

사이버안보법제의 강화와 ‘사이버 아이언돔(가칭)’ 구축을 위한 제도화 방안 연구

A Study on the Enhancement of Cyber Security Legislation and the Institutionalization of the ‘Cyber Iron Dome’ Establishment

신유리*

Shin, YuLee

요약

본 논문에서는 전 세계적으로 사이버공간에서 발생하는 위협 등에 대한 대응으로 다각적인 방식에서의 사이버공간 내 행위에 대한 제재와 통제에 대한 법제변화에 대한 연구를 토대로 최근 사회주의체제 국가들에서의 적극적인 사이버공간 내 규제를 위한 입법동향을 비교·분석하고 있다. 더불어 현재 사이버안보법, 사이버기본법 등 사이버공간상 보안과 안보에 연계된 관련 입법안들이 사회적으로 논의가 지속되고 있는 상황에서 개인정보 등 헌법상 가치를 보호함과 동시에 국가차원의 사전적 방어를 위한 방안으로 ‘사이버 아이언돔(가칭)’ 구축과 이를 위한 제도화를 제안하고 있다.

Keywords : 사이버안보법, 사이버기본법, 사이버안보, 아이언돔, 사이버아이언돔, 네트워크안전법, 베트남 사이버보안법

1. 서론

최근 러시아의 우크라이나 침공에 대한 미국의 경제제재가 길어짐에 따라 러시아 지원을 받는 해킹조직이 러시아 경제제재에 동참한 미국 기업과 미국에 대해 보복성 사이버공격을 펼칠 것으로 우려되고 있다. 이에 러시아로부터 사이버공격을 받을 가능성이 있는 경로를 예의주시하면서 2022년 3월 15일 미국 조 바이든(Joe Biden) 대통령은 중요 인프라 기업에게 사이버 사건을 신고할 법적 의무를 부과하는 ‘2022년 미국 사이버보안 강화법’(Strengthening American Cybersecurity Act of 2022)에 서명하였다.¹⁾ 이전에는 지침 또는 가이드라인 형태로 기업·대학·연구소의 활동을 규율하였다면 우크라이나 사태를 계기로 사이버 위협이 증대되면서 미국은 주요 인프라 기업에 대해 해킹 또는 랜섬사고 발생 시 당국에의 보고 의무를 부과하고, 이를 이행하지 않을 때를 대비하여 법적 강제수단을 마련하는 등 미국을 포함하여 전 세계는 사이버보안과 관련하여 정보를 제한하고 강화하는 정책기조를 법제에서 분명하게 드러내고 있다.

2. 본론

사회주의체제 국가들의 경우 체제보호 및 선전과 관련하여 이를 보다 직접적으로 입법화하고 있다. 베트남『사이버보안법(Luật An ninh mạng)』은 2018년 6월 12일 제정, 2019년 1월 1일부터 시행되어 사이버공간에서의 국가보안보호 및 사회질서 안전의 보장활동, 관련 개인·기관·단체의 책임에 관하여 규정하고 있다. 베트남 입법부는 이 법이 사이버 공간상에서의 관계들을 조정함으로써 국가안보, 사회안전을 지키고, 개인과 단체의 합법적인 권리와 이익을 보호를 목적으로 하고 있으며²⁾ 사이버 공간에서의 베트남 사회주의 공화국에 대한 불온한 선전 정보, 사이버 공간상 폭동 유발이나 안보와 공공질서를 파괴할 수 있는 정보, 사이버 공간상 모욕·비방적인 정보, 사이버 공간상 경제관리질서를 위반하는 정보와 국민 사이에 혼란을 유발하고 사회경제적 활동을 손상시키며 정부 기관 또는 공무집행을 어려움 유발, 다른 기관·단체 및 개인의 정당한 권리와 이익을 침해하는 사이버 공간상 허위 및 거짓 정보 등을(제16조) 제재하기 위해 베트남 내 데이터를 보관하고(시행령 27조), 위의 정보들에 대해서는 24시간 이내 삭제하도록(제26조) 규정하고 있다. 중국 역시 마찬가지다. 2016년 11월 7일 제12기 전국 인민대표대회 상무위원회 제24차 회의에서 결의된 중국의『네트워크안전법(中华人民共和国网络安全法)』은 중화인민공화국 경내에서의 네트워크 구축, 운영, 유지 사용에 있어 보안의 관리, 감독은 이 법의 적용을 받도록 규정(제2조)하고 네트워크 안전에 해를 끼치는 정보로

* 정회원 · 동국대학교 경찰사법대학 연구교수 ssslch@daum.net

1) 정민정, “바이든 대통령의 ‘사이버보안 강화법’ 서명의 의미와 시사점”, 이슈와 논점, 제1937호, 국회입법조사처, 1면.

2) 한국인터넷진흥원, 「베트남 사이버보안법(Law on Cybersecurity)의 주요 내용 및 전망」, 2018, 214면.

국가의 안전과 영예, 이익에 해를 끼치고 국가의 정권과 사회주의 제도를 뒤엎도록 부추기며 나라를 분열시키고 국가의 통일을 파괴하도록 부추기며 테러리즘과 극단주의를 선양하고 민족원한을 부추기거나 폭력과 음란물의 유포, 허위정보를 날조하여 퍼뜨려 경제질서와 사회질서를 혼란에 빠지게 하거나 타인의 명예와 사생활과 지적재산권 및 기타 합법적 권익을 침해하는 활동을 네트워크 안보 침해행위로 규정하고(제39조) 이를 제재함으로써 적극적인 네트워크 통제에 나서고 있다. 그리고 이러한 중국의 사이버공간에 대한 입장은 향후 북한의 관련 사이버 법제정비에 있어서도 직접적으로 이러한 규정들을 수용하여 채택하는 방식으로 영향을 미칠 것으로 예측되고 있다.

3. 결론

중국이나 베트남과 우리는 다르다. ‘통제’와 ‘관리’ 이는 극히 제한적인 범위에서만 진행되어야 하며, 국민의 기본권을 침해해서는 안된다는 헌법적 가치가 훼손되어서는 안된다. 하지만 이제 현실세계와 사이버공간으로 대변되는 가상공간의 구분은 점점 희미해지고 있다. 문제는 한국의 기반시설도 랜섬웨어 공격으로부터 안전하지 않다는 것이다. 한국의 사이버보안 법체계는 미국식을 채택하고 있다. 우리 역시 사이버안보법, 사이버기본법 등 보안과 안보에 연계되어 관련 입법안들이 사회적으로 논의가 되고 있다. 개인정보보호와의 가치 충돌로 여전히 국회에서 통과되지 못하고 사회적 합의를 거치는 중이지만, 우리도 미국 바이든 행정부의 사이버안보 관련 입법 논의에 대한 분석을 보다 적극적으로 해나갈 필요가 있다. 이를 토대로 중요 인프라(반도체, IT 등) 기업의 사이버 사건의 경우 개별적인 보안시스템의 유무나 고도화 정도와 관계없이 강제적으로 사건을 신고하도록 법적 의무를 강제하게 하는 등 국가차원의 사전적 방어를 위한 ‘사이버 아이언돔(가칭)’ 등 관련 시스템 구축을 위한 제도화를 준비해나가야만 한다.

참고문헌

정민정 (2022), 바이든 대통령의 ‘사이버보안 강화법’ 서명의 의미와 시사점, 이슈와 논점, 제1937호, 국회입법조사처.