인터넷·정보보호 법제동향

Vol. 196 | January 2024

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Contents

국내 입법 동향

〈공포된 법령〉

〈국회 제출 법률안〉

해외 입법 동향

〈중국〉

〈미국〉

국내 입법 동향 요약

■ 공포된 법령

법령명	공포일	주요내용
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률	2024. 1. 23.	- 정보보호 관리체계(ISMS)의 간편인증 제도 도입 및 영세·중소기업의 인증기준 및 절차 등 완화 - 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근 가능한 프로그램 또는 기술적 장치 등을 정보통신망 또는 정보시스템에 설치하거나 이를 전달 및 유포하는 행위 금지
「정보통신기반 보호법」 일부개정법률	2024. 1. 23.	- 관계중앙행정기관의 장이 주요정보통신기반시설에 대한 침해사고가 발생한 때에는 관리기관의 장에게 시설의 복구 및 보호에 필요한 조치 명령 가능 - 주요정보통신기반시설에 대한 보호조치 불이행 시 과학기술정보통신부장관, 국가정보원장 등이 관계중앙행정기관의 장을 대신하여 보호조치 명령 가능
「디지털의료제품법」 제정법률	2024. 1. 23.	- 디지털의료제품의 제조·수입 등 취급과 관리 및 지원에 필요한 사항을 규정하여 안전성 및 유효성 확보 - 디지털의료제품 안전관리에 관한 종합계획 수립 및 디지털의료기기에 대한 허가·인증을 통하여 전자적 침해행위로부터의 보호 조치 규정

■ 국회 제출 법률안

법안명	대표발의 (날짜)	주요내용
「디지털서비스의 안정성 관리 및 지원에 관한 법률안」 제정법률안	박성중의원 (2024. 1. 30.)	- 디지털서비스 안정성 관리계획 중심의 디지털 재난관리 체계 정비 및 중장기적 정책방향 설정을 위한 디지털 서비스 안정성 종합계획을 수립하고 디지털 위기관리 본부의 구성·운영 등의 기반 마련 - 대규모 디지털서비스 장애 발생 시 과기정통부장관이 디지털서비스 사업자에게 복구 및 재발방지 대책 수립·시행에 대한 권고 가능
「개인정보 보호법」 일부개정법률안	김도읍의원 (2024. 1. 16.)	- 고유식별정보 중 주민등록번호의 경우 별도의 규정을 두어 엄격하게 처리를 제한하고 있으나 위반에 대한 제재수준이 상이하여 불균형에 대한 문제를 제기 - 이에 주민등록번호 처리 제한 위반에 대한 처벌을 강화하여 고유식별정보 처리 제한 위반의 처벌과 일치하도록 함

국내 입법 동향

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률

(공포 2024. 1. 23., 시행 2024. 1. 23.)

■ 소관 상임위원회 : 과학기술정보통신부

■ 개정이유 및 주요내용

○ 불법스팸 전송자에 대한 처벌을 강화하고, 통신사의 불법스팸 전송 방지에 대한 책임을 강화하는 등 불법스팸 대응을 위한 제도를 개선(제50조 개정 및 제50조의8 신설)

○ 정보보호 관리체계(ISMS) 간편인증 제도를 도입하여 영세·중소기업의 인증기준 및 절차 등을 완화(제47조의7 신설)

○ 본인확인기관이 이용자의 주민등록번호를 비가역적으로 암호화한 정보를 생성·처리하는 경우 해당 정보 생성·처리의 안전성 확보를 위한 물리적·기술적·관리적 조치를 하도록 의무화(제23조의 5 및 제23조의6 신설)

○ 국내에 데이터를 임시적으로 저장하는 서버를 설치·운영하는 정보통신서비스 제공자 중 일정 기준에 해당하는 자가 불법정보의 유통을 방지하기 위한 기술적·관리적 조치를 하도록 의무화(제44조의7제5항 신설)

○ 누구든지 정당한 사유 없이 정보통신망의 정상적인 보호·인증 절차를 우회하여 정보통신망에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신망 또는 이와 관련된 정보시스템에 설치하거나 이를 전달·유포하는 행위를 금지(제48조제4항 신설)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「정보통신기반 보호법」 일부개정법률

(공포 2024. 1. 23., 시행 2025. 1. 24.)

■ 소관 상임위원회 : 과학기술정보통신부

■ 제안이유 및 주요내용

○ 주요정보통신기반시설을 관리하는 기관의 장에 대하여 주요정보통신기반시설 보호지침 준수 의무를 부여(제7조제1항제3호, 제11조, 제14조제4항 및 제5항 신설)

○ 주요정보통신기반시설에 대한 침해사고가 발생한 경우 관계 중앙행정기관의 장 또는 과학기술정보통신부장관 등이 주요정보통신기반시설을 관리하는 기관의 장에게 복구 및 보호에 필요한 조치명령을 할 수 있도록 함(제10조제2항 제11조제2항, 제30조제1항 신설)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「디지털의료제품법」 제정법률

(공포 2024. 1. 23., 시행 2025. 1. 24.)

■ 소관 상임위원회 : 식품의약품안전처

■ 제정이유

○ 디지털의료제품의 제조 · 수입 등 취급과 관리 및 지원에 필요한 사항을 규정하여 디지털의료제품의 안전성과 유효성을 확보하고 품질 향상을 도모하여 국민보건 향상과 디지털의료제품의 발전에 이바지함

■ 주요내용

○ 디지털의료제품을 디지털의료기기, 디지털융합의약품 및 디지털의료 · 건강지원기기로 정의하고, 디지털의료제품의 사용목적과 인체에 미치는 잠재적 위해성(危害性) 등의 차이에 따라 디지털의료제품을 분류하여 등급을 지정할 수 있도록 함(제2조 및 제3조)

○ 식품의약품안전처장이 디지털의료제품의 안전성 및 유효성을 확보하고 연구개발 및 국제경쟁력 강화를 촉진하기 위하여 3년마다 디지털의료제품 안전관리에 관한 종합계획을 수립 · 시행하도록 하고, 의료기기위원회 등에 디지털의료제품에 관한 자문을 요청할 수 있도록 함(제6조 및 제7조)

○ 디지털의료기기의 제조나 수입을 업으로 하려는 자는 식품의약품안전처장의 허가를 받도록 하고, 제조 또는 수입하려는 디지털의료기기에 대하여 허가 · 인증을 받거나 신고를 하도록 하며, 전자적 침해행위로부터의 보호 조치 등을 규정함(제8조부터 제14조까지)

○ 디지털의료기기에 대한 실사용 평가, 우수 관리체계 인증을 도입하고, 디지털의료기기소프트웨어에 대한 품질관리기준 적합판정 등을 규정함(제15조부터 제28조까지)

○ 디지털융합의약품의 제조나 수입을 업으로 하려는 자는 식품의약품안전처장의 허가를 받도록 하고, 제조 또는 수입하려는 디지털융합의약품에 대하여 허가를 받도록 함(제29조 및 제30조)

○ 디지털의료 · 건강지원기기를 제조 또는 수입하여 판매하려는 자가 디지털의료 · 건강지원기기에 대하여 식품의약품안전처장에게 신고할 수 있도록 하고, 디지털의료 · 건강지원기기에 대한 성능인증 및

유통관리를 도입함(제33조부터 제35조까지)

○ 디지털의료제품에 대한 영향평가, 건강보험 급여에 대한 검토요청, 디지털의료제품의 구성요소에 대한 성능평가, 지식재산권 보호 지원, 연구개발 및 표준화 지원, 전문인력 양성, 국제협력 등에 대한 근거를 마련함(제36조부터 제48조까지)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「디지털서비스의 안정성 관리 및 지원에 관한 법률안」 제정법률안

(박성중의원 대표발의, 2024. 1. 30. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유

○ 지난 판교 데이터센터 화재 및 카카오 · 네이버 서비스 장애 사고('22. 10. 15.)로 인해 국민 실생활에 밀접한 디지털서비스의 장애가 발생하여 대규모의 국민 불편 및 피해를 유발함에 따라, 「방송통신발전기본법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「전기통신사업법」의 개정('23. 1. 3.)을 통해 디지털 재난관리 체계를 강화함으로써 대규모 디지털서비스 장애로부터 국민을 보호하고 있음

○ 그러나 현행 디지털 재난관리 체계는 3개 법률에 분산하여 규정되어 있어 규율 대상과 내용의 유사성으로 인한 중복규제 소지가 있고, 디지털 전 분야를 아우르는 종합적인 디지털 재난관리를 수행하기 어려운 실정임

○ 따라서 디지털 안전 법체계의 일원화를 통해 네트워크 · 서비스 · 데이터 등 디지털 전 분야에 대한 상시적 · 체계적인 재난관리를 수행 등, 기술 발전 및 서비스 유형 다양화 등 디지털 환경의 변화에 적시 대비함으로써, 국민 생활에 큰 영향을 미치는 디지털서비스의 신뢰성과 안정성을 확보할 필요가 있음

○ 이에 디지털서비스 안정성 관리계획을 중심으로 한 디지털 재난관리 체계 정비, 중장기적 정책 방향 설정을 위한 디지털서비스 안정성 종합계획의 수립, 상시적 위기관리 조직인 디지털 위기관리 본부의 구성 · 운영 및 전담기관 지정 · 위탁 등을 통해 국민에게 디지털서비스를 중단 없이 제공하기 위한 기반을 마련하려는 것임

■ 주요내용

○ 과학기술정보통신부장관은 디지털서비스에 대한 새로운 위협요인과 미래 디지털 환경 변화에 체계적으로 대비하기 위하여, 디지털서비스의 안정성 관리 및 촉진 · 지원 정책의 효율적 · 체계적 추진을 위한 디지털서비스 안정성 종합계획을 3년마다 수립 · 시행하여야 함(디지털서비스 안정성 종합계획의 수립, 안 제5조)

○ 모든 디지털서비스 사업자가 책임성을 갖고 소관 디지털서비스의 안정성 확보를 위한 조치를 수행하도록 일반적 노력 의무를 부과함(디지털서비스의 안정성 확보, 안 제9조)

○ 일정 기준을 충족하는 주요디지털서비스 사업자는 과학기술정보통신부장관이 마련한 수립지침에 따라 소관 디지털서비스의 안정성 확보를 위한 관리계획을 매년 수립하도록 하고, 기존 「방송통신발전 기본법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 및 「전기통신사업법」에 산재되어 있는 재난·안전 관리조치를 이 법에 따른 관리계획을 중심으로 통합하여 디지털서비스 안정성 관리체계를 정비함(관리계획의 수립, 안 제10조)

○ 과학기술정보통신부장관이 주요디지털서비스 사업자의 관리계획 이행 현황을 점검할 수 있도록 관련 자료의 제출 요구 및 현장 출입·점검에 대한 근거를 규정하고, 동일한 관리조치에 대한 중복 점검을 최소화하기 위하여 다른 법에 따른 점검을 통과하는 경우에는 해당 항목에 대하여 관리계획을 이행한 것으로 보는 간주 규정을 마련함(관리계획의 이행 및 점검, 안 제11조)

○ 상시적인 디지털서비스 장애의 모니터링, 디지털 위기관리본부 운영 지원, 재난·안전 관리조치 이행 현황 점검 및 관련 기술개발·인력양성 등 디지털서비스 안정성 관련 업무의 수행을 지원하는 분야별 전담기관의 지정 및 위탁 근거를 마련함(전담기관의 지정 및 위탁, 안 제8조, 제22조, 제33조)

○ 디지털서비스 안정성 확보를 위한 사업자의 자발적인 노력을 유도하고 이용자의 알권리 보장을 위하여, 대국민 서비스를 제공하는 기간통신서비스 및 부가통신서비스 분야 주요디지털서비스 사업자 중 일정 기준을 충족하는 자는 디지털서비스 안정성 확보를 위한 투자, 인력 확보 및 인증 획득 등 각종 노력에 관한 사항을 포함한 서비스 안정성 보고서를 작성하고 공개하여야 함(서비스 안정성 보고서의 공개, 안 제14조)

○ 대규모 디지털서비스 장애의 재발방지를 위해 체계적인 원인분석을 수행할 수 있도록 과학기술정보통신부장관의 장애 원인조사 실시 근거를 마련하고, 필요시 정보통신·전기·소방 등 각 분야 전문가가 참여하는 민·관합동조사단을 구성할 수 있도록 함(원인조사, 안 제19조)

○ 대규모 디지털서비스 장애 발생 시 신속한 복구와 재발방지를 위하여, 과학기술정보통신부장관이 장애가 발생한 디지털서비스 사업자에 대해 복구 및 재발방지 대책의 수립·시행 권고와 행정적·기술적 지원을 할 수 있도록 하고, 유사 장애 사고방지를 위해 동종 업계 사업자에 대한 디지털서비스 안정성 관리 현황조사 규정을 신설함(복구 및 재발 방지, 안 제20조)

○ 기존 「방송통신발전 기본법」에 따른 방송통신재난 대책본부를 대체하는 디지털 위기관리본부의 상시적인 운영 근거를 마련하고, 디지털 위기관리본부를 「재난 및 안전관리 기본법」에 따른 중앙사고수습본부로 간주함(디지털 위기관리 본부의 운영 등, 안 제22조)

○ 주요 디지털서비스 장애 및 우수 대응 사례 등 사업자 간 정보 공유를 확대하고 디지털서비스 및 설비 정보의 현황 관리 등을 위하여, 과학기술정보통신부장관이 디지털서비스 안정성 통합관리시스템을 구축·운영할 수 있도록 함(디지털서비스 안정성 통합관리시스템의 구축·운영, 안 제27조)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

국내 입법 동향

「개인정보 보호법」 일부개정법률안

(김도읍의원 대표발의, 2024. 1. 16. 제안)

■ 소관 상임위원회 : 정무위원회

■ 제안이유 및 주요내용

○ 현행법은 고유식별정보의 처리 제한에 관하여 규정하고 있으며, 고유식별정보 중 주민등록번호의 경우 별도의 규정을 두어 더욱 엄격한 요건 하에서 처리하도록 하여 그 처리 제한을 강화하고 있음

○ 그런데 현행법상 고유식별정보 처리 제한 위반에 대하여는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하여 형사처벌의 벌칙규정을 두고 있는 반면, 보다 엄격한 요건을 규정하고 있는 주민등록번호의 처리 제한 위반에 대하여는 3천만원 이하의 과태료만을 부과하도록 하고 있어 그 제재수준에 불균형이 발생한다는 지적이 있음

○ 이에 주민등록번호 처리 제한 위반에 대하여 고유식별정보 처리 제한 위반과 동일하게 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하도록 하여 제재수준의 불균형을 해소하고, 주민등록번호 처리 제한에 대한 처벌을 강화하여 개인정보를 보다 두텁게 보호하고자 함(안 제71조제5호, 제75조제2항제7호 삭제)

• Reference

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

해외 입법 동향

중국 국가인터넷정보판공실, 「네트워크 보안 사고 보고 관리 조치」 초안 발표 (2023. 12. 8.)

중국 국가인터넷정보판공실(CAC[1]), 네트워크 보안 사고 발생 시 사고를 규모에 따라 분류하고 보고 및 관리하도록 하는 「네트워크 보안 사고 보고 관리 조치」 초안을 발표 (2023. 12. 8.)

■ 개요

○ 중국 국가인터넷정보판공실은 2023년 12월 8일에 네트워크 보안 사고를 분류하고 보고하도록 하여 손실·피해를 줄이고 국가의 네트워크 보안을 유지하기 위하여 「네트워크 보안 사고 보고 관리 조치[2]」 초안을 발표

■ 주요 내용

○ **(사고 보고 의무)** 네트워크 보안 사고 발생 시 네트워크 운영자는 즉시 비상 대응 계획을 수립해야 하고, 「네트워크 보안 사고 분류 지침」에서 분류하는 사고 요건에 해당하는 경우 1시간 이내에 보고해야 함(제4조)

- **(「네트워크 보안 사고 분류 지침[3]」)** 본 지침은 네트워크 보안 사고가 ▲중요 네트워크 및 정보시스템에 매우 심각한 시스템 손실이 발생하여 시스템 중단 및 부분 마비 ▲국가 기밀 정보, 중요·민감 정보 및 데이터의 분실 또는 도난 등 국가 안보에 심각한 위협 ▲기타 국가 안보, 사회 질서 등 공공의 이익에 매우 심각한 위협과 영향을 미치는 경우 중 하나가 충족되면, 요건에 따라 3가지(중대한, 매우 중대한, 대규모)로 분류함

〈네트워크 보안 사고 분류〉

구분	요건
· 중대한 네트워크 보안 사고[4]	- 현(县)급 이상 시의 당 및 정부 기관의 포털 웹사이트가 마비되어 주요 웹사이트 공격 또는 장애로 인해 6시간 이상 접속할 수 없는 경우 - 중요 정보 인프라가 전체적으로 2시간 이상 중단되거나 주요 기능이 6시간 이상 중단되는 경우 - 단일 시·군·구 행정 구역에 거주하는 인구의 30% 이상이 업무 및 생활에 영향을 받는 경우 - 수도, 전기, 가스, 석유, 난방 또는 교통 측면에서 100만 명 이상에게 영향을 미치는 경우 - 국가 안보 및 사회 안정에 심각한 위협이 되는 중요 데이터의 유출 또는 도난

1) 国家互联网信息办公室(Cyberspace Administration of China)
2) 网络安全事件报告管理办法
3) 网络安全事件分级指南

구분	요건
	- 1,000만 명 이상의 개인정보가 유출된 경우 - 당 및 정부 기관의 포털, 주요 뉴스 웹사이트, 온라인 플랫폼이 공격 및 변조되어 불법적이고 유해한 정보가 광범위하게 유포되는 경우 - 2,000만 위안 이상의 직접적인 경제적 손실을 초래한 경우 - 기타 국가 안보, 사회 질서, 경제 건설 및 공공의 이익에 심각한 위협을 가하고 심각한 파장을 일으키는 네트워크 보안 사고
· 매우 중대한 네트워크 보안 사고[5]	- 성(省) 수준 이상의 당 및 정부 기관의 포털 웹사이트와 주요 뉴스 웹사이트가 공격 또는 장애로 인해 24시간 이상 접속할 수 없는 경우 - 중요 정보 인프라가 전체적으로 6시간 이상 중단되거나 주요 기능이 24시간 이상 중단되는 경우 - 단일 지방 행정 구역에 거주하는 인구의 30% 이상이 업무 및 생활에 영향을 받는 경우 - 물, 전기, 가스, 석유, 난방 또는 교통 측면에서 1,000만 명 이상의 사람들에게 영향을 미치는 경우 - 국가 안보 및 사회 안정에 매우 심각한 위협이 되는 중요한 데이터의 유출 또는 도난 - 1억 명 이상의 개인정보가 유출된 경우 - 당 및 정부 기관의 포털, 주요 뉴스 웹사이트, 네트워크 플랫폼 등 중요 정보 시스템이 공격 및 변조되어 불법적이고 유해한 정보가 대규모로 유포되는 경우 - 1억 위안 이상의 직접적인 경제적 손실을 초래한 경우 - 국가 안보, 사회 질서, 경제 건설 및 공공 이익에 매우 심각한 위협을 가하고 심각한 파장을 일으키는 기타 네트워크 보안 사고
· 대규모 네트워크 보안 사고[6]	- 현(县)급 및 직할 시급 이상의 당 및 정부 기관의 포털 및 주요 뉴스 웹사이트가 공격 또는 장애로 인해 2시간 이상 접속할 수 없는 경우 - 중요 정보 인프라가 전체적으로 30분 이상 중단되거나 주요 기능이 2시간 이상 중단되는 경우 - 단일 시·군·구 단위 행정구역 내 인구의 10% 이상이 업무 및 생활에 영향을 받는 경우 - 수도, 전기, 가스, 석유, 난방 또는 교통 측면에서 10만 명 이상에게 영향을 미치는 경우 - 국가 안보 및 사회에 심각한 위협이 되는 중요 데이터의 유출 또는 도난 - 당 및 정부 기관의 포털, 주요 뉴스 웹사이트 및 온라인 플랫폼이 공격 및 조작되어 불법적이고 유해한 정보가 광범위하게 유포되는 경우 - 500만 위안 이상의 직접적인 경제적 손실을 초래한 경우 - 국가 안보, 사회 질서, 경제 건설 및 공공의 이익에 더 심각한 위협을 가하고 더 심각한 영향을 미치는 기타 네트워크 보안 사고

- **(주체별 보고 의무)** 동 지침은 네트워크 및 시스템을 ①정부 및 국가 기관 또는 관리하에 있는 기관, ②중요 정보 인프라 또는 ③기타로 분류하고 해당 주체별로 보고해야 할 대상이 달라짐

  · **(정부 및 국가기관 등)** 정부 및 국가 기관 또는 이들의 관리를 받는 기업인 경우, 해당 운영자는 부서의 네트워크 보안 및 정보화 부서에 보고해야 하고, 보고를 받은 보안 부서는 중대하거나, 매우 중대하거나, 또는 대규모 보안 사고의 경우 1시간 이내에 국가 네트워크 정보 부서에 보고해야 함

  · **(중요 정보 인프라)** 중요 정보 인프라인 경우, 운영자는 보안 부서와 공안 기관에 보고해야 하고, 보고를 받은 보안 부서는 중대하거나, 매우 중대하거나, 또는 대규모 보안 사고의 경우 1시간 이내에

4) 重大网络安全事件(Significant cybersecurity incidents)
5) 特别重大网络安全事件(Particularly significant cybersecurity incidents)
6) 较大网络安全事件(Major Cybersecurity Incident)

국가인터넷정보판공실과 국무원 공안 부서에 보고해야 함

· **(기타 네트워크 및 시스템)** 기타 네트워크 및 시스템 운영자는 보안 사고를 지역 네트워크 보안 및 정보화 부서에 보고해야 하고, 보고를 받은 부서는 중대하거나, 매우 중대하거나, 또는 대규모 보안 사고의 경우 1시간 이내에 상급 네트워크 보안 및 정보화 부서에 보고해야 함

○ **(사고 보고 신고 양식)** 운영자는 다음 내용을 포함하고 신고 양식에 따라 사고를 신고해야 함(제5조)

주요 내용
· i) 사건이 발생한 부서의 이름과 사건이 발생한 시설, 시스템, 플랫폼에 관한 기본정보 · ii) 사건이 발견되거나 발생한 시간 및 장소, 사건의 종류, 발생한 영향과 피해, 취해진 조치와 그 영향, 랜섬웨어의 경우 몸값의 금액 · iii) 상황의 악화 가능성 및 추가 예상 피해 · iv) 사건 원인에 대한 예비 분석 · v) 공격자 정보 및 경로 등 조사 및 분석에 필요한 단서 · vi) 취해야 할 추가 대응조치 및 지원 요청 · vii) 사고 현장의 보호 조건 · viii) 보고해야 할 기타 상황

○ **(예외 사항)** 사건의 원인, 영향, 또는 추세를 1시간 이내에 판단할 수 없는 경우에는 ▲사건이 발생한 부서의 이름과 사건이 발생한 시설, 시스템, 플랫폼에 관한 기본정보(제5조제1항) ▲사건이 발견되거나 발생한 시간 및 장소, 사건의 종류, 발생한 영향과 피해, 취해진 조치와 그 영향 및 랜섬웨어의 경우, 몸값의 금액(제5조제2항)에 대한 내용을 먼저 보고하고, 기타 상황은 24시간 이내에 보고해야 함(제6조)

○ **(사고 후속 조치)** 사고 처리 후 운영자는 영업일 기준 5일 이내에 사고 원인, 비상 대응 조치, 시정 상황 등에 대한 종합 분석 및 요약을 실시하고 이에 대한 보고서를 작성해야 함(제7조)

○ **(상기 의무)** 서비스를 제공하는 조직 및 개인은 운영자에게 중대하거나, 매우 중대하거나, 또는 대규모 네트워크 보안 사고가 발생한 것을 인지하는 경우 운영자에게 사건을 보고하도록 상기시켜야 하고, 조직 및 개인은 운영자가 고의로 은폐하거나 신고를 거부하는 경우 국가 및 지방 사이버 부서에 신고할 수 있음(제8조)

○ **(처벌)** 운영자가 본 조치 초안의 방법에 따라 네트워크 보안 사고를 보고하지 않을 경우, 네트워크 정보 부서는 관련 법률, 행정법규의 규정에 따라 처벌을 가함

- **(운영자)** 운영자가 네트워크 보안 사고를 지연, 누락, 보고 또는 은폐하여 중대한 피해를 야기하는 경우, 운영자 및 관련 책임자는 법에 따라 더욱 엄중하게 처벌받음

- **(관련 부서)** 관련 부서가 본 조치에 따른 네트워크 보안 사고를 보고하지 않을 경우, 상급 기관은 시정을 명령하고, 직접 책임이 있는 책임자는 법에 따라 처벌되며 범죄 혐의가 있는 사람은 형사책임을 지게 됨

■ 전망 및 시사점

○ 「네트워크 보안 사고 관리 조치」 초안은 네트워크를 구축·운영하거나 관련 서비스를 제공하는 자에게 네트워크 보안의 위협 및 관련 정부 기관에 심각한 피해를 끼칠 수 있는 사고가 발생한 경우 신고하도록 의무를 부과함

- 국가인터넷정보판공실은 대중들에게 2024년 1월 7일까지 해당 초안에 대한 피드백을 요청하여 의견을 수렴할 예정임

○ 「네트워크 보안 사고 관리 조치」 초안 규정에는 이미 중국의 다른 네트워크 보안 및 데이터 보호 규정과 유사한 규제 사항이 있고, 특히 주요 용어에 대한 명확한 정의가 부족하다는 비판도 있음

- 반면에, 본 초안이 아직 의견 수렴을 위해 공개되었으며 최종 버전이 공개되고 채택되기 전에 용어에 대한 정의를 명확히 하는 등 이러한 문제 중 일부가 해결될 수 있다는 의견도 존재함

• Reference

http://www.cac.gov.cn/2023-12/08/c_1703609634347501.htm
https://www.china-briefing.com/news/chinas-cybersecurity-regulator-issues-draft-measures-on-incident-reporting/
https://www.lexology.com/library/detail.aspx?g=7548679f-cd15-4e96-a380-edd336396812

해외 입법 동향

미국 하원, 「AI 파운데이션 모델 투명성 법(안)」 발의(2023. 12. 22.)

미국 하원은 인공지능을 통한 지식 재산권 침해 및 편향된 정보 제공 방지를 위한 「AI 파운데이션 모델 투명성 법(안)[1]」(2023. 12. 22.)을 발의함

■ 개요

○ 미국 하원은 특정 파운데이션 모델을 사용하거나 서비스를 제공하는 개인, 파트너십, 또는 법인이 인공지능 파운데이션 모델에 사용되는 학습 데이터와 알고리즘에 대한 정보를 공개적으로 명시하도록, 연방거래위원회(FTC)가 표준을 수립하는 내용의 「AI 파운데이션 모델 투명성 법(안)」을 발의함(2023. 12. 22)

■ 주요 내용

○ **(정의)** 본 법안은 인공지능, 파운데이션 모델 등 주요 용어를 다음과 같이 정의함

구분	정의
인공지능 (Artificial Intelligence)	· 인공지능 이니셔티브법 제5002조[2]에 따른 의미, 즉 실제 또는 가상 환경에 영향을 미치는 예측, 권장 또는 결정을 할 수 있는 기계 기반 시스템
파운데이션 모델 (Foundation Model)	· ▲광범위한 데이터에서 교육받고 ▲일반적으로 자체 감독을 사용하며 ▲최소한 10억 개의 매개변수를 포함하고 ▲다양한 맥락에서 적용 가능하며 ▲보안, 경제안보, 공중보건 또는 안전에 심각한 위험을 초래할 수 있는 작업에서의 고성능을 갖춘 인공지능 모델
적용 대상(Coverd Entity)	· ▲월간 10만 건 이상의 출력 인스턴스(텍스트, 이미지, 비디오, 오디오 또는 기타 형식)를 생성하는 파운데이션 모델을 사용하거나 서비스를 제공하고 ▲월간 사용자 수가 3만 명 이상인 파운데이션 모델을 사용하거나 서비스를 제공하는 개인, 파트너십 또는 법인
추론(Inference)	· 파운데이션 모델이 결과를 생성하기 위해 사용자에 의해 작동되는 경우
학습 데이터(Training Data)	· 파운데이션 모델이 학습된 데이터

○ **(표준 수립)** 연방거래위원회는 본 법안 제정일로부터 9개월 이내에 미합중국법 제5편 제553조[3]에 따라 파운데이션 모델 투명성을 향상시키기 위해 적용 대상이 관련 정보(학습 데이터, 모델 문서화, 추론을 위한 데이터 수집, 파운데이션 모델 운영)를 명시하는 표준을 수립하는 규정을 공포해야 함

1) AI Foundation Model Transparency Act of 2023 (H.R.6881)
2) Section 5002 of the National Artificial Intelligence Initiative Act of 2020
3) Section 553 of title 5, United States Code

- 한편, 연방거래위원회가 표준을 수립함에 있어 국립표준기술연구소(NIST) 소장, 과학기술정책국(OSTP) 국장, 저작권 등록청, 기타 관련 이해관계자와 협의해야 함

○ **(고려 사항)** 연방거래위원회는 표준을 수립함에 있어 파운데이션 모델에 관한 다음 정보를 고려해야 함

고려 사항
· **학습 데이터의 출처**(개인 데이터 수집 및 저작권 소유자 또는 데이터 라이선스 보유자가 저작권 또는 라이선스 보호를 강화하는데 필요한 정보 포함) · 포괄적인 인구통계학적 정보, 언어 정보 및 기타 속성 정보를 포함한 학습 데이터의 크기 및 구성에 대한 설명 · **학습 데이터가 어떻게 편집되거나 필터링 되었는지**를 포함한 데이터 거버넌스 절차에 대한 정보 · 학습데이터에 라벨이 지정된 방식, 라벨링 과정의 유효성이 어떻게 평가되었는지에 대한 정보 · **파운데이션 모델의 목적과 예상되는 제한 또는 위험에 대한 설명, 해당 모델에 대한 과거 편집 개요**, 해당 모델의 버전 및 해당 모델의 공개 날짜 · **적용 대상이 해당 파운데이션 모델의 투명성을 다음 항목과 맞추기 위한 노력**에 대한 설명 - 국립표준기술연구소의 AI 위험 관리 프레임워크(또는 그 후속 프레임워크) - 연방 정부가 승인한 유사한 합의 기술 표준 · **부정확하거나 유해한 정보를 제공할 위험이 높은 상황에 대응하기 위해 파운데이션 모델이 취하는 예방 조치**를 포함하여 공개 또는 업계 표준 벤치마크에서 자체 주도 또는 감사를 통해 **평가받는 성능 중 다음과 관련된 것** - 의료, 건강, 또는 의료보험 질문 - 생물학 또는 화합물 합성 - 사이버보안 - 선거 - 예측 치안을 포함한 치안 활동 - 금융 대출 결정 - 교육 - 고용 또는 채용 결정 - 공공 서비스 - 동 및 보호 계급을 포함한 취약 계층에 대한 정보 · 파운데이션 모델을 훈련하고 운영하는 데 사용된 계산 전력에 관한 정보 · 위원회가 국립표준기술연구소 소장과 협의하여 개선하기로 결정한 다른 필요한 정보

- 표준에는 적용 대상이 공개적으로 명시해야 하는 정보에 대한 형식과 방식이 명시되어야 함

형식 및 방식
· 적용 대상이 제공하는 파운데이션 모델과 관련된 적용 대상의 웹사이트에서 어떤 정보를 이용할 수 있는지 명시해야 함 · 연방거래위원회가 호스팅하는 웹사이트의 중앙 위치에 어떤 정보가 표시될 지 명시해야 함 · 적용 대상과 연방거래위원회의 웹사이트에 명시된 정보는 기계가 판독 가능한 형식을 사용해야 함 · 연방거래위원회에서 제2항에 따라 명시된 정보가 있는 URL을 호스팅해야 함 · 연방거래위원회가 적절하다고 판단하는 추가 사항을 명시함

○ **(특정 유형의 파운데이션 모델에 대한 대체 조항 고려)** 연방거래위원회는 표준을 설정하고 지침을 발행할 때 ▲오픈 소스 파운데이션 모델 ▲다른 파운데이션 모델에서 파생되거나 구축된, 또는 일정 부분 재훈련되거나 적응된 파운데이션 모델을 위한 대체 조항의 포함 여부를 고려해야 함

○ **(적용)** 연방거래위원회가 규정을 공포한 날로부터 90일 후에 적용됨

○ **(업데이트)** 연방거래위원회가 규정을 공포한 날로부터 2년 이내에, 그 이후 매년 최소 1회 국립표준기술연구소 소장과 협의하여 수립된 표준을 평가하고 적절한 업데이트를 통합하기 위해 해당 규정을 업데이트 하도록 함

○ **(연방거래위원회의 집행과 권한)** 표준규정의 위반은 「연방거래위원회법」의 불공정하거나 기만하는 행위 또는 관행에 관한 규정[4] 위반으로 취급되고, 공포된 규정을 위반하는 모든 해당자는 처벌 대상이 됨

■ 전망 및 시사점

○ 「AI 파운데이션 모델 투명성 법안」은 파운데이션 모델을 개발하고 배포하는 사람들의 지식 재산권을 저해하지 않으면서, 소비자가 자신의 저작권 보호를 강화하고 파운데이션 모델 정보에 기반한 결정을 내릴 수 있도록 한다는 평가를 받음

○ 본 법안은 파운데이션 모델의 저작권 소유자가 자신의 정보가 도용되었음을 알 수 있어 AI 파운데이션 모델에 대한 투명성 표준을 수립하는 데 도움이 될 것으로 보이지만, 미국 대통령 선거 운동이 시작되기 전에 법안이 통과될지 여부가 불확실하다는 견해가 있음

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/6881/text?s=10&r=6&q=%7B%22search%22%3A%22Cybersecurity%22%7D
https://www.theverge.com/2023/12/22/24012757/ai-foundation-model-transparency-act-bill-copyright-regulation

4) 57a Unfair or deceptive acts or practices rulemaking proceedings (a)(1)(B), 연방거래위원회는 상업에 영향을 미치는 불공정하거나 기만적인 행위 또는 관행을 구체적으로 정의하는 규칙을 규정할 수 있으며, 본 호에 따른 규칙에는 그러한 행위나 관행을 방지하기 위한 목적으로 규정된 요건이 포함될 수 있음

해외 입법 동향

미국 하원, 인공지능 기술 혁신에 따른 위험관리를 위한 「2024 연방 인공지능 위험관리법(안)」 발의(2024. 1. 10.)

미국 하원, 미국 연방정부가 인공지능 사용 시 국립표준기술연구소(NIST[1])의 「AI 위험관리 프레임워크[2]」 요구사항을 준수하도록 하는 「2024 연방 인공지능 위험관리법(안)[3]」을 발의(2024. 1. 10.)

■ 개요

○ 미국 하원은 2024년 1월 10일에 미국 연방기관 및 공급업체가 인공지능을 사용할 시 국립표준기술연구소가 개발한 「AI 위험관리 프레임워크」의 요구사항을 이행하도록 성문화하기 위하여 「2024 연방 인공지능 위험관리법(안)」을 발의함

■ 주요 내용

○ **(정의)** 본 법안은 인공지능, 기관, 프레임워크 등 주요용어를 다음과 같이 정의함

구분	정의
인공지능 (Artificial Intelligence)	· 인공지능 이니셔티브법 제5002조[4]에 따른 의미, 즉 실제 또는 가상 환경에 영향을 미치는 예측, 권장 또는 결정을 할 수 있는 기계 기반 시스템
관리자 (Administrator)	· 연방 조달 정책을 관리하는 자
기관 (Agency)	· 연방 정부 행정부의 모든 부서, 독립 기관, 공기업, 또는 기타 기관
기관장 (Director)	· 본 법안에서 기관장은 미국 국립표준기술연구소장을 의미함
프레임워크 (Framework)	· 국립표준기술연구소의 「AI 위험관리 프레임워크」 및 모든 후속 문서
프로파일 (Profile)	· 프레임워크 사용자의 요구사항, 위험 허용 범위 및 리소스를 기반으로 특정 설정 또는 애플리케이션에 대한 인공지능 위험관리 기능, 범주 및 하위 범주를 구현하는 것

1) National Institute of Standards and Technology
2) Artificial Intelligence Risk Management Framework (NIST AI 100-1, AI RMF 1.0)
3) Federal Artificial Intelligence Risk Management Act of 2024 (H.R.6936)
4) Section 5002 of the National Artificial Intelligence Initiative Act of 2020

① 기관의 인공지능 사용에 관한 요건

○ **(국립표준기술연구소의 지침)** 본 법의 제정일로부터 1년 이내에 국립표준기술연구소장은 관리자와 협의하여 기관들의 인공지능 위험관리 활동에 프레임워크를 통합할 수 있도록 지침을 발행해야 함

- **(프레임워크)** 본 지침에서는 프레임워크와 일치하는 표준, 관행 및 도구(tools)를 제공하는 한편, 기관이 인공지능의 개발, 조달 및 사용에 있어서 사람(People)과 지구(Planet)에 대한 위험을 감소시키기 위해 프레임워크의 활용 방법을 포함해야 함

- **(사이버보안 도구)** 인공지능 시스템의 보안을 향상시키기 위해 적합한 사이버보안 전략과 사이버보안 도구의 설치에 대한 부분을 명시해야 함

- **(표준 제공)** 동 지침은 ▲백악관 예산관리국(OMB)[5]의 프레임워크 및 예산편성지침[6]과 일치 ▲사람(People)과 지구(Planet)를 위협하는 위험 수준 고려 ▲기관의 장이 공급업체로부터 인공지능 프로그램을 조달하기 전 공급업체로서 적합한지 증명하도록 하는 표준을 제공해야 함

- **(교육 권장)** 동 지침은 인공지능 프로그램의 조달을 담당하는 각 기관에 프레임워크 및 지침 교육을 권장함

- **(요구사항 설정)** 동 지침은 각 기관이 프레임워크와 일치하는 인공지능을 사용 프로파일을 개발하기 위하여 최소 요구사항을 설정해야 함

- **(중소기업)** 동 지침은 중소기업이 프레임워크를 사용을 위한 프로파일을 개발해야 함

○ **(백악관 예산관리국(OMB)의 지침)** 백악관 예산관리국장은 국립표준기술연구소의 지침을 발표한 날로부터 180일 이내에 기관들이 프레임워크와 지침을 통합하여 인공지능 위험을 관리하도록 하는 지침을 발행해야 함

○ **(준수 요건)** 각 기관의 장은 해당 기관의 인공지능 시스템의 설계, 개발, 배포 및 사용 등에 적용되는 모든 정책, 원칙, 관행, 절차 또는 지침을 프레임워크 및 백악관 예산관리국의 지침과 부합하도록 해야 함

○ **(보고 요건)** 백악관 예산관리국장은 본 법의 제정일로부터 1년 이내에, 이후 3년에 1회 이상 기관별 프레임워크 이행 및 준수 여부에 관한 보고서를 의회에 제출해야 함

○ **(예외 사항)** 본 법안은 국가안보시스템[7]에는 적용되지 않는다고 예외 사항을 명시함

5) Office Of Management Budget
6) CIRCULAR NO. A-119 Revised(https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf)
7) Section 3552 of title 44, United States Code에 정의된 "국가안보시스템"

② 기관의 인공지능 프로그램 조달 요건

○ **(연방조달위원회(FARC[8]) 지침)** 연방조달위원회는 국립표준기술연구소의 지침이 발행된 후 1년 이내에 프레임워크에 따른 위험 기반의 인공지능 제품, 서비스, 도구 및 시스템을 인수하기 위한 요건 및 인공지능 인수를 위해 사용되는 계약 조항이 포함된 규정을 공표해야 함

③ 인공지능 인력에 관한 사항

○ **(계획 수립)** 본 법의 제정일로부터 180일 이내에 백악관 예산관리국장은 연방총무청장[9]과 협의하여 해당 기관의 장이 인공지능에 관한 전문지식을 요청하는 경우 이를 제공하기 위한 이니셔티브를 수립해야 함

- **(이니셔티브 사항)** ①인공지능 도구의 개발, 조달, 사용 및 평가에 있어 기관을 지원할 수 있는 다양한 분야의 전문가 모집 및 채용, ②모범사례 통합을 위해 미국 디지털 서비스 및 연방총무청의 기술혁신 서비스를 포함한 기존 이니셔티브와의 합의, ③기관을 지원할 수 있는 인공지능 위험관리 도구의 개발 및 배포 지침을 수립하기 위한 프로세스가 포함되어야 함

④ 인공지능의 인수를 위한 테스트 및 평가

○ **(연구)** 본 법의 제정일로부터 90일 이내에 국립표준기술연구소장은 연방이 인공지능의 인수를 위한 테스트·평가·검증과 관련한 합의 표준을 검토하는 연구를 완료해야 함

- **(합의 표준 개발)** 국립표준기술연구소장은 연구 완료일로부터 90일 이내에 인공지능 인수에 대한 테스트·평가·검증의 합의 표준 개발을 위하여 관련 이해관계자를 소집해야 함

- 국립표준기술연구소장은 합의 표준 개발을 완료하거나 1년 이내에 둘 중 보다 조속한 시일에 인공지능 인수에 대한 테스트·평가·검증을 수행하기 위한 ▲원칙을 개발해야 하고 ▲자원을 확립하고 ▲모니터링 및 검토를 실시하고 ▲인공지능 인수와 관련하여 각 기관장에게 사람 및 지구에 대한 위험성을 검토하도록 권고해야 함

■ 전망 및 시사점

○ 「2024 인공지능 위험관리법(안)」은 미국 연방기관 및 공급업체가 국립표준기술연구소의 「AI 위험관리 프레임워크(AI RMF)」를 준수하도록 성문화하는 한편, 프레임워크를 통합함으로써 AI 기술과 관련된 위험을 완화하는데 도움이 될 것으로 평가

※ 현재 NIST의 AI 위험관리 프레임워크(AI RMF)는 신뢰할 수 있는 AI 시스템 사용의 보장을 위한 자발적 표준에 해당

8) Federal Acquisition Regulation Council(회원으로는 미 국방부, 우주항공국, 연방총무청으로 구성)
9) Administrator of the General Services Administration

- 본 법안은 미국 연방정부의 인공지능 안전성 확보 및 올바른 활용이 기대됨에 따라 MS사, Workday 등의 영향력 있는 민간기업은 물론 학계 유명 인사들의 지지를 받음

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/6936
https://www.meritalk.com/articles/rep-lieu-introduces-companion-bill-to-codify-nist-ai-rmf/

해외 입법 동향

미국 하원, 「2024 인공지능 허위 및 무단 복제 금지법(안) (NO AI FRAUD Act)」 발의 (2024. 1. 10.)

미국 하원은 개인의 음성 및 초상권 보호를 위하여 「2024 인공지능 허위 및 무단 복제 금지법(안)[1](NO AI FRAUD Act)」을 발의함(2024. 1. 10.)

■ 개요

○ 미국 하원은 최근 인공지능(AI) 기술의 발전과 딥페이크 소프트웨어 개발이 개인의 음성 및 초상권을 도용하는 등 개인에게 부정적인 영향을 미친다는 의회 조사결과[2]에 따라 「2024 인공지능 허위 및 무단 복제 금지법(안)」을 발의함(2024. 1. 10.)

■ 주요 내용

○ **(정의)** 본 법안에서 사용되는 주요용어의 정의는 아래와 같음

용어	의미
디지털 묘사 (Digital depiction)	· 디지털 기술을 사용하여 전체 또는 일부를 생성하거나 변경한 개인의 외형을 복제, 모방 또는 유사하게 형상화하는 것
개인 맞춤형 복제 서비스 (Personalized cloning service)	· 알고리즘, 소프트웨어, 도구 또는 그 밖의 기술, 서비스 또는 장치로서 하나 이상의 디지털 음성 복제 또는 특정 개인의 디지털 묘사물을 제작하는 것을 주된 목적 또는 기능으로 함
디지털 음성 복제 (Digital voice replica)	· 디지털 기술을 사용하여 전체 또는 부분적으로 생성되거나 변경되고, 실제 개인이 수행하지 않았음에도 개인을 복제, 모방 또는 근사치화 한 것을 포함하는 시청각물(audiovisual work) 또는 오디오 녹음(sound recording)에 고정된 오디오 렌더링(audio rendering)을 뜻함
음성 (Voice)	· 컴퓨터, 인공지능, 알고리즘 또는 기타 디지털 기술, 서비스 또는 장치에 의해 녹음되거나 생성된 개인의 실제 음성 또는 음성의 시뮬레이션을 포함하는 모든 매체의 소리로서, 묘사되거나 시뮬레이션된 개인의 음성 소리 또는 음성 시뮬레이션, 또는 이와 관련하여 표시되는 그 밖의 정보로부터 쉽게 식별할 수 있는 정도의 소리를 의미함

1) No Artificial Intelligence Fake Replicas And Unauthorized Duplications Act of 2024 (NO AI FRAUD Act) (H.R.6943)
2) AI 기술을 사용하여 ▲아티스트 Drake와 The Weeknd의 목소리를 모방한 "Heart on My Sleeve"라는 노래 제작하였으며, 조회수는 1100만회 이상 기록(2023년 4월 4일경)
▲치과 보험 광고에서 톰 행크스의 얼굴이 포함된 허위 보증을 생성함(2023년 10월 1일경)
▲뉴저지 주 웨스트필드에서 여고생의 거짓되고 합의되지 않은 성적인 이미지를 생성함(2023년 10월16일부터 20일까지)
▲저스틴 비버(Justin Bieber), 대디 양키(Daddy Yankee), 배드 버니(Bad Bunny)의 목소리를 조작한 'Demo #5: nostalgia'라는 노래를 제작하였고, TikTok에서 2,200만 조회수, YouTube에서 120만 조회수 기록함(2023년 가을)
▲ "딥페이크 신원의 증가하는 위협"(국토안보부 보고서, '20.10)에 따르면, 연구원들은 당사자의 동의나 인지 없이 생성된 여성의 가짜 누드 이미지 100,000개 이상 보고
▲Pew Research Center에 따르면, 미국인 중 약 63%가 조작 또는 변경된 비디오가 현재 문제의 기본 사실에 혼란을 야기한다고 함

용어	의미
초상 (Likeness)	· 창작 수단에 관계없이 개인의 얼굴, 유사성, 기타 구별되는 특징 또는 그 유사성 관련한 정보 등을 통해 개인을 쉽게 식별할 수 있는 실제 또는 흉내된 이미지나 외관을 뜻함
디지털 기술 (Digital technology)	· 컴퓨터 소프트웨어, 인공지능, 머신러닝, 양자 컴퓨팅 등 현재 또는 향후 생성될 기술 또는 장치를 뜻함

○ **(초상 및 음성에 관한 재산권)** 모든 개인은 각자의 초상 및 음성에 대한 재산권을 소유함

- (성격) 해당 권리는 지식재산권으로서 전체 또는 부분적으로 자유롭게 양도 및 상속 가능하며, 개인이 사망했을 경우 해당 권리가 생전동안 상업적으로 이용되었는지 여부와는 관계없음

- (양도성) 해당 개인이 생존하는 동안, 그리고 사망 후 10년간 유언 집행자, 상속인, 양수인 또는 수증자에게 적용됨. 다만, ▲유언집행자, 양수인, 상속인 또는 수증자가 개인의 사망 후 최초 10년간(이후 2년 동안) 개인의 초상이나 음성을 상업적 목적으로 사용하지 않았다는 증거, 또는 ▲모든 유언집행자, 양수인, 상속인 또는 수탁자가 사망하는 경우에는 종료됨

○ **(유효성)** 광고 또는 표현작품(expressive work)에서 새로운 퍼포먼스 연출을 위해 디지털 묘사를 하거나 디지털 음성 복제를 하기 위한 사용 승인 계약을 할 때에는 다음의 요건을 준수해야 함

구분	내용
계약 대상	· ▲거래 시 변호사가 대리하고 서면으로 계약서가 작성되어야 하며, ▲계약 체결 당시 18세 이상이거나 18세 미만인 경우 해당 주법에 따라 법원의 승인을 받아야 함
계약 조건	· 그 계약은 단체협약(Collective Bargain Agreement)을 따름

○ **(허가받지 않은 음성 또는 초상의 시뮬레이션)** 음성 또는 초상권을 보유한 개인의 동의없이 다음과 같은 행위를 통해 미국 내 주(州)간 또는 외국 상거래에 영향을 미치는 경우(혹은 각 주(州)간 또는 외국 상거래의 수단이나 시설을 사용하는 경우)에는 손해배상 책임을 짐

위반행위	배상 책임
· (A) 무단으로 개인 맞춤형 복제 서비스를 대중에게 배포, 전송 또는 그 밖의 방법으로 제공함	- 위반시 $50,000 또는 무단 사용으로 인한 피해 당사자의 실제 손해, 또한 무단 사용으로 인한 이익은 실제 손해 계산 시 고려되지 않음
· (B) 무단으로 개인의 디지털 음성 복제 또는 디지털 묘사물을 출판, 수행, 배포, 전송하거나 기타 방법으로 대중이 이용할 수 있도록 함	- 위반시 $5,000 또는 무단 사용으로 인한 피해 당사자의 실제 손해, 또한 무단 사용으로 인한 이익은 실제 손해 계산 시 고려되지 않음

※ 한편, 피해를 입은 음성 또는 초상권을 보유한 개인이 해당 행위에 동의하지 않았다는 것을 알면서도 위 (A) 또는 (B)의 위반행위를 함에 있어 실질적인 기여나 지시 또는 다른 방법으로 용이하도록 하는 경우 또한 위반행위에 해당함

○ **(수정헌법 제1조[3]와의 관계)** 본 법안의 '허가받지 않은 음성 또는 초상의 시뮬레이션' 위반행위의 경우, 수정헌법 제1조에 따른 표현의 자유 등의 보호가치와 상반될 수 있으나, 다음의 요소를 고려하여

3) First Amendment, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." (출처 : https://constitution.congress.gov/constitution/amendment-1/)

음성 또는 초상에 대한 지식재산권과의 이익과 균형을 고려해야 함

고려 사항
▲ 상업적인 용도로 사용되었는지 여부, ▲문제가 되는 음성이나 이미지의 소유권자가 해당 작품의 주요 표현 목적에 관련성이 필수적인지 여부, ▲문제가 되는 음성 또는 초상권의 소유자 또는 인가받은 자의 작품 가치에 부정적인 영향을 미치거나 경쟁적인지 여부

○ **(면책)** ‘허가받지 않은 음성 또는 초상의 시뮬레이션’ 위반행위 당사자 등은 위반행위로 인하여 ▲음성 또는 초상권의 주체가 재정적·신체적 피해가 발생하거나 피해 위험이 높아지는 경우, ▲동의없이 사용된 음성 또는 초상권의 주체가 심각한 감정적 고통을 겪는 경우, ▲해당 사용이 대중, 법원 또는 재판소를 기만할 가능성이 있는 등의 위해(harm) 정도가 경미한 경우에는 면책될 가능성이 있음

- (유해성) 아동 성적 학대물을 포함하거나 성적으로 노골적인 성적 이미지를 포함하는 모든 디지털 묘사 또는 디지털 음성 복제물의 경우 절대적인 유해성이 인정됨

○ **(소멸시효)** 당사자가 위반 사실을 발견했거나 상당한 주의를 기울여 위반 사실을 발견한 후 4년 이내에 민사소송을 제기하지 않을 경우, 해당 권리는 소멸됨

○ **(기타)** 본 법안에 명시된 권리는 1934년 통신법 제230조(e)(2)[4]에 따른 지식재산에 관한 법률로 간주되며, 동 법안은 본 법 제정일로부터 180일 후에 발효됨(해당 발효일 이전에 개인이 사망했는지 여부는 관계없음)

■ 전망 및 시사점

○ 본 법안은 개인이 자신의 이미지와 목소리를 사용하는데 있어 개인의 지식재산권을 갖는다는 것을 연방법에 명시함으로써 자국민의 신원을 보호하기 위함임

- 한편, 본 법안은 표현의 자유를 명시한 수정헌법 제1조와의 이익 균형을 고려하고 있는 바, 이는 예술 창작 활동에 있어 표현의 자유는 필수적이지만 자신의 권리가 타인에 의해 악용되지 않도록 보호되어야 함을 강조하였음

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/6943/text?s=3&r=212
https://www.meritalk.com/articles/lawmakers-music-industry-push-for-support-of-no-ai-fraud-act/

4) Section 230 of the Communications Act of 1934 (47 U.S.C. 230) – Protection for private blocking and screening of offensive material–
(e) Effect on other laws
(2) No effect on intellectual property law
Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.

인터넷·정보보호 법제동향
Vol. 196 (January 2024)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

ㅣ 발 행 처 ㅣ 한국인터넷진흥원
(58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원
Tel. 1433-25
ㅣ 기획 · 편집 ㅣ 법제연구팀
ㅣ 발간 · 배포 ㅣ www.kisa.or.kr