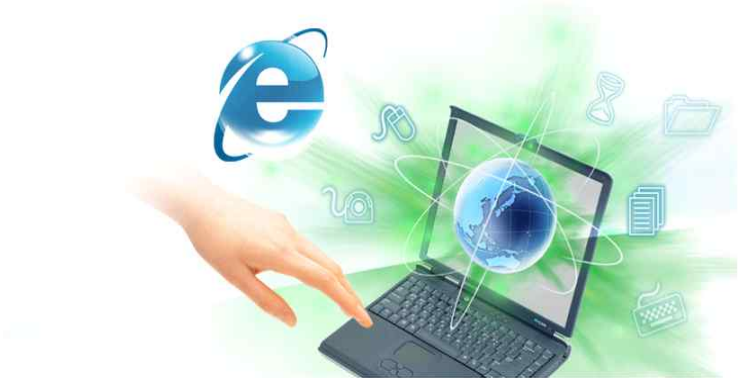
(月刊) 인터넷 법제동향

제101호 (2016년 2월)



이정현
- 팀장/ 법제팀
- hyunlee@kisa.or.kr

양승설
- 선임연구원/ 법제팀
- yss0907@kisa.or.kr

김도연
- 주임연구원/ 법제팀
- kimdoyeon@kisa.or.kr

김윤영
- 연구원/ 법제팀
- yoony77@kisa.or.kr

KISA 한국인터넷진흥원

목 차

인터넷 법제동향

Ⅰ 국내 입법 동향

1. 국회 제출 법률안

1 「통신비밀보호법」 일부개정법률안 (서영교 의원 대표발의, 2016. 2. 4. 제출)

❑ 소관 상임위원회 : 법제사법위원회

❑ 제안 이유

○ 현행법은 재판상 필요한 경우 법원에서 전기통신사업자에게 통신사실 확인자료제공을 요청할 수 있도록 규정하고 있는바, 재판상 필요한 경우란 개인정보보호의 필요성 보다 실체적 진실발견의 필요성이 높은 경우로, 통신사실 확인자료는 법원의 재판에 있어 반드시 필요한 자료임

○ 그러나 개인정보보호의 중요성이 높아지고, 전기통신사업자의 개인정보 관리에 대한 책임도 강하게 요구되고 있어, 법원의 통신사실 확인자료제공 요청에 대한 전기통신사업자의 자료제공 의무가 재량규정으로 해석될 수 있고 또한 자료제공에 대하여 전기통신사업자의 손해배상 책임이 발생할 여지가 있음

❑ 주요 내용

○ 법원의 통신사실 확인자료제공 요청에 대한 전기통신사업자의 자료제공 의무를 명확히 규정하고, 자료제공요청을 받은 사실을 전기통신 가입자에게 통지하도록 함(안 제13조의2)

※ 출처 : 국회 (http://www.assembly.go.kr)

2 「국민보호와 공공안전을 위한 테러방지법안」 (이철우 의원 대표발의, 2016. 2. 22. 제출)

❑ 소관 상임위원회 : 정보위원회

❑ 제안 이유

○ 2001년 9·11테러 이후 알카에다, 'ISIL'(이슬람국가)를 비롯한 극단주의 추종 세력들의 테러활동이 계속되고 있음

○ OECD 34개 국가 대부분이 테러방지를 위한 법률을 제정하였음에도 불구하고 아직 우리나라는 국가 대테러활동 수행에 기본이 되는 법적 근거조차 마련하지 못하고 있음

○ 이에 테러방지를 위한 국가 등의 책무와 필요한 사항을 명확하게 규정하여 국가 안보 및 공공의 안전은 물론 국민의 생명과 신체 및 재산을 보호하려는 것임

❑ 주요 내용

○ 대테러활동의 개념을 테러의 예방 및 대응을 위하여 필요한 제반 활동으로 정의하고 테러의 개념을 국내 관련법에서 범죄로 규정한 행위를 중심으로 적시함(안 제2조)

○ 대테러활동에 관한 정책의 중요사항을 심의·의결하기 위하여 국무총리를 위원장으로 하여 국가테러대책위원회를 둠(안 제5조)

○ 대테러활동과 관련하여 임무분담 및 협조사항을 실무 조정하고, 테러경보를 발령하는 등의 업무를 수행하기 위하여 국무총리 소속으로 대테러센터를 둠(안 제6조)

○ 관계기관의 대테러활동으로 인한 국민의 기본권 침해 방지를 위해 대책위원회 소속으로 대테러 인권보호관 1명을 둠(안 제7조)

○ 국가정보원장은 테러위험인물에 대한 출입국·금융거래 정지 요청 및 통신 이용 관련 정보를 수집할 수 있도록 함(안 제9조)

○ 관계기관의 장은 테러를 선전·선동하는 글 또는 그림, 상징적 표현이나 테러에 이용될 수 있는 폭발물 등 위험물 제조법이 인터넷 등을 통해 유포될 경우 해당기관의 장에 긴급 삭제 등 협조를 요청할 수 있도록 함(안 제12조)

○ 관계기관의 장은 외국인테러전투원으로 출국하려한다고 의심할만한 상당한 이유가 있는 내·외국인에 대하여 일시 출국금지를 법무부장관에게 요청할 수 있도록 함(안 제13조)

○ 테러 계획 또는 실행 사실을 신고하여 예방할 수 있게 한 자 등에 대해 국가의 보호의무를 규정하고, 포상금을 지급할 수 있도록 하고, 피해를 입은 자에 대하여 국가 또는 지방자치단체가 의료지원금, 특별위로금 등을 지급할 수 있도록 함(안 제14조~16조)

○ 테러단체를 구성하거나 구성원으로 가입한 경우 처벌하는 조항을 신설하며, 타인을 형사처분 받게 할 목적으로 테러관련 범죄에 대해 무고 또는 위증을 하거나 증거를 날조·인멸·은닉한 자는 가중처벌하며, 대한민국 영역 밖에서 이같은 죄를 범한 외국인에게도 국내법을 적용함(안 제17조~19조)

※ 출처 : 국회 (http://www.assembly.go.kr)

3 「개인정보 보호법」 일부개정법률안(대안) (안전행정위원장, 2016. 2. 29. 제출)

❑ 소관 상임위원회 : 안전행정위원회

❑ 제안 이유

○ 주민등록번호 사용의 엄격한 관리·통제 및 정보주체의 개인정보 자기결정권 강화 등을 통해 개인정보 처리 시 안전성을 확보하고자 함

❑ 주요 내용

○ 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 정보주체에게 수집 출처·처리 목적 등을 고지하도록 함(안 제20조제2항부터 제4항까지 신설)

○ 개인정보처리자가 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 하기 위해 안전성 확보에 필요한 조치를 의무화 함(안 제23조제2항 신설)

○ 주민등록번호를 수집할 수 있는 법령의 범위를 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙으로 한정함(안 제24조의2제1항제1호)

○ 개인정보 보호책임자의 성명 또는 개인정보 보호 업무 및 관련 고충사항을 처리하는 부서의 명칭·연락처와 인터넷 접속정보파일 등 개인정보 자동 수집 장치의 설치·운영 및 그 거부에 관한 사항을 개인정보 처리방침에 포함하도록 함(안 제30조제1항)

※ 출처 : 국회 (http://www.assembly.go.kr)

4 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안(대안) (미래창조과학방송통신위원장, 2016. 2. 29. 제출)

❑ 소관 상임위원회 : 미래창조과학방송통신위원회

❑ 제안 이유

○ 최근 정보통신망을 통한 개인정보 유출로 인해 많은 피해가 발생하고 있음

- 유출된 개인정보로 인한 2차 피해의 발생 가능성을 줄이기 위한 대책을 마련할 필요가 있음
- 개인정보 취급위탁의 안전성을 보장하고 불법 개인정보 거래를 적극적으로 단속하여야 함

○ 현행법상 개인정보 유출시 책임을 지는 방식인 법정손해배상제만으로는 재산적 피해를 보전하거나 피해방지의 실효성을 확보하는 데 어려움이 있으므로 징벌적 손해배상제도를 도입하여 정보통신서비스 제공자의 책임성을 강화하고자 함

○ 현재 한국인터넷진흥원은 수입금의 처리방식에 대한 법적 근거규정 없이 업무 수행에 따라 발생하는 수수료 수입을 자체수입으로 사용하고 있고, 이는 모든 세입과 세출 일체를 예산에 편입·계상하여야 하는 예산총계주의 원칙에 위반됨

❑ 주요 내용

○ 스마트폰 응용프로그램 개발자나 개발회사가 이용자 스마트폰에 대한 접근권한을 획득하고자 할 때, 접근권한이 필요한 항목과 이유를 이용자가 명확히 인지하도록 알리고 이용자로부터 동의를 받도록 함(안 제22조의2제1항 신설)

○ 개인정보 취급위탁이 문서로써 이루어지도록 하고, 개인정보 취급 업무의 동의 없는 재위탁을 금지함(안 제25조제6항 및 제7항 신설)

○ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하고, 필요 시 사업주 등에게 보고하여야 함(안 제27조제4항 신설)

○ 정보통신서비스 제공자 등의 개인정보 분실·도난·유출·위조·변조 또는 훼손 행위에 대한 징벌적 손해배상 및 개인정보 관련 범죄로 인한 이익을 환수하기 위한 몰수·추징 규정을 도입함(안 제32조제2항·제3항 신설 및 제75조의2 신설)

○ 정보통신망을 통하여 개인정보가 노출된 경우 방송통신위원회 또는 한국인터넷진흥원은 해당 정보의 삭제·차단을 정보통신서비스 제공자등에게 요청할 수 있으며, 정보통신서비스 제공자등이 필요한 조치를 취하지 않을 경우 3천만원 이하의 과태료를 부과함(안 제32조의3 신설, 제76조제1항제12호)

○ 한국인터넷진흥원이 사업을 수행하는 데 필요한 경비는 정부의 출연금, 제52조제3항 각 호의 사업수행에 따른 수입금, 그 밖에 인터넷진흥원의 운영에 따른 수입금으로 충당하도록 함(안 제52조제4항)

○ 개인정보 국외 이전의 유형을 '제공(조회되는 경우를 포함), 취급위탁, 보관'으로 명시하고, 이용자의 동의없이 개인정보를 국외로 제공한 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하의 과징금을 부과함(안 제63조제2항, 제64조의3제1항제8호 신설)

○ 정당한 사유없이 악성프로그램을 전달 또는 유포한 자 및 정당한 권한없이 또는 허용된 접근권한을 넘어 정보통신망에 침입한 자에 대한 처벌을 각각 '7년 이하의 징역 또는 7천만원 이하의 벌금' 및 '5년 이하의 징역 또는 5천만원 이하의 벌금'으로 상향함(안 제70조의2 신설, 안 제71조제8의2호 신설)

○ 정보통신망법의 규정을 위반하여 미래창조과학부장관 또는 방송통신위원회로부터 부과받은 시정조치 명령을 이행하지 아니한 정보통신서비스 제공자등에게 3천만원 이하의 과태료를 부과함(안 제76조제1항제12호)

※ 출처 : 국회 (http://www.assembly.go.kr)

2. 입법예고된 법률안

5	「국가 사이버테러 방지 등에 관한 법률안」 (입법예고 기간 : 2016. 2. 23. ~ 2016. 3. 8.)

❑ 소관 상임위원회 : 정보위원회

❑ 개정 이유

○ 과거 1·25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비 사태 발생과 사이버테러로 국가기밀 및 첨단기술의 유출 등 국가·사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 높아지고 있음

- 우리나라는 아직 국가차원에서 사이버테러 방지 및 위기관리업무를 체계적으로 수행할 수 있는 제도와 구체적 방법 및 절차가 정립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있음

○ 이에 정부와 민간이 참여한 국가차원의 종합적이고 종합적이고 체계적인 대응체계를 구축하여, 위기 발생 시 신속히 대응할 필요가 있음

❑ 주요 내용

○ 사이버테러 예방 및 대응을 위해 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제6조)

○ 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이나 보안관제전문업체가 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조)

○ 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 함(안 제9조)

○ 정부는 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있음(안 제10조)

○ 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민/관/군 전문가가 참여하는 사이버위기대책본부를 구성 및 운영할 수 있음(안 제11조)

○ 정부는 사이버테러 기도에 관한 정보를 제공하거나 사이버테러를 가한 자를 신고한 자 등에 대하여 포상금을 지급할 수 있음(안 제13조)

○ 직무상 비밀을 누설한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 피해의 복구 및 확산방지를 이행하지 아니한 경우에는 1천만원 이하의 과태료에 처할 수 있음(안 제14조 및 제15조)

※ 출처 : 국회입법예고시스템 (http://pal.assembly.go.kr)

II 해외 입법 동향

1. 입법 동향

1 미국, 유럽시민의 개인정보보호 피해구제 강화를 위한「사법배상법」 제정 (2016. 2. 24.)

❑ 개관

○ 버락 오바마(Barack Obama) 미국 대통령은 범죄의 예방, 발견, 조사 및 기소 목적을 이유로 공유된 유럽 시민의 개인정보가 제대로 보호받지 못한 경우 유럽시민이 미국 정부를 상대로 소송을 제기할 수 있도록 하는「사법배상법」*(Judicial Redress Act)에 서명하였음(2016. 2. 24.)

* 「사법배상법」은 미국과 유럽연합(EU)간의 데이터보호 및 사생활보호 협정(EU-US Data Protection and Privacy Agreement, 일명 Umbrella Agreement) 체결의 전제조건이 되는 법임

❑ 배경 및 입법 경과

○ 2000년, 미국과 유럽연합은 미국 기업들이 유럽 내 이용자들의 웹 기록 등 개인신상정보를 미국으로 전송할 수 있도록 허용하는 세이프 하버(Safe Harbor Agreement) 협정을 체결함

- 2013년, 전직 미국 국가안전보장국(NSA)요원인 에드워드 스노든(Edward Snowden)은 미국 정보당국이 구글 등 미국의 IT기업 서버에 별도 프로그램을 설치하여 사이트 이용자들을 지속적으로 감시해왔다고 폭로하였고, 이로 인해 EU는 미국의 개인정보처리지침을 불신하게 되었음

○ 유럽사법재판소, 유럽시민의 개인정보보호 보장을 위해 세이프 하버 협정을 사실상 폐기하는 내용의 판결을 내림(2015. 10. 6.)

○ **이로 인해 유럽에서 활동하는 미국 IT기업의 이용자 개인정보 수집 및 반출이 어려워졌고, 미국 정부는 유럽연합의 무너진 신뢰를 되찾기 위해 세이프 하버 협정을 대체하기 위한 방법을 마련함**

- **미국과 유럽연합은 개인정보 공유 및 전송을 위한 협정인 '프라이버시 쉴드'(Privacy Shield)를 체결(2016. 2. 2.)하였고, 유럽시민의 개인정보보호 피해 구제방법을 마련한「사법배상법」을 제정하였음(2016. 2. 24.)**

❑ 주요 내용

○ **1974년 제정된 미국의「사생활보호법」[1]에 저촉되는 방식으로 본인의 동의 없이 개인정보(성명, 주소, 범죄 기록 등)가 공개된 경우 미국 시민 및 법적 거주자 뿐만 아니라 유럽 국가의 시민도 미국 정부를 상대로 민사소송을 제기할 수 있도록 규정함**

- 유럽시민이 부정확한 개인정보 수정 또는 본인 기록 열람을 신청하였으나, 지정된(designated) 미국 정부기관에 의해 그 신청이 거부당한 경우 해당 기관을 상대로 소를 제기할 수 있음

○ 「사법배상법」이 적용되는 유럽국가 및 미국 정부기관은 미국 법무부가 정함

❑ 평가

○ 미국 정부는 미국과 EU 간 신뢰관계를 재구축하기 위해 EU 측의 입장을 최대한 수용하여 미국 법정에서 유럽 시민들이 개인정보 보호권을 행사하도록 하는 등 EU시민의 데이터 프라이버시권 보장을 위해 많은 노력을 하고 있음

- 사법배상권 발효가 미국과 유럽연합 간 데이터보호 및 사생활 보호 협정 체결에 긍정적인 영향을 미칠 것으로 보임

○ 본 법이 EU가 요구하는 개인정보 보호 기준에 부합하는 지의 여부는 좀 더 지켜봐야 함

1) 사법배상법의 근간을 이루는 1974년 사생활보호법(Privacy Act of 1974)은 연방정부에 의한 개인정보의 수집, 보관, 사용 및 유포를 다루고 있음. 개인의 기록에 대한 공개는 해당 개인의 서면 동의 없이는 금지하고 있으며 개인들에게 자신의 기록에 대한 접근 및 기록의 변경을 위한 방법을 제시하고 있음

※ 참고자료

https://www.govtrack.us/congress/bills/114/hr1428
http://www.canadiantechlawblog.com/2016/02/19/judicial-redress-act-grants-european-citizens-legal-redress-for-privacy-breaches-in-transatlantic-data-sharing/
http://www.justice.gov/opcl/doj-systems-records
http://europa.eu/rapid/press-release_IP-16-216_en.htm
http://europa.eu/rapid/press-release_MEMO-15-5612_en.htm
https://www.congress.gov/bill/114th-congress/house-bill/1428
http://europa.eu/rapid/press-release_STATEMENT-16-401_en.htm
https://papersplease.org/wp/2016/02/25/why-the-judicial-redress-act-is-worthless/
http://www.lexology.com/library/detail.aspx?g=f073cace-e335-47b6-9892-db118954bea0
http://www.securityprivacyandthelaw.com/2016/02/eu-commission-and-united-states-agree-on-new-framework-for-transatlantic-data-flows-eu-us-privacy-shield/

2 싱가포르, 새로운 사이버보안법(안) 제안 계획 발표(2016. 1. 21.)

❑ 개요

○ 2016년 1월 21일, 싱가포르 정부[2]는 연내 사이버보안청(Cyber Security Agency of Singapore)에 중요정보인프라(critical information infrastructure)관련 권한을 강화하는 내용의 사이버보안법(안) 제안 계획을 발표

❑ 주요 내용

○ 최근 공공 및 민간에 대하여 발생하는 지속적인 사이버 침해사고[3]로 기존 사이버보안기구의 권한강화 등 현행 법제개선의 의지를 밝힘

- 현재 싱가포르 정부는 '모니터링 및 관제센터(Monitoring and Operations Control Centre)[4]' 및 '사이버보안청[5]'을 설립하여 싱가포르 內 사이버보안의 기틀을 다졌으며,

- 날로 진화하는 사이버위협 기술에 대응하기 위해 2016년 사이버보안기구 기능 강화를 골자로 한 사이버보안 법제를 정비하고자 함

2) 해당 내용은 정보통신부장관(Minister for Communications and Information)이자 사이버보안 책임 장관(Minister-in-charge of Cyber Security)을 겸직중인 야콥 이브라힘(Yaacob Ibrahim)이 발표하였으며, 2016년 하반기에 싱가포르 의회에 제안될 예정이다.(2016.1.21.)

3) 싱가포르 內 주요 사이버 침해사고 현황(표) 참조

일자	주요 사이버 침해사고 현황
2013	· 정부부처 및 개인 웹사이트 등에 대한 해킹사건 발생(2013.11월)
2014	· 공공분야 전자공인인증서 싱패스(SingPass: Singapore Personal Access)의 개인정보 1,560건 유출사고 발생(2014.6월) · 가라오케 체인의 회원 데이터베이스 해킹으로 317,000명의 개인정보 유출사고 발생(2014.9월)
2015	· 개인정보보호위원회(Personal Data Protection Commission) 사칭 도메인네임 이용사건으로 사이트 다운 등 사이버침해사고 발생(2015.1월) · 멀웨어를 통한 인터넷뱅킹 피싱(phishing) 사이트 연동 등 사이버침해사고 발생 및 7,000달러의 금전적 손해 등 2차피해 발생(2015.10월) · 스마트폰 안드로이드 업데이트 과정에서 악성코드를 통해 신용정보가 유출되어 이용자에게 수천 달러의 손해가 발생(2015.12월)
2016	· 과학·기술학교(polytechnic) 사칭 웹사이트 제작 등 파밍위협 발생(2016.1월)

4) 2014년 12월에 설립하였다.

5) 2015년 4월에 사이버 위협에 대응하고자 사이버 보안전략 수립 및 시행을 위하여 설립된 싱가포르 정보통신부 산하 국가기관으로 싱가포르 총리실(Prime Minister's Office) 지원 하에 운영 중이다. 사이버보안청은 국내 사이버사이버 관련 보안전략 수립 및 유관산업 육성 정책 개발 등의 업무를 수행하고 있다. (※ 참고 : www.csa.gov.sg)

○ 사이버보안법(안)은 현행법(Computer Misuse and Cybersecurity Act)[6]에 비하여 내무부장관 발급면허[7] 취득대상 사업 분야를 확대 및 권한 강화[8], 新유형의 사이버 범죄 신설, 사이버 침해사고에 대한 보고를 의무화[9] 하는 등의 내용으로 규정될 것으로 예상됨[10]

< 사이버보안법(안) 예상내용 비교 >

구분	현행	예상(안)
내무부장관 발급면허의 취득대상 사업 확대	· 국가안보 · 방위 · 외교 · 통신기반사업(이하 필수공익사업) · 은행업 · 금융업 · 공익사업 · 대중교통 및 육상교통기반사업 · 항공운송 · 해상운송 · 공중 핵심 인프라 · 긴급구조서비스	· 국가안보 · 방위 · 외교 · 통신기반사업(이하 필수공익사업) · 은행업 · 금융업 · 공익사업 · 대중교통 및 육상교통기반사업 · 항공운송 · 해상운송 · 공중 핵심 인프라 · 긴급구조서비스 · 에너지 · 수자원 · 교통 · 보건 · 정부 · 인포콤 · 미디어 · 보안 · 긴급 서비스 · 은행업 · 금융업
범죄 유형 확대	· 접근 제한된 자의 무단 정보통신기기 접근 및 무단 수정 등	· 사이버보안 범죄유형 추가
사업자 보고의무 강화	-	· 사고관련 보고의무 추가
내무부장관의 권한 강화	· 개인·단체에 대하여 면허발급 및 임무수행을 허가함	· 명시적으로 알려진 바 없음

❑ 향후 대응

○ 아시아태평양 내 사이버보안 취약국 조사 결과, 인터넷 의존도가 높은 한국·싱가포르·호주·뉴질랜드·일본이 사이버 공격에 가장 취약[11]한 한 것으로 나타나, 사이버 보안 법제 개선이 시급할 것으로 보임

○ 계속해서 진화하는 지능적 사이버침해 위협요인에 적절히 대응하기 위해서는, 전담기구의 권한강화 및 체계의 보완 등 현행 법제 개선노력 뿐만 아니라 관련 기술력의 확보 등 기술적 측면에서의 제도화가 필요할 것으로 보임

6) 동 법률은 1993년에 최초 제정되었으며, 2013년 3월 13일 마지막 개정절차를 밟았다.

7) 예를 들어 내무부장관은 면허(certificate)의 발급 등을 통해 개인 또는 단체로 하여금 싱가포르의 국가안보, 방위, 외교 및 필수공익사업에 대한 사이버보안 위협의 감지 및 예방에 필요한 절차를 밟거나 특정 의무를 준수하도록 승인, 지시 또는 강제할 수 있다.

8) 통화청(Monetary Authority of Singapore)은 소관 금융기관들로 하여금 관내 IT 시스템에 발생하는 보안 침해 사건에 대하여 그 사건 발생을 안 때로부터 한 시간 이내에 싱가포르 통화청에 초기 통지를 하고 사건이 발생한 날부터 14일 이내에 상세 보고서를 제출할 것을 의무화하고 있는데, 이러한 방식을 채택할 가능성도 제기되고 있다.

9) 현재 「컴퓨터 오용 및 사이버보안법」 상에 침해사고 관련 보고의무는 명시적으로 규정된 바가 없다.

10) 해당 법안은 아직 회람되지 않았으나, 싱가포르의 핵심정보인프라를 보호하기 위해 사이버보안청에 보다 강한 권한을 부여하는 방향으로 제정될 것으로 예상되고 있으며, 본 절에서는 예상되는 내용을 바탕으로 정리하였음

11) 딜로이트 컨설팅, 2016 딜로이트 아시아태평양 국가보안 전망 보고서(2016 Deloitte Asia-Pacific Defense Outlook)에 따르면, 중국·인도는 인구가 가장 많이 분포하고 있음에도 불구하고 인터넷 연결 비율이 낮아 사이버공격에 상대적으로 덜 취약한 것으로 조사됨(2016.2월.)

※ 참고문헌

http://www.singaporelawwatch.sg/slw/attachments/77677/1602-04%20Cyber%20security.pdf
http://www.straitstimes.com/singapore/new-centre-to-help-spore-boost-cyber-security
http://www.enterpriseinnovation.net/article/cyber-security-center-excellence-government-launched-singapore-566273235
http://www.ibtimes.co.uk/japan-australia-singapore-south-korea-new-zealand-most-vulnerable-cyberattacks-says-report-1545598
https://www.ida.gov.sg/Tech-Scene-News/Smart-Nation-Vision
http://www.enterpriseinnovation.net/article/study-asia-pacifics-cyber-five-nations-more-vulnerable-cyberattack-785022503
http://www.legislation.gov.uk/ukpga/1990/18/pdfs/ukpga_19900018_en.pdf

3 일본, 사이버보안추진체제의 기능강화에 관한 방침 발표(2016. 1. 25.)

❑ 개관

○ 2016년 1월 25일, 내각사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity. 이하 'NISC'라 한다)는 「일본의 사이버보안 추진체제의 기능강화에 관한 방침(이하 '방침'이라고 한다')」[1]을 발표함

○ 2015년 1월 「사이버보안기본법」(이하 '기본법'이라고 한다)의 전면시행에 따라 NISC는 정부의 사이버보안에 관련된 능력을 향상시키는 기능을 담당해 옴

○ 이러한 상황 하에서 2015년 5월 일본연금기구의 개인정보(약 125만건) 유출 사건이 발생함

○ 이를 계기로 정부는 심각해지고 있는 사이버공격에 대비해서 정부기관 등을 시작으로 한 사이버보안추진체제의 기능강화를 위한 구체적인 방향성을 제시하기 위해 동 방침을 발표

❑ 사이버보안추진체제 강화책

○ 사이버보안추진체제를 강화하기 위해 제시되는 방안은 크게 6가지로 구성됨

- ①국가가 수행하는 부정통신 감시 등의 범위를 기존 국가의 행정기관정보시스템에서 독립행정법인 및 지정법인(국가가 지정하는 특수법인 및 인가법인)까지 확대
- ②NISC 직원의 증원을 포함은 사이버보안 관련 정부인재 확충 및 개인정보보호위원회, 내각관방(사회보장개혁담당실), 총무성 등의 체제정비
- ③관계 기관 간의 정보공유와 연계 및 「사이버보안기본법」에 근거한 사이버보안전략본부의 운용으로 사고발생 시 적절하고 신속한 초동 대응태세 구축
- ④지방자치단체를 포함한 중요인프라사업자 등의 사이버보안확보에 대한 NISC의 적극적인 지원 및 2016년 말을 목표로 '중요인프라정보보안대책에 관련한 제3차 행동계획'의 개정 검토계획 수행

1) 「我が國のサイバーセキュリティ推進体制の更なる機能强化に關する方針」

- ⑤개인번호(My Number)사업의 원활한 도입 및 추진을 위해 기존 주민시스템 등을 인터넷으로부터 분리시키고, 지방자치단체의 사고대응체계 충실화 및 정보보안클라우드 구축 추진
- ⑥2020년 개최되는 동경올림픽 성공을 위해 동경올림픽추진본부에 설치된 보안간사회 사이버보안업무팀과 관계 정부기관 등의 긴밀한 연계를 추진

❑ 앞으로의 대응

○ 본 방침에 근거한 대응은 가급적 신속하게 실시하도록 함

○ 사이버공격에 대한 위협이 증대되고 심각해짐에 따라 각 행정기관의 사이버보안 대책의 추진상황, 2020년 올림픽개최를 대비한 준비상황 등, 시시각각 변화하는 정세를 감안하여 법제의 추가적인 정비 등에 대해서도 검토가 이루어질 것으로 예상되고 있음

※ 참고자료

http://www.nisc.go.jp/active/kihon/pdf/cs_kyoka_hoshin.pdf#search='%E6%88%91%E3%81%8C%E5%9B%BD%E3%81%AE%E3%82%B5%E3%82%A4%E3%83%90%E3%83%BC%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E6%8E%A8%E9%80%B2%E4%BD%93%E5%88%B6%E3%81%AE%E6%9B%B4%E3%81%AA%E3%82%8B%E6%A9%9F%E8%83%BD%E5%BC%B7%E5%8C%96%E3%81%AB%E9%96%A2%E3%81%99%E3%82%8B%E6%96%B9%E9%87%9D'

4 프랑스, 「디지털 공화국을 위한 법률」(안) 1차 독회 통과 (2016. 1. 26.)

❑ 개요

○ 「디지털 공화국을 위한 법률」(안)*(Projet de loi pour une République numérique, n°3318, 정부제출법안[2], The Digital Republic Bill) 국민의회에 제출[3](2015. 12. 9.)

○ 본 법안은 공화국 헌법, 법률, 행정위원회(la commission des lois constitutionnelles, de la législation et de l'administration générale de la république)에 이송되었고,

○ 동 위원회는 총840여개의 수정안을 검토하여 최종 수정사항을 반영한 텍스트를 제정함[4](TEXTE DE LA COMMISSION DES LOIS CONSTITUTIONNELLES, DE LA LÉGISLATION ET DE L'ADMINISTRATION GÉNÉRALE DE LA RÉPUBLIQUE)(2016. 1. 15.)

○ 「디지털 공화국을 위한 법률」(안)(Projet de loi pour une République numérique), 1차 독회 통과(2016. 1. 26.)

- 기존에 41개 조항으로 구성되었던 정부발의안이 총48개 조항으로 수정됨

❑ 주요내용

○ 공공정보의 열람 및 자유로운 사용을 통해 데이터와 지식의 유통을 촉진시키고자 함

○ 온라인 상의 개인정보보호를 위해 노력하고, 모든 사람이 제한이나 차별 없이 공공디지털 서비스에 보편적으로 접근할 수 있도록 하는 내용을 담고 있음

2) 프랑스 헌법 제39조 제1항 : 수상과 국회의원은 법률안 발의권을 가진다.
3) 헌법 제39조 제2항 : 정부제출법률안은 국사원의 의견을 청취하고 국무회의 심의를 거쳐 양원 중 한 원에 제출된다.
4) 헌법 제 44조 제1항 : 의회 의원들과 수상은 수정권을 가진다.

❑ 시사점

○ 입법과정시 인터넷을 통해 국민의 활발한 참여를 유도함

- 국민이 법안의 수정 및 개선 사항에 대해 자유롭게 의견을 제시할 수 있는 공간을 제공함

○ 정책에 프랑스 대중의 요구를 적극적으로 반영하고 하는 등 디지털 민주주의의 초석을 이루었다는 평가를 받고 있음

※ 참고자료

http://www.assemblee-nationale.fr/14/dossiers/republique_numerique.asp
http://www.senat.fr/leg/pjl15-325.pdf
http://www.assemblee-nationale.fr/14/ta-pdf/3399-p.pdf
http://www.lemonde.fr/pixels/article/2016/01/14/un-amendement-protegeant-les-hackeurs-qui-signalent-des-failles-informatiques-rejete_4847366_4408996.html
http://www.assemblee-nationale.fr/14/documents/index-ta.asp
https://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=2690411E2D38D9EEA709650905F09BF6.tpdila10v_3?idDocument=JORFDOLE000031589829&type=expose&typeLoi=proj&legislature=14

2. 판례 및 이슈

5	**유럽인권재판소, 뉴스포털이 누리꾼의 악성 댓글에 대해 법적 책임을 지지 않는다고 판결 (2016. 2. 2.)**

❑ 사실 관계

○ 헝가리의 인터넷 콘텐츠 제공자 자율 규제 기관인 MTE와 헝가리 주요 인터넷 포털인 인덱스(index)는 부동산 관리 웹사이트 운영 회사의 광고 서비스가 비윤리적이라고 비난하는 기사를 게시하였고, 기사를 접한 누리꾼들은 회사를 강하게 비난하는 댓글을 게시함(2010. 2.)

○ 이에, 위 회사(원고)는 사업체에 대한 악성 댓글로 인해 회사의 인격권과 명성이 훼손당했다고 MTE와 인덱스를 상대로 부다페스트 지방법원에 소송을 제기함(2010. 2. 17.)

- 포털 회사는 해당 부동산 회사의 소송제기를 알고 난 후 즉시 소송의 원인이 된 댓글을 삭제함

○ 1심(2011. 3. 31.)·2심(2011. 10. 27.)·3심(2012. 6. 13.) 모두 피고가 패소하였고, 피고 측이 표현의 자유가 침해되었다고 제기한 헌법소원(2013. 1. 3.)도 기각되었음(2014. 5. 27.)

- 포털 기사에 달린 악성 댓글 내용이 표현의 자유의 수인한계를 넘어섰고, **운영자에게 그런 댓글을 달 수 있는 공간을 제공한 것에 대해 객관적인 책임을 부과하여야 한다고 판결함**

❑ 유럽인권재판소의 판결 내용

○ 유럽인권재판소(the European Court of Human Rights), 뉴스 포털 기사에 게시된 이용자의 악성 댓글 내용에 대해 포털 운영자가 책임을 지지 않는다고 판결함(2016. 2. 2.)

- 헝가리 국내법원의 판결은 **유럽인권협약 제10조[1]의 표현의 자유를 침해함**

○ **포털 운영자는 표현의 자유와 원고의 상업적 명성 보호 사이에 적절한 균형을 유지하기 위해 '통지 후 조치 시스템'*(Notice and take down system)을 마련함**

* 서비스제공자에게 문제가 되는 댓글의 삭제를 요청하면 댓글 작성자로 하여금 이에 대한 조치를 취하도록 하거나 서비스제공자가 직접 댓글을 일부 수정·삭제하는 시스템

- **또한 운영자는 사전에 이용자의 댓글에 법적 책임을 지지 않으며 악성 댓글을 웹사이트에 업로드할 수 없다는 점을 공지했음**

○ 회사의 명성은 상업적 이익과 관련된 내용으로 도덕적인 성격이 있다고 볼 수 없고, 사람의 명성에 관한 내용이 아니므로 유럽인권협약 제8조[2]에 의해 보호받을 수 없음

- **본 댓글이 비록 모욕적인 내용이라 할지라도 허위 내용을 작성한 것이 아니며, 이미 원고의 사업 관행은 소비자 단체로부터 많은 질타를 받았음**

❑ 평가

○ **헝가리 법원의 판결은 민주사회에서 언론이 행하는 공익적 성격을 고려하지 못했다는 평가가 있음**

- 인터넷에서의 표현의 자유를 위축시킨다면 모든 댓글 공간이 폐쇄될 수 있음

1) 유럽인권협약 제10조(표현의 자유) 1. 모든 사람은 표현의 자유에 대한 권리를 가진다. 이 권리는 의견을 가질 자유와 공공당국의 간섭을 받지 않고 국경에 관계없이 정보 및 사상을 주고받는 자유를 포함한다. 이 조가 방송, 텔레비전 또는 영화 사업자에 대한 국가의 허가제도를 금지하는 것은 아니다. 2. 이러한 자유의 행사에는 의무와 책임이 따르므로, 법률에 의하여 규정되고, 국가안보, 영토의 일체성이나 공공의 안전, 무질서 및 범죄의 방지, 보건과 도덕의 보호, 타인의 명예나 권리의 보호, 비밀리에 얻은 정보의 공개 방지, 또는 사법부의 권위와 공정성의 유지를 위하여 민주사회에서 필요한 형식, 조건, 제약 또는 형벌에 따르게 할 수 있다.

2) 유럽인권협약 제8조(사생활 및 가족생활에 대한 존중권) 1. 각인은 사생활 및 가족생활, 그의 거처, 그의 통신에 대한 존중권을 가진다. 2. 관청은 그 침해가 법률상 예정이 되어 있거나, 민주적인 사회에서 국가의 국가적·공공적·경제적 안녕을 위해서이거나, 질서의 유지를 위해서, 범죄행위로 부터의 보호를 위해서, 건강·도덕의 보호를 위하여, 또는 다른 사람의 권리와 자유의 보호를 위하여 필수적인 경우를 제외하고는 이러한 각인의 권리의 실현을 침해하면 안 된다.

※ 참고자료

유럽인권법원 판결 전문 : http://hudoc.echr.coe.int/eng?i=001-160314#{"itemid":["001-160314"]}

관련 기사 : http://www.heise.de/newsticker/meldung/Gerichtshof-fuer-Menschenrechte-spricht-News-Portal-von-Haftung-fuer-Nutzerkommentare-frei-3092738.html

http://www.lto.de/recht/hintergruende/h/egmr-22947-13-haftung-forenbetreiber-meinungsfreiheit-hass-kommentare/

http://www.mycsc.de/recht/egmr-haftung-des-seitenbetreibers-fuer-hass-kommentare/

참고 웹사이트

1. 국내 웹사이트

[1] 국회 (http://www.assembly.go.kr)

2. 국외 웹사이트

[1] https://www.govtrack.us
[2] http://www.canadiantechlawblog.com
[3] http://www.justice.gov
[4] http://europa.eu
[5] https://www.congress.gov
[6] https://papersplease.org
[7] http://www.lexology.com
[8] http://www.securityprivacyandthelaw.com
[9] http://www.singaporelawwatch.sg
[10] http://www.straitstimes.com
[11] http://www.enterpriseinnovation.net
[12] http://www.ibtimes.co.uk
[13] https://www.ida.gov.sg
[14] http://www.legislation.gov.uk
[15] http://www.nisc.go.jp
[16] http://www.assemblee-nationale.fr
[17] http://www.senat.fr
[18] http://www.lemonde.fr
[19] https://www.legifrance.gouv.fr
[20] http://hudoc.echr.coe.int
[21] http://www.heise.de
[22] http://www.lto.de
[23] http://www.mycsc.de

인터넷 법제동향

발행처 한국인터넷진흥원
주 소 05717 서울특별시 송파구 중대로 135(가락동 78) IT 벤처타워