형사정책연구 Korean Criminological Review
제31권 제1호(통권 제121호, 2020・봄)

디바이스 복호화 명령과 자기부죄거부특권:
미국 법원의 실행과 영국의 입법례를 중심으로

송영진*

국 | 문 | 요 | 약

스마트폰은 기존의 무선 통신 기기에서 모바일 컴퓨터로 진화했고 스마트폰에서 생성되고 저장되는 데이터의 양도 방대해졌다. 또한 이러한 스마트폰 기기 자체의 암호화로 인해서 지문, 홍채, 안면인식 등 생체정보 또는 PIN번호 없이는 기기 내의 정보를 열람할 수 없는 문제가 발생하고 있다. 이 논문에서는 이와 같이 최근 제기되고 있는 많은 문제점에 대한 해결방안을 모색하기 위하여 수사기관의 데이터 수집 권한과 암호 기술 등의 충돌에 대한 미국에서의 "Going dark" 논의와 디바이스 복호화 명령과 관련된 미국 연방법원과 주 법원의 최근 판례를 분석하고자 한다. 또한, 영국의 암호화된 데이터에 대한 키 제출 명령을 규정하고 있는 수사권한법의 내용에 대하여 살펴볼 것이다. 마지막으로 관련 논의가 우리나라에서는 어떻게 이루어지고 있는지 살펴보고 디바이스 암호화에 따른 형사정책적 시사점을 도출하고자 한다.

우리나라에는 아직 스마트폰 등 디바이스 복호화에 대한 문제가 심각하게 대두되고 있지 않지만 몇몇 사례가 언론을 통해 보도되고 있다. 향후 스마트폰 압수수색 시 잠금해제 거부는 수사상 걸림돌로 작용할 수 있으며, 또한 잠금 해제를 요구하는 것이 적법한가에 대한 법적 논란이 발생할 소지가 있다. 우리나라도 스마트폰 압수수색 관련 법적 논란을 사전에 차단하고 수사과정에서 인권 침해를 최소화하기 위해서 미국의 판례와 영국의 입법례를 참고할 필요가 있다. 또한 발생 가능한 다양한 법적 쟁점에 대한 연구와 심도 깊은 논의가 필요하고 기술적으로도 암호화 문제를 극복할 수 있는 방안을 모색해야 할 것이다.

DOI : https://doi.org/10.36889/KCR.2020.03.31.1.159

❖ 주제어 : 복호화 명령, 암호화, 자기부죄거부특권, 암흑화(Going Dark), 범죄수사, 프라이버시, 개인정보보호, 디지털 포렌식, 스마트폰 암호해제

* 경찰대학 경찰학과 교수, 국제 사이버범죄 연구센터 겸임연구위원.

Ⅰ. 서론

오늘날 기술의 진화와 발전은 수사기관에게 기회를 제공하기도 하지만 한편으로는 장애물로 작용하기도 한다. 일각에서는 수사기관이 예전보다 더 많은 정보를 확보할 수 있다고 주장하지만, 다른 한편에서는 수사기관이 기술의 변화 속도를 따라잡지 못해 점점 어려움(going dark)에 봉착하고 있다고 주장한다[1]. 이러한 기술적 장애물로는 강력한 단대단(end-to-end) 암호화 기술, 데이터 보관(data retention) 기간의 제한, 서비스제공자가 특정 데이터를 수사기관에 제공할 수 있는 법적 권한의 한계, TOR(The Onion Router)나 VPN(Virtual Private Network)과 같은 온라인상 익명화 도구, 다양한 통신 네트워크의 혼재 등이 포함된다. 획득할 권한이 부여되지 않은 경우에 수사기관이 특정 정보에 접근하는 것은 불가능하다. 최근의 여러 논의는 강력한 암호 기술과 수사기관의 수사상 어려움에 관해 이루어지고 있다.

지난 수십 년간 수사기관의 권한과 기술의 변화 사이의 긴장으로 법적 쟁점들과 입법적 대안들이 제기되어왔다. 특히 미국에서 통신 기기에 백도어(back door)를 삽입하고 강력한 암호 코드의 배포를 제한하는 법안이 나오면서 이러한 긴장 상태는 더욱 고조되었다. 1994년 미국 의회에서는 “법집행기관을 위한 통신지원법(the Communications Assistance for Law Enforcement Act, 이하 ‘CALEA’라 함)”을 통과시켰고 동 법에서는 전기통신에 디지털 기술과 무선기술이 접목된 이후 수사기관이 통신감청을 할 수 있는 권한을 계속 유지할 수 있도록 하였다.

소위 “Going Dark” 문제는 점차 발전하는 암호화 기술 및 범죄자들이 감시와 수사망을 우회하기 위해 사용하는 기술의 확산으로 인해 수사기관이 테러리스트를 포함해 국가안보에 위협을 가하는 인물들이나 중범죄자들의 활동을 점차 파악하지 못하게 되거나 수사기관이 범죄 수사에 있어 난관에 봉착하게 되는 상황을 의미한다[2]. 암호화 기술의 발전과 확산으로 인해 수사기관이 디지털 증거에 접근하는 것

1) 수사기관의 권한 확대에 반대하는 측, 주로 시민단체와 미국의 주요 기업들은 수사기관이 암호화된 기기에 접근할 수 있도록 허용한다면 이는 이미 “감시의 황금시대(golden age of surveillance)”에 프라이버시 침해를 영구화하는 것이라고 비판한다. 또한, 이들은 이미 정부가 국가 안보를 목적으로 지나치게 감시하고, 수사기관이 개인 정보에 접근하고 있으며 개인의 프라이버시와의 균형이 깨어지면서 무게 중심이 너무 정부의 이익에 쏠려 있다고 주장한다.

이 점점 더 어려워지고 있으며 이러한 문제 해결을 위한 논의가 진행 중이다.

"Going dark" 논의는 원래 움직이고 있는 데이터, 즉 실시간 통신내용의 감청에 관하여 이루어져 왔다. 그러나 최근의 기술 변화로 인해 실시간 감청뿐만 아니라 저장된 데이터에 대해서도 수사기관이 접근하기 어려워지고 있다. 현재의 논의는 수사기관이 어떠한 유형의 정보에 대해서 어떠한 경우에 접근할 수 있는지와 관련이 있다. 스마트폰은 기존의 무선 통신 기기에서 모바일 컴퓨터로 진화했고 스마트폰에서 생성되고 저장되는 데이터의 양도 방대해졌다. 또한 이러한 스마트폰 기기 자체의 암호화로 인해서 지문, 홍채, 안면인식 등 생체정보 또는 PIN번호 없이는 기기 내의 자료를 열람할 수 없는 문제가 발생하고 있다[3]. 수사기관은 음성통신, 통화내역, GPS정보, 기기에 저장되어 있는 데이터, 클라우드에 저장되어 있는 데이터에 접근하는데 많은 난관에 봉착하게 된다.

2015년 미국 캘리포니아 주 San Bernadino에서는 총기 테러 사건이 발생하여 14명이 사망하고 22명이 중상을 입었다. 이 사건의 용의자 파룩(Farook)은 도주 과정에서 경찰의 총격을 받고 사망하였다. 미국 연방수사국(FBI)은 수사 과정에서 용의자 Farook이 소지하고 있었던 아이폰 5C 기종의 스마트폰에 대한 포렌식 분석을 시도하였으나 이는 4자리의 비밀번호로 잠금기능이 활성화되어 있었다. FBI는 이를 해독하기 위해 제조사인 애플(Apple)에 잠금해제를 요청하였으나 애플은 자사 제품의 보안성을 약화시킬 우려가 있다는 이유로 이를 거부하였다. 미국 연방수사국(FBI)는 이른바 "모든 영장 법(All Writs Act)"에 근거하여 "애플은 FBI의 요청에 협조해야 한다"는 명령을 하였고, 연방수사국(FBI)는 이를 근거로 집행을 시도하였다[4].

---

2) 전현욱 외, 사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구, 경제·인문사회연구회 미래사회 협동연구총서 15-17-01, 2015, pp. 364-368.

3) 2014년 워싱턴 D.C. 브루킹스 연구소에서 있었던 연설에서 제임스 코미 전 FBI 국장은 "사건해결의 열쇠가 되는 중요한 정보가 핸드폰이나 노트북 등 모바일 기기에 저장되어 있는 경우가 점차 많아지고 있고 앞으로도 계속 증가할 것으로 예상된다"고 하면서 "수사당국이 비밀번호를 풀지 못해 증거를 입수하지 못한다면 범죄를 발견하고 기소하는 것이 더욱 어려워 질 것"이며, "스마트폰의 잠금설정과 기능, 하드디스크 암호화로 인해 사법정의가 실현되지 못할 수도 있다"고 우려하였다. James B. Comey, "Going Dark: Are Technology, Privacy and Public Safety on a Collision Course?" (October 16, 2014). https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course 참조.

연방 치안판사는 1977년 모든 영장법(All Writs Act)을 근거로 애플에 연방수사국(FBI)이 제안한 소프트웨어를 제공하라는 명령을 발부하였으나 애플의 CEO Tim Cook은 공개서한을 통해 고객의 프라이버시 보호를 이유로 법원의 명령을 이행할 수 없다고 주장하였다. 결국 FBI는 제3의 기관을 통해 아이폰 잠금해제에 성공하였고 법원에 대해 요청을 철회하였다[5].

또한, 미국, 영국, 호주, 캐나다, 뉴질랜드로 구성된 이른바 'Five Eyes' 국가들은 2018년 9월 호주 골드코스트에서 법무장관 회담을 갖고, "증거에 대한 접근과 암호화에 대한 원칙 선언(Statement of Principles on Access to Evidence and Encryption)"을 발표하였다[6]. 이 공동성명에서 동 국가들은 법집행기관이 암호화로 인해 데이터에 대한 접근이 어려워지고 있으며 합법적인 데이터 접근에 관한 법원의 결정은 점점 무의미해져가고 있다고 언급하였다[7]. 공동성명에는 정보통신기술 회사들과 서비스 제공자들이 법집행기관을 지원할 상호적인 책임을 가지며, 자발적으로 법집행기관에게 합법적인 데이터 접근 솔루션을 제공하는 서비스 제공자는 그 방식을 선택할 자유를 갖는다는 내용이 포함되어 있다[8].

오늘날 '개인의 프라이버시와 데이터 보안'과 '공공의 안전과 국가안보' 사이의 균형을 어떻게 맞추어야 하는가? 현재 수사기관의 정보수집 권한이 정말 광범위한가? 수사기관은 스마트폰 등 디바이스 암호화로 인해 해당 디바이스에 저장된 정보에 접근이 불가능한 경우 어떻게 해결해야 하는가? 수사기관이 법원의 명령을 통해 피의자에게 스마트폰의 암호를 풀도록 요구하는 것이 불리한 진술을 강요하는 행위인가?

---

4) Grossman, Lev, "Inside Apple CEO Tim Cook's Fight With the FBI", Time (March 17, 2016).

5) Benner, Katie; Lichtblau, Eric, "U.S. Says It Has Unlocked iPhone Without Apple", The New York Times (March 28, 2016).

6) Five Countries Ministerial Quintet Meeting of the Attorneys-General, Statement of Principles on Access to Evidence and Encryption, 2018. https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf.

7) Susan Landau, The Five Eyes Statement on Encryption: Things Are Seldom What They Seem, Lawfare (September 26, 2018). https://www.lawfareblog.com/five-eyes-statement-encryption-things-are-seldom-what-they-seem 참조.

8) Susan Landau, The Five Eyes Statement on Encryption: Things Are Seldom What They Seem, Lawfare (September 26, 2018).

만약 수사기관이 피의자를 대상으로 스마트폰에 지문[9], 홍채 또는 안면 인식을 하도록 하는 것은 현행법상 가능한가?[10] 마지막으로, 미국 San Bernadio 사건과 같이 만약 스마트폰의 소유자가 사망하였거나 실종된 경우, 스마트폰의 제조사를 상대로 디바이스 복호화에 대한 기술적 지원(technical assistance)을 요구할 수 있는가?

이 논문에서는 위와 같이 최근 제기되고 있는 많은 문제점에 대한 해결방안을 모색하기 위하여 수사기관의 데이터 수집 권한과 암호 기술 등의 충돌에 대한 미국에서의 "Going dark" 논의의 역사와 주요 쟁점에 대해 살펴볼 것이다. 그런 다음 스마트폰 등 디바이스 복호화 명령과 관련된 미국 연방법원과 주 법원의 최근 판례를 분석하고자 한다. 또한, 이러한 관련 논의가 우리나라에서는 어떻게 이루어지고 있는지 살펴보고 디바이스 암호화에 따른 형사정책적 시사점을 도출하고자 한다.

Ⅱ. 복호화 명령(Compelled Decryption)과 자기부죄거부특권

미국에서는 복호화 명령(compelled decryption, 영장에 의해 피고인(피의자)으로 하여금 수사기관에 공개하지 않은 상태에서 패스워드를 입력하도록 강제하는 것)에 대하여 어떠한 기준을 적용해야 하는지에 대한 논의가 이루어지고 있으며, 그에 대한 법원의 판결례가 최근 증가하고 있다[11]. 여기에서는 자기부죄거부특권과 관련하

9) 이미 국내외 여러 연구에서 수사기관이 AFIS와 같은 지문 데이터베이스를 활용하여 모조지문을 제작하고 이를 스마트폰 암호해제에 활용하는 방안도 제시되고 있다. 손유리, 박성현, 손지훈, 김기범, 김영웅, 지문정보 이용 스마트폰 포렌식과 통제방안, 한국치안행정논집 제16권 제1호, 2019.

10) State v. Diamond, 905 N.W.2d 870, 875 (Minn. 2018) 사건에서 법원은 스마트폰 잠금해제를 위해 지문을 제공하는 것은 수정헌법 제5조상의 진술에 해당하지 않는다고 판단하였다.

11) 최근 미국 내에서는 이와 관련된 연구도 활발하게 수행되고 있다. 관련 논문으로는 Cohen, Aloni, and Park, Sunoo, Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries, Harvard Journal of Law & Technology, Vol. 32, No. 1, 2018; Coulon, Jesse, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018; Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019; Kerr, Orin S. and Schneier, Bruce, Encryption Workarounds, Georgetown Law Journal, Vol.106, 2018; Sacharoff, Laurent, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203, 2018 참조.

여 대표적인 선례 두 가지를 통해 발전되어 온 미국 헌법상 자기부죄거부특권의 원칙과 예외에 대하여 알아보기로 한다.

가. 미국 수정헌법 제5조에서의 자기부죄거부특권

미국 수정헌법 제5조(The Fifth Amendment)에서는 우리나라 헌법 제12조 제2항과 같은 자기부죄거부특권(또는 자기부죄금지의 원칙, privilege against self-incrimination)에 대하여 규정하고 있다. 즉 수정헌법 제5조는 "누구도 형사상 자신에게 불리한 진술을 강요당하지 않아야 한다(nor shall be compelled in any criminal case to be a witness against himself)"고 규정하고 있다. 연방대법원의 선례에 따라 수정헌법 제5조의 특권을 보호받기 위해서는 의사소통이 진술에 해당하고(testimonial), 형사상 불리하여야 하며(incriminating), 강요되어야(compelled) 한다.

이러한 수정헌법 제5조와 관련하여 "과연 암호화된 스마트폰, 컴퓨터나 하드디스크에 수사기관이 접근하기 위해서 영장을 발부받아 피의자에게 암호화의 해제, 즉 복호화할 것을 강제할 수 있는가?"가 문제된다. 즉 강제된 암호화 해제가 자신에게 불리한 진술을 강요당하는 것으로 해석할 수 있는가, 만약 그렇다면 어떤 것이 진술인가? 또한 이러한 원칙의 예외가 인정되기 위해서 수사기관이 입증해야 할 것은 무엇인가?

일반적으로 compelled decryption 사건은 패스워드를 제공하는 것이 수정헌법 제5조에서의 진술에 해당하는지에 대한 문제만을 제기한다. 해당 행위가 진술에 해당하는지 판단하기 위해서, 법원은 피고인이 "자신의 머릿속에 있는 내용을 공개할 것(to disclose the contents of his own mind)"을 강요당하는지를 판단한다[12]. 이러한 기준에 따라, John Paul Stevens 판사는 1988년 그의 반대의견에서 피고인은 자신에게 불리한 문서가 보관되어 있는 금고의 열쇠를 넘겨주도록 강제될 수 있으나 말로 또는 행동으로 금고의 비밀번호를 공개하도록 강요될 수 없다고 판시한 바 있다[13]. 아래에서는 수정헌법 제5조와 관련하여 미국 연방대법원의 일련의 판례에서

12) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 771.

13) Doe v. United States, 487 U.S. 201(1988).

도출된 원칙에 대해서 살펴보기로 한다.

나. Fisher v. United States 사건

자기부죄거부특권에 대한 가장 오래된 선례는 1976년 연방대법원의 Fisher v. United States 사건[14]이다. Fisher 사건에서의 쟁점은 정부가 납세자를 상대로 납세 신고와 관련된 회계사의 서류를 제출하도록 명령할 수 있는지 여부에 관한 것이었다. 법원은 정부의 명령에 따르는 것은 묵시적으로 서류의 존재와 납세자가 그 서류를 소지 또는 관리하고 있다는 것을 인정하는 것이며, 납세자가 해당 서류가 소환장에 적시된 서류라는 것을 알고 있다는 사실을 의미하는 것이라고 보았다[15].

법원은 이 사건에서 정부의 손을 들어 주었는데, 제시된 사실에 의거하여 해당 서류는 대부분 회계사에 의해 준비된 것이며, 정부는 서류의 존재 또는 접근을 입증하기 위해 납세자의 증언에 의존하지 않았다는 점을 강조하였다. 또한 법원은 소환장에 응하는 것이 서류의 진정성을 입증하는 것이라는 가능성은 배척하였다. 또한 제출은 단순히 납세자가 해당 서류가 소환장에 적시된 서류라는 점에 관한 생각을 보여주는 것에 불과하다고 보았다. 결론적으로 법원은 서류의 존재와 위치는 필연적인 결론이며 납세자는 사실 그에게 서류가 있다고 인정함으로써 정부가 알고 있는 정보 이상의 그 어떤 정보도 추가하지 않았다고 판시하였다[16].

이 사건에서 연방대법원은 자기부죄거부특권에 대한 두 가지 원칙을 정립하였는데, 하나는 제공행위의 원칙(Act of Production Doctrine)이고 다른 하나는 필연적인 결론 원칙(Foregone Conclusion Doctrine)이다[17]. 기본적으로 자기부죄거부특권은 다음 3가지 요건을 충족하여야 적용될 수 있다. 첫째, 수사기관에 협조할 사법적 강요를 받아야 하며, 둘째, 강요되는 행동이 "진술(testimonial)"에 해당하여야 한

14) Fisher v. United States, 425 U.S. 391, 410 (1976).

15) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 772.

16) Fisher v. United States, 425 U.S. 391 (1976), para. 411; Coulon, Jesse, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 231.

17) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 771.

다[18]. 마지막으로 강요된 진술이 자신에게 형사상 불리한 내용이어야 한다.

제공행위의 원칙은 이 중 두 번째 요건에 대한 것으로 강요되는 행동이 진술에 해당할 것을 요구한다. 필연적인 결론의 원칙은 자기부죄거부특권의 예외에 해당하는 경우로, 강요된 진술의 내용이 이미 수사기관이 알고 있는 정보에 해당할 경우에는 수정헌법 제5조상 자기부죄거부특권에 의해 보호받지 못한다[19].

다. Doe v. United States 사건

Doe 판결에서 연방대법원은 피고에게 불리한 증거가 들어있는 금고의 열쇠를 넘겨주도록 강제하는 것과 금고를 열 수 있는 비밀번호(combination)를 제출하도록 강제하는 것을 구분하였다[20]. Doe 판결에서 피고는 유류 화물에 대한 영수증을 위조하고 소득을 신고하지 않은 혐의로 대배심 수사의 대상이 되었다.

대배심에서는 Doe의 거래은행을 상대로 Doe의 은행계좌 거래내역을 제출하도록 소환장을 발부하였으나 은행은 Doe의 동의 없이는 정보를 제공할 수 없다며 소환장 이행을 거부하였다. Doe는 그의 은행이 정부에 계좌 정보를 제공하는데 동의하

18) 우리나라 대법원은 음주측정이 헌법 제12조 제2항에서 규정하고 있는 진술거부권의 "진술"에 해당하지 않는다고 판단하였다.
"헌법 제12조 제2항은 "모든 국민은 고문을 받지 아니하며, 형사상 자기에게 불리한 진술을 강요당하지 아니한다."고 규정하여 형사책임에 관하여 자신에게 불이익한 진술을 강요당하지 아니할 것을 국민의 기본권으로 보장하고 있고, 헌법이 진술거부권을 기본적 권리로 보장하는 것은 **형사피의자나 피고인의 인권을 형사소송의 목적인 실체적 진실발견이나 구체적 사회정의의 실현이라는 국가이익보다 우선적으로 보호함으로써 인간의 존엄성과 가치를 보장하고, 나아가 비인간적인 자백의 강요와 고문을 근절**하려는 데 있고, 여기서 **"진술"이라 함은 생각이나 지식, 경험사실을 정신작용의 일환인 언어를 통하여 표출하는 것을 의미**하는데 반해, 도로교통법 제44조 제2항에 규정된 **음주측정은 호흡측정기에 입을 대고 호흡을 불어 넣음으로써 신체의 물리적, 사실적 상태를 그대로 드러내는 행위에 불과하므로 이를 두고 "진술"이라 할 수 없으며,** 따라서 주취운전의 혐의자에게 호흡측정기에 의한 주취 여부의 측정에 응할 것을 요구하고 이에 불응할 경우에는 같은 법 제150조 제2호에 따라 처벌한다고 하여도 이를 형사상 불리한 "진술"을 비인간적으로 강요하는 것에 해당한다고 볼 수는 없으므로, 도로교통법의 위 조항들이 자기부죄금지의 원칙을 규정한 헌법 제12조 제2항에 위반된다고 할 수 없다." (대법원 2009. 9. 24., 선고, 2009도7924, 판결).

19) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 773.

20) Doe v. United States, 487 U.S. 201 (1988); Coulon, Jesse, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, pp. 228-229.

는 것이 자신의 수정헌법 제5조상의 권리를 침해하는 것이라고 주장하였다[21].

연방대법원은 피고로 하여금 외국 은행에 자신의 계좌 정보를 제공하도록 강제하는 것은 피고로 하여금 진술을 하도록 요구하는 것이 아니므로 수정헌법 제5조상의 권리를 침해하는 것이 아니라고 판시하였다[22]. 또한 연방대법원은 개인으로 하여금 은행에게 자신의 계좌 거래내역을 제공하는데 동의하도록 강제하는 것은 피고 자신에게 형사상 불리한 증거가 들어있는 금고의 열쇠를 넘기도록 강제하는 것과 유사하다고 보았다[23].

열쇠를 넘겨주는 행위는 개인에게 자신의 머릿속에 있는 생각을 공개하도록 강제하는 것이 아니기 때문에 수정헌법 제5조에 의해 보호받지 못한다. 만약 열쇠 대신에 영장이 개인에게 금고를 열 수 있는 비밀번호를 제출할 것을 강제하는 내용이었다면 그러한 비밀번호는 수정헌법 제5조에 의해 보호받을 수 있다. 개인에게 비밀번호를 제출하도록 강제하는 것은 그 개인의 머릿속에 있는 생각을 표현하도록 요구하는 것이며, 그러한 행위는 진술에 해당하게 된다[24]. 따라서 금고에 대한 비밀번호가 진술에 해당한다면, 암호화된 디바이스의 비밀번호 역시 진술에 해당하게 된다.

Ⅲ. 미국 법원의 판례 분석

오늘날 대부분의 현대인들은 스마트폰의 잠금 기능을 이용하고 있으며, 이는 범죄수사의 장애물로 작용하게 된다. 최근 몇 년간 미국의 연방법원과 주법원에서는 피고인으로 하여금 전자기기를 잠금해제하도록 명령하는 것이 자기부죄거부특권을 규정하고 있는 수정헌법 제5조에 위배되는지가 쟁점이 되어 왔다. 이하에서는 연방

21) Doe v. United States, 487 U.S. at 208; Coulon, Jesse, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 229.

22) Doe v. United States, 487 U.S. at 217-218.

23) Doe v. United States, 487 U.S. at 210.

24) Coulon, Jesse, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 230.

항소법원과 주 법원에서 복호화 명령을 인정한 사례와 인정하지 않은 사례로 나누어 분석하기로 한다.

가. 복호화 명령을 인정한 사례

1) United States v. Apple MacPro Computer[25]

미국 연방 제3순회항소법원(The United States Court of Appeals for the Third Circuit)은 아동음란물 사건에서 영장에 의해 수사기관이 압수한 두 개의 외장하드에 대하여 복호화를 거부한 피고인에 대하여 법정모독죄를 선고하였다. 항소법원은 1심법원의 판결을 지지하면서, 수사기관의 수사결과에 따라 아동음란물 파일이 저장매체에 존재했다는 사실은 이미 필연적인 결론(foregone conclusion)이었으므로 피고인의 수정헌법 제5조상의 권리가 침해되지 않았다고 판단하였다[26].

수사기관은 피고인이 온라인 아동음란물에 접근한 사건과 관련한 수사 과정에서 피고인의 아이폰 2대와 애플 맥프로 컴퓨터 및 외장 하드디스크 두 개를 압수하였다[27]. 피고인은 자발적으로 아이폰에 대한 패스워드를 제공하였으나, 암호화된 정보가 담겨있는 아이폰 어플리케이션에 대한 접근에 대해서는 협조를 거부하였다[28]. 포렌식 분석을 통해 아이폰의 암호화된 데이터베이스에는 2,000개가 넘는 이미지와 비디오 파일이 포함되어 있음을 확인하였다. 또한 포렌식 분석관은 컴퓨터의 패스워드를 알아내었고 분석을 통해 아동음란물 이미지와 “toddler_cp”, “lolicam”, “tor-childporn” 등 같은 아동착취와 관련된 웹사이트 방문기록을 확인하였다[29]. 치안판사는 피고인에게 아이폰, 컴퓨터, 외장하드를 완전히 암호화되지 않은 상태로 제출할 것을 명령하였으나 피고인은 이에 응하지 않았고 패스워드가 기억나지 않는다고 주장하였다. 지방법원은 피고인에게 법정모독죄를 선고하였고 피고인은 이에 항소하였다.

---

25) United States v. Apple MacPro Computer, No. 15-3537 (3d Cir. 3/20/17). https://www.lexology.com/library/detail.aspx?g=c5ab5e3c-2ba5-4236-9bb9-14207cc2c95d 참조.

26) United States v. Apple MacPro Computer, No. 15-3537 (3d Cir. 3/20/17).

27) United States v. Apple MacPro Computer, No. 15-3537 (3d Cir. 3/20/17), pp.3-4.

28) United States v. Apple MacPro Computer, No. 15-3537 (3d Cir. 3/20/17), p. 6.

29) United States v. Apple MacPro Computer, No. 15-3537 (3d Cir. 3/20/17), p. 4.

제3순회법원은 수사기관이 유효한 수색영장에 의해 압수한 디지털 기기에 대하여 암호화 해제를 강제할 수 있는지에 대하여 분석하였다. 피고인은 지방법원이 암호화 해제 명령에 대한 사물관할이 없으며, 명령 자체가 자기부죄거부특권에 관한 수정헌법 제5조를 위반한 것이라고 주장하였으나, 제3순회법원은 이러한 피고인의 주장을 배척하였다[30].

1심에서 치안판사는 연방법원이 관련된 관할권 및 법의 원칙과 적용을 위해 필요하거나 적절한 모든 영장을 발부할 수 있도록 허가하는 '모든 영장법(All Writs Act)[31]'을 법적 근거로 삼았다. 피고인은 수사기관은 모든 영장법이 아니라 대배심 절차를 통해 명령 준수를 강제하여야 하므로, 치안판사는 암호화 해제 명령을 발부할 관할권이 없다고 주장하였다. 제3순회법원은 피고인의 주장을 배척하고 기존 수색영장의 효력을 발생시키기 위해 필요하고 적절한 수단이라고 판시하였다.

제3순회법원은 수정헌법 제5조 이슈에 대한 선결적 고려를 위한 항소를 할 수 없는 절차적 근거에 대해 판단하였다. 또한 항소법원은 1심 법원의 결정에 대한 어떠한 오류도 발견하지 못하였다고 판시하였다. 제3순회법원은 자기부죄거부특권이 적용되어야 한다고 판시한 제11순회법원의 판결을 참조하였다. 그러나 제3순회법원은 제11순회법원 판결의 사안과 해당 사건을 구분하여야 한다고 보았다. 이 사건에서는 수사기관은 기기의 암호화된 영역에 파일이 존재하며, 피고인이 이러한 파일에 접근할 수 있다는 점을 입증하는 증거를 제출하였으므로, 피고인의 행위의 진술적 요소가 "필연적인 결론"에 해당한다고 보았다. 따라서 암호화 해제 명령이 피고인의 수정헌법 제5조상의 권리를 침해하지 않는다고 판시하였다.

제3순회법원은 이 이슈를 판단한 두 번째 연방순회법원이다[32]. 또한 이 사건은

---

30) Nixon Peabody LLP, Third Circuit upholds the forced decryption of hard devices, April 5 2017. https://www.lexology.com/library/detail.aspx?g=c5ab5e3c-2ba5-4236-9bb9-14207cc2c95d 참조.

31) 28 U.S. Code § 1651.
(a) The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.
(b) An alternative writ or rule nisi may be issued by a justice or judge of a court which has jurisdiction.

32) In *In re: Grand Jury Subpoena Duces Tecum Dated March 25, 2011: U.S. v. John Doe*, 670 F.3d 1335 (11th Cir. 2012).

피고인에 대하여 암호화되지 않은 데이터의 제출을 강제하기 위해 모든 영장법의 사용을 지지한 최초의 판례이며, 자기부죄거부특권에 대한 피고인의 주장을 극복하기 위하여 "필연적인 결론" 원칙을 적용한 최초의 판례이다. 이 판례가 수사관들에게 주는 시사점은 피의자가 기기를 소유하거나 소지하거나 사용하고 있다는 사실, 기기 내의 내용에 대하여 알고 있다는 사실, 데이터가 패스워드로 보호되거나 암호화되어 있다는 것을 알고 있다는 사실, 해당 내용을 복호화할 수 있는 능력에 대하여 입증할 수 있는 증거를 확보함으로써 "필연적인 결론" 원칙을 입증하는 것이 중요하다는 것이다[33].

2) Commonwealth v. Jones

2019년 3월, 미국의 매사추세츠 주 최고 법원은 Commonwealth v. Jones 사건에서 정부가 특정 상황 하에서 피고인에게 전자 기기를 잠금해제하도록 강제할 수 있다고 판시하였다[34]. 법원은 compelled decryption 사건에서 두 가지의 헌법적 쟁점에 대하여 판단하였다. 첫 번째, 법원은 정부가 "피고인이 패스워드를 알고 있다는 것이 필연적인 결론이 되도록 피고인이 전자기기를 복호화할 수 있는 패스워드를 알고 있었다는 사실을 입증하여야 한다"고 판시하였다. 두 번째, 법원은 피고인이 패스워드를 알고 있다는 사실이 필연적인 결론이라는 것을 정부가 합리적인 의심을 넘어선 정도로(beyond the reasonable doubt) 입증할 책임이 있다고 판시하였다[35].

이 사건의 사실관계를 살펴보면, 2016년 경찰은 한 여성으로부터 신고를 받았는데, 신고 내용은 피고인 Dennis Jones가 신고자에게 성매매 여성으로 일하지 않겠냐고 권유했다는 것이었다. 경찰의 수사 결과, Jones가 LG 스마트폰을 사용하고 있었다는 것을 확인하였으며, 신고자는 수사기관에 그와 대화를 나눌 당시 그 해당

33) Robert Cauthen, The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes, and/or Passwords (Case Law Update), The Informer, Federal Law Enforcement Training Center(FLETC), Department of Homeland Security, April 2017, p.7.

34) Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019).

35) Nathaniel Sobel, The Massachusetts High Court Rules That State Can Compel Password Decryption in Commonwealth v. Jones, Lawfare, April, 2019. https://www.lawfareblog.com/massachusetts-high-court-rules-state-can-compel-password-decryption-commonwealth-v-jones 참조.

스마트폰을 사용하고 있었다고 진술하였다. LG 스마트폰의 전화번호는 신고자의 스마트폰 전화번호부에 Jones의 이름으로 저장되어 있었고 신고자의 스마트폰 분석 결과 신고자의 스마트폰과 LG 스마트폰간의 성매매와 관련된 통신 내역이 다수 발견되었다. 또한 신고자를 사교모임 동반자로 광고하는 웹사이트 포스팅에도 LG 스마트폰 전화번호가 연락처로 기재되어 있었다.

수사를 개시한 직후, 경찰은 Jones를 체포하였고 이후 그를 인신매매 관련 죄명으로 기소하였다. 경찰은 Jones의 호주머니에서 LG 스마트폰을 발견하였고 해당 스마트폰에 대한 수색영장을 발부받았다. 이후 스마트폰이 암호로 잠겨있다는 사실을 발견하였고 수사관들은 그들이 잠금기능을 우회하는 기술적 역량을 보유하고 있지 못하여 수색영장을 집행하는 것이 불가능하다고 판단하였다.

수사기관은 Jones에게 LG 스마트폰의 잠금을 해제하도록 강제하는 법원의 명령을 신청하였으나, 판사는 해당 신청을 기각하였다. 판사는 수사기관이 Jones의 패스워드 지득 사실이 필연적인 결론이라는 점을 입증하지 못하였다고 판단하였다. 다음날 수사기관은 법원에 Jones의 패스워드 지득이 사실상 수정헌법 제5조상의 필연적인 결론이라는 점을 입증하는 추가적인 정보를 제출하였다. 이러한 정보에는 다음과 같은 내용이 포함되었다.

- LG 스마트폰의 가입자정보를 통한 스마트폰과 피고인의 연관성
- LG 스마트폰의 기지국 위치 정보 기록
- 과거에 동 범죄사실과 관련 없는 사건에서 피고인이 LG 스마트폰이 자신의 전화번호라고 경찰에 진술했던 내용

필연적인 결론 원칙을 어떻게 적용할 것인지와 관련하여, 법원은 2014년 Commonwealth v. Gelfgatt 사건[36]의 결정을 인용하였다. 동 사건에서 정부는 사기 및 사문서위조 등의 혐의로 기소된 피고인 Leon Gelfgatt에 대하여 피고인의 집에서 발견한 컴퓨터의 복호화 명령을 신청하였다. 법원은 "피고인이 암호를 해제하는 행위가 전달하는 사실은 피고인이 컴퓨터와 컴퓨터에 저장된 내용에 대한 소유권과

36) Commonwealth v. Gelfgatt, 468 Mass. 512, 520-526 (2014).

통제권한을 가진다는 사실, 암호화된 사실을 알고 있음, 암호화 키를 알고 있음을 포함"하며, 이러한 사실은 이미 수사기관이 알고 있는 사실에 해당하고 필연적인 결론 원칙이 적용되므로 복호화 명령은 수정헌법 제5조를 위반하지 않았다고 판단하였다[37].

그러나 이러한 법원의 판시에서는 정부가 단순히 피고인이 암호를 알고 있다는 사실을 입증함으로써 필연적인 결론을 증명하였는지에 대해서는 명시적으로 나타나지 않고 있다. Jones 판결의 각주에서 법원은 Gelfgatt 분석이 분명하지 않다는 점을 인식하면서, 원칙을 개선하였다.

법원은 우선 강제 암호해제 이슈에 있어서 "피고인에게 암호화된 전자기기에 암호를 입력하도록 강제함으로써 전달되는 유일한 사실은 피고인이 암호를 알고 있고 따라서 기기에 접근할 수 있다는 것이라는 점"을 언급하였다. 또한 법원은 피고인이 전자기기를 복호화할 수 있는 암호를 알고 있다는 점을 수사기관이 반드시 입증하여야 한다고 판시하였다. 또 다른 각주에서 법원은 Gelfgatt 사건에서의 기준이 암호 입력 행위가 기기와 그 내용에 대한 소유권을 내포하는 것이라고 해석되어서는 안 된다고 설명하였다. Gelfgatt 기준을 축소하면서 법원은 "암호를 알고 있다는 사실은 기기와 내용에 대한 소유권이나 통제권한과는 구분되어야 한다"고 판단하였다.

Barbara Lenk 판사는 그의 보충의견에서 다수의견의 접근방식은 "디지털 시대에서 자기부죄거부특권의 헌법적 보호의 종말을 알리는 조짐(death knell)"이라고 보았다. 보충의견에서는 필연적인 결론의 예외가 적용되기 위해서는 수사기관은 확보하고자 하는 문서나 증거를 상당히 상세하게(with reasonable particularity) 설명할 수 있어야 한다고 요구하였다. Lenk 판사는 이러한 접근방식을 지지하는 두 가지 근거를 제시하였다. 첫째, 필연적인 결론 원칙은 상당히 상세하게 기기에 유죄를 입증할 파일의 존재와 위치를 입증할 것을 요구한다. 둘째, Lenk 판사는 수정헌법 제4조와 제5조가 완전히 분리되어 존재하지 않는다고 주장하였다. 보충의견에서는 수정헌법 제4조상 정부가 증거를 확보하도록 허가하는 것과 개인에게 증거를 제출하

37) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 240.

도록 요구하는 수정헌법 제5조의 제한이 조화를 이루도록 하는 것은 수정헌법 제5조상의 보호를 더욱 의미 있게 만들 수 있다고 주장하였다[38].

입증책임과 관련하여, 법원은 주 헌법이 연방 수정헌법 제5조보다 개인의 기본권을 더욱 강력하게 보호하고 있다고 판단하였고, 궁극적으로 형사법에서 가장 높은 기준인 “합리적인 의심을 넘어서는(beyond a reasonable doubt)” 입증 기준을 채택하였다. 다수의견은 판결에서 선례로부터의 2가지 내용을 근거로 제시하였다[39]. 먼저, 법원은 "피고인의 헌법적 권리와 관련된 일부 중요한 사실들은 합리적인 의심을 넘는 입증을 필요로 한다"고 판결한 자백의 임의성에 관한 사건과 피고인의 미란다 권리 포기에 관한 사건을 살펴보았다. 둘째, 법원은 그 선례가 수정헌법 제5조보다 주 헌법 상 자기부죄거부특권을 더욱 광범위하게 해석하였다는 점에 주목했다.

또한 다수의견은 “합리적인 의심을 넘어선” 기준이 필연적인 결론 예외의 취지와 목적을 존중하기 위하여 필수적이라고 판시하였다. 다수의견은 연방대법원의 Fisher 판결은 “예외가 적용되기 위해서는 피고인의 제공행위(act of production)가 수사기관이 이미 알고 있는 정보 이상의 것을 제공하지 않는다는 점에 대해서 수사기관이 상당히 높은 수준의 확신을 가지고 있어야 한다”는 것을 보여주는 것이라고 판단하였다.

---

38) 다수의견은 이러한 보충의견에 대해 장문의 각주로 대응하였다. 보충의견에서 제기한 수정헌법 제4조와 제5조 간의 상호관계에 대하여, 법원은 정부가 적법하게 영장을 발부받았기 때문에 수정헌법 제4조가 이 쟁점과 관련이 있다고 한 주장에 반대하였다. 법원은 수정헌법 제4조와 제5조가 각각 서로 다른 목적, 기능, 요건을 가지고 있으며, 수정헌법 제4조와 제5조는 폰에 저장되어 있는 특정 파일들의 디지털 프라이버시를 보호하기 위한 이중의 보호장치(double protection)를 구성한다고 보았다. 또한 다수의견은 Lenk가 인용한 연방항소법원 사건에 대한 다른 해석을 내놓았다. 다수의견은 제11순회법원 사건에서는 수사기관이 피고인에게 컴퓨터와 외장하드의 “암호화되지 않은 내용을 제출”하도록 요구하였으며 암호를 요구한 것은 아니었다는 점을 강조하였다. 제3순회법원 사건과 관련해서 다수의견은 항소법원이 “수사기관이 해당 기기에 저장된 내용을 알고 있다는 사실이 compelled decryption 명령에 있어 ‘필연적인 결론’의 핵심내용을 구성하지 않는다고 판단하였음”을 명시적으로 언급하면서 해당 사건에 다른 심사기준을 적용하기로 결론 내렸다는 점을 강조하였다.

39) 캘리포니아 연방법원은 이전 선례에서 전자기기의 패스워드를 피고인이 알고 있다는 사실이 수정헌법 제5조 상의 필연적인 결론이라는 점을 입증할 책임은 정부에게 있다는 점을 분명히 언급하였다. 해당 사건에서 법원은 “명백하고 확실한 증거(clear and convincing evidence)”가 적절한 기준이라고 판단하였다.

3) State v. Stahl[40]

State v. Stahl 사건에서 피고인은 어느 가게에서 쇼핑하고 있던 여성 피해자의 신체를 몰래 촬영하려고 시도했다는 혐의로 체포되어 불법 비디오촬영죄(video voyeurism)[41]로 기소되었다[42].

체포과정에서 피고인은 Sarasota 카운티 경찰에게 그는 스마트폰을 소지하지 않고 있고 스마트폰이 집에 있다고 진술하였다. 경찰은 영장을 발부받아 그의 자택을 수색하여 스마트폰을 압수하였으나, 암호 없이는 잠금을 해제할 수 없었다. 피고인은 암호를 제공하지 않고 협조를 거부하였으며, 플로리다 주 정부는 암호를 제출하도록 강제하는 명령을 법원에 신청하였다[43].

1심 법원에서는 주 정부의 신청을 기각하였고 피고인에게 암호를 넘겨주도록 강제하는 것은 그의 수정헌법 제5조 자기부죄거부특권을 침해하는 것이라고 판시하였다. 암호를 넘겨주는 행위는 피고인에게 암호를 기억해내도록 강제하는 과정에서 "그의 머릿속에 있는 내용을 사용"하도록 강요하는 것이 된다. 만약 증거의 강제가 피고인에게 머릿속에 있는 내용을 공개하도록 하는 것이라면, 해당 증거는 형사상 불리한 진술에 해당하므로 수정헌법 제5조에 의해 보호되어야 한다.

또한 1심 법원은 해당 사건에서 필연적인 결론 원칙을 적용할 수 없다고 보았다. 주 정부는 증거의 위치(location), 존재(existence) 및 진정성(authenticity)을 이미 알고 있다는 것을 입증함으로써 필연적인 결론 원칙의 요건을 충족하여야 한다[44]. 그러나 해당 사건에서 1심 법원은 주 정부가 압수한 스마트폰과 피고인이 범행장소에

40) State v. Stahl, 206 So. 3d 124 (Fla. App. Ct. 2016).

41) 이는 우리나라 「성폭력범죄의 처벌 등에 관한 특례법」 제14조(카메라 등을 이용한 촬영)에 대응하는 범죄라고 볼 수 있다.

42) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 232.

43) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 233.

44) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, pp. 233-234.

서 가지고 있었던 스마트폰이 동일한 것임을 입증할 수 없었으므로 주 정부가 증거의 위치 요소를 입증하는데 실패했고, 따라서 필연적인 결론 원칙이 적용되지 않는다고 판시하였다. 또한 피고인의 집에는 다수의 사람들이 거주하고 있었고 주 정부는 압수한 스마트폰이 피고인 소유의 스마트폰이었는지 입증하지 못하였다.

항소법원에서는 두 가지 이유로 1심 법원의 결정을 파기하였다. 항소법원은 비밀번호가 진술에 해당하지 않고 수정헌법 제5조상의 자기부죄거부특권에 의해 보호되지 못한다고 보았다. 또한 항소법원은 필연적인 결론의 원칙이 적용될 수 있다고 보았고 비밀번호의 강제가 진술에 해당한다고 하더라도 이를 강제할 수 있다고 판시하였다.

항소법원은 만약 강제된 증거가 피고인의 머릿속에 있는 생각을 광범위하게 사용하지 않거나 그가 기소된 범죄와 직접적으로 관련이 없다면, 강제된 정보는 그것이 누군가의 머릿속에서 나온 것이든 아니든 간에 중요한 진술에 해당하지 않고 따라서 수정헌법 제5조의 보호를 받지 못한다고 판시하였다[45].

1심 법원의 판단을 파기하면서 항소법원은 이 사건에서 필연적인 결론 원칙이 적용되며, 만약 비밀번호가 진술에 해당한다고 할지라도 주 정부가 독립적인 방법을 통해 증거의 존재, 소유 및 진정성을 입증했기 때문에 수정헌법 제5조의 보호를 받지 못한다고 판시하였다[46].

항소법원은 주 정부가 비밀번호를 입력하지 않고는 스마트폰을 수색할 수 없기 때문에 비밀번호는 존재한다는 사실을 입증하였다고 보았으며, 주 정부가 상당히 상세하게 스마트폰이 피고인의 것이고 따라서 비밀번호가 피고인의 소유라는 점을 입증하였다고 보았다[47].

---

45) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 235.

46) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 235.

47) Jesse Coulon, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018, p. 236.

나. 복호화 명령을 인정하지 않은 사례

1) In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011[48]

동 사건의 사실관계는 다음과 같다. 수사기관은 아동음란물 사건을 수사하면서 John Doe라고 알려진 익명의 용의자에게 아동음란물이 들어 있는 것으로 의심되는 여러 개의 하드디스크의 복호화된 내용을 제출하도록 요구하는 소환장을 발부받아 제시하였다[49]. Doe의 하드디스크에 대한 포렌식 분석 결과, 하드디스크가 TrueCrypt라는 프로그램으로 부분적으로 암호화되어 있는 것으로 나타났다. 분석관은 하드디스크의 일부에 접근할 수 있었지만, 해당 부분은 비어 있었고 TrueCrypt를 사용하여 암호화된 하드디스크의 특정 부분에 접근할 수 없었다[50]. 분석관은 로 데이터(raw data)를 확인하여 TrueCrypt가 사용되었다는 점을 발견하였으나 복호화할 경우 어떤 정보가 포함되어 있을지는 알 수 없었다. Doe는 복호화된 내용을 제출하지 않았고 거부 사유로 자기부죄거부특권을 주장하였다.

제11순회법원 Tjoflat 판사는 Doe가 유효한 자기부죄거부특권을 향유하고 있으며, 소환장을 응하도록 강요받아서는 안 된다고 판시하였다[51]. Tjoflat 판사는 소환장에 응하는 것이 Doe가 "잠재적으로 유죄를 입증할 수 있는 파일의 존재와 위치를 알고 있으며, 하드디스크의 암호화된 부분을 그가 소유, 통제하고 있고, 접근할 수 있다는 사실, 그리고 해당 파일들을 복호화할 수 있는 능력이 있다는 것"을 진술하는 것과 같게 된다고 보았다[52]. 판결문에는 왜 암호해제 행위가 이러한 진술을 함축하는지에 대한 분석이 드러나 있지 않다.

법원은 필연적인 결론 원칙이 적용되지 않는다고 판단하였는데, Tjoflat 판사는

48) In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1349 (11th Cir. 2012).

49) Orin S. Kerr, Computer Crime Law, Fourth Edition, West Academic Publishing, 2018, pp. 601-607.

50) Orin S. Kerr, Computer Crime Law, Fourth Edition, West Academic Publishing, 2018, pp. 601-607.

51) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 786.

52) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 786.

이 원칙이 정부가 하드디스크 내의 정보를 이미 알고 있다는 사실을 상당히 상세하게 입증할 수 있어야만 적용된다고 보았다. 이 사건에서는 정부가 암호화된 디스크에 어떤 정보가 저장되어 있는지 알지 못하였기 때문에 필연적인 결론 원칙은 적용되지 않는다고 보았다[53]. 제11순회법원은 정부가 발견하고자 하는 내용을 충분히 특정해서 설명하지 못했다는 점이 문제였다고 지적하면서 정부가 Doe로부터 제출을 요구할 당시에 하드디스크에 어떠한 파일이 있는지에 대한 충분한 지식을 소명하지 못하였다고 판시하였다[54]. 암호화된 벽 뒤에 숨겨진 것이 무엇인지 알지 못한 상태로 정부는 확보하고자 하는 파일을 법원에 소명하지 못하였고 따라서 필연적인 결론 원칙이 적용되지 못한 것이다[55].

2) Seo v. State[56]

인디애나주 Hamilton County 경찰은 Seo를 피해자 D.S.에 대한 스토킹과 협박, 프라이버시 침해 및 D.S.에 대한 접근금지 명령을 위반한 혐의로 기소하였다. 경찰이 Seo를 체포할 당시 그녀는 스마트폰(아이폰 7S 기종)을 소지하고 있었고 D.S.에게 보낸 다수의 메시지에 사용된 번호가 해당 스마트폰의 번호와 일치하였다. 그녀는 체포 이전에 D.S.를 강간 혐의로 고소하였는데, 체포 당시 소지한 스마트폰은 당시 경찰에게 자발적으로 잠금해제하여 제출한 스마트폰과 동일한 것이었다[57].

Hamilton 법원은 Seo에게 스마트폰에 대한 복호화를 명령하는 영장을 발부하였는데, Seo는 그것이 수정헌법 제5조 상의 자기부죄거부특권을 침해하는 것이라고 주장하며, 명령에 대한 이행을 거부하였다. 법원은 Seo에 대하여 법정모독죄(contempt)를 선고하였고 이를 면하기 위해서는 스마트폰을 잠금해제하거나 비밀번

53) Orin S. Kerr, Computer Crime Law, Fourth Edition, West Academic Publishing, 2018, pp. 601-607.

54) Orin S. Kerr, Computer Crime Law, Fourth Edition, West Academic Publishing, 2018, pp. 601-607.

55) Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019, p. 786.

56) Katelin Enjoo Seo v. State of Indiana, No. 29A05-1710-CR-2466, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018).

57) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), paras. 4-7.

호를 “1234”로 변경하라고 명령하였다[58].

Seo는 이에 항소하였고 1심 법원의 스마트폰 복호화 명령은 수정헌법 제5조상의 자기부죄거부특권을 침해하는 것이라고 주장하였다[59]. Seo는 그녀의 스마트폰 비밀번호가 사실상 진술에 해당하고 이를 공개하거나 스마트폰 잠금을 해제하라고 강제하는 것은 수정헌법 제5조 상 강요당하지 않을 진술에 해당한다고 주장하였다[60].

인디애나 주는 1심 법원의 명령에 대해서는 그것이 Seo에게 비밀번호를 공개하라고 강제한 것이 아니라 비밀번호를 이용해서 잠금기능을 해제하라고 요구한 것이므로 수정헌법 제5조가 적용되지 않는다고 주장하였다[61].

법원은 Seo가 잠금을 해제하여 스마트폰에 있는 정보를 복호화하는 행위는 진술에 해당한다고 보았다. 그 이유는 단순히 비밀번호가 연방대법원의 Doe 판결에서의 금고 비밀번호(combination)와 유사하기 때문이 아니라 Seo의 복호화 행위가 주 정부가 발견하고자 하는 파일을 재생성(recreate)하는 것이 되기 때문이다[62]. 스마트폰 또는 다른 저장매체의 정보가 암호화되어 있을 경우, 암호문(cyphertext)은 사람이 지득할 수 없고, 구분할 수 없는 형태로 존재한다. 이러한 파일들은 비밀번호가 입력되고 복호화되기 전까지는 유의미하게 존재하지 않게 된다. 따라서 법원은 Seo에게 스마트폰의 잠금을 해제하라고 명령하는 것은 종이로 된 문서의 제출과는 완전히 다른 성격의 것이라고 보았고, 복호화 명령은 정부가 찾고 있는 정보를 말 그대로 재생성하라는 명령으로 볼 수 있기 때문에 디지털 정보의 재생성은 단순한 문서제출보다 더더욱 진술에 해당한다고 판단하였다[63].

필연적인 결론의 원칙과 관련하여 인디애나 주는 이 사건에서 필연적인 결론의 원칙이 적용되기 때문에 Seo에 대한 복호화 명령이 수정헌법 제5조를 위반하지 않는다고 주장하였다[64]. 인디애나 주는 본 사건의 사실관계에 따라 필연적인 결론의 원칙이 적용되어야 한다고 주장하였다. 인디애나 주는 해당 스마트폰의 정보가 아

58) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), paras. 8-9.
59) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 17.
60) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 33.
61) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 34.
62) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 40.
63) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 40.
64) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 42.

닌 비밀번호 자체에만 초점을 맞추었다[65].

그러나 Seo는 이 사건에서 주 정부가 스마트폰에서 발견하고자 하는 디지털 파일이나 증거에 대하여 상당히 상세하게 설명하지 못하고 있으므로 필연적인 결론 원칙이 적용되지 않는다고 주장하였다[66].

Seo에게 비밀번호를 입력하도록 강제하는 것은 스마트폰 내에 저장된 모든 정보를 재생성하도록 하기 위함이다. 따라서 이 사건에서 강제되고 있는 것은 단순히 비밀번호가 아니라 아이폰에 저장된 모든 정보이다. 따라서 주 정부는 상당히 상세하게 스마트폰에 저장된 정보에 대해 설명할 수 있어야 한다[67].

법원은 주 정부가 아이폰의 정보를 압수하기 위하여 발부받은 수색영장에는 주 정부가 발견하고자 하는 디지털 정보에 대한 상세한 설명이 포함되어 있지 않았다고 보았다[68]. 따라서 법원은 주 정부가 디지털 파일을 식별하거나 디지털 파일의 위치에 대해 상세한 설명을 할 수 있음을 입증하지 못하였기 때문에 필연적인 결론 원칙의 요건을 충족하지 못하였다고 보았다[69].

Ⅳ. 영국의 수사권한법과 키 제출 명령[70]

2007년부터 영국은 수사권한규제법(Regulation of Investigatory Powers Act, RIPA)에 따라 복호화 명령을 허용해왔다. 2016년 수사권한법(Investigatory Powers Act of 2016, IPA)은 이러한 권한을 유지하고 더욱 확장했다. 수사권한법은 영장에 따라 통신을 복호화하는데 기술적 협조를 의무화하였고, 기업들에게 단대단 암호통신을 복호화할 수 있도록 강제할 수 있는 권한을 부여하였다.

2000년 영국은 수사권한규제법(RIPA)을 제정하였고 복호화는 동법에 핵심적인

65) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 45.
66) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 47.
67) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 49.
68) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 51.
69) Seo v. State, 109 N.E.3d 418 (Ind. Ct. App., Aug. 21, 2018), para. 54.
70) Daniel Severson, The Encryption Debate in Europe, pp. 6-11.

내용이었다. 전문에서는 이 법이 “통신 감청”권한 뿐만 아니라 암호 또는 패스워드로 보호된 데이터를 복호화하거나 접근할 수 있도록 하는 수단도 제공하기 위하여 제정되었음을 명확히 하고 있다. 동법의 제3부에서는 “암호화 등으로 보호된 전자데이터의 수사”를 규정하고 있다. 특히 정부가 “보호된 정보”를 적법하게 취득한 경우에, 특정 공무원은 소위 “제49조 통지서(Section 49 Notice)”를 발부할 수 있으며, 이를 통해 특정인에게 암호화 키를 공개하거나 정보를 인지할 수 있는 형태로 제출할 것을 요구할 수 있다. 제49조 통지서는 (1) 국가안보 이익을 위하여, (2) 범죄를 탐지하거나 예방하기 위하여, 또는 (3) 영국의 경제적 이익을 위하여 필요한(necessary) 경우에 발부될 수 있다. 국무장관은 복호화 비용을 상쇄하기 위하여 적절한 배상을 제공할 수 있다.

그러나 이러한 통지에 불응하면 2년 이하의 징역에 처하고 국가안보 사건이나 아동음란물 사건의 경우에는 5년 이하의 징역에 처한다. 제49조 통지서는 비밀유지의무도 포함하고 있는데 만약 이러한 통지서를 송달한 자는 해당 사실에 대한 비밀유지의무가 있고 이를 위반할 경우에 벌금 또는 5년 이하의 징역형이 규정되어 있다. 영국 의회가 2000년에 RIPA를 제정하였으나 내무부는 이러한 복호화 규정을 바로 적용하지는 않기로 했다. 왜냐하면, 당시에는 암호기술의 사용이 예상보다 그리 많지 않았기 때문이다. 이러한 복호화 권한은 2007년 10월 1일 발효되었고, 당시 내무부는 관련된 실무규칙(code of practice)을 발표하였다. Office of the Surveillance Commissioners(OSC)[71]에서는 연례보고서를 통해서 영국의 정보기관인 정부통신본부(Government Communications Headquarters (GCHQ)) 산하의 국가기술지원센터(National Technical Assistance Centre (NTAC))의 통계를 제공하고 있다[72]. NTAC는 공공기관, 특히 법집행기관이나 정보기관에게 기술지원을 제공하고 있으며, 암호화된 전자정보를 적법하게 획득하기 위한 시설 및 장비를 제공하고 있다.

71) Office of Surveillance Commissioners (OSC)는 공공기관의 비밀 감시 및 비밀 인적자원정보 활동을 감독하는 기관이며, 2016년 수사권한법에 의하여 현재는 Investigatory Powers Commissioner's Office로 변경되었다.

72) 2014년에서 2015년 사이에, NTAC는 제49조 통지서 발부 신청 총89건 중에서 88건을 허가하였다. 이 중 22건의 복호화 명령은 이행이 거부되었으나 대부분의 경우 정부는 명령불이행으로 기소하지 않기로 결정했다. 2014~2015년 사이에 제49조 통지서 불이행으로 기소되어 유죄가 선고된 건수는 총3건이었다.

2016년 영국 의회는 수사권한법을 제정하였다. 총291페이지에 달하는 구체적이고 기술적인 이 법은 영국의 정보기관, 안보기관 및 법집행기관의 감시 권한을 더욱 강화하였다. 수사권한법은 통신내용과 메타데이터의 감청과 보관에 대하여 규정하고 있으며 장비 감청(equipment interference)과 복호화에 대한 규정도 포함하고 있다. 영국에서는 최초로 수사권한법에서 영장에 대한 사법심사를 도입하였다,

수사권한법은 RIPA 제3부 하의 암호화된 데이터의 수사를 그대로 유지하면서 일부를 개정하였다. 수사권한법은 제49조 통지서를 수사권한 감독관(Investigatory Powers Commissioner(IPC))의 강화된 감독 권한 하에 두었다. IPC는 정부의 수사권한 사용을 감독하여야 하고 매년 국무총리에게 보고서를 제출하여야 한다. 또한 IPC는 암호로 보호된 전자정보의 수사를 독자적으로 심사하여야 하며, 법집행기관은 개인에게 암호화 키를 제출하라고 요구하는 제49조 통지를 할 때마다 IPC에게 통보하여야 한다. 또한 수사권한법은 제49조 통지서가 발부될 수 있는 경우를 확대하였는데, RIPA는 정부가 통신감청을 통해 보호된 정보를 획득한 경우에만 제49조 통지서 발부를 허용한 반면, 수사권한법은 정부가 “통신의 이차적 데이터(secondary data from communications)” 즉, 메타데이터의 감청을 통해 보호된 정보를 획득한 경우에도 제49조 통지서 발부를 허용한다.

또한 수사권한법은 복호화를 강제할 수 있는 광범위한 법적 권한을 신설하였다. 그러나 법 규정에서는 암호화(encryption)이라는 용어는 사용하지 않았다. 제253조에서는 국무장관이 전화통신 서비스제공자에게 정부기관에게 협력할 것을 요구하는 “기술역량 통지서(technical capability notices)”를 제시할 수 있다고 규정하고 있다. 이러한 기술역량 통지서를 통해 부과할 수 있는 의무의 범위는 광범위하다. 정부는 서비스제공자에게 디바이스, 설비, 또는 서비스를 무제한적으로 제공하라고 요구할 수 있고 “서비스제공자에 의해 적용된 통신 또는 데이터의 전자적 보호”를 제거하도록 요구할 수 있으며, “정보의 처리 또는 공개와 관련된 의무”를 이행할 것을 요구할 수 있다. 동 법은 국무장관으로 하여금 기술자문위원회 및 다른 이해관계자와의 협의하여 이러한 광범위한 권한을 적절한 규정을 통해서 이행할 것을 요구하고 있다.

국무장관은 그것이 필요성의 원칙과 비례의 원칙을 충족하고 사법 당국에서 이를

승인한 경우에 기술역량 통지서를 발부할 수 있다. 그러한 통지서를 발부함에 있어서 국무장관은 이행에 드는 비용과 기술적 실현가능성을 고려하여야 하고 그로 인해 영향을 받을 수 있는 이용자의 수도 고려하여야 한다. 정부는 영국 밖에 있는 자에 대하여도 기술 역량 통지서를 제시할 수 있다. 또한 이러한 기술역량 통지서에 대해서는 아무런 시간적 제한이 없고 국무장관이 "합리적인" 기간이라고 판단하는 만큼의 기간까지 연장이 가능하다.

Ⅴ. 우리나라에 대한 시사점

우리나라에서도 수사과정에서 스마트폰 잠금해제를 하지 못한 사례가 종종 언론을 통해 보도되고 있다. 2016년도에는 참여연대 공직선거법 위반 사건 수사 과정에서 압수한 스마트폰(아이폰 6)의 잠금해제 비밀번호를 피의자가 알려주지 않아 분석하지 못한 사례가 있었고[73], 최근에는 청와대 하명수사 의혹과 관련하여 사망한 수사관의 스마트폰(아이폰X)의 잠금해제를 하지 못한 사례가 보도되었다[74].

위에서 살펴본 미국의 사례와 같이 우리나라에서 수사기관이 스마트폰 암호화 해제 또는 암호화된 디스크의 파일을 복호화하라고 요구하는 것이 현행법상 가능한가? 이와 관련하여 도박사이트 수사 과정에서 서울북부지원이 스마트폰 잠금해제를 위해 필요한 지문정보에 대한 검증영장을 발부한 사례가 있다.[75]

만약 위 사례의 경우 압수수색검증영장의 집행을 거부하면 어떻게 되는가? 우선 현재 영장집행을 강제할 법적 근거는 없으며, 미국과 같이 법원의 명령을 불이행하는 경우 사법방해죄 또는 법정모독죄로 처벌하는 것도 현행법상 불가하다.

국내 일선의 수사 실무에서는 일부 특수한 경우를 제외하고 스마트폰 등 디바이

73) 한겨레, "최신 폰 잠금 못풀어 쩔쩔매는 경찰", 2016년 11월 23일자. http://www.hani.co.kr/arti/PRINT/771673.html 참조.

74) 한국일보, "아이폰 비밀번호에 막힌 '靑 하명수사 의혹' 수사", 2019년 12월 4일자. https://www.hankookilbo.com/News/Read/201912041702343159 참조.

75) 법률신문, "스마트폰 잠금 해제 위한 '지문 검증' 영장 논란", 2019년 12월 9일자. https://www.lawtimes.co.kr/Legal-News/Legal-News-View/Content/Article?serial=157842 참조.

스 내 전자정보에 대한 압수수색 영장 집행 과정에서 대부분의 피의자나 피압수자가 잠금해제 비밀번호 제공에 협조하고 있다[76].

만약 압수수색영장 집행 시 스마트폰 잠금 해제를 위한 비밀번호를 알려주지 않는 경우, 형사소송법 제120조 제1항[77] 규정상의 "건정을 여는 것" 또는 "기타 필요한 처분"을 근거로 지문정보 등을 요구하거나 기술적인 잠금해제 시도를 해볼 수 있겠으나 실무에서는 통상 추가로 지문, 홍채 등 생체정보에 대한 검증영장을 발부받아 이를 해결하고 있다.

현재 일반적인 범죄수사 과정에서는 피의자들 대부분이 스마트폰 압수수색 과정에서 잠금암호의 제공에 응하고 있으나, 안보 사건이나 중범죄의 경우 잠금암호의 제공을 거부하거나 법정에서 다투어지는 경우가 종종 발생하고 있고 선진국의 사례에 비추어 앞으로 이러한 사례는 더욱 증가할 것이다. 스마트폰 자체에 저장되어 있는 정보 및 스마트폰의 계정과 연동되어 클라우드에 저장되어 있는 정보 등 스마트폰 압수수색을 통해 파악할 수 있는 정보는 무궁무진하다. 이로 인해 수사기관은 사건과 관련 없는 데이터를 과도하게 확보하게 되며, 개인의 프라이버시가 과도하게 침해될 가능성이 높아진다.

향후 스마트폰 압수수색시 잠금해제 거부는 수사상 걸림돌로 작용할 수 있으며, 또한 잠금 해제를 요구하는 것이 적법한가에 대한 법적 논란이 발생할 소지가 있다. 우리나라도 스마트폰 압수수색 관련 법적 논란을 사전에 차단하고 수사과정에서 인권 침해를 최소화하기 위해서 미국의 판례와 영국의 입법례를 참고할 필요가 있다.

국내에서는 아직까지 법정에서 쟁점이 되어 다투어진 사례는 없으나 미국에서는 주 법원과 연방항소법원에서의 판례가 계속 나오고 있다. 그러나 아직 확실하게 정립된 원칙은 없으며 각각의 사실관계가 다르고 주 법원에서 판단하기 때문에 판시내용도 일관되지 못하다. 그럼에도 불구하고 일련의 미국의 판례를 통해 수사기관의 입증책임에 대해서 시사점을 도출해 볼 수 있다. 수사기관은 스마트폰이나 노트

76) 경찰청 훈령 "디지털 증거 수집 및 처리 등에 관한 규칙" 별지 제5호 서식을 살펴보면, 모바일기기의 원본 반출시에 반출 원본 목록에 잠금암호, 백업암호, 잠금패턴 등을 작성하도록 되어 있으며, 대부분 잠금해제 패턴 또는 비밀번호를 제공하는데 협조하고 있다. 서울지방경찰청 수사관 대면 인터뷰(2020. 1. 20.).

77) 제120조(집행과 필요한 처분) ① 압수 · 수색영장의 집행에 있어서는 건정을 열거나 개봉 기타 필요한 처분을 할 수 있다. (밑줄 저자 첨가)

북과 같은 디바이스의 복호화를 위해 어떠한 사실관계를 입증하여야 하는가? 자기부죄거부특권과 관련하여 형사상 불리한 진술이 무엇인가?

우선 스마트폰과 같은 디바이스의 암호를 해제하는 행위에 함축되어 있는 의미를 살펴볼 필요가 있다. 특정인이 디바이스의 암호를 해제할 수 있다는 사실에서 도출할 수 있는 사실은 "해당 디바이스는 나의 소유 또는 점유 하에 놓인 물건이다.", "나는 디바이스의 암호를 알고 있다." 등 두 가지이다. 미국 판례에서 도출된 원칙을 적용하기 위해서는 즉, 수사기관은 이 두 가지의 사실을 입증하여야 한다.

또한 미국의 판례에서 도출된 필연적인 결론 원칙이 적용되기 위해서는 수사기관은 "해당 디바이스에는 형사상 불리한 정보가 저장되어 있다"는 점을 입증하여야 한다. 이를 입증하게 되면 디바이스 복호화 명령에 대하여 자기부죄거부특권을 주장할 수 없게 되기 때문이다. 통상 스마트폰의 경우에는 가입자정보, 사용의 빈번성 등을 통해 스마트폰 소유자와 사용자 등을 입증하기가 용이하다. 그러나 PC 내에 저장된 파일에 대해서는 특히 공용 PC나 사무실에서 사용하는 PC일 경우 입증이 힘들다. 디바이스 내에 범죄와 관련된 증거가 저장되어 있는지 여부의 경우는 스마트폰의 경우 입증하기가 굉장히 힘들다. 이러한 경우 디지털 포렌식, 감청, 진술 등 다른 방법으로 수집된 증거를 통해서 입증하여야 하는데 예를 들어 국가안보 사건의 경우 감청을 통해 수집한 증거를 통해 입증하는 것도 가능할 것이다.

그렇다면 디바이스 복호화 명령을 위해서 수사기관은 어느 정도로 관련 사실을 입증하여야 하는가. 즉 입증의 정도에 대해서는 개연성만으로는 부족하고 상당한 정도로 입증할 것이 필요할 것이다.

영국은 수사권한법을 통해 진술거부특권을 우회할 수 있는 키 제출 명령을 입법화하고 있다. 수사권한법에서는 키 제출명령을 할 수 있는 범죄의 유형을 별도로 규정하고 있지는 않으나, 이러한 명령을 거부하였을 경우 형량을 범죄 유형별로 달리 규정하고 있다. 수사권한법에서는 아동음란물 사건 또는 국가안보 사건의 경우 더 중하게 처벌하고 있다. 우리나라는 아직 이러한 입법이 마련되어 있지 않으나 만약 영국의 수사권한법과 같은 입법을 마련할 경우 통신비밀보호법 상 통신제한조치가 적용되는 특정범죄에만 한정하여 인정하는 것도 가능할 것이다.

Ⅵ. 결론

스마트폰의 잠금을 해제하거나 비밀번호를 제공하라고 강제하는 것이 진술에 해당하는지에 대해서 아직까지 미국 연방대법원이 직접적으로 판단을 내린 적이 없다. 그러나 일련의 판례에서 연방대법원은 문서를 제출하는 특정 행위가 수정헌법 제5조의 취지상 진술에 해당하는지에 대해서는 판단한 바 있다. 중요한 것은 이러한 판례들은 인터넷이나 스마트폰이 존재하지 않던 시절에 발달된 것이라는 점이다.

연방대법원은 형사상 불리할 수 있는 신체적 특징(physical characteristic)을 공개하도록 강제하는 것은 수정헌법 제5조가 적용되지 않는다고 판시한 바 있다[78]. 연방대법원은 여러 신체적 특징 중에서 지문은 진술에 해당하지 않는다고 판시한 바 있다[79]. 그러나 오늘날 안면 인식이나 홍채 스캔과 같은 생체정보를 통한 최첨단 보안 기술의 발전을 고려하면 당시의 판례를 현대 사회에 적용하기에는 무리가 있다.

2018년 미국 연방대법원 역시 Carpenter 판결에서 ”디지털 기술로 인해 발생되는 새로운 문제에 직면했을 때, 연방대법원은 기존의 선례를 무비판적으로 확장하지 않기 위해 신중하게 접근해왔다“[80]고 언급하였는데, 결국 기존의 문서나 유형의 물건에 적용되던 기준을 새로운 디지털 기술에 그대로 수용하여 적용하는 것은 문제가 있다는 지적이다.

대부분의 미국 법원에서는 수정헌법 제5조의 자기부죄거부특권 조항이 기밀성(confidentiality)과 관련하여 프라이버시를 보호하는 조항이라고 인식하고 있다. 따라서 전통적인 종이 기반의 매체와 비교하여 스마트폰에 저장된 디지털 정보의 양은 질적으로나 양적으로 어마어마한 차이가 난다. 또한 스마트폰은 이를 사용하는 개인의 프라이버시가 집약되어 있는 디바이스[81]라고 할 수 있다. 따라서, 스마트폰 비밀번호의 공개를 강제하는 것은 프라이버시와 관련하여 분명 시사점이 있다고 할

78) United States v. Hubbell, 530 U.S. 27 (2000), 35.

79) Schmerber v. California, 384 U.S. 757, 763-65 (1966)); United States v. Hook, 471 F.3d 766, 773-74 (7th Cir. 2006).

80) Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018).

81) 이러한 점 때문에 혹자는 스마트폰을 사용자의 디지털 쌍둥이(digital twin)이라고 언급하기도 한다. Roberto Saracco, My smartphone, my (future) digital twin?, IEEE Blog, January 21, 2019. https://cmte.ieee.org/futuredirections/2019/01/21/my-smartphone-my-future-digital-twin/ 참조.

수 있다. 디지털 정보의 저장매체에 대한 법적인 평가는 기존의 문서에 대한 법적 평가와는 분명히 달라야 하고 법원은 보다 설득력 있는 접근방식을 도입해야 할 것이다.

우리나라에는 아직 스마트폰 등 디바이스 복호화에 대한 문제가 심각하게 대두되고 있지 않지만 몇몇 사례가 언론을 통해 보도되고 있다. 향후 이러한 문제에 대비하여 다양한 법적 쟁점에 대한 연구와 심도 깊은 논의가 필요하고 기술적으로도 암호화 문제를 극복할 수 있는 방안[82]을 모색해야 할 것이다.

82) 최근 발표된 기술적 대안에 관한 논문으로는, 이민형, 이상진, 인증정보 획득을 이용한 클라우드 메신저의 사용자 데이터 획득 기법에 관한 연구, 디지털포렌식연구 제13권 제4호, 2019 참조.

참고문헌

1. 국내문헌

박희영, 암호통신감청 및 온라인수색에서 부수처분의 허용과 한계, 형사정책연구 제30권 제2호, 2019.

손유리, 박성현, 손지훈, 김기범, 김영웅, 지문정보 이용 스마트폰 포렌식과 통제방안, 한국치안행정논집 제16권 제1호, 2019.

이민형, 이상진, 인증정보 획득을 이용한 클라우드 메신저의 사용자 데이터 획득 기법에 관한 연구, 디지털포렌식연구 제13권 제4호, 2019.

이흔재, 미국의 휴대전화에 대한 통신감청 및 위치정보 확인수사의 법제 및 최근 판례에 대한 비교법적 연구, 법학논총, 제31권 제3호, 2019.

이흔재. 휴대전화 압수·수색관련 문제점에 대한 비교법적 고찰, 법조 제67권 제4호, 2018.

전현욱, 김기범, 조성용, Emilo C. VIANO, 사이버범죄의 수사 효율성 강화를 위한 법제 개선 방안 연구, 경제·인문사회연구회 미래사회 협동연구총서 15-17-01, 2015.

조도준, 디바이스 암호화에 따른 복호화명령 제도 도입의 필요성, 서울대학교 융합과학기술대학원 석사학위논문, 2016.

2. 해외문헌

Cauthen, Robert, The Fifth Amendment and Compelling Unencrypted Data, Encryption Codes, and/or Passwords (Case Law Update), The Informer, Federal Law Enforcement Training Center(FLETC), Department of Homeland Security, April 2017.

Cohen, Aloni, and Park, Sunoo, Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries, Harvard Journal of Law & Technology,

Vol. 32, No. 1, 2018.

Coulon, Jesse, Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in State v. Stahl, Boston College Law Review, Vol. 59, Issue. 99, 2018.

Encryption Working Group, Moving the Encryption Policy Conversation Forward, Carnegie Endowment for International Peace, 2019.

Finklea, Kristin, Encryption and the “Going Dark” Debate, Congressional Research Service, 2016.

Kerr, Orin S., Compelled Decryption and the Privilege Against Self-Incrimination, Texas Law Review, Vol. 97, Issue. 4, 2019.

Kerr, Orin S., Computer Crime Law (American Casebook Series), 4th Edition, West Academic Publishing, 2018.

Kerr, Orin S. and Schneier, Bruce, Encryption Workarounds, Georgetown Law Journal, Vol.106, 2018.

Peter Swire, Kenesa Ahmad, ‘Going Dark’ Versus a ‘Golden Age for Surveillance’, Center for Democracy and Technology, 2011.

Sacharoff, Laurent, What Am I Really Saying When I Open My Smartphone?: A Response to Professor Kerr, Texas Law Review Online, Vol. 97, 2019.

Sacharoff, Laurent, Unlocking the Fifth Amendment: Passwords and Encrypted Devices, 87 Fordham L. Rev. 203, 2018.

Severson, Daniel, The Encryption Debate in Europe, Aegis Paper Series No. 1702, Hoover Institution, 2017.

Zittrain, Jonathan L., Matthew G. Olsen, David O'Brien, and Bruce Schneier, "Don't Panic: Making Progress on the “Going Dark” Debate", Berkman Center Research Publication, 2016.

Compelled Decryption and the Privilege Against Self-Incrimination: Recent Court Decisions in the United States and Legislation of the United Kingdom

Song, Young-jin*

Smartphones have evolved from conventional wireless communication devices to mobile computers, and the amount of data generated and stored on smartphones has become vast. In addition, encryption of the device itself is causing problems in which information within the device cannot be accessed without biometric or PIN numbers. In order to explore solutions to many of these recent problems, this paper analyzes recent "Going Dark" debates and recent court rulings related to the compelled decryption and the privilege against self-incrimination in U.S. federal and state courts. This paper will also explore the Investigatory Powers Act 2016 of the United Kingdom, which stipulates key disclosure orders for encrypted data. Finally, this paper would like to examine how related discussions are being held in Korea and draw criminal policy implications based on device encryption and compelled decryption.

There is no serious problem in Korea yet with device encryption however several cases have been reported through the media. In the near future, the denial of unlocking devices could pose a stumbling block to the criminal investigation and digital forensics. South Korea also needs to refer to U.S. court cases and British legislation to prevent legal disputes regarding smartphone search in advance and minimize human rights violations during the investigation process. It will also require research and in-depth discussion of the various legal issues that may arise

* Professor, Department of Police Science, International Cybercrime Research Center, Korean National Police University

and seek to overcome the issue of encryption.

❖ Key words : Compelled Decryption, Encryption, Privilege Against Self-Incrimination, Going Dark, Criminal Investigation, Privacy, Data Protection, Digital Forensics, Smartphone Decryption

투고일 : 2월 29일 / 심사일 : 3월 25일 / 게재확정일 : 3월 25일