방통융합정책연구 KCC-2019-31

국민정서에 부합하는 인터넷 규제 개선 방안 연구

A Study for Internet Regulation in accordance with Public Sentiment

이찬구/천혜선/신혜인/지혜인/김유석

2019. 12

연구기관 : (사)미디어미래연구소

방송통신위원회
Korea Communications Commission

이 보고서는 2019년도 방송통신위원회 방송통신발전기금 방송통신 융합 정책연구사업의 연구결과로서 보고서 내용은 연구자의 견해이며, 방송통신위원회의 공식입장과 다를 수 있습니다.

제 출 문

방송통신위원회 위원장 귀하

본 보고서를 『**국민정서에 부합하는 인터넷 규제 개선방안 연구**』의 연구결과보고서로 제출합니다.

2019년 12월

연구 기관: 미디어미래연구소
총괄책임자: 이찬구
참여연구원: 천혜선
신혜인
지혜인
김유석

목 차

표 목 차

그 림 목 차

요 약 문

1. 제 목

국민정서에 부합하는 인터넷 규제 개선방안 연구

2. 연구 목적 및 필요성

SNI필드 정보를 이용한 불법사이트 접속차단(2.11) 조치 도입 이후, 디지털성범죄물, 도박 등 불법사이트 차단과 인터넷상 표현의 자유 간의 적절한 균형이 필요하다는 여론이 제기되었다. 특히 SNI 차단조치('19.2.11)에 반대하는 국민청원이 26만 건을 돌파하는 등 불법정보 유통 방지 기술적 조치 도입과정에서 국민 공감대 형성에 미흡했다는 의견이 제기되었다.

본 연구는 이러한 사회적·정책적 요구를 반영하고 불법정보 유통방지를 위한 기술적 조치 도입의 절차적 보완을 위해, 사회적 논의기구인 "인터넷 규제개선 공론화 협의회"를 구성·운영하여 불법정보 유통방지 관련 제도 개선 방안을 도출하는 데에 목표를 둔다.

3. 연구의 구성 및 범위

본 연구 결과보고서의 제 2장은 국내 불법정보 유통현황과 관련제도를 분석한 결과와 SNI 차단조치('19.2.11) 이후 청원·민원·댓글 등 국민여론 분석결과를 담고 있다. 국내 불법정보의 범위와 유통 현황 및 국내 불법정보 유통방지 제도 현황에 대한 분석을 제시하고, SNI 차단 조치 이후 청원·민원·댓글 등을 분석하여 SNI 차단 조치와 국내 불법정보 유통방지 제도와 관련한 주요 쟁점을 도출했다. 제 3장은 2019년 6월 13일부터 운영된 "인터넷 규제개선 공론화 협의회"의 운영결과를 담고 있다. 이 장은 ① 추진 배경, ② 사안별 검토의견 ④ 인터넷규제개선을 위한 권고사항으로 구성되어 있다.

공론화 협의회는 기술적 조치 비기술적 대안과 도입절차의 투명성 제고방안, 이용자 권익

보호, 법·제도적 쟁점 등을 검토하는 전체회의와 접속차단 기술의 실효성, 기술적 대안 등을 검토하는 특별기술소위로 나뉘어 운영되었다. 이에 따라 전체회의는 불법정보 유통방지를 위한 비기술적 대안, 기술적 조치 도입절차의 투명성 제고 방안, 이용자 권리 보호 방안, 불법정보 유통방지를 위한 기술적 조치와 관련한 법·제도 등을 논의하였으며, 특별기술소위원회는 현행 불법정보 유통방지 기술 검토, 불법정보 유통방지를 위한 기술적 대안, 이용자 이익 보호 방안을 논의하였다.

4. 연구 내용 및 결과

본 연구는 인터넷 규제의 바람직한 방향과 적정한 수준에 대한 국민적 공감대를 형성하기 위해 '인터넷 규제개선 공론화협의회' 구성하여 접속차단의 기술적 조치의 기술 방식, 불법정보 유통방지를 위한 기술적·비기술적 대안, 접속차단 조치 도입절차의 투명성, 이용자 권리 보호, 국내 불법정보 유통방지와 관련한 법·제도적 쟁점 등을 검토하고 개선방안을 논의하였다.

5. 정책적 활용 내용

본 연구는 공론화협의회 논의결과를 바탕으로 ① 청원·민원·댓글 등 국민여론 분석자료를 토대로 한 논의배경, ② 공론화협의회 검토의견 ③ 정부 권고사항을 방송통신위원회에 제출하였으며, 전문가들의 권고사항은 향후 불법정보 유통방지를 위한 제도 개선에 반영될 것으로 기대된다.

6. 기대효과

공론화협의회의 논의 결과를 공유하여 불법정보 유통방지를 위한 법제도적 정책개선에 대한 국민의 신뢰를 제고하고, 이해당사자와 국민이 참여하는 공개의견수렴 절차를 통해 숙의적 정책결정에 기여할 것으로 기대된다.

제 1 장 서 론

제 1절 연구의 필요성 및 목적

○ (사회적 요구) 디지털성폭력물, 불법저작물, 불법도박 등 불법정보의 유통으로 피해자 권리침해 문제가 심각해지면서 불법정보에 대한 실효적인 유통 방지가 중요해짐과 동시에, 인터넷상 표현의 자유 증진에 대한 사회적 요구가 증가함

※ 불법촬영물 등 경찰 수사 급증('17년 6,465건), 온라인 불법저작물의 시장침해 규모 2조 5,646억원('17년), 온라인 불법도박의 시장규모는 47조원('15년)

○ (정책적 요구) 해외사이트를 통한 불법정보 유통 방지를 위해 도입된 기술적 조치†로 인해 제기된 국민정서와 인터넷규제 간의 간극을 해소 필요

- SNI 차단조치('19.2.11)에 반대하는 국민청원이 26만 건을 돌파하는 등 음란물을 포함한 인터넷상 표현의 자유 증진에 대한 요구와 불법정보 유통 방지 기술적 조치 도입 과정에서 국민 공감대 형성에 미흡했다는 의견 확대
- 인터넷 규제의 바람직한 방향과 적정한 수준에 대한 사회적 공론화 및 이를 통한 국민적 공감대 형성 필요

○ (목표) 이러한 사회적·정책적 요구를 반영하고 불법정보 유통방지를 위한 기술적 조치 도입의 절차적 보완방안을 마련하기 위해, 사회적 논의기구인 "인터넷 규제개선 공론화 협의회"를 구성·운영하여 불법정보 유통방지 관련 제도 개선 방안을 도출하는 데에 본 연구의 목표가 있음

제 2절 연구의 방법과 구성

○ 본 연구는 국민정서에 부합하는 인터넷 규제 개선방안 마련이라는 연구 목표 달성을 위해 '인터넷 규제개선 공론화 협의회('19. 6. 13. 발족)' 협의회의 원활한 운영을 지원

하여 인터넷상 표현의 자유보장과 해외 불법사이트 차단이라는 공익 간의 적절한 균형을 고려한 인터넷 규제 개선 방안을 모색함

- 이를 위해 불법정보 유통현황 및 관련제도를 분석하고, 접속차단 조치에 대한 여론 자료를 취합 및 분석하여 접속차단 조치를 계기로 제기된 주요 쟁점을 도출함
- 인터넷규제개선공론화협의회는 도출된 쟁점을 검토하여 사회변화와 국민정서에 부합하는 제도 개선방향을 제시함

제 2 장 불법정보 유통 현황 및 관련제도 분석

제 1절 불법정보의 범위와 유통현황

1. 불법정보의 범위

○ (적용범위) 「정보통신에 관한 심의규정」 제3조(적용범위)[1]에 근거하여 '정보통신망을 이용하여 일반에게 공개되어 유통하는 정보'로서, 국내에서 유통되는 경우에 적용하고 있음

○ (종류) 불법정보는 실정법(형법, 정보통신망법, 성폭력처벌법, 청소년성보호법 등)에 위배되는 정보로서, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "정보통신망법") 제 44조의7이 각 실정법에서 정의한 불법정보를 받아 재정의하고 있음

- 정보통신망법 제44조의 7[2]은 불법정보의 종류를 음란, 명예훼손, 사이버스토킹, 해킹/바이러스 유포, 청소년 유해매체물 표시의무 위반, 도박 등 사행행위, 개인정보거래, 국가기밀누설, 국가보안법 위반, 범죄관련정보 등의 9가지 유형으로 규정

<표 2-3> 정보통신망법 제 44조의 7에 따른 불법정보의 범위

구분	주요 내용
제1호 (음란)	음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공연히 전시하는 내용의 정보
제2호 (명예훼손)	사람을 비방할 목적으로 공연히 사실 또는 허위의 사실을 적시하여 타인의 명예를 훼손하는 내용의 정보
제3호 (사이버스토킹)	공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하게 하는 내용의 정보

1) 「정보통신에 관한 심의규정」 제3조(적용범위) ① 이 규정은 정보통신망을 이용하여 일반에게 공개되어 유통되는 정보에 한하여 적용한다.
② 이 규정은 국외에서 제공되는 정보라도 국내에서 일반에게 공개되어 유통되는 경우에는 적용한다.

2) [법률 제16825호, 2019. 12. 10., 일부개정안] [시행 2020. 6. 11.]

제4호 (해킹, 바이러스 유포)	정당한 사유없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
제5호 (청소년유해매체물 표시의무 위반)	「청소년보호법」에 의한 청소년유해매체물로서 상대방의 연령확인, 표시의무 등 법령에 의한 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
제6호 (도박 등 사행행위)	법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
제6호2호 (개인정보 거래)	이 법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보
제6호3호 (총포・화약류)	총포 · 화약류(생명 · 신체에 위해를 끼칠 수 있는 폭발력을 가진 물건을 포함한다)를 제조할 수 있는 방법이나 설계도 등의 정보
제7호 (국가기밀 누설)	법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
제8호 (국가보안법 위반)	국가보안법에서 금지하는 행위를 수행하는 내용의 정보
제9호 (범죄관련 정보)	그 밖에 범죄를 목적으로 하거나 교사 또는 방조하는 내용의 정보

2. 불법정보 유통 현황

○ (유통 양상) 미디어환경의 변화로 인해 소셜미디어나 해외 플랫폼, 웹하드 등을 통해 불법정보의 유통이 더욱 빠르고 광범위하게 이루어지고 있으며, 특히 국내법의 적용을 받지 않는 해외 인터넷 사업자를 통한 불법정보 유통이 증가하고 있음

- 방송통신심의위원회는 지난해 인터넷을 통해 유통되는 불법·유해정보 23만8천246건에 대해 삭제 및 차단 등 시정요구를 의결했는데, 이는 2016년(20만1천791건)보다도 20%가량 늘어난 상황임
- 특히 시정요구 중 '해외 불법정보에 대한 국내 접속차단'이 18만7천980건으로 전체의 78.9%를 차지하여, 국내법의 규제 및 단속을 회피해 불법정보를 유통하는 수단으로 해외 웹서비스가 악용되고 있는 상황

※ (다크웹) 아동대상 성범죄 영상공유사이트의 운영자가 한국인이었고, 검거된 이용자 338명 중 223명(71.9%)가 한국인인 등 해외에 서버를 두는 형태로 국내이용자를 대상으로 불

법적인 정보를 제공하는 행위가 확산되고 있음

❍ (한계) 국경이 없는 서비스인 인터넷서비스의 발전으로 인해 한 국가의 규제 관할권의 범위 밖에 서버를 두고 있는 해외 불법사이트를 경유하여 국내로 유통되는 불법유해정보 유통방지의 어려움이 증가하고 있음

- 불법 및 음란의 기준† 이 나라마다 다르기 때문에 해외사업자의 정보통신서비스에 게시된 게시물이나 게시글을 개별적으로 필터링하거나 삭제를 강제할 수 없으며 국제공조를 통한 국내법 집행에도 한계

  † 아동포르노와 강간물을 제외하고 성기 노출 등 직접적인 성행위 묘사는 나라에 따라 합법인 경우도 존재하기 때문에 국가간 공조에도 제한

- 인터넷 서비스에 대한 행정규제는 사업자 스스로 이행하여야 하고 다른 제3자가 임시조치를 대행하기 어려우므로 해외 사업자가 자발적으로 법적의무를 준수하지 않을 경우 불법정보 유통과 그로 인한 피해 방지가 어려움

  ※ 텀블러 사례: 2017. 8. 방송통신심의위원회는 인터넷 음란물이 상당히 게시되어 있는 텀블러(Tumblr)에 대하여 '불법콘텐츠 대응에 대한 협력'을 이메일로 요청하였으나, 텀블러 측은 2017. 8. 말 방송통신심의위원회의 협력 요청을 거부하고, "텀블러는 미국 법에 의해 규제되는 미국회사이며, 대한민국에 물리적 사업장을 두고 있지 않으며 대한민국의 사법관할권이나 법률 적용을 받지 않는다"고 회신한 사건

- 해외사업자의 경우 행정조사, 처분 문서의 송달, 의견 제출 또는 청문의 진행 등 행정절차 진행에 어려움이 많아 규제집행이 불가능한 경우가 있다는 문제점이 지적됨

제 2절 불법정보 유통 방지 제도의 현황

1. 정보통신서비스 제공자 및 이용자의 책무

○ (불법정보 유통금지 책무) 정보통신망법은 정보통신망을 통한 불법 정보의 유통을 금지하는 책무를 정보통신서비스 제공자 및 이용자의 책무를 부여

- 제2조에 정의된 정보통신서비스 제공자에게 제3조 1항에 따라 건전하고 안전한 서비스를 제공하여 이용자의 권익보호에 이바지해야하는 책무를 부여하고, 제3조 2항에 따라 이용자에게도 또한 건전한 정보사회의 정착을 위해 노력할 책무를 부여

  ※ 제3조(정보통신서비스 제공자 및 이용자의 책무)

  ① 정보통신서비스 제공자는 이용자의 개인정보를 보호하고 건전하고 안전한 정보통신서비스를 제공하여 이용자의 권익보호와 정보이용능력의 향상에 이바지하여야 한다.

  ② 이용자는 건전한 정보사회가 정착되도록 노력하여야 한다.

  ③ 정부는 정보통신서비스 제공자단체 또는 이용자단체의 개인정보보호 및 정보통신망에서의 청소년 보호 등을 위한 활동을 지원할 수 있다.

- 제44조의 7에서는 누구든지 정보통신망을 통하여 불법정보를 유통하여서는 아니된다고 정의하여 정보통신서비스제공자와 이용자 모두에게 책무를 부여하고 있음

  ※ 제44조의7(불법정보의 유통금지 등) ① 누구든지 정보통신망을 통하여 다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.

2. 통신심의-시정요구-시정명령의 체계

○ (통신심의) 독립기구인 방송통신심의위원회가 「방통위설치법」 제21조(심의위원회의 직무) 및 동법 시행령 제8조(심의위원회의 심의대상 정보 등)에 따라 심의

- 정보통신망으로 유통되는 불법정보는 방심위의 통신심의 절차를 거치게 되며, 대부분 통신심의소위원회에서 의결되나, 사안에 따라 전체회의에서 상정될 수 있음

- 심의의 시작은 심의대상을 인지하는 단계부터 시작하고, 이는 이용자의 신고나 자체

모니터링, 또는 타기관의 요청을 통함

- 인지된 심의대상은 확인 및 구분절차를 거쳐 안건이 상정되는 심의부서 검토 절차를 거친 후, 통신·권익보호특별위원회의 자문을 거쳐 통신심의소위원회의 심의로 상정되어 처리됨

〈표 2-4〉 방송통신심의위원회 통신심의 절차 및 내용

통신심의 절차	절차별 내용
심의대상 인지	• 이용자 신고† • 방심위 자체 인지/모니터링 • 타기관 요청
심의부서 검토	• 심의대상 확인 및 구분 • 안건 작성 및 상정
특별위원회 자문	• 통신·권익보호특별위원회 자문
위원회 심의	• 통신심위소위원회 전체회의 심의·의결 - 시정요구(삭제, 이용해지, 접속차단 등 의결) ※ 당사자 의견진술 사전 청취
심의결과 처리	• 요청기관 등에 심의결과 통보 • 해당 업체에 심의결과 통보

† 불법유해정보의 신고는 방심위, 경찰청, 개인정보침해신고센터 및 각 포털 고객센터로 신고

○ (시정요구) 방통위법 시행령 제8조제2항에 따라, 정보통신망법 제44조의 7에 해당하는 불법정보의 심의 결과를 근거로 정보통신서비스제공자 또는 게시판 관리·운영자에 대해 시정요구가 가능함

- 시정요구의 종류에는 '해당 정보의 삭제', '접속 차단', 혹은 이용자에 대한 '이용정지' 또는 '이용해지', 청소년유해정보 표시가 있음

- 사업자는 시정요구를 받은 15일 이내에 심의위원회에 시정요구에 대한 이의신청을 할 수 있음

○ (시정명령) 정보통신서비스제공자 또는 게시판 관리·운영자가 방송통신심의위원회의 시정요구에 따르지 않을 경우 방송통신위원회가 해당 사업자에 대하여 불법정보에 대한 취급 거부·정지 또는 제한하도록 명령할 수 있음

- 방통위는 망법 제44조의 7에 근거하여 정보통신서비스 제공자에게 해당 정보의 취급 거부 및 정지를 요청하거나 행정제재를 시행할 수 있음

<표 2-5> 통신심의 결과의 처리 절차와 주체

구분	절차	내용
방송통신심의 위원회	심의	망법 제 44조의 7에 규정된 사항의 심의 및 대통령령이 정하는 사항의 심의
	제재요청	망법 제 44조의 7 소정의 불법정보 유통에 대한 취급의 거부·정지 또한 제한조치 결정 및 제재 요청
	시정요구	방통위 설치법 시행령 제8조제2항 1. 해당정보의 삭제 또는 접속차단 2. 이용자에 대한 이용정지 또는 이용해지 3. 청소년 유해정보의 표시의무 이행 또는 표시방법 변경 등과 그 밖에 필요하다고 인정하는 사항
방송통신 위원회	제재조치 명령	취급의 거부 및 정지

○ (정보의 삭제 및 임시조치) 정보통신서비스제공자는 망법 제 44조의 2와 3에 근거, 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 정보의 삭제 및 임시조치 등을 취할 수 있음

<표 2-6> 정보통신망법상 불법정보 유통방지 조치의 법률 조항

관련법령	규제 근거
제 44조의 2(정보의 삭제요청 등)	① 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우 그 침해를 받은 자는 해당 정보를 취급한 정보통신서비스 제공자에게 침해사실을 소명하여 그 정보의 삭제 또는 반박내용의 게재(이하 “삭제등“이라 한다)를 요청할 수 있다. ② 정보통신서비스 제공자는 제1항에 따른 해당 정보의 삭제등을 요청받으면 지체 없이 삭제·임시조치 등의 필요한 조치를 하고 즉시 신청인 및 정보게재자에게 알려야 한다. 이 경우 정보통신서비스 제공자는 필요한 조치를 한 사실을 해당 게시판에 공시하는 등의 방법으로 이용자가

	알 수 있도록 하여야 한다. ③ 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 제42조에 따른 표시방법을 지키지 아니하는 청소년유해매체물이 게재되어 있거나 제42조의2에 따른 청소년 접근을 제한하는 조치 없이 청소년유해매체물을 광고하는 내용이 전시되어 있는 경우에는 지체 없이 그 내용을 삭제하여야 한다. ④ 정보통신서비스 제공자는 제1항에 따른 정보의 삭제요청에도 불구하고 권리의 침해 여부를 판단하기 어렵거나 이해당사자 간에 다툼이 예상되는 경우에는 해당 정보에 대한 접근을 임시적으로 차단하는 조치(이하 “임시조치“라 한다)를 할 수 있다. 이 경우 임시조치의 기간은 30일 이내로 한다.
제 44조의 3 (임의의 임시조치)	① 정보통신서비스 제공자는 자신이 운영·관리하는 정보통신망에 유통되는 정보가 사생활 침해 또는 명예훼손 등 타인의 권리를 침해한다고 인정되면 임의로 임시조치를 할 수 있다.

3. 불법정보 유통방지를 위한 기술적 조치

[그림 2-1] 불법·유해정보(사이트)에 대한 차단 페이지 (URL차단방식)

○ (접속차단 조치) 접속차단이란 해외사이트에 의한 불법정보의 국내 유입을 막기 위해 실시되는 조치로, 실무적으로는 시정 요구 및 명령 등 행정 제재가 용이하지 않은 해외사업자의 사이트 전체에 대한 접근을 막는 방식으로 운영되고 있음(최진응, 신용

우., 2019. 4. 29)

○ (기존의 접속차단 방식) 불법정보 유통 사이트에 이용자의 접근을 차단하기 위해 사이트의 IP주소 차단, DNS 차단, URL 차단 방식이 시행됨

- IP 차단 방식은 사이트에 해당하는 IP 주소를 직접 차단하는 방식이며, DNS 차단방식은 클라이언트가 해당 사이트의 IP를 확인하기 위해 DNS에 접속할 때 이를 차단하여 접속차단페이지로 이동시키는 방식이며, URL차단 방식은 도메인(domain)과 IP단위뿐만 아니라 하위 디렉토리 및 페이지 단위까지 차단하는 방식을 의미

- 그러나 이러한 기존의 접속차단 방식으로는 사이트 주소(URL)가 암호화되는 보안프로토콜 (https†)을 이용할 경우 불법정보임에도 불구하고 차단을 시행할 수 없다는 한계가 존재

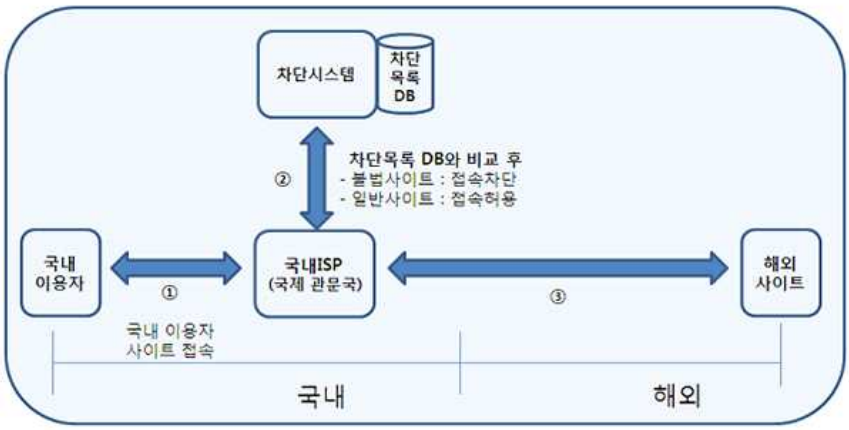
† HyperText Transfer Protocol over Secure Socket Layer의 약어로, 인터넷에서 감청 위협으로부터 데이터를 안전하게 보호하기 위해 전송되는 데이터를 암호화하여 송수신하는 프로토콜

※ 전체 웹 트래픽 중 보안접속(https)은 50%이상으로, 비중이 계속 증가할 것으로 예상('시스코 2018 연례 사이버 보안 보고서', '17. 10월 기준)

○ (SNI필드영역을 활용한 기술적 조치) 기존 접속차단 방식을 실시할 수 없었던 보안접속(https)을 활용하는 해외 불법사이트에 대해서도 IP주소를 확인하고 접속차단을 실시 할 수 있어, 효율적인 불법정보 유통방지 대안으로 '19년 2월 방송통신위원회가 도입

- SNI(Server Name Indication) 필드 영역을 활용한 접속차단이란, HTTPS통신이라도 최초 연결시(Hand Shake) 사용자가 접속하려는 서버 주소(호스트이름) 부분만 암호화되어 있지 않아서 이를 인식하여 필터링 하는 방식

[그림 2-5] 접속차단 조치의 개념도



출처: 방송통신위원회(2019)

- 방심위에서 심의한 불법정보 차단목록(예:sex.com)과 SNI 필드의 서버 네임(예: sex.com)이 일치하면 통신사업자가 차단 시스템에서 이용자의 해당 사이트 접속을 차단하는 기계적 방식의 접속차단조치임

제 3절 접속차단 조치 도입의 주요 쟁점 분석

1. 쟁점분류

○ 새로 도입된 접속차단 조치 관련 여론(민원, 언론보도, 인터넷게시글 등)자료를 취합·분류

- 불법정보 유통방지를 위한 기술적 조치가 시행된 이후(2019. 2. 11.~ 8. 6.)까지 국민신문고에 접수된 국민청원 및 제안, 민원, 언론보도와 인터넷 게시글을 취합·분석하고 주제별 관련성에 따라 5가지 쟁점† 으로 분류

† 접속차단 기술의 실효성, 이용자 권리침해 여부, 불법정보 유통방지를 위한 대안, 기술적 조치 도입절차의 투명성, 기술적 조치와 관련된 법·제도 검토 등

○ 도출된 쟁점별로 여론자료 분석결과, 관련 시민단체와 전문가 의견청취 결과 등을 취합·요약하여 정리함

2. 접속차단 조치의 효과성 관련

○ 여론자료 분석결과, 접속차단 조치의 효과성과 관련해서 4개의 하위 쟁점이 도출

- (서비스 제공자에 의한 우회) 불법사이트 제공자가 접속차단을 우회해서 국내 이용자들에게 서비스를 제공할 수 있다는 우려

- (서비스 이용자에 의한 우회) 국내 인터넷 이용자가 현재의 접속차단 조치를 우회할 수 있는 우회기술과 방법들이 있다는 우려

- (기술변화에 따른 효과) 새로운 보안통신기술의 발전으로 인해 새로 도입된 기술적 조치의 효과가 경감될 것이라는 우려

- (접속환경에 따른 효과) 접속환경이나 ISP에 따라 불법사이트의 차단 효과가 다르다는 우려

가. 서비스 제공자에 의한 우회

○ 접속차단 조치에도 불구하고 불법사이트 제공자가 도메인을 변경하여 우회제공이 가능하다는 주장이 제기되었음

- 불법정보의 인지-심의-시정요구-시정명령에 이르는 절차가 약 2주 정도 걸리는 점을 악용*하여, 불법정보의 제공자가 불법사이트의 도메인 변경 등을 통해 손쉽게 접속차단 조치를 우회할 수 있다는 우려가 제기되었음

- 불법사이트 운영자가 사이트 주소에 숫자를 붙이거나 연관된 사이트 명칭으로 변경하는 등, 사이트 주소 변경을 통해 접속차단을 우회하는 경우들이 발생하고 있음

  * 차단된 웹사이트의 주소에 연속되는 아라비아 숫자를 붙이거나, 색상을 나타내는 단어들을 변경하여 붙이는 등의 연관어를 이용하여 주소를 변경하는 방식

- 불법사이트 운영자들이 공개된 커뮤니티 게시판, 공개된 SNS계정, 또는 일반 웹사이트에서 변경된 주소를 공유하는 방식으로 불법사이트의 접속을 유도하는 일들이 발생하고 있음

  * 이용자들에게 소셜네트워크 사이트, 별도의 웹사이트, 인터넷 커뮤니티 게시판 등을 이용하여 불법사이트의 변경된 주소를 공지하여 접속을 유도하는 행위([그림 2-3] 참조)

[그림 2-6] 제3의 웹사이트를 통해 불법사이트의 변경된 주소 공유 사례

○ 접속차단 우회를 방지하기 위해 불법사이트의 변경주소를 사전에 예측하여 차단하거나, 통신심의 절차를 간소화하여 불법사이트의 차단 실효성을 높이자는 주장이 있음

- 불법사이트 운영자가 주소를 변경할 것을 경험적으로 예측할 수 있기 때문에, 변경할 것으로 예측되는 주소들을 선제적으로 차단하고 이후에 심의하는 선차단 후심의가 가능하다는 의견도 제시됨

- 그러나 접속차단 조치는 이미 발생한 불법정보 확산을 방지하기 위해 행해지는 조치로서, 서비스 제공자가 변경할 것으로 예상되는 예측가능한 사이트 주소를 사전에 차단하는 것은 과잉규제의 우려가 있다는 지적이 있음

- 또한 방통위 설치법에 따라 합의제 기구로서의 특성을 부여 받은 방송통신심의위원회는 통신내용의 불법성을 개인이 판단하지 않고, 심의위원들의 합의에 근거하여 판단하도록 하고 있음

- 따라서 통신심의를 거치지 않은 선차단 조치를 시행하는 것은 정보제공자 및 게시자, 일반 인터넷 이용자의 표현의 자유와 정보접근권이 제한될 우려가 있어 임의 차단은 바람직하지 않다는 것이 일반적인 의견임

○ 불법사이트 모니터링을 강화함으로써 불법사이트 제공자가 사이트 주소를 변경하여 접속차단을 우회하는 행위를 방지할 수 있음

- 현재 방송통신심의위원회는 긴급한 조치가 필요한 불법정보의 확산 방지를 위해 집중 모니터링을 실시하는 등 불법사이트의 모니터링을 강화하고 있음

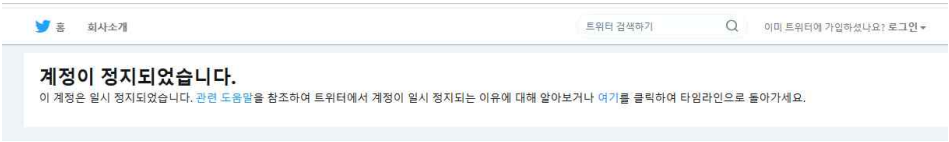
○ 이외에도 불법행위를 조장하는 게시물이나 게시자에 대해 SNS 플랫폼 운영자와 인터넷 이용자의 자율적인 정화 노력을 유도하여, 서비스 제공자의 접속차단 우회 행위를 방지할 수 있음

- 방송통신심의위원회는 국내 이용자가 사용하는 일부 해외 SNS 사업자들에게도 불법사이트 주소 정보나 홍보글 등의 게시물에 대해 해당정보의 삭제, 이용자에 대한 이용

정지 또는 이용해지, 청소년 유해정보 표시 등의 시정조치를 요구하고, 국내법 적용을 강제할 수 없는 한계를 보완하기 위해 자율심의 협력 시스템 참여를 독려하고 있음

※ 일례로 해외 SNS사업자인 트위터가 대표적인 불법 웹툰사이트의 변경주소를 공유하던 계정에 대해 운영원칙 위배를 이유로 계정을 일시 정지한 바 있음([그림 2-5]참조).

[그림 2-7] 불법사이트 접속정보를 제공하는 트위터 계정의 삭제 후 모습



나. 서비스 이용자에 의한 우회

○ 서비스 이용자가 우회프로그램을 이용하거나 전송 크기를 조정하는 등 우회기술들을 사용하면 현재에도 접속차단 조치를 우회할 수 있다는 우려가 제기 되었음

- 접속차단 조치를 우회할 수 있는 방법들로 인터넷 이용자들 사이에서 웹 프록시(proxy) 서버 이용, VPN이용, MTU 조정(TCP packet fragmentation), ESNI를 지원하는 브라우저 이용 방법 등의 정보가 공유되고 있음

- VPN이나 웹프록시를 사용한 '차단우회 어플' 등의 다운로드 건수가 점차 증가하고 있어, 접속차단의 효과가 경감될 것이라는 우려가 있음

※ 대표적인 차단우회어플로 알려진 '유니콘'의 경우 월평균활성이용자수(MAU)가 안드로이드에서 18만3천명, iOS에서 6만6천명(APP APE 기준, 2019년 5월 기준)으로 알려짐

○ 해외 웹 프록시(proxy) 서버를 이용할 경우 DNS 통신을 익명화하여 접속제한을 우회할 수 있다고 알려져 있으나, 웹프록시 서버를 사용할 경우 접속속도와 품질 저하 등의 문제가 있어 일반화되지는 않을 것이라는 지적이 있음

- 웹 프록시 서버는 클라이언트와 서버 사이를 중계하는 특수한 서버로서, 클라이언트가 도메인 네임을 입력하면 프록시 서버가 클라이언트를 대신하여 서버에 IP주소를 요청하고 서버로부터 웹사이트의 정보를 전송받아 캐시로 저장하여 클라이언트에 제공

하는 방식

- 웹 프록시 서버는 네트워크에서 다른 서버로의 자원요청을 중계하기 때문에 클라이언트의 지역 정보를 익명화하고 프록시 서버가 있는 지역에서 접속한 것으로 인식될 수 있어, 지역에 한정된 접속제한 등을 우회할 수 있음

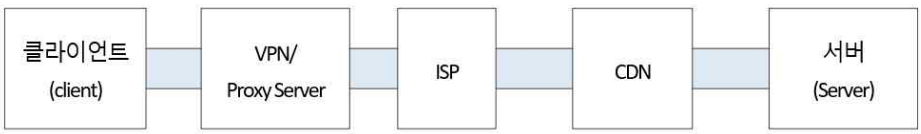
- 따라서 해외 웹 프록시 서버를 사용하게 되면 사용자 IP의 지역정보를 암호화 할 수 있기 때문에, 인터넷 사용자들 사이에서 웹 프록시 서버를 이용하여 SNI접속 차단을 우회할 수 있다고 알려져 있음

- 그러나 일반적인 인터넷 사용자들 사이에 공유되는 웹 프록시 서버들은 대부분 접속 속도와 품질이 떨어진다는 한계를 가지고 있으며, 특히 동영상 등의 스트리밍 서비스를 이용하기에 적합하지 않을 정도로 접속 속도와 품질이 떨어지는 경우가 많음

- 또한 웹 프록시 제공 사이트 내에서 정보를 이용해야한다는 문제가 있고, 유료 프록시 사이트의 경우 비용 상의 부담이 발생하며, 대부분의 무료 웹 프록시 서버들은 팝업 광고 등으로 인한 이용 상의 불편함이 있다는 지적이 있음

○ VPN(Virtual Private Network)도 웹프록시와 마찬가지로 클라이언트와 서버의 통신을 중계할 뿐만 아니라 DNS 통신과정을 익명화하여 접속제한을 우회할 수 있다고 알려져 있으나, 일반 인터넷 이용자들 사이에서 일반적으로 사용될 수준의 전송속도와 품질이 보장되는지에 대해서 전문가들의 부정적인 시각이 많음

[그림 2－8] In-path방식(VPN과 웹프록시 서버)의 개요도



- 첫째, 이용자가 불법사이트 접속을 위해 VPN을 사용할 경우 동영상을 시청하기에는 적합하지 않은 속도저하를 야기할 수 있다는 지적이 있음

※ VPN 서비스를 이용할 경우 사용자의 위치정보를 암호화 하기 위해 VPN 서버라는 중간 거점을 거치기 때문에 인터넷속도가 저하될 수밖에 없으며, 이로 인해 특히 음란물 등의 불법동영상 등에 적용되기 어려움

- 둘째, 무료 VPN 프로그램을 사용할 경우 해킹에 취약하여 위치정보, 접속기록 등 개인정보 유출 가능성이 높고, 일부 VPN제공업체는 과도한 개인정보를 수집할 수 있는 권한을 요청하는 등 개인정보 유출 등의 문제가 있다는 지적이 있음

  * 안드로이드 기기에 제공되는 VPN앱 중 60% 정도가 1개 이상의 과도한 사용자 데이터나 별도의 사용자 허가가 필요한 앱 접근권한을 요청하는 등, 개인정보 보호가 취약할 수 있다는 지적이 있으며(Cimpanu, 2019. 3. 4.), 인터넷이용자들 사이에서도 VPN을 켠 상태에서 신용카드를 쓰거나 아이디 로그인을 하는 등의 개인정보 유출이 가능한 활동을 하지 말라는 정보 등이 공유되고 있음

- 특히, 개인정보보호 규정이 약한 해외에서 제공되는 VPN프로그램을 사용할 경우 포르노사이트를 포함한 콘텐츠 서비스 업체, 인터넷 회선을 제공하는 해외통신사업자 등에게 사용자의 온라인 행동정보가 제공될 우려가 높아짐

- 셋째, 유료 VPN을 사용할 경우 비용이 발생하기 때문에, 일반적인 인터넷 이용자들에게는 가용성이 떨어진다는 지적이 있음

○ 초기 메시지(Client Hello)의 패킷값을 쪼개어 보내는 방식으로 MTU값*을 조정하는 TCP fragmentation**으로 접속차단을 우회할 수 있다는 주장이 제기됨

  * MTU(Maximum Transmission Unit)는 한번에 전송하는 패킷의 최대 단위를 의미함

  ** 사용자가 접속차단된 도메인 주소를 잘게 쪼개어 전송하여 접속차단을 우회하는 방식

- 전송하는 패킷의 최대 전송 단위를 조정(MTU값 조정)하여 사용자가 패킷을 쪼개서 접속차단의 대상이 되는 불법사이트의 IP주소를 분할하여 전송할 경우 접속차단을 우회할 수 있다는 주장임

- TCP fragmentation에 대해서는 소프트웨어나 하드웨어 업데이트를 통해서 우회접속을 방지하는 것이 가능하다는 전문가 의견이 있음

○ 반면, 다양한 우회접속을 하는 방법들이 인터넷 이용자들 사이에서 공유되고 있으나, 우회접속 앱을 활용하거나 TCP fragmentation을 활용한 인터넷 접속이 일반적인 인터넷 접속방식으로 활성화될 것으로 예상하지 않는다는 전문가들의 의견도 있음

- 다만 VPN이나 웹프록시, TCP fragmentation 사용현황에 대한 국내 통계 및 조사 등이 이뤄지고 있지 않아 실태를 파악하기 어려운 한계가 있음

- 또한 인터넷 이용자가 VPN이나 웹프록시를 사용하는 앱이나 프로그램을 사용한다고 하더라도 이용자가 반드시 불법사이트에 접속하기 위한 목적이 아닐 수도 있어 실태조사가 필요함

※ 유튜브 프리미엄 서비스 등 IP주소정보를 이용해 지역별로 서비스 요금이 다르거나 지역 제한이 있는 상업적 서비스를 활용하기 위해 VPN이나 웹프록시를 사용하는 현상이 나타나고 있음(김정민, 2020. 1. 5).

다. 기술변화에 따른 효과

○ 인터넷 통신기술이 보안통신을 강화하는 방향으로 발전하고 있어, 접속차단 기술의 불법정보 유통 방지 효과가 경감될 것이라는 우려가 제기됨

- 사용자 단말과 서버 간의 통신보안이 강화되면 평문으로 전송되던 SNI필드 정보가 암호화되어, 현재와 같이 SNI필드의 암호화되지 않은 주소정보를 확인하고 불법사이트의 접속을 차단하는 기술적 조치를 적용하기 어려워질 것이라는 주장이 제기됨

※ IETF(I(Internet Engineer Task Force, 이하 IETF)의 새로운 통신 프로토콜인 TLS 1.3(The Transport Layer Security Protocol Version 1.3, RFC8446)† 에 SNI필드 정보까지 암호화하는 규격이 포함되어 있기 때문에 네트워크 레벨에서 IP주소를 확인해서 차단하는 방식이 적용될 수 없을 것이라는 내용이 인터넷 사용자들 사이에서 공유되고 있음

† TLS(Transport Layer Security): 사용자의 단말과 서버간의 통신에서 도청, 변조, 메시지 위조를 방지하기 위한 암호화 프로토콜로서, 현재는 TLS1.2가 사용되고 있으며, 2018년 8월 28일에 TLS 1.3 (RFC 8446)이 발표됨

- 이미 애플, 클라우드플레어, 모질라 등에서 TLS 1.3을 전제로 한 확장규격으로서의 암호화된 SNI(ESNI) 규격의 초안을 마련하는 등 SNI정보의 암호화 기술에 상당한 진전이 있어 현재에도 접속차단의 효과가 제한적이라는 주장이 제기됨

- 특히 구글크롬과 모질라파이어폭스 등 일반인터넷이용자들이 사용하는 주요 브라우저들도 도메인네임시스템(DNS) 통신 암호화를 위해 DoH(DNS over HTTP)를 도입하고 있어, SNI필드 정보를 확인하여 접속을 차단하는 기술적 조치의 효과가 경감된다는 주장이 제기됨

○ TLS 1.3에서도 SNI필드 정보를 확인하여 접속차단을 하는 현행의 접속차단 방식은 불법사이트 접속차단을 위한 기술방식으로서 유효하다는 것이 전문가들의 의견임

- 현행 접속차단 방식은 사용자 단말에서 서버로 전달되는 초기메시지(ClientHello) 에서 서버네임(server name)을 확인하여 불법사이트를 기계적으로 자동차단하는 방식으로, TLS 1.3에서도 사용자 단말에서 서버로 가는 초기메시지(ClientHello)는 암호화되지 않음

- TLS 1.3 표준논의에서 초기메시지 부분인 SNI필드데이터의 암호화는 포함되지 않았으며, 인증이 완료된 후의 클라이언트와 웹서버 사이의 통신이 암호화되는 것이지 인증과정의 통신은 암호화되지 않음

- 웹브라우저의 경우 최신버전의 크롬, 파이어폭스, 사파리 등에서 TLS 1.3을 적용하고 있으나, 아직까지 사용자가 직접 TLS 1.3을 활성화한 경우에만 적용되고 있음. 특히 TLS 1.3을 브라우저의 기본값(default)으로 설정할 경우 TLS 1.2가 적용된 웹사이트와 완벽하게 호환이 된다고 보장할 수 없기 때문에, 아직까지 이들 브라우저 이용자들 사이에서도 TLS 1.3의 활성화가 일반적이지는 않을 것으로 추정하고 있음

  ※ 미국의 CDN(content delivery network)/DNS(domain name server) 제공업체인 클라우드플레어(cloudflare)가 TLS 1.3을 적용하고 있으나, TLS 1.3 채택이 일반적이지 않은 상황임

○ TLS 1.3을 전제로 SNI필드 정보를 암호화하는 ESNI(Encrypted SNI) 기술개발이 이뤄지고 있으나, 통신환경과 기술채택의 속도를 고려할 때 ESNI가 일반화되는 데

에는 상당시간이 소요될 것으로 전망됨

- 일부 벤더(클라우드 플레어, 모질라 등)에 의해서 SNI필드데이터를 암호화하는 ESNI 초안(draft)이 개발되었으나, 아직까지 ESNI구현이 초안 수준이고 TLS 1.3에 필수적으로 적용되는 규약이 아님

- ESNI 기술을 활용하여 접속차단을 우회하기 위해서는 웹브라우저와 서버 모두에서 TLS 1.3이 적용되어야 하는데, 현재는 웹브라우저나 호스팅 서비스에서 TLS 1.3의 채택이 일반적이지 않음

- 사용자들이 ESNI기술이 적용된 브라우저를 사용하더라도 불법정보를 제공하는 사이트도 ESNI 기술을 적용하여 구축되어야만 불법사이트 접속이 가능하므로, ESNI를 통한 불법사이트 우회접속이 단기간에 확산될 가능성은 낮은 편임

- 특히 다크웹이나 불법사이트 서버 측에서 ESNI를 적용한 서버를 채택해야하고 사용자 단말에서도 ESNI기술을 적용한 브라우저에서 ESNI를 활성화해야하는데, 다크웹이나 불법사이트의 경우 서버 변경이 잦은 등 운영안정성이 상대적으로 낮아 단기적으로 ESNI로 인한 불법사이트 우회접속이 일반적인 현상이 될 가능성은 낮은 것으로 평가됨

○ 접속차단의 효과 평가를 위해서는 현행 접속차단 조치의 효과를 경감할 수 있는 관련 기술의 개발 및 채택 동향에 대한 신뢰할만한 분석 자료와 사용 실태 파악이 필요함

- 다크웹이나 불법사이트의 경우 일반적으로 안정성(reliability)이 낮아 ESNI채택률 등의 실태조사가 쉽지 않고 도메인 특징상 정보를 파악하기 어렵다는 한계가 있음

- 간접적으로 SNI차단 정책 이전과 이후를 기준으로 파이어폭스와 같은 브라우저의 사용점유율이나 VPN, Tor 네트워크 사용자 변동률을 확인할 수 있다고 주장하고 있으나, 해당 이용률에 대한 공인된 통계자료도 부족한 현황

- 따라서 지속적으로 관련기술의 개발 및 채택에 대한 신뢰할만한 자료 수집이 필요함

라. 접속환경에 따른 효과

○ 새로운 접속차단 조치 도입 이후, 인터넷 게시글 등에서 접속가능한 사이트와 접속이 가능하지 않은 사이트에 대한 정보가 게재되었으며 이 과정에서 접속환경이나 ISP에 따라 접근 가능한 사이트가 다르거나 차단시점이 다르다는 의견이 제기되었음

- 접속차단된 해외 불법 사이트 중 일부가 접속차단이 해제되었다거나 특정 ISP에서는 접속차단된 해외 불법 사이트에 접속이 가능하다거나 하는 의견이 게재됨

○ 방송통신위원회와 방송통신심의위원회가 사실확인 결과(방송통신위원회·방송통신심의위원회, 2019. 2. 28), 접속차단된 해외 불법 사이트 중 일부가 접속 차단이 해제되었다는 것은 사실이 아님을 확인함

- 다만 ISP사업자 중에서 KT가 방송통신심의위원회가 요청한 접속차단 사이트 목록 외에 기존 URL 차단방식을 적용하던 대상목록의 사이트까지 차단하였다가 이를 정정하는 과정에서 접속환경에 따라 차단되는 사이트가 다르다는 오해가 발생됨

- KT는 해당 사실 인지 후 요청받은 사이트에 대해서만 SNI 접속차단이 적용되도록 변경하였으며, 현재 ISP에 상관없이 동일 불법사이트에 대해서 접속차단이 이뤄지고 있음

○ 새로운 차단방식의 기술특성상 이용자가 차단된 불법 인터넷사이트 접속을 시도할 때 해당 사이트의 화면이 암전(black out) 상태로 표시되며 「해당 사이트는 불법으로 접속이 불가능하다」는 불법·유해정보 차단안내(warning.or.kr)나 경고문구가 제공되지 않아, 사용자 입장에서 특정 사이트에 접속할 수 없을 경우 접속차단 때문인지 인터넷 접속이 원활하지 않기 때문인지 확인할 수 없다는 기술적 한계가 있음

3. 인터넷이용자의 권리와 보호

○ 인터넷이용자의 권리에 대해서는 공공복리와 개인권익에 대한 상반된 시각이 공존하고 있음

- 불법사이트에 대한 접속 차단조치로 인해 불법정보의 유통으로 인한 피해방지, 안전한

인터넷 환경과 같은 공공복리적 차원의 긍정적 효과가 발생할 것이라는 기대가 있는 반면, 개인의 정보 접근권이 제한될 것이라는 우려가 제기되었음

- 해외 서버를 경유하여 불법촬영물, 불법도박, 불법음란물, 불법저작물 등 불법정보가 국내 인터넷 사용자들에게 유통됨으로써 발생하는 피해를 방지할 수 있다는 점에서 긍정적인 기대가 있으며, 해외에서 합법이라도 국내 통신심의에서 명백한 불법사이트로 판단된 경우에는 국내에서 접속을 제한할 수 있다는 주장이 있음

- 한편, 해외에서 불법이 아닌 정보를 접근하는 것을 제한함으로써 개인의 정보 접근권이 제한될 것이라는 부정적인 견해도 있음

○ 이외에도 인터넷 이용자의 권익과 관련하여 SNI필드 정보에서 사용자의 접속하고자 하는 주소 정보를 확인할 수 있다면, 개별 사용자의 인터넷 접속기록을 ISP가 수집·저장하거나 저장하여 다른 목적으로 사용할 수도 있을 것이라는 우려가 제기됨

- SNI필드 정보를 확인하여 불법사이트 접속차단을 하는 기술적 조치를 허용함에 따라, ISP가 개별 사용자의 인터넷접속기록을 실시간으로 모니터링하고 감시할 수도 있다는 우려가 인터넷사용자들 사이에서 제기되었으며, 이는 헌법상 통신비밀보호 침해에 해당한다는 주장이 제기됨

  ※ 헌법 제2장 17조 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다'와 18조'모든 국민은 통신의 비밀을 침해받지 아니한다'

- 새로 도입된 접속차단 조치가 암호화된 패킷 정보까지 들여다 볼 수 있어 개인 인터넷 사용자의 통신내용까지 공개된다는 의혹이 제기

○ 이전의 접속차단 기술과 비교할 때, 새로 도입된 접속차단 기술이 인터넷 사용자의 개인정보나 통신비밀에 대한 침해 가능성이 더 높지 않다는 것이 전문가들의 의견임

- 암호화되기 전 단계의 정보를 활용하고 불법사이트 및 불법게시물의 목록 DB와 사용자가 접속하려고 하는 주소 정보를 매칭하는 기계적 방식을 사용하다는 점에서 기존의 HTTP 차단 방식이나 새로 도입된 HTTPS 차단 방식이 동일함

- 따라서 새로운 접속차단 방식이 도입되었다고 해도 기존의 접속차단 방식에 비해 통신비밀이나 개인정보 침해의 위험이 더 커질 가능성은 낮음

○ 개별 사용자의 인터넷접속기록을 동의 없이 수집하거나 저장하는 행위는 정보통신망법을 통해서 규제하고 있음

- 개인정보의 수집제한 및 사용동의에 대해서는 정보통신망법 제 22조와 제 23조에서 규정하고 있음

<표 2-7> 정보통신망법의 개인정보의 수집제한 및 사용동의에 관한 조항

조항	내용
개인정보보호법 제22조 (개인정보의 수집·이용 동의 등)	① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다. 1. 개인정보의 수집·이용 목적 2. 수집하는 개인정보의 항목 3. 개인정보의 보유·이용 기간
제23조(개인정보의 수집 제한 등)	① 정보통신서비스 제공자는 사상, 신념, 가족 및 친인척관계, 학력(學歷)·병력(病歷), 기타 사회활동 경력 등 개인의 권리·이익이나 사생활을 뚜렷하게 침해할 우려가 있는 개인정보를 수집하여서는 아니 된다. 다만, 제22조제1항에 따른 이용자의 동의를 받거나 다른 법률에 따라 특별히 수집 대상 개인정보로 허용된 경우에는 필요한 범위에서 최소한으로 그 개인정보를 수집할 수 있다. ② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 범위에서 최소한의 개인정보만 수집하여야 한다. ③ 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

- 개인정보 이용제한 및 벌칙에 대해서는 정보통신망법 제 24조와 제 71조에서 규정하고 있음

<표 2-8> 정보통신망법의 개인정보의 이용제한 관련 조항

조항	내용
개인정보보호법 제24조(개인정보의 이용 제한)	정보통신서비스 제공자는 제22조 및 제23조제1항 단서에 따라 수집한 개인정보를 이용자로부터 동의받은 목적이나 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.
개인정보보호법 제71조(벌칙)	①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. 1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자

- 개인정보의 제3자 제공에 대해서는 정보통신망법 제 24조의 2에서 규정하고 있음

<표 2-9> 정보통신망법의 개인정보의 제3자 제공 관련 조항

조항	내용
제24조의2(개인정보의 제공 동의 등)	① 정보통신서비스 제공자는 이용자의 개인정보를 제3자에게 제공하려면 제22조제2항제2호 및 제3호에 해당하는 경우 외에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 1. 개인정보를 제공받는 자 2. 개인정보를 제공받는 자의 개인정보 이용 목적 3. 제공하는 개인정보의 항목 4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간 ② 제1항에 따라 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우 외에는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다. ③ 제25조제1항에 따른 정보통신서비스 제공자등은 제1항에 따른 제공에 대한 동의와 제25조제1항에 따른 개인정보 처리위탁에 대한 동의를 받을 때에는 제22조에 따른 개인정보의 수집 · 이용에 대한 동의와 구분하여 받아야 하고, 이에 동의하지 아니한다는 이유로 서비스 제공을 거부하여서는 아니 된다.

○ SNI필드 정보만으로 암호화된 패킷 정보까지 들여다 볼 수 있지는 않음

- 새로 도입된 접속차단 조치로 암호화된 패킷 정보까지 들여다 볼 수 있지 않을까 하는 우려가 있으나, SNI 필드 기반 접속차단 방식은 암호화되지 않고 노출된 서버네임이 불법사이트와 일치하면 기계적으로 접속을 자동 차단하는 방식으로 데이터의 내용을 저장하여 분석하고, 재조합하여 패킷의 내용을 확인하는 패킷감청과 구분된다고 방송통신위원회(2019. 2. 12)가 밝힌 바 있음

  † (2016헌마263) "인터넷 회선 감청은, 인터넷 회선을 통하여 흐르는 전기신호 형태의 '패킷'을 중간에 확보한 다음 재조합 기술을 거쳐 그 내용을 파악하는 이른바 '패킷감청'의 방식으로 이루어진다."

○ 그럼에도 불구하고 안전하고 신뢰할 수 있는 인터넷통신에 대한 국민들의 요구에 대응하기 위해서, 국민의 신뢰를 얻을 수 있는 제도 마련을 위해 지속적인 노력이 필요하다는 의견이 있음

- 인터넷 이용자들이 제기한 의혹과 불안은 새로 도입한 기술적 조치의 기술적 특성 때문이라기보다는 일반적인 신뢰의 문제라는 의견도 있으며, 이에 따라 국민 신뢰를 위한 노력이 필요하다는 지적이 있음

4. 불법정보 유통방지를 위한 대안

○ 안전한 인터넷 환경 조성을 위해 보다 긴급하고 즉시적으로 대응할 수 있는 불법정보 차단 조치가 필요하다는 주장과 다른 기술적·비기술적인 불법정보 유통 방지 대안이 있음에도 불구하고 사이트 전체를 차단하는 기술적 조치를 채택함으로써 과잉 차단이라는 주장이 공존함

○ SNI 필드값을 확인하지 않고도 불법정보 유통 방지를 위한 다른 대안적 수단이 있을 수 있음에도 불구하고 사이트 전체를 차단하는 조치를 도입했다는 주장이 제기됨

- 불법정보만을 선별적으로 삭제하거나 차단할 수 있음에도 불구하고 불법사이트 전체를

차단하는 기술적 조치를 선택해서 과잉규제의 우려가 있다는 의견이 제기됨

- 또한 불법사이트 운영자나 불법정보 제공자에 대한 처벌을 강화하거나 해외불법사이트 규제를 위해서 국제적인 공조 수사 등의 비기술적 수단을 통해 불법정보 유통 방지가 가능함에도 불구하고, 접속차단이라는 기술적 조치를 적용함으로써 과잉차단의 우려가 있다는 주장도 제기됨

○ 과잉차단을 방지하기 위해서 비기술적 수단이 우선적으로 사용되어야 하며 기술적 수단은 제한적으로 사용되어야 한다는 의견이 제기됨

- 다만 디지털복제와 온라인을 통한 빠른 정보 확산이 가능한 인터넷 환경에서 불법정보의 유통으로 인한 피해를 방지하기 위해서는 국제 공조나 가해자에 대한 처벌 강화 등의 비기술적 수단에만 의존하는 데에는 한계가 있다는 현실적인 한계가 있음도 지적됨

- 기술적 수단은 저작권 침해나 디지털성폭력물 등의 긴급한 피해 방지가 필요한 정보 등으로 한정하여 적법한 절차를 거쳐 제한적으로 적용되어야 한다는 의견이 제기됨

○ 방송통신위원회는 현행법에 근거한 통신심의-시정요구-시정명령의 절차에 따라, 방송통신심의위원회에서 명백한 불법사이트로 판단된 사이트에만 한정적으로 접속차단을 적용하는 것을 원칙으로 하고 있음

- 현재에도 과잉차단 방지를 위해 HTTP로 시작되는 웹사이트 주소에 대해서는 도메인의 하위 디렉토리 및 페이지 단위의 세부주소 URL을 지정하여 불법게시물을 특정해서 차단하고 있음(URL 차단방식)

- HTTPS에도 적용할 수 있는 SNI필드 정보를 활용한 접속차단 방식은 서비스 단위(mail, news 등)로 차단하기 때문에 기존의 URL차단방식에 비해 해당 사이트에 존재하는 적법한 다른 정보의 유통을 제한할 우려가 넓음

- 따라서 차단의 범위를 최소화하기 위해서 명백한 불법정보를 과도하게 유통하는 일부

해외 인터넷사이트를 대상으로 통신심의에서 불법사이트로 판단한 경우에 한정하여 적용한다고 밝힘(방송통신위원회, 2019. 2. 12.)

○ 방송통신심의위원회는 과잉차단의 우려를 방지하기 위해 통신심의를 통해 명백하고 현저하게 불법성이 있다고 판단된 경우에 한하여, '해당 정보의 삭제', '이용해지' 등의 시정요구를 할 수 없거나 세부URL 단위의 접속차단이 불가능한 경우에 한정적으로 접속차단을 결정하고 있음

5. 접속차단 조치 도입과정의 절차적 투명성

○ 접속차단 조치 도입의 목적과 기술적 방식에 대한 사전의 정보공개나 의견수렴 절차가 없었다는 지적이 제기됨

- 접속차단 조치의 도입 목적, 방법, 시기 등에 대한 정보가 사전에 공개되고 의견을 수렴하는 공론화 절차가 부재했다는 점이 지적됨

- 불법사이트 이외에 다른 사이트를 차단하지 않았는지 등을 확인할 수 있는 절차 등이 부재했다는 지적이 있음

○ 방송통신위원회는 2018년 6월부터 총 5회에 걸쳐 SNI차단 방식 도입을 위한 협의를 실시하였으나, 이 과정에서 공청회 개최나 시범적용 등 일반 인터넷 이용자 대상 의견수렴 과정이 없었다는 감사원의 지적(2019. 7.)이 있었음

- 방송통신위원회는 2018년 6월 "해외 불법사이트 접속차단 고도화 추진계획"을 수립한 후 5회에 걸쳐 정보통신서비스 제공자 등과 SNI 차단방식 도입을 위한 협의를 실시하고, 이듬해 2019년 2월 1일에 정보통신서비스 제공자 및 방심위에 불법사이트 접속차단 시 URL 차단방식과 함께 SNI 차단방식을 적용하는 공문을 발송하였음

- 방송통신위원회는 불법사이트 차단 과정에서 접속차단 방식을 공개할 경우 불법사이트 제공자와 이용자들이 우회접속기술을 사전에 개발하여 접속차단을 회피할 우려가 있었다고 판단하고, SNI차단방식을 도입함과 동시(2019. 2. 12.)에 새로운 접속차단

기술과 도입취지를 설명하는 보도자료를 배포함

- 이후 방송통신위원회는 SNI 접속차단의 기술 방식 등을 설명하는 자료를 배포(19. 2. 14.)하고, https 차단 방식 반대에 대한 국민청원에 대한 답변을 실시하여 불법사이트 차단 조치에 대한 국민적 이해를 제고하기 위한 노력을 일부 병행함

- 이후 감사원(2019. 7.)은 "국민청원이 제기되는 등 불필요한 논란을 야기(p. 11)"했다고 지적하고, "앞으로 정보통신서비스 제공자 등에게 새로운 불법사이트 접속차단방식을 도입하도록 하는 경우, 새로운 방식을 시행하기 전에 그에 관한 근거와 절차를 마련하고 공론화 과정을 거치는 등(p.12)"의 대응을 요청함

○ 새로운 기술적 조치를 도입하는 과정에서 인터넷 정책에 대한 국민 공감대 형성에 미흡했다는 의견을 반영하여, 방송통신위원회는 2019년 6월에 「인터넷규제개선 공론화 협의회」를 발족함

6. 불법정보 규제체계

○ 현행 접속차단 조치는 정보통신망법 제 44조의7, 방송통신위원회의 설치 및 운영에 관한 법률 제21조 제3호 및 제4호, 동법 시행령 제8조에 근거하여 도입되었으나, 이를 계기로 불법정보의 판단기준과 불법정보의 범위가 변화하는 국민정서를 충분히 반영한 것인지에 대한 문제제기와 현행 불법정보 규제 체계에 대한 개선 필요성에 대한 의견이 제기됨

- 현행의 불법정보와 유해정보의 범위가 현재의 국민정서가 적절하게 반영된 것인지에 대한 문제제기가 많았으며, 특히 이번 접속차단 조치의 도입을 계기로 음란물과 성인물의 범위에 대한 재정의가 필요하다는 의견이 많았음

- 또한 불법성 판단의 공정성, 통신심의부터 시정요구와 시정명령에 이르는 불법정보 규제체계의 적절성 등의 보다 근본적인 규제체계 개선 논의가 필요하다는 주장이 제기되었음

○ 현행 불법정보 규제체계는 정보통신망법, 방통위 설치법에 근거한 것으로, 사회적 요구와 국민정서에 따라 변화할 필요가 있다면 중장기적인 논의와 사회적 합의에 따른 입법 절차가 필요하다는 의견이 다수 제기됨

- 정보통신망법 상에서 불법정보는 실정법에 따라 불법정보의 유형을 나열한 것으로, 심의대상의 범위와 불법정보의 범위에 대한 중장기적인 사회적 논의와 합의에 근거하여 법령 개정이 필요함

「인터넷규제개선 공론화 협의회」 운영결과

※ 다음은 「인터넷규제개선 공론화 협의회」 위원들의 논의 결과에 대한 최종 결과이며, 방송통신위원회에 정책제안 형식으로 제출되었습니다.

제 3장 인터넷규제개선공론화 협의회 운영결과

제 1 절 추진배경 및 진행경과

1. 추진배경

○ 불법음란물, 불법복제물 등의 유통으로 피해자 권리침해 문제가 심각해지면서 불법정보에 대한 효과적인 유통차단이 중요해짐에 따라 보안접속(HTTPS)을 이용한 해외 불법사이트의 접속차단 조치(2.11) 실시

※ 불법촬영물 등 경찰 수사 급증(2017년 6,465건), 온라인 불법저작물의 시장침해 규모 2조 5,646억원(2017년), 온라인 불법도박의 시장규모는 47조원(2015년)

○ 이 과정에서 인터넷상 표현의 자유 보장과 불법사이트 차단이라는 공익 간의 적절한 균형이 필요하다는 의견이 제기되는 등, 인터넷 규제의 바람직한 방향과 적정한 수준에 대한 사회적 공론화 및 이를 통한 국민적 공감대 형성 필요 증가

※ SNI 차단조치(2.11)에 반대하는 국민청원이 26만건을 돌파하는 등 음란물을 포함한 인터넷상 표현의 자유 증진에 대한 사회적 요구 증가

○ 이에 방송통신위원회는 인터넷 규제의 바람직한 방향과 적정한 수준을 논의하기 위한 공론화 협의회 구성·운영('19. 6. 13. ~ '19. 12. 31., 6.5개월)

2. 협의회 구성 · 운영방식

○ (운영체계) 위원 간 논의 결과(6.13, 6.27)에 따라, 전문성을 위해 접속차단기술에 특화된 특별기술소위원회를 별도 운영하고, 특별기술소위원회의 자문을 수렴하여 인터넷 규제 개선을 위한 공론화협의회 운영

- 접속차단기술 관련 안건(기술적 대안, 이용자보호 등)들은 특별기술소위원회에서 논의하고, 특별기술소위원회의 논의내용을 협의회 전체회의에서 수렴하여 결과보고서를 작성함

○ (운영기간) 약 6.5개월간 운영 ('19. 6. 13. ~ '19. 12. 31.)

○ (구성) 학계, 법조계, 시민단체 및 유관기관 등으로 구성된 인터넷 규제 개선을 위한 공론화협의회를 운영하고, 기술자문을 위해 특별기술소위원회를 별도로 운영함

- (전체회의) 학계, 법조계, 시민단체 및 유관기관 등 14인으로 구성하여, 6.5개월 간 총 7차례 전체회의 개최

<표 3-1> 「인터넷 규제개선 공론화 협의회」 전체회의 구성원

구분	성 명(직책)	소속	비고
학계 (5인)	김명주(교수)	서울여자대학교 정보보호학과	위원장
	김승주(교수)	고려대학교 정보보호대학원	
	황용석(교수)	건국대학교 미디어커뮤니케이션학과	
	심재웅(교수)	숙명여자대학교 미디어학부	
	권헌영(교수)	고려대학교 정보보호대학원	
법조계 (2인)	강신욱(변호사)	법무법인 세종	
	박지연(변호사)	법무법인 태평양	
시민단체 및 유관기관 (7인)	한석현(팀장)	서울YMCA 시청자시민운동본부	
	정지연(사무총장)	한국소비자연맹	
	강혜란(대표)	한국여성민우회	
	오병일(대표)	진보네트워크센터	
	권오주(정책위원장)	학부모정보감시단	
	신익준(사무처장)	한국인터넷자율정책기구	
	통신심의국장	방송통신심의위원회	

- (특별기술소위) 인터넷 보안 및 접속차단 기술 관련 학계, 법조계, 시민단체 및 유관기관 등 총 10인으로 구성하여, 6개월간 총 3차례 특별 기술 소위원회 회의를 개최함

<표 3-2> 「인터넷 규제개선 공론화 협의회」 특별기술 소위원회 구성원

구분	성 명(직책)	소속	비고
학계 (3인)	김승주(교수)	고려대학교 정보보호대학원	소위원장
	이경문(교수)	중부대학교 소프트웨어공학부	
	허준범(교수)	고려대학교 컴퓨터학과	
법조계 (2인)	강신욱(변호사)	법무법인 세종	
	박지연(변호사)	법무법인 태평양	
시민단체 및 유관기관 (5인)	정운영(팀장)	한국정보화진흥원(NIA)	
	박진완(팀장)	한국인터넷진흥원(KISA)	
	오병일(대표)	진보네트워크센터	
	이남경(책임연구원)	한국전자통신연구원(ETRI)	
	확산방지팀장	방송통신심의위원회	

○ (논의의제) 접속차단 조치('19.2.11)로 인해 제기된 ① 국민여론 분석 결과, ② 시민단체의 의견 청취 결과, ③ 협의회 위원들이 제안한 의제들을 취합하여, 종합적으로 논의 안건을 도출함

- (전체회의) 불법정보 유통방지를 위한 비기술적 대안, 기술적 조치 도입절차의 투명성 제고 방안, 이용자 권리 보호 방안, 불법정보 유통방지를 위한 기술적 조치와 관련한 법·제도 등을 검토함

- (특별기술소위원회) 현행 불법정보 유통방지 기술 검토, 불법정보 유통방지를 위한 기술적 대안, 이용자 이익 보호 방안을 검토함

○ (국민의견수렴) 국민청원, 민원, 언론보도, 인터넷 게시글 등 국민여론 자료를 수집·분석하여 이를 토대로 위원 간 논의를 진행하고, 관련 시민단체의 의견 청취를 실시함

- 기술적 조치가 시행된 이후('19. 2. 11.~'19. 8. 27) 접수된 국민청원 및 제안, 민원, 언론보도, 주요 온라인 커뮤니티의 인터넷 게시글 등을 수집 하고 내용분석을 실시해 주요 쟁점을 발굴함

- 해외 불법사이트 접속차단과 관련한 국민여론의 적극적 수렴을 위해 위원 간 합의에 따라 주요 시민단체† 의견 청취(오픈넷, 한국사이버성폭력대응센터, 2019. 10. 17.)

† 시민단체 의견청취내용은 <부록 1> 참조

3. 협의회 운영 결과

○ (전체회의) 2019. 6. 13.부터 약 6.5개월간 총 7회 회의를 통해 불법정보 유통방지를 위한 비기술적 대안, 기술적 조치 도입절차의 투명성 제고 방안, 이용자 권리 보호 방안, 불법정보 유통방지를 위한 기술적 조치와 관련한 법·제도 등의 안건을 논의함

<표 3-3> 「인터넷 규제개선 공론화 협의회」 전체회의 운영결과

구분	안건	주요내용
1차	발족식	▪ 협의회 발족
2차	운영방안 및 계획	▪ 협의회 운영방안 및 계획 논의 ▪ 발제 및 질의응답 - 불법정보 유통방지 정책 관련 쟁점 및 과제 (최경진 교수) - 온라인 접속 차단 기술의 현황 및 전망 (허준범 교수)
3차	논의의제 발굴	▪ 협의회 논의의제 발굴 - 기술적 조치 관련 국민 여론자료 분석 결과 보고(간사기관) ▪ 발제 및 질의응답 - 해외불법정보 유통 대응현황(방심위) ▪ 안건논의 - 비기술적 규제 대안을 통한 불법정보 유통 방지 방안 검토
4차	비기술적 대안 및 도입절차의 투명성	▪ 발제 및 질의응답 - KISO의 민간자율심의 체계 현황(KISO) ▪ 안건논의 - 자율규제방안 등 불법정보 유통방지의 비기술적 규제 대안 검토 - 기술적 조치 도입절차의 투명성 확보 방안 논의
5차	법제도적 쟁점	▪ 접속차단에 대한 시민단체의 의견 청취 및 질의응답 ▪ 안건논의

		- 불법사이트 접속차단 조치의 법제도적 쟁점 및 이용자 권리 침해 등 검토(Ⅰ)
6차	이용자 권리 침해	▪ 안건논의 - 불법사이트 접속차단 조치의 법제도적 쟁점 및 이용자 권리 침해 등 검토(Ⅱ)
7차	결과보고서 검토	▪ 정책건의사항 발굴 ▪ 공론화협의회 결과보고서 검토

○ (특별기술소위원회) 2019. 6. 27.부터 약 6개월간 총 3회 회의를 통해 불법정보 유통방지의 기술 검토, 이용자 권리 보호 방안, 불법정보 유통방지를 위한 기술적 대안 검토 등의 안건을 검토함

<표 3-4> 「인터넷 규제개선 공론화 협의회」 특별기술 소위원회 운영 결과

구분	안건	주요내용
1차	운영계획 및 안건발굴	▪ 소위원회 운영계획 및 방안 논의 ▪ 안건발굴
2차	접속차단 기술방식 검토	▪ 불법정보 차단조치의 기술방식 및 이용자 권리 보호 방안 검토
3차	기술적 대안 검토	▪ 기술적 대안 검토 ▪ 특별기술소위원회 결과보고서 확정

제 2 절 사안별 검토의견

1. 접속차단 기술의 실효성 검토

가. 논의 배경

○ 인터넷 기술은 보안통신을 강화하는 방향으로 발전하고 있는데, TLS 1.2에 기반한 이번 접속차단 조치는 조만간 무력화될 우려가 있음

- 향후 SNI 필드 정보를 암호화할 수 있는 ESNI(Encrypted SNI) 기술이 일반화될 것이기 때문에, SNI 필드의 암호화되지 않은 주소정보를 확인한 후 이를 토대로 불법 사이트 접속을 차단하는 현행 기술적 조치는 곧 무용지물이 될 수 있음

○ 불법정보를 유통하는 사이트 운영자나 사이트 이용자가 현행 접속차단 조치를 우회할 수 있는 기술과 방법을 활용할 수도 있어서 현행 접속차단 조치의 기술적 실효성이 낮다는 우려가 있음

- 불법정보의 인지-심의-시정명령-차단에 이르는 절차가 약 2주 정도 걸리는 점을 악용† 하여, 불법정보 사이트 운영자가 사이트 도메인 변경 등을 통해 접속차단 조치를 우회할 수 있음

  † 불법 사이트의 기존 주소를 변경한 후, 해당 사이트의 이용자들에게 SNS나 인터넷 게시판 등을 이용하여 변경된 사이트 주소를 알려줌으로써 예상되는 접속차단을 수시로 우회하는 행위

- 사이트 이용자가 별도의 앱이나 프로그램을 이용할 경우 현행 접속차단을 우회하여 불법 사이트에 접속† 할 수 있음

  † 앱스토어 등을 통해 모바일 차단 우회용 앱을 이용하거나, 해외 차단 우회용 프로그램 및 서비스를 이용하여 우회접속을 시도하는 행위

나. 검토 의견

○ TLS† 분야의 기술발전이 진행되어도 현행 접속차단 조치에서 사용하고 있는 암호화

되지 않은 SNI 필드 기반의 접속차단 기술은 상당기간 유효할 것으로 판단됨

† TLS(Transport Layer Security): 사용자의 단말과 서버간의 통신에서 도청, 변조, 메시지 위조를 방지하기 위한 암호화 프로토콜로서 현재는 TLS 1.2가 사용되고 있음

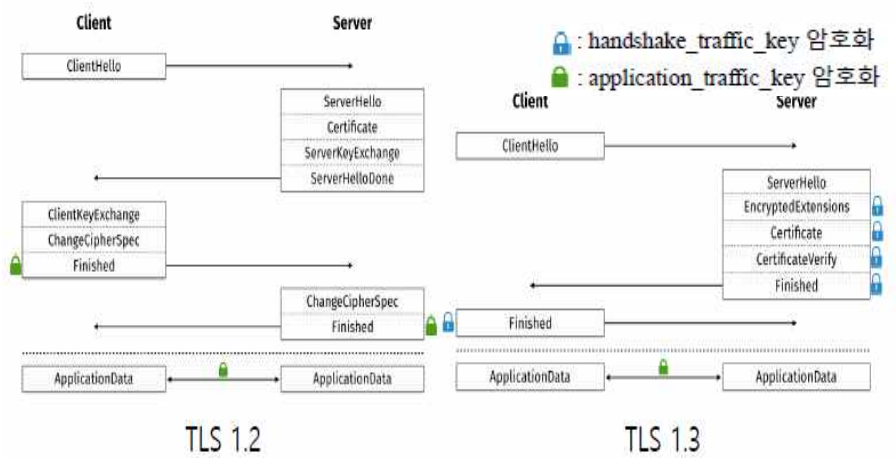
- 현행 접속차단 조치는 사용자가 통신을 시작하기 위해서 서버에 전달하는 암호화되지 않은 초기메시지(ClientHello) 중에서 서버네임(server name)을 확인하여 불법 사이트를 기계적으로 자동 차단하는 방식임

- 통신보안이 강화된 새로운 인터넷 전송계층 보안 프로토콜 표준인 TLS 1.3이 배포되면, 초기메시지에서 서버네임을 확인하여 불법사이트 접속여부를 파악할 수 없게 되어 현행 접속차단 방식이 효과가 경감될 것이라는 주장이 제기된 바 있으나,

- 현재 사용되고 있는 인터넷 전송계층 보안 프로토콜 표준인 TLS 1.2 버전과 현재 개발되고 있는 새로운 표준인 TLS 1.3‡ 버전 모두는 사용자의 단말(Client)에서 서버(Server)로 가는 초기메시지를 암호화하지 않고 있음

‡ 2018년 8월 28일에 발표한 TLS 1.3 (RFC 8446) 방식에서도 초기메시지인 클라이언트 헬로 메시지는 암호화되지 않음(<그림 3-1> 참조)

[그림 3-1] TLS 핸드쉐이크(Handshake) 프로토콜 개요



출처: 허준범, 온라인 접속차단 기술의 현황 및 전망, 2019.

- 아울러 인터넷상의 정보를 암호화하여 송수신하는 통신 프로토콜의 개발주기가, 우선 배포하고 문제에 대한 해결 패치를 추가 배포함으로써 문제점을 수정하는 기존 방식에서, 문제점을 충분히 수정한 후 나중에 배포하는 방식으로 변경됨에 따라, TLS 1.3 표준 발표 이후에도 완전히 배포될 때까지 상당한 시간이 걸릴 것으로 예상함

  ※ 경험적으로도 TLS 1.2 표준이 2008년에 발표되어 현재까지 10여 년간 최신 표준으로 유지되었던 것을 고려할 때, TLS 1.3도 상당기간 유지될 것으로 예상함(<그림 2> 참조)

[그림 3-2] SSL/TLS 발전과정

출처: 허준범, 온라인 접속차단 기술의 현황 및 전망, 2019.

- 따라서 인터넷상의 정보를 암호화하여 송수신하는 통신 프로토콜 분야의 새로운 기술 개발로 인하여 현행 접속차단에서 사용하는 기술적 조치가 쉽게 무력화되지는 않을 것으로 예상하며, 향후 상당한 시간 동안 유효한 기술적 조치로 활용될 수 있음

○ SNI 필드 정보를 암호화하는 ESNI(Encrypted SNI) 기술에 대한 기술채택 및 확산속도 등을 고려할 때 단기간에 확산될 가능성은 낮아서 현재의 조치가 상당기간 유효

- ESNI가 작동하려면 다크웹이나 불법사이트 뿐만 아니라 서버에서도 ESNI를 지원해야 함

- ESNI가 도입된 HTTPS 통신규약이 나왔지만 아직 표준화 합의를 이루지 못했고, 이를 적용하기 위해서는 사용자 브라우저에서부터 서버 단까지 많은 패치들이 이루어져야하므로 단시간에 확산되지는 않을 것임

- 특히 ESNI 관련 국내에서의 기술채택 및 확산속도를 감안할 때 ESNI로 인하여 현행 접속차단 조치가 단기간에 효력을 잃을 가능성은 낮음

○ 인터넷 이용자가 차단 우회용 프로그램이나 앱 등을 사용하여 불법사이트에 대한 접

속차단을 우회하는 행위는 일반화되지 않을 것임

- 이용자가 불법 사이트 접속을 위해 VPN을 사용할 경우, 동영상을 시청하기에는 적합하지 않은 ① 속도 저하를 일으킬 수 있고, ② 유료 VPN의 경우 추가 비용을 지불해야 하며, ③ 무료 VPN의 경우 개인정보 유출 등의 문제를 안고 있어서 일반화되지는 않을 것임

- 국내에서 차단된 불법 사이트 접속을 위해서는 해외 VPN 서비스를 사용해야 하므로, 가용성 측면에서 일반인들에게는 제약이 큼

- 따라서 VPN을 사용하여 우회 접속하는 방법들이 인터넷 이용자들 사이에서 일부 공유되고는 있지만 활성화 또는 일반화될 것으로 보이지는 않음

- 다만, VPN 사용현황에 대한 국내 통계 및 조사가 잘 이뤄지지 않고 있어 향후 방통위 등 관련 기관 및 단체에서 VPN을 비롯한 우회기술 사용현황을 체계적으로 조사할 필요가 있음

○ 전송하는 패킷의 최대 전송 단위를 조정(MTU값 조정†)하여 패킷을 쪼개서 보내는 TCP fragmentation‡ 에 대해서는 우회접속의 가능성이 있어서 ISP의 소프트웨어 업데이트를 통해서 이를 방지할 필요가 있음

† MTU(Maximum Transmission Unit)는 한번에 전송하는 패킷의 최대 단위를 의미함

‡ 사용자가 접속 차단된 도메인 주소를 잘게 쪼개어 전송함으로써 접속차단을 우회하는 방식

- 초기 메시지(ClientHello)의 패킷 값을 쪼개어 보내는 방식으로 MTU값을 조정하여 우회접속이 이루어질 경우, 접속차단의 실효성이 약화될 수 있음

- 따라서 ISP에서 소프트웨어 업데이트 등을 통하여 TCP fragmentation을 이용한 우회접속을 방지할 수 있는 기술적 대책 마련이 필요함

○ 사이트 주소 변경을 통하여 접속차단을 우회하는 행위를 방지하기 위한 모니터링 강화가 필요함

- 불법 사이트가 인지되어 접속차단 절차에 이르는 시간 동안 불법 정보 제공자는 접속차단을 우회하기 위해서 기존 사이트 주소에 숫자를 붙이거나 사이트 명칭을 유사하게 변경하는 방법 등을 사용하여 불법 사이트 주소변경을 정기적으로 시도함으로써 접속차단 조치를 우회하는 경우가 발생하고 있음

- 이러한 경우 불법정보 제공자는 사이트 주소를 변경한 후 SNS나 커뮤니티 게시판을 통해 변경된 주소정보를 이용자들에게 제공하고 있음

  ※ 소○○, 밤○○, 봉○○○ 등의 대표적인 불법사이트들은 트위터나 웹아카이브 서비스 등을 통해서 약 2주마다 새로운 사이트 주소를 공지하여, 방송통신심의위원회의 심의와 접속차단 조치를 회피하고 있음

- 이와 같은 접속차단 우회를 방지하려면 불법 사이트의 변경될 주소를 사전에 예측하여 차단하거나, 접속차단 심의절차를 더 간소화하여 불법사이트에 대한 차단 실효성을 높여야 한다는 의견이 제기됨

- 반면에 접속차단 조치는 이미 발생한 불법정보 확산을 방지하기 위해 행해지는 사후 조치이므로, 변경이 예상되는 사이트 주소를 미리 예측하여 차단하는 것은 과잉차단이라는 의견이 제기됨

- 불법 사이트 주소 변경에 대한 모니터링을 강화하고 이를 통한 불법정보 확산에 신속하게 대응하는 조치 강화가 필요함

  ※ 디지털성범죄 피해방지 종합대책의 차원에서 경찰청, 여성가족부, 방송통신심의위원회는 디지털성범죄물을 “24시간 이내” 심의 후 신속히 삭제·차단하는 디지털성범죄심의지원단을 2019년 하반기부터 신설·운영하고 있음

2. 이용자 권리 침해 여부 검토

가. 논의 배경

○ SNI 필드 기반 차단이라는 새로운 기술을 활용하여 불법 사이트에 대한 접속을 차단

하기 때문에 개인별 접속정보 자체가 수집·저장되어 다른 목적으로 사용되지 않을까 하는 우려가 있음

- 새로운 기술적 조치는 암호화되지 않은 SNI 필드 값 뿐만 아니라 암호화된 패킷의 내부 정보까지 볼 수 있다는 우려가 제기됨

- ISP가 특정 사이트에 대한 접속을 단순히 차단하는 것을 넘어, 개인별 접속기록까지 실시간으로 모니터링함으로써 이용자 행위를 감시한다거나, 불법 사이트에 대한 개인별 접속기록을 외부에 제공할 수 있다는 우려가 제기됨

○ 현행 접속차단 조치가 정보 접근권, 알 권리 등에 있어서 인터넷 이용자의 권리를 침해하는지에 대한 서로 다른 의견이 제기됨

- (정보 접근권) 현행 접속차단 조치는 사이트 전체에 대한 국내 접속을 막고 있어서 차단된 사이트와 관련된 합법적 정보 유통까지도 차단함으로 정보 접근권을 과도히 제한한다는 의견이 있는 반면, 합법적 심의 결과에 따라 현저하게 불법성이 있는 사이트에 대해서만 제한적으로 차단하기 때문에 정보 접근권이 침해되지 않는다는 의견이 모두 존재함

- (알 권리) 일부 외국에서는 합법적인 성인물을 국내에서는 접속조차 할 수 없게 되어 성인들의 알 권리가 침해된다는 의견이 있는 반면, 이번 접속차단이 국내에서 합법적인 성인물을 차단하는 것은 아니므로 성인의 알 권리 침해가 아니라는 의견이 모두 존재함

- (피해자 보호) 이번 접근차단 조치는 안전한 인터넷 환경을 조성하려는 적극적 조치로서 불법정보 확산 방지 및 피해자 보호 차원에서 반드시 필요하다는 의견이 존재함

○ SNI 접속차단 조치로 인해 인터넷의 특정 기술(HTTPS, ESNI 등) 분야에 있어서 보안 침해와 기술발전을 저해한다는 우려가 제기됨

- 이번 접속차단 조치(HTTPS 보안접속 차단)로 인하여 HTTPS로 시작되는 모든 사이트

주소에 대한 접속을 차단하는 것으로 오해하거나 인터넷의 보안통신을 저해한다는 우려가 있음

나. 검토 의견

○ 접속차단의 기술적 프로세스를 검토한 결과, SNI 필드 차단으로 인하여 인터넷 이용자의 통신비밀 및 개인정보 침해가 실질적으로 더 증가한다고 보기는 어려움

- HTTPS(SNI 필드) 차단방식은 암호화되지 않은 메시지(ClientHello)를 통해 불법 사이트 접속 시도를 확인한다는 점을 제외하고는, 불법 사이트 및 불법 게시물에 대한 목록 DB를 대상으로 이용자가 접속하려는 사이트 주소를 매칭하여 ISP에서 차단한다는 점에서 기존의 HTTP 차단방식과 상이하지 않음(<표 3-5> 참조)

<표 3-5> 접속차단기술의 기술적 특성 비교

구분	2008년 이후 현재 차단기술	새로운 차단 기술(병행)
기술방식	HTTP 차단방식	HTTPS(SNI 필드) 차단방식
차단방식	- 해외 관문국에 전용장비를 설치하여 불법 유해사이트를 필터링하여 차단하는 방식 - Domain과 IP단위 뿐만 아니라 하위 디렉토리 및 페이지 단위까지 차단 가능 - 단, TLS를 통해 암호화되는 경우 차단 불가능	- 보안접속시에도 암호화되지 않은 영역인 SNI필드에서 차단 대상의 서버네임을 특정하여 차단하는 방식 - TLS를 통해 암호화되는 경우에도 차단 가능
개요도	 - 기존 차단방식: HTTP 헤더영역에 표시되는 서버호스트 이름을 통해 해당 서버사이트 차단 - SNI필드 차단: TLS handshake 프로토콜의 ClientHelloSNI 필드를 통해 해당 서버 접속 확인 후 차단	

- HTTPS 프로토콜 차단이라 할지라도 SNI 필드 정보는 사용자가 사이트를 접속할 때 이용자의 IP주소 같은 정보들이 암호화되기 전 단계에서 기계적으로 자동 차단하며 통신의 내용은 확인하지는 않기 때문에 기존의 접속차단 방식에 비하여 통신비밀 및 개인정보 침해가 실질적으로 더 증가하지는 않음

○ 동의 없는 개인정보 이용은 정보통신망법에 따라 규제하고 있으나, ISP가 이를 준수하고 있는지를 다시 한 번 검토할 필요함

- ISP가 접속차단의 기술적 조치를 시행함에 있어 개인별 접속정보나 IP 주소 정보 등을 당사자의 동의 없이 이용할 수 있다는 우려에 대하여 정보통신망법은 동의 없는 개인정보의 위법 이용에 대해 이미 엄격하게 규제하고 있음

- 국내 정보통신망법의 제22조 제1항, 제71조 제1항 제1호는 동의 없이 개인정보를 이용할 경우 5년 이하의 징역 또는 5천만원 이하의 벌금형에 처하고 있음

※ 현재 ISP의 개인정보처리와 관련한 위법사항은 정보통신망법에 따라 제재되며, 개인정보보호법 일부개정법률안 제 2016621호(2018.11.15.)과 정보통신망법 일부개정법률안 제 2016622호(2018.11.15.)이 국회본회의를 통과함에 따라 향후 개인정보보호법에 따라 제재됨

[정보통신망법]

제22조(개인정보의 수집 · 이용 동의 등) ① 정보통신서비스 제공자는 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.

1. 개인정보의 수집 · 이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유 · 이용 기간

제71조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다. <개정 2016. 3. 22., 2018. 12. 24.>

1. 제22조제1항(제67조에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자

○ SNI 접속 차단은 실행 과정에서 SNI 필드 내용을 자동적으로 인식하기는 하지만, 정보수사기관의 감청과 같이 통신 내용을 기록하거나 통신 사실을 제3자에게 제공하는

것은 아님. 허가받지 않은 감청에 대해서는 통신비밀보호법에 따라 규제되고 있음

- ISP가 접속차단의 기술적 조치를 시행함에 있어 개인의 통신내용을 기록하거나 통신사실을 제3자에게 제공할 수 있다는 우려에 대하여 국내 통신비밀보호법은 전기통신을 감청하는 행위를 규제하고 있음

- 국내 통신비밀보호법 제3조 제1항, 제16조 제1항 제1호는 통신망을 이용한 감청행위에 대해 10년 이하의 징역 및 5년 이하의 자격정지를 할 수 있도록 규정되어 있음

[통신비밀보호법]

제3조(통신 및 대화비밀의 보호) ①누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 다만, 다음 각호의 경우에는 당해 법률이 정하는 바에 의한다.

1. 환부우편물등의 처리 : 우편법 제28조·제32조·제35조·제36조등의 규정에 의하여 폭발물등 우편금제품이 들어 있다고 의심되는 소포우편물(이와 유사한 郵便物을 포함한다) 을 개피하는 경우, 수취인에게 배달할 수 없거나 수취인이 수령을 거부한 우편물을 발송인에게 환부하는 경우, 발송인의 주소·성명이 누락된 우편물로서 수취인이 수취를 거부하여 환부하는 때에 그 주소·성명을 알기 위하여 개피하는 경우 또는 유가물이 든 환부불능우편물을 처리하는 경우
2. 수출입우편물에 대한 검사 : 관세법 제256조·제257조 등의 규정에 의한 신서외의 우편물에 대한 통관검사절차
3. 구속 또는 복역중인 사람에 대한 통신 : 형사소송법 제91조, 군사법원법 제131조, 「형의 집행 및 수용자의 처우에 관한 법률」 제41조·제43조·제44조 및 「군에서의 형의 집행 및 군수용자의 처우에 관한 법률」 제42조·제44조 및 제45조에 따른 구속 또는 복역중인 사람에 대한 통신의 관리
4. 파산선고를 받은 자에 대한 통신 : 「채무자 회생 및 파산에 관한 법률」 제484조의 규정에 의하여 파산선고를 받은 자에게 보내온 통신을 파산관재인이 수령하는 경우
5. 혼신제거등을 위한 전파감시 : 전파법 제49조 내지 제51조의 규정에 의한 혼신제거등 전파질서유지를 위한 전파감시의 경우

16조(벌칙) ①다음 각 호의 어느 하나에 해당하는 자는 1년 이상 10년 이하의 징역과 5년 이하의 자격정지에 처한다.

1. 제3조의 규정에 위반하여 우편물의 검열 또는 전기통신의 감청을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취한 자

○ 해외에서 합법적인 사이트라고 하더라도 국내법을 위반하며 국내 이용자들이 접근·이용한다면 국내 이용자에 대한 접속차단 조치는 타당함

- 성범죄 영상물 유포 사이트, 불법 도박 사이트들은 해외에 운영 서버를 두는 방식으로 국내 수사를 피해가고 있는데 해당 서비스 제공자와 이용자가 실질적으로 한국인이 경우가 있음

  ※ 한국, 영국, 미국 등 32개국 수사기관이 '다크웹'(dark web)'에 개설된 아동음란물 사이트를 공조 수사해 사이트 운영자와 이용자를 검거한 결과, 아동대상 성범죄 영상공유사이트의 운영자가 한국인이었고 검거된 이용자 338명 중 223명(71.9%)이 한국인인 등 해외에 서버를 두는 형태로 국내이용자를 대상으로 불법 정보를 제공하는 행위가 확산되고 있음

- 이번 접속차단 조치는 디지털성범죄물 유통과 그로 인한 디지털성범죄 피해 확산에 대한 적절한 대응조치를 마련하라는 국민적 요구에 대응하는 행정적 조치로 도입되었다는 점을 고려해야 함

- 디지털성범죄물 등 불법정보를 배포하는 해외 소재 불법 사이트에 대한 국내 접근을 차단하더라도 해외 이용자들은 여전히 해당 불법 사이트를 접속할 수 있어서 이러한 접속차단 조치는 피해 확산 방지 조치로서는 제약이 있음

- 글로벌 네트워크라는 인터넷의 이러한 특성으로 인하여 국내 이용자들에 대한 접속차단만으로는 불법정보의 유통으로 인한 피해자가 겪게 되는 피해를 충분히 방지할 수 없으므로 원활한 국제 사법공조는 지속적으로 확산될 필요가 있음

○ 이번 접속차단 조치로 합법적인 정보에 대한 이용자의 권리는 제한될 가능성은 있으나, 불법정보의 차단을 위해서 사이트 전체를 차단할 필요가 있으며, 통신심의 결과에 따라 현행법상 현저하게 불법성이 있다고 판단된 사이트로 한정하여 적용되도록 노력할 필요가 있음

- 차단조치가 이뤄진 사이트들은 현행법 상 명백한 불법정보(아동청소년음란물, 불법촬영물, 불법도박 등)를 포함하고 있는 사이트로 판단됨

- 그러나 이용자의 정보 접근권과 알 권리를 보다 적극적으로 보장하기 위해서는 차단

대상 사이트의 불법성이 해소된 경우, 불법 사이트 목록 DB에서 해당 사이트를 삭제하는 회복 조치도 마련할 필요가 있음

- 아울러 불법사이트 목록 정보, 통신심의 및 차단절차 등에 대한 투명성을 더욱 높이기 위한 과정이 필요함

- 불법정보가 제공되는 사이트 전체에 대한 접속차단으로 인하여 과잉차단의 우려를 해소하려면 불법정보만 선별하여 삭제·차단할 수 있는 기술적 대안 마련이 필요함

○ 현행 접속차단 조치가 인터넷의 특정 보안기술 자체를 금지하거나 차단하는 것은 아님

- 현행 접속차단 조치는 HTTPS로 시작되는 불법 사이트의 주소를 확인하여 접속을 차단하는 기술이지만 HTTPS로 시작되는 사이트 모두를 차단하지는 않음

- 현행 접속차단 조치가 인터넷 통신의 보안 취약점을 이용하거나 인터넷 보안을 취약하게 하는 것은 아님. 그러나 사이트 차단이라는 공공정책 목적을 위해 보안 프로토콜을 활용하는 것이 인터넷 보안에 대한 신뢰를 저해한다는 이견도 있었음

- 기술 하나로 모든 불법 사이트를 차단하는 기술은 아직 존재하지 않을 뿐 아니라, 차단기술과 이에 대한 우회기술은 창과 방패의 관계처럼 서로 대응하는 과정에서 기술이 발전한다고 볼 수 있으므로 현행 접속차단 조치가 국내 인터넷 보안기술의 발전을 가로막는다고 보기는 어려움

3. 불법정보 유통방지를 위한 대안 검토

가. 논의 배경

○ SNI 필드 값을 기반으로 사이트 접속을 차단하는 현행 방법 이외에 불법정보 유통방지를 위한 다른 기술적 대안이 가능하다는 의견이 존재함

- 불법정보에 대한 선별적 삭제 및 차단을 통해 불법정보 확산을 방지할 수 있는 다른 기술적 대안이 있음에도 불구하고 불법 사이트 차단으로 과잉규제가 이뤄진다는 의견이 있음

- SNI 필드 값을 확인하지 않고서도 불법 사이트를 차단할 수 있는 기술적 대안 조치가 가능할 수 있다는 의견이 있음

○ 기술적 규제수단에 과도하게 의존하는 것보다는 비기술적 규제수단을 활성화하는 것이 중요함

- 비기술적 규제수단(처벌강화, 국제공조 수사, 자율규제 등)을 불법정보 유통방지를 위해 활용할 필요가 있음

나. 검토 의견

○ 해시목록 기반 방식이나 DNA목록 기반 방식, AI기술을 활용한 영상물 분석기반 방식 등이 불법정보 확산방지를 위한 기술들로 논의되고 있으나, 해외불법사이트 접속차단을 위한 기술적 대안은 아님

- 해시목록 기반 방식이나 DNA목록 기반 방식은 웹하드 사업자들이 관련 법령에 따라 불법영상물의 요약정보를 목록화하고 해당 목록과 일치하는 데이터를 삭제하는 방식임
  - ▸ 해시 목록 기반 방식: 현재 유포된 불법정보에 대한 요약(해시 정보)를 생성한 후 해당 해시 정보를 목록(DB)화하여 유통되는 불법정보를 DB의 해시 정보와 비교하여 식별하는 기술
  - ▸ DNA 목록 기반 방식: 불법정보가 가지는 고유의 특징(색상, 모션, 오디오 주파수, 화면 특징점 등)을 목록(DB)화하여 유통되는 불법정보를 DNA 목록과 비교하여 식별하는 기술
  - ▸ AI를 활용한 영상물 분석 기반 방식: 이미 불법정보라고 판단된 샘플(영상물)들을 학습용 데이터 집합 안에 방대하게 구축하여 이를 기반으로 기계학습을 진행함으로써 불법정보 여부를 판단하는 인공지능이 구축하여 향후 유통될 영상물 정보를 대상으로 불법 여부를 자동으로 식별하는 기술

- 해시 목록 기반 방식과 DNA 목록 기반 방식은 암호화 통신이 이루어지는 TLS 기반 인터넷 환경에서는 식별 자체를 할 수가 없어서 가용하지 않음

- 암호화되지 않은 인터넷 통신 환경하에서도, 이러한 기술적 대안들은 ISP가 유통되는 정보의 내용을 식별하여 차단해야하기 때문에 SNI 필드 정보를 활용한 현재의 접속

차단 기술보다 개인정보 침해 및 통신비밀보호 위반 등의 우려가 커짐

- AI 기술을 활용한 영상물 분석 기반 방식은 웹하드 사업자 등에서 일부 활용이 시도되고 있으나 해외불법사이트를 통해 유통되는 불법정보에 적용하기 위해서는 아직까지 실용화를 위한 기술개발이 필요하고, 영상물의 내용을 직접 식별해야한다는 점에서 해시 목록 기반 방식이나 DNA 목록 기반 방식과 유사하게 개인정보 침해 및 통신비밀 보호 위반 등의 우려가 있음

○ 불법정보 유통방지를 위해서 비기술적 수단을 사용하는 것이 바람직하지만, 불법성이 명백하게 확인된 불법 사이트에 대하여 다른 규제수단을 사용할 수 없는 경우에 한정하여 기술적 조치를 사용해야 함

- 가해자 및 유포자에 대한 처벌 강화, 국제 공조를 통한 수사 등의 비기술적 규제수단이 불법정보 유통방지를 위하여 우선적으로 사용되어야 하며, 접속차단을 위한 기술적 조치는 보완적으로 사용하는 것이 바람직함

○ 자율규제 활성화를 위한 지원 및 제도를 개선할 필요가 있음

- 인터넷 게시글 등에 대한 내용적 판단의 범위가 확대될수록 판단의 주체인 사업자들의 책임범위도 확대되므로, 사업자들의 자율규제를 지원하고 부작용을 최소화할 필요가 있음

4. 기술적 조치 도입절차의 투명성 검토

가. 논의 배경

○ 이번 기술적 조치에 따라 차단된 불법 사이트들의 목록이 이용자에게 직접 공개되지 않아서 사이트 차단의 정당성에 대한 의문이 발생하고 기술적 조치 도입절차의 투명성 제고에 대한 요구가 있음

- 불법정보의 유통방지를 위해 차단된 불법사이트의 주소를 공개하지 않기 때문에, 차단된 사이트가 명백하게 불법사이트인지 아닌지를 이용자들이 직접 확인할 수 없다는 의견이 존재함

- 특히, SNI 필드를 활용한 접속차단의 경우 기술적 조치의 특성상 접속이 차단된 원인을 이용자가 직접 인지하기가 힘들기 때문에, 차단 목록을 공개하라는 요구가 기존 차단 방식보다 많음

※ 일반 URL 접속차단의 경우, 인터넷 이용자가 차단 사이트를 접속할 경우 warning.or.kr로 리다이렉트되어 불법사이트 차단조치에 의해서 접속이 불가능함을 확인할 수 있으나, SNI 필드를 활용한 접속차단에서는 접속차단의 사유를 이용자가 명확하게 확인할 수 없음

- 아울러 접속차단 조치 도입 초기에는, 개인별 인터넷 접속환경에 따라 접근 가능한 사이트가 상이하거나, 가입한 ISP별로 접근 가능한 사이트나 차단 시점이 상이하다는 의견이 있었음

○ 새로운 접속차단 방식 도입과정에서 충분한 여론 수렴이 이뤄지지 않아, 공론화를 통한 사회적 합의 과정이 미흡했다는 의견이 있음

- 새로운 불법 사이트 접속차단방식을 도입할 경우 인터넷접속사업자에게 차단장비의 설치를 요구할 근거, 차단장비 및 설치방법 등을 정한 업무지침이나 고시 마련의 필요성이 있음을 감사원이 지적한 바 있음(<감사원 지적사항>† 참고)

- 2008년 정보통신부는 감사원의 지적에 따라 URL 차단방식 도입과 관련하여 인터넷접속사업자에게 URL 차단장비의 설치를 요구할 근거, 차단장비 및 설치방법 등을 정한 "해외 불법정보 차단업무 처리지침"을 마련·운용한 바 있음

† 감사원 지적사항

[조치할 사항] 앞으로 정보통신서비스 제공자 등에게 새로운 불법사이트 접속차단방식을 도입하도록 하는 경우, 새로운 방식을 시행하기 전에 그에 관한 근거, 범위, 정보통신서비스 제공자에게 요구할 수 있는 내용 및 절차 등을 명확히 하고 공청회나 시범적 적용 등의 공론화 과정을 거치는 등 불필요한 논란이 발생하지 않도록 관련 업무를 철저히 할 것

나. 검토 의견

○ 접속환경이나 가입한 ISP에 따라 접근 가능한 사이트가 달라진다는 의견은 SNI 필드

차단방식이 이전 차단방식과 달리 차단 안내페이지(warning.or.kr)로 리다이렉트(redirect)할 수 없다는 기술적 특성으로 인하여 발생하는 오해임

- SNI 필드 접속차단은 기술적 특성상 이전의 차단 안내페이지(warning.or.kr)로 이동하지 않고 빈 페이지(blank)만 내보내는 문제가 존재함

- 특정 사이트를 접속할 수 없는 이용자는 해당 사이트가 접속차단으로 인해 서비스가 불가능한 것인지 아니면 ISP 등 다른 요인으로 인한 서비스 불가능인지를 파악하지 못하는 현상이 발생함

○ SNI 필드 기반 접속차단 조처로 인하여 이용자의 개인정보 침해문제가 새롭게 발생하는 것은 아님

- 그럼에도 불구하고 인터넷 이용자가 표명한 불안과 우려는 불법 사이트 차단 자체보다는 ISP가 임의적으로 특정 사이트를 차단하거나 개인별 접속기록을 수집하는 등 인터넷 이용자의 개인정보에 대한 악용·오용이 발생했을 때 이에 대한 관리·감독이 제대로 이뤄지고 있는지에 대한 이용자의 확신이 부족해서 발생한다고 판단됨

- 따라서, 이용자들의 개인정보보호를 위한 방지책, 위반 시 인터넷접속사업자(ISP)의 법적 책임 등에 대한 방침을 정리하여 인터넷 이용자들에게 지속적으로 알릴 필요가 있음

○ 사이트 차단의 정당성 및 새로운 기술적 조치 도입절차의 투명성 확보를 위한 조치가 현행 수준보다 더욱 확대될 필요가 있음

- 현재 방송통신심의위원회는 회의록, 심의절차 등에 관한 정보는 심의규칙에 따라서 공개하고 있음. 다만, 차단된 불법사이트에 대한 주소 정보는 비공개를 원칙으로 하고 있음

※ 방송통신심의위원회는 「방송통신심의위원회 회의공개 등에 관한 규칙」의 제3조(회의공개)와 제4조(회의방청)에 따라 위원회의 회의를 공개하고 있으며, 제9조(회의록 공개)에 따라 회의결과를 홈페이지에 게재하고 있음. 또한 「정보통신에 관한 심의규정」의 제23조(심의자료의

공개 등)에 따라 개인정보를 노출하거나 특정인을 식별할 수 있는 정보를 제외하고 '공공기관의 정보공개에 관한 법률'에 따라 심의 관련자료를 공개할 수 있음

- 차단된 불법사이트 목록을 일반 시민에게 공개할 경우 불법정보의 우회접속을 조장할 위험이 있음

※ 불법사이트 목록에 대한 정보공개청구가 이미 제기되었으나 중앙행정심판위원회에서도 국민의 안전을 위해 공개하지 않는 것이 합당하다고 판단함

- 차단목록검색시스템을 구축하여 ISP 사업자별로 고객응대 직원이 접속 및 검색하여 이용자 민원을 일부 해소할 수 있도록 할 예정임

- 사이트 차단의 정당성 및 새로운 기술적 조치 도입절차의 투명성 확보를 위해서 차단된 불법 사이트 정보를 권한이 있는 기관이나 민원인은 확인할 수 있는 절차를 지속적으로 확대·제공할 필요가 있다는 의견도 있음

○ 향후 기술적 조치나 비기술적 조치를 신규로 도입할 경우 근거 규정을 미리 마련할 필요가 있으며, 국민여론 수렴 과정은 물론 전문가 집단을 중심으로 한 영향평가 등을 적극 도입할 필요가 있음

- 새로운 조치를 시행하기 전에 도입 절차와 운용, 사업자 협조 의무 등과 관련한 법적, 제도적 근거로서 근거 규정(지침이나 고시 등)을 미리 마련해 놓을 필요가 있음

- 근거 규정을 마련하는 과정에서 국민의 여론 수렴 및 관련 전문가들의 자문을 거치고, 새로운 조치를 시행할 경우 근거 규정에 따라 사전적·사후적으로 정책영향 평가, 공청회·세미나 등 국민 여론수렴 절차 등을 거칠 필요가 있음

5. 기술적 조치와 관련된 법・제도 검토

가. 논의 배경

○ 새로운 기술적 조치 도입 실시에 따른 법적 근거 조항 유무에 대한 서로 다른 의견이 있음

- 이번 접속차단은 방통위설치법 및 정보통신망법 제44조의7에 근거하여 방심위가 불법 사이트 접속차단을 요청하고 ISP가 차단하는 조치이므로 현행법상 법적 근거가 있다는 의견이 있음

- 반면에 방심위의 시정요구에 따라 ISP가 이용자의 사이트 접근을 차단하는 것 자체에 대한 법적 근거가 명확하지 않으므로 이와 관련한 법리적 검토가 필요하다는 의견이 있음

- 또한 접속차단조치와 관련해서 '사업자의 소명 절차† 등이 존재하고 있는지', '접속차단 절차가 합법적으로 이뤄졌는지' 등에 대한 의견이 있음

† 접속을 차단할 경우 그 사유를 해당 콘텐츠 서비스/제공자나 이용자에게 통보하고, 긴급하지 않은 불법정보(사이트)에 대해서는 차단조치 이전에 소명 절차 등이 제공되는지에 대한 질의

○ 암호화되지 않은 SNI 필드 영역을 활용해 불법사이트 접속을 차단하는 기술적 방식이 통신비밀 보호 및 사생활 침해에 해당되는지에 대한 서로 다른 의견이 있음

- 이전에는 접속차단을 위해 사용되지 않았던 SNI 필드 영역을 추가로 읽어서 접속차단에 사용하는 것은 헌법에서 보장하는 통신비밀보호‡ 침해에 해당한다는 의견이 있음

‡ 헌법 제2장 17조 '모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다'와 18조 '모든 국민은 통신의 비밀을 침해받지 아니한다'

- 암호화되지 않은 평문 형태의 SNI 필드 영역을 읽어서 접속차단에 사용하는 것은 헌법 상의 보호대상인 통신비밀을 침해하지는 않는다는 의견이 있음

○ 해외에서 합법인 사이트를 불법 사이트로 지정하여 접속 차단하는 것은 표현의 자유를 침해할 수 있다는 의견과, 이러한 접속차단 조치는 현행법률이 규정하고 있는 불법정보의 국내 유통을 제한하기 위한 정당한 법 집행이라는 의견이 모두 존재함

- 해외에서 합법인 사이트에 대한 접속을 국내에서 차단하는 것은 표현의 자유를 과다하게 제한한다는 의견이 있음

- 명백하게 불법 사이트로 판단된 사이트만을 차단하기 때문에 국내법상 불법인 정보의 국내 유통을 제한하는 조치는 정당한 제한이라는 의견이 있음

○ 행정기관이 불법 여부를 심의하여 사이트 차단 여부를 결정하는 것은 표현의 자유를 침해할 수 있다는 의견이 있음

나. 검토 의견

○ 새로운 접속차단 조치는 “통신심의-시정요구-시정명령”라는 기존 절차를 따라 시행되며 관련 법령에 근거하여 운영되고 있음

- (통신심의) 방송통신심의위원회는 ‘방송통신위원회의 설치 및 운영에 관한 법률’ 제21조 제3호 및 제4호, 동법 시행령 제8조에 따라 통신심의 업무를 수행하고 있으며, 전기통신회선을 통하여 일반에게 공개되어 유통되는 불법정보 및 청소년에게 유해한 정보 등 심의가 필요하다고 인정되는 정보를 법률적 근거에 따라 심의하고 있음

- (시정요구) 시정요구는 ‘방송통신위원회의 설치 및 운영에 관한 법률 시행령’ 제8조 제2항에 따라, 해당정보의 삭제 또는 접속차단, 이용자에 대한 이용정지 또는 이용해지, 청소년유해정보의 표시의무 이행 또는 표시방법 변경등과 그밖에 필요하다고 인정되는 사항들에 대해 실시하고 있음

- (시정명령) ‘정보통신망법’ 제44조의7 제2항 및 제3항에 따라, 방송통신위원회는 불법정보에 대해 심의위원회의 심의를 거쳐 정보통신서비스제공자나 게시판의 관리ㆍ운영자에게 그 처리를 거부ㆍ정지 또는 제한하도록 명할 수 있음

○ SNI 필드 정보를 활용한 HTTPS 접속을 차단하는 기술적 조치는 기존의 통신심의를 통한 접속차단 조치와 동일한 법률적 근거를 가지고 있음

- 이번 SNI 필드 정보를 활용하여 HTTPS를 차단하는 기술적 조치는 정보통신망법 제44조의7, 방송통신위원회의 설치 및 운영에 관한 법률 제21조 제3호 및 제4호, 동법 시행령 제8조에 근거하여, “통신심의-시정요구-시정명령” 절차를 따라 이루어지고

있음

- 이번 SNI 필드 정보를 활용하여 HTTPS를 차단하는 기술적 조치는 불법 사이트 여부를 심의하여 시정요구 및 명령을 내리는 현행 접속차단 조치의 절차를 그대로 따르고 있으므로, 기존의 접속차단 도입과 다른 법적 근거가 추가적으로 필요하다고 볼 수 없음

○ 방송통신심의위원회는 시정요구 시 당사자에게 의견진술 기회를 부여하고(방통위 설치법 제25조제2항), 이의신청권을 부여하여 이용자의 신속한 권리구제가 가능한 절차를 마련하고 있으며(동법 시행령 제8조제5항), 사법기관을 통한 불복을 보장하고 있어(동법 제25조제6항), 현행법에서 이의신청의 기회가 보장되고 있으나 현실적인 한계는 있음

- (이의신청) '정보통신에 관한 심의규정' 제16조(이의신청)에 따라 정보통신서비스 제공자, 게시판 관리·운영자 및 이용자가 시정요구를 받은 날로부터 15일 이내에 이의신청할 수 있음

- (의견진술) '정보통신에 관한 심의규정' 제18조(당사자등의 의견진술)에 따라, 제17조에 따른 제재 조치가 이뤄지기 전에 명령의 대상이 되는 당사자 또는 그 대리인에게 미리 의견을 진술할 기회가 부여됨

- (현실적 한계) 의견을 제출하거나 진술을 받도록 법에 명시되어 있으나 명백한 불법 사이트나 해외에 서버를 둔 경우에는 인터넷 게시자나 제공자의 연락처를 확인하거나 연락을 할 수 있는 방법에 한계가 있음

○ 접속차단조치 이전에 해당 콘텐츠/서비스 제공자에게 사전 의견 진술 기회를 제공하거나, 이의신청을 적극적으로 보장하는 등 콘텐츠/서비스 제공자의 방어권 보호를 위해 더욱 노력할 필요가 있다는 의견이 있음

※ 방심위는 해외사업자일지라도 시정요구의 대상이 되는 당사자 또는 그 대리인의 정보가 공개된 경우, 심의규정(심의규정 제 18조)과 설치법(설치법 시행령 제8조 제5항)에 근거하여 이의신청 및 의견 진술의 기회를 보장하고 있음

○ SNI 필드 기반 접속차단 조치는 이용자의 통신내용을 들여다보는 것은 아니며, 통신 비밀 보호 및 사생활 침해를 일으킨다고 보기 힘듦

- SNI 필드 기반 접속차단 방식은 암호화되지 않고 노출된 서버네임이 불법사이트와 일치하면 기계적으로 접속을 자동 차단하는 방식임

○ 이번 SNI 필드 기반 접속차단은 ISP 사업자와 이용자간 체결한 이용약관에 근거하여 도입되었음. 다만, 이용약관에 따른 동의 추정에 다른 시각이 존재함

- ISP 사업자와 이용자 간 이용약관에는 '방송통신심의위원회의 시정요구가 있을 경우 서비스의 전부 또는 일부의 이용을 제한할 수 있다'고 명기하고 있어 이를 근거로 접속차단 조치를 도입

- 다만 이용약관에 명기한 이용제한 조항에 근거하여 불법 사이트에 대한 접속차단 조치도 이용자가 명시적으로 동의한 것으로 추정할 수 있다는 시각과 그렇지 않다는 시각이 존재함

○ 명백하게 불법적이고 불가역적이며 급속한 피해가 예상되는 불법정보의 유통방지를 위한 긴급한 조치로서, 이번 SNI 필드 기반 접속차단 조치가 시행됨

- SNI 필드 기반 접속차단 조치는 긴급한 조치가 필요한 불법정보 유통에 적절하게 대응해달라는 사회적 요구에 대응하기 위한 조치로 도입됨

- 다만 불법정보의 종류에 따라 긴급성을 요하지 않는 경우도 있으므로, 시대적·사회적 흐름에 따른 국민 인식 변화를 고려하여 통신심의의 대상이 되는 정보의 명확한 범위에 대한 지속적인 논의와 사회적 합의가 필요함

○ 차단 대상이 되는 정보의 범위에 대하여 서로 다른 의견이 존재함

- 명백하게 피해자가 존재하는 디지털성범죄물이나 저작권 침해물에 한정하여 접속차단 조치를 시행해야 한다는 의견이 있음

- 반면에 국내 디지털성범죄의 특성과 음란물 제작·유통 환경을 고려할 때 디지털성범죄물과 음란물이 현실적으로는 잘 구분되지 않고 있으므로 접속차단의 대상이 되는 불법정보의 범위를 확대해야 한다는 의견도 있음

※ SNI 필드 기반 접속차단으로 차단된 현행 불법사이트들은 불법정보에만 한정되어 있으며, 유해정보로 인한 SNI 필드 기반 접속차단 사례는 없음

- 현행법상 불법정보가 아니지만 합성 등을 통해 편집된 디지털성범죄물, 혐오표현 등의 유해정보를 보다 적극적으로 심의해야 한다는 의견도 있음

- 시대적, 사회적 변화에 따라 불법정보에 대한 국민 인식도 변화하고 있으므로, 불법정보의 범위와 불법성 여부에 대한 새로운 국민적 공감대 형성을 위한 논의와 개선과정이 진행될 필요가 있음

- 개방적 공간인 인터넷 상에서 표현과 소통의 자유가 보장되어야 한다는 사회적 요구가 증가함에 따라, 망법상의 불법정보의 범위와 통신심의의 대상이 되는 정보의 범위가 제한되어야 한다는 의견도 있음

- 아울러 인터넷상의 표현의 자유를 보장하기 위해서는 불법 사이트 전체에 대한 접속차단보다는 해당 불법게시물만 선별하여 삭제할 수 있는 기술적 보완이 이루어질 수 있도록 노력할 필요가 있음

○ 불법정보의 판단 주체에 대하여 서로 다른 의견이 존재함

- 인터넷을 통한 불법정보 유통제한을 위해 시급한 조치가 필요한데 현행 국내 사법체계에서는 모든 불법정보에 대해 사법적 판단을 받기 어려운 한계가 있고 시급한 조치가 힘들므로 지금과 같은 임시적 행정조치가 불가피함

- 다만 모든 불법정보의 유통제한이 시급성을 요구하는 것이 아니고, 사법체계에서도 신속한 절차를 둘 수 있으므로 궁극적으로는 불법정보의 판단주체는 법원일 필요성이 있으며, 불법성 판단을 행정기관이 시행할 경우 자칫 자의적 판단이 이루어질 가능성이 있으므로 법원에서 판단해야 한다는 의견이 있음

- 그러나 현행 사법체계에서는 피해자(소송의 당사자)가 특정화된 사안에 대해서만 판단을 할 수 있고, 특정화된 피해자가 존재하지 않은 사안이나 사회적 법익 침해와 같은 사안을 판단할 수 없음

- 따라서 불법정보 판단을 법원에서 하기 위해서는 해외사례 등을 참조하여 사법적 판단절차의 신속성 제고방안과 사회적 법익 침해에 대한 판단절차 등이 검토될 필요가 있음

- 아울러 콘텐츠/서비스 제공자의 자율규제 및 이용자의 자율적인 정화를 지향하여 정부의 지원과 사회적 합의가 가능하도록 노력할 필요가 있음

제3절. 인터넷 규제개선을 위한 권고

1. 인터넷 규제 프레임워크에 대한 권고

가. 불법정보 유통방지 수단 활용에 대한 권고

○ 현행 기술환경에서 국내 이용자의 해외불법사이트 접속을 막기 위해서 접속차단의 기술적 조치를 사용하고 있으며 그 필요성은 인정함. 궁극적으로는 불법정보 유통방지를 위해서 접속차단의 기술적 조치에만 의존하지 않도록 노력할 필요가 있음

- 가급적 비기술적 수단을 우선 사용해야 하며, 명백한 불법성이 확인된 불법사이트에 한정하여 다른 규제수단을 사용할 수 없거나 피해구제의 긴급성을 요 하는 경우 제한적으로 기술적 조치를 적용한다는 기조를 유지할 필요가 있음

- 불법정보 유통방지를 위해서 처벌강화, 국제공조 수사 등 비기술적 규제수단을 우선적으로 사용하고, 기술적 조치에만 의존하지 않도록 노력할 필요가 있음

나. 기술적 조치 도입 절차의 투명성에 대한 권고

○ 이전에는 읽지 않았던 SNI 필드 정보를 활용하게 되어 이용자들이 사생활 침해에 대한 불안을 느낄 수 있으므로, 이를 해소하기 위해 기술적 조치의 도입 목표, 접속차단 과정과 그에 따른 결과에 대한 정확한 고지 노력이 필요함

- 현행 접속차단 조치가 인터넷의 특정 보안기술 자체를 금지하거나 차단한다는 이용자들의 오해를 방지하기 위하여 현행 접속차단 기술 및 절차에 대한 설명과 안내가 필요함

- 불법사이트 목록 정보, 통신심의 및 차단절차 등에 대한 투명성을 더욱 높임으로써 정보 접근권 및 알 권리 등 이용자의 권리가 제한되지 않음을 적극적으로 설명하는 과정이 필요함

○ SNI 필드 기반 접속차단 조처 시행에 따라 이용자들의 개인정보보호를 위한 방지책, 위반 시 인터넷접속사업자(ISP)의 법적 책임 등에 대한 방침을 정리하여 인터넷 이용자들에게 지속적으로 알릴 필요가 있음

○ 차단된 불법사이트 목록을 공개하는 것은 불법정보 우회접속을 조장할 위험이 있어 일반시민에게는 비공개를 원칙으로 하되, 권한 있는 기관이나 민원인 등 제한된 범위에서라도 차단된 이유를 확인할 수 있는 방안을 마련할 필요가 있음

- 차단목록 검색시스템을 구축하여 ISP 사업자별로 고객응대 직원이 접속 및 검색하여 이용자 민원을 일부라도 해소할 필요가 있음

- 이용자의 정보 접근권과 알 권리를 보다 적극적으로 보장하기 위해서는 차단 대상 사이트의 불법성이 해소된 경우, 불법 사이트 목록 DB에서 해당 사이트를 삭제하는 회복 조치도 마련할 필요가 있음

○ 향후 기술적 조처나 비기술적 조처를 신규로 도입할 경우 근거 규정을 미리 마련할 필요가 있으며, 국민여론 수렴 과정은 물론 전문가 집단을 중심으로 한 영향평가 등을 적극 도입할 필요가 있음

- 새로운 조처를 시행하기 전에 도입 절차와 운용, 사업자 협조 의무 등과 관련한 법적, 제도적 근거로서 근거 규정(지침이나 고시)를 미리 마련해 놓을 필요가 있음

- 근거 규정을 마련하는 과정에서 국민의 여론 수렴 및 관련 전문가들의 자문을 거치고, 새로운 조치를 시행할 경우 근거 규정에 따라 사전적·사후적으로 정책영향 평가, 공청회·세미나 등 국민 여론수렴 절차 등을 거칠 필요가 있음

○ 콘텐츠 서비스 제공자 또는 게시자의 방어권 보호와 이용자의 정보 접근권 보장을 제고하기 위해 접속차단 조치 이전에 해당 콘텐츠 제공자 및 게시자에게 사전 의견 진술의 기회를 제공하거나 이의신청을 적극적으로 보장할 수 있는 노력이 필요함

- 기존 차단사이트에서 불법성이 해소되었다고 확인되었을 경우, 불법사이트 목록에서

해당사이트를 삭제하는 조치를 마련하는 등 합법적인 정보접근권 보장을 위한 추가적인 노력이 필요함

- 사이트 전체에 대한 접속차단이 아닌 불법정보만 선별하여 삭제하거나 차단하는 방안 마련을 위한 지속적인 노력이 필요함

다. 인터넷 불법정보의 내용규제 제도 개선에 관한 권고

○ 접속차단 조치는 불법정보 유통과 그로 인한 피해 확산에 대한 긴급하고 적절한 조치를 마련하라는 국민적 요구에 대응하는 행정적 조치로 도입된 제도임. 다만 표현의 자유와 인터넷 이용자의 권익 보호 등의 공익목표를 고려한 균형적 운용을 위한 추가적인 노력이 필요함

- 긴급한 조치가 필요한 불법정보의 경우, 국제공조에 의한 수사, 법적 피해구제나 처벌 등의 절차는 신속성이 떨어져 한계가 있으므로 임시적 조치로서 SNI 필드 기반 접속차단 도입은 불가피함

- 다만 불법정보의 종류에 따라 긴급성을 요 하지 않는 경우도 있으므로, 시대적·사회적 흐름에 따른 국민 인식 변화를 고려하여 통신심의의 대상이 되는 정보의 명확한 범위에 대한 지속적인 논의와 사회적 합의가 필요함

○ 인터넷상에서의 표현의 자유에 대한 요구가 증가하고, 불법정보에 대한 국민 인식이 변화하고 있기 때문에, 국민적 공감을 얻을 수 있는 인터넷 규제체계 개선을 위해 여러 이해관계자가 참여하는 다자간 논의틀을 구성할 필요가 있음

- 현행 국내법 체계에서 디지털성범죄나 지적재산권 침해 등과 같이 신속한 처리를 요구하는 사안에 대해 법원이 신속한 판단을 내리는 것은 어렵다는 현실적 한계에 대한 지적이 있음

- 인터넷의 개방성을 보호하고 표현의 자유를 보장하기 위해서 정보의 불법성 여부를 궁극적으로 사법부에서 실효성 있게 판단할 수 있는 제도 개선이 필요하다는 의견이

제기되었음

라. 사회적 자율개선 역량에 관한 권고

○ 콘텐츠 제공자 및 게시자 스스로의 자율적인 개선노력 강화를 위해 사회적 합의와 정책적 지원을 위해 노력이 필요함

- 콘텐츠 제공자 및 게시자들의 자율규제 운영 현황 등을 모니터링하고 피드백을 제공할 수 있는 민관 협력 체계를 구축할 필요가 있음

○ 인터넷 이용자 스스로 불법정보의 확산을 방지할 수 있는 자율적인 개선 역량을 확보할 수 있도록, 다양한 정책적 지원 수단을 적극적으로 활용할 필요가 있음

- 불법정보 접속 및 유포 행위에 대한 인식 개선과 인터넷 윤리와 미디어 리터러시 교육 등을 통한 인터넷 이용자의 자율적인 개선 역량 강화가 요구됨

2. 기술적 차단조치에 대한 권고

가. 불법정보 유통방지의 실효성 제고를 위한 권고

○ 현재 기술수준에서 기술적 차단조치가 상당기간 유효할 것으로 예상되며, ESNI 표준화로 인해 기술적 접근차단 조치가 약화되지는 않을 것으로 판단됨

- 다만 접속차단 조치의 실효성을 평가할 수 있도록 관련 기관 및 단체에서 우회기술 사용현황을 조사할 필요가 있음

- ISP에서 소프트웨어 업데이트를 하는 등 TCP fragmentation을 이용한 우회접속을 방지할 수 있는 기술 대책 마련이 필요함

- VPN 사용현황에 대한 국내 통계 및 조사가 잘 이루어지지 않고 있어 향후 방통위 등 관련 부처 및 기관, 단체에서 VPN을 비롯한 우회기술 사용현황을 체계적으로 조사할 필요가 있음

- 불법 사이트 주소 변경에 대한 모니터링을 강화하고 이를 통한 불법정보 확산에 신속하게 대응하는 조치 강화가 필요함

○ 불법사이트 운영자가 사이트 주소를 변경하여 접속차단을 우회하는 행위에 신속히 대응할 수 있도록 주소변경 행위 등을 분석하는 알고리즘 기술개발이 필요하며 이를 불법사이트 모니터링에 활용할 필요가 있음

○ 불법정보가 게시된 사이트 전체에 대한 접속차단으로 인한 과잉차단 우려를 해소하고, 불법정보 유통방지의 실효성을 높이려면 불법정보만 선별하여 삭제·차단할 수 있는 기술적 대안 마련이 필요함

참 고 문 헌

국내 문헌

김정민 (20201.1.5.), 『8690원짜리를 500원에...인도 유튜브 프리미엄 이용 불법일까』, 중앙일보.

박찬제 (2019.12.18.), 『SNS에 버젓이 마약광고 뜨는데… '헤롱헤롱' 방통위, 겉 핥기 단속』, 뉴데일리.

방송통신위원회・방송통신심의위원회(2019. 2. 28.) 『해외 불법사이트 접속차단 해제 논란 관련 설명자료』, 보도자료, 방송통신위원회.

해외 문헌

Cimpanu, C. (2019. 3. 4). "Some Android VPN apps request access to sensitive permissions they don't need", ZDNET, Retrieved from *https://www.zdnet.com/article/some-android-vpn-apps-request-access-to-sensitive-permissions-they-dont-need/*

Cloudflare(2018. 5. 17). "You get TLS 1.3! You get TLS 1.3! Everyone gets TLS 1.3!", *The Cloudflare Blog*, Retrieved as of 12. 27. 2019 from https://blog.cloudflare.com/you-get-tls-1-3-you-get-tls -1-3-everyone-gets-tls-1-3/.

부 록

1. 시민단체 의견청취 결과

가. 추진배경

○ 배경: 해외 불법 사이트 접속차단과 관련하여 여론을 보다 적극적으로 수렴하기 위해 서로 다른 관점을 가진 시민단체들의 의견을 청취함

○ 대상: 오픈넷, 한국사이버성폭력대응센터

나. 의견청취 내용 요약

1) 오픈넷

○ 표현의 자유 침해 여부에 대한 의견

- 접속차단이 곧바로 정부가 개별 이용자들의 패킷이나 접속기록 내용을 직접 파악하는 형식의 감청은 아니고, 기존 접속차단 방식도 이용자들의 통신 패킷을 읽고 송·수신을 방해하는 방식이었다는 점에서, SNI 필드 차단에서만 새롭게 감청 논란을 제기할 것은 아님

- SNI 필드가 망사업자(통신사) 본연의 접속· 연결 업무를 하는 데에 필요한 기존 설비로도 읽고 통제할 수 있는 패킷이었는지, 아니면 본연의 업무와 무관하여 기존 설비로는 읽을 수 없는 패킷이었음에도, 정부가 적극적인 요구로 이를 읽고 통제할 수 있는 새로운 기술·설비를 도입하게 함으로써 그 영역을 넓힌 것인지, 현재로서 정확히 파악할 수는 없으나 그에 따라서도 평가가 달라질 수 있음

- SNI 필드 정보를 활용한 차단방식의 도입으로 국민의 통신비밀과 자유가 침해될 위험이 한층 높아진 것은 아닌지 앞으로도 민감하게 논의되고 감시될 필요는 분명히 존재함

○ 불법정보의 범위에 관한 의견

- 웹사이트 전체 차단 결정은 대부분 불법정보에 대해서만 이루어지고 있다고 하더라도, 심의할 수 있는 '정보통신망법상 불법정보' 가 지나치게 광범위함

- 행정기관에 의한 내용심의는 사법부의 불법 여부 판단을 기다릴 수 없을 정도로 사회적 해악이 심대하고 명백한, 매우 예외적인 경우(아동청소년이용음란물, 디지털성범죄물, 기타 국민의 신체, 재산에 명백하고 급박한 위해를 가할 위험이 있는 불법정보)에만 허용되어야 함

○ 심의체계에 관한 의견

- 행정기관은 사법부보다 불법 여부 판단에 있어서 전문적이지도 않을뿐더러, 규제기구로서의 성격 때문에 보다 규제주의적인 시각에서 심의 대상을 판단할 수밖에 없음

- 현재 판례상 방통심의위의 접속차단 시정요구도 일종의 행정처분임에도, 이러한 심의과정 및 결과가 직접 기본권을 제한당하는 일반 국민에게 제대로 고지되지 않고 있다는 점도 큰 문제임. 그 결과 어떤 웹사이트가 어떠한 근거로 차단 결정이 내려진 것인지, 즉, 그 행정처분이 적법하게 이루어진 것인지 행정 감시 및 적절한 불복이나 이의제기가 불가능함. 이번 SNI 필드 차단 방식의 경우에는 기술적 한계로 인하여 페이지 접속이 불가한 상태만이 나타나고 있어 더욱 문제되고 있음. 이는 행정절차의 적법성의 문제, 행정의 불투명성 문제를 야기하고 있음.

- 행정기관은 사법부보다 불법 여부 판단에 있어서 전문적이지도 않을뿐더러, 규제기구로서의 성격 때문에 보다 규제주의적인 시각에서 심의 대상을 판단할 수밖에 없음. 유엔과 국가인권위의 권고와 같이 근본적으로 민간자율기구에 통신심의 권한을 이양할 것이 요구됨.

2) 한국사이버성폭력대응센터

○ 표현의 자유 침해 여부에 대한 의견

- 표현의 자유는 보장되어야 하나, 타인의 권리를 침해하는 표현행위는 제한되어야 하며 디지털성범죄물과 같은 급박하고 명백한 피해가 발생하는 정보에 대한 차단은 사이버 공간 상에서 불법 행위의 피해자의 피해 확산을 방지하여 프라이버시 보호와 존엄을 보호하기 위한 최소한의 조치임

○ 불법정보의 범위에 관한 의견

- 제작된 음란물과 디지털성범죄물이 뒤섞여 유통되는 일반적 상황이 고려되어야 함

- 성폭력처벌법 등 국내법의 입법 공백 및 한계로 인해 명백한 피해자가 있음에도 불구하고 사이버성폭력으로 처벌할 수 없는 정보(예: 피해자의 얼굴이 합성된 음란물, 온라인 그루밍 등)가 있어 이에 대한 규제가 필요함

○ 심의체계에 관한 의견

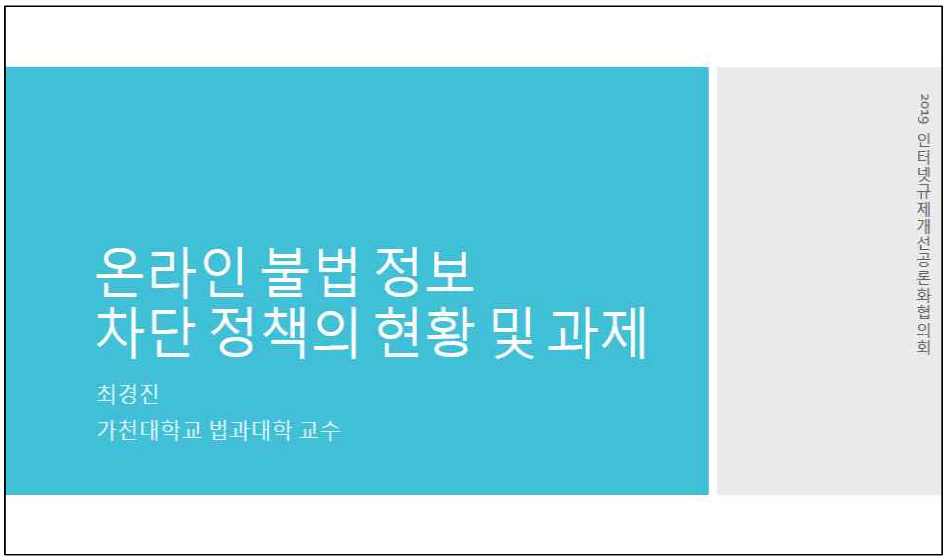
- 국내에는 긴급한 조치가 필요한 사안에 대해 신속하게 판단 및 조치를 내릴 수 있는 사법체계가 구축되어 있지 않기 때문에 현재로서는 통신심의를 통한 접속차단이 최소한의 조치로서 필요함

- 또한 디지털성범죄물 등과 같이 불법정보가 빠른 시간 내에 복제되어 광범위하게 퍼져나가 2차, 3차의 피해가 발생하는 사이버 공간의 특수성을 고려할 때 긴급한 접속차단 조치가 없다면 이를 방치하는 것과 동일하며, 디지털성폭력의 특성상 처벌은 그 의미가 작음

- 합성/편집, 계정 사칭, 지인능욕, 온라인 그루밍 등의 디지털성범죄물은 해외서버를 기반으로 한 불법 포르노사이트 및 P2P 사이트를 통해 무분별하게 무제한적으로 유포되는 현실을 고려할 때, 오랜 사회적 합의의 기간을 거쳐 법이 제·개정되는 것을 기다리기에는 사이버성폭력의 유포 속도와 범위가 통제 불가능한 영역이므로 수단적 필요성이 인정됨

2. 발제자료

○ 온라인불법정보 차단 정책의 현황 및 과제 (발제자: 최경진 교수, 가천대학교)




세계일보

https 차단·'주전자닷컴'…'벌레 잡겠다고 집 다 태웠다'

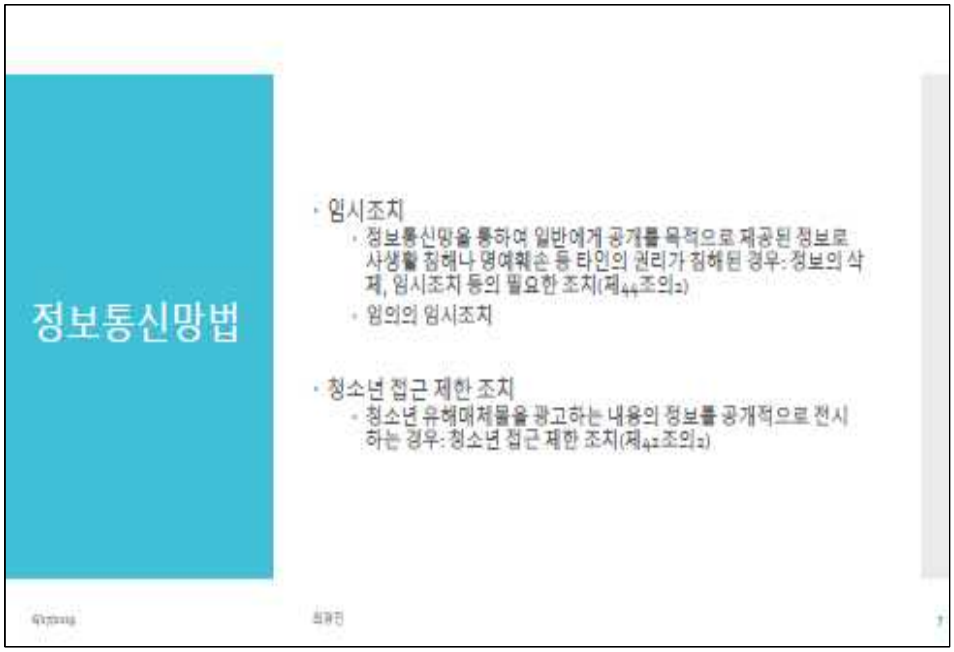
방통위 규제 두달째… 네티즌 "행정 편의" 만발 확산 / 검부 불법사이트 막는 新기술 놓고 / "감청 우려 여전한데 일방적 시행" / 靑 국민청원 게시판 반대글 수백건 / 초등생 제작한 게임 올린 사이트도 / "심의 단 받았다" 70만개 삭제 조치 / "예비창작 기회 뺏어" 비판 쏟아져

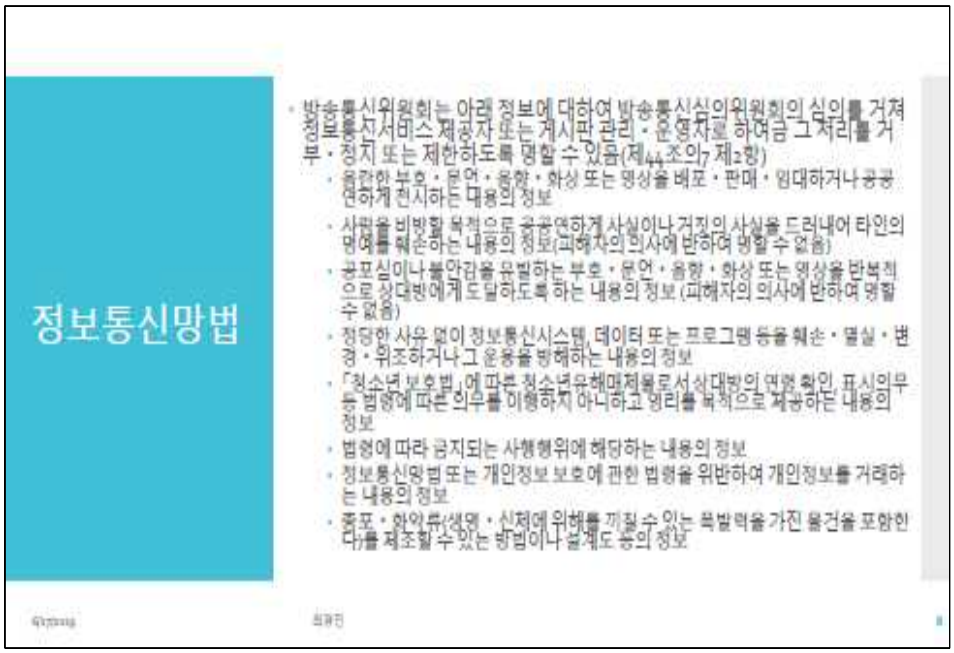
무엇이
문제인가?

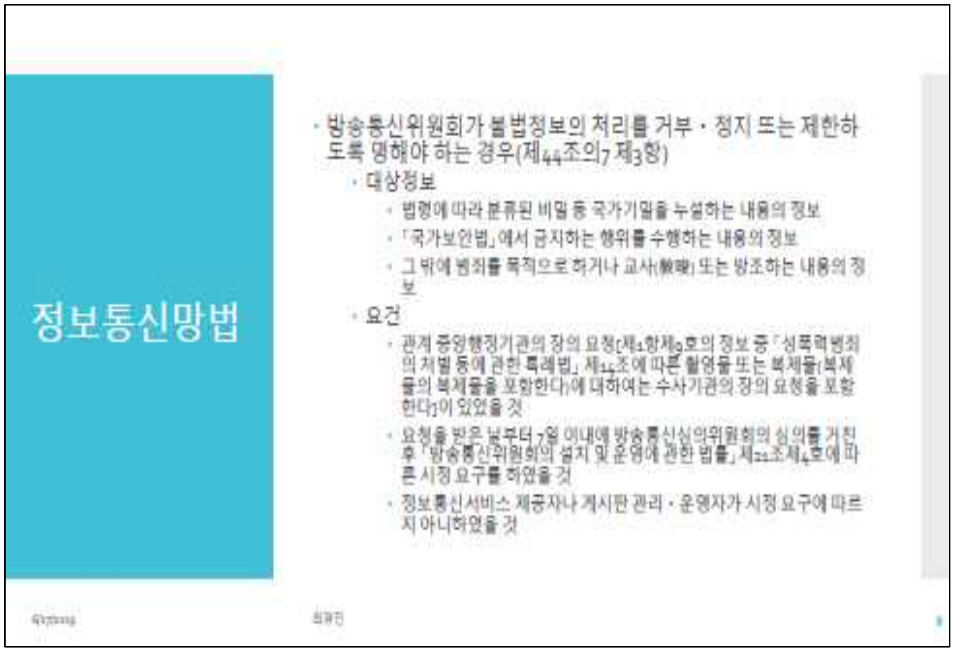
법.....감정

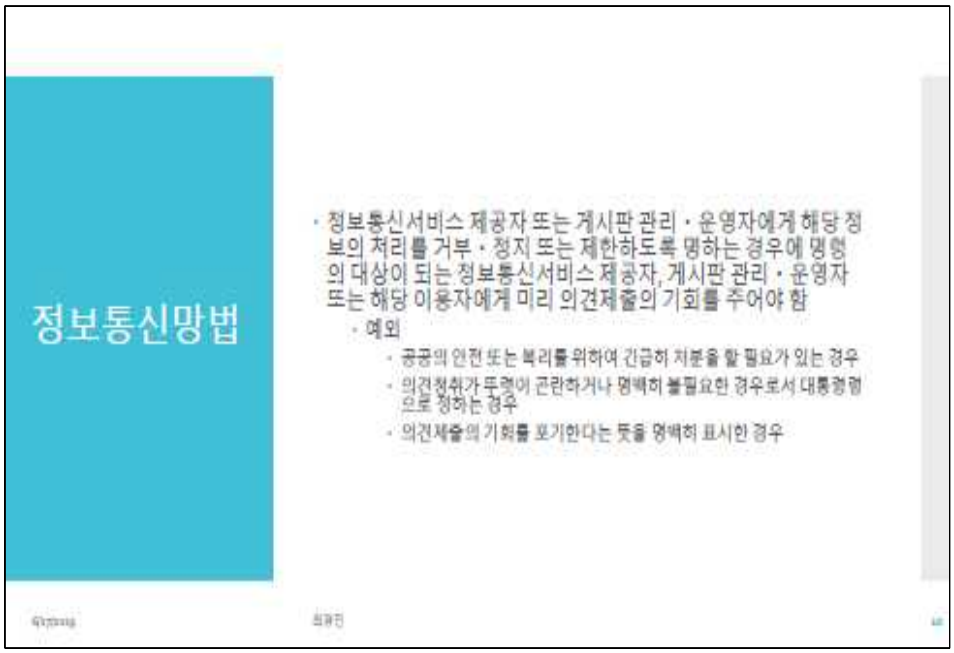
법, 해석, 적용, 집행

현실, 경험, 역사, 불신, 실효성


정보통신망법
• 임시조치
• 정보통신망을 통하여 일반에게 공개를 목적으로 제공된 정보로 사생활 침해나 명예훼손 등 타인의 권리가 침해된 경우: 정보의 삭제, 임시조치 등의 필요한 조치(제44조의2)
• 임의의 임시조치
• 청소년 접근 제한 조치
• 청소년 유해매체물을 광고하는 내용의 정보를 공개적으로 전시하는 경우: 청소년 접근 제한 조치(제42조의2)


정보통신망법
• 방송통신위원회는 아래 정보에 대하여 방송통신심의위원회의 심의를 거쳐 정보통신서비스 제공자 또는 게시판 관리·운영자로 하여금 그 처리를 거부·정지 또는 제한하도록 명할 수 있음(제44조의7 제2항)
• 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
• 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보(피해자의 의사에 반하여 명할 수 없음)
• 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보 (피해자의 의사에 반하여 명할 수 없음)
• 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
• 「청소년 보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
• 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
• 정보통신망법 또는 개인정보 보호에 관한 법령을 위반하여 개인정보를 거래하는 내용의 정보
• 폭포·화약류(생명·신체에 위해를 끼칠 수 있는 폭발력을 가진 물건을 포함한다)를 제조할 수 있는 방법이나 설계도 등의 정보


정보통신망법
• 방송통신위원회가 불법정보의 처리를 거부·정지 또는 제한하도록 명해야 하는 경우(제44조의7 제3항)
• 대상정보
• 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
• 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
• 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보
• 요건
• 관계 중앙행정기관의 장의 요청(제1항제9호의 정보 중 「성폭력범죄의 처벌 등에 관한 특례법」 제14조에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다)에 대하여는 수사기관의 장의 요청을 포함한다)이 있었을 것
• 요청을 받은 날부터 7일 이내에 방송통신심의위원회의 심의를 거친 후 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호에 따른 시정요구를 하였을 것
• 정보통신서비스 제공자나 게시판 관리·운영자가 시정요구에 따르지 아니하였을 것

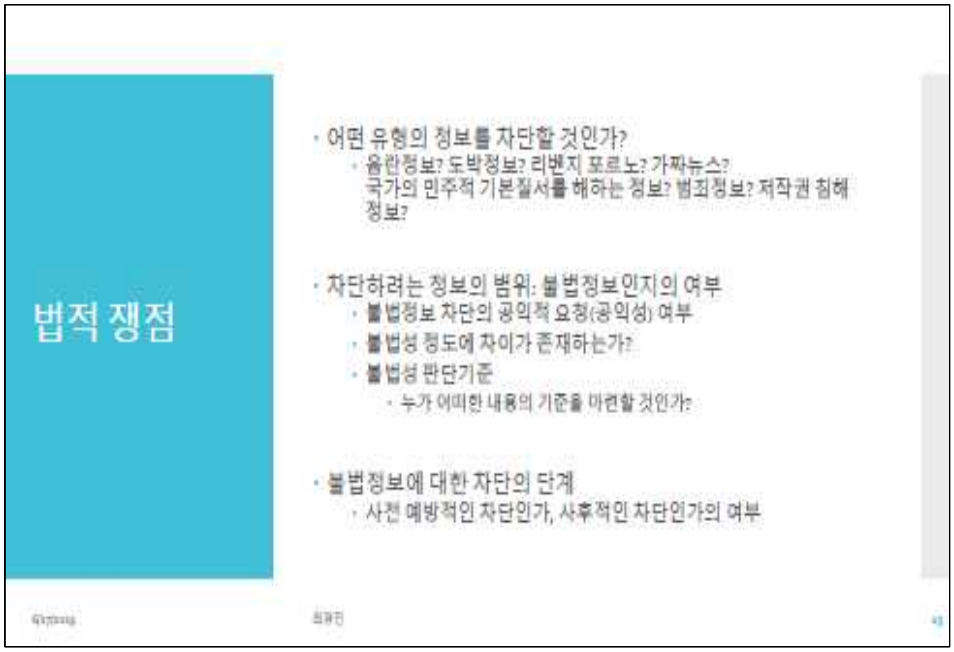

정보통신망법
• 정보통신서비스 제공자 또는 게시판 관리·운영자에게 해당 정보의 처리를 거부·정지 또는 제한하도록 명하는 경우에 명령의 대상이 되는 정보통신서비스 제공자, 게시판 관리·운영자 또는 해당 이용자에게 미리 의견제출의 기회를 주어야 함
• 예외
• 공공의 안전 또는 복리를 위하여 긴급히 처분을 할 필요가 있는 경우
• 의견청취가 뚜렷이 곤란하거나 명백히 불필요한 경우로서 대통령령으로 정하는 경우
• 의견제출의 기회를 포기한다는 뜻을 명백히 표시한 경우

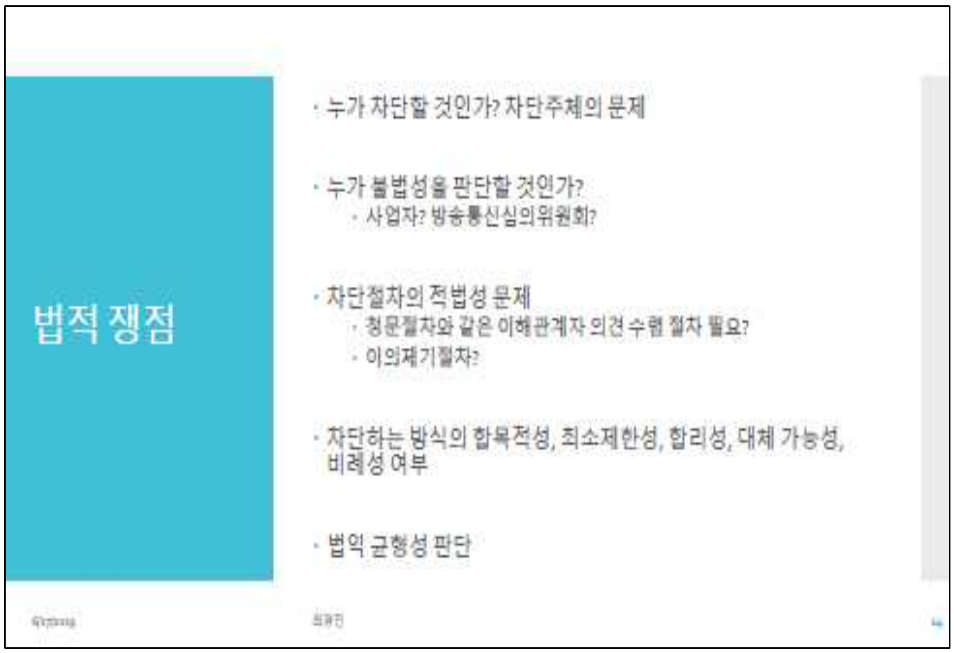
아동청소년의 성보호에 관한 법률

- 온라인서비스제공자의 의무(제17조)
  - 자신이 관리하는 정보통신망에서 아동·청소년이용음란물을 발견하기 위하여 대통령령으로 정하는 조치를 취하여야 함
  - 자신이 관리하는 정보통신망에서 발견된 아동·청소년이용음란물을 즉시 삭제하고, 전송을 방지 또는 중단하는 기술적인 조치를 취하여야 함
  - 특수한 유형의 온라인서비스제공자의 표시의무
    - 「저작권법」 제104조에 따른 특수한 유형의 온라인서비스제공자는 이용자가 컴퓨터 등에 저장된 저작물 등을 검색하거나 업로드 또는 다운로드를 할 경우 해당 화면이나 전송프로그램에 아동·청소년이용음란물을 제작·배포·소지한 자는 처벌을 받을 수 있다는 내용이 명확하게 표현된 경고문구를 대통령령으로 정하는 바에 따라 표시하여야 함

불법정보 차단방식

- 서버 IP 차단
- DNS 차단
- HTTP 통신 헤더의 호스트 정보를 이용한 차단
- SNI(Server Name Indication) 차단 방식


법적 쟁점
· 어떤 유형의 정보를 차단할 것인가?
· 음란정보? 도박정보? 리벤지 포르노? 가짜뉴스? 국가의 민주적 기본질서를 해하는 정보? 범죄정보? 저작권 침해 정보?
· 차단하려는 정보의 범위: 불법정보인지의 여부
· 불법정보 차단의 공익적 요청(공익성) 여부
· 불법성 정도에 차이가 존재하는가?
· 불법성 판단기준
· 누가 어떠한 내용의 기준을 마련할 것인가?
· 불법정보에 대한 차단의 단계
· 사전 예방적인 차단인가, 사후적인 차단인가의 여부


법적 쟁점
· 누가 차단할 것인가? 차단주체의 문제
· 누가 불법성을 판단할 것인가?
· 사업자? 방송통신심의위원회?
· 차단절차의 적법성 문제
· 청문절차와 같은 이해관계자 의견 수렴 절차 필요?
· 이의제기절차?
· 차단하는 방식의 합목적성, 최소제한성, 합리성, 대체 가능성, 비례성 여부
· 법익 균형성 판단

불법정보 차단의 법적 평가 기준

- 불법성 판단
  - "표현의 자유에서 요구하는 명확성의 요청 및 죄형법정주의의 명확성원칙"에 맞게 차단되는 불법 정보가 명확히 특정될 수 있어야 함
  - 2010. 12. 28. 2008헌바157, 2009헌바88(병합)

SNI 필드 차단방식이 적용된 해외 불법정보

(2019.4.10.기준, 단위: 건)

도박	음란	디지털 성범죄	권리 침해	저작권	불법 식·의약품	기타 불법	합계
7,451	1,610	1	1	308	118	136	9,625

※ 기타불법 : 명예 51건, 불법금융 32건, 성로린 위반 3건, 개인정보 침해 48건, 여론기기 2건

자료: 방송통신심의위원회 제출자료(2019.4.11.)

[2002. 6. 27. 99헌마480 전원재판부]

1.표현의 자유를 규제하는 입법에 있어서 명확성의 원칙은 특별히 중요한 의미를 지닌다. 무엇이 금지되는 표현인지가 불명확한 경우에, 자신이 행하고자 하는 표현이 규제의 대상이 아니라는 확신이 없는 기본권주체는 대체로 규제를 받을 것을 우려해서 표현행위를 스스로 억제하게 될 가능성이 높기 때문에 표현의 자유를 규제하는 법률은 규제되는 표현의 개념을 세밀하고 명확하게 규정할 것이 헌법적으로 요구된다. 그런데, "공공의 안녕질서 또는 미풍양속을 해하는"이라는 불온통신의 개념은 너무나 불명확하고 애매하다. 여기서의 "공공의 안녕질서"는 위 헌법 제37조 제2항의 "국가의 안전보장·질서유지"와, "미풍양속"은 헌법 제21조 제4항의 "공중도덕이나 사회윤리"와 비교하여 볼 때 동어반복이라 해도 좋을 정도로 전혀 구체화되어 있지 아니하다. 이처럼, "공공의 안녕질서", "미풍양속"은 매우 추상적인 개념이어서 어떠한 표현행위가 과연 "공공의 안녕질서"나 "미풍양속"을 해하는 것인지, 아닌지에 관한 판단은 사람마다의 가치관, 윤리관에 따라 크게 달라질 수밖에 없고, 법집행자의 통상적 해석을 통하여 그 의미내용을 객관적으로 확정하기도 어렵다.
2.전기통신사업법 제53조는 "공공의 안녕질서 또는 미풍양속을 해하는"이라는 불온통신의 개념을 전제로 하여 규제를 가하는 것으로서 불온통신 개념의 모호성, 추상성, 포괄성으로 말미암아 필연적으로 규제되지 않아야 할 표현까지 다함께 규제하게 되어 과잉금지원칙에 어긋난다. 즉, 헌법재판소가 명시적으로 보호받는 표현으로 분류한 바 있는 '저속한' 표현이나, 이른바 '청소년유해매체물' 중 음란물에 이르지 아니하여 성인에 의한 표현과 접근까지 금지할 이유가 없는 선정적인 표현물도 '미풍양속'에 반한다 하여 규제될 수 있고, 성(性), 혼인, 가족제도에 관한 표현들이 "미풍양속"을 해하는 것으로 규제되고 여민한 정치적, 사회적 이슈에 관한 표현들이 "공공의 안녕질서"를 해하는 것으로 규제될 가능성이 있어 표현의 자유의 본질적 기능이 훼손된다.
3.전기통신사업법 제53조 제2항은 "제1항의 규정에 의한 공공의 안녕질서 또는 미풍양속을 해하는 것으로 인정되는 통신의 대상 등은 대통령령으로 정한다"고 규정하고 있는바 이는 포괄위임입법금지원칙에 위배된다. 왜냐하면, 위에서 본 바와 같이 "공공의 안녕질서"나 "미풍양속"의 개념은 대단히 추상적이고 불명확하여, 수범자인 국민으로 하여금 어떤 내용들이 대통령령에 정하여질지 그 기준과 대강을 예측할 수도 없게 되어 있고, 행정입법자에게도 적정한 지침을 제공하지 못함으로써 그로 인한 행정입법을 제대로 통제하는 기능을 수행하지 못한다. 그리하여 행정입법자는 다분히 자신이 판단하는 또는 원하는 "안녕질서", "미풍양속"의 관념에 따라 헌법적으로 보호받아야 할 표현까지 얼마든지 규제대상으로 삼을 수 있게 되어 있다. 이는 위 조항의 위임에 의하여 제정된 전기통신사업법시행령 제26조 제2호와 제3호가 위 전기통신사업법 제53조 제1항에 못지 않게 불명확하고 광범위하게 통신을 규제하고 있는 점에서 더욱 명백하게 드러난다.
4.불온통신의 취급거부, 정지, 제한에 관한 전기통신사업법 제53조 제3항 및 불온통신의 개념을 정하고 있는 같은법시행령 제26조는 위헌인 같은 조 제2항, 제1항을 전제로 하고 있어 더 나아가 살필 필요 없이 각 위헌이다.

2010. 12. 28. 2008헌바157, 2009헌바88(병합)

공익을 해할 목적으로 전기통신설비에 의하여 공연히 허위의 통신을 한 자를 형사 처벌하는 전기통신기본법 제47조 제1항(이하 '이 사건 법률조항'이라 한다)은 은 표현의 자유에 대한 제한입법이며, 동시에 형벌조항에 해당하므로, 엄격한 의미의 명확성원칙이 적용된다. 그런데 이 사건 법률조항은 "공익을 해할 목적"의 허위의 통신을 금지하는바, 여기서의 "공익"은 형벌조항의 구성요건으로서 구체적인 표지를 정하고 있는 것이 아니라, 헌법상 기본권 제한에 필요한 최소한의 요건 또는 헌법상 언론·출판의 자유의 한계를 그대로 법률에 옮겨 놓은 것에 불과할 정도로 그 의미가 불명확하고 추상적이다. 따라서 어떠한 표현행위가 "공익"을 해하는 것인지, 아닌지에 관한 판단은 사람마다의 가치관, 윤리관에 따라 크게 달라질 수밖에 없으며, 이는 판단주체가 법전문가라 하여도 마찬가지이고, 법집행자의 통상적 해석을 통하여 그 의미내용이 객관적으로 확정될 수 있다고 보기 어렵다. 나아가 현재의 다원적이고 가치상대적인 사회구조 하에서 구체적으로 어떤 행위상황이 문제되었을 때에 문제되는 공익은 하나로 수렴되지 않는 경우가 대부분인바, 공익을 해할 목적이 있는지 여부를 판단하기 위한 공익간 형량의 결과가 언제나 객관적으로 명백한 것도 아니다. 결국, 이 사건 법률조항은 수범자인 국민에 대하여 일반적으로 허용되는 '허위의 통신' 가운데 어떤 목적의 통신이 금지되는 것인지 고지하여 주지 못하고 있으므로 표현의 자유에서 요구하는 명확성의 요청 및 죄형법정주의의 명확성원칙에 위배하여 헌법에 위반된다.

불법정보 차단의 법적 평가 기준

- 법익 균형성 판단
  - 달성하려는 공익과 제한되는 사익 사이의 법익 균형성이 확보되어야 함
  - 2011. 12. 29. 2007헌마1001, 2010헌바88, 2010헌마173 * 1941(병합)

[2011. 12. 29. 2007헌마1001, 2010헌바88, 2010헌마173 · 191(병합)]

인터넷은 누구나 손쉽게 접근 가능한 매체이고, 이를 이용하는 비용이 거의 발생하지 아니하거나 또는 적어도 상대적으로 매우 저렴하여 선거운동비용을 획기적으로 낮출 수 있는 정치공간으로 평가받고 있고, 오히려 매체의 특성 자체가 '기회의 균형성 · 투명성 · 저비용성의 제고'라는 공직선거법의 목적에 부합하는 것이라고도 볼 수 있는 점, 후보자에 대한 인신공격적 비난이나 허위사실 적시를 통한 비방 등을 직접적으로 금지하고 처벌하는 법률규정은 이미 도입되어 있고 모두 이 사건 법률조항보다 법정형이 높으므로, 결국 허위사실, 비방 등이 포함되지 아니한 정치적 표현만 이 사건 법률조항에 의하여 처벌되는 점, 인터넷의 경우에는 정보를 접하는 수용자 또는 수신자가 그 의사에 반하여 이를 수용하게 되는 것이 아니고 자발적 · 적극적으로 이를 선택(클릭)한 경우에 정보를 수용하게 되며, 선거과정에서 발생하는 정치적 관심과 열정의 표출을 반드시 부정적으로 볼 것은 아니라는 점 등을 고려하면, 이 사건 법률조항에서 선거일전 180일부터 선거일까지 인터넷상 선거와 관련한 정치적 표현 및 선거운동을 금지하고 처벌하는 것은 후보자 간 경제력 차이에 따른 불균형 및 흑색선전을 통한 부당한 경쟁을 막고, 선거의 평온과 공정을 해하는 결과를 방지한다는 입법목적 달성을 위하여 적합한 수단이라고 할 수 없다.
또한, 대통령 선거, 국회의원 선거, 지방선거가 순차적으로 닥쳐올 때에 비추어 보면, 기본권 제한의 기간이 지나치게 길고, 그 기간 '통상적 정당활동'은 선거운동에서 제외됨으로써 정당의 정보제공 및 홍보는 계속되는 가운데, 정당의 정강 · 정책 등에 대한 지지, 반대 등 의사표현을 금지하는 것은 일반 국민의 정당이나 정부의 정책에 대한 비판을 통해하여 정당정치나 책임정치의 구현이라는 대의제도의 이념적 기반을 약화시킬 우려가 있다는 점, 사이버선거부정감시단의 상시적 운영, 선거관리위원회의 공직선거법 위반 정보 삭제요청 등 인터넷 상에서 선거운동을 할 수 없는 자의 선거운동, 비방이나 허위사실 공표의 확산을 막기 위한 사전적 조치는 이미 별도로 입법화되어 있고, 선거관리의 주체인 중앙선거관리위원회도 인터넷 상 선거운동의 상시화 방안을 지속적으로 제시해오고 있는 점, 일정한 정치적 표현 내지 선거운동 속에 비방 · 흑색선전 등의 부정적 요소가 개입될 여지가 있다 하여 일정한 기간 이를 일률적 · 전면적으로 금지하고 처벌하는 것은 과도하다고 볼 수 밖에 없는 점 등을 감안하면, 최소침해성의 요건도 충족하지 못한다.
한편, 이 사건 법률조항에 대한 법익균형성 판단에는 국민의 선거참여를 통한 민주주의의 발전 및 민주적 정당성의 제고라는 공익 또한 감안하여야 할 것인데, 인터넷상 정치적 표현 내지 선거운동을 금지함으로써 얻어지는 선거의 공정성은 명백하거나 구체적이지 못한 반면, 인터넷을 이용한 의사소통이 보편화되고 각종 선거가 빈번한 현실에서 선거일 전 180일부터 선거일까지 장기간 동안 인터넷 상 정치적 표현의 자유 내지 선거운동의 자유를 전면적으로 제한함으로써 생기는 불이익 내지 피해는 매우 크다 할 것이므로, 이 사건 법률조항은 법익균형성의 요건도 갖추지 못하였다고 할 것이다.

불법정보 차단의 법적 평가 기준

- 최소 침해성 판단
  - "광범위하게 정하여 법집행자에게 자의적인 집행의 여지를 부여하고, 목적달성에 필요한 범위를 넘는 과도한 기본권 제한"이 없도록 하여야 함
    - 2012. 8. 23. 2010헌마47·252(병합)
  - "권한 남용을 방지하고 관련 기본권 제한이 최소화될 수 있도록 입법적 조치가 제대로 마련되어 있어야 한다"
    - 헌재 2018. 8. 30. 2015헌마263

[2012. 8. 23. 2010헌마47·251(병합)]

인터넷게시판을 설치·운영하는 정보통신서비스 제공자에게 본인확인조치의무를 부과하여 게시판 이용자로 하여금 본인확인절차를 거쳐야만 게시판을 이용할 수 있도록 하는 본인확인제를 규정한 '정보통신망 이용촉진 및 정보보호 등에 관한 법률'(2008. 6. 13. 법률 제9119호로 개정된 것) 제44조의5 제1항 제2호, 같은 법 시행령(2009. 1. 28. 대통령령 제21278호로 개정된 것) 제29조, 제30조 제1항(이하 위 조항들을 통칭하여 '이 사건 법령조항들'이라 한다)가 표방하는 건전한 인터넷 문화의 조성 등 입법목적은, 인터넷 주소 등의 추적 및 확인, 당해 정보의 삭제·임시조치, 손해배상, 형사처벌 등 인터넷 이용자의 표현의 자유나 개인정보자기결정권을 제약하지 않는 다른 수단에 의해서도 충분히 달성할 수 있음에도, 인터넷의 특성을 고려하지 아니한 채 본인확인제의 적용범위를 광범위하게 정하여 법집행자에게 자의적인 집행의 여지를 부여하고, 목적달성에 필요한 범위를 넘는 과도한 기본권 제한을 하고 있으므로 침해의 최소성이 인정되지 아니한다.

또한 이 사건 법령조항들은 국내 인터넷 이용자들의 해외 사이트로의 도피, 국내 사업자와 해외 사업자 사이의 차별 내지 자의적 법집행의 시비로 인한 집행 곤란의 문제를 발생시키고 있고, 나아가 본인확인제 시행 이후에 명예훼손, 모욕, 비방의 정보의 게시가 표현의 자유의 사전 제한을 정당화할 정도로 의미 있게 감소하였다는 증거를 찾아볼 수 없는 반면에, 게시판 이용자의 표현의 자유를 사전에 제한하여 의사표현 자체를 위축시킴으로써 자유로운 여론의 형성을 방해하고, 본인확인제의 적용을 받지 않는 정보통신망상의 새로운 의사소통수단과 경쟁하여야 하는 게시판 운영자에게 압무상 불리한 제한을 가하며, 게시판 이용자의 개인정보가 외부로 유출되거나 무당하게 이용될 가능성이 증가하게 되었는바, 이러한 인터넷게시판 이용자 및 정보통신서비스 제공자의 불이익은 본인확인제가 달성하려는 공익보다 결코 더 작다고 할 수 없으므로, 법익의 균형성도 인정되지 않는다.

따라서 본인확인제를 규율하는 이 사건 법령조항들은 과잉금지원칙에 위배하여 인터넷게시판 이용자의 표현의 자유, 개인정보자기결정권 및 인터넷게시판을 운영하는 정보통신서비스 제공자의 언론의 자유를 침해한다.

[헌재 2018. 8. 30. 2016헌마263]

인터넷회선감청은 인터넷회선을통하여 흐르는 전기신호형태의 패킷 을 중간에 확보한 다음 재조립 기술을거쳐 그 내용을 파악하는 이른바 패킷감청 의 방식으로 이루어진다. 따라서 이를 통해 개인의 통신뿐만 아니라 사생활의 비밀과 자유가 제한됨은 모불설 인터넷 사용이 일상화됨에 따라 국가 및 공공의안전, 국민의 재산이나 생목 신체의 안전을 위협하는 범행의 저지나 이의 처질러진 범죄수사에 필요한 경우 인터넷 통신망을 이용하는 전기통신에 대한 감청을 허용할 필요가 있으므로 이 사건 법률조항은 입법목적의 정당 성과 수단의 적합성이 인정된다.

인터넷회선 감청으로 수사기관은 타인 간 통신 및 개인의 내밀한 사생활의 영역에 해당하는 통신자료까지 취득할 수 있게 된다. 따라서 통신제한조치에 대한 법원의 허가 단계에서는 물론이고, 집행이나 집행 이후 단계에서도 수사기관의 권한 남용을 방지하고 관련 기본권 제한이 최소화될 수 있도록 입법적 조치가 제대로 마련되어 있어야 한다.

법은 '범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할만한 충분한 이유가 있는 경우' 보충적 수사방법으로 통신제한조치가 활용하도록 요건을 정하고 있고, 법원의 허가 단계에서 특정 피의자 내지 피내사자의 범죄수사를 위해 그 대상자가 사용하는 특정 인터넷회선에 한하여 필요한 범위 내에서만 감청이 이루어지도록 제한하고 있어 입다(법 제5조, 제6조).

그러나 패킷감청의 방식으로 이루어지는 인터넷회선 감청은 수사기관이 실제 감청 집행을 하는 단계에서는 해당 인터넷회선을 통하여 흐르는 불특정 다수인의 모든 정보가 패킷 형태로 수집되어 일단 수사기관에 그대로 전송되므로, 다른 통신제한조치에 비하여 감청 집행을 통해 수사기관이 취득하는 자료가 비교할 수 없을 정도로 매우 방대하다는 점에 주의할 필요가 있다.

불특정 다수가 하나의 인터넷회선을공유하여 사용하는 경우가 대부분이므로, 실제 집행 단계에서는 법원이 허가한 범위를 넘어 피의자 내지 피내사자의 통신자료뿐만 아니라 동일한 인터넷회선을 이용하는 불특정 다수인의 통신자료까지 수사기관에 모두 수집 저장된다. 따라서 인터넷회선 감청을 통해 수사기관이 취득하는 개인의 통신자료의 양을 전화감청 등 다른 통신제한조치와 비교할 바는 아니다.

따라서 인터넷회선 감청은 집행 중 그 이후에 제3자의 정보나 범죄수사와 무관한 정보까지 수사기관에 의해 수집 보관되고 있지는 않은지, 수사기관이 원래 허가받은 목적, 범위 내에서 자료를 이용,처리하고 있는지 등을 감독 내지 통제할 법적 장치가 강하게 요구된다.

그런데 현행법은 관련 공무원 등에게 비밀준수의무를 부과하고(법 제11조), 통신제한조치로 취득한 자료의 사용제한(법 제12조)을 규정하고 있는 것 외에 수사기관이 감청 집행으로 취득하는 막대한 양의 자료의 처리 절차에 대해서 아무런 규정을 두고 있지 않다.

현행법상 전기통신 가입자에게 집행 통지는 하게 되어 있으나 집행 사실 자체는 알려주지 않아야 하고, 수사가 장기화되거나 기소중지 처리되는 경우에는 감청이 집행도 사실조차 알 수 있는 길이 없으며 심지어 법 제9조의2는 더욱 제한적이고 사후적인 통지가 아닙다. 또한 현행법상 감청 집행으로 인하여 취득된 전기통신의 내용은 법원으로부터 허가를 받은 범죄와 관련된 범죄를 수사·소추하거나 그 범죄를 예방하기 위하여도 사용이 가능하므로(법 제12조 제1호) 특정인의 통항 따악이나 정보수집을 위한 목적으로 수사기관에 의해 남용될 가능성도 배제하기 어렵다.

인터넷회선 감청으로 통신비밀보호법상 감청을 수사상 필요에 의해 허용하면서도, 관련 기본권 침해를 최소화하기 위하여 집행 이후에도 주기적으로 경과보고서를 법원에 제출하도록 하거나, 감청을 허가한 판사에게 감청 자료를 봉인하여 제출하도록 하거나, 감청자료의 보관 내지 파기 여부를 판사가 결정하도록 하는 등 수사기관이 감청 집행으로 취득한 자료에 대한 처리 등을 객관적으로 통제할 수 있는 절차를 마련하고 있는 입법례가 상당수 있다.

이상을 종합하면, 이 사건 법률조항은 인터넷회선 감청의 특성을 고려하여 그 집행 단계나 집행 이후에 수사기관의 권한 남용을 통제하고 관련 기본권의 침해를 최소화하기 위한 제도적 조치가 제대로 마련되어 있지 않은 상태에서, 범죄수사 목적을 이유로 인터넷회선 감청을 통신제한조치 허가 대상 중 하나로 정하고 있으므로 침해의 최소성 요건을 충족한다고 할 수 없다.

이러한 여건 하에서 인터넷회선의 감청을 허용하는 것은 개인의 통신 및 사생활의 비밀과 자유에 심각한 위협을 초래하게 되므로 이 사건 법률조항으로 인하여 달성하려는 공익과 제한되는 사익 사이의 법익 균형성도 인정되지 아니한다.

그러므로 이 사건 법률조항은 과잉금지원칙에 위반하는 것으로 청구인의 기본권을 침해한다.

라. 이 사건 법률조항은 청구인의 기본권을 침해하여 헌법에 위반되지만, 단순위헌결정을 하면 수사기관이 인터넷회선 감청을 통한 수사를 할 수 없는 법률적 근거가 사라져 범죄의 실행 저지가 긴급히 요구되거나 국민의 생명, 신체, 재산의 안전을 위협하는 중대 범죄의 수사에 있어 범죄 분백이 발생할 우려가 있다.

한편, 이 사건 법률조항이 가지는 위헌성은 인터넷회선 감청의 특성에도 불구하고 수사기관이 인터넷회선 감청으로 취득하는 자료에 대해 사후적으로 감독 또는 통제할 수 있는 규정이 제대로 마련되어 있지 않다는 점에 있으므로 구체적 개선방안에 관한 기준과 요건에 따라 마련될 것인지는 입법자의 재량에 속한다.

이러한 이유로 이 사건 법률조항에 대해 단순위헌결정을하는 대신헌법불합치결정을 선고하되, 입법자가 이 사건 법률조항의 위헌성을 제거하고 합리적인 내용으로 개정할 때까지 계속 적용을 명하는 것이 타당하다.

또 다른
법적 쟁점 &
논란

불법 정보 차단을 위한 SNI 필드 차단이 감청인가?

6/17/2019 최경진 23

또 다른
법적 쟁점
- 감청

- 감청: 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치 등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것 (통신비밀보호법 제2조 제7호)
  - '전기통신의 감청'은 '감청'의 개념 규정에 비추어 전기통신이 이루어지고 있는 상황에서 실시간으로 전기통신의 내용을 지득·채록하는 경우와 통신의 송·수신을 직접적으로 방해하는 경우를 의미하는 것이지, 이미 수신이 완료된 전기통신에 관하여 남아 있는 기록이나 내용을 열어보는 등의 행위는 포함하지 않음(대법원 2016. 10. 13. 선고 2016도8137 판결)
  - 일반적으로 감청은 다른 사람의 대화나 통신 내용을 몰래 엿듣는 행위를 의미. 대상이 되는 전기통신의 송·수신과 동시에 이루어지는 경우만을 의미(대법원 2012. 10. 25. 선고 2012도4644 판결)
  - 통신비밀보호법에 규정된 '통신제한조치'는 '우편물의 검열 또는 전기통신의 감청'을 말함(통신비밀보호법 제3조제2항, 대법원 2016. 10. 13. 선고 2016도8137 판결)

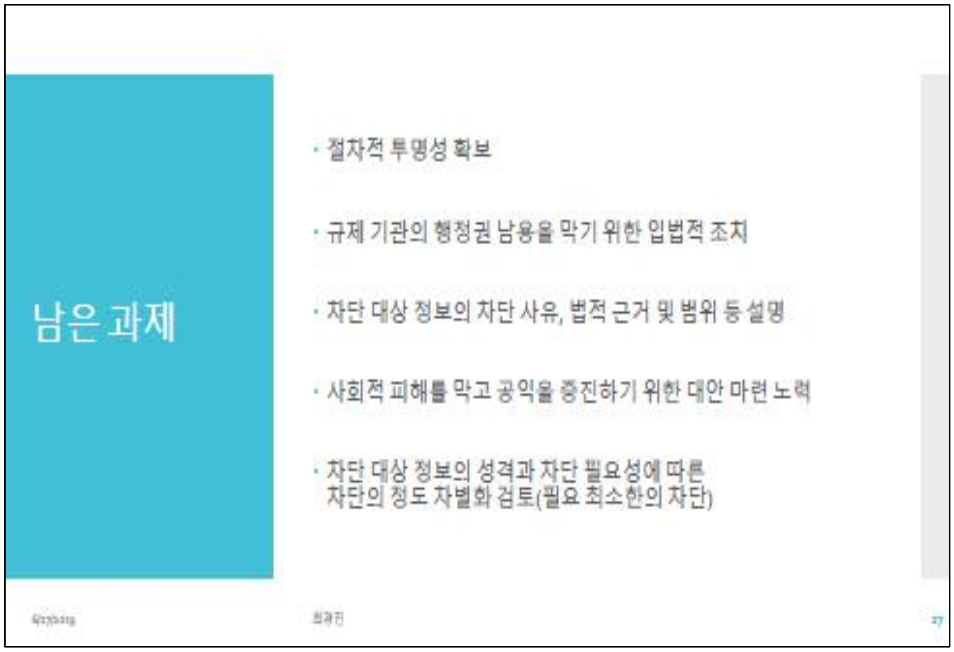
6/17/2019 최경진 24

또 다른 법적 쟁점 - 감청

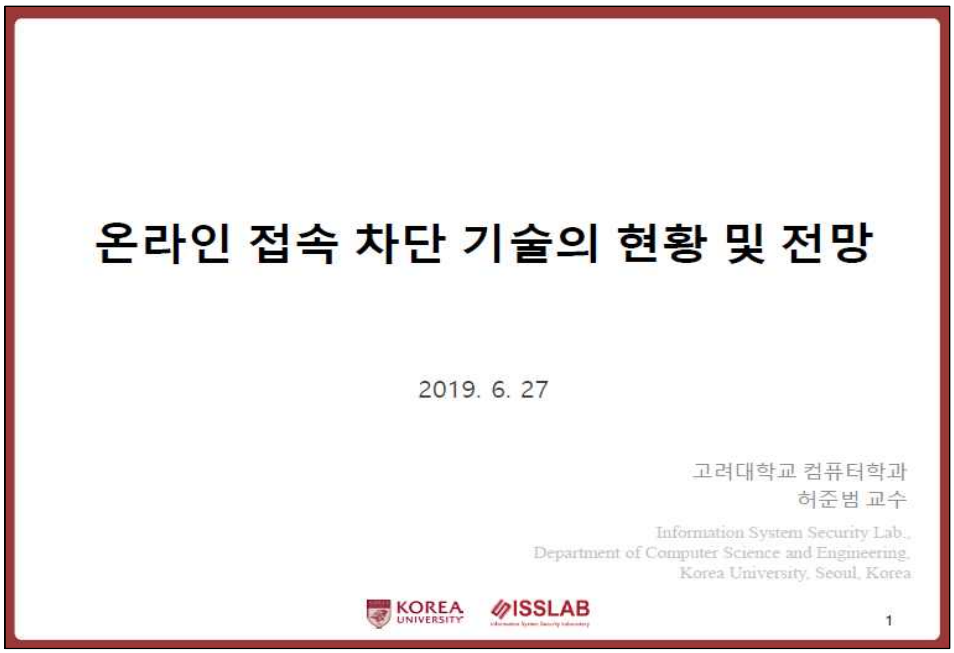
- 패킷 감청 논란
  - 패킷 감청: 전기신호 형태의 패킷(packet)을 중간에 확보하여 그 내용을 지득하는 행위(대법원 2012. 10. 11. 선고 2012도7455 판결)

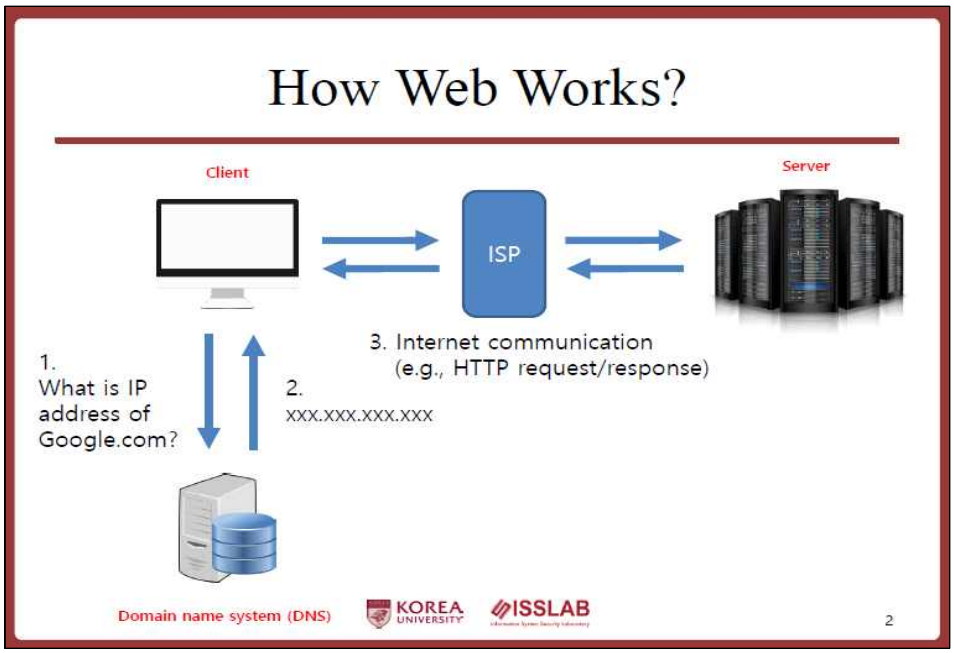
정책적 쟁점

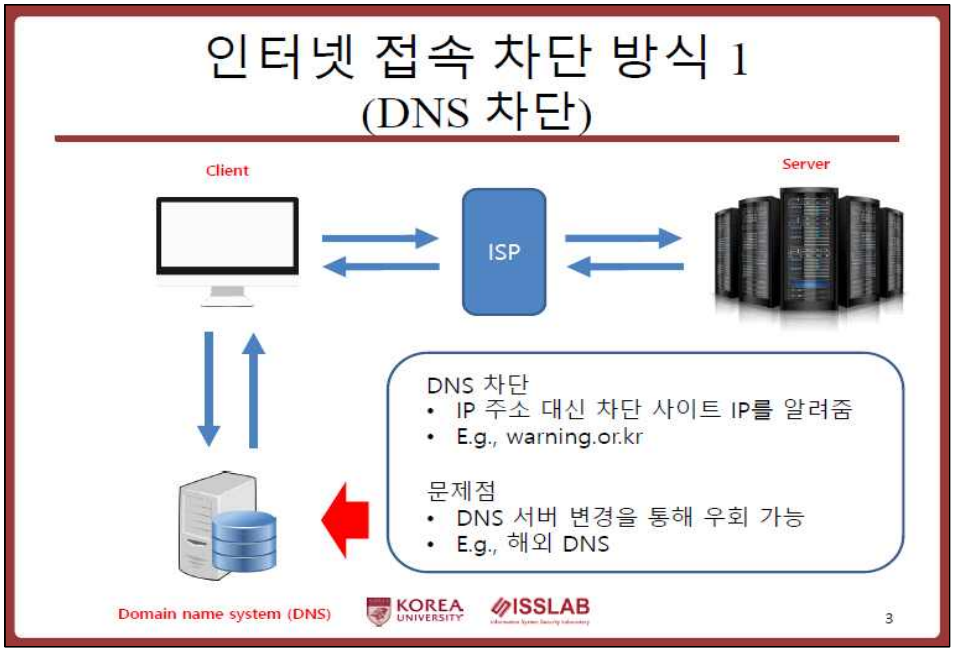
- 차단 방식을 변경하거나 추가하는 경우에 국민들의 Consensus를 모을 절차적 과정이 필요한가?
  - 감청 혹은 검열, 온라인 사찰(효果)에 대한 트라우마
- SNI 차단 방식이 실제 불법정보를 차단하는데 실효성이 있는가?
- SNI 차단이나 DNS 차단 등 다양한 방식을 활용한 '불법정보 차단 정책' 그 자체가 필요한가?
- 불법정보를 차단하기 위한 대안은 불가능한가?

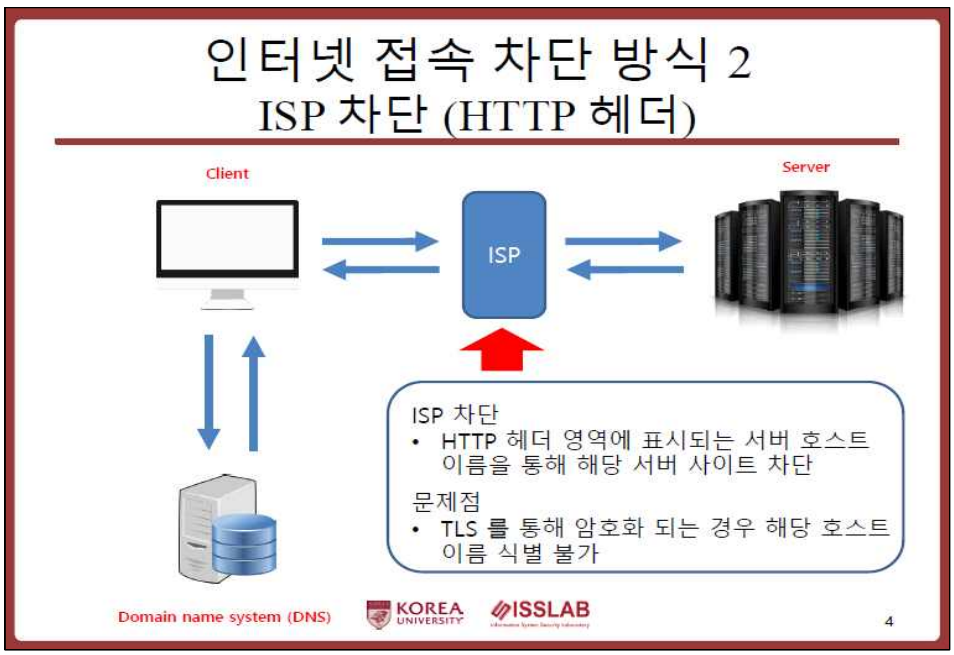

남은 과제
· 절차적 투명성 확보
· 규제 기관의 행정권 남용을 막기 위한 입법적 조치
· 차단 대상 정보의 차단 사유, 법적 근거 및 범위 등 설명
· 사회적 피해를 막고 공익을 증진하기 위한 대안 마련 노력
· 차단 대상 정보의 성격과 차단 필요성에 따른
차단의 정도 차별화 검토(필요 최소한의 차단)

○ 온라인 접속차단 기술의 현황 및 전망 (발제자: 허준범 교수, 고려대학교)






인터넷 접속 차단 방식 1
(DNS 차단)
Client
Server
ISP
DNS 차단
• IP 주소 대신 차단 사이트 IP를 알려줌
• E.g., warning.or.kr
문제점
• DNS 서버 변경을 통해 우회 가능
• E.g., 해외 DNS
Domain name system (DNS)
KOREA UNIVERSITY
ISSLAB
3


인터넷 접속 차단 방식 2
ISP 차단 (HTTP 헤더)
Client
Server
ISP
ISP 차단
• HTTP 헤더 영역에 표시되는 서버 호스트 이름을 통해 해당 서버 사이트 차단
문제점
• TLS 를 통해 암호화 되는 경우 해당 호스트 이름 식별 불가
Domain name system (DNS)
KOREA UNIVERSITY
ISSLAB
4

HTTP & HTTPS

- HTTP (HyperText Transfer Protocol)
  - WWW 상에서 client와 server가 정보를 주고받는 (request/response) 프로토콜
  - 주로 HTML 문서를 주고받음
- HTTPS
  - HTTP over TLS
  - HTTP를 통해 주고받는 통신 데이터를 TLS 암호화를 통해 보호

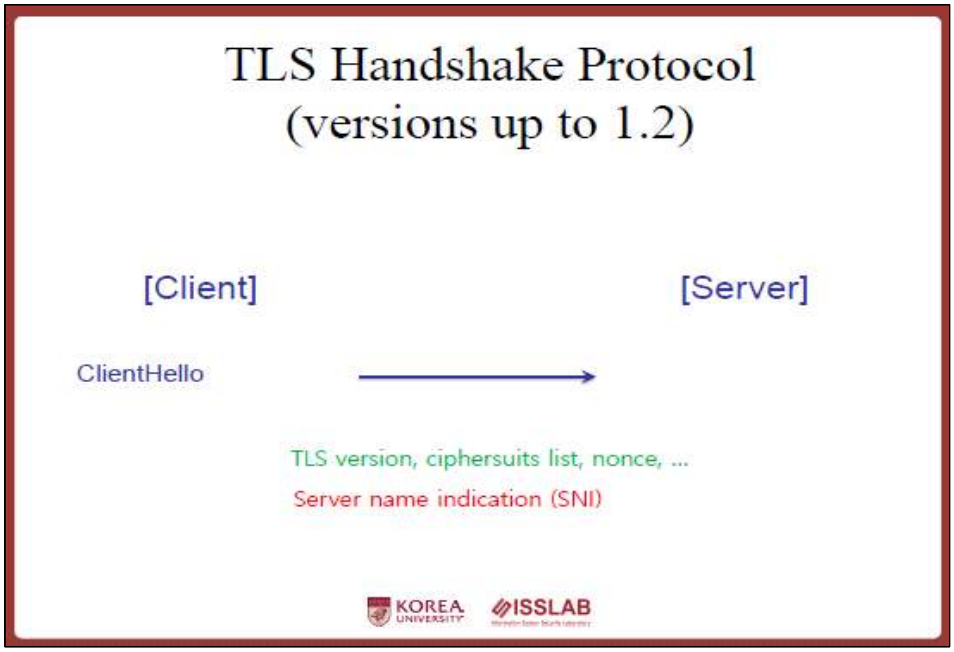
KOREA UNIVERSITY ISSLAB

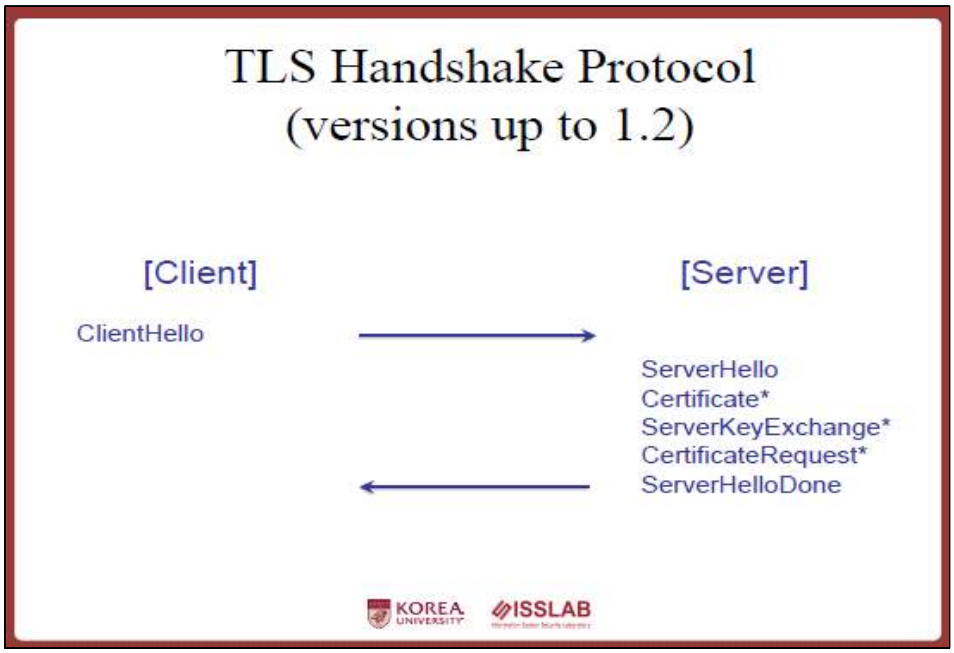
5

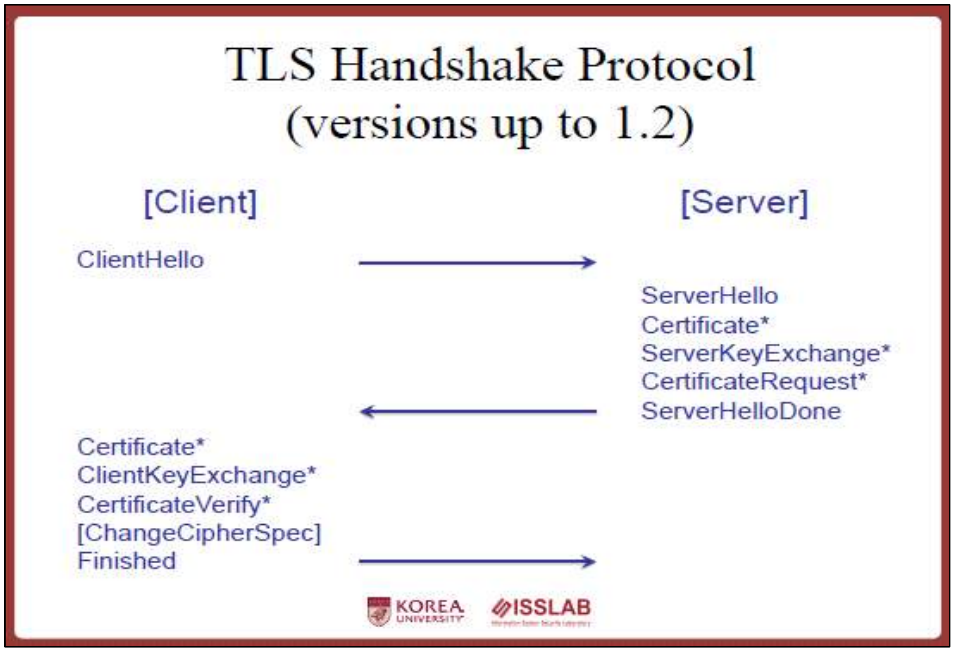
Transport Layer Security

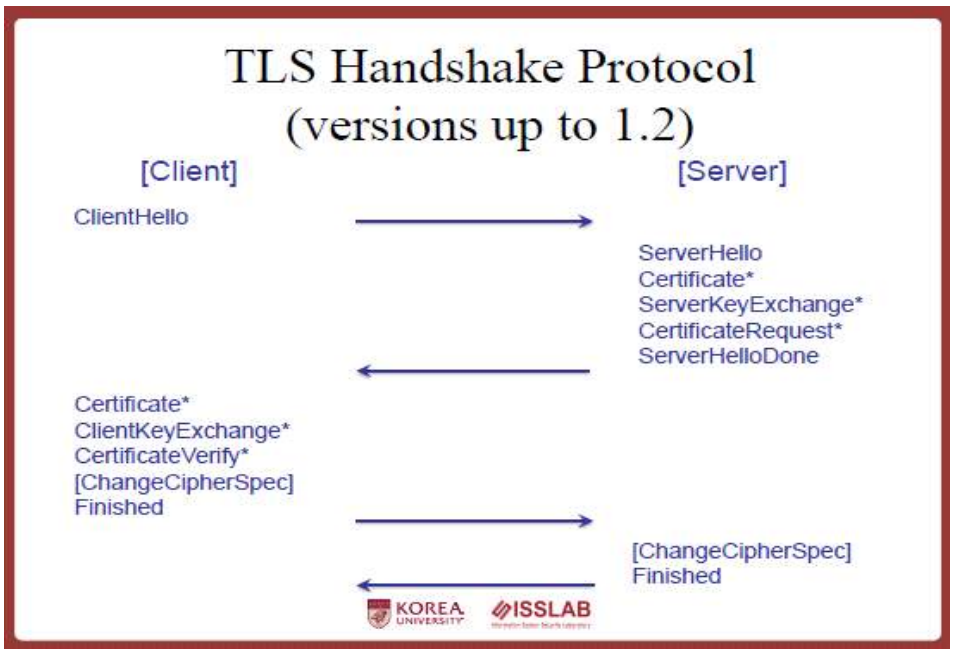
- Transport Layer Security (TLS) and its predecessor Secure Sockets Layer (SSL) are cryptographic protocols designed to provide communications security over a computer network
- The primary goal
  - Provide privacy and data integrity between two communicating computer applications

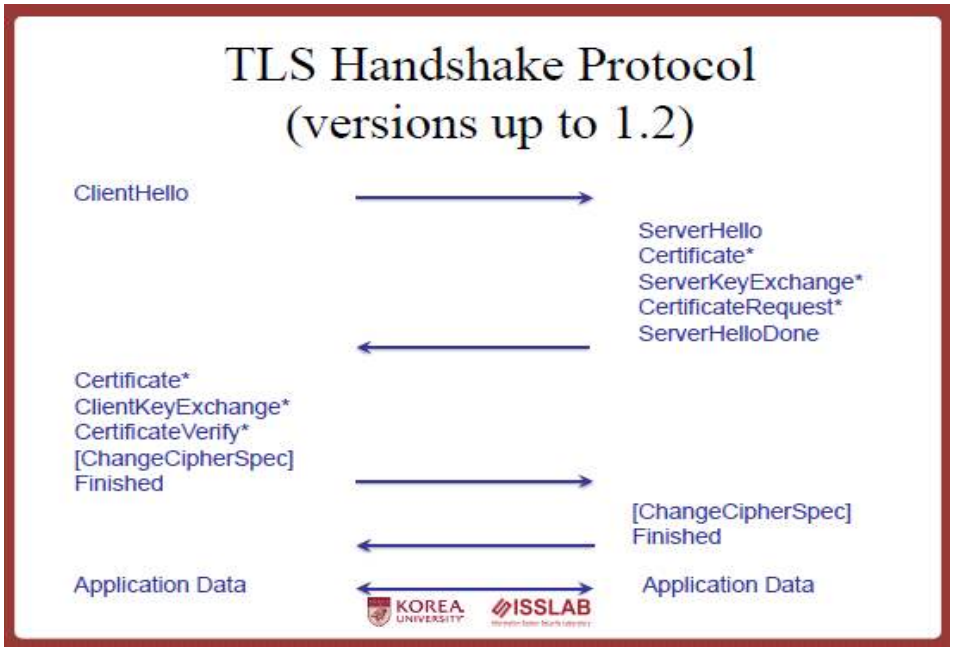
KOREA UNIVERSITY ISSLAB

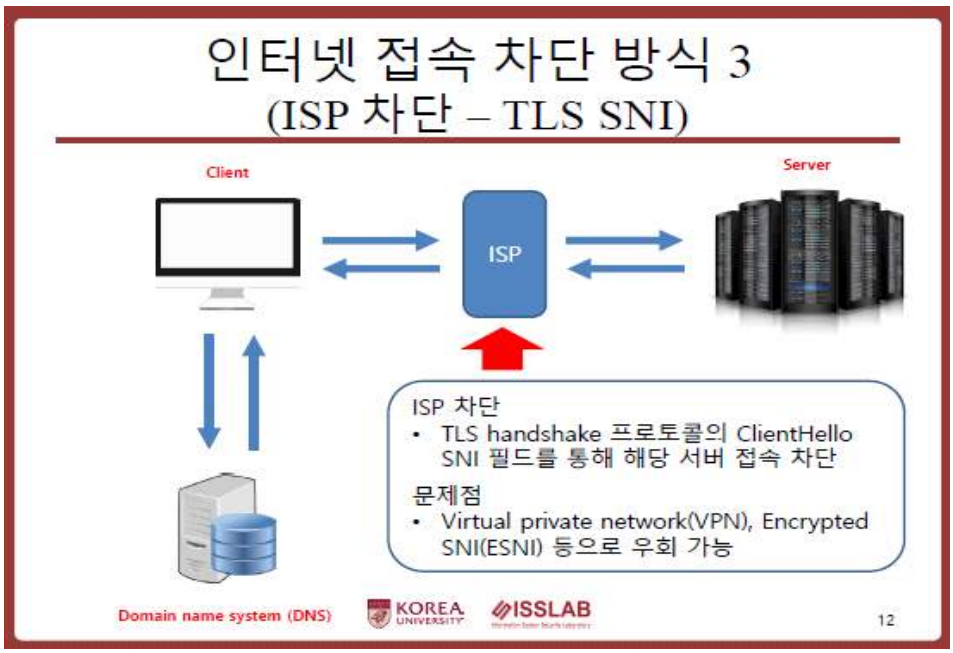

TLS Handshake Protocol
(versions up to 1.2)
[Client]
[Server]
ClientHello
TLS version, ciphersuits list, nonce, ...
Server name indication (SNI)
KOREA UNIVERSITY
ISSLAB


TLS Handshake Protocol
(versions up to 1.2)
[Client]
[Server]
ClientHello
ServerHello
Certificate*
ServerKeyExchange*
CertificateRequest*
ServerHelloDone
KOREA UNIVERSITY
ISSLAB


TLS Handshake Protocol
(versions up to 1.2)
[Client]
[Server]
ClientHello
ServerHello
Certificate*
ServerKeyExchange*
CertificateRequest*
ServerHelloDone
Certificate*
ClientKeyExchange*
CertificateVerify*
[ChangeCipherSpec]
Finished
KOREA UNIVERSITY
ISSLAB

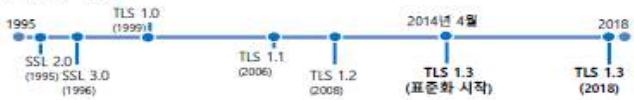

TLS Handshake Protocol
(versions up to 1.2)
[Client]
[Server]
ClientHello
ServerHello
Certificate*
ServerKeyExchange*
CertificateRequest*
ServerHelloDone
Certificate*
ClientKeyExchange*
CertificateVerify*
[ChangeCipherSpec]
Finished
[ChangeCipherSpec]
Finished
KOREA UNIVERSITY
ISSLAB


TLS Handshake Protocol
(versions up to 1.2)
ClientHello
ServerHello
Certificate*
ServerKeyExchange*
CertificateRequest*
ServerHelloDone
Certificate*
ClientKeyExchange*
CertificateVerify*
[ChangeCipherSpec]
Finished
[ChangeCipherSpec]
Finished
Application Data
Application Data
KOREA UNIVERSITY
ISSLAB


인터넷 접속 차단 방식 3
(ISP 차단 – TLS SNI)
Client
Server
ISP
ISP 차단
• TLS handshake 프로토콜의 ClientHello SNI 필드를 통해 해당 서버 접속 차단
문제점
• Virtual private network(VPN), Encrypted SNI(ESNI) 등으로 우회 가능
Domain name system (DNS)
KOREA UNIVERSITY
ISSLAB
12

TLS 1.3 표준화

- SSL/TLS 발전 과정



  - 개발주기가 design-release-break-patch 에서 design-break-fix-release cycle로 변경
  - 기존 TLS와 새로 제안된 프로토콜에 대한 취약점 연구를 연계한 표준화 진행
  - 2018년 8월 28일, TLS 1.3 (RFC 8446) 발표
  - 주요 오픈소스 암호라이브러리 및 상용 브라우저 TLS 1.3 지원

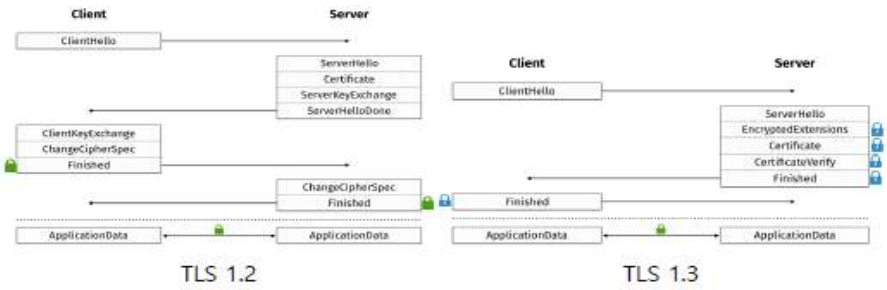
TLS 1.3 이후 SNI 기반 인터넷 차단기술이 유용할 것인가?

KOREA UNIVERSITY ISSLAB

13

TLS Full Handshake Protocol Overview

- Full Handshake



: handshake_traffic_key 암호화
: application_traffic_key 암호화

TLS 1.3 ClientHello 메시지는 암호화되지 않음

KOREA UNIVERSITY ISSLAB

14

After TLS 1.3

- TLS SNI 기반 차단 방식은 당분간 유효한 인터넷 차단 기술로 활용 가능
  - VPN 등에 대한 이용률이 높지 않은 상황
  - TLS 1.2는 최근 10년간 최신 표준으로 사용
  - TLS 1.3은?

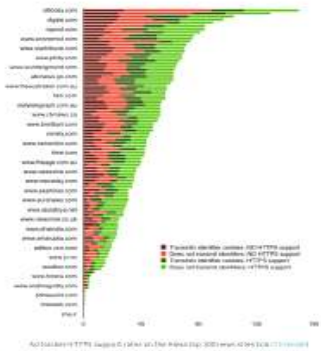
KOREA UNIVERSITY ISSLAB

15

What ISPs Can See?

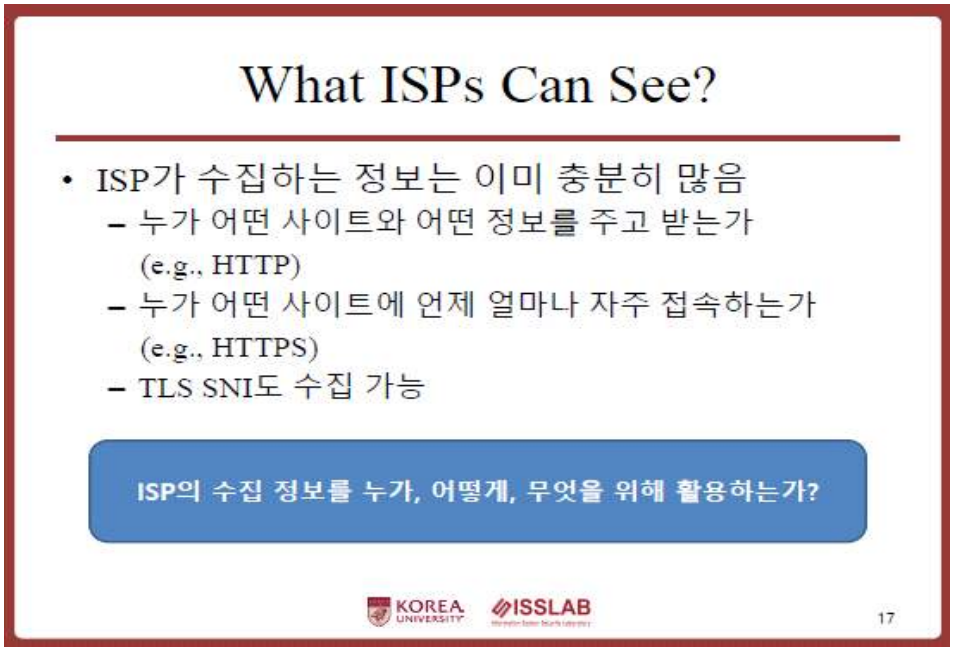
- https://www.upturn.org/reports/2016/what-isps-can-see/

Today, ISPs can see a significant amount of their subscribers' Internet activity, and have the ability to infer substantial amounts of sensitive information from it. This is especially true when that traffic is unencrypted. However, even when Internet traffic is encrypted using HTTPS, ISPs generally retain visibility into their subscribers' DNS queries. Detailed analysis of DNS query information on a per-subscriber basis is not only technically feasible and cost-effective, but actually takes place in the field today. Moreover, ISPs and the vendors that serve them have clear opportunities to develop methods of inferring important information even from encrypted data flows. VPNs are one tool that subscribers can use to protect their online activities, but VPNs are poorly adopted, can be difficult to use, and often provide incomplete protections.

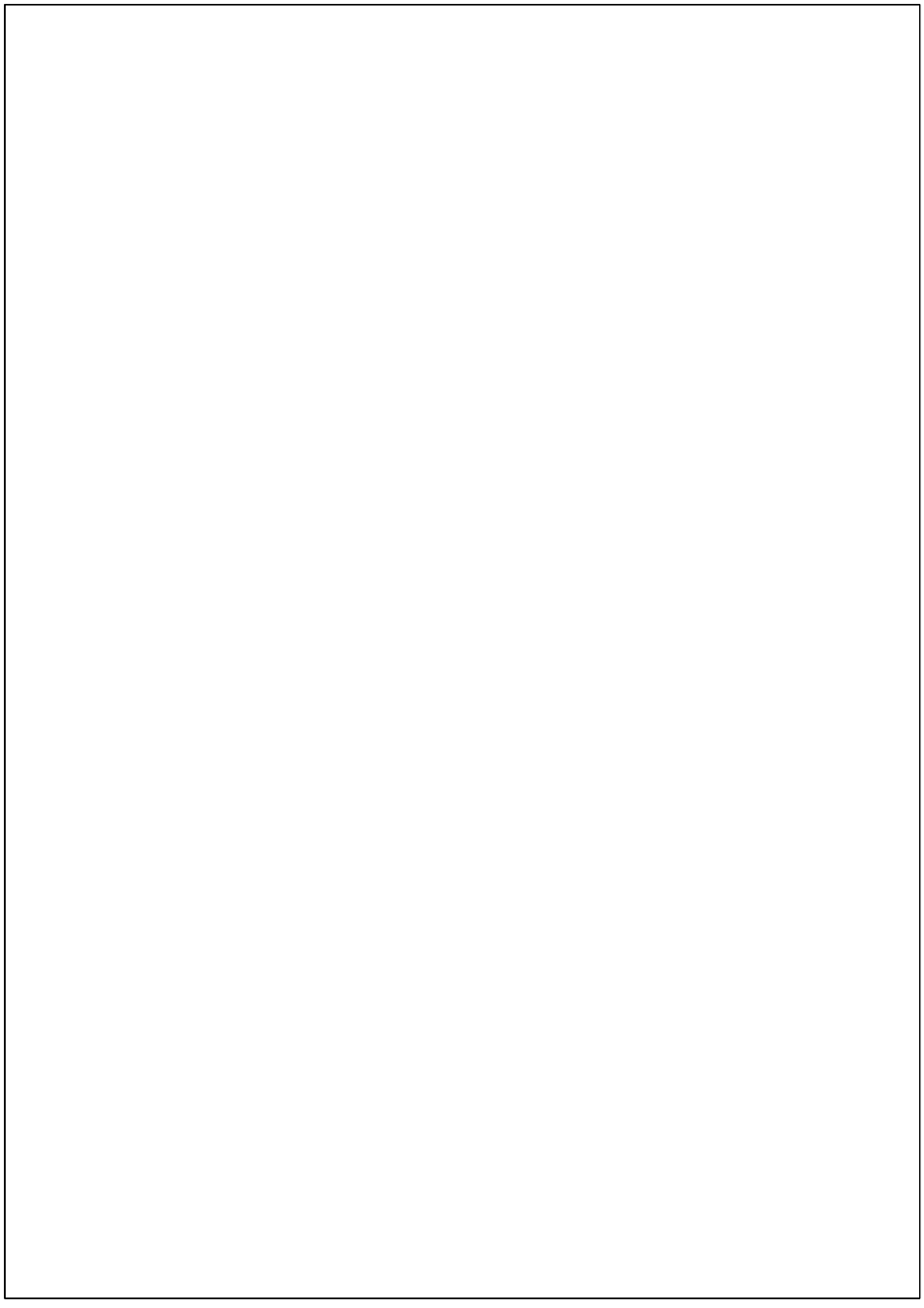


KOREA UNIVERSITY ISSLAB

16


What ISPs Can See?
• ISP가 수집하는 정보는 이미 충분히 많음
– 누가 어떤 사이트와 어떤 정보를 주고 받는가
(e.g., HTTP)
– 누가 어떤 사이트에 언제 얼마나 자주 접속하는가
(e.g., HTTPS)
– TLS SNI도 수집 가능
ISP의 수집 정보를 누가, 어떻게, 무엇을 위해 활용하는가?
KOREA UNIVERSITY
ISSLAB
17

○ 해외 불법정보 유통방지 대응현황(발제자: 방송통신심의위원회)



URL 차단방식의 기술적 한계를 보완하는「SNI필드 차단 방식」 도입 방안을 논의하였고, 2019년 2월 11일부터 본격적으로 시행하기로 결정하였음.

지난 2월 11일 이후 7월 31일 현재까지, 해외 불법정보로 시정요구(접속차단)하여 SNI필드 차단방식이 적용된 사이트는 총 28,011건으로, 도박 19,924건, 음란* 5,462건, 저작권 1,460건, 불법 식·의약품 678건, 마약 234건, 개인정보 침해 131건, 불법금융 82건, 기타 불법 40건(상표권 침해 26건 등)임.

※ 특히, 음란물의 경우에는 성인사이트가 아닌 해외 불법 음란사이트(포르노 사이트)임.

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

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

제74조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 1년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

2. 제44조의7제1항제1호를 위반하여 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시한 자

「형법」

제244조(음화제조 등) 제243조의 행위에 공할 목적으로 음란한 물건을 제조, 소지, 수입 또는 수출한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

< 해외 불법정보 SNS 필드 차단방식 통계 >

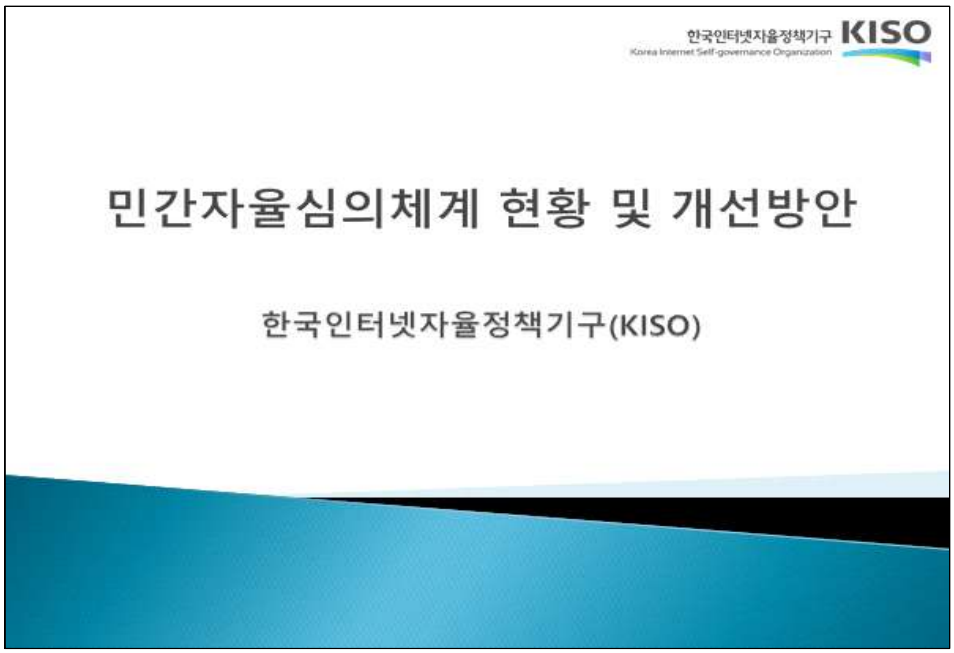
(2019.7.31. 기준, 단위 : 건)

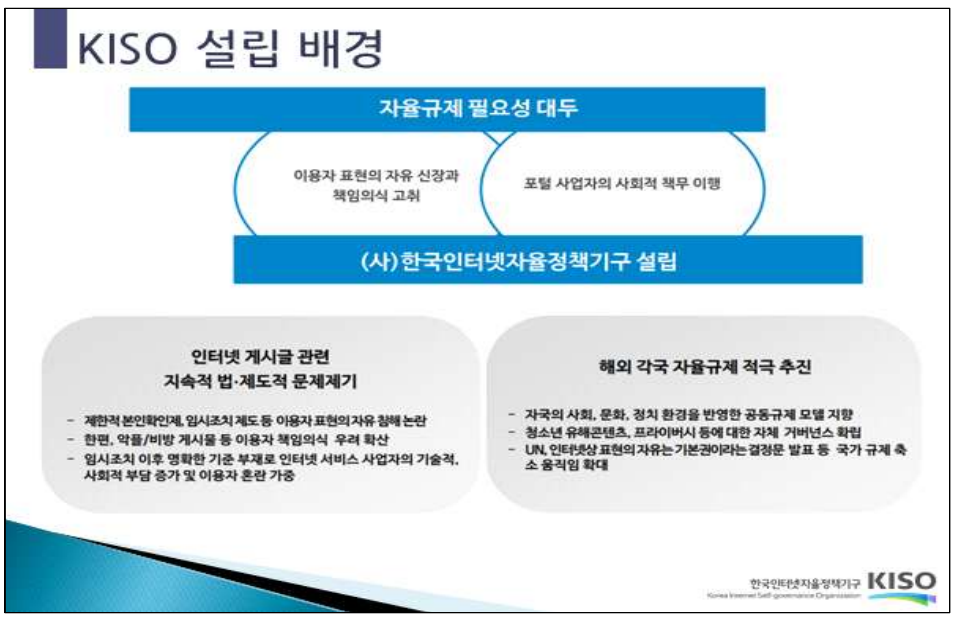
도박	음란	저작권	불법 식의약품	마약	개인정보 침해	불법 금융	기타 불법	합계
19,924	5,462	1,460	678	234	131	82	40	28,011

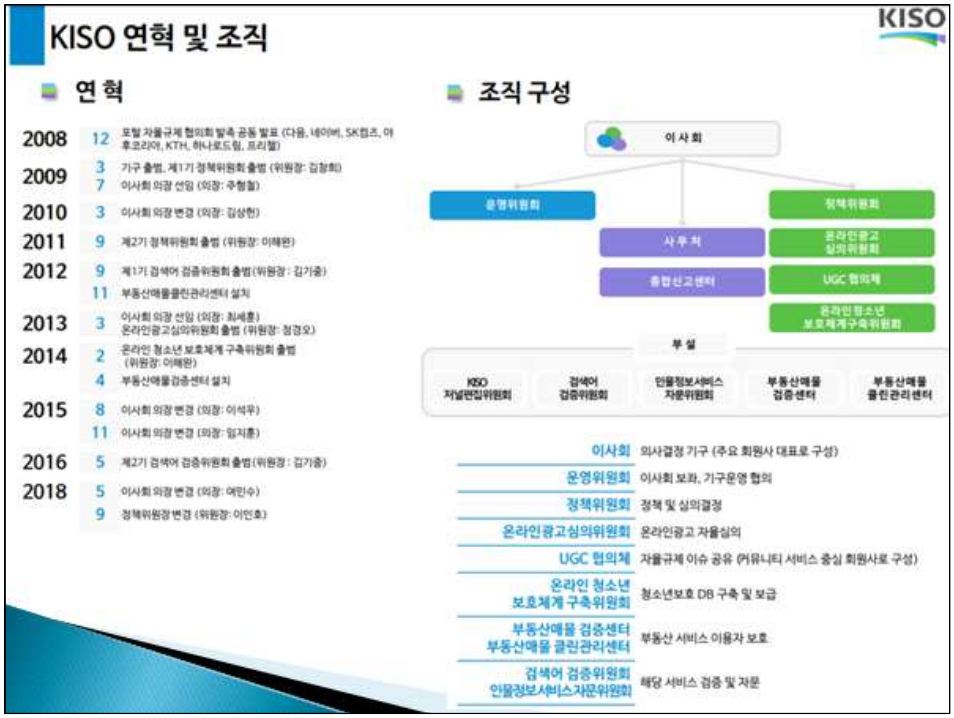
※ 기타불법 : 상표권 침해 26건 등

방송통신심의위원회는 관련 법률과 규정에 따라 불법정보 유통방지 등을 위한 법정직무를 성실하게 수행하고 있으며, 디지털 성범죄 피해의 확산, 웹툰 작가의 창작의욕을 상실케 하는 저작권 침해사이트의 급증, 서민경제 파탄을 야기하는 사이버 도박 중독 증가 등과 같은 사회적 병폐를 최소화 하고 건전한 정보통신 문화 창달을 위해 적극적으로 노력할 계획임.

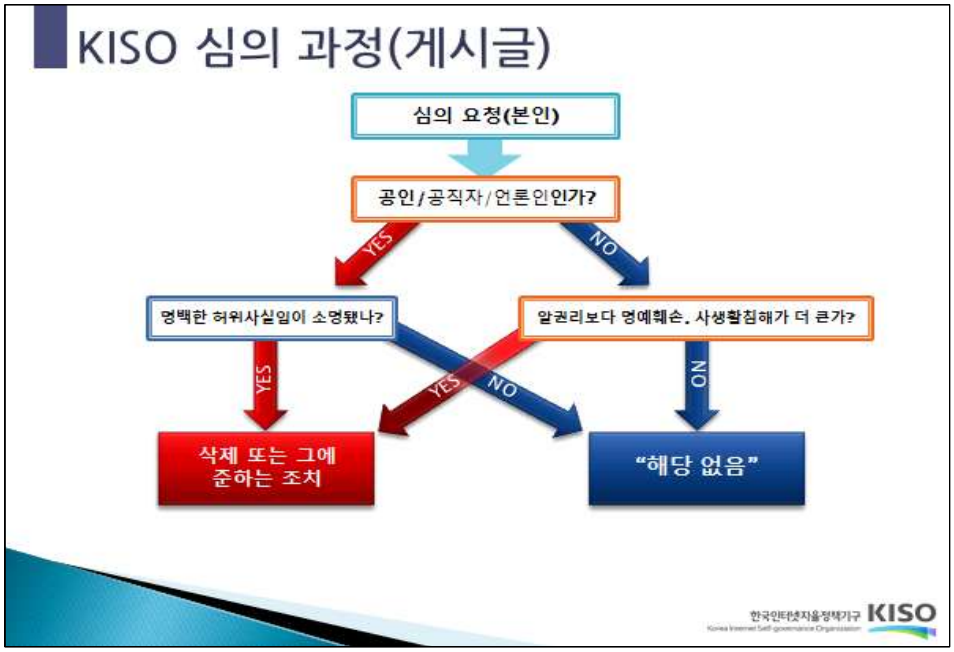
○ 민간자율심의체계 현황 및 개선 방안(발제자: 한국인터넷자율정책기구)

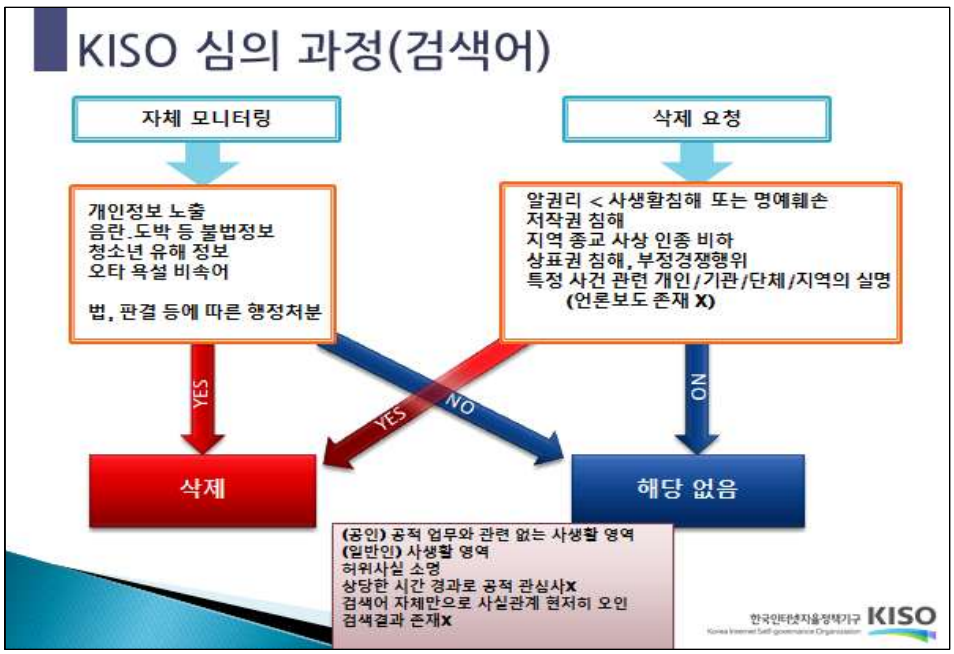





KISO 연혁 및 조직
KISO
연혁
2008 12 모빌 자율규제 협의회 발족 공동 발표 (다음, 네이버, SK컴즈, 야후코리아, KTH, 하나로드림, 프리챌)
2009 3 기구 출범, 제1기 정책위원회 출범 (위원장: 김창희)
7 이사회 의장 선임 (의장: 주형철)
2010 3 이사회 의장 변경 (의장: 김상헌)
2011 9 제2기 정책위원회 출범 (위원장: 이해완)
2012 9 제1기 검색어 검증위원회 출범 (위원장 : 김기중)
11 부동산매물클린관리센터 설치
2013 3 이사회 의장 선임 (의장: 최세훈)
온라인광고심의위원회 출범 (위원장: 정경오)
2014 2 온라인 청소년 보호체계 구축위원회 출범 (위원장: 이해완)
4 부동산매물검증센터 설치
2015 8 이사회 의장 변경 (의장: 이석우)
11 이사회 의장 변경 (의장: 임지훈)
2016 5 제2기 검색어 검증위원회 출범 (위원장 : 김기중)
2018 5 이사회 의장 변경 (의장: 여민수)
9 정책위원장 변경 (위원장: 이인호)
조직 구성
이사회
운영위원회
정책위원회
사무처
온라인광고 심의위원회
종합신고센터
UGC 협의체
온라인청소년 보호체계구축위원회
부설
KISO 자널편집위원회
검색어 검증위원회
인물정보서비스 자문위원회
부동산매물 검증센터
부동산매물 클린관리센터
이사회 의사결정 기구 (주요 회원사 대표로 구성)
운영위원회 이사회 보좌, 기구운영 협의
정책위원회 정책 및 심의결정
온라인광고심의위원회 온라인광고 자율심의
UGC 협의체 자율규제 이슈 공유 (커뮤니티 서비스 중심 회원사로 구성)
온라인 청소년 보호체계 구축위원회 청소년보호 DB 구축 및 보급
부동산매물 검증센터 부동산매물 클린관리센터 부동산 서비스 이용자 보호
검색어 검증위원회 인물정보서비스자문위원회 해당 서비스 검증 및 자문


KISO의 주요 기능 및 현황
KISO
주요 기능
- 정책결정/심의결정을 통한 회원사 게시물 자율규제 지원
정관 제4조(주요기능)
1. 기구 강령 및 가이드라인 수립
2. 회원사 등으로부터 요청 받은 인터넷 게시물 처리 정책에 관한 사항
3. 국제 자율규제기구와의 교류 협력 및 국제기구 활동 참여
4. 인터넷 자율규제 활동과 관련한 서적 또는 정기간행물의 인쇄 및 출판
5. 기타 기구 목적에 부합되는 사업
6. 기타 기구 목적에 부합되는 수익사업
회원사 현황 및 운영 재원
- 회원사 : 국내 주요 포털, UGC 회원 등 총 12개사
- 운영 재원 : 회비, 분담금, 후원금, 수익사업 등
NAVER kakao SK communications PPOMPPU
SLR CLIEN.net PARKOZ
zum internet afreecaTV kth INVEN
회원사 현황
회사명 서비스명(URL) 주요 사업
카카오 다음 (www.daum.net) 종합포털 모바일 서비스
네이버 네이버 (www.naver.com) 종합포털
SK커뮤니케이션즈 네이트 (www.nate.com) 종합포털
뽐뿌커뮤니케이션 뽐뿌 (www.ppomppu.co.kr) 쇼핑 정보공유 커뮤니티
씨나인 오늘의 유머 (www.todayhumor.co.kr) 유머공유 커뮤니티
㈜인비전커뮤니티 SLR CLUB (www.slrclub.com) 카메라관련 정보공유 커뮤니티
씨엘커뮤니케이션즈 클리앙 (www.clien.net) IT및일반 정보공유 커뮤니티
파코즈 하드웨어 파코즈 하드웨어 (www.parkoz.com) 컴퓨터하드웨어 정보공유 커뮤니티
중인터넷 주식회사 zum.com (www.zum.com) 개방형 포털
㈜아프리카TV 아프리카TV (www.afreeca.com) 개인 인터넷 방송 플랫폼 서비스
KTH KTH (www.kth.com) 디지털 콘텐츠 사업
㈜ 인벤 INVEN (www.inven.co.kr) 게임 미디어


KISO 심의 과정(게시글)
심의 요청(본인)
공인/공직자/언론인인가?
YES
NO
명백한 허위사실임이 소명됐나?
알권리보다 명예훼손, 사생활침해가 더 큰가?
YES
NO
YES
NO
삭제 또는 그에 준하는 조치
"해당 없음"
한국인터넷자율정책기구 KISO

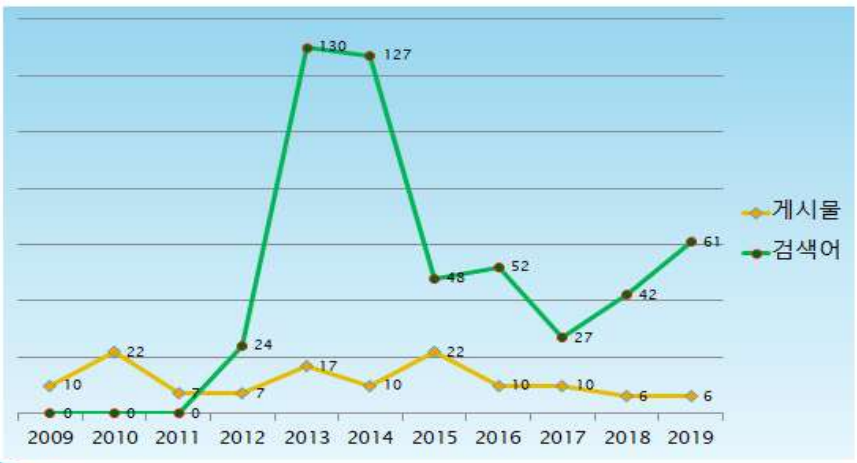

KISO 심의 과정(검색어)
자체 모니터링
삭제 요청
개인정보 노출
음란_도박 등 불법정보
청소년 유해 정보
오타 욕설 비속어
법, 판결 등에 따른 행정처분
알권리 < 사생활침해 또는 명예훼손
저작권 침해
지역 종교 사상 인종 비하
상표권 침해, 부정경쟁행위
특정 사건 관련 개인/기관/단체/지역의 실명
(언론보도 존재 X)
YES
NO
YES
NO
삭제
해당 없음
(공인) 공적 업무와 관련 없는 사생활 영역
(일반인) 사생활 영역
허위사실 소명
상당한 시간 경과로 공적 관심사X
검색어 자체만으로 사실관계 현저히 오인
검색결과 존재X
한국인터넷자율정책기구 KISO

KISO 정책위원회 심의 실적

심의 안건			심의결과		
연도	게시물	검색어	해당없음	삭제 또는 그에 준하는 조치	기타
2009	10	-	**3**	1	6
2010	22	-	**14**	3	5
2011	7	-	**4**	1	2
2012	7	24	**16**	12	3
2013	17	**130**	**108**	34	5
2014	10	**127**	41	**95**	1
2015	22	48	**62**	6	2
2016	10	52	**36**	26	-
2017	10	27	**26**	11	-
2018	6	42	**32**	16	-
2019	6	61	27	**37**	3
누계	127	511	**369**	**242**	**27**

한국인터넷자율정책기구 KISO

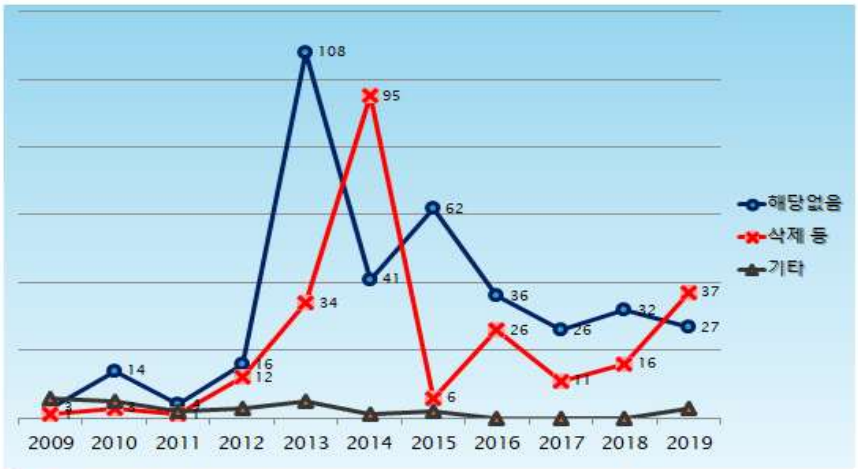
유형별 심의 현황



7

한국인터넷자율정책기구 KISO

유형별 심의 결과



7

한국인터넷자율정책기구 KISO

문제점

- **임시조치 제도 악용**
  - 중고거래 카페에 올린 사기판매자 정보 및 사기수법 공개 게시글도 임시조치
  - 업체의 불법 행위를 고발하는 게시글도 임시조치 되는 경우 많아
  - 대표적인 악용 사례는 제주국제영어마을 사건
- **명백한 허위사실? 팩트 체크는 어떻게?**
  - 허위사실, 또는 공적 관심사의 기준 가운데 하나가 언론 보도
  - 문제는 언론 보도가 사실인지 오보인지 검증 불가
  - 법원 판결로는 신속한 판단 및 조치 불가
- **회원사(국내 사업자) 역차별 문제?**
  - 일간베스트, 디씨인사이드, 워마드 등 비회원사 규제방안은?
  - 구글(유튜브) 페이스북, 트위치, 텀블러 등 해외사업자 규제방안은?

한국인터넷자율정책기구 KISO

저 자 소 개

이 찬 구

· 한국외국어대 신문방송학과 졸업
· 한국외국어대학교 신문방송학과 석사
· 한양대학교 경영학과 박사
· 현 미디어미래연구소 미디어경영센터 부센터장

천 혜 선

· 이화여대 신문방송학과 졸업
· 이화여대 신문방송학과 석사
· 뉴욕주립대 커뮤니케이션학과 박사
· 현 미디어미래연구소 미디어경영센터 센터장

신 혜 인

· 한국외대 언론정보학과 졸업
· 현 미디어미래연구소 연구원

지 혜 인

· 한국외대 언론정보학과 졸업
· 한국외대 신문방송학과 석사
· 현 미디어미래연구소 연구원

김 유 석

· 한림대 언론정보학부 졸업
· 고려대 언론학과 석사
· 고려대 언론학과 박사수료
· 현 미디어미래연구소 콘텐츠정책실 실장

방송융합정책연구 KCC-2019-31

국민정서에 부합하는 인터넷 규제 개선방안 연구

2019년 12월 31일 인쇄
2019년 12월 31일 발행

발행인 방송통신위원회 위원장
발행처 방송통신위원회
경기도 과천시 관문로 47
정부과천청사
TEL: 02-2110-1323
Homepage: www.kcc.go.kr