2021년 제5호 (통권12호)

데이터산업 동향 이슈 브리프

# ISSUE BRIEF

2021.5

# 데이터 거버넌스 법적 프레임워크 국제 비교

Kdata 한국데이터산업진흥원

데이터산업 동향 이슈 브리프

C/O/N/T/E/N/T/S

## 데이터 거버넌스 법적 프레임워크 국제 비교


Ⅰ. 검토 배경 ····· 1

Ⅱ. 문헌 검토와 조사 분석 방법 ····· 2

1. 문헌 검토 ····· 2
2. 조사 분석 방법 ····· 3

Ⅲ. 분석 결과 ····· 6

1. 분석 내용 ····· 6
2. 주요 결과 ····· 8

Ⅳ. 결론 및 시사점 ····· 20

# 요 약


● 디지털 데이터가 기하급수적으로 증가하면서 데이터 및 개인데이터보호에 대한 관심이 높아지는 동시에 데이터 활용의 촉진 환경을 조성하는 데이터 거버넌스 문제가 주요 현안으로 대두

- 데이터를 적절히 활용하면 포괄적 경제 성장을 촉진하고 공공서비스 전달을 개선할 수 있음. 반면에 데이터 침해 및 개인의 권리 침해 가능성이 높아지면서 데이터 보호와 보안에 대한 우려도 증가해 각국 정부는 데이터 보호 및 보안 개선을 위해 다양한 접근 방식을 채택
- 그러나 국가별 데이터 거버넌스 규제 환경의 강건성(robustness)을 평가할 수 있는 기준점 역할을 할 데이터셋은 제한적
- 최근 세계은행이 발간한 글로벌 데이터 규제 진단* 보고서는 국가별 데이터 경제 규제 환경을 측정하기 위한 객관적이고 표준화된 지표 개발을 목적으로 함

  * World Bank, Mapping Data Governance Legal Frameworks Around the World : Findings from the Global Data Regulation Diagnostic, 2021.4

● 동 보고서에서 채택한 지표의 기본 구조는 "세계 개발 보고서 2021 : 더 나은 삶을 위한 데이터(이하 WDR21)"에서 제시된 '신뢰' 프레임워크를 따름

  * World Bank, World Development Report 2021: Data for Better Lives. 2021.3

- 이 프레임워크는 신뢰를 창출하고 데이터 기반 경제 개발을 촉진하는 법적이고 규범적인 '보호조치(safeguard)'와 '촉진조치(enabler)'라는 2가지를 식별
- 보호조치와 촉진조치에는 공식적인 법률과 여러 사회 규범이 모두 포함되어 있지만, 동 보고서에서는 조사대상 80개국의 공식적인 규제 환경만을 평가
- 보호조치 관련 하위 지표 4가지와 촉진조치 관련 하위 지표 3가지에 대해 총 37개의 세부 질문(붙임 참조)을 포함한 설문조사를 실시

● 조사 결과, 촉진조치와 보호조치를 비교해보면 전체적으로 촉진조치에 대한 모범 규제 사례 도입률이 보호조치보다 높게 나타남

- 조사 대상 국가는 촉진조치에 대해 측정된 모범 규제 사례의 47%를 도입했으며, 저소득 국가 30%, 고소득 국가 62% 도입

● 우리나라의 경우 데이터 거버넌스 수준으로 볼 때 다른 국가와 마찬가지로 촉진조치 측면이 보호조치보다 더 나은 양상을 보이고 있어 향후 보호조치 측면에 대한 보다 많은 고려가 필요

- 우리나라는 촉진조치의 경우 전체 4위인 데 비해 보호조치는 27위를 나타내 두 핵심지표 간 격차가 매우 큰 것으로 판단됨
- 특히 사이버보안/사이버범죄와 국가 간 데이터 이동 지표에서 각각 40위와 33위를 기록하고 있어 이에 대한 데이터 거버넌스가 선진 수준으로 나아가기 위해서는 보완과 검토가 필요

# PART Ⅰ 검토 배경

## 디지털 데이터가 기하급수적으로 증가하면서 데이터 및 개인데이터보호에 대한 관심이 높아지는 동시에 데이터 활용의 촉진 환경을 조성하는 데이터 거버넌스* 문제가 주요 현안으로 대두

* 본 보고서에서는 세계은행의 디지털비즈니스지표(Digital Business Indicator) 프로젝트에서 사용되고 있는 데이터 프라이버시와 보안을 데이터 거버넌스로 새롭게 명명

- 개인, 기업, 정부를 비롯한 경제주체의 디지털 데이터 및 데이터 활용이 급증
  - 개인은 일상생활에서 디지털 발자국을 남기고, 기업은 고객의 행동과 선호도에 대한 데이터 축적 및 활용을 통해 효율성 향상과 거래 촉진을 도모하며, 정부는 데이터 분석을 정책 결정에 통합하는 등 데이터 축적을 주도

- 데이터를 적절히 활용하면 포괄적 경제 성장을 촉진하고 공공서비스 전달을 개선할 수 있음. 반면에 데이터 침해 및 개인의 권리 침해 가능성이 높아지면서 데이터 보호와 보안에 대한 우려도 증가해 각국 정부는 데이터 보호 및 보안 개선을 위해 다양한 접근 방식을 채택
  - EU는 식별 가능한 데이터 주체의 권리를 강조하는 일반개인정보보호법(GDPR)을 채택했으며, 미국과 아시아태평양경제협력체(APEC)는 자발적인 민간 부문 표준에 의존하는 자유방임 또는 시장 중심의 접근 방식을 표방
  - 그러나 국가별 데이터 거버넌스 규제 환경의 강건성(robustness)을 평가할 수 있는 기준점 역할을 할 데이터셋은 제한적

## 최근 세계은행이 발간한 글로벌 데이터 규제 진단* 보고서는 국가별 데이터 경제 규제 환경을 측정하기 위한 객관적이고 표준화된 지표 개발을 목적으로 함

* World Bank, Mapping Data Governance Legal Frameworks Around the World : Findings from the Global Data Regulation Diagnostic, 2021.4

- 동 보고서에서 채택한 지표의 기본 구조는 "세계 개발 보고서 2021 : 더 나은 삶을 위한 데이터(이하 WDR21)"[1)]에서 제시된 '신뢰' 프레임워크를 따름
  - 이 프레임워크는 신뢰를 창출하고 데이터 기반 경제 개발을 촉진하는 법적이고 규범적인 '보호조치(safeguard)'와 '촉진조치(enabler)'라는 2가지 핵심지표를 식별

- 이 지표들은 국가가 데이터 경제의 '신뢰' 프레임워크를 구성하는 규제 요소 채택을 평가하는 진단 도구의 역할을 하는 것을 목표로 함
  - 또한 관련 규제 개혁을 시간의 경과에 따라 추적할 수 있는 기준을 형성하는 데에도 활용 가능
  - 규제 개혁 필요성을 파악하고 우선순위를 정하기 위한 첫 번째 단계는 모범 규제 사례와의 격차를 이해하는 것이며, 이는 데이터 경제의 위험을 방지하면서 이점을 따라잡아야 하는 신흥국에 특히 중요

1) World Bank, World Development Report 2021: Data for Better Lives. 2021.3

# PART Ⅱ 문헌 검토 및 조사 분석 방법

## 1 문헌 검토

- 온라인 상에서 데이터 기반 기술, 서비스 제공업체 및 기타 개인과 단체 간 신뢰를 어떻게 구축하느냐가 데이터 경제 활동 활성화에서 중요한 문제로 부상
  - OECD는 풍부한 데이터·초연결 디지털 환경에서 디지털 경제의 잠재력 활용이 경제·사회적 번영으로 이어지기 위해서는 신뢰가 필요하다고 지적[2)]
  - 새로운 데이터 기반 제품이나 서비스의 대량 유입과 가상 상호작용 환경은 기존의 신뢰 구축 방법에 대한 도전과제를 부여[3)]
    - 새롭게 부상하고 끊임없이 변화하는 데이터 기반 제품 또는 서비스에 대한 사전 지식 부족과 이러한 상품의 제공 기업에 대한 신빙성과 신뢰성을 평가하거나 검증하는 것이 어려움
- 데이터 경제의 신뢰 형성을 위해 데이터 규제가 중요한 역할을 담당
  - 규제는 데이터 관련 제품에 대한 법적 인정과 데이터의 사용 및 재사용 관련 규칙과 표준 설정을 통해 확실성을 제공하며 데이터의 사용 및 재사용을 촉진
  - 또한, 시장 참여자의 권리와 책임을 규정해 이들에게 제도화된 형태의 구제 수단을 제공

    ※ 예를 들어, 플랫폼 규칙에 대한 정부의 규제는 판매자 간의 규정 위반의 가능성을 줄이며[4)], 인터넷 거래의 법률과 규제는 기술에 대한 소비자의 태도에 영향을 줌[5)]
  - 신제도주의경제학에서는 데이터 규제가 데이터 경제의 신뢰 형성에 미치는 영향에 대해 거래비용 경감, 정보주체의 권리 보호, 시장 참가자의 신뢰 창출 등의 효과가 있다고 설명한 바 있음[6)]
    - 첫째, 데이터 컨트롤러* 또는 프로세서**의 책임을 명확하게 정의하는 데이터 규제는 고객을 대신하여 서비스 제공자를 심사하는 기능을 하여 거래 비용을 경감

      * 개인데이터의 처리 목적과 수단을 단독 또는 공동으로 결정하는 자연인, 법인, 공공기관, 에이전시, 기타 단체

      ** 컨트롤러를 대신해 개인데이터를 처리하는 자연인, 법인, 공공기관, 에이전시, 기타 단체

2) OECD, "Managing Digital Security and Privacy Risk.", 2016
3) O'Neill, Brian, "Trust in the Information Society." Computer Law & Security Review 28(5), 2012
4) Koo, Wesley Wu-Yi, "An Institutional Perspective on Platform Rules and Government Regulation." Academy of Management Annual Meeting Proceedings. Vol. 2019, No. 1., 2019
5) AlGhamdi, Rayed, Steve Drew, and Waleed AlGhaith, "Factors Influencing E-Commerce Adoption by Retailers in Saudi Arabia: A Qualitative Analysis." The Electronic Journal of Information Systems in Developing Countries 47 (1), 2011
6) North, Douglass C, "The New Institutional Economics." Journal of Institutional and Theoretical Economics (JITE)/Zeitschrift für die gesamte Staatswissenschaft 142 (1), 1986 ; North, Douglass C, Institutions, Institutional Change and Economic Performance. Cambridge: Cambridge University Press, 1990

- 둘째, 규제는 거래 당사자가 권리와 의무를 준수하도록 국가의 강제력을 행사하는 보호 조치를 통해 데이터 경제 활동에 대한 시민과 기업들의 참여 의욕과 신뢰를 제고
- 셋째, 비즈니스 거래에서 한 거래 당사자가 의도적으로 정보를 숨기거나 위조하는 등 정보 비대칭이 발생될 수 있는데, 활성화된 제도적 환경은 시장 참가자에게 신뢰를 주는 기초 및 안전망의 역할 수행

## 2 조사분석 방법

### (1) 조사 내용

▶ 보호조치와 촉진조치에는 공식적인 법률과 여러 사회 규범이 모두 포함되어 있지만, 동 보고서에서는 공식적인 규제 환경만을 평가

- 보호조치(Safeguard)란 데이터의 오용이나 데이터 침해를 방지함으로써 데이터 경제에 참여하는 개인이나 단체의 권리를 보호하는 것을 목적으로 하는 규범 및 법적 프레임워크
  - 데이터 컨트롤러 또는 데이터 프로세서에 적용되는 보안 요구 사항이 전형적 보호조치임
- 촉진조치(Enabler)는 데이터 이동성 메커니즘, 오픈데이터법 등 데이터의 사용 및 재사용을 촉진하는 규범과 법률을 의미

▶ WDR21에 따르면, 보호조치 및 촉진조치를 사용하는 법적 프레임워크는 다양한 데이터(개인, 비개인), 부문(공공, 민간), 거래 유형(국내, 국가 간)을 포함하는 다차원적 특성을 가져야 함

- 개인데이터(개인식별정보 등 개인이 직접 제공한 데이터)와 비개인데이터(개인식별정보를 포함하지 않는 데이터)는 민감도가 상이하므로 맞춤형 보호 장치가 필요
  - 국제법은 개인데이터 사용에 대한 반대, 불만 제기, 시정 요구 등에 대한 권리를 인정하며, 지적 재산권 보호는 비개인데이터를 보호
- 데이터가 공공 또는 민간 부문에서 생성·제어되는지 여부에 따라 촉진조치도 달라질 수 있음
  - 정부는 규제 또는 정책 개혁을 직접 도입하여 공공 데이터에 대한 접근 또는 사용을 의무화할 수 있지만, 민간 데이터의 경우 민간 주체의 자발적 데이터 공유를 촉진하는 인센티브 창출 및 장벽 제거로 역할이 제한됨
- 국내 및 국가 간 데이터 흐름 모두에 촉진조치 및 보호조치가 적용되지만, 국가 간 데이터 거래에서 수신 관할권에서 적절한 보호 및 거래 당사자의 책임을 보장하기 위해 특정한 규제 조항이 필요

▶ 본 조사는 80개국의 국내법, 규제, 행정 요건에 대한 상세한 평가를 기반으로 함

- 조사 대상 국가는 소득, 지역, 디지털 기술 개발 수준 등을 기준으로 고르게 분포되도록 선정했으며, 소득에 따라 고소득, 중상위소득, 중하위소득, 저소득으로 분류

**| 표 1 | 소득별 국가 그룹**

| 고소득 | 중상소득 | 중하소득 | 저소득 |
|---|---|---|---|
| 호주<br>캐나다<br>칠레<br>에스토니아<br>이스라엘<br>한국<br>모리셔스<br>오만<br>카타르<br>사우디 아라비아<br>싱가포르<br>UAE<br>영국<br>우루과이 등 | 아르헨티나<br>아르메니아<br>브라질<br>중국<br>콜롬비아<br>도미니카 공화국<br>가봉<br>조지아<br>인도네시아<br>이란<br>이라크<br>요르단<br>카자흐스탄<br>레바논<br>말레이시아<br>멕시코<br>페루<br>러시아 연방<br>남아공<br>태국<br>터키 등 | 앙골라<br>방글라데시<br>베냉<br>볼리비아<br>캄보디아<br>카메룬<br>코트디부아르<br>이집트<br>가나<br>온두라스<br>인도<br>케냐<br>키르기스스탄<br>라오스<br>몰도바<br>모로코<br>미얀마<br>네팔<br>니카라과<br>나이지리아<br>파키스탄<br>파푸아뉴기니<br>필리핀<br>세네갈<br>스리랑카 등 | 아프가니스탄<br>부르키나파소<br>콩고<br>에티오피아<br>감비아<br>아이티<br>라이베리아<br>마다가스카르<br>말라위<br>말리<br>르완다<br>시에라리온<br>타지키스탄<br>토고<br>우간다 등 |

- 보호조치 관련 하위 지표 4가지와 촉진조치 관련 하위 지표 3가지에 대해 총 37개의 세부 질문(붙임 참조)을 포함한 설문조사를 실시
  - 데이터 거버넌스 및 ICT 전문 변호사들이 표준 설문지를 작성했으며 2,000여 명의 관련 종사자에게 설문지를 보내 300건의 답변을 회수
  - 법 문서의 상세한 검토와 응답자와의 후속 질문을 통해 데이터를 추가 검증한 후, 세계은행그룹의 디지털 개발 글로벌 사무실 지역 담당자와 데이터 수집 결과 및 예비 조사 결과를 공유해 해당 국가에 대한 지식을 바탕으로 한 최종 검증을 수행

**| 표 2 | 핵심 지표 및 하위 지표**

| 핵심 지표 | 하위 지표(질문 수) |
|---|---|
| 보호조치 | ① 개인데이터 보호(12)<br>② 비개인데이터 보호(2)<br>③ 사이버보안 및 사이버범죄(4)<br>④ 국가 간 데이터 이동(3) |
| 촉진조치 | ⑤ 전자상거래(5)<br>⑥ 공공데이터(7)<br>⑦ 민간데이터(4) |

### (2) 산출 방법

- 각국의 데이터 거버넌스 수준을 정량적으로 분석하기 위해 하위 지표별 응답에 따라 점수를 계산
  - 모범 규제 사례의 도입 여부에 따라 0(아니다)과 1(그렇다)을 부여
    - 예를 들어, 전자상거래를 명시적으로 규율하는 법규가 있으면 1, 없으면 0을 할당
  - 객관식 설문의 경우 선택 문항 각각을 전체 선택 문항 수로 나누어서 계산
    - 예를 들어, 데이터 프로세서/컨트롤러에 대한 6가지 사이버보안 요구 사항에 대해 각각 1/6의 점수를 할당
- 위의 계산을 기초로 해당국($j$)의 지표별 수준($X_{ij}$)을 (식1)과 같은 방식으로 산출

$$X_{ij} = 100 * \left[ \frac{GP_{ij} - GPmin_i}{GPmax_i - GPmin_i} \right] \qquad \text{(식1)}$$

  - 여기에서 $GP_{ij}$는 국가 $j$가 지표 $i$에 대해 채택한 모범 규제 사례의 수이고, $GPmin_i$ 과 $GPmax_i$는 각각 지표 $i$에 대한 최소(항상 0) 및 최대 모범 규제 사례의 수를 의미
    - 위의 식에서 얻은 값을 0에서 100까지 정규화(normalize)
      ※ 100은 규제 프레임워크의 강건성에 있어 최고 점수이며 0은 최하 점수를 의미
  - 각각의 하위 지표에 대한 모든 질문의 비가중 평균(unweighted average)을 통해 해당 지표에 대한 점수를 산출하며, 모든 하위 지표의 비가중 평균을 통해 각각의 핵심 지표에 대한 점수를 산출
    - 그러나 각각의 지표에 대한 점수로 국가의 전체 점수를 산출하지는 않았는데, 그 이유는 이 진단의 목적이 국가 순위를 매기는 것이 아니라 각 규제 프레임워크에서 격차를 파악하는 것이기 때문

# PART Ⅲ 분석 결과

## 1 분석 내용

- 조사 대상 국가들은 보호조치와 촉진조치 점수에 따라 4개의 수준(선진-중간-점진적 발전(이하 발전)-기본)으로 구분
  - 75~100점은 선진, 50~75점은 중간, 25~50점 발전, 25점 미만은 기본 수준으로 분류
    - 보호조치와 촉진조치 점수는 해당 하위 지표별 질문 응답값($GP_{ij}$)의 비가중 산술평균임
- 보호조치의 경우 조사 대상 국가 중 에스토니아만 선진 수준으로 분류되고, 조사 대상 국가의 60% 이상이 기본과 발전 수준에 해당
  - 나이지리아, 몰도바, 베냉은 중하소득 국가 그룹 중 가장 높은 점수를 기록
    - 3개국 모두 개인데이터보호법을 갖고 있고, 사이버보안 위협을 식별, 조사, 해결하기 위한 인프라와 기관을 포함하는 사이버보안 전략을 채택하고 있음
  - 토고와 우간다는 저소득 국가 그룹 중 데이터 보호를 위한 적절한 수준의 규제 제도 제공

| 표 3 | 소득 그룹별 보호조치 수준 국가 수

| 소득/수준 | 선진(Advanced) | 보통(Moderate) | 발전(Evolving) | 기본(Basic) |
|---|---|---|---|---|
| 고소득 | 1 | 8 | 3 | 2 |
| 중상소득 | 0 | 6 | 8 | 7 |
| 중하소득 | 0 | 13 | 7 | 10 |
| 저소득 | 0 | 2 | 6 | 7 |
| 합계(80개국) | 1 | 29 | 24 | 26 |

- 촉진조치의 경우 고급 수준의 규제 제도를 갖고 있는 국가는 영국, 에스토니아, 멕시코, 한국 등 4개국이고, 조사 대상 국가의 절반 이상이 기본과 발전 수준에 해당
  - 선진 수준을 갖춘 4개국은 전자상거래, 공공데이터, 민간데이터에 대한 일련의 모범 규제 제도를 도입
    - 에스토니아의 'X-tee' 데이터 교환 플랫폼은 정부기관 간 시스템 상호운용성의 우수 사례
    - 멕시코는 개인데이터 이동권을 보장하여 개인이 서비스 또는 제품 공급자를 전환할 때 개인데이터를 원활하게 합법적으로 이동할 수 있도록 함
    - 한국에서는 개인이 온라인 디지털 ID 시스템으로 자신을 인증하여 정부의 서비스에 접근할 수 있으며, 민간 부문 서비스 제공자는 ID 시스템에 저장된 데이터를 바탕으로 개인의 신원을 확인하거나 인증 가능

- 부르키나파소는 저소득 그룹 국가 중 가장 높은 촉진조치 점수를 기록한 국가로, 공개데이터 정책을 도입했으며 개인에게 정부기록이나 데이터 접근을 요청할 수 있는 권리를 부여

**| 표 4 | 소득 그룹별 촉진조치 수준 국가 수**

| 소득/수준 | 선진(Advanced) | 보통(Moderate) | 발전(Evolving) | 기본(Basic) |
|---|---|---|---|---|
| 고소득 | 3 | 7 | 4 | 0 |
| 중상소득 | 1 | 11 | 8 | 1 |
| 중하소득 | 0 | 12 | 16 | 2 |
| 저소득 | 0 | 1 | 9 | 5 |
| 합계(80개국) | 4 | 31 | 37 | 8 |

**촉진조치와 보호조치를 비교해보면, 전체적으로 촉진조치에 대한 모범 규제 사례 도입률이 보호조치보다 높게 나타남**

- 조사 대상 국가는 촉진조치에 대해 측정된 모범 규제 사례의 47%를 도입했으며, 저소득 국가 30%, 고소득 국가 62% 도입
- 보호조치에 대한 모범 규제 도입률은 41%로 촉진조치보다 낮게 나타났는데, 고소득 및 중상위 소득 국가들의 상대적으로 부진한 성과에 기인
- 인도네시아, 태국, 탄자니아는 촉진조치에서 중간 수준의 적당한 환경을 갖고 있으나 보호조치는 기본 수준에 머물러 있음
  - 이들 국가는 포괄적인 전자상거래법을 갖고 있고, 오픈데이터법 등 공공데이터의 활용을 지원하는 규제가 실시되고 있지만, 개인데이터와 비개인데이터에 대한 보호조치는 부재
- 예외적으로 유럽, 중미, 사하라 이남 아프리카 지역은 촉진조치에 비해 보호조치 수준이 높음
  - 유럽 및 중앙아시아의 경우 모든 국가에 개인데이터의 사용, 수집 및 처리를 관리하는 데이터보호법이 존재
  - 대부분의 사하라 이남 아프리카 지역 국가가 공공데이터 활용을 위한 오픈라이선스 제도 미채택
  - 모리셔스도 공공데이터, 민간데이터의 사용/재사용을 지원하는 법률이 없었지만, '17년 국가데이터 보호법을 통해 사이버보안과 함께 개인데이터 보호 규제 제도 확립

**| 표 5 | 소득 그룹별 보호조치와 촉진조치 평균 수준**

| 보호조치 평균 점수 | | 촉진조치 평균 점수 | |
|---|---|---|---|
| 고소득 | 54 | 고소득 | 62 |
| 중상소득 | 40 | 중상소득 | 52 |
| 중하소득 | 40 | 중하소득 | 44 |
| 저소득 | 33 | 저소득 | 30 |
| 합계(80개국) | 41 | 합계(80개국) | 47 |

- 한편 국가별 촉진조치와 보호조치 수준 간에는 0.38 정도의 양의 상관관계를 보인다는 것이 특기할 만함
  - 이는 데이터 활성화에 대해 견조한 촉진조치 규제 환경을 도입한 국가는 데이터 보호를 위한 강력한 규제 환경을 가지고 있을 가능성이 높다는 것을 의미

## 2 주요 결과

### (1) 개요

- 고소득 그룹 국가들은 보호조치와 촉진조치 모두에서 평균적으로 높은 점수를 나타내나, 모든 하위 지표에서 선진 수준을 기록한 국가는 없음
  - 전자상거래 지표에서 모범 규제 사례 도입률이 평균 70%를 넘어 모든 소득 그룹에서 가장 높은 점수를 기록했으며, 공공데이터 및 사이버보안/사이버범죄가 그 뒤를 따름
    - 공공데이터와 사이버보안 및 사이버범죄의 규제 제도는 저소득 국가 그룹을 제외하고 대부분의 국가가 중간 수준을 기록
  - 민간데이터에서 모범 규제 사례 도입률은 평균 17%에 그쳤으며, 국가 간 데이터 이동, 민간데이터의 규제 제도는 모든 국가가 기본 또는 발전의 수준을 나타냄

**| 표 6 | 소득 그룹별 지표별 모범 규제 사례 도입률(%)**

| 소득\지표 | 보호조치 | | | | 촉진조치 | | |
|---|---|---|---|---|---|---|---|
| | 개인데이터 보호 | 비개인 데이터보호 | 사이버보안/ 사이버범죄 | 국가 간 데이터 이동 | 전자상거래 | 공공데이터 | 민간데이터 |
| 고소득 | 59 | 43 | 73 | 42 | 86 | 69 | 30 |
| 중상소득 | 46 | 29 | 57 | 30 | 74 | 62 | 20 |
| 중하소득 | 43 | 38 | 55 | 24 | 72 | 44 | 15 |
| 저소득 | 31 | 47 | 39 | 13 | 59 | 28 | 3 |
| 합계(80개국) | 44 | 38 | 56 | 27 | 73 | 50 | 17 |

- 7개 지표 전반에서 국가 점수 간 상관계수는 0.27이며, 2개 지표 간 상관계수는 -0.22에서 0.82까지 분포

※ 공공데이터-비개인데이터보호의 규제 제도 간 상관계수 -0.22, 개인데이터보호와 국가 간 데이터 이동의 규제 제도 간 상관계수 0.82

  - 2개 지표 간 상관계수가 통계적으로 유의미하고, 경우에 따라 실제로 크게 나타난다는 사실은 정부가 규제 프레임워크에서 특정 영역군을 동시에 해결하는 경향이 있다는 점을 시사
    - 국가 간 데이터 이동 허용의 규제 제도를 도입한 국가는 민간데이터 접근 허용(0.5573), 강력한 개인데이터 보호(0.8216), 사이버보안 규정(0.6087)을 구축할 가능성이 높음
    - 또한 전자상거래법을 제정한 국가에서는 공공 및 민간데이터 공유를 촉진할 가능성이 높아짐(각각 0.2979, 0.3496)

- 그러나 전자상거래와 개인데이터보호의 상관계수가 낮게 나타나(0.085) 전자상거래 촉진 제도를 갖춘 정부가 개인데이터보호제도를 도입하지 않는 것으로 해석됨
  - 예로 인도네시아의 경우 '08년 전자상거래법을 갖추었으나 개인데이터보호법은 부재
- 한편, 비개인데이터보호의 경우 다른 지표와의 낮은 상관관계 또는 부의 상관관계를 보여, 대부분의 국가가 이 영역에 대한 관심이 부족한 것을 시사

**| 표 7 | 지표별 규제 수준 점수 간 상관관계**

| | 전자상거래 | 공공데이터 | 민간데이터 | 개인데이터 보호 | 비개인 데이터보호 | 사이버보안/ 사이버범죄 | 국가 간 데이터 이동 |
|---|---|---|---|---|---|---|---|
| 전자상거래 | 1 | | | | | | |
| 공공데이터 | 0.2979* | 1 | | | | | |
| 민간데이터 | 0.3496* | 0.3998* | 1 | | | | |
| 개인데이터보호 | 0.0875 | 0.1736 | 0.4589* | 1 | | | |
| 비개인데이터보호 | -0.1046 | -0.2214* | -0.0853 | 0.1249 | 1 | | |
| 사이버보안/사이버범죄 | 0.2924* | 0.4031* | 0.6232* | 0.5423* | -0.1744 | 1 | |
| 국가 간 데이터 이동 | 0.1329 | 0.2458* | 0.5573* | 0.8216* | 0.0348 | 0.6087* | 1 |

주: * 5% 이상 수준에서 상관계수가 유의미함을 나타냄

## (2) 보호조치

### ① 개인데이터보호

**전체 조사 대상 국가의 58%가 포괄적인 데이터 보호법을 제정한 것으로 나타남**

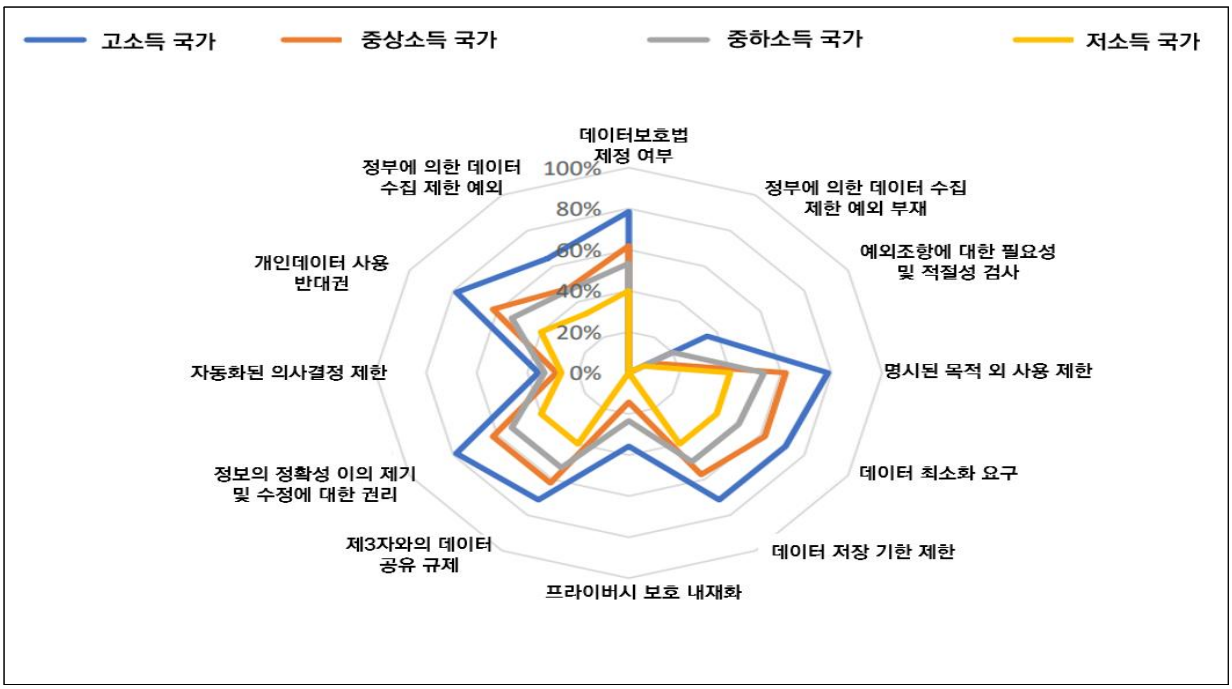
- 소득 그룹별로 보면, 저소득 국가의 40%, 중하 소득 국가의 53%, 중상 소득 국가의 62%, 고소득 국가의 80%가 포괄적 데이터보호법을 갖고 있음
- 포괄적 데이터보호법이 있는 모든 국가에서 정부의 데이터 수집과 처리를 제한하는 것에 예외조항을 두고 있으나, 그런 예외의 합법적 적용에 대한 필요성과 적절성 평가는 18%의 국가에서만 존재

**개인데이터보호법의 일부 조항에 대한 소득그룹별 성과는 높은 일관성을 보이나 실제 시행과는 잠재적인 격차가 나타남**

- 처리 목적 제한, 개인데이터의 정확성에 대한 이의 제기 등 개인 권리 조항은 고소득 국가 79%, 중상 소득 국가 62%, 중하 소득 국가 53%, 저소득 국가 40%에서 구비
  - 이는 국가가 개인데이터보호법을 도입할 때 이러한 모범 규제 사례들이 일반적으로 규제 프레임워크에 포함된다는 것을 의미
- 그러나 감독 기관을 갖춘 국가는 전체 조사 대상 국가의 47%로 전체 개인데이터보호법 도입률(58%)에 비해 낮았으며, 저소득국 그룹에서는 33% 수준에 그침

▶ 프라이버시 보호의 내재화와 자동화된 의사결정 부문은 개선의 여지가 많음

- 특정 IT 시스템 또는 비즈니스 관행에서 개인데이터 생애주기의 모든 단계에 걸쳐 개인데이터의 자동적인 보호를 지향하는 프라이버시 보호의 내재화의 경우, 전체 국가의 18%만이 도입
  - 고소득 국가(예 : 우루과이)는 36%, 중상소득 국가는 14%, 중하소득 국가는 23%의 도입률을 보임
- 다양한 데이터 경제 활동에서 프로파일링 관행이 증가함에 따라 자동화된 처리에 전적으로 의존하는 의사 결정을 제한하는 것이 중요한데, 전체 국가의 30%가 이와 관련한 규제를 도입한 것으로 보이며 소득 수준별 차이는 미미함
  - 프로파일링 등에 의한 자동화된 의사 결정은 데이터 컨트롤러의 효율성과 비용 절감을 촉진할 수 있지만, 데이터 주체에 대한 부당한 차별 등 심각한 악영향을 미칠 가능성이 높음




| 그림 1 | 소득그룹별 개인데이터보호 규제 제도 비율(%)

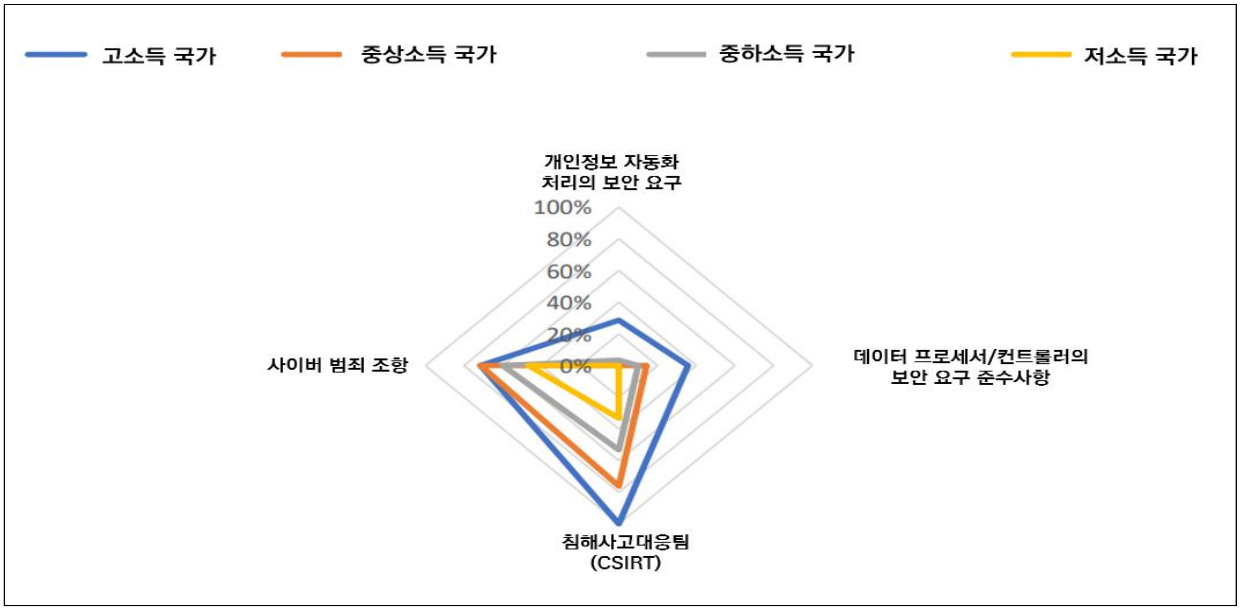
### ② 비개인데이터보호

▶ 조사 대상 국가의 다수가 지식재산권 사용을 통한 비개인데이터 공유 방지를 허용하지 않으며, 비개인 정부 데이터(예 : 공식통계의 기초가 되는 기업등록부, 기업 데이터)의 제3자 기밀 유지 조항을 포함하는 규제 프레임워크를 구축한 국가는 매우 적은 수준

- 조사 대상 국가의 70%가 지식재산권 사용을 통한 비개인데이터 공유 방지를 허용하지 않거나 이에 대한 특정 규정이 없고, 저소득 국가는 대부분 관련 법률이 전혀 없음
- 비개인 정부 데이터의 보호와 관련하여 캐나다를 비롯한 고소득 국가의 14%가 관련 규제 제도를 보유하고 있고, 대상국 전체로는 7% 수준이며, 저소득 국가 그룹에서는 규제되지 않음

### ③ 사이버보안 및 사이버범죄

- 사이버보안과 관련하여 고소득 국가의 29%에서 데이터 프로세서/컨트롤러가 자동화된 데이터 처리의 보안 요구사항을 준수해야 하는 것으로 나타남
  - 중하소득 국가 중 케냐는 이러한 보안 요구 사항이 있는 유일한 국가
    - 케냐의 경우 데이터 프로세서와 컨트롤러에게 개인데이터의 암호화 및 가명화, 물리적/기술적 사고 발생 시 개인데이터의 가용성 및 접근성 복원 등의 보안 요구사항 적용
  - 또한 사이버보안 표준 적용에 대한 설문에 대해 이러한 규제 제도가 있다고 응답한 국가는 저소득 국가에서는 없었고, 중하소득 국가의 10%, 중상소득 국가의 14%, 고소득 국가의 36%를 차지
  - 조사 대상국가의 66%가 사이버보안계획과 침해사고대응팀(CSIRT)을 갖추고 있는 것으로 나타나는데, 고소득 국가는 100%, 저소득 국가는 1/3 정도로 큰 격차가 존재
- 한편, 사이버범죄 조항은 조사 대상 국가의 62%가 갖고 있음
  - 저소득 국가의 이러한 조항 도입률은 47%인데, 예를 들어 르완다 ICT법('16년)은 데이터 무단 접근, 컴퓨터 서비스 차단, 컴퓨터 관련 도난, 사기 등의 사이버범죄를 다룸

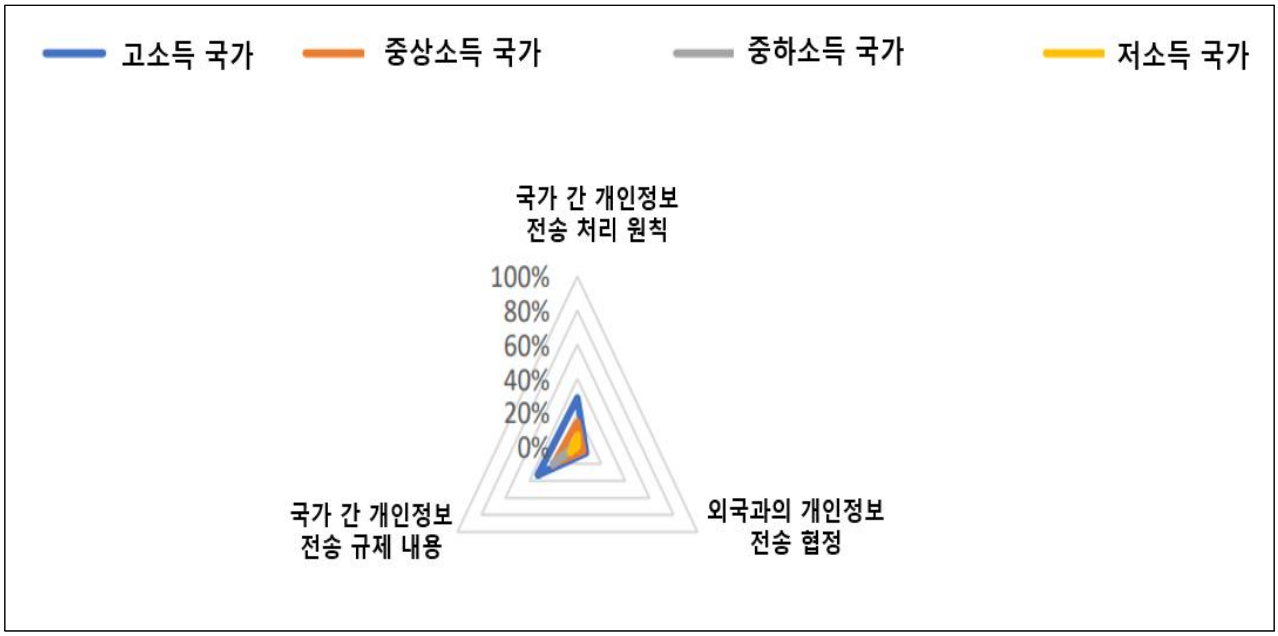



| 그림 2 | 소득그룹별 사이버보안 및 사이버범죄 규제 제도 비율(%)

### ④ 국가 간 데이터 이동

- 각국 정부는 적절성(adequacy)과 책임성(accountability)의 두 가지 접근방식을 통해 국외 데이터 전송을 규제
  - (적절성 접근 방식) 일반적으로 데이터 당국의 결정에 따라 유사한 데이터 보호조치를 보장하는 국가들에 대해 국제 데이터 전송을 허용하는 방식
  - (책임성 접근 방식) 국제 데이터 전송에 대해 어떤 내용의 보호조치를 실시할지 평가하고 결정하는 책임을 특정 조직에 부여하는 방식

- OECD 가이드라인[7]은 보다 유연한 책임성 접근방식을 권장하고 있는데, 이러한 관점에서 영감을 받은 규제 프레임워크는 책임성 접근방식을 채택
  - 조사 대상 국가의 거의 50%가 적절성 접근 방식을 채택하고 있고, 고소득 국가의 29%가 두 가지 방식을 모두 적용(중하소득 국가 7%, 저소득 국가 3%)
  - 예를 들어, 필리핀은 책임 접근법이고, 나이지리아, 러시아, 베트남은 개인데이터를 국내에서만 처리하도록 규정하며, 중국에서는 중요 인프라 사업자 정보를 국내에서만 처리하도록 함
- 고소득 국가의 7%, 중상소득 국가의 5%가 개인데이터의 국외 전송에 대한 협정에서 적절한 허용 목록, 구속력 있는 기업 규칙(BCR), 조약 등의 제도를 모두 갖춘 것으로 나타남
  - 상호인정 협정이나 조약의 경우는 보편적이어서 전체의 30%에 이름(예 : 필리핀과 싱가포르)
  - 고소득 국가의 1/3 정도가 국가 간 개인데이터의 전송과 관련하여 적절한 수준의 보호를 구성하는 모든 요소를 갖추고 있는 데 비해 저소득 국가는 거의 없음




| 그림 3 | 소득그룹별 국가간 데이터 이동 규제제도 비율(%)

### (3) 촉진조치

#### ① 전자상거래

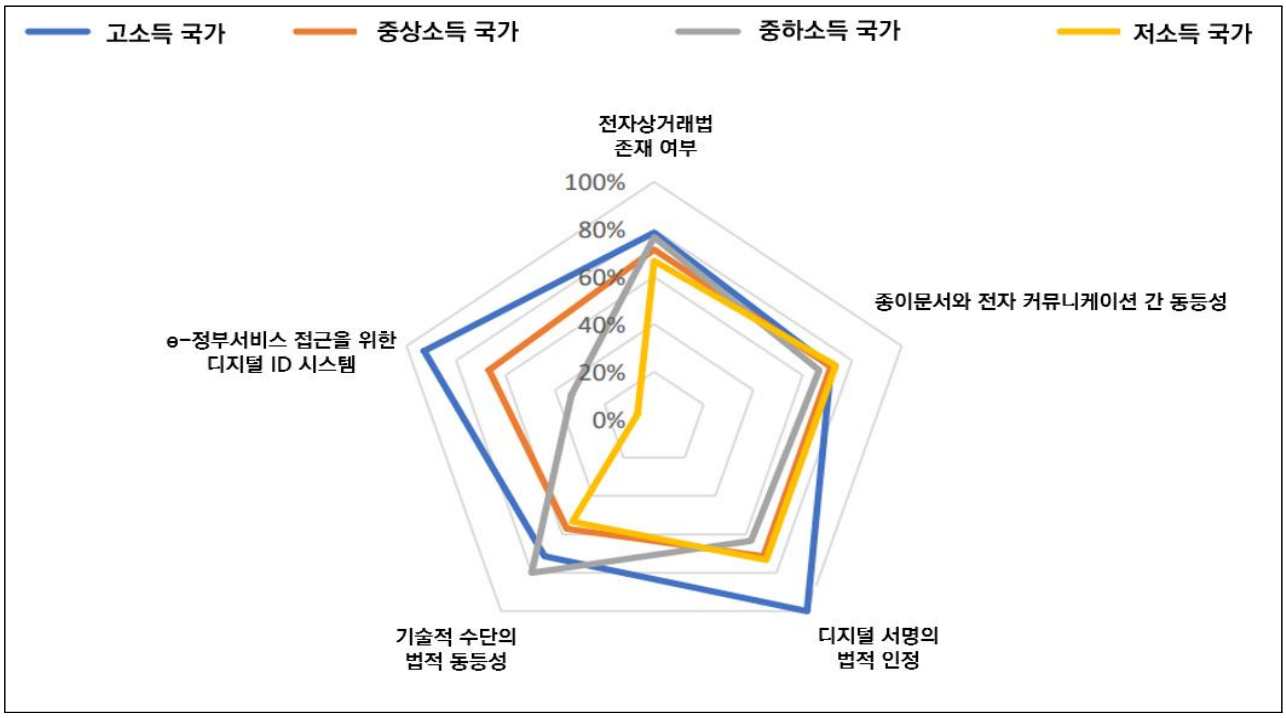
- 기술 중립 원칙 관련 규제는 전자상거래분야에서의 전자서명 및 전자통신에 필요한 기술에 대해 개방성을 보장하고, 특정 기술에 유리하거나 해당 기술의 지위를 강화하는요구사항을 부과하지 않고 혁신과 변화에 대응하도록 함
  - 기술중립성의 원칙에 대한 규제는 고소득 국가에서 71%, 중하소득 국가에서 80%가 실시되고

7) OECD, "Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data", 2013

있는 데 비해 저소득 국가에서 53%, 중상소득 국가에서 57%가 실시되고 있음

- 예를 들어, 우크라이나의 전자신뢰서비스법은 e-서비스의 기술중립성 규정을 도입

- 정부 서비스 접근을 위한 디지털 인증 시스템은 사용자를 디지털 기술 또는 생체 인식을 통해 고유하고 안전하게 확인할 수 있도록 함
  - 정부의 e-서비스에 접근하게 하는 디지털 ID 시스템은 민감데이터, 응용프로그램 및 e-서비스에 사용자가 효과적으로 접근할 수 있게 함으로써 형평성 증대 효과
  - 이 시스템의 도입 비율은 고소득 국가와 중상소득 국가에서 각각 93%와 62%이나, 중하소득 국가는 30%, 저소득 국가는 6% 수준임
    - 예를 들어, 싱가포르는 SignPass 디지털 ID 시스템을 통해 200개 이상의 정부 e-서비스 접근 가능




| 그림 4 | 소득그룹별 전자상거래 규제제도 비율(%)

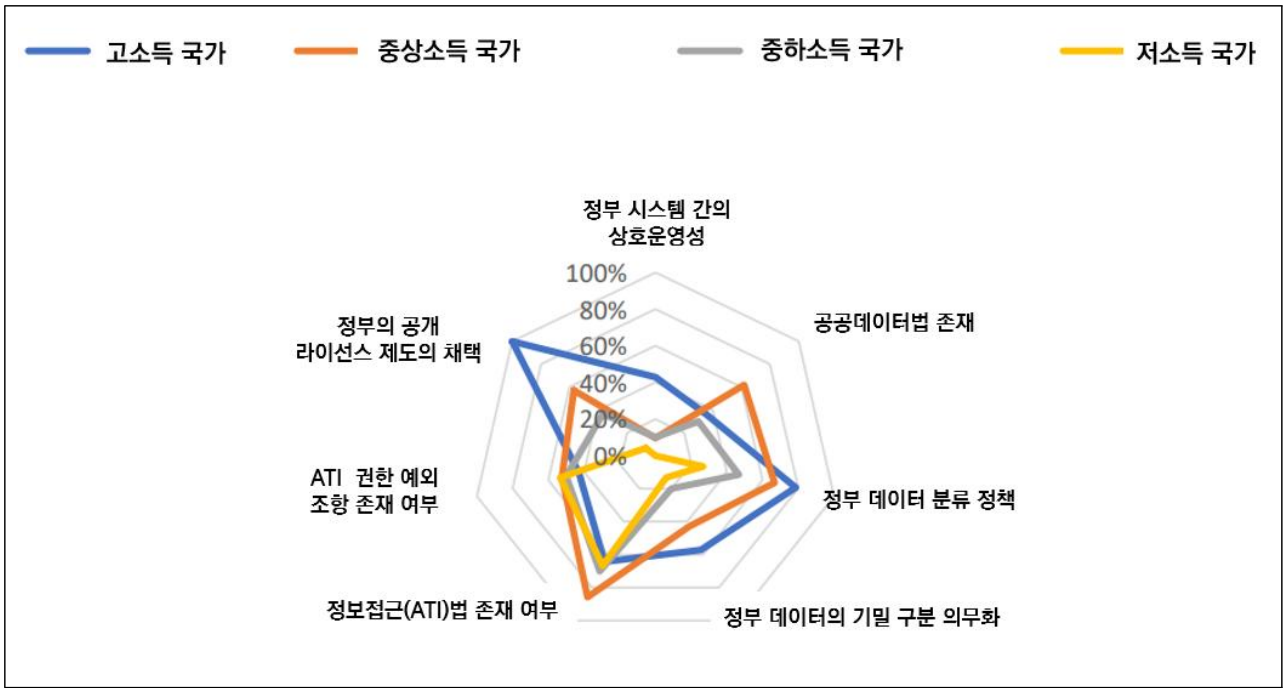
### ② 공공데이터

- 공공 부문의 정보 접근(ATI)법을 통한 정보 접근과 유통은 정보 및 표현 자유의 초석이자 유엔 지속가능목표의 하나로서 조사 대상국 70% 정도에서 채택하고 있음
  - 조사 대상 국가의 절반 정도가 ATI법에 정보 접근에 대한 예외 조항 포함

- 데이터 공개법은 정보의 공개에 대한 사전 책임을 설정하는 것으로 중상소득 국가의 60%에서 제정
  - 이 법의 대표적 사례는 한국의 공공기관의 정보공개에 관한 법률(약칭 정보공개법)[8]임

8) 공공기관이 보유·관리하는 정보에 대한 국민의 공개청구 및 공공기관의 공개의무에 관하여 필요한 사항을 정한 법률(1996.12.31. 제정, 1998.1.1. 시행)

- 데이터 공개와 관련하여 저작권자가 특별한 조건을 설정해 이용을 허용하는 크리에이티브 커먼즈 라이선스 제도의 경우 소득별 국가 그룹 간에 차이가 크게 나타남
  - 모든 고소득 국가에서는 이러한 오픈 라이선스 제도를 도입했고, 중상소득 국가는 57%, 중하소득 국가는 37%이며, 저소득 국가는 7%로 매우 낮은 수준임
- 공공데이터의 사용을 용이하게 하기 위해서는 정부기관 간 데이터 시스템의 상호운용성이 필수 요건
  - 사우디아라비아의 'Yesser' 전자정부 프로그램은 사람들이 전자정부 포털 서비스(Gov.sa)에 접근할 수 있도록 하는 상호운용 가능한 데이터 교환 플랫폼의 모범 사례
  - 이러한 플랫폼은 고소득 국가의 43%가 채택하고 있는 데 비해 중상소득 국가와 중하 소득 국가의 경우 10%가 채택했으며, 저소득 국가에는 부재
- 정부의 민감데이터(개인데이터 및 국가안보 관련 데이터)는 데이터 공개법을 통한 공개에 적합하지 않을 수 있기 때문에 데이터 기밀 분류 정책을 통해 공개에 따른 위험에 대한 사전 평가가 필요
  - 데이터 생애주기 전반에 걸쳐 다양한 수준의 기밀성을 고려하여 데이터를 분류함으로써 효과적이고 안전한 데이터의 사용이 이루어지도록 해야 함
  - 데이터 기밀 분류 정책은 저소득 국가의 26%, 고소득 국가의 78%가 도입했으며, 저소득 국가의 13%, 중하소득 국가의 20%, 중상소득 국가의 42%, 고소득 국가의 57%에서 의무화




| 그림 5 | 소득그룹별 공공데이터 규제제도 비율(%)

### ③ 민간데이터

- 민간데이터의 이동성 보장은 그 데이터의 사용을 용이하게 함으로써 기업 간의 경쟁을 강화하면서

사용자가 자신의 데이터를 제어할 수 있도록 하는 이중 효과 제공

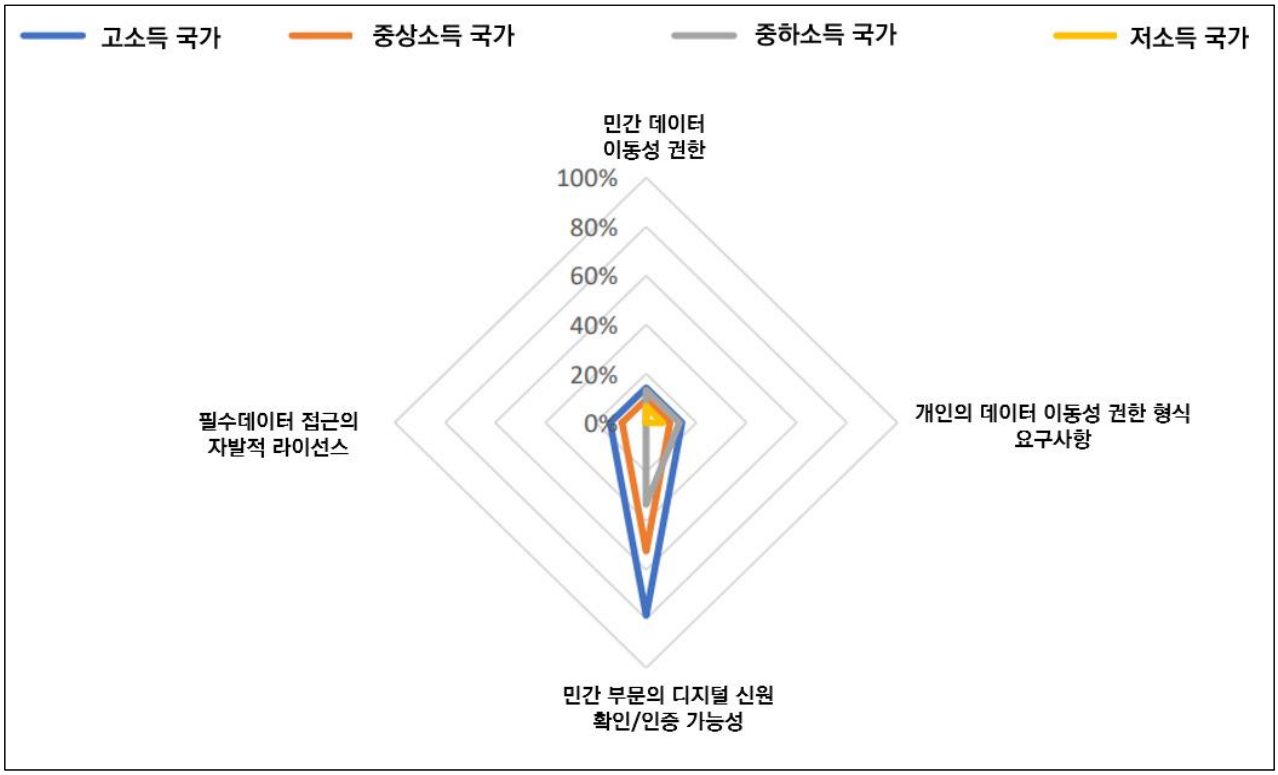
- 소비자 행동 데이터 등의 민간 데이터 활용은 비즈니스 성장, 생산성 향상, 혁신의 원천
- 이러한 민간 데이터 이동성 권한은 조사 대상국의 10%가 채택했고, 소득 그룹별로는 고소득과 중하소득 국가는 14%, 중상소득 국가는 9%, 저소득 국가는 6%로 나타남

▶ 특허 등의 민간데이터 활용과 관련하여 자발적 라이선스는 기술공유를 통한 혁신과 경제 성장을 촉진하는 효과가 있기 때문에 표준 설정기관이 표준 필수 특허에 대해 이러한 자발적 라이선스를 요구하는 경우가 있음

- 고소득 국가와 중상소득 국가에서는 각각 14%와 9%가 이러한 표준 필수 특허 접근에 대한 자발적 라이선스 제도를 도입한 데 비해 중하소득 국가와 저소득 국가에서는 부재

▶ 민간데이터의 온라인 인증은 효율적인 디지털 거래를 위해 필수적인데, 고소득 국가의 경우 79% 이상이 도입했고, 중상소득 국가의 경우 절반에 이르는 데 반해, 저소득 국가에서는 미적용

- 캐나다 SecureKey 기술은 민간 기업이 온라인 인증을 통해 사용자를 디지털로 식별하는 대표적 사례




| 그림 6 | 소득그룹별 민간데이터 규제제도 비율(%)

### (4) 법의 존재와 강건성 및 데이터 거버넌스 관리 수준

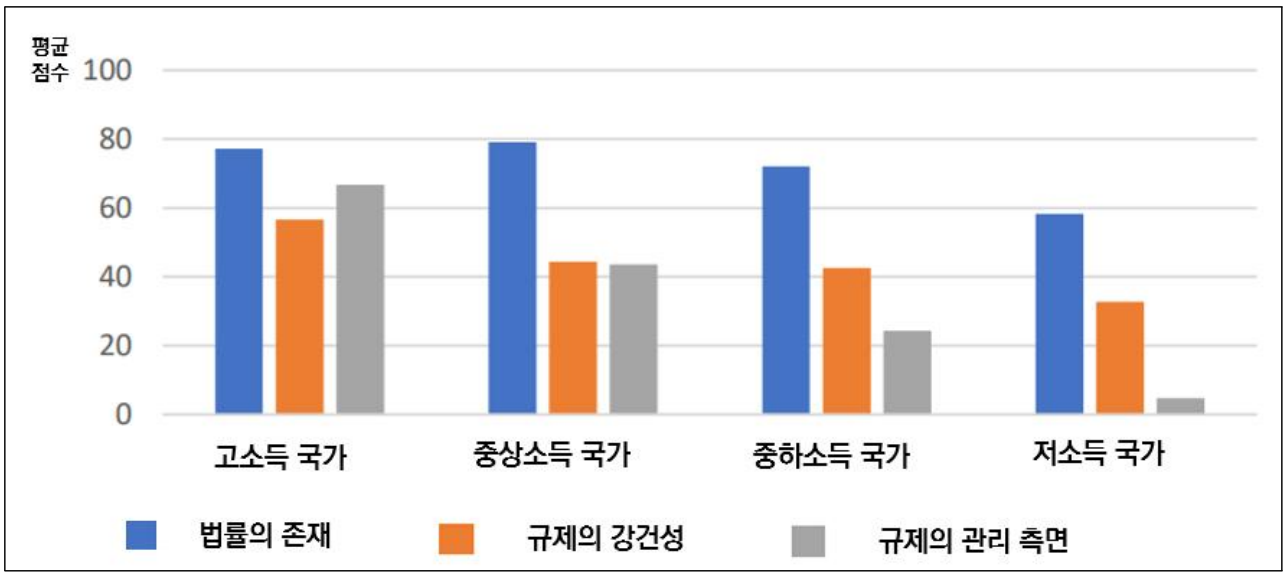
▶ 기존의 관련 조사연구(UNCTAD의 e-거래 데이터베이스, 로펌회사 DLA Piper의 데이터보호법 조사 등)와

달리 동 보고서의 조사는 규제 자체의 존재만이 아니라 규제의 특성 및 실행의 강건성을 파악

- 조사분석 결과, 저소득 국가는 e-서비스를 위한 디지털 ID 시스템의 존재, 정부기관 시스템의 상호운용성을 확보하기 위한 공통 기술 표준의 사용 의무 등과 같은 강력한 데이터 거버넌스를 가능하게 하는 기술 인프라 또는 제도 설정에서 취약함
- 이에 비해 고소득 국가는 일부 법률이 모든 영역에서 바람직한 규제를 포함할 정도로 견고하지는 않더라도 데이터 거버넌스 관리 면에서 높은 수준을 보임

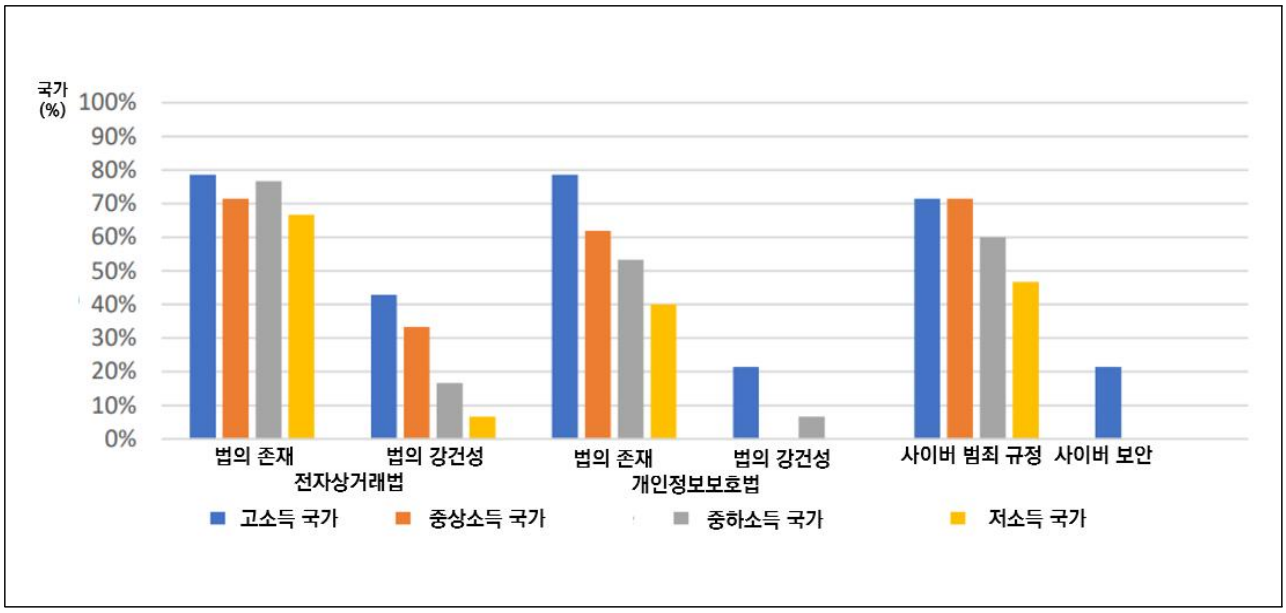
법의 존재와 강건성 격차는 개인데이터보호법과 사이버보안 및 사이버범죄를 통해 잘 드러남

- 중상소득 국가의 60% 이상이 개인데이터보호에 관한 법률을 갖추고 있으나 실행과 관련된 모든 규제 제도를 채택하고 있는 나라는 없음
- 또한 조사 대상 국가의 60% 이상이 사이버범죄를 규제하기 위한 포괄적인 규정을 채택하고 있지만 전반적인 사이버보안 규제는 미흡한 것으로 나타남
  - 다만 고소득 국가의 일부 국가(예 : 영국)가 개인데이터의 자동화된 처리를 위한 보안 요구 사항, 데이터 프로세서/컨트롤러에 대한 사이버보안 요구, 사이버보안 위협의 식별, 조사, 해결을 위한 사이버보안 전략, 인프라 및 기관 구축 등 모든 영역의 규제 제도를 운영




| 그림 7 | 소득 그룹별 데이터 거버넌스 요소 점수

주 : 관리적 측면은 e-서비스를 위한 ▲디지털 ID 시스템 ▲정부기관 시스템 간의 상호운용성 확보를 위한 공통 기술 표준의 사용 의무 ▲정부 시스템 전체의 데이터 기밀 분류 의무화 ▲오픈 라이선스 제도 도입 ▲민간 부문의 디지털 ID 확인/인증 ▲공정·합리·비차별적 원칙(FRAND basis)을 기반으로 한 필수 데이터에 대한 접근의 자발적 라이선스 의무화 등의 존재 여부를 포함. 규제 프레임워크의 강건성은 글로벌 데이터 규제 진단에서 측정된 모든 규제 속성의 평균 점수에 기초(관리적 측면 및 전자상거래법, 개인데이터보호법, ATI법, 오픈데이터법 또는 정책, 사이버범죄 조항에 대한 질문을 제외)




| 그림 8 | 주요 규제 지표에 대한 법의 존재 여부와 강건성 점수

### (5) 타 지표와의 비교

- 동 보고서에서 조사분석한 데이터 거버넌스의 수준과 기존에 세계은행이 작성한 세계 거버넌스 지표(WGI, World Governance Indicator, 2020)와의 비교를 통해 유사한 지표 간에 높은 상관관계를 나타내는 것을 확인

  - 동 보고서와 관련하여 WGI의 지표 중 규제의 품질과 여론 반영 지표와 비교
    - WGI의 규제 품질 지표는 정부가 민간 부문의 개발을 허용하고 촉진하는 건전한 정책 및 규제 구축과 시행 능력을 반영하는 것으로, 동 보고서의 보호조치와 0.45, 촉진조치와 0.60의 상관관계를 나타냄
    - WGI의 여론 반영 지표는 정부 결정에 대한 시민 참여 범위와 표현, 결사, 언론의 자유를 반영하는 것으로서 동 보고서의 보호조치와 0.45, 촉진조치와 0.50의 상관관계를 나타냄

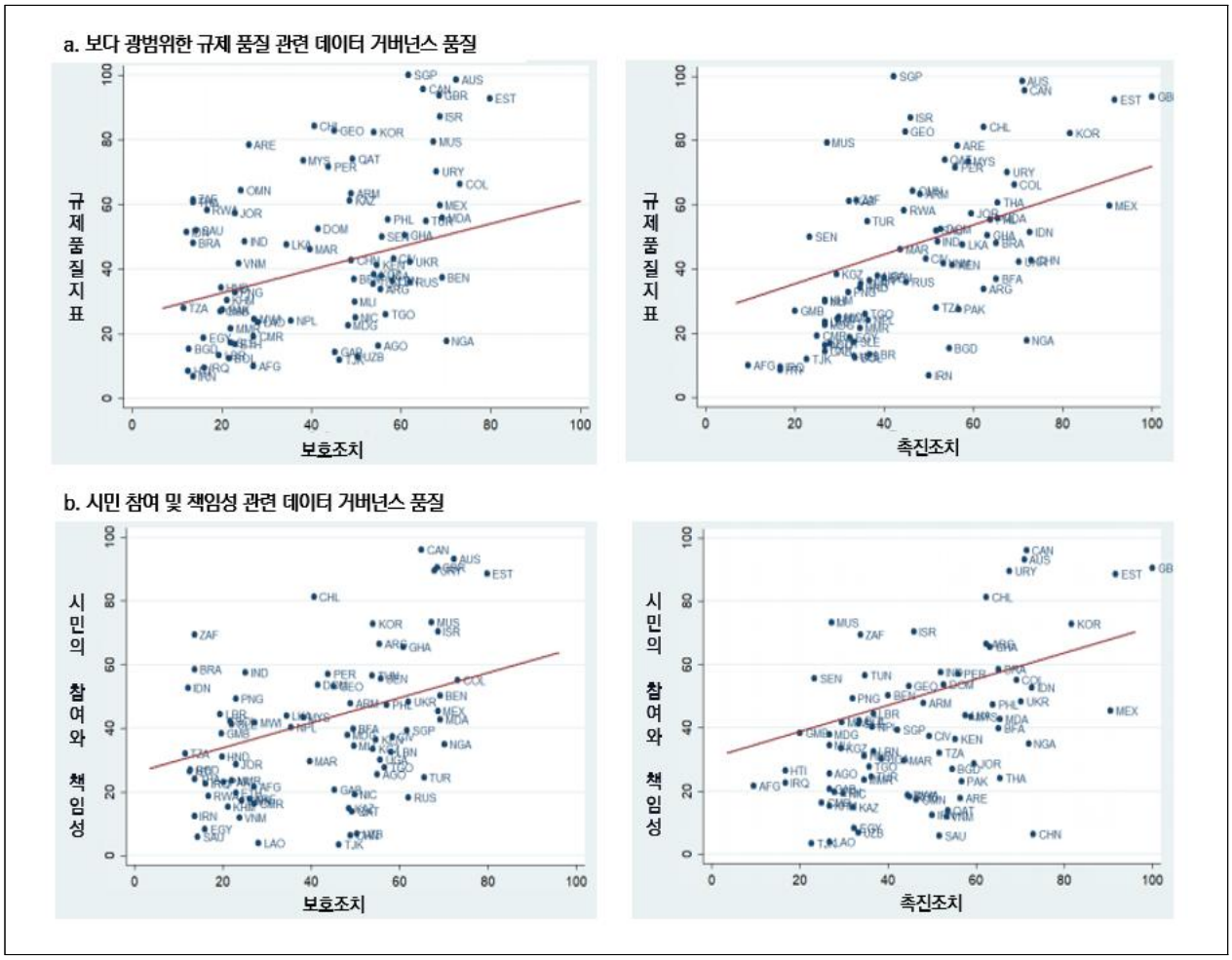
- 이러한 높은 정의 상관관계는 비교적 합당한 규제 문화를 가진 나라가 데이터를 포함한 다양한 분야에서도 그에 맞는 규제 제도를 갖고 있다는 것을 의미

  - 촉진조치의 모범 규제 사례가 증가하면, 공공·대민서비스 및 이들의 독립성 등 다양한 정부 기능 및 기관에 대한 신뢰가 증대
    - 이는 특히 정부의 효율성을 개선하기 위한 오픈데이터의 사용/재사용 촉진을 목적으로 하는 공공데이터 지표와 관련이 높을 것임
  - 또한 데이터 거버넌스를 위한 보다 강력한 규제 프레임워크는 시민들이 여론 및 책임성에 있어 더 많은 권한을 부여받는 것으로 체감하는 국가와 상관관계가 높음

- 서로 다른 관점에서 접근한 지표들간의 높은 양의 상관관계는 데이터 규제 프레임워크가 보다 광범위한

국가 거버넌스 프레임워크와 분리될 수 없다는 것을 의미

- 즉, 보다 광범위한 규제 환경에 대해 보다 높은 수준의 신뢰를 보이는 국가들에서 데이터 규제에 대한 점수가 더 높게 나타난다는 것을 의미
  - WGI는 데이터 경제에 대한 대중의 신뢰를 직접 측정하는 것이 아니라 거버넌스 환경에 대한 대중의 신뢰를 측정하는 것에 유의해야 함




| 그림 9 | 데이터 거버넌스 및 보다 광범위한 거버넌스 특성의 품질 간 상관관계

## (6) 코로나19와의 관련성

- 코로나19를 계기로 많은 정부가 바이러스 확산 방지를 위한 데이터 기반 솔루션을 모색하고 있기 때문에 그 어느 때보다 강력한 데이터 거버넌스 환경의 중요성이 부각
  - 예를 들어, 접촉자 추적은 공공기관이나 앱 개발자 등의 민간부문에 의한 개인데이터 수집과 처리에 크게 의존하게 됨
    - 이러한 활동의 증가로 인해 데이터 보호와 사이버보안 문제가 크게 부각되고 있으며, 개인의 권리를 보호하면서 공중보건 목적의 데이터 사용을 위한 투명하고 일관성 있는 규칙과 규제가 필요
- 동 보고서의 연구팀은 조사 대상국의 코로나19 긴급 규제 제도의 도입 상황을 조사하여 그것이

데이터 보호조치의 추가나 기존 보호조치의 억제로 이어졌는지를 평가

- 조사대상국 중 15개국이 데이터 보호에 영향을 미치는 긴급 규정을 채택한 것으로 나타남
  - 이 중 9개국(아르메니아, 코트디부아르, 이스라엘, 한국, 마다가스카르, 모리셔스, 모로코, 페루, 영국)은 기존에 데이터보호법이 있었고, 나머지 6개국(브라질, 중국, 인도네시아, 이란, 요르단, 파푸아뉴기니)에는 없었음
  - 기존에 개인데이터보호법이 있었던 국가에서는 일반적으로 공공기관이나 민간기관이 공공 안전 유지를 위해 개인데이터를 수집할 수 있는 법적 근거와 조건을 명시하는 조항을 포함하고 있었음

▶ 데이터보호법이 도입된 국가의 20%가 개인데이터 수집을 통한 코로나19의 확산 억제를 위한 긴급 규정을 채택('20.6.1일 기준)

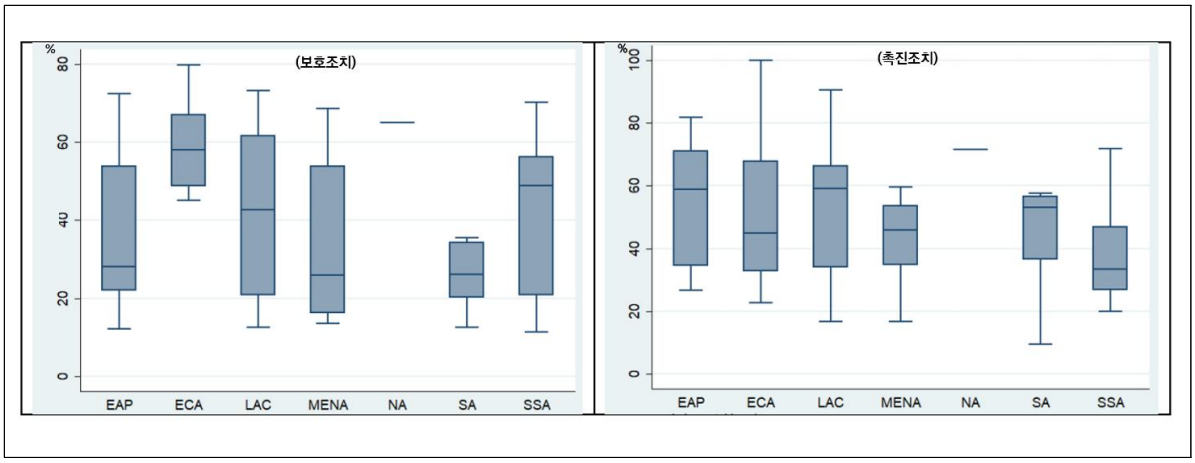
- 이들 어느 국가에서도 이러한 규정을 통해 전염병 퇴치를 구실로 데이터 주체가 갖는 기존의 권리를 억제하지 않았음
- 모리셔스의 경우 기존 '17년에 제정된 데이터보호법의 개정을 포함한 긴급 규제를 채택('20.5)
  - 여기에는 법 적용의 예외에 대한 적절성 및 필요성, 코로나19 기간 동안에 오픈 라이선스 허가 또는 승인 발행 조항이 포함
- 이스라엘도 이와 유사한 긴급조치를 선언하고, 국가보안기관인 샤박(Shabak)에 접촉자 추적 권한을 부여
  - 이 조치는 우려를 야기했지만 이스라엘 대법원은 이 조치가 데이터 최소화 원칙을 준수했고 비상사태 동안의 데이터 처리가 전염병 방지를 위해 필요한 영역에 제한되었다고 판결

▶ 데이터보호법이 없는 국가의 18%는 개인데이터 수집에 대한 개인의 권리에 대한 긴급 규정을 공포

- 그러한 긴급규정이 일부 적절한 규제 내용을 담고 있지만 넓은 범위의 보호조치를 제공하는 것은 아니었음
  - 브라질의 경우 코로나19에 대응하여 채택된 법률은 공공기관 간 개인데이터의 공유를 전염병 확산 방지 목적에 한정할 것을 요구하는 일반 규정 이외에 특정한 데이터 보호 수단을 포함하지 않았음
  - 파푸아뉴기니에서도 국가 팬데믹법의 제정을 통해 처리 목적 달성에 필요한 개인데이터만을 수집할 것을 규정했지만 실제로는 국가가 개인데이터 수집에서 광범위하고 강력한 권한을 행사

# PART Ⅳ 결론 및 시사점

- 데이터 경제의 급속한 발전으로 데이터를 기반으로 한 다양한 제품, 서비스, 비즈니스 모델이 출현하면서 그에 대응하는 정책과 규제가 필요
  - 한편으로는 시민과 기업의 권리를 보장하는 보호 규제와 다른 한편으로는 데이터 활용을 촉진하는 규제를 동시에 포함하는 데이터 거버넌스의 구축이 요구됨
  - 그러나 개발도상국을 비롯한 많은 국가에서 현재의 데이터 거버넌스 수준을 파악하고, 향후 규제 개혁의 우선순위를 설정하기 위해 충분한 조사가 필요
- 80개국에 대한 데이터 규제 조사분석은 그동안 이루어진 데이터 거버넌스 관련 법률 및 규제의 가장 포괄적인 평가라고 할 수 있음
  - 본 조사분석에서는 보호조치와 촉진조치의 2가지 핵심 지표 하에 개인데이터, 비개인데이터, 사이버보안/사이버범죄, 국가 간 데이터 이동, 전자상거래, 공공데이터, 민간데이터 지표의 규제 수준에 대한 정량적 측정값을 제공
- 동 연구를 통해 발견된 주요 분석 사항은 다음과 같음
  - 각국이 보호조치보다 촉진조치에 더 많은 노력을 기울이고 있고, 각각의 규제 개발의 수준은 아직 중간 단계에 해당
    - 보호조치의 경우 조사 대상국의 41%, 촉진조치는 47%가 모범 규제 사례를 채택하고 있는 것으로 나타남
  - 국가소득 그룹별로 보면, 고소득 국가가 저소득 국가에 비해 보호조치 및 촉진조치의 규제 채택 점수가 전반적으로 높게 나타남
  - 지역별로 보면, 촉진조치의 측면에서는 사하라 사막 이남 아프리카 국가를 제외하고 동아시아와 태평양 지역이 다소 앞선 가운데 비슷한 수준을 나타내고 있고, 보호조치의 측면에서는 유럽과 중앙아시아 지역이 다른 지역보다 높은 수준을 보임




**| 그림 10 | 지역별 보호조치와 촉진조치 규제 제도 채택 비율 분포**

주 : 1. 박스플롯 그래프의 위와 아래는 최대값, 최소값, 박스상단은 75%, 박스내 중간선은 50%, 박스하단은 25%의 수준을 의미 2. EAP(동아시아/태평양), ECA(유럽/중앙아시아), LCA(라틴아메리카/카리브해 연안국), MENA(중동/북아프리카), NA(북미), SA(남아시아), SSA(사하라 사막 이남 아프리카)

● 보호조치와 촉진조치 하의 7개 지표별로 볼 때, 모든 지표에서 선진 단계의 규제 수준을 나타내는 소득 그룹은 없음

- 모든 조사 대상 국가는 전자상거래 지표에서 가장 높은 점수를 달성했고, 조사 대상국의 절반 이상이 채택하고 있는 공공데이터 접근 지표와 조사 대상국의 60% 이상이 채택하고 있는 사이버보안 지표는 저소득 국가 그룹을 제외한 국가들에서 비교적 양호한 수준
- 모든 조사 대상 국가는 민간데이터 사용과 국가 간 데이터 이동 차원에서 발전 혹은 기본 수준에 있음
- 한편, 최근 코로나19사태로 인해 많은 국가들이 그동안 부재했던 개인데이터보호법을 도입하거나 기존의 법제를 보다 명확히 하거나 강화하는 움직임을 보임

**| 표 8 | 주요 국가의 보호조치, 촉진조치 하위 지표별 점수**

| 국가 | 보호조치 | 개인데이터 | 비개인 정보 | 사이버보안/ 사이버범죄 | 국가간 데이터이동 | 촉진조치 | 전자상거래 | 공공데이터 | 민간데이터 | 소득그룹 |
|---|---|---|---|---|---|---|---|---|---|---|
| 한국 | 53.93 (27) | 75 (17) | 50 (4) | 53.21 (40) | 37.5 (33) | 81.67 (4) | 95 (17) | 100 (1) | 50 (6) | 고소득 |
| 영국 | 68.45 | 91.67 | 0 | 100 | 82.14 | 100 | 100 | 100 | 100 | 고소득 |
| 에스토니아 | 79.76 | 91.67 | 50 | 100 | 77.38 | 91.67 | 100 | 100 | 75 | 고소득 |
| 멕시코 | 68.63 | 83.33 | 50 | 90 | 51.19 | 90.48 | 100 | 96.43 | 75 | 중상소득 |
| 중국 | 48.9 | 4.17 | 50 | 95 | 46.43 | 73.02 | 100 | 69.05 | 50 | 중상소득 |

주: 괄호 안은 조사 대상국 가운데 차지하는 순위, 넥스텔리전스 편집

▶ 동 조사분석의 장점은 법률 자체의 존재의 유무 뿐 아니라 주요 규제의 유무를 통해 그 규제의 전반적인 안정성 및 실행성까지 파악하는 것임

● 전반적으로 각국은 데이터 규제 관련법은 도입했으나 법 시행의 강건성이나 관리 측면에서는 약한 것으로 나타남

- 데이터 거버넌스의 강건성 강화와 경제·사회적 영향에 대한 보다 깊은 이해를 위해서는 향후 연구가 더 진행되어야 할 것임

- 우리나라의 경우 데이터 거버넌스 수준으로 볼 때 다른 국가와 마찬가지로 촉진조치 측면이 보호조치보다 더 나은 양상을 보이고 있어 향후 보호조치 측면에 대한 보다 많은 고려가 필요
  - 우리나라는 촉진조치의 경우 전체 4위인 데 비해 보호조치는 27위를 나타내 두 핵심지표 간 격차가 매우 큰 것으로 판단됨
  - 특히 사이버보안/사이버범죄와 국가 간 데이터 이동 지표에서 각각 40위와 33위를 기록하고 있어 이에 대한 데이터 거버넌스가 선진 수준으로 나아가기 위해서는 보완과 검토가 필요

# (붙임)지표별 설문 내용

## (1) 보호조치

### ① 개인데이터보호

**| 붙임 1 | 개인데이터보호 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 법적 근거 | 개인데이터와 개인 식별 정보의 사용, 수집 및 처리를 명시적으로 규율하는 데이터 보호/ 개인데이터 보호법이 있는가? ① 예 ② 아니오, 부문별로만 적용함 ③ 아니오, 헌법상에서는 프라이버시 또는 데이터 보호권을 보장함 ④ 아니오, 중요한 판례나 행정결정은 존재함 |
| 예외 사항 | 관련 법률과 규정에서 정부의 데이터 수집 또는 처리 제한에 대한 예외를 제공하는가?<br>① 예 ② 아니오 |
| 필요성 및 적절성 | 이러한 예외의 합법적 적용 여부를 결정하기 위해 '필요성 및 적절성' 평가가 있는가?<br>① 예 ② 아니오 |
| 목적 제한 | 개인데이터의 수집 및 사용을 명시된 목적으로 제한하는 법률 또는 규정이 있는가? ① 예 ② 아니오 |
| 데이터 최소화 | 개인데이터 수집과 사용이 처리 목적에 비례하고 적절하며 필요한 것으로 제한하는 법률 또는 유사한 표준이 있는가?<br>① 예 ② 아니오 |
| 저장 제한 | 개인 데이터가 처리 목적에 필요한 기간보다 오래 보관되지 않도록 요구하는 법률 또는 규정이 있는가?<br>① 예 ② 아니오 |
| 프라이버시 보호 내재화 | 데이터 프로세서에 대해 프라이버시 보호의 내재화를 요구하는 정책, 법률 또는 규정이 있는가?<br>① 예 ② 아니오 |
| 제3자와의 정보공유 | 제3자와의 개인데이터 공유를 허용, 제한 또는 다루는 법률, 규정 또는 정책이 있는가?<br>① 예 ② 아니오 |
| 정확성 및 수정권리 | 개인이 개인데이터의 정확성에 대한 이의를 제기하거나 정보를 수정 또는 삭제할 권리가 있는가?<br>① 예 ② 아니오 |
| 자동화된 의사결정 | 전적으로 자동화된 처리에 의존해 개인에 대한 의사결정을 하는 것을 제한할 권리가 있는가?<br>① 예 ② 아니오 |
| 반대권 | 개인이 개인데이터 사용에 반대하고 불만을 제기하고 시정을 요구할 권리가 있는가?<br>① 예 ② 아니오 |
| 감독기관 | 법과 규정이 데이터 보호 기관(DPA) 혹은 데이터 보호 책임자 또는 조직(DPO)의 설립을 규정하는가?<br>① 예 ② 아니오 |

### ② 비개인데이터보호

**| 붙임 2 | 비개인데이터보호 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 지식재산권 활용 | 데이터 공유를 방지하기 위해 지식재산권을 사용할 수 있는가? |
| | 법률에 비개인 정부 데이터(기업등록부, 비즈니스 데이터)의 기밀성을 규제하는 조항이 포함되어 있는가? |

### ③ 사이버보안 및 사이버범죄

**| 붙임 3 | 사이버보안 및 사이버범죄 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 데이터 보안 | 데이터 프로세서/컨트롤러는 개인데이터의 자동 처리를 위해 다음의 보안 요구 사항을 준수해야 하는가? ① 암호화 ② 익명화/가명화 ③ 데이터 및 시스템 복원 기능 ④ 시스템의 지속적 테스트, 평가 |
| 사이버보안 표준의 적용 | 데이터 프로세서/컨트롤러는 다음의 사이버보안 요구사항을 준수해야 하는가? ① 위반 감지와 방지 내부 절차 ② 데이터/시스템 기밀 유지 ③ 관리자 선임 ④ 내부통제 ⑤ 유출 피해 평가 ⑥ 임직원 교육 |
| 침해사고 운영팀 (CERT) | 사이버보안 위협을 식별, 조사 및 해결하기 위한 사이버보안 전략, 인프라 및 기관의 구성을 위한 법률, 규정 또는 정책이 있는가? ① 국가인프라 보호를 위한 사이버보안 계획 ② 국가 CERT |
| 사이버범죄 | 사이버범죄 조항이 있는가? |

### ④ 국가 간 데이터 이동

**| 붙임 4 | 국가 간 데이터 이동 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 국외 이동 원칙 | 어떤 원칙에 근거하여 국내의 개인데이터를 국외에 전송하는가? ① 적절성 접근 방식 ② 책임성 접근 방식 |
| 타 국가(기관)와의 협정 | 국가 간 개인데이터 전송을 요구, 허용 또는 제한하기 위해 외국 또는 다국적 기관과 어떤 내용의 협정을 맺고 있는가? ① 적절성 결정/허용 목록 ② 구속력 있는 기업 규칙 ③ 상호 인정 협정 ④ 첨단정보공유 기법 ⑤ 조약 ⑥ 특정 계약에 따른 자체 인증/자체 평가 ⑦ 표준 계약 조항 |
| 국가 간 이동시 개인데이터 보호 내용 | 개인데이터를 국외로 전송할 때 적절한 수준의 보호를 구성하는 내용은 무엇인가? ① 개인데이터의 성격 ② 정보의 출처 국가 ③ 목적지 국가 ④ 데이터가 처리되는 목적 및 기간 ⑤ 당사국 시행 관련법 ⑥ 제3국의 규제기관 존재 및 기능 ⑦ 데이터 주체의 구제사항 ⑧ 당사국의 국제조약 ⑨ 당사국에서 실행 가능한 표준계약(SCCs)및 구속력 있는 기업규칙(BCRs) |

## (2) 촉진조치

### ① 전자상거래

**| 붙임 5 | 전자상거래 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 법적 기반 | 전자 상거래를 명시적으로 규율하는 법률 또는 규정이 있는가? ① 예 ② 아니오 |
| 법적(기능적) 동등성 | 종이 기반과 전자 기반의 통신 및 거래의 동등성 조항이 있는가? ① 전자 통신/메시지 ② 전자 계약 ③ 전자 서명 ④ 전자 증거 |
| 전자 서명 | 전자서명의 법적 규정 형식은 무엇인가? ① 모든 전자서명 ② 디지털 전자서명(예 : PKI)만 |
| 기술적 중립성 | 전자 통신 및 거래에 대해 특정한 기술 형태를 규정하고 있는가? ① 예 ② 아니오 |
| 정부서비스 디지털 ID 시스템 | 개인이 온라인 인증으로 정부서비스에 접근할 수 있는 디지털 ID 시스템이 있는가? (예 : 세금 신고) ① 예 ② 아니오 |

## ② 공공데이터

**| 붙임 6 | 공공데이터 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 의미적 상호운용성 | 정부기관은 의미적 상호운용성(semantic interoperability)을 가능케 하는 공통 기술 표준을 요구받고 있는가? ① 공개 API ② 'Ask Once' 원칙 의무화 ③ 메타데이터 접근을 위한 표준 통신 프로토콜 ④ 데이터/메타데이터용 시맨틱 카탈로그 |
| 오픈 데이터 | 공공 부문에 대한 데이터 공개 정책 혹은 법이 있는가? ①법 ②정책 ③없음 |
| 데이터 분류 | 정부 데이터 기밀 분류 정책이 존재하는가? ① 예 ② 아니오 |
| | 모든 정부 데이터베이스, 응용프로그램, 시스템에 일반 데이터 기밀 분류를 사용하는가? ① 예 ② 아니오 |
| 정보접근(ATI) | 개인의 정부 기록 및 데이터 접근(ATI)을 허용하는 법이 있는가? |
| | ATI법은 예외조항을 갖고 있는가? ①국가 안보 ②영업 비밀 ③개인데이터 ④법 집행 ⑤특권 정보 ⑥공공 조사 및 감사 |
| 공개 라이선스 제도 | 정부는 공개 라이선스 제도(예 : 저작자 표시에 의한 크리에이티브 커먼즈 라이센스(Creative Commons License)를 채택했는가? ① 예 ② 아니오 |

## ③ 민간데이터

**| 붙임 7 | 민간데이터 설문 내용**

| 구분 | 설문 내용 |
|---|---|
| 데이터 이동성 | 개인은 데이터 컨트롤러가 자신의 정보를 다른 서비스 또는 제품 제공업체로 전송하도록 요청할 권리가 있는가? ① 예 ② 아니오 |
| | 개인은 구조화되고 기계 판독 가능한 형식으로 컨트롤러에 의해 처리된 데이터를 얻을 권리가 있는가? ① 예 ② 아니오 |
| 개인 ID 인증 | 민간 서비스 제공업체가 ID 시스템으로 개인의 신원을 디지털 방식으로 확인하거나 인증할 수 있는가? ① 예 ② 아니오 |
| 자발적 지식재산 라이선스 | 표준 설정 조직은 지식재산권자가 공정하고 합리적이며 비차별적인 조건에 따라 표준 필수 데이터 또는 응용프로그램에 대한 자발적 라이선스 접근을 제공하도록 요구할 수 있는가? ① 예 ② 아니오 |

# 참 고 문 헌


- World bank, Mapping Data Governance Legal Frameworks Around the World : Findings from the Global Data Regulation Diagnostic, 2021.4.7.

데이터산업 동향 이슈 브리프

ISSUE BRIEF

| **발행일** 2021년 5월 31일

| **발행처** Kdata 한국데이터산업진흥원
서울시 중구 세종대로 9길 42, 부영빌딩 7, 9, 11층

| **기획 및 편집** 데이터산업본부 산업기획팀

| **문의처** Tel: 02-3708-5362, 5363

* 본 지에 실린 내용은 한국데이터산업진흥원의 공식 의견과 다를 수 있습니다.
본 내용은 무단전재를 금하여, 가공/인용할 경우 반드시 출처를 밝혀주시기 바랍니다.