중국의 데이터 법제 현황

박현지
법무법인(유)지평, 국제그룹/변호사

1. 들어가며

전세계적으로 데이터에 대한 의존도가 높아지면서 '데이터'는 국가 발전의 핵심 자원으로 인식되고 있다. 실제로 데이터는 디지털 경제 시대의 핵심 자원으로서 경제 발전과 더불어 국가 안보에 중요한 전략적 가치를 지닌다. 아울러, 개인정보 보안 이슈도 민감한 현안으로 부각되고 있는데, 데이터 보안의 핵심 사항은 다름 아닌 '데이터 남용'과 '데이터 유출'의 방지이다. 2020년 중국 정보통신기술원 발표에 따르면, 전 세계 데이터 침해 건수는 이전 15년 간 총 침해 건수를 초과하였으며, 이는 데이터 보안 문제가 시급히 해결해야 할 과제임을 보여주는 지표이다[1]. 따라서 데이터를 안전하게 활용하면서도 무분별한 오용이나 유출을 예방하고 대응하는 체계를 갖추는 것이 무엇보다 중요하다.

중국의 경우 '데이터는 국가 발전의 핵심 생산요소'라는 기조 아래 데이터 기반 혁신을 강력히 추진하고 있다. 2020년에는 데이터를 토지, 노동, 자본, 기술과 함께 제5의 생산 요소로 공식 지정하였으며, 디

1) 참고 사이트 주소: https://www.chinalawinsight.com/2025/05/articles/uncategorized/data-breach-notification-system-and-compliance-essentials/ (방문날짜: 2025.7.12)

전문가가 바라본
글로벌 핵심 이슈와 시사점

지털화와 국가 발전의 기반으로 인식하고 있다[2]. 그러나 미국이나 유럽 등의 접근법과 비교하면, 중국은 정보주체의 개인 프라이버시 보호보다는 국가 안보와 사회 질서 유지를 위한 엄격한 규제와 통제를 중시하는 경향이 두드러진다. 예를 들어, 유럽연합(EU)은 개인정보보호지침(GDPR) 등을 통해 개인의 자율성과 프라이버시 권리를 최우선으로 보호하는 반면, 중국은 데이터 거버넌스에서 국가 이익과 안보를 우선시하며 강력한 규제와 제재 수단을 강조하고 있는 것으로 보여진다.

한편, 다른 나라들과 마찬가지로 중국 내에서도 개인정보 대량 유출 사건과 그로 인한 피해가 계속 발생하고 있다. 이러한 사안들은 개인정보 유출에 대한 국민적 불안감을 증폭시키고, 정보주체의 권리를 더욱 두텁게 보호할 필요성을 환기시켰다. 결국 데이터 경제를 발전시키면서도 개인정보 유출을 방지하기 위해서는, 개인정보 정보주체의 권리를 한층 유연하면서도 강화된 수준으로 보호할 수 있는 법제 개선과 실효적 집행이 요구된다. 이에 본고에서는 이러한 배경을 바탕으로 중국의 개인정보 보호 관련 법제 현황과 데이터 유출 방지를 위한 제도적 개선 방향을 살펴보고자 한다.

2. 중국의 개인정보 보호 규정

기존의 입법 체계상 산발적이고 분산적으로 마련되어 있던 형법 또는 '네트워크 안전법' 등 관련 법률에서는 개인정보 규율에 대한 제도적 공백이 존재하였다. 이에 따라 전면적이고 통합적인 법체계의 필요성이 차츰 대두되었으며, 2021년 8월 20일 개인정보보호법[3](이하 '동법' 또는 '개인정보보호법')이 전국인민대표대회 상무위원회에서 통과되어 2021년 11월부터 시행되고 있다. 종합하면, 사이버보안법(CSL, 2017년 시행), 데이터안전법(DSL, 2021년 시행), 개인정보보호법(PIPL, 2021년 시행)을 포함한 소위 '데이터 3법'이 중국의 데이터 처리방식에 대한 기준을 규율하고 있다. 개인정보보호법이 통과된 이후로 세부적인 하위 규범들도 마련되고 있다. 중국 국가인터넷정보판공실(이하, 'CAC')은 2022년 7월 「데이터 국외이전 보안평가 방법」을 발표하여 중요 데이터 또는 대량의 개인정보를 해외로 이전할 때 사전 보안평가를 거치도록 의무화하였으며(2022년 9월 1일 시행), 2023년 2월에는 「개인정보 국외이전 표준계약 규정」을 제정하여 표준계약 조항을 통해 개인정보 이전 요구사항을 구체화한 바 있다. 최근 CAC는 개인정보보호법 및 네트워크 데이터 보안 행정규정[4](국무원령 제790호, 2025년 1월 1일부

2) 2021년 중국 정보통신연구원(CAICT) 보고서(중문 명칭: 中国数字经济发展白皮书) 참조
3) 중문명: 中华人民共和　人信息保护法
4) 중문 명칭:《网络数据安全管理条例》

터 시행)에 근거한 「개인정보 보호 준수 감사 관리조치」[5]를 제정하여, 2025년 5월 1일부로 시행하고 있다. 이 행정 조치는 기업의 내부 통제 강화를 유도하기 위하여 1천만 명 이상의 개인정보를 처리하는 데이터 처리자를 대상으로 2년마다 외부 감사 보고서를 의무화하였으며, CAC 등 관련 당국에게 감사 실시 권한을 부여하는 내용 등을 규정하고 있다.[6]

3. 개인정보보호법의 주된 내용

1) 개인정보 및 적용 범위: 중국 개인정보보호법상 '개인정보'의 정의는 식별 혹은 식별 가능 자연인 관련 정보이다('익명화된 정보'는 개인정보의 범위에서 제외) 개인정보 처리 범위에는 개인정보의 수집, 저장, 사용, 전송, 공개, 삭제 등 일련의 단계가 포함된다. 또한 중화인민공화국 안에서 이뤄지는 개인정보 처리는 모두 중국 개인정보보호법의 역내 적용 범위에 해당한다. 반면 중국 영토 밖에서 개인정보 처리가 이뤄지더라도, (i) 중국 내 자연인에게 상품 혹은 서비스를 제공하기 위하여, 혹은 (ii) 중국 내 자연인 행위에 대한 분석 및 평가, 혹은 (iii) 기타 법령에 따른 기타 사유에 의한 경우에는 개인정보보호법상 역외적용 범위에 속한다. 특히 해외에 소재한 개인정보 처리자가 동법의 적용 대상에 해당할 경우에는 반드시 중국 내 개인정보보호책임자(DPO)를 지정하거나 전문 기관을 설립해야 하며, 중국 내 개인정보보호책임자의 이름과 연락처를 중국 당국에 제출해야 한다.

2) 개인정보 처리원칙 및 적법처리 근거: 개인정보 처리 목적과 방법에 관한 기본 원칙으로 합법/정당/필요/신의성실 원칙 등이 요구된다. 개인정보는 사전에 목적과 범위를 명확히 고지하고 정보주체의 자발적인 동의를 받은 경우에만 필요최소한으로 처리하는 것이 원칙이다. 개인정보 처리를 위해서는 동의 방식 외에도, 계약 이행, 법정 의무, 공중보건/긴급보호, 공익 보도, 공개한 정보, 기타 법령 등이 합법성 근거사유로써 규정되어 있다(제13조). 한편으로, 중국 법령이 정하는 '공익'이나 '법정 의무' 범위가 넓게 해석되면 남용 소지가 있다는 지적이 제기되고 있는데, 실제 집행의 경우에는 안보 내지 공공보건 목적에만 국한되어 해석되는 추이를 보인다.

3) 정보주체의 동의 및 권리

(i) 정보주체의 동의 요건과 철회: 정보주체의 동의는 자발적이고 명시적이며 충분히 고지된 동의여야 하며, 처리 목적이나 방법, 범위를 변경할 때는 재동의가 필요하다. 개인정보 동의에 대하여는 철회권이 보장된다.

(ii) 자동화 의사결정에 대한 설명 요구권: 자동화 의사결정, 즉 알고리즘 프로파일링의 공개 및 설명 요구에 대응해야 하도록 하여, 기업에게 알고리즘 운영에 대한 상당한 책임을 부과하는 규정이다. 다만, 기업 입장에서는 자동화된 의사결정 (알고리즘)이 영업비밀에 해당하는 경우가 많기 때문에, 알고리즘에 대한 투명성 요구시 영업 비밀 보호 요구와 충돌할

5) 중문 명칭:《个人信息保护合规性审计管理办法》
6) 참고 웹사이트 주소: https://natlawreview.com/article/china-issues-measures-data-protection-compliance-audits (방문날짜: 2025.7.11)

가능성이 있다.[7)]

4) 민감정보 규정: 민감정보 정의는 생체정보/종교정보/특정 신분정보 /의료정보/금융정보/행위경로/14세 미만 아동 정보 등으로 광범위하게 규정되어 있다(제28조). 민감정보를 처리할 때는 별도 동의를 받도록 의무화되어 있으며, 처리 목적을 특정하여 충분히 필요한 범위 내에서만 처리해야 하고 그에 상응하는 엄격한 보호조치를 취해야 한다고 규정하고 있어, 민감정보에 대한 처리 기준이 상당히 엄격한 편이다. 또한, 이러한 민감정보 유형은 목적의 정당성과 필요성을 고려하여 최소한으로만 수집/이용해야 한다(제29조). 참고로, 14세 미만 아동 정보는 기업에게 별도 규칙 제정 의무를 규정하고 있어(제31조), 연령 검증 및 부모 동의 프로세스 절차 부담과 같은 기업의 컴플라이언스 요구가 한층 강화된 측면이 있다.

5) 국외 이전 및 데이터 현지화 요건

(i) 국외이전 요건: 중국 개인정보보호법의 적용되는 기업에게는 역외 적용 및 국외 이전에 대한 절차로 표준계약서 체결 및 안전성 평가에 대한 대응이 요구되고 있다. 이에 CAC에서 정한 안전평가를 통과하거나(경외이전 보안평가 방법 [8)] 참조), 2023년 2월 CAC에서 발표한 '국외 이전 표준계약 방법'에 따른 계약을 체결한 경우, 혹은 [9)] 중국이 체결한 조약이나 협정이 있는 경우에는 개인정보의 국외 이전이 예외적으로 허용된다.

국외이전에 요구되는 또 다른 요건으로 개인정보처리자는 전문기관의 개인정보보호 인증을 통과하여 개인정보 처리 시스템의 안전성을 입증하여야 한다(「네트워크 보안 표준 실무지침: 개인정보 국경 간 처리 활동 보안 인증 규범」 [10)]참조)[11)]. 참고로, 중요 데이터 또는 개인정보가 포함되지 않은 경우, 특정한 요건이 충족되면, 안전평가, 표준계약 체결 및 개인정보보호 인증 절차 등이 면제될 수 있다.

(ii) 데이터 현지화 의무: 중요 정보기초시설 운영자(CIIO) 및 대규모 처리자는 중국 본토로 저장 즉, 역내 저장이 원칙이며, 개인정보 역외 이전시 CAC 안전성 평가를 필수적으로 받아야 한다. 상기 언급된 '대규모 처리자'에 대한 수량 기준은 하위 규범에 위임되어 있으므로 별도로 확인하여야 한다.

---

7) 중국은2022년부터 알고리즘 규제에 관한 규정(중문명: 互联网信息服务算法推荐管理规定)을 시행함으로써, 사용자 맞춤 추천 알고리즘의 등록 및 공개 요구 등을 의무적으로 부과하고 있다.

8) 중문명:《数据出境安全评估办法》

9) 개인정보 수출자와 해외 수령자 간에 표준조항을 포함한 계약을 맺고, CAC에 계약을 제출하여 신고함으로써 이전을 수행한다. 2023년 6월 1일부터 표준계약 제도가 시행되어, 기업들은 6개월 내 기존 데이터 이전 활동을 정비하도록 유예기간이 부여되었다. 참고로, 2024년 3월 중국 당국은 「데이터 국경간 이동 관련 편리화 규정」을 발표하여, 일정 조건 하에서 개인정보 국외 이전을 안전평가 또는 표준계약 체결 없이도 허용하는 완화 정책을 내놓았다. 비(非) CIIO 기업이 1년간 10만 명 미만의 일반 개인정보를 국외 이전하는 경우에도 관련 절차를 면제하여, 중소 규모 데이터 이전은 규제 대상에서 제외하였다.

10) 중문명:《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》 참고로, 2022년 12월 공개된 이 지침에 따르면, 다국적 기업이나 동일한 경제, 동일한 사업 실체에 소속된 자회사 또는 관계 회사 간의 국경 간 이전의 경우에는 보호 인증 방식을 우선 적용해야 한다고 규정되어 있다.

11) 중국인터넷 안전심사 기술 및 인증 센터(中国网路安全审查技术与认证中心, 홈페이지: https://www.isccc.gov.cn) 참고

개인정보 처리자의 의무사항: 민감정보, 자동화 결정, 제3자 제공, 국외 이전 등에 대해서는 사전 영향평가가 요구되며, 사전 영향평가 보고서는 3년 동안 보관해야 하는 의무사항이 있다.

6) 관리감독기관: 국가시장감독관리부서(SAMR)는 CAC와 공동으로 개인정보 국외 이전 개인정보보호 인증 활동을 감독한다. 이러한 기관들 외에도 국무원 부처 및 지방정부 관련 부처에서는 문서 열람, 현장 검사, 설비 조사 및 압수 등 제재/조사 조치 등을 행사할 권한이 있다.

7) 공익소송: 인민검찰원이나 소비자단체 등에서 공익소송을 제기할 수 있는 규정이 도입되어, 집단피해 회복을 위한 민사구제 메커니즘이 강화되었다.

8) 위반 책임: 데이터 유출 사고가 발생하는 경우, 기업은 개인정보보호 규정 위반으로 상당한 벌금을 부과받을 수 있다. 먼저 일반적 위반사항의 경우에는, 시정명령 외에도 100만 위안 이상의 벌금이 부과될 수 있다. 그리고 책임자의 경우, 10만 위안 이하의 벌금에 처해질 수 있다. 이어서 중대한 위반사항에 해당하는 경우에는, 5,000만 위안 이하 또는 전년도 매출의 5% 이하 벌금이 부과될 수 있으며, 영업정지/허가취소 처분이 부과될 수 있다. 이 밖에도 상술한 규정들을 위반하는 경우에는 공공기관 책임(제68조), 신용정보 공시 제재(제67조) 조치가 병과 적용될 수 있으며, 이에 따라 기업 신용도나 평판이 훼손될 가능성이 있다.

4. 맺음말

앞서 중국 개인정보보호법의 국외 데이터 이전 요건에 관한 규정을 살펴보면, 중국 정부가 데이터 주권을 확고히 하는 동시에 개인정보의 국외 유출을 엄격히 통제하려는 의도가 반영되어 있다.

또한 중국의 개인정보보호법은 2021년 시행 이후 지속적으로 세부 규범과 실행 지침이 보완되고 있으며, 특히 2025년 시행된 「개인정보 보호 준수 감사 관리조치」와 같은 후속 규정들을 통해 기업에 대한 감독과 제재가 더욱 강화되고 있는 추세이다. 이는 중국이 개인정보 보호를 단순한 개인의 권리 보장 차원을 넘어, 국가 안보와 데이터 주권 확립의 핵심 수단으로 활용하고 있음을 시사한다.

본법에 따른 집행 판례가 나날이 축적되고 있으며 데이터 보안 규범에 대한 환경 변화와 개인정보 권리 주체에 대한 실질적인 보호 추세에 비추어보면, 향후 개인정보보호법이 보다 탄력적으로 정비될 가능성이 높다.

향후 중국 개인정보보호법의 개선 방향과 관련하여는 다음과 같은 변화가 예상된다. 첫째, 디지털 경제 발전 및 기술 혁신에 따른 새로운 개인정보 처리 방식에 대한 규범 마련이 지속될 것이다. 둘째, AI와 빅데이터 활용이 확산됨에 따라 자동화 의사결정과 알고리즘 투명성에 대한 규제가 더욱 구체화될 것으로 예상된다.

그러므로 이러한 변화에 따라 중국 개인정보보호법

의 적용을 받는 중국 경내·외 사업자로서는(해외 사업체 포함) 다음과 같은 대응 전략을 수립해야 할 것이다. 우선적으로 관련 법령에 대하여 수시로 모니터링하는 체계 및 법령과 지침 변화에 신속하게 대응할 수 있는 컴플라이언스 시스템을 구축해야 한다. 또한, 일련의 데이터 처리 과정에 걸친 리스크 평가와 보호 조치를 사전에 설계하는 한편 데이터 침해 대응 체계를 강화하고, 통지 시스템을 효과적으로 운영하여야 한다. 특히 국외 이전이나 민감정보 처리가 필요한 경우에는 사전 영향평가와 적절한 법적 근거 마련이 필수적이다.

종합하면, 중국의 개인정보보호 법제는 단순한 개인정보 보호를 넘어 국가 차원의 데이터 거버넌스 체계의 핵심 구성 요소로 기능하고 있으며, 이에 대한 종합적이고 전문적인 접근이 요구되는 상황이다. 따라서 데이터 컴플라이언스 전략을 수립하기 위한 현지 전문가의 종합적인 법률 자문이 반드시 필요하다고 판단된다. 끝.