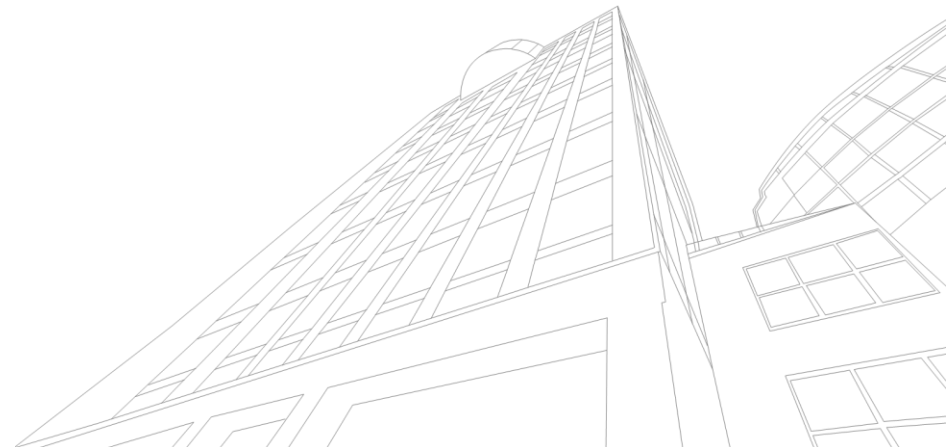


중국 정보통신망 보안법 주요내용 및 시사점

2017. 6. 1.

태충남(太忠男)
법무법인(율촌) 중국변호사



- I. 들어가는 말씀
- II. 정보통신망 보안법 주요내용
- III. 법규1-정보통신망 제품과 서비스
안전심사방법(시행)
- IV. 법규2- 개인정보와 중요데이터
국외송출보안평가방법(의견수렴안)
- V. 최근 동향
- VI. 시사점

중국법률체계 소개

현행 법률체계

- 전국인민대표대회 및 상무위원회 ----- 법률 ----- 정보통신망보안법
형법, 치안관리처벌법, 전자서명법
반테러법, 소비자보호법, 국가안전법
- 국무원 ----- 규정 ----- 컴퓨터정보시스템안전보호조례
인터넷정보서비스관리방법, 관건기초시설관련
- 지방인민대표대회 – 각 부처 ----- 지방규정 - 업종별 규정 - 인터넷안전보호기술조치규정
정보시스템안전등급보호기본요구
전신과 인터넷사용자개인정보보호규정
- 지방인민정부 ----- 지방정부법규



중국 정보통신망 보안법 주요내용

1. 적용대상



(1) 정의 규정:

- 정보통신망(网络):

컴퓨터 또는 기타 정보단말기 관련 설비로 구성된 일정한 규칙과 절차에 따라 정보에 대한 수집, 저장, 전송, 교환, 처리를 하는 시스템.

- 정보통신망 보안(网络安全):

필요한 조치를 통해 정보통신망에 대한 공격, 침입, 간섭, 파괴 내지 불법상용과 돌발사고를 방지하여 정보통신망이 안정적이고 또 믿을 수 있는 운영 상황을 유지하도록 하고 정보통신망 데이터의 완전성, 비밀유지성, 가용성의 능력을 보장하는 것.

- 정보통신망 운영자(网络运营者):

정보통신망의 소유자, 관리자와 정보통신망 서비스 제공자.

- 정보통신망 데이터(网络数据):

정보통신망을 통해 수집, 저장, 전송, 처리 및 생산되는 각종 전자 데이터.



(1) 정의 규정:

- **개인정보(个人信息):**

전자 또는 기타 방식으로 기록된 단독 또는 다른 정보와 결합하여 자연인 개인의 신분을 식별할 수 있는 각종 정보로서 이에겐 자연인의 성명, 출생일자, 신분증번호, 개인의 식물식별정보, 주소, 전화번호 등을 포함하나 이에 한하지 않는 것.

- 국민개인정보(公民个人信息) 개념에서 발전
- 단독 또는 다른 정보와 결합하여 식별할 수 있는 사용자의 서비스 사용의 사건 및 장소 등 정보는 불 포함되어 2013년 <전신과 정보통신망 이용자 개인정보보호규정>보다 범위가 다소 좁음.



(2) 적용대상:

- 중국 내에 건설, 운영, 유지 및 사용되는 정보통신망과 그 안전에 관한 감독 관리에 대하여 본 법이 적용됨(법 제2조)
- 앞에서의 정보통신망의 정의에 의하면, 일정한 물리적 존재를 전제하고 있는 개념임.
- 즉 법의 적용대상인 정보통신망은 반드시 중국 내의 물리적 설비에 의존해야 함.
- 국외에 있는 정보통신망에 대하여서는 그 정보통신망이 중국의 법률이나 행정법규에서 금지하는 정보를 발표하거나 전송하는 경우 관련기구에 통지하여 기술적으로 또는 기타 조치를 취하여 그 전달을 차단할 수 있음(법 제50조).
- 해외에서의 관건정보기초시설에 대하여 침입 또는 공격하는 행위에 대하여 법적 책임을 추궁하며, **중국내 자산동결** 등 제재조치를 취할 수 있음(법 제75조)

2. 보안등급 보호제도 실시



국가의 보안등급보호제도 실시 의무주체자: 운영자

- 중국 정부는 정보통신망의 보안등급보호제도를 실시함. 운영자는 보안등급보호제도의 요구에 맞게 보안보호의무를 이행하여야 함.
- (1) 내부 보안관리제도 실시와 실시규정을 제정하고 보안 책임자를 확정하여 보안보호책임을 실시. (2) 바이러스와 사이버공격, 침입 등 보안을 해치는 행위에 대하여 기술적 조치를 취함. (3) 운영상태를 모니터링 및 기록하고, 보안사건에 대하여 기술적 조치를 취하고 관련 정보통신망 일지를 6개월 이상 보존함. (4) 데이터 분류, 중요 데이터 백업조치와 암호화 조치 실시.(법 제21조)
- 현재 입법현황
처음으로 규정한 것이 아님, 2007년公安部 등 기관에서 발표한 <정보보안등급보호관리방법>(信息安全等级保护管理办法) 제7조에서 5개 등급으로 나누고, 정보시스템보안등급보호실시 가이드라인에 따라 등급보호 업무를 실시하고 있음. 처음으로 법률형태로 보안등급제도를 규정하였다는데 의미가 있음. 다만 구체적인 방법과 표준에 관한 규정이 아직 없어 기존 보안등급보호제도에 따라 운영될 수 밖에 없음.

3. 핵심정보기반시설에 대한 보호



(1) 의미 및 운영자의 강화된 의무

- 국가는 공공통신과 정보서비스, 에너지, 교통, 수계, 공공서비스, 전자정부 등의 중요한 산업과 영역, 그리고 일단 파괴되거나 기능을 상실하여 데이터가 유실되면 국가안전, 국민경제생활, 공공이익에 피해가 큰 핵심정보기반시설에 대해 정보통신망 보안등급 보호제도의 기초 위에 중점적인 보호를 실시 함. 구체적인 핵심정보기반시설의 범위와 보안방법에 대하여 국무원이 별도로 제정.
- 국가는 핵심정보기반시설 이외의 정보통신망 운영자가 자발적으로 핵심정보기반시설 보호시스템에 참여하는 것을 장려함.
- 운영자의 강화된 추가 의무(제34조):
 - 특별 보안관리기구와 보안관리 책임자를 배치하고 보안경력 심사
 - 종사자에 대하여 정기적으로 보안교육, 기술훈련, 기능평가 실시
 - 중요한 시스템과 데이터에 대해 재해 대비 백업자료 준비
 - 보안사건 응급대응방안 제정하고 정기적으로 훈련을 실시



(2) 운영자의 구매행위, 국내 저장 원칙, 정기검측 의무

- **구매행위 관련**
- 정보통신망 제품과 서비스를 구매할 때 **국가안전에 영향을 미칠 가능성이 있는 경우** 국가의 인터넷 정보부문, 국무원 관련 부분이 조직한 국가안전 심사를 통과하여야 함(법 제35조)
- **관련 정보의 중국 내 저장원칙**
- 핵심정보기반시설 관련 정보의 중국 내 저장원칙을 명확히 규정하고 있음.
- 반드시 중국 내 저장하여야 함.
- 업무상 외국에 저장할 필요가 있을 경우 안전평가를 받아야 함.
- **위반할 경우:** 시정명령, 위법소득 몰수, 5만위안 이상 50만 이하의 과징금 부과, 업무 잠정중단, 영업중지 정비, 사이트 폐쇄, 영업허가 말소, 직접 책임 실무자 등에 1만위안 이상 10만위안 이하 과징금 부과 등(법 제66조)
- 자체적 또는 보안서비스기구에 위임하여 매년 최소 1회 이상 모니터링 평가 실시

4. 개인정보보호제도의 개선



(1) 운영자의 개인정보 보호의무

- **비밀유지의무** 및 건전한 이용자 정보 보호제도 건립(법 제40조)
- 수집 및 사용한 개인정보는 합법, 정당, 필요의 원칙에 부합, 수집 및 사용 규칙을 **공개**, 목적과 범위, 방식을 명시, 피수집인의 **동의**를 받아야 함(법 제41조)
- 서비스와 **무관**한 개인정보를 수집할 수 없으며, 법 위반 또는 쌍방약정 위반하면서 개인정보를 수집 및 사용하여서는 아니 됨.
- 누설, 임의변경, 훼손하여서는 아니 되며, 피수집인의 동의 없이 **타인에게 정보를 제공**할 수 없음. 필요한 조치를 취하여 개인정보의 안전을 확보하여야 하고, 누설, 훼손, 분실을 방지하여야 함. 누설 사고 발생 시 즉시 보안조치를 취하고 이용자에게 **고지**하고, 관련 부문에 **보고**하여야 함(법 제42조)
- 개인이 운영자가 위법으로 개인정보를 수집 및 사용하는 것을 발견한 경우 **삭제를 요구**할 권리가 있고, 잘못된 정보에 대하여 **수정을 요구**할 권리가 있음(법 제43조)



(2) 개인정보의 불법적인 획득 및 거래 금지

- 어떠한 개인이나 조직도 개인정보를 **절취 또는 기타 불법적인 방법**으로 획득해서는 아니되며, **불법 판매** 또는 다른 사람에게 제공하여서는 아니됨.
- 처벌조항:
- 범죄에 해당 되지 않을 경우 중국 **공안기관**은 위법소득 몰수, 위법소득의 1 배이상 10배 이하의 과징금을 부과, 소득이 없는 경우 100만위안 이하의 과징금을 부과(법 제64조)

5. 인터넷 실명제 실시



의미 및 위반책임

- 최초로 법률 수준에서 인터넷 실명제도를 규정하였음.
- 의무 주체: 정보통신망 운영자
- 행위:
 - (1) 이용자를 위하여 정보통신망으로의 접속, 도메인등록 서비스, 가정용전화 신청, 모바일전화 등을 통해 정보통신망으로의 **접속 절차**를 진행할 때
 - (2) 이용자에게 정보의 발표, 인스턴트 메시지 등 서비스를 제공하면서 이용자와 **계약을 체결하거나 서비스 제공 확인**을 받을 때
- 위반책임:
 - 위반 시 시정명령, 거절 하거나 상황이 심각할 경우 5만원 이상 10만원 이하의 과징금 부과, 관련 업무의 잠정중단, 영업중지 정비, 사이트폐쇄, 영업허가 말소, **직접 실무책임자**에 대하여 1만원 이상 10만원 이하 과징금 부과할 수 있음.

6. 정보통신망 이용자의 의무



- 어떠한 개인이나 조직도 스스로 정보통신망을 사용하는 행위에 대하여 책임을 져야 하며, 사기, 범죄방법의 전수, 금지물품, 통제물품 등의 제작 또는 판매 등의 위법한 범죄활동에 이용되는 사이트, 단체 채팅방을 개설해서는 아니 되고, 이러한 정보를 반포하여서도 아니 됨(법 제46조)
- 어떠한 개인이나 조직이 발송한 전자정보, 제공하는 어플 소프트웨어에는 악성 프로그램을 설치하여서는 아니 되며 법규에서 전송을 금지하는 정보가 포함되어서는 아니 됨(법 제48조)

7. 정보통신망 제품 또는 서비스에 대한 요구사항



- 정보통신망 제품과 서비스는 **국가 표준의 강행규정**에 부합하여야 하고 정보통신망 제품, 서비스의 제공자는 **악성 프로그램을 설치**하여서는 아니 됨
- 보안상 결함이나 공백 등의 위험이 있는 경우 **즉시** 이를 **보안하는 조치**를 취하고 규정에 따라 즉시 이용자에게 **고지**하고 주관부문에 **보고**하여야 함(법 제22조)
- 지속적인 보안유지를 하여야 하고, **약정한 기한 내에 보안유지업무를 종료**하여서는 아니 됨.
- 이용자의 정보를 수집하는 경우 **개인정보보호 관련 규정 준수**하여야 함.
- 정보통신망 핵심설비와 보안 전문제품은 국가 표준의 강행규정에 부합해야 하고, 자격을 갖춘 **보안인증합격 또는 보안검사 요건**에 부합한 후에야 비로서 판매 또는 제공 가능
- 중국 인터넷정보부문은 국무원 기타 부문과 핵심설비와 보안 전문제품 목록을 제작 및 공포하고, 보안인증과 보안검사결과를 서로 사용할 수 있게 하여 중복 인증이나 검사를 피하게 함(법 제23조)

정보통신망 제품과 서비스 안전심사방법(시행)

《网络产品和服务安全审查办法（试行）》

주요 내용

위원회설립

- 정보통신망 안전심사 위원회(网络安全审查委员会)

국가안전과 관련된 정보통신망과 정보시스템 구매의 중요한 정보통신망제품과 서비스는 반드시 정보통신망 안전심사를 받아야 함.

국가 인터넷정보사무실은 관련 부문과 같이 안전심사위원회를 설립하고, 해당 위원회는 안전심사의 중요정책을 심의하고, 안전심사업무를 실시하는 주관부서가 될 것임.

외부에서 전문가를 초빙하여 안전심사 전문가 위원회를 만들어 제3기관의 평가에 대하여 안전리스크 및 제공자의 안전신임(安全可信) 사항을 종합평가를 하게 됨.

주요 내용

실시영역

금융, 전신, 에너지, 교통 등 중점업종과 영역에서는 주관부문이 안전심사업무요구에 따라 자체 업종과 영역 내에서의 정보통신망 제품과 서비스 안전심사업무를 전개함.

공공통신과 정보서비스, 에너지, 교통, 수계, 공공서비스, 전자정부 등의 중요한 산업과 영역 및 기타 관건정보기초시설의 운영자가 정보통신망 제품과 서비스를 구매할 때 국가안전에 영향이 있을 경우 안전심사를 반드시 받아야 함. 국가안전에 영향이 있는지 여부는 업무부서에서 확정함.

본 규정은 2페이지 임. 내용이 매우 추상적이고 구체적인 심사방법 및 제출자료 등이 명시되지 않고 있음.



개인정보와 중요데이터 국외송출보안평가방법(의견수렴안)

《个人信息和重要数据出境安全评估办法（征求意见稿）》

데이터 국외송출이란

정의

- 운영자가 중국 경내에서 정보통신망 운영 중에 수집 내지 생산한 개인정보와 중요한 데이터를 국외에 있는 기구, 조직, 개인에게 제공하는 행위임.

데이터의 국내 보존 원칙:

반드시 중국 내에서 보존하여야 함. 다만 업무상의 필요에 따라 국외 제공이 필요한 경우 보안평가를 받아야 함. 개인이나 기타 조직이 중국 내 수집 내지 생산한 개인정보 및 중요한 데이터의 국외 송출에 대한 보안평가 업무에도 준용됨.

개인정보의 국외송출은 개인정보의 주체에게 데이터의 송출의 목적, 범위, 내용, 수신처와 수신처 소재국가 또는 지역을 설명하고, 동의를 얻어야 함.

위법행위 처벌: 어떠한 개인과 조직은 위법행위에 대하여 중국 인터넷정보부서,公安부서에 고발권리가 있음. 관련 법규에 따라 처벌할 수 있음.

보안평가의 내용

평가대상

- 국외송출의 필요성
- 개인정보 관련하여 수량, 범위, 유형, 민감정도, 동의여부 등
- 중요데이터 관련하여 수량, 범위, 유형과 그 민감정도 등
- 데이터 수신처의 보안보호 조치, 능력, 수준, 소재지 국가와 지역의 정보통신망 보안 환경 등
- 국외송출과 재이전 후 해당 정보가 누설, 훼손, 임의수정, 남용 될 수 있는 리스크
- 데이터 국외송출과 누적이 국가안전, 사회공공이익, 개인 합법적인 이익에 가져올 수 있는 리스크 등

보안평가의 내용

사전보안평가 신청 대상

- 50만명(누적 인원 포함) 이상의 개인정보의 국외 송출
- 데이터 용량이 1000GB를 초과하는 경우
- 핵시설, 화학물질, 국방군사공업, 인구건강 등 영역의 데이터, 대형공정활동, 해양환경과 민감한 지리 정보 등의 데이터
- 핵심정보기초시설의 시스템상의 공백이나 보안 방호 등의 정보통신망 보안 관련 정보
- 핵심정보기초시설 운영자가 국외로 제공하는 개인정보와 중요데이터
- 국가안전과 사회공공이익에 영향을 미칠 수 있는 사항으로 업종주관부서 또는 감독관리부서에서 평가를 해야 한다고 판단되는 부분

업종주관부서 또는 감독관리부서가 보안평가를 조직하여 실시할 경우 60영업일 내 완성하고 운영자에게 적시에 피트백을 주고 국가 인터넷정보부서에 보고하여야 함.
주관부서 또는 감독관리부서가 불명확할 경우 국가 인터넷정보부서에서 평가를 함.

국외송출이 금지되는 정보

금지사항

- 개인정보의 국외 송출이 개인정보 주체의 동의를 받지 못한 경우이거나 개인의 이익을 침해하는 경우
- 데이터 국외송출이 국가 정치, 경제, 과학기술, 국방 등의 안전에 리스크를 가지고 있을 수 있어 국가 안전, 사회공공이익에 영향을 끼칠 수 있는 경우
- 국가 인터넷 정보부서,公安부서, 안전부서 등 관련 부서에서 국외송출이 불가능하다고 판단한 경우

국외송출 보안평가의 1차적인 책임은 운영자에게 있고 매년 1회의 보안 평가를 실시하고 적시에 평가상황을 주관부서에 보고하여야 함.

비교적 변경 사항이 있을 경우에는 다시 보안평가를 실시하여야 함.



최근 동향



최근 동향

• 중국 내 반응

- 사이트 해킹, 인터넷 범죄, 경제적 피해 약 7000억위안, 랜섬웨어 악성코드사례 발생- 보안 취약성과 보안관리의 필요성 대두
- 인터넷은 사적공간이 아니라 공적인 공간이라는 의견, 긍정적인 여론반응
- 하지만 아직 체계적이고 구체적인 법인 아니라는 의견이 있음
- 올해부터 미시적인 법규들이 제정될 것임. 예를 들면 온라인 쇼핑몰 플랫폼, 개인정보보호 및 소셜미디어 안전에 대한 규정



중국 정부 동향

- 법 홍보 및 사이버 보안인식 제고를 위한 다양한 활동 진행
각 부처 실무자 및 담당자 260명 대상 특강 (중국 중앙인터넷 안전과 정보화팀, 2017년 3월 30일)
- 일반시민 대상 카툰 동영상 관람, 법 홍보, 설문조사
- 교육기관에서는 각 교육처에 법 홍보 교육 강화 통지문 배포
- 公安部, 사이버 보안법의 원활한 집행과 점검을 위해 3월-9월까지 정기적인 회의를 통하여 점검 실시.

최근 동향

• 중국기업에 미치는 영향 및 동향

- 중국 사이버 보안산업이 고속 성장의 기회를 맞이할 것,
- 향후 3-5년간 연 평균 25~30%의 성장을 예상
- 사이버 보안 분야의 투자가 현재 전체 IT분야의 2%에서 10%로 성장할 것,
- 특히 보안 솔루션, 보안 인력 교육, 보안 하드웨어 분야 투자가 집중
- 다만 대형 포털 업체 등 고민, 가입자 가 수억명 됨. 최대한 협조



해외 동향:

- 세계 46개 상공단체와 글로벌 기업들의 거센 반발
초안, 리커창 총리 서한, 자국기업에만 혜택 제공, 외국기업 차별
구글, 페이스북, 트위터 차단, 미디어와 IT기업의 상황도 악화,
회사운영의 정보유출 우려,
- 사생활 침해 및 표현의 자유 침해 우려, 인권 측면에서의 비판
회사들에게 검열을, 사용자에게는 개인정보를 강요라는 비판
미국과 유럽 아시아기업들을 대표하는 상공단체 법 시행 연기
요청(5.16)



시사점



중국 정보통신망 보안법 주요 요구

법 규정 요구	기업 과제
개인 정보는 반드시 안전하게 보호, 중국 내에 저장	완벽한 고객 데이터와 사행할 정보 보호 방안 구비여부
핵심업종(예를 들면 교통업) 반드시 정부가 수권하고 인가한 정보통신망 제품 및 서비스를 사용하여야 함.	IT전략기획과 IT구매관리 혁신 필요
중국정부는 정보통신망의 차단과 제한에 대하여 권리를 보류하고 있음	안심할 수 있게 지속적인 업무계획을 가지고 있는지 여부
중국 정부는 사용자데이터 및 기술방안에 대하여 검사권한을 가지고 있음(예를 들면 후문 프로그램)	결함에 대하여 유효하고 신속하게 대응할 능력이 있는지
핵심업종기업은 정기적으로 안전리스크 평가를 실시하여야 함	정기적으로 안전리스크평가가 이루어지고 있는지

향후 추세

시진핑의 총체적인 국가안전관에 대한 이해

- 2014년 4월 제기, <반테러법>, <국가안전법>, <통신정보망 보안법>
- 법률 차원에서의 법이 제정된 후 세부적인 법규들이 지속적으로 제정 및 실시되어 법 체계와 적용이 더욱 엄격해질 것으로 예상.
- 예를 들면, 안전검사, 차단, 검사, 특정구역 임시조치 등

개인정보 보호 점차 강화

이에 대한 이해와 적응 노력이 필요할 것으로 보임.

개인정보의 외국송출 규정 곧 발표

의견 수렴안이지만, 기업들의 업무에 상당한 영향을 줄 수 있음.



감사합니다



태충남 변호사

PH: 1350-115-0852

E-mail: taizhn@yulchon.com



법무법인(유)
율촌

서울특별시 강남구 테헤란로 518, 12층 (대치동)

Tel: 02-528-5200

Fax: 02-528-5228

<http://www.yulchon.com>