『전기통신사업법』 일부개정안 입법예고에 대한 의견서

2016. 7.

(사) 오픈넷

대표자: 남희섭

주소: (우)-6650 서울시 서초구 서초대로 50길 62-9, 402 (서초동, 한림빌딩)

전화번호: 02-581-1643 팩스: 02-581-1642

Ⅰ. 부가통신사업자 불법정보 유통방지 의무 신설에 대한 반대의견

1. 개정이유 및 내용

○ 모든 부가통신사업자들이 자신이 관리하는 정보통신망에 음란물이 유통되는 사정을 명백히 인식한 경우에는 지체없이 해당 정보를 삭제 또는 그 유통을 차단할 의무를 부과하고 미이행시 시정명령 및 과태료를 부과할 수 있도록 함(안 제22조의5, 제92조제1항제1호, 제104조제3항제1호의2 신설)

○ 본 규정 신설 이유에 대하여 방송통신위원회는 보도자료를 통해 '최근 인터넷 방송, 채팅앱 등에서 불법정보가 유통되는 것을 방지하기 위해 이를 방치하고 있는 부가통신사업자에게 해당 불법정보에 대한 유통 방지 의무를 부과하여 사업자의 관리책임을 제고'하기 위함이라 밝힌바 있음

2. 반대의견

가. 서

○ 위 개정안은 다음과 같은 이유에서 부가통신사업자들에게 부당하게 과도한 유통 방지 의무 및 관리책임을 부과하여 국내 인터넷 산업의 발전을 저해하고 결과적으로 인터넷 이용자들의 권익을 침해하는 결과를 가져오는 것으로서 재고되어야 함

나. 정보매개자에 대한 일반적 감시의무 부과

○ 안 제22조의5에서 '명백히 인식한 경우'의 의미가 불명확하여 사업자들이 의무 위반을 피하기 위해서는 모든 게시물을 일일이 모니터링할 수 밖에 없게 될 것임. 이로 인하여 본조는 정보매개자들이 이용자들이 유통하는 정보의 불법성을 사적으로 검열하도록 하는 '일반적 감시의무' 부과 조항으로 기능하게 될 가능성이 높음

○ 정보의 생산자가 아닌 정보유통을 매개하는 자, 즉 정보매개자(intermediary)에 대한 일반적 감시의무 부과는 사업자에게 과도한 부담을 지우고 이로써 자유로운 인터넷 이용 환경과 문화를 저해하여 이용자들의 표현의 자유를 위축시킨다는 비판으로 인하여 국제적으로 금지되고 있음. 한-EU FTA의 기반이 된 유럽연합의 전자상거래지침(Directive 2000/31/EC)은 모든 불법정보(저작권 침해 정보, 음란 정보, 아동 포르노물)에 대한 일반적 감시의무를 금지하고 있음. 또한 '정보매개자책임에 관한 마닐라 원칙'도 정보매개자에게 적극적 모니터링 의무를 부과해서는 안 된다는 점을 명시하고 있음

○ 또한 일반적 감시의무를 부과하는 기존의 규제들은 '기술적 조치'만을 요구하여 '기술적 조치'가 존재하지 않을 경우에는 법조항이 적용되지 않는다는 해석이 가능하지만 동 조항상 의무는 "명백히 인식한 경우"라는 주관적이고 추상적인 기준을 사용하고 있어 훨씬 광범위하고 침익적임

<기존 규제와의 비교>

	적용게시물	적용대상	벌칙	해석
아청법 제17조 '기술적 조치'	아동·청소년 이용음란물	모든 OSP	3년 이하의 징역 또는 2천만원 이하의 벌금	전송을 방지·중단하는 기술적 조치가 가능할 때 의무 발생 ('기술적으로 현저히 곤란한 경우' 면책)
저작권법 제104조 '기술적 조치'	저작물	특수 유형 OSP	3천만원 이하의 과태료	전송을 차단하는 기술적 조치가 가능할 때 의무 발생
전기통신사업법 제22조의3 '기술적 조치'	음란물	특수 유형 부가통신사업자	2천만원 이하의 과태료	유통 방지를 위한 기술적 조치가 가능할 때 의무 발생
전기통신사업법 방통위안 제22조의5 '유통방지'	음란물	모든 부가통신사업자	2천만원 이하의 과태료	'유통되는 사정을 명백히 인식'했다고 여겨지면 의무 발생

다. 인터넷 이용자들의 표현의 자유, 알 권리, 통신비밀의 침해

○ ‘음란물’ 개념의 불명확성으로 인하여, 사업자들은 청소년에게만 금지되어도 족한 ‘선정성 정보’ 혹은 ‘성인 정보’마저 모두 일률적으로 삭제, 차단하는 과잉 검열의 결과가 필연적으로 나타나게 됨. 이로써 정당한 성인의 알 권리 및 표현의 자유가 침해될 가능성이 높음

○ 또한 채팅앱 서비스의 경우 불법정보가 유통되는지를 확인하기 위해서는 사업자가 이용자들의 사적 통신내용을 들여다 보아야 하므로 이용자의 통신비밀의 자유 침해 문제도 발생함

라. 부가통신사업자 및 국내 사업자의 평등권 침해

○ ISP, 이동통신사업자 등 망사업자들에게는 적용하지 않으면서 대부분의 인터넷기업, 온라인서비스제공자가 해당되는 부가통신사업자에게만 유통방지 의무를 부과하고 위반시 시정명령 및 과태료 부과 등의 행정적 제재를 가하는 것은 근거없는 차별로써 평등권 위반의 소지가 있고, 국내에서 부가통신사업을 신고한 자들에게만 적용되기 때문에 국내 사업자들을 역차별하는 결과를 낳을 수 있음. 이로써 이용자들도 사업자가 게시물을 상시적으로 모니터링하여 사적 검열과 감시의 위험이 있는 국내 서비스보다 자유롭고 통신비밀이 보장되는 해외 서비스를 선호하여 국내 인터넷 산업의 쇠퇴를 가져올 위험이 있음

○ 특히 본조의 규제 대상인 불특정 다수의 이용자들이 자유로이 ‘실시간’으로 정보를 유통시키는 형식의 인터넷 플랫폼 서비스(인터넷 개인방송, 채팅앱, SNS 등)의 경우 실시간 모니터링 역량에 따라 책임의 범위가 달라지는 불합리한 결과가 나타날 수 있음. 이에 따라 사업자는 오히려 적극적인 모니터링을 회피하는 역효과가 나타날 수도 있음

3. 결론

○ 음란 방송 등 불법적인 행위를 한 이용자들을 형법을 비롯한 현행법으로 처벌하여 사전적 예방을 할 수 있고, 또한 현행 방송통신심의위원회의 시정요구 제도 및 방송통신위원회의 제재명령 제도, 청소년 유해정보 표시 및 성인인증을 통한 청소년접근제한 조치를 통해 입법목적은 이미 충분히 달성되고 있음

○ 또한 현행법과 판례에 따르더라도 정보매개자 역시 일정 요건 하에서 음란물 및 기타 불법정보 유통에 따른 책임을 부담하고 있음. 이와 같은 상황에서 본조를 신설하는 것은 결국 불필요하게 정보매개자에 대하여 국제적 흐름에 반하는 일반적 감시의무를 부과하고 과도한 관리책임을 지움으로서 국내 인터넷 산업의 발전을 저해하며 결과적으로 이용자들의 권익을 침해하는 결과를 가져오기 때문에 이상과 같이 반대함

Ⅱ. 불법유해정보 차단수단 제공의 예외에 대한 검토의견

1. 개정이유 및 내용

○ 청소년의 사생활의 비밀과 자유 및 부모의 교육권 침해를 최소화하기 위하여 법정대리인이 신청하는 경우에는 불법유해정보 차단수단을 설치하지 않을 수 있도록 선택권을 부여하는 예외 규정을 신설(안 제32조의7제1항 단서 신설)

2. 검토의견

가. 서

○ 부모의 교육권 침해를 최소화하기 위해 선택권을 부여하는 예외 규정의 신설은 바람직함

○ 그러나 시행령에서 이통사의 차단수단 '설치여부 확인' 및 법정대리인에 대한 '통지' 의무를 규정하고 있어 청소년의 사생활의 비밀과 자유 및 개인정보자기결정권 침해 문제가 존재함. 또한 가장 널리 사용되는 차단수단인 "스마트보안관" 앱이 심각한 보안문제가 있는 것으로 밝혀진 바 있어 현존하는 차단수단의 안전성에 대한 전반적인 검증이 필요함

나. 청소년의 사생활의 비밀과 자유 침해

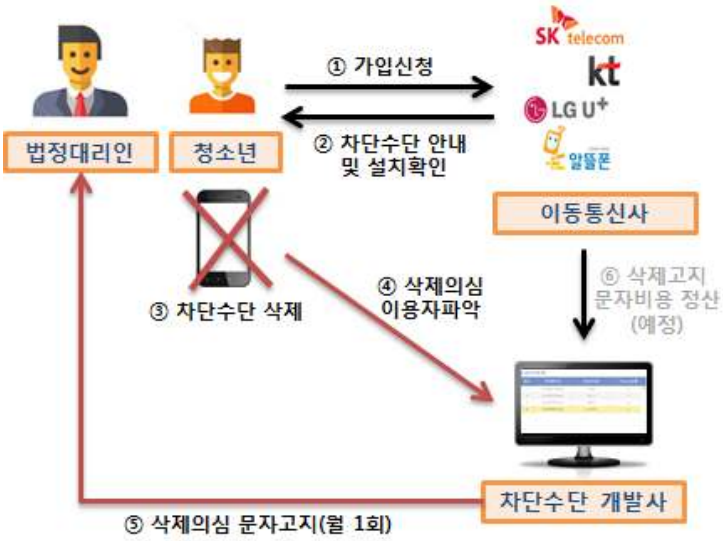
○ 시행령에 의하면 이통사는 차단 앱이 삭제되거나 15일 이상 작동하지 않는 경우 법정대리인(주로 부모)에게 그 사실을 통지하도록 되어 있음. 결국 이통사는 차단 앱 작동 여부를 확인하기 위해 청소년의 스마트폰을 상시 감시해야 하며, 이 과정에서 청소년의 사생활의 비밀과 자유가 침해됨

○ 또한 대부분의 차단수단은 자녀용과 부모용으로 나뉘어 있으며 부모용을 통해 청소년의 스마트폰 사용 내역 등을 감시할 수 있게 하고 있음.

이러한 정보는 부모뿐만 아니라 사업자도 접근할 가능성이 있어 스마트폰 사용과 관련한 청소년의 프라이버시를 심각하게 침해함

다. 개인정보자기결정권 침해

○ 법 시행령 규제영향분석서의 차단수단 제공 흐름도는 아래와 같이 되어 있음



○ 위 흐름도에 따르면 차단수단 개발사가 차단수단 삭제 여부를 파악해서 문자 등으로 고지를 하게 되어 있음. 이 과정에서 개발사는 청소년과 법정대리인의 개인정보를 수집·보관해야 하며 결과적으로 개인정보가 과도하게 집적 및 유통될 위험이 있음

라. 안전한 차단수단의 부재

○ 현재 시장에서 제공되고 있는 차단수단, 즉 스마트폰 애플리케이션 중 보안감사를 거쳐 안전함이 확인된 차단 앱이 전무한 상태이며, 특히 방통위가 개발 및 홍보예산을 지원하고 한국무선인터넷산업연합회(MOIBA)에서 개발해 2012년부터 보급해오고 있었던 “스마트보안관”은 보안이 매우 취약한 것으로 밝혀짐

○ 2015년 캐나다 토론토대학교 산하 시티즌랩 연구소는 스마트보안관에 대한 보안 감사 보고서를 2차에 걸쳐 발표함

- 2015년 9월 20일 발표된 1차 보고서에 의하면 스마트보안관에 대한 보안 감사를 통해 26건의 보안 취약점들이 발견됨(첨부 1. 참조). 이에 시티즌랩은 즉시 스마트보안관서비스를 중단할 것을 권고함. 또한 이러한 보안 취약점들은 개인정보보호법 및 정보통신망법상 요구되는 개인정보보호조치 위반일 뿐만 아니라, 스마트보안관의 약관과 개인정보보호정책에서 주장하는 보안 수준에도 미치지 못해 계약상의 의무의 위반임이 밝혀짐

- 보고서 발표 직후 방통위는 보도자료를 통해 취약점을 수정하기 위한 조치가 취해졌으며 “앞으로도 필요시 보안취약점을 지속적으로 개선”해 나가겠다고 대응한 바 있음

- 그러나 11월 1일 공개된 2차 보고서에 의하면 스마트보안관의 취약점은 제대로 수정되지 않았거나 그대로 남아 있어 청소년들을 여전히 위험에 노출시키고 있는 것으로 드러남(첨부 2. 참조)

마. 일본 법제와의 비교

○ 본 예외규정은 일본의 「청소년이 안전하게 안심하고 인터넷을 이용할 수 있는 환경의 정비 등에 관한 법률」 제17조 제1항 단서 조항과 유사함

○ 일본은 우리와 같은 강력한 청소년보호를 위한 규제가 존재하지 않기 때문에 특별법이 필요한 면이 있으나, 우리나라는 이미 세계에서 제일 강한 수준의 청소년보호 규제가 존재

○ 또한 일본법은 청소년의 주체성을 인정하고 인터넷 리터러시의 습득과 청소년 보호간의 균형 및 민간에 의한 자율적 대응을 기본이념으로 하나, 우리 법은 이러한 고려가 없이 사업자를 통해 일방적으로 국가후견적인 제도를 강제

○ 결론적으로 정책의 정신 내지 이념은 전혀 반영하지 않고 수단만 도입하여 우리나라 기존 청소년보호정책 전반의 문제점을 그대로 답습하고 있음

3. 결론

○ 청소년들을 온라인에서 범람하는 유해매체물로부터 보호해야 한다는 점에 대해서는 논란의 여지가 없으나, 국가가 사회의 취약한 집단에게 특정의 보호조치를 강제하고자 할 때에는 그러한 보호조치가 진정으로 필요한 것인지 내지 안전한지에 대한 철저한 검증이 선행되어야 함

○ 궁극적으로는 '스마트보안관' 사례와 같이 개인의 통신기기를 타인이 감시할 수 있는 소프트웨어를 설치하도록 국가가 법으로 강제하게 되면 프라이버시 침해와 함께 심각한 보안상의 위험을 발생시키므로, 신중한 논의를 거쳐 도출된 사회적 합의가 있을 경우에만 도입해야 함

○ 동 제도의 유지 여부에 대해 전반적인 재검토가 필요하며, 검토 과정에서는 반드시 당사자인 청소년을 포함한 모든 이해관계자 및 전문가의 의견수렴이 있어야 할 것임