

# 2018 한국인터넷거버넌스포럼(KrIGF) 워크숍 보고서

작성자 : 유혜민(서강대학교)

세션명	데이터 거버넌스: 소셜 네트워크와 프라이버시			
일시	2018.07.05(목) 13:30~15:00	장소	서울창업허브 세미나실 4	
참석자	사회	최은창(Free Internet Project, 펠로우)	발제	최은창(Free Internet Project, 펠로우)
	패널	정명현(고려대학교, 교수)		이재림(네이버 프라이버시&시큐리티팀, 부장)
정영훈(한국소비자원, 선임연구원)		윤재석(KISA 개인정보협력팀, 팀장)		
플로어	약 25명 참여			

제안내용	<p>최근 인터넷 플랫폼에서 광범위하게 수집하는 사용자의 개인 정보, 활동 패턴 등의 데이터를 많은 기업들이 데이터를 저장, 분석하여 마케팅에 사용하고 있다. 그런데 수집되는 데이터가 늘어날수록 사용자의 동의를 받더라도 데이터가 제3자의 손에 넘어가서 정치적, 상업적 목적으로 남용되는 경우도 나타나고 있다. 5천만명의 페이스북 사용자가 데이터가 캠브리지 애널리티카(Cambridge Analytica)라는 영국 데이터 분석업체에 넘어간 사건이 대표적이다.</p> <p>이러한 상황은 걱정된 디지털 데이터의 활용 범위와 프라이버시 보호에 대한 우려를 던져주고 있습니다. 국내의 경우 '비식별화'된 데이터를 사용할 수 있도록 비식별 조치 가이드라인이 실행 중이다. 한편 2018년 5월부터 발효된 유럽연합의 개인정보규제(GDPR)는 우리나라 기업들도 간접적으로 그 적용 대상이어서 위반 행위의 유형이 무엇인가에 대한 관심이 커지고 있다.</p> <p>이러한 배경에서 디지털 데이터의 합법적인 활용과 사용자 프라이버시 보호의 균형을 논해보는 기회를 가져보려 한다.</p>
요약내용	<p>소셜 네트워크의 등장으로 개인의 데이터는 이전보다 훨씬 방대하게 수집되고 있다. 데이터가 더 많이 수집될수록 정보주체의 동의 없이 데이터가 제 3자에게 전달되는 프라이버시 침해 사례 또한 증가하고 있다. 그렇다면 과연 제 3자가 수집한 데이터는 제한적으로 사용되고 있을까? 이 문제에 대해서는 제 3자의 데이터 사용에 대한 적절한 심사 체계가 존재하지 않아 정보주체의 권리가 침해된다는 의견과 제 3자의 데이터 사용에 있어서 로그인 이상의 개인정보 제공은 이용자에게 선택권 부여하므로 침해하지 않는다는 대립된 의견이 제시되었다.</p> <p>개인정보 프라이버시 침해를 막기 위한 방안, 다시 말해 데이터 거버넌스의 방안에 대한 논의는 크게 세 가지 측면으로 이루어졌다. 첫째는 법을 통한 규제이다. 법을 통한 규제에 관해서는 최초로 데이터를 수집할 때, 명확한 기준이 담긴 동의를 받아야 한다는 의견이 제시되었다. 이 때 정보주체에게 동의의 내용을 알기 쉽게 해 진정한 동의를 이끌어 낼 수 있도록 해야 한다는 점이 강조되었다. 또한 '데이터 이동성'을 골자로 기업의 무분별한 데</p>

	<p>이더 사용을 규제하기 위해 유럽에서 시행 중인 GDPR에 대한 논의도 이루어졌다. 논의는 GDPR의 데이터 이동성을 국내에 도입할 때의 효과를 중심으로 진행되었다. 패널들은 애초에 기업 간 데이터가 상호 호환되지 않고 있다는 점, 만약 데이터 이동권이 국내에 도입된다 하더라도 가공된 정보는 예외라는 점, 그리고 플랫폼의 영향력이 강력한 상황에서 이용자들이 비슷한 서비스를 이용한다는 점에서 데이터 이동권 도입이 과연 개인정보 관리에 대한 개인의 주체성을 향상시킬지 의문이라는 회의적인 입장을 표했다.</p> <p>프라이버시 보호를 위한 두 번째 방안은 플랫폼의 설계 단계부터 프라이버시 보호를 내재화 하는 것이다. 이에 대해서는 ‘가명화조치’와 코딩을 할 때부터 식별성이 드러나지 않도록 코딩하는 ‘secure coding의 제도화’ 등이 제시되었다.</p> <p>프라이버시 보호를 위한 마지막 방안은 바로 기업 간 경쟁을 촉진하는 것이다. 정부의 인증을 바탕으로 소비자가 기업을 선택하게 해 기업이 자발적으로 프라이버시 보호를 위해 노력하게 해야 한다는 내용이 중심이 되었다.</p>
<p style="writing-mode: vertical-rl; text-orientation: upright;">논의 세부 내용</p>	<p><b>I. 소셜 네트워크와 개인 프라이버시</b></p> <p><b>1. 개인 프라이버시를 침해하는 소셜 네트워크 기업(최은창 발제자)</b></p> <p>1) 소셜 네트워크가 발전할수록 늘어나는 개인 데이터 수집</p> <ul style="list-style-type: none"> <li>- 2004년부터 소셜 미디어는 이용자도 모르게 많은 메타 데이터를 수집하고 있음</li> <li>- 디지털 풋프린트: 무심코 클릭한 모든 것들이 데이터로 생성</li> <li>- 핸드폰, 소셜 네트워크 플랫폼에서 데이터 가장 많이 수집됨</li> <li>- 수집된 데이터는 마케팅에 이용되며, 기업이 원하는 상품/모델을 현실화시키는 데 도움이 됨</li> </ul> <p>2) 보호되지 않는 개인 프라이버시</p> <ul style="list-style-type: none"> <li>- 캠브리지 애널리틱스의 이용자 데이터 유출 사건: ‘디스이즈유어디지털라이프’라는 Facebook에 설치된 성격퀴즈 앱으로부터 수집된 데이터를 캠브리지 애널리틱스라는 정치 광고 기업이 구매. 수집된 데이터를 트럼프 당선에 이용. 이 때 성격퀴즈 앱을 통해 설문조사에 응했던 사람은 약 27만 명이었지만, 실제로는 Facebook 이용자의 친구정보 등을 통해 5,000만 명의 데이터를 수집</li> <li>- Facebook 이용자 데이터가 앱을 통해 수집되어 제 3자에게 전달되며, 이용자의 동의 없이 다른 목적으로 사용될 수 있다는 점에서 충격을 안겨 주었음</li> </ul> <p>3) 데이터 이동 수단: Graph API와 소셜 로그인</p> <ul style="list-style-type: none"> <li>- Graph API는 Facebook의 다양한 정보를 나타내는 ‘소셜 그래프’를 읽고 쓰는 기본 수단이며, Facebook 플랫폼에서 데이터를 가져오고 내보내는 기본 방법임</li> <li>- 앱에는 수많은 Graph API가 포함되어 있지만, Facebook은 앱 개발자가 Graph API 사용에 대해 허락 말지 않도록 함</li> <li>- 소셜 로그인에 Graph API가 포함되어 있어, 소셜 로그인은 데이터의 이동을 위한 주요 통로라고 볼 수 있음</li> </ul> <p>4) 데이터 주체의 권리 보호를 위한 ‘데이터 거버넌스’</p> <ul style="list-style-type: none"> <li>- 누가 데이터에 접근할 권한을 가지고 있는가에 대한 문제</li> </ul>

- 규제의 부재로 합법적 데이터 사용의 경계가 모호한 미국  
: 미국 연방법에는 프라이버시 법이 약해 사실상 데이터 사용 범위를 기업의 가이드라인에 맡기고 있는 실정임
- GDPR을 통해 규제를 강화한 유럽(5월부터 GDPR 시행 중)
  - > GDPR은 EU 거주자의 개인정보를 다루는 모든 기업이나 단체가 프라이버시 보호와 관련된 광범위한 규정들을 준수하도록 강제하는 것을 골자로 함
  - > GDPR 프레임워크는 이용자들에게 데이터에 대한 더 많은 통제권을 부여함으로써 이용자들에게 더 많은 권리 부여
  - > GDPR 제 20조, 데이터 이동권에 따르면 이용자는 이용 중인 서비스에서 자신의 개인 데이터를 다른 서비스로 이동시킬 수 있음 --> 온라인 플랫폼(기업)에 불리
  - > 유럽에 진출해 있는 한국 기업들로 인해 한국은 GDPR의 간접적 영향권에 속함
- 한국은 개인정보 보호 규제에 관한 법이 있지만, 집행이 잘 이루어지지 않고 있음

## 2. 소셜 로그인이 야기하는 문제와 소셜 네트워크 사업자의 책임의식(정영훈 패널)

### 1) 소셜 로그인이 야기하는 문제

- 대표적인 앱마켓의 앱의 50% 정도는 소셜 로그인이 제공되고 있을 정도로 현재 소셜 로그인이 보편화 되어 있음
- 소셜 로그인을 통해 제공되는 정보 또한 예상 외로 많음
- 그러나 소셜 로그인에 대한 대중의 인식은 많이 부족함

### 2) 소셜 네트워크 사업자의 책임의식

- 소셜 네트워크 사업자들에게 데이터 사용에 대한 책임을 부과해야 함
- 책임을 부과하기 위해서는 데이터와 사업자의 이익 관계에 대해 먼저 판단해야 함. 사업자들은 앱을 통한 상거래, 행위들에 대한 정보 등 이용자의 데이터를 통해 수익이 생길 수밖에 없는 구조임. 따라서 소셜 네트워크 사업자들에게 책임을 부과해야 함.
- 소셜 네트워크 사업자가 사실상 소비자의 개인정보 제공 범위를 조절하는 것이 합당한가에 대한 논의도 필요함. 현행 소셜 로그인 방식은 '필수 제공 정보', '선택 제공 정보'를 사업자들이 선택해 동의를 받는 구조이며 소비자는 서비스를 이용하기 위해 동의할 수밖에 없는 구조임

## 3. 소셜 로그인에 관한 오해와 GDPR의 이면(이재림 패널)

### 1) 소셜 로그인에 관한 오해

- 언론은 캠브리지 애널래티카 사건의 원인을 소셜 로그인이라고 보도하며 네이버, 카카오의 소셜로그인에 대한 문제 제기함
- 그러나 캠브리지 애널래티카 사건의 원인은 엄밀히 말하자면 '소셜 로그인'이 문제가 아닌 'Graph API'가 문제되는 사건임
- Graph API로 Facebook 특정 이용자의 '친구정보'까지 받아올 수 있던 시절이 있어 지나치게 많은 정보가 제 3자인 개발자에게 제공된 것이지, 소셜 로그인과는 상관없음
- 소셜 로그인은 제공되는 정보가 매우 제한적이며 이용자 정보만 제공되지 친구 정보

까지 제공되지 않음.

- 이용자의 편리를 위해 소셜 로그인 사용하는 부분도 큼
  - > 새로 회원가입 해야하는 불편함 방지
  - > 이용자의 안전한 인터넷 이용 위한 지원
    - : 작은 업체의 경우, 보안인력이 불충분해 개인정보 관리에 대한 어려움을 겪고 있음. 또한 작은 사이트의 보안을 뚫어 네이버, 카카오에 일일이 정보를 대입해 네이버, 카카오 등 대형 업체의 개인 정보 취득하는 경우 많음. 소셜 로그인은 이를 방지.

#### 2) 이용자 동의를 기반으로 한 정보제공에 대한 의문

- 이용자의 동의를 기반으로 한 정보제공이 과연 소비자를 위한 것일까?
- GDPR에서도 이용자동의를 여러 적법 처리 중 하나일 뿐. 이용자동의를 가장 후순위로 검토되고 있음.

#### 3) GDPR의 이면

- GDPR은 순수하게 소비자를 위한 목적만 갖고 있지 않음
- 미국 테크노 기업에 대한 유럽인들의 거부로 유럽 자국 검색엔진을 위한 프로젝트 시행하고자 했지만, 2008 경제위기로 좌초.
- 이에 대한 대안으로 '데이터 이동성'을 골자로 한 GDPR 제시.
- 그러나 GDPR 시행 이후, 규제를 준수할 수 있는 충분한 자원이 있는 Google, Facebook이 더 유리해짐.
- 작은 회사들은 규제를 준수할 자원의 부족으로 오히려 더 피해 입음.
- 규제를 강화하는 것이 과연 대기업을 막을 수 있는 방법일까?

### 4. 개인정보 보호와 활용의 균형점(정명현 패널)

#### 1) 개인정보 보호와 활용의 균형점

- 개인정보는 보호되어야 하는 원칙을 갖고 있음
- 그러나 빅데이터의 중요성이 커지고 있는 현재, 빅데이터의 활용 또한 필요함
- 따라서 개인정보의 보호와 활용의 균형을 어느 정도로 할 것인지에 대한 논의와, 활용 시 안전장치를 어떠한 방식으로 갖출 것인지에 대한 논의 필요

#### 2) 개인정보에 관한 법: EU의 GDPR

- EU의 GDPR은 기본적으로 개인정보 보호를 위해 규제를 가하는 법이지만, 동시에 GDPR은 공익을 위한 문서보존 목적, 과학적/역사적 연구 목적, 통계적 목적을 위한 개인정보 처리에는 예외를 두고 있음
- GDPR은 디지털 시대에서의 활용에 초점을 맞추고 있어, E-프라이버시와 관련된 지침들을 함께 개정하고 있음
- 한국은 GDPR의 혁신적인 제도를 한국에 적합하게 받아들여야 함

#### 3) 원칙과 남용의 구분

- 원칙을 준수하게 하는 시스템 수립이 일차적 문제라면 시스템 이행은 이차적 문제임
- 원칙과 남용의 문제를 구별해야 함

- 이를 개인정보에 적용시키자면, 개인정보 거래와 개인정보 유출은 구분되어야 함
- 캠브리지 애널리티카 사례는 정보 수집과정에서 개인의 제대로 된 동의를 받지 않은 개인정보 유출의 사례임.

## 5. GDPR의 한계(윤재석 패널)

### 1) GDPR의 목적

- GDPR의 데이터 이동권은 미국 다국적기업의 지배력을 줄이고 유럽지역의 자생적 기업을 활성화하기 위한 나름의 이면의 목적을 갖고 만든 규정.
- 그러나 오히려 플랫폼이 막강한 구글 등에서 더 서비스를 잘 제공하고 있어 소비자에게 신뢰를 더 주고 있음.
- 따라서 애초의 구상과는 다르게 작동하고 있음

### 2) GDPR의 한계

- 현재 정보주체의 권리권한 확보를 위한 GDPR의 집행력은 실질적으로 부족한 상태로 아직까지 처벌한 사례 없음
- 데이터 이동권을 확보하기 위한 집행력 뿐만 아니라 정책적, 기술적 이행방법도 명확하지 않음
- GDPR에서 제시된 정보주체의 권리 보장이 실질적으로 담보될 수 있을지에 대한 의문 존재. 이용자의 동의만으로 정보를 제공하면 안되며, 동의는 예외적인 차원에서 제공될 수 있도록 해야 함.

## II. 데이터 거버넌스에 관한 패널 간 토론

### 1. 소셜 네트워크를 통해 수집된 데이터가 제한적으로 사용되고 있는 것인가?

#### (정영훈 패널)

- 앱을 사용하기 위해서 이용자는 정보 수집에 동의할 수밖에 없음.
- 그러나 필수정보와 선택정보의 범위를 사업자가 정함. 정보 수집 범위가 사업자에게 전적으로 맡겨져 있음
- 또한 정보 필요성에 대한 사업자의 판단 근거도 부재하므로 문제의 소지가 있음.
- 소셜 로그인인 경우에도, 미디어업체들이 소셜 로그인을 오픈할 때 서드파티에게 필요한 정보 심사 체계가 존재하지 않음.

#### (이재림 패널)

- 현재 필수로 제공하는 것은 로그인을 할 수 있는 토큰값, 식별자 정도임
- 네이버의 아이디, 패스워드가 외부에 제공되지 않으며 로그인 시켜주는 기능만 제공 그 이상의 개인정보 제공은 이용자에게 선택권 부여
- 개인 정보 문제를 규제로만 대응하기 보다는 기업들의 경쟁을 촉진시키는 것도 하나의 방법임. 소비자들은 개인정보 보호를 강점으로 내세우는 기업을 이용할 것이므로

로 기업 간 경쟁이 촉발될 것이며, 이는 결과적으로 더 나은 데이터 거버넌스를 수립할 수 있도록 할 것임.

**(최은창 발제자)**

- 기술 플랫폼 기업들이 기술적 디자인, 설계 단계에서부터 개인정보가 보호되도록 설계 해야 함

**2. 제 3자가 다른 용도로 수집한 데이터를 사용할 때 통제방안은?**

**(정명현 패널)**

- 최초로 데이터를 수집할 때, 명확한 기준이 담긴 동의를 받아야 함.
- 제 3자에게 정보를 제공할 때, 제 3자 제공에 대한 동의를 받지 않고 개인정보를 이전하는 것은 규범을 위반하는 것임.
- 비식별화 조치, 공익의 목적, 연구의 목적 등 예외적으로 가능한 경우들이 있지만 캠프리지 애널리틱스의 경우 상업적 목적으로 이용했으므로 규범 위반임.

**(윤재석 패널)**

- 캠프리지 애널리틱스의 경우 법률 위반 사례가 맞음. 그러나 문제는 위반 사실을 쉽게 파악할 수 없다는 점임. 특히 Facebook과 같은 다국적기업의 경우 파악하기 더 어려워, 국내기업의 역차별 이슈로 대두되기도 함.

**3. 데이터 이동권이 국내에도 도입된다면, 이용자의 자기 정보 통제권은 더 잘 보장될까요?**

**(윤재석 패널)**

- 데이터 이동권이 국내에 도입이 이용자의 자기 정보 통제권 강화로 이어진다는 것에 대해서 회의적임.
- 데이터 이동권에서 사업자가 이용자가 제공한 정보를 통해 가공한 정보(ex. 익명정보, 가명화 된 정보, 업체에서 통계목적용 통해 활용한 정보 등)는 예외 사항임. 따라서 제공된 정보가 남아 활용될 가능성 존재.
- 현재와 같이 플랫폼의 영향력이 강력한 상황에서 이용자들은 비슷한 서비스 이용할 것임. 이러한 상황에서 데이터 이동권이 도입이 과연 개인정보 권리에 대한 개인의 주체성이 향상할 지에 대한 의문.
- 국회 차원에서도 법률적으로 아직 데이터 이동권 도입하려는 움직임 부재

**(최은창 발제자)**

- 익명화된 데이터의 소유권은 누구에게 있는가에 대한 문제
- 아직 법적으로 클라우드 데이터에 알맞은 균형점 존재하지 않음

**4. 한국의 데이터 시장 성장에 데이터 이동권이 유용하게 사용될 수 있을까?**

**(이재림 패널)**

- 현재 상태로는 데이터 이동권과 개인정보 열람권이 다를 것이 없음.
- 개인정보를 열람에서 다운로드해서 타 기업에 이전할 수 있도록 하는 것이 데이터 이동권
- 이를 위해서는 양쪽의 데이터가 호환가능하게 개발되었어야 했지만 현재 시스템상 호환불가능

- 데이터 이동권은 현실적으로 개인정보자기열람권과 유사한 제도
- 따라서 데이터 이동권을 통해 효과를 보기에 어렵다고 생각

**5. 플랫폼 설계 단계부터 프라이버시 보호를 기본적으로 내재화 하는 방안은?**

**(윤재석 패널)**

- 가명화조치
  - : 가명정보는 여러 통계, 과학적 목적으로 활용 가능. 동시에 가명화를 통해 개인정보 유출, 피해 가능성을 예방할 수 있음
- Secure coding
  - : 코딩을 할 때 애초에 식별성이 드러나지 않도록 코딩하는 것.
  - : 이를 제도화 한다면 프라이버시를 기본적으로 내재화 할 수 있을 것이라고 생각

**6. 데이터 이동권 보장에 의한 프라이버시 패러독스 현상?**

**(최은창 발제자)**

- 프라이버시 패러독스란 개인정보에 관련해 이용자에게 더 많은 권리를 줄수록 이용자들이 오히려 더 쉽게 개인정보 제공하는 현상.
- 단순히 이용자들에게 모든 권리를 부여하면 오히려 개인정보 더 확산될 수 있음

**(이재림 패널)**

- 개인정보 보호를 잘 지키는 기업들을 정부가 인정해 소비자가 기업을 선택하는 방향으로 나아가야 함.
- 이 때 정보보호 등급제 등의 인증제도가 활용될 수 있음

**(정명현 패널)**

- 동의에 기반한 개인정보 처리가 기업 입장에서는 리스크를 줄이는 방법 중 하나일 수 있지만, 정보 주체의 동의가 진정한 동의라고 볼 수 있는지 의문임.
- 많은 정보주체들이 개인정보 제공에 동의를 할 때 동의내용에 대해 충분한 검토 하지 않음
- 동의는 정보주체의 의사표현을 기반으로 하므로, 동의 기반 계약에서 '의지'가 가장 중요하게 여겨짐. 따라서 정보주체가 진정한 동의라고 인정하지 않는다면, 기업 입장에서 대응하기 어려울 수 있음
- 또한 정보주체에게 동의의 내용(고지되는 내용)을 알기 쉽게 해 진정한 동의를 이끌어 낼 수 있도록 해야 하지만 현재의 동의는 그렇지 않음

**(이재림 패널)**

- 개인정보 동의가 기업 입장에서는 가장 편리한 방법임.
- 그러나 과연 개인정보 동의가 과연 바람직한 것인가?에 대한 기업의 인식 제고 필요

**III. 플로어**

**(참석자 1: 이동만 카이스트 교수)**

- 공개된 데이터들의 개인정보 보호 중요한 이슈.
- 그러나 규제로 인해 데이터 접근권한이 점점 줄어들어, 공공의 이익과 학문의 발전을 위해 쓸 수 있는 데이터 점점 줄어들
- 공익을 목적으로 한 데이터 사용에 대해서 어떻게 생각?

**(윤재석 패널)**

- 개인정보 활용과 보호에 대한 사회적 합의를 찾는 것이 중요.
- 가명정보가 빅데이터, 즉 4차산업혁명의 핵심 요소임.
- GDPR의 가명정보가 어디까지 활용가능한지에 관한 문제  
:GDPR에 따르면 과학적인 연구목적, 통계목적을 위한 가명정보 활용 가능하지만 상업적, 마케팅적 목적에 대한 가명정보 활용은 명시적으로 언급 되어있지 않음.

**(이동만 카이스트 교수)**

- 데이터 보호는 오히려 데이터를 상업화하려는 사람들의 권력을 더 높이는 계기가 될 수 있다는 맹점 존재
- 데이터 보호가 데이터 가진 사람들의 가치를 올리는데 일조할 수 있음

**(최은창 발제자)**

- 데이터를 가장 많이 보유하고 있는 주체는 정부
- 정부가 데이터를 공개하고 싶어도 법의 규제로 인해 공개할 수 없음
- 그 대안으로 정부가 내세운 것이 '익명조치 가이드라인'
- 그러나 가명화된 데이터를 몇 가지만 조합하면 누구인지 파악할 수 있다는 점이 문제

**(참석자 2)**

- 익명화된 정보를 자유롭게 사용해도 되는 것인지 여부. 익명화된 정보가 축적되다 보면 개인정보권리를 침해할 수 있지 않나?

**(윤재석 패널)**

- '해당 시점', 즉 현재의 기술발전 수준에서 식별할 수 있으면 가명화된 정보, 식별할 수 없으면 익명화된 정보임