Vol. 142 (July 2019)

인터넷 법제동향

Laws and Policy Trends of the Internet

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

국내 입법 동향

해외 입법 동향

기고

<국회 제출 법률안>		
법령명	**대표발의 의원 (발의날짜)**	**주요내용**
• 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	박명재의원 (2019. 7. 24.)	- 정보통신서비스 제공자등이 법률을 위반한 경우 과징금 산정 기준인 매출액 정보의 확인이 어려워 관할 세무관서의 장에게 과세정보 제공을 요청할 수 있도록 함
	서영교의원 (2019. 7. 25.)	- 불법정보에 화폐·지폐권 또는 은행권을 위조 또는 변조할 수 있는 방법 등의 정보와 「마약류 관리에 관한 법률」에 따른 금지행위에 관한 정보를 명시함
	김성수의원 (2019. 7. 30.)	- 방송통신위원회의 소속기관 장에게 권한의 일부를 위임할 수 있는 근거를 명시
• 「개인정보 보호법」 일부개정법률안	이찬열의원 (2019. 7. 11.)	- 개인정보 분쟁조정위원회의 민간위원에게 「형법」상 뇌물죄를 적용하는 경우에는 공무원으로 의제할 수 있도록 함
	신창현의원 (2019. 7. 25.)	- 목욕탕, 화장실, 숙박업소 등 각종 시설 관리자가 시설 내부의 몰래카메라 설치여부 점검 및 신고를 의무화하고 과태료 규정을 신설
• 「국가정보화 기본법」 일부개정법률안	정종섭의원 (2019. 7. 8.)	- 국가기관 등이 정보통신망을 통하여 전자출판물을 서비스할 때 장애인·고령자 등의 접근성 보장을 위해 표준제정, 기술개발, 품질인증을 받을 수 있도록 함
• 「소프트웨어산업 진흥법」 일부개정법률안	박선숙의원 (2019. 7. 26.)	- 기본계획 수립주기를 3년으로 법률에 명시하고 시행계획의 추진실적에 대한 평가를 시행계획에 반영하도록 함
• 「위치정보의 보호 및 이용 등에 관한 법률」 일부개정법률안	박명재의원 (2019. 7. 24.)	- 과징금을 부과하기 위하여 필요한 경우에 관할 세무서의 장에게 과세정보 제공을 요청할 수 있도록 함
• 「전기통신사업법」 일부개정법률안	심기준의원 (2019. 7. 8.)	- 국세청장 및 지방국세청장이 정보통신망을 이용하여 통신판매 또는 통신판매중개를 하는자에게 조세 부과·징수하기 위한 통신자료제공을 요청할 수 있도록 함
• 「정보통신산업 진흥법」 일부개정법률안	박선숙 (2019. 7. 26.)	- 기본계획 수립주기를 3년으로 법률에 명시하고 시행계획의 추진실적에 대한 평가를 시행계획에 반영하도록 함
• 「전자상거래 등에서의 소비자 보호에 관한 법률」 일부개정법률안	심기준의원 (2019. 7. 8.)	- 전자상거래 등에서의 소비자보호에 관한 법률에 주문제작 및 해당 상품의 환불에 대한 조항을 추가함

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(박명재의원 대표발의, 2019. 7. 24. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 정보통신서비스 제공자등이 법률을 위반한 경우 매출액의 100분의 3 이하에 해당하는 금액을 방송통신위원회가 과징금으로 부과·징수할 수 있도록 규정하고 있으나, 과징금 산정의 기준이 되는 매출액 정보의 확인이 어려워 과징금의 부과와 징수가 원활하게 이루어지지 못하고 있는 상황임

o 매출액 산정을 위해서는 과세 정보의 확인이 필수적이나 동 정보를 보유·관리하고 있는 세무관서는 「국세기본법」 제81조의13(비밀유지) 조항을 근거로 개별 법률에 구체적인 요청 근거가 명시된 경우에만 정보 제공이 가능하다는 입장임

▶ 주요내용

o 방송통신위원회가 과징금을 부과하기 위하여 필요한 경우에는 관할 세무관서의 장에게 과세정보 제공을 요청할 수 있도록 함으로써 금전적 행정제재가 적정하고 효율적으로 운영되도록 하려는 것임(안 제64조의4 신설)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(서영교의원 대표발의, 2019. 7. 25. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현현행법은 음란정보, 다른 사람의 명예를 훼손하는 정보 등을 불법정보로 규정하고, 불법정보가 정보통신망에 유통될 경우 방송통신위원회가 정보통신서비스 제공자에게 해당 불법정보의 처리를 거부·정지 또는 제한할 것을 명하도록 규정하고 있음

o 「형법」에 따라 화폐·지폐권 또는 은행권의 위조·변조가 금지되고 있으며, 「마약류 관리에 관한 법률」에 따라 허가받지 않은 자의 마약류 제조 등이 금지되고 있음에도 위조통화의 위조·변조방법 또는 마약류의 제조방법 등에 관한 정보가 정보통신망에 유통되고 있음

▶ 주요내용

o 현행법의 불법정보에 화폐·지폐권 또는 은행권을 위조 또는 변조할 수 있는 방법 등의 정보와 「마약류 관리에 관한 법률」에 따른 금지행위에 관한 정보를 명시함으로써 정보통신망의 건전한 이용에 이바지하려는 것임(안 제44조의7제1항제6호의4 및 제6호의5 신설 등)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안
(김성수의원 대표발의, 2019. 7. 30. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 지난해 9월, 방송통신위원회의 소속기관으로 방송통신사무소가 설립됨에 따라, 방송통신위원회의 권한 중 일부가 방송통신위원회의 소속기관인 방송통신사무소에 위임되었음

o 현행법은 과학기술정보통신부장관 또는 방송통신위원회의 권한 중 일부를 과학기술정보통신부 소속 기관의 장 또는 지방우정청장에게 위임·위탁할 수 있도록 법에 규정하고 있음

o 방송통신위원회가 방송통신위원회 소속기관에 위임할 수 있는 내용은 규정하고 있지 않아, 방송통신위원회가 기관 권한 중 일부를 이미 방송통신사무소에 위임하여 처리하고 있음에도 이에 대한 명시적인 근거가 마련되어 있지 않은 상황임

▶ 주요내용

o 방송통신위원회의 권한의 일부를 방송통신위원회의 소속기관의 장에게 위임할 수 있는 근거를 명시적으로 마련하려는 것임(안 제65조제1항)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「개인정보 보호법」 일부개정법률안
(이찬열의원 대표발의, 2019. 7. 11. 제안)

▶ 소관 상임위원회 : 행정안전위원회

▶ 제안이유

o 최근 행정의 전문성·효율성 확보를 위하여 공무원이 아닌 사람도 공공업무에 참여하는 경우가 많은데, 대부분의 경우 공공업무를 수행하는 민간인의 부패행위를 방지하기 위하여 공공업무를 수행하는 민간인이 그 업무와 관련하여 범죄를 저지른 경우 이들을 공무원과 동일하게 처벌할 수 있도록 공무원 의제 규정을 두고 있음

o 현행법은 개인정보에 관한 분쟁을 조정하기 위하여 개인정보 분쟁조정위원회를 두고 있는데, 분쟁조정의 전문성을 확보하기 위하여 공무원 뿐만 아니라 민간인도 개인정보 분쟁조정위원회의 위원으로 선임하도록 하고 있음

o 그러나 현행법은 개인정보 분쟁조정위원회의 민간위원에 대한 공무원 의제 조항이 없어 민간위원이 부정행위를 한 경우 그 처벌이 공무원인 위원보다 가벼워 공정성·책임성 확보가 곤란함

▶ 주요내용

o 개인정보 분쟁조정위원회의 민간위원에게 「형법」상 뇌물죄를 적용하는 경우에는 공무원으로 의제할 수 있도록 하여, 부패 사각지대를 개선하고 공정하고 투명한 업무 수행을 가능하게 하려는 것임(안 제69조제1호 신설)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「개인정보 보호법」 일부개정법률안
(신창현의원 대표발의, 2019. 7. 25. 제안)

▶ 소관 상임위원회 : 행정안전위원회

▶ 제안이유

o 최근 공중화장실, 탈의실, 목욕실 등 장소를 불문하고 이른바 '몰카 범죄'가 잇따르고 있어 국민들의 불안감은 더욱 커지고 있음. 실제로 서울시가 시민 1,500명을 대상으로 실시한 설문조사 결과, 응답자의 69%가 불법 촬영에 불안감을 느끼고 있었고, 불안감이 높은 장소로 숙박업소가 약 43%로 가장 많았으며 공중화장실이 36%, 수영장이나 목욕탕이 9%를 차지했음

o 경찰청 통계에 따르면 2007년 564건에 불과했던 몰래카메라 범죄는 2018년 5,925건으로 10배 이상 급증하였으며 '카메라 등 이용 촬영죄 처벌의 문제점과 개선방안' 보고서에 따르면 1,866건의 불법촬영 관련 소송 중 5회 이상 불법촬영 범죄를 저지른 비율이 31.2%나 되는 등 상습범의 비율도 높아 더욱 문제가 되고 있음

▶ 주요내용

o 목욕탕, 화장실, 숙박업소를 비롯한 각종 시설 관리자가 해당 시설 내부에 몰래카메라 설치여부를 수시로 점검하고 몰래카메라 발견 시 지체 없이 관할 경찰관서에 신고할 것을 의무화함(안 제25조제3항 신설)

o 시설 관리자가 몰래카메라를 관할 경찰관서에 신고하지 아니했거나 불법 촬영으로 인한 피해가 발생한 경우 5천만원 이하의 과태료를 부과하도록 하였으며, 몰래카메라를 설치·운영한 자에 대한 처벌을 5천만원 이하의 과태료에서 3년 이하의 징역 또는 3천만원 이하의 벌금으로 강화하여 몰래카메라 범죄를 예방하고자 함(안 제75조제1항제4호 및 제72조제1호 신설)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「국가정보화 기본법」 일부개정법률안
(정종섭의원 대표발의, 2019. 7. 8. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 최근 국가기관, 지방자치단체, 공공기관(이하 "국가기관 등"이라 함)에서 정보의 제공의 목적으로 다양한 전자출판물을 제작 서비스함에 따라, 전자책 이용이 익숙하지 않은 장애인·고령자의 접근성 문제가 제기되고 있음

o 현행법은 국가기관 등이 정보통신망을 통하여 정보나 서비스를 제공할 때 웹사이트 및 이동통신단말장치에 설치되는 응용소프트웨어에 대한 장애인·고령자 등의 접근성을 보장하도록 하고 있으나, 전자출판물에 대한 구체적인 접근성 보장 및 인증제도에 대해서는 규정되어 있지 않음

▶ 주요내용

o 국가기관 등이 정보통신망을 통하여 전자출판물을 서비스할 때 전자출판물에 대한 장애인·고령자 등의 접근성을 보장하기 위하여 표준제정, 기술개발, 품질인증을 받을 수 있도록 하여 실질적 정보접근권을 보장하도록 하려는 것임(안 제32조, 제32조의2, 제32조의4, 제32조의5)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「소프트웨어산업 진흥법」 일부개정법률안
(박선숙의원 대표발의, 2019. 7. 26. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 소프트웨어산업의 진흥을 위하여 중장기적인 기본계획(이하 "기본계획"이라 함)과 기본계획에 따른 세부 시행계획(이하 "시행계획"이라 함)을 수립하도록 규정하고 있음

o 그런데 기본계획의 수립 주기가 법률에 명시되어 있지 않고, 기본계획 수립 시 관계 전문가 등의 의견을 청취하고, 전문성 있는 위원회의 심의를 거치는 절차가 마련되어 있지 않음

o 기본계획과 시행계획의 추진실적을 국회에 보고하여 심도 있는 논의를 하는 것이 필요함에도 불구하고 현행법에는 이에 관한 규정이 없으며, 시행계획의 추진실적에 대한 평가 결과를 다음 계획에 반영하는 환류체계가 미흡하다는 지적이 제기되고 있음

▶ 주요내용

o 기본계획의 수립 주기를 3년으로 명시하고, 기본계획 수립 시 관계 전문가 등의 의견 청취와 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」에 따른 정보통신 전략위원회의 심의를 의무화하는 한편, 기본계획 및 시행계획의 추진실적에 대한 평가 결과를 국회 소관 상임위원회에 보고하고, 시행계획의 추진실적에 대한 평가 결과를 기본계획 및 다음 연도의 시행계획에 반영하도록 하려는 것임(안 제4조)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「위치정보의 보호 및 이용 등에 관한 법률」 일부개정법률안
(박명재의원 대표발의, 2019. 7. 24. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 위치정보사업자 및 위치기반서비스사업자가 법률을 위반하여 사업정지를 명하려는 경우 방송통신위원회가 이에 갈음하여 매출액의 100분의 3 이하의 과징금을 부과·징수할 수 있도록 하고 있으나, 과징금 산정의 기준이 되는 매출액 정보의 확인이 어려워 과징금의 부과와 징수가 원활하게 이루어지지 못하고 있는 상황임

o 한편, 매출액 산정을 위해서는 과세 정보의 확인이 필수적이나 동 정보를 보유·관리하고 있는 세무관서는 「국세기본법」 제81조의13(비밀유지) 조항을 근거로 개별 법률에 구체적인 요청 근거가 명시된 경우에만 정보 제공이 가능하다는 입장임

▶ 주요내용

o 방송통신위원회가 과징금을 부과하기 위하여 필요한 경우에는 관할 세무관서의 장에게 과세정보 제공을 요청할 수 있도록 함으로써 금전적 행정제재가 적정하고 효율적으로 운영되도록 하려는 것임(안 제37조의2 신설)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「전기통신사업법」 일부개정법률안
(심기준의원 대표발의, 2019. 7. 8. 제안)

▶ **소관 상임위원회 : 과학기술정보방송통신위원회**

▶ **제안이유**

o 최근 사회관계망서비스(SNS)를 이용하여 통신판매 또는 통신판매 중개를 하는 경우가 증가하고 있음

o 현행법은 국세청장 및 지방국세청장이 일부 범칙사건의 조사를 위해 필요한 경우에만 전기통신사업자에게 통신자료제공을 요청할 수 있도록 하고 있으나, 사회관계망서비스를 이용하여 통신판매를 하는 경우 판매자의 인적사항에 관계된 정보를 파악하기 어려워 세금의 부과 및 징수가 어려운 상황임

▶ **주요내용**

o 국세청장 및 지방국세청장이 정보통신망을 이용하여 통신판매 또는 통신판매중개를 하는 자에게 조세를 부과·징수하기 위한 정보수집에 필요한 경우에는 통신자료제공을 요청할 수 있도록 하려는 것임(안 제83조제4항 등)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「정보통신산업 진흥법」 일부개정법률안
(박선숙의원 대표발의, 2019. 7. 26. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 정보통신산업의 진흥에 관한 중·장기 정책목표 및 방향을 설정하기 위하여 정보통신산업 진흥계획(이하 "진흥계획"이라 함)과 연차별 계획을 수립하도록 규정하고 있음

o 그런데 진흥계획의 수립 주기가 법률에 명시되어 있지 않고, 진흥계획 수립 시 관계 전문가 등의 의견을 청취하고, 전문성 있는 위원회의 심의를 거치는 절차가 마련되어 있지 않음

o 연차별 계획의 추진실적을 평가하여 그 결과를 다음 계획에 반영하는 환류체계가 미흡하다는 지적이 제기되고 있음

▶ 주요내용

o 진흥계획의 수립 주기를 3년으로 명시하고, 진흥계획 수립 시 관계 전문가 등의 의견 청취와 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」에 따른 정보통신 전략위원회의 심의를 의무화하는 한편, 연차별 계획의 추진실적에 대한 평가 결과를 진흥계획 및 다음 연도의 연차별 계획에 반영하도록 하려는 것임(안 제5조)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「전자상거래 등에서의 소비자보호에 관한 법률」 일부개정법률안

(심기준의원 대표발의, 2019. 7. 8. 제안)

▶ 소관 상임위원회 : 정무위원회

▶ 제안이유

o 최근 전자상거래에서의 환불 거부에 의한 소비자 피해사례가 급증하고 있는데 특히 주문제작 상품이라는 이유를 들어 판매자가 환불을 거부하는 사례가 다수 집계됨

o 한국소비자원에 따르면 최근 3년간('16~'18) 온라인 주문제작 상품에 대한 피해구제 신청이 늘고 있으며, 가장 많은 피해구제 신청 이유가 환불 거부(37.8%)로 나타남

o 그러나 현행법상 주문제작 상품에 대한 근거조항이 없기 때문에, 온라인마켓 판매자가 주문제작에 대한 해석을 자의적으로 하여 환불 거부 등으로 소비자의 권리를 침해할 우려가 있음

▶ 주요내용

o 전자상거래 등에서의 소비자보호에 관한 법률에 주문제작 및 해당 상품의 환불에 대한 조항을 추가하여 안전한 온라인마켓 생태를 구축하고자 함(안 제17조제2항)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

미국 상원, 중소기업 사이버보안 지원 법안 발의 (2019. 6. 27.)

미국 상원은 중소기업개발센터(SBDC)[1]와 국토안보부(DHS)[2]가 협력하여 중소기업에 사이버보안 관련 정보와 도구, 교육 등을 지원하도록 하는 《중소기업 사이버보안 지원 법안》[3]을 발의 (2019. 6. 27.)

▶ 개요 및 경과

o 미국 상원은 최근 중소기업에 대한 사이버보안 위협이 증가함에 따라 중소기업청(SBA)의 중소기업개발센터(SBDC)를 통해 각종 정보자원과 컨설팅, 보조금 등을 지원하도록 하는 《중소기업 사이버보안 지원 법안》을 발의

- 중소기업의 사이버 공격에 대한 대응 능력을 강화하기 위해 미국 전역에 설치되어 있는 SBDC를 활용하여 실질적인 요구사항에 대한 지원을 실시

- SDBC는 정부 보조금을 사용하여 중소기업에 사이버보안 관련 정보 및 도구, 교육을 제공할 수 있으며, 국토안보부(DHS)는 온라인 사이버보안 콘텐츠 개발에 협력

o 지난 2018년에 제정된 《NIST 소기업 사이버보안법》[4]은 국립표준기술연구소(NIST)[5]의 주도로 소기업의 사이버보안 인식 제고를 위해 보안 장비 구입 예산 등을 지원하는 것으로 이번에 발의된 법안과 지원 담당 기관, 목적 등에 차이가 있음

▶ 주요 내용

o **(SBDC의 역할 및 지원 확대)** 중소기업 개발 지원 기능을 강화하기 위해 SDBC의 역할에 사이버보안에 관한 관리 및 교육・기술 지원 업무를 추가

- 동 법안에 따라 미국 연방 법전 중 SBDC 프로그램 승인[6]과 관련된 규정이 개정됨

---

1) 중소기업 개발센터(Small Business Development Centers, SBDC): 미국 중소기업청(Small Business Administration, SBA) 내의 조직으로 미국 전역에 63개소가 운영 중에 있으며, 소기업을 대상으로 경영 및 기술 지원, 교육 컨설팅 등을 제공하고 있음.

2) 국토안보부(United States Department of Homeland Security, DHS): 미국의 국가 안보 및 치안 유지에 필요한 기구를 통합하여 국가 안전 보장 업무에 신속히 대응하기 위해 2002년에 설립된 연방 중앙 행정기관임.

3) Small Business Cybersecurity Assistance Act of 2019 (S.2034)

4) NIST Small Business Cybersecurity Act(S.770)

5) National Institute of Standards and Technology. 미국 내 산업 경쟁력을 증진시키는 미국 상무부 산하 기관

6) 15 U.S. Code §648. Small business development center program authorization: 중소기업개발센터의 설립 및 중소기업 활동 지원을 위한 보조금과 관련된 규정으로 동 법안에 따라 사이버보안 관련 내용이 추가됨.

o **(정보유통 체계 및 교육 서비스 운영)** 중소기업청(SBA)은 DHS와 협력하여 중소기업이 사이버보안과 관련된 정보를 쉽게 취득하고 서로 공유할 수 있는 플랫폼을 구축·운영 해야 함

- 중소기업의 사이버보안 관련 요구사항과 관심을 가지는 주제에 초점을 맞추어 정보 서비스를 개발 및 온라인으로 제공

- 본 플랫폼을 통해 SBDC 및 중소기업 업무 관련 연방 산하 기관에 근무하는 직원에게 사이버보안과 관련된 정기적인 교육이 제공[7]되어야 하며, 해당 자료는 중소기업과 관련된 상담 및 컨설팅 등에 활용해야 함

o **(중소기업에 지원하는 사항)** 전국 각 지역의 중소기업 및 예비 창업자는 해당 법안을 통해 다른 정부 기관에서 생산된 사이버보안 정보자원을 쉽게 취득하고, SBDC의 상담 및 컨설팅을 통해 사이버공격으로부터 자산을 보호하기 위한 적절한 조치를 지원 받을 수 있음

- SBDC는 중소기업의 사이버보안 대응 능력 강화를 위해 정부 보조금 지원이 가능

- 중소기업을 위한 사이버보안 정책·절차·대응 전략, 사이버보안 관련 온라인 Tool 및 소프트웨어 교육 등을 제공

o **(기존 유사법 비교)** 2018년에 제정된 《NIST 소기업 사이버보안법》과 본 법안의 차이점은 다음과 같음

< 본 법안과 기존 유사 법 비교 >

구분	본 법안 (중소기업 사이버보안 지원 법안, 2019년)	기존 유사법 (NIST 소기업 사이버보안법, 2018년)
목적	• 중소기업 및 예비 창업자의 사이버보안 대응 역량 강화 • 사이버공격 사전 예방·사후 관리 고려	• 중소기업의 사이버보안 인식 제고 • 보안 장비 예산 확보등이 어려운 소기업에 최소한의 자원을 지원
지원 담당기관	• 중소기업개발센터(SBDC) - 중소기업청(SBA) 내의 조직	• 국립표준기술연구소(NIST) - 상무부 산하 기관
협력기관	• 국토안보부(DHS) - 정보 제공, 서비스 공동 운영 등 협력 역할을 명시	• 관련 연방기관의 장 - 제공 자원 내역 선정 시에 협의
지원 내용	• 사이버보안 정보 및 교육 서비스 • SW, 전략, 정부 보조금 등 지원 • 자산 보호 조치 컨설팅 지원	• 사이버보안 가이드, 표준, 방법론 등 • NIST 기금으로 보안 장비 확보 지원

7) DHS는 SBDC의 직원이 사이버보안 전문 상담을 실시할 수 있도록 교육훈련 프로그램을 제공함.

▶ 시사점

o 금년 3월에 미국 중소기업청과 국토안보부는 중소기업들이 사이버보안 대책을 구현하는데 직면한 문제들을 정리한 사이버 전략보고서[8]를 공동으로 발간한 바 있으며, 해당 보고서의 주요 전략을 구현하기 위해 본 법안이 제안된 것임

o 향후 본 법안이 통과되면 현재 미국 전역에 설치·운영 중인 중소기업개발센터(SBDC)를 통해 중소기업 및 예비창업자에 대한 사이버보안 관련 지원이 활성화 될 것으로 기대

※ **Reference**

https://www.congress.gov/bill/116th-congress/senate-bill/2034/all-info
https://www.congress.gov/116/bills/s2034/BILLS-116s2034is.pdf

8) SBA and DHS, March 2019, Small Business Development Center Cyber Strategy.

해외 입법 동향 EU

유럽 사법기구(Eurojust), 사이버범죄 퇴치를 위한 공통 과제 발표 (2019. 7. 5.)

유럽 사법기구(Eurojust)[1]는 국경을 초월하여 발생하는 사이버범죄에 관계기관의 공동 대응 강화를 요구하는 《사이버범죄 퇴치를 위한 공통 과제》[2]를 발표 (2019. 7. 5.)

▶ 개요 및 경과

o 유럽 사법기구(Eurojust)는 사회의 모든 분야에서 디지털화가 진행되면서, 국경에 제한이 없는 사이버범죄에 적극적으로 대응하기 위해 해결해야 할 주요 분야에 대한 EU 공동의 조치를 요구하는 《사이버범죄 퇴치를 위한 공통 과제》를 발표

- Eurojust와 Europol[3]의 유럽 사이버범죄 센터에서 그 동안 운영 및 경험한 내용을 기초로 전문가 검토를 통해 사이버범죄 퇴치를 위한 주요 과제를 선별하여 제시함

- EU 관계기관 간 공동 대응 방안으로 대규모 사이버보안 사건 및 암호해독·암호화와 관련된 문제는 유럽네트워크정보보호원(ENISA)[4]과 협력

o Eurojust는 사이버범죄와 관련된 조사·정보교환과 관련된 문제를 해결하고 수사 및 기소의 효율성을 높이기 위해 2016년부터 관계기관의 실무자 간 협력체계인 유럽 사이버범죄 네트워크[5]를 운영 중에 있음

▶ 주요 내용

o **(목적)** 사이버범죄를 퇴치하는데 필요한 공통적인 과제를 법 집행과 사법적인 관점에서 도출하고 EU 관계기관의 공동대응을 요구

- 사이버범죄는 다른 범죄의 영역에도 영향을 미치며, 국경에 제한이 없이 나타나므로 국제적인 공동의 조치를 필요로 함

1) 유럽 사법기구는 EU의 사법 협력을 담당하는 기관으로 국경을 넘는 중대 범죄에 대한 대응 강화를 위해 1999년 창설된 기관임. 기관 내의 구성원은 각 회원국의 검찰, 판사, 경찰관 등이며, 2009년 Eurojust 강화에 관한 이사회 결정으로 이해관계자 간의 정보 교환 및 제3국과의 관계 강화를 도모하는 등 그 역할이 확대되고 있으며, 최근 사이버범죄의 증가로 인해 조사 및 기소를 지원하는 사건도 증가하고 있음.

2) Europol and Eurojust, 2019, Common challenges in combating cybercrime

3) 유럽 형사경찰기구는 EU의 범죄 대책 기구로 회원국의 경찰 기관이 서로 정보를 공유하여 중대한 국제 범죄에 대처하는 것을 목적으로 1999년부터 실질적으로 활동을 시작하였음. 기관 자체적으로 수사나 체포 권한은 없고, 각 경찰기관을 위해 정보의 교환과 분석, 전문기술 제공 및 훈련을 지원함.

4) The European Union Agency for Network and Information Security: EU 전역의 네트워크 및 정보보안을 개선하기 위해 2004년 설립된 기관으로 회원국의 사이버보안 관련 전문성 강화를 위한 조정 및 지원역할을 수행함.

5) European Judicial Cybercrime Network (EJCN)

o **(주요 추진 과제)** 사이버범죄 퇴치를 위해 해결해야 할 주요과제로 ▲데이터 및 위치정보 확보 ▲법률체계 개선 ▲국제 협력 체계 확립 ▲민관 파트너십 강화를 다음과 같이 제시

< 사이버범죄 퇴치를 위해 해결해야 할 주요과제 >

구분	내용
데이터 및 위치정보 확보	• 전자 데이터는 모든 사이버범죄 영역에서 성공적인 조사를 위한 기반이 되나, 정보 취득 가능성이 낮거나 제한되어 있음 • 최근의 경향을 분석한 결과 법 집행기관이 가해자의 물리적 위치나 범죄 인프라 또는 전자적 증거를 확보하기 어려운 상황 • 따라서 사이버범죄 조사와 관련된 데이터와 위치정보 확보방안 마련이 필요
법률체계 개선	• EU 회원국 간의 법률 체계의 차이로 인해 국제적인 사이버범죄 조사에 심각한 장애가 되고 있으므로, EU 및 국가 법률체계의 개선이 요구됨
국제 협력 체계 확립	• 국제적으로 신속한 증거 공유를 위한 공통적인 법적 프레임워크가 부재하여 협력에 장애가 되고 있고, 국경을 초월한 의사소통과 빠른 정보 교환을 위해 새로운 협력체계를 확립해야 함
민관 파트너십 강화	• 사이버범죄에 표준화된 대응수칙이 마련되어 있지 않아 체계적인 조사 및 대응에 어려움이 있으며, 이를 개선하기 위해서 민관 협력을 강화하는 것이 필요

o **(공동 대응 및 협력 기관)** 본 과제에서 ENISA는 아래와 같이 ▲대규모 사이버보안 사건에 대한 공동 연습 ▲사이버보안 및 암호와 관련된 법적·기술적 문제에 대한 협력 부문을 담당

- 대규모 사이버보안 사건에 대한 공동 연습: 2018년에 서명한 MOU[6]를 통해 사이버보안 사건과 관련된 정보 교환을 강화하고, 대규모 사이버보안 사건에 대한 공동의 연습 및 기술 협력 실시

- 사이버보안 및 암호 관련 법적·기술적 문제에 대한 협력: ▲사이버보안 관련 전문지식 네트워크 구축 ▲대체 조사기법 개발 ▲사이버보안 교육 프로그램 ▲범죄 수사에 활용되는 암호해독·암호화 능력 향상과 관련된 법적·기술적 문제에 대한 지원 수행

6) Europol, ENISA, EDA and CERT-EU, 26 June 2018, EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises Council conclusions.
다음 링크 참조 https://data.consilium.europa.eu/doc/document/ST-10086-2018-INIT/en/pdf

▶ 시사점

o 이번에 발표한 보고서는 사이버범죄 퇴치를 위해 향후 추진해야 할 중점 과제를 도출한 것으로, EU 사이버보안 관련 법제도 개선의 중요한 방향성을 제시하고 있다는 데 그 의의가 있음

o 유럽 사이버보안 역량 강화를 담당하는 ENISA는 사이버범죄의 퇴치를 위해 대규모 사이버보안 사건에 대한 공동 대응을 강화하고, 범죄수사 시 사이버보안 및 암호와 관련된 법적·기술적 지원을 수행하는 등 그 역할이 더욱 확대될 것으로 전망

※ **Reference**

http://www.eurojust.europa.eu/press/PressReleases/Pages/2019/2019-07-05.aspx

http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/Casework/Joint%20report%20of%20Eurojust%20and%20Europol%20on%20Common%20challenges%20in%20combating%20cybercrime%20%28June%202019%29/2019-06_Joint-Eurojust-Europol-report_Common-challenges-in-combating-cybercrime_EN.PDF

해외 입법 동향 EU

유럽 은행감독청(EBA), 핀테크 서비스의 규제 및 허가에 대한 보고서 발표 (2019. 7. 19.)

유럽 은행감독청(EBA)[1]은 핀테크[2] 서비스의 규제체계와 허가 원칙·방법을 안내하는 《핀테크 서비스의 규제 및 허가에 대한 보고서》[3]를 발표 (2019. 7. 19.)

▶ 개요 및 경과

o 유럽 은행감독청(EBA)은 유럽의 핀테크 기업에 당면한 현행 규제체계와 관련된 주요 과제를 도출하고, 국경을 넘나드는 핀테크 산업의 특성을 고려하여 서비스 허가 시 동일한 원칙을 적용할 것을 제안하는 《핀테크 활동 규제 및 권한 부여에 대한 접근방법 보고서》를 발표함

- 핀테크 서비스 허가 시 신청자가 제시하는 사업 모델 형태에 상관없이 《지불서비스 지침(PSD2)》[4]에 따라 비례적이고 유연성있는 원칙[5]을 적용
- 국가별 제도의 특수성을 고려하기 위해 지속적인 모니터링을 실시

o 이번에 EBA가 발간한 보고서는 지난 2018년 3월 유럽집행위원회에서 발표한 《핀테크 실행계획》[6]에 포함된 혁신 핀테크 사업모델에 대한 허가 및 라이센스 접근방법 지원의 일환으로 작성된 것임

▶ 주요 내용

o **(목적)** 유럽 핀테크 서비스에 적용하는 규제 관련 체계를 분석하여 향후 해결해 나가야 할 주요과제를 도출하고, 핀테크 기업에 적용하는 EBA의 허가 원칙과 방법을 안내

1) European Banking Authority: 유럽 은행부문에 대한 건전성 규제 및 감독, 각종 금융 규제 정책의 조정을 담당하는 금융 감독기구로 2011년에 설립됨
2) FinTech: '금융(finance)'과 '기술(technology)'이 결합한 서비스로 금융과 IT기술의 융합을 통한 금융 서비스 및 산업의 변화를 의미함
3) EBA publishes Report on regulatory perimeter, regulatory status and authorisation approaches in relation to FinTech activities
4) Payment Services Directive 2 (Directive (EU) 2015/2366): EU 지역의 지불 서비스에 대해 동일한 규칙을 적용하여 효율적이고 통합된 시장을 만들기 위한 것으로, 비 은행권의 결제 산업 참여가 가능하며 공평한 거래 환경을 제공하는 데 그 목적이 있음. 제29조제5항은 EBA가 비례성의 원칙에 따라 적용할 규제 기술 표준을 개발해야 한다고 명시하였으며, 본조 제6항은 동 표준에 국경을 초월하여 운영되는 기관의 감독 및 교환할 정보 범위 등의 협력 방법·수단 등을 명시하여 일관성 있고 효율적인 감독을 보장하도록 규정함.
5) 국경을 초월한 새로운 핀테크 서비스에 통일된 규칙을 적용하되, 서비스 간 규모·리스크 특성·복잡성 등을 감안하여 기준을 차등화 하는 등 유연하게 제도를 운영
6) The European Commission's FinTech Action Plan ((COM)2018) 109 final

o **(주요 내용)** 본 보고서에서 제시한 핀테크 서비스 관련 규제 현황 및 허가 원칙을 정리하면 다음과 같음

< 핀테크 활동 관련 규제 현황 및 허가에 대한 접근법 >

구분	주요 내용
규제 현황	• 현재 금융 당국의 핀테크 활동 관련 규제를 확대하기 위한 추가적인 권장사항은 없다고 판단되지만 새로운 핀테크 서비스 도입 등으로 추가적인 규제가 필요한 경우를 대비해 지속적인 모니터링을 실시할 예정 • 현행 PSD2 지침에 대부분의 핀테크 기업이 적용 대상이 되며, 이 외의 경우에도 본질적으로 비 재무적이라는 점에서 필요한 추가 조치는 없음 • 그러나 현재 각 국의 규제기관이 서로 다른 규제 방법[7]을 사용함에 따라 국경을 초월한 새로운 핀테크 서비스의 확대에 어려움이 있으므로, 유럽 전체의 공통된 원칙을 적용하는 것이 필요
핀테크 서비스 허가 원칙	• 규제기관[8]은 핀테크 기업이 관련 서비스를 신청하는 경우 사업 모델에 상관없이 PSD2 지침에 따라 비례적이고 유연성 있는 원칙을 적용하기 위해 노력해야 함 - 국경을 초월한 새로운 핀테크 서비스에 통일된 규칙을 적용 - 서비스 간 규모・리스크 특성・복잡성 등을 감안하여 기준을 차등화 하는 등 유연하게 제도를 운영 • 특히 결제 또는 전자화폐 기관으로 허가를 받는 경우 핀테크 서비스의 응용프로그램에 비례성이 사용되는지 여부를 평가할 예정

▶ 시사점

o 이번에 EBA가 발간한 보고서는 유럽의 핀테크 사업모델에 대한 허가 및 라이센스 접근방법의 일환으로 작성된 것으로 향후 관련된 입법 및 허가 기준에 대한 방향성을 제시한다는 점에서 그 의의가 있음

o 특히 본 보고서에서 국경을 초월한 클라우드 펀딩 사업자 및 소비자에게 통일된 규칙을 적용하는 것을 기본적인 정책방향으로 제시하고 있어 향후 국경을 넘나드는 핀테크 서비스 산업의 규제차익 거래[9]가 최소화 될 것으로 전망

※ **Reference**

https://eba.europa.eu/documents/10180/2551996/Report+regulatory+perimeter+and+authorisation+approaches.pdf

https://eba.europa.eu/-/eba-publishes-report-on-regulatory-perimeter-regulatory-status-and-authorisation-approaches-in-relation-to-fintech-activities

7) 사전 허가와 사후 승인 등 국가별 관행 및 규제기관 여건에 따라 접근 방법을 달리 적용하고 있음.
8) EBA, EU 및 국가별 금융규제관련 기관
9) 어떤 거래가 특정 국가에서 금지되거나 원치 않는 방식의 규제와 과세가 적용될 경우 해당 국가를 피해 다른 나라에서 더 유익한 거래를 선택하는 것을 의미함.

영국 재무부, 디지털 서비스에 세금을 부과하는 법률 초안 발표 (2019. 7. 11.)

영국 재무부는 2020년 4월부터 발생하는 주요 디지털 서비스 활동 수익에 대하여 세금을 부과하는 《디지털 서비스에 대한 세금법 초안》[1]을 발표 (2019. 7. 11.)

▶ 개요 및 경과

o 영국 재무부는 대형 디지털 서비스 사업자가 자국 내에서 창출하는 디지털 서비스 활동 수익에 대하여 2020년 4월부터 세금을 부과하는 《디지털 서비스에 대한 세금법 초안》을 발표

- 본 법안에 적용되는 디지털 서비스 활동은 소셜 미디어 플랫폼과 인터넷 검색 엔진, 온라인 디지털 시장이며, 온라인 광고 사업도 포함됨

- 세금 부과 기준은 디지털 서비스 활동으로 인해 전 세계적인 수익이 5억 파운드 이상이고 영국으로부터 창출된 수익이 2천5백만 파운드 이상인 경우, 해당 디지털 서비스 수익의 2%를 부과

o 영국 정부는 재정법 개선의 일환으로 금년 2월에 디지털 서비스 세금에 대한 중앙부처 및 관계기관 의견을 사전에 수렴한 바 있으며, 이번에 공개한 법안 초안에 대해서 2019년 9월 5일까지 대국민 공개 의견수렴 및 관계기관 협의를 실시

▶ 주요 내용

o **(목적)** 대형 디지털 서비스 사업자가 영국 내 이용자들로부터 벌어들인 수익에 세금을 부과하는 새로운 디지털 서비스 세금을 도입

o **(용어 정의)** 본 법안에서 정의한 주요용어를 정리하면 다음과 같음

- 디지털 서비스 활동(Digital services activity): 소셜 미디어 플랫폼과 인터넷 검색 엔진, 온라인 마켓[2]을 통해 서비스를 제공하는 활동으로, 온라인 광고 사업을 포함[3]

- 디지털 서비스 수익(Digital services revenues): 기업 구성원의 디지털 서비스 활동과 관련한 총 수익 금액

---

1) Finance Bill 2019-20 to establish a Digital Services Tax(DST)
2) 다음을 충족하는 온라인 플랫폼을 의미함. 플랫폼의 주요 목적 또는 주요 목적 중 하나가 사용자에 의해 특정 물건(서비스, 상품 또는 기타 자산) 판매를 촉진하는 것, 사용자가 플랫폼에서 특정 물건을 판매하도록 다른 사용자에게 광고 등을 제공하는 것
3) 금융 및 결제 서비스 제공자는 제외됨

- 영국 사용자: 보통 영국에 거주하고 있는 사용자로, 온라인 마켓에서 거래 당사자들 중 하나가 영국 사용자인 경우 그 거래에서 발생하는 모든 수익은 영국 사용자들로부터 창출된 것으로 간주함

o **(주요 내용)** 본 법안에서 정의한 주요용어 및 적용대상, 세금 부과 기준을 정리하면 다음과 같음

< 영국 디지털 서비스 세금의 적용대상 및 부과기준 >

구분	내용
적용대상	• 본 법안에 따라 신설되는 디지털 서비스 세금은 소셜 미디어 플랫폼 및 인터넷 검색엔진, 온라인 광고 사업을 포함한 온라인 마켓 서비스를 제공하여 영국 사용자로부터 수익을 창출하는 대규모 다국적 기업에게 적용되며, 금융 및 결제 서비스 사업자는 세금 부과 대상에서 제외
부과기준	• 2020년 4월부터 발생하는 디지털 서비스 활동 수익에 대하여 디지털 서비스 활동으로 인한 글로벌 수익이 연간 5억 파운드 이상이고 영국 사용자들로부터 창출된 수익이 2천5백만 파운드 이상인 경우, 디지털 수익의 2%를 세금으로 부과

o **(보고 의무)** 세금 부과기준이 충족될 경우 해당 기업은 영국 국세청에게 관련 정보를 보고할 의무가 있음

- 국세청은 보고의무와 관련된 방법 및 항목[4]을 회계기간 종료일 이전 90일 이내에 공표해야 함

- 1차 의무보고 회계기간은 2020년 4월 1일부터 2021년 3월 31일까지로 함

o **(기타 사항)** 재무부는 2025년까지 디지털 서비스 세금 부과에 대한 검토 보고서를 작성하고, 의회에 보고서를 제출해야 함

▶ 시사점

o 영국은 디지털 경제에서 발생하는 사업 중 상당수가 사용자와의 상호 작용 및 참여에서 가치를 창출하고 있는 것으로 판단하고, 창출된 가치와 수익의 과세 간 불일치가 발생하는 문제를 해소하기 위해 새로운 디지털 서비스 세금을 도입함

o 본 법안이 시행되면 영국 정부는 디지털 서비스 활동과 관련된 세금 체계의 공정성을 확보할 것으로 기대하고 있으며, 향후 관련된 국제적인 표준이 마련될 경우 이를 따를 수 있도록 재검토 규정을 두는 등 탄력적으로 운영할 계획임

※ **Reference**

https://www.gov.uk/government/publications/introduction-of-the-new-digital-services-tax

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/816361/Digital_services_tax.pdf

4) 관련된 세부 지침은 2020년 4월까지 제정할 계획임

프랑스 국회, 온라인 혐오 관련 콘텐츠의 삭제 의무를 강화하는 법안 채택 (2019. 7. 9.)

프랑스 국회는 온라인 소셜 미디어 등을 통한 혐오 관련 발언을 억제하기 위해 소셜 플랫폼 등에 매출의 일정비율을 벌금으로 부과할 수 있는 《인터넷 혐오 대응 법안》[1] 채택 (2019. 7. 9.)

▶ 개요 및 경과

o 프랑스 국회는 페이스북 및 트위터 등 온라인 소셜미디어를 통한 증오・모욕 및 차별 발언을 억제하기 위해 해당 플랫폼 등에 관련 콘텐츠 삭제를 의무화하고, 미준수 시 전년도 글로벌 매출의 최대 4%를 벌금으로 부과할 수 있는 《인터넷 혐오 대응 법안》을 채택

- 온라인 플랫폼 사업자는 인종・종교・성적 성향・장애를 이유로 한 혐오 관련 콘텐츠를 게시 24시간 이내에 삭제해야 함
- 고등시청각위원회(CSA)[2]는 해당 플랫폼 운영자로부터 인터넷 혐오 관련 콘텐츠 삭제 여・부를 확인하는데 필요한 정보를 수집할 수 있고, 위반사항이 발생한 경우 권고 및 제재를 실시
- 본 법안에 따라 《디지털 경제의 상호신뢰에 관한 법률》[3] 일부가 개정될 예정

o 지난 2019년 5월 프랑스 파리에서 17개국과 8개 소셜미디어 사업자는 폭력극단테러리즘을 억제할 것을 약속하는 자발적 서약서를 체결한 바 있으며, 특히 트위터는 본 법안에 대하여 지지의사를 표명

▶ 주요 내용

o **(목적)** 온라인 플랫폼 사업자에게 혐오 등 불법 콘텐츠를 제거할 의무를 부여하여 사업자의 책임을 강화하고, 혐오 콘텐츠의 인터넷 확산 방지

---

1) PROPOSITION DE LOI visant à lutter contre les contenus haineux sur internet

2) Conseil supérieur de l'audiovisuel (CSA): 프랑스의 방송분야 독립규제기관으로, 국민의 시청각 권리 및 자유 보장을 목적으로 1989년에 설립되었으며 미디어 전반에 대한 각종 규제제정 및 방송 사업자의 인허가, 프로그램의 규제를 담당하고 있음

3) Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique(LCEN): 온라인 통신의 자유, 전자상거래, 디지털 경제에서의 보안과 관련된 사항으로 구성되어 있음. 특히 제6조는 인터넷 서비스 제공자가 범죄・테러・증오・폭력에 대한 선동 및 인간의 존엄성에 대한 공격 등과 관련된 콘텐츠를 관할 공공 당국에 통보하도록 규정함

o **(주요 내용)** 동 법안은 크게 ▲온라인 플랫폼 사업자가 혐오 콘텐츠를 제거할 의무 ▲온라인 혐오 콘텐츠에 대한 신고 절차 개선 ▲온라인 플랫폼 운영자[4]의 정보 제공 의무 ▲CSA의 역할 및 벌금 관련 규정 ▲범죄 대응 효과 강화로 구성되며, 부문별 주요 내용을 요약하면 다음과 같음

< 인터넷 혐오 대응 법안의 주요 내용 >

구분	주요 내용
온라인 플랫폼 사업자가 혐오 콘텐츠를 제거할 의무와 관련된 규정	• 온라인 공공 통신 서비스를 제공하는 온라인 플랫폼 사업자는 테러 행위, 인종·종교·민족 및 장애·나이·성적성향으로 인해 사람이나 집단에 대한 증오·폭력·차별·모욕을 선동하는 행위와 관련된 콘텐츠가 발견·신고되면 24시간 이내에 해당 콘텐츠를 철회하고, 해당 불법 콘텐츠를 철회했음을 나타내는 메시지로 대체할 의무가 있음 • 삭제된 불법 콘텐츠는 형사범죄를 수사·적발·기소할 목적으로 최대 1년간 보관해야 하며, 사법당국이 정보를 이용할 수 있도록 해야 함
온라인 혐오 콘텐츠에 대한 신고 절차 개선	• 온라인 플랫폼 사업자는 혐오 콘텐츠 제거 의무 이행을 위해 CSA가 권고하는 사항을 준수 • 접수된 통지가 신속하게 처리되도록 노력하고 통지된 내용을 적절히 검토하여 부당한 철회 위험을 방지해야 함
온라인 플랫폼 운영자의 정보 제공 의무	• 온라인 플랫폼 사업자는 사용자에게 이용 가능한 사법적 구제책에 관한 사항 등 공공 정보를 명확하고 상세하며 쉽게 접근할 수 있도록 제공 • 온라인 플랫폼 사업자가 혐오 콘텐츠를 제거할 의무 규정에 따른 활동은 지체 없이 관할 공공기관에 통지하여야 하며, 국민에게 서비스의 일반적 이용조건을 정확하고 쉽게 이해할 수 있도록 객관적인 용어로 제공 • 상기한 의무 준수를 위해 도입한 인적·기술적 자원, 예방 및 대응 조치 등의 결과는 CSA에 보고해야 함
CSA의 역할 및 벌금 관련 규정	• CSA는 온라인 플랫폼 사업자가 지켜야할 의무의 적절한 이행을 위해 모니터링 수행 및 권고안 제시, 법 적용에 대한 연간 평가를 실시 • 대상 사업자가 권고 등에 따라 적절한 수단[5]을 실시하지 않은 경우 CSA는 전년도 글로벌 총 매출액의 4%를 초과하지 않는 한도로 벌금을 부과
범죄 대응 효과 강화	• 범죄 대응 효과를 강화하기 위해 관리 당국은 검색 엔진 등에 혐오 콘텐츠 접근을 제공하는 주소 참조를 중단하도록 명할 수 있음 • 사법 판결이 범죄에 해당하는 경우 사이트 및 서버, 콘텐츠 접근을 차단

4) 동 법안에는 그 기준이 명확하게 나타나 있지 않고 현재 논의 중에 있는 것으로 파악되며, 프랑스 주요 언론에 따르면 월 200만회 이상의 사용자가 방문하는 소셜 미디어 플랫폼을 기준으로 예상하고 있음.
5) 적절한 인적자원의 투입 및 기술적인 방법을 통해 권고사항에 대한 효과적인 처리를 실시(예방 수단을 사용자에게 제공하는 것도 포함)하는 것을 의미함

▶ 시사점

o 본 법안은 소셜 미디어의 투명성 제공 및 테러리즘 관련 데이터 제공 등을 요구하는 조치를 강화하기 위해 새로운 법을 도입한다는 데 그 의의가 있음

o 프랑스의 일부 의원 및 단체들은 법 시행 과정에서 온라인 플랫폼 콘텐츠가 임의로 평가 및 삭제될 수 있다는 것을 우려하고 있으나, 트위터 등 주요 온라인 소셜 미디어 사업자가 동 법안에 지지하고 있어 내용의 큰 변동 없이 법안이 통과될 것으로 전망

※ **Reference**

http://www.assemblee-nationale.fr/15/ta/ta0310.asp
http://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_contre_haine_internet

해외 입법 동향 일본

일본 국토교통성, 자율주행 서비스를 도입하는 버스・택시 사업자를 위한 가이드 발표 (2019. 6. 26.)

일본 국토교통성은 Level4 자율주행 서비스[1]의 안정성 및 편의성 확보를 위해 여객자동차 운송사업자가 준수해야 할 사항을 권고하는 가이드라인[2]을 발표 (2019. 6. 26.)

▶ 개요 및 경과

o 일본 국토교통성은 한정된 지역[3]에서의 Level4 자율주행 서비스를 도입하는 여객자동차 운송사업자를 대상으로 해당 서비스의 안전성과 편의성을 확보하기 위해 대응해야 할 기본적인 사항을 권고하는 《무인 자율주행 서비스를 도입하는 버스・택시 사업자를 위한 가이드라인》을 발표함

- 본 가이드라인은 원격 조작자 감시 등을 통해 안전 확보 조치가 마련된 한정된 지역에서의 Level4 자율주행 서비스를 실시하는 여객자동차 운송사업자를 대상으로 함

- 사업자가 준수해야 할 사항은 ▲교통규칙 준수 및 여객의 안전 확보 ▲차량 안전 확보를 위한 점검・정비 ▲비상대응 및 연락체계 정비 ▲운행 및 사고 기록 실시 ▲운행체제 개선 부문으로 구성

o 지난 2018년에 일본 내각부는 《자동운전에 관한 제도 정비 체계》[4]를 통해 2020년에 한정된 지역에서의 Level4 자율주행 서비스를 실시하고, 2025년에는 자가용까지 확대하는 것을 발표한 바 있음

▶ 주요 내용

o **(목적)** 무인 자율주행 서비스를 도입하는 여객자동차 운송사업자가 한정된 지역에서 해당 서비스의 안전성과 편리성 확보를 위해 준수해야 할 기본 사항을 권고

o **(적용 대상)** 원격 조작자 감시 등에 의한 안전 확보 조치[5]를 전제로 한정된 지역에서 무인 자율주행서비스를 실시하는 버스・택시 등의 여객자동차 운송사업자

1) 자율주행차량수준은 국제자동차기술자협회(SAE International)의 정의를 따르며, 레벨 4는 높은 수준의 자동화로 고속도로 등 특정 주행 환경 하에서 모든 주행 동작 수행이 가능하며 사람의 개입이 필요 없는 단계임 (인터넷 법제동향, Vol. 134, November 2018, p39 참조)
2) 限定地域での無人自動運転移動サービスにおいて旅客自動車運送事業者が安全性・利便性を確保するためのガイドライン
3) 본 가이드라인에서의 '한정된 지역'이란 공항 시설, 대학 캠퍼스 등 비교적 교통량이 적고 단순한 노선으로 운행하는 지역을 의미함.
4) 高度情報通信ネットワーク社会推進戦略本部・官民データ活用推進戦略会議,《自動運転に係る制度整備大綱》, 2018. 4. 17.
5) Level4 자율주행 서비스에서 원격으로 감시・조작이 가능한 경우 도로교통법 제77조에 따른 도로사용허가가 가능함.

o **(기본 방향)** Level4 자율주행 서비스를 실시하는 여객자동차 운송사업자는 운전자가 차 내에 있는 경우와 동등한 안전성을 확보하도록 노력하고, 차량의 정비・확인 등의 책임을 가지고 필요한 대응 업무를 수행

- 원격 감시 조작자도 《도로운송법》[6] 및 《도로교통법》[7]의 운전자와 동일한 의무가 있으며, 운전자 이외의 승무원은 비상시 적절하게 상황을 파악하고 《여객자동차 사업운수규칙》[8]을 준수해야 함

o **(사업자 준수 사항)** 상기한 기본방향에 따라 여객자동차 운송사업자가 부문별로 준수해야 할 사항을 요약하면 다음과 같음

< Level4 자율주행 서비스를 실시하는 여객자동차 운송사업자의 준수 사항 >

구분	내용
교통규칙 준수 및 여객의 안전 확보	• 운전자가 차 내에 있는 경우와 동등한 안전성을 확보하기 위해 교통규칙을 준수하고, 통신 지연 등에 대한 충분한 대처방안 마련 • 승강구의 문 개폐 및 운행 중 실내와 외부 상황을 파악할 수 있는 카메라 등을 통해 승객의 안전을 확보
차량 안전 확보를 위한 점검・정비	• 정기적인 소프트웨어의 업데이트 등 사이버보안 확보 조치 실시 • 자동차 제조사가 발간한 점검정비 매뉴얼 등을 활용 • 운행 전 차량 시스템의 점검 필수
비상대응 및 연락체계 정비	• 비상 상황[9] 발생 유・무 및 발생한 경우 장소 등을 정확히 파악 • 원격지로부터 적절한 대응이 마련되기 전에는 승무원을 승차시켜 비상 상황 발생 시 수동운전 등으로 대응할 수 있도록 조치
운행 및 사고의 기록	• 자율주행 시스템의 작동 상황 및 차량 실내 및 외부의 영상기기 등 운행 및 사고 상황 파악을 위해 기록을 보존해야 함
운행체계 개선	• 운행 정보의 입력 및 운행 중인 차량의 위치 파악이 가능하도록 조치 • 고령자와 장애인의 탑승에 대한 도움, 안내 등 편의사항을 지원해야 함

6) 《道路運送法》: 도로운송분야에서 이용자 수요의 다양화 및 고도화에 정확하게 대응한 서비스를 원활하게 제공하는 것을 촉진하여 수송의 안전을 확보하고 공공의 복지를 증진하는 것이 목적이며, 운전자와 관련하여 제23조의4(운행관리자의 의무), 제25조(운전사의 제한) 등의 규정이 있음.

7) 《道路交通法》: 도로교통에서의 위험과 장애를 방지하여 안전하고 원활한 도로교통을 도모하는 것을 목적으로 하며, 운전자 의무는 제71조(운전자의 준수 사항) 등에 규정되어 있음.

8) 《旅客自動車運送事業運輸規則》: 여객자동차 운송사업의 적절한 운영을 확보하여 교통안전 및 승객의 편의를 도모하는 것을 목적으로 하며, 승무원과 관련된 규정은 제15조(차장의 승무), 제49조(승무원), 제50조(운전자), 제51조(차장)임.

9) 운행 중단・사고, 자연재난, 차량의 중대한 고장 발견, 건널목 운행 불능, 여객이 차내 법령 규정 및 공공질서에 반하는 행위를 할 경우 등이 있음.

▶ 시사점

o 일본 내각은 지난 3월에 Level3 자율주행자동차의 도로주행을 허용하는《도로교통법》및《도로운송차량법》개정안을 의결[10]하여 금년 12월에 개정된 법이 시행될 예정이며, 이번에 발표한 가이드라인은 자율주행 서비스의 다음 단계인 Level4 자율주행 서비스 실시의 기준이 된다는 점에서 그 의의가 있음

o 일본 정부는 이번에 발표한 가이드라인에 따라 현재 시범적으로 실시하고 있는 Level4 자율주행 서비스의 안전성・편의성 확보 및 향후 해당 서비스의 확대 기반을 마련할 수 있을 것으로 기대

※ **Reference**

http://www.mlit.go.jp/report/press/jidosha02_hh_000379.html
http://www.mlit.go.jp/common/001295527.pdf

10) 인터넷 법제동향, Vol. 138 (March 2019) 31p 참조.

해외 입법 동향 중국

중국 국가인터넷정보판공실(CAC), 클라우드 서비스 보안 평가 규정 발표 (2019. 7. 22.)

중국 국가인터넷정보판공실(CAC)[1]은 정부와 국가 중요 인프라에서 사용하는 클라우드 서비스의 보안 평가·인증을 의무화 하는《클라우드 서비스 보안 평가 규정》[2]을 발표 (2019. 7. 22.)

▶ 개요 및 경과

o 중국 국가인터넷정보판공실(CAC)은 관계부처[3]와 공동으로 2019년 9월부터 정부 및 공공기관, 국가 중요 인프라에 클라우드 서비스를 제공하려는 경우 보안 평가 및 인증 취득을 의무화 하는《클라우드 서비스 보안 평가 규정》을 발표함

- 본 규정에 의한 보안 평가는 ① 클라우드 서비스 제공 업체가 CAC에 보안 평가 신청 ② CAC 평가 전문가 팀의 신청자료 검토 ③ CAC가 신청 업체에 평가 승인여부 통보 순으로 진행

- 클라우드 서비스 보안 평가 시 일반적인 경영상황 외에 보안관리 능력과 업무의 연속성을 중점적으로 검토할 것을 명시

- 본 규정은 2019년 9월 1일부터 시행

o CAC의 사이버보안 검토 사무국은 2014년에《클라우드 컴퓨팅 서비스 보안 가이드》[4] 및《보안기능 요구 사항》[5]을 제정하였고, 그 동안 정부부처의 클라우드 컴퓨팅 서비스에 대한 보안 관리 강화[6]를 지속적으로 요구한 바 있음

▶ 주요 내용

o **(목적)** 정부 및 공공기관, 국가 주요 정보 인프라에서 사용하는 클라우드 서비스의 안전성을 향상하기 위해 보안 평가 및 인증 제도를 도입

1) 國家互聯網信息辦公室(Cyberspace Administration of China, CAC): 중국의 인터넷 관련 규제와 정책을 총괄하는 국무원 산하 기관으로 인터넷 정보와 관련된 법규 및 정책 제정, 유관기관들에 대한 인터넷 정보 내용 관리 강화 지도, 인터넷 정보 등에 대한 심사·허가와 감독 관리 업무를 수행하며 2011년에 설립됨
2) 云计算服务安全评估办法
3) 국가발전개혁위원회(国家发展和改革委员会), 공업정보화부(工业和信息化部), 재무부(财政部)가 공동으로 참여하여 본 규정을 개발함
4) 国家标准《信息安全技术 云计算服务安全指南》(GB/T 31167-2014)
5) 国家标准《信息安全技术 云计算服务安全能力要求》(GB/T 31168-2014)
6) 中网办发文〔2014〕14号, 关于加强党政部门云计算服务网络安全管理的意见

o **(보안 평가 및 인증 대상)** 정부 및 공공기관, 국가 주요 정보 인프라에 클라우드 컴퓨팅 서비스 플랫폼을 제공하는 업체로 클라우드 컴퓨팅 서비스 SW 및 HW, 관리 시스템이 보안 평가 및 인증 대상임

o **(보안 평가 신청 시 제출 자료 및 중점 검토 사항)** 본 규정에 따라 클라우드 서비스의 보안 평가를 신청하는 경우 업체가 제출해야할 자료와 CAC가 중점적으로 검토할 내용을 정리하면 다음과 같음

< 클라우드 서비스 보안 평가 신청 시 제출 자료 및 중점 검토 사항 >

구분	주요 내용
제출자료	• 클라우드 서비스 업체가 CAC에 보안 평가 신청 시 제출해야 할 자료 - 클라우드 서비스 보안 평가 신고서 - 클라우드 서비스 시스템의 보안 계획서 - 사업연속성 및 공급망의 보안성 보고서 - 데이터의 이식성[7] 분석 보고서 - 안전성 평가에 필요한 기타 자료
중점 검토 사항	• CAC가 보안 평가 시 중점적으로 검토해야 할 사항 - 업체 경영현황 및 신용정보와 같은 기본 정보 - 클라우드 서비스 공급업무 담당 인력에 대한 정보 - 클라우드 플랫폼 관련 보유 기술, 제품 및 서비스 공급망의 보안 현황 - 보안 관리 능력 및 업무 연속성, 데이터 이동의 편의성 및 호환성 - 클라우드 서비스 보안에 영향을 줄 수 있는 기타 요소

o **(인증 유효기간 및 갱신)** 클라우드 서비스 보안 평가 인증서는 3년간 유효하며, 평가 기간을 연장해야 하는 경우 클라우드 서비스 제공 업체는 만료일 최소 6개월 전에 CAC에 인증 갱신을 요청해야 함

▶ 시사점

o 중국 정부는 국가 중요 인프라의 사이버보안 수준을 향상하기 위해 최근 활용이 확대되는 클라우드 서비스에 대한 보안 인증 제도를 도입

o 이번에 발표한 규정에 따라 중국 정부 및 국가 중요 정보 인프라에 클라우드 서비스를 제공하려는 업체는 CAC의 보안 승인을 취득한 경우에만 공공조달 시장에 참여가 가능하므로 향후 민간 부문에도 보안 평가 및 인증이 확대되어 클라우드 서비스 전반의 사이버보안 수준이 향상될 것으로 전망

7) 하나의 플랫폼에서 다른 플랫폼으로 옮기는 것이 용이한 것을 의미함

※ **Reference**

http://www.cac.gov.cn/2019-07/22/c_1124781475.htm
http://www.cac.gov.cn/2019-07/22/c_1124781522.htm
http://www.xinhuanet.com/2019-07/23/c_1124785708.htm

호주 연방의료제품청(TGA), 산업용 의료기기의 사이버보안 지침 발표 (2019. 7. 18.)

호주 연방의료제품청(TGA)[1]는 SW와 전자부품이 포함된 산업용 의료기기의 제조·공급 업체에게 사이버보안 기준을 안내하는 《산업 의료기기 사이버보안 지침》[2]을 발표 (2019. 7. 18.)

▶ 개요 및 경과

o 호주 연방의료제품청(TGA)은 최근 의료기기에 IoT 및 AI 기술 활용의 확대로 인해 증가하는 사이버보안 위협에 대응하기 위해 산업용 의료기기의 제조·공급 업체에게 사이버보안 기준을 안내하는 《산업 의료기기 사이버보안 지침》을 발표함

- 본 지침의 적용 대상은 디자인에 인공지능 기술이 접목된 장치를 포함한 의료기기용 소프트웨어 개발 및 의료기기 제조·공급 업체임

- 주요 내용은 ▲의료제품의 수명 주기와 사이버보안 위험 모니터링 ▲사이버보안의 기술적 요구 사항 ▲사이버보안 위협 대응 및 정보공유 관련 사항으로 구성

▶ 주요 내용

o **(목적)** 호주 의료기기 부문의 사이버보안 수준 향상을 위해 산업 의료기기 개발·제조·공급 업체가 관련 규정 및 전략을 이해할 수 있도록 지원하고, 준수해야 할 보안 기준을 제시

- 본 지침은 사이버보안 측면에서 《의약품법》[3] 및 《의약품규정》[4]을 준수하기 위해 필요한 세부사항의 검토와 호주 정부의 《사이버보안 전략》[5]을 고려하여 작성

o **(적용 대상)** 본 지침은 SW 및 전자부품을 포함한 의료기기의 개발·제조·공급 업체를 대상으로 하며, 의료기기는 디자인·설계에 인공지능 기술이 접목된 SW 및 사이버보안 위협에 취약할 수 있는 구성요소가 내재된 장치도 해당됨

---

1) Therapeutic Goods Administration: 호주 보건부(Australian Government Department of Health) 산하의 기관으로 호주 내 새로운 의료 제품 유통 심사·허가 및 모니터링 등의 규제업무를 담당하고 있음
2) TGA, July 2019, Medical device cyber security guidance for industry
3) Therapeutic Goods Act 1989: 의료제품의 품질·안전성·적기 이용가능성·유효성 관리를 목적으로 호주 내 의료제품의 등록 및 의료기기 관련 사항을 규정함
4) Therapeutic Goods (Medical Devices) Regulations 2002: 의료기기의 안전과 성능 특성에 관련된 규정으로 안전성 등을 위해 준수해야 할 기본적인 원칙을 포함하고 있음
5) Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2016, Australia's Cyber Security Strategy: 호주 정부가 2016년에 발표한 2020년까지의 사이버안보 전략으로, 5개 주제(국가 사이버 협력 관계, 강력한 사이버 방어, 국제적 책임과 영향력, 성장과 혁신, 사이버 스마트 국가)별 전략을 제시함

o **(주요 내용)** 본 지침에서 사이버보안과 관련된 주요 내용을 정리하면 다음과 같음

< 호주 산업 의료기기에 대한 사이버보안 지침의 주요 내용 >

구분	내용
의료기기의 수명 주기 및 사이버보안 위험 모니터링	• 호주 의료제품 등록부(ARTG)[6]에 등록되지 않은 의료기기는 호주 내에서 유통될 수 없으며, 총 제품 수명주기(TPLC)[7]에 걸쳐 사이버보안에 취약한지 검토해야 함 • 의료기기 제조업체는 ARTG에 등록된 의료기기에 새로운 사이버보안 취약점이 발견되는지 지속적으로 정보를 모니터링하고, 수집된 보안 취약점 등의 정보를 TGA와 공유
의료기기 사이버보안의 기술적 요구 사항	• 의료기기 제조업체는 환자 안전에 대한 위험이 제거·축소되도록 기기의 시판 전에 사이버보안을 고려하여 제품을 개발해야 함 - 설계 단계에서부터 중요한 SW 구성요소가 다른 SW에 의해 영향을 받지 않도록 사이버보안 모듈을 독립적으로 분리하고, 검증된 모듈의 재사용에 노력 • 사이버보안 전문가 등을 통한 평가 및 모의 침투 테스트 실시 - 개발팀과 별도로 독립된 전문가가 다양한 시나리오 및 방법을 활용하여 사이버보안 성능 테스트를 수행 - 침투 테스트 결과에 대한 조치 및 새로운 취약성에 대한 지속적 평가 실시 • 실제 소비자들이 사용하는 모바일 기기 및 웹, 클라우드 서비스 등을 활용하여 사이버보안 위험 평가를 실시 • 의료기기가 필요한 네트워크에만 접속할 수 있도록 보장하고, 다단계 인증 및 데이터 암호화 실시
의료기기 사이버보안 위협 대응 및 정보공유	• 의료기기의 제조·공급 업체는 사이버보안 위협으로 인한 환자의 위해성을 평가하고, 발생한 위험에 대하여 아래와 같은 대응 조치를 실행 - 의료기기에 결함이 있거나 잠재적 결함이 있는 것으로 확인된 경우 반드시 TGA와 협의하여 적절한 조치[8]를 취해야 함 • 호주사이버보안센터(ACSC)에서 운영하는 사이버보안 위협 정보 공유 시스템 활용을 권장

6) Australian Register of Therapeutic Goods: 의약품법(Therapeutic Goods Act 1989)에 따라 호주에서 수입·판매·수출 하고자하는 모든 의료기기 및 의약품은 TGA의 심사를 받아 등록받아야 하며, 사전에 적합성 평가 인증서를 획득해야 함. 등록 허가 절차는 제조공장의 품질 심사 및 평가, 제품의 시판 전 적합성 검사, 시판된 제품의 규격에 대한 지속적 적합성 검사로 진행됨

7) Total product life cycle: 제품의 개발 및 운용, 유지보수에 내포된 프로세스, 활동과 업무를 포함하고 제품의 수명을 요구사항의 정의에서 사용 종료에 이르기까지 전체를 포괄하는 개념임. 의료기기 소프트웨어 수명주기와 관련된 국제표준규격은 IEC 62304(Medical devices software - Software life cycle processes)를 참조

8) 사용자 또는 공중 보건의 건강과 안전에 중대한 위협이 되는 사이버 보안 문제의 경우 즉시 회수 절차(Uniform recall procedure for therapeutic goods, URPTG)를 실시하며, 절차별 내용은 다음의 링크를 참조. https://www.tga.gov.au/recall-procedure

▶ 시사점

o 호주 정부는 인터넷 연결 및 AI기술이 접목된 의료기기의 경우 사이버보안 측면에서 잠재적인 위험성이 높다고 판단하고 있음

o 이번에 발표한 지침은 의료기기의 전체 수명주기를 포함하여 설계단계에서부터 사이버보안을 고려하도록 요구한다는 특징이 있으며, 향후 호주 내 새로운 의료제품과 관련된 유통 심사·허가 및 모니터링 등의 규제업무를 담당하는 TGA의 역할도 더욱 확대될 전망

※ **Reference**

https://www.tga.gov.au/publication/medical-device-cyber-security-guidance-industry

https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

기고

인터넷상 불법정보 차단의 법적 쟁점

정경오 법무법인 린 변호사

- (現) 법무법인 린 변호사
- (前) 정보통신정책연구원 부연구위원
- (前) 방송통신심의위원회 전문위원
- (前) 정보통신윤리위원회 심의실장
- 제43회 사법시험 합격

Ⅰ. 개요

최근 정부가 도입한 해외 음란·도박사이트 등 불법사이트에 대한 접속차단을 두고 검열이니 표현의 자유 침해니 논란이 뜨겁다. 보안전문가와 일부 시민단체 등은 불법사이트에 대한 정부의 접속차단조치는 통신감청에 해당하며 정부가 인터넷 검열을 시작하는 것이라고 주장하고 있다. 이에 방송통신위원회는 "통신감청과는 무관하다"고 해명자료까지 내놓을 정도까지 이를 지경이다.

이번에 논란이 되고 있는 SNI 차단방식 이전에도 불법정보에 대한 접속차단은 이전에도 있었는데, 최근 도입한 SNI 차단방식에 대해서만 유독 통신감청이니 인터넷 검열이니 하는 논란이 일고 있는지에 대하여 법적인 관점에서 살펴보고자 한다.

Ⅱ. 인터넷상 불법정보 차단이 감청에 해당하는지 여부

1. 인터넷상 불법정보 차단

인터넷상 불법정보는 우리가 흔히 알고 있는 인터넷 사이트에서 유통되는 음란정보 또는 도박정보 등을 말한다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '정보통신망법'이라 한다) 제44조의7 제1항은 11가지의 불법정보의 유형을 규정하고 이러한 불법정보의 유통을 금지하고 있다.[1)]

1) **제44조의7**(불법정보의 유통금지 등) ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.
1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보

기고

인터넷상 불법정보에 대한 접속차단은「방송통신위원회의 설치 및 운영에 관한 법률」(이하 '방통위설치법'이라 한다)에 근거를 두고 있다. 방통위설치법 제21조는 방송통신심의위원회의 직무를 규정하고 있는데, "전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 대통령령이 정하는 정보의 심의 및 시정요구(제4호)"가 접속차단의 근거이다. 방통위설치법 시행령 제8조는 시정요구의 종류로 '접속차단'을 명시하고 있다.[2)]

2. 불법정보 차단방식

불법정보를 차단하는 방식에는 DNS(Domain Name System)차단방식, IP차단방식, URL(Uniform Resource Locator)차단방식, SNI(Server Name Indication)차단방식이 있다.

DNS(Domain Name System)차단방식은 이용자가 불법사이트(불법.com)에 접속할 경우 통신사가 DNS서버에서 불법사이트 IP주소 대신 방송통신심의위원회의 차단안내서버 (warning.or.kr) IP주소를 알려주어 불법사이트 접속을 차단하는 방식이다. 이용자가 국내 통신사의 DNS서버를 이용하지 않고, 외국 통신사의 DNS서버를 이용하거나 직접 해당 IP주소를 입력하는 경우 차단을 할 수 없다는 단점이 있다.

IP차단방식은 라우터 장비에 차단 IP를 입력하여 해당 IP에 대한 Routing(해당 웹서버로 찾아가는 경로)을 알려주지 않는 방법으로 차단하는 방법이다. IP차단방식은 고급 사양의 라우터는 IP뿐만 아니라 Domain 단위의 차단도 가능하고, 국제 관문에서 일괄적 차단은 거의 모든 불법 트래픽에 대한 차단이 가능하며 이용하기 쉽다는 장점이 있다. 반면, 일부 라우터를 제외하고는 Domain 단위의 차단이 불가하며, 차단 대상의

---

3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
5.「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
6의2. 이 법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보
6의3. 총포·화약류(생명·신체에 위해를 끼칠 수 있는 폭발력을 가진 물건을 포함한다)를 제조할 수 있는 방법이나 설계도 등의 정보
7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
8.「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

2) **제8조**(심의위원회의 심의대상 정보 등) ① 법 제21조제4호에서 "대통령령이 정하는 정보"란 정보통신망을 통하여 유통되는 정보 중「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제44조의7에 따른 불법정보 및 청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보를 말한다.
② 법 제21조제4호에 따른 시정요구의 종류는 다음 각 호와 같다.
1. 해당 정보의 삭제 또는 접속차단
2. 이용자에 대한 이용정지 또는 이용해지
3. 청소년유해정보의 표시의무 이행 또는 표시방법 변경 등과 그 밖에 필요하다고 인정하는 사항

증가 시 시스템 속도가 저하되고, 해당 웹 서버의 IP가 변경되었을 경우 지속적인 IP 변경이 없다면 유해하지 않은 사이트도 차단한다는 과잉 차단의 단점이 있다.[3)]

URL(Uniform Resource Locator)차단방식은 이용자가 불법사이트(불법.com/123.htm)에 접속하는 경우 DNS서버를 거쳐 서버 IP주소를 확인하고 불법 서버에 접속할 때, 통신사의 차단장비에서 암호화되지 않는 URL정보(불법.com/123.htm)와 차단목록(불법.com)을 기계적으로 비교하여, 불법사이트가 아닌 경우 정상적으로 연결하고, 일치하면 차단안내서버(warning.or.kr)로 연결하여 차단한다.

SNI(Server Name Indication)차단방식은 이용자가 불법사이트(불법.com)에 접속하는 경우 DNS서버를 거쳐 서버 IP주소를 확인하고 불법서버에 접속할 때, 통신사의 차단장비에서 통신연결 전에 암호화되지 않은 SNI의 '도메인정보(불법.com)'와 차단목록(불법.com)'을 기계적으로 비교하여 불법사이트가 아닌 경우 정상 연결하고, 일치하면 불법사이트(불법.com) 연결을 차단하는 방식이다.

3. 감청요건

감청이란 "전기통신에 대하여 당사자의 동의 없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것"을 말한다(통신비밀보호법 제2조제7호).

통신비밀보호법상 감청이 되기 위해서는 ① 당사자의 동의가 없을 것, ② 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것, ③ 감청이 실시간으로 송·수신하는 전기통신 또는 전기통신의 송·수신과 동시에 이루어지는 경우일 것 등의 요건을 충족하여야 한다.

①의 요건과 관련해서 불법사이트에 접속하기 위해서는 이용자가 먼저 통신사에게 불법사이트의 주소(도메인이름 또는 IP주소를 의미)를 요청하고 통신사가 주소를 회신하면, 이용자는 회신 받은 IP주소를 통해 불법사이트에 접속하게 된다. 그런데 통신사는 약관을 통해 불법사이트에 대한 방송통신심의위원회의 시정요구가 있는 경우 서비스의 전부 또는 일부에 대한 제한(여기서는 접속차단을 의미)에 대하여 이용자의 동의를 받고 있다고 볼 수 있다.

②의 요건과 관련해서 판례에 따르면, 전기신호 형태의 패킷(packet)을 중간에 확보하여 그 내용을 지득하는 경우를 감청으로 보고 있다(대법원 2012. 10. 11. 선고 2012도7455 판결). 패킷은 인터넷 서비스 연결을 위해 필요한 정보와 개인이 주고받는 정보로 구분할 수 있는데, SNI 차단방식은 인터넷 서비스 연결을 위해 필요한 SNI의 도메인 정보를 차단목록과 기계적으로 비교하는 방식이며, 개인이 주고받는 정보의 내용을 확인하는

3) 이향선 외4(2011),『건전한 미디어환경 조성을 위한 방송통신심의위원회 역할 제고 방안 연구』, 108-112면

것이 아니므로 그 내용을 지득하는 경우로 볼 수 없다고 할 것이다.

③의 요건과 관련해서 이 사건에서 SNI 방식에 의한 차단은 암호화된 패킷 교환 이전에 이용자가 상대방 기기(불법서버)와 사전에 정의된 정보를 상호 교환하는 단계에서 통신사가 차단목록과 비교하여 일치하면 불법사이트가 아닌 방송통신심의위원회의 경고 사이트에 접속하게 하는바, 이를 송수신하는 전기통신 또는 전기통신의 송수신과 동시에 이루어지는 경우로 본다면 ③의 요건을 충족한다고 볼 수 있다.

4. 소결

따라서 SNI 차단방식은 이용자와 불법서버 사이에 암호화된 통신을 수행하기 위해서 상대방 기기와 사전에 정의된 정보를 상호 교환하는 단계에서 이용자가 불법사이트에 접속을 시도하는 과정에서 통신사가 차단목록과 비교하고 일치하면 이용자의 불법사이트 접속을 차단하는 것이다. 이는 송·수신하는 전기통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득하는 경우로 볼 수 없다. 또한 실시간으로 송수신을 방해하는 행위에는 해당할 여지가 있다고 하더라도 사전에 방송통신심의위원회의 시정요구가 있는 경우 서비스 이용의 전부 또는 일부를 제한하는데 이용자의 동의가 있는 것이므로 통신비밀보호법상 감청의 요건을 충족하지 못하고 있다고 할 것이다.

Ⅲ. 음란물이 표현의 자유 보호대상인지 여부

1. 표현의 자유

헌법은 제21조제1항에서 "모든 국민은 언론·출판의 자유와 집회·결사의 자유의 자유를 가진다."고 규정하고 있고, 표현의 자유는 사상 또는 의견의 자유로운 표명을 하는 발표의 자유와 그것을 전파할 전달의 자유를 의미하는 것으로서, 개인이 인간으로서의 존엄과 가치를 유지하고 행복을 추구하며 국민주권을 실현하는 데 필수불가결한 것이고, 종교의 자유, 양심의 자유, 학문과 예술의 자유 등의 정신적인 자유를 외부적으로 표현하는 자유라고 판단하고 있으며(헌재 1989. 9. 4. 88헌마22, 헌재 1992. 11. 12. 89헌마88), 또한 표현의 자유의 내용으로서는 의사표현·전파의 자유, 정보의 자유, 신문의 자유 및 방송·방영의 자유 등이 있는데, 이러한 언론·출판의 자유의 내용 중 의사표현·전파의 자유에 있어서 의사표현 또는 전파의 매개체는 어떠한 형태이건 가능하며 그 제한이 없으므로, 담화·연설·토론·연극·방송·음악·영화·가요 등과 문서·소설·시가·도화·사진·조각·서화 등 모든 형상의 의사표현 또는 의사전파의 매개체를 포함한다고 판단하고 있다(헌재 1993. 5. 13. 91헌바17, 헌재 1996. 10. 4. 93헌가13등, 헌재 2001. 8. 30. 2000헌가9 등 참조).

기고

2. 음란물이 표현의 자유의 보호대상인지 여부

불법사이트에 대한 접속차단이 표현의 자유를 제한하는지 여부에 대해서는 먼저 불법정보가 표현의 자유의 보호대상인지 여부에 대한 판단이 이루어져야 하는데, 이에 대한 불법정보 중 음란물과 관련하여 표현의 자유의 보호대상인지 여부에 대한 헌법재판소의 결정이 변경되는 과정을 검토한다.

헌법재판소는 "이 사건 법률조항이 규율하는 음란 또는 저속한 표현 중 '음란'이란 인간존엄 내지 인간성을 왜곡하는 노골적이고 적나라한 성표현으로서 오로지 성적 흥미에만 호소할 뿐 전체적으로 보아 하등의 문학적, 예술적, 과학적 또는 정치적 가치를 지니지 않은 것으로서, 사회의 건전한 성도덕을 크게 해칠 뿐만 아니라 사상의 경쟁메커니즘에 의해서도 그 해악이 해소되기 어렵다고 하지 않을 수 없다. 따라서 이러한 엄격한 의미의 음란표현은 언론·출판의 자유에 의해서 보호되지 않는다고 할 것이다.(헌재 1998. 4. 30. 95헌가16)"라고 판시하여, '음란표현'은 헌법상 언론·출판 자유의 보호영역 밖에 있다고 판단한 바 있다.

그 후 헌법재판소는「청소년의 성보호에 관한 법률」제2조제3호 등 위헌제청 사건에서 "본 건에 있어서 문제되고 있는 '청소년이용음란물' 역시 의사형성적 작용을 하는 의사의 표현·전파의 형식 중 하나임이 분명하므로 언론·출판의 자유에 의하여 보호되는 의사표현의 매개체라는 점에는 의문의 여지가 없는바, 이 사건 법률 제2조제3호 및 제8조제1항은 이의 제작·수입·수출 행위를 처벌함으로써 위와 같은 의사표현의 매개체에 의한 일정한 내용의 표현을 금지하고 있다는 점에서 헌법상 보장되고 있는 표현의 자유, 즉 언론·출판의 자유를 제한하는 것으로 볼 수 있다."라고 판시하고, 이어서 "그러나, '청소년이용음란물'이 헌법상 표현의 자유에 의한 보호대상이 되고 따라서 그 제작 등의 행위에 대하여 형사상 중한 처벌을 가하는 것이 이러한 기본권을 다소 제한하게 되는 결과가 된다 하더라도, 이는 공공복리를 위하여 필요한 제한으로서 헌법 제37조 제2항의 비례의 원칙에 반하지 아니한다 할 것이다.(헌재 2002. 4. 25. 2001헌가27)"라고 판시하여, '음란표현'도 헌법상 언론·출판 자유의 보호영역 안에 있다고 판단한 바 있다.

헌법재판소는 "음란표현도 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역에는 해당하되, 다만 헌법 제37조 제2항에 따라 국가 안전보장·질서유지 또는 공공복리를 위하여 제한할 수 있는 것이라고 해석하여야 할 것이다. 결국 이 사건 법률조항의 음란표현은 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역 내에 있다고 볼 것인바, 종전에 이와 견해를 달리하여 음란표현은 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역에 해당하지 아니한다는 취지로 판시한 우리 재판소의 의견(헌재 1998. 4. 30. 95헌가16)은 이를 변경하기로 하며, 이하에서는 이를 전제로 하여 이 사건 법률조항의 위헌 여부를 심사하기로 한다."라고 판시하여 기존 판례를 변경한 바 있다.

기고

3. 소결

헌법재판소의 변경된 결정에 따르면, 음란표현도 헌법상 표현의 자유의 보호영역 안에 있다고 보아야 하므로 음란물 등과 같이 불법정보를 제공하는 불법사이트 차단의 경우 헌법상 표현의 자유를 제한하는 것으로 볼 수 있다. 다만, 헌법 제21조제4항은 "언론·출판은 타인의 명예나 권리 또는 공중도덕이나 사회윤리를 침해하여서는 아니된다."고 규정하고 있는 바, 이는 언론·출판의 자유에 따르는 책임과 의무를 강조하는 동시에 언론·출판의 자유에 대한 제한의 요건을 명시한 규정으로 볼 것이다.

따라서 음란표현도 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역에는 해당하되, 다만 헌법 제37조 제2항에 따라 국가 안전보장·질서유지 또는 공공복리를 위하여 제한할 수 있는 것이라고 해석하여야 한다. 그러므로 음란물사이트에 대한 차단은 헌법상 표현의 자유 제한에 해당하지만, 헌법 제37조제2항을 근거로 그 제한이 정당화된다고 할 것이다.

IV. 결론

음란표현의 헌법상 표현의 자유의 보호 영역 안에 있지만 헌법 제37조제2항의 국가 안전보장·질서유지·공공복리를 위한 제한이 가능하다. 따라서 이용자가 음란사이트에 접속하려는 경우 DNS차단방식, URL차단방식, SNI차단방식 등을 통해 차단(정보통신망법상 불법정보의 유통금지(제44조의7) 및 방통위설치법상 시정요구 중 한 유형으로서 접속차단(법 제21조제4호)하는 것은 헌법상 표현의 자유를 제한하는 것으로 볼 수 있다. 다만, 이러한 차단은 사전에 당사자 일방인 이용자가 약관을 통해 방송통신심의위원회의 시정요구 시 서비스 이용의 제한에 사전에 동의한 것으로 볼 수 있고 송·수신하는 전기통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득하는 경우로 볼 수 없어 통신비밀보호법상 감청에는 해당하지 않고 또한 헌법 제37조제2항의 국가 안전보장·질서유지·공공복리를 근거로 정당한 제한에 해당한다고 할 것이다.

※ **Reference**

1. 이향선 외4(2011), 『건전한 미디어환경 조성을 위한 방송통신심의위원회 역할 제고 방안 연구』, 방송통신심의위원회, 2011. 12.
2. 곽희양, 경향신문 기사(http://news.khan.co.kr/kh_news/khan_art_view.html?art_id=201903101547001)
3. 김시소, 전자신문 기사(https://news.v.daum.net/v/20180710113505633)
4. 김태진, ZD NetKorea 기사(https://www.zdnet.co.kr/view/?no=20190308192133)
5. 하선영, 중앙일보 기사(https://news.joins.com/article/23372607)

기고

자율주행과 개인정보 규제 패러다임의 혁신

이상직 법무법인(유한) 태평양 변호사

- (現) 개인정보보호법학회 부회장
- (現) 대한상사중재원 중재인
- (前) 주식회사 케이티 법무센터장
- (前) 정보통신부 통신위원회 사무국 과장

Ⅰ. 자율주행차의 개요 및 최근 동향

1. 개요

「자동차관리법」 제2조제1호 및 제1의3호,「자율주행자동차 상용화촉진 및 지원에 관한 법률」 제2조제1호에서 자동차는 "원동기에 의하여 육상에서 이동할 목적으로 제작한 용구 또는 이에 견인되어 육상을 이동할 목적으로 제작한 용구"이고, 자율주행자동차는 "운전자 또는 승객의 조작 없이 자동차 스스로 운행이 가능한 자동차"를 말한다.「자동차관리법 시행규칙」 제26조의2제3항에 따른 국토교통부의 「자율주행 자동차의 안전운행요건 및 시험운행 등에 관한 규정」 제2조제4호는 자율주행시스템에 관하여 정의하고 있는바, 운전자의 적극적인 제어 없이 주변상황 및 도로정보를 스스로 인지하고 판단하여 자동차의 가·감속, 제동 또는 조향장치를 제어하는 기능 및 장치로 보고 있다.

자율주행자동차는 일반차량과 달라 「자동차관리법」상 등록을 할 수 없다. 다만,「자동차관리법」 제27조제1항 단서에서는 자동차를 등록하지 아니하고 일시 운행을 하려는 자는 대통령령으로 정하는 바에 따라 국토교통부장관 또는 시·도지사의 임시운행허가를 받아야 한다고 규정하되, 자율주행자동차를 시험·연구 목적으로 운행하려는 자는 허가대상, 고장감지 및 경고장치, 기능해제장치, 운행구역, 운전자 준수사항 등과 관련하여 국토교통부령으로 정하는 안전운행요건을 갖추어 국토교통부장관의 임시운행허가를 받아야 한다고 규정하고 있다. 따라서 자율주행자동차를 시험 연구 목적으로 운행하려면 임시운행허가를 받아야 한다.

자율주행차는 기존의 자동차 기술과 함께 인공지능, 빅데이터, 딥러닝, 사물인터넷, 5G 통신망 등 IT가 유기적으로 연계되며 발전되는 산업군과 기술 분야이다.

2. 최근 동향

우리 정부는 2018년6월에 혁신성장동력 추진현황 및 계획을 통해 2020년까지 고속도로 내 자율주행차 상용화(레벨3)와 2030년 완전 자율주행 상용화 로드맵을 발표했다. 규제샌드박스를 도입하고 자율주행차 분야 선제적 규제혁파 로드맵을 통해 2020년까지 운전자 범위에 자율주행시스템을 포함하고 2026년 이후에는 자율주행차 전용 면허를 신설하기로 했다. 자동차, IT기업, 대학 연구진들은 자율주행차 기술개발에 적극 나서고 있고, 경기 화성시에는 자율주행 실증도시 K시티를 만들기도 했다.

보스턴컨설팅그룹은 글로벌 자율주행차 시장규모가 2025년에 약 420억달러(약 50조원)에 이르고, 2035년이 되면 770억 달러(약 90조원) 규모로 성장할 것이라고 한다. 2035년에는 세계 자동차 판매량의 25%는 자율주행차가 차지할 것이고 완전한 자율주행기능를 갖춘 차는 1,200만대, 부분적으로 자율주행기능을 갖춘 차는 1,800만대에 이를 것이라고 전망했다. 미국의 시장조사업체 Navigant Research는 자율주행차 비중이 2025년 4.4%에서 2030년 40.5%, 2035년 75%로 확대되어 연간 8,500만대에 이를 것으로 예상한다.

테슬라, 구글 등 자율주행에 관하여 높은 기술력을 갖춘 기업들이 있는 미국은 2016년 이후부터 자율주행차의 안전과 보안을 위한 지침과 산업 연구를 촉진하기 위한 자율주행 법률을 제안하고 있다. 이들 법령은 사이버보안, 시스템안전, 비상대처, 기술중립성, 사생활보호 등에 관한 사항을 포함하고 있다.

독일은 2017년 자율주행차 기술의 고도화와 일반 도로에서의 허용을 위해 도로교통법을 개정하여 운전자가 비상상황이 발생한 경우에 적시에 차량에 대한 통제를 할 수 있도록 경고시스템을 갖추는 것을 전제로 자율주행을 허용하고 있다.

일본은 2019년 자율주행차의 일반도로 주행을 위한 도로교통법 개정안, 도로운송차량법 개정안을 준비하고 있고, 빠르면 2020년부터 시행할 것을 목표로 하고 있다.

우리나라는 자율주행 인프라 구축, 교통체계 개선, 안전구간 및 시범운행지구 설치 등을 담은 「자율주행자동차 상용화촉진 및 지원에 관한 법률」을 제정하였다(2019.4.30. 제정, 2020.5.1.시행).

Ⅱ. 자율주행과 개인정보

1. 자율주행 등 제4차 산업혁명과 개인정보의 관계

우리나라는 헌법 제17조에서 사생활의 비밀과 자유를 침해받지 않는 권리를 규정하면서 대법원판례로 위 헌법 제17조와 인간의 존엄과 가치, 행복추구권을 규정한

기고

헌법 제10조를 근거로 개인정보자기결정권을 인정하고 있다. 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 정보주체가 스스로 결정할 수 있는 권리이다(대법원 2016.8.17.선고 2014다235080판결).

제4차 산업혁명은 자율주행, 인공지능 등 첨단 정보통신기술이 단순한 기술혁신에 그치지 않고, 정치・경제・사회・문화 인프라 전반에 '구조적인 변화'까지 야기하는 것을 의미한다. 기존의 산업혁명은 기계의 도입, 제조공정에서의 자동화시스템 등으로 좋은 제품을 저렴한 가격에 공급할 수 있게까지는 했지만, 고객의 속마음, 니즈(needs)를 정확히 예측하는 것은 그다지 성공적이지 못했다. 그 결과 초과생산에 따른 재고가 발생하고, 잘 팔리지 않거나 수요량 예측을 넘어서는 상품, 서비스에 대한 과소비를 부추기면서 허위 과장 광고의 홍수, 소비자 불만의 폭증, 인플레이션 등이 발생하였다.

이에 대해 자율주행 등 4차 산업혁명은 고객의 니즈를 인공지능, IoT센서, 온라인이나 SNS 등을 통해 수집하고, 이를 해석, 정확한 결과를 내놓을 가능성이 매우 높아졌고, 수집된 데이터를 빅데이터로 묶어 분석함에 있어서도 인공지능을 사용하고, 제품과 서비스를 개발함에 있어서도 인공지능・로봇・3D프린터 등을 이용하며, 유통에 무인항공, 자율주행차량 등을 사용할 수 있게 됨에 따라 고객이 언제 어디서나 원하는 방식과 절차에 따라 원하는 상품이나 서비스를 만날 수 있게 하였다.

그 결과 개인정보의 수집・이용, 제3자 제공 등 일련의 프로세스에서 정보주체가 개인정보의 흐름 등을 기술적으로 이해하기 어려울 뿐 아니라 개인정보의 활용가치가 더욱 증가함에 따라 개인정보에 대한 위협은 증가하고 있는 상황이다.

그러나 자율주행 등 제4차 산업혁명의 기술적 발전은 개인정보에 대한 침해 위협을 높이는 반면에 그 기술을 잘 개발하고 활용하면 정보주체의 개인정보자기결정권을 보호하는 수단으로서도 작동할 수 있을 것이다. 예를 들면, 블록체인기술의 도입은 개인정보의 흐름을 정보주체도 낱낱이 확인할 수 있는 기회를 제공할 수 있고, 인공지능 기기는 개인정보가 과다하게 수집한 것이 없는지, 부당하게 이용되는 것이 없는지, 동의 없이 제3자에게 이전되는 것은 없는지 확인하는 작업을 대행할 수 있고, 동의해야 할 사항과 그렇지 않은 사항을 분류하여 의사결정을 지원하는 기능도 수행할 수 있을 것이다.

2. 자율주행과 개인정보 패러다임의 변화

자율주행, 인공지능 등으로 대표되는 지능정보사회의 특성에 따라 개인정보처리자의 대량, 신속, 자동화된 정보처리, 계약관계를 전제로 하지 않는 비거래관계에서의 정보수집 등이 빈발할 것으로 예상된다. 그렇다면 기존에 중점을 두어왔던 개인정보 침해행위에 대한 예방이나 제재를 넘어 정보주체가 스스로 자신을 보호할 수 있는 환경을 어떻게

만들 것인지가 매우 중요하다. 자신의 개인정보를 보호할 수 있는 여건을 갖춘 정보주체와 그렇지 않은 정보주체 간에 발생하는 다양한 격차와 소외 문제를 어떻게 할 것인지도 살펴야 한다.

현재 개인정보 수집·이용 등에 관한 규제는 동의기반 방식(정보주체의 동의를 얻어 개인정보 수집 이용 등의 적법성을 확보하는 방식), 법령기반 방식(정보주체의 동의가 없더라도 개인정보 수집 이용을 허용하는 법령의 규정에 의하여 그 적법성을 확보하는 방식)이 있다.

기존의 동의기반 방식은 개인정보 수집·이용·활용, 제3자 제공 등에서 계약 등 거래관계에 있거나 거래관계에 임박 또는 거래관계가 종료된 정보주체의 동의를 얻는 것을 원칙으로 하고, 예외로 법령이나 개인정보처리자의 정당한 이익, 계약의 체결과 이행을 위한 경우에 동의를 얻지 않아도 되도록 하고 있다.

그러나 개인정보처리자는 자율주행을 함에 있어서 직접 자율주행에서 맞닥뜨리거나 지능형교통시스템에서 제공받는 다양하고 많은 정보를 통해 원활하고 안전한 교통상황과 체계를 유지할 수밖에 없는 바, 계약 등 거래관계 보다는 비거래관계에서 개인정보의 수집 이용 제공이 일어날 수밖에 없다. 또한 정보주체도 자율주행차에 탑승한 자이거나 보행자 또는 인근 건물에 있는 자인지에 관계없이 자신과 교통의 안전을 위하여 자신이 보유한 자율주행차 또는 개인휴대 단말과 주위에 연결된 네트워크 등 인프라를 통하여 주위의 정보를 수집할 수 있고, 그 정보는 개인정보도 당연히 포함할 것이다. 결국 어느 정도 정착된 자율주행의 시대에는 정보주체가 곧 개인정보처리자인 상황으로 흘러갈 것이다. 물론, 완전한 자율주행이 한순간에 오는 것이 아니고 단계별로 순차적으로 오며, 그 일부는 몇 개의 중복된 단계에 있을 수도 있으므로 합리적인 법령과 그에 따른 합리적인 해석이 요구될 수밖에 없다.

이와 같은 상황의 도래는 기존의 개인정보 규제체계의 전반적 혁신을 요구하게 될 것이고, 이러한 단계에서 개인정보를 어떻게 보호하는 것이 가장 효과적인지에 관한 관심을 높이고 있다. 이와 관련하여 유럽 GDPR에서 도입된 Data protection by design을 잘 구현하는 것이 해결책의 하나가 아니겠냐는 의견도 등장하고 있다. 즉, 개인정보처리자가 개인정보를 보호하기 위한 합리적 설계(reasonable design for protecting personal data)를 갖추어 정비하고 신뢰성 있는 기관의 인증, 승인 등의 확인을 받는다면 자율주행 같은 사업을 하면서 개인정보를 수집할 수 있는 자격을 주는 등의 방안이다. 물론, 그 자체가 개인정보 침해를 가져오는 행위에 대하여 면책을 주는 것은 아니다.

3. 자율주행과 개인정보의 세부 이슈

(1) 자율주행에서 수집되는 개인정보

자율주행차는 GPS, 센서, 카메라, 정밀지도기술, V2X 통신기술 등을 이용하여 차선, 횡단보도 인식기능, 충돌위험 감지기능을 수행하고, 도로에 눈이 오거나 폭우가 오는 경우, 도로에 장애물이 떨어져 있는 경우, 사고차량이 있는 경우 등 도로 관련 정보를 직접 또는 지능교통시스템, 도로교통 관련 인프라 등 제3의 기관, 다른 차량을 통하여 제공받고 제공하기도 한다. 이를 통해 수집되는 데이터에는 당연히 개인정보도 포함되는바, 위치정보, 영상정보, 보행자 등 신체의 외형이나 특징, 동반자, 행태정보, 자동차번호 등 다양하고 그 수도 많다.

(2) 자율주행과 정보주체의 특정

자율주행에서의 정보주체는 자율주행차의 사용자, 보행자, 다른 차량의 사용자 등 자율주행차 또는 자율주행시스템에 의하여 수집되거나 이용되는 개인정보의 주체이다. 다만, 앞서 본 바와 같이 정보주체는 자신의 안전이나 업무를 위하여 직접 또는 제3기관이나 업체의 지원을 받아 교통상황에서의 다른 정보 등을 수집 이용하는 경우에는 개인정보처리자의 지위를 함께 가질 수도 있다.

(3) 자율주행과 개인정보처리자의 특정

교통상황 또는 운행상황에 따라 차량 제조사를 개인정보처리자로 볼 것인지, 차량 소유자 또는 탑승자를 개인정보처리자로 볼 것인지 특정할 필요가 있다. 자율주행차가 사용할 운영체계, 시스템을 누가 지배하고 주도하는지도 중요한바, 이에 따라 자동차 제조사 또는 정보통신서비스 제공자가 개인정보처리자가 될 것으로 보인다.

제조사는 차량을 제조하여 공급하는 것에 그치지 않고 차량 운행을 위하여 필요한 정보를 수집하고 그 정보에 개인정보가 포함되어 있다면 업무목적의 개인정보처리자에 해당할 수 있다.

통신망에 연결된 자율주행차의 경우에는 플랫폼운영자, 정보통신서비스제공자도 개인정보처리자의 지위에 놓이게 될 수 있다. V2X 통신 단계에 이르러서는 자율주행차 제조사, 자율주행차와 의사소통을 하는데 핵심적인 통제기능, 관리 역할을 하는 지능형교통시스템을 운영하는 자가 단독 또는 공동으로 개인정보처리자가 될 수도 있다.

(4) 자율주행과 개인정보 수집・이용, 목적외 사용 또는 제3자 제공 동의

자율주행에서는 계약 등 거래관계가 없는 다른 차량의 운전자나 보행자로부터 개인정보의 수집에 동의를 받기가 매우 어렵고, 차량운행에서 부지불식간에 이루어지는 레이더, 센서 등에 의한 정보 수집이 불가피하므로 현행 개인정보보호법의 개인정보의 수집・이용, 제공의 동의기반 원칙을 유지하기 어렵다.

구체적으로 보면, 자율주행이 고도화되면 특정한 도로와 운행 환경에서 차량의 모든

기능을 자동적으로 제어할 수 있는데, 자동화된 방식으로 다른 차량의 위치정보 등을 수집하여 처리하여야 한다. 이는 자동차 소유자와 사용자가 스스로 입력한 정보, 카메라, 레이더, 센서 등을 통해 수집된 정보를 분석하는 작업이 우선되어야 한다. 초기에는 자율주행차가 직접 수집하기도 하겠지만, 점진적으로는 지능형교통시스템 등 외부에서 수집된 정보를 제공받아 결합하여 이용할 수도 있다.

횡단보도나 인도에서 보행자를 인식하고 피하거나 주의를 기울이는 것도 중요하다. 자율주행차는 도로나 인도상의 신호, 표식 등을 여러 개의 카메라와 센서 등으로 인식하고 적정한 거리 간격에 보행자가 있으면 정지하고 보행자가 없으면 다시 출발한다. 이러한 정보는 차선만을 확인하는 것이 아니라 교통 지도의 정밀도를 높이는 일에 이용되기도 하고, 그 과정에서 보행자 등의 정보가 수집・이용, 전송될 수 있다.

위와 같은 사항을 고려한다면, 자율주행차 사용자 또는 지능형교통시스템 운영자가 보행자 정보를 수집하는데 보행자의 개별 동의를 받는 것은 불가능하다. 비거래관계의 정보수집도 많을 것이므로 계약의 이행을 위한 경우나 개인정보처리자의 정당한 이익을 위한 경우로 예외를 인정받기도 쉽지 않다.

궁극적으로 자율주행 등의 경우에 법령으로 개인정보 수집・이용 등의 예외를 인정하거나 합리적 설계방식 기반의 개인정보 보호 제도를 도입해야 할 것이다. 이와 더불어 보행자에 대한 경고 기능을 활성화하는 것도 필요하다. 예를 들면, 차량의 외부에 적절한 표시를 통해 자율주행차로 각종 교통 관련 정보를 수집하고 있음을 알 수 있도록 하고 인근에 자율주행차가 다닌다는 표식을 설치하는 등의 방법, 통신단말 등을 통해 실시간으로 자율주행 현황을 안내 공지하는 방법 등으로 보행자가 자신의 정보가 최소한으로 수집되도록 다양한 조치를 할 수 있는 기회를 주는 것이다.

자율주행차와 다른 차량에서 수집된 정보 등을 네트워크를 통하여 지능형교통시스템에 보내거나 제3자의 서비스를 자율주행차 등의 탑승자 등에 제공하기 위하여 개인정보를 제3자에게 제공해야 하는 경우가 있다.

자율주행차 제조사 또는 제3의 업체가 자율주행차의 수집・이용 정보를 제공받아 직접 또는 제3업체를 통해 콘텐츠 등 미디어 서비스, 원격 제어, 차량 관리, 길안내, 친구찾기, 맛집 안내 등 다양한 서비스를 제공할 수 있게 된다. 차량에서 멀리 떨어진 곳에서도 스마트폰 등 제어 단말기를 통해 통신망으로 연결하여 에어컨 등 차내 설비의 기능 제어, 주차위치 확인, 차문 잠그기 등을 할 수 있게 한다. 실시간으로 수집되는 교통 상황 정보와 예측 교통 정보를 이용하여 정체구간을 피할 수 있도록 해줄 수도 있다. 자율주행 중에 다양한 미디어 콘텐츠를 제공하거나 회사 업무에 필요한 소프트웨어 등이나 자료 등을 클라우드에서 다운로드할 수 있는 서비스를 제공할 수도 있을 것이다. 차량공유플랫폼을 통하여 자율주행차가 이용되는 경우에는 자율주행차가 스스로 이동하여 약속 장소에 대기하고 최적의 경로 고객들에게 운송서비스가 제공될 것인 바,

이를 위하여 자율주행차의 정보 등이 차량공유플랫폼이나 해당 플랫폼의 이용자에게 제공될 수 있다. 이 경우 현행 개인정보보호 관계법령에 의하면 제3자 제공 또는 목적외 이용 등에 대한 동의가 필요할 것인데, 신속한 정보수집과 그 분석을 통해 자율주행의 편의 증진과 안전을 도모해야 하는 특성상 그렇게 하는 것이 그 시대에 바람직한지는 고민이 필요하다.

Ⅲ. 결론

앞서 본 바와 같이 자율주행 시대에서는 개인정보 수집·이용을 더 이상 동의기반 방식에 의존하기 어렵다. 정보주체가 자신의 자율주행이나 안전한 보행을 위하여 자율주행차나 주위 인프라의 정보를 다운로드할 수 있고, 정보주체가 개인정보처리자가 되거나 개인정보처리자 처럼 정보를 수집·이용하게 되기도 한다.

개인정보의 수집 이용 제3자 제공이 빅데이터 분석 가공을 통하여 더욱 풍요로운 시대를 가져올 수 있다는 점도 고려되어야 한다.

그렇다면, 동의기반 방식, 법령기반 방식 외에 정보주체의 개인정보자기결정권의 필요충분한 행사를 조건으로 합리적 설계 방식의 개인정보 수집·이용 등도 허용할 필요가 있다. 그를 통한 경제성장이나 해당 자율주행 기업의 발전에 정보주체의 기여가 있는 만큼 정보주체가 인공지능, 블록체인기술 등 다양한 기술을 저렴하게 이용하여 자신의 개인정보를 지킬 수 있는 법제도 정책적 환경을 제공하고, 자율주행 등 개인정보 처리자가 이를 용인하거나 그 비용의 일정 부분을 부담하게 하는 것도 필요할 것으로 보인다. 나아가 개인정보가 산업발전에 활용된 점을 고려하여 정보주체에게 적절한 보상을 하는 것도 생각해 볼 수 있다.

※ **Reference**

1. 이백진 등, 첨단인프라 기술발전과 국토교통 분야의 과제: 자율주행 자동차를 중심으로, 국토연구원, 2016
2. 박준환, 자율주행자동차 관련 국내외 입법 정책 동향과 과제, 국회입법조사처, 2017
3. 강성준, 김민지, 자율주행자동차 활성화를 위한 법제개선방안 및 입법(안) 제안, 한국과학기술기획평가원, 2017
4. 이중기 외, 홍익대 산학협력단, 자율주행차의 개인정보 보호체계 및 규제방식에 관한 연구, 개인정보보호위원회, 2017

인터넷 법제동향
Vol. 142 (July 2019)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

| 발 행 처 | 한국인터넷진흥원
(58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원
Tel. 1544-5118
| 기획・편집 | 법제연구팀
| 발간・배포 | www.kisa.or.kr