

정혜련 경찰대학 법학과
법학박사(S.J.D/상법,경제법)

목 차

I. 서론

II. 미국의 데이터 정책과 관련법안

III. 유럽 데이터 입법 동향

IV. 비교 및 분석

V. 결론

I . 서론

I. 서론

개인정보와 데이터 정책: 개인정보 국외이전

2020년 중국업체 바이트댄스의 sns인 틱톡은 개인정보법규 위반을 이유로 방송통신위원회로부터 1억8천만원의 과징금과 600만원의 과태료의 제재

틱톡이 법정대리인의 동의 없이 만14세 미만의 개인정보를 수집, 이용자의 개인정보를 국외 이전하면서 그 사실을 알리고 동의를 받지 않은 것이 문제가 되었음

작년 22일 아일랜드 데이터보호위원회 DPC는 메타에 개인정보보호법 위반을 이유로 12억유로(한화 1조 7천억원)의 과징금을 부과하고 6개월 내에 이용자들의 관련 데이터를 미국으로 전송하는 것을 중단 및 관련 데이터 삭제를 명함

동 조치는 미국이 유럽의 개인정보를 미국으로 전송할 수 있는 근거가 되었던 프라이버시 실드가 2020년 유럽사법재판소에 의해 무효로 결정된 이후, 새로운 협정이 발표되지 않은 데에서 기인. 이로 인하여 메타 뿐만이 아닌 다른 수천개의 미국 기업도 EU의 개인정보보호 조사 대상이 될 수 있게 됨

I. 서론

개인정보와 데이터 정책: 개인정보 국외이전

오늘날 빅테크 플랫폼의 등장으로 국경을 넘은 서비스 이용이 가능해 서비스 제공 및 이용을 위해서는 데이터 수집과 처리가 기본적으로 필요함

데이터의 가치가 높아짐에 따라 데이터를 둘러싼 쟁점이 다각화

마이데이터사업 활성화와 같이 데이터 소유권에 대한 적극적인 개념의 도입을 위한 제도(cf.데이터신탁제도)를 만들어 개인정보를 포함한 데이터의 적극적인 유통을 위한 체계 장려하기도 함

데이터 정책에 있어서의 중요한 두 축은 데이터 이전 및 유통의 자유에 관한 부분과 데이터의 현지화 관련 부분

데이터 이전 및 유통의 문제: 데이터 수집과 활용에 필연적으로 연계됨

민감 데이터의 유출, 데이터 왜곡과 남용 등-> 국가안보에 부정적 영향을 끼친다는 인식-> 데이터의 자유로운 이동이 제한 -> 데이터 및 개인정보의 이전 및 유통의 제한 여부, 데이터의 자국 내 서버 저장 강제화 등(데이터 현지화 이슈)

데이터 현지화는 데이터를 처리하거나 저장하는 컴퓨팅 설비를 한 국가의 관할권 내에 위치하도록 하여 결국 컴퓨팅 설비에 저장된 데이터를 그 국가의 영토에 머물도록 하므로 데이터의 국외 이전을 제한하는 효과

II. 미국의 데이터 정책과 관련법안

데이터 이동 및 국가간 이동에 관한 폭넓은 자율성

글로벌 데이터 시장을 선점하고 있는 미국의 빅데이터 기업들이 지속적으로 우월적이고 독점적 지위를 시장에서 유지함으로써 미국의 산업경쟁력을 강화

미국의 데이터 정책은 ①데이터 주권의 주체인 개인의 정보보호 정책

② 개인정보 국외 이전의 자유와 데이터 현지화 금지

미국의 개인정보 보호정책-> 빅데이터 산업의 활성화에 대한 전제

디지털 서비스의 신뢰와 투명성 확보를 위해 개인정보 보호를 위한 정책을 강화

다만, 민간영역을 포괄적으로 규율하는 연방 차원의 개인정보 보호법은 존재하지 않지만, 공공 부문의 the Privacy Act가 존재하고, 민간부문의 아동프라이버시 보호법(COPPA), 건강보험법(HIPAA), 전자통신에서 프라이버시 보호법(ECTPA) 등 영역별 법제를 취하고 있음.

개인정보보호 정책은 개인정보 침해 문제가 대두된 2010년대에 강화

- '캘리포니아주 프라이버시 권리법(CPRA)' 개인의 데이터 주권을 강화하는 대표적인 법제로, 2020년 11월 3일 캘리포니아 주가 제정. 타 법령과 달리 전 산업에 걸쳐 적용되는 일반법 성격의 개인정보보호법

II. 미국의 데이터 보호 법률과 관련법안: '해외정보이용 합법화법(CLOUD Act)',

FTA

2018년 미국 정부기관에게 실제 데이터가 저장된 위치에 관계없이 제공 요청을 할 수 있는 권한을 부여한
은 국가안보를 이유로 역외 정보에 대한 접근권을 인정한 법령

통상정책:

미국은 개인정보 국외 이전의 자유 및 데이터 현지화 금지를 통상정책과 연계하여 추진

- 디지털 무역 관련 규범과 규칙을 FTA와 연계하는 방식으로 나타남.

2001년부터 2016년까지 체결된 FTA 가운데 90개의 FTA가 디지털 무역 관련 규칙을 직간접적으로 포함
이 중 69개의 FTA는 별도의 챕터에서 디지털 무역 규칙을 명문화하였으며, 21개의 FTA는 독립 챕터는
아니나 디지털 무역 관련 조항을 FTA 협정문에 포함시키는 방식을 취하고 있음.

II. 미국의 데이터 보호 법률과 관련법안: 통상정책 CPTPP

-아시아 태평양 지역 11개국의 참여 아래 2018년 12월 30일 발효한 CPTPP는 최종적으로는 미국이 참여하지 않았지만 미국의 주도 아래 협상이 시작된 협정이자, 디지털 교역의 기본 틀을 처음으로 제시한 협정이기에 동 협정의 의미는 큼.

동 협정은 회원국에게 정보의 국경 간 이전에 대해 각 당사국이 스스로 규제할 수 있음을 확인 (제14.11조 1항)

사업수행을 목적으로 하는 경우 정보의 국경 간 이전을 허용할 것을 회원국의 의무로 규정(제 14.11조 2항). 예외로 회원국의 공공정책 목적을 달성하기 위한 경우에는 정보의 국경 간 이전을 제한할 수 있으나, 이 경우에도 국제교역을 제한하기 위한 목적이거나 과도한 제한을 실시하는 것은 금지(제14.11조3항).

데이터 현지화와 관련하여서도 동일한 구조로 이루어져 있고, 회원국은 컴퓨팅 설비의 사용에 대해 스스로 규제할 수 있으나(제14.13조 1항), 자국 영토 내의 컴퓨팅 설비를 이용하거나 자국 영토 내에 컴퓨팅 설비를 위치할 것을 요구하는 것은 금지함(제14.13조 2항).

예외로 회원국의 정당한 공공정책 목적(LPPO: Legitimate Public Policy Objective)을 달성하기 위한 경우에는 규제권한을 가지지만 이 경우에도 국제교역을 제한하기 위한 목적이거나 과도한 제한을 실시하는 것은 금지(제 14.13조 3항)

II. 미국의 데이터 보호 법률과 관련법안: CPRA

캘리포니아주 프라이버시 권리법(The California Privacy Rights of 2020, “CPRA”) 2018년 제정된 캘리포니아소비자개인정보보호법(The California Privacy Act, CCPA)의 수정 버전

소비자의 권리와 기업의 의무를 강화하고 미국 최초의 개인정보보호 전달 집행기관 신설 내용을 포함

CPRA 적용 대상 기업으로는

- ①연 매출이 2,500만 달러 이상이거나
- ②소비자 개인정보를 10만 건 이상 보유하고 있거나
- ③개인정보 판매 및 공유에 따른 매출이 총 매출의 50% 이상을 차지하는 경우로 제한

<주요내용>

- ㉠ 새로운 원칙의 도입 및 개인정보보호 관련 개념의 확장
- ㉡ 소비자 권리 강화
- ㉢ 기업의 의무와 책임성 강화
- ㉣ 개인정보보호 감독기구 신설

1. CALERA 법안

2021년 2월 4일 미국 상원 Amy Klobuchar 의원이 대표 발의한 CALERA 개정안(The Competition and Antitrust Law Enforcement Reform Act) 일반적인 경쟁법의 개정안

주요특징:

경쟁법의 적극적인 집행과 목적의 확대

경쟁을 감소시키는 위험 중심의 기준(appreciable 'risk' of lessening competition)을 도입
반경쟁성의 기준을 설정(materially)하여 기업결합에 대한 경쟁법 집행의 효과성 제고를 기대
기업결합에 있어서 반경쟁성의 입증 책임을 결합 기업 당사자(merging parties)에 전가하고,
관련 시장 획정을 생략하며, 구매자 독점(monopsony)을 추가하는 등 반독점법의 실효성을 회복하여
빅테크 기업들을 겨냥하고자 함

2. 미국경제에서의 경쟁촉진에 관한 행정명령

2021년 7월 9일 바이든 대통령은 미국 경제와 산업의 독과점적 시장구조를 개선하고 경쟁제한 폐해를 시정하기 위해 「미국경제에서의 경쟁촉진에 관한 행정명령」에 서명

행정명령은 경쟁당국(FTC, DOJ)뿐만 아니라 농림, 산업, 국방, 보건, 에너지, 노동, 교통, 주택 등을 관장하는 10여개이상 부처에 72개 의무적 조치(calls on and directs)와 권고적 조치(encourages and urges) 시행할 것 규정

- ① 주요 산업별 독과점 이슈와 행정명령의 정책적 방향성(Section 1. Policy)
- ② 범정부적 차원 경쟁정책 법적근거(Section 2. The Statutory Basis of a Whole-of-Government Competition Policy)
- ③ 행정명령의 효과적 실행을 위한 부처간 협력(Section 3. Agency Cooperation in Oversight, Investigation, and Remedies)
- ④ 백악관 내 경쟁위원회의 설치와 역할(Section 4. The White House Competition Council)
- ⑤ 독과점 시장구조 개선을 위한 각 부처별 추진 업무(Section 5. Further Agency Responsibilities)

3. SOE 법안: The Open App Market Act

SOE법(「A Stronger Online Economy: Opportunity, Innovation, and Choice」)은 「The American Innovation and Choice Act」, 「The Platform Competition and Opportunity Act」, 「The Ending Platform Monopolies Act」, 「The Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act」, 「Merger Filing Fee Modernization Act」의 5개로 구성된 패키지 법안

2020년 발표된 ‘디지털시장에서의 경쟁상황 조사:

보고서 및 권고사항(Investigation of Competition in the Digital Marketplace: Majority Staff Report and Recommendations)’ 을 기반으로 함

3. SOE 법안: The Open App Market Act

<p>American Innovation and Choice Online Act</p>	<p>플랫폼 사업자(covered platform operator)에 의한 차별적 행위, 특히 자사우대(self-preferencing) 금지</p>
<p>Platform Competition and Opportunity Act</p>	<p>시장지배적인 온라인 플랫폼 기업의 잠재적 경쟁자에 대한 인수합병 행위 규제</p>
<p>Ending Platform Monopolies Act</p>	<p>대상 플랫폼 사업자가 현재 운영하고 있는 플랫폼 사업에서의 시장지배력을 다른 사업부문에까지 전이하는 행위 제한</p>
<p>Augmenting Compatibility and Competition by Enabling Service Switching Act</p>	<p>소비자 및 비즈니스 사용자의 서비스 전환비용 및 진입장벽을 낮추기 위한 목적 온라인 플랫폼 이용자의 데이터 권익 보호 플랫폼간 서비스 상호운용성 강화</p>
<p>Merger Filing Fee Modernization Act</p>	<p>반독점 집행 활성화, 경쟁보호 조치 적극적으로 시행하기 위한 미국 경쟁당국(FTC, DOJ)의 예산 확충 목적</p>

3. SOE 법안: The Open App Market Act

The Open App Market Act

<p>SEC. 3. Protecting a Competitive App Market</p>	<p>아래 행위 금지</p> <p>(1) 앱스토어에 대한 사용조건으로 개발자에게 CC 자신의 인앱결제 시스템을 사용하도록 요구하는 행위</p> <p>(2) 타 앱스토어의 이용약관보다 가격조건이 유리하도록 약관을 요구하는 행위</p> <p>(3) 특정 앱에 대해 불합리한 우대·랭킹으로 차별하는 행위 등</p> <p>CC는 자신이 운영하는 시스템에 사용자가 쉽게 접근할 수 있는 수단을 허용·제공하여야(Interoperability)</p>
<p>SEC. 4. Protecting the Security and Privacy of Users</p>	<p>의무 준수</p> <p>(1) 사용자의 개인정보보호, 보안 또는 디지털 안전 의무</p> <p>(2) 스팸 또는 사기 예방 의무</p>

4. 미국혁신경쟁법(United States Innovation and Competition Act) 및 미국경쟁법(The America COMPETES Act)

<미국경쟁법>

미국의 국가경쟁력 강화와 중국견제 등 미국혁신경쟁법과 유사한 내용

반도체 제도 인센티브나 연구 및 혁신, 안보나 금융, 자원 이슈를 다루는 위원회 등을 규정

정보 보호와 관련하여, 지적재산권을 위반한 우선관찰대상국의 상품 금지에 대한 규정

법안 외에도 미국의 중국 전자상거래 기업 견제 확인 가능

4. 미국혁신경쟁법(United States Innovation and Competition Act) 및 미국경쟁법(The America COMPETES Act)

대(對)중국 경쟁법

중국계 플랫폼기업의 지적재산권 침해나 산업 스파이 활동, 기타 법률 위반 등에 대해 국가적인 대응에 나설 것

세부 법안명	주요내용
CHIPS and USA Telecom Act	반도체 산업에서 미국의 기술우위 유지, 중국산 통신장비 의존방지
Endless Frontier Act	국립과학재단(NSF) 내 기술국 신설, 연구안보 강화, STEM 인재양성 촉진
Strategic Competiton Act	중국위협에 대비한 국제협력, 미국가치 수호, 수출통제 강화 등
Securing America's Future Act	중국산에 대응할 Buy American 적용 강화, 사이버안보 인력 양성
Meeting the China Challenge Act	중국의 인권탄압 등 행위에 대응할 기존 및 신규 제재의 적극활용
Trade Act of 2021	일반특혜관세(GSP) 및 기타수입관세임시철폐제도(MTB) 재개, 301조 추가관세 면제 재개, 강제노동/지재권 탈취제품 수입금지 등
Other Matters	미 고등교육기관의 공자학원 연계성 조사, 합병수수료 체계 현실화 등

평가 및 소결

미국의 데이터 정책은
데이터 주권의 주체인 개인의 정보보호 정책과 개인정보 국외 이전의 자유와 데이터 현지화 금지
미국의 개인정보 보호정책-> 빅데이터 산업의 활성화에 대한 전제 (경쟁정책: 빅데이터 및 인공지능 산업
진흥 위한 기반 조성

디지털 서비스의 신뢰와 투명성 확보를 위해 개인정보 보호를 위한 정책을 강화

미국의 경우 빅테크 기업에 의한 경쟁제한성에 대한 우려가 존재하는 것은 사실이나,
아직 규제의 효용 검증이 되지 않았다는 우려 역시 공존

플랫폼 규제에는 강력한 법 집행이 아닌 간접적 방법을 이용하였고,
다른 국가와의 관계에서 자국의 이익을 보호하기 위한 차선을 개발하는 데에 그 주안점

III. 유럽 데이터 정책 동향

1. 디지털시장법(Digital Markets Act, 이하 “DMA”)

DMA는 유럽연합(EU)가 미국 빅테크의 독점 구조를 개선하기 위해 입법을 추진하여 2020년 12월 15일 초안이 발표됐으며, 2022년 3월 24일 EU의 입법기구인 유럽의회와 행정부인 집행위원회, 기구인 유럽이사회는 디지털 시장법의 세부 사항에 대한 합의를 이루고 법안 도입을 확정

주요 내용: 다른 플랫폼 정보도 동일하게 검색되게 함으로써 경쟁사에 대한 차별 금지, 인수합병 시 당국에 사전 신고 의무화, 혐오표현, 위조상품 판매 등 저지, 맞춤형 광고등 서비스 대한 정보 공개 요구

1. 디지털시장법(Digital Markets Act, 이하 “DMA”)

DMA는 일정조건 이상의 빅테크 기업들을 ‘게이트키퍼’로 규정짓고 규제대상에 포함한다. 시가 총액 750억 유로 또는 유럽경제지역내 매출이 연간 75억 유로 이상인 기업을 대상으로 한다. 이에 해당하는 기업으로는 구글, 마이크로소프트, 메타, 애플, 아마존 등이 있으며 알리바바, 부킹닷컴도 규제 대상에 포함

이를 위반할 시 해당 기업 글로벌 매출의 최대 10%를 과태료로 부과할 수 있고, 반복 위반시 EU내 플랫폼 운영 중단, 자산 매각 또는 기업 분할을 명령할 수 있음

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

DSA는 DMA와 함께 EU가 빅테크 기업들을 견제하기 위해 입법이 추진되어 유럽 연합의 행정부 격인 집행위원회가 2020년 12월 15일 법안 초안을 공개했다. 플랫폼 사업자 등을 대상으로 하는 광범위한 규제와 EU의 디지털 단일시장을 위한 규제강화는 2019. 12. 취임한 EU 집행위원장 Ursula von der Leyen의 주요한 정책목표 중 하나

주요 내용으로는 온라인 플랫폼 기업에 고객 보호 조치에 대한 더 큰 책임을 촉구하고 불법 콘텐츠에 대한 모니터링을 강화하는 것이 있다. 또한 알고리즘 편향성과 조작 가능성에 대한 논란으로 알고리즘 설계방법을 공개할 것을 요구하였고, 이용자가 알고리즘 추천 기능을 OFF할 수 있도록 하는 기능을 갖출 것을 요구하였다. 악용될 위험이 높은 민감한 개인정보를 활용한 타겟광고를 자제하였으며 특히 어린이 이용자에 대한 타겟광고를 전면 금지하였다. DSA 규제 대상은 DMA와 동일하며 과태료는 해당 기업의 글로벌 매출 6%까지 부과 가능

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

구분	조항	내용
수범자	Art. 2 Definitions (f), (h)	- 적용대상은 중개서비스업자, 온라인플랫폼업 그 리고 대규모 온라인플랫폼업으로 나뉘며, 중개 서비스업자는 단순전달(mere-conduit), 캐싱 (caching) 서비스 및 호스팅 서비스(hosting) 으로 구분
적용의무	Sec. 1 Provisions applicable to all providers of intermediary services	중개서비스업 및 (대규모) 온라인플랫폼업 공통 의무로서 - 규제부처와 전자적으로 연락 가능한연락창구 (Contact Point)를 구축(법 제11조) - 명확하고 쉽게 접근 가능한 이용조건 제시(약 관에 관한 의무: 법 제12조) - 투명성 보고 의무(법 제13조)
	Sec. 3 Additional provisions applicable to online platforms	SMEs 등 중소기업의 적용 배제(법 제16조) - 고충처리 및 분쟁해결 절차 확보 의무(법 제 17 · 18조) - 판매자 신원정보 확인 의무(법 제22조) - 광고의 투명성(법 제24조)
	Sec. 4 Additional obligations for very large online platforms to manage systemic risks	선정기준: 대규모 온라인플랫폼 업자는 EU내 월 평균 활동이용자 수가 4500만명 이상인 경우에 해당되며, 이 조건은 일정 시간 이후 EU 전체인 구의 10% 이내에서 조정이 가능 (법 제25조) - 제공하는 서비스의 위험성 평가 및 완화 의무 (법 제26 · 27조) - 추천 시스템 정보 제공 의무(법 제29조) - 온라인 광고의 추가 투명성(법 제30조)

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

(1) 불법 정보 대응 의무

모든 중개서비스는 규제 당국의 정보 삭제 명령에 대해 신속하게 대응하고, 그에 대한 보고를 신속하게 수행(제8조)

이러한 과정들의 신속성을 위한 연락담당자(point of contact)와 법률 대리인 마련(제10-11조)

호스팅 서비스를 제공하는 업체들은 이용자가 불법 정보로 여기는 콘텐츠를 쉽게 신고할 수 있는 메커니즘을 설치, 이에 대해 신속하고 구체적으로 대응하고, 조치 사항을 신고자에게 알려야 함(제14-15조)

플랫폼들은 플랫폼이 취한 조치에 대한 불만을 처리 할 수 있는 내부 시스템 마련(제17조)

분쟁이 내부적으로 조정되지 않는 경우, 규제 당국이 인증한 법정 외 조정 기구 이용 여건 마련(제18조)

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

(1) 불법 정보 대응 의무

개인 이용자뿐 아니라 시민단체 등에 의해 구성된 신뢰 기반 신고자(trusted flagger)의 감시와 신고에 협조할 의무 부과(제19조)

피해가 큰 범죄와 관련된 것으로 의심되는 콘텐츠에 대해 구체적인 정보를 당국에 보고할 의무(제21조)

대형 플랫폼들은 적어도 1년에 한 번 서비스의 기능이나 그 이용으로 인한 잠재적 위험에 대한 평가, 그로부터 파악된 ‘체계적 위험’에 상응하는 조치, 이와 관련한 EU 집행위원회와의 협의 또는 지도 (제26조, 제27조).

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

(2) 투명성 의무

중개서비스 전체에 부과된 기본 요건은 주로 불법 정보 처리의 사후적 보고(제13조), 사업자 분류에 따라 차등적으로 의무 부과

<온라인 플랫폼>

콘텐츠 관리(content moderation)조치에 대한 분쟁 조정 메커니즘에 관한 정보가 투명성 보고에 포함. 이용 정지 처분 수도 포함(제23-24조).

자동화된 콘텐츠 관리시스템의 스펙, 정확도에 관한 정보를 투명성 보고에 추가(제23조1항c호)

이용자가 개별 광고로부터 식별할 수 있는 추가적인 정보를 노출(해당 정보가 광고라는 사실, 광고주, 특히, 광고 추천을 위해 이용한 주요한 변수들에 대한 ‘의미 있는 정보’를 포함)(제24조).

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

(2) 투명성 의무

<대형 플랫폼>

추천시스템의 주요변수와 이용자가 이를 조작할 수 있는 방법에 대해 이용 약관에 분명하게 설명, 해당 기능을 쉽게 이용할 수 있는 방식으로 제공 및 개인정보에 기반하지 않은 대체 옵션이 적어도 하나 존재(제29조).

공중이 API를 통해 접근할 수 있는 정보 보관소(repository)를 운영, 개별 광고의 구체적 내용, 타겟팅한 이용자 그룹, 얼마나 많은 사람에게 해당 광고가 보여졌는지 등에 대해서 최소 1년간 공개(제30조)

매년 스스로의 비용으로 DSA에 대한 준수여부를 평가하기 위한 외부 감사 진행(제28조)

규제 당국과 인증된 연구자들이 DSA 준수 여부를 평가하는데 ‘필수적인’ 데이터에 대해 접근할 수 있도록 하는 조치(제31조)

2. 디지털서비스법(Digital Services Act, 이하 “DSA”)

(2) 투명성 의무

단순 전달	불법 정보 대응 의무	투명성 의무
중개 서비스 제공자	<ul style="list-style-type: none"> • 정보 삭제 명령에 대한 신속한 대응 • 연락담당자, 법적대리인 보유 	<ul style="list-style-type: none"> • 투명성 보고(수령한 명령 수, 불법정보에 대한 신고 수, 삭제에 대한 항의의 수, 콘텐츠 관리의 방식과 횟수 등)
호스팅 서비스 제공자	<ul style="list-style-type: none"> • 불법 정보 신고에 대응하는 메커니즘 	
소상공인 또는 소기업	<ul style="list-style-type: none"> • 대응에 대한 항의 처리 시스템 • 분쟁에 대한 국가에서 인증하는 중재 시스템 • 신뢰 기반 신고자에 대한 대응 메커니즘 • 특히 위험한 불법 정보에 대해서 국가에 신고 의무 	<ul style="list-style-type: none"> • 추가 투명성 보고 의무(분쟁 수, 이용 정지 처분, 콘텐츠 관리를 하나의 자동화된 수단에 대한 정보) • 광고 투명성
대규모 온라인 플랫폼	<ul style="list-style-type: none"> • 불법 정보로 인한 위험에 대한 주기적 위험 평가 • 평가된 위험을 감소시키기 위한 조치들 	<ul style="list-style-type: none"> • 주의 의무사항 수행에 대한 외부 감사 • 추천 알고리즘에 대한 공개 • 광고 투명성에 대한 추가 의무 • 정부의 평가와 연구를 위한 데이터 공개 의무

3. 유럽연합 일반 데이터 보호 규칙(General Data Protection Regulation, 이하 “GDPR”)

수년 간의 논의 끝에 GDPR이 2016년 6월 24일부터 제정

GDPR은 개인 정보 보호를 강화하기 위해 개인 정보 처리와 보호에 대한 책임을 지는 기업들에게 개인 정보의 처리 범위, 수집 방법, 저장기간 등을 명확히 규정

개인 데이터의 이전을 제한하고, 개인 데이터의 이전이 필요한 경우에는 **개인 정보 보호 수준이 동일한 국가로 한정**
개인 정보 처리에 대한 동의 원칙을 강화하고,

개인정보처리 전에 개인 정보 수집에 대한 동의를 받도록 규정

기업이 개인 정보 보호와 관련된 법적 책임을 지도록 규정

개인 정보 보호를 강화하고 개인 정보 처리에 대한 권리를 보호

이를 위해 개인 정보 처리에 대한 정보를 제공하고, 개인 정보 처리를 거부할 권리를 보호하고 있다.

4. 소결

유럽은 자국 데이터 주권에 대한 완고한 태도

페이스북, 인스타 등의 자국 점유율이 상당히 높은데도 불구하고 국내 철수에 관대한 입장을 표명

DMA를 통한 데이터 호환성 및 데이터 유동성 확보를 통해 빅테크 기업 없이도 자국 빅테크 산업의 진입장벽을 낮추려는 시도를 하고 있음

하지만 앞서 살펴본 바와 같이 DMA는 시장경쟁에서의 데이터 유통의 효율성을 증진시키는 수단으로의 기능이고 DSA와 같은 정보 제공자의 적극적 이용 수단은 아님

국외 글로벌 빅테크 기업의 완전한 배제 및 자국 내 산업을 육성하려는 움직임을 보이고 있으며

DMA에서 시가총액 750억 유로 이상이므로 MAGA만을 배제하려는 움직임이 확실하다고 볼 수 있음

더불어 DSA의 비대칭적 상호주의 의무는 빅테크 기업의 서비스를 이용하는 EU의 소비자들을 보호하는 기능을 할 수 있으며, 이에 더하여 현재 성장 중인 EU의 플랫폼 기업들은 상대적으로 가벼운 의무를 담당하여 규제의 부담을 덜 수 있도록 하고 있음

GDPR은 개인정보보호 정책을 바탕으로 미국 빅테크 기업, 나아가 미국 데이터 안보 위협을 견제하는 데 조력하고자 하는 의지

IV. 입법례 비교 및 분석

IV. 입법례 비교 - 1. 유럽

EU GDPR은 정보주체의 기본권과 자유를 보호하고 EU 회원국 전체에 **개인정보 보호**에 관하여 동일한 기준을 적용하기 위한 목적에서 제정

EU 전체의 차원에서 통일적인 법 적용을 가능하게 하고, 개인정보의 보호에 관한 단일한 규범으로써 **개인정보처리자**가 부담하는 규제 비용의 절감에 기여할 것으로 기대

현실의 기술 발전을 반영하는 정보주체의 권리를 강화하고 개인정보처리자가 준수하여야 할 사항을 명시함으로써 디지털 시대의 개인정보 보호 법제 방향을 선도하여 제시

IV. 입법례 비교 - 1. 유럽

<GDPR 5조 원칙>

구분	원칙	내용
1	적법성(lawfulness)·공정성(fairness) ·투명성(transparency)	개인정보는 적법·공정·투명하게 처리되어야 함
2	목적 제한(purpose limitation)	개인정보는 특정하고 명확하며 정당한 목적을 위해 수집되어야 함
3	최소 수집(data minimisation)	개인정보는 처리 목적에 필요한 것으로 제한되어 수집되어야 함
4	정확성(accuracy)	개인정보는 정확해야 하고, 필요한 경우 최신성을 유지해야 함
5	보관 제한(storage limitation)	개인정보는 처리 목적에 필요한 기간에 한해 보관되어야 함
6	무결성(integrity)과 비밀성(confidentiality)	개인정보는 기술적·관리적 조치 등 적절한 보안 하에 처리되어야 함

IV. 입법례 비교 - 1. 유럽

GDPR 주요내용

구분	조항	내용
1	제15조	<p>정보주체의 접근권(right of access by the data subject)</p> <ul style="list-style-type: none"> - 자신의 개인정보가 처리되고 있는지를 확인받을 권리 - 정보주체는 개인정보처리자가 자신의 개인정보를 처리하는 목적, 이용 대상이 된 개인정보, 개인정보가 저장될 예상 기간 등에 관한 정보에 접근할 수 있음
2	제16조	<p>정보주체의 정정권(right to rectification)</p> <ul style="list-style-type: none"> - 자신에 관하여 정확하지 않은 개인정보를 정정하여줄 것을 요청할 권리 - 정확하지 않은 개인정보의 처리로 인하여 정보주체의 정당한 권리 행사가 방해 받지 않도록 이를 지체 없이 정정하여줄 것을 요구할 수 있음
3	제17조	<p>정보주체의 '잊혀질 권리'(right to be forgotten)</p> <ul style="list-style-type: none"> - 개인정보처리자가 보유·관리하는 자신의 개인정보를 삭제하여줄 것을 요청할 권리 - 개인정보의 수집·처리 목적이 달성되어 더 이상 개인정보가 필요하지 않은 경우, 개인정보의 처리를 정하는 다른 법적 근거가 없는 가운데 정보주체가 개인 정보 처리에 관한 동의를 철회한 경우, 개인정보가 불법적으로 처리된 경우 등에 자신의 개인정보를 지체없이 삭제하여줄 것을 요구할 수 있음
4	제18조	<p>정보주체의 처리제한권(right to restriction of processing)</p> <ul style="list-style-type: none"> - 자신의 개인정보에 대한 처리를 차단·제한하여줄 것을 요청할 권리 - 정보주체가 법적 청구권을 설정·행사하거나 개인정보의 정확성 및 개인정보 처리의 불법 여부에 관한 다툼이 있는 때에 개인정보처리자의 개인정보 이용 및 삭제를 제한할 것을 요구할 수 있음

IV. 입법례 비교 - 1. 유럽

GDPR 주요내용

구분	조항	내용
5	제19조	<p>정보주체의 개인정보 이동권(right to data portability)</p> <ul style="list-style-type: none"> - 자신의 개인정보를 기계적으로 판독이 가능한 형식(machine-readable format)으로 제공하여줄 것을 요청할 권리 - 특히 정보주체는 자신의 개인정보를 제3의 개인정보처리자에게 기계적으로 판독 가능한 형식으로 제공하여줄 것을 요구할 권리를 지님
6	제20조	<p>정보주체의 반대권(right to object)</p> <ul style="list-style-type: none"> - 정보주체가 자신의 특별한 상황(particular situation)을 이유로 자신의 개인정보 처리를 반대할 수 있는 권리 - 정보주체가 반대권을 행사하는 경우 개인정보처리자가 개인정보 처리의 정당성을 입증하지 못하면 더 이상 개인정보를 처리할 수 있지 않음
7	제21조	<p>정보주체의 프로파일링을 포함한 자동화된 개별 의사결정에 관한 권리</p> <ul style="list-style-type: none"> - 정보주체는 자신에게 중대한 영향을 미치는 프로파일링(profiling)을 포함한 자동화된 의사결정에만 근거한 결정을 따르지 않을 수 있는 권리를 지님

IV. 입법례 비교 - 1. 유럽

GDPR은 우리나라의 개인정보 보호 관련 법제에서 직접 정하고 있지 않은 ‘개인정보 이동권’과 ‘자동화된 개별 의사결정에 관한 권리’를 정하고 있음

정보주체의 개인정보 이동권은 정보주체가 자신의 개인정보를 기계적으로 판독 가능한 형식으로 제공받을 권리와 정보주체가 지정하는 제3의 개인정보처리자에게 자신의 개인정보를 기계적으로 판독 가능한 형식으로 제공하여줄 것을 요청할 권리를 포함

정보주체는 서비스 제공자 선택권을 보장받아 특정한 개인정보처리자가 제공하는 서비스에 종속되지 않을 수 있음

개인정보 이동권이 보장됨으로써 정보주체는 특정 개인정보처리자에게 자신의 개인정보가 축적되었음을 이유로 다른 서비스로 변경하지 못하는 상황을 회피할 수 있으므로, 정보주체의 자기결정권이 강화

GDPR 제22조에서 정하는 자동화된 개별 의사결정에 관한 권리는 사람의 개입이 배제된 상태에서 오직 기계적으로만 개인정보가 처리되는 것을 방지하기 위한 것

GDPR 제4조제4호에서 자동화된 의사결정의 하나인 ‘프로파일링(profiling)’을 정의하고, 최근의 정보통신기술(ICT)과 이를 토대로 하는 각종 상업적 마케팅 기법의 발달 추세를 반영한 것

IV. 입법례 비교 - 2. 미국

캘리포니아주 프라이버시 권리법(The California Privacy Rights of 2020, “CPRA”)
2018년 제정된 캘리포니아소비자개인정보보호법(The California Privacy Act, CCPA)의 수정
버전

소비자의 권리와 기업의 의무를 강화하고 미국 최초의 개인정보보호 전달 집행기관 신설 내용을
포함

CPRA 적용 대상 기업으로는

- ①연 매출이 2,500만 달러 이상이거나
- ②소비자 개인정보를 10만 건 이상 보유하고 있거나
- ③개인정보 판매 및 공유에 따른 매출이 총 매출의 50% 이상을 차지하는 경우로 제한

<주요내용>

- ㉠ 새로운 원칙의 도입 및 개인정보보호 관련 개념의 확장
- ㉡ 소비자 권리 강화
- ㉢ 기업의 의무와 책임성 강화
- ㉣ 개인정보보호 감독기구 신설

IV. 입법례 비교 - 2. 미국

㉠ 새로운 원칙의 도입 및 개인정보보호 관련 개념의 확장

CPRA는 CCPA에서 언급되지 않았던 개인정보보호 원칙을 추가하고 '민감정보 (Sensitive Personal Information)와 동의 기준 (Consent Standard) 개념을 확대하여 적용

(데이터 최소화 원칙) CPRA는 그동안 중요한 원칙으로 회자되어왔던 데이터 최소화(data minimization)의 원칙을 미국 법령 최초로 명문화

(목적 제한 원칙) 소비자에게 통지하지 않고는 개인정보를 공시된 수집목적에 부합하지 않은 용도로 이용할 수 없도록 규정

(데이터 저장 제한) CCPA가 데이터 저장과 보유에 대한 원칙을 제시하지 않은 것과 달리, CPRA는 공시된 목적을 위해 "합리적으로 필요한" 기간보다 더 오랫동안 개인정보를 저장하는 것을 금지

(민감정보) 민감정보의 개념을 새롭게 도입하고 민감정보의 이용 및 공개를 제한함으로써 엄격하게 보호

(동의 기준) '동의(consent)'는 CCPA에서도 중요한 개념으로, CPRA는 동의가 "합의 의사를 나타내는(signifies agreement) "명확하고도 긍정적인 행위(clear affirmative action)"여야 한다는 점과 일명 "다크패턴"을 통해 동의를 확보할 수는 없다는 점을 강조

IV. 입법례 비교 - 2. 미국

㉔ 소비자 권리 강화

CPRA는 소비자의 권리를 추가로 더 보장하는 방식으로 정보주체의 권리 강화 추세를 반영

(정정 요구권) 소비자는 기업이 보유한 부정확한 개인정보에 대해 수정을 요청할 수 있는 권리를 보장받으며, 기업은 이러한 권리에 부응하여 부정확한 정보를 수정하도록 상업적으로 합당한 노력(commercially reasonable efforts)을 기울이도록 규정

(공유 거부권) 개인정보 '공유'란 소비자의 행태정보를 활용한 광고를 위해 사업자가 개인정보를 제3자에게 전송하거나 제공하는 것을 의미하며, 정보주체인 소비자는 이를 거부할 수 있는 권리를 보유

(자동화된 의사 결정 거부권) 프로파일링 등에 따른 자동화된 의사 결정의 결과로 고용이나 계약에 있어 차별을 당하지 않도록 이를 거부(옵트아웃)할 수 있는 권리를 보장

(정보주체의 대응 범위 확대) 비암호화된 개인정보는 물론 암호화된 개인정보에 대해서도 무단 열람, 유출, 도난 사고가 발생했을 경우 정보주체가 대응 행동에 나설 수 있도록 범위를 확대

IV. 입법례 비교 - 2. 미국

㊤ 기업의 의무와 책임성 강화

CPRA는 소비자의 권리 강화에 상응하는 기업의 의무와 책임을 강화

(계약의 의무) 기업이 소비자의 개인정보를 판매 또는 공개하기 위해서는 그러한 비즈니스 상대자(제3자, 서비스 제공업체, 도급 업체 등)와 개인정보 제공의 목적, 개인정보를 제공받는 자의 CPRA 준수 의무 등의 조건을 명시한 계약서를 작성하도록 의무화 한다.

(보안 의무) 기업이 개인정보의 특성에 적합한 합리적인 보안 절차 및 관행을 구현 하여 무단 또는 불법적인 접근, 파괴, 이용, 변형, 공개 행위로부터 개인 정보를 보호하도록 요구 (고위험 활동에 대한 개인정보영향평가 및 보안 감사) 개인정보 침해 위험이 높은 활동에 대해서는 개인정보영향평가와 정보보안 감사 (cybersecurity audits) 관련 규정을 발행하고 위험평가 결과는 신설 예정인 캘리 포니아주 개인정보보호 감독기구에 "정기적으로" 제출하도록 요구한다.

(CPRA 적용대상 기업 범위 조정) CCPA에서는 5만 건 이상의 개인정보를 보유한 기업에 대해 법률을 적용했으나 CPRA는 10만 건 이상의 소비자 개인정보를 보유 한 기업에 적용되도록 기준을 상향 조정함으로써 **소규모 사업자들은 CPRA의 적용 대상에서 제외한다.**

IV. 입법례 비교 - 2. 미국

㉔ 개인정보보호 감독기구 신설

CCPA는 캘리포니아주 개인정보보호 감독기구(CalPPA)를 신설하고 주 법무장관으로 부터 법집행 권한을 이전 받을 수 있는 근거를 마련

CalPPA는 미국 최초의 소비자 개인정보보호 법집행 전문 기관으로서 법률 위반 사안에 대한 조사, 행정처분, 규칙 공포 등의 권한을 확보한다.

사업자의 소비자 개인정보 처리 활동으로 인해 소비자의 프라이버시나 보안에 중대한 위협을 초래하는 경우 연간 사이버보안 감사를 실시하고 위험성 평가 결과를 제출하도록 관련 규칙을 제정하는 한편, 소비자 프라이버시에 관한 캘리포니아주의 보험 관련 법규를 검토하여 CPRA보다 강력한 개인정보보호를 보장하지 않는 경우 새로운 규칙을 제정하게 될 전망이다.

CalPPA 이사회는 5인으로 구성되며, 캘리포니아 주지사가 위원장을 포함한 2명을 지명하고 나머지 의석은 법무장관, 캘리포니아 상원 규칙위원회(California Senate Rules Committee), 캘리포니아 의회 의장(Speaker of the California Assembly)이 임명한다.

IV. 입법례 비교 - 2. 미국

연방개인정보보호법안(American Data Privacy and Protection Act, “ADPPA”)

연방 단위의 개인정보보호 일반법, 2022년에 발의, 회기 내 통과되지는 못함

<p>개인정보 처리원칙</p>	<p>데이터 최소화 원칙 명시 민감정보와 인터넷 검색 및 브라우징 내역의 수집, 처리 및 이전의 제한 상품 또는 서비스의 설계나 개발, 구현과 관련하여 프라이버시 위험을 식별하고 완화할 의무 부과</p>	<p>GDPR도 데이터 최소화의 원칙이 명시. GDPR은 원칙 준수에 대한 입증책임을 컨트롤러에게 부과</p>
<p>소비자의 권리</p>	<p>FTC에 ADPPA 설명자료를 작성하고 공개할 의무를 부과하고 있으며 사업체에는 개인정보처리방침의 작성·공개·개별통지, 간편고지의 의무를 부과. 소비자의 데이터 권한으로는 데이터를 열람, 정정, 삭제, 이전할 권리</p>	<p>GDPR에서는 자동화된 의사결정을 거부할 권리도 규정</p>
<p>기업 의무</p>	<p>동의 철회수단이나 맞춤형 광고의 거부, 옵트아웃 수단 제공 의무 등 부과</p>	
<p>법의 집행 및 적용</p>	<p>법의 집행 및 구제 절차 부분에서는 개인정보보호나 피해구제 관련 기구의 설치와 FTC의 권한, 타법과의 관계와 민사소송 관련 사항 규정</p>	

IV. 입법례 비교 - 2. 미국

연방개인정보보호법안(American Data Privacy and Protection Act, “ADPPA”)

ADPPA는 미국의 연방 단위 개인정보보호 관련 기본법으로, EU의 GDPR에 대응
데이터 최소화 원칙이나 개인정보 이전 요구권 규정, 데이터 및 사이버 보안 규정 등 비슷한
내용을 양측에서 확인

ADPPA에서는 **개인정보 국외 이전에 대한 제한 규정을 두고 있지 않음.**

GDPR의 경우에는 제5장에서 ‘**제3국 및 국제기구로의 개인정보 이전**’을 규정.

GDPR 제45조 제1항

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

IV. 입법례 비교 - 2. 미국

미국혁신경쟁법(UNITED STATES INNOVATION AND COMPETITION ACT)

「Endless Frontier Act」

중국으로의 기술유출 방지

중국 기업은 'Manufacturing USA Program'이나 'Manufacturing USA Network'에 가입이 제한
과학기술정책실장이 연방의 자금으로 개발된 지적 재산이 중국에 있거나 중국에 있는 외국 기업체와
제휴했거나 그 자회사인 회사에 의해 사용되는 범위를 검토하도록 함.

과학기술정책실장이 연방 기금으로 개발된 지적 재산이 외국 사업체나 중국기업체와 제휴했거나 그
자회사인 회사에 의해 사용되지 않도록 하는 권고안을 개발하도록 함.

「Strategic Competition Act」

중국으로부터의 국가안보 위협에 대처

홍콩이나 신장 위구르, 티벳과 중국 간의 갈등에 미국이 개입할 것임을 재확인, 동맹국과의 파트너십 강화를
통해 중국에 대응할 것을 규정

데이터 보안과 관련하여 지식재산 절도행위 및 미국에 설립된 기업들이 소유한 기술의 이전에 관여한
중국의 국유기업 목록을 발표

IV. 입법례 비교 - 2. 미국

미국혁신경쟁법(UNITED STATES INNOVATION AND COMPETITION ACT)

「Strategic Competition Act」

중국으로부터의 국가안보 위협에 대처

홍콩이나 신장 위구르, 티벳과 중국 간의 갈등에 미국이 개입할 것임을 재확인

동맹국과의 파트너십 강화를 통해 중국에 대응할 것을 규정

데이터 보안과 관련하여 지식재산 절도행위 및 미국에 설립된 기업들이 소유한 기술의 이전에 관여한 중국의 국유기업 목록을 발표

IV. 입법례 비교 - 2. 미국

미국혁신경쟁법(UNITED STATES INNOVATION AND COMPETITION ACT)

「Meeting the China Challenge Act」

중국의 시장교란 행위, 국가안보 위협 행위 관련 규정

영업기밀 탈취와 관련하여, 이를 통해 이득을 얻는 외국 주체들에게 자산 동결, 수출통제 명단(Entity List)

포함, 금융기관으로부터의 대출금지, 비자발급 중지 등의 제재를 부과

IV. 입법례 비교 - 2. 미국

미국혁신경쟁법(UNITED STATES INNOVATION AND COMPETITION ACT)

「Trade Act of 2021」

중국의 지식재산권 탈취나 디지털 검열, 관세회피 이슈에 대한 대응과 이로 인해 미국이 겪는 부작용을 최소화하기 위한 무역통상 개혁 내용을 입법화

미국 무역대표부(Office of the United States Trade Representative, “USTR”)가 국무부와 협력하여 호주, 캐나다, EU, 한국 등과 공동하여 지식재산권 탈취로 만들어진 제품을 수입금지하는 협상을 개시

USTR이 자국 내외의 검열 강제나 미 국민 데이터에 불법적으로 접근하는 외국의 정책, 법령, 행위를 파악.
요주의 국가'의 지정 및 연방관보 게재

IV. 입법례 비교 - 2. 미국

미국경쟁법

2022. 1. 25. 미국 하원에서 발의

미국의 국가경쟁력 강화와 중국견제

반도체 제도 인센티브, 연구 및 혁신, 안보와 금융, 자원 이슈를 다루는 위원회 등을 규정
정보 보호와 관련하여, 지적재산권을 위반한 우선관찰대상국의 상품 금지에 대해 규정

IV. 입법례 비교 - 2. 미국

해외정보이용합법화법(CLOUD ACT): 안전강화분쟁해결? 미정부 해외서버접근가능

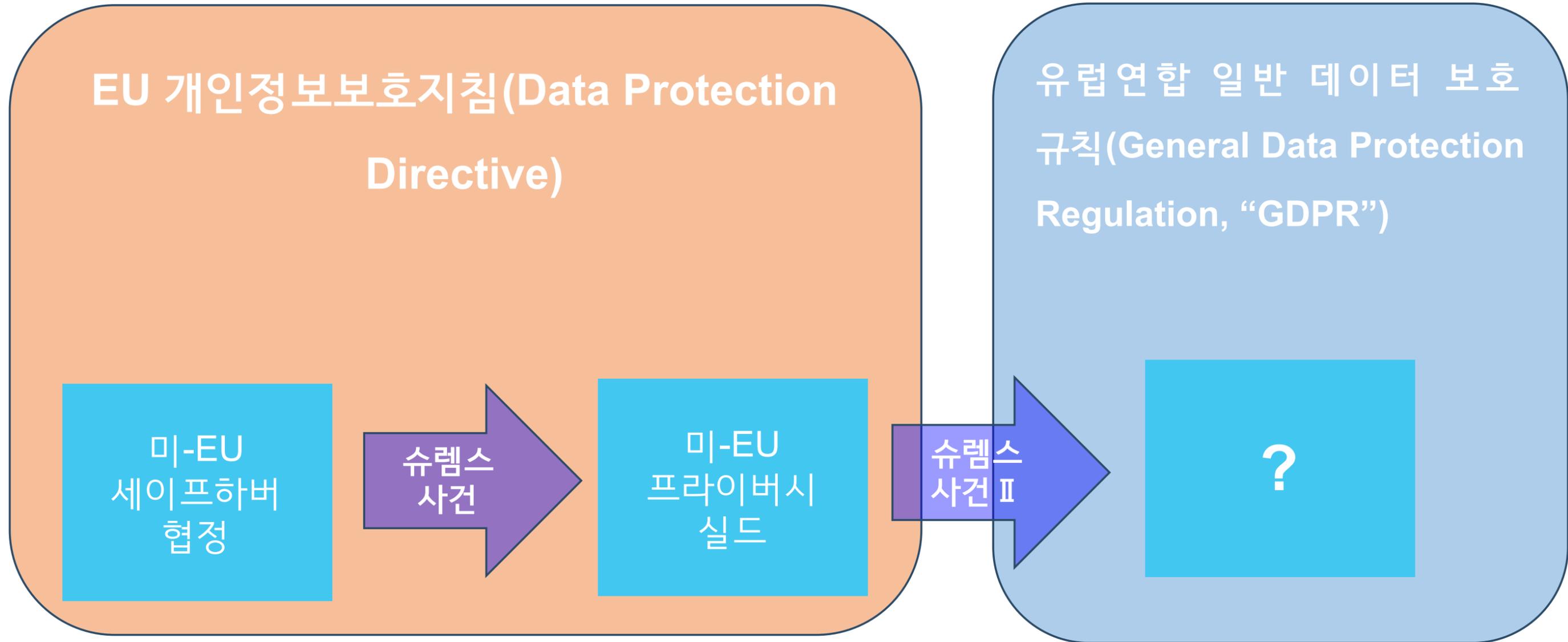
‘CLOUD’는 ‘Clarifying Lawful Overseas Use of Data’의 약어

미 정부에서 ‘해외에서의 데이터 이용 내역을 좀 더 명확하게 밝힐 수 있는 법적 여건 조성’을 위해 법안을 도입. 각종 데이터 확보를 용이하게 함으로써 국가 안전을 유지하고 각종 법률 분쟁을 수월하게 해결할수 있도록 하는 것을 목적으로 함

동법을 통해 미국 사법당국은 미국 기업이 해외 서버에 저장한 데이터에 접근할 수 있는 권한을 갖게 됨. 데이터의 소재지가 해외이더라도 미국에 본사를 둔 업체가 통제하는 데이터라면 복잡한 절차없이 열람 가능이 가능함. 예를 들어 구글, 아마존을 비롯한 각종 인터넷 서비스 업체들은 정부의 요청이 있을 시,

‘해외 국가의 Privacy Law와 무관하게 이를 제공해야 함.’

IV. 입법례 비교 - 3. 개인정보 국외 이전



V. 결론

V. 결론

미국: 기존에는 경쟁 및 소비자 보호의 측면에서 빅테크의 시장 실패를 중점으로 강경한 정부의 개입을 추진하였으나, 기술의 급진적 발전과 그 패권이 단순 경제 뿐 아니라 사회·정치 영역에도 큰 영향력을 미친다는 것을 재인식

->정책 기조를 자국의 빅테크 기업에 대한 규제에서 **중국 기업에 대한 규제**로 전환

+자국 내의 스타트업 시장 또한 성장을 추진하기 위하여 행정명령과 주법, 판례 등을 통해 다각적 발전을 도모

데이터유통 및 보안 관리 체계를 위한 국가적 지원체계 마련 및 점검

EU: 유럽의 경우 현재 글로벌 시장에서 큰 지위를 점한 빅테크 플랫폼을 겨냥: 기존 규제를 강화하거나 새로운 규제를 도입하는 등 더욱 박차를 가함

미국의 빅테크 플랫폼 견제 및 EU 내 플랫폼 성장 도모: 온라인플랫폼을 통한 혐오발언이나 허위정보의 확산 등 부작용 방지를 강조

DSA의 비대칭적 상당주의의무

우리나라: <새로운 규제에 대한 기준을 마련시 필수 고려 요소>

① '미국정부의 정보 및 데이터 관리체계에서의 선택과 집중적 체계의 인프라에 대한 벤치마킹 및 유럽 입법 및 입법안의 차등적 보상 및 책임분배 체계에서의 지원설계 및 시장 개척 및 접근성 발견, ② 개별 거래관계와 시장 구조적 관점에서의 동시적 접근, ③ 디지털 경제에서 기존 규범체계의 유효한 작동 여부 확인과 개선 방향, ④ 실체법 및 절차법적 차원의 병행적 대응 필요 등에 대한 고려

우리나라의 개정개인정보보호법, 마이데이터 산업 활성화 노력

플랫폼 산업 시대의 개인정보보호 중요성 + 데이터이동성통한 시장경쟁력

정보보호 수준 ->국가 간 정보 '통상'으로 연결

감사합니다

lawknp@police.ac.kr