인터넷 트래픽 관리와 DPI (Deep Packet Inspection)

강 유 리*

심층 패킷 분석(Deep Packet Inspection, DPI)은 아직까지 표준화된 기술이 아니므로 그 정의가 유동적이나 일반적으로 패킷의 콘텐츠가 담긴 심층부분까지 검사할 수 있는 기술로 통용된다. 대규모 네트워크 환경에서 짧은 시간안에 다양한 애플리케이션을 식별할 수 있다는 DPI의 특징은 광범위한 네트워크를 운영하는 인터넷제공사업자(Internet Service Provider, ISP)에게 매력적인 기술로 다가온다. 실제로 네트워크에 전송되는 애플리케이션이 복잡, 다양해지고 데이터 트래픽이 급격하게 증가하면서 이에 따른 혼잡제어 등 더 정교한 트래픽 관리를 위해 ISP의 DPI에 대한 관심은 증가하고 있다.

이러한 관심은 "망 중립성" 또는 인터넷 "트래픽 관리" 논쟁의 연장선에서 DPI 사용이 정당한지에 대한 찬반논의를 불러일으키고 있다. DPI 사용이 정당함을 주장하는 쪽에서는 네트워크 전체의 성능 및 서비스 품질을 개선할 수 있는 장점을 부각시키고 있으며, 그 반대편에서는 이용자의 이익을 저해시키거나 DPI가 어떤 목적으로 사용되는지 명확하게 알 수 없고 네트워크를 파편화시킬 것이라는 우려를 표명하며 대립하고 있다.

이러한 논란에도 불구하고 2011년에는 전 세계 70개국의 주요 ISP 중 절반 정도가 트래픽 관리를 위해 DPI를 실행하고 있는 것으로 나타났다. 그리고 DPI 사용에 대한 정보가 투명하게 공개되는 조건에서 "합리적"으로 DPI를 사용할 수 있다고 결론 내려진 DPI 분쟁 사례를 고려할 때, 트래픽 관리 도구로써 DPI 자체가 문제의 소지가 있다고 간주하는 것은 성급한 판단일 수 있다. 본고는 트래픽 관리 차원의 DPI로 연구 범위를 한정하여 기술적 특징, 논의 동향 및 관련 분쟁 사례를 통해 향후 합리적 수준의 DPI가 어떻게 시장에 정착되어야 할 것인지에 대한 출발점을 제공하고자 한다.

* 정보통신정책연구원 창조경제연구실 전문연구원, (02)570-4257, xiaojie622@kisdi.re.kr

목 차

Ⅰ. 서 론

심층 패킷 분석(Deep Packet Inspection, DPI)은 기본적으로 패킷 내부의 콘텐츠까지 파악하는 기술로 이해된다. 이러한 기술이 사용되는 이유는 인터넷에서 전송 제어 프로토콜(Transport Control Protocol, TCP)이 갖고 있는 한계 때문이다. 즉, TCP는 전체 데이터가 호스트간에 잘 전송될 수 있도록 데이터의 흐름을 조절하고 성공적으로 상대편에 도착할 수 있도록 보장하는 역할을 하지만, 호스트당 연결 경로의 수를 제한하는 메커니즘을 갖고 있지 않다. 그러므로 특정 애플리케이션이 다중 경로를 사용하는 경우 단일 경로를 사용하는 애플리케이션의 연결이 불리해지는 문제가 발생한다. 만일 특정 애플리케이션(예: P2P 파일 공유[1])이 여러 경로를 점유하여 전송속도를 높이고자 하는 경우 별도의 트래픽 관리가 없다면, VoIP나 온라인 게임과 같이 전송 속도는 높지 않더라도 실시간 전송이 중요한 애플리케이션의 이용이 어렵거나 불가능해지는 결과가 초래될 수 있다.

인터넷의 이러한 단점을 보완하고 기본적으로 바이러스 및 말웨어 등으로부터 네트워크를 보호하고자 인터넷제공사업자(Internet Service Provider, ISP)들은 오래전부터 트래픽 관리를 해 왔다. 최근에는 트래픽 폭증으로 인한 혼잡을 제어하면서 네트워크를 좀 더 효율적으로 운영하는 것뿐만 아니라 사업상의 다양한 목적을 위해 정교한 트래픽 관리의 도구로써 DPI에 대한 관심이 증가하고 있다. 이에 따라 트래픽 관리 또는 망 중립성 관련 논쟁의 연장선상에서 DPI 사용이 정당한 것인지에 대한 논란이 이어지고 있다.

1) 웹 브라우징과 같은 클라이언트-서버 애플리케이션은 서버에 하나 또는 경우에 따라 몇몇의 서버

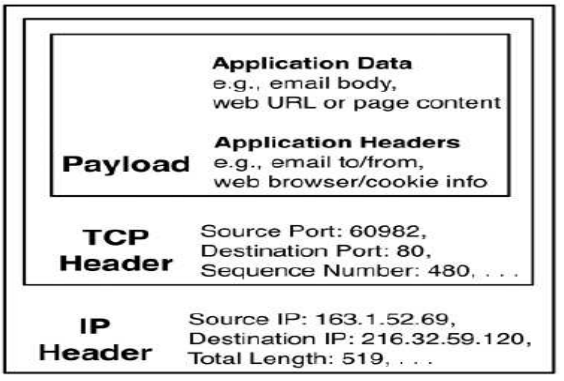
본고는 트래픽 관리 측면에서의 DPI에 초점을 두고 논의를 전개하였다. 이를 위해서 패킷 검사 개요와 관련 기술을 살펴보고, DPI를 둘러싼 이슈를 검토하였다. 마지막으로 DPI를 수단으로 한 트래픽 관리 분쟁 사례를 분석하였다.

Ⅱ. 패킷 검사와 DPI

1. 패킷과 트래픽 관리

"Deep Packet Inspection"이란 용어 자체에도 담겨 있듯 DPI를 논의하기 위해서는 우선 패킷(packet)에 대한 이해가 필요하다. 일반적으로 패킷은 IP(Internet Protocol) 네트워크 상에서 전송되거나 라우트되는 가장 작은 단위이다. 패킷은 크게 헤더(header)와 페이로드(payloads)로 구분되며, 헤더는 다시 IP 헤더와 프로토콜 헤더로 나눌 수 있다.

〔그림 1〕 패킷의 구조



자료: Cooper(2011), p.142.

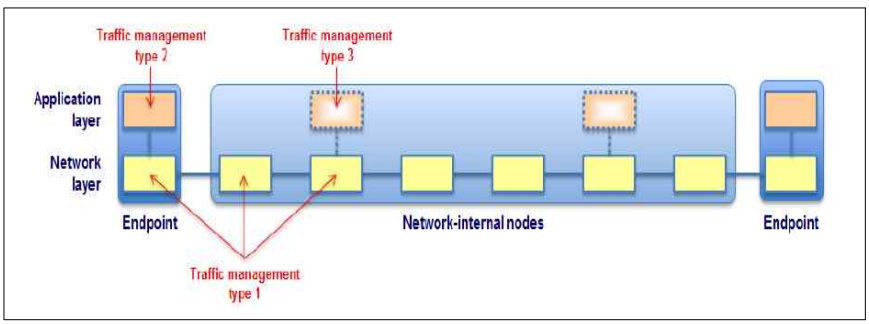
IP 헤더는 패킷의 가장 바깥에 있는 부분으로 IP의 출발 주소, 도착 주소 및 패킷의 바이트(byte)[2] 단위 길이 등과 같은 정보를 담고 있다. 이는 엽서에서의 주소와 비슷

에 소수의 연결만을 열게 되는 것과 다르다.

한 역할을 한다고 볼 수 있으며, 전송의 우선순위와 같은 다른 정보도 포함할 수 있다. IP 헤더 안쪽으로는 전송계층 헤더가 있는데 여러 가지 전송계층 프로토콜 가운데 TCP가 가장 널리 사용되고 있다. TCP는 패킷이 전달되어야 할 단말단의 주소(포트라고 부름)를 식별하고 패킷 손실시 오류 검출 정보를 제공하는 기능을 담당하며, TCP 헤더는 착·발신 포트, 시퀀스 넘버 등으로 구성되어 있다. 예를 들면, 인터넷 상에서 웹페이지 등을 요청할 때 쓰는 HTTP는 포트 80을, 이메일은 포트 25를 사용한다. 페이로드는 전송되는 실제 콘텐츠나 데이터를 담고 있는 패킷의 심층 부분을 말한다. 즉, 이메일 메시지, VoIP 통화 및 웹서핑 세션 등을 구성하는 모든 비트(bits)가 페이로드에 해당한다.

이렇게 구성된 패킷들은 네트워크라는 전송매체를 통해서 전달되는데 ISP들은 네트워크를 운영하는 과정에서 필요에 따라 트래픽 관리를 시행한다. 유럽전자통신규제기구인 BEREC(Body of European Regulators for Electronic Communications)은 어느 계층, 어느 네트워크의 위치에서 트래픽 관리가 이뤄지는지에 따라 트래픽 관리를 세 가지로 분류하고 있다.

〔그림 2〕 트래픽 관리의 종류



자료: BEREC(2012), p.1.

2) 8비트(bits)로 구성되는 정보의 기본단위로 일반적으로 8개 혹은 9개의 비트를 묶어서 표현한다. 여기서 비트(bit)는 정보의 최소단위로 이진법의 한 자리수로 표현된다.

트래픽 관리 타입 1은 네트워크 끝단이든 네트워크 내부 노드든 관계없이 네트워크 계층에서 이뤄지는 트래픽 관리를 말한다. 트래픽 관리 타입 2, 3은 애플리케이션 계층에서 이뤄지는 트래픽 관리로, 트래픽 관리 타입 2는 네트워크 끝단에서, 트래픽 관리 타입 3은 네트워크 내부 노드에서 실행된다.

트래픽 관리 타입 1은 패킷 헤더의 도착 주소나 다른 비슷한 정보에 기반하여 IP 패킷을 네트워크 상에서 다른 링크로 라우팅(routing)이나 포워딩(forwarding)하는 것을 말한다. 대표적으로 DiffServ[3]나 MPLS[4] 등이 있다. 트래픽 관리 타입 2는 혼잡제어(Congestion Control)나 동적 적응 부호화(Dynamic Adaptive Coding)와 같은 기능을 포함한다. 예를 들어, 혼잡제어[5]는 네트워크가 혼잡해지면 끝단에서 전송속도를 줄여서 상황이 심화되는 것을 막는 역할을 한다. 트래픽 관리 타입 3은 트래픽 필터링, 트래픽 변경 및 비슷한 다른 용어로 지칭되는 기술들을 포함한다. 이 단계는 패킷의 가장 심층 부분을 검사하기 때문에 DPI로 불리기도 하며, 미리 지정된 트래픽 관리정책에 따라 개별 IP 패킷이 분류, 전달, 지연 및 폐기된다.

2. 패킷 검사의 분류

데이터는 전송될 때 분할, 암호화, 압축 및 포장되어 전달된 뒤, 다시 포장을 풀고, 암호를 풀고, 압축을 풀고, 분할된 것을 다시 조립하는 과정을 거친다. 이러한 과정은 일반적으로 OSI(Open System Interconnection) 계층으로 불리는 네트워크 참조모델

3) DiffServ는 Differentiated Service(차등화 서비스)의 약자로 미리 정의된 서비스 품질 수준에 따라 트래픽을 클래스별로 구분하여 우대 처리하는 기술로 구현이 용이하고 확장성이 용이한 프로토콜이다.

4) MPLS는 Multi Protocol Label Switching(다중 프로토콜 레벨 스위칭)의 약자로 인터넷의 백본망 등에서 대량의 트래픽을 고속으로 처리하기 위해 매 라우터마다 패킷의 헤더를 조사하여 다음 라우터로 경로를 설정하는 것이 아니라 MPLS망에 진입하는 시점에서 단 한번만 헤더를 조사하고 우편번호와 같이 짧은 라벨을 이용하여 경로를 설정하는 방식을 말한다.

5) 혼잡제어(Congestion Control)는 혼잡관리(Congestion Management)의 한 종류이다. 혼잡관리는 이용자의 PC 같은 끝단이나 네트워크 내부의 노드에서 실행될 수 있으며, 네트워크 끝단에서 진행되는 경우를 혼잡관리라고 한다.

(Reference Model)로 구현된다. 이 OSI 계층과 패킷의 구조를 연관지어 보면, 헤더는 1~4계층까지, 페이로드는 5계층 이상에 해당한다.

〈표 1〉 OSI 계층

계층	OSI 계층	기능	Payload/Header 구분
7	애플리케이션 계층 (Application Layer)	사용자가 사용하는 층으로 HTTP, FTP, 이메일 등 서비스 의미	페이로드 (Payload)
6	프리젠테이션 계층 (Presentation Layer)	정보의 표현방식 관리, 암호화, 정보압축	
5	세션 계층 (Session Layer)	응용 프로세서간 대화 관장	
4	트랜스포트 계층 (Transport Layer)	한 컴퓨터 안에서 포트 번호로 프로그램들을 구분	TCP 헤더 (TCP Header)
3	네트워크 계층 (Network Layer)	IP 주소를 통해 바이너리 집합체 전송	IP 헤더 (IP Header)
2	데이터링크 계층 (Data Link Layer)	MAC 주소를 통해 바이트들로 나열된 집합체 전송 및 데이터 전송상의 에러 확인	
1	물리 계층 (Physical Layer)	전자 신호 전송(비트정보 전달)	

자료: http://blog.daum.net/jty71/15645329

이러한 맥락에서 패킷 검사는 네트워크 계층의 어느 부분까지를 살펴보는 지로 세분화할 수 있는데, 그 세분화 정도에 있어 명확히 정해진 것은 없다. Parsons(2008)은 3단계로 구분하며, Cooper(2010)은 2단계로 나누기도 한다. 본고는 Parsons(2008)의 분류를 기준으로 살펴보도록 한다. 3단계의 패킷 분석은 단층 패킷 분석(Shallow Packet Inspection 또는 Stateful Packet Inspection, SPI), 중층 패킷 분석(Medium Packet Inspection, MPI), 심층 패킷 분석(Deep Packet Inspection, DPI)을 가리킨다. SPI, MPI 및 DPI를 앞에서 나온 OSI 계층과 연관시키면, 다음과 같이 도식화할 수 있다.

〔그림 3〕 OSI 계층과 패킷 검사 수준

자료: Parsons(2008), p.6.

SPI는 주로 네트워크 방화벽(firewall) 시스템을 위해 개발되어 온 기술로 패킷의 헤더 정보를 조사하고 이들 정보가 블랙리스트에 있으면 패킷을 전달하지 않는다. 즉, SPI는 세션 및 프리젠테이션이나 애플리케이션 계층을 읽을 수 없고, 이는 패킷의 페이로드 부분까지 들여다 볼 수 없음을 의미한다. 패킷의 헤더 정보만을 통해 트래픽을 판단하기 때문에 트래픽에 대한 정교한 분석(특히, 애플리케이션 관련 추론)은 어렵지만, DPI에 비해 대용량의 트래픽을 매우 빠르게 처리할 수 있다.

MPI는 애플리케이션 프락시(Application Proxies)를 의미하는데, 이는 데이터를 가져올 때 해당 사이트에서 바로 PC로 가져오는 것이 아니라 프락시라는 임시 저장소를 거쳐서 가져오기 때문이다. 패킷이 프락시 장비로 들어오면 프락시 장비는 패킷 헤더의 정보를 파스리스트(parse-list)에 따라서 검토한다. 애플리케이션 프락시는 네트워크 라우팅 장비와 함께 일렬로 놓이는데, 이는 네트워크를 지나는 모든 트래픽이 프락시 장비를 거쳐 감으로써 네트워크 관리자가 미리 정해놓은 규칙을 일괄적으로 적용하기 위해서이다.

패킷의 전송 허용여부를 판단함에 있어 SPI의 블랙리스트는 IP 주소만을 보는데 반해, MPI의 파스리스트는 특정 패킷의 전송여부를 데이터 포맷의 종류와 인터넷에서의 위치에 기반하여 결정한다. 예를 들면, MPI 장비를 사용해 관리자는 YouTube로부터의 플래시 파일이나 SNS에서의 이미지 파일이 클라이언트 컴퓨터에서 열리지 않도록 할 수 있다. 한편 MPI 장비들은 확장성이 떨어져서 애플리케이션이 다양해질수록 각 애플리케이션에 대한 별도 애플리케이션 게이트웨이를 필요로 한다. 이는 전송속도를 지연시키는 요인으로 작용할 수 있기 때문에 다양한 애플리케이션이 구현되는 대규모의 네트워크를 운영하는 ISP에게는 유용성이 떨어진다고 할 수 있다.[6)]

DPI는 2000년경부터 나오기 시작한 개념으로, 표준화된 기술이 아니어서 그 의미가 다소 유동적이다. 일반적으로 패킷의 헤더뿐만 아니라 콘텐츠가 담긴 페이로드부분까지 보는 기술로 알려져 있지만 이를 어떻게 구현하는지는 DPI 벤더간 차별화 요소로 대부분 밝혀지지 않고 있다. 애플리케이션 식별에 한계가 있는 SPI 및 MPI와 달리 DPI는 매초에 수십만 건을 실시간으로 처리하며, 무슨 프로그램이 어떠한 패킷을 생성하는지 판단할 수 있도록 고안되었기 때문에 대규모 네트워크 환경에서 사용될 수 있다.

DPI 장비는 이미 식별된 패킷의 종류에 매칭시킬 수 있는 충분한 정보를 가질 때까지 수십만의 패킷을 검사 장비의 메모리에 저장한다. 일단 새로운 패킷이 이미 장비에 의해 식별된 패킷 리스트에 매칭되면, 장비는 무슨 애플리케이션이 패킷을 생성하고 보내는지를 알게 되고 패킷 전송을 허용할지 말지의 규칙을 적용한다.[7)] 만일 DPI 장비가 패킷 헤더와 페이로드 부분까지 검사를 해도 애플리케이션을 식별할 수 없으면, DPI 장비는 컴퓨터간에 패킷이 어떻게 교환되는지 그 패턴을 검토한다.[8)]

---

6) 확장성이 떨어짐에도 불구하고 MPI 장비는 프리젠테이션 계층의 패킷 페이로드를 읽고, 애플리케이션 계층까지 식별할 수 있어 오늘날의 DPI 기술의 전 단계로 중요성을 갖는다.

7) Parsons(2008), p.9.

8) 이를 휴리스틱 평가 방식이라고 부르며, 데이터 암호화에 따른 패킷 검사의 문제를 효과적으로 우회할 수 있는 것으로 알려져 있다. 휴리스틱 평가에 대한 자세한 설명은 Allot Communications (2007)을 참고하라.

〈표 2〉 DPI 적용 과정 예시

애플리케이션 사업자는 자신 서비스의 패킷 헤더 정보를 속이거나 페이로드 데이터를 암호화함으로써 패킷 검사 장비가 자신의 패킷을 식별하는 것을 우회할 수 있다. 예를 들어, Skype 패킷이 완전하게 암호화되고 헤더의 정보가 위조되었다면, ISP는 Skype 트래픽을 감지하기 위해서 다른 방법을 적용해야 한다. 이 경우, DPI 장비는 Skype 이용자가 음성통화를 시작할 때 발생하는 데이터의 교환 패턴을 모니터링한다. 무작위로 보이는 패킷의 초기 버스트(burst)[9]가 경험적으로 식별되는 과정에서 Skype 애플리케이션과 관련이 있다고 볼 수 있는 공통적인 패턴이 발견된다. 이를 통해 ISP는 식별된 애플리케이션의 패킷을 지연시킬지나 우선순위를 주어 전송할지 등을 결정한다.

3. DPI의 특징 및 사용 유인[10]

라우터와 스위치들이 패킷의 헤더뿐만 아니라 데이터의 콘텐츠가 들어 있는 페이로드까지 실시간으로 읽고 분석하는 기술인 DPI는 발전과정에서 다음과 같은 두 가지 특징을 갖게 되었다. 첫째, DPI 기술은 실시간으로 인터넷 트래픽을 분석하여 차별적으로 처리할 수 있도록 진화하였다. 둘째, 다양한 기능들을 하나의 장비에 구현할 수 있도록 발전하였다. 이로 인해서 보안, 트래픽 관리, 유해 콘텐츠 차단, 맞춤 광고 제공 등 다양한 목적을 위해 사용될 수 있다.

예를 들어, 가입자단의 대역폭 확대에 한계를 느끼는 네트워크 사업자들이 말웨어나 대용량 트래픽을 유발하는 애플리케이션 관리를 통해 네트워크 운영의 효율성을 도모하고자 할 수 있다. ISP들의 경우, 추가적으로 수입을 창출하길 원하거나 애플리케이션 사업자의 음성전화 또는 VoD 등으로부터 자사 서비스의 수익 보전 차원에서 DPI를 사용하여 자사 서비스와 타 서비스간 품질 차이를 제공할 유인을 가질 수 있다. 콘텐츠 사업자들도 자신들의 지적 자산이 허가없이 불법적으로 유통되는 것을 필터링하기 위해 DPI에 관심을 갖고 있다. 이와 같이 다양한 플레이어들이 각각의 목적에 따라 DPI 기술을 사용할 유인이 있다는 것은 기존에 유지되어 온 인터넷의 특징이 변할 수 있음을 의미한다.

9) 디지털 데이터 전송에서 신호 펄스열의 덩어리와 같이 차례로 전송되는 신호 중 특정한 규약에 따라 한 덩어리의 정보로 다루어지는 신호의 모임을 말한다(자료: Daum 백과사전).

10) Bendrath(2009)

〈표 3〉 DPI의 다양한 이용 목적

목 적	내 용
네트워크 보안	- 바이러스, 말웨어 및 위해 트래픽 차단
네트워크 관리	- 희소한 주파수 자원을 효율적으로 운영하기 위해 P2P와 같이 원치 않는 트래픽을 저하·차단하거나 트래픽 종류에 따른 라우팅 최적화
콘텐츠 규제	- 아동 학대부터 국가 및 사회 안정성을 해칠 수 있는 불법 또는 유해 콘텐츠 차단
저작권 보호	- P2P 등을 통해 저작권이 보호된 콘텐츠의 유통 방지
맞춤형 광고 제공	- 개별 이용자가 발생하는 인터넷 트래픽에 기반한 맞춤형 광고 제공

실제로 상당수의 ISP가 DPI를 사용하고 있는데, Asghari et al.(2012)의 연구에 따르면 DPI 보급률은 2010년에 64%로 가장 높았다가 2011년에 48%로 감소한 것으로 나타났다.

〈표 4〉 전 세계 ISP의 DPI 사용 현황(2009년~2011년)

년도	DPI 사용 정도에 따른 ISP 수				총 ISP (DPI 적용 사업자 비중)
	알 수 없음 DPI Score〈0.09	No DPI 0.09≤DPI Score〈0.13	Medium use 0.13≤DPI Score〈0.4	High use Score≤0.4	
2009	35	116 (48%)	68 (28%)	59 (24%)	278 (52%)
2010	49	80 (36%)	85 (39%)	56 (25%)	270 (64%)
2011	31	109 (52%)	68 (33%)	31 (15%)	239 (48%)

주: 1. 케이블, DSL, WiMAX, FTTH를 통해서 최종이용자에게 인터넷접속서비스를 제공하는 ISP 대상으로 기본적으로 유선 기반의 ISP일 것으로 볼 수 있음
2. ISP가 BitTorrent 등 특정 트래픽을 차단하거나 저하시키는지를 테스트 할 수 있는 서비스를 제공하는 Glasnost를 실행시켜 원시데이터를 추출함
3. DPI Score는 각 ISP가 DPI를 사용한다고 나온 Glasnost 횟수를 그 ISP의 네트워크에 대해서 돌린 총 Glasnost 횟수로 나눈 값이며, 그 값에 따라 DPI 사용 수준을 판단함
4. 조사 기준에 따라 총 75개국의 288개 ISP가 모집단으로 추출되었고, 연도별로 유효 데이터가 추출된 국가 및 ISP 수에는 변동있음
5. 괄호안의 퍼센트는 DPI 사용여부가 확인되지 않은 ISP를 제외하고 계산한 비율임

자료: Asghari et al.(2012), p.10. 수정 인용

DPI 이용 비중이 증가하다가 감소한 것에 대해서는 좀 더 정교한 분석이 필요할 것으로 보이나,[11] 여전히 상당수의 ISP들이 P2P 트래픽 관리를 목적으로 DPI를 사용하고 있다는 것은 비교적 자명한 사실로 볼 수 있다. 한편 전 세계 DPI 장비 시장은 2018년에 약 38억 달러 규모에 달해 2012년부터 연평균 36.6%씩 성장할 것으로 예측된다.[12]

Ⅲ. DPI 관련 이슈[13]

1. 망 중립성과 트래픽 관리

망 중립성은 인터넷망 위에 흐르는 데이터 트래픽을 그 내용, 유형, 인터넷 주소, 제공사업자, 부착된 단말기기 등에 관계없이 동등하게 처리하는 것을 의미한다. 그러나 네트워크 보안, 혼잡관리 및 기타 사업상의 목적에 따라 트래픽 관리의 필요성이 증가하면서 트래픽 관리가 망 중립성을 저해하는 것이 아닌지에 대한 논란이 제기되고 있다. 비록 망 중립성 규제를 지향하는 국가들에서 망 중립성 규제시 예외적으로 합리적 트래픽 관리를 인정하는 경향을 보이고 있으나,[14] 망 중립성과 트래픽 관리의 관계에 대한 논란은 쉽게 종식되지 않을 것으로 예상된다.[15]

---

11) Asghari et al.(2012)는 DPI 기술 가격에 대한 부담이 완화되고 DPI의 활용성이나 편익에 대한 ISP의 인식이 높아짐에 따라 2010년까지는 DPI 이용이 확산되다가 이에 대해서 이용자 및 정치권 등의 부정적 반응으로 ISP의 DPI 채택이 점차 저하되면서 2011년의 보급률이 낮아진 것이라 추측하고 있다.

12) Broadband Traffic Management(2013. 2. 14)

13) DPI 관련 이슈에는 망 중립성 이외에 프라이버시 침해가 있다. 2012년 10월, ITU-T는 Y.2770 표준으로 알려진 차세대 통신망에서 적용할 DPI 요구사항을 승인하였다. 비록 DPI 시스템이 어떻게 작동하는지에 대해서는 명시하지 않았지만, 표준에서 제정된 요구사항들이 오히려 프라이버시 침해 가능성을 높일 수 있다는 비판이 제기되고 있다. 그러나 본고는 트래픽 관리 측면에서 DPI를 다루고 있으므로 프라이버시 침해에 대한 이슈는 논외로 하며, 더 자세한 내용은 Daly(2010)나 Mochalski & Schulze(2009)를 참고하길 바란다.

14) 나성현(2012)

15) 이하 각 입장에 대해서는 Mochalski & Schulze(2009)를 참고 및 보완하였다.

망 중립성 규제를 찬성하는 진영에서는 첫째, 트래픽 관리가 인터넷의 가장 전통적인 원칙인 단대단 원칙(end-to-end principle)에 위배된다고 주장한다. 트래픽 관리를 통해 ISP가 양 끝단에서 전송되는 애플리케이션이나 서비스를 간섭하거나 변경할 수 있기 때문에 ISP가 "단순한 전송" 기능만을 담당해야 한다는 원칙에 반하게 되는 것이다. 둘째, ISP가 트래픽 관리를 통해 비즈니스 모델을 계층화시켜 경쟁을 저해하고 이용자 이익을 해칠 수 있다고 본다. 예를 들면, 수직 결합된 ISP가 DPI를 통해 자회사나 더 빠른 접속을 위해 돈을 더 지불한 콘텐츠 사업자에게 우선순위를 부여하는 비즈니스 모델은 제3의 콘텐츠 사업자나 추가적 돈을 지불하지 않은 콘텐츠 사업자의 경쟁력을 저하시킬 수 있다. 뿐만 아니라 자신의 가입자에게만 매력있는 서비스를 배타적으로 제공함으로써 경쟁사의 네트워크를 이용하는 가입자는 경쟁력이 없는 서비스를 이용해야 하는 상황이 벌어질 수 있다. 이러한 우려는 특히 인터넷접속 시장이 경쟁적이지 못한 경우 발생할 가능성이 높다. 셋째, 애플리케이션 및 콘텐츠 사업자들이 트래픽 관리를 우회하기 위해 서비스나 콘텐츠의 암호화에 대한 불필요한 경쟁(arms race)을 할 우려도 제기되고 있다. 이는 인터넷 생태계에 대한 진입장벽을 높이는 원인이 되면서 동시에 ISP로 하여금 이에 대응하여 독자적인 트래픽 관리 기술을 개발 및 채택함으로써 네트워크가 이음새 없이(seamless) 연결되기 보다는 파편화(balkanization)되는 악순환의 반복으로 인터넷 생태계의 혁신이 저해될 수 있다는 비판으로 이어지고 있다.

한편, 망 중립성 규제를 반대 진영에서는 트래픽 관리가 오늘날 인터넷의 단점을 보완할 수 있음을 주목하고 있다. 첫째, 현재의 트래픽의 폭증에 대한 ISP의 대응 역량이 미흡하기 때문에 망 중립성만을 주장하는 것은 오히려 ISP의 네트워크에 대한 투자를 저해하고 결국에는 이용가능한 대역폭을 제한하는 결과를 초래할 수 있다고 본다. 그러므로 대역폭에 우선순위를 적용하는 등의 트래픽 관리가 인터넷 혁신에 필요하다는 시각이다. 이와 함께 오늘날의 최선형 인터넷일지라도 실시간 트래픽이 파일 전송 및 민감하지 않은 트래픽보다 우선시되고 있어 사실상 네트워크가 중립적이지 않음을 언급하고 있다.[16] 둘째, 품질을 보장하기 위해 일부 데이터를 차별화하는

것은 문제가 아니며 사실상 매우 바람직하다는 주장이다. 오히려 P2P 통신, mVoIP 등의 서비스가 오히려 표준 사용 계약(good usage contract)을 어기고 네트워크 성능을 저하시키고 있으며, 현재의 정액 과금 모델을 해치는 것이라고 보고 있다.[17] 셋째, 애플리케이션별로 다른 서비스 속성을 지니고 있기 때문에 이를 정교하게 구분하기 위해서라도 심층부분까지 조사하는 트래픽 관리가 필요하다는 주장이다. 예를 들어, VoIP는 매우 적은 대역폭을 필요로 하지만 항상 최소한의 품질이 보장되어야 하나, 파일 공유 애플리케이션은 가능한 많은 대역폭을 필요로 하는 반면 매우 낮은 전송속도가 유지되어도 된다. 게다가 이용자별로 이러한 애플리케이션을 이용하는 패턴은 다르기 때문에 애플리케이션 중립적 또는 모든 이용자에게 공평하게 대역폭을 배분하는 접근방법이 혼잡을 해결할 수 없을 뿐만 아니라 결코 현명하지 않다고 지적한다.

2. 트래픽 관리와 DPI

희소한 자원인 네트워크는 제한된 대역폭에 많은 트래픽이 몰릴 경우 혼잡 문제에서 자유롭지 못하다. Bendrath(2009)는 오늘날 HD급의 비디오 스트리밍이나 P2P 파일 공유와 같은 대용량 트래픽을 유발하는 애플리케이션이 증가함에 따라, 인터넷의 백본보다 가입자단(last mile)에서 혼잡이 발생하기 시작했다고 지적하고 있다. 하지만 이러한 혼잡 문제가 네트워크 자원 자체의 희소성에서만 기인하는 것은 아니다. 일반적으로 사업자들은 모든 인터넷 가입자들이 동시에 인터넷을 이용하거나 또는 항상 최대 속도를 필요로 하지 않을 것이라는 가정 하에 전체 가입자 규모에 비해 좁은 대역폭을 제공하고 있다.[18] 이를 초과가입(oversubscription)이라고 부르며, 사업자 측면에서 경제적으로도 타당한 전략이라고 볼 수 있지만, 이로 인해 혼잡 문제가 가중되기도 한다.

인터넷 프로토콜은 이를 다루기 위한 자체 방식을 내재하고 있으며, 이를 TCP/IP

16) Wu(2003)

17) Zahariadis & Perdikeas(2012), p.7.

18) 대부분의 ISP들은 광고나 약관을 통해서 실제 속도가 아닌 기술적으로 가능한 "최대" 속도를 제시하고 있다.

혼잡제어라고 한다. 그러나 보통의 TCP/IP 혼잡제어 메커니즘은 애플리케이션이 공평한 방식으로 행동하는 경우(즉, 동시에 다중 경로를 형성하지 않거나 혹은 IETF[19] 에서 제시한 혼잡제어 표준을 위반하지 않는 경우)에만 작동하기 때문에 P2P 등의 애플리케이션이 여러 경로를 점유하는 상황에서는 적합하지 않은 측면이 있다.[20] 이에 따라 상당수의 ISP들은 별도의 트래픽 관리를 하고 있으며, 그 수단으로 DPI 기술을 이용하고 있는데 이의 타당성에 대해서는 논란이 발생하고 있다.

(1) ISP의 DPI 사용에 대한 타당성[21]

DPI는 문제가 되는 애플리케이션이나 패킷을 표적으로 설정하여 그것들의 우선순위를 떨어뜨리거나 차단함으로써 네트워크 전체의 성능 및 서비스 품질을 개선할 수 있다. 이러한 장점을 부각함에 있어 ISP들은 다음과 같은 주장을 하고 있다.

첫째, DPI가 실질적으로 내용을 파악하는 것이 아니라는 점이다. 일반적으로 DPI에 대한 비난을 하면서 편지나 소포를 배달하는 집배원이 그 내용을 보는 것으로 비유하고 있는데 이는 적절한 비유가 아니라는 의견이다. 오히려 패킷은 누구나 볼 수 있도록 공개되었다는 점에서 동봉된 편지나 소포보다는 엽서에 비유하는 것이 더 적합하다는 것이다. 그리고 DPI는 음성, 이메일, 말웨어 등 전송되는 객체들의 특성을 이해하기 위한 기술로, 사적인 내용을 “읽는” 것이 아니라 그 패턴을 스캔함으로써 어떻게 최적으로 전송할 것인지를 결정하는 수단으로 봐야 한다고 주장한다. 둘째, 전송되는 패턴을 파악하기 때문에 정확하게 프로토콜이나 애플리케이션의 분류가 가능하다는 점이다. 오늘날 많은 애플리케이션들이 다이내믹 포트나 기존에 다른 애플리케이션에 의해 이용되던 포트를 사용하기도 하여 헤더의 정보만으로 프로토콜이나 애플리케이션에 대한 신뢰성 있는 분류가 불가능해지고 있다. 예를 들면, Skype 및 다른

19) Internet Engineering Task Force, 인터넷의 운영, 관리, 개발에 대해 협의하고 프로토콜과 구조적인 사안들을 분석하는 인터넷 표준화 작업기구로 망 설계자, 운영자, 업체, 연구자들로 구성되었다.

20) Bendrath(2009), p.19.

21) 이하는 Mochalski & Schulze(2009)를 참고하여 요약하였다.

P2P 애플리케이션은 웹에 최적화시키기 위해 또는 다른 포트에 대해 부과되는 제약을 피하기 위해 웹 트래픽용으로 많이 사용되는 포트 80을 종종 사용하기도 한다. 즉 웹 트래픽 포트를 사용하지만 실제는 P2P 파일 공유 용도로 사용되기 때문에 이러한 경우는 DPI를 통해야 실질적으로 프로토콜을 구분할 수 있다는 것이다. 셋째, DPI는 전 계층의 패킷을 분석함으로써 서비스 세분화를 통해 이용자별 일정한 서비스 수준의 보장을 가능케 한다는 것이다. 즉, 이를 비즈니스 모델과 연관시키면 이용자의 수요에 맞게 서비스 제공 수준에 대한 과금체계를 구성할 수 있다. 현재 20%의 이용자가 80%의 트래픽을 점유한다고 알려져 있는데,[22] 많은 트래픽을 유발하는 이용자는 더 많은 요금을, 적게 이용하는 이용자는 저렴한 요금을 내도록 함으로써 이용자 편익 증대 및 네트워크 투자 재원 마련이 가능할 것이라는 시각이다.

(2) ISP의 DPI 사용에 대한 우려[23]

DPI는 ISP뿐만 아니라 CDN 사업자나 캐싱 서비스 제공사업자들도 충분한 사용 유인을 갖고 있다. 그러나 유독 ISP의 DPI 사용에 대한 우려가 매우 높게 제기되고 있음은 ISP가 갖는 다음의 세 가지 특성에 기인한다.

첫째, ISP는 인터넷 게이트웨이로서의 역할을 한다. 지금까지는 인터넷은 단순한 전송 매체라는 전제에서 개인적이거나 상업적인 통신, 거래 등이 온라인을 통해 이뤄져 왔다. 그러나 DPI를 통해서 ISP가 단순 전송 매체 제공자에서 게이트웨이로서의 역할을 강화시킬 가능성이 제기되고 있다. 이는 이용자로 하여금 스스로 자기 통제를 하거나 중요한 거래는 하지 않는 등 이용자 측면에서 인터넷의 자유로운 이용을 저해할 유인을 유발할 수 있다는 것이다. 둘째, ISP의 전환 비용이 높다는 점이다. ISP를 전환하는 것은 검색 엔진이나 웹 브라우저를 변경하는 것과 달리 장애가 존재한다. 검색엔진이나 웹 브라우저 변경이 단순 클릭이나 소프트웨어 다운로드와 같은 간단한 절차를 포함하는 반면에 ISP의 전환은 상대적으로 복잡한 과정(예: 대체 상품 검색, 필요

22) Mochalski & Schulze(2009), p.6.
23) 이하는 Cooper(2010)을 참고하여 정리하였다.

시 지불방법 변경, 해지시의 위약금 계산 등)을 수반하고 있다. 이러한 전환 장벽으로 가입자들은 자신이 이용중인 ISP가 DPI 기반의 트래픽 관리를 도입하는 것을 원치 않아도 다른 ISP로 전환할 수 없거나 이에 대한 어려움을 느낄 수 있다. 셋째, 용도 변경(mission creep)의 가능성이다. 즉, 초기에 어떤 특정 목적을 위해 도입한 DPI가 시간이 지남에 따라 다양하고 새로운 목적에 사용될 수 있다는 점이다. DPI는 장비별로 패킷 오류 수정(intercepting packet), 패턴 매칭, 원시 데이터 저장, 데이터에 수집 및 이에 대한 결론 등의 다양한 컴퓨팅 능력을 갖고 있다. 각각의 DPI 장비들은 이들 기능 중 일부 혹은 전부를 사용하는데, DPI 벤더들은 기술 진화와 함께 다양한 목적에 두루 적합하도록 DPI 장비를 제작하는 것이 더 효율적이고 비용을 절감하는 것이라고 판단하고 있는 추세이다. 이에 따라 다양한 기능이 하나의 DPI 장비에 집약되면서, 원래의 사용 목적 이외의 다른 목적으로 사용하는 것이 가능해지고 있다. 문제는 이러한 일들이 이용자들에게 공개되지 않은 채 진행될 경우이다. 뿐만 아니라 DPI 장비 자체가 네트워크 및 이용자의 경험에 최소한의 영향을 미치도록 설계되기 때문에 만일 용도 변경이 발생해도 이용자가 이를 식별하기는 쉽지 않다. 실제로 캐나다의 한 대형 ISP는 “DPI를 데이터 수집 차원에서 도입하였으나 결국에는 트래픽 제어에 사용하기로 결정했다”는 사실을 시인한 바 있다.[24)]

Ⅳ. DPI를 통한 트래픽 관리 분쟁

1. 미국 Comcast 사례

(1) Comcast의 DPI 사용

미국의 케이블 인터넷 사업자인 Comcast는 2005년 5월부터 10월까지 자사의 트래픽을 분석하고 혼잡이 어디서 발생하는지 확인하기 위해 DPI 벤더인 Sandvine과 함께 분석에 착수했다. 양사는 몇몇의 P2P 프로토콜이 정기적으로 비정상적인 상향 트

24) Cooper(2011), p.149.

래픽을 유발한다고 결론을 내리고, 2006년 1월부터 2007년 8월까지 Comcast의 네트워크에 Sandvine의 Policy Traffic Switch 모델 8210을 설치했다. DPI 분석은 Ares, BitTorrent, eDonkey, FastTrack, Gnutella의 P2P 프로토콜을 타깃으로 하였고, 각 P2P 프로토콜에서 발생하는 단방향 업로드 세션의 수를 측정하였다. 만약 그 세션의 수가 사업자가 정한 한계치에 도달하면 DPI 박스는 그 장비가 관리하는 지리적 구역의 이용자 트래픽 흐름을 방해하는 리셋 패킷을 발생시키는데, 가장 엄격한 제약은 BitTorrent에 적용되었다. Comcast의 DPI 실행은 P2P를 이용하는 고객들의 서비스에 제한적으로 적용되었는데, 이러한 방침의 변화는 고객들에게 고지 및 서비스 계약상의 변경없이 진행되었다.[25)]

이용자들은 2007년 중반부터 Comcast의 DPI 사용에 대한 불만을 제기하기 시작했고, 소프트웨어 테스터인 Robb Topolski가 Comcast의 DPI 사용에 대한 글을 블로그 및 전문 웹사이트에 게재하면서 본격적으로 이 사실이 알려지기 시작했다. 당시 미국에서 망 중립성에 대한 논의가 한창이던 시점이었고, 망 중립성 지지자들은 망 중립성 원칙 부재시의 위험에 대한 좋은 예로서 Comcast 사건에 주목하였다. 2007년 11월, 망 중립성 지지단체인 Free Press와 Public Knowledge 등은 FCC에 Comcast의 관행에 대해 고소를 하였다. 2주 후에 비슷한 청원이 P2P 소프트웨어를 통해 비디오 콘텐츠를 유통하는 공개 엔터테인먼트 플랫폼 개발 업체인 Vuze Inc.에서 제기되었다.

(2) FCC의 결정

Comcast의 행위의 합법성에 의문이 지속적으로 제기되자, FCC는 Free Press와 Vuze Inc.의 청원을 하나로 합친 내용을 바탕으로 공식적인 공공자문을 개시했다. 2007년 2월에서 7월에 걸친 공공자문 기간 동안 상당수가 DPI가 감시 용도로 사용될 위험성에 대한 지적을 하였다. FCC는 Comcast의 관행이 차별적이며, 합리적인 네트워크 관리가 아니라는 결론을 내렸다. 이와 함께 이용자들에게 관행에 대한 고지를

25) 이는 미국 통신법에 따라 케이블 모뎀 인터넷이 "정보서비스"로 분류되어, 기간사업자의 의무가 면제되고 있음에 따라 케이블 ISP인 Comcast가 일방적으로 DPI 이용을 할 수 있었다는 견해가 있다(Mueller & Asghari, 2012).

하지 않은 혐의가 있다고 판단하였다. FCC의 결정에 따라 Comcast는 P2P를 차단하는 기존의 방법을 중단하고, 프로토콜 중립적인 새로운 방법 개발 및 현재 사용중인 DPI 방법에 대한 기술적 상세내용을 공개하라는 명령을 받게 되었다.

(3) 추후 경과

FCC의 결정과 별개로 Comcast는 부정적 여론, 소송 및 규제적 조치 등이 쇄도함에 따라 2008년 8월 27일에 FCC에 자사의 P2P 차단 관행 변경에 대한 "자발적 협약"을 제출하였다. 결국 2008년 9월 19일 FCC에 등록된 Comcast의 새로운 대역폭 관리 방법은 더 이상 P2P 프로토콜을 차단하거나 저하시키는 것이 아니라 15분 간격으로 지리적으로 획정된 네트워크 부분의 혼잡 한계치를 체크하는 것이었다. 혼잡이 발생하면 애플리케이션에 관계없이 어떤 이용자가 가장 많이 혼잡에 기여하는지 식별하고 그 이용자의 패킷에 15분 동안 낮은 우선순위가 부여되도록 설계되었다. 새로운 방법은 DPI 장비를 통해 트래픽을 모니터링 하여 다량의 트래픽을 유발하는 이용자 식별에만 이용하고, 패킷의 콘텐츠는 검사하지 않는 것으로 변경되었다. 즉, DPI의 적용이 특정 프로토콜에 초점을 맞추던 것에서 프로토콜 중립적으로 변화된 것이다. 이와 함께 Comcast는 모든 가정용 고객에게 월 250GB의 데이터 상한을 부과하기로 하였다.

한편, 2009년 12월 Comcast는 FCC의 명령에 대해 사법부에 소송을 제기하였다. Comcast의 주장은 FCC의 명령이 1934년 통신법 또는 합법적인 고시에 근거하지 않았으며, 법적 구속력이 없는 FCC 가이드라인(2005년)의 4가지 원칙에 근거해서 이루어진 조치로 1934년 통신법에서 정한 FCC의 권한을 남용하였다는 것이다. 2010년 4월 연방항소심에서는 Comcast의 BitTorrent 차단금지를 명령한 FCC에 대해 그 규제 권한을 넘어섰다는 판결이 내려졌다. 그럼에도 불구하고 FCC 2010년 12월에 오픈 인터넷 규칙을 통과시킴으로써 투명성, 차단금지 및 합리적인 네트워크 관리를 인정하면서도 비합리적인 차별을 금지하는 것을 골자로 한 새로운 규칙을 제정하였다. 그러나 FCC의 오픈 인터넷 규칙은 망 중립성을 지지하는 편에서는 약한 규제라는 비난을 ISP쪽에서는 너무 강력한 규제라는 비난을 동시에 받고 있어 이와 관련한 소송이 이어지고 있다.[26)]

2. 캐나다 Bell Canada 사례

(1) Bell Canada의 P2P 속도 제한

캐나다의 네트워크 사업자들은 P2P 프로토콜을 타깃으로 DPI를 사용하고 있었으며, 사업자별로 그 구현 및 정책은 상이하였다. 케이블사업자인 Shaw Communications는 2005년부터 DPI를 사용하여 최번시에만 상향 P2P 트래픽을 제한했고, Cogeco와 Rogers는 2008년 7월부터 상시적으로 상향 P2P 트래픽의 속도를 저하시켰다. 반면 SaskTel, Telus 및 Videotron은 DPI를 사용하지 않고 이용자가 이용할 수 있는 데이터 상한을 설정하였으며, 그 외 다른 사업자들은 별도의 트래픽 관리를 하지 않고 네트워크 고도화에 의존하였다.

캐나다 최대 ISP인 Bell Canada는 2007년 10월부터 DPI를 사용해서 자사 소매 인터넷 포털 서비스인 Sympatico의 이용자들에 의한 P2P 프로토콜을 제어하기 시작했다. Bell은 제한적으로 오후 4시 30분부터 새벽 2시까지 모든 P2P 애플리케이션의 상향과 하향 속도를 낮추었다. 소매단에 이러한 DPI 정책을 적용하는 것에 대해서 어느 정도의 불만이 제기되긴 하였지만, 본격적인 문제로 부각된 것은 DPI가 도매서비스에로 확대 적용되면서 부터였다.

캐나다에서 Bell이나 Rogers와 같은 설비기반 대규모 ISP는 대역폭을 경쟁 ISP에 재판매해야 하며, 그 요금은 인가의 대상이다. Bell 입장에서 도·소매에 대해 DPI 정책을 어떻게 적용할 것인지는 일종의 딜레마였다. 즉, 소매단에서만 속도를 제한하고 도매를 그냥 놔두면 혼잡이 여전히 발생할 수 있으며, 이는 대역폭을 임대한 경쟁사의

---

26) 법적소송 Ⅰ(2011. 4): Verizon이 오픈 인터넷 규칙이 연방통신법에서 위임된 규제 권한을 위반한다며 소송을 제기하였으며, 법원은 오픈 인터넷 규칙이 백악관 심사 중이라는 이유로 이를 기각하였다.
법적소송 Ⅱ(2011. 9): Free Press라는 미국의 미디어 관련 시민단체가 FCC의 오픈 인터넷 규칙이 망 중립성을 보호하기에 부족하다며 2011년 9월 소송을 제기하였으나 2012년 7월 Free Press가 소송을 취하하였다.
법적소송 Ⅲ(2012. 7): 오픈 인터넷 규칙이 발효됨에 따라 Verizon이 다시 소송을 제기했으며 현재 진행중이다.

이용자들에게 Bell의 소매 이용자들보다 사실상 우선순위를 부여하는 결과를 가져왔다.[27] Bell의 경영진은 소매단에서만 DPI를 통한 P2P 속도 저하가 혼잡 문제를 제대로 해결하지 못한다고 판단하고, 2008년 3월말부터 도매 Gateway Access Service(GAS)에도 소매단과 같은 P2P 속도 제한을 적용하기 시작했다. 이러한 변화는 일방적으로 진행되었으며, 별도로 고지를 하거나 동의를 구하는 과정은 없었다.

DPI 기반의 속도제한이 도매 GAS에 적용된다는 것은 Bell의 설비를 이용하는 소규모 ISP도 Bell의 속도제한 정책을 따라야 함을 의미하는 것이었다. 즉 Bell의 가입자뿐만 아니라 경쟁 ISP의 가입자들도 영향을 받게 되면서 캐나다 소매 ISP들이 Bell의 DPI 사용에 대해 강력하게 저항하기 시작하였다. 이에 따라 캐나다 인터넷제공사업자연합(Canadian Association of Internet Providers, CAIP)은 Bell이 P2P 파일 공유로부터 발생되는 인터넷 트래픽의 속도제한을 중단하도록 요구하는 리포트를 캐나다방송통신위원회(Canadian Radio-television and Telecommunications Commission, CRTC)에 제출하였다. CAIP는 Bell이 GAS 요금에 트래픽 변경(shaping)에 대한 조항을 담고 있지 않으며, GAS 고객에게 일방적으로 트래픽 변경을 적용하는 것은 위원회에 사전 승인을 받지 않고 서비스의 약관을 수정한 것이라고 주장하였다.

당시 미국에서 Comcast 사건이 한창 진행 중이었고, BitTorrent의 이용이 범국가적으로 이뤄지고 있어 캐나다뿐만 아니라 미국 이용자들도 Bell의 사건에 많은 관심을 가졌다. 시민단체 및 CIPPIC(Canadian Internet Policy and Public Interest Clinic) 등의 참여가 이뤄짐에 따라 CAIP는 Bell의 대역폭을 임대한 사업자의 가입자와 Bell이 직접적인 계약관계가 없는데도, 이들의 트래픽까지 조사하는 것은 “불필요하고 합의되지 않은 개인정보를 수집 및 사용”한 것이므로 국내의 개인정보법을 위반하였음을 주장하며, 2008년 5월 개인정보위원회에 고소하였다.

(2) CRTC의 결정

Bell의 사건은 공유 대역폭 관할에 대한 적합한 규칙과 원칙이 무엇인지에 대한 복

27) 결과적으로 Bell의 이용자에게 속도제한을 통해 확보한 여분의 대역폭을 재판매용으로 전환시키는 것이기 때문이다.

잡한 논의를 불러왔다. Bell은 P2P 트래픽이 혼잡을 유발함으로써 다른 이용자들의 인터넷 서비스를 저하시킨다고 주장하였다. 그러나 CAIP 등은 Bell이 접근하는 혼잡에 대한 정의와 이를 측정하는 방법이 잘못되었다고 반박하며, P2P 애플리케이션이 다른 애플리케이션보다 많은 대역폭을 점유한다는 것을 부정하였다. CAIP는 Bell의 DPI가 SSH, VoIP 등의 P2P 프로토콜이 아닌 프로토콜에 대해서도 속도를 저하시키며, Bell의 일반적 약관을 네트워크 기반의 체계적인 트래픽 변경으로 인정할 수 없다고 보았다. 그들의 입장에서 혼잡에 대한 적절한 대응은 모든 P2P 프로토콜 속도 저하가 아닌 대역폭을 많이 점유하는 특정 서비스를 제한하거나 차단하는 것이어야 한다는 입장이었다.

2008년 11월, CRTC는 CAIP의 주장을 기각하며, 소송과정에서 제기된 거의 모든 이슈에 대해 Bell의 편을 들어줬다. 즉, CRTC는 Bell이 GAS 요금 약관을 위반하지 않았다고 보았는데 그 근거는 다음과 같다. 첫째, Bell의 트래픽 변경은 Bell에게 차별적인 경쟁 우위를 제공하지 않았으며, 둘째, Bell은 실질적으로 해결해야 할 혼잡 문제와 용량의 한계라는 이슈를 갖고 있었다는 것이다. 셋째, Bell의 DPI 사용이 전송되는 콘텐츠를 불법적으로 변경하지 않았으며, 넷째, DPI 사용 그 자체로 프라이버시권을 침해한 것은 아니라고 보았다. 단, Bell의 도매 고객들에게 DPI 적용에 대해서 사전 고지를 하지 않은 점에 대해서는 가벼운 경고를 받았다.

⑶ 추후 경과

그러나 이러한 결정이 모든 이슈를 해결한 것은 아니며, 오히려 트래픽 관리와 망 중립성에 대한 일반적인 정책을 어떻게 가져갈 것인가가 중요한 관심사항이 되었다. 이에 따라 2009년 10월 CRTC는 수용할 수 있는 인터넷 트래픽 관리 관행(Internet Traffic Management Practices) 프레임워크를 명료화하였다. CRTC는 캐나다 국민이 인터넷을 다양한 목적으로 이용할 수 있는 자유와 ISP가 프라이버시 법을 준수하면서 네트워크에서 발생하는 트래픽을 관리하고자 하는 합법적인 이해(interest)간의 균형을 추구하고 있으며, “투명성, 혁신, 명료성, 경쟁력 있는 중립성”이라는 네 가지 원칙을 제시하였다.

이와 함께 캐나다에서는 투명성과 이용자 선택권 관점에서 경제적 트래픽 관리가 효율적이라는 시각에 따라 도매시장에도 용량 기반 요금제가 도입되었다.[28] 이에 따라 도매시장에서 트래픽에 대한 경제적 관리가 가능해졌고, Bell 등은 P2P 트래픽에 대한 기술적 관리를 중지하였다.

3. 네덜란드 KPN 사례

(1) KPN의 DPI 이용 발표

2011년 4월 네덜란드의 KPN은 WhatsApp과 같은 무료 기반의 서비스가 유발하는 데이터 트래픽에 요금을 부과할 것이라고 결정에 따라, DPI를 통해 애플리케이션을 구분하겠다는 방안을 발표하였다. 당시 네덜란드 통신규제기관인 우편통신규제청(Onafhankelijke Post en Telecommunicatie Autoriteit, OPTA)과 EU 집행위원회는 요금 산정 방식이 투명하다면 문제가 되지 않는다며 긍정적인 반응을 보였다.[29] 그러나 이용자들은 KPN의 특정 서비스에 대한 차별적 요금부과에 대해 반발하였다. 또한 자신들이 사용하는 애플리케이션에 대해 ISP가 알게 되는 것에 불만을 표시하였다. 시민단체인 Bits of Freedom 및 Consumentenbond 등은 KPN이 DPI를 이용하는 과정에서 정보보호법을 위반하였다고 주장하며 규제기관의 조사를 촉구하였다.

(2) OPTA의 결정

OPTA와 네덜란드 정보보호국(College Bescherming Persoonsgegevens, CBP)은 KPN의 DPI 사용이 정보보호법을 위반했는지 여부에 대해 2011년 5월 조사에 착수

28) 도매시장과 달리 소매시장은 요금을 규제하고 있지 않아, 주요 ISP들이 소매요금에 데이터 상한을 설정하고 추가 과금을 하고 있다. 그러므로 소매시장에서 P2P 트래픽 등에 대한 기술적 관리 유인이 작다.

29) OPTA는 KPN의 새로운 요금제가 이용자가 자신의 필요에 따라 적합한 패키지 형태의 요금제를 선택할 수 있도록 함으로써 소비자의 선택권을 넓혔다고 언급했다. 한편 EU 집행위원회는 이통사가 특정 서비스를 차단하거나 속도를 제한하지 않는 한, 서비스 접속에 따라 차등화 된 요금제를 적용할 수 있다는 입장을 표명하였다.

했으며, 법무부는 6월에 조사를 개시하였다. 이에 대해 KPN은 DPI 기술을 이용해 왔다는 점은 인정하였으나, 그 과정에서 정보보호법을 위반하지 않았다고 주장하였다. 이러한 논란은 때마침 의회에서 네덜란드 통신법 개정에 대한 논의가 벌어진 시점과 겹치면서, 통신법 개정 과정에서 망 중립성 이슈도 고려 대상이 되었다. 2011년 6월 네덜란드 하원 통과 후 약 1여년 만인 2012년 5월 상원까지 통과하면서 네덜란드는 유럽에서 처음으로 망 중립성 법을 통과시킨 나라가 되었다.

⑶ 추후 경과

KPN, Vodafone, T-Mobile, Tele2를 대상으로 DPI를 어떻게 시행하고 있는지에 대해 간이 조사를 한 결과, 사업자들이 DPI를 시행하고 있음을 드러났다. 그러나 OPTA는 사업자들이 사진을 보거나 이메일을 읽는다는 정황이 없어, 현 단계에서 사업자들에 대해서 엄격한 감시 조치를 부과할 근거가 없다고 판단하였다. 그렇지만 사업자들의 분석 방법과 가공된 데이터들을 정당하고 적정한 방법으로 취급하는지는 명확하지 않기 때문에 CBP로 결과를 넘겨 심층 조사를 진행하고 있다. 시민단체인 Bits of Freedom이 조사결과 보고서의 공개를 OPTA에 요청하였지만, 사업자들이 보고서에 담긴 영업상 기밀 정보가 노출될 것을 우려하고 있으며, CBP에서 심층 조사가 진행 중이라는 이유로 OPTA는 공개를 거절한 바 있다.[30)]

Ⅴ. 결 론

다양한 특성을 지닌 애플리케이션 증가 및 데이터 트래픽의 폭증에 대응하여 ISP의 트래픽 관리에 대한 요구는 증가하고 있다. 뿐만 아니라 망 중립성 규제시에도 예외적으로 합리적 트래픽 관리를 인정하고 있는 경향은 트래픽 관리의 필요성이 부당한 것으로만 볼 수 없음을 의미한다. 그러나 트래픽 관리에 대한 어느 정도의 공감대가 형성되었다고 해서 이와 관련된 수단인 DPI에 대해서까지 논의가 충분히 진행된 것은

30) Telecompaper(2011. 8. 29)

아니다. 오히려, 인터넷 생태계를 둘러싼 규제적 환경이 다소 모호하고, 혼잡 및 보안의 필요성이 빠르게 증가하며, ISP들이 자신들의 네트워크 상에서 활동하는 콘텐츠에 대해서 어느 정도의 대가를 받길 원하는 한 DPI의 이용을 둘러싼 논란은 가중될 것으로 예상된다.

해외사례에서 살펴보았듯이, DPI를 둘러싼 분쟁의 원인은 유사하더라도 해결 방식은 다양하게 나타날 수 있다. 미국에서는 ISP의 DPI 사용을 둘러싼 이슈를 해결하기 위해서 망 중립성을 지지하는 차원에서 특정 애플리케이션에 대한 속도 제한 등은 규모가 매우 축소되거나 금지되는 등 ISP의 DPI 관행이 상당부분 영향을 받게 되는 식으로 결론이 났다. 반면에 캐나다에서는 ISP들이 DPI를 이용할 수 있도록 하되, 중립적이면서 비차별적으로 행하도록 중립적인(uncontested) 규제기관에 네트워크 관리 방법을 규제할 수 있는 권한이 부여되었다. 즉 미국은 규제기관이 개입을 통해 DPI 관행을 바꾼 반면에 캐나다는 DPI 이용 관행을 인정한 것으로 볼 수 있다. 이는 DPI에 대한 논의의 해결책에 일괄적으로 적용될 수 있는 만병통치약이 없음을 의미한다. 인터넷 트래픽 증가에 따라 일정 수준의 트래픽 관리는 불가피한 것으로 보인다. 이러한 인식을 바탕으로 향후 합리적 수준의 트래픽 관리(또는 DPI)가 어떻게 시장에 정착될 수 있을지에 대한 논의가 진전되기를 기대한다.

참고문헌

나성현 (2012), “통신망의 합리적 관리 및 이용에 관한 기준(안)”, 통신망의 합리적 관리·이용과 트래픽 관리의 투명성에 관한 토론회, 2012. 7. 13.

Allot Communications (2007). “Digging Deeper Into Deep Packet Inspection(DPI).”

Asghari, H., van Eeten, M., & Mueller, M. (2012). “Unraveling the Economic and Political Drivers of Deep Packet Inspection.” GigaNet 7th Annual Symposium. 2012. 11. 5.

Bendrath, R. (2009). “Global technology trends and national regulation: Explaining

Variation in the Governance of Deep Packet Inspection." International Studies Annual Convention. New York City. 2009. 2. 15~18.

BEREC (2012). "BEREC response to EC questionnaire on specific aspects of transparency, traffic management and switching in an Open Internet." BoR(12)145 rev.1. 2012. 12. 19.

Broadband Traffic Management (2013. 2. 14). "〔Transparency Market Research〕: DPI Market to Reach $3.8B by 2018."

Cooper, A. &, Llans, E. (2012). "Adoption of Traffic Sniffing Standard Fans WCIT Flames." Center for Democracy & Technology. 2012. 11. 28.

Cooper, A. (2010). "The Singular Challenges of ISP Use of Deep Packet Inspection." Deep Packet Insepction.ca.

_____ (2011). "Doing the DPI Dance." 2011. 4. 11.

Daly, A. (2010). "The legality of deep packet inspection." First Interdisciplinary Workship on Communications Policy and Regulation 'Communications and Competition Law and Policy-Challenges of the New Decade'. University of Glasgow. 2010. 6. 17.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L 281. 1995. 11. 23.

Milton, L. M. & Asghari, H. (2012). "Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States." Telecommunications Policy. Vol. 36. Issue 6. pp.452~475.

Mochalski, K. & Schulze, H. (2009). "Deep Packet Inspection, Technology, Applications & Net Neutrality." Ipoque.

Ou, G. (2009). "Understanding Deep Packet Inspection(DPI) Technology." Digital

Society.

Parsons, C. (2008). "DPI in perspective: tracing its lineage and surveillance potential." thenewtransparency surveillance and social sorting. Working paper.

Telecompaper (2011. 8. 29). "Opta rejects request for info on DPI investigation." http://www.telecompaper.com/news/opta-rejects-request-for-info-on-dpi-investigation--823541.

Wu, T. (2003). "Network Neutrality, Broadband Discrimination." Journal of Telecommunications and High Technology Law. Vol. 2. pp.141~179.

Zahariadis, Th. & Perdikeas, M. (2012). "Is Deep Packet Inspection violating the Network Neutrality." Position Paper. Project No: FP7-ICT-248036. COAST Consortium.