미국 통신 분야 프라이버시 보호 사례를 통한 우리나라 적용 방안

박은엽*, 임종인*

*고려대학교 정보보호대학원/정보보호기술연구센터

The Study on Electronic Communication Privacy Protection of United State

Eun-Yeop Park*, Jong-In Lim*

*Center for Information of Security of Technologies(CIST), Korea University.

요 약

정보화 사회로 변하고 있는 지금 통신기술 역시 발전하고 있으며 음성통신 및 비음성통신(전자 매체를 통한 통신)의 활용도가 점점 증가하고 있고, 사용되는 정보의 양 역시 늘어나고 있다. 그러나 정보의 흐름이 대량화, 가속화됨에 따라 통신매체를 통해 각종 개인정보가 노출될 위험이 증가하고 있으며 이에 따라 개인의 프라이버시 역시 위협받고 있다. 본고에서는 통신기술의 발달과 개인의 통신비밀 보호를 어떻게 조화시킬 수 있는가를 미국의 사례를 통하여 알아보겠다.

I. 서론

유비쿼터스 컴퓨팅 환경은 무수한 정보기술의 융합으로 이루어진 환경이며 통신 역시 여러 정보기술의 융합으로 이루어져 있다. 이런 환경에서는 유선 및 무선에서의 개인 활동이 증가하게 된다. 이에 따라 개인을 정보 노출의 위험이 증가하게 되고 개인정보를 불법으로 취득하려는 사람들의 움직임 역시 많아지게 될 것이다. 개인정보의 부적절한 사용으로 인한 프라이버시 침해문제는 기술·정보화 사회로의 발전을 저해하는 요소로 작용할 것이다.

이에 따라 본고에서는 통신과 통신보호의 선진국이라 할 수 있는 미국에서 과연 사적 통신의 비밀 보호 방안을 판례로 살펴보고, 우리나라의 통신비밀 보호에 어떻게 적용될 수 있으며, 법이 다루지 못하는 부분에 대해서 살펴보고 추가되어야 하는 부분에 대해 고찰해 본다. 또한 기술의 발달과 개인의 통신비밀 보호 사이에 법 균형 방안을 도출해 보겠다.

II. 미국의 통신비밀 보호 방안

미국법에 있어서 통신비밀은 수정헌법 제4조에 의하여 보호된다. 미국 수정한법 제4조는 정당한 이유(probably cause)에 의하여 발부된 영장에 의하지 아니하고는 신체, 주거에 대한 부정당한 압수 및 수색을 받지 않을 권리를 인정하고 있다. 이처럼 미국은 일찍이 프라이버시권을 보장하고 있으며 통신과 관련해서도 프라이버시 보호를 위한 태도를 명확히 하고 있다.

본고에서는 통신과 연관된 미국의 판례를 중심으로 몇 가지 대표적인 사례를 분석해 본다.

Olmstead 판결(Olmstead v. United States 277 U.S. 438(1928))에서 미국대법원은 주거지에 대한 신체 및 기구의 침입이 없이 단순히 대화를 엿듣는 행위는 신체적 침범이나 유형적인 물체에 대한 압수를 포함하지 아니하므로

수정헌법 제4조는 이에 적용되지 아니하고 따라서 수정헌법 제4조는 도청(wiretapping)에는 적용되지 않는다고 판시하였다. 이 Olmstead 판결의 영향으로 미국은 1934년에 통신법(the Federal Communication Act)을 제정할 때, 605조에 전화 도청이 연방 범죄임을 규정하게 되었다. 그리고 1968년에 개별법인 *Wiretap Act*를 제정하였다.

그러나 1967년의 Katz 판결(Katz v. United States389 U.S 347(1967))에서 공중전화박스안의 통화를 도청한 사안에 대하여 미국대법원은 수정헌법 4조가 보호하는 것은 "장소(places)"가 아니라 "사람(people)"이라고 전제하고, 비록 특정인의 주택이나 사무실에 있더라도 공공에 노출되어 있는 경우(what a person knowingly exposes to the public)는 수정 헌법 4조의 보호대상이 아니며, 공공에 노출되어 있는 장소라도 사적으로 유지하기를 원하면(what he seeks to preserve as private) 수정헌법 4조의 보호대상이 된다고 판시하여 수정헌법 제4조가 도청에도 적용됨을 명백히 하였다. 이 판결은 수정 헌법 4조의 해석을 문자 그대로 하여, 프라이버시 보호대상을 물리적인 영역에 한정해 온 판례에서 벗어나, 인간의 존엄성과 관련된 프라이버시 영역으로 확대 발전시킨 획기적인 판례라 할 수 있다. 미국의회는 1968년 Katz 판결에 대응하여 Title Ⅲ of the Omnibus Crime Control and Safe Street Act를 제정하여 전화통신 및 대화의 감청을 규제하였으며, 1986년 전자통신(Electronic Communication)을 규율하는 규정을 마련하여 *the Electronic Communication Privacy Act(ECPA)*[1]를 제정하였다.

1979년 Smith 판결에서 미국법원은 수정헌법 제4조는 고객이 자발적으로 펜 레지스터(pen register)[2]에 의하여 감청당하는 전화번호를 전화를 걸기 위하여 송신하였기 때문에 영장 없는 펜레지스터의 사용에는 수정헌법 제4조가 적용되지 않는다고 판시하고 있다. 즉, 제3자(third parties)인 전화회사에 자발적으로 제공한 정보는 제3자의 소유이므로 통신기록에 대한 control power가 전화회사에 있다고 봐서 수정헌법 4조에 의한 보호대상이 되지 않는다는 것이다. 이 판결을 계기로, 미국에서는 이메일 주소(e-mail address)나 로그(log) 기록, 전화번호와 같은 통신기록 등을 보호하는 개별법인 *Pen Trap Act*를 제정하였다.

Ⅲ. 우리나라의 통신비밀보호법

우리나라는 통신비밀보호법(1993.12.27)을 제정하여 통신 비밀을 보장하고 있다. 이 법은 통신 및 대화의 비밀과 자유에 대한 제한은 그 대상을 한정하고 엄격한 법적 절차를 거치도록 함으로써 통신 비밀을 보호하고 통신의 자유를 신장함을 목적으로 하고 있다.

우리나라의 통신비밀보호법 제3조 1항에 의하면, "누구든지 이법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신[3]의 감청 또는 통신사실 확인자료[4]의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다."고 규정하였고, 3항에서는 "누구든지 단말기기 고유번호를 제공하거나 제공받아서는 아니 된다."고 규정하였다. 현행 우리의 통신비밀보호법에 따르면, Olmstead 사건이나 Katz 사건에서 논란이 되고 있는 편지와 전화 통화에 대한 보호는 동등한 가치로 보호되며, 도청이 집안이건 집밖에서 이루어지건 상관없이 영장 없는 도청은 불법이다.

---

1) the Electronic Communication Privacy Act(ECPA)은 전선, 구두, 전기통신을 보호하고 있다.

2) 전화선에 연결되면 그 선에 연결된 전화에 의하여 다이얼되는 전화번호를 기록하는 것이다.

3) "전기통신"은 유선, 무선, 광선 및 기타의 전자적 방식에 의하여 모든 종류의 음향, 문언, 부호 또는 영상을 송신하거나 수신하는 것을 말한다.

4) "통신사실 확인자료"는 통신일시, 개시 및 종료시간, 상대방 번호, 사용도수, 로그기록, 위치추적자료 등을 말한다.

그러나 우리나라의 통신비밀보호법에 있어서 과연 통신감청을 위한 요건으로 송신중인 통신임을 요건으로 하고 있는가는 또 다른 문제이다. 미국은, Wire trap Act(1968), Pen trap Act(1980), ECPA(1986) 등 필요에 따라 여러 개별법을 제정해 왔으며 음성인지, 실시간(real time)인지, 내용이 아닌 단순로그기록인지 등을 구별하여 규정하고 있지만 우리나라의 법은 단순히 전기통신의 보호에 대하여만 규정하고 있어 그 보호의 범위가 어디까지 인가가 문제가 되고 있다. 제 3조의 규정은 현재 "송신 또는 수신"하는 것만을 의미하는가 또는 송수신되어 통신서비스제공자에 의하여 "저장"되었거나 이미 "도착"한 통신까지 포함하는가에 대한 문제를 가지고 있다.

또한 Smith사건에서와 같이 영장 없이 통신사업자의 시설에 펜 레지스터(pen register)를 설치하여 정보를 수집하는 것도 우리 통신비밀보호법은 허용하지 아니한다. 우리 법에는 통신기록과 같은 통신사실 확인 자료를 통신 사업자에게 요청할 경우에도 서면으로 관할 지방법원의 허가를 받아야 하며, 긴급한 경우에는 통신 사업자에게 요청 후 지체 없이 법원의 허가를 받아야 한다. 이 또한 통신과 관계없는 제3자에 의한 감청이 허용되지 않는 것은 당연하다. 그렇다면 한쪽 당사자에 의한 감청은 어떠한가. 이 부분에 대하여 우리의 법은 명확한 규정을 두고 있지 않다.

위의 세가지 판례에서 보듯이 증거능력에 대하여 미국의 ECPA가 전자통신과 구두(즉 대화), 전선통신을 구별하여 각 증거배척의 범위를 달리함에 비하여 우리나라의 통신비밀보호법에서는 제4조에서 "불법감청에 의하여 지득 또는 채록된 전기통신의 내용은 재판 또는 징계절차에서 증거로 사용할 수 없다"라고 규정하고 이를 제14조 제2항에서 "타인의 대화비밀침해"에 대하여도 이를 준용하고 있음을 유의하여야 한다. 즉 통신비밀보호법에 위반한 일체의 불법한 통신감청은 불법이고 증거능력이 없다는 엄격한 태도를 취하고 있어 법을 지키며 수사 하는데 어려움이 있다. 엄격한 법이 오히려 법을 우회하는 방법을 택하게 하는 문제가 우리나라의 통신비밀보호법에는 존재하고 있다.

이를 종합해 보면, 미국은 앞서 본 사례로 보아 국민의 프라이버시 보호와 수사기관의 원활한 수사권 행사를 균형적으로 감안하여 입법하고 있으며, 법원 판례도 이러한 균형감각을 유지하고자 하는 고심이 보인다.

그러나 우리나라의 경우는, 엄격하게 프라이버시 보호를 우선하고 있다. 우리 법에 따르면, 통신제한 조치는 범죄 수사 또는 국가안전보장을 위하여 보충적인 수단으로 이용되어야 하며 국민의 통신 비밀에 대한 침해가 최소한도에 그치도록 노력하여야 한다는 선언적 규정을 두고 있다. 아울러 통신제한조치를 할 수 있는 범죄도 제한하고 있을 뿐만 아니라 범죄를 계획 또는 실행하고 있거나 실행하였다고 의심할 만한 충분한 이유가 있고 다른 방법으로는 그 범죄의 실행을 저지하거나 범인의 체포 또는 증거의 수집이 어려운 경우에 한하여 할 수 있도록 하였다. 그리고 명문으로 독수독과 원칙을 규정하여, 불법 감청에 의한 정보는 증거로 채택할 수 없도록 하였다.

Ⅳ. 결어

이상과 같이 간략하게 미국의 통신비밀보호에 관련된 판례들을 살펴보고 이와 관련하여 우리나라 법 간략하게 검토하여 보았다. 논의된 내용들이 우리나라의 통신비밀보호 관련 법규들을 이해하는데 참고가 되기를 기대하며 간단하게 입법론으로 첨언하고자 한다.

첫째 저장된 통신을 우리 통신비밀보호법에서 규율하고 있지 않다는 것을 전제로 저장된 통신 즉 전자우편 등이 송신되기는 하였으나 수신자가 열람하지 아니한 경우에 대하여도 일반적인 통신과 같은 정도의 보호가 주어져야 한다. 개인 간의 의사의 소통수단이라는 점에 비추어 다른 통신수단과 보호를 구별할 필요는 없는 것으로 보인다. 다만 일정한 기간이 지난 통신에 대하여 그 보호를 완화하는 것은 바람직하다고 본다.

둘째 현재 각 기업이나 학교에서도 통신설비를 설치하여 사원들이나 학생들이 전자우편을 이용할 수 있는 환경이 일반화되고 있기 때문에, 이러한 경우 위와 같은 서비스제공의 주체인 기업과 학교 등과 그 이용자인 사원, 학생들과 사이에 통신비밀의 보호에 대한 규정이 마련되어야 한다. 이에 관하여는 서비스제공자의 권리와 재산을 보호하기 위하여 필요한 경우 감청을 허용하는 규정, 사용자에게 명시적·묵시적 동의를 받는 등의 절차가 필요하다. 이에 관한 우리나라의 전기통신기본법 및 전기통신사업법상의 규정들은 모호할 뿐 아니라 충분하지 않다.

마지막으로 통신서비스제공자가 범죄행위에 속하는 통신내용을 게시판 등을 유지·관리하는 과정에서 지득한 경우 수사기관에 이를 신고하는 의무규정을 도입할 필요가 있다. 전기통신서비스제공자들은 그 공적인 성격으로 인하여 위와 같은 사회 질서 유지에 있어서 협력의무를 지닌다고 볼 것이므로 이들에게 범죄행위[5]의 신고의무를 부과하여야한다. 다만 위와 같은 신고의무의 강조가 건전하고 자유로운 통신문화 발달의 제약요인으로 작용하여서는 안되므로 이러한 신고의무가 감시의무로 이해되어서는 안 되며 필요최소한도에 그쳐야 한다. 따라서 단순히 통신설비의 유지관리과정에서 "우연히" 발견한 것으로 한정되어야 함은 물론이다.

우리나라는 통신비밀보호법을 제정하여 프라이버시권을 보호하려는 노력을 하고 있으며 기술의 발달에 따라 최초 제정 이후 여러 차례 개정을 거쳐 프라이버시 보호를 강화하려는 노력을 해왔다. 그러나 발달하는 기술을 법이 따라가지 못하는 문제가 있다. 앞으로 시대상황의 변화에 따라 국민의 프라이버시 보호와, 범죄수사의 효율성을 두루 고려하는 법 개정 검토가 요구될 것으로 예상된다.

5) 범죄정보의 교환, 어린이 포르노그래피의 유통, 지적소유권침해물품 유통, 불법 도박 등을 들 수 있다.

[참고문헌]

[1] 권영설, 사용자의 근로자 이메일전자감시와 사업장에서의 사생활권, 개인정보연구 제2권 제1호, 한국정보보호진흥원, 2003.

[2] Mark S. Kende, The Issues of E-mail Privacy and Personal Jurisdiction: What Clients Need to Know About Two Practical Constitutional Questions Regarding the Internet, 63 Mont. L. Rev. 301, 2002.

[3] Todd M. Wesche, Reading Your Every Keystroke: Protecting Employee E-mail Privacy, 1 J. High Tech. L. 101. 2002.

[4] 개인정보보호 핸드북, 한국정보보호진흥원, 2005.

[5] Bennet, Colin J. & Raab, Charles D. The Governance of Privacy: policy instruments in global perspective .Hampshire: Ashgate, 2003.

[6] 유석진 외, 유비쿼터스시대의 국가 간 개인정보 유통정책의 해외사례 연구 및 우리나라의 대응방안, 정보통신부 보고서, 2005