AI보안 법·제도·정책
현황 및 전망

2021.12

연구기관 : ㈜이언컨설팅그룹

한국인터넷 진흥원 KISA

제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 「AI보안 법·제도·정책 현황 및 전망」의 연구결과 보고서로 제출합니다.

2021년 12월

연 구 기 관 : ㈜ 이언컨설팅그룹

총괄책임자 : 정진훈 (㈜ 이언컨설팅그룹 상무)

참여연구원 : 김성민 (㈜ 이언컨설팅그룹 부장)

전우선 (㈜ 이언컨설팅그룹 책임연구원)

요 약 문

1. 서문

가. 연구배경 - 인공지능 시대와 보안, 정보의 활용과 보호.

인공지능 시대를 맞아 정보가 자원이 되었다. 정보의 보호화 활용을 동시에 추진하기 위하여 각국은 자국의 법·제도·정책을 정비하고 있으며 새로운 인공지능에 관한 윤리도 정립중이다.

나. 연구범위 - AI보안과 관련된 윤리·법·제도·정책 현황

인공지능 산업은 이제 막 시작되었고 이를 규율하거나 육성하는 윤리·법·제도·정책도 같은 상황이다. 따라서 아직까지는 AI보안에 특화된 내용은 찾기가 어렵다. 향후 산업이 성숙되며 윤리가 법으로 확정되고, 영역별 분화가 진행되며, 세계표준화가 이루어질 것으로 예상된다.

이번 연구에서는 보안 영역과 인공지능 영역에 나타난 규범을 살피며 새롭게 나온 인공지능 윤리에 관한 내용도 고찰한다.

2. 인공지능 윤리 - 방향제시, 자율규제

가. 인공지능 분야에서 윤리의 필요성 및 역할

윤리는 산업이 발전하는 초기 단계에서 이를 규율하는 기본적인 원칙을 세워주고 앞으로 나아갈 방향을 제시하는 기능을 수행한다. 그리고 산업이 성숙함에 따라 많은 사항들이 차츰 법으로 확정되는 모습을 보인다. 현재 인공지능 산업 역시 발전초기라는 점에서 이에 관한 윤리의 정립은 우선되어야 하며 매우 필요하다.

인공지능에 대한 사회구성원들의 합의를 도출하기 위한 가장 기본적인 원칙을 제공하고 있다. 그리고 윤리원칙, 가이드라인, 권고사항의 형태로 지침을 제시하고 있다. 즉, 법적 규제가 본격적으로 행해지기 이전 단계에서 자율 규범, 맞춤형 규범의 역할도 하고 있다. EU, 미국, 중국과 우리나라의 인공지능 윤리를 살펴보았다.

나. EU의 인공지능 윤리

EU는 전통적으로 개인정보 보호를 매우 중시해 왔으며 이에 따라 인공지능의 역기능 방지에 많은 관심을 기울여왔다. '신뢰할 만한 AI 윤리 가이드라인 (`19.4)' 으로 인공지능 윤리의 기준을 제시하는 것에서 나아가 '인공지능 규제안 (`21.4)'을 발표하여 최초로 인공지능을 규제하는 모습까지 보이고 있다.

다. 미국의 인공지능 윤리

미국은 혁신을 가로막는 규제에 소극적이었으나 소비자 보호를 위해 다국적 플랫폼 기업의 독과점을 규제하는 모습을 보여주고 있다. '기업들의 AI 및 알고리즘 사용 시 관리 지침 (`20.4.8)' 으로 인공지능 기업의 소비자 보호 지침을 제시하였으며 '기업의 AI 사용에 대한 진실성과 공정성, 공평함을 위한 지침 (`21.4)' 으로 인공지능 기업이 편향성과 불공정을 피하기 위해 지켜야 할 지침을 제공하였다.

라. 중국의 인공지능 윤리

중국은 인공지능 산업을 국가전략 차원으로 중시하고 있으며 정부주도로 급속한 발전을 추진하고 있다. 인공지능 시스템 개발의 가이드라인을 제시한 '차세대 인공지능 관리원칙 (`19.6)' 을 제시한 바 있으며 '차세대 인공지능 윤리규범 (`21.9)'에서는 인공지능과 관련된 다양한 활동을 제시하고 윤리지침을 제공하였다.

마. 우리나라의 인공지능 윤리

주요국에 비해 다소 늦은 출발을 했으나 다수의 기관에서 여러 가지 인공지능 윤리 기준을 발표하며 빠르게 움직이고 있다. 그 중 '인공지능 윤리기준 (`20.12)'과 '신뢰할 수 있는 인공지능 실현 전략 (`21.5)'을 살펴 본다.

3. 법·제도 - 정보보호 강조, 정보활용 허용

가. 현황

인공지능이 보안영역에 들어오면서 법·제도 면에서는 개인정보 보호법제가 크게 변화하였다. 기존의 보호 위주에 활용이 더해졌으며 더불어 보호는 더욱 강화되었다. 이런 상황에서 EU는

최초로 일반개인정보보호법인 GDPR을 제정하였다. 세계 각국은 이를 참고하여 자국의 법제를 정비하고 있어 GDPR은 점차 세계 표준이 되고 있다. GDPR을 먼저 살펴본 후 이를 바탕으로 미국, 중국과 우리나라의 일반 개인정보보호법을 살펴보았다.

나. GDPR (EU일반개인정보보호법) (`18.5)

EU가 세계 최초로 제정된 일반개인정보보호법이다. 여러 이유로 세계 표준화되고 있는 법이므로 자세하게 살펴볼 필요가 있다. GDPR의 주요내용으로는 개인정보의 정의, 역외적용, 가명처리의 허용, 개인정보 주체의 권리 명시, 개인정보 처리자의 의무 강화, 개인정보 역외이전 제한, 위반에 대한 강력한 제재 등이 있다.

다. 미국의 법·제도

개인정보보호가 개별법으로 진행되어 왔으나 최초로 캘리포니아주에서 CCPA가 제정되었다. 이후 주별로 법률이 만들어지고 있으며 연방법이 제정준비중이다. CCPA의 주요내용으로는 소비자의 권리 확대, 기업의 의무강화, 개인정보 감독기구 설립, 적용대상 일부 축소, GDPR원칙의 제한적 도입 등이 있다.

라. 중국의 법·제도

GDPR의 제정에 영향을 받아 빠른 속도로 일반개인정보법을 제정하였다. 개인정보의 국외이전에 매우 엄격한 모습을 보이는 등 폐쇄적인 특징이 있다. 중국 개인정보보호법의 주요내용으로는 역외적용, 개인의 권리, 처리자의 의무, 개인정보의 국외이전 요건, 위반에 대한 엄격한 처벌 등이 있다.

마. 우리나라의 법·제도

우리나라도 이러한 세계적인 흐름에 대응하기 위해 데이터3법의 전면 개정을 실시하였다. 곧이어 미진한 부분의 추가 개정을 위해 개인정보보호법의 2차 개정이 추진되고 있다.

데이터3법의 주요내용으로는 개인정보 법제 및 감독기구 일원화, 개인정보 활용 기반 조성, 개인정보 보호 강화, 해외 법제와의 상호운용성 고려 등이 있으며, 개인정보보호법 2차 개정안의 주요내용으로는 개인정보전송요구권 도입, 자동화된 의사결정에의 대응권 도입, 이동형 영상정보처리기기 운영 기준 마련, 개인정보 국외이전 방식 다양화 및 중지 명령권 신설, 형벌 중심의 제제를 경제벌 중심으로 전환 등이 있다.

4. 정책 - 인공지능 산업 육성, 사이버보안 강화

가. 현황

대부분의 국가에서 사용가능한 정책 수단을 총동원하여 인공지능 산업을 육성하고 있으며 아울러 사이버보안을 강화하고 있다. 각국의 정책 수단들은 정책자금지원, R&D지원, 민관협력, 고급인력양성, 산업기반조성 등에서 서로 상당히 유사한 모습을 보이고 있으나, 각 국가별로 자신의 특수한 상황에 맞추어 특색있는 모습도 있다. 미국, 중국과 우리나라의 인공지능 정책과 사이버안보 정책을 살펴보았다.

나. 미국의 정책

인공지능 산업 세계1위이자 사이버보안 최강국이다. 미래 산업에서의 주도권을 지킴과 동시에 날로 증가하는 경쟁국의 위협으로 사이버보안을 지키기 위한 노력을 지속중에 있다. 주요 인공지능 정책으로는 미국 AI 이니셔티브 행정명령 (`19.2), 국가 AI R&D 전략계획 업데이트 (`19.6) 등이 있으며, 주요 사이버보안 정책으로는 미국국가사이버보안전략 (`18.9), 클린 네트워크 프로그램 (`20.8) 등이 있다.

다. 중국의 정책

정부주도로 인공지능 산업을 급속히 성장시키고 있다. 인구에 비례하여 엄청난 데이터를 소유하고 있으며 자국의 데이터가 타국으로 유출되지 못하도록 강한 통제를 하고 있다. 주요 인공지능 정책으로는 차세대 AI 발전규획 (`17.7), 국가 차세대 AI 표준 체계 구축 지침 (`20.8) 등이 있으며, 주요 사이버보안 정책으로는 국가 사이버공간 보안전략 (`16), 사이버보안법 (`17.6) 등이 있다.

라. EU의 정책

인공지능 산업분야에서 미국, 중국에 비해 상대적으로 열세인 상황을 각종 법과 제도의 세계표준화로 만회하려 하고 있다. 주요 인공지능 정책으로는 유럽 AI 전략 (`18.4), Horizon2020 (`14~`20) 등이 있으며, 주요 사이버보안 정책으로는 EU 사이버보안법 (`19.3)이 있다.

마. 우리나라의 정책

주요국에 비해 늦은 출발을 다양한 정책의 적극적인 시행으로 만회하고 있다. 특히 '제2차 정

보보호산업 진흥계획'으로 AI보안 발전을 위한 다양한 정책을 시행중이다. 주요 인공지능 정책으로는 디지털뉴딜(`20.7), 인공지능 법제도규제 정비로드맵(`20.12) 등이 있으며, 주요 사이버보안 정책으로는 국가 사이버안보 기본계획 (`19.9), 제2차 정보보호산업 진흥계획 (`20.6) 등이 있다.

5. 결론 및 제언

보안의 영역에 인공지능이 들어오면서 정보의 보호와 활용이 동시에 중요해졌다. 세계 각국은 급속히 인공지능 산업을 성장시키는 정책을 수행하는 동시에 그 역기능을 해소하기 위해 윤리를 새롭게 만들고 법·제도를 정비하고 있다.

인공지능 산업에서 미국이 현재 선두에 있는 가운데, 중국이 추격하고 있으며, EU는 부족한 기술력을 법·제도의 표준화로 보완하고 있다. 우리나라는 법·제도를 정비하여 발전의 기반을 구축하고 다양한 정책을 펼쳐 인공지능 산업을 빠르게 육성하고 있다.

인공지능 산업은 아직 발전초기라 아직까지 AI보안이 특화되지 못하였다. 가까운 시일내에 산업 성숙에 따라 자연스럽게 별도의 독립된 분야가 될 것이며 법·제도 등도 그에 맞게 등장할 것이 예상된다.

다른 주요국에서 배울 장점들을 수용하여 인공지능 산업에서 선두권으로 도약하는 시기를 앞당겨야 할 것이다. 인공지능 총괄기관 신설, 예산 대폭 증액, 해외인재 유치를 위한 별도계획 등이 그 사례가 될 것이다. 아울러 이번 연구에 참여한 자문위원들의 제언도 우리나라의 발전에 큰 도움이 될 것이다. AI기술을 활용하는 스타기업을 발굴하고, 정책자금 집행자의 전문성 제고로 자금효율을 향상시키며, 데이터 제공자에 대한 인센티브 등 혜택 제도 정착으로 데이터 산업을 발전시키는 것이 그 주된 내용이었다.

목 차

1. 서문

가. 연구배경 - AI보안, 정보의 활용과 보호

AI는 인간의 모든 영역에 빠른 속도로 전파되면서 혁신을 일으키고 있다. 이러한 인공지능은 빅데이터를 머신러닝, 딥러닝하여 성장하는데 이러한 빅데이터는 대부분 개인정보로 구성된다는데 보안분야에서 변화의 핵심이 있다. 즉, 개인정보가 더 이상 보호의 대상만이 아닌 활용의 대상이 된 것이다. 이러한 시대의 변화에 대응하기 위해 세계 각국은 경쟁적으로 법·제도·정책 정비를 서두르고 있다. 그리고 이와 더불어 새로운 윤리의 정립에도 힘을 쏟고 있다.

나. 연구범위 - AI보안과 관련된 윤리·법·제도·정책 현황 및 전망

인공지능 산업은 이제 시작 단계에 있다. 산업 시작 단계에서 흔히 볼 수 있는 법·제도·정책의 특징으로 미성숙, 미분화를 들 수 있다. 즉 산업전반이 미성숙 상태이다 보니 이를 규율할 법도 막 등장하는 상황이며 법의 이전 단계 규범인 윤리가 중요한 역할을 하는 경우가 많다. 또한 인공지능의 영향으로 변화한 내용들이 아직까지는 영역별로 분화되어 고찰되지 못하고 있어 AI보안만을 위한 윤리·법·제도·정책은 찾기 힘들다.

산업이 성숙될수록 규제의 중심이 윤리에서 법으로 이동할 것이며 정보 활용 위주에 보호를 수반하는 방향으로 세계표준화가 가속될 것으로 예상된다. 특히 자국의 정보를 보호하고 타국으로의 이전을 제한하는 성향이 점차 강해질 것이 예상된다. 현재는 인공지능 산업 전반을 육성 및 규제하는 상황이나 향후 분야별 세분화 및 구체화가 점차 진행될 것이다.

이 연구에서는 기존의 보안 영역을 규율하는 규범들과 새롭게 인공지능을 규율하기 위해 나타난 규범들 중 주요한 것들을 찾아보고 그 중 AI보안과 관련 있는 내용을 살펴보았다. 그리고 이에 부수하여 인공지능 윤리에 관한 내용도 간략히 고찰하였다. 다만 윤리가 법·제도·정책 보다 선행하는 규범이며 기본 원칙인 점을 고려하여 윤리를 먼저 고찰하였다. 법·제도는 정보보호에 중심이 있고 정책은 인공지능 육성에 주된 목적이 있는 관계로 이들을 각각 나누어 고찰하였다.

2. 인공지능 윤리 - 방향제시, 자율규제

가. 인공지능 분야에서 윤리의 필요성 및 역할

새로운 산업이 등장하는 상황에서는 윤리가 매우 중요해진다. 발전초기라서 규제요소가 미확정 또는 불분명하므로 법률로 규제 곤란한데다 고도의 기술영역에서는 비전문가인 법률가의 이해부족으로 적절한 규제가 어렵기까지 하다. 이러한 상황에서 윤리는 사회구성원의 합의를 도출하고 가장 기본적인 원칙을 제시하며 법의 미비나 공백을 메우고 향후 법이 나아가야 할 방향을 앞서서 제시한다. 그리고 원칙 중심의 자율적인 규제를 가능케 하여 수범자의 능동적이고 정확한 준수를 가능하게 한다. 이는 강한 법률 규제시 수범자는 최소한의 책임회피만을 위한 수동적인 대응을 할 우려가 생기는 모습과 상반된다.

인공지능 산업 역시 새롭게 등장한 산업이라는 점에서 같은 상황에 놓여 있다. 세계 각국에서는 기존의 법률의 개정하거나 새로운 법률을 만들기도 하지만 동시에 다양한 인공지능 윤리 규범을 제시하고 있다. 윤리원칙, 가이드라인, 권고사항의 형태를 가지고 있는 윤리규범들이 그것이다. EU, 미국, 중국과 우리나라의 인공지능 윤리를 살펴보았다.

나. EU의 인공지능 윤리

인공지능 산업의 발전에서 미국과 중국에 다소 뒤쳐져 있는 EU에서는 윤리·법·제도·정책 등의 선제적 정비를 통해 세계표준화 함으로써 격차를 좁히려 하고 있다. 특히 전통적으로 개인정보보호를 인간의 중요한 기본권으로 인식하여 왔기에 인공지능 시대에도 개인정보를 보호하기 위한 노력을 아끼지 않고 있으며 이는 윤리에서도 보여지고 있다. '신뢰할 만한 AI 윤리 가이드라인 (`19.4)' 으로 인공지능 윤리의 기준을 제시하는 것에서 나아가 '인공지능 규제안 (`21.4)'을 발표하여 최초로 인공지능을 규제하는 모습까지 보이고 있다.

(1) 신뢰할 만한 AI 윤리 가이드라인 (`19.4)

■ 3대 요소

- 적법성, 윤리성, 견고성

■ 7대 요구사항

- 인간 행위자와 감독, 기술적 견고성과 안전성, 프라이버시와 데이터 거버넌스, 투명성,

다양성·차별금지·공정성, 사회·환경적 복지, 책임성

(2) 신뢰할 만한 AI 윤리 평가 목록 (`20.7)

■ 목적

- AI 개발 시 설계에서 출시에 이르는 전 과정에서 윤리 이슈를 자체 점검가능한 평가목록

■ 항목구성

- 인간 기본권과 AI 윤리 7대 요구사항 관련 140여 가지 질문포함

(3) 인공지능 규제안 (`21.4)

■ AI 정의

- 기계학습, 논리·지식기반 접근법 또는 통계적 접근법을 활용해 인간이 상호작용하는 환경에 영향을 주는 콘텐츠, 예측, 추천, 의사결정을 생성하는 소프트웨어

■ 위험수준을 기준으로 AI 시스템 구분 및 규제

- 용납될 수 없는 위험 : 금지
- 고위험 : 관리 및 준수 의무 부과
- 제한된 위험 : 투명성 의무 부과
- 최소한의 위험 : 규제 없음

다. 미국의 인공지능 윤리

인공지능 산업을 민관협력을 통해 발전시키고 있는 미국에서는 혁신을 가로막는 규제를 제정하는데 다소 소극적인 모습을 보여왔다. 그러나 거대 테크 기업의 등장으로 독과점, 불평등, 이익독식 등 문제점이 발생하자 소비자 보호를 목적으로 각종 규제를 시작하였다. 미국의 인공지능 윤리는 주로 기업들에게 행동지침을 제시하는 내용을 보이고 있다. '기업들의 AI 및 알고리즘 사용 시 관리 지침 (`20.4.8)' 으로 인공지능 기업의 소비자 보호 지침을 제시하였으며 '기업의 AI 사용에 대한 진실성과 공정성, 공평함을 위한 지침 (`21.4)' 으로 인공지능 기업이 편향성과 불공정을 피하기 위해 지켜야 할 지침을 제공하였다.

(1) 기업들의 AI 및 알고리즘 사용 시 관리 지침 (`20.4)

■ 목적

- AI기업의 소비자 보호 지침 제시

■ 내용

- 투명성, 의사결정 이유설명, 의사결정 공정성 보장, 데이터와 모델의 견고성·타당성 보장,

규정준수·윤리·공정성·비차별에 대한 책임

(2) 기업의 AI 사용에 대한 진실성과 공정성, 공평함을 위한 지침 (`21.4)

■ 목적

- AI기업이 편향성과 불공정을 회피하여 AI를 활용할 수 있는 지침을 제시

■ 내용

- 올바른 기초에서 시작, 차별적 결과에 주의, 투명성과 독립성 확보, 알고리즘의 성능·공정성·편향성 과장 금지, 데이터 사용방법 허위고지 금지, 사회적 득실 고려, 알고리즘의 성능에 책임

라. 중국의 인공지능 윤리

중국은 미국을 추월하여 인공지능 세계 1위를 차지하겠다는 야심찬 목표하에 중앙정부와 지방정부 주도로 빠른 속도로 인공지능 산업을 발전시키고 제도를 정비하여 왔다. 인공지능 윤리에 대한 논의는 육성정책이나 제도정비에 비해 상대적으로 적은 편이었으나 최근 급속한 발전에 따른 부작용이 곳곳에서 드러남에 따라 이를 관리하기 위한 윤리지침을 새롭게 제정하고 있다. 인공지능 시스템 개발의 가이드라인을 제시한 '차세대 인공지능 관리원칙 (`19.6)'을 제시한 바 있으며 최근에는 '차세대 인공지능 윤리규범 (`21.9)'에서는 인공지능과 관련된 다양한 활동을 제시하고 윤리지침을 제공하였다.

(1) 차세대 인공지능 관리원칙 (`19.6)

■ 목적

- 인공지능 시스템 개발의 가이드라인을 제시

■ 원칙

- 화합과 우호, 공평과 공정, 포용과 공유, 프라이버시 존중, 제어 가능한 보안, 공동의 책임, 개방과 협력, 민첩한 관리

(2) 차세대 인공지능 윤리규범 (`21.9)

■ 목적

- 인공지능과 관련된 활동을 하는 자에게 윤리지침을 제공
- 관리활동, R&D활동, 공급활동, 사용활동 등

■ 요구사항

- 인류 복지 증진, 공평성·공정성 강화, 개인정보보호 및 데이터 보안, 통제가능성·신뢰가능성 확보, 책임담당 강화, 윤리적 소양 강화

마. 우리나라의 인공지능 윤리

비록 인공지능에 대한 관심 및 집중은 다른 주요국에 비해 늦게 시작되었으나 정부와 대기업 위주로 각종 정책과 투자가 집중되며 빠른 발전을 보이고 있다. 인공지능 윤리 역시 인공지능 산업 관련 정부부처와 대기업에서 다수 발표하고 있는데 그 중 '인공지능 윤리기준 (`20.12)'과 '신뢰할 수 있는 인공지능 실현 전략 (`21.5)'을 살펴 본다.

(1) 인공지능 윤리기준 (`20.12) : 과학기술정보통신부, 정보통신정책연구원,

■ 3대 기본원칙

- 인간 존엄성 원칙, 사회의 공공선 원칙, 기술의 합목적성 원칙

■ 10대 핵심요건

- 인권보장, 프라이버시 보호, 다양성 존중, 침해금지, 공공성, 연대성, 데이터 관리, 책임성, 안전성, 투명성

(2) 신뢰할 수 있는 인공지능 실현 전략 (`21.5) : 과학기술정보통신부

■ 비전

- 누구나 신뢰할 수 있는 인공지능, 모두가 누릴 수 있는 인공지능 구현

■ 목표

- 책임있는 인공지능 활용, 신뢰있는 사회, 안전한 사이버국가

■ 추진전략

- 신뢰가능한 인공지능 구현 환경 조성
- 안전한 인공지능 활용을 위한 기반 마련
- 사회 전반 건전한 인공지능 의식 확산

■ 실행과제

- 인공지능 제품·서비스 신뢰 확보 체계 마련, 민간 신뢰성 확보 지원, 인공지능 신뢰성 원천기술 개발, 학습용 데이터 신뢰성 제고, 고위험 인공지능 신뢰 확보, 인공지능 영향평가 추진, 신뢰 강화 제도 개선, 인공지능 윤리 교육 강화, 주제별 체크리스트 마련, 인공지능 윤리정책 플랫폼 운영

(3) 인공지능 개인정보보호 자율점검표 (`21.5) : 개인정보위원회

■ 6대 원칙

- 적법성, 안전성, 투명성, 참여성, 책임성, 공정성

■ 단계별 개인정보보호 자율점검표

- 단계별(또는 상시)로 법령상 준수해야 할 의무 또는 권장하는 내용
- 16개 점검항목 , 54개 확인사항으로 구성

3. 법제도 - 정보보호 강조, 정보활용 허용

가. 현황

인공지능이 보안에 들어오면서 법·제도 측면에서는 개인정보 보호법제의 변화가 가장 눈에 띄고 있다. 보안에서 개인정보는 주로 보호의 대상이었으나 인공지능이 들어오면서 새롭게 활용의 대상이 되었다. 따라서 보호에만 중점이 맞춰져 있던 기존의 개인보호 법제에 활용을 보장하는 내용이 추가되었다. 그러나 여전히 정보보호의 가치에는 변함이 없으며 오히려 인공지능의 역기능 방지를 위해 더욱 강조되고 있다.

EU는 오랜 시간 논의와 검증을 거쳐 최초로 개인정보에 관한 일반법인 GDPR을 제정하였다. 이 법은 정보활용과 보호를 동시에 추구하며 유럽을 넘어 유럽과 거래하고자 하는 모든 국가에 적용된다는 특징을 지녔다. 최초의 법이라는 점과 준수해야만 유럽과 거래가 가능하다는 점 때문에, 우리나라를 비롯해 주요국이 자국의 개인보호 법제에 벤치마킹하게 되었으며 자연히 세계표준이 되어가고 있다. GDPR을 먼저 살펴본 후 이를 바탕으로 미국, 중국과 우리나라의 일반 개인정보보호법을 살펴보았다.

나. GDPR (EU일반개인정보보호법) (`18.5)

(1) 의의

GDPR (`18.5)은 EU의 일반개인정보보호법이다. 개인정보보호의 법적 요소를 최대한 포함하고 있으며 최근의 경향까지 반영하고 있다. 유럽이 법·제도를 통해 세계 시장의 선도국으로 도약하기 위한 목적도 가지고 있다. 개인정보의 보호와 활용의 균형을 추구하고 있으며 모든 EU 회원국 및 외국의 EU거래자에게도 적용된다는 특징을 보인다. 제정이후 다른 국가들에 벤치마킹 되고 있으며 점차로 세계표준이 되어가고 있어 각국의 법제를 살피는데 있어 매우 중요한 비중을 차지하고 있다.

GDPR의 주요내용으로는 개인정보의 정의, 역외적용, 가명처리의 허용, 개인정보 주체의 권리 명시, 개인정보 처리자의 의무 강화, 개인정보 역외이전 제한, 위반에 대한 강력한 제재 등이 있다.

(2) 주요내용

■ 목적

- 정보주체의 개인정보보호에 대한 권리를 보호
- EU 내에서 개인정보의 자유로운 이동을 보장

■ 적용범위

- EU 거주자와 거래하는 자에게 적용
  EU 밖에서 EU 내에 있는 정보주체에게 재화나 용역을 제공하는 경우,
  또는 EU 내에 있는 정보주체가 수행하는 활동을 모니터링 하는 경우
- GDPR 적용되는 사례
  EU 내에 거주하는 외국인,
  EU 내에 사업장이 없이 EU 거주자와 거래하는 기업체

■ 개인정보의 정의, 구분, 적용범위

- 개인정보란, 식별되었거나 또는 식별가능한 자연인(정보주체)와 관련된 모든 정보
  예시) IP주소, 쿠키ID, RFID태그, 위치정보 등도 개인정보
- 민감정보란, 민감한 성격의 개인정보로 유전정보, 생체인식정보를 포함
- 가명정보란, 개인정보를 추가정보 없이는 정보주체를 식별할 수 없도록 처리한 정보
- 개인정보를 가명처리, 분리보관 및 특별조치하여 활용하는 것을 허용

■ 개인정보 주체의 권리

- **접근권, 정정권, 삭제권, 처리 제한권, 개인정보 이동권, 반대권,**
  프로파일링을 포함한 자동화된 의사결정의 대상이 되지 않을 권리
- 삭제권 : 잊힐 권리. 단, 예외적으로 삭제거부 가능
- 처리제한권 : 보존 필요시에 이용은 제한하고 삭제는 보류할 것을 요구할 권리
- 개인정보 이동권 :
  자기정보를 받을 권리, 다른 컨트롤러에게 자기정보를 이전할 것을 요구할 권리
- 반대권 : 처리에 반대할 권리. 컨트롤러는 처리를 중지해야 함.
- 프로파일링 :

의미) 개인의 사적인 측면의 평가, 분석, 예측을 위한 모든 형태의 자동화된 정보처리

대상) 업무사항, 경제사항, 건강, 개인취향, 신뢰성, 태도, 위치, 이동경로, 관심사 등

■ **개인정보 처리자의 의무**

- 개인정보 처리활동의 기록

컨트롤러· DPO의 이름 및 연락처, 처리목적, 정보주체·개인정보의 범주에 대한 설명, (가능한 경우) 개인정보 유형별 보유기간, (가능한 경우) 기술적 관리적 보호조치 설명

- 개인정보 영향평가 수행

개인정보 처리 이전에 처리의 필요성, 권리침해 위험성, 보호대책 등을 사전에 평가

- DPO 선임의무 data protection officer

공공민간 모두 선임의무 있음, 관련 전문지식 보유자, 조직내외 모두에서 선임가능

- Data protection by design and by default :

설계 단계에서부터 기술적으로 프라이버시를 보호하는 구조를 만드는 것.

■ **개인정보 역외이전 가능한 경우**

- 적정성을 인정받은 국가
- 적절한 보호조치의 제공 & 정보주체의 권리 행사 보장 & 효과적인 법적 구제 수단의 존재
- 예외요건에 해당 (명시적 동의, 계약의 이행 또는 정보주체의 요청, 공익의 중요한 이유 등)

■ **제재**

- 각각의 개인정보 처리에 따라 제재 규정을 적용
- 사업체 집단 매출을 바탕으로 과징금을 부과
- 일반적 위반 : 전세계매출액2% or 1천만유로, 더 큰 금액을 상한으로 부과
  심각한 위반 : 전세계매출액4% or 2천만유로, 더 큰 금액을 상한으로 부과

다. 미국의 법·제도

(1) 현황

미국은 연방법, 개별법으로 양분되는 법체계를 가지고 있다. 두 체계 모두 개별법에서 관련 내용을 규정하는 형태로 개인정보를 보호하고 있었으며 포괄하여 단일하게 보호하는 일반법은 없었다. GDPR의 제정에 영향을 받아 미국 최초로 캘리포니아주에서 일반개인정보보호법으로 CCPA (`20.7)가 제정되었고 이후 다수의 주에서 같은 법이 제정되었다. 연방법은 제정 준비 중에 있다.

CCPA의 주요내용으로는 소비자의 권리 확대, 기업의 의무강화, 개인정보 감독기구 설립, 적

용대상 일부 축소, GDPR원칙의 제한적 도입 등이 있다.

(2) 캘리포니아주 개인정보보호법

(가) CCPA 캘리포니아 소비자 개인정보 보호법 (`20.7)

- 소비자에게 개인정보에 대한 폭넓은 통제권을 부여
- 사업자에게 다양한 개인정보의무를 부여
- 해당 법률을 관장하는 별도의 감독기구는 없음

(나) CPRA 캘리포니아 개인정보 보호 권리법 (CCPA 개정법) (`23.1. 시행예정)

■ 소비자의 권리 확대

- 부정확한 정보에 대한 정정 청구권
- 자동화된 의사결정 거부권 등

■ 기업의 의무 강화

- 개인정보보호 의무를 명시한 계약 작성 의무화 등

■ 개인정보 감독기구 설립 : California Privacy Protection Agency

- 감독기구 설립 근거조항 마련
- 감독기구가 법률 위반자에게 행정벌을 부과할 근거 마련

■ 적용대상 축소

- 영세 사업자를 적용대상에서 제외하여 부담 경감

■ GDPR 원칙 일부 도입

- 개인정보 최소처리 원칙, 목적 제한 원칙, 보유기간 제한 원칙 등

(3) 향후 전망

연방법으로 일반개인정보 보호법을 조만간 제정할 것으로 예상된다. 기업 등 법규를 준수해야 하는 입장에서는 수십 개의 주법 보다는 하나의 단일한 연방법 준수가 유리한데다 연방법으로

일반개인정보 보호법을 제정하면 EU가 자국과의 거래에 필수적으로 요구하는 적정성 획득에 유리하기 때문이다. 현재 연방의회는 연방 개인정보 보호법 입법 노력에 착수하였다.

라. 중국의 법·제도

(1) 현황

중국은 단일법 제정이전에는 다양한 법에서 개인정보를 부분적으로 보호하고 있었으며 일반개인정보보호법 (`21.11)을 제정하여 법체계를 일원화하였다. 이 법에는 GDPR의 영향을 받은 내용도 일부 있으며 중국 특유의 폐쇄성을 보이는 부분도 있다. 중국외 적용, 강력한 벌칙 규정 등이 전자의 대표적 예라면 엄격한 개인정보 국외이전 요건이 후자의 예라 할 수 있다.

중국 개인정보보호법의 주요내용으로는 역외적용, 개인의 권리, 처리자의 의무, 개인정보의 국외이전 요건, 위반에 대한 엄격한 처벌 등이 있다.

(2) 개인정보보호법 (`21.11)

■ 적용범위

- 중국 내에서 개인정보를 처리하는 자에게 적용됨은 물론
- 중국 외에서 중국인의 개인정보를 처리하는 자에게도 적용
  (중국 외에서 중국 내 자연인에게 재화 또는 서비스 제공, 중국 내 개인의 활동을 분석·평가, 기타 법률에 규정된 사항에 적용)

■ 개인정보 처리의 법적 근거

- 정보주체의 동의
- 정보주체가 당사자인 계약의 체결 또는 수행
- 법적 의무의 이행
- 공중위생 사건 대응 등 긴급한 비상사태에서 개인의 생명, 건강, 재산 보호
- 공익을 위한 뉴스보도, 여론조사 등을 목적으로 합리적인 범위 내에서 개인정보를 처리

■ 개인의 권리

- 알권리, 결정·제한·거절 권리, 열람·복제·정정·보완·파기·해석·설명 요구 권리

■ **처리자의 의무**

- 내부 관리제도의 수립 및 보안기술조치 실시
- 개인정보보호 책임자 지정
- 사전 위험평가 실시

■ **개인정보의 국외이전 요건**

● **개인정보 국외 이전 시 조건 충족, 정보주체 동의 획득**

- 국가 네트워크 정보 부처 기관의 안전성 평가 통과
- 국가 네트워크 정보 부처 규정에 근거하여 전문 기관의 개인정보 보호 인증 진행
- 국외에서 이전받는 자와 계약을 체결하여 개인정보 처리 행위가 법규에 맞는지 감독
- 법률, 행정법규 또는 국가 네트워크 정보 부처에서 규정한 기타 조건

● **개인정보 중국 내 보관 의무 및 국외 이전요건 준수**

- 주요정보기반시설 운영자, 처리 규모가 특정 기준에 해당하는 개인정보 처리자
- 개인정보 중국 내 보관 및 국외 이전 시 안전성 평가 통과

● **국제 사법 공조 또는 행정 상 협조를 위하여 개인정보 국외 이전 시 주관 부처의 승인**

● **특정 경우에 개인정보 제공 제한·금지 가능**

- 국외 기관·개인이 중국 국민의 개인정보 권익 침해, 중국의 국가 안보, 공공이익 위협 시, 개인정보제공 제한·금지 목록에 포함하고 개인정보 제공 제한·금지 조치
- 중국 정부에서 해외 서비스를 차단하는 근거 조항으로 활용 가능

● **상호주의**

- 임의 국가·지역이 중국에 차별적 금지, 제한 시 해당 국가·지역에 상응하는 조치 가능

■ **처벌**

- 최대 5천만 위안 (약 85억원) 또는 전년도 매출액의 5%에 해당하는 벌금을 부과
- 직접 책임자 등에게 1만에서 10만 위안의 벌금 부과

(3) 향후 전망

국가 안보를 우선시하여 외국 기업 활동 위축 시키는 상황이 발생될 것으로 예상된다. 개인정보 국외 이전 시 안전성 평가를 통과해야하는 까다로운 조건을 부여, 개인정보 중국 내 보관, 국외 이전 제한 강화, 개인정보 제공 제한·금지 목록 운영, 개인정보처리자의 배상 책임 등은 외국 기업의 중국 내 활동을 제한하는 수단이 될 수 있다.

마. 한국의 법·제도

(1) 현황 - 데이터 3법 개정이전 상황

우리나라도 이러한 세계적인 흐름에 대응하기 위해 개인정보보호법제에 대한 전면 개정을 실시하였다. 데이터3법 (`20.8)은 기존의 개인정보 보호법, 정보통신망법, 신용정보법을 말하는데 이들을 개정하여 데이터 활용의 길을 열고 개인정보 보호도 강화한 것이다. 한편 미진한 부분의 추가 개정을 위해 개인정보보호법의 2차 개정이 추진되고 있다.

데이터3법의 주요내용으로는 개인정보 법제 및 감독기구 일원화, 개인정보 활용 기반 조성, 개인정보 보호 강화, 해외 법제와의 상호운용성 고려 등이 있으며, 개인정보보호법 2차 개정안의 주요내용으로는 개인정보전송요구권 도입, 자동화된 의사결정에의 대응권 도입, 이동형 영상정보처리기기 운영 기준 마련, 개인정보 국외이전 방식 다양화 및 중지 명령권 신설, 형벌 중심의 제제를 경제벌 중심으로 전환 등이 있다.

(2) 데이터3법

(가) 데이터3법 1차개정 (`20.8)

■ 개인정보 법제 및 감독기구 일원화

- 여러 법에 분산되어 있던 개인정보 보호 규정을 개인정보보호법에 통합
- 행안부, 방통위, 금융감독위 등에 분산된 개인정보 감독권한을 개인정보보호위에 집중시킴
- 개인정보보호위를 독립된 중앙행정기관으로 격상시켜 권한확대·강화

■ 개인정보 활용 기반 조성

● 개인정보 개념 명확화 및 처리요건 완화

- 개인을 알아볼 수 있는 정보 또는 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보
- 당초 수집 목적과 합리적으로 관련된 범위 내에서 정보주체의 동의없이 수집이용제공 가능

● 가명정보 개념 도입 및 활용가능 명시

- 통계작성, 과학적연구, 공익적 기록보존을 위하여 정보주체의 동의 없이 처리가능
- 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하고, 과학적연구를 과학적 방법을 적용하는 연구로 규정하여 민간의 자유로운 정보활용 기초마련
  (과학적 방법을 사용하면 사기업에서도 가명정보의 자유로운 활용이 가능)

■ **개인정보 보호 강화**

● **가명정보에 대한 안전조치의무 및 결합제한**

- 가명정보를 원상복원할 수 있는 추가정보를 별도로 분리하여 보관 관리 의무
- 서로 다른 개인정보처리자 간의 가명정보 결합은 별도의 전문기관만이 가능

● **개인정보 영향평가**

- 공공기관은 개인정보침해 우려시 위험요인 분석 및 개선사항 도출을 위한 평가를 실시의무

■ **해외 법제와 상호운용성 고려**

● **국내에 주소 또는 영업소가 없는 외국기업 등에게 국내 대리인의 지정의무 부과**

- 국내 개인정보주체의 권리보호 및 편익증진

● **국외 이전 개인정보의 보호 및 상호주의**

- 정보주체의 동의 하에 개인정보 국외 이전을 허용
- 상대국의 개인정보 국외이전 제한 수준에 상응하는 제한 가능

■ **제재강화**

- 전체 매출액의 3%이하에 해당하는 금액을 과징금으로 부과 가능

(나) 개인정보보호법 2차 개정안

■ **개인정보 전송 요구권 도입**

- 정보주체가 자신의 정보를 본인 및 다른 처리자에 전송을 요구할 수 있는 권리
- 자신의 정보를 수동적으로 지키는 권리를 넘어 능동적으로 활용하도록 권리강화
  (마이데이터 사업의 근거규정이 됨)

■ **자동화된 의사결정에의 대응권 도입**

- 정보주체가 해당 결정에 대한 거부, 이의제기, 설명요구를 할 수 있는 권리
- 개인정보를 자동으로 처리하여 개인을 평가시 낙인, 차별 등 불이익이 발생할 위험을 제거

■ **이동형 영상정보처리기기 운영 기준 마련**

- 촬영사실을 표시하였음에도 거부의사를 밝히지 않는 경우 촬영을 허용
- 이동형 기기(드론, 자율주행차 등)를 규율할 수 있는 근거 마련
  (CCTV같은 고정형 기기만을 규율하고 있어 발생하는 법률 미비를 해소)

■ 개인정보 국외이전 방식 다양화 및 중지 명령권 신설

● 개인정보 국외이전 방식 다양화

- 적정한 개인정보 보호 수준이 보장되는 국가 또는 기업으로 이전을 허용
- 동의 외에 다양한 방식을 규정하여 해외법제와 상호운영 원활에 기여

● 개인정보 국외이전 중지 명령권

- 감독기관에 개인정보 추가이전을 제한하는 중지 명령권을 부여함
- 개인정보를 보호가 취약한 지역으로 이전하는 것을 제한하여 국외이전 개인정보를 보호

■ 형벌 중심의 제재를 경제벌 중심으로 전환

- 형벌 규정은 과징금으로 전환하고 형벌은 '자기 또는 제3자의 이익을 목적'인 경우로 제한
- 과징금 상한액을 '위반행위 관련 매출액'의 3%이하에서 '전체 매출액'의 3% 이하로 상향
- 기존 형벌 중심의 제재는 보호 담당자에게 과도하고 기업에는 미흡하다는 여론을 반영

(3) 향후 전망

개인정보 활용이 더욱 많아질 것으로 예상된다. 정보주체 권리침해 우려로 개인정보 활용을 강조하는 개인정보보호법의 방향에 반대하는 목소리가 상당수 있음에도 불구하고 경제적 필요성, 세계적 흐름 등의 이유로 우리나라의 법제도는 개인정보 활용을 지원하는 방향으로 나아갈 것이다. 그리고 EU, 미국, 중국 등의 법제도 변화에 따른 불이익이 발생하지 않도록 선제적 대응을 강화하는 것이 필요해지고 있다. 따라서 주요 인공지능 선도국의 법제도의 참조 및 반영이 활발할 것으로 예상된다.

4. 정책 - 인공지능산업 육성, 사이버보안 강화

가. 현황

다수 국가에서 정책자금지원, R&D지원, 민관협력, 고급인력양성, 산업기반조성 등 정책의 대강에서는 상당히 유사한 모습을 보이고 있으나, 각 국가별로 자신의 특수한 상황에 맞추어 다른 모습도 보이고 있다. 주요국은 인공지능의 중요성을 인식하여 국가 전략 산업으로 적극 육성중이며 한편으로는 날로 증가하는 사이버보안의 위협에 대응하기 위한 정책도 동시에 펼치고 있다. AI보안이라는 독립영역은 앞으로 만들어질 것으로 예상되나 아직은 인공지능과 보안 양쪽의 영역에서 별도의 정책이 각각 진행되고 있는 모습을 보이고 있다. 이 연구에서는 미국, 중국, EU, 우리나라의 인공지능 육성 정책 및 사이버보안 강화 정책 중 관련 있는 내용을 선별하여 간략히 소개한 후 주된 정책을 고찰하였다.

나. 미국의 정책

인공지능 선도국으로 세계 1위를 지키기위해 노력중이며, 민관협력에 집중하고 있다. 원천기술, 고급인력, 첨단반도체 설계, 제조업부문에서 강점을 가지고 있다. 사이버보안 최강국임에도 수많은 고강도 공격에 노출되어 있어 방어에 국가적 차원의 노력을 기울이고 있다. 중국을 견제하기 위해 주요 네트워크 등에 중국의 영향을 배제하는 정책인 클린 네크워크 프로그램을 발표하였다.

주요 인공지능 정책으로는 미국 AI 이니셔티브 행정명령 (`19.2), 국가 AI R&D 전략계획 업데이트 (`19.6) 등이 있으며, 주요 사이버보안 정책으로는 미국국가사이버보안전략 (`18.9), 클린 네트워크 프로그램 (`20.8) 등이 있다.

(1) 주요정책 소개

■ AI정책

● 국가 AI R&D 전략계획 (`16.12)
- 연방정부의 장기투자강화 위한 7개 분야 R&D 제시

● AI 정상회의 (`18.5) :
- 혁신 규제장벽 제거와 'AI선정위원회' 설치 등 AI활성화 방안 논의

● 미국 AI 이니셔티브 행정명령 (`19.2)
- 국가 AI 추진원칙·목표, 추진조직·역할 정의

● 국가 AI R&D 전략계획 업데이트 (`19.6)

- 민관협력 추가, 분야별 보완
● 미국 AI 이니셔티브 1주년 이행 보고서 (`20.2)
- R&D투자, 자원공급, 인력양성, 국제환경 조성 등에서 진척사항 점검

■ 사이버보안 정책
● 사이버안보를 위한 국가전략 (`03)
- 공공부문과 민간부문을 아우르는 사이버보안 정책
● 미국국가사이버보안전략 (`18.9)
- 사이버 위협으로부터 보호 및 연방정부의 사이버 역량 강화를 위한 수행 단계 제시
● 사이버보안 인력 확충에 관한 행정명령 (`19.5)
- 경진대회, 적성평가실시, 직무순환프로그램 등 사이버보안 인력 확충 대책 제시
● ICT 공급망 보호에 관한 행정명령 (`19.5)
- 미국내 ICT 공급망의 보안성, 무결성, 신뢰성을 보장하여 안보위협에 대처
● 클린 네트워크 프로그램 (`20.8)
- 미국의 중요한 통신과 기술 인프라 보호를 위해 중국 IT기업을 미국 네트워크에서 배제

(2) AI 이니셔티브 행정명령 (`19.2)

■ 배경 : AI 선도국의 국가차원 대규모 투자 전략에 대응, 특히 중국의 첨단기술전략 견제
■ 의의 : 미국 최초 국가차원 AI 전략, 추진원칙·전략목표·추진조직의역할을 정의
■ 내용 :
● 추진원칙
- 연방정부, 산업계, 학계 전반에 걸친 AI의 기술적 진보를 촉진
- 기술 표준 개발, AI 기술 테스트 및 AI 기술 적용에 따른 장벽 완화
- 미국 노동자의 AI 기술 개발 및 적용 스킬 강화
- AI 기술에 대한 국민의 신뢰와 자신감 고취 및 적용과정에서 미국의 가치를 보호
- AI 분야에서의 미국 기업의 기술적 우위 확보, 미국 기업의 핵심 AI 기술 보호, AI 연구 및 혁신지원, 우호적 국제환경 형성 등
● R&D
- AI 특별위원회 설립, AI R&D 전략계획 발표
- 연방 R&D 우선순위 확보와 투자 효율 담보
- 인프라·데이터·표준 등 기반 연구 강조
● 산업
- 자국 산업 보호, 경쟁력 강화, 규제완화 원칙하에 산업 분야별 AI 응용정책 개발
- 중심분야는 교통, 의료 제조, 금융, 농업, 기상, 해양, 우주, 안보 방위
● 인력
- 노동자 보호를 위한 정부 조정 역할 및 민간 참여 독려
- 고급 개발 인력 확충 위한 STEM 교육정책 강화
● 기타
- AI 개발과 활용을 위한 기술 및 윤리적 가이던스 개발
- 국제기구의 AI 개발 원칙 수립에 적극적 역할을 하여 글로벌 AI 리더쉽 강화

(3) 국가 AI R&D 전략 계획 업데이트 (`19.6)

■ 의의 : AI R&D 투자 우선순위 강화를 위해 'AI R&D 전략계획 (`16.12)'를 업데이트

■ 내용 :

● 8대 추진전략

- 근본적인 AI 연구과제에 대한 장기적인 투자 지속
- 효과적인 인간-AI 협업방식 개발
- AI의 윤리·법·사회적 영향 이해 및 대응
- AI 시스템의 보안·안전 보장
- AI 훈련·시험을 위한 공유·공공 데이터셋 및 환경 개발
- 표준 및 벤치마크를 활용한 AI 기술 측정과 평가
- 국가 AI R&D 인력 관련 니즈 파악
- AI 발전 가속화를 위한 민간협력 확대

● 14개 응용분야

- 농업, 통신, 교육, 금융, 정부서비스, 법률, 물류, 제조, 마케팅, 의료, 개인서비스, 과학·공학, 보안, 교통

다. 중국의 정책

인공지능 분야에서 미국의 아성에 도전하는 경쟁국이며, 중앙 및 지방정부의 주도로 정책을 추진하고 있다. 많은 인구 및 미약한 개인정보 보호의식 등의 이유로 엄청난 양의 데이터를 축적하였으며 이를 바탕으로 빅데이터에 강점을 가지고 있다. 사이버보안 문제를 국가 안보 차원에서 다루고 있으며 강한 정보통제를 실시하고 있다.

주요 인공지능 정책으로는 차세대 AI 발전규획 (`17.7), 국가 차세대 AI 표준 체계 구축 지침 (`20.8) 등이 있으며, 주요 사이버보안 정책으로는 국가 사이버공간 보안전략 (`16), 사이버보안법 (`17.6) 등이 있다.

(1) 주요정책 소개

■ AI정책

● 중국 제조 2025 (`15.5)

- 제조분야에 대한 포괄적 지능화로 세계 최고 제조국가 달성

● 차세대 AI 발전규획 (`17.7)

- AI를 중국미래를 선도할 국가적 전략으로 제시

● AI 산업 3개년 발전촉진계획 (`17.12)

- AI 관련 글로벌 경쟁에서 우위 선점을 목표

● 차세대 AI 특구 지정 계획 (`19.6)

- `23년까지 차세대 AI 특구 20개 지정 계획

● 국가 차세대 AI 표준 체계 구축 지침 (`20.8)
- AI 산업의 건전하고 지속가능한 발전을 위한 지침 제시

■ 사이버보안 정책
● 총체적 국가 안전관 (`13)
- 사이버 공간을 국가 주권의 영향력 범위로 확대
● 국가 사이버공간 보안전략 (`16)
- 사이버 보안을 4대원칙과 9대 임무를 통해 관리
● 사이버보안법 (`17.6)
- 외국기업에 대한 데이터 중국내 저장 의무화
● 데이터보안법 (`21.6)
- 중국내에서 수집한 데이터의 역외 이전 제한
● 개인정보보호법 (`21.8)
- 개인정보의 국외 이전 요건 충족 시 허가

(2) 차세대 AI 발전규획 (`17.7)

■ 3단계 전략 목표
● AI 핵심산업 규모 1,500억 위안, 관련 산업 규모 1조 위안 이상 (`20년)
- 다른 국가들에 경쟁력을 유지하며 AI 개발 여건을 최적화
● AI 핵심산업 규모 4,000억 위안, 관련 산업 규모 5조 위안 이상 (`25년)
- 세계 최고의 AI 기술국으로 도약
● AI 핵심산업 규모 1조 위안, 관련 산업 규모 10조 위안 이상 (`30년)
- AI 이론·기술·응용 등 전분야에서 미국을 뛰어넘어 세계 1위 국가로 등극
■ 6대 중점 과제
- 개방·협력형 AI 과학 기술 혁신 시스템 구축
- 최첨단·고효율의 스마트 경제 육성
- 안전하고 편리한 스마트 커뮤니티 건설
- AI 분야의 군민융합 및 국가안보 지원 강화
- 안전, 고효율의 스마트 인프라 체계 구축
- 차세대 AI 중대 프로젝트의 선도적 추진

(3) AI 산업 3개년 발전촉진계획 (`17.12)

- '중국제조 2025', '차세대 AI 발전규획'의 실행 계획
■ 핵심목표
- AI 적용 제품 및 응용 범위 확대
- AI 전반의 핵심 기술 향상
- 스마트제조 발전
- AI 지원 시스템 및 인프라 개선
■ 주요추진과제

- 의료, 교통, 농업, 금융, 물류, 교육, 문화, 여행 등 영역의 애플리케이션을 집중적으로 개발
- 환경감지, 인간-기계 인터페이스, 민첩·정확 제어, 실시간 그룹협동 가능 스마트 설비 개발
- 상품이해, 모드 인식, 언어이해·분석, 의사결정 등 핵심기술에 대한 연구와 상용화 추진
- 스마트 센서와 신경망 반도체 개발을 골자로 하는 기초 기술 개발, 개방형 플랫폼 구축
- 제조업의 스마트화를 통해 2020년까지 차세대 산업용 로봇의 대량 생산과 응용을 실현
- 업종별 표준 테스트 및 지식재산(IP) 플랫폼 구축, 네트워크 설비 보강, 민관협력으로 정책적 지원을 늘리고 창업을 독려, 인재를 육성하면서 환경 조성

(4) 국가 차세대 AI 표준 체계 구축 지침 (`20.8)

■ 2단계 표준화 목표

● 1단계 : `21년까지 AI 표준화 최상위 설계 확정

- 표준 간 관계 명확화, AI 표준화 작업의 질서있는 발전 지도, 핵심범용기술, 핵심영역기술, 윤리 등 표준체계 구축 및 표준 개발에 관한 총체적 규칙 연구를 실시

● 2단계 : '23년까지 초보적 수준의 AI 표준 체계 구축

- 데이터, 알고리즘, 시스템, 서비스 등 시급한 중점 표준 우선 연구
- 제조, 교통, 금융, 보안, 주거, 양로, 환경보호, 교육, 의료건강, 사법 등 우선 추진
- AI 표준 시험 및 검증 플랫폼 구축 및 공공 서비스 기능 제공 등 실시

■ 8개 부문 AI 표준 체계 기본틀

- 기초 공통 표준, 지원 기술·제품 표준, 기초 SW/HW 플랫폼 표준, 핵심범용기술 표준, 핵심분야기술 표준, 제품·서비스 표준, 산업 응용 표준, 안전·윤리 표준

라. EU의 정책

미국, 중국에 비해 뒤쳐진 인공지능 분야의 경쟁력을 확보하기 위해 노력중이며, 윤리·법·제도 등을 선제적으로 제정하여 세계표준을 주도하는데 주력하고 있다. 지역내 디지털통합을 추진하고 있으며 R&D 지출을 증대하여 유럽 전반의 인공지능 경쟁력 개선을 도모하고 있다.

주요 인공지능 정책으로는 유럽 AI 전략 (`18.4), Horizon2020 (`14~`20) 등이 있으며, 주요 사이버보안 정책으로는 EU 사이버보안법 (`19.3)이 있다.

(1) 유럽 AI 전략 (‘18.4)

■ 의의 : AI가 산업·기술 경쟁력 제고 및 유럽적 가치에 기반한 신뢰를 담보 가능

■ 목표 : AI 기술·산업 역량 제고 및 도입 확대, AI로 초래될 사회·경제 변화 대응, 적절한 윤리·법적 제제 확립

(2) Horizon 2020 (`14~`20)

■ 의의 : 연구개발 프레임워크 프로그램
■ 내용 :
- 로봇, 빅데이터, 건강, 교통, 미래·신흥기술 등 AI관련 분야에 총 260억 유로를 투입
- `20년 이후에는 매년 200억 유로에 달하는 공공 및 민간 투자 시행
- 빅데이터가치 민간파트너쉽, 로봇관련 SPARC 민관파트너쉽은 유럽 AI발전에 협력 약속

(3) `21년 디지털유럽프로그램 출범예정 (`21~`27)

■ 의의 : 유럽의 디지털 역량 개발 및 강화, 국제 경쟁력 향상을 위한 투자 프로그램
■ 내용 :
- 5개분야에 `21~`27년 동안 총 92억 유로 투자 (고성능컴퓨터, AI, 사이버보안 및 신뢰, 첨단디지털스킬, 경제·사회 전반에서 디지털 기술의 광범위한 활용)
- 경제·사회 전반에서의 인공지능 확산을 목표로 직접적인 AI연구에만 총 25억 유로 투입

마. 한국의 정책

인공지능 분야에서 출발이 늦었으나 정책자금지원, R&D지원, 인력양성지원, 민관협동 등 다른 주요국에서 시행중인 정책들을 서둘러 진행하며 경쟁에 본격적으로 합류하고 있다. AI 보안 분야에 '제2차 정보보호산업 진흥계획'을 중심으로 상세한 지원계획이 수립되어 시행중에 있다.

주요 인공지능 정책으로는 디지털뉴딜(`20.7), 인공지능 법제도규제 정비로드맵(`20.12) 등이 있으며, 주요 사이버보안 정책으로는 국가 사이버안보 기본계획 (`19.9), 제2차 정보보호산업 진흥계획 (`20.6) 등이 있다.

(1) 제2차 정보보호산업 진흥계획 [2021~2025] (`20.6)

■ 정보보호 데이터 활용기반 조성
- 정보보호 데이터 활용을 통한 AI 기반 보안기술 확산
● AI 기반 보안제품 확산을 위한 학습데이터 가공·공유 체계 구축
- 분산된 원천 데이터를 수집·가공 (AI 학습데이터 공유 기반 마련 도모)
- 양질의 AI 학습데이터를 단계적으로 제공 (정보보호제품의 품질 향상 도모)
- AI 보안 학습데이터를 개방 (기업의 제품개발 지원)
● 정보보호기업의 AI 학습데이터 이용 지원
- 학습데이터 구매 및 가공 지원 (정보보호기업의 기능형 보안제품·서비스 개발 지원)
- 비식별 처리 및 비식별 처리기술 개발 지원 (AI 보안 학습데이터의 안전한 활용 도모)
- AI 보안 테스트 지원 (AI 보안 머신 학습의 정확도 개선과 제품 고도화 도모)
- AI 보안 기술개발 챌린지 대회 개최 (한국형 캐글)

■ AI 기반 물리보안 산업 육성
- 국민 삶의 질 제고를 위한 물리보안 산업 육성 및 응용 확대
● 물리보안 선도적 기술 개발
- 지능형 CCTV 선도 기술 개발 및 기업에 기술이전
- 물리보안 통합 플랫폼 개발 및 확산
● 물리보안 산업 기반 강화
- 성능인증 대상 확대 (품질우수 제품의 확산 도모)
- 혁신기술 제품·서비스 실증단지 구축
- 물리보안 경진대회 개최
● 물리보안 응용 서비스 확산
- 응용서비스 확대
- 무인서비스 기술고도화

■ 정보보호기업 성장 지원
- 정보보호기업의 혁신 성장을 위한 선순환 생태계 구축
● AI 기반 등 혁신 보안 기업 고성장 지원 체계 강화
- 우수 AI 보안 기술을 가진 유망 기업 선정·육성 (발굴부터 해외진출까지)
- 맞춤형 3SS 성장 프로그램 도입
- 투자기반 확충
● 대기업과 정보보호기업 매칭형 기술개발 지원 사업
- 데이터, 네트워크, 인공지능 관련 보안 신기술 개발
- 대기업에 기술개발과제 지원, 중소기업에 기술개발지원급 지급, 양자간 매칭 추진
- 보안 신기술 연구 집중지원 (AI보안, 5G보안, 클라우드보안, 데이터보안, 반도체보안 등)

■ 차세대 보안 신기술 확보
- 4차 산업혁명 시대를 앞당길 미래 선도 보안기술 육성
- 디지털 전환에서 새로운 사이버 위협에 대비 위해 정보보호 R&D 투자 확대
  (`25년 정보보호 R&D 예산 규모 1,000억원)
● 디지털 경제 활성화를 위한 신기술 집중 투자 (`21~`25, 250억/년)
- 비대면 서비스 보안강화 및 신뢰성 보장 기술 개발 중점 지원
- AI학습데이터 보호 위한 신기술 개발 추진
- AI 기반 보안기술 및 AI 자체 보안 집중

■ 정보보호 전문인력 양성
- 정보보호 인력체계 혁신을 통한 정보보호산업 성장 주도
● 정보보호 전문인력 양성
- 정보보호 특성화대학·융합보안대학원 확대
- 재직자 실무역량 및 신기술 분야 보안 역량 강화 지원
- 우수인재 발굴·육성 기반 강화 (초중고 교육, 경진대회 개최, 부서간 협력체계구축 등)

5. 결론 및 제언

(1) 결론

전통적인 보안의 영역에 인공지능이 들어오며 많은 변화가 발생하였다. 인공지능 산업의 발전을 위해 정보의 활용이 필수가 되었으며 아울러 정보의 보호가 더욱 강조되는 상황이 된 것이다.

인공지능 분야 주요국은 윤리와 법·제도를 통해 시대의 변화를 담은 새로운 질서를 정립하고 있으며 정책을 통해 새로운 산업을 적극 육성하고 있다. 윤리·법·제도 측면에서 인공지능에 대한 기본원칙을 정립하고 역기능을 방지하고 있으며, 정책으로는 자국의 산업을 육성하고 기술·자원을 보호하며 나아가 세계 선도국의 지위를 차지하기 위해 치열한 경쟁을 하고 있다.

미국은 오랜 연구, 원천 기술, 고급 인재 등을 바탕으로 명실공히 세계 1위 자리를 굳건히 지켜왔으나, 최근 중국이 많은 인구와 정보보호 인식의 부족을 바탕으로 다량의 빅데이터를 확보하며 맹추격하고 있는 상황이다. 한편 EU는 양대 강국 보다 다소 뒤쳐져 있으나 법률과 제도를 먼저 정비하며 표준을 마련하는 방식으로 선도국 경쟁에 합류하고 있다.

우리나라는 미국, 중국, EU에 비해 비록 출발은 다소 늦은 감이 있으나 뛰어난 순발력을 발휘하여 윤리·법·제도 전반에 걸쳐 거의 대등한 모습을 보이고 있으며 특히 인공지능과 보안을 하나로 묶어 ‘AI보안’을 정책적으로 육성하는 부분에 있어서는 상세한 모습을 보이고 있다.

(2) 제언

다른 주요국에서 보이는 장점들을 수용하여 인공지능 산업에서 선두권으로 도약하는 시기를 더욱 앞당길 필요가 있다고 판단된다. 미국의 민관협력, 중국의 정부주도, EU의 법제도정비가 우리가 참고해야할 큰 방향이라면 인공지능을 총괄하는 기관을 신설하여 업무효율을 극대화한다거나, 관련 예산을 대폭 증액하고, 해외인재를 유치하기 위한 별도의 계획을 신설하며, 기업 간의 교류를 실제적으로 활성화하는 것 등 세부적인 방식에 관한 내용도 시급히 도입할 필요가 있다고 판단된다.

이번 연구에 참가한 자문위원들로부터도 다양한 제언을 받았다. 선별하여 요약하였다.

AI 기술을 활용한 대형 사업을 발굴하고 시행할 필요가 있다. 소수의 기업이 혜택을 분점하는 형태를 지양하여 스타기업이나 스타기술을 육성하고 국가나 대기업이 활용하는 사업을 발굴하여 지속성 확보하는 것이 필요하다. 데이터3법에 대한 명확한 가이드라인이 필요하다. 아울러 중소기업을 위한 문제해결 도구(S/W)가 필요하다.
AI & Data 관련 신기술 개발을 위한 AI관련 아이디어 공모, 경진대회 등 정책지원이 필요하다. 우수한 기술이 개발시 실제 적용가능한 기관이나 업체와 연결하는 것이 필요하다. 우수인력 양성을 위해 재직자 또는 대학원 수준의 인력에 대한 투자가 필요하다. 정책자금을 정말

필요하고 가치있는 기술에 지원하기 위한 방편으로, 공공기관 담당자에 대한 전문교육이 필요하다. AI & Data 품질에 대한 규정 및 인증 제도가 필요하다.
데이터를 제공받을 수 있는 루트가 조금더 다양해지고 늘어나야 한다. 현재 제공되고 있는 다수의 데이터가 활용에 부적절하거나 현실성이 없는 문제가 있다. 기업의 데이터 저장 비용부담을 줄이기 위한 방안이 개발되었으면 한다. 데이터를 제공하는 기관, 단체, 개인 등에게 인센티브를 주어 데이터를 제공하는 것이 자신에게 도움이 되는 제도를 만들 필요가 있다.

참 고 문 헌

관계부처 합동, 국가 사이버안보 기본계획, `19.9
관계부처 합동, 제2차 정보보호산업 진흥계획, `20.6
국가정보원 외, 2021 국가정보보호백서,
KIAT, 최근 미국과 중국 AI 정책동향 및 시사점, `20.9
KISA, EU 데이터 전략 계획 주요 내용 분석, `20.3
NIA, EU 인공지능법(안)의 주요 내용과 시사점, `21.4
한국수출입은행, 인공지능산업 현황 및 주요국 육성 정책, `21.10
정보통신기획평가원, 주요국 인공지능 정책 동향과 시사점, `19.11
정보통신정책연구원, 미중일 AI인재 확보 정책 비교 및 시사점, `20.6
AI타임스, [세계 속 AI ① 중국: 상 정책편] 미국 넘어서는 세계 초일류 AI국가, `21.6
소프트웨어정책연구소, 주요국 통계 현황 비교를 통한 국가 AI산업 통계 체계 발전방안, `21.2
과학기술정보통신부, 주요국 인공지능 정책 동향 분석
한중과학기술협력센터, 중국의 인공지능 정책동향, `20.4
금융보안원, 중국의 차세대 인공지능 발전 규획 및 실행 계획, `18.5
개인정보보호위원회, 인공지능(AI) 개인정보보호 자율점검표, `21.5
주간동아, 미 ‘클린 네트워크’ 5개 수단 동원, 중국판 ‘카톡’ 퇴치전, `20.11
관계부처 합동, 신뢰할 수 있는 인공지능 실현 전략(안), `21.5
정보통신정책연구원, 신뢰할 수 있는 인공지능을 위한 최근 주요국 대응동향 및 시사점, `21.6
소프트웨어정책연구소, 유럽(EU)의 인공지능 윤리 정책 현황과 시사점, `21.3
관계부처 합동, 인공지능 국가전략, `19.12
관계부처 합동, 사람이 중심이 되는 「 인공지능(AI) 윤리기준 」, `20.12
한중과학기술협력센터, 중국 차세대 인공지능 관리 원칙 발표, `19.6
정보통신신문, 인공지능 활용 사이버 보안 급성장, `21.2
KISA, 2020글로벌 정보보호 산업시장 동향조사 보고서, `21.3
관계부처 합동, 인공지능 법·제도·규제 정비 로드맵, `20.12
KISA, [심층분석]미국 개인정보보호 법률 및 입법현황, `21.9
KISA, 중국 개인정보보호 법제 동향 분석, `21.2
김성현, 이창무, EU GDPR과 국내 개인정보보호 법제 비교분석, `18.12
KISA, 방송통신위원회, 2020EU일반개인정보보호법 가이드북,
윤상필, 인공지능 시대의 보안 패러다임과 책임 구조의 변화, `17.12