Journal of The Korea Society of Computer and Information
Vol. 20, No. 5, May 2015
www.ksci.re.kr
http://dx.doi.org/10.9708/jksci.2015.20.5.123

압수수색과 개인정보 보호의 문제

김 운 곤*

Privacy protection of seizure and search system

Woon-Gon Kim*

요 약

정보통신의 눈부신 발전은 우리 사회에 편리함과 더불어 또 하나의 문제를 야기하고 있다. 즉 전자기기로 무제한적 감시가 가능한 사회로 변모 되고 있어, 이를 잘못 관리할 경우 또 다른 재앙으로 낳을 수 있다는 문제가 있다. 이러한 사회 속에서 살아가는 우리는 거주지의 문을 나서면서부터 곳곳에 설치되어 있는 폐쇄회로 카메라(CCTV-Closed Circuit Television)와 개인이 사용하는 스마트 폰을 통하여 감시의 덫 속에서 살아가고 있는 것이다. 한편으로는 정보통신의 발전과 함께 개인정보를 쉽게 수집, 저장하게 되면서 기업에게는 마케팅을 위한 기업의 소중한 자산가치가 되면서 이를 불법적으로 수집하고자 하는 사람들이 늘어나게 되고, 실제로 이와 관련된 사건들이 많이 발생하기도 하였다.

이러한 정보사회 속에서는 수사도 범죄행위로 인해 남게 되는 디지털 흔적을 얼마나 잘 찾아낼 수 있느냐가 그 수사의 성공도를 가늠할 수 있을 정도로 여겨지고 있으면서 수사기관은 이를 찾기 위해 노력하게 된다. 따라서 사건을 수사하면서 범죄자가 사용하였던 컴퓨터나 스마트폰의 사용흔적에 관한 압수 수색의 절차는 이제 필수적인 절차가 되었으며, 이러한 전자적인 증거를 수집할 수 있느냐는 수사의 성패를 가름하는 결정적인 요소가 되었다. 그런데 이때 수사기관들은 전자 증거자료들을 압수 또는 수색하면서 포괄적으로 이루어지는 경우가 많아 피압수자의 정보자기결정권을 침해할 우려가 높아지는 추세이다. 따라서 많은 국민들이 수사기관이 행하는 전자정보의 포괄적 압수수색에 대하여 불안감이 노출되면서 '사이버 망명'이라는 용어까지 탄생시키고 있다.

이러한 점에서 전자적 정보의 압수수색 범위를 어떻게 설정하여야 할 것인지를 검토하였다.

▸ Keywords : 전자증거, 압수수색, 사생활의 비밀과 자유, 정보자기결정권, 영장주의, 압수방법의 제한

Abstract

Bright development of information communication is caused by usabilities and another case to our society. That is, the surveillance which is unlimited to electronic equipment is becoming a transfiguration to a possible society, and there is case that was able to lay in another disasters if manage early error. Be

* 제1저자 김운곤
* 투고일 : 2015. 4. 1, 심사일 : 2015. 4. 16, 게재확정일 : 2015. 4. 21.
* 조선이공대학교 해양경찰과(Dept.of Maritime Police, Chosun College of Science & Technology)

what is living on at traps of surveillance through the Smart phones which a door of domicile is built, and the plane western part chaps, and we who live on in these societies are installed to several places, and closed-circuit cameras (CCTV-Closed Circuit Television) and individual use. On one hand, while the asset value which was special of enterprise for marketing to enterprise became while a collection was easily stored development of information communication and individual information, the early body which would collect illegally was increased, and affair actually very occurred related to this.

An investigation agency is endeavored to be considered the digital trace that inquiry is happened by commission act to the how small extent which can take aim at a duty successful of the inquiry whether you can detect in this information society in order to look this up. Therefore, procedures to be essential now became while investigating affair that confiscation search regarding employment trace of a computer or the telephone which delinquent used was procedural, and decisive element became that dividing did success or failure of inquiry whether you can collect the act and deed which was these electronic enemy. By the way, at this time a lot of, in the investigation agencies the case which is performed comprehensively blooms attachment while rummaging, and attachment is trend apprehension to infringe discretion own arbitrary information rising. Therefore, a lot of nation is letting you come into being until language called exile 'cyber' while anxiety is exposed about comprehensive confiscation search of the former information which an investigation agency does.

Will review whether or not there is to have to set up confiscation search ambit of electronic information at this respect how.

▸ Keywords : electronic evidence, search and confiscation, authority to decide oneself information, necessity for warrants, restriction on confiscation

I. 서 론

정보통신의 눈부신 발전은 우리 사회에 편리함과 더불어 사회의 많은 변화를 초래하고 있다. 고도의 정보통신사회의 발전은 이러한 시스템을 범죄로 악용하거나 범죄와 관련된 자료들이 전자 관련 기록 매체에 남아있어 범죄를 찾아내는 중요한 수단으로도 떠오르고 있다. 따라서 범죄 수사를 위해서는 네트워크의 이용을 추적하거나 각종 시스템이나 기록매체 속에 존재하는 정보를 찾아내서 피의자와 결합시키는 것이 수사절차에서 중요한 증거확보 방법의 하나로 등장하였다.

그러므로 기존의 압수수색절차는 유체물로 한정되어 있었다면, 현대 수사절차에서 압수수색은 디지털 증거를 얼마나 효율적으로 압수수색할 수 있느냐의 문제로 귀결되고 있다. 또한 현재 운용되고 있는 「형사소송법」도 압수수색과 관련된 규정들이 유체물을 대상으로 한 규정들이기 때문에 이 규정을 그대로 디지털 증거에 적용하는데 있어서도 많은 문제를 야기할 수 있다.

예컨대 디지털 증거를 압수하면서 압수할 기록을 다른 저장물에 복사 저장하여 압수한다거나 원격지 정보를 압수하기 위하여 네트워크를 통하여 압수하는 방법, 압수현장에 있는 PC를 다른 장소로 옮겨서 분석과 검증을 하는 경우, 이를 법정에서 그 사건의 증거능력을 갖춘 증거물로 인정할 수 있는지 등을 검토해야 할 필요성이 있다.

이와 더불어 디지털 증거의 압수수색의 범위를 유체물 증거와 같이 하게 된다면, 디지털 증거 속에 내재되어 있는 수많은 사람들의 개인정보가 그대로 노출될 수 있는 위험성도 가지고 있다.

즉 수사기관들은 피의자와 관련된 전자 증거자료들을 압수 또는 수색하면서 포괄적으로 하여, 그 전자 증거자료 속에 포함되어 있는 개인정보들이 무차별적으로 수사기관의 압수수색

과 함께 노출되면서 개인정보 주체자의 정보자기결정권을 침해할 우려가 높아지는 추세이다. 따라서 많은 국민들이 수사기관이 행하는 전자정보의 포괄적 압수 수색에 대하여 불안감이 노출되면서 '사이버 망명'이라는 용어까지 탄생시키고 있다.

이러한 점에서 전자적 정보의 압수수색 범위를 어떻게 설정하여야 형사소송절차에서 추구하는 실체적 진실발견의 목적도 이루면서 개인정보를 무제한적으로 노출되는 것을 방지할 수 있는지를 검토하고자 한다.

II. 개인정보의 법적 성격과 법체계상 문제

통신 네트워크의 급속한 발전과 함께 많은 양의 정보를 보관할 수 있는 디지털화의 발전은 정치, 경제와 사회, 문화 등 모든 영역에서 많은 영향을 미치고 있을 뿐만 아니라, 개인적인 삶의 영역에 미치는 파장은 개인이 감당할 수 없을 정도로 큰 편이다. 즉, 개인이 얻을 수 있는 정보의 범위가 넓어져 정보의 평등화가 이루어진 반면에 개인정보를 이용한 프라이버시의 침해는 개인의 삶을 포기하게 하는 등 심각한 사회적 문제를 야기하고 있다.

이러한 IT기술은 과거에 일어났던 일까지 현재진행으로 만들고 있다[1]. 이처럼 인터넷 상에서는 옛날에 일어났던 사건과 관련된 개인의 정보가 오랜 시간이 지난 후까지도 현재진행형처럼 기록되어 있기 때문에 피해를 당하거나 곤란을 겪는 경우가 많아지고 있다[2].

특히 2014년 정기국회를 가장 뜨겁게 달구었던 내용이 사이버 검열' 논란이었다. 검찰 등 수사기관이 개인적 통신 내용을 들여다 볼 수 있다는 가능성 때문에 온 국민들을 불안에 빠뜨리고, 외국에 서버를 두고 있는 통신사로 옮기는 '사이버 망명' 사태까지 불러일으켰다[3].

이처럼 우리 사회에서도 개인정보에 관한 관심도가 높아졌지만, 수사기관의 개인정보에 관한 보호수준은 아직 미미하다고 할 수 있다.

여기에서는 개인정보라는 무엇을 말하는지를 검토하고, 우리나라에서도 개인정보자기결정권을 인정하고 있는지에 관한 검토를 하고자 한다.

1. 개인정보의 개념

개인정보의 개념은 다양하게 정의할 수 있겠지만, 우리나라 「개인정보 보호법」 제2조 제1호에서는 '살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다)를 말한다.'라고 정의하고 있다. 이 법에서 정의하고 있는 것처럼 어떠한 내용의 정보가 그 정보만으로는 특정한 개인을 나타내지는 않더라도, 그 정보를 이용하여 특정한 개인을 알아낼 수 있다면 그 사람의 개인정보에 해당한다는 포괄적인 의미로 해석하는 것이 일반적이다.

2. 개인정보자기결정권의 법적 성격

2.1. 개인정보 보호의 필요성

국가 등 힘을 가진 단체나 개인이 국민 개개인의 행동을 관찰하는 등 개인의 정보를 수집·처리하는 사회 속에서 우리 개개인은 자유롭게 행동하면서 생활할 수 있는지를 생각해 본다면, 그러한 관찰 속에서 행동의 자유를 누릴 수 있는 경우는 그리 많지 않을 것이다. 즉 개인의 행동을 자연스럽게 제약하게 되고, 혹 비밀을 간직하고 있는 개인의 존재는 항상 두려움에 휩싸일 수 있는 등 불안한 사회로 전락할 것이다.

그리고 사물인터넷(Internet of Things)시대에 살고 있는 개개인은 정보망을 가지고 있는 국가가 개인의 개별 자료를 결합하여 그 사람의 동선, 생각 등 모든 사항을 파악할 수 있는 시대이기 때문에 이를 이용하면 쉽게 개인의 자유를 억압할 수 있는 새로운 시대로 진입하고 있다. 비록 개별적 정보로는 아무것도 안되지만 이러한 미미한 정보들을 결합하게 되면 그 사람의 전체적 또는 부분적 인격상을 형성할 수 있게 되고 있기 때문이다.

또한 이렇게 미미한 정보들을 무제한적으로 수집하고 결합할 수 있는 집단은 개인의 행위를 예측하고 조종할 수 있는 기준을 얻을 수 있다는 데 심각한 문제가 있다.

2.2. 개인정보 자기결정권

개인정보자기결정권에 관하여 우리 헌법재판소는 "자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주제가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특정 짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함 한다."라고 정의를 내리고 있다[4].

이와 더불어 헌법재판소는 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다고 판시하고 있다.

대법원은 한나라당 조○혁 의원이 전교조 소속 교사의 명단을 공개한 사건에서, "학생이나 학부모가 교육 관련기관의 정보공개에 관한 특례법과 그 시행령이 정한 공시범위를 넘어서 특정 교원의 노동조합 가입 여부나 특정 노동조합에 대한 정보를 수집하고 그 제공을 요구할 경우, 이는 필연적으로 헌법 등에 의하여 보호되는 교원의 인격권 등에서 비롯된 개인정보자기결정권을 침해하는 것"이라고 판시하였다[5].

우리나라 헌법재판소와 대법원의 태도를 보더라도 개인정보자기결정권은 헌법상 사생활의 비밀과 자유 그리고 행복추구권으로부터 도출되는 헌법상 기본권이라고 할 수 있다.

3. 개인정보 관련 법체계상의 문제

우리나라 법체계에서 개인정보를 정확하게 파악하기 위하여는 20여개 정도의 개별 법령을 검토하여야만 알 수 있을 정도로 신용정보, 의료정보 등의 개인정보가 개별적 법률로 규정되어 있다. 이와 더불어 규제의 내용도 각 법률마다 제각각으로 규정되어 있어 그에 따른 책임도 평준화 되어 있지 않은 형편이다.

예컨대 행정자치부에서 주관하는 「개인정보 보호법」은 공공기관이나 기업에 적용되고, 방송통신위원회가 주관하는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 온라인 기업, 금융위원회에서 주관하는 「신용정보의 이용 및 보호에 관한 법률」은 금융기관, 보건복지부가 주관하는 「의료법」은 의료기관에 적용되는 등 다양하게 규정되어 있는 형편이다.

또한 개인정보를 유출한 경우의 규제 내용을 살펴보면, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 과징금 규정이 있지만, 「신용정보의 이용 및 보호에 관한 법률」과 「개인정보 보호법」에서는 과징금 규정이 없다. 즉 개인정보를 유출한 행위에 대하여 어느 법률을 적용하느냐에 따라 제재 여부가 달라지는 현상이 발생할 수 있다.

개인정보를 위탁한 행위에 대해서도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에서는 정보주체의 동의를 받도록 규정되어 있는 반면, 「개인정보 보호법」에서는 이러한 규정이 없어, 어느 법률을 적용받느냐에 따라 손쉽게 위탁할 수 있느냐의 문제와도 귀결되도록 규정되어 있다.

따라서 우리나라의 개인정보를 규제하는 법률 체계는 일반인의 입장에서 산만하게 규정되어 있어, 이를 이해하기란 참으로 어렵게 되어 있어 체계적인 정비가 필요하다고 하겠다.

III. 디지털 증거의 압수수색·검증

1. 디지털 증거의 의의

1998년 디지털 증거에 관한 과학실무그룹(Scientific Working Group on Digital Evidence: SWGDE)[1]에서는 '디지털 형태로 저장되어 있는 정보 또는 디지털 형태로 전송되는 증거가치가 있는 정보'라고 정의하고 있다.

여기에서 말하는 디지털 형태 정보는 이미지, 음향 및 영상 녹화물과 텍스트 등 다양한 종류의 정보들로서 이진수의 숫자조합의 형태로 존재한다.

디지털 증거는 유체물로 되어 있는 증거와는 달리 원본과 사본의 동일성, 매체독립성, 대량성, 네트워크성, 취약성 등의 특성을 가지고 있다. 이러한 점 때문에 수사기관의 압수·수색 과정에서 고전적으로 이루어져 왔던 유체물로 된 증거에 관한 강제처분과 다른 문제들이 많이 발생하고 있다.

디지털 증거의 수집도 원칙적으로 임의수사방법에 따르고, 강제수사는 강제수사법정주의에 따라 법률에 규정된 경우에 한하여 예외적으로 허용된다. 따라서 디지털 증거를 수집하는 절차에서도 영장주의와 비례성의 원칙을 엄격하게 적용하여야 한다.

2. 디지털 증거분석의 법적 성격

압수·수색영장의 집행으로 획득된 디지털 정보를 전문가가 삭제된 데이터를 복구하거나 증거가치가 있는 디지털 정보의 범위를 확정하는 등의 방법으로 파일이나 저장매체를 분석한다. 이는 영장 집행 현장에서 저장매체를 검색하여 관련성 있는 정보를 복사하는 경우와 구별하여야 하는데, 디지털 증거분석은 압수영장의 집행 이후에 이루어진다는 점이 다르다.

여기서 압수영장의 집행 이후에 이루어지는 디지털 증거분석의 법적 성격과 새로운 강제처분으로 별개의 압수수색검증영장을 필요로 하는지가 문제된다.

2.1. 압수 대상으로서 디지털 증거

2011. 7. 18. 신설된 「형사소송법」 제106조 제3항에서는 "법원은 압수의 목적물이 컴퓨터용디스크, 그 밖에 이와

1) 미국 법무부 마약수사청, 연방수사국, 국세청 범죄수사단, 관세청, 항공우주국 등 연방기관의 증거분석 연구소들을 중심으로 구성되었다.

비슷한 정보저장매체인 경우에는 기억된 정보의 범위를 정하여 출력하거나 복제하여 제출받아야 한다. 다만, 범위를 정하여 출력 또는 복제하는 방법이 불가능하거나 압수의 목적을 달성하기에 현저히 곤란하다고 인정되는 때에는 정보저장매체 등을 압수할 수 있다."라고 규정함으로써 정보저장매체 증거에 대한 압수는 범위가 정해진 정보를 제출받는다고 규정하고 있다. 즉 디지털 정보를 이 규정에 포함시켜 압수할 수 있는지가 문제된다. 만약 디지털 정보를 압수대상물로 본다면, 유체물의 압수와 같은 규정을 적용하여 압수할 수 있는지가 문제된다.

디지털 정보는 무체성으로 이를 바로 증거물로 사용할 수는 없다. 따라서 디지털화된 내용을 분석하여 유체물로 출력하거나 유체물인 기록매체로 수록하여야 증거로 사용할 수 있다. 그러므로 디지털화 된 정보를 분석하여 유체물로 만드는 과정을 하나로 파악하여 디지털 정보를 압수할 수 있다고 보는 긍정적 견해가 있다[6]. 이에 반하여 2011. 7. 18. 제106조 제3항과 제4항이 신설되기 이전에는 현행법상 압수의 대상은 유체물이고, 디지털 정보들은 유체물이 아니기 때문에 종전 형사소송법 제106조의 규정으로는 압수·수색이 불가능하다는 견해도 있다[7].

그러나 「형사소송법」 제106조 제3항과 제4항이 신설되었고, 문리적 해석으로는 컴퓨터용 디스크나 그와 비슷한 정보저장매체로 해석할 수 있으나, 거기에 저장된 정보의 범위를 정하여 출력하거나 복제하여 제출 받게 할 수 있기 때문에 압수의 대상은 전자정보이다. 이 때 전자정보는 그 저장매체를 말하는 것이 아니라 저장매체에 저장되어 있는 정보의 내용을 말하는 것이기 때문에 그 압수대상은 전자정보라고 보는 견해이다[8].

대법원은 일심회 사건[9], 영남위원회 사건[10] 등에서 수사기관이 컴퓨터디스켓에 포함된 디지털 증거를 압수한 행위에 대하여 위법하다고는 하지 않았으나, 디지털 정보가 압수의 대상인지, 압수의 방법과 절차가 적법한 것인지 등에 대해서는 언급하지 않았다.

그러나 전국교직원노동조합 시국선언문 사건에서는 디지털 증거에 대한 압수수색영장의 집행에서 원칙적으로 혐의사실과 관련된 부분만을 출력하거나 복사하는 방식으로 이루어져야 한다면서, 그 범위를 적극적으로 설정하고, 예외적인 사정으로 인정될 수 있어 디지털 정보를 옮겨 담아 수사기관에서 이를 열람·복사할 경우에는 복사의 대상인 디지털 정보의 왜곡이나 훼손, 오·남용이나 임의적인 복제나 복사 등을 막기 위한 적절한 조치가 이루어져야 한다고 판시하였다.

또한 압수수색의 대상은 디지털 정보의 저장매체 내에 있는 정보여야 하고, 압수목록을 작성·교부하여야 한다고 판시하여 복사하여 증거로 사용할 경우 갖추어야 할 점 등의 가이드 라인을 설정하였을 뿐만 아니라 그 절차까지도 제시하여 판시하였다.

2.2. 디지털 증거분석의 법적 성격

디지털로 된 증거물은 압수·수색절차 이후에 전문가가 한 분석 작업을 통하여 현출시켰을 때, 재판과정에서 사용할 수 있는 증거로서 가치를 가질 수 있다.

그러나 이러한 분석 작업은 새로운 법익을 침해하거나 인권을 침해하는 일은 발생하지 않지만, 그 수사 대상의 범죄와 관련이 없는 개인의 정보나 프라이버시에 관계되는 내용들이 노출될 수 있는 위험성이 도사리고 있다.

수사대상이 된 범죄사실과 관련된 내용의 디지털 정보물은 압수·수색·검증 영장의 청구와 발부에 따라 예정되어 있다고 할 수 있으나[11], 그 디지털 정보 속에 내재되어 있는 수사대상 범죄와 관련이 없는 내용의 개인정보나 프라이버시는 압수·수색·검증 영장의 청구와 발부에 포함되어 있다고 볼 수 없다.

이에 대하여 조국 교수는 영장의 집행 이후에 수사기관의 시설 내에서 이루어지는 컴퓨터 관련 증거의 검색 등에 대하여 수색·검증이라고 전제하면서 피고인이나 변호인의 참여 없이 분석하여 획득한 디지털 증거는 형사소송법 제121조, 제122조 및 제145조를 위반한 위법수집증거라고 보고 있다[12]. 그러므로 컴퓨터 전자기록이 스크린에 현출되는 것과 같이 수사기관의 관찰에 현출되었을 때 수색·검증이 시작된다고 보아 압수영장과 달리 새로운 수색·검증영장을 받아야 한다고 주장한다[13].

그렇지만 수집한 증거를 분석하는 것까지 영장을 받아야 하는 문제는 법원이 압수·수색·검증 영장을 발부할 때, 압수수색의 범위와 장소를 엄격하게 제한한다면 해결될 수 있는 문제이고, 형사절차에서는 수사의 효율성을 통한 실체적 진실 발견도 함께 고려하여야 할 문제이기 때문에, 수색·검증 영장을 다시 받아서 해결하는 것보다, 처음의 영장을 발부할 때 법원이 제한적으로 영장을 발부하는 것이 개인정보의 침해나 개인의 인권을 침해하는 문제를 방지할 수 있다고 생각한다[14].

그러므로 법원은 영장을 발부할 때 수사기관에서 수사 대상 범죄와 관련이 없는 개인의 정보와 프라이버시에 관련된 내용은 검증에서 제외할 수 있도록 제한하여야 하며, 이를 어기고 노출시켰을 경우에는 증거능력을 제한할 수 있도록 하여야 할 것이다.

대법원도 전국교직원노동조합 소속 교원 17,000여명의 서명이 담긴 미디어법 입법 중단 등을 요구하는 시국선언문 발표사건에서 저장매체 자체를 수사기관 사무실 등으로 옮긴 후 영장에 기재된 범죄 혐의 관련 전자정보를 탐색하여 해당 전자정보를 문서로 출력하거나 파일을 복사하는 과정 역시 전체적으로 압수·수색영장 집행의 일환에 포함된다고 보면서 수사기관 사무실 등으로 옮긴 저장매체에서 범죄 혐의와의 관련성에 대한 구분 없이 저장된 전자정보 중 임의로 문서출력 혹은 파일복사를 하는 행위는 특별한 사정이 없는 한 영장주의 등 원칙에 반하는 위법한 집행이 된다고 판시하고 있다[15].

3. 영장주의와 수사상 문제

우리 형사소송법에서는 일반영장을 금지하도록 하고 있으며, 이에 따라 법원도 일반영장의 발부를 금지하고 있다. 또한 영장에 기재되지 않은 대상물은 압수할 수 없도록 하고 있어, 실무상 수사기관이 압수·수색현장에서 새로운 증거물을 발견하였을 경우에는 긴급 수색이나 긴급 압수로 진행할 수 있는 경우에는 「형사소송법」 제216조와 제217조에서 규정하고 있는 절차대로 진행하고, 그렇지 않은 경우에는 새로운 영장을 발부받아야 한다는 문제가 있다고 주장한다[16].

이렇게 발견된 증거를 현장에서 확보하지 못하면, 그 증거는 수사기관이 확보할 수 없는 경우가 발생되어 그 범죄자를 처벌할 수 없는 문제점이 발생할 수 있다. 따라서 수사기관이 적법하게 발견한 증거를 확보할 수 있도록 해야 할 필요가 있다고 주장한다[17].

물론 수사기관은 범죄현장에 있는 증거물들을 사전에 정확하게 파악할 수 없기 때문에 법원에 영장을 청구할 때 정확하게 청구할 수 없다는 문제는 인정된다. 그래서 우리 형사소송법은 이러한 문제를 해결하기 위하여 긴급 압수수색의 규정을 두고 있다. 또한 긴급 압수수색의 규정으로도 해결되지 않은 문제가 발생한다면 다음의 내용과 같은 디지털 증거의 보전요구와 보전명령제를 도입할 필요가 있다고 생각한다.

4. 디지털 증거의 보전요구와 보전명령 도입 필요

수사기관이 범죄적 증거를 눈앞에 놔두고도 범죄자가 그 증거를 인멸할 수 있도록 방치한다는 문제도 검토되어야 할 것이다. 특히 최근 IT기술의 발달로 인하여 디지털 정보를 이용한 범죄행위도 늘어날 뿐만 아니라, 수사기관이 범죄수사를 위하여 수사에 들어갈 경우, 그 대상자는 디지털 정보를 일시에 삭제할 수 있는 위험성이 내재되어 있다. 이러한 점을 극복하기 위해서는 디지털 정보의 보전조치를 명할 수 있는 근거 규정이 필요하다. 즉 수사기관은 법원에 디지털 증거의 보전요구를 청구할 수 있고, 법원은 수사기관의 청구에 따라 디지털 정보의 보전명령을 발할 수 있어야 한다. 디지털 정보의 보전요구와 보전명령은 임시적 조치이므로 수사기관이 압수·수색·검증영장을 발부 받아 집행할 수 있는 기간으로 제한하여야 할 것이다.[2)]

Ⅳ. 압수·수색·검증절차에서 개인정보 활용

1. 수사절차에서 개인정보 활용

최근 수사기관이 일어난 범죄행위를 수사하면서 범죄자 즉 피의자를 특정하거나 피의자의 동선을 파악하기 위하여 가장 많이 사용되는 수법이 CCTV자료 등 전기통신의 과거자료 수색일 것이다.

이처럼 수사기관이 전기통신의 자료를 많이 활용하면 활용할수록 이를 이용하는 개인의 정보와 사생활은 정부의 제한으로부터 자유로울 수 없다는 문제가 발생한다.

새정치연합 소속인 정청래 국회의원 등 10인은 2014년. 12. 9.「통신비밀보호법」 일부개정법률안(의안번호 13005)을 발의하면서 수사기관이 통신제한조치 등을 집행하면 그 집행이 있는 날부터 90일 이내에 수사대상이 된 가입자에게 수사기관이 집행한 내역을 통지하도록 하여야 한다. 다만 국가안보·공공의 안녕질서나 사람의 생명·신체·재산에 위험을 초래하는 경우에는 1년까지 유예할 수 있도록 해야 한다고 주장하였다.

현행 「통신비밀보호법」에서는 이를 30일로 규정하고 있어, 공소유지를 위한 경우 유예할 수 있다는 규정과 상치되어 이 규정을 형해화할 수 있기 때문이다. 따라서 수사대상이 되었던 통신가입자에게 수사기관이 집행한 내역을 통지하는 기간을 현행 30일에서 90일로 변경한다면 공소 관련 처분 여부와 관계없이 국민의 사생활 비밀과 개인정보를 보호할 수 있을 것이다.

그렇지만 정청래 의원의 개정안 중 '국가의 안전보장·공공의 안녕질서를 위태롭게 할 염려가 있다고 믿을 만한 충분한 이유가 있는 경우'를 폭넓게 해석하게 되면, 수사기관은 이를 확대 적용할 수 있게 되고, 그렇게 되면 많은 수사 사례에서 수사기관이 집행한 내역의 통지를 유예할 수 있다는 문제가

2) 캐나다에서는 형사소송법이 따로 없고 형법에 함께 규정되어 있다(The Criminal Code of Canada, s. 487.012. Production order).

발생할 수 있다. 그러므로 이 조항을 엄격하게 규정하든지 그렇지 않고, 위의 내용대로 규정 된다면 법원은 이 규정의 해석을 엄격하게 해야 할 것이다.

2. 수사절차에서 개인정보 침해에 대한 미국 대법원의 태도

개인정보의 침해가 심한 유형의 압수·수색인 경우에는 수사의 조건에 해당하면 할 수 있다고 추상적으로 제시할 수 있지만, 현행 우리나라 형법과 형사소송절차법에서 이 기준을 제시하고 있는 법률이 없기 때문에 명확한 기준을 제시하지 못하고 있다.

미국의 경우에는 2008년 아놀드(Arnold)사건[18]에서 연방항소법원이 내린 판결[3] 및 2011년 같은 법원이 코터맨(Cotterman)사건에서 내린 판결에서 적용된 기준은 국경에서 출입국자 개인이 소지하고 있는 랩톱컴퓨터을 압수·수색할 때는 '합리적인 의심조차 요구되지 않는다'라는 기준을 제시하고 있다[19]. 위와 같은 문제는 전통적인 의미의 범죄로부터 사회보호와 개인의 인권보호라는 가치 기준이 디지털 정보시대에 그대로 적용될 수 있느냐가 새로운 문제로 제기되고 있다.

위와 같은 문제에 관하여 우리에게 시사점을 주는 미국의 사례로는 United States v. Antoine Jones사건이라고 볼 수 있다. 이 사건에서 연방대법원은 2012년 1월 23일 공중이 사용하는 도로에서 개인 차량의 움직임을 모니터하기 위하여 GPS 추적 장치를 부착한 것이 미국 헌법 수정 제4조에서 말하는 수색 혹은 압수(search or seizure)에 해당하는지 여부를 판단했다는 점이다[20].

미국의 수사기관은 Antoine Jones의 마약 밀거래 범죄를 수사하기 위하여 Antoine Jones의 차량에 GPS를 부착하고, 이 차량의 이동경로를 파악하여 증거자료로 제시하였고, 1심에서는 '자동차를 운전하는 사람이 공중이 통행하는 도로를 이용하여 다른 장소로 이동하는 상태에 있을 때에는 이동에 관한 프라이버시의 합리적인 기대를 가진다고 볼 수 없다'면서 이 증거를 채택하였다[21].[4] 그러나 이 사건의 항소법원인 컬럼비아 구역 연방항소법원은 '영장도 발급받지 않은 상태에서 GPS장치를 사용하여 취득한 증거는 미국 연방헌법 수정 제4조에 위배된다'며 원심의 유죄판결을 파기하였다.

미국 연방대법원도 '수사기관이 수사대상자의 개인 소유 동산인 차량에 GPS장치를 설치하고 그 차량의 움직임을 파악한 것은 수색에 해당한다[22]. 따라서 미국 연방헌법 수정 제4조는 사람, 주택, 서류 그리고 동산들(in their persons, houses, papers, and effects)을 불합리한 압수나 수색으로부터 보호받을 권리[5]를 보장하고 있는 점 등으로 보아 이를 위반한 수사방법에 기초하여 취득한 증거는 증거능력이 없다'고 보았다[23].

V. 결 론

디지털 증거에 포함된 개인정보의 압수수색도 기본권을 제한하는 강제처분이다. 따라서 헌법상 보장된 영장주의 및 강제처분법정주의를 적용받아야 마땅하다.

그래서 디지털 증거에 포함된 개인정보를 압수·수색·검증하는 절차도 당연히 헌법 또는 형사소송법에 규정된 절차에 따라 진행되어야 한다. 특히 법원은 영장주의 원칙에 따라 수사기관의 청구로 디지털 증거의 압수·수색 영장을 발부할 때 수사기관에게 디지털 증거에 포함된 개인정보가 한정된 범위 내에서 열람할 수 있도록 하고, 열람한 후에도 수사상 필요가 없거나 수사가 끝나면 바로 폐기처분하여 개인정보가 침해되지 않도록 하여야 할 것이다.

수사기관에서는 ITC의 발달에 따라 영장주의를 엄격하게 적용하면 범죄로부터 사회를 보호할 수 없다며 디지털 증거의 압수·수색에서는 일반영장의 발부를 일부 허용되어야 한다고 주장하고 있으나, 수사시관의 수사 편의를 위하여 일반영장이 허용된다면, 범죄로부터 사회를 보호하는 이익보다 수사기관이 침해하는 개인정보의 피해가 더 커질 수 있다는 점을 감안하여야 할 것이다.

이와 같은 점에서 디지털 증거를 압수·수색·검증 과정에서

3) 현재 미국의 연방 항소법원은 총 12개의 지역적으로 구분된 법원으로 구성되어 있다. 콜럼비아 구역 항소법원(U.S. court of appeals for the district of columbia circuit)과 1-11 항소법원으로 나뉜다. 한편 federal district court는 미국 대륙에만 총 89개로서 원칙적으로 최소 1주에 1개, 텍사스주 같은 경우에는 동·서·남·북의 4개 구역으로 나누어 각 연방법원을 두고 있다. 동 법원은 연방관할의 형사 및 민사사건의 사실심(하급심) 법원이라고 할 수 있다.

4) 종래 미국 연방대법원은 공도(공도)상의 전화선에 부착된 도청장치는 그것이 피고인의 주거나 사무실을 침입하는 것이 아니기 때문에 수정 제4조의 수색이 아니라고 보아왔다. 특히 1967년 캣츠(Katz v. United State)사례에서 미국 연방대법원은 '수정 제4조는 사람을 보호하는 것이지 장소를 보호하는 것이 아니며, 도청장치를 공중전화 부스에 설치하는 것은 수정 제4조의 침해'라고 판시했던 것이다.

5) 미국 연방대법원은 미국 연방헌법 수정 제4조가 불합리한 압수·수색의 보호대상으로서, '그들 자신(의 신체), 집들, 서류들 그리고 동산들'을 열거하고 있는 것은 이 규정이 재산(Property)과 밀접한 관련성이 있다는 것을 반영해 주는 문구라고 해석하고 있다.

고려하여야 할 내용을 요약하면 다음과 같다.

첫째 개인의 정보를 보호하기 위해서는 누구나 쉽게 이해할 수 있도록 「개인정보 보호법」을 비롯한 개인정보 관련 법규들을 체계화 할 필요가 있다. 현재 20여개의 개개 법률에 산재되어 있는 개인정보 보호 관련 법규들을 일원화하거나, 일원화가 어려울 경우 관련 규정에 따른 형사제재가 다르게 규정되지 않도록 통일화를 할 필요가 있다. 그래야만 어느 법률을 적용하더라도 똑같이 제제를 받도록 하여야 한다.

둘째, 디지털 증거에 포함된 개인정보도 압수·수색·검증 영장을 발부받아 압수·수색·검증을 할 수 있도록 하여 영장주의와 형사절차법정주의를 지킬 필요가 있다. 항상 범죄로부터 사회를 보호한다는 명분아래 개인의 권리가 침해되어서는 안되기 때문이다. 물론 일반영장이 규제에 따라 수사기관이 영장의 범위 설정을 잘못함으로써 범죄현장에 있는 증거물을 압수할 수 없는 문제가 발생될 수 있으나 이는 개인의 권리가 우선적으로 보호 되어야 한다는 점에서 양보할 수 없는 문제이다.

셋째, 이와 같은 수사상 문제를 개선하기 위하여 디지털 증거의 보전요구와 보전명령 제도를 도입할 필요가 있다. 수사기관이 일반영장 금지의 원칙을 제대로 준수할 수 있도록 하기 위해서는 압수·수색·검증 현장에서 발견되는 새로운 증거를 새로운 영장을 발부 받아서도 충분하게 확보할 수 있는 제도적 보완이 이루어져야 하기 때문이다.

넷째, CCTV를 통한 수사상 증거확보나 하이패스를 이용한 증거확보 과정에서도 미국 대법원의 판례 등을 검토할 필요가 있다.

REFERENCES

〔1〕 Anita L. Allen, "Dredging up the past : Life logging, Memory, and Surveillance", 75 U. Chi. L. Rev. 2008, p.63.

〔2〕 Viviane Reding, "Privacy matters - Why the EU needs new personal data protection rules", The European Data Protection and Privacy Conference, Brussels, 30 November 2010.

〔3〕 E-today, 2015. 1. 24.

〔4〕 The Constitutional Court, 2005. 7. 21, 2003헌마282·425 Full Bench.

〔5〕 SCP 2014. 7. 24, 2012다49933.

〔6〕 Lee, Chul., "Admissibility of electronic records and Investigation of Computer Crimes(Ⅱ)", Lawyers Association Journal, Vol.40. No.9, 1991. 9, p.34.

〔7〕 Lee, Eun-Mo.,"The Problems on Investigation for Electronic Records", Criminal Law Review, The Korean Criminal Law Association, Vol.23, 2005. 6, p.158; Lee, Kyung Lyul., "Grundlagende Überlegungen über Durchsuchung und Beschlagnahme von ≫ Digital Evidence ≪", Sungkyunkwan Law Review, Vol.21 No.2, 2009. 8, p.319.

〔8〕 Oh, Gi Du., Exigent, Search and Seizure of Digital Information of the Revised Criminal Procedure Act, Presentation Paper at Jurisprudence Conference, The Korean Criminal Procedure Law Association, 2012. 2. 17. p.5.

〔9〕 SCP 2007. 12. 13, 2007도7257.

〔10〕 SCP 2001. 3. 23, 2000도486.

〔11〕 Chun, Seung Soo., "A study on search, seizure and admissibility of digital evidence in criminal procedure", Dissertation, Law School, Seoul National University, 2011, p.86.

〔12〕 Cho, Kuk., "Requirements for the Legitimate Warrants for Searches and Seizures of Computer Data", Korean Journal of Criminology, Vol.22 No.1, Korean Association of Criminology, 2010. 7, p.109.

〔13〕 Supra Note 12, pp.109-110.

〔14〕 Supra Note 11, p.85.

〔15〕 SCP 2011. 5. 26, 2009모1190.

〔16〕 Lee, Wan Kyu., "Search and Seizure of the Digital Evidence and the Concept of Relevancy", Lawyers Association Journal, Vol.62 No.11, 2013. 11, pp.100-101.

〔17〕 Supra Note 16, p.101.

〔18〕 United States v. Arnold, 533 F. 3d 1003 (9th Cir. 2008).

〔19〕 Peter W. Low/John C. Jeferies, Jr./Curtis A. Bradley, Federal Courts and the Law of Federal-State Relations, 7th Ed., Foundation Press, 2011.

〔20〕 United States v. Antoine Jones, 556 U.S. 2012.

〔21〕 Joshua Dressler/Alan C. Michaels, Understanding Criminal Procedure, Vol. 1: Investigation, Lexis Nexis, 2010, p.68.
〔22〕 United States v. Antoine Jones, 556 U.S. 4 (2012).
〔23〕 United States v. Chadwick, 433 U.S. 1, 12 (1977).

저 자 소 개

김 운 곤
1993: 조선대학교
법과대학 법학과 법학사.
1995: 조선대학교
법학과 법학석사.
1998: 조선대학교
법학과 법학박사
현 재: 조선이공대학교
해양경찰과 교수
관심분야: 형사법, IT
Email : john1216@cst.ac.kr