인터넷·정보보호 법제동향

Vol. 191 | August 2023

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

Contents

국내 입법 동향

〈국회 제출 법률안〉

해외 입법 동향

〈미국〉

〈중국〉

〈해외 단신〉

국내 입법 동향 요약

■ 국회 제출 법률안

법안명	대표발의 (날짜)	주요내용
「전기통신사업법」 일부개정법률안	민형배의원 (2023. 8. 9.)	- 기간통신사업자와 다르게 부가통신사업자는 영향력에 비해 현행 법령에 의한 사회적 책무가 가볍다는 문제점 제기 - 부가통신사업자의 전기통신설비 구축 등에 대한 경제적 부담을 완화하고 빅테크 기업의 사회적 책무를 강화하여 통신서비스 안정성 향상 및 취약계층의 디지털 복지·접근성을 확대함
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	하영제의원 (2023. 8. 31.)	- 비대면 서비스가 활성화됨에 따라 인증 서비스의 중요성도 증가하고 있으나, 공인인증제도의 삭제와 본인확인업무 범위의 불명확성 등이 인증 서비스 발전에 장애가 된다는 문제점 제기 - 연계정보 개념을 정의하고 본인확인업무의 내용 및 범위를 명확화하며 전자서명인증자로 인정을 받은 자로 하여금 연계정보 관련 업무를 수행할 수 있도록 하는 규정 신설
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	홍석준의원 (2023. 8. 16.)	- 최근 불특정 다수의 시민을 대상으로 생명·신체에 위해를 가하겠다는 내용의 온라인 게시물 등으로 사회적 불안과 공포를 야기하지만, 현행법으로 처벌할 규정이 없다는 문제점 제기 - 불특정 다수 또는 사람의 생명·신체에 위해를 가하려는 내용을 정보통신망에 유포하거나 게시하는 자에 대한 처벌 규정 신설
「전자문서 및 전자거래 기본법」 일부개정법률안	김의겸의원 (2023. 8. 18.)	- 전자서명 등이 본인의 고의·과실 없이 제3자에 의해 위조되거나 부정한 방법으로 발급된 경우 전자문서의 의사표시를 작성자의 것으로 인정하지 않는 규정이 없다는 문제점 제기 - 전자서명 등이 고의·과실 없이 위조 또는 부정한 방법으로 발급된 경우 전자문서에 포함된 의사표시를 작성자의 것으로 볼 수 없도록 명시하는 규정 신설
「디지털 서비스 이용자 보호에 관한 법률」 제정법률안	정필모의원 (2023. 8. 23.)	- 다양해지는 디지털 환경에서 이용자에 대한 새로운 권리침해 유형 등 디지털 서비스 이용자의 보호 및 권리 보장의 필요성 대두 - 디지털 서비스 제공자에게 이용자 보호를 위한 정보 제공 등의 의무를 부과하고 이용자 보호의 원칙 마련 및 관련한 권리를 규정
「온라인플랫폼시장의 공정경쟁 촉진에 관한 법률」 제정법률안	박성준의원 (2023. 8. 23.)	- 온라인플랫폼시장에서 독점적 지위를 이용한 불공정행위로 인한 폐해가 나타나 공정한 경쟁 환경 조성을 위한 법규 마련의 필요성 - 공정거래위원회는 시장지배적 플랫폼 사업자의 시장지배적 지위 남용행위 금지 등의 의무를 부과하고 사업자가 기업결합 시 심사를 받도록 하는 등 시장의 공정한 경쟁 환경을 마련하는 조항 신설
「위치정보의 보호 및 이용 등에 관한 법률」 일부개정법률안	임호선의원 (2023. 8. 29.)	- 현행법은 보호의무자가 아동, 피성년후견인 등의 개인위치정보의 수집·이용 또는 제공에 동의하는 경우 동의로 규정 - 고령화에 따라 치매환자에 대한 생명 또는 신체 보호를 위하여 보호의무자가 개인위치정보의 수집·이용 또는 제공에 동의할 수 있도록 규정하여 치매환자에 대한 적극적인 보호 규정 신설

법안명	대표발의 (날짜)	주요내용
「국가전략기술 육성에 관한 특별법」 일부개정법률안	박정의원 (2023. 8. 2.)	- 국가전략기술이 외교·안보 측면의 전략적 중요성과 연관 산업에 미치는 영향이 크므로 무분별한 정보 유출 방지의 필요성 제기 - 기술육성주체가 국가전략기술 관련 정보의 제공을 요청받을 경우 관계 중앙행정기관장과 협의하여 제공 여부를 결정함으로써 국가전략기술에 대한 체계적인 정보보호와 보안 수행
「인공지능 책임 및 규제법」 제정법률안	안철수의원 (2023. 8. 8.)	- 인공지능기술이 특정 분야에서 인간의 통제수준을 넘어서 고의적으로 악용될 수 있는 문제에 대한 법적 규제 필요성이 대두됨 - 신뢰할 수 있는 인공지능의 사용환경 조성, 인공지능의 유형 구분을 통한 이용자 보호 등 안전하고 신뢰할 수 있는 인공지능 기술 및 정책의 제도적 기반 조성
「전자정부법」 일부개정법률안	이만희의원 (2023. 8. 25.)	- 인공지능, 빅데이터 등의 디지털 신기술의 발전과 디지털플랫폼정부 구현을 위한 전자정부서비스에 대한 법적 근거 마련의 필요성 제기 - 전자정부서비스 이용자의 편의 증진을 위한 관리체계 마련, 전자정부서비스 민간개방 활성화 등 디지털플랫폼정부 구현을 위한 법적 근거 마련

국내 입법 동향

「전기통신사업법」 일부개정법률안

(민형배의원 대표발의, 2023. 8. 9. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 일정 규모 이상의 부가통신사업자가 그 사회적 영향력에 상응하는 책무를 이행하도록 하고자 함

○ 현행법은 기간통신사업자에 보편적 역무 제공 또는 그 손실보전 의무, 공익을 위한 전기통신서비스의 요금감면 등 각종 사회적 책무를 부여함

○ 반면, 부가통신사업자는 사회 전반에 미치는 지대한 영향력에 비하여 법령에 의한 사회적 책무는 매우 가볍고 대표적으로 구글, 넷플릭스, 카카오, 네이버 등 '빅테크'가 있음

○ 이 같은 일부 부가통신사업자의 서비스 고품질화 · 고용량화 추세는 국내 통신망 트래픽 부담 가중으로 이어지며 전기통신설비의 구축·운용에도 일정 역할을 해야 한다는 지적이 있음

○ 아울러 시민들에게 부가통신사업자의 서비스도 일종의 필수재로 인식되기에, 기존 전기통신서비스의 요금감면처럼 취약계층 부가통신역무 요금감면이 필요함

○ 이에 부가통신사업자의 전기통신설비 구축 · 운용 및 취약계층 경제적 부담 완화 노력을 규정하고자 하며, 특히 일정 규모 이상 부가통신사업자의 사회적 책무 이행 책임 강화를 담음

○ 빅테크 기업의 사회적 책무 강화는 통신서비스 안정성 향상 및 취약계층 디지털복지와 디지털접근성 확대를 위한 것임(안 제22조의10 신설)

• Reference

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

국내 입법 동향

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(하영제의원 대표발의, 2023. 8. 31. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 인터넷의 발달 및 코로나19 바이러스의 확산 등으로 인해 비대면 서비스가 활성화됨에 따라 핀테크, IT 서비스 등이 국민들의 일상에 필수적인 요소로 자리잡으며, 이러한 서비스의 관문 역할을 수행하는 인증 서비스의 중요성도 날로 증가하고 있음

○ 이러한 변화에 따라 「전자서명법」 개정으로 전자서명에서 공인인증제도가 사라지고 다양한 민간 서비스가 활발히 경쟁하는 체계를 구축한 현재, 이 법에 따른 본인확인업무 범위의 불명확성, 일반적인 본인확인과의 의미 혼란, 연계정보의 활용가능성에 대한 불명확성으로 인하여 인증 서비스의 발전에 장애가 되고 있음

○ 아울러, 국내의 본인확인기관은 주로 통신사와 은행이 본인확인기관으로 인증을 받아 업무를 수행하고 있지만, 미국, 영국, 일본의 해외사례를 살펴보면 본인확인기관은 주로 정부 산하 기관 또는 연방의 각 행정기관이 IT 기술업체와의 협력을 통해 이뤄지고 있어 주요 선진국과 같이 IT업체, 전자서명인증사업자 등 기술보유업체에도 본인확인기관 지정의 필요성이 인정되고 있음

○ 이에 연계정보의 개념을 정의하고 본인확인업무의 내용과 범위를 분명히 하며 「전자서명법」에 따른 운영기준 준수사실의 인정을 받은 전자서명인증사업자로 하여금 연계정보 관련 업무를 수행할 수 있도록 하여 인증 서비스의 발전을 도모하고자 함(안 제2조, 제23조의3부터 제23조의5까지 및 제76조)

• Reference

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

국내 입법 동향

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(홍석준의원 대표발의, 2023. 8. 16. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 최근 불특정 다수의 시민을 대상으로 생명·신체에 위해를 가하겠다는 내용의 온라인 게시물 등으로 인해 사회적 불안과 공포를 야기하고, 경찰 출동 및 학교 휴교 등 공무집행방해와 업무방해가 발생하고 있음

○ 하지만, 현행법은 이에 대한 명확한 처벌 규정이 없어 법 개정이 시급함

○ 반면, 부가통신사업자는 사회 전반에 미치는 지대한 영향력에 비하여 법령에 의한 사회적 책무는 매우 가볍고 대표적으로 구글, 넷플릭스, 카카오, 네이버 등 '빅테크'가 있음

○ 이에 불특정 또는 다수의 사람의 생명·신체에 위해를 가하려는 내용을 정보통신망에 유포하거나 게시하여 공중의 공포심이나 불안감을 유발한 자에 대한 처벌 규정을 명시하려는 것임(안 제71조제1항제12호 신설)

• Reference

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

국내 입법 동향

「전자문서 및 전자거래 기본법」 일부개정법률안

(김의겸의원 대표발의, 2023. 8. 18. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 현행법에 따르면 전자문서의 수신자는 전자문서가 작성자의 것이었는지를 확인하기 위하여 미리 작성자와 합의한 절차를 따른 경우 등에는 전자문서에 포함된 의사표시를 작성자의 것으로 보아 행위할 수 있고, 예외적으로 수신자가 작성자로부터 전자문서가 작성자의 것이 아님을 통지받고 필요한 조치를 할 상당한 시간이 있었던 경우 등에는 전자문서에 포함된 의사표시를 작성자의 것으로 인정하지 않도록 하는 규정을 두고 있음

○ 그런데 전자서명 등이 본인의 고의나 중대한 과실 없이 제3자에 의해 위조되거나 부정한 방법으로 발급된 경우는 현행법상 전자문서에 포함된 의사표시를 작성자의 것으로 인정하지 아니하는 경우로 규정되어 있지 않아 제3자가 전자서명 등을 위조하거나 불법적으로 발급하고 이를 금융사기 등의 범죄에 이용하여 피해가 발생하더라도 피해자가 전자서명 등의 사법상 효력을 부인할 수 없게 되는 문제가 있음

○ 이에 전자서명 등이 작성자의 고의나 중대한 과실 없이 제3자에 의하여 위조 또는 그 밖의 부정한 방법으로 발급된 경우에는 전자문서에 포함된 의사표시를 작성자의 것으로 볼 수 없도록 명시함으로써 전자문서의 불법적 도용 등으로 인한 피해를 방지하려는 것임(안 제7조제3항제3호 신설)

• Reference

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

국내 입법 동향

「디지털 서비스 이용자 보호에 관한 법률」 제정법률안

(정필모의원 대표발의, 2023. 8. 23. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유

○ 최근 정보통신기술이 급속하게 발전하고 이용자의 정보통신서비스 이용양상이 다양해지는 디지털 환경하에서 새로운 권리침해 유형으로부터 디지털 서비스를 이용하는 이용자에 대한 보호 및 권리 보장을 강화할 필요가 있음

○ 그러나 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」이나 「전기통신사업법」 등 현행법만으로는 새로운 디지털 환경에 따른 이용자 보호 및 권리 보장이 미흡하다는 지적이 제기됨

○ 이에 변화하는 디지털 환경에 따른 이용자 보호 방안, 디지털 서비스 제공자의 의무 및 이용자의 권리 보장 등에 관한 사항을 별도의 법률에서 규정함으로써 이용자의 권익을 증진하고 피해를 예방하려는 것임

■ 주요내용

○ 디지털 서비스 제공자가 디지털 서비스를 제공하는 경우 고려하여야 하는 이용자 보호의 원칙과 디지털 서비스 이용자의 디지털 서비스 이용과 관련한 권리를 규정함(안 제3조 및 제4조)

○ 대규모 디지털 서비스 제공자가 정보 추천 알고리즘을 활용한 검색 또는 추천 서비스를 제공하는 경우 정보의 노출 순서 · 방식 등을 결정하는 주요 기준을 이용자가 알기 쉽게 공개하도록 함(안 제7조)

○ 디지털 서비스 제공자가 맞춤형 서비스를 제공하려는 경우 맞춤형 서비스를 제공한다는 사실을 이용자가 쉽게 인지할 수 있도록 알리고 동의를 받도록 함(안 제8조)

○ 디지털 서비스 제공자가 아동 · 청소년에게 디지털 서비스를 제공하는 경우 아동 · 청소년의 연령 등을 고려하여 아동 · 청소년의 권리가 침해되지 아니하도록 노력하고, 아동 · 청소년의 연령을 고려하여 아동 · 청소년이 쉽게 이해할 수 있도록 이용약관 등 정보를 제공하도록 함(안 제10조)

○ 이용자가 디지털 서비스 이용에 관한 권리 또는 이익을 침해받은 경우이거나 디지털 서비스 제공자가 이 법 또는 관계 법령을 위반하여 디지털 서비스를 제공한다는 사실을 알게 된 경우에는 방송통신위원회 또는 전문기관에 그 사실을 신고할 수 있도록 함(안 제23조)

○ 디지털 서비스 제공자에게 이용자를 기만하여 디지털 서비스를 제공하는 행위, 이용자의 선택을 왜곡하는 방식으로 디지털 서비스를 제공하는 행위, 디지털 서비스 제공이 제한 또는 중단되는 경우 그 사실 및 이유를 이용자에게 즉시 고지하지 아니하는 행위, 정당한 사유 없이 이용약관 등과 다르게 디지털 서비스를 제공하는 행위, 이용자의 디지털 서비스 이용정보를 부당하게 이용하는 행위를 하여서는 아니 되는 의무를 부과함(안 제26조)

○ 사실조사의 대상이 된 디지털 서비스 제공자는 해당 사실조사의 대상이 되는 행위가 해소되었거나 이용자의 피해구제 · 권익증진에 관한 방안을 마련하는 경우 동의의결을 하여 줄 것을 방송통신위원회에 신청할 수 있고, 방송통신위원회는 사실조사의 대상이 되는 행위가 해소되어 사실조사가 불필요하다고 인정하거나 이용자의 피해구제 · 권익증진에 관한 방안이 이용자 보호에 적합하다고 판단하는 경우에는 사실조사를 하지 아니한다는 취지의 동의의결을 할 수 있도록 함(안 제30조)

• Reference

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

국내 입법 동향

「온라인플랫폼시장의 공정경쟁 촉진에 관한 법률」 제정법률안

(박성준의원 대표발의, 2023. 8. 23. 제안)

■ 소관 상임위원회 : 정무위원회

■ 제안이유

○ 온라인플랫폼시장이 급성장하면서 다양한 사회적 · 경제적 편익을 발생시키고 있으나 일부 영역에서는 대형 플랫폼 업체들의 '수수료 인상', '배달료 후려치기', '입점업체 차별' 등과 같은 독점적 지위를 이용한 불공정행위로 인하여 공정한 경쟁과 소비자 편익이 저해되고 기업의 혁신을 방해하는 등 전형적인 독점의 폐해가 나타나고 있음

○ 그런데 「독점규제 및 공정거래에 관한 법률」 중심의 시장지배적 지위에 대한 판단 기준이나 시장지배적지위 남용행위에 대한 규제가 온라인플랫폼시장에는 적합하지 않아 온라인플랫폼시장의 공정한 경쟁 환경 조성을 위한 새로운 법규를 마련할 필요가 있다는 의견이 제기되고 있음

○ 이에 온라인플랫폼시장에서 과도한 시장지배력의 확장을 억제하되 독점적 지위에 있지 않은 온라인플랫폼 사업자에 대해서는 필요한 지원이 가능하도록 근거 법률을 제정함으로써 온라인플랫폼시장의 공정한 경쟁을 촉진하고 기업의 균형 성장을 도모하며 국민경제의 균형 발전에 이바지하려는 것임

■ 주요내용

○ 이 법의 목적을 온라인플랫폼시장에서 과도한 시장지배력 확장을 억제함과 아울러 시장지배적 지위에 있지 아니하는 온라인플랫폼 사업자를 지원함으로써 공정경쟁 촉진과 기업의 균형 성장을 도모하고 선순환 산업 생태계 구축 및 국민경제의 균형 발전에 이바지하는 것으로 함(안 제1조)

○ "온라인플랫폼시장"을 온라인플랫폼을 통하여 온라인플랫폼서비스가 거래되거나 온라인플랫폼서비스를 이용하여 재화 등이 거래되는 시장으로, "온라인플랫폼서비스"를 온라인플랫폼을 통하여 이용자들 간의 거래, 정보교환 등 상호작용을 촉진하는 온라인 중개서비스, 온라인 검색서비스, 온라인 사회관계망서비스 등의 서비스로, "온라인플랫폼 사업자"를 온라인플랫폼서비스 제공을 업으로 하는 자로 정의함(안 제2조)

○ 공정거래위원회는 온라인플랫폼시장에 대한 시장조사를 2년마다 실시하도록 하고, 시장조사 결과보고서를 작성 및 공표하도록 함(안 제6조)

○ 공정거래위원회는 온라인플랫폼시장에 대한 시장조사 결과 시장지배력이 있다고 인정되거나 시장점유율이 50% 이상인 온라인플랫폼사업자를 잠정적 시장지배적 플랫폼 사업자로 지정하도록 함(안 제7조)

○ 잠정적 시장지배적 사업자가 연평균 매출액 1조원 이상 등 일정 요건에 해당하게 되면 공정거래위원회에 신고하도록 의무를 부과함(안 제8조)

○ 공정거래위원회는 시장점유율이 50% 이상인 잠정적 시장지배적 사업자 또는 안 제8조에 따라 신고한 잠정적 시장지배적 사업자의 시장지배적 지위가 인정되면 시장지배적 플랫폼 사업자로 지정하도록 함(안 9조)

○ 공정거래위원회로 하여금 시장지배적 플랫폼 사업자가 제공하는 온라인플랫폼서비스 목록을 작성하여 관리하도록 함(안 제10조)

○ 온라인플랫폼시장의 공정경쟁 환경을 조성하기 위한 시장지배적 플랫폼 사업자의 의무를 명시하고, 시장지배적 플랫폼 사업자의 시장지배적지위 남용행위, 부당한 차별행위, 보복조치행위, 탈법행위를 금지함(안 제13조부터 제17조까지)

○ 시장지배적 플랫폼 사업자에게 개인정보 보호를 위한 조치 의무를 부여함(안 제18조)

○ 시장지배적 플랫폼 사업자가 주식 취득, 영업 양수, 합병 등의 기업결합을 하는 경우 공정거래위원회에 신고하여 경쟁 제한 여부에 관한 심사를 받도록 함(안 제19조)

○ 공정거래위원회로 하여금 2년마다 온라인플랫폼시장의 공정경쟁 환경 조성과 공정경쟁 촉진을 위한 공정경쟁촉진종합계획을 수립·시행하도록 함(안 제20조)

○ 중소벤처기업부장관 및 공정거래위원회로 하여금 시장지배적 플랫폼 사업자가 아닌 온라인플랫폼 사업자를 지원하기 위한 지원계획을 수립·시행하고 지원책을 마련하도록 함(안 제21조 및 제22조)

○ 공정거래위원회는 신고 또는 직권으로 위반행위를 조사할 수 있도록 하고, 이 법의 위반행위나 이 법에 따른 의무를 이행하지 아니한 온라인플랫폼 사업자에게 시정조치를 명하거나 시정권고를 할 수 있도록 함(안 제23조부터 제26조까지)

○ 공정거래위원회는 시장지배적 플랫폼 사업자가 시장지배적지위 남용행위 금지, 부당한 차별행위 금지, 보복조치행위 금지 규정을 위반한 행위로 온라인플랫폼 이용사업자 또는 최종이용자에게 회복하기 어려운 손해가 확산될 우려가 있어 이를 예방할 긴급한 필요성이 인정되는 경우 그 시장지배적 플랫폼 사업자에

대하여 해당 행위 또는 영업의 전부 또는 일부를 일시 중지할 것을 명할 수 있도록 함(안 제27조)

○ 공정거래위원회의 조사나 심의를 받고 있는 온라인플랫폼 사업자의 시장지배적 지위를 이용한 불공정한 거래 내용의 자발적 해소, 온라인플랫폼 이용사업자 등의 피해구제 또는 거래질서 개선 등을 위한 시정방안에 대한 동의의결 제도를 도입함(안 제28조)

○ 공정거래위원회는 시장지배적지위 남용행위 금지, 부당한 차별행위 금지, 보복조치행위 금지, 탈법행위 금지 규정을 위반한 시장지배적 플랫폼 사업자에게 과징금을 부과할 수 있도록 함(안 제30조)

• Reference

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

국내 입법 동향

「위치정보의 보호 및 이용 등에 관한 법률」 일부개정법률안

(임호선의원 대표발의, 2023. 8. 29. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유 및 주요내용

○ 현행법은 8세 이하의 아동, 피성년후견인 등(이하 “아동등”이라 함)의 보호의무자가 아동등의 생명 또는 신체의 보호를 위하여 아동등의 개인위치정보의 수집 · 이용 또는 제공에 동의하는 경우 본인의 동의가 있는 것으로 본다고 규정함

○ 그런데 최근 인구구조가 고령화되고 치매환자에 대한 국가의 책임이 강조됨에 따라 치매환자의 경우에도 생명 또는 신체의 보호를 위하여 보호의무자가 개인위치정보의 수집 · 이용 또는 제공에 동의할 수 있도록 하여 치매환자의 실종 등에 신속하게 대응하여야 한다는 지적이 제기됨

○ 이에 「치매관리법」 제2조제2호에 따른 치매환자로서 대통령령으로 정하는 기준에 해당하는 사람의 보호의무자가 치매환자의 개인위치정보의 수집 · 이용 또는 제공에 동의하는 경우 치매환자의 동의가 있는 것으로 보도록 규정하여 치매환자에 대한 적극적인 보호를 하려는 것임(안 제26조)

• Reference

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

국내 입법 동향

「국가전략기술 육성에 관한 특별법」 일부개정법률안

(박정의원 대표발의, 2023. 8. 2. 제안)

■ 소관 상임위원회 : 과학기술방송통신위원회

■ 제안이유 및 주요내용

○ 현행법은 기술육성주체가 외국의 정부 등으로부터 국가전략기술과 관련된 정보의 제공을 요청받은 경우 그 사실을 관계 중앙행정기관의 장에게 알리도록 규정하고 있음

○ 그런데 국가전략기술은 외교·안보 측면의 전략적 중요성이 인정되고 국민경제 및 연관 산업에 미치는 영향이 큰 정보라는 점에서 국가 안전보장이나 국민경제에 악영향을 미치지 않도록 무분별한 정보의 유출을 방지하여야 할 필요성이 있음

○ 이에 기술육성주체가 외국의 정부 등으로부터 국가전략기술과 관련된 정보의 제공을 요청받은 경우 관계 중앙행정기관의 장과 협의를 거쳐 해당 정보의 제공 여부를 결정하도록 함으로써 국가전략기술에 대한 정보보호와 보안이 체계적으로 이루어질 수 있도록 하려는 것임(안 제27조)

• Reference

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

국내 입법 동향

「인공지능 책임 및 규제법」 제정법률안

(안철수의원 대표발의, 2023. 8. 8. 제안)

■ 소관 상임위원회 : 과학기술정보방송통신위원회

■ 제안이유

○ 세계적으로 인공지능이 교통, 의료, 서비스 등 다양한 분야에 활용되면서 일상생활의 편의 증진은 물론 산업적 활용 가능성에 대한 기대를 높이고 있음

○ 이처럼 인공지능의 개발·이용이 거의 모든 산업분야에 적용되어 부가가치를 창출할 것으로 예상되고 있으나, 다른 한편으로는 인공지능의 위험성에 대한 우려도 확대되고 있음. 특히 인공지능기술은 대량의 데이터를 학습하여 성능을 향상시키는 기계학습에 기반하고 있어 불확실성과 불투명성을 가지고 있으며, 노이즈 데이터로 인한 오류생성 가능성도 큼

○ 따라서 인공지능기술이 특정 분야에서 인간의 통제수준을 넘어서서 고의적으로 악용될 수 있는 문제에 대한 법적 규제의 필요성이 있음

○ 이에 향후 신뢰할 수 있는 인공지능의 사용환경을 조성하기 위하여 인공지능의 개발 및 이용에 관한 기본원칙, 인공지능사업자의 책무 및 이용자의 권리를 규정하고, 금지된 인공지능·고위험 인공지능·저위험 인공지능으로 인공지능의 유형을 구분하여 이용자를 보호하기 위한 인공지능과 관련한 시책을 구분하여 마련하도록 하는 등 안전하고 신뢰할 수 있는 인공지능기술·정책의 제도적 기반을 조성하려는 것임

■ 주요내용

○ 안전하고 신뢰할 수 있는 인공지능의 개발·이용을 위한 기반 조성 및 인공지능 관련 정책의 수립·추진에 필요한 사항을 규정하여 국민의 권익과 존엄성을 보호하고 국민의 삶의 질을 높이는 것을 목적으로 함(안 제1조)

○ 인공지능, 금지된 인공지능, 고위험 인공지능, 저위험 인공지능 및 인공지능사업자 등에 대하여 정의함(안 제2조)

○ 금지된 인공지능 이외의 인공지능 개발 및 이용에 대하여 우선허용 · 사후규제 원칙을 정함(안 제5조)

○ 금지된 인공지능은 원칙적으로 개발을 금지함(안 제6조)

○ 저위험 인공지능의 개발 및 이용은 원칙적으로 허용하되, 이용자의 생체정보를 감지해서 상호작용을 하는 경우 또는 사진 · 음성 · 영상 등을 실제와 같이 만들어 내는 경우에는 해당 사실을 공시하도록 함(안 제7조)

○ 고위험 인공지능으로부터 이용자 보호를 위한 정부의 역할, 사업자의 책무, 이용자의 권리 등을 규정함(안 제8조부터 제11조까지)

○ 과학기술정보통신부장관이 3년마다 인공지능의 안전하고 합리적인 개발 및 이용을 위하여 인공지능 기본계획을 인공지능위원회의 심의 · 의결을 거쳐 수립 · 시행하도록 하고, 기본계획에는 인공지능에 관한 정책의 기본 방향과 전략, 신뢰 기반 조성 등에 관한 사항이 포함되도록 함(안 제12조)

○ 인공지능사회의 구현, 인공지능산업의 신뢰 확보와 관련된 사항을 심의 · 의결하기 위하여 국무총리 소속으로 인공지능위원회를 두도록 하고, 인공지능위원회는 기본계획의 수립 및 그 추진상황 점검 · 분석에 관한 사항 등을 심의 · 의결하도록 함(안 제13조 및 제14조)

○ 과학기술정보통신부장관이 인공지능 등이 국민의 생활에 미치는 잠재적 위험을 최소화하고 안전한 인공지능의 이용을 위한 신뢰 기반을 조성하기 위한 시책을 마련하도록 함(안 제19조)

○ 금지된 인공지능 및 고위험 인공지능에 대한 확인제도를 마련함(안 제21조부터 제23조까지)

○ 고위험 인공지능사업자는 인공지능의 신뢰성과 안전성을 확보하기 위한 조치를 하도록 함(안 제24조)

• Reference

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

국내 입법 동향

「전자정부법」 일부개정법률안

(이만희의원 대표발의, 2023. 8. 25. 제안)

■ 소관 상임위원회 : 행정안전위원회

■ 제안이유

○ 최근 인공지능, 빅데이터 등 디지털 신기술에 기반한 과학적 의사결정, 지능형 서비스 제공이 가능해지고 국민의 디지털 환경에 대한 적응력 및 이해가 높아짐에 따라, 정부도 이를 반영한 새로운 혁신전략으로 디지털플랫폼정부로의 전환을 천명하고 실현계획을 발표하여 추진 중임

○ 특히 디지털플랫폼정부 구현을 위한 추진과제 상당수가 전자정부서비스를 기반으로 진일보하고 있어 이를 뒷받침하기 위한 법제의 보완이 필요한 상황임

○ 이에 개별법령 개정으로 추진 중이었던 전자신분증 전반에 대한 포괄적인 근거를 마련하고, 기존의 서비스 제공방식을 확장하여 이용자에게 필요한 공공서비스를 선제적으로 안내하며, 이용자 누구나 공공웹·앱에 쉽게 접근할 수 있도록 전자정부서비스 설계에 대한 관리체계를 마련하고, 이용자가 개별 공공웹사이트를 방문할 필요 없이 전자정부서비스를 한 곳에서 이용할 수 있는 통합창구를 구축하는 한편, 민간웹·앱에서도 전자정부서비스를 제공받을 수 있도록 하기 위한 법적 근거를 마련하고자 함

○ 또한, 기존에는 본인에 관한 행정정보를 제3자에게 제공하도록 요구할 수 있는 당사자가 개인으로 한정되어 있던 것을 기업, 단체 등으로 확대하고, “개인 및 기업, 단체 등”에게 본인정보를 열람하고 정정을 요구할 수 있는 권리를 새롭게 부여하며, 행정정보 공동이용 활성화를 위하여 승인요건을 완화하고, 기관 간 행정정보를 유통할 필요가 있는 경우 이를 지원하기 위한 정보유통 시스템의 근거를 마련하고자 함

■ 주요내용

○ 전자신분증 발급근거 및 인증체계 마련(안 제10조의2, 제10조의3, 제10조의4)

- 행정기관등의 장은 정보주체의 신청에 따라 전자신분증을 발급할 수 있고, 발급된 전자신분증은 전자적 형태라는 이유만으로 신분증으로서의 효력이 부인되지 아니하도록 규정함

- 행정기관등, 법인 또는 단체 등은 전자신분증을 발급받아 저장하고, 이를 표시하거나 제출하는 등의 서비스를 제공할 수 있고, 이 중 공공기관, 법인 또는 단체 등은 대통령령으로 정하는 인증 기준에 따라 행정안전부장관에게 인증을 받도록 하는 규정을 신설함

○ 이용자에게 공공서비스를 선제적으로 안내할 수 있는 근거 마련(안 제12조의2, 제12조의3, 제12조의4)

- 행정안전부장관이 공공서비스의 자격요건 등을 확인하여 이용가능성이 있는 공공서비스를 안내(이하 “공공서비스 맞춤 안내”)하고, 공공서비스 맞춤안내를 위하여 이용자의 사전 동의를 받아 다른 행정기관등이 보유한 자료의 제공을 요청할 수 있도록 함

○ 전자정부서비스 이용자의 편의 증진을 위하여 서비스 설계 지침에 기반한 관리체계 마련(안 제16조, 제16조의2)

- 중앙사무관장기관의 장은 이용자의 편의 증진을 위한 서비스 설계에 관한 지침을 정하여야 하고, 행정기관등의 장은 특별한 사유가 없으면 이 지침을 준수하도록 함

- 중앙사무관장기관의 장은 행정기관등에서 개발 · 제공하는 전자정부서비스에 대하여 지침 준수 여부, 이용자 편의 수준 등을 점검하고 그 결과를 공표할 수 있고 필요한 경우 개선을 권고할 수 있으며, 권고를 받은 행정기관등의 장은 개선에 필요한 조치를 하여야 함

○ 전자정부 통합포털 구현(안 제20조)

- 행정안전부장관은 행정기관등이 제공하는 전자정부서비스를 한 곳에서 통합적으로 제공할 수 있도록 전자정부 통합포털(이하 “통합포털”)을 구축 · 운영하고, 행정기관등의 장은 통합포털과 소관 전자정부서비스를 상호 연계하도록 함

- 전자정부서비스 이용자가 통합포털에서 전자정부서비스를 신청한 경우에는 해당 전자정부서비스에 관한 법률 또는 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 및 대통령령에 따라 해당 전자정부서비스를 소관하는 행정기관등에 전자정부서비스를 신청한 것으로 보도록 함

○ 전자정부서비스 민간개방 활성화(안 제21조)

- 행정안전부장관은 전자정부서비스를 개방하려는 경우 이를 효율적으로 지원할 수 있는 정보시스템을 구축 · 운영할 수 있고, 행정기관등의 장은 전자정부서비스를 개방하려는 경우 해당 정보시스템의 활용을 우선적으로 고려하도록 함

- 행정안전부장관은 전자정부서비스 개방에 관하여 필요한 요건, 절차 및 기술 표준 등을 정할 수 있으며 ,행정기관등의 장은 특별한 사유가 없으면 이를 준수하도록 함

○ 행정정보 공동이용 활성화(안 제39조, 제43조)

- 행정안전부장관은 공동이용 승인을 하기 전에 행정정보보유기관의 장의 의견을 들어야 하며, 행정정보보유기관의 장은 1개월 이내에 의견을 제시할 수 있도록 함

- 법률에 규정한 사유 외에 행정정보 공동이용 절차의 간소화가 필요한 경우 대통령령으로도 정할 수 있도록 함

○ 본인정보 통제권 강화(안 제43조의2, 제43조의3, 제43조의4)

- 민간등(개인 및 기업, 단체 등)은 본인정보를 보유하고 있는 행정기관등의 장에게 본인정보를 제3자에게 전자적으로 제공하도록 요구할 수 있도록 함

- 민간등은 본인정보를 보유하고 있는 행정기관등의 장에게 본인정보에 대한 열람을 요구할 수 있고, 해당 정보가 사실과 다른 경우 정정을 요구할 수 있도록 함

- 행정기관등의 장은 정보주체가 「개인정보보호법」제35조의2에 따른 전송 요구를 통하여 본인에 관한 개인정보를 제공하는 경우에는 정보주체에게 별도로 요구할 수 없도록 함

○ 공통기능 서비스 제공 근거 신설(안 제51조)

- 행정안전부장관은 다수의 전자정부서비스에 공동 활용할 수 있는 표준화된 기능(이하 “공통기능”)을 제공할 수 있고, 행정기관등의 장은 전자정부서비스를 개발할 때 공통기능을 우선적으로 활용할 수 있도록 함

○ 정보유통시스템 구축 · 운영 근거 마련(안 제52조의2)

- 행정안전부장관은 제36조에 따른 행정정보 공동이용, 제43조의2에 따른 본인에 관한 행정정보의 제공 요구 등이나 그 밖에 기관 간 행정정보를 유통할 필요가 있는 경우, 이를 통합적으로 지원하는 정보시스템을 구축 · 운영할 수 있도록 함

○ 전문기관의 역할 확대(안 제71조)

- 전문기관이 수행하는 업무 범위에 제51조에 따른 공통기능의 제공 및 활용에 관한 업무, 제52조의2에 따른 정보유통 시스템 구축 · 운영에 관한 업무를 추가함으로써 그 역할을 확대함

• Reference

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

해외 입법 동향

미국 증권거래위원회, 상장사에 대한 사이버보안 위험 관리 및 사고 공개에 관한 규칙 채택(2023. 7. 26.)

미국 증권거래위원회(SEC[1])는 상장사에 대한 중대한 사이버보안 사고, 사이버보안 위험 관리, 전략, 거버넌스와 관련된 중요정보를 매년 공개하도록 요구하는 규칙을 채택(2023. 7. 26.)

■ 개요

○ 미국 증권거래위원회(SEC)는 지난 7월 26일 상장사에서 발생하는 중대한 사이버보안 사고를 공개하도록 하는 한편 사이버보안 위험에 대한 관리 등 중요한 정보를 매년 공개하도록 하는 규칙을 채택하였으며, 9월 5일에 발효될 예정임

- 특히, 증권거래위원회(SEC)의 의장은 “사이버보안 사고로 수백만 개의 파일을 손실하는 것은 투자자들에게 중요한 문제”라며 현재 많은 상장사가 투자자에게 사이버보안 사고에 대한 정보를 공개하여 제공하고 있지만, 동 규칙을 통해 공개 방식이 일관된 방식으로 이루어지길 바란다고 언급함

■ 주요내용

① 중대한 사이버보안 사고 공개

○ **(사이버보안 사고 정의)** 동 규칙은 사이버보안 사고를 “등록자의 정보시스템이나 그 안에 있는 모든 정보의 기밀성, 무결성 또는 가용성을 위태롭게 하는 등록자의 정보시스템에서 또는 정보시스템을 통해 무단으로 발생한 사고”로 광범위하게 정의함

○ **(공개 시기)** 기업은 사이버보안 사고의 발생을 인지할 시 지체없이 중대성 여부를 판단하여야 하며, 중대하다고 판단하는 경우 중대성 결정 후 영업일 기준 4일 이내에 해당 사고를 공개해야 함

- 다만, 중대한 사이버보안 사고에 해당하더라도 공개해야하는 정보가 제출 시점에 결정되지 않거나 사용할 수 없는 경우 추후에 공개 내용을 업데이트해야 함

1) U.S. Securities and Exchange Commission

- **(예외 사항)** 증권거래위원회(SEC)는 중대한 사이버보안 사고 공개 지연에 대해 다음의 경우에 한하여 예외적으로 허용함

  · **(위험가능성)** 미국 법무부(DOJ[2])장관이 해당 사고가 즉시 공개될 경우 국가 안보나 공공 안전에 상당한 위험을 초래한다고 결정한 때에는 증권거래위원회(SEC)에 서면으로 통보해야 함

  · **(연방통신위원회 통지 규칙과의 충돌 가능성)** 고객정보(CPNI[3])관련 위반사항에 대해 연방통신위원회(FCC[4])의 통지 규칙[5]의 적용을 받는 기업은 증권거래위원회(SEC)에 서면 통지를 통해 최대 7일까지의 지연을 허용함

※ 증권거래위원회(SEC)는 연방통신위원회(FCC)가 7일의 대기 기간을 없애는 내용의 규칙 개정을 제안했으며, 제안이 채택될 경우 충돌이 해소될 것이라고 언급함

○ **(공개 범위)** 기업은 중대한 사이버보안 사고를 공개할 때, 사고의 성격, 범위 및 시기, 재무 상태 및 운영 결과를 포함하여 회사에 미치는 중대한 영향에 대한 측면을 공개해야 함

② 사이버보안 위험 관리, 전략, 거버넌스 공개

○ **(위험 관리 및 전략 공개)** 기업은 사이버보안 위협에 따른 중대한 위험을 평가, 식별 및 관리하기 위하여 투자자가 합리적으로 프로세스를 이해할 수 있도록 충분히 설명해야 하며 공개 시 기업은 다음과 같은 항목을 다루어야 함

- ▲프로세스가 기업 전체의 위험 관리시스템 또는 프로세스에 통합되었는지 여부 및 방법 ▲기업이 프로세스 관련 컨설턴트, 감사 또는 제3자에 대한 고용 여부 ▲기업이 타 서비스 제공업체와 관련된 사이버보안 위협으로부터 위험을 감독하고 식별하는 프로세스를 갖추고 있는지 여부

- 또한, 기업은 이전 사이버보안 사고의 결과를 포함하여 사이버보안 위협에 따른 위험이 사업 전략, 기업 운영, 재무 상태를 포함하여 기업에 실질적인 영향을 미치거나 어떻게 영향을 미칠 가능성이 있는지를 설명해야 함

○ **(거버넌스 공개)** 동 규칙은 기업이 이사회에게 사이버보안 위협으로 인한 위험에 대한 설명을 요구하고 위험을 감독할 책임이 있는 이사회 위원회 또는 소위원회를 식별하며 위험에 대해 통지받는 프로세스와 중대한 위험을 평가하고 관리하는 경영진의 역할을 설명해야 하며 다음과 같은 항목의 확인을 요구함

2) Department of Justice
3) Customer Proprietary Network Information, 유선 및 무선 통신 회사의 가입자에 대하여 얻는 정보
4) Federal Communications Commission
5) 46 CFR § 64.2011(b)(1), 해당 기업은 고객정보(CPNI)와 관련한 위반에 대해 합리적으로 판단한 후 영업일 기준 7일 이내에 미 비밀경호국(USSS) 및 연방수사국(FBI)에 통지해야 하며 7일이 경과할 때까지 위반 사실을 공개하여서는 아니 됨

- ▲위험을 평가하고 관리할 책임이 있는 관리 직책 또는 위원회의 존재 여부와 해당 전문지식을 설명하는데 필요한 세부 정보 ▲해당 직원 또는 위원회가 사이버보안 사고의 예방, 탐지, 완화 및 해결에 대한 정보를 얻고 모니터링하는 프로세스 정보 ▲해당 직원 또는 위원회가 위험에 대한 정보를 이사회 또는 이사회의 위원회 또는 소위원회에 보고하는지 여부

○ **(비(非)미국 발행사[6])** 동 규칙은 비(非)미국 발행사에 대해서도 위험 관리, 전략 및 거버넌스 항목과 유사한 요건을 요구하고 기존 제출 양식 항목에 "중대한 사이버보안 사고" 관련 내용을 추가하였으며, 비(非)미국 발행사는 외국 관할권의 증권거래소 또는 증권 보유자에게 공개하는 중대한 사이버보안 사고 관련 정보를 제출 양식에 따라 제공해야 함

■ 고려사항 및 다음 단계

○ **(새로운 요구사항에 대응)** 기업은 사이버보안 사고에 대응하기 위한 절차를 검토 및 테스트하고 새로운 보고 요건에 따라 고려되는 절차 및 관련 문서를 적절하게 수정하고 보완해야 함

○ **(공개 지연에 대한 제한적 허용)** 중대한 사이버보안 사고의 공개를 연기하는 경우에 대해 극히 일부의 상황에서만 자격이 주어진다는 점을 고려할 필요가 있음

○ **(프로세스 재검토)** 최종 채택된 규칙은 제안된 규칙보다는 덜 규범적이지만, 여전히 기업이 사이버보안 위험 관리 프로세스와 관련하여 공개할 세부 사항이 많아 프로세스의 개발 시 재검토를 해야 함

○ **(신중한 초안 작성)** 기업은 중대한 사이버보안 사고 및 기업의 위험 관리 프로세스에 관하여 증권거래위원회(SEC)에 해당 정보를 공개 함에 있어 신중한 초안 작성이 요망됨

- 기업은 중요한 정보를 적시에 공개해야 하는 의무가 있고 해당 정보의 공개를 통해 의도치 않게 기업의 사이버보안 약점이 노출되어 악의적인 행위자가 악용할 수 있으므로 둘의 균형을 적절하게 맞추는 내용의 초안을 신중히 작성해야 함

6) Foreign Private Issuers

■ 시사점

○ 미국 증권거래위원회(SEC)는 2022년 3월 동 규칙의 초안을 제안한 바 있으나, 최종 채택된 현재 규정은 기업의 규제 부담을 보다 완화하는 한편, 일부 공개사항을 변경하고 간소화하도록 수정·보완되었음

○ 동 규칙은 상장사가 중대한 사이버보안 사고 공개, 사이버보안 위험 관리 등 중요한 정보를 매년 일관성 있는 방식으로 공개하도록 함으로써 기업이 사이버보안에 대한 더 높은 관심과 중요성을 인지하도록 하는 점에서 긍정적인 효과가 기대됨

- 또한, 사이버보안 관련 중요한 정보를 매년 공개하도록 하여 투자자들의 의사결정에 있어 도움을 줄 것으로 예상됨

• Reference

https://www.sec.gov/news/press-release/2023-139
https://www.gibsondunn.com/sec-adopts-new-rules-on-cybersecurity-disclosure-for-public-companies/
https://www.wfw.com/articles/sec-adopts-new-rule-regulating-cybersecurity-disclosures/
https://www.lexology.com/library/detail.aspx?g=acdcf1a2-5669-4ce0-9b7f-347e3e15f4dd
https://www.lexology.com/library/detail.aspx?g=24f0fd5e-efe7-4405-b020-5e4102120878

해외 입법 동향

미국 하원, 「 2023 사이버쉴드법(안)」 발의
(2023. 7. 13.)

미국 하원은 사이버보안 및 데이터 보안을 준수하는 인터넷 연결 제품의 식별 및 홍보를 위하여 자발적인 사이버쉴드 프로그램을 구축하도록 하는 「2023 사이버쉴드법(안)[1]」 발의 (2023. 7. 13.)

■ 개요

○ 미국 하원은 사이버보안 및 데이터 보안의 기준, 가이드라인, 모범 사례, 방법, 절차, 프로세스 등을 충족하는 인터넷 연결 제품(Internet-connected products)을 파악하고 홍보하기 위하여 자발적인 사이버쉴드 프로그램을 구축하도록 하는 「2023 사이버쉴드법(안)」 발의함

■ 주요내용

○ **(사이버쉴드 자문위원회[2])** 상무부 장관[3]은 본 법 제정일로부터 90일 이내에 사이버쉴드 자문위원회를 설립해야 함

- **(자문위원회 의무사항)** 자문위원회는 본 법 제정일로부터 1년 이내에 상무부 장관에게 ▲사이버쉴드 라벨 형식 및 내용 ▲자발적 사이버보안 및 데이터 보안에 대한 벤치마크[4]의 식별, 확립, 보고, 채택, 유지 및 촉진을 위한 프로세스에 대한 권고사항을 제공해야 하며(안 제3조b(1)), 해당 권고사항을 일반에 공표하는 한편 의견 제시의 기회를 제공해야 함(안 제3조b(2))

- **(자문위원회의 구성)** 상무부 장관은 일정 자격요건을 갖춘 자를 자문위원회 위원으로 임명함

구분	자문위원회 구성
자격요건	·(i) 중소기업 및 대기업을 포함한 대상제품(covered products) 산업의 대표자; ·(ii) 암호 분석, 하드웨어 및 소프트웨어 보안, 무선 및 네트워크 보안, 클라우드 보안, 데이터 프라이버시 등의 분야를 전문으로 하는 사이버보안 연구원을 포함한 사이버보안 전문가; ·(iii) 공익운동가

1) Cyber Shield Act of 2023 (H.R.4623)
2) Cyber Shield Advisory Committee
3) Secretary of Commerce
4) '벤치마크'란 기준, 가이드라인, 모범 사례, 방법, 절차 및 프로세스를 뜻함(안 제2(2))

구분	자문위원회 구성
	· (iv) 국립표준기술연구소법 제21조(a)에 따라 설립된 정보보안 및 개인정보보호자문위원회[5]의 연락 담당자로서, 해당 제21조 (a) 제3항에 기술된 해당 위원회의 위원; · (v) ▲상무부[6] ▲국립표준기술연구소[7] ▲연방 무역 위원회[8] ▲연방통신위원회[9] ▲소비자 제품 안전 위원회[10]의 인증, 적용대상 장치 또는 사이버보안에 대한 전문 지식을 보유한 연방 직원 등

○ **(사이버쉴드 프로그램)** 상무부 장관은 사이버보안을 강화하고 데이터를 보호하기 위해 업계 최고의 사이버보안 및 데이터 보안 벤치마크를 충족하는 대상제품 및 대상제품의 부속품(subsets)에 대한 자발적 인증 및 라벨링을 통해 대상제품을 식별하고 인증하는 자발적인 프로그램을 수립해야 함(안 제4조(a))

· **(라벨)** 사이버쉴드 프로그램에 따라 대상제품에 적용되는 라벨은 ▲디지털로 구성되며, 가능할 경우 물리적이어야 하며, 대상제품 또는 포장에 부착되어야 하며, ▲ 사이버보안 및 데이터 보안 벤치마크 충족 정도를 표시하는 다양한 등급의 형태임

– **(상무부 장관의 역할)** 상무부 장관은 이해당사자와 기타 연방기관의 장을 소집하고 협의함으로써 사이버쉴드 라벨이 부착된 대상제품의 사이버보안 및 데이터보안 벤치마크를 설정하고 관리하여 보다 좋은 성능을 발휘하도록 보장해야 하므로 다음의 역할을 수행해야 함(안 제4(c))

〈 사이버쉴드 프로그램 수행을 위한 상무부 장관의 주요 역할 〉

주요 역할	해당 내용
기준 수립	· (i) 공개적인 대중의견 수렴 및 절차에 참여해야 함 · (ii) 자문위원회와 협의하여 각 부속품(subsets)과 관련하여 다음의 사항을 기준으로 사이버보안 및 데이터 보안 벤치마크를 식별하고 적용해야 함 * (기준 사항) ▲ 하위집합의 대상제품과 관련된 사이버보안 및 데이터 보안 위험; ▲ 하위집합의 대상제품에 따라 수집, 전송 또는 저장되는 정보의 민감도; ▲하위집합에 포함된 대상제품의 기능성; ▲하위 집합의 대상제품을 개발하고 제조하는 데 사용되는 보안 관행 및 테스트 절차; ▲ 대상제품의 사이버보안을 책임지는 하위집합의 대상제품 제조업체가 고용한 직원의 전문성, 자격 및 전문적인 인증 수준 ▲ 기타 자문위원회와 장관이 필요하고 적절하다고 결정하는 기준 · (iii) 국립표준기술연구소가 2019년 7월에 발표한 "보안 IoT 장치를 위한 핵심 사이버보안 기능 기준선: IoT 장치 제조업체를 위한 출발점[11]"에 정의된 사이버보안 및 데이터 보안 벤치마크 또는 그 후속모델을 가능한 범위 내에서 통합해야 함
라벨 부착 허가	· 장관은 대상제품이 사이버쉴드 라벨 적용 대상에 해당할 경우 제조업체 또는 유통업체가 해당 라벨을 표시할 수 있도록 허가해야 함
기술·관행·정책 촉진	· ▲사이버 보안 강화 ▲ 대상제품의 라이프사이클의 모든 측면에 통합되도록 사이버보안 보장 ▲데이터 보호를 위해 시장에서 선호되는 기술, 관행 및 정책을 결정함
인식 개선	· 공공 지원, 교육, 연구 개발 및 기타 수단을 통해 사이버쉴드 라벨에 대한 일반의 인식 개선을 위해 노력해야 함

5) Information Security and Privacy Advisory Board
6) Department of Commerce
7) National Institute of Standards and Technology
8) Federal Trade Commission
9) Federal Communications Commission
10) Consumer Product Safety Commission
11) Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers"

주요 역할	해당 내용
라벨의 무결성 보존	· 사이버쉴드 라벨의 무결성을 보존해야 함(필요시 해당 제품이 다음 사항에 대해 적절한 적합성 표준을 충족할 때까지 사이버쉴드 프로그램에 따른 인증 대상 제품으로 취급하지 않을 수 있음) * (적합성 표준 기준) ▲(A)공인된 제3자 인증 실험실 또는 사이버쉴드 프로그램에 따른 기타 기관의 시험과 관련된 표준 ▲(B) 대상제품이 사이버보안 및 데이터 보안 벤치마크를 충족한다는 것을 (A)호에 따른 실험실 또는 단체로부터의 인증

- **(관계기관과의 협의)** 상무부장관은 이해당사자, 보건복지부 장관[12], 식품의약청장[13], 국토안보부 장관[14] 및 기타 관계 연방기관의 장과 협의하여 본 법률 시행 90일 이내 프로세스를 수립하여야 하며(안 제4(b)), 사이버보안 및 데이터 보안 벤치마크를 임의적으로 또는 재량권을 남용하여 설정할 수 없음

- **(프로그램 평가)** 상무부 감사관[15]은 사이버보안 및 데이터 보안 벤치마크를 설정한 날로부터 3년 후(이후 매 3년마다) 다음 조치를 수행해야 함(안 제4(f))

  · ▲ 사이버쉴드 프로그램 평가 ▲ (i) 상원 상업, 과학 및 교통 위원회[16] (ii) 하원 에너지 및 상업 위원회[17]에 평가 결과 보고서 제출

〈 사이버쉴드 프로그램 평가 요건 〉

구분	평가 항목
사이버쉴드 프로그램 평가 요건	· ▲(i) 사이버 보안 및 데이터 보안 벤치마크가 사이버 보안 및 데이터 보안 위협을 다루는 정도 (ii) 사이버 보안 및 데이터 보안 벤치마크의 개선 여부 및 새로운 사이버 보안 및 데이터 보안 위협에 대응하는지 여부 평가 ▲사이버쉴드 프로그램에 따른 인증 시험의 무결성을 평가하기 위해 대상제품의 진단테스트 실시 ▲사이버쉴드 프로그램에 참여하는 대상제품의 제조업체 비용 평가 ▲대상제품 제조업체의 사이버쉴드 프로그램 참여 수준 ▲사이버쉴드 라벨에 대한 대중의 인식 및 소비자 인식 수준 평가 ▲사이버쉴드 프로그램과 유사한 민간 부문 또는 국제 사이버 보안 인증 프로그램의 존재여부 검토 (존재하는 경우, 해당 인증 프로그램과 사이버쉴드 프로그램과의 상호 관계 비교·평가)

○ **(사이버쉴드 디지털 대상제품 포털[18])** 상무부장관은 상무부 웹사이트에서 검색할 수 있도록 ▲사이버쉴드 프로그램 정보를 제공하는 웹 페이지 ▲사이버쉴드 프로그램에 따라 인증된 대상제품의 데이터베이스 ▲소비자의 질문/불만 사항을 접수 할 수 있도록 사이버쉴드 프로그램 인증 적용된 대상제품의 제조업체 연락처 정보 등을 일반에 공개해야 함

■ 전망 및 시사점

12) Secretary of Health and Human Services
13) Commissioner of Food and Drugs
14) Secretary of Homeland Security
15) Inspector General of the Department of Commerce
16) Committee on Commerce, Science, and Transportation of the Senate
17) Committee on Energy and Commerce of the House of Representatives
18) CYBER SHIELD DIGITAL COVERED PRODUCT PORTAL

○ 본 법안은 지난 2017년에 발의된 사이버쉴드법[19]과 유사한 내용으로써, 미 상무부로 하여금 사이버쉴드 자발적 프로그램을 구축하도록 하고 해당 기준에 부합할 경우 인터넷 연결 제품의 안정성을 식별, 인증 및 라벨링할 수 있도록 하는 사이버보안 인증제도의 성격임

○ 한편, 미국 연방통신위원회(FCC)는 8월 24일에 IoT 제조업체가 NIST의 개발 기준에 따른 엄격한 사이버보안 요건을 충족할 경우 'US 사이버 신뢰 마크[20]'를 부착할 수 있도록 하는 사이버보안 라벨링 프로그램에 대한 규칙제정안을 공고(NPRM[21])하였고, 의견 수렴을 진행하고 있음

- FCC가 제안한 사이버 신뢰 프로그램은 소비자가 인터넷 연결기기를 구매할 경우 관련 정보를 식별할 수 있도록 하는 한편, 제조업체가 더 높은 사이버보안 표준을 충족하도록 인센티브를 제공하기 위함

○ 이렇듯, 최근 IoT기기의 사용도가 증가함에 따라 관련 위협이 높아지고 있어 제품의 안정성과 신뢰성을 보다 강화하기 위해 인증제도 도입 등의 움직임이 활발해지고 있으며 이를 통해 소비자 보호 효과가 기대됨

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/4623/text?s=9&r=581
https://incompliancemag.com/fcc-releases-nprm-on-cybersecurity-labeling-program/
https://www.meritalk.com/articles/fcc-seeking-comments-on-new-u-s-cyber-trust-mark-label/
https://www.congress.gov/bill/115th-congress/house-bill/4163?q=%7B%22search%22%3A%5B%22Cyber+Shield+Act%22%5D%7D&s=2&r=1

19) 본 법안(H.,R.4163)은 지난 2017년 10월 115th 의회에서 발의되었으나 입법화 되지 못하고 폐기됨
20) 'U.S. Cyber Trust Mark', NIST에서 발표한 사이버보안 기준을 기반으로 강력한 암호, 데이터 보호, 소프트웨어 업데이트 및 사고 탐지 기능 등을 충족하는 IoT제품에 라벨을 부착하도록 하는 것임
21) Notice of Proposed Rulemaking

해외 입법 동향

미국 하원, 「연방 사이버보안 취약성 감소법(안)」 발의

(2023. 8. 22.)

미국 하원은 연방계약자들을 대상으로 NIST지침에 따른 취약성 공개 정책[1]을 준수하도록 하는 내용의 「연방 사이버보안 취약성 감소법(안)[2]」 발의 (2023. 8. 22.)

■ 개요

○ 미국 하원은 연방 사이버보안 취약성 감소를 위하여 연방계약자들을 대상으로 'NIST지침에 따른 취약성 공개 정책(이하 '취약성 공개 정책')'을 준수하도록 하는 내용의 법안을 발의함

■ 주요내용

○ **(연방조달규정 내 취약성 공개 정책)** 본 법 제정일로부터 180일 이내에 예산관리실장[3]은 CISA청장[4], 국가사이버국장[5]과 NIST소장[6] 및 기타 관계 행정부 장관과 협의하여 연방조달규정(FAR)[7] 계약 조건 및 계약자 취약성 공개 프로그램 언어[8]등에 대해 검토하고 연방조달규정위원회(FAR위원회)[9]에 관련 업데이트 사항을 권고해야 함(안 제2(a))

- 권고사항에는 'IoT를 포함한 정보시스템과 관련된 보안 취약점에 대한 공개 프로세스 지침(2020년 IoT 사이버보안 개선법[10] 제5항)'에 따라 대상계약자(Covered contractors)[11]를 위한 취약성 공개 정책을 구현하도록 설계된 요구조건에 대한 업데이트가 포함되어야 함

○ **(조달 요건)** 연방조달규정위원회는 제2조(a)항에 따라 수립된 계약 언어를 검토하고 대상계약자가

1) vulnerability disclosure policy
2) Federal Cybersecurity Vulnerability Reduction Act of 2023 (H.R.5255)
3) Director of the Office of Management and Budget
4) Director of the Cybersecurity and Infrastructure Security Agency
5) National Cyber Director
6) Director of the National Institute of Standards and Technology
7) Federal Acquisition Regulation
8) language for contractor vulnerability disclosure programs
9) Federal Acquisition Regulation Council.
10) IoT Cybersecurity Improvement Act of 2020
11) 미국 행정명령(United codes) 제41장 제7101조에 정의된 개념을 인용하는 것으로 단순화된 취득 임계값과 같거나 보다 큰 금액으로 계약된 계약자를 뜻함(본 법안 제2조(f)(1)에 해당 정의규정 명시)

'계약자가 소유하거나 통제하는 정보시스템과 관련된 잠재적 보안 취약성 정보'를 받기 위한 요건 등을 통합하기 위해 필요한 경우 연방조달규정을 업데이트 해야 함(안 제2(b))

〈 연방조달규정 업데이트 요건 (안 제2(c)) 〉

구분	연발조달규정 업데이트 사항
요건	• IoT를 포함한 정보시스템과 관련된 보안 취약점에 대한 공개 프로세스 지침[12] 및 IoT를 포함한 기관 정보시스템과 관련된 보안 취약점의 공동 공개 구현[13](2020년 IoT 사이버보안 개선법[14] 제5항 및 제6항)에 따라 요구되는 NIST지침 및 계약자를 위한 OMB 이행사항에 최대한 부합해야함 • 산업계의 우수사례 및 국제표준기구의 표준 등과 최대한 일치해야 함
예외	• 단, 계약금액이 단순화된 취득 임계값보다 크지 않은 계약자에게는 적용되지 않음
면책 사항	• CIO[15]가 국가 보안 또는 연구 목적을 위해 필요하다고 판단할 경우[16], 취약성 공개 정책 요건 면책 사항에 해당함 (안 제2(d))

○ **(국방부의 연방조달규정 보완조치)** 국방부장관은 위 연방조달규정 취약성 공개 정책을 구현하도록 계약조건 및 계약자 취약성 공개프로그램 언어를 검토하는 한편, 계약자에 대해 NIST지침에 부합하는 취약성 공개 정책을 구현하도록 설계된 요구사항에 대한 업데이트를 개발해야 함(안 제2(e))

■ 전망 및 시사점

○ 본 법안은 연방 계약자들에 대해 취약성 공개 정책(VDP) 이행을 준수하도록 함으로써 계약자들이 소프트웨어 등의 취약점을 신속하게 식별하고 해결할 수 있도록 사이버보안에 대한 사전 조치를 강화하는 것으로 평가됨

- '2020년 IoT 사이버보안법'에 따라 정보시스템을 제공하는 연방 계약업체를 대상으로 VDP를 이행하도록 하였으나, 본 법안은 VDP 이행 대상을 단순화된 취득 임계값 이상의 모든 정부 계약으로 그 적용범위를 확장하는 것임

- 이를 통해 사이버 공간의 안정성 강화 및 높은 회복탄력성을 통한 디지털 시대의 신뢰와 보안 효과 기대

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/5255/text?s=1&r=41
https://federalnewsnetwork.com/cybersecurity/2023/08/house-bill-would-require-federal-contractors-to-adopt-cyber-vulnerability-disclosure-policy/

12) GUIDELINES ON THE DISCLOSURE PROCESS FOR SECURITY VULNERABILITIES RELATING TO INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES
13) IMPLEMENTATION OF COORDINATED DISCLOSURE OF SECURITY VULNERABILITIES RELATING TO AGENCY INFORMATION SYSTEMS, INCLUDING INTERNET OF THINGS DEVICES
14) IoT Cybersecurity Improvement Act of 2020
15) Chief Information Officer
16) IoT Cybersecurity Improvement Act of 2020 제7(b)를 근거로 함

해외 입법 동향

중국, 「안면인식 기술 적용 안전관리 규칙」 초안 발표(2023. 8. 8.)

중국 사이버공간관리국(CAC[1])은 안면인식 기술 사용자에게 특정 목적이 존재하고 충분한 필요성이 있는 경우에만 기술을 사용하도록 하는 내용의 「안면인식 기술 적용 안전관리 규칙」 초안을 발표(2023. 8. 8.)

■ 개요

○ 중국 사이버공간관리국(CAC)은 8월 8일에 개인정보보호 영향평가 등 개인정보와 관련된 조항과 영상 수집 장비 및 개인 식별 장비에 대한 위험성 평가를 실시하도록 하는 등 정보보호와 관련된 조항의 내용을 골자로 하는 규칙 초안을 발표함

- 동 규칙 초안에 대한 대중들의 의견수렴은 9월 7일까지 진행할 예정임

■ 주요내용

① 개인정보보호 관련 조항

○ **(개인 동의)** 안면정보를 처리하기 위하여 법률 및 행정법규에서 개인의 동의를 얻도록 요구하지 않는 경우를 제외하고 개인의 개별적 동의 또는 서면 동의를 받아 안면인식 기술을 사용해야 함(제5조)

○ **(식별 장치 설치·운영 제한)** 공공장소에서 영상 수집 및 개인 식별 장치를 설치하는 경우, 공공 안전에 필요하고 관련된 국가 규정을 준수하여야 하며 쉽게 눈에 띄는 안내판을 설치하여야 함(제7조)

- 또한, 공공장소에서의 영상 수집, 개인 식별 장치를 설치 및 사용을 하는 담당자는 수집한 정보를 대중들에게 불법적으로 공개하거나 제공하지 말아야 하는 비밀 유지 의무가 있으며, 수집된 정보는 공공 안전을 유지하는 목적으로만 사용해야 하고 개인의 동의가 없는 한 다른 목적으로의 사용이 금지됨

○ **(안면인식 기술 사용 제한)** 특정 자연인을 원격 방식으로 식별하기 위한 공공장소 및 사업장에서 안면인식 기술의 사용은 개인이나 이해관계자의 요청에 따라 진행되어야 하며 긴급상황에서 국가의 안보·공공의 안전을 유지하거나 자연인의 생명·건강·재산의 안전을 위하여 필요한 경우로 제한해야 함

1) Cyberspace Administration of China

- 한편, 안면인식 기술 사용자가 개인 또는 이해관계자의 요청에 따라 특정 개인 또는 이해관계자를 원격으로 식별하기 위해 기술을 사용하는 경우, 해당 서비스는 필요 최소한의 시간, 장소 또는 집단으로 한정해야 하고 개별적이거나 관련 없는 요청은 제한되어야 함(제10조)

○ **(민감정보 분석 금지)** 어떠한 조직이나 개인도 안면인식 기술을 사용하여 개인의 인종, 민족, 종교 등의 민감한 개인정보를 분석해서는 아니 됨(제11조)

○ **(개인정보보호 영향평가)** 안면인식 기술 사용자는 안면 정보를 처리할 때 다음과 같은 내용의 영향평가를 실시하고 기록해야 하고 이 기록을 최소 3년 동안 보관해야 하며 처리 목적과 방법 변경 및 중대한 보안사고 발생 시 재평가를 수행해야 함(제15조)

- ▲법령, 행정법규 및 국가표준의 의무 요건과 윤리에 부합하는지 여부 ▲안면정보 처리의 특정 목적 및 필요성 ▲목적 달성에 필요한 정확성, 정밀성 및 거리 요건에 한정되는지 여부 ▲보호조치가 적법하고 효과적이며 위험 정도에 부합하는지 여부 ▲안면 정보 유출, 변조, 불법 사용 등으로 인한 위험과 발생할 수 있는 피해 가능성 ▲개인의 권익에 대한 피해량과 영향 가능성 및 영향을 줄이기 위한 조치가 효과적인지 여부

○ **(익명 처리)** 안면정보 처리를 위해 안면인식 기술을 사용하는 경우, 서비스 제공과 관련 없는 정보 수집을 지양하고 불가피한 경우 적시에 삭제하거나 익명 처리하여야 함(제18조)

② 정보보호 관련 조항

○ **(일반인에 대한 안면인식 기술 서비스 제공)** 안면인식 기술 서비스를 일반인에게 제공하는 경우, 해당 기술 시스템은 네트워크 보안수준 또는 3등급 이상의 보호요건을 준수하여야 하며, 안면정보의 안전을 위하여 데이터 암호화, 보안감사, 접근통제, 권한관리, 침입탐지 및 방어 등의 조치를 채택하여야 하며, 중요정보 인프라에 속하는 경우에는 관련 요건을 충족하도록 하는 한편, 안면인식 기술 사용자는 익명의 안면정보를 제외하고는 원본 이미지, 사진, 동영상 등을 저장할 수 없음(제17조)

○ **(위험성 평가)** 안면인식 기술 사용자는 영상 수집 장비 및 개인 식별 장비의 안전 및 발생 가능한 위험성에 대해 매년 검사 및 평가를 수행해야 하며 이를 기반으로 보안 정책을 개선하고 신뢰도 기준을 조정하는 효과적인 조치를 취해야 함(제19조)

○ **(인증 및 국가표준 준수)** 관련 국가 규정에 따라 네트워크 장비 및 보안 관련 특수 제품 목록에 나열된 정보 수집 장비 및 개인 식별 장비는 자격을 갖춘 기관의 인증을 받거나 관련 국가표준의 요구 사항에 따라 요구사항을 충족하여야 판매하거나 제공할 수 있음(제20조)

○ **(유관부서 협력)** 네트워크 정보부서는 전신기관, 공안기관, 공안기관 등 유관부서와 함께 안면인식 기술 사용에 대한 감독 검사를 강화하고 기술 사용자에 대한 지도 및 감독을 강화함(제21조)

■ 전망 및 시사점

○ 동 규칙 초안은 안면인식 기술이 특정 조건과 충분한 요구가 있는 경우에만 데이터를 처리하는데 사용된다고 명시하는 등 주로 개인정보보호 측면의 내용을 다루고 있지만, 정보 수집 장비 등에 대한 안전 및 위험성 평가 조항도 명시하여 보안 측면의 내용도 다루고 있음

- 디지털화가 빠르게 진행되면서 안면인식이 일반적인 부분이 되었으며 이는 편의성의 향상을 촉진하는 반면, 다양하고 심오한 보안 위험을 야기하여 보안 관련 조항을 통해 위험을 관리하려는 것으로 해석

○ 한 언론사는 중국 사이버공간관리국(CAC)이 최근 중국이 민간에 대한 폐쇄회로(CCTV)의 무분별한 안면인식 기술 남용으로 중국 소수민족의 인권을 침해하고 있다는 서방국의 비난 및 논란을 잠재우기 위해 해당 규칙 초안을 발표한 것이라고 해석함

- 전 세계에서 가장 적극적으로 정부 차원의 안면인식 기술을 활용하는 나라로 평가받는 중국은 9월 7일까지 대중 의견수렴 과정을 거친 후 추후 정확한 시행 일정을 발표할 것으로 예상됨

• Reference

http://www.cac.gov.cn/2023-08/08/c_1693064670537413.htm
http://www.xinhuanet.com/tech/20230809/42fcc0e4449145b78017ed483aae85f0/c.html

해외 단신

미국 하원, 주요시설의 사이버보안 관리를 강화하는 법안 발의

○ 미국 하원은 주요시설의 사이버보안 강화를 위하여 연방의 사이버보안 관리계획을 강화하는 「전략비축유 저장소 보안평가법(안)[2]('23.7.25 발의)」 및 「연방재난관리청 사이버보안 향상법(안)[3]('23.8.11 발의)」을 발의함

○ **(전략비축유 저장소 보안평가법(안))** 미국 에너지부 장관[4]은 전략비축유 저장소(SPR)[5] 의 관련 시설, 저장 시설에 대한 물리적 또는 사이버 보안의 연간 사고평가 사항이 담긴 보고서를 의회에 제출하도록 함

- 해당 연간 사고평가 보고서에는 물리적· 사이버 보안의 ▲사고 발생일, ▲사고 해결, ▲사고 완화를 위해 지원한 지방, 주, 연방기관, ▲기타 장관이 필요하다고 판단하는 정보가 포함되어야 함(본 법안은 「에너지 정책 및 보존법[6]」 제161조 개정안임)

○ **(연방재난관리청 사이버보안 향상법(안))** 연방재난관리청장은 CISA청장과 협의하여 연방재난관리청의 사이버보안 위험 완화를 위한 연방재난관리청의 조치 사항이 담긴 보고서를 미국 의회[7]에 제출해야 함 (본 법안은 「국토안보법 2002[8]」 제523(a)조 개정안임)

• Reference

https://www.congress.gov/bill/118th-congress/house-bill/4859/text?s=4&r=364
https://www.congress.gov/bill/118th-congress/house-bill/5201/text?s=2&r=95

2) Strategic Petroleum Reserve Security Assessment Act '23,7,25 (H.R.4859)
3) FEMA Cybersecurity Improvement Act, '23.8.11 (H.R.5201)
4) United States Secretary of Energy
5) Strategic Petroleum Reserve
6) Energy Policy and Conservation Act
7) 미국 하원의 국토안보위원회 및 교통·기반시설 위원회(Committee on Homeland Security and the Committee on Transportation and Infrastructure of the House of Representatives) 및 상원의 국토안보위원회 및 정무위원회(Committee on Homeland Security & Governmental Affairs of the Senate)
8) Homeland Security Act of 2002

인터넷·정보보호 법제동향
Vol. 191 (August 2023)

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