「法과 政策」第21輯 第1號, 2015. 3. 30.
濟州大學校 法과政策硏究院

빅데이터 시대의 온라인 마케팅과 개인정보 보호

Online Marketing and Protection of Personal Data in the Age of Big Data

김 상 찬* · 강 재 정**
Kim, Sang-Chan · Kang, Jae-Jung

목 차

국문초록

오늘날 정보사회의 발전으로 급속도로 데이터가 생산되고 축적되는 이른바 빅데이터(big data)시대에 접어들고 있으며, 기업은 빅데이터의 활용과 분석을 통하여 온라인 마케팅을 포함한 사업과 정책개발에 큰 도움을 얻고 있다. 빅데이터는 기술적 측면, 비즈니스적 측면, 국가경쟁력 제고 측면에서 빅데이터 자체가 정보사회의 발전을 위한 새로운 패러다임으로 인식되기도 하지만, 빅데이터의 분석과 활용과정에서 개인정보가 노출되고 개인의 프라이버시를 침해한다는 매우 부정적인 위험을 안고 있으며, 우리나라에서도 해마다 수백

논문접수일 : 2015. 02. 20.
심사완료일 : 2015. 03. 08.
게재확정일 : 2015. 03. 11.
* 법학박사 · 제주대학교 법학전문대학원 교수(주저자)
** 경영학박사 · 제주대학교 경영학과 교수(교신저자)

만건에서 수천만건의 개인정보 유출사고가 발생하고 있다.

이러한 개인정보의 오·남용 또는 유통으로 인한 개인 프라이버시 등의 침해에 대응하여 세계 각국은 이른바 '잊혀질 권리'를 포함한 개인정보보호에 관한 논의와 입법적 규제가 활발히 이루어지고 있으며, 2013년 OECD가 제정한 '개인정보의 보호를 위한 가이드라인', 2012년 1월 EU가 제정한 '개인정보의 처리와 보호에 관한 규칙' 등이 대표적이라 할 수 있다. 우리나라에서도 지난 2011년 '개인정보보호법'을 제정하는 등 개인정보 보호를 위하여 노력하고 있지만, 개인정보 보호 업무가 각 부처에 산재해 있고, 각 분야에 대한 개별법이 별도로 존재하고 있어 개인정보보호법과 중복되거나 모순되는 내용의 조항들이 남아있는 등 많은 문제를 가지고 있다.

본고에서는 미국과 프랑스 그리고 EU의 개인정보보호 제도의 최근 동향에 대하여 살피고 있다. 특히 EU에서 말하는 이른바 '잊혀질 권리'가 우리나라에서 제도적으로 얼마나 수용되고 있는지에 관하여 살펴보기 위하여 우리 개인정보보호법과 EU의 개인정보보호규칙의 내용을 비교·분석하고 있으며, 아울러 우리나라의 개인정보보호 제도와 정책상의 문제점을 지적하고 개선방안을 제시하고 있다.

주제어 : 빅데이터, 온라인마케팅, 프라이버시, 개인정보보호, 개인정보보호법, 잊혀질 권리, 유럽연합(EU), 데이터보호규칙

Ⅰ. 서론

현대는 정보화의 시대이다. 오늘날 기업과 정부는 디지털 개인정보를 활용하여 새로운 상품과 서비스를 개발뿐만 아니라 신산업과 정책개발에도 적극적으로 활용하고 있다. 최근 주목받고 있는 빅데이터(big data)는 기업과 정부기관에서 고민해온 난제에 대한 해결책을 제공해 주면서, 기존의 프로세스와 조직, 산업 전반, 심지어 사회 자체를 변화시킬 수 있는 새로운 방법을 제시하고 있다. 그러나 그 이면에는 개인정보의 오·남용으로 인한 프라이버시

등의 침해라는 심각한 문제가 존재하고 있다. 이러한 문제를 해결하기 위하여 개인정보에 대한 익명화가 이루어지고 있으나, 빅데이터 분석을 통하여 개인정보의 재식별화가 가능하기 때문에 개인정보가 노출되거나 유출될 가능성이 항상 존재한다. 물론 개인정보의 유출은 기업뿐만 아니라 개인의 불법행위에 의해서도 이루어지고 있지만, 최근 고도화되고 전문화되고 있는 해킹기술은 개인정보 유출의 가능성을 더욱 높이고 있다.

실제적으로 우리나라에서 지난 2008년 한 인터넷 오픈마켓의 1천여만건의 개인정보유출을 비롯하여 2011년 인터넷 업체가 3천 5백만여건의 개인정보를 유출하는 등, 해마다 수백만건에서 수천만건의 개인정보가 유출되는 사고가 발생하고 있다. 최근 카드 3사(KB국민카드, 롯데카드, 농협카드)의 개인정보 유출 사건으로 우리나라 인구의 두 배 가까운 1억여건의 정보가 유출되었다. 금융감독원의 발표에 의하면, 유출된 정보는 이름과 전화번호, 직장명 등 단순 정보이며, 예금 계좌번호, 비밀번호, 신용카드 비밀번호, CVC 값 등 금융거래 관련 민감정보는 포함하지 않아 카드 위변조, 현금 불법 인출 등 고객 피해 가능성은 없다고 하지만, 유출 정보를 확인한 결과 카드 발급을 위해 고객이 기입한 정보인 성명, 이메일, 휴대전화 번호, 직장 전화 번호, 자택 전화 번호, 주민번호, 직장주소, 자택주소, 직장정보, 결혼 여부, 자가용 보유여부, 주거상황, 이용실적금액, 결제계좌, 결제일, 연소득 이외에도 신용한도금액, 연체금액, 신용등급 등과 같이 고객이 작성하지 않은 정보를 포함해 총 19개 항목에 달하는 것으로 나타났다.[1)]

이와 같은 개인정보가 유출되어 타인에 의하여 악의적으로 사용하게 되면 금융상의 불이익뿐만 아니라 국가적으로도 금융마비가 발생할 정도로 문제가 심각해진다. 또한 개인의 위치정보, 구매내역정보, CCTV정보, 자신이 올린 블로그나 트위터의 내용을 취합하여 개인에 대한 구체적인 정보를 이용하여 범죄나 경제적 이익을 갈취할 수도 있기 때문에 정부차원 뿐만 아니라 기업차원에서도 문제가 크다고 하겠다.

최근 온라인상에서 이루어지고 있는 개인정보의 오용, 남용 또는 유통으로

1) www.itworld.co.kr/news/85630, 2014. 1.20.

인한 개인 프라이버시 등의 침해에 보다 효과적으로 대응하기 위하여 세계 각국에서는 이른바 '잊혀질 권리(the right to be forgotten)'를 포함한 개인정보보호에 관한 논의가 활발히 이루어지고 있다. 2013년 OECD는 1980년 마련된 사생활 보호와 국경을 넘어 유통되고 있는 개인정보의 보호를 위한 가이드라인을 개정하여 발표하고 있으며, 2012년 1월 EU는 1995년에 제정된 '개인정보의 처리와 보호에 관한 지침'을 개정하여 프라이버시보호를 강화하고 있다.

우리나라에서도 지난 2011년 '개인정보보호법'을 제정하는 등 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호하려고 노력하고 있지만, 개인정보 보호에 관련된 업무가 거의 모든 정부부처에 산재해 있고, 법률 또한 기본법인 '개인정보보호법' 이외에 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률', '신용정보의 이용 및 보호에 관한 법률' 등 각 분야에 대한 개별법이 별도로 있어 개인정보보호법과 개별법이 중복되거나 내용이 모순되기도 한다.

본 연구에서는 정보화 사회에서 개인정보의 보호에 관한 주요 국가의 동향을 살펴보고, 특히 '잊혀질 권리'를 중심으로 우리나라의 온라인상의 개인정보처리와 보호제도의 현상에 대하여 살핀 후 개선방안에 관한 정책적 제언을 제시하고자 한다.

Ⅱ. 온라인 마케팅과 빅데이터

1. 온라인 마케팅

인터넷의 성장은 국게거래의 세계화를 가져왔다. 인터넷과 정보통신기술의 발전은 산업사회의 질서와는 다른 정보네트워크사회를 만들고 있으며, 정치, 경제, 사회, 문화, 미디어 등에서 새로운 변화를 일으키고 있다. 컴퓨터상의 온라인 마케팅이나 TV의 홈쇼핑은 이미 대기업이나 중소기업, 나아가 신생기업의 입장에서도 각광을 받고 있으며, 최근에는 스마트폰을 이용한 온라인 마케팅이 새롭게 자리를 잡아가고 있다. 온라인에서 상품을 구입하기 위해서는 기

본적으로 해당 홈페이지에 가입하는 등 이용자의 개인정보를 기업에 제공할 수밖에 없으며, 이러한 이용자의 개인정보는 기업의 입장에서는 가장 중요한 자원이 되므로 개인정보의 수집에 최대한 노력할 수밖에 없다. 온라인 업체들이 개인정보의 수집에 관심을 갖는 이유는 고객의 욕구에 적합한 상품과 서비스를 개발하고, 효과적으로 마케팅을 수행하기 위한 것이다.

그러나 최근 온라인 마케팅에서 가장 큰 논란 중의 하나는 빅데이터[2] 분석이라 할 수 있다. 빅데이터 분석을 통하여 기업에서는 고객 행동에 대한 이해와 예측 능력을 향상시킴으로써 고객과의 상호작용과 효과적인 마케팅이 가능하다. 매매거래와 다채널 상호작용, 소셜 미디어, 멤버십 카드 같은 소스를 통해 입수한 신디케이트 데이터(syndicated data), 여타 고객 관련 정보들은 기업이 고객의 기호와 요구 사항을 파악할 수 있게 도와준다. 기업에서는 고객에 대한 깊은 이해를 바탕으로 모든 분야의 기업들이 기존 고객 및 잠재 고객과 상호작용할 수 있는 새로운 방법을 찾을 수 있다. 이와 같이 빅데이터는 새로운 가치를 제공해 줄 새로운 자원으로 인식되기도 하고, 더 나아가서는 기술적 측면, 비즈니스적 측면, 국가경쟁력 제고 측면에서 빅데이터 자체가 정보사회의 발전을 위한 새로운 패러다임으로 인식되기도 한다.[3]

하지만 빅데이터의 도래는 개인의 모든 삶이 기록에 남는 라이프 로그의 시대로 접어들었음을 의미한다.[4] 디지털 기술과 전 세계적 네트워크로 인하여 망각은 예외적인 현상이 되고 디지털화를 통한 기억이 일반적인 현상으로 되어 가고 있는 것이다.[5] 개인이 블로그, SNS에 올리는 글은 물론 휴대전화에 내장된 GPS, 카메라, NFC 등 센서들이 개인이 어디를 방문하고 쇼핑하는지와 같은 라이프 로그 정보를 자동으로 생성·수집하는 역할을 한다. 특히

2) 빅데이터를 의미 그대로 해석하면 매우 큰 데이터란 뜻으로, 기존의 관리나 분석체계로는 감당할 수 없을 정도로 거대한 데이터의 집합을 말한다(채승병, "정보홍수 속에서 금맥찾기: '빅데이터(Big Data)' 분석과 활용", 「SERI경영노트」 제91호, 삼성경제연구소, 2010, 37면).

3) 정지선, "신가치 창출 엔진, 빅데이터의 새로운 가능성과 대응전략", 「IT & Future Strategy」, 한국정보화진흥원, 2011, 18면; 조성우, 「Big Data 시대의 기술」, KT종합기술원, 2011, 24면; 국가정보화전략위원회, 「빅데이터를 활용한 스마트정부 구현방안」, 2011, 11면.

4) 류성일, 「빅데이터 시대가 가져올 비즈니스 패러다임의 변화」, KT경제경영연구소, 2011, 9면.

5) Viktor Mayer-Schönberger, Delete : The Virtue of Forgetting in the Digiral Age, Princeton University Press, New Jersey, 2009, 구본권 역, 「잊혀질 권리」, 지식과 날개, 2011, p.17.

SNS는 사용자 정보가 자동적으로 다른 사용자에게 전달되는 구조를 가지고 있어서 정보유출과 관련해서는 매우 취약하다고 할 수 있다. 트위터를 통해 친구들과 주고받는 대화에서 본인의 기분이나 감정, 정치적 성향이나 가치관 등 본인도 잘 알지 못하는 것들까지도 전부 드러나게 한다. 페이스북이나 트위터 등 SNS사이트의 계정을 만드는 것은 공짜처럼 보이지만 사용자가 올리는 글이나 자신이 사용한 위치정보, 검색 및 구매정보 등이 모두 데이터마이닝(data mining)을 통해 광고나 마케팅 등에서 활용될 수 있다.[6] 페이스북, 트위터, 카카오톡 등 대부분의 SNS업체에서는 사용자의 실명, 주민등록번호, 주소, 이메일, 휴대폰결제지, 이동전화번호, 통신사, 결제승인번호 등을 수집할 수 있다는 약관을 제시하고 있는 것도 좀 더 개인화된 정보를 빼내려는 의도라고 할 수 있다.

최근에 통신기술과 온라인 추적기술이 더욱 발전하면서 고객별로 온라인 행위추적(online behavioral tracking)이 가능해지고, 이에 따라 고객 맞춤형 서비스를 개발할 수 있지만, 반면에서 행위정보가 유출됨으로써 범죄와 다른 목적으로 유용될 가능성도 높다. 이와 같이 온라인 행위정보가 이용자의 의사에 반하여 유출된다면 이는 필연적으로 프라이버시 침해로 이어질 수밖에 없다.[7] 지금까지 논의되고 있는 빅데이터 분석과 활용에 따른 위험으로는, 개인정보 침해, 물리적 재난, 사이버테러, 바이러스 등에 의한 위험, 빅데이터를 효과적으로 관리하고 활용하는데 실패함으로서 발생되는 경쟁력상실이나 혼란 등으로 요약할 수 있다.

이 중에서도 빅데이터가 초래하는 가장 큰 위험은 개인의 프라이버시 침해라고 할 수 있다.[8] 기존의 정보사회에서 수집되는 정보는 고정형 정보(주소, 주민번호, 학력, 재산, 병력, 범죄기록, 위료기록 등)나 반고정형 정보(CCTV 등을 통한 행동정보, 신용카드 내역, 인터넷 활용시간, 접속 사이트 등)가 대

6) 장규원·윤현석, "사이버공간에서의 개인 정보보호:소셜네트워킹서비스(SNS)를 중심으로", 「형사정책연구」 제22권 제3호, 한국형사정책연구원, 2011, 105면 이하.

7) 실제로 페이스북은 2010년 4월부터 6월까지 SNS상의 개인정보보호법의 제정을 저지하기 위하여 캘리포니아 주정부를 상대로 로비해온 것이 드러나 논란이 일어나기도 했다(inews24.com 2010.10.24.).

8) Bollier David, "The Promise and Peril of Data", The ASPEN Institute, 2010 p.23.

부분이었으나 빅데이터 분석에서는 개인의 취향, 사고, 행동 패턴뿐만 아니라 감정과 분위기에 더 나아가 본인도 인지하는 못하는 습관이나 버릇까지 수집되고 분석된다. 또한 소셜미디어에 존재하는 메시지뿐만 아니라 접속기록, 검색패턴, 데이터 속성(메타데이터)이 기록된 그림자 데이터의 증가는 프라이버시의 침해위험을 확대시킨다.[9)]

이와 같이 빅데이터 분석은 기업에게는 고객에 대한 광범위한 데이터를 분석을 통하여 고객의 욕구에 부합하는 제품개발과 마케팅, 그리고 서비스를 제공할 수 있지만 개인의 프라이버시 침해라는 부정적인 측면과 정면으로 충돌한다.

예컨대 자사가 판매하는 제품에 자동인식 기능을 심어, 이들 정보를 본사의 시스템에 자동 전송하도록 한 후에 이를 분석하여 고객의 취향, 패턴, 불만 등을 감지하고 마케팅에 활용할 수 있다. 최근의 자동차는 전자기술이 집약되어 있어 정교한 운전제어를 위한 많은 센서와 CPU가 내장되어 있다. 볼보(volvo)는 소비자의 자동차의 운전과정에서 수집된 데이터를 본사의 분석시스템에 자동으로 전송하도록 하여 빅데이터를 축적하고, 이를 이용하여 제품개발단계에서 알기 어려운 다양한 결함과 소비자의 잠재적 요구를 파악하여 빠르게 대응하는데 성공하였다.[10)] 개별경제 주체인 경우에는 마케팅을 위하여 수집하고 가공하며, 다른 업체에게도 판매하는 경우가 많아 개인정보의 수집·활용에 대하여 많은 논란이 있다. 일반적으로 빅데이터 분석을 위해서는 분야와 용도에 따라서 개인식별정보와 다양한 형태의 개인비식별정보, 그리고 여러 가지 형태의 사물에 대한 정보들이 수집되어 가공된다. MGI의 보고서에 의하면, 빅데이터가 활용되는 분야 중 많은 부분에서 개인정보가 수집·활용되고 있지만, 공공부문은 이미 엄격한 규제를 받고 있어 문제되지 않는다고 한다. 예컨대 보건의료분야에서 개인의료정보는 '의료법'등 관련법규에 의하여 민감한 개인정보로 분류되어 엄격한 규제를 받고 있기 때문이다. 하지만 웹로그 데이터나 소셜네트워크 분석데이터는 개인 비식별정보에 해당하는 경우가

9) 윤상오, "빅데이터의 두얼굴 : 기대와 위험", 「빅데이터와 위험정보사회」, 커뮤니케이션북스, 2013, 59면.

10) 윤상오, 상게논문, 65면.

많지만, 정보기술의 발전으로 이러한 데이터들을 연결하고 가공하면 어느 정도의 식별성을 가질 수 있기 때문에 개인정보의 유출가능성이 높아지므로 기업의 마케팅적 수요를 충족시키면서도 어떻게 개인정보의 보호와 관리를 효과적으로 수행할 것인지에 대한 정책적·법률적 논의는 매우 중요하다고 할 수 있다.

2. 빅데이터와 프라이버시 문제

인터넷의 보급은 데이터와 정보의 활용 기회를 높이고 있지만, 그 이면에는 개인정보의 유출로 인한 프라이버시의 침해라는 새로운 위험을 확대시키고 있다. 원래 프라이버시의 개념은 '홀로 있을 권리'라는 소극적 개념으로 출발하였으나 정보사회인 오늘날에는 "사적 영역에 부당한 침해나 공개를 당하지 않고, 개인정보에 대한 외부로부터의 부당한 접근을 방지하며, 자신의 동의하에 자신에 관한 정확한 정보가 유통될 수 있도록 통제할 권리"라고 할 수 있다.[11] 특히 정보통신기술의 발전과 컴퓨터의 대량보급으로 개인에 대한 정보가 손쉽게 수집·보관·처리되는 상황이 도래하면서 자기정보를 통제할 수 있는 권리라는 적극적 개념으로 사용되고 있다.

일반적으로 온라인에서의 프라이버시는 정보 프라이버시, 접근 프라이버시, 표현 프라이버시의 세 가지로 구분된다.[12] 정보 프라이버시란 온라인에서의 개인정보에 대한 통제력을 가지는 정도를 의미하며, 접근 프라이버시란 온라인에서 타인이 개인정보에 접근할 수 없도록 차단하는 것을 의미한다. 표현 프라이버시란 개인정보를 표현하는 것에 대한 자유를 의미한다.

초창기의 프라이버시의 문제는 서비스의 제공을 위해 불가피하게 수집된 '개인식별정보(PII, Personally Identifiable Information)의 유출과 관련된 것들

11) 노동일·정완, "사이버공간상 프라이버시 개념의 변화와 그에 대한 법적 대응방안", 「경희법학」 제45권 제4호, 경희대학교 법학연구소, 2010, 181면.

12) DeCew, J. W., In Pursuit of Privacy : Law, Ethics and The Rise of Technology, Cornell University, 1997, p.24; 김종기·김상희, "온라인 사용자의 프라이버시 보호행동에 대한 연구: 프라이버시 역설 관점에서,"「인터넷전자상거래연구」 제13권 제1호, 한국인터넷전자상거래학회, 2013, 41면 이하.

이 대부분이었다. 스마트 폰과 같은 다양한 디바이스 등이 등장하면서 개인식별정보와 함께 개인의 행위정보를 자동적으로 수집하고 축적할 수 있는 기술이 발전하고 빅데이터 분석이 가능해짐에 따라 다른 차원의 프라이버시의 문제점을 야기하고 있다. 특히 빅데이터 분석이 초래할 수 있는 새로운 프라이버시 위험에 대한 이슈는 크게 네 가지로 요약할 수 있는데, ① 행위패턴에 대한 프라이버시 위험, ② 정보취합의 프라이버시 위험, ③ 재식별화 위험, ④ 잊혀질 권리를 박탈할 위험 등이 그것이다.[13]

첫째, 행위패턴에 대한 프라이버시 위험이란 빅데이터 분석으로 개별적인 정보로는 제공하지 못했던 개인의 새로운 프라이버시를 밝혀내면, 이러한 정보에 대하여 개인의 프라이버시권을 주장할 수 있는가의 문제이다. 개인정보만으로는 알 수 없었던 개인에 대한 정보가 다양한 데이터를 기반으로 빅데이터 분석을 통하여 개인의 특성 패턴과 취향과 관련된 정보를 찾아내는 경우가 이에 해당된다. 둘째, 정보취합의 프라이버시 위험으로 이미 공개되어 있는 정보를 바탕으로 빅데이터 기술을 이용하여 정보를 취합한 경우에 원래 정보의 제공자가 그것에 대한 통제권을 가질 수 있는가의 문제이다. 셋째, 재식별화의 위험으로 만약 빅데이터가 그 이전에는 제한되었던 개인식별정보를 찾아내고 활용할 가능성이 있다면 그것이 프라이버시를 침해하는가의 문제이다. 넷째, 잊혀질 권리를 박탈할 위험으로 빅데이터에 포함된 개인정보의 통제권을 누가 갖고, 삭제할 권리가 있는가에 대한 문제이다. 빅데이터는 개인이 온라인 행위를 하는 과정에서 자발적으로 생성되는 디지털 흔적(digital footprints)뿐만 아니라 타인에 의해 생성된 디지털 그림자(digital shadows)도 포함되기 때문에 프라이버시의 침해에 따른 삭제권한이 누구에게 있는가를 판단하는 것은 매우 중요한 일이다. 예를 들어 트위터나 페이스북, 플리커나 유튜브 등 공유사이트에 다른 사람이 올린 나에 관한 정보가, 내 존재와는 별개로 지속적으로 남아 있으며, 또한 축적되고 재활용된다면 이에 대한 권한이 누가 어떻게 처리할 수 있는가는 과거와는 다른 문제인 것이다.[14]

---

13) Goldberg N and Miller M, The practice of law in the age of 'Big Data', 2011, p.139; 황주성, "빅데이터 환경에서 프라이버시 문제의 재조명", 「빅데이터와 위험정보사회」, 커뮤니케이션북스, 2013, 220면.

체스터가 말했듯이 현대사회는 이미 '디지털 루비콘(Digital Rubicon)'을 건넜을지도 모른다.[15] 인터넷이용자는 본인이 원하든 원치 않든 개인정보 전쟁에 관여하게 되었다는 것이다. 모든 것을 디지털 이전의 시대로 돌릴 수 없듯이 빅데이터 이전의 상태로 돌리기도 어렵다. 기업도 더 이상 개인정보에 대한 책임을 이용자에게 전가함으로써 프라이버시 문제로부터 자유로울 수 없다는 것을 인식해야 한다. 빅데이터는 기업이나 정부 데이터에서 '잠자고 있던 데이터'를 살려낼 수 있기 때문에 사회적으로 주목받고 있다. 그러나 빅데이터는 프라이버시에 대한 재평가를 요구하고 있다. 무엇보다도 빅데이터 기술로 인한 개인정보의 수집·가공·거래·활용·보관 등 빅데이터 라이프사이클 전체에 대한 정확한 현상파악이 필요하며, 이를 토대로 빅데이터로 인한 프라이버시 침해와 더불어 그 반대측변인 빅데이터가 주는 혜택을 유형화할 필요가 있다. 그라므로 빅데이터의 부정적인 측면과 긍정적인 측면을 동시에 고려한 사회 전체적 비용편익에 대한 분석이 필요하다.

Ⅲ. 주요국가의 프라이버시 보호 동향

오늘날 프라이버시와 개인정보는 많은 경우에 동일한 것으로 혼용되고 있다. 개인정보 보호에 관한 활발한 논의와 함께 개인정보관련 법률들이 제정되면서, 프라이버시 침해문제도 과거와 달리 개인정보 유출과 인터넷상의 프라이버시 침해문제로 그 모습이나 관점이 변화되고 있다. 입법에 있어서도, 1974년의 미국 프라이버시법, 1982년의 캐나다 프라이버시법, 1988년의 오스트레일리아 프라이버시법 등은 실제로 '개인정보'를 그 법적 보호 대상으로 하고 있음을 볼 수 있다.[16] 그래서 본 연구에서는 '개인정보 보호'라는 용어를 주로

14) 황주성, 상게논문, 227면.

15) Chester J, Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the 'Big Data' ear, In Gutwirth et al.(eds.), European Data Protection: In Good Health?, B.V: Springer Science Business Media, 2012, p.47.

16) 岡村久道·新保史生, 「電子ネットワークと個人情報保護」, 經濟產業調査會, 2002, 74面.

사용하면서, '프라이버시'라는 용어를 함께 사용하려 한다.

프라이버시에 대하여 유럽은 전통적으로 국민의 기본권으로 인식하고 절대 불가침의 대상으로 취급해온 반면, 영미에서는 프라이버시도 거래할 수 있는(tradable) 대상으로 보았다. 이러한 기본적 가치관의 차이로 인하여 프라이버시 관련 법제와 정책도 유럽과 영미가 대조를 이루고 있는 바, 여기에서는 미국과 프랑스 그리고 EU의 개인정보보호 제도의 최근 동향에 대하여 살피고자 한다.

1. 미국

미국은 1974년 프라이버시법(Privacy Act of 1974)이 제정되면서 프라이버시에 대한 권리가 명문화되었다. 미국은 개인정보보호에 관해서는 민간부문과 공공부문을 나누어 개별법들에 의하여 규율하고 있는데, 프라이버시법은 공공부문을 규율하는 법에 해당된다. 민간부문은 분야별로 개별법들이 존재하며, 강한 '언론의 자유'의 영향으로 개인정보의 처리에 대한 규제는 법보다는 사적 계약이나 사회규범에 의하여 이루어져 왔다고 할 수 있다. 이는 정보의 자유로운 유통을 기반으로 하는 표현의 자유에 대한 중시를 나타낸다고 할 수 있다.[17] 이 때문에 미국은 온라인상 개인정보 수집과 이용 및 제3자에 대한 제공을 규제하는 일반적인 법률을 가지고 있지 않고 민간영역의 각 부문별로 존재하는 입법들도 주로 개인정보의 정확성에 초점을 두고 있으며, 정보주체에게 열람 및 정정청구권도 일반적으로 허용되고 있지 않았다.[18]

인터넷 비즈니스의 대표적인 수익모델로서 온라인 광고가 활성화되면서 행태정보 기반의 온라인 광고를 집행하는 과정에서 프라이버시 침해의 위험이 커지자, 미국연방거래위원회(FTC : Federal Trade Commission)는 2009년 2월

17) Franz Werro, The Right to Inform v. the Right to Be Forgotten : A Transatlantic Clash, In Liability in the Third Millennium, 285-300 Baden-Baden, F.R.G.: Nomos., 2009, pp.290-292; James Q. Whitman, "The Two Western Cultures of Privacy : Dignity Versus Liberty", 113 The Yale Law Journal, 2004, p.1153.

18) 성낙인 외, 「개인정보보호법제에 관한 입법평가」, 한국법제연구원, 2008, 364면 이하; 함인선, "'잊혀질 권리'에 관한 고찰-EU개인정보보호법안과 우리나라 「개인정보보호법」의 비교를 중심으로-", 「인권과 정의」 제427호, 대한변호사협회, 2012.8, 51면 이하.

에 '행태정보 기반 온라인 광고에 대한 자율구제 원칙(Self-Regulatory Principles for Online Behavioral Advertising)'을 발표하고 관련 업계의 자율규제를 요청하였다. 그 주요 원칙으로는 투명성과 소비자에 의한 통제, 소비자정보에 대한 적절한 보안과 정보 보유의 제한, 프라이버시 정책 변경시 명시적 동의 획득, 행태기반 광고 목적의 민감한 정보 이용에 대한 명시적 동의 획득 등이 있다. 이에 대응하여 미국의 5대 광고단체는 2009년 7월에 FTC의 원칙에 부합하는 '온라인 행태광고를 위한 자율구제안'을 발표하였고, FTC는 개인식별정보뿐만 아니라 온라인 광고를 위하여 수집된 특정 개인과 연관될 수 있는 모든 정보가 보호대상이 되어야 한다고 하였다.

2010년 9월, 미국 하원의 통신·기술·인터넷 소위원회에서 인터넷상의 프라이버시 보호를 위한 포괄적인 법률로서 '인터넷 프라이버시법안(Internet Privacy Act)'을 발표하였는데, 그 주요 내용을 보면, 첫째 개인정보를 수집하는 기업은 프라이버시 정책을 공개하고, 해당 개인에게 이해하기 쉬운 표현으로 고지해야 할 것, 둘째 일반적인 개인정보 수집에 대해서는 사후동의(opt-out)를 원칙으로 하되, 민감한 정보는 사전동의(opt-in)를 얻을 것, 셋째 개인식별정보를 제3자와 공유하기 위해서는 사전동의를 받을 것 등이다.

2011년 2월에는 스페이어 상원의원이 인터넷브라우저가 인터넷 이용자의 온라인 행위를 추적하는 것을 금지할 권한을 이용자에게 부여하는 'Do Not Track Online Act of 2011'을 제안하였다. 이 법안은 브라우징 업체의 호응과 비판을 동시에 받았는데, 추적금지 옵션은 이용자들이 개인정보 수집에 대하여 거부할 수 있는 선택권을 갖는 시스템이며, 이용자들로 하여금 자신의 개인정보 추적 수준을 제한할 수 있게 한다. 이와 관련하여 2011년 5월에 아동추적금지법(Do Not Track Kids Act of 2011)이 발의되었으며, 여기에서는 EU에서 고안된 온라인에서 '잊혀질 권리'와 유사한 내용을 담은 개념인 'ERASER BUTTON'을 인터넷 사이트에 설정할 것을 서비스제공자에게 의무화하고 있었지만 이 법안은 상임위원회에 회부되었을 뿐 임기만료로 폐기되었다.[19]

2011년 4월에는 개인정보 보호를 위한 FTC의 포괄적인 규제 프레임워크로서

19) 이민영, "이른바 '잊혀질 권리'와 개인정보보호", 「법학논총」 제20집 제1호, 조선대학교 법학연구소, 2013, 65면.

상원의 상무·과학·교통위원회에서 '상거래 프라이버시 권리헌장(Commercial Privacy Bill of Right Act)'을 발의하였고, 이 헌장에는 개인정보 보호와 관련된 기존의 원칙들이 종합적으로 포함되어 있으며 법안 적용대상 기관, 보호대상 정보, 수집가능 정보 및 보관기간, 벌칙조항 등이 상세히 규정하고 있다.

미연방정부는 디지털 경제의 발전과 함께 소비자의 프라이버시가 위협받고 있는 상황을 개선하여 지속적인 혁신을 촉진하면서도 디지털 경제에 대한 소비자의 신뢰를 공고히 하고자 '네트워크화된 세계에서 소비자 데이터 프라이버시(Consumer Data Privacy in a Networked World)'를 발표하였는데, 이 보고서의 중심에 있는 '소비자 프라이버시 헌장(Consumer Privacy Bill of Right)'은 소비자의 온라인 프라이버시를 보호하기 위하여 다음과 같은 7대 원칙을 제시하였다. 즉 ① 소비자 자신의 데이터에 대한 개별 통제권, ② 기업의 프라이버시 업무에 대한 투명성, ③ 개인 데이터의 공개 및 이용이 허락된 최초 상황의 존중, ④ 소비자는 자신의 데이터에 대한 보안성을 요구할 권리를 가짐, ⑤ 소비자는 개인 데이터에 접근할 수 있고 오류를 수정할 수 있음, ⑥ 소비자는 자신에 대한 데이터 수집에 제한을 가할 수 있음, ⑦ 기업은 프라이버시 권리장전을 지키고 있음을 소비자에게 설명할 책임이 있음 등이다.

FTC는 기업간 공정경쟁과 함께 소비자 보호업무를 담당하는 독립기관으로 온라인 프라이버시 보호의 문제에 관하여 업계 전반을 관찰하면서 업계의 자율규제를 유도하는 방향을 추구해 왔다. FTC는 광고업계와 소비자 단체 및 프라이버시 전문가들 사이에 진행되었던 일련의 논쟁을 바탕으로 2012년 3월에 '급변하는 시대의 소비자 프라이버시 보호(Protecting Consumer Privacy in an Era of Rapid Change)'를 발표하였다. 이 보고서의 목적은 소비자들이 인지하지 못하는 개인정보의 노출에 의한 프라이버시 침해에 대처하는데 있으며, 그 방안으로 2011년에 스페이어 상원의원에 의하여 제안된 'Do Not Track'을 다시 제시하였다. 이에 대하여 디지털 광고연합이 동의하였으며 조만간 관련 업계 전반의 동의를 얻어낼 전망이다.

그밖에도 FTC는 모바일 앱 개발업체들에게도 프라이버시 대책을 마련할 것을 권고하였으며, 데이터 브로커의 정체를 일반에게 공개하고 이들이 어떤 정보를 어떤 방법으로 수집하는지를 소비자들에게 알려주도록 관련법의 정비

를 요청하였다. 그리고 2012년 8월에 FTC는 페이스북에 대해 종합적인 개인정보 프로그램을 수립하고, 그 이행 여부를 독립적인 감독기관으로부터 감사받을 것을 명령하였다.[20]

2. 프랑스

프랑스는 '잊혀질 권리(the right to be forgotten)'에 관한 논의를 가장 활발하게 하는 국가 중의 하나이다. 그래서 Jeffrey Rosen(2012)은 '잊혀질 권리'의 지적 근원을 망각권(le droit à l'oubli)을 인정하고 있는 프랑스법에서 찾고 있다. 2009년 11월 프랑스 상원은 '잊혀질 권리'와 관련된 규정을 포함한 '디지털 시대에서의 사생활권 보장 관련 법안(De loi visant à l'heure du numérique, text no 93(2009-2010)'을 발의하였고, 동 법안에 대하여 2010년 2월 프랑스 하원이 의견서를 제출하였다.[21]

프랑스 정부도 2010년 1월부터 디지털경제부에서 개인정보 유통기한의 설정 등을 내용으로 하는 '잊혀질 권리'의 입법화를 위한 캠페인을 전개하는 한편, 동년 9월에는 '웹사이트와 검색엔진에서의 잊혀질 권리헌장(Charte du Droit à l'oubli numérique dans les sites collaboratifs et moteurs de recherche)'을 공표하였다. 이 헌장은 인터넷 관련기업 13개사가 서명하였으며, 인터넷서비스 이용자가 인터넷서비스 제공자가 보유한 자신의 정보를 색인(Index)할 수 있는 권리, 개인정보의 삭제를 요청할 권리, 최신의 정보를 업데이트 할 수 있는 권리 등이 명시되어 있다.

3. EU

EU에서는 프라이버시를 인간의 기본권으로 인식하며, 인권보호의 차원에서

20) 그 주요내용으로는 개인정보를 공유할 때 당사자의 동의를 얻을 것, 소비자 약관에서 프라이버시 및 보안과 관련된 기만적인 표현을 개선할 것, 향후 20년간 관련 사항의 이행여부에 대한 감사를 받을 것 등이다.

21) 한국인터넷진흥원, 「인터넷법 제동향」, 제41호, 2011.2, 31면.

개인정보 보호에 관한 법제를 정비하여 왔다. EU는 1995년 개인정보보호의 근거법으로서 '데이터보호지침'[22]을 제정하고 개인정보 보호 감독기구로서 유럽데이터보호감시국(European Data Protection Supervisor)을 설치하였다. 이 지침의 목적은 기업이 자신의 고객이 원하지 않는 방식으로 고객에 대한 정보를 사용하는 것을 금지하는데 있으므로, 유럽에서 영업하고 있는 모든 기업은 동등한 프라이버시보호를 보장하지 못하는 타국으로의 개인정보 전송을 금지하는 것이 핵심내용이다.[23] 이 지침에는 개인정보 보호의 원칙을 비롯하여 개인정보의 처리기준과 방법 및 절차, 정보주체의 권리, 피해구제, 감독기구의 의무 등이 구체적으로 규정되어 있어 유럽뿐만 아니라 세계의 다른 국가들의 개인정보 보호 관련 법제에 큰 영향을 주었다. 이 지침은 공공부문과 민간부문에 공통적으로 적용된다는 점에서 미국의 법제와 대조된다.

2002년에 EU는 모바일 단말기의 위치데이터 처리를 규제하기 위하여 '프라이버시와 전자통신에 관한 지침'[24]을 제정하고, 통신비밀, 스팸, 위치정보, 쿠키 등을 온라인상 개인정보를 규제하였는데, 여기에서는 미국처럼 사전통지와 거부권으로 정보사업자의 쿠키 수집을 어느 정도 용인해 주는 옵트아웃제(opt-out rule)를 채택하고 있었다. 즉 사업체들은 쿠키 정보의 수집을 공지해야 하지만, 이용자가 개인적으로 거부하지 않은 수집을 허용하는 것이 관행이었다. 그러나 2009년에는 이 지침을 개정하여 개인정보의 이용목적을 명시할 것을 의무화하고 명시된 목적 이외의 이용을 금지하였으며, 이용자가 명백한 동의를 한 경우에만 한하여 수집할 수 있다는 옵트인제(opt-in rule)가 적용되었다.

EC는 프라이버시 보호대책의 강화를 위하여 1955년에 EU가 제정한 '데이터보호지침'을 전면 개정한 새로운 법안을 마련하여 의견수렴을 거친 후 2012. 1. 25.에 '데이터보호규칙안'[25]을 발표하고 동년 1. 27.에 동 법안(이하 '2012년

22) Directive 1995/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

23) 이민영, 전게논문, 70면.

24) Directive 2002/58 on Privacy and Electronic Communication.

25) European Commission, 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, COM(2012) 11 final, Brussels, 2012.1.25,

법안'이라고 한다)을 유럽연합이사회에 제출하였다. 2014년부터 시행되고 있는 이 규칙의 특징은 ① 입법형식이 지침(Directive)이 아니라 규칙(Regulation)의 형식을 취하고 있는 점, ② '잊혀질 권리'를 명시적으로 도입하고 있는 점, ③ 단일의 유럽정보보호위원회(European Data Protection Board)를 설치하고 있는 점, ④ 위반시 강력한 제재규정(최고 백만 유로 또는 회사의 연간 전세계 매출액의 2%)을 두고 있는 점, ⑤ 규정이 11장 91조나 되는 방대한 체계를 가지고 있는 점 등을 들 수 있다.[26] 즉, 프라이버시 보호 강화 및 개인정보 보호 규정의 실효성 강화를 위해서는 넓은 의미의 '개인정보'의 개념 유지가 필요하며, 이를 위하여 '정보주체'의 식별가능성을 강조하고 있고, 특히 프로파일 이용의 금지, 자연인은 사후 자신에게 불리한 프로파일링 조치의 대상이 되지 않을 권리의 명시 등 프로파일링에 대한 강한 규제방안이 주목을 끌고 있다.

4. 시사점

미국과 유럽은 프라이버시에 대한 가치관이 다르고, 법제적 전통도 다르기 때문에 온라인 프라이버시의 문제에 대한 제도에 대해서도 차이가 크다는 것을 알 수 있다. 미국은 기본적으로 기업의 자율규제를 중시하기 때문에 수차례의 입법 시도에도 불구하고 온라인 프라이버시 문제에 대한 새로운 법이 제정되지 않고 있고, 'Do-Not-Track'과 같이 개인이 정보주체로서의 권리를 적극적으로 행사하는 방향으로 기업들을 유도하고 있다. FTC는 개별기업들에 대한 관찰을 강화하고 문제가 있는 경우 프라이버시 정책을 강화하도록 요구하고, 관리 감독을 강화하는 방향으로 나아가고 있다. 유럽은 EU의 개인정보보호 기본법인 기존의 '데이터보호지침'을 대폭 개정하여 강력한 규제수단들을 법제화하는 방향으로 가고 있다. 따라서 개인정보보호를 위한 개인의 적극적인 역할보다는 보호자로서 국가의 역할을 강조하고 있다고 할 수 있다.

개인정보를 전적으로 민간 기업에 맡기는 것은 한계가 있다. 개인정보를 이

hereinafter 'COM(2012)'.

26) 함인선, 전게논문, 58면.

용하여 명백한 이익을 얻고 있는 기업들이 스스로 불이익을 감수하면서 개인정보를 보호하지는 않을 것이기 때문이다. 지금까지 업계에서는 자율규제를 주장해 오고 있지만 그것은 프라이버시 문제를 피해 나가기 위한 기업의 방어논리일 뿐이다.[27]

미국과 EU의 정책방향을 비교하면 비록 형식과 수단에 있어서는 차이가 있지만, 개인정보보호의 강화라는 큰 방향은 일치하며 프라이버시 보호를 위해 기업의 책임과 의무를 강조하고 있다는 점도 같다. 예컨대 EU가 최근 프로파일링을 금지하는 방향으로 정책을 결정한 것이나 미국의 FTC가 온라인 광고를 위하여 수집된 개인과 연관될 수 있는 모든 정보가 보호 대상이 되어야 한다고 밝힘으로써 대인화된 프로파일링에 대한 강한 규제를 시사하고 있는 것 등이 이와 관련이 있다.

Ⅳ. 잊혀질 권리와 개인정보 보호

빅데이터 시대에서 빅데이터에 포함된 개인정보의 궁극적인 통제권을 누가 가질 것인가 하는 것이 이른바 '잊혀질 권리를 박탈할 위험'의 문제이다. 이미 살펴본 바와 같이, 빅데이터는 개인이 온라인 행위를 하는 과정에서 발생하는 디지털 흔적은 물론, 타인에 의하여 생성된 디지털 그림자도 포함된다. 말하자면 트위터나 페이스북, 플리커나 뉴튜브 등 공유사이트에 다른 사람이 올린 자신에 관한 정보도 포함된다. 이들은 자신의 의지와 관계없이 지속적으로 남아있으며 축적되고 활용된다는 측면에서 과거와는 다른 문제를 갖는 것이다. 이와 관련하여 앞에서 살펴본 미국이나 EU에 있어서 논의되고 있는 '잊혀질 권리'는 그 시사하는 바가 매우 크다.

잊혀질 권리는 다음과 같은 세 가지 측면을 포함하고 있다. 첫째, 누구로부터 보호할 것인가, 둘째, 언제, 왜, 그 권리가 문제될 수 있는가, 셋째, 어떻게 그 권리를 보장할 수 있는가 하는 것이다.[28] 잊혀질 권리에 대한 주요한 관점

27) 황주성, 전게논문, 234면.

은 개인정보를 일정한 기간을 두고 삭제해야 한다는 것이다. 보호해야 하는 상대는 데이터수집·관리주체이며, 시간적으로는 일정한 소멸시기를 지정하는 것이 원칙이다. 하지만 사후적으로 문제가 발생하면 당사자의 요청에 의하여 삭제해야 한다. 이것은 이용자의 자기정보결정권과 관련된 것으로, 유럽의 데이터보호지침의 개정안에서도 논의된 바 있다. 하지만 빅데이터의 유용성을 위해서는 데이터의 장기간 축적이 필수적이므로 본질적인 갈등이 존재한다. 그리고 예방 차원의 성격이므로 기간설정 등이 법적 적합성을 확보하기도 쉽지 않다. 이의 대안으로 빅데이터의 보존은 허용하지만 정보제공자에게 부정적인 영향을 줄 때에는 동의를 구하도록 하는 방안이 제시되고 있다. 이러한 방안은 근본적인 대책이 될 수 없는 조치이지만 현재로서는 빅데이터가 프라이버시의 어느 부분을 얼마나 침해할지 아무도 짐작할 수 없다.

EU의 '잊혀질 권리'의 입법은 미국을 비롯한 세계 각국이 민감한 반응을 나타내고 있으며, 우리나라에도 적지 않은 영향을 미칠 것으로 예상된다. 2011년 방송통신위원회에서는 국가정보화전략위원회에서 '잊혀질 권리'를 도입하여 SNS사업자가 게시물이나 컨텐츠에 대해서 보유기간 설정 및 외부공개 차단 기능 등을 이용자에게 제공하거나 회원탈퇴 시에는 이를 지체없이 파기하도록 하는 방안 등을 검토하겠다고 밝혔다.[29]

이하에서는 우리나라에서 EU에서 말하는 이른바 '잊혀질 권리'가 제도적으로 수용되고 있는지, 만약 수용되고 있다면 얼마나 수용되고 있으며, 현행법상 인정 근거를 어디에서 구할 것인지에 대하여 살펴보려 한다.

1. 잊혀질 권리의 헌법적 근거

우리나라에서 '잊혀질 권리'는 정보주체인 개인의 자신과 관련된 개인정보의 삭제와 처리의 제한을 그 주된 내용으로 한다는 점에서 개인정보자기결정권의 하나로 간주되고 있다.[30] 이러한 개인정보자기결정권의 헌법적 근거와 관

28) 황주성, 상게논문, 236면.
29) 방송통신위원회, 「소셜플랫폼 기반의 소통·창의·신뢰 네트워크 사회구현전략」, 2011. 5, 29면.
30) 함인선, 전게논문, 59면; Chris Conley, "The Right to Delete", AAAI Publications, 2010

련하여 우리나라에서는 헌법 제10조에서 구하는 견해와 헌법 제17조에서 구하는 견해로 나뉘고 있다.[31]

전자는 다시 우리 헌법이 사생활의 비밀과 자유를 자유권 조항에서 규정하고 있으므로 사생활의 비밀과 자유는 소극적인 권리라고 보고 정보사회에서 개인의 존엄을 보장하기 위한 정보에 대한 적극적인 자기결정권은 헌법 제10조에서 보장된다고 하는 입장[32]과 일반적인 개인정보자기결정권의 근거는 헌법 제10조 제1문 후단의 행복추구권에 그 근거가 있는 일반적인 인격권에서 찾아야 한다고 보는 입장[33]으로 나뉜다. 후자는 사생활에 대한 권리가 전통적으로 개인이 외부의 간섭을 받지 않고 혼자 그대로 있을 수 있는 권리를 중심적 내용으로 하지만, 과학기술의 발달과 함께 도래한 정보사회에서는 개인정보의 수집·처리·관리의 대량·집단화로 인하여 개인의 사생활 비밀과 자유가 침해될 가능성이 현저하게 증대하였고, 이에 따라 개인의 개인정보자기결정권이 중요한 내용으로 추가되었다고 보는 입장이다.[34]

개인정보자기결정권의 근거와 관련하여 헌법재판소는, 헌법 제10조 제1문 및 제17조에 그 근거를 구하는 입장[35]과 새로운 독자적 기본권이라고 보는 입장[36]이 혼재하고 있다. 후자의 입장은 "……개인정보자기결정권으로 보호하려는 내용을 위 각 기본권들 및 헌법원리들 중 일부에 완전히 포섭시키는 것은 불가능하다고 할 것이므로, 그 헌법적 근거를 굳이 어느 한두개에 국한시키는 것은 바람직하지 않은 것으로 보이고, 오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본

AAAI Spring Symposium Series, 2010.3, p.53-59.

31) 이민영, 전게논문 75면; 함인선, 상게논문, 60면.

32) 김철수, 「헌법학개론」, 박영사, 2000, 519면.

33) 정태호, "개인정보자기결정권의 헌법적 근거 및 구조에 관한 고찰", 「헌법논총」 제14집, 헌법재판소, 2003, 417면 이하.

34) 김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 「공법연구」 29권 3호, 한국공법학회, 2001.5, 87면 이하; 성낙인, 「헌법학」, 법문사, 2011, 617면; 이인호, "정보사회와 개인정보자기결정권", 「중앙법학」 창간호, 중앙법학회, 1999.6, 61면 이하.

35) 헌재 2010.9.30, 2008헌마132; 헌재 2009.9.24, 2007헌마1092; 헌재 2008.10.30, 2006헌마1401·1409; 헌재 2005.7.21, 2003헌마282·425; 헌재 1995.12. 28, 91헌마114 등.

36) 헌재 2010.5.27, 2008헌마663; 헌재 2009.10.29, 2008헌마257; 헌재 2005.5.26, 99헌마513, 2004헌마190.

권이라고 보아야 할 것이다"라고 하고 있다.

생각건대, 개인정보자기결정권으로서의 '잊혀질 권리'는 사생활의 비밀과 자유가 문제되는 영역에서 그 기능을 발휘할 것이므로 보다 직접적인 헌법상의 근거는 제17조에서 찾아야 할 것이나, 제17조를 적용할 수 없는 영역, 예컨대 공적 생활에서 형성되거나 이미 공개된 개인정보 등도 있으므로, 헌법 제17조와 제10조 제1문에서 함께 구하는 것이 타당할 것이다.[37]

2. 잊혀질 권리의 법률적 근거

우리나라에서 '잊혀질 권리'에 대하여 법률적 근거를 구하고자 할 때 검토대상이 되는 법률은 '개인정보보호법'과 '정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보통신망법'이라 한다)'을 들 수 있다.

첫째로 보호되는 '개인정보'에 관하여, '개인정보보호법'은 "살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)"라고 하고 있고(동법 제2조 제1호), '정보통신망법'은 "생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)"라고 규정하고 있다(동법 제2조 제6호). 이 법률들에서 말하는 개인정보는 살아있는 특정 개인에 관한 정보를 말하며, 이러한 정보를 통하여 특정 개인을 알아볼 수 있는 식별가능성이 있는 것이어야 한다.[38] 요컨대, 이들 법률상의 개인정보와 '잊혀질 권리'의 대상인 프라이버시 내지 개인정보는 거의 유사하다고 해야 한다.

둘째로 정보주체의 자신의 개인정보처리에 관하여 가지는 권리에 대하여, '개인정보보호법'은 제4조의 총칙적 규정에서 ① 정보제공을 받을 권리, ② 동

37) 함인선, 전게논문, 62면.

38) 함인선, "개인정보 보호법의 법적용관계와 입법적 과제 - 위치정보법과의 관계를 중심으로 하여 -", 「인권과 정의」 제419호, 대한변호사협회, 2011.8, 67면.

의여부, 동의 범위 등을 선택하고 결정할 권리, ③ 개인정보처리여부를 열람할 권리, ④ 개인정보의 처리 정지, 정정, 삭제 및 파기를 요구할 권리, ⑤ 공정한 절차에 따라 피해구제를 받을 권리 등을 규정하고, 이들 각 권리를 개별규정에서 상세히 규정하고 있다(동법 제15조, 제21조 제1항, 제36조 제1항, 제37조 제1항 등). '정보통신망법'은 개별조항에서 이용자의 정정요구권, 정보통신서비스 제공자 등의 개인정보 파기의무 등에 대하여 규정하고 있다(동법 제30조 제2항,제29조). 위의 권리 중 '개인정보의 처리 정지, 정정, 삭제 및 파기를 요구할 권리'는 '잊혀질 권리'와 상당한 관련이 있다고 할 수 있다.

우리 '개인정보보호법'은 그 적용범위가 넓어 EU의 2012년 법안상의 '잊혀질 권리'의 대부분에 대하여 대응할 수 있을 것으로 생각된다. 동법 제58조 제1항에 해당하는 경우, 특히 언론보도 등과 관련된 경우에 차이가 있을 수 있지만, 2012년 법안도 표현의 자유와 관련하여 예외를 인정하고 있기 때문에[39] 큰 차이가 없다.

3. '잊혀질 권리' 위반에 대한 규제와 구제

'잊혀질 권리'를 개인의 권리로 인정하더라도 그것을 어떻게 실현하고, 또한 지극히 광범위한 온라인 세계에서 자신의 프라이버시 침해에 대하여 구제를 받을 수 있는가 하는 것이 문제된다. 말하자면 단순히 '잊혀질 권리'라는 개념을 인정하고 법적인 근거를 찾는다는 것만으로는 이 권리의 의미를 충분히 실현하였다고 할 수 없다는 것이다. '잊혀진 권리'의 내용을 충실히 법률로 규정하는 것도 중요하지만 그러한 권리를 어떻게 실현시킬 것인가 하는 것(권리의 규제)과 더불어 개인정보가 침해된 경우 '잊혀진 권리'의 침해로서 어떤 구제를 받을 수 있는가하는 것(권리의 구제)도 중요하다고 할 것이다.

(1) 권리위반에 대한 규제

2012년 법안은 '잊혀질 권리'에 대한 규정을 위반하면 감독기관이 행정적 제

39) COM 2012 11 final Article 17(3)(a)

재를 부과하도록 하고 있다.[40] 예컨대 잊혀질 권리 또는 삭제권을 준수하지 않은 경우, 기한 준수를 보장할 제도적 장치를 하지 않을 경우, 또는 정보주체가 개인정보에의 링크나 그 복사 또는 복제를 삭제할 것을 요구하는 사실을 제3자에게 통지하기 위한 모든 조치를 취하지 않는 경우에는 50만유로 이하 또는 연간매출액의 1% 이하의 과태료를 부과할 수 있는데, 과태료의 액수는 위반행위의 성질, 정도, 기간, 침해의 성격, 위반자의 책임정도, 감독기관과의 협력정도 등을 고려하여 결정하도록 규정하고 있다.[41]

우리 '개인정보보호법'은 개인정보처리자가 정보주체의 삭제 또는 정정요구를 받고, 필요한 조치를 하지 않거나 처리가 정지된 개인정보를 파기하지 않은 경우에는 5천만원 이하의 과태료를 부과하고(동법 제75조 제2항), 개인정보의 정정·삭제 또는 처리 정지와 관련하여 정보주체에게 알려야 할 사항을 알리지 않은 경우 1천만원 이하의 과태료를 부과하며(동법 제75조 제3항), 정정·삭제 등 필요한 조치를 하지 않고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 경우 또는 개인정보의 처리를 정지하지 않고 계속 이용하거나 제3자에게 제공한 경우 2년 이하의 징역 또는 1천만원 이하의 벌금을 과할 수 있도록 규정(제73조 제3항)하고 있다.

(2) 권리침해에 대한 구제

2012년 법안은 개인정보 침해가 발생되었다고 판단하는 경우 모든 정보주체는 물론,[42] 정보주체의 권리·이익의 보호를 목적으로 하는 단체(기구, 조직, 협회 등)도 독자적으로 EU가맹국의 감독기관에도[43] 고충을 제기할 권리를 인정하고 있다. 동 법안은 모든 자연인은 개인정보가 침해되었다고 판단한 경우 사법적 구제권을 가진다고 규정함[44]과 동시에, 감독기관이 고충에 대하여

40) Ibid. Article 79(1)
41) Ibid. Article 79(2)
42) Ibid. Article 73(1)
43) Ibid. Article 73(2)
44) (Ibid. Article 75(1)

필요한 결정을 하지 않거나 결과에 대한 통지를 하지 않을 때에는 감독기관에게 고충제기에 따른 행위를 의무지우는 사법적 구제권도 인정하고 있다.[45] 뿐만 아니라 동 법안은 정보주체의 권리·이익의 보호를 목적으로 하는 단체들에게도 정보주체를 위하여 소를 제기할 권리를 인정하고 있고,[46] 감독기관도 소송참가권과 소제기권을 가지도록 규정하고 있다.[47] 가맹국에게 침해를 종료시키고 가구제를 포함한 신속한 조치를 채택할 것을 보장하여야 할 의무를 지우고 있다.[48]

또한, 동 법안은 불법적인 개인정보의 처리나 동 법안과 양립할 수 없는 행위의 결과로 손해를 입은 자는 그 손해에 대하여 정보관리자 또는 정보처리자로부터 배상을 받을 권리가 있다고 규정하고 있다.[49] 이 때 정보관리자 또는 정보처리자는 손해를 입힌 사건에 대하여 책임이 없음을 입증한 경우 전부 또는 일부 면책될 수 있다.[50]

우리 '개인정보보호법'은 개인정보의 주체는 개인정보와 관련한 분쟁이 발생한 경우 '개인정보분쟁조정위원회'에 조정을 신청할 수 있고(동법 제43조 제1항), 이에 의하여 조정이 성립한 경우 이 조정의 내용은 재판상 화해와 동일한 효력을 가지게 된다(동법 제47조 제5항). 비슷한 유형의 침해를 받은 다수의 정보주체는 일정한 경우 집단분쟁조정을 신청할 수도 있다(동법 제49조 제1항). 또한 개인정보의 침해를 받은 자는 안전행정부장관에게 그 침해사실을 신고할 수 있고(동법 제62조 제1항), 행정안전부장관은 전문기관을 지정(동법 시행령에 의하여 '한국인터넷진흥원'을 지정하고 있음)하여 개인정보침해 신고센터를 설치·운영하여, 신고의 접수·상담, 사실의 조사·확인, 관계자의 의견청취 등을 하도록 규정하고 있다(동조 제2항, 제3항). 또한 동법은 제51조 내지 57조에서 일정한 법정요건을 갖춘 단체에 '개인정보 단체소송'을 허용하고 있는데, 이 소송은 개인정보처리자가 집단분쟁조정을 거부하거나 집단분쟁

45) Ibid. Article 74(2)
46) Ibid. Article 76(1)
47) Ibid. Article 76(2)
48) Ibid. Article 76(5)
49) Ibid. Article 77(1)
50) Ibid. Article 77(3)

조정 결과를 받아들이지 않을 때 법원에 권리침해 행위의 금지·중지를 구하는 소송으로 법원의 소송허가를 받아야 한다. 한편, 손해배상책임과 관련하여 동법은, 정보주체가 개인정보처리자의 위법행위로 인하여 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있고, 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다고 하고 있다(동법 제39조 제1항).

V. 결론

우리나라의 경우에도 최근 개인정보의 불법적 침해는 매년 급증하고 있다. 개인정보침해신고센터에 의하면 개인정보침해 신고건수가 2010년 54,832건, 2011년 122,215건, 2012년 166,801건, 2013년 177,736건으로 해마다 증가하고 있다. 그러나 이에 대한 피해자 구제는 잘 이루어지지 않고 있어서, 개인정보분쟁조정위원회의 분쟁조정실적을 보면 2010년 191건, 2011년 126건, 2012년 143건, 2013년 173건에 불과한 실정이다.[51] 뿐만 아니라, 소비자분쟁조정위원회에서 처리한 집단분쟁조정실적의 경우도 2010년 15건, 2011년 15건, 2012년 10건, 2013년 10건에 불과하다.[52]

개인정보보호에 관한 큰 문제 중의 하나는 보호해야 할 개인정보의 범위와 정의가 모호하다는 점이다. 개개의 법률에서 최소한의 개인정보만을 수집하도록 되어 있고 관리책임자를 두도록 하고 있으며 수집의 목적이 다한 경우 폐기하도록 되어 있지만 그 구체적인 범위와 내용이 명확하지 않다는 점이다. 그 결과 이번 카드사의 개인정보유출 사태에서 나타난 것과 같이, 개인의 신용정보나 결재계좌에 이르는 사생활 전반을 포괄하는 정보를 기업이 보유하고 있고 심지어 사망자, 탈회자의 개인정보도 거의 영구적으로 보관하고 있는 경우가 나타나고 있다. 또한, 개인정보보호에 관한 기업의 인식 또한 큰 문제의

51) 개인정보분쟁조정위원회·한국인터넷진흥원, 「개인정보분쟁조정사례집」, 2012. 20면, 2014. 20-24면.

52) http//www.kca.go.kr.

하나라고 할 수 있다. 2013년 안전행정부에서 실시한 '개인정보보호 실태조사'에 따르면, 개인정보보호 관리책임자를 지정하고 있지 않은 사업자가 71.5%, 개인정보 보호를 위한 예산을 확보하고 있지 않은 사업자가 95.9%에 달하고 있으며, 개인정보 보호를 위한 임직원에 대한 교육을 실시하고 있지 않은 사업자도 86.4%에 이르는 것으로 나타나고 있다.

우리나라는, 2004년 '금융지주회사법'에서 지주회사 내의 정보공유에 대해 정보주체의 동의 요건을 배제하는 특례조항을 두었으나, 2011년 '개인정보보호법'이 제정된 이후 그러한 특례에 대한 재검토가 없었던 것으로 보인다. 이로 인하여 고객의 개인신용정보가 금융지주회사 내에서 과도하게 공유되었고, 상당수가 광고나 홍보 등 마케팅에까지 무분별하게 활용되기에 이르렀으며, 이는 최근의 카드회사 고객정보의 대량유출 사태와 무관하지 않다. 2013년 방송통신위원회는 '빅데이터 개인정보보호 가이드라인(안)'을 발표하면서, 블로그나 SNS 등에 공개된 정보는 해당 시민의 동의 없이 수집·가공해 제3자에게 제공할 수 있다는 내용을 포함시킨 바 있다. 이는 법률상 근거도 없이 정보주체의 동의권을 배제한 것으로, 개인정보보호의 측면보다 빅데이터 개인정보의 이용을 활성화하는 데 더 치우친 것이라 할 수 있어서 문제가 있다.

뿐만 아니라 우리나라에서는, 개인정보보호에 관한 정책결정기능, 분쟁조정기능, 감독기능 등이 여러 행정기관에 분산되어 있어 업무상 중복을 초래하고 효율적인 법집행을 어렵게 하며 국민들에게도 피해구제 절차에 혼란을 줄 가능성이 크다. 또한 행정각부는 다른 부처의 개인정보보호 관련 업무에 대하여 독립적인 지위에서 감독기능을 제대로 수행할 수 없다. 그러므로 현행법상 독립적인 심의·의결기구로서 출범한 '개인정보보호위원회'가 개인정보보호에 관한 집행 및 감독기능까지 수행하도록 하는 것이 바람직하다. 만약 개인정보보호법이나 관련 개별법상의 집행권을 소관 행정부처에 맡겨둘 수밖에 없다고 한다면 적어도 개인정보보호에 관한 정책결정, 분쟁조정, 피해구제, 제도연구 등의 기능만이라도 '개인정보보호위원회'로 이관시키는 것이 필요하다.

요컨대, 개인정보 보호정책이 전반적으로 강화되는 방향으로 나아가고 있는 오늘날 온라인마케팅 사업을 위하여 개인정보에 대한 규제완화를 기대하기는 어렵다. 특히 개인화된 표적광고와 개인 수준의 고객세분화가 소비자 후생과

사회후생에 부정적인 영향을 줄 가능성이 높기 때문에 EU에서 추진하고 있는 것처럼 개인화된 프로파일링에 대하여 강한 규제가 요청된다. 우리 '개인정보보호법' 제23조는 개인의 정치적 견해를 민감정보에 포함하여 정보처리에 강한 규제를 하고 있는바, 개인화된 프로파일링에 의하여 획득된 개인의 선호나 라이프로그 정보 등도 개인의 정치적 견해와 마찬가지로 민감정보의 범주에 포함시킬 필요가 있으며, 이러한 정보를 프로파일링하는 행위에 대하여는 사전동의와 같은 강한 규제가 바람직하다. 특히 빅데이터와 프라이버시 문제는 사회적으로 민감한 이슈일 뿐 아니라 전 세계적으로 개인정보 보호 수준이 강화되는 추세이므로 온라인 마케팅 분야에서 자칫 프라이버시 문제를 소홀히 하면 빅데이터 사업 전 분야에 부정적인 인식을 심어줄 수도 있다. 공공분야 등 다양한 빅데이터의 활용분야와 잠재적 가치를 고려할 때 개인화된 프로파일링으로 마케팅 분야에서 창출하는 빅데이터의 가치는 상대적으로 크지 않기 때문에 프라이버시 보호를 위해 개인화된 프로파일링을 엄격히 규제하는 것이 바람직하다.

또한, 빅데이터의 활용분야와 잠재적 가치를 고려할 때, 개인화된 프로파이링 정보에 대한 균형적인 시각을 갖출 필요가 있다. 만약 무조건 불가능하다는 관점에서 접근하다보면 외국업체에게 고객을 빼길 염려와 함께 국가의 경쟁력이 떨어질 수밖에 없고, 허용한다면 개인의 프라이버시와 인권침해의 문제로 비화될 수 있기 때문에 적절한 균형점을 찾는 방안을 강구하는 것이 필요하다. 예를 들어 이용자가 명백한 동의를 한 경우에만 한하여 개인정보를 수집할 수 있는 옵트인제(opt-in rule)을 적용하더라도 여러 원천의 정보와 결합하여 사용하는 경우에는 규제의 범위와 내용이 달라질 수밖에 없을 것이다.

참고문헌

개인정보분쟁조정위원회・한국인터넷진흥원, 「개인정보분쟁조정사례집」, 2012-2014.
국가정보화전략위원회, 「빅데이터를 활용한 스마트정부 구현방안」, 2011.
김종기・김상희, "온라인 사용자의 프라이버시 보호행동에 대한 연구: 프라이

버시 역설 관점에서," 「인터넷전자상거래연구」 제13권 제1호, 한국인터넷전자상거래학회, 2013.

김일환, "정보자기결정권의 헌법상 근거와 보호에 관한 연구", 「공법연구」 제29권 3호, 한국공법학회, 2001.5.

김철수, 「헌법학개론」, 박영사, 2000.

노동일 · 정완, "사이버공간상 프라이버시 개념의 변화와 그에 대한 법적 대응방안", 「경희법학」 45권 4호, 경희대학교 법학연구소, 2010.

류성일, 「빅데이터 시대가 가져올 비즈니스 패러다임의 변화」, KT경제경영연구소, 2011.

방송통신위원회, 「소셜플랫폼 기반의 소통 · 창의 · 신뢰 네트워크 사회구현전략」, 2011. 5.

윤상오, "빅데이터의 두얼굴: 기대와 위험", 「빅데이터와 위험정보사회」, 커뮤니케이션북스, 2013.

이민영, 「인터넷 개인정보보호에 관한 법제도 연구」, 정보통신정책연구원, 2000.

이민영, "이른바 '잊혀질 권리'와 개인정보보호", 「법학논총」 제20집 제1호, 조선대학교 법학연구소, 2013.

이인호, "정보사회와 개인정보자기결정권", 「중앙법학」 창간호, 중앙법학회, 1999.6.

성낙인, 「헌법학」, 법문사, 2011.

성낙인 외, 「개인정보보호법제에 관한 입법평가」, 한국법제연구원, 2008.

장규원 · 윤현석, "사이버공간에서의 개인 정보보호: 소셜네트워킹서비스(SNS)를 중심으로", 「형사정책연구」제22권 제3호, 한국형사정책연구원, 2011.

정태호, "개인정보자기결정권의 헌법적 근거 및 구조에 관한 고찰", 「헌법논총」 제14집, 헌법재판소, 2003.

정지선, "신가치창출 엔진, 빅데이터의 새로운 가능성과 대응전략", 「IT & Future Strategy」, 한국정보화진흥원, 2011.

조성우, 「Big Data 시대의 기술」, KT종합기술원, 2011.

채승병, "정보홍수 속에서 금맥찾기: '빅데이터(Big Data)' 분석과 활용",

「SERI경영노트」 제91호, 삼성경제연구소, 2010.
한국인터넷진흥원, 「인터넷법제동향」 제41호, 2011.2.
함인선, "'잊혀질 권리'에 관한 고찰-EU개인정보보호법안과 우리나라 개인정보보호법의 비교를 중심으로-", 「인권과 정의」 제427호, 대한변호사협회, 2012.8.
함인선, "개인정보 보호법의 법적용관계와 입법적 과제-위치정보법과의 관계를 중심으로 하여-", 「인권과 정의」 제419호, 대한변호사협회, 2011.8.
황주성, "빅데이터 환경에서 프라이버시 문제의 재조명", 「빅데이터와 위험정보사회」, 커뮤니케이션북스, 2013.
岡村久道・新保史生, 「電子ネットワークと個人情報保護」, 經濟產業調査會, 2002.
Bollier David, The Promise and Peril of Data, The ASPEN Institute, 2010.
Chester J, Cookie wars: How new data profiling and targeting techniques threaten citizens and consumers in the 'Big Data' ear, In Gutwirth et al.(eds.), European Data Protection: In Good Health?, B.V: Springer Science Business Media, 2012.
Chris Conley, "The Right to Delete", AAAI Publications, 2010 AAAI Spring Symposium Series, 2010.3.
DeCew, J. W., In Pursuit of Privacy: Law, Ethics and The Rise of Technology, Cornell University, 1997.
Franz Werro, The Right to Inform v. the Right to Be Forgotten : A Transatlantic Clash, In Liability in the Third Millennium, 285-300 Baden-Baden, F.R.G.: Nomos., 2009.
Goldberg N and Miller M, The practice of law in the age of 'Big Data', 2011.
IDC & EMC, Digital Universe Study 2011, June 28, 2011.
James Q. Whitman, "The Two Western Cultures of Privacy : Dignity Versus Liberty", 113 The Yale Law Journal, 2004.
McKinsey Global Institute, Clouds, big data and smart assets: Ten tech-enabled business trends to watch, McKinsey and Company, August

2010.

Viktor Mayer-Schönberger, Delete : The Virtue of Forgetting in the Digiral Age, Princeton University Press, New Jersey, 2009, 구본권 역, 「잊혀질 권리」, 지식과 날개, 2011.

Jeffrey Rosen, "The Right to be Forgotten", 64 Stan L. Rev. Online 88, 2012.

European Commission, 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, COM(2012) 11 final, Brussels, 2012.1.

[Abstract]

Online Marketing and Protection of Personal Data in the Age of Big Data

Kim, Sang-Chan

Ph. D., Professor, Jeju National University

Kang, Jae-Jung

Ph. D., Professor, Jeju National University

With the advancement of information society today, so called age of big data has become when data is produced and accumulated, and organizations have received great help in their business including online marketing and policy development through employing and analyzing big data. While big data is in itself often recognized as a new paradigm for developing information society in terms of technology, business and boosting national competitiveness,

it is involved with very negative danger in that personal information is leaked and privacy is invaded in the process of analyzing and using big data. There have been recently from millions to tens of millions of personal data leaks each year in this country as well.

Discussions and legislative regulations in relation to personal data protection have been made actively including so called 'right to be forgotten' in each country in response to invasion of personal privacy etc. due to the misuse or distribution of personal data, and it can be said that 'OECD guidelines on the protection of privacy and personal data' established by OECD in 2013, and 'regulation of personal data processing and protection' established by EU in January are typical examples. Although this country had made an effort to protect personal data such as enacting 'Personal Information Protection Act' in the year of 2011, it has a variety of problems as the tasks of personal data protection are scattered in many departments, and since separate laws exists in each area, there are articles left which are overlapped with or inconsistent with Personal Information Protection Act.

This paper examines recent trends of protection systems of personal data in the USA, France and EU. In particular, in order to examine how so called 'right to be forgotten' mentioned by EU is accepted systematically in our country, it is making a comparative analysis of our personal information protection act and regulation of personal data processing and protection made by EU in terms of their contents, and also it is pointing out problems of this country' systems of personal data protection and policy and is proposing improvement measures.

Key words : Big Data, Online Marketing, Privacy, Personal Data Protection, Personal Information Protection Act, Right to Be Forgotten, EU Regulation of Data Protection