Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.1, Feb. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.1.99

국가 암호정책에 대한 연구 : 암호접근권한을 중심으로

김 동 훈,[1†] 권 헌 영,[2‡] 홍 석 희[2]
[1,2]고려대학교 (대학원생, 교수)

A Study on the National Cryptographic Policy : About the Right to Access the Cryptographic

Dong-hoon Kim,[1†] Hun-yeong Kwon,[2‡] Seokhie Hong[2]
[1,2]Korea University (Graduate student, Professor)

요 약

최근 정보통신기술의 발전으로 통신망을 통하여 소통하는 정보가 증가하고 있으며, 이를 보호하기 위한 기반기술로 암호가 널리 활용되고 있다. 한편, 초창기 암호기술은 군사적 활용을 목적으로 개발되어 국가가 조정·통제하였으나, 정보통신기술의 향상에 따라 민간으로 상당 부분 이전되어 발전되고 있다. 이로 인해, 세계 각 국에서는 민간영역의 암호이용 자유화에 대한 요구와 국가차원의 암호 활용 권한 우위를 두고 마찰이 발생하여 왔다. 본 논문에서는 각 국의 암호 정책 수립과정에서 나타난 국가와 민간의 갈등을 살펴보고 국내의 암호정책 현실을 알아보았다. 이를 바탕으로 균형 있는 암호정책의 적용과 암호산업 발전을 도모하며, 국가의 암호접근 권한을 확보하기 위하여 국가 암호해독 전문기관 설립 필요성과 암호 부정사용에 대한 법적 제재 방안의 입법 필요성을 제시한다.

ABSTRACT

With the recent development of ICT, information exchange through data communication network is increasing. Cryptography is widely used as the base technology to protect it. The initial cryptography technology was developed for military use and authorized only by the nation in the past. However, nowadays, much of the authority was unwillingly transferred to the private due to the pervasive use of ICT. As a result, there have been conflicts between the private demand to use cryptography and the nation's authority. In this paper, we survey the conflicts between nations and the private in the process of formulating the cryptography policy. Morever, we investigate the reality of the cryptography policy in Korea. Our investigations are expected to help the government apply cryptographic control policy in a balanced manner and plan development of cryptography industries. Lastly, we propose a need to establish a cryptanalysis organization and to legislate a legal sanction against fraudulent use of cryptography.

Keywords: cryptanalysis, cryptography policy, national security, misuse cryptography

I. 서 론

정보화 사회로 접어들면서 인터넷과 이동통신기술이 발전함에 따라 이를 활용한 민간영역의 경제활동이 증가하게 되었다. 이로 인해, 인터넷을 활용한 전자상거래 등이 활성화되면서 중요한 정보들이 인터넷을 통해 소통되게 되었다. 이와 같은 정보들의 신뢰성 및 안전성 보장과 기밀성 보호, 개인정보 보호 등을 위해 다방면에서 전자적 기술 기반의 암호 활용이 증가하고 있다. 또한, 그 형태도 대칭키, 공개키, 해시함수 등 다양한 형태로 발전되어왔다. 초창기에는 군사적 목적으로 유통되는 정보들의 기밀성 보호를

Received(09. 17. 2020), Modified(11. 19. 2020), Accepted(01. 05. 2021)
† 주저자, dhkim85@korea.ac.kr
‡ 교신저자,khy0@korea.ac.kr(Corresponding author)

목적으로 암호가 많이 활용되었다면, 최근에는 민간영역으로 확대되어 인증 및 무결성 보장 등 다양한 서비스를 지원하는 형태로 암호기술이 확대되어 활용되고 있다. 반면, 암호를 악용하여 주요 범죄 증거를 암호화하여 은닉하거나 수사과정에서 단서가 될 수 있는 데이터를 암호화하여 수사를 방해하는 등 국가나 법 집행기관의 공공의 안녕 유지에 심대한 장애를 끼치기도 한다. 특히, 테러나 간첩 활동 등 국가안보에 심대한 위해를 끼치는 범죄들의 경우 암호기술을 적극적으로 활용하여 자신들의 범죄기도를 은폐하거나 은닉하기도 한다. 최근 들어서는 '랜섬웨어' 방법을 활용하여 상대방의 데이터를 임의로 암호화시킨 후 금전을 요구하는 사이버 공격방법도 성행하고 있다. 이처럼 암호는 그 사용에 따라 정보를 보호하는데 큰 기여를 하기도 하고 심대한 지장을 주기도 하는 '동전의 양면'과 같은 성질을 가지고 있다.

이에, 세계 각국에서는 국가주도로 암호를 관리하기 위한 제도적 장치를 마련하여 암호의 불법적 사용을 방지하려는 노력을 기울이고 있다. 한편, 시민단체와 기업체 등 민간에서는 암호산업의 육성과 개인 프라이버시의 보장을 위해 암호에 대한 국가의 개입을 반대하고 있어 갈등이 지속되고 있다.[1]

본 논문에서는 정보보호의 핵심요소인 암호정책이 세계 각국에서 수립되는 과정과 우리나라의 암호정책의 사례를 살펴보았다. 그 과정에서 나타나는 국가의 암호권한과 민간영역의 암호자유화에 대한 갈등을 분석해보고 우리나라의 입장에서 보완점을 제시하였다.

II. 암호의 정책적 관리

2.1 각국의 암호정책

암호는 최초 전쟁에서 가장 핵심적인 정보의 기밀성을 유지하기 위한 목적으로 이용하였기 때문에 1980년대 이전에는 암호를 사용할 수 있는 기반 시스템들이 국방부 등 군과 주요 정부 부처 위주로 구성되어 있었다. 이에, 암호를 취급하거나 개발하는 인력들도 소수였으며 암호 관련 정책이나 법령의 적용도 국가의 힘에 의해서 한정적으로 사용할 수 있도록 제정되어 있었다.[2] 그러나, 컴퓨터 기술의 발전으로 민간영역에서도 전자상거래나 의료정보 등 기밀성 유지가 필수적인 정보들이 많아짐에 따라 1980년대 DES(Data Encryption Standard)가 민간에서도 사용가능한 표준암호로 제정되었으며[3], Diffie- Hellman에 의해서 공개키의 개념이 제시[4]되는 등 학계 중심의 연구가 활성화되었다. 이에, 암호 관련 정책도 민간을 중심으로 옮겨지기 시작한다. 특히, 1990년도 후반에는 민간 위주의 암호 연구 및 개발과 이용이 활발해 지면서 암호규제의 완화에 대한 요구가 증가하게되었다.

본 장에서는 우리나라의 암호정책을 분석해보기 위한 대조군으로 암호정책이 비교적 자유롭게 제정된 미국과 중도적 입장을 지니는 유럽의 대표국가인 프랑스, 강력한 국가주도 정책을 펼치는 중국의 암호정책을 비교 분석하여 보았다. 이를 위해서 표 1에서 보는 것처럼 국가의 암호권한 정도와 민간영역 통제 여부, 암호에 대한 진흥정책이 반영되어 있는지를 살펴보고 어떠한 법률에 의하여 관리되고 있는지를 확인해보았다. 또한, 각국의 전반적인 암호관련 규정을 정리한 OECD 가이드 라인을 통해 공통적으로 제시하는 바를 확인해보았다. 표 1에서 보는 것처럼 국가주도 정책을 펼치고 있는 경우는 O로 표시하였으며, 국가의 개입이 없는 경우는 X로 표기하였다. 두 가지 경우가 혼재되어 있는 경우에는 △로 표기하였다.

2.1.1 미국

1990년대 초반 미국 클린턴 행정부에서는 암호수출과 암호사용을 통제하기 위해서 Clipper 정책을 발표하였다. 이 정책은 암호장비에 NSA가 비공개로 설계한 Skipjack암호를 내장시킨 Clipper Chip이 설치된 장비만 사용하거나 수출할 수 있으며, 암호키

Table 1. Comparative analysis of Cryptography policies in several states

Category	US	France	China	Korea
the superiority of the state	×	△	○	×
Control of Private Sector	×	△	○	×
Have the ability to promote of Cryptography	○	○	○	△
Related Law	×	LCEN	China Enacts Encryption Law	×

사이즈도 56bit 이내로 제약하는 법안이다. 특히, Clipper 정책에서는 암호키를 생산할 경우 Clipper Chip에 의하여 암호키의 사본이 생성되고, 이를 정부기관에 임치하여 암호해독이 필요한 경우에는 국가기관에서 언제든지 사용하도록 강제하였다. 그러나, 시민단체 및 민간에서 키 임치는 국가의 프라이버시 침해이며 무분별한 남용이 우려된다는 비판여론을 지속하자 1998년에 암호정책을 수정하여 발표하였다. 이 정책에서는 미국 내에서는 암호사용을 자유롭게 허가하며 키 복구기능이 내재된 제품에 대해서는 키 사이즈에 관계없이 수출·입이 가능하도록 규제를 완화하였다. 또한, 국가차원의 암호접근을 별도로 추진할 것을 천명하였다.[5]

한편, 미국의 연방정부에서는 1997년에 키 복구기능이 없는 암호사용, 미국 암호제품의 수출통제 완화, 복호화 키에 대한 정부접근 차단 등을 골자로 하는 E-Privacy Act가 제시되었으나 상정되지 못하고 폐기되었으며, 1998년에는 국내 민간영역의 암호에 대한 키 위탁 금지, 키 복구에 필요한 법원명령 요구 등을 주요 내용으로 McCAIN-Kerrey Act가 발의되기도 하였다.[6] 현재 미국에는 암호에 대한 법적인 강제조항이 남아있기는 하지만 실질적으로는 암호의 자유화에 비중을 두고 있다. 그 예로, 2014년 FBI가 14명을 살해한 범죄자인 샌버다디노의 증거품으로 애플사의 아이폰을 확보한 후 구체적 증거를 확보하기 위해 암호해독을 요청하였다. 그러나, 애플사에서 개인 프라이버시 문제와 아이폰 암호해독이 선례가 될 경우 보안상 취약점이 발생할 것을 이유로 거절하여 법정 싸움으로 확대되었다. 결국, FBI가 아이폰의 잠금 기능을 미상 경로로 해제한 후 분쟁을 철회하였다. 이와 별개로 철회 직전 열린 판결에서 국가는 애플이 아이폰 잠금 기능을 해제하도록 강요할 수 없다고 판결하였다.[7]

미국의 암호정책을 평가해보면, 암호에 대한 통제를 시도하였으나 자유화에 대한 요구에 직면하자 전반적인 제한을 모두 해제하였다고 평가할 수 있다. 이에, 암호의 접근권한은 민간에 치우쳐져 있으며, 국가에서 도청기관인 NSA를 통하여 한정적인 암호해독을 하고 있다.

2.1.2 프랑스

프랑스는 유럽 국가 중에 가장 늦게까지 국가주도의 암호정책을 유지하였다. 1990년에 제정된 프랑스 법 90-1170에 따르면, 암호장비의 사용이나 수출에 대해서는 총리의 재가를 받아야 하며, 이를 위반할 경우 50만 프랑에 해당하는 벌금과 3개월의 구류에 처하도록 되어있다. 또한, 암호의 이용이나 수출은 40bit 이하에 대해서만 가능하도록 강력하게 통제하였다. 그러나, 인터넷 환경의 발달로 정보통신망 이용에 제한이 발생하자, 프랑스 정부에서는 40bit 이하의 암호는 자유롭게 활용하고 40bit이상일 경우 정부기관에 암호키를 임치하도록 정책을 변화하였다. 암호에 대한 강제적 통제는 1999년에 '암호 자율화 정책'이 발표되면서 암호키 임치제도가 폐지되었으며, 1999년에는 통제했던 암호키 길이를 128bit로 확대하는 암호 자유화 정책을 펼치면서 규제를 완화하였다. 이와는 별개로, 프랑스 법률 01-1062에 따르면 범죄조사 과정에서 암호해독에 대한 자격을 갖춘 사람에게는 암호에 대한 해독을 강요할 수 있으며, 이를 미준수시 3년의 징역과 €45,000 벌금에 처하며, 만약 미준수로 인하여 범죄행위가 발생하였을 경우 5년의 징역과 €75,000의 벌금에 처하도록 하는 등 국가차원의 암호강제 법률도 제정되어 있다.

한편, 암호 자유화에 대한 법률이 제정되자 프랑스 군 및 경찰, 비밀경호 부서 등은 강력한 암호 활용 필요성을 주장하며 정책에 반대하는 입장을 제시하였다. 반면, 많은 시민단체 및 학계에서는 프랑스 정보기관들이 암호를 통제하면서 불법적인 감청을 통해 프라이버시를 침해한 사실을 들어 더 이상 국가가 암호통제의 중심에 있어서는 안 된다고 주장했다. 이에, 현재 프랑스 정보기관들의 암호 활용은 제한되고 있는 실정이다.[8]

프랑스는 미국의 경우와 동일하게 암호에 대한 통제를 하였으며, 암호사용 자유화의 요구에 상업적인 측면은 해제해 주는 반면 공적으로 필요시에는 암호를 통제할 수 있는 일부 권한을 보유하고 있다. 또한, 내무부 산하에 암호해독기술지원센터를 설립하여 암호의 권한의 일부를 국가가 소유하고 있다.

2.1.3 중국

중국은 국제 사회에서 가장 강력한 암호통제 정책을 적용하고 있는 나라이다. 중국에서는 1999년 "商用密碼管理條例(NCECR)"을 제정하여 자국내 승인받지 않은 민간의 암호제품 제조 및 외산 암호의 이용을 엄격히 규제하고 있으며, 암호의 판매나 수입할 경우에도 국가의 승인을 받도록 강제하였다. 또한,

외국인이나 외국기업들이 중국에 들어와서 암호를 사용할 경우에도 NCECR의 승인을 받도록 하였다. 이에, 중국 내에서 사용하는 모든 암호는 자국산 암호를 사용하고 있다.

심지어 국제적 WiFi 표준인 WAP도 적용하지 않고 자체 표준인 WAPI를 사용하도록 통제하고 있다. 이는, 중국 정부에서 WAPI의 경우 키를 생성하여 가지고 있을 수 있는 점을 고려시 암호해독이 필요할 경우에 활용하기 위한 국가주도정책을 펼치는 것으로 볼 수 있다.[9]

중국의 경우는 정치적 상황과 맞물려서 민간영역의 암호사용을 강력하게 통제하고 있다. 이는 국가주도의 암호정책을 통하여 암호의 오용과 남용을 사전 차단하고 있다고 볼 수 있다.

2.2 OECD 암호정책 가이드라인

2.2.1 가이드라인 제정의 의의

OECD는 국가들간의 공통적으로 영향을 미치는 경제사회정책에 대한 다자간 논의와 협력체계를 구축하기 위해 마련된 정부간 기구이다. OECD에서는 약 200여개 주제에 대한 위원회와 그룹이 존재하며 세계적인 이슈에 대한 논의를 통하여 공식적인 지침과 규정을 제시한다. OECD는 법적 권한을 가지고 있지 않아 규정과 지침이 회원국에 구속력이 있지는 않다. 그러나, 회원국들이 정책을 만들때에는 적어도 OECD의 지침을 고려하고 있으며 정책 결정에 큰 영향을 끼친다.[10]

OECD 암호정책 가이드라인은 1997년에 파리에서 열린 Workshop on Cryptography Policy에서 가입 국가들의 암호정책에 대한 가이드라인 8가지를 다음과 같이 제시하였다. 이 가이드라인은 민간영역과 정부의 암호관련 정책들이 대립하고 있는 가운데 균형잡힌 정책방향을 제시하고 있다.

이러한 가이드라인이 제시된 이유는 인터넷 기술의 발달로 전자상거래 기술이 발전하면서 관할권 설정을 명확하게 하기가 어려우며, 특정 국가의 암호정책이 국제 무역에 대한 장벽으로 작용할 수 있는 등 범 세계적인 영향력을 미치기 때문이다.[11]

2.2.2 세부 가이드라인

2.2.2.1 신뢰할 수 있는 암호화 방법 적용

산업계 및 학계 등 민간영역에서는 신뢰할 수 있는(trustworthy) 암호화 방식을 적용하여 사용자들의 신뢰를 받을 수 있어야 한다. 또한, 정부의 규제나 허가, 암호사용의 방법 및 평가에 대해서도 신뢰받을 수 있어야 한다. 암호키 관리시스템의 경우에는 시스템이 적용받을 수 있는 법적 관할권을 지정해야 한다.

2.2.2.2 암호화 방법에 대한 선택 권리

사용자는 암호화 방법을 선택할 수 있는 권리가 있어야 한다. 사용자는 자신이 필요한 암호를 사용하여 보안을 적용할 수 있어야 한다. 또한, 정보 및 데이터를 다루는 개인이나 조직은 데이터의 기밀성 및 무결성 보장에 대한 책임이 있다. 즉, 사용자는 법이 정한 한계 내에서 암호를 자유롭게 사용하고 구현할 수 있으며 사용자가 보안에 대한 책임을 가진다. 정부는 통제를 최소화하고 사용자의 선택을 존중해야 한다. 그러나, 정부가 암호사용에 대한 법률제정을 최소화 해야한다고 강제하는 것은 아니다.

2.2.2.3 시장주도의 암호개발

암호화 방법은 개인이나 정부의 필요 및 요구에 의해서만 개발되어야 한다. 암호방법의 개발 및 제공은 개방적이고 경쟁적 환경인 시장에서 결정되어야 하며 시장주도여야 한다. 정부는 기업이나 연구소와 협업하여 암호기술을 발전시키도록 장려해야 한다. 암호화 방식과 관련된 국제 기술표준이나 프로토콜의 개발도 시장 주도로 이루어져야 한다.

2.2.2.4 암호화 방법의 표준

암호관련 표준 및 정책들은 국가 혹은 국제적 수준에서 결정되어야 한다. 국제적으로 인정된 표준기관과 정부, 기업 및 암호 전문가들은 암호에 대한 정보를 공유하고 개발 및 공표하기 위해 협력하여 상호운용성 및 호환할 수 있도록 해야한다. 또한, 국제표준이 제정되면 광범위하게 수용해야 한다.

2.2.2.5 프라이버시 및 개인정보 보호

통신에 대한 비밀성 보장 등 개인의 프라이버시에 대한 기본적인 권리는 국가 암호정책에서 존중되어야 한다. 암호화는 기밀성 유지와 더불어 개인정보수집을 차단할 수 있는 중요한 도구가 될 수 있다. 전자상거래에서 데이터의 무결성을 보장하기 위한 암호화 기법은 프라이버시 보호의 수준을 향상시켜준다. 특히, 개인을 식별할 수 있는 데이터가 포함된 시스템에는 프라이버시에 대한 보호장치가 수반되어야 한다.

2.2.2.6 정부의 합법적 접근 보장

국가는 암호정책으로 암호화된 데이터와 관련된 키나 평문에 대한 합법적 접근을 허용할 수 있다. 만약 암호화 방법에 대한 합법적 접근을 고려한다면, 공공의 이익이나 법적 강제가 국가안보에 미치는 영향이나 남용에 대한 위험을 고려해야 한다. 평문이나 암호키에 대한 접근을 적법절차에 의해 요구하는 경우 해당 조직이나 개인은 평문에 대해 법적 소유권을 가져야 하며 합법적 목적으로 사용해야 한다. 또한, 암호키를 얻는 과정은 합법적으로 기록되어야 한다. 또한, 키 관리 시스템은 해독 가능한 솔루션이 제공되어야 한다. 이러한 기술은 데이터를 복구하거나 키를 잃어버렸을 때 활용된다.

2.2.2.7 법적 책임 부여

법률에 근거하여 암호 서비스는 제공되어야 하며, 암호키를 보유하고 접속하거나 사용하는 실체에 대한 책임은 명확히 기술되어야 한다. 또한, 암호키의 오·남용에 대한 사용자의 책임 또한 분명해야 한다. 암호키 소유자는 암호화된 데이터의 암호키나 평문을 합법적으로 제공하는 것에 대한 책임을 지지 않아야 한다. 또한, 합법적 접근권한을 가진 당사자는 자신이 획득한 암호키나 평문에 대한 오용에 대해서는 명확한 책임을 져야 한다.

2.2.2.8 국제 협력

정부는 암호정책에 대해서 서로 협력하고 암호정책이라는 이름으로 무역에 장애가 되는 것을 피해야 한다. 각 국이 선택하는 암호정책들은 다른 나라와 유사하게 조정되어야 하며, 국가 키 관리시스템은 적절한 경우 국제적 사용을 허용해야 한다. 어떤 정부도 자신의 관할권 내에 있는 암호화된 데이터의 자유로운 흐름을 방해해서는 안된다. 국제 무역에서는 세계 전자상거래간 부당한 장애를 일으키는 암호정책과 관행을 개발하는 것은 피해야 한다.

2.2.3 분석 및 평가

이 가이드라인은 암호기술에 대한 경제적 이익과 국가의 통제 및 국가 간의 정치적 문제에 대해서 적절한 균형적 관점으로 제안되었다. 1990년 초반만 하더라도 인터넷의 활용은 소수에게만 적용되는 기술이었다. 그러나, 급속한 발전으로 인하여 전자상거래가 활성화 되면서 기존의 규제위주의 암호정책이 암호 자유화에 대한 요구로 변하게 되었다. 이런 시대적 요구에 따라 제정된 OECD 암호 가이드라인은 변화를 이끄는 계기로 작용하였다.[12]

세부 조항들을 살펴보면 기존의 암호규제 완화에 대한 내용들이 주를 이루고 있으며, 암호의 개발 및 이용 분야도 민간영역에 자유화를 부여하도록 구성되어 있다. 한편으로는, 암호가 개인에 의해 오용될 경우를 방지하기 위한 국가의 개입이 필요한 조항도 포함되어 있다. 이러한 조항들은 일부 서로 상충되기도 하지만 가이드라인의 법적 권한이 무조건적 적용이 아닌 각 국가의 상황에 맞추어 적절히 채택하는 권고의 형식을 지니고 있어 각 국의 정치 및 경제적 상황에 따라서 적용할 수 있도록 하였다. 이에, 같은 OECD 가입국 내에서도 정치적 상황에 따라 법적으로 강제하는 부분이 상이하게 적용되었다.

또한, 이 가이드라인을 기점으로 시장주도의 암호수출 등이 활성화 되면서 암호에 대한 연구 및 경제적 가치가 증가하게 되는 계기도 되었다. 가이드라인 제정과정이 약 1년 만에 이루어질 정도로 급박하게 이루어지는 등 전례없는 대중의 관심을 가져왔고 기존 회담들이 미국을 중심으로 이루어지던 것에 비해 일본, 스웨덴, 독일 등 여러 국가가 암호정책에 대해 목소리를 냄으로서 전 세계가 암호정책에 대한 같은 시각을 견지할 수 있는 계기가 되었다.

2.3 한국의 암호정책

2.3.1 암호정책 특징

국내의 경우 정보화 인프라가 세계 최고수준으로

Table 2. Policies and laws of Cryptography in Korea

Category		Article
Law	MilitaryCriminal ACT	Article 81 (Unlawful Use of Secret Code) Any of the following persons shall be punished by imprisonment with or without labor for a limited term of not less than two years: - A person who transmits any secret code without permission - A person who makes another person, who is not authorized to receive a secret code, receive the secret code - A person who fails to deliver a secret code that he/she receives or makes a false delivery of such a secret code
	Framework Act On National Infomatization	Article 37 (Establishment of Policies on Protection of Information) The Government may prepare measures capable of aiding the development and use of encoding technologies, and contributing to the safety of information communications services that use encoding technologies.
	Framework Act On Electronic Document And Transaction	Article 14 (Use of Encryption Products) (1) Any electronic transaction business entity may use an encryption product to ensure the security and reliability of electronic transactions. (2) If the Government deems it necessary for national security, it may restrict the use of encryption products, and take necessary measures to gain access to the original text of encrypted information or encryption technology.
Regul-ation	Regulation on Managemnt Of Security	Article 7(Supply and Return of Crytography Code book), Article 8(Handle of Secret・Crytography Code book), Article 9(Authorized Person who handle Secret ・Crytography Code book), 10조(Aurhorization and Revocation of handle Secret・Crytography Code book)

발달되어 있으며 이를 활용한 정보의 이용도 활발하게 이루어지고 있다. 그러나, 데이터를 보호하기 위한 암호정책 분야에 대해서는 명확한 법적 제도가 제정되어 있지 않다가 OECD 암호가이드라인이 발표된 이후 1999년도에 '암호이용촉진법' 제하로 논의가 이루어졌다. 그러나, 암호키 강제해독에 대한 논란으로 입법화되지 못하였다. 이후에도 개인 프라이버시 강화와 인권침해 우려 등으로 구체적인 암호화 정책에 대한 법적 제정에 대한 논의가 이루어지지 않고 있는 실정이다.[13]

이와는 별개로, 군이나 민간영역의 암호활용에 대한 규제나 국가의 책임 등은 표1에서 보는 것처럼 일부 법령에 조항으로 포함되어 있다.

2.3.2 강・약점 분석 및 평가

우선, 군형법 및 대통령령인 보안업무규정을 살펴보면 국가용 암호를 사용하는 군이나 정부 기관의 암호 사용지침을 제시하거나 오용했을 경우 처벌규정을 명시하고 있다. 또한, 이러한 규정은 공공기관 및 민간기관의 내부 보안규정에서도 사용한계점을 명시해 두었다. 그러나, 이러한 규정들은 OECD 가이드라인에서 제시된 암호이용의 활성화를 위한 정책으로 보기에는 어려움이 있다.

다음으로 국가정보화 기본법을 살펴보면 정부가 암호이용의 활성화와 촉진을 하도록 책임을 부여하고 있다. 이를 위해 KISA에서 암호이용활성화 사이트를 운영하는 등 암호진흥을 위해 노력하고 있다. 그러나 규모가 1개 팀으로 조직되어 작으며 소스코드 제시 등 기술적 지원 위주로 운용되고 있어 민간영역의 암호 활성화를 지원하기에는 한계점이 있다. 특히, 암호키 관리 안내서, 암호정책 수립기준 설명서 등 암호관련 안내서들을 제작하여 배포하고 있는데 법적인 강제력이 없어 암호의 오・남용이나 권고 사항을 미준수할 경우에 대한 대책이 미비한 실정이다.

마지막으로 전자문서 및 전자거래 기본법에서는 국가의 암호접근 권한을 법적으로 명시해 두었다. 그러나, 기술적 접근이나 정책적 접근 등 구체적인 접근 방법이 제시되지 않아 국내에서는 실질적으로 암호접근을 강제하는 사례는 식별되지 않고 있다.

종합적으로 보면, OECD 가이드라인에서 제시한 수준의 정책들은 법령들속에 일부 포함되어 있지만 실질적으로 적용하기에는 구체적이지 않다. 또한, 외국의 사례와 비교를 해볼 경우에는 자유로운 암호사용을 장려하고 국가적 통제를 하지않는 미국과 유사하다고 볼 수 있다. 한편으로는 암호 이용을 활성화

할 수 있는 제반 법령이나 규정도 명확하지 않아 정부가 암호이용을 장려한다고 보기도 어렵다. 즉, 암호이용에 대한 전반적 제도적 뒷받침이 미미하다고 분석할 수 있어 국가의 관심도가 필요한 실정이다.

III. 암호 정책에 관한 논쟁

3.1 암호 사용에 대한 갈등

민간영역의 암호기술 사용 확대로 국가위주로 관리하던 암호통제 영역의 범위가 급속도로 확장되었다. 특히, 우리나라의 경우에는 기존부터 민간분야의 암호에 대한 강력한 통제가 없어 암호정책에 대한 법적 한계점 설정이 미비하고 법제화에 대한 인식도 떨어지는 실정이다.

암호에 대한 가장 큰 쟁점은 암호사용의 투명성이다. 서두에 언급한 것처럼 암호는 정보를 보호하기 위한 가장 강력한 장치인 동시에 범죄 등에 악용될 수 있는 무기가 될 수도 있다. 이를 해소하기 위해 각 국에서는 암호에 대한 접근 권한을 가지기 위한 다양한 시도를 해왔다. 외국사례를 살펴보면 앞서 소개한 샌버다디노 사건에 대한 이슈로 90년대 이후 수면 아래에 있던 국가 차원의 합법적인 암호접근 권한에 대한 문제가 대두되었다. 국가의 입장에서는 테러, 간첩행위 등 국가안보에 심대한 위해를 끼치거나 생명과 직결된 범죄행위, 마약 거래 등 대형범죄를 방지하기 위해서 암호해독에 대한 접근 권한은 불가피하다고 주장한다. 한편, 시민단체나 기업들의 입장에서는 암호해독 권한이 국가 차원에서 남용되어 무분별한 감청이나 개인의 프라이버시 침해를 야기할 가능성이 높다고 주장한다. 또한, 민간 암호개발자들은 암호해독을 위한 백도어 등 추가적인 장치를 설치할 경우 암호에 대한 완전성 저하가 우려된다는 주장을 하며 팽팽하게 대립하고 있다. 유럽 내 일부 국가에서는 암호의 중요성을 인식하여 국가 차원의 역량을 확보하여 암호에 대한 우위를 선점하기 위해 국가 주도의 암호연구 및 해독기관을 만들어 암호접근 권한을 확보하기도 한다.

한편, 우리나라의 경우는 국가의 암호해독에 대한 권한보다 개인의 프라이버시를 더 높은 가치로 인정하고 있어 중요범죄의 수사나 내사에서 어려움을 겪고 있다. 물론, 검찰이나 경찰에서 디지털포렌식을 통해 압수된 전자증거에 대한 암호를 해독하려는 노력을 기울이고 있지만, 암호해독은 포렌식 절차 중 일부분에 한정된 분야로서 많은 발전이 이루어지지는 않았으며, 일부 수학자나 암호학자들에 의해 이론적 연구에 치중되어 이루어지고 있다.

최근들어 정보통신망이 발전하면서 대부분의 개인이 스마트폰을 소유하고 있다. 스마트폰의 특성상 인터넷을 자유롭게 사용할 수 있어 수 많은 정보가 저장되어 있으며, 범죄가 발생시에도 스마트폰의 정보에 따라서 범죄여건의 성립 여부가 결정될 수 있는 가능성이 매우 높아졌다.

결국, 오늘날 암호화에 대한 이슈는 암호화된 스마트폰이나 SNS에 대하여 국가 차원에서 강한 해독권한을 가질 수 있는지에 대해 이루어진다. 국가에 암호접근 권한이 없을 경우에는 국가안보에 위해를 끼치는 범죄나 범죄기도를 사전 억제하기에 많은 어려움이 있어 공공의 안전보장이라는 기능을 달성할 수 없다.

3.2 법률적 쟁점

헌법 18조를 살펴보면 모든 국민은 통신의 비밀을 침해받지 않을 권리를 가지고 있는 반면, 37조에서 국민의 모든 자유와 권리는 국가 안전보장·질서유지 또는 공공복리를 위하여 필요한 경우에 법률로서 제한할 수 있다는 조항이 있다. 또한, 통신비밀보호법 5조에서는 중요 범죄수사 및 국가보안법, 군형법 및 군기법 등 국가안보 목적에서는 통신에 대한 정보를 적법한 절차에 의해서 수집할 수 있어 개인의 통신상의 비밀도 국가 안전보장을 위해서는 침해할 수 있다고 볼 수 있다. 이에, 통신을 통해 소통되는 정보에 대한 법적인 강제력은 충분히 발휘될 수 있을 것으로 판단된다. 한편, 이러한 통신데이터를 보호하기 위한 암호도 국가가 강제할 수 있는지에 대해서 조금 더 알아보았다.

첫째, 암호가 구속력을 가질 수 있는 실체인지에 대해서 살펴보았다. 우선, 법령상에서 전자정보는 컴퓨터 등 전산정보 처리장치에 의하여 디지털 형태로 저장되거나 전송되는 정보로서 이용자에 의하여 작성되어 저장된 정보뿐만 아니라, 이용자의 의사와 관계없이 디지털기기에 의하여 생성된 정보를 포함한다. 이와 관련, 통신에 대한 정보를 확인하기 위해서는 암호에 대한 해독이 수반되어야 하여 암호 또한 통신의 일종으로 보는 것이 타당하다. 이에, 범죄에 사용된 암호의 경우에는 영장이 발부된 경우 압수수색 대상이 될 수 있을 것으로 판단된다.[14]

둘째, 각 국에서 이슈가 되고 있는 암호 키 복구 문제에 대해서 살펴보았다. OECD 가이드라인에도 명시되었듯이 국가는 암호 접근권한을 가질 수 있다. 흔히, 각 국에서 적용하고 있는 권한은 키 복구와 키 위탁으로 나누어진다. 키 복구는 암호화된 데이터에 대한 평문 정보나 해독할 수 있는 키 정보를 제 3자나 암호개발자에게 위탁시키고 일정 조건하에서 위탁된 키나 암호문에 대한 평문을 복호화하여 적법 권한이 부여된 정부나 수사권이 있는 부서에 인도하는 것을 의미한다. 한편, 키 위탁은 미국에서 시도하던 정책으로 암호키를 생산시 사본 키를 생산하여 정부에 키를 맡긴 후 복호화에 대한 소요 발생시 사본 키로 평문이나 키를 복호화하는 방법이다.

이에 대해서는 법적으로 첨예하게 대응할 수 밖에 없다고 본다. 개인의 자유를 가장 중시하는 미국의 경우에도 내란 및 외환죄와 반역, 간첩, 사보타주, 테러리즘과 같은 범죄영역에 대해서는 감청 활동과 비합법적 정보수집이 허용되고 있다.[15] 현재 우리나라에서도 국가안보 목적의 통신제한조치 수단으로 감청을 하는 등 범죄에 대한 증거확보나 국가 안보목적으로 필요할 경우 개인의 자유를 충분히 침해할 수 있기 때문이다. 암호의 경우에도 특정한 목적이 있을 경우에는 충분한 합법적 절차를 거쳐 키 복구를 할 수 있을 것으로 판단된다.

IV. 암호정책 발전방안

4.1 법률적 요건 확보

앞에서 살펴본 우리나라의 암호정책을 보면 실제 암호에 대한 통제가 전무한 수준으로 정책이 추진되어 왔다. 이에, 국가차원의 암호산업 육성 및 안보목적의 적절한 권한 획득 차원에서 암호에 대한 지위에 대해 법적으로 제시할 수 있어야 한다.

앞 장에서 살펴본 것처럼 암호를 데이터로 볼 수 있도록 명확한 법적 정리가 필요하다. 범죄에 대한 증거를 확보하기 위해 압수수색 진행간 대상정보와 범죄사실의 관련성이 입증되어야 하는 등 포괄적 압수수색이 금지되어야 한다. 따라서, 현재 법률상에서는 압수수색에 암호도 포함될 수 있는지에 대한 논쟁 가능성이 상존한다. 즉, 정보를 보호하기 위해 사용된 데이터 자료로서 주어진 데이터와 결합된 하나의 전자정보로 볼 수 있도록 법적으로 명시되어야 한다.

또한, 암호해독에 대한 강제를 국가가 할 수 있는 권한이 확보되어야 한다. 이를 위해 앞서 살펴본 프랑스의 경우와 같이 주요 범죄 해결에 한정하여 암호키 복구를 강제할 수 있도록 암호개발 업체나 정보통신망 사업자를 통제해야 한다. 그러나, 민간의 주장처럼 민간기업이 아닌 국가가 키를 소유할 경우 불법 감청 등 악용될 소지가 있다. 따라서 인증받은 민간기관들을 이용한다면 법적 갈등은 최소화 될 것이라고 판단된다.

4.2 국가 암호해독 기관 설립

최근 이슈가 된 'n번방 사건'의 증거인 휴대폰 암호를 해독하는데 약 2개월이 소요되었다고 보도되었다.[16] 이처럼 암호해독이 제한으로 수사가 지연되거나 중요정보를 확보하지 못하는 사건들이 발생되고 있다.

또한, 우리나라의 경우 안보환경상 북한과 대치중인 휴전국가로서 간첩 등의 활동이 국가보안에 영향을 미칠 수 있는 사건들의 발생 가능성이 상존하고 있다. 이에, 국가안보에 위해를 가할 목적으로 암호가 부정적으로 사용될 가능성을 배제할 수 없어 암호에 대해 많은 연구와 전문적인 지식이 필요함은 당연하다. 그러나, 세계 여러 국가들이 겪고 있듯이 민간영역의 암호를 국가가 강하게 통제하는 것도 국민의 자유를 침해하는 소지가 있어 위헌소지가 발생한다.

이에, 국가 차원의 암호해독 기관을 설립하고 암호해독에 대한 연구와 특정 길이 이상의 암호키를 위탁할 필요성이 있다. 국가용 암호나 고비도의 암호는 국가기관에서 접근권한을 확보하고 연구역량을 길러서 국가 안보목적의 암호해독 이슈가 발생할 경우 주도권을 가지도록 한다. 한편, 현재 널리 사용되고 있는 112bit 이하의 블록암호는 민간영역에서 자유롭게 개발 및 활용하고 자발적 키 복구를 위한 시스템을 구축하도록 장려해야 한다. 이를 통해 민간영역에서 키 분실 등으로 키 복구가 필요할 때에는 활용할 수 있도록 제도적 장치를 마련해야 한다. 이러한 방법을 적용할 경우 민간영역의 암호 자율성도 보장될 수 있다. 이를 통해 균형된 암호정책을 적용할 수 있을 것으로 생각된다.

또한, 암호에 대한 해독기관을 설립하는 경우에는 국가 예산을 기반으로 연구를 할 수 있어 전문적인 암호연구능력 향상은 물론 국가 암호산업 발전도 기대된다. 우리나라는 인터넷은 물론 이동통신망 등 각종 정보통신 분야가 최첨단을 달리고 있어 이를 보호

할 수 있는 암호기술이 발전할 수 있는 좋은 인프라가 형성되어 있다. 이에, 입법을 통해 암호해독기관을 설립하고 학계 및 민간과 암호정보를 공유해나간다면 세계적인 암호기술을 보유할 수 있을 것이라 전망한다.

외국의 사례를 보면 국가 정보기관이나 군에서 암호해독을 연구하고 있다. 현재 우리나라에서도 군의 안보지원사령부와 국정원 등 정보기관에서 암호에 대한 업무를 수행하고 있다. 이러한 조직을 활용해서 암호해독 조직을 구성한다면 기존의 노하우들을 유지한 상태에서 암호해독 능력을 확보할 수 있는 계기가 될 수 있다.

4.3. 암호부정사용에 대한 입법화

현재에는 민간영역의 암호사용을 별도로 통제하지 않고 있다. 이에, 범죄를 저지르거나 테러 등 국가안위에 위해한 계획을 수립하면서 자신들의 범죄사실을 은닉하기 위해 암호기술을 적용한다면 국가에 상당한 위험이 될 수 밖에 없다. 이에, 국가 차원에서는 중요범죄나 국가위해 목적으로 암호를 제작하거나 사용하는 것에 대한 제제를 할 수 있도록 입법화가 필요하다. 현재에는 군용 암호에 대해서만 군형법에 의해 오용할 경우에 한해 처벌을 할 수 있는 근거를 만들어 두었다. 그러나, 현재에는 암호를 이용하는 주체가 민간영역까지 넓게 확대되어 있으므로 불법적인 목적의 암호개발에 대해서도 제제할 필요성이 있다. 이에, 민간 형법에서도 암호를 부정사용할 경우 처벌을 할 수 있도록 법제화 한다면 부정한 암호사용을 최소화할 수 있을 것으로 판단된다.

또한, 국가에 암호 접근권한이 부여될 경우에 이를 집행하는 인원에 의한 암호부정 사용이 항상 논쟁이 되고 있다. 이에, 암호부정사용에 대한 죄가 법제화 될 경우 암호를 오·남용 하는 상황도 방지할 수 있을 것이라 생각된다.

V. 결 론

본 논문에서는 국내·외 암호정책에서 이슈가 되고 있는 자유화와 규제의 관점에서 충돌하는 문제점을 알아보았다. 특히, 우리나라의 경우 암호관련 법적 근거가 미약하여 악의적 암호사용에 대한 대응이 어려운 실정이다. 이에, 본 논문에서는 암호사용에 대한 균형과 건전한 암호사용 환경 조성 및 암호산업 발전을 도모할 수 있도록 국가 암호해독 기관 설립 및 민간영역 암호부정사용에 대한 입법화 방안을 제시하였다. 앞으로 4차산업혁명 시대가 되면 개인과 연결된 모든 사물들이 정보통신망을 통해 연결되고 이를 보호하기 위한 암호기술 발전의 필요성은 '명약관화'한 사실이다. 암호에 대한 국가적 관심과 민간의 참여를 유도하여 우리나라가 암호 강국으로 거듭날 수 있도록 정책적 강화는 반드시 이루어져야 할 것이다.

References

[1] Lin, Herbert S. "Cryptography and public policy." Journal of Government Information 25.2 (1998): pp. 135-148.

[2] Davies, Donald. "A brief history of cryptography." Information Security Technical Report 2.2 (1997): pp. 14-17.

[3] PUB, NIST FIPS. "46-3. Data Encryption Standard." Federal Information Processing Standards, National Bureau of Standards, US Department of Commerce (1977).

[4] Diffie, Whitfield. "New direction in cryptography." IEEE Trans. Inform. Theory 22 (1976): pp. 472-492.

[5] Campbell, Ryan. "Brademas Intern August 18, 2019 Keeping it Cryptic: The Enduring Debate on Privacy and Lawful Access On July 23, at the International Conference on Cyber Security in New York City." (2019).

[6] OECD legal instrument, "Recommendation of the Council OECD Legal Instruments concerning Guidelines for Cryptography Policy" Workshop on Cryptography Policy, Paris, 1997

[7] Schulze, Matthias. "Clipper meets Apple vs. FBI: a comparison of the cryptography discourses from 1993 and 2016." Media and Communication 5.1 (2017): pp. 54-62.

[8] Segell, Glen M. "French cryptography

policy: The turnabout of 1999." International Journal of Intelligence and CounterIntelligence 13.3 (2000): pp. 345-358.

[9] Saper, Nathan. "International cryptography regulation and the global information economy." Nw. J. Tech. & Intell. Prop. 11 (2012): xv.

[10] Baker, Stewart A. "Decoding OECD Guidlines for Cryptography Policy." Int'l L.. Vol. 31. 1997.

[11] Herson, David. "The Changing Face of International Cryptography Policy: Part 20-OECD Security Guidelines." Computer Fraud & Security 2001.9 (2001): pp. 8-9.

[12] Hyun Joe Kwon, Kilsoo Chun, Jae-il Lee "Current status of domestic and foreign Cryptography legal and Polices." Korea Institute Of Information Security And Cryptology 15.2 (2005): pp. 37-53.

[13] Korea Information Protection Center, "A Study on the Cryptographic Use Policy in the Domestic Private Sector" Technical Policy Study, 1998.12.

[14] Sook-yeon Lee. "Search and Seizure, Fundamental Rights, and Doctrine of Warrants Concerning Electronic Information" constitutional studies 18 (2012): pp. 1-44.

[15] Hee Won, Han, "A Legal Study on The Intelligence/Investigation Combination Phenomena According to The Security Paradigms Shift After Cold War Era - From Warfighting To Crimefighting" Korean Association of Laws study of law 2017.6.

[16] Chosun Ilbo "'Cho Ju-bin's cell phone password was released in two months." (2020. 5. 15.) https://news.mt.co.kr/mtview.php?no=2020051511022977954

〈저자소개〉

김 동 훈 (Dong-hoon Kim) 학생회원
2009년 2월: 육군3사관학교 전자공학과 학사
2019년 3월~2021년 2월: 고려대학교 정보보호학과 석사
〈관심분야〉 정보보호, 대칭키 암호분석, 암호정책

권 헌 영 (Hunyeong Kwon) 종신회원
1992년 2월: 연세대학교 법학과 학사
1998년 2월: 연세대학교 법학과 석사
2005년 2월: 연세대학교 법학과 박사
2008년 3월~2015년 8월: 광운대학교 법과대학 교수
2015년 9월~현재: 고려대학교 정보보호대학원 교수/사이버보안정책센터 센터장
〈관심분야〉 정보보호, 사이버보안, 사이버안보, 정보화, 전자정부, ICT 관련 법 및 정책

홍 석 희 (Seokhie Hong) 종신회원
1995년: 고려대학교 수학과 학사
1997년: 고려대학교 수학과 석사
2001년: 고려대학교 수학과 박사
1999년 8월~2004년 2월: ㈜시큐리티 테크놀로지 선임연구원
2003년 3월~2004년 2월: 고려대학교 정보보호기술연구센터 선임연구원
2004년 4월~2005년 2월: K.U. Leuven ESAT/SCD-COSIC 박사후 연구원
2005년 3월~2013년 8월: 고려대학교 정보보호대학원 부교수
2013년 9월~현재: 고려대학교 정보보호대학원 정교수
〈관심분야〉 대칭키 및 공개키 암호 알고리즘, 부채널 공격 및 대응기법, 디지털 포렌식