2024 Vol. 7

PRIVACY REPORT

2024 개인정보 이슈
심층 분석 보고서

플랫폼 기업

KISA 한국인터넷진흥원

PRIVACY REPORT

2024 개인정보 이슈 심층 분석 보고서

| CONTENTS |

2024 Vol. 7

플랫폼 기업

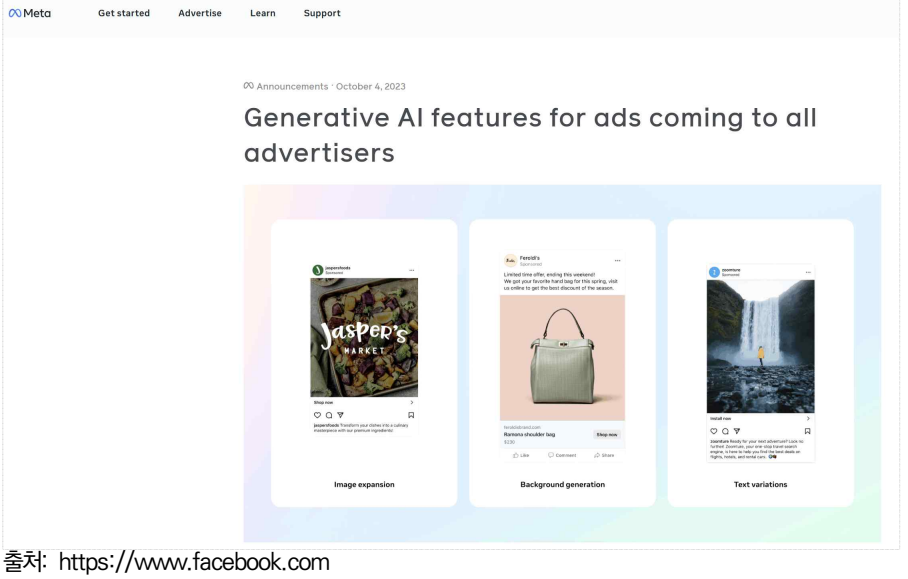
건강한 '맞춤형 광고' 생태계 조성을 향하여
: 맞춤형 광고 오남용 방지와 소비자 효용 제고

유승철
이화여자대학교 커뮤니케이션-미디어학부 교수

1. AI 시대의 소비자 맞춤형 광고

디지털 경제에서 맞춤형 광고는 소비자의 행동 데이터를 기반으로 한 개인화된 마케팅의 핵심 요소로 자리 잡았다. KOBACO(한국방송광고진흥공사)에서 발표하는 방송통신광고비조사에 따르면, 2023년 디지털 광고 시장 규모는 이미 9조 2,831억 원을 넘었으며 이 중 맞춤형 광고(Personalized Advertising)가 차지하는 비중은 60~70% 정도로 추정된다. 이처럼 맞춤형 광고가 디지털 광고의 대표주자가 되어가는 상황에서, 데이터 보호와 산업 성장을 조화시키기 위한 정책이 시급하다. 광고주에게는 높은 마케팅 효율성을, 소비자에게는 최적화된 경험을 제공하는 맞춤형 광고 모델은 동시에 '개인정보 보호와 프라이버시 침해'라는 근원적인 딜레마를 발생시키게 된다. 이런 맥락에서 맞춤형 광고는 소비자 권리와 상업적 자유 간의 상충 문제로 각국의 규제체계에 따라 다양한 접근방식을 통해 해결하려는 노력이 이루어지고 있다. 본고는 최근 맞춤형 광고에 대한 업계 동향을 살펴보고 유럽연합(EU), 미국, 일본, 중국의 맞춤형

그림 1 메타가 선보인 생성형AI활용 맞춤 광고 솔루션



출처: https://www.facebook.com

광고 규제를 종합적으로 비교 분석하며, 이러한 규제가 각국의 법적·경제적·사회적 맥락에서 어떠한 역할을 수행하는지 논의하려고 한다. 이를 통해 한국의 맞춤형 광고 규제 방향에 대한 시사점을 제시하려고 한다.

2. 맞춤형 광고의 소비자 개인정보 침해와 기업의 대응

맞춤형 광고는 사용자의 온라인 활동, 검색 기록, 위치 정보 등을 기반으로 광고 내용을 개인화하여 제공하는 광고 방식이다. 그러나 이러한 데이터의 수집과 사용 과정에서 필연적으로 프라이버시 침해 문제가 발생하게 된다. 예를 들어, 사용자가 동의하지 않은 상태에서 비식별화된 데이터를 활용해 개인을 식별할 수 있는 위험이 크다는 점이 우려로 지적된다. 구체적으로 온라인 클라우드 환경의 대중화는 다양한 보안 위협에 노출 가능성을 높이고 있다. 클라우드 환경에서 데이터는 중앙 서버에 저장되며, 이는 외부 공격자나 내부 관리자의 부정 접근에 의해 유출될 수 있는 위험이 커지고 있다. 특히 금융 및 의료 데이터와 같은 민감한 정보는 이러한 유출로 인해 심각한 피해를 초래할 수 있다.

클라우드 서비스 제공자의 보안 취약점도 문제로 지적된다. 클라우드 서비스 제공자는 다양한 고객의 데이터를 관리하고 있으며, 서비스 제공자의 보안 체계에 허점이 있을 경우 다수의 고객 데이터가 동시에 위협받을 수 있다. 이는 클라우드 사용자가 보안 통제를 완전히 할 수 없다는 점에서 더 큰 문제로 부각된다. 실제로 한 조사(infosecurity-magazine 실시)에 따르면 미국 기업 중 클라우드 데이터의 80% 이상을 암호화하는 기업은 10% 미만인 것으로 나타났다. 미국의 대형 통신사 T모바일의 경우 수차례 개인정보 유출 사고를 겪었는데, 2018년에는 230만 명의 고객 정보가 유출되었고, 2021년 8월에는 7,600만 명의 고객 정보가 대규모 사이버 공격으로 유출되었다. 이로 인해 2022년에는 3억 5천만 달러 규모의 집단소송 합의금을 지불했으며, 2024년에는 미국 연방통신위원회(FCC)로부터 3,150만 달러의 벌금을 부과받았다.

그림 2 T모바일 개인정보 누출 관련 논란을 다룬 뉴스

출처: https://audetlaw.com/archive/t-mobile-data-breach-lawsuit/

AI 기술의 발전은 빅데이터를 연료로 삼고 있다는 점에도 주목해야 한다. 더 많은 데이터는 더 정확한 AI 모델을 만들기 때문에, AI는 끊임없이 대량의 데이터를 수집하고 학습하는 것은 당연한 흐름이다. 그러나 이러한 데이터 중에는 소비자의 민감한 개인정보가 포함되어 있을 수 있으며 AI가 개인의 신원이나 행동 패턴을 추론하는 과정에서 새로운 개인정보가 '자동으로 도출'될 수 있는 위험도 커지고 있다. 이러한 상황에서 AI 기술의 혁신과 개인정보 보호 간의 균형을 맞추는 것이 심각한 주제로 부각되고 있다.

그림 3 유명인을 활용한 딥페이크 광고의 문제를 다룬 CNBC 뉴스

출처: https://www.youtube.com/watch?v=M5X1sHAX_rU

기업은 빅데이터를 활용하여 경쟁력을 강화하는 동시에, 개인정보 보호에 대한 책임을 져야 한다. 첫째, 데이터 최소화 원칙을 준수하여 필요한 최소한의 데이터만을 수집하고, 이를 명확한 목적 하에 활용해야 한다. 이는 불필요한 데이터 수집을 방지하고, 데이터 유출 시 피해를 최소화하는 데 기여한다. 다음으로 데이터 익명화 및 가명화 기술을 적용하여 개인을 식별할 수 없도록 조치해야 한다. 이러한 기술적 보호 조치는 데이터 분석 과정에서 개인정보의 노출을 방지하며, 법적 준수를 돕는다. 또한, 기업은 내부 데이터 관리 정책을 강화하고, 직원들에게 개인정보 보호 교육을 실시하여 데이터 처리 과정에서의 실수를 줄여야 한다. 이는 조직 내에서 개인정보 보호 문화를 정착시키는 데 중요한 역할을 한다. 실제로 애플(Apple)은 iOS 14.5 출시와 함께'앱 추적 투명성(App Tracking Transparency, ATT)' 기능을 도입해 앱 사용자 추적에 대한 명시적 동의를 요구했다. 이를 통해 사용자들은 앱별로 데이터 추적을 차단할 수 있으며, 이에 따라 페이스북 광고 효과가 줄어드는 등 큰 영향을 미친 바 있다. 이러한 개인정보 보호 정책 방향은 긍정적인 결과로 이어졌다. 2024년 기준 글로벌 사용자의 개인정보 추적 동의율이 50%까지 증가했는데(2021년 대비 10% 상승한 수치), 그 결과 iOS의 광고 매출은 28% 증가했다. 이는 개인정보 보호 정책이 소비자 신뢰도 향상과 기업의 수익성 제고로 이어질 수 있음을 보여주는 사례이다.

3. 맞춤형 광고와 개인정보 보호 기술의 도입

개인정보 보호 기술(Privacy-Preserving Technology)은 소비자의 데이터를 보호하면서도 데이터의 맞춤형 광고 효과성을 위해 적용되고 있는 기술을 말한다. 이 기술은 데이터 최소화(Data Minimization: 데이터를 필요한 범위 내에서만 수집하고 저장), 익명화(Anonymization)와 가명화(Pseudonymization: 데이터를 식별 가능한 개인과 분리하여 보호), 목적 제한(Purpose Limitation: 데이터 활용 목적을 명확히 규정하고, 목적 외 사용을 제한하는 것)에 기반한다. 최근 산업에 적용되고 있는 대표적인 개인정보 보호 기술은 아래와 같다.

(1) 연합학습(Federated Learning)

연합 학습은 데이터를 중앙 서버로 전송하지 않고, 각 디바이스에서 모델을 학습한 후 결과를 종합하는 분산형 학습 방식이다. 예를 들어, 구글의 Gboard는 사용자의 키보드 입력 데이터를 로컬에서 학습하여 개인 데이터를 외부로 전송하지 않고도 서비스를 개선한다.

(2) 차등 프라이버시(Differential Privacy)

차등 프라이버시는 데이터 세트에 통계적 노이즈를 추가하여 개인을 식별할 수 없도록 하는 기술이다. 이를 통해 광고주와 연구자는 데이터의 전체적인 패턴을 분석할 수 있지만, 개별 소비자의 프라이버시는 보호된다. 예를 들어, 애플은 차등 프라이버시를 활용하여 사용자 데이터를 익명화하면서 제품 개선에 활용하고 있다.

(3) 동형 암호화(Homomorphic Encryption)

동형 암호화는 데이터가 암호화된 상태에서도 연산이 가능하게 하여, 데이터 소유자가 아닌 제3자가 데이터를 활용할 수 있도록 한다. 이 기술은 특히 클라우드 기반 데이터 분석에서 유용하다.

개인정보 보호 기술은 소비자가 자신의 데이터가 안전하게 보호되고 있다는 확신을 갖게 하여 신뢰를 증진시키는 중요한 역할을 한다. 이는 소비자가 광고 콘텐츠를 긍정적으로 수용하게 만드는 주요 요소로 작용한다. 또한, 이러한 기술은 데이터 프라이버시를 보장하면서도 광고 타기팅의 정밀도를 유지하도록 돕는다. 차등 프라이버시와 연합 학습 기술의 도입은 광고주가 소비자의 데이터 패턴을 활용하여 개인화된 맞춤형 광고를 제공하는 데 매우 유용하다. 더 나아가, 글로벌 규제가 강화되는 상황에서 개인정보 보호 기술은 기업들이 규제를 준수하는 동시에 광고 전략을 유지할 수 있는 효율적인 해결책을 제공한다. 이를 통해 법적 비용과 운영 리스크를 줄이고, 보다 안정적인 광고 운영 환경을 조성할 수 있다.

4. 해외 관련 기관들의 맞춤형 광고 규제

(1) 유럽연합(GDPR): 개인정보 자기결정권 강화를 위한 강력한 규제

유럽연합의 GDPR(General Data Protection Regulation)은 전 세계적으로 가장 강력한 개인정보 보호 규제다. GDPR은 맞춤형 광고에서 개인정보 수집과 처리 시 명시적 동의(Explicit Consent)를 필수적으로 요구하며, 프라이버시권(Right to Privacy)과 개인정보 자기결정권(Information Self-Determination)을 보장하는 데 중점을 두고 있다(European Commission, 2024). GDPR의 핵심 법적 기반은 유럽연합 기본권 헌장(Charter of Fundamental Rights of the European Union)과 유럽인권협약(European Convention on Human Rights, ECHR)에서 비롯된 개인정보 보호의 헌법적 권리다. GDPR의 강력한 법적 보호는 소비자의 권리를 보장하는 동시에, 기업에게는 높은 행정 벌금(Administrative Fines) 부과라는 법적 억제력(Legal Deterrence)을 통해 엄격한 규제를 준수하게 만든다. GDPR은 유럽연합 외부의 기업들도 유럽 시민의 데이터를 처리할 경우 규제를 적용받게 하여, '글로벌 디지털 광고 산업'에 막대한 영향을 미치고 있다. 그러나 GDPR의 엄격한 규제로 인해 중소기업(Small and Medium Enterprises, SMEs)들은 준수 비용이 부담으로 작용하여, 맞춤형 광고 도입과 데이터 활용에 어려움을 겪고 있는 것도 사실이다. 이는 규제와 혁신 간의 균형을 모색해야 할 필요성을 시사한다. 2024년 8월 발효되고 2026년부터 전면 시행될 '유럽연합의 인공지능법(Ai Act)'과 함께 GDPR은 보다 광범위한 개인정보 보호를 위한 거버넌스 체계로 진화할 것으로 기대된다.

(2) 미국(CCPA): 상업적 표현의 자유와 개인정보 보호 간의 균형

미국의 CCPA(California Consumer Privacy Act)는 연방 차원이 아닌 주 차원에서 시행되는 대표적인 개인정보 보호법으로, 특히 제1조 수정헌법(First Amendment)의 보호를 받는 상업적 표현의 자유(Commercial Speech)와 개인정보 보호 간의 균형을 중시한다. CCPA는 GDPR과는 달리 명시적 동의(Explicit Consent)를 요구하지 않으나, 소비자가 원할 경우에는 데이터 판매를 차단할 수 있는 데이터 판매 금지권(Right to Opt-Out of Sale)을 제공한다. CCPA의 이러한 유연한 접근은 맞춤형 광고 산업에 상대적으로 자유를 부여하는 한편, 소비자 권리 보호에도 일조하고 있다고 평가할 수 있다. 하지만 주별로 규제가 상이하여, 연방 차원에서 통일된 법적 기준이 없는 점은 법적 복잡성을 증가시키며, 특히 다수의 주에서 사업을 영위하는 기업들에게 혼란을 야기하고 있다. 또한, 미국의 규제는 주별로 법적 기준이 다르기 때문에, 법적 혼란을 줄이기 위해 연방 차원의 통일된 규제 마련이 필요하다는 목소리가 높아지고 있다.

(3) 일본(APPI): 유연한 법적 접근과 상업적 자유 보호

2003년 최초 제정된 일본의APPI(Act on the Protection of Personal Information:

日本の個人情報保護法)는GDPR과 비교할 때 상대적으로 유연한 규제체계를 제공하며, 상업적 자율성(Commercial Autonomy)과 개인정보 보호 간의 균형을 중요하게 생각한다. APPI는 데이터 최소화 원칙(Data Minimization Principle)과 목적 제한 원칙(Purpose Limitation Principle)을 준수하지만, 익명화된 데이터(Anonymized Data)를 사용하는 경우, 맞춤형 광고에 더 많은 자유를 부여하고 있다. APPI는 특히 유럽연합과의 적합성 평가(Adequacy Decision)를 통해 일본 기업이 GDPR의 요구를 충족하는 동시에 유럽 시장에서 데이터를 자유롭게 활용할 수 있는 법적 기반을 마련하였다. 이는 일본이 글로벌 데이터 거래에서 경쟁력을 유지하는데 큰 도움이 되었다. 다만, APPI의 벌금이 상대적으로 낮고 규제 강도가 덜 엄격해, 규제가 충분한 법적 억제력을 발휘하지 못할 위험이 있다고 지적된다.

(4) 중국(PIPL): 국가 주권 강화와 엄격한 개인정보 보호

중국의 PIPL(Personal Information Protection Law)은 개인정보 보호와 관련하여 매우 강력한 법적 통제를 요구하며, 국가 안보(National Security)와 데이터 주권(Data Sovereignty)을 우선시한다. PIPL은 맞춤형 광고에서 사용자의 명시적 동의를 요구하며, 이를 위반할 경우 엄청난 행정 벌금(Administrative Fines)과 처벌이 부과된다. 중국의 법적 체계는 특히 국외 데이터 이전 제한(Restrictions on Cross-Border Data Transfers)을 강조하며, 이는 맞춤형 광고 산업에서의 글로벌 운영을 제한하는 요인으로 작용한다. PIPL은 국가가 데이터를 직접 통제할 수 있는 법적 수단을 제공하며, 데이터 주권과 공공질서를 보호하는 데 중점을 둔다(China Cybersecurity Administration, 2024). 이러한 접근은 데이터 보호를 강화하는 동시에, 광고주의 상업적 자유를 억제하고 국가 통제(State Control)를 강화하는 결과를 초래하고 있다.

5. 각국 맞춤형 광고 규제의 법적·경제적·사회적 함의

각국의 맞춤형 광고 규제를 종합적으로 분석해 보면, 소비자 보호(Consumer Protection)와 상업적 자유(Commercial Freedom) 간의 균형을 유지하는 것이 매우 중요함을 알 수 있다. 법적 접근의 차이는 각국의 사회적·경제적 상황과 헌법적 가치관에 따라 달라진다. 예를 들어, 유럽은 프라이버시권을 헌법적 권리로 인식하여 강력한 법적 보호를 강조하고, 중국은 국가 안보와 주권 강화에 초점을 맞춘다. 이러한 점에서 한국은 이러한 국제적 흐름을 반영하여, 비례성 원칙(Principle of Proportionality)과 법적 합리성(Legal Reasonableness)을 고려한 균형 잡힌 규제를 마련해야 할 것이다.

한국은 유럽, 미국, 일본, 중국의 맞춤형 광고 규제 방식을 참고하여 소비자 보호와 상업적 자유 간의 균형을 맞출 수 있는 규제체계를 마련할 필요가 있다. 특히, 중소기업과 대기업 또 글로벌 기업 간의 법적 준수 능력 차이를 고려하여, 기업의 규모에 맞는 유연한 규제 시스템을 도입할 수 있다. 이는 중소기업이 준수 비용으로 인해 어려움을 겪지 않도록 하고, 동시에 소비자의

권리를 보호하는 법적 근거를 마련하는 방향으로 나아갈 수 있을 것이다. 또한, 개인정보 보호의 강화가 불가피한 상황에서, 한국은 광고 산업의 자율적 규제(Self-Regulation)와 정부 규제를 조화롭게 활용하여 효율적인 법적 환경을 조성해야 한다. 이와 같은 접근은 글로벌 테크 기업과 중소기업 간의 형평성을 고려하고, 지나친 규제가 초래할 수 있는 산업 위축을 방지할 수 있는 길이다.

한국의 맞춤형 광고 규제는 데이터 보안 및 관리 기술의 발전과 함께 점진적으로 발전해야 한다. 차등 프라이버시(Differential Privacy) 등 새로운 데이터 보호 방법을 도입하면, 광고주가 소비자 데이터를 안전하게 활용할 수 있는 기술적 기반이 마련할 수 있을 것이다. 이러한 기술은 기업들이 규제 준수에 필요한 법적 부담을 줄이고, 데이터 보호 수준을 높일 수 있는 효과적인 대안이 될 수 있다. 또한, 비례성 원칙(Principle of Proportionality)을 준수하여 기업의 규모와 업종별로 규제 강도를 달리 적용할 수 있다. 이를 통해 중소기업의 경쟁력을 보호하고, 과도한 규제가 초래할 수 있는 산업 경제의 위축을 방지할 수 있을 것이다. 이와 같은 유연한 규제는 GDPR과 같은 엄격한 규제체계로 인한 경제적 부작용을 최소화할 수 있는 방법으로 평가된다.

개인정보 보호와 광고 산업의 지속 가능한 발전을 위해 공공과 민간의 협력 체계를 강화하는 것이 필요하다. 유럽연합의 GDPR처럼 한국에서도 개인정보보호위원회와 같은 규제 기관이 주도하여 법적 준수와 소비자 권리 보호를 감독하고, 동시에 민간 기업이 자율적으로 데이터 보호 규정을 준수할 수 있도록 기술적·재정적 지원을 제공할 수 있다. 일본의 APPI와 유사하게 기업에게 유연성을 부여하는 동시에, 정부는 가이드라인과 모니터링을 통해 소비자 보호 수준을 보장할 수 있을 것이다. 또한, 정부와 민간 간의 긴밀한 협력은 법적 효율성을 높이고, 법적 안정성(Legal Stability)을 유지하는 데 기여할 수 있다. 예를 들어, 기업들은 개인정보 보호를 위해 기술 연구와 개발을 진행하고, 정부는 이를 위한 인프라와 지원을 제공함으로써 상업적 자유와 개인정보 보호가 조화를 이루도록 할 수 있을 것이다.

다음으로 한국은 글로벌 시장에서의 경쟁력을 유지하기 위해 국제적 규제 조화(International Regulatory Harmonization)를 고려해야 한다. 유럽의 GDPR과 일본의 APPI는 국제 데이터 거래에서 상호 적합성을 인정받아 데이터를 자유롭게 활용할 수 있는 기반을 제공하고 있으며, 한국도 유사한 방안을 모색할 필요가 있다. 이는 데이터 적합성(Adequacy Decision)을 기반으로 한국의 규제 체계가 국제적 표준에 맞도록 조정함으로써 글로벌 기업의 데이터 활용을 촉진하고, 한국 기업이 국제 시장에서 경쟁력을 유지하는 데 기여할 수 있다. 특히, 중국의 PIPL과 같은 엄격한 국경 간 데이터 이동 제한을 일부 조정하여, 한국의 맞춤형 광고 산업이 글로벌 시장에서 데이터 거래에 제약을 받지 않도록 하는 것이 필요하다. 이를 통해 한국은 글로벌 데이터 시장에서 경쟁력을 확보하고, 데이터 보호와 상업적 자유를 동시에 추구할 수 있을 것이다.

6. 마치는 글

AI 시대에 맞춤형 광고 오남용에 따른 개인정보 보호를 위한 첫 번째 대응 방안은 관련 법과

규제의 정비다. 한국은 개인정보 보호법을 통해 이미 기본적인 보호 체계를 갖추고 있지만, AI의 특수성을 반영한 구체적인 규정 보완이 필요하다. 특히, AI 시스템이 맞춤형 광고 구현을 위해 개인정보를 수집하고 처리하고 또 추정하는 과정에서 발생할 수 있는 위험을 사전에 감지하고 이를 관리할 수 있는 법적인 장치가 마련되어야 한다. 예를 들어, AI 시스템에 대한 정기적인 데이터 보호 평가나 기업의 프라이버시 임팩트 평가를 의무화하는 방안이 고려될 수 있다. 유럽, 미국, 일본, 중국의 다양한 규제 접근 방식을 종합적으로 살펴본 결과, 각국의 법적 전통과 사회적·경제적 맥락에 따라 상이한 법적 접근 방식을 채택하고 있음을 확인할 수 있었다. 한국은 이러한 국제적 규제 흐름을 참고하여 법적 안정성을 유지하면서도 산업의 혁신을 지원할 수 있는 '균형적 규제'를 마련해야 할 것이다. 특히, 데이터 보호 기술의 발전과 규제의 유연성을 결합하여 중소기업의 준수 부담을 줄이고, 정부와 민간의 협력 체계를 통해 법적 효율성을 높일 수 있다. 또한, 국제적 규제 조화를 통해 국내 광고 산업이 글로벌 시장에서 경쟁력을 유지하도록 하는 것이 중요하다. 이를 통해 한국은 개인정보 보호와 광고/미디어 산업 혁신을 동시에 달성할 수 있는 균형적이고 지속 가능한 맞춤형 광고 규제 체계를 구축할 수 있을 것이다.

참고문헌

ADR.org. (2024). Explaining The New Data Privacy Framework. https://www.adr.org/blog/explaining-the-new-data-privacy-framework-privacy-shields-replacement

AppsFlyer. (2024, April 26). AppsFlyer data reveals increase in user opt-in rates and ad spend on iOS three years after Apple's App Tracking Transparency. https://www.appsflyer.com/company/newsroom/pr/att-data-findings/

Consilium Europa. (2024, June 13). Data protection: Council agrees position on GDPR enforcement rules. https://www.consilium.europa.eu/en/press/press-releases/2024/06/13/data-protection-council-agrees-position-on-gdpr-enforcement-rules/

Enzuzo. (2024). Global Data Privacy Laws in 2024 (Updated!). https://www.enzuzo.com/blog/data-privacy-lawsEY Japan. (2024). China data laws could impact global businesses. https://www.ey.com/en_jp/insights/forensic-integrity-services/how-chinas-data-privacy-and-security-rules-could-impact-your-business

European Commission. (2024). Artificial Intelligence Act: Ensuring Ethical and Trustworthy AI. Retrieved from https://ec.europa.eu

Greenleaf, G. (2023). Global data privacy laws 2023: 162 national laws and 20 Bills. Privacy Laws & Business International Report.

Morgan Lewis. (2023). How to Comply with the New EU-US Data Privacy Framework. https://www.morganlewis.com/pubs/2023/07/how-to-comply-with-the-new-eu-us-data-privacy-framework

Osano. (2024). Data Privacy Laws: What You Need to Know in 2024. https://www.osano.com/articles/data-privacy-laws

TMO Group. (2024). Data Protection Laws in China: Overview. https://www.tmogroup.asia/insights/china-data-protection-laws/

World Bank. (2024). Data protection and privacy laws | Identification for Development. ID4D. https://id4d.worldbank.org/guide/data-protection-and-privacy-laws

구글 프라이버시 샌드박스의 개인정보 관련 이슈

이진규
주식회사 네이버 CISO/CPO

1. 프라이버시 샌드박스 개요

구글(Google)은 프라이버시 샌드박스 이니셔티브(Privacy Sandbox Initiative)가 온라인에서 개인정보를 보호하는 동시에 기업과 개발자에게 성공적인 디지털 비즈니스를 구축할 수 있는 도구를 제공하는 기술을 개발하는 것을 목표로 한다고 설명한다. 또한, 프라이버시 샌드박스는 사이트 간 및 앱 간 추적(tracking)을 줄이는 동시에 온라인 콘텐츠와 서비스를 누구나 자유롭게 이용할 수 있도록 지원할 것이라 설명한다.[1]

구글이 언급한 프라이버시 샌드박스는 크게 두 가지의 이니셔티브로 구분할 수 있는데, 하나는 웹(Web)에서의 프라이버시 샌드박스이고, 다른 하나는 안드로이드(Android)에서의 프라이버시 샌드박스이다. 전 세계에서 75%에 달하는 점유율의 크롬 브라우저(Chrome Browser)와 Apple의 iOS와 함께 모바일 운영체제 시장을 양분하고 있는 안드로이드에 각각 프라이버시 보호를 강화하려는 다양한 기술적 조치를 적용하려는 것이다.[2]

구글은 프라이버시 샌드박스를 제안한 배경으로, 제3자 쿠키 메커니즘을 제한하거나 삭제하면서 효과적인 대안을 제시하지 않는 타 사업자들의 조치로 인해 생태계의 중요 기능에 부정적 영향을 미칠 수 있고, 이용자에 대한 추적 기능이 은밀하게 도입되어 개인정보가 오히려 보호되지 않는 위험이 발생할 수도 있다고 설명한다. 따라서, 온라인 추적 식별자를 활용하지 않고도 주요 생태계 요구사항을 지원하는 새로운 솔루션을 개발·출시하고, 이를 활용한 개발자로 하여금 개인정보를 보호하는 방식으로 무료 콘텐츠를 제공하고 비즈니스를 성장시키도록 할 필요가 있다는 것이 구글의 주장이다.

구글은 이와 같은 프라이버시 샌드박스의 도입 계획을 2020년 1월에 발표했고, 2022년 2월엔 웹뿐만 아니라 모바일에서도 광고식별자(Google Advertising ID, GAID) 지원을 중단하겠다고 밝혔다. 또한, 크롬 브라우저에서의 제3자 쿠키 지원 중단 계획도 야심차게 밝혔으나, 몇 차례의 연기를 발표한 끝에 올해 7월 쿠키 지원 중단에 관한 계획을 전격적으로 수정하여, 이용자에게 통제권을 주는 방식으로 제3자 쿠키 지원을 이어나갈 예정임을 밝혔다.

2. 프라이버시 샌드박스 기술

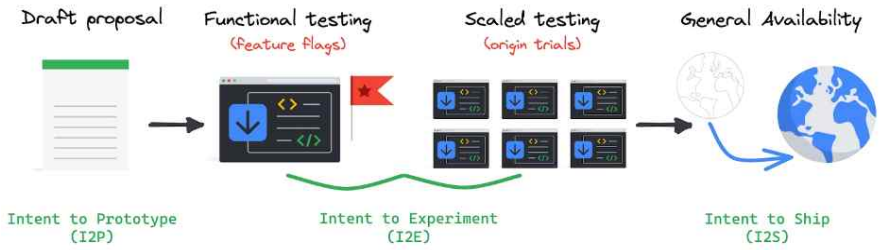
웹에서의 프라이버시 샌드박스 기술 가운데 핵심적인 제안을 정리하면 아래 표와 같다.[3]

표 1 웹 프라이버시 샌드박스 기술 범주와 주요 제안

	기술 범주	세부 기술 제안
웹에서의 프라이버시 샌드박스	사이트 간 프라이버시 경계 강화	▸ CHIPS: 개발자가 최상위 사이트마다 별도의 쿠키 항아리를 사용하여 분할 저장소에 쿠키를 옵트인 할 수 있도록 허용함 ▸ Related Website Sets: 동일한 주체가 소유한 관련 도메인 네임이 동일한 1st party에 속하는 것으로 선언하도록 허용함 ▸ Shared Storage: 사이트가 파티션되지 않은 사이트 간 데이터를 저장하고 액세스할 수 있는 범용 API를 생성함. 이 데이터는 유출을 방지하기 위해 안전한 환경에서 읽어야 함. ▸ Storage Partitioning: localStorage 또는 쿠키와 같은 모든 형태의 사용자 에이전트 상태를 단일 오리진이나 사이트가 아닌 최상위 사이트와 로드 중인 리소스의 오리진별로 이중 키로 설정할 수 있도록 함 ▸ Fenced Frames: 사이트 간 데이터를 공유하지 않고도 페이지에 콘텐츠를 안전하게 임베드할 수 있도록 함 ▸ Network State Partitioning: 모든 요청에 리소스를 재사용하기 위해 반드시 일치해야 하는 네트워크 파티션 키가 있는지 확인하여 브라우저 네트워크 리소스가 퍼스트 파티 컨텍스트에서 공유되는 것을 방지함 ▸ Federated Credential Management (FedCM): 사용자가 명시적으로 동의하지 않는 한, 사용자의 이메일 주소 또는 기타 식별 정보를 타사 서비스 또는 웹사이트와 공유하지 않고 연합 ID를 지원함
	연관 있는 콘텐츠 및 광고 노출	▸ Topics API:관심 기반 사용 설정 서드 파티 쿠키를 사용하거나 사용자 행동을 추적하지 않는 광고 확인할 수 있음 ▸ Protected Audience API: 리마케팅 및 맞춤 타깃 사용 사례를 제공하기 위한 광고 선택은 타사에서 사이트 전반의 사용자 검색 행동을 추적하는 데 사용할 수 없도록 설계됨
	디지털 광고 성과 측정	▸ Attribution Reporting: 광고 클릭 또는 광고 조회수를 전환과 연관시킴. 광고 기술자는 이벤트 수준 또는 요약 보고서를 생성할 수 있음 ▸ Private Aggregation API:사이트 간 데이터로 노이즈가 많은(noisy) 요약 보고서를 생성함
	은밀한 추적 예방	▸ User-Agent reduction and User-Agent Client Hints: 수동적으로 공유되는 브라우저 데이터를 제한하여 핑거프린팅을 유발하는 민감한 정보의 양을 제한함 ▸ IP Protection: IP 주소가 추적에 사용되지 않도록 보호하여 사용자 개인정보 보호 강화 ▸ Bounce tracking mitigations: 여러 컨텍스트에서 사용자를 인식하는 바운스 추적 기능을 줄이거나 없애는 제안 ▸ Privacy Budget: 사이트에 노출되는 개별 사용자 데이터의 양을 제한하여 은밀한 추적을 방지함
	웹 스팸 및 사기 대응	▸ Private State Tokens: 웹사이트가 수동적인 추적 없이 한 브라우징 컨텍스트에서 다른 컨텍스트(예: 사이트 간)로 제한된 양의 정보를 전달하여 사기를 방지할 수 있게 함

위의 표에서 확인할 수 있듯, 프라이버시 샌드박스는 다양한 기술적 제안을 검증하고 적용하는 일련의 체계인데, 최근까지 크롬 및 생태계 관계자들이 제안한 세부 기술은 총 30종이 넘는다.[4] 이런 방식으로 검증된 일부 기술은 W3C(World Wide Web Consortium)가 채택하는 웹 표준으로 기능할 수도 있다. 프라이버시 샌드박스의 제안 생명주기는 초안 제안(draft proposal), 기능 검증(functional testing), 확대 검증(scaled testing, origin trials라고도 함), 일반 배포(general availability) 등의 과정을 거치게 된다.

그림 1 프라이버시 샌드박스에서의 제안 생명주기



출처: Google

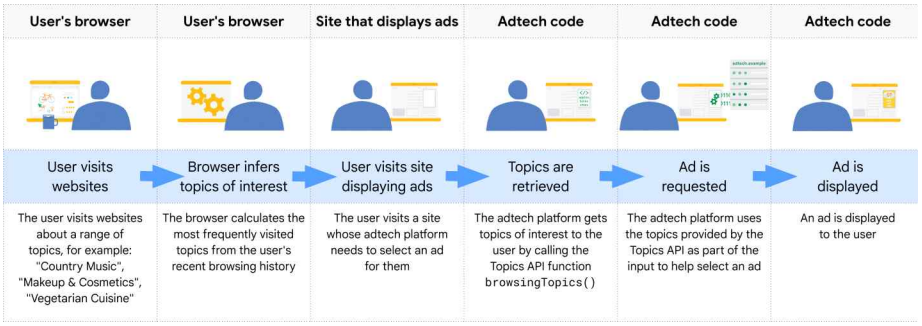
배포가 되었다고 하여 모든 기술이 전체 개발자가 사용할 수 있고, 이용자들이 그 기능을 향유할 수 있는 것은 아니다. 일부 기술은 점진적으로 배포가 되고, 그 과정에서 구글 및 개발자들은 잠재적 이슈에 대응할 수 있는 시간을 확보한다. 일부 기술 및 기능은 이용자가 그 설정에 관여하도록 하여 통제권을 제공하기도 한다.

프라이버시 샌드박스는 개발 전체 과정에서 피드백을 수용하고, 이를 바탕으로 '피드백 보고서(Feedback Report)'를 분기별로 발행한다. 크롬 브라우저의 경우 전용 피드백 양식을 공개하고 있고, W3C 포럼을 통한 피드백을 받기도 하며, 특정 제안에 대한 메일링 리스트를 운용하기도 하는 등 다양한 피드백 채널을 운용한다. 안드로이드는 GitHub를 통해 이슈를 제보받는다.

3. 프라이버시 샌드박스의 개인정보 관련 이슈

프라이버시 샌드박스에 제기된 개인정보 관련 논란은 초기엔 FLoC(Federated Learning of Cohorts) API에서 불거졌다. 개인에 대한 추적을 제한하고, 특정한 이용자(브라우저)에게 부여된 코호트 ID를 광고 사업자에게 전송하는 방식을 적용한 것이 FLoC API이다. 해당 코호트 ID에 매칭되는 연관성 있는 광고를 노출하는 방식으로 이용자 프라이버시를 보호하고, 광고 연관성은 매우 높은(=기존의 제3자 쿠키를 이용하는 것과 유사한) 수준을 유지할 수 있게 한 것이라서 시장에서 높은 호응을 얻을 것으로 기대되었다. 그러나, 감시 자본주의를 지속하는 기제로서 작용할 우려, 제3자 쿠키가 제공하는 기능 제공과 동등한 기능 제공의 한계, 광고 연관성 저하, 민감 정보에 기반한 타기팅 가능성, 브라우저 핑거프린팅 유지, 관심사를 웹에 전달하는 것 등에 관한 문제가 제기되어 2022년 초에 Topics API로 대체되기에 이르렀다.[5][6]

그림 2 FLoC API를 대체한 Topics API의 활용 방식



출처: Google

FLoC API 이슈는 구글이 추진하는 프라이버시 샌드박스가 결국 자사의 이익을 추종하고, 프라이버시 보호에는 도움이 되지 않지만, 사람들에겐 그럴듯한 대안으로 보이는 소위 '프라이버시 워싱(privacy-washing)'에 해당하는 것이 아니냐는 비판으로 이어지기도 했다.[7]

FLoC API로 불거진 개인정보 보호 이슈는 점차 프라이버시 샌드박스 전반으로 확산됐다. 이들 중 다수는 Google이 온라인 광고 생태계에서의 주도권을 유지·강화하기 위해 이용자 프라이버시 보호와 퍼블리셔들의 수익성을 약화시킬 것이라는 점에 초점이 맞춰져 있다. 프라이버시 샌드박스에 제기된 개인정보 보호 이슈를 정리하면 다음 표와 같다.

표 2 프라이버시 샌드박스에 제기된 개인정보 보호 이슈

구분	주요 내용
구글의 독점적 소유권	구글이 전체 프라이버시 샌드박스 시스템을 통제하는 독점적 소유권으로 인해 사용자 데이터에 대한 권한 집중에 대한 우려가 제기됨. 다양한 피드백을 수용하지만, 일단 배포되고 나면 구글이 프라이버시 샌드박스 기술에 대한 독점적 소유권을 갖고 전횡을 휘두를 가능성을 배제할 수 없음[8]
브라우저 기술과 광고의 통합	개인정보 보호 샌드박스는 브라우저 기술, 사용자 추적 및 광고를 통합하여 사용자 데이터가 맞춤형 광고 경험에 사용될 수 있도록 함. 결국, 기존에 이용자 추적을 서버에서 하던 방식을 이용자 기기(브라우저)로 옮긴 것에 다름없음
제한된 투명성 및 통제권	일부 프라이버시 샌드박스 제안은 데이터 사용 방식에 대한 사용자 투명성과 통제력을 제한함(예를 들어, 토픽 API 제안은 기업이 사용자의 검색 습관을 기반으로 사용자를 타기팅할 수 있도록 허용하지만, 사용자는 사용된 특정 토픽을 보거나 제어할 수 없음)
온라인 트래킹 통제의 이전	온라인 추적 제어권을 타사 추적업체에서 Google로 전환하여 Google의 Chrome 브라우저가 사용자를 추적하고 웹사이트 및 광고주와 인사이트를 공유하게 함[9]
제3자 쿠키 지원 유지	제3자 쿠키 지원 중단에 대한 계획을 접고, 이용자에게 통제권을 부여한다는 구실로 여타 주요 브라우저의 정책과 달리 제3자 쿠키를 지속적으로 지원함. 이로 인해 기존의 제3자 추적을 유지하여 광고 생태계에서의 주도권을 지속하고, 이용자 프라이버시 보호를 후퇴시킴

4. 제3자 쿠키 지원 중단 계획 '번복' 논란

올해 7월, 구글은 크롬 브라우저에서 제3자 쿠키 지원을 중단하겠다는 계획을 전격 철회한다고 발표하면서 이용자에게 더 많은 선택권을 부여하는 새로운 방식을 적용하겠다고 밝혔다.[10] 구글은 이러한 조치가 영국 경쟁 감독 당국(Competition and Markets Authority, CMA), 영국 개인정보 감독기관(Information Commissioner's Office, ICO), 퍼블리셔, 웹 개발자 및 웹 표준 단체 등과 협의하여 내린 결정이라고 밝혔지만, Safari, Firefox, Brave 등 세계 주요 브라우저들이 제3자 쿠키 지원을 전면 중단한 것과는 상반된 입장이라서 큰 논란이 일어났다. 특히, 제3자 쿠키 지원 중단을 공언하고, 다양한 업계 파트너사들과 테스트까지 수행했던 터라 더욱 논란이 되었다.[11]

구글은 "타사 쿠키를 더 이상 사용하지 않는 대신 사용자가 웹브라우징 전반에 걸쳐 정보에 입각한 선택을 할 수 있는 새로운 환경을 크롬에 도입하고 언제든지 그 선택을 조정할 수 있도록 할 것입니다."라고 밝혔으나, 구체적으로 어떤 방식을 도입할 것인지 현재로서는 명확하지 않다. 다만, Apple이 자사의 iOS에 적용한 앱추적투명성(ATT, App Tracking Transparency)과 유사한 방식을 적용하여, 크롬 브라우저에서의 제3자 쿠키 기반 추적을 이용자 스스로 선택(동의)하도록 하는 방식을 적용할 것이라는 의견이 우세하다.

그림 3 최종 번복 전, 구글의 제3자 쿠키 지원 중단 추진상황

출처: OnAudience

이와 같은 방식은 애플이라는 경쟁사가 성공한 방식을 크롬 브라우저에 이식하여, 크롬 브라우저에서의 제3자 쿠키 지원을 유지하는 것에 대한 비판으로부터 스스로를 방어하는 동시에, 기존 광고 시장에서 통용되어 온 제3자 쿠키 기반의 다양한 광고 캠페인 수행 활동을 지원하여 광고 시장에서의 확보한 지배력을 유지 및 강화하려는 조치로 이해된다.

5. 나가며

결국, 프라이버시 이니셔티브는 구글이 온라인 시장을 과점하고 있는 제품군(브라우저, 모바일 OS)에서의 프라이버시 보호조치를 강화하여 기존에 확보한 지배력을 유지하거나 강화하는 동시에 프라이버시 보호에 대한 다양한 관계자들의 요구사항을 일부 수용하여 규제당국의 공격과 이용자들의 비판을 회피하려는 자기보호적 접근방식으로 볼 여지가 있다.

프라이버시 보호를 강화하려는 기술적 제안 방식이기 때문에, 구글의 프라이버시 샌드박스가 개인정보 보호와 관련하여 기술적 상세 수준에서 미진한 지점에 대한 지적이나, 정책적 측면에서 부적절한 요구를 제안하는 점에 대한 비난이 크게 불거질 것이라 예상하는 것은 쉽지 않다. 그러나, 온라인 영역, 특히 광고 및 모바일 운영체제 시장에서의 지위를 유지하고 강화하려는 조치가 프라이버시와 (시장) 경쟁 영역에서의 충돌을 불러일으키고 있어 프라이버시 샌드박스는 앞으로도 세계 각국 프라이버시 및 경쟁 감독 당국의 주목을 지속적으로 받게 될 가능성이 작지 않다. 프라이버시 샌드박스의 전개 방식을 상시 관찰하고, 필요 시 적극적으로 대응해야 할 이유가 여기에 있다.

주석

[1] Google, “Privacy Sandbox: Overview”,
URL: https://developers.google.com/privacy-sandbox

[2] 크롬 브라우저의 모바일 점유율은 40.6%로 데스크탑 점유율과 비교하여 다소 낮은 편이다. 이에 관한 상세한 내용은 다음 기사를 참조 – 디지털데일리, “삼성·네이버, 구글 ‘크롬’ 독주에도 놓지 못하는 웹브라우저 시장…왜?”, 2024. 01. 10.,
URL: https://ddaily.co.kr/m/page/view/2024010919454659722

[3] Google, “Privacy Sandbox: What is the Privacy Sandbox”,
URL: https://developers.google.com/privacy-sandbox 의 내용을 번역 및 정리함

[4] 제안된 전체 리스트는 다음 정보를 참조
– URL: https://github.com/w3c/web-advertising#ideas-and-proposals-links-outside-this-repo

[5] FLoC API에 제기된 프라이버시 및 경쟁 관점에서의 이슈는 다음 글을 참조
– 이진규, 이재림, “Google FLoC 적용과 프라이버시 고려사항”, DAIG 2021년 제2호, p. 181 – 190.
URL: https://sapi.co.kr/wp-content/uploads/2021/09/Google%EC%9D%98-FLoC-%EC%A0%81%EC%9A%A9%EA%B3%BC-%ED%94%84%EB%9D%BC%EC%9D%B4%EB%B2%84%EC%8B%9C-%EA%B3%A0%EB%A0%A4%EC%82%AC%ED%95%AD_0923_2.pdf

[6] 전자프런티어재단(Electronic Frontier Foundation)은 구글의 FLoC를 비판하면서, 이를 “최악의 발명품”이라 부르기도 했다. 서버에서의 추적을 브라우저 레벨로 전환한 것 외에 프라이버시 보호에 도움이 되지 않는다는 주장이다. 이에 대한 상세 정보는 다음 기사를 참조
– 보안뉴스, “서드파티 쿠키 대신 플록 제안한 구글, 사실은 덫을 놓았나?”, 2021. 3. 8.
URL: https://www.boannews.com/media/view.asp?idx=95418

[7] INPLP, “Tracking trouble: AS Watson's €600,000 fine and Google’s Privacy Sandbox under scrutiny”, 2024. 3. 10.,
URL: https://inplp.com/latest-news/article/tracking-trouble-as-watsons-EUR600000-fine-and-googles-privacy-sandbox-under-scrutiny/

[8] HeyData, “Data Privacy Concerns with Google’s Privacy Sandbox”, 2023. 4. 10.,
URL: https://heydata.eu/en/magazine/data-privacy-concerns-with-google-s-privacy-sandbox

[9] EFF, “Why Privacy Badger Opts You Out of Google’s ”Privacy Sandbox“”, 2024. 7. 22.
URL: https://www.eff.org/deeplinks/2024/07/why-privacy-badger-opts-

you-out-googles-privacy-sandbox

[10] Anthony Chavez, “A new path for Privacy Sandbox on the web”, 2024. 7. 22., URL: https://privacysandbox.com/news/privacy-sandbox-update/

[11] Google Developers, “Preparing for the end of third-party cookies”, 2023. 10., URL: https://developers.google.com/privacy-sandbox/blog/cookie-countdown-2023oct

해외 개인정보보호 자율규제 사례 및 동향

정상호
개인정보보호협회 팀장

1. 자율규제의 법적 개념

한 영역에 대한 규제가 마련되기까지는 해당 분야에 대한 정보와 경험을 축적하고 다양한 이해관계의 조정은 물론 규제에 대한 사회적 합의를 도출하기 위한 충분한 시간이 필요하다. 이 경우 법률의 원칙적이고 큰 틀 내에서 민간의 자율규제가 규제 공백 해소와 규제의 수용력 제고를 위해 효과적인 대안으로 받아들여지기도 한다.[1]

일반적으로 '규제'란 원래 개인의 자유로운 선택과 경쟁에 맡겨져 있는 영역에 관하여 공권력의 주체인 정부가 간섭과 통제를 하는 것, 즉 '정부규제'를 의미한다.[2] 그런데, '자율규제'라는 용어는 서로 반대되는 개념인 "자율 vs. 규제"를 결합한 조어(造語)이기 때문에 그 자체로 모순적이다. '자율'에 방점을 둔다면 정부의 관여를 전적으로 배제하고 시장 참여자들이 자체적으로 규칙을 정하여 준수하는 '자기규제' 또는 규제 자체를 백지화하고 시장에 맡기는 '탈규제'도 자율규제에 해당될 수 있다. 반면 '규제'에 방점을 둔다면 시장 참여자들의 자율이 일부 허용되지만 사실상 전통적인 정부규제와 크게 다르지 않은 형태, 예컨대 정부의 지시나 명령에 의하여 시장 참여자들이 형식적·타율적으로 자체 규율 체계를 조직하고 운영하지만 정부가 여전히 사전적·사후적으로 강력한 감독 권한을 행사하는 것도 자율규제의 개념에 포섭할 수 있다.[3]

이처럼 자율규제의 개념에 대해서는 다양한 견해가 존재할 수 있으나, 이러한 견해들의 핵심 개념 징표는 정부의 개입은 줄이고 시장의 자율은 늘리는 것, 다시 말해 '행정에 의한 통제'에서 '시장 참여자의 자기책임 원칙'으로의 패러다임(paradigm) 전환이라 할 수 있다.[4] 그러한 의미에서 자율규제는 '사업자 또는 사업자단체가 이용자 보호 또는 시장의 투명성·신뢰성 확보를 위해 스스로 행하는 자정 노력'이며, 규제를 전적으로 배제하는 무규제(un-regulation), 과도한 공적 규제를 제거하는데 초점을 둔 탈규제(de-regulation)와는 전혀 다른 개념이다.[5]

2. 디지털 플랫폼에서의 자율규제 논의 배경

전통적으로 기업에 대한 규제는 독과점 방지, 공정한 시장 질서 유지 등을 위한 경쟁법적 측면에서의 규제체계였으나, 데이터 기반의 플랫폼 시장 급성장과 빅데이터의 활용 증가로 인해 개인정보의 정당한 처리와 정보주체의 개인정보 자기결정권 보장 필요성에 대한 관심도 증대되고 있다.

디지털 플랫폼이란 인터넷을 통해 서비스 제공자와 사용자 간의 상호작용을 중개하고 촉진하는 기술 기반의 서비스라고 정의할 수 있다.[6] 이러한 플랫폼은 방대한 양의 데이터를 수집하고 이를 활용하여 개인화된 경험과 타깃 광고를 제공한다.

2000년대 중반부터 플랫폼의 경제적인 영향력이 두드러지면서 독점적 지위와 시장 지배력에 대한 우려가 커지고, 결국 반독점 조사와 규제 강화로 이어졌다. 그즈음 개인정보 보호에 대한 사회적 인식이 높아지고, 대규모 개인정보 유출 사건들이 발생하면서 규제 당국은 개인정보 보호를 강화하기 시작했다. 2018년 유럽연합의 GDPR 도입은 이러한 변화를 대표하는 사건으로, 전 세계적으로 개인정보 보호 규제의 표준이 되었다.[7] 또한, 디지털 플랫폼의 사회적 책임에 대한 논의도 활발해졌으며, 잘못된 정보 확산과 혐오 발언, 사이버 괴롭힘 등이 주요 이슈로 부각되었다.[8]

3. 해외 개인정보 보호 자율규제 사례

디지털 플랫폼 규제가 강화되고 있는 가운데 유럽연합과 미국에서도 자율규제의 중요성이 부각되고 있다. 이는 자율규제가 법적 사전 규제보다는 플랫폼의 자율성을 존중하고, 플랫폼이 빠르게 변화하는 기술 환경에 적응할 수 있도록 하는 효과적인 수단이기 때문이다.[9] 이하에서는 해외 주요국의 플랫폼에 대한 자율규제 사례 중 개인정보 보호와 관련된 사례에 대해 살펴본다.

(1) 유럽데이터·마케팅연맹(FEDMA)의 자율규제

FEDMA(Federation of European Data& Marketing)는 유럽연합을 포함하여 스위스, 헝가리, 폴란드 등 12개 국가의 협회를 회원으로 하고 있는데, 각 국가의 협회는 소비자단체, 서비스제공 업체, 미디어제공업체 등을 대표한다.

FEDMA는 EU「전자상거래지침」(Directive 2000/31/EC)에 근거[10]하여「전자상거래 및 쌍방향 마케팅에 대한 행동강령(FEDMA Code on E-Commerce and Interactive Marketing)」과「개인정보 사용에 대한 행동강령(FEDMA Code of Practice for the use of Personal Data)」을 발표하였다. 행동강령에는 제품·서비스의 온라인 판매에 있어서 판매자가 소비자에게 지켜야 할 윤리적인 행동기준(운영상의 투명성, 거래보안, 개인정보 및 데이터 보호, 미성년자 보호, 모니터링 및 제재 등)을 제공하고 있다.

행동강령에 참여하고 이를 준수하는 협회와 기업에 대해서는 인증마크, 보증 등이 부여되고, 소비자 민원 해결 메커니즘과 분쟁 해결을 위한 체계가 제공된다.

(2) 미국의 디지털광고연맹(DAA)의 디지털 광고 책임성 프로그램[11]

"디지털 광고 연맹(Digital Advertising Alliance, DAA)"은 광고 및 마케팅 업계 단체들이 주도하는 독립적인 비영리조직으로, 디지털 광고와 관련한 개인정보 보호 관행을 수립·시행한다.

DAA는 웹 및 모바일 광고에 대한 자율규제의 일환으로 2011년에 '책임성 프로그램(Accountability Program)'을 개발했는데, 동 프로그램은 기업이 광고를 위한 데이터 수집 및 이용에 대한 투명성과 소비자 선택권을 제공함으로써 디지털 광고 시장의 신뢰를 구축하는 것을 목적으로 한다. 디지털 광고 기업들은 '책임성 프로그램'에 따라 소비자 개인정보 보호를 위해 다음과 같은 내용을 준수하여야 한다.[12]

- 적극적 고지(enhanced notice): 인터넷 기반 광고에 대해 적극적인 고지 활동이 필요
- 정밀 위치 데이터(precise location data): 게임 앱을 중심으로 불필요하게 정밀한 위치 데이터 수집을 지양하거나 수집 시 적극적 고지 필요
- 민감 데이터 원칙(sensitive data principles): 아동 온라인 프라이버시 보호법(Children's Online Privacy Protection Act of 1998)에 따라 어린이의 민감 데이터 수집 지양
- 복수 기기(cross-device) 광고 : 하나의 단말과 연동된 여러 기기 상에서의 광고에 대해 소비자 고지에 수동적인 문제 개선

책임성 프로그램은 회원사의 자발적인 협력에 의한 자율규제를 원칙으로 하지만, 이에 협조하지 않는 기업에 대해서는 연방거래위원회(FTC)에 해당 기업의 위반 사례를 이첩할 수 있다.

(3) 미국 무선통신산업협회(CTIA)의 IoT 인증[13]

미 정부는 IoT 보안에 대한 직접적인 개입 방식보다는 국립표준기술연구소(NIST)를 통한 기술 가이드 역할을 수행하며, 민간은 NIST 규격을 토대로 인증 프로그램을 운영한다. 미 통신업계의 대표적 산업단체인 무선통신산업협회(Cellular Telecommunications and Internet Association, CTIA)의 경우, IoT 기기 보안 테스트를 통과한 제품에 대하여 인증 등급을 부여하는 제도[14]를 운영하며 IoT 기기 보안과 소비자의 선택권 향상을 도모하고 있다.

CTIA의 IoT 사이버보안 인증 프로그램은 기능 구현의 난이도에 따라 1~3단계로 구분하는데 개인정보 보호와 관련된 인증 요구항목은 다음과 같다.

표 1 미국 CTIA IoT 인증: 개인정보보호 관련 인증 요구 사항

단계	준수사항
1단계	서비스 약관 및 개인정보정책, 기기상 비밀번호 관리 규정 준수, 사용자별 기기 접근 제어 기능, 감사 로그 수집 및 통합관제시스템 전송
2단계	다양한 암호화 통신 표준 지원, 다인증요소 로그인, 통합관제시스템의 기기 원격 제어, 부팅 시 외부 공격 가능성 차단 메커니즘, 비정상적 또는 악의적 활동 로그 기록
3단계	디지털 서명 생성 및 유효성, 저장 데이터 암호화, 보안설계내재화

(4) 스페인 Confianza Online의 트러스트 마크 씰 'Sello de Confianza'[15]

'Confianza Online'는 2003년에 설립된 스페인 소재 비영리단체로, 업계의 자율적인 규제 준수를 독려하는 'EU 전자상거래 지침(제16조)'에 따라 소비자 신뢰 기업에 트러스트 마크(Trust mark) 인증을 부여하고 소비자 분쟁 해결을 위한 중재 기능을 제공하고 있다.

자율규제의 실효성 담보와 업계 내 전자상거래 시 소비자 및 개인정보보호 등의 법규 준수를 정착시키기 위해 Confianza Online에 참여하는 기업에 대해 'Sello de Confianza'라는 트러스트 마크 씰(Seal)을 부여한다. 씰을 부착한 기업은 소비자 만족도나 품질 면에서 안전하고 검증된 전자상거래를 지원하는 것으로 간주되며, 씰 사용에 대한 별도의 비용은 없다. 참여 기업은 Confianza 규약에 따라 법률적인 요구사항뿐만 아니라 미성년자 보호, 거래자의 투명성, 결제 보안, 광고 및 프라이버시 등과 관련된 다양한 규범적인 요구 사항도 함께 준수해야 한다.

씰이 부여된 제품이나 서비스에서 문제가 발생될 경우 소비자는 Confianza Online을 통해 민원사항을 접수할 수 있으며, Confianza Online은 자체 규약에 따라 '대체적 분쟁 해결 절차(alternative dispute resolution procedure)'에 착수한다. 규제 위반 기업에 대해서는 인증마크 활용의 일시 정지 또는 영구 철회 등의 조치가 가능하다.

(5) 미국 자율규제 가이드라인(아동의 개인정보 보호)

미국은 아동의 개인정보 보호와 관련하여 자율규제를 권장하며 안전항(Safe Harbor)[16] 제도를 운영하고 있다. 해당 제도는 사업자단체가 자율규제 가이드라인을 연방거래위원회(FTC)에 제출하여 승인요청을 하면, FTC가 관보게시를 통한 공공의견 수렴을 거쳐 180일 이내에 승인여부를 결정하는 제도이다. 자율규제 가이드라인이 승인될 경우, 해당 사업자단체에 소속된 구성원은 아동 개인정보의 수집 및 이용에 대한 규제를 이행하고 있는 것으로 간주되어 보다 자유로운 사업운영을 할 수 있다는 이점을 얻게 된다.

사업자단체의 자율규제 가이드라인이 FTC로부터 승인을 받기 위한 기준은 '아동 온라인 프라이버시 보호법(COPPA)' 시행령 제312.11조에 명시되어 있다. 승인된 자율규제

가이드라인이 변경될 경우, 변경 내용이 기존 가이드라인에 어떤 영향을 미치는지 FTC에 제출해야 하며, 승인된 자율규제 가이드라인의 실행에 미흡함이 있을 경우 FTC는 언제든지 승인을 취소할 수 있다. 운영자가 COPPA 및 COPPA 시행령을 위반하여 아동의 온라인 개인정보를 침해한 경우, 불공정이나 기만행위 또는 관행에 영향을 주는 상업행위를 규제하기 위한 연방거래위원회(FTC)법 제18조 (a)(1)(B)항 위반으로 간주된다.[17]

(6) 미국 연방거래위원회(Federal Trade Commissions: FTC)

연방거래위원회(이하 'FTC')는 독과점과 불공정거래를 규제하는 국가기관이나, 미국의 자율규제에서 중요한 역할을 차지하고 있다. 현재 맞춤형 광고나 온라인 플랫폼, 알고리즘 등을 모두 FTC가 관할하고 있으며, DAA 외에도 다양한 기구가 FTC와 긴밀한 관계를 맺으며 자율규제를 시행하고 있다. 미국의 자율규제는 가이드라인을 사업자단체나 시민단체들이 설정하지만, 결과적으로 규제의 준수를 FTC에 의존하고 있다.[18]

FTC의 규제를 뒷받침하는 가장 주요한 법은 FTC법 제5조'Section 5 of the Federal Trade Commission (FTC) Act'라고 할 수 있다. FTC는 자체적으로 제정한 가이드라인이나 긴밀한 연결 관계에 있는 기구들이 수립한 가이드라인에 대한 위반행위가 있을 때에는 해당 조항을 위배한 것으로 간주한다.[19] FTC는 'Safe Harbor'로 대표되는 면책시스템을 통해 자율규제를 시행하고 있고, 위에서 언급한 FTC법 제5조를 통해 자율규제 시스템을 뒷받침한다. COPPA에 규정된 Safe Harbor 조항은 FTC 자율규제의 대표적인 유형을 보여준다.

4. 해외 온라인 플랫폼 규제 입법 동향 및 시사점

전 세계적으로 온라인 플랫폼 기업의 투명성·공정성 제고뿐만 아니라 개인정보 보호 등을 통한 정보주체 권리 보장을 위한 새로운 법률들이 제정되고 있다. 플랫폼 규제 입법 여부에 대한 입장은 우리나라뿐만 아니라 해외 주요국에서도 다양하다. 대표적으로 EU와 미국의 플랫폼 규제 현황이 그러한 상황을 반영하고 있다.[20]

유럽연합(EU)의 경우 기존 경쟁법의 방식에서 벗어나, 사전적으로 적용 대상 핵심 플랫폼 서비스를 지정하고 게이트키퍼(gatekeeper)[21]가 이행하여야 하는 의무를 부과하며 불공정하다고 판단되는 행위를 금지하는 등 비전통적 형식의 규제를 도입하면서 플랫폼 규제에 가장 적극적인 입장을 보이고 있다. EU집행위원회는 디지털시장법(The Digital Markets Act)을 기반으로 'Alphabet, Amazon, Apple, Bytedance, Meta, Microsoft' 등 6개 사를 게이트키퍼로 지정하고, 이들 6개 사의 서비스 중 22개를 핵심 플랫폼 서비스로 지정하였다.[22]

반면, 미국은 2021년에 빅테크 기업의 독과점 규제를 강화하기 위하여 사전규제적 성격을 가진

'더욱 강력한 온라인 경제: 기회, 혁신, 선택'(A Stronger Online Economy: Opportunity, Innovation, Choice)이라는 5개의 패키지 법안을 발의한 바 있다. 그러나, 자국 내 소비자 및 산업에 미치는 영향을 우려하여 이후 최종 합의에 이르지 못한 채 2023년 1월, 회기 만료로 모두 폐기되었다. 따라서 미국은 아직 전통적 방식에 따라 기존 경쟁법을 적용하여 반독점 행위를 감시하고 있다.[23]

온라인 플랫폼 규제 강화에 강한 목소리를 내왔던 미국이 결국 관련 입법에는 신중한 입장을 취하였다는 점은 다른 국가들의 입법에도 시사하는 바가 크다. 특히 우리나라의 경우 특수한 플랫폼 시장 상황과 규모를 감안하여 별도의 입법을 통한 플랫폼 규제가 필요한 것인지 아니면 기존 경쟁법 체계를 통한 규제가 효율적인지 많은 논의가 있어야 할 것이다.

주석

[1] 김유향, "해외 인터넷 자율규제의 변화와 한국 자율규제의 미래", KISO저널 제49호, 2022.12 (https://journal.kiso.or.kr/?p=12040)

[2] 황성기, “ICT 분야에서의 자율규제”, 공법연구 제50집 제3호(2022. 2.), 35~36면.

[3] 이해원, “개인정보 보호 자율규제의 사법적(私法的) 의의 및 개선방안”, 법제(22. 12월호), 법제처, 131~132면

[4] 최철호, “행정법상의 자율규제의 입법형태에 관한 연구”, 법학논총 제23집, 숭실대학교 법학연구소(2010. 2.), 358-359면.

[5] 김민호, “윤석열 정부 의 ICT 자율규제 의미와 전망”, KISO 저널 제47호(2022. 6.), 7면.

[6] 디지털플랫폼은 주로 검색 엔진(예: 구글), 소셜미디어(예: 페이스북), 전자상거래(예: 아마존), 앱스토어(예: 애플 앱스토어), 콘텐츠 스트리밍(예: 넷플릭스)과 같은 형태로 존재한다.

[7] Bevir, M., & Bowman, Q. (2022). Digital Governance: Rethinking Regulation for the Digital Age. Oxford University Press.

[8] Flew, T., et al. (2019). Understanding Digital Media: A User's Guide. Oxford University Press.

[9] 황용석, “디지털플랫폼 자율규제, 평가와 과제”, KISO저널 제55호, 2024년 7월 2일 (https://journal.kiso.or.kr/?p=12794)

[10]「전자상거래지침」제16조(행동강령)에서는 회원국과 집행위원회가 지역사회 차원의 행동강령과 미성년자 보호 등 인간의 존엄성 보호를 위한 행동강령을 작성하도록 지원할 것을 규정하고 있다.

[11] 한국인터넷진흥원, “디지털 소비자 및 개인정보보호 분야 해외 자율규제 적용 현황”, 개인정보보호 월간동향분석, 2021. 5월, 14면

[12] The National Law Review, Interest-Based Advertising Enforcer Hits 100, 2019.6.3

[13] 한국인터넷진흥원, 앞의 글, 19~20면

[14] CTIA, IoT Cybersecurity Certification Program Management Document-Version 1.0, 2018.10

[15] 한국인터넷진흥원, 앞의 글, 17~18면

[16] Safe Harbor(안전항): 규제 당국이 제시한 요건이나 기준을 충족하면 해당 규범을 준수한 것으로 보아 더 이상 위법한 것으로 취급하지 아니하는 법제. 예를 들어, 운전자에게 "과속 운전을 하지 말 것"을 요구하는 법령의 맥락에서 "시속 25마일 미만으로 운전하는 것은 과속 운전에 해당하지 않는 것으로 결정적으로 간주한다"고 명시해 시속 25마일 미만 운전에 대해서는 도로교통 규정 상의 과속 운전 의무를 회피하거나 면제하는 것 http://www.koreanlii.or.kr/w/index.php/Safe_harbor_principle https://en.wikipedia.org/wiki/Safe_harbor_(law)

[17] 전윤선·나종연, "아동 소비자의 온라인 개인정보보호 관련 미국, EU, 영국, 한국의 법제도 비교 고찰", 소비자문제연구, 제51권 제2호, 2020, 8, 10면.

[18] 정혜련, 플랫폼 자율규제 연구, 스타트업얼라이언스 플랫폼규제연구모임, 2023. 2, 4, 6~47면

[19] 이문지, 미국 연방거래위원회법 제5조에 의한 소비자 개인정보 보호 – 자율규제에 의한 소비자 개인정보 보호의 안전장치 –, 경영법률 14집, (2016). 448~449면

[20] 최은진, "지배적 플랫폼 사업자의 규제 이슈에 대한 검토", 「NARS 현황분석」 제315호, 국외입법조사처, 2024.2, 14면

[21] 게이트키퍼는 2023년 5월부터 EU에서 시행하는 디지털시장법(Digital Markets Act)에서 규정하는 시장지배적 영향력을 지닌 핵심 플랫폼 서비스를 보유한 사업자를 말한다.

[22] EU Commission, "Digital Markets Act : Commission designates six gatekeepers", 2023.9.6

[23] 강일 등, "미국 등 해외 온라인 플랫폼 규제 입법 동향 및 시사점", 법률신문(인터넷 2023-01-17) www.lawtimes.co.kr/LawFirm-NewsLetter/184598

Privacy Report
2024 개인정보 이슈
심층 분석 보고서

『Privacy Report 2024 개인정보 이슈 심층 분석 보고서』는
디지털·정보보호 관련 글로벌 트렌드
및 주요 이슈를 분석하여
정책 자료로 활용하기 위해 한국인터넷진흥원에서
기획, 발간하는 심층 보고서입니다.

본 보고서의 내용은
한국인터넷진흥원의 공식 견해가 아님을 알려드립니다.

발행

발행일 2024년 12월

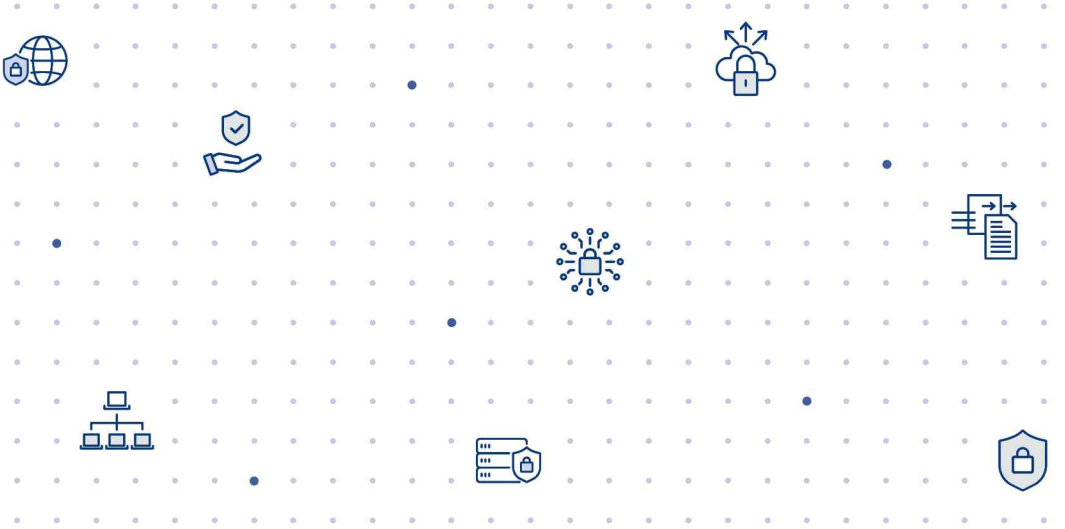
발행처 한국인터넷진흥원 개인정보제도팀
전라남도 나주시 진흥길 9
Tel : 061-820-1231

PRIVACY REPORT

2024 개인정보 이슈
심층 분석 보고서

2024 Vol. 7

PRIVACY REPORT



KISA 한국인터넷진흥원