

# 중국 네트워크 안전법 동향

정태인\*, 김주영\*, 김원\*

## 요약

중국은 인터넷 인프라가 지속적으로 정비되면서 인터넷 사용자 수가 급속히 증가하여, 2016년에 7.3억명에 도달하였다. 그러나 인터넷 기술은 발전하였으나, 관련법은 이를 따라가지 못하는 실정이었다. 이에 중국 전국인민대표대회에서는 2016년 11월 네트워크 안전법(中华人民共和国网络安全法)을 통과시키고, 2017년 6월 시행할 예정이다. 본고에서는 해당 법의 제정 배경 및 경과를 설명하고, 주요 내용을 살펴보고자 한다.

## I. 서론

중국은 인터넷 인프라를 지속적으로 정비하고 있어, 인터넷 사용자 수가 급속히 증가하고 있다. 특히 국토가 넓다는 특징 때문에 유선 인터넷 인프라보다 휴대폰을 이용한 인터넷 사용자 비율이 높다. 인터넷 사용자 수는 2016년에 7.3억 명에 도달하였다[1]. 한편 2015년 중국 정부는 “인터넷 플러스(互联网+)” 정책[2]을 발표하고, 인터넷과 기존 산업의 융합을 통해, 고부가가치 산업으로의 변화를 강조하였다. 이러한 정부 정책에 힘입어, 인터넷 관련 산업 규모도 급속히 증가하고 있다. 바이두(百度), 알리바바(阿里巴巴), 텐센트(腾讯) 등의 관련 기업도 상당한 규모로 성장하였으며, 이외에도 신규 스타트업 기업들이 계속 창업하는 추세이다.

한편 인터넷 사용의 증가에 따라 다양한 부작용이 나타나고 있다. 특히 개인정보보호에 관한 구체적인 법이 없는 것을 악용하여, 개인정보를 무단으로 수집하고, 이를 매매하거나 범죄에 악용하는 사례가 증가하고 있다. 특히 2016년 8월 쉬위위(徐玉玉)라는 산둥성의 가정 형편이 어려운 대학 입학 예정자가 등록금을 전화 사기로 잃어버린 후에 심장마비로 사망한 사건은 여러 언론에서 보도되어 큰 사회 문제가 되었다[3].

이러한 사회적 필요성을 반영하여, 중국은 2016년 11월 네트워크 안전법을 통과시키고, 2017년 6월에 시행할 예정이다. 본 고에서는 해당 법의 제정 배경 및 경과를 소개하고, 법의 주요 내용을 소개하고자 한다.

## II. 중국의 법률 체계 및 유관 법률

중국의 입법법(立法法)에서는 중국 법률을 헌법, 법률, 행정법규, 지방성법규, 자치조례·단행조례·부문규장으로 정의하고 있다[4]. 각각은 입법 주체에 따라 구분되며, 상세한 내용은 [표 1]과 같다. 특이한 점은 법률이라고 하더라도, 법이라는 명칭을 사용하지 않는 경우도 있고, 각 법률에서 결의(決議), 결정(決定), 규정(規定), 방법(辦法) 등의 명칭을 혼용하는 경우도 있다는 것이다.

[표 1] 중국의 법률 체계

유형	입법 주체	예
헌법	전국인민대표대회	헌법
법률	전국인민대표대회	기본법률(민법통칙, 형법)
	전국인민대표대회 상무위원회	기본법률 이외(상표법)
행정법규	국무원	인터넷 정보 서비스 관리 방법
지방성 법규	지방 인민대표대회 및 상무위원회	북경시 식품 안전 조례
자치조례, 단행조례, 부문규장	민족자치구역 자치기관	연길 조선족 자치주 자치 조례
	국무원 산하 부처	인터넷 뉴스 정보 서비스 관리 규정

\* 한국인터넷진흥원 (tjung@kisa.or.kr, kjy@kisa.or.kr, wkim1015@kisa.or.kr)

### Ⅲ. 네트워크 안전법 제정 배경 및 경과

#### 3.1. 제정 배경

네트워크 안전법(中华人民共和国网络安全法, People's Republic of China Network Security Law)은 번역에 따라 인터넷 안전법, 인터넷 보안법, 사이버 안전법, 사이버 보안법 등으로 번역할 수 있다. 중국어의 “网络”는 네트워크, “互联网”은 인터넷을 의미하나, 혼재되어 사용되기도 한다. 또한 “安全”은 안전을 의미하나, 보안으로 번역해도 무방하다. 본 고에서는 인터넷을 포함한 네트워크가 보다 적합한 용어라고 생각하여, 네트워크 안전법이란 명칭을 사용하였다.

네트워크 안전법 이전에는 개인정보보호와 관련하여 형법 등에 해당 조항이 제정되어 시행되고 있었다[5]. 개인정보보호법 초안은 2008년 국무원에 제출되었으나, 실제로 통과되어 법으로 시행되지는 않았다[6]. 이번 네트워크 안전법에는 개인정보보호 관련된 주요 조항들이 포함되어 있다. 중국 정부에서는 개인정보보호법을 단독으로 제정하는데 어려움이 있어서, 네트워크 및 정보보호 등의 내용을 모두 포함하여 네트워크 안전법을 제정한 것으로 생각된다. 개인정보보호와 관련된 주요 법률은 [표 2]와 같다. 표에서 성격은 ① 법률, ② 행정법규, ③ 부문 규정, ④ 기타로 구분하였다.

[표 2] 개인정보보호 관련 법률 조항

법률(성격)	조항	주요 내용
형법(①)	253조1	개인정보 판매, 제공, 절도 시 처벌
	283조1	네트워크 서비스 제공자가 이용자 정보 유출로 피해 초래 시, 처벌
인터넷 정보보호 강화 결정(①)	전체	개인정보 수집 시 동의, 인터넷 서비스 제공자의 개인정보보호 의무, 개인정보 판매 금지 등
권익침해책임법(①)	62조	의료기관 및 의료 종사자의 환자 사생활 비밀 준수
소비자권익보호법(①)	29조	소비자 개인정보 수집 시 동의, 소비자의 개인정보 유출, 판매, 불법 제공 금지
모바일인터넷애플리케이션서비스관리규정(④)	7조	이용자 정보 보호 체계 수립, 개인정보 수집 시 동의

법률(성격)	조항	주요 내용
통신과 인터넷 이용자 개인정보보호규정(③)	전체	통신과 인터넷 이용자의 권익 보호, 개인정보 수집 시 동의, 개인정보 훼손, 매매, 불법 제공 금지 등
소비자권익침해법행위처벌방법(③)	11조	소비자 정보 수집 시 동의, 개인정보 누설, 출판, 불법 제공 금지 등
정보안전기술 공공 및 상용 서비스 정보시스템 개인정보보호지침(④)	전체	개인정보보호 관련 국가 표준으로 개인정보 수집, 가공, 이전, 삭제 단계별로 필요 사항 규정
통신망 사기범죄 방지와 단속에 관한 통보(③)	6조	개인정보 불법 획득, 판매, 제공 금지
인터넷 예약 택시 경영서비스 관리 실시방법(③)	26조, 37조	차량 예약자와 승객의 개인정보 불법 이용 및 누출 금지, 처벌

한편 기존 법률은 구체적으로 집행 부서를 명시하고 있지 않거나 처벌 조항이 미비하여, 종종 선언적인 의미에 그치는 경우가 있었다. 최근에 사회 문제로 대두된 개인정보 관련 보이스 피싱 사건의 경우에도, 처벌 조항이 마땅하지 않아서 형법을 적용하는 경우가 많았다[7]. 따라서 이번 네트워크 안전법의 제정은 여러 가지 법률에 분산되어 있었던 관련 법률 조항을 하나의 법률로 통합하고 체계화하였다는데 이의가 있다.

#### 3.2. 제정 경과

네트워크 안전법(网络安全法)[8]은 2015년 6월 초안이 공개되어 3차의 심의를 거쳐 2016년 11월 최종 통과되었다[9]. 본 법은 2017년 6월 시행될 예정이다. 또한 법의 상세한 내용을 규정하는 “네트워크 제품과 서비스 안전 심사 방법”(网络产品和服务安全审查办法, 이하 “방법1”)[10,11]과 “개인정보와 중요 데이터 경외 반출 안전 평가 방법”(个人信息和重要数据出境安全评估办法, 이하 “방법2”)[12]이 공고되었다. 제정 경과는 [표 3]과 같다.

### Ⅳ. 네트워크 안전법 및 관련 법률 개요

네트워크 안전법은 중국 내에서의 네트워크 구축, 운영, 유지와 사용 및 네트워크 안전의 감독 관리를 규정

[표 3] 네트워크 안전법 제정 경과

연도	법률	내용
2015년 6월	네트워크 안전법	제12기 전인대 상무위원회 15차 회의, 1차 심의
2016년 6월		제12기 전인대 상무위원회 21차 회의, 2차 심의
2016년 11월		제12기 전인대 상무위원회 24차 회의, 3차 심의 및 통과
2017년 2월	네트워크 제품과 서비스 안전 심사 방법	국가 인터넷 정보 판공실에서 의견 수렴안 공고
2017년 5월	네트워크 제품과 서비스 안전 심사 방법	국가 인터넷 정보 판공실에서 시행안 공고
2017년 4월	개인정보와 중요 데이터 경외 반출 안전 평가 방법	국가 인터넷 정보 판공실에서 의견 수렴안 공고

하고 있으며, 2개 방법은 법의 구체적인 내용을 규정하는 시행령·시행규칙의 성격을 가진다. 한국의 법률 체계와 비교하면 [표 4]와 같다.

[표 4] 한국 관련법과 비교

중국	한국	비교
네트워크 안전법	정보통신망 이용촉진 및 정보보호 등에 관한 법률, 정보통신기반 보호법, 개인정보 보호법	법률
방법1, 방법2	해당 시행령/시행규칙	한국의 시행령/시행규칙

본 법의 적용 대상은 중국 내 네트워크 사업자, 핵심 정보 인프라 시설 운영자 등이다. 네트워크 사업자(网络运营者)는 인터넷 서비스 제공자(Internet Service Provider), 유선전화·휴대전화 운영자, 정보 발표 및 메신저 서비스 제공 사업자를 포함하며, 한국 정보통신망법의 “정보통신서비스 제공자”와 유사한 개념으로 판단된다. 핵심 정보 인프라 시설(关键信息基础设施)은 파괴·데이터 유출 시, 국가 안전에 중대한 손실이 발생하는 시설로, 한국 정보통신기반 보호법의 “정보통신기반 시설”과 유사한 개념으로 판단된다. 이외 주요 용어들은 [표 5]와 같다.

[표 5] 주요 용어

용어	정의	법률
네트워크 (网络)	컴퓨터 또는 기타 정보 단말기 및 관련 장비로 구성된 일정한 규칙과 프로세스에 따라 정보에 대한 수집, 저장, 전송, 교환, 처리를 진행하는 네트워크	법 제76조
네트워크 안전 (网络安全)	필요한 조치를 취해 네트워크에 대한 공격, 침입, 방해, 파괴와 불법 사용 및 의외의 사고를 방지하고 네트워크가 안정된 운영 상태를 유지하고 네트워크 데이터의 완결성, 비밀 유지성, 유용성 능력 보장	법 제76조
네트워크 사업자(网络运营者)	네트워크의 소유자, 관리자와 네트워크 서비스 제공자	법 제76조
네트워크 데이터(网络数据)	네트워크를 통해 수집, 저장, 전송, 처리와 생성되는 각종 전자 데이터	법 제76조
개인정보 (个人信息)	전자 또는 다른 방식으로 기록되는 단독 또는 기타 정보와 결합하여 자연인의 개인신분을 식별할 수 있는 각종 정보를 지칭하는데, 이름, 출생일, 신분증번호, 개인생물식별정보, 주소, 전화번호 등을 포함	법 제76조
핵심 정보 인프라 시설(关键信息基础设施)	공공통신과 정보서비스·에너지·교통·수리·금융·공공서비스·전자정부 등 중요 산업과 영역에서 일단 파괴·기능 상실·데이터 유출이 발생하면 국가 안전, 국가 경제, 국민 생활, 공공이익에 중대한 손상을 줄 수 있는 시설	법 제31조
네트워크 사업자(网络运营者)	네트워크의 소유자, 관리자, 네트워크 서비스 제공자	방법2 제17조
데이터의 경외 반출(数据出境)	네트워크 사업자가 중화인민공화국 경내에서 사업 중 수집하고 생산한 개인정보와 중요 데이터를 경외에 위치한 기구, 조직, 개인에게 제공하는 것	방법2 제17조
개인정보 (个人信息)	전자 또는 기타 방식을 기록된, 단독으로 또는 기타 정보와 결합하여 자연인의 개인신분을 식별할 수 있는 각종 정보로서, 자연인의 성명, 출생일자, 신분증번호, 개인생물식별정보, 주소, 전화번호 등을 포함하되, 이에 한정되지는 않음	방법2 제17조
중요 데이터 (重要数据)	국가안전, 경제발전, 사회공공이익과 밀접하게 관계된 데이터를 가리키는 데, 구체적인 범위는 국가 유관 표준과 중요 데이터의 식별지침을 참고	방법2 제17조

## V. 네트워크 안전법 주요 내용

본 법은 7장 79조로 구성되어 있으며, 네트워크 운영 안전, 핵심 정보 인프라 시설 보호, 개인정보보호, 불법 정보 단속, 네트워크 제한 조치, 법률 책임 등을 규정하고 있다. 목적은 “네트워크 안전을 보장하고 네트워크 공간 주권과 국가 안보, 사회 공공 이익을 수호하고 국민, 법인과 기타 조직의 합법적 권익을 보호하면서 경제 사회 정보화의 건전한 발전을 촉진”하는 것이다. 적용 범위는 “중화인민공화국 경내에서의 네트워크 구축, 운영, 유지와 사용 및 네트워크 안전의 감독 관리”이다. 즉, 중국 내에 네트워크를 보유한 사업자는 모두 대상이 된다.

### 5.1. 네트워크의 운영 안전

#### 5.1.1. 네트워크 사업자의 안전 보호 의무(제21조)

- 국가는 네트워크 안전 등급 보호 제도(网络安全等级保护制度)를 시행
- 네트워크 사업자는 네트워크 안전등급 보호 제도의 기준에 따라, 안전 보호 의무 이행
  - 내부의 안전관리제도와 운영규정을 제정하고 네트워크 안전 책임자를 지정하여 네트워크 안전 보호 책임 이행
  - 컴퓨터 바이러스와 네트워크 공격, 네트워크 침입 등 네트워크 안전 침해행위를 방지하는 기술 조치 시행
  - 네트워크 운영 상태와 네트워크 안전 사건의 기술 조치를 검사·기록하고, 네트워크 일지를 최소 6개월간 보존
  - 데이터 분류, 중요한 데이터 백업과 비밀번호 설정 조치 시행

#### 5.1.2. 네트워크 제품 및 서비스(제22조)

- 네트워크 제품, 서비스는 관련된 국가표준, 업계표준에 부합하여야 하고, 악성 프로세스 설치 금지
- 공급자는 네트워크 제품, 서비스의 안전 결함, 취약성 등의 위험을 발견하면, 즉시 보완조치를 취하고, 규정에 따라 이용자에게 고지하고 유관 주관 부문에 보고

#### 5.1.3. 네트워크 핵심 장비(网络关键设备) 및 네트워크 안전 전용 제품(网络安全专用产品)에 대한 안전 인증, 안전 검측 제도(제23조)

- 네트워크 핵심 장비와 네트워크 안전 전용제품은 안전 인증(安全认证) 합격 또는 안전 검측(安全检测) 기준에 부합하여야 판매 또는 제공 가능
- 국가 네트워크 정보 부문, 국무원 유관 부문은 네트워크 핵심 장비, 네트워크 안전 전용 제품의 목록을 제정 및 발표하고, 안전 인증과 안전 검측 결과의 상호 인증을 추진

#### 5.1.4. 이용자 실명제(제24조)

- 네트워크 사업자는 네트워크 접속, 도메인 등록 서비스, 유선전화, 휴대전화 등의 가입 수속 시, 혹은 이용자를 위해 정보 발표(信息发布), 메신저 등의 서비스 제공을 위해 이용자와 협의 체결 시, 이용자 신원 정보 확인 필요

#### 5.1.5. 네트워크 사업자의 안전 위험 대처(제25조)

- 네트워크 사업자는 네트워크 안전 사건의 비상 매뉴얼을 제정하여 적시에 시스템의 취약성, 컴퓨터 바이러스, 네트워크 공격, 네트워크 침입 등 안전 위험에 대처
- 네트워크 안전에 해를 가하는 사건이 발생할 경우, 즉시 비상 매뉴얼을 가동하여 상응한 보완조치를 취하고 규정에 따라 관련 주관 부문에 보고

#### 5.1.6. 네트워크 사업자의 공안기관 협조(제28조)

- 네트워크 사업자는 공안기관, 국가안전기구의 안보 및 범죄활동 조사를 위해 기술 지원과 협조 제공

## 5.2. 핵심 정보 인프라 시설 보호

### 5.2.1. 핵심 정보 인프라 시설(关键信息基础设施) 보호 (제31조)

- 공공통신과 정보서비스·에너지·교통·수리·금융·공공서비스·전자정부 등 중요 산업과 영역에

서 일단 파괴, 기능 상실, 데이터 유출이 발생하면 국가 안전, 국가 경제, 국민 생활, 공공이익에 중대한 손상을 줄 수 있는 핵심 정보 인프라 시설에 대하여, 네트워크 안전 등급 보호 제도에 기초하여, 중점 보호 실행

핵심 정보 인프라 시설의 구체적인 범위와 안전 보호 방법은 국무원이 제정한다고 정의하고 있다. 2016년 6월에 발표한 “국가 네트워크 보안 검사 운영 지침(网络安全检查操作指南)”에 핵심 정보 인프라에 대한 내용이 포함되어 있다. 이 지침은 법 제정 전에 만들어진 것인데, 국무원에서 핵심 정보 인프라 시설의 구체적인 범위와 안전 보호 방법 제정 시, 참고할 것으로 예상된다.

#### 5.2.2. 핵심 정보 인프라 시설 안전 보호 의무(제34조)

- 전문 안전 관리 기구 설치, 안전 관리 책임자 지정, 안전 배경 심사
- 네트워크 안전 교육, 기술 교육, 기능 평가 진행
- 주요 시스템 및 데이터베이스의 재난 대비 백업
- 네트워크 안전 사전 비상 매뉴얼 제정, 정기 훈련

#### 5.2.3. 핵심 정보 인프라 시설 사업자의 네트워크 제품 및 서비스 구매(제35조)

- 핵심 정보 인프라 시설 사업자의 네트워크 제품 또는 서비스 구매가 국가 안보에 영향을 줄 수 있을 경우, 국가 네트워크 정보 부문이 국무원의 관련 부문과 함께 구성한 국가 안전 심사(安全审查) 통과 필요

#### 5.2.4. 핵심 정보 인프라 시설의 개인정보 및 중요 업무 데이터 중국 내 저장(제37조)

- 핵심 정보 인프라 시설 사업자는 중국 경내(境内)에서 운영 중 수집하고 생성한 개인정보와 중요 업무 데이터를 반드시 경내에 저장
- 업무의 필요에 의해 반드시 해외에서 저장 또는 해외 기관 또는 개인에게 제공해야 할 경우, 국가 네트워크 정보 부문이 국무원의 유관 부문과 함께 제정한 방법에 따라 안전 평가(安全评估)를 진행

#### 5.2.5. 핵심 정보 인프라 시설 사업자의 검사 및 평가 (제38조)

- 핵심 정보 인프라 시설 사업자는 자체적으로 또는 전문기관에 의뢰하여 네트워크 안전성 등에 대해 매년 최소한 한 차례의 검사와 평가를 진행하여, 해당 부문에 결과 보고

### 5.3. 개인정보보호

#### 5.3.1. 이용자 비밀 유지(제40조)

- 네트워크 사업자는 수집한 이용자 정보에 대해서 반드시 엄격하게 비밀을 유지하고, 이용자 정보보호 제도를 정착

#### 5.3.2. 개인정보 수집 및 사용(제41조)

- 네트워크 사업자의 개인정보 수집 및 사용은 합법, 정당, 필요의 원칙을 준수하고 정보 수집과 사용의 목적, 방식과 범위를 공지하고 수집 대상자의 동의 필요
- 네트워크 사업자는 제공 서비스와 무관한 개인정보를 수집해서는 안 됨
- 네트워크 사업자는 법률, 행정법규의 규정과 쌍방의 약정을 어기면서 개인정보를 수집 및 사용해서는 안 됨
- 네트워크 사업자는 법률, 행정법규의 규정 또는 이용자와의 약정을 준수하면서 그가 저장 및 보관하고 있는 개인정보를 처리

#### 5.3.3. 개인정보 유출, 변조, 훼손 금지(제42조)

- 네트워크 사업자는 수집한 개인 정보를 유출, 변조, 훼손해서는 안 되며, 수집 동의를 받지 않으면, 타인에게 개인 정보를 제공해서는 안 됨. 특정 개인을 식별할 수 없도록 처리하여 복원할 수 없는 경우는 제외
- 네트워크 사업자는 기술 조치와 기타 필요한 조치를 취해 수집한 개인정보의 안전을 확실히 보장하고 그가 수집한 개인정보의 유출, 훼손, 분실을 방지
- 개인정보 유출, 훼손, 분실 상황이 발생하거나 또는 발생할 가능성이 있을 경우, 즉시 보완조치를 취하고,

적시에 이용자에게 고지 및 관련 주관 부문에 보고

5.3.4. 개인정보 삭제 및 정정 요구 권리(제43조)

- 개인은 네트워크 사업자가 규정 또는 약정을 어기고, 개인정보를 수집·사용하는 것을 발견 시, 개인정보 삭제를 요구할 수 있으며, 본인의 개인정보 오류 존재 시, 정정 요구 가능

5.3.5. 개인정보 매매 등 금지(제44조)

- 개인정보 절도·취득·불법 판매·불법 제공 금지

5.3.6. 개인정보 비밀 유지(제45조)

- 유관 부문은 직책 이행 과정에서 알게 된 개인정보, 사생활 등의 비밀 유지, 유출·판매·제공 금지

5.4. 불법 정보 단속

5.4.1. 개인 및 조직의 불법 사이트, 통신 그룹 개설 금지 (제46조)

- 개인과 조직은 사기, 범죄방법 전수, 금지물품·통제 물품 제작 또는 판매 등 불법 범죄 활동을 실시하는 사이트·통신그룹을 개설 금지
- 해당 사이트를 이용하여 사기, 금지물품·통제물품 제작 또는 판매 그리고 기타 불법 범죄 활동에 관련된 정보 공개 금지

5.4.2. 네트워크 사업자의 불법 정보 차단 및 보고(제47조)

- 법률에서 발표·전송 금지 정보 발견 시, 전송 중단, 제거, 확산 방지, 기록 보관 등의 조치 수행 및 유관 부처 보고

행정법규인 “인터넷 정보 서비스 관리 방법(互联网信息服务管理办法)”[13]에서는 인터넷 정보 서비스 공급업자들이 제작·복제·발표·전파해서는 안 되는 항목들을 9가지로 규정하고 있다.

5.4.3. 응용 소프트웨어 등에 불법 정보 포함 금지(제48조)

- 전자 정보나 응용 소프트웨어에 악성 프로세스를 설치해서는 안 되며, 법률이 금지하는 정보를 포함해서는 안 됨

5.5. 네트워크 제한 조치

5.5.1. 국가기관의 네트워크 제한 조치(제58조)

- 국가 안보, 사회 질서 유지 등을 위하여, 국무원의 결정·비준에 의해, 특정 지역에서 네트워크 통신 제한 등의 임시 조치 가능

5.6. 법률 책임

5.6.1. 법 위반에 따른 처벌(제59-69조)

- 위반 조항 및 정도에 따라서 벌금 부과, 불법 소득 몰수, 구류, 업무 일시 중단, 영업 중단 및 정돈, 웹 사이트 폐쇄, 관련 서비스 인허가 취소, 사업자 등록(영업집조, 營業執照) 말소 등 조치

VI. 네트워크 제품과 서비스 안전 심사 방법 주요 내용

본 방법은 16조로 구성되어 있으며, 안전 심사 대상, 내용, 안전 심사 위원회, 심사 통과 및 서비스 구입, 핵심 정보 인프라 시설의 네트워크 안전 심사 등을 규정하고 있다. 목적은 “네트워크 제품과 서비스 안전에 대한 관리 수준을 향상하고 공급 사슬 상에 보안 위협을 방지하며 국가의 보안과 공공 이익을 유지”하는 것이다. 대상은 “국가 보안과 공공 이익에 연관되는 정보 시스템이 이용하는 중요한 네트워크 제품과 서비스”이다.

6.1. 안전 심사 대상(제2조)

- 국가 보안과 공공 이익에 연관되는 정보 시스템이 이용하는 중요한 네트워크 제품과 서비스(重要网络产品和服务)는 네트워크 안전 심사(安全审查)를 받아야 함

## 6.2. 안전 심사 내용(제4조)

- 제품과 서비스가 불법적으로 통제, 간섭 및 운영 중단될 위험
- 제품과 핵심 부품의 연구 개발, 인도, 기술 지원 과정에서 위험
- 제품과 서비스 공급업자가 제품과 서비스를 제공하는 편의 조건을 이용하여 사용자의 관련 정보를 불법적으로 수집, 저장, 처리, 이용하는 위험
- 제품과 서비스 공급업자가 제품과 서비스에 대한 의존성에 의해 부정 경쟁을 하거나 사용자의 이익을 훼손하는 위험
- 국가의 보안과 공공 이익을 훼손하는 기타 위험 등

## 6.3. 안전 심사 위원회(제5조)

- 국가 인터넷 정보 판공실은 네트워크 안전 심사의 중요한 정책을 심사하고 사업을 총괄하며, 네트워크 안전 심사 위원회를 구성함
- 네트워크 안전 심사 판공실은 네트워크 안전 심사 사업을 구체적으로 실행함

## 6.4. 심사 통과 제품 및 서비스 구입(제10조)

- 정부 부처와 중점 산업에서는 심사 통과된 네트워크 제품과 서비스를 우선 순위로 구입하고, 미통과 제품과 서비스는 구입 불가

## 6.5. 핵심 정보 인프라 시설의 네트워크 안전 심사 (제11조)

- 핵심 정보 인프라 시설 운영자가 구입한 네트워크 제품과 서비스가 국가의 보안에 영향을 주는 경우, 네트워크 안전 심사(安全審査)를 거쳐야 함

## VII. 개인정보와 중요 데이터 경외 반출 안전 평가 방법 주요 내용

본 방법은 18조로 구성되어 있으며, 네트워크 사업자의 개인정보 및 중요 데이터 경외 제공 시 안전 평가, 개인정보 경외 반출 시, 개인정보 주체의 동의 필요, 데이터 경외 반출 안전 평가, 경외 반출 금지, 경외 반출

내역 보고 등을 규정하고 있다. 목적은 “개인정보와 중요 데이터의 안전을 보장하고, 네트워크 공간의 주권과 국가 안전, 사회 공공 이익을 수호하며, 국민과 법인 및 기타 조직의 합법적인 권익을 보장”하는 것이다. 대상은 네트워크 사업자이다.

### 7.1 네트워크 사업자의 개인정보 및 중요 데이터 경외 제공 시 안전 평가(제2조)

- 네트워크 사업자(网络运营者)는 중화인민공화국 경내에서 수집하거나 생산한 개인정보와 중요 데이터를 경내에 저장
- 업무의 필요로 인해 경외(境外)에 제공할 필요가 있을 경우, 안전 평가(安全评估) 진행

### 7.2. 개인정보 경외 반출 시, 개인정보 주체의 동의 필요(제4조)

- 개인정보의 경외 반출은 개인정보 주체에게 데이터의 경외 반출의 목적, 범위, 내용, 접수자, 접수자의 소재 국가나 지역을 설명하고 동의를 얻어야 함
- 미성년자 개인정보의 경외 반출은 보호자의 동의를 얻어야 함

### 7.3. 데이터 경외 반출 안전 평가(제8조)

- 데이터 경외 반출의 필요성
- 개인정보 관련 상황, 즉, 개인정보의 수량, 범위, 유형, 민감도 및 개인정보 주체의 자신의 개인정보 경외 반출에 대한 동의 여부 등 포함
- 중요 데이터 관련 상황, 즉, 중요 데이터의 수량, 범위, 유형 및 민감도 등 포함
- 데이터 접수자의 안전보호 조치, 능력, 수준 및 소재 국가나 지역의 네트워크 안전 환경 등
- 데이터의 경외 반출 및 재전이 후의 유출, 훼손, 변경, 남용 등 위험
- 데이터의 경외 반출 및 경외 반출 데이터의 축적으로 국가 안전, 사회 공공이익, 개인의 합법적인 권익에 대해 위험 초래 가능
- 기타 평가가 필요한 중요 사항

7.4. 경외 반출 데이터 조건(제9조)

- 50만 명 이상의 개인정보를 포함 또는 누계로 포함
- 데이터 용량이 1000GB를 초과
- 핵시설, 화학생물, 국방군수, 인구건강 등 영역 데이터, 대형 공정 활동, 해양환경 및 민감한 지리 정보 데이터 등 포함
- 핵심 정보 인프라 시설(关键信息基础设施运营者)의 시스템 취약점, 안전보호 등 네트워크 안전정보 포함
- 핵심 정보 인프라 시설(关键信息基础设施运营者) 사업자가 경외에 개인정보와 중요 데이터를 제공
- 기타 국가 안전과 사회 공공이익에 영향을 줄 가능성이 있고, 업계 주관 또는 감독관리 부문이 마땅히 평가해야한다고 판단한 경우

7.5. 경외 반출 금지(제11조)

- 개인정보가 개인정보 주체의 동의를 거치지 않았거나, 개인의 이익을 침해할 가능성이 있음
- 데이터의 경외 반출이 국가 정치, 경제, 과학기술, 국방 등 안전에 위협을 초래하여, 국가 안전에 영향을 주고, 사회의 공공이익에 손해를 가할 가능성이 있음
- 기타 국가 네트워크정보 부문, 공안부문, 안전부문 등 유관 부문이 경외 반출이 불가하다고 판단한 경우

7.6. 경외 반출 내역 보고(제12조)

- 네트워크 사업자는 업무 발전과 네트워크 사업 상황에 근거해, 매년 데이터 경외 반출에 대해서 한 차례의 평가를 진행하고, 평가 상황을 적시에 업계 주관 및 감독관리 부문에 보고
- 데이터의 접속자가 변경되거나 데이터 경외 반출의 목적, 범위, 수량, 유형 등에 비교적 큰 변화가 있을 시에, 데이터 접속자 또는 경외 반출 데이터에 중대 안전 사건이 발생할 시에, 안전 평가를 적시에 다시 실시

VIII. 고 찰

네트워크 안전법은 기존에 산재되어 있던 네트워크 보호 및 개인정보보호 조항을 하나의 법으로 체계화하였다는데 의미가 있으며, 한국의 정보통신망법과 유사

한 역할을 할 것으로 예상된다. 또한 기존의 법은 처벌 조항이 미비하여 선연적인 의미가 강하였지만, 본 법은 구체적인 처벌 조항을 적시하고 있어, 정부의 의지가 있는 경우 강력한 집행이 가능하다. 따라서 본 법의 시행에 따라 중국의 개인정보보호 수준이 향상될 것으로 기대되나, 네트워크 상에서의 콘텐츠 검열도 지속될 것으로 예상된다.

본 법에서 적용 대상자에 대한 정의를 규정하고 있으나, 구체적인 대상을 특정하기에는 부족한 점이 있다. 예를 들어 네트워크 사업자를 한국의 “정보통신서비스 제공자”에 준하여 법을 집행하는 경우, 네트워크를 소유, 관리하는 사업자가 모두 해당되어 대부분의 기업에 적용될 것으로 판단된다. 핵심 정보 인프라 시설은 한국의 “정보통신기반시설”과 유사한 개념으로 판단되나, 구체적인 범위를 국무원이 제정하도록 하여, 어떠한 시설이 해당되는 지는 현재 확인할 수 없다. 만약 중국내 특정 기업의 시설이 핵심 정보 인프라 시설에 해당하는 경우, 여러 가지 의무 조항에 대한 준수 책임이 발생하기 때문에, 시설 해당 여부에 주목할 필요가 있다. 또한 네트워크 핵심 장비, 네트워크 안전 전용 제품을 구체적으로 규정하고 있지 않은데, 만약 외국 기업의 네트워크 제품, 정보보호제품이 해당이 되는 경우, 안전 인증, 안전 검증을 위한 추가적인 부담이 발생할 수 있다. 따라서 중국 관련 업무를 수행하는 기업들은 지속적인 관심을 가질 필요가 있다.

한편 법과 방법은 한국의 법률과 시행령과 유사한데, 일부 조항에서 상위법과 상충되는 내용도 포함되어 있

[표 6] 해당 조항 비교

법률	조항
법 제37조	핵심 정보 인프라 시설 사업자는 중화인민공화국 경내에서 운영 중 수집하고 생성한 개인정보와 중요 업무 데이터를 반드시 경내에 저장하여야 한다. 업무의 필요에 의해 반드시 해외에서 저장 또는 해외 기관 또는 개인에게 제공해야 할 경우, 국가 네트워크 정보 부문이 국무원의 유관 부문과 함께 제정한 방법에 따라 안전 평가(安全評估)를 진행하여야 한다. 법률, 행정 법규에 별도의 규정이 있을 경우, 해당 규정을 따른다.
방법2 제2조	네트워크 사업자는 중화인민공화국 경내에서 수집하거나 생산한 개인정보와 중요 데이터를 경내에 저장해야 한다. 업무의 필요로 인해 경외에 제공할 필요가 있을 시에는 본 방법에 따라 안전 평가(安全評估)를 진행해야 한다.



다. 즉, 개인정보와 중요 데이터 경외 이전 시, 적용 대상이 핵심 정보 인프라 시설 사업자와 네트워크 사업자로 상이하다. 구체적인 내용은 [표 6]과 같다.

## IX. 결 론

본 고에서는 중국의 네트워크 안전법의 제정 배경과 경과, 주요 내용을 살펴보았다. 본 법의 시행을 전후하여, 다양한 제도적 변화가 예상된다.

향후 네트워크 안전법과 한국의 정보통신망법 등 유사 법률을 조항 단위로 상세히 비교하는 것이 필요하다. 또한 법 시행에 따라 좀 더 구체적인 정책 및 제도를 확인하고 이에 대한 비교도 필요할 것이다. 특히 본 법이 시행되고 난 후 중국에서 발생하는 개인정보보호 관련 사고 사례들을 수집하여 한국과 비교 분석하는 것도 매우 유용할 것으로 생각된다.

## 참 고 문 헌

- [1] 國家互聯網信息辦公室, 中國互聯網絡信息中心, 中國互聯網絡發展狀況統計報告, pp. 1, 2017
- [2] 마화팅, 장샤오핑, 인터넷플러스혁명, 비즈니스북스, pp. 11, 2016
- [3] 사건 기사(<http://news.163.com/17/0315/14/CFIU-DO6300018AOR.html>)
- [4] 입법법([http://www.npc.gov.cn/npc/dbdhhy/12\\_3/2015-03/18/content\\_1930713.htm](http://www.npc.gov.cn/npc/dbdhhy/12_3/2015-03/18/content_1930713.htm))
- [5] KISA, 중국 내 한국인 개인정보 노출 대응 방안 연구, 한국인터넷진흥원, pp. 8, 2016
- [6] 전은정, 김학범, 염홍열, “일본·중국의 개인정보 보호 법·제도 동향”, 정보보호학회지, 22(5), 2012.
- [7] KISA, 중국 내 한국인 개인정보 노출 대응 방안 연구, 한국인터넷진흥원, pp. 101, 2016
- [8] 네트워크 안전법([http://www.npc.gov.cn/npc/xinwen/2016-11/07/content\\_2001605.htm](http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm))
- [9] 네트워크 안전법 경과(<https://www.ishuo.cn/doc/wkfbriqf.html>)
- [10] 네트워크 제품과 서비스 안전 심사 방법([http://www.cac.gov.cn/2017-02/04/c\\_1120407082.htm](http://www.cac.gov.cn/2017-02/04/c_1120407082.htm))
- [11] 네트워크 제품과 서비스 안전 심사 방법 관련 질의 및 응답([http://www.cac.gov.cn/2017-02/08/c\\_1120426803.htm](http://www.cac.gov.cn/2017-02/08/c_1120426803.htm))

- [12] 개인정보와 중요 데이터 경외 반출 안전 평가 방법([http://www.cac.gov.cn/2017-04/11/c\\_1120785691.htm](http://www.cac.gov.cn/2017-04/11/c_1120785691.htm))
- [13] 인터넷 정보 서비스 관리 방법([http://www.gov.cn/fwxx/bw/gjgbdydszj/content\\_2263004.htm](http://www.gov.cn/fwxx/bw/gjgbdydszj/content_2263004.htm))

## <저자 소개>

### 정 태 인 (Jung Taein)

정회원

1992년 2월 : 한양대학교 전기공학과 학사 졸업  
2000년 2월 : KAIST 전기및전자공학과 석사 졸업  
2000년 1월~2001년 6월 : 데이콤  
2001년 7월~현재 : 한국인터넷진흥원 수석연구원



관심분야: 개인정보보호, 정보보호

### 김 주 영 (Kim JuYoung)

정회원

2005년 8월 : 한양대 공학대학원 컴퓨터공학 석사 졸업  
2016년 8월 : 숭실대 IT정책경영학과 공학박사  
2001년 1월~2002년 3월 : 정보통신 교육원



2002년 4월~현재 : 한국인터넷진흥원 개인정보대응센터장  
관심분야: 개인정보보호, 정보보호

### 김 원 (Kim Weon)

1984년 2월 : 한양대학교 전자공학과 학사 졸업  
1989년 2월 : 한양대학교 일반대학원 전자공학과 석사 졸업  
2002년 8월 : 경희대학교 일반대학원 전자공학과 박사 졸업  
1989년 1월~1992년 6월 : 데이콤



1992년 7월~1999년 6월 : 한국전산원  
1999년 7월~현재 : 한국인터넷진흥원 개인정보보호 본부장  
관심분야: 개인정보보호, 정보보호