

빅데이터 시대 개인정보 보호와 활용

페이스북과 EU의 공방



성선제
고려대 정보보호대학원 초빙교수
미국 변호사

1. 빅브라더 v. 빅데이터

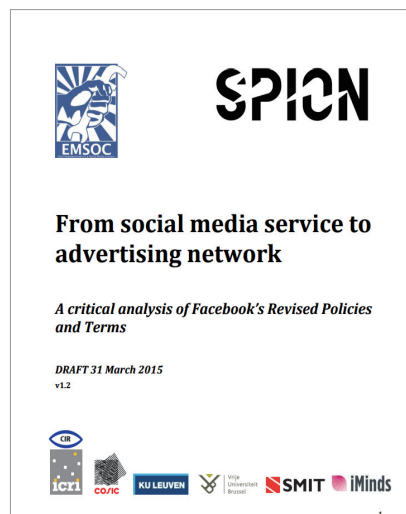
1,697시간 - 작년 우리 국민 한 사람이 디지털 세상에서 보낸 평균 시간이다. 하루 평균 4시간 40분이다. 잠자는 시간을 빼면 하루의 4분의 1이상이다. 컴퓨터 사용시간 평균 1시간, 음성통화를 제외한 스마트폰 사용시간 평균 3시간 40분이라고 한다. 갈수록 상상을 초월하는 디지털 세상이 될 것이다. 1,697시간 매 순간 우리는 디지털에 흔적을 남긴다. 흔적은 개인정보다. 당신이 남기는 개인정보로 누군가는 막대한 돈을 번다. 그런데 당신은 그 사실을 모르고 있다. 오히려 공짜로 사용할 수 있게 해 주었다고 고마워한다. 아이러니의 극치가 아닐 수 없다.

페이스북과 같은 빅데이터(Big Data)를 활용하는 글로벌 정보기술(IT) 기업의 개인정보 수집이 갈수록 정교해지고 있다. 빅데이터 시대가 도래하면서 비즈니스 분석 소프트웨어 시장이 급성장하고 있으며 페이스북은 정형 데이터보다 실시간 비정형 데이터를 기반으로 한 비즈니스 분석 수요를 증대시키고 있다. 빅데이터 시대가 열리면서 개인정보의 활용 가치가 높아지고 있으며, 이러한 데이터 수집 욕구 또한 증대되고 있는 것이다. 기업이 가공한 '소비자 데이터' 소유권을 누가 가질지, 기업에 남아 있는 '프라이버시' 관련 '소비자 데이터'를 삭제할 권리가 소비자에게 있는 것인지 등 다양한 이슈들이 새롭게 등장하고 있다. 스마트폰 확산으로 엄청난 양의 센서 및 소셜 데이터 등이 양산되고 컴퓨팅 기술 발전으로 개인정보에 대한 분석도 용이해졌다. 스마트폰은 이용자가 언제 어디에 있는지 실시간으로 파악한다. 어디서든 정보 수집이 가능한 센서, 주파수 등으로 데이터는 소비자가 전혀 인지하지 못하는 상황에서도 수집되고 활용된다. 또한 페이스북에 오늘 점심은 무엇을 먹었는지, 오늘 기분은 어떤지에 관한 짧은 글을 남기는 순간에도

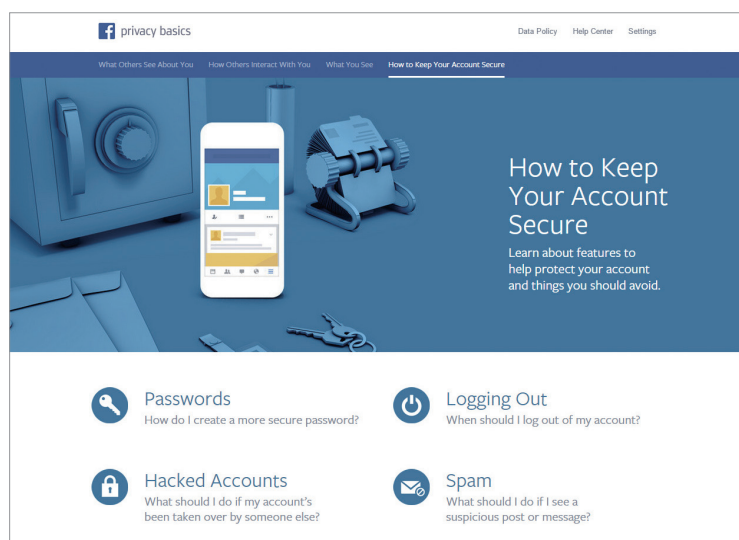
사람들의 위치 정보는 물론, 취향이나 습관, 검색 패턴, 구매 기록 등의 개인정보까지 살살이 알아낼 수 있는 막대한 양의 데이터가 차곡차곡 쌓이고 있다.

“만일 당신이 어떤 서비스를 공짜로 쓰고 있다면 당신은 고객이 아니라 ‘상품’이다.” 미국 인터넷 커뮤니티 ‘메타필터’ 이용자 ‘블루 비틀’이 2010년 언급해 유명해진 이 말은 이제 현실이 됐다. 스마트폰, 태블릿 PC 등 모바일 기기를 통해 어디서나 정보를 검색할 수 있고, SNS에 접속해 지인과 연락을 주고받는 편리한 시대지만 ‘빅브라더(Big Brother)’의 감시는 한층 촘촘해지고 있는 것이다. SNS 이용자들은 “온라인에서 행동 하나하나가 관찰당하는 기분”이라며 불쾌감을 드러내고 집단소송을 제기하기에 이르렀다.

페이스북과 더불어 구글도 그동안 광고 목적의 개인정보 침해 혐의가 꾸준히 제기됐다. 구글은 2013년 11월 애플의 사파리 브라우저를 통해 개인정보를 수집했다는 혐의로



지난 3월 31일 공개된 벨기에 연구진의 보고서. 이 보고서에 따르면, 페이스북은 회원이 아닌 이용자들의 웹 브라우저 이용 경로까지도 동의 없이 추적했다. (출처: 『가디언』, “Facebook ‘tracks all visitors, breaching EU law’”, 2015년 3월 31일자 및 벨기에 루뱅 대학 홈페이지)



페이스북 내 개인정보 관련 안내 웹페이지(출처: 페이스북 홈페이지)

미국 37개 주정부로부터 1,700만 달러의 벌금이 부과되었다. 페이스북은 2013년 10월 사용자가 특정 광고나 게시물을 클릭하지 않고 마우스만 올려놔도 커서의 움직임을 분석해 기록을 남기는 기술을 개발하고 있다는 의혹을 받았다.

페이스북은 약관을 통해 이용자로부터 포괄적인 정보 제공 동의를 얻지만 실제로 어떤 개인정보가 어떻게 쓰이고 있는지는 공개하지 않고 있다. 페이스북의 개인정보 제공 동의 절차가 지나치게 포괄적이고 추상적이라는 비난이 쏟아지는 이유이다. 이 같은 불만에도 페이스북은 개인정보 침해 의혹에 대해 이용자에게 동의를 얻었기 때문에 문제가 없다는 입장을 고수하고 있다.

점차 개인 맞춤형 광고의 중요성이 부각되면서 명확한 개인 동의를 거치지 않고 개인 정보를 수집할 수 있는 이른바 ‘꼼수 기술’에 대한 관심은 점차 높아지고 있다. 앞으로 정보제공 동의 절차가 충분히 엄격한 수준인지, 소프트웨어가 정보를 스캔하는 것을 모니터링에 포함시켜야 하는지 등의 쟁점을 둘러싸고 논란이 점차 거세질 전망이다.

이런 가운데 지난 4월 9일 유럽 내 페이스북 법정 공방이 새로운 국면을 맞았다. 비엔나 지방법원에서 페이스북을 상대로 한 민사소송 공판이 열린 것이다. 페이스북 법정 공방은 갈수록 정교해지는 빅데이터 활용에 대한 이용자 불신이 끓아 터진 대표적인 사건이다. 2만 5천여 명의 집단소송단이 페이스북을 상대로 제기한 이 소송은 오스트리아 법대생 막스 슈렘스가 문제를 제기하면서 시작되었다. 그는 2011년 페이스북이 자신의 개인정보를 EU 법에 맞게 활용하고 있는지 궁금해 페이스북에 자신의 개인정보 이용목록 열람을 요청했다. 우편으로 받은 내역은 수천 쪽에 달했다. 이후 세계에서 비슷한 요청이 쇄도하면서 페이스북은 현재의 자동화된 개인정보 내려받기 시스템을 만들었다. 소송을 제기한 원고들은 소장에서 “이용자들의 개인정보가 페이스북의 수익창출



페이스북에 개인정보 문제를 제기한 막스 슈렘스

(출처: 『로이터』, "25,000 angry users: Facebook privacy class action lawsuit to be heard by European court", 2015년 1월 27일자)

기회를 제공한다.”며 “감시당하는 걸 알았다면 드러내지 않았을 정보들”이라고 주장했다. 이러한 현상에 대해 에릭 클레먼스 펜실베이니아대 와튼 스쿨 교수는 “법은 기술보다 늦기 때문에 이용자들이 스스로 정보 공개 현황을 체크해야 한다.”며 “눈을 감고 있으면 침해는 더 커질 것”이라고 경고한 바 있다.

여기에서는 정보 프라이버시(Data Privacy) 관련 현황과 쟁점을 다뤄보고자 한다. 쟁점과 관련하여 프라이버시에 관한 미국과 EU 법체계가 어떻게 다른지, 페이스북의 정책이 유럽 내에서 위법한지 등을 구체적으로 살펴보고, 이번 페이스북 개인정보 관련 사건의 전개 및 그 속에서 페이스북과 유럽의 입장차, 빅데이터 시대에 필요한 개인정보 보호정책에 대한 방향성 등을 다뤄보고자 한다.

2. EU 프라이버시법제

유럽연합(이하 EU) 개인정보보호법제는 「1995년 유럽연합 개인정보보호지침(The Data Protection Directive of the European Union)」이 핵심이다. 이 지침은 EU 회원국뿐 아니라 전 세계 개인정보보호법제의 발전을 가져오는 원동력이 되었다. 물론 EU 개인정보보호지침의 채택 이전에도 각국에서 개인정보의 보호를 위한 법제도를 가지고 있었다. 그런데 이들 관련 국내법 규범은 개인정보의 보호라는 공통의 목적을 가지고 있었지만, 각 국가의 사정과 전통에 따라 다소 차이점을 가지고 있었다. 이러한 차이는 EU 회원국들 사이에서 정보의 자유로운 이전을 제한하게 되었고, EU의 공동시장 발전에 장애요인이 되었다. 이러한 현실을 개선하기 위하여 EU 차원의 통일된 개인정보보호를 위한 입법이 요구되었고, 그 결과로 개인정보보호지침이 제정되었다.

EU 개인정보보호지침의 적용범위는 매우 넓다. 이 지침은 온라인인지 오프라인인지 혹은 자동인지 수작업이 필요한지 여부를 불문하고 개인정보의 모든 처리에 적용된다. 또한 개인정보보호지침은 개인정보를 보유한 모든 기관에 적용된다. 또한 개인정보보호지침은 기술적으로 중립적이어서 개인정보의 처리에 사용된 기술적 수단에 상관없이 적용된다.

EU 개인정보보호지침의 주요 내용은 다음과 같다. 첫째, EU 개인정보보호지침은 전적으로 또는 부분적으로 자동화 수단을 통해 처리되는 개인정보에 적용될 뿐만 아니라 수작업 데이터에도 적용된다. 그러나 이 지침은 공공안전, 국방, 국가안보 및 형사법 분야의 회원국 활동에는 적용되지 않는다. 또한 이 지침은 가사활동에도 적용되지 않는다.

둘째, 개인정보 처리의 조건으로 정보주체의 동의를 규정하고 있다. 하지만 법적 의무를 준수하기 위한 경우, 정보주체의 핵심적 이익을 보호하기 위한 경우, 공공 이익을 위한 경우, 공적 권한의 행사를 위한 직무의 경우는 예외로 한다.

셋째, 개인의 민감 정보는 엄격한 조건하에서만 처리될 수 있도록 했다. 민족, 인종, 정치적 견해, 종교적·철학적 믿음, 노동조합 가입여부, 건강·성생활에 관한 정보, 법의 위반과 유죄판결에 관한 정보는 엄격한 조건하에서만 처리될 수 있다. 즉, 민감한 개인 정보의 처리에 대해서는 정보주체의 명백한 동의를 요구한다.

넷째, 정보주체의 권리를 폭넓게 인정하고 있다. 정보주체는 제약 없이 그리고 과도한 지연이나 비용을 들이지 않고 자신의 개인정보에 접근할 권리를 가진다. 또한 완전하지 않거나 정확하지 않은 데이터를 교정·삭제 또는 차단할 권리를 가진다. 정보주체는 개인정보의 처리에 반대할 권리를 가지며, 정당한 경우 처리를 중단시킬 수 있고, 또한 직접 마케팅의 목적으로 사용되는 개인정보에 반대할 권리를 가진다.

다섯째, 개인정보의 외국으로의 이전을 규정하고 있다. 일반적으로 타국가가 정보주체의 권리 보호를 보장하는 경우에 개인정보가 이전될 수 있다. 그러나 정보주체가 동의하거나 정보 이전이 계약 이행이나 공익 차원에서 법적으로 요구되는 경우에는 예외가 인정된다.

한편 EU는 급속도로 변화하는 IT환경에 부합하는 개인정보보호법제를 마련하기 위하여 이러한 지침(Directive)이 아닌 규정(Regulation)의 형태로 규제의 형식을 격상하고, 이른바 ‘잊혀질 권리’(Right to Be Forgotten)를 도입하는 등 개인정보 보호를 강화하는 것을 그 내용으로 하는 「2012 개인정보보호규정안」을 발표한 바 있다. 그 주요내용은 첫째, 개인정보관리기관 사전 등록제도의 시행이다. 관리기관이 개인정보를 처리하기 위해서는 반드시 사전에 동의를 취득하여야 한다. 둘째, ‘잊혀질 권리’를 도입하는 것이다. 자신의 정보가 불법적으로 인터넷에 공개된 경우, 해당 정보를 삭제하거나 추가로 공개하지 않도록 인터넷서비스제공자에게 요구할 수 있는 권리를 인정하는 것이다. 셋째, 개인정보관리기관으로부터 제3자에게 이전할 수 있도록 요구할 수 있는 권리를 인정하는 것이다. 자신의 정보를 저장장치에서 전자적으로 복제하여 얻을 수 있고, 개인정보관리기관으로부터 제3자에게 이전할 수 있도록 요구할 수 있는 권리(Right of Data Portability)를 신설하는 것이다.

3. 미국 프라이버시법제

미국의 개인정보보호제도는 1966년 정보공개법(Freedom of Information Act) 제정에 따라 연방정부가 보유하고 있는 정보를 원칙적으로 공개하되 1974년 프라이버시법(Federal Privacy Act)에 의해 정부에 대한 규제를 가하고, 민간부문에는 정보의 자유로운 유통을 보장하며 개별 분야에서의 개인정보보호를 목적으로 한 영역별 보호 법제를 가지고 있다는 점이 특색이다. 미국은 1974년 프라이버시법이 제정된 이래 1978년 금융

프라이버시법, 1986년 전기통신보호법, 1988년 컴퓨터 자료의 상호 비교 및 프라이버시 보호법, 1994년 전기통신 프라이버시법, 1996년 통신법 및 의료기록 비밀보호법을 각각 제정하였다. 생활영역별, 기술별로 개별법을 제정하여 개인정보를 보호한 것이다. 미국 개인정보보호법제의 특색인 영역별 방식에 따라 개인정보보호를 위한 많은 개별 법률이 제정되고 있는데 개별법의 장점은 특히 보호가 필요한 개인정보의 취급영역에 한정하여 법적 규제를 행하는 점이라고 하겠다. 그러나 단점으로는 개별 영역별로 법률을 제정하기 때문에 관련업체나 이익단체의 영향을 받을 수 있는 우려가 많다는 것이다.

민감 정보는 종교, 인종, 정치, 성 정체성, 건강, 노동조합 가입여부 등으로 이에 해당하는 데이터를 수집 또는 활용하기 원하면 데이터 제공자의 동의가 반드시 필요하다. 또한, 연방공정거래위원회는 데이터를 안전하게 처리 및 유통하지 않는 웹사이트, 데이터베이스 등의 매체에 대해서는 소비자보호법을 적용한다고 명시하고 있다. 연방공정거래위원회는 이미 오프라인과 온라인의 데이터 활용을 위반한 기업에 대해 규제를 가하고 있고 웹사이트에 개인정보보호방침이 없을 경우 불공정거래행위로 취급하여 이를 처리한다.

한편 미국은 국가정보통신기반 구축을 위해 정보통신기반 전담팀에 정보정책위원회를 구성하여 세 개의 팀을 두었는데 그 중 하나인 프라이버시 팀이 1995년 6월에 ‘프라이버시와 개인정보제공 및 이용의 원칙’을 작성했다. 이 원칙은 계약 자유에 따라, 제공자의 통지와 소비자의 동의라는 두 개의 필수조건을 감안하면서 업계의 자율적인 규제가 우선이라는 것을 강조하고 있다.

근래에 급속히 변화하는 IT환경을 반영한 개인정보보호법제의 대표적인 것은 오바마 행정부의 소비자 프라이버시 권리장전이다. 소비자 프라이버시 권리장전은 소비자 프라이버시 프레임워크의 핵심 내용이다. 오바마 행정부는 2012년 소비자 프라이버시에 대한 새로운 프레임워크를 발표하면서 그 배경을 “미국 소비자들은 그들의 개인정보가 안전하다는 확신을 줄 수 있는 명확한 규칙을 더 이상 기다릴 수 없는 실정이고, 더불어 인터넷이 발전함에 따라, 소비자의 개인정보관리에 대한 신뢰는 디지털 경제의 지속적인 성장에 필수적이라 할 것”이라고 설명했다. 특히, 디지털 시대에 신뢰유지는 온라인 상의 경제활동을 보호하는 것이며, 특히 소비자들의 신뢰를 높이기 위해 기술적·관리적 차원에서 개인 사생활의 보호가 매우 중요하다는 것을 천명하였다. 이는 오프라인을 기반으로 하는 시장 활동이 온라인 기반으로 전환되면서, 클라우드 컴퓨팅, 위치 기반 서비스 등을 중심으로 미국 경제활동의 패러다임이 전환되었고, 경제적 이익의 지속적인 유지를 위하여 소비자의 기술네트워크에 대한 신뢰를 확보하는 게 중요한 과제로 부각된 것을 보여준다.

소비자 프라이버시 프레임워크는 네 가지 요소로 이루어져 있다. 각각의 요소는 (1)

소비자를 위한 프라이버시 권리장전의 제정, (2) 인터넷 업체, 소비자 등 다양한 이해관계인의 합의를 바탕으로 한 소비자 프라이버시 권리장전에 부합하는 실효적인 법규의 제정, (3) 연방공정거래위원회의 법집행 강화, (4) 정보장벽을 낮추기 위한 세계 여러 나라와의 프라이버시 기준의 상호 운용성 고려이다.

네 가지 요소 중 가장 핵심인 소비자 프라이버시 권리장전의 주요 내용은 첫째, 자기 정보통제권이다. 소비자는 자기 자신에 대한 정보의 권리 주체로서, 개인정보 수집기관의 수집정보의 유형 및 이용방법 등에 관하여 통제권을 행사할 수 있다. 이에 대하여 기업은 개인정보의 권리자인 소비자가 쉽게 이용하고 접근할 수 있는 서비스를 제공하지만, 개인정보의 수집 및 이용에 관하여 소비자가 직접 선택할 수 있도록 지원하여야 한다. 최근에는 사생활 보호기능을 강화하는 ‘추적 금지(Do Not Track)’ 기술을 통하여 소비자가 자신의 개인정보를 통제할 수 있도록 지원하고 있다.

둘째, 투명성 강화이다. 소비자는 개인정보보호 및 보안실무에 관한 정보를 알 권리가 있다. 또한 소비자는 사생활 침해위험과 관련된 의미 있는 정보를 가장 적절한 시기에 제공받아 개인별 통제권을 행사할 수 있다. 이에 대하여 기업은 수집하는 정보, 이용방법, 삭제 등에 관한 설명을 제공하여야 하는데, 사생활 보호관련 서비스의 소비자 접근을 높이기 위하여, 인지하기 용이하며 효과적인 방법으로 제공하여야 한다. 특히, 최근 스마트폰의 발달로 인하여 스마트폰을 사용하는 경우가 많기 때문에, 이러한 특성을 고려하여 스마트폰 이용자를 위하여 정보의 제공방법을 효과적으로 제시하여야 한다.

셋째, 맥락의 존중이다. 소비자는 기업의 개인정보 수집·이용·공개가 일관된 맥락에서 이루어질 것을 기대할 권리가 있다. 기업은 소비자에게 사전 공지한 내용과 같은 방식으로 정보를 활용하되, 개인정보 공개를 최소화해야 하는 의무가 발생하게 된다. 만약, 기업이 개인정보를 목적 외로 이용하거나 공개할 경우 투명성 및 개인통제권의 침해로 간주하여 사건 발생 즉시 소비자는 기업을 고발할 수 있다. 따라서 기업은 소비자의 나이와 교양 수준 등에 따라 적절한 방침을 적용하도록 의무를 다해야 하는 것이다.

넷째, 접근성 및 정확성 강화이다. 소비자는 데이터의 민감도·위험도를 고려하여, 적절한 방법과 이용 가능한 형태로 개인정보에 접근하거나 이를 수정할 수 있는 권리가 있다. 한편, 기업은 합리적인 방법을 통해 개인정보를 보유 및 관리할 의무가 있다.

다섯째, 최소수집의 원칙이다. 소비자는 특정 기업의 개인정보 수집 및 보유에 관하여 합리적 제한을 할 수 있다. 이에 대해서 기업은 목적달성을 위한 최소한의 개인정보를 수집하여야 하며, 목적이 달성된 개인정보는 안전하게 삭제하여야 한다.

여섯째, 책임성 강화의 구현이다. 소비자는 기업이 소비자 개인정보 인권선언을 준수하며, 소비자의 개인정보를 적절한 방법으로 처리하도록 요구할 권리가 있다. 이에 대하여 기업은 정부와 소비자가 해당 개념의 권리를 시행할 수 있도록 할 의무가 발생한다.

다. 기업은 직원이 해당 개념의 책임이 있음을 숙지시켜야 하며, 이에 따른 개인정보 취급이 이루어지도록 교육하고 평가하여야 한다. 또한 개인정보 침해사고의 발생 시, ‘책임’의 개념에 따라 계약상의 의무를 다하지 못하였기 때문에 기업은 법적인 처벌을 받을 수 있다.

위에서 언급한 소비자 프라이버시 권리장전을 구체화하기 위하여 연방공정거래위원회는 인터넷상에서 방대한 양의 개인정보를 자신도 모르게 노출하고 있는 인터넷 이용자들의 프라이버시를 보호하고자, 2012년 ‘급속한 변화의 시대에 맞춘 소비자 개인정보 보호’라는 제목의 보고서를 발간하였다. 연방공정거래위원회는 이 보고서를 통하여 사업자가 이용자의 개인정보보호를 위해 적용해야 하는 구체적인 프레임워크 및 개인정보정책 마련에 필요한 권고안을 제시하고 있다.

그 주요 내용은 첫째, 추적금지 옵션 제공을 의무화하고 있다. 여기서 추적(Tracking)이란 인터넷 이용자의 행동 및 구독 습관의 기록을 공간, 가상공간, 시간과 연결시킬 수 있는 정보를 습득하는 것을 말한다. 사업자는 추적을 통해 소비자의 개인정보를 임의로 가공하여 사업자 간 일종의 상품으로서의 가치를 가질 수 있을 만큼 발전시킬 수 있으므로 개인정보의 중요성이 갈수록 커져가고 있다. 이것은 인터넷 이용자와 사업자 간의 수·발신 정보의 대응방법을 정책적으로 다루기 위한 조항이라 할 수 있다. 추적금지 옵션 제공의 의무화는 이용자들이 직접 개인정보 추적 수준을 제한할 수 있도록, 브라우저 벤더들(Browser Vendors)들에게 추적 금지 옵션을 제공할 것을 의무화하는 것이다. 추적금지 옵션은 이용자가 개인정보 수집을 거부할 선택권을 갖는 시스템이며 이용자가 자신의 개인정보 추적 수준을 제한할 수 있는데, 이에 대해 페이스북, 구글 등 주요 기업은 추적금지 버튼을 도입하였다. 기술적 측면을 살펴보면, 이용자가 웹을 통해서 정보를 송수신할 때, 컴퓨터 요청문에는 헤더(Header)라고 불리는 작은 정보를 가지게 되는데, 이 헤더는 이용자가 이용하고 있는 웹브라우저, 이용자 컴퓨터의 언어설정, 그 외 기술적 세부정보들을 포함하고 있다. 추적금지는 이 헤더에 컴퓨터 언어로 “Do-Not-Track”이라는 의사표시의 내용을 포함하여, 이용자가 원할 경우 원클릭 버튼을 통해 이용자 본인의 이용내역을 추적하지 않도록 하는 명령문을 실행하는 것이다.

둘째, 기업에게 ‘프라이버시 중심 디자인’(Privacy by Design) 도입을 촉구하는 것이다. ‘프라이버시 중심 디자인’은 개인정보보호 설계 단계부터 이용자의 프라이버시를 고려해야 한다는 개념으로서, 개인정보보호를 위한 설계 단계에서 기업이 서비스·상품의 성격 및 개인정보 주기를 반영한 취급방침을 마련하고, 개인정보취급방침을 통해 개인정보의 기술적 보호, 최소한의 정보 수집, 목적에 합당한 보유 기간 설정, 개인정보 파기 방침 설정, 정확성의 유지 등을 보장하도록 하고 있다.

셋째, 이용자의 선택권을 강화하는 것이다. 개인정보의 수집·수집 목적 외 이용·특정 목적을 위해 이용자의 민감 정보를 수집할 경우에, 이용자의 동의를 구해야 하고, 기업은 이용자에게 강요하지 않고 선택권을 보장해야 한다는 내용을 담고 있다. 또한 행태 정보를 수집하는 사업자는 추적금지 기술과 같이 이용자가 정보수집 여부를 선택할 수 있는 시스템을 제공하여야 한다.

넷째, 데이터 브로커를 규제하는 것이다. 정보 수집에 대한 투명성 강화를 위해 중앙 집권적으로 관리할 수 있는 웹사이트를 만들어 데이터 브로커들의 정체를 공개하고 이용자의 개인정보를 수집하는 방법 등에 대해 밝힐 것을 요구하였다. 또한 이용자 개개인이 데이터 브로커가 수집한 정보에 접근할 수 있도록 하여 줄 것을 의회에 요청하였다.

다섯째, 자율규제의 시행을 추진하는 것이다. 보고서에서는 기업과 개인정보보호를 주장하는 시민단체가 자율규제 시행을 위한 기준을 마련할 것을 요구하고, 이것이 마련되면 연방공정거래위원회는 이것이 집행될 수 있도록 최대한 돕는 것을 촉구하였다.

여섯째, 개인정보취급방침의 투명성을 증진하는 것이다. 기업은 이용자에게 개인정보취급방침을 고지함에 있어서 명확하고, 간결하며, 표준화가 되어 있어야 한다고 권고하고 있다. 특히 표준화에 대하여 연방공정거래위원회는 각 산업 분야별 수집 정보의 다양성을 인정하지만, 정보주체인 이용자의 명확한 이해를 위하여 상무부 주도아래 개인정보 관련 용어 및 취급방침의 표준화에 대하여 논의를 진행하기로 했다. 또한 개인정보 성격에 따라 다른 접근권을 보장하도록 하였다. 이에 대해 연방공정거래위원회 보고서는 3가지 형태로 나누어 설명하고 있는데, 먼저 상품 및 서비스를 제공하는 업체의 경우에는 이용자의 개인정보에 대해 자신들이 수집하고 보관하고 있는 개인정보의 리스트를 공개하도록 하고 있다. 다음으로 은행·보험·고용 등 업무적으로 이용하는 경우에는 이용자에게 자기 정보 접근 및 정정 요구권 등을 보장하도록 하고 있다. 마지막으로 최근 급격하게 시장이 커진 SNS나 검색 엔진 등의 경우에는 사업자가 이용자에게 수집하는 정보의 종류 및 수집 경로를 공개하도록 권고하고 있다.

4. 페이스북 v. EU 개인정보 소송 공방

EU와 미국은 개인정보를 대하는 관점이 기본적으로 다르다. EU는 개인정보를 정보주체 자신이 처분하는 것에 한계가 있는 권리로 바라보지만, 미국은 개인정보를 정보주체 자신이 전적으로 처분할 수 있는 권리로 바라본다. 또한 EU의 개인정보보호법제는 전통적으로 공공영역과 민간영역의 개인정보보호 처리절차를 하나의 법에서 다룬다. 반면

미국의 개인정보보호법제는 생활영역별, 기술별로 개별법을 제정하여 규율하고 있다.

우리는 IT 서비스에 가입할 때 반강제적으로 개인정보를 제공하지만, 정작 내 정보가 어떻게 쓰이는지는 알지 못한다. 권리가 침해되어도 그 사실을 알 수 없다면 권리를 지킨다는 것은 원천적으로 불가능하다. 이번에 문제가 된 페이스북은 북미 지역을 제외한 모든 국외 이용자와의 계약을 ‘페이스북 아일랜드’가 맺는다고 밝히고 있다. 즉 페이스북의 개인정보 제공 정책은 EU의 법을 따른다. EU 개인정보보호지침은 개인정보 처리의 조건으로 정보주체의 사전 동의를 의무화하고 있다.

페이스북이 행태 정보를 수집하기 전에 이용자에게 명시적 동의를 구하지 않은 점은 EU 실정법 위반에 해당할 가능성이 크다. 정보주체가 당사자인 계약의 이행에 필요한 경우, 법적 의무를 준수하기 위한 경우, 정보주체의 핵심적 이익을 보호하기 위한 경우, 공공이익을 위한 경우 또는 공적권한의 행사에서 수행되는 직무를 이행하기 위한 경우, 정보관리자의 정당한 이익을 충족하기 위한 경우로서 정보주체의 이익 또는 기본권과 자유가 이러한 이익에 우선하는 경우 등 정보주체의 사전 동의 예외사항에도 해당되지 않기 때문이다.

국내법으로 보면 어떻게. 페이스북이 소셜 위젯을 통해 비회원의 행태 정보를 수집한 것이 국내법에도 저촉될 소지가 크다. 이용자에게 명시적인 동의를 구하지 않고도 데이터를 수집할 수 있는 경우는 두 가지이다. 첫째, 약관에 동의하는 것처럼 명시적으로 동의하지 않더라도 묵시적으로 동의한 경우이다. 예를 들면 웹사이트 방문자에게 “이 웹사이트를 계속 이용하면 우리 약관에 동의하는 것”이라고 알려주는 경우가 이에 해당한다. 국내 대다수 웹사이트는 이런 방법을 쓴다. 첫 페이지에 보여주지 않더라도 이용 약관을 들여다보면 이런 문구를 적어둔다. 대다수 웹사이트가 쿠키를 쓰는 상황이니 웹사이트를 이용하는 것만으로 쿠키를 심고 이걸 활용해 행태 정보를 수집하는 데 동의했다고 여기는 것이다.

하지만 이런 상황에도 페이스북의 정보 수집이 묵시적 동의를 얻었다고 보기는 어렵다. ‘facebook.com’ 도메인을 쓰는 웹사이트에 접속했을 때 페이스북이 정보를 수집하는 경우에는 묵시적 동의를 얻었다고 볼 수도 있다. 하지만 페이스북은 소셜 위젯을 심은 외부 웹사이트에서도 정보를 수집했다. 예를 들면 『언론중재』 웹사이트에 들어온 독자가 『언론중재』 기사를 읽으면 페이스북에도 자기 정보가 흘러간다는 사실을 알고 묵시적으로 동의했다고 해석하기는 힘들기 때문이다.

둘째, 정보처리자가 얻는 이익이 정보 주체 이익보다 훨씬 큰 경우이다. 법률 용어로 ‘이익형량’이라고 한다. 두 주체 또는 법률의 이익이 충돌하는 경우 어느 쪽의 이익이 더 큰지 가늠해 보는 것이다. 하지만 이 경우에도 페이스북이 불리하다. 페이스북이 면죄부를 받으려면 이용자(정보 주체)에게 동의를 안 받아 페이스북(정보처리자)이 누리는 이익이 월등하게 앞서야 하는데, 우리 개인정보보호법은 EU보다 더 엄격하다. 법적 근

거가 없으면 개인정보를 수집할 수 없도록 하고, 수집하더라도 명시적으로 동의를 받도록 못 박은 국내 개인정보보호법의 엄격한 방향성에 비춰보면, 맞춤 광고에 쓰려고 누리꾼의 행태 정보를 광범위하게 수집한 페이스북의 이익이 인정받기란 어려워 보인다.

페이스북이 심은 쿠키에는 이용자를 특정하는 기능도 들어 있다. 이걸 빅데이터를 활용할 때 개인을 특정할 수 없도록 ‘비식별 조치’를 취하도록 한 방송통신위원회의 ‘빅데이터 개인정보 가이드라인’에도 어긋난다. 이에 대해 윤종수 변호사는 국내법에 비춰봐도 페이스북의 광범위한 정보 수집은 문제가 있다고 해석했다. “이 사건은 법률적으로도 그렇고, 실질적인 인식 면에서도 문제 소지가 있다고 보인다. 마치 다른 웹사이트에 스파이를 심어놓은 거나 마찬가지다.” 박지환 변호사는 “이번 사건을 계기로 우리나라에서도 행태 정보 수집에 관해 특별 조항을 법제화하든지, 동의 없이 수집할 경우 처벌해야 하는지 균형 잡힌 논의를 시작할 필요가 있다.”며 쿠키 사용에 관한 지침을 따로 마련할 것을 주장한다.¹⁾

5. 빅데이터 시대에 필요한 개인정보보호정책

비약적인 IT발전은 빅데이터 산업의 활성화라는 긍정적인 기여도 있는 반면 개인정보의 오·남용 가능성을 피할 수 없게 만들었다. 현행 정보통신망법 등 개인정보보호 관련 법령상 개인정보 수집·이용을 위해서는 반드시 이용자의 사전 동의가 필요하다. 그러나 대량의 데이터를 수집하고 처리하는 빅데이터 산업 특성상 사전 동의를 얻기가 쉽지 않아, 이로 인해 발생할 수 있는 프라이버시 침해 우려가 끊임없이 제기됐다. 이에 대처하기 위하여 방송통신위원회는 2014년 12월 빅데이터를 처리·활용하는 경우 개인정보를 보호하기 위한 구체적인 기준을 정한 「빅데이터 개인정보보호 가이드라인」을 발표했다. 이 가이드라인은 사업자 등에게 새로운 의무나 제한을 가하지 않도록 하되, 현행 법령 테두리 안에서 개인정보보호를 위해 사업자가 지켜야 할 기술적·절차적 사항을 구체적으로 규정한 것이다. 구체적으로, 빅데이터 처리 과정에서 수집된 데이터에 개인정보가 포함된 경우, 이를 다른 정보로 대체하거나 다른 정보와 결합하여도 특정 개인을 식별하기 어렵도록 하는 ‘비식별화’ 조치가 선행된다면 정보 수집·활용이 가능하도록 했다. 사업자들의 규제 불확실성을 최소화하기 위해 현행 법령 내에서 공개된 정보 등을 합법적으로 수집·활용할 수 있는 구체적인 기준을 제시한 것이다. 아울러,

1) 윤종수 변호사와 박지환 변호사의 발언은 『블로터닷넷』, 2015. 4. 7. 안상욱, ““페이스북 무차별 정보 수집, 국내법 위반 소지 커”,” <http://www.bloter.net/archives/224675>(검색일: 2015. 5. 14.)에서 인용하였다.

데이터의 수집 단계에서 개인정보를 비식별화하였다 하더라도 조합·분석 단계에서 다른 정보와 결합하여 재식별화 될 수 있는 가능성이 있는 경우 반드시 이를 즉시 파기하거나 추가적인 비식별화 조치를 취하도록 명시하였다. 또한 기존 정보통신망법과 마찬가지로 빅데이터 처리 사실·목적·수집출처 및 정보활용 거부권 행사 등에 대해 개인 정보취급방침을 통해 이용자에게 투명하게 공개하도록 하였으며, 특정 개인의 사상 등 민감 정보 생성이나 이메일·문자 통신 내용의 이용 등은 금지된다.

결론적으로 “만일 당신이 어떤 서비스를 공짜로 쓰고 있다면 당신은 고객이 아니라 ‘상품’이다.”라는 앞의 말을 잊지 말아야 한다. 서비스제공자는 자선사업가가 아니다. 그들은 당신의 개인정보로 돈을 버는 것이다. 따라서 세상에 공짜는 없다. 단, 공짜가 아니라면 공짜가 아니라고 분명히 말해야 한다. 공짜가 아니라고 분명히 말하지 않았다면 그에 대한 책임에서 자유롭지 못할 것이다.