정보주체의 개인정보 통제권 강화를 위한 개인정보보호법 쿠키 동의 개정안

전주현* 이경현**

*부경대학교 대학원 정보보호협동과정

**부경대학교 IT융합응용공학과

A Proposal for Amended Cookie Consent of Personal Information Protection Act to Strengthen Data Subjects' Right to Control Personal Information

Ju-Hyun Jeon* Kyung-Hyune Rhee**

* Interdisciplinary Program of Information Security, The Graduate School, Pukyong National University

* Department of IT Convergence & Application Engineering, Pukyong National University

요 약

현재 개인정보처리방침에 공개된 쿠키 설정은 텍스트적인 공개로 실제 정보주체의 개인정보 자기결정권에 영향을 주기는 어렵다. 이는 개인정보처리자보다 정보주체에게 책임을 전가하는 형태로 명시되고 있으며 보다 구체적이고 명확한 기술적 구현을 통해 정보주체가 쉽게 개인정보자기결정권을 행사 가능 하도록 개선해야 한다. 본 논문에서는 해외 쿠키 정책을 비교 분석해 웹 사이트 접속 시 브라우저상에서 사용자가 직접 통제 가능한 기술적 개선을 통해 개인정보처리자의 책임을 부각시키고 정보주체가 직관적으로 개인정보처리 접근성에 대한 선택권을 부여하여 개인정보 보호를 강화하는 기술적 구현을 GDPR과 비교 분석해 제안하였다..

키워드 개인정보, GDPR, 개인정보처리방침, 쿠키 동의, 브라우저

I.서론

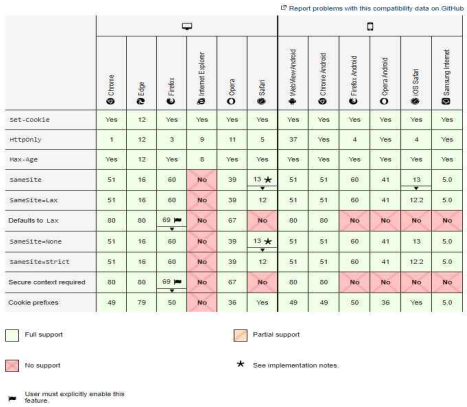
지난 2020년 2월 크롬, 엣지, 파이어폭스 등 사용자가 많은 브라우저에 교차사이트와 동일 사이트 쿠키에 대한 정책이 변경 되었다. 웹 브라우징의 개인정보보호 및 보안을 개선하기 위한 노력이 지속되고 있다. 현재 개인정보처리방침에 따라 공개된 쿠키 설정에 대한 고지사항이 있지만 사용자에게 단순 정보공개에 의존한 텍스트상의 내용에 불과해 실질적 정보주체 보안에 영향을 주는지는 의문이다. 본 논문에서는 개인정보처리방침에 공개하는 쿠키 정책을 보다 정보주체 친화적이고 기술적 구현을 통해 해외 사례와 개인정보 추적 기술에 대응하는 정보주체 권리 대한 기술적 연구를 국내 개인정보보호법과 유럽의 GDPR(General Data Protection Regulation)을 비교 분석해 보았다.

II. 브라우저 쿠키 정책

프랑스의 개인정보보호 기구가 사용자 동의 없이 '쿠키'를 설치해 광고에 활용한 구글과 아마존에 각각 1억유로(약1천317억원), 3천500만 유로(약461억원)의 과징금을 부과했다[1].

사용자가 많은 엣지, 크롬, 모질라, 오페라 브라우저 등 최근 브라우저에서 쿠기관련 보안을 강화하고 있는 흐름을 <그림-1>에서 보이고 있다.

<그림-1> 브라우저 적합성 메트릭스



2.1 교차사이트와 동일사이트 쿠키

웹 사이트는 일반적으로 개인화된 광고, 추천, 위젯, SNS 삽입 등 외부 기능을 통합하고 있으며 웹을 탐색할 때 외부 서비스는 사용자 브라우저에 쿠키를 저장한 후 개인화된 서비스를 제공하거나 행태(behavior) 측정이 가능하다. 모든 쿠키는 연결된 도메인이 있으며 사용자가 사용하는 웹사이트 도메인과 연결되지 않은 외부 서비스와 일치하는 경우 '교차사이트' 또는 '제3자 사이트'라고 한다.

반면에 동일한 사이트에서 쿠키 액세스는 쿠키 도메인이 사용자 주소 표시줄의 도메인과 일치하는 경우 '동일 사이트'로 인식하고 개별 웹 사이트에 로그인한 상태를 유지하고 개인행태 분석을 지원한다[2].

2.2 사이트간 위조공격(CSRF)

OWASP TOP 10에 빠지지 않고 웹 공격기법으로 언급되고 있는 사이트간 교차 공격에 대한 사항으로 이는 쿠키를 이용한 웹 공격의 대표적인 공격기법이다. 공격자가 웹 응용 프로그램의 출력에 스크립트를 삽입하여 브라우저가 페이지의 일부라고 판단하여 스크립트가 실행되게 하는 공격이다[3]. 즉 공격자는 스크립트가 실행 가능한 링크를 타켓에게 보내 클릭하게 함으로써 피해자의 웹 브라우저에서 쿠키, 세션, 사용자 자격증명 등을 악용하는 공격이다. 사용자가 사이트에서 인증이 되면 사이트는 합법적인 요청과 위조된 요청을 구분하기 어렵다.

2.3 개인정보처리방침 및 공개방법

개인정보보호법 제30조에 따르면 개인정보처리방침을 수립·공개 하도록 되어있다. 동법 제30조제1항7호에는 '인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)'을 공개하도록 법률에 명시하고 있으며 실제 대부분의 사이트에서 공개된 개인정보처리방침 현황을 살펴보면 정보주체에게 브라우저상에서 각 개인이 설정하도록 안내만 되어있다. 즉, 브라우저에서 설정을 하지 않은 사용자의 경우 쿠키를 통한 각 개인의 행태정보 등이 모두 수집 가능하다고 해석이 되어 정보주체에게 불리하게 포괄적 규정만 명시해 놓은 상황이다.

III. GDPR에서 요구하는 쿠키 정책

GDPR에서는 사이트 이용의 경우 이용자의 동의를 구할 때 다음 사항이 반드시 포함되어야 한다[6].

- 정보수집하는 기업과 파트너사의 구체적이고 명확한 정보를 제공해야 한다.
- 개인정보 수집의 목적을 구체적이고 명확하게 밝혀야 한다.
- 언제든지 동의를 철회할 권리 등에 관한 구체적인 정보를 제공해야 한다.
- 동의란 정보주체의 진술 또는 적극적인 행위로 이루어져야 하며 모호하지 않아야 한다. (자동체크 안됨)
- 동의 거부에 대한 불이익이 없어야 하며 이용약관으로부터 동의를 분리해야 한다.
- 복수의 목적과 다른 유형의 처리에 대해서는 개별적으로 동의하는 세부 옵션을 제공해야 한다.

실제로 GDPR은 IP주소, MAC주소, 온라인 쿠키 등을 통해 정보주체 식별이 가능한 경우에는 해당 정보를 개인정보로 간주하고 있다[4].

3.1 EU e-privacy Directive

2002년에 제정된 EU e-privacy Directive가 2009년에 개정되어 '인터넷 쿠키를 이용자 PC에 저장하기 위해서는 해당 이용자의 명시적인 동의(explicit consent)를 구해야 한다'는 내용이 포함되었다. 2년의 유예기간을 거쳐 2011년5월 26일부터 시행 되었으며 '쿠키법'이라고도 불린다. 2011년5월 이전에는 현재 국내 개인정보보호법 제30조 개인정보처리방침에서 명시하듯이 개괄적으로 웹사이트에 게재하는 것을 법률적 요구사항으로 하였으나 2011년5월 이후부터는 쿠키 관련해 명시적인 동의를 받고 있다[5].

3.2 EU GDPR 시행에 따른 쿠키정책

GDPR 시행 이전 쿠키는 e-privacy 법령에 따라 통신전송의 목적에 따라 사용했으나 쿠키 적용에 동의가 요구되지는 않았다. 하지만 GDPR 시행 이후에는 쿠키 식별값도 개인정보의 한 종류이기 때문에 처리를 위해 적법한 근거가 필요하였다. 대표적인 방법으로 쿠키에 대한 '동의'를 사용하고 있다.

3.3 개인정보보호법 동의철회

개인정보보호법 제39조의7에 '정보통신서비스제공자 등은 제1항에 따른 동의철회, 법 35조에 따른 개인정보 열람, 법 제36조에 따른 정정을 요구하는 방법을 개인정보의 수집 방법보다 쉽게 하여야 한다'고 명시하고 있다. 이는 정보통신서비스제공을 하는 이용자로 한정되어 있어 특례조항으로 규정하고 있다. 실제 한번 동의한 사항은 다시 철회나 정정을 요구하는 절차가 복잡해 정보주체가 적극적으로 개인정보 자기결정권을 행사하기 위한 기술적 방법이 제시되어야 한다.

IV. 개인정보보호법 개정 제안

4.1 개인정보 보호법 개정

본 논문에서는 개인정보보호법 제35조 개인정보처리방침 개정을 제안한다. 개인정보처리방침 공개시에 쿠키정책에 대한 조항을 개정해 사이트를 방문 시에는 의무적으로 '쿠키 동의'를 얻도록 한다. 개인정보처리방침 제1항제7호에 명시되어 있는 자동접속기술에 대한 사항을 이용자에게 브라우저 설정 정도로만 안내하는 것이 아닌 이용자나 정보주체가 직접 관련 조항에 대한 사항을 선택적으로 사용 가능하게 옵션을 제공하도록 다음 <표 1>과 같이 법 개정을 제안한다.

<표 1> 개정 제안안

현 행	개 정 안
제30조(개인정보처리방침의 수립 및 공개) ①항	제30조(개인정보처리방침의 수립 및 공개) ①항
7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)	7.---------- ---------- ---------- ---------- ---------- ---------- -에 대해 동의 방법을 알려야 한다. (해당하는 경우에만 정한다)

4.2 쿠키 동의 기술적 제안

해외 사례에서도 보면 "당신의 향상된 서비스를 위해 쿠키를 수집하고 있습니다. 웹 사이트를 계속 이용하려면 쿠키에 동의한 것으로 간주 하겠습니다." 라는 알림 팝업을 보게 된다. 이는 유럽의 GDPR 시행 이후 모두 불법이다. 정보주체의 적극적인 행위의 동의가 이루어지지 않았기 때문이다. 국내 현행법 하에서는 정보주체의 쿠키 동의에 대한 적극적 행위가 제도적으로 반영돼 있지 않다.

본 논문에서 정보주체(정보통신서비스는 이용자)가 적극적인 개인정보처리에 따른 쿠키 동의에 대한 방법을 제안한다.

<그림-2>와 <그림-3>에서처럼 이용자가 웹사이트에 방문하면 자동으로 수집하는 개인정보 장치 설치·운영에 대한 동의를 받도록 한다. 메뉴는 4가지로 구성을 한다. 첫 번째는 모든 쿠키에 대해 동의한다. 두 번째는 현재 방문하고 있는 동일 사이트에만 허용한다. 세 번째는 접속 사이트 서비스 이용에 직접적인 저장과 접근에만 쿠키를 허용하고 나머지는 거부한다. 네 번째는 모든 쿠키에 대해 거부한다.

<그림-2> 쿠키동의 제안모델

<그림-3> 쿠키 옵션별 제안모델

기본값은 '동일 사이트 쿠키허용'과 '거부(OFF)'로 되어 있어 사이트를 접속하고 이용하려면 정보주체의 명시적이고 적극적인 행위를 하도록 제안한다. 두 번째와 세 번째 차이점은 두 번째는 일상적인 사이트 이용자의 행태분석까지 가능한 허용범위를 나타내고 세 번째는 사이트 이용함에 있어 가장 기본적인 쿠키 기술에 대한 접근과 저장을 의미하며 성향이나 행태분석은 거부하는 옵션이다.

V. 결론 및 향후 방향

데이터 3법 개정 이후 국내 개인정보에 대한 법 제도는 규제 중심에서 활용도를 높이도록 완화되었다. GDPR시행은 이런 측면에서 동의 만능주의에 있는 국내 개인정보보호 관련 법률에 참고 할 사항이 많다. 4차산업혁명 기술의 중심에 있는 인공지능과 빅데이터 기술을 제대로 활용하려면 자동화된 기술의 개인정보처리 과정에서 침해하는 행위가 있어서는 안된다. 최근 언론에서 이슈화된 인공지능 데이터 관련 문제도 정보주체의 명시적인 동의 없이 사용했다는 점에서 많은 시사점을 보여주고 있다. 본 논문에서 제안하고 있는 자동화 기술 설치 운영에 따른 '쿠키 동의'에 대한 법률 개정 제안과 구현 기술은 향후 인공지능, 빅데이터 활용에 정보주체(이용자)의 적극적인 행위로 동의를 반영한 컴플라이언스 리스크를 해소하는데 기여할 것으로 기대한다. 또한, 향후 동의 철회나 3자 제공에 대한 정보주체의 철회를 개선하는 제도적·기술적 연구를 지속할 예정이다.

[참고문헌]

[1] 프랑스 당국 '동의없는 쿠키광고' 구글에 1천317억원 과징금, 연합뉴스. 2020.12.10

[2] 접근제어를 이용한 교차 사이트 스크립트 필터링, 202 한국정보과학회 봄 학술집. vol29. no1

[3]https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

[4] 한국인터넷진흥원, 2020년 GDPR상담사례집

[5] Bond Robert, The EU E-Privacy Directive and Consent to Cookies, The Business Lawyer. 68(1):215-223. 2012

[6] 행정자치부, 우리기업을 위한 GDPR안내서, PIWIK.pro. 영국감독기구 동의 가이드라인