http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.25, No.4, November 2020, pp.1-14
https://doi.org/10.7838/jsebs.2020.25.4.001

개인정보 관련 국내기업의 역차별 상황에 관한 규제 분석과 개선방안에 관한 연구

A Regulatory Analysis on the Reverse Discrimination against Korean Domestic Businesses in relation to the Data Protection and Regulatory Improvement Orientation

이인호(Inho Lee)*, 김서안(Seo-An Kim)**

초 록

국내의 IT기업들은 개인정보보호에 관한 국내법의 규제와 집행이 엄격히 적용되는 반면, 해외 기업들에게는 여러 이유로 법의 적용과 집행이 동등하게 이루어지지 못하는 상황이다. 이에 따라 국내기업들은 해외기업에 비해 경쟁력이 약하여 규제의 역차별 상황에 놓여 있다. 이에 본 글에서는 개인정보보호법제상 규제항목을 5가지로 유형화하고 분석하였다. 또한 국내에 서비스를 제공하는 대표적 사이트(네이버(Naver), 다음(Daum), 구글(Google), 페이스북(Facebook))이 제시하는 개인정보처리방침(privacy policy)을 비교분석하고, 위의 규제항목별로 의무사항에 부합하는지 검토한다. 그리고 역차별 해소를 위한 종합적 법제 개선 방안을 3가지 측면으로 제안한다.

ABSTRACT

IT businesses in Korea have relatively strong regulations. While providing the same service, domestic businesses are in a situation of 'reverse discrimination of regulations' as they are less competitive than global IT companies in accordance with the application of the personal information protection legislation in Korea. In this paper, Personal Information Protection legislation was classified and laws of major countries were analyzed in comparative ways. It also compared and analyzed the "private policy" presented by representative Internet sites (Naver, Daum, Google, Facebook) that provide services to users in Korea. We also proposed three aspects of legislation improvement to address reverse discrimination.

키워드 : 규제의 역차별, 개인정보보호법제, 일반개인정보보호규칙, 개인정보처리방침, 개인정보보호법제의 개선 방안
Reverse Discrimination of Regulations, Personal Information Protection Legislation, General Data Protection Regulation, Privacy Policy, Comprehensive Improvement of the Personal Information Protection Legislation

---

본고는 개인정보보호위원회에서 2018년 발주하여 저자가 참여한 "개인정보 관련 국내기업의 역차별에 관한 실태조사"보고서의 일부를 논문형식으로 재구성한 것이며, 2017년도 중앙대학교 CAU GRS 지원에 의하여 작성되었습니다.

* First Author, Professor, School of Law, Chung-Ang University(inho61@cau.ac.kr)
** Corresponding Author, Ph.D. Candidate, Department of Law, Graduate School of Chung-Ang University (vizlady@cau.ac.kr)

Received: 2020-06-01, Review completed: 2020-09-16, Accepted: 2020-10-14

1. 서 론

구글, 애플 등의 해외 IT기업이 국내 앱 시장에서 차지하는 점유율이 2017년 87.7%(7조 5061억 원), 2018년 기준 87.8%(8조 3082억 원)를 기록했고, 2020년 매출액 전망치도 88.1%(93,865억 원)를 차지할 것으로 예상된다. 이들의 점유율은 90%에 가까워 독과점 상황을 보이는 데 반하여 국내 기업들의 점유율은 점점 줄어들고 있다[20]. 이러한 상황의 원인 중 하나로 지적되는 것이 국내 개인정보보호법제상의 각종 규제가 국내의 인터넷사업자에게는 엄격하게 집행되는데 반하여 해외기업에게는 규제가 어렵다는 것이다[11].

포털, SNS, 게임, 쇼핑, 의료, 헬스케어, 핀테크, 온라인광고, 사물인터넷 등의 다양한 서비스 영역에서 국내의 인터넷기업들은 글로벌 인터넷기업과 치열하게 경쟁하고 있으나, 개인정보보호법, 정보통신망법, 위치정보보호법, 신용정보보호법 등 개인정보보호에 관한 국내법의 규제가 상대적으로 강하여 국내의 기업들이 어려움을 겪고 있다[24]. 국내의 인터넷 기업들에게는 강력한 규제와 집행이 이루어지는 반면, 국내에서 동일한 서비스를 제공하는 해외 기업들에게는 여러 이유로 법의 적용과 집행이 동등하게 이루어지지 못하고 있다[11]. 이로 인해 동일한 서비스를 제공하면서도 개인정보의 수집・이용 및 제공, 처리 등에 대해 국내 개인정보보호법제가 적용되어 해외기업에 비해 경쟁력이 약한 입장에 놓여 있다. 이른바 '규제의 역차별' 문제가 발생하고 있는 것이다.

이에 본 연구에서는 우선 개인정보보호법제상 역차별을 야기하는 규제항목을 분석하기 위하여 주요한 규제항목을 5가지로 유형화하였다(제 2장). 즉 규제항목을 사전 동의의 원칙, 개별적 및 선택적 동의 방식, 개인데이터의 파기 또는 삭제, 안전성 확보 조치 의무, 정보주체의 개인정보자기결정권으로 나누고 이에 대하여 비교법적 분석을 하였다. 제 3장에서는 주요 국내・외의 인터넷사업자(네이버(Naver), 다음(Daum), 구글(Google), 페이스북(Facebook))들이 시행하는 개인정보처리방침(Privacy Policy)이 2장에서 분석한 규제항목 중 5가지(사전 동의의 원칙, 개별적 및 선택적 동의방식, 개인데이터의 파기 또는 삭제, 안전성 확보조치의무, 개인정보자기결정권)를 준수하고 있는지에 대하여 조사하였다. 마지막으로 제 4장에서는 이상의 분석을 바탕으로 역차별 해소를 위한 종합적 법제개선방향을 3가지 측면(①보호규제 수준의 글로벌 표준화 ②보호법제의 역외적용 및 집행력 강화 ③국내・외 협력체계의 구축)으로 제안하고자 한다.

2. 개인정보보호법제상 규제항목의 유형화 및 비교법적 분석

국내・외 기업들이 국내 개인정보보호법제상의 규제를 준수하고 있는지 검토하기 위하여 규제항목 중 주요한 5가지 항목(사전 동의의 원칙, 개별적 및 선택적 동의방식, 개인데이터의 파기 또는 삭제, 안전성 확보조치 의무, 정보주체의 개인정보자기결정권)에 대하여 그 내용을 분석하고, 유럽연합과 일본에서는 같은 항목에 대하여 어떻게 규율하고 있는지 비교법적 분석을 하고자 한다.

2.1 사전 동의의 원칙

한국의 개인정보보호법제에서는 개인정보처리자(기업 등)가 개인데이터를 수집・이용하거나 제공할 때 정보주체로부터 사전에 동의를 받아야만 합법적인 것으로 인정하는 '사전동의의 원칙'을 채택하고 있다. 물론 일부 예외가 인정되지만 제한적이다. 이는 추론된 정보 등에 대해서도 마찬가지이며 정보의 유용을 위하여 개별 형량의 여지가 필요하다는 지적이 있다[22].

유럽연합의 「일반개인정보보호규칙」(General Data Protection Regulation; 이하 'GDPR') 제6조제1항에서는 개인데이터를 수집・이용・제공 시에 6가지의 합법적 처리 요건을 규정하는데 그 요건에서 동의뿐만 아니라 계약체결・이행, 법적인 의무의 이행, 정보주체 또는 제3자의 중대한 이익보호, 공적인 업무처리 또는 공적 권한 행사, 개인정보처리자 또는 제3자의 정당이익의 달성의 경우도 인정하고 있다.

또한 일본에서는 (민감정보를 제외한) 일반개인데이터를 수집할 때 이용목적만 분명히 특정하면 정보주체의 동의 없이 수집・이용이 가능하고(일본 개인정보보호법 제15조), 제3자 제공에 있어서도 소위 'opt-out 방식(사후적 처리거부)'을 채택하여 제3자 제공의 합법성을 넓게 인정하고 있다(일본 개인정보보호법 제23조).

2.2 개별적 및 선택적 동의

한국의 개인정보보호법제에서는 개인정보처리자(기업 등)가 정보주체로부터 사전 동의를 받을 때, 수집・이용 및 제공에 대한 포괄적인 동의를 하는 것을 금지하고, 동의가 필요한 사항에 대하여 개별적 혹은 선택적 동의를 하는 방식을 취한다(개인정보보호법 제15조제2항, 제17조제1항 내지 제3항 등).

반면에 일본의 개인정보보호법은 한국과 같은 개별적 및 선택적 동의방식을 채택하고 있지 않고 수집할 때 이용의 목적만 분명히 특정하면 동의 없이 수집할 수 있고(일본 개인정보보호법 제15조제1항), 처음 안내한 이용목적과 연관성이 있다고 합리적으로 인정되는 범위 안에서 목적을 변경할 수 있다(일본 개인정보보호법 제15조제2항). 해당 이용 목적을 벗어난 이용은 원칙적으로 동의를 받아야 하지만 4가지의 예외사유를 인정한다(일본 개인정보보호법 16조제1항). 민감데이터('배려를 요하는 개인정보')를 취득할 때도 동의를 받아야 하지만 6가지 예외 사유를 인정하며(일본 개인정보보호법 제17조제2항), (민감데이터가 아닌 일반개인데이터의) 제3자 제공은 사후적 처리거부(opt-out) 방식에 의해 동의 없이 가능하지만, 사전 동의(opt-in)를 받으면 합법적인 처리로서 가능하도록 규정하고 있다.

유럽 GDPR에서는 (민감데이터가 아닌) 일반개인데이터를 수집할 시점에 이용 및 제공에 대한 포괄동의를 받을 수 있고(GDPR 제6조제1항(a)), 민감데이터(특수유형의 개인데이터)를 수집할 시점에 이용 및 제공에 대한 명시적 동의를 포괄적으로 받을 수 있다(GDPR 제9조제2항(a)). 온라인특별법인 「e-Privacy Directive (이-프라이버시 지침)」는 쿠키(cookie)를 단말기에 저장할 때 동의를 받아야 하며(e-Privacy Directive 제5조제3항), 위치데이터(location data)는 익명처리하거나 동의를 받아서 처리해야 한다(e-Privacy Directive 제9조제1항)고 규정하고 있다.

2.3 개인데이터의 파기 또는 삭제

한국의 개인정보보호법(제21조), 위치정보법(제23조)은 개인데이터의 보유기간이 종료하거나 처리의 목적을 달성한 경우에, 그 개인데이터를 지체 없이 파기하도록 규정하고 있다. 개인정보보호법(제37조제4항)은 정보주체의 처리정지의 요구에 따라 처리를 정지한 경우, 그 처리가 정지된 개인정보를 지체 없이 파기하는 등의 조치를 취하도록 하고 있다. 위치정보법(제24조)은 정보주체가 동의를 철회하면 수집된 개인정보를 지체 없이 파기하는 등 필요한 조치를 하도록 규정하고 있다. 또한 위치정보사업 또는 위치기반서비스사업을 휴업하거나 폐업하는 경우 개인위치정보를 휴업 또는 폐업과 동시에 파기하도록 규정한다(위치정보법 제8조 및 제11조).

유럽연합의 GDPR은 처리의 목적을 달성한 경우에도 반드시 삭제나 파기를 요구하지 않고 대신에 비식별의 형태로 보관할 것을 요구하며, 자료보존·연구·통계 목적의 경우에는 보유기간을 넘겨 보관할 수 있도록 허용한다(GDPR 제5조제1항(e)). 한편, 일본은 이용의 목적을 달성한 경우 지체 없이 파기할 노력의무만을 부과할 뿐 제재를 가하지 않는다(일본개인정보보호법 제19조).

2.4 안전성 확보조치 의무

한국의 개인정보보호법제는 개인정보의 안전성을 확보하기 위한 관리적, 기술적 조치의무를 규정하고 있다. 법률과 시행령은 조치의무사항만을 정하고 그 세부기준은 고시와 해설서에서 정하고 있다. 그리고 이 기준을 위반한 경우 형사처벌의 대상이 되기도 한다. 개인정보보호법은 관리적, 기술적 조치의무를 위반하여 개인데이터를 분실, 도난, 유출, 위조, 변조, 훼손당한 경우에 2년 이하의 징역 또는 2천만 원 이하의 벌금과 5천만 원 이하의 과태료를 부과하고 있다(개인정보보호법 제73조, 제75조). 특히 위치정보법은 관리적, 기술적 조치의무를 위반했다는 것만으로 1년 이하의 징역에 처하고 있다(위치정보법 제16조).

유럽연합의 GDPR은 안전조치의무 위반에 대해 과징금만을 부과하고 있으며(GDPR 제32조, 제83조제4항) 일본의 개인정보보호법은 안전조치의무 위반의 경우 우선 시정권고한 후, 이에 불이행하면 시정명령을 내리고, 시정명령을 불이행하면 형사처벌(6월 징역)을 하는 순서로 소위 '순차적 집행방식'을 채택하고 있다(일본 개인정보보호법 제20조).

2.5 정보주체의 개인정보자기결정권

한국의 개인정보보호법제는 정보주체에게 여러 개인정보자기결정권(열람청구권, 정정청구권, 삭제청구권, 처리정지청구권)을 인정하고 있다. 그러나 행사요건과 예외규정이 거의 없어 마치 절대적인 개인정보자기결정권 또는 개인정보통제권을 부여하고 있는 것으로 평가된다(개인정보보호법 제35조제1항, 위치정보법 제24조제3항 등). 유럽연합의 GDPR 제16조(정정청구권), 제17조(삭제청구권), 제18조(처리정지청구권) 등이나 일본의 개인정보보호법은 권리의 행사요건과 예외를 규정하고 있어 정보주체의 권리 행사에 일정한 제한을 가하고 있다. 개인정보자기결정권의 행사는 정보처리자 혹은 사업자의 이익의 측면을 고려해야 하는 것이

균형의 관점에서 볼 때 바람직하다고 보며, 이에 따라 우리나라의 개인정보자기결정권의 행사에도 요건과 예외사항을 규정하여 합리적이고 실질적으로 운영해야 한다.

3. 국내・외 기업의 「개인정보처리방침」 비교 분석

3장에서는 2장에서 분석한 규제항목을 기준으로 국내・외 기업들이 국내의 개인정보보호법제를 준수하고 있는지를 파악하기 위하여 국내・외의 주요 사이트인 네이버(Naver), 다음(Daum), 구글(Google), 페이스북(Facebook)의 개인정보처리방침을 분석하였다.

3.1 사전 동의의 원칙

국내의 대표적 포털사이트인 네이버(Naver)와 다음(Daum)은 개인정보의 수집과 이용에 관하여 명확하게 구분하여 정보주체에게 알리고 있고 이에 대하여 사전 동의를 받고 있었다. 반면 구글(Google)의 경우 “이메일, 유튜브 동영상에 다는 댓글, 사진 등 사생활에 속하는 개인적인 정보를 수집한다.”고 규정하고 있는데, 이는 수집하는 정보의 종류를 확정하여 수집하고 있는 국내 사업자와 비교하여 광범위한 데이터를 수집하고 있어 차별적 상황이 우려된다. 페이스북(Facebook)도 “정보주체 및 다른 사람들의 활동 및 제공하는 정보를 수집하고 있고 콘텐츠의 작성, 공유, 타인과의 메시지 전송 또는 커뮤니케이션 포함하여 수집한다.”고 설명하고 있다. 더욱이 구글(Google)의 경우에는 “‘상황에 따라’ 구글(Google)은 공개적으로 액세스할 수 있는 소스에서 사용자에 대한 정보를 수집을 한다.”고 하여 정보주체의 입장에서는 어떤 상황에서 어떤 정보를 수집하는지 명확하게 알 수 없다. 페이스북(Facebook)의 경우에도 “사진이 촬영된 장소나 파일이 생성된 날짜와 같이 회원님이 제공한 콘텐츠에 포함되거나 관련된 정보(메타데이터 등)가 포함될 수 있다.”고 하여 다소 모호하게 설명하고 있다. 이렇게 수집된 정보를 통해 페이스북은 사용주체에 대하여 수많은 정보를 보유하고 있다[6]. 개인정보보호법 제3조 제1항에서는 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다는 개인정보보호원칙을 규정하고 있고, 동법 제16조 제1항 내지 제2항에서는 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다고 규정하고 있다. 또한 정보주체에게 최소한의 정보 외에 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집해야 하고, 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니한다고 규정하고 있다. 구글(Google)과 페이스북(Facebook)의 경우에는 광범위한 정보를 수집하고 있고 이를 명확하게 구분하지 않은 상태로 동의를 받고 있다고 평가된다. 비용의 절감을 위해서는 데이터의 보관을 축소시키는 것이 기업의 측면에서는 유리하겠지만, 글로벌 IT기업들의 경우에는 막강한 자본력을 이용하여 정보 수집과 보관의 능력을 보유하고

있고 이에 따라 데이터 활용 산업도 계속 발전시키고 있다[3, 25]. 한정된 정보만을 수집하고 있는 국내기업이 불리한 상황으로 차별이 발생할 우려가 있고 글로벌 IT기업과의 경쟁에서 뒤처질 우려가 있다. 이러한 상황에서 기업들도 데이터를 다양하게 수집하여 활용할 수 있도록 제도 개선을 요구하고 있는 상황이다[10].

3.2 개별적 및 선택적 동의

개별적 및 선택적 동의 사항에 대한 준수여부에 관하여 각 기업들의 개인정보처리방침을 살펴보면, 네이버(Naver)의 경우 “추가로 개인정보를 수집할 경우에는 해당 개인정보 수집 시점에서 이용자에게 ‘수집하는 개인정보 항목, 개인정보의 수집 및 이용목적, 개인정보의 보관기간’에 대해 안내 드리고 동의를 받는다.”고 하고, 다음(Daum)의 경우에도 “이용자의 개인정보를 다음과 같은 목적으로만 이용하며, 목적이 변경될 경우에는 반드시 사전에 이용자에게 동의를 구하도록 하겠습니다.”라고 하여 국내법을 잘 준수하고 있다. 반면 구글(Google)과 페이스북(Facebook)은 이에 대한 선택적 동의 사항을 구분하고 있지 않다. 구글(Google)은 “비즈니스 파트너 등에게서 사용자에 대한 정보를 수집할 수 있고 광고 및 리서치 서비스를 제공하기 위하여 광고주로부터 정보를 받기도 한다.” 라고 설명하고, 페이스북(Facebook)은 “당사는 또한 당사 파트너들이 당사에서 제공한 데이터를 이용하고 공개하는 방법에 엄격한 제한을 가하고 있습니다. 당사가 정보를 공유하는 제3자의 유형은 다음과 같습니다.” 라고 하여 제3자 정보제공의 경우 별도의 동의가 필요함에도 이에 대한 절차를 거치지 않고 정보를 공유하고 있어 국내 기업이 개인 정보의 활용에 불리한 상황에 있다. 이러한 상황에서 정보주체는 자신의 정보가 어떻게 활용되는지 알 수 있어야 하고 마케팅을 위해 자신의 정보가 광고주에게 제공이 되는 경우에는 그때마다 이용자의 동의를 구해야 할 필요가 있다[26]. 자신의 정보가 마케팅에 활용이 되면 이용자들은 맞춤 서비스를 받을 수 있어 편리한 측면도 있지만, 자신의 프라이버시 침해의 가능성이 있기 때문이다[2, 21]. 유럽연합의 GDPR의 경우에도 민감 데이터가 아닌 일반개인데이터를 수집할 시점에 이용 및 제공에 대한 포괄 동의를 받을 수 있지만 민감 데이터, 쿠키, 위치데이터는 별도의 동의를 요하고 있어 구글(Google)과 페이스북(Facebook)의 정책은 GDPR 규정에도 반할 소지가 있고 국내기업과 비교하여 볼 때 차별적 상황이 있어 국내기업이 역차별을 받고 있다고 볼 수 있다.

3.3 개인데이터의 파기 또는 삭제

국내 사업자의 경우에는 개인정보의 파기와 관련된 부분에도 법령을 준수하고 있다. 네이버(Naver)는 “회사는 원칙적으로 이용자의 개인정보를 회원 탈퇴 시 지체 없이 파기하고 있습니다. 단, 이용자에게 개인정보 보관기간에 대해 별도의 동의를 얻은 경우, 또는 법령에서 일정 기간 정보보관 의무를 부과하는 경우에는 해당 기간 동안 개인정보를 안전하게 보관합니다.” 라고 하며, 다음(Daum)의 경우에도 “이용자의 개인정보에 대해 개인정보의 수집・이용목적이 달성된 후에는 해당 정보를 지체 없이 파기합니다.” 라고 하여 법령에 의하여 별도 보관하는 경우 또한 자세히 규정하고 있다.

반면, 구글(Google)과 페이스북(Facebook)은 정보의 파기라는 측면보다는 사용자에게 삭제 청구권을 주고 있다는 측면에서 설명하고 있다. 구글(Google)의 경우 “사용자는 언제든지 구글(Google) 계정에서 자신의 정보에 대한 사본을 내보내거나 삭제할 수 있습니다. 사용자는 백업하거나 구글(Google) 외부 서비스에서 사용하기 위해 구글(Google) 계정의 콘텐츠 사본을 내보내기할 수 있습니다.”라고 하며, 페이스북(Facebook)의 경우에는 “저희는 데이터 액세스, 수정, 복사 및 삭제 기능을 제공합니다.”라고 설명하고 있다. 따라서 정보의 파기에 대하여 개인정보처리자에게 적극적으로 파기 의무를 부여받는 국내 사업자가 불리한 면이 있다. 글로벌 기업들의 경우 콘텐츠(contents)의 삭제명령에 대해 따를지에 대해 상당한 재량을 행사하고 있기도 하다[5]. GDPR의 경우에는 파기를 원칙으로 하지 않고 비식별 형태로 보관을 허용하고 있다. 개인정보의 파기와 관련한 우리나라의 법은 GDPR과 일본의 관련법과 비교할 때 과도한 규제를 가하고 있고 형사처벌까지 부과하고 있어 사업자의 부담이 크다. 유럽연합의 GDPR의 경우 파기를 원칙으로 하지 않고 비식별 형태로 보관하는 것을 허용하고 있고 한국처럼 일방적인 파기의무를 부과하는 것이 아니라 삭제청구권을 제한적으로 행사하도록 하고 있고, 일본의 개인정보보호법에서는 소거 노력의 의무를 부과할 뿐, 제재를 가하지 않고 있다. 이처럼 우리나라도 유럽이나 일본의 수준으로 개정을 하여 국내 사업자가 받는 차별적 상황을 줄이는 것이 바람직하다.

3.4 안전성 확보조치 의무

네이버(Naver)와 다음(Daum)의 경우 개인정보를 암호화 하고, 전담조직을 운영, 인증을 취득하는 등의 다양한 방식을 통하여 안정성을 확보하기 위한 조치를 하고 있고, 구글(Google)과 페이스북(Facebook)의 경우에도 암호화를 사용하고 2단계 인증을 사용하는 등의 방법으로 안정성을 확보하는 조치를 취하는 것으로 보인다. 안전성 확보조치의무는 네 기업 모두 잘 준수하고 있는 것으로 평가된다. 안전성 확보조치에 관한 국내법과 시행령은 조치의무사항만을 정하고 그 세부기준은 고시와 해설서에서 정하고 있다. 그런데 이 의무를 준수하지 않은 경우 형사 처벌의 대상으로 삼고 있는데 형사 처벌의 경우 그 요건이 법률에 명확하게 규정이 필요하기 때문에 그 안전성 확보조치의 세부기준도 법률로 규정하는 것이 바람직하다.

3.5 정보주체의 개인정보자기결정권

정보주체의 개인정보자기결정권에 관하여는 국내・외 사업자 모두 잘 준수하고 있는 것으로 보인다. 네이버(Naver)의 경우 언제든지 자신의 정보를 조회하거나 수정이 가능하고 수집 및 이용 동의 철회가 가능하며 정정청구를 할 수 있고, 다음(Daum)의 경우에도 개인 정보의 조회와 수정이 언제든지 가능하며 정보제공 동의에 대한 철회권과 회원가입해지 요청 등을 자유로이 할 수 있다. 구글(Google)의 경우에도 정보주체가 스스로 자신의 정보를 관리하고 검토할 수 있고 업데이트가 가능하며 정보의 제거와 삭제가 가능하며, 페이스북(Facebook)도 데이터 액세스와 수정, 복사 및 삭제권을 부여하고 있다.

〈Table 1〉 Compliance with Domestic Privacy Laws of Private Policy

	Naver	Daum	Google	Face book
Principle of Prior Consent	O	O	△	△
Individual and Selective Agreements	O	O	△	△
Exporting or Deleting Personal Information	O	O	△	△
Duty of Action to Secure Safety	O	O	O	O
The Right to Control Personal Information of Data Subject	O	O	O	O

3.6 소결

Jang[9]의 연구에 따르면 인터넷 이용자 중 개인정보처리방침 공개를 인지하고 있는 이용자는 70.9%이고, 지침을 확인하는 이용자는 29.1%라고 한다. 개인정보처리방침의 내용이 너무 많고 다소 복잡한 내용이 이용자들이 쉽게 이해하기 어렵다는 것이다[9]. 그럼에도 불구하고 국내의 대표적인 인터넷 기업인 네이버(Naver)와 다음(Daum)의 개인정보처리방침은 국내법을 준수하고 있고 사용하는 용어와 표현도 법에서 요구하는 수준으로 잘 설명되어 있다. 반면 구글(Google)과 페이스북(Facebook)의 경우에는 이용자의 “이메일, 댓글과 같은 개인적인 정보를 수집한다.”고 한다거나 “이용자가 제공하거나 관련된 정보(메타데이터)를 포함될 수 있다.”는 표현을 사용하여 이용자가 어느 범위까지 자신의 정보가 수집되고 이용되는지 파악하기가 어렵다. 또한 이 방침들의 위법 여부를 판단하기도 쉽지 않다는 문제점이 있다[27]. 국내의 엄격한 개인정보보호법제에 의하여 국내 기업은 강하게 규제를 받고 있고 해외 기업은 규제를 피하고 있는 현재의 상황을 개인정보처리방침에서도 잘 살펴볼 수 있다.

4. 역차별 해소를 위한 종합적 법제개선방향

4.1 법제 개선의 필요성(규제의 역설(逆說)과 역차별)

한국에서 규제의 역차별로 인한 국내 인터넷 사업자의 경쟁력 약화 현상이 어디에 기인하는지는 우리나라 인터넷 규제의 역사를 조금만 거슬러 올라가보면 알 수 있다.

2007년에 도입된 ‘인터넷게시판 본인확인제’, 2009년에 시행된 ‘저작권 삼진아웃제’ 등의 규제로 인해, 국내 동영상 사이트운영자들은 실시간 모니터링 등 의무이행을 위한 막대한 인력과 비용을 떠안아야 했고, 그와 동시에 이들 제도에 불편을 느낀 인터넷 이용자들은 피난처를 찾아 유튜브(YouTube)로 대거 이동하였다. 유튜브는 회원 가입 시 국가 항목을 자유롭게 선택할 수 있게 하여 규제를 우회하였던 것이다. 이러한 규제로 인하여 2008년에 2%의 점유율을 갖고 있던 유튜브(YouTube)는 2013년에 점유율 74%를 기록한 반면, 반면에 당시 국내 1위였던 판도라TV의 점유율은 42%에서 4%로 떨어졌으며, 2위였던 다음TV팟은 34%에서 8%로 내려갔다. 역설적이게도, 정부의 ‘무리한 규제’가 규제의 역차별을 불러오고 결국 국내 인터넷기업의 경쟁력을 약화시키는 주요 원인이 되었던 것이다.

이런 '규제의 역설(逆說)'은 헌법재판소가 2012년에 인터넷게시판 본인확인제에 대해 마침내 위헌결정을 내리면서 그 위헌의 논거로 제시된 바 있다(헌재 2012. 8. 23. 2010헌마47). "이 사건 법령조항들의 경우, 우리 법상의 규제가 규범적으로 또는 현실적으로 적용되지 아니하는 통신망이 존재하고 그에 대한 인터넷 이용자의 자유로운 접근이 가능함에도 외국의 입법례에서 찾아보기 힘든 본인 확인제를 규정함으로써 국내 인터넷 이용자들의 해외 사이트로의 도피, 국내 사업자와 해외 사업자 사이의 차별 내지 자의적 법집행의 시비로 인한 집행 곤란의 문제를 발생시키고 있는바, 결과적으로 당초 목적과 같은 공익을 실질적으로 달성하고 있다고 보기 어렵다. 인터넷은 전 세계를 망라하는 거대한 컴퓨터 통신망의 집합체로서 개방성을 그 주요한 특징으로 하므로 외국의 보편적 규제와 동떨어진 우리 법상의 규제는 손쉽게 회피될 수 있고, 그 결과 우리 법상의 규제가 의도하는 공익의 달성은 단지 허울 좋은 명분에 그치게 될 수 있음을 간과한 것이다."(헌재 2012. 8. 23. 2010헌마47). 우리의 입법자들이 반드시 경청해야 할 경고(警告)가 아닐 수 없다.

위 규제의 역설을 낳은 과거의 아픈 교훈과 헌법재판소의 경고는 개인정보보호법제와 관련한 현재 국내 인터넷사업자들에게 가해지는 규제의 역차별 문제를 다룸에 있어서 그대로 타당하게 적용된다. 개인데이터를 보호한다는 명분으로 세계 유례(類例)가 없을 정도로 강력한 규제야말로 역설적으로 외국 인터넷사업자들의 경쟁력을 키워주고 국내 사업자들의 경쟁력을 억제시키는 주된 요인 중의 하나임을 분명히 인식할 필요가 있다.

통신기술의 발달에 따라 점점 더 많은 데이터가 수집되고 있고[3], 이 과정에서 정보보호, 보안, 프라이버시 등의 문제가 불가피하게 발생된다[4]. 특히 사이버공간 안에서는 익명의 커뮤니케이션이 발달하게 되고, 프라이버시 등의 문제가 필연적으로 생기게 된다[21]. 이에 관하여 최근의 한 연구에 의하면, 프라이버시 규제를 강화한다고 해서 소비자의 신뢰가 높아지고 디지털기술의 이용이 증가하는 것은 아니라고 한다[19]. 전통적으로 이렇게 이해해 왔지만, 그러나 규제와 신뢰의 관계는 선형적 비례관계(linear proportional relation)에 있지 않다는 것이다[19]. 프라이버시 보호를 위한 합리적 규제가 기본적인 수준(baseline level)까지는 소비자의 신뢰를 비례적으로 향상시키지만, 그러나 규제가 그 이상의 수준에 이르면 프라이버시 보호를 높인다고 해서 소비자의 신뢰가 추가적으로 높아지지 않는다는 것이다[19]. 즉, 프라이버시 규제와 소비자의 신뢰 사이의 관계는 계단식 함수관계(stepwise function)에 놓여 있다고 한다[19]. 나아가, 프라이버시 규제와 디지털기술의 이용 사이의 관계 또한 선형적 비례관계에 있다는 전통적 시각과는 달리, 실제로는 의도하지 않게 '뒤집힌 U 곡선'의 관계를 보인다는 것이다[19]. 왜냐하면, 기본적인 수준 이상의 추가적인 규제는 비용을 늘리고 수입을 줄여서 기업들이 새로운 상품과 서비스에 투자하지 않게 되어 디지털 기술의 공급을 억제하게 되고, 결국 소비자가 그 디지털기술을 향유하지 못하는 결과를 낳기 때문이다.

4.2 보호규제 수준의 글로벌 표준화

현행 한국의 개인정보보호를 위한 규제는 미국, 일본보다 훨씬 강하며 심지어 유럽연합의 GDPR보다 어떤 측면에서는 더 강하다[17, 18]. 개인정보 처리의 전 과정에 대해 규율하고 있고,

법 위반시 형벌 등을 부과하고 있기 때문이다[14]. 기본적으로 규제내용이 엄격하여 개인정보보호의 목표를 효과적이고 효율적으로 달성할 수 없도록 되어 있다. 정보주체의 권리에 강하게 주목한 것은 개인정보보호법의 목적조항에서도 확인할 수 있다[12].

한국의 현행 개인정보보호법제는 세계에서 가장 강력한 규제법제로 널리 알려져 있다. 외국의 평가를 몇 가지 소개 한다: ①"한국은 아시아에서 가장 강력한 데이터보호법(the strongest data privacy laws in Asia)을 가지고 있는데, 심지어 개인의 사진이나 목소리까지 보호대상에 포함시키고 있다. 2011년에 제정된 법은 엄격하게 집행되고 있다."[7]; ② "국제프라이버시전문가협회(International Association of Privacy Professionals)에 따르면, 한국은 세계에서 가장 엄격한 프라이버시보호법(the world's strictest privacy laws)을 가지고 있다."[23]; ③ "한국의 포괄적인 개인정보보호법은 2011년 9월 30일 제정되었다. 그 법은 세계에서 가장 엄격한 프라이버시 규제체계 중의 하나이다(one of the world's strictest privacy regimes)[1]."

김경환 변호사의 비교분석에 의하면, 유럽연합의 GDPR이 실체적 규제가 가장 낮고, 그 다음이 일본 개인정보보호법이며(GDPR의 1.4배), 그 다음이 한국의 개인정보보호법(GDPR의 2.6배), 그 다음으로 한국의 정보통신망법(GDPR의 3.4배)이 가장 높다고 한다[15].

규제의 내용 측면에서 공정한 개인정보처리의 기준과 의무를 글로벌 기준에 맞추어 보호와 이용의 균형을 확보할 수 있도록 정교하게 다듬는 작업이 필요하다[25]. 주(主)와 산업별로 규율하는 미국[7] 또는 기본법과 개별법으로 규율하는 일본의 보호수준이 약하다면, 유럽연합 GDPR이 제시하는 수준의 균형이라도 맞추어야 한다. 이에 대하여 GDPR의 과징금처럼 우리도 GDPR처럼 현실화할 필요가 있다는 의견도 있다[8].

4.3 보호법제의 역외적용 및 집행력 강화

유럽연합의 GDPR은 규칙의 적용범위를 역내의 모든 개인정보처리자와 수탁처리자의 데이터처리에 적용하도록 하면서, 외국기업이라도 역내에 사업체가 있어서 그 사업 활동과 관련한 개인데이터의 경우 그 처리를 설령 유럽연합의 역외에서 하더라도 본 규칙이 적용된다고 명시하고 있다: "본 규칙은 개인정보처리자 혹은 수탁처리자의 업무조직(또는 사업체)이 유럽연합 역내에 있는 경우 그 업무가 수행하는 업무활동과 관련해서 이루어지는 개인데이터의 처리에 적용된다. 그 데이터의 처리가 유럽연합 역내에서 이루어지든 혹은 역외에서 이루어지든 상관없다."

또한 제3조 제2항은 역외의 개인정보처리자나 수탁처리자가 역내 유럽시민의 개인데이터를 처리하는 두 가지 경우에 GDPR이 적용된다는 점을 분명히 하고 있다: "본 규칙은, 개인데이터의 처리가 다음의 어느 하나와 관련된 것일 때에는, 유럽연합 역내에 활동거점이 없는 개인정보처리자 혹은 수탁처리자라도 유럽연합 역내에 있는 정보주체의 개인데이터를 처리하는 경우에 적용된다. (a) 유럽연합 역내에 있는 정보주체에게, 비용지불을 요구하는지와 상관없이(유료이든 무료이든), 상품이나 서비스를 제공하는 때; 또는 (b) 그들 정보주체의 활동이 유럽연합 역내에서 이루어지고 있는 경우에, 그들의 활동을 모니터(추적관찰)하는 때."

우리도 유럽연합의 GDPR처럼 역외적용 관련 규정의 흠결을 보완하고, 나아가 해외의 인터넷사업자에 대한 법집행을 보다 강화할 수 있도록 법제를 정비해갈 필요가 있다. 2018. 9. 18. 개정된 정보통신망법상의 국내대리인 지정제도는 그 방안 중의 하나이다.

4.4 국내 · 외 협력체계의 구축

개인정보보호기관은 국내 · 외의 다른 보호기관들과 긴밀한 협력체계를 구축하여 개인정보보호의 집행력을 높여나가야 한다. 외국의 주권을 존중하면서 해외기업에 대한 집행력을 높이기 위해서는 외국과의 긴밀한 공조체계가 필수적이기 때문이다. 유럽연합의 GDPR도 국제협력의 중요성을 인정하여 구체적인 국제협력 추진사항을 규정하고 있다(제50조). 즉, 개인정보 보호 법률의 효과적인 집행을 위한 국제적인 협력 매커니즘의 개발, 적절한 안전조치를 위한 조사지원 등 국제적인 지원 제공, 국제협력 촉진을 위한 활동에 이해 당사자의 참여, 제3국과의 사법적인 분쟁 등에 개인정보 보호법 및 관행의 교류와 문서화 등을 규정하고 있다.

우리의 현행 개인정보보호법(제14조)은 국제협력을 위한 시책을 마련하도록 추상적으로 요구하고 있지만, 보다 구체적이고 적극적인 협력체계 구축이 요구된다. 더욱이 2020년 8월 개인정보보호위원회가 독립된 기구로 출범되어 그 역할이 더 커지고 전문성을 갖추게 되었다[16]. 위원회는 글로벌 기준에 부합하는 감독기구로서의 역할을 수행해야 할 것이다[13]. 우리는 국제사회에서 주도적으로 협력체계를 구축하고 리더십을 발휘해야 하며, 이 과정에서 필요하다면 국제협약의 체결 등 정부의 다각적인 노력이 필요하다. 또한 최근 국내 · 외 기업 간에 인수합병(M&A)이 이루어지는 사례가 늘어남에 따라 국내 기업의 핵심 기술이 유출되지 않도록 이에 따른 법률의 구축과 함께 M&A 단계별 가이드라인을 마련하고[2], 이의 원활한 집행을 위하여 국내 · 외의 관련 기구 간 협력체계를 견고하게 구축해야 한다. 데이터 처리 과정에서 각 기업 간의 보안 수준에 따라 데이터보호의 침해가 발생할 우려가 있기 때문이다[6].

5. 결 론

구글(Google), 애플(Apple), 페이스북(Facebook) 등의 해외 IT기업들의 인터넷 시장 점유율은 점점 높아지고 있는 추세이다. 반면 국내 기업들이 사업 확장과 운영에 어려움을 겪고 있는데, 그 원인 중 하나를 우리나라의 강력한 규제로 들 수 있고, 이로 인해 국내기업이 국외 기업과의 경쟁에서 오히려 역차별을 당하는 난항에 봉착하고 있다. 국내 · 외 주요 IT기업인 네이버(Naver), 다음(Daum), 구글(Google), 페이스북(Facebook)의 개인정보처리방침을 분석한 결과 우리나라 기업의 경우 한국의 개인정보보호법제를 준수하고 있다고 평가되는 반면 해외 IT기업의 처리방침의 경우 수집되는 범위에 관하여 명확하지 않은 표현을 사용하여 이용자가 자신의 정보가 어느 수준까지 수집되는지 알기가 어렵다. 또한 선택적 동의 사항을 구분하고 있지 않고 있고, 개인데이터의 삭제 혹은 파기의 경우에도 이용자에게 그 청구권을 주고 있어 적극적으로 파기 의무를 부여받는 국내사업자가 불리한 규제의 역차별을 받고 있는 상황에 놓여 있다. 2008년 당시 '구글(Google)의

유튜브(YouTube)'의 시장점유율은 2%였지만 2018년 기준86%를 차지할 정도로 성장하였으나, 국내 기업의 경우 동영상 시장의 2위인 '아프리카 TV'가 3%를 차지하고 있어 그 격차가 매우 크다. 이러한 격차의 발생은 국내의 강력한 개인정보보호법제의 규제가 그 원인 중 하나일 것이며, 이로 인하여 국내기업의 성장을 방해하고 오히려 외국 기업의 시장점유율을 높이는 규제의 역차별 상황을 초래하였다. 2012년 헌법재판소가 인터넷게시판 본인확인제에 대한 위헌결정의 논거 중 "국내 인터넷 이용자들의 해외 사이트로의 도피, 국내 사업자와 해외 사업자 사이의 차별 내지 자의적 법집행의 시비로 인한 집행 곤란의 문제를 발생시킬 뿐 당초 목적의 공익을 달성하고 있다고 보기 어렵다"(헌재 2012. 8. 23. 2010헌마47)는 내용은 이의 맥락을 함께한다고 볼 수 있다. 외국에서도 한국은 엄격한 프라이버시보호법을 가지고 있다는 평가를 받고 있는데 글로벌 기준에 맞추어 이용과 보호의 균형을 모색할 수 있는 작업이 필요하다. 또한 유럽연합의 GDPR처럼 역외적용과 관련한 규정의 흠결을 보완하고 해외 인터넷사업자에 대하여 법집행이 가능하도록 법제를 정비해나가야 한다. 마지막으로 개인정보보호기관은 국내·외 다른 보호기관들과 긴밀한 협력체계를 구축하여 개인정보보호의 집행력을 높여나가야 한다.

References

[1] Alex Wall, "GDPR matchup: South Korea's Personal Information Protection Act," Jan. 8, 2018.

[2] An, Y. B. and Chang, H. B., "A Study on Minimization of Leakage of Important Information in M&A," The Journal of Society for e-Business Studies, Vol. 25, No. 1, pp. 215-228, 2020.

[3] Buckner, T. K. and Knowles, B. L., "Privacy-Management, Legal Issues and Security Aspects", Nova, 2012.

[4] Determann, L., "Determann's Field Guide to Data Privacy Law," Edward Elgar, 2015.

[5] Floridi, L., "Protection of Information and the Right to Privacy-A New Equilibrium?," Springer, 2014.

[6] Grimmelmann, J., "Saving Facebook," 94 Iowa Law Review, pp. 1137-1206, 2009.

[7] Gustke, C., "Which countries are better at protecting privacy?," BBC Capital, Jun. 26, 2013.

[8] Hong, S. K. and Ko, Y. M., "A Study on the Countermeasures for the Fourth Industrial Revolution and the GDPR Focused on the Personal Information Protection Law," Dankook Law Review, Vol. 43, No. 1, pp. 313-337, 2019.

[9] Jang, W. and Shin, I., "The Online Privacy Policy: Recognition, Confirmation and its Effects on Online Transaction Behavior," Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 6, pp. 1419-1427, 2012.

[10] Jun, G. G., "A Study on the utilizable Scope of Personal Information," Ajou Legal Research, Vol. 6, No. 1, pp. 479-502, 2012.

[11] Kim, H.-K., “Study on Asymmetric Regulation Improvement of Online Services Based on Regulatory Principles on ICT Services,” SungKyunKwan Law Review, Vol. 26, No. 3, pp. 487-521, 2014.

[12] Kim, H.-W., “Constitutional Review of Personal Information,” Public Law Journal, Vol. 20, No. 4, pp. 63-98, 2019.

[13] Kim, I. H., “A Study on the Role and Function of Personal Information Protection Commission,” Study on American Constitution, Vol. 28, No. 2, pp. 219-273, 2017.

[14] Kim, I. H., “Streamlining Plan of Object of Application on the Personal Information Protection Act,” Public Law, Vol. 43, No. 1, pp. 31-54, 2014.

[15] Kim, K.-H., “Comparison of the Personal Information Protection legislation of Korea, EU, and Japan in terms of regulations,” NAVER Privacy White Pater, pp. 1-38, 2017.

[16] Kim, S.-A., “Meanings and Tasks of the Three Revised Bills which Ease Regulations on the Use of Personal Information,” Convergence Security Journal, Vol. 20, No. 2, pp. 59-68, 2020.

[17] Lee, I. H., “Analyzing the Concept of ‘Personal Data’ under the Personal Data Protection Act of Korea,” Journal of Korea Information Law, Vol. 19 No. 1, pp. 59-87, 2015.

[18] Lee, I. H., “Framework for Transatlantic Personal Data Flows,” Chonnam Law Review, Vol. 36, No. 3, pp. 79-108, 2016.

[19] McQuinn, A. and Castro, D., “Why Stronger Privacy Regulations Do Not Spur Increased Internet Use,” Jul. 11, 2018.

[20] MOIBA, “Mobile Content Industry Report 2019,” Ministry of Science and ICT, pp. 1-196, 2019.

[21] Nicoll, C., Prins, J. E. J., and van Dellen, M. J. M., “Digital Anonymity and The Law,” T・M・C, Asser Press, 2003.

[22] Park, K. B., Chae, S. H., and Kim, H. J., “Legal Treatment of Inferred Data in Korea,” Journal of Korea Information Law, Vol. 21, No. 2, pp. 159-202, 2017.

[23] Paul Sutton, “Data Protection in South Korea: Why You Need to Pay Attention,” Vistra(web), Aug. 15, 2018.

[24] Shim, W. H., “The Development of IoT Systems: Regulatory Issues and Directions,” KIPA Research Report, pp. 2070-2393, 2018.

[25] Son, H. S., “A study on the Direction of Korean Law by the review ing the A mended Act on the protection of Personal Information of Japan,” Public Law, Vol. 46, No. 2, pp. 295-329, 2017.

[26] Son, S. W., “Legal Issues on Facebook and Data Protection,” Gachon Law Review, Vol. 5, No. 1, pp. 305-335, 2012.

[27] Yun, J. H., “A Study on the Application of Law According to Change of Privacy Policy,” Kyungpook National University Law Journal, Vol. 41, pp. 391-428, 2013.

저 자 소 개

이인호 (E-mail: inho61@cau.ac.kr)
1985년 중앙대학교 법과대학 법학과 (학사)
1991년 중앙대학교 대학원 법학과 (석사)
1996년 중앙대학교 대학원 법학과 (박사)
1997년~2000년 헌법재판소 헌법연구원/헌법연구관보
2000년~현재 중앙대학교 법과대학/법학전문대학원 교수(헌법, 정보법)

김서안 (E-mail: vizlady@cau.ac.kr)
2009년 중앙대학교 법과대학 법학과 (학사)
2017년 중앙대학교 대학원 법학과 (석사)
2019년 중앙대학교 대학원 법학과 (박사 수료)