Vol. 146 (November 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	박인숙의원 (2019. 11. 11.)	- 광고성 정보를 전송할 때 사전 동의를 받도록 하는 시간의 범위를 확대하고, 광고성 정보 수신동의 여부 확인 주기를 1년으로 단축함
	김광수의원 (2019. 11. 15.)	- 「전자상거래 등에서의 소비자보호에 관한 법률」을 개정하여 국외 통신판매업자가 위반행위를 반복하는 경우 공정거래위원회가 방송통신위원회에 요청하여 정보의 처리를 거부·정지 또는 제한 명령을 할 수 있도록 함
	박광온의원 (2019. 11. 15.)	- 이용자가 불법정보에 대해 임시차단등을 요청할 수 있고, 정보게재자의 이의신청이 없을 경우 삭제할 수 있음 - 대통령령 기준에 해당하는 정보통신서비스 제공자는 불법정보의 유통 방지를 위한 담당자를 두고, 불법정보의 임시차단 및 유통 방지 업무를 하도록 함
	박광온의원 (2019. 11. 18.)	- 이용자가 정보통신서비스 제공자 또는 다른 이용자의 위반행위로 손해를 입은 경우 손해배상을 청구할 수 있도록 함
	송희경의원 (2019. 11. 20.)	- 검색유인행위를 하는 것을 금지하고, 정보통신서비스 제공자로 하여금 의무적으로 검색유인행위를 방지하기 위한 조치를 하도록 함
	박광온의원 (2019. 11. 20.)	- 개인정보 처리자가 이용자의 개인정보에 접근할 경우 컴퓨터를 통한 인증 외에 보안성이 강화된 방식을 통하여 본인 여부를 확인받도록 함
	박대출의원 (2019. 11. 29.)	- 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급을 포함하도록 함
• 「국가정보화 기본법」 일부개정법률안(대안)	과학기술정보방송통신위원장 (2019. 11. 18.)	- 정보통신망을 통한 정보·서비스를 제공할 때 유·무선 정보통신에 대한 장애인·고령자 등의 접근성을 보장함
• 「민법」 일부개정법률안	김세연의원 (2019. 11. 18.)	- 데이터를 물건의 정의에 포섭되도록 개정하고, 데이터 계약을 민법상 전형계약으로 인정하는 규정을 신설
• 「인공지능산업 진흥에 관한 법률안」 제정안	김경진의원 (2019. 11. 21.)	- 과학기술정보통신부장관은 인공지능 기술 촉진에 필요한 전문인력의 양성과 자질 향상을 위해 교육 및 훈련을 실시하고, 예산을 지원 - 국내외 인공지능 기술 집약기업을 유치하거나 육성하기 위하여 인공지능 거점지구를 조성하도록 함
• 「정보통신기반 보호법」 일부개정법률안(대안)	과학기술정보방송통신위원장 (2019. 11. 18.)	- 주요정보통신기반시설의 보호를 위하여 필요한 경우와 주요정보통신기반시설에 취약점 분석·평가가 필요한 경우 소관 분야의 주요정보통신기반시설 관리기관의 장에게 평가를 명할 수 있음

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(박인숙의원 대표발의, 2019. 11. 11. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 누구든지 전자적 전송매체를 이용하여 영리목적의 광고성 정보를 전송하려면 그 수신자의 명시적인 사전 동의를 받도록 하고 있으며, 특히 오후 9시부터 그 다음 날 오전 8시까지의 시간에 광고성 정보를 전송하려면 추가적으로 별도의 사전 동의를 받도록 하고 있음

o 그런데 현행법에서 광고성 정보를 전송할 때 별도의 사전 동의를 받도록 하고 있는 오후 9시부터 그 다음 날 오전 8시까지의 시간은 그 범위가 지나치게 좁아 국민의 쉴 권리를 충분히 보장하지 못하고 있다는 지적이 있음

o 현행법은 광고성 정보 전송에 대한 사전 동의를 받은 자는 정기적으로 광고성 정보 수신동의 여부를 확인하도록 하고 있으며, 시행령은 그 주기를 2년으로 정하고 있음

o 그러나 수신자의 권리 보호를 위하여 그 주기를 2년에서 1년으로 단축하고, 그 내용을 법률에서 명시적으로 규정할 필요가 있음

▶ 주요내용

o 광고성 정보를 전송할 때 별도의 사전 동의를 받도록 하는 시간의 범위를 오후 6시부터 그 다음 날 오전 9시까지로 확대하는 한편, 광고성 정보 수신동의 여부를 확인하여야 하는 주기를 1년으로 단축하고 그 내용을 법률에 상향하여 규정(안 제50조)

※ **Reference**

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안
(김광수의원 대표발의, 2019. 11. 15. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 최근 온라인여행사 등 국외 통신판매업자의 인터넷 홈페이지를 통하여 숙박·항공권 등을 예약하는 것이 일상화되고 있으나, 국외 통신판매업자와 계약을 한 경우 청약철회·환불 등이 인정되지 않는 사례가 발생하고 있어 소비자 보호를 위하여 이에 대한 규제를 강화할 필요가 있음

▶ 주요내용

o 「전자상거래 등에서의 소비자보호에 관한 법률」을 개정하여 국외 통신판매업자가 위반행위를 반복하는 경우 공정거래위원회가 방송통신위원회로 하여금 해당 국외 통신판매업자가 운영하는 사이버몰에 관한 정보의 처리를 거부·정지 또는 제한하도록 정보통신서비스 제공자 또는 게시판 관리·운영자에게 명령할 것을 요청하도록 하면서, 요청을 받은 방송통신위원회가 해당 정보의 처리를 거부·정지 또는 제한 명령을 할 수 있도록 함으로써 전자상거래를 이용하는 소비자를 보호하려는 것임(안 제44조의9 신설 등)

※ 이 법률안은 김광수의원이 대표발의한 「전자상거래 등에서의 소비자보호에 관한 법률」(의안번호 제2211 9호)의 의결을 전제로 하는 것이므로 같은 법률안이 의결되지 아니하거나 수정의결 되는 경우에는 이에 맞추어 조정되어야 할 것임

※ **Reference**

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(박광온의원 대표발의, 2019. 11. 15. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 정보통신망의 불법정보에 대해 이용자의 삭제 요청 등 정보통신망에서의 이용자 보호방안을 두고 있으나, 불법정보로 인한 이용자의 피해구제 등이 용이하지 않아 정보통신망으로 인한 이용자의 피해 문제가 계속하여 지적되고 있음

o 이에 불법정보에 대한 임시차단 등 요청 범위 확대, 정보통신서비스 제공자의 불법정보 유통방지 담당자 배치, 불법정보와 관련된 당사자 간 분쟁의 조정을 위한 온라인분쟁조정위원회 설치 등 불법정보로 인한 이용자의 피해를 신속하게 구제하기 위한 제도적 절차를 마련하고 정보통신서비스 제공자의 관리책임을 명확히 규정하는 등 제도적 미비점을 개선하여 정보통신망에서의 이용자의 권익 보호를 강화하려는 것임

▶ 주요내용

o 국외에서 이루어진 행위라도 국내 시장 또는 이용자에게 영향을 미치는 경우에는 이 법을 적용하도록 함(안 제5조의2 신설)

o 이용자가 불법정보에 대해 임시차단등을 요청할 수 있도록 하고, 해당 정보게재자의 이의신청이 없을 경우 해당 불법정보를 삭제할 수 있도록 하며, 이의신청이 있을 경우 온라인분쟁조정위원회의 조정 및 절차와 그 조정 결과를 따르도록 함(안 제44조의2)

o 정보통신서비스 제공자로 하여금 프로그램, 인공지능 등을 사용하여 불법정보의 유통을 방지하기 위한 기술적·관리적 조치를 하도록 함(안 제44조의7제5항 및 제6항 신설)

o 정보통신서비스 제공자 중 일일 평균 이용자의 수, 매출액 등이 대통령령으로 정하는 기준에 해당하는 자는 불법정보의 유통을 방지하기 위한 담당자(이하 "불법정보 유통방지 담당자" 라 함)를 두고, 불법 정보의 임시차단 및 불법정보의 유통방지 업무를 담당하도록 함(안 제44조의9 신설)

※ **Reference**

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(박광온의원 대표발의, 2019. 11. 18. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 정보통신망에서 불법정보를 유통하는 것을 금지하고, 정보통신망에 유통되는 정보로 권리를 침해받은 경우 정보통신서비스 제공자에게 삭제등을 요청할 수 있도록 하는 등 정보통신망에서의 다양한 이용자 보호방안을 마련하고 있음

o 그런데 정보통신서비스 제공자 또는 이용자의 위법행위로 인해 이용자가 입는 손해는 큰 반면, 이에 대한 제재수단 마련이 미흡하여 이용자의 손해에 대한 구제가 제대로 이루어지지 않고 있으며, 그 손해를 입증하여 손해배상을 받기도 어려운 상황임

▶ 주요내용

o 이용자가 정보통신서비스 제공자 또는 다른 이용자의 위반행위로 손해를 입은 경우 손해배상을 청구할 수 있도록 하면서, 그 손해를 입힌 자가 고의·과실이 없음을 입증하도록 하는 한편, 고의 또는 중대한 과실로 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보를 유통하여 손해가 발생한 경우 그 손해액의 3배를 넘지 않는 범위 내에서 손해배상을 하도록 하는 징벌적 손해배상제도를 도입하여 정보통신망에서의 책임성을 강화하려는 것임(안 제44조의11 신설)

※ **Reference**

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(송희경의원 대표발의, 2019. 11. 20. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 최근 여론에 영향을 미칠 목적으로 또는 사생활 침해나 명예 훼손 등 타인의 권리를 침해할 목적으로 특정 검색어의 검색을 유인하는 내용의 정보를 게재하는 행위(이하 "검색유인행위"라 함)가 빈번하게 일어나고 있음

o 정보통신망에서 일어나는 이러한 검색유인행위로 인하여 정보통신망이 특정 집단의 의사를 관철하고 여론을 조작하는 장(場)으로 변질되고 있어 이에 대한 제재가 필요하다는 지적이 제기됨

▶ 주요내용

o 검색유인행위를 하는 것을 금지하는 한편, 정보통신서비스 제공자로 하여금 의무적으로 검색유인행위를 방지하기 위한 조치를 하도록 하려는 것임(안 제44조의9 신설 등)

※ **Reference**

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(박광온의원 대표발의, 2019. 11. 20. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 정보통신서비스 제공자등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위해 기술적·관리적 조치를 하도록 하고 있음

o 그런데 정보통신망을 통해 처리되는 개인정보가 증가함에 따라 개인정보처리자의 고의나 과실에 의한 유출사고가 지속적으로 발생하고 있으며, 최근에는 APT 공격(지능형 지속 공격)으로 개인정보처리자의 컴퓨터가 악성코드에 감염되어 개인정보가 유출되는 사례도 증가하고 있어 개인정보처리자에 대한 관리가 강화될 필요가 있음

▶ 주요내용

o 개인정보를 처리하는 자가 이용자의 개인정보에 접근할 경우 컴퓨터를 통한 인증 외에 보안성이 강화된 서로 다른 경로의 인증 방식을 통하여 본인 여부를 확인받도록 하고, 개인정보 접근에 대하여 실시간으로 승인을 받도록 하여 이용자의 개인정보를 두텁게 보호하려는 것임(안 제28조제1항제3호의2 신설)

※ **Reference**

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(박대출의원 대표발의, 2019. 11. 29. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 최근 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 딥페이크(Deep Fake) 정보가 인터넷에 유통되는 사례가 늘어나고 있음

o 그런데 딥페이크 정보가 정교할수록 이용자가 해당 정보의 거짓 여부를 판별하기 어려워 이를 식별할 수 있는 기술을 개발·보급하는 것이 시급함

▶ 주요내용

o 과학기술정보통신부장관 또는 방송통신위원회가 마련하는 시책에 정보통신망을 통하여 유통되는 정보 중 인공지능 기술을 이용하여 만든 거짓의 음향·화상 또는 영상 등의 정보를 식별하는 기술의 개발·보급을 포함하도록 함으로써 건전한 정보통신망 이용환경을 조성하려는 것임(안 제4조제2항제7호의2 신설)

※ **Reference**

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

「국가정보화 기본법」 일부개정법률안(대안)

(과학기술정보방송통신위원장 발의, 2019. 11. 18. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 4차산업혁명에 따른 변화에 대응하기 위하여 정보화 선도사업의 내용에 정보통신 신기술의 활용 촉진을 명시적으로 규정하고, 정보화 선도사업의 추진 및 확산을 위하여 정보화 선도사업 거점지구의 지정 등에 관한 근거를 마련하려는 것임

o 아울러 국가기관등이 정보통신망을 통하여 제공하는 정보나 서비스에 대한 장애인·고령자 등의 접근성을 확대하여 보장하도록 하려는 것임

▶ 주요내용

o 정보화 선도사업의 내용에 정보통신 신기술의 활용 촉진을 명시적으로 규정함(안 제23조의2)

o 정보화 선도사업 거점지구의 지정 등에 관한 근거를 마련함(안 제23조3 신설)

o 국가기관등이 정보통신망을 통하여 정보나 서비스를 제공할 때 대통령령으로 정하는 유·무선 정보통신에 대한 장애인·고령자 등의 접근성을 보장하도록 함(안 제32조)

※ **Reference**

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

「민법」 일부개정법률안
(김세연의원 대표발의, 2019. 11. 18. 제안)

▶ **소관 상임위원회 : 법제사법위원회**

▶ **제안이유**

o 4차 산업혁명 시대의 도래와 정보기술의 발달에 따라 개인정보 등 데이터는 21세기 유전이라 불리며 새로운 핵심 자원으로 여겨지고 있음. AI 등 지능화 산업의 확대로 데이터는 제품・서비스・프로세스를 지원하는 보조재가 아닌 그 자체로서의 경제적 가치를 가지는 중요한 자산이 되었음

o 따라서 사회 변화 흐름에 따라 민법상 물건의 정의 규정에 대하여 수정 및 확대해석은 필수불가결한 부분이며 데이터 경제 사회를 만들기 위해서는 이에 대한 법률이 마련될 필요가 있음

o 현행법은 소유권의 대상을 유체물 및 전기 기타 관리할 수 있는 자연력으로 규정하고 있어서 새로운 데이터 경제 시대의 핵심이라고 할 수 있는 데이터에 대하여는 보호가 어려운 면이 있으나 모든 데이터에 대하여 일반적・전면적으로 소유권을 인정하는 것은 다른 권리와의 관계나 다양한 이해관계자의 이익의 균형에 해가 될 수도 있음

o 따라서 소유권의 성질에 부합하는 경우에는 데이터에 대해서도 소유권을 인정할 수 있도록 최소한의 여지를 만들 필요가 있음

▶ **주요내용**

o 데이터를 물건의 정의에 포섭될 수 있도록 개정하고, 데이터 계약을 민법상 전형계약으로 인정하는 규정을 신설하고자 하는 것임(안 제98조, 제674조의10부터 제674조의15까지)

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

「인공지능산업 진흥에 관한 법률안」 제정안
(김경진의원 대표발의, 2019. 11. 21. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 4차 산업혁명시대에 인공지능은 IoT, 빅데이터, 자율주행차 등과 함께 높은 관심을 바탕으로 세계 각국의 인공지능 산업에 대한 대규모 투자를 체계적으로 진행하고 있으며 인공지능 활용 촉진 정책들을 담은 법률을 제정하고 있음

o 우리나라는 인공지능 산업의 중요성은 인지하고 있으나 이에 대한 체계적이고 효율적인 지원 제도를 갖추지 못하고 개별 부처나 사업별로 분산적으로 추진됨에 따라 제도적 개선이 필요하다는 지적이 제기되고 있기에 글로벌 시장에서 인공지능 산업의 경쟁력을 제고하고, 국가경제의 발전과 국민의 삶의 질을 향상 및 인공지능산업의 법적 기반을 마련하려는 것임

▶ 주요내용

o 과학기술정보통신부장관은 인공지능 기술개발의 촉진을 위해 기술수준 조사, 기술의 연구·개발 또는 개발된 기술의 실용화 등의 사업을 추진하도록 하고, 이를 위한 사업을 하려는 자에게 자금의 전부 또는 일부를 지원할 수 있도록 함(안 제8조)

o 과학기술정보통신부장관은 인공지능 기술의 촉진에 필요한 전문인력의 양성과 자질 향상을 위하여 교육 및 훈련을 실시하도록 하고, 이에 필요한 예산을 지원할 수 있도록 함(안 제10조)

o 과학기술정보통신부장관은 인공지능 산업과 관련한 산업계·학계 및 연구계가 일정한 지역에서 유기적 연계를 통하여 인공지능 기술개발의 효율을 높이고, 국내외 인공지능 기술 집약 기업을 유치하거나 육성하기 위하여 인공지능 거점지구를 조성할 수 있도록 함(안 제14조)

o 인공지능 거점지구와 관련된 관계 중앙행정기관의 장등 및 인공지능 사업자 등이 익명처리된 개인정보의 활용하는 경우 「개인정보 보호법」 등 다른 법령의 적용을 받지 아니하도록 함(안 제15조)

※ **Reference**

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

「정보통신기반 보호법」 일부개정법률안(대안)

(과학기술정보방송통신위원장 발의, 2019. 11. 18. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 최근 지속적인 전자적 침해행위로 공공기관·언론·금융사 등의 피해가 빈번하게 발생하고 있어 주요정보통신기반시설의 취약점을 조기에 파악하여 전자적 침해행위의 가능성을 차단하지 않을 경우 개인과 사회의 안전에 큰 피해가 발생할 것으로 예상되나, 현행법에 따른 주요정보통신기반시설의 취약점 분석·평가는 정기적으로만 실시하도록 되어 있어 새로운 형태의 전자적 침해행위가 수시로 등장하는 경우 이에 대한 대비가 어려운 상황인바, 이에 대한 개선이 필요하다는 요구가 있음

▶ 주요내용

o 중앙행정기관의 장으로 하여금 새로운 형태의 전자적 침해행위의 등장 등 주요정보통신기반시설의 보호를 위하여 필요한 경우와 주요정보통신기반시설에 중대한 변화가 발생하여 별도의 취약점 분석·평가가 필요하다고 판단하는 경우 소관 분야의 주요정보통신기반시설 관리기관의 장에게 시설의 취약점을 분석·평가할 것을 명할 수 있도록 함 (안 제9조제2항 신설)

※ **Reference**

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

미국 상원, 딥페이크 기술 사용 등에 대한 보고서 작성 법안 통과 (2019. 10. 24.)

미국 상원은 딥 페이크(Deepfake)[1] 기술을 이용한 디지털 콘텐츠 위조 등에 대한 보고서를 국토안보부 장관이 매년 발간하도록 하는 《딥 페이크 보고 법안》[2]을 의결 (2019. 10. 24.)

▶ 개요 및 경과

o 미국 상원은 딥 페이크 기술 등을 이용한 디지털 콘텐츠의 조작 현황과 이에 대한 국가적 대응 조치·방안을 포함한 보고서를 국토안보부 장관이 매년 발간하도록 지시하는 《딥 페이크 보고 법안》을 의결함

- 이 법에서 정의하는 디지털 콘텐츠 위조는 인공지능과 기계학습을 포함한 새로운 기술을 이용하여 영상과 오디오, 또는 텍스트 내용 등을 조작하는 것을 의미함
- 국토안보부 장관은 동 법 제정일로부터 1년 이내에 디지털 콘텐츠 위조 기술 및 대응 방안에 대한 최초의 보고서를 의회에 제출하고, 5년 동안 연차보고서를 발간해야 함

o 동 법안은 지난 2019년 7월 9일 상원에서 최초로 소개되었으며, 2019년 7월 24일에는 일몰 조항 등을 추가한 수정된 안이 채택됨

▶ 주요 내용

o **(목적)** 최근 AI 기술의 발전으로 디지털 콘텐츠 조작이 국가 안보와 대중의 신뢰에 영향을 미치고, 연방정부 차원에서 관련된 기술에 대한 현황을 조사·평가하고 적절한 대응책을 마련할 수 있도록 연차보고서 발간을 지시

o **(정의 규정)** '디지털 콘텐츠 위조(Digital content forgery)'란 인공지능 및 기계학습 등을 포함한 새로운 IT 기술을 사용하여 사람들을 오도하려는 의도로 영상과 오디오, 또는 텍스트 내용 등을 조작하는 것을 의미함

o **(보고)** 이 법의 제정일로부터 1년 이내에 국토안보부 장관은 과학기술부 차관과 협력하여 디지털 콘텐츠 위조 기술 현황 및 대응방안에 대한 최초의 보고서를 작성하고, 향후 5년 간 다음과 같은 내용을 포함한 연차보고서를 의회에 제출해야 함

1) 딥 페이크(Deepfake) 란 "Deep learning(인공지능이 축적된 자료를 기반으로 스스로 학습하는 기술)"과 "Fake(모조품)"의 합성어로, 인공지능 기반의 영상 합성·조작 기술임
2) Deepfake Report Act of 2019 (S.2065)

< 디지털 콘텐츠 위조에 대한 연차보고서에 포함되어야 할 사항 >

구분	내용
위조 기술	• 위조 디지털 콘텐츠를 제작 또는 전파하는데 사용되는 기술에 대한 조사 및 평가
콘텐츠의 유형	• 위조된 디지털 콘텐츠의 유형 • 연방법에 따른 시민권의 침해 및 사기, 위해성 등의 내용을 포함한 주요 위조 콘텐츠의 유형별 설명을 수록
국가 안보	• 국가 안보를 해치는 디지털 콘텐츠 위조와 관계된 외국 정부의 네트워크에 대한 조사·평가 • 비정부기구 등에서 디지털 콘텐츠를 위조 및 위조할 수 있는 방법에 대한 평가
개인 영향 및 위험성	• 디지털 콘텐츠 위조가 개인에게 미치는 영향을 조사·평가 • 위조에 사용되는 기술의 위험성과 기술부문별 차이점을 평가
판단 기준 및 이용자 경고 등	• 디지털 콘텐츠가 위조 기술을 통해 생성되었는지 여부를 판단할 수 있는 분석 방법 • 의심스러운 콘텐츠와 정보를 식별하고 이용자 등 관계자에게 경고를 제공하는 절차·방법
대응 조치	• 디지털 콘텐츠 위조 기술에 대한 우려를 해소하기 위해 사용될 수 있는 대응 조치 방안 • 국토안보부 장관이 적절하다고 판단하는 추가적인 정보 등

o **(공청회 등)** 보고서 작성 시 국토안보부 장관은 필요하다고 판단되는 연방정부 기관과 협의를 실시하고, 공청회를 개최하여 이해관계자들이 보고서 작성과 관련된 정보 및 조언을 제시·제공할 수 있도록 함

▶ 시사점

o 최근 AI와 같은 신기술을 이용한 디지털 콘텐츠 조작이 사이버공간을 통해 확산되면서 국가 안보를 위협하고 국민의 사생활 보호에 부정적인 영향을 미치는 등 다방면에서 우려가 커지고 있음

o 본 법안은 디지털 콘텐츠 조작으로 인한 피해를 방지하는데 도움이 되는 현황 분석 및 대응 체계 마련을 위한 기초자료로 정부가 보고서를 작성하도록 명시하고 있어, 향후 이와 관련된 다양한 법제도 및 정책들이 추진될 것으로 전망

※ **Reference**

https://www.congress.gov/116/bills/s2065/BILLS-116s2065es.pdf
https://www.congress.gov/bill/116th-congress/senate-bill/2065

EU 집행위원회, NIS지침에 따른 필수 서비스 제공자 식별 보고서 발표 (2019. 10. 28.)

EU 집행위원회는 《NIS 지침》[1]에 따른 필수 서비스 제공자를 식별하는 국가별 방법론을 비교하고, 국가 간 방법론의 불일치 해소 방향을 제시하는 보고서[2]를 발표 (2019. 10. 28.)

▶ 개요 및 경과

o EU 집행위원회는 NIS 지침에 따른 필수 서비스 제공자(OES)[3]를 식별함에 있어 회원국이 취한 접근 방법을 비교하고, 국가 간 적용한 방법론의 불일치 해소를 위해 개선해야 할 방향을 제시하는 보고서를 발표함

- 국가별 OES를 식별하는데 사용한 방법론을 검토한 결과, 서로 다른 수준이나 NIS 지침 조문의 해석 등으로 인해 불일치하고 있는 것으로 나타남
- 특히 국경을 넘나드는 운송과 에너지 부문의 서비스는 회원국 간 격차가 큰 편으로 서로 협력하여 일관성을 확보하도록 권장
- EU 집행위원회는 OES 식별 방법의 불일치 등을 해소하기 위해 내년 중에 가이드라인을 개발 및 제공할 계획임

▶ 주요 내용

o **(목적)** 본 보고서는 NIS 지침 제23조제1항[4]에 따라 회원국이 OES를 식별하는데 사용하는 접근방식의 일관성을 평가하여 궁극적으로 동 지침 제23조제2항[5]에 규정된 NIS 지침의 평가 시 반영 및 개선 방안을 마련하기 위한 것임

---

1) 네트워크 및 정보 보안 지침(The Directive on Security of Network and Information Systems, NIS Directive), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union: EU 회원국 내 사이버보안 역량 강화 및 EU 차원의 효과적인 사이버보안 위협 대응·협력을 향상시키기 위해 각 회원국이 국가 사이버보안전략을 수립·채택하고, 네트워크 및 정보 시스템의 보안을 높은 수준으로 유지하기 위한 정책 및 규제 수단을 마련해야 함을 주요 내용으로 담고 있음

2) REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, COM(2019) 546 final

3) Operators of essential services: 에너지, 교통, 금융, 보건 등의 영역에서 사업하는 자로 네트워크 및 정보 시스템에 의존해 사회·경제 활동의 유지를 위해 사회기반서비스를 제공하는 자를 의미함.

4) NIS 지침 제23조제1항: 위원회는 필수 서비스 운영자를 식별하는데 회원국이 취한 접근 방식의 일관성을 평가한 보고서를 2019년 5월 9일까지 유럽의회와 이사회에 제출해야 함

5) NIS 지침 제23조제2항: 위원회는 본 지침의 기능을 정기적으로 검토하여 유럽의회 및 이사회에 보고해야 하며(부속서 II의 필수서비스 제공자 식별의 일관성 평가 내용이 포함), 첫 번째 보고서는 2021년 5월 9일까지 제출해야 함

o **(식별된 OES의 수)** 위원회에 보고된 OES의 총 수는 회원국 평균 633개로 나타났으나, 그 기준에 차이가 발생하고 있음

o **(NIS 지침 부속서 II 외에 도출된 추가 부문)** 총 28개 회원국 중 7개 회원국은 NIS 지침 부속서 II[6]에 포함되지 않는 새로운 서비스 부문에 대하여 총 157개의 OES를 식별함[7]

- 현행 부속서 II의 범위가 적절한지에 대한 추가적인 검토가 필요

o **(국경 간 협의)** 내부 시장에서 국경 간 서비스의 중요성이 높음에도 불구하고 다른 회원국과 협의가 원활하게 진행되지 않았으며, 주요 원인은 다음과 같음

- 관련된 정보를 안전하게 전달할 수 있는 보안 채널이 부족
- 국경 간 협의에 대한 회원국 간의 목표 및 범위가 다름
- 회원국 간에 적용하고 있는 기준에 차이가 있음

o **(일관성 확보 방향)** OES 식별의 일관성을 확보하기 위해 EU 위원회가 제시하는 회원국 및 EU 차원의 정책 추진 방향은 다음과 같이 정리할 수 있음

< OES 식별의 일관성 확보 방향 >

구분	내용
회원국	• 국가별 담당 기관은 정기적으로 OES 목록을 검토하여 기존의 필수 서비스가 모두 식별[8]되도록 하고, 내부 시장 전반에 걸쳐 일관성 격차가 감소하도록 조치해야 함 • 특히 운송과 에너지와 같이 국경을 넘나드는 서비스 부문은 개별적으로 적용하는 기준의 일관성 확보를 위해 적극적으로 협력 • 회원국은 국경을 초월하는 사업자 및 유사한 사이버보안 사고 등에 대한 보고가 가능하도록 국가 당국 간 협의를 강화해야 함
EU	• NIS 협력그룹의 역할을 전반적으로 강화 • 국경을 초월하는 영향이 있는 서비스의 경우 NIS 협력 그룹이 협의 과정을 검토하고, 안전한 정보 교환이 이루어지도록 지원 • 회원국 간에 NIS 지침의 해석 및 적용의 차이로 인해 발생되는 문제를 해결하기 위해 위원회가 주도의 사례 논의 활성화

6) 부속서 II에는 에너지(전기, 석유, 가스), 운송(항공, 철도, 해운, 도로), 은행, 금융 시장 인프라, 건강, 식수 공급・유통, 디지털 인프라의 7개 부문을 제시하고 있음

7) OES 목록을 제출한 7개 회원국 외에 4개 회원국은 NIS 지침 부속서 II에 포함되지 않는 새로운 서비스 부문을 발견하였으나, 구체적인 OES 목록을 제출하지는 않음

8) 다수의 회원국이 지침이 정한 기간(2019년 5월) 내에 OES 식별 프로세스를 완료하지 않았으며, 본 보고서는 2019년 9월까지 취합된 결과를 수록한 것임. 총 28개 회원국 중 23개 회원국은 모든 자료제출을 완료하였으나, 5개 회원국은 일부 자료를 제공하였으므로 자료 제출이 완료되지 않은 회원국의 경우 나머지 자료를 최단 기간 내에 위원회에 제출하도록 권고함.

▶ 시사점

o EU는 최근 국경을 넘나드는 운송과 에너지 부문의 서비스가 확대됨에 따라 NIS 지침 상의 보안 조치 의무 대상인 OES를 식별하는 공통된 방법론 개발을 모색하고 있음

o 본 보고서에서 제시한 방향에 따라 향후 OES의 디지털 서비스 유형 및 하위 목록에 대한 세부 평가를 실시하고, 그 결과는 NIS 지침의 광범위한 평가 및 개선 시 반영될 것으로 전망

※ **Reference**

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0546&from=EN
https://ec.europa.eu/digital-single-market/en/news/report-assessing-consistency-approaches-identification-operators-essential-services

프랑스 국가정보시스템보안청(ANSSI), 디지털 위험 관리 지원을 위한 가이드 발표 (2019. 11. 18.)

프랑스 국가정보시스템보안청(ANSSI)[1]은 공공・민간 분야의 사이버보안 관리자 및 위험관리 담당자를 대상으로 《디지털 위험 관리 가이드》[2]를 발표 (2019. 11. 18.)

▶ 개요 및 경과

o 프랑스 국가정보시스템보안청(ANSSI)은 기업위험・보험관리 협회(AMRAE)[3]와 협력하여 공공・민간 조직의 사이버보안 관리자 및 위험관리 담당자를 대상으로 공통적으로 활용할 수 있는 사이버보안 위험관리 절차 등을 제시하는 《디지털 위험 관리 가이드》를 개발하여 발표함

- 사이버보안 위험 관리 절차를 크게 ▲디지털 위험 이해 및 체계화 ▲ 보안 기반 구축 ▲디지털 위험 관리 및 사이버보안 강화로 구분하여 제시
- 사이버보안 보험과 관련한 정책 방향 설정 시 고려해야 할 사항을 수록
- 디지털 위험 실적 관리를 위한 지표와 측정 기준을 제공

▶ 주요 내용

o **(목적)** 최근 ICT의 발달로 모든 조직들이 디지털 위험에 노출되고 그 피해가 급증하고 있는 상황으로, 본 가이드는 조직 내의 관리자 및 위험 관리 담당자들이 디지털 위험 관리 정책을 수립・실행할 때 적용할 수 있는 기본적인 절차 등을 제공하는 것임

o **(사이버보안 위험 관리 절차의 구성)** 총 15개 단계를 업무 진행 순서 및 내용에 따라 다음의 3개 부문으로 구분하여 제시

- 디지털 위험 이해 및 체계화(1~6단계): 디지털 위험 관리에 대한 이해를 돕고, 전략 수립 및 거버넌스 구현을 위한 개념을 체계화

1) Agence nationale de la sécurité des systèmes d'information: 2009년 프랑스 총리 소속으로 설립된 국가정보시스템 보호 규정 및 정책 입안을 지원하는 기관임. 중요 인프라 시스템 보호 및 관련 교육・정보 제공, 해킹 등 정보통신망 침해에 대응하는 기술개발 점검 등의 업무를 담당함

2) DIGITAL TRUST: ANSSI AND AMRAE PUBLISH A GUIDE ON DIGITAL RISK MANAGEMENT FOR MANAGERS

3) Association pour le Management des Risques et des Assurances de l'Entreprise: 프랑스 기업의 위험 및 보험관리에 대한 협회로 1993년에 설립. 현재 1,100명의 공공기관 회원 및 700여개 민간단체가 참여하고, 위험 관리에 대한 방법론 개발・개선 및 전문가 교육을 실시하고 있음

- 보안 기반 구축(7~11단계): 앞서 수립한 디지털 위험 관리 전략을 수립하기 위한 조치를 설명하고, 사이버방어・복원력의 원칙을 제시
- 디지털 위험 관리 및 사이버보안 강화(12~15단계): 사이버보안 위험 관리 측면에서 지속적인 개선 과정을 설명하며, 이와 관련된 성과 관리 방안을 제시

o **(단계별 주요 내용)** 사이버보안 위험 관리를 위한 단계별 주요 내용은 아래와 같음

< 사이버보안 위험 관리 단계별 주요 내용 >

구분	단계	주요 내용
디지털 위험 이해 및 체계화	1	• 디지털 위험에 대한 조직 체계를 정의
	2	• 조직 구성원의 디지털 활동 및 역할에 대한 이해 • 중요한 비즈니스 자산을 식별하고, 이해관계자를 파악
	3	• 사이버보안 위험이 허용되는 임계값[4]을 파악
	4	• 조직 여건에 적합한 최악의 사이버보안 위험 시나리오 설정
	5	• 디지털 보안 전략 정의 및 우선순위, 인센티브 등을 설정
	6	• 활동 중단 등의 손실에 대비한 적절한 사이버보안 보험 상품 선정 - 예방・지원・범위・책임 보상 측면에서 평가하고, 적합성 테스트 실시
보안 기반 구축	7	• 인적 요소를 정보 보안 정책에 반드시 포함하고, 관련된 교육 실시
	8	• 조직의 보안 목표에 따라 중요한 디지털 서비스에 대한 인증[5] 실시
	9	• 법적 규제 및 의무에 따라 조직에 적합한 보안 기준・표준을 선정
	10	• 사이버방어의 방향성을 정하고 적절한 예방 탐지 체계 구현
	11	• 사이버보안 복원력 향상을 위한 위기대응 및 업무 연속성 계획 수립
디지털 위험 관리 및 사이버보안 강화	12	• 과거의 사이버보안 위협 정보와 최신의 사이버공격 기술을 정확히 이해하여, 새로운 위협・취약성에 올바른 대처를 할 수 있도록 함
	13	• 조직의 구성원 및 이해관계자들로부터 다양한 의견을 수렴하여 전략을 수립・실행하고, 실전과 같은 훈련을 실시
	14	• 조직의 보안 수준을 유지하도록 감사・통제와 관련된 사항을 반드시 전략에 포함하고, 정기・지속적인 검토 및 개선을 실시
	15	• 사이버보안 활동에 대한 이익을 정량화하여 투자를 촉진시키고, 조직 성장에 긍정적인 이미지 변화를 이끌어 냄

4) 프랑스 표준화 협회에서 발간한 다음 문서를 참조. "Management du risque : une approche stratégique", AFNOR edition, 2018

5) 정부부처 간 일반지침 No.1300(Interministerial General Instruction no. 1300, SGDSN, 2011), 일반정보 보호기준(The General Security Baseline, ANSSI, 2014), 국가정보시스템 보안정책(The State Information Systems Security Policy, ANSSI, 2014), 군사계획법(The Military planning law 2014 to 2019)에 해당하는 경우 의무적으로 인증을 받아야 함

▶ 시사점

o ANSSI는 프랑스 국가정보시스템의 보호와 관련된 규정과 정책 지원 업무를 담당하는 사이버보안 핵심기관으로, 이번에 발표한 가이드의 방향을 반영하여 관련된 법제도 제·개정 및 정책 수립 시 사이버보안 위험관리 및 보험 부문이 강화될 것으로 전망

o 프랑스 정부는 앞으로 민간 부문에서 사이버보안 위험 관리의 중요성이 부각되어 관련된 일자리가 늘어날 것 예상하고 있으며, 위험 관리 대응 방안으로 사이버보안 보험의 도입도 활발해질 것으로 기대

※ **Reference**

https://www.ssi.gouv.fr/uploads/2019/11/anssi_amrae-guide-controlling_digital_risk-trust_advantage.pdf
https://www.ssi.gouv.fr/en/guide/controlling-the-digital-risk-the-trust-advantage/

독일 연방정보보안청(BSI), 의료기기의 사이버보안 강화를 위한 가이드 발표 (2019. 11. 18.)

독일 연방정보보안청(BSI)은 의료기기를 제조·공급하는 업체에게 의료기기 보안에 대한 생산자 공개문(MDS2)[1]을 작성하도록 권장하는 가이드[2]를 발표 (2019. 11. 18.)

▶ 개요 및 경과

o 독일 연방정보보안청(BSI)은 독일 내의 의료기기 제조 및 공급 업체가 현재 미국 내 의료기기 공공조달 시장에서 사용 중인 MDS2를 작성하는 것을 권장하도록 안내하는 가이드를 발표함

- 산업계와 공공기관에서 의료기기의 사이버보안과 관련된 특징과 기능을 구조화된 형태로 표시하는 MDS2를 통신수단으로 권장함
- MDS2의 작성은 자발적이며, 법적 의무문서에 해당되지는 않음
- MDS2는 의료기기에 대한 설명 데이터, 무단 사용자의 접근 및 오용 방지 능력, 복구 능력 등의 24개 항목으로 구성

o 본 가이드는 사이버공격에 대한 복원력 강화를 목표로 현재 약 4천개의 기업 및 단체가 제휴하고 있는 BIS의 사이버보안 협업 조직[3]이 개발한 것으로, 다양한 분야를 영위하는 산업계의 의견이 반영된 것임

▶ 주요 내용

o **(목적)** 최근 의료기기 분야에서 디지털화 및 네트워크 활용이 증가하고 있고, 의료기기의 특성 상 병원에서의 안전한 사용 및 제품의 긴 수명이 요구되는 등 특별한 사이버보안 요건을 필요로 하고 있으므로 전반적인 의료기기의 사이버보안 강화를 위해 국제적으로 널리 활용되는 MDS2 작성을 권장하고 그 작성 방법 등을 안내하고자 함

- MDS2 양식이 작성되면 공공·의료기관 및 의료기기 소비자 등은 구매하려는 의료기기에 대한 사이버보안 수준 및 특성을 쉽게 파악할 수 있음

1) 의료기기 보안에 대한 생산자 공개문(Manufacturer Disclosure Statement for Medical Device Security, MDS2)은 2004년에 미국전기제조업협회(National Electrical Manufacturers Association, NEMA)가 최초로 개발한 것으로 현재 미국 내 의료기기 시장에서 공공조달 시 활용됨
2) Medica 2019: BSI-Leitfaden zur Cyber-Sicherheit von Medizinprodukten
3) Allianz für Cyber-Sicherheit

o **(MDS2 항목)** 본 가이드에서 제시하는 MDS2 양식에 포함되는 24개 항목 및 주요 특징은 다음과 같이 정리할 수 있음

< MDS2 작성 항목 및 주요 특징 >

구분	내용
의료기기 설명	• 의료기기를 설명하기 위한 데이터: 제조업자 정보, 제품설명 등
개인 데이터 관리	• 제품이 개인 데이터를 처리하는 방법
자동 로그아웃	• 장치를 일정기간 사용하지 않은 경우 무단 사용자의 접근 및 오용 등을 방지하는 기능
변경 제어	• 제품 내 활동을 안정적으로 기록 및 모니터링 할 수 있는 능력
권한	• 제품이 사용자 권한을 인식하는 능력
보안 업그레이드	• 현장 또는 원격에서 보안 업데이트를 실시할 수 있는 능력
데이터 식별	• 제품에 사용자 식별이 가능한 정보를 직접 제거할 수 있는 능력
백업・복구	• 데이터, HW 및 SW 손상 또는 파괴 후 복구 가능성
비상 접근	• 제품 사용자가 비상 시 개인 데이터에 접근 할 수 있는 가능성
무결성	• 인증 없이 제품에 저장된 데이터가 변경・삭제되지 않도록 하는 능력
멀웨어 탐지・보호	• 악성 SW를 효과적으로 예방 및 탐지할 수 있는 능력
통신 파트너 인증	• 통신 파트너 및 노드를 인증하는 제품의 능력
연결 가능성	• 네트워크 및 이동식 미디어와의 연결 능력
사용자 인증	• 사용자 인증을 위한 제품 구성 능력: 사용자 이름, 암호, 관리자 등
물리적 접근 차단	• 무단 사용자가 물리적으로 접근할 수 없도록 하는 능력
전체 수명 주기	• 수명 주기 및 타 사의 구성 요소 보안을 지원하는 제조업체의 계획
SW 구성요소 목록	• 제품에 포함된 SW 전체 구성요소 목록으로, 비상 관리 정보도 포함
시스템 저항력	• 제품에 내재되어 있는 사이버공격 및 악성SW에 대한 저항 능력
운영자 보안 가이드	• 제품 운영・관리자를 위한 안전 지침 및 사후 서비스
무결성과 기밀성	• 제품에 저장된 개인 데이터 무결성과 기밀성을 유지하는 능력
안전한 데이터 전송	• 데이터 전송 시 정보의 기밀성을 보장하는 제품의 능력
전송 데이터 무결성	• 전송된 데이터의 무결성을 유지하는 제품의 능력
원격 대기	• 유지보수 기술자가 원격으로 작업을 수행하도록 지원하는 능력
기타 추가 사항	• 제조사가 고려하는 제품의 안전 특성을 명시

▶ 시사점

o 기존에 미국에서 사용 중인 MDS2의 작성을 BSI가 권장함에 따라 독일 의료기기 제조업체들의 MDS2 작성이 확대될 것으로 보이며, 독일 내 의료기기의 전반적인 사이버 보안 수준이 향상됨과 동시에 사이버보안에 대한 소비자들의 관심도 증대될 것으로 예상됨

※ **Reference**

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/Expertenkreis_CyberMed_MDS2.pdf;jsessionid=B7ED8CE7EAAAAD42BBCC5775417A243E.2_cid341?__blob=publicationFile&v=2#download=1
https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/Leitfaden_Med-Produkte_231019.html

해외 입법 동향 일본

일본 내각사이버보안센터, 중요 인프라 사업자를 위한 정보 공유 지침서 발표 (2019. 10. 28.)

일본 내각사이버보안센터(NISC)는 중요 인프라 사업자의 사이버보안 위협 정보 공유 확대를 위해 정보 공유의 절차와 방법을 구체적으로 안내하는 지침서[1]를 발표 (2019. 10. 28.)

▶ 개요 및 경과

o 일본 내각사이버보안센터(NISC)는《국가 중요 인프라의 정보 보안 대책에 대한 제4차 행동계획(이하 '행동계획' 이라 함)》[2]에 따라 중요 인프라 사업자에게 사이버보안 위협 정보 공유의 방법과 절차 등을 구체적으로 안내하는 지침서를 발표함

- NISC와 소관부처, 주요 인프라 사업자 간 사이버보안 취약점 및 사고 관련 정보 등을 공유하고, 정보 공유 시의 업무 절차와 수행 방법을 제공
- 사이버보안 위협 정보 공유의 범위는 TLP(Traffic Light Protocol) 체계[3]와 연계하여 레드・엠버・그린・화이트의 4단계로 구분하여 제시

o 본 지침서는 관련된 업무를 알기 쉽게 해설하는 것이 주된 목적으로, 법령 용어 등의 해석이 필요한 경우 상위법[4] 및 행동 계획이 우선 적용됨

▶ 주요 내용

o **(목적)**《국가 중요 인프라의 정보 보안 대책에 대한 제4차 행동계획》에 따른 정보를 원활히 공유할 수 있도록 국가 주요 인프라와 사업자에게 사이버보안 위협 정보 공유의 구체적인 절차와 내용을 제공

---

1) 《"重要インフラの情報セキュリティ対策に係る第４次行動計画"に基づく情報共有の手引書(試行版)》
2) 《重要インフラの情報セキュリティ対策に係る第４次行動計画(2017년 4월 18일 제정)》: 정보통신, 금융, 항공, 공항, 철도, 전력, 가스 등 국가 중요 인프라에 해당하는 14개 부문을 지정하고, 소관부처와 중요 인프라 사업자 간 정보를 공유할 수 있는 체계를 구축하도록 함
3) 원활한 사이버보안 위협 정보 공유를 위한 정보공유 범위에 관한 프로토콜로, 민감한 정보가 적절한 대상과 공유되도록 하기 위해 사용하는 일련의 설정임. 1990년에 설립된 국제침해사고대응팀협의회(The Forum of Incident Response and Security Teams, FIRST)에서 정의하는 TLP 지침은 수신자가 예상한 공유의 경계를 나타내기 위해 4가지 색상체계 (레드・엠버・그린・화이트)을 제시하고 있으며, 세부 내용은 다음 링크를 참조. https://www.first.org/tlp/
4) 《사이버시큐리티기본법(サイバーセキュリティ基本法, 2014.11.6. 제정)》: 국가 사이버보안 정책의 기본 이념, 국가 및 지방 공공 단체의 책무, 사이버보안 전략 개발 등 시책의 기본적인 사항을 정하고 있음. 중요 인프라 사업자 등의 사이버보안과 관련하여 국가는 관련된 기준의 책정, 연습 및 훈련, 정보 공유 및 기타 자발적인 활동의 촉진, 기타 필요한 시책을 강구해야함 (제14조)

o **(정보 공유 대상)** 행동계획 별첨의 정보연락 및 정보제공에서 명시하고 있는 다음의 내용을 포함한 시스템 오류 등에 대한 정보가 공유 대상에 해당됨

- 국가 주요 인프라 서비스의 장애를 포함한 시스템 오류나 전조 증상에 대한 정보
- 사이버보안 사고와 관련된 원인・결과 및 보안 취약점 등의 정보

o **(정보 공유 범위)** 정보의 확산으로 인해 사이버보안 위협이 증대될 우려가 있는 기밀정보 등이 포함될 수 있으므로, 다음의 TLP 체계에 따라 공유 범위를 설정

< 국가 중요 인프라 서비스와 관련된 정보 공유 범위 >

구분	정보 공유 범위	세부 범위
Red	• NISC • 중요 인프라 소관부처	• 정보 발신・수신자 간에 한정
Amber	• NISC • 중요 인프라 소관부처 • 직접적인 관계가 있는 CEPTOAR[5] 구성원 및 중요 인프라 사업자	• 해당 기관의 직원 및 컨설턴트, 비밀유지 계약에 따라 정보 시스템의 개발・운용 등의 업무를 위탁받아 수행 하는 자 • 업무 수행을 위해 정보를 알 필요가 있는 자
Green	• NISC • 중요 인프라 소관부처 • 사안 대응 및 정보보안 관계 부처 • 방재 관계 부처 • 사이버보안 관련 사업자	• 해당 기관의 직원 및 컨설턴트, 비밀유지 계약에 따라 정보 시스템의 개발・운용 등의 업무를 위탁받아 수행 하는 자
White	• 제한 없음	• 기밀정보로 취급되지 않음 • 저작권을 준수하는 경우 정보의 출판 및 방송, 인터넷 상에 공개도 가능

o **(중요 인프라 사업자의 정보 제공)** 중요 인프라 서비스 장애를 비롯한 시스템 오류 등이 발생한 경우[6] 중요 인프라 사업자는 소관 부처를 통해 다음의 사항을 포함한 정보를 NISC로 제공함

5) CEPTOAR: Capability for Engineering of Protection, Technical Operation, Analysis and Response: IT 장해를 미연에 방지하고 사고발생 시 피해확대를 방지, 신속한 복구 및 재발방지를 위해 정부 부처 등에서 제공된 정보에 대해 주요 인프라 사업자에게 제공하고 공유하는 중요 인프라 간 연락 협의체로, 일본은 《중요 인프라의 정보 보안 대책에 대한 제1차 행동계획, 2005년 12월》 및 《제1차 사이버보안 기본계획, 2006년 2월》에 따라 금융・항공・ 철도・전력 등 국가 중요 인프라 분야의 협의체가 설립되었음

6) 관계 법령에서 주요 인프라 관할 부처에게 보고를 의무화한 경우, 관계 주체가 국민생활이나 중요 인프라 서비스에 심각한 영향이 있다고 판단한 경우, 중요 인프라 사업자가 정보를 공유하는 것이 적절하다고 판단한 경우가 포함됨. 동 지침서에서는 중요 인프라 서비스 부문별로 계획에 따라 책정되어 있는 안전기준 등을 참고하여 사업 지속 등에 영향이 없도록 가시화돌 가능성이 높은 IT장해를 선정하고, 중요 인프라 사업등의 특성을 고려하여 설정하도록 제시하고 있음. 심각한 영향 등에 대한 사례는 본 지침서 p10(정보 연락을 하는 원인의 사례) 및 p12(대상이 되는 중요 인프라 사업자 등의 중요 시스템 사례). p13~16(중요 인프라 서비스에 대한 설명과 장애 사례)을 참조

- ▲제목 및 개요 ▲정보 공유 범위 ▲일시 및 담당자 정보 ▲사건의 분류 및 원인 ▲중요 인프라 서비스 등에 미치는 영향 ▲다른 사업자 등으로의 파급 가능성 ▲조치 및 계획 ▲교훈 및 개선 사항 등

o **(NISC의 정보제공)** 상기한 기관・조직에서 제공된 정보를 종합・분석한 후에 관련된 기관・조직에게 미리 제시한 정보 공유가 가능한 범위에 해당하는 정보를 제공하며, 정보 공유가 가능한 범위를 초과하여 정보를 공유할 필요가 있다고 NISC가 판단한 경우에는 공유 범위를 변경할 수 있음

- NISC는 중요 인프라 소관 부처에게 정보를 제공하고, 소관 부처는 CEPTOAR 사무국 또는 직접 중요 인프라 사업자 등에게 정보를 공유・제공함

▶ 시사점

o 일본은 중요 인프라 사업자에게 요구되는 높은 보안 수준을 유지하기 위해서 관민 간 사이버보안 위협에 대한 정보 공유가 확대되어야 함을 주요 정책 과제로 선정하고, 이에 대한 다양한 방안을 모색하고 있음

o 동 지침서는 중요 인프라 사업자의 정보 공유 확대를 지원하기 위해 구체적인 방법과 절차를 제공한다는 점에서 그 의의가 있으며, 향후 중요 인프라 관련 사업자들의 정보 공유가 활성화될 것으로 예상

※ **Reference**

https://www.nisc.go.jp/conference/cs/ciip/dai20/pdf/20shiryou07-2.pdf
https://www.nisc.go.jp/conference/cs/ciip/dai20/pdf/20shiryou07-1.pdf

중국 전국인민대표회의, 국가 안보 및 암호의 관리를 위한 암호법 의결 (2019. 10. 26.)

중국 전국인민대표회의 상무위원회는 국가 안보 측면에서 암호의 표준화 및 관리 수준을 향상하고, 암호 산업의 발전을 촉진하기 위한 《암호법》[1]을 최종 의결함 (2019. 10. 26.)

▶ 개요 및 경과

o 중국 전국인민대표회의 상무위원회는 최근 네트워크 정보 기술이 급속히 발전함에 따라 요구되고 있는 높은 수준의 정보 보안을 보장하기 위해 국가 안보 측면에서 체계적인 암호 관리를 추진하고, 암호화 연구개발 및 관련된 산업의 발전·활용을 촉진하기 위한 《암호법》을 통과시킴

- 동 법은 국가 안보 및 암호의 관리를 위한 것으로, '암호'는 특정 변환 방법을 사용하여 정보를 암호화·보호하는 기술·제품·서비스로 정의

- 국가는 핵심 및 일반 암호를 과학적으로 관리하고 관련된 시스템 보안을 강화할 의무가 있으며, 상용 암호는 상업용으로 연구개발 및 학술교류 등을 통해 암호화 산업 발전을 촉진하도록 규정

- 국가 안보 및 사회적 공익과 관련된 상업용 암호화 제품은 이 법에 따라 네트워크 핵심 장비 및 보안 제품 목록에 포함되어야 하고, 《네트워크안전법》[2]에 따른 인증을 통과한 후에만 판매될 수 있음

o 이 법은 2020년 1월 1일부터 발효됨

▶ 주요 내용

o **(목적)** 이 법은 암호의 적용·관리를 규범화하고, 암호산업의 발전 촉진 및 네트워크 정보 보안을 보장하며, 국가 안보·공공의 이익 및 공민·법인·기타 조직의 합법적 권익을 보호하는 것을 그 목적으로 함

1) 《中华人民共和国密码法》(2019年10月26日, 第十三届全国人民代表大会常务委员会第十四次会议通过)

2) 《中华人民共和国网络安全法》(2016.11.7. 제정, 2017.6.1. 시행): 네트워크 보안을 보장하여 네트워크 사이버 주권과 국가안보, 사회공공이익을 수호하고, 개인·법인과 그 밖의 조직의 합법적 권익을 보호하며, 정보화의 건전한 발전을 촉진하는 것을 목적으로, 이 법의 적용을 받는 정보는 중국 공민의 개인정보와 네트워크 안전에 위해가 되는 정보를 포함하고 있음. 네트워크 운영자와 핵심정보 인프라 운영자는 네트워크 보안 등급별로 명시된 안전 보호 의무를 이행해야 하며, 법 위반 시 벌금은 최대 1억원 및 영업정지 처분 등이 가능함. 또한 감독 당국은 국가의 단결을 저해하거나 사회주의 체제의 전복과 관련된 내용을 즉각적으로 검열할 수 있으며, 인터넷 접속을 차단할 수 있는 권한을 가지게 됨

o **(구성 및 주요 내용)** 총 5개장의 44개조로 구성되어 있으며, 각 장별 주요 내용은 다음과 같음

< 암호법의 각 장별 주요 내용 >

구분	내용
제1장 총칙	• 암호화 작업은 국가 안보 개념을 준수하며, 국가 암호화 지도 기구[3]는 국가 암호화 작업의 지침·정책을 수립하고, 관련된 주요 사안 등을 조정 • 국가암호관리부서는 전국의 암호업무를 관리하고, 지방암호관리부서는 관할 행정구역의 암호업무를 관리 • 국가는 암호를 핵심·일반·상용암호로 분류 - 핵심 및 일반암호는 국가 비밀정보보호에 사용 - 상용암호는 국가의 비밀에 속하지 않는 정보를 보호하는데 사용 • 국가는 암호 보안 교육을 강화하고, 암호 업무를 재정 예산에 반영해야 함
제2장 핵심 및 일반 암호	• 국가는 핵심·일반 암호의 과학적 관리 및 보안 수준을 강화할 의무가 있음 • 국가 비밀정보를 저장·처리하는 정보시스템은 핵심·일반 암호를 사용 • 국가 암호 관련 업무 조직을 강화하고, 암호 관리 기관은 핵심·일반 암호의 누설 및 보안에 미치는 중대한 위험이 발견되는 경우 보안 위험을 즉각적으로 제거하는 등의 대응 조치를 실시해야 함
제3장 상용 암호	• 국가는 상용 암호 기술의 연구개발 및 학술 교류, 성과 및 응용의 확산 등 관련 산업의 발전을 장려·촉진해야 함 • 상용 암호의 연구·생산·판매·서비스와 수출·입 시 국가 안보 및 사회 공공의 이익 또는 타인의 합법적 권익을 훼손하지 않아야 함 • 국가는 상용 암호의 표준체계를 수립·보완할 의무가 있으며, 국제 표준화 활동에 참여해야 함 • 상용암호검출인증체계의 구축을 추진 - 국가 안전 및 사회적 공공 이익과 관련된 상용암호제품은 이 법에 따라 네트워크 핵심 장비와 사이버보안 전용품목 목록에 포함되어야 하며, 자격을 갖춘 기관의 인증을 통과해야 판매·제공할 수 있음 - 중요 정보 인프라 운영자가 상용암호와 관련된 제품과 서비스를 정부에 납품하는 경우 국가암호관리부서 등 관련부서의 국가안전심사를 받아야 함
제4장 법적 책임	• 핵심·일반 암호의 유출 및 보안에 영향을 미치는 문제가 발견된 경우, 즉각적인 대응 조치를 취하지 않은 경우 기밀·암호 관리부서는 관련 기관의 담당자 및 법적 책임이 있는 직원을 처벌할 수 있음 • 상용 암호 인증을 통과하지 못한 제품·서비스를 판매·제공하는 경우 암호관리부서는 정정 및 중단 명령을 실시하고, 불법 제품 및 소득을 압수할 수 있음. 불법 소득이 10만 위안을 초과하는 경우 소득의 최대 3배 부과 • 전자정부 전자인증서비스 종사 승인을 거치지 않을 경우 불법 제품과 소득을 압수 할 수 있음. 불법 소득이 30만 위안 이상이면 최대 3배의 벌금 부과, 30만 위안 미만일 경우 10만~30만 위안 이하의 벌금을 부과함
제5장 부칙	• 국가암호관리부서는 법률 및 관리 규정에 따라 암호 관리 규칙을 수립해야 함 • 이 법은 2020년 1월 1일에 발효됨

3) 中央密码工作领导机构: 중국 공산당 중앙위원회 산하의 암호관련 조직이며, 국가 암호 분석·평가 및 관련 정책연구를 수행하는 국가 암호 관리 연구소를 포함

▶ 시사점

o 중국은 최근에 급속한 디지털화와 함께 네트워크 정보 기술이 발전함에 따라 정보 보안의 핵심요소인 암호화를 국가안보의 중요한 전략적 자원으로 보고 있으며, 이 법은 중국의 암호화 분야에서 최초로 제정된 기본법이라는 데 그 의의가 있음

o 특히, 상업용 암호화 제품 및 서비스의 경우 동 법에 따라 암호 인증을 획득하여야 하므로 산업계에서 암호와 관련된 연구개발이 활발해질 것으로 보이며, 국가 암호화 지도 기구 및 국가 암호 관리 연구소, 각 부처 및 지방정부의 암호관리 부서의 역할도 강화될 것으로 전망됨

※ **Reference**

http://www.gov.cn/xinwen/2019-10/27/content_5445395.htm
http://www.npc.gov.cn/npc/c30834/201910/8ac670a396214bc4a6efa18c4c0c0299.shtml

기고

SNS 인플루언서를 활용한 광고, 마케팅 규제 방안

최민식 경희대학교 법무대학원 교수

(약력)
- (現) (사)한국지적재산경상학회 출판이사
- (現) (사)소비자권익포럼 정보통신위원장
- (前) 한국인터넷기업협회 정책실장
- (前) 한국콘텐츠진흥원 책임

1. 문제의 제기

SNS를 통해 일상적인 경험을 공유하면서 소비자들에게 높은 영향력과 파급효과를 미치는 소위 '인플루언서(influencer)'가 등장하였고, 사업자들은 인플루언서에게 제품 사용후기 게시를 의뢰하는 등 이들을 활용한 광고 마케팅 규모는 2020년 기준 글로벌 약 11조원, 국내 약 2조원 규모로 전망되고 있다.[1)]

2019년 4월 서울시 전자상거래센터 조사에 따르면 인스타그램 등 SNS를 통해서 상품 구매 경험이 있는 소비자는 응답자의 55.7%이고, SNS를 통한 상품구매의 가장 큰 이유는 높은 인지도와 많은 팔로워(follower)를 보유한 인플루언서가 공동구매나 이벤트를 진행하는 경우가 많아 제품·브랜드 관련 소식을 빠르게 접할 수 있고 이들이 제공하는 다양한 정보 등을 신뢰하기 때문이다. 그러나 이러한 신뢰를 저버리는 일부 인플루언서의 허위, 과장, 기만광고 등으로 인한 국내 소비자 피해경험은 2016년 23%에서 2018년 28%로 증가하고 있다.[2)]

「추천·보증 등에 관한 표시·광고 심사지침(공정거래위원회예규 제271호)」에서는 추천·보증 등의 내용이나 신뢰도 등에 영향을 미칠 수 있는 경제적 이해관계가 존재하는 경우에 이를 공개'하도록 규정하고 있으나, 대가를 지급받은 SNS 인플루언서를 통해 광고하면서 이와 같은 사실을 밝히지 않고 소비자를 기만하는 부당 광고행위가 빈번하므로 11월26일 공정거래위원회는 이러한 행위를 한 7개 사업자에 대하여 「표시·광고의 공정화에 관한 법률」 위반을 이유로 시정명령과 과징금 부과를 결정했다.[3)]

---

1) 나스미디어, "인플루언서 시장 현황 및 마케팅적 활용", 2019 Trend Keyword.
2) "인스타 마켓 사기, 환불거부…소비자 피해 증가 추세", 서울시전자상거래센터 보도자료, 2019.4.1.
3) 엘브이엠에치코스메틱스, 엘지생활건강, 아모레퍼시픽, 다이슨코리아, 티지알앤, 에이플네이처 등 6개 사업자는 조사 과정에서 위반 게시물을 삭제하거나 수정(경제적 대가를 표시)하는 방법으로 대부분 시정하였으나, 엘오케이는 총 1,130건의 위반 게시물 중 254건(22%)을 시정하지 않은 점을 고려하여 과징금, 시정명령과 함께 공표명령도 부과하였다, "표시광고법 위반 7개사 제재", 공정거래위원회 보도자료, 2019.11.26.

이러한 조치는 경제적 대가를 지불한 개별 사업자에 대해서만 해당되며 글로벌플랫폼사업자나 SNS 인플루언서에 대해서는 구체적인 조치를 취할 수 없는 현실이다. 이하 소비자의 합리적인 구매의사결정을 방해하는 SNS 인플루언서에 대한 국내외 법정책 현황 및 사례를 살펴보고 SNS 플랫폼사업자에 대한 제도 개선 방안에 대해서 검토하고자 한다.

2. SNS 광고마케팅과 규제

우리나라에서 동영상을 이용하기 위하여 가장 많이 사용하는 매체는 유튜브가 압도적이다. 기업은 물론 정치인, 연예인, 일반인들도 유튜브 채널을 개설하여 크리에이터(creator)이자 '인플루언서로 활동하고 있다. 2018년 조사에서 초등학생들이 장래 희망 직업 5위로 '유튜버(youtuber)'를 꼽고 있다.[4] 유튜브가 인기 있는 주요 이유는 일정 수준 구독자를 모으면 자신의 영상에 광고를 올릴 수 있고 구독자 광고 시청 시간에 비례하여 보상하므로 광고수익으로 손쉽게 돈을 벌 수 있다는 점이다. 유명한 사례로 미국의 7살 어린이가 장난감을 가지고 노는 유튜브 동영상은 월 시청 조회 수 10억 회가 넘으며 광고 수익으로 240억 원을 벌 수 있었다.[5] 국내에서는 유튜브 채널을 운영하는 어린이의 가족회사가 빌딩을 매입한 사실이 알려지는 등[6] SNS를 활용한 광고, 마케팅으로 수익을 창출하는 것이 각광을 받고 있다.[7]

SNS가 효율적인 마케팅 수단으로 각광 받기 시작하면서 소통·교류, 정보 공유의 장에서 상업적 광고의 장으로 변질됨에 따라, SNS 광고로 인한 소비자의 불만과 피해가 증가하고 있는 것은 앞에서 살펴본 바와 같으며, 우리나라에서는 현재 SNS 광고에 대해 인터넷 광고 관련 규제를 적용하고 있으며 이와 같은 규제는 법적규제와 자율규제로 구분할 수 있다.

국내 광고를 규율하는 법적규제는 크게 소비자보호를 위한 「소비자기본법」, 공정거래질서 확립을 위한 「표시·광고의 공정화에 관한 법률」, 전자상거래소비자보호를 위한 「전자상거래 등에서의 소비자보호에 관한 법률」 및 개별 상품에 대한 광고 규제를 두고 있는 다양한 법률로 사업자 규제를 할 수 있으며 자율규제로는 광고주, 광고대행사, 광고매체사 등이 소비자 보호 관점에서 사업자단체 등의 행동규약 및 윤리강령, 가이드라인 등을 통한 사전규제, 불법광고 사후 모니터링 등을 하고 있다.[8]

법적 규제를 통하여 국내 사업자에 대해서는 적극적인 소비자보호 조치를 할 수 있으나 유튜브, 인스타그램 등 글로벌플랫폼사업자에 대해서는 느슨하게 작동하고 있다. 자율규제 측면에서도 공정거래위원회는 '카페·블로그의 상업적 활동에 대한 가이드라인'에 따라 국내 사업자의 카페·

4) 정은진, "2018 초·중등 진로교육 현황조사", 한국직업능력개발원, 2018.12, 112~113면 <표 3-2-21> 학생의 희망 직업 - 상위 20개.
5) Madeline Berg, "How This 7-Year-Old Made $22 Million Playing With Toys", Forbes, 2018.12.3.
6) 김경진, "대한민국 '파워 유튜버'…어떤 콘텐트로 얼마나 벌까?", 중앙일보, 2018.11.28.
7) '2018 인터넷이용실태조사'에 따르면 국내 주이용 SNS는 페이스북(65.7%), 카카오스토리(49.6%), 인스타그램(41.0%), 네이버밴드(33.3%) 순서이다, 한국인터넷진흥원, "2018 인터넷이용실태조사", 2019.5, 66면.
8) 국민권익위원회, "청소년보호를 위한 인터넷상의 선정적 광고 개선방안", 국민권익위원회의결 제2014-439호, 2014.10, 5~7면.

블로그에 협찬 사실 표기, 소비자피해신고, 자체제재 방안 마련 등을 준수하도록 하고 있으나 글로벌플랫폼사업자에게는 적용이 어려운 현실이다.

3. 국외의 SNS 인플루언서 규제 현황

(1) 미국

미국 연방거래위원회(FTC, Federal Trade Commission)는 인터넷을 포함한 모든 매체 광고 규제를 하고 있으며 소비자를 오도하고 제품 및 서비스 이용에 간섭하는 인터넷 광고를 기만적인(deceptive) 것으로 규정하고 이를 금지하고 있다.[9] FTC법(Federal Trade Commission Act)에서는 '상업활동(commerce)에 영향을 미치는 불공정하거나 허위인 모든 행위나 관행'을 불법으로 규정함으로써 오해의 소지가 있거나 의도적으로 정보를 생략한 광고를 규제하고 있다.[10]

FTC는 2017년 4월 인스타그램에서 활동하는 21명의 SNS 인플루언서들에게 경고문을 보내 후원받는 모든 브랜드와 관계를 공개하라고 통보했으며,[11] 2017년 9월 SNS 인플루언서들에게 수천달러를 지불한 도박사이트(CSGO Lotto) 소유자에 대해 후원을 공개하라는 최초의 행정명령을 하고, 같은 해 11월 이들의 후원공개에 대한 동의를 승인했다.[12] 이 사례는 SNS 인플루언서를 FTC법 준수 대상으로 인식하고 FTC가 직접 규제한 최초 사례이다. 이 후 FTC는 SNS 인플루언서에 대해 경제적 후원관계 등을 표시하라는 가이드라인 및 질의응답을 지속적으로 업데이트하고 있으며,[13] 2019년 11월 5일 현재 '소셜미디어 인플루언스에 대한 공개 101'로 업데이트하였다.[14] 이와 같은 가이드라인이 실효성이 있는 이유는 법률이 위반되었거나 위반되고 있다고 FTC에서 "믿을만한 이유"가 있을 때 행정명령을 할 수 있고 이러한 명령을 위반하면 최대 40,654달러의 벌금이 부과될 수 있기 때문이다.[15]

(2) 독일

독일에서 광고의 분리와 표시는 언론의 자유와 표현의 자유, 미디어 제공의 독립성과 무결성, 제공자의 신뢰성과 진실성, 그리고 사용자를 오도로부터 보호하기 위하여 텔레미디어법(TMG, Telemediengesetz)과 연방방송협약(RStV, Rundfunkstaatsvertrag)에 의해 규제되고 있다.[16] SNS

9) 한국소비자원, "온라인(모바일) SNS 광고 문제점 및 개선방안", 2016.5, 18면.
10) §45. (Sec.5)(a)(1) "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."
11) https://www.ftc.gov/news-events/press-releases/2017/04/ftc-staff-reminds-influencers-brands-clearly-disclose
12) https://www.ftc.gov/news-events/press-releases/2017/11/ftc-approves-final-consent-order-against-owners-csgo-lotto
13) https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking
14) https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf
15) https://www.ftc.gov/news-events/press-releases/2017/09/csgo-lotto-owners-settle-ftcs-first-ever-complaint-against

인플루언서와 관련하여 2017년 6월 8일 니더작센(Niedersachsen)주 고등법원에서는 SNS 인플루언서를 이용한 광고마케팅에서 단지 '#ad' 해시태그만으로 광고 여부를 알리는 것은 불충분하고 광고게시물은 누구나 한 번에 알아볼 수 있어야만 하며 유사한 문제가 재발할 경우 건당 25만 유로의 벌금을 부과한다고 판결하여 SNS 인플루언서에 대한 최초의 사법 판단을 하였다.[17]

독일 연방미디어청(Die Medienanstalten)은 이러한 판결이 나온 후 SNS 인플루언서를 활용한 광고에 대해 가이드라인을 발표하였다. 가이드라인은 각 상황별로 필요한 대처방안을 제시하였다. 첫째, 인플루언서가 직접 제품을 구입한 경우이다. 둘째, 제품을 기업으로부터 무료로 제공받는 경우이다. 셋째, 기업으로부터 돈 혹은 반대급부를 제공받고 제품을 알리는 경우로 명백히 광고에 해당한다. 넷째, 제품 사이트에 링크를 거는 경우이다. 연방미디어청은 가이드라인에 인스타그램, 페이스북, 스냅챗, 트위터를 활용한 이미지 포스팅 관련 팁도 추가하였다. SNS 인플루언서는 팔로워들에게 광고 여부를 분명하게 제시해야 한다. 이를 위해 광고를 뜻하는 독일어 #werbung 혹은 #anzeige를 포스팅 맨 앞에 배치하고, 다른 해시태그 사이에 두지 않아야 한다. 반면 #ad, #sponsperd by, #powered by 같은 외래어 표기는 하지 않아야 한다.[18]

(3) 영국

영국은 1961년 소비자보호법(Consumer Protection Act)과 1973년 공정거래법(Fair Trading Act)이 제정되면서 광고규제가 본격화되었고 2003년 커뮤니케이션위원회(Ofcom, The Office of Communications) 출범으로 방송과 광고 관련 규제가 일원화 되었다.[19] 기본적으로 정부기관의 법적 규제와 다양한 사업자의 자율규제로 공동 규제하는 형태이며 SNS 인플루언스와 관련해서는 민간기구인 광고표준위원회(ASA, The Advertising Standards Authority), 광고실무위원회(CAP, The Committee of Advertising Practice)와 정부기관인 경쟁시장청(CMA, The Competition and Markets Authority)이 공동으로 '광고가 광고임을 명확하게 하는 인플루언서 가이드라인'을 만들어 금전적 보상이 따르는 게시물에 광고를 뜻하는 'AD'를 미리 표시해야 하고 언제든 볼 수 있고 모바일을 포함한 모든 기기에서 적합하게 표시해야 한다. AD 대신 'SP'(sponsored)나 'in collaboration with', Thanks to [brand] for making this possible 등 다른 단어를 넣는 것도 금지하였다.[20]

SNS 인플루언서들이 후원 받은 게시물은 영국 소비자보호법의 적용을 받으며, 후원자가 게시물에 대한 통제권을 갖게 되면 그들은 자율규약인 영국 광고규칙(UK Advertising Code)의 적용을 받게 된다. 2018년 8월 CMA는 SNS 인플루언서들이 보상을 받았을 때 제대로 알리지 않는다는 우려로 조사에 착수했으며 2019년 1월에는 SNS 인플루언서가 그들이 보증한 제품에 대해 보상을 받았는지에 대해 확인을 받았다.[21]

---

16) https://www.die-medienanstalten.de/service/rechtsgrundlagen/
17) 한국콘텐츠진흥원, "2017 해외 콘텐츠시장 동향조사", 2018.1, 1007면.
18) Leitfaden der Medienanstalten, Werbekennzeichnung bei Social Media-Angeboten. https://www.die-medienanstalten.de/fileadmin/user_upload/Rechtsgrundlagen/Richtlinien_Leitfaeden/Leitfaden_Medienanstalten_Werbekennzeichnung_Social_Media.pdf
19) 한국소비자원, 앞의 보고서, 19면.
20) An Influencer's Guide to making clear that ads are ads, p.10. https://www.asa.org.uk/uploads/assets/uploaded/3af39c72-76e1-4a59-b2b47e81a034cd1d.pdf

4. 결어

SNS 인플루언서 광고마케팅 등으로 발생하는 소비자 피해를 방지하기 위하여 한국소비자원이 제시하는 SNS 플랫폼사업자에 대해 SNS 광고 차단 서비스 제공 등 소비자 선택권 확대, SNS 이용시 간편하게 신고할 수 있는 체계 마련, SNS상의 불법·유해 정보에 대해 방송통신심의위원회 등 관계 기관의 모니터링 및 감독 강화, 정부기관과 사업자의 자율심의협력시스템 활성화 등 법적 규제와 자율규제로 공동규제를 강화하는 형태의 개선방안을 검토할 필요가 있다.[22] 또한 공정거래위원회가 구글에 대해 시행한 우리나라 소비자에 불공정한 약관 시정 등 글로벌플랫폼 사업자에 대한 적극적인 법 집행 사례도 검토해야 한다.[23]

이와 같이 우리나라 소비자 보호에 대해 글로벌플랫폼사업자들이 우회 또는 회피하는 경우 우리 정부와 사법기관에서 적극적으로 법령을 해석하고 집행할 필요가 있다. 특히 규제 정당성 확보와 불균형규제 해소를 위해서는 국제적 기준에 부합하는 국내 법제 정비가 선행되어야 한다. 국내 기업에만 작동하고 글로벌사업자에게는 적용되지 않는 규제를 양산해서는 안된다.

또한 표시광고와 관련한 법적 규제의 대상은 사업자나 사업자단체에 한정되어 있으므로 정부에서는 미국, 독일, 영국 등과 같이 SNS 인플루언서와 같은 개인을 대상으로 적용될 수 있는 자율규제 가이드라인을 제시하고 지속적인 업데이트로 관리해야 한다.

※ **Reference**

국민권익위원회, "청소년보호를 위한 인터넷상의 선정적 광고 개선방안", 2014.10.
나스미디어, "인플루언서 시장 현황 및 마케팅적 활용", 2019 Trend Keyword.
정은진, "2018 초·중등 진로교육 현황조사", 한국직업능력개발원, 2018.12.
한국소비자원, "온라인(모바일) SNS 광고 문제점 및 개선방안", 2016.5.
한국인터넷진흥원, "2018 인터넷이용실태조사", 2019.5.
한국콘텐츠진흥원, "2017 해외 콘텐츠시장 동향조사", 2018.1.
Madeline Berg, "How This 7-Year-Old Made $22 Million Playing With Toys", Forbes, 2018.12.3.
서울시전자상거래센터, https://ecc.seoul.go.kr
공정거래위원회, http://www.ftc.go.kr
독일연방미디어청, https://www.die-medienanstalten.de/
미국연방거래위원회, https://www.ftc.gov
영국광고표준위원회, https://www.asa.org.uk
영국경쟁시장청, https://www.gov.uk
중앙일보, https://news.joins.com

21) https://www.gov.uk/government/news/celebrities-pledge-to-clean-up-their-act-on-social-media
22) 한국소비자원, 앞의 보고서, 32~34면.
23) http://www.ftc.go.kr/www/selectReportUserView.do?key=10&rpttype=1&report_data_no=8188

인터넷 법제동향
Vol. 146 (November 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**