Open Net - Harvard Berkman Center Seminar on Intermediary Liability

정보매개자책임의 국제적 흐름

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

opennet.or.kr

T. 02-581-1643 E-mail. master@opennet.or.kr

정보매개자책임의 국제적 흐름

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

정보매개자책임의 국제적 흐름

Open Net-Harvard Berkman Center Seminar on Intermediary Liability

대한민국국회

일자 2015년 5월 28일 (목)

시간 09:30~18:00

장소 국회의원회관 제1소회의실

주최 국회의원 박주선, 염동열, 유승희 ※ 가나다 순

opennet | 국회입법조사처 NATIONAL ASSEMBLY RESEARCH SERVICE | BERKMAN CENTER FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

한국언론법학회 | KILA 사단법인 한국인터넷법학회 KOREA INTERNET LAW ASSOCIATION | 고려대학교 법학연구원 LEGAL RESEARCH INSTITUTE OF KOREA UNIVERSITY | 서울대학교 기술과 법 센터 Center for Law & Technology

후원 방송통신위원회 KOREA COMMUNICATIONS COMMISSION | 한국저작권위원회 KOREA COPYRIGHT COMMISSION

이용자 권리 보호와 ICT 산업 발전을 위한 플랫폼사업자의 책임원칙

정보매개자책임의 국제적 흐름

International Trends on Intermediary Liability

Designing Intermediary Liability Regime for Promotion of User Rights and ICT Industry

Session 2

Intermediary Liability and Digital Ecosystem

정보매개자 책임과
ICT 생태계

Main Speaker / 주제 발표

Anupam Chander
아누팜 챈더

▪ Professor of Law at UC Davis

Anupam Chander is Director of the California International Law Center and Professor of Law at the University of California, Davis, where he is a Martin Luther King, Jr. Hall Research Scholar. He has been a visiting professor at Yale Law School, the University of Chicago Law School, Stanford Law School, and Cornell Law School. He has published widely in the nation's leading law journals, including the Yale Law Journal, the NYU Law Journal, the University of Chicago Law Review, the Texas Law Review, and the California Law Review.

A graduate of Harvard College and Yale Law School, he clerked for Chief Judge Jon O. Newman of the Second Circuit Court of Appeals and Judge William A. Norris of the Ninth Circuit Court of Appeals. He practiced law in New York and Hong Kong with Cleary, Gottlieb, Steen & Hamilton.

Main Speaker / 주제 발표

Oliver Süme
올리버 쥬메

▪ EurolSPA President

Oliver J. Süme is President of EuroisPA, the worlds largest ISP Associaion, representing more than 2300 Internet Service Providers across the EU and EFTA Countries. He is also deputy chair of the board of the German Internet Industry Association (eco) since 2000. There, he oversees the activities of the Political and Legal Affairs Department, which includes responsibility for representing the political interests of the association and its over 800 member companies. Süme is also a trained lawyer and partner at the Hamburg–based law firm of Richter Süme, where he has worked since 1997, primarily as an advocate for companies in the Internet and IT sectors. Süme is a certified IT–Lawyer and member of the IT Law Committee of the Hanseatic Bar Association. He is co–founder and CEO of Hamburg Top–Level–Domain, the registry for the new Top–Level–Domain ".hamburg".

Moderator / 좌장

Kim, Jewan
김제완

▪ 1998	Ph.D. 박사	Graduate School of Law, Korea University 고려대학교 법과대학
▪ 1994	M.A. 석사	Graduate School of Law, Korea University 고려대학교 법과대학
▪ present	Professor 교수	Korea University Law School 고려대학교 법학전문대학원
▪ present	President 원장	Legal Research Institute, Korea University 고려대학교 법학연구원
▪ present	Member 위원	Bar Reform Committee, Ministry of Justice 법무부 변호사제도개선위원회 위원
▪ present	Member 자체평가위원	Fair Trade Commission 공정거래위원회
▪ present	Member 실행위원	PSPD Judicial Watch Center 참여연대 사법감시센터

Panelists / 토론자

Kim, Minjeong
김민정

▪ –	Ph.D. 박사	School of Journalism and Mass Communication, University of North Carolina 미국 노스캐롤라이나대학교 저널리즘&매스컴
▪ –	M.A. 석사	School of Journalism and Mass Communication, University of North Carolina 미국 노스캐롤라이나대학교 저널리즘&매스컴
▪ –	M.A. 석사	Dept. of Mass Communication, Hankuk University of Foreign Studies 한국외국어대학교 신문방송학과
▪ Present	Associate Professor 부교수	Division of Media and Communication, Hankuk University of Foreign Studies 한국외국어대학교 사회과학대학 미디어커뮤니케이션학부
▪ Present	Director of Research 연구이사	Korean Society for Media Law, Ethics and Policy Research 한국언론법학회
▪ 2012 ~ 2013	Associate Professor 부교수	Colorado State University 미국 콜로라도 주립대학교

Panelists / 토론자

Lee, Inho
이인호

▪ –	Ph.D. 박사	Graduate School of Law, Chung-Ang University 중앙대학교 대학원 법학
▪ Present	Professor 교수	Chung-Ang University Law School 중앙대학교 법학전문대학원
▪ Present	Co-President 공동회장	Korea Association For Informedia Law 한국정보법학회
▪ Present	Commissioner 위원(비상임)	Central Administrative Appeals Commission 중앙행정심판위원회
▪ Present	Member 위원	Legislation Support Committee of the National Assembly Secretariat 국회사무처 입법지원위원회
▪ Present	Vice President 부회장	Korean Society for Media Law, Ethics and Policy Research 한국언론법학회

Panelists / 토론자

Yoon, Jongsoo
윤종수

▪ 1989	M.A. 석사	Graduate School of Law, University of Seoul 서울시립대학교 법과대학
▪ Present	Partner 파트너 변호사	Shin&Kim 법무법인 세종
▪ Present	Chairperson 위원장	Advisory Board for Development of Internet Search Service 인터넷 검색 서비스 발전을 위한 자문위원회
▪ Present	Vice President 부회장	Korea Association For Informedia Law 한국정보법학회
▪ Present	Member 위원	Korea Copyright Commission 한국저작권위원회
▪ present	Board Member 이사	Creative Commons 크리에이티브 커먼스

Main Speaker / 주제발표

The "Electronic Silk Road" and Intermediary Liability

Prof. **Anupam Chander**
(UC Davis School of Law)

"e-실크로드"와
정보매개자 책임

아누팜 챈더 교수 (미 UC데이비스 로스쿨)

The Electronic Silk Road and Information Intermediaries

Nearly every company set up in a garage in Silicon Valley hopes to take over the world. There is reason for such optimism. Again and again, Silicon Valley firms have become the world's leading providers of Internet services. How did Silicon Valley become the world's leading supplier of Internet services?

Popular explanations for Silicon Valley's recent success revolve around two features. First, Silicon Valley bestrides the great academic centers of Stanford University and the University of California, Berkeley, and sits near the artistic and intellectual hub of San Francisco. Second, the center of venture capital in the United States also happens to be in Menlo Park, California, allowing both industries to profit from each other in a symbiotic relationship. But education and money coincide in other parts of the United States as well. Why did those parts not prosper in the manner of Silicon Valley? More fundamentally, did not the Internet make geography irrelevant? Scholars answer that Silicon Valley's advantage lies in the economies of agglomeration. Ronald Gilson argued that California's advantage was its labor law, which he believes encourages "knowledge spillovers" and agglomeration economies by facilitating employee mobility. While these standard accounts do much to explain the dynamism of Silicon Valley relative to other parts of the United States, they do not explain the relative absence of such Internet innovation hubs outside the United States, or the success of Silicon Valley enterprises across the world.

Law played a far more significant role in Silicon Valley's rise and its global success than has been previously understood. It enabled the rise of Silicon Valley while simultaneously disabling the rise of competitors across the world. In this Article, I will argue that Silicon Valley's success in the Internet era has been due to key substantive reforms to American copyright and tort law that dramatically reduced the risks faced by Silicon Valley's new breed of global traders. Specifically, legal innovations in the 1990s that reduced liability concerns for Internet intermediaries, coupled with low privacy protections, created a legal ecosystem that proved fertile for the new enterprises of what came to be known as Web 2.0. I will argue that this solicitude was not accidental—but rather a kind of cobbled industrial policy favoring Internet entrepreneurs. In a companion paper, Uyên Lê and I show that these aspects of copyright and tort law were not driven by commercial considerations alone, but were undergirded in large part by a constitutional commitment to free speech. As we argue there, a First Amendment–infused legal culture that prizes speech offered an ideal environment in which to build the speech platforms that make up Web 2.0.

I will compare the legal regimes not between Silicon Valley and Boston's Route 128, but between the United States and key technological competitors across the globe. The indulgence of American law for Internet enterprise appears in sharper relief when contrasted with the legal regimes faced by web entrepreneurs elsewhere. In Europe, concerns about copyright violations and strict privacy protections hobbled Internet startups. Asian web enterprises faced not only copyright and privacy constraints, but also strict intermediary liability rules. I will contrast the leading cyberlaw statutes and cases in the United States, with their explicit embrace of commerce and speech, with those from Europe and Asia, which are more attendant to the risks of this new medium for existing interests. I will show that Google and Yahoo were so worried that Japanese copyright law would make search engines illegal that they placed their search servers offshore. A Japanese computer science professor advised his students to publish their software outside Japan. British Prime Minister David Cameron suggested that Google's search engine might have been illegal under English copyright law.

This Article upends the conventional wisdom, which sees strong intellectual property protections as the key to innovation—what the World Intellectual Property Organization calls a "power tool" for growth. Understanding the reasons for Silicon Valley's global success is of more than historical interest. Governments across the world, from Chile to Kenya to Russia, seek to incubate the next Silicon Valley. My review suggests that overly rigid intellectual property laws can prove a major hurdle to Internet innovations, which rely fundamentally on empowering individuals to share with each other. This study helps make clear what is at stake in debates over new laws such as the Stop Online Piracy Act (SOPA) and its relatives, highlighting the effect of these laws on Silicon Valley's capacity for innovation. I show that government has the power to enable, or disable, a new industry. The power to make in this case implies the power to break.

Innovation scholars worry about the "valley of death," the stage between start-up idea and successful commercialization, in which most start-up enterprises founder. Cyber scholars fond of citing Joseph Schumpeter's "creative destruction" need to attend to his focus as well on the finance needed by innovators.

Imagine the boardroom in a Silicon Valley venture capital firm, circa 2005. A start-up less than a year old has already attracted millions of users. Now that start-up, which is bleeding money, needs an infusion of cash to survive and scale up. The start-up lets people share text, photos, and videos, and includes the ability to readily share text, pictures, and videos posted by one's friends. If that start-up can be accused of abetting copyright infringement on a massive scale, or must police its content like a traditional publishing house lest it face damages claims or an injunction, your hundred-million-dollar investment might simply vanish to plaintiffs' lawyers in damages and fees. An injunction might stop the site from continuing without extensive human monitoring that could not be justified by potential revenues. Because of the insulation brought by U.S. law reforms in the 1990s, American start-ups did not fear a mortal legal blow. The legal privileges granted to Internet enterprises in the United States helped start-ups bridge the valley of death.

Let me anticipate criticism. First, legal realists might object that I have spoken about law on the books. What about law in action? I demonstrate through actual cases the practical importance of the liberal American law and the strict European and Asian laws. Second, some might seek to trivialize my thesis: law always matters to the success of an enterprise because it could have made that enterprise illegal, but did not. That is not my claim; rather, my claim is that U.S. authorities (but not those in other technologically advanced states) acted with deliberation to encourage new Internet enterprises by both reducing the legal risks they faced and largely refraining from regulating the new risks they introduced. Third, some will insist that if law was relevant, it was only because it got out of the way. After all, the last person hired at a Silicon Valley start-up is the lawyer. I show that the story of Silicon Valley is not only a story of brilliant programmers in their garages, but also a legal environment specifically shaped to accommodate their creations.

My claim may resonate with students of American legal history. Morton Horwitz famously argued that nineteenth-century American courts modified liability rules to favor the coming of industrialization. I suggest an even more widespread effort, with the Executive, Congress, and the Courts, each in their own way promoting Internet enterprise. Horwitz decried the nineteenth-century's laws' implicit subsidy to industrialists, which he saw as being borne on the backs of society's least fortunate. The limitations on Internet intermediary liability and the lack of omnibus privacy protections beyond those that are promised contractually by websites mean that there is a price to be paid for the amazing innovation of the past two decades. Even while we celebrate innovation, we must recognize its costs.

But the benefits have been enormous, not only in the economic impact of the information that is being shared, but also in the radical democratization of the freedom of speech.

In the United States, Congress and the courts recognized that broad liabilities on Internet intermediaries would impinge on the speech of ordinary persons. Free speech depends on a free press. Today, Internet intermediaries are increasingly replacing the press of old, just as radio and television replaced print in earlier eras. Where early interpretations of the First Amendment had focused on direct governmental regulation, beginning with New York Times v. Sullivan, the U.S. Supreme Court recognized that speech could be burdened indirectly, by delegating the right to sanction speech to private parties.

When it comes to speech, Internet intermediaries are likely to be ensnared, caught in the middle of the worldwide war fueled by copyright interests, users' privacy, and governments' desire to control what is said and to listen in on what people are saying. Internet intermediaries are often the most vulnerable and effective points of control for any government keen on controlling speech.

The First Amendment reveals itself as the industrial policy for an information age. In an information age, free speech greases the economic engine. By revealing the free speech foundations of American cyberlaw, I hope to encourage other countries around the world eager to incubate the next Silicon Valley to embrace free speech. Governments from Brazil to India to Russia to South Korea, seeking to incubate their own Silicon Valleys, must recognize the vital role that free speech plays in enabling Internet enterprise.

e-실크로드와 정보매개자

실리콘 밸리의 차고에서 시작하는 대부분의 회사들은 세계 정복을 꿈꾼다. 이러한 낙관론에는 이유가 있다. 실리콘밸리 기업들이 계속해서 세계 유수의 인터넷 서비스 제공업체로 자리매김하고 있기 때문이다. 그렇다면 실리콘밸리는 어떻게 세계적인 인터넷 서비스 제공지가 되었는가?

실리콘밸리의 최근 성공 비결에는 두 가지 요소가 있다는 것이 일반적인 견해이다. 첫째, 스텐포드대학교와 캘리포니아대학교 버클리캠퍼스라는 위대한 학문의 전당 사이에 위치한 실리콘밸리는 샌프란시스코의 예술과 지식의 허브 인근에 자리하고 있다는 점이다. 둘째, 미국 벤처금융 중심이 캘리포니아 멘로공원(Menlo Park)에 있기 때문에, 실리콘밸리와 벤처금융은 공생관계를 통해 상호 이익을 거둘 수 있다. 하지만 교육과 자금이라는 요소는 미국 다른 지역에서도 공존하고 있는데, 왜 이러한 지역들은 실리콘밸리와 같은 방식으로 번영하지 않는 것일까? 보다 근본적인 질문은 인터넷으로 인해 지역적인 요소는 무의미해지지 않았는가? 학자들은 실리콘밸리의 장점은 집합 경제학에 있다고 답한다. Ronald Gilson은 캘리포니아의 장점은 노동법으로 종업원들의 이동을 조장함으로써 집합 경제와 "지식의 전이(knowledge spillover)"를 촉진한다고 주장했다. 이 같은 일반적인 설명은 미국내 타 지역 대비 실리콘밸리의 역동성을 잘 설명해 주지만, 이러한 인터넷 혁신이 타국에서 찾아보기 힘들다는 점이나 실리콘밸리 기업들이 거둔 세계적인 성공을 설명해주기에는 부족하다.

실리콘밸리의 부상과 세계적인 성공에 있어 법은 지금까지의 인식보다 훨씬 더 중요한 역할을 했다. 법은 실리콘밸리의 부상을 가능하게 했을 뿐 아니라 동시에 세계적으로 경쟁자들의 부상을 막기도 했다. 본 논문에서 인터넷 시대에 실리콘밸리의 성공은 미국의 저작권

불법행위법(copyright and tort law)에 대한 주요 개혁에서 기인하며, 이러한 개혁으로 인해 실리콘밸리의 신생 국제 무역업체들이 직면할 수 있는 위험부담이 극적으로 줄어들었다고 필자는 주장한다. 보다 구체적으로, 낮은 수준의 개인정보 보호 정책들과 아울러 인터넷 정보매개자들의 법적 책임 우려를 낮춘 1990년대 법적 혁신을 통해 웹2.0으로 알려진 신생 기업들에게 비옥한 토대를 제공한 법적 생태계를 마련한 것이다. 이 같은 배려들은 우연의 산물이 아니라 인터넷 기업들을 위해 마련된 산업정책이었음을 본 논문에서 밝히고자 한다. 다른 논문에서 필자와 Uyên Lê는 이러한 저작권 불법행위법의 이러한 측면들이 상업적인 고려사항만으로 추진된 것이 아니라 주로 표현의 자유에 대한 헌법적 약속에 의해 뒷받침되었음을 제시했다. 해당 논문에서 주장한 바와 같이 수정 제1조는 표현의 자유를 소중하게 여기는 법적 문화를 조성했고, 웹2.0을 구성하는 표현의 기반이 구축될 수 있는 이상적인 환경을 제공했다.

본 논문에서는 실리콘밸리와 보스턴의 128번 도로가 사이가 아니라 미국과 세계적인 주요 기술 경쟁자들간의 법적 체제를 비교하고자 한다. 인터넷 기업을 위한 미국법의 관대함은 다른 나라에서 인터넷 기업들이 직면하고 있는 법적 체제와 대조될 때 보다 뚜렷이 부각된다. 유럽에서 저작권 위반에 대한 우려와 엄격한 개인정보 보호 정책들은 신생 인터넷 기업에게 장애물로 작용했다. 아시아의 온라인 기업들은 저작권과 개인정보 제약뿐 아니라 엄격한 매개자 책임 규정에 직면했다. 본 논문에서 미국과 유럽의 대표적인 사이버 법령과 사례들을 대조해볼 예정인데, 미국은 상업과 표현의 자유를 공개적으로 반영한 반면, 유럽은 기존의 이익을 보호하기 새로운 인터넷이라는 매체의 위험에 보다 집중했다. 구글과 야후가 일본 저작권법이 검색엔진을 불법화할 것이라고 우려한 나머지 검색 서버를 해외에 두기로 결정한 사례도 제시할 것이다. 한 일본 컴퓨터공학과 교수는 제자들에게 소프트웨어를 일본이 아닌 타국에서 출시하라고 조언하기도 했다. 데이비드 캐머론 영국 총리는 구글 검색엔진이 영국저작권법에 따르면 불법이었을 것이라고 주장했다.

본 논문은 세계지적재산권기구(WIPO)가 성장의 "강력한 도구"라고 부르는 강력한 지적재산권 보호를 혁신의 핵심으로 간주하는 기존의 통념을 뒤집는다. 실리콘밸리의 세계적인 성공 원인을 이해하는 것은 역사적 차원을 넘어서는 일이다. 칠레에서 케냐, 러시아에 이르기까지 세계 모든 정부는 제2의 실리콘밸리를 만들고자 한다. 필자는 과도하게 엄격한 지재권법이 인터넷 혁신에 주요한 장애가 될 수 있다고 주장하는데, 인터넷의 혁신은 근본적으로

개인들이 서로 정보를 공유하도록 권한을 주는데 기반하고 있기 때문이다. 본 연구는 '온라인 저작권 침해 금지 법안(SOPA)'와 관련 법안 등 신규 법률에 관한 논쟁에 걸린 문제들을 명확히 파악하는데 도움이 되며, 이러한 법들이 실리콘밸리의 혁신 역량에 미치는 영향을 중점적으로 분석하고자 한다. 정부가 신규 산업의 성패를 결정할 수 있는 능력이 있다는 사실도 본 논문에서 제시될 예정이다. 여기에서 성공하게 만드는 능력은 곧 실패하게 만드는 능력인 것이다.

혁신 학자들은 창업 아이디어와 성공적인 상업화 중간 단계인 "죽음의 계곡(valley of death)"에 대해 우려를 표명하는데, 대부분의 스타트업 창업자들이 여기에 위치해있다. Joseph Schumpeter의 "창의적 파괴"를 즐겨 인용하는 사이버 학자들은 혁신가들이 필요한 자금뿐 아니라 Schumpeter의 핵심 주장에도 주의를 기울일 필요가 있다.

2005년경 실리콘 밸리의 한 벤처금융 기업의 이사회실을 상상해 보자. 설립된 지 채 1년이 되지 않은 이 스타트업은 이미 수백만 명의 사용자들을 모았다. 현재 적자상태인 이 기업은 생존과 확장을 위해 현금 수혈이 필요하다. 이 기업은 사용자들이 문자, 사진, 영상을 올리고 친구들이 올린 문자, 사진, 영상도 즉시 공유할 수 있는 기능을 제공한다. 만약 이 회사가 대규모 저작권 침해를 방조한다는 혐의로 고소되거나 손해배상이나 명령을 받지 않기 위해 기존 출판사처럼 컨텐츠를 감시해야 한다면, 수억 달러의 투자금이 원고측 변호사의 손해배상액과 수수료로 사라질 수 있다. 법원 명령을 통해 해당 사이트는 잠재적인 수입으로는 감당하기 어려운 수준의 대규모 인적 모니터링 없이는 운영을 중단해야 할 수도 있다. 1990년대 미국법 개혁으로 인한 법적 보호로 인해 미국 스타트업들은 치명적인 법적 처벌을 두려워하지 않게 되었다. 미국 인터넷 기업들에 부여된 법적 특권은 스타트업들이 이 죽음의 계곡을 건널 수 있도록 도왔다.

이 같은 주장에 대해 다음과 같은 비판이 제기될 수 있다. 첫째, 법적 현실주의자들은 필자가 교과서상의 법에 대해 말하고 있다고 반론을 펼칠 수 있을 것이다. 그렇다면 실제 실행되고 있는 법은 어떠한가? 본 논문에서는 실제 사례를 통해 자유로운 미국법과 엄격한 유럽 및 아시아 법들의 실용적인 중요성을 제시하고자 한다. 둘째, 법은 기업을 불법화할 수 있기 때문에 기업의 성공에 있어 항상 중요하지만 실제로 불법화지 않았다는 필자의 이론을 일축하고자 할 수 있다. 이는 필자의 주장이 아니다. 오히려 미 당국(다른 기술적으로

앞선 국가들의 당국이 아닌)은 신생 인터넷 기업들이 직면했던 법적 위험을 낮추고 이들이 가져오는 새로운 위험을 규제하지 않음으로써 이러한 기업들을 장려하기 위한 의도적인 행동을 취했다는 것이 필자의 주장이다. 셋째, 만약 법적인 연관성이 있다면 이는 법이 단지 방해하지 않았기 때문이라고 주장할 수도 있다. 결국 실리콘밸리의 스타트업은 변호사를 절대 고용하지 않을 것이다. 실리콘밸리의 이야기는 차고에서 일하는 뛰어난 프로그래머들의 이야기일 뿐 아니라 이들의 창업에 부응하도록 특별히 고안된 법적 환경에 관한 이야기임을 본 논문에서 제시하고자 한다.

필자의 주장은 미국법 역사 학도의 공감을 얻을 수 있을 것이다. Morton Horwitz 는 잘 알려진 바와 같이 19세기 미국 법원이 산업화 도래에 우호적인 방향으로 법적 책임 규정을 수정했다고 주장했다. 필자는 행정부, 의회, 법정이 각각의 방식을 통해 인터넷 기업을 촉진하기 위해 보다 방대한 노력을 기울였다고 주장한다. Horwitz는 19세기 법이 경영주들에게 은밀히 보조금을 제공했다고 주장했는데 이는 사회에서 가장 불운한 사람들을 등에 업고 탄생한 제도라고 그는 생각했다. 인터넷 정보매개자들의 책임에 대한 제한과 웹사이트가 계약을 통해 약속한 수준을 넘어선 일괄적인 개인정보 보호의 부재는 지난 20년간의 놀라운 혁신에 대해 지불해야 할 가격이 있다는 것을 의미한다. 혁신을 축하할 때에도 이 비용은 인정되어야 한다.

하지만 공유되는 정보의 경제적 효과뿐 아니라 표현의 자유의 급진적인 보편화가 가져온 혜택은 막대했다.

미국에서 의회와 법정은 인터넷 정보매개자에 대한 광범위한 법적 책임이 일반인들의 표현의 자유를 침해할 수 있다고 인정했다. 표현의 자유는 언론의 자유에 달려있다. 과거 라디오와 TV가 인쇄매체를 대체했듯이 오늘날 인터넷 정보매개자들은 갈수록 기존 언론을 대체하고 있다. 수정 제1조의 초창기 해석은 New York Times v. Sullivan사건을 비롯해 직접적인 정부 규제에 초점을 뒀지만, 미대법원은 언론을 제재할 권리를 민간 당사자들에게 이양하게 되면 표현의 자유에 간접적으로 부담을 줄 수 있다고 인정했다.

표현의 자유에 있어 인터넷 정보매개자들은 저작권 이해, 사용자 개인정보, 여론을 통제하고 파악하고자 하는 정부의 바램에 의해 펼쳐지는 세계적인 전쟁 한가운데서 사면초가 상황에 빠질 수 있다. 인터넷 정보매개자들은 언론을 통제하고자 하는 정부에 있어 가장 손쉽고 효과적인 통제 포인트이다.

수정 제1조는 정보화 시대를 위한 상업 정책이라는 점이 자명하다. 정보화 시대에 표현의 자유는 경제라는 엔진의 윤활유 역할을 한다. 미국 사이버법의 표현의 자유라는 토대를 제시함으로써 필자는 제2의 실리콘밸리의 주인공이 되고자 열망하는 세계 다른 국가들이 표현의 자유를 포용하도록 장려하기를 희망한다. 브라질에서 인도, 러시아, 한국에 이르기까지 제2의 실리콘밸리를 만들고자 하는 정부들은 표현의 자유가 인터넷 기업을 장려함에 있어 수행하는 핵심 역할을 수행한다고 인정해야 할 것이다.

Main Speaker / 주제발표

E-Commerce Directive and Experience of European ISPs

Mr. **Oliver Süme**
(President, EuroISPA)

EU 전자상거래지침과
유럽 ISP의 경험

올리버 쥬메 회장 (유럽ISP협회)

Intermediary Liability in Europe : The Electronic-Commerce-Directive

1. Article 14: “Actual Knowledge”

The “actual knowledge” requirement has proven to be a cornerstone of the safer-harbor regime for both caching and hosting providers. The general wording introduced in the Directive was elaborated on purpose to ensure that the decision on the legality of a given piece of content would only be taken by a court or an administrative authority with trained personnel able to make balanced assessments. This approach proved to be useful in the prevention of active monitoring of allegedly illegal activities in compliance with the “no general monitoring obligation” in Article 15.

However, the lack of a specific definition of “actual knowledge” gave rise to interpretative problems at national level concerning the exact conditions under which a service provider was effectively acquiring such knowledge. In some cases, it is unclear if the intermediary acquires actual knowledge when a user is simply making a complaint or flagging a content deemed inappropriate, as opposed to a court order or decision establishing that a piece of content is effectively illegal.

In this context several questions arise:

- What kind of information is necessary in order to provide actual knowledge to the intermediary?
- How detailed must this information be?
- Can this information be provided by any third party or is it necessary that it is provided by the affected party?
- Concerning the actual knowledge about the illegality of content, does the intermediary need to carry out a legal analysis or must such illegality be apparent for everyone?

In order to cope with such concerns and minimize the risks related to hypothesis of ignorance, purposefully disinformation or inadvertency, the provider has been generally deemed having actual knowledge of the illegal deeds once a competent authority has declared the content illegal and has ordered its withdrawal, limitation to its access or declared the existence of damages, and the service provider knew about such decision.

Similar objective facts have been established, for example, by a detailed notice from a copyright owner. This, sometimes, requires service providers to address complex issues, such as whether particular acts that have been notified, such as terrorism or hate speeches allegations, are illegal or not, whether a product has been "put on the market" in the EU, is second-hand, is a tester, etc.

Actual knowledge, therefore, needs to be linked to a notification which fulfills certain minimum requirements such as:

- the notification should be in writing;
- the complainant should provide adequate identification of the specific item of content alleged to be infringing (a general description of the type of content, that requires the intermediary to investigate to discover which particular items match that description, is not sufficient);
- the notification should be sent to an e-mail address reserved for this purpose by the service provider;

- it should clearly specify which information or activity the complaint relates to;
- it should provide evidence that the complainant possesses the rights which he claims to be violated;
- it should include an assertion that the publisher or person making the work available is infringing their rights and does not have a lawful basis for publishing the work or making it available (whether by means of a license or by operation of law);
- it should include details of the unlawful nature of the activity or information in question;
- it should contain an assertion of truthfulness and accuracy of the above and include an admission of liability for action taken in reliance on the same.

It is noteworthy an Italian recent case where an ISP had "actual knowledge" from a third party warning alleging infringement of copyright by the ISP's users, through a notification meeting the above minimum requirements.

The Court stated that the ISP only obligation was to foreword to the competent authorities (i.e. Public Prosecutor's office and Ministry of Communications) all the information relating to the alleged infringements of copyright contained into the warning (order of Tribunal of Rome no. 415 of 2010).

2. Voluntary industry agreements

The above does not prejudice procedures of detection and content removal that service providers might implement under voluntary agreements and other means of actual knowledge that may be established. Such procedures are voluntary mechanisms for cooperation set forth in the ECD, through which the interested party can report the existence of an alleged illegal activity to an ISP with a view to the ISP reviewing the purportedly content and, as the case may be, assessing the advisability of removing or disabling access to it.

However, EuroISPA believes that there are a number of requirements and conditions that must be considered when setting up voluntary industry agreements.

The aim should also be to reinforce legal certainty for ISPs and their liability limitations, and create the context for a true collaboration with parties to the agreement. In principle Articles 12 – 15 should not be affected by voluntary industry agreements. In particular it must be excluded that any voluntary agreements give rise to a presumption of actual knowledge that would expose the service provider to liability.

3. Article 14: "Expeditiously"

Service providers must expeditiously remove, or block access to, information once they are aware of their illegal nature. The Directive does not define this requirement and leaves to Member States to "[establish] specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information" (Recital 46).

Generally speaking, the term "expeditious" offers the necessary flexibility for case-by-case assessments. It cannot be laid down without the individual circumstances of the particular case.

If the expeditious action of a provider is due when the notice is coming from a court, a different assessment should be done in case of voluntary mechanisms. Indeed, while in the former case the intermediary has legal certainty, in the latter it could be required to act as soon as it is put on notice regardless of whether it has all the elements and the level of certainty needed to make a decision about the illegality of the content to be removed or disabled. Calling for expeditious removal in these cases, could result in the disabling access to sites or content that are not illegal, with far reaching consequences for the person unduly affected.

4. Article 14: notice and take-down

The notification procedure of allegedly illegal material for hosting providers in Article 14 ECD does not clearly define the mechanism to adopt in order to establish "actual knowledge" or "awareness of facts or circumstances". As consequence, diverging approaches have been adopted across Member States which could be gathered in the following categories:

a A formal, official notification by a competent judicial authority (notice and take down): this option ensures the actual knowledge and provide legal certainty for intermediaries.

b Simple notification determining actual knowledge: several shortcomings can be easily identified with the fact that the notice could come from official as well as unofficial sources; the burden of proving the illegality would stay with the provider (i.e. obvious crime vs complex query); the risk of such a system is to have the notice and take down applied consistently by the intermediary on all notifications and without proper legal assessment in order to escape liability. As mentioned above, it is of key importance to clarify and define minimum requirements as to when a provider has "actual knowledge" to reduce legal uncertainties for all parties involved. The UK law has laid down requirements similar to those listed under Question 53.

c Statutory requirements: some countries do not provide a formal or simple notification procedure but set specific requirements to be observed by courts (i.e. location of the information, nature, contact details of the sender, etc.).

EuroISPA believes that the establishment of notice and stay down or notice and notice procedures should be evaluated comprehensively. We have reservations that the establishment of these procedures will have additional value. In principle, disputes should be solved directly between the parties concerned. ISPs, in their role of intermediaries, are an uninvolved third party. EuroISPA questions the practicability

of these procedures that could lead to legal uncertainty and impose obligations that will undermine the established liability regime. Moreover, it must be safeguarded and ensured that ISPs, in their role of intermediaries, do not become judges of the illegality of content.

4-1. Notice and notice

EuroISPA believes that an additional notification procedure maybe an option that could resolve disputes amicably and put the liability where it should lie, i.e. in the hands of parties disagreeing on the legality of a given piece of content. Such a system could come into consideration exclusively for hosting providers and limited to the forwarding of a notification. Privacy laws and the secrecy of telecommunications should be respected, and fundamental freedoms must be strictly adhered to.

Furthermore, it has to be taken into account that any notification procedure, like the notice and notice, is based on the general assumption that:

- intermediaries are exempted from liability;
- the general no-monitoring obligation is preserved;
- a penalty against a claimant that files a wrongful notice is introduced.

4-2. Notice and stay down

EuroISPA believes that such a system raises legal uncertainty, turns ISP in judges of the illegality of the content and imposes ongoing filtering or monitoring on users' communications while completely by-passing the judge intervention.

Such filtering or monitoring methods are not only costly to implement and present a risk for users' fundamental rights, but they also have no proven effectiveness.

In practice, "notice and stay down" is incompatible with the principle in Article 15, "no duty to monitor" as in order to discharge a requirement that certain material stay down a hosting provider would have to constantly monitor their service for the reappearance of the notified material. Moreover, unless the notification was extremely narrowly construed to refer to exact digital copies of the same file, notice and stay down would be impossible to implement (for example, a notice demanding the removal and continued suppression of libelous content could not be considered to cover a repetition of the same libelous assertion in different words).

5. Filtering measures

The discussions on filtering should in no case be limited to technical feasibility and the preliminary question one may expect from the European Commission is whether it is desirable, in line with Europe's values and economic interest, to even consider filtering methods. Such methods are difficult to be efficiently implemented in a resilient environment like the Internet that was designed to avoid barriers and blocks and find alternative ways to deliver information. This is particularly true in situations where the telecommunications providers' role is only a "mere conduit" of real-time transmissions, for example in peer-to-peer networks. The impracticability

of such measures is grounded on several reasons:

Form a technological point of view: an effective filtering is not possible. Easy to circumvent, all content is affected (particularly legal content). There are an impact and adverse effects on the network resilience, security and efficiency of the infrastructure. All content has to be transported/checked by a centralized filtering infrastructure in the ISP network. The risk is high for a general monitoring of content/users to have collateral damages such as hypothesis of over-blocking.

From a broader perspective:

- Filtering measures bring with obvious implications with regard to the violation of fundamental freedoms;
- not for-profit providers cannot be expected to put in place filtering technologies;
- the needed economic investments in infrastructures and personnel are burdensome for providers and would significantly and durably impact the development of the European Information Society in a negative way. It also exists a risk of "mission creep", i.e. start addressing a specific issue and then enlarge the monitoring to other issues as well;
- it exists a risk of "technology creep", i.e. the need to constantly up-to-date the filter in accordance to the technological evolution of the Internet communications (ex: encryption). Filtering leads to the development of encrypted protocols and never ending investments to catch up with illegitimate uses and services (as oppose to deal with the problem at its source), resulting in costly and ineffective measures.

Additionally, if an Internet access provider has to actively roll out a filtering technology with regard to (part of) the data transmitted on its network, it could be argued that it would have the unintended consequence of neutralising the application of Article 12 of the Directive which exempts the access provider from any liability regarding the information transmitted via its network on condition that it does not select or modify the information contained in the transmission. However, if one considers that filters do not imply the selection of the information contained in the

transmission as they consist of “mere technical instruments”, then the liability exemption would be lifted with the consequence that the provider risks to be held liable for the malfunctioning of the filtering technology on its network causing, for instance, illegal content not being intercepted. In other words, the ISP characterization as “mere conduit” could be jeopardized with serious consequences for the provider, its customers and the respect of Fundamental Rights.

As established in the context of the Belgian Scarlet-SABAM case, where the technical solution “Audible Magic” was proposed as a possible filter for peer-to-peer traffic, the Belgian court acknowledged that it well might not be effective or scalable. Indeed, it seems impossible that a technology could make a waterproof distinction on the basis of the legal/illegal nature of the communication or even the identification of what is in a file. Indeed, this depends on specific considerations not directly related to the filter technology but, for instance, to the authorization or concrete license terms granted by the author or the collecting society and on the possible interference of statutory exceptions to copyright.

6. Proportionality

As mentioned, there is considerable doubt as to whether existing network filtering technologies would be effective in achieving their stated goal, particularly as users can be expected to use relatively simple encryption techniques to remain “one step ahead” of the technology. Encryption of peer-to-peer traffic is already happening at an increasing rate; filtering measures are likely to serve only to encourage universal adoption of encryption to avoid detection. At the same time, filtering can be expected to result in a risk of degradation of network services, of user experience and in the inadvertent blocking of access to legitimate content. Additionally, the increased costs such technology bring with would contribute creating a further barrier to address the digital divide.

As detailed in the WIPO Conventions and the Copyright in the Information Society Directive (2001/29/EC), exemptions to copyright for legitimate, agreed purposes are recognized and uncontroversial parts of intellectual property legislation. It is entirely possible for users to wish to exchange files which do not breach copyright but which, nonetheless, would risk being "filtered" by network filtering technologies that only allow "approved" files to get through. Both the EU and Council of Europe have had a global leadership position for many years in promoting free speech and access to information. There is simply no existing filtering technology that would allow full use of current technologies while ensuring that legitimate users' behaviours are not restricted.

To what extent can it be considered proportionate or even desirable at any level that intermediaries, which do not benefit in any way from the alleged illegal activity, should finance, or be obliged to finance network filtering technologies?

How much less acceptable does this approach seem when we consider that there is widespread agreement that these technologies offer no answer, or expectation of an answer, to the issue of encrypted files, meaning that an ISP investing heavily in such technology would see the investment rendered meaningless in a short space of time?

On a wider scale, imposing filtering in a way which is likely either to result in legal content being made inaccessible or results in cross-border effects (where legal material becomes unavailable because it is illegal in another country, for example) has international legal implications. The UN Covenant on Civil and Political Rights (Article 19) states that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice". A similar provision also appears in the European Convention on Human Rights.

The general obligation under Article 15 ECD proved to be sufficiently flexible and well drafted as to allow public authorities to put additional obligations on ISPs. Indeed, if the "general" monitoring obligation is forbidden, Member States are not prevented from imposing "specific, limited and clear" obligations on ISPs for individual cases. This interpretation is confirmed by Recital 47 of the directive which adds that courts can still request an ISP, even if not liable for the infringement, to terminate or prevent it through injunctions. However, when imposing specific obligations, a public authority should carefully assess the scope of it to avoid that the measure produces effects equivalent to a generalized monitoring.

* * *

ANNEX:

Relevant articles from the E-Commerce directive:

Section 4: Liability of intermediary service providers

Article 12

"Mere conduit"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

a does not initiate the transmission;

b does not select the receiver of the transmission; and

c does not select or modify the information contained in the transmission.

2. The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 13

"Caching"

1. Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that:

a the provider does not modify the information;

b the provider complies with conditions on access to the information;

c the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

d the provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

e the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

2. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.

Article 14

Hosting

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

a the provider does not have **actual knowledge** of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b the provider, upon obtaining such knowledge or awareness, acts **expeditiously** to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

Article 15

No general obligation to monitor

1. Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.

2. Member States may establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.

유럽의 정보매개자 책임: 전자상거래 지침을 중심으로

1. 제14조: “실질적 인식”

“실질적 인식(actual knowledge)” 요건은 캐싱 및 호스팅 서비스 제공자의 면책 체제에 있어 결정적인 계기임이 입증되었다. 지침이 제시한 총칙은 특정 콘텐츠의 합법성에 대한 결정은 균형잡힌 평가가 가능한 전문적 훈련을 받은 인력을 보유한 법정이나 행정당국에 의해서만 내려지도록 정교하게 의도된 것이다. 이러한 접근법은 제15조 “일반적 모니터링 의무 금지” 조항에 따라 불법이라고 주장된 활동에 대한 적극적 감시를 예방하는 데에 유용한 것으로 판명되었다.

하지만 “실질적 인식”에 대한 구체적인 정의가 없어 각국 수준에서 서비스 제공업체가 실제로 이와 같은 지식을 습득하는 정확한 요건들과 관련한 해석의 문제가 발생했다. 사건에 따라 정보매개자가 법원의 명령 혹은 결정으로 콘텐츠가 실제로 불법이라고 판명된 것이 아니라 이용자가 단순히 불만을 신고하거나 부적절하다고 판단한 콘텐츠에 표시했을 때 실질적으로 인식하였는가가 불분명한 경우도 있다.

이러한 맥락에서 다음의 몇 가지 의문이 생긴다.

- 정보매개자에게 실질적 인식을 제공하기 위해 필요한 정보의 종류는 무엇인가?
- 해당 정보는 얼마나 상세해야 하는가?
- 해당 정보가 제3자에 의해 제공될 수 있는가 아니면 당사자에 의해서만 제공되어야 있는가?
- 콘텐츠의 불법성에 관련한 실질적 인식에 대해, 정보매개자가 법적 분석을 수행할 필요가 있는가 또는 이러한 불법성은 만인에게 명백해야 하는가?

이와 같은 우려를 해소하고 부지, 의도적 왜곡 또는 태만의 가정과 관련된 리스크를 최소화하기 위해 통상 서비스 제공자는 관할 기관이 해당 콘텐츠가 불법이라고 선언하고, 그 삭제, 접근의 제한을 명하거나, 피해가 있는 것으로 결정하며, 제공자가 이러한 결정을 알고 있을 때, 불법성에 대한 실질적 인식을 갖고 있는 것으로 여겼다.

그 동안 저작권 소유자로부터의 상세한 통지에 의해서도 유사한 객관적 사실이 성립되었다. 이 경우, 서비스제공자는 테러행위나 혐오발언 혐의 등 통지된 특정의 행위의 불법성 여부, 유럽연합 "시장에 출시된" 제품이 중고 또는 시험용 제품인지 여부와 같이 복잡한 문제에 대응해야 할 때가 있다.

따라서 실질적 인식은 다음과 같은 최소 요건을 충족하는 통지와 관련되어야 한다.

- 통지는 서면으로 이루어져야 한다.
- 통지자는 불법 혐의가 있는 콘텐츠의 구체적 항목에 대해 충분히 적시해야 한다(콘텐츠 유형에 대한 일반 설명, 즉 정보매개자가 해당 설명에 맞는 특정 항목을 찾기 위해 별도로 조사해야 하는 설명으로는 불충분함).
- 통지는 서비스제공자가 본 목적을 위해 개설한 별도 이메일 주소로 발송되어야 한다.
- 통지에는 문제되는 정보나 행위가 분명하게 명시되어야 한다.
- 통지에는 통지자가 침해 받았다고 주장하는 권리의 소유주임을 증명하는 증거가 제공되어야 한다.

- 통지에는 발행인 또는 저작물을 시중에 공개한 자가 자신의 권리를 침해하고 있으며 저작물의 발행 또는 공개의 법적 근거가 없다는 주장(라이선스나 법적용을 통해)을 포함해야 한다.
- 통지에는 관련 행위 또는 정보의 불법적 성격의 상세한 내용을 포함해야 한다.
- 통지에는 이상의 내용에 대한 사실성 및 정확성에 대한 주장과 이와 관련하여 취한 행동에 대해 책임을 인정한다는 주장이 포함되어야 한다.

이상의 최소 요건을 충족하는 통지를 통해, 이용자들의 저작권 침해를 주장하는 제3자의 경고에 의해 ISP가 "실질적 인식"을 갖게 되었다고 본 최근의 이탈리아 판례는 주목할 만하다.

법원은 ISP의 유일한 의무는 경고장에 포함된 저작권 침해 주장과 관련된 모든 정보를 관할 기관(즉 검찰 및 통신부)에 전달하는 것이라고 판결했다(2010년 로마지방법원 명령 no.415).

2. 자발적 업계 협약

이상의 내용은 서비스제공업체가 자율 협약과 성립될 수 있는 기타 실질적 인지수단들에 따라 수행할 수 있는 적발과 콘텐츠 삭제의 절차를 침해하지 않는다. 이러한 절차는 유럽 공동체 지침에 명시된 협조의 자발적 메커니즘이며 이를 통해 이해당사자가 불법이라고 주장된 행동이 있음을 ISP가 불법이라고 알려진 콘텐츠를 검토하고 필요에 따라 이를 삭제 또는 그 접근을 제한할 타당성을 평가하게 만들 목적으로 ISP에게 보고할 수 있다.

그럼에도 불구하고 EuroISPA는 자발적 업계 협약 체결 시, 몇몇 요건이 고려되어야 한다고 믿는다.

이는 ISP와 그 책임의 제한과 관련한 합법적 확실성을 강화하고, 협약 당사자들과 함께 진정한 협력에 이르는 바탕을 마련하기 위한 목적도 있다. 원칙적으로 제12~15조는 자발적 업계 협약으로 영향을 받아서는 안 된다. 특히 어떤 자발적 협약도 실질적 인식에 대한 추정을 일으켜 서비스제공자가 책임에 노출되도록 하는 일은 없어야 한다.

3. 제14조: “신속하게”

서비스제공업체는 정보의 불법성을 인지한 즉시 이를 신속하게 삭제하거나 접근을 막아야 한다. 지침은 이 요건을 정의하고 있지 않으며 “정보의 삭제 또는 제한을 두기에 앞서 신속하게 충족시켜야 하는 구체적 요건[을 설립]”(제정취지recital 46)하는 것을 회원국의 몫으로 둔다.

일반적으로 “신속하게”라는 개념 때문에 사건 별로 평가하기 위해 필요한 유연성이 제공된다. 특정 사건의 개별 상황과 무관하게 규정할 수는 없다.

자발적 메커니즘의 경우, 법원으로부터 통보를 받아 서비스제공자의 신속한 행위가 필요할 경우에는 별도의 평가가 필요하다. 전자의 사건에서는 정보매개자에게 합법적 확실성이 존재하나, 후자의 경우에는 정보매개자가 삭제 혹은 제한을 두기로 한 콘텐츠의 불법성 여부를 결정하기 위해 필요한 확실성의 모든 요소나 수준을 갖추고 있는가와 상관없이 신고 받은 즉시 행동을 취해야 할 수 있다. 이러한 경우, 신속한 삭제를 요구한다면 필요이상으로 피해 받는 사람에게 지대한 영향을 미쳐 불법이 아닌 웹사이트나 콘텐츠에 대한 접근 제한을 초래할 수 있다.

4. 제14조: 통지 및 삭제(notice-and-takedown)

지침 제14조의 불법이라고 주장된 콘텐츠 관련 호스팅서비스제공자에 대한 신고 절차는 “실질적 인식” 또는 “사실이나 정황에 대한 인지”를 성립시키기 위해 채택해야 할 메커니즘을 명확하게 정의하고 있지 않다. 그 결과 그 동안 회원국 별로 다양한 방법이 채택되었고 이를 다음과 같이 분류할 수 있다.

a 관할 사법당국에 의한 공식 통보(통지삭제): 이 방법은 실질적 인식을 확보하고 정보매개자에게 합법적 확실성을 제공한다.

b 실질적 인식을 결정하는 간단한 통지: 해당 통지가 공식 혹은 비공식 경로로 내려질 수 있다는 사실로부터 몇 가지 단점을 지적할 수 있음; 불법성의 입증은 제공자

의 책임(즉 명백한 불법 vs 복잡한 문의절차); 이러한 시스템의 리스크는 정보매개자가 책임을 면하기 위해 제대로 된 합법성에 대한 평가 없이 모든 통지에 대해 통지삭제를 적용하는 것이다. 앞서 언급한대로 관련된 모든 이해당사자들에게 법적 불확실성을 줄이기 위해 서비스제공자가 언제 "실질적 인식"을 하였는가와 관련해 최소한의 요건을 명확하게 정의하는 것은 매우 중요하다. 영국법은 Question 53에 나열된 바와 유사한 요건을 규정하고 있다.

c 제정법상의 요건: 일부 국가는 공식 혹은 단순 통지 절차를 제공하고 있지 않으며 법원이 준수해야 하는 일련의 특정 요건을 정하고 있다(정보의 위치, 특성, 발신자의 상세 연락처 등).

EuroISPA는 통지 및 차단유지(notice and stay down) 또는 이중 통지(notice and notice) 절차의 도입은 종합적으로 평가되어야 한다고 믿는다. 이러한 절차의 성립이 부가적 가치를 가질 것이라고는 생각하지 않는다. 원칙적으로 법적 분쟁은 이해당사자간에 직접적으로 해결되어야 한다. 정보매개자 역할을 하는 ISP는 관련되지 않은 제3자이다. EuroISPA는 성립된 책임 체계를 약화시킬 의무를 부과하고 법적 불확실성을 일으킬 수 있는 이러한 절차의 실효성에 의문을 갖고 있다. 나아가 ISP가 정보매개자 역할에 있어 불법 콘텐츠를 판별하는 법관이 되지 않도록 확실한 안전장치가 필요하다.

4-1. 이중 통지(notice and notice)

EuroISPA는 추가적인 통지 절차가 분쟁의 원만한 해결과 정당한 책임 분배(해당 콘텐츠의 합법성에 대해 이견을 가진 양당사자에게 책임)의 방법이 될 수 있다고 믿는다. 이와 같은 시스템은 호스팅서비스제공자의 경우에만 고려할 수 있으며 통지의 전달에 국한된다. 프라이버시법과 통신비밀은 존중되어야 하며 기본권도 엄격하게 존중되어야 한다.

나아가 2차에 걸친 통지와 같은 모든 통지 절차는 다음과 같은 일반 가정에 기반하여 고려해야 한다.

- 정보매개자 면책
- 일반적 감시의무 금지 원칙 유지
- 잘못 통지한 자에 대한 제재의 도입

4-2. 통지 및 차단유지(notice and stay down)

EuroISPA는 이러한 시스템은 법적 불확실성을 높이고 ISP가 콘텐츠의 불법성을 결정하는 판결자로 만들며, 이용자간 커뮤니케이션에 지속적인 필터링과 모니터링을 강요하는 동시에 판사의 개입을 완전히 우회하게 만든다고 믿는다.

이와 같은 필터링 및 모니터링 방법은 이행에 큰 비용이 들고 이용자의 근본적인 권리를 침해할 위험이 있을 뿐만 아니라 그 효과가 검증되지도 않았다.

실제로 "통지 및 차단유지"는 특정 콘텐츠의 삭제요청을 처리하기 위해서 호스팅업체는 지속적으로 자사 서비스를 모니터링해 신고된 내용물의 재등록을 감시해야 하기 때문에 제15조의 "감시 의무 금지" 원칙과 양립될 수 없다. 또한 동일 파일에 대한 정확한 디지털 복사본을 지목할 정도로 통지 내용의 범위가 극히 좁지 않는 한 통지 및 차단유지는 이행이 불가능하다(예를 들면 명예훼손적 콘텐츠의 삭제 및 지속적인 통제는 동일한 주장이 다른 문구로 반복하여 재등장하는 것까지 포함한다고 할 수 없다).

5. 필터링 조치

필터링에 대한 논의는 어떠한 경우에도 기술적 타당성에 국한되어서는 안되며 유럽연합 집행위원회로부터 기대할 수 있는 가장 중요한 질문은 유럽의 가치와 경제적 이해에 비추어 필터링 방법을 논하는 것 자체가 바람직한가 이다. 이와 같은 방법은 장벽과 차단장치를 피해 정보전달의 다른 경로를 찾도록 설계된 인터넷과 같이 복원력이 큰 환경에 효과적으로 시행하기 어렵다. 정보통신제공업체의 역할이 p2p 네트워크 등과 같이 실시간 전송의 "단순도관(mere conduit)"에 불과한 상황에서는 더더욱 그러하다. 이러한 조치의 실행 불

가능한 측면은 다음과 같은 이유에 근거한다.

기술적 시각: 효과적인 필터링이 불가능. 우회가 쉬우며 모든 콘텐츠가 영향을 받는다(특히 합법적 콘텐츠). 네트워크 복원력, 보안, 인프라의 효율성에 대한 충격과 역효과를 미친다. 모든 콘텐츠는 ISP 네트워크의 중앙집중화된 필터링 인프라로 이동시켜 검사를 거쳐야 한다. 콘텐츠와 이용자에 대한 통상적인 모니터링은 과도한 차단의 가능성과 같은 부수적인 피해에 대한 리스크가 크다.

보다 광의의 시각:

- 필터링 조치는 기본권의 침해와 관련해 뻔한 결과를 초래할 것임.
- 비상업적인 정보서비스제공자가 필터링 기술을 운영할 것으로 기대할 수 없음.
- 서비스제공자에게 인프라와 인력에 대한 소요되는 투자는 부담이 되며, 유럽 정보사회 발전에 상당하고 지속적으로 부정적인 영향을 줄 것임. "임무 과잉"의 리스크, 즉 특정 이슈에 대응하는 것으로 시작해 모니터링을 다른 이슈들로 확대할 위험도 있으며;
- "기술 과잉"의 리스크, 즉 인터넷 통신의 기술발전(암호화 등)에 발맞춰 필터를 지속적으로 업데이트해야 할 위험이 있다. 필터링은 암호화된 프로토콜의 개발과 위법한 사용 및 서비스에 대응하기 위한 끝없는 투자로 이어져(문제의 근본원인에 대처하는 대신에) 결국 고비용의 효과 없는 조치가 될 것이다.

또한 인터넷 접속서비스제공자가 자사 네트워크로 전송되는 데이터(혹은 그 일부)와 관련하여 적극적으로 필터링 기술을 출시해야 한다면 이는 의도하지 않게 접속서비스제공자가 자사 네트워크로 전송된 정보와 관련하여 전송된 정보를 선택 또는 수정하지 않는 한 모든 책임을 면책하는 지침 제12조의 적용을 무력화시키는 결과를 초래한다는 주장이 제기될 수 있다. 하지만 필터가 "단순한 기술적 도구"라는 이유로 전송된 정보의 선택을 시사하지는 않는다고 한다면 면책이 해지되어 결과적으로 서비스제공자는 자사 네트워크에 사용된 필터 기술의, 예를 들어 불법 콘텐츠를 차단하지 못하는 등의 결함에 대해 책임을 져야 할 위험에 처한다. 다시 말해, ISP를 "단순도관"으로 특징짓는 것은 서비스업체, 그 고객, 그리고 기본권에 대한 존중 모두에 심각한 결과를 초래하는 등 위태로울 수 있다.

기술솔루션 "Audible Magic"이 p2p 트래픽에 대한 필터 기술 후보로 제안된 벨기에의 Scarlet-SABAM 건의 판례 맥락에서 보듯이, 벨기에 법원은 필터링이 효과는 물론 대규

모 확장성도 없다고 봐도 무방하다고 인정했다. 물론 한 기술로 커뮤니케이션의 합법/불법성에 기초해 이를 완벽하게 구분한다거나 심지어 파일 내 내용을 알아내는 것조차 불가능해 보인다. 필터 기술과 직접적 관련이 없으나 예를 들면 저자 또는 저작권 협회에 의한 허가 또는 구체적인 라이선스 조건과 관련된 구체적 내용, 그리고 저작권에 대한 법적 예외에 의한 간섭 가능성에 따라 달라질 수 있다.

6. 비례성

앞서 언급한 바와 같이, 기존 네트워크 필터링 기술이 당초 목적달성에 효과적일 것인가에 대해 상당히 회의적인 시각이 있으며, 특히 해당 기술보다 "한발 앞서기" 위해 이용자들은 상대적으로 단순한 암호화 기법을 사용하기만 해도 되기에 더더욱 회의적이다. p2p 트래픽의 암호화는 이미 빠르게 이루어지고 있으며, 필터링 조치도 결국 검사를 피하기 위한 암호화 기술의 보편적 사용을 장려하게 될 뿐이다. 동시에 필터링은 네트워크 서비스, 이용자 경험의 품질저하, 그리고 합법적 콘텐츠에 대해 의도하지 않은 접근차단을 초래할 위험이 있다. 또한 이와 같은 기술로 증가된 비용은 디지털 불평등 해소에 더 큰 장벽을 만들게 할 것이다.

세계지적재산권기구(WIPO) 협정과 정보사회의 저작권 지침(2001/29/EC)에 상세히 명시된 바와 같이, 정당하고 합의된 목적을 위한 저작권 예외는 지적재산권법 제정에서 인정되고 이견이 없는 부분이다. 사용자가 저작권을 침해하지는 않지만 "승인된" 파일만 통과시키는 네트워크 필터링 기술로 "걸러질" 위험이 있는 파일들을 교환하는 것이 얼마든지 가능하다. 그 동안 EU와 유럽 평의회는 지난 수년간 전세계에서 발언과 정보접근의 자유를 전파하기 위한 선도적 지위에 있었다. 현 기술의 활용을 극대화하는 동시에 정당한 이용자들의 행태가 제한되지 않도록 보장할 현존하는 필터링 기술은 없다.

불법이라고 주장된 활동으로 어떠한 형태의 이익도 취하지 않는 정보매개자가 어느 수준까지 네트워크 필터링 기술에 투자하거나 투자해야 할 때, 비례성에 맞거나 적어도 바람직하다고 여길 수 있을까?

위 기술이 암호화된 파일 문제에 대해 해법이 될 수 없으며, 해법을 기대할 수도 없다는, 즉 ISP가 이러한 기술에 많은 투자를 해도 단기적으로 무의미한 투자였음을 알게 될 것이

라는 광범위한 합의가 있다는 점을 고려할 때, 이러한 방법은 얼마다 더 용인하기 힘들게 될까?

더 크게 보면, 합법적 콘텐츠에 접근이 차단되거나 크로스보더 효과가 발생(예를 들어, 합법적인 콘텐츠가 다른 국가에서 불법이라는 이유로 접근 불가하게 되는)하도록 필터링을 적용하는 것은 국제적인 법적 결과를 초래하게 된다. 시민적 및 정치적 권리에 관한 UN 규약(제19조)은 "모든 사람은 표현의 자유를 가지며; 여기에는 국경과 관계없이 구두, 서면, 혹은 인쇄로, 예술의 형태 또는 선택가능 한 모든 매체를 통해 모든 유형의 정보와 아이디어를 탐구, 수령, 전파하는 자유가 포함된다"고 명시하고 있다. 유럽 인권협약에도 유사한 문구가 있다.

유럽 공동체 지침 제15조에 따른 일반적 의무 조항은 충분히 유연하고 잘 명시되어 공공 당국이 ISP에 추가적인 의무부과가 가능한 것으로 입증되었다. 실제로 "일반적인" 모니터링 의무가 금지된다고 해도 회원국은 ISP에 대해 사건 별로 "특정되고, 한정되며, 분명한" 의무를 부과할 수 있다. 이러한 해석은 법원이 불법행위에 대한 법적 책임이 없는 ISP에게도 여전히 명령을 통해 침해의 중단 또는 예방을 요구할 수 있다고 추가적으로 명시하고 있는 지침의 개정설명 47조에 의해서도 확인되고 있다. 그럼에도 불구하고 특정된 의무를 부과할 때, 공공기관은 해당 조치가 일반적 모니터링에 준하는 효과를 일으키는 것을 방지하기 위해 그 범위에 대해 세심한 검토가 있어야 한다.

* * *

부 록

전자상거래 지침 관련조항:

제4부 정보매개서비스제공자의 책임

제12조

"단순도관(Mere conduit)"

1. 통신망에서 서비스 수혜자에 의한 정보의 전송 또는 통신망으로의 접속 제공을 포함한 정보사회 서비스가 제공되는 경우, 회원국은 해당 서비스제공자가 다음의 조건에 해당하는 한, 전송된 정보에 대해 서비스제공자의 면책을 보장해야 한다.

a 전송을 개시하지 않을 것

b 전송의 수신자를 선택하지 않을 것

c 전송에 포함된 정보를 선택 또는 수정하지 않을 것

2. 제1항의 전송 및 접속제공 행위에는 통신망에서 전송을 실행할 목적으로만 발생하고, 해당 정보가 전송에 합리적으로 필요한 기간보다 초과하여 저장되지 아니하는 한, 송신된 정보의 자동적이고, 매개적이며, 임시적인 저장이 포함된다.

3. 본 조는 법원 또는 행정당국이 회원국의 법체계에 따라 서비스제공자에게 침해의 중단 혹은 예방을 요구할 가능성에 영향을 주지 않는다.

제13조

"캐싱(Caching)"

1. 정보통신망에서 서비스 수혜자에 의한 정보의 전송을 포함한 정보사회 서비스가 제공되는 경우, 회원국은 다른 서비스 수혜자의 요청에 의한 그 수혜자에 대해 이루어지는 정보의 계속적 전송을 더 효율화하기 위한 목적으로만 실행된 정보의 자동적이고, 매개적이며, 임시적인 저장에 대해 다음의 조건 하에서 서비스제공자의 면책을 보장해야 한다.

a 제공자가 해당 정보를 수정하지 않을 것;

b 제공자가 해당 정보에 대한 접근 요건을 준수할 것;

c 제공자가 업계에서 폭넓게 인정되고 사용되는 방식으로 명시된 정보의 갱신에 관한 규칙을 준수할 것;

d 제공자가 해당 정보의 이용에 대한 자료 취득에 있어 업계에서 폭넓게 인정되고 사용되는 기술의 합법적 이용에 개입하지 않을 것; 그리고

e 제공자가 전송의 원천에 있는 정보가 통신망에서 삭제 또는 접근 제한되었거나 법원 또는 행정당국이 이와 같은 삭제 또는 제한을 명령했다는 사실에 대해 실질적으로 인지한 즉시 저장한 해당 정보를 신속하게 삭제 또는 제한할 것

2. 본 조는 법원 또는 행정당국이 회원국의 법체계에 따라 서비스제공자에게 침해의 중단 혹은 예방을 요구할 가능성에 영향을 주지 않는다.

제14조:
호스팅(Hosting)

1. 서비스 수혜자가 제공한 정보의 저장으로 구성된 정보사회 서비스가 제공되는 경우, 회원국은 서비스 수혜자의 요청에 의해 저장된 정보에 대해 다음의 조건 하에서 서비스제공자의 면책을 보장해야 한다.

a 제공자가 불법 행위나 불법 정보에 대해 **실질적 인식(actual knowledge)**이 없으며, 손해배상 청구와 관련하여 불법 행위 또는 불법 정보가 명백하게 드러난 사실 또는 정황을 인지하지 못할 것; 또는

b 제공자가 이와 같은 인식 또는 인지가 있을 경우 **신속하게** 해당 정보를 삭제하거나 그 접근을 금지했을 것

2. 제1항은 서비스수혜자가 제공자의 권한 또는 통제 하에 행동하는 경우에는 적용되지 않는다.

3. 본 조는 법원 또는 행정당국이 회원국의 법체계에 따라 서비스제공자에게 침해의 중단 혹은 예방을 요구할 가능성에 영향을 미치지 않으며, 회원국이 정보의 삭제 또는 그 접근의 금지를 규정하는 절차를 수립할 가능성에도 영향을 미치지 않는다.

제15조
일반적 모니터링 의무 금지

1. 회원국은 제12, 13, 14조가 적용되는 서비스의 제공 시, 서비스제공자가 자신이 전송 또는 저장하는 정보를 모니터링할 일반적 의무를 부과해서는 안되며, 불법 행위임을 드러내는 사실 또는 정황을 적극적으로 조사할 일반적 의무도 부과해서는 안 된다.

2. 회원국은 정보사회 서비스제공자에게 자사 서비스 수혜자에 의해 행하여진 불법이라고 주장되는 행위 또는 이들이 제공한 정보에 대해 관할 당국에 지체 없이 알려야 할 의무 또는 서비스제공자가 저장계약을 맺은 자사 서비스 수혜자의 신상을 파악할 수 있는 정보를 관할 당국의 요청에 따라 제공할 의무를 규정할 수 있다.

Discussion / 토론

Old and New Challenges in Actualizing the Ideals of Digital Public Sphere: Giant Intermediaries Posing New Threats to Digital Ecosystem

Dr. **Minjeong Kim**
(Associate Professor of Media and Communication, HUFS)

김민정 교수

(한국외대, 한국언론법학회 연구이사)

At the outset, I would like to make it clear that I agree with Professor KS Park's criticism over Korea's intermediary liability regime. I believe it is particularly problematic that a government agency, namely the Korean Communication Standards Commission, has been acting as a regulator of content in non-copyright issues. This content-based regulation has resulted in government censorship over various types of content including political speech. A bedrock principle underlying the constitutional guarantee of freedom of speech and of the press should be the right to criticize the government and the right to express controversial or unpopular ideas and opinion. Thus, the state paternalism manifested in Korea's intermediary liability regime is very worrisome. Like Professor Park, I also believe that Article 44-2 of the Act Regarding Promotion of Use of Information Communication Networks and Protection of Information and Article 103 of the Copyright Act ought to be revised. The current Korean laws are troublesome because they have created, as Professors Gasser and Schulz (2015) pointed out, "asymmetric incentive structures" that may result in over-compliance and private censorship.

That said, I would like to turn to the main idea expressed by Professor Chander and Mr. Olive Süme. Both speakers suggest that laws imposing rigid liability on intermediaries hinder Internet innovations in that the legal regimes enforcing strict rules to protect copyright and privacy may disable the development of a new industry. I think the argument is valid. Professor Chander suggests that Silicon Valley's success owes a great debt to key substantive reforms to U.S. copyright and tort law in the 1990s that reduced liability concerns for Internet intermediaries. This seems to me a reasonable conclusion to draw.

However, the success of less regulation for Silicon Valley does not necessarily mean that there are no new challenges to figuring out the health of digital ecosystem. For example, thanks to the legal privileges offered to them, some intermediaries, like Google and Facebook, have grown and flourished. Intermediaries like Google and

Facebook not only crossed over "the valley of death" but also became so successful that they now play a significant and critical role in shaping the nature of digital ecosystem. Goggle processes 67-percent of U.S. search queries on PC, 83-percent of U.S. search queries in mobile, and above 90-percent of European search queries (Sterling, 2014). A 2014 survey by the Pew Research Center revealed that nearly half of Web-using U.S. adults get news about politics and government on Facebook. In South Korea, Naver—the local portal--maintained over 76-percent of Korean search queries both on PC and in mobile, followed by Daum with about 20-percent in 2014. These two portals are also the main platforms for online news consumption in Korea. As of 2015, it is estimated that over 34-percent of Naver portal news come from the Yonhap News Agency that has pro-government tone and is subsidized by the government.

Some commentators worry that giant intermediaries have become too powerful. Eli Pariser (2011) warned that "the filter bubble" created by services like Google's personalized search and Facebook's personalized news stream insulate each of us in "the Web of one", making it difficult for us to have a meaningful conversation on collective concerns. Tarleton Gillespie (2010) argued that platforms like YouTube became the "curator of public discourse" and yet they downplay their role, as merely an intermediary, to limit their legal liability while exercising control over what content remain circulated on their services. It is also known that Google has been lobbying U.S. lawmakers aggressively since 2006 and has been vocal on a number of policy issues (Phillips, 2006). People like Nathan Newman (2013) and Frank Pasquale (2015) make a strong argument on the negative impact on user data and privacy stemming from Google's market dominance and its questionable monopoly practices in recent years. Pasquale (2015) contends that "too many still believe that the digital economy is by its nature open, competitive, and subject to the disruption" but that it is very unlikely for a start-up with valuable new search technology and even with millions in venture capital funding to be brewing in somebody's garage. It seems to me that the lack of regulation of giant digital intermediaries is increasingly eroding upon a democratic digital ecosystem.

Thus, I would like to ask both speakers what their thoughts are on these giant intermediaries posing new threats to online public discourse, online privacy, and digital economy. Also, do the session speakers believe if and how law can or should play a role in addressing these new threats (i.e., "the costs" of the amazing innovation of the past two decades")?

After all, I believe we all want the same thing—actualizing the full potential of the Internet. That is, an open, free, innovative communication medium overcoming the shortcomings of the traditional marketplace of ideas and enabling anyone and everyone to speak their mind, to share their creativity, etc. Unfortunately, the main obstacles Korean online users face are still old challenges –censorship by the government and by intermediaries outsourced by the government. Yet, these old problems are being compounded by new challenges brought by giant intermediaries that seem almost "too big to fail." I think it is incumbent on us now to work our way through both challenges old and new.

References

Gasser, U. & Schulz, W. (2015). "Governance of Online Intermediaries: Observations From a Series of National Case Studies", The Berkman Center for Internet and Society Research Publication No. 2015-5, at https://cyber.law.harvard.edu/publications/2015/online_intermediaries

Gillespie, T. (2010). "The Politics of 'Platforms.'" New Media & Society, 12(3), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1601487

Mitchell, A. etc. al. (Oct. 21, 2014). "Social Media, Political News and Ideology", at http://www.journalism.org/2014/10/21/section-2-social-media-political-news-and-ideology/

Newman, N. (2014). "Search, Antitrust and the Economics of the Control of User Data," Yale Journal on Regulation, 30(3), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2309547

Pariser, E. (2011). "Beware Online 'Filter Bubbles'", TED talk, at http://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press: Cambridge, MA.

Phillips, K. (Mar. 28, 2006). "Google Joins the Lobbying Herd." The New York Times, at http://www.nytimes.com/2006/03/28/politics/28google.html?pagewanted=print&_r=0

Sterling, G. (Sept. 22, 2014). "Google Market Share: 67 Percent on PC, 83 Percent In Mobile, at http://searchengineland.com/googles-search-market-share-67-percent-pc-83-percent-mobile-203937

Discussion / 토론

Mr. Jongsoo Yoon

(Partner, Shin&Kim)

윤종수 변호사

(법무법인 세종)

기술적 진보의 양면성에 대한 법적 판단의 고전으로 지금도 계속 거론되고 있는 사례가 미 연방대법원의 소니(Sony) 사건이다. 유니버설 스튜디오 등 방송프로그램에 대한 저작권자가 베타맥스 VCR의 제조자인 소니를 상대로 VCR의 이용자들에 의한 저작권 침해행위에 대한 책임을 물은 사건인데, 소가 제기 된지 8년이 지난 1984년 미 연방대법원이 팽팽한 격론 끝에 5:4로 내린 결론은 '상업상 주요물품론'(staple article of commerce doctrine)'이었다. 즉, 소니가 저작권침해의 용도로 쓰일 수 있는 VCR을 제조하였더라도 이 기술이 상당부분 적법한 용도로도 쓰일 가능성이 있으면 그 침해의 가능성에 대한 추상적 인식만으로는 기여책임이 없다는 판단이다. 우리의 법제에는 없는 기여책임이라는 간접책임의 판단에 관한 것이므로 이를 그대로 가져올 수는 없지만, 새로운 기술이 비록 부작용이 있더라도 유용한 기술이라면 법은 그 기술을 보호하여 기술혁신에 대한 여유 공간을 남겨두어야 한다는 취지여서 국내에서도 자주 인용되고 있다. 그러나 위 사건에서 미연방대법원이 결론에 이르게 된 과정에 고려한 주요한 요소임에도 제대로 주목받지 못한 부분이 있다. 미연방대법원은 위 판결에서, 저작권은 유용한 예술을 증진하기 위하여 제한된 시간 동안 저자에게 의회가 부여한 권능으로서 이는 어디까지나 법규의 창설에 의존하는 것이므로, 주요한 기술적 혁신이 저작물의 시장에 영향을 미쳤을 때 그로부터 불가피하게 영향을 받는 충돌하는 이해관계들의 다양한 배열을 수용할 권한과 능력은 의회에 있고, 따라서 법원이 의회가 그러한 이익형량을 한바 없는 사안에 대해서 법을 적용할 때에는 신중하여야 한다고 판시한 바 있다. 즉 저작권은 이익형량에 따른 결과물로 의회가 창설한 권리이므로 명확한 입법적 제시가 없을 때에는 그 보호의 범위를 함부로 확장할 수 없다는 취지이다. 비록 저작권의 보호 범위에 대해서 설시한 것이기는 하지만, 기존의 이해관계와 새로운 기술 또는 혁신이 충돌할 경우 이를 조정할 지위가 의회에 있음을 명확히 하고 의회로 하여금 치밀한 이익형량을 통해 기존 권리와 새로운 기술혁신의 수용 범위를 끊임없이 고민하도록 요구한 것이라 할 수 있다.

인터넷 시대에 실리콘밸리의 성공이 미국의 저작권법과 불법행위법에 대한 주요 개혁에서 기인하며, 낮은 수준의 개인정보 보호정책들과 아울러 인터넷 정보매개자들의 법적 책임 우려를 낮춘 1990년대 법적 혁신을 통해 웹2.0으로 알려진 신생 기업들에게 비옥한 토대를 제공한 법적 생태계를 마련하였다는 아누팜 챈더 교수의 지적은 다소 도발적으로 들

릴 수도 있겠지만, 위 판결에 나타난 태도를 보면 충분히 수긍할 만하다. 가장 공고한 지적재산권의 포트폴리오를 갖추고 전 세계적인 공세를 펼치고 있는 미국이 저작권법의 개혁을 통해 신생 정보서비스 기업들에게 우호적인 환경을 만들어 주었다는 점이 어색하게 다가올 수는 있다. 물론 디지털 시대의 미국의 저작권법이 권리를 축소하거나 그 보호를 완화하는 쪽으로 변화되어 온 것은 결코 아니다. 권리보호기간을 대폭 연장하여 전 세계의 입법을 선도한 이른바 미키마우스법에서 알 수 있듯이 오히려 권리보호 범위는 계속 확대되어 왔고, 효율적인 집행을 위한 다양한 입법들이 시도되어 온 것이 사실이다. 지난 SOPA 사태에서 볼 수 있듯이 권리보호확대를 위한 입법시도는 거세게 이어지고 있고 이를 저지하기가 쉽지 않은 상황이다. 하지만, ISP, 즉 정보매개자라는 새로운 혁신의 주체들에 대해서는 그 어느 나라보다 앞서 명확한 선을 그어 새로운 환경에서 신흥 정보매개자들이 부담하게 될 법적 책임을 완화시켜 주었다는 점에서 소니 판결에서 정립된 입장이 계속 승계되어 오고 있다는 점은 확실하다. 정보매개자인 P2P 서비스에 대해 만장일치로 법적 책임을 인정한 2005년의 글록스터 케이스처럼 예상 외로 정보매개자의 책임을 확실하게 인정한 경우도 있었지만, 애초부터 비즈니스 모델 자체에서 침해행위를 유발하고 있다는 사실을 인정하고 그에 기해서 책임을 부과하였다는 점에서 표현의 자유라는 최고의 헌법적 법익에 의하여 뒷받침 되고 있는 유용한 기술의 보호를 위한 세이프 하버(Safe Harbor)는 여전히 기능하고, 소니 판결에서 나타난 법리 역시 계속 유지되고 있다고 할 수 있다.

이에 비해 국내의 상황은 다소 애매하다. 저작권법은 2003년부터 온라인서비스제공자(OSP)의 책임제한에 대해서 규정하여 왔지만 다소 불명확한 요건들과 대부분 임의적인 감면 규정만 둔 탓에 실질적으로 책임제한 규정으로서 독자적인 역할을 하였다고는 보기 어렵다. 2011년부터는 위 책임제한 규정을 미국 DMCA의 규정과 거의 유사하게 개정(동법 제102조, 제103조)하여 서비스의 종류에 따라 구체적인 요건을 정하고 그에 따른 효과도 필요적 면책으로 규정하였으며, 특히 온라인서비스제공자에게 모니터링 의무나 침해행위에 대한 적극적 조사의무가 없음을 명확히 규정 한 바 있으나, 과연 위 개정으로 인해 책임제한의 경우가 얼마나 확대될지는 장담하기 어렵다. 무엇보다도 법원에 의하여 온라인서비스제공자의 법적 책임근거로 확립된 방조에 의한 공동불법행위의 외연이 아주 광범위하기 때문이다. 해석상 방조는 타인의 불법행위를 '용이하게 하는 직접·간접의 모든 행위'이면 되고, 과실에 의한 방조도 가능하며 그 침해행위나 직접침해자가 누군지도 인식할 필요도 없다. 따라서 저작물 등을 정보통신망을 통하여 복제 또는 전송할 수 있도록 하는 서비스를

제공하는 온라인서비스제공자의 책임을 이러한 방조로 구성하는 한 서비스제공자가 방조책임에서 벗어나기가 쉽지 않은데, 서비스 모델에 따라서는 방조책임을 면하기 위해서는 적극적인 모니터링 의무의 이행이 요구되는 것으로 해석되고 있어 위 책임제한 규정이 서비스제공자의 법적 안정성이나 예측 가능성을 끌어내기에는 여전히 미흡하다고 밖에 볼 수 없다. 이러한 사정은 명예훼손 등과 관련해서 적용되는 정보의 삭제요청에 따른 프로세스를 규정한 정보통신망법의 규정(동법 제44조의2) 역시 마찬가지이다. 요청에 따른 절차를 밟을 경우 그로 인한 배상책임을 감면할 수 있도록 규정하고 있으나 저작권 침해의 경우와 마찬가지로 폭넓게 방조책임이 인정되고 있는 실정이고, 정보통신서비스제공자를 위한 세이프 하버는 역시 실효성 있는 기능을 하지 못하고 있는 것으로 평가된다.

물론 미국과 국내의 상황을 그대로 비교하기는 어렵다. 표현의 자유만 해도 헌법적 가치의 상위에 위치하고 있는 미국의 경우와 달리 국내에서는 여타의 헌법적 가치와 같은 수준에 위치하고 있어 구체적 사건에서 법익의 형량을 통하여 다른 가치에 밀릴 여지가 상대적으로 큰 만큼 표현의 자유에 터 잡아 정보매개자를 우선적으로 보호하기에는 법리적으로도 미흡한 부분이 있다. 문화적 전통과 법체계가 다르고 그 동안의 경험이 서로 상이한 이상 미국의 상황을 그대로 적용하는 것은 적절하지 않다는 지적에 대해서도 반박하기 쉽지 않다. 게다가 글로벌 정보기술기업의 공세와 독점적 지위에 대한 실리적인 방어라는 다소 전통적인 시각 역시 계속 유지되고 있어 국제 기준, 더 구체적으로는 미국의 기준을 그대로 원용하는 것에 대해 반감을 가지고 있는 경우도 적지 않다. 하지만 ICT 분야의 발전을 저해하는 요인으로 줄기차게 지적되고 있는 규제문제라는 차원에서 보면 정보매개자에 대한 우리의 입장은 여전히 규제의 영역에서 그다지 멀리 나아가지 못하고 있고, 그로 인해 무거워진 ICT 생태계는 변화된 환경에 재빠르게 적응하지 못하고 있다. 우리나라 정보화 법제는 정책 추진의 근거로서 강한 '조직법'적 성격을 보이면서 IT 변화에 발 빠르게 대응하는 등 괄목할 만한 성장을 보였다고 할 수 있으나, 그 결과 과도한 양의 입법, 잦은 개정으로 인한 수범자의 혼란 야기 등을 초래하였다는 지적은 초기의 정부 주도적인 성장이 갖는 부작용을 잘 설명해주는데, ICT 산업의 성장에 따라 드러나는 여러 문제들을 해결하기 위해 '규제법'적 성격이 강화되면서 과도한 규제라는 또 다른 문제를 야기하고 있는 것이다.

규제 자체가 불필요하다거나 규제의 역할이 ICT 산업의 원활한 발전과 대척되는 점에 있다고 보기는 어렵다. 규제는 부작용의 제거를 통해 성장을 가능하게 하는 중요한 수단이다. 정보화 거버넌스는 성장과 규제가 함께 협력하는 모델로 구현되며, 이는 입법에 있어서도 "성장"과 "규제"를 적절히 반영하는 균형적 형태로 나타날 수밖에 없다. 문제는 규제 자체에 있다기보다 규제의 선택 및 그 적용 방법에 있다. 어느 곳에 어떤 규제를 적용할 것인지, 그러한 규제의 목적 및 영향이 무엇인지에 대한 치밀한 검토 없이 어설픈 대응으로 성급히 규제를 도입하는 경우 ICT 생태계는 균형을 잃고 비틀거리게 된다. 우리의 규제입법에 있어 가장 취약한 모습을 보여온 것은 이른바 '파괴적 혁신'을 가져오는 기술의 경우였다. 파괴적 혁신이 기존 시장을 바꿀 수 있는 가장 큰 원인은 '성공의 저주'에 있다. 즉, 이미 성공적인 위치를 차지한 기업은 그 성공이 오히려 족쇄가 되어 파괴적 기술에 대응할 기회를 알면서도 놓친다는 데에 있다. 필름 시장의 최강자였던 코닥이 업계 최초로 디지털 카메라를 만들었고 디지털 사업부를 밀었음에도 기존에 차지하고 있는 필름시장에 대한 미련과 당장 수입이 나지 않는 디지털 카메라에 대한 의심으로 인한 내부 반발에 부딪혀 디지털 카메라 시장에 제대로 대응하지 못해 파산해 버린 일화는 그러한 성공의 저주를 극명하게 보여준다. 이는 파괴적 기술에 대응하는 입법에 있어서도 마찬가지이다. 기존의 시장과 질서에 집착한 나머지 새로운 시장과 질서를 만들어 낼 수 있는 혁신에 대한 평가를 제대로 하지 못하고 '파괴'의 억제에만 치중해왔고 그것이 정보매개자에 대한 우리의 기본적인 태도라 할 수 있다.

국내의 인터넷 규제체계는 사회안전과 질서유지 패러다임을 기반으로 한 정부개입중심의 위계적 규제모델에 가깝다. 인터넷에 대한 과다한 규제가, 인터넷을 권위적이고 일방적이며 폐쇄적인 기존 미디어를 보완하는 하나의 '공론장(publicforum)'으로 기능하는 대안매체로 보기보다는 또 하나의 '영향력 있는 매스미디어'에 불과한 것으로 보는 경향이 강하고, '무절제한 참여, 폐쇄적이고도 상호불관용의 담론 형성, 사익을 위한 공유'로 점철되어 있는 안전하지 못한 공간으로 의심하는데 기인한다는 지적은 충분히 수긍할 만하다. 인터넷 산업에서의 과다규제의 심각성은 단순히 규제의 정도가 심하다는 점이 아니라 규제의 동기가 산업 자체의 측면보다는 산업 외의 정치.사회 등 다른 측면에서의 고려가 큰 비중을 차지하고 있다는 점에 있다. 규제의 효율성이 '시장의 효율성 제고'에 의하여 평가되지 않고 시장이나 산업 외의 다른 기준에 의한 효율성 확보로 평가된다면 산업 자체에 긍정적인

영향을 미치기가 어려운 것은 당연하다. 물론 거시적으로는 산업도 정치나 사회·문화적인 환경의 정비와 개선으로 인해 도움을 받을 수도 있지만, 인터넷의 파괴적 혁신성에 대한 조급한 대응은 그러한 가능성마저 기대하기 어렵게 만든다. 정보매개자에 대한 논의 역시 이 틀을 크게 벗어나지 못하고 있다.

아누팜 챈더 교수가 언급하였듯이 혁신의 성취에 대해서는 지불해야 할 가격이 뒤따를 수밖에 없고, 혁신을 축하할 때에도 이 비용이 인정되어야 한다. 이 비용을 어떻게 부담하고 그로 인한 충격을 완화시키는지가 또 하나의 큰 숙제가 될 수밖에 없을 것이다. 하지만 우리가 처한 현재의 어정쩡한 상황은 과실도 확실히 챙기지 못한 채 그 보다 더 많은 비용을 야기하고 있는 것으로 보인다. 이 비용을 과연 누가 부담할 것인지 곰곰이 생각해 볼 일이다.

Discussion / 토론

Prof. Inho Lee

(Chung-Ang University)

이인호 교수

(중앙대, 정보법학회 회장)

1 앞서, 개서 교수님, 나오코 변호사님, 챈더 교수님, 그리고 쥬메 회장님이 발제한 내용은 한국의 관련자들에게 매우 소중한 지식과 정보를 제공해 주고 있다. 이 분들이 던지는 메시지를 요약하면, 정부는 복잡한 디지털 생태계에서 정보매개자들을 활용해서 규제의 목적을 달성하고자 하지만, 이러한 '개입'은 항상 과잉규제의 위험을 수반하게 되고, 종국적으로는 인터넷 이용자의 기본권, 기술과 서비스의 혁신, 그리고 디지털 경제에 부정적인 영향을 미친다는 것이다. 정보매개자에게 불법정보를 판단하는 책임을 지우면 지울수록, 디지털 정보생태계가 더욱 교란되고 정상적인 발전이 저해된다는 것이다. 전적으로 찬성한다.

2 현재 한국의 온라인 정보매개자들은 인터넷상의 불법정보의 유통에 대해 상당히 무거운 부담을 지는 여러 종류의 책임과 규제의 벽에 갇혀 있다.

① 대표적인 것이 정보통신망법상의 임시차단조치이다. 앞에서 박경신 교수님이 충분히 설명을 하였다. 이 규제에 대해 2012년에 헌법재판소가 전원일치로 합헌결정을 했지만, 그 결정에는 아쉽게도 오늘 세미나에서 논의하는 '정보매개자 책임의 국제적 흐름'에 대한 충분한 이해가 결여되어 있다. 오늘의 세미나가 먼저 있었으면, 아마 헌법재판소의 결정이 달라지지 않았을까 생각한다.

② 2009년에 대법원은 '인터넷포털의 명예훼손책임 인정 사건'에서 포털이 제공하는 게시공간(댓글창, 블로그, 카페 등)에 게시된 이용자의 명예훼손 게시물에 대해 피해자의 삭제 또는 차단요구가 없더라도 그 게시물의 존재를 인식할 수 있었으면 그 게시물을 삭제하거나 차단시킬 의무가 있다고 인정하였다.

③ 다음으로, 수사기관의 정보제공요청에 대한 정보매개자의 책임 문제를 들 수 있다. 2012년에 서울고등법원은 이른바 '김연아 회피 동영상 유포 사건'에서 정보매개자에게 이용자의 정보제공에 대한 개별적인 이익형량책임과 손해배상책임을 부과하였다. 이 사건에서 서울고등법원은, 수사기관이 법적 절차에 따라 이용자의 '통신자료'(ID, 이름, 연락처 등의 신원확인정보)를 제공해 달라는 요청을 온라인 정보매개자에게 한 경우, 정보매개자는 수사기관의 정보제공요청에 대해 개별 사안별로 제공할 것인지 여부를 적절히 심사하여야 한다는 책임을 정보매개자에게 부과하면서 그러한 책임을 이행하지 않았다는 이유로 손해배상책임을 인정하였다. 현재 대법원에서 심리 중에 있다.

④ 또 하나, 개인정보보호법의 규제를 들 수 있다. 한국의 개인정보보호법은 '정보주체의 사전 동의'와 '형사처벌'에 기반을 둔 강력한 사전규제법이다. 세계적으로 보기 드물게 개인정보의 '활용'보다는 '보호'에 지나칠 정도로 치우쳐 있다. 이로 인해 빅 데이터나 사물인터넷을 활용한 새로운 서비스의 개발과 혁신에 커다란 장애요인이 되고 있다. 또한 '개인정보자기결정권'(informational privacy)이라는 위험예방을 위한 권리 앞에서 이용자의 '정보소통의 자유'는 크게 후퇴하고 있다. 최근에는 소위 '잊힐 권리'(right to be forgotten)라는 또 다른 실체가 불분명한 권리 주장이 온라인 정보매개자들의 책임을 더욱 가중시킬 태세에 있다.

3 전반적으로, 현재 한국의 디지털 정보생태계는 정부의 후견적(paternalistic) 간섭과 개입으로 인해 기술과 서비스가 혁신될 수 있는 가능성과 기회가 점차 줄어들고 있다. 그 배경과 관련해서는 네 가지 원인을 지적할 수 있다.

① 한국의 규범질서에서 민주주의(democracy)와 법치주의(rule of law)의 여러 원칙들이 잘 작동하고 있지만, 한편으로 정부의 후견적 간섭주의(paternalism)가 광범위하게 작용하고 있다. 근본원인은, 시민들이 스스로 해결하려고 하기 보다는 정부가 먼저 나서서 문제를 해결해 주기를 바란다는 데에 있다.

② 또한, 권한을 계속해서 확대하고자 하는 공무원들의 관료주의(bureaucracy)가 이에 편승하여 정부의 후견적 간섭과 개입을 더욱 조장하고 있다.

③ 다른 하나는, 의회주의(parliamentarism)의 기능 저하를 들 수 있다. 그때그때 여론에 편승한 무리한 법률들이 우후죽순으로 발의되고, 법률안 심의 과정에서 깊이 있고 진지한 토론은 거의 찾아보기 어려우며, 입법기술의 수준은 낮아서 상충하는 가치와 이익들을 정교하게 조정하지 못하는 비합리적인 법률들이 양산되고 있다.

④ 법원과 헌법재판소는 온라인 정보생태계에 대한 이해와 인식의 부족으로 이러한 문제상황을 적절히 통제하지 못하는 것으로 보인다.

여기에 덧붙여, 이 분야 법학자와 법률가들이 세계의 선진적인 법제에 대한 치밀한 분석과 정확한 정보를 제때 충실히 제공하지 못하고 있다.

4 향후 한국에서도 정보매개자의 책임과 관련해서 미국과 유럽에서 채택하고 있는 세이프 하버(safe harbor)의 규제기법이 적극적으로 도입되어야 할 것으로 판단된다.