No. 1 | 발행일 | 2019년 5월 9일



한국정보화진흥원

# EU, 디지털 단일시장에 적용되는 저작권 지침 제정

○ 유럽의회는 디지털 환경에서 저작권 적용을 유럽차원에서 조정하기 위하여 「디지털 단일시장(Digital Single Market) 저작권 지침」 최종안 승인(’ 19. 03. 26)

- 해당 지침은 4월 15일 유럽연합 이사회의 승인을 받았으며, 관보를 통해 공포 후 2년 내 각 회원국 국내법에 적용 예정
- 지침은 온라인 플랫폼상 콘텐츠에 대해 정당하고 공정한 보상을 원하는 저작자와 이익과 기술 혁신 및 표현의 자유를 추구하는 플랫폼 사업자 간의 균형을 도모하기 위한 것임

## 주요 내용

- **(언론출판물)** 주로 언론의 성격을 가진 어문 저작물로 구성되어있는 편집물을 의미하나, 기타 저작물이나 보호의 대상이 되는 저작물도 포함될 수 있음 (학술 목적 정기간행물 제외)
- **(정보사회서비스)** 통상적으로 서비스 이용자가 개별적으로 요청할 경우 전자수단을 통해 원거리에서 유료로 제공되는 모든 서비스를 의미 (EU 지침 2015/1535 제1조 제1항 제b호)
- **(온라인콘텐츠 공유서비스 제공자)** 영리목적으로 이용자가 보호되는 저작물 또는 그 밖에 보호의 대상이 되는 것을 업로드하여 공중의 이용에 제공하게 하는 것을 주된 목적 또는 그러한 목적 중의 하나로 하는 정보사회서비스 제공자를 말함
- **(텍스트 및 데이터 마이닝)** 학술 연구 목적으로 텍스트 및 데이터 마이닝은 가능
- **(교육 목적 제한)** 수업 설명을 위한 저작물의 디지털 이용을 허용하나 권리자에게 정당한 보상을 해야 함
- **(언론출판물 보호)** 언론출판사의 복제권 및 공중이용제공권은 언론출판물의 사적 이용 또는 비영리 목적으로 이용하는 개인 이용자, 하이퍼링크, 개별 단어 및 매우 짧은 발췌물에는 적용되지 않음
- **(온라인콘텐츠 공유서비스 제공자에 의한 콘텐츠 이용)** 온라인콘텐츠 공유서비스 제공자가 이용자에 의해 업로드된 저작물 또는 보호 대상을 공중에게 전달 또는 공중의 이용에 제공할 경우 권리자로부터 허락을 받아야 함

○ 지침 제15조는 언론출판물(press publications)의 온라인 이용과 관련한 언론출판물 제작자의 권리를 인정하고, 정보사회 서비스 제공자에게 적절한 이익을 분배하도록 규정

- 단, 개별 이용자에 의한 사적 이용 또는 비영리 목적 이용, 하이퍼링크, 개별 단어의 사용 또는 매우 짧은 발췌물(very short extracts)에 대해선 제작자의 권리를 인정하지 않음
- 제15조의 실제 적용에 있어 "매우 짧은 발췌물"의 범위에 관한 문제와 제17조의 효과성에 대한 많은 논란이 제기되고 있음

※ 최근 독일과 스페인이 유사한 저작권 조항을 도입하였는데, 그 효과성에 관한 문제가 제기된 바 있음

○ 지침 제17조는 온라인콘텐츠 공유서비스 제공자(OCSSP, online content-sharing service provider)가 콘텐츠 라이센스 등의 형식을 통해 권리자의 승인을 얻도록 의무화함

- 소셜미디어, 영상 및 음악 공유 사이트, 게임 스트리밍 플랫폼 사업자는 권리자 허락을 얻어야 하며, 면책을 위해 신속한 통지 등 "최선의 노력(best efforts)"을 입증하여야 함
- 단, 비영리 교육 사이트 또는 프라이빗 클라우드 플랫폼, 콘텐츠가 인용, 비평, 캐리커처, 패러디, 패스티시(pastiche) 등을 위하여 이용되었을 경우에는 적용되지 않음
- OCSSP 책임 여부를 판단하기 위해서는 서비스의 유형과 규모, 이용자, 업로드한 저작물의 유형 등을 고려하여야 함
- 회원국들이 해당 조항을 어떻게 유연하게 국내법에 적용할 것인지가 관건이며, "최선의 노력" 등 모호한 용어에 대한 EU 사법재판소 해석 필요

○ 지침은 현행법을 근대화하는 동시에 디지털 단일 시장을 향한 첫 걸음이 될 것임

- 지침 관련 문제에 대해 향후 유럽 집행위원회가 적절한 가이드를 발표할 것으로 기대
- 서비스제공자들은 이미 새로운 지침 준수를 위하여 업로드시 저작물의 보호 필요 여부를 이용자들에게 서술하게 하는 기능 및 필터 도입을 고려하고 있음

참조 : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2016:0593:FIN

## 미국, 생체 인식 관련 개인정보보호 법안 발의

○ 미국 상원의원 Roy Blunt과 Brian Schatz는 “상용 안면인식 프라이버시법안 (CFRPA, Commercial Facial Recognition Privacy Act of 2019)” 발의 (’19.04.05)

- 법안은 생체정보 인식 기술, 특히 안면인식 기반 기술을 대상으로 하며, 생체인증 관련 소비자보호를 위하여 제안된 연방 차원의 최초 법안임

○ 법 제정 목적은 최종 이용자의 동의를 얻지 않은 상태에서 개인의 신원을 확인하고 추적할 수 있는 안면 인식 기술의 이용을 일부 제한하기 위함

- 안면인식 기술은 사회에 새로운 이익을 창출하므로 지속적으로 개발하여야 하나, 얼굴은 개인 정체성을 나타내며 종종 편견의 대상이 되는 생체정보로서 중요하게 다루어져야 하므로, 기업들이 개인의 얼굴을 추적하고 분석하기 위해서는 개인의 동의를 받도록 함

**법안 주요 내용**

- **금지되는 행위 및 일반 요건**
  - 안면인식 기술을 활용하기 위해서는 개인의 “긍정 동의(affirmative consent)”를 받어야 함
    ※ 개인의 긍정 동의는 데이터 수집 및 활용에 관한 자발적·명시적인 동의여야 함
  - 동의를 받는 경우 정보처리자는 최종 이용자가 이해할 수 있도록 안면 인식 데이터의 수집, 저장 및 이용과 관련한 구체적 처리 관행을 상세히 설명하여 통지하여야 함
  - 정보처리자를 대신하여 제3자가 안면 인식 데이터를 수집, 이용 및 저장할 경우 해당 상황에 대한 설명을 포함하여야 함
  - 정보처리자는 안면인식 기술이 해당 서비스 제공에 필수적인 것이 아니면, 동의하지 않았다는 이유로 서비스 제공을 거부할 수 없음
  - 안면인식 정보를 제3자와 공유할 경우 별도의 동의가 필요
- **적용 제외**
  - 안면인식 기술을 사용하지 않는 응용 프로그램으로서, ① 영상 이미지에서 고유한 개인 얼굴의 특징을 분석하거나, ② 고유한 영구 식별자를 할당하거나, ③ 특정 개인을 개별적으로 식별할 수 있는 응용 프로그램에는 적용되지 않음
  - 안면인식 응용 프로그램을 "보안 응용 프로그램" (절도 및 사기 등 범죄 행위방지를 위한 응용 프로그램)으로 사용할 경우 개인의 동의 요건을 적용하지 않음
- **보안 요건 및 집행**
  - FTC(연방거래위원회)와 NIST(기술표준원)은 법의 효력이 발생한 날로부터 180일 이내에 데이터 보안 및 보유 기준을 정하여야 함
  - 법 위반 행위는 공정거래법(FTC Act)에 따른 불공정 또는 기만 행위로 간주

참조:https://www.blunt.senate.gov/news/press-releases/blunt-schatz-introduce-bipartisan-commercial-facial-recognition-privacy-act

## 미국, 알고리즘 책임법(안) 발의

○ 미국 상원은 기업이 개인의 안면 인식이나 광고 타켓팅 등 머신러닝 기반의 시스템을 활용할 경우, 편견을 방지하기 위하여 감사를 시행해야 한다는 내용의 알고리즘 책임법(안) (Algorithmic Accountability Act)을 마련 ('19.04.10)

- 법안은 일반적인 머신러닝 공정설계를 규율하기 위하여 제안되었으며, 이를 위하여 기업들이 주도적으로 AI시스템의 잠적적인 영향을 주도적으로 평가할 것을 요구

  ※ 법안은 Housing and Urban Development社가 페이스북의 광고 타겟팅 시스템이 주택 광고를 보는 개인을 부당하게 제한한다고 주장하면서 페이스북을 고소한지 불과 몇주 만에 제안됨

○ 법안은 머신러닝 시스템의 윤리적 이용과 민감한 소비자 데이터의 프라이버시와 보안을 주요 내용으로 하고 있으며, 기업은 AI툴과 시스템의 "정확성, 공정성, 편견, 차별, 프라이버시 및 보안"을 고려하여야 함

- 머신러닝 모델은 일반적으로 경험적 데이터와 과거 결과에 근거한 결정론적 결과를 도출하기 위하여 대규모 데이터셋을 적용하기 때문에 알고리즘 편견은 다양한 AI시스템내에 존재

- 편향된 AI시스템은 자체적으로 내제된 편견을 식별하거나 개선할 수 없기 때문에 법안은 FTC로 하여금 기업이 자신들의 머신런닝 시스템을 감사하도록 강제할 수 있는 권한을 부여

- 기업이 프라이버시나 개인정보의 보안에 심각한 위험을 가져오는 민감정보 처리의 경우 또는 상당한 규모의 소비자 개인정보를 처리하는 경우 영향평가에 의하여 프라이버시와 보안 위험에 대한 감사를 수행하여야 함

- 법의 적용을 받는 기업은 대규모 정보에 접근하는 대기업으로, 연 5천만불 이상 규모이면서 1백만 명 이상의 사람 또는 디바이스에 관한 정보를 보유하거나, 소비자 정보 매매나 중개를 주된 사업으로 영위하는 기업임

○ 법안에 따라 FTC(연방거래위원회)는 "고도로 민감한" 자동화 시스템을 평가하기 위한 규칙을 제정하여야 함

참조 :
https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf

## 말레이시아, 해외 디지털 서비스에 서비스세 부과

○ 말레이시아는 2019년 4월 외국 서비스업체와 국내 서비스업체 간 형평성을 위하여 새로운 B2C 서비스세 체계를 도입하는 내용의 서비스세법을 개정하였고, 2020년 1월부터 디지털세를 부과하기로 결정

- 새로운 B2C 서비스세 체계는 외국계 서비스 제공자가 말레이시아 내 제공하는 모든 디지털 서비스에 적용되며, 제공한 디지털 서비스 총 가치의 6% 요율로 부과될 예정

**주요 내용**

- **디지털 서비스**
  - 인터넷 또는 기타 전자 네트워크를 통해 제공·구독되는 모든 서비스로, 정보기술을 활용하지 않고는 제공받을 수 없으며 서비스 제공이 본질적으로 자동화된 것을 말함
  - 음악·영상 스트리밍, 클라우드 스토리지 서비스, 온라인상 제공되는 소프트웨어, 디지털 광고 서비스 등이 포함됨
- **외국계 서비스 제공자**
  - 말레이시아 권역 밖에서 소비자에게 디지털 서비스를 제공하는 자를 말함
  - 말레이시아 권역 밖에서 상품을 매매하거나 서비스를 제공하기 위한 온라인 플랫폼을 운영하는 자, 그리고 타인을 대신하여 디지털 서비스 제공에 필요한 거래를 행하는 자도 포함
- **소비자** : ① 말레이시아의 금융기관 또는 기업이 제공하는 신용 또는 체크카드를 이용하여 디지털 서비스의 대가를 지불하고; ② 말레이시아 내 등록된 IP 주소 또는 말레이시아 국가 번호(전화)를 부여받은 국제 모바일폰을 이용하거나, 말레이시아 내 거주하며 디지털 서비스를 획득한 자
- **외국계 서비스 제공자**(FSP, Foreign Service Provider)
  - 말레이시아 내 소비자에게 디지털 서비스를 제공하기 위해서는 의무적으로 등록을 행하여야 하며, 말레이시아 세관 당국 (RMCD)에 서비스세 등록을 해야 함
  - RMCD 등록 이후 FSP는 말레이시아 소비자가 디지털 서비스에 대해 지급한 금액의 6%를 디지털 서비스세로 납부하고, 디지털 서비스 거래 (전자적 또는 종이문서 등 형태 불문) 관련 사항이 포함된 송장(invoice) 또는 서류를 발행하여야 함

○ 이러한 과세 조치로 인하여 말레이시아 소비자들은 외국계 기업이 제공하는 디지털 서비스에 대하여 높은 비용을 부담하게 될 것으로 예상되며,

- 디지털 서비스를 제공하는 외국계 기업은 법안의 효력 발생 전 자신의 서비스가 과세 대상인지 여부를 평가하여야 하는 부담 발생

참조 : https://www.bakermckenzie.com/en/insight/publications/2019/04/service-tax-on-imported-digital-services

## 영국, 정보보호법 위반에 40만 파운드 벌금 부과

○ 영국 개인정보감독기구인 ICO(Information Commissioner's Office)는 정보보호법(Data Protection Act)을 위반한 임신 및 육아 클럽 Bounty社에게 40만 파운드의 벌금 부과('19.04.09)

- Bounty社는 임산부에게 온라인 앱 및 오프라인 서류 등을 통해 개인 데이터를 수집하고, 데이터 중개 서비스를 제공
- ICO는 Bounty社가 마케팅 목적으로 1,400만명 이상의 개인 데이터를 39개 다른 회사와 공유했으며, 사상 최대의 공개 규모(총 3천 5백만 건 이상 개인 데이터 공개)였다고 발표

○ ICO는 Bounty社가 개인정보의 공정하고 합법적 처리를 규정한 GDPR(General Data Protection Regulation) 제5조 제1항 원칙을 위반했다고 결정

- Bounty社의 개인정보 보호정책은 개인정보가 특정되지 않은 제3자와 공유될 수 있다고 규정하고 있는데, Bounty社는 데이터 주체에게 어떤 조직과 어떤 데이터를 공유할 것인지 명확히 고지하지 않았음
- 신용 평가 기관, 마케팅 및 프로파일링 기업과 개인정보를 공유하는 것은 데이터 주체의 합리적인 기대 범위 내에 있다고 볼 수 없으므로 공정성 요건을 충족하지 못하였고, Bounty社가 이를 통해 금전적 이득을 얻었다고 봄

**ICO의 벌금 부과시 고려사항**

① 영향을 받는 데이터 주체의 규모

② 개인 데이터가 다수의 조직과 빈번히 공유되었는지의 여부

③ 행동이 지속되고 연장된 기간

④ 데이터 주체의 잠재적인 취약성

⑤ 공개가 개인정보 보호법상 고지된 내용에 반하며 개인의 합리적기대 범위를 벗어날 가능성이 있는지의 여부

⑥ 데이터의 본질

⑦ 개인이 데이터에 대한 통제권을 상실할 수 있는지의 여부

⑧ 위반 기업의 재무 상태 및 자발적으로 행위를 중단했는지 여부, GDPR, 개인정보 보호 및 전자 통신 규정 준수를 위해 데이터 관련 관행을 변경하였는지의 여부

○ 특히 ICO는 데이터 공유 행위가 고의적으로 이루어져 정보보호법 위반의 우려가 있고, 상당한 피해 및 고통을 초래할 가능성이 있었음에도 불구하고 Bounty社가 위반 방지를 위한 조치를 취하지 않았다고 판단

참조 : https://ico.org.uk/media/action-weve-taken/mpns/2614757/bounty-mpn-20190412.pdf

## EU, 에너지 부문 사이버보안 관련 권고 발표

○ 유럽위원회는 에너지 부문 사이버 보안에 관한 권고 발표

- 최근 EU의회가 입법한 NIS 지침(NIS Directive 2016/1148) 및 EU 사이버보안법(Cybersecurity Act) 관련 권고를 포함
- 기존 기술의 활용 및 국가간 연결된 시스템에 관한 사항 등 에너지 부문의 특성을 고려한 높은 수준의 사이버 보안 가이드 제공
- 에너지 부문의 기술이 급속히 디지털화하고 네트워크 연결이 심화되어 감에 따라, 사이버 공격 및 보안 사고에의 노출 가능성도 높아짐

**주요 내용**

- **에너지 인프라의 실시간 보안 요구사항**

  유럽위원회는 에너지 네트워크 운영자에게 다음 사항을 권고함

  ① 새롭게 구축되는 시스템에는 최신 보안 기준을 적용하고, 기존 시스템에는 보안 조치에 의해 충분히 보호를 받을 수 없을 경우 보완책으로 물리적 보안 조치를 고려할 것

  ② 사이버 보안에 관한 국제 기준을 도입하고, 관련 보안 제품이 상용화되는 즉시 적절한 기술 기준을 적용할 것

  ③ 민간이 보유하고 있는 네트워크에는 실시간 대응에 필요한 서비스 수준을 보장하기 위해 원격 보호제도(teleprotection scheme)를 고려할 것

- **계단형으로 파급될 수 있는 사이버 보안 준비 조치 도입**

  ① 해당 지역의 중요성을 고려하여 IoT 기기를 포함한 새로운 디바이스에 적절한 수준의 사이버 보안을 적용

  ② 사업 연속성을 정기적으로 검토할 경우 사이버 보안의 물리적 효과를 적절히 고려

  ③ 그리드의 아키텍처 및 설계 요건을 수립할 것을 권고함

- **레거시 시스템과 신기술의 결합**

  - 기존 기술 : 30년~60년의 수명을 가지며, 사이버 보안 도입 전 설계된 것
  - 신규 기술 : 최신 디지털 및 스마트 디바이스로 구성된 기술
  - 기술 공급자는 기존 또는 신규 기술 내 보안 문제 발생시 "관련 보안 문제가 알려진 후 즉시 무료로" 해당 문제 해결을 위해 검증된 솔루션을 제공
  - 에너지 네트워크 운영자는 다음 사항을 준비하여야 함

    ① 기존 시스템과 IoT 기기 연결에 따른 위험 분석

    ② 로봇에 의한 악의적 공격에 대응하기 위하여 필요한 조치

    ③ 기존 및 IoT 환경에서 보안 사안을 자동 모니터링하고 분석하는 역량

    ④ 모든 기존 시스템에 관한 정기적인 사이버 보안 위험 분석

    ⑤ 기존 및 IoT 시스템의 소프트웨어와 하드웨어를 최신 버전으로 현행화

참조:https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

# 지능정보사회 해외 법제 동향

기 획 : 한국정보화진흥원 정책본부
지능화법제도팀

발 행 일 : 2019년 5월

1. 본 보고서의 무단전재를 금하며, 가공·인용할 때는 반드시 출처를 「한국정보화진흥원(NIA)」이라고 밝혀 주시기 바랍니다.
2. 본 보고서의 내용은 한국정보화진흥원(NIA)의 공식 견해와 다를 수 있습니다.