.

2011년 2월 기준으로 위치정보사업자는 81개사, 위치기반서비스사업자는 235개사에 달하고 있으며 그 증가속도도 매우 가파르다. 허가제의 본질은 사업자 수를 통제해 일종의 독점권을 부여하는 것이나 방송통신위원회의 정책은 오히려 그 수를 늘려 유효경쟁을 유도하는 면도 있으므로 본래의 허가제와는 다르게 운영되고 있다고 보이고, 위치기반서비스사업자는 우후죽순처럼 생겨나 신고제로써 담보해야 할 감독기능이 제대로 동작하고 있는지 의문이 있다. 사업자로 하여금 개인위치정보를 제대로 보호하게 하기 위해서는 허가·신고 제도가 중요한 것이 아니라 EU 정보보호반 의견서와 같이 사업자들이 준수해야 할 사항을 유형별·사안별로 분명하게 정해 주고 이를 준수하게 하는 것이 본질적인 대책일 것이다. 이와 같은 관점에서 보면, 현재의 허가·신고 제도는 위치정보를 준수하고자 하는 국내의 양심적인 사업자들에게만 적용되어 이들에게 수개월 동안의 서류작업을 요구하는 부담스러운 절차로 전락

할 가능성이 높다. 이러한 상황이라면 허가·신고 제도를 전면적으로 개편하는 사고를 할 때라고 판단된다. 특히 앱서비스사업자 등 위치기반서비스사업자의 증가추세가 가파르므로 이들에 대한 신고제도를 중점적으로 검토해야 할 것이다. 2011년 정부가 제안한 위치정보법 개정안도 개인위치정보를 대상으로 하지 않는 위치정보사업 및 위치기반서비스사업에 대해서는 허가·신고 제도를 면제하는 것을 제안하고 있다. 결국 위치정보·위치기반서비스사업의 유형을 구체적으로 분석해 개별사업에 대해 허가·신고가 필요 없는지 여부를 정하는 것이 중요하다.

긴급구조를 위한 개인위치정보 이용

긴급구조기관은 급박한 위험으로부터 생명·신체를 보호하기 위해 개인위치정보 주체, 개인위치정보 주체의 배우자, 2촌 이내의 친족 또는 민법 제928조 규정에 따른 후견인의 긴급구조요청이 있는 경우 긴급구조 상황 여부를 판단해 위치정보사업자에게 개인위치정보의 제공을 요청할 수 있다. 여기서 긴급구조기관은 재난 및 안전관리기본법 제3조 제7항에서 정한 소방방재청, 소방본부 및 소방서를 말하며 다만, 해양에서 발생한 재난의 경우에는 해양경찰청, 지방해양경찰청 및 해양경찰서를 말한다. 이러한 긴급구조요청은 대통령령이 정하는 특수번호 전화서비스를 통한 호출에 의해야 하는데 시행령은 이를 119·122로 제한하고 있다. 이에 따라 유괴·납치 등 범죄행위로 인한 급박한 위험으로부터 긴급구조가 요구되는 상황에서도 경찰에 의한 긴급구조는 위치정보법상 불가능했다. 개인위치정보 주체 측의 긴급구조요청에 의해 발신자 추적을 하는 것은 경찰력 낭용과 본질적인 관계가 없다고 할 것이므로 긴급구조를 위해 개인위치정보를 이용한다는 취지에서 비추어 경찰에 대해서도 긴급구조요청을 할 수 있도록 하고 특수번호에도 112를 추가할 필요가 있다.

이러한 논의를 바탕으로 최근 개정된 위치정보법은 경찰관서에 특수 번호 전화서비스 호출에 의한 긴급구조요청 시 개인위치정보를 제공받을 수 있도록 하고 긴급구조기관, 경찰관서 및 위치정보사업자는 개인위치정보를 요청하거나 제공하는 경우 그 사실을 해당 개인위치정보 주체에게 즉시 통보하도록 했다(위치정보법 제29조 제2항, 제6항). 개정법 초안에는 경찰력 남용에 대비해 경찰에 의한 개인위치정보 이용 시 법원의 사후승인을 얻을 것을 요건으로 했으나, 긴급구조행위는 범죄수사와 같은 사법작용이 아니라 행정작용이므로, 긴급구조를 위해 개인위치정보 수집·이용에 대한 법원의 승인을 얻을 필요는 없다는 지적에 따라 2012년 5월 2일 마지막 법사위 회의에서 삭제되었다. 경찰관서의 개인위치정보 오남용을 방지하기 위해서는, 경찰관서가 제공받은 개인위치정보에 대해 개인위치정보 주체가 이를 열람·복사할 수 있도록 하고(위치정보법 제29조 제9항), 긴급구조 목적으로 제공받은 개인위치정보를 긴급구조 외 목적에 사용하는 것을 금지하고 이를 위반하는 경우 형사처벌을 하는 규정(위치정보법 제29조 제8항, 제39조)을 엄격하게 운용할 필요가 있다고 판단된다.

이용활성화 측면에서 본 위치정보법

우리나라 위치정보법은 법률 이름에서도 알 수 있듯이 정보보호뿐만 아니라 이용활성화도 입법목적으로 하고 있다. 만약 위치정보법에 이용활성화 규정이 없다고 한다면, 위 법은 기존의 정보통신망법이나 개인정보보호법에 통합되는 것이 법체계상 적절할 것이다. 위치정보법은 이용활성화 규정으로 제5장에 기술개발의 추진(제33조), 표준화의 추진(제34조), 위치정보의 이용촉진(제35조), 위치정보심의위원회(제36조) 규정을 두고 있는데, 전체적으로 보면 위 규정은 정보통신망법상의 이용촉진에 관한 규정과 유사하고 이러한 국가R&D, 정부에 의한 사업시행 등은 현

재 민간 위치정보서비스 시장의 발전추세 및 동향을 볼 때 중복되거나 불필요하다고 볼 여지가 있으므로 이의 신중한 운영이 요구된다. 또한 현재 제출된 정부개정안(제35조의 2)을 보면, 방송통신위원회에게 위치정보사업 및 위치기반서비스사업에 대한 효율적인 경쟁체제 구축과 공정한 경쟁환경 조성을 위해 경쟁상황 평가를 할 수 있도록 되어 있는데, 이는 공정거래위원회의 업무영역과 중첩되는 것으로서 양 기관의 중복적인 감독수행이 우려된다.

5. 결어

우리나라 위치정보법의 정보보호정책의 골자는 위치정보의 수집, 이용, 제공의 각 단계에서 정보 주체의 사전 동의를 얻으라는 것이고 획득된 정보의 안전성 확보를 위해 기술적·관리적 보호조치를 취하라는 것이다. 이러한 태도는 법 제정 후 지금까지 그대로 유지되었고 현행 개인정보보호법 체계와 부합된다고 판단된다. 다만, 사업자의 진입규제 수단으로 허가제·신고제를 채택하고 개인위치정보의 제3자 제공 시 즉시 통보 의무를 부과한 것은 법 제정 당시의 현실에 비추어 타당한 면이 있으나 지금의 현실에서 볼 때는 개선의 여지가 있다고 보인다. 그리고 현행법은 개인위치정보와 단순위치정보의 차이를 크게 두고 있지 않는데, 단순위치정보는 개인정보가 아니므로 정보보호법상의 보호대상이 될 수 있는지 의문이 있다. 개인정보 보호법률이라는 전체적 관점에서 보면, 개인정보와 마찬가지로 개인위치정보의 범위가 불명확하다는 단점이 있고 이것이 광범위한 형사처벌 규정과 연결됨에 따라 죄형법정주의 및 수사기관의 과도한 개입 우려가 있다.

위치정보의 이용활성화 측면에서 보면, 우리나라 위치정보법은 적어

도 개념상으로는 세계 최초로 위치정보 관련 사업을 명시적으로 규정하고 이용촉진을 도모했다는 점에서 의의가 있다. 다만, 위치정보법상의 허가제가 애플 아이폰의 국내 진입을 사실상 거부하는 수단이 되었다는 점에서 위치정보의 보호와 이용활성화가 허가·신고제 영역에서 충돌한 바 있음을 확인할 수 있다. 정보보호와 이용활성화는 현실적으로 어느 정도 서로 배타적인 성질을 띠고 있으므로, 이용 내지 서비스 활성화를 위해 정보보호 규정은 일부 개정이 불가피하다. 그러나 개인위치정보의 수집·이용·제공의 각 단계에서 요구되는 기본적인 동의권을 제한해서는 아니 될 것이다.

향후 우리나라 위치정보법 운영에 있어 고려해야 할 점은, 다양한 중소 규모의 국내 위치기반서비스사업자가 탄생할 것이고 이들이 해외의 사업자와 경쟁할 것이라는 사실이다. 국내의 위치정보법이 국내 사업자를 역으로 차별하지 아니하고 공정한 경쟁의 기회를 부여함과 더불어 이들 사업자가 탈법의 유혹에 빠져 개인위치정보를 침해하는 것을 방지하기 위해 앱모니터링제도 또는 컴퓨터 백신 시장과 같은 앱모니터링 시장이 형성되어야 할 것으로 본다.

주

- 1) 함인선, “개인정보보호법의 적용관계와 입법적 과제-위치정보법과의 관계를 중심으로 해서”, 인권과 정의, 2011. 8, 50면
- 2) 이러한 미국 내의 논란에 관해서는 방송통신위원회, 한국인터넷진흥원, 『위치정보의 보호 및 이용 등에 관한 법률 해설서』, 2010.1, 10면 참조
- 3) http://www.franken.senate.gov/files/docs/110614_The_Location_Privacy_Protection_Act_of_2011_One_pager.pdf
- 4) <http://www.govtrack.us/congress/bills/112/s913>
- 5) 출처 <http://blog.naver.com/emnetblog?Redirect=Log&logNo=1100986443> 72
- 6) 방송통신위원회, 한국인터넷진흥원, 모바일광고플랫폼사업자 대상 위치정보법 설명회 자료, 12면, 2012. 3.7
- 7) 방송통신위원회도 같은 견해로 보인다. 방송통신위원회, 한국인터넷진흥원, 모바일광고플랫폼사업자 대상 위치정보법 설명회 자료, 2012. 3.7, 15면 참조
- 8) 도학선, “위치정보의 보호 및 이용 등에 관한 법률의 개선을 위한 제언”, 2012. 2, 16면
- 9) 도학선, “위치정보의 보호 및 이용 등에 관한 법률의 개선을 위한 제언”, 2012. 2, 9면
- 10) 위 시행령 조항은 모범에 근거가 없어 법체계상 문제가 있다고 판단된다.
- 11) 스마트폰이 보다 빠르게 위치를 파악하도록 위치정보사업자가 스마트폰 내에 일시적으로 저장되도록 설계한 위치정보 DB의 일부.

- 도학선, “위치정보의 보호 및 이용 등에 관한 법률의 개선을 위한 제언”, 정보법학회 2012년 2월 사례연구회 발표자료.
- 방송통신위원회, 한국인터넷진흥원, 『위치정보의 보호 및 이용 등에 관한 법률 해설서』, 2010. 1.
- 함인선, “정보사회에서의 개인위치정보의 보호와 이용에 관한 법적 고찰”, 『인터넷법률』 통권 제44호.

인터넷에서의 아동 보호

이숙연*

1. 들어가는 글

인터넷은 현실세계보다 더 다양하고 복잡다기하며 더욱 막강한 파괴력과 전파력을 가진 ‘사이버공간’을 구축하고 있다. 인터넷에 범람하는 각종 정보들은 인터넷을 ‘정보의 바다’ 혹은 ‘표현의 자유의 장’이 아니라 ‘불법과 음란의 바다’로 전락시키기도 한다. 인터넷에 넘쳐나는 음란물과 폭력물은 신체적·정신적으로 미성숙한 청소년에게 심각한 영향을 미칠 수 있다. 최근에는 폭력적·선정적인 내용의 온라인게임과 이에 대한 과다몰입이 영똥하게도 학교폭력과 청소년의 정신적·신체적 건강악화의 주범으로 지목되고 있다.

표현의 자유나 행복추구권 등은 우리 헌법이 보장하고 있는 중요한 기본권이나, 사회의 미래를 이끌어갈 청소년의 건전한 육성과 보호 또한 사회존립을 위한 포기할 수 없는 가치라 할 것이다. 이하에서는 청소년을 이용한 음란물의 온라인 유통금지와 청소년의 음란물에 대한 노출방지를 위한 각국의 입법과 실무례를 살펴보기로 한다. 또한 폭력적인 내용의 온라인게임으로부터 청소년보호와 청소년의 온라인게임 중독방

*판사, 서울고등법원