[제3회 망 중립성 이용자 포럼]

“트래픽 관리, 프라이버시 침해인가?”

■ 일시 : 2012년 9월 6일(목) 15:30~18:00

■ 장소 : 국회 의원회관(신관) 제1세미나실

■ 주최 : 최채천 의원실, 망중립성 이용자포럼

[제3회 망 중립성 이용자 포럼]

“트래픽 관리, 프라이버시 침해인가?”

통신사의 자의적인 트래픽 관리가 망중립성을 위반한다는 논란과 함께, 이용자 프라이버시 침해 우려도 제기되고 있습니다. 특히, 트래픽 관리에 사용되는 심층패킷감시(DPI) 기술은 패킷의 내용 분석을 기반으로 트래픽 관리, 패킷 기반 타겟 광고 등에 이용될 수 있어 자칫 상업적인 '감청'으로 이어질 수 있다는 우려도 있습니다. 트래픽 관리와 망중립성 논란과 연관하여 심층패킷감시(DPI)란 무엇인지, 트래픽 관리는 어떤 방식으로 이루어지는지, 트래픽 관리 과정에서 프라이버시 침해 우려는 없는지, 프라이버시 보호를 위한 조건은 무엇인지 등에 대한 사회적 논의도 심층적으로 이루어질 필요가 있습니다. 또한, 통신비밀보호법, 정보통신망법, 전기통신사업법 등 관련 법에서 트래픽 관리로 인한 프라이버시 침해 문제를 적절하게 규제할 수 있는지, 규제의 공백이 있다면 어떠한 보완이 필요한지에 대해서도 검토가 필요합니다.

이에 <망 중립성 이용자 포럼>은 제3회 포럼을 통해 트래픽 관리와 프라이버시 침해의 문제를 심도깊게 논의해보고자 합니다.

■ 포럼 개요

○ 일시 : 2012년 9월 6일(목) 15:30~18:00
○ 장소 : 국회 의원회관(신관) 제1세미나실
○ 주최 : 최채천 의원실, 망중립성 이용자포럼

■ 포럼 진행 순서

○ 사회 : 강정수 (연세대학교 커뮤니케이션연구소 전문연구원)

○ 발제 :
- DPI를 포함한 트래픽 관리의 기술적 이해 / 강장묵 교수 (동국대 전자상거래연구소)
- DPI의 남용과 프라이버시 / 오길영 교수 (신경대학교 경찰행정학과)

○ 토론
이창범 (한국인터넷법학회 부회장)
장여경 (진보네트워크센터)
써머즈 (인터넷주인찾기)

토론 쟁점

○ 쟁점 1 : 트래픽 관리와 프라이버시 침해 가능성

- 통신사의 트래픽 관리는 항상 프라이버시를 침해하는가, 혹은 어떠한 경우에, 어떠한 조건에서 프라이버시를 침해할 수 있는가
- DPI가 아닌 방식의 트래픽 관리는 프라이버시 침해 위험이 없는가
- 이용자의 동의가 있으면 프라이버시 침해가 아닌가. 이용자의 동의는 어떠한 조건을 갖추어야 하는가.
- 현재 이루어지고 있는 망사업자의 트래픽 관리는 이용자의 프라이버시를 침해하고 있는가

○ 쟁점 2 : 방통위의 트래픽 관리 가이드라인

- 방통위의 트래픽 관리 가이드라인은 프라이버시 침해를 방지할 수 있는가
- 프라이버시 측면에서 가이드라인은 어떠한 보완이 필요한가

○ 쟁점 3 : 트래픽 관리와 법적 규제

- 트래픽 관리는 현행 법률(전기통신사업법, 정보통신망법, 통신비밀보호법 등)에 의해 어떠한 규제를 받고 있는가
- 현재 이루어지고 있는 트래픽 관리를 현행 법률 위반 소지가 있는가? 혹은 트래픽 관리가 어떤 방식으로 이루어질 경우 현행 법률을 위반하게 되는가
- 이용자 프라이버시 침해를 방지하기 위해 현행 법률 조항의 한계는 무엇이고, 어떠한 개선이 필요한가

DPI의 남용과 프라이버시*

— 망중립성에 있어서의 논의를 중심으로 —

오길영
신경대학교 경찰행정학과 교수
eclaw@daum.net

I. 시작하며

DPI(Deep Packet Inspection, 이하 DPI)가 또다시 도마에 올랐다. 이번에는 망중립성(Network Neutrality, 이하 망중립성) 논의에서의 DPI가 그것이다. 사실 그간 몇 편의 글과 각종의 토론회를 통해 DPI의 문제점과 위험성을 밝히기 위해 제법 오랜 기간 노력해 왔음에도 불구하고, 애써 외면해온 부분이 바로 망중립성 논의에서의 DPI 문제이다. 물론 DPI 문제의 본격적인 발단이 바로 망중립성 논의에서부터였음을 잘 알고, 동시에 네트워크의 미래를 위해서는 반드시 짚고 넘어가야 할 부분임 또한 숙지하고 있었던 터이다. 그러나 고백하건대, 굳이 손을 대고 싶지는 않았다.^^ 이는 단순히 지쳤거나 열정이 부족해서가 아니다. 일의 규모가 단숨에 해치울 수 있는 규모가 아니라 엄두가 나지 않기도 했으나, 무엇보다 이 논의는 법학에서의 논의만으로는 도무지 해결책이 나오지 않는 난삽한 쟁점들이 산재하여 있기 때문이다. 즉 쟁점을 둘러싸고 있는 다면적 요소에 관하여, 다층적인 시각에서의 다학제간 접근(interdisciplinary approach)을 통한 분석이 필요한 것이다.
따라서 글의 시작에 앞서 밝히건대, 이 문제에 있어 규범적 검토가 가지는 의미는 어디까지나 일부분에 지나지 않음을 명심해야 한다. 또한 '미룬다고 해결되는 것이 없다' 고 말씀하시던 어머니께 뒤늦은 존경을 표하면서, 짧은 글을 시작하고자 한다.

Ⅱ. DPI의 개관

주지하는 바와 같이, DPI는 망중립성 논의의 발아이자 미결의 쟁점이기도 하다.[2] 여기서는 법적 논의의 전개를 위해 필요한 한도 내에서 간략히 DPI에 관하여 살피기로 한다.

---

* 이 글은 토론을 위한 바탕글이므로 완성된 원고가 아님을 미리 밝혀두는 바이다.

2) 망중립성의 개념과 함의, 그리고 DPI의 기술적 개념과 망중립성 논의와의 관련성 등의 기본적인 사항에 대한 설명은 본고에서 생략하기로 한다. 다른 영역에서의 전공자와 전문가가 다수 존재하는 상황에서, 전문지식이 일천한 필자가 지면을 빌어 이를 설명하는 것이 그리 바람직하지 않기 때문이다.

1. DPI의 활용

OSI 7계층 가운데 하위 4계층까지의 분석을 SPI(Shallow Packet Inspection, 이하 SPI), 상위 3계층에 대한 분석을 DPI로 파악하고 있음은 망중립성 이슈를 주목하고 있는 이들에게는 일종의 상식이다. 즉 DPI는 운송을 위한 정보가 기록되어 있는 '헤더(Header)' 부분이 아니라 '페이로드(Payload)', 즉 패킷(Packet)의 컨텐츠(Contents) 부분을 검사하는 것을 말한다. 이를 통해 DPI는 패턴검사(Pattern matching), 행태분석(Behavioral analysis), 통계분석(Statistical analysis) 등의 기능을 수행한다고 한다.[3] 이러한 기능을 통해 ① 네트워크 보안(Network security), ② 대역관리(Bandwidth management), ③ 소비자 분석(Customer profiling), ④ 수사용 감청(Governmental surveillance), ⑤ 컨텐츠 규제(Content regulation), ⑥ 저작권 제재(Copyright enforcement) 등 많은 영역에서 활용되고 있다.[4] 또한 하나의 기능에 특성화되어 있던 초창기와는 달리, 요즘은 하나의 장비에 다수의 기능을 복합적으로 담아내는 장비가 주류를 이루고 있기도 한 상황이다. 복합기가 경제적이라는 측면도 이유가 되겠으나, 무엇보다 급속도로 발전한 하드웨어의 역량 덕분이 아닌가하고 추측해 본다.

2. 검토대상의 확정

이렇듯 주요한 6가지의 기능 가운데, 망중립성과 관련하여 언급되는 것은 대체로 ①과 ②의 경우이다. 주로 '인터넷 맞춤광고'의 문제로 부각되어온 ③의 경우[5]와 소위 '패킷감청'의 문제로 큰 이슈가 되어 온 바 있는 ④의 경우,[6] 그리고 흔히 음란사이트 접속시에 마주치게 되는 ⑤의 경우와 유튜브(YouTube)에서 종종 목격하게 되는 ⑥의 경우[7] 등은 망중립성에 대한 본격적인 논의와는 조금 거리가 있는 것이 사실이다.[8]
이런 이유로 다시금 ①과 ②를 주목하자면, 우리는 주목할 만한 사실 하나를 발견하게 된다. 독약이 곧 묘약이라고 했던가? 동일한 기술을 통하여 이렇듯 양립하는 취지로 활용되는 경우를 바로 파악할 수 있다. 네트워크에 대하여 지극히 공익적일 수밖에 없는 ①의 경우, 그리고 정반대로 극도한 상업주의가 빚어낸 흉물스런 사익인 ②의 양립이 바로 그것이다.
어찌되었건, 이 두 경우 모두 DPI의 놀라운 역작임은 부정할 수 없다. 즉 순수하게 '기술적 중립성' 만을 견지(堅持)하여 바라볼 때, DPI 자체는 매우 훌륭한 작품인 것이다.

---

3) Milton L. Mueller, "Convergence of control? Deep Packet inspection and future of the Internet", Communications & Convergence Review, 제2권 제2호, 2010, 94-95쪽.
4) Milton L. Mueller, 앞의 글, 95-96쪽.
5) 이에 관한 상세와 그 법적 검토는 오길영, "감청의 상업화와 그 위법성", 민주법학 제43호, 2010 참조.
6) 이에 관한 상세와 그 법적 검토는 오길영, "인터넷 감청과 DPI", 민주법학 제41호, 2009; "국가정보원의 패킷감청론에 대한 비판", 민주법학 제48호, 2012 참조.
7) ⑤와 ⑥의 경우에 대한 상세는 박희영, "DPI 기술의 운영과 ISP의 형사책임", Internet and Information Security 제2권 제1호, 2011, 109-111쪽 참조.
8) 물론 넓은 의미에서의 망중립성 논의는, 이들 모두를 포함하기도 한다. 그러나 본고에서는 '대역관리', 다시 말해 소위 '트래픽 관리(Traffic Management)'와 직접적으로 관련된 양자로 그 논의의 범위를 줄여 검토하기로 한다.

Ⅲ. DPI와 프라이버시

먼저 ①의 경우, 즉 '네트워크 보안'은 말 그대로 특정한 네트워크의 보안을 위한 방화벽 시스템(Firewall System) 등에서 DPI를 사용하는 경우를 말한다. 즉 기업이나 조직의 차원에서, 기업·조직의 내부를 구성하고 있는 컴퓨터의 정보 보안 위하여 외부에서 내부, 내부에서 외부의 네트워크에 침입하는 것을 차단하는 기술로 사용된다. 바이러스(Virus)나 웜(Worm)의 차단, 그리고 최근 부쩍 잦아진 DDoS(Distributed Denial-of-Service Attack, 분산 서비스 거부)를 해결하기 위한 기능으로, 본래 DPI가 개발된 목적이자 기원이기도 하다. 이는 오늘날 네트워크의 현상을 고려할 때에, 반드시 필요한 기능이라 할 수 있다.
한편 ②의 경우인 '대역관리'는, 트래픽의 흐름(Streams of Traffic)이나 애플리케이션(Application)의 종류 등을 식별하여 특정 패킷을 우선하여 그 질을 보장하거나 혹은 차별하여 감속이나 차단·삭제시키는 등의 일련의 네트워크 관리행위를 말한다. 이는 네트워크의 안녕과 종속을 위해 거시적인 시각에서는 정당성을 가짐이 분명하나, 구체적으로는 이러한 네트워크 관리행위가 망사업자의 선택에 의해 작위적으로 진행된다는 점에서 적지 않은 문제의 소지를 가지고 있다. 특히 다분히 공공재로서의 성격[9]을 가지고 있는 네트워크를 실제 운영하는 망사업자가 이익추구에 매진하는 기업이자 상인이라는 점에서, 네트워크에 대한 상업적 해석과 공익적 취지의 충돌이 필연적으로 발생하게 되는 것이다. 즉 특정 패킷에 대한 우열을 결정하는 전권이 영업을 목적으로 하는 사인의 손에 가있다는 점, 바로 여기에서부터 뜨거운 망중립성 논의가 비롯되는 것이다.

1. 양자의 공통점: 고도의 침해성

'네트워크 보안'과 '대역관리', 이 양자의 공통점은 숙지하는 바와 같이 DPI를 사용한다는 것이다. DPI는 패킷의 '헤더'가 아니라 '페이로드' 부분을 직접 검사하게 되므로, 그 파악의 범위가 단순히 운송을 목적으로 기록된 부분에 그치지 않는다. 즉 우편의 예를 들자면, 편지봉투에 적힌 주소 등을 살피는 것(SPI)만이 아니라 봉투안의 내용까지도 검사를 한다는 것(DPI)이다. 따라서 DPI는 고도의 프라이버시 침해 가능성을 가질 수밖에 없다. 이것이 바로 DPI의 본연적 독성이다.[10]
이러한 독성의 폐해가 극명하게 부각되는 것은 바로 DPI의 '망라적 특성' 부분이다. 즉 DPI를 위해서 네트워크 자체를 가로막고, 이를 지나는 모든 패킷을 대상으로 전방위적인 검사가 수행된다는 점이 바로 그것이다. 다시 말해 차별의 대상이 되는 패킷은 물론이고 우선시되는 패킷조차도, 일단 DPI가 실시되는 이상 프라이버시 침해를 피해볼 방도가 없다. 그 우열의 선별은, 무차별적인 DPI가 있은 이후에나 가능하기 때문이다.

---

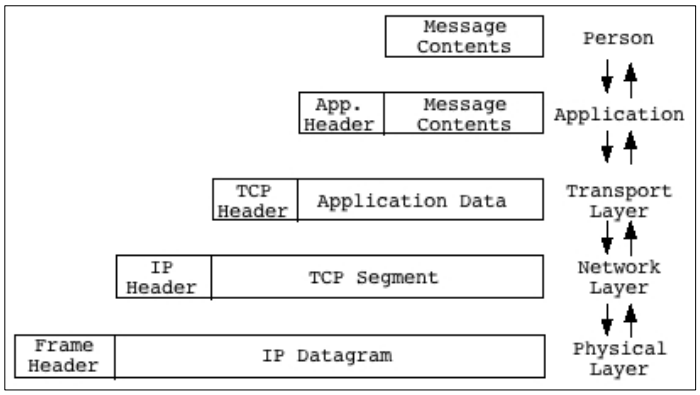
9) 네트워크를 공공재로 바라보는 시각은 다분히 논쟁의 소지가 있다. 그러나 이러한 접근은 비단 필자만의 독특한 논의가 아니며, 우리나라에서 진행되어온 망사업의 연혁을 살펴보아도 충분히 타당한 논의임을 밝히고 싶다. 흔히 네트워크를 도로에 비유하는 이유도 바로 이러한 연유임은 물론, 이러한 유사성을 이유로 양자를 동등한 대상으로 전제하여 규범적으로 검토한 우수한 논문도 어렵지 않게 발견할 수 있다: 이희정, "네트워크 동등접근에 관한 一考: 도로법제로부터의 시사점", 경제규제와 법, 제4권 제1호, 2011.

10) DPI의 이러한 특성은 망중립성 입법으로 직결되기도 한다. 예를 들어 네덜란드의 경우, 이러한 프라이버시 침해성을 이유로 망중립성 법안이 마련된 바 있다. 이에 관한 상세는 감상철/민대홍, "네덜란드의 망중립성 법제화 동향", 전자통신동향분석 제26권 제5호, 2010 참조.

2. 양자의 차이점: 규범적 평가의 상이

이에 관하여는 두 가지의 반론을 예상해 볼 수 있다. 먼저 '네트워크 보안'의 경우에서 보듯 DPI는 '독'이 아니라 오히려 '약'이 아닌가 하는 논의가 있을 수 있다. 지금에 와서 DPI가 없는 보안시스템을 강요하는 것은 현실성이 없고, 망중립성의 논의 이전에 망 자체의 안녕과 존립을 고려해야 한다는 점이 주요한 논거가 될 것이다. 그러나 기술적 중립성을 견지하여 아주 정확히 바라본다 하여도, 이러한 발상은 일종의 '착오'에 불과한 것이다. 왜냐하면 DPI가 '네트워크 보안'에 사용된다고 하여 정당화될 수 있는 것이 아니기 때문이다. 앞서 살핀바와 같이 DPI는 본래 치명적인 위법성을 가지고 있으나, '네트워크 보안'에서만큼은 그 사회적 필요에 의해 위법성을 부득불 조각해 주는 것이다. 즉 부득이한 경우 독약을 치료의 처방으로 사용하기도 하지만, 그렇다고 하여 독성이 없다는 것은 아니라는 것이다.[11]

다음으로 독성이 없는 DPI도 생각해 볼 수 있지 않는가 하는 발상이 있을 수 있다. 흔히 망사업자에 의해 언급되곤 하는 이러한 논의는 '해독제 개발 주장'이라 칭해볼 수 있을 것이다. 이를 좀 더 구체적으로 파악하기 위하여 아래의 도안을 주목해 보자.



<The Message and the Accumulation of Headers[12]>

애플리케이션 계층에서 또다른 헤더인 '애플리케이션 헤더'를 발견할 수 있다. 즉 SPI가 아니라 DPI의 대상이 되는 계층에서, '컨텐츠'가 아니라 '헤더'를 발견할 수 있다는 것이 도안의 핵심이 되겠다.[13] 따라서 DPI를 통해 패턴분석 등의 작업을 실시할 때, 프라이버시 침해가 없는 '애플리케이션 헤더'를 검사하게 되어 독성을 제거한 DPI가 수행된다는 것이 이 주장의 주요한 근거이다.[14]

---

11) 따라서 '부득이'의 여부가 핵심적인 쟁점이 될 것이다. 통상 이러한 '부득이성'을 인정하기 위해서는 '법적 확신'에 이를 정도로 명확한 사회적 합의가 전제되어야 하고, 구체적인 규정의 마련을 통해 제도적인 뒷받침을 하는 것이 일반적이다.

12) 이 도안은 Roger Clarkae, "Deep Packet Inspection: Its Nature and Implications", <http://dpi.priv.gc.ca/index.php/essays/deep-packet-inspection-its-nature-and-implications/>, 검색일자: 2012.9.5.에서 인용하였다. 원저자의 의도를 존중하기 위해, 제목을 번역하지 않고 그대로 두기로 한다.

13) 본 도안의 의미와 '애플리케이션 헤더'에 관한 구체적인 설명은, 이를 전공하신 강장묵 교수님의 역량에 의지하기로 한다.

14) 이러한 논의는 '헤더와 페이로드를 명확히 구분하는 것이 곤란'하다는 주장으로 변모하여 나타나기도 한다. 이에 관한 상세는 <http://republicans.energycommerce.house.gov/Media/file/Hearings/Telecom/042309_P

그러나 그 가부와 기술적 검토를 차치하고서라도, 이러한 주장은 두 가지의 점에서 논리적 모순이 있다.
첫째로, DPI에서의 검사행위(Inspection)가 '애플리케이션 헤더' 만을 콕! 집어내어 검사를 수행하는 방식인가 하는 것이다. 즉 도안을 그대로 살피자면, '애플리케이션 헤더'가 페이로드의 일정 부분에 자리하고 있으므로, 이를 열람하기 위해서는 페이로드 전체를 검사하게 될 것이라는 논리적 반박이 그것이다. 즉 애플리케이션 헤더에 대한 정확한 선별열람이 기술적으로 완벽해야만 모순이 발생하지 않는다.
둘째로, '애플리케이션 헤더'에 대한 열람은 프라이버시 침해성이 전무한가 하는 점이다. 그 의미상 '애플리케이션 헤더'를 통해 습득한 정보는 사용한 애플리케이션을 구분하는 용도로 활용될 것인데, 이를 편지봉투 겉면의 주소와 동등하게 취급할 수 있는가 하는 점이다. 어떠한 편지지를 사용한 것인가 또는 어떤 색깔의 잉크를 사용했는가 하는 내용은, 규범적 입장에서는 엄연히 프라이버시의 보호영역 안에 있는 것들이다. 어떤 종류의 속옷을 입었는지 또는 어떤 색깔의 속옷을 입었는지에 대한 지득이 프라이버시 침해가 아니란 말인가?!

3. 기술의 남용과 프라이버시

망중립성 논의에 있어 DPI에 대한 비난은 크게 두 가지의 차원에서 접근하여 볼 수 있다.
먼저 '대역관리'라는 논리로 포장된 '이익추구'를 위해 헌법이 보장하는 기본권인 프라이버시를 침해한다는 것이 타당한 것인가 하는 점, 즉 기술의 남용이라는 시각이 첫 번째의 접근이다. 이를 규범적으로 바라보자면 '비례의 원칙' 위반이 되겠다. 즉 '과잉금지의 원칙'으로서 '목적의 정당성', '방법의 적정성', '피해의 최소성', '법익의 균형성' 등이 평가의 틀이 되겠다. 굳이 상세한 검토를 하지 않아도 될 정도로 그 결과는 분명해 보인다.
다음으로 이렇듯 위해한 DPI가, 네트워크 사용자의 승낙이나 동의 없이 망사업자에 의해 작위적으로 진행된다는 점이다. 즉 DPI의 특성상 네트워크 사용자는 사용의 당시에 DPI가 실행되고 있음을 파악할 수 없고, 설사 다른 수단을 강구하여 망사용자 스스로 DPI 사실을 발견한다고 하여도 이를 저지할 방도도 없다. 또한 서비스 계약체결의 관행을 고려해볼 때 DPI에 대한 명시적인 동의절차는 애초부터 배제된 상태임은 물론, 네트워크에의 접속 시점이나 종료 시점에 망사업자로부터 DPI와 관련한 어떠한 통지도 받지 못한다. 결국 사용자의 권리는 철저하게 무시되는 것이다.
생각건대, 이러한 맹점에 대한 고민이 바로 망중립성 논의의 한가운데에 서있는 DPI의 운명을 결정하게 될 것이다. 즉 침해성의 우회 가능성은 없는가, 그리고 DPI 규제에 적합한 제도적 방안은 무엇인가 하는 질문들이 지금의 우리에게 던져진 미결의 과제인 것이다.[15]

---

rivacy/Center%20for%20Democracy%20and%20Technology%20-%20Harris.pdf>, 검색일자: 2012.9.5.에서 찾아볼 수 있다.

15) 이에 관한 기술적인 측면에서의 분석과 대안의 모색, 현행 법령의 분석과 입법안의 모색 또는 구체적인 동의의 절차와 방식 등의 규범적인 측면에서의 검토, 나아가 현 정부와 망사업자측에서 취하고 입장에 대한 비판과 대응방안의 마련 등 세부적인 사항에 대한 본격적인 논의는, 본고의 발제에서가 아니라 토론의 시점에 진행되어야 한다.

Ⅳ. 마치며

지금까지의 내용을 종합하여 볼 때, 망중립성 논의에 있어 DPI 문제는 핵심적인 사항이기는 하나 그리 복잡한 문제는 아님을 확인할 수 있다. DPI 기술자체의 본질적 위법성이 자명하므로 이러한 위법성을 조각할 정도의 중대한 사유가 아닌 이상 당연히 금지되어야 한다는, 매우 간명한 명제로 정리할 수 있기 때문이다. 이는 현재 '패킷감청'의 경우 헌법소원이 청구되어 헌법재판관의 책상위에 놓여있다는 점, '인터넷 맞춤광고'의 경우 우리나라를 비롯한 많은 국가에서 배척되었다는 점, 그리고 무엇보다 DPI의 폐해를 공감한 많은 네티즌들이 국경을 초월한 저지활동을 지속적으로 해오고 있다는 점 등의 사실을 통해 확연히 증명되고 있다.

요컨대, 망중립성 논의에 있어 DPI의 침해성은 더 이상의 다언을 요하지 않는다. 지금 우리의 앞에는, 네트워크의 철학과 속성에 정합성을 가진 규제의 수립만이 남아있을 뿐이다.

<별첨>

통신비밀보호법

[시행 2010.5.3] [법률 제9819호, 2009.11.2, 타법개정]

제1조 (목적) 이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신비밀을 보호하고 통신의 자유를 신장함을 목적으로 한다.

제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다. <개정 2001.12.29, 2004.1.29, 2005.1.27>

1. "통신"이라 함은 우편물 및 전기통신을 말한다.
2. "우편물"이라 함은 우편법에 의한 통상우편물과 소포우편물을 말한다.
3. "전기통신"이라 함은 전화·전자우편·회원제정보서비스·모사전송·무선호출 등과 같이 유선·무선·광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향·문언·부호 또는 영상을 송신하거나 수신하는 것을 말한다.
4. "당사자"라 함은 우편물의 발송인과 수취인, 전기통신의 송신인과 수신인을 말한다.
5. "내국인"이라 함은 대한민국의 통치권이 사실상 행사되고 있는 지역에 주소 또는 거소를 두고 있는 대한민국 국민을 말한다.
6. "검열"이라 함은 우편물에 대하여 당사자의 동의없이 이를 개봉하거나 기타의 방법으로 그 내용을 지득 또는 채록하거나 유치하는 것을 말한다.
7. "감청"이라 함은 전기통신에 대하여 당사자의 동의없이 전자장치·기계장치등을 사용하여 통신의 음향·문언·부호·영상을 청취·공독하여 그 내용을 지득 또는 채록하거나 전기통신의 송·수신을 방해하는 것을 말한다.
8. "감청설비"라 함은 대화 또는 전기통신의 감청에 사용될 수 있는 전자장치·기계장치 기타 설비를 말한다. 다만, 전기통신 기기·기구 또는 그 부품으로서 일반적으로 사용되는 것 및 청각교정을 위한 보청기 또는 이와 유사한 용도로 일반적으로 사용되는 것중에서, 대통령령이 정하는 것은 제외한다.

8의2. "불법감청설비탐지"라 함은 이 법의 규정에 의하지 아니하고 행하는 감청 또는 대화의 청취에 사용되는 설비를 탐지하는 것을 말한다.

9. "전자우편"이라 함은 컴퓨터 통신망을 통해서 메시지를 전송하는 것 또는 전송된 메시지를 말한다.
10. "회원제정보서비스"라 함은 특정의 회원이나 계약자에게 제공하는 정보서비스 또는 그와 같은 네트워크의 방식을 말한다.
11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.

가. 가입자의 전기통신일시
나. 전기통신개시·종료시간
다. 발·착신 통신번호 등 상대방의 가입자번호
라. 사용도수

마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료

바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적 자료

사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료

12. "단말기기 고유번호"라 함은 이동통신사업자와 이용계약이 체결된 개인의 이동전화 단말기기에 부여된 전자적 고유번호를 말한다.

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. <개정 2000.12.29, 2001.12.29, 2004.1.29, 2005.3.31, 2007.12.21, 2009.11.2>

1. 환부우편물등의 처리 : 우편법 제28조·제32조·제35조·제36조등의 규정에 의하여 폭발물등 우편금제품이 들어 있다고 의심되는 소포우편물(이와 유사한 우편물을 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

②우편물의 검열 또는 전기통신의 감청(이하 "통신제한조치"라 한다)은 범죄수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며, 국민의 통신비밀에 대한 침해가 최소한에 그치도록 노력하여야 한다.<신설 2001.12.29>

③누구든지 단말기기 고유번호를 제공하거나 제공받아서는 아니된다. 다만, 이동전화단말기 제조업체 또는 이동통신사업자가 단말기의 개통처리 및 수리 등 정당한 업무의 이행을 위하여 제공하거나 제공받는 경우에는 그러하지 아니하다.<신설 2004.1.29>

제14조 (타인의 대화비밀 침해금지) ①누구든지 공개되지 아니한 타인간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취할 수 없다.

②제4조 내지 제8조, 제9조제1항 전단 및 제3항, 제9조의2, 제11조제1항·제3항·제4항 및 제12조의 규정은 제1항의 규정에 의한 녹음 또는 청취에 관하여 이를 적용한다.<개정 2

001.12.29>

정보통신망 이용촉진 및 정보보호 등에 관한 법률

[시행 2012.8.18] [법률 제11322호, 2012.2.17, 일부개정]

제2조(정의) ① 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2004.1.29, 2007.1.26, 2007.12.21, 2008.6.13, 2010.3.22>

1. "정보통신망"이란 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

2. "정보통신서비스"란 「전기통신사업법」 제2조제6호에 따른 전기통신역무와 이를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 것을 말한다.

3. "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.

4. "이용자"란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.

5. "전자문서"란 컴퓨터 등 정보처리능력을 가진 장치에 의하여 전자적인 형태로 작성되어 송수신되거나 저장된 문서형식의 자료로서 표준화된 것을 말한다.

6. "개인정보"란 생존하는 개인에 관한 정보로서 성명·주민등록번호 등에 의하여 특정한 개인을 알아볼 수 있는 부호·문자·음성·음향 및 영상 등의 정보(해당 정보만으로는 특정 개인을 알아볼 수 없어도 다른 정보와 쉽게 결합하여 알아볼 수 있는 경우에는 그 정보를 포함한다)를 말한다.

7. "침해사고"란 해킹, 컴퓨터바이러스, 논리폭탄, 메일폭탄, 서비스 거부 또는 고출력 전자기파 등의 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하는 행위를 하여 발생한 사태를 말한다.

8. "정보보호산업"이란 정보보호제품을 개발·생산 또는 유통하는 사업이나 정보보호에 관한 컨설팅 등과 관련된 산업을 말한다.

9. "게시판"이란 그 명칭과 관계없이 정보통신망을 이용하여 일반에게 공개할 목적으로 부호·문자·음성·음향·화상·동영상 등의 정보를 이용자가 게재할 수 있는 컴퓨터 프로그램이나 기술적 장치를 말한다.

10. "통신과금서비스"란 정보통신서비스로서 다음 각 목의 업무를 말한다.

가. 타인이 판매·제공하는 재화 또는 용역(이하 "재화등"이라 한다)의 대가를 자신이 제공하는 전기통신역무의 요금과 함께 청구·징수하는 업무

나. 타인이 판매·제공하는 재화등의 대가가 가목의 업무를 제공하는 자의 전기통신역무의 요금과 함께 청구·징수되도록 거래정보를 전자적으로 송수신하는 것 또는 그 대가의 정산을 대행하거나 매개하는 업무

11. "통신과금서비스제공자"란 제53조에 따라 등록을 하고 통신과금서비스를 제공하는 자를 말한다.

12. "통신과금서비스이용자"란 통신과금서비스제공자로부터 통신과금서비스를 이용하여 재화등을 구입·이용하는 자를 말한다.

② 이 법에서 사용하는 용어의 뜻은 제1항에서 정하는 것 외에는 「정보화촉진기본법」으로 정하는 바에 따른다.<개정 2008.6.13>

제21조(전자문서 등의 공개 제한) 전자문서중계자는 전자문서중계설비에 의하여 처리되는 전자문서 또는 관련 기록을 적법한 절차에 따르지 아니하거나 전자문서 발신자 및 수신자의 동의 없이 공개하여서는 아니 된다.

[전문개정 2008.6.13]

제23조(개인정보의 수집 제한 등) ① 정보통신서비스 제공자는 사상, 신념, 과거의 병력(病歷) 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 그 개인정보를 수집할 수 있다.

② 정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우에는 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보 외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니 된다.

[전문개정 2008.6.13]

제49조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.

[전문개정 2008.6.13]

제49조의2(속이는 행위에 의한 개인정보의 수집금지 등) ① 누구든지 정보통신망을 통하여 속이는 행위로 다른 사람의 정보를 수집하거나 다른 사람이 정보를 제공하도록 유인하여서는 아니 된다.

② 정보통신서비스 제공자는 제1항을 위반한 사실을 발견하면 즉시 방송통신위원회나 한국인터넷진흥원에 신고하여야 한다.<개정 2009.4.22>

③ 방송통신위원회나 한국인터넷진흥원은 제2항에 따른 신고를 받거나 제1항을 위반한 사실을 알게 되면 다음 각 호의 필요한 조치를 하여야 한다.<개정 2009.4.22>

1. 위반 사실에 관한 정보의 수집·전파

2. 유사 피해에 대한 예보·경보

3. 정보통신서비스 제공자에 대한 접속경로의 차단요청 등 피해 확산을 방지하기 위한 긴급조치

[전문개정 2008.6.13]

개인정보 보호법

[시행 2012.3.30] [법률 제10465호, 2011.3.29, 제정]

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보”란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.

2. “처리”란 개인정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

6. “공공기관”이란 다음 각 목의 기관을 말한다.

가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체

나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관

7. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적합하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보의 익명처리가 가능한 경우에는 익명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

전기통신사업법

[시행 2012.7.18] [법률 제11201호, 2012.1.17, 일부개정]

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다. <개정 2011.5.19>

1. "전기통신"이란 유선·무선·광선 또는 그 밖의 전자적 방식으로 부호·문언·음향 또는 영상을 송신하거나 수신하는 것을 말한다.
2. "전기통신설비"란 전기통신을 하기 위한 기계·기구·선로 또는 그 밖에 전기통신에 필요한 설비를 말한다.
3. "전기통신회선설비"란 전기통신설비 중 전기통신을 행하기 위한 송신·수신 장소 간의 통신로 구성설비로서 전송설비·선로설비 및 이것과 일체로 설치되는 교환설비와 이들의 부속설비를 말한다.
4. "사업용전기통신설비"란 전기통신사업에 제공하기 위한 전기통신설비를 말한다.
5. "자가전기통신설비"란 사업용전기통신설비 외의 것으로서 특정인이 자신의 전기통신에 이용하기 위하여 설치한 전기통신설비를 말한다.
6. "전기통신역무"란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다.

7. "전기통신사업"이란 전기통신역무를 제공하는 사업을 말한다.

8. "전기통신사업자"란 이 법에 따른 허가를 받거나 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무를 제공하는 자를 말한다.

9. "이용자"란 전기통신역무를 제공받기 위하여 전기통신사업자와 전기통신역무의 이용에 관한 계약을 체결한 자를 말한다.

10. "보편적 역무"란 모든 이용자가 언제 어디서나 적절한 요금으로 제공받을 수 있는 기본적인 전기통신역무를 말한다.

11. "기간통신역무"란 전화·인터넷접속 등과 같이 음성·데이터·영상 등을 그 내용이나 형태의 변경 없이 송신 또는 수신하게 하는 전기통신역무 및 음성·데이터·영상 등의 송신 또는 수신이 가능하도록 전기통신회선설비를 임대하는 전기통신역무를 말한다. 다만, 방송통신위원회가 정하여 고시하는 전기통신서비스(제6호의 전기통신역무의 세부적인 개별 서비스를 말한다. 이하 같다)는 제외한다.

12. "부가통신역무"란 기간통신역무 외의 전기통신역무를 말한다.

13. "특수한 유형의 부가통신역무"란 다음 각 목의 업무를 말한다.

가. 「저작권법」 제104조에 따른 특수한 유형의 온라인서비스제공자의 부가통신역무

나. 그 밖에 타인 상호간에 컴퓨터를 이용하여 「국가정보화 기본법」 제3조제1호에 따른 정보를 저장·전송하거나 전송하는 것을 목적으로 하는 부가통신역무

제3조(역무의 제공 의무 등) ① 전기통신사업자는 정당한 사유 없이 전기통신역무의 제공을 거부하여서는 아니 된다.

② 전기통신사업자는 그 업무를 처리할 때 공평하고 신속하며 정확하게 하여야 한다.

③ 전기통신역무의 요금은 전기통신사업이 원활하게 발전할 수 있고 이용자가 편리하고 다양한 전기통신역무를 공평하고 저렴하게 제공받을 수 있도록 합리적으로 결정되어야 한다.

제50조(금지행위) ① 전기통신사업자는 공정한 경쟁 또는 이용자의 이익을 해치거나 해칠 우려가 있는 다음 각 호의 어느 하나에 해당하는 행위(이하 "금지행위"라 한다)를 하거나 다른 전기통신사업자 또는 제3자로 하여금 금지행위를 하도록 하여서는 아니 된다.

1. 설비등의 제공·공동활용·공동이용·상호접속·공동사용·도매제공 또는 정보의 제공 등에 관하여 불합리하거나 차별적인 조건 또는 제한을 부당하게 부과하는 행위

2. 설비등의 제공·공동활용·공동이용·상호접속·공동사용·도매제공 또는 정보의 제공 등에 관하여 협정 체결을 부당하게 거부하거나 체결된 협정을 정당한 사유 없이 이행하지 아니하는 행위

3. 설비등의 제공·공동활용·공동이용·상호접속·공동사용·도매제공 또는 정보의 제공 등으로 알게 된 다른 전기통신사업자의 정보 등을 자신의 영업활동에 부당하게 유용하는 행위

4. 비용이나 수익을 부당하게 분류하여 전기통신서비스의 이용요금이나 설비등의 제공·공동활용·공동이용·상호접속·공동사용·도매제공 또는 정보의 제공 등의 대가 등을 산정하는 행위

5. 이용약관(제28조제1항 및 제2항에 따라 신고하거나 인가받은 이용약관만을 말한다)과 다르게 전기통신서비스를 제공하거나 전기통신이용자의 이익을 현저히 해치는 방식으로 전

기통신서비스를 제공하는 행위

6. 설비등의 제공・공동활용・공동이용・상호접속・공동사용・도매제공 또는 정보 제공의 대가를 공급비용에 비하여 부당하게 높게 결정・유지하는 행위

7. 「전파법」에 따라 할당받은 주파수를 사용하는 전기통신역무를 이용하여 디지털콘텐츠를 제공하기 위한 거래에서 적정한 수익배분을 거부하거나 제한하는 행위

② 전기통신사업자와의 협정에 따라 전기통신사업자와 이용자 간의 계약 체결(체결된 계약 내용을 변경하는 것을 포함한다) 등을 대리하는 자가 제1항제5호의 행위를 한 경우에 그 행위에 대하여 제52조와 제53조를 적용할 때에는 전기통신사업자가 그 행위를 한 것으로 본다. 다만, 전기통신사업자가 그 행위를 방지하기 위하여 상당한 주의를 한 경우에는 그러하지 아니하다.

③ 제1항에 따른 금지행위의 유형 및 기준에 관하여 필요한 사항은 대통령령으로 정한다.

<별첨2>

통신망의 합리적 관리 및 이용에 관한 기준(안)

I. 목적

1. 이 기준은 '망 중립성 및 인터넷 트래픽 관리에 관한 가이드라인'('11.12.26 제정 '12.1.1 시행)에 근거하여 합리적인 트래픽 관리 및 트래픽 관리의 투명성에 관한 세부사항을 정함으로써, 인터넷접속서비스 제공사업자의 투명하고 합리적인 트래픽 관리를 유도하고 망 자원의 합리적이고 효율적인 이용환경을 조성하여 ICT 생태계의 건전하고 지속가능한 발전을 도모함을 목적으로 한다.

II. 적용 대상

2. 이 기준은 일반적인 인터넷접속서비스에 적용되며, 관리형 서비스에 대하여는 적용되지 아니한다.

* 관리형서비스(managed service)는 인터넷접속서비스제공사업자가 일반적으로 통용되는 인터넷의 제공 방식과 달리 트래픽 전송 품질을 보장하는 서비스를 말한다.

III. 타 법령과의 관계

3. 인터넷접속서비스제공사업자가 이 기준에 따라 트래픽 관리를 시행하고자 하는 경우에는 전기통신사업 관련 법령이 정하는 바에 의하여 이용약관을 개정한 후 시행하여야 한다.

* 기존 이용약관에 포함되어 있거나, 내용상 이용약관에 포함되는 사항이 아닌 경우(콘텐츠 제공사업자와 인터넷접속서비스제공사업자간 협의를 통하여 정하는 사항 등)는 제외한다.

4. 인터넷접속서비스제공사업자는 트래픽 관리를 시행함에 있어 전기통신사업법, 통신비밀보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률 등 관련 법령을 준수하여야 한다.

IV. 트래픽 관리의 기본원칙

5. 인터넷접속서비스제공사업자는 트래픽 증가에 대응함에 있어서 지속적인 망 고도화를 통해 이를 해결하도록 노력해야 한다.

인터넷접속서비스제공사업자는 망 과부하로 인한 문제를 해결하거나 이를 방지하기 위해 필

요한 한도 내에서 제한적으로 트래픽 관리를 시행할 수 있으나, 해당 트래픽 관리의 목적에 부합하고, 트래픽 관리가 이용자에게 미치는 영향이 최소화될 수 있는 방안을 강구하여야 하며, 유사한 콘텐츠, 애플리케이션, 서비스, 기기 등을 불합리하게 차별해서는 아니 된다.

인터넷접속서비스제공사업자는 트래픽 관리에 있어 유무선 등 망의 유형이나 구조, 서비스 제공방식, 주파수 자원의 제약 등 기술적 특성을 고려할 수 있다.

V. 합리적 트래픽 관리로 인정되는 경우(1)

6. 인터넷접속서비스제공사업자의 합리적인 트래픽 관리의 필요성이 인정되는 경우는 다음과 같다. 이 기준에 적시되지 않은 경우에도 방송통신위원회는 기술의 발전과 새로운 서비스의 등장, 인터넷 이용형태의 변화 등에 의해 발생할 수 있는 트래픽 관리 필요성 등을 고려하여 사안별로 그 합리성 여부를 판단할 수 있다.

- 망의 보안성 및 안정성 확보를 위한 경우 (예 : DDos, 해킹 대응 등)
- 망 혼잡으로부터 다수이용자의 이익을 보호하고, 공평한 인터넷 이용환경을 보장하기 위해 불가피하게 제한적으로 트래픽 관리를 시행하는 경우
- 관련법령의 규정에 근거하거나 법령 집행을 위해 필요한 경우
  (예 : 정보통신망법상 불법정보 – 음란. 사행정보 등- 을 법적 절차에 따라 차단 등)
- 법령이나 약관에 근거한 이용자의 요청이 있는 경우 (예: 스팸, 유해콘텐츠 차단 등)
- 적법한 계약 등 이용자의 동의를 얻어 트래픽을 제한하는 경우

* 이밖에도 방통위가 기술발전 등을 고려하여 사안별로 합리성 여부를 판단

V. 합리적 트래픽 관리로 인정되는 경우(2)

① DDos, 악성코드, 해킹 또는 이와 유사한 수준의 사이버 공격 및 통신장애에 대응하기 위한 트래픽 관리 등 망의 보안성 및 안정성 확보를 위해 필요한 경우

<예시1> DDos 공격 시 방송통신위원회 및 한국인터넷진흥원의 요청에 따라 DDos 공격의 원인이 되는 좀비 PC를 망에서 차단하는 경우

<예시2> 망에 위해를 주는 악성코드,, 바이러스 등에 대응하기 위한 경우

<예시3> 망의 장애 상황 또는 장애가 명백하게 예상되는 상황에서 그 원인이 되는 트래픽을 긴급히 제한할 필요성이 있는 경우

V. 합리적 트래픽 관리로 인정되는 경우(3)

② 일시적 과부하 등에 따른 망 혼잡으로부터 다수 이용자의 이익을 보호하고 전체 이용자의 공평한 인터넷 이용환경을 보장하기 위하여, 불가피하게 제한적으로 트래픽 관리를 시행하는 경우

V. 합리적 트래픽 관리로 인정되는 경우(4)

②-1. 망 혼잡 관리를 위한 P2P 트래픽의 전송 제한 인터넷에 접속하는 이용자들의 수가 집중되는 특정시간대(최번시) 등 특별히 망 혼잡이 우려되는 특정한 조건 하에서 P2P 트래픽 전송을 최소한의 범위 내에서 제한하는 경우

P2P 트래픽에 대한 관리가 불가피하게 요구되는 망의혼잡 상황 판단기준은 인터넷접속서비스제공사업자가망의 특성과 망 구축 현황, 망의 안정적 운영을 위한 자체 관리기준, 이용 상황 등을 종합적으로 고려하여 정한다.

P2P 트래픽을 제한할 수 있는 특정한 조건은 최번시 이용자 접속률과 같은 객관적인 근거를 바탕으로 결정되어야 하며, 무조건적이고 상시적인 P2P 제한은 허용되지 아니한다.

인터넷접속서비스제공사업자는 이 기준 제7항에 따른 트래픽 관리 방침 공개 시 위의 기준을 공개하여야 한다.

<예시4> 이용자의 접속이 가장 많은 시간대(통상 오후 9시~11시. 사업자별 상황에 따라 달라질 수 있음)에 P2P 트래픽의 전송 속도를 일정 속도 이하로 제한하는 경우

V. 합리적 트래픽 관리로 인정되는 경우(5)

②-2. 소수의 초다량이용자(heavy user)에 대한 트래픽 제한

통상적인 인터넷 이용 수준을 넘어서 지나치게 다량의 트래픽을 유발하고 과도한 대역폭을 점유함으로써, 명백하게 다른 이용자의 인터넷 이용환경을 저해할 우려가 있는 이용자(“초다량이용자”)의 트래픽을 제한하는 경우

다만, 이 경우에도 인터넷 검색, 이메일 등 대용량의 트래픽을 유발하지 않는 서비스는 이용할 수 있도록 하여야 한다.

이용자의 데이터 사용량 한도 설정 등 초다량이용자에 대한 트래픽 관리 방법은 인터넷접속서비스제공사업자가 망의 특성과 망 구축 현황, 망의 안정적 운영을 위한 자체 관리기준, 이용 상황 등을 종합적으로 고려하여 정한다.

특히, 유선인터넷에서 제이터 사용량 한도를 정할 때에는 트래픽을 과도하게 유발하는 소수의 초다량이용자들에 한해 적용될 수 있도록 그 기준을 정함으로써, 대다수 이용자들의 원활한 인터넷 이용에 영향을 미치지 않도록 하여야 한다.

인터넷접속서비스제공사업자는 이 기준 제7항에 따른 트래픽 관리 방침 공개 시 위의 기준을 공개하여야 한다.

<예시5> 유선인터넷에서 이용자의 월별 사용량 한도를 정하고, 이를 초과하는 이용자의 트래픽에 대하여 일시적으로 전송속도를 일정 속도 이하로 제한하는 경우

<예시6> 무선인터넷에서 특정지역내에서의 일시적인 호 폭주 등 망 혼잡이 발생하였거나, 망 운영 상황, 트래픽 추세변화, 자체 관리 기준 등에 근거하여 망 혼잡 발생 가능성이 객관적이고 명백한 때, 데이터 사용량 한도를 초과한 이용자에 대해 동영상서비스(VOD) 등 대용량 서비스의 사용을 일시적으로 제한하는 경우

V. 합리적 트래픽 관리로 인정되는 경우(6)

②-3. 망 혼잡으로 트래픽 관리가 불가피한 상황에서, 정당한 사유 없이 산업계에서 널리 인정되는 공신력 있는 국내외 표준화기구가 망의 효율적 이용을 위해 제정한 표준을 준수하지 않는 콘텐츠, 애플리케이션, 서비스(이하 '콘텐츠 등'이라 한다)를 유사한 콘텐츠 등 중에서 우선적으로 제한하는 경우

다만, 이 경우에도 표준을 준수하지 않았다는 이유만으로 무조건적이고 상시적으로 해당 콘텐츠 등을 제한하여서는 아니 된다.

인터넷접속서비스제공사업자는 표준을 준수하지 않는 콘텐츠 등을 제한하기에 앞서 콘텐츠 등의 제공사업자에게 표준의 준수 또는 대안의 모색에 대해 충분히 권고하고 협의하여야 한다.

또한 해당 콘텐츠 등에 대한 제한은 해당 콘텐츠 등의 기술적 특성과 표준과의 직접적인 연관관계 존재 여부, 표준 미준수 사유 기술적 준비 등에 소요되는 기간, 표준을 준수하기 위해 요구되는 비용, 표준 적용 시 실제 망 혼잡 감소 효과 등을 고려하여 결정되어야 한다.

<예시7> 한국정보통신기술협회(TTA)가 빈번한 Keep Alive 신호 등에 따른 이동통신장애에 대비 "이동 통신망에서의 Push 알림 구현방법"을 기술표준으로 마련('11.12)한 것과 관련, 이를 준수할 것을 사전에 충분히 권고하고 망 혼잡으로 트래픽 관리가 불가피한 경우 이를 준수하지 않은 애플리케이션을 유사한 애플리케이션들 중 우선적으로 제한하는 경우

V. 합리적 트래픽 관리로 인정되는 경우(7)

③ 관련 법령의 규정에 근거하거나, 법령 집행을 위해 필요한 경우

<예시8> '정보통신망 이용촉진 및 정보보호에 관한 법률' 제44조의 7 제1항에 규정한 불법정보(음란 정보, 청소년유해매체물 표시의무를 이행하지 아니한 정보, 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보 등)에 대해 방송통신위원회가 방송통신심의위원회의 심의를 거쳐 인터넷접속서비스제공사업자에게 제한할 것을 명한 정보를 차단하는 경우

④ 스팸, 유해 콘텐츠 차단 등 법령이나 이용약관 등에 근거한 이용자의 요청이 있는 경우

<예시9> 청소년보호법 제2조 제3호의 청소년유해매체물로부터 미성년자인 자녀를 보호하기 위해 관련 서비스 약관에 따라 부모가 접속 차단을 요청한 경우

V. 합리적 트래픽 관리로 인정되는 경우(8)

⑤ 적법한 계약 등의 방법으로 이용자의 동의를 얻어 트래픽을 제한하는 경우, 다만, 이 경우 그 합리성 판단에 있어서는 시장의 경쟁상황에 따라 이용자에게 요금정도에 비례한 서비스에 대한 실질적인 선택권이 보장되고 있는지의 여부 등이 고려되어야 한다.

<예시10> 시장에서 사업자간 경쟁이 존재하는 상황에서 무선인터넷서비스의 요금제에 따라 mVoIP 트래픽의 제한 여부 또는 제한의 수준을 다르게 규정하면서 이용자가 그 필요에 따라 선택할 수 있도록 하는 경우

망 중립성 및 합리적 트래픽 관리에 대한 요구가 인터넷접속서비스제공사업자에게 이용자와의 개별적인 거래조건과 무관하게 모든 이용자에게 동일한 인터넷 이용환경을 제공할 의무를 부과하는 것은 아님

VI. 트래픽 관리정보의 투명한 공개

공개대상 정보

7. 인터넷접속서비스제공사업자는 이용자의 선택권 보장을 위해, 트래픽 관리의 범위와 트래픽 관리가 적용되기 위한 조건, 절차, 방법 및 이에 따른 영향 등 자신의 트래픽 관리에 관한 정보를 이용자에게 공개하여야 한다.

<예시11> 일시적 망 혼잡 시 트래픽 관리 실행 절차 혼잡에 대한 인지(모니터링) -> 이용자 고지 -> 트래픽관리 -> (필요 시 사후 고지) -> 혼잡상황 모니터링 -> 혼잡

상황 해제 시 트래픽 관리 종료

이 경우, 제공 서비스의 종류 또는 상품에 따라 차이가 있는 경우에는 이를 구분하여 표시하여야 한다.

인터넷접속서비스제공사업자는 이용자에게 실질적인 트래픽 관리정보가 제공될 수 있도록, 공개되는 정보의 내용을 지속적으로 현행화하여야 한다.

공개 방법

8. 방송통신위원회는 인터넷접속서비스제공사업자에 대하여 이용자들이 이해하기 쉽고, 타 인터넷접속서비스제공사업자와 비교할 수 있도록 트래픽 관리 정보 공개에 관한 공통양식(별지 참조)을 정하여 공개할 것을 권고할 수 있으며, 인터넷접속서비스제공사업자는 공통 양식에 따르거나 또는 자율적으로 양식을 정하여 사용 할 수 있다.

다만, 인터넷접속서비스제공사업자가 자율적 양식을 사용하는 경우에도 공통양식에 명시된 사항에 관한 정보는 반드시 포함하여야 한다.

VII. 이용자 보호

이용자에 대한 고지

9. 인터넷접속서비스제공사업자는 트래픽 관리정보에 관한 사항을 이용약관에 규정하는 외에도 인터넷 홈페이지 등 이용자의 접근이 용이한 방식을 통해 안내하여야 한다.

10. 개별 이용자 차원의 트래픽 관리가 시행되는 경우, 인터넷접속서비스제공사업자는 그 사실을 해당 이용자에게 이메일, 단문메시지 서비스(SMS) 등을 통하여 고지하여야 하며, 개별적인 고지가 어려운 경우에는 인터넷접속서비스제공사업자의 인터넷 홈페이지 등 다양한 수단을 통해 해당 사실을 이용자에게 널리 알리기 위하여 노력하여야 한다.

11. 인터넷접속서비스제공사업자는 개별 이용자의 자기 통제권 보장과 합리적 인터넷 이용을 위해 기술적으로 가능한 범위내에서 이용자가 자신의 트래픽 사용 현황을 확인할 수 있도록 하여야 한다.

민원처리기구의 운영

12. 인터넷접속서비스제공사업자는 트래픽 관리와 관련된 문의, 트개픽 관리에 대한 사실확인 및 이의제기 등 이용자의 민원사항을 처치할 수 있는 전담 기구를 설치. 운영하여야 한다.

VIII. 트래픽 관리의 합리성 판단 기준

13. 방송통신위원회는 인터넷접속서비스제공사업자의 트래픽 관리의 합리성 여부를 판단하는 경우 다음의 사항을 고려하여야 한다.

① (투명성) 인터넷접속서비스제공사업자가 트래픽 관리에 관한 정보를 사전에 충분히 공개하였는지 여부와, 구체적인 트래픽 관리 조치를 시행하는 경우 이용자 및 트래픽 관리로부터 직접적인 영향을 받는 자에게 트래픽 관리에 관한 정보를 사전에 또는 부득이한 경우 사후에 충분히 고지하였는지 여부

② (비례성) 인터넷접속서비스제공사업자의 트래픽 관리 행위가 트래픽 관리의 목적. 동기와 부합하는지 여부 및 당해 트래픽 관리의 영향을 최소화하는 방법을 강구하였는지 여부

<예시11> 혼잡을 유발하는 콘텐츠가 특정될 수 있는 경우, 혼잡관리를 위해 당해 콘텐츠가 아닌 다른 콘텐츠를 제한하거나, 기기에 대한 접근을 차단하는 행위는 합리적인 트래픽 관리로 보기 어려움

<예시12> 혼잡관리를 위해서는 전송 속도 제한으로 충분한 상황임에도 불구 하고 트래픽을 전면 차단하거나 필요 이상으로 전송속도를 저하시키는 행위는 합리적인 트래픽 관리로 보기 어려움

③ (비차별성) 유사한 형태의 콘텐츠 등, 기기 또는 장비에 대하여 정당한 사유 없이 차별하여 취급하지 않았는지 여부

<예시13> 트래픽 관리의 필요성에 비추어 동일한 트래픽 관리가 적용되어야 할 것으로 보이는 유사한 서비스 A와 B에 대해, A서비스는 제한하고 B서비스는 허용하는 것은 합리적인 트래픽 관리로 보기 어려움

④ (기술적 특성)유무선 망의 유형 및 구조, 서비스 제공방식, 주파수 자원의 제약 등 기술적 특성

14. 인터넷접속서비스제공사업자는 방송통신위원회의 요청이 있는 경우 당해 트래픽 관리 행위의 합리성을 입증할 수 있는 객관적 자료를 제출하여야 한다.

IX. 통신망 자원의 조화로운 이용을 위한 노력

15. 통신망을 이용하는 콘텐츠 등의 제공사업자와 기기 및 장비 제조사는 인터넷접속서비스제공사업자가 합리적 트래픽 관리의 필요성에 따라 트래픽에 관한 정보를 요청하는 경

우 특별한 사유가 없는 한 이를 제공하여야하며, 신규서비스 등을 개발하는 경우 망에 대한 부하를 최소화하는 기술을 적용하는 등의 방법으로 망의 공평하고 효율적인 관리와 활용을 위하여 노력하여야 한다.

16. 인터넷접속서비스제공사업자는 통신망을 기반으로 하는 콘텐츠 등의 제공사업자 또는 기기 및 장비 제조사가 신규서비스 개발 등을 위해 필요한 망의 관리에 관한 정보를 요청하는 경우 특별한 사유가 없는 한 이를 제공하여야 한다.

17. 인터넷접속서비스제공사업자, 콘텐츠 등의 제공사업자와 기기 및 장비 제조사는 정보의 제공 등에 대해 사업자간 협의가 이루어지지 않는 경우 방송통신위원회에 조정을 요청하거나 또는 전기통신사업법 제45조에 따른 재정을 신청할 수 있다.

X. 후속조치

18. 인터넷접속서비스제공사업자는 방송통신위원회가 이 기준을 확정한 날로부터 6개월 이내에 트래픽 관리 정보를 자사의 인터넷 홈페이지 등에 공개하여야 한다.

별지 : 인터넷접속서비스제공사업자의 트래픽 관리정보

공개 양식(예시)