http://dx.doi.org/10.15539/KHLJ.50.4.1

정부기관의 정보열람 요구와 ISP의 협조의무

박 훤 일*

| 국문 요약 |

2016년 3월 대법원은 세간의 화제였던 '회피 연아' 사건에서 정보주체의 동의 없이 경찰에 통신자료를 제공한 NHN의 행위가 적법하였다며 원고에 대한 손해배상 책임이 없다는 판결을 내렸다. 원심이 ISP에 대한 통신자료 요청 시 법원의 영장을 요한다고 한 것을 뒤집은 것이다. 3월 초에는 많은 논란을 빚은 테러방지법이 국회를 통과하여 정부기관의 ISP에 대한 통신자료 요청은 더욱 늘어날 전망이다.

2013년 NSA에서 일하던 스노든이 미 정보기관의 글로벌 감시(PRISM) 프로그램을 폭로한 이후 각국은 정부기관의 정보접근에 매우 민감한 실정이다. EU에서는 2015년 10월 최고재판소가 정부기관의 ISP 정보열람이 허용되는 미국과 EU가 맺은 세이프하버 협정이 무효임을 선언하였고, 12월에는 회원국에 직접 법률로서 효력을 갖는 GDPR이 확정되었는데 정부기관의 정보열람을 엄격히 제한하고 있다.

6년을 끌었던 '회피 연아' 사건의 본질은 수사기관이 ISP가 보관하는 개인정보를 어느 범위까지 어떤 식으로 접근할 수 있는가로 요약할 수 있다. ISP가 수사기관의 통신자료 제출요청에 응할지 여부는 관련법에 그 기준과 절차가 정해져 있다. 이용자 인적사항은 익명을 많이 쓰는 ID를 제외하고는 전화번호부 수준이라 할 수 있다.

개인정보는 신성불가침이 아니고, 프라이버시권이 '홀로 있을 권리'에서 '개인정보 자기결정권'으로 바뀐 것처럼 빅데이터, 핀테크 등에 필수적인 개인정보는 'IT편의성을 증진하는 개인의 특권'으로 변모하고 있다. 정보주체의 권리인 만큼 자신에 관한 정보가 오·남용되는 것을 알았다면 지체 없이 시정하고 이를 야기한 책임자가 있다면 그로부터 응분의 피해보상을 받을 수 있어야 한다.

상기 대법원 판결에도 불구하고 ISP는 이용자들의 항의나 손배청구 소송을 우려하여 수사기관의 통신자료 제출요청에 영장 없이는 응하지 않을 방침이라고 한다. 개인정보 유출이나 오·남용 피해를 입은 개인에 대하여 ARCO(열람·정정·거부)권을 보장하고, 시차를 두더라도 개인정보가 수집된 정보주체에 대해서는 통지하는 절차가 필요하다고 본다.

---

* 경희대학교 법학전문대학원 교수, 법학박사. 경희법학연구소 연구위원.
(투고일자 : 2016.05.25, 심사일자 : 2016.06.15, 게재확정일자 : 2016.06.15.)

주제어 : 개인정보 열람, 통신자료 제출요청, 프라이버시권, IT편의성 증진, ARCO권

< 차 례 >

Ⅰ. 머리말

2016년 3월 10일 대법원이 내린 '통신자료 제공 관련 손해배상청구' 사건의 판결[1]은 국내외의 비상한 관심을 모았다. 그 이유는 세간의 화제를 모았던 사건의 재판 결과 원심 판결은 인터넷 포털 업체(Internet Service Provider: ISP)에 대한 통신자료 요청 시 법원의 영장을 요한다고 했는데 4년 만에 나온 대법원의 판단은 ISP가 영장 없이 통신자료의 요청에 응해도 적법한 행위라고 함으로써 해석상 혼란을 불러 일으켰기 때문이다.

이 사건은 인터넷 상에서 이른바 "회피 연아" 사건으로 널리 알려져 있었던 데다 저간의 상세한 내용이 외지에도 소개되고 학술논문[2]으로도 다루어진 바 있었다. 더욱이 3월 2일에는 야당의원들이 필리버스터까지 하면서 반대하였음에도 테러방지법이 국회를 통과하여 수사기관의 ISP에 대한 통신자료의 요청과 그에 따른 정보주체의 구제수단이 주목을 받았다.

국제적으로는 유럽연합(EU)에서 정부기관의 민간부문 개인정보의 열람이 허용

1) 대법원 2016.3.10.선고 2012다105482 판결 <http://glaw.scourt.go.kr/wsjo/panre/sjo100.do?contId=2197481>.

2) 예컨대 서울대 정상조 교수는 옥스퍼드 대학 학술지에 이에 관한 논문을 게재하였다. Sang Jo Jong, "Systematic Government Access to Private-Sector Data in the Republic of Korea", International Data Privacy Law (Oxford University Press), Vol.4, Issue 1 (2014), pp. 21-29.

되는 미국과의 세이프하버 협정(Safe Harbor Agreement)이 무효 선언을 받고, 회원국에 대한 직접적인 법률로서 효력을 갖는 개인정보보호규정(General Data Protection Regulation: GDPR)[3]이 확정되어 2018년 5월부터 시행될 예정이다.[4]

이 글은 상기 대법원 판결의 내용을 검토(II)하고 ISP의 통신자료 제공 협조 관행에 제동을 걸었던 원심 판결의 무엇을 문제 삼았는지 비교·분석(III)한 다음 이와 비슷한 사례인 EU 최고재판소의 쉬렘스 케이스(Schrems decision)와 비교(IV)해 보기로 한다. 이러한 비교·분석을 통하여 정보화 시대를 살고 있는 우리가 개인정보보호 법규를 실제 해석하고 적용함에 있어서 통신자료 등을 취급할 때에는 무엇을 유의해야 하는지 그 기준을 제시하고자(V) 한다.

Ⅱ. 정부기관 앞 통신자료 제공에 관한 대법원 판결

1. 대법원 2012다105482 판결의 요지

[1] 헌법 제10조의 인간의 존엄과 가치, 행복추구권과 헌법 제17조의 사생활의 비밀과 자유에서 도출되는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 정보주체가 스스로 결정할 수 있는 권리이다. 개인정보 자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 인격주체성을 특징짓는 사항으로

3) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL>

4) 우리 정부는 EU로부터 개인정보보호 법제의 수준이 EU기준에 비추어 적정하다는 평가(adequacy assessment)를 받기로 방침을 정한 바 있다. GDPR은 기존 개인정보보호 지침(Directive 95/46/EC)을 대체하기 위해 2012년 처음 제안되어 28개 회원국 간의 이견을 해소하고 2015년 말에 타결됨으로써 그 자체만으로 큰 의미를 갖는다. 그 밖에도 잊힐 권리(삭제요구권)의 인정, 개인정보 보호책임자(DPO)의 의무화, 위반 시 전세계 매출액 기준 과징금 부과 등 혁신적인 내용을 담고 있다.

서 개인의 동일성을 식별할 수 있게 하는 일체의 정보를 의미하며, 반드시 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지도 포함한다.

또 헌법 제21조에서 보장하고 있는 표현의 자유는 개인이 인간으로서의 존엄과 가치를 유지하고 국민주권을 실현하는 데 필수불가결한 자유로서, 자신의 신원을 누구에게도 밝히지 않은 채 익명 또는 가명으로 자신의 사상이나 견해를 표명하고 전파할 익명표현의 자유도 보호영역에 포함된다.

한편 헌법상 기본권의 행사는 국가공동체 내에서 타인과의 공동생활을 가능하게 하고 다른 헌법적 가치나 국가의 법질서를 위태롭게 하지 않는 범위 내에서 이루어져야 하므로, 개인정보자기결정권이나 익명표현의 자유도 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에는 헌법 제37조 제2항에 따라 법률로써 제한될 수 있다.

[2] 검사 또는 수사관서의 장이 수사를 위하여 구 전기통신사업법(2010. 3. 22. 법률 제10166호로 전부 개정되기 전의 것) 제54조 제3항, 제4항[5]에 의하여 전기

5) 구 전기통신사업법 제54조(통신비밀의 보호)
③ 전기통신사업자는 법원, 검사 또는 수사관서의 장(군 수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장으로부터 재판, 수사(조세범 처벌법 제10조제1항, 제3항 및 제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청받은 때에 이에 응할 수 있다. <개정 2002.12.26, 2007.1.3, 2010.1.1>
1. 이용자의 성명
2. 이용자의 주민등록번호
3. 이용자의 주소
4. 이용자의 전화번호
5. 아이디(컴퓨터시스템이나 통신망의 정당한 이용자를 식별하기 위한 이용자 식별부호를 말한다)
6. 이용자의 가입 또는 해지 일자
④ 제3항의 규정에 의한 통신자료제공의 요청은 요청사유, 해당이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 "자료제공요청서"라 한다)으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있는 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 해소된 때에 지체없이 전기통신사업자에게 자료제공요청서를 제출하

통신사업자에게 통신자료의 제공을 요청하고, 이에 전기통신사업자가 위 규정에서 정한 형식적·절차적 요건을 심사하여 검사 또는 수사관서의 장에게 이용자의 통신자료를 제공하였다면, 검사 또는 수사관서의 장이 통신자료의 제공 요청 권한을 남용하여 정보주체 또는 제3자의 이익을 부당하게 침해하는 것임이 객관적으로 명백한 경우와 같은 특별한 사정이 없는 한, 이로 인하여 이용자의 개인정보자기결정권이나 익명표현의 자유 등이 위법하게 침해된 것이라고 볼 수 없다.

2. 사건의 경위

2010년 3월 초 인천공항에서는 밴쿠버에서 귀국한 동계올림픽 선수단 환영식이 열리고 있었다. 당시 유인촌 문화체육관광부장관은 동계올림픽 피겨스케이팅 종목의 금메달리스트인 김연아 선수를 환영하면서 두 손으로 어깨를 감싸 안으려 하자 김연아 선수가 이를 회피하는 듯한 장면이 TV방송 취재진에 의해 촬영되었다. 인터넷에서 이 동영상을 발견한 인터넷 이용자 C는 이를 캡처하여 NHN이 운영하는 네이버 카페의 유머 게시판에 올렸다.

이 사진을 보고 수치스럽게 여긴 문화체육관광부장관은 그 다음날 이 사건 게시물을 인터넷에 올린 사람들을 종로경찰서에 명예훼손죄로 고소하였고, 이에 서울종로경찰서장은 2010년 3월 8일 NHN에 대해 "요청사유: 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반(명예훼손), 해당 이용자와의 연관성: 용의자 수사" 등을 기재한 자료제공요청서를 보내 원고의 인적 사항을 제공해 달라고 요청하였다. NHN 측은 이틀 뒤 종로경찰서장에게 원고의 "네이버 아이디, 성명, 주민등록번호, 이메일 주소, 휴대폰 번호, 네이버 가입일자"를 제공하였다.

종로경찰서장은 위와 같이 제공된 통신자료에 의하여 원고를 소환하여 명예훼손 혐의에 대해 조사를 하였으나, 그 다음 달 원고에 대한 고소가 취하되어 사건이 종결되었다.

그러나 C는 NHN이 자신의 동의를 받지 않고 개인정보를 경찰에 제공함으로써 자신이 경찰의 수사를 받는 등 개인정보 및 프라이버시를 침해 받았다고 주장하고 참여연대 공익법센터와 함께 NHN에 대하여 손해배상 청구 소송을 제기하였다.

여야 한다. <신설 2000.1.28>

Ⅲ. 원심과 대법원 판결의 비교·분석

1. 원심 판결의 개요

서울고등법원[6]은 위와 같은 사실관계를 토대로 하여, 전기통신사업자인 NHN에는 전기통신사업법에 의한 수사기관의 개인정보 제공 요청에 대해 개별 사안에 따라 그 제공 여부 등을 적절히 심사하여 이용자의 개인정보를 실질적으로 보호할 수 있는 역량을 갖추어야 하고, 구체적으로는 침해되는 법익 상호 간의 이익 형량을 통한 위법성의 정도, 사안의 중대성과 긴급성 등을 종합적으로 고려하여 개인정보를 제공할 것인지 여부 및 어느 범위까지의 개인정보를 제공할 것인지에 관한 세부적 기준을 마련하는 등 이용자의 개인정보를 보호하기 위한 충분한 조치를 취할 의무가 있다고 전제하였다. 그리고 이 사건 게시물은 공적 인물인 장관을 대상으로 한 것으로서 표현 대상과 내용, 표현 방법, 원고가 위 게시물을 게재한 동기와 경위 등에 비추어 위 게시물이 장관의 명예를 훼손하는 것이라고 보기 어려울 뿐만 아니라, 원고는 위 게시물을 직접 생산하거나 편집한 바 없이 다른 인터넷 사이트에 게시된 것을 이 사건 카페의 유머게시판에 그대로 옮긴 것에 불과하여 위 게시물로 인한 법익침해의 위험성이 원고의 개인정보 보호에 따른 이익보다 훨씬 중대한 것이라거나 수사기관에게 개인정보를 급박하게 제공하여야 할 특별한 사정이 있다고 보이지 않는다고 판단하였다.

따라서 피고인 NHN이 수사기관에 원고의 주민등록번호와 전화번호 등 인적사항 일체를 제공한 행위는 원고의 개인정보를 충실히 보호하여야 할 의무에 위배하여 원고의 개인정보자기결정권과 익명표현의 자유를 위법하게 침해한 것이라고 보고 금50만원의 손해배상을 명하는 원고 일부승소 판결을 내렸다.

2. 대법원 판결의 논거

대법원이 이 사건에서 원심판결을 파기한 논거를 간추리면 다음과 같다.

6) 서울고등법원 2012. 10. 18. 선고 2011나19012 판결.

(1) 구 전기통신사업법 제54조 제3항[7]은 "전기통신사업자는 법원, 검사 또는 수사관서의 장, 정보수사기관의 장으로부터 재판, 수사, 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 이용자의 성명, 주민등록번호, 주소, 전화번호, 컴퓨터시스템이나 통신망의 정당한 이용자를 식별하기 위한 이용자 식별부호인 아이디, 이용자의 가입 또는 해지 일자 등 통신자료의 열람이나 제출을 요청받은 때에 이에 응할 수 있다"[8]고 규정하여, 전기통신사업자에게 이용자에 관한 통신자료를 수사기관의 요청에 응하여 합법적으로 제공할 수 있도록 하고 있다.[9]

그리고 전기통신사업법 제54조 제4항은 위 제3항의 규정에 의한 통신자료 제공의 요청은 원칙적으로 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 '자료제공요청서'라 한다)으로 하도록 규정하고 있다.

위 각 규정에 따라 전기통신사업자가 수사기관의 통신자료제공 요청에 응하여 통신자료를 제공한 것이 위법하다고 하기 위해서는, 수사기관의 통신자료 제공 요청이 있을 때 전기통신사업자가 개별 사안의 구체적 내용을 살펴 그 제공 여부 등을 실질적으로 심사할 의무가 있다고 인정되어야 할 것이다. 그러나 다음과 같은 이유에서 일반적으로 전기통신사업자에게 그러한 의무가 있다고 볼 수는 없다.

(2) 전기통신사업법에 의하면 전기통신사업자는 통신자료 제공요청에 응할 수 있다고만 규정하고 있을 뿐 개별 사안의 구체적 내용을 살펴 그 제공 여부 등을 실질적으로 심사하도록 정하고 있지 않으며, 전기통신사업자에게 사안의 중대성과 긴급성 등의 심사를 기대하기도 어렵다. 오히려 전기통신사업자가 이러한 심사가 행하는 과정에서 혐의사실의 누설이나 그 밖에 사생활 침해 등을 야기할 가능성이 더 크다. 입법취지를 보더라도 통신비밀보호법에 의하면 현재 또는 과거에 이루어진 전기통신의 내용이나 외형적 정보[즉 통신사실확인 자료]에 대하여는 법원의 허가나 법관의 영장에 의하여만 이를 제공받을 수 있도록 한 반면,

---

7) 2010. 3. 22. 법률 제10166호로 전부 개정된 후에는 제83조 제3항으로 바뀌었다.

8) 전기통신사업법 2010. 3. 22. 전부 개정 시에는 본문의 술부 "요청받은 때에 이에 응할 수 있다"를 "요청하면 그 요청에 따를 수 있다"고 고치고 제5호의 "아이디(…)"를 "이용자의 아이디(…)"로 수정하였을 뿐이다.

9) 헌법재판소 2012. 8. 23. 선고 2010헌마439 전원재판부 결정 참조.

전기통신사업법에서는 수사상 신속과 다른 범죄의 예방 등을 위하여 통신자료에 대하여는 법원의 허가나 법관의 영장 없이도 수사기관의 자료제공요청서만으로 이를 제공하여 수사에 협조할 수 있도록 한 것이다.

(3) 전기통신사업법에서 수사기관의 요청에 의하여 전기통신사업자가 제공할 수 있는 통신자료는 이용자의 인적 사항에 관한 정보로서, 이는 주로 수사의 초기단계에서 범죄의 피의자와 피해자를 특정하기 위하여 가장 기초적이고 신속하게 확인하여야 할 정보에 해당한다. 이 규정에 따른 통신자료 제공으로 범죄에 대한 신속한 대처 등 중요한 공익을 달성할 수 있음에 비하여, 통신자료가 제공됨으로써 제한되는 사익은 해당 이용자의 인적 사항에 한정되므로 비례성의 원칙에도 반하지 않는다. 그리고 수사기관은 수사과정에서 취득한 비밀을 엄수하도록 되어 있어(형사소송법 제198조 제2항), 해당 이용자의 인적 사항이 수사기관에 제공됨으로 인한 사익의 침해 정도가 상대적으로 크지 않다고 할 수 있다.

(4) 물론 전기통신사업자가 수사기관의 통신자료 제공 요청에 따라 통신자료를 제공함에 있어서 수사기관이 그 권한을 남용하는 경우에는 해당 이용자의 개인정보와 관련된 기본권 등이 부당하게 침해될 가능성도 있다. 그러나 수사기관의 권한남용에 대한 통제는 국가나 해당 수사기관에 대하여 직접 이루어져야 하므로 전기통신사업자에게 실질적 심사의무를 인정하여 일반적으로 그 제공으로 인한 책임을 지게 하는 것은 국가나 해당 수사기관이 부담하여야 할 책임을 私人에게 전가시키는 것과 다름없다. 따라서 수사기관의 권한 남용에 의해 통신자료가 제공되어 해당 이용자의 개인정보에 관한 기본권 등이 침해되었다면 그 책임은 이를 제공한 전기통신사업자가 아니라, 이를 요청하여 제공받은 국가나 해당 수사기관에 직접 추궁하는 것이 타당하다. 그러므로 검사 또는 수사관서의 장이 통신자료의 제공 요청 권한을 남용하여 정보주체 또는 제3자의 이익을 부당하게 침해하는 것임이 객관적으로 명백한 경우와 같은 특별한 사정이 없는 한, 이로 인하여 해당 이용자의 개인정보자기결정권이나 익명표현의 자유 등이 위법하게 침해된 것이라고 볼 수 없다.

(5) 이 사건에서는 명예훼손 사건을 수사하는 종로경찰서장이 전기통신사업자인 피고에게 이 사건 게시물에 관한 통신자료의 제공을 요청하자, 피고가 위 규정에서 정한 요건과 절차에 따라 원고의 성명, 주민등록번호 등 통신자료와 함께

원고의 이메일 주소도 제공하였으나 그 이메일 주소는 원고의 네이버 아이디에 '@naver.com'이 붙어 있는 것이어서 법 규정에서 정한 제공의 범위를 초과하였다고 볼 수 없으며, 달리 종로경찰서장이 그 권한을 남용하여 통신자료 제공을 요청하는 것임이 객관적으로 명백하였다거나 그로 인하여 원고의 이익을 부당하게 침해할 우려가 있었다는 등의 특별한 사정을 찾을 수 없다.

따라서 피고가 종로경찰서장의 요청에 따라 이용자의 통신자료를 제공한 것은 전기통신사업법 규정에 따른 적법한 행위로서, 그로 인하여 피고가 원고에 대해 손해배상책임을 부담한다고 볼 수 없다.

그럼에도 원심은 이와 달리 피고가 원고의 개인정보자기결정권 및 익명표현의 자유를 위법하게 침해하였다고 판단하여 피고의 원고에 대한 손해배상책임을 인정하였으므로, 이러한 원심의 판단에는 전기통신사업법 제54조 제3항에 따른 전기통신사업자의 통신자료 제공을 위한 심사의 범위, 손해배상책임의 성립요건 등에 관한 법리를 오해하여 판결에 영향을 미친 위법이 있다.[10]

Ⅳ. EU 사법재판소의 쉬렘스 판결

1. 사건의 경위

오스트리아의 대학원생 막스 쉬렘스(Maximillian Schrems)는 그가 사회관계망 회원으로 가입한 SNS인 페이스북에 올린 자신의 글과 사진이 미국에 있는 페이스북 서버에서 처리되는 과정에서 미국 정부기관(NSA, CIA 등)이 이를 열람하지 않을까 하는 의구심을 갖게 되었다.[11] 유럽에서 페이스북의 SNS 사업은 아일랜

10) 대법원 1부[대법관 김소영(재판장), 이인복(주심), 이기택]는 나머지 상고이유에 대한 판단을 생략한 채 원심판결 중 피고 패소 부분을 파기하고, 이 부분 사건을 다시 심리·판단하도록 원심법원에 환송하였다.

11) 미국 실리콘밸리의 산타클라라 대학교에 교환학생으로 가서 공부하던 막스 쉬렘스는 페이스북 사내변호사의 특강을 듣고 나서 시험 삼아 페이스북에 있는 자신의 정보열람을 청구하였다. 그리고 미 기업들이 EU의 개인정보보호 법제에 소홀한 것을 지적하기 시작했

드 현지법인이 수행하고, 페이스북은 미국과 EU 간에 체결된 세이프하버 협정[12]에 따라 세이프하버 인증(Safe Harbor certification)을 받았기에 유럽 내 페이스북 이용자에 관한 모든 데이터를 아무 제한 없이 미국으로 가져가 미국에 있는 서버에서 처리하고 있었다.

2013년 쉬렘스는 아일랜드 개인정보감독기구에 대하여 페이스북이 유럽 이용자에 관한 데이터를 미국으로 가져가서 처리하는 것이 EU 법제를 준수하고 있는지 조사하고, 만일 위반하였다면 유럽 내 페이스북 이용자들의 데이터를 미국으로 이전하는 것을 금지시켜 달라고 요청하였다.

이에 아일랜드 개인정보감독기구는 EU 집행위원회가 미국과의 세이프하버 협정을 통해 미국 기업에 개인정보를 이전하는 것이 적정하다고 판정(Safe Harbor Adequacy Decision, 이하 세이프하버 "적정성 판정"이라 함)한 것에 따랐을 뿐이라며 쉬렘스의 요청을 거부하였다.[13]

쉬렘스는 이에 불복하여 아일랜드 고등법원에 제소[14]하였는데 아일랜드 법원에서는 회원국의 개인정보보호감독기구가 세이프하버 판정에 기속되는지 여부를 명확히 가려줄 것을 EU사법재판소(Court of Justice of the European Union)에 요청하였다.

다고 한다. Wikipedia 참조 <https://en.wikipedia.org/wiki/Max_Schrems>.

12) 미국은 개인정보보호 법제가 부문별로 개별법 위주로 되어 있어 전체적으로 개인정보보호가 적절하게 이루어지고 있는지 판단하기 어려웠다. 이에 따라 미 정부는 EU와 협상을 하면서 고지와 선택, 제3자 전송, 안전성 등에 관한 세이프하버 원칙을 정하고 관련기업들이 이 원칙을 자발적으로 준수하겠다고 미 상무부(DOC)에 신고하면 역외 전송되는 개인정보에 대하여 국가적으로 적절한 보호가 이루어지고 있다고 연방거래위원회(FTC)가 인증을 해주었다. 이를 토대로 2000년 7월 EU 집행위원회는 미국 정부가 개인정보를 적절하게 보호하고 있다는 세이프하버 판정을 내림으로써 세이프하버 인증을 받은 미국 기업(금융기관 제외)은 EU와 아무 제한 없이 개인정보를 포함한 정보의 교류를 할 수 있게 되었다.

13) Sarah Cadiot and Laura De Boel, "Safe Harbor invalid: What to expect after the ruling?", *Privacy Laws & Business International Report* Issue 137, October 2015, pp. 1, 3.

14) Case C-362/14 *Maximillian Schrems v. Data Protection Commissioner* [2015], available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=139721

2. 쉬렘스 판결의 골자

2015년 10월 6일 전세계적으로 관심이 집중된 가운데 EU사법재판소는 판결을 내렸다. 우선 집행위원회의 적정성 판정에 관계없이 개인정보보호 감독기구는 역외 제3국으로의 개인정보 이전이 적법한지 개별적으로 심사할 수 있다고 판단하였다. 그리고 적정성 판정과 같은 EU의 처분에 대하여는 사법재판소만이 무효를 선언할 수 있는데 여러 가지 사정에 비추어 볼 때 EU-미국 간에 체결된 세이프하버 협정은 무효(invalid)라고 선언하였다.

EU 사법재판소가 15년 동안 시행되어 온 세이프하버 판정을 뒤집은 것은 다음과 같은 이유에서였다.

무엇보다도 2013년 에드워드 스노든이 폭로한 미 정부기관의 전세계적인 정보통신 감청 사례에 비추어 EU 집행위원회가 세이프하버에 대하여 비판적인 의견[15]을 내놓은 것에 주목하였다. EU 사법재판소는 미국 측에서 주장하는 국가안보의 예외 사유가 EU의 개인정보보호 지침(EU Data Protection Directive 95/46/EC) 및 EU 기본권 헌장[16]에서 인정하는 기본권 보장을 침해할 수 있는 등 비례성의 원칙에 반함(disproportionate interference with the fundamental rights)을 지적했다. 그리고 EU 사법재판소는 아일랜드의 디지털권리에 관한 법률[17]을 들어 개인정보보호에 대한 예외 사유는 엄격히 해석하여 꼭 필요한(strictly necessary) 경우에만 인정할 수 있다고 말했다. 미국 정부기관이 행하고 있는 대중에 대한 감청(mass surveillance)은 엄격히 해석하여 꼭 필요한 범위를 벗어난다고 지적했다.

---

15) Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows' (COM(2013) 846 final, November 27, 2013) and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final, November 27 2013).

16) EU 기본권헌장(Charter of Fundamental Rights)은 EU 시민의 정치적·사회적·경제적 권리를 보장하는 법률문서로서 2000년에 채택되었는데 2009년 리스본협정을 계기로 본격 발효되어 EU의 각 기관과 회원국들은 이 헌장을 준수해야 한다: <http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm>

17) C-293/12 and C-594/12 Digital Rights Ireland and Others [2014], available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=153045&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=109775.

이와 아울러 사법재판소는 EU 주민들에 대한 정보를 미 정부기관이 열람하였을 때 이의신청이나 사법적으로 구제받을 수 있는 방법이 결여되어 있음을 비판했다. 세이프하버 협정에 의한 미 연방거래위원회의 인증 절차나 분쟁해결방법으로는 EU 시민들이 자신의 개인정보를 열람하거나 정정, 삭제할 수 없고, 미국의 감청 프로그램 하에서는 개인정보의 수집과 처리에 대한 행정적·사법적 구제방법이 결여되어 있다는 것을 문제 삼았다.

3. 쉬렘스 판결의 파급효

EU 사법재판소의 쉬렘스 판결은 다음 사항에 있어서 중요한 의미를 갖는다.

첫째, 각 회원국의 개인정보 감독기구는 EU 시민의 개인정보를 국제이전하는 것이 집행위원회의 적정성 판정에 따른 것이라 할지라도 그의 적법성에 관하여 독자적으로 조사권을 갖는다는 것과 EU 차원의 적정성 판정이라 해도 EU 지침이 각국의 개인정보보호 감독기구에 부여한 독립성이나 권한을 제한하거나 축소시키지 않는다는 것을 확인하였다. 다만, 각 회원국의 개인정보보호 감독기구는 적정성 판정 자체를 무효화할 수 없고 이러한 권한은 EU 사법재판소만이 행사할 수 있기 때문에 같은 개인정보의 처리를 놓고서 EU 역내시장이 적법과 부적법으로 분할(fragmentation of internal market)될 위험이 있다. 집행위원회나 EU지침 제29조 실무작업반의 가이드라인이 없는 한 그러한 위험의 소지가 크다.

둘째, EU 사법재판소는 어느 회원국에 설립된 특정 기업이 실제로 개인정보를 처리하지는 않더라도 정보처리와 관련된 영업활동(예컨대 판매활동)을 수행한다면 그 나라의 개인정보보호법이 적용되고 해당국의 개인정보보호 감독기구가 권한을 행사할 수 있다고 보았다. 이로 인한 불일치는 EU의 개인정보보호규정(GDPR)에 원스톱 숍과 회원국 간의 상이한 법제를 일치시키는 메커니즘이 도입되었기 때문에 크게 문제되지는 않을 전망이다.[18]

셋째, 세이프하버 룰에 대한 대안으로서는 어느 한 가지 방법만으로 해결할 수 없는 실정이다. 해당 기업의 데이터 처리 활동, 기업구조, 국제적인 정보이전의 성격과 빈도를 고려하여 다음의 대안 중에서 해결방안을 모색할 것으로 보인다.

18) 주 13)의 PLBI 기사 p. 3 참조.

즉, 정보주체의 동의(consent) 그밖에 EU 개인정보보호 지침에서 인정하는 예외사유(derogations)에 해당하면 그에 따른다. EU의 표준계약서 또는 특별약정에 의한 개인정보이전 계약의 체결하거나, 구속력 있는 기업규칙(Binding Corporate Rules: BCRs)[19]을 채택할 것으로 예상된다.

결국 세이프하버 룰에 의존해 왔던 기업들은 표준계약서나 BCRs를 이용하지 않을 수 없게 되었다. 이러한 표준계약서 조항이나 BCRs를 심사하는 각국의 개인정보보호 감독기구의 역할과 중요성은 상대적으로 더 커졌다고 말할 수 있다.

이와 함께 종전에는 그다지 이용되지 않았던 정보주체의 개별 동의를 받는 방안도 중요시되고 있는데 회원가입 화면에 동의 박스를 설치하는 것이 한 가지 예이다. 다만, 동의를 거부하거나 사후적으로 동의를 철회하는 이용자에 대한 대책도 마련해두어야 한다.

물론 미국과 EU 집행위원회는 기존 세이프하버 룰을 강화하거나 업그레이드하는 방안을 모색하고 있다. 2013년 11월 집행위원회가 미국 측에 요구한 13개항의 권고사항[20]을 토대로 국가안보를 이유로 한 예외 인정에 대하여 좀 더 강력한 보안대책을 추가하는 등 이른바 '세이프하버 2.0'을 논의한 바 있으며, 아예 세이프하버 룰을 대체할 수 있는 프라이버시 방패(Privacy Shield)를 설치하는 것도 심도 있게 검토하고 있다.[21]

---

19) 개인정보의 국외이전에 관한 EU 표준계약이나 BCRs는 제3국의 정보처리자에 대하여 현지 정부기관으로부터 정보제출 요구를 받았을 때 정보주체가 계약당사자는 아니지만 제3수익자(third party beneficiary) 조항을 근거로 피해구제 등 권리주장을 할 수 있게 하고 있다. 박훤일, 개인정보의 국제적 유통에 따른 법적 문제와 대책, 집문당, 2015, 161면.

20) European Commission's Memo "Restoring Trust in EU-US data flows - FAQs", 27 November 2013, available at http://europa.eu/rapid/pressrelease_MEMO-13-1059_en.htm. Laura Linkomies and Oliver Butler, "EU-US Safe Harbor at crossroads: A solution is urgently needed", *Privacy Laws & Business International Report* Issue 136, August 2015, pp.14-15.

21) Laura Linkomies, "From Safe Harbor to Privacy Shield: Where are we now?", *Privacy Laws & Business International Report* Issue 138, February 2016, pp.1, 3.

Ⅴ. 정부기관의 정보열람에 대한 안전대책

1. 논의의 필요성

앞서 설명한 '회피 연아' 사건이나 쉬렘스 케이스는 정부기관이 ISP에 대하여 통신자료의 제공을 요청할 경우 어떻게 대처해야 하는지 협조와 비협조의 선을 긋고 있다. 아직은 ISP나 이용자의 입장에서는 그 경계선이 모호하기 때문에 좀 더 명확한 가이드라인이 필요한 실정이다.

우리나라의 '회피 연아' 사건은 한국 최대의 인터넷 포털 네이버를 운영하는 NHN으로 하여금 수년 간 송사에 휘말리게 한 후 2016년 총선을 한 달 앞두고 대법원에서 최종 결론이 났다. 사건이 매우 중요한 의미를 내포하고 있음에도 비슷한 시기에 국회를 통과한 테러방지법만큼 주목을 받지는 못 했다.

이 사건의 본질은 정부 수사기관이 ISP가 보관하는 개인정보를 어느 범위까지 어떤 식으로 접근할 수 있느냐, 서비스 이용자의 간단한 인적사항(이용자의 ID, 성명, 주소 등)을 법원의 허가(사후 본인 앞 통보) 없이 조회할 수 있는가로 압축할 수 있다. 이를테면 정보통신의 '*habeas corpus*'(인신보호영장)라 할 수 있다. 정부기관의 정보통신에 대한 접근에 민감할 수밖에 없는 것은 2013년 스노든의 폭로로 인하여 "정보수사기관은 정보통신 내역을 무엇이든지 들여다보려고 한다"는 의구심에서 비롯되었기 때문이다.

이 문제는 EU 사법재판소가 쉬렘스 사건에서 중점적으로 다룬 만큼 우리나라의 개인정보보호 법제가 EU의 기준에 비추어 적정한지 판정을 신청[22]함에 있어서 반드시 정리해두어야 할 사안이라고 생각된다. 이를 위해서는 EU 집행위원회와 개인정보보호 감독기구, 사법재판소에서 문제를 삼은 미국 정보기관의 대중감시 내용과 우리나라 검사, 사법경찰관, 정보수사기관이 ISP에 대해 요청할 수 있는 통신자료와 통신사실확인자료의 내용을 비교해볼 필요가 있다. 다시 말해서 우리나라 정부기관이 ISP에 저장된 EU 시민의 개인정보를 임의로 열람한다거나 EU 시민에게 사법적 구제수단을 제공하지 않는다면 부정적인 판정을 받을 수 있기 때문이다.

22) 행정자치부 보도자료, "[EU 개인정보보호 적정성 평가] 국내 개인정보보호 수준, 국제기준에 맞춘 개인정보보호법 개정", 2015.12.15.

2. 정부기관의 정보열람에 대한 ISP 협조의 범위

'회피 연아' 사건에서 드러난 것처럼 우리나라의 ISP가 수사기관의 개인정보 제출요청에 대응하는 것은 관련법에 그 기준이 정해져 있다. 바로 이용자의 인적사항으로 성명과 주소, 전화번호, ID 등이며 익명(anonym)이나 가명(pseudonym)을 많이 쓰는 ID를 제외하고는 전화번호부(white page) 수준이라 할 수 있다. 이러한 차이점으로 인하여 수사기관의 통신자료 요청에 대해 이동통신사는 '114 전화번호 안내'나 다름없이 그 요청에 응하는[23] 반면 ISP는 정보주체 식별이 가능한 ID를 포함한 통신자료를 제공하는 데 주저하는 것이다. 이 때문에 이 사건의 원심 판결에서는 ID를 포함한 통신자료의 제공에 있어서도 ISP의 내부적 심사 또는 법원의 허가가 필요하다고 보았던 것이다.

전기통신사업자의 통신자료와 통신사실확인자료

구 분	통신 자료	통신사실확인 자료
내 용	1. 이용자의 성명 2. 이용자의 주민등록번호 3. 이용자의 주소 4. 이용자의 전화번호 5. 이용자의 아이디(컴퓨터시스템/통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호) 6. 이용자의 가입일 또는 해지일	1. 가입자의 전기통신일시 2. 전기통신개시·종료시간 3. 발·착신 통신번호 등 상대방의 가입자번호 4. 사용도수 5. 컴퓨터통신 또는 인터넷의 사용자의 컴퓨터통신/인터넷의 로그기록자료 6. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료 7. 컴퓨터통신/인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

23) 이러한 연유에서 SKT, KT, LG U+ 등 국내 이동통신 3사는 수사기관의 개인정보 제공요청에 계속 응하고 있다. 수사기관이 영장 없이 제출받은 통신자료는 2012년 787만여 건, 2013년 957만여 건, 2014년 1296만여 건으로 해마다 늘고 있다.

구 분	통신 자료	통신사실확인 자료
근거규정	전기통신사업법 제83조(통신비밀의 보호) 제3항	통신비밀보호법 제2조(정의) 11호, 제13조(범죄수사를 위한 통신사실 확인자료제공의 절차), 13조의2(법원에의 통신사실 확인자료제공), 제13조의4(국가안보를 위한 통신사실 확인자료제공의 절차 등)
요청기관	검사 또는 수사관서 정보수사기관 법원	검사, 사법경찰관 정보수사기관 법원
요청절차	요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(통신자료제공요청서)을 4급 이상 공무원, 총경 등의 결재를 득한 후 요청	요청사유, 해당 가입자와의 연관성, 필요한 자료의 범위를 기록한 서면을 검사·사법경찰관은 법원의 허가(정보수사기관은 고법 수석부장판사의 허가)를 얻어 요청
사후절차 사업자에 대한 규제	전기통신사업자는 미래창조과학부에 현황 보고하고, 내부적으로 통신비밀 보호 준수, 통신자료제공 관련 서류 보관, 통계보고 및 전담기구를 설치·운영	수사기관은 가입자에게 통지 전기통신사업자는 미래창조과학부에 현황 보고

요컨대 대법원은 전기통신사업법 해당 규정의 해석과 관련하여[24] 전기통신사업자인 ISP의 대정부 협조의무에 명확히 선을 그었다고 볼 수 있다. 즉, 수사기관의 자료요청에 대하여 ISP는 사안의 중대성과 긴급성 등 실질적 심사를 할 의무가 없으며, 법에 규정된 통신자료를 제공함으로써 신속한 수사와 다른 범죄의 예방이라는 공익을 달성하는 것이 해당 이용자의 사익을 제한하는 것[25]보다 상

24) 국회입법조사처의 심우민 조사관은 “프라이버시 보호를 위한 통신자료 제공제도의 개선방향” 보고서를 통해 이 제도는 1993년 제정된 공중전기통신사업법에 바탕을 두고 있는데, 사실상 유선전화 시절의 체계를 상당부분 유지하고 있다고 말하고, “현대 모바일 환경에서는 사실상 이용자와 기기가 1대 1로 대응하는 만큼 과거 통신자료 제공에 비해 기본권 제약의 가능성이 커 제도개선이 필요하다”고 지적했다. 국회입법조사처, “프라이버시 보호를 위한 통신자료 제공제도의 개선방향”, 이슈와 논점 1135호, 2016.3.16.

25) 수사기관은 수사과정에서 취득한 비밀을 엄수하도록 되어 있어(형사소송법 제198조 2항), 해당 이용자의 인적 사항이 수사기관에 제공됨으로 인한 사익의 침해 정도가 상대적으로 크지 않다고 할 수 있다.

대적으로 크다고 볼 수 있고, 수사기관의 권한남용으로 볼 만한 특별한 사정이 없다면 ISP의 통신자료 제공은 적법한 행위라는 것이다.

위의 대법원 판결에도 불구하고 국내 인터넷 포털 업체들은 이용자의 ID를 포함한 통신자료를 수사시관에 제출하지 않더라도 이에 대한 벌칙 규정이 없는 데다[26] 서울고등법원의 2012년 판결 이래로 이용자들로부터 손해배상청구 소송을 당할 수 있다는 점 때문에 수사기관의 협조요청에 잘 응하지 않는 것으로 알려졌다.[27] 수사기관에 통신자료를 제출한 경우에는 법률로 의무화되어 있는 것은 아니지만 사후에 이용자에게 통보하는 것을 검토하고 있다.[28]

국민보호와 공공안전을 위한 테러방지법의 입법과정에서 대테러센터가 테러방지 및 수사를 위해 거의 제약 없는 정보수집활동을 벌이지 않을까 우려되었으나 국회를 통과한 최종안에서는 국가정보원장이 테러위험인물에 대하여 출입국·금융거래 및 통신이용 등 관련 정보를 수집하는 경우 출입국·금융거래 및 통신이용 등 관련 정보의 수집에 있어서는 출입국관리법, 관세법, 특정 금융거래정보의 보고 및 이용 등에 관한 법률, 통신비밀보호법의 절차에 따르도록 하여 일반의 우려를 불식하였다(제9조 1항). 그리고 테러위험인물에 대한 개인정보(민감정보 포함)와 위치정보를 개인정보보호법의 개인정보처리자와 위치정보의 보호 및 이용 등에 관한 법률의 위치정보사업자에게 요구할 수 있게(제9조 3항)[29] 하는 한편 대테러 인권보호관(ombudsman, 제7조)을 두도록 하였다.

---

26) 헌법재판소는 2012년 구 전기통신사업법상에 규정되었던 같은 내용의 통신자료 제공에 대한 헌법소원 사건(헌법재판소 2012.8.23. 선고 2010헌마439 전원재판부 결정)에서 "해당 법률조항에 따르면 수사관서의 장이 이용자에 관한 통신자료제공을 요청하더라도 이에 응할 것인지 여부는 전기통신사업자의 재량에 맡겨져 있다"며 "따라서 수사관서의 장의 통신자료제공 요청과 이에 따른 전기통신사업자의 통신자료 제공 행위가 있어야 비로소 통신자료와 관련된 이용자의 기본권제한 문제가 발생할 수 있는 것이지, 이 사건 조항만으로 이용자의 기본권이 직접 침해된다고 할 수 없다"면서 각하 결정한 바 있다.

27) 국내 제2위 포털업체인 다음카카오의 투명성 보고서에 따르면, 통신자료의 요청건수가 2012년 상반기 8,425건에서 2015년 하반기에는 98건으로 급감했다고 한다. 다음카카오의 같은 기간 처리건수는 6,005건에서 제로(0)가 되었다. <http://privacy.kakaocorp.com/transparence/report/request>

28) 통신사실확인 자료는 전기통신사업자로부터 제출을 받은 수사기관이 사후에 가입자에게 이 사실을 통지하도록 되어 있다.

29) 국가정보원장은 대테러활동에 필요한 정보나 자료를 수집하기 위하여 대테러조사 및 테러위험인물에 대한 추적을 할 수 있는데, 이 경우 사전 또는 사후에 국가테러대책위원회 위원장에게 보고하도록 했다(테러방지법 제9조 4항).

미국의 경우에는 우리와 사정이 크게 다르다. 9.11 테러 사건 이후 정보통신자료의 중요성이 부각되자 2007년 국가정보국(NSA)을 중심으로 미국내 ISP들로부터 인터넷 통신자료를 수집하는 PRISM 작전[30]이 개시되었다. PRISM은 외국첩보감시법(Foreign Intelligence Surveillance Act: FISA)에 의하여 설치된 특별법원(FISA Court)의 감독 하에 운영되는데 2007년 부시 행정부의 미국수호법(Protect America Act)이 미 의회를 통과함에 따라 출범하였다. 2008년 FISA 개정법률 제702조에 의거하여 NSA는 구글, 페이스북, 마이크로소프트, 유투브 같은 ISP에 대해 보관 중인 대상자의 인터넷 통신자료(target communications)를 요청할 수 있다. 이러한 은밀한 정보수집활동은 스노든에 의해 전세계에 알려졌으며, 그는 정보수집의 범위가 일반이 알고 있는 것보다 훨씬 광범위하고 아주 위험한 범죄활동에 대한 정보도 포함되어 있다고 폭로했다.[31]

미국 정부의 부인에도 불구하고 PRISM에 의한 통신정보의 수집은 외국의 테러용의자 외에도 유명 정치인, 재계인사, 국내 인물들까지 대상으로 하고 있으며, 워낙 은밀하게 행해지는 첩보작전이기에 그 대상자에 대한 통지나 사법절차를 통한 권리구제는 생각할 수도 없는 실정이었다. 그러나 2015년 여름 의회를 통과한 미국자유법(USA Freedom Act)에 의하여 NSA는 같은 해 11월 29일부터 미 국민의 전화통신정보(bulk collection of telephone metadata)를 직접 보관하지 못하게 되었다.[32] 통화 내용을 엿듣는 것은 아니지만 통화대상자, 장소와 시간, 통화지속시간 같은 데이터를 축적함으로써 개인의 프로파일을 생성할 수 있는 것들이다.[33]

미국자유법은 그 동안 비밀에 가려졌던 PRISM의 감독기구 FISA법원에 대해서도 결정사건의 비밀분류를 해제하고 외부인이 이의할 수 있는 여지를 만들어 두었다. 프라이버시 보호론자들도 특정 테러용의자나 위험인물을 겨냥한 감시

30) 2013년 6월 NSA의 직원이었던 에드워드 스노든이 폭로한 바에 의하면 PRISM이란 미 정부 코드네임이 SIGAD US-984XN인 감청(mass surveillance) 프로그램이다.

31) 스노든의 폭로는 2013년 6월 3일 영국 가디언지와 미국 워싱턴포스트지에 게재되어 세계적으로 엄청난 충격과 폭발적인 반향을 일으켰다. PRISM으로 수집되는 정보는 NSA의 분석을 위한 가공되지 않은 상태의 이메일, 음성, 사진, 비디오, 인터넷전화(VoIP), 화상통화, 로그인정보, SNS메시지 등을 망라하고 있다. Wikepedia <https://en.wikipedia.org/wiki/PRISM>

32) 전화통화가 아닌 인터넷이나 SNS 메시지 같은 대량의 통신정보는 계속 수집·보관할 수 있다.

33) 미국 NSA가 수집·보관하였던 개인의 통신정보는 우리나라 관련법 상의 이용자에 관한 통신자료가 아니라 통신사실확인 자료에 해당하는 것임을 알 수 있다.

(targeted surveillance) 활동 자체를 반대하는 것은 아니다. 그들이 주장하는 것은 효과가 입증되지도 않은 무차별적인 대중에 대한 감시활동을 접으라는 것이다. 그들은 미국이나 유럽 각지에서 벌어졌던 테러 사건에서 테러범이 접촉한 인물을 찾는 것도 중요하지만 대부분 정보당국에 알려진 용의자들이었지 전화통화기록을 뒤져서 알아낸 인물은 거의 없었다고 지적했다.[34]

Ⅵ. 결론 - 새로운 개념정립의 필요성

각 개인은 헌법상 사생활의 비밀을 보장받으므로 프라이버시 침해의 우려가 있는 개인정보에 대하여 법적인 보호를 받는 것이 당연하다. 프라이버시권(right to privacy)은 본래 타인으로부터 홀로 있을 권리(right to let alone)를 뜻하였으나 자신에 관한 정보를 스스로 통제할 수 있다는 개인정보 자기결정권으로 바뀌었다.[35]

정보화 시대인 지금은 패러다임이 달라져야 한다.[36] 개인정보는 무조건 보호받아야 한다고 하기보다 누구든지 개인정보가 상당히 세상에 알려져 있는 만큼[37]

34) The Guardian, “The NSA's bulk metadata collection authority just expired. What now?”, November 28, 2015. <http://www.theguardian.com/us-news/2015/nov/28/>

35) 권건보, “정보주체의 개인정보자기결정권”, 고학수 편, 개인정보 보호의 법과 정책, 박영사, 2014, 3～10면.

36) 개인정보는 민감정보를 제외하고는 그 자체가 신성불가침의 권리는 아니라 할 수 있다. 개인정보의 유출이나 오·남용으로 2차적인 피해가 우려되기 때문에 그에 대한 보호가 강화되고 있다. 2014년 초의 신용카드정보 대량유출 사고 때 경험한 바와 같이 실제 피해를 입었다고 보고된 사례는 거의 없었음에도 ID와 비밀번호의 변경, 계좌이동 등으로 막대한 사회적 비용을 지불하는 일은 지양해야 한다. 최근 피해가 속출하고 있는 보이스피싱이나 파밍은 개인정보의 유출로 인한 것이라기보다 대부분 이미 알려진 개인정보의 관리나 대처를 소홀히 하여 금전적 피해가 발생한 것이다.

37) 사회생활을 하면서 주고받는 개인명함(business card)에 수록되어 있는 정보는 설령 그로 인한 피해를 입었다 하더라도 정보가 유출된 원인을 찾거나 손해발생과의 인과관계를 인정하기 어렵기 때문에 개인정보로서 보호받아야 함을 주장하기 어렵다. 그리고 많은 사람이 가입한 사회관계망(social network)을 통해 주고받는 개인정보 역시 개인정보의 보호보다는 오·남용의 방지가 더 중요한 이슈로 대두되고 있다.

이러한 개인정보가 오·남용되는 것을 피하고 보다 유익하고 가치 있는 정보를 창출하는 데 기여할 수 있어야 한다. 다시 말해서 프라이버시를 다소 양보하더라도 공개적으로 유용한 정보를 얻을 수 있다면 비례성의 원칙, 투명성이 확보될 수 있다고 본다. 예컨대 빅데이터, 핀테크 등에 필수적으로 쓰이는 개인정보는 "정보기술의 편의성을 증진하는 개인의 특권(privilege to enhance IT convenience)"이라 할 수 있다.[38] 이와 같은 개인정보에 대한 인식의 전환은 사회경제적 활동에도 유리하고 개인정보·위치정보를 이용하는 산업의 발전에도 도움이 될 것이다. 다른 한편으로는 자신에 관한 정보가 오·남용되는 것을 알았다면 이를 지체 없이 시정하고 이를 야기한 책임자가 있다면 그로부터 응분의 피해보상을 받을 수 있어야 한다.

이러한 견지에서 이 글에서 다룬 대법원 판결은 개인명함에 수록된 개인정보나 다름없는 통신자료에 대하여 전기통신사업자에게 엄중한 책임을 부과하지 않은 점에서 올바른 결정이라 생각한다.[39] 다른 한편으로는 개인정보에 대한 의식이 투철해진 이용자들의 항의나 손해배상 청구소송을 우려하여 ISP가 정부기관에 대한 통신자료를 영장 없이는 제공하지 않는 것도 그에 대한 제재 규정이 없는 이상 나무랄 일이 아니다. 정보화 시대에는 모든 정보통신 서비스 가입자들이

38) 빅데이터의 이용이 급증함에 따라 한국방송통신위원회(KCC)는 2014년 12월 「빅데이터 개인정보보호 가이드라인」을 제정하였고, 금융위원회는 2016년 4월 개인신용정보를 빅데이터로 활용하여 핀테크 산업을 활성화하기 위한 신용정보법령의 개정안을 입법예고한 바 있다. 일부 시민단체와 인권단체의 반대를 무릅쓰고 정부가 개인정보의 활용을 원활히 하는 방향으로 규범을 바꾸는 것은 개인정보의 IT편의증진 기능을 중시하는 데 따른 것으로 풀이된다.

39) 어느 대학이 강연회를 개최하면서 참가신청서에 학적번호, 이름, 주소 및 전화번호를 기재하도록 하였는 바, 주최자가 이를 경찰에 제공한 사건이 있었다. 일본 최고재판소는 "자기가 원하지 않는 타인에게 함부로 이를 알리지 않도록 생각하는 것은 자연스러운 것이며 이러한 기대는 보호되어야 할 것"이라며 주최자가 이를 사전에 참가신청자의 동의를 구하는 것이 곤란하였다는 특별한 사정이 엿보이지 않는다면 이는 참가신청자의 프라이버시를 침해한 것으로 불법행위를 구성한다고 판시하였다. 最高裁 2003.9.12. 第2小法廷判決 (民集 57·9·783). 이 판결에는 2명의 재판관이 반대의견을 냈는데, 주최자가 대학으로서 학문의 자유, 집회의 자유를 주장할 수 있었고, 소속학과와 학년을 알 수 있는 학번이 포함된 점, 경찰이 이러한 자료를 요청할 수 있는 근거규정이 없었다는 점 등이 고려된 것으로 보인다. 본건 사건과 비교할 때 이메일이 일반우편을 대체하게 된 오늘날 이메일 주소도 일반 주소나 다름없이 취급될 수 있을 것이다.

나름대로 범죄예방이나 국가안보와 같은 공익의 실현과 프라이버시라는 사익의 보호에 대한 균형감각을 갖고 있기 때문이다.

개인정보는 국경을 넘어 원활히 유통(transborder data flow: TBDF)되는 것이 바람직하므로 다른 나라에서도 우리 국민의 개인정보가 적절하게 보호받을 수 있는지, 또 다른 나라 국민의 개인정보가 본국에서와 같은 수준 이상으로 보호받을 수 있는지 확실히 해두는 것도 중요하다.[40] 이 경우에도 피해를 입은 개인은 국적 불문하고 사법적으로 구제받을 수 있는 길이 보장되어야 할 것이다.

이러한 개인정보의 새로운 개념에 입각하여 EU 사법재판소의 쉬렘스 판결과 GDPR 규정, 그리고 만물 인터넷(Internet of Everything: IoE) 시대의 빅데이터 개념을 살펴보기로 한다. EU 측 재판관들은 미국의 PRISM 프로그램에 의해 인터넷 상의 개인정보가 무차별적으로 정부기관(NSA)에 의해 수집되고 있으며 EU 시민들의 개인정보 역시 NSA가 들여다 볼 것임을 우려하였다. 또한 인공지능을 장착한 슈퍼컴퓨터가 가동되고 있는 상황에서 요구되는 것은 개인명함에 수록되어 있는 정도의 정보수집(bulk collection of metadata)이 아니라 정보의 오·남용 피해를 입은 개인에 대하여 이른바 ARCO권(열람·정정·거부의 권리: rights to access, rectification and objection)을 보장하는 것임을 분명히 했다. 미국 정부도 스노든의 폭로 후 국제사회의 반발, 특히 세이프하버 협정의 무효 선언에 따라 FISA법원의 존재를 일부 공개하고 미국자유법을 시행하는 등 절차를 개선할 움직임을 보이고 있다. 쉬렘스 판결에 있어서도 미국의 대테러 조사활동을 문제 삼았다기보다도 EU 시민들의 사법구제 공백을 우려한 것이므로 약간의 시차를 두더라도 개인정보가 수집된 정보주체에 대해서는 통지하는 절차가 반드시 필요하다고 본다. GDPR에서도 정보주체에 대하여 기본적으로 ARCO권을 보장하고 있을 뿐만 아니라(GDPR 제13조~제17조) 이를 위반한 감독기관의 결정이나 정보처리로 인하여 피해를 입은 정보주체가 이의(complaint)를 하거나 사법구제(judicial remedy)를 청구할 수 있는 길을 열어놓고 있다(GDPR 제77조, 제79조 등).

그리고 만물 인터넷(IoE) 시대에는 개인정보·위치정보가 보호대상이라기보다는 비식별화·익명화를 조건으로 한 이용대상으로 바뀌고 있으므로[41] 역시 ARCO권

40) 행정자치부에서도 개인정보의 국제이전에 있어서 정보주체의 동의 외에도 체계적인 안전대책을 요하는 개인정보보호법의 개정을 추진 중인 것으로 알려졌다.

41) 일본이 2015년에 개정한 개인정보보호법은 '익명가공정보'(anonymous processed information)라는 개념을 신설하고(제2조 9항, 10항) 특정 개인을 식별할 수 없도록 개인정보를 가공

을 전제로 침해 시에는 징벌적 손해배상을 포함한 사법구제를 받을 수 있음을 명시하여야 한다. 이것이 제대로 이루어지고 있는지 감시하는 시민단체, 인권단체의 모니터링 활동도 정부가 이를 지원하는 것이 바람직하다.

한국에서는 수사기관의 협조요청에 따라 통신자료를 제공한 ISP의 행동이 적법하였다고 판단한 대법원 판결이 나온 뒤 한 달 후에 총선이 있었다. 그 결과 집권당이 많은 의석을 잃고 두 야당이 다수석을 점하는 與小野大의 정국이 등장하였다. 단순 통신자료는 법원의 심사 없이 수사기관에 제공할 수 있도록 한 전기통신사업법의 해당 규정을 입법적으로 해결할 수 있는 상황이 도래한 것이다.[42] 입법적으로 해결을 도모하지는 않더라도 통신자료와 통신사실확인 자료를 구별하여 전자의 경우에는 전기통신사업자가 이용자들의 반응을 염두에 두고 처리하고 있는 현재의 관행이 지속될 전망이다. 요컨대 정부기관이 ISP가 보관하고 있는 개인정보를 ISP의 협조를 얻어 어디까지 열람할 수 있느냐의 문제는 선거권자를 포함한 서비스 이용자들의 변화하고 있는 의식,[43] 즉 개인정보의 보호가 중요하냐 아니면 효과적인 활용이 우선하느냐에 달려있다고 하겠다.

한 것이라고 정의하는 한편, 그 가공방법을 규정하고 사업자에 의한 공표 등 그 취급에 관하여 까다로운 규율을 마련하도록 했다(제36조~제39조).

42) 민주사회를 위한 변호사 모임과 참여연대 등의 단체들은 2016년 4월 총선 이후 헌법소원과 함께 수사기관과 전기통신사업자를 대상으로 한 손해배상소송까지 예고했다. 장혜진, "'통신자료 제공' 논란 속 당사자에 통지 싸고 '갑론을박'", 법률신문, 2016.4.4.

43) 예컨대 통신사실확인자료는 법적으로 당사자 통지를 일정기간 유예할 수 있는 반면 통신자료제공은 당사자가 전기통신사업자에게 확인하면 곧바로 확인할 수 있게 되어 있다. 수사기관에서는 수사의 밀행성이 요구되는 공안사범 수사 등 국가안보를 위해 특별히 필요한 경우에는 일정기간 통신자료제공 사실도 확인해 줄 수 없도록 해야 한다는 주장이 나왔다. 위의 법률신문 기사 참조.

참고문헌

고학수 편, 개인정보 보호의 법과 정책, 박영사, 2014.

박훤일, 개인정보의 국제적 유통에 따른 법적 문제와 대책, 집문당, 2015.

Sang Jo Jong, "Systematic Government Access to Private-Sector Data in the Republic of Korea", *International Data Privacy Law* (Oxford University Press), Vol.4, Issue 1, 2014.

Sarah Cadiot and Laura De Boel, "Safe Harbor invalid: What to expect after the ruling?", *Privacy Laws & Business International Report* Issue 137, October 2015.

Graham Greenleaf, *Asian Data Privacy Laws —Trade and Human Rights Perspective*, Oxford University Press, December 2014.

_____, "Japan: Toward international standards–except for 'big data'", *Privacy Laws & Business International Report* Issue 135, June 2015.

Laura Linkomies, "From Safe Harbor to Privacy Shield: Where are we now?", *Privacy Laws & Business International Report* Issue 138, February 2015.

_____ and Oliver Butler, "EU-US Safe Harbor at crossroads: A solution is urgently needed", *Privacy Laws & Business International Report* Issue 136, August 2015.

인터넷 자료 [2016. 5. 18. 최종접속]

법률신문, "'통신자료 제공' 논란 속 당사자에 통지 싸고 '갑론을박'". 2016.4.4.
<https://www.lawtimes.co.kr/Legal-News/Legal-News-View?Serial=99441&kind=AD02>

행정자치부, "[보도자료: EU 개인정보보호 적정성 평가] 국내 개인정보보호 수준, 국제기준에 맞춘 개인정보보호법 개정", 2015.12.15.

국회 입법조사처, "프라이버시 보호를 위한 통신자료 제공제도의 개선방향", 이슈와 논점 1135호. <http://www.nars.go.kr/>

The Guardian, "The NSA's bulk metadata collection authority just expired. What now?", November 28, 2015. <http://www.theguardian.com/us-news/2015/nov/28>

다음카카오 투명성 보고서 <http://privacy.kakaocorp.com/transparence/report/request>

EU법령 검색 <http://eur-lex.europa.eu/homepage.html?locale=en>

Wikipedia <https://en.wikipedia.org/>

Abstract

Government Access to Personal Data and ISPs' Response

Park, Whon-Il*

In March 2016, the Supreme Court rendered a noteworthy decision that an Internet portal service provider (ISP) need not pay compensation to the plaintiff who argued the ISP had provided his personal data to police without his consent. The highest court reversed the appellate court ruling which said ISP's provision of such personal data required the court warrant on account of customers' constitutional rights of self-determination and anonymous speech. The above Supreme Court decision came right after the National Assembly passed the controversial Anti-terrorism Act, which authorizes the head of the National Intelligence Service (previously known as the Korean CIA) to collect personal information as well as location information of a certain terrorist suspect from ISPs pursuant to the existing laws.

Since Edward Snowden disclosed the global surveillance (PRISM) programme of the National Security Agency to the world in June 2013, the government accesses to personal data in the private sector have been a hot issue around the world. At this juncture, the Court of Justice of the European Union declared the Safe Harbor Agreement between the European Union and the United States invalid. In December 2015, the General Data Protection Regulation, which is legally binding all member states and strictly limiting government accesses to personal data, was consolidated to become effective in May 2018.

The main question of the six-year long "Minister Avoiding" Yuna litigation seemed to be to what extent the government investigation agency may access to personal data stored by ISPs, and whether the government agency may request ISPs to provide simple personal data without court warrants. The Telecommunications Business Act provides the statutory ground for ISPs to respond to such requests. The scope of

* Ph.D., Professor of Law at Kyung Hee University Law School.

personal data requested by the prosecutors or police officers is the personal information including name, address, telephone number and email address, which is usually contained in an ordinary business card.

It should be noted that personal information is no more sacrosanct right in the Information Age. Historically, the right to privacy has changed from the right to be let alone (as termed by Warren and Brendeis) to the right of self-determination of personal information. Nowadays personal information, subject to appropriate processing of de-identification or anonymization, has become inevitable to Big data and Fintech businesses. Then the right to privacy has turned out to be an individual privilege to enhance IT convenience. Also any data subject should be ensured the rights to access, rectification, cancellation and objection (ARCO) relating to his/her personal data and the effective administrative and judicial remedies including pecuniary compensation and punitive damages, if necessary, in case of abuse or misuse of personal information.

At the moment, the above mentioned Supreme Court decision is not supposed to change the year-long practices that government agencies need to obtain warrants in order to have personal data disclosed by ISPs. After the said Supreme Court decision, big portal operators seem to maintain their policy of no-more-cooperation with the investigation authority. It's because they know the failure to disclose personal data to the government agency would cause no punishment but clamorous requests from investigators while any delivery of personal data would bring avalanche of users' lawsuit for damages. In the long run, the awareness of privacy or increasing inclination towards IT convenience on the part of users could determine the future of the relevant provisions of the Telecommunications Business Act and the prevailing government practices.

Key Words : government access to data, request of communications data, right to privacy, individual privilege to enhance IT convenience, ARCO rights