Contents

국내 입법 동향

국외 입법 동향

인터넷 법제동향

•• 국내 입법 동향 ••

1. 입법동향

1 「국가정보화 기본법」 일부개정안 국회제출 (김광진 의원 대표발의, 2014. 11. 26.)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

■ 정보화시대에 개인의 자유와 창의성을 최고도로 발휘하여 혁신을 주도하는 벤처 · 스타트업 기업의 중요성이 커지고 있음

– 그러나 성과에 급급한 일부 국가기관 및 지방자치단체 등에서 우월적 지위를 활용하여 우수한 민간 벤처 · 스타트업 기업이 창작 · 제조한 성과나 서비스를 모방하여 벤처 · 스타트업 기업들의 지식재산에 관한 권리와 이익을 침해하고, 민간의 사업의지와 혁신동력을 좌절시키는 사례가 빈번하게 발생하고 있음

– 이러한 사례는 정부가 개인과 기업의 경제의 자유와 창의를 존중하여야 한다는 헌법이념에 배치되며, 개인과 기업의 혁신을 지원하여야 하는 정부의 역할에 부합하지 않음

■ 이에 국가정보화와 관련하여 국가기관, 지방자치단체 및 공공기관이 민간의 창작물 · 제조물 및 서비스의 모방 · 도용 등을 포함한 지식재산에 관한 권리 또는 이익의 침해를 금지하고, 이로 인해 피해를 당한 자를 구제하기 위하여 국가정보화 심의조정위원회를 설치하려는 것임

주요내용

■ 국가정보화의 기본 이념에 인터넷의 기본 이념인 자유와 개방성을 반영함 (안 제2조)

■ 국가와 지방자치단체에 국가정보화 추진 과정에서 민간과 구분되는 고유의 역할에 충실하여 민간의 자유와 창의를 존중하고, 국민이 국가정보화의 성과를 보편적으로 누릴 수 있도록 편의성과 접근성 등을 개선하도록 하는 책무를 부여함 (안 제4조)

■ 국가기관, 지방자치단체 및 공공기관이 추진하는 국가정보화 정책이나 사업이 국가정보화 추진 원칙에 적합한지를 심의 · 조정하기 위하여 미래창조과학부장관 소속으로 국가정보화 심의조정위원회를 두도록 함 (안 제8조의2제1항 및 제8조의3제3항)

■ 국가정보화 심의조정위원회에는 정보통신서비스 제공자 및 이용자를 대표할 수 있는 위원을 각각 포함하고, 국가정보화 심의조정위원회가 분쟁당사자에게 필요한 자료를 요청하고 의견을 들을 수 있도록 함 (안 제8조의2제2항 및 제8조의3제5항 · 제6항)

■ 국가기관, 지방자치단체 및 공공기관이 국가정보화를 추진하면서 민간의 지식재산에 관한 권리 또는 이익을 침해하지 않도록 책무규정을 신설함 (안 제42조제2항 신설)

※ 출처 : 국회 (http://www.assembly.go.kr)

2 「방송법」 일부개정안 국회제출 (조해진 의원 대표발의, 2014. 11. 26.)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

- 현행법상 방송사업자는 외주제작 방송프로그램 편성의무와 특수관계자 방송프로그램 편성비율의 제한을 따라야 함. 외주제작 방송프로그램 편성 의무화에 따라 다양한 독립제작사가 등장하여 지상파 독과점을 막고 제작주체가 다양화되고 있으나, 방송사업자 제작 역량 약화 등의 한계도 노출되고 있음

- 한편, 특수관계자 방송프로그램 편성비율의 제한은 외주제작이 활성화되기 이전에 지상파 방송사업자가 특수관계자를 통해 외주물량을 확보하는 폐해를 막기 위해 도입된 것으로 외주제작 비율이 50%에 이를 정도로 활성화 된 현재 상황과는 괴리가 있음

주요내용

- 이에 방송사업자의 외주제작 편성의무는 유지하되, 특수관계자 방송프로그램 편성비율 제한 규정은 삭제함으로써 외주제작 의무편성의 기본취지는 살리면서, 방송사업자 규제완화를 통한 투자확대와 방송사와 외주제작사 간 바람직한 제작환경 조성을 도모해 국내 및 해외 시장을 선도할 콘텐츠 산업 경쟁력을 높이려는 것임 (안 제72조).

※ 출처 : 국회 (http://www.assembly.go.kr)

3 「전파법」 일부개정안 국회제출 (강기윤 의원 대표발의, 2014. 11. 26.)

소관 상임위원회 : 미래창조과학방송통신위원회

제안이유

- 현행법은 주파수를 할당받은 자에게 주파수이용권을 부여하고, 이를 효율적으로 관리하기 위하여 주파수이용권 관리대장을 유지 · 관리하도록 하며, 수수료를 납부하고 주파수이용권 관리대장을 열람하거나 그 사본을 발급받도록 규정하고 있음

- 그러나 주파수이용권 관리대장에 기재되어 있는 사항이 주파수 할당시 공고된 사항과 대부분이 일치하여 주파수이용권 관리대장을 열람하거나 그 사본을 발급받을 필요성이 적고, 실제로 수수료를 납부하고 주파수이용권 관리대장을 열람하거나 사본을 발급받은 사례가 없어 개정이 요구됨

주요내용

- 주파수이용권 관리대장을 열람하거나 사본을 발급받을 때 수수료를 내도록 하는 조항을 삭제하여 실효성이 없는 불필요한 규제를 폐지하고자 함(안 제69조제1항제1호의2 삭제)

※ 출처 : 국회 (http://www.assembly.go.kr)

4 「소프트웨어산업 진흥법」 일부개정안 (대안) (미래창조과학방송통신위원장 제안, 2014. 12. 8.)

소관 상임위원회 : 미래창조과학방송통신위원회

제안경위

■ 2013년 10월 1일 장하나 의원이 대표발의한 「소프트웨어산업 진흥법 일부개정법률안」과 2014년 1월 20일 권은희 의원이 대표발의한 「소프트웨어산업 진흥법 일부개정법률안」및 2014년 4월 30일 강은희 의원이 대표발의한 「소프트웨어산업 진흥법 일부개정법률안」을 함께 심사하여 3건의 법률안의 내용을 통합 · 조정한 대안을 제안하기로 함

제안이유

■ 소프트웨어사업은 다양한 분야의 전문지식과 기술이 요구되기 때문에 여러 기업과의 협업이 필수적이며, 이로 인해 하도급 거래가 자연스럽게 이뤄지고 있음. 그러나 과도한 다단계 하도급 거래로 인하여 소프트웨어사업의 품질 저하, 소프트웨어기술자의 처우 악화, 비정규직 양산 등 국내 소프트웨어산업 전반의 경쟁력을 떨어뜨리는 요인이 발생하고 있음

■ 이에 도급, 하도급 등 관련 정의규정 신설 및 소프트웨어사업의 전부 하도급 금지, 다단계 하도급 제한 등을 통해 국내 소프트웨어산업의 건전한 생태계를 조성하려는 것임

■ 현행법은 소프트웨어공제조합의 이익배당을 금지하고 있어 다른 업종의 사업자에 비해 상대적으로 불리하고, 그로 인해 타산업과의 형평성 문제가 있으므로, 소프트웨어공제조합의 운영에서 발생한 이익이 있는 경우에는 이를 배당할 수 있게 하여 소프트웨어사업자의 재무적 건전성을 제고하고 소프트웨어산업의 건전한 발전에 이바지하려는 것임

주요내용

■ 발주자, 도급, 하도급, 수급인, 하수급인 등 하도급 관련 용어에 대하여 정의함 (안 제2조 제9호부터 제13호까지 신설)

■ 공공소프트웨어사업에서 일정비율 이상의 하도급을 제한하고, 하도급 사업의 재하도급을

원칙적으로 금지하며, 하도급 또는 재하도급하는 경우 사전에 국가기관등의 장으로부터 승인을 받도록 함 (안 제20조의3제1항, 제2항 및 제3항)

■ 국가기관등의 장은 전체 과업에서 일정비율을 초과하는 과업을 하도급받는 소프트웨어사업자의 공동수급체 참여를 요청할 수 있도록 하고, 요청받은 사업자는 특별한 사유가 없으면 이에 응하도록 함 (안 제20조의3제4항)

■ 국가기관등의 장은 하도급 비율 또는 재하도급 제한 규정을 위반한 소프트웨어사업자에게 시정을 요구하여야 하고, 시정요구를 이행하지 않은 사업자에게는 2년 이내의 범위에서 입찰참가자격을 제한함 (안 제20조의4 신설)

■ 소프트웨어공제조합의 이익금을 조합원에게 배당할 수 있도록 하고, 공제조합이 조합원의 지분을 취득할 경우 지분 변동을 반영할 수 있도록 함 (안 제33조3항, 제35조제1항 및 안 제35조제3항 신설)

※ 출처 : 국회 (http://www.assembly.go.kr)

5 사이버 사찰 방지를 위한 개정 법률(안) 발의 현황

1 통신비밀보호법

제안이유

■ 「통신비밀보호법」은 수사기관이 통신 관련 조치를 한 경우 그에 대한 통지는 해당 사건에 대한 공소 제기 등의 처분이 결정된 날부터 30일 이내에도 가능하도록 규정함 (법 제9조의2 및 제9조의3, 제13조의3)

– 이에 따라, 공소 관련 처분이 장기간 결정되지 않을 경우 국민은 무한정 자신의 사생활 비밀과 개인정보보호가 제한되고 있음에도 그 사실조차 알 수 없다는 문제가 야기됨

■ 통신 이용 범죄의 증가로 국가 수사권의 전기통신에 대한 개입이 증가되고 이로 인하여 이용자의 사생활의 비밀과 개인정보 보호에 제한이 가해지고 있는 만큼, 보완제도 마련이 시급하다고 판단됨

주요내용

■ 수사기관이 통신제한조치 등을 집행하면 그 집행이 있는 날부터 90일 이내에 수사대상이 된 가입자에게 수사기관이 집행한 내역을 통지*하도록 함 (안 제9조의2 및 제9조의3, 제13조의3 개정)

* 국가안보 · 공공의 안녕질서나 사람의 생명 · 신체 · 재산에 위험을 초래하는 경우에도 유예기간이 1년을 넘을 수 없도록 규정함(안 제9조의2제4항)

수사기관의 통지 의무 강화

- (제9조의2) 통신제한조치의 집행에 관한 통지 ⇒ 집행 후 90일 내
- (제9조의3) 압수 수색 · 검증의 집행에 관한 통지 ⇒ 집행 후 90일 내
- (제13조의3) 범죄수사를 위한 통신사실 확인자료의 제공의 통지 ⇒ 제공받은 후 90일 내

2 전기통신사업법

제안이유

■「전기통신사업법」은 법원의 허가나 영장 없이도 수사기관이 이용자의 성명, 주민번호, 주소 등이 담긴 통신자료의 제공을 요청하면 전기통신사업자가 요청에 따를 수 있다고 규정함 (법 제83조 제3항)

- 그러나, 정보주체인 가입자의 동의 없이 수사기관의 요청만으로 통신자료를 취득하는 것은 영장주의 위배의 소지가 있을 뿐만 아니라 헌법상 사생활 비밀과 자유 침해의 우려가 있어 개선이 필요함

주요내용

■ 개인정보에 대한 헌법상 기본권을 보장하기 위하여 통신자료의 제공에 대해서는 법원의 압수수색영장을 통하여 이루어질 수 있도록 함으로써 요청 절차를 강화함(안 제83조 제3항 등 개정)

■ 통신제한조치 등의 집행에 대한 사항*을 기재한 대장을 일반에 공개하도록 하여 국민의 알 권리를 보장하도록 함(안 제83조 제6항 개정)

* 전기통신사업자가 요청 또는 위탁받거나 협조한 통신제한조치, 통신사실 확인자료 제공, 압수 · 수색 등의 집행 현황에 대한 통계 등

3 개인정보 보호법

제안이유

■「개인정보 보호법」은 다른 법률에 따라 진행 중인 감사 · 조사, 성적 평가, 입학자 선발, 채용 등의 업무와 관련한 개인정보 등에 대하여는 정보주체의 열람을 제한할 수 있도록 규정함 (법 제35조 제4항)

- 그러나, 열람권의 제한 요건을 한정하지 않음으로 인하여 정보주체의 개인정보자기결정권을 침해가 우려된다는 비판이 지속 제기됨

■ 또한, 정보주체의 요구가 있는 경우에 한해 개인정보처리자가 이용내역을 통보하도록 규정하고 있어(법 제35조 등),

- 정보주체 입장에서는 본인의 개인정보가 어떻게 이용되는지 용이하게 파악하기가 어렵다는 문제점이 있음

주요내용

■ 정보주체가 개인정보처리자에 대하여 ①개인정보의 제3자 제공현황, ②개인정보처리자가 처리하는 자신의 개인정보 등에 대한 열람을 요구할 수 있도록 명시함 (안 제35조 제1항 개정)

■ 개인정보처리자가 정보이용 내역을 주기적으로 통지하도록 하여, 정보주체의 개인정보 자기결정권을 강화하도록 함(안 제38조의2 신설)

4 형사소송법

제안이유

■ 「형사소송법」은 검사 등은 수사에 관하여 공무소 기타 공사단체에 조회하여 필요한 사항의 보고를 요구할 수 있도록 규정 (법 제199조 제2항)

- 이에 따라 공공기관이 수사기관이 요청한 공문만으로 무분별하게 개인정보를 제공한다는 비판이 지속 제기됨

주요내용

■ 수사기관이 수사에 관하여 공무소 기타 공사단체에 조회하여 보고를 요구할 수 있는 사항을 최소한도의 범위 안에서 필요한 사항으로 한정하도록 규정하여 (안 제199조 제2항 개정),

- 공공기관에 대한 수사기관의 과도한 보고 요구권의 남용을 방지하고 무분별한 개인정보의 제공을 억제하도록 함

※ 출처 : 국회 (http://www.assembly.go.kr)

붙 임 일부개정 법률(안) 개정 사항

1 통신비밀보호법 개정안 ('14.12.9, 정청래 의원 대표발의)

현 행	개 정 안
제9조의2(통신제한조치의 집행에 관한 통지) ①검사는 제6조제1항 및 제8조제1항의 규정에 의한 통신제한조치를 **집행한 사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지 결정을 제외한다)을 한 때에는 그 처분을 한** 날부터 **30일** 이내에 우편물 검열의 경우에는 그 대상자에게, 감청의 경우에는 그 대상이 된 전기통신의 가입자에게 통신제한조치를 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 한다.	**제9조의2(통신제한조치의 집행에 관한 통지)** ①----------**종료한**----------**90일**----------.
②사법경찰관은 제6조제1항 및 제8조제1항의 규정에 의한 통신제한조치를 **집행한 사건에 관하여 검사로부터 공소를 제기하거나 제기하지 아니하는 처분(기소중지 결정을 제외한다)의 통보를 받거나 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그** 날부터 **30일** 이내에 우편물 검열의 경우에는 그 대상자에게, 감청의 경우에는 그 대상이 된 전기통신의 가입자에게 통신제한조치를 집행한 사실과 집행기관 및 그 기간 등을 서면으로 통지하여야 한다.	② ----------**종료한**----------**90일**----------.
③ (생 략)	③ (현행과 같음)
④제1항 내지 제3항의 규정에 불구하고 다음 각호의 1에 해당하는 사유가 있는 때에는 그 사유가 해소될 때까지 통지를 유예할 수 있다. **〈단서 신설〉**	④----------. **다만, 그 유예 기간은 1년을 넘을 수 없다.**
1. · 2. (생 략)	1. · 2. (현행과 같음)
⑤ 검사 또는 사법경찰관은 제4항의 규정에 의하여 통지를 유예하고자 하는 경우에는 소명자료를 첨부하여 미리 **관할지방검찰청검사장의 승인을** 얻어야 한다. 다만, 검찰관 및 군사법경찰관이 제4항의 규정에 의하여 통지를 유예하고자 하는 경우에는 소명자료를 첨부하여 미리 관할 **보통검찰부장의 승인을** 얻어야 한다.	⑤----**관할 지방법원의 허가를**----------. ----------**보통군사법원의 허가를**----------.

현 행	개 정 안
⑥ (생 략)	⑥ (현행과 같음)
제9조의3(압수 · 수색 · 검증의 집행에 관한 통지) ① 검사는 송 · 수신이 완료된 전기통신에 대하여 압수 · 수색 · 검증을 집행한 경우 그 **사건에 관하여 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는 그 처분을 한** 날부터 **30일** 이내에 수사대상이 된 가입자에게 압수 · 수색 · 검증을 집행한 사실을 서면으로 통지하여야 한다.	**제9조의3(압수 · 수색 · 검증의 집행에 관한 통지)** ①----------**집행이 있는**----------**90일**----------.
② 사법경찰관은 송 · 수신이 완료된 전기통신에 대하여 압수 · 수색 · 검증을 집행한 경우 그 사건에 관하여 검사로부터 공소를 제기하거나 제기하지 아니하는 처분의 통보를 받거나 내사사건에 관하여 입건하지 아니하는 처분을 한 때에는 그 날부터 30일 이내에 수사대상이 된 가입자에게 압수 · 수색 · 검증을 집행한 사실을 서면으로 통지하여야 한다.	**② 제1항에도 불구하고 다음 각 호의 어느 하나에 해당하는 사유가 있는 경우에는 그 사유가 해소될 때까지 통지를 유예할 수 있다. 다만, 그 유예 기간은 1년을 넘을 수 없다.** **1. 압수 · 수색 · 검증의 집행사실을 통지할 경우 국가의 안전보장 · 공공의 안녕질서를 위태롭게 할 염려가 있다고 믿을 만한 충분한 이유가 있는 경우** **2. 압수 · 수색 · 검증의 집행사실을 통지할 경우 사람의 생명 · 신체 · 재산에 위험을 초래할 염려가 있다고 믿을만한 충분한 이유가 있는 경우**
제13조의3(범죄수사를 위한 통신사실 확인자료제공의 통지) ①제13조의 규정에 의하여 통신사실 확인자료제공을 받은 **사건에 관하여 공소를 제기하거나, 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정을 제외한다)을 한 때에는** 그 **처분을 한** 날부터 **30일** 이내에 통신사실 확인자료제공을 받은 사실과 제공요청기관 및 그 기간 등을 서면으로 통지하여야 한다.	**제13조의3(범죄수사를 위한 통신사실 확인자료제공의 통지)** ①----------**경우에는**----------**제공을 받은**------**90일**----------.
② (생 략)	② (현행과 같음)

2 전기통신사업법 개정안 ('14.12.9, 정청래 의원 대표발의)

현 행	개 정 안
제83조(통신비밀의 보호) ① · ② (생 략)	제83조(통신비밀의 보호) ① · ② (현행과 같음)
③ 전기통신사업자는 법원, 검사 또는 수사관서의 장(군수사기관의 장, 국세청장 및 지방국세청장을 포함한다. 이하 같다), 정보수사기관의 장이 재판, 수사(「조세범처벌법」 제10조제1항 · 제3항 · 제4항의 범죄 중 전화, 인터넷 등을 이용한 범칙사건의 조사를 포함한다), 형의 집행 또는 국가안전보장에 대한 위해를 방지하기 위한 정보수집을 위하여 다음 각 호의 자료의 열람이나 제출(이하 "통신자료제공"이라 한다)을 요청하면 그 요청에 따를 수 있다. 1. 이용자의 성명 2. 이용자의 주민등록번호 3. 이용자의 주소 4. 이용자의 전화번호 5. 이용자의 아이디(컴퓨터시스템이나 통신망의 정당한 이용자임을 알아보기 위한 이용자 식별부호를 말한다) 6. 이용자의 가입일 또는 해지일	〈삭 제〉
④ 제3항에 따른 통신자료제공 요청은 요청사유, 해당 이용자와의 연관성, 필요한 자료의 범위를 기재한 서면(이하 "자료제공요청서"라 한다)으로 하여야 한다. 다만, 서면으로 요청할 수 없는 긴급한 사유가 있을 때에는 서면에 의하지 아니하는 방법으로 요청할 수 있으며, 그 사유가 해소되면 지체 없이 전기통신사업자에게 자료제공요청서를 제출하여야 한다.	〈삭 제〉
⑤ 전기통신사업자는 제3항과 제4항의 절차에 따라 통신자료제공을 한 경우에는 해당 통신자료제공 사실 등 필요한 사항을 기재한 대통령령으로 정하는 대장과 자료제공요청서 등 관련 자료를 갖추어 두어야 한다.	〈삭 제〉
⑥ 전기통신사업자는 대통령령으로 정하는 방법에 따라 통신자료제공을 한 현황 등을 연 2회 미래창조과학부장관에게 보고하여야 하며, 미래창조과학부장관은 전기통신사업자가 보고한 내용의 사실 여부 및 제5항에 따른 관련 자료의 관리 상태를 점검할 수 있다.	⑥ 전기통신사업자는 다음 각 호의 자료를 대통령령으로 정하는 방법에 따라 연 2회 미래창조과학부장관에게 보고하고, 그 내용을 인터넷 홈페이지 등을 통하여 공개하여야 한다. 다만, 국가의 중대한 이익을 현저히 해칠 우려가 있다고 인정되는 정보에 관하여는 공개하지 아니할 수 있다. 1. 「통신비밀보호법」 제9조 제3항, 제13조 제5항의 대장 2. 「형사소송법」 제106조 및 제109조에 따라 집행된 압수 · 수색 현황을 기재한 대장

현 행	개 정 안
⑦ 전기통신사업자는 제3항에 따라 통신자료제공을 요청한 자가 소속된 중앙행정기관의 장에게 제5항에 따른 대장에 기재된 내용을 대통령령으로 정하는 방법에 따라 알려야 한다. 다만, 통신자료제공을 요청한 자가 법원인 경우에는 법원행정처장에게 알려야 한다.	〈삭 제〉
⑧ (생 략)	⑧ (현행과 같음)
⑨ 자료제공요청서에 대한 결재권자의 범위 등에 관하여 필요한 사항은 대통령령으로 정한다.	〈삭 제〉
제94조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 2억 원 이하의 벌금에 처한다.	**제94조(벌칙)** ----------.
1. ~ 4. (생 략)	1. ~ 4. (현행과 같음)
5. 제83조제3항을 위반하여 통신자료제공을 한 자 및 그 제공을 받은 자	〈삭 제〉
제104조(과태료) ① ~ ④ (생 략)	**제104조(과태료)** ① ~ ④ (현행과 같음)
⑤ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만 원 이하의 과태료를 부과한다.	⑤ ----------.
1. ~ 13. (생 략)	1. ~ 13. (현행과 같음)
〈신 설〉	13의2. 제83조제6항을 위반하여 통신사실확인자료제공 현황 등을 미래창조과학부장관에게 보고하지 아니하였거나 공개하지 아니한 자
14. 제83조제7항을 위반하여 중앙행정기관의 장에게 통신자료제공 사실 등이 기재된 대장의 내용을 알리지 아니한 자	〈삭 제〉
15. ~ 17. (생 략)	15. ~ 17. (현행과 같음)
⑥ (생 략)	⑥ (현행과 같음)

3 개인정보 보호법 개정안 ('14.12.9, 정청래 의원 대표발의)

현 행	개 정 안
제35조(개인정보의 열람) ① 정보주체는 <u>개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당</u> 개인정보처리자에게 <u>요구할</u> 수 있다.	제35조(개인정보의 열람) ① ----------<u>해당</u>---------- ----------<u>다음 각 호에 대하여 열람을 요구할</u>-----.
<u>〈신 설〉</u>	<u>1. 개인정보의 제3자 제공현황</u>
<u>〈신 설〉</u>	<u>2. 그 밖에 개인정보처리자가 처리하는 자신의 개인정보</u>
② · ③ (생 략)	② · ③ (현행과 같음)
④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 <u>열람을</u> 제한하거나 거절할 수 있다. <u>〈단서 신설〉</u>	④ ---------- <u>제1항 각 호에 따른 열람을</u>----------. <u>다만 제3호의 업무에 대해서는 제1항제2호에 한정하여 열람을 제한하거나 거절할 수 있다.</u>
1. ~ 3. (생 략)	1. ~ 3. (현행과 같음)
⑤ (생 략)	⑤ (현행과 같음)
<u>〈신 설〉</u>	제38조의2(개인정보 처리내역의 통지) <u>① 개인정보처리자로서 대통령령으로 정하는 기준에 해당하는 자는 제15조제1항, 제18조제2항, 제23조 단서 및 제24조제1항 · 제3항에 따라 수집한 개인정보의 처리 내역(제17조제1항에 따른 제공 및 제26조에 따른 개인정보의 처리 업무 위탁을 포함한다)을 주기적으로 정보주체에게 통지하여야 한다. 다만, 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니하다.</u> <u>② 제1항에 따라 정보주체에게 통지하여야 하는 내역, 통지 주기, 방법, 그 밖에 처리 내역 통지에 필요한 사항은 대통령령으로 정한다.</u>

4 형사소송법 개정안 ('14.12.9, 정청래 의원 대표발의)

현 행	개 정 안
제199조(수사와 필요한 조사) ②수사에 관하여는 공무소 기타 공사단체에 조회하여 <u>필요한</u> 사항의 보고를 요구할 수 있다.	제199조(수사와 필요한 조사) ②---------- ---------- <u>최소한도의 범위 안에서 필요한</u>---------.

1. 입법 동향

1 일본, 사이버보안 (Cyber security)기본법 제정 (2014. 11. 6.)

개요

■ 일본은 정부의 사이버보안전략의 기반조성이라는 목표아래 사이버보안기본법의 제정을 추진하였다. 자민당 IT전략특명위원장(히라이타구야(平井たくや))은 올해 2월 의원입법으로 「사이버보안에 관한 기본법」을 입법추진하고 있다는 것을 공개적으로 밝힌 후, 신속하게 관련 법안을 국회에 제출하여 올해 11월 6일 동 법안이 통과되었으며, 11월 12일 공포되었다.

배경 및 입법 방향

■ 사이버공간에서 표적형 공격메일 등에 의한 기밀정보와 기술정보의 절취와 금융, 전력, 철도 등 중요 인프라(사회기반)에 대한 공격과 같은 사이버위협이 증가하고, 국경을 초월한 사이버공격 등 사이버 위협이 가해지고 있다.

– 이에 일본정부는 정보통신 인프라 정비와 정보통신기술의 이용 및 활용에 의한 행정, 의료, 교육 분야를 시작으로 하는 다양한 분야의 효율화와 서비스의 질을 향상시키면서 사이버위협에 대처하기 위해 사이버보안을 포함하는 정보보안의 필요성을 인지하고, 사이버보안체제의 강화를 위해 사이버기본법을 제정하게 되었다.

■ 이 법은 2013년 6월 내각에서 결정된 “세계 최첨단 IT국가창조선언”에 근거하여 모든 분야에서 정보통신기술의 이용 및 활용을 추진하고, 민간의 주도적인 역할 등을 정한 IT기본법의 기본적 틀을 따른다.

- IT의 이용 및 활용을 지원하는 정보보안에 관한 대응으로 산학관의 연계가 극히 중요하며, 특히 정부기관 등의 사이버위협에 대한 방어체제의 강화라는 국가안전보장에 관련하는 사이버보안의 관점에서 국가의 주도적인 역할의 명확하게 하고,

- 미국이나 영국 등 정보보안을 담당하는 국가조직의 기능강화와 체제의 확립이 계속해서 이루어지고 있는바 일본도 사이버보안에서 기본적인 가치관을 국가들 간 공유하고 나아가 국민들이 스스로 정보보안을 인식하고 지키도록 하여 국내산업을 활성화할 수 있는 방향을 제시하고자 한다.

■ 이를 위해 사이버보안의 강화를 포함하는 정보보안정책의 올바른 모습에 대해서 기본이념, 국가와 지방자치단체 등의 관계자의 책무, 국가에 의한 기본시책 그리고 이들의 종합적이고 효과적인 추진체계 등을 규정한 IT기본법의 특별법으로서의 "사이버보안기본법"이 필요하다.

- 동법의 제정으로 정부가 담당해야 하는 사이버보안강화를 위한 자세를 명확히 함과 동시에 그것을 위한 체제강화를 도모하고 2020년 개최예정인 동경올림픽의 사이버보안대책에 대해서 만전을 기하려는 것이기도 하다.

사이버보안기본법의 주요 내용

■ 사이버보안기본법은 총칙, 사이버보안전략, 기본적 시책, 사이버보안전략 본부의 4장과 부칙으로 구성되어 있으며, 전체적인 구성과 구체적인 내용은 다음 표와 같다.

■ **(목적)** 이 법은 정보의 자유로운 유통과 사이버보안의 확보를 위한 기본이념과 국가 등의 책무 등을 밝히는 것을 목적으로 하고 있다. 또한 경제사회의 활력향상과 지속적인 발전, 안전한 사회의 실현 및 국제사회의 평화확보 등에 기여하고자 한다(1조).

■ **(정의)** 사이버보안이란 전자적 방식, 자기적 방식, 그 외 다른 사람이 인식할 수 없는 방식으로 기록 및 수 · 발신되는 정보의 유출, 분실 또는 훼손방지, 그 외 해당 정보의 안전관리를 위해 필요한 조치로써 정보통신 네트워크의 안전성 및 신뢰성확보를 위해 필요한 조치가 마련되고, 적절하게 유지 관리되는 것이라고 정의하고 있다(2조).

사이버보안 기본법	
구성	주요내용
제1장 총칙	• 목적(제1조) • 정의(제2조) • 기본이념(제3조) • 관계자(국가 · 지방공공단체 · 중요사회기반사업자 · 사이버관련사업자 · 교육연구기관 · 국민)의 책무 등(제4~9조) • 법제상의 조치(제10조) • 행정조직의 정비 등(제11조)
제2장 사이버보안전략	• 사이버보안전략(제12조)
제3장 기본적 시책	• 행정기관 등에서의 사이버보안의 확보(제13조) • 중요사회기반사업자 등의 사이버보안확보의 촉진(제14조) • 민간사업자, 교육연구기관의 자발적인 대응의 촉진(제15조) • 다양한 주체의 연계(제16조) • 범죄단속 및 피해확대의 방지(제17조) • 국가의 안전에 중대한 영향을 미칠 우려가 있는 사안에 대한 대응(제18조) • 산업진흥 및 국제경쟁력 강화(제19조) • 연구개발추진(제20조) • 인재확보(제21조) • 교육 및 학습진흥, 보급계몽(제22조) • 국제협력의 추진(제23조)
제4장 사이버보안 전략본부	• 설치, 소관업무 등(제24~35조)
부칙	• 시행기일(제1조) • 필요한 법제의 정비(제2조) • 방어능력을 강화하는 시책의 검토(제3조) • IT기본법의 일부개정(제4조)

■ **(기본이념)** 제3조에서는 사이버보안기본법의 기본이념에 대해 다음의 사항을 규정하고 있다.

- 인터넷과 고도 정보통신네트워크의 정비 및 정보통신기술의 활용으로 표현의 자유 증진, 혁신(innovation)창출, 경제의 활성화 등을 저해하는 사이버 공간에서의 위협을 민관의 연계를 통해 능동적이고 적극적으로 대응한다.

- 국민 각자가 정보보안에 관한 인식을 높이고, 자발적인 활동을 촉진하여 피해를 방지하고, 피해가 발생한 경우 원활하고 신속하게 복구할 수 있는 체제를 구축하기 위한 대응을

적극적으로 추진한다.

- 미래의 정보통신기술의 혜택을 누릴 수 있도록 지속적인 개발 및 이용을 통해 창조적이고 활력 있는 경제사회를 구축하는 것이 중요하며 이를 위한 대응을 적극적으로 추진한다.

- 사이버공간에서 국제적 질서형성 및 발전을 위한 협조, 국제규범 형성, 신뢰양성조치, 개발도상국에 대한 능력구축지원 등의 적극적인 실시를 통해 일본이 국제사회의 선도적인 역할을 담당한다.

■ **(의무사항)** 국가, 지자체, 중요사회기반사업자, 사이버관련사업자, 교육연구기관 등의 관계자들이 부담하는 의무에 대해 규정하고 있다. (4조~8조)

- 국가는 관계부처 및 그 외 관계자와 최대한 연계하여 정보보안에 관한 종합적인 정책을 결정하고 실시한다.

- 지방공공단체는 사이버보안의 강화를 포함한 정보보안에 관한 시책에 관하여 국가와의 적절한 역할분담을 통해 자주적인 정책을 결정하고 실시하도록 노력한다.

- 중요 인프라 사업자 및 사이버관련사업자는 스스로 서비스를 지속적으로 안정적인 제공을 위해 정보보안의 중요성에 관한 이해와 관심을 높여서 정보보안에 노력함과 동시에 국가 또는 지방공공단체가 실시하는 사이버보안의 강화를 포함한 정보보안에 관한 정책에 협력한다.

- 교육연구기관은 적극적이고 자주적으로 사이버보안확보, 사이버보안관련 인재육성과 사이버보안에 관한 연구 및 성과 보급에 노력하며 정부 또는 지방공공단체가 실시하는 관련 정책에 협력한다.

■ **(사이버보안전략)** 정부가 사이버보안에 관한 정책을 종합적이고 효율적으로 추진하기 위해 사이버 보안전략을 수립하도록 하고 있다. 사이버 보안전략에는 ① 사이버보안에 관한 시책에 대한 기본방침 ② 행정기관 등의 사이버보안확보에 관한 사항 ③ 중요사회기반사업자와 그가 조직한 단체, 지방공공단체(이하 "중요사회기반사업자 등"이라고 한다)에서의 사이버보안 확보의 촉진에 관한 사항 ④ 앞의 3가지 외에 사이버보안에 관한 정책을 종합적이고 효과적으로 추진하기 위해 필요한 사항이 포함될 것을 규정하고 있다.

■ **(국가에 의한 기본적 정책)** 제13조에서 제23조까지는 국가에 의해 아래와 같은 기본적

시책을 추진할 것을 규정하고 있다.

주체	내용
행정기관 및 독립행정법인	• 정보보안에 관한 기준을 정비하고, 인터넷을 통한 외부 공격에 대한 감시 및 분석, 행정기관에서 발생하는 정보보안에 관한 사건에 관한 모의훈련 및 국내 · 외 관계자와의 긴급 연락 망과 대처방안, 행정기관간의 정보공유 등 추진
인프라(사회기반)사업자	• 정보보안에 관한 기준, 정보공유, 인프라 사업자 등에게 발생하는 정보보안에 관한 사건에 관한 모의연습 또는 훈련, 그 외 자주적인 대응 촉구
기업 및 교육연구기관	• 기업 및 교육기관에서 보유한 국제적으로 경쟁력있는 지적재산권 등에 관한 정보에 대하여 자발적으로 보안 활동을 수행하여 정보보안의 중요성에 관한 이해와 관심을 증진하고, 정보공유 및 상담체제의 정비, 조언 등을 수행
국가	• 사이버보안에 관한 범죄의 단속과 피해확대의 방지를 위해 필요한 정책을 마련
	• 정보보안을 자립적으로 수행할 능력을 일본이 보유하는 것에 대한 중요성을 부각하여 사이버 관련산업이 고용기회를 창출할 수 있는 성장산업이 되도록 신사업의 창출 및 건전한 발전 및 국가경쟁력의 강화를 도모하기 위해 정보보안에 관한 선도적이고 실용적인 연구개발의 추진, 성과의 보급, 국제표준화 및 평가와 인증 등 추진
	• 대학, 민간사업자 등과 긴밀한 협력을 도모하여 정보보안에 관련한 다양한 능력 및 지식경험을 갖고 있는 인재의 직무 및 직장환경이 개선으로 인재의 확보, 양성 및 자질향상을 위해 자격제도의 활용 및 청년기술자양성을 추진
	• 국민을 대상으로 정보보안에 관한 교육 및 학습의 진흥, 개발 및 지식보급 등을 수행
	• 국제적인 정보보안의 향상을 실현하기 위해 정보보안에 관한 국제규범 및 국제표준화 등에 관해 주체적으로 참여, 신뢰양성조치의 추진, 개발도상국에 대한 능력구축지원의 적극적인 실시 및 그 외 국제적인 연계확보를 위해서 필요한 조치를 강구, 국제적인 정보공유의 추진 및 필요한 국제협력을 추진

■ **(사이버보안전략 본부)** 제24조에서 제35조까지는 사이버전략본부의 설치, 소관사무, 조직, 권한 등에 대해 규정하고 있다.

– 일본의 경우 기존에는 정보보안에 관한 중요사항을 관방장관(官房長官)*을 의장으로 하는 정보보안정책회의에서 결정하며, 그 사무국을 내각관방정보보안센터(NISC)가 담당하고 있었다.

* 내각관방을 통솔하여 여러 사무를 처리하고, 내각의 중요한 결정 사항에 대해 조정을 실시한다. 또한 주요 사항에 대한 보고나 여러 가지 사태에 대한 정부의 공식 견해를 발표하는 '정부 보도관'등의 역할도 수행하므로, 언론에서 내각총리대신과 함께 노출되는 경우가 많고, 인지도가 높은 중요한 직위이다.

- 2005년 설치된 이래 정보보안에 대한 관련 경험과 지식을 축적해오고 있으나 법적으로 일정한 지위를 부여받은 기관은 아니므로 각 부처를 아우르는 기능을 충분히 발휘하고 있다고는 할 수 없는 상황이다.

- 따라서 사이버보안전략 본부의 법제화를 통해 법적인 근거를 부여함으로써 강력한 지도력을 갖고 민관 전체를 이끌 수 있도록 하고 있다.

- 이를 위해 사이버보안기본법에서는 사이버보안전략 본부(이하 "본부")가 기존의 정보보안 정책회의가 담당하고 있는 전략안과 정부기관보안기준의 책정에 더해서 중대사고의 원인규명(조사)와 행정기관의 경비 · 시책의 평가를 수행하도록 하고 있다.

- 사이버보안전략 본부의 법제화에 따라 행정기관에게 자료제출의무를 부과하고, 사이버보안전략 본부에는 행정기관에 대한 권고권과 조치보고의 청취권한을 부여한다. 또한 사이버보안전략 본부는 수상에게 의견을 보고할 수 있도록 하고 있다.

■ **(부칙)** 부칙에서는 시행일정(공포일부터 시행)과 관련규정 및 조직의 정비, IT기본법의 개정에 관한 사항을 규정하고 있다. 사이버보안기본법의 제정에 따라 기존의 정책회의 사무국기능을 담당하고 있는 내각관방정보보안센터(NISC)에 대해서는 부칙 2조에서 법제화를 명기하고 있고, 동조 제2항에서는 전문가의 임용, 내각법의 개정에 의해 내각홍보관, 내각정보관과 함께 차관급의 내각사이버보안(Cyber Security)관(官)을 신설할 방침을 나타내고 있다.

■ **(기타사항)** 일본정부는 이미 사이버보안기본법의 구체적 시행을 위한 조치를 서두르고 있으며, 국가주도의 사이버보안에 관한 구체적인 정책들이 이어질 것으로 예상되고 있다.

- 내각관방은 2015년 예산에 사이버보안전략 본부의 창설과 관련하여 "NISC기능강화 사업비"로서 15억 9천만 엔(한화 1조 5900억 원)을 우선과제추진비로 계상하였다. [1]

전망

■ 관련 산업의 고용확대와 신산업창출이라는 측면에서도 구체적인 움직임이 나타나고 있는데, 민간기업인 NEC가 사이버보안기본법의 국회통과 후 얼마 되지 않아 사이버보안사업과 관련한 인원을 대폭 확충하고 관련 사업을 강화하여 2017년에 관련매출의 목표를 2,500억 엔

1 http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=2

(한화 250조 원)으로 발표[2]하는 등 실제 경제 활성화의 움직임이 나타날 것으로 예상하고 있다.

참고자료

사이버보안기본법: http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm
「わが国のサイバーセキュリティ体制の強化に向けての提言」

https://www.hirataku.com/wp-content/themes/hirataku/pdf/6b98e5eeff44c9f7df98a4a7fd85f70e.pdf#search='%E3%82%8F%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%E4%BD%93%E5%88%B6%E5%BC%B7%E5%8C%96%E3%81%AB%E5%90%91%E3%81%91%E3%81%A6%E6%8F%90%E8%A8%80'

http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=1

http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=2

http://headlines.yahoo.co.jp/hl?a=20141119-00000060-impress-sci

2 독일 야당, 공개 무선랜 운영자의 책임을 완화하는 텔레미디어법 개정법률안 제출 (2014. 11. 5.)

개요

■ 독일 야당인 녹색당과 좌파정당인 링케는 공개 무선랜 운영자의 책임을 제한하는 텔레미디어법(Telemediengesetz, TMG)개정안을 제출하였다(2014. 11. 5.).

- 공개 무선랜 운영자의 책임과 관련하여 연방상원(Bundesrat)은 이와 관련한 입법안을 제정해 줄 것을 연방정부에 촉구하였고(2012. 10. 12.),

- 사회민주당(SPD)은 무선랜 운영자의 책임제한과 관련한 정책안을 연방하원에 제출하였으며(2012. 10. 23.),

2 http://headlines.yahoo.co.jp/hl?a=20141119-00000060-impress-sci

- 좌파정당 링케(Linke)는 무선랜 운영자의 책임제한 법률안을 연방하원에 제출(2012. 10. 23.)하였으나 국회 회기 만료로 더 이상 진행되지 못하다가,

- 이번 야당의 입법안 제출로 연방하원에서 입법논의가 다시 시작되었다.

배경

■ 디지털 사회로의 전환을 위해 독일에는 현재 수백만개의 사설무선랜과 공공무선랜(WLAN, Wireless Local Area Network)이 운영되고 있어 인터넷 접근이 누구나 어디에서든지 가능해졌다. 그러나 대다수의 무선랜 운영자들은 제3자의 공동 이용에 대해서 원치 않는 책임을 지지 않기 위해서 자신의 무선랜을 보호하고 있다.

- 이것은 연방대법원의 2010년 5월 12일자 '우리 인생의 여름 판결'[3]에서 암호를 제대로 설정하지 않은 무선랜을 권한없는 제3자가 몰래 이용하여 타인의 권리를 침해한 경우 그 무선랜 운영자는 '방해자책임'을 부담해야 한다는 판결의 영향이다. 이는 텔레미디어법의 입법목적에 반할 뿐만 아니라 이 법률이 근거로 삼고 있는 EU의 전자상거래 지침에도 반한다.

무선랜 운영자의 방해자책임

■ 무선랜 운영자는 타인의 권리를 직접 침해하지 않았기 때문에 손해배상 책임은 없다. 다만 그 침해에 어떠한 형태로든지 상당한 원인을 제공한 경우 장래에 이러한 침해가 다시는 발생하지 않도록 보호조치를 취해야 하고 피해자가 자신의 권리를 확보하기 위해서 지불한 비용에 책임이 있다. 이러한 방해자책임*은 오늘 날 제3자에게 무선랜 접근을 제공하는 데 중대한 장애가 되고 있다.

* 방해자책임(Störerhaftung) : '방해자책임'이란 어떠한 방식으로든 상당한 원인을 제공하여 제3자의 위법한 권리 침해(행위방해자)나 침해의 유지(상태방해자)에 기여한 경우에 인정되는 독자적인 민사책임의 한 유형으로 점검의무를 요건으로 한다. 점검의무는 침해의 제거나 장래 침해의 예방 조치를 내용으로 하며, 일반적으로 방해자가 권리침해를 인식한 경우에 인정된다. 점검의무 위반 시 그 법적 효과는 침해제거 및 침해예방청구의 대상이 되고, 만일 소송이 제기된 경우 소송비용과 변호사 비용을 부담해야 한다. 방해자책임은 물권법상 방어청구권에 근거를 두고 있으며, 방해자가 제3자의 위법한 침해에 공동행위자나 방조자 또는 교사자로 책임을 지지 않는 경우에 비로소 적용된다. 하지만 권리침해를 통지받은 후 의도적으로 이에 대한 조치를 지체 없이 취하지 않으면 불법행위(주로 방조자)가 인정되어 손해배상책임을 부담할 수 있다. 독일 판례는 이때 '지체없이'의 의미를 약 2주간으로 보고 있다.

3 BGH, Urteil vom 12.05.2010 – I ZR 121/08. 인터넷 가입자가 암호를 제대로 설정하지 않은 무선랜을 사용하던 중, 제3자가 이를 이용하여 타인의 저작권을 침해한 경우, 인터넷가입자가 어떠한 법적 책임을 지는가의 사안에서 연방대법원은 암호를 제대로 설정하지 않은 점에 대하여 방해자 책임을 부과하였다.

■ **(연방대법원)** 판례는 무선랜이 자주 암호화되어서 비용을 지불하지 않는 제3자의 공동이용은 불가능하다고 본다. 그러나 이것은 무선랜 운영자가 자신의 무선랜을 공동으로 이용하도록 개방하는 여러 가지 이유가 있음을 간과하는 것이다.

- 예를 들어, 무선랜을 제공함으로써 사업체 운영자는 고객에게 추가적인 서비스를 제공하거나, 사회적으로 어려운 사람들에게 인터넷 접근을 가능하게 하거나 자치단체에서 이웃 간의 시민네트워크가 가능해진다.

- 무선랜 운영자에 대한 법적인 불안정이 존재해 오고 있기 때문에 연방상원은 오래 전부터 방해자책임을 제거하여 텔레미디어법에 규정된 서비스제공자의 면책을 확대해야 한다고 연방정부에 요청하였다.

■ **(연방정부)** 자신의 '디지털 아젠더'의 공표와 관련하여 조만간에 법률안을 제출하겠다고 통지하였다. 이를 통해 "무선랜을 통한 모바일 인터넷의 보급과 이용을 개선하기 위해 공공장소(예를 들어 공항, 호텔, 카페 등)에서 그러한 무선랜 제공자의 법적 안정성을 마련할 것이며 무선랜 제공은 기본적으로 이들의 고객의 권리침해에 대하여 책임을 지지 않고 조만간 이에 상응한 법률안을 제출할 것이다"라고 하였다.

- 현재 연방정부가 계획하고 있는 '법적명확성을 마련할 것'이라는 말은 방해자책임이 상업적인 제공자에게는 더 이상 적용되지 않지만, 제공자가 사인인 경우에는 계속해서 적용되는지의 문제와 관련하여 아직 명확하지 않다. 이 점은 지금까지 연방정부가 공지한 것과 모순되며 스스로 진단한 무선랜 운영자의 법적 불안정이 부분적으로만 제거되는 것이다. 상업적 제공자와 사인의 제공자 사이에 그러한 구별을 하는 것은 지금까지와 다르기 때문에 눈여겨 봐야한다.

텔레미디어법 개정 내용

■ **(인터넷서비스 제공자 면책 규정)** 독일에서 인터넷서비스 제공자 (이하 ISP)의 면책에 관한 내용은 텔레미디어법(Telemediengesetz, TMG)에 규정되어 있다. 이 법률은 주로 정보통신망에서 유통되는 정보의 내용 규제와 특히 ISP의 책임과 관련되는 사항을 규정하고 있으며[4] ISP의 책임규정은 공법적, 민법적, 형법적 책임에 공통으로 적용되는 일반적 규정으로 되어 있다. 면책 규정은 ISP의 기능에 따라 다음과 같이 분류하고 있다.

4 정보통신망의 기술적인 부분은 전기통신법(TKG)에서 규정하고 있음.

주체	내용
콘텐츠 제공자	• 콘텐츠 제공자(즉 정보제공자)는 자신의 정보에 대하여 일반법률(민법 내지 형법)에 의하여 책임을 진다(텔레미디어법 제7조).
접속중개자	• 인터넷 접속중개자는 중개되는 타인의 정보에 대하여 원칙적으로 책임을 지지 않는다(텔레미디어법 제8조).
캐싱서비스 제공자	• 캐싱과 같이 정보가 임시 저장되는 경우 이의 운영자도 책임을 지지 않는다(텔레미디어법 제9조).
호스트서비스제공자	• 타인의 정보를 자신의 서버에 저장하는 Host Provider의 경우 위법한 행위나 위법한 정보를 인지한 후 지체 없이 조치를 취하여 정보를 제거하거나 접근을 차단한 경우에는 책임을 지지 않는다(텔레미디어법 제10조).

■ **(면책 책임의 배제)** 책임(제1항)의 배제는 상업적 · 비상업적 공개 무선랜 운영자도 포함한다(법률안 제8조 제3항). 이러한 책임의 배제는 금지 청구권도 포함된다(법률안 제8조 제4항).

■ **(금지청구권)** 연방대법원은 공동 이용에 대해서 완전하게 보호조치가 되지 않은 무선랜 운영자에 대한 책임을 금지청구권에 근거를 두고 있다.

※ 금지청구권(Unterlassungsanspruch) : 일정한 행위를 금지하도록 할 것을 내용으로 하는 청구권(부작위청구권, 중지청구권, 유지청구권이라고도 함)이다. 장래 그 침해의 위험이 임박한 경우에 대비하여 예방적 목적에서 인정되는 청구권인 부작위청구권은 현재의 침해행위에 대한 사후적 보호조치인 침해결과 제거 청구권(Beseitigungsanspruch)과 함께 권리의 침해에 대한 방어청구권의 일종이다. 점검의무를 위반하여 방해자책임이 인정되면 금지청구의 대상이 될 수 있다.

- 절대적 권리의 침해의 경우 직접 침해자나 침해에 참여한 자(교사자나 방조자)가 아니지만 어떠한 방식으로 의욕적이고 상당한 인과관계에 기하여 그 권리의 침해에 기여한 자는 방해자로서 금지청구의 대상이 될 수 있다. 완전하게 보호조치가 되지 않은 무선랜의 운영은 제3자가 이 무선랜을 통하여 행하는 권리침해에 상당한 인과관계가 인정된다. 사인의 무선랜 운영자도 그러한 점에서 권리침해에 대한 방해자책임이 되는 점검의무를 부담하게 된다.

- 따라서 권리침해에 대한 방해자책임은 제3자에게 공개된 무선랜 접속의 경우 배제되어야 하고, 무선랜 운영자가 의도적으로 또는 과실에 의해서 인터넷 접근을 이용하게 함으로써 타인의 권리침해를 모르는 경우가 아닌 한, 법적으로 금지청구의 대상이 되지 않는다.

- 인터넷 접속을 이용하게 한 자를 제3자의 권리침해에 대해서 청구의 대상이 되게 하는 것을

배제하는 것은 자치단체나 사업체 운영자 그리고 사인에게 공개적으로 접근하게 하거나 한정된 범위의 사람들에게 접근할 수 있는 무선랜 접속을 이용하는 것에 대한 요건이다.

■ **(공개무선랜 제공자)** 법률안 제8조 제3항은 공개 무선랜 운영자도 텔레미디어법 제8조의 서비스제공자로 간주되며 면책조항도 적용되어야 한다는 점을 명확히 하고 있다. 텔레미디어법 제8조는 제공자를 중심으로 편성되어 있다. 하지만 다른 서비스제공자도, 즉 텔레미디어법 제2조 제1문 제1호에 의해서 자신 또는 타인의 텔레미디어를 이용에 제공하거나 접근을 중개하는 모든 자연인 및 법인을 포함한다. 이미 오늘 날 무선랜 운영자도 여기에 포섭될 수 있다. 하지만 지금까지 논쟁이 되고 있어 법적안정성 측면에서 바람직하지 않다.

■ **(방해자 책임의 면책 조항 적용)** 법률안 제8조 제4항은 금지청구권에도 면책규정이 적용된다는 것을 명확히 함으로써 제1항의 책임규정을 소위 방해자책임으로 확대하는 것이다. 제8조 제1항은 이미 통신망에서 타인의 정보만을 전달하거나 타인의 정보 이용을 위한 접근을 중개하는 서비스제공자에게 면책을 규정하고 특히 전문적인 제공자를 염두에 두고 있다. 하지만 다른 서비스제공자도 여기에 포함된다. 텔레미디어법 제2조 제1문 제1호에 의하면 자신 또는 타인의 텔레미디어를 이용하도록 제공하거나 이용 접근을 중개하는 모든 자연인 및 법인을 제공자로 보고 있다. 따라서 여기에는 사인 및 상업적인 무선랜도 포함된다. 제3항을 통해서 이를 다시 한 번 명백하게 강조하고 있다.

– 제8조 제1항의 면책이 어느 범위에서 금지청구권에도 배제되는지에 대해서는 아직 불명확하지만 연방대법원은 이 문제를 심사하지 않았다. 면책이 금지청구권에도 명백하게 규정됨으로써 지금까지의 법적불안정은 제거되어야 한다. 동시에 법률안 제3항을 통하여 무선랜 운영자도 텔레미디어법상의 서비스 제공자로 간주될 수 있고 텔레미디어법 제8조 제1항 및 제4항의 면책도 적용되어야 한다.

향후 계획

■ **(바이에른 주 전 지역에 공개 무선랜 보급 계획)** 공개 무선랜과 관련하여 바이에른 주는 2014년 11월 27일 주 전 지역에 무료 공개무선랜을 보급하겠다고 발표하였다. 먼저 2015년부터 성(Burg), 성(Schloss), 국가 운영하는 배에 60개의 무료 무선랜을 설치하고, 두 번째 단계에는 2016년부터 바이에른 주의 모든 관공서, 그리고 마지막 단계에서 모든 지방자치단체에 무선랜을 보급하여 2020년에는 모든 주에 무료 무선랜이 보급되어 바이에른

네트워크를 구축할 것이라고 한다.[5] 다만 이때 공개무선랜은 공공기관에만 해당하고 사인의 무선랜에는 해당하지 않는다.

참고자료

법률안 : http://dip21.bundestag.de/dip21/btd/18/030/1803047.pdf

http://www.golem.de/news/gruene-und-linke-gesetzentwurf-gegen-stoererhaftung-offener-wlans-vorgelegt-1411-110417.html

http://www.heise.de/newsticker/meldung/Bayerns-Finanzminister-Soeder-verspricht-freies-WLAN-im-laendlichen-Raum-2466894.html.

3 터키, 전자상거래 서비스 제공자의 이용자 보호의무를 강화하는 전자상거래 규제법 공포 (2014. 11. 5.)

개요

■ 터키 「전자상거래 규제법」(Law Regulating Electronic Commerce)이 11월 5일 공포되어 2015년 5월 1일부터 발효될 예정이다.

배경 및 경과

■ 터키 「전자상거래 규제법」은 「유럽의회 및 정보사회 서비스의 법률에 관한 위원회의 지침」(the Directive 2000/31/EC of the European Parliament and of the Council on Certain Legal Aspects of Information Society Services)과 조화를 이루기 위한 것으로, 지난 3년동안 의회에서 계류되어 있다가 2014년 10월 23일 의회를 통과하였다.

5 http://www.heise.de/newsticker/meldung/Bayerns-Finanzminister-Soeder-verspricht-freies-WLAN-im-laendlichen-Raum-2466894.html.

주요내용

■ **(서비스제공자의 통지 의무)** 전자 미디어를 통하여 계약을 이행하기 이전에 서비스 제공자는 계약에 대한 설명정보, 계약 이행의 기술적인 단계 및 기밀관련 규칙과 관련한 거래관련 정보를 제공하여야 한다.

- 서비스 제공자는 계약조건 및 일반적 조건을 고객이 보관할 수 있도록 하고, 주문정보 확인 및 수정할 수 있는 기회의 제공 등을 반드시 이행해야한다.

- 또한 서비스 제공자는 주문 영수증을 전자 통신 기기를 통하여 바로 확인해주어야 하는 의무가 있고, 서비스 제공자가 발송하는 상업적 전자 메시지의 내용을 열어보지 않고도 수신자가 발송자의 정보(신원 및 연락처 정보)에 대해서 알 수 있도록 하며 제3자를 대신하여 전자 메시지가 발송된 경우 그 제3자에 대한 정보도 포함되어야 한다.

■ **(서비스제공 중개자의 의무)** 타인의 상업적 행위를 위해 전자상거래 환경을 제공하는 중개자연인 혹은 법인은 그가 제공하는 상품 및 서비스가 법을 준수하는지 여부에 대해 점검할 의무를 지지 아니한다.

■ **(개인정보 보호의무)** 서비스 제공자 및 서비스 제공 중개자는 전자상거래를 통하여 획득한 개인정보의 저장 및 보안에 책임이 있으며, 개인의 사전 동의 없이 다른 목적을 위하여 제3자에게 해당 개인정보를 전송하거나 사용해서는 안된다.

■ **(사전동의 획득 의무)** 이 법은 상업적 전자메시지의 전송에 대해 "옵트인(opt-in)"시스템을 채택하여 SMS, 전자메일 혹은 전화 등 전자 장비를 통하여 상업적 메시지를 전송할 경우에 수신자의 사전 동의를 얻도록 한다.

- 다만 제공된 상품 및 서비스 내용의 변경 또는 사용 및 유지에 관한 상업적 전자메시지를 발송하는 경우는 예외이지만 이 경우에도 상업적 전자 메시지의 수신자가 사전에 연락을 받을 목적으로 자신의 연락정보를 공유한 경우에만 가능하다.

※ 이러한 옵트인 제도의 예외는 기존에 판매된 소프트웨어 혹은 모바일 어플리케이션의 업데이트 등에 해당할 것으로 보임

■ **(과태료 부과) 동 법을 위반하는 서비스 제공자 및 서비스 제공중개자는 TRY1,000(한화 500,000원)부터 15,000(한화 7,500,000원)에 이르는 과태료를 납부해야한다.**

- 만일 상업적 전자메시지가 사전 동의 없이 1인 이상의 수신자에게 전송 된 경우 개별 과태료의 10배에 달하는 과태료가 부과된다.

평가

- 사업자와 고객사이 원거리 계약은 이미 소비자보호법 (Code of Consumer Protection) 및 관련 법령에 따라 규율되고 있어, 원거리 계약이 전자상거래 형태로 이루어지는 경우 해당 법률등과의 유사성으로 인한 적용범위에 혼란이 발생할 우려가 있다는 의견이 있다.

참고자료

http://www.lexology.com/library/detail.aspx?g=d4afd0a7-bb33-49f7-86c8-f0f5e0280204&utm_source=Lexology+Daily+Newsfeed&utm_medium=H%E2%80%A6

http://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm

http://www.mondaq.com/x/354756/IT+internet/Parliament+Finally+Approves+ECommerce+Law

http://www.morogluarseven.com/news/save-date-may-1-2015-e-commerce-turkey

2. 판례 및 이슈

1 EU정보보호기관, '잊혀질 권리'와 관련한 검색엔진의 검색 결과목록 삭제기준을 제시하는 가이드라인 결정 (2014. 11. 26.)

개요

■ EU의 28개 회원국의 데이터보호기관들(European Data Protection Authorities, DPA)은 EU시민들의 권리를 보장하기 위해 구글(google)과 빙(bing) 등의 검색엔진 운영자에 대해서 삭제 대상 도메인을 전 세계 도메인으로 확대하여 이행하기 위한 가이드라인을 결정하였다 (2014. 11. 26.).

– 이는 2014년 5월 유럽사법재판소의 '잊혀질 권리'판결[6]을 반영한 것이다.

EU의 '잊혀질 권리'판결 (C–131/12)

사건 경위

• 스페인 변호사 코스테하 곤잘레스가 구글 검색에서 이미 오래전에 완전히 해결된 일인 본인의 사회보장 채무와 부동산 강제 경매에 대한 신문기사가 계속 검색되는 것에 대해 스페인 개인정보보호기구(AEPRD)에 진정하여, 해당신문사에는 기사 삭제 또는 특정 Tool을 이용하여 더 이상 검색엔진에 드러나지 않을 것을 요청함과 동시에 구글측에 검색결과를 삭제 혹은 숨겨줄 것을 요청함.

양측 주장

• (구글 측 주장) 개인정보 삭제 요구는 개인정보의 처리가 정보주체의 특별한 상황에 따라 지침이나 강행 법규에 위반되는 경우만 적용하여야 하며, 비례성 원칙을 고려하여 기본권들 간의 균형을 맞추어야 한다고 주장
• (정보주체측 주장) 완전히 해결된 과거사건으로 정보주체에게 불리하거나 프라이버시 또는 개인정보 보호를 위한 기본권을 해치는 개인정보 유포가 검색엔진을 통해 일어났다면 정보주체가 자신과 관련된 검색엔진상의 개인정보 삭제 또는 공개를 거부할 권리가 있다고 주장

6 ECJ, 13.5.2014, C–131/12.

판결 요지

- 제3자가 작성한 합법적 공표물의 검색결과에 대한 검색엔진의 책임을 인정함. 즉, 프라이버시권 보호를 위해 표현의 자유 침해가 있을 수 있으며 정보주체의 프라이버시권과 특정 정보에 접근한 인터넷유저들의 잠재적인 합법적 이익(정보의 자유)과의 균형을 고려하여 판단할 때 현 사안에서 검색엔진의 책임을 인정함
- 모든 정보를 삭제 가능한 것은 아니지만 특정의 시간이 지난 뒤에는 '잊혀지는 것(Forgotten)'을 원하거나 정보주체에게 불리한 정보, 동의기간 만료 정보, 유효기간이 도과된 정보 또는 수집 · 이용 목적을 넘어선 경우라면 제3자에 의해 합법적으로 발행된 자료에 관한 검색 결과물에 대해서도 검색엔진 사업자의 책임을 인정함

- 데이터보호기관들은 지금까지 구글의 검색엔진 결과목록을 삭제해 달라는 절차요건이 명확하지 않다고 판단하고 구글과 마이크로소프트에 검색 결과의 링크 삭제를 유럽을 넘어서 전 세계를 대상으로 이행할 것을 요청하였으나 이것이 제대로 되지 않는다고 판단하여 가이드라인을 결정하게 되었다.

- 구글의 최근 보고에 따르면 지난 5월 이후 602,479의 링크가 포함된 174,226개의 삭제신청을 받았고 이 중에서 41.5%은 유럽에서 삭제되었다고 한다.[7]

가이드라인의 주요 내용

■ **(데이터 처리 책임자로서의 검색엔진)** 검색엔진운영자는 개인데이터(개인정보)를 처리하므로 데이터 처리책임자로서의 지위를 가진다.

■ **(프라이버시 기본권과 경제적 이익 사이의 공정한 균형)** "검색엔진제공자의 데이터 처리가 프라이버시 기본권과 데이터 보호에 미치는 잠재적 영향력의 심각성을 고려할때 일반적으로 데이터 주체의 권리가 검색엔진운영자의 경제적 이익과 검색엔진을 통해서 개인 정보에 접근할 인터넷 이용자의 이익보다 우월하다"고 한다. 하지만 해당 기본권과 이익들은 균형을 이루어야 하고 처리되는 데이터의 성격과 민감성 그리고 특별한 정보에 접근할 공공의 이익에 따라 사안별로 판단해야 한다.

■ **(검색 결과목록 삭제와 정보 접근의 상관성)** 실제로 검색 결과목록 삭제가 개인의 표현의

7 http://www.heise.de/newsticker/meldung/EU-Datenschuetzer-Google-muss-Links-weltweit-loeschen-2466684.html; http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en.

자유와 정보 접근권에 미치는 영향은 미비할 것이다. 데이터보호기관은 정보에 접근하려는 공중의 이익을 체계적으로 고려하여 공중의 이익이 데이터 주체의 권리보다 큰 경우에는 검색결과 목록을 삭제하지 않는다.

- **(원천적인 정보의 삭제)** 개인의 이름을 입력하여 얻은 검색 결과에만 삭제 요청이 영향을 미치고 검색엔진의 인덱스에서 링크의 삭제를 요구하지 않으므로 원래의 정보는 여전히 다른 검색어를 사용하거나 발행자의 원래의 소스를 통해 직접 접근할 수 있다.

- **(검색 결과목록 삭제를 위한 방법)** 검색 결과목록 삭제 결정은 데이터 주체의 권리를 효과적이고 완벽하게 EU 법률에 부합하는 방법으로 이행되어야 한다. 이때 도메인 ".com"을 포함하여 모든 도메인에서 검색 결과목록의 삭제가 이행되어야 효과가 있다.

- **(공중에게 정보삭제에 대한 통지)** 이용자의 조회로 나타나는 검색 결과의 목록이 일부 정보가 삭제되어 완전하지 않다는 것을 검색 엔진의 이용자에게 통지하는 것은 데이터 보호법이 정한 법적 근거가 없으므로 관행에 따르도록 한다.

검색 결과목록 삭제를 위한 가이드라인

- **(개인과 관련된 정보)** 검색 결과가 자연인으로서의 데이터 주체의 이름을 검색하여 나온 것인지에 따라 개인과 관련된 정보임을 판단한다. 구글 판결은 개인의 이름을 기반으로 한 인터넷 검색이 개인의 사생활에 중대한 영향을 준다는 것을 인식하고 있고 데이터보호기관 역시 가명과 별명이 개인의 신원(ID)과 링크되어 있는 것을 증명할 수 있는 경우에는 그러한 가명과 별명도 삭제 대상으로 고려해야 한다고 명시하고 있다.

- **(공인으로서의 데이터 주체)** 데이터 주체가 공인인 경우에 이러한 정보에 접근하는 공중의 이익을 고려하여 목록 삭제 요청의 예외를 인정하고 있다. 이 기준은 '공인'의 기준보다 더 광범위하게 해석한다.

  - 정치인, 고위직 공무원, 규제를 받는 사업가, 전문직 종사들은 공적 생활을 하는 것으로 간주하여 공중이 이들의 공적인 역할과 활동에 관한 정보를 검색이 가능하게 하여 이들의 부적절한 공적인 행위나 전문적인 행위를 예방하기 위함이다.

  - 또 '공적인물'이 누구인지에 대해서 일반적으로 이들의 기능이나 책임 때문에 미디어에 노출되는 사람들이라 정의한다.

※ 프라이버시 권리에 관한 유럽평의회의 1998년 결의안 1165

이 결의안은 '공인'에 대한 개념 정의를 제공하고 있다. 이에 따르면 '공인'이란 공무를 담당하고 있거나 공적 자원을 이용하고 있는 사람들을 의미한다. 보다 광범위하게 말하면 정치, 경제, 예술, 사회적 영역, 스포츠 또는 그 밖의 다른 영역에서 공적인 역할을 하고 있는 모든 사람들이라고 정의하고 있다. 지극히 사적인 공인에 관한 정보, 예를 들어 건강이나 가족 구성원에 관한 정보들에 대해 삭제할 수 있는지에 대해서는 유럽인권법원(European Court on Human Rights, ECtHR)의 판례가 특별히 중요하다.

유럽인권법원의 Hannover v. Germany (no.2), 2012 판결

- "당사자의 역할과 기능 그리고 보도 또는 사진 촬영 주체의 활동 성격은 다른 중요한 기준이 된다. 이와 관련하여 사적인 개인과 공적인 맥락에서 활동하는 사람, 예를 들어 정치적 인물이나 공적 인물 사이에는 구별이 있어야 한다. 따라서 공중에게 알려지지 않은 사적인 개인은 자신의 프라이버시 권리의 특별한 보호를 주장할 수 있는 반면에 공인에게는 그렇지 않다. 예를 들어 정치인들의 공식적인 기능의 행사에서 정치인과 관련하여, 민주주의 사회에서 논의에 기여할 수 있는 보도 사실과 그러한 기능을 수행하지 않는 개인의 사생활을 보도하는 것 사이에는 명확한 구별이 있어야 한다" 고 판단했다.

■ **(미성년자인 데이터 주체)** 일반적으로 데이터 주체가 법적으로 미성년자인 경우(정보의 공개 시점에 만 18세가 되지 않은 경우) 데이터보호기관은 해당 검색 결과를 목록에서 삭제하게 할 것이다. 이때 '아동의 최선의 이익'을 고려해야 하며 이는 EU 기본권 헌장 제24조 "공공기관이나 사설기관에서 행해지는 아동과 관련한 모든 조치들은 아동의 최선의 이익을 우선적으로 고려하여야 한다"를 근거로 한다.

■ **(데이터의 정확성)** 일반적으로 '정확한'이란 의미는 사실관계가 정확한지를 말한다. 타인의 의견으로 관련이 있는 검색 결과와 명확한 사실에 관한 정보를 포함하는 검색결과 사이에는 구별이 있어야 한다.

- 데이터보호법에서 정확성, 적절성(타당성), 불완전성(불충분성)의 개념들은 밀접하게 연관되어 있다. 데이터보호기관은 사실의 문제에 대해 부정확하고 불충분하거나 오해를 야기할만한 개인의 의견을 게시한 경우에는 검색 결과의 목록 삭제가 적절한 것으로 간주한다.
- 데이터 주체가 정보가 부정확한 것을 이유로 검색 결과에 이의를 제기하며 입증을 위해 필요한 모든 정보를 이의 제기자가 제공한다면 데이터보호기관은 그러한 요청을 다룰 수 있다. 정보의 정확성에 관하여 다툼이 아직 진행 중인 경우 (예를 들어 법원에 계류 중이거나 경찰의 수사가 진행 중이거나 하는 경우)에는 데이터보호기관은 그 절차가 종료될 때까지 개입하지 않도록 한다.

- **(데이터의 관련성)** 검색 결과에 포함되어 있는 정보가 일반적인 공익과 관련이 있는지 아닌지를 평가하는 것이다. 관련성은 데이터가 공개된 시점과 밀접하게 관계된다. 사법재판소의 판결 사안에서 보면 예컨대 15년 전에 공개된 정보는 1년 전에 공개된 정보보다 관련성이 적다고 보았다.

- **(민감한 정보인지의 여부)** 일반적으로 민감한 데이터(지침 95/46/EC 제8조에서'특별한 데이터 범주'로 정의된)는 보통 개인 데이터보다도 데이터 주체의 사생활에 훨씬 더 많은 영향을 준다. 예를 들어 개인의 건강, 성생활 또는 신앙에 관한 정보 등이 해당한다.

- **(데이터의 최신성)** 최신 데이터인지 데이터가 처리 목적에 필요한 것 보다 더 오랫동안 이용(접근)되고 있는지를 판단한다. 일반적으로 데이터보호기관은 시사성이 없는 정보이거나 오랜 시간이 흘러 정확하지 않게 된 정보는 삭제되어야 한다는 목적을 가지고 이 요인을 기준으로 삼았다.

- **(데이터주체에 관한 편견을 가져오는 민감정보)** 데이터처리가 데이터주체에 관한 편견을 야기하는지 판단한다. 검색결과로 인해 데이터 주체에게 편견을 야기할 수 있는 증거가 되는 경우에는 이것은 목록 삭제를 위한 중요한 요인이 된다.

- **(데이터주체에게 위험을 주는 정보)** 검색결과가 데이터 주체에게 위험을 주는 정보와 연결되어 있는지 판단한다. 데이터보호기관은 인터넷 검색을 통해서 어떤 정보를 이용할 가능성이 데이터 주체에게 아이디 절도나 스토킹과 같은 위험에 노출될 수 있도록 한 경우 삭제가 적절한 것으로 고려할 것이다.

- **(정보 발행의 맥락)** 내용이 데이터 주체에 의해서 자발적으로 공개되었는지, 합리적으로 정보의 공개를 인지했는지 고려해야한다. 인터넷에서 개인 데이터를 이용할 수 있게 한 유일한 법적 근거는 동의이지만 이러한 동의를 철회하면 그 처리 활동의 법적 근거를 상실되어 처리가 중단된다. 삭제 요청을 심사하는 경우 데이터보호기관은 이름과 정보가 사전에 또는 동시에 원래의 소스로부터 삭제된 경우에도 링크가 삭제되어야 하는지를 고려한다. 특히 데이터 주체가 원래의 공개를 동의하였지만 이후에 이러한 동의를 철회할 수 없었고 삭제 요청이 거부된 경우에 데이터보호기관은 일반적으로 검색 결과의 목록 삭제는 적절하다고 보아야 한다.

- **(언론 보도의 목적으로 공개)** 정보가 언론 보도의 목적으로 공개되었는지를 고려하는 것은

중요하다. 정보를 공중에게 알리는 저널리스트에 의해서 공개된 사실은 비교적 균형 갖춘 정보이지만 이 기준만으로는 삭제요청을 거부할 충분한 근거를 제공하지는 못한다. 사법재판소 판결에서 미디어 공개에 대한 법적 근거와 개인의 이름에 기초하여 검색결과를 구성하는 검색 엔진의 법적 근거는 명확하게 구별하고 있기 때문이다.

- **(데이터 발행인의 정보를 공개할 법적 권한)** 데이터의 발행인은 개인 데이터를 공개할 법적 권한이나 법적 의무를 가지는지 판단한다. 예를 들어 선거 후보자 등록을 위한 경우 등 개인에 관한 어떤 정보를 공개할 법적 의무가 있다. 정보 공개의 법적 의무는 회원국의 법률과 관습에 따라서 다양하고 이러한 경우에 공공 기관에게 정보를 공개할 요건이 지속되는 한 데이터보호기관은 삭제가 적합하다고 고려하지 않을 수 있다. 하지만 이것은 사안별로 평가되어야 할 것이며 시의에 맞지 않는지 어느 정도 관련 있는지 등을 함께 고려하여야 할 것이다.

- **(범죄와 관련된 데이터)** 데이터가 범죄와 관련되는지 판단한다. EU 회원국은 범죄자의 정보를 공개하는 것에 대해서는 의견차이가 있어 데이터보호기관은 각국의 원칙을 준수하면서 사례를 다룰 것이다. 대부분의 각국 데이터보호기관은 오래 전에 발생한 상대적으로 경미한 범죄와 관련되는 검색 결과의 목록 삭제를 고려할 것이지만 이러한 이슈들은 신중한 고려가 필요하고 사안별로 다루어져야 할 것이다.

전망

- EU 정보보호기관들이 수개월에 걸쳐 작업한 이 가이드라인은 법적 강제력은 갖고 있지 않다.[8] 따라서 정보보호기관들의 요구대로 지침이 잘 활용될지는 의문이다. 그러나 이 가이드라인을 통해 지난 5월 유럽사법재판소의 구글 판결에서 아직 명확하게 다루지 못한 여러 가지 법적인 문제들을 명확히 할 수 있는 기회가 될 것이다.

참고자료

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf

http://www.heise.de/newsticker/meldung/EU-Datenschuetzer-Google-muss-Links-weltweit-loeschen-2466684.html

http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en

http://www.jurablogs.com/go/eu-datenschuetzer-fordern-weltweite-loeschung-von-links

8 http://www.jurablogs.com/go/eu-datenschuetzer-fordern-weltweite-loeschung-von-links.

2 EU 데이터보호 특별조사위원회, 전자프라이버시지침은 디바이스 핑거프린팅(Device Fingerprinting)에 적용된다는 의견 발표 (2014. 11. 25.)

개요

■ EU 데이터보호 특별조사위원회(Articl 29 Data Protection Working Party, WP29)는 인터넷에서 이용자를 추적하기 위한 디지털 지문을 채취하는 디바이스 핑거프린팅(Device Fingerprinting)*은 EU 전자프라이버시지침에 적용된다는 의견서를 발표하였다(2014. 11. 25.).

* 디바이스 핑거프린팅은 저작권자나 판매자의 정보가 아닌 콘텐츠를 구매한 사용자의 정보를 삽입함으로써 이후에 발생하게 될 콘텐츠 불법 배포자를 추적하는데 사용하는 기술이다. 저작권자 또는 판매자의 정보를 멀티미디어 콘텐츠에 삽입하는 측면에서 워터마킹(water marking)과 동일하지만 저작권자나 판매자의 정보가 아닌 콘텐츠를 구매한 사용자의 정보를 삽입하여 이후에 발생하는 콘텐츠 불법 배포자를 추적하는데 사용하는 기술이다.

배경

■ 이용자의 데이터보호에 주안점을 둔 것으로 수많은 온라인 서비스는 전자프라이버시지침 제5조 제3항의 동의가 필요 없는 분석이나 트래킹(추적)을 가능하게 할 목적으로 디바이스 핑거프린팅을 HTTP 쿠키의 대안으로 제안해 왔다. 이는 디바이스 핑거프린팅에 의해서 제기되는 위험들이 단순히 이론적인 것이 아니며, 이미 디바이스 핑거프린팅이 부당하게 이용되고 있는 것을 보여주고 있다.

■ **(기술적 배경)** 인터넷과 웹은 탄력적이고 개방형 구조의 네트워크 환경을 구축하기 위해 발전되어 왔다. 이러한 필요성을 충족하기 위해서 디바이스들은 정보 요소들을 전송하여 많은 프로토콜들은 수많은 필수적인 정보요소나 선택적인 정보요소들 포함하고 있다.

- 예를 들어 HTTP/1.1 프로토콜은 서버와 클라이언트가 하이퍼텍스트에 관한 부가 정보를 포함하도록 허용하는 헤더 필드를 구체적으로 명시한다. 이들 중 일부는 구체적으로 서버가 클라이언트의 유형을 인식하도록 의도되어 있다.

- 또한 사용자 에이전트 문자열(User Agent String)를 사용하는 전형적인 이유는 특별한 디바이스의 유형을 위한 콘텐츠 레이아웃의 최적화를 포함시키기 위한 것이다. 구체적인 이용자의 콘텐츠를 대상으로 삼기 위해 이 정보를 이용하거나 보안 또는 분석 목적으로 이

디바이스에 관한 정보를 수집하기 위해서 사용자 에이전트 문자열을 사용한다.

■ **(법적 배경)** 수정된 전자프라이버시 지침 2002/58/EC 제5조 제3항은 다음을 규정하고 있다. "가입자 및 이용자의 단말 장치에 이미 저장되어 있는 정보를 저장하거나 이 정보에 접근을 획득하는 것"은 지침 95/46/EC(데이터보호지침)에 따라 특히 처리의 목적에 관하여 명확하고 이해할 수 있는(포괄적인) 정보를 제공하여 가입자 또는 이용자가 동의를 한 경우에만 허용된다.

- 2012년 4월 의견에서 쿠키의 이용을 통한 정보의 저장 및 접근과 관련하여 전자프라이버시 지침 제5조 제3항을 고려하였다. 이 의견은 제5조 제3항이 전적으로는 적용되는 것은 아니지만, "유사한 기술"에 적용될 수 있다고 본다. 제3자가 적극적으로 제5조 제3항의 동의 요건을 회피할 목적으로 쿠키의 대안을 찾고 있다는 보도가 증가하고 있으며 특히 기기(장치) 또는 응용장치의 신원을 유일하게 확인하기 위해서 정보 요소들을 결합하는 예로서 소위 디바이스 핑거프린팅이 검토되고 있다.

디바이스 핑거프린팅과 데이터 보호

■ **(디바이스 핑거프린팅)** EU 데이터보호 특별조사위원회의 의견서에서 핑거프린트를 '디바이스 및 어플리케이션 인스턴스를 확인하는 정보 요소의 결합체'라고 정의하고 있다. 광범위하게 사용한 개념으로 이용자, 사용자 에이전트(통신망) 또는 기기를 통해 개인 식별정보 및 기록을 추론하는데 이용될 수 있는 모든 정보를 포함하는 의미로 광범위하게 사용한다.

- 디바이스 핑거프린팅은 개인 정보를 구성할 수도 있다. 중요한 데이터보호 문제와 관련하여 여러 정보 요소들, 특히 IP주소와 같이 유일한 식별자들이 결합되고, 온라인 행동 광고(behavioural advertising,이용자의 인터넷 패턴에 따라서 제공되는 맞춤 광고)과 같이 웹사이트를 통해서 시간이 지남에 따라 이용자의 신원을 확인하는 것을 처리하는 것이 목적이다. 이러한 경우 데이터 처리는 데이터 보호 지침에 정해진 규칙을 준수해야 한다.

- 디바이스 핑거프린팅 기술은 데스크탑 PC에서 전통적인 웹브라우저의 구성매개변수(configuration parameters)에 한정되지 않는다. 디바이스 핑거프린팅은 특별한 프로토콜에도 얽매이지도 않지만 인터넷에 광범위하게 연결된 기기들(예를 들어 소비자의 전자제품 및 응용기기들, 휴대용 기기, 스마트 TV, 게임 콘솔, 전자북 리더, 인터넷 라디오, 자동차 시스템 또는 스마트 계량기(즉 사물인터넷)등)의 디지털 지문을 채취하는데 사용될 수 있다.

- 개인의 HTTP 헤더는 전형적으로 고유값을 갖지 않기 때문에, 이용자들은 정보 요소만으로는 개인적으로 거의 식별되지 않는다. 예를 들어 브라우저에 의해서 지원되는 미디어 유형은 흔히 동일한 브라우저 버전을 이용하고 있는 다른 많은 이용자들에서 동일하다. 따라서 고립되어 처리는 경우 비고유 정보 요소는 일반적으로 데이터 보호의 위험성을 보여주지 않는다.

- 하지만 디바이스 또는 어플리케이션 인스턴스(application instance)를 위한 고유한 핑거프린트로서 충분히 고유하게 (특히 발신 IP주소와 같은 다른 식별자와 결합하는 경우) 실행할 수 있는 세트를 제공하는데 수많은 정보 요소들이 결합될 수 있다. 그러한 핑거프린트는 디바이스를 구별할 수 있는 능력을 제공하고 시간이 지남에 따라 인터넷 이용 형태를 추적하는 쿠키의 대안으로 은밀하게 이용될 수 있다. 그 결과 개인이 연관될 수 있다.

■ **(데이터 보호 위험성)** 디바이스 핑거프린팅으로 인한 데이터 보호 위험성은 고유한 정보 요소의 세트가 웹사이트 발행자에게 제공될 수 있을 뿐 아니라, 다수의 제3자에게도 제공될 수 있다는 사실에 의해서 높아지고 있다.

- 데이터 보호의 위험은 제3자의 추적에 한정되지 않는다. 클라이언트 디바이스에 있는 응용프로그램 인터페이스(API)를 통해서 획득된 데이터의 결합으로 소프트웨어 디바이스 핑거프린팅의 위험성을 보여주고 있다. 다른 소프트웨어, 플랫폼, API는 각각 디바이스에 저장되어 있는 다른 정보 요소들에 접근을 제공하려고 한다.

- HTTP 쿠키와는 달리 디바이스 핑거프린팅은 은밀하게 운영될 수 있다. 사용자들이 이 활동을 막을 간단한 방법은 없다. 리셋하거나 핑거프린트를 작동하는 데 사용되고 있는 어떤 정보 요소를 수정하는 제한된 방법들이 있다. 그 결과 디바이스 핑거프린트는 제3자에 의해서 타겟 콘텐츠의 잠재적이용자를 비밀리에 확인할 수 있고 선별할 수 있으며 또한 이용자를 차별하여 취급할 수 있다.

법적 체계

■ 핑거프린트가 사용자의 단말기에 저장되어 있는 정보의 저장이나 접근을 통해서 생성되는 경우에는 전자프라이버시지침이 적용된다. 데이터보호 작업반의 의견서에 기술되어 있는 바와 같이 지침 제5조 제3항은 다음의 기준 중 하나가 충족되는 경우에는 동의 요건이 면제되는 데이터 처리로서 허용된다.

- 기준 A : “전자적 통신망을 통해서 통신의 전송을 수행하기 위한 유일한 목적을 위한”기술적 저장이나 접근인 경우

- 기준 B : “가입자 또는 이용자의 명백한 요구에 의해서 정보사회서비스 제공자가 그 서비스를 제공하기 위해서 엄격하게 필요한”기술적 저장이나 접근인 경우

■ 웹사이트 운영자는 이용자의 신호를 나타내는 어떤 다른 신호의 정의된 의미를 존중해야 한다. 디바이스 핑거프린팅이 개인 데이터를 처리하는 경우, 이 지침의 각 관련 규정을 준수하여 행해져야 한다.

- 전자 프라이버시 지침 제5조 제3항은 사용자의 단말기에 저장되어 있는 정보를 저장하거나 접근하려는 의도를 가진 당사자는 사용자의 동의가 필요하다. 비록 그 정보가 아직 개인 데이터로서 고려되지 않는다고 하더라도 데이터보호 특별조사위원회는 온라인 행동 광고에 관하여 일반적인 고려와 특별한 고려하고 또한 제5조 제3항의 맥락에서 동의의 요건과 쿠키를 논의하였다.

■ 전자 프라이버시 지침 제정 이유 중 “보장되지 않는 사생활 침해”를 언급하고 있고 제5조는 통신의 비밀을 위한 요건을 명확히 하고 있다. 제5조 제3항은 정보의 기밀성을 이용자의 디바이스에 저장되거나 접근되는 것으로 확대한 것으로 간주될 수 있다. 따라서 제3자가 그 디바이스의 행동에 영향을 주는 것을 시도하는 처리나 그 디바이스에 관한 정보를 저장하거나 접근하게 하는 처리 또는 그 디바이스에 의해서 노출되게 하는 처리는 제5조 제3항의 범위 내에 있다.

- “저장되거나 접근되는”이란 문언을 사용한 것은 저장과 접근이 동일한 통신 내에서 발생할 필요는 없으며 동일한 제3자에 의해서 행해질 필요도 없다는 것을 의미한다. 한 당사자에 의해서 저장된 정보(이용자 또는 디바이스 제작자에 의해서 저장된 정보를 포함하여)는 다른 당사자에 의해서 이후에 접근이 되는 정보로 제5조 제3항의 범위 내에 있다.

■ 따라서 제3자는 디바이스 핑거프린팅이 이용자의 디바이스에 관한 정보의 저장이나 접근을 요구하는 경우 동의를 받아야 한다는 사실을 기억하는 것이 중요하다. 비록 몇몇의 정보 요소들이 비록 정보의 저장이나 접근을 요청하지 않았다고 하더라도 이것은 여전히 적용된다.

결론

■ 이 의견은 디바이스 핑거프린팅의 전자프라이버시 지침(2002/58/EC)의 적용가능성을 다루었다. 이전의 쿠키(Cookie)의 동의 면제에 관한 의견을 더 상세하게 보충하고 있으며 디바이스 핑거프린팅은 이용자의 단말기 정보에 접근하고 저장하고 있다는 사실을 확인하였다. 따라서 이용자의 단말장치의 정보에 접근하고 저장을 통하여 발생시키는 디바이스 핑거프린팅를 운용하고자 하는 자는 (면제가 되지 않는 한) 우선 이용자의 유효한 동의를 얻어야 한다.

참고자료

의견 전문 :
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

관련 기사 :
http://www.heise.de/newsticker/meldung/EU-Datenschuetzer-warnen-vor-Tracking-mit-digitalem-Fingerabdruck-2468675.html

3 EU의회, 항공기 승객의 개인정보 전달에 관한 협정안을 유럽사법재판소에 제소하기로 결정 (2014. 11. 25.)

개요

■ EU의회는 현재 추진 중인 EU와 캐나다 사이의 '항공기 승객의 개인정보 전달 및 처리에 관한 협정안'이 EU 조약과 일치하는지의 여부를 유럽사법재판소에서 판단해 줄 것을 요청하는 결의안을 채택하였다(2014. 11. 25.). 이 결의안[9]으로 인해 유럽사법재판소는 항공기 탑승자의 개인정보를 전달하고 처리하는 것이 EU법에 일치하는지를 판단하여야 한다.

9 European Parliament resolution on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record (PNR) data (2014/2966(RSP))

배경

■ '항공기 승객의 개인정보 전달 및 처리에 관한 협정안'이 EU조약의 기본권과 일치하는지에 대해서 명확하지 않다. 특히 이번 결의안은 지난 4월 유럽사법재판소의 통신정보보관지침의 무효판결[10]과 관련이 있다. 의회 및 법률전문가들의 견해에 따르면 통신정보보관지침의 무효판결은 통신에서의 개인 정보의 수집 및 이용에만 국한되는 것이 아니며 항공기 탑승자의 개인정보의 교환은 이 판례와는 관련이 없다는 견해를 가지고 있었다.

결의안 주요내용

■ **(협약 체결의 이유)** 캐나다 국경 감시대(Canada Border Services Agency)는 캐나다 세관법, 승객 정보 규칙, 이민 및 난민 보호법에 근거하여 캐나다에 이착륙하는 항공기 승객의 데이터(PNR date)에 전자적으로 접근을 요청할 권한을 가지고 있다.

- 이를 통해 국경 감시대가 승객 도착 전에 효과적으로 위험요소를 평가하고 안전한 여행을 보장할 수 있게 한다. EU는 캐나다의 테러 및 국경을 초월한 중대범죄에 공동으로 대처하고 국제적 차원에서 경찰 및 사법 공조의 일환으로 승객 데이터의 전달을 고려한다. 이를 위해서 캐나다가 요청한 승객 데이터를 포함한 분석 정보는 회원국의 관할 경찰과 사법기관 및 유로폴(유럽 형사경찰기구)과 유럽검찰에 위탁하여 서로 교환될 수 있다.

- 승객 데이터는 개별 승객의 여행정보에 대한 기록으로 항공사가 예약을 위해서 처리하고 점검하기 위해서 필요한 전체 정보를 포함하며 항공사의 컴퓨터로 지원되는 예약 및 처리시스템으로 수집되어 저장되어 있다. 항공사는 캐나다 국경 감시대가 특정한 승객 데이터에 접근하는 것을 보장할 의무가 있다.

- EU 데이터보호규정에 의하면 유럽 외의 목적지로 운항하는 유럽 및 다른 항공사는 적합한 보호조치를 취하지 않은 승객 데이터를 적정한 보호를 제공하지 않는 제3국으로 전달하는 것을 금지하고 있다. 테러 및 국경을 초월하는 중대범죄를 예방하기 위해 승객 데이터 이용의 필요성 측면에서 보면 EU에서 캐나다로 승객 데이터를 전달하는 법적 근거를 제공하는 해결방안이 마련되어야 하고 동시에 항공사에게 법적 안정성을 제공해야 한다. 이는 EU 전체 회원국에 적용되어야 한다.

■ **(협정의 목적)** 공공의 안전을 보장하기 위해서 어떠한 조건하에서 승객의 정보를 전달하고

10 ECJ, 8.4.2014, C-293/12, C-594/12.

이용하고 어떻게 보호할 것인가를 정한다(제1조).

■ **(주요 개념)** 협약에서 언급하는 용어는 다음과 같이 정리한다.

- '항공사'란 캐나다와 EU 사이에 승객의 운송을 위해서 항공기를 투입하는 상업적 운송기업을 말한다.

- '항공기 승객 정보'(PNR data)란 승객이 예약한 항공여행을 위해서 항공사가 그 예약의 처리와 통제를 위해서 수집되는 정보를 말한다. 이 협약에서 말하는 승객 정보는 부칙에 구체적으로 기술되어 있다.

〈부칙규정〉 승객 데이터의 구성요소

1. 승객의 예약코드(지역 코드)
2. 예약 날짜 및 티켓 발권 날짜
3. 예상 여행기간
4. 성명
5. 자주 이용하는 비행기 및 유용한 정보 (예를 들어 자유 티켓, 업그레이드 등)
6. 일행
7. 데이터 입력자의 신원을 확인할 수 있는 정보
8. 지불정보 및 정산정보 (여행과 관련된 거래내역이 없는 신용카드 또는 계좌)
9. 여행 동선
10. 여행사 및 담당자
11. 코드 공유 정보
12. 예약 분할 정보
13. 승객의 여행상태(확인 및 체크 인 상태 포함)
14. 발권 정보, 발권번호, 편도 티켓 및 자동 티켓 요금
15. 수하물 정보
16. 좌석번호
17. OSI, SSI, SSR 정보를 포함한 일반적인 정보
18. 예약 목적으로 수집된 추가 여행 정보(API)
19. (1) 에서 (18)에 기술된 승객 데이터와 관련한 변경된 히스토리 정보.

- '민감한 정보'란 인종적 민족적 기원, 정치적 견해, 종교적 또는 철학적 신념, 노동조합 회원 여부에 관한 정보 또는 개인의 건강 및 성생활에 관한 정보를 말한다.

- '테러범죄'란 정치적, 종교적 또는 사상적 목적으로 행해지거나 경제적 안전을 포함한 일반

공중의 안전에 관하여 일반 공중을 위협할 의도로 사람, 정부, 국내 또는 국제기구를 대상으로 행해지는 작위나 부작위 그리고 다음 각 행위 중의 어느 하나에 해당하는 행위를 의도적으로 한 작위 또는 부작위를 말한다. 또한 적용 가능한 테러투쟁을 위한 국제적 협약 및 프로토콜에서 범죄로 규정한 행위 및 범죄 행위를 의미한다.

(ⅰ) 사망 또는 중대한 신체상해를 야기하는 행위
(ⅱ) 개인의 생명을 위태롭게 하는 행위
(ⅲ) 일반 공중의 건강이나 안전을 중대하게 위태롭게 하는 행위
(ⅳ) (ⅰ) 부터 (ⅲ)에 언급된 손해에 이르게 하는 재물손괴를 야기하는 행위.
(ⅴ) 중대한 의미가 있는 서비스, 시설 또는 시스템의 심각한 침해 및 장애를 야기하는 행위로서 (ⅰ) 내지 (ⅲ)에 언급한 손해를 의도하지 않은 합법적 또는 불법적 이익대리, 시위고지, 스트라이크와 같은 노동거부 또는 노동포기(폐업)와 같은 것

- '테러단체'란 (ⅰ) 목적 또는 활동이 앞서 언급한 작위 부작위를 원활히 하거나 수행하는데 있는 사람, 단체 또는 조직 (ⅱ) 본질적으로 (ⅰ)에 언급한 사람, 단체 또는 조직의 위탁으로, 지휘 하에 또는 결합하여 행위 하는 사람, 단체 또는 조직

- '국경을 초월한 중대범죄'란 캐나다 법률에 의하여 최고 4년 이상의 자유형에 해당하거나 그 이상의 모든 범죄를 말하며 이 범죄가 국경을 초월한 성격을 가져야 한다.

요건

(a) 한 국가 이상에서 행해진 범죄
(b) 한 국가에서 행해졌지만, 이 범죄의 예비, 계획, 지휘(지도, 조종), 감시가 다른 나라에서 발생한 범죄
(c) 한 국가에서 조직범죄와 관련하여 행해지고 추적되는 범죄
(d) 한 국가에서 행해졌지만, 다른 국가에 심각한 영향을 미친 범죄
(e) 한 국가에서 행해지고 범죄자가 다른 나라에 체류하고 있는 경우

■ **(항공기 승객정보의 이용)** 캐나다는 관할 캐나다 관청이 이 협약을 근거로 보유한 승객 정보를 오로지 테러범죄와 국경을 초월한 중대 범죄를 예방하고, 조사하고 형사소추를 위한 목적으로만 처리하도록 하도록 확보해야 한다.

■ **(승객 데이터의 제공 보장)** EU는 캐나다 관할 관청이 이 협정을 근거로 승객의 데이터를 전달받는 것을 방해받지 않도록 배려를 해야 한다. 캐나다는 항공사가 아직 예약 목적으로

수집하지 않았거나 저장하지 아니한 승객 데이터를 항공사에게 요청해서는 안 된다. 또한 이 협약을 근거로 항공사로부터 전달받은 모든 데이터 중 언급하지 아니한 경우에는 이를 삭제해야 한다. 당사자는 항공사가 캐나다의 관할 관청에 항공사의 명의와 책임으로 대리인을 통하여 협정에 언급한 조건하에서 승객 데이터를 전달할 수 있다.

■ **(민감한 데이터의 이용)** 승객의 데이터가 민감한 정보를 포함하고 있는 경우 캐나다는 민감한 정보를 자동시스템에 의해서 식별할 수 없도록 처리하게 해야 한다. 식별할 수 없도록 해야 하는 민감한 정보를 식별하기 위한 코드와 용어의 목록을 EU 집행위원회에 제공해야 한다. 캐나다는 이 목록을 협정의 발효 후 90일 이내에 전달한다. 또한 다음의 기준에 의한 경우 외에는 더 이상 처리해서는 안 되도록 해야 한다.

- 개인의 생명과 신체에 위험이 존재하여 그 처리가 불가피한 경우에는 개별적인 사안에서 예외적으로 민감한 정보를 처리할 수 있다.

- 캐나다는 민감한 정보가 오로지 엄격한 절차법상의 규정에 따라서 관할 캐나다 관청의 장의 허가가 있어야 하고, 민감 정보는 오로지 이에 대해서 특별히 개인적으로 권한이 있는 자에 의해서 처리되어야 하며, 식별할 수 없도록 한 것을 폐기한 후에는 민간 정보는 자동 시스템에 의해서 처리되지 않는다.

- 데이터를 저장하지 않는 한, 늦어도 데이터를 전달받은 후 15일 이내에 삭제해야 한다.

- 캐나다는 가능한 한 빨리 처리 시점에 이 회원국의 관청에 알림으로써 캐나다와 이 회원국 사이에 형사소추나 정보교환의 영역에 관한 합의를 준수하여 통지해야 한다.

■ **(데이터의 보안과 무결성)** 캐나다는 승객 데이터의 처리나 분실이 부당하게 또는 권한 없이 발생한 경우에 이에 대한 접근을 방지하기 위하여 규제적, 절차적, 기술적 조치를 취해야 한다.

■ **(감독)** 이 협정과 관련하여 승객 데이터의 처리가 데이터보호의 보장을 준수하는지를 독립된 관청이나 기관은 감독하여야 한다.

■ **(투명성 보장)** 캐나다는 관할 관청이 투명성 보장을 위하여 웹사이트에 다음의 정보를 제공하여야 한다.

요건

(a) 승객 데이터의 수집을 허용하는 법률 규정의 표시
(b) 승객 데이터가 수집근거
(c) 승객 데이터 이용 상태
(d) 데이터 전달방법
(e) 접근, 정정, 분쟁의 기록 및 법적구제에 관한 정보.
(f) 문의를 위한 접촉 정보.

– 투명성을 촉진하기 위해서 당사자들은 항공여행사와 같은 관심 있는 당사자들과 함께, 우선 예약 시점에 승객에게 다음의 정보를 제공한다.

정보

(a) 승객 데이터 수집의 이유
(b) 승객 데이터의 이용
(c) 승객 데이터의 접근을 요구하는 절차
(d) 승객 데이터의 정정을 요구하는 절차

■ **(개인을 위한 접근)** 캐나다는 각 개인이 자신의 승객 정보에 접근할 수 있도록 보장해야 한다. 또한 범죄를 예방, 수사 또는 형사소추를 위한 공공의 안전과 국가의 안전을 위한 관련 당사자의 개인의 정당한 이익을 고려하여 합리적인 법적 요건과 제한에 따라서 정보를 공개할 수 있다.

요구사항

(a) 개인이 서면으로 승객 데이터를 청구한 경우에는 승객 데이터의 사본을 제공해야 한다.
(b) 요청에 서면으로 응답해야 한다.
(c) 개인이 확인을 요청한 경우에는 개인의 승객 데이터가 제공되었다는 것을 확인하는 정보를 개인에게 제공한다.
(d) 개인의 승객 데이터에의 접근을 거절하는 경우 그 법적 사실을 밝혀야 한다.
(e) 승객 데이터가 존재하지 않는 경우에는 그 개인에게 통지해야 한다.
(f) 개인이 이의를 제기할 수 있다는 것과 이의제기의 절차를 통지해야 한다.

■ **(개인의 정정과 고지)** 캐나다는 각 개인이 자신의 승객데이터를 수정할 수 있도록 보장해야 한다. 관할 관청의 정정을 위한 모든 서면 요청을 고려하고, 합리적인 기간 내에 다음을 하도록 확보해야 한다.

요구사항

(a) 승객 데이터를 정정하고 정정이 되었다는 사실을 개인에 통지하여야 한다.

(b) 정정의 일부 또는 전부를 거절하여야 한다. (ⅰ) 요청된 어떠한 정정이 거절되었는지를 추론할 수 있는 승객 데이터를 메모해서 첨부한다. (ⅱ) 개인에게 통지한다. ⅰ. 정정요청이 거절되었고, 그 거절의 법적 또는 사실적 이유를 설명해야 한다. ⅱ. (ⅰ)에 의한 기록은 승객 데이터에 첨부한다.

(c) 개인이 이의를 제기할 수 있다는 사실과 이의제기 절차를 알려야 한다.

■ **(행정적 사법적 권리구제)** 캐나다는 독립 공공 기관이 또는 독립적인 방식으로 기능을 수행하여 자신의 승객 데이터에 대한 접근, 정정, 기록에 관하여 개인에 의하여 제기된 이의제기를 접수하고, 조사하고 응답할 것을 확보해야 한다. 자신의 권리가 승객 데이터와 관련한 결정이나 처분에 의해서 침해되었다는 견해를 가지고 있는 개인은 사법적인 관점에서 캐나다의 법률에 따라서 효과적인 사법적 구제를 추구할 수 있도록 보장해야 한다.

■ **(자동화 처리의 근거로 한 결정)** 캐나다는 오로지 승객 데이터의 자동화 처리라는 이유로 승객에게 중대한 영향을 미치는 결정을 해서는 안 된다.

■ **(승객 데이터의 보관)** 승객 데이터를 입수한 날로부터 최고 5년 동안 저장하여 보관한다. 접근이 허락된 자들을 한정하여 이 데이터에 대한 접근을 제한여야 한다. 승객 데이터의 입수 후 30일간 전체 승객 데이터의 성명을 인식할 수 없도록 익명화 조치를 취한다. 승객 데이터의 입수 후 2년간 정보를 식별할 수 없도록 익명화 조치를 취한다.

■ **(승객 정보의 처리에 대한 로그인과 기록)** 승객 데이터의 모든 처리를 로그해야 한다. 이 로그기록이나 기록물을 다음 각 사유를 위해서만 사용하여야 한다.

요건

(a) 자체 모니터 또는 데이터 처리의 정당성을 점검

(b) 적절한 데이터 무결성을 확보

(c) 데이터 처리의 보안성을 확보

(d) 공공 행정기관의 감독과 번명 의무를 확보

■ **(캐나다 내에서 공개)** 다음 각 사유에 해당하는 경우 캐나다 내의 다른 정부 기관에 승객 데이터를 공개하여야 한다.

요건

(a) 승객 데이터가 직접 관련되는 기능을 가진 정부 기관에 전달되는 경우

(b) 승객 데이터가 사안별로 공개되는 경우

(c) 특별한 사정이 있는 경우에는 그 전달은 언급한 목적을 위해서 필요한 경우

(d) 승객 데이터의 최소한의 분량만이 공개

(e) 승객데이터를 전달받은 정부 기관은 이 협정에 정해진 안전과 동일한 보호를 요청하는 경우

(f) 승객 데이터를 제공받은 정부 기관은 이를 다른 기관에게 전달해서는 안 된다. 그 전달이 캐나다의 관할 관청에 의해서 허가되지 않는 한 이 항에 규정된 조건을 준수하여야 한다.

■ **(캐나다 외부의 전달)** 다음의 조건이 충족되는 경우에 한해서 EU의 회원국이 아닌 다른 국가의 정부 기관에 승객 데이터를 공개할 수 있다.

요건

(a) 승객 데이터는 그 직무의 적용범위와 직접 관련이 있는 국가기관에게 전달되는 경우

(b) 승객 데이터가 사안별로 전달되는 경우

(c) 승객 데이터가 제3조에 규정된 목적을 위해서 필요한 경우

(d) 캐나다의 관할 관청이 다음을 보장하는 경우

(i) 승객 데이터를 전달받는 외국 관청이 이 협정에서 정한 기준과 동일하게 승객 데이터를 보호하는 기준을 적용하거나, 이 협정에 따라서 그리고 이러한 기준들을 정한 협정을 적정히 고려하는 것

(ii) 외국 관청이 EU와 합의한 승객 데이터를 보호하기 위한 기준을 적용하는 것

■ **(전달절차)** 항공사는 캐나다의 관할 관청에 승객데이터를 오로지 푸시(push) 방법으로만 (요청이 아니라 제공의 방식) 전달하여야 하며 다음의 절차적 요건들도 준수하면서 전달하도록 당사자들은 확보하여야 한다.

요건

(a) 전자적 방식의 승객 데이터 전달은 기술적인 장애가 있는 경우에 적정한 데이터의 보안 수준이 보장되는 경우 혹은 그 밖의 다른 적합한 방식으로 전달

(b) 서로가 인식할 수 있는 전달포맷을 사용한 승객 데이터의 전달

(c) 캐나다의 관할 관청에 의해서 요청한 공통의 프로토콜을 사용하여 안전한 방식으로 승객 데이터를 전달

■ **(데이터 전달의 빈도수)** 승객 데이터가 예정된 대로 전달될 것. 이 경우 첫 번째 전달은 항공기의 이륙 72시간 이전에 가능해야 한다. 승객 데이터는 항공기 당 최대 다섯 번만 전달되어야 한다. 전달 시점을 알리도록 보장해야 하고 특정한 위험에 대응하기 위하여 이 데이터에 추가적인 접근이 필요하다는 정황이 있는 경우에는 캐나다의 관할 기관은 항공사에게 예정된 전달 이전, 중간, 또는 이후에도 요청할 수 있다. 캐나다는 제20조에 의한 전달절차의 투입 및 비례성원칙을 준수하여 그리고 신중을 다하여 재량의 여지를 이용한다.

평가

■ EU 의회는 모든 항공기 승객의 개인정보를 이유 없이 저장하는 것은 유럽 데이터보호법과 일치하지 않는다고 하였다. 유럽사법재판소는 캐나다와의 협정에서 제기되는 이러한 의문에 대해서 해결 방안을 제시해야 할 것이라고 한다. 사법재판소의 판단은 이미 체결된 미국 및 호주 사이의 협정에도 적용될 것이라고 한다.

참고자료

http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2014-0265&language=DE

http://www.heise.de/newsticker/meldung/Europaeischer-Gerichtshof-soll-Transfer-von-Fluggastdaten-pruefen-2463138.html

참고 웹사이트

국내 웹사이트

[1] 국회 (http://www.assembly.go.kr)

국외 웹사이트

[1] http://www.shugiin.go.jp/internet/itdb_gian.nsf/html/gian/honbun/houan/g18601035.htm「わが国のサイバーセキュリティ体制の強化に向けての提言」

[2] https://www.hirataku.com/wp-content/themes/hirataku/pdf/6b98e5eeff44c9f7df98a4a7fd85f70e.pdf#search=’%E3%82%8F%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%E4%BD%93%E5%88%B6%E5%BC%B7%E5%8C%96%E3%81%AB%E5%90%91%E3%81%91%E3%81%A6%E6%8F%90%E8%A8%80’

[3] http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=1

[4] http://itpro.nikkeibp.co.jp/atcl/esi/14/527562/103000002/?P=2

[5] http://headlines.yahoo.co.jp/hl?a=20141119-00000060-impress-sci

[6] http://dip21.bundestag.de/dip21/btd/18/030/1803047.pdf

[7] http://www.golem.de/news/gruene-und-linke-gesetzentwurf-gegen-stoererhaftung-offener-wlans-vorgelegt-1411-110417.html

[8] http://www.heise.de/newsticker/meldung/Bayerns-Finanzminister-Soeder-verspricht-freies-WLAN-im-laendlichen-Raum-2466894.html.

[9] http://www.lexology.com/library/detail.aspx?g=d4afd0a7-bb33-49f7-86c8-f0f5e0280204&utm_source=Lexology+Daily+Newsfeed&utm_medium=H%E2%80%A6

[10] http://www.resmigazete.gov.tr/eskiler/2014/11/20141105-1.htm

[11] http://www.morogluarseven.com/news/save-date-may-1-2015-e-commerce-turkey

[12] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[13] http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20141126_wp29_press_release_ecj_de-listing.pdf

[14] http://www.heise.de/newsticker/meldung/EU-Datenschuetzer-Google-muss-Links-weltweit-loeschen-2466684.html

[15] http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en

[16] http://www.jurablogs.com/go/eu-datenschuetzer-fordern-weltweite-loeschung-von-links

[17] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

[18] http://www.heise.de/newsticker/meldung/EU-Datenschuetzer-warnen-vor-Tracking-mit-digitalem-Fingerabdruck-2468675.html

[19] http://www.usatoday.com/story/tech/2014/10/01/fda-medical-devices-cybersecurity/16543731/

[20] https://www.lda.bayern.de/lda/datenschutzaufsicht/p_archiv/2014/pm013.html

[21] http://www.gesetze-bayern.de/jportal/portal/page/bsbayprod.psml?doc.id=JURE140015287&st=ent&showdoccase=1&paramfromHL=true

[22] http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B8-2014-0265&language=DE

[23] http://www.heise.de/newsticker/meldung/Europaeischer-Gerichtshof-soll-Transfer-von-Fluggastdaten-pruefen-2463138.html

[24] http://www.pcpd.org.hk/english/infocentre/press_20141006.htm

[25] http://www.pcpd.org.hk/english/publications/files/GN_banking_e.pdf

[26] http://www.lexology.com/library/detail.aspx?g=c1770f49-cac4-4715-9d8c-837866b5e89a

[27] http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2880

[28] http://www.out-law.com/en/articles/2014/october/hong-kong-watchdog-issues-new-data-protection-guidelines-for-banks-amidst-rising-number-of-complaints/

[29] https://privacyassociation.org/news/a/belgiums-new-government-sets-privacy-high-on-the-agenda-appointing-minister-of-privacy/