2024 Vol.6

PRIVACY REPORT

개인정보보호
월간동향분석

2024년 6월호

KISA 한국인터넷진흥원

PRIVACY REPORT

2024 개인정보보호 월간동향분석

| CONTENTS |

2024년 6월호

데이터 수집

중국-미국 간 데이터 관련 이슈 동향

[목 차]

1. 개요

▌중국과 미국이 자국의 데이터 보안을 위해 디지털 장벽을 높이면서 인터넷 세상이 진영에 따라 나뉘는 '스플린터넷(Splinternet)*' 현상이 뚜렷해지고 있음

* '나누다'라는 뜻의 스플릿(split)과 인터넷(Internet)의 합성어

- 디지털 시대에 데이터는 혁신을 촉진하는 전략적 자산으로 부상했으며, 이에 데이터 보안은 국가 안보에 직접적인 영향을 미치는 주요 요소가 됨
- 중국은 방화벽을 통해 자국민들을 타국 정보로부터 분리시키고 있으며, 미국은 중국 앱이 미국인의 데이터를 수집하여 악용하는 것을 막기 위해 규제 수위를 높이고 있음

▌미국은 중국 IT 플랫폼, 커넥티드 차량, 바이오 기업 등을 통해 자국민의 민감한 데이터가 중국에 넘어갈 것을 우려하여 해당 부문에서의 규제를 강화하는 추세

- 중국은 데이터 관련 법*를 통해 데이터 현지화(data localization)를 명문화함으로써 해외 사업자의 인터넷 데이터를 반드시 중국에 보관하도록 하고, 필요시 정부가 기업 데이터를 획득할 수 있도록 하는 등 중국 정부가 데이터 통제를 용이하게 할 수 있는 구조를 형성

  * 중국 네트워크안전법(网络安全法) 제37조 및 개인정보보호법(个人信息保护法) 제40조에서는 핵심정보인프라시설 운영자가 중국 내에서 운영하여 수집하고 생산한 개인정보 및 중요 데이터를 중국 역내에 저장해하도록 규정하고 있음

- 미국 정부는 중국이 이러한 국가 데이터 보안법을 악용해 미국 시민들로부터 상당한 양의 개인정보를 수집하는 행위가 국가 안보에 위협이 된다고 강조하며, 중국 기업(IT 플랫폼, 커넥티드 차량, 바이오 기업 등)을 대상으로 규제 및 제재를 강화

2. 중국-미국 간 데이터 관련 이슈 동향

(1) 중국 IT 플랫폼의 대규모 데이터 수집 관련 이슈

▌바이든 행정부는 인기 소셜 미디어 플랫폼 TikTok(틱톡)에서 수집한 미국인 정보가 중국 정부로 유출되는 것을 방지하고자 일명 '틱톡금지법'으로 일컬어지는 법안에 서명('24.4.24.)

- '16년 틱톡이 미국에서 서비스를 시작한 이후 미국 사용자가 급격히 확산하며 중국 공산당이 중국에 본사를 둔 틱톡의 모회사 ByteDance(바이트댄스)를 통해 미국 사용자 데이터에 접근할 수 있다는 우려가 꾸준히 제기되어 옴
  - 특히 틱톡이 사용자의 거주지, 직장, 인간관계 등을 추적하며, 중국 정부에 비판적이거나 민감한 문제를 다루는 콘텐츠 노출을 검열·제한한다는 의혹이 제기
  - '20년 트럼프 행정부 집권 당시에도 국가안보, 외교 정책 및 경제 위협을 이유로 앱스토어에서의 틱톡 앱 다운로드를 금지하는 행정명령*을 발동했으나, 법원에 의해 무효화된 바 있음
    * Executive Order on Addressing the Threat Posed by TikTok
- 이에 바이트댄스가 1년 내 틱톡 앱을 미국 자본에 매각하지 않으면 미국 내 사업을 금지하는 내용의 법안(틱톡금지법)*이 바이든 대통령의 서명으로 제정
  * 바이든 대통령은 '24년 4월 24일에 '국가안보 추가 예산안(House Resolution 815 Making emergency supplemental appropriations for the fiscal year ending September 30, 2024, and for other purposes)'에 서명했으며, 동 예산안은 제1절(Division I) 하에 '2024년 외국 적대국으로부터의 미국인 데이터보호법(Protecting Americans' Data from Foreign Adversaries Act of 2024)'을 포함하고 있음
  - 동 법에 따르면 바이트댄스는 9개월 안으로('25년 1월 19일까지) 틱톡을 미국 자본에 매각해야 하며, 미국 대통령은 1회에 한하여 매각 시한을 3개월 연장할 수 있음
  - 한편 바이트댄스는 틱톡금지법의 시행을 막고자 올해 소송을 제기할 예정
  - 다만 민감한 사안인 만큼 소송에서 패소하는 측이 대법원에 항고하는 등 분쟁이 장기화될 가능성이 크기에, 실제로 동 법안이 '26년 안으로 시행되기는 어려울 것으로 예측
- 틱톡금지법을 둘러싼 미국 내 찬반 논란이 거센 가운데, 찬성론자들은 틱톡에 대한 안보 우려가 상당 부분 근거가 있다고 평가
  - 존스홉킨스대 정보보안연구소의 사이버 보안 전문가 안톤 다부라(Anton Dahbura)는 '미국의 주요기반시설은 원자력 발전소나 군사 시설 등에 국한되지 않고 식품, 제약, 금융기관 등도 포함된다'고 언급하며 '틱톡이 수집하는 사용자 데이터를 통해 특정인을 표적으로 삼은 피싱 공격 등이 가능하다'고 주장

- 미국 전략국제문제연구소(CSIS)의 제임스 앤드루 루이스(James Andrew Lewis) 전략기술프로그램 디렉터는 '틱톡이 미국 정치를 혼란스럽게 하기 위한 중국 정부의 영향력 공작의 플랫폼으로, 미국인의 개인정보를 수집하는 데 쓰인다'며 틱톡의 위험성을 강조

- 한편, 틱톡이 미국의 안보를 위협한다는 것에 대한 명확한 증거 부족 및 표현의 자유 침해 가능성 등을 우려하는 의견도 다수
  - 틱톡의 부상에 관한 저서를 출판한 저널리스트 크리스 스토켈-워커(Chris Stokel-Walker)는 '수년 동안 틱톡과 중국 정부 간 연관성을 찾기 위해 노력해 왔으나 그 누구도 아직까지 결정적인 증거를 찾지 못했다'고 언급
  - 미국시민자유연맹(ACLU)의 제나 레벤토프(Jenna Leventoff)는 '수억 명의 미국인이 자신을 표현하는 데 사용하는 플랫폼을 금지하는 것은 수정헌법 제1조에서 보장하고 있는 권리에 치명적인 결과를 초래할 것'이라고 비판
- 미국 정보기술과혁신재단(ITIF)은 중국 IT 기업이 보유한 데이터에 대한 중국 정부의 잠재적 접근에 대한 우려가 정당함을 인정한 한편, 이에 대한 논쟁이 주로 중국 법률에 대한 광범위한 분석, 일화적인 언론 보도 및 중앙정보국의 모호한 진술에만 근거하고 있음을 지적
  - 앞서 미국 정보 당국자들은 기밀 브리핑에서 상원의원들에게 중국 정부가 바이트댄스에 대한 직접적이고 절대적인 통제권을 이용해 사용자를 감시할 수 있다고 언급
  - 그러나 ITIF는 중국 정부의 민간 부문 데이터 및 서비스 접근과 관련해 공개된 명확하고 상세한 정보가 부족하므로, 바이든 행정부가 선별적으로 기밀이 해제된 정보를 제공해 투명성을 높일 필요가 있다고 주장

▌'24년 5월 호주 싱크탱크 연구소(ASPI)가 발간한 보고서에 따르면 중국 공산당이 국가 선전 활동을 강화하고자 IT 플랫폼 기업과의 연계로 국내외 데이터를 대규모 수집하고 있으며, 특히 미국에서 서비스 중인 이커머스 플랫폼 테무(Temu)가 공산당과 밀접한 연결성이 있다고 분석

- 동 보고서에 의하면 중국 공산당은 국내외 다양한 출처의 데이터를 활용하고 신흥 기술에 투자함으로써 글로벌 정보 생태계를 지배하고자 하며, 동시에 중국 기술과 기업이 글로벌 데이터 발전 및 데이터 공유의 중심이 될 수 있도록 하는 데 초점을 두고 있음
  - 특히 공산당은 계속해서 진화하는 정보 생태계에 맞추어 접근 전략을 조정
  - 대표적으로 기존의 '당이 통제하는 미디어'에서 '당이 통제하는 데이터(党管数据)'로 전략 초점을 바꿈으로써, 데이터를 단순히 상업적 활용을 위한 자원이 아니라 선전 활동에 활용 가능한 전략적 자산으로 보는 시각이 확대
  - 이러한 당의 데이터 통제 전략의 전선에는 중국 공산당 중앙위원회가 통제하는 국유기업인

인민데이터관리유한공사(人民数据管理有限公司)가 있음

- 중국 공산당은 테무와 같이 중국 밖에서 운영되는 자회사에서 수집한 데이터까지 통제권을 확장함으로써 여론의 흐름을 효과적으로 측정하여 사회적 트렌드와 선호도에 대한 전례 없는 통찰력을 확보하고자 함
  - 인민데이터관리유한공사는 정부, 기업, 기관 간 데이터 공유를 보장하는 데 중점을 두고 있으며, 현재 국방부·문화관광부·국가안전부 등의 정부 파트너와 30개 이상의 기업 파트너를 보유하고 있으며, 중국 전역 15개 이상의 빅데이터 교환 센터와 협력 계약을 체결
  - 이러한 기업 파트너 중 대표적인 예시로 이커머스 플랫폼 테무를 운영하는 웨일코 주식회사(Whaleco Technology Ltd.)의 모회사인 핀둬둬(PDD) 홀딩스가 있음
  - 테무 앱은 '24년 4월 기준 구글에서 1억 회 이상 다운로드 되었으며, 미국 월간 사용자 수는 약 7,750만 명에 달함
- 테무와 PDD 홀딩스는 데이터 수집 활동으로 인하여 국제적 논란의 대상이 되고 있음
  - '23년 3월, 구글은 PDD 앱에서 악성 소프트웨어가 발견되었다는 보고로 인해 구글 앱스토어에서 PDD 앱을 금지
  - 애플 또한 테무가 ▲개인정보보호 의무를 위반하고 ▲데이터 사용 방식에 대해 사용자를 오도했으며 ▲사용자에게 인터넷에서 추적받지 않을 선택지를 제공하지 않았다고 밝힌 바 있음
- PDD 홀딩스와 그 자회사가 국영 인민데이터 플랫폼을 통해 공유하는 데이터의 유형은 공개적으로 이용 가능한 출처에서 확인되지 않음
  - 그러나 테무의 개인정보 처리방침을 고려했을 때, PDD 홀딩스와 인민데이터관리유한공사 간의 데이터 공유 계약에는 테무를 통해 생성된 데이터 공유도 포함될 수 있다고 가정하는 것이 합리적이라는 것이 ASPI의 분석
  - 테무의 개인정보 처리방침은 개인정보가 '기업 모회사, 자회사 및 계열사'는 물론 '규정 준수 및 보호 목적에 필요하거나 적절하다고 판단되는 법 집행기관, 정부 기관 및 민간 당사자'와 공유할 수 있다고 명시하고 있음
  - 여기서 '규정 준수 및 보호 목적'에는 정부 당국의 소환장 또는 요청에 응하는 것과 같은 관련 법률, 합법적인 요청 및 법적 절차를 준수하는 것이 포함됨
- 테무는 의사결정 습관과 같은 소비자 선호도를 나타내는 데이터를 저장하고 있는데, 이러한 데이터는 지리적 위치에 따라 특정 사용자의 프로필 데이터를 포함하기도 함
  - 이는 특정 인구 통계를 타겟팅하는 데 도움이 될 수 있으며, 국가 기관이 테무 플랫폼에 생성된 글로벌 사용자 데이터에 접근하여 활용할 경우 해외 선전 및 정보 캠페인에 활용 가능*

* 예를 들어, 선거를 앞둔 특정 국가, 특정 언어 그룹 또는 세계적으로 중요한 이슈에 대해 특정 지역에

초점을 맞춘 해외 선전 및 정보 캠페인이 가능

- 미국을 포함한 기타 관할권에서는 데이터 브로커 생태계와 관련된 '공급업체 기반 국가 안보 위험(vendor-based national security risks)'을 해결하기 위한 프레임워크를 개발하고 있으며, 여기에는 테무와 같은 공급업체가 포함될 가능성이 높음

(2) 중국산 커넥티드 차량(스마트카) 규제 동향

▌바이든 행정부, 자국의 운전자/승객의 개인정보 수집 우려에 따라 중국산 커넥티드 차량에 대한 조사 및 대책 수립을 지시

- 미국은 커넥티드 차량이 카메라와 센서를 통해 수집하는 정보뿐만 아니라 승객 및 운전자와 관련된 대량의 민감한 정보를 수집하는 것에 대해 우려하고 있음
  - 이러한 우려는 커넥티드 차량이 주요기반시설에 대한 정보를 수집할 수 있는 능력과 원격으로 차량을 조종·비활성화할 수 있는 능력을 탑재하게 되며 더욱 가중
- '19년 5월, 미 트럼프 행정부는 행정명령 13873호 '정보통신 기술 및 서비스(ICTS, Information and Communications Technology and Services) 공급망 보안'을 발표한 바 있음
  - 이 행정명령은 미국 공급망에서 외국의 적대적 ICTS가 제한 없이 배치되고 사용되는 것을 국가 비상사태로 선언하고, 상무부 장관에게 국가안보에 중대한 위험을 초래하는 외국의 적대적 ICTS와 관련된 특정 거래를 금지하도록 하는 권한을 위임
  - 이후 상무부는 외국 적대자의 개입으로 인해 부당하거나 허용할 수 없는 위험이 있는지를 판단하기 위해 ICTS 거래를 검토할 수 있는 절차를 마련
- '24년 2월, 바이든 행정부는 상무부에 중국과 같은 우려 국가의 기술을 활용하는 커넥티드 차량으로 발생하는 잠재적 보안 위협에 대한 조사를 주도하도록 하고 필요한 조치를 취하도록 지시
  - 백악관은 성명에서 "커넥티드 차량은 운전자와 승객에 대한 방대한 양의 민감한 데이터를 수집하고, 정기적으로 카메라와 센서를 사용하여 미국의 인프라에 대한 자세한 정보를 기록하고, 중요한 인프라와 직접 상호 작용하며, 원격으로 조종하거나 비활성화할 수 있다"고 언급
  - 또한 "중국을 포함한 우려 국가의 기술과 데이터 시스템에 의존하는 커넥티드 차량은 국가 안보를 위협하는 방식으로 악용될 수 있다"고 덧붙임
  - 고위 행정부 관리들은 현재 우려 국가와 연결된 차량(커넥티드 차량) 수가 아직 적더라도, 향후 미국 도로에 이러한 차량이 더욱 많이 다니기 전에 조치하는 것이 중요함을 강조
- 이에 행정부와 상무부는 조사를 지원하고자 커넥티드 차량용 ICTS 규정 마련을 위한 '규정

제정안 사전통지문(ANPRM, Advance Notice of Proposed Rulemaking)'을 공개

- 미 상무부 산업안보국(BIS)은 ANPRM을 발표하며 업계 이해관계자로부터 규제에 가장 적합한 기술 및 시장 참여자*를 결정하는 데 도움이 될 피드백을 요청

  * 여기에는 자동차 주문자 상표 부착 생산업체(OEM), 1차, 2차, 3차 공급업체, 애프터마켓 부품 회사, 서비스 제공업체가 포함

- BIS는 ▲중국의 사이버 스파이 활동 ▲국가가 민간 기업을 동원하여 목적을 달성할 수 있는 법적 구조 ▲중국 내 자동차 제조업체가 지리적 위치 정보를 포함한 실시간 차량 데이터를 중국 정부 모니터링 센터에 전송할 법적 의무가 있다는 점을 들어 중국 커넥티드 차량의 ICTS를 중대한 우려 사항으로 강조

  - 또한, 해외 공격자가 악용할 경우 부당하거나 허용할 수 없는 위험을 초래할 가능성이 가장 높은 자동차 소프트웨어 시스템으로 ▲차량 운영 체제 ▲텔레매틱스 시스템 ▲첨단 주행 보조 시스템 ▲자율 주행 시스템 ▲위성 또는 셀룰러 통신 시스템 ▲배터리 관리 시스템 등을 선정

- BIS는 특히 ▲커넥티드 차량에 필수적인 ICTS와 관련된 '외국의 적대적' 당사자와의 특정 거래를 금지하고 ▲시장 참여자가 국가 안보 위험을 충분히 완화할 수 있는 경우 금지된 거래를 허용하는 규칙을 제안하는 방안을 고려 중

- 한편 '24년 5월 미 상무장관 지나 라이몬도(Gina Raimondo)는 상무부가 '24년 가을에 중국의 커넥티드 차량에 대한 제안된 규칙을 발표할 계획이라고 언급

  - 라이몬도 상무장관은 상원위원회에서 중국 커넥티드 차량이 국가안보에 미치는 위험이 상당히 심각하여 조치를 취하기로 결정했다고 하며, 미국이 중국산 자동차 수입을 금지하거나 제한을 가하는 '극단적인 조치'를 취하는 것까지 고려하고 있음을 암시

- 또한, '24년 5월 미 행정부는 전기차 배터리, 부품, 주요 광물에 대한 새로운 관세를 부과하는 것과 함께 중국산 자동차에 대한 관세를 4배로 인상한다고 별도로 발표[1)]

(3) 생체인식정보·유전자 정보 수집 규제 동향

▌미 상·하원, 미국인 유전정보를 중국에 제공할 수 있다는 우려에 따른 중국 바이오 기업과의 거래 제한 법안인 Biosecure Act 발의

- (하원 발의 법안) '24년 1월, 미 하원 중국 특별위원회가 연방 자금 지원을 받는 의료 서비스 제공자가 국가안보에 위협이 되는 '외국의 적대적인 바이오테크 기업'에 대한 접근을

1) Reuters, Biden sharply hikes US tariffs on an array of Chinese imports, 2024.5.15. 참고 (URL: https://www.reuters.com/markets/us/biden-sharply-hikes-us-tariffs-billions-chinese-chips-cars-2024-05-14/)

허용하지 못하도록 제한하는 내용을 담은 'Biosecure Act(바이오보안법)'을 발의

- 해당 법안을 발의한 의원 중 한 명인 민주당 라자 크리슈나무르티(Raja Krishnamoorthi) 의원은 이 법안이 미국의 바이오 경제와 국가안보를 보호하고 게놈 데이터를 안전하게 보호하는 첫 번째 단계라고 언급
- 바이오보안법은 중국 정부와 연계된 것으로 의심되는 중국의 바이오테크 기업을 명시적으로 겨냥하고 있음
- 1월에 발의된 법안은 우려기업으로 ▲WuXi AppTec(우시 앱텍) ▲Beijing Genomics Institute(베이징 유전체학 연구소) ▲Complete Genomics(컴플리트 지노믹스) ▲MGI 등 4개 기업*을 명시

  * 중국인민해방군과 연계된 위 기업들이 미국인의 유전자 정보를 중국 당국에 넘길 수 있다고 의심됨

- 이후 '24년 5월, 크리슈나무르티 의원과 웬스트럽(Wenstrup) 의원은 '32년 1월 1일까지 중국 기반 기업과의 기존 계약에 여유를 주는 조항이 포함된 바이오보안법안 수정안을 발표
  - 해당 법안은 지난 1월에 발표된 법안의 우려 기업 리스트에 우시 바이오로직스(WuXi Biologics)를 추가하였으며, 이러한 기업과 협력하는 바이오 제약 회사도 미국 정부와 협력하는 것을 금지하는 내용을 담고 있음
- (상원 발의 법안) '24년 3월에는 하원이 발의한 법안과 유사한 내용으로 상원 국토안보위원회가 자국민의 생체 데이터와 유전자 정보를 중국으로부터 보호하기 위해 만든 '바이오보안법(Biosecure Act)'을 가결한 바 있음
  - 동 법안은 연방정부가 국가안보를 위협하는 것으로 판단한 중국 바이오 기업과 계약을 체결하는 것을 금지하고 있음
  - 또한, 문제 기업의 장비나 서비스를 이용하는 기업과도 정부 계약을 체결할 수 없고, 이들 기업에 차관이나 보조금을 제공하는 것도 금지
- 바이오보안법이 최종 제정되기 위해서는 상·하원 의결을 거친 다음 대통령 서명을 받아야 하며, 중간에 일부 내용이 수정될 가능성이 있어 다소 시간이 걸릴 것으로 예상
  - 그러나 하원과 상원이 모두 발의된 바이오보안법안을 의결함에 따라 미국의 중국 바이오기업 제재 가능성은 더 커진 것으로 보인다는 평가
- 중국 바이오기업의 직접적 타격 이외에도 많은 제약회사가 자사 제품에서 중국 소재 계약 제조업체에 의존하는 비율이 높아 법안이 적용되면 업계에 광범위한 영향을 미칠 것
  - 바이오의약품 위탁생산업체인 우시 앱텍은 미 펜실베니아주와 캘리포니아주 등 미 전역에서 시설을 운영하며 매출의 66% 가량이 미국 시장에서 발생하여 큰 타격 예상
  - 임산부의 다운증후군 산전 검사에 사용되는 니프티검사(NIPT) 선두주자인 BGI의 미국

판매도 막히게 될 것

- 우시 앱텍과의 파트너십을 보유한 머크(Merck), 아이오벤스 바이오테라퓨틱스(Iovance Biotherapeutics), 키버나 테라퓨틱스(Kyverna Therapeutics) 등의 기업들은 향후 잠재적 영향에 대해 미 SEC와 논의를 진행 중

3. 결론 및 전망

▌미국의 자국민 데이터 보호를 위한 중국 기업 규제 강화 기조는 한동안 지속될 것으로 예상

- (IT 플랫폼) 틱톡이 미국에서 사업을 시작한 이후 지속적인 보안 우려가 제기되어 왔지만 최근 틱톡금지법 발효는 단일 회사를 대상으로 법을 만들어 규제한 거의 첫 번째 사례라는 점에서 놀라운 결과
  - 여러 플랫폼에서 일어나는 안보 위협에 대비한 포괄적인 법안이 아닌 중국계인 틱톡만 겨냥한 매우 좁은 형태의 규제
  - 데이터 안보의 측면 이외 11월 미 대선을 앞두고 정치적 상징성도 크다는 평가
- 또한, 초저가 전략으로 미국에서 빠르게 사용자 수를 늘려가던 중국 이커머스 앱 테무도 모회사인 PDD 홀딩스가 중국 정부와의 밀접하게 연결되어 미국 사용자 데이터를 공유할 수 있는 가능성이 크다는 분석 의견이 제기
- (커넥티드 차량) 수많은 센서와 칩이 연결된 커넥티드 차량에서 수집된 미국인의 많은 데이터가 중국으로 바로 들어갈 수 있다는 우려로 미 정부는 올해 2월 중국산 커넥티드 차량 관련 보안 위협에 대한 조사를 시작하였으며, 올해 가을 관련 규정을 발표할 계획
  - 미 상무장관은 중국산 자동차 수입을 금지하거나 제한하는 강한 제재가 이루어질 수도 있다고 밝힌 바 있음
- (바이오기업) 미국인의 생체인식·유전 정보가 중국에 유출되는 것을 막고자 중국 정부와 연계되었다고 의심되는 기업과의 협력, 계약 등을 금지하는 내용의 바이오보안법(Biosecure Act)이 상원과 하원에서 각각 발의
  - 최종 법 제정까지는 많은 시간이 걸릴 것으로 예상되나 상원과 하원 모두 유사한 법안을 추진하고자 한다는 점에서 중국 바이오기업에 대한 제재 가능성이 높음

출처 |

1. ASPI, Truth and reality with Chinese characteristics: The building blocks of the propaganda system enabling CCP information campaigns, 2024.5.1.
2. BioSpace, Companies Detail Potential Fallout as Pressure on WuXi AppTec Builds, 2024.4.4.
3. Council on Foreign Relations, The U.S. Governement Banned TikTok From Federal Devices. What's Next?, 2023.1.13.
4. Hogan Lowells, Biden Administration investigates national security risks of Chinese connected vehicles in the U.S., 2024.2.29.
5. H.R.7085 – BIOSECURE Act, 2024.1.25.
6. ITIF, If China Is Weaponizing Access to U.S. Data, We Need to See the Evidence, 2024.4.5.
7. Politico, Booming Chinese shopping app faces Western scrutiny over data security, 2023.7.24.
8. Reuters, Biden sharply hikes US tariffs on an array of Chinese imports, 2024.5.15.
9. Reuters, US House bill would curb genetic info sharing with China's Wuxi Apptec, BGI, 2024.2.27.
10. Reuters, US to issue rules on Chinese connected vehicles this autumn, 2024.5.16.
11. S.3558 – A bill to prohibit contracting with certain biotechnology providers, and for other purposes, 2023.12.20.
12. The Verge, Biden signs TikTok 'ban' bill into law, starting the clock for ByteDance to divest it, 2024.4.25.
13. THE WHITE HOUSE, FACT SHEET: Biden-Harris Administration Takes Action to Address Risks of Autos from China and Other Countries of Concern, 2024.02.29.
14. VOA News, US Investigating Potential Security Threats From Connected Cars, 2024.2.29.
15. 국민일보, "운전자 정보 샌다"…美 올가을 '中 커넥티드 카' 규제, 2024.5.16.
16. 매일경제, "우리 국민 건강 데이터 손대지 마"···이번엔 바이오 싸움 나선 美中, 2024.3.27.
17. 세계일보, 틱톡금지법·라인 사태… '데이터 주권'에 높아지는 e국경 [세계는 지금], 2024.05.10.

EU AI 법 및 GDPR의 상관관계 분석

[목 차]

1. 개요 및 EU AI 법 추진 경과

▌인공지능(AI) 기술이 빠르게 발전하고 상용화됨에 따라 세계 각국 정부는 AI를 규제해야 할 필요성에 대해 고심

- 미국, 영국, 중국 등은 AI 전략과 가이드라인을 도입했으며, 다른 국가들도 AI 규제 프레임워크를 마련하는 과정에 있음
  - 미국은 AI 행정명령을 발표했으며, 영국 정부는 구속력이 없는 AI 원칙을 선언, 중국은 기술 발전을 가속화하기 위해 산업 친화적인 AI 규제를 시행한 바 있음
- 이러한 맥락에서 EU에서 최근 입법을 확정한 Artificial Intelligence Act(이하 EU AI 법)는 세계 최초의 포괄적인 AI 규제 프레임워크이며, 선구적인 조치로 평가받고 있음
  - EU AI 법은 AI 사용에 대해 위험 기반(risk-based) 접근방식을 택한 점이 특징
  - 즉, AI 기술 자체를 제한하기보다는 기업이 AI 기술을 사용하는 방법 및 목적에 대한 기준을 설정하는 데 중점을 두고 있음

EU AI 법은 총 12개의 장으로 이루어진 본문, 13장의 부속서(annex) 및 171개 전문 조항으로 구성된 방대한 규범으로, 현재 법으로 제정되기까지 EU 관보* 게재만을 앞둔 상황

* 유럽의회(European Parliament)와 EU 이사회(European Council)의 공식 승인 후 법안은 EU 관보인 Official Journal of the European Union에 게재됨으로써 제정

- '20년 10월, EU 이사회는 디지털 전환에 대한 논의를 거친 후 EU 집행위원회(EC, European Commission)에 다음을 요청
  - AI 연구, 혁신 및 배포에 관한 유럽 및 각국의 공공·민간 투자를 확보할 수 있는 방법을 제안할 것
  - 우수성(excellence)을 기반으로 유럽 연구기관 간 조정과 시너지 효과를 보장할 것
  - 고위험(high-risk) AI 시스템에 대한 명확하고 객관적인 정의를 제공할 것
- 이에 EU 집행위원회는 '21년 4월, AI에 대한 신뢰도를 향상하고 AI 기술의 개발 및 성장을 촉진하기 위해 AI에 관한 일관적인 표준을 설정하는 법안을 제안
- '22년 12월, EU 이사회는 EU AI 법(안)에 대한 입장을 채택했으며, 이후 EU 집행위원회와 유럽의회, EU 이사회는 3자 협의 끝에 법률 최종안에 합의
  - 특히 유럽의회가 AI 법안을 검토하는 과정에서 생성형 AI 챗봇 ChatGPT의 부상으로 생성형 AI 규제의 시급성이 대두되며, 법안에 생성형 AI에 관한 내용을 추가로 반영
  - '21년 당시 EU 집행위원회가 제출한 EU AI 법안 초안은 생성형 AI에 대해 별도로 언급하지 않았으며, AI 시스템을 포괄적으로 정의하고 있었음
  - 이후 동법(안)은 '24년 6월 유럽의회와 EU 이사회(the Council) 의장의 최종 서명을 득함
- EU AI 법은 예정된 EU 관보 게재 후 20일이 지난 시점에 효력이 발생하며, 다음과 같은 일부 조항을 제외하고 발효 24개월 후('26년 6월)부터 전면 적용
  - 금지된 AI 시스템(Prohibited AI System)에 대한 규정은 AI 법이 시행된 후 6개월 후로부터 적용('24년 12월)
  - 범용 AI 시스템(General-Purpose AI System, GPAI)에 대한 규정은 12개월 후부터 적용('25년 6월)
  - 부속서 III에서 열거한 AI 기술 목록에 따라 분류된 고위험 AI 시스템(High-Risk AI System)은 AI 법 시행 후 24개월 후부터 규제 대상이 됨('26년 6월)
  - 부속서 II의 EU 조정법(harmonised legislation) 목록에 따라 분류된 고위험 시스템은 AI 법 시행 후 36개월 후부터 규제 대상이 됨('27년 6월)

표 1 EU AI 법 입법 추진 경과('24.6. 기준)

날짜	주요 내용
'21.4.21.	• EU 집행위원회, EU AI 법안 제안 및 의견 수렴 절차 개시
'21.8.6.	• EU 집행위원회, EU AI 법안에 대한 공개 자문 기간 종료 (304건의 의견 접수)
'21.8.6.	• 유럽의회 시민권 및 헌법정책국, 윤리적·법적 관점에서 생체인식기술 사용 분석 연구 발간
'21.11.29.	• EU 집행위원회, ▲소셜 스코어 ▲생체인식 시스템 ▲고위험 앱 관련 변경 사항이 반영된 초안을 EU 이사회 및 유럽의회에 제출
'22.4.20.	• 유럽의회 내부시장위원회(IMCO) 및 시민자유위원회(LIBE), 보고서 초안 발표
'22.5.13.	• EU 이사회, 이미지 및 음성 이해, 오디오 및 비디오 생성 등에 관한 수정안 발표
'22.9.5.	• 유럽의회 법제위원회, 검토 마지막 위원회로써 AI 법안 채택
'22.12.6.	• EU 이사회, 만장일치로 일반합의(general approach) 채택
'23.6.14.	• 유럽의회, AI 법안에 대해 찬성 499표, 반대 28표, 기권 93표로 가결
'23.12.9.	• 유럽의회 및 EU 이사회, 법률 최종안에 잠정 합의
'24.2.13.	• 유럽의회 내부시장위원회 및 시민자유위원회, 71:8로 EU 회원국과 법안 협상 결과 승인
'24.3.13.	• 유럽의회 최종 채택
'24.5.21.	• EU 이사회 최종 승인
'24.6.13.	• 유럽의회 및 EU 이사회 의장, AI 법에 서명

출처: Timeline of Developments(FLI, 2024), 넥스텔리전스(주) 정리

▌이에 본고에서는 EU AI 법의 주요 내용을 소개하고, EU의 기존 개인정보보호 규제 프레임워크인 GDPR과의 AI 법의 상호관계 및 쟁점을 점검하고자 함

2. EU AI 법 주요 내용

(1) 일반 규정

▌(정의) EU AI 법은 AI 시스템, 고위험 AI 시스템, 및 범용 AI 모델에 대한 정의를 제공

표 2 주요 용어 정의

용어	정의
AI 시스템 (제3조제1항)	• 다양한 수준의 자율성을 가지고 작동하도록 설계되었으며 배치(deploy) 후 적응력을 발휘할 수 있고 명시적 또는 암묵적 목표를 위해 수신한 입력으로부터 물리적 또는 가상환경에 영향을 미칠 수 있는 예측, 콘텐츠, 추천 또는 결정과 같은 출력을 생성하는 방법을 추론하는 머신 기반 시스템
고위험 AI 시스템 (제6조)	• AI 시스템이 다음 주 가지 조건을 충족하는 경우 고위험군으로 간주: – AI 시스템이 ① AI 법의 부속서 II에 나열된 특정 EU 법률(예: 민간 항공, 차량 보안, 장난감, 해양 장비, 리프트, 개인 보호 장비 및 의료 기기)의 적용을 받는 제품(또는 제품의 안전 구성 요소로 사용하려는 경우), – ② 해당 특정 법률에 따라 해당 제품을 시장에 출시하거나 서비스에 투입하기 위해 제3자 적합성 평가를 받아야 하는 경우 • 이 외에도 부속서 III에서 열거하고 있는 AI 시스템 또한 고위험 AI 시스템으로 간주
범용 AI 모델 (제3조제63항)	• 대규모 자체 감독을 사용하여 대량의 데이터로 학습된 AI 모델로서 상당한 일반성을 나타내며 모델이 시장에 출시되는 방식에 관계없이 다양한 고유 작업을 능숙하게 수행할 수 있고 다양한 다운스트림 시스템 또는 애플리케이션에 통합될 수 있는 AI 모델을 포함하며, 시장에 출시되기 전에 연구, 개발 또는 프로토타이핑 활동에 사용되는 AI 모델은 제외

(적용 범위) AI 시스템 공급자, 제조업체, 사용자, 수입업체 및 유통업체 등을 포함한 AI 운영자(operator)에게 AI 법이 적용

- AI 시스템이 EU 시장에 출시되거나 그 사용이 EU에 거주하는 사람들에게 영향을 미치는 한, EU 역내·외 공공 및 민간 행위자 모두에게 동법이 적용
  - 이는 공급자(provider)* 및 사용자(deployer)**에게 모두 적용되는 사항
    * EU 시장에서 AI 시스템을 개발하거나 제공하는 자 또는 법인
    ** 비전문적 활동 과정에서 사용되는 경우를 제외하고 권한 하에 AI 시스템을 사용하는 자 또는 법인
  - 또한 제3국의 AI 시스템을 EU 시장에 출시하거나 제공하는 수입업체(importer)* 및 유통업체(distributor)**에게도 적용
    * 제3국에 설립된 자 또는 법인의 이름 또는 상표를 사용하는 AI 시스템을 시장에 출시하는 자로 EU에 소재
    ** 공급자 또는 수입업체가 아닌 공급망에 속한 자 또는 법인으로, EU 시장에서 AI 시스템을 제공
- 단, ▲과학적 연구 목적으로만 사용하는 AI 모델 또는 시스템 ▲순수하게 가정 활동을 위해 사용되는 AI 시스템 ▲군사, 방어 또는 국가 안보 목적으로만 사용되는 AI 시스템은 적용 범위에서 제외하고 있음

(2) 위험 기반 규제

▌(개요) EU AI 법은 AI 시스템과 모델을 4가지 카테고리로 분류하여 위험 수준에 비례해 규제 수행

- 사람의 안전에 허용할 수 없는 위험(수용 불가 위험)을 초래하는 AI 시스템은 엄격히 금지하고 있음
- 동 법에서 규정하는 대부분 의무사항은 고위험 AI 시스템을 대상으로 하고 있음
- 제한적인 위험성을 가진 AI 시스템과 관련된 공급자에게는 경량의 투명성 의무를 부과함
- 최소한의 위험수준을 가진 AI 시스템은 동 법에서 별도로 규제하고 있지 않음

표 3 위험 수준 기반 AI 시스템 분류

위험 수준	분류 기준 및 의무	예시
최소위험/무위험 (minimal risk)	• ▲제한된 위험 ▲고위험 ▲수용 불가 위험 등 3가지 주요 위험 등급 중 하나에 해당하지 않는 기타 모든 AI 시스템은 최소/무위험으로 분류 • AI 법안은 최소위험 AI 시스템의 자유로운 사용을 허용하는 한편, 자발적인 행동 규약을 권장	• AI 기반 추천 시스템 • 스팸 필터
제한된 위험 (limited risk)	• 제한된 위험만 존재하는 AI 시스템에는 사용자가 향후 사용에 대해 정보에 입각한 결정을 내릴 수 있도록 콘텐츠가 AI로 생성되었다는 사실을 공개하는 등 최소한의 투명성 의무가 적용	• 챗봇 • 특정 감정 인식 및 생체 인식 시스템 • 딥페이크 생성 시스템
고위험 (high risk)	• 건강, 안전, 기본권, 환경, 민주주의, 법치주의에 중대한 잠재적 위해를 가할 수 있는 AI 시스템은 고위험군으로 분류 • 고위험 AI로 분류된 AI 시스템은 위험 완화, 데이터 거버넌스, 문서화, 인간에 의한 감독, 투명성, 견고성, 정확성, 사이버 보안과 관련된 포괄	• 수도, 가스 및 전기 분야 등의 특정 주요기반시설 • 의료기기 • 교육기관 접근 결정 및 채용시스템 • 법 집행, 국경 통제, 사법 행정 등에서 사용되는 특정 시스템 • 생체인식, 분류 및 감정 인식 시스템

	적인 규정 준수 의무가 적용	
수용 불가 위험 (unacceptable risk)	• 인간의 기본권에 대한 명백한 위협으로 간주되는 AI 시스템은 수용 불가 위험군으로 분류 • 수용 불가 위험을 내포한 AI 시스템은 특별한 예외가 없는 한 사용 자체가 금지됨	• 민감정보를 사용하는 생체인식 분류 시스템 • 얼굴 인식 데이터베이스 생성을 위해 인터넷·CCTV영상에서 얼굴 이미지를 불특정 스크래핑(untargeted scraping)하는 행위 • 직장 및 교육기관에서의 감정 인식 • 소셜 스코어링(social scoring) • 인지 행동을 조작하여 자유 의지를 우회하는 AI 시스템

출처 : 넥스텔리전스(주) 정리

▌(고위험 AI 의무사항) EU AI 법은 고위험 AI 시스템 제공과 관련해 공급자(provider)에게 적용되는 의무사항을 명시하고 있음

- AI 시스템의 수명 주기 전반에 걸친 **위험 관리 프로세스를 수립, 구현, 문서화 및 유지하여** 고위험 AI 시스템이 EU AI 법을 준수하여 설계, 개발 및 배포되도록 보장해야 함
  - 공급자는 ▲정상적인 사용 및 오용에 따른 예측 가능한 위험을 식별 ▲시판 후 모니터링 데이터를 통해 추가적인 위험을 고려 ▲식별된 위험을 해결하기 위한 적절한 조치를 구현해야 함
- 공급자는 효과적이고 적절한 **데이터 거버넌스를 수행하여** 사용하는 데이터 세트가 충분한 관련성과 대표성을 가지며, 데이터 품질 및 정확성을 보장해야 함
- 또한, 규정 준수를 입증하는 **기술 명세서를 작성 및 보관하고** 규제 관할 당국에 규정 준수 여부를 평가할 수 있는 정보를 제공해야 함
- 고위험 AI 시스템을 **기록 보관용(record-keeping)으로 설계함으로써** 국가 수준의 위험을 식별하는데 관련된 사건들과 시스템 수명 주기 전반에 걸친 중요한 수정사항들을 자동으로 기록할 수 있도록 해야 함
- 다운스트림 사용자가 규정을 준수할 수 있도록 **AI 시스템의 사용 지침을 제공해야 함**
- 아울러, **▲인간에 의한 감독을 보장하고 ▲적절한 정확성, 견고성 및 사이버보안을 보장하도록 고위험 AI 시스템을 설계·배포**해야 함
- 규정 준수를 위해 **품질관리 시스템을** 구현해야 함

▌또한, AI 법 제27조는 특정 유형의 고위험 AI 시스템 사용자(deployer)에게 기본권 영향평가(FRIA,

Fundamental Rights Impact Assessment)를 수행할 의무를 부여

- FRIA는 AI 시스템으로 인한 부정적 영향으로부터 개인의 기본권을 보호하는 것을 목표로 함
- FRIA를 수행할 의무가 있는 대상은 다음과 같음
  - 공법의 적용을 받는 기관인 사용자
  - 공공 서비스를 제공하는 민간 기관인 사용자
  - 자연인의 신용도 평가, 신용 점수 설정 또는 생명·건강 보험의 맥락에서 위험 및 가격 평가를 위한 고위험 AI 시스템 사용자
- 동법에 의거하여 FRIA 수행 의무 대상은 다음과 같은 단계를 포함하여 영향평가를 수행해야 함
  - (설명) 고위험 AI 시스템의 개요, 해당 시스템의 의도된 목적, 기간 및 영향을 받는 사람에 대한 설명
  - (평가) 영향을 받는 사람에게 영향을 미칠 수 있는 구체적인 피해 가능성
  - (위험 관리) 이러한 위험을 해결하려는 조치 및 인간에 의한 감독 조치 이행에 대한 설명
- FRIA를 수행한 후, 사용자는 각 EU 회원국에서 지정한 관할 시장 감시 기관에 평가 결과를 보고해야 함

▌부속서 III에서는 AI 시스템을 고위험군으로 분류할 수 있는 사례(use cases)를 열거

표 4 고위험 AI 시스템 사례

구분	주요 내용
생체인식	• 원격 생체 인식 식별 시스템 • 생체인식 분류에 사용되도록 의도된 AI 시스템 • 감정 인식에 사용되도록 의도된 AI 시스템
주요기반시설	• 중요 디지털 인프라, 도로 교통의 관리 및 운영 또는 물, 가스, 난방 또는 전기 공급에서 안전 구성 요소로 사용되도록 의도된 AI 시스템
교육 및 직업 훈련	• 교육 및 직업 훈련 기관에 대한 접근 또는 입학을 결정하거나 사람을 배정하는 데 사용되도록 의도된 AI 시스템 • 학습 성과를 평가하는 데 사용되도록 의도된 AI 시스템 • 교육을 평가하는 목적으로 사용되도록 의도된 AI 시스템 • 학생의 금지된 행동을 모니터링하고 감지하는 데 사용되도록 의도된 AI 시스템
고용, 근로자 관리	• 타깃 구인 광고를 게재하고, 구직 신청서를 분석 및 필터링하고,

및 자영업 접근	후보자를 평가하기 위해 사람들을 모집 또는 선발하는 데 사용되도록 의도된 AI 시스템 • 사람들의 성과 및 행동을 모니터링하고 평가하는 데 사용되도록 의도된 AI 시스템
필수적 공공·개인 서비스 혜택 접근	• 필수 공공 지원 혜택 및 서비스에 대한 자격을 평가하고 이러한 혜택 및 서비스를 부여, 감소, 취소 또는 회수하는 데 사용되도록 의도된 AI 시스템 • 신용도를 평가하거나 신용 점수를 확립하는 데 사용되도록 의도된 AI 시스템 • 생명 및 건강보험 대상자의 위험 평가 및 가격 책정에 사용되도록 의도된 AI 시스템 • 사람들의 긴급 전화를 평가하고 분류하거나 경찰, 소방관, 의료 지원 및 응급 의료 환자 분류 시스템을 포함한 응급 대응 서비스를 파견하거나 파견 우선순위를 설정하는 데 사용되는 AI 시스템
법 집행	• 법 집행기관 또는 관련 지원기관에서 범죄 희생자가 될 위험을 평가하기 위해 사용하거나 대신 사용하도록 의도된 AI 시스템 • 법 집행기관 또는 관련 지원기관에서 폴리그래프 또는 유사한 도구로 사용하도록 의도된 AI 시스템 • 법 집행기관 또는 관련 지원기관에서 범죄의 수사 또는 기소 과정에서 증거의 신뢰성을 평가하기 위해 사용하도록 의도된 AI 시스템 • 법 집행기관 또는 관련 지원기관에서 범죄 또는 재범 위험을 평가하기 위해 사용하도록 의도된 AI 시스템 • 법 집행기관 또는 관련 지원기관에서 범죄 또는 재범 위험을 평가하기 위해 사용하도록 의도된 AI 시스템
이주, 망명 및 국경 통제 관리	• 기관에서 폴리그래프 또는 이와 유사한 도구로 사용하도록 의도된 AI 시스템 • 기관에서 회원국의 영토에 입국하려는 또는 이미 입국한 사람이 초래하는 보안 위험, 불법 이주 위험 또는 건강 위험을 포함한 위험을 평가하도록 의도된 AI 시스템 • 기관이 망명, 비자 또는 거주 허가 신청을 검토하고 신분을 신청하는 사람의 자격과 관련된 불만을 처리하도록 지원하도록 의도된 AI 시스템 • 기관에서 이주, 망명 또는 국경 통제 관리의 맥락에서 사람을 탐지, 인식 또는 식별하는 목적으로 사용하도록 의도된 AI 시스템(단, 여행 서류 검증은 제외)
사법 행정	• 사법기관에서 또는 사법기관을 대신하여 사실과 법률을 조사하고 해석하고 구체적 사실에 법률을 적용하는 데 사법 기관을 지원하거나

및 민주적 절차	대체 분쟁 해결에서 유사한 방식으로 사용하도록 의도된 AI 시스템 • 선거 또는 국민투표의 결과 또는 선거 또는 국민투표에서 투표를 행사하는 사람의 투표 행동에 영향을 미치도록 의도된 AI 시스템

출처 : 넥스텔리전스(주) 정리

▌(범용 AI 의무사항) 모든 GPAI 모델 공급자는 일반적으로 다음과 같은 의무를 준수해야 함

- 교육 및 테스트 과정과 평가 결과를 포함한 **기술 문서 작성**
- GPAI 모델을 자체 AI 시스템에 통합하고자 하는 다운스트림 공급업체가 해당 모델의 기능과 한계를 이해하고 준수할 수 있도록 **관련 정보 및 문서를 작성하여 제공**
- **저작권 지침(Copyright Directive, Directive (EU) 2019/790)을 준용**하는 정책을 수립
- GPAI 모델 **학습에 사용된 콘텐츠에 대해 상세한 개요를** 공개

▌한편, GPAI 모델 중에서도 시스템적인 리스크(systematic risk)*가 존재할 경우, 추가적인 규제사항을 적용

* 범용 GPAI 모델로 인하여 EU 시장에 중대한 영향을 미치며 공공 보건, 안전, 안보, 기본권 또는 EU 사회 전체에 실질적으로 또는 합리적으로 예측 가능한 부정적인 영향을 미칠 위험

- 시스템적인 리스크를 식별하고 완화하기 위해 **적대적 테스트(adversarial testing)**를 수행하고 문서화하는 등 모델 평가를 수행
- 발생 원인을 포함해 **잠재적인 시스템적 위험을 평가하고 완화**
- **심각한 사고와 가능한 시정 조치를 추적 및 문서화** 하여 **지체 없이 AI 사무국 및 관련 국가 관할 당국에 보고**
- 적절한 **사이버 보안 보호 수준을** 보장

(3) 거버넌스

▌EU AI 법의 적절한 집행을 보장하기 위해 다음과 같은 담당 기관들을 운영

- EU 집행위원회 산하에 **AI 사무국(AI Office)**을 두어 EU 전역에 공통으로 적용되는 규칙을 집행하도록 함
- **독립적인 과학전문가패널(scientific panel of independent experts)**을 구성하여 집행 활동을 지원
- 각 회원국 대표로 구성되는 **AI 이사회(AI Board)**를 출범하여 회원국 간 일관되고 효과적인 법 집행을 위해 자문을 제공하도록 함

- 산업계, 학계, 시민사회, 스타트업, 중소기업 등 다양한 이해관계자를 대표하는 **자문 포럼(advisory forum for stakeholders)**을 구성하여 AI 이사회와 EU 집행위원회에 기술적인 전문지식을 제공

(4) 패널티

▌EU AI 법 위반에 대한 과징금은 위반 기업의 직전 회계연도 글로벌 연간 매출액 또는 미리 정해진 금액 중 더 높은 금액으로 책정

- 한편 중소기업과 스타트업의 경우, 각 위반 범주에 대해 두 금액 중 낮은 금액을 과징금으로 책정

표 4 EU AI 법 위반에 대한 패널티

위반사항	위반 시 패널티(둘 중 높은 금액 부과)
신고 기관 및 국가 관할 당국에 부정확하거나, 불완전하거나, 오해의 소지가 있는 정보 제공	• 750만 유로 또는 해당 기업의 전 세계 연간 총 매출액의 1.5%
범용 AI 모델에 대한 규정 위반 등 기타 요건 미준수	• 1,500만 유로 또는 해당 기업의 전 세계 연간 총 매출액의 3%
금지된 관행에 대한 위반 또는 데이터 관련 요건 미준수	• 3,500만 유로 또는 해당 기업의 전 세계 연간 총 매출액의 7%

출처: European Commission(2023.12.12.), 넥스텔리전스(주) 정리

3. EU AI 법과 GDPR의 관계성 및 쟁점

(1) 적용 범위

▌GDPR이 의무 대상자를 컨트롤러(controller)와 프로세서(processor)를 구분하듯, EU AI 법 또한 규제 대상 사업자를 공급자(provider), 사용자(deployer) 등으로 분류

- (GDPR) GDPR은 기본적으로 EU 시민들의 개인정보* 처리에 대한 규칙 및 원칙을 수립
  * 즉, 식별되거나 식별가능한 살아있는 개인과 관련된 모든 정보
  - 물적 범위에는 전체적·부분적 자동화된 수단에 의한 개인정보 처리 또는 (해당 개인정보가 관련 파일링 시스템의 일부를 구성하는 경우에 한하여) 비자동화 수단에 의한 개인정보의

수동 처리가 해당

- 지리적 범위로는 EU 내에 기반을 둔 컨트롤러/프로세서, 그리고 EU 내 정보주체를 대상으로 하는 비EU 컨트롤러/프로세서에 적용

- (AI 법) EU AI법은 데이터의 성격과 관계없이 AI 가치사슬 전반에 걸쳐 동법에서 정의한 AI 시스템에 대해 적용

- GDPR과는 달리 EU AI 법은 엄격한 위험 분류 체계를 갖추고 있으며, AI 위험성 범주를 기반으로 차등적인 의무를 부과함

- 지리적으로는 GDPR과 마찬가지로 역외 적용 범위를 가지고 있어, AI 시스템 제공자 및 배포자가 EU 역외에 있더라도 AI 시스템을 통해 생성된 결과물이 EU에서 사용되는 경우 동 법이 적용

- 즉, 개인정보를 처리하는 AI 시스템은 GDPR의 개인정보보호 원칙과 AI 법의 데이터 거버넌스 요건을 모두 준수해야 함

- 반면 개인정보를 처리하지 않거나 EU 역외 정보주체의 개인정보를 처리하는 AI 시스템은 EU AI 법의 적용을 받을 수 있지만, GDPR의 적용을 받지는 않음

- 아울러 GDPR은 개인정보보호의 기본권을 바탕으로 정보주체의 권리를 보장함으로써 개인이 본인 개인정보의 소재와 사용에 대한 정보 제공 및 제어권을 요구할 수 있는 반면, EU AI 법은 'AI'라는 제품의 소비자 보호 권리에 더 초점을 두고 있음

  ※ 다만, AI 법은 EU 기본권 헌장을 비롯해 EU법에서 보호하는 기본권을 존중하는 방식으로 AI 시스템이 사용되도록 보장할 것을 언급하고 있음

- 이에, 개인은 결함이 있는 AI 시스템으로부터 간접적으로 보호받을 수 있으나, EU AI 법은 GDPR과 같은 방식으로 개인의 권리를 명시적으로 언급하지 않음

- 따라서, 개인정보를 사용하는 불법적인 AI 시스템을 중단시키는 조치는 AI 법에 근거하여 이루어지나, AI 시스템이 처리한 개인정보와 관련하여 정보주체가 권리를 행사하는 것은 GDPR에 근거

(2) 인간에 의한 감독 및 자동화된 의사결정

▌AI 법과 GDPR 모두 자동화된 의사결정 및 프로파일링과 관련된 문제를 다루고 있음

- GDPR은 개인에게 본인과 관련하여 법적 효력을 발생시키거나 이와 유사한 중대한 영향을 미치는 프로파일링을 비롯한 자동화된 처리만을 기반으로 한 결정의 대상이 되지 않을 권리를 부여하며, 두 가지 종류의 인간 개입 매커니즘을 명시

- 사람의 개입이 의사결정에 필수적인 요소로 포함되는 경우(제22조제1항)

- 안전장치로써 사람의 개입이 자동화된 처리에 포함되는 경우(제22조제2항)

- 마찬가지로 EU AI 법도 인간의 적절한 감독과 개입을 허용함으로써 정보주체의 기본권과 자유를 보호하는 데 중점을 두고 있음
  - 동법은 공급업체가 AI 시스템을 설계·개발할 때 해당 시스템의 사용 기간 동안 사람이 효과적으로 감독할 수 있는 인간 감독 인터페이스 도구를 구현할 것을 요구
  - 다만 AI 법은 AI 시스템의 작동 방식, 사용되는 데이터의 종류, AI 시스템의 추천을 평가하는 방법 등에 관해 어떤 조치를 취해야 하는지 구체적으로 명시하고 있지 않음

(3) 리스크 평가

▌고위험 AI 시스템도 개인정보를 처리하므로, AI 법에서 규정한 FRIA는 GDPR의 DPIA 요건과 중복될 가능성이 있음

- 두 평가 모두 프로세스 초기에 위험을 식별하고 이를 완화하기 위한 조치를 채택하여 개인정보와 기본권 보호를 강화하는 것을 목표로 한다는 점에서 유사함

- 다만 DPIA는 개인정보 처리로 인해 영향을 받는 정보주체의 권리와 자유에만 초점을 맞추는 반면, FRIA는 비개인 데이터와 관련된 위험에 대해서도 다룸
  - 또한 FRIA 결과가 반드시 관할 시장 감독기관에 보고되어야 하는 한편, DPIA는 잔존하는 위험 수준이 높은 경우에만 감독기관에게 보고할 의무가 있음

- AI 법은 제27조제4항에서 이러한 상충 가능성을 언급하며 DPIA를 통해 이미 일부 요건이 충족된 경우, FRIA는 해당 DPIA를 “보완(complement)”하는 역할을 한다고 명시

(4) 거버넌스 및 감독

▌EU 전역에 걸친 일관적인 법 집행 및 적용을 위해 GDPR은 개인정보 감독기관을 설립하고, AI 법은 AI 사무국 및 AI 이사회의 출범을 규정

- (GDPR) ▲각 회원국의 개인정보 감독기관이 주도적인 역할을 수행하고 ▲EU 개인정보보호이사회(EDPB) 및 개인정보보호감독관(EDPS)이 자문 및 집행 일관성 메커니즘을 통화 보완하는 2단계 집행 모델을 채택

- (AI 법) AI 법 또한 마찬가지로 법의 적용 및 이행을 감독하고 시장 모니터링 활동을 담당하는 하나 이상의 국가 관할 당국을 지정하도록 규정하며, 각국 관할 당국을

지원하는 AI 사무국과 AI 이사회를 둘 것을 제안

- 이에 개인정보를 처리하는 AI 시스템과 관련한 일관되고 효과적인 감동을 보장하기 위해서는 두 거버넌스 구조 간의 조정이 필요

4. 결론 및 전망

- EU AI 법은 끊임없이 진화하는 기술을 고려했을 때 현 법률이 시대에 뒤떨어지지 않도록 보장하고자 AI 시스템을 의도적으로 광범위하게 정의한 점이 특징
  - 동법은 AI 시스템의 다양한 위험 수준을 식별하고 GPAI를 포함한 AI 시스템에 대한 명확한 정의를 제공하고 있음
  - 고위험 AI 시스템에 대해서는 결과 지향적인 요건을 설정하고 있지만, 구체적인 기술 솔루션 및 운영은 업계 주도적인 표준에 맡겨 법적 프레임워크가 다양한 활용 사례에 유연하게 적용되고 새로운 기술 솔루션을 가능하게 할 수 있도록 보장하고 있음
  - 또한, AI 법은 위임법 및 시행령을 통해 향후 개정될 수 있음
- 특히 AI 법은 AI 시스템이 개인의 기본적인 권리에 미치는 영향을 의무적으로 평가하는 FRIA 요건을 도입한 세계 최초의 법인 점에서 의미가 있음
  - 이는 조직이 고위험 AI 시스템을 개발할 때 책임감 있는 방식으로 행동했음을 문서화할 수 있는 기회를 제공
  - FRIA 요건의 이행 방식과 관련해서는 세부 가이드라인 등을 통해 구체화되어야 하나, 이와 같은 의무를 설정함으로써 고위험 범주에 속하는 AI 시스템을 사용하는 조직들의 규제 준수 경각심을 제고하는 데 기여할 것으로 평가
- 개인정보가 처리되는 한 AI 법이 시행된 이후에도 GDPR은 계속 적용될 전망이기에, AI 시스템을 개발하거나 사용하는 과정에서 개인정보를 처리하는 조직은 GDPR 및 EU AI 법에 따른 역할을 면밀히 분석해야 할 것임

출처 |

1. Dataguidance, EU: Council gives final approval to AI Act, 2024.5.21.
2. Dataguidance, International: The interplay between the AI Act and the GDPR – AI series part 1, 2023.11.
3. DLA Piper, Europe: The EU AI Act's relationship with data protection law: key takeaways, 2024.4.25.
4. European Commission, Artificial Intelligence – Questions and Answers*, 2023.12.12.
5. European Council, Artificial intelligence (AI) act: Council gives final green light to the first worldwide rules on AI, 2024.5.21.
6. European Council, Timeline – Artificial Intelligence, 2024.
7. European Parliament, Artificial Intelligence Act, 2024.3.13.
8. Future of Life Institute(FLI), Timeline of Developments, 2024.
9. KISTEP, EU 인공지능(AI) 규제 현황과 시사점, 2024.2.13.
10. 법무법인(유) 세종, 글로벌 인공지능(AI) 규제의 확산: 우리 기업의 새로운 비즈니스 전략이 필요한 결정적 시기, 2024.3.27.
11. 법무법인(유한) 태평양, EU 인공지능법(The Artificial Intelligence Act)의 주요내용 및 시사점, 2024.6.17.

2024
개인정보보호 월간동향분석
발간 목록

No.	호수	제목
1	1월 1호	EU 데이터법(Data Act) 주요 내용 분석 및 시사점
2	1월 2호	EU 내 메타의 무광고 유료 서비스 모델의 개인정보 침해 이슈 분석
3	2월 1호	미국 주(州) 개인정보 보호법에 대한 평가 및 분석
4	2월 2호	DPO 지정 및 역할에 대한 CEA 2023 조사 분석
5	3월 1호	미국 백악관의 정부 데이터 및 민감 개인정보보호를 위한 행정명령 분석
6	3월 2호	EDPB, GDPR 주 사업장에 관한 성명 발표
7	4월 1호	생체인식정보에 대한 개인정보보호 이슈
8	4월 2호	미국 AI 에듀테크 시장 관련 개인정보보호 규제 현황 및 고려사항
9	5월 1호	미국 APRA(American Privacy Rights Act) 주요 내용 분석
10	5월 2호	EDPS 2023 연례보고서 분석
11	6월 1호	중국-미국 간 데이터 관련 이슈
12	6월 2호	EU AI 법 및 GDPR의 상관관계 분석

2024
개인정보보호 월간동향분석

『2024 개인정보보호 월간동향분석 보고서』는
개인정보보호위원회 출연금으로 수행한
사업의 결과물입니다.

발행

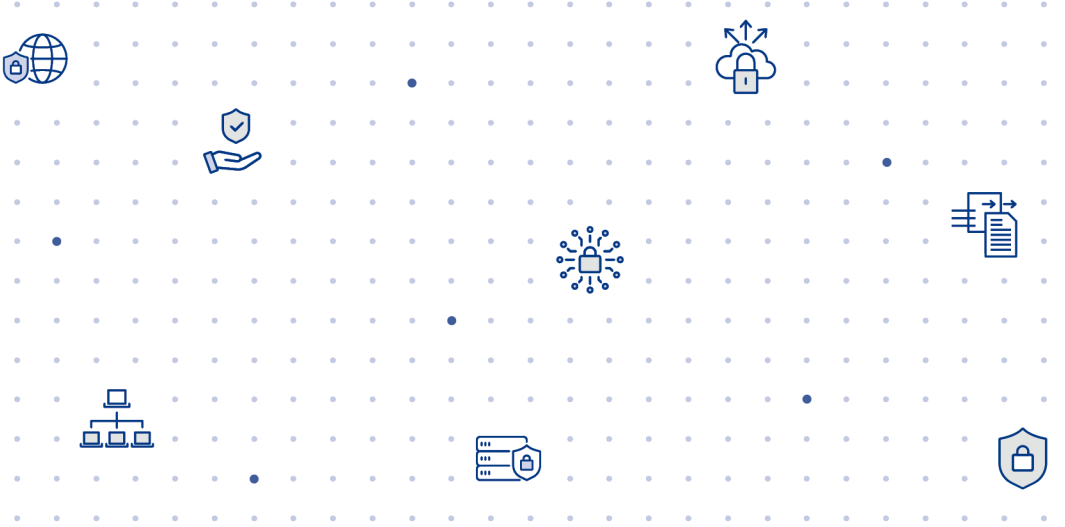
발행일 2024년 7월

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

2024
개인정보보호
월간동향분석

2024 Vol.6

PRIVACY REPORT



KISA 한국인터넷진흥원