발 간 등 록 번 호
11-1620000-000388-01

12th Informal ASEM Seminar on Human Rights

제12차 아셈인권세미나 사전회의

"Balancing Freedom of Expression and the Right to Privacy in an Informatization Society"

"정보화 사회에서의 프라이버시권과 표현의 자유의 균형적 조화"

| 일시 | 2012년 6월 27일(수), 09:30-12:00

| 장소 | 플라자 호텔, 그랜드 볼룸 (B2)

| 주최 | 국가인권위원회

국가인권위원회
National Human Rights Commission of Korea

개 회 사

안녕하십니까?
국가인권위원회 상임위원 홍진표입니다.

오늘 **제12차 아셈 인권세미나 사전회의**에 참석하여 자리를 빛내주신 내·외빈 여러분께 감사의 말씀을 드립니다.

이번 인권세미나의 토론주제인 **'정보통신 기술과 인권'**은 비교적 새로운 인권 이슈입니다. 정보화시대를 맞아 인류는 편리한 생활을 누리고 있지만, 동시에 사이버공간에서의 개인정보 보호, 표현의 자유 등 인권 주제들이 등장했습니다.

정보통신기술의 발전이 지구촌의 삶을 근본적으로 변화시키고 있는 상황에서 아셈인권세미나가 '정보통신기술과 인권'이란 주제를 택한 것은 매우 시의적절하다고 확신합니다.

특히 한국은 전 세계가 주목하는 IT강국으로, 정보화시대 특유의 사회현상도 먼저 겪고 있습니다. 한국은 다양한 선행 경험을 통해 국제사회의 정보인권 논의를 풍부하게 할 책임도 있다고 믿습니다.

한국인권위는 정보인권에 관한 한국의 축적된 경험과 논의를 국제적으로 널리 공유하기 위한 방법을 찾아 오늘 바로 이 자리의 사전회의를 마련하게 되었습니다.

오늘 회의의 주제는 “정보화 사회에서의 프라이버시권과 표현의 자유의 균형적 조화”이며, 한국 시민사회의 대표적인 정보인권 논의를 접할 수 있는 좋은 기회가 될 것입니다.

이번 사전회의는 아셈 인권세미나에서 최초로 시도되는 것이고, 오늘 논의 결과는 아셈 인권세미나 본회의에도 보고되어 반영될 예정입니다.

따라서 오늘 회의가 정보인권의 현안에 대해 진단하고 해법을 모색하는 자리가 되기를 기대합니다.

끝으로 그동안 시도되지 않았던 사전회의가 개최될 수 있도록 관심과 지원을 해주신 ASEF 운영위에 특별히 감사의 말씀을 드립니다.

다시한번 오늘 회의에 참석하여 자리를 빛내 주신 모든 분들께 감사드리며, 이번 회의가 훌륭한 성과를 내는 자리가 되기를 기대합니다. 감사합니다.

2012. 6. 27.

국가인권위원회 상임위원 **홍 진 표**

Opening Remark

Good morning,

Our distinguished guests, ladies and gentlemen,

I am Jin-pyo Hong, Standing Commissioner of the National Human Rights Commission of Korea.

First of all, I would like to extend my sincere gratitude to distinguished guests and all participants here for the Side Event of the 12th ASEM Informal Seminar on Human Rights.

Information and Communication Technology (ICT) is a relatively new issue in human rights field. Entering the informationized society, mankind is benefiting from ICT, however, it also brings about unprecedented issues such as personal data protection and the right to freedom of expression in the virtual world.

As the development of ICT is fundamentally transforming the world, it is well-timed to discuss "Information Communication Technology and Human Rights" as a topic of the ASEM Informal Seminar on Human Rights this year.

In particular, Korea is experiencing extraordinary social phenomenon of the Informationized society as a country of leading ICT. With its abundant precedents, Korea

has responsibility to enrich discussions on Information and Human Rights in the international community.

In light of current circumstances, the National Human Rights Commission of Korea is hosting the side event here in order to publicize Korea's cumulated experiences and knowledge internationally.

Today's theme is "Balance between the Right to Privacy and the Right to Freedom of Expression in the Informationized Society", which is one of the hottest issue in the society.

The side event is the first case in the series of ASEM Informal Seminar on Human Rights. Its discussion outcomes will be reported at the plenary session tomorrow.

In this regard, I hope this meeting serves as a forum to explore countermeasures to existing concerns in the area of Information and Human Rights.

Lastly, I would like to express my special gratitude to ASEF with their support to the side event.

Again, I welcome everyone here and wish you bring a fruitful outcome from this conference.

Thank you.

June 27, 2012

Standing Commissioner of NHRCK **Hong Jin-pyo**

프로그램

❖ 일시 : 2012년 6월 27일(수) 09:30～12:00
❖ 장소 : 플라자 호텔, 그랜드 볼룸(B2)

09:00 ~ 09:30	회의참가 등록	
09:30 ~ 09:40	개 회	사 회 : **김일환** (성균관대학교 법학전문대학원 교수) 개회사 : **홍진표** (국가인권위원회 상임위원)
09:40 ~ 09:50	이벤트 시연	포털사이트를 통한 주민등록번호에 의한 신상털기 시연 **박성훈** (국가인권위원회)
09:50 ~ 10:30	주제발표	• "정보프라이버시권 : 한국에서의 도전과 응전" **이인호** (중앙대학교 법학전문대학원 교수) • "정보환경의 변화와 표현의 자유" **이민영** (가톨릭대학교 법학부 교수)
10:30 ~ 11:40	패널토론	• **김범수** (연세대학교 정보대학원 교수) • **전응휘** (녹색소비자연대 상임이사) • **장용근** (홍익대학교 법학부 교수) • **Wolfgang Benedek** (Professor at the Faculty of Law at Graz University) • **Andrew Puddephatt** (Director of Global Partners)
11:40 ~ 12:00	전체토론 폐 회	• 전체토론 • 폐회사 **Michel Filhol** (Executive Director, Asia-Europe Foundation)

Program

❖ 12th Informal ASEM Seminar on Human Rights

09:00 ~ 09:30	Registration	
09:30 ~ 09:40	Opening Remark	• Moderator **KIM, Il-Hwan** (Professor, Law School of Sungkyunkwan University) • Opening Remark **HONG, Jin-Pyo** (Standing Commissioner, National Human Rights Commission of Korea)
09:40 ~ 09:50	Technical Demonstration	Demonstration of scanning personal data by searching resident registration numbers on a public web portal **PARK, Seong-Hoon** (National Human Rights Commission of Korea)
09:50 ~ 10:30	Presentation	• Right to Information Privacy: Korea's Challenges and Response **LEE, In-Ho** (Professor, Chungang University) • The Changing Information Environment and its Implications for Freedom of Expression **LEE, Min-Yeong** (Professor, Catholic University of Korea)

❖ 12th Informal ASEM Seminar on Human Rights

10:30 ~ 11:40	Panel Discussion	• **KIM, Beom-Soo** (Professor, Yonsei University) • **CHUN, Eung-Hwi** (Standing board member, Green Consumer's Network) • **CHANG, Young-Kuen** (Professor, Hongik University) • **Wolfgang Benedek** (Professor, Graz University) • **Andrew Puddephatt** (Director of Global Partners)
11:40 ~ 12:00	Plenary Discussion Closing Remark	• Plenary Discussion • Closing Remark **Michel Filhol** (Executive Director, Asia-Europe Foundation)

목 차

❖ 제12차 아셈인권세미나 사전회의

❖ 제12차 아셈인권세미나 사전회의

주제발표

"정보화 사회에서의 프라이버시권과 표현의 자유의 균형적 조화"

■ **이 인 호** (중앙대학교 법학전문대학원 교수)
■ **이 민 영** (가톨릭대학교 법학부 교수)

주제발표

“정보프라이버시권 : 한국에서의 도전과 응전”

이 인 호

(중앙대학교 법학전문대학원 교수)

Ⅰ. 감시의 일상화와 역감시체계 구축의 과제

디지털 정보기술로 촉발된 정보사회(information society)는 한 마디로 “기록사회”(recording society)이다. 모든 것이 기록된다. 시민 개인의 일상적인 삶의 궤적들이 누군가에 의해 디지털정보로 기록되고 가공 혹은 분석되어 이용된다. 그리고 이렇게 처리된 그 개인기록은 지워지지도 않은 채 무한히 복제되어 또 다른 사람들에 의해 공유되고 또 쉽게 통합된다.

얼마 전까지만 해도 이런 현상은 컴퓨터로 네트워크화된 사이버공간에서만 일어나는 것으로 생각되었다. 그러나 최근의 BcN(Broadband Convergence Network), USN(Ubiquitous Sensor Network), RFID(Radio Frequency Identification), IPv6 등의 유비쿼터스 기술은 상호작용하는 소형컴퓨터를 사물 속에 심어 그 사물의 속성과 관련 정보를 외부에 전달하고 공유하게 만들고 있다. 사이버공간과 현실공간의 구분이 모호해지게 된 것이다.

향후의 유비쿼터스 사회(ubiquitous society)에서는 사회의 전 구성원들이 언제 어디서나 네트워크로 연결되어 커뮤니케이션하는 단계(P2P: Person to Person)를 거쳐, 사람과 사물이 언제 어디서나 연결되는 단계(P2O: Person to Object)를 지나, 종

국에는 사물과 사물이 자동으로 커뮤니케이션하는 단계(O2O: Object to Object)로 발전해 갈 것이다. 이 사회에서 사람들은 컴퓨터나 네트워크를 의식하지 않고 시간과 장소에 상관없이 네트워크에 접속되어 다른 사람 또는 사물과 커뮤니케이션을 하게 될 것이다. 이러한 유비쿼터스 환경은 우리들에게 새로운 편익과 혜택, 그리고 무한한 가능성을 제공해 주겠지만, 그 역기능도 결코 만만치 않다. 특히 유비쿼터스 사회는 "감시사회"(surveillance society)의 본질을 필연적으로 가지고 있다.

유비쿼터스 사회에서 감시(surveillance)는 개인의 삶에서 떼려야 뗄 수 없는 일부분으로 상존하게 될 것이다. 실로 개인의 모든 것이 기록되고 저장되며 공유될 것이다. 유비쿼터스 컴퓨팅 시스템(Ubiquitous Computing System)은 개인의 신원(identity), 위치(location), 활동(activity), 그리고 주변의 상황(context)에 관한 개인정보를 자동적으로 그리고 실시간(real time)으로 수집하고 공유할 것이다.

유비쿼터스 환경에서의 놀라운 감시기술(surveillance technologies)들은 개인의 공적 삶이든 사적 삶이든 그 일거수일투족을 추적할 뿐만 아니라 그 추적의 결과들을 자동으로 저장·처리하여 개인의 프로파일을 만들 것이다. 더 나아가, 이렇게 디지털화된 개인기록들은 손쉽게 통합되어 개인의 실존인격과 분리된 또 다른 디지털인격을 형성하게 된다.

나의 삶의 하나하나가 추적당한다는 느낌은 나의 자유의 습관을 변화시킬 것이다. 감시가 점차 내면화되면 될수록 나의 인격의 주체성은 조금씩 상실되어 갈 것이다. 더불어 나의 자유의 공간은 그 만큼 축소되어진다. 더 나아가, 내가 인식하지도 못한 채 형성되어 있는 또 다른 나의 디지털인격이 지워지지도 않은 채 나의 실존인격을 규정짓게 될 것이다. 나에 관한 정부와 시장의 결정은 나의 실존인격이 아닌 디지털인격에 기초해서 내려질 것이기 때문이다.

그러나 개인 인격의 주체성 및 자유의 확보는 자유민주주의체제의 포기할 수 없는 전제조건이다. 개인의 삶에 대한 총체적인 감시체계는 자유민주주의체제의

전제조건을 훼손할 위험성을 안고 있다.

그렇지만 한편으로 이 위험성 때문에 기술의 발전과 진보를 막을 수는 없다. 기술의 위험성과 유용성은 결국 그것을 사용하는 사회체계의 선택에 달려 있는 문제이다. 현 시점에서 우리에게 주어진 과제는 정보기술의 발전이 개인의 프라이버시에 던지는 위험성을 최소화하면서 동시에 개인정보처리의 국가적 및 사회적 이익을 수용할 수 있는 역감시의 모델을 정립하고 그것을 사회체계 속에 구현해나가는 일이다.

그런데 이 같은 역감시의 모델을 정립함에 있어서 문제해결을 더욱 어렵게 만드는 요인은, 개인의 삶 속에 일상화된 감시가 그 나름의 정당성을 가지고 있다는 점이다. 현대의 국가는 단순히 물질적 생산조건의 확보라는 기능을 넘어서서 복지나 사회정책 등 사회적 재생산조건을 보장하기 위한 기능을 담당하게 되었고, 이러한 기능을 효율적으로 수행하기 위해서는 무엇보다 개인정보의 수집과 처리가 불가결한 요소가 되고 있다. 특히 최근에는 정보기술의 활용을 통하여 대국민 고객지향성이라는 이념 하에 작고 효율적인 시민위주의 질 좋은 행정서비스를 제공한다고 하는 전자정부의 개념이 구체화되고 있다. 이전의 김대중 정부와 노무현 정부, 그리고 현재의 이명박 정부는 개인정보를 포함한 행정정보의 공동이용을 전자정부의 핵심요소 중의 하나로 인식하고 있다. 효율적인 법집행과 국민의 안전, 복지사기의 방지, 조세포탈의 방지, 국민보건의 증진, 대국민서비스의 향상 등은 개인정보처리의 필요성과 당위성을 강화시켜 준다. 한편, 시장에 있어서도 기업에 의한 고객의 개인정보처리는 자원배분의 효율성을 극대화할 뿐만 아니라 소비자인 정보주체에게는 거부할 수 없을 정도의 달콤하고 편리한 이익을 안겨준다. 기업과 사회는 개인정보의 처리를 통해서 자원배분의 효율성을 극대화하게 되며, 정보기술이 개인에게 제공하는 편익과 안락 또한 개인정보의 수집과 공유를 전제로 해서 가능하게 된다.

우리의 고민은 여기에서부터 시작된다. 요컨대, 우리에게 던져진 핵심적인 과제

는 “감시의 정당성을 훼손하지 않으면서 그 위험성을 상쇄시킬 수 있는 역감시체계를 구축하는 일”이라고 하겠다.

이를 위해서는 (ⅰ) 먼저, 감시체계의 정당성을 엄밀하게 규명하여야 한다. 표면적으로 주장되는 감시기능의 정당성이 진정한 것인지를 해명하는 작업이 필요하다. (ⅱ) 다음으로, 감시체계를 운영하는 자가 정당한 목적과 권한을 가지고 있는지, 필요한 범위를 넘어서고 있는지, 정당한 절차에 따라 운영되고 있는지를 엄밀하게 검증하여야 한다. 그러기 위해서는 그 검증의 기준을 명확하게 밝혀내어야 한다. (ⅲ) 감시체계를 설계하고 디자인하는 단계에서부터 역감시체계가 작동하여야 한다. (ⅳ) 역감시체계를 어떻게 구축할 것인지 그 합리적인 방법을 모색하여야 한다. (ⅴ) 역감시체계가 효과적으로 작동할 수 있는 방안을 모색하여야 한다.

Ⅱ. 역감시체계의 규범적 접근: 개인정보자기결정권과 개인정보보호법

1. 개인정보처리의 효용과 위험성

오늘날 모든 공·사의 기관들은 자신들의 업무수행을 위하여 개인에 관한 수많은 정보들을 디지털화된 형태로 가지고 있다. 인구학적 기본통계, 교육, 재정, 의료, 신용정보, 고용, 납세, 출입국, 치안관련자료, 사회복지, 군복무, 자동차관리, 백화점, 사회단체, 금융 등과 관련한 개인정보는 일부에 지나지 않는다.

그런데 디지털화된 개인정보는 관리의 측면에서 이전과 비교할 수 없는 효율성을 가지게 된다. 발전된 DBMS(Database Management System)의 활용으로 인해 개인에 대한 정보의 입력, 처리, 검색, 출력이 신속하고 정확하게 이루어질 뿐만 아니라 더 나아가 표준식별번호(universal identification number)에 의한 컴퓨터결합(computer matching)을 통해 분산되어 있는 개인정보들을 용이하고 효율적으로 통

합·처리할 수 있게 되었다.

이러한 디지털기술에 의한 개인정보의 처리는 정부와 사회에 커다란 효용을 가져다준다. 국가기능의 효율적인 수행은 국민들의 개인정보의 효과적인 처리에 달려 있다. 기업과 사회도 개인정보의 처리를 통해서 자원배분의 효율성을 극대화하게 되며, 정보기술이 개인에게 제공하는 편익과 안락 또한 개인정보의 수집과 공유를 전제로 해서 가능하게 된다.

예컨대, 정부는 사회복지행정에 있어서 복지서비스를 받는 개인에 관한 정보를 통합 관리함으로써 정부서비스의 효율성을 제고시킬 뿐만 아니라 복지사기를 방지하여 예산낭비를 줄일 수 있다. 그밖에도 개인정보의 통합관리와 공동이용은 범죄수사, 치안, 세무행정, 교육 등 각 분야에서 능률의 향상을 가져온다. 예컨대, 컴퓨터결합(computer matching)이나 컴퓨터 프로파일링(computer profiling) 내지 데이터마이닝(data mining)의 기법을 통해 관련 자료들을 분석함으로써 범죄자나 위험인물 등을 미리 분류하여 사전 예방할 수 있으며 세무관리와 소비관리 등을 통하여 탈세혐의자 등을 쉽게 포착해 낼 수 있다.

또한 기업의 경우 개인정보데이터베이스를 활용한 DB마케팅 활동은 기업의 주된 경쟁력의 원천으로 인식되고 있고, 실제로 고객의 개인정보를 얼마나 확보하느냐가 기업 마케팅전략의 중요 부분을 차지한다. 그리하여 통신서비스업체, 유통업체, 항공사, 금융기관 등은 고객의 평소 이용행태를 분석해 관련 데이터를 자세히 기록해두고 영업에 반영하는 지식기반영업시스템을 도입하고 있는데, 이는 기술적으로 데이터웨어하우징(Data Warehousing)이라는 시스템에 의하여 운영된다. 이 시스템을 통하여 월별, 성별, 연령별 고객과 매장별, 상품별 매출추이를 분석해보면 어느 매장에서 특정한 고객이 특정한 상품을 특정한 기간에 잘 구매한다는 등의 고객성향을 알 수 있고 이를 바탕으로 여러 가지 경영전략이나 효율적인 마케팅활동을 할 수 있게 되는 것이다.

최근 전자상거래의 발전으로 인해 고객의 개인정보 처리는 더욱 용이하게 되었

을 뿐만 아니라 더욱 필요하고도 불가피한 것이 되어 가고 있다. 전자상거래를 통해 수집・분석된 소비자의 개인정보가 기업들의 마케팅에 활용될 경우, 기업과 소비자 모두에게 유익한 측면이 있기 때문이다. 특히 개인정보가 국경을 초월하여 국제적으로 수집・관리되고 분석될 경우, 국제상거래활동에 크게 기여할 뿐만 아니라 소비자들에게도 폭넓은 선택의 기회를 부여할 수 있다. 다시 말해서, 이제 기업은 극히 적은 비용과 노력으로 세계 각국의 소비자들의 소비행태를 분석할 수 있고 특정 소비자가 현재 어떤 상품에 관심을 갖고 있는지를 정확히 분석해 낼 수 있기 때문에 소비자의 니즈(needs)를 정확히 반영해서 당해 소비자를 공략할 수 있고 소비자로서도 세계 각지로부터 적기에 필요한 상품정보를 받아 볼 수 있게 되는 것이다. 결국 고객의 개인정보의 처리 및 활용은 시장에 있어서 자원배분의 효율성에 기여한다는 긍정적인 측면을 가지고 있다.

그러나 이러한 효용에 못지않게 개인정보처리의 위험성도 동시에 증가하고 있다. 나의 실존인격을 완전하게 반영하지 못하는 왜곡된 디지털인격이 갖는 위험성은 개인정보를 수집・처리・이용하는 각 국면에 따라 다양한 형태로 표출되어 나타난다.

첫째, 개인정보의 정확성(accuracy)의 문제이다. 데이터베이스에 수록된 개인정보가 실제와 다른 경우 그러한 틀린 개인정보에 기초해서 정책결정(정부부문)이나 경영결정(시장부문)이 행하여진다면 그것이 개인의 사회생활에 미치는 파장은 대단히 심각해진다. 그렇기 때문에 개인정보는 정확하게 입력되어야 할뿐만 아니라 잘못된 정보에 대한 수정이 신속하게 이루어져야 하는 것이다. 또한 시간이 경과하여 이미 입력된 자료의 내용이 시의성을 가지지 못하는 경우에도 개인정보의 정확성을 해치게 된다.

둘째, 개인정보의 완전성(integrity)의 문제이다. 이는 주로 개인정보를 처리하는 과정에서 발생하는데, 예컨대 컴퓨터연결의 과정에서 적절하지 못한 방식으로 개

인자료가 통합되거나 재분류되는 경우 출력된 개인정보는 정보주체를 완전하게 반영하지 못하게 된다. 또한 처리프로그램의 내재적인 문제로 인하여 출력된 개인정보가 체계적으로 왜곡될 수도 있다. 이러한 문제는 하드웨어의 오작동이나 조작자의 실수에 의해 복합적으로 나타날 수도 있다. 이처럼 체계적으로 왜곡된 개인정보에 의하여 실존인격이 규정되는 경우 그 위험성은 더욱 커지게 된다.

셋째, 개인정보의 보안성(security)의 문제이다. 이는 개인정보의 관리과정에서 발생하는 문제로서 외부 또는 내부에 의한 불법적인 침입에 의해 개인정보가 누출되는 경우이다. 정보통신망의 확산으로 인해 개인정보의 데이터베이스는 다른 물리적 공간에 존재하지만 상호 연결되어 있기 때문에 외부의 침입에 취약할 수밖에 없게 되었다. 최근 해킹이나 크래킹에 의한 불법적인 침입은 보안기술의 발달에도 불구하고 줄어들지 않고 있다. 또한 보안성은 내부자에 의해 의도적으로 침해될 수 있다. 즉 개인정보 데이터베이스에 합법적으로 접근할 수 있는 사람이 개인적인 이득을 취하기 위하여 개인정보를 외부에 유출하는 경우이다.

넷째, 개인정보의 적합성(adequacy)의 문제를 들 수 있다. 이것은 개인정보의 수집 및 이용과정에서 수집목적의 정당성 및 이차적 이용의 타당성에 관련된 문제이다. 개인정보 데이터베이스는 주로 특정한 목적을 위하여 구축되는데, 그렇게 구축된 개인정보가 본래의 수집목적이나 취지를 벗어나서 사용되는 경우 적합성의 위반문제가 발생한다.

이처럼 정보 입력의 정확성, 정보 처리의 완전성, 정보 관리의 보안성, 정보 이용의 적합성이 확보되지 않는 경우 개인정보의 왜곡이 일어나게 되고, 그에 따르는 위험성은 실존인격에 치명적인 손상을 가할 수도 있게 된다.

한편 더 나아가, 개인정보를 축적·처리하는 공·사의 기관은 개인에 대한 강력한 통제와 감시의 수단을 확보하고 있는 셈이다. 그리하여 이들 개인정보를 토대로 일정 부류의 사람들을 사회적으로 낙인을 찍는 일(예컨대, 신용불량자나 취업

기피인물명단의 작성・유통)이 얼마든지 가능해지게 되고, 그 결과 그들을 사회로부터 고립시키거나 선택권을 제한하게 만들 수 있다.

또한, 개인정보의 수집・처리가 일상화되면서, 정보주체는 자신의 삶의 하나하나가 추적당한다는 느낌을 갖게 되고 그것은 곧 그의 자유의 습관을 변화시킬 것이다. 감시가 점차 내면화되면 될수록 그의 인격의 주체성은 조금씩 상실되고 더불어 자유의 공간은 그 만큼 축소되어져 갈 것이다. 사실 개인 인격의 주체성 및 자유의 확보는 자유민주체제의 포기할 수 없는 전제조건이다.

2. 새로운 위협에 대한 법적 대응

기록과 감시의 일상화 속에서 그 위험성을 최소화하면서 개인정보처리의 국가적 및 사회적 이익을 수용하기 위한 균형추로서 제시된 것이 정보인권으로서의 개인정보기결정권(Recht auf informationelle Selbstbestimmung; Information Privacy)이다. 그리고 이 정보인권을 구체화하는 법률인 '제2세대 프라이버시보호법' 내지 '개인정보보호법'이 1970년대 초부터 선진 각국에서 채택되기 시작하였다.

1960년대 컴퓨터 및 디지털기술이 등장한 이래 1970년대 초부터 이미 개인정보의 자동처리에 따르는 위험성을 인식하고 그로부터 개인의 프라이버시를 보호하기 위한 규범적 대응방안이 마련되었다. 유럽에서는 최초로 스웨덴이 1973년에 공공부문과 민간부문에서의 개인정보처리를 규율하는 법률(Data Act of 1973)을 제정하였으며, 이후 독일, 덴마크, 오스트리아, 프랑스, 노르웨이, 룩셈부르크가 모두 1978년에, 영국이 1984년에, 네덜란드가 1988년에 각각 개인정보보호법을 제정하였다. 한편, 미국은 스웨덴보다 1년 늦었지만 세계에서 두 번째로 1974년에 공공부문을 규율하는 개인정보보호법인 「프라이버시법」(Privacy Act of 1974)을 제정하였다.

또한 1980년대 이후에는 국제기구들이 개인정보를 보호함과 동시에 개인정보의 국제적 유통을 원활히 하기 위하여 개인정보처리의 기본원칙들을 확인하여 오고

있다. 이들 원칙은 1980년의 경제협력개발기구(OECD) 가이드라인,[1] 1980년 유럽평의회(Council of Europe)의 개인정보보호협약,[2] 1990년 국제연합(UN)의 가이드라인,[3] 1995년 유럽연합(EU)의 개인정보보호지침[4] 등에 구현되어 있다. 그리고 이 기본원칙들은 각국의 개인정보보호법에 개인정보처리기관의 의무와 정보주체의 권리의 모습으로 다양하게 구체화되고 있다.

Ⅲ. 개인정보자기결정권에 대한 오해

한국에서 1995년에 공공부문 개인정보보호법(「공공기관의 개인정보보호에 관한 법률」)이 시행된 이래 2012년 현재까지 17년여 동안 개인정보처리의 허용기준과 관련하여 한국 사회에서 가장 논쟁적이었던 이슈를 든다면, 개인정보의 처리(=수집・이용・제공)에 있어서 정보주체의 동의 요건을 합법적인 개인정보처리의 원칙적인 기준으로 설정할 것인가 하는 문제였다.

다시 말해서, 개인정보처리자는 정보주체의 동의 없이는 다른 사람의 개인정보를 원칙적으로 수집・이용・제공할 수 없도록 해야 하는가? 정보주체의 동의를 받지 않고 합법적으로 처리(=수집・이용・제공)할 수 있는 경우를 어느 정도 허용할 것인가? 개인정보자기결정권 내지 자기정보통제권(Recht auf informationelle Selbstbestimmung; Informational Privacy)[5]이라고 하는 것이 정보주체의 동의 없는

1) 「프라이버시보호 및 개인정보의 국제적 유통에 관한 가이드라인」(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data).
2) 「개인정보의 자동처리와 관련한 개인의 보호를 위한 유럽이사회 협약」(Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 September 1980).
3) 「컴퓨터화된 개인정보파일의 규율을 위한 가이드라인」(Guidelines for the Regulation of Computerized Personal Data Files).
4) 「개인정보의 처리 및 자유로운 전송에 관한 개인보호 지침」(Directive of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data; 95/46/EC).
5) 독일 연방헌법재판소는 1983년의 인구조사판결(BVerfGE 65, 1)에서 "정보적 자기결정권"(Recht auf informationelle Selbstbestimmung)을 처음으로 인정하였다.

개인정보의 처리를 원칙적으로 금지시키는 것인가?

이 문제는 타인이 수집하여 처리・이용하고 있는 나의 개인정보는 누구의 것이며, 정보주체인 나는 그 개인정보에 대하여 어느 정도의 인격적 이익을 가지며 또 어느 정도의 통제권을 가지는가 하는 문제이다.

2005년 5월 26일 헌법재판소는 「주민등록 지문정보DB 사건」[6]에서 처음으로 개인정보자기결정권을 "새로운 독자적인 기본권"으로 인정하는 결정을 내렸다. 이 사건에서는 주민등록 목적으로 수집된 시민의 지문정보를 범죄수사목적으로 활용하는 공권력행사가 다투어졌다. 즉, 행정안전부장관이 주민등록증(=성인 시민에게 발급되는 신분증명카드)을 발급하는 과정에서 신원확인 목적으로 수집한 성인 시민 3,900만 명 이상의 열 손가락 지문정보[7]를 경찰청장에게 넘겨 경찰청이 이를 보관하면서 전산화하여[8] 범죄수사목적에 활용하는 것이 문제가 된 것이다. 이 사건에서 헌법재판소는 이러한 지문자동검색시스템(Automatic Fingerprint Identification System: AFIS)의 가동으로 인하여 지문정보의 주체인 청구인들의 개인정보자기결정권이 제한되고 있음을 인정하였다. 그렇지만 정당한 목적의 달성을 위해 필요한 제한이라는 이유로 6(합헌) : 3(위헌)으로 합헌결정을 내렸다.

헌법재판소는 "현대의 정보통신기술의 발달[에 따라] 개인정보의 수집・처리에 있어서의 국가적 역량의 강화로 국가의 개인에 대한 감시능력이 현격히 증대"되는 상황을 이 새로운 기본권을 승인하는 사회적 배경으로 제시하였다. 그리고 이 새로운 기본권은 그 내용이 기존의 기본권조항(제10조 제1문의 인간의 존엄과 가

---

6) 헌재 2005. 5. 26. 99헌마513등 (주민등록 지문정보DB 사건) [6(합헌) : 3(위헌)].

7) 주민등록증 발급과 관련한 열 손가락 지문날인제도는 1975. 8. 26. 시행된 주민등록법시행령(대통령령)에서 처음 도입되었다.

8) 경찰청에서는 1990년부터 지문자동검색시스템(AFIS)을 도입하여 가동하기 시작하였다. 이 시스템은 개인의 인적 사항, 열 손가락 지문 등이 포함되어 있는 주민등록증발급신청서를 고속의 대용량컴퓨터에 이미지 형태로 입력한 다음, 필요시 단말기에 현출시켜 지문을 확인하거나 또는 변사자의 인적 사항 및 현장유류지문을 자동으로 검색하여 동일인 여부를 확인하는 시스템이다. 그리고 1990. 10.경 최초로 지문정보를 컴퓨터에 입력하기 시작하여 1998. 2. 이전까지는 좌우 손가락 세 개씩 여섯 손가락 지문만을 입력하고, 그 이후에는 열 손가락 지문 모두를 입력하는 방식으로 2003. 6. 15. 당시까지 경찰청이 보관하고 있던 약 3,900만 명의 지문정보에 대한 전산화가 완료되었다.

치 및 행복추구권, 제17조의 사생활의 비밀과 자유)과 헌법원리(전문의 자유민주적 기본질서, 국민주권원리, 민주주의원리) 중 어느 하나에 완전히 포섭될 수 없는 것이라고 하면서, "오히려 개인정보자기결정권은 이들을 이념적 기초로 하는 독자적 기본권으로서 헌법에 명시되지 아니한 기본권"이라고 판시하고 있다.

이 결정에서 헌법재판소는 "개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다."고 규정하였다. 그리고 이 권리의 보호대상이 되는 개인정보는 "개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서의 형성되었거나 이미 공개된 개인정보까지 포함"하며, 그러한 개인정보를 대상으로 하는 "조사・수집・보관・처리・이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다."고 판시하고 있다.

그런데 개인정보자기결정권에 대한 헌법재판소의 이러한 판시는 자칫 오해를 불러일으킬 수 있다. 마치 수집에서부터 이용 및 제공에 이르기까지 정보주체가 그 과정을 직접적으로 결정하거나 통제할 수 있는 권리인 것처럼 오해될 소지가 있다. 그러나 개인정보자기결정권은 개인정보처리자가 행하는 개인정보처리의 전 과정을 "직접적으로 결정하거나 통제하는 권리"는 아니다. 개인정보처리의 결정권은 개인정보를 처리하는 자에게 있다. 대신에 정보주체의 개인정보자기결정권은 그러한 처리의 과정에 "참여하는 권리"이다. 나에 관한 정보가 누구에 의해서 어떻게 수집・이용・제공되고 있는지를 알 권리(열람청구권), 분명한 처리목적을 설정하고 그 목적달성에 필요한 만큼의 정보만을 처리하도록 요구할 권리, 정보의 정확성과 최신성을 유지하기 위하여 틀린 정보나 낡은 정보를 수정하거나 삭제를 요구할 권리, 권한 없는 자에 의한 정보접근을 제한하고 부당한 누출의 방지를 요구할 권리 등이 개인정보자기결정권의 내용이다.[9]

9) 그런데 위 「주민등록 지문정보DB 사건」의 본안판단에서 헌법재판소는 이러한 개인정보자기결정권의 내용에 주목하지 않았다. 3,900만 명에 달하는 거대한 국민의 지문정보를 주민등록의 신원확인목적으로 수집해서 경

최근 한국 사회에서 개인정보보호를 절대화하려는 경향이 발견되고 있다. 이런 경향에 의하면, 정보주체의 동의 없는 개인정보의 수집・이용・제공은 원칙적으로 불법이라고 평가된다. 그러나 이것은 개인정보자기결정권을 잘못 이해한 결과이다. 자칫 이러한 경향은 우리 사회에서 필요한 개인정보의 이용과 유통의 사회적 가치를 몰각하고 모든 개인정보를 비밀정보로 취급하는 우를 범할 수 있다.

개인정보가 정보주체의 인격적 징표이지만 그 인격적 징표 그 자체를 가두어두고 보호하려고 해서는 안 된다. 사회의 존립과 기능유지는 많은 경우 타인에 대한 정확한 평가에 기초하고 있다. 그리고 타인에 대한 평가가 가능하기 위해서는 그의 인격적 징표가 유통될 수 있어야 한다. 만일 개인정보를 인격적 징표라는 이유만으로, 그리하여 마치 정보주체의 동의 없는 개인정보의 유통의 금지를 인격권이나 개인정보자기결정권의 한 내용으로 오해한다면, 누구든지 자신에게 불리한 인격적 징표의 유통을 금지하고자 할 것이고 그렇게 되면 사회는 그에 대한 정확한 평가를 내리는 것이 불가능하게 될 것이다. 그 종국적 결과는 사회의 정상적인 기능의 마비 내지 위축으로 나타날 것이다.

불행하게도 이러한 우려가 2011. 3. 29. 공포되어 2011. 9. 30. 시행된 「개인정보보호법」에서 현실화되었다. 이 법률은 종래 개인정보보호를 위한 개별입법들이 공공부문과 민간부문으로 이원화되어 영역별로 존재하고 있던 것[10]을 공공부문과 민간부문을 포괄하여 규율하기 위한 '일반법'으로 제정된 것이다.[11] 그런데 이 법

찰청이 이를 전산화하여 본래의 수집목적이 아닌 범죄수사목적으로 이용하는 것에 대하여 개인정보의 정확성・완전성・보안성・적합성을 충분히 담보할 수 있는 규범체계 및 사실상의 안전장치가 제대로 갖추어져 있는지를 평가하였어야 했다.

10) 한국에서 개인정보보호의 문제를 본격적으로 법제화한 것은 1994년 1월 7일 공포된 「공공기관의 개인정보보호에 관한 법률」(1995. 1. 8 시행)이었으며, 곧 이어 민간부문에서 「신용정보의 이용 및 보호에 관한 법률」이 1995년 1월 5일 공포되었다(1995. 7. 6 시행). 그리고 온라인상의 개인정보보호를 최초로 법제화한 것은 1999년 2월 8일 「정보통신망 이용촉진 등에 관한 법률」(2000. 1. 1 시행)이다. 또한 2004년에는 민간부문에서의 유전정보(유전자검사의 결과로 얻어진 정보)의 이용과 보호를 특별히 규율하기 위한 「생명윤리 및 안전에 관한 법률」(2005. 1. 1. 시행)이 제정되었으며, 그리고 2005년에는 이동통신기술의 급속한 발달로 물류・보안・상거래 등의 영역에서 위치정보를 이용하는 다양한 서비스가 등장함에 따라 위치정보의 유출 및 오・남용으로부터 개인의 프라이버시 등을 보호하고 위치정보의 안전한 이용환경을 조성하기 위하여 「위치정보의 보호 및 이용 등에 관한 법률」(2005. 7. 28. 시행)이 제정되었다.

11) 이 법률에 의해서 기존에 공공부문을 규율하던 「공공기관의 개인정보 보호에 관한 법률」은 폐지되고 그 내

률은 일반법이면서도 지나칠 정도로 개인정보의 '보호'에 치우쳐 '이용'의 현실적 가치를 상당히 무시하는 우를 범하고 있는 것으로 평가된다. 아마도 세계에서 가장 강력한 개인정보보호법이 아닌가 생각된다. 그러나 자칫 사회적으로 필요한 개인정보의 이용과 유통을 과도하게 억제함으로써 타인에 대한 합리적인 평가에 기반하고 있는 정상적인 사회적 기제들을 위축시킬 우려가 높다.

이 법률은 '신원을 확인할 수 있는 개인에 관한 일체의 정보'를 보호의 대상으로 하면서도 그 개인정보 모두를 마치 개인의 '비밀정보'로 취급하여[12] 그 정보주체에게 거의 절대적인 통제권을 인정하고 있다. 즉, 개인정보의 수집의 경우 정보주체의 '동의'를 원칙으로 하면서 단지 몇 가지 예외를 설정하고 있으며(제15조, 제16조), 나아가 이용 및 제3자 제공에 있어서는 이러한 동의의 원칙을 더욱 강화하고 있다(제17조, 제18조). 이 규율에 따르면, 기업이 고객과의 거래관계에서 상품이나 서비스제공을 위해 수집했던 단순한 연락처정보(contact information)를 이용하여 다른 상품이나 서비스의 홍보 혹은 마케팅에 활용하는 것조차 '수집목적 외 이용'에 해당되어 정보주체에 의한 별도의 추가적인 동의를 받아야 하고, 별도의 추가적인 동의 없이 이를 활용하여 마케팅을 하면 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하여질 수 있다(제18조 제1항 및 제2항, 제71조 제2호). 또 기업이 고객과의 거래관계에서 분쟁이 발생하여 변호사의 법적 자문을 구하기 위해 거래관계에서 수집된 개인정보(간단한 신상정보조차도)를 그 정보주체의 별도의 동의 없이 변호사에게 제공하면 역시 '수집목적 외 제공'이 되어 형사처벌의 대상이 된다.

그 밖에도 이 법률은 정보주체의 권리로서 개인정보의 '정정・삭제요구권'을 아무

용이 이 법률에 흡수되었다. 그러나 기존에 민간부문에서 일부 영역별로 존재하던 개인정보보호법들(=「신용정보의 이용 및 보호에 관한 법률」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「생명윤리 및 안전에 관한 법률」, 「위치정보의 보호 및 이용 등에 관한 법률」)은 그 영역의 특별법으로서 계속 존속하고 있다. 따라서 일반법인 「개인정보보호법」은 이들 특별법이 규율하지 않는 민간의 다른 영역들에서의 개인정보처리를 규율한다.

12) 법률 제1조(목적)는 "개인정보의 수집・유출・오용・남용으로부터 사생활의 비밀 등을 보호"하는 것을 입법목적으로 명시하고 있다. 그러나 다른 나라의 개인정보보호법들은 개인정보의 '보호'와 '안전한 이용'의 조화를 입법목적으로 규정하고 있다.

런 제약 없이 인정하고 있다(제36조 제1항). 개인정보처리자는 정보주체로부터 요구를 받았을 때에는 지체 없이 그 요구에 따라 정정 혹은 삭제조치를 한 후 그 결과를 정보주체에게 알려주어야 한다(제36조 제2항). 이는 곧 정보주체 자신에게 불리한 정보를 마음대로 정정하거나 삭제할 수 있는 권능을 정보주체에게 주는 것이다. 그러나 정정・삭제요구권은 수집된 정보에 오류가 있거나 낡은 정보로 인해 정보처리의 정확성과 완전성이 훼손되어 있는 경우 또는 처리목적과 전혀 관련 없는 자신의 사생활을 침해할 수 있는 정보가 있는 경우에 한하여 인정되어야 할 것이다.

특히 우려되는 점은 「개인정보보호법」의 규율대상에 대한 오해이다. 이 법률은 "업무를 목적으로 개인정보파일(=개인정보DB를 가리킴)을 운용하는 개인정보처리자"를 그 규율대상으로 명시하고 있다(제2조 제4호 및 제5호). 그럼에도 불구하고 일부 전문가들은 개인정보DB의 운용과 관계없이 특정 개인에 관한 개인정보를 개별적으로 수집・이용・제공하는 행위에 대해서까지 이 법률의 규율대상인 것으로 확장해석을 하는 경향이 있는 것으로 보인다.

근래에 한국 사회에서 개인정보보호를 절대화하는 사고가 잘못 표출되어 나타난 또 다른 실례를 든다면, 경찰청이 범죄피해자를 긴급구조하기 위해 그 피해자의 위치를 추적할 수 있는 법률적 근거를 새로이 마련해야 하는지를 놓고 정치권에서 논란이 벌어졌던 사례를 들 수 있다.

그 동안 「위치정보의 보호 및 이용 등에 관한 법률」에는 긴급구조를 위한 위치추적을 소방방재청과 해양경찰청만이 할 수 있도록 되어 있었는데, 2012년 4월 1일 발생한 수원의 살인사건에서 경찰청이 피해자의 신고를 받고도 위치추적을 하지 못해 결국 피해자가 성폭행범에 의해 살해되는 어처구니없는 사건이 발생하면서, 경찰청도 긴급구조를 위한 위치추적을 할 수 있도록 법률이 신속하게 개정되어야 한다는 여론이 일었다. 국회에서는 2008년에 이미 경찰청의 위치추적을 허용하는 개정법률안이 발의되어 있었던 상태였는데, 그 동안 국회의 법제사법위원회에서 검찰 출신 위원들의 문제제기로 4년째 표류하고 있었던 것이다. 그 위원들의

문제제기는 '범죄피해자의 긴급보호도 수사의 첫 단계이므로 위치추적을 위해서는 검찰을 거쳐 법원에 영장을 신청해야 한다'는 것이었다고 한다. 그리고 2012년 4월에 신속한 법개정의 여론이 비등해졌는데도, 야당의 원내수석부대표는 '경찰에 자동위치추적권한을 주는 것은 사생활 침해 및 불법사찰 등에 악용될 우려가 있다'는 논리로 국회통과를 막고 있었다.

그러나 범죄피해자가 범죄로부터 자신을 구조해 달라고 요청하는데도 정부가 그 피해자의 사생활을 운운하면서 위치추적을 못한다는 것은 거의 코미디 수준이다. 범죄피해자는 구조를 요청할 때 이미 자신의 위치정보에 관한 프라이버시권을 포기한 것이다. 과거에도 위치정보법이 제정되기 전에 지리산에서 조난자가 휴대폰으로 구조를 요청한 뒤 전원이 꺼져 위치추적을 해야 하는 상황에서 구조당국은 위치정보보호라는 명분으로 머뭇거리다가 결국 조난자가 사망한 후 구조현장에 도달했던 딱한 사례가 있었다. 범죄피해자나 조난자의 중대한 생명과 신체를 놓고 그 정보주체의 사생활보호(위치정보프라이버시권)를 운운하는 것은 균형적 사고를 현저히 잃은 것임이 분명하다.

Ⅳ. 제2세대 프라이버시보호법으로서의 개인정보보호법의 특징

개인정보보호법은 제1세대 프라이버시보호법과 구별되어야 한다. 19세기 후반에 비로소 사생활의 비밀과 평온의 가치를 법적으로 보호해야 한다는 관념이 생겨나고 그러한 사생활의 가치가 프라이버시권(right to privacy)으로 승격되고 난 이후 1970년대에 개인정보보호법이 출현하기까지의 시기를 소위 "제1세대 프라이버시보호법 시대"라고 할 수 있다. 이 시기의 프라이버시보호법은 "보호할 가치있는" 개인의 사적 정보(private information)나 비밀정보(confidential information)에 "부당하게" 접근(access)하거나 혹은 그것을 "부당하게" 공표(public disclosure) 또는 누설(divulge)하는 행위를 형사적 또는 민사적 제재로써 "직접" 금지하여 왔다.

그러나 제2세대 프라이버시보호법으로서의 개인정보보호법은 신원을 확인할 수 있는 개인에 관한 일체의 정보(personal information)를 보호대상으로 하면서도 그것의 처리(=수집・이용・제공)를 금지하는 것이 아니라 정당한 업무수행목적의 처리를 허용하되 그 오・남용의 위험성을 막기 위해 공정한 처리(fair practice)를 요구한다. 이처럼 양자는 입법목적, 보호의 대상이 되는 개인정보의 범위, 규율대상이 되는 행위, 규율의 방식 등이 각각 다르다.

입법 목적	1세대 프라이버시보호법	현실적으로 발생한 해악(프라이버시침해)에 대해 제재를 가하고자 함
	개인정보보호법	업무수행과정에서 이루어지는 개인정보처리의 오・남용을 사전에 막음으로써 정보주체의 다양한 법익이 침해될 수 있는 위험을 예방하고자 하는 것임
규율 대상	1세대 프라이버시보호법	사생활평온을 깨뜨리는 행위
	개인정보보호법	개인정보DB의 형태로 처리되는 모든 개인정보의 처리과정
규율 방식	1세대 프라이버시보호법	침해의 기준을 설정하고 기준위반에 대해 민사적 또는 형사적 제재를 가함
	개인정보보호법	공정한 개인정보처리의 기준 설정, 정보처리과정에의 정보주체의 참여 보장, 감독기구에 의한 감시・고충처리・교육

개인정보보호법은 개인정보처리의 가치를 기본적으로 인정하면서 그 위험성을 예방하고자 하는데 근본취지가 있다. 외국의 모든 개인정보보호법은 이 점을 목적조항에서 명시하고 있다. 세계 각국 개인정보보호법의 입법모델이 되고 있는 1995년의 유럽연합의 개인정보보호지침(95/46/EC)은 제1조(이 지침의 목적)에서 두 가지 입법목적을 명시하고 있다: “1. 이 지침에 따라서, 회원국들은 자연인의 기본적인 권리와 자유, 특히 개인정보의 처리와 관련한 프라이버시권(right to privacy with respect to the processing of personal data)을 보호하여야 한다. 2. 회원국들은 위

제1항에 근거해서 주어지는 보호와 관련된 이유를 들어 회원국 사이의 개인정보의 자유로운 유통(the free flow of personal data between Member States)을 제한하거나 금지해서는 아니 된다." 이는 개인정보의 처리(=수집・이용・제공)를 금지한다는 것이 아니라, 그 처리를 허용하되 그 오・남용을 막음으로써 정보주체의 프라이버시권을 보호해야 하지만, 보호를 이유로 회원국 간의 필요한 개인정보의 유통을 막아서는 안 된다는 것이다.[13]

또한 일본의 기본법이면서 민간부문의 일반법인 「개인정보의 보호에 관한 법률」 제1조(목적)도 "이 법률은 고도정보통신사회의 진전에 따라 개인정보의 이용이 현저하게 확대되고 있는 점에 비추어, 개인정보의 적정한 취급과 관련하여 기본이념 및 정부에 의한 기본방침의 작성 기타 개인정보의 보호에 관한 시책의 기본이 되는 사항을 정하고, 국가 및 지방자치단체의 책무 등을 명확히 함과 동시에, 개인정보를 취급하는 사업자가 준수하여야 할 의무 등을 규정함으로써 개인정보의 유용성을 배려하면서도 개인의 권리이익을 보호하는 것을 목적으로 한다."고 규정하고 있다. 독일의 공공・민간부문을 포괄하는 일반법인 연방의 「개인정보보호법」(Datenschutzgesetz) 제1조도 개인정보가 저장, 전달, 수정 및 처리되는 과정에서 잘못 이용되지 않도록 함으로써 보호되어야 할 다른 개인의 권리와 이익이 침해되는 것을 막기 위한 것이 이 법의 목적임을 밝히고 있다.

때문에 개인정보보호법을 제정하고 해석함에 있어서 그 보호대상이 되는 "개인정보"를 마치 "사적 정보나 비밀정보"로 취급해서 그것을 수집하는 단계에서부터 금지해야 한다거나 혹은 그 처리과정에 정보주체의 동의를 필수적인 요건으로 설

---

13) 사실 위 유럽연합의 개인정보보호지침이나 1980년의 OECD 개인정보보호가이드라인은 세 가지 제정목적을 가지고 있었다. 첫째, 개인정보의 원활한 국제적 유통을 담보하기 위한 것이다. 경제가 세계화되면서 은행이나 보험과 같은 경제의 중요한 부문에서 개인정보의 국제적 유통은 필수적이기 때문이다. 둘째, 1970년대부터 OECD 회원국들은 각각 서로 상이한 개인정보보호법을 국내법으로 제정하기 시작하였다. 이러한 국내법 상호간의 법적 편차는 개인정보의 국제적 유통에 커다란 지장을 줄 수 있었기 때문에 이들 국가 간의 법적 편차를 줄이고 개인정보처리의 기준을 통일시킬 필요가 있었던 것이다. 이 점은 유럽연합의 개인정보보호지침의 제정의도이기도 하다. 셋째, 개인정보의 처리(=수집・이용・제공)에 따르는 개인의 권리나 이익의 침해를 막기 위한 안전장치를 법적으로 확보할 필요가 있었다.

정하거나 해석해서는 안 된다. 개인정보보호법은 정보주체에게 정보처리에 대한 전면적인 동의권을 부여하는 법률은 아니다. 다시 말해서, 개인정보보호법이 정보주체의 동의 없는 개인정보처리를 금지하는 것으로 이해해서는 안 된다. 정보주체의 동의는 개인정보처리의 기본적 요건이 아니라 부수적 요건이며, 동의가 있으면 당연히 법적으로 허용되는 수준을 넘어선 처리(=수집・이용・제공)가 가능하게 된다. 세계 어느 나라의 개인정보보호법도 정보주체의 동의를 개인정보처리의 기본적 요건으로 설정하고 있는 경우는 없다는 점에 유의할 필요가 있다.

다만, 개인정보보호법은 정보주체에게 정보처리과정에의 참여를 보장한다. 예컨대, 1980년의 OECD 개인정보보호가이드라인의 "개인 참여의 원칙"(Individual Participation Principle)에 의하면, (i) 정보주체는 자기에 관한 정보를 개인정보처리자가 가지고 있는지 여부를 확인할 권리(소재확인권)를 가지며, (ii) 자기에 관한 정보를 ① 합리적인 기간 내에 ② 과도하지 않은 비용으로 ③ 합리적인 방법에 의해 ④ 알기 쉬운 형태로 전달받을 권리(열람권)를 가진다. (iii) 그리고 소재확인권과 열람권이 거부되는 경우에 개인은 그 이유를 구하고(거부이유를 알 권리) 그 거부에 대하여 다툴 수 있는 권리(이의청구권)가 있으며, (iv) 그 다툼에서 이기는 경우에는 해당 정보의 삭제・정정・수정・보완을 요구할 권리(처리정보변경권)를 가진다.[14] 또한 유럽연합, 영국, 독일, 일본 등 대부분 국가의 개인정보보호법도

14) PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION.
Individual Participation Principle
13. An individual should have the right:
a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
b) to have communicated to him, data relating to him
within a reasonable time;
at a charge, if any, that is not excessive;
in a reasonable manner; and
in a form that is readily intelligible to him;
c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

기본적으로 이러한 권리 규정을 두고 있다. 더 나아가, 유럽과 일본은 정보주체의 동의 없는 정보처리를 광범위하게 허용하면서도, 일정한 경우 정보처리에 대한 사후거부권(right to object)을 정보주체에게 부여하고 있다. 또한 유럽은 일정한 형태의 "자동결정에 구속되지 않을 권리"를 정보주체에게 인정하고 있다.

이와 같이 제1세대 프라이버시보호법이 개인의 사적 영역을 외부의 침입이나 외부에의 공표로부터 소극적으로 보존하고자 하는 데에 초점이 맞추어져 있다면, 개인정보보호법은 개인정보의 수집·이용·제공을 원칙적으로 허용하면서 그에 따른 오·남용을 막기 위한 안전장치로서 정보주체에게 정보처리과정에 참여할 수 있는 권리(소재확인권, 열람권, 이의청구권, 처리정보변경권, 사후거부권)를 부여하고자 하는 법이다. 즉 종래의 사생활보호법이 "은둔으로서의 사생활보호"(privacy as seclusion)에 그 중심이 있었다면(이른바 "은둔모델"), 개인정보보호법은 "참여로서의 사생활보호"(privacy as participation)라는 접근방법을 취하고 있다(이른바 "참여모델"). 정보주체는 자신에 관한 정보가 누구에 의해 어떤 목적으로 어떻게 이용되는지를 명확하게 인식하고 그러한 정보처리의 과정에 함께 참여할 수 있어야 한다는 것이다. 이러한 참여로서의 프라이버시보호 모델은 특히 정부 또는 사기업이 개인정보처리의 오·남용을 통해 개인을 감시하고 통제하고자 하는 위험을 차단시키는 역감시의 기능을 수행한다.

개인정보보호법은 정보주체에게 이러한 참여권을 부여하는 외에도, 오·남용을 막기 위한 개인정보처리의 공정한 기준으로서 수집·이용·제공의 적법기준을 설정한다. 어떤 경우에 개인정보를 수집·이용·제공하는 것이 허용되는지를 규율한다. 이는 개인정보처리자에게 요구하는 실체적 요건이다. 또한 개인정보보호법은 개인정보의 정확성과 완전성을 담보하기 위하여 네 가지의 절차적 요건(목적명시 요건, 품질관리 요건, 고지 요건, 보고 요건)을 설정하고 이것을 개인정보처리자에게 요구한다. 더 나아가, 개인정보보호법은 정보주체의 참여권 보장만으로는 역감시의 기능을 충분히 담보할 수 없기 때문에 개인정보처리의 법적 기준을

준수하는지 여부를 예방적으로 감시·감독하는 독립된 감독기구를 설치한다.

이처럼 개인정보보호법은 디지털기록사회에서 기록과 감시의 일상화에 따른 새로운 프라이버시 위협에 대응하기 위하여 정보주체의 참여권 보장, 개인정보처리의 허용기준 마련, 개인정보처리에 있어서의 절차적 요건의 설정, 개인정보감독기구의 설치 등을 통하여 역감시의 체계를 구축하는 제2세대 프라이버시보호법이다.

Ⅴ. 역감시체계의 기본원칙

지난 30여년에 걸쳐 세계의 주요 국제기구와 각국은 개인정보처리와 관련한 정보주체의 프라이버시 보호를 위해 요구되는 개인정보처리의 기본원칙들을 확인하여 왔다. 최근의 유비쿼터스 환경에서 이 기본원칙은 다음과 같은 12대 원칙으로 확장할 필요가 있다.

1. 익명거래의 원칙	정보주체는 정부 또는 기업과 교섭 내지 거래를 할 때 불필요하게 자신의 신원을 밝히지 않고 거래할 수 있어야 한다.
2. 합법성의 원칙	개인정보처리시스템은 법률의 의사에 따라 합법적으로 구축되어야 한다.
3. 분리처리의 원칙	특정 목적을 위해 수집된 개인정보는 다른 기관에서 다른 목적을 위해 수집된 개인정보와 통합되지 않고 분리된 상태로 유지되어야 한다.
4. 시스템공개의 원칙	개인정보처리시스템의 설치 여부, 설치목적, 정보처리방식, 처리정보의 항목, 시스템운영책임자, 처리시스템에 의한 자동결정이 이루어지는지 여부 등이 일반에게 투명하게 공개되어야 한다.
5. 수집제한의 원칙	개인정보의 수집은 (i) 정당한 수집목적 하에 (ii) 필요한 범위 내에서 (iii) 공정하고 합리적인 방식으로 (iv) 정보주체의 분명한 인식 또는 동의 하에 수집되어야 한다.
6. 목적구속의 원칙	개인정보를 수집하는 목적은 (i) 수집 당시에 명확히 특정되어 있어야 하고(목적의 특정성), (ii) 그 후의 이용은 이 특정된 수집목적과 일치하여야 한다(목적일치성).

7. 제공제한의 원칙	수집기관 외부의 제3자에게 개인정보를 제공하는 것은 정보주체의 사전 동의 또는 분명한 인식 하에 이루어져야 한다.
8. 정보정확성의 원칙	개인정보는 정확성・최신성・완전성을 항상 유지하여야 하며, 처리과정에서 부당하게 변경・훼손되어서는 아니 된다.
9. 참여의 원칙	정보주체는 자신에 관한 정보의 소재를 확인할 권리를 가지며, 필요한 경우에는 자신에 관한 정보의 내용을 합리적인 기간 내에 합리적인 비용과 방법에 의해 알기 쉬운 형태로 열람할 권리를 가진다. 정보주체는 정확성・시의성・적실성을 상실한 자기정보를 수정・보완・삭제를 요구할 권리를 가진다. 이들 권리가 거부되는 경우 효과적인 구제수단을 보장받아야 한다.
10. 보안의 원칙	개인정보는 적절한 보안장치를 통해 내부자 및 외부자에 의한 불법적인 접근・사용・훼손・변조・공개 등의 위험으로부터 보호되어야 한다.
11. 책임의 원칙	개인정보의 관리주체를 명확히 설정하고, 관리주체에게는 상술한 원칙들이 지켜지도록 필요한 조치를 취해야 할 책임이 부여되어야 한다.
12. 감독의 원칙	개인정보처리원칙의 이행 여부를 감시・감독할 수 있는 전문적이고 독립적인 감독체계가 마련되어야 한다.

Ⅵ. 한국의 개인정보보호체계에 대한 평가

1. 현황

2012년 5월 현재 한국의 개인정보보호법제는 일반법과 특별법의 체계를 갖추고 있다. 민간부문과 공공부문의 개인정보처리를 포괄하여 규율하는 단일의 일반법인 「개인정보보호법」이 2011. 3. 29. 공포되어 2011. 9. 30.부터 시행되고 있다. 이 법률은 종래 개인정보보호를 위한 개별입법들이 공공부문과 민간부문으로 이원화되어 영역별로 존재하고 있던 것을 공공부문과 민간부문을 포괄하여 규율하기 위한 '일반법'으로 제정된 것이다. 이 법률에 의해서 기존에 공공부문의 일반법이었던 「공공기관의 개인정보 보호에 관한 법률」[15]은 폐지되고 그 내용이 이 법률에 흡수되었다.

이렇게 일반법인 「개인정보보호법」이 최근에 제정되었지만, 기존에 공공과 민간의 두 부문에서 개별영역을 규율하던 특별법들은 그대로 존속하고 있다.

그리하여 공공부문의 특별법으로 「주민등록법」, 「가족관계의 등록 등에 관한 법률」, 「통계법」에서는 각각 주민등록정보, 가족관계의 신분정보, 통계정보의 처리·이용에 관해서 규율하고 있다. 그 밖에 학생정보는 2003년 전국단위 교육행정정보시스템(NEIS) 사태를 계기로 2005년 3월에 학생정보의 이용과 보호를 규율하기 위해 「초·중등교육법」이 개정되었다. 또한 중앙인사위원회가 관리하는 국가인재데이터베이스의 구축 및 운영을 규율하기 위해 대통령령으로서 「공직후보자에 관한 정보의 수집 및 관리에 관한 규정」이 2005년 9월 30일 제정·공포되었다. 또한 민감한 개인정보(sensitive data)라고 할 수 있는 개인의 범죄기록의 수집·이용·제3자 제공을 특별히 규율하는 법으로 「형의 실효 등에 관한 법률」이 있다. 그리고 공공기관 사이에 개인정보를 포함한 행정정보의 공동이용을 규율하는 「전자정부법」이 마련되어 있다.

한편, 민간부문의 특별법으로 「신용정보의 이용 및 보호에 관한 법률」이 1995년 1월 5일 공포되었다(1995. 7. 6 시행). 그리고 온라인상의 개인정보보호법으로 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(2000. 1. 1 시행)이 있으며, 2004년에는 민간부문에서의 유전정보(유전자검사의 결과로 얻어진 정보)의 이용과 보호를 특별히 규율하기 위한 「생명윤리 및 안전에 관한 법률」(2005. 1. 1. 시행)이 제정되었다. 그리고 2005년에는 이동통신기술의 급속한 발달로 물류·보안·상거래 등의 영역에서 위치정보를 이용하는 다양한 서비스가 등장함에 따라 위치정보의 유출 및 오·남용으로부터 개인의 프라이버시 등을 보호하고 위치정보의 안전한 이용환경을 조성하기 위하여 「위치정보의 보호 및 이용 등에 관한 법률」(2005. 7. 28. 시행)이 제정되었다.

---

15) 이 법률은 한국에서 개인정보보호를 본격적으로 법제화한 최초의 것으로서, 1994년 1월 7일 공포되어 1995년 1월 8일 시행되었었다.

2. 보호체계에 있어서 불균형의 존재

현재 한국의 개인정보보호체계에는 몇 가지 점에서 불균형이 존재한다고 평가할 수 있다. 보호체계의 불균형성이란 개인정보의 이용과 보호라는 두 가치를 균형 있게 조정하면서 개인정보처리의 위험성이 높고 그만큼 보호필요성이 큰 분야에 보다 엄격한 보호체계가 마련되어야 함에도 그러한 체계성이 부족하다는 것을 의미한다.

위에서 살핀 바와 같이 일반법인 「개인정보보호법」에서부터 지나칠 정도로 개인정보의 '보호'에 치우쳐 '이용'의 현실적 가치를 무시하는 불균형성을 안고 있다. 특히 「개인정보보호법」의 강력한 규율은 민간부문에 집중되고 정작 높은 보호수준이 요구되는 공공부문에서는 그 보호의 수준이나 집행체계가 미약한 상태라고 할 수 있다.

더구나 공공기관 사이의 개인정보의 공동이용을 규율하는 특별법인 「전자정부법」은 전자정부의 운영원칙으로서 "개인정보 및 사생활의 보호"를 선언하고 있지만 동시에 "행정정보의 공동이용의 확대"를 규정하고 있다(제4조). 그리고 이 법률의 제4장(행정정보의 공동이용)에서는 "수집·보유하고 있는 행정정보를 필요로 하는 다른 행정기관 등과 공동으로 이용하여야 [한다]"(제36조)고 규정하면서 행정정보공동이용센터를 설립하고 있다(제37조). 그리고 공동이용의 대상이 되는 행정정보에는 주민등록정보를 비롯하여 가족관계정보, 부동산등기정보, 세무정보 등 여러 개인정보가 포함된다(제38조 및 동법시행령 제43조). 다만, 이들 개인정보를 공동이용하려는 경우에는 「개인정보보호법」에 의해 설립된 개인정보보호위원회의 심의·의결을 거쳐 행정안전부장관이 공동이용을 승인하도록 하고 있다(제39조 제4항).

이러한 개인정보의 공동이용은 개인정보DB들을 상호 연동 혹은 연계하는 방식(computer matching)으로 이루어지고 있어 그 오·남용가능성에 대한 충분한 안전장치가 규범적으로 확보되어 있다고 말할 수 있는지는 의문이다. 「전자정부법」에

서는 개인정보를 공동이용하기 전에 정보주체의 사전동의를 받도록 하고 있지만, 몇 가지 예외가 있고, 또 설령 동의를 받는다 하더라도 민원인의 입장에서 동의는 거의 형식에 그칠 가능성이 높다. 개인정보의 공동이용에 대한 예방적·사후적 감독체계가 제대로 작동할 수 있어야 할 것으로 보인다. 현재의 개인정보보호위원회가 이러한 감독권한을 가지고 있는지 조차 의문이다.

3. 예방적 집행기능의 미흡: 처벌 위주의 사후집행체계

개인정보보호법제는 개인정보의 이용과 보호라는 상충하는 가치를 미묘하게 조정하는 법제이기 때문에 합법적인 처리(=수집·이용·제공)의 기준이 칼로 두부 자르듯이 선명하게 그어지지 않는다. 복잡한 이익형량의 과정을 거칠 수밖에 없는 영역이 개인정보보호의 영역이다. 개인정보보호법에서는 개인정보처리(=수집·이용·제공)의 허용기준을 정하고 나아가 수집·이용·제공의 과정에서 준수하여야 할 절차적 요건들을 규정한다. 또 정보주체에게는 열람·정정·거부권 등을 주고 이들 권리의 행사를 통해 정보처리의 과정에 참여하게 하여 사전에 개인정보처리의 오·남용을 막음으로써 정보주체의 인격적 이익이나 파생되는 다른 권리와 이익의 침해를 예방하고자 하는 데 그 기본 목적이 있다.

바로 그러하기 때문에 개인정보보호체계에서는 법적 기준을 준수하도록 하는 "예방적 집행"이 무엇보다 중요하다. 예방적 집행이란 개인정보처리의 위험성을 사전적·예방적인 차원에서 막기 위하여 개인정보처리기관이 개인정보보호법의 실체적 규정(수집·이용·제공의 허용기준)과 절차적 규정(목적명시 요건, 품질관리 요건, 고지 요건, 보고 요건)을 제대로 준수하도록 사전에 유도하는 기능이다. 이러한 예방적 집행은 감사(auditing), 자문(consulting), 교육(educating), 그리고 자율규제의 유도(inducing self-regulation)의 방식을 통하여 이루어진다.

그런데 우리의 현행 개인정보보호체계를 보면 이러한 예방적 집행기능이 상당히 미약한 것으로 보인다. 특히 민간부문 온라인개인정보보호법인 정보통신망법

은 수집・이용・제공의 법적 기준 위반에 대한 사후처벌 위주로 집행체계가 구축되어 있다. 그것도 법적 기준이 보호의 가치 쪽에 치우쳐 있을 뿐만 아니라 그 기준 자체가 다소 불명확하고 애매한 상태에서 그러한 법적 기준의 위반 여부를 행정청이 일방적으로 결정하여 행정제재를 가하거나 형사처벌의 대상으로 삼고 있다. 심지어 일반법인 「개인정보보호법」도 민간부문에 있어서는 동일한 입법방향을 가지고 있다. 그러나 이러한 사후제재 위주의 집행방식은 개인정보보호체계에서는 결코 효과적이지 못한 방식이다. 단발적인 효과는 있을지 모르지만, 지속적이고 실질적인 집행의 효과, 즉 안전한 개인정보의 이용이라는 입법목표는 달성되기 어려울 것이다.

4. 표준개인식별자로서의 주민등록번호의 존재와 그 위험성

전 국민 개개인에게 유일하고 영구적인 표준개인식별자(universal identifier)를 부여하여 그것을 기초로 전 국민의 신원확인을 용이하게 할 수 있는 통합관리시스템을 구축하고자 하는 시도는 그 무시할 수 없는 효용 때문에 어느 정부도 쉽게 포기할 수 없는 유혹이다. 최근 미국과 유럽에서는 불법이민의 고용통제, 범죄방지 등의 효율적인 법집행, 복지사기의 방지, 조세포탈자의 추적, 국민보건의 증진 등의 강력한 논거에 입각하여 개인정보통합관리시스템의 구축을 주장하는 목소리가 점차 높아지고 있다.

우리들은 거래연관에 따라 여러 개인식별자(personal identifier)를 가지고 있다. 예금계좌번호, 신용카드번호, 운전면허번호, 의료보험번호, 여권번호 등이 그것이다. 이들은 원래는 각자 다른 목적을 위해 분리되어 사용되는 것으로 예정되었다. 그리고 이들이 분리되어 존재한다는 사실 자체가 개인정보통합관리시스템의 형성에 있어 자동적인 방화벽이 될 수 있는 것이다.

그러나 전 국민이 표준개인식별자로서의 주민등록번호를 강제로 부여받고 있고, 또한 정부와의 거래 또는 민간에서의 거의 모든 거래에 있어 주민등록번호의

제출을 요구했던 최근까지의 한국의 상황은 개인정보통합관리시스템의 형성을 막을 수 있는 방화벽이 이미 허물어졌다는 것을 의미한다. 이미 정부와 기업이 보유하고 있는 수많은 개인정보DB는 거의 예외 없이 주민등록번호를 중심으로 구축되어 있다. 이러한 사실은 곧 정부와 시장이 의도하기만 하면 포괄적인 개인정보통합관리시스템을 쉽게 구축할 수 있는 가능성이 열려 있다는 것을 의미한다. 달리 말하면, 주민등록번호 하나만 가지고도 개인의 모든 것을 추적해 들어갈 수 있는 것이다.

최근 제정된 「개인정보보호법」이 주민등록번호와 같은 고유식별정보의 수집과 이용을 규율하고 있지만(제24조), 이미 주민등록번호를 중심으로 구축된 개인정보DB에서 주민등록번호의 이용을 당장 금지할 수도 없는 상황이다. 어려운 과제로 남아 있다. 이와 관련해서 정부는 2012. 4. 20. 행정안전부, 방송통신위원회, 금융위원회의 부처 합동으로 '주민번호 수집·이용 최소화 종합대책'을 마련하여 개인정보보호위원회의 의결을 거쳐 발표하였다. 향후 공공기관이나 민간기업에서 주민번호를 수집·이용하는 것을 원칙적으로 금지하고 수집된 주민번호에 대한 관리책임을 대폭 강화한다는 내용이다. 뒤늦은 감이 있지만 정부의 종합대책이 개인정보통합관리시스템의 형성을 막는 중요한 기제가 되기를 기대해 본다.

Presentation

Right to Information Privacy: Korea's Challenges and Response

LEE, In-Ho

(Professor, Chungang University Law School)

Ⅰ. Daily Surveillance and the Building of a Counter-Surveillance System

Shaped by digital information technology, the information society is, in a nutshell, a recording society. Everything is recorded. Every trace of an individual citizen's daily life is recorded as digital information, which is then processed or analyzed by someone. Far from being deleted, such processed personal data is then copied countless of times, shared with other people and easily integrated with other data.

Until quite recently, this was a phenomenon that was presumed to happen only in cyberspace, a space created by a networked computer. But the latest ubiquitous technologies, including BcN (Broadband Convergence Network), USN (Ubiquitous Sensor Network), RFID (Radio Frequency Identification) and IPv6, implant a miniature interactive computer into an object, externally transmitting and sharing information related to the nature of the object. The line between cyberspace and reality has begun to fade.

In tomorrow's ubiquitous society, all social members will move beyond the stage of communicating anytime anywhere through an always-on network (P2P: Person to Person) to where people and objects are always connected (P2O: Person to Object) and eventually, to where communication is automatically-driven between objects (O2O: Object to Object). People will no longer even be conscious of computers or networks. They will be connected to a network, regardless of time or place, and communicate either with another person or object. Such a ubiquitous environment will, undoubtedly, offer new conveniences and benefits, and unlimited possibilities, but the side effects will be no easy challenge. In particular, a ubiquitous society inevitably possesses the nature of a surveillance society.

In a ubiquitous society, surveillance will be a co-existent factor inextricable from a person's life. Everything about that person will be recorded, stored and shared. The ubiquitous computing system will automatically collect and share real-time personal data on that individual's identity, location, activity and context.

Surveillance technologies in a ubiquitous environment will not only track everything about a person's public and private life, but also automatically store and process the results of such tracking, creating a profile of every individual. Furthermore, the digitalized personal records will be easily integrated and thereby create a completely new digital character separated from the real character of the individual.

The feeling of being watched will change a person's habits. As surveillance gradually becomes a part of one's life, it will gnaw away their subjectivity. Their space of freedom will also be diminished. Meanwhile, one's digital character, created without

their knowledge, will define their real character. This is critical since any decisions about that person made by the government and market will be based on one's digital character instead of their real character.

Given that a person's subjectivity and freedom are prerequisites to a free democratic system, a comprehensive surveillance system over a person's life has the possibility of infringing them.

Nevertheless, this should not hinder the advancement and progress of technology. The danger and utility of technology depends on the choices made by the social system that adopts such technologies. The challenge we face at this junction is to establish a counter-surveillance model, which can minimize the danger the development of IT imposes on individuals' privacy, while simultaneously accommodating national and social interests in processing personal data, and implementing the model within the social system.

Solving problems related to the establishment of such a counter-surveillance model is difficult because surveillance over a person's every day life does not lack legitimacy. The responsibility of the modern state has moved beyond the simple acquisition of physical production conditions and today, must guarantee social reproduction through welfare and social policy. In order to undertake this function efficiently, the collection and processing of personal data are inevitable. In particular, the concept of an electronic government is becoming more concrete. Electronic government or e-government provides small and efficient, high quality administrative citizen-oriented services based on the philosophy of creating a citizen-driven government through IT. The former Kim Dae-Jung and Roh Moo-Hyun administrations, and the current Lee

Myung-Bak administration recognizes the joint use of administrative information, including personal data, as one of the core elements of e-government. Reasons such as efficient law enforcement, public safety, prevention of welfare fraud, prevention of tax evasion, enhancement of national health and improvement of public services, reinforce the need and justification for the processing of personal data. This also applies to the private sector as the processing of customer's personal data by a company not only maximizes efficiency in resource distribution, but also bestows an interest so irresistibly sweet and convenient to the data subject, the consumer. Both corporate entities and societies maximize efficiency of resource distribution through personal data processing, and the convenience and comfort provided by IT are only possible if such personal data is collected and shared.

This is where our problem begins. In brief, the core challenge that we face is to "build a counter-surveillance system which does not impair the justification of surveillance while offsetting its risks".

This calls for, first of all, (i) a close investigation into the justification of a surveillance system. Justification in surveillance is often superficially declared, and therefore, its sincerity must be carefully examined. Next, (ii) the purposes and authority of the body operating the surveillance system, the extent of the surveillance boundary, and the fairness of operational procedures must be strictly verified. This requires the clear identification of a verification criteria. (iii) The counter-surveillance system must be validated during the designing phase of the surveillance system. (iv) A rational way to build the counter-surveillance system must be found. (v) More ideas should be gathered for the effective operation of the counter-surveillance system.

Ⅱ. A Normative Approach to the Counter-Surveillance System: Right to Information Privacy and the Personal Data Protection Act

1. Utility and Risks of Personal Data Processing

Today, all public and private organizations store large quantities of personal digital data for their business. Personal data related to basic demographics, education, fiscal, medical, and credit data, employment, tax, arrivals/departures, security related information, social welfare, military service, vehicle management, department store purchases, social organization activities, and finances, among many others, comprise only a small part of such personal digital data.

Digitalized personal data management has such high utility that it is incomparable to the time before such information was digitalized. The DBMS (Database Management System) not only enables swift and accurate input, processing, search and output of personal data, but also the easy and efficient integration and processing of dispersed personal data through computer matching using the Universal Identification Number.

The processing of personal data using digital technology has high utility for bith the government and society. A country can only function efficiently if the personal data of its people is processed effectively. Companies and societies can also maximize efficiency in resource distribution, and the convenience and benefits of IT to individuals can only be realized through the collection and sharing of personal data.

For instance, in terms of social welfare administration, the government can enhance the efficiency of government services while also reducing budget wasted by preventing

welfare fraud through a comprehensive management of information on individuals receiving welfare services. In addition, integrated management and joint use of personal data enhances capability in every field, namely crime investigations, security, tax administration and education. Examples include preventing crimes by analyzing related data and categorizing potential criminals or dangerous individuals, or capturing tax evasion suspects based on tax and spending information management by using techniques such as computer matching, computer profiling and data mining.

Companies regard DB marketing activities based on personal data database as the major underlying source for their competitiveness, and in truth, collecting customers' personal data occupy a significant part of a company's marketing strategy. This is why telecommunications services companies, distribution companies, airlines, and financial organizations, among others, adopt the knowledge-based sales system and thereby carefully analyze and record their customers' purchase and usage patterns to reflect them to their sales. This system is technically operated by the Data Warehousing system.

Customer preference, such as who tends to purchase what, when, where, can be identified through an analysis of sales trends by month, gender, age, store and product by using this system. Based on such analysis results, businesses can devise various management strategies or efficient marketing activities.

With the recent advancement in e-Commerce, the processing of customers' personal data is becoming not only more useful, but also inevitable. This is because the collection and analysis of such information through e-Commerce is beneficial to both

businesses and customers themselves. In particular, on an international level, it not only contributes immensely to international commercial activities, but it can also offer a wider range of choices to consumers. In other words, businesses can now analyze the consumption patterns of consumers worldwide, thus accurately analyzing which consumers are currently interested in which products. This enables them to reflect consumers' needs and target them accurately, whereas consumers can acquire timely product information from all over the world. This is why the processing and utilization of consumers' personal data has a positive aspect in terms of the market in that it contributes to resource distribution efficiency.

On the other side of the coin, however, lies mounting risks. According to the different aspects of collecting, processing and utilizing personal data, the risks imbedded in the formation of a distorted digital character, which fails to fully reflect a person's real character, can result in various consequences.

The first problem is about the accuracy of personal data. In case the personal data recorded on the database should differ from reality, and if policy decisions (government-side) or management decisions (market-side) are based upon such inaccurate information and implemented, it would have a serious effect on that individual's social life. This is why personal data should not only be inputted accurately, but any changes to inaccurate information should be made swiftly. Cases where the inputted information loses timeliness due to the passage of time and is no longer valid can also impair the accuracy of personal data.

The second problem is about integrity. This usually occurs during the information processing stage. For example, if personal data is integrated or re-categorized in an

inappropriate manner during the computer input process, the output will fail to fully reflect the subject of such information. In addition, an internal error in the processing program could systematically distort the output information. This could result from a malfunctioning of the hardware or a mistake on the system operator. The identification of a real character based on systematic distortion of personal data increases the risks involved.

The third problem is about security. This occurs during the management stage, when personal data is divulged due to illegal internal or external penetration. Though they exist in different physical locations, personal data databases are inherently vulnerable to external intrusion since they are increasingly inter-connected as a result of an expanding telecommunications network. Recently, illegal penetrations through hacking or cracking are not decreasing despite the advancement of security technologies. In addition, security may be breached by an internal person. In other words, a person with legal access to the database could divulge such personal data to external sources for personal profit.

The fourth problem is regarding adequacy of personal data. This is related to the justification of collection and adequacy in secondary use of such information. personal data databases are usually built for specific reasons, but when they are used for purposes other than for which they were originally collected is when a violation of adequacy occurs.

Unless there is accuracy in information input, integrity in information processing, security in information management and adequacy in information usage, personal data can be distorted. This entails risks that could fatally damage the real character of a person.

Furthermore, this means that the private and public organizations that accumulate and process such personal data also have a powerful control and surveillance tool over that certain individual. This enables the social stigmatization of certain people (for example, by drawing up and distributing a list of credit defaulters or people who should be avoided during employment) and as a result, those people could be either marginalized from society or face limited choices.

As the collection and processing of personal data becomes a part of every day life, the data subject will feel as if every detail of their private life is being tracked and this will change their habits. As surveillance gradually becomes more internal, one's character will lose subjectivity and freedom. Yet, both are prerequisites to a free and democratic society.

2. Legal Response against New Threats

Amidst the generalization of recording and surveillance, Information Privacy (Recht auf informationelle Selbstbestimmung) was proposed as an information human right in order to minimize the risks while accommodating the national and social interests in personal data processing. This led to the enactment of laws that defined information rights, such as the *Second Generation Privacy Protection Law or Personal Data Protection Act*, by advanced countries since the early 1970s.

Ever since the emergence of computer and digital technology in the 1960s, the risks that accompanied the processing of personal data were already recognized in the early 1970s and normative response measures to protect personal privacy were adopted. Sweden was the first European country to enact a law regulating personal data

processing in private and public sectors in 1973 (Data Act of 1973), followed by Germany, Denmark, Austria, France, Norway and Luxemburg in 1978, England in 1984 and the Netherlands in 1988. Meanwhile, the United States was the second country in the world to enact the personal data Protection Act regulating the public sector in 1974, one year later than Sweden.

Since the 1980s, international organizations have been affirming the basic principles of personal data processing in order to protect personal data while at the same time facilitating its international distribution. The principles are embodied in the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data of 1980, the Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data of 18 September 1980 of the Council of Europe, the Guidelines for the Regulation of Computerized Personal Data Files of the United Nations of 1990, and the Directive of the European Parliament and the Council on the protection of individuals with regards to the processing of personal data and the free movement of such data (95/46/EC). Additionally, the obligations and rights of the data subject in personal data protection laws adopted by each country are becoming increasingly sophisticated.

Ⅲ. Misconceptions of Informational Privacy

Since the Personal Data Protection Act in the public sector (Act on the Protection of Personal Data Maintained by Public Institutions) was implemented in 1995, the greatest controversial issue regarding the criteria in personal data processing over the past

seventeen years leading up to 2012 was in relation to whether or not to make the acquisition of consent of the data subject a legal basic principle.

In other words, in principle, should the personal data controller be prevented from collecting, using and providing personal data of another person without first gaining their consent? Should it be legally permitted, to a certain extent, to process information (collection, usage and provision of personal data) without acquiring the consent of the data subject? Does the right to control one's information or Information Privacy (Recht au informationelle Selbstbestimmung)[1] prevent, in principle, the processing of personal data without pior consent of the data subject?

This is a question regarding who is the owner of personal data that is being collected, processed and used by another entity, how much characteristic interest of such information is actually owned by the data subject and what is the extent of his control over it.

On May 26, 2005, the Korean Constitutional Court made a decision that recognized Information Privacy as a "new individual basic right" for the first time in the "Case on Resident Registration Fingerprint Information DB"[2]. It was a case where the public authorities had utilized their citizens' fingerprint information collected for the purpose of resident registration for crime investigation purposes. More specifically, the Minister of Public Administration and Safety had handed over to the Chief of the National Police Agency fingerprints (of both hands) of more than 39million Korean adult

1) The Federal Constitutional Court of Germany recognized "Informational Privacy (Recht auf informationelle Selbstbestimmung)" for the first time in a population census ruling (BVerfGE 65, 1) in 1983.
2) Constitutional Court Case No. 2005. 5. 26. 99 Constitutional Appeal for the Remedy of Violation of Private Right 513 etc (Resident Registration Fingerprint Information DB Case [6(Constitutional) : 3(Unconstitutional)].

citizens collected for identification purposes in the process of issuing resident registration cards (ID cards issued to adult citizens)[3], which were stored, computerize d[4] and used for criminal investigation purposes. The Korean Constitutional Court recognized that the Information Privacy of the claimants, who were the subject of the fingerprint information was being limited due to the Automatic Fingerprint Identification System (AFIS). However, it was considered a necessary limitation in order to achieve a justifiable purpose and ruled it as constitutional by a vote of six (constitutional) to three (unconstitutional).

The Constitutional Court explained that the "significant increase of the state's surveillance capability over individuals according to greater national capacity in collecting and processing personal data with (due to) the advancement of modern information technology" as the social background to authorizing the new basic right. In addition, it was declared that this new basic right would not be completely subsumed by any of the articles on existing basic rights ("Human worth and dignity and right to pursue happiness" as provided in Article 10 and "Privacy" as provided in Article 17 of the Korean Constitution) or Constitutional Principles ("basic free and democratic order" as provided in the Preamble, principles of national sovereignty and democracy), and therefore ruled it as a "basic individual right ideologically based on the above but

3) The ten fingerprint system related to the issuance of the resident registration card was initially adopted in the Resident Registration Enforcement Ordinance (Presidential Decree) implemented on August 26, 1975.

4) The National Police Agency adopted and operated the Automatic Fingerprint Identification System (AFIS) since 1990. This is a system which inputs the Resident Registration Card Application Form, which has personal data and ten fingerprints of the applicant, on to a high-speed high-capacity computer in the form of an image. This image can be accessed via a terminal to verify fingerprints or used to check the identity of a corpse by automatically searching for personal data and any fingerprints left on the scene. The fingerprint data was first inputted on the computer around October 1990. Prior to February 1998, a record of fingerprints of only three fingers of each hand, totalling six fingers, was kept, but this was later expanded to include all ten fingers. The fingerprint data of approximately 39 million people, which was the data the police had collected up to June 15, 2003, was completely computerized.

undefined in the Constitution".

In this ruling, the Constitutional Court declared, "Information Privacy is a right which the data subject can decide who and when, and to what extent, will have access to their personal data. To be more specific, the data subject has the right to decide for oneself the disclosure and usage of personal data". Furthermore, the personal data that falls under such right is "not limited to one's secret or private life, but includes all personal data created during one's public life and already disclosed personal data", and "all actions such as investigation, collection, storage, processing and usage of such personal data are, in principle, limit one's Information Privacy".

However, such a ruling can lead to various misconceptions. There is the danger of misunderstanding that the data subject has the right to directly decide or control the entire process of collection and provision of personal data. But Information Privacy is not a right which directly "decides or controls" the entire personal data processing process undertaken by the processing entity. The decision to process personal data remains with the entity that processes the information. Rather, the Information Privacy of the data subject is a "right to participate" in the information processing process. It is about the right to know how personal data is collected, utilized and provided by whom (claim for inspection), to demand the setting of a clear purpose for processing, to demand the processing of information required solely to achieve the specific goal, to demand the modification or deletion of inaccurate or outdated information in order to maintain the accuracy and timeliness of information, and to demand restricted access against unauthorized persons and prevention of unjustified divulgence of information.[5]

5) However, in the original ruling in the Resident Registration Fingerprint DB Case, the Constitutional Court failed to focus on Information Privacy right. In regards to the Police's collection of fingerprints of a huge

There is a recent trend in Korean society to make personal data protection absolute. According to this trend, the collection, usage and provision of personal data without the consent of the data subject is, in principle, illegal. However, this is a result of misunderstanding the concept of Information Privacy. This could lead to the mistake of ignoring the social values in the usage and distribution of personal data essential to our society and treating all personal data as confidential data.

Although personal data is the a token of personality for the data subject, the personality itself should not be locked up and protected. The society is, in many cases, sustained by an accurate evaluation of its citizens and based on which, it maintains its functions. To make this possible, the distribution of people's characteristic symbols is vital. However, if the prohibition of the distribution of personal data without the consent of the data subject leads to a misunderstanding that it is a part of personality right or Information Privacy since it is the characteristic symbol of that person, people will try to prevent the distribution of characteristic symbols unfavorable to them. This will make any accurate evaluation of a person by society impossible, and the result will be a paralysis or contraction of the society's normal functions.

Unfortunately, this concern was materialized with the enactment of the Personal Data Protection Act on March 29, 2011, which was implemented on September 30 the same year. This law brought together existing separate laws on personal data protection[6] for

---

population reaching 39 million for identification purposes in resident registration, computerization of such information and utilization, not for its original purpose, but for criminal investigation purposes, there should have been an assessment of the installation of appropriate safety measures and a normative system which could sufficiently ensure the accuracy, integrity, security and adequacy of personal data.

6) The first true legislation on the personal data protection issue in Korea was the Act on the Protection of Personal Data Maintained by Public Institutions which was proclaimed on January 7, 1994 (implemented on January 8, 1995), followed by the Use and Protection of Credit Information Act in the private sector

the public and private sectors into a single 'general law' regulating both sectors[7]. Regardless of this fact, it focuses exceedingly on the "protection" of personal data and ignores, to a considerable extent, the realistic value of the "use" of personal data. It may presumably be the world's most strict personal data protection law. However, it raises serious concern since the excessive restriction on the use and distribution of personal data necessary to society may contract normal social mechanisms based on the rational assessment of people.

The law proclaims the protection of "all information related to an identifiable individual", treating all personal data as "confidential"[8] and recognizing the information subject's near absolute right to control one's personal data. In other words, it maintains that, in principle, personal data should be collected upon the "consent" of the data subject with some exceptions (Articles 15 and 16). Furthermore, this principle is even more strictly applied in the use and provision of the information to a third party (Articles 17

---

proclaimed on January 5, 1995 (implemented on July 6, 1995). The Act on Promotion of Information and Communications Network Utilization and Information Protection enacted on February 8, 1999 (implemented on January 1, 2000) was the first legislation on personal data protection online. In 2004, the Bioethics and Safety Act (implemented on January 1, 2005) was enacted to specifically regulate the use and protection of genetic information (information acquired as a result of a genetic analysis) in the private sector. In 2005, with the rapid development in mobile telecommunications technology and emergence of various services utilizing location information in terms of logistics, security and e-Commerce, the Act on the Protection, Use of Location Information (implemented on July 28, 2005) was enacted to create an environment which protects individuals' privacy from divulgence, misuse and abuse of location information and enables the safe use of such information.

7) The former regulation in the public sector, the Act on the Protection of Personal Data Maintained by Public Institutions, was abolished and its content was integrated into this Act. However, other personal data protection laws that existed by field in the private sector (Use and Protection of Credit Information Act, Act on Promotion of Information and Communications Network Utilization and Information Protection, Bioethics and Safety Act and Act on the Protection, Use of Location Information) still remain in effect as special laws in their relevant fields. The Personal Data Protection Act, which is a general law, regulates personal data processing in the private sector not covered by these special laws.

8) Article 1 (Purpose) defines the "protection of privacy from the collection, divulgence, misuse and abuse of personal data" as the objective of the legislation. However, personal data protection laws of other countries emphasize the harmony between the protection and safe use of personal data as their legal objective.

and 18). Pursuant to this law, utilizing contact information collected for the provision of a product or service during a transaction with customers in the promotion or marketing of another product or service is considered as “non-purpose use” and necessitates the acquisition of additional consent from the data subject. If this provision fails to be observed, the company may be subject to a sentence of up to five years’ imprisonment or a penalty of up to fifty million Korean Won (Article 18 Clause 1 and Article 2, Article 71 Clause 2). Another example is in the event of a dispute between a company and customer during a transaction. If, in seeking legal counsel, the company provides the personal data (including basic identification information) of the customer collected during the transaction to its lawyer without the prior consent of the data subject, it will also be regarded as a “non-purpose provision” and be subject to criminal penalty.

In addition, this law recognizes unlimited “right to demand any corrections or deletion” of personal data as the right of the data subject (Article 36 Clause 1). Upon receiving a request from a data subject, the personal data controller shall, without delay, correct or delete certain information according to the request and notify the data subject of the result (Article 36 Clause 2). This is identical to bestowing full authority to correct or delete disadvantageous information to the data subject. However, the right to request for correction or deletion should only be recognized when there is an error in the collected information, when the accuracy and integrity of the processed information is impaired due to outdated information, or when it includes information completely unrelated to the purpose of processing that can infringe the person’s privacy.

What is more concerning is the misunderstanding about the subject of regulation under the Personal Data Protection Act. The law defines “personal data controller”,

which is the entity managing personal data files (refers to personal data database) as part of its duties (Articles 2, 4 and 5), as the subject of regulation. Nevertheless, some experts are inclined to interpret the provisions too broadly and include the collection, use and provision of personal data about another person by an individual who does not operate personal data databases as being applicable to regulation.

Another practical example is the heated political controversy over whether or not to enact a new law enabling the National Police Agency to track the location of a crime victim in case of an emergency.

So far, the Act on the Protection, Use of Location Information authorizes only the National Emergency Management Agency and the National Maritime Police Agency to track location of people for emergency purposes. On April 1, 2012, however, a preposterous murder case happened in Suwon as a result of the National Police Agency not having this authority. A victim of sexual violence had called the police for help. But not having the authority to track the victim, the police failed to act and later, the victim was found murdered. This case stimulated voices calling to amend the law to enable the National Police Agency to track locations of victims in emergency cases. Unfortunately, a bill on this same note was already motioned at the National Assembly in 2008, but former prosecutor-parliament members on the Legal Affairs and Judiciary Committee continuously opposed this bill, leaving it to drift in mid-air for four years. The members claimed that “the protection of a crime victim in an emergency is the first phase of investigation, and therefore the police must request for a court warrant through the Prosecutor’s Office in order to conduct location-tracking”. Even when public sentiment calling for swift legal amendment was aroused in April 2012, the Senior Deputy Floor

Leader of the opposition party prevented the bill from passing, claiming that “granting the police the authority to automatically track locations raises concern of potential authority abuses, including privacy infringement and illegal inspections.”

The current situation where the government cannot track the location of a victim calling for help from a potential crime because it has to respect the victim’s privacy is almost laughable. It can be said that the moment the victim requests for help, he or she abandons their right to privacy of their location information. There was also a case before the enactment of the Location Information Act where an accident victim on Jiri Mountain called for help using his mobile phone, which soon ran out of batteries. The authorities were in a situation where they had to track the location of the victim, but hesitated to take swift measures because of information protection reasons. They arrived on-site belatedly, only after the victim had died. Advocating the protection of privacy (right to location information privacy) of the data subject in a critical life-or-death situation is clearly the result of irrational thinking.

Ⅳ. Features of the Personal Data Protection Act as a Second Generation Privacy Protection Law

The Personal Data Protection Act must differ from the first generation privacy protection law. It was only during the late 19th Century when the concept of protecting the confidentiality of privacy and value of peace by legal means was born. The value of privacy was later elevated to the “right to privacy”. From the beginning of this period leading up to the enactment of the Personal Data Protection Act of the 1970s is the so-called “Age of the First Generation Privacy Protection Law”. The Privacy

Protection Act at the time “directly” prohibited any “unjustifiable” access, public disclosure or divulgence of private or confidential information.

The second generation personal data protection law treats all personal data of identifiable individuals as a subject for protection while allowing information processing for justified purposes and requiring fair practice to prevent any risks of abuse or misuse of personal data instead of prohibiting the processing (collection, usage and provision) of such information. As such, the two laws differ in terms of legislation purpose, limits of personal data under protection, regulated actions and method of regulation.

Purpose of legislation	First Generation Privacy Protection Law	In order to sanction any damages occurred in reality (privacy infringement).
	Personal Data Protection Act	In order to prevent any infringement of various legal interests of the data subject by preventing the abuse or misuse of personal data processing during business operation.
Subject of regulation	First Generation Privacy Protection Law	Actions that damage peace in one’s private life
	Personal Data Protection Act	All phases of personal data processing in the form of personal data DB
Method of regulation	First Generation Privacy Protection Law	Establish criteria for infringement and impose civil or criminal sanctions on violations of such criteria.
	Personal Data Protection Act	Establish criteria for fair personal data processing and guarantee participation of the data subject in the information processing process. Supervision organization to monitor, adjust grievances and educate the public.

The fundamental purpose of the Personal Data Protection Act lies in recognizing the value of personal data processing while preventing the risks that accompany it. All

personal data protection laws of other countries clarify this point in the purpose article. The 1995 European Directive on Protection of Personal Data (95/46/EC), which has become a legislative model for personal data protection laws, clarifies two legislative purposes in Article 1 (the article which depicts the objective of the law): "1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data. 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1." This does not mean that it prohibits the processing (collection, use and provision) of personal data. Rather, it permits it, but it must also protect the right to privacy of the data subject by preventing its abuse or misuse. It also underlines that the distribution of personal data necessary between Member States shall not be deterred due to protective reasons.[9)]

Furthermore, the Protection of Personal Data Act of Japan, which is both a basic law and a general law for the private sector, depicts in Article 1 (Purpose): "The purpose of this Act is, given the significant increase of the use of personal data in response to the advancement of a sophisticated telecommunications society, to protect the rights and interests of individuals while taking into consideration the usefulness of personal data,

9) In fact, the above EU Directive on Protection of Personal Data or the 1980 OECD Guidelines on the Protection of Privacy had three initial objectives. The first objective was to ensure the international distribution of personal data. With the progress of globalization in the economy, the international distribution of personal data was essential in critical economic sectors, such as banks and insurance. Since the 1970s, OECD member states began to enact varying personal data protection laws on a national level. Such legal differences could adversely affect the international distribution of such personal data, which was why there was a need to bridge legal gaps among countries and integrate the criteria for personal data processing. This was the second objective and also the underlying intention behind the enactment of EU's Directive on Protection of Personal Data. The third objective was to establish a legal safety measure against the infringement of individual rights or interests resulting from the processing of personal data (collection, use and provision).

by laying down the basic principles and basic government policy in relation to the appropriate treatment of personal data, defining the basis for other measures on the protection of personal data, clarifying the duties of the state and local autonomies and identifying the obligations of businesses that deal with personal data." The German federal Data Protection Act (Datenschutzgesetz), a general law covering both public and private sectors, identifies its objective in Article 1 as the protection of personal data during storage, delivery, modification and processing to prevent misuse and thereby prevent it from infringing upon other rights and interests of the individual that must also be protected.

This is the reason why, in the enactment and interpretation of the Personal Data Protection Act, "personal data" should not be treated as "private or confidential information" that should not be collected or the acquisition of consent of the data subject made mandatory in the processing of such information. The Personal Data Protection Act is not a law which grants the data subject the full right to give consent in information processing. In other words, the Act must not be understood as prohibiting the processing of personal data without the consent of the data subject. It is an additional condition, not a basic one, and once the consent is acquired, the information can be processed (collected, used, provided) beyond the legally permitted scope. It is worth noting that no other country in the world necessitates the acquisition of consent of the data subject as a basic condition in processing personal data in their personal data protection law.

Provided, however, the Personal Data Protection Act ensures the participation of the data subject in the processing of their information. For instance, according to the

Individual Participation Principle of the 1980 OECD Guidelines on the Protection of Privacy (and Transborder Flows of Personal Data), “An individual should have the right (i) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him (right to confirm possession); (ii) to have communicated to him, data relating to him within a ① reasonable time; ② at a charge, if any, that is not excessive; in a ③ reasonable manner; and ④ in a form that is readily intelligible to him (right to inspection), (iii) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial (right to make claims); and (iv) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended (right to change processed information). In addition, the personal data protection laws of most countries, including the EU, England, Germany and Japan, basically have such provisions on the rights of individuals. Moreover, Europe and Japan broadly allows the processing of personal data without the consent of the data subject while granting the right to object ex post facto the processing of certain information. Furthermore, Europe recognizes a certain form of “a right not to be binded by automatic decision” of the data subject.

As the above, if the first generation privacy protection law concentrated on passively preserving an individuals’ privacy from external intrusion or disclosure, the Personal Data Protection Act is a law which, by principle, allows the collection, use and provision of personal data while granting the data subject the right to participate in the information processing process (right to confirm possession, right to inspection, right to make claims, right to change processed information, and right to deny) as a safety clause to prevent any misuse or abuse of such data. More specifically, if the former

privacy protection law focused on “privacy as seclusion” (the so-called “Seclusion Model”), the Personal Data Protection Act adopts a “privacy as participation” approach (the so-called “Participation Model”). The data subject should be able to clearly understand which personal data is being used for what reasons by whom in what manner, and be able to participate in the process of processing the information. The Participation Model has a counter-surveillance function which prevents any danger of surveillance or control over the individual through the misuse or abuse of personal data processing especially by the government or private business entity.

In addition to the granting of such participation rights to the data subject, the Personal Data Protection Act lays down the legal criteria of collection, use and provision as the fair standard of personal data processing to prevent its misuse and abuse. It regulates the instances when the collection, use and provision of personal data are permitted. This is a substantive condition demanded of the personal data controller. In addition, the Personal Data Protection Act sets four procedural conditions (identification of objective, quality management, notice and report) in order to ensure the accuracy and integrity of personal data and demands their observation by the personal data controller. The Personal Data Protection Act, however, cannot sufficiently guarantee the counter-surveillance function by ensuring the participation right of the data subject, and thus, as a precautionary measure, installs an independent supervision organization to monitor and conduct supervision on whether the personal data controllers observe the legal criteria in personal data processing .

As such, the Personal Data Protection Act is a second generation privacy protection law which constructs a counter-surveillance system by ensuring the participation rights

of the data subject, establishing the authorized criteria and procedural conditions of personal data processing and installing a supervision organization of personal data in order to address new privacy threats that arise as records and surveillance become a part of everyday life in today's digital recording society.

Ⅴ. Basic Principles of the Counter-Surveillance System

For more than thirty years, major international organizations and countries around the world have affirmed the basic principles in personal data processing required for the protection of the data subject's privacy. In today's ubiquitous environment, the basic principles should be expanded to the following Twelve Principles:

1. Anonymity–based Transaction Principle	The data subject should be able to engage in a negotiation or transaction with the government or company without having to unnecessarily identify oneself.
2. Legality Principle	The personal data DB must be built legally according to the intention of the law.
3. Separate Processing Principle	Personal data collected for specific purposes must be maintained in separate form and not integrated with the personal data collected for another purpose by another organization.
4. Openness Principle	The installation of a personal data DB, purposes of such installation, information processing method, information items processed, system operation manager, and whether an automatic decision is reached according to the system should be declared to the public in a transparent manner.
5. Collection Limitation Principle	The collection of personal data should be made (i) under justifiable objectives (ii) within necessary boundaries (iii) in a fair and rational manner and (iV) with the clear recognition by or consent of the data subject.

6. Purpose Specification Principle	The purpose of the collection of personal data should be (i) clearly stated during collection (specific purpose) and (ii) its use must be consistent with the purpose of collection (purpose consistency).
7. Disclosure Restriction Principle	The provision of personal data to a third party different from the collecting organization should be made with the prior consent of or clear recognition by the data subject.
8. Data Quality Principle	Personal data must always maintain accuracy, timeliness, and integrity, and must not be unjustly altered or damaged during the information processing process.
9. Participation Principle	The data subject holds the right to check the location of personal data, and if the need arises, the right to inspect it in easily readable form within a reasonable period and at reasonable cost. The data subject has the right to request the correction, complement or delete self-information which has lost accuracy, timeliness and adequacy. In the event such a right is denied, the data subject should be ensured of an effective relief method.
10. Security Principle	Personal data must be protected from risks related to illegal access, use, damage, alteration or disclosure by an internal or external party by using adequate security measures.
11. Accountability Principle	The manager of personal data must be clearly defined and given the responsibility to take necessary measures to observe the above principles.
12. Supervision Principle	A specialized and independent supervision system must be built which can monitor and supervise the implementation of the principles of personal data processing.

Ⅵ. Assessment of Korea's Personal Data Protection System

1. Current Overview

As of May 2012, the current Korean personal data protection legal system comprises of general and special laws. A single general law, the Personal Data Protection Act,

which regulates personal data processing in both private and public sectors, was proclaimed on March 29, 2011 and came into effect on September 30 the same year. This law was enacted as a comprehensive general law in order to regulate what had formerly been regulated by separate laws. The Act on the Protection of Personal Data Maintained by Public Institutions, which was a former general law for the public sector, was abolished and its content absorbed into this more recent act. As the above, the Personal Data Protection Act was only recently enacted, but the special laws that regulate independent areas in both private and public sectors are still valid.

As for special laws in the public sector, the Resident Registration Act, Act on the Registration of Family Relationship and the Statistics Act provide for the processing and use of resident registration information, identity information in family relationships and statistical information, respectfully. In addition, after the nationwide National Education Information System (NEIS) incident in 2003, the Elementary and Secondary Education Act was amended to regulate the use and protect student information in March 2005. In order to regulate the construction and operation of a National Manpower Resources Database managed by the Civil Service Commission, the Presidential Decree on the Regulations relating to the Collection and Management of Information on Public Official Candidates was enacted and proclaimed on September 30, 2005. The Act on the Lapse of Criminal Sentences is a law which specifically regulates the collection and use of an individual's sensitive data - their criminal records - and their provision to a third party. The Electronic Government Act was also enacted to provide for the joint use of administrative information, including personal data, between public organizations.

Meanwhile, special laws in the private sector include the Use and Protection of Credit Information Act, which was proclaimed on January 5, 1995 (implemented on July 6, 1995), the Act on Promotion of Information and Communications Network Utilization and Information Protection, which was enacted as an online personal data protection law (implemented on January 1, 2000), and the Bioethics and Safety Act, which specifically regulates the use and protection of genetic information (information acquired as a result of a genetic analysis) in the private sector. In 2005, with the rapid development in mobile telecommunications technology and emergence of various services utilizing location information in logistics, security and e-Commerce, the Act on the Protection, Use of Location Information (implemented on July 28, 2005) was enacted to create an environment which protects individuals' privacy from divulgence, misuse and abuse of location information and enables such information to be used safely.

2. Imbalance in the Protection System

The current personal data protection system in Korea can be said to harbor some imbalances in various aspects. A careful balance should be maintained between the two values of using and protecting personal data. However, imbalance in the protection system refers to the lack of a stricter protection system in an area which calls for greater protection due to a higher risk in personal data processing.

As examined above, the Personal Data Protection Act focuses exceedingly on the 'protection' of personal data and ignores the realistic values of the 'use' of such data, thereby creating an imbalance in the system. The stringent provisions of the Personal Data Protection Act focuses on the private sector, but it is the public sector which truly

requires a higher level of protection but has a vulnerable protection and implementation system.

Furthermore, the Electronic Government Act, which is the special law that provides for the joint use of personal data between public organizations, proclaims the "protection of personal data and privacy" as its operating principle, but at the same time, provides for the "expansion of joint use of administrative information (Article 4)". In Chapter 4 (Joint Use of Administrative Information) of the Act, it depicts that the "administrative information collected and possessed should be shared with another administrative agency which requires such information (Article 36)" while establishing an Administrative Information Joint Use Center (Article 37). The administrative information subject to joint use includes various personal data, including family relations information, real estate registration information and tax information (Article 38 of the Act and Article 43 of the enforcement ordinance of the same Act). Provided, however, in the event the administrative agencies need to jointly use such personal data, the Minister of Public Administration and Safety must authorize it after the deliberation and resolution by the Personal Data Protection Commission established pursuant to the Personal Data Protection Act (Article 39 Clause 4).

Such joint use of personal data is enabled by interconnected personal data DBs or computer matching, but there is skepticism regarding the installation of sufficient normative safety measures against potential misuse or abuse. The Electronic Government Act provides for the mandatory acquisition of prior consent of the data subject in the event of such joint use, but it is not without exceptions. Even if the consent were acquired, it would only be a mere formality for the civilian. This is why

the preventive and ex post facto supervision system regarding the joint use of personal data must operate effectively. Unfortunately, it is doubtful if the current Personal Data Protection Commission even possesses such supervision authority.

3. A Poor Preventive Administrative Function: Punishment-focused *Ex Post Facto* Administrative System

Personal data protection laws are legislations that delicately adjusts two conflicting values of use and protection of personal data. This is why the criteria for legal treatment (collection, use and provision) cannot be defined in black and white. Personal data protection is a field which must inevitably go through a complicated process of measuring the value of related interests. The Personal Data Protection Act not only lays down the criteria for authorized personal data processing (collection, use and provision), but also defines the procedural conditions that must be observed during the process of collection, use and provision. Furthermore, its basic goal lies in preventing the infringement of the personality interests and other rights and interests of the data subject by preventing the misuse or abuse of personal data processing.

This is the reason why in a personal data protection system, the "preventive enforcement" is of utmost importance. Preventive enforcement obligates the observation of legal criteria. It refers to the inducement of the personal data controller to faithfully observe the substantive provisions (authorized criteria of collection, use and provision) and procedural provisions (conditions to clarify purpose, quality management, notice and report) of the Personal Data Protection Act. Such preventive enforcement can be implemented through auditing, consulting, educating and the inducement of self-regulation.

The current personal data protection system, however, is worryingly vulnerable in terms of preventive enforcement. In particular, the Act on Promotion of Information and Communications Network Utilization and Information Protection, which is the online personal data protection law for the private sector, has an enforcement system which is concentrated on *ex post facto* punishment for any violations of legal criteria of collection, use and provision of personal data. The legal criteria not only puts greater emphasis on the value of protection, but the criteria itself is considerably unclear and vague. Based on such legal criteria, the administrative authorities unilaterally decides whether to impose an administrative sanction or criminal punishment. To make matters worse, the direction of the legislation is identical to that of the Personal Data Protection Act in the private sector. However, this ex post facto punishment-oriented enforcement is not effective in the personal data protection system. It may have a short-term effect, but with it, creating a continuous and practical enforcement effect, in other words, achieving the legislative purpose of safe use of personal data will not be no easy feat.

4. Resident Registration Number as a Universal Identifier and its Dangers

Granting every individual citizen a unique and permanent universal identifier and building an integrated management system enables the efficient identification of a country's citizens. This system offers such incredible efficacy that it is a temptation too great for any government to give it up easily. Recently in the United States and Europe, there are increasing voices proposing to build an integrated personal data management system. This proposal is based on a powerful rationale of employment control of illegal immigrants, efficient law enforcement, such as crime prevention,

prevention of welfare fraud, tracking down of tax evaders and enhancement of national health.

We all have various personal identifiers according to different transactions. Bank account numbers, credit card numbers, driver's license numbers, national health insurance numbers and passport numbers are but a few examples. They were originally made to be used separately for different purposes. The very fact that they exist in separate form can also be an automatic firewall against the formation of an integrated personal data management system.

Every Korean citizen receives, without a choice, a resident registration number as a universal identifier. Until very recently, they were required to submit their resident registration number in almost all transactions with the government or in the market. This is a tell-tale sign signifying that the firewall which could prevent the formation of an integrated personal data management system has already collapsed. Countless personal data DB already possessed by the government and companies have been built, without exception, based on resident registration numbers. This means that if the government and the market have the will, they can easily build a comprehensive integrated personal data management system. In other words, using the resident registration number of a person, they can trace virtually everything about that individual.

The recently amended Personal Data Protection Act regulates the collection of universal identifiers, such as resident registration numbers (Article 24). However, it is not possible to immediately prohibit the use of such ID numbers in existing personal

data databases already built with resident registration numbers. This remains a colossal challenge. In this regard, the Ministry of Public Administration and Safety, the Korea Communications Commission (KCC) and the Financial Services Commission (FSC) collaborated and announced the “Comprehensive Plan to Minimize the Collection and Use of Resident Registration Numbers”, which was passed by the Personal Data Protection Commission, on April 4, 2012. It provides, as a principle, to prevent the collection and use of resident registration numbers by public or private organizations in the future, and amplifies their responsibility to manage already collected data. Though the move comes somewhat belatedly, the government’s comprehensive countermeasure may hopefully become an important stimulant which halts the creation of an integrated personal data management system.

주제발표

“정보환경의 변화와 표현의 자유”

이 민 영*

(가톨릭대학교 법학부 교수)

Ⅰ. 논의를 시작하며

현재 우리의 정보환경[1]은 기존의 법제도에 대한 이론적·실증적 재검토를 요구하고 있다. 현실세계와 다름없이 인터넷으로 대표되는 정보사회에서도 사회적 비난이나 제재가 윤리적·법제적 규범위반의 결과로 나타나기 마련이지만,[2] 정보기술 발달과 행위규율의 대상인 의사소통체계 변모에 따른 입법수요 증대로 말미암아 법리적 쟁점이 부각되기 때문이다.

그런데 온라인상의 표현행위로 현실적인 권리침해를 받기도 하지만 당해 행위

* 가톨릭대학교 법학부 교수, myoegi@catholic.ac.kr

1) 정보환경이란 정보사회를 구성하는 기술적 환경을 뜻한다. 그 변화요인은 정보전달체계의 변모에서 비롯될 수도 있고 전송되는 정보의 형식의 변용으로 말미암을 수도 있지만, 핵심요건이 되는 것은 다름 아닌 기술발전이라 하겠다. 이는 물론 시스템 측면에서의 기술변이를 포함하는 것이지만, 전달내용인 정보 자체의 디지털화로 인해 매체속성에 구애받지 않아 통합적인 정보환경을 구축할 수 있는 계기를 마련하기 때문이다. 결국 정보환경은 정보기술을 근간으로 하여 정보사회를 형성하는 주요인이며, 그 변화에 따른 정보사회의 변모는 의사소통체계의 변혁으로 이루어지기 마련이다. 따라서 정보환경은 정보처리기술로만 형성되지 않는다. 사회적으로 의미 있는 정보전달체계와 연결되어 오히려 정보환경은 의사소통체계 자체를 뜻하는 개념으로 이해될 수도 있기 때문이다.

2) 따라서 바다를 이루는 인터넷의 정보가 불법적인 경우 기존의 형사법적·민사법적 대응이 적용될 수 있었으며, 인터넷의 특성에 기인하여 특유한 법제적 장치를 마련하는 조치가 필요한 때에는 이러한 역기능의 예방과 제거에 관한 제반논의가 입법적으로 뒤따르게 된다; Jessica L. *Chilson, Unmasking John Doe: Setting a Standard for Discovery in Anonymous Internet Defamation Cases*, 95 Va. L. Rev. 389, 389-390 (2009).

자체가 온라인상에서 누려야 하고 보호받아야할 권리를 제약하는 경우도 있기 때문에 이 같은 권익체계의 논의는 정보사회의 역기능 방지와 권리구제 차원에서 반드시 선행되어야 할 뿐만 아니라 그 구체화 과정에서 입법적·정책적 대책의 마련으로 이어져야 한다.[3)]

한편으로 정보사회에서의 전지구적 상호의존성은 인권정책의 수립에 있어 새로운 국면을 가져오는바,[4)] 인권옹호의 강화에 대한 구체적이고 효과적인 구조적 대응체계를 구축하기 어려운 상황에서 종래 시민적·정치적 자유의 전통적인 범주에 추가되는 보장대상으로서 인권 영역의 확대에 따라 보편적이면서 시대를 초월하는 인권 관념과는 상이하게도 사회환경의 변화에 응대하는 인권정책은 사회경제적인 변화로부터 자유로울 수 없는 역동적 속성을 지니고 있다고 볼 때 이를 제도화하는 법적 규율 역시 유연해야 한다.[5)]

우리의 경우 종래 정보인권에 대하여는 시민사회에서 인권의 보장과 증진에 이바지해온 시민사회단체를 중심으로 정보환경의 변화에 대응하는 정보사회에서의 인권 문제에 관심을 가지면서 '정보' 또는 '정보사회' 그리고 '인권'에 관한 숙려를 지속적으로 진행해온 데서 실천적 함의를 지닌다. 여기서 확인할 수 있듯이 '그리고(and)'라는 접속어는 짧고 간략한 단어임에도 불구하고 학문적 의미의 완결성에 있어서는 에티켓이나 예의상 또는 절차에 필요한 그 이상의 것(de rigueur)이 되었는바, 예를 들어 규제와 법·권리, 경제와 법·권리 및 문화와 법·권리

3) 현재 정보사회의 개념이 '정보의 생산·처리 및 활용기술이 사회발전의 원동력이 되고 사회구조를 지배하게 되는 사회'라는 의미로 통용되고 있으나 그 내용이 정확히 무엇을 뜻하는지 명백히 정의내리기란 그리 용이한 것만은 아니다; *Vgl.* Hans-Heinrich Trute, *Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung*, VVDStRL(Veroffentlichungen der Vereinigung der Deutschen Staatsrechtslehrer) 57, Berlin: Walter de Gruyter GmbH, 1998, S. 216f.

4) 모름지기 인권(人權; human rights)이라 함은 인간이 인간답게 존재하기 위한 보편적인 인간의 모든 정치·경제·사회·문화적 권리 및 지위와 자격을 총칭하는 개념이다. 다시 말하자면, 인권은 인간이 인간이기 때문에 당연히 가질 수 있고 누릴 수 있는 인간의 권리(*Menschenrecht*)인 것이고, 인간만이 보유하는 천부적 권리(inherent rights)이며, 법의 관할지역(jurisdiction)이나 그 밖에 민족 또는 국적 등과 상관없이 적용되는 것으로 정의된다.

5) Paolo Garonna & Evren Balta, *Measuring human rights: The challenges for the information society,* Statistical Journal of the UN Economic Commission for Europe 19(4), Amsterdam: IOS Press, 2002, pp.277~278.

등과 같이 새롭게 등장한 정보기술과 법·권리의 문제를 보다 함축적인 표현으로서 정보인권이라는 용어를 사용함으로써 정보사회에서의 다각적이고 다채로운 인간과 기술 그리고 권리와 법에 관한 제반문제에 직면할 수 있게 된다.[6] 어떠한 제한이나 통제 없이 자시의 견해를 피력하고 스스로 웹사이트를 운영할 수 있는 가능성이 누구에게나 열려있어 인터넷은 표현의 자유를 실현하기 위한 주요매체라 할 수 있지만,[7] 기본적 인권 역시 절대적인 것은 아니고 다른 사람의 권리를 존중하기 위해서나 공적 질서의 고려 차원에서는 일정한 제약이 요구된다는 점에서 오·남용되어서는 아니될 것이기 때문이다.[8]

인터넷을 위시한 정보통신망의 발전과 정보통신기술의 비약적 발전으로 말미암아 이른바 디지털콘텐츠라는 정보내용이 급속히 전달되는 현실 속에서 국가행정기관의 내용규제적 활동이 행정내부적 통제가 발휘되어야 할 현실적 요청은 증대된다. 물론 내용심의권한을 민간영역으로 이양하고 자율적으로 협의기준에 구속되도록 하는 방안이 중요쟁점이 될 수 있으므로 이를 아울러 여기서는 현행 규율체계 내에서 정보환경의 변화에 대응하는 내용규제의 정책적 방향과 그 통제방안을 모색하는 데 단초를 되짚어기로 한다.

---

6) Thérèse Murphy, *New Technologies and Human Rights*, NY: Oxford University Press Inc., 2009, p.7.

7) 인터넷에는 PC 통신처럼 모든 서비스를 제공하는 중심이 되는 호스트 컴퓨터도 없고 이를 관리하는 조직도 없으며, 인터넷상의 어떤 컴퓨터 또는 통신망에 이상이 발생하더라도 통신망 전체에는 영향을 주지 않도록 실제의 관리와 접속은 세계각지에서 분산적으로 행해지고 있다. 다만, 인터넷을 대표하는 조직으로 1992년 비영리기구로 설립된 ISOC(Internet Society; www.isoc.org)가 존재하고 있으나 이는 인터넷망의 총괄적 관리기구는 아니다. 한편, 이러한 다대다(多對多) 혹은 쌍방향 의사소통의 매체특성을 지니는 인터넷으로 말미암아 정보 수용자는 소비자군에서 소비와 동시에 생산을 담당하는, 즉 생산자와 소비자의 위치가 혼합된 개념으로서 생비자(生費者; prosumer) 지위로 전환되고 정보환경은 Web 2.0시대를 맞이하였다.

8) *See* Ronald Leenes, Bert-Jaap Koops, and Paul De Hert, *Constitutional Rights and New Technologies: A Comparative Study*, Hague: T·M·C·Asser Press, 2008, p.122.

Ⅱ. 정보인권으로서 표현의 자유 보장

1. 국제적 동향

주지하다시피, 일찍이 1953년 발효된 바 있는 유럽인권협약(European Convention for the Protection of Human Rights and Fundamental Freedoms; ECHR)[9]의 경우 제1조에서 '인권을 존중할 의무(obligation to respect human rights)'를 천명하면서,[10] 제8조에서는 '사생활과 통신에 관한 권리(right to respect for his private life and correspondence)'[11] 그리고 제10조에서는 '표현의 자유(freedom of expression)'에 대한 보장을 명시하고 있다.[12]

프랑스의 경우 1789년 8월 26일의 「프랑스 인권선언(인간과 시민의 권리선언;

9) 1950년 11월 4일에 채택되고 1953년 9월 3일부터 그 효력이 발생한 유럽인권협약은 세계인권선언 중 몇 가지 권리의 집단적 보장을 확보하기 위한 적절한 최초의 수단을 취하는 데 목적이 있으며, 조인 당시 합의에 이르지 않았거나 후에 합의할 필요가 있는 것에 대해서는 의정서에 의해서 보충하는 형식을 취하고 있다. 이는 세계 최초의 종합적인 인권조약으로서 유엔인권규약 제정에 영향을 주었다; Thomas Buergenthal, *International Human Rights*, St. Paul, Minn.: West Publishing Co., 1988; 양건·김재원 譯, 국제인권법, 교육과학사, 2001, 68쪽.

10) European Convention for the Protection of Human Rights and Fundamental Freedoms §1 (obligation to respect human rights) The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.

11) European Convention for the Protection of Human Rights and Fundamental Freedoms §8 (Right to respect for private and family life) ① Everyone has the right to respect for his private and family life, his home and his correspondence.
② There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

12) European Convention for the Protection of Human Rights and Fundamental Freedoms §10 (Freedom of expression) ① Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
② The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Declaration des droits de l'homme et du citoyen)」 제11조[13]에서 그 유래를 찾을 수 있는 프랑스 헌법에서의 표현의 자유에 관한 권리 역시 가장 중요하고 핵심적인 인권 가운데 하나로서 사상과 견해의 자유로운 의사소통으로 인식되어진다. 그리고 표현의 자유에 대한 보장의 중핵은 이용되는 수단이나 매개체와는 상관없는 의사소통 그 자체라고 할 수 있다.[14]

한편, 독일에서는 표현의 자유 보장을 천명하고 검열금지원칙을 선언하고 있는 기본법 제5조제1항은 "*Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt.*"[15]라고 명시하여 헌법상 기본적 인권으로서 그 보호가 자유민주주의의 핵심이라 할 수 있고 광의의 정보인권에 해당하는 표현의 자유에 대한 헌법적 근거를 정립하고 있다.[16]

미국에서는 정보에 관한 권리가 공적으로 가용한 정보를 자유롭게 검색하고 타인이 의사소통을 위해 교환하려는 모든 정보를 수취할 권리로서 정보의 자유가 사상과 의견의 표현권(right to express opinions)과 아울러 표현에 관한 자유(freedom of expression)[17]에서 도출된다고 여긴다.[18] 물론 여기서의 접근대상이자

13) *La libre communication des pensées et des opinions est un des droits les plus précieux de l'Homme: tout Citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté, dans les cas déterminés par la Loi.*

14) Ronald Leenes, Bert-Jaap Koops, and Paul De Hert, *Constitutional Rights and New Technologies: A Comparative Study*, Hague: T・M・C・Asser Press, 2008, pp.122~123.

15) "Every person shall have the right freely to express and disseminate his opinions in speech, writing, and pictures and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorship."

16) *BVerfG Urteil vom* 15.11.1982, *BVerfGE* 62, 230, 247; 26.07.1990, *BVerfGE* 82, 272, 281.

17) *See* 「American Convention on Human Rights(Signed at the Inter-American Specialized Conference on Human Rights, San Josi, Costa Rica, 22 November 1969)」 §13 (Freedom of Thought and Expression) ① Everyone has the right to freedom of thought and expression. This right includes freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing, in print, in the form of art, or through any other medium of one's choice.

권리객체로서 정보는 공적 정보(public information or official information)와 사적 정보(private information or personal information)를 모두 아우르며, 이로써 보호법익이 되는 권리는 정보제공자 관점에서 수동적인 개념인 '알 필요(need to know)'에 머무르지 않고 정보수신자 측면에서 적극적인 '알 권리(right to know)'로의 변모에서 비롯되는 정보접근[19] 및 정보공개청구를 중핵으로 한다.[20] 이러한 견지에서 정보(접근)권[right to (access) information; RTI]과 정보의 자유(freedom of information; FOI)는 기본적 인권(fundamental human rights)로서 동일한 개념으로 파악되는바, 정보의 결핍으로 인하여 일반 국민이 그들의 잠재력을 충분히 계발하고 광범위한 인권을 실현하는 기회를 박탈되는 까닭에 이와 같은 정보인권의 의의는 공적 권

---

② The exercise of the right provided for in the foregoing paragraph shall not be subject to prior censorship but shall be subject to subsequent imposition of liability, which shall be expressly established by law to the extent necessary to ensure:

a. respect for the rights or reputations of others; or

b. the protection of national security, public order, or public health or morals.

③ The right of expression may not be restricted by indirect methods or means, such as the abuse of government or private controls over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions.

④ Notwithstanding the provisions of paragraph 2 above, public entertainments may be subject by law to prior censorship for the sole purpose of regulating access to them for the moral protection of childhood and adolescence.

⑤ Any propaganda for war and any advocacy of national, racial, or religious hatred that constitute incitements to lawless violence or to any other similar action against any person or group of persons on any grounds including those of race, color, religion, language, or national origin shall be considered as offenses punishable by law.

18) Kyrre Eggen, *The Protection of Freedom of Expression in Article 10 in the European Convention of Human Rights*, Oslo: Oslo University Press, 1994, p.63.

19) 이와 같은 정보(접근)권은 민주적인 참여와 이해로써 공감대를 형성하고 과오를 청산하는 데 이바지하며 의사결정절차의 투명성을 제고할 뿐만 아니라 타인의 권리를 보호하는 데 그 의의가 있다; Rikke Frank Jørgensen, *Human Rights in the Global Information Society*, Cambridge, MA: The MIT Press, 2006, pp.73~77.

20) Philip Coppel, *Information Rights: Law and Practice*, Portland, Oregon: Hart Publishing, 2010, pp.36~37; 미국에서는 알 권리의 헌법상 근거로서 주로 표현의 자유(freedom of expression)에 관하여 "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances"라고 규정하고 있는 연방헌법 증보(The United States Constitution Amendment) 제1조를 드는 것이 일반적이지만 여기에 국민주권원리를 결부하여 파악하는 견해도 유력하다.

위에 대한 접근을 보장하면서 궁극적으로 통치체제에 대한 투명성과 책임성을 제고하는 데 있다고 볼 것이다.[21]

국제연합총회에서 1948년 12월 10일 채택된 세계인권선언(Universal Declaration of Human Rights)은 제19조에서 "모든 사람은 의견과 표현의 자유에 관한 권리를 가진다. 이 권리는 간섭받지 않고 의견을 가질 자유와 모든 매체를 통하여 국경에 관계없이 정보와 사상을 추구하고 접수하며 전달하는 자유를 포함한다."고 규정하고 있는데,[22] 이것이 정보기본권의 직접적인 근거는 될 수 없다 하더라도 '알 권리'를 명시하고 있는 것이며 그 구체성에 있어서는 이를 참조한 우리 헌법조문보다 정확성을 보유하고 있다는 점을 알 수 있다. 그렇기에 일반 국민에 대한 정보접근권은 헌법적으로 제도 보장이 갖추어져 있는 것으로 해석할 수 있는 것이며, 우리 헌법재판소의 결정례는 알 권리와 관련 정보접근권에 대해 설시하고 있어 판례로써 확인된다고 할 것이다.[23]

아무튼 이러한 규범적 인정은 정보환경의 변화에 따라 표현의 자유에 대한 정보표현권적 지위를 저목하게 한다. 지난 2003년 12월 8일 만장일치로 채택된 '정보사회 세계정상회의시민사회 최종선언문(Civil Society Declaration to the WSIS)'은 「인류의 요구에 상응하는 정보사회의 형성(Shaping Information Societies for Human Needs)」이라는 제언 아래 정보사회에서의 기본적 인권(human rights that are fundamental to the information and communications society),[24] 즉 정보인권의 구심점(Centrality of Human Rights)으로 표현의 자유(Freedom of Expression)를 위시한 세부 유형을 열거하여 포괄적 접근 시각에서 이를 논의하고 있음은 이를 반영하고 있다.[25] '정보사회 세계정상회의(WSIS)'의 목표는 정보사회에서 공유해야 할 원칙

21) KM Shrivastava, *The Right to Information: A Global Perspective*, Frankfort, IL: Lancer Inter Consult, Inc., 2009, p.1.

22) 물론 위 선언은 도의적 지침에 지나지 않지만 이 내용은 1976년에 발효된 '시민적 및 정치적 권리에 관한 국제규약(International Covenant on Civil and Political Rights)' 제19조에 반영되어 규약당사국에 대해 국제법상 구속력을 발휘하고 있다.

23) 대표적인 결정례로 헌법재판소 1989. 9. 4. 88헌마22결정 참조.

24) http://www.itu.int/wsis/docs/geneva/civil-society-declaration.pdf

과 행동강령을 통하여 국제사회의 정보적 대응에 지도적 지원을 행하고 이에 대한 실행과 실천을 확장적으로 이끌어가는 데 있기 때문이다.[26]

2. 국내의 현황

정보표현권은 우리 헌법 제1조에 그 근간을 둔 기본적 인권이다. 정보를 매개로 사상・의견 등을 전달하는 광의의 의미로도 여겨지지만, 정보의 수령이나 제공 그리고 그 거부에 관한 독자적인 정보취급권으로서 좁은 의미의 정보인권을 내포한다고도 볼 수 있다. 다시 말해 표명과 전달의 대상이 정보의 표현일 수도 있고 아닌 경우도 있으며 표현이 아닌 오로지 정보의 취급과 관련될 수도 있기 때문이다.

「대한민국헌법」 제21조는 제1항과 제2항에서 "모든 국민은 언론・출판의 자유를 가지며, 언론・출판에 대한 허가나 검열은 인정되지 아니한다."고 규정하고 있는바, 여기서 언론・출판은 표현에 대한 예시로서 표현의 자유에 대한 일반적 보장을 명시한 것이라 하겠다.

인간의 존엄과 가치의 유지 및 국민주권의 실현에 있어 필수불가결한 것으로 오늘날 민주국가의 인권체계 중 국민이 갖고 있는 가장 중요한 기본권의 하나로서의 지위를 차지하고 있는 표현의 자유는, 역사적으로 개인의 의견표명이나 정치적 비판이 공권력에 의해서 제한되고 탄압을 받은 결과 이에 대항하여 그 보장이 확립된 것이다. 그렇기 때문에 표현의 자유는 비단 개인적 기본권에 그치지 않고 민주적 여론형성에 필수적인 제도라 할 수 있다. 이와 같은 의미에서 표현의 자유는 민주주의의 제도적 토대이자 한 사회에서의 민주화의 척도로서 민주적 정치질서 내지는 법질서를 이루는 수단이 된다고 할 것이며, "표현의 자유가 다른 기본

25) '정보사회 세계정상회의(WSIS)'의 인권 평가에 대하여는 *See generally* Meryem Marzouki & Rikke Frank Jørgensen, *A Human Rights Assessment of the World Summit on the Information Society*, Information Technologies and International Development Vol.1: 3-4, Los Angeles, CA: Annenberg Press, University of Southern California, 2004, pp.86~88.

26) Rikke Frank Jørgensen, *Human Rights in the Global Information Society*, Cambridge, MA: The MIT Press, 2006, pp.5~6.

권에 우선하는 헌법상 지위를 갖는다."라고 일컬어지는 것도 그것이 단순히 개인의 자유에 그치는 것이 아니라 통치권자를 비판함으로써 피치자(被治者)가 스스로 지배기구에 참가한다는 자치정체(自治政體)의 이념을 그 근간으로 하고 있기 때문이라고 할 수 있다. 일찍이 John Milton이 영국 정부의 출판 검열조치에 반발하여 불법 출판했던 「Areopagitica」에는 진실과 거짓이 맞붙어 싸우게 된다면 결국 진실이 승리하기 마련이므로 정부의 언론통제는 불필요하다는 주장을 펼치는 대목이 기술되어 있는바,[27] 여기에는 설령 유해한 사상이나 표현이라도 그 해악의 교정은 사상의 공개시장에서 대립되는 사상이나 표현에 의한 경합을 통해 이루어져야 한다는 믿음이 깔려있고 종국적으로 표현의 자유에 대한 민주주의의 근간의 확신을 역설하고 있다. 물론 표현의 자유에 관하여 규정하고 있는 우리 헌법 제21조 역시 이러한 이념적·철학적 토대에 근거해 있다고 하겠다. 그리고 이러한 표현의 자유는 전통적으로는 사상 또는 의견의 자유로운 표명(발표의 자유)과 그것을 전파할 자유(전달의 자유)를 의미하고 그 내용으로 의사표현·전파의 자유, 정보의 자유, 신문의 자유 및 방송·방영의 자유 등이 있는데, 의사표현·전파의 자유에 있어서 매개체는 담화·연설·토론·연극·방송·음악·영화·가요 등과 문서·소설·시가·도화·사진·조각·서화 등 모든 형상의 의사표현 또는 의사전파의 매개체를 포함한다.[28]

27) "진리와 허위가 대결하게 하라.…모든 사람으로 하여금 자유롭게 말할 수 있게 하라. 그러면 진리의 편이 반드시 생존하고 승리한다. 허위와 불건전은 사상의 공개시장(the open marketplace of ideas)에서 다투다가 마침내는 패배하리라. 권력은 이러한 선악의 싸움에 일체 개입하지 말라. 설혹 허위가 일시적으로 득세하는 일이 있더라도 선악과 진위가 자유롭게 싸워간다면 마침내 선(善)과 진(眞)이 자기교정과정(self-righting process)을 거쳐 궁극적인 승리를 얻게 되리라."; John Milton, *Areopagitica; A Speech of Mr. John Milton for the Liberty of Unlicensed Printing to the Parliament of England*, 1644: 김동민, 언론법제의 이론과 현실, 한나래, 1993, 15쪽.

28) 헌법재판소 1993. 5.13. 91헌바17, 판례집 5-1, 275, 284; 2001. 8.30. 2000헌가9, 판례집 13-2, 134, 148; 2002. 4.25. 2001헌가27, 판례집 14-1, 251, 265; 2004. 1.29. 2001헌마894, 판례집 16-1, 114, 132 참조.

Ⅲ. 방송통신심의 법제에 관한 재검토

1. 문제의 제기

우리 헌법 제21조제1항은 “모든 국민은 언론·출판의 자유와 집회·결사의 자유를 가진다.”고 규정하여 언론의 자유를 일반적으로 보장하고, 제2항은 “언론·출판에 대한 허가나 검열과 집회·결사에 대한 허가는 인정되지 아니한다”고 규정하여 언론에 대한 검열금지원칙을 명문화하고 있다. 하지만 헌법은 언론에 대한 검열금지원칙을 선언하면서 헌법이 금지하는 검열이 구체적으로 어떠한 것인지에 대하여는 규정하고 있지 않다. 헌법재판소는 영화법 제12조 등에 대한 위헌제청 사건에서 다음과 같이 검열제도가 금지되어야 하는 이유와 헌법 제21조 제2항에서 규정하는 검열개념의 기준을 제시하였다.[29]

> 헌법 제21조 제1항과 제2항은 모든 국민은 언론·출판의 자유를 가지며, 언론·출판에 대한 허가나 검열은 인정되지 아니함을 규정하고 있다. 여기서의 검열은 행정권이 주체가 되어 사상이나 의견 등이 발표되기 이전에 예방적 조치로서 그 내용을 심사·선별하여 발표를 사전에 억제하는, 즉 허가받지 아니한 것의 발표를 금지하는 제도를 뜻한다. 이러한 검열제가 허용될 경우에는 국민 예술활동의 독창성과 창의성을 침해하여 정신생활에 미치는 위험이 클 뿐 아니라 행정기관이 집권자에게 불리한 내용의 표현을 사전에 억제함으로써 이른바 관제의견이나 지배자에게 무해한 여론만이 허용되는 결과를 초래할 염려가 있기 때문에 헌법이 직접 그 금지를 규정하고 있는 것이다. 그러므로 헌법 제21조 제2항이 언론·출판에 대한 검열금지를 규정한 것은 비록 헌법 제37조 제2항이 국민의 자유와 권리를 국가안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률로써 제한할 수 있도록 규정하고 있다고 할지라도, 언론·출판의 자유에 대하여는 검열을 수단으로 한 제한만은 법률로써도 허용되지 아니함을 밝힌 것이다. 물론 여기서 말하는 검열은 그 명칭이나 형식에 구애됨 없이 실질적으로 위에서 밝힌 검열 개념에 해당되는 모든 것을 그 대상으로 하는 것이다. 그러나 검열금지의 원칙은 모든 형태의 사전적 규제를 금지하는 것이 아니고, 단지 의사표현의 발표 여부가 오로지 행정권의 허가에 달려있는 사전심사만을 금지하는 것을 뜻한다. 따라서 검열은 일반적으로 허가를 받기 위한 표현물의

29) 헌법재판소 1996.10. 4. 선고 93헌가13등 결정, [판례집 8-2] 212, 222-223.

제출의무, 행정권이 주체가 된 사전심사절차, 허가받지 아니한 의사표현의 금지 및 심사절차를 관철할 수 있는 강제수단 등의 요건을 갖춘 경우에만 이에 해당하는 것이다.

여기서 헌법재판소는 허가를 받기 위한 표현물의 제출의무, 행정권이 주체가 된 사전심사절차, 허가를 받지 아니한 의사표현의 금지, 심사절차를 관철할 수 있는 강제수단 등의 요소를 사전검열의 판단기준으로 제시하였는 바, 이후 지난 2001년 8월 30일 헌법재판소는 영화진흥법 제21조 제4항 위헌제청 사건에서 위 기준에 입각하여 영상물등급위원회가 영화에 대한 등급분류를 일정기간 보류할 수 있게 하는 영화진흥법상의 영화등급분류보류제도가 헌법이 금지하는 사전검열에 해당하는 것으로 보아 헌법에 위반됨을 선언하였다.[30]

하지만 정보가 유통된 이후 국가행정기관이 사후적으로 이에 대하여 제한하는 것은 사전검열에 해당하지 않으면서도 내용규제(內容規制)라는 구체적 법집행[31]이 이루어지고 있다.[32] 그러므로 규범적으로 적법하지 못한 것으로 상정되어 있는 정보의 유통에 대하여는 국가행정기관이 그 차단을 법집행작용으로서 행하며,

---

30) 영상물등급위원회의 경우에도…(中略)…그 구성방법 및 절차에 관하여 필요한 사항은 대통령령으로 정하도록 하고 있으며, 국가예산의 범위 안에서 운영에 필요한 경비의 보조를 받을 수 있도록 하고 있는 점 등에 비추어 볼 때, 행정권이 심의기관의 구성에 지속적인 영향을 미칠 수 있고 행정권이 주체가 되어 검열절차를 형성하고 있다고 보지 않을 수 없다. 영상물등급위원회가 비록 그의 심의 및 등급분류활동에 있어서 독립성이 보장된 기관이라 할지라도, 그것이 검열기관인가 여부를 판단하는 데 있어서 결정적인 것이라고는 할 수 없다. 심의기관의 독립성이 보장되어야 하는 것은 단지 심의절차와 그 결과의 공정성 및 객관성을 확보하기 위하여 모든 형태의 심의절차에 요구되는 당연한 전제일 뿐이기 때문이다. 국가에 의하여 검열절차가 입법의 형태로 계획되고 의도된 이상, 비록 검열기관을 민간인들로 구성하고 그 지위의 독립성을 보장한다고 해서 영화진흥법이 정한 등급분류보류제도의 법적 성격이 바뀌는 것은 아니다; 헌법재판소 2001. 8.30. 선고 2000헌가9 결정, [판례집 13-2] 134, 150.

31) 지난 1997년 8월 법률 제5368호로 제정된 「행정규제기본법」은 '행정규제에 관한 기본적인 사항을 규정하여 불필요한 행정규제를 폐지하고 비효율적인 행정규제의 신설을 억제함으로써 사회·경제활동의 자율과 창의를 촉진하여 국민의 삶의 질을 높이고, 국가경쟁력의 지속적인 향상을 도모함'을 목적으로 하며, 제2조제1항제1호에서 행정규제의 개념을 적극적으로 정의하여 '국가 또는 지방자치단체가 특정한 행정목적을 실현하기 위하여 국민의 권리를 제한하거나 의무를 부과하는 것으로서 법령 등 또는 조례·규칙에 규정되는 사항'으로 새기고 있다. 따라서 내용규제 역시 법규성을 보유한 추상적 규범을 구체적 법집행으로 실현하는 행정작용이라 할 것이다.

32) 정보매체에 대한 규제는 그 소유 및 운영, 시장내 질서, 다른 매체나 역무와의 관계를 규율하는 구조적 규제(structural regulation)로서의 形式規制와 이를 제외한 나머지 부분으로서 정보내용의 실질과 편성에 관한 內容規制로 유형화할 수 있다. 전자적 정보(electronic information)를 전달하는 정보매체의 개념에 대하여는 拙著, 컨버전스와 미디어법, 한국학술정보, 2008, 이하 참조.

이와 같은 행정작용이 취소되지 않는 한 사법권의 종국적인 판단이 내려지기까지는 그 공정력(公定力)으로 적법성을 추정받게 되는 것이다. 다시 말하자면, 당해 행정청이 표현의 자유에 대한 제한으로서 정보내용을 규제하는 것을 직권으로 취소하거나 법원의 재판에 따라 취소되지 않는 한 해당 규제작용은 위법하지 않은 것으로 간주된다는 것이다. 이런 까닭에 행정의 법률적합성을 관철하기 위한 행정통제적 기제가 내외적으로 발동되어 규제에 있어서 행정기관이 보유하는 재량권의 유월이나 절차적 준수사항의 위배 등을 사전에 봉쇄할 필요성이 존재한다.

2. 쟁점 재검토

최근 「방송통신위원회의 설치 및 운영에 관한 법률」 제21조제4호 위헌제청사건에 대한 헌법재판소 결정에서 본안 판단 이전에 논의된 재판의 전제성에 대한 판단 부분은 그 결론을 차치하고서라도 문제가 있다고 판단된다.[33]

가. 시정요구의 성격

(1) 심의위원회가 행정기관인지 여부

이 사건 법률조항은 방송통신심의위원회(이하 '심의위원회'라 한다)의 직무의 하나로 '전기통신회선을 통하여 일반에게 공개되어 유통되는 정보 중 건전한 통신윤리의 함양을 위하여 필요한 사항으로서 대통령령이 정하는 정보의 심의 및 시정요구'를 규정하고 있다.

심의위원회는 방송 내용의 공공성 및 공정성을 보장하고 정보통신에서의 건전한 문화를 창달하며 정보통신의 올바른 이용환경 조성을 위하여 「방송통신위원회의 설치 및 운영에 관한 법률(이하 '방송통신위원회법'이라 한다)」에 의하여 설립된 기관으로(제18조 제1항), 심의위원회의 위원은 대통령이 위촉하고, 구성과 운영

33) 헌법재판소 2012. 2.23. 2011헌가13 결정.

에 관하여 필요한 사항은 대통령령으로 정하도록 하고 있으며(제18조 제3항, 제7항), 별도의 기금 이외에 국고에서 심의위원회의 운영 등에 필요한 경비를 지급받을 수 있도록 하고 있다(제28조). 심의위원회는 이 사건 법률조항에서 정한 정보의 심의 및 시정요구 외에 방송법 제100조에 따른 제재조치 등에 대한 심의·의결 등을 할 수 있고, 심의규정의 제정 및 공표를 하며, 심의규정에 위반되는 경우에는 그 제재조치를 결정할 수 있다(제21조, 제24조, 제25조).

이와 같이 심의위원회의 설립, 운영, 직무에 관한 내용을 종합하면, 심의위원회를 공권력 행사의 주체인 국가행정기관이라 인정할 수 있다.

(2) 시정요구의 종류 및 효과

(가) 시정요구의 종류는 해당 정보의 삭제 또는 접속차단, 이용자에 대한 이용정지 또는 이용해지, 청소년유해정보의 표시의무 이행 또는 표시방법 변경 등과 그 밖에 필요하다고 인정하는 사항이다(방송통신위원회법 시행령 제8조 제2항).

(나) 정보통신서비스제공자 또는 게시판 관리·운영자는 시정요구를 받은 경우 그 조치결과를 심의위원회에 지체 없이 통보하여야 한다(방송통신위원회법 시행령 제8조 제3항).

정보통신서비스제공자 등이 시정요구에 따르지 아니하는 경우, 해당 정보가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 '정보보호법'이라고 한다)」 제44조의7 제1항 제1호부터 제6호까지의 규정에 따른 불법정보인 때에는, 심의위원회는 방송통신위원회에 정보통신서비스제공자 등으로 하여금 그 취급거부·정지 또는 제한을 하도록 하는 명령을 하여 줄 것을 요청할 수 있고(방송통신위원회법 시행령 제8조 제4항), 방송통신위원회는 이에 따라 정보통신서비스제공자 등으로 하여금 그 취급을 거부·정지 또는 제한하도록 명할 수 있다. 다만, 정보보호법 제44조의7 제1항 제2, 3호

에 해당하는 '사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보'나 '공포심이나 불안감을 유발하는 부호・문언・음향・화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보'의 경우에는 해당 정보로 인하여 피해를 받은 자가 구체적으로 밝힌 의사에 반하여 그 취급의 거부・정지 또는 제한을 명할 수 없다(정보보호법 제44조의7 제2항).

또한 해당 정보가 정보보호법 제44조의7 제1항 제7호부터 제9호까지의 정보에 해당하는 경우에는 관계 중앙행정기관의 장의 요청이 있고, 심의위원회가 시정요구를 하였지만 정보통신서비스제공자 등이 시정요구에 따르지 아니하였을 것을 요건으로 방송통신위원회는 정보통신서비스제공자 등에게 해당 정보의 취급을 거부・정지 또는 제한하도록 명하여야 한다(정보보호법 제44조의7 제3항).

정보보호법 제44조의7 제2항 및 제3항에 따른 방송통신위원회의 명령을 이행하지 아니한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다(정보보호법 제73조 제5호).

(다) 한편 시정요구에 대하여 정보통신서비스제공자 등과 이용자는 그 시정요구를 받은 날부터 15일 이내에 심의위원회에 이의신청을 할 수 있다(방송통신위원회법 시행령 제8조 제5항).

(3) 표현의 자유와의 관련성

(가) 우리 헌법은 모든 국민에게 표현의 자유를 보장하고 있는바(헌법 제21조), 그 중요성을 고려할 때 형사처벌 등 법적 제재가 수반되지 않더라도 만일 해당 공권력의 행사가 표현의 자유를 위축시켜 상대방으로 하여금 스스로 표현행위를 자제하게 만든다면, 그 공권력 작용은 그 정도에 따라 표현의 자유를 제한하는 것이라고 볼 수도 있다.

(나) 이 사건 시정요구는 행정지도 내지 권고의 외관을 띠고 있지만, 그 요구의 상대방은 표현의 자유를 침해당하는 해당 정보의 게시자가 아니라 사실상 제3자인 서비스제공자 등이고, 서비스제공자 등은 게시글의 유지보다는 사업상의 감독기관인 방송통신위원회 및 심의위원회와의 원활한 협조관계에 월등한 이해관계를 갖고 있으므로, 정보의 삭제 등 시정이 정보게시자의 의사나 동의에 의해서가 아니라 행정기관의 개입과 이에 따르는 서비스제공자 등의 이행에 의하여 이루어질 가능성이 높다.

또한 시정요구는 해당 정보의 삭제 또는 접속차단을 넘어 이용자에 대한 이용정지 또는 이용해지에까지 이를 수 있으므로, 정보통신망의 이용자의 표현의 자유를 위축시켜 스스로 표현행위를 자제하게 만드는 위축효과가 결코 작다고 할 수 없다.

(4) 소결

(가) 이상에서 본 바와 같이, 행정기관인 심의위원회의 시정요구는 정보통신서비스제공자 등에게 조치결과 통지의무를 부과하고 있고, 정보통신서비스제공자 등이 이에 따르지 않는 경우 방송통신위원회의 해당 정보의 취급거부·정지 또는 제한명령이라는 법적 조치가 예정되어 있으며, 행정기관인 심의위원회가 표현의 자유를 제한하게 되는 결과의 발생을 의도하거나 또는 적어도 예상하였다 할 것이므로, 이는 단순한 행정지도로서의 한계를 넘어 규제적·구속적 성격을 갖는 것으로서 헌법소원 또는 항고소송의 대상이 되는 공권력의 행사라고 봄이 상당하다.

(나) 따라서 이 사건 법률조항의 재판의 전제성이 인정된다.

이와 같이 헌법재판소는 심의위원회의 법적 성격을 국가행정기관으로 규정짓고 심의위원회의 시정요구를 쟁송법상 처분 개념, 즉 '행정청이 행하는 구체적 사실

에 관한 법집행으로서의 공권력의 행사 또는 그 거부와 그 밖에 이에 준하는 행정작용'에 포섭시키고 있다. 그렇지만 쟁송법상 처분은 기능적 관점에서 행정청으로 파악되는 기관(organ)의 집행권 행사인 까닭에 국가행정기관에 한정되어 발현되는 것은 분명 아니다. 「행정소송법」 제2조제2항이 "이 법을 적용함에 있어서 행정청에는 법령에 의하여 행정권한의 위임 또는 위탁을 받은 행정기관, 공공단체 및 그 기관 또는 사인이 포함된다."라고 규율하고 있는 것도 이 때문이며, 따라서 지방자치단체의 기관이나 공공기관도 행정청이 될 수 있다고 하겠다. 이러한 논의는 심의위원회의 내용규제가 사전심사에 해당할 경우 헌법에서 명시되어 있는 검열금지원칙과 충돌하는 것인지 여부 그리고 현행 법제구조의 현황 및 문제점을 진단해 바람직한 규제구도를 형성하는 데 결정적 단서를 제공하기 때문이라는 점을 우선 분명히 해두도록 한다.

원래 심의는 사전적으로는 '어떤 사항에 관하여 상세하고 치밀하게 토의하는 일'이라고 정의할 수 있는바, 법적 개념으로서 심의(審議; deliberation)는 완전한 결정을 내리기 위하여 논리와 추론의 사용을 강조하는 의사소통방식으로서 법적 발견을 토론하는 과정이자 논쟁에 대한 결정을 말한다.[34] 그리고 '자유로운 토론과 자유로운 투표'라는 원칙에 따라 이루어지는 것이라는 점에서 심의는 결국 심리(審理; hearing)와 의결(議決; resolution)의 합성개념이라 볼 수 있다.[35] 여기서 심리라 하면 공정한 심의의 기초가 되는 사실관계 및 법률관계를 명확히 하기 위하여 조사하는 공식적 심사행위이며, 의결이라 하면 공정한 심의를 이끌어내기 위하여 심리한 사항에 대해 합의체에서 그 의사를 결정하는 종국적 행위라 할 수 있다. 그러기에 심의는 심리와 의결의 연속적 결합행위라 할 것이며, 이러한 심의는 특히 정보매체에 대한 규제 가운데 정보내용의 실질과 편성에 관한 내용규제에 있어서 규제기준에 의거하여 내용물, 즉 콘텐츠에 대하여 행하는 검토과정이라 하겠다.

---

34) http://en.wikipedia.org/wiki/deliberation

35) 관련법령에서는 이를 '심의·의결'이라는 용어를 사용하고 있지만, 여기서는 내용규제의 1차적 단계로서 의사결정 이전의 심사절차를 뜻하는 '심리'와 종국적 판단으로서의 '의결'이 결합된 '심의'라는 용례를 취하기로 한다.

한편, 방송통신심의라 함은 정보매체로서 방송 및 정보통신에 있어서의 내용규제적 검토과정인 심의를 함께 묶어 표현한 것이라 할 것인데, 이에 대하여는 방송과 통신이 융화하고 결합하는 정보환경에 관한 논의가 결부되어 있다. 주지하는 바와 같이 이처럼 기존의 방송과 통신의 경계가 허물어지고 융합(convergence)[36] 하는 정보환경을 통신방송융합이라 칭하며,[37] 그 법적 토대로서 방송통신위원회법의 제정을 기초로 하여 방송통신위원회의 제도적 발족이 이루어졌음이야말로 방송통신심의의 태생적 배경이라고 할 수 있다. 환원하자면, 기존의 통신과 방송의 각 영역으로 분산하여 내용규제적 검토과정인 심의를 구(舊) 정보통신윤리위원회와 방송위원회가 분장하여 담당해온 과거의 체제에 대응하여 융합환경에서 새롭게 등장하는 매체(media)와 역무(service)에 대한 심의를 전담케 함으로써 해당 내용물이 방송프로그램인지 정보통신 콘텐츠인지를 분별하게 하고 그 경계영역의 것이라 할지라도 내용규제적 심사와 종국적 의사결정이 이행될 수 있는 구조적 장치가 바로 방송통신심의라 할 수 있다. 이와 같은 방송통신심의는 행정법상 준법률행위적 행정행위로서 확인(確認)에 해당한다.[38] 그리고 심의위원회의 심의결

---

36) 사전적 의미에서의 융합은 서로 다른 방향으로부터 같은 지점으로 접근하거나 서로 교차하는 것을 의미하며 나아가 연합(union) 및 공통적인 결론(common conclusion)을 향하여 움직이는 것을 뜻한다. 이 용어가 커뮤니케이션 분야에 적용될 때에는 서로 다른 매체체제나 조직형태가 결합하고 교차하는 것을 말한다; E. E. Dennis & J. V. Pavlik, The coming of convergence and its consequences, in: Demystifying Media Technology, Mountain View, CA: Mayfield, 1993, p.2.

37) 일반적으로 융합이란 독립하여 존재하는 두 가지가 화합하여 새로운 제3의 것을 탄생시키는 것을 말하며, 기술발전에 따라 종래 분리 규율되어온 음성·영상 및 데이터 역무 등이 융화되는 현상이 주목받고 있다. 다시 말해, 통신방송융합이란 별개로 분리된 영역이었던 방송과 통신이 기술의 발전과 수용의 다양화에 따라 망(network)과 역무(service)의 구분이 점차 사라져 산업적 구조와 제도가 지속적으로 통합되어 가는 현상을 말한다고 할 것이다. 하지만 융합이라는 것이 화학적인 완전한 용해를 의미하기 보다는 결합되는 양자가 그 속성을 유지한 채 중첩된 영역을 만들고 각각 그 요인에 영향을 받는 것이므로, 서로 다른 두 영역이 완전히 합치되는 것이 아님에 유의할 필요가 있다; 拙稿, 정보매체의 규제조직에 관한 법적 연구, 공법연구 제36집 제3호, 한국공법학회, 2008, 488쪽.

38) 행정행위는 그 구성요소 및 법률효과의 발생원인에 따라 법률행위적 행정행위와 준법률행위적 행정행위로 구분된다. 법집행을 위한 효과의사를 요소로 하고 효과의사의 내용에 따라 법률효과가 발생하는 행정행위를 법률행위적 행정행위라 하는 반면, 준법률행위적 행정행위는 판단이나 인식 같은, 효과의사 이외의 정신작용을 요소로 하고 법규가 정하는 바에 따라 법률효과가 발생하는 행정행위를 말한다. 또한 준법률행위적 행정행위의 한 유형으로서 확인은 특정한 사실 또는 법률관계에 관하여 의문이나 다툼이 있는 경우에 공권적으로 그 존부(存否) 또는 정부(正否)를 판단·확정하는 행위를 말하며, 법선언적 행위이자 준사법적 행위(quasi-judicial act)가 될 수 있다. 그리고 확인은 일반적으로 특정한 법률사실 또는 법률관계의 존재나 정당성을 공권적으로

과인 의결로서의 결정은 심의위원회 명의로 외부에 표시되고 당사자에 대한 의견진술의 기회가 부여되므로 객관적으로 이를 처분으로 인식할 정도의 외형을 갖추고 있는 점, 심의결과인 결정에 이은 제재조치처분의 요청에 기하여 방송통신위원회는 실질적 심사 없이 제재조치의 처분을 명령하여야 하고 이에 따라 당해 표현물에 관하여 「방송법」 또는 정보보호법 소정의 각종 의무가 발생하는 점, 심의위원회는 제재조치에 관한 의결을 취소함으로써 위 의무를 소멸시킬 수 있는 권한도 보유하고 있는 점 등 관련 법령의 내용과 취지에 비추어 볼 때 심의위원회의 제재조치결정은 항고소송의 대상이 되는 행정처분에 해당한다고 봄이 상당하다. 이처럼 처분성의 인정은 방송통신심의가 "명령·규칙 또는 처분이 헌법이나 법률에 위반되는 여부가 재판의 전제가 된 경우에는 대법원은 이를 최종적으로 심사할 권한을 가진다."라고 규정하고 있는 우리 헌법 제107조제2항 소정의 처분에 해당하는 까닭에, 방송통신심의가 헌법이나 법률에 위반되는 여부가 재판의 전제가 된 경우에는 대법원은 이를 최종적으로 심사할 권한을 가지며 그 제1심 관할법원은 「행정소송법」 제9조제1항 본문에 따라 피고인 심의위원회의 소재지를 관할하는 서울행정법원이 될 것이다.

그런데 심의위원회의 법적 성질에 대하여 방송통신위원회법 의안원문에서는 '방송·통신의 내용심의 기능은 위원회로부터 분리하여 민간 독립기구로 설치할 필요성이 제기됨'이라고 하여 민간 독립기구로 적시되어 있었으나, 다음과 같은 논거에서 심의위원회를 민간조직으로 보기 어렵다고 할 수 있다.

첫째, 방송통신위원회법 제18조가 제1항에서 심의위원회는 '방송 내용의 공공성

확정하는 효과를 지니므로 행정청 자신도 직권으로 자유로이 당해 행정행위를 취소·변경·철회할 수 없는 실질적 존속력으로서 불가변력(不可變力)을 발생하며, 행정심판의 재결과 같은 것이 이에 속한다. 그렇다면 방송통신심의위원회의 심의결과로서 의결은 제재조치에 관한 일정한 판단이고 이해관계인이 참가하여 이해관계를 판단하는 까닭에 실질적으로 쟁송의 결정·재결과 유사하며, 법적 발견을 토론하는 과정으로서 심리를 전제로 하는 논쟁에 대한 결정으로서 표현에 대한 형식적 사건에 대하여는 관여치 않는 표현물에의 내용심사과정인 까닭에 준법률행위적 행정행위로서 확인에 해당한다고 보아야 할 것이다; *Vgl*. Hans D. Jarass, *Die Freiheit der Massenmedien; Zur staatlichen Einwirkung auf Presse, Rundfunk, Film und andere Medien*, Baden-Baden: Nomos Verlagsgesellschaft, 1978, S.161.

및 공정성을 보장하고 정보통신에서의 건전한 문화를 창달하며 정보통신의 올바른 이용환경 조성을 위하여 독립적으로 사무를 수행'함을 알 수 있는바, 여기서의 '독립'은 합의제행정기관과 같이 행정기관 상호간의 대등하지 않은 관계에서 의사결정 과정은 물론 지휘감독권도 행사할 수 없지만 인사권은 지니는 소할(所轄)이라고 볼 수는 없다. 같은 조 제3항에 명시된 바와 같이 9인의 심의위원은 대통령이 위촉하는 바, 인사권이 방송통신위원회에 존재하지 않기 때문에 그렇게 볼 수 없다고 하겠다.[39] 그럼에도 불구하고 「변호사법」 제2조에 규정된 바(변호사는 공공성을 지닌 법률전문직으로서 독립하여 자유롭게 그 직무를 수행한다)와 같이 직무상 외부로부터의 어떠한 지시나 간섭도 배제한다는 취지만으로 해석하기에는 무리가 있다. 합의체의 조직을 구성하고 있기 때문에 그러하다. 그렇다고 하여 별도의 민간기구인 주식회사 자체 내부조직으로서 「상법」 제393조의2에 규정된 위원회와는 전적으로 다르다고 할 수 있다. 판단컨대, 여기서의 독립은 국가와 자치단체 사이에 권력이 분배되어 자치단체가 그들 고유의 필요사항에 관하여 자유로운 행정권한을 보유하는 자치분권(décentralisation)의 개념으로 해석해야 할 것으로 본다.

둘째, 방송통신위원회법 제18조제7항에서는 "(방송통신)심의위원회의 구성과 운영에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다."라고 규정하고 있는바, 방송통신위원회법 시행령 제7조제3항의 경우 "이 영에서 규정한 것 외에 심의위원회의 구성 및 운영 등에 필요한 사항은 심의위원회 규칙으로 정한다"라고 하고 있어 일견 행정위원회의 준입법적 기능과 유사한 태양을 보이고 있다.[40] 이에 따

39) 구 방송위원회와 마찬가지로 독립행정위원회의 법적 지위를 가지는 국가인권위원회의 경우 「국가인권위원회법」 제5조제2항에 따라 위원은 인권문제에 관하여 전문적인 지식과 경험이 있고 인권의 보장과 향상을 위한 업무를 공정하고 독립적으로 수행할 수 있다고 인정되는 자중에서 국회가 선출하는 4인, 대통령이 지명하는 4인, 대법원장이 지명하는 3인을 대통령이 임명하는바, 독립행정위원회의 구성에 3부가 관여하여 민주적 정당성을 관철하고 있는 것이다. 심의위원회의 경우는 이와 유사하다. 그럼에도 불구하고 국가인권위원회 위원장과 상임위원은 정무직 공무원으로 보하는바, 국가행정기관의 여부에 있어서는 구별되어질 수밖에 없는 것이라 하겠다.

40) 「행정기관의 조직과 정원에 관한 통칙」 제21조 (합의제행정기관의 설치) 정부조직법 제5조의 규정에 의하여 행정기관에 그 소관사무의 일부를 독립하여 수행할 필요가 있을 때에는 법률이 정하는 바에 의하여 행정기능과 아울러 규칙을 제정할 수 있는 준입법적 기능 및 이의의 결정 등 재결을 행할 수 있는 준사법적 기능을 가지는 행정위원회 등 합의제행정기관을 둘 수 있다.

른다면 심의위원회는 행정위원회로서 「정부조직법」 제5조에 따른 합의제행정기관이라 할 수 있다. 그렇지만 위 규칙의 제정주체인 심의위원회를 공공단체로 볼 경우에도 행정청으로서 행정입법의 주관조직이 될 수 있다는 점은 다르지 않다.

셋째, 방송통신위원회법 제4조는 방송통신위원회를 5인의 상임위원으로 구성하도록 규정되어 있는바, 위원은 정무직 공무원으로 보하며 「정부조직법」 제10조에도 불구하고 정부위원이 된다. 이와는 달리 심의위원회의 경우 심의위원은 「국가공무원법」 제2조제1항 소정의 공무원은 아니지만, 방송통신위원회법 제20조에 따라 직무를 수행함에 있어 외부의 부당한 지시나 간섭을 받지 아니하고 그 신분보장에 관하여는 방송통신위원회법 제8조제1항이 준용되며, 방송통신위원회법 제27조에 따라 청렴 및 비밀유지의무준수가 요청된다는 점 등을 이유로 순수한 민간인의 신분으로 볼 수 없다고 하겠다. 즉, 국가 또는 공공단체의 공무를 담당하는 일체의 자로서 헌법 제7조제1항(공무원은 국민전체에 대한 봉사자이며, 국민에 대하여 책임을 진다) 소정의 광의의 공무원 의미로 새겨야 할 것이다. 이렇게 본다면 행정기관에는 그 업무의 성질과 양에 따라 적정한 종류와 규모의 공무원의 정원을 배정하여야 하므로[41] 심의위원회의 경우 합의제행정기관 및 더 나아가 독립행정위원회 등과 같은 행정기관으로 볼 개연성은 거의 없겠다. 그럼에도 불구하고 심의위원은 공직자로서 광의의 공무원에 해당한다.

넷째, 심의위원회의 소관직무와 관련하여 볼 때 방송통신위원회법 제21조 각 호에 규정된 것은 방송 및 정보통신 관련 심의가 주축인바, 특히 그 가운데 방송통신위원회법 제25조에 규정된 제재조치를 정하는 것은 공적 소임에서 중요한 부분이라 할 것이며 여기서 제재조치를 정하려는 때에는 미리 당사자 또는 그 대리인에게 의견을 진술할 기회를 주도록 되어 있어 행정절차와 연계되어 있음에 유념할 필요가 있다.[42] 다만, 심의위원회가 제재조치를 정한 때에는 방송통신위원회에

41) 「행정기관의 조직과 정원에 관한 통칙」 제5조제2항 참조.

42) 방송통신위원회법 제25조 (제재조치 등) ① 심의위원회는 방송 또는 정보통신의 내용이 제24조의 심의규정에 위반된다고 판단하는 경우에는 다음 각 호의 어느 하나의 제재조치 등을 정할 수 있다.
1. 「방송법」 제100조제1항에 따른 제재조치·권고 또는 의견제시

지체 없이 제재조치의 처분을 요청하여야 하고 방송통신위원회는 심의위원회로부터 제재조치처분의 요청을 받은 때는 해당 사업자 등에 대하여 그 제재조치의 처분을 명령하여야 한다. 이렇게 보면 심의위원회의 사전적인 의사결정에 기속되어 방송통신위원회의 처분이 행사된다. 물론 이와 관련해 심의위원회의 행정기관성을 인정하지 않는다 하더라도 제재조치에 대한 판단을 확인으로 이해하는 데 현행법상 장애는 없다.

다섯째, 방송통신위원회법 제28조는 "국가는 다음 각 호의 기금 또는 국고에서 심의위원회의 운영 등에 필요한 경비를 지급할 수 있다"라고 규정하고 있기 때문에, 정부의 일반회계로 운영되지 않는 심의위원회를 행정기관으로 보기 어렵다. 오히려「보조금의 예산 및 관리에 관한 법률」제2조제1호에서 규정하고 있는 바와 같이 "보조금이라 함은 국가외의 자가 행하는 사무 또는 사업에 대하여 국가가 이를 조성하거나 재정상의 원조를 하기 위하여 교부하는 보조금·부담금 기타 상당한 반대급부를 받지 아니하고 교부하는 급부금으로서 대통령령으로 정하는 것을 말한다"라는 문언의 해석상 위 경비는 법인격을 보유하고 있진 않지만 비법인 공공단체로서의 심의위원회에 대하여 지원되는 보조금으로 볼 수 있다. 이러한 정부의 각종 지원 때문에 사업계획서나 예·결산 내역을 주무부장관에게 보고하게 되는 것이다.

여섯째, 방송통신위원회법 제26조의 경우 심의위원회의 사무를 처리하기 위하

2.「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제44조의7에 따른 불법정보 유통에 대한 취급의 거부·정지 또는 제한

② 심의위원회는 제1항의 제재조치를 정하려는 때에는 미리 당사자 또는 그 대리인에게 의견을 진술할 기회를 주어야 한다.

③ 심의위원회는 제1항의 제재조치를 정한 때에는 위원회에 지체 없이 제재조치의 처분을 할 것을 요청하여야 한다.

④ 심의위원장은 제21조제1호 내지 제4호에 따른 직무를 수행하기 위하여 필요한 경우에는 방송사업자 또는「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」제2조제1항제3호의 정보통신서비스제공자에게 관련 자료의 제출을 요구할 수 있다.

⑤ 위원회는 제3항에 따라 심의위원회로부터 제재조치의 처분을 요청받은 때에는「방송법」또는「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」이 정하는 바에 따라 해당 사업자 등에 대하여 그 제재조치의 처분을 명령하여야 한다.

여 사무처를 두도록 하면서 사무처의 운영과 보수 등에 관하여 필요한 사항을 규칙으로 정하게 규정하고 있는데 사법인의 경우 이에 관하여 정관에 따르도록 하면 될 것인데 외부적 효력을 갖는 심의규정과 동일한 지위의 규칙에 이를 포섭토록 하는 것은 그 법적 성질이 공적 성격, 즉 공익성과 공공성을 내포하고 있음을 반증해준다. 뿐만 아니라 심의위원, 사무총장, 그 밖의 사무처 직원은 「형법」 또는 다른 법률에 따른 벌칙 적용에 있어서는 각각 공무원으로 보도록 의제한 규정의 경우 공무원에 준하는 책임을 부여함으로써 공법상의 특별한 법률관계를 예정해 놓고 있는 것인데, 사인들이 자유로운 의사에 기초하여 법인을 설립하기 위하여 스스로 정관을 만들고 기관을 구성한 후 정부로부터 허가를 받아 행정과정의 일부로서 이루어지는 일반법인과는 다른 지위의 형태임을 여실히 보여주고 있다 할 것이다.

일곱째, 심의위원회는 방송통신위원회법 제24조에 따라 심의규정을 제정・공표하며, 방송통신위원회법 제29조에 따라 심의위원회 규칙을 제정・개정・폐지하려는 때에는 20일 이상의 예고와 심의위원회의 의결을 거쳐야 하며 이를 관보에 게재・공표하여야 한다. 현재 「심의위원회 기본규칙」을 필두로 심의위원회규칙 제19호로 제정된 「방송심의에 관한 규정」과 심의위원회규칙 제20호로 제정된 「방송광고심의에 관한 규정」 등이 심의위원회 규칙으로 존재하는바, 특히 심의규정은 심의위원회 규칙 가운데 대외적 구속력과 관련성이 크므로 그 예・공고는 「행정절차법」 제41조 내지 제45조의 적용을 받는다.[43] 여하튼 심의위원회 규칙에 대한 관보에의 게재・공표는 국가가 일반 국민에게 주지시킬 사항을 편찬하여 발행하는 공보기관지에 수록토록 하는 것이기에 민간조직과의 결부성 수용은 용이하지 않다.

---

43) 「행정절차법」은 「행정소송법」 및 「행정심판법」 각 제2조제2항과 마찬가지로 제2조제1호에서 행정청의 개념을 '행정에 관한 의사를 결정하여 표시하는 국가 또는 지방자치단체의 기관 기타 법령 또는 자치법규(이하 '법령 등'이라 한다)에 의하여 행정권한을 가지고 있거나 위임 또는 위탁받은 공공단체나 그 기관 또는 사인'으로 정의하고 있기 때문에, 위 심의규정의 경우 법 제29조에도 불구하고 「행정절차법」 제41조 내지 제45조의 적용을 받게 된다. 「행정절차법」에는 법 제29조제2항에서 규정하지 않은 인터넷·신문·방송 등의 공고 및 공청회를 통한 의견수렴 등이 규정되어 있다.

살피건대, 국가와 사업자 이외의 제3자로서 비법인단체인 심의위원회가 내용규제로서의 심의를 하는 것으로 보면, 내용규제에 있어 작동하는 제재적 구조[44]는 민간단체의 심사에 따라 결정지어져 행정권에 의해 수행되는 양태를 취하게 된다. 해당 사업자가 속한 단체나 협회에서 자율적으로 제재하는 것이 아니라 국가행정권이 발동을 전제로 하여 그 부적법성의 판단을 중립적인 제3자가 담당하는 것으로 볼 수 있겠는데, 결국 심사의 기준이 되는 심의규정이 어떠한 법적 성질을 지니고 있는가가 관건이 될 것이다. 심사척도 자체가 자율적인 의견수렴에 의한 것인지 아니면 제재적 구조와 연계된 국가행정권의 범주 내의 것인지를 분별하여야만 방송통신심의가 갖는 성질을 제대로 파악할 수 있다.

정리하자면, 심의위원회가 민간조직이라면 비법인단체에 해당하며 여기서의 심의는 행정적 제재 여부를 결정하는 중립적 준법률행위로서 민간단체의 자율적인 판단이라 하겠다. 다만, 이를 사업자(단체)의 자정적 규제활동을 총칭하는 자율규제라 보기는 어려울 것이다. 그럼에도 현행법제상 심의위원회를 일반법인으로 볼 수 없음은 상술한 바와 같다. 물론 공무원으로 구성되지 아니한 심의위원회를 국가행정기관이라 할 수는 없을 것이나, 이는 구 방송위원회가 독립행정위원회가 되고 그 사무처 소속 직원이 공무원이 아니었던 점과는 다르다.[45] 즉, 방송통신심의위원이 공무원 신분이 된다면 구 방송위원회의 조직과 유사한 지위에서 이를 국가행정기관으로 파악할 수 있겠으나, 심의위원회는 심의위원의 위촉과정에서 행정부와 입법부의 관여를 받을 뿐 그 신분이 민간인이라는 점에서 차이가 있으므로 비법인공공단체라 여겨야 할 것으로 본다.

그렇다면 비법인공공단체로서 심의위원회는 특히 내용규제로 방송통신위원회

---

44) 방송통신위원회법 제25조에 따르면 심의위원회가 방송 또는 정보통신의 내용이 심의규정에 위반된다고 판단하는 경우에는 제재조치·권고·의견제시 또는 불법정보 유통에 대한 취급의 거부·정지·제한 가운데 어느 하나의 제재조치 등을 정할 수 있고, 이 경우 미리 당사자 또는 그 대리인에게 의견을 진술할 기회를 주어야 하며, 심의위원회는 제재조치를 정한 때에는 방송통신위원회에 지체 없이 제재조치의 처분을 할 것을 요청하여야 하며 제재조치의 처분을 요청받은 방송통신위원회는 해당 사업자 등에 대하여 그 제재조치의 처분을 명령하여야 한다.

45) 이에 관한 상세는 拙稿, 같은 글(註37), 491~498쪽 참조.

가 행하는 제재처분의 전단계인 심리·의결을 담당하는바, 그 준거규범은 심의위원회의 내부규정이 아니라 대외적 효력을 발휘하는 법규명령이라 할 것이고 이를 적용한 방송통신심의는 법률관계의 변동을 가져와 권리를 제한하거나 의무를 부과하는 처분이라 할 것이다.[46]

판단컨대, 방송통신심의의 경우 제재조치의 처분을 방송통신위원회가 직접 조치하지만, 그 제재 여부에 대한 판단을 심의위원회가 심의규정에 따라 행하므로 권리제한·의무부과의 법률관계 변동에 작용하는 심의 역시 처분성을 지닌다고 봄이 타당할 것이다. 여기서 방송통신위원회의 제재처분에 대한 사전판단인 방송통신심의의 잣대로서의 심의규정은 방송통신위원회법 시행규칙의 지위를 갖는다는 해석이 체계정합성에 맞을 수 있을 것이다.

요컨대, 심의위원회를 방송위원회와 같이 국가행정기관으로 볼 수도 없을 뿐만 아니라, 방송통신심의에 따른 권리의무관계가 귀속하는 행정주체는 국가가 아닌 심의위원회라는 비법인공공단체 자신이다. 이는 심의위원회에서 행하는 방송통신심의가 방송통신위원회법에 따라 국가가 사무적으로 분권하고 위탁한 사무인 까닭에 그러하며, 이에 대하여는 국가가 일정한 감독권을 행사하기 마련이다. 다만, 준사법적 판단작용으로서 준법률행위적 행정행위인 확인에 해당하는 방송통신심의에 국가행정기관인 방송통신위원회의 제재조치의 처분이 기속되어 있으므로 그 판단활동의 중립성이 관철될 수 있도록 제도적 보완이 요청되며, 그 방향성은 국가의 후견적 감독이 심의위원회의 독립성 및 자율적 운영 보장을 위하여 일정하게 제약되어야 한다는 점에 놓일 것이다.

무엇보다 방송통신심의는 행정처분으로서 정보의 유통과 표현의 자유에 관한

46) 물론 이와 같이 국민의 구체적인 권리·의무를 발생·변경·소멸시키는 직접적인 법적 효력을 갖는 규율에 한정하지 아니하고 행정의 적법성 통제대상이 되는, 그 위법성을 확인할 수 있는 행위라 한다면 처분으로 봄이 옳겠다. 여하튼 프랑스, 영국, 미국 및 유럽공동체에서 행정소송의 대상이 되기 위한 핵심적 징표가 '결정(décision)'이며 이는 바로 우리 법상의 '법집행'에 상응하는 것이라 할 수 있는바, 방송통신심의의 심리·의결이 갖는 법집행성에는 영향을 주지 아니할 것이다. 이에 대한 상세는 박정훈, 행정법의 구조와 기능, 박영사, 2006, 174~177쪽 참조.

내용규제적 제한으로 이루어지는 것이므로 그 중립적 판단의 공정성 담보를 위하여 다수(多數)에 의한 의사결정기구로서의 위원회조직을 채택하게 된 귀결이 심의위원회이며, 이렇듯 그 작용법적 논의와 조직법적 논의가 연계되어 있는 구도에 방송통신심의가 놓여 있는 것이다. 따라서 판단이라는 정신작용을 필요로 하는 확인으로서 방송통신심의는 구체적 처분의 형식으로 행하여지는데, 이것이 바로 심리와 의결이 복합된 행정행위로서의 심의가 되는 것이고 의사결정기구로서 합의체의 위원회조직을 갖춘 비법인공공단체로서 그 자신이 행정주체이자 외부적 의사표현에 있어서 행정청으로 작동하여 방송통신심의의 결과로 방송통신위원회라는 국가행정기관의 처분을 이끌어내는 구조라 하겠다. 이렇게 방송통신과 관련된 내용규제적인 제한에 있어 심의위원회가 방송통신심의를 행하고 이어서 방송통신위원회에서 제재조치를 하도록 하는 이원적 구조를 채택한 것은 방송통신심의의 중립성과 공정성이 독립적 위상에서 발현되도록 한 것인데, 선행처분인 방송통신심의와는 별개인 후행처분으로서 제재조치가 독립하여 별개의 효과를 목적으로 하는 것이 아님에도 불구하고 제재조치의 성격상 이는 국가행정기관에서 담당하는 것이 타당하고 이 같은 국가사무 이전에 중립적인 판단이 이루어지면 방송통신심의의 부적법성을 밝혀 권리구제의 실효성을 확보하려는 데 연유한다.

여기서 방송통신심의라는 선행처분과 후행처분으로서 제재조치가 연속적으로 행해지는 경우 선행처분과 후행처분이 서로 결합하여 하나의 법률효과를 완성하므로 만일 선행처분인 방송통신심의에 하자가 있으면 그 하자는 후행처분에 승계되므로 선행처분에 불가쟁력이 생겨 그 효력을 다툴 수 없게 된 경우에도 선행처분의 하자를 이유로 후행처분의 효력을 다툴 수 있는 까닭에, 청구기간 또는 제소기간의 경과로 하자 있는 방송통신심의의 효력을 다툴 수 없게 된 때[47]에는 그 내용에 기속되는 제재조치에 위 하자가 승계되므로 방송통신심의의 하자를 이유로

47) 행정심판 청구는 처분이 있음을 안 날부터 90일 이내에 제기하여야 하며, 정당한 사유가 없는 한 처분이 있은 날로부터 180일을 경과하면 제기하지 못한다. 또한 취소소송의 경우 처분이 있음을 안 날부터 90일 이내에 제기해야 하며, 정당한 사유가 없는 한 처분 등이 있은 날부터 1년을 경과하면 이를 제기하지 못한다.

제재조치에 대한 쟁송취소를 구할 수 있다. 이처럼 헌법상 금지되는 검열이 아닌 내용규제에 있어서 효과적 권리구제가 제도화되어 있는 형국은 긍정적이지만, 근래 논란이 된 사례에서 되짚을 수 있듯 방송통신심의의 중립성을 저해할 수 있는 행정권 수행은 방송통신위원회법 제18조제3항에 따라 심의위원을 대통령이 위촉하되, 3인은 국회의장이 국회 각 교섭단체 대표의원과 협의하여 추천한 자를 위촉하고, 3인은 국회의 소관 상임위원회에서 추천한 자를 위촉함으로써 정치적 대립구도 속에 방송통신심의가 수행되는 것과 무관하지 않다. 다만, 방송통신심의제도의 중립적 운영을 위한 심의위원 구성이 정치적 영향력으로 말미암아 '방송의 공공성' 및 '표현의 자유' 침해 문제를 증폭시키고 그 공정성 확보에 걸림돌이 될 수 있음을 주목하여야 한다.

Ⅳ. 개인정보에 관한 권리충돌의 문제

1. 논의의 전제

무릇 프라이버시의 권리(right to privacy)와 표현의 자유(freedom of expression)는 국민의 기본권 보장과 실현에 그 목표를 두는 근대 입헌주의헌법에서부터 핵심적이고 근본적인 권리로 인정되어 왔다. 하지만 이들 권리는 서로 충돌되는 때가 많다. 즉, 정보매체를 통하여 이루어지는 표현의 자유는 이러한 표현에서 논의되는 사안과 관련된 인물의 프라이버시를 종종 침해하기도 하는 한편, 프라이버시[48] 보호의 확장은 표현의 자유 보장을 위축하는 결과를 초래하기도 한다.[49] 환언하

48) 프라이버시의 어원(語原)은 '사람의 눈을 피한다'는 의미의 라틴어인 *privatue*에서 유래한다. 다만 프라이버시의 개념은 '타인의 방해를 받지 않고 개인의 사적 영역(personal space)을 유지하고자 하는 이익 또는 권리'를 통칭하는 다차원적 개념으로서, 미국에서도 그 다의성으로 인해 많은 그 개념정의에 통일적인 합의를 이루지 못한 것으로 알려져 있다; Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca: Cornell University Press, 1992, p.25.

49) *See* Richard Clayton & Hugh Tomlinson, *Privacy and Freedom of Expression*, New York: Oxford University Press Inc., 2001, p.ⅳ.

자면 프라이버시의 권리와 표현의 자유가 개인의 존엄성을 실현하고 진리탐구와 정부통제를 가능하게 한다는 점에서 자유민주주의사회에서 불가결한 요소라고 할 것이지만 이 두 가치는 본질적으로 긴장관계에 놓여있기에 그 조율이 중요하며, 미국의 관련 판례 역시 이들의 상호충돌에 관한 조화를 추구해왔다고 할 것이다.

주지하다시피, 지난 1948년 12월 제3차 국제연합총회에서 채택된 세계인권선언(Universal Declaration of Human Rights)은 제12조에서 사생활의 비밀과 보호를, 제19조에서는 의견과 표현의 자유를 천명하고 있는바, 전자(前者)가 곧 '홀로 있을 권리(right to be let alone)'로 대별되는 프라이버시에 관한 권리이고 후자(後者)는 '알 권리(right to know)'를 중핵으로 하는 언론·출판의 자유에 관한 것이며 그 내포된 가치가 상호 배치되는 까닭에 그 조율이 관건이 된다고 하겠다. 한편으로 이러한 프라이버시와 개인정보보호(personal information protection)라는 언명으로 일컬어지는 개인정보에 관한 정보주체의 권리는 본질적으로 상이한 측면을 취하는바, 이를 대별하는 관점에서 언론의 자유와의 긴장관계를 천착하는 것이 요구된다.

또한 프라이버시는 인격의 자유로운 발전과 인간의 존엄성을 유지하게 하며 개인주의와 자유주의를 존립하게 하지만, 진실의 자유로운 공개가 사회의 보호와 육성을 위하여 필요하고 때로는 이러한 개인의 권리는 공익에 양보되어야 할 경우가 존재한다.[50] 이는 언론의 자유와 국민의 알 권리[51]가 어떤 사실을 백일하에 공표함으로써 국민을 보호한다는 데 기초하며,[52] 프라이버시의 권리는 이러한 사회

50) 프라이버시의 권리는 그 본질에 있어 반사회적(anti-social)이며 공중의 주시와 호기심으로부터 도피하려는 인간의 본성을 전제로 하지만, 언론보도의 자유와 필연적인 대립관계에 놓여있다는 데 문제가 있다; Louis Nizer, *The Right of Privacy: A Half Century's Developments*, 39 Michigan Law Review 526, 528-529 (1941).

51) '정보의 자유(*Informationsfreiheit*)'와 동일한 의미로 이해되어지는 알 권리는 특히 그 내용으로서 정보수집자유의 경우 국민이 일반적으로 접근할 수 있는 정보원으로부터 방해받지 않고 정보를 수령할 권리의 단계를 넘어 적극적으로 정보를 수집하는 자유를 보장하는 단계에 이른 것이다. 미국에서 '알 권리'라는 용어는 제2차 세계대전 이후 냉전체제의 구축과정에서 정부의 비밀주의 경향에 대항하는 언론운동에서 주창되었는바, 정보를 입수할 권리, 사전억제 없이 인쇄할 권리, 적법절차에 따르지 않는 보복의 금지와 두려움 없이 인쇄할 권리, 커뮤니케이션에 필수적인 시설과 자료에 접근할 권리, 위헌적으로 법을 악용한 정부의 간섭은 물론이고 법을 무시하는 시민의 방해마저도 받지 않고 정보를 확산할 권리 등이 그 핵심으로 거론된다; *See* James R. Wiggins, *Freedom or Secrecy*, New York, NY: Oxford University Press, 1956, pp.3~4.

52) Emerson은 표현의 자유가 지니는 가치와 기능에 대하여, "표현의 자유는 개인의 자아실현을 촉진시키고, 지식의 성장과 진리발견을 위한 필수적 도구이며, 개인으로 하여금 민주적 결정과정에 참여할 수 있게 할 뿐만

적 권익과 상충하는 이념의 소산이기에 이들 이념이 지닌 비중에 대한 점진적 조절에 의하여 가치의 균형이 이루어질 수 있다.[53]

2. 법제적 분석

우리 헌법재판소는 "부동산 소유권의 회복을 위한 입증자료로 사용하고자 청구인이 문서의 열람·복사 신청을 하였으나 행정청이 이에 불응하였다고 하더라도 그 불응한 행위로 인하여 청구인의 재산권이 침해당하였다고는 보기 어려우나, 청구인의 정당한 이해관계가 있는 정부 보유의 정보의 개시에 대하여 행정청이 아무런 검토 없이 불응한 부작위는 헌법 제21조에 규정된 표현의 자유와 자유민주주의적 기본질서를 천명하고 있는 헌법 전문, 제1조, 제4조의 해석상 국민의 정부에 대한 일반적 정보공개를 구할 권리(청구권적 기본권)로서 인정되는 '알 권리'를 침해한 것이고 위 열람·복사 민원의 처리는 법률의 제정이 없더라도 불가능한 것이 아니다."라는 입장을 확고히 한 바 있으며,[54] 이로써 알 권리 또는 정보공

아니라, 보다 안정적이고 융통성 있는 공동체를 달성하기 위한 방편, 즉 사회의 안전밸브(safety valve)를 제공한다'"고 정리한 바 있다: Thomas I. Emerson, *Toward a General Theory of the First Amendment*, New York: Random House, 1963, pp.4~15.

한편, 사회의 안전밸브기능과 관련하여 연방대법원의 Brandeis대법관은 "처벌에 대한 위협은 탄압을 낳고, 탄압은 증오를 낳고, 증오는 정부의 안전을 위협한다."고 하면서 표현의 규제보다는 표현의 자유를 사회의 안전밸브(safety valve)로서 강조하였는데, 그 근거는 침묵의 강제와 표현의 억압은 순교자들을 양산할 뿐이고, 불만이 체제 내에서 수용되지 못할 경우에는 근본적인 체제의 변혁을 요구하는 세력이 등장한다는 것이었다; Whitney v. California, 274 U.S. 357, 373 (1927).

53) Louis Nizer, *supra note 50*, p.500.

54) 우리나라는 헌법 제21조에 언론·출판의 자유, 즉 표현의 자유를 규정하고 있는데, 이 자유는 전통적으로는 사상 또는 의견의 자유로운 표명(발표의 자유)과 그것을 전파할 자유(전달의 자유)를 의미하는 것으로서, 개인이 인간으로서의 존엄과 가치를 유지하고 행복을 추구하며 국민주권을 실현하는데 필수불가결한 것으로 오늘날 민주국가에서 국민이 갖는 가장 중요한 기본권의 하나로 인식되고 있는 것이다. 그런데 사상 또는 의견의 자유로운 표명은 자유로운 의사의 형성을 전제로 하는데, 자유로운 의사의 형성은 충분한 정보에의 접근이 보장됨으로써 비로소 가능한 것이며, 다른 한편으로 자유로운 표명은 자유로운 수용 또는 접수와 불가분의 관계에 있다고 할 것이다. 그러한 의미에서 정보에의 접근·수집·처리의 자유, 즉 '알 권리'는 표현의 자유에 당연히 포함되는 것으로 보아야 하는 것이다.…(中略)…'알 권리'의 법적 성질을 위와 같이 해석한다고 하더라도 헌법 규정만으로 이를 실현할 수 있는가 구체적인 법률의 제정이 없이는 불가능한 것인가에 대하여서는 다시 견해가 갈릴 수 있지만, 본건 서류에 대한 열람·복사 민원의 처리는 법률의 제정이 없더라도 불가능한 것이 아니라 할 것이고, 또 비록 공문서 공개의 원칙보다는 공문서의 관리·통제에 중점을 두고 만들어진 규정이기는 하지만 「정부공문서 규정」 제36조제2항이 미흡하나마 공문서의 공개를 규정하고 있는 터이

개청구권이 헌법상 모든 국민이 향유하고 국가가 침해하여서는 안 될 기본적 인권으로 인정된다는 점도 「공공기관의 정보공개에 관한 법률(이하 '정보공개법'이라 약칭한다)」 제정 이전에도 헌법해석론적으로 받아들여져 왔다.[55] 그럼에도 불구하고 이러한 권리가 절대적인 성격의 것이 아니라 상호 충돌하는 법익과의 긴장관계 속에서 가치판단에 따라 조율되어야 할 상대적인 권리라는 관점에 시선을 두고 어떻게 정보공개원칙을 구현할 것인가에 관한 해법을 논의해야 한다. 이처럼 정보공개원칙에 배치되는 예외적 면제사유가 법률상 보호이익으로 명시되어 있는 바, 이른바 '비공개대상정보'의 의미와 범위에 대한 해석적 탐색은 정보공개원칙을 명문화하고 있는 정보공개법의 입법취지를 훼손하지 않으면서 상충이익의 균형과 조화를 모색하는 시각에서 접근되어 '비공개대상정보'의 비공개 필요성을 확인할 수 있는 적정규준 정립으로 이어져야 할 것이다.

왜냐하면 정보공개제도의 본질적인 의욕과 그 본연적인 입법목적에도 불구하고 정보보유기관의 재량적 판단에 따라 공개 여부가 결정되는 구조적 모순이 내포되어 있다는 점에서 비공개대상정보는 아킬레스건(Achilles' tendon)의 은유(metaphor)로 여겨질 수 있기 때문이다. 이는 정보공개법 제3조가 '정보공개의 원칙'이라는 조문명 아래 "공공기관이 보유·관리하는 정보는 이 법이 정하는 바에 따라 공개하여야 한다."라고 선언적으로나마 규정하고 있는바, 비공개대상정보라는 예외적 설

므로 이 규정을 근거로 해서 국민의 '알 권리'를 곧바로 실현시키는 것이 가능하다고 보아야 할 것이다. 이러한 관점에서 청구인의 자기에게 정당한 이해관계가 있는 정부 보유 정보의 개시 요구에 대하여 행정청이 아무런 검토 없이 불응하였다면 이는 청구인이 갖는 헌법 제21조에 규정된 언론 출판의 자유 또는 표현의 자유의 한 내용인 '알 권리'를 침해한 것이라 할 수 있으며, 그 이외에도 자유민주주의 국가에서 국민주권을 실현하는 핵심이 되는 기본권이라는 점에서 국민주권주의(제1조), 각 개인의 지식의 연마, 인격의 도야에는 가급적 많은 정보에 접할 수 있어야 한다는 의미에서 인간으로서의 존엄과 가치(제10조) 및 인간다운 생활을 할 권리(제34조 제1항)와 관련이 있다 할 것이다; 헌법재판소 1989. 9. 4, 88헌마22, 판례집 1, 176, 188-190.

55) 지난 1991년 법률의 위임 없이 청주시의회 30인의 의원 발의로 마련된 「청주시 행정정보 공개조례」로부터 출발한 우리나라의 정보공개법제는 비록 국민의 권리의무관계에 변동을 주고 재판규범으로서 국가기관을 구속하는 법규(*Rechtssatz*)로서의 성질을 지니지는 못하지만 중앙정부 차원의 내부규범으로 기능하는 「행정정보공개운영지침」을 마련함으로써 제도적 시행을 맞이하게 되었는바, 그 입법적 결실은 이후 3년여의 논의과정을 거친 연후에 공공기관이 보유·관리하는 정보에 대한 국민의 공개청구 및 공공기관의 공개의무에 관하여 필요한 사항을 정함으로써 국민의 알 권리를 보장하고 국정에 대한 국민의 참여와 국정운영의 투명성을 확보함을 목적으로 하는 정보공개법이 1996년 12월 31일 법률 제5242호로 제정되어 1998년 1월 1일부터 시행되고 있다.

정을 구비하고 그 해당 여부에 따른 정보공개 여부를 정보공개법 제11조제1항에 의거 해당 국가기관 등이 결정함으로써 '정보공개의 원칙'으로 상징되는 정보공개법의 입법취지가 잠식된다고 환언할 수 있다는 점에 기인한다.

원론적으로 국가가 보유하는 행정정보를 국민에게 공개하는 행정정보공개제도는 무엇보다 행정정보의 공개를 원칙으로 의무 지워 국민에게 행정정보공개청구권을 보장하여야 한다는 것을 의미하지만 개인의 사생활에 관한 정보 등은 예외적으로 비공개이어야 하며, 다만 행정정보공개청구권은 국민의 알 권리의 구체화이므로 행정정보는 원칙적으로 모두 공개한다는 전제에 입각하여 법정예외사유는 그와 같은 예외가 인정되는 본래의 취지에 따라 엄격하게 해석하여야 할 것이다. 이는 곧 개인정보보호와 관련하여 정보공개의 허용범위를 확정하는 문제가 되는 바, 정보공개의 한계 설정기준으로서 보호가치 있는 개인정보의 기능이 발휘된다. 그러므로 두 법익간의 충돌에 대한 관계정립, 즉 법익형량이 요구되므로 입법자가 어떻게 최적화명령을 실현할 것인가를 획정함이 우선과제라 할 것이다.

여기서는 정보공개가치와 정보보호가치의 조율이 법규범적으로 형성되어야 하며, 공개대상이 될 수 없는 개인정보에 대하여는 고유한 권익을 보장하여야 한다. 그러기 위해서는 보다 큰 공익이 인정되어야 하지만 다른 수단으로 공개의 목적을 달성할 수 없는 극히 예외적인 경우에 한정하여 공개가 가능하도록 새겨야 할 것이다. 더욱이 전자정부에서는 정보의 열람 등 정보공개의 편익성이 극대화되므로 그와 필연적 표리관계에 대한 개인정보보호에 대한 숙의와 개인정보보호를 통한 인격의 자유로운 발현가치 및 정보공개를 통한 민주주의 이념의 실현가치의 법익형량의 모색을 거친 후에 도출되는 사회적 합의를 법제화할 필요성이 존재한다.

원래 정보의 자유에 대한 관념은 책임 있는 정부를 만들기 위해 계몽사상에 기인한 혁명철학에서 비롯된 것인바, 일찍이 1766년 헌법에서 정보공개원칙을 언론·출판의 자유 일부로 명시한 이후 1810년에 제정된 「출판자유법(den svenska förordningen om Skiv-och tryckfriheten)」을 기원으로 정부기록에 대한 공개와 문서

의 제공에 대한 시민의 청구권을 인정함으로써 세계 최초의 정보공개법이 스웨덴에서 마련된 것을 그 유래로 한다.[56]

앞의 헌법재판소 결정례는 "정보에의 접근·수집·처리의 자유, 즉 알 권리는 표현의 자유에 당연히 포함되는 것으로 보아야 한다."고 하면서 '정보의 자유'와 동일한 의미로 이해되어지는 알 권리의 내용으로 정보수집의 자유와 관련해서는 국민이 일반적으로 접근할 수 있는 정보원(情報源)으로부터 방해받지 않고 정보를 수령할 권리에 머무르는 것을 넘어 적극적으로 정보를 수집하는 자유를 보장하는 단계에 이른 것으로 새겨야 함을 설시하고 있다. 같은 논리선상에서 지난 2004년 6월 18일 벨기에 브뤼셀에서 열린 「유럽헌법제정조약회담(Conference on Treaty establishing a Constitution for Europe)」은 '정보의 자유(freedom of information)'[57]를 유럽헌법이 보장하는 기본적 인권(fundamental human rights)[58]에 편입시키고 있다.[59]

그렇지만 알 권리의 실현과 행정의 투명성 확보를 위하여 정립되어진 정보공개

---

56) *See generally* Stephen Lamble, *Freedom of Information: A Finnish Clergyman's gift to democracy*, Freedom of Information Review Vol.97, Brisbane: Department of Justice and Attorney-General, Queensland Government, 2002, pp.2~8; Siegfried Lamnek und Marie-Theres Tinnefeld, *Globalisierung und informationelle Rechtskultur in Europa: Informationelle Teilhabe und weltweite Solidarität*, Baden-Baden: Nomos Verlag, 1998, p.118; The Chancellor of the Duchy of Lancaster, *Your Right to Know: The Government's Proposals for a Freedom of Information Act*, London: Her Majesty's Stationery Office, 1997, available at <http://www.archive.official- documents.co.uk/document/caboff/foi/foi.htm>.

57) Treaty establishing a Constitution for Europe §II-71 (Freedom of expression and information)
① Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.
② The freedom and pluralism of the media shall be respected.

58) 국가의 책무이자 국제사회의 주요관심사로서 인권 보장은 시대적·사회적 변화에 따라 다양한 스펙트럼을 보이며 개진되어 온 핵심주제이었던 까닭에 수세기에 걸쳐 기본적 인권 개념이 논의되었다; *See generally* Paul Gordon Lauren, *The Evolution of International Human Rights: Visions seen*, Philadelphia, PA: University of Pennsylvania Press, 2003, pp.4~28.

59) 유럽연합(EU) 및 유럽공동체(EC)·유럽경제공동체(EEC) 아래 체결·비준된 50여 개 이상의 조약과 의정서·부속문서를 하나의 헌법의 형태로 집약해 유럽연합 가맹국의 의사결정을 통일화하려는 유럽헌법제정조약의 발효를 위해서는 모든 가맹국의 비준이 필요하지만, 그 절차는 각 나라에 따라 다르다. 의회 결의만으로 비준하는 국가도 있고 국민투표를 시행하는 나라도 있으며, 국민투표 또한 의회가 이에 대해 다시 비준할 수 있는 나라와 구속력을 갖는 나라로 갈린다. 또한 투표율에 따라 구속력이 생기는 나라도 있다. 2005년 2월의 스페인에서 실시된 국민투표에서는 조약이 가결되었지만, 5월의 프랑스와 6월의 네덜란드에서는 부결되었다; Thérèse Murphy, *New Technologies and Human Rights*, New York, NY: Oxford University Press Inc., 2009, pp.139~140.

의 원칙에도 불구하고 모든 공공정보가 예외 없이 공개될 수만은 없는 노릇이다. 정보공개청구권과 긴장관계로 얽힌 상충가치가 법적 이익으로 존재하기 때문에 이 같은 규범적 갈등을 정보공개청구사안에서 현명하게 저울질할 수 있는 법적 근거 역시 필요하다고 할 것인바, 정보공개법은 비공개대상정보를 명문으로 규정함으로써 예외적 정보공개 면제사유를 포괄적이나마 제시하고 있는 것이다. 그 가운데 개인에 관한 정보가 포함되어 있다.[60]

정보공개법 제3조 및 제5조・제9조제1항에 따르면 모든 국민은 공공기관이 보유·관리하는 정보의 공개를 청구할 권리를 가지고 공공기관이 보유·관리하는 정보는 법이 정하는 바에 따라 공개되어야 함이 원칙이나 다만 예외적으로 정보공개법 제9조제1항 각 호에서 정한 비공개대상정보에 대하여는 이를 공개하지 아니할 수 있는 것이므로 비공개대상정보를 규정하고 있는 정보공개법 제9조제1항 각 호를 확장하여 해석하여서는 안 될 것인 반면, 같은 조항 각 호 단서에서 다시 비공개 대상에서 제외되는 영역의 경우 이를 축소할 경우 알 권리 보장 차원의 관점이 다른 권리와의 상충에서 균형을 잃게 될 우려가 있기 때문이다. 정보공개청구권은 알 권리의 당연한 내용이며, 알 권리는 헌법 제21조 소정 표현의 자유에 당연히 포함되는 개인의 자유권적 기본권에 해당하므로 국민의 알 권리 또는 정보공개청구권이 다른 법익 또는 기본권과 갈등을 빚는 경우에는 헌법의 통일성을 유지하기 위하여 상충가치 모두가 최대한 그 기능과 효력을 발휘할 수 있도록 규범조화

60) 정보공개법 제9조 (비공개대상정보) ① 공공기관이 보유·관리하는 정보는 공개대상이 된다. 다만, 다음 각 호의 1에 해당하는 정보에 대하여는 이를 공개하지 아니할 수 있다.
6. 당해 정보에 포함되어 있는 이름·주민등록번호 등 개인에 관한 사항으로서 공개될 경우 개인의 사생활의 비밀 또는 자유를 침해할 우려가 있다고 인정되는 정보. 다만, 다음에 열거한 개인에 관한 정보는 제외한다.
가. 법령이 정하는 바에 따라 열람할 수 있는 정보
나. 공공기관이 공표를 목적으로 작성하거나 취득한 정보로서 개인의 사생활의 비밀과 자유를 부당하게 침해하지 않는 정보
다. 공공기관이 작성하거나 취득한 정보로서 공개하는 것이 공익 또는 개인의 권리구제를 위하여 필요하다고 인정되는 정보
라. 직무를 수행한 공무원의 성명·직위
마. 공개하는 것이 공익을 위하여 필요한 경우로써 법령에 의하여 국가 또는 지방자치단체가 업무의 일부를 위탁 또는 위촉한 개인의 성명·직업

적 해석방안을 모색하되, 법익형량의 원리 및 입법에 의한 선택적 재량 등을 종합적으로 참작하여 심사하여야 하기 때문이다.[61]

물론 정보공개법의 경우 수집 목적의 범위 내에서 이용하는 것이지만, 그 인정의 판단을 해당 공공기관이 담당할 것이 아니라 「개인정보 보호법(이하 '개인정보법'이라 한다)」 제7조에 따른 개인정보 보호위원회가 심의·의결하도록 정보공개법에서 이를 명시하는 개정이 이루어져야 할 것으로 본다.[62] 현재로서는 개인정보보호와 무관하게 정보공개제도 차원에서 보유기관이 그 인정 여부를 판단하고 분쟁이 발생한 경우에 이르러서야 법원이 종국적으로 그 판단의 적정성 여부를 심사하게 되는 구조인 까닭에 개별적 권리구제로 해소되지만, 개인정보보호의 관점에서 법령 개정이 필요하다고 볼 것이기 때문이다.[63]

원칙적으로 공적 영역에 있어 개인정보의 활용은 공권력에 의한 기본권침해(基本權侵害)의 소지가 있는 것이므로 적절한 통제가 요구되는 것이고 다만 정당한 목적의 공익을 위한 개인정보의 활용이 법률유보원칙에 위배되지 않거나 비례원칙의 위반이 없다면, 혹은 기본권의 본질적 내용을 침해하지 않을 때에 예외적으로 기본권제한(基本權制限)이 된다.[64] 그리고 이를 법률유보의 원칙에 대입하여

---

61) 헌법재판소 2010.12.28. 2009헌바258, 판례집 22-2(하), 721, 730; 2007.10.25. 2005헌바96, 판례집 19-2, 467, 474; 1991. 9.16. 89헌마165 결정, 판례집 3, 518, 528 참조.

62) 개인정보 보호위원회는 개인정보보호 전담기구로서 태생적인 내재적 한계를 떠안고 있다. 그럼에도 불구하고 그 심의기능을 정보공개 여부의 판단과 관련하여 개인정보자기결정권과의 충돌문제에 대하여는 역할론적 재정립이 필요하다고 볼 것이다. 상론은 拙稿, 개인정보보호 전담기구의 법적 쟁점, 월간 법조 통권 제655호, 법조협회, 2011, 76~116쪽 참조.

63) 원칙적으로는 공공기관의 모든 정보는 '관료의 전유물이 아니라 국민의 것'이므로 모든 정보를 적극적으로 공개하여 국민의 알 권리 보장과 행정의 투명성 제고에 대한 사고의 전환이 필요한 것이 사실이지만, 이미 언급한 바와 같이 정보공개법에 의한 비공개대상정보 관련 조항이 지극히 추상적이고 모호하게 규정되어 있어 헌법의 명확성원칙에서 볼 때 문제점이 적지 않고 기본권제한이 불가피하더라도 알 권리 침해는 필요최소한의 원칙(less restrictive alternative principle)에 따라 최소화되어야 한다는 관점에서도 비례원칙을 위협하고 있음에 주목할 필요가 있다.

64) 물론 헌법이 공익이라는 용어를 직접 사용하고 있는 것은 아니지만, 헌법 제37조 제2항 및 제23조 제2항의 '공공복리', 제23조 제3항의 '공공의 필요', 제77조의 '공공의 안녕질서' 등의 개념은 공익 개념 그 자체를 말하고 있다고 보아도 무방할 것이다. 그리고 현행 헌법상 최고이념은 헌법 제10조의 '인간의 존엄과 가치의 실현'이라는 목표에 있다고 판단되므로, 행정은 궁극적으로 이에 봉사하는 것이어야 하며 이를 이루는 과정에서 공익의 구체적 내용이 공간과 시간상 제한된 국가이해를 전제로 영속적으로 구체화될 수 있는 것이다.

행정정보의 공개에 적용한 것이 바로 정보공개법이라는 점은 공공부문에 있어서 개인정보자기결정권 침해라는 공권력에 의한 침익적 행정작용을 통제하기 위해 개인정보보호법리가 관철되어야 하고, 다만 공익적 요청이 있는 경우 정당화사유가 충족되어야만 정보공개법에 따라 제한적으로 개인정보가 공개될 수 있는 구조를 보이고 있다.

한편, 방송통신심의와 관련해서는 정보보호법 제44조의10에서 방송통신심의위원회에 '정보통신망을 통하여 유통되는 정보 중 사생활의 침해 또는 명예훼손 등 타인의 권리를 침해하는 정보'와 관련된 분쟁의 조정업무를 효율적으로 수행하기 위하여 5명 이하의 위원으로 구성된 '명예훼손 분쟁조정부'를 두도록 규정한 것도 표현의 자유로 인한 권리침해의 분쟁해결에서 개인정보자기결정권의 침해가 성립하는 사안에서는 이른바 '대체적 분쟁해결수단(Alternative Dispute Resolutions; ADR)' 중 민법상 화해계약과 동등한 효력을 보유하는 조정(調停; mediation)을 제도적으로 구축한 것이 특이사항으로 꼽혀질 수 있겠으나, 5명의 위원으로 구성된 명예훼손 분쟁조정부에 대하여 1명 이상은 변호사의 자격이 있는 자로 위촉하도록 명시한 규정과 달리 분쟁해결의 전문성을 갖추려면 법조인은 1명으로 족하고 오히려 정보통신분야나 표현의 자유를 위시한 상충가치의 권리에 대하여 이해력을 발휘하는 전문가를 인력풀로 활용하는 방안을 강구할 필요가 있다고 생각한다.[65]

Ⅴ. 결론에 갈음하여

정보매체를 규제할 때 그것이 어떠한 의사전달방식을 사용하는지를 파악하여 내용규제의 기준을 정하며, 형식규제에 있어서는 우선 설비기준에 관한 입법적 사항은 진입규제가 실증적으로 유연화하여야 할 것이고 그밖에 전송역무에 대하여

65) 법원의 판결도 아닌 분쟁의 조정결정을 도출하는 데 있어서 현재 방송통신심의위원회 소속 위원회로 편성된 명예훼손 분쟁조정부는 언론계 1인, 법학교수 1인, 변호사 3인으로 구성되어 있다.

는 공정경쟁이 이루어질 수 있도록 체계화될 수 있을 것이다. 이는 곧 헌법 제21조 제2항 내지 제4항의 적용에 관한 것이며, 이를 구체화하는 최적명령이 요구된다. 특히 이 부분에서 중요한 것은 표현의 자유의 제한법리를 역으로 적용하여 정보매체를 이용하는 정보수용자의 측면에서 얼마나 능동적으로 의사교환에 참여할 수 있는지를 차별적으로 유형화하고 그 내용을 규제함에 있어 상이한 기준을 삼되, 원칙적으로 정보내용을 전송하는 정보매체의 운영에 참가함에 있어서는 등록·신고 등 완화된 진입규제를 유지하고 공정경쟁이 유지될 수 있는 시장체제를 구조화하는 것이 중요하다. 왜냐하면 이제 정보매체의 공익성은 해당역무의 공공성에서 비롯되는 것이 아니라 그 파급효과와 사회적 영향력에 따라 정보내용을 얼마나 규제할 수 있는지 아니면 보호법익이 있는 비밀로서 내용규제에 해당하지 않는지가 결정될 때 이를 세분화하는 기준의 설정이 중요하기 때문이다. 이것이 정보매체의 규제에 있어 관철될 때 우리는 통제력을 확보한 법리를 발견할 수 있을 것이다. 하지만 현행 법제도에서 심의위원회는 비록 쟁송법상의 행정청에 해당하기는 하지만, 국가행정기관은 아니라 할 것이다.

그럼에도 불구하고 정치적 영향력과 후견적 감독에 따른 법리적 통제 외에도 현실적 간여가 가능한 구도 속에서 심의위원회의 판단작용으로 말미암아 생성되는 공법관계의 분쟁을 고려하여 자율규제로의 전환을 모색하려는 논의는 유의미하다. 정보환경의 변모 속에서 관공서의 내용규제를 융합매체를 포함한 정보매체 전반에 대한 규제정합성의 재검토에서 규제조직의 재편성에 이르기까지 다시 살펴볼 필요가 있기에 그러하다.[66]

66) 기술적 변화가 불러온 정보매체의 변모는 매체산업의 능률성과 정보유통의 적정성이라는 공익목적을 위해 포괄적이고 통일적인 규제법리를 요구하고 있다. 정보통신기술의 발달과 서비스의 개발, 규제의 완화 및 경쟁의 활성화 등으로 인하여 별개로 분리된 영역이었던 방송부문과 통신부문이 기술의 발전과 수용의 다양화에 따라 산업적 구조와 제도가 지속적으로 통합되어 가는 현상을 낳고 있기 때문이다. 이에 따라 통신과 방송이 엄격히 분리될 수 있었던 과거의 규제논리를 새로운 서비스에 그대로 적용하는 데에는 문제가 있으므로 통신과 방송을 모두 담당하는 통합된 규제기관을 채택하려는 시도나 규제기관의 기능적 조직을 전환하려는 논의가 이어지고 있다. 표현의 자유는 표현의 내용인 정보에 접근하고 그 활용을 표현의 수단인 매체를 통하여 실현하게 되는바, 전통적으로 통신이란 양방향의 통신망을 구축하여 역무이용자 사이에 양방향적인 송수신이 이루어지는 것을 의미하며 그 내용은 음성역무가 주를 이루어 온 반면 방송이란 전기통신설비를 이용하는 송

그러나 자율규제의 도입에 있어서는 불필요한 법령의 개폐가 필요함을 상기하여야 한다. 인터넷 거버넌스에 있어서 자율규제의 실효성을 담보하기 위해서는 국가의 강제력은 일정 부분 불가피한 것으로 여겨지지만, 순수한 의미에서의 전형적인 자율규제를 담보하기 어렵더라도 국가의 개입은 최소화되어야 하고 강행규범의 남발은 지양되어야할 것이기 때문이다. 그러기에 우선 법령에 근거한 자율규제가 비록 강제적 자율규제(enforced or coerced self-regulation) 혹은 규제된 자율규제(regulated self-regulation)를 구성하더라도 바람직한 방향에서의 인터넷 자율규제는 인터넷서비스와 관련된 모든 영역들의 주체가 참여한 가운데 합의에 의해 형성되는 공동자율규제라 할 것이고, 따라서 협의의 공공단체나 공무수탁사인에 의한 자율규제가 지니는 강제적 속성에 착안하여 행정주체[67]로서 자치분권(*décentralisation*)이나 민간위탁(contracting-out)에 따른 직무의 수행이 아니라 사적 자치(*Privat autonomie*)에 따른 규제와 통제인 자율규제를 지향해야 할 것으로 본다. 자율규제기구의 조직법적 근원에 대한 법적 규율로써 공법상 법인으로 '행정권의 보유자'이자 '행정에 관한 권리·의무의 귀속주체'인 행정주체가 되는 자치단체를 인정한다면 분권화된 국가사무를 필요적 공공사무로 수행하는 것이어서 국가가 아닌 별개의 행정주체가 행하는 작용으로 구별될 뿐 거버넌스에서 긴밀한 협력으로 '상호의존성, 자율성, 파트너십 및 네트워크' 등의 공동분모를 지닌다고 하기 어렵기 때문이다. 그러므로 여기서 중요한 것은 자율규제의 실행의사(implementation intention)와 실천이성(*praktische Vernunft*)이라 할 것인데, 자율규제의 공익적 특성에만 치우쳐 그 근거가 법령에 자리지울 당위성은 존재하지 않는다. 이렇게 볼 때 방송통신심의의 경우 비법인공공단체로 새겨지는 현행 심의위원

신망을 구축하며 이를 통하여 불특정 다수에 대해 음성 및 영상이 포함된 방송프로그램을 단방향으로 전달하는 것을 의미한다고 이해되어 왔다. 따라서 전통적으로 통신은 산업적 측면을 강조해온 반면, 방송은 공익적 측면을 강조해 왔다는 점에서 정책목적상 근본적인 차이점이 존재한다. 그 규제의 방향 역시 상이하여 통신의 경우 경쟁의 활성화와 소비자 편익의 증진 등에 중점을 두는 반면, 방송의 경우 공익성 확보를 위해 상대적으로 엄격한 진입규제, 다양한 편성규제 및 내용규제 등을 특징으로 한다.

67) 행정주체는 행정상 권리·의무관계의 주체가 되는 자를 말하며, 국가·지방자치단체 및 협의의 공공단체와 같이 공법상 법인격을 보유하는 공법인 그리고 공무를 위탁받은 사인인 공무수탁사인으로 분류될 수 있는 개념이다.

회가 분명 거버넌스의 축을 이루고 있지만 자율규제의 확산 측면에서는 민법상 재단법인 또는 비법인단체의 선상에서 조직적 모형이 내용규제의 작용적 역할과 연계해 형성될 수 있는 법제도적 개선을 도모할 현실적 요청이 존재한다는 언급으로써 결론에 갈음할까 한다.

Presentation

The changing information environment and its implications for freedom of expression

LEE, Min-Yeong*

(Professor, Catholic University of Korea)

Ⅰ. Introduction

Our current information environment is calling for a review of the existing relevant law and institutions, in both theoretical and practical terms. Even in the information society mainly characterized by the widespread use of the Internet, just like in the non-cyber real life, a violation of ethical or legal norms would result in a form of social outcry or legal sanction, but the growing demand for legislative adaptations due to the advancement of information technologies and the transformation of the communication systems which are subject to the regulations on people's expressions have attracted more attention to the legal issues involved in the information environment.

Given that, more often than not, online expressions have not only eroded the real-life rights but they have also restricted the rights that should be enjoyed and protected in

* Professor of Legal Faculty at the Catholic University of Korea, myoegi@catholic.ac.kr

the cyber space, the discussions on the rights and interests to be protected online and offline must be made in advance, for the purposes of avoiding the dysfunctions of the information society and facilitating right remedies, being accompanied by specific legislative and policy responses in due process.

In the meantime, the increasing global interdependency in the information society is opening a new phase for the formulation of human rights policies. Now it is more difficult to set up a concrete and effective structure of responses to the stronger human rights advocacy, since the realm of human rights has expanded as the traditional definition of civil and political freedom is replaced by a broader one with additional rights to be guaranteed. Considering that, in contrast to the universality and timelessness of the fundamental ideas on human rights, the policies concerning human rights are of dynamic nature in that they should be counteractive to the transforming social environment and cannot be free from the social and economic changes, the legal regulations governing human rights policies need to be flexible enough.

In the case of Korea, the information human rights has practical implications when we look back on the contributions that the civil society, notably including the civic and social organizations for human rights advocacy, has made to guaranteeing and promoting human rights, while being consistently interested in the issue of human rights in the information society affected by the changes in the information environment and making continuous considerations about ‘information’, ‘information society’ and ‘human rights’. As is confirmed here, the short and simple conjunction ‘and’ has become *de rigueur* for etiquette, decorum or formality to perfect the integrity of academic significance. For instance, the emerging issues of information technologies

and the law and rights, in the similar previous combinations of the regulation and the law and rights, the economy and the law and rights and the culture and the law and rights, are grouped into a more implicational term ‘information human rights’, allowing us to face diverse and multilateral issues involved in the human being and technologies and the law and rights in the information society. Although the Internet is a major medium by which to realize freedom of expression as everyone has access to the chance to express themselves on the Internet and run an Internet-based website while not being controlled or restricted by others, it should not be abused or misused, in that fundamental rights are not absolute ones but rather must be subject to certain restrictions for the purpose of the respect of others’ rights or the maintenance of public order.

At the time when, thanks to the expansion of the information and telecommunications network and the remarkable advancement of the IT technologies, the so called ‘digital contents’ are being transmitted at a rapid pace, the practical demand is increasing for internal control over the State administrative agencies’ actions to regulate the contents. Of course, it might be argued that the authority to review the contents should be transferred to the private sector and the contents providers and users should be bound to the standards that are agreed upon voluntarily among themselves. Therefore, I attempt here to suggest some possible clues to the policy orientation for contents regulation in response to the changing information environment but within the current regulating system, and to the approach of controling the regulating actions.

Ⅱ. Guarantee of freedom of expression as an information human right

1. International trends

As is widely known, the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) provides for 'the obligation to respect human rights' in article 1 and specifies the guarantee of 'the right to respect for his private life and correspondence' in article 8 and 'freedom of expression' in article 10. In France, the constitutional right to freedom of expression, which originates from article 11 of the *Declaration des droits de l'homme et du citoyen* (French Declaration of the Rights of the Man and of the Citizen) of August 26, 1789, is also one of the major and core human rights and is regarded as a safeguard for free communication of ideas and opinions. It should be noted here that at the core of the guarantee of freedom of expression is the communication itself, irrespective of the means or media used for communication purpose.

Meanwhile, in Germany, article 5 (1) of *Grundgesetz* (German Constitution) stipulates that "Every person shall have the right to freely express and disseminate his opinions in speech, writing and pictures and to inform himself without hindrance from generally accessible sources. Freedom of the press and freedom of reporting by means of broadcasts and films shall be guaranteed. There shall be no censorhip (*Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt)*." This explicit declaration of the guarantee of freedom of expression and the principle of no censorship means that the protection of freedom of

expression as a constitutional fundamental right is at the heart of the liberal democracy, providing a constitutional foundation for the freedom of expression which is included in a broader definition of information rights.

In the United States, the right to information refers to the right to search freely for any publicly available information and to receive any information that others want to exchange for communications purpose, and it is believed that freedom of information derives from freedom of expression, as well as the right to express ideas and opinions. Of course, the information here, which is not only the subject of access but also the rights object, covers both public information (official information) and private information (personal information). Thus the information rights to be legally protected are based on the core elements of information access and information disclosure claims, which derive from the transition process from 'need to know', a passive notion from the perspective of information providers, to 'right to know', a positive one on the part of information receivers. In this light, the right to (access) information (RTI) and freedom of information (FOI) are considered identical in terms of fundamental human rights. Since the lack of information often deprives ordinary people of their opportunity to fully develop their potential and realize a wide range of human rights, the significance of information rights seems to lie in guaranteeing their access to public authority and, ultimately, enhancing the transparency and accountability of the governing regime.

The Universal Declaration of Human rights, which was adopted by the UN General Assembly of December 10, 1948, states in article 19 that "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." This article clearly provides for the 'right to know',

even though it may not be a direct justification for the fundamental right to information. We can also see that the article is more specific and accurate than the corresponding clause of the Korean Constitution which made reference to the article. Accordingly, it is understood that the right to access information for the general public is well-protected by constitutional provisions, which is confirmed by the specific rulings of the Constitutional Court on the right to know and the right to access information.

After all, this recognition of the right to information in national and international instruments has directed more attention to freedom of expression as the right to information and expression, especially in step with the changes in the information environment. In an illustrative example, the 'Civil Society Declaration to the World Summit on the Information Society (WSIS)' which was unanimously adopted on December 9, 2003 enumerates specific rights, including freedom of expression, as the 'human rights that are fundamental to the information and communications society', that is, the 'Centrality of Human Rights', and takes a general approach in discussing them, under the title of 'Shaping Information Societies for Human Needs'. WISI is aimed at providing guiding support for the informative response in the international community, by way of the principles and the platform for action to be shared in the information society, and leading the extensive implementation and application of the principles and platform.

2. Recent developments at home and abroad

The right to information and expression is a fundamental right based on article 1 of the Korean Constitution. This right is not only construed as a broad definition covering the transmission of ideas and opinions through information media, but also implies a narrow definition of the information right, that is, the right to handle information

independently in receiving, providing or refusing to receive or provide it. In other words, the subject of statement or delivery may or may not be the expression of information, or only the handling of information, not its expression, may be concerned.

The Korean Constitution specifies in article 21 (1) and (2) that “all citizens shall enjoy freedom of speech and the press and licensing or censorship of speech and the press shall not be recognized”. Considering the ‘speech and the press’ in the paragraphs are two exemplary forms of expression, it is understood that the Constitution provides for the general guarantee of freedom of expression.

Freedom of expression, which is now positioned as one of the most important fundamental rights that are indispensible for the respect of human dignity and values and the materialization of popular sovereignty and should be enjoyed by the people in a democratic society, has gone through a long history of the governmental authorities’ restriction and oppression on the statements of personal opinions or political criticism and the protests against such restriction and oppression before its guarantee has been well-established. Accordingly, freedom of expression is not only a fundamental right for individual persons but also is an indispensible instrument for shaping public opinions in a democratic manner. In this light, freedom of expression is a measure to assess the extent of democracy in a society, as well as a building block of the democratic system, serving as a means of building the democratic political or legal order. Similarly, the proposition that “freedom of expression has a constitutional status that supersedes that of any other fundamental right” implies that freedom of expression is not confined to a form of individual freedom but is based on the notion of ‘self-governed political regime’ - that is, the ruled participate in the governing body by criticizing the ruler. John Milton, in

his “Areopagitica” that he published unlawfully in protest against the British government’s censorship of the press, said that if Truth and Falsehood fought with each other, Truth would win the battle after all, asserting that there was no need for the government’s censorship. His argument was built on the belief that the correction of even harmful ideas or expressions should be made in the open marketplace of ideas after they are fought out by the conflicting ideas or expressions, and was also indicative of his firm belief that freedom of expression is integral to the democracy. Of course, it can be said that article 21 of the Korean Constitution on freedom of expression is also rooted in the same ideological or philosophical groundwork. Traditionally, freedom of expression refers to the freedom to present ideas or opinions (freedom of presentation) and spread them (freedom of delivery), specifically including freedom to express and spread opinions, freedom of information, freedom of newspapers and freedom of broadcasting and televising. In particular, the media which can be used to enjoy the freedom to express and spread opinions include all forms of media that are available for the expression or delivery of one’s opinions, such as statements, addresses, discussions, theatrical plays, broadcasting, music, films and popular songs; and documents, novels, poetry, paintings, photographs, sculptures and calligraphy.

Ⅲ. The issue of conflicting rights on personal information

1. Assumptions of the discussion

In general, the right to privacy and freedom of expression have been recognized as crucial and fundamental rights since the outset of the modern constitutionalism which is aimed to guarantee and realize fundamental rights for citizens. However, the two are

frequently in conflict with each other. More precisely, freedom of expression which is exercised through information media often infringes on the privacy of the person(s) related to the matter discussed in the expression made; whereas the extended protection of privacy may result in the contraction of freedom of expression. Put another way, it is indisputable that both the right to privacy and freedom of expression are indispensible for a liberal democratic society as they make it possible to realize the human dignity for individual persons, search for the truth and control the government, but it is important to fine-tune the two as they are essentially in a tense relationship with each other. This is why the relevant court rulings of the United States have sought after the reconciliation of the conflicts between the right to privacy and freedom of expression.

As is widely known, the Universal Declaration of Human Rights which was adopted at the 3rd session of the UN General Assembly of December 1948 provides for secrecy and protection of privacy in article 12 and the right to freedom of opinion and expression in article 19. The former concerns the right to privacy, which is generally understood as 'the right to be let alone', while the latter relates to the freedom of speech and the press whose core element is 'the right to know'. As the values involved in these two types of rights are contradictory to each other, it is critical to ensure that the conflicting rights are fine-tuned. Meanwhile, since the right of data subjects to personal information, which is covered in the declarations for privacy and personal information protection, has basically different dimensions, it is required to have a close look at its tense relationship with the freedom of the press, from a comparative and contrastive perspective.

Furthermore, it is true that privacy is necessary for the free development of personality and the maintenance of human dignity and is crucial for the existence of individualism and liberalism, but truth needs to be freely disclosed for the purpose of

the protection and advancement of the society and, for this reason, in some cases, individual rights should give way to public interests. This is based on the idea that freedom of the press and people's right to know can protect people by ensuring that certain facts are made public. Although the right to privacy is a product of the ideology which is in conflict with the notion of social interests, it is possible to strike the balance between the conflicting values included, by gradually adjusting the weights given to the values.

2. Legislative analysis

The Constitutional Court of Korea ruled, with regard to the case where the petitioner had asked the administrative office to allow him to inspect and photocopy a document with the intention to use the copy as documented evidence required to recover the ownership of real estate but the office refused to do so, that "although it can hardly be seen that the administrative office's omission has done any harm to the petitioner's property right, the office still seems to have violated the 'right to know', that is, the right of the citizens to ask the government for disclosure of information (the right of claim as a fundamental right), which is explicit in article 21 of the Constitution on freedom of expression and implicit in the preamble and articles 1 and 4 of the Constitution that provide for the public order of liberal democracy, when it refused to offer the petitioner the document for inspection and photocopying without any review of feasibility although the petitioner had a justifiable interest in the information contained in the document." The Court added that "the processing of such application for document inspection or photocopying would not be impossible even in the absence of the governing legislation". This ruling does not only confirm that the right to know or the right to ask for disclosure of information is a constitutional fundamental right

that should be enjoyed by every citizen and should not be violated by the government, but also affirms that this fundamental right has been recognized from constitutional interpretation since before the legislation of the Act on Disclosure of Information by Public Agencies (hereinafter "Information Disclosure Act"). Nevertheless, the discussions on how to realize the principle of information disclosure need to be made, with the focus being on the viewpoint that this right is not an absolute one but a relative one whose value should be fine-tuned in a tense relationship with other conflicting rights or interests. Accordingly, the law enumerates exceptional reasons which may defect from the coverage of the information disclosure principle. In interpreting the definition and the scope of the so called 'non-disclosure information', an approach must be taken to ensure that the purpose of the Information Disclosure Act which has an expressly provision for the information disclosure principle is not damaged and the conflicting interests involved are properly balanced and reconciled, leading to the establishment of a set of criteria by which to verify justifiability of information non-disclosure.

Non-disclosure information may be likened to 'Achilles' 'tendon', under this structural inconsistency in which an administrative agency is given the discretion to decide whether to disclose the information it holds, despite the presence and the ultimate purpose of the legal requirement on information disclosure. In other words, although the Information Disclosure Act declares in article 3 under the heading of 'information disclosure principle' that "the information that is kept and maintained by public agencies shall be made public, as is prescribed in the Act", it also sets up an exceptional category of non-disclosure information and, in article 11 (1), allows State agencies to decide, by reference to the exceptional category, whether to disclose some

particular information which they keep, potentially eroding the legislative purpose of the Information Disclosure Act which is symbolized by the 'information disclosure principle'.

In principle, the administrative information disclosure system which requires the State to disclose any administrative information it keeps to the general public should give highest priority to the information disclosure principle, guaranteeing the right of the citizens to claim disclosure of administrative information. Still, the information on privacy needs to be an exceptional case. However, as the right to claim disclosure of administrative information is an embodiment of the right to know, it is important that, on the assumption that administrative information is all open to the general public, the exceptional reasons written in law should be strictly interpreted in light of the intended purpose of such exceptionality. This is directly associated with the question of "To what extent can personal information be disclosed without prejudice to the purpose of personal information protection?", and here the personal information worth protecting would function as a measure to set the threshold of information disclosure. Thus it is important to reconcile the two conflicting rights, that is, balance the interests involved, and the first and foremost thing for the legislator to do in this respect is to determine how to materialize the optimization command.

It is necessary that the value of information disclosure and the value of information protection should be balanced in terms of legal norms while inherent interests should be protected for such personal information as is not to be made public. To this end, it should be ensured that the disclosure of personal information is confined to extremely exceptional circumstances where the disclosure of personal information serves the public interest

which is larger than the personal interest involved in not disclosing the information and there exists no other means to accomplish the purpose for which the particular information needs to be disclosed. Furthermore, in the electronic government where the convenience and the benefit of information disclosure, including information inspection, are maximized, it is necessary that full considerations should be made about the significance of personal information protection and attempts should be made to balance the interests involved in the conflicting values: free expression of personality through personal information protection vs. realization of the democratic ideology through information disclosure. The consequent social consensus should be incorporated into law.

Historically speaking, the ideas about freedom of information derived from the revolutionary philosophy which, rooted in the ideology of enlightenment, sought after a responsible government. In Sweden, the Constitution of 1766 specified the information disclosure principle as part of the freedom of speech and the press, and the Act on Freedom of the Press (*den svenska förordningen om Skiv-och tryckfriheten*) of 1810 recognized the citizens' right to claim disclosure of the government records and availability of the government documents, positioning itself as the first national law on information disclosure in the world.

The aforementioned ruling of the Korean Constitutional Court also stated that "the freedom to access, collect and process information, that is, the right to know, should be viewed as being naturally included in freedom of expression", noting that, in particular, with regard to the freedom to collect information as part of the right to know which is identical in its meaning to 'freedom of information', people are not simply entitled to receive information from the generally accessible information source without any

hindrance but are also guaranteed the freedom to collect information actively. In the same context, the Conference on Treaty establishing a Constitution for Europe which was held in Brussels, Belgium on June 18, 2004 agreed to incorporate 'freedom of information' into the fundamental human rights under the Constitution for Europe.

Despite the principle of information disclosure which is aimed to realize the right to know and secure administrative transparency, all public information cannot be made public with no exception. Considering that the values in conflict with those inherent in the right to claim information disclosure also take the form of legal interests to be protected, there is a strong need of the legal grounds by which to weigh the conflicting values in a balanced way. In this respect, the Information Disclosure Act includes a written provision on the exceptional category of non-disclosure information, making a list of exceptional reasons, albeit in a broad sense. Among them is personal information.

According to articles 3, 5 and 9 (1) of the Information Disclosure Act, every citizen is entitled to claim disclosure of the information that is kept and maintained by public agencies and such information should be made public in accordance with what is prescribed in the Act. However, the exceptional category of non-disclosure information defined in the subparagraphs of article 9 (1) may deviate from the disclosure principle. On one hand, these subparagraphs should not be interpreted for expansive application and, on the other hand, the provisos attached to the subparagraphs that sort out the areas not to be covered by the non-disclosure information category should not be interpreted for narrower application so that the balance between the right to know and the other rights may not be broken in disfavor of the former. Given that the right to

claim information disclosure is an essential part of the right to know which, in turn, is included in freedom of expression that is specified in article 21 of the Constitution, in case the right to know or the right to claim information disclosure comes into conflict with any other legal interest or fundamental right, a solution should be sought after to balance the interests or rights in a way to ensure that all the conflicting values involved are fully functional and effective, taking into full account the theory of balancing of interests and the selective discretion under the law.

With regard to disclosure of personal information under the Information Disclosure Act, although the Act provides that information shall be used only for the given purpose of collection, it seems that the Act needs to be amended to include a new provision that the Personal Information Protection Committee under article 7 of the Personal Information Protection Act, not the public agency concerned, shall decide whether to allow particular personal information to be made public or not. At present, public agencies decide to disclose personal information, simply in accordance with the information disclosure requirement but with no consideration made about the dimension of personal information protection, and only after a dispute breaks out over the information disclosure does the court intervene to review the adequacy of the agency's decision to disclose information. If the decision is found not adequate, the case shall be subject to the process of individual right remedies. In sum, it is required that the Information Disclosure Act should be revised to reinforce protection of personal information.

In principle, the use of personal information in the public space might result in the risk of the violation of the fundamental right by the governmental authority, which is

why an adequate degree of control is required. However, personal information may be used for a justifiable purpose of public interest in exceptional cases of the limitation of fundamental rights, unless the use of personal information is incompatible with the principle of law-based administration or is in violation of the principle of proportionality. Given that this justifiable limitation of fundamental rights, in combination with the principle of law-based administration, serves the basis of the Information Disclosure Act, the legal principles of personal information protection should be fully implemented to prevent the public authorities' administrative actions that are detrimental to the right to information self-determination. Currently, the Act allows personal information to be made public in such limited cases as are prescribed in the Act and meet any of the justifiable reasons for public interest purpose.

Meanwhile, in relation to the issue of broadcasting and communications review, article 44-10 of the Personal Information Protection Act provides for the establishment of the 'defamation dispute mediation division' made up of up to 5 members within the Korean Communications Standards Commission, in order to promote efficiency in performing the work of mediating the disputes over 'the information circulated through the information and communications network which has allegedly infringed on others' rights, including through privacy violation or defamation. It is notable that the instrument of 'mediation', one of the 'alternative dispute resolutions (ADR)' which has the same effect as a contract of compromise under the Civil Code, has been adopted to settle the dispute over the violation of the right to information self-determination as a consequence of the exercise of freedom of expression. In particular, with regard to the composition of the mediation division, the Act stipulates that one or more members should be a qualified lawyer. However, it is advisable that the lawyer quota should be

limited to one and, instead, a larger pool of the experts with more insights into IT fields or the rights of conflicting values, including freedom of expression, should be utilized.

Ⅳ. Conclusion

With regard to the regulation on information media, the standards for contents regulation should be based on a clear understanding about what methods are used by a particular medium to deliver opinions; whereas the standards for form regulation should include facilities requirements which provide greater entry flexibility and the legal requirements for transmission services which ensure fair competition among the service providers. This is crucial to application of the provisions in article 21 (2) and (4) of the Constitution and the optimization command is required to embody the provisions. What is of particular importance in this respect is to apply reversely the legal theory of limitation of freedom of expression to classify the information media into different groups depending on how active the information receivers who use the information media can be in participating in the opinion-exchanging process, and set up different standards of contents regulation for different groups. It is also important to maintain weak entry regulation, for example, by allowing applicants to participate in the business of operating the information media by which to transmit digital contents once they have completed a simple process of registration or reporting, and to establish a market structure in which fair competition is sustained. Now that the public benefit of an information medium does not depend on whether the service concerned is in the public sphere or not, but depends on the extent to which the contents can be regulated

or whether the information contains such secrets as are to be legally protected and, therefore, are subject to contents regulation, it is of great significance to create the criteria by which information media can be divided into different specific groups. Only after the above is accomplished with regard to the regulation on information media can we have a sufficiently empowered legal theory.

Within the current legal framework, the Korean Communications Standards Commission is not a State administrative authority, although it is classified as an administrative office under the Administrative Procedural Act. Nevertheless, given that, under the current structure which is subject to practical intervention, as well as to judicial control affected by the political influence and guardianship, the judgments of the Commission may result in public-law disputes, it is meaningful to discuss the ways to transfer to self-regulation. Similarly, in light of the changes in the information environment, it is necessary to review the whole process of contents regulation by the governmental authorities, not only to check the regulation conformity for all information media, including convergence media, but also to restructure the organization of regulation.

However, it should be reminded that the revision or repeal of unnecessary legal provisions is required for the introduction of self-regulation. Although it is admitted that the enforcing power of the State is inevitable to some extent to secure the effectiveness of self-regulation in the Internet governance and that the pure self-regulation can be hardly guaranteed, the intervention of the State should be minimized and the abuse of peremptory norms should be avoided. Accordingly, even if the law-based self-regulation constitutes ‘enforced or coerced self-regulation’ or

'regulated self-regulation', the desirable form of Internet self-regulation would be 'joint self-regulation' which is agreed upon by all the actors in the areas related to Internet services. Therefore, considering the enforcing nature inherent in the self-regulation by public organizations in a narrow sense or the persons commissioned with public service, it is advisable that self-regulation should be implemented in the form of private autonomy (*Privat autonomie*), not in the form of decentralization or contracting-out. If the legal provisions on the organization of self-regulating agencies admit the municipalities which are not only 'legal persons' under the public law but are also administrative actors that 'hold the administrative power' and 'are accountable for the rights and duties concerning administration', their work, which is the decentralized State work to be performed for essential public service, can be simply classified as the work done by an administrative actor other than the State. In this case, it cannot be expected that their presence will promote close cooperation in the governance, leading to the shared elements of 'interdependency, autonomy, partnership and network'. Therefore, what is important here is the implementation intention and practical reason (*praktische Vernunft*) for self-regulation, but because too much emphasis is placed on the public-interest aspect of self-regulation, it is not likely that the legal grounds for other aspects will be established. In this light, although the Korean Communications Standards Commission, classified as an unincorporated public organization, constitutes a major part of the governance now, there exists a practical need, for the purpose of extended self-regulation, to seek after legislative improvements which might be accomplished by linking the organizational model similar to the foundation or unincorporated organization under the Civil Code with the active role of contents regulation.

패널토론

"정보화 사회에서의 프라이버시권과 표현의 자유의 균형적 조화"

- **김 범 수** (연세대학교 정보대학원 교수)
- **전 응 휘** (녹색소비자연대 상임이사)
- **장 용 근** (홍익대학교 법학부 교수)
- **Wolfgang Benedek** (Professor, Graz University)
- **Andrew Puddephatt** (Director of Global Partners)

토론

소셜네트워크 환경에서의 알권리, 표현의 자유 및 프라이버시권의 상충과 균형

김 범 수

(연세대학교 정보대학원 교수)

Discussion

A Collision and Balance between the Right to Know, Freedom of Expression and the Right to Privacy in the Social Network Environment

KIM, Beom-Soo

(Professor, Yonsei University)

토론

정보사회에서의 표현의 자유와 프라이버시에 대한 몇 가지 성찰

전 응 휘

(녹색소비자연대 상임이사)

- 정보사회에서 이용자의 중심적인 권리로 제기되는 것은 표현의 자유와 프라이버시 두가지 권리이다. 이것은 정보사회 - 사실은 정보통신 네트워크 사회가 한편으로는 인터넷과 같은 네트워크를 통해 개개인에게 정보접근의 기회와 더불어 의견제시, 표현수단을 제공함으로써 주어진 새로운 이용자의 정보와 커뮤니케이션 환경을 제공한다는 사실과 정보통신테크놀로지가 개개인의 표현행위와 선택행위에서부터 다양한 전자적 상호작용을 뛰어넘어 오프라인 영역에서의 다양한 행태에 이르기까지 모니터할 수 있는 모니터링 환경을 제공한다는 사실을 반영한다. 그러므로 정보통신 네트워크는 한편으로는 프라이버시에 대한 도전과 위협을 다른 한편으로는 표현행위의 다양한 가능성을 제공한다.

- 정보통신네트워크가 개개인의 표현과 의사소통의 채널을 개방하게 됨에 따라 “언론기관의 자유”에 머물렀던 언론의 자유는 개개인의 “표현의 자유”에 대한 관심으로 확대되었다. 전통적으로 개개인의 통신행위는 책임있는 공적 소통행위와는 다르게 개개인의 교신내용의 비밀을 국가가 보호해야 하는 영역이었으

나 인터넷으로 인해 이러한 사적 교신과 공적 발언의 경계가 불분명해지고 있다. 다만, 개개인의 이같은 소통채널이 과거 언론처럼 배타적 독점적으로 특권을 가진 자에게만 부여되는 것이 아니므로, 따라서 사회적 여론에 독점적 영향을 주는 것이 아니므로 개개인의 공적 의견개진에 대하여 배타적, 독점적 의사소통의 수단을 가진 언론매체의 보도나 논평에서처럼 엄격한 사회적 책임을 요구하는 것은 부당하다. 그러한 사회적 미덕은 권장될 수 있는 것이지만 강제되어야 하는 것은 아니다. 그리고 기성 언론매체의 편향된 의견개진에 대해서는 사회적으로 독자의 반론권이 요구되었지만 인터넷에서는 얼마든지 반대의견이나 다른 의견이나 사실에 대한 반박이 가능하므로 별도의 반론절차를 마련해야 할 이유도 없다. 그런 점에서 개개인 표현행위에 대하여 공공질서와 미풍양속을 해할 수 있다는 이유로 제한하려 하거나 사회적 제재를 가하려는 행위는 근본적으로 개개인의 의견개진을 제한하는 행위에 다름 아니다.

- 사전제재 금지원리의 기준은 출판과 유통시점이 아니라 법원의 판정시점이다. 네트워크를 통해 유통되는 정보에 대한 행정기구의 정보통제는 그것이 표현물의 출판과 유통 이후에 이루어진다 하더라도 검열에 해당한다. 그러한 정보통제는 행정목적이나 정치적 목적에 의해 보호해야 할 표현조차 왜곡하여 제한할 수 있다. 따라서 모든 표현행위에 대한 제한은 소통의 구성원으로 이루어지는 공동체의 합의에 따라 자율적으로 이루어지는 것이 최선이다. 자율적 내용규제는 필요에 따라 공동체의 합의 형성과정을 통해 규제의 기준을 바꿀 수 있다. 자율규제의 기준을 국가가 부과하는 것은 사실상 변형된 행정검열에 해당한다.

- 역설적으로 표현행위의 다양한 가능성이 실제로 구현되기 위해서는 프라이버시 보호가 가장 근본적인 전제이자 요구가 된다. 하지만 이와는 대조적인 가

장 극명한 예가 바로 실명제이다. 특히 인터넷게시판실명제는 익명표현의 자유에 대한 본질적 침해이며 사실상 복수계정의 보유 및 사용을 불가능하게 하고, 개인의 신상털기를 용이하게 함으로서 프라이버시 보호를 원천적으로 불가능하게 한다. 실명제는 고유식별번호의 사전 확인 및 등록을 통해 정보사회에서 다양한 출처에서 수집되어 축적되는 개인정보를 특정 개인 생활의 입체적인 단면을 드러내는 프러파일링의 형태로 활용하는 것을 가능케 함으로써 프라이버시를 심각하게 위협한다. 고유식별번호가 제한없이 시민생활의 거의 모든 영역에 제한없이 사용됨으로써 이같은 프라이버시 약화는 보편화되었고 주민번호의 대량 유출사고를 통해 주민번호는 이미 본인확인의 효력까지도 상실했다. 주민번호의 유출로 인해 다양한 형태의 피싱이 일상화됨으로써 재산상의 손실 우려가 높아졌다. 유비쿼터스 사회라는 비젼속에서 등장하는 유비쿼터스 기술들은 유무선기술과 다양한 센서를 통해 개개인의 위치, 행태, 상호작용 등을 임시식별자로 수집하지만, 인터넷게시판실명제는 이러한 임시식별자를 고유식별자로 바꾸어 사실상 벌거벗은 사회, 프라이버시가 투명하게 노출된 사회로 바뀌게 한다.

실명제와 관련하여 국가인권위는 일찍이 다음과 같은 결론을 내린 바 있다.

- 인터넷 언론사 선거게시판 실명제는 선거게시판에 의견을 게시하고자 하는 모든 국민을 허위정보 및 타인에 대한 비방을 유포하는 자라는 사전적인 예단을 전제로 하는 것으로, 명백한 사전검열에 해당하며 익명성에서 기인하는 인터넷상의 표현의 자유와 여론형성의 권리를 제한하여, 세계인권선언 제19조와 헌법 제21조의 표현의 자유에 반하고 개인정보가 본래의 수집 목적에서 벗어나 개인의 의사와 관계없이 광범위하게 이용될 수 있다는 점에서 헌법 제17조의 개인의 자기정보 관리 통제권을 침해할 우려가 있으며, 헌법 제37조의 국

민의 기본권 제한의 원칙에도 어긋납니다.

- 실제로 표현행위자에 대한 신원노출은 정치적 이견으로 인한 탄압에 대한 두려움을 조장하며 내부자 고발에 대한 억압, 소수자에 대한 차별, 표현행위에 대한 냉각효과를 유도함으로써 사실상 표현의 자유를 제한한다. 결국 이것은 결과적으로 민주주의와 인권의 형해화를 가져온다.

익명 표현의 자유가 타인의 프라이버시를 침해할 수 있다는 우려가 있지만, 개인의 권리침해와 같은 범죄적 표현행위에 대해서는, 관련 표현에 대한 일련의 절차에 따르는 접근차단이나 삭제 등이 가능할 뿐 아니라 표현행위의 사전신원확인이 아닌 IP주소 등을 통한 사후 신원추적을 통해 범죄행위자에 대한 규명도 가능하므로 그러한 우려를 이유로 익명표현의 자유를 제한해야 할 이유가 없다.

- 실명제는 사이버아이덴티티의 프라이버시 보호를 원천적으로 불가능하게 한다. 하지만 익명성을 전제로 하는 사이버아이덴티티/id에 대해서도 프라이버시 보호가 필요하다. 이를 위해서는 복수의 계정사용이 가능해야 하고, 계정의 이용기록과 관련된 다양하고 통합적이며 선택적이고 이용자 친화적인 프라이버시 보호수단 제공을 권장해야 한다. 정보통신기술의 발달로 인해 계정의 복합적이고 누적적인 이용기록을 이용하여 이용자에게 더 향상되고 이용자 친화적인 서비스를 제공하는 것이 가능하고, 이용자는 이를 선택하여 사용할 수 있지만, 프라이버시 보호를 위해서 이용자가 필요할 경우 이용자의 요구에 따라 사용할 수 있는 세분화된 개인정보 제공 철회수단이 제공되지 않을 경우, 개인정보의 자기결정권은 유명무실화될 것이다.

- 프라이버시 보호기제에서 개인의 자기정보통제권의 가장 중요한 수단으로 사

용되는 “동의”는 정보통신기술 발전에 따라 그 효력 자체가 도전에 직면하게 되었다. 개인정보의 수집에 대한 인지 자체가 어렵고, 인지한다 하더라도 합리적 판단에 따른 선택이 어렵고, 합리적 선택을 한다 하더라도 수집되는 정보들이 여타 경로로 이루어지는 빅데이타 수집과 연관되어 어떻게 통합되어 사용될지 여부에 대하여 충분한 사전 인지가 어렵기 때문에 “동의”는 필요하긴 하지만 그 자체로 자기정보통제권의 충분한 수단이 되지 못한다. 따라서 “동의”에 대한 보완적 기제가 필요하다.

- 따라서 정보통신 네트워크 사회에서 개개인의 자기정보통제권을 적극적으로 구현하기 위한 수단은 오히려 익명권을 보장하고 강화하는 것이어야 한다. 개인정보자기통제권이 수집된 개인정보의 방어와 보호에 치중하는 것이라면, 익명성은 프라이버시를 모든 표현과 행위에서 적극적으로 그리고 예방적으로 프라이버시권을 실현하는 것이다. 정보통신 네트워크 환경에서 개인정보에 대한 익명권은 원칙적으로 권장되고, 불가피할 경우에 한해서만 자기정보에 대한 수집에 대한 선택적 동의가 허용되어야 한다.

- 익명권 보장과 함께 또다른 보완수단으로서 개인정보 수집목적의 허용범위에 대한 제한 을 검토해야 한다. 정보통신기술의 발달에 따라 다양한 형태의 행태정보의 수집방식과 모바일 수집환경의 결합 등으로 인해 개개인으로서는 사전에 합리적 판단에 따라 “동의”의 의사결정을 내리기 쉽지 않은 상황들이 존재한다. 이것은 개개인의 위치정보, 건강기록이나 재무상태 등 민감한 개인정보에 관련된 요소들의 경우에는 더욱 그러하다.

- 개인정보의 수집목적외 사용을 허용하는 “공공목적”의 범위 역시 제한되어야 한다. 가장 민감한 진료기록을 포함하는 건강보험 급여청구 기록이 다양한 형

태의 “공공적 목적”이라는 명목으로 여타 행정행위를 위한 수단으로 활용되는 것은 개인정보 남용의 가장 불행한 사례이다. 개인의 건강관련 정보는 보험급여 이외의 목적에 사용되더라도 공중보건이나 질병연구와 같은 동일 분야의 공공적 목적으로 사용을 제한하고, 동일 분야 이외의 예외적 사용의 경우에도 영장제도와 같은 별도의 법원의 허가절차에 따르도록 엄격하게 제한해야 한다.

- 개인정보의 남용방지 및 역감시체계 구축을 위해서는 공공목적을 위해 개인정보를 목적외로 사용하는 경우들에 대한 조사, 행정정보의 공유시스템에 대하여 주기적으로 이루어지는 투명한 정보공개 리뷰 및 프라이버시 감사가 필요하다.

- 방송통신융합은 매체의 다원화를 통해 정보채널을 다원화하고, 다양한 정보소스와 비시장적 정보의 생산 및 배포, 공유를 가져온다. 방송매체에 대한 규제의 근거는 주파수의 희소성과 채널의 독점성, 영향의 침투성에 있기 때문이다. 방송미디어의 이같은 특수성은 앞으로도 상당기간 유효한 것으로 남을 것이므로 여전히 교차소유규제나 자본의 소유지분제한 등은 유효하다. 그러나 방송컨텐츠의 채널이 다양한 온라인 컨텐츠의 유통경로로 분화되고 방송통신융합화의 진전이 이루어짐에 따라 전통적인 방송규제도 내용규제의 수준을 완화해야 하며, 개개인의 표현의 자유의 가능성도 더욱 확장해야 한다. 방송내용에 대한 인위적 공정성 규제를 강화하고 인터넷에서의 표현행위에 대하여 방송규제에 버금가는 수준의 내용규제를 시도하는 것은 융합이 가져오는 커뮤니케이션 환경의 변화와 새로운 기회에도 불구하고 언론의 자유와 표현의 자유를 위축시키는 것이다.

Discussion

Some Reflections on Freedom of Speech & Privacy Rights in Information Society

CHUN, Eung-Hwi

(Standing board member, Green Consumer's Network)

- Freedom of speech and Privacy Rights are the most significant rights in information society. This reflects two faces of information society – on the one hand, the fact that the networked society of information and communication provides for new opportunities for information access as well as a variety of instruments for putting forth opinion and expression throughout those electronic channels like the internet, completely different environment for information and communication from the past. On the other hand, the other fact that Information and Communication Technology(ICT) also provides for watching environment to be able to monitor individual's speech, optional behavior, diverse electronic transactions, and even lots of actions conducted in offline world. Therefore, the information and communication network provides for diverse possibilities of speech and expression and also simultaneously is giving new challenge and threat to privacy.

- As information and communication network opens up those channels for individual's speech and communication behavior, the freedom of speech developed

and expanded from the freedom of press into the freedom of individual's speech. While traditionally, the confidentiality of individual communication has been protected by the state as private communication, differently from accountable public communication, now internet has blurred the borderline between private communication and public speech. However, since these new individual communication channels are not exclusively monopolized by the few like mass media, and that would never make an monopolizing effect on public opinion, it must be unfair to demand a rigid social accountability to this public speech of the individual as much as those reports or comments of the press and other mass media, which have owned the exclusively monopolizing communication channels, had been required. Such a social virtue could be encouraged but should not be enforced. So, while reader's right of reply had been socially required against those biased views of the press, this separate procedure of reply is not necessarily required since internet provides for the way of opposition or different talks or suggestion of different facts. In this respect, in the name of public order and morality, making an attempt to restrict individual speech or to impose social sanctions on it is fundamentally to oppress the freedom of speech.

- The threshold of "Prior Restraint" is not the moment of publishing and distributing of information and communication but that of judicial judgment. The direct information control of administration agency for the information flow over the Internet, even if it is to be carried out even after the publishing and distributing of the contents, is itself a censorship. Such an information control could distort or limit even the "protected speech". Accordingly, the best option of all restriction of speech is the autonomous regulation based on community consensus of all

stakeholders. Such a self regulation would change the criteria for regulation through forming community consensus if necessary. However, to impose those criteria by the state is a variant of administrative censorship.

- For the purpose of realizing those diverse possibilities of speech, concurrently the privacy protection is to be fundamentally assumed and to be basically required. However, the most contrasting case of this is the framework of pre-identification of internet speech, which is now being implemented in Korea. This framework is particularly the essential infringement of freedom of anonymous speech and to make it unable to own and use multiple accounts or ids and to enable to "gather and expose individual's identity information over the Internet" behavior, and the privacy protection is led to be essentially invalid. This framework, by using prior confirmation or registration of inherent distinctive number (registered residential number) and by enabling to profile one identity's complex sides through gathering and accumulating all possible information on the person from a variety of different sources based on common key information of the distinctive number, severely threatens the person's privacy. This weakening of privacy has already been predominated because this inherent distinctive number has been recklessly used even to every corner of all living lives. And due to the accident of breaking into big commercial service providers' systems and stealing almost all people's residential number a few times, that number has no longer had identification capacity and the routinization of phishing by exploiting those stolen residential number is threatening people's loss of financial property. Moreover, ubiquitous technologies which is being introduced in ubiquitous model cities designing in the vision of ubiquitous society, collects individual's location information, behaviors,

and transactions as ad-hoc identifiers through wireline or wireless communication technology and lots of sensors, but this anonymous big data could be mixed with this framework of pre-identification of internet speech and finally to form a naked society, where all peoples' identities are transparently exposed.

- Concerned with this framework, National Human Rights Commission of Korea had already concluded in 2004 as follows;

1) As for internet press, the pre-identification of bulletin board service writing in the time of election presupposes that all people wishing to make a speech on the bbs could be potentially those who would be trying to publish and to distribute false information and defamation. This is obviously prior censorship and restricting the freedom of speech and the rights of making public opinion over the Internet which is based on anonymity. Therefore, it is against the freedom of speech which had been declared in the Universal Declaration of Human Rights article 19 and Constitution article 21.
2) And it opens up the possibility of the abuse of the collected personal information beyond the prior specified collecting purposes. This could infringe the self-control rights of personal information, which is statutory in Constitution article 21.
3) Also it is against the limitation principles of people's basic rights of Constitution article 37.

- Practically, the identification exposure of speech maker, which this framework of pre-identification of internet speech demands, terrifies writers into the political oppression against different views, and lead to the oppression of conscience

accuser, the discrimination of the minority, and finally to the cooling effect of the freedom of speech. This results in a wreck of democracy and human rights.

- There is some worry that the freedom of anonymous speech would infringe the other's privacy, but this criminal behavior of speech like defamation could be effectively prevented by a procedural mechanism of blocking or deleting those speeches together with respecting the writer's publishing rights. And internet protocol address could also be available for identifying those criminal writers afterwards. Therefore, this potential negative effect of harmful expression could not be an pretext of restricting the freedom of anonymous speech.

- This framework of pre-identification of internet speech forecloses the privacy protection of cyber-identity. However, the privacy of cyber-identity which is essentially based on anonymity is also to be protected. For this purpose, multiple use of online account/id should be allowed. And diverse, optional, user-friendly integration interface for privacy protection into those account activity records like in a format of log file should be encouraged to be provided. Those activity records could be optionally used for providing for better and more user-friendly services, but without more effective and differentiated consent withdrawal instrument, this technical possibility would only exacerbate the privacy environment. In this context, the self-control rights of personal information would be incompetent.

- The effectiveness of user's consent rights, which have long been the key instrument to maintain the self-control rights of personal information, is being challenged as the ICT develops. Consent is necessary but not enough for the

protection of the self-control rights of personal information in today's technological environment where to be aware of whether personal information is being collected or not is itself very difficult, and where reasonable decision making for optional consent is neither easy even after the awareness, and where prior full knowledge of the way of how those collected personal information would be used mixing with other big data coming from unidentified sources could not be provided even after reasonable choice. Therefore, more complementary mechanism should be provided.

- One possible option is to ensure and to reinforce the anonymity of speaker as a positive instrument to protect the self-control rights of personal information in the networked society of information and communication. While up to now the self-control rights have defensively protected the security and use of the collected personal information, anonymity rights is positively, preemptively and preventively realizing privacy rights in all speech and expression behaviors. In the network environment of information and communication, the anonymity rights of personal information should be encouraged as a default principle and the optional consent of collected personal information should be allowed only under inevitable conditions where anonymous speech or action could not be carried out.

- As another complementary mechanism, to restrict the scope of the legitimate purpose of collecting personal information could be taken into account. There are many difficult conditions where the individual could not easily make a decision of consent due to the mixture of diverse collecting techniques and mobile wireless collection environment. This is particularly tough when such sensitive information as personal location information, health information or financial records are concerned.

- The exceptional scope of “public purposes” condition, which is allowed to use the collected personal information regardless of its original collecting purposes, should not be unconditionally allowed. Personal health record, which are recorded in hospitals and submitted to the health insurance authorities for insurance payment are being abused for a variety of administrative purposes, and it is the worst and unfortunate example. This kinds of health information could be used for the same sector’s public purposes like public health or disease research, but the other exceptional use of such personal information should be rigidly restricted in a way of depending on separate judicial procedure like warrant request.

- To prevent the abuse of the collected personal information and to launch reverse watching scheme, those surveys on public purpose use of personal information differently from the collection purposes should be implemented. And periodical transparent information disclosure how administration information sharing system is operating and periodic privacy audit should be institutionalized.

- The convergence of broadcasting and telecommunication is diversifying media and makes multiple channels available, and also this leads to the development of diverse information sources and the production, distribution and sharing of non-market information. Since the rigid regulation of broadcasting has deeply rooted on the scarcity of electronic wave resources, the monopoly of the limited number of channels, the pervasiveness of broadcast effect, and those foundations are being shaken and weakened, traditional rigid regulation of broadcast contents should be reviewed. Because this particularities of broadcast would be sustained for the time being, traditional regulation tools like cross ownership regulation or

ownership portion limit should be maintained, but contents regulation of broadcast should be deregulated as much as diversified and more channels are available including online contents services. Concurrently, the freedom of speech of the individual should be expanded. Then, the reinforcement of artificial fairness doctrine in broadcast or semi-broadcast level contents regulation being applied to internet speeches is to shrink the freedom of press and the freedom of speech despite of the changing communication environment including digital convergence.

토론

표현의 자유와 책임
- 정보보호권의 헌법적 보호

장 용 근

(홍익대학교 법학부 교수)

민주주의는 대화와 토론을 전제로 한 다수결을 통해서 공공선을 추구하는 과정이라고 할 수 있는데 이러한 민주주의를 이루기 위한 기본권으로는 의견과 표현의 자유가 반드시 보장되어야 한다. 결국 이러한 측면에서 단지 개인의 차원이 아닌 시민권이라는 측면에서 과거의 소극적 측면이 아니라 적극적으로 국가의 정책결정에 참여하면서 국가의 권력을 통제하려는 의미에서 접근할 수 있겠다.

하버마스는 기존의 언론매체는 권력 기관화되어 국민의 의사를 반영하기 보다는 자신들의 목소리만 내는 경우가 많아 졌다. 하지만 인터넷은 이러한 기존의 언론과는 달리 국민들이 직접 참여하여 자신의 목소리와 다양한 국민의 소리들을 들을 수 있게 하여 인터넷뉴스 등의 새로운 매체 등을 생성하게 하였다. 우리나라는 하버마스가 지적한 대로 기존의 언론이 권력 기관화되어서 국민들의 목소리를 내기보다는 자신들의 목소리를 냄으로써 국민과의 괴리현상이 깊어져만 갔다. 이러한 언론은 정치권력마저 위협을 가할 수 있는 상황에서 국민들의 목소리는 이 나라에서 주인이면서 전혀 자신들의 목소리는 낼 수 없고 언론기관의 사주의 목소리만 낼 수 있었다. 하지만 우리나라에서 오마이 뉴스를 시작으로 새로운 대안언론이외에 기존의 언론들도 인터넷사이트를 만들어 국민들의 목소리를 듣고 이

를 적극적으로 받아들이려 한다. 이는 표현의 자유의 기능적 관점에서 검토해 볼 때, 전자신문 등의 등장은 형식화된 국민주권주의가 실질화 되고 있으며 그 어느 나라 못지 않게 표현의 자유가 증진되고 있다고도 볼 수 있다. 다만 특정한 정치 사안에서의 정권실세들의 과민반응은 문제가 되고 있으나 전반적으로는 과거 어느 때보다 더 표현의 자유가 보장되고 증진된다고 전체적으로 평가할 수 있을 것이다. 또한 실제로 수많은 목소리를 낼 수 있게 되어 그 자체가 민주주의의 발전을 이루게 되었다. 여기서 사이버상의 표현의 자유를 논하는 것은 시장의 자유모델에 입각하여 자기지배의 원칙의 연장선상에서 표현의 자유를 이해하고 인터넷의 중요한 특성인 익명성으로 인해서 기존의 표현의 자유와는 다른 폭넓은 보장을 받음으로 해서 진정으로 표현의 자유의 황금기를 구가하고 있다. 프라이버시의 침해와 표현의 자유의 남용에 대해서는 엄격한 책임을 지움으로써 진정한 표현의 자유의 정립을 위하여 검토의 필요성이 있으나 표현의 자유의 공익적 기능을 고려하여 최대한 보장되어야 한다.

하지만 표현의 자유의 남용 또한 방지되어야 하기에 우선 개넌내제적인 표현의 자유의 보호영역에 대해서 검토될 필요가 있다. 이는 확립된 표현의 자유의 보호영역(아동외설은 확립되게 배제)에 해당 시에는 당해 조항의 적용대상이 아니기에 처벌되지 아니하기 때문이다. 물론 경계선상에 있는 표현의 자유의 경우(상대적 보호영역-성인음란물)에는 헌법 37조 2항상 처벌의 대상이 될 여지도 있다. 하지만 보호영역에 해당하지 아니한 경우에도 당연히 처벌대상인 것은 아니다. 이는 무시내지는 관용, 민사상손해배상, 행정적 제재 등으로 해결이 가능할 것일 수도 있기 때문이다.

표현의 자유의 헌법적 보호영역은 정신적, 이성적 방법에 의한 언어나 행동의 표출을 의미하기에 이성적인 방법에 의하지 않는 표현은 헌법상 보호되지 않는다. 또한 여기서의 표현의 자유는 국민의 알권리를 위한 정보전달적인 목적으로 행해져야 한다[1]. 표현행위는 사실주장과 의견표현행위로 분류될 수 있다. 의견표현은

그것이 공적으로 항으로서 원칙적으로 허용된다는 추정을 받지만 사실주장은 허위의 경우는 보호를 받지 못하고 진실한 사실일지라도 그것이 명예훼손적 발언인 경우 공익에 도움이 되지 않는 한 원칙적으로 면책이 되지 않는다.

표현의 자유의 천국인 미국에서도 화자가 조기폭력단에게 린치를 가하도록 선동하는 표현, 폭력적 반응을 유발시키는 이른바 투쟁적 언사나 진정한 협박, 아동외설, 명예훼손, 서비스나 상품과 관련된 허위의 표현, 성차별을 조장하는 불법적 표현 등은 금지되고 처벌되는 것으로 허용되고 있으며 미국의 수정헌법 제 1조는 결코 규제되지 아니하는 수다(talkatives)를 보호하려는 것은 아니다[2]. 하지만 미국의 수정헌법 제 1조는 정부에 대한 반대의견의 억압이나 대중적이지 아니한 견해표명의 억제에 대해서는 금지하면서 오히려 이러한 견해들은 보호하려고 하고 있으며 이는 민주사회의 장점인 다양성을 보호하고자 한다는 점에서 근거하고 있다.

과거 영국에서는 국가나 공무원을 비난하는 성명서를 발표하는 것이 문서선동죄로 간주되어서 처벌된 경우가 있었으나 후에 관행적으로 그리고 입법에 의하여 제한이 가해지게 되었다[3]. 하지만 오늘날 이에 대한 문제는 전세계적으로 정치적 표현의 자유로 허용되어서 공익에 도움이 되고 진실한 사실이라면 허용되기에 해결되게 되었다. 사실적 주장의 경우에는 진실하고 공익에 적어도 해가 되지 아니할 것이어야 한다. 다만 이를 방지하기 위해서 처벌까지 가야 하는지에 대해서는 진지한 검토가 필요하다. 명예훼손이나 모욕, 음란한 표현 등은 공익에 해하는 표현의 구체적 예시이자 표현의 자유의 한계이자 보호영역에 속하지 않는다. 물론 공익을 위하여 진실한 사실을 공연히 표현하는 경우는 현행형법 310조상 위법성이 조각되는 것은 당연한 규정이다. 음란한 표현도 국가에 따라서는 표현의 범위

1) Rodney A. Smolla, Smolla and Nimmer, On Freedom of speech ; A Treatise on The Amendment, Student Edition, Matthew Bender, 1994, p.5.
2) Ronald D. Rotunda, The Warren Court and Freedom of the Press, in the Warren Court (Bernard schwarts, ed., Oxford University Press 1996)이부하, 표현의 자유와 미국헌법, 한국학술진흥정보,2007, 12-13면에서 재인용 참조.
3) 이부하, 표현의 자유와 미국헌법, 한국학술진흥정보원, 2007, 36-37면 참조.

에 속할 수 있다.

구체적으로 허위사실에 기초한 폭력적 선동은 보호영역에 해당하지 않으나 특히 미발표 내지는 미확정의 사실의 경우 어느 정도의 추측성이나 예측성표현은 공익을 위하여 표출하는 경우, 후에 이것이 허위라고 증명되더라도 이는 표현행위 당시에 미리 대비함으로써 공익에 해가 되는 것을 예방할 수 있는 경우에는 표현의 자유의 보호 영역에 해당한다. 사실에 기초한 폭력적 선동의 경우도 무조건 처벌하여야 하는 것은 아니고 무시내지는 관용으로 해결할 것도 존재한다[4]. 이는 표현의 자유의 보호영역에 해당하거나 해당하지 아니하여도 37조 2항의 대상이 되어서 당연히 제재의 대상이 될 수 없고 공익에 해가 되는 경우에만 가능하기 때문이다.

해가되지 아니하는 일반적 행동의 자유와 알 권리를 전제로 하는 표현의 자유를 동일시할 수는 없다. 그리고 그 보호의 정도도 다르다고 할 것이다. 즉 당해 조항의 공익을 해할 목적의 허위의 사실을 전기통신망을 통해서 유포하는 행우는 표현의 보호영역에 포함되지는 아니하나 이를 처벌하는 것이 과잉금지인지 여부는 신체의 자유나 일반적 행동의 영역에 해당할 수 는 있다고 할 것이다.

하지만 헌법재판소는 일명 미네르바사건 즉 전기통신기본법 47조 1항사건[5]에서 “표현이 어떤 내용에 해당한다는 이유만으로 표현의 자유의 보호영역에서 애당초 배제된다고는 볼 수 없으므로, ‘허위사실의 표현’도 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역에는 해당하되, 다만 헌법 제37조 제2항에 따라 제한될 수 있는 것이다.”라고 하여 허위사실의 표현이 표현의 자유의 보호영역이라고 판시하나 이는 잘못된 결정이라고 보인다. 이는 권리와 권리의 남용을 혼동한

4) 미국산소고기촛불집회에서 시위여성이 강간당하고 시위대에게 무차별 폭행한다는 허위사실을 유포한 경우에는 표현의 자유의 영역에 해당하지 아니하지만 이를 형사처벌로 하는 것은 바람직한 민주주의의 발전을 위하여서 관용의 정신으로 이해하는 것이 타당하다고 보인다. 또한 만우절에 있어서 거짓말이나 친구사이의 거짓말이 중대한 해악을 끼치지 않는 한 단지 웃음이나 거질말쟁이로 사회적 평가로 끝낼 사항도 존재한다. 하지만 사회적 해악이 크다면 단지 관용으로 끝낼 일은 아니다.

5) 헌재 2010.12.28, 2008헌바157

결정으로서 권리만을 보호하여야 하는 헌법재판소의 역할에 반한다고 보인다. 다만 진실인지 허위인지 모호한 경우에는 허위사실이 아닌 진실한 사실로 보아야 할 것이다.

음란표현은 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역 내에 있다고 볼 것인바, 종전에 이와 견해를 달리하여 음란표현은 헌법 제21조가 규정하는 언론·출판의 자유의 보호영역에 해당하지 아니한다는 취지로 판시한 우리 재판소의 의견을 변경하기도 하였으나 포르노가 허용된 미국에서도 표현의 자유의 보호영역이라고 인정되지 아니한 영역가지 확대한 무리한 결정이라고 보인다.

오늘날 사상의 자유시장이 더 중요한 의미를 가지는 데에는 정보격차의 해소의 문제와도 관련이 있다. 즉 표현의 자유의 신장을 통해서 국민들에게 더 풍부하고 우수한 정보를 국가이외에도 민간에서 자유롭게 공급한다는 측면에서 사상의 자유시장이론은 오늘날도 중요한 역할을 할 것이다. 미네르바사건 등이 발생한 데는 중요한 정보가 정부가 독점되어 있고 그에 대한 접근은 소수에게만 있다는 정보격차의 문제를 민간인이 이를 국민들에게 알리려고 하였다는 점을 보면 앞으로도 사이버상의 표현의 자유시장은 더 확대되고 공익에 해가 되지 아니하는 한 보장되어야 할 것이다.

그렇다고 국가가 자유방임적 입장을 취해서는 아니된다고 보인다. 헌법적 측면에서는 알권리 차원의 문제이자 정보복지권[6]에서의 문제라고 할 것이며 이러한 정보의 차이는 단지 직업이나 재산이나 기회의 차이의 문제만이 아니라 국민주권의 실질화에 역행한다고 할 것이라고 할 것이다. 그런 점에서 정보 격차의 해소는 국민주권의 실질화를 위해서 반드시 필요한 요소 중에 하나라고 생각된다. 오늘날 국민들의 진정한 자유를 위해 복지국가가 도래한 것과 마찬가지로 정보에 있어서도 통제가 아닌 정보의 복지국가적 관점에서의 정확한 정보의 제공과 기반시설의 마련이라는 의미에서의 정보국가는 의미가 있다고 보인다 결론적으로 되도록이면

6) 김문조·김종길, 전게논문, 148면.

국가의 개입은 정보의 제공과 서비스의 제공으로 국민들 스스로 판단하도록 도와주어야 하고 다만 예외적인 경우만 그것도 정치적 영역의 경우에는 더욱더 개입을 자제하고 민생이나 경제적 영역을 중심으로 행정적 규제나 형사적 규제로 대응하여야 할 것이다. 미국에서는 상업적 언론에 대해서 비상업적 언론과 동일하게 다루다가 1930년대의 경제공황을 계기로 경제적 활동으로 보아 강한 규제대상으로 되기도 하였다.[7] 따라서 정부비판적인 정치적 표현의 자유는 되도록 최대한 절대적인 수준에서 보호받아야 하고 경제관련적 표현의 자유는 민생에 미치는 영향을 중심으로 좀 더 많은 제한이 가능하다고 볼 수 있을 것이다. 이는 우리 경제가 국가신인도의 실추와 그로 인한 국민들의 삶의 커다란 충격을 경험하였고 지금도 경험하고 있는 상황에서 경제적 표현을 정치적 표현과 동일선상에서 검토하는 것은 재고의 여지가 있다고 보인다. 따라서 경제적 표현도 원칙적으로 정치적 표현 못지않게 보호되어야 하나 불특정다수인의 매우 큰 피해가 예상되는 경우에는 공익에 미치는 해악이 클 수 있기에 제한의 정도가 더 클 수 있을 것이다.

본인확인제에 대한 기술적 대안으로는 IP 추적의 방법와 ISP의 자율적 규제를 들 수 있을 것이다. 그러나 IP 추적은 법률상 규정되지 않기에 이용자의 경각심 제고의 효과가 없으며 한국적 상황에서 PC방 등에서 여러 명이 같은 PC를 이용하는 경우 IP 추적을 한 뒤 다시 게시자를 추적해야 하는 어려움이 있다.ISP의 자율적 규제로는 우선 미국과 같이 ISP의 면책을 전제로 한 '적극적 선의'(Good Samaritan)에 의한 인터넷 정화제도를 들 수 있다. 또한 ISP의 불법 콘텐츠 감시의무는 배제하지만, ISP가 호스팅한 콘텐츠의 불법을 인식하고도 고의로 방치한 경우에 그에 대한 책임 추궁 가능성을 열어두고 있는 EU의 입법적 장치와 함께, 프랑스의 FDI나 독일의 FSM과 같은 인터넷 자율규제기구의 활성화를 생각해 볼 수 있을 것이다.

---

7) Daniel E. Troy, Advertising: Not Low Value Speech, 16 Yale J.on Reg, 85, 1999.

또한 지금까지는 주로 공개된 표현의 자유와 프라이버시의 침해를 중요한 문제로 다루었다면 앞으로의 정보화사회는 정보 수집을 통한 프라이버시의 침해를 같은 비중내지는 더 큰 비중으로 검토하여야 할 것이다. 이를 위해 우리나라와 같이 법률단계에서의 규정도 필요하지만 장기적으로 헌법에서 규정하는 체계가 필요한데 유럽에서는 경제협력개발기구(OECD)와 유럽연합(EU) 등 국제기구에서는 개인정보의 국가간 유통이 활발해지면서 국제적으로 통일된 기준을 마련할 필요성이 제기됨에 따라 각각 '프라이버시 보호와 개인정보의 국가간 유통에 관한 가이드라인(1980.9.23)'과 '개인정보의 처리와 자유로운 유통에 관한 개인 정보 보호지침(1995.9.24)' 등 각종 국제규범을 마련하여 시행하고 있다. 이에 따라 이탈이아, 그리스, 스웨덴, 영국 등 EU 회원국에서는 'EU 지침'에 따라 국내법의 정비를 완료하였고, 여타 회원국에서도 국내법의 정비를 추진하였고, 현재는 2009년 12월 1일에 발효된 미니헌법이라 불리는 "리스본조약"에서 개인정보보호권을 기본권으로 격상시킨 후 유럽헌법[8]에도 이를 규정 한 바가 있는데 향후 우리의 입법례는 장기적으로 헌법에 규정하는 방향으로 가야 할 것인데 이는 사이버상의 표현의 자유는 이미 상당한 보장을 넘어서서 남용방지를 위한 책임추궁의 방안의 검토가 필요한 시점인데 반해 현재 우리나라를 포함한 상당수 국가에서 더 큰 사회적 문제를 일으키고 있는 프라이버시의 침해를 방지하기 위한 경각심내지는 예방적 효과를 거두기 위해서이다.

8) 유럽헌법 8조
① 모든 사람은 자신과 관련한 신상정보를 가진다.
② 전항의 정보는 당사자의 동의에 의해서나 법률의 근거하여 신의 성실의 원칙에 따라 처리되어야 한다. 전항의 정보는 당사들이 열람하고 정정을 요구할 수 있다.
③ 전항의 정보들은 독립기관에 의해서 관리되어야 한다.

Discussion

The right to freedom of expression and its responsibility
- Data Protection in the Constitution

CHANG, Young-Kuen
(Professor, Hongik University)

Democracy is a process of pursuing common good by a majority vote based on discourse and discussion. In order to establish this democracy, the right to freedom of expression and opinion should be secured as fundamental human rights. As a result, the right to freedom of expression and opinion can be approached from the civil rights' perspective that it can control the power of the government by positively participating in policy-making rather than from the conservative perspective in the past that the right only belongs to a personal level.

According to Habermas, the existing media became an authoritarian institution and often reflect their voice only rather than people's. However, internet is a forum for the public where everyone can raise their voice and listen to others' via the new medium such as internet news and so on. In the case of the Republic of Korea, as Habermas noted, the existing media is now a powerful institution which delivers only their opinions, exacerbating the gap between them and the public. This media could only reflect the opinion of the head of the company instead of that of people who are the ruler of the country even during political crisis. However, alternative media such as *Oh,*

My News started to create a website to communicate with people and so did the existing media companies. From the perspective of the function of the right to freedom of expression, the emergence of e-news paper enabled “the principle of popular sovereignty” in name to function in practice and the right to freedom of expression is getting enhanced. Although over reaction from the powerful to sensitive political affairs is still problematic, overall, the right to freedom of expression has been promoted and guaranteed the most in history.

In reality, multiple voices actually became heard, which contributed to the establishment of democracy. Discussing the right to freedom of expression on the internet means that understanding the right in line with the principle of self-governance based on the free market model and a broad scope of freedom of expression guaranteed by anonymity which is an important feature of the internet contributes to the golden age of freedom of expression. Regarding privacy intrusion and misuse of freedom of expression, imposing a serious responsibility may be reviewed to restore the genuine meaning of freedom of expression, however, the freedom should be guaranteed as much as possible for the public interest. At the same time, since misuse of freedom of expression should be prohibited, the scope of protection area for freedom of expression needs to be reviewed. This is because that established protection area of freedom of expression (which completely excludes child pornography) is not punishable by law. Of course, the gray area in the protection area of freedom of expression (relative protective - adult pornography) can be punished pursuant to Article 37(2) of the Constitution. However, even though some things do not belong to the protection area, it does not mean that they are all punishable. This is because that they can be resolved by disregard, tolerance, compensation by civil suit, administrative sanction and etc.

Constitutional protection area of freedom of expression means verbal or behavioral

expression by psychological and rational means. Thus, expression by irrational means cannot be protected by the Constitution. In addition, freedom of expression in this context should be exerted in order to deliver information for people's right to know. Expression actions can be categorized into "assertion" and "opinion expression". The opinion expression is considered to be basically allowed, however, an assertion cannot be protected in case it is fraud, and not be immune in principle if the assertion has defamation of character and does not contribute to the public interest even though it is true.

Even in the U.S., a country of freedom of expression, agitation remarks which provoke gangs to lynch, aggressive remarks or a genuine threat triggering violence, child pornography, defamation, fraudulent expression regarding commercial service and products, illegal expression manipulating sexual discrimination are subject to punishment. Article 1 of the United States Constitution does not intend to protect talkatives which are not regulated. However, Article 1 does protect opinions against the Government or of minority, and prohibit suppression against such comments in order to safeguard diversity which is an important advantage of democracy.

In the past, making statements condemning the Government or public servants was considered to be sedition and thus punished in England, but the punishment was restricted by law and practice later. However, nowadays, such statement which is now regarded as political freedom in the world is allowed as long as it is true and benefits the public. In case of an assertion, it should be truthful and not harm the public interest at least. However, whether or not to punish an assertion in order to prevent any harm needs a thorough review. Defamation, insult, and obscene remarks are specific examples of expression which harms the public interest and does not fall under the protection area of freedom of expression. Of course, expressing honest truth for the public interest negates illegality pursuant to Article 310 of the Criminal Act. Obscene

expression can be under the scope of freedom of expression in some countries.

Aggressive incitement specifically based on the fraudulent fact does not belong to the protection area. However, conjecture is permissible to some extent for the common good even though the assertion later turn out to be false. Violent agitation based on the fact is not always subject to punishment. There are some cases which need to be dealt with disregard or tolerance. This is because it is a subject of Article 37(2) and thus is not a subject of regulation unless it harms the public interest. It is not fair to put freedom of behavior which is not harmful to others and freedom of expression on the ground of the right to know in the same class. The protection levels of each freedom are different as well. So to speak, disseminating the fraudulent fact aiming to injure the public interest via online network does not fall under the protection area of freedom of expression, but, whether or not the punishment is overreacted restriction belong to freedom of body or general behavioral area.

However, the Constitutional Court ruled on so called “Minerba case” in relation to Article 47(1) of the Framework Act on Telecommunications that “it is not likely that certain expression is automatically excluded from the protection area of freedom of expression only because the expression is one of specific categories, ‘expression of false fact’ is also under the umbrella of freedom of speech and publication which is enshrined in Article 21 of the Constitution. However, it can be limited by Article 37(2).” It seems that they regard expression of false fact as freedom of expression, however, in my opinion, this is an error. It is against the role of the Constitutional Court which should protect the right as a result of confusion of the right and misuse of the right. In case of vague truth, it should be deemed as a truthful fact.

Speaking of whether or not pornographic expression belongs to the protection area of freedom of expression, recognizing it as freedom of expression is far too progressive

considering it that pornography is not protective freedom of expression in the U.S. where pornography is allowed.

The fact that a free market of thoughts is more meaningful today is related to resolving the “digital divide”. In other words, by promoting freedom of expression, more useful information will be provided by the private sector as well as the public sector, which means a free market of thoughts plays a key role these days. The reason why incidents such as “Minerba case” happened is that important information is monopolized by the Government and a natural person tried to release it. Taking it into consideration, an on-line free market of thoughts will be expanded and it should be safeguarded unless it harms the common good.

However, it is not always right that the Government takes a laissez-faire policy because the “digital divide” is a matter of popular sovereignty as it contains issues of the right to know and informational welfare. In this regard, the “digital divide” should be resolved in order to realize the principle of popular sovereignty. Today, as welfare was introduced for the genuine freedom of people, the delivery of accurate information and establishment of infrastructure are meaningful from the perspective of informational welfare country. In conclusion, Government’s intervention should be limited within provision of information and service, and administrative or criminal regulations. In the U.S., commercial media and non-commercial media were treated equally but in 1930, after the Great Depression, commercial media started to be controlled strongly. Therefore, political critics should be protected to the most possible extent while freedom of expression related to business activities can be more restricted. Noting that our economy suffered from sovereign credit rating drop and its severe aftermath, expression of economic opinions and that of political ones need different consideration. Therefore, even though expression of economic opinions should be protected, the

restriction on that could be heavier when foreseeable damage to the public is expected.

Alternative technology to an identification system has two options such as IP tracking and ISP Self-Regulation. However, IP tracking is not regulated by law which does not help alert users to its risk and it is not useful in Korea where many people share the same IP at an internet cafe. As an example of ISP Self-Regulation, there is internet purification system by the Good Samaritan on the assumption of ISP immunity in the U.S. Furthermore, vitalizing internet self-regulation organizations such as FDI in France and FSM in Germany can be another option as well as EU's legislation which spells out ISP's responsibility to delete illegal contents as soon as it recognizes their existence on the website while ISP is not liable for monitoring such contents.

So far, publicized freedom of expression and intrusion of privacy have been an issue, but in the future, intrusion of information by collection of information will become a bigger problem. In this regard, a legislative system in the Constitution regulation such act will be needed in Korea. Internationally, OECD adopted Guidelines on the Protection of Privacy and Transborder Flow of Personal Data (November 23, 1980) and EU the Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (November 24, 1995). In this regard, EU Member States such as Italy, Greece, Sweden and England reformed their domestic legislation and others are following them. At present, after the Treaty of Lisbon has promoted the right to privacy to basic human rights, the Treaty establishing a Constitution for Europe also stipulated it. In the future, it is necessary for Korea to follow the precedent in order to prevent intrusion of privacy.

Discussion

- Professor Wolfgang Benedek

Wolfgang Benedek

(Professor at the Faculty of Law at Graz University)

토론

- Wolfgang Benedek 교수

Wolfgang Benedek

(Graz University 교수)

Discussion

Human Rights and the Internet

Andrew Puddephatt

(Director of Global Partners)

The growth and development of digital communications is one of the most important phenomena of the last decade of the 20th Century and the first decade of the 21st Century. In simple terms, the digitalisation of information – whether words, music or pictures - and the ability to access that information through a variety of devices, from the personal computer to the television to the mobile phone, have created a networked communications environment that represents a scale of change comparable to Gutenberg's invention of the printing press. For the first time in history, human beings with access to the digital world can reach almost infinite amounts of content of all kinds. Barriers that previously restricted communication are being broken down. These include the need to have access to an expensive printing press, permission to use broadcast spectrum, and, with the spread of broadband internet, bandwidth limitations.

Digital communications have also transformed social activism through the use of websites, e-mails, social networking platforms and mobile phones in ways that would have been inconceivable even a few years previously. Communications used to be slow

and expensive. For example, it might have cost upwards of $100 to make an international telephone call in the middle of the 20th Century. Now mobile phone and e-mail communications have dramatically reduced costs, and have almost ubiquitous reach. The implications of the emergence of digital networked communications are far more radical than previous developments in communications technology, such as the evolution of cinema film into video. Digital communications are creating new opportunities for collaboration, publishing, mobilisation and observation. Whilst the same technologies can assist criminals, paedophiles and terrorists to work together more effectively, and create new opportunities for authoritarian governments to control dissent, the potential to empower people across the world cannot be denied.

Communication is fundamental to human society. Indeed, it is impossible to conceive of human society existing without communication. From a human rights perspective there are three generally accepted reasons why communication is vital:

- It is a human need to be ourselves and have our own identity, and expressing ourselves through communication is how we experience our own humanity. In this sense, communication is essential to our human integrity.
- It is the foundation for other rights and freedoms. Without the ability to communicate it is impossible to realise or defend human rights, or organise politically in any meaningful way.
- More recently economists such as Amartya Sen have argued that communication is the pre condition of social and economic development[1].

1) See for example Dreze and Sen (1987)

In order to communicate with a wider range of people beyond face to face conversation, we need communication tools or platforms. For example, we can use a megaphone to amplify a human voice, and a cave painting or wall poster can be seen by many people even when the creator is not physically present. A newspaper or radio or TV transmitter reaches even further. All of these communication platforms - whether cave paintings, wall posters, books, print or broadcast, - use a model of communication that we might call *"one to many"*, in which there is a source of production of content that is then distributed to a wider audience. In the past, the focus of human rights activity has been on the source of that content and the ability of that source - journalist, artist or publisher - to communicate free of censorship.

However, the growth of digital communication has changed this model dramatically. As the costs of connecting to the internet decrease across the world[2], the start-up costs for a digital media platform such as a blog similarly decrease. Content is being produced, shared, edited, re edited and moderated by a growing community of online actors. This new model of communication can be described as ***"peer to peer",*** in which the creation and sharing of content is distributed among many people who are simultaneously and directly communicating using digital platforms that can be accessed via a broad range of devices (from mobile phone to computer, TV or radio).

Peer to peer networks have a number of characteristics that make them different to conventional one to many communication models. They are not controlled so easily, or

2) Between 2008 and 2009 the cost of ICT services dropped in all of the 161 countries included in the International Telecommunication Union's analysis of affordability (ITU, 2010, 5). Costs of mobile phone and internet services fell on average 15%. However, it should be noted that significant "digital divides" in access and affordability persist at international and local levels. On average, high speed internet connections cost 500% of the average monthly GNI per capita in Africa (ibid, 8).

in the same ways, as offline media, meaning that both conventional censorship mechanisms and editorial standards are hard to apply. The model facilitates the production of large amounts of content, and we are increasingly dependent on applications and intermediaries of various kinds to arrange and curate that content, such as search engines. Users of digital communications have a much greater choice of content and impact upon the ways that it is presented and accessed than radio and newspaper audiences.

It is not that "one to many" models of communication are dying out (although increasingly some traditional media, such as newspapers in the most developed markets are finding a sustainable economic model increasingly difficult) but that they are challenged and are being mutated by "peer to peer" forms of collaboration. The news media have historically responded to long term trends in its audience but now it has to foster continual communication with its audience. The more progressive media companies are becoming increasingly interactive, encouraging audiences to communicate with news producers through the use of mobile phones and cameras, texting, and email. Consumers of news want to be producers, and user generated content is appearing on social networking sites, and from there migrating into traditional media outlets.

Because of these trends, traditional journalism has to be more "consumer-led" than in the past; it has to respond to what consumers want or lose their attention. Whereas the human right to freedom of expression has been in the hands of elites for much of human history – writers, journalists, editors and publishers battling with governments and with each other – it is now increasingly democratised, and placed in the hands of

the public for safe keeping. We can now bypass gatekeepers and communicate directly with each other.

This is a big challenge for human rights groups. In the past, few human rights activists worried about the technology that delivered the content – their concern was whether content had been censored in any way. After all who cared where the newsprint came from or what type of camera was used to film a demonstration? But in the digital world, content that is available is often reshaped by the technology. Equipment that provides network access can also be used to block access to sites for political reasons. Search engines that provide access to information can be programmed to exclude information unpalatable to the authorities. Mobile phone technology that is used to provide maps and navigation services to the user can also be used by hostile governments to monitor and track citizens. Human rights advocates and defenders therefore need to think about applying human rights standards and values to the whole communication environment, rather than just to the content as they did previously.

1. The digital challenge

The modern, digital communications environment can best be understood using a "layer" model (see below). At each layer there are different actors, different policy challenges and different interests.

For human rights groups there will be policy issues at each level.

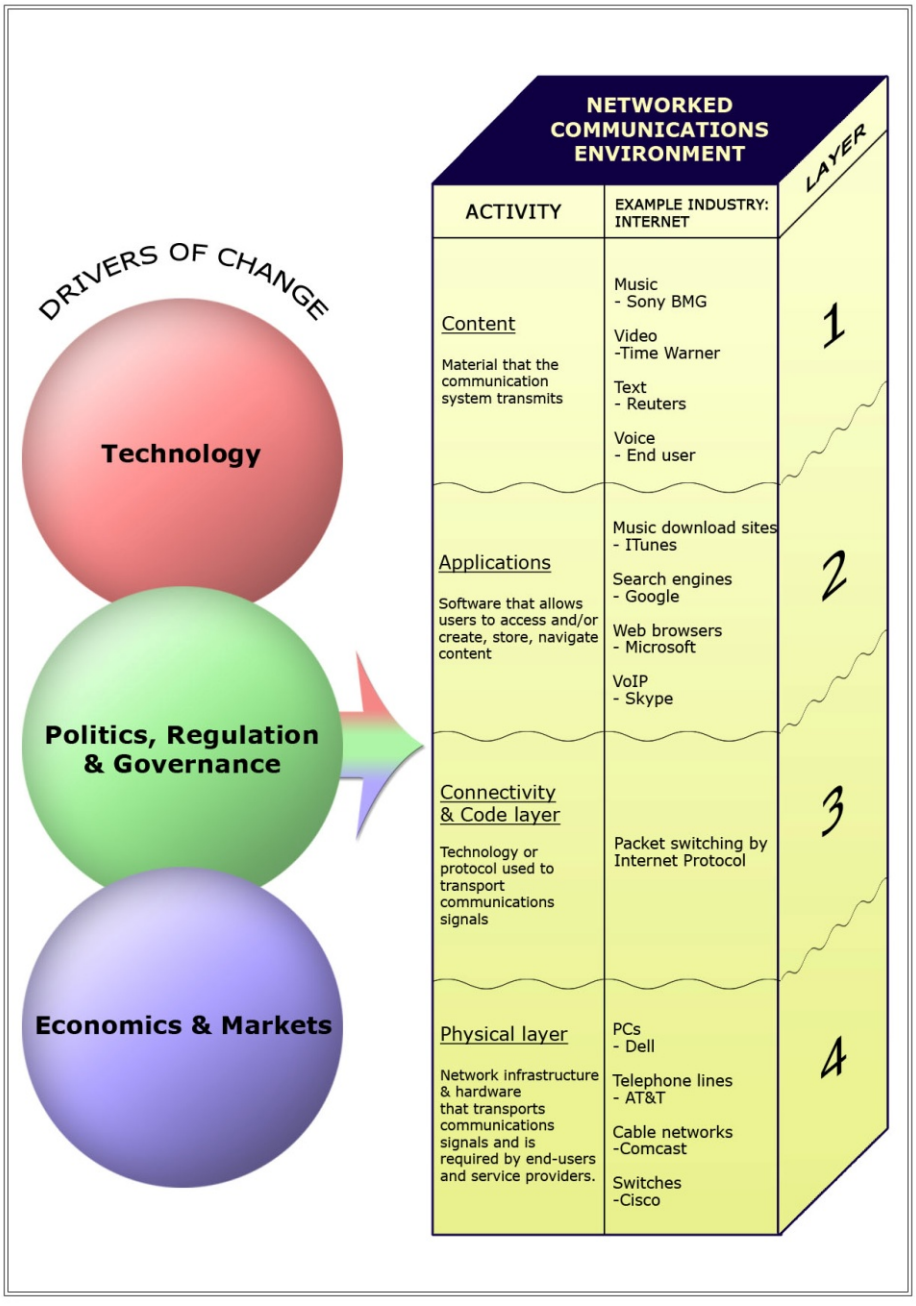
- At the content level there will be a focus upon direct censorship, whether by legal or normative means; copyright is increasingly emerging as a human rights

issue where content companies seek to impose punitive conditions upon intermediaries who make available content.

- At the application level, privacy is emerging as a major issue, with the question of who owns the personal data that companies like Google harvest to support their business model. About 80% of the data held online is unstructured – notes, photos, etc but as new techniques are developed to harvest that "big data" it will become a increasingly valuable and sought after resource – the oil of the C21st.
- At the connectivity level there are a range of issues including about whether the networks should all treat all Internet traffic equally, without discrimination. At its broadest this network neutrality would prevent restrictions on content, sites, platforms, types of equipment that may be attached, and modes of communication. For human rights, the most open and least selective environment offers the most possibilities for change.
- Finally, at the level of infrastructure there are issues to do with affordable and equitable access and whether or how the world's poor will be able to come online.

A complication is that at each level corporate and government interest varies. Governments which promote internet freedom may also push for tough copyright laws. Companies that oppose copyright (like Google) will be fierce opponents of attempts to protect personal privacy. While application companies (such as Google or Facebook) can be located out of jurisdiction, connectivity and infrastructure companies such as Vodafone or Nokia-Siemens are based in a local national jurisdiction and are vulnerable to a different set of pressures, as we saw in Egypt and Iran. Advocacy needs to be sophisticated and nuanced.

However, human rights principles operate across all the layers.



In defending internet freedom, in the broadest sense, we face particular challenges and opportunities.

2. Weakness of human rights voice

As set out above, human rights groups are facing a range of challenges across the world – from legal attacks to resource and capacity problems and to the fact that many younger activists prefer to operate in a mobile, unorganised manner, aided by smart digital technologies. These problems are highlighted in the digital sphere, by the disconnect between "tekkie" activists and the human rights world.

The Internet was built by libertarian engineers who saw policy as irrelevant or as a constraint. But under pressure from governments' desire to regulate and control the Internet and companies wishing to dominate it economically those early libertarian assumptions have collapsed. Unless the Internet is shaped by human rights values and principles we will lose its liberating, mobilising and organising potential and it will become another passive communications medium, a form of global cable television.

But the tech community rarely sees the need to reach out to the human rights community and are often hostile to an attempt to articulate a human rights approach. The human rights movement in turn does not generally understand policy issues or is unable to understand how the various "technical" issues have a significant human rights dimension. As a result civil society advocacy is weak and uncoordinated and there are divisions between human rights and digital activists. Moreover, where many human rights NGOs are used to dealing with governments on a zero-sum basis, as the enemy, in this field it is necessary to have a more nuanced relationship where they are both allies and opponents. This requires an ongoing, intelligent conversation in which we deploy a high level of advocacy skills. It is particularly important to develop these new capacities and alliances in the global south and not just the global north given the shift in geo-political power.

3. Divisions between global north and global south

There's an emerging tension between parts of the global north on Internet governance between countries in the global south – not just repressive anti-democrats but democracies such as Brazil, South Africa and India (IBSA) – which is also reflected in civil society and which is exacerbated by US commercial dominance of the Internet. The "governance" of the net is dispersed between administrative and engineering functional bodies (ICANN, IETF, http and html working parties) but many governments see this as a mask for US commercial interests or as an unacceptably uncontrolled environment. Some governments, with some civil society support, are pushing for state control of the Internet. While superficially attractive to some, state control is likely to lead much greater regulation of content, heavy restrictions upon applications (we're already seeing this throughout the world), limitations on connectivity to create "national" internets that shut domestic users off from the wider global community and infrastructure development that favours wealthy elites rather than the poor. This makes developing human rights capacity in the global south, and effective global alliance building, a necessity.

4. Engaging governments and the corporate sector

An increasing number of governments across the world are taking hostile positions to Internet freedom, even those active in promoting it externally. In turn they are exerting pressure on companies to limit access to content – effectively privatizing control and censorship. While a few application companies based in US are willing to promote internet freedom (as we saw with Wikipedia and other websites going dark in response to the recent Stop Online Piracy Act) the vast majority that deliver connectivity or

infrastructure – from telecommunications such as ATT, Verizon, Vodafone (Egypt being a good example) Telefonica or France Telecom providers to network companies such as Nokia Siemens network (who provided mobile phone networks to Iran) require a local legal registration and are more vulnerable to pressure. There's a need find ways to bring companies onboard to a realistic strategy to defend Internet freedom.

The Opportunity

5. Creating coordinated human rights advocacy

Over the past few years there is a growing awareness of the importance of bringing a human rights dimension into the communications debate as well as understanding the implications of digital communications for the human rights movement itself. What is needed is to:

- Demonstrate the human rights implications of the various digital communications issues (set out in the layer model)
- Demonstrate the value of the human rights frame in keeping the internet free
- Stocktake current human rights capacity in each region on these issues
- Build a shared understanding of new skills and capacities that are available to the human rights movement
- Identify the current needs and potential for advocacy – information sharing, messaging, common action
- Build a human rights constituency to act in global policy forums.

6. Promoting positive values in global forums

The internet is not governed in a conventional sense – there is no treaty for the internet and no ruling body. Governance is functional – problems are fixed by groups of engineers and technologists working together. The analogy is with car mechanics – they are only concerned with whether the car works, not where it is driven. Those international policy forums that look at the internet – including the UN Internet Governance Forum, the Council of Europe and the Organisation of for Economic Cooperation are not rule making; they drive and shape standards, values and guidance on best practice. This is linked to the growth of multi stakeholder working, bringing together government, business and civil society to collaborate, share information and exchange best practice. It is not just human rights groups who are part of this exchange but civil society activists from different disciplines such as education, health, digital activists etc.

Governments are seeking greater control over the internet because of its increased importance to economy and society. In the past couple of years this trend has become even more dominant with increasing numbers of governments seeking to minimize the role of multistakeholder participation. Most civil society organisations active in this field (e.g. APC, CDT, EFF,[3])along with governments such as the US, Sweden, the UK, Kenya, Ghana and Japan argue that the multi stakeholder system of policy making which is light touch, committed to maintaining the openness of the environment and avoiding government control offers the best opportunities for civil society and human rights groups to participate and shape policy. In addition, given that the private sector

3) Association of Progressive Communications, Center for Democracy and Technology, the Electronic Frontier Foundation

controls much of the infrastructure of the Internet in fast paced world, effective governmental oversight maybe difficult or impossible to achieve.

To offset the drive for regulation a recognisable trend in recent years has been the proliferation of sets of principles which act as normative values designed shape behaviour and expectations on the internet. Examples include:

- The OECD principles for internet policy making – currently a communiqué has been issued and is likely to become a recommendation (equivalent to soft law for signatory countries);
- The Council of Europe's broad Declaration of Guiding Principles for Internet Governance. This needs to be approved by Ministerial Committee which meets in early September;
- Civil society groups have adopted the Internet Rights and Principles Charter of Human Rights and Principles for the Internet – endorsed by some businesses and governments (copy attached). Other examples of NGO initiatives include the Association for Progressive Communications Internet Charter and the Global Network Initiative Principles, which have support from three large application companies, and some NGOs.

Principles such as these are better suited than hard law to the internet because they are more flexible (they allow for different national regulatory regimes; fast changing technology; cross-border issues etc.). They also help define what standards should be upheld in Internet governance as an advocacy, campaigning or information sharing tool and are particularly driven by a need to define what human rights mean in the context

of the internet. One of the main thrusts of argument has been that it is necessary to preserve the openness of the public space in the digital world and to base the framework for the internet upon the protections offered by universally agreed covenants on the exercise of human rights in the physical world. The purpose of declaratory principles such as those above – and particularly the Internet Rights and Principles Charter of Human Rights and Principles for the Internet is to apply existing human rights norms and values to the online world. It is also based on a recognition that big business and certain governments are seeking to limit those freedoms.

These various initiatives underline the importance of seeing human rights as a framing for thinking about digital communications issues, and as a way of analysing the obstacles.

7. Strengthening alliances with companies and users

We are fortunate there is an alignment between some corporate interests and Internet freedom (though there are also contradictions and tensions to be managed at different layers). What the campaign against US intellectual property legislation SOPA showed was that the real power on the internet comes from the millions of users. If mobilised, selectively and when necessary, this mass opinion represents tremendous force that can promote human rights. Some companies played an crucial role along side civil society in mobilising opposition to the act which would have had severe global consequences.

Our goal with companies should be twofold: -

- To encourage them to fulfil their human rights responsibilities as corporate entities (using the Ruggie framework as a baseline)
- To encourage them to take appropriate steps to empower their users to defend human rights online

This would mean promoting application of Ruggie framework to communication companies and engaging with key platform companies able to mobile user support for internet freedom (as with SOPA) to see how such support can be ongoing.

Conclusion

How might we summarise the range of human right policy issues that need to be considered. Diagrammatically and using the layer model a representation of this might be as follows:

Figure 2 –Policy principles for each communications layer in the networked environment.

COMMUNICATIONS PLATFORMS

CONTENT LAYER

a) The right to freedom of expression should be protected. The expansive definition of Article 19 of the ICCPR should be used which includes positive rights and associated responsibilities.
b) The range of content available should be diverse, representing the whole spectrum of cultures, interests and knowledge.
c) The objective of intellectual property and licensing agreements should be to balance respect for the rights of creators with the need for maximal creativity and innovation.

APPLICATIONS LAYER

a) Gatekeepers of content should be transparent about the norms and protocols used to select content.
b) Service providers should not be held liable for content they help users access.
c) Companies and organisations with access to user data should adhere to transparent privacy policies that protect privacy rights as established in international human rights law.
d) People should have access to the means of developing new applications tailored to meet specific needs, for example through open source software development.

CONNECTIVITY AND CODE LAYER

a) Communications infrastructure and protocols should be interoperable whenever possible.
b) Protocols governing access to public content should enable access for all people who want and need it.
c) Networks should be 'neutral' in the sense that the flow of content should not be subject to undue or arbitrary discrimination for monetary, cultural or political reasons. Controls should not be embedded in networks themselves.

PHYSICAL LAYER

a) All people should have affordable and equitable access to the means of receiving and disseminating opinion, information and culture.
b) Regulation to achieve equitable access should be tailored to local conditions and should be flexible, subject to ongoing evaluation and review.

If the internet were to reflect these values, we would have made significant progress. The internet has transformed the scope of human rights work. Even in the most repressive regimes it is now possible to find information about human rights concerns even though conventional media are prevented from carrying such news. The globalised nature of the environment means there is now a global information environment. One hundred years ago, most horizons were local - now access to information exists on a scale unparalleled in history and with it the potential for global mobilisation. We are reaching a world where governments cannot commit human rights abuses on a significant scale in secret.

Furthermore, the internet facilitates new kinds of connections. People can create, edit, and share information and ideas with each other and with a wider audience. People can have low cost instantaneous communications with individuals all over the world, and these communications are much more resistant to government and private surveillance. Whereas in the past, freedom of expression lay in the hands of elites – governments, publishers, editors, journalists, now anyone can express themselves in the public domain. This amounts to the democratisation of freedom of expression, taking it out of the hands of elites and placing it in the hands of ordinary people.

토론

인권과 인터넷

Andrew Puddephatt
(Director of Global Partners)

지난 20세기와 21세기 동안 일어난 가장 혁명적인 발달은 디지털 통신이다. 간단히 말하자면 글, 음악, 사진 등 디지털화된 정보들과 그러한 정보들에게 접근할 수 있는 개인 컴퓨터, 휴대폰, 텔레비전 등 다양한 매개체들이 통신망으로 연결된 커뮤니케이션 환경에 마치 구텐베르크(Gutenberg)의 인쇄기와 같이 거대한 변화를 일으킨 것이다. 역사상 처음으로 인류는 디지털 시대를 맞이하여 무한한 정보를 접할 수 있게 되었다. 이로써 과거에 존재했던 통신의 장벽들은 허물어지고 있다.

디지털 통신은 웹사이트, 전자우편, 소셜 네트워크, 그리고 불과 몇 년 만에 크게 발달한 휴대폰 등을 통하여 사회 운동에도 개혁을 일으켰다. 과거 통신은 느리고 비용이 많이 들었다. 예를 들어, 20세기 중반까지만 해도 국제전화 한 통의 요금은 100달러를 웃돌았다. 현재 휴대폰과 전자우편 등 보편화된 통신수단들이 이러한 비용을 크게 줄였다. 디지털 통신은 협력, 출판, 이동성, 그리고 감시 등의 전에 없던 새로운 기회를 제공해주고 있다. 한편, 이러한 새로운 발전은 테러리스트 조직, 소아성애자 등의 범죄자들에게 역시 도움이 되는 실정이며 정부가 시민들의 반정부 활동을 억압할 수 있도록 도움을 주고 있다는 것도 무시할 수 없다.

의사소통은 인간 사회에 있어서 핵심적이다. 의사소통이 없었다면 인간사회는 존재하지 못했을 것이다. 인권의 관점에서 바라볼 때 의사소통은 다음과 같은 세 가지 이유에서 필수적이라고 볼 수 있다.

- 의사소통은 사람이 자기 자신이 되기 위해 기본적으로 필요한 것이며 자신의 정체성을 갖기 위해서 필수적이다. 우리는 의사소통을 통해 우리의 정체성과 우리의 경험을 표현할 수 있다. 이러한 관점에서 보면 의사소통은 온전한 사람됨에 필수적이다.
- 의사소통은 다른 권리들과 자유의 기반이다. 의사소통 없이 인권을 수호할 수도, 의미 있는 어떠한 정치적 활동도 할 수가 없다.
- 최근 아마티아 센(Amartya Sen)과 같은 경제학자들은 의사소통은 사회와 경제 발전에 있어 전제조건이라고 여긴다.

마주보고 하는 대화 그 이상의 의사소통을 위해서 우린 통신수단들이나 플랫폼이 필요하다. 예를 들어, 우리는 더 많은 사람들이 목소리를 들을 수 있도록 확성기를 쓸 수 있고, 창조자가 비록 더 이상 존재하지 않더라도 그가 남긴 동굴의 벽화 등의 작품을 볼 수 있다. 신문, 라디오, 텔레비전 등의 매개체를 통하면 더 많고 넓은 세상과 의사소통이 가능하다. 동굴벽화, 벽보, 책, 인쇄물 또는 방송 등 종류와 상관없이 이러한 모든 플랫폼들은 “하나에서 다수 (one to many)” 라는 모델의 의사소통이라고 할 수 있다. 즉, 하나의 생산의 원천을 다수의 관중에게 유통시키는 형태인 것이다. 과거의 인권활동의 관심은 기자, 예술가 그리고 출판사 등 컨텐츠 생산자가 과연 검열을 통하지 않고 자유롭게 의견을 표명할 수 있는가였다.

그러나, 디지털 통신의 성장으로 인해 이러한 모델에는 극적인 변화가 왔다. 전 세계적으로 인터넷 접속 비용이 줄어들면서, 블로그 등 새로운 신규 디지털 미디어 플랫폼

을 만드는 비용 역시 줄었다. 그 속에서 컨텐츠들은 생성되고, 나누어지고, 편집되고, 다시 편집되고, 중화되어 간다. 이러한 새로운 의사소통 모델은 "피어투피어 (peer to peer)" 모델 이라고 불린다. 이것은 다수의 사람들이 컴퓨터 또는 휴대폰을 이용해 온라인 공간에서 지속적으로 그리고 직접적으로 의사소통 하는 형태를 말한다.

"피어투피어" 모델은 "하나에서 다수" 모델과 여러 면에서 다르다. "피어투피어" 모델의 네트워크들은 쉽게 통제되지 않는다. 즉, 전통적인 검열도구나 편집 기준이 쉽게 적용되지 않는 것이다. 이 모델은 다량을 정보를 생산할 수 있게 해주며, 우리는 급속도로 어플리케이션, 검색 엔진 등에 의존해가고 있다. 라디오나 신문 등의 미디어에 비해 온라인을 이용하는 이용자들은 훨씬 더 다양한 정보와 접할 수 있고 정보들 역시 다양한 형태와 큰 영향력을 갖추고 있다.

이것은 "하나에서 다수" 모델의 커뮤니케이션이 도태되어 간다는 뜻은 아니라 "피어투피어" 모델에 의해 도전받고 있으며 그것과 협동하기 위하여 형태가 바뀌어 가는 것이다. (다만 신문 등의 전통 미디어는 경제적인 성장에 있어서 어려움을 겪고 있다.) 뉴스 미디어는 본래 시청자들 사이에서 오래도록 주목 받아오는 이슈들에 반응을 하는 형태였지만 이제 뉴스 미디어는 계속해서 시청자들과 의사소통을 하는 매체로 성장하고 있다. 미디어 회사들이 더욱 발전할수록 그들은 더욱 더 쌍방상호적으로 변해가고 있다. 더욱 진보적인 방송국들은 시청자들이 휴대폰, 카메라, 문자, 전자우편 등 다양한 매체를 통하여 뉴스 프로듀서들과 소통할 것을 격려한다. 소비자들은 프로듀서가 되길 원하고 이러한 이용자들은 정보를 풍부하게 활성화시키며 과거의 미디어로부터 벗어나고 있다.

이러한 추세에 의해 전통적 저널리즘은 이제 보다 "소비자 주도형"이 되어가고 있다. 이들은 소비자의 의견에 대응하며 그렇지 못한 경우 더 이상의 관심을 끌

수 없다. 지난 역사 속에서 소수의 엘리트들 즉 정치가, 기자, 출판사들이 서로 투쟁했다면 이제는 점점 더 민주화 되어 시민들 역시 자유롭고 적극적으로 참여할 수 있게 되었다. 이제 우리는 문지기들을 바로 지나쳐서 직접적으로 서로 의사소통 할 수 있게 된 것 이다.

이는 인권 단체들에게 커다란 도전 과제이다. 과거에는 몇몇의 인권 활동가들만이 통신기술에 의해 의사소통이 검열되는 것에 대해 염려해왔다. 어쨌든 누가 신문이 어디서 인쇄되어 왔는지 어떠한 카메라와 필름이 사용되었는지 궁금해 하였겠는가? 하지만 디지털 시대에서는 유효한 정보가 기술에 의해 그 모양이 규정된다. 네트워크 접근권을 확보하는 기술은 정치적인 이유 등으로 그러한 접근권을 봉쇄하는 데에도 쓰여진다. 정보를 제공하는 데에 쓰여지는 검색 엔진은 권력자들(정부)의 구미에 맞지 않을 경우 그 정보들이 차단할 수도 있다. 휴대폰의 지도와 네비게이션 기능은 유용한 반면 정부로 하여금 시민들을 모니터하고 추적하는 형태로도 쓰여질 수 있다. 인권 옹호자들과 인권 운동가들은 이러한 현대 통신사회에 그에 맞는 인권 기준을 마련하는 것이 중요하다고 생각하는 바이다.

1. 디지털 도전과제

현대의 디지털 커뮤니케이션 환경은 “단층”모델로써 (영문 원고 참고) 설명할 수 있다. 각각의 층에는 다른 행위자, 다른 정책집행의 어려움, 다른 이익들이 있다.

인권 단체들에게는 각 단계에서 다음과 같은 정책 논의점들이 있다.

- 컨텐츠 레벨에서는, 법적 혹은 규범적인 방법으로 직접적인 감시하는 것에 초점이 맞춰질 것이다. 저작권이 인권 이슈로 떠오르면서 컨텐츠 회사는 컨텐츠를 이용가능하게 하는 중개자들에게 징벌적 조건을 부과하려고 한다.

- 적용 단계에서는, 프라이버시가 주요 이슈로 떠오르며 구글과 같은 회사들이 자신들의 사업 모델을 지지하기 위해 수집한 개인정보의 소유자는 누구인가라는 문제가 있다. 온라인상 개인 정보의 약 80%가 체계적으로 관리되고 있지 않다. 개인적인 글, 사진 하지만 새로운 기술이 발전함에 따라 그와 같인 "빅 데이터"를 수집하는 것이 더욱 중요해지고 자원을 캐는 것과 같아서 데이터 수집은 21세기의 석유와 같을 것이다.

- 접속 가능성 단계에서는, 네트워크가 모든 인터넷 트래픽을 동등하게 대해야 할 것인가 하는 이슈가 있다. 최대의 네트워크 중립화는 컨텐츠, 싸이트, 플랫폼, 그에 부착된 도구들, 커뮤니케이션 방법들에 대한 제한을 방지할 것이다. 인권을 위해서는, 가장 개방되고 비차별적인 환경이 변화의 가능성을 가장 높인다.

- 마지막으로, 기반시설 단계에서는, 감당할 수 있는 비용으로 형평성 있는 인터넷 접근, 즉, 세계의 빈곤층이 인터넷을 이용할 수 있는지, 혹은 어떻게 그러할 수 있는지에 대한 이슈가 있다.

각각의 단계에서 기업과 정부의 이해관계가 다르다. 인터넷 자유를 추구하는 정부는 강력한 저작권 법을 밀어부칠 것이다. 구글과 같이 저작권에 반대하는 기업들은 개인 사생활을 보호하려고 하는 시도에 격렬히 반대할 것이다. 어플리케이션 회사들 (구글이나 페이스북과 같은) 사법영역과 접속 가능성 영역외에 위치할 수 있을 것이다. 그리고 보다폰과 노키아-시멘스와 같은 사회기반 회사들은 국내 사법관할권에 있으며 이집트와 이란에서 보았듯이 다른 압력주체들에 취약하다. 이들을 옹호하는 것은 정교해야 할 것이다. <표 참조>

그러나 인권 원칙들은 모든 영역에 거쳐 작동한다. 인터넷 자유를 보호하는 데, 우리는 특정한 도전과제들과 기회를 직면한다.

2. 인권 옹호 목소리의 취약점

이전에 기술하였듯이, 인권 그룹들은 전 세계적으로 다양한 도전과제들을 직면하고 있다. 재원, 역량 문제에 대한 법적 공격으로부터 많은 어린 활동가들이 핸드폰과 같은 스마트 디지털 기기로 체계없이 활동한다는 사실에까지 어려움은 다양하다. 이러한 문제들은 디지털 기기를 능숙하게 다루는 활동가들과 인권 세계의 단절로써 디지털 공간에서 부각되었다.

인터넷은 정책이 제약이라고 생각하는 자유주의자인 엔지니어들에 의해 세워졌다. 그러나 인터넷을 통제하고 싶어하는 정부와 그리고 경제적으로 인터넷을 지배하고 싶어하는 기업들의 압력하에, 이러한 자유주의자들의 가정은 무너졌다. 인터넷이 인권 가치와 원칙에 의해 모양이 갖춰지지 않는 이상, 우리는 잠재력을 자유롭게 하고, 이동하고 체계화하는 것을 잃어버리게 될 것이다. 그리고 인터넷은 세계의 케이블 티비처럼 또 다른 수동적인 커뮤니케이션 도구로 전락할 것이다.

그러나 기술 집단은 인권 단체들에게 손 내밀 필요를 느끼지 못 하고 종종 인권적 접근을 표현하는 것을 적대시한다. 인권 운동은 차례로 대체적으로 정책적 눈의점을 이해하지 못 하고 어떻게 다양한 “기술적” 이슈들에 중요한 인권 측면이 있는지 이해할 수 없다. 결과적으로 시민 사회 운동가들은 약하고 조직적이지 못하며 인권과 디지털 활동가들 사이에 차이가 생겼다. 더욱이, 과거에 많은 인권 시민단체들이 정부들과 제로썸 기반에서 대립하던 것에 익숙했던 것에 비해, 시민단체들은 적군으로써, 이 분야에서는 조금 더 미묘한 관계, 즉, 인권 단체와 정부 사이가 연합군이기도 하고 적군이기도 한 관계를 형성할 필요성이 있다. 이것은 우리가 수준 높은 인권옹호 기술을 적용해야 하는 아직도 진행중인 지적인 대화를 필요로 한다. 이것은 특히 저개발국가들이 새로운 역량과 연합을 발전시키는데 중요하며 선진국이 그저 지역-정치적 권력을 넘겨주는 것이 아니다.

3. 선진국과 저개발국가의 차이

인터넷 거버넌스에 대해 선진국과 저개발국에서 긴장관계가 조성되고 있다. 이 긴장관계는 억압적인 반민주주의 국가뿐만 아니라 브라질, 남아프리카와 인도와 같은 민주주의 국가와 선진국 사이에서도 일어난다. 이것은 시민 사회에 반영되며 미국의 인터넷의 상업적 지배에 의해 더욱 악화된다. 인터넷의 "거버넌스"는 행정적 그리고 기술적 단체 (ICANN, IEFT, http and html 사업단체들) 사이에 분산되었다. 하지만 많은 정부는 이것을 미국의 상업적 이익의 가면으로 보거나 받아들이기 힘든 규제되지 않은 환경이라고 받아들인다. 어떤 정부들은, 몇몇 시민 사회의 지원과 함께, 인터넷에 대한 정부의 규제를 요구한다. 어떤 이들에게는 피상적으로 매력적일지 모르나, 정부 규제는 훨씬 더 심한 컨텐츠 단속, 어플리케이션에 대한 심각한 규제, (우리는 이것을 이미 전 세계적으로 목격하였다.) 국내 사용자들로 하여금 더 넓은 전 세계 커뮤니티로의 접속을 차단하여 인터넷을 "국내용"으로 만드는 연결성에 대한 제한, 그리고 저소득층보다는 부유한 엘리트층에게 혜택을 주는 기반시설 발전을 야기할 것이다. 이것은 저개발국가들 사이의 인권 역량 강화와 효과적인 전 세계 연합을 필요한 것으로 만든다.

4. 정부와 기업 영역에 관계하기

전 세계적으로 점점 더 많은 정부들이 인터넷 자유에 대해 적대적인 입장을 취하고 있다. 외부적으로는 그것을 옹호하는 것처럼 보이는 국가들 역시 그러하다. 차례로, 그들은 효과적으로 규제와 감시의 기능을 민영화함으로써 민간기업들로 하여금 컨텐츠 차단을 하도록 압력을 행사한다. 미국 내 어플리케이션 회사들 몇 개가 인터넷 자유를 지지하는 가운데 (최근 온라인 저작권 침해 금지 법안에 반발하여 위키피디아와 다른 웹싸이트들이 접속되지 않는 것을 우리는 목격하였다.) 대부분의 회사들 - ATT, Verizon, Vodafone (이집트가 좋은 예이다) Telefonica 혹은

프랑스 텔레콤 서비스회사에서 노키아 시멘스 네트워크 (핸드폰 통신망을 이란에 공급하였다) 와 같은 통신망 회사들에게 접속망과 기반시설을 제공하는 민간기업들 - 은 국내 법적 등록을 요구하고 압력에 더욱 취약한다. 인터넷 자유를 수호하기 위해 기업들이 현실적인 전략을 찾을 필요가 있다.

기회

5. 조화로운 인권 보호 창조

지난 몇 년간, 인권적인 측면을 통신에 대한 논의에 끌어오는 것과 인권 운동에 디지털 통신이 갖는 의미를 이해하는 것이 얼마나 중요한가에 대한 인식이 높아졌다. 이를 위해서는 다음과 같은 것이 필요하다.

- 다양한 디지털 커뮤니케이션 이슈에서 인권이 갖는 의미를 보여주는 것 (단층 모델에 나와 있다)
- 인터넷을 자유롭게 두기 위해 인권적인 틀이 가지는 의미를 보여주는 것
- 이러한 이슈들에 대해 각 지역에서 현재 인권 역량을 축적하는 것
- 인권운동에 이용할 수 있는 새로운 기술과 역량에 대한 공통된 이해를 쌓는 것
- 인권 옹호에 있어 현재 요구되는 점과 잠재성을 발견하는 것 (정보 공유, 메시지를 보내는 것, 단체 행동)
- 전 세계의 정책장에서 인권 지지층을 쌓는 것

6. 세계의 토론장에서 적극적인 가치를 도모하는 것

인터넷은 전통적인 관점에서 볼 때 다스려지지 않고 있다. - 인터넷에 대한 조약이나 규제 기관이 없다. 거버넌스는 기능적이다. - 엔지니어와 고급 기술자들이 협력하면 문제

점을 고칠 수 있다. 이것에 관련된 비유는 차 정비와 같다. 차 정비에 있어서는 단 한 가지 걱정거리가 있다. 그것은 차가 움직이는 지 여부이다. 차가 어디로 가는지는 중요하지 않다. 유엔 인터넷 거버넌스 포럼과 유럽회의, 그리고 유럽경제연합을 포함한 인터넷에 대해 논의한 국제적인 정책 토론장을 살펴보면 지금 그들은 규율을 만들지 않고 있다. 그들은 모범 사례에 대해 기준, 가치 그리고 지침을 다듬는다. 이것은 다양한 이해관계자들의 협력, 정부, 기업 시민사회가 협력할 수 있게 한 데 모으는 것, 정보를 공유하고 모범 사례를 나누는 것과 관련 있다. 이런 정보교환에 참여하는 것은 인권 단체 뿐만 아니라 교육, 보건, 디지털 활동가들처럼 시민사회 활동가들이기도 하다.

인터넷이 경제와 사회에 미치는 영향이 더욱 커짐에 따라 정부는 인터넷에 대한 좀 더 강력한 규제를 원한다. 몇 년 전만 해도, 이런 경향은 더 많은 국가가 다양한 이해관계자들의 영향력을 최소화하려는 시도에서 더 심하게 나타났다. 이 분야에서 활발하게 활동하는 대부분의 시민사회 단체들은 (APC, CDT, EFF) 미국, 스웨덴, 영국, 케냐, 가나, 일본 정부와 함께 다자 이해관계자 시스템, 인터넷 환경의 개방성을 유지하고 정부간섭을 적게 하는 정책이 시민사회와 인권 단체가 정책에 참여하고 정책을 만드는 데 가장 좋은 기회를 제공한다고 한다. 더불어, 이렇게 빠르게 변화하는 세상에서 인터넷의 기반시설의 대부분을 민간부문이 담당하는 것에 비추어 볼 때, 효과적인 정부의 감시는 어렵거나 아예 불가능할지 모른다.

규제에 대한 추진력을 상쇄시키기 위해, 최근 몇 년 간 눈에 띄는 트렌드는 인터넷에서 행동과 기대에 대한 규범적인 가치로 작동하는 원칙들의 급증이었다. 다음과 같은 예들이 있다.

- 인터넷 정책입안을 위한 OECD 원칙
- 유럽회의의 인터넷 거버넌스를 위한 지침 선언문

- 시민 사회는 인터넷 권리와 원칙 인권과 인터넷 원칙의 헌장을 채택하였다. 또한 진보적인 통신 인터넷 헌장을 위한 연합과 글로벌 네트워크 이니시티브 원칙들이 시민 사회가 주도한 것들이다.

이런 원칙들은 강성법보다 인터넷에 좀 더 잘 적용되는 데 이것은 그것들이 더욱 유연하기 때문이다. (이 원칙들은 각 국가마다 다른 국내 규제 체제, 빠르게 변화하는 기술, 여러 영역에 걸친 이슈들을 참작한다.) 이들은 또한 어떤 기준이 옹호, 캠페인이나 정보 공유 도구 등으로써 인터넷 거버넌스에서 지지되어야 하는지를 결정하는 데 도움을 준다. 그리고 특히 이들은 인터넷 맥락에서 무엇이 인권인지 정의하는 것에 대한 필요성에 의해 만들어 졌다. 논의의 주요 내용중 하나는 디지털 세계에서 공적인 영역에서 개방성을 보전하는 것이 필요하다는 것이다. 그리고 인터넷 틀을 오프라인 세계에서 인권의 행사에 대해 보편적으로 동의된 협약이 제공하는보호 위에 세워야 한다는 것이다. 앞선 언급한 것들, 그리고 특히 인터넷 권리와 원칙 인권과 인터넷 원칙의 헌장과 같은 선언적 원칙들의 목적은 현존하는 인권 규범과 가치를 온라인 세상에 적용시키는 것이다. 이것은 또한 대기업과 특정 정부가 그러한 자유를 제한하고자 하는 것에 대한 인식을 바탕으로 제정되었다.

이런 여러 가지 계획들은 인권을 디지털 커뮤니케이션 이슈에 대한 사고의 틀과 문제를 분석하는 방법으로써 보는 것에 대한 중요성을 말해 준다.

7. 기업과 사용자간의 연합 다지기

기업 이익과 인터넷 자유 사이에 연합이 있다는 것이 다행이다 (비록 다른 단계에서 처리되어야 할 모순과 긴장이 또한 있기는 하지만 말이다.) 미국 지적 재산권 법안 SOPA에 반대하는 캠페인이 보여준 것은 인터넷의 실세는 수백만의 사용

자들이라는 것이다. 만일, 이 사용자들이 이동한다면, 선별적으로 그리고 필요시, 이런 대중 의견은 인권을 증진하는 데 엄청난 원동력이 될 수 있다. 몇몇 기업들은 전 세계의 심각한 결과가 되었을 뻔한 이 법안에 반대하는 의견을 형성하는 데 시민사회와 함께 결정적인 역할을 하였다.

기업과 함께 우리의 목표는 두 가지일 것이다.

- 기업들로 하여금 그들이 인권 책임을 완수할 수 있도록 도모하는 것 (기준으로 루지 체계를 이용)
- 그들의 사용자들을 온라인 상에서 인권을 옹호할 수 있도록 적절하게 역량강화를 하도록 하는 것

이것은 루지 체계를 통신회사들에게 이용하는 것과 어떻게 지지가 지속될 수 있는지 보기 위해 인터넷 자유를 위한 사용자의 지지(SOPA에서처럼)를 이끌어 낼 수 있는 주요 플랫폼 회사들을 포함시키는 것을 의미한다.

결론

고려되어야 할 인권정책이슈의 범위를 요약할 수 있을 것인가? 다음 표에서와 같이 단층 모델을 사용하여 설명할 수 있을 것이다. <표2, 영문원고 참고>

만약 인터넷이 이러한 가치들을 반영하는 것이었다면, 우리는 매우 현저한 발전을 이룩했을 것이다. 인터넷은 인권 업무의 범위를 변형시켰다. 가장 억압적인 정부에서도 전통적인 미디어가 그러한 뉴스를 전달하지못 하는 상황에서도 이제는 인권 주요 이슈에 대해 검색할 수 있다. 이렇게 세계화된 환경은 정보환경 또한

세계화가 되었다는 것을 의미한다. 100년 전에는, 대부분 사고의 범위는 국내에 머물렀다. 그러나 지금은 정보 접근은 역사에 선례가 없을 정도로 넓은 범위이며 이것과 함께 세계적 유동성의 잠재력이 존재한다. 우리는 이제 정부가 비밀스럽게 현저한 범위로 인권 유린을 저지를 수 없는 세계에 도달하고 있다.

더욱이, 인터넷은 새로운 종류의 연계를 도모한다. 사람들은 정보와 사상을 좀 더 많은 사람들과 함께 생성하고, 편집하고 공유할 수 있다. 사람들은 저렴하게 즉각적인 의사소통을 전 세계에 있는 사람들과 할 수 있으며 이러한 의사소통은 정부와 민간 감시자들에게 훨씬 더 저항적이다. 과거에는 정부, 출판업계, 편집자, 저널리스트와 같은 엘리트들의 손에 표현의 자유가 달려 있었지만, 지금은 공적인 곳에서 누구나 자신의 의견을 말할 수 있다. 이것은 표현의 자유의 민주화를 이루는 것이며 표현의 자유를 엘리트들 손에서 빼내어 일반 사람들의 손에 돌려 놓는 것이다.

12th Informal ASEM Seminar on Human Rights

제12차 아셈인권세미나 사전회의

"정보화 사회에서의 프라이버시권과 표현의 자유의 균형적 조화"

| 인 쇄 | 2012년 6월
| 발 행 | 2012년 6월

| 발행인 | **현 병 철** (국가인권위원회 위원장)
| 발행처 | **국가인권위원회 정책교육국 인권정책과**
| 주 소 | (100-842) 서울특별시 중구 무교동길 41
금세기B/D (을지로1가 16번지)
| 전 화 | (02) 2125-9729 | F A X | (02) 2125-9733
| Homepage | www.humanrights.go.kr

| 인쇄처 | 도서출판 **한학문화**
| 전 화 | (02) 313-7593 | F A X | (02) 393-3016

발간등록번호 11-1620000-000388-01

12th Informal ASEM Seminar on Human Rights

제12차 아셈인권세미나
사전회의

국가인권위원회
National Human Rights Commission of Korea

100-842 서울시 중구 무교동길 41 금세기빌딩 인권정책과
Tel. (02)2125-9729 Fax. (02)2125-9733 www.humanrights.go.kr