형사정책연구 Korean Criminological Review
제27권 제4호(통권 제108호, 2016 · 겨울)

정보통신망 모니터링에 의한 범죄통제의 적합성

오 기 두*

국 | 문 | 요 | 약

정보통신망 모니터링은 국가기관이 범죄예방 목적으로나 수사목적으로, 인터넷 등 유선 또는 스마트폰 통신망과 같은 무선의 정보통신망을 통하여, 패킷단위로 전송되는 인터넷 통신회선에 접속하거나 상대방이나 ISP의 컴퓨터 서버에 침입하여, 일시적으로나 지속적으로 그 상대방 모르게 실시간 통신 내역을 엿보거나 저장된 데이터를 수집하는 것을 말한다. 이러한 정보통신망에 대한 모니터링은 정보에 대한 기본권이나 프라이버시 침해로 과잉수사 및 과잉처벌의 위험가능성을 상존케 한다. 정보통신망 모니터링, 특히 온라인 수색이라는 수사 활동을 합법화하자는 입법론이 제기되고 있으나 그러한 논의를 하기 이전에 그와 같은 수사기법이 갖는 법리적(특히 헌법적)인 문제점을 충분히 검토하여야 한다. 범죄예방이나 수사, 유죄판결의 집행을 위해 무차별적으로 정보통신망 모니터링을 실시하는 것은 세계인권선언 등 국제인권규약 및 헌법상 보장되고 있는 정보기본권, 프라이버시, 통신비밀, 표현의 자유 등을 침해할 수 있으므로, 그 한계 안에서 정보통신망 모니터링을 실시해야 한다. 그리고 형사소송법 제106조 제1항 및 제215조가 요구하는 바와 같이 수사기관이 구체적으로 범죄혐의를 잡고 있는 범죄사실과 주관적, 객관적, 시간적으로 관련된 전자정보에 한하여 수색·검증, 압수할 수 있다고 해야 한다. 수사기관이 필요로 하는 데이터가 저장되어 있는 컴퓨터 서버의 소재지가 영장에 특정되어 있지 않은데도 입력장치에 대한 압수·수색을 하면서 그 서버에 보관된 정보를 압수·수색하는 이른바 원격지 컴퓨터의 압수·수색을 해서는 안 된다. 이것은 영장주의 원칙 중 영장기재 특정의 원칙을 위반하고 당사자의 참여권을 배제하는 수사활동이기 때문이다.

❖ 주제어 : 정보통신망 모니터링, 온라인 수색, 정보기본권, 관련성, 영장주의

* 서울동부지방법원 부장판사·법학박사

Ⅰ. 서설

오늘날의 디지털정보 시대에서 현실로 등장하고 있는 다음과 같은 사례들을 생각해 보자.

사례 1 :

가. 국제학술지 사이언스는 최근 미국 피츠버그 경찰국이 2016년 10월부터 시행하고 있는 '크라임 스캔'(CrimeScan) 프로그램을 소개했다. 카네기멜런대 컴퓨터 과학자들은 과거 범죄기록을 토대로 앞으로 범죄가 발생할 가능성이 높은 지역과 시각을 컴퓨터 화면에 표시하는 기술을 개발했다. 경찰은 범죄 예상 지역 순찰을 강화한다. 범죄가 일어난 뒤에 경찰이 대응을 하는 것이 아니라 사전에 미리 경찰이 현장에 출동하는 이른바 '예측 치안'(predictive policing)이다.[1] 예측 치안은 과거 범죄 기록과 범죄에 영향을 미치는 요인에 대한 방대한 데이터를 기반으로 하여 소프트웨어로 과거 범죄 데이터에서 패턴과 연관성을 조사하고, 과거 범죄에 연루된 사람의 사회관계를 분석한다. 컴퓨터 알고리즘으로 미래에 범죄가 언제 어디서 발생할지 예측하고 잠재적 범죄자나 피해자를 확인한다. 그리하여 범죄 발생 예상 지역에 경찰을 집중 배치하고 잠재적 피해자에게 위험에 처했음을 고지하거나 사회적 지원을 제공하는 것이다.[2]

나. 서울중앙지방검찰청은 2014. 9. 25. '사이버 허위사실 유포 수사전담팀'을 구성하고 인터넷 모니터링을 강화하겠다고 발표하였다. 그 발표 이후 같은 해 10. 9. 인터넷 시장조사업체 랭키닷컴에 따르면 같은 해 9. 28. - 10. 4.까지 메신저 '카카오톡'의 국내 이용자는 하루 평균 2605만명으로 집계되어 1주일 전에 비해 41만명이 줄어든 것으로 나타났다. 카카오톡 이용자들 사이에 메

1) 조선일보 이영완 과학전문기자, "'예측 치안' 프로그램 시행 영화 '마이너리티 리포트' 현실로", 위 신문 2016. 10. 6.자 B11쪽.

2) 위 조선일보 신문기사의 그림 도표 참조.

신저로 주고 받는 개인적 대화까지 당국이 모두 들여다보는 거 아니냐는 불안감이 확산된 것이다.[3)]

사례 2 :

대한민국 검찰이 휴대폰에 들어 있는 디지털 정보를 분석하는 '모바일 포렌식' 기술을 대폭 강화한다. 삼성 갤럭시 S7 같은 최신 휴대폰의 보안 기능을 무력화하는 것은 물론 휴대폰 속 주요 앱(응용프로그램) 100개를 추가로 '해킹'하는게 목표다. … 2016년 7월 21일 검찰 등에 따르면 대검찰청은 휴대폰에 설치된 보안기능과 대부분 앱의 사용 내용을 한 눈에 들여다 볼 수 있는 '모바일 포렌식' 기술 개발을 민간 전문 업체에 의뢰해 2016년 말까지 끝낼 예정이다.[4)]

오늘날 디지털정보 시대에 국가나 거대 기업, 그리고 개인에 의한 전자감시는 야누스처럼 긍정적인 얼굴과 부정적인 얼굴을 함께 갖고 있다. 국가는 전자정보 시스템을 이용하여 사회의 안전을 보장하고, 복지정책을 추진하며, 범죄억지를 도모한다. 정보통신 기술의 발전에 따라 정보통신 환경의 공유성으로 인해 개인들도 감시체제에 의한 속박을 받는다고 생각하기보다 감시시스템에 순응하여 사회에 참가한다고 생각하는 경향이 크다.[5)] 2016년 현재 글로벌 정보기술(IT) 기업의 최대 격전장으로 떠오른 클라우드 컴퓨팅 기술은[6)] 이러한 의식을 가속화하고 있다. 또한 개인정보가 거래의 대상이 되고 있는 정보화시대에 개인정보자기결정권을 불가침의 절대적인 기본권인 것처럼 인식하는 것도 시대의 흐름과 동떨어진 것이라고 볼 여

3) 이인묵·윤주헌 기자, "하루 55억건 오가는 '카톡' … 실시간 감시는 불가능", 조선일보 2014. 10. 10.자 A3쪽 및 박순찬 기자, "카톡 등 메신저 이용자들 '사이버 亡命'", 조선일보 2014. 9. 29.자 A8쪽.

4) 고윤상 기자, "檢, 모든 국산 휴대폰 보안기능 뚫는 기술 연내 개발", 한국경제, 2016. 7. 22.자 A29쪽.

5) David Lyon,『Surveillance Society : Monitoring Everyday Life』, Buckingham : Open University Press(2001), pp. 3-35. ; 박정훈, "전자감시와 프라이버시 관계 정립에 관한 연구", 법조협회,『법조』 통권 제645호(2010. 6.), 139쪽 및 주26), 150쪽 이하.

6) 이호기 기자, "IT 공룡들 클라우드 격돌", 한국경제 2016. 9. 28.자 D1쪽.

지도 있다.[7] 그러나 국가가 실시하는 유·무선의 정보통신망에 대한 모니터링은 정보에 대한 기본권이나 프라이버시 침해로 과잉수사 및 과잉처벌의 위험가능성을 상존케 한다. 수사기관이나 정보기관에서 스마트폰 통신 내역을 해킹하는 프로그램을 개발하거나 구매하여 대규모의 민간인 사찰을 하고 있는 것이 아닌가 하는 불안감이 급속히 사회 전체적으로 퍼져갈 수도 있다.[8] 이 글은 이러한 정보통신망 모니터링이 갖는 법리적인 문제점을 고찰해 보고자 작성되었다.

Ⅱ. 정보통신망 모니터링 기법

1. 의의

정보통신망 모니터링은 국가기관이[9] 범죄예방 목적으로나 수사목적으로, 인터넷 등 유선 또는 스마트폰 통신망과 같은 무선의 정보통신망을 통하여 동의 없이 패킷 단위로 전송되는 인터넷 통신회선에 접속하거나 상대방이나 ISP의 컴퓨터 서버에 침입하여, 일시적으로나 지속적으로 그 상대방 모르게 실시간 통신 내역을 엿보거나 그에 저장된 자료를 수집하는 것을 말한다. 예컨대 수사기관이 잠재적 범죄자로 여기고 있는 개인의 컴퓨터에 해킹프로그램을 설치하여 그 컴퓨터를 통하여 교환되는 모든 통신내역이나 그 컴퓨터에 저장된 데이터를 감시하고 획득하는 것이[10] 이

7) 정찬모, “직장 내 전자우편 모니터링 규제의 신조류와 시사점”, 법조협회, 『법조』 통권 제645호 (2010.6.). 207, 8쪽 ; 강성주(미래창조과학부 정보화전략국장), “경계에 선 ‘개인정보 자기결정권’”, 대한변협신문, 2014. 9. 1.자, 10쪽.

8) 우리나라에서 2015년 7월 경 국가정보원이 이탈리아 회사에 국내용 카카오톡과 갤럭시폰의 해킹 기능 개발을 의뢰한 사실로 인해 정치권에서 국가정보원에 의한 민간인 상대의 도·감청 의혹이 일기도 하였다. 정우상 기자, “해킹 프로그램 구입 논란”, 조선일보 2015. 7. 15.자 A6쪽, ; 조의준·이정원 기자, “해킹 프로그램 핵심의문점과 국정원의 해명”, 조선일보, 2015. 7. 17.자 A4쪽 기사. 이 글의 주10), 주22)에 기재한 사건과 같은 사건이다.

9) 국가정보원·미래창조과학부·방송통신위원회·안전행정부 발간, 『국가정보보호백서』(2014) 참조.

10) 위키리크스는 2015. 7. 14.경 트위터를 통해 이탈리아 「해킹팀」이 2013. 9. 16.경 'SKA'(South Korea Army Intelligence)를 도와 한 변호사(lawyer)의 컴퓨터에 해킹프로그램을 설치했다는 업체 직원의 이메일을 공개한 바 있다. 정우상 기자, “위키리크스, ‘국정원, 변호사 1명 해킹’”, 조선일보 2015. 7. 16.자 A6쪽 기사.

에 해당한다. 피의자에 대한 정보를 보관하는 제3자가 자국에 서버를 두고 있지 않은 경우 패킷감청이 유력한 강제수사 방법이 된다.[11] 핸드폰으로 이루어지는 실시간 통화내역을 감청하는 것도 이에 해당한다. 인터넷 등 유선통신망이나 스마트폰의 무선통신망을 이용한 통신에 관한 메타정보를 대량으로 수집하는 수사기관의 활동도[12] 전자적 정보통신망에 대한 모니터링의 한 방법이라고 할 수 있다. 물론 인터넷 홈페이지 게시판 등에 공개된 정보를 국가기관이 모니터링하는 방법으로 행해질 수도 있다.

이들 전자적 정보통신망에 대한 모니터링은 온라인상에서 행해질 때 온라인 모니터링이라고 하지만, 반드시 유선통신망에 대한 모니터링을 의미하지는 않는다. 스마트폰 통신 등 무선통신망에 대한 모니터링도 행해질 수 있다. 전자적인 온라인 모니터링이나 무선통신망에 대한 모니터링은 전자감시(electronic surveillance)의[13] 한 수단이지만, 모니터링은 그러한 전자감시를 포함하는 좀 더 넓은 범위의 감시수단을 의미하는 용어라고 할 수 있다. 정보통신망에 대한 모니터링은 실시간 전자통신 내역을 감시하는 감청의 방식으로 행해지거나, 이미 통신업체 소유의 컴퓨터 서버에 저장되어 있는[14] 통신 내역을 탐색하는 온라인 수색의 방식으로 행해질 수도 있기 때문이다. 온라인 수색은 일회에 한하여 타인의 컴퓨터시스템에 저장된 데이터를 복제하기 위해 비밀리에 접근하는 '온라인 열람'과 다소 장기간 작동 중인 컴퓨터시스템의 이용상황을 비밀리에 감시하는 '온라인 감시'로 구분할 수 있다.[15] 앞서

---

11) 이숙연, "전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여", 한국헌법학회, 『헌법학연구』 제18권 제1호 (2012. 3.), 8쪽.

12) 미국 2nd Circuit Court의 ACLU et.al. v. NSA et. al.(2015. 5. 7.자) 판결.

13) 전자적 감시와 미국 연방수정헌법 제4조에 관련된 미국 판례와 입법례의 흐름을 잘 정리한 문헌으로, 윤지영, "미국의 통신감청 관련 법규 및 논의 동향", KiC『형사정책연구소식』(2016 봄), 34쪽 이하 ; 손지영·김주석, 『디지털 증거의 증거능력 판단에 관한 연구』, 대법원 사법정책연구원(2015), 88-92쪽 참조.

14) 수신이 완료된 문자메시지 내용을 열람하는 행위는 통신비밀보호법상의 '감청'은 아니다. 대법원 2012. 10. 25. 선고 판결. 법률신문, 2012. 11. 5.자 5쪽 기사 참조.

15) 박희영, "예방 및 수사목적의 온라인 비밀 수색의 허용과 한계",『원광법학』 제28권 제3호(2012), 154쪽 및 그곳 주1)에서 인용한 Sieber의 논문 참조. 다만, 박희영은 국가가 타인의 컴퓨터시스템에 비밀리에 접근하는 행위를 온라인 접근(Online-Zugriff)이라고 한 후 그 하위개념으로 일시적으로 이루어지는 온라인 접근을 온라인 수색(Online-Durchsuchung), 다소 장기간에 걸쳐 이루어지는 온라인 접근을 온라인 감시(Online-Überwachung)이라고 지칭하여 이 글의 본문에서 사용한 용어

든 사례 2.의 경우와 같이 개인의 휴대폰에 저장되어 있는 통신내역을 탐색, 압수하는 방식도 넓게 보아서는 정보통신망에 대한 모니터링이라고 할 수 있다. SNS 서비스에 가입하여 이를 활용하는 이용자들의 대화 내용, 사진, 동영상 등이 저장된 서비스 업체들의 서버에 대한 수색이 이루어질 수도 있다. 네트워크를 통해 전송되는 전자증거를 공판정에 제출할 필요가 커지게 됨에 따라,[16] 정보통신망 모니터링은 주로 범죄수사 단계에서 행해진다. 그러나 그 모니터링은 형집행 과정에서 행해질 수도 있다. 나아가 이 글의 첫머리에서 든 사례1.의 경우들처럼 일반적인 범죄예방 목적에서 범죄혐의자나 범죄혐의가 특정되지 않은 상태에서 온라인 모니터링이 행해질 수도 있다. 이 글에서는 이들을 모두 아우르는 말로 정보통신망 모니터링이라는 용어를 사용하면서, 그 범주에 드는 국가기관의 범죄예방 경찰활동, 범죄수사 활동, 형집행 활동 등에 관련된 법리적 문제를 고찰한다.

2. 전자기술적 측면

IT 기술적으로는 대상이 특정되지 않은 인터넷 감시도 매우 저렴한 비용으로 신속하게 하는 것이 가능하다. 범죄통제를 목적으로 개인에 대한 감시를 의도하는 국가기관은 네트워크상의 특정 주요지점을 흘러가는 트래픽을 잡아내기 위해 유동네트워크(driftnet)를 설치하면 된다. 자동화된 트래픽 필터링과 처리는 국가기관이 미리 선정한 조건에 합치되는 데이터를 흘려보내거나 통상적이지 않은 데이터를 보내는 인물을 잡아낼 수 있도록 해 준다. 국가기관은 그러한 불특정 대상에 대한 감시활동을 통해 알게 된 정보를 저장, 보관하여 둔 후 미래의 어떤 수사 등 범죄억지 활동을 위해 해당 정보를 이용할 수 있다.[17] 빅 데이터(big data)로부터[18] 가치 있

아닌 용어를 혼용하고 있다. 박희영, "독일에 있어 경찰에 의한 '예방적' 온라인 수색의 위헌여부", 경찰대학, 『경찰학연구』 20호(2009.8.), 185쪽.

16) 정교일, "디지털증거의 압수와 공판정에서의 제출방안", 대검찰청, 『형사법의 신동향』 통권 25호(2010. 4.), 128쪽.

17) John Palfrey, "The Public and Private at the United States Border with Cyberspace", 『Missipi Law Journal』(Winter 2008), 78 Miss. L.J. 241, 280 ; 오기두, "주관적 관련성 있는 전자정보만의 수색·검증, 압수", 사법발전재단, 『사법』 28호(2014. 6.), 204쪽, 주10).

18) 강성주(미래창조과학부 정보화전략국장), "'빅 데이터'는 미래를 만들어 나가는 열쇠", 대한변협신

는 정보를 찾아내기 위해 선택(select), 탐색(exploring), 분석 및 모델링(modeling) 하는 데이터 마이닝(Data Mining) 기법이나[19] 웨어러블 디바이스도[20] 정보통신망 모니터링을 가능하게 하는 기술적 전제조건이 될 것이다. 국가가 정보통신망 모니터링을 이용하고자 하는 욕구를 갖는 것은 인터넷이나 다른 디지털 네트워크가 갖는 감시 친화적인 속성 때문이다. 유비쿼터스 사회 구현에 이바지하는 무선주파수 신원확인(Radio Frequency Identification, RFID), 폐쇄회로티비(CCTV), 스마트폰, 사물인터넷(IoT) 등은 모든 사람과 사물에 대한 위치·상태 등의 전자감시를 가능하게 한다. 그리고 오늘날의 인터넷 기술은 인터넷 교환점(Internet Exchange Point), 인터넷 서비스제공업체(Internet Service Provider, ISP), 블로킹 호스트 같은 수많은 포인트를 네트워크에 설정해 두는 것을 그 속성으로 하고 있다. 스크린세이버, 게임 프로그램, 채팅프로그램 등 컴퓨터에 저장되어 있거나 그 컴퓨터를 통과하여 흘러간 데이터로 다량의 수많은 개인정보가 수집될 수도 있다. 지금은 네트워크상으로 국가가 개인을 감시하기가 참으로 쉬워진 시대라고 하지 않을 수 없다.[21]

수사단계에서 정보통신망 모니터링은[22] 예컨대 패킷 감청으로 하게 된다. 원래

문, 2015. 2. 2.자, 11쪽.

19) Madhu. G et al., “Hypothetical Description for intelligent Data Mining”, 『International Journal on Computer Science and Engineering』 Vol.2. No.7(2010), p. 2349. ; 양종모, “수사기법으로서의 데이터 마이닝에 대한 법적 고찰”, 대검찰청, 『형사법의 신동향』 통권 40호(2013. 9.), 145쪽 이하 및 150쪽 주9).

20) 이영완 기자, “어제 진짜 야근했어? 웨어러블 기기는 다 알고 있다”, 조선일보 2015. 1. 6.자 A2쪽 기사 참조.

21) Jonathan Zittrain, “Internet Points of Control”, 『44 B.C.L.Rev. 653』(2003) ; Marjorie A. Shields, “Annotation, Fourth Amendment Protections, and Equivalent State Consitutional Protections, as Applied to the Use of GPS Technology, Transporter, or the Like, to Monitor Location and Movement of Motor Vehicle, Aircraft, or Watercraft”, 『5 A.L.R.6th 385』 (2005) ; 위 John Palfrey, “The Public and the Private at the United States Border with Cyberspace”, at 243. : 오기두, 위 “주관적 관련성 있는 전자정보만의 수색·검증, 압수”, 205쪽, 주14).

22) 우리나라에서 2015년 7월경 국가정보원 직원이 이탈리아 「해킹팀」사로부터 구입한 해킹프로그램(Remote Control System, RCS)으로 내외국인을 상대로 스마트폰 해킹을 하였다는(이른바 민간인 사찰) 의혹이 일어 관련 직원이 자살하고 국회 정보위가 조사에 나섰으며, 관련 단체가 찬반 성명을 발표하는 등 정치·사회적 혼란이 일었다. 이 사건도 정보통신망 모니터링에 의한 범죄예방이나 범죄통제에 관련된 사례로 들 수 있겠다. 안준호 기자, “민낯 드러낸 사이버安保 시스템” 등 조선일보 2015. 7. 17.자 A4쪽 기사들 참조, 그 밖에 위 신문 2015. 7. 27.자 A1쪽, A35쪽 기사 및 광고도 참조.

인터넷은 분산형 네트워크, 패킷전송망 방식을 특징으로 한다. 즉 개별 컴퓨터 사이에 데이터를 동일한 경로로 전달하는 방식이 아닌, 데이터를 패킷이라는 최소 단위로 쪼개어 이를 통신망의 상황에 따라 각각 다른 경로를 통해 보낸 뒤 목적지에 다다라 다시 온전한 데이터로 재구성하는 전달 방식을 택하고 있는 것이다.[23] 인터넷 전용선을 통하여 흐르는 전기신호 형태의 패킷도 유선·무선·광선 및 기타의 전자적 방식에 의하여 송·수신되는 음향·문언·부호 또는 영상으로서 전기통신에 해당하는 것이므로 통신제한조치의 요건을 구비한 경우에는 인터넷 전용선(패킷)에 대한 통신제한조치도 통신비밀보호법상 가능하다.[24]

3. 정보통신망 모니터링의 그늘

디지털 정보에 의한 감시와 분석 기술이 더 강력해지고 효율적으로 될수록 국가는 영장주의나 다른 절차적 기본권 보장 장치를 잠탈하고서라도 문제 발생 이전에 잠재적인 문제아들을 더 효과적으로 잡아내고자 하는 욕구를 강하게 갖게 된다.[25] 특히 전체국가적 감시체제(National Surveillance State)는 사후적인 체포와 구속보다 사전적인(ex ante) 범죄예방에 집착하는 속성을 갖는다. 그것을 통해 전체주의 국가는 전통적인 헌법상의 권리장전규정(Bill of Rights)을 우회하는 수단을 찾으려고 끊임없이 시도할 것이다. 현대 디지털 정보화 사회에서 이러한 전체주의 국가가 등장할 위험가능성은 상존한다.[26] 디지털 정보의 비휘발성으로 인해 작성한 글이나 전송한 메시지가 사라지지 않고 유·무선의 정보통신망에 언제까지나 떠다닐 수 있게 된[27] 현대 사회에서 역설적으로 전체주의의 망령이 출몰하고 있는 것이다. 정보

23) 정관영, "패킷(packet) 감청 허용의 한계", 대한변협신문 2014. 10. 13.자, 13쪽.

24) 서울중앙지방법원 2011. 12. 22. 선고 2009고합348 판결 ; 서울고등법원 2012. 6. 8. 선고 2012노82 판결 ; 대법원 2012. 10. 11. 선고 2012도7455판결 참조.

25) Jack M. Balkin, "The Constitution in the National Surveillance State", 『Minnesota Law Review』 (2008.11.), (93 Minn. L. Rev. 1), 16. ; 오기두, 위 "주관적 관련성 있는 전자정보만의 수색·검증, 압수", 206쪽, 주18).

26) 위 Jack M. Balkin, "The Constitution in the National Surveillance State", at 15. ; 오기두, 위 "주관적 관련성 있는 전자정보만의 수색·검증, 압수", 251쪽, 주121).

27) 최창호, "기술의 발전과 프라이버시", 대한변협신문, 2015. 1. 19.자, 13쪽.

통신망 모니터링을 통해 수집한 자료는 디지털 방식으로 쉽사리 저장, 복제, 분석, 전파할 수 있다. 그리고 그 디지털 데이터는 전자적 서버에 영구적으로 저장될 수 있다. 이제 현대 국가는 개인의 행위를 "절대로 잊지 않는 국가"(State that Never Forgets)가 된 것이다.[28] 그래서 이 글의 첫머리에 제시한 사례 1.나.에서와 같이 정보통신망 모니터링으로 헛소문을 퍼트린 사람을 잡아내겠다는 국가의 시도는, 마녀 행각을 하는 것을 보았다는 헛소문 만에 근거해 자행된 마녀재판만큼이나[29] 국민의 기본권을 심각하게 침해하는 결과를 초래할 수 있다.

정보통신망 모니터링은 수사기관이 독자적으로 행하기는 어렵고, 인터넷 서비스 제공업체의 협력을 얻거나 강제처분의 방식으로 이루어져야 한다. 이때 전기통신사업자 등 인터넷 서비스업체가 수행하는 이용자들의 인터넷 이용행태 관련데이터 수집도 권위적인 정부에 의해 감시수단으로 이용될 수 있다. 예컨대 2008. 2. 파키스탄 정부가 이슬람에 반대하는 내용의 동영상이 게시된 싸이트(YouTube.com)에 자국민들이 접속하는 것을 금지하기 위해 파키스탄의 ISP에게 특정 URL에 그 ISP 이용자들이 접속하지 못하도록 조치하였다. 그러자 많은 파키스탄 사람들이 어떤 회사(AnchorFree)가 제공하는 무료 프로그램(Hotspot Shield)을 이용하여 위 싸이트(YouTube.com)에 접속하려고 시도하였다. 그런데 위 회사(AnchorFree)는 이용자들의 웹 브라우징 습관을 추적하는 광고회사였다. 즉 위 프로그램(HotSpot Shield) 이용자들은 그 회사(AnchorFree)에 웹 브라우징을 하면서 교환된 모든 데이터를 제공한 셈이었다. 그래서 원래의 의도와는 달리 위 회사(AnchorFree)는 자국민들의 특정 싸이트(YouTube.com) 접속을 금지하려한 파키스탄 정부의 조치로

---

28) New York Civil Liberties Union, "Who's watching?: Video Camera Surveillance in New York City and the Need for Public Oversight"(2006), http://www.nyclu.org/pdfs/ surveillance _cams _report _121306.pdf ; Patricia L. Bellia, "The Memory Gap in Surveillance Law", 『75 U. Chi. L. Rev』, 137, (2008). at 137-38, 148-49. ; 오기두, 위 "주관적 관련성 있는 전자정보만의 수색·검증, 압수", 218쪽, 주52).

29) 1692년 미국 매사추세츠 주의 인구 500여명에 불과한 작은 마을인 세일럼(Salem)에서 마녀행각을 하는 것을 보았다는 헛소문에 근거해 유죄판결을 받고 수감된 마을사람이 150명이나 되었는데, 그 중 19명이 교수형에 처해졌고, 1인은 고문으로 사망했으며, 아기 등 5명이 감옥에서 사망하였다. 개 두 마리도 마녀재판을 받고 죽임을 당했다. '저 피고인이 마녀다!'라는 공판정의 증인이 한 증언(헛소문)만으로 가히 미친 짓이라고 불러도 좋을 사법살인이 행해진 것이다. Carol Domblewski, 『The Salem Witch Trials』, Scholastic Inc., (2003).

인해 파키스탄 사람들을 감시하는 역할을 수행하게 되었다.[30] 이러한 인터넷 사용 제한 조치도 국가가 전산망 중립성을[31] 훼손한 경우에 해당한다. 전산망 중립성에 관해서는 거대 전기통신사업자에 의한 망중립성 침해 뿐 아니라,[32] 국가에 의한 전체주의적 통제도 논의의 대상으로 삼아야 할 것이다. 인터넷 통신에 관해 통신비밀보호법에 따른 적법한 감청 뿐만 아니라 법관의 영장 없는 위법한 정보통신망 모니터링이 범죄통제 욕구에 충만한 국가기관에 의해 행해질 가능성도 충분히 있기 때문이다. 설령 법관의 영장을 발부받아 정보통신망 모니터링을 하여 범죄통제를 꾀한다고 하더라도 그것이 반드시 형사정책적으로 적절하냐 하는 점도 검토해야 한다.

Ⅲ. 정보통신망 모니터링에 의한 범죄억지

1. 입법례 검토

아래에서 보는 입법례는 정보통신망 모니터링 중 범죄수사와 관련된 규정인데, 논자에 따라 뒤에서 보는 원격지의 컴퓨터 압수수색을 허용하는 입법례로 들고 있는 것들이다.[33] 그러나 다음에서 구체적으로 살펴보는 바와 같이 이들 외국 입법례가 수사에 필요하다는 이유만으로 정보통신망 모니터링을 직접적으로 또는 일반적으로 허용하고 있는 것은 아님을 유의할 필요가 있다. 그러므로 이하의 제도를 들어 우리 형사소송법상의 압수수색 법제에서도 정보통신망 모니터링, 그 중에서도 원격지 컴퓨터 시스템에 대한 온라인 수색을 허용해야 한다고 주장하기는 어렵다고 보인다. 정보통신망 모니터링을 일정한 경우 허용하고 있는 단초를 마련하고 있는 입법례로서 참고하는 선에서 그쳐야 한다고 하겠다.

---

30) 위 John Palfrey, “The Public and the Private at the United States Border with Cyberspace”, at 259-60. ; 오기두, 위 “주관적 관련성 있는 전자정보만의 수색·검증, 압수”, 227쪽, 주73).

31) 망중립성에 관해서는 윤성주, “망중립성에 관한 규제 개관”, 서울대학교 기술과법센터, 『LAW & TECHNOLOGY』 제10권 제3호 (2014.5.), 69-80쪽 참조.

32) 강태욱, “‘망 중립성’ 논의”, 법률신문, 2016. 9. 26.자, 15쪽.

33) 국가인권위원회, 『사이버 수사 및 디지털 증거수집 실태조사』(2012.12), 212-217쪽.

가. 우선 일본 형사소송법 제99조 제2항 및 제218조 제2항은 다음과 같이 규정하고 있다.

「압수할 물건이 컴퓨터인 경우, 그 컴퓨터에 전기통신회선으로 접속되어 있는 기록매체로서, 그 컴퓨터로 작성되거나 변경된 전자적 기록 또는 그 컴퓨터로 변경 또는 소거할 수 있는 것으로 여겨지는 전자적 기록을 보관하기 위하여 사용되고 있다고 인정하기에 족한 상황에 있는 것으로부터, 그 전자적 기록을 그 컴퓨터 또는 다른 기록매체에 복사한 후 당해 컴퓨터 또는 그 다른 기록매체를 압수할 수 있다.」[34)]

위 일본 형사소송법 규정은 전기통신으로 접속되어 있는 기록매체를 대상으로 하고 있는 점에 비추어, 피압수자가 서버에 접속하여 작업 중인 경우나 기타 휘발성 정보를 획득하는 경우가 아니라, 이미 과거에 원격지 컴퓨터에 저장되어 있는 데이터에까지 전산망으로 접속하여 수색할 수 있는 권한을 수사기관에 부여한 법률이라고 단정하기는 어렵다.[35)]

나. 그리고 유럽평의회(Council of Europe) 사이버범죄 방지 조약(Convention on Cybercrime) 제19조는[36)] 「저장된 컴퓨터 데이터의 압수수색」(Search and seizure of stored computer data)이라는 제목 아래에 다음과 같은 내용을 규정하고 있다.

「1. 각 체약당사국은 영토 내에 있는 다음의 대상을 수색하거나 그와 비슷한 접근을 할 수 있도록 관할 기관에 필요한 권한을 부여하는 입법조치나 기타 대책을 강구하여야 한다.

a. 컴퓨터시스템 또는 그 일부와 그곳에 저장된 데이터, 그리고

34) 差し押さえるべき物が電子計算機であるときは、當該電子計算機に電氣通信回線で接續している記錄媒體であつて、當該電子計算機で作成若しくは変更をした電磁的記錄又は當該電子計算機で変更若しくは消去をすることができることとされている電磁的記錄を保管するために使用されていると認めるに足りる狀況にあるものから、その電磁的記錄を當該電子計算機又は他の記錄媒體に複寫した上、當該電子計算機又は當該他の記錄媒體を差し押さえることができる.

35) 오길영, “사이버 수사 및 디지털 증거수집 실태조사 결과 발표 토론문”, 국가인권위원회, 『사이버 수사 및 디지털 증거수집 실태조사 결과 발표 및 토론회』(2012.12), 50쪽.

36) http://edoc.coe.int/en/cybercrime/6559-convention-on-cybercrime-prtocol-on-xenophobia-and-racism.html(2016.10.17.방문).

b. 컴퓨터데이터가 저장되어 있을 것으로 여겨지는 컴퓨터데이터 저장 장치

2. 각 체약당사국은 관할 기관이 위 1.a.와 같이 특정 컴퓨터시스템이나 그 일부를 수색하거나 수색에 유사한 접속을 할 수 있고, 그 영토 내에 있는 다른 컴퓨터시스템이나 그 일부에 찾고자 하는 데이터가 저장되어 있다고 믿을만한 근거가 있으며, 그 데이터에 원래의 시스템에서 합법적으로 접근할 수 있거나 데이터를 이용할 수 있을 때, 당해 기관이 신속하게 그 다른 시스템에까지 확장하여 수색하거나 수색에 유사한 접속을 할 수 있도록 필요한 입법적 조치나 기타 대책을 강구하여야 한다.」[37]

위 제19조 제2항에 의하면, ① 정보통신망 모니터링의 대상이 된 컴퓨터서버가 체약국의 영토 내에 있지 않고 국외에 있거나, ② 수사기관 등 관할 기관이 원하는 데이터가 있을 개연성마저 없이 막연히 범죄자를 적발하기 위해 정보통신망 모니터링을 하거나, ③ 다른 컴퓨터시스템에 접속하거나 그 시스템에서 제공하는 데이터를 원래의 시스템에서 이용하는 것이 불법적이라면(또는 정당하지 않다면), 정보통신망 모니터링을 할 수 없다. 또한 위 조약이 바로 체약당사국의 국내법으로 직접 적용되는 것은 아니므로, 각 체약당사국은 원격지 컴퓨터시스템을 탐색할 수 있도록 국내 법집행기관 등 관할기관에 권한을 부여하는 입법조치를 하거나 그 밖의 수단을 강구할 의무를 지고 있을 뿐이다.[38]

---

37) 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a. a computer system or part of it and computer data stored therein; and
b. a computer-data storage medium in which computer data may be stored in its territory.
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

38) 오길영, 위 "사이버 수사 및 디지털 증거수집 실태조사 결과 발표 토론문", 49쪽.

다. 한편, 오스트레일리아 Crimes Act 1914 3LA는 '컴퓨터나 컴퓨터시스템에 접근할 수 있도록 조력할 수 있는 등의 지식을 가진 사람'(Person with knowledge of a computer or a computer system to assist access etc.)이라는 제목 아래 다음과 같은 규정을 두고 있다.

「경찰관은 특정인에 대해 컴퓨터나 데이터 저장장치에 저장되어 있는 데이터에 접근하거나 그것들로부터 접근할 수 있도록 합리적이고 필요한 정보와 조력을 제공하라는 명령을 해 줄 것을 부판사에게 신청할 수 있다. 그 컴퓨터나 데이터 저장장치는 (i) 영장에 기재된 장소에 위치하고 있거나, (ii) 3K(2)항에 의해 이동되어 조사와 처리를 하기 위한 장소에 위치하고 있거나, (iii) 이 장에 의해 압수되었어야 한다.」[39]

그러나 위 규정 내용 자체에 의하더라도 정보통신망을 통하여 원격지 컴퓨터에 대해 온라인 수색이나 모니터링을 허용하는 규정이라고 할 수는 없다. 위 조항 (a)(ii)에서 말하는 3k(2)항도 영장집행장소에서 발견된 컴퓨터를 검색하고 처리하기 위해 합리적으로 필요한 장소에 이동한 경우를 의미할 뿐, 경찰관이 일반적으로 원격지 컴퓨터 서버에 강제로 접근하여 수색할 수 있음을 의미하지는 않는다.

라. 이밖에 미국 연방형사소송규칙 제41조(b)는 "영장발부권한"(Authority to Issue a Warrant)라는 제목 아래 다음과 같이 규정하고 있다.

「연방 법집행 공무원이나 검사장의 요청이 있으면,

(2) 영장을 담당하는 연방지방법원 부판사는 영장 발부당시를 기준으로 관할 구역 내에 소재하던 사람이나 물건이 영장 집행 이전에 관할 구역 밖으로 이주하거나 이주될 가능성이 있는 경우에도 그 사람이나 물건에 대해 영장을 발

39) A constable may apply to a magistrate for an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a constable to do one or more of the following:
(a) access data held in, or accessible from, a computer or data storage device that:
(ⅰ) is on warrant premises; or
(ⅱ) has been moved under subsection 3K(2) and is at a place for examination or processing; or
(ⅲ) has been seized under this Division;

부할 수 있다.

(5) 범죄에 관련된 행위가 발생한 연방지구이면 어디든, 또는 컬럼비아 연방지구의, 관할 지역 영장 담당 부판사는 관할 구역 밖인 주나 연방지구에 소재하는 물건에 관한 영장을 발부할 수 있다. 그러나 그 물건은 다음 구역 안에 있어야 한다. (A) 미합중국 영토, 속령, 또는 준주(準州). (B) 외국에 소재하는 미합중국의 외교나 영사목적 공관(소유자가 누구인지를 불문함)으로서 부속건물, 건물의 일부, 해당 목적에 공여되는 부지 또는 (C) 미합중국이 소유하고 있거나 임대한 것으로서 외국에서 미합중국의 외교나 영사 임무를 수행하는 미합중국 직원이 사용하는 거주지와 부속 토지.」[40]

그런데 이들 조항이 정보통신망 모니터링이나 원격지 컴퓨터 압수수색(온라인 수색)을 허용하는 영장을 발부할 수 있다고 직접적으로 규정하고 있는 것은 아니다. 단지 연방국가인 미국에서 특정 관할 구역 법원에서 발부된 영장이 다른 관할구역에서 집행될 수 있음을 규정하고 있는 것에 불과하다.[41] 따라서 이 조항에 의해 원격지 소재 컴퓨터 시스템에 관하여 그 시스템 관리자의 동의를 받지도 않은 채 강제로 그 원격지 컴퓨터 시스템에 접속하여 수사기관이 필요로 하는 디지털 증거를 탐색하고 수집할 수 있는 것은 아니다.

---

40) At the request of a federal law enforcement officer or an attorney for the government

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth

(B) the premises-no matter who owns them-of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purpose; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

41) 오길영, 위 “사이버 수사 및 디지털 증거수집 실태조사 결과 발표 토론문”, 50쪽.

마. 정보통신망 모니터링과 관련하여 우리가 특히 주목해야 할 입법례는 독일의 경우이다. 독일 연방대법원은 2007. 1. 31. 독일 형사소송법상 온라인 수색은 허용될 수 없다고 판시하였다.[42] 이어 독일 연방헌법재판소는 2008. 2. 27. 타인의 정보기술시스템에 대한 수사기관의 비밀접근을 허용하는 노르트라인 베스트팔렌 주 헌법보호법의 온라인 수색 관련 규정에 대한 헌법소원 사건에서, 정보기술시스템 자체에 대한 기밀성 및 무결성 보장에 관한 기본권,[43] 또는 '정보기술시스템의 신뢰성과 완전성에 대한 기본권' 개념을 창설하면서, 그 기본권을 침해한 위 헌법보호법은 무효라고 판시하였다.[44] 이에 의하면 정보기술 시스템 이용자가 스스로 생성하여 저장한 데이터뿐만 아니라 그에 기초해 해당 정보기술 시스템 자체가 생성해 내는 데이터 등이 포함된 다양한 데이터를 저장하고 있는 위 시스템을 국가기관 등 제3자가 밀행적이고 강제적으로 침입하여 이용한다면, 그 자체만으로도 정보기술 시스템에 대한 데이터 주체의 인격권이 침해될 수 있다고 한다.[45] 이러한 판결이 선고된 후 그 판시에 따라 연방 범죄수사청법, 바이에른주 헌법보호법, 바이에른주 경찰법, 라인란트-팔츠주 경찰법 등에서 온라인 수색을 엄격한 제한 아래에서만 허용하고 있다.[46]

2. 원격지 컴퓨터에 대한 탐색, 압수 관련 입법론들

범죄수사 현장에서 압수수색 장소에 있는 컴퓨터와 네트워크로 연결되어 있는 원격지 컴퓨터나 외부서버에 해당 사건 범죄와 관련된 증거가 있는 경우 이러한 원격

42) BGH, Beschluß vom 31. 1. 2007 - StB 18/06. ; 박희영, 「독일형사판례연구 I, 사이버범죄」, 한국학술정보(2011), 191-202쪽.

43) 박희영, "온라인 수색과 IT-기본권", 『독일연방헌법재판소 판례연구 1, -정보기본권』, 11쪽 이하. ; 이숙연, 위 "전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여", 14쪽 주27).

44) 박희영, "정보기술 시스템의 기밀성 및 무결성 보장에 관한 기본권(상)(하) : 독일연방헌법재판소 결정 1BvR 370/07, 1BvR 595/07 ; 오기두, 『전자증거법』, 박영사 (2015), 231쪽.

45) 명재진, "IT(정보기술) 기본권의 체계화에 관한 연구", 헌법재판소, 『헌법논총』 제20집, 296쪽, 310쪽. ; 오기두, 위 『전자증거법』, 509쪽.

46) 상세한 내역은 박희영, 위 "독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향", 90쪽 이하.

지 컴퓨터나 외부서버에 접속하여[47] 범죄관련 정보를 탐색하고 수집하는 것도 정보통신망 모니터링이라고 할 수 있는데, 국내에서도 이를 허용하자는 입법론이 제시되고 있다. 한국형사법학회가 2010년에 마련한 형사소송법개정안 제115조의3은 정보통신망에 의하여 접속이 가능한 정보에 대해 수사기관이 정보처리장치를 통하여 접속한 후 수색할 수 있다는 규정을 두고 있었다.[48] 다만, 그러한 법률안 규정을 마련한 이유에 관한 설명은 없었다. 한편 곽병선·노명선·이종찬·권양섭도 2012년에 그와 유사한 법률안을 제시한 바 있다. 그에 의하면 현행 형사소송법 제106조에 다음과 같은 항목을 삽입하자고 한다.

「압수할 전자정보가 수색장소에 있는 컴퓨터 등 정보처리장치(이하 '컴퓨터 등'이라 한다)와 접속된 다른 컴퓨터 등에 기억되어 있다고 인정되고 수색장소의 컴퓨터 등을 통해 다른 컴퓨터 등에 접속할 정당한 권한이 있는 경우에 한하여 다른 컴퓨터 등에서 전자정보를 이전받거나 복제한 후 압수할 수 있다.」

나아가 위 법률안에서는 형사소송법 제109조에 다음과 같은 항목도 추가할 것을 제안하고 있다.

「수색장소에서 전자정보를 압수하기 위하여 컴퓨터 등 정보처리장치(이하 '컴퓨터 등'이라 한다)를 수색하는 경우에 압수할 전자정보가 다른 컴퓨터 등에 기억되고 있다고 인정되고 수색장소의 컴퓨터 등을 통해 다른 컴퓨터 등에 접속할 정당한 권한이 있는 경우에 한하여 다른 컴퓨터 등에 대한 수색을 할 수 있다.」[49]

한편, 노명선 교수는 형사소송법 제109조 제1항 단서 및 제215조 제3항에 다음과 같은 내용을 신설할 것을 제안한다.[50]

「(특히 제215조 : 검사 또는 사법경찰관은 제1항 또는 제2항에 따라[51]) 전자정보를 압수하기 위하여 컴퓨터 등 정보처리장치(이하 '컴퓨터 등'이라 한다)를 수색하는 경우에 압수할 전자정보가 이와 접속된 다른 컴퓨터 등에 기억되어 있다고 인정

47) 곽병선·노명선·이종찬·권양섭, "사이버 수사 및 디지털 증거수집 실태조사", 국가인권위원회, 『사이버 수사 및 디지털 증거수집 실태조사 결과 발표 및 토론회』(2012.12), 14쪽.

48) 신양균, "한국형사소송법학회 형사소송법개정안"(2010. 12. 20. 대법원 형사실무연구회 발표문).

49) 곽병선·노명선·이종찬·권양섭, 위 글, 36쪽.

50) 노명선, "국회 디지털증거 압수수색에 관한 개정법률안 공청회 발표문", 사단법인 한국포렌식학회, 한국저작권위원회 개최, (2012.11.13.자).

51) 필자가 삽입함.

되고 그 컴퓨터 등을 통해 다른 컴퓨터 등에 접속할 정당한 권한이 있는 경우에 한하여 다른 컴퓨터 등에 대한 수색을 할 수 있다.」

또한 박종근 검사는 조문 제목을 '정보통신망에 의하여 접속 가능한 정보의 압수·수색'이라고 하여 형사소송법 제115조의3으로 다음과 같은 조항을 두자고 제안한다.[52)]

「① 정보에 대한 압수·수색을 집행하는 자는 압수·수색 집행 대상인 정보처리장치와 정보통신망으로 연결돼 있고 압수·수색의 대상이 되는 정보를 보관하고 있다고 인정되는 다른 정보처리장치에 대하여 압수·수색 집행대상인 정보처리장치를 통하여 접속한 후 수색을 할 수 있다.

② 제1항의 경우에 다른 정보처리장치에 보관되어 있는 압수 대상 정보는 이를 압수·수색 집행 대상인 정보처리장치로 이전 또는 사본하여 그 정보처리장치를 압수하거나 다른 저장매체에 이전 또는 사본하여 그 다른 저장매체를 압수하거나 내용을 인쇄 출력하여 출력물을 압수할 수 있다.」

이러한 입법적 제안들은 앞서 입법례에서 살핀 다른 나라의 제도를 모방하여 정보통신망 모니터링, 특히 온라인 수색이라는 수사 활동을 합법화하자는 의견이다. 수사의 효율적 진행을 위해 그러한 제도가 필요하다는 것을 부정할 수는 없다. 그러나 이러한 논의를 하기 이전에 이같은 수사기법이 갖는 법리적인, 특히 헌법적인 문제점을 충분히 검토하였는지는 의심스럽다. 무엇보다도 헌법상 영장기재 특정의 원칙을 위반하고 영장제시 원칙이나 당사자의 참여, 통지 등 헌법상 적법절차 구현 수단이 지켜질 수 없기 때문이다(후술).

52) 박종근, "디지털 증거 압수·수색과 법제", 대검찰청, 『형사법의 신동향』 제18호(2009), 93쪽.

Ⅳ. 정보통신망 모니터링의 헌법적 문제

1. 기본권 보장

가. 정보기본권과 프라이버시 보호

정보통신망 모니터링이 제도화되려면 당연히 개인의 정보에 대한 자기결정권 및 프라이버시 등 기본권 보호와의 균형점을 찾아야 하는 문제가 등장한다. 특히 국가기관에 의한 정보통신망 모니터링을 둘러싼 프라이버시 보호 문제와 관련하여서는 '프라이버시에 대한 합리적 기대'(reasonable expectation of privacy) 기준 충족 여부를 판단함에 있어 사적 기업 내 고용주와 근로자간의 정보통신망 모니터링 기준보다[53] 엄격한 기준을 적용해야 한다. 즉 사기업체 내에서는 정보처리자인 사용자의 정당한 경영 목적달성을 위한 근로자에 대한 정보통신망 모니터링인지 여부가 기준이 된다면, 국가기관에 의한 범죄통제 목적을 위한 정보통신망 모니터링에 관해서는 그 목적의 정당함 및 수단의 적정성과 아울러 최소한의 불가결한 규제인지, 기본권 침해성이 덜한 대안이 있는지 여부 등이 기준이 된다.

나아가 정보기술 시스템의 신뢰성과 완전성에 관한 기본권도 보장되어야 한다. 정보통신망 모니터링은 해당 전자정보 시스템에 대한 완전성을 침해하는 방법으로 수행될 수도 있다. 그런데 ISP 등의 전자정보 시스템에 저장된 데이터가 제3자에 의해 이용되는 과정에서 그 정보시스템의 신뢰성이나 완전성이 침해된다면 그것만으로도 당해 데이터 주체의 인격권이 침해된다. 개인의 전자정보를 저장하고 있는 정보처리 시스템에 대한 추적 수사활동도 그 시스템 자체에 대한 신뢰성과 완전성을 침해하지 않도록 수행되어야 한다.[54] 국가기관이 자체 프로그램을 개발하여 ISP

53) 미국의 사례로 Smyth v. Pillsbury, 914 F. Supp. 97, E. D. Pennsylvania District Court, (1/18/96) ; Bourke v. Nissan Motor Corp, Federal California Court of Appeal, 2nd Appellate District, Division 5, (7/26/93). 유럽인권재판소의 사례로 Copland v. The United Kingdom, Case No. 62617/00, (2007) 45 EHRR 37. 정찬모, 위 "직장 내 전자우편 모니터링 규제의 신조류와 시사점", 183쪽 및 주7), 주9), 191쪽 및 주23). 211쪽.

54) 1BvR 370/07, 1BvR 595/07 [178] ; 명재진, "IT(정보기술) 기본권의 체계화에 관한 연구", 헌법재판소,『헌법논총』제20집(2009), 296쪽, 310쪽 ; 오기두, "전자정보에 대한 기본권 보장과 위치정보추적 수사권", 헌법재판소,『헌법논총』제21집(2010), 534쪽 이하.

나 그 이용자의 컴퓨터 서버에 침입하여 온라인 수색을 하는 것은 원칙적으로 이러한 기본권을 침해하는 위헌적인 수사방법이라고 해야 한다.

나. 통신비밀의 보호

정보통신망 모니터링은 헌법 제18조 뿐 아니라 규범력을 발휘하고 있는 국제조약(시민적 및 정치적 권리에 관한 국제규약, International Covenant on Civil and Political Rights 제17조(1), 이하 ICCPR)[55] 등에서 보장하는 통신비밀에 관한 기본권을 침해하는 국가작용이다. 피처분자인 개인의 범주와 범죄의 특성, 기간의 제한, 모니터링 결과의 이용제한, 삭제, 기소되지 않거나 무죄판결을 받는 경우 어떻게 되는지 등에 관하여 구체적으로 명시된 법률과 영장에 근거하여 그 요건을 준수하는 집행이 되어야 정보통신망 모니터링의 정당성이 확보될 수 있다.[56]

다. 표현의 자유

정보통신망 모니터링은 인터넷 등을 통해 국경 없이 사상과 의견 표현이 가능한 오늘날의 정보 기술사회에서 표현의 자유를 침해하는 국가작용이 될 수 있다. 세계인권선언 제19조는 “어떤 매체를 통해서든 그리고 국경에 관계없이 정보와 사상을 찾고, 주고받는 자유”를 보장할 것을 문명국가의 의무로 선언하고 있고, 위 ICCPR 제19조 2.는 “구두, 서면 또는 인쇄, 예술의 형태 또는 스스로 선택하는 기타의 방법을 통하여 국경에 관계없이 모든 종류의 정보와 사상을 찾고 주고받는 자유”를 보장할 것을 체약당사국에 요구하고 있다. 표현의 자유의 한계는 타인의 인격권을 침해하는 표현, 국가안보, 공공질서 또는 공중보건, 도덕을 침해하는 표현이다(ICCPR 제19조 3.).[57] 따라서 범죄 예방이나 범죄수사, 유죄판결의 집행을 위해 무차별적으로 정보통신망 모니터링을 실시하면 이러한 국제인권규약을 위반하는 것이다. 그 한계 안에서 정보통신망 모니터링을 실시해야 한다.

---

55) 국제인권법연구회 편, 『국제인권법과 사법』(2016), 79-82쪽. 우리나라는 1990. 4. 10.에 가입하였다.
56) 유럽인권재판소의 Huvig v. France(1990) 사건 참조. 위 국제인권법연구회 편, 80쪽.
57) 위 국제인권법연구회 편, 191쪽.

2. 수권규범 문제

온라인 수색 등 정보통신망 모니터링에 관하여, 은밀성이 특히 요구되고 침해강도와 중요성이 압수·수색에 미치지 못하므로 법률적 수권 규범이 없더라도 허용되는 수사기법이라는 견해를 취할 수도 있다.[58] 그러나 일반에 공개된 데이터를 대상으로 하지 않는 한 정보통신망 모니터링은 그 자체로 국민의 정보기본권을 침해할 수 있으므로,[59] 정부기관이 그러한 행위를 함에는 법률에 의한 위임이 있어야 한다. 헌법 제12조 제1항에 의한 강제처분 법정주의에 비추어 법률에 근거가 없는 온라인 수색이나 온라인 모니터링은 위법하며, 위헌이라고 해야 한다.[60] 온라인 수색 등 정보통신망 모니터링을 명시적으로 허용하지 않고 있는 경찰관직무집행법(특히 제2조)이 수권규범이 되는 것도 아니다.[61] 정보통신망 모니터링을 허용하는 입법을 한다고 하더라도 그 법률의 규정 내용은 프라이버시 등 관련 기본권의 핵심영역을 침해하면 안 된다. 예컨대 특정인이 혼자 있거나, 특별한 신뢰관계에 있는 사람과 단둘이 있는 경우의 정보통신망 모니터링이나 시간적·공간적인 포괄적 감시는 사생활의 핵심영역을 침범하므로 헌법적으로 허용되지 않는다고 해야 한다. 나아가 관련 기본권의 비핵심영역에 대한 제한도 기본권제한의 일반 원리인 비례의 원칙을 준수해야 한다. 이것은 독일연방헌법재판소가 정식화한 '이단계 구조의 통제법리' 및 'je-desto' 공식을 적용해야 한다는 의미이다.[62]

---

58) 독일의 컴퓨터 검색수사(Rasterfahndung)에 관해 이러한 주장을 하는 견해로 Ermish, "Die systematisiert Fahndung - Rasterfahndung -", in Wissenshaftliche Kriminalistik, Kube/Storzer/Brugger(Hg.), Wisbaden (1984). 310쪽 이하. 이원상, "온라인 수색에 대한 고찰 - 독일의 새로운 논의를 중심으로", 한국형사법학회,『형사법 연구』제20권 제4호(2008년 겨울). 339쪽 및 주8) 재인용.

59) 오기두,『전자증거법』, 박영사(2015), 262-4쪽.

60) 오기두, 위『전자증거법』, 245, 246쪽.

61) 박희영, 위 "예방 및 수사목적의 온라인 비밀 수색의 허용과 한계", 165-6쪽.

62) BVerfGE 100, 313 ; BVerfGE 115, 320 (360 f.) ; BVerfG, 1 BvR 2368/06 vom 23. 2. 2007 ; VGH Mannheim Urteil vom 21. 7. 2003. ; 박정훈, 위 "전자감시와 프라이버시 관계 정립에 관한 연구", 167-9쪽 및 주 81-4).

3. 영장주의

이것은 영장주의, 특히 영장기재의 특정 원칙과 관련된 문제이다. 정보통신망 모니터링을 통제하는 수단은 우선 구체적 범죄혐의 사실과 관련되는 전자정보만 그 모니터링의 대상으로 허용하는 것이다. 현행 형사소송법 제106조 제1항 및 제215조가 이를 요구하고 있다. 그 관련성의 의미는 주관적,[63] 객관적, 시간적으로 수사기관이 구체적으로 범죄혐의를 잡고 있는 범죄사실에 한하여 수색·검증, 압수할 수 있다는 것으로 해석해야 한다.[64] 서울중앙지방법원 등[65] 전국 각급 법원 영장 담당 법관들의 실무도 그렇게 운용되고 있다.[66] 그러므로 수많은 전자정보를 저장하고 있는 인터넷 서비스업체의 서버 자체를 수색·검증,[67] 압수하는 것은 원칙적으로 금지된다. 서버 등 전자기록 매체 자체를 압수하거나 이미징하기 위해서는 피처분자의 동의를 얻어야 한다.[68] 수사기관이 피의자 a의 공직선거법 위반 범행을 범죄사실로 하여 발부받은 압수·수색영장의 집행 과정에서 b, c 사이의 대화가 녹음된 b의 휴대전화를 압수하여 그 녹음파일을 증거로 제출하여 b, c의 별개 범죄사실을 입증하는 것은 주관적 관련성 원칙을 위반한 것이다.[69] 적법한 체포를 하는 경우라고 할지라도 긴급상황(exigent circumstances)이 아닌 한,[70] 피처분자의 수많은 개인정보가 담겨 있는 스마트폰 자체를 압수하여 그 스마트폰이나 클라우드(cloud)에 저장된 모든 정보를 모니터링해서도 안 된다.[71]

---

63) 오기두, 위『전자증거법』, 281-332쪽.

64) 대법원 2011. 5. 26.자 2009모1190 결정 ; 대법원 2015. 7. 16.자 2011모1839 전원합의체 결정.

65) 최연진·박상기 기자, "'디지털情報 압수수색제한'에 …", 조선일보 2015. 8.4.자 A12쪽 기사.

66) 위 대법원 2015. 7. 16. 선고 2011모1839 전원합의체결정 ; 손지영·김주석,『디지털 증거의 증거능력 판단에 관한 연구』, 대법원 사법정책연구원(2015), 73-9쪽.

67) 압수·수색에 필요한 최소한의 범위내에서 '제3자에의 이동'과 같이 새로운 영장 집행방법이나 '수색과 검증'이라는 피압수자의 부담을 경감하는 새로운 영장제도를 만들어야 한다는 견해로 노명선, "전자정보의 압수·수색을 위한 새로운 영장제도의 제언", 대한변협신문, 2015. 11. 30.자, 12쪽.

68) 이에 관해 상세한 내용은 오기두, "전자정보의 수색·검증, 압수에 관한 개정 형사소송법의 함의", 한국형사소송법학회,『형사소송 이론과 실무』제4권 제1호 (2012), 127쪽 이하 참조.

69) 대법원 2014. 1. 16. 선고 2013도7101 판결 ; 오기두, 위『전자증거법』, 333-351쪽. ; 손지영·김주석, 위『디지털 증거의 증거능력 판단에 관한 연구』, 107쪽, 158쪽.

70) 위 오기두, "전자정보의 수색·검증, 압수에 관한 개정 형사소송법의 함의", 173쪽.

71) Supreme Court of the United States, Riley v. California (No 13-132) & US v. Wurie (No.

온라인 수색도 관련성 없는 전자정보에 대한 무차별적인 수색이 이루어진다는 점에서 허용될 수 없는 수사기법이다.[72] 더욱이 클라우드(cloud computing)나[73] 빅데이터(big-data)와 같이 다수의 대형 컴퓨터 시스템이 운영되는 곳에 대한 네트워크 수사가 가능하게 될 때 그러한 대규모의 데이터와 연결된, 범죄와 관련 없는 많은 사람들에 대한 정보기본권이 침해될 우려를 상정해보면,[74] 정보통신망 모니터링을 일반적으로 허용하기에는 주저하지 않을 수 없다.

설령 법관의 압수수색 영장을 발부받았다고 해서 온라인 수색이 당연히 허용된다고 할 수 있는지도 살펴야 한다. 왜냐하면 정보통신망 수색을 허용하는 것은 수색장소를 특정하지 않는 수색을 허용하는 것이 되기 때문이다. 특히 수사기관이 필요로 하는 데이터가 저장되어 있는 컴퓨터 서버의 소재지를 영장에 특정하지 않더라도 입력장치에 대한 압수·수색을 하면서 그 서버에 보관된 정보를 압수·수색할 수 있도록 허용하는 이른바 원격지 컴퓨터의 압수·수색을 해서는 안 된다. 이것은 영장주의 원칙 중 영장기재 특정의 원칙을 위반하는 수사활동이다. 원격지 컴퓨터나 서버 자체도 형사소송법상의 수색·검증, 압수에 있어 장소적인 공간에 위치하므로[75] 수사관의 영장집행장소가 특정되어야 하는 것이다. 따라서 수색·검증, 압수 장소를 특정하지 않은 채 정보통신망 수색을 허용하는 영장을 청구해서도 안 되고 법관이 이를 발부해서도 안 된다. 더욱이 정보통신망을 통한 피의자의 컴퓨터시스템 수색(온라인 수색이나 온라인 모니터링)은 감시 장소나 감시 기회가 특정되어 있는 통신감청과 달리 범죄발생 위험과 무관하거나 이미 발생한 범죄와 무관한데도 피의자와 정보통신망으로 연결된 제3자까지 감시할 수 있게 되는 점에서도[76] 영장기재의 특정성 원칙을 위반하는 것이다. 그러므로 설령 정보통신망 수색을 허용하는 영장을

13-212), (2014. 6. 25.), III. B. 2. 134 S.Ct. 2473.

72) 오기두, 위 "전자정보의 수색·검증, 압수에 관한 개정 형사소송법의 함의", 159쪽, 주61).

73) 김경환, "클라우드발전법", 법률신문, 2015. 3. 9.자 15쪽. 2015. 3. 3. 국회는「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」을 의결 통과시켰다.

74) 오기두, "2012. 11. 13.자 사단법인 한국포렌식학회, 한국저작권위원회 개최, 국회 디지털증거 압수수색에 관한 개정법률안 공청회, 토론문", 국가인권위원회,『사이버 수사 및 디지털 증거수집 실태조사 결과 발표 및 토론회』(2012.12), 91-2쪽.

75) 오기두, 위 "사이버 수사 및 디지털 증거수집 실태조사 결과 발표 토론문", 84쪽.

76) 박희영, 위 "독일에 있어 경찰에 의한 '예방적' 온라인 수색의 위헌여부", 195쪽.

발부받아 이를 집행한다고 하더라도 그 영장은 위헌적인 영장이 되어 그로 인해 수집한 전자증거의 증거능력이 위법수집증거로서 배제될 수 있다고 해야 한다.

나아가 설령 법관의 영장을 발부받아 행해진다고 하더라도 온라인 수색은 밀행적으로 이루어지는 수사활동으로서 형사소송법 제121조 및 제123조에 의해 보장되는 피의자, 변호인, ISP 등 전자정보 저장장치의 소유자, 보관자 또는 관리자의 참여권을 배제하는 위법한 수사가 된다.

Ⅴ. 특별법상의 한계 설정

1. 통신비밀보호법 등에 의한 규제

정보통신망 모니터링은 그 자체로 통신의 비밀을 침해한다. 그러므로 통신비밀보호법을 위반하는 수사방식으로 정보통신망 수색이나 감청을 하는 것은 허용될 수 없다.[77] 위 법률에 의하지 않고는 유선·무선·광선 및 기타 전자적 방식으로 이루어지는 모든 종류의 음향·문언·부호 또는 영상의 송수신에 관한 감청, 타인간 대화의 녹음 또는 청취 등을 할 수 없기 때문이다(위 법률 제3조). 그에 위반하여 취득한 대화내용은 증거능력이 부정되고(위 법률 제4조), 감청을 행한 자는 처벌된다(제16조 제1항).

그러므로 통신비밀보호법이 대상으로 하고 있는 범죄(국가보안법위반, 뇌물죄, 살인죄, 감금죄, 약취유인죄, 강도죄 등 위 법률 제5조 제1항)에 관한 정보통신망 모니터링만이 허용된다고 하겠다. 또한 예컨대 패킷 감청은 영장주의와 비례원칙에 의하여 제한적으로만 허용되어야 한다. 피고인이 공소외인과 지속적으로 통신하면

77) 최근인 2016년 8월 16일과 17일에 걸쳐 저녁 8시 뉴스에서 MBC가 청와대 민정수석에 대한 특별감찰을 진행 중인 특별감찰관이 특정 언론사 기자에게 감찰 진행 상황을 누설해 온 정황을 담은 소셜네트워킹서비스(SNS) 내용을 입수했다고 보도하면서, 누군가가 도청이나 해킹을 통해 문제가 된 SNS 내용을 빼낸 것으로 통신비밀보호법을 위반한 것일 수도 있다는 의혹이 언론 등에 의해 제기되었다. 전수용·양은경 기자, " '감찰관·기자 대화내용' 담은 SNS, 누가 몰래 들여다봤을까", 조선일보 2016. 8. 18.자 A5쪽 기사 참조.

서 송·수신한 이메일을 즉시 삭제하여 인멸한다는 사정(필요성)과 패킷 감청의 대상으로 피고인의 사무실에 설치된 인터넷 전용선으로 한정하여 통신비밀의 침해가능성이 크지 않은 점(비례성)이 인정되는 경우가 그에 해당한다.[78] 그리고 통신비밀보호법의 통신 감청은 전기통신이 이루어지고 있는 상황에서 실시간으로 그 통신내용을 지득·채록하는 행위와 통신의 송·수신을 직접적으로 방해하는 행위를 말하고, 카카오톡 등 민간업체에 위탁하여 하는 통신감청도 그러한 경우에 국한되며, 이미 수신이 완료되어 전자정보의 형태로 저장되어 있던 대상자들의 카카오톡 대화내용을 3~7일마다 정기적으로 서버에서 추출하여 수사기관에 제공하는 방식으로 통신제한조치 영장을 집행할 수는 없다.[79] 나아가 민간업체나 통신당사자의 동의 없이 이루어지는 온라인 수색도 통신비밀보호법 등에 근거를 두지 않는 위법한 수사활동이라고 해야 한다. 온라인 수색은 범죄혐의자와 제3자 사이의 실시간 통신내역을 감시하는 것이 아니라 전기통신 수단으로 그들의 컴퓨터 하드드라이브나 통신업체의 서버에 접속하여 그에 저장되어 있는 전자데이터를 비밀리에 획득하는 행위로서 통신비밀보호법이 예정하는 수사활동이라고 할 수 없기 때문이다.[80]

그리고 필요성과 비례성을 요건으로 하여 감청이 허용되어야 하는데도, 감청영장 발부현실을 보면 이러한 요건이 제대로 준수된 상태에서 영장이 발부되고 있는지 의심스럽게 한다. 최근 5년간 검찰의 감청허가 청구를 보면, 2012년 117건, 2013년 163건, 2014년 158건, 2015년 82건, 2016년 8월까지 31건 등이 청구되었다(국가정보원이 그 중 63.6%에 이르는 339건을 신청하였다[81]). 이에 관해 법원은 각각 3건, 2건, 7건, 4건, 2건 등을 기각했을 뿐이다. 즉 발부율이 96.7%에 달한다는 것이다. 법원의 감청에 대한 통제기능이 제대로 작동되는지 의구심을 불러일으키는 통계수치라고 하지 않을 수 없다.[82] 감청영장 발부에 신중을 기해야 한다. 특히 SNS 콘텐

78) 앞서 든 서울중앙지방법원 2011. 12. 22. 선고 2009고합348 판결 ; 서울고등법원 2012. 6. 8. 선고 2012노82 판결 ; 대법원 2012. 10. 11. 선고 2012도7455판결 ; 정관영, 위 "패킷(packet) 감청 허용의 한계".

79) 대법원 2016. 10. 13. 선고 2016도8137 판결.

80) 박희영, 위 "예방 및 수사목적의 온라인 비밀 수색의 허용과 한계", 168쪽 및 그곳 주54)에서 인용한 BGH, Beschl. v. 31.1.2007 - StB 18/06, MMR 2007, S. 239.

81) 서유미 기자, "4년간 허가받은 감청 64%는 국가정보원", 서울신문, 2016. 9. 28.자, 11쪽.

82) 신동화 기자, "감청 허가율 97%에 달해" 기사 참조. 내일신문, 2016. 9. 7.자, 20쪽.

츠에 대한 실시간 감청을 허가할 경우 범죄혐의사실과 무관한 정보, 대상자의 SNS 계정과 연동된 제3자의 대화 내용까지 무차별적으로 모니터링의 대상이 될 우려가 크다.

수사기관의 요청 만에 의해 전기통신사업자가 통신자료(이용자의 성명, 주민등록번호, 주소, 전화번호, 아이디, 가입일 또는 해지일)를 제공해도 구 전기통신사업법 제54조(현행법은 제83조) 제3항, 제4항에 위반되지 않으며, 불법행위책임을 지지 않는다는 것이 대법원의 입장이다.[83] 그러나 통신비밀보호법상의 통신사실확인자료 뿐 아니라 위와 같은 통신자료를 전기통신사업자가 수사기관에 제출하는 것도 법원의 허가대상으로 해야[84] 영장주의 원칙 준수나 이용자의 정보기본권, 익명표현의 자유 등 기본권 보장에 충실하게 된다.[85]

나아가 통신제한조치의 집행에 관한 통지(통신비밀보호법 제9조의2), 송·수신이 완료된 전기통신에 대한 압수·수색·검증의 집행에 관한 통지(위 법률 제9조의3), 통신사실확인자료 제공에 관한 통지(위 법률 제13조의3) 등[86] 뿐만 아니라, 전기통신사업법에 의해 전기통신사업자가 수사기관에 이용자의 통신자료를 제공한 때에도 이용자 본인에게 통지하도록 해야 한다.[87]

2. 개인정보의 보호

2011년 9월부터 개인정보보호법이 제정 시행되고 있다. 개인정보는 헌법상으로 보호받아야 할 중대한 기본권일 뿐만 아니라 오늘날의 정보통신기술 사회에서 사회적 자본(Social Capital)인 공공재로서 경제질서의 근간을 이룬다.[88] 경찰, 국가정보원, 검찰, 국군기무사령부, 국세청 등을 포함한 국가기관 구성원이 이 글에서 고찰

83) 대법원 2016. 3. 10. 선고 2012다105482 손해배상(기) 판결.

84) 곽병선·노명선·이종찬·권양섭, 위 “사이버 수사 및 디지털 증거수집 실태조사”, 29쪽, 37쪽.

85) 오기두, “전기통신사업자의 이용자 정보 보호책임”, 법원도서관, 『사법논집』 제59집(2014), 43-78쪽.

86) 임석순, “통신제한조치 등 집행통지와 정보기본권 보호”, KiC 『형사정책연구 소식』(2015. 가을), 23쪽.

87) 서울지방변호사회도 2016. 9. 22. ‘2016 사법제도개혁과제 보고회’에서 같은 취지의 주장을 한 바 있다. 법률신문, 2016. 9. 26.자, 2쪽 기사.

88) 문금주, “개인정보 보호를 위한 기업의 역할”, 대한변협신문, 2014. 9. 22.자, 12쪽.

한 한계를 위반하여 정보통신망 모니터링을 실시함으로써 개인의 민감정보를 처리하면 개인정보보호법 제23조, 제71조에 의해 5년 이하의 징역 또는 5천만 원 이하의 벌금형에 처해질 수 있다.[89] 제3자에 의한 자유로운 활용이 허용되는지 여부가 분명치 않은 이른바 '그레이 존'(gray zone)에 있는 개인정보도[90] 최대한 보호하는 선에서 모니터링이 실시되어야 한다.

3. 전자적 위치정보를 이용한 범죄통제

구「특정 성폭력범죄자에 대한 위치추적전자장치부착에 관한 법률」에 의거하여 2008. 9. 1.부터 시행되고 있는 성폭력 범죄자에 대한 전자발찌(ankle monitor)도 RFID 기술을 이용한 것으로,[91] 형집행 단계의 전자모니터링 시스템의 하나라고 할 수 있다. 성범죄자에 대한 전자발찌 소급부착도 합헌이라는 것이 헌법재판소의 판단이다.[92] 현행의「특정 범죄자에 대한 보호관찰 및 전자장치부착 등에 관한 법률」도 전자파를 발신하고 추적하는 원리를 이용하여 위치를 확인하거나 이동경로를 탐지하는 일련의 기계적 설비인 '위치추적 전자장치'에 대하여 규정하고 있다.[93] 대법원은 위 법률이 그 목적달성을 위한 합리적 범위 내에서 전자감시제도를 탄력적으로 운영하도록 하면서 그에 따른 피부착자의 기본권 침해를 최소화하기 위한 방안을 마련하고 있다고 하면서 합헌이라고 판시하였다.[94] 전자감시제도는 기본적으로 보안처분으로서 형벌과는 그 목적이나 심사대상을 달리한다는 관점도 피력하고 있다.[95] 한편 법무부는 전자발찌 착용자가 재범 징후를 보이면 즉시 담당 보호관찰관

89) 이에 관해 참조할 글로, 이성기, "국내 민간인 불법사찰을 방지하기 위한 '준 법률적' 통제방안 모색 -미국의 국내정보(Domestic Intelligence)에 관한 FBI의 통제 가이드라인 논의를 중심으로-", 한국외국어대학교 법학연구소,『외법논집』제36권 제3호(2012. 8.), 102쪽.

90) 윤해성, "일본의 개인데이터 이용과 활용에 관한 제도동향", KiC『형사정책연구소식』(2014. 가을), 28쪽.

91) 위 박정훈, "전자감시와 프라이버시 관계 정립에 관한 연구", 133쪽, 주12).

92) 헌재 2012. 12. 27. 2010헌가82 결정.

93) 김상순, "베르세르크와 전자발찌 -웨어러블 디바이스(Wearable Device)", 대한변협신문, 2014. 10. 13.자, 8쪽.

94) 대법원 2009. 9. 10. 선고 2009도6061, 2009전도13 판결.

95) 대법원 2009. 5. 14. 선고 2009도1947, 2009전도5 판결.

에게 알려 현장에 출동하게 하는 지능형 전자감시 시스템을 2017년부터 운영한다고 한다.[96] 전자발찌에 의한 모니터링은 위 대법원의 입장과 같이 특정 범죄자의 재범위험성을 요건으로 피부착자의 신체의 자유를 박탈하지 않고, 단지 기본권을 제한하기만 하는 자유제한적 보안처분이라고 해야 할 것이다.[97] '작고 약한 여성'인 여자 어린이와 같은 극도의 사회적 약자를[98] 성범죄자로부터 보호하기 위해 이러한 전자적 모니터링 제도를 이용할 필요가 있음을 부정할 수 없다. 또한 피부착자 아닌 타인의 눈에 띄지 않도록 발목에 차게 하였고 행동의 자유도 보장하고 있는 점에서 방법, 수단의 측면에서 적정하다고 할 수 있다.[99]

그러나 일반적인 범죄 예방목적으로 경찰 등 국가기관에게 「위치정보의 보호 및 이용 등에 관한 법률」에 의해 위치추적권을 부여하기 위해서는 헌법상의 영장주의 원칙과 관련하여[100] 신중을 기할 필요가 있다고 하겠다.[101] 2012. 5. 14. 법률 제11423호로 개정된 위 법률 제29조 제2항은 긴급구조를 위한 경우에 한정하여 개인위치정보의 제공을 요청할 권한을 경찰에 부여하였다.

Ⅵ. 결어

정보통신망 모니터링은 국가기관이 범죄예방 목적으로나 수사목적으로, 인터넷 등 유선 또는 스마트폰 통신망과 같은 무선의 정보통신망을 통하여, 패킷단위로 전송되는 인터넷 통신회선에 접속하거나 상대방이나 ISP의 컴퓨터 서버에 침입하여, 일시적으로나 지속적으로 그 상대방 모르게 실시간 통신 내역을 엿보거나 그에 저장된 자료를 수집하는 것을 말한다. 국가가 실시하는 유·무선의 정보통신망에 대한

96) 고윤상 기자, "재범징후 사전탐지 '지능형 전자발찌' 나온다.", 한국경제 2016. 10. 26.자 A29쪽.
97) 같은 취지, 이춘화, "위치추적 전자장치 부착명령의 위헌성 유무", 한국형사판례연구회편, 『형사판례연구[18]』 (2010), 620쪽.
98) 홍숙영, "TV다큐멘터리의 아동성폭력 재현 방식 - 'KBS시사기획 쌈'을 중심으로", 『한국콘텐츠학회논문지』 Vol. 11, No. 1(2011), 105쪽.
99) 위 이춘화, 628쪽.
100) 오기두, 『전자증거법』, 박영사 (2015), 476쪽 이하.
101) 이경미 기자, "'경찰에 위치추적권' 법개정안 논란", 한겨레(2012.4.24.자), 11쪽.

모니터링은 정보에 대한 기본권이나 프라이버시 침해로 과잉수사 및 과잉처벌의 위험가능성을 상존케 한다. 범죄 예방이나 범죄수사, 유죄판결의 집행을 위해 무차별적으로 정보통신망 모니터링을 실시하는 것은 세계인권선언 등 국제인권규약 및 헌법상 보장되고 있는 정보기본권, 프라이버시, 통신비밀, 표현의 자유 등을 침해할 수 있으므로, 그 한계 안에서 정보통신망 모니터링을 실시해야 한다. 그리고 형사소송법 제106조 제1항 및 제215조가 요구하는 바와 같이 수사기관이 구체적으로 범죄혐의를 잡고 있는 범죄사실과 주관적, 객관적, 시간적으로 관련된 전자정보에 한하여 수색·검증, 압수할 수 있다고 해야 한다.

정보통신망 모니터링, 특히 온라인 수색이라는 수사 활동을 합법화하자는 입법론이 제기되고 있으나 그러한 논의를 하기 이전에 그와 같은 수사기법이 갖는 헌법 등 법리적인 문제점을 충분히 검토하여야 한다. 무엇보다도 헌법상 영장기재 특정의 원칙을 위반하고 영장제시 원칙이나 당사자의 참여, 통지 등 헌법상 적법절차 구현수단이 지켜질 수 없기 때문에 이러한 수사기법을 법제화하는 데는 신중해야 한다.

참고문헌

국가인권위원회,『사이버 수사 및 디지털 증거수집 실태조사』(2012.12)

국제인권법연구회 편,『국제인권법과 사법』(2016)

박희영,『독일형사판례연구 Ⅰ, 사이버범죄』, 한국학술정보 (2011)

손지영·김주석,『디지털 증거의 증거능력 판단에 관한 연구』, 대법원 사법정책연구원 (2015)

오기두,『전자증거법』, 박영사 (2015)

강성주, "경계에 선 '개인정보 자기결정권'", 대한변협신문, 2014. 9. 1.자

_____, "'빅 데이터'는 미래를 만들어 나가는 열쇠", 대한변협신문, 2015. 2. 2.자

강태욱, "'망 중립성' 논의", 법률신문, 2016. 9. 26.자

곽병선·노명선·이종찬·권양섭, "사이버 수사 및 디지털 증거수집 실태조사", 국가인권위원회,『사이버 수사 및 디지털 증거수집 실태조사 결과 발표 및 토론회』(2012.12)

김경환, "클라우드발전법", 법률신문, 2015. 3. 9.자

김상순, "베르세르크와 전자발찌 - 웨어러블 디바이스(Wearable Device)", 대한변협신문, 2014. 10. 13.자

노명선, "국회 디지털증거 압수수색에 관한 개정법률안 공청회 발표문", 사단법인 한국포렌식학회, 한국저작권위원회 개최, (2012.11.13.자)

_____, "전자정보의 압수·수색을 위한 새로운 영장제도의 제언", 대한변협신문, 2015. 11. 30.자

명재진, "IT(정보기술) 기본권의 체계화에 관한 연구", 헌법재판소,『헌법논총』제20집 (2009)

문금주, "개인정보 보호를 위한 기업의 역할", 대한변협신문, 2014. 9. 22.자

박정훈, "전자감시와 프라이버시 관계 정립에 관한 연구", 법조협회,『법조』통권 제645호 (2010. 6.)

박종근, "디지털 증거 압수·수색과 법제", 대검찰청,『형사법의 신동향』제18호, (2009)

박희영, “독일에 있어 경찰에 의한 ‘예방적’ 온라인 수색의 위헌여부”, 경찰대학, 『경찰학연구』 20호 (2009.8.)

_____, “독일에 있어서 경찰의 온라인 수색에 관한 판례 및 법제 동향”, 『최신외국법제정보』 2011년 2호

_____, “예방 및 수사목적의 온라인 비밀 수색의 허용과 한계”, 『원광법학』 제28권 제3호 (2012)

신양균, “한국형사소송법학회 형사소송법개정안”(2010. 12. 20. 대법원 형사실무연구회 발표문)

양종모, “수사기법으로서의 데이터 마이닝에 대한 법적 고찰”, 대검찰청, 『형사법의 신동향』 통권 40호 (2013. 9.)

오기두, “전자정보의 수색·검증, 압수에 관한 개정 형사소송법의 함의”, 한국형사소송법학회, 『형사소송 이론과 실무』 제4권 제1호 (2012).

_____, “전기통신사업자의 이용자 정보 보호책임”, 법원도서관, 『사법논집』 제59집 (2014)

오길영, “사이버 수사 및 디지털 증거수집 실태조사 결과 발표 토론문”, 국가인권위원회, 『사이버 수사 및 디지털 증거수집 실태조사 결과 발표 및 토론회』 (2012.12)

윤성주, “망중립성에 관한 규제 개관”, 서울대학교 기술과법센터, 『LAW & TECHNOLOGY』 제10권 제3호 (2014.5.)

윤지영, “미국의 통신감청 관련 법규 및 논의 동향”, KiC 『형사정책연구소식』 (2016 봄)

윤해성, “일본의 개인데이터 이용과 활용에 관한 제도동향”, KiC 『형사정책연구소식』 (2014. 가을)

이성기, “국내 민간인 불법사찰을 방지하기 위한 ‘준 법률적’ 통제방안 모색 -미국의 국내정보(Domestic Intelligence)에 관한 FBI의 통제 가이드라인 논의를 중심으로-,” 한국외국어대학교 법학연구소, 『외법논집』 제36권 제3호 (2012.8)

이숙연, “전자정보에 대한 압수수색과 기본권, 그리고 영장주의에 관하여”, 한국헌법학회, 『헌법학연구』 제18권 제1호(2012. 3.)

이원상, “온라인 수색에 대한 고찰 - 독일의 새로운 논의를 중심으로”, 한국형사법학

회,『형사법 연구』 제20권 제4호 (2008년 겨울)

이춘화, “위치추적 전자장치 부착명령의 위헌성 유무”, 한국형사판례연구회편,『형사판례연구[18]』(2010)

임석순, “통신제한조치 등 집행통지와 정보기본권 보호”, KiC『형사정책연구 소식』(2015. 가을),

정관영, “패킷(packet) 감청 허용의 한계”, 대한변협신문, 2014. 10. 13.자

정교일, “디지털증거의 압수와 공판정에서의 제출방안”, 대검찰청,『형사법의 신동향』통권 25호 (2010. 4.)

정찬모, “직장 내 전자우편 모니터링 규제의 신조류와 시사점”, 법조협회,『법조』통권 제645호 (2010.6.).

최창호, “기술의 발전과 프라이버시”, 대한변협신문, 2015. 1. 19.자

홍숙영, “TV다큐멘터리의 아동성폭력 재현 방식 - ‘KBS시사기획 쌈’을 중심으로”,『한국콘텐츠학회논문지』Vol. 11, No. 1(2011)

Domblewski, Carol,『The Salem Witch Trials』, Scholastic Inc., (2003).

A. Shields, Marjorie, “Annotation, Fourth Amendment Protections, and Equivalent State Consitutional Protections, as Applied to the Use of GPS Technology, Transporter, or the Like, to Monitor Location and Movement of Motor Vehicle, Aircraft, or Watercraft”,『5 A.L.R.6th 385』, (2005)

L. Bellia, Patricia, “The Memory Gap in Surveillance Law”,『75 U. Chi. L. Rev, 137』, (2008)

M. Balkin,, Jack, “The Constitution in the National Surveillance State”,『Minnesota Law Review』(2008.11.)

Palfrey, John, “The Public and Private at the United States Border with Cyberspace”,『Missipi Law Journal』(Winter 2008).

Zittrain, Jonathan, “Internet Points of Control”,『44 B.C.L.Rev』. 653(2003)

New York Civil Liberties Union, “Who's watching?: Video Camera Surveillance in New York City and the Need for Public Oversight”(2006), http://www.nyclu.org/pdfs/surveillance_cams_report_121306.pdf

Reviewing the Crime Control by Monitoring Information-Communication Network

Oh, Gi-Du*

A monitoring of the Information-communication network would be made by a government agency for the purpose of preventing or investigating crimes. That network includes wire network such as the Internet or wireless network for smart-phones. Of course, that monitoring is committed by the agency without the consent of the parties of that communication. The agency accesses to the Internet that sends messages through digital packet unit, or intrudes into the computer servers of the parties of that communication or ISP. With that procedure, the agency can temporarily or constantly wiretap the communication or gather the data stored in that server. This kind of monitoring has the risk to overly restrict the fundamental rights of citizens to Information or privacy. Someone insists that monitoring Information-communication network, especially on-line search should be legalized. However, before that argument, we need to thoroughly review the constitutional and legal issues related with that monitoring. Those issues include the fundamental rights to Information, privacy, confidential communication and freedom of expression which are protected by the Universal Declaration of Human Rights and the Constitutional Law. To search and seize for the digital data via the monitoring, the government agency also has to follow the limit of subjective, objective and time-based relevancy regulated by the Section 106 ① and Section 215 of the Criminal Procedure Law. On-line search is unconstitutional when the location of a computer system is not specified on the search warrant, because that is a general and vague warrant.

* Presiding Judge in the Seoul Eastern District Court/Ph.D. in Law

❖ Key Words: monitoring of Information-communication network, on-line search, Fundamental rights to Information, relevancy, warrant.

투고일 : 11월 8일 / 심사일 : 12월 9일 / 게재확정일 : 12월 9일