

강화된 불법 음란물 차단 정책: 인터넷 사전 검열인가, 디지털 성범죄 방지책인가

김승주 고려대학교 정보보호대학원 교수 *

1. 서론

지난 2월 11일 방송통신위원회는 KT나 LGU+ 등과 같은 국내 인터넷서비스 제공 사업자(ISP: Internet Service Provider)를 통해 SNI(Server Name Indication)를 이용한 웹 사이트 차단 시스템을 가동했다. 차단 시스템은 방송통신심의위원회에서 차단을 결정한 도박, 포르노 등 '불법' 해외 사이트 895곳을 우선 대상으로 했다. 불법 사이트를 HTTPS로 우회 접근하는 것을 방지하기 위한 정부의 이번 정책은 거센 후폭풍을 불러왔으며, 급기야 국민청원으로 이어져 참여인원이 2월 21일 기준 25만 명을 넘어서기에 이르렀다.

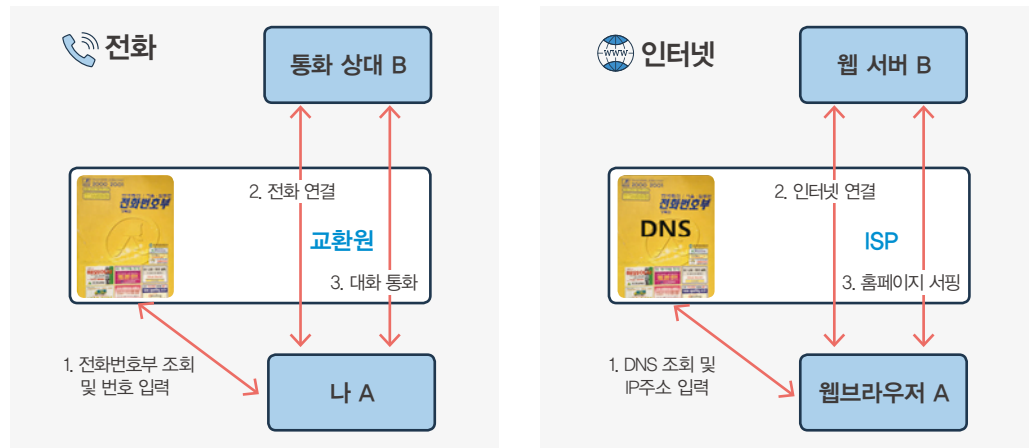
불법 사이트 차단이야 이미 과거에서부터 계속해 왔던 것인데 왜 새삼스레 이런 논란을 야기했을까? 이렇게 된 원인으로 필자는 △정부의 소통 부족, △언론의 전문성 결여, 그리고 △공론화를 통한 합의 과정의 부재를 꼽고 싶다.

* skim71@korea.ac.kr

2. 불법 사이트 차단 기술의 작동 원리

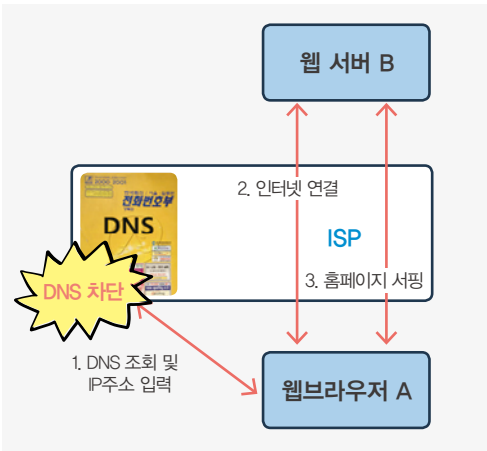
우리가 인터넷을 이용하는 과정은 전화를 하는 것과 매우 유사하다. 전화를 할 때 우리는 우선 전화번호부를 찾거나 114에 문의해 상대방의 전화번호를 알아낸 후, 해당 전화번호를 누르면 교환원이 상대방 번호로 연결해 주는 과정을 거치게 된다. 인터넷도 이와 유사해서 우리가 웹브라우저 창에 'www.korea.ac.kr'과 같은 도메인 네임(domain name)을 입력하면, 웹브라우저는 인터넷상에서 114와 같은 역할을 해주는 DNS(Domain Name Server)에 해당 도메인 네임의 주소(일명, IP 주소)를 문의하게 된다. DNS로부터 '163.152.100.100'와 같은 IP주소를 수신한 웹 브라우저는 다시 KT나 LGU+, SK브로드밴드 등과 같은 국내 인터넷서비스 제공 사업자에게 해당 주소로의 연결을 요청하게 되고, 그러면 요청을 받은 사업자는 고객이 원하는 IP주소를 가진 홈페이지로 연결해 준다.

<그림 1> 인터넷을 통해 홈페이지에 접속하는 과정



과거 우리 정부가 쓰던 방식은 'DNS 차단방식'으로, DNS에 주소를 문의할 때 해당 도메인 네임이 불법 사이트 목록에 등재된 것이라면 실제 IP주소가 아닌 엉뚱한 IP주소(예를 들면, warning.or.kr 사이트의 IP주소)를 알려주는 방식이다. 그러자 우리 네티즌들은 국내 인터넷서비스 제공 사업자들이 운영하는 조작된 DNS가 아닌 구글과 같은 해외 업체에서 제공하는 온전한 DNS를 이용해 정부의 차단을 우회하기 시작했다.

<그림 2> DNS 차단방식

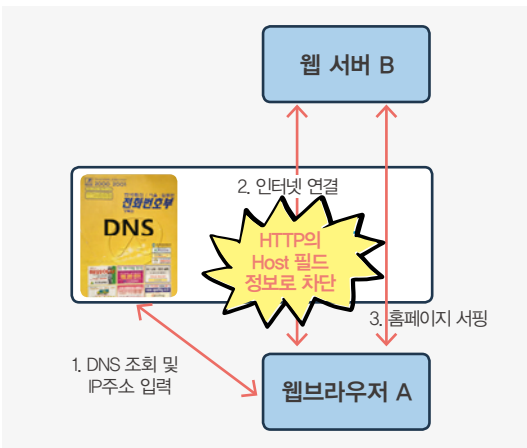


<그림 3> warning.or.kr 사이트



이래서 등장한 것이 'HTTP 차단방식'이다. 이는 DNS로부터 IP주소를 수신한 웹브라우저가 국내 인터넷서비스 제공 사업자에게 해당 주소로의 연결을 요청하는 순간, 이것이 불법 사이트 목록에 등재된 것일 경우 이를 차단하는 방식이다. 그러자 불법 사이트들은 HTTPS라는 암호화 접속을 이용해 차단을 무력화했다. HTTPS란 'HTTP Secure'의 줄임말로 이를 이용할 경우 사용자 웹브라우저와 홈페이지 사이의 모든 통신 내용이 암호화돼, 인터넷 서비스 제공 사업자는 사용자의 웹브라우저가 어느 주소로 연결되는지 알 수 없게 된다.¹⁾

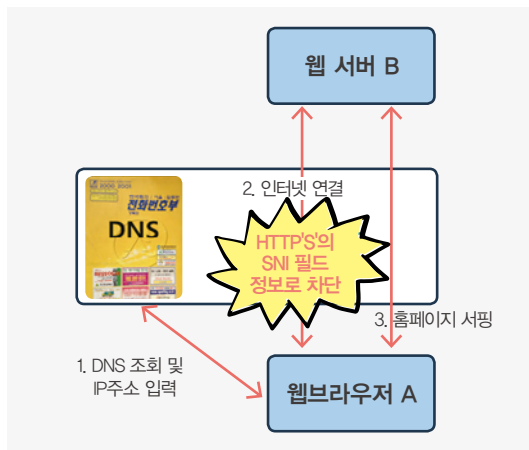
<그림 4> HTTP 차단방식



1) 웹브라우저 또는 운영체제의 작업표시줄 하단에 자물쇠 아이콘이 표시되면, 이는 현재 HTTPS 암호화 통신이 사용되고 있음을 나타낸다.

이러한 HTTPS를 이용한 우회방식을 막기 위해 등장한 것이 바로 이번에 논란이 된 ‘HTTPS 차단(또는 SNI 차단)방식이다. 사실 암호화 통신을 하겠다고 해서 곧바로 이를 개시할 수 있는 것은 아니다. 암호화 통신을 하려면 사전에 쌍방이 서로 어떤 암호방식을 쓸지 또 어떤 비밀번호를 이용할지 등을 결정해야 한다. 이를 환경설정이라고 하는데 HTTPS도 마찬가지다. HTTPS 암호화 통신을 하려면 사용자의 웹브라우저와 홈페이지는 앞에서 언급한 환경설정 과정을 거쳐야 하는데, 이때 SNI라는 영역에 접속하려는 홈페이지의 주소가 순간적으로 노출되는 약점이 있다. HTTPS 차단방식이란 바로 이 정보를 이용해 불법 사이트 접속을 차단시키는 것을 말한다.

<그림 5> HTTPS(또는 SNI) 차단방식



사실 과거의 DNS 차단 방식이건 지금 논란이 되고 있는 HTTPS 차단 방식이건 간에 인터넷 서비스 제공 사업자가 접속하려는 홈페이지의 주소를 보고 정부가 작성·배포한 목록과 비교해 차단한다는 점에서 기술적으로는 큰 차이가 없다. 혹자는 HTTPS 차단 방식을 중국 정부 등이 시행하고 있는 심층패킷분석(DPI: Deep Packet Inspection)에 비유하기도 하는데, 이는 인터넷회선을 통해 오가는 데이터의 내용 자체를 들여다보는 기술로 단순히 편지 봉투에 적힌 주소가 아닌 편지를 뜯어 그 내용물 자체를 읽고 검열한다는 점에서 HTTPS 차단 방식과는 상당한 차이가 있다.²⁾

2) 단층 패킷 분석 (Shallow Packet Inspection) : 1계층(물리계층)에서 4계층(전송계층, TCP/UDP)까지 분석하는 것으로서, 마치 편지 봉투에 적힌 주소를 보고 검열하는 것과 같음. DNS 차단방식, HTTP 차단방식, HTTPS(또는 SNI) 차단방식 등이 이에 해당함.
 심층 패킷 분석 (Deep Packet Inspection) : 5계층(세션 계층)에서 7계층(응용계층)까지 분석하는 것을 말함. 따라서 DPI는 패킷의 내용까지 보게 되며, 마치 편지를 뜯어 그 내용물 자체를 읽고 검열하는 것과 같음.

3. 대규모 사회적 반발의 원인

이번 논란을 보면서 필자가 아쉬운 것은 국민의 눈높이에 맞는 정부의 소통이 너무나도 부족했다는 것이다. 아무리 과거에 해왔던 방식들과 유사하다 하더라도 이를 국민에게 이해시키고 공론화하는 과정을 거치지 못한 점, 결국에는 그로 인해 여러 기술적인 오해와 소모적인 논쟁까지도 과도하게 촉발시켰다는 점에서 우리 정부는 일차적인 비난을 면하기 어렵다.

또한 언론의 전문성 결여 및 공정한 공론화 장 마련의 실패 또한 되짚어볼 문제이다. 비록 정부의 설명이 부실했다고는 하나 언론은 여러 전문가들과의 인터뷰를 통해 정확한 해설 기사를 싣고 국민의 이해를 도울 의무가 있었다. 그러나 이번의 경우 초기 유튜브 등에서 떠도는 잘못된 기술 설명을 확인도 않고 그대로 전달해 대중의 오해를 증폭시킨 책임이 없지 않다.

더욱이 이번 HTTPS 차단 정책을 두고 인터넷의 개방성을 옹호하는 시민단체에서는 정부의 인터넷에 대한 간섭이 있어서는 안 될 일이라고 했지만, 반대로 여성인권단체에서는 리벤지 포르노(revenge porn) 등에 대한 정부의 더 적극적이고도 신속한 차단을 요구한 바 있다.³⁾ 언론은 이러한 양쪽의 의견을 동등하게 전달하고 이에 대한 공론화가 이루어지도록 할 의무가 있었으나, 이번 경우에는 그렇지 못했다. 실제로 불과 일 년여 전만 하더라도 각종 언론들은 텬블러 등 외국의 인터넷 사이트를 통한 음란물 유포가 늘고 성범죄 모의 사례까지 발견되고 있다며, 표현의 자유로 포장된 범죄를 방치하지 말고 정부가 보다 적극적으로 나서줄 것을 질타했었다. 이에 당시 청와대 국민청원 게시판에는 텬블러를 규제하자는 청원이 올라와 수만 명이 동참하기도 했다.⁴⁾

〈그림 6〉 청와대 국민청원 게시판에 올라온 텬블러 규제 관련 청원



- 3) 대법원의 '성폭력범죄의 처벌 등에 관한 특례법 위반(카메라 등 이용 촬영) 1심 판결 현황'에 따르면, 2012년부터 2017년까지 6년간 불법촬영 혐의로 재판을 받은 7446명 가운데 징역형을 받은 피고인은 647명(8.7%)에 불과함. 음란물 유포의 경우에는 더 처벌이 약한데, '정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반(음란물 유포) 1심 판결 현황'에 따르면 1680명 중 징역형은 30명(1.8%)에 불과했음.
- 4) 당시 '텀블러'로 검색한 규제 관련 국민청원만 한 페이지를 넘어갔으며, 청원인원만 무려 12만 명을 넘어서는 청원까지 있었다. 이에 방송통신심의위원회는 텬블러에 '불법 콘텐츠 대응에 대한 협력'을 요청했지만 텬블러 측은 '텀블러는 미국 법률에 의해 규제되는 미국 회사라며 '텀블러는 대한민국 법률의 적용을 받지 않는다'라며 이를 거부한 바 있다.

언론이 그때 그때의 상황에 따라 자신의 편집방향과 일치하는 인터뷰만을 신는 편향적 보도 행태는 국민들의 분별력을 떨어뜨려 현실에 대해 왜곡된 시각을 갖게 하고, 궁극적으로는 객관적인 공론화 과정을 방해한다는 점에서 절대로 있어서는 안 된다.

4. 결론 및 우리의 과제

인터넷은 사익과 공익이 공존하는 공간이며, 하나의 정답을 내리기가 매우 어렵다. 미국의 국제인권단체 프리덤하우스(Freedom House)가 최근 발표한 “인터넷 자유 지수(Freedom on the Net) 2018” 보고서를 보면 한국은 인터넷 콘텐츠 제한(Limits on Content) 항목에서 35점 만점(낮을수록 자유도 높음)에 13점을 받았다. 중국(31점)이나 러시아(24점), 싱가포르(14점)보다는 낮지만 일본(8점)이나 미국(8점), 프랑스(6점), 독일(5점), 영국(6점) 등의 국가들보다는 높은 수준이다.

보고서에 따르면 영국은 아동음란물, 테러선동 등 부정정보를 관련법에 따라 인터넷서비스 제공 사업자에서 차단하고 있으며, 프랑스는 아동포르노, 테러선동물 등에 대한 차단 권한이 경찰청에 있고 정부는 불법 게시물의 게시자에게 삭제 요청을 하고난 후 24시간 뒤에는 인터넷서비스 제공 사업자로 하여금 해당 사이트를 차단하도록 할 수 있다. 그러나 우리나라의 경우 형법상의 음란물 유포죄와 아동청소년의 성보호에 관한 법률에 따라 아동포르노뿐만이 아닌 포르노 산업 자체가 불법이고, 인터넷이나 스마트폰의 속도와 보급률이 다른 국가에 비해 월등하다는 점에서 단순히 인터넷 콘텐츠의 차단 정도만을 가지고 비교하는 것은 무리가 있다.

정부의 ‘온라인 개입’에 대한 타당성 논란은 이미 전세계적인 이슈이다. 세계 최대 소셜미디어 페이스북의 창업자인 마크 저커버그(Mark Elliot Zuckerberg)는 지난 3월 30일(현지시간) 그동안의 입장을 바꿔 각국 정부가 인터넷 규제에서 “더욱 적극적인 역할”을 맡아야 한다고 주장했다. 저커버그는 이날 워싱턴포스트에 낸 “인터넷은 새로운 규칙을 필요로 한다(The Internet needs new rules. Let’s start in these four areas.)”는 제목의 칼럼에서 “나는 정부와 규제 당국의 더욱 적극적인 역할이 필요하다고 본다”고 밝히며, 새로운 인터넷 규제가 필요한 4대 분야로 ▲유해 콘텐츠(harmful content) ▲선거 보호(protecting elections) ▲프라이버시(privacy and data protection) ▲데이터 이동성(data portability) 등을 꼽았다. 현재 인터넷 상에는 저커버그의 주장에 대한 갑론을박이 이어지고 있다.

우리 또한 이번 일을 계기로 우리에게 맞는 올바른 인터넷 정책은 무엇인지 정부와 국민 모두가 함께 고민해 나가야 하겠다. 🇰🇷