중국의 정보통신망보안법(网络安全法) 반포와 우리나라 기업에 대한 시사점

2016년 11월 7일 제12기 전국인민대표대회 상무위원회 제24차 회의에서 중화인민공화국 정보통신망 보안법(中国人民共和国网络安全法 , 이하 "본 법"이라고 약칭합니다)이 통과되었습니다. 본 법은 모두 7장, 79조로 이루어져 있고 그동안 세 번의 심의 과정을 거치면서 적지 않은 부분의 초안 내용이 수정을 거듭한 끝에 비로소 최종안이 이번에 통과되어 2017년 6월 1일부터 시행될 예정입니다. 본 법은 우선 중국에서 정보통신망의 보안 문제를 종합적으로 다루는 첫번째 법률이라는 측면에서 많은 시사점과 동시에 한계를 내포하고 있습니다. 본 뉴스레터에서는 본 법의 반포와 시행예정에 따라 그 주요내용과 우리나라 기업에 대한 시사점에 대해 말씀 드리고자 합니다.

I. 중국 정보통신망보안법의 주요 내용

1. 본 법의 적용대상

가. 본 법에서 사용되는 용어 정의

본 법에 사용되는 용어들의 정의를 먼저 살펴보면 다음과 같습니다.

(1) 정보통신망(网络)[1]은 "컴퓨터 또는 기타 정보단말기 관련 설비로 구성된 일

[1] 중국어 본문에는 网络라고 표현되는데 이 단어의 사전적 의미에 따른 번역은 통상 네트워크를 말합니다. 일부 번역에는 이를 인터넷이라고 표현하기도 하는데 중국의 다른 법률법규에서 별도로 인터넷 (互联网) 이라는 용어를 사용하는 경우도 있습니다. 한편 우리나라의 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 의하면 "정보통신망"이란 "「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의

정한 규칙과 절차에 따라 정보에 대한 수집, 저장, 전송, 교환, 처리를 하는 시스템",

(2) 정보통신망 보안이란 "필요한 조치들을 통해 정보통신망에 대한 공격, 침입, 간섭, 파괴 내지 불법사용과 돌발사고를 방지하여 정보통신망이 안정적이고도 믿을 수 있는 운영 상황을 유지하도록 하고 정보통신망 데이터의 완정성, 비밀유지성, 가용성의 능력을 보장하는 것",

(3) 정보통신망 운영자란 "정보통신망의 소유자, 관리자와 정보통신망 서비스 제공자",

(4) 정보통신망 데이터란 "정보통신망을 통해 수집, 저장, 전송, 처리 및 생산되는 각종 전자 데이터",

(5) 개인정보란 "전자 또는 기타 방식으로 기록된 단독 또는 다른 정보와 결합하여 자연인 개인의 신분을 식별할 수 있는 각종 정보로서 이에는 자연인의 성명, 출생일자, 신분증번호, 개인의 생물식별정보, 주소, 전화번호 등을 포함하나 이에 한하지 않는 것"을 각 의미합니다(법 제76조)

나. 본 법의 적용대상

중화인민공화국 국내에 건설, 운영, 유지 및 사용되는 정보통신망과 그 안전에 관한 감독 관리에 대해서 본법이 적용됩니다(법 제2조). 그리고 앞에서 설명한 정보통신망의 정의에 따르면 정보통신망은 일정한 물리적 존재를 전제하고 있는 개념입니다. 즉, 본 법의 적용대상인 정보통신망은 반드시 중국 국내의 물리적 설비에 의존해야

이용기술을 활용하여 정보를 수집・가공・저장・검색・송신 또는 수신하는 정보통신체제를 말한다."라고 규정하고 있는데 정보통신망이란 표현이 법률적 개념에서 중국의 网络와 가장 근접한 개념으로 사료되어 본문에서는 "정보통신망"이라는 표현을 사용하기로 합니다. 다만, 우리나라의 언어 환경에서는 정보통신망에 대해 네트워크, 사이버 등의 표현을 사용하는 경우도 많아 본 법의 조문에서 조문 규정의 배경이나 언어의 환경에 따라 정보통신망 보다는 인터넷(예, 인터넷 실명제, 网络实名制)으로 바로 표현하는 것이 더 이해에 용이한 부분도 있어서 그런 부분은 바로 인터넷이라고 표현하였습니다. 그리고 安全이라는 말도 보안이라는 말이 적절한 경우도 있고, 안전생산(安全生产)이라고 할 때에는 그대로 안전이라고 표현하는 것이 더 적절한 경우도 있어 언어환경에 따라 보안 또는 안전이라고 번역하였음을 미리 양해해 주시기 바랍니다.

합니다. 다시 말하면 일정한 주체가 완전히 중국 국외에서 중국 국외에 있는 정보통신망 시설을 통해 온라인 서비스를 제공하는 경우에는 정보통신망의 상호접속, 상호연동(互联互通)이라는 본질적인 성질로 인해 중국 국내에서 해당 서비스를 받을 수 있다고 하더라도 이러한 행위는 본 법의 적용범위가 아니게 됩니다. 이러한 국외의 정보통신망에 대해서는 그 정보통신망이 중국의 법률이나 행정법규에서 금지하는 정보를 발표하거나 전송하는 경우에는 관련 기구에 통지하여 기술적 또는 기타 조치를 취하여 그 전달을 차단시킬 수 있습니다(법 제50조). 한편 군사 정보통신망의 보안보호 문제는 중앙군사위원회가 별도로 규정하도록 하고 있어 본 법의 적용대상이 아닙니다(법 제78조).

2. 정보통신망 보안 등급 보호제도(网络安全等级保护制度)의 실시

가. 국가의 보안등급 보호제도 실시의무

국가는 정보통신망 보안등급 보호제도를 실시합니다. 정보통신망 운영자는 국가의 정보통신망 보안등급 제도의 요구에 맞게 아래의 보안보호의무를 이행해야 하고 정보통신망이 간섭을 받거나 파괴되거나 권한 없이 방문되는 것을 방지하고 정보통신망 데이터가 누설, 절취 또는 임의변경되는 것을 방지해야 합니다. ① 내부 보안 관리제도와 실시규정을 제정하고 정보통신망 보안 책임자를 확정하고 정보통신망 보안보호책임을 실시해야 합니다. ② 컴퓨터 바이러스와 정보 통신망의 공격, 정보통신망 침입 등의 정보통신망 보안을 해치는 행위에 대한 기술적인 조치를 취합니다. ③ 정보통신망의 운영 상태를 모니터링 및 기록하고, 정보통신망 보안사건에 대해 기술적인 조치를 취하고 규정에 따라 관련 정보통신망 일지를 6개월 이상 보존해야 합니다. ④ 데이터 분류, 중요 데이트 백업조치와 암호화 등의 조치를 합니다. ⑤ 법률, 행정법규가 규정한 기타 의무(법 제21조)를 이행해야 합니다.

나. 정보통신망 보안등급 보호제도의 현재 입법 현황

본 법이 규정한 정보통신망 보안등급 보호제도는 본 법에 처음 규정된 것은 아닙니다. 이미 공안부, 국가비밀유지국, 국가비밀번호 관리국 국무원 정보화 업무 사무처 등의 기관이 2007년에 제정한 정보보안등급보호관리방법(信息安全等级保护管理办法)

제7조는 정보 시스템의 보안보호 등급을 5등급으로 나누어 정보시스템을 운영, 사용하는 조직은 정보시스템보안등급보호실시 가이드라인(信息系统安全等级保护实施指南)에 따라 구체적으로 등급보호 업무를 실시할 것을 규정하였습니다. 정보시스템 건설이 완성된 이후에는 이를 운영 내지 사용하는 조직 또는 그 주관부문은 해당 방법이 규정한 조건에 부합하는 평가기구를 선택하여 정보시스템 보안등급보호평가 요건 등의 기술표준에 따라 정기적으로 정보시스템 보안등급 상황에 대한 등급 측정을 실시하고 상응하는 신고 절차를 이행하도록 하였습니다. 본 법은 최초로 법률의 형식으로 국가의 정보통신망 보안등급 보호제도를 규정하였다는데 의미가 있습니다. 그러나 본 법은 등급보호제도에 관한 구체적인 방법과 표준에 관한 규정이 없습니다. 따라서 상당 기간 동안은 여전히 기존에 제정된 보안등급 보호제도에 따라 제도가 운영될 수 밖에는 없을 것으로 보입니다.

3. 핵심정보기반시설(关键信息基础设施)에 대한 보호

가. 핵심정보기반시설의 의미

국가는 공공통신과 정보 서비스, 에너지, 교통, 수계, 금융, 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 실시합니다. 구체적인 핵심정보기반시설의 구체적인 범위와 보안보호 방법에 대해서는 국무원이 별도로 제정을 하게 하였습니다. 국가는 핵심정보기반시설 이외의 정보통신망 운영자가 자발적으로 핵심정보기반시설 보호시스템에 참여하는 것을 장려합니다(법 제31조).

나. 핵심정보기반시설 운영자의 의무

(1) 핵심정보기반시설 운영자의 강화된 의무

핵심정보기반시설은 목적사업이 안정적이고 지속적으로 운영될 수 있게 지원하는 기능을 가져야 하고 보안기술조치와 함께 규획, 건설, 사용될 수 있게 해야 합니다(법 제33조). 일반적인 정보통신망 운영자의 의무에 추가하여 핵심정보기반시설 운영자는 아래의 추가적인 보호의무를 이행해야 합니다. ① 특별 보안관

리기구와 보안관리 책임자를 배치하고 책임자와 핵심직책의 인원에 대해서는 보안경력 심사를 해야 합니다. ② 종사자에 대한 정기적인 정보통신망 보안교육, 기술훈련과 기능평가를 실시해야 합니다. ③ 중요한 시스템과 데이터에 대해 재해에 대비한 백업자료를 준비해야 합니다. ④ 정보통신망 보안사건 응급대응방안을 제정하고 정기적인 훈련을 실시해야 합니다. ⑤ 법률, 행정법규에 규정한 기타 의무(법 제34조)를 이행해야 합니다.

(2) 핵심정보기반시설 운영자의 구매행위 관련 의무

그리고 핵심정보기반시설의 운영자가 정보통신망 제품과 서비스를 구매할 때 국가안전에 영향을 미칠 가능성이 있는 경우에는 국가의 인터넷 정보부문, 국무원 관련 부문이 조직한 국가안전심사를 통과해야 하며(법 제35조), 이 때에는 규정에 따라 제공자와 보안 비밀유지 계약을 체결하고 보안, 비밀유지의무와 책임을 명확하게 해야 합니다(법 제36조).

(3) 핵심정보기반시설 관련 정보의 국내 저장원칙

핵심정보기반시설 관련 정보의 국내 저장 원칙을 명확하게 규정하였습니다. 핵심정보기반시설의 운영자는 중화인민공화국 국내에서 운영 중에 수집과 생성된 개인정보와 중요 데이터를 반드시 국내에 저장해야 합니다. 업무상 필요에 의하여 국외에 제공이 필요한 경우에는 국가 인터넷 정보부문과 국무원 관련 부문이 제정한 방법에 따라 평가를 진행하고 법률, 행정법규에 다른 규정이 있는 경우는 그에 따릅니다(법 제37조). 한편 이와 같은 규정에 위반하여 국외에 정보통신망 데이터를 저장하거나 국외로 정보통신망 데이터를 전송한 경우에는 관련주관 부분은 시정을 명하고 경고를 하며 위법한 소득을 몰수하며 5만 위안 이상 50만 위안 이하의 과징금에 처하며 관련업무의 잠정중단, 영업중지 정비, 사이트 폐쇄, 관련 영업허가 또는 영업집조의 말소를 할 수 있고, 직접적인 책임이 있는 실무책임자와 기타 직접책임자에 대해서도 1만 위안 이상 10만 위안 이하의 과징금에 처합니다(법 제66조).

(4) 핵심정보기반시설의 운영자의 정기검측 의무

핵심정보기반시설의 운영자는 자체적으로 또는 정보통신망 보안서비스 기구에 위임을 하여 정보통신망의 보안성과 혹시나 존재할 수 있는 위험에 대해서 매년 최소 한 차례 이상의 모니터링 평가를 실시해야 합니다. 이러한 모니터링 평가의 상황과 개선 조치들에 대해서는 관련 핵심정보기반시설의 보안보호관련 부문에 보고를 해야 합니다(법 제38조).

다. 핵심정보기반시설 관련 정부부문의 책임

(1) 국가 인터넷 정보부문의 조치의무

국무원의 규정에 따른 직무 분담에 따라 핵심정보기반시설의 보안보호 작업을 하는 부문은 각 해당산업, 해당영역에서의 핵심정보기반시설 보안규획을 편제 및 조직하고 핵심정보기반시설의 안전운영과 보호작업을 지도 및 감독합니다(법 제32조). 국가 인터넷 정보부문은 관련 부문과 통합 협조를 통해 핵심정보기반시설의 보안보호에 대하여 아래와 같은 조치들을 취해야 합니다. ① 핵심정보기반시설의 보안위험에 대한 선별 검측을 실시하고 개선 조치를 추진하며 필요한 경우에는 정보통신망 보안 서비스 기구에 위임하여 정보통신망에 존재하는 보안위험에 대해 검측, 평가를 실시합니다. ② 정기적으로 핵심정보기반시설의 운영자에 대해 정보통신망 보안 응급훈련을 조직하여 정보통신망 사건에 대한 대응 수준과 협조, 지원 능력을 제고합니다. ③ 관련부문, 핵심정보기반시설 운영자, 관련 연구기구, 정보통신망 보안서비스 기구간에 정보통신망 보안 정보를 공유하게 합니다. ④ 정보통신망 보안사건의 응급처리와 정보통신망 기능의 회복 등에 대해 기술 지원과 협조를 제공합니다(법 제39조).

(2) 해당업종의 현실을 반영한 보안보호업무 수행

핵심정보기반시설의 보안보호 업무의 책임 부분은 해당업종, 해당영역의 건전한 정보통신망 보안모니터링 예비경보와 정보통보제도를 건립하고 규정에 따라 정보통신망 보안모니터링 예비경보 정보를 보고합니다(법 제52조). 국가 인터넷 정보 부문은 관련 부문과 협조하여 온전한 정보통신망 보안평가와 응급업무 메카니즘를 수립하고 정보통신망 보안사건 응급대응방안을 제정하고 정기적으로 모

의훈련을 조직합니다(법 제53조 제1항). 핵심정보기반시설 보안보호 업무의 책임 부문은 각 해당업종, 해당영역의 정보통신망 보안사건 응급대응방안을 제정하고 정기적으로 모의훈련을 조직합니다(법 제53조 제2항). 정보통신망 보안사건 응급대응방안은 마땅히 사건 발생후의 위험의 정도, 영향의 범위 등 요소에 따라 정보통신망 보안 사건에 대해 등급을 매기고 상응하는 응급처치 조치를 규정해야 합니다(법 제53조 제3항).

4. 개인정보 보호제도의 개선

가. 본 법의 개인정보의 범위에 관하여

본법은 개인정보를 "전자 또는 기타 방식으로 기록된 단독 또는 다른 정보와 결합하여 자연인 개인의 신분을 식별할 수 있는 각종 정보로 이에는 자연인의 성명, 출생일자, 신분증번호, 개인의 생물식별정보, 주소, 전화번호 등을 포함하나 이에 한하지 않는다"라고 규정하고 있습니다. 이미 반포되어 있는 개인정보보호 관련 법률 법규와 마찬가지로 개인 정보의 "식별가능성"을 강조하고 있습니다. 본 법이 규정하고 있는 개인정보의 범위는 일응 상당히 광범위 해 보이나 2013년에 반포된 전신과 정보통신망 이용자 개인정보보호규정(电信和互联网用户个人信息保护规定)과 비교해 보았을 때 본 법의 개인정보의 범위에는 단독 또는 다른 정보와 결합하여 이용자가 사용하는 서비스의 사건, 장소등의 정보는 개인정보의 개념에서 제외되어 있어서 이 점에서는 범위가 좁다고도 할 수 있습니다.

나. 정보통신망 운영자의 개인정보 보호의무

정보통신망 운영자는 수집한 이용자의 정보에 대해 비밀유지를 철저히 해야 하며 건전한 이용자 정보 보호제도를 건립해야 합니다(법 제40조). 정보통신망 운영자가 수집, 사용한 개인정보는 합법, 정당, 필요의 원칙에 부합해야 하고 수집, 사용규칙을 공개하고, 정보를 수집, 사용하는 목적, 방식과 범위를 명시하며 피수집인의 동의를 구해야 합니다(법 제41조). 정보통신망 운영자는 그가 제공하는 서비스와 무관한 개인정보를 수집해서는 안되고 법률, 행정법규의 규정, 쌍방의 약정을 위반하여 개인정보를 수집, 사용해서는 안되며 법률, 행정법규의 규정과 이용자와의 약정에

따라 그 보존하는 개인정보를 처리해야 합니다(법 제41조). 또한 정보통신망 운영자는 수집한 개인정보를 누설, 임의변경, 훼손해서는 안되고 피수집인의 동의 없이는 다른 사람에게 그 개인정보를 제공해서는 안됩니다. 다만 일정한 처리를 거쳐 특정 개인이 식별되지 않고 원상회복이 불가능한 경우는 예외로 합니다. 정보통신망 운영자는 기술적인 조치와 기타 필요한 조치를 통해 그 수집한 개인정보의 안전을 확보해야 하고 정보누설, 훼손, 분실을 방지해야 합니다. 개인정보의 누설, 훼손, 분실 상황이 발생 또는 발생할 가능성이 있는 경우에는 즉시 보완조치를 취해야 하고 규정에 따라 적시에 이용자에게 고지하고 관련부문에 보고해야 합니다(법 제42조). 개인이 정보통신 운영자가 법률, 행정법규의 규정 또는 쌍방 약정을 위반하여 본인의 개인정보를 수집, 사용하는 것을 발견한 경우에는 정보통신망 운영자에게 개인정보의 삭제를 요구할 권리가 있고, 정보통신 운영자가 수집, 저장한 본인의 개인정보가 잘못된 것일 때에는 정보통신망 운영자에게 수정을 요구할 권리가 있습니다. 정보통신망 운영자는 적절한 조치를 취하여 이를 삭제 또는 수정하여야 합니다(법 제43조).

다. 개인정보의 불법적인 획득 및 거래 금지

어떠한 개인이나 조직도 개인정보를 절취 또는 기타 불법적인 방법으로 획득해서는 안되며 불법적으로 판매하거나 다른 사람에게 제공해서는 안됩니다(법 제44조). 위 규정에 위반하여 개인정보를 절취 또는 기타의 불법적인 방법으로 획득하거나 불법 판매 또는 불법적으로 다른 사람에게 제공한 경우에 그러한 상황이 범죄에 해당되지 않는 경우에는 공안기관이 위법한 소득을 몰수하고 위법한 소득의 1배 이상 10배 이하의 과징금에 처하며 위법한 소득이 없는 경우에는 100만 위안 이하의 과징금에 처합니다(법 제64조 제2항).

5. 인터넷 실명제(网络实名制)의 실시

가. 인터넷 실명제의 의미

본 법은 최초로 법률 수준에서 인터넷 실명제도를 규정하였습니다. 정보통신망 운영자가 이용자를 위해 정보통신망으로의 접속, 도메인등록 서비스, 가정용전화 신청,

모바일 전화 등을 통해 정보통신망으로의 접속 절차를 진행할 때 또는 이용자에게 정보의 발표, 인스턴트 메시지 등의 서비스를 제공하면서 이용자와 계약을 체결하거나 서비스 제공 확인을 받을 때에는 이용자에게 진실된 신분 정보를 요청해야 하고 이용자가 진실한 신분정보를 제공하지 않으면 정보통신망 이용자는 관련 서비스를 제공해서는 안됩니다. 국가는 정보통신망에서 신뢰 가능한 신분 확인 정책을 시행하고 안전하고 편리한 전자 신분 인증 기술의 연구개발을 지원하며 서로 다른 전자신분 인증방법간의 상호 인증을 추진합니다(법 제24조).

나. 인터넷 실명제 위반에 대한 책임

정보통신망 운영자가 인터넷 실명제에 위반하여 이용자에게 진실한 신분정보를 요구하지 않거나 진실한 신분정보를 제공하지 않은 사람에게 관련 서비스를 제공한 경우에는 관련부문이 우선 시정을 명령하고 시정을 거절하거나 상황이 심각한 경우에는 5만 위안 이상 10만 위안 이하의 과징금에 처하고 관련부문은 관련업무의 잠정중단, 영업중지 정비, 사이트 폐쇄, 관련 영업허가 또는 영업집조의 말소를 할 수 있으며, 직접적인 책임이 있는 실무책임자와 기타 직접책임자에 대해서 1만 위안 이상 10만 위안 이하의 과징금에 처합니다(법 제61조).

6. 정보통신망 이용자의 의무

어떤 개인이나 조직도 스스로 정보통신망을 사용하는 행위에 대해 책임을 져야 하며 사기, 범죄방법의 전수, 금지물품, 통제물품 등의 제작 또는 판매 등의 위법한 범죄활동에 이용되는 사이트, 단체 채팅방을 개설해서는 안되고 정보통신망을 이용해서 사기, 금지물품, 통제물품 등의 제작 또는 판매와 기타 위법한 범죄활동의 정보를 반포해서는 안됩니다(법 제46조). 또한 어떠한 개인이나 조직이 발송한 전자정보, 제공하는 어플 소프트웨어에는 악성 프로그램을 설치해서는 안되고 법률, 행정법규가 반포 혹은 전송을 금지하는 정보를 포함해서는 안되며(법 제48조), 전자정보 발송 서비스 제공자와 어플 다운로드 서비스 제공자는 보안관리의무를 이행해야 하고 이용자가 위와 같은 위법한 행위를 하는 것을 알았을 때에는 서비스 제공을 중단하고 제거하는 등의 처리조치를 취하고 관련 기록을 보존하며 관련 주관부문에

보고해야 합니다(법 제48조).

7. 정보통신망 제품 또는 서비스에 대한 요구사항

정보통신망 제품과 서비스는 국가 표준의 강행규정에 부합하여야 하고 정보통신망 제품, 서비스의 제공자는 악성 프로그램을 설치해서는 안됩니다. 그리고 그 정보통신망 제품 서비스에 보안상의 결함이나 공백 등의 위험이 있는 경우에는 즉시 이를 보완하는 조치를 취해야 하고 규정에 따라 즉시 이용자에게 고지하고 주관부문에 보고해야 합니다(법 제22조). 또한 해당 제품, 서비스에 대해 지속적으로 보안 유지를 해야 하고 규정 또는 당사자가 약정한 기한 내에 보안 유지업무를 종료해서는 안됩니다. 또한 정보통신망 상품과 서비스가 이용자의 정보를 수집하는 기능이 있는 경우에는 그 제공자는 이용자에게 명시적인 동의를 구해야 하며 이용자의 정보와 관련이 있는 경우에는 본 법과 관련법률, 행정법규의 개인정보 보호에 관한 규정을 준수해야 합니다. 정보통신망 핵심설비와 정보통신망 보안 전문 제품은 국가 표준의 강행규정에 부합해야 하고 자격을 갖춘 기구의 보안인증합격 또는 보안검사 요건에 부합한 후에야 비로소 판매 또는 제공이 가능합니다. 국가의 인터넷 정보 부문은 국무원 관련 부문과 함께 정보통신망 핵심설비와 정보통신망 보안 전문제품 목록을 제작, 공포하고 보안인증과 보안검사결과를 서로 사용할 수 있게 하여 중복 인증이나 검사를 피하게 합니다(법 제23조).

8. 국가의 정보통신망 보안과 관련한 의무

가. 보안모니터링 예비경보와 정보통보제도(网络安全监测预警和信息通报制度)의 수립

국가는 정보통신망 보안모니터링 예비경보와 정보통보제도를 수립합니다. 국가의 인터넷 정보 부문은 관련 부분과 통합 협조하여 정보통신 보안정보의 수집, 분석과 통보 작업을 하고 규정에 따라 통일된 정보통신망 보안모니터링 예비경보 정보를 반포합니다(법 제51조). 정보통신망 보안사건의 위험이 증가할 때에는 성급 이상 인민정부 관련 부문은 규정된 권한과 절차에 따라 정보통신망 보안 위험의 특징과 발생 가능한 위험에 따라 아래와 같은 조치들을 취해야 합니다. ① 관련부문과 기구,

인원에 대해서 즉시 관련 정보의 수집, 보고를 요청하고 정보통신망 위험의 모니터링을 강화해야 합니다. ② 관련부문, 기구, 전문인원을 조직하여 정보통신망 위험정보에 대해 분석, 평가를 진행하고 사건 발생의 가능성, 영향범위와 위험 정도를 예측해야 합니다. ③ 일반에 정보통신망 보안위험 예비경보를 발령하고 위험을 회피, 감경할 수 있는 조치들을 반포합니다(법 제54조).

나. 정보통신망 보안사건에 대한 응급대응

정보통신망 보안사건이 발생하면 정보통신망 보안사건의 응급대응방안을 즉시 개시하고 정보통신망 보안사건에 대한 조사와 평가를 진행하며 정보통신망 운영자로 하여금 기술적인 조치와 기타 필요한 조치를 취하도록 요청하고 잠재적인 보안위험을 제거하고 위험의 확대를 방지하며 적시에 사회와 대중에게 관련 경보를 반포합니다(법 제55조). 성급이상의 인민정부의 관련부문은 정보통신망 위험감독 관리업무 수행 중에 정보통신망에 비교적 큰 보안상의 위험이 있거나 보안사건의 발생을 알게 된 때에는 규정된 권한과 절차에 따라 정보통신망 운영자의 법정대리인 또는 주요 책임자와 면담을 실시합니다. 정보통신망 운영자는 요청에 따라 필요한 조치를 취하고 잠재적인 보안위험을 개선하고 제거합니다(법 제56조).

다. 관련법규들과의 연계처리

나아가 정보통신망 보안사건으로 인해 돌발사건 또는 생산안전사고가 발생한 경우에는 중화인민공화국의 돌발사건대응법《中华人民共和国突发事件应对法》, 중화인민공화국안전생산법《中华人民共和国安全生产法》등의 관련법률, 행정법규에 따라 처리합니다(법 제57조). 또한 국가안전과 사회공공질서를 수호하기 위하여 중대한 돌발 사회안전사건의 처리가 필요한 경우에는 국무원의 결정 또는 비준을 거쳐 특정구역의 정보통신망에 대해 제한 등의 임시조치를 취할 수 있습니다(법 제58조).

II. 우리나라에 기업에 대한 시사점

1. 본 법률이 제정된 현재 이미 중국도 대중창업 만인혁신의 구호 하에 O2O산업의 비약적인 성장, 전자상거래 플랫폼의 발전, IOT 산업 및 빅데이터, 클라우드

컴퓨터 산업의 개발 수준이 다른 어느 나라에 뒤떨어지지 않습니다. 이런 시대적 상황하에 반포된 본 법률이 과연 정보통신망 운영자 내지 이용자, 관련 사업자들의 권리를 보장 내지 보호하기 위한 법률인지 아니면 제한을 강화되는 법률인지에 대해서는 중국 현지에서도 의견이 분분합니다.

2. 특히 본 법은 앞 부분 20개의 조항에 걸쳐 정보통신망 관련 사업자, 개인에 대한 각종 책임과 의무에 관한 조항을 두고 있는데 이러한 일반적인 규정에 비추어 보면 정보통신망 운영에 관한 법률 체계와 적용이 향후 더 엄격해질 것으로 예상됩니다. 또한 본 법은 국가안전과 사회공공질서를 수호하기 위하여 중대한 돌발 사회안전사건의 처리가 필요한 경우에는 국무원의 결정 또는 비준을 거쳐 특정구역의 정보통신망에 대해 제한 등의 임시 조치를 취할 수 있게 됨을 유의하여야 합니다.
3. 본 법은 정보통신망 운영자의 행위를 규제함과 동시에 "정보통신망 핵심 설비와 정보통신망 안전 전문 제품(网络关键设备和网络安全专用产品)"에 대한 관련 경영자에 대해서도 특별한 요건을 규정하였습니다. 즉, 이러한 설비와 제품은 국가표준의 강행규정에 부합하는 자격을 가진 기구의 안전인증 합격 또는 안전검측 요건에 합격한 후에 비로소 판매 또는 제공이 가능합니다. 또한, 핵심정보기반시설의 운영자가 정보통신망 제품과 서비스를 구매할 때 국가안전에 영향을 미칠 가능성이 있는 경우에는 국가의 인터넷 정보부문, 국무원 관련 부문이 조직한 국가안전심사를 통과해야 한다는 점을 유의해야 합니다.
4. 본 법에도 상세하게 규정되어 있다시피 중국의 개인정보 보호는 점차 강화되고 있으므로 이에 대한 우리나라 기업들의 이해와 적응 노력이 필요할 것입니다.
5. 본 법은 아직 대부분의 개념이 미확정입니다. 즉, 핵심정보기반시설이 무엇을 의미하는지, 외국에 전송할 수 있는 정보의 범위에 대해서도 장차 구체적인 세부 법규들이 제정되어야 합니다. 내년 본격적인 법률 시행 전에 관련 법규들이 점차 완비될 것으로 예상됩니다. 그러므로 중국과 정보통신망 관련 사업을 하는 우리나라 기업들은 관련 법률법규의 변화 추세에 지속적인 관심을 가지고 이를 follow-up 해야 할 것으로 보입니다.

CONTACT

변웅재 변호사	02-528-5797	ujbyun@yulchon.com
허욱 변호사	+86-185-0085-2518	whuh@yulchon.com
태충남 중국 변호사	+86-10-8567-0828	taizhn@yulchon.com
백혜 중국 변호사	02-528-5072	hbai@yulchon.com