수사기관의 정보수집에 관한 최신 해외 사례와 시사점

강철하
한국 IT 법학연구소 소장

최근 클라우드컴퓨팅 환경의 확산과 새로운 정보기술의 발전에 따라 정보의 저장과 유통이 국경을 초월하여 신속히 이루어지고 있다. 이처럼 우리의 생활관계가 디지털 환경에서 이루어지다 보니 수사기관의 입장에서도 사이버범죄나 정보기술을 악용한 테러범죄 등 다양한 범죄수사를 위해 디지털 정보의 수집이 요구되고 있다. 하지만 범죄 대응이라는 목적만으로 수사기관의 과도한 정보수집이 정당화되는 것은 아니다. 이런 점에서 본 고에서는 수사기관의 전자정보 수집에 관한 최근의 해외 사례 및 법적 쟁점을 검토하여 정책적 시사점을 제시하고자 한다.

Ⅰ. 서론

최근 정보기술의 발전과 네트워크의 고도화에 따라 정보의 저장과 유통이 전 세계적으로 이루어지고 있다. 이에 따라 수사기관 입장에서도 정보기술을 악용한 범죄에 신속히 대처하기 위해 정보통신망을 통해 유통되는 범죄혐의 정보의 수집 필요성이 점점 높아지고 있다. 하지만 만일 수사기관이 범죄수사 과정에서 과도하게 정보를 수집할 경우에는 해당 피의자뿐만 아니라 제3자의 정당한 프라이버시를 침해할 위험이 있고 기업의 정상적인 영업행위를 방해할 수도 있기 때문에 실체적 진실 발견이라는 공적 가치를 실현하고 프라이버시에 관한 개인의 권리를 제한함에 있어서 신중한 법 집행이 요구된다.

이처럼 정보기술의 발전 과정에서 “수사기관의 정보수집 필요성”과 “국민의 프라이버시 침해 위험성” 간의 긴장관계가 최근 전 세계적으로 나타나고 있으며, 최근 몇 달 동안에 나타난 이슈만 보더라도 이러한 긴장상황은 여전히 현재 진행중임을 알 수 있다. 따라서 본 고에서는 최근 해외에서 발생한 수사상 정보수집 이슈를 검토해 보고 우리에게 있어서 정책적 시사점은 무엇인지 확인해 보고자 한다.

* 본 내용은 강철하 소장(☎ 070-7010-8772, kangceo@cyberlaw.or.kr)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP 의 공식적인 입장이 아님을 밝힙니다.

Ⅱ. 최신 해외 사례

1. 미국의 사례

가. 서비스 제공자에 대한 과도한 비밀준수의무 논란

2017 년 2 월 8 일 미국 워싱턴 지방법원(US District Court for the Western District of Washington)은 정부의 비밀준수명령이 헌법에 위반된다는 Microsoft 의 주장에 대해 상급법원에서 다툴 여지가 있다는 판단을 내놓았다[1]. Microsoft 는 2016 년 4 월, 제 3 자의 컴퓨터에 저장된 전자정보에 대한 정부의 접근을 규율하는 SCA(Stored Communications Act)의 제 2705 조(b), 제 2703 조가 미국 수정헌법 제 1 조 및 제 4 에 위반된다며 소송을 제기하였다[2]. 여기서 제 2703 조는 정부가 서비스 제공자로부터 회원(subscriber)의 정보를 얻을 수 있도록 하는 권한을 부여해 주고 있다. 또한, 제 2705 조는 정부가 서비스 제공자로부터 회원의 정보를 확보한 경우, 서비스 제공자가 이러한 사실을 회원에게 통지하지 못하도록 하는 내용을 담고 있다. 예컨대, 제 2705 조(b)의 비밀준수명령(gag order)은 회원의 정보가 정부에 의해 수집되었다는 사실에 대한 서비스 제공자의 통지행위를 금지하고 있다. 이와 관련하여 Microsoft 는 동 조항들은 "특수한 상황과 관계없이(without regard to the circumstances of the particular case) 영장에 의해 수집된 정보의 소유자(회원)에게 통지해야 할 정부의 의무를 면제하고 있다"고 주장하였다. 또한, Microsoft 는 이러한 비밀준수명령은 사업자와 고객 간의 관계를 파괴하고 있으며, 실제로 연방법원이 약 20 개월에 걸쳐 3,250 회의 비밀준수명령을 발부한 바 있고, 이 중 약 3 분의 2 는 무기한(an indefinite length of time)으로 집행할 수 있는 것이었다고 주장하였다. 이처럼 동 사건에 대한 법원의 판결이 나지 않은 상황이지만 서비스 제공자의 입장에서는 수사기관의 정보 압수수색 시 수사상황에 대한 '비밀준수의무'를 부담하는 동시에 고객과의 관계에서는 개인정보의 제 3 자 제공에 관한 '통지의무'를 부담할 수 있기 때문에 일견 상호 모순되는 법적 의무에 대한 해결이 요구되고 있다.

나. 해외 서버에 저장된 고객의 이메일 정보에 대한 수색 가능성

2017 년 1 월 24 일 미국 제 2 순회 항소법원(US Court of Appeals for the Second Circuit)은 해외 서버에 저장된 고객 이메일에 접근하기 위해 정부가 SCA 규정에 근거하여 발부 받은 영장의 효력을 무효화했던 2016 년 사건에 대한 전원합의체 재심리(en banc) 요청을 거절하였다.

법원은 이미 2016 년 판결에서 미국 정부는 미국 영토 밖에 저장된 고객 이메일을 제공받기 위해 기업에게 강요할 수 없다고 결정한 바 있다. 하지만 동 판결에 대한 반대자들은 해당 사건은 국가안보와 공공안전을 위해 "예외로 삼아야 될 중요한 문제(a matter of exceptional importance)"라며 재심의를 주장하였다.

한편, 이와 달리 2017 년 2 월 3 일 미국의 펜실베이니아 동부 지방법원(US District Court for the Eastern District of Pennsylvania)은 FBI 가 발부 받은 영장에 기재된 바와 같이 해외에 저장된 e-mail 의 일부 정보를 공개하도록 Google 에게 명령하였다[3]. 그런데 이번 결정은 앞의 제 2 순회 법원의 결정과 배치되는 것이다. 이와 관련하여 Google 은 이메일이 Google 의 전자메일 서버에 분산 저장/처리되는 방식으로 인해 미국에서 어떤 이메일을 보내고 받았는지 여부를 해독할 수 없고, 제 2 순회 법원 판결에 근거하여 해외에 저장되어 있는 이메일 정보를 FBI 에게 제공하는 것을 거부하였다.

하지만 본 사건의 판사는 ① 프라이버시 침해 문제는 미국에서 발생하고, ② 전자 데이터에 대한 수색은 미국에서 발부한 영장에 따라 Google 에 의해 공개되는 것이며, ③ 요청된 정보는 SCA 조항의 적용 가능한 국내적 사용에 포함된다고 보았다. 나아가 이메일 정보의 공개가 ④ 이메일에 대한 '압수(seizure)'를 의미한 것은 아니며, ⑤ 이메일 계정 보유자의 '소유 이익(possessory interest)'에 대한 의미 있는 간섭을 야기하는 것도 아니라고 판단하였다.

이처럼 최근 미국에 있어서 해외 서버에 저장된 고객 정보를 ECPA 에 근거한 수색영장으로 수색 가능한 것인지 문제가 되고 있으나 이에 대해서는 법원에 따라 입장을 달리하고 있다.

다. 미국 정부의 통신정보 추적시스템 사용과 이에 대한 소송제기

최근 인권보호 로펌인 'Loevy and Loevy'는 시카고 경찰 당국에서 운영하는 비밀 휴대폰 추적시스템에 대해 법원에 소송을 제기했다(Jerry Boyle v. Chicago et al)[4]. 이번 소송은 2015 년 마틴 루터킹 주니어 데이(Martin Luther King Jr. Day) 흑인 시위 현장에서 경찰이 자신의 핸드폰으로부터 정보를 탈취했다고 주장하는 전국변호사협회(National Lawyers Guild) 소속 Jerry Boyle 변호사를 대신하여 제기되었다. 동 사건에서 Boyle 은 경찰의 정보 탈취로 인해 수정헌법 제 1 조 및 제 4 조에 대한 자신의 권리가 침해되었다고 주장하였다.

여기서 '가오리(stingray)'라고 불리는 문제된 시스템은 기지국(cell tower)의 기능을 모방하여 모바일폰의 위치를 특정 목표로 지정된 핸드폰과 근처의 기기 간의 통신이나 텍스트 메시지 정보를 가로채는데 사용될 수 있는 기기로 알려져 있다.

사실 상기의 '가오리'와 같은 통신정보 추척시스템은 그 동안 미국 내의 여러 법원을 통해 다양한 법적 취급을 받아 왔다. 예컨대 2016 년 11 월 제 7 순회 항소법원에서는 영장 없이 자신의 위치를 추적하기 위해 위스콘신 경찰이 추척시스템을 불법 사용하였다는 형사피고인의 주장을 배척하였다. 동 법원에서는 프라이버시에 대한 정당한 기대(a legitimate expectation of privacy)를 가질 수 없는 장소인 공공장소에서 상당한 이유(probable cause)와 체포영장에 의해 체포된 자는 경찰이 자신의 위치를 어떻게 알았는지에 대해 이의를 제기할 수 없다고 판단하였다.

하지만 이와 달리, 2014 년 매사추세츠 주 대법원(Supreme Judicial Court of Massachusetts)에서는 법집행기관이 용의자의 이동을 추적하기 위해 '가오리'와 같은 추척시스템을 사용하기 위해서는 그 전에 영장을 받아야 한다고 판단(Commonwealth vs. Shabazz Augustine)[5]하였으며, 2013 년 뉴저지 주 대법원(New Jersey Supreme Court)에서도 경찰은 휴대폰 서비스 제공자로부터 정보를 추적하기 전에 영장을 확보해야 한다는 판결을 내놓기도 하였다.

이처럼 과거 '가오리'와 같은 통신정보 추척시스템 사용에 관한 사건들은 대부분 형사사건의 맥락 속에서 검토되어 왔던 측면이 있다. 하지만 이번 Boyle 의 사건은 아직 판결이 확정되지는 않았지만, 수사기관의 추척시스템 사용과 관련하여 민사소송 차원에서 접근한 첫 번째 사례라는 의미를 가지고 있다.

라. 미국 하원의 이메일 프라이버시법(Email Privacy Act) 개정

2017 년 2 월 6 일 미국 하원(US House of Representatives)에서는 이메일과 클라우드 스토리지 등에서의 정보수집에 관한 프라이버시법 개정안(H. R. 387, 18 USC §2703-Email Privacy Act)[6]을 통과시켰다. 물론 동 법안이 성안되기 위해서는 상원(Senate)의 통과와 함께 대통령의 서명이 이루어져야 한다.

동 법안은 Google, Facebook, Dropbox 와 같은 제 3 의 서비스 제공자에게 저장된 미국 시민의 데이터를 수사기관이 수색함에 있어서 사전 영장을 얻도록 요구하고 있다. 1986 년에 만들어진 종래의 전자통신프라이버시법(Electronic Communications Privacy Act, ECPA)에 의하면, 서비스 제공자가 보유하고 있는, 고객으로부터 회수되지 않은 180 일 이내의 통신자료는 ECPA 하에서 수색영장에 의한 보호[7]를 받게 된다. 예컨대, 미국법전 §2703(a)에 의한 수색영장은 개인 서비스 제공자(a private provider) 또는 일반 공중에 서비스를 제공하는 서비스 제공자(a public service provider) 모두에게 적용되며, 서비스 제공자는 회수되지 않은 통신내용을 자발적으로라도 수사기관에 공개할 수 없다. 이와 달리 180 일 이상 저장된 데이터에 대해서는 "마치 버려진

데이터처럼" 영장 없는 수색이 허용되었다. 하지만 동 법안에서는 법집행기관이 클라우드컴퓨팅 서비스 제공자의 전산자원에 저장된 이메일에 접근하기 전에 "상당한 이유(probable cause)"에 근거한 영장을 받아야 한다는 것이 미국 수정 헌법 제 4 조의 요구사항이라는 제 6 순회 연방항소법원의 'United States v. Warshak' 판결[8]에 영향을 받아 이를 성문화하였다. 이처럼 최근 미국의 입법부 및 사법부에서는 점점 고도화되는 정보통신 환경과 광범위한 데이터 유통환경에 따라 시민의 프라이버시 보호를 위해 이른바 '디지털 적법절차(Digital Due Process)'를 강조하고 있다.

2. 유럽의 사례

가. 유럽의 정보보존법 폐기 움직임

2015 년 3 월 11 일 헤이그 지방법원(The District Court of The Hague)은 테러리즘(terrorism)과 조직범죄(organized crime) 대응을 위해 정부가 12 개월까지 네덜란드 시민의 전화기록과 인터넷 데이터를 보유[9]할 수 있도록 하는 2009 년에 시행된 데이터보존법이 EU 시민의 프라이버시권을 침해한다며 폐기 결정하였다. 물론 동 법에 따르면, 인터넷, 이메일, 텔레폰의 트래픽이나 위치 데이터 등을 보존하는 것으로 통신 내용의 보존을 의미하는 것은 아니었으며, 서비스 제공자도 정부에 대해 보관 데이터의 제출로 인한 관리비용이나 직원운영 비용의 상환을 요청할 수 있었다.

하지만 법원은 동 법이 유럽연합 기본권헌장[10]에서 규정하는 '사생활 및 가정생활에 대한 존중(제 7 조)'과 '개인정보의 보호(제 8 조)' 조항에 위반된다고 판단하였다.

마찬가지로 2014 년 4 월에는 유럽사법재판소(European Court of Justice)가 개인정보를 수집/저장하도록 규정한 EU 지침(data retention directive)을 폐기 결정하기도 하였다. 2006 년에 제정된 동 법에서는 중범죄와 테러리즘을 예방, 수사, 기소하기 위해 28 개 회원국의 인터넷서비스 제공자(ISP's)에게 적어도 6 개월에서 2 년까지 전송 데이터를 보관하도록 요구하고 있었다. 하지만 유럽사법재판소는 데이터 보존지침(data retention directive)에 따라 공중이 이용 가능한 서비스 제공자에 의한 데이터 트래픽 및 위치정보의 수집은 조직범죄나 테러리즘 대응에 대한 유용성에도 불구하고 사생활의 존중 및 개인정보 보호에 관한 기본권을 심각한 방식으로 침해하고 있다고 판단하였다[11].

사실 상기 유럽사법재판소의 결정은 아일랜드와 오스트리아 법원의 요청에 따른 것으로, 실

제 영국 정부는 전화 및 인터넷 데이터에 대한 광범위한 수집을 허용하는 이른바 '스파이 헌장(Snoopers Charter)'에 대한 계획을 가지고 있었으며, 이런 점에서 동 판결은 나중의 조사를 위해 12 개월까지 영국 시민의 인터넷 및 전화 사용기록을 수집 · 저장할 수 있도록 하는 데이터 보유 계획을 입법화하려는 움직임(Theresa May's plans)에 대한 저지를 의미한다[12].

나. 영국의 수사권법(Investigatory Powers Act 2016)의 위법성 논란

2017 년 1 월 17 일 영국의 변호사단체인 'Liberty'는 최근 통과된 정보감시법의 법적 다툼을 추진하는데 사용하기 위한 소송비용 마련과 관련하여 크라우드 펀딩(crowding funding) 목표액(1 월 17 일 현재, £18,485, USD $22,475)을 달성했다고 발표했다.

여기서 영국의 정보감시법인 수사권법(Investigatory Powers Act)[13]은 테러리즘, 사이버불링, 조직범죄의 대응을 위해 1 년의 기간까지 모든 영국 시민의 인터넷 히스토리를 기록할 수 있도록 허용하고 있다. 이에 따라 Liberty 는 이러한 입법적 조치는 전례가 없는 상당한 수준의 프라이버시 침해를 야기한다고 주장하고 있다. 특히, Liberty 의 책임자인 Martha Spurrier 는 "정부는 불안과 혼란스러움을 틈타 민주주의 역사상 가장 극단적인 감시체제를 조용히 만들었다"고 하면서 "우리의 자유에 대한 전례 없는 정당하지 않은 공격이라고 생각하기 때문에 수십만 명의 사람들이 이 법안의 폐지를 요구하고 있다"고 주장하였다.

사실 영국은 지난 몇 년 동안 정보감시법의 통과를 시도해 왔던 국가들 중에 하나다. 그 동안 유럽 국가들의 정보감시법 제정 움직임에 따라 유럽사법재판소(European Court of Justice)는 2016 년 12 월에 이러한 종류의 입법이 유럽연합 기준에 위배된다는 결정을 내놓기도 하였다[14]. 다시 말해, 유럽사법재판소는 EU 법이 정부에 의해 이메일 및 그 밖의 전기통신(트래픽 데이터 및 위치 데이터 등)의 일반적이고 무차별적인 보존을 배제(general and indiscriminate retention of e-mails and other electronic communications by governments is illegal)하고 있다는 취지를 강조한 것이다. 하지만 실제에 있어서 영국이 유럽연합을 탈퇴하였기 때문에 이러한 유럽사법재판소의 결정[15]이 영국 정부에 영향을 주기에는 한계가 있을 것으로 보인다.

다. 유럽연합 집행위원회의 전기통신 보호 규칙 제안

유럽집행위원회(European Commission)는 사생활의 존중 및 개인정보의 보호, 전기통신의 신뢰와 보안을 강화하기 위한 새로운 규칙을 제안하였다[16]. 유럽집행위원회는 이러한 제안을 통해 EU 데이터보호 프레임워크를 완성하고, Facebook 이나 WhatsApp 과 같은 더 많은 사이트에

전기통신 보호규정이 적용될 수 있으며, 새로운 비즈니스 기회의 제공 및 스팸 방지가 강화될 것으로 기대하고 있다. 또한, 동 제안은 "법집행기관의 협력 강화와 함께 높은 수준의 데이터 보호를 보장함으로써" 집행력의 향상과 국제적인 커뮤니케이션의 강화도 예상되고 있다.

여기서, 제안된 규칙(안)을 간략히 살펴보면, ① 제 1 장 일반규정에서 규칙의 제정 목적(Article 1)과 적용범위(Article 2, Article 3) 및 개념정의(Article 4)를 다루고 있고, ② 제 2 장에서는 자연인 및 법인의 전기통신 보호와 단말장치(terminal equipment)에 저장된 정보의 보호를 규정하고 있는데, 구체적으로는 전기통신 데이터의 비밀성 유지(Article 5), 전기통신 데이터의 승인된 처리(Article 6), 전기통신 데이터의 저장 및 삭제(Article 7), 엔드유저의 단말기에 저장된 정보의 보호(Article 8), 제시된 프라이버시 설정 정보와 선택(Article 10)을 규정하고 있으며, 제 5 조에서 제 8 조까지의 권리・의무에 관한 사항을 회원국의 법으로 제한할 수 있음(Article 11)을 명시하고 있다. 다만 그러한 제한이 가능한 경우에도 공공의 이익을 보호하기 위한 것으로써 민주사회에서 요구되는 필요성, 적절성 및 비례성을 갖추어야 하며 기본적 권리와 자유에 대한 본질적인 내용을 존중하여야 한다(Article 11①).

한편, ③ 제 3 장에서는 자연인 및 법인의 전기통신에 대한 통제권을 규율하고 있는 바, 전화 및 연결된 회선의 식별 표시 및 제한(Article 12)과 그 예외(Article 13), 수신차단 조치(Incoming call blocking, Article 14), 공개적으로 이용 가능한 명부(Publicly available directories, Article 15), 원치 않는 통신에 관한 사항(Article 16), 탐지된 보안위협 정보의 고지(Article 17)를 규정하고 있다. 여기서 수신차단 조치(Incoming call blocking)는 번호 기반의 통신서비스 제공자가 특정한 번호나 익명의 사람으로부터 걸려온 전화를 차단하는 조치를 의미하며, 공개적으로 이용 가능한 명부 제공자는 그 디렉토리 내에 개인정보가 포함되어 있는 경우, 해당 자연인인 엔드유저의 동의(consent)를 얻도록 하고 있다. 또한, 서비스 제공자는 그러한 데이터의 확인, 수정, 삭제 수단을 무료로 제공해야 한다. 나아가 원치 않는 통신에 관한 사항과 관련하여서는 엔드유저의 동의를 얻은 경우에 다이렉트 마케팅을 위해 전기통신 서비스를 사용할 수 있음을 규정하고 있다.

또한, ④ 제 4 장에서는 독립적인 감독 권한 및 집행에 관한 사항을, ⑤ 제 5 장에서는 사법적 구제(Article 21)와 책임(Article 22) 및 벌칙(Article 23, Article 24)에 관한 사항을, ⑥ 제 6 장에서는 위임입법과 이행입법에 관한 사항(Article 25, Article 26) 등을 규율하고 있다.

Ⅲ . 정책적 시사점

1. '비밀준수의무'와 '통지의무' 충돌 문제 해소를 위한 예외규정 명시

전술한 Microsoft 사례에서 본 바와 같이 수사기관이 서비스 제공자의 정보를 수집한 경우에 서비스 제공자에게는 '비밀준수의무'와 함께, 이와 상반된 방향에서 '고객에 대한 통지의무'가 동시에 발생할 수 있다. 이 경우 서비스 제공자는 어떤 의무를 우선해야 하는지 문제될 수 있다.

마찬가지로 우리의 경우에도 현행 「통신비밀보호법」상 통신제한조치나 통신사실 확인자료제공에 관여한 통신기관의 직원 또는 그 직에 있었던 자는 해당 조치에 관한 사항을 외부에 공개하거나 누설하는 행위를 금지하고 있다(제 11 조 및 제 13 조의 5). 그런데 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 「정보통신망법」이라 한다)에서는 이용자가 정보통신서비스 제공자 등에 대해 본인에 관한 개인정보를 이용하거나 제 3 자에게 제공한 현황의 열람이나 제공을 요청할 수 있고(제 30 조 제 2 항 제 2 호), 정보통신서비스 제공자 등은 열람 또는 제공을 요구 받으면 지체 없이 필요한 조치를 하도록 의무화하고 있다(제 30 조 제 4 항). 이런 이유에서 만일 이용자가 수사기관에서 압수 · 수색한 사항의 열람 · 제공을 정보통신서비스 제공자에게 요구할 경우 이에 응할 의무가 있는지 논란이 될 수 있다.

그런데 이와 관련해서는 우리의 경우 이미 대법원을 통해 사법적 판단이 내려진 상태다. 즉 대법원은 위 법적 쟁점에 대해 ① 「통신비밀보호법」 제 9 조의 3 은 전기통신에 대한 압수 · 수색 집행사실의 가입자에 대한 통지에 관해 별도의 규정을 두어 "통지의 주체를 수사기관으로 한정"하고 통지의 시기도 압수 · 수색 직후가 아닌 일정 기간 이후로 규정하고 있는데, 이는 전기통신에 대한 압수 · 수색의 대상이 된 자의 알권리와 수사상 기밀유지의 필요성을 함께 고려한 것으로 보이고, ② 이러한 입법 목적을 달성하기 위해서는 「통신비밀보호법」 이외의 다른 법률에 기하여 수사기관 이외의 제 3 자가 전기통신에 대한 압수 · 수색 사항을 가입자에게 별도로 통지하는 것은 제한할 필요가 있는 점, ③ 「정보통신망법」 제 5 조는 정보통신망 이용촉진 및 정보보호 등에 관해 다른 법률에서 특별히 규정된 경우 외에는 이 법으로 정하는 바에 따른다고 규정하고 있어 「통신비밀보호법」 제 9 조의 3 은 「정보통신망법」 제 30 조 제 2 항 제 2 호, 제 4 항의 특칙에 해당하는 점, ④ 전기통신사업자가 통신사실 확인자료 제공 사항에 관하여는 비밀준수의무를 부담하면서도 통신사실 확인자료 제공 사항과 불가분적으로 결합된 전기통신에 대한 압수 · 수색 사항에 대하여는 비밀준수의무를 부담하지 아니한다고 보면 통신

사실 확인자료 제공 사항에 관한 비밀준수의 취지가 몰각된다는 점에서 전기통신사업자는 「정보통신망법」 제30조 제2항 제2호, 제4항에 기한 이용자의 압수・수색 사항의 열람・제공 요구에 응할 의무가 없다고 판단하였다[17].

이처럼 대법원은 「통신비밀보호법」상의 비밀준수의무가 「정보통신망법」상의 열람・제공의무보다 우선하여 적용된다는 입장이지만, 그렇다고 해서 정보주체의 권리가 배제되는 것은 아니다. 다시 말해 압수수색 상황에서 정보주체에 대한 통지의무가 배제되는 것이 아니라 그 통지의무 주체가 '서비스 제공자'에서 '수사기관'으로 전환된다고 보아야 한다. 따라서 수사기관은 「통신비밀보호법」 제9조의3에 따라 공소를 제기하거나 공소의 제기 또는 입건을 하지 아니하는 처분(기소중지결정 제외)을 한 때 등 일정한 처분을 한 날부터 30일 이내 수사대상이 된 가입자에게 압수・수색・검증을 집행한 사실을 서면으로 통지해야 할 것이다.

다만, 이처럼 서비스 제공자의 비밀준수의무와 통지의무의 충돌문제를 해석론에 맡겨둘 경우에는 다이나믹한 시장상황에 대처해야 하는 서비스 제공자에게 구체적인 상황에서 항시 법해석 작업을 요구하는 등 "법적 불안정 상태"를 야기할 수 있기 때문에 「정보통신망법」에 분명한 요건을 설정하여 통지의무 또는 열람・제공의무의 예외조항을 신설할 필요가 있다.

2. 수사비례의 원칙과 적법절차(Due Process)에 의한 정보수집

클라우드 컴퓨팅 환경의 확산 등 정보기술의 발전 속에서 테러나 조직범죄 등의 범죄수사를 위해 수사기관은 디지털정보를 수집할 필요가 있을 것이다. 이는 최근 몇 년 사이 유럽의 정보감시법의 제정 움직임이나 미국의 통신 추적시스템의 도입 사례를 통해 확인할 수 있다.

하지만 이러한 '범죄 수사의 필요성・효율성'이 '범죄수사의 합법성・정당성'을 보장해 주는 것은 아니다. 2014년 4월 유럽사법재판소(European Court of Justice)가 적절히 지적한 바와 같이 데이터 트래픽이나 위치정보의 수집이 조직범죄(organized crime)나 테러리즘(terrorism) 대응에 유용한 수단이긴 하지만 과도한 정보수집이나 보관이 이루어질 경우 사생활의 자유와 개인정보 보호에 관한 기본권을 침해할 위험이 있기 때문에 압수수색과 같은 대물적 강제처분은 "필요한 최소한도의 범위 안에서만" 보충성・최소침해성・균형성을 고려하여 시행하여야 할 것이다(수사비례의 원칙).

또한, 우리 「형사소송법」이 임의수사를 원칙(형소법 제199조제1항 전단)으로 하면서 강제처분은 "법률에 특별한 규정이 있는 경우에 한한다(형소법 제199조제1항 후단, 강제처분법

정주의)"고 규정하고 있다는 점에서 정보기술의 발전에 따라 나타나는 통신수사, 디지털 포렌식(digital forensics) 등의 새로운 수사기법도 그것이 "임의수사의 범위를 넘는 한", 법률의 근거를 마련하여 법적 통제 속에서 활용되어야 할 것이다.

나아가 새로이 등장하는 과학수사 기법의 활용에 있어서 영장주의가 적용되는지 문제될 수 있다. 원칙적으로 영장주의는 개인의 프라이버시의 정당한 기대를 보호하기 위해 개인의 권리나 이익을 침해하는 강제처분에 관하여 사법심사를 받도록 하는 헌법상의 원칙이다[18]. 따라서 새로이 등장하는 과학수사 기법이라 하더라도 그것이 ① 상대방의 의사에 반하여 ② 권리 · 이익을 실질적으로 침해하는 처분인지 여부를 기준으로 이에 해당할 경우 영장주의의 적용을 받는다고 보아야 할 것이다.

3. 국가간 협력관계 형성 및 국제적인 정보처리 규범의 마련

앞의 미국 사례에서 검토한 바와 같이 "해외 서버에 저장된 고객 정보의 수색가능성"과 관련하여 국제적으로 합의된 기준이 존재하는 것은 아니다. 그런데 '분산처리기술'과 '가상화 기술'을 특징으로 하는 클라우드 컴퓨팅 환경의 확산에 따라 향후 이러한 문제는 지속적으로 발생할 것으로 예상된다. 이와 같이 국경을 초월하여 정보가 유통 · 저장되는 경우에 있어서 해외 서버에 대한 압수수색은 필연적으로 관할권(jurisdiction) 문제를 야기하게 된다. 물론 형식론적으로 접근해 보면, 우리나라에 소재하는 시스템을 국내에서 공격한 경우(속지주의), 해외에서 우리나라 시스템을 공격한 경우(보호주의), 우리나라 국민이 해외의 시스템을 공격한 경우(속인주의) 등의 경우에도 우리의 관할권이 인정될 수 있다. 하지만 이러한 관할권은 ① 해외 국가도 동시에 주장할 수 있고, ② 현실적으로 해외에 소재하는 시스템을 압수수색하기란 쉽지 않은 일이며, ③ 압수수색 과정에서 타국의 주권 침해 논란을 야기할 위험도 있다. 따라서 결국 해외 서버에 대한 압수수색 문제는 "타국과의 신뢰관계 구축을 통한 국제형사사법 공조의 차원에서" 접근하는 것이 바람직할 것이다.

나아가 최근 인공지능(AI), 사물인터넷(IoT), 빅데이터(Big data) 등 새로운 기술의 발전에 따라 4 차 산업혁명의 성장잠재력에 대한 기대가 높다. 이러한 기술환경의 도입과 전환을 위해서는 무엇보다 4 차 산업혁명의 기반을 이루는 핵심 인프라 자원인 데이터가 요구된다. 따라서 4 차 산업혁명이나 성공적인 데이터 혁신을 위해서는 데이터에 대한 접근성, 공개성, 정보이동성, 상호운용성을 보장할 필요가 있다. 왜냐하면, ① 데이터의 공개가 높아질수록 '데이터 혁신'의

사회・경제적 효과가 높아질 수 있고, ② 데이터 접근성 및 이동성 보장은 정보 비대칭(information asymmetries)과 데이터 집약에 의한 힘의 불균형(power inbalances) 문제를 감소시켜 줄 수 있으며, ③ 새로운 기술에 대한 표준 정립(상호운용성)은 판매업체에 대한 종속(vendor lock-in), 소비자 선택권 축소와 같은 반경쟁 활동을 예방[19]하면서 데이터의 활용성을 높일 수 있기 때문이다. 따라서 4 차 산업혁명이나 데이터 혁명의 성장잠재력을 끌어 올리기 위해서는 국내는 물론, 해외에서 유통되는 데이터에 대한 접근성, 공개성, 정보이동성, 상호운용성을 높일 필요가 있다.

하지만 이러한 기대에도 불구하고 현실은 정반대 방향으로 흐르고 있는 듯하다. 예컨대, 나이지리아는 정부의 데이터가 자국의 영토 내에서 운영될 것을 요구하고 있고, 베트남은 인터넷 서비스 제공자에게 향후 발생 가능한 정부 조사를 위해 베트남 내에 데이터의 복제본을 유지할 것을 요구하고 있으며, 호주의 전자건강기록법(Personally Controlled Electronic Health Records Act)은 호주 영토 밖으로 건강 데이터의 이전을 금지하고 있다. 나아가 2015 년 9 월 러시아에서는 가장 높은 수준의 로컬 데이터법(data localization law)으로 분류되는 법을 시행하였다. 동 법에서는 러시아로부터 수집된 개인정보는 러시아에 위치한 서버에 저장・처리되어야 한다는 “포괄적인 적용범위”를 규정하고 있기 때문에 동법에 따라 러시아 내에서 법 위반자의 웹사이트를 차단하는 것을 포함하여 관련법을 준수하도록 외국기업에 대해서도 동등한 강제력을 적용하고 있다. 물론 이러한 로컬 데이터법은 비즈니스 관점에서 부정적인 영향을 줄 가능성이 있지만, 경우에 따라 오히려 이점을 제공할 수 있다는 주장도 있다. 예컨대, 자국 영토 내의 서버에 데이터를 저장시키도록 한 법률은 그 국가에 더 많은 일자리와 투자를 늘리는데 도움이 된다는 것이다[20].

그러나 향후 도래할 4 차 산업혁명과 데이터 혁명 시대의 흐름에 올라타기 위해서는 데이터의 접근성, 공개성, 정보이동성을 높일 수 있는 대책 마련이 필요하다. 이를 위해서는 무엇보다 ‘정보 보호’ 노력을 통해 국제사회로부터 신뢰를 받는 것이 우선이다. 나아가 정보의 안전한 저장・유통・삭제 등의 처리체계를 반영한 국제규범의 개발과 활용을 위해 세계 각국과 적극적인 공동대응 노력이 필요하다. 예컨대 앞에서 검토한 유럽연합 집행위원회(EC)의 전기통신 보호 규칙의 제안 목적에 따르면, 사생활의 존중, 개인정보의 보호, 전기통신의 신뢰와 보안 강화 측면 외에도 “새로운 비즈니스 기회의 제공”을 위한 측면도 있었다는 점은 우리에게 시사하는 바가 크다.

4. 향후 정보보호 이슈 발생에 대비한 현실성 있는 이슈대응체계 마련

지금까지 수사기관의 정보수집 및 정보보호에 관한 해외의 최근 사례를 살펴 보았다. 물론 해외 유사 사례나 입법례를 통해 우리 정보보호 법제에 있어 정책적 시사점을 도출하고 개선방향을 연구하는 것은 유의미한 작업이라 할 것이다. 하지만 모든 제도가 그러하듯이 정보보호 법제의 경우에도 한 사회의 '고유성'과 '특수성'을 반영해야 하기 때문에 아무리 좋아 보이는 해외 입법례가 있더라도 우리 사회 내에서 제대로 작동할 수 있는지를 검토하지 않고 이를 기계적으로 적용하는 것은 바람직하지 않다.

이처럼 한 국가의 프라이버시법의 제정은 각 국가의 개인정보에 대한 사용 및 오용에 대한 그 사회의 뿌리깊은 관심을 반영한다. 예컨대 유럽의 국가들은 파시스트 정부가 반대자를 색출하고 처단하기 위해 개인정보를 수집했던 2차 세계 대전 당시의 개인정보의 오남용 사례에 대한 우려 때문에 엄격한 데이터보호법을 도입하는 경향이 있다. 이와 달리 미국의 경우에는 개별법(개별 산업) 중심의 프라이버시법제를 마련하여 개별 영역에 있어 유연성과 탄력성을 높이고 있다.

우리의 경우에 있어서도 최근 4차 산업혁명에 대한 기대와 새로운 정보기술의 발전에 따라 향후 "개인정보의 활용 범위를 어디까지로 할 것인지", "개인정보 활용을 위한 조건은 무엇인지" 등에 관한 상당한 논의가 진행될 것으로 예상된다. 하지만 그 과정에서 '정보의 보호 측면' 또는 '정보의 활용 측면'만을 강조하여 성급한 결론을 내리기보다는 오히려 이해관계자의 참여 속에 우리 사회의 현실을 반영한 제도가 개발될 수 있도록 이슈 발생 시 이를 해결할 수 있는 합리적 논의 구조와 대응체계를 미리 설계해 두는 것이 바람직할 것이다.

[참고문헌]

[1] Microsoft Corporation v. United States Department of Justice, No.C16-0538JLR. 2017. 2. 8. (https://www.documentcloud.org/documents/3457853-Microsoft-DOJ-ruling-on-gag-orders.html)

[2] Microsoft Corporation v. United States Department of Justice, et al, No.C16-0538JLR, 2016. 8. 29. (https://docs.justia.com/cases/federal/district-courts/washington/wawdce/2:2016cv00538/229935/46)

[3] In re Search Warrant No. 16-960-M-01 to Google; In re Search Warrant No. 16-1061-M to Google. (www.washingtonpost.com/news/volokh-conspiracy/wp-ontent/uploads/sites/14/2017/02/Opinion.pdf)

[4] http://www.loevy.com/content/uploads/2017/01/Jerry-Boyle-v.-Chicago-et-al.pdf

[5] Commonwealth v. Shabazz Augustine, No.SJC-11482, 2013. 10. 10. (https://aclum.org/sites/all/files/legal/csli/csli_20140218.pdf)

[6] 미국 의회 웹사이트(https://www.congress.gov/bill/115th-congress/house-bill/387/text)
[7] 강철하, “디지털증거 압수수색에 관한 개선방안”, 성균관대 대학원 박사학위논문, 2012, p.135,
[8] United States v. Warshak 631 f.3d 266(6th Cir. 2010). 자세한 판결문은 스탠포드대 웹사이트 참조 (http://stanford.edu/~jmayer/law696/week7/United%20States%20v.%20Warshak.pdf).
[9] 네덜란드 상원 웹사이트(https://www.eerstekamer.nl/wetsvoorstel/31145_wet_bewaarplicht)
[10] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION(2000/C 364/01)
[11] 유럽사법재판소 웹사이트(http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pagelndex=0&doclang=en&mode= req&dir=&occ=first&part=1&cid=313923)
[12] “EU court of justice overturns law that would enable ‘snoopers’ charter”, 2014. 4. 8. (www.theguardian.com)
[13] 영국 의회 웹사이트(http://services.parliament.uk/bills/2015-16/investigatorypowers.html)
[14] 유럽사법재판소 2016 년 12 월 21 일 보도자료(Court of Justice of the European Union PRESS RELEASE No 145/16, 21 December 2016)
[15] 유럽사법재판소 웹사이트(http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492 & pagelndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=735356)
[16] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications.
[17] 대법원 2015. 2. 12. 선고 2011 다 76617 판결
[18] 노명선・이완규, 「형사소송법」, 성균관대학교출판부, 2009.10, pp.157-158.
[19] 한국정보산업연합회/한국 IT 법학연구소, “제 4 차 산업혁명의 핵심은 데이터다”, FKII Report, 2016. 11, p.34.
[20] Courtney Bowman, “Data Localization Laws: an Emerging Global Trend”, jurist.org, 2017. 1. 6. (http://www.jurist.org/hotline/2017/01/Courtney-Bowman-data-localization.php)