

글로벌 인터넷사업자의 개인정보침해에 대한 규제 - 아바타 이론의 제안

박 현 일*

요 약

최근 들어 인터넷사업자들이 웹상에서 제공하는 새로운 서비스가 각국의 개인정보보호 법제에 저촉되는 사례가 늘고 있다. 인터넷사업자들이 국경을 넘어 정보를 수집하고 이를 가공처리, 저장하는 과정에서 본인의 동의를 얻지 않거나 개인정보를 익명처리하지 않은 것이 주요 문제가 되고 있다. 본고는 국제적으로 서비스를 하고 있는 대형 인터넷사업자가 프라이버시 침해 혐의를 받고 있는 사례를 알아보고, 무엇이 문제가 되는지 쟁점을 검토하였다. 특히 현지 감독당국이 글로벌 인터넷사업자의 위법사실을 적발하였더라도 해당 사업자가 대리인이나 분신·도구를 통하여 행동한 사실이 없으면 본사에 제재를 가할 수 없는 실정이다.

사이버공간에서는 실제 위반행위자가 없더라도 중대한 개인정보를 침해하는 결과를 가져온다면 영화 <아바타>에서와 같은 해결방법을 모색해볼 수 있다. 아바타는 독자적인 사고나 판단능력이 전혀 없지만, 나비죽이 사는 낙원이 지구인에 의하여 파괴될 수 있는 상황에서 아바타와 이를 조종하는 사람들이 한 몸이 되어 나비죽과 힘을 합쳐 아름다운 낙원을 지켜낸다. 즉, 인터넷사업자가 국내 실재하지 않더라도 그의 활동결과로 볼 수 있는 침해행위가 발생하고, 그 결과 회복할 수 없는 피해가 발생할 우려가 있으며, 본인과 아바타를 한 몸으로 볼 수 있다면 아바타를 통해 위법행위를 저지른 본사의 책임자를 처벌할 수 있어야 한다. 만일 그 책임자를 특정할 수 없더라도 그의 감독책임이 있는 본사 법인에 책임을 물을 수 있다고 본다.

만일 법원에서 이러한 ‘아바타 이론’을 수용한다면 국내에서도 외국 본사에 벌금을 과하는 등 처벌이 가능할 것이다. 다만, 해당 인터넷사업자의 반발도 만만치 않을 것이므로 주요국 개인정보 감독기구는 수사정보를 교환하는 등 국제적으로 긴밀한 협조체제를 갖출 필요가 있다.

I. 서 론

오늘날 사이버공간에서는 국경의 구분이 사라지고 있다. 인터넷을 통해 서울에 거주하는 개인이 동네 서점에서 책을 고르듯이 미국의 아마존닷컴에 서적을 주문할 수 있고, 미국 내 은행계좌에서 돈을 인출할 수 있다. 구글맵을 통해서도 루브르 박물관 주변의 거리를 직접 현장에 가 있는 것처럼 둘러볼 수 있다.

이와 같은 서비스를 인터넷 이용자들에게 제공하기 위하여 국제적인 인터넷사업자들(Internet service providers: ISPs)은 국경을 넘어 정보를 수집하고 이를 가공처리하여 저장해 두고 있다. 이 과정에서 수많은 개

인정보가 본인의 동의 없이 수집·저장·가공·이용·제공되고 있는 것이다.

최근 들어 이들 인터넷사업자들이 웹상에서 인맥을 쌓을 수 있게 해주는 소셜네트워크 서비스(social network service: SNS)를 강화하면서 개인정보 침해가 종종 문제가 되고 있다. 구글이나 페이스북처럼 기존 이용자·회원들의 정보를 본인의 동의를 받지 않고 SNS에 이용하거나 검색 광고 등에 사용하는 것이 개인의 프라이버시를 침해할 수 있기 때문이다.

본고는 국제적으로 서비스를 하고 있는 대형 인터넷사업자가 프라이버시 침해 혐의를 받고 있는 사례를 알아보고, 무엇이 문제가 되는지 개인정보보호와 관련된

본고는 2011.6.3 한국인터넷진흥원(KISA) 주관으로 제주도에서 열린 제35차 아시아-태평양 프라이버시감독기구(Asia-Pacific Privacy Authorities: APPA) 포럼에서 필자가 발표한 제안 “How to Tame Global ISPs”을 논문으로 정리한 것이다.

* 경희대학교 법학전문대학원 교수(oncpark@khu.ac.kr)

쟁점을 검토한다. 특히 글로벌 인터넷사업자가 현지에 사업거점을 두지 않은 상태에서 위법사실을 적발한 현지 감독당국이 해당 사업자에 대하여 무슨 조치를 취할 수 있는지 중점적으로 살펴보고자 한다.

II. 글로벌 인터넷사업자의 개인정보침해 사례

최근 들어 글로벌 인터넷사업자들이 개인정보를 침해하였거나 침해할 우려가 있다고 국내의 언론에 보도된 사례는 다음과 같다. 해당 사업자들은 지적받은 사안에 대하여 잘못을 시인하지 않고 관할 당국의 조치에 맞서고 있는 형국이다.

2.1 구글의 버즈 서비스

구글(Google)은 2010년 2월 소셜네트워크 서비스(SNS)인 버즈(Buzz) 사업을 개시하면서 기존 이메일 서비스(Gmail) 이용자들이 자주 쓰는 이메일 주소를 본인의 동의를 받지 않고 자동으로 버즈에 공개하였다. 이에 캐나다를 비롯한 미국, 프랑스 등 10개국의 개인정보감독기구들은 구글에 공식 서한을 보내 새로운 정보통신 서비스나 상품을 출시할 때에는 개인정보의 보호를 강화하도록 권고하고, 향후 서비스하는 국가의 개인정보법제를 어떻게 준수할 것인지 설명할 것을 요구했다.^[1] 더욱이 Gmail 사용자들이 프라이버시 침해를 이유로 집단소송을 제기하자, 구글은 회사의 잘못을 시인한 것은 아니지만 집단소송을 재판상 화해(settlement)로 해결하는 조건으로 850만달러 기금을 조성해 인터넷 개인정보보호에 사용하기로 했다.

2.2 구글맵의 스트리트뷰 서비스

구글은 2007년부터 실제 거리에 가 있는 것처럼 보여주는 스트리트뷰 서비스를 전세계 30여 국가에 제공하면서 주변의 사람 모습, 자동차 번호판 등을 그대로 노출해 사생활 침해 논란에 휩싸였다. 이에 따라 그리스와 스위스의 개인정보 감독당국은 2009년 현지 도시들에 대한 영상 촬영을 금지하거나 자국의 거리 영상을 삭제할 것을 요구했다. 2010년 초에는 개인의 무선인터넷(Wi-Fi) 정보까지 수집한 사실이 알려지면서 그 해 8월 한국 경찰의 압수 수색을 받기도 했다.

구글은 2010년 5월 공식 블로그를 통해 이런 사실을

인정하면서도 수집된 개인정보를 활용하지 않았고 검색 엔진 등 다른 서비스를 통해 공개한 적도 없다고 해명했다. 현재 한국을 비롯한 미국·독일·호주 등 세계 16개국에서 조사가 진행되고 있다.

2.3 구글의 무선통신 이용정보 수집

경찰청 사이버테러대응센터는 2011년 1월 작년 8월 구글코리아 사무실을 압수수색할 때 확보한 하드디스크의 암호를 해독해 개인정보를 무단수집한 혐의를 확인했다고 밝혔다. 경찰은 2, 3개월에 걸쳐 구글 하드디스크의 암호를 풀고 저장된 정보를 분석한 결과 무선인터넷(Wi-Fi)을 통해 오고간 수십만 건의 개인정보가 본인의 동의 없이 수집된 사실을 확인했다. 구글은 스트리트뷰의 한국 서비스를 위해 2009년 10월부터 2010년 5월까지 서울 등 주요 도시의 거리를 촬영한 바 있다. 이때 거리 풍경사진과 함께 거리 주변 무선랜 접속장치(AP)의 시리얼 번호 등을 수집하면서 e메일 등 개인정보를 무단으로 확보한 것으로 보인다.

경찰은 2010년 12월 한국계 미국인 등 구글 본사 실무진 4, 5명을 한국으로 소환해 조사하고, 본사 임원 여러 명도 e메일을 통해 조사했다. 경찰은 검찰에 기소 의견으로 사건을 송치하였다. 미국 등 다른 나라에서도 구글 개인정보 수집과 관련한 조사가 진행되고 있지만, 수사기관이 혐의를 입증해 기소 단계까지 나간 것은 한국이 사실상 처음이었다.

2.4 페이스북의 회원 추천 서비스

국내 가입자 수가 이미 2백만 명을 넘어선 페이스북(Facebook)은 가입자가 요청하지 않았는데도 그가 알 만한 다른 회원들의 명단을 사진과 함께 서비스하고 있다. 화면 오른쪽에는 가입자 별로 개인정보를 분석해 맞춤형 광고를 게시한다. 방송통신위원회는 2010년 12월 페이스북이 이러한 서비스를 제공을 하면서 개인정보를 수집한다는 고지를 제대로 하지 않았고 동의 절차도 미비하다는 점에서 한국의 개인정보보호 수준을 충족하지 못했다며 관련 자료의 제출 및 제도개선을 요구했다.

이에 대해 페이스북은 가입자정보는 스스로 통제하는 것이 가장 중요하다는 답변을 보내 왔다. 페이스북이 회원가입 시 개인정보활용 동의 절차를 명시, 인터넷 게시판의 본인확인제 등 국내법 준수를 약속하지 않는 이

상 페이스북이 추진하고 있는 국내 법인설립은 다소 지체될 전망이다.

2.5 구글과 다음의 위치정보 수집

경찰은 2011년 5월 구글과 다음이 스마트폰 사용자의 위치정보(location information)를 무단으로 수집한 혐의를 잡고 이들의 사무실을 압수수색했다. 일각에서는 경찰이 최근 일부 스마트폰 앱(application) 개발업체의 불법 위치정보 사용을 적발하면서 무리하게 수사를 확대하고 있다고 말했다. 미국에서는 지난 4월 애플이 아이폰 트래커라는 프로그램을 통해 사용자들의 위치정보를 추적해 온 사실이 CNN 인터넷판 보도를 통해 알려졌다. 이미 애플은 위치서비스 질 향상을 위해 아이폰의 위치정보를 익명의(anonymous) 형태로 전송받고 있다는 사실을 고지하였음에도 실제 지도 위에 촘촘히 표시된 자신의 궤적을 눈으로 확인한 사용자들은 불안감을 감추지 못했다.

애플과 구글, 다음은 전송된 위치정보는 모두 익명이며 스마트폰 내의 데이터베이스 파일을 오래 저장하지 않는다고 해명했지만,¹⁾ 익명성이 보장되지 않을 경우 발생할 수 있는 프라이버시 침해에 대한 우려는 여전히 남아 있다. 구글과 다음의 압수수색 역시 익명의 위치정보가 아니고 개인별 식별이 가능한 위치정보 수집으로 인한 법률 위반 혐의를 염두에 둔 것으로 보인다.

Ⅲ. 글로벌 인터넷사업자에 대한 규제방안

3.1 개인정보 규제-감독의 딜레마

세계적인 인터넷사업자가 새로 론칭하는 인터넷 기

1) 위치정보 서비스의 내용은 크게 위치정보 사업자인지 혹은 위치기반 서비스 사업자인지에 따라 달라진다. 위치정보 사업자는 위치정보를 수집해 위치기반 서비스 사업자에게 제공하는 사업을 영위한다. 즉 위성항법장치(GPS) 등 측위장비를 이용해 위도와 경도 등의 위치좌표값을 직접 수집하는 한편, 이를 위치기반 서비스 사업자에게 제공하는 사업자를 의미한다. 한편 위치기반 서비스 사업자는 자체적으로 위치정보를 수집하지는 못하지만, 위치정보사업자로부터 위치정보를 제공받아 이를 기반으로 서비스에 활용하는 사업자이다. 위치정보 사업자는 방통위로부터 허가를, 위치기반 서비스 사업자는 방통위에 신고를 해야 하며 각각 이용약관에 명시한 뒤 이용자로부터 동의를 얻어야 한다.

반 서비스나 상품이 이를 출시한 나라의 개인정보보호 법제를 따라야 함은 물론이다. 그렇다고 관련 법규를 위반하였다고 무조건 규제를 가할 수도 없는 실정이다. 법 집행을 위해서는 문제가 된 서비스나 상품이 위법임을 입증하는 것도 쉽지 않거니와 해당 서비스나 상품이 수행하는 사업 자체를 위축시킬 수 있기 때문이다. 최근 무한한 발전 가능성을 보여주고 있는 소셜네트워크 서비스, 위치기반 서비스가 이에 해당한다.

위치기반 서비스를 예로 들어보자. 어느 스마트폰 사용자가 도심 변화가에서 길을 찾는 검색 서비스를 이용하였을 때 그의 라이프스타일을 고려한 쓸 만한 상품이나 가볼 만한 업소를 추천하는 것은 그에게 매우 유용할 수 있다. 그러나 어떻게 그의 취향을 알고 이렇게 추천할 수 있을까 생각해보면 누군가 그의 라이프스타일과 행동 패턴을 꿰뚫어 보고 있다는 오싹한 느낌을 갖게 될 것이다. 이와 같이 새로운 정보통신 서비스는 개인정보의 침해 가능성과 관련산업의 발전 가능성 사이에서 매우 어려운 선택의 문제를 제기하는 경우가 많다. 프라이버시 침해에 따른 규제의 칼을 드는 순간 새로운 서비스 산업의 싹을 자르는 결과를 가져올 수 있기 때문이다.

가장 바람직하기는 첨단 산업의 발전 가능성을 간직하면서 개인의 사생활의 자유를 침해하지 않도록 일정한 선을 그어 놓고 관련 인터넷서비스 사업자들로 하여금 이를 준수하게 하는 일이다. 이를테면 새로운 질서를 형성하기 위해 인터넷사업자와 감독기구가 서로를 ‘길 들여 가는’ 과정²⁾ 이라고 할 수 있다.

3.2 개인정보 침해 책임의 소재

경찰은 구글코리아에서 압수한 750GB 상당의 하드 디스크에 저장된 데이터를 해독한 결과 스트리트뷰 정보의 제작 과정에서 분명히 위법사실이 있다는 수사결과를 발표했다. 이에 따라 검찰에서도 구글 본사의 고위 책임자를 형사처벌하기로 방침을 정했다(실제로는 책임자 확인이 어려워 기소중지). 이와 유사한 사안을 심리 하였던 미 연방법원 샌프란시스코 지방법원은 2011년 6월 29일 “구글의 스트리트뷰 제작 과정에서 개인정보 수집이 도를 넘었으며, “암호화되지 않은 와이파이에 노출된 정보라도 도청금지법(the Wiretap Act)의 보호를 받는다”고 판시하였다. 재판부는 “암호화 처리가 안된 무선 인터넷 데이터는 누구나 수신하는 라디오 방송

과 같다”며 집단소송 청구를 기각해 달라는 구글 측 주장을 배척하고, “구글이 와이파이망의 정보를 수집, 해독하려고 장비를 동원한 것은 위법”임을 인정하여 이 사건을 정식재판(full trial)에 회부하였다.

구글 본사에 책임이 있음을 확인하였다면 현장에서 스트리트뷰 정보를 수집·제작한 실무자를 처벌할 게 아니라 본사의 고위급 임원을 한국 법정에 세우고 사법처리해야 마땅하다²⁾. 구글 코리아는 압수수색을 당하였지만 법적으로 구글 본사와 독립된 법인인 테다 사업목적상 처벌대상으로 삼기 어렵다. 그렇다면 실정법적으로 확대관할법(Long Arm Statute)³⁾을 시행하고 있는 미국과는 달리 우리나라에서는 해당 책임자로 하여금 꼼짝없이 한국 법정에 서게 하거나 당해 법인에 책임을 지우는 법논리를 개발할 필요가 있다.

전통적으로 법인을 앞세워 위법을 자행한 배후의 실세에 책임을 묻기 위해 여러 가지 이론이 제시되었다. 분신(alter ego)이나 도구(mere instrumentality) 이론, 이에 바탕을 둔 법인격 부인(disregard of corporate entity, “Piercing the corporate veil”) 이론이 그것이다⁴⁾. 종래 외국 기업의 국내 활동에 대하여는 국내에 영업소 등 고정 사업장(permanent establishment)이 없으면 효과적으로 제재를 가할 수 없었다. 국제거래법에서는 실제 위법행위자가 본사의 대리인(agent), 분신, 도구처럼 행동한 사실이 있으면 본사에 제재를 가할 수 있다고 본다.

사이버공간에서는 대리인, 분신, 도구로 볼 수 있는 실제 위반행위자(real law breaching actor)가 없는 경

우가 많다. 구글의 스트리트뷰 사건에서처럼 위반행위를 지시한 책임자가 해외에 거주하며 수사에 불응하는 경우에는 구성요건상의 행위자를 확정하기도 곤란하고 기소 등 사법처리가 어려워진다. 그렇다고 개인정보를 침해하는 사태가 사이버공간에 만연함에도 이를 처벌할 수 없다면 법집행(law enforcement)의 공백상태가 벌어지고 만다. 이것이 새로운 이론이 필요한 소이(所以)이다.

3.3 ‘아바타 이론’의 제안

2009년에 개봉되어 전세계적으로 흥행 돌풍을 일으킨 제임스 카머런 감독의 영화 <아바타(Avatar)>가 그에 대한 답을 시사하고 있다.

아바타는 분신과는 달리 독자적인 사고능력이 전혀 없고, 본인이 콘트롤 유닛에서 나오면 더 이상 도구로서의 기능을 수행할 수 없다. 그러나 영화에서는 나비 죽이 대대로 살아 온 낙원 ‘판도라’가 탐욕스러운 지구인들에 의해 파괴될 위기에 처하자 아바타들도 그를 조종하는 사람들과 한 몸이 되어 나비 죽 전사들과 힘을 합쳐 아름다운 낙원을 지켜내는 장면을 보여준다. 이러한 장면의 전개를 사이버공간에 대입해 보면 그 솔루션이 자명해진다.

외국에 실체가 있는 대리인이나 분신·도구에 해당하는 조직에 의하지 않고, 정보통신망을 통해 독자적인 사고·판단능력이 없는 아바타를 일일이 콘트롤하는 것은 글로벌 인터넷사업자가 사업을 영위하는 방식과 흡사하다. 해외 현지에서 개인정보를 침해하는 상황이 벌어질 경우에는 아바타가 본사의 책임자와 일체가 되어 행동하는 것으로 볼 수 있다. 따라서 죄형법정주의의 원칙상 본사의 책임자가 누구인지 특정하지 않고서도, 해외 현지에서 벌어지는 개인정보 침해의 현상에 대하여 아바타와 그를 조종하는 본인을 한 몸(一體)으로 보아 책임을 물을 수 있는 것이다.

이를 글로벌 인터넷사업자에 대하여 적용하기로 한다면, 다음과 같은 요건이 구비되어야 할 것이다. 즉, ① 본인이 우리나라에 현존하지는 않더라도 사이버 공간에서 국내에서 그의 활동결과로 볼 수 있는 침해행위가 있을 것, ② 우리나라에서 중대한 프라이버시권을 침해하고 그 결과 회복할 수 없는 피해가 발생할 것, ③ 본인이 빠지면 아바타도 행동을 멈추는 등 본인과 아바타를 한 몸으로 볼 수 있을 것 등이다.

구체적으로 글로벌하게 소셜네트워크 서비스를 영위

- 2) 이와는 달리 프랑스의 개인정보감독기구(CNIL)는 2011.3.21 구글이 스트리트뷰를 제작하면서 수집한 개인정보가 위법임을 확인하고 세계에서 처음으로 구글에 10만유로(약 1억5천만원)의 벌금을 부과했다. 네덜란드 개인정보감독기구(CBP)도 2011.4.19 구글에 대하여 같은 혐의를 놓고 본인에게 개인정보를 수집하였으니 본인이 원하면 DB에서 제외(opt-out)할 수 있다는 것을 알도록 하고, 이에 불응하면 최대 1백만 유로의 과태료를 부과한다는 행정명령을 발하였다.
- 3) 일례로 뉴욕주 소송법(2006 New York Code) 제302조(Personal Jurisdiction by Acts of Non-domiciliaries)은 다음과 같은 경우에 인적 재판관할을 확대하고 있다. ① 피고가 재판지에서 사업의 영위(doing business)를 넘어서는 사업상의 거래(transaction of business)를 하였을 것, ② 재판지에서 불법행위에 해당하는 행동(tortious act)을 하였을 것, ③ 재판지 밖에서 불법행위가 자행되었을지라도 재판지 내의 사람이나 재산에 손해(injury)를 끼쳤을 것, ④ 재판지 내의 부동산을 소유·이용 또는 점유하고 있을 것.

하는 인터넷사업자가 한국에서도 영업거점 없이 서비스를 개시하였다고 하자. 이 SNS사업자가 본인의 동의 없이 개인정보를 수집, 이용하고 이를 광고와 같은 영업 활동에 이용하고 있다면 이는 국내에서 아바타를 통해 위법행위를 자행한 것이라 볼 수 있다. 그러므로 이러한 상황에서는 국내에서의 아바타를 조종하였던 본사의 임직원을 그의 비협조로 특정할 수 없다 할지라도 최종적인 감독책임이 있는 본사 법인의 책임은 물을 수 있다고 본다⁴⁾. 만일 법원에서 이러한 ‘아바타 이론’을 수용한다면 국내에서도 형사처벌을 하는 데 아무 문제가 없다고 생각한다. 다만, 개인정보를 침해하는 행위로 인하여 정통망법(2011.9.30 이후에는 새로 제정된 개인정보 보호법)에 규정된 벌칙을 적용하는 경우 책임자에 대한 징역형이 아니라 본사 법인에 대한 벌금형이 부과될 것이다⁵⁾.

IV. 결 론 - 국제적 협력의 필요성

위에서 말한 아바타 이론이 얼마나 실효성이 있는지 알아보기 위해 앞서 소개한 2010년 이후 글로벌 인터넷 사업자의 개인정보 침해 사례에 하나씩 적용해보기로 한다.

첫 번째, 구글의 버즈 서비스에 기존 Gmail 이용자들의 이메일 주소를 본인의 동의 없이 제공하는 것은 구글이 국내 현지법인을 통하지 않고 본사에서 직접 서비스하는 사업이다. 그렇지만 본인의 동의를 얻는 절차가 미흡하여 기존 Gmail 이용자들이 자동적으로 버즈의 회원이 되는 폐단이 있다. 이 경우 개인정보를 어떻게 침해하였는지, 본인에게 무슨 위해가 가해졌는지 다툼이 있을 수 있으므로⁶⁾ 우리 개인정보 감독당국에서는

우리나라에서 버즈 서비스를 하는 경우에는 반드시 현행법상의 본인 동의 절차를 거치도록 서비스 방법의 개선을 촉구하여야 한다.

두 번째, 구글맵의 스트리트뷰 서비스는 구글 측이 스트리트뷰 제작차량이 현재 위치를 확인하기 위해 Wi-Fi 정보를 수집한 것일 뿐 수집된 개인정보를 활용하지 않았고 검색엔진 등에 노출시키지 않았다고 항변하고 있다. 그러나 이러한 정보가 사고로 유출될 수도 있고, 회사의 비공개 방침이 바뀔 수도 있으므로 구글이 법 규정에 위반하여 개인정보를 수집하였고 문제가 된 개인정보를 보관하고 있는 사실이 달라지는 것은 아니다. 현재 이 문제를 조사하고 있는 16개국 당국자들이 수사정보를 교환하고 공유함으로써 구글 측의 정보수집 의도를 파악하고 그로 인해서 어떠한 법익이 침해된 것인지 감독기구와 법원에 명백히 입증할 수 있어야 한다.

세 번째, 페이스북 회원 추천 서비스도 가입자에게 무슨 위해가 가해졌는지, 그것이 회복할 수 없는 손해의 수준인지 여부가 다투어질 수 있으므로, 이 문제는 첫 번째 구글 버즈 케이스에 준하여 생각하면 될 것이다.

네 번째, 구글과 다음의 위치정보 수집 사례는 인터넷사업자가 수집한 정보가 과연 익명으로 처리되어 있는지, 보관 중인 정보의 익명성이 깨질 경우에는 정보주체에게 무슨 위해가 가해질 수 있는지 사실관계부터 정확히 파악할 필요가 있다. 위의 스트리트뷰 케이스와 마찬가지로 여러 곳에서 행해진 개인정보수집 사례를 광범위하게 조사하여 사업자의 정보수집 의도를 파악하고 그로 인해 침해될 수 있는 보호법익을 입증할 수 있어야 한다⁷⁾.

그리하여 잘못을 저지른 글로벌 인터넷사업자에 대해

4) 이 경우 행위자, 즉 피고인을 특정하지 아니한 공소장 및 판결문이 유효한지 문제가 된다. 본사의 책임자를 특정하지 아니한 채 해외 현장에서 위법한 침해행위를 야기한 ‘성명 불상자’로 표기할 수도 있을 것이다. 그러나 최종적인 감독 책임이 있는 본사 법인을 피고인으로 하여 벌금형을 과할 수 있다고 생각한다.

5) 우리 법에는 벌칙에 양벌규정이 포함되어 있으나(정통망법 제75조, 개인정보보호법 제74조) 양벌규정이 없는 경우에는 매우 위력적인 법 운용이 될 것이다.

6) 서울고등법원은 2011.6.27 GS칼텍스 주유소의 1,150만 회원정보가 유출되어 정신적 피해를 입었다는 고객들이 집단 청구한 손해배상 소송의 항소심에서 GS칼텍스 측에 책임이 없다고 판결했다. 1심에 불복한 5천900여명이 GS칼텍스와 자회사 GS빅스테이션을 상대로 손해배상 청구소송을 제기

하였으나, 항소심 재판부는 "개인정보가 유출되어 자기정보 결정권이 침해됐다는 것만으로 바로 정신적 손해가 발생했다고 할 수 없다"며 "이는 개인정보의 종류나 성격, 유출정도 등을 고려해 개별적으로 판단해야 한다"고 밝혔다. 이어 "새나간 정보가 성명, 주민등록번호, 전화번호 등 개인 식별 정보일 뿐 사상, 신념, 정치적 견해나 금융정보 등 경제적 이익을 침해할 정보에 해당하지 않는 데다 유출 직후 바로 회수되어 구체적 피해가 발생했다고 인정하기 어렵다"고 덧붙였다.

7) 2011.7. 창원에서 어느 아이폰 사용자가 애플로부터 100만 원을 지급받은 사실이 알려지면서 이 사건을 수임한 변호사에게 소송을 신청하는 사람들이 몰려들었다. 그러나 이는 소송의 위차로 지급명령 신청에 애플이 불응하여 법원이 그 지급을 명한 것일 뿐 애플의 위치정보 수집행위가 위법하다고 판단을 내렸기 때문이 아니다.

여는 주요국의 개인정보감독기구들이 단합된 노력(concerted efforts)을 기울여 제재를 가하도록 한다. 인터넷 사업자로서도 한두 나라이면 버틸 수도 있겠지만 세계 주요국들이 일제히 포위공격을 한다면 결국 손을 들지 않을 수 없을 것이다.^[4] 우선 구글이 스트리트뷰를 제작 하면서 세계 각처에서 개인정보를 침해한 사건에서부터 위와 같은 국제적인 협력을 전개할 필요가 있다.

우리나라에서 새로 제정된 개인정보보호법에서도 “정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다”(제14조 2항)고 정부에 의무를 지우는 한편 관련 시책 중에 국제협력의 필요성을 예정하고 있다.^[5] 그러나 문제는 위와 같은 정부당국의 조치에 대한 해당 인터넷 사업자들의 반발이 만만치 않다는 점이다. 그러므로 앞에서 제안한 아바타 이론을 주장하기 위해서는 최근에 결성된 글로벌 프라이버시 집행 네트워크(Global Privacy Enforcement Network: GPEN)⁸⁾에 적극 참여하여 이를 본격 가동하여야 한다. 그리하여 주요국 개인정보 감독당국과 수사정보를 교환하는 등 국제적으로 긴밀한 협조체제를 구축할 필요가 있다.

G-8 차원에서도 이러한 국제협력의 필요성이 강조되고 있다. 개인정보침해에 대한 우려가 커질수록 인터넷에 대한 신뢰가 떨어져 인터넷 기반의 경제활동이 위축될 우려가 있으므로 프라이버시 문제를 최우선 과제로 논의하자는 움직임이 일고 있다. 이것은 비단 정부 차원의 문제만은 아니다.^[6] 인터넷사업자들도 지속가능한 산업발전을 위해서는 인내심을 갖고 낱알이 이용자 및 감독기구와 친밀해지도록 노력해야 하며,^[2] 개인정보보호 법제를 위반하지 않도록 스마트하게 기술개발을 하면서 각 기업의 프라이버시 정책을 완벽해 나가야 할 것이다.^[7]

8) GPEN은 프라이버시 집행에 관한 국제협력의 필요성을 강조한 OECD와 APEC의 권고에 따라 미 연방거래위원회(FTC)이 주도하여 2009년 가을 뜻을 같이 하는 캐나다, 프랑스, 뉴질랜드, 이스라엘, 호주(연방) 등의 관계기관과 국제협력 네트워크를 결성하기로 합의했다. 이에 참여한 13개국 대표들은 2010. 3. 10 파리에 모여 네트워크의 방향을 설정하고 GPEN을 출범시켰다. GPEN의 공식 웹사이트는 <<https://www.privacyenforcement.net/>>.

참고문헌

- [1] Laura Linkomies, “Privacy Commissioners form global enforcement group and warn Google,” Privacy Laws & Business International Report Issue 105, June 2010.
- [2] 박원일, “How to Tame Global ISPs,” 제35차 APPA 포럼 발표자료, 2011.6.3.
- [3] Laura Hundter Dietz, et al., “Alter ego or instrumentality theories,” 18 American Jurisprudence 2nd Ed., Corporations §51, March 2011.
- [4] L. Linkomies, “Google, Facebook face increased pressure from the regulators,” Privacy Laws & Business International Report Issue 110, pp.17-18, April 2011.
- [5] 박원일 역, “국경간 프라이버시 집행을 위한 APEC 협약”(CBEA), 국제법무연구, 15(1), pp. 201-202, 2011년 2월.
- [6] Christopher Wolf, “eG8 discusses privacy - a step forward in global cooperation,” Privacy Laws & Business International Report Issue 111, pp.10, July 2011.
- [7] 박원일, “E-Commerce and the Compliance Issue in Respect of Data Protection,” 경희법학, 45(3), pp.530, 2010년 9월.

<著者紹介>



박원일 (Park Whon-il)

중신회원

1975년 2월 : 서울대학교 법학과 학사

1977년 ~ 2000년 : 한국산업은행 근무

2000년 2월 : 경희대학교 대학원 법학과 박사(상법)

2000년 ~ 현재 : 경희대 법과대학 법학전문대학원 교수

2001년 ~ 현재 : KISA 자문교수 <관심분야> 국제거래법, 기업금융법, 프라이버시보호