

# 국가에 의한 정보인권 침해 현황 및 정보인권 향상을 위한 과제 — 동아시아 3국을 중심으로 —

김주영 / 2019.12.09.

## 1. 서론

### 가. 문제 상황

21세기 정보화 시대를 맞아 우리의 생활 양상에는 과거와 비교했을 때 큰 변화가 생겼는데, 그것은 바로 누구나 스마트폰 등의 디지털 장비를 가지고 다닌다는 것이다. 그리고 이러한 디지털 장비는 사용자의 사용 내역을 디지털 정보로 기록하고 다른 장비로 보낸다는 공통점을 가진다. 다시 말해 우리의 위치정보나 인터넷 이용내역 등의 민감한 정보들이 자동으로 축적되고 다른 누군가에게 보내져 실 시간으로 분석된다는 것이다.

정보화 시대의 또 다른 특징은 새로운 기술의 등장 속도가 매우 빠르다는 것이다. 이것은 이러한 기술에 대한 충분한 정보를 얻을 수 있는 시간적인 여유를 빼앗는다. 무인 자동차나 드론과 같은 새로운 기술은 충분한 설명이나 정보 없이 우리 앞에 나타나기에, 우리는 이들의 정보 처리에 관해 제대로 이해하지 못한 채로 이들을 받아들일 수밖에 없다.

이러한 정보화 시대의 두 가지 특징은 정보인권 침해라는 새로운 사회 문제를 등장시킨다. 우리가 제대로 이해하지 못하는 기술이 우리의 정보를 가져가서 실시간으로 분석하여 우리에게 영향을 미친다면, 우리는 해당 기술에 의한 정보처리의 모든 단계에서 정보처리자의 의도에 무방비로 노출되고, 이는 곧바로 정보인권 침해로 이어진다.

### 나. 정보인권 침해 사례 분석 목적 및 절차

이런 과정이 정보인권 침해로 이어질 수 있음을 명확히 이해하기 위해, 본 분석에서는 동아시아 3국을 중심으로 정보인권 침해 사례를 먼저 다뤄볼 것이다. 그리고 이들로부터 발견한 공통점을 기반으로 정보인권 침해 문제를 해결하기 위한 제도적인 과제를 살펴 정보인권이 개선될 수 있는 환경을 조성하는데 도움이 되고자 한다.

이번 분석은 특정한 정보인권 침해 사례에 대한 실천적인 해결 방안을 도출하는 것에 목적을 두고 있는 것이 아니라, 동아시아 3국에서 주로 발생하는 정보인권 침해 사례에서 공통점을 찾고, 이러한 공통적인 문제 요소를 해결하기 위한 제도적인 과제를 도출하는 것이 그 목적이다.

## 2. 정보인권에 대한 소개

### 가. 정보인권의 정의와 유형

정보인권의 정의는 “인권 중에서 정보의 유통에 관한 개인의 기본적 권리들”(2013 국가인권위원회)로 요약할 수 있다. 보다 구체적으로는 “정보통신 기술에 의하여 디지털화된 정보가 수집, 가공, 유통, 활용되는 과정과 그 결과로 얻어진 정보가치에 따라 인간의 존엄성이 훼손되지 않고 자유롭고 차별 없이 이용할 수 있는 기본적 권리”(2013 국가인권위원회)이다.

정보인권에는 표현의 자유나 사생활의 보호 등 이미 헌법에서 보호하고 있는 권리도 있지만 현행 헌법

에서 다루지 못하는 것들도 존재한다. 진보네트워크센터에 의하면 정보인권의 세부적인 분야로는 인터넷 표현의 자유, 반감시와 통신비밀의 보호, 정보문화 향유권, 망중립성, 인터넷 거버넌스 등이 있다.

## 나. 한국의 정보인권 이슈 전개 과정 소개

한국에서 정보인권에 대한 요구는 주로 시민사회로부터 시작되었다고 볼 수 있다. 처음으로 시민단체의 목소리가 높아진 것은 1995년 내무부의 전자주민증 계획이 등장했을 때였는데 새삼스럽게 반대 여론이 높아진 것은 전자주민증 도입으로 인해 개인정보 유출이나 국가에 의한 감시의 가능성이 발생했기 때문이다. 김대중 정부는 이 계획을 백지화하였다.

인터넷 표현의 자유에 대한 요구는 2000년에 특히 등장하였는데, 당시 정보통신부가 추진한 통신질서 확립법은 내용등급제를 의무화하는 인터넷 등급제를 담고 있었기 때문이다. 가장 큰 문제는 등급 부여 권한을 정보통신윤리위원회가 독점하겠다는 구상이었다. 시민사회의 반발이 확산되자 인터넷 등급제는 자율적으로 도입하는 것으로 수정되었고 2002년 헌법재판소는 인터넷 표현의 자유를 인정하는 취지의 결정(99헌마480)을 하였다.

하지만 정보인권이 독자적인 개념으로 확립된 것은 2003년 교육행정정보시스템(NEIS) 도입 논쟁이 시작된 이후이다. 이 시스템은 모든 교육행정기관 및 초중등학교를 인터넷으로 연결하여 모든 제반 업무를 연계 처리하기 위해 구상되었다. 국가인권위원회는 교육행정정보시스템에 대하여 인권 침해라는 결정을 내렸고, 이 시스템은 문제를 피하기 위해 시도교육청 단위로 쪼개졌다. 인터넷 개인정보 자기결정권은 2011년 개인정보보호법이 제정됐을 때 비로소 적극적으로 보장되기 시작했다. 인터넷 표현의 자유 또한 헌법재판소가 인터넷 실명제 위헌 결정을 함으로서(2010헌마47 등) 제도화되었다.

망중립성은 최근에 등장한 개념으로, 2011년 통신사들이 무선인터넷을 이용한 전화 서비스를 차단한 것이 이슈가 되어 정부가 망중립성 가이드라인과 트래픽 관리 지침을 만드는 계기가 되었다. 하지만 정부는 망중립성에 관해 일체의 규제 권한을 행사한 적이 없다. 참고로 국가인권위원회는 2013년 발간한 정보인권보고서에서 망중립성을 포함한 정보접근권을 정보인권의 한 유형으로 보았다.

## 3. 동아시아 3국의 국가에 의한 정보인권 침해 사례

### 가. 한국의 국가에 의한 정보인권 침해 사례

가장 중요한 사례로는 국민보호와 공공안전을 위한 테러방지법을 들 수 있다. 테러의 개념과 테러위험 인물의 개념은 모호할 수밖에 없다. 어떤 사람이 테러위험인물인지를 결정하는 것은 결국 행정부이기 때문이다. 따라서 테러위험인물에 대하여 정보 수집을 보다 광범위하게 할 수 있도록 허용하는 것은 그 자체로 위험한 접근이다. 특히 영장 없는 사찰을 정당화하는 것이 문제가 되었다. 제9조제4항은 자료수집 과정에서 법이 어떤 행위를 제한할지에 대한 내용조차 없고, 언제까지 추적하는지 등이 오직 정보를 처리하는 대테러기관에게 맡겨져 있는데, 사전 또는 사후 통지 또한 보장되지 않는데다, 이 모든 사항이 영장을 필요로 하지 않기 때문에 개인정보 추적 대상자의 기본권을 침해한다.

그리고 대테러활동에 필요한 경우를 국가안전보장에 대한 상당한 위험이 예상되는 경우와 동일하게 두고 통신비밀보호법 일부를 개정하는 부칙의 내용 또한 문제적이다. 법률 자체는 통신비밀보호에 있어 대테러활동에 필요한 경우에 상당성을 요구하며, 상당성을 이유로 영장을 청구하도록 규제해도 과잉금지를 금하는 원칙을 위반한다고 볼 수 없다. 그런데 부칙에 있는 필요할 경우라는 문구를 근거로 영장을 청구할 수 있게 되면 영장 청구가 남발할 수 있다.

또 다른 사례로는 방송통신위원회의 SNI 차단이 있다. 방송통신위원회는 불법정보에 대한 단속을 위해 최근에 SNI(Server Name Indication) 차단 방식을 도입하였다. 인터넷 규약에서 SNI 필드는 인터넷 보안접속(HTTPS) 과정에서도 암호화 되지 않고 평문으로 전송되는데, 이 필드에서 차단 대상 도메인을 인식하여 차단하는 것이다. 방송통신위원회는 URL이 통신 내용이 아니기 때문에 SNI 선별 행위가 감청이 아니라고 주장한다. 그러나 URL은 이용자의 통신 내용을 알 수 있는 정보이다. 설령 이것이 통신사실만을 알려 주는 정보라 하더라도, 헌법재판소가 비내용적 정보에 대한 보호가 강화될 필요가 있다고 결정했다는 사실을 기억할 필요가 있다. 통신비밀 침해를 제도적으로 확대하기 시작하면 국가가 불법이라고 생각하는 모든 인터넷 트래픽에 대한 감시가 정당화될 수 있다.

기타 사례로는 2016년 행정자치부가 개인정보 비식별조치 가이드라인을 발표하며 개인정보에 비식별화 조치를 취하면 정보주체의 동의 없이도 이를 활용하거나 제3자에게 제공할 수 있도록 허용한 사례를 들 수 있다. 개인정보로 재식별될 수도 있고, 현행 개인정보 보호법과도 상충하는 내용이다. 낮은 단계에서의 광범위한 정보수사 관행도 문제이다. 대표적인 사례로는 특정 시각에 특정 기지국에 기록된 휴대전화 번호를 통째로 넘겨받아 수사하는 기지국 수사를 들 수 있다. 실제로 매년 1000만 건 이상의 통신자료가 정보 수사기관에 제공된다.

## 나. 중국의 국가에 의한 정보인권 침해 사례

중국은 대표적인 인터넷 검열국가이다. 몇 가지 예를 들면, 먼저 2008년 티베트 독립 시위 장면 동영상 상이 올라온 후, 중국에서의 유튜브 접속이 차단됐다. 이후 유튜브가 구글의 자회사로 편입되면서 현재도 중국에서는 유튜브 접속이 불가능하다. 바이두의 포럼인 테바도 금칙어 검열로 악명이 높았다. 정치적으로 민감한 단어나 상업성 광고 및 성적 요소를 포함하고 있는 단어들이 대상이다. 해당 단어들이 포함되어 있으면 게시물을 올릴 수 없다.

문제는 이런 기계적인 검열은 위의 의도가 전혀 없는 경우에도 적용된다는 것이다. 또한 중국은 2017년부터 대대적인 VPN 단속을 진행하여, VPN 서비스를 통한 구글이나 유튜브의 우회 접속이 힘들어질 전망이다. 다수의 VPN 서비스 제공업체들이 서비스를 중단했다.

사회활동을 기반으로 한 신용평가제도 도입도 문제이다. 세서미 크레딧은 중국의 알리바바 그룹이 중국 정부와 합작하여 만들어 냈다고 하는 전자상거래 기반의 신용평가회사로, 신용평가의 기준이 모호하고 자의적이어서 그 성격에 대해 논란이 다소 있다. 먼저 신용평가 기준이 기업비밀이기 때문에 정확한 전체 기준을 아무도 알지 못한다. 그리고 천안문 광장 사진을 올리거나 주가 폭락 등의 정보를 링크하면 세서미 크레딧의 점수가 떨어지지만, 경제 상황이 호조라는 뉴스를 링크하면 점수가 오르는 등의 현상이 제보되었다.

이 점수가 일정 정도 쌓이면 여행할 때 서류 심사나 대출이 쉬워지는 등 혜택이 따르며, 반대로 세서미 크레딧 점수가 낮으면 인터넷 속도가 느리다거나 취업의 어려움이 생기는 등 불이익이 따른다. 자신과 사회적 관계를 맺고 있는 사람들의 점수도 볼 수 있는데, 타인의 점수가 높을수록 자신도 점수가 올라가지만, 반대로 중국 체제에 반하는 성향의 사람과 관계를 맺고 있다면 점수가 떨어지게 된다. 중국은 2020년 세서미 크레딧을 의무화할 계획이다.

## 다. 일본의 국가에 의한 정보인권 침해 사례

일본의 모든 공항과 항만을 통해 입국하는 모든 외국인은 지문과 얼굴 사진을 제공해야 한다. J-BIS이라 불리는 이 조치는 이미 미국에서 US-VISIT이라는 이름으로 실시된 바가 있으나, 미국에서는 그간

이 조치가 당초 목표로 한 테러리스트 적발에는 아무 도움도 되지 못할뿐더러, 오히려 인권활동가들의 명단이 블랙리스트로 만들어져서 입국을 거부당하는 등의 사실이 밝혀져 크게 비판을 받아 왔다. 이와 관련하여 국제앰네스티 일본지부와 이주노동자와 연대하는 전국네트워크 등의 시민단체들은 J-BIS 도입을 반대하는 성명을 낸 바가 있다. 이들은 생체정보 취득, 보관, 이용, 폐기에 관한 확실한 법률적 규정이 없는 상황에서 이러한 제도를 도입하는 것은 외국인에 대한 차별과 고정관념을 강화할 뿐이라고 지적했다.

일본의 다른 사례로는 공모법 논쟁이 있다. 공모법은 흔히 공모죄로 불리는 테러 등의 준비죄를 신설하는 법률이다. 공모법은 정보인권과 직접적인 관련이 없어 보일 수도 있으나, 테러를 공모하였음을 수사기관에서 입증하기 위해서는 결과적으로 사이버 감청이 필요해지기 때문에 문제가 된다. 아베 정부는 2020년 도쿄올림픽을 앞두고 테러 방지를 위해서 공모죄가 필요하다고 주장해왔지만 공모법에 의해 처벌이 가능한 범죄가 277개나 되고 범죄 집단이나 준비행위 같은 규정이 불명확해 수사당국의 자의적 법 적용을 우려하는 목소리가 많았다. 특히 우려되는 것은 공모죄의 조문이 모호하여 시민들이 시위를 진행하는 것까지 처벌할 가능성이 있다는 점이었다.

마지막으로는 마이넘버 논쟁에 주목해야 한다. 마이넘버는 2016년 신설된 것으로, 주민번호와 유사한 역할을 하는 것이다. 마이넘버가 발급되고 이것을 정부가 관리하게 되면 마이넘버를 통해 개인이 열람할 수 있는 모든 정보를 국가 또한 열람할 수 있게 될 가능성이 있는데, 이는 수사기관의 감청에 큰 도움이 된다. 일본에서는 시민사회를 중심으로 마이넘버 거부 운동이 일어나고 있다.

#### 4. 정보인권 침해 방지를 위한 제도적 과제

위의 정보인권 침해 사례를 정리해 보면 국가가 부적절하게 민간 영역의 정보에 접근해서 발생하는 문제로 요약된다. 두 가지로 나누면, 먼저 인터넷 검열, 서서미 크레딧, J-VIS의 사례들과 같이 국가가 정보를 수집하고 통제하기 때문에 생기는 문제와, 그 다음으로는 SNI 차단, 테러방지법, 공모죄 처벌법의 사례들과 같이 국가가 정보통신을 감청하기 때문에 생기는 문제로 요약된다.

따라서 정보인권의 침해를 방지하기 위한 제도적 과제로는 가장 우선적으로 국가가 민간 영역의 정보에 임의적으로 접근할 수 없도록 해야 한다. 그런데 정보인권의 침해는 보통 사법부의 견제가 매우 부족한 환경에서 행정부에 의해서 일어나는 것으로 보인다. 그렇기 때문에 정보인권에 관해 사법부가 개입할 법적인 여지를 보다 강화하는 것이 도움이 될 것이다. 영장 없는 감청을 완전히 금지하는 것이 매우 중요하고, 국가가 민간 통신에 접근하기 위해서는 사법부의 동의를 받도록 할 수 있다.

행정부에 의한 정보인권의 침해는 입법을 통해 지지되는 경우가 많으므로, 행정부가 정보인권을 침해하는 것을 지원하는 법률이 제정되지 않도록 입법부를 감시하는 것도 대단히 중요하다. 특히 영장 없는 감청을 금지하는 것에 관련하여 예외를 도입하려는 입법 시도를 막아내야 한다.

마지막으로 정보인권에 대한 대중의 인식을 보다 강화해야 하며, 민간에서 정보인권과 관련된 활동을 계속해온 만큼 그 역량을 인정하고, 민간에서의 정보인권 관련 활동을 제도적으로 육성하여 민간에 의한 행정부에 대한 견제를 강화하는 것도 필요하다.

#### 인용 문헌

1. 진보네트워크센터/정보인권연구소(2016). 정보인권 가이드북 III: 정보인권의 이해.
2. 진보네트워크센터 홈페이지. 정보인권. 검색일: 2019년 12월 3일.
3. 국가인권위원회 인권정책과(2013). 정보인권 보고서.