Journal of Knowledge Information Technology and Systems(JKITS), Vol. 15, No. 4, pp. 507-514, August 2020
https://doi.org/10.34163/jkits.2020.15.4.007

Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

A Study on Legislative Improvement Measures for Cyber Security-Focused on the Revised Communication Secret Protection Act

Su-Jin Kwon*

Senior Researcher of Glocal Science and Technology Law Institute

ABSTRACT

This paper seeks to recognize the importance of cyber-security in national security, especially in the Internet environment, in the reality of building a smart ecosystem globally. Digital transformation and 5G innovation are happening more rapidly after the Corona 19 incident. The dailyization of information and communication and the expanded use of cyberspace can be felt in our real life. Globalization of global villages, the realization of smart cities and e-government in Korea is happening realistically. The use of information and communication in the essential daily life of everyone, such as finance, medical care, and education, is taken for granted, and the problem of cyber space is not a problem of only a specific group, but a problem that is directly related to all citizens. In order to protect the nation's important facilities and systems from packet-type cyber terrorism and attacks, we will look at monitoring and regulation of Internet circuits in terms of national security. The purpose of this study is to grasp the technical characteristics of communication restriction measures (aka' packet interception') on Internet circuits and to suggest the direction of investigation on interception of packets through comparative law review. Review and revise the Constitutional Inconsistency Case of the Constitutional Court regarding whether the communication restriction measures (packet interception) through the Internet line prescribed by the Communication Secret Protection Act contradicts the principle of excess provision and proportion of Article 37 (2) of the Constitution. Through the provisions of the secret law, we will look into the problems and improvement measures of the current cyber security system, especially related to national security.

KEYWORDS: Cyber security, National security, Communication secret Protection act, Packet monitoring, National security, Cyber security system

ARTICLE INFO: Received 19 June 2020, Revised 8 July 2020, Accepted 10 August 2020.

*Corresponding author is with the Department of Information & Communication Engineering, JeongBo University, 100 Hyecheon-ro Seo-gu Daejeon, 35408, KOREA. *E-mail address*: jblee@jeongbo.ac.kr

1. 서 론

오늘날의 사회는 국가안보의 개념을 기존의 주권을 기반으로 한 물리적 영토의 개념에서 인터넷 공간을 기반으로 한 사이버안보를 포함하는 개념으로 넓게 보고 있다. 사이버테러는 집단화되고 있으며 국가들의 개입이 이루어지는 바, 사이버 공간에서의 안보의 문제는 비단 특정한 개인이나 집단의 문제가 아니라, 국가 전체적인 문제로 그 중요성이 인정된다. 사이버 공간에서 모든 시스템의 제어와 동작은 패킷데이터(Packet Data) 형태로 이루어진다. 사이버공간의 특성상 패킷감청에 의하지 않고서는 사이버범죄를 미리 사전에 인지하고 수사하는 것은 매우 힘들다[1]. 본 논문에서는 사이버범죄와 패킷 감청의 필요성을 살펴보면서 기존의 사이버범죄의 수사의 한계점과 인터넷회선 감청(패킷감청)기술의 개념과 필요성에 대하여 살펴보고자 한다. 비교법적 검토를 통하여 선진국의 경우 사이버범죄에 관하여 어떠한 규정을 두고 있는지 살펴보고 우리나라 사이버범죄 규정에 대한 검토와 개선방안을 제시하고자 한다. 마지막으로 사이버안보를 위한 법제개선방안을 검토하면서 통신비밀보호법 규정의 문제점과 헌법재판소의 헌법불합치 판례를 살펴보고자 한다. 특히 개정된 통신비밀보호법을 중심으로 국가안보를 보장하기 위한 법체계의 구축과 개선방안을 살펴보고자 한다.

2. 사이버범죄와 패킷감청의 필요성

2.1 사이버범죄와 기존수사의 한계

현대사회에서 기술의 발달로 모든 생활에서 인터넷 사이버공간을 기반으로 하고 있고 범죄의 수법도 사이버공간의 익명성을 이용하여 더욱 교묘해지고 복잡해지고 있다. DDOS, APT와 같은 사이버 테러 사이버범죄가 계속적으로 발생하고 있으며 이는 국가의 중요시설을 마비시키고 국가안보를 위협하는 중대한 문제가 될 수 있다. 이러한 상황에서 수사기관이 사이버공간에서의 테러와 범죄를 적극적으로 대응하기 위한 수사기법을 적극적으로 활용하는 것은 국가의 안전보장, 안보사항과도 밀접한 관계가 있다. 특히 사이버범죄의 경우 기존의 물리적 기반의 수사방법으로는 전쟁으로까지 이어질 수 있는 사이버안보를 위한 수사방법을 적극적으로 고려하여야 한다[2].

2.2 패킷감청의 개념과 필요성

패킷감청은 통신사업자가 고객을 위해 할당한 IP에 감청장비를 연결하여 해당 IP의 인터넷 회선을 사용하는 패킷을 가로채는 것으로 DPI (심층패킷분석: Deep Packet Inspection) 방식을 사용한다. [3]. DPI방식을 사용하는 단계에서 같은 IP 회선을 사용하는 수사목적과 무관한 제3자의 통신내용까지 감청한다는 비판이 있다[4]. 패킷데이터의 송수신 행위는 스마트 시티, 전자정부를 구축하는 사이버생태계 환경 하에서 개인과 사회 및 국가의 요청을 실시간으로 반영하고, 직접 민주주의를 실현할 수 있는 순기능을 가진다. 반면 국가안보를 위협하는 목적의 반국가적 행위와 테러행위 다양한 악성 프로그램과 랜섬웨어(Ransom ware) 등을 이용한 국가중요기반시설의 파괴와 국가기밀사항을 해킹하는 등의 반국가적 활동을 용이하게 하는 역기능도 갖는다.[5,16] 법원의 통제와 수사기관의 정당한 절차에 의한 패킷감청에 대해서 기본권 침해 우려가 있다는 이유로 불허한다는 것은 오히려 범죄로부터 보호받아야 할 피해자의 기본권이 침해되는 결과를 가져올 수 있다. 패킷감청은 기술적 특징에도 불구하고, 현재 사이버범죄 정보를 탐지할 수 있는 최적의 방법이며, 이를 통하여 개인과 사회 안전을

지키는 필수적인 수사기법으로 중요성이 인정된다.

3. 비교법적 검토

3.1 부다페스트 조약

국제사이버 범죄와 관련된 조약으로 '부다페스트 조약' (Budapest Treaty)이 있다. 부다페스트 조약은 사이버공간에서의 범죄를 예상하기 위한 목적으로 유럽평의회에 의하여 최초로 국제적 협약을 맺은 것으로 중요성이 인정된다. 부다페스트 조약을 통하여 사이버공간에서의 정보의 오남용을 방지하고, 정보데이터가 가지는 특징인 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)를 침해하는 행위를 방지하도록 하였다[6]. 이 조약을 통하여 사이버공간에서의 범죄에 대한 국가 간의 상호협력과 사이버범죄를 신속하고 효과적으로 처벌하기 위한 국제적 공조를 마련하기 위한 것이다[6].

3.2 비교법적 검토

미국, 영국, 독일, 일본과 같은 선진국에서 통신제한조치를 어떻게 규율하는지 살펴보면, 일반범죄와 국가안보범죄에 차등을 두어 절차와 요건을 다르게 규정함을 알 수 있다.

3.2.1 미국

미국은 국제사이버범죄조약에 따라 컴퓨터 시스템 또는 데이터에 의도적으로 접근한 경우 범죄행위로 간주하고, 데이터의 손괴나 취득이 이루어지지 않은 경우에도 범죄의 실행으로 본다[7]. 미국은 유보조항에서 규정하였듯이 미국의 국가안전보장에 피해를 입히는 경우 자위권 행사를 정당화 하고 있으며 사이버범죄와 관련하여 국가안보에 중점을 두고 있다.

3.2.2 영국

영국은 대규모의 통신 감시를 허용하는 수사권한법(The Investigatory Powers Act)의 시행을 통하여 국가안보 및 중대범죄에 관한 처벌규정을 두고 있다. 국가안보와 관련 있는 데이터와 기술통신사업에 영향을 미치는 시도에 관한 규율을 하고 있다.

3.2.3 독일

독일에서는 급증하는 사이버테러에 대응하기 위해 행정절차법(Vervaltungsverfahrensgesetz) 3a조에 전자적 소통(Elektronische Kommunikation) 에 대한 조항을 추가하여 사이버안보의 중요성을 반영하였다. 또한 독일형법에서도 '정보해킹죄'를 신설하여 사이버보안을 강화하고 2015년 사이버안보에 관한 일반법으로 IT안보법(IT-Sicherheitsgesetz)을 시행하였다. 기업 뿐 아니라 연방행정기관들도 동법에서 규정한 기준에 충족하도록 의무부과규정을 두었으며 기업과 기관들로 하여금 사이버 공격이 의심되는 경우 행정청에 신고를 의무화하는 규정을 두었다. 한편으로 사이버테러를 막기 위한 과정에서 정보수집의 남용을 억제하기 위한 정보보호법 (Bundesdatenschuzgesetz)도 제정되었다[8].

3.2.4 일본

일본의 경우에는 사이버범죄와 관련된 개인과 기업 국가의 침해와 손해에 관하여 사이버범죄와 관련한 통신수사를 허용하고 있다[9]. 우리나라도

특히 사이버범죄와 관련하여서는 공공과 민간 금융부분으로 영역을 분리하여 각 부문별로 법률의 보호이익과 목적에 따라 체계화된 법적체계를 구축할 필요가 있다. 특히 국가안보와 관련된 사이버범죄의 경우 별도의 규정과 수사권, 접근절차와 허용범위, 허용기관, 국제적 공조 부문을 세분화하여 우리나라 실정에 맞도록 체계화하는 노력이 필요하다[10].

4. 사이버 안보를 위한 법제개선 방안

4.1 현행 통신비밀보호법의 문제점과 법제개선방안

4.1.1 헌법재판소 헌법불합치 결정

헌법재판소는 통신비밀보호법 제5조 제2항은 '수사기관이 국가보안법 위반 사건 수사를 위해 용의자가 보내거나 받은 우편물 및 전기통신에 대해 통신제한조치를 할 수 있다'는 내용을 담고 있다. 헌법재판소는 2018년 8월 30일 패킷감청의 근거가 된 통신비밀보호법 규정에 대하여 헌법불합치 결정을 내렸다. 헌법재판소는 인터넷 회선 감청은 집행 및 그 이후에 제3자의 정보나 범죄수사와 무관한 정보까지 수사기관에 의해 수집. 보관되고 있지는 않는지 수사기관이 원래 허가받은 목적 범위 내에서 자료를 이용·처리하고 있는지 등을 감독 내지 통제할 법적 장치가 강하게 요구된다고 하였다[11]. 또한 현행 통신비밀보호법은 관련 공무원 등에게 비밀준수의무를 부과하고(통신비밀보호법 제11조), 통신제한조치로 취득한 자료의 사용제한(통신비밀보호법 제12조)를 규정하고 있는 것 외에는 수사기관이 감청집행으로 취득하는 막대한 양의 자료를 처리하는 절차에 대해서 아무런 규정을 두고 있지 않음을 지적하였다. 구체적으로 살펴보면 기존 패킷감청 절차가 헌법 제37조 제2항의 과잉금지원칙에 위배된다는 헌법불합치 판결이 나왔지만 이는 절차에 대한 일부법률 개정안을 요구하는 것이지 패킷감청 자체를 허용하지 않는 취지는 아니다[12]. 패킷감청을 통한 불법정보는 전통적인 통신수단과 차이점이 존재하며, 정보통신사업자의 경우에도 모든 데이터의 내용을 저장하기는 불가능하다는 점, 불법통신내용에 관한 압수영장만으로는 수사의 목적을 달성하기 어렵다는 점 등을 고려할 때 수사수단으로서 국가안전보장을 위한 적정성을 필요성이 인정된다[13]. 통신비밀보호법 관련한 조항이 헌법 제37조 제2항의 과잉금지원칙에 반하여 수사목적과 무관한 제3자의 기본권을 과도하게 침해하는지 여부에 관하여 헌법재판소는 패킷감청의 기술적 특성으로 인하여 감청기간 동안 특정 인터넷 회선의 모든 패킷데이터가 총체적으로 수집되지만 혐의자 이외의 제3자에 대한 감청은 선별기능을 가진 소프트웨어를 통해 순차적으로 범위가 압축되며 패킷감청은 암호화된 패킷데이터를 수집하는 것으로 패킷감청 자체가 곧바로 청취 및 공독을 의미하지는 않으므로 수사목적과 무관한 제3자의 통신비밀의 자유와 사생활의 자유, 표현의 자유와 같은 기본권을 과도하게 침해하지는 않는다. 현행 통신제한조치의 규정을 보면 보충성 원칙을 갖추었는지 여부를 판단하고 사법적 통제와 근거에 따른 허가요건을 갖추어야 통신제한이 가능하다는 점, 개인의 침해되는 기본권 제한이라는 사익과 통신제한조치를 통하여 보호되는 법익은 국가나 사회의 안녕과 질서유지 그밖의 개인의 생명이나 신체의 안전이라는 보다 큰 이익이라는 점을 보았을 때 수사목적과 무관한 제3자에 대한 패킷감청이 있었다 하더라도 그것은 반국가행위와 사이버테러의 수사를 위하여 행위자를 선별하기까지 불가피한 수단이었다는 점, 일시적으로

이루어지는 것이며 형사소송법 제308조의 2 위법수집증거 배제규정과 통신비밀보호법 제12조의 통신제한조치로 취득한 자료의 사용제한 규정 그밖의 관련 담당자의 비밀누설금지 규정 등에 비추어 볼 때 헌법상 과잉금지원칙을 위반하지 않는다[14]. 다만 통신제한조치를 통하여 수집한 자료의 삭제와 보관에 관한 사후적 절차규정 등을 통하여 입법개선 조치를 취할 필요성은 인정된다.

4.1.2 개정된 통신비밀보호법 규정 검토

입법개선으로 통신비밀보호법이 2019. 12. 31, 2020. 3. 24 두 차례 개정되었다. 인터넷 회선에 대한 통신제한 조치(패킷감청)관련 규정이 통신비밀보호법 제12조의 2로 신설되었는데 통신제한조치로 취득한 자료의 관리에 대한 사후통제 규정을 마련하였다는 특징이 있다. 이러한 입법개선에도 불구하고 패킷감청의 기술적 특징으로 인한 수사목적과 무관한 제3자의 기본권 침해에 관한 보호가 미흡하다는 비판도 존재하지만, 국가안보를 보장하기 위한 불가피한 수사방법으로 필요성을 인정하여야 한다. 다만 인터넷회선제한을 통해 취득한 감청자료에 대한 사후적 조치를 마련함으로써 절차적 투명성과 객관성을 확보할 수 있다. 구체적 방안으로 감청을 허가한 판사에게 감청자료를 봉인하여 제출하는 방안과 수사기관에서 수사목적과 무관한 제3자의 감청자료에 대하여 오토딜리트(Otto-Delete, 자동화삭제프로그램)과 같은 기술적 장치를 마련하는 방안이 있다. 오토딜리트의 경우 일정기간이 지나면 혐의자와 관련이 없는 일반인의 통신감청 자료는 자동으로 삭제되도록 프로그램하고 사용자의 로그(Log)기록을 저장하여 국가기관에서의 위조·변조를 방지하는 프로그램 구현을 통하여 절차의 객관성과 신뢰성 투명성을 확보할 수 있다.

5. 결 론

기존 패킷감청 절차가 헌법 제37조 제2항의 과잉금지원칙에 위배된다는 헌법불합치 판결이 나왔지만 이는 절차에 대한 일부법률 개정안을 요구하는 것이지 패킷감청 대상범죄에 대한 언급을 한 취지는 아니다. 부다페스트 조약과 같은 국제조약에서패킷감청을 요구하고 있어 주요 사이버범죄를 통신비밀보호법의 통신제한조치 대상에 포함시키는 것이 국제적인 추세를 따르는 것이다. 코로나19 사태 이후 디지털트랜스포메이션, 5G혁신이 더욱 빠르게 일어나고 있다. 정보통신의 일상화와 사이버공간의 활용 확대는 우리의 실생활에서도 느낄 수 있으며 국제적으로 글로벌 빌리지화나 국내에서의 스마트 시티, 전자정부의 실현이 현실적으로 일어나고 있다[15]. 금융, 의료, 교육 등 모든 사람들의 필수적 일상에서 정보통신의 활용이 당연시되고 있으며 사이버 공간의 문제는 어느 특정 집단만의 문제가 아니라 모든 국민에게 직결되는 문제로 중요성이 인식된다. 이러한 현실에서 사이버테러, 위협, 더 나아가 사이버전쟁으로부터 사이버보안체계를 구축하는 것이 어느 때보다 중요하다. 특히 북한으로부터의 전쟁 위협과 미국 등 선진국들이 사이버안보 위협에 대처하기 위해 정보역량 확충에 매진하고 있는 만큼, 우리나라도 국가정보기관도 보다 더 유기적이고 효율적인 정보협력 체제를 구축하고, 구체적이고 체계적인 법체계를 구축하여야 한다. 통신비밀보호법과 국가기밀보호법의 규정의 개정을 통하여 특히 국가안보와 관련된 사항의 경우 패킷감청과 같은 사이버범죄를 예방하고 파악할 수 있는 수사기법을 적극적으로 활용할 수 있도록 하여야 한다. 사이버공격은 소리없는 전쟁이며 좀비프로그램 악성코드는 코로나바이러스와 유사한 점이 있다. 코로나에 있어 무증상 보균자가 돌아다니는 것처럼 악성코드와 사이버테러

의 위험성은 언제든 존재한다. 코로나를 질병관리본부에서 전문가 집단이 정보를 빠르게 공유하고, 진단하여 효과적인 대응책을 마련하는 것처럼 국가안보 사안과 관련된 사이버보안에 있어서는 국정원과 국가사이버안전센터(NCSC)와 같은 기관이 전문성을 발휘할 수 있도록 법적근거를 마련하여야 한다. 사이버보안법을 제정하여 사이버보안 체계의 구축을 함으로써 효과적인 보안정책을 실현하여야 한다. 내실 있고 지속적인 사이버 안보 전략 이행을 위한 법·제도 기반을 마련하고 예산과 인력, 법·제도의 구축을 위한 국가 사이버 안보 조직 간 거버넌스를 강화하는 세부적인 조항을 두고, 정부와 민간이 협력하여 국가 차원에서 체계적이고 일원화된 사이버 공격 예방·대응 업무를 수행하기 위한 통합법 제정을 하여야 한다. 그밖에도 정보기관에 대한 국민들의 신뢰구축을 위하여 내부감찰 강화하고 패킷감청과 같은 수사기법의 단점을 보완하기 위한 오토딜리트(Otto-delete 자동화 삭제)시스템의 구축과 같은 기술적 요소를 갖춘 객관적인 통제장치를 마련하여야 한다. 또한 사이버 안보와 관련한 국가의 예산을 늘리고 관련 기관과 학계에서의 연구 및 교육과정 시스템을 통하여 사이버안보의 중요성을 알리고 국민적 관심을 갖도록 하여야 한다.

References

[1] G. M. Yang, and S. J Lee, *Necessity to include cyber-crime in crimes subject to communication restrictions*, Criminal policy research, Vol. 30, No. 4, pp. 272-302, 2019.

[2] S. S. Han, *A study on institutional improvement for dark web cyber-crime investigation: Focusing on packet monitoring and online search,* dongguk university master's thesis, pp. 1-69, 2019.

[3] Michael Chertoff and Tobby Simon, *The impact of the dark web on internet governance and cyber security,* CIGI, Global commission on internet governance, 2015.

[4] G. M. Yang, S. J. Lee, *Necessity to include cybercrime in crimes subject to communication restrictions*, Criminal Policy Research, Vol. 30, No. 4, pp. 271-302, 2019.

[5] H. W. Kim, and P. S. Park, *Usability evaluation of android-based smart phone soft keyboard*, proceedings of the 12nd Spring conference of The korean knowledge information society, 2010.

[6] S. C. Park, *A study on improvement of communication investigation to enhance basic rights,* master's thesis, Sungkyunkwan university, pp. 1-100, 2020.

[7] 18.U.S.C. §1030(a)(1), 18.U.S.C. §1030(c)(1)

[8] G10 Act (Act on the limitation of secrets to letters, postal and telecommunications): Gesetz zur Beschränkung des Brief, Post und Fernmeldegeheimnisses) BGBl.IS.1 It is regulated by the telecommunications Act (Telekommunikationsgesetz) and federal law to strengthen countermeasures against international terrorism; H. W Park, *Germany of the law on the ratification of the cyber crime prevention treaty*, International criminal law research institute, legislation, pp. 20-34, 2009.

[9] H. W. Kim, *A review of the german terrorism counter measures,* Korean terror society, Vol. 11, No. 3, pp. 211-229, 2018.

[10] H. J. Lee, *Cell site location information investigation about mobile phone and*

notification system in germany - focused on review and improvement proposal of amendment on protection of communications secrets ac, KLAJ, Vol. 68, No. 4, pp. 497-528, 2019.

[11] H. W. Kim, *Review of japan's counter-terrorism measures on the international terrorism*, korean terror society, Vol. 12, No. 1, pp. 150-166, 2019.

[12] Due to the nature of packet interception, packet interception can not be ruled out only by the concern that the content of communication by third parties other than the purpose of investigation may also be intercepted; Supreme court 2012. 10. 11. verdict 2012, 7455 ruling.

[13] I. S. Kim, J. D Bae, and S. D Lee, *Criminal legal response to the information society*, Comparative criminal law research Vol. 2, No. 3, pp. 31-61, 2002.

[14] Y. Y. Cho, *Direction of reforms in electronic communications privacy law with regards to latest major issues,* criminal law research, Vol. 26, No. 4, pp. 105-138, 2014.

[15] Schmitt, *Tallinnmanual on the international law applicable cyber warfare*, Cambridge, 2013.

[16] S. C. Kim, *Research on improvement plans for the communication monitoring system*, central law, Vol. 10, No. 1, pp. 247-269, 2008.

사이버안보를 위한 법제 개선방안 연구 - 통신비밀보호법 중심으로

권수진

성균관대학교 글로컬과학기술법연구소 선임연구원

요 약

본 논문에서는 전 세계적으로 스마트생태계를 구축하고 있는 현실에서 국가안보 특히 인터넷 환경에서 사이버안보의 중요성을 인식하고자 한다. 코로나19사태 이후 디지털트랜스포메이션, 5G혁신이 더욱 빠르게 일어나고 있다. 정보통신의 일상화와 사이버공간의 활용 확대는 우리의 실생활에서도 느낄 수 있다. 국제적으로 글로벌 빌리지화나 국내에서의 스마트 시티, 전자정부의 실현이 현실적으로 일어나고 있다. 금융, 의료, 교육 등 모든 사람들의 필수적 일상에서 정보통신의 활용이 당연시 되고 있으며 사이버 공간의 문제는 어느 특정 집단만의 문제가 아니라 모든 국민에게 직결되는 문제이다. 패킷형태로 이루어지는 사이버테러와 공격으로부터 국가의 중요시설과 시스템을 방어하기 위하여 국가안전보장 측면에서 인터넷회선에 대한 통신제한조치(일명 '패킷감청')의 필요성에 대하여 살펴보고자 한다. 인터넷 회선에 대한 통신제한 조치의 기술적 특성을 파악하고, 비교법적 검토를 통하여 시사점을 얻고자 한다. 통신비밀보호법이 규정한 인터넷회선을 통한 통신제한조치가 헌법 제37조 제2항의 과잉금지원칙과 비례의 원칙에 반하는지와 관련하여 헌법재판소의 헌법불합치 판례와 개정입법규정을 살펴보고자 한다. 특히 통신비밀법 규정을 통하여 국가안보를 보장하기 위한 사이버안보체계의 개선방안을 살펴보고자 한다.

Su Jin Kwon received Ph.D. in law from Sungkyunkwan University, lectured on public law introduction at Kyunghee Cyber University, and lectured on Constitutional and Administrative Law at Hansung University. She is a senior researcher at Sungkyunkwan University Glocal Science and Technology Law. Institute.

E-mail address: ksimaro@naver.com