情報保護學會論文誌
第20卷 第6號, 2010. 12

피의자 개인의 암호이용 통제정책에 대한 연구*

백 승 조,† 임 종 인‡
고려대학교 정보경영공학전문대학원

A Study on National Control Policy for the Use of Encryption Technologies by an Accused Person*

Seung-Jo Baek,† Jongin Lim‡
Graduate School of Information Management and Security, Korea University

요 약

본 논문은 범죄에 사용될 수 있는 암호의 이중사용의 특성 때문에 발생 가능한 수사권 약화라는 암호의 역기능과 키 복구 시스템과 복호화명령제도와 같은 피의자 개인의 암호이용에 대한 통제정책에 대해 살펴본다. 또한 피의자로서의 개인의 암호이용에 대한 통제 정책에서 발생가능한 수사권과 프라이버시권 등 다양한 개인의 헌법적 권리들에 대한 침해 위험을 살펴보고, 각 정책을 과잉규제금지원칙을 적용하여 구체적으로 분석해본다. 마지막으로 국민의 권리와 수사권 확보를 보장하는 균형 잡힌 국내암호통제정책 수립을 위해 고려해야 할 요소들과 대안적인 정책방향을 제시한다.

ABSTRACT

In this paper, we study the dysfunctions of cryptography as dual-use goods and national domestic encryption control policies like key recovery system and decryption order. And we examine risks of the breach of the peoples' constitutional rights like the right to privacy in these policies and analyze these policies by applying the principle of the ban on the over-restriction. Finally, we propose the direction and requirements of our national domestic encryption control policy that maintains the balance of peoples' constitutional rights and investigatory powers.

Keywords: Cryptography Policy, Key Recovery System, Decryption Order, Privacy, Privilege against Self-incrimination

I. 서 론

1.1 연구 배경

누구나 읽을 수 있는 평문을 암호시스템이나 암호알고리즘에 따라 일정한 변형을 통해 인식 불가능한 암호문으로 치환하는 암호(Cryptography)기술은 네트워크화된 현대사회에서 개인의 프라이버시와 기업의 정보자산을 보호하기 위한 필수적인 도구가 되어가고 있다. 반면 암호기술이 범죄와 테러의 수단으로 오용되면서 국가안보를 위태롭게 하고 법집행을 어렵게 하는 역기능 또한 발생하고 있는 상황이다. 즉, 자산이나 개인정보를 강력하게 보호함으로써 사이버범죄를 억제하는 역할을 하는 한편으로 사이버범죄자들이 자신의 공모사실이나 범죄흔적을 효과적으로 숨김으로써 범죄를 촉진하는 역할도 수행할 수 있는 것이다. 특히 암호화 기술은 디지털 증거를 수집하는 디지털 포렌식 기술을 우회하고 회피하기 위한 안티 포렌식 기술의 하나로 활용되고 있다. 이처럼 최근 민간분야에서의 암호 사용이 활성화되면서 암호화된 파일을 적시에 효과적으로 법적 증거로 확보하는 문제는 정보화 사회의 정보기관 및 수사기관의 수사력에 심각한

접수일(2010년 9월 26일), 수정일(2010년 12월 13일), 게재확정일(2010년 12월 16일)
* 이 연구에 참여한 연구자(의 일부)는 '2단계 BK21사업'의 지원비를 받았음
† 주저자, nomadvirus@korea.ac.kr
‡ 교신저자, jilim@korea.ac.kr

〔표 1〕 민간 개인 암호 이용 규제방식의 구분

유형 / 코드	규제 방식	대표적인 예
기술적 코드	키복구/키위탁 시스템[3]	Clipper Chip (美)
규범적 코드	복호화키 제출명령	RIPA Part III (英)

도전요소가 되고 있다. 그 사회가 어떠한 암호이용 통제정책을 가지고 있는지에 따라 암호화된 파일에 대한 디지털 증거의 확보 가능성이 크게 좌우될 수 있다. 만일 강력한 암호이용 통제정책을 가지고 있는 경우 암호화된 파일로부터 디지털 증거를 확보할 수 있는 수사력은 높아지는 반면, 개인이나 기업들이 자신의 개인정보나 기업자산을 충분히 강력하게 보호하지 못하게 되어 범죄의 대상이 될 가능성이 높아지게 되며, 암호이용 통제정책 자체가 개인의 헌법적 권리와 충돌하게 되는 경우도 발생할 수 있다. 따라서 디지털 수사권과 개인의 헌법적 권리, 그리고 암호를 통한 민간의 자산보호능력이 모두 존중될 수 있는 균형 잡힌 암호정책이 요청되고 있다.

이러한 암호기술의 양면성과 이중 기능 도구(dual use technology)라는 성격 때문에 국제기구인 OECD 또한 국가 및 범세계적 정보통신 인프라, 네트워크와 시스템에서의 데이터의 보안성을 보장하고 프라이버시를 보호하기 위해 암호사용을 권장하는 한편, 이러한 암호사용의 권장이 부당하게 공공의 안녕, 법집행 및 국가 안보를 저해해서도 안된다고 명시함으로써 각국이 국가암호정책수립을 하는데 있어 이러한 이중성을 고려해야 함을 명시하고 있다. 이러한 이유 때문에 세계 각국은 암호기술 이용을 촉진하는 한편 악의적인 암호 이용을 규제하기 위한 다양한 정책을 수립하고 있는 상황이다. 지금까지 프라이버시와 법집행간의 균형을 유지하기 위한 국내외의 암호이용 통제시도로는 〔표 1〕에서 보이는 바와 같이 크게 기술적 코드를 이용한 방식과 법을 이용한 방식들이 존재해왔다[2].

첫 번째 방식은 암호시스템에 법집행기관이 필요시에 쉽게 접근할 수 있도록 일종의 백도어를 설치하는 것으로, 대표적인 것으로는 미국의 Clipper Chip 시스템을 들 수 있다. 두 번째 방식은 용의자에게 복호화를 강제할 수 있는 권한을 법에 명시하는 것으로, 대표적인 사례로는 영국 법률인 RIPA (Regulation of Investigatory Powers Act) Part III를 들 수 있다. Bert-Jaap Koops는 가능한 국가암호이용통제정책의 4가지 모델로 ①키복구 및 위탁시스템 등 기술적 코드를 이용한 규제방식, ②복호화명령 및 키제출명령과 같은 법적 코드를 이용한 규제방식, ③직접적인 도청방법을 이용한 규제방식, ④아무 규제도 하지 않는 방임방식 등을 들고 있다〔1〕. 그의 분류법에서 ①이 기술적 코드, ②가 법적 코드에 해당되며, ③과 ④는 별도의 강제적 규제는 두지 않고 국가의 기술적 복호화 능력에만 의존하는 일종의 무규제 방임정책을 말한다.

최근 암호정책의 국제적인 추세를 살펴보면 강제 키복구정책은 여러 문제점 때문에 대부분 도입을 포기하고 있으며, 복호화 강제명령이 그 대안으로 모색되고 있는 상황이지만, 아직까지 도입한 국가들은 그리 많지 않은 상황이다.

Clipper Chip I, II, III, IV 등의 강제 키복구 제도를 추진했던 미국의 경우 프라이버시 침해 논란 등으로 현재 공식적으로 어떠한 자국 내 암호이용 통제도 하고 있지 않고 있으며, RIPA법을 가지고 있는 영국을 포함한 호주, 인도, 말레이시아, 프랑스, 네덜란드 등 일부 국가에서 법집행기관에 복호화명령제도를 두고 있다.

국내의 경우 현재 공식적인 암호이용 통제정책은 존재하지 않는 상황이지만 강제적 키복구 정책에서 복호화 명령에 이르기까지 지속적인 검토와 국내로의 적용가능성을 타진해오고 있는 중이다. 국내에서는 1999년에 민간암호사용을 위한 법규를 제정하려는 시도가 국가정보원, 정보통신부 등에 의하여 최초로 시도되었다. 국가정보원은 전문가들로 실무팀을 구성하여 민간 암호사용과 키 복구제도를 명시한 '암호법' 제정을 추진하였으며, 한국인터넷진흥원(구 한국정보보호진흥원)은 1999년 〈정보사회에서의 암호이용촉진을 위한 법제도 환경 개선방안〉〔2〕이라는 보고서에서 암호복구제도를 포함한 법안을 제안했으며, 정보통신부도 민간의 암호이용을 촉진하고 암호산업 육성을 위한 가칭 '암호이용촉진법'의 제정을 밝혔다.

2) 레식(Lawrence Lessig)은 저서 〈Code〉에서 규제수단을 법적 코드와 기술적 코드로 구분하고 있다. 그가 말하는 법적 코드인 '동부 연안 코드'는 의회가 제정한 성문법을 의미하며, 기술적 코드인 '서부 연안 코드'는 사이버공간을 작동하게 하는 소프트웨어와 하드웨어 내부에 새겨져 있는 명령들을 의미한다.

3) Bert-Jaap Koops는 이러한 기술적 코드를 통한 암호규제를 통틀어서 Built-in Law-Enforcement Access to Keys (LEAK)이라고 부르고 있다.

1999년 12월에 발표된 정보통신정책연구원의 〈암호 활용촉진을 위한 법제도 정비방안〉[3]에서는 강제적 복구제도에 대해 실효성은 없으면서 프라이버시에 대한 반비례적인 침해를 가져올 뿐이라며 반대의견을 밝히고 있으며, 자발적 복구를 원칙으로 하고 복구기관에 대해 합법적으로 복구정보를 요청하는 방식을 취하고 있다. 특히 피의자 본인에게 복구정보 제공을 강제하는 방안은 피의자에게 진술거부권이 존재하므로 복호화 강제가 어려울 것이라는 부정적 의견을 제시하고 있다. 같은 해 박민성의 논문 〈정보적 자기결정권과 암호〉[4]에서도 강제적 키복구제도가 정보적 자기결정권이라는 기본권의 본질적 내용을 제한하며 프라이버시권을 심각하게 침해할 위험이 존재하므로 자발적 키복구제도 도입을 제안했다. 또한 법집행력 확보를 위한 대안으로 국가의 복호능력 획득을 위한 복호지원 전문기구의 설립 등을 들고 있다. 이에 반해 2003년 서광현의 논문 〈암호기술의 적법한 사용을 위한 정책개발에 관한 연구〉[5]는 클리퍼정책을 포함한 강제적 키복구제도에 대해 프라이버시 위험성을 지적하면서 암호이용촉진 등에 관한 법률안을 제안하면서 RIPA와 유사한 '정보의 강제공개'를 대안으로 제시하고 있다. 하지만 개인 및 법인에 의한 부정적인 목적의 암호이용 가능성은 높아지고 효과적인 암호이용통제정책에 대한 요구는 높아지고 있는데 반해, 최근에는 오히려 프라이버시 및 인권침해 우려 등으로 인해 암호화 정책 자체에 대한 논의 자체가 이루어지고 못하고 있는 상황이다.

1.2 연구 대상 및 연구 방법론

일반적으로 국가암호통제정책은 암호제품의 수출입 통제정책과 자국 내 암호이용 통제정책으로 구분해볼 수 있다. 암호는 무결성 보장 및 인증을 주된 목적으로 하는 인증용 암호와 비밀 내용을 다른 사람이 알지 못하도록 보관하거나 전송하기 위한 목적으로 사용되는 기밀성 암호로 구분할 수 있는데, 본 논문에서는 위의 다양한 국가암호정책 중에서 디지털 수사에 있어 직접적인 쟁점이 되고 있는 기밀성 암호에 대한 이용 통제정책을 대상으로 한다. 또한 기밀성 암호에 대한 국가 암호이용 통제정책은 프라이버시에 대한 합리적 기대[4]와 자기부죄거부권리[5], 공익적 가치의 유무 및 정도 등을 기준으로 아래와 같이 규제 대상을 분류할 수 있다.

〔표 2〕 기밀성 암호에 대한 국가 암호이용 통제정책 구분

군사적			군사 목적의 암호이용 통제정책
비군사적	공공		공공 기관의 암호이용 통제정책 (공무원 및 업무 PC)
	민간	법인	법인의 암호이용 통제정책
		자연인	피의자 이외 개인의 암호이용 통제정책
			피의자로서의 개인의 암호이용 통제정책

본 논문은 위의 〔표 2〕의 네 가지 영역 중 디지털 수사와 관련하여 가장 민감하고 쟁점이 되는 핵심 영역이라고 할 수 있는 피의자로서의 개인 영역의 적절한 암호이용 통제정책에 대해 살펴본다. 이를 위해서 피의자로서의 개인에 대한 암호이용 통제에 있어 고려해야 하는 개인의 권리에 대해 살펴보며 과잉금지규제 금지원칙기준에 근거하여 강제적 키복구 정책과 복호화 명령 제도와 같은 대표적인 암호이용통제정책들을 평가해본다. 또한 이 영역에서의 적절한 정책이 갖추어야 할 요건들과 고려해야 할 사항들에 대해 살펴본다. 국가안보 등의 공공의 이익을 이유로 헌법상 기본권인 프라이버시권이나 자기부죄거부권리 등을 제한하기 위해서는 과잉규제금지의 원칙을 만족시켜야 하는데[6], 과잉규제금지 원칙의 기준은 목적 정당성, 방법의 적정성, 피해의 최소성, 법익의 균형성으로 구성된다. 이 네 가지 기준 중 어느 하나의 기준이라도 만족시키지 못하는 법률은 헌법적 기본권을 침해하는 위헌적인 법률이나 정책으로 취급된다. 이러한 원칙들은 〔표 3〕과 같다[6].

본 논문은 개인의 암호이용에 관한 기존의 두 가지

4) 프라이버시에 대한 합리적 기대(reasonable expectation of privacy)는 사생활 침해와 관련한 불법행위 책임을 인정하기 위한 결정적인 요건으로 불법행위책임이 인정되기 위해서는 어떤 특정 상황에서 개인이 자신의 사생활을 침해받지 않을 것이라고 기대하고 있어야 하며, 그 기대가 합리적일 것을 요구한다. 예를 들어 공공장소인 대로변에서 자신이 감시당하지 않을 것이라고 기대하는 것은 합리적이지 않으므로 불법행위 책임을 인정할 수 없다.

5) 형사상 자기에게 불리한 진술을 강요당하지 아니하는 개인에게 부여된 권리를 말하며, 진술거부권이라고도 부른다. 암호와 관련하여서는 피의자 본인이 패스워드나 복호화키를 제공하지 않을 수 있는 권리를 말한다.

6) 과잉규제금지 원칙은 비례성 원칙이라고도 하며, 국민의 기본권 제한에 대해 국가권력이 한계를 설정하기 위해 헌법에서 유래되어 공법 영역에 적용되는 일반원칙을 말하며, 국내 헌법재판소의 위헌법률심사 기준의 하나로 사용되고 있다.

〈표 3〉 과잉규제금지원칙 기준

주요 원칙	의 미
목적의 정당성	국민의 기본권을 제한하려는 입법의 목적이 헌법 및 법률의 체제상 그 정당성이 인정되어야 한다[7].
방법의 적절성 (적합성원칙)	입법목적의 달성을 위하여 그 방법이 효과적이고 적절하여야 한다.
피해의 최소성 (필요성원칙)	입법권자가 선택한 기본권 제한의 조치가 입법목적달성을 위하여 설사 적절하다 할지라도 보다 완화된 형태나 방법을 모색함으로써 기본권의 제한은 필요한 최소한도에 그치도록 하여야 한다. 즉, 목적 달성에 적합한 수단이 여럿일 경우 그 중 가장 기본권 침해가 적은 수단을 사용해야 한다.
법익의 균형성 (비례성원칙)	목적 달성에 적합하고 최소 침해를 가져오는 수단일지라도 그 목적에 관계된 이익과 수단에 의해 침해되는 이익이 균형적인 것이어야 한다. 즉, 그 입법에 의하여 보호하려는 공익과 침해되는 사익을 비교형량 할 때 보호되는 공익이 더 커야한다.

주요 통제정책이라고 할 수 있는 키복구 정책과 복호화명령제도를 위의 기준에 따라 과잉규제여부를 평가해보고 마지막으로 균형 잡힌 암호통제정책이 갖춰야 할 요소에 대해 살펴보도록 한다.

1.3 기존 논의의 한계와 본 연구의 의미

지금까지 국내에서는 강제적 키복구 제도와 키위탁 기술에 대한 학술적인 논의는 있었지만, RIPA법과 같은 복호화 명령제도에 대해서는 학술적 논의가 제대로 진행된 적이 없었다. 박민성의 논문[4]은 과잉규제금지원칙을 강제적 키복구 정책에 적용하고 있을 뿐 키복구 명령제도에는 적용하고 있지 않고 있으며, 단지 서광현의 논문에서 필요성에 대해서만 지적하고 있을 뿐이다. 본 논문에서는 이러한 복호화 명령제도에 대해서도 박민성의 논문에서 사용했던 과잉규제금지원칙을 적용하여 비판적으로 검토했으며, 복호화 명령제도를 국내에 도입하기 위한 논의가 다시 본격화 될 경우 어떠한 부분을 고려해야 하는지에 대해서도 살펴보았다. 또한 강제적 키복구 제도와 복호화 명령제도 모두에 대한 비판적 검토를 통해 국내환경에 맞는 개인의 암호이용 통제정책 수립 시에 고려해야 할 점을 제시하였다.

II. 피의자로서의 개인영역의 암호이용 통제정책의 특성 및 요구사항

본 장에서는 앞서 〔표 2〕에서 살펴보았던 영역들 중 기존 법 및 기본권과의 충돌 가능성이 가장 많은 민감한 영역인 피의자로서의 개인영역의 암호이용 통제정책 수립 시 고려해야 할 원칙들과 개인들이 갖는 기본권들에 대해 살펴본다. 이러한 원칙들을 기반으로 III장과 IV장에서는 피의자로서의 개인영역의 암호이용 통제정책으로 해외에서 제시되었던 대표적인 정책들인 키복구 정책과 복호화 명령제도에 대해 앞서 살펴본 고려사항과 기본권들과의 관계를 중심으로 각각 살펴본 후 과잉규제금지원칙에 기반하여 피의자로서의 개인영역에 적절한 암호이용 통제정책을 제시한다.

개인의 암호이용을 규제하는 암호이용 통제정책은 아래와 같은 국민의 헌법적 기본권들과 충돌할 수 있다. 따라서 개인의 자유와 권리에 심각한 침해를 줄 수 있는 암호이용 통제정책은 다음과 같은 개인의 권리들을 고려하여 만들어져야 한다.

2.1 암호 이용의 헌법적 보장

헌법에서 보장하고 있는 통신의 자유는 통신비밀이 침해되지 않도록 보장된 자유이자 네트워크화된 정보사회의 형성과 발전에 있어서 기본적이고 핵심적인 권리로 인정받고 있다. 이 통신의 자유에는 소극적인 차원의 통신비밀 침해에 대한 처벌 및 보상을 기대할 수 있는 권리에서부터 자신의 통신비밀과 프라이버시를 보호하기 위해 간단한 패스워드 사용에서부터 길이가 긴 암호화키를 사용하는 암호기술 등을 이용하여 적극적인 조치를 취할 수 있는 권리까지도 포함한다. 따라서 네트워크 통신에서 암호를 사용하여 자신의 프라이버시와 통신내용을 보호할 권리는 헌법적으로 보장받고 있다고 할 수 있다[5].

2.2 암호와 프라이버시권

프라이버시에 대한 이론적·실정법적 근거는 일반적으로 헌법상의 사생활의 자유 및 자기정보통제권에서 찾을 수 있다. 헌법 제17조는 '모든 국민은 사생활

7) 일반적으로 정당한 입법 목적으로 인정되는 것으로는 국가안전보장, 질서유지, 공공복리 등을 들 수 있다.

의 비밀과 자유를 침해받지 아니한다.'라고 사생활의 자유권을 명시하고 있으며, 보안사의 민간인 사찰에 대한 국가배상소송에서 대법원은 '모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 가진다.'라고 명시한 헌법 제10조의 조항과 위의 헌법 제17조 조항을 들면서, "이들 헌법 규정은 개인의 사생활 활동이 타인으로부터 침해되거나 사생활이 함부로 공개되지 아니할 소극적인 권리는 물론, 오늘날 고도로 정보화된 현대사회에서 자신에 대한 정보를 자율적으로 규제할 수 있는 적극적인 권리까지도 보장하려는 데에 그 취지가 있는 것으로 해석된다."고 판시함으로써, 정보주체의 자기정보통제권[8]을 헌법상의 기본권으로 인정하고 있다. 이처럼 개인의 사생활의 자유와 자기정보통제권으로서의 프라이버시는 일반적으로 헌법적인 권리로서 보장된다. 암호는 통신내용 및 개인정보를 숨길 수 있는 사생활 자유 및 정보적 자기결정권의 실현도구이기도 하면서, 암호화과정에서 사용된 키는 정보적 자기결정권의 대상이 되기도 한다는 점에서 직접적으로 프라이버시권과 연결된다.

2.2.1 정보적 자기결정권 실현도구로서의 암호

정보적 자기결정권 실현도구로서의 암호와 관련하여서는 다음과 같은 쟁점사항이 존재한다.

2.2.1.1 암호문에는 프라이버시에 대한 합리적 기대가 존재하는가?

평문은 흔히 엽서에 비유되며, 암호문은 편지지를 편지봉투에 넣은 것에 비유된다. 실제 미국의 ex parte Jackson 판례에서는 편지봉투에 비밀 편지를 넣고 봉인하는 행위는 프라이버시를 보호하기 위한 적절한 조치를 취한 것으로 보았으며, 편지봉투를 허락 없이 개봉한 행위를 불법도청에 준하는 것으로 보아 프라이버시 침해로 판결했다. 또한 암호문이나 패스워드 걸린 파일은 금고에 비밀문서를 넣고 자물쇠로 잠그는 것으로도 비유가 되곤 하는데, 이 또한 United States v. Block 판례에서 금고에 넣고 자물쇠에 넣어 보관한 것은 프라이버시에 대한 합리적 기대(reasonable expectation of privacy)가 존재한다고 판결이 내려진바 있다. 봉인된 편지봉투와 자물쇠로 잠겨진 금고에 넣는 행위가 암호화에 대한 은유로 사용되어 일반적으로 암호문에는 프라이버시에 대한 합리적 기대가 존재한 것으로 파악되어 암호는 프라이버시권에 의해 보호됨이 인정되어왔으며, 미국 수정헌법 4조에 의해 정부의 규제로부터 보호받아왔다. 반면 암호문은 봉인된 편지나 잠긴 금고와 열쇠의 은유보다는 갈기갈기 찢어진 종이나 번역된 외국어와 유사하다며 U.S. v. Scott, United States v. Longoria 등의 판례를 들어 암호문에는 프라이버시에 대한 합리적 기대가 존재하지 않는다는 의견도 존재한다[7].

2.2.1.2 암호문의 복호화에 새로운 영장이 필요한가?

두 번째 논점은 바로 압수한 암호문을 법집행기관에서 복호화하거나 당사자에게 암호문의 복호화를 요구하는데 별도의 새로운 영장이 필요한가와 관련된 것이다. 이와 관련해서 앞서 암호문 자체에 프라이버시에 대한 합리적 기대가 존재하지 않는다는 입장에서는 복호화에 별도의 영장은 불필요하다고 주장하고 있다. 즉, 복호화는 압수된 문서에 대해 필수적으로 수반되는, 압수, 수색영장의 집행과 압수물에 대한 '필요한 처분'에 해당한다고 보아, 일단 적법하게 압수된 문서에 대해서는 별도의 영장이 불필요하다는 의견이다. 이와 달리 암호문에 프라이버시에 대한 합리적 기대가 존재한다는 입장을 가진 한 보고서에서는 현행 형사소송법상에서 데이터에 대한 압수수색이 인정되지 않으므로(컴퓨터장치에 대한 압수수색만 가능), "필요한 처분" 또한 데이터에 대해서 인정되지 않으므로, "필요한 처분"이라는 이유만으로 복구정보 제출을 요구할 수 없으며 암호문의 복호화 요청을 위해서는 별도의 새로운 영장이 필요하다고 주장하고 있다[3].

이러한 암호와 프라이버시와의 관계와 관련된 쟁점들에 대해 간단히 살펴보면, 우선 첫 번째 쟁점과 관련하여서는 암호문에 대한 봉인된 편지와 열쇠-자물쇠 은유가 비록 100% 적당한 것은 아니라고 할지라도, 암호문에서의 프라이버시에 대한 합리적 기대가 부정되는 것은 아닌 것으로 보인다. 비록 암호화가 잠그고 특정 공간에 집어넣는 것이 아니라 이진 데이터가 불규칙적으로 뒤섞인(scrambling) 것일 뿐이라는 점에서 차이가 있을지는 모르지만, 암호기술이 예전에

8) 정보적 자기결정권 혹은 개인정보 자기결정권은 자신과 관련된 모든 정보들에 대해 정보처리의 전 과정(수집, 저장, 사용)에서 스스로가 주체적으로 지배 관리할 수 있는 권리를 주는 것으로 흔히 혼자 있을 권리(right to be let alone)로서의 소극적 의미의 프라이버시권와 비교하여 적극적 의미의 프라이버시권으로 알려져 있다.

편지봉투에 편지를 넣었던 것처럼 현대사회에서 프라이버시를 보호받기 위한 적절한 조치로 공공연하게 인정받기 충분하며 프라이버시보호의 수단으로서 그 중요성이 크다는 점, 열쇠-자물쇠처럼 특정한 도구-비밀정보(열쇠, 패스워드, 키 등)가 없이는 비밀정보에 쉽게 접근하기 어려워 프라이버시가 침해되기 어렵다는 점에서 찢겨진 종이나 외국어처럼 숨겨진 특정 도구의 도움 없이 공개된 정보나 손쉬운 노력에 의해 복구가 가능한 또 다른 은유와는 구분되므로, 암호문에 대한 프라이버시 기대는 존재한다고 할 수 있다. 즉, 일반적으로 암호 사용이 프라이버시 및 표현의 자유와 직결되며, 특히 인터넷과 같은 신뢰할 수 없는 개방 네트워크에서 "비밀이 보장된다는 확신을 가지고 이야기할 수 있는" 핵심적인 기술로 인정받고 있으며, 각국 프라이버시법제와 가이드라인에서도 기본적이면서도 핵심적인 조치로 암호화를 들고 있는 상황이므로, 사람들이 인터넷을 사용하는데 있어 암호화 조치를 하는 것은 일반적으로 프라이버시에 대한 합리적 기대가 존재한다고 인정되고 있다.

또한 두 번째 논점에 대해서는 원칙적으로는 암호의 프라이버시에 대한 합리적 기대가 존재하므로 암호문의 압수는 적법한 과정에 따라 이루어져야 하며, 일단 압수된 암호문에 대한 복구정보제출에 대해서도 별도의 영장이 필요한 것으로 보인다. 이처럼 암호문 그 자체는 겉으로 보기에는 내용을 알 수 없는 난수열에 불과할지 모르나 평문의 등가물로 헌법 17조의 "모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다."는 프라이버시 법익의 보호대상이 된다고 할 수 있으며, 암호화 행위에는 프라이버시에 대한 합리적 기대가 있다고 할 것이므로 필요에 따라 추가적인 영장에 의해 적법 절차에 따라 처리되어야 할 것으로 보인다.

2.2.2 정보적 자기결정권 대상으로서의 암호

암호화키 자체 또한 정보적 자기결정권의 대상이 될 수 있다는 의견이 존재한다[4]. 즉, 자신의 복구정보(패스워드, 복호화키)를 자기 스스로 지배 관리할 권리가 있다는 것이다. 정보적 자기결정권의 소극적 방어권은 자신의 정보를 국가나 타인으로부터 수집하는 것을 방어할 수 있게 해주며, 이러한 정보적 자기결정권을 제한하기 위해서는 헌법 37조 2항에 따라 국가안전보장, 질서유지 또는 공공복리를 위하여 필요한 경우에 한하여 법률에 의거하여 적법한 절차에 따라 제한할 수 있으며, 이 경우에도 기본권의 본질적 내용은 침해할 수 없다고 할 수 있다. 패스워드와 복호화키 등은 일단 공개되면 자신이 암호화했던 사적인 내용이 공개될 수 있는 가능성이 존재하므로 비밀로 유지되어야 하는 개인정보로서 적극적 의미의 프라이버시인 정보적 자기결정권의 대상이므로, 패스워드의 수집, 저장, 사용 등을 스스로 통제할 수 있어야 하며, 자신이 허락하거나 국가안전보장 등의 공익과 관련되지 않는 한 수집되거나 무단 사용되지 않을 권리가 있다. 이 때문에 키복구 기관이나 ISP 등 사용자의 패스워드나 키를 보관하고 있는 기관은 이러한 목적으로 적법한 절차에 의한 요청에 의해 불가피하게 수사기관에 키나 패스워드를 제공하거나 키를 이용한 복호화를 수행한 경우, 또는 실수나 공격에 의해 노출된 경우 이에 대해 키와 패스워드 소유자에게 고지해야 한다.

이처럼 암호와 프라이버시의 관계를 살펴보자면, 암호화는 프라이버시 보호를 위한 적절한 조치에 해당하므로 암호화의 결과인 암호문은 프라이버시에 대한 합리적 기대가 존재하므로 프라이버시 보호법익에 따라 보호되어야 할 대상이 되며, 암호문의 복호화에 사용되는 비밀정보인 복호화키와 패스워드 등은 보호되어야 할 개인정보로 사용자는 정보적 자기결정권을 가지게 된다. 즉, 암호화는 정보적 자기결정권의 실현도구이기도 하면서, 암호화과정에서 사용된 키는 정보적 자기결정권의 대상이 되기도 하는 것이다. 따라서 법집행기관은 법집행을 위해 암호문을 복호화하거나 복호화키를 입수하기 위해서는 프라이버시권을 침해하지 않기 위해 이러한 과정이 적법한 절차에 따라 이루어지도록 특별한 주의를 기울여야 할 것으로 보인다.

2.3 암호와 자기부죄거부권리 (Privilege against Self-incrimination)

자기부죄거부권리란 헌법 12조 2항에서 "모든 국민은 형사상 자기에게 불리한 진술을 강요당하지 아니한다."라고 헌법상 보장된 권리를 말한다. 즉, 형사사건에 있어 수사기관에게 자신에게 불리한 증언을 하지 않을 권리가 있다는 것으로 특히 암호와 관련하여서는 암호화된 문서에 대한 복호화 명령과 자기부죄거부권리가 할 가능성이 존재한다. 이러한 자기부죄거부권리는 논문의 주요대상인 피의자 본인에게만 존재하며, 법인이나 제3자 개인에게는 적용되지 않는다. 암호와 자기부죄거부권리와의 관계에 대한 판례들을 보여주는 영국과 미국의 판례들을 살펴보면 다음과 같다.

2.3.1 판례1 : R v S and A (2008)

영국의 RIPA Part III와 관련하여 테러리즘 용의자가 테러공모 관련 증거에 대한 암호키 제출 실패로 처벌 받은 최초의 판례라고 할 수 있다. 본 사건에서 영국 항소법정은 RIPA에 근거한 암호키 제출 명령이 영국법의 자기부죄거부권리와 유럽인권조약 6조 공정재판을 받을 권리를 침해하는 것이 아니라는 판결을 내렸다[8]. 본 사건에서 법집행기관은 테러용의자 두 명의 노트북에서 열리지 않는 몇몇 의심스러운 파일들을 발견하고 RIPA법 53조에 따라 이들에게 암호키 제출을 명령했지만 피고들은 이러한 명령을 거부했다. 법원은 암호화코드 제출 명령이 자기부죄거부권리를 유발하지 않는다며 상세하게 설명하지 않았으며, 암호화키는 잠긴 서랍과 열쇠의 관계처럼 주체의 의지와는 독립적으로 존재하며, 비록 피고가 키를 처음 생성했지만, 일단 생성되고 나면 그것을 변경하기 전까지는 그의 기억에만 존재할 뿐 항소인의 의지와는 독립적으로 데이터로 존재할 뿐이라고 판시했다. 또한 피고가 암호화키를 알고 있다는 사실 그 자체가 피고를 유죄로 만드는 것이 아니며, 판사는 그러한 증거를 배제함으로써 국가안보와 비교 형량하여 자기부죄거부권리에 대한 침해를 최소화할 수 있도록 할 수 있을 것이라고 판시했다.

2.3.2 판례2 : In re Boucher[9] (2007)

미국 버몬트 주의 In re Boucher 재판에서 판사는 앞서 영국 법원의 판결과는 달리 피고가 유아포르노를 감추기 위해 사용했던 암호화키를 제출하거나 입력하여 평문화하여 검찰에 제출하는 행위는 수정헌법 5조의 자기부죄거부권리를 침해하는 것이라는 판결을 내렸다. 앞서 영국 법원의 경우 암호화키를 서랍속의 열쇠로 비유한데 반해, 미국 법원은 Doe v. United States 판례를 인용하면서 피고가 자신이 알고 있는 것을 드러내는 경우 증언이 아닌 문서나 사물을 제출하는 행위도 증언이 될 수 있다고 판시하고 있다.

2.3.3 판례3 : Doe v. US[10] (1988)

앞서 In re Boucher 판례에서 인용했던 암호와 자기부죄거부권리와 관련된 대표적인 판례로, 본 사건에서는 압수수색영장을 가지고 용의자의 컴퓨터로부터 합법적으로 확보한 암호화 증거에 대해 수사관은 용의자에게 영장을 제시하면서 암호화된 증거자료를 해독할 수 있는 암호키를 제출할 것을 요구하였다. 법원은 미국 수정헌법 5조 자기부죄거부권리에 의거하여 "강요된 자백은 증거능력이 없다"고 판단하여 증거로 채택하지 않았으며, 용의자는 암호키를 알려줄 의무가 없다고 판결을 내렸다. 또한 영국 법원과 마찬가지로 열쇠와 잠긴 서랍 은유를 이용하여 설명하고 있지만, 영국법원과는 반대로 열쇠 제출을 요청하는 것과 달리 패스워드를 말하라고 하는 것은 피고로 하여금 마음속에 있는 내용을 드러내도록 하는 것이므로 증언에 해당한다고 판시했다.

지금까지 암호이용 통제정책과 충돌할 가능성이 존재하는 개인들의 권리들에 대해 살펴보았다. 미국은 전통적으로 복호화명령에 대해 복호화 및 암호키 제출을 증언으로 인정하여 자기부죄거부권리를 적용하고 있는데 반해[11], 영국은 RIPA법에 근거한 복호화명령에 대해 증언으로 인정하지 않아 자기부죄거부권리를 적용하지 않고 있다는 차이가 존재한다. 암호이용 통제정책은 이러한 기본적 헌법적 권리들과 충돌하지 않고 최대한 균형을 이루면서 적법절차에 따라 수사권을 보장받을 수 있는 방법을 모색해야 한다. 다음 III장과 IV장에서는 앞서 설명한 과잉규제금지원칙들을 키복구 정책과 복호화명령제도에 적용하여 이러한 주요 암호이용 통제정책이 이러한 개인의 권리들과의 균형을 유지하고 있는지 여부에 대해 평가해보도록 한다.

III. 키복구(Key Recovery) 정책 분석

3.1 강제적 키복구 정책 개요

강제적 키복구 정책이란 민간 암호가 대중화, 고도화되면서 범죄에 암호가 이용됨에 따라 범죄증거에 접근하여 평문정보를 획득하기 어려워지자 법집행당국의 정보에의 신속한 접근을 보장하기 위해 나온 기술적 조치라고 할 수 있다. 키복구 기술이란 이처럼 정부의 접근뿐 아니라 사용자 본인이 키 분실, 도난 등에 의해 대비하여 자신의 키에 대한 접근을 보장하기 위한 목적도 있으며, 필요한 경우 암호문의 소유자나

9) In re Boucher, No. 2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007)

10) Doe v. United States, 487 U.S. 201, 209-212 (1988)

11) 이러한 이유 때문에 미국의 경우 강제적 키복구 정책 포기 이후 복호화명령 도입을 적극적으로 고려하고 있지 못하고 있는 상황이다.

적절한 권한을 가진 자가 사전에 약속된 특정한 조건 하에서 키를 복구하여 제공할 수 있는 암호시스템을 통틀어서 말한다. 이러한 키복구 기술은 사용자의 비밀키를 신뢰받는 키위탁 기관에 위탁해놓고 유사시에 키를 복구할 수 있도록 하는 키위탁(key escrow) 방식과 각각의 메시지 전송 및 파일 저장시마다 키복구 필드를 생성해서 메시지에 부가함으로써 유사시에 암호문의 복구영역의 정보를 추출해서 복구기관에 보내면 복구기관이 암호문을 복구해주는 키캡슐화(key encapsulation) 방식으로 구분된다. 특히 '강제적' 키복구 정책은 암호화를 이용하는 모든 사람들에게 의무적으로 키복구센터를 이용하도록 하여 국가안보, 치안 등의 목적일 경우 정부에 의한 합법적인 접근을 기술과 제도로서 강제하는 것을 말한다. 이에 반해 '자발적' 키복구 정책이란 암호시스템 사용자 스스로의 선택에 따라 키복구 기술을 이용할 수 있도록 하는 것을 말한다. 미국은 1993년부터 정부가 평문에 접근할 수 있는 통로인 백도어를 설치한 클리퍼칩을 모든 암호화 장비에 설치하도록 강제함으로써 정부의 합법적인 법집행 권한을 보장하는 클리퍼(Clipper) 정책을 발표하고 유럽 등 전세계에 도입할 것을 부추겨왔는데, 이 클리퍼 정책이 강제적 키복구 제도의 대표적인 예이다.

3.2 강제적 키복구 제도의 문제점

강제적 키복구 제도는 프라이버시 침해의 위험성을 포함한 여러 측면에서 문제가 제기되어왔으며, 이러한 문제점들 때문에 강제적 키복구 제도는 효과는 없으면서 비용은 높고 프라이버시권에 대한 심각한 피해가 예상된다는 이유로 최근에는 미국을 비롯한 대부분의 국가들이 채택을 포기하게 되었다. 강제 키복구 제도의 문제점을 살펴보면 다음과 같다.

3.2.1 강제적 키복구 시스템의 보안취약성

강제적 키복구 정책은 프라이버시 보호라는 암호의 목적을 무력화시킬 수 있으며, 그 의도와는 반대로 프라이버시에 대한 강력한 침해요소가 될 수 있다. 먼저 키복구 시스템의 위험성 때문에 오히려 프라이버시 침해의 가능성이 높아지는 경우이다. 키복구 시스템은 다음과 같은 위험성을 가지고 있다. 첫째, 강제적 키복구 제도의 도입은 기술의 복잡도를 증가시켜 오류와 보안구멍을 늘려 보안취약성을 증가시키게 된다. 둘째, 키복구 기관에 비밀정보들이 집중되면서 공격이 키복구 기관으로 집중되며, 일단 공격이 성공하면 많은 비밀정보들이 한꺼번에 유출될 수 있다. 셋째, 키복구 기관의 내부자에 의한 오남용이 발생할 수 있다. 넷째, 권한 없는 자가 키복구 시스템에 설치된 백도어를 이용하여 훔쳐보기를 할 수 있다. 이러한 키복구 시스템의 보안취약성에 비례하여 프라이버시 침해의 가능성은 증가하게 된다. 특히 외국의 해커들이 키복구 시스템의 보안취약성을 이용하였을 경우 국민 개개인의 프라이버시 침해와 보안약화로 인해 전체적인 국가전산망 보안에도 심각한 보안위험이 야기될 수 있으며, 국가안보에도 위험을 가져올 수 있는 등 키복구 시스템의 목적인 프라이버시 보호와 법집행권 확보를 통한 국가안보의 보장에 모두 위험을 가져올 수 있다.

3.2.2 감청을 통한 프라이버시 침해의 위험성

강제적 키복구 시스템은 암호의 사용목적을 가리지 않고 모든 데이터에 대한 복구정보를 요구하므로 내밀한 개인의 프라이버시 영역까지 노출될 수 있기 때문에 영장에 명시된 목적 이상으로 프라이버시가 침해될 위험성이 존재한다. 또한 키복구 시스템을 이용하여 영장 없는 불법감청이 이루어질 위험성이 상존한다. 키위탁방식의 키복구 시스템의 경우 영장을 통해 일단 획득된 비밀키를 법집행기관이 영장의 효력이 다한 이후에도 보관하고 있다가 지속적으로 감청을 하게 될 위험성도 존재한다는 것이다. 암호화를 하는 것이 오히려 프라이버시를 침해할 위험에 노출될 수 있다고 암호이용자들이 느끼게 된다면 국민들의 암호이용에 대한 냉각효과가 생기게 될 수 있다. 이런 경우 국민들이 암호기술을 사용하는데 꺼려함에 따라 법집행당국의 의도와는 다르게 반대로 암호사용이 위축되어 사이버범죄에 노출되게 될 위험성이 존재한다. 키위탁 시스템의 경우 암호를 사용하는 모든 국민들의 비밀키를 무조건 위탁하도록 하게 하는 것은 일종의 예비범죄인으로 보고 있다는 점에서 인권침해의 소지가 높고, 통신비밀이 침해되지 않을 국민의 기본권리인 통신자유를 침해할 여지도 높다. 마지막으로 자신의 개인정보인 비밀키 정보를 소유자가 규제할 권리와 자유를 심각히 제한하며 비밀키 획득 시 원소유자에게 통지하는 규정도 없다는 점에서 적극적인 프라이버시권인 정보적 자기결정권을 침해하고 있다고 할 수 있다.

3.2.3 강제적 키복구 시스템의 회피 가능성

강제적 키복구 시스템이 도입된다고 하더라도 범죄자들이나 테러리스트들은 오히려 키복구 기능이 없는 암호를 사용하려 할 것이며, 스테가노그래피를 이용하여 암호화 사실 자체를 알리지 않으면서 비밀통신을 하려 할 것이므로 실제 키복구 시스템을 이용하는 사람들은 대부분 암호를 이용한 범죄하고는 상관없는 선량한 사람들이 될 가능성이 높다. 범죄자들은 키위탁 시스템에 위탁한 키로는 복호화할 수 없는 다른 키로 암호화하여 전송하는 방식으로 키복구 시스템을 무력화시킬 수도 있다. 또한 전세계적으로 강제적 키복구 시스템을 채택하지 않는 한, 다른 나라로부터 강력한 암호시스템을 수입해오는 등 다른 나라의 암호서비스를 이용하여 자국의 키복구 시스템을 우회할 가능성이 상존한다.

3.2.4 강제적 키복구 시스템의 과다한 비용

암호 자체는 한계비용이 매우 값싼 기술인데 반해, 키복구 시스템은 그 복잡성으로 인해 소프트웨어/하드웨어 제품 설계비용과 제반 통신설비 및 상호인증 장비 구축비용, 키복구 기관 운영비용, 제품을 평가하고 기관들을 허가, 감독하기 위한 관리비용 등 상당한 비용이 소모될 것으로 예상된다. 미국의 경우 사용자들이 복구시스템을 사용하면서 복구기관에 지불해야 하는 사용료로 연간 평균 60억 달러가 될 것으로 추산하고 있다[4].

〔표 4〕 강제적 키복구 시스템의 과잉규제금지원칙 적용

주요 원칙	분석 내용
목적의 정당성	국가안보와 테러방지라는 목적은 일반적으로 정당하다.
방법의 적절성 (적합성원칙)	범죄자나 테러리스트들이 강제적 키복구 시스템을 회피할 가능성들이 다양하게 존재하므로, 암호를 이용한 범죄를 막기 위한 법집행력 확보라는 목적은 달성되기 힘들다.
피해의 최소성 (필요성원칙)	자발적 키복구 시스템과 복호화명령과 같은 침해가 덜한 수단이 존재한다.
법익의 균형성 (비례성원칙)	실제 얻을 수 있는 법집행력 확보에 대한 실익에 비교해보았을 때 통신의 자유라는 헌법적 권리와 개인의 프라이버시권에 미치는 영향과 침해정도 및 구축 및 운용에 드는 비용이 상대적으로 너무 크다.

지금까지 강제적 키복구 시스템 개요 및 문제점에 대해 살펴보았다. 강제적 키복구 시스템에 과잉규제금지원칙을 적용해보면 아래 〔표 4〕와 같다.

결국 강제적 키복구 시스템은 범죄자나 테러리스트들의 암호를 이용한 범죄를 막기 위한 법집행력 확보라는 원래의 목적은 달성하지 못하면서 선량한 국민들에 대한 광범위한 프라이버시 침해위험만 증대시킬 뿐이며 비용을 낭비하게 되는 결과를 낳게 될 것이다. 또한 집행 가능성도 희미한 규제를 무리하게 두는 것은 순진하게 규제에 순응하는 대다수 사람에게 불이익을 줄 뿐 이러한 규제를 교묘하게 우회할 수 있는 사람에게는 특별한 불이익을 주지 않게 되어 도덕적 해이가 초래될 가능성이 존재한다. 이러한 이유로 미국을 포함하여 강제적 키복구 시스템을 추진하던 많은 나라에서 이 계획을 철회 혹은 유보했으며 자발적 키복구 시스템과 다음 장에서 살펴볼 복호명령이 새로운 대안으로 대두되었다.

3.3 자발적 키복구 정책

자발적 키복구 정책은 강제적 키복구 시스템과 유사한 키복구 시스템을 이용하되 원하는 사람에 한해서 스스로 선택하여 키복구 시스템을 이용하도록 하는 것이다. 일반 개인들이나 기업들도 실수나 분실에 의한 키의 멸실의 위험성이 항상 존재하기 때문에 이러한 불가피한 상황에 대비하여 안전한 키복구 서비스를 이용해야 할 필요성을 갖게 되므로 불법행위 등 특별한 조건에서는 자신의 키 관련 정보가 적법한 절차를 밟은 법집행기관에게 공개될 수 있다는 사실을 인지한 후 키복구 서비스에 따른 장단점을 비교 판단하여 서비스에 참여여부를 결정하게 된다. 또한 법집행기관은 무차별적 프라이버시 침해에 대한 의혹과 부담을 덜면서 일정 정도의 법 집행력을 확보할 수 있게 된다. 자발적 키복구 시스템에의 가입은 사용자 스스로 키의 처분에 대해 선택한 것이므로 기본적으로는 정보적 자기결정권에 대해서도 침해가 일어나지 않는다. 하지만, 키복구 시스템 가입자들에 대한 불법적 감청이 이루어질 가능성과 키복구 시스템이 갖는 보안취약성 등에 따른 위험이 여전히 상존하며, 법집행기관은 이 시스템에 가입되지 않은 범죄와 테러 용의자들에 대해 법집행력을 확보하는 문제가 여전히 남게 된다.

IV. 복호화명령제도(Decryption Order) 분석

4.1 복호화명령제도 개요

복호화 명령은 용의자나 관련조직에 암호화된 정보를 평문과 같이 이해 가능한 형식으로 제공할 수 있도록 명령할 수 있는 권한을 주는 것을 말하는데, 이 강제적 키복구 제도의 프라이버시 및 기본권 침해소지를 줄이면서 법집행력을 확보하기 위한 민간암호정책의 대안으로 최근 많은 국가에서 채택 혹은 검토하고 있다[12]. 전세계의 주요 복호화명령제도 현황과 각 제도의 양벌규정은 아래 〔표 5〕와 같다.

복호화 명령은 크게 암호문에 대한 복호화를 요청할 수 있는 권리(demanding decryption)와 암호문을 복호화할 수 있는 복호화키 제공을 요청할 수 있는 권리(key delivery)로 나눌 수 있으며, 또한 용의자 개인에게 복호화 명령을 내리는 경우와 용의자가 개인이 아닌 기업인 경우, 용의자 이외의 개인, 단체에게 복호화 명령을 내리는 경우로 구분할 수 있다. 대표사례인 영국 RIPA(Regulation of Investigatory Powers Act)는 2000년에 제정된 영국의 수사권한 규제법으로 Part III 부분인 Investigation of Electronic Data Protected by Encryption에서 암호화/패스워드로 보호조치가 되어있는 데이터의 복호 및 접근 보장의 내용을 포함하고 있으며, 구체적으로 암호문을 평문으로 공개하도록 하는 명령할 수 있는 권리와 복호화키 제출을 복호화 명령에 대신할 수 있는 것을 포함하는 복호화 명령권에 대한 내용을 담고 있다. 복호화 명령은 권한이 있는 자가 복호화키를 가지고 있다고 판단되는 사람에게 평문 정보공개의 요구를 담은 통지를 보냄으로써 개시되며, 이 통지를 받은 사람이 복호화를 불이행했을 경우에는 2년 이하의 징역이나 벌금형에 처해지게 된다[9]. 영국의 반테러법은 테러 용의자가 키의 제출을 거부했을 경우 최대 5년 이하의 징역을 부과할 것을 명시하고 있다.

〔표 5〕 전세계 복호화 명령제도 현황

국가	관련법제	양벌규정[16]
영국	Regulation of Investigatory Powers Act (2000)	2년 이하의 징역 (테러리즘 관련 사건 제외)
	Anti-Terrorism Crime & Security Act (2001)	5년 이하의 징역
프랑스	Code of Criminal Procedure Title IV (2001)	3년 이하 징역이나 45,000유로 이하 벌금
호주	Cybercrime Act (2001)	6개월 이하 징역
싱가포르	Computer Misuse Act(1999)	3년 이하 징역이나 10,000달러 이하 벌금
남아공	Regulation of Interception of Communications and Provision of Communication-related Information Act (2002)	10년 이하 징역이나 2백만 Rand 이하 벌금 (자연인), 500만 Rand 이하 벌금 (법인)
인도	Information Technology Act (2000)	7년 이하 징역
말레이시아	Communications and Multimedia Act (1998)	100,000 Ringgit 이하 벌금 혹은 2년 이하 징역

4.2 복호화명령제도의 문제점

복호화명령제도는 강제적 키복구 제도에 비해 프라이버시나 통신자유와 같은 개인의 기본권의 침해요소가 줄어드는 반면 정보적 자기결정권을 보장하면서도 일정 수준의 법집행력을 확보할 수 있다는 장점이 존재한다고 알려져 왔다. 확실히 어느 정도위험성들을 감소시킨다고 할 수 있지만, 강제적 키복구 제도와는 다르게 자기부죄거부권리에 대한 침해라는 복호화 명령권만이 가지는 근본적인 문제를 가지고 있다.

4.2.1 프라이버시 침해 위험

강제적 키복구 정책에 비해 복호화 명령방식은 분명 프라이버시권 침해 요소를 덜고 있음은 분명해 보인다. 일단 강제적 키복구 제도가 전체 암호사용자들을 예비범죄자들로 간주하고 있는 반면, 복호 명령 방

12) 프랑스의 경우에도 1996년도에 강제적인 키위탁정책을 채택하였다가 1999년도에 키위탁정책이 폐지되고 복호화명령정책이 도입되었는데, 2001년도에 개정된 형사절차법에서는 수사 진행 중에 암호화된 파일이 발견되었을 경우에는 적법한 자에게 복호화키를 받거나 복호화할 수 있는 권한을 부여하고 있으며, 수사관이 CTA (기술지원센터: Centre technique d'assistanace)에 암호화된 데이터를 크랙하도록 요청할 수 있도록 하고 있다.

식은 형사 피의자들에 한해서 범죄자들로 추정한다는 것에 있어 인권 및 프라이버시권 침해의 범위를 줄이고 있다. 하지만, 기본적으로 두 경우 모두 유죄판결이 나기까지는 무죄로 추정한다는 무죄추정원칙을 위반한다는 공통점이 존재한다. 일반적으로 복호화 명령권에는 특정 파일을 복호화할 것을 명령할 수 있는 권한과 복호화 키를 제출할 것을 명령할 수 있는 권한이 존재하는데, 특히 후자의 경우에는 심각한 프라이버시 침해가 발생할 소지가 있다. 즉, 마스터키나 비밀키를 법집행기관에 제출하게 되면, 심각한 프라이버시 위험이 발생할 수 있다. 일단 마스터키나 비밀키를 제출받게 되면 명령 영장에 명시되어 있는 목적과 대상 외의 목적으로 추후에도 지속적으로 영장 이외의 목적으로 다른 문서들에 대한 영장 없는 불법 감청 및 복호화에 사용될 수 있다[1]. 일단 비밀키가 공개되고 나면 비밀키 소유자는 강제 키복구 방식과 동일한 정도의 프라이버시 침해 위험이 존재한다. 복호화해서 평문으로 제출하도록 하는 경우에는 복호 명령을 내린 암호문과 제출된 복호화한 평문이 일치함을 확인하기 위해서는 믿을만한 기관에서 복호화하는 경우가 아니라면 용의자 등이 복호화하는 자리에 법집행기관의 인원이 반드시 참석해야 한다는 한계가 존재한다. 이에 비해 복호화키를 제출하는 경우는 복호화키를 받아 법집행기관에서 직접 복호화하면 되므로 법집행당국에서는 복호화키를 제출하는 경우를 선호하게 되는 편이다. 하지만 프라이버시 침해가능성을 최소화하기 위해서는 복호화 명령권을 복호화 암호문의 복호화 명령으로 한정하고, 복호화키 제출 명령의 경우는 본인이 원하는 사람에 한해서 자발적으로 복호화 키를 제출하는 것으로 복호화 명령을 대치하는 경우로 한정되는 것이 바람직하다. 복호화 명령도 키복구 제도의 경우와 마찬가지로 복호화 전까지는 어떤 내용인지 알 수 없기 때문에 개인의 내밀한 부분을 포함한 모든 통신 및 저장된 파일을 가리지 않고 그 대상으로 할 수 있다는 점에서 개인정보 유출 피해나 기업의 영업비밀 등의 민감한 자료의 노출로 인한 피해가 발생할 가능성이 존재한다.

4.2.2 복호화 명령의 우회

강제 키복구 정책이 단순히 지정 키복구 시스템을 이용하지 않음으로써 강제 키복구 제도를 회피할 수 있는 반면, 복호화 명령은 이러한 시스템 제한이 없으므로 회피하거나 우회하기는 어렵다는 특징이 있다. 하지만, 복호화 명령의 경우에도 범죄자들과 테러리스트들이 다양한 우회 및 회피 방법들이 존재하므로 법집행력 확보 가능성에 대한 문제가 제기되고 있다. 여전히 스테가노그래피처럼 암호화되었는지 자체를 숨길 수 있는 암호화방식을 이용하여 통신채널을 이용하여 비밀정보들을 주고받을 수 있으며, 시스템의 경우에도 스테가노그래피 파일시스템의 암호화를 이용하면 컴퓨터 안에 암호화된 파일이 있는지 자체를 숨길 수도 있기 때문에 복호화 명령을 원천적으로 우회할 수 있는 것이다[10]. 또한 키복구 명령을 제도화하지 않은 다른 나라에 복호키를 위탁 혹은 저장함으로서 키 제출 의무를 피할 수 있으며, 이러한 서비스를 제공하는 일종의 암호-피난처(crypto-heaven) 서비스가 생겨날 경우 키복구 명령에 의한 법집행은 더욱 어려워질 것이다. 다국적 기업 등의 경우, 마스터키 제출의 강제될 위험과 핵심기술 등 영업비밀이 누설될 위험이 존재하기 때문에 아예 복호화 명령 정책을 가지는 국가에 진출하거나 투자를 하는데 주저하게 될 수도 있다. 이 밖에도 기술적인 방법으로 복호화 명령을 우회하는 경우도 존재하는데, 이러한 방법으로는 duress code[13], deniable encryption, VAMP-Ware[14], 패스워드를 잊었다고 우기는 방법, 랜덤 데이터로 우기는 방법[15] 등을 들 수 있다[11].

13) duress code는 숨기려고 하는 평문을 암호화해서 나온 암호문에 대한 복호명령에 대해 진짜 키가 아니라 다른 평문으로 복호화할 수 있는 또 다른 키를 사용하여 복호화한 다른 평문을 제출하는 것을 말한다.

14) VAMP-Ware를 이용하면 두 가지 우회 공격 혹은 오용 공격이 가능하다. 먼저 첫 번째 경우를 살펴보면 악의를 가진 M이 선량한 사람 A를 모함하기 위해 그 사람의 시스템에 키나 패스워드를 성공적으로 바꾸고 스스로 소멸되는 악성코드를 심어놓은 후 그 후에 법집행당국에 A를 밀고하는 경우를 생각해볼 수 있다. A는 복호화요청에 대해 자신이 알고 있는 잘못된 패스워드나 키를 제공할 수 있을 뿐 올바로 복호화할 수 없기 때문에 어떠한 증거도 제출할 수 없을 것이고 결국 2년 동안 실형을 살아야 할 위기에 처하게 된다. 그가 주장할 수 있는 것이라고는 'Virus Ate My Password (VAMP)'라는 항변일 뿐이다. 이러한 공격을 수행하는 맬웨어를 VAMP-Ware라고 하며, RIPA의 복호화 요청은 이러한 공격에 취약하다[12]. 이와 관련된 또 하나의 가능한 시나리오는 피의자인 A가 복호화 명령에 대한 거부를 위한 변명거리를 만들기 위해 자신의 시스템에 VAMP-Ware를 스스로 심어놓은 후 패스워드를 다 바꾸게 하는 것이다. 법집행당국의 디지털 포렌식 팀은 A의 시스템에서 VAMP-Ware를 발견하게 되고 A는 이를 근거로 복호화 불가에 대한 항변을 하게 된다. 이러한 방법은 RIPA 복호화 명령의 법집행을 무력화시키게 될 것이다.

4.2.3 복호화가 불가능한 경우

실제로 복호화가 불가능한 경우들이 존재한다. 패스워드를 잃어버렸을 수도 있고, 복호화키를 실수로 지워버리거나 혹은 다른 사람이 강제로 지워버렸을 수도 있다. 이 경우 키복구 서비스를 받지 않았다면 복호화가 영원히 불가능할 수도 있다. 공개키 암호시스템이라면 복호키가 파일 소유자에게 없을 수도 있다. 혹은 누군가 아예 복호화가 불가능한 난수로 채워진 가짜 파일을 피의자의 파일에 심어놓았을 수도 있다. 또는 이메일과 같은 일방향 통신이 이루어진 이후 공개키-비밀키 쌍을 바꾸고 나서 이전의 쌍을 찾지 못했을 경우도 있고, 쌍방향 통신에서 이전 세션에 이루어졌던 세션키를 복호화하지 못하는 'perfect-forward secrecy'에 의해 예전 키를 찾을 수 없는 경우도 존재한다[11]. 이런 경우들은 모두 의도적으로 복호화 명령을 거부할 목적은 아니지만 복호화명령을 준수할 수 없는 경우로, 이 경우에도 이러한 사실을 피의자가 증명하지 못한다면 2년의 실형을 살 수도 있게 된다. 이렇게 복호화가 불가능한 상황에 처한 선의의 피해자에 대해 시시비비를 가리고 구제할 수 있는 합리적인 방안을 찾지 못한다면 사람들은 복호화키를 잃어버려 2년의 징역형에 처해질 것을 두려워하여 암호기술을 이용하는 것을 꺼리게 되는 냉각효과가 발생하게 된다.

4.2.4 자기부죄거부권리와의 충돌

복호화 명령권에 있어서 가장 핵심적인 문제가 되는 부분이 바로 헌법상에서 보호하고 있는 자기부죄거부권리 및 진술거부권 침해여부와 관련된 것이다. 자기부죄거부권리란 자기에게 불리한 진술을 강요당하지 않을 헌법상 보장된 권리를 말하는데, 복호화 명령은 피의자 본인에게 요청된 경우 피의자의 자기부죄거부권리와 충돌하게 된다. 앞서 살펴본 대로 미국의 Doe v. United States 판결에서는 비밀문서가 담긴 박스의 열쇠가 유형의 물리적인 것이 아니라 개인이 고유하게 알고 있는 비밀번호일 경우에는 역시 수정헌법 5조에 의해 행위의 형태이든 언어의 형태이든 간에 그 내용을 알려줄 필요가 없다는 판결이 내려졌다. 호주 Walsh Report도 개인 당사자들에게 키제출이나 복호화를 요청하는 것은 자기부죄거부권리에 의해 성공하기 힘들 것이라고 적고 있다[13]. 복호화 명령과 관련하여 자기부죄거부권리는 입증책임권한의 전환과 연결되는데, 이에 대해서도 간단히 알아보면 다음과 같다.

4.2.4.1 입증책임의 전환(Reversal of burden of proof)

일반적으로 형사사건에서 피의자의 유죄 입증책임은 검사에게 있게 되는데, 이러한 입증책임의 원칙은 바로 위의 무죄추정의 원칙[16]에 의해 도출된 다. 검사는 피의자의 유죄를 증명하기 위해서 검사가 증거 등을 수집하여 죄의 유무를 입증해야 하며, 만약 검사의 증거가 피의자의 유죄를 입증시키기에 불충분하면 피의자는 유죄를 선고받게 된다. 입증책임의 전환은 특수한 상황인 경우 검사가 피의자의 유죄를 입증할 책임을 갖는 일반원칙과 달리 피의자로 하여금 자신의 무죄를 증명하는 입증책임을 갖는 것을 말한다. 현재 입증책임의 전환은 의료사고사건에서 피의자인 의사에게 무죄입증책임을 두게 하는 등 제한적으로만 적용하고 있다. RIPA의 Part III에서 피의자에게 복호화키를 제출하거나 평문으로 제출하게 하는 것 또한 일종의 입증책임을 전환한 것이라고 할 수 있다. 기존의 입증책임에 따르면, 검사측에서 암호증거를 복호화한 후 증거화해서 범행사실을 증명해야 하는데 반해, 복호화 명령제도에서는 피의자가 검찰이 복호화를 요청하는 암호문을 복호화해서 원하는 문서가 기소된 범행과 관련이 없음을 보여야 하는 셈이 되기 때문이다. 앞의 의료사고의 예처럼 입증책임의 전환의 예는 거의 민사소송의 경우이고, 그 취지도 의사와 환자의 관계처럼 피해자가 피의자의 범행을 증명할만한 전문성이 현저히 낮아 일반인이 보기에 입증을 위한 정보의 불균형이 큰 경우에 한정된다. 하지만, 형사사건에서 복호화 능력과 기타 국내 최고수준의 암호기술을 가지고 있는 법집행기관과 피의자가 입증책임을 전환할만한 불균형이 존재하는지에 대한 고려를 통해 암호증거의 입증책임 전환이 논의되어야 한다. 만일 이것이 입증되지 않는다면 암호증거입증책임을 검찰이

15) 마지막 두 가지는 말 그대로 아예 패스워드를 잊었다고 우기거나 암호문이 아니라 랜덤 데이터라고 우기는 것이다. 이 경우는 그러한 사실을 증명할 수 있어야 한다는 단서가 붙지만, 충분히 가능하고 민감한 시나리오라고 할 수 있다.

16) 무죄추정의 원칙이란 피의자는 최종적으로 유죄선고를 받기 전까지는 범법자 취급해서는 안 되며, 법정에서 무죄인 상태로 추정하는 것으로 피의자의 인권을 보호하기 위한 기본적인 수단이다. 우리나라 헌법 제27조 제4항에서도 "형사피고인은 유죄가 확정될 때까지는 무죄로 추정된다."라고 하여 무죄추정의 원칙을 명시하고 있다.

아닌 형사 피의자에게 피고인을 범죄인으로 가정하는 것으로 이해될 수 있어 무죄추정의 원칙에 위반되는 것이며, 이에 따라 피의자의 인권을 심각하게 침해할 수 있는 위험이 존재한다. 이처럼 개인 피의자에게 복호화 명령 및 복호화키 제출 명령을 내리는 것은 입증책임의 전환에 해당하며 이는 결국 헌법에서 보장한 자기부죄거부권리와 무죄추정의 원칙을 위반한 것으로 헌법이 보장하는 피의자 인권을 침해하는 것으로 볼 수 있을 것이다.

4.2.4.2 강요에 의해 취득된 증거

자기부죄거부권리를 가지고 있는 피의자에게 암호문의 복호화 및 복호화키 제출을 강요함으로써 취득한 증거일 경우 불법수집증거배제의 원칙에 따라 키 자체도 증거로 인정이 되지 않으며, 독수의 과실이론(fruits of the poisonous tree)에 의해 그 복호화키에 의해 복호화한 평문 또한 증거로서 인정이 되지 않을 수 있게 된다.

4.3 미국 E-Discovery 제도의 식별가능 증거개시

위에서 설명한 복호화명령제도가 형사소송을 염두에 두고 있는 암호이용 통제정책이라면 미국 이디스커버리(E-Discovery)제도의 식별가능증거개시요구는 민사소송에 적용되는 것으로, 복호화명령제도는 아니지만 이와 동일한 효과를 제공한다. 미국 민사소송절차(FRCP)상의 증거에 대한 제출 요구 제도인 디스커버리에서는 민사소송에서 소송당사자들이 재판 전에 소송과 관련된 증거를 제출하도록 증거개시의무를 요구하고 있으며, 이러한 요구사항을 준수하지 못하고 개시에 실패하였을 경우에는 불리한 판결 및 벌금을 부과하도록 하고 있다. 이 디스커버리 제도에서는 증거개시 시에 식별 가능한 상태로 개시할 것을 요구하고 있다. FRCP Rule 34(B)와 FRCP Rule 45(D)에서는 "요청 데이터의 형식이 명시되지 않았다면, 일반적으로 보관되는 형식이나 이용 가능하다고 합리적으로 인정되는 형식으로 제출해야 한다"라고 명시하고 있다. '이용가능하다고 합리적으로 인정되는 형식'은 문서파일의 경우 암호화된 파일이 아니라 가독성이 제공될 것을 요구하고 있으므로, 위의 조항은 실질적인 증거 복호화를 요구하는 것이라고 보아도 무방할 것이다. 즉, 디지털 증거에 대해서 애초부터 합리적으로 이용 가능한 형식으로 제출할 것을 요구함으로써 암호화된 증거문제를 당사자 본인이 해결하도록 하고 있다[17]. 즉, E-Discovery의 증거개시의무 또한 일종의 변형된 복호화명령이라고 할 수 있을 것이다. 하지만, E-Discovery에서의 복호화 제출 문제는 개인정보 유출 위험 및 기업비밀 등이 노출될 수 있는 위험성이 존재하며, 이러한 비밀정보를 획득하기 위한 남소의 가능성도 존재한다. 또한 민사소송상의 규제방식을 형사사건에 도입을 하려는 시도들은 앞서 설명했던 자기부죄거부권리 등과 충돌할 수 있으므로 법인범죄 등으로 한정하여 적용하는 등 신중한 검토가 요구된다.

4.4 복호화명령정책 도입 논의 시 고려사항

현재 우리 학계에서도 강제적 키복구 정책에 대해서는 회의적인 의견들이 많거나 더 이상 논의되지 않는 상황이며, 복호화 명령 정책에 대한 적용 가능성이 논의되고 있는 중이므로, 복호화 명령 정책을 우리 사회에 적용하는데 있어 몇 가지 고려해야 될 점을 살펴보도록 하겠다. RIPA법과 같은 복호화 명령 정책을 한국 사회에 적용하는데 있어 고려해야 할 점은 다음과 같다.

첫째, RIPA법은 영국이라는 특수한 상황을 반영하고 있다는 것이다. IRA나 아랍국가에 의한 테러 등의 위협의 일상화와 테러 과정에 암호가 사용되었다는 증거의 존재는 자기부죄거부권리와 같은 헌법적 기본권과 자신의 프라이버시권을 일부 유보할 수 있을 정도로 암호에 의한 범죄를 막는 것이 영국 사회의 핵심적인 쟁점이었기 때문이다[18]. 이러한 특수한 상황의 산물을 그대로 우리 상황에 적용한다면 부작용을 일으킬 수도 있다. 국민들의 프라이버시권을 포함한 기본권을 축소하면서까지 법집행기관이 자신의 목적을 달성하기 위해서는 단순히 법집행의 어려움이 존재한다는 이

17) 호주의 The Walsh Report도 암호규제정책의 대안으로 수사 및 재판절차에서 사용되는 모든 문서증거를 가독성 있는 형태로 제출할 것을 요구하는 의무규정을 설정하는 방안을 제시하고 있다.

18) 2000년 제정 이후 Part III 부분이 5년간 발효되지 못했던 이유는 보안전문가 및 인권단체들의 반대와 아직 암호화가 사회에 널리 사용되지 않고 있기 때문에 정치적 부담에 비해 그다지 실효성이 없다는 상황적 조건 때문이었다. 하지만 최근 암호 사용 비율이 증가하였고 IRA가 무장해제한 반면 영국의 이라크전쟁 개입 이후 아랍권에 의한 테러가 증가했으며, 테러에 암호 사용 사실이 공개되면서 테러 및 범죄용의자에 대한 복호화 강제실시를 위한 분위기가 무르익었다고 판단했기 때문이다.

유만으로는 부족하고 그 사회의 핵심적인 쟁점이자 공익적 의미가 존재한다는 것을 증명해야 한다. 국내 상황을 객관적으로 평가하고 영국 등의 경우와 비교해보기 위해서는 암호를 이용한 범죄율이나 암호오용 발생빈도 등과 같은 실증적 자료에 대한 분석이 우선적으로 필요하다.

둘째. RIPA법은 최초 발의부터 지금까지 영국 내에서도 심한 반발을 사고 있으며[19], 특히 복호화명령을 다루고 있는 Part III는 특히 인권침해의 위험 등에 의해 5년간 유예가 되었다는 점, 2007년 Part III 정식 발효된 이후에도 영국 RIPA법에서 명시되고 있는 수사권을 지원하기 위해 복호화 기술과 서비스를 지원하는 기관인 NTAC(National Technical Assistance Center)에 의한 프라이버시 침해 가능성과 실효성, 그리고 제출된 키들과 민감한 정보들에 대한 보안실패로 인한 유출 위험성 등에 대해 지속적으로 의문이 제기되고 있는 상황이다[14]. 영국의 경우에도 법집행당국과 국민들의 생각에는 여전히 간극이 존재하며, 모두가 입증책임전환과 복호화 명령에 찬성하고 있는 것은 아니라고 한다. 또한 영국 RIPA Part III가 아직 실행 초기이므로 서둘러 받아들이기보다는 지속적으로 운영과정을 지켜보면서 실제 실행상의 장단점을 지켜볼 필요가 있다.

〔표 6〕 복호화 명령의 과잉규제금지원칙 적용

주요 원칙	분석 내용
목적의 정당성	국가안보와 테러방지라는 목적은 일반적으로 정당하다.
방법의 적절성 (적합성원칙)	강제적 키복구 시스템보다는 나은 편이긴 하지만 여전히 범죄자나 테러리스트들이 복호화 명령을 근본적으로 우회하거나 명령을 회피할 가능성들이 존재하므로, 복호화 명령만으로는 암호를 이용한 범죄를 막기 위한 합리적 수준의 법집행력 확보라는 목적이 쉽게 달성되기는 어려울 것이다.
피해의 최소성 (필요성원칙)	아직까지 어떠한 조치를 취하지 않는 zero option을 제외하고는 더 기본적 침해가 적은 법적, 기술적 수단은 나온 바 없다.
법익의 균형성 (비례성원칙)	강제적 키복구 시스템에 비해서는 나은 편이지만 실제 얻을 수 있는 법집행력 확보에 대한 실익에 비교해보았을 때 개인의 프라이버시권에 미치는 영향과 자기부죄거부권리와 같은 헌법적 기본권에 대한 침해정도가 상대적으로 여전히 큰 편이라고 할 수 있다.

19) 영국의 암호학자인 Ross Anderson을 위시한 많은 보안전문가들과 인권단체들이 그 실효성과 위헌성에 대해 지속적으로 문제제기 한 바 있다[10].

지금까지 강제적 복호화명령제도 개요 및 문제점에 대해 영국 RIPA법을 중심으로 살펴보았다. 복호화명령제도에 과잉규제금지원칙을 적용해보면 아래 〔표 6〕과 같다.

복호화 명령은 분명 프라이버시 침해의 위험도나 비용을 포함한 여러 면에서 강제 키복구 정책에 비해 진일보한 면을 보여주기는 하나 여전히 프라이버시 침해 위험이 상존하고 있으며 피의자에 대한 복호명령권을 부여하기 위해서는 자기부죄거부권리라는 헌법적 기본권 침해 문제를 해결해야 하는 커다란 장애물이 놓여있고 복호화 명령을 우회할 수 있는 다양한 가능성도 존재하고 있기 때문에 실제로 목적한 바의 수사권을 확보할 수 있을지는 더 논의되어야 할 것으로 보인다.

V. 대안 : 합리적인 암호이용 통제정책 수립

본 장에서는 강제적 키복구 정책과 복호화 명령제도에 대한 검토를 통해 국내에 적용 가능한 합리적인 수준의 피의자 개인의 암호이용 통제 정책을 수립하기 위해 고려해야 할 점들을 제시해보도록 한다. 이를 위해 먼저 강제적 키복구 정책과 복호화 명령제도의 한계를 극복할 수 있는 대안적 암호통제 정책 수립을 위한 원칙들을 제안하고, 다음으로 수사권 보장 차원에서 피의자 개인뿐만 아니라 피의자 법인, 공공기관, 피의자를 제외한 개인을 포괄하는 영역별 민간 암호이용 통제정책의 필요성에 대해 제시한다.

5.1 피의자 개인의 암호이용 통제정책 수립 원칙

앞서 살펴보았던 것처럼 현재 우리 학계에서는 강제적 키복구 정책에 대해서는 회의적인 의견들이 많거나 더 이상 논의되지 않는 상황이며, 복호화 명령 정책에 대한 적용 가능성이 논의되고 있는 중이므로, 복호화 명령 정책을 우리 사회에 적용하는데 있어 고려해야 할 점들을 살펴볼 필요가 있다. 따라서 위 II, III, IV장에서 행한 해외의 피의자 개인의 암호이용 통제정책에 대한 분석을 기반으로 국내 피의자 개인의 암호이용에 대한 통제정책 수립 시 고려해야 할 원칙들을 수립해보면 다음과 같다[20].

5.1.1 OECD 암호정책 가이드라인 준수

암호정책과 관련하여 국제적인 기준인 OECD 암호정책 가이드라인을 만족시켜야 하며, 개인의 암호이용으로 인한 순기능과 역기능을 모두 고려해야 하며, 개인의 헌법적 권리와 법집행력이 균형을 이룰 수 있도록 해야 한다.

5.1.2 개인의 암호이용의 원칙적 자율화

개인의 암호이용은 원칙적으로 자율화해야 하며, 개인정보와 기업의 기밀을 보호하기 위한 암호화 기술은 촉진되어야 한다. 소수 범죄자들의 암호이용을 규제하기 위해 선량한 대다수 국민의 적법한 암호 이용을 억제시키는 냉각효과를 제공해서는 안 된다.

5.1.3 암호화키의 보호 및 정보적 자기결정권 보장

암호화키는 정보적 자기결정권의 대상이 되므로, 각국의 프라이버시 법률에서 제공되는 개인정보에 대한 보호가 제공되어야 한다. 제출된 암호화키는 안전하게 보관되어야 하며, 재사용 불가능하도록 삭제되어야 한다. 만일 수사기관에 의해 유출된 경우 데이터주체의 정보적 자기결정권과 통제권 보호 차원에서 데이터 주체에 통지해야 한다.

5.1.4 암호문의 프라이버시에 대한 합리적 기대 인정

암호문에는 일반적으로 프라이버시에 대한 합리적 기대가 존재하므로, 복호화를 위해서는 새로운 영장이 필요하며 적법절차에 따라 처리되어야 한다.

5.1.5 암호화 이용 범죄의 가중 처벌

앞서 살펴본 것처럼 이중목적 도구로서의 암호가 범죄적 목적으로 이용되는 것에 대해 헌법적 권리나 프라이버시에 대한 심각한 침해 없이 기술적 코드나 법적 코드를 사용함으로써 모든 우회가능성을 완벽하게 차단할 수 있는 방법은 아직까지는 존재하지 않는 상황이다. 또한 범죄적 목적의 암호화가 전체 암호화 이용에서 차지하는 비율도 미미한 정도이다. 따라서 암호화를 범죄행위에 이용한 행위를 원천봉쇄하기 보다는 암호화의 악의적 이용에 대한 행위 책임을 물어 암호 오용행위 결과에 대해 가중 처벌하는 방안이 모색되어야 한다.

5.1.6 공개 여론 수렴 과정의 활용

영국의 경우 RIPA 제정 당시 및 시행령 작성을 위해 각계의 전문가들과 일반인들의 의견을 공개적으로 수렴하는 과정을 거쳤고, 네덜란드의 경우 자국에 적합한 암호정책을 선택하기 위해서 무작위로 선발된 일반인들을 한 자리에 모아놓고 암호이용 통제정책에 대한 의견을 수렴하는 대안적 실험이 이루어졌다[1]. 이와 같은 외국의 예에서처럼 국내에서도 공개적으로 각계 전문가들과 일반인들의 의견을 모아나가는 합의과정을 통해 좀 더 합리적이고 균형 잡힌 암호정책을 만들어나가려는 적극적인 노력을 할 필요가 있을 것이다.

5.1.7 개인정보영향평가 수행

기술적 코드를 이용한 암호화 규제의 경우 개인정보 침해 위험이 높긴 하지만, 이러한 위험을 최소화함으로써 프라이버시권과 수사권의 균형을 유지하기 위한 기술적 코드 구현 노력들이 존재한다[21]. 이러한 기술적 코드를 이용한 암호화 통제의 경우, 자동화 등으로 인한 사회적 영향력을 고려하여 필수적으로 좀 더 엄격한 사전 개인정보영향평가를 수행하여야 한다. 또한 민간암호이용통제법 제정 시에도 해당 법안에 대해 반드시 사전 개인정보영향평가를 수행해야 한다[22]. 만일 개인정보영향평가의 결과 프라이버시 침

20) 호주 암호법 제정을 위한 목적으로 작성된 The Walsh Report는 암호 이용 범죄행위의 가중처벌, 수사 및 재판절차에서 사용되는 모든 문서증거를 가독성 있는 형태로 제출할 것을 요구하는 의무규정 설정, 정황증거 인정범위 확장, 암호해독원천기술 개발능력 강화, 가독성 있는 평문 증거로의 변환제출 의무화 등을 대안으로 제시하고 있다[13].

21) 이러한 노력들로는 키 정보 분산을 통하여 특정 임계치 이상의 정보가 모여야지만 키정보를 복구할 수 있도록 함으로써 적법한 법적 권한 및 절차에 의해서만 키를 복구할 수 있음을 보장하고 프라이버시 침해를 최소화하기 위한 키복구 방식인 Partial Key Escrow(PKE), Robust Thres-hold Key Escrow Scheme (RT-KES) 등이 존재한다.

22) 개인정보영향평가는 단순히 기술적 코드뿐만 아니라 개인의 프라이버시에 심각한 영향을 줄 수 있는 법적 코드의 경우에도 입법영향평가 차원에서 수행될 수 있다. 예를 들어 호주의 경우 개인정보 취급과 관련된 새로운 법령이 출현했을 경우 개인정보영향평가를 수행하도록 하고 있으며, 실제 자금세탁방지법안의 관련 조항들에 대

해위험이 높아서 수사권과 프라이버시권의 균형이 심각하게 훼손된다면 해당 기술적 코드와 법적 코드는 채택되어서는 안 된다.

5.1.8 암호이용에 대한 과잉규제금지원칙기준 수립

암호이용을 규제하기 위한 법제도 수립 시에는 과잉규제금지원칙을 준수하고 있는지 반드시 적용해보아야 한다. 특히, 암호이용 통제정책은 각각 [표 7]에서 제시하고 있는 원칙을 준수하고 있는지 검토되어야 한다.

[표 7] 민간암호이용에 대한 과잉규제금지원칙 기준

주요 원칙	의미
목적의 정당성	-국민의 기본권을 제한하려는 입법의 목적이 국가안전보장, 질서유지, 공공복리 등 헌법 및 법률의 체제상 그 정당성이 인정된 범위로 최소화되어야 한다. -당시에 핵심적인 쟁점이거나 확실한 공익적 가치가 존재해야 한다.
방법의 적절성 (적합성원칙)	-범죄자들에 의한 우회가능성이 최소화되어야 한다. -민간부문의 적법한 암호이용에 냉각효과를 제공해서는 안 된다.
피해의 최소성 (필요성원칙)	-복호화대상파일은 반드시 필요한 파일들로 최소화되어야 한다. -복구정보 및 제출된 키 정보는 관련 없는 곳에 재활용 되어선 안 된다. -관련이 없거나 이용된 복호화문서나 개인정보는 삭제되어야 한다. -법집행기관의 오용을 통한 감청 가능성이 최소화되어야 한다. -보안 취약성으로 인한 추가적인 위험이 발생하지 않아야 한다.
법익의 균형성 (비례성원칙)	-프라이버시권,무죄추정원칙,자기부죄거부권리 등 기본권 및 기본원칙들과 균형을 이루어야 한다. -최초설치비 및 운영비가 과다하지 않아야 한다.

5.1.9 암호분석기술 연구 및 개발 강화

자기부죄거부권리를 가지고 있는 피의자에 대해서는 복호기술력의 배가와 복호화 명령이 아닌 다른 방식의 증거확보를 위한 다양한 방법들[23]을 사용하여 증거를 확보하는 방안에 대해서도 지속적으로 연구할 필요가 있다. 특히 수사기관의 복호화 기술을 배가하여 적법절차에 따라 이용하는 것은 용의자의 프라이버시나 자기부죄거부권리와 충돌하지 않으므로 가장 확실하면서도 안전한 암호의 범죄적 이용에 대한 대책이 될 수 있다. 이미 암호화된 디지털 파일에 대한 복호화 기술은 삭제된 파일의 복구 기술과 함께 디지털 증거 분석 절차에서 사용되는 주요 디지털 포렌식 기술 중의 하나로 자리 잡고 있다[24]. 디지털 수사역량 강화의 차원에서 민간이 사용하는 암호기술의 발전에 대응할 수 있는 암호화된 디지털 파일에 대한 복호화 기술에 대한 연구 개발을 강화할 수 있는 정책이 수립되어야 한다.

5.2 영역별 민간암호이용 통제 정책 연구

앞의 장들에서 살펴보았던 것처럼 피의자로서의 개인의 경우에는 프라이버시에 대한 합리적 기대가 높고 자기부죄거부권리가 존재하므로 강제적 키복구 정책이나 복호화 명령제도는 해당 영역의 암호이용 통제정책으로 적당하지 않다. 따라서 피의자로서의 개인에 대해서는 별도의 적용될 수 있는 정책은 없으며 단지 영장에 의한 암호화 파일 수집 후에 별도의 복호화 영장을 취득한 후 복호화 기술을 통하여 복호화하며 증거를 확보하는 것이 가장 현실적인 대안이라고 할 수 있다[25]. 따라서 이 영역에서의 암호이용 통제정책을 위해서는 수사기관 차원의 복호화 기술에 대한 연구개발과 적법한 복호화 절차의 마련이 필요하다. 하지만, 암호이용 통제대상은 각 대상이 암호이용 통제 정책 수립 시 주요 고려사항인 프라이버시에 대한 합리적 기대와 자기부죄거부권리의 수준에 따라 여러 영역으로 구분될 수 있다. 본 논문에서 주로 살펴보았던 피의자 개인처럼 높은 수준의 프라이버시에 대한 합리적 기대와 자기부죄거부권리를 가진 대상이 있는 반면,

---

해 개인정보영향평가를 수행하기도 했다.

23) 예로 컴퓨터로부터 방출하는 전자기의 모니터링을 통해 입력되는 신호를 확인하는 TEMPEST 공격과 Scarfo 사건에서 사용되었던 KLS(Key Logger System)의 활용 등을 들 수 있다. KLS는 PGP로 암호화된 이메일을 복호화하기 위한 비밀번호를 알아내기 위한 도구였다[15].

24) 디지털 포렌식 기술 중 복호화 기술로는 암호해독기술(cryptanalysis) 및 암호키 및 패스워드를 추측하거나 복구해내는 기술(password recovery)을 들 수 있으며, 이와 관련해서는 Paraben Decryption Collection과 같은 도구가 존재한다.

25) Bert-Jaap Koops는 Rawls Procedure에 따라 수행한 네덜란드 암호규제정책을 결정하는 방법론을 통해 무규제 방임정책을 대안으로 도출하여 제안하고 있다[1].

법인이나 공공기관처럼 프라이버시에 대한 합리적 기대나 자기부죄거부권리가 낮은 대상이 존재한다. 이처럼 다른 수준의 권리를 갖는 대상에게 동일한 암호이용통제정책을 두는 것은 합리적이지 못하다. 따라서 암호이용통제대상 영역을 프라이버시와 자기부죄거부권리 유무를 통해 구분하고 그에 대한 적절한 암호이용 통제정책을 두는 영역별 정책수립이 필요하다.

지금까지의 논의들은 암호이용 통제정책의 대상 영역은 소송당사자 개인에만 한정된 것이 아니라, 공공기관, 법인, 피의자 이외의 개인들 등 피의자로서의 개인과는 다른 성격과 권리수준이 다른 다양한 영역들로 이루어져 있다는 것을 간과해왔다는 것이다. 피의자 본인의 암호이용 통제가 가장 민감하고 중요한 영역이긴 하지만, 법인범죄에서의 안티 포렌식 목적의 암호화 활용 등이 높아지는 상황에서 상대적으로 프라이버시 등 권리침해가 덜 민감한 영역들에서 영역별 적절한 암호이용 통제정책을 수립하는 것은 법인범죄 등에서의 암호 이용 가능성을 최소화하고 권리침해 논란으로 민감할 수 있는 피의자를 제외한 다른 대상들로부터 적법한 방식으로 안전하게 디지털 증거를 확보하는데 도움이 될 수 있을 것이다.

VI. 결 론

지금까지 암호이용의 이중적 의미에 대해서 알아보았고, 이 때문에 발생할 수 있는 안티 포렌식 기술로서의 암호의 역기능에 대해서도 살펴보았다. 이러한 역기능을 최소화하기 위한 방안으로 국가차원의 암호이용 통제정책이 필요하며, 적절한 국가암호이용정책의 수립이 안티 포렌식 대응 관점에서도 그 의미와 필요성이 더욱 중요해지고 있음을 알아보았다. 또한 이러한 암호이용 통제정책 수립에 있어 프라이버시권과 자기부죄거부권리를 포함한 개인의 헌법적 권리와의 균형의 중요성에 대해서도 살펴보았다. 그리고, 암호이용 통제정책의 두 가지 큰 흐름이라고 할 수 있는 강제적 키복구 정책과 복호화 명령 정책들에 대해 과잉규제금지원칙을 적용하여 피의자 개인에 대한 암호이용 통제정책으로 적당한지 각각 평가해봄으로써 과연 이러한 정책들이 개인의 헌법적 권리와 수사권의 균형을 유지해주는 적절한 암호정책이 될 수 있는지도 알아보았다.

정리해보자면 강제적 키복구 정책은 법집행력 확보라는 목표를 달성하기 어려운 반면 피의자의 프라이버시권을 포함한 기본인권에 대한 침해가 너무 과도하므로 지금은 거의 모든 나라에서 채택하지 않고 있는 상황이다. 복호화 명령 정책은 현재 여러 나라에서 채택하거나 채택을 고려하고 있는 중으로 프라이버시 침해나 비용 등 여러 면에서 강제적 키복구 정책보다 낫기는 하지만 여전히 정보화 사회에서의 법집행력 확보라는 목적을 달성할 수 있을지에 대해서는 미지수이며, 피의자의 자기부죄거부권리와의 마찰이라는 큰 장애물이 존재하고 있다는 것을 알게 되었다. 따라서 본 논문에서는 피의자 개인에 대한 암호이용 통제는 무규제 방임정책을 사용하는 것으로 하되 악의적 이용에 대한 행위책임을 엄하게 묻는 쪽으로 제시했다. 마지막으로 해외 암호이용 통제정책의 사례를 바탕으로 피의자 개인 영역의 균형 잡힌 암호이용 통제정책 수립을 위한 암호화이용범죄의 가중처벌, 암호분석기술연구 및 개발강화 등과 같은 대안들에 대해 짚어보았으며, 피의자 개인을 제외한 피의자 이외의 개인, 기업의 암호 이용에 대한 합리적인 규제 정책의 필요성에 대해서도 살펴보았다.

본 논문에서 제시한 피의자 개인의 암호이용 규제정책 개발 요구사항은 암호와 유사하게 개인과 법인이 자신들의 산업기밀이나 개인정보를 보호하기 위한 선한 목적으로 이용하기도 하고 범죄증거를 은멸하기 위한 악한 목적으로 사용되기도 하는 이중적인 역할을 하는 사용도구의 하나인 안티 포렌식 기술에 대한 균형 잡힌 대응정책을 개발하는데도 효과적으로 적용될 수 있을 것으로 기대된다.

참고문헌

[1] Bert-Jaap Koops, The crypto controversy, Kluwer Law International, 1999.

[2] 고승철, 박광진, 정연수, 주덕규, "정보사회에서의 암호이용촉진을 위한 법제도 환경 개선 방안," 한국정보보호진흥원, 1999.

[3] 신일순, 오병철, 박민성, 정찬모, 강준모, "암호활용과 촉진을 위한 법제도 정비방안," 정보통신정책연구원, 1999.

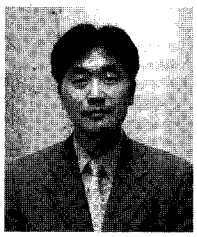
[4] 박민성, "정보적 자기결정권과 암호," 한국정보보호센터 '99 정보보호우수논문집, 1999.

[5] 서광현, "암호기술의 적법한 사용을 위한 정책개발에 관한 연구," 박사학위논문, 고려대학교, 2003.

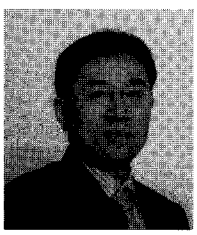
[6] 이승선, "방송불가 판정 광고사전심의의 위헌성에 관한 연구," 광고연구, 제69호, pp. 219-249, 2005.

[7] Orin Kerr, "The fourth amendment in cyberspace : can encryption create a reasonable expectation of privacy," Connecticut Law Review, Vol. 33, pp. 503-533, 2001.
[8] "UK court parts with US court regarding compelled disclosure of encryption keys," Privacy Law Blog, 31 Oct. 2008. http://privacylaw.pro-skauer.com/2008/10/articles/international/uk-court-parts-with-us-court-regarding-compelled-disclosure-of-encryption-keys/
[9] 국가보안기술연구소 정책연구실, "영국 수사 권한 규제법(RIPA) Code of Practice 주요내용," 2006.
[10] Foundation for Information Policy Research, "FIPR response to the home office," 2006.
[11] Bert-Jaap Koops, "Crypto and self-incrimination FAQ," Version 1.1, Aug. 1999, http://rechten.uvt.nl/koops/casi-faq.htm#2
[12] Caspar Brown, "Some open problem with RIPA Pt.3," Aug. 2006.
[13] Gerard Walsh, "Walsh Report: Review of policy relating to encryption technologies," Australian Attorney-General's Department, 1997.
[14] "유럽-인터넷 감시기구 설치 싸고 英정부-업계 설전," 전자신문, 2002년 6월 17일
[15] 김소정, 임종인, 오일석, "사이버범죄의 암호화된 증거 수집에 관한 연구," 정보보호학회지, 13(5), pp. 113-122, 2003년 10월.
[16] Bert-Jaap Koops, "Crypto Law Survey," Version 26.0, Jul. 2010.http://rechten.uvt.nl/koops/cryptolaw/

〈著者紹介〉



백 승 조 (Seung-Jo Baek) 정회원
2007년 8월: 고려대학교 정보경영공학전문대학원 석사
2007년 9월~현재: 고려대학교 정보경영공학전문대학원 박사과정
〈관심분야〉 정보보호정책, 정보법학, 디지털포렌식, 개인정보보호, 사이버전 등



임 종 인 (Jongin Lim) 종신회원
1980년 2월: 고려대학교 수학과 졸업
1982년 2월: 고려대학교 수학과 이학석사
1986년 2월: 고려대학교 수학과 이학박사
1986년 3월~2001년 1월: 고려대학교 자연과학대학 정교수
2001년 2월~현재: 고려대학교 정보경영공학전문대학원((구)정보보호대학원) 원장, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 행정안전부 정책자문위원회 위원, 방송통신위원회 인터넷협의회 운영위원 등
〈관심분야〉 정보법학, 디지털포렌식, 개인정보보호, 전자정부보안, 융합기술보안 등