경제규제와 법(Journal of Law & Economic Regulation)
제11권 제2호 (통권 제22호). (Vol. 11. No. 2). 2018. 11. pp.00~00

일반논문

미국 '데이터 브로커' 제도의 국내법적 함의

Study on the Domestic Legal Implications of US Data Broker System

김 현 경(Kim, Hyun-Kyung)*

목차

〈국문초록〉

기업의 인재채용, 국가의 범죄자 예측 등 빅데이터・인공지능에 기반하여 이루어지는 데이터(개인정보를 포함한)의 처리과정은 복잡한 수학적 공식에 의하므로 일반인들이 이해하기 힘들어졌다. 이러한 처리과정의 불투명성은 정보주체가 개인정보의 처리결과에 대하여 이의를 제기하기 어렵게 만든다. 미국의 경우 이러한 현상이 인공지능이나 빅데이터로 대별되는 기술 이전에, '데이터 브로커'를 통해 이미 상용화되어 왔다. 미국의 데이터 브로커 산업은 이미 개인정보 법제가 자리 잡기 이전부터 집적화된 개인정보를 자산으로 보유해 왔고 최근 빅데이터・인공지능 등 데이터 분석 기술의 고도화는 이들의 개인정보 활용가치와 영역을 더욱 확대시키고 있다. 본 연구는 이러한 미국의 데이터 브로커 현황과 규율법제를 검토하고 국내의 개인정보 규율방향에 대한 시사점을 도출하였다. 우선 미국의 데이터 브로커는 우리법상 개인정보처리자에 해당된다. 그러나 우리법은 민간에서 개인정보의 처리를 위해서는 정보주체로부터 사전에 명확한 동의를 득해야 한다. 한편 미국의 데이터 브로커는 정보주체의 사전 동의 없이 거의 100년 이상 개인정보를 수집, 누적해 왔고 지금도 그러하므로 실질적으로 국내의 개인정보처리자가 미국과 같은 데이터 브로커 사업을 영위하는 것은 불가능하다. 미국은 최근 데이터 브로커에 대하여 규제하고자 하는 입법을 추진하고 있으나 최초의 규제법인 버몬트주법의 경우도 '정보주체의 동의'를 전제로 하는 규제보다는 후발적으로 데이터 브로커의 개인정보 처리과정에 있어서 일정한 의무를 부여하고 사업등록을 통해 정부의 관리감독을 꾀하고자 하는 방향으로 규율하고 있다. 연방차원에서 데이터 브로커를 규제하고자 하는 여러 개의 법안이 제안되었으나 지금까지 어떠한 법안도 통과되지 못했다. 아마 이미 형성되어있는 데이터 브로커 산업에 대한 부담과 4차산업혁명이라는 기술적 변혁속에서 데이터 활용의 중요성이 부각되면서 이러한 법안의 실행은 쉽지 않을 것으로 보인다.

4차산업혁명의 달성에 필요한 핵심기술과 서비스가 모두 데이터에 기반한다는 사실에 비추어볼 때, 또한 데이터의 속성(비배타성/비배제성)으로 인해 데이터규범의 집행이 물리적 '국경' 안에서 이루어지기 곤란하다는 점을 감안할 때, 집합적 데이터에 대한 규율방향의 근본적 변화를 모색할 필요가 있다. 비단 미국의 데이터 브로커를 언급하지 않아도 이미 통신, 금융, 의료 영역의 특정기업에 의해 전 국민의 개인정보가 수집되어 있다는 사실은 우리나라나 미국이나 별반 다르지 않다. 그럼에도 불구하고 현행 「개인정보 보호법」상 정보주체의 권리 보장방식은 엄격한 사전 동의, 정정・삭제 요구권 중심이다. 이미 대부분의 개인정보가 수집되어 있는 상태에서 '수집' 중심의 규율체계는 정보주체의 프라이버시 보호에 취약할 수밖에 없다. 따라서 개인정보의 이용, 제공 과정에서 공정한 처리를 담보하기 위한 공익적 감독방안의 도입 등 개인정보 수집 후 처리과정에 있어서

* 서울과학기술대학교 조교수, 법학박사.

공정성을 담보하기 위한 제도들이 강구될 필요가 있다. 편향된 데이터의 채택으로 인해 정보주체에게 발생하게 되는 불이익을 막고, 부당한 차별과 불평등한 처우를 위해 개인정보가 처리되는 것을 감독하여야 할 것이다. 또한 엄격한 사전 동의 보다는 엄정한 약관심사 등을 통해 개인정보 처리와 관련된 공정한 계약 체결이 이루어지도록 하는 것이 기업과 정보주체 간의 불평등한 관계를 감안해 볼 때 정보주체 권리 보장을 위해 더욱 현실적이다.

Ⅰ. 문제의 제기

개인정보가 어떠한 목적으로든 이용의 대상이 된다는 것은 부인할 수 없는 사실이다. 기존에 개인정보는 고용, 복지, 마케팅 등 사회 각 영역에서 처리, 이용되고 그러한 이용은 '정보주체의 동의' 혹은 '각종 공익적 처리'에서 정당화되었다. 개인정보의 이용자가 누구인지, 그 처리과정은 어떠한 기준과 프로세스에 의해 이루어지는지 알고자 한다면 비교적 쉽게 파악할 수 있었다.

그러나 대용량 데이터를 기반으로 하는 알고리즘의 진화는 이용자가 개인정보를 직접 처리하는 것이 아니라, 데이터 전문가를 통해 처리된 개인정보를 이용하는 형태로 변화하고 있다. 일례로, 기업은 원하는 인재를 뽑기 위해 지원자의 각종 개인정보를 데이터 전문가에게 의뢰하여 특정 알고리즘에 적용시켜 원하자는 대상과 원치 않는 대상을 구분한다. 국가는 범죄자 예측을 위해 인종, 거주지, 신용 등 개인의 특정화된 정보 값을 변수로 설정하여 그 범죄가능성을 예측한다. 빅데이터・인공지능에 기반하여 이루어지는 데이터(개인정보를 포함한)의 처리과정은 복잡한 수학적 공식에 의하므로 일반인들이 이해하기 힘들어졌다. 그 결과 막상 특정 알고리즘을 통해 처리된 개인정보 처리결과에 대하여 이의를 제기하는 것이 곤란하다.

미국의 경우 이러한 현상이 인공지능이나 빅데이터로 대별되는 기술 이전에, 이미 상용화되어 왔다. 기업이 누군가를 고용하기 위해 구직자의 신용정보나 기타 정보를 정보주체의 의지와 무관하게 데이터 브로커를 통해 제공받는다. 데이터 브로커는 기업, 공공기관 등 특정 고객이 득하기를 원하는 개인정보를 보유하고 있으며 이를 기반으로 고객이 원하는 정보를 분석하여 제공한다. 이러한 데이터 브로커는 주로 소비자 신용을 분석하여 보고하는 기업 형태로 존재하였으나, 최근에는 빅데이터 기술을 활용하여 산업 전 영역에 데이터 분석서비스를 제공하는 기업으로 진화하고 있다. 따라서 개인정보의 가치와 활용영역도 더욱 다각화되며 광범위해지고 있다.

초기 미국에서 프라이버시권에 대하여 논의될 당시만 해도 '개인정보'는 재산적 권리가 아니라 인격권적 성격에 초점을 맞춘 것이었다.[1] 그러나 현 시점에서 개인정보의 의미는 "프라이버시 권"의 한계를 넘어서고 있다. 혼자 있을 자유를 보장받아야 한다는 측면에서 프라이버시권의 보호객체가 될 수 있으나, 표현의 자유를 보장받는다는 의미에서 공개의 대상이 될 수 있고, 영업의 자유 측면에서 재산권의 객체이기도 하다.[2] 즉 기술발달에 따라 사회변화를 수용하면서 개인정보는 일의적으로 정의내리기 곤란하게 되었다. 특히 데이터 분석기술의 고도화를 전제로 하는 빅데이터 환경은 정보주체와 개인정보파일을 이용하고자 하는 자 간의 갈등과 충돌을 일으키며 다의(多義)화된 개인정보의 성격을 표출시키고 있다. 이러한 갈등과 충돌은 이미 개인정보 법제가 자리 잡기 이전부터 집적화된 개인정보를 자산으로 보유해 온 미국의 데이터 브로커 산업을 중심으로 더욱 첨예하게 나타나고 있다. 따라서 본고에서는 미국의 데이터 브로커 산업의 현황과 규율법제를 검토하고 국내 상황에 적합한 시사점을 도출하고자 한다.

---

1) Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890). at 205. As Warren and Brandeis wrote: "he principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality."

2) 김현경, 개인정보의 개념에 대한 논의와 법적 과제, 미국헌법연구 第25卷 第2號, 2014년, 135~136면.

Ⅱ. 미국의 데이터 브로커 현황과 규율법제

1. 데이터 브로커 현황

가. 데이터 브로커의 개념

브로커는 장래의 잠재적 구매자와 판매자 사이에서 중개자 또는 협상가로 활동하는 대리인이다. 무역 또는 상거래 등의 사안에서 다른 사람들 사이의 계약을 성사시키기 위해 고용된 사람이라고 할 수 있다.[3] 데이터 브로커라 함은 정보 재판매업자(information resellers)로도 불리 우며, 소비자의 개인 정보를 수집해서 그 정보를 제3자와 공유하거나 재판매하는 기업을 의미한다.[4] 기업, 연구소, 공공기관 등 수많은 기관이 개인정보를 수집, 처리하나 데이터 브로커는 이러한 기관들이 개인정보를 수집하는 것과 다른 양상을 보인다.

우선 수집의 출처를 명확히 인용하지 않는다. 대학과 혹은 연구기관 역시 데이터를 모으고, 분석하고, 연계점을 만들고, 가치평가에 활용하며 이러한 면에서 데이터 브로커와 유사하다고 볼 수 있다. 그러나 가장 큰 차이점은 이러한 연구기관은 데이터의 출처를 인용하여야만 한다는 것이다. 그러나 데이터 브로커는 화폐(통화)의 거래와 유사하게 과거와의 연결을 끊고 그 출처를 공개하지 않는다. 즉 데이터 브로커를 구분하는 방법은 그들의 출처를 검토하는 것이다.

둘째, 다른 기관들이 통상 특정 업무를 위해 데이터를 사용하는 것과는 달리, 데이터 브로커는 데이터 수집 및 판매 이외의 다른 비즈니스를 수행하지 않는다. 즉 데이터 브로커는 해당 비즈니스와 직접적 관련성을 가지지 않는 소비자에 대한 정보를 모으고 판매하는 것을 주된 업으로 한다.

셋째, 데이터 브로커는 온라인 구매기록, 공공기록, 위치 데이터, 충성도 프로그램, 구독 정보 등 여러 출처에서 소비자에 관한 수백 또는 수천 개의 데이터를 수집한다. 그런 다음 데이터 브로커는 데이터의 정확성을 확보하기 위해 데이터를 평가, 분석하고 이를 제3자에게 패키지화하여 판매한다.

넷째, 데이터 브로커가 제공하는 서비스영역은 매우 포괄적이다. 타겟 마케팅, 신용보고, 뒷(배경)조사, 정부정책을 위한 제공, 위험관리, 사기 탐지, 인명검색, 은행・보험사 등의 중요한 결정, 정치캠페인에서 유권자 타겟팅과 캠페인 전략 등에 현대 경제활동에 제공되는 대부분의 서비스에 있어서 중요한 역할을 한다.

이러한 특성으로 인해 데이터 브로커는 소비자가 직접적 관계를 가지는 비즈니스를 영위하는 기업과 다른 양상을 보인다. 우선 전통 및 전자 상거래 비즈니스와 직접적인 관계가 있는 소비자는 해당 비즈니스와 관련된 자신의 데이터 수집에 대해 어느 정도의 통제권을 가질 수 있다. 해당 비즈니스가 제공하는 데이터 수집 정책을 검토, 고려하여 특정 데이터 수집 관행을 거부할 수 있다. 또한 해당 비즈니스의 고객 담당자가 누구인지 확인하고 문제가 발생하였을 시 이의를 제기할 수 있다. 더불어 소송을 통해 계약상의 이행사항을 다툴 수 있다. 반면 소비자는 데이터 브로커가 자신의 정보를 가지고 있는지, 그들이 어느 회사인지, 그들이 어떤 정보를 수집하는지, 접근 가능한 출처는 어디인지 알 수 없다.

나. 데이터 획득방법

데이터 브로커가 보유데이터의 출처를 공개하지는 않지만 그들의 정보를 얻는 곳은 크게 두 가지 방법으로 분류될 수 있다. 그 하나가 공공기록이며, 다른 하나는 사적 영역에서의 제공이다. 소비자로부터 직접 데이터를 수집하지 않는다.

미국에서 법원의 결정문 등을 포함하여 공공기록에 대한 접근권은 오랜 기간동한 확립된 권리이다.[5] 따라서 고용주 등이 직원을 고용하기 위하여 그들의 범죄기록 등을 확인하는 것은 오랫동안 관행적으로

3) BLACK'S LAW DICTIONARY 219 (9th ed. 2009).

4) Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability." 2014, I.

5) Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978) 등.

이루어져 왔다. 그러나 1990년대 초반 인터넷이 출현한 이후로 미국은 데이터 브로커 산업을 폭발적으로 경험하게 되었다.[6] 그 이전에는 공공 기록에서 정보를 얻는 것이 매우 지역화된 작업에 불과했다. 일반적으로 고용주는 고용과 관련된 개인에 대한 정보를 획득함에 있어 개별적으로 그러한 정보를 직접 관리하는 주 또는 지방 정부 기관을 통해 직접 획득하였다. 또한 그러한 기록은 통상 종이형태로 보관되어 있으므로 정보의 획득은 종이문서를 통해 이루어지게 된다. 디지털화된 기록이 아니며 복제는 오직 사진형태로 가능하였다.[7] 인터넷의 보편화와 개인 데이터 브로커 산업의 창설 이전에, 개인의 범죄 기록에 관한 정보를 취업이나 주거 목적으로 얻는 주된 방법은 주정부 기관으로부터 직접 획득하는 것이었다. 그러나 현재는 다르다. 개인의 범죄기록 등을 담고 있는 소비자보고서는 제3의 기업이나 인터넷을 통해 널리 유용하게 사용가능하다.[8] 그러한 기록을 획득하는 과정이나 획득 가능한 유형의 기록도 개별 주법에 따라 차이가 있다. 그러나 현재의 데이터 브로커들은 정보를 사건별로 획득하는 것이 아니라, 주 및 지역 출처에서 일괄적/대량으로 구매하고 그러한 정보를 그들의 데이터베이스에 저장한다.[9] 시간이 지나면서 이러한 데이터베이스는 상당한 규모로 쌓여졌으며, 그 안에 포함된 데이터는 종종 여러 관할 구역을 포함하며 수년을 거슬러 올라가는 축적된 기록이 된다.[10]

그밖에 데이터 브로커가 취득하는 연방정부 데이터로는 센서스국(U.S. Census Bureau)의 인구통계정보, 주소, 선거구 등 행정 정보, 사회보장국(Social Security Administration)의 사망자 명부 정보, 우편서비스(U.S. Postal Service)의 주소 변경 정보, 연방법원의 파산 정보 등이다. 주정부와 지방정부 데이터로는 전문직 면허 정보, 부동산, 유권자, 자동차등록, 법원 정보 등이 대표적이다.

민간 상업 정보로는 소매업과 카탈로그 회사의 거래 내역, 잡지사의 구독자 정보, 전자상거래, 뉴스, 여행 사이트, 금융회사의 거래 정보, 다른 데이터 브로커의 보유 정보 등이 해당된다.[11]

다. 전국적 데이터 집합으로 확장

대형 데이터 브로커들은 소위 '대량데이터구매(bulk data purchases)'라 불리는 방식을 통해 기록을 얻게 된다. 이는 한 번에 여러 개인에 대한 범죄기록을 대량으로 구매하는 방식이다. 주 또는 지역 기록 관리 기관으로부터 정보를 수집한 다음 해당 정보를 "즉시 검색"을 위해 독점 데이터베이스에 저장한다.[12]

데이터 브로커 산업의 발전 초기에 지역에이전시(local agency)들은 공공기록을 데이터 브로커에게 판매함으로서 돈을 벌 수 있다는 것을 인식하였고 그러한 지역에이전시들은 현재 그러한 관행으로부터 상당한 이익을 얻고 있다.[13][14] 일부 개별 주들은 주법 또는 관행적으로 이를 제한하고 있음에도 불구하고,[15] 여전히 지역 에이전시들은 공공기록을 데이터 브로커에게 자유로이 주고 그 과정에서 수익을 취하고 있다.

더욱이 데이터 브로커 산업이 처음 융성하기 시

6) SEARCH REPORT, SEARCH, NAT'L CONSORTIUM FOR JUSTICE INFO. & STATISTICS, REPORT OF THE NATIONAL TASK FORCE ON THE COMMERCIAL SALE OF CRIMINAL JUSTICE RECORD INFORMATION 82-83 (2005), p. 29.
7) David S. Ardia, Reputations in a Networked World: Revisiting the Social Foundations of Defamation Law, 45 HARV. C.R.-C.L. L. REV. 261, 310 (2010).
8) SEARCH REPORT, 앞의 글, pp. 7-9.
9) 위의 글, 7-8면, 10면; Adam Liptak, Criminal Records Erased by Courts Live to Tell Tales, N.Y. TIMES, Oct. 17, 2006, p. A1.
10) 위의 글, 7-8면.
11) 정용찬, "빅데이터 산업과 데이터 브로커", 프리미엄 리포트 15-04, 정보통신정책연구원, 2015.8, 9면.
12) SEARCH REPORT, 앞의 글, 10-12면.
13) Rebecca Oyama, Note, Do Not (Re)Enter: The Rise of Criminal Background Tenant Screening as a Violation of the Fair Housing Act, 15 MICH. J. RACE & L. p. 189.
14) 일부 주정부 및 지방 정부 기관은 가격으로 범죄 기록을 판매하는 것이 수익이 된다는 것을 인식하였다. 일례로 인디애나 폴리스 경찰국은 자신의 웹 사이트 (http://www.civicnet.net/allservices.html)에서 검색 당 $ 15의 범죄 기록을 제공한 바 있으며, 사우스 캐롤라이나 법 집행 부서는 이름으로 범죄 확인을 할 수 있도록 이름 당 $ 25를 청구한다.
15) 몇몇 주는 범죄기록을 포함한 특정 데이터의 판매를 금지하거나 제한하는 법안을 통과시킨 바 있다. SEARCH REPORT, 앞의 글, 39-43면.

작하였을 때, 데이터베이스는 통상 하나의 관할권 또는 기껏해야 하나의 주로 제한된 정보였다. 그러나 시간이 지나면서 데이터 브로커들은 전 국가적 범위의 데이터베이스를 광고하기 시작하였다. 그러한 광고에 의하면 전 국가적 범위의 데이터베이스는 이용자가 모든 주에서 1억 6천만 건 이상의 범죄기록이 포함된 독점적 데이터베이스를 거의 즉시 검색할 수 있다고 한다.[16]

근본적으로 개인의 사적인 배경을 조사하는 시장의 규모가 커지면서, 특히 9.11사태 이후 범죄기록확인 및 소비자 보고에 대한 수요가 급증하였는데,[17] 가장 많은 정보를 가장 신속하게 제공한 기업이 경쟁우위를 차지할 수밖에 없었다. 이러한 수요를 충족시키기 위해, 데이터 브로커들은 사건별로 개인에 대한 기록을 요청하여 획득하는, 시간이 오래 걸리는 방식보다는, 주/지역 에이전시를 통해 대량으로 기록을 축적함으로서 데이터베이스를 구축하는 방식을 선호하게 되었다.[18]

특히 시장에서 특정정보에 대한 수요는 매우 강력하게 요구된다. 이러한 경우 정보의 최신성이나 신뢰성과 무관하다. 예를 들어 범죄 기록과 관련된 오명은 매우 강하고 부정적이어서 집주인과 고용주는 기록이 있다는 사실만으로 범죄 기록이 있는 개인에 대한 주택 및 고용을 거부하고자 한다. 이러한 이유로 데이터 브로커들은 이미 공적기관에 의해 말소된 기록들을 공개하지 않도록 해달라는 어떠한 압력을 받을 이유도 없다. 실제로 고용주와 집주인은 말소기록의 공개에 긍정적이므로 실제로 데이터 브로커에게는 과거 기록을 현재에 부합하도록 갱신하거나 수정할 어떠한 유인책도 없다.[19] 즉 당연히 데이터 브로커는 정확한 정보를 제공하여야만 하고 그리하여 소비자와의 신뢰를 확보하여야 함에도 불구하고 특정 정보의 경우 이렇게 신규성·정확성을 유지하고자 하는 인센티브가 없다. 앞선 예에서 오히려 소비자에 해당되는 집주인이나 고용주는 과거의 기록에 더 만족스러워 할 것이다.

또한 공공기관에서 이미 기록이 삭제된 정보에 해당되는 경우 주정부나 지역의 기록관리 기관은 더 이상 그러한 정보를 가지고 있지 않으나, 데이터 브로커들은 여전히 그들의 고객에게 가치가 있는 정보를 보유하고 있으므로 그러한 정보(예를 들어 이미 삭제된 범죄기록 등)를 가지고 있는 유일한 출처가 될 것이다.

개인에 대한 범죄기록이 관할 법원 및 기록관의 파일 캐비넷에 보관된 경우, 이제는 이동 및 신속한 복제가 가능하고, 전자적 형식으로 쉽게 접근할 수 있다.[20] 또한 그러한 정보는 방대하고 사적으로 관리되는 데이터베이스에 저장되어 있으며, 거의 현행화되지도 않는다. 결국 현행화할 필요가 없다는 산업계의 요구와 그러한 산업의 성장을 통해 엄청나게 증가된 정보에 대하여 접근하게 되며, 이는 곧 부정확하거나 유해한 정보가 이용되게 됨을 의미한다.[21] 얼마나 자주 현행화되고 있는 정보인지, 또는 기록이 삭제된 정보인지 등에 대하여 불명확함에도 불구하고 업계관행에 의하면 그러한 정보가 놀라운 빈도로 발생하고 있다고 한다.[22]

2. 데이터 브로커 산업의 양과 음

가. 긍정적 혜택

데이터 브로커 산업은 현대 경제에 있어서 중요한 서비스를 제공한다. 데이터 브로커에 의해 수집되고 판매된 소비자정보는 각종 거래에 있어서 리스크 감소, 마케팅, 인물이나 상품검색 등 다양한

16) 위의 글, 11면.
17) James Jacobs & Tamara Crepet, The Expanding Scope, Use, and Availability of Criminal Records, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 204-05 (2007),; Adam Liptak, Criminal Records Erased by Courts Live to Tell Tales, N.Y. TIMES, Oct. 17, 2006; Oyama, 앞의 글, 187면.
18) Logan Danielle Wayne, "The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy", 102 J. Crim. L. & Criminology 253 (2013), p. 264.
19) 위의 글, 265면.
20) Oyama, 앞의 글, 187면.
21) Jacobs & Crepet, The Expanding Scope, Use, and Availability of Criminal Records, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177 (2007) p. 212.
22) Wayne, 앞의 글. 266면.

목적으로 사용된다.[23]

우선 리스크 감소와 관련하여 법 집행 기관, (예비)고용주 및 집주인이 사용하는 배경 조사가 포함된다. 또한 금융업의 경우 고객의 신원을 확인함으로써 사기/횡령 등의 위험을 사전에 탐지할 수 있다.

상품 마케팅은 비즈니스를 잠재적 고객과 연계시킨다. 전통적으로 우편이나 방문을 통해 물건을 판매하는 방식뿐만 아니라, 웹사이트를 통한 타겟 마케팅을 가능하게 함으로써 소비자와 영업자의 비용과 시간을 절약시킬 수 있다. 특히 웹사이트를 이용함에 있어서 무료 서비스는 타겟 광고로부터 얻는 수익이 기반이 되기 때문에 타겟 마케팅에의 이용은 더욱 중요하다. 타겟 광고와 그로 인한 수익이 없다면 무료 인터넷 서비스는 현실적으로 존재하기 힘들다.

또한 인물검색서비스는 이미 전화번호부 등을 통한 전통적 의미의 인물검색방식을 대체한지 오래이며, 더 광범위하게 글로벌한 방식으로 발전하고 있다. 사람들은 기업임원이나 경쟁자를 검색할 수 있으며 과거의 지인을 찾아낼 수 있고, 족보(가족력)를 조사할 수 있으며 기타 친척, 범죄경력, 취미 등 다른 수많은 정보를 찾아낼 수 있다.

나. 위해

통상적으로 데이터 브로커는 두 가지 측면에서 소비자에게 위해를 발생시킬 수 있다. 첫째, 소비자의 자기 정보에 대한 인지 및 통제권과 관련된 부분이다. 둘째는 소비자 정보에 대한 무단 접근, 즉 정당한 권한 없는 접근으로 인해 발생하는 위해이다.[24]

자기에 대한 데이터를 인식하고 통제할 수 있는 능력은 데이터의 부정확성이 널리 만연된 환경일수록 더욱 중요하다. 2012년 FTC는 조사대상 소비자의 21%가 삼대 주요 신용보고기관에서 발행한 신용보고서 중 하나에서 "중요한 오류"를 확인하였고 소비자의 5.2%는 수정되지 않았더라면 잘못된 신용정보로 인해 더 높은 이율 부담을 지게 되었을 것이라고 조사된 바 있다.[25]

개인의 데이터파일은 잘못된 행위 혹은 실수로 손상될 수 있다. 데이터 수집의 복잡성에 비추어 볼 때 그러한 실수는 일상적으로 만들어질 수 있으며, 일단 그러한 실수가 만들어진 다음에는 그러한 오류 데이터가 판매되고 재판매될 수 있다. 이는 중요한 문제이고 실제 미국의 연방정부와 주정부가 해결하려는 가장 큰 과제이다.[26]

데이터 브로커는 공통된 특성으로 개인을 범주화하여 그 리스트를 판매한다. 그러나 일부 데이터 브로커는 매우 높은 해를 발생시킬 위험이 있는 개인 목록을 판매한다. 업계 관계자는 이러한 목록에 대해 합법적인 마케팅 등 합법적 다른 목적을 위해 사용된다고 주장하나 이러한 리스트는 종종 파렴치한 사람들 혹은 더 사악한 사람들(스토커, 사기범 등)에게 노출시킬 수 있다.[27] 이들에 의해 노출되는 정보는 강간 희생자 명단, 가정폭력쉼터 주소(법에 의해 비밀유지의무가 있는 장소에 해당됨에도 불구하고), 경찰관 및 경찰관들의 자택 주소, 유전병 환자, 치매노인, HIV/AIDS환자, 술・도박・약물 등 중독자, 질명 및 처방전 복용 정보, 신용점수가 낮은 자의 명단 등이다. 이렇게 데이터 브로커를 통해 획득된 정보는 스토거 등에게 있어서 개인을 추적을 더욱 용이하게 해주며, 악의적 행위자가 신원도용 또는 기타 사기에 쉽게 개입할 수 있는 가능성을 높여준다.

일례로 2013년 데이터 브로커인 US Court Ventures가 신분 도용자에게 데이터를 판매하였고

23) Office of the Attorney General Department of Financial Regulation, Report to the General Assembly of the Data Broker Working Group issued pursuant to Act 66 of 2017, December 15, 2017, pp. 6-7.

24) United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, June 30, 2014.

25) FTC, Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003, Dec. 2012.

26) 이를 위해 연방차원의 공정신용정보법이 존재한다. 이에 대하여는 후술한다.

27) World Privacy Forum, Testimony of Pam Dixon Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information do Data Brokers Have on Consumers, and How Do They Use It?, Dec. 18, 2013.

그는 또 다른 신원 도용자에게 해당 데이터를 재판매 한 사실이 밝혀진 바 있다.[28] 또한 2016년 FTC는 Leap Lab이라는 데이터 브로커가 은행계좌정보와 사회보장번호가 포함되어 있는 수십만 건의 대출상환신청서를 사기꾼에게 재판매한 사례를 밝혀낸 바 있다.[29]

뿐만 아니라 데이터 브로커는 민감한 개인정보를 한곳에 대량으로 보관하므로 해커들의 주요 공격대상이며 보안 취약성이 문제될 수밖에 없다. 가장 큰 규모의 데이터 브로커 업체 중 하나인 Acxiom은 2003년에 해킹을 당했는데 2년에 걸쳐 이름, 주소, 이메일 주소 등 16억 건이 넘는 개인정보가 유출되었으며, 스팸 발송자에게 판매되기도 하였다.[30] 또한 Experian은 2015년 1,400만 건의 기록(T-Mibile의 데이터이나, Experian서버에 저장되어 있었다)이 서비스 제공을 위한 소비자 앱을 통해 접근가능한 상태로 있었던 것이 밝혀진 바 있다. 여기에는 사회보장번호, 생년월일, 이름, 주소 등의 개인정보가 포함되어 있었다. LexisNexis의 모회사인 RELX는 2005년 사회 보장 번호, 운전면허증 정보 및 31만 명의 주소가 도난당하였으며,[31] 2009년에는 3만 3천명,[32] 2013년에는 1건 수백만 개의 기록들을 도난당했다.[33]

3. 규율법제

가. 미국의 개인정보 법제 일반

연방차원에서 개인 정보 보호를 위한 법규가 만들어져 있으나 영역별/부문별(sectoral)규제로 제한된다. 즉 공공부문의 프라이버시 보호법(the Privacy Act, 1974), 민간부문의 아동온라인 프라이버시 보호법,[34] 건강보험법,[35] 전자통신에서 프라이버시 보호법[36] 등 영역별 법제를 취하고 있다. 특정 산업 또는 활동을 규제하며, 연방 차원의 포괄적 개인 정보 보호법은 없다. 데이터 브로커의 활동은 영역을 가로지르는 경향이 있기 때문에 불완전한 규제가 적용될 수밖에 없다. 연방법이 각 주의 법규에 우선하여 적용되지만, 개별 사안에 따라 연방법과 주법이 동시에 적용되어야 하는 경우도 있고, 개인정보가 소비자 권리침해와 관련될 경우 연방통상위원회(FTC)의 시정조치나 가이드라인도 중요한 역할을 한다.

이처럼 데이터 브로커 산업을 직접적으로 규제하는 별도의 법률은 존재하지 않는다. 다만 1970년 제정된 '공정신용보고법(Fair Credit Reporting Act, 이하 "FCRA"라 한다)'은 신용, 고용, 보험, 주택구입 등 분야에서 '소비자보고기관(CRAs: Consumer Reporting Agencies, 이하 "CRA"라 한다)'에 관한 규정을 두고 있으므로 현재 데이터 브로커산업을 규제할 수 있는 유일한 연방법이라고 할 수 있다.

28) Brian Krebs, Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records, KrebsOnSecurity, Mar. 10, 2014, https://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/. See also Transcript of Waiver of Indictment and Plea to Information Hearing, U.S. v. Hieu Minh Ngo, Docket No. 1:12-cr-00144 Doc. 27, Mar. 7, 2014.

29) Press Release, F.T.C., Data Broker Defendants Settle FTC Charges They Sold Sensitive Personal Information to Scammers, Feb. 18, 2016, www.ftc.gov/news-events/press-releases/2016/02/data-broker-defendants-settle-ftc-charges-they-sold-sensitive (2018.11.9.확인).

30) John Leyden, Acxiom Database Hacker Jailed for 8 Years, The Register, Feb. 23, 2006, https://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/ (2018.11.9.확인).

31) Heather Timmons, Security Breach at LexisNexis Now Appears Larger, N.Y. Times. Apr. 13, 2005, https://www.nytimes.com/2005/04/13/technology/security-breach-at-lexisnexis-now-appears-larger.html (2018.11.9.확인).

32) Angela Moscaritolo, LexisNexis admits to another major data breach, SC Magazine, May 4, 2009, https://www.scmagazine.com/lexisnexis-admits-to-another-major-data-breach/article/555843/ (2018.11.9.확인).

33) 31Juan Carlos Rodriguez, LexisNexis Could Have Suffered Data Breach, FBI Says, Law360., Sept. 26, 2013, https://www.law360.com/articles/475918/lexisnexis-could-have-suffered-data-breach-fbi-says(2018.11.9.확인); Brian Krebs, Data Broker Giants Hacked by ID Theft Service, KrebsOnSecurity, Sep. 25, 2013, https://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/ (2018.11.9.확인).

34) the Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§6501-6506).

35) the Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. §1301 et seq.).

36) the Electronic Communications Privacy Act (18 U.S.C. §2510).

나. FCRA[37]

FCRA는 앞서 언급하였듯이 데이터 브로커를 규율할 수 있는 유일한 연방법임에도 불구하고, FCRA의 규정은 데이터 브로커를 규제하기 위하여 설계된 법령이 아니기 때문에 현재 데이터 브로커에 의한 사생활침해를 위한 적절한 수단이라고 볼 수 없다는 지적이 있다.[38]

FCRA는 데이터 브로커에게 그들의 기록들을 현행화하도록 적극적 의무를 부여하지 않고 있으며, 이 법의 집행은 여전히 개인에 대한 법집행준수를 중심으로 규율하고 있다. 이 법이 1970년 만들어졌을 때, 현재의 이러한 인터넷 환경은 고려되지 못하였다. 어떠한 소비자정보나 공공기록도 모두 '종이' 형태였다. 따라서 정보가 쉽게 복제/배포될 수 있는 현재의 기술적 환경에서 이 법의 의도가 제대로 발현되기는 힘들 수밖에 없다.[39] 이후 개정법에 의하더라도 FCRA는 데이터 브로커가 범죄기록 등을 사인(私人)에게 판매하는 모든 경우에 적용되지는 않는다. 더욱이 몇몇 데이터 브로커는 명시적으로 본인들의 업무가 FCRA가 규율하는 신용, 보험, 고용 관련 데이터를 제공하지 않으므로 FCRA의 규율대상이 아니라고 하면서, 규율을 회피하고자 한다. FCRA는 CRA가 소비자 신용 정보, 사적 정보, 보험정보 및 기타 정보를 취급함에 있어 상거래 요구를 충족시키기 위한 합리적인 절차를 채택하도록 하기 위해 만들어졌다. 이러한 정보는 그러한 정보의 기밀성, 정확성, 관련성 및 적절한 정보의 활용과 함께 소비자에게 공정하고 공평한 방식으로 취급되어야 한다.[40]

즉 FCRA는 특정 목적을 위해 "소비자 보고서"를 제공하는 CRA에 적용된다.[41] 데이터 브로커는 비즈니스에 따라 CRA가 될 수도 있고 되지 않을 수도 있다. 마찬가지로 데이터 브로커는 "소비자 보고서"와 같은 자격을 가진 데이터를 거래할 수 있으나, 그렇지 않은 데이터를 거래하기도 한다. 예를 들어, FTC는 마케팅 목적으로 판매된 데이터, 사기를 탐지하거나 사람들을 찾아내는 데이터가 FCRA의 적용을 받지 않는다고 하였다.[42] 전통적인 '신용 보고서'를 발행하는 세 개의 주요 신용 조사 기관은 FCRA의 적용을 받으나 이러한 기관들은 FCRA가 적용되지 않는 다른 서비스를 제공하기도 한다.

FCRA는 신용보고서의 발행자, 그러한 보고서의 사용자(채권자, 보험사, 집주인 등), 그리고 정보의 제공자(CRA에게 소비자와의 거래정보를 제공하는 비즈니스)에게 각각 별도의 의무를 부여한다.

보고서 발행자는 (1) 소비자 보고서를 소비자에게 1년에 한 번 무료로 제공하고, (2) 정보를 받는 모든 당사자의 신원을 보고서에 공개하며, (3) 소비자가 제기한 분쟁을 조사하고 (4) 부정확한 정보를 삭제하거나 수정하고, (5) 소비자가 사용자에게 보고서를 제공하는 것을 승인했는지 확인하는 보호조치를 취해야 한다. 신용 보고서의 사용자가 보고서의 정보를 기반으로 소비자에게 신용, 보험 또는 고용을 거부하는 경우 다음 사항을 준수해야 한다.: (1) 거부 사실이 보고서의 정보로 인한 것임을 소비자에게 알려야 하고 (2) 보고서 발급자의 이름과 주소를 제공하고 (3) 소비자에게 보고서의 사본을 받고 그 정확성에 대한 이의를 제기할 권리를 알려야 한다. CRA에 정보를 제공하는 채권자 또는 다른 상인은 (1) 고의적으로 오류가 있는 정보를 CRA에 보고하는 것이 금지되며, (2) 알려진 오류를 수정해야 한다. (3) 소비자가 시작한 모든 분쟁을 CRA에 통보해야 하고 (4) 분쟁이 된 정보의 내용을

37) 15 USC § 1681 et seq. 2003 년에 FCRA는 공정하고 정확한 신용 거래법(FACTA)(117 Stat. 1952, 15 U.S.C. §§ 1681-1681x에 성문화 된)에 의해 개정되었습니다. 이 FCRA에 대한 설명은 FACTA 개정안을 포함한다.

38) Wayne, 앞의 글, 267면.

39) Elizabeth D. De Armond, Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation, 41 VAL. U. L. REV. 1061, 1075-.96 (2007), pp. 1098-1118.

40) FCRA § 1681(b).

41) A "consumer reporting agency" is defined as "any person which…regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."

42) FTC 2014 Report at i.

조사하고 부정확한 정보를 삭제하며 부정확한 정보의 대상이 되는 모든 수령인에게 보고해야 한다.

1998년에 FTC(Federal Trade Commission)는 FCRA가 고용목적으로 범죄기록정보를 제공하는 기관에게까지 적용되어야 한다는 보고서를 간행한 바 있다.[43] 그러나 많은 데이터 브로커들은 여전히 본인들은 FCRA의 적용을 받는 업체가 아니라고 하면서 규율을 회피하고자 한다. 또한 엄격히 이러한 범죄기록에 대한 사항이 FCRA의 일반적인 정신에 부합된다고 볼 수도 없다. 이 법의 기본 목적은 범죄 기록이 아닌 금융 및 기타 소비자 신용 데이터와 관련하여 소비자를 보호하는 것이다. 뿐만 아니라 2003년 개정을 통해 7년 이상 된 범죄 유죄 판결 기록의 이용을 금지하는 규정을 삭제함으로서[44] 데이터 브로커가 범죄기록을 영구적으로 보유할 수 있도록 허용하였다.[45] 이러한 개정이 FCRA의 입법취지를 명확히 하기 위한 개정일지는 몰라도 데이터 브로커 산업의 규율에 있어서 실효성을 약화시킨 것임에는 틀림없다. 이러한 개정은 공적기관에 의해 삭제된 범죄기록 등의 민감한 개인정보의 공개와 활용을 더 북돋아주게 된다.[46] 더욱이 FCRA가 모든 데이터 브로커에게 적용된다 할지라도 데이터 브로커에게 적용되는 유일한 규제는 그들이 가능한 최대한의 정확성을 담보하기 위한 합리적 절차를 준수하여야 한다는[47] 추상적이며 애매모호한 규정뿐이다. 이러한 규정은 데이터 브로커에게 기록을 현행화, 최신화해야 할 어떠한 의무도 부여하지 않는다.

이러한 FCRA의 한계가 지적되면서 FTC는 2014년 5월 9개 데이터 브로커의 실태를 분석한 조사 보고서를 발표하고 의회에 데이터 브로커사업자의 투명성 확보와 소비자의 정보접근 및 수정 권한을 규정한 법률안을 만들 것을 권고한 바 있다. FTC는 미 의회에 상품 카테고리별로 소비자 보호 방안의 입법화 제안하였다. 마케팅 부문과 관련하여서는 데이터 브로커 사업자들의 정보 수집 및 사용 절차, 소비자들의 정보접근 도구 및 옵트 아웃 권한을 제공하는 인터넷 포털 사이트의 운영을 규정할 것을 제안하였으며, 또한 개인정보를 바탕으로 추론하는 '민감한(sensitive)' 데이터 프로그램이나 메모리와 데이터 카테고리에 대한 접근을 보장할 것, 원 데이터는 물론이고 이 데이터로부터 추론한 데이터를 공개하고, 데이터 소스의 이름과 카테고리를 공개할 것 등을 제안하였다.

리스크 감소를 위해 개인의 권리를 제한하는 소비자 정보 제공시 소비자들에게 투명성하게 공개할 것, 특히, 정보의 오류를 수정할 수 있는 접근권을 보장할 것의 내용을 포함하고 있으며, 인물 검색과 관련하여서도 소비자가 자신의 정보에 접근할 수 있도록 하며 옵트 아웃에 관한 권리를 보장해야 하며, 데이터 브로커들은 자신들이 취득한 개인정보의 소스를 공개하는 내용을 담고 있다.

다. 버몬트 주 : 「데이터 브로커와 소비자 보호에 관한 법률」

미국 버몬트 주 의회는 2018년 5월 22일 「데이터 브로커와 소비자 보호에 관한 법률(H.764: An act relating to data brokers and consumer protection)」을 제정하였다. Equifax Inc.사건[48]으로 인해 버몬트 주의 소비자정보가 대량 유출된 후 주의회와 법무부의 대책마련에 대한 조사를 기초로 한 것이다.

43) Advisory Letter from William Haynes, Division of Credit Practices, Fed. Trade Comm'n, to Richard LeBlanc, Due Diligence, Inc. (June 9, 1998), available at http://www.ftc.gov/os/statutes/fcra/leblanc.shtm (regarding Sections 603, 607, and 609 of the Fair Credit Reporting Act).

44) Fair and Accurate Credit Transactions Act of 2003(FACTA), Pub. L. No. 108-159, 117 Stat. 1952 (2003).

45) Jon Geffen & Stefanie Letze, Chained to the Past: An Overview of Criminal Expungement Law in Minnesota—State v. Schultz, 31 WM. MITCHELL L. REV. 1331, 1335(2005) p. 1339.

46) Wayne, 앞의 글, 269면.

47) FCRA § 1681e(b).

48) 2017 년 9 월 7 일, 미국의 3대 주요 신용보고기관 중 하나인 Equifax Inc.는 1억 4,300만 명의 미국 소비자 정보(이후 14550만 개로 증가) 관련된 보안 위반 사례가 발생했다고 발표했다. 이로 인해 버몬트 주의 시민 247,607명(버몬트 인구의 약 40%)의 개인 정보가 유출되었고 이러한 개인정보에는 이름, 사회 보장 번호, 생년월일, 주소, 경우에 따라 운전 면허증 번호가 포함된다. 부가적으로 약 209,000개의 신용 카드 번호와 분쟁 관련 문서, 그리고 약 182,000명의 미국 소비자에 대한 정보가 노출되었다.

입법의도에 대하여는 다음과 같이 밝히고 있다. 첫째, 소비자에게 데이터 브로커와 그들의 데이터 수집 관행에 대하여 더 많은 정보를 제공하고, 소비자의 개인정보 처리에 대하여 사후적으로 철회할 권리(the right to opt out)를 부여하기 위함이다. 둘째, 데이터 브로커들에게 적절한 보안기준을 준수하도록 하기 위함이다. 즉 데이터 브로커로 하여금 적절한 기술적·물리적·관리적 세이프가드를 제공하는 정보보안프로그램을 채택하도록 함으로써 잠재적 사이버공격으로부터 보호하기 위함이다. 셋째, 부당한 행위를 하려는 의도로 개인 정보를 수집하는 것을 금지하고자 함이다. 즉 스토킹, 괴롭힘, 사기, 신원 도용 또는 차별을 목적으로 하는 개인 정보의 획득 또는 사용을 금지함으로써 버몬트 주의 시민들이 잠재적인 피해를 입히지 않도록 하기 위함이다. 넷째, 소비자 신용 정보를 보호하기 위해 재정적 장벽을 제거하고자 함이다. 즉 신용보고기관이 보안동결[49]을 위해 요금을 부과하는 것을 금지함으로써 신용 보고서에 보안 동결을 하고자 하는 버몬트 시민에게 재정적인 장벽을 제거하고자 하는 것이다.[50]

동 법은 소비자 보호 차원에서 데이터 브로커를 직접적으로 규율한 미국 최초의 법률이다.[51] 주요 내용은 다음과 같다.[52]

우선 '데이터 브로커'에 대하여 "단독 또는 공동으로 자사의 비즈니스와 직접적인 관계가 없는 소비자의 '중개된 개인정보(brokered personal information)'[53]를 고의로 수집하고 판매하거나 제3자에게 라이선스를 부여하는 단일 사업자 또는 사업자의 결합체"라고 개념정의 하고 있다(§ 2430).[54]

이때 i) 사업자의 제품 또는 서비스의 이용자에 해당하는 등 자사의 비즈니스와 직접적인 관계가 있는 경우[55] ii) 일회성, 간헐적 또는 우발적인 데이터 판매 또는 라이선스를 부여하는 경우, iii) 업무의 위탁관계에 의해 데이터를 중개처리하는 경우나 공개적으로 이용가능한 정보를 제공하는 것[56]은 데이터 브로커의 범위에서 제외한다.

다음으로 본 법률은 데이터 브로커에 대하여 등록의무를 부여하였다는데 의의가 있다. 데이터 브로커에 대하여 규율하기 위해서는 누가 데이터 브로커 비즈니스를 영위하고 있는지에 대한 현황파악이 우선되어야 한다. 따라서 이 법은 데이터 브로커로 하여금 버몬트 주 법무장관에 등록하도록 의무를 부여하였다(§ 2446). 등록 시 데이터 브로커는 "i) 데이터 브로커의 명칭, 주된 거주지(사업지), 이메일주소 및 인터넷 주소, ii) 소비자가 데이터 브로커의 개인정보 수집·판매를 거부(옵트아웃) 할 수 있는 방법, iii) 소비자가 옵트아웃 할 수 없는

49) 보안동결(security freeze)이란, 신용, 대출 및 기타 서비스가 신용주체의 동의 없이 그의 이름으로 승인되는 것을 막기 위해 고안된 개인이 할 수 있는 데이터 판매 제어 제도. 미국의 거의 모든 주에서 주 법을 통해 인정하고 있으며, Credit freeze, credit report freeze, credit report lock down으로도 불림. 보안동결을 하면, 개인이 데이터 공개에 대한 권한을 부여할 때까지 신용 보고 기관의 데이터를 잠금(lock the data). 명의 도용 피해를 방지할 수 있는 가장 효과적인 방법으로 평가받고 있음(출처 : Wikipedia).

50) https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2018/06/H-0764.pdf (2018.10.15. 확인).

51) https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/ (2018.10.14.확인).

52) 법안의 주요내용에 대하여는 '법률 원문' 및 '한국인터넷진흥원, 해외 개인정보보호 동향보고서, 2018.7' 내용을 참조함.

53) § 2430. 용어정의 (1)(A)"중개된 개인정보(Brokered personal information)"라 함은 "소비자에 대한 전산화된(computerized) 정보 중 다음 중 하나 또는 그 이상을 의미한다. 다만 소비자의 영업 또는 전문성과 관련하여 공개되어 이용 가능한 정보는 포함하지 아니한다. : i)이름, ii)주소, iii)생년월일, iv)출생지, v)어머니의 혼전 이름, vi)지문, 망막, 홍채 이미지 또는 기타 고유한 신체적 특성을 나타내는 바이오정보(biometric data) vii)소비자의 직계 가족 또는 가족 구성원의 이름 또는 주소, viii)사회보장번호 또는 정부에서 발행한 신분증 번호, ix)판매되거나 라이선스가 제공된 다른 정보와 단독 또는 조합하여 사용함으로써 소비자를 식별할 수 있는 기타 정보".

54) §2430. DEFINITIONS(4)(A) "Data broker" means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship.

55) i)소비자가 현재 또는 과거에 사업자 제품 또는 서비스에 등록된 고객, 구독자, 이용자인 경우 ii)사업자에 고용된 직원, 계약자인 경우 iii)투자자인 경우 iv)기부자인 경우 등.

56) i) 타사 전자 상거래 또는 응용 프로그램 플랫폼 개발 또는 유지관리, ii) 통신 사업자를 대신하여 또는 통신 사업자의 기능으로 이름, 주소 및 전화번호를 포함한 디렉토리 서비스를 제공하는 행위, iii) 소비자의 사업이나 직업과 관련하여 공개적으로 이용가능한 정보를 제공하는 것, iv) 건강 또는 안전 목적으로 실시간 경고를 통해 공개적으로 이용 가능한 정보를 제공하는 것.

데이터의 수집·판매의 경우를 명시하는 문구, iv) 전년도에 데이터 보안 침해 사실이 있는지 여부와 그로 인해 영향을 받는 소비자의 수, v) 데이터 브로커가 미성년자의 중개된 개인정보를 보유하고 있다는 사실을 인지하는 경우, 미성년자의 중개된 개인정보에 적합한 수집 관행, 데이터베이스, 영업 활동, 옵트아웃 정책에 대해 상세히 기술(記述)한 별도의 진술서, vi) 데이터 수집 관행과 관련하여 데이터 브로커가 제공하기로 선택한 추가 정보"를 제공하여야 한다.

다음으로 데이터 브로커에게 '정보보호의무'를 부여하고 있다.[57] 데이터 브로커는 데이터 브로커의 규모, 범위, 유형 등에 적합한 기술적·관리적·물리적 안전조치를 포함하는 포괄적인 "정보 보안 프로그램(Information security program)"을 개발, 구현, 유지해야 한다. 이러한 정보 보안 프로그램이 포함하여야만 하는 최소한의 사항에 대하여도 규정하고 있다.[58]

그리고 "소비자에 대한 정보공개"를 규정하고 있다.[59] 이 규정은 모든 데이터 브로커에게 적용되는 것이 아니라 CRA에게 적용된다. CRA는 소비자의 요청이 있고 소비자에 대한 적절한 식별이 가능한 경우, 소비자 요청에 따라 정보의 이용자가 사용할 수 있는 모든 정보를 소비자에게 명확하고 정확하게 공개해야 한다. 공개정보는 "i) FTC에서 발급한 의견이나 지침을 준수하는 형태 및 방식으로 소비자와 관련된 신용 점수 또는 예측 변수, ii) 이전 12개월 동안 소비자에 관한 정보를 요청한 사용자의 이름 및 각 요청 날짜, iii) 정보에 대한 명확하고 간결한 설명"이다.

다만 연간 등록[60], 기술적 요구사항[61], 소비자에 대한 정보 공개[62] 요건 등 데이터 브로커에 관한 사항은 2019년 1월 1일부터 발효된다.

Ⅲ. 법적 현안과 쟁점

1. 우리법제와 데이터 브로커

가. 데이터 브로커와 개인정보처리자

우리 「개인정보 보호법」은 '개인정보처리자'를 '업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등'으로 정의하고 있다. 그러나 여기서의 '개인정보파일'은 '개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)'로서 전자적 형태로 구성된 데이터베이스뿐만 아니라 그 외에 체계적인 검색·열람을 위한 색인이 되어 있는 수기(手記) 문서 자료 등도 포함된다.

미국의 데이터 브로커는 우리법률에 의하면 모두 개인정보처리자에 해당된다. 다만 우리법상 개인정보처리자는 '업무'를 목적으로 개인정보를 처리함에 있어 그 업무자체가 반드시 '개인정보'에 대한 업무만을 의미하는 것은 아니다. 재화와 서비스의 거래과정에서 개인정보의 수집 등 처리가 필수 불가결하므로 대부분 개인정보의 처리는 다른 업무수행을 위한 부수적 업무이다. 예를 들어, SKT 등 통신사는 통신서비스를 제공하기 위하여, 아마존은 물건의 매매를 위하여 개인정보를 처리한다. 이들의 주된 업무는 통신서비스 제공 또는 물건의 매매이다. 그러나 데이터 브로커는 개인 정보를 수집해서 그 정보를 제3자와 공유하거나 재판매하는

57) Subchapter 5. Data Brokers, § 2447. DATA BROKER DUTY TO PROTECT INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS.

58) i) 프로그램 유지를 위한 직원 1명 이상 지정 및 직원에 대한 보안 훈련, ii) 프라이버시 위험평가(privacy risk assessments)를 수행하고, 현행 보호조치의 효과를 평가하고 개선하는 프로세스 확보, iii) 정보보안 프로그램 규칙 위반 시 징계 조치 관련 기록 보관 등이다.

59) § 2480b. DISCLOSURES TO CONSUMERS.

60) Subchapter 5. Data Brokers, § 2446. ANNUAL REGISTRATION.

61) Subchapter 5. Data Brokers, § 2447. DATA BROKER DUTY TO PROTECT INFORMATION; STANDARDS; TECHNICAL REQUIREMENTS.

62) Subchapter 5. Data Brokers, § 2480b. DISCLOSURES TO CONSUMERS.

것이 주된 업무의 내용이다.

얼핏 개인정보처리 업무를 수탁받은 '수탁자'와 데이터 브로커의 업무내용이 유사할 수 있으나, 개인정보처리업무의 위수탁관계에서 수탁자는 위탁자 즉 개인정보처리자의 업무를 보조해 주는 것이지, 정보주체와의 관계에서 직접적인 개인정보처리자는 아니다. 개인정보의 오·남용으로 발생한 정보주체에 대한 손해는 위탁자인 개인정보처리자의 몫이다. 따라서 수탁자의 업무는 대부분 보관, 관리 등 위탁받은 범위 내의 수동적 업무에 그치며 적극적 판매나 제공은 불가하다. 그러나 데이터 브로커는 개인정보에 대한 직접적 처리/지배권을 가진다. 개인정보의 분석, 제공, 판매 등 개인정보처리업무는 자신의 본업이지, 타인을 위하여 하는 업무가 아니다.

나. 개인정보의 처리 : 제3자 제공, 판매 등

우리나라는 개인정보의 판매 등을 포함한 제공에 엄격한 규율을 적용하고 있다. 정보주체의 동의, 법령상 업무 수행 등 법령에 열거된 사유에 해당되지 않는 한 개인정보의 수집, 제공은 엄격히 제한된다. 특히 우리법상 개인정보 규제의 기본방향은 정보주체의 동의에 기반 한 개인정보처리(수집·이용·제공을 포함한다)라 해도 과언이 아니다. '개인정보 보호법' 제15조 제1항은 개인정보(민감정보 제외)의 수집 이용이 정당화되기 위한 요건을 6가지로 제시하고 있다. 정보주체의 동의(제1호)를 여러 합법성 요건 중의 하나로 제시하면서, 법령상의 무나 법령상 소관업무의 수행을 위한 경우(제2호 및 제3호), 계약의 체결·이행을 위한 경우(제4호), 정보주체 등의 생명·신체·재산의 이익을 위하여 필요한 경우(제5호), 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우(제6호) 등을 규정하고 있다. 법령상 의무나 법령상 소관업무의 수행을 위한 경우는(제2호 및 제3호) 대부분 공익적 차원에서 정보주체의 사전동의권이 제한되는 경우이므로 이를 제외한다면 실질적으로 나머지 각호의 경우는 모두 정보주체의 사전동의를 명시적으로 규정하지 않았다 할지라도 그 동의가 전제되어 있다고 볼 수 있다. 개인정보의 판매를 포함한 제3자 제공의 경우에는 더 엄격한 규제가 적용되며, 결국 '수집·이용'과 같이 '동의'에 기반하고 있음에 비추어 볼 때 대동소이하다.

이러한 우리법제의 환경에서 특별히 정보주체의 동의 없이 개인정보를 수집, 판매, 제공 등의 업무를 처리하는 데이터 브로커라는 업역은 현실적으로 불가능하다. 앞서 언급한 바와 같이 미국은 민간의 개인정보처리에 대하여 의료, 교육 등 영역별 규율을 하고 있는 바, 데이터 브로커의 개인정보 수집, 판매, 제공을 직접적으로 규율하는 법규는 없다. 데이터 브로커가 신용, 보험, 고용 관련 데이터를 제공하는 경우에만 FCRA가 적용될 수 있다.

다. 데이터 브로커 산업에 대한 비판과 한계

미국에서도 데이터 브로커의 위해에 대한 지적 및 비판이 제기되고 있다. 소비자의 사후 철회권 행사의 곤란, 데이터 브로커들의 보안기준 미흡으로 인한 유출, 부당한 목적의 개인정보 수집 등에 대한 비판과 이를 개선하기 위한 입법에 대한 수요가 지속적으로 제기되고 있다.[63] 이를 반영하듯 연방차원의 데이터 브로커 규제의 시도가 여러 차례 있었지만 실질적으로 입법화되지 못하였다. Bill S.1815는 2017년 9월 14일 미국 상원에서 제안된 바 있다. 이 법안은 소비자로 하여금 데이터 브로커가 수집한 정보를 검토, 수정할 수 있도록 하며, 소비자에게 마케팅 목적으로 특정 정보를 공유하지 않도록 선택할 수 있는 권리(the Right to Opt-Out)를 부여하는 내용을 담고 있다. 또한 데이터 브로커에게 수집하는 정보의 정확성을 보장하고 포괄적인 개인정보 보호 및 데이터 보안 프로그램을 구현하는 절차를 수립하도록 규정하고 있다. 또한 데이터 브로커가 허위로 개인 정보를 획득하는 것을 금지하고 있다. 2014년과 2015년에도 이와 유사한 내용을 담고 있는 법안이(S.668 및 S. 2025/H.R) 제안된 바 있다. 2014년에 제안된 S.1995 법안 역시 데

63) Wayne, 앞의 글, pp. 266~271 ; Office of the Attorney General Department of Financial Regulation, 앞의 글, pp. 3-12.

이터 유출 문제의 해결을 위해 데이터 브로커에게 적용되는 보안 표준에 대하여 규율한 바 있다. 그러나 그 법안 중 어느 것도 지금까지 통과하지 못했다. 아마도 이미 형성되어있는 데이터 브로커 산업에 대한 부담과 4차산업혁명이라는 기술적 변혁속에서 데이터 활용의 중요성이 부각되면서 이러한 법안의 실행은 쉽지 않을 것이다.

현행법상 정보주체의 권리가 보장되기 위해서는 우선 정보주체가 자신의 개인정보가 어떠한 형태로 누가 가지고 있는지를 인지하여야 한다. 그러나 데이터 브로커는 이미 오랜 시간 정보주체가 알 수 없는 출처와 방식으로 개인정보를 수집, 처리, 판매해 왔다. 이미 연혁적으로 볼 때 인터넷이나 이메일이 등장하기 훨씬 전부터 마케팅을 목적으로 소비자 데이터를 수집하여 왔으며, 우편물을 통한 마케팅뿐 아니라 전화 마케팅 등의 목적을 위해 공공정보, 사회 조사 결과 등을 활용한 소비자 정보의 축적이 진행되었다.

일례로 미국의 대표적 데이터 브로커, 액시엄(Acxiom)은 인터넷이나 컴퓨터가 보편화되지 않은 1969년 설립되었다. 지금은 액시엄은 수만 대의 서버에 미국인 3억 명을 포함한 전 세계 약 7억 명 이상의 소비자 정보를 저장하고 있으며, 저장된 개인 한명에 대한 정보가 약 1500여 종에 이른다. 전 세계에서 가장 많은 데이터베이스(DB)를 보유하고 판매하고 있으며, 미국 연방 정부뿐만 아니라 포춘 100대 기업이 이 회사에서 데이터를 구매해 비즈니스에 활용하고 있다.[64] 인터넷의 보편화와 그로 인한 전자상거래 등 파생산업의 확산, 특히 스마트폰의 대중화는 이들이 수집하는 소비자 정보의 양을 급속도로 확장시켰다. 빅데이터 환경에서 데이터 분석기술이 고도화되면서 이들이 제공하는 데이터에 대한 데이터생태계의 의존도도 더 높아질 수밖에 없다.

미국의 데이터 브로커 시장에서 정보주체에 해당하는 소비자는 데이터 브로커가 어떻게 존재하는지, 데이터 브로커에 해당하는 기업이 누구인지, 그들이 어떠한 정보를 어디로부터 수집하는지 알 수 없다. 따라서 데이터 브로커에 대한 정보주체의 권리들-열람청구권, 정정·삭제청구권, 처리정지 청구권 등-의 실행은 무색하다.

결국 버몬트주법도 데이터 브로커의 정보수집 자체를 막을 수는 없으며(정보주체의 완벽한 인식하에 데이터 브로커가 개인정보를 수집하게 하는 것을 불가능할 것이다) 후발적으로 데이터 브로커의 개인정보 처리과정에 있어서 일정한 의무를 부여하고, 사업등록을 통해 정부의 관리감독을 꾀하고자 하는 방향으로 규율한 것이라 할 수 있다.

우리나라의 경우 개인정보의 수집단계에서 엄격한 사전동의를 요건으로 하므로 실질적으로 데이터 브로커 산업 자체가 미비하다. 그러나 통신, 의료, 금융업에서 지니고 있는 소비자 개인정보는 거의 전 국민의 것이라 해도 무방할 정도로 이미 개인정보 자체는 특정기업에 의해 대규모로 수집되어 있는 상태다.

즉 특정기업에 의해 전국민의 개인정보가 수집되어 있다는 사실은 구지 데이터 브로커 산업을 언급하지 않아도 우리나라나 미국이나 별반 다르지 않다. 그렇다면 엄격한 사전동의 중심의 현재 우리나가 개인정보 규율체계가 과연 데이터산업혁명 속에서 정보주체의 권리를 합당히 보호할 수 있는지에 대하여는 재고해 볼 필요가 있다. 그러기 위해서는 개인정보의 법적 성격에 대하여도 다시 고찰해 볼 필요가 있다. 이하에서는 이러한 쟁점들에 대하여 검토해 보기로 한다.

2. 법적 현안과 규율방향

가. 개인정보DB에 대한 재산적 가치의 존중

1) 개인정보의 법적 성격

개인정보의 법적 성격을 일의적으로 정의내리기 곤란하며, 기술발달에 따라 사회변화를 수용하면서

64) 일례로 액시엄은 9.11 테러 직후 미국 정부에 협조해 자사가 보유하고 있던 신원 정보 DB에서 19명의 비행기 납치범 중 11명의 신원의 정보를 찾아 제공했으며, 이를 비행기 탑승명단과 대조, 분석해 범인을 찾을 수 있었다.

그 법적 성격도 다각화된 측면에서 검토할 필요가 있다. 초기 미국에서 프라이버시권에 대하여 논의될 당시만 해도 '개인정보'는 재산적 권리가 아니라 인격권적 성격에 초점을 맞춘 것이었다.[65] 그러나 이제는 빅데이터, 인공지능 등의 기술을 활용한 서비스를 영위하기 위해서 없어서는 안 되는 영업자산이다. 개인정보가 없는 '인스타그램'이나 '페이스북', '유튜브'를 상상할 수 없다. 즉 개인정보는 프라이버시 보호측면으로서 뿐만 아니라 영업의 자유, 표현의 자유, 알 권리 등의 측면에서도 작용하게 된다. 혼자 있을 자유를 보장받아야 한다는 측면에서 프라이버시권의 보호객체가 될 수 있으나, 표현의 자유를 보장받는다는 의미에서 공개의 대상이 될 수 있고, 영업의 자유 측면에서 재산권의 객체이기도 하다. 따라서 '개인정보'는 그 보호법익에 따라 탄력적 해석운용이 필요하다.[66] 따라서 그 법익 간 충돌의 경우에는 이익형량을 통해 균형을 맞출 필요가 있다. 특히 '데이터 브로커' 산업 형성의 근간이 된 개인정보 데이터베이스의 경우 데이터베이스제작자 입장에서는(그가 개인정보 처리자이건 그렇지 않던 간에) 개인정보 데이터베이스 구축을 위해 상당한 투자가 부여된 것이다. 따라서 이러한 경우 개인정보의 처리와 관련하여 재산적 법익과 개별 정보주체의 개인정보 자기결정권 간의 갈등은 더 첨예할 수밖에 없다.

2) 개인정보, 개인정보파일, 개인정보데이터베이스

'개인정보'를 칭할 때 통상 개인정보'파일'이나 개인정보'데이터베이스'를 의미하기 보다는 개개의 개인정보를 의미한다고 볼 수 있다. 우리 「개인정보 보호법」은 '개인정보파일'에 대하여 '개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)'로 규정하고 있다. 여기에는 전자적 형태로 구성된 데이터베이스뿐만 아니라 그 외에 체계적인 검색·열람을 위한 색인이 되어 있는 수기(手記) 문서 자료 등도 포함된다. 즉 '개인정보파일'은 검색의 용이성을 갖춘 개인정보라는 소재의 집합물이다.

「저작권법」에 의해 보호되는 데이터베이스는 "소재를 체계적으로 배열 또는 구성한 편집물로서 개별적으로 그 소재에 접근하거나 그 소재를 검색할 수 있도록 한 것"으로 정의되고 있다(저작권법 제2조제19호). "편집물"은 "저작물이나 부호·문자·음·영상 그 밖의 형태의 자료(이하 "소재"라 한다)의 집합물"을 말한다(저작권법 제2조제17호). 즉 데이터베이스에서 소재는 굳이 저작물일 필요가 없으며, 데이터, 정보, 지식을 망라한다. 즉 '검색의 용이성'을 갖춘 '소재'의 '집합물'이 데이터베이스다.

이렇게 볼 때 '검색의 용이성'을 갖춘 이상 개인정보라는 소재의 집합물로서 '개인정보파일'은 「저작권법」상 '데이터베이스'에 해당될 여지가 다분하다. 뿐만 아니라 개인정보를 수집함으로써 개인정보파일을 만든 자는 대부분 '개인정보처리자' 이므로, 이들은 대부분 '데이터베이스 제작자'에 해당되게 된다. 그러나 「개인정보 보호법」상 '개인정보파일'에 대한 규율은 정보주체의 권리를 보장하기 위해 개인정보처리자를 강력하게 규제하는 것이며, 「저작권법」상 '데이터베이스'의 경우 저작물은 아니나, '데이터베이스'를 제작하는데 소요된 투자가치를 인정하여 데이터베이스제작자에게 재산적 권리를 부여하는 것이므로 '개인정보'를 소재로 하는 '데이터베이스'의 경우 개인정보처리자로서의 의무와 데이터베이스제작자로서의 권리, 그리고 정보주체의 권리 간에 상충문제가 발생할 수밖에 없다.

3) 데이터베이스제작자의 권리와 정보주체의 권리 조화 필요

저작권법은 "데이터베이스의 제작 또는 그 소재의 갱신·검증 또는 보충(이하 "갱신등"이라 한다)

65) Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890). at 205. As Warren and Brandeis wrote: "he principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality **not the principle of private property, but that of an inviolate personality**."

66) 김현경, 개인정보의 개념에 대한 논의와 법적 과제, 미국헌법연구 第25卷 第2號, 155~157면.

에 인적 또는 물적으로 상당한 투자를 한 자"를 "데이터베이스제작자"라고 하며 그에게 5년간 데이터베이스의 전부 또는 상당한 부분을 복제・배포・방송 또는 전송(이하 이 조에서 "복제등"이라 한다)할 권리를 부여한다(저작권법 제93조제1항 및 제95조제1항). 엄격히 저작자가 아님에도 불구하고 이러한 데이터베이스제작자의 권리를 보장하는 것은 데이터베이스의 제작에 들이는 막대한 투자에도 불구하고, 제3자가 이를 추출하여 재이용하는 것이 용이하고, 이러한 행위는 제작자의 투자와 노력이라는 법익에 대한 침해가 되며, 이는 궁극적으로 데이터베이스 산업과 활용을 저해할 것이라는 우려에 기인한다.

따라서 현행 저작권법은 데이터베이스제작자에 대하여 저작인접권[67]과 유사한 방법에 의한 보호를 취하고 있으며 데이터의 선택과 배열의 창작성이 아니라 데이터베이스를 구성하는 데이터의 체계화와 이와 관련된 상당한 투자를 보호하는 것이다. 데이터베이스의 제작자는 이러한 투자에 근거해서 권리를 취득하며, 또 이러한 투자가 미치는 범위 내에서 보호를 받는 것이다.[68] 즉 여기서 보호받는 데이터베이스란 제작자에 의한 "상당한" 투자를 전제로 하는 일련의 데이터 축적물로서 그 체계성과 검색가능성으로 인해 보호를 받게된다.

따라서 개인정보처리자가 개인정보라는 소재를 구성요소로 하는 체계화된 검색가능한 축적물을 상당한 투자를 통해 제작한 경우 「저작권법」상 '데이터베이스 제작자'에 해당되어 그러한 개인정보 데이터베이스(개인정보파일)에 대한 복제, 배포, 방송, 전송할 권리를 취득하게 된다. 그러나 이러한 권리는 사실상 「개인정보 보호법」상 '정보주체의 동의' 없이는 행사할 수 없다.

2003년 데이터베이스에 대한 보호제도가 도입되어 약 15년 가까이 운영되었으나 지금까지 실질적으로 도입당시의 기대만큼 제도가 활발히 활용된 것은 아니다.[69] 그러나 빅데이터, 4차산업혁명 등 현재의 데이터를 둘러싼 기술적・경제적 환경은 다르다. 이미 GDPR 제20조에 정보주체의 '정보이동권' 도입된 것 등을 이유로 데이터의 오너쉽에 대한 논의가 진행 중이며,[70] '개인정보'에 경쟁법에서 규정하는 필수설비원리(Essential Facilities Doctrine)를 적용할 수 있다는 의견[71] 등 개인정보의 재산적 가치에 근거한 신규 권리여부의 논의가 진행 중이다.

개개의 개인정보는 정보주체의 인격적 보호와 밀접한 관련이 있으며, 개인정보처리자에게 어떠한 재산적 가치를 가지는 것은 아니다. 그러나 대량화된 개인정보 즉 개인정보파일은 개인정보처리자의 투자와 노력이 들어간 자산이다. 개별 개인정보의 재산적 가치에 대하여는 논란이 분분할 수 있겠지만 집합화된 개인정보는 해당 기업의 주요 자산으로 그 재산적 가치는 무시할 수 없다. 개인정보가 대량화・데이터베이스 되었을 때 그 활용의 가치는 더 극대화되고 그만큼 보호의 필요성도 더 커진다. 데이터 브로커가 보유, 지배하는 개인정보는 이미 미국 내 전국적 수준의 규모로 확대되었음은 앞서

67) 저작권제도는 1차적으로 인간의 사상 또는 감정을 표현한 창작물(copyright work)을 보호하는 제도이나 문화 및 관련산업 발전의 취지상 저작물은 아니지만 그와 인접한 객체를 보호하는 저작인접권(copyright-related rights)이라는 제도를 두고 있다. 저작권법이 인정하고 있는 저작인접권자로는 가수, 무용수, 성우 등 실연자(performer), 음반의 제작에 투자하고 책임을 부담하는 음반제작자(phonogram producer), 방송을 공중에 전달하고 프로그램 편성과 관련된 책임을 부담하는 방송사업자(broadcasting organization) 등이 해당된다. 실연자는 그 예술성에 근거하여 보호를 받지만, 음반제작자와 방송사업자는 다분히 투자에 대한 대가로서 일종의 재산권을 부여받는 것이라고 평가되고 있다.

68) 이일호/김기홍, "빅데이터는 누구의 소유인가?: 빅데이터의 저작권법에 의한 보호와 공공부문의 빅데이터 활용 문제", 「한국지역정보화학회지」 제19권 제4호, 2016, 43면.

69) 데이터베이스의 보호를 강변했던 산업계 역시 해당 제도를 거의 활용하지 않고, 이 때문에 중요한 지침이 될 수 있는 판례들도 축적되지 못한 상황이다. 위의 글, 51-53면.

70) GDPR 제20조는 정보주체가 개인정보처리자에게 자신의 개인정보를 다른 개인정보처리자에게 이동시켜달라고 요구할 수 있는 권리인 '정보이동권(Right to data portability)'을 도입하였다. 이같은 배타적인 권리규정은 개인정보에 대한 재산권적 접근으로서 데이터 소유권(data ownership) 인식에 한발 다가선것이 아닌가 라는 해석이 있다. Nadezhda P., "빅데이터 변화 이후에도 개인정보의 재선권적 성격은 타당한가?", 「경제규제와 법」, 제10권 제2호(통권 제20호), 2017.11, 224~227면.

71) A. Vanberg, M. Ünver, The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?, European Journal of Law and Technology Vol 8, No 1, 2017.

주지한 바이다. 우리나라 역시 개인정보의 집적화(통신, 의료, 금융 영역에 있어서)는 무시할 사항이 아니다. 따라서 현행법상 데이터베이스제작자의 권리와 정보주체의 권리를 공존시킬 수 있는 개인정보데이터베이스에 대한 특별한 취급이 필요하다.[72]

특히 미국의 데이터 브로커 산업이 해외에 서버를 두고 국내에서 내국민을 상대로 데이터분석 처리 서비스를 행하게 될 경우 이들에게 현행의 우리 「개인정보 보호법」을 적용하기에는 한계가 있다. 이들은 각종 소스를 통해 개인정보를 무작위로 수집, 가공하나, 이에 대하여 국내법 위반을 이유로 방송통신위원회나 경찰 등이 수사나 조사를 수행하는 것이 얼마나 비실효적인지는 이미 구글, 페이스북 등 외국 기업 사례를 통해 확인된 바 있다. 「정보통신망 이용촉진 및 정보보호등에 관한 법률」의 개정으로 국내 대리인을 지정한다 할지라도 해당 조문의 실효성에 대하여는 여전히 불확실하다. 수집의 출처가 불명확하므로 이들이 우리 국민의 개인정보를 처리하고 있다는 사실확인 자체가 곤란하기 때문이다.

4차산업혁명의 달성에 필요한 핵심기술과 서비스가 모두 데이터에 기반한다는 사실에 비추어 볼 때, 또한 데이터의 속성(비배타성/비배제성)으로 인해 데이터규범의 집행이 물리적 '국경' 안에서 이루어지기 곤란하다는 점을 감안할 때,[73] 집합적 데이터에 대한 규율방향의 근본적 변화를 모색할 필요가 있다.

나. 정보주체의 권리의 현실화 : 수집의 정당성에서 '처리의 공정성'으로

1) '수집'의 만연(蔓延)화와 정보주체의 통제권 행사 곤란

앞서 검토하였듯이 미국에서 정보주체가 데이터 브로커의 기록에서 본인과 관련된 기록을 삭제하는 유일한 방법은 개인적으로 그러한 정보를 삭제해 달라고 요청하는 것이다. 이러한 과정은 매우 힘들며 법원 처분 및 환급 명령을 포함한 여러 문서 제출을 필요로 한다. 일부 데이터 브로커는 웹사이트의 보고서에 표시되는 여러 정보의 사본을 함께 제출하도록 요구하기도 한다. 이러한 요구는 정보주체가 본인의 기록이 브로커의 데이터베이스에 있는지 여부를 확인하기 전에 브로커의 소비자보고서를 구매하도록 강요하는 결과를 초래하기 때문에 더더욱 문제가 된다. 정보주체가 가까스로 하나의 데이터베이스에서 본인의 정보를 삭제하였다 할지라도 이러한 개별적 실행은 매우 비효율적일 수밖에 없다. 동일한 정보를 가지고 있는 모든 다른 데이터 브로커에게 일일이 동일한 절차를 밟아 정보를 삭제하여야 한다. 종종 여러 데이터 브로커 기업들은 별도의 데이터베이스를 유지관리 하므로, 각각의 데이터 브로커에게 모두 연락을 취하여 정보를 삭제하도록 요청하여야 한다.[74]

앞서 언급한 대로 비단 미국의 데이터 브로커를 언급하지 않아도 이미 통신, 금융, 의료 영역의 특정기업에 의해 전 국민의 개인정보가 수집되어 있다는 사실은 우리나라나 미국이나 별반 다르지 않다. 예를 들어 우리나라의 경우도 개인의 의료정보(진료기록 등)가 병원, 보험회사, 약학정보원, 보건복지부 등 여러 기관에서 수집, 처리되고 있지만 정보주체로서는 어디에서 어떠한 형태로 보유, 처리되고 있는지 알 수 없다. 동일한 정보가 동일한 형태로 보유, 활용되고 있는지 현행화 되지 못한 상태로 활용되고 있는지 알 수가 없다. 정보주체가 알 수 없다는 것은, 사전 동의권, 정정·삭제권 등 우리가 이상적으로 설정해 놓은 통제권을 실질적으로 행사하기 곤란하다는 것을 의미한다.

2) 데이터 기술의 발달과 처리의 불투명성

기존에 개인정보를 단순한 데이터 처리 기술을 통해 처리할 경우 정보주체가 통상적으로 그 처리

72) 김현경, "개인정보의 개념에 대한 논의와 법적 과제", 「미국헌법연구」 第25卷 第2號, 157-158면.

73) 김현경, "데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰", 「토지공법연구」 78권, 2017, 213-260면.

74) Wayne, 앞의 글, 267~268면.

과정을 파악할 수 있다. 예를 들어 채용과정에서 개인정보를 처리하는 경우 경력, 학력, 전공 등의 개인정보를 바탕으로 어떠한 가중치를 통해 누가 채용되는지 어느 정도 파악과 예측이 가능하다. 따라서 처리의 공정성에 이의를 제기할 수 있으며, 처리과정이 수정될 수도 있다. 그러나 인공지능, 빅데이터, 클라우드 컴퓨팅 등을 기반으로 하는 데이터 분석 기술은 개인정보 처리과정을 외부에서 파악하는 것을 매우 어렵게 한다. 따라서 처리과정에 대하여 이의를 제기한다는 것 또한 실질적으로 곤란하다. 정보주체는 본인의 현행화된 개인정보가 공정하게 처리되기를 원하지만, 복잡한 처리 산식으로 포장된 딥 러닝 과정에서 개인정보가 어떠한 방식으로 활용되었는지 알 수가 없기 때문이다.

3) 정보주체의 권리보장 현실화

이처럼 데이터 기술의 발달은 개인정보의 광범위한 수집과 처리과정의 불투명성을 야기하고 있다. 그럼에도 불구하고 현행 개인정보보호법상 정보주체의 권리 보장방식은 엄격한 사전 동의, 정정·삭제 요구권 중심이다. 이미 대부분의 개인정보가 수집되어 있는 상태에서, 또한 처리과정을 정확이 파악할 수 없는 상태에서 이러한 '수집' 중심의 규율체계는 오히려 정보주체의 프라이버시 보호에 취약할 수밖에 없다.

개인정보에 대한 수집단계에서의 엄격한 규율은 '형식적 클릭동의'의 문제를 차치하고서라도 이미 실효성을 상실했다고 보아도 무리가 아니다. 따라서 정보주체의 수집동의권은 정보주체의 프라이버시가 정보처리자의 이익에 현저히 우월한 경우에만 적용되게 하는 것이 타당하다.[75] 그러므로 개인정보가 재산권의 객체로 취급되는 경우에 있어서는 정보주체의 동의권을 엄격히 하기보다는 정보주체와 이용자 간의 계약원리에 비추어 규율하는 것이 바람직하다. 개인정보를 거래하는 시장에 의하여 투명하게 개인정보가 관리되고, 개인정보 주체들은 개인정보를 이용하고자 하는 기업들과 협상을 통하여 공개범위를 결정함으로써 자신의 개인정보를 자율적으로 통제할 수 있도록 규율할 필요가 있다.[76] 다만 기업과 정보주체간 계약당사자의 불평등함을 감안하여 엄정한 약관심사 등을 통해 개인정보 처리와 관련된 공정한 계약 체결이 이루어지도록 하는 것이 정보주체 권리 보장을 위해 더욱 현실적이다. 또한 식별성이 낮은 정보와 민감하지 않은 정보의 경우 개인정보 규제에 있어서 서비스 제공을 위해 개인정보가 필요한 경우 혹은 서비스 제공과 개인정보의 수집이 사실상 대가관계에 있는 경우에는 개인정보의 수집 및 이용에 대한 규제의 필요성과 서비스제공의 유용성 사이의 균형이 중요한 요소로 고려되어야 할 것이다.

개인정보의 이용, 제공 과정에서 공정한 처리를 담보하기 위한 공익적 감독방안의 도입 등 개인정보 수집 후 처리과정에 있어서 공정성을 담보하기 위한 제도들이 더 견고하게 강구될 필요가 있다. 편향된 데이터의 채택으로 인해 정보주체에게 발생하게 되는 불이익을 막고, 부당한 차별과 불평등한 처우를 위해 개인정보가 처리되는 것을 감독하여야 할 것이다. 2016년 5월, 미국 백악관은 '빅데이터: 알고리즘 시스템, 기회와 시민권(Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights)'이라는 제목의 보고서에서[77] "데이터를 기반으로 하는 알고리즘 시스템은 인간의 편향되고 부적절한 판단을 없애는데 어느 정도 기여할 수 있지만, 오랜 기간 동안 규범, 사법제도 등으로

75) 2001년 스웨덴정부는 95년EU디렉티브에 따라 개인정보보호법을 제정하여 시행해본 결과, 95년디렉티브가 '표현의 자유 및 정보의 자유를 과도하게 제약하며….수집부터 삭제까지의 모든 단계를 규제하는 방식이 아니라 정보의 남용만을 규제하는 방식으로 규제모델을 바꿔야 한다'는 의견서를 제출하면서 그러한 방식으로 디렉티브를 개정할 것을 요청한 바 있다. Swedish Ministry of Justice, November 26, 2001, "Note in Preparation for the Internal Market Council Meeting on Directive 95/46/EC".

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

77) Executive Office of the President, 2016.5 ; 이원태, "EU 알고리즘 규제 이슈와 정책적 시사점", 정보통신정책연구원, 2016, 6-7면.

잘 억제되어왔던 기존의 차별과는 다른 새로운 차별을 만들어 낼 수 있음"을 시사한 것 역시 이러한 제도 도입의 맥락과 동일하다고 볼 수 있다.

Ⅳ. 결론

기술변혁과 산업발달에 있어서 글로벌 환경에 상응하는 변혁을 꾀하지 못하였을 경우 국가가 얼마나 어려운 상황에 놓이게 되는지 우리는 힘든 역사적 경험을 통해 잘 알고 있다. 또한 혁신적 기술과 서비스로 이끄는 산업적 변혁을 선도하였을 때 그에 상응하는 보상과 결과가 국가에 얼마나 긍정적으로 작동하는지 역시 우리는 경험을 통해 알고 있다.

4차산업혁명을 이끄는 기술과 서비스의 핵심 재료가 '데이터'라는 것을 누구도 부인하지 못하며, 우리나라는 4차산업혁명이라는 글로벌 환경에 상응하는 변혁을 꾀하여야만 하는 상황이다.

본 연구는 데이터를 기반으로 하는 경제에서 전세계적으로 시장지배적 사업을 보유하고 있는 미국의 데이터 규제에 대하여 검토하였다. 특히 '데이터 브로커 산업'이라는 고유한 산업영역에 대한 규범을 중심으로 검토하였다. 이미 검토한 바와 같이 미국 내에서도 '데이터 브로커 산업'의 폐해를 인지하고 이를 규율하기 위한 입법을 지속적으로 시도하나 현실화 되는 것은 쉽지 않아 보인다. 이미 형성된 데이터 브로커 산업에 작용하게 될 부정적 효과에 대한 부담과, 기술과 서비스 혁신을 선도해야 한다는 부담이 함께 작동한 것이라고 보인다.

우리나라의 경우 ICT 영역에서 혁신적 기술과 서비스는 어느 선진국에 에 비해 뒤지지 않으나 엄격한 '사전동의' 기반의 데이터 규범은 이러한 기술과 서비스의 진보에 상당부분 상충되는 것은 주지한 바이다. 규범의 설계방향이 국익에 부합해야 한다는 당연한 명제를 기반으로 데이터 규범의 변화방향에 대한 근본적 논의를 신속히 추진해야 할 필요가 있다. 그 하나의 방향성으로 본 연구에서는 '수집의 정당성'에서 '처리의 공정성'으로 개인정보 규율체계의 변화방향을 제안하였다.

[참고문헌]

<국내문헌>

[단행본]

김민호, 「행정법」, 박영사, 2018. 2.

김성수, 「개별행정법」, 법문사, 2004.

이원우, 「경제규제법론」, 홍문사, 2010.

[논문]

김민호・김일환, 민간영역에서 개인정보의 처리와 이용에 관한 비교법적 고찰, 토지공법연구 46권, 2009.

김민호, 공공부문 개인정보보호법제의 현황과 과제, 토지공법연구 제37집 제1호 2007년 8월.

Nadezhda P. 김미리/권헌영 공역, 빅테이터 변화 이후에도 개인정보의 재산권적 성격은 타당한가?, 경제규제와 법, 제10권 제2호(통권 제20호), 2017.

김현경, 개인정보의 개념에 대한 논의와 법적 과제, 미국헌법연구 第25卷 第2號, 2014년.

김현경, 데이터 속성과 국지화 규범의 법적 쟁점에 대한 고찰, 토지공법연구 78권, 2017.

이일호, 김기홍, 빅데이터는 누구의 소유인가?: 빅데이터의 저작권법에 의한 보호와 공공부문의 빅데이터 활용 문제, 「한국지역정보화학회지」 제19권 제4호, 2016.

이원태, EU 알고리즘 규제 이슈와 정책적 시사점, 정보통신정책연구원, 2016.

정용찬, 빅데이터산업과 데이터 브로커, 프리미엄 리포트 15-04, 정보통신정책연구원, 2015.8.

행정안전부, 개인정보 보호법령 및 지침 고시 해설, 2011.

<외국문헌>

Adam Liptak, Criminal Records Erased by Courts Live to Tell Tales, N.Y. TIMES, Oct. 17, 2006.

A. Vanberg and M. Ünver, The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?, European Journal of Law and Technology Vol 8, No 1, 2017.

Brian Krebs, Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records, KrebsOnSecurity, Mar. 10, 2014.

David S. Ardia, Reputations in a Networked World: Revisiting the Social Foundations of Defamation Law, 45 HARV. C.R.-C.L. L. REV. 261, 310, 2010.

Elizabeth D. De Armond, Frothy Chaos: Modern Data Warehousing and Old-Fashioned Defamation, 41 VAL. U. L. REV. 1061, 1075 – .96, 2007.

Federal Trade Commission, "Data Brokers: A Call for Transparency and Accountability." 2014.

FTC, Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003, Dec. 2012.

James Jacobs and Tamara Crepet, The Expanding Scope, Use, and Availability of Criminal Records, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 204 – 05. 2007.

Jacobs & Crepet, The Expanding Scope, Use, and Availability of Criminal Records, 11 N.Y.U. J. LEGIS. & PUB. POL'Y 177, 2007.

John Leyden, Acxiom Database Hacker Jailed for 8 Years, The Register, Feb. 23, 2006.

Jon Geffen & Stefanie Letze, Chained to the Past: An Overview of Criminal Expungement Law in Minnesota – State v. Schultz, 31 WM. MITCHELL L. REV. 1331, 1335, 2005.

Logan Danielle Wayne, The Data-Broker Threat: Proposing Federal Legislation to Protect Post-Expungement Privacy, 102 J. Crim. L. & Criminology 253, 2013.

Office of the Attorney General Department of Financial Regulation, Report to the General Assembly of the Data Broker Working Group issued pursuant to Act 66 of 2017, December 15, 2017.

Rebecca Oyama, Note, Do Not (Re)Enter: The Rise of Criminal Background Tenant Screening as a Violation of the Fair Housing Act, 15 MICH. J. RACE & L.

Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193, 1890.

SEARCH REPORT, SEARCH, NAT'L CONSORTIUM FOR JUSTICE INFO. & STATISTICS, REPORT OF THE NATIONAL TASK FORCE ON THE COMMERCIAL SALE OF CRIMINAL JUSTICE RECORD INFORMATION 82 – 83, 2005.

United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, June 30, 2014.

World Privacy Forum, Testimony of Pam Dixon Executive Director, World Privacy Forum, Before the Senate Committee on Commerce, Science, and Transportation: What Information do Data Brokers Have on Consumers, and How Do They Use It?, Dec. 18, 2013.

<ABSTRACT>

Study on the Domestic Legal Implications of US Data Broker System

Kim, Hyun-Kyung

The processing of data (including personal information) based on big data and artificial intelligence, such as corporate recruiting and forecasting of criminals in the country, is complicated by mathematical formulas, making it difficult for the public to understand. The opacity of this process makes it difficult for an personal information subject to object to the processing results of personal information. In the United States, this phenomenon has already become commercially available through 'data brokers' before technologies such as artificial intelligence or Big Data are introduced. The data broker industry in the United States has already held integrated personal information as an asset prior to the adoption of the Personal Information Legislation Act. Recently, the advancement of data analysis technology based on Big Data and Artificial Intelligence has increased their use of personal information. This study examines the status of data brokers in the United States and the disciplinary law, and draws implications for the direction of personal information discipline in Korea. First of all, the data broker in the United States is a personal information processor under our law. However, our law requires clear consent beforehand from the information subject for the processing of personal information in the private sector. In the meantime, US data brokers have collected and accumulated personal information for almost 100 years without the prior consent of the subject, and as such, it is virtually impossible for a domestic personal information processor to conduct a data broker business such as the United States. The United States is currently pushing legislation to regulate data brokers. However, in the case of the Vermont State Act, which is the first regulatory law, it is necessary to provide a certain obligation in the process of personal data processing of data brokers, rather than the regulation based on the consent of the information subject. Several legislative proposals have been proposed to regulate data brokers at the federal level, but no legislation has been passed so far. Perhaps it is not easy to implement such a bill because of the burden on the already established data broker industry and the importance of data utilization in the technological transformation of the fourth industrial revolution.

Given the fact that all the core technologies and services required to achieve the Fourth Industrial Revolution are data-based, it is also difficult to enforce data norms within the physical “border” due to the nature of the data (non-exclusivity / non-dominance) It is necessary to seek a fundamental change in the direction of discipline on collective data. Even without mentioning US data brokers, certain companies in the telecommunications, finance, and healthcare sectors are already collecting personal information from almost everyone. In this situation, 'collecting' - based discipline system is inevitably vulnerable to the privacy of information subjects. Therefore, it is necessary to establish systems for guaranteeing fair-

ness in the processing process after collection of personal information, such as introduction of supervision to ensure fair treatment in the use and provision of personal information. We should prevent disadvantages to the subject of information due to the processing of biased data and supervise the processing of personal information for unfair discrimination and unequal treatment. In addition, it is more realistic to guarantee the rights of information subjects to ensure fair contracts related to personal information processing through examination of strict terms rather than strict prior agreement.

Keywords : 데이터 브로커(data broker), 미국 데이터 브로커 규제법(regulation on data broker industry in U.S), 개인정보(personal information), 데이터베이스(database), 정보주체의 권리(the right of data subject)