연구논문

독일의 사이버 보안법*
– 정책 · 거버넌스 · 법률 –

양 천 수**
김 중 길***

현대사회가 초연결사회로 접어들면서 새로운 법적 문제가 등장하고 있다. 사이버 보안에 관한 문제가 대표적인 예에 해당한다. 사이버 보안에 관해서는 다음과 같은 문제가 제기된다. 사이버 보안에 관한 통합법제가 필요한가, 사이버 보안에 관한 거버넌스를 어떻게 구축해야 하는가, 사이버 보안에 관한 정보공유를 어떻게 강화할 것인가, 사이버 보안을 위한 예방적 조치를 어떻게 마련할 것인가 등의 문제가 그것이다. 이에 관해서는 다양한 논의가 진행되고 있지만, 여전히 만족할 만한 해결책을 도출하지 못하고 있다. 이러한 상황에서 이 글은 우리 법에 많은 영향을 미친 독일이 사이버 보안에 관해 어떤 법정책을 추진하고 있는지 살펴본다. 이때 정책, 거버넌스, 법률에 중점을 둔다. 먼저 독일의 사이버 보안 전략을 살펴보고(II), 다음으로 사이버 보안에 관한 주요 조직을 분석한다(III). 여기서는 연방정보기술보안청과 연방망관리청이 주된 분석대상이 된다. 이어서 사이버 보안에 관한 법률의 최근 현황을 분석한다(IV). 여기서는 IT 보안법, NIS지침, 연방정보기술보안청법, 통신법, 텔레미디어법이 분석된다. 마지막으로 이러한 논의에서 우리의 사이버 보안 법정책에 관해 의미 있는 시사점을 도출한다(V). 이 글은 다음과 같은 시사점을 도출한다. 첫째, 독일은 사이버 보안을 전담하는 독자적인 거버넌스를 갖추고 있다. 연방정보기술보안청이 바로 그것이다. 둘째, 독일은 연방정보기술보안청에 사이버 보안에 관한 강력한 권한을 부여한다. 셋째, 독일은 사이버 보안을 위해 공적 영역과 사적 영역의 상호협력을 강화한다. 넷째, 사이버 보안을 위해 정보공유와 기술적 · 관리적 조치를 강화하고 있다.

주제어: 독일의 사이버 보안법, 연방정보기술보안청, 연방망관리청, 연방정보기술보안청법, IT 보안법, NIS지침

---

* 이 글은 필자들이 참여한 연구보고서 『안전한 지능정보사회 구축을 위한 정보보호 관련 법제도 개선방안 연구』, 과학기술정보통신부, 2018에서 필자들이 집필한 부분을 바탕으로 하여 이를 대폭 수정 및 보완한 것입니다.

** 영남대학교 법학전문대학원 교수·법학박사(yang1000soo@hanmail.net, 주저자)
*** 영남대학교 천마인재학부 강사·법학박사(kig0411@hanmail.net, 교신저자)

목 차

Ⅰ. 서론

현대사회가 이른바 '초연결사회'로 접어들면서 한편으로는 사회적 공리가 전체적으로 증대하면서도, 다른 한편으로는 새로운 법적 문제가 등장하고 있다.[1] 그 중에서도 가장 대표적인 문제로 '사이버 보안'(cyber security) 문제를 언급할 수 있다.

1) 이에 관해서는 우선 양천수, "현대 초연결사회와 새로운 인격권 보호체계", 『영남법학』 제43집, 영남대학교 법학연구소, 2016, 209-239쪽 참고.

특히 '사물인터넷'(IoT) 등으로 사회의 거의 모든 영역이 서로 연결되면서 사이버 보안이 침해될 위험성이 그만큼 증가하고 있다. 이에 따라 어떻게 하면 현대 초연결사회에서 사이버 보안 문제에 적절하게 대응할 수 있는지가 현대사회의 중요한 법적 문제로 대두하고 있다.

사이버 보안에 관해서는 구체적으로 다음과 같은 문제가 제기된다.[2] 첫째, 사이버 보안의 영어 원어인 'cyber security'를 어떻게 우리말로 개념화할 것인지가 문제된다.[3] 이에 관해서는 '사이버 보안', '사이버 안보'라는 개념이 제시된다. 이외에도 사이버 보안을 포괄하는 개념인 'information security'를 전제로 하여 '정보보안'이나 '정보보호'라는 개념을 사용하기도 한다. 현재 우리 정보보호 관련 법제는 '정보보호'를 실정법상 개념으로 사용한다.[4] 이 문제는 'cyber security'나 'information security'를 어떤 관점과 목적에서 접근하는가에 따라 달라진다.[5] 다만 오늘날과 같은 초연결사회에서 이러한 개념 논쟁이 과연 실제적인 의미를 가질까 의문이 들기도 한다. 사이버 침해가 실제로 어떤 유형인지에 상관없이 일단 그것이 발생하면 결과적으로 큰 피해를 야기할 것이기 때문이다. 그래서 더욱 중요한 문제는 사이버 보안을 어떻게 개념화할 것인가 하는 점보다는 어떻게 이에 대처하고 예방할 것인가 하는 점일 것이다.

둘째, 현재 우리는 사이버 보안에 관해 통합적인 법제를 갖추고 있지 않은데, 오늘날 발생하는 사이버 보안 침해행위에 적절하게 대응하기 위해서는 통합적인 법제를 구축해야 할 필요가 있을 것인지가 문제된다. 이를테면 우리는 사이버 보안 침해에 대응하기 위해 「국가사이버안전관리규정」, 「정보통신기반 보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등을 구축하고 있는데, 현대 초연결사회에서 사이버 보안 문제에 성공적으로 대응하기 위해서는 통합적인 「사이버 보안법」 또는 「통합정보보호법」이 필요한지, 아니면 현재처럼 복수의 개별법을 통해 사이버 보안 문제에 대응하는 것이 바람직한지가 문제된다.[6] 참고로 최근에는 이에 더하여 「정보통신안전법」 제정이 논의되기 시작하였다.[7]

---

2) 이를 분석하는 김재광, "사이버안보 위협에 대한 법제적 대응방안", 『법학논고』 제58집, 경북대학교 법학연구원, 2017, 145-177쪽 참고.

3) 이 문제에 관해서는 정필운, "사이버보안이란 개념 사용의 유용성 및 한계", 『연세 의료 · 과학기술과 법』 제2권제2호, 연세대학교 법학연구원 의료 · 과학기술과 법센터, 2011, 1-25쪽 참고.

4) 이를테면 「정보보호산업 진흥에 관한 법률」 등을 들 수 있다. 이 법률의 법명이 명시적으로 보여주는 것처럼, 우리 법체계는 '정보보호'라는 개념을 사용한다.

5) 이외에도 법이론적으로는 'security'와 'safety'가 개념적으로 구분되는가의 문제도 제기된다. 김대근, "안전 개념의 분화와 혼용에 대한 법체계의 대응방안", 『법과 사회』 제47호, 법과사회이론학회, 2014, 39-75쪽 참고.

6) 이에 관해서는 양천수, "제4차 산업혁명과 정보보호 법정책의 방향", 『공법학연구』 제18권제4호, 한국비교공법학회, 2017, 369-395쪽 참고.

7) 관계부처 합동, "통신재난 방지 및 통신망 안정성 강화 대책"(2018. 12. 27) 참고.

셋째, 위 두 번째 문제에 맞닿아 있는 것으로서 사이버 보안 문제에 적극 대처하기 위해서는 통합적인 거버넌스가 필요한지, 아니면 현재처럼 각 영역을 관할하는 거버넌스를 다원적으로 병존시킬 것인지가 문제된다.[8)]

넷째, 미국의 「사이버보안 정보공유법」이 시사하는 것처럼, 사이버 보안을 위해 어떻게 정보공유를 강화할 것인지가 문제된다.[9)] 가령 정보공유에 관한 독자적인 법령을 마련해야 할 필요가 있는지, 정보공유를 강제할 것인지, 아니면 이를 자율적으로 실행하도록 권고할 것인지가 문제된다. 오늘날 사이버 보안 침해행위가 기술적으로 고도화되고 있는 점을 고려하면, 침해행위가 발생하였을 때 비로소 이에 대응하는 것보다는 이를 사전에 예방하는 것이 더욱 중요하다. 그렇게 하기 위해서는 사이버 보안과 관련된 정보를 모든 국가기관뿐만 아니라 주요 민간기관이 공유할 수 있도록 해야 할 것이다. 그렇지만 현재는 정보공유에 대한 명확한 법정책적 방향이 설정되어 있지 않은 듯하다.[10)]

다섯째, 오늘날 발생하는 사이버 보안 침해행위에 적절하게 대처하기 위해서는 현재적 · 사후적 조치보다는 사전적 · 예방적 조치를 더욱 강화해야 할 필요가 있다. 그런데 이와 관련해서는 적법절차에 관한 문제, 개인정보침해에 관한 문제 등 다양한 문제가 대립적으로 관련을 맺고 있다. 이 때문에 현실적으로 이를 실행하는 것은 생각보다 쉽지 않다.

이외에도 사이버 보안에 관해 다양한 문제를 언급할 수 있을 것이다. 결국 현대 초연결사회에서 사이버 보안 문제에 성공적으로 대처할 수 있는가 하는 문제는 위에서 언급한 문제들을 얼마나 성공적으로 해결할 수 있는가에 달려 있다고 해도 과언이 아니다. 그렇지만 여러 이론적 · 현실적 여건으로 인해 아직까지는 만족할 만한 해결방안이 도출되고 있지 않다.

이러한 상황에서 이 글은 비교법적 연구의 일환으로 현재 독일이 사이버 보안에 관해 어떤 법정책을 펼치고 있는지 분석하고자 한다. 구체적으로 사이버 보안에 관해 어떤 전략을 마련하고 있는지, 이를 실행하기 위해 어떤 거버넌스를 갖추고 있는지, 이를 법적으로 뒷받침하는 법률에는 무엇이 있는지 살펴보고자 한다. 이를 통해 우리의 사이버 보안 정책에 관해 의미 있는 몇 가지 시사점을 도출하고자 한다.

---

8) 이 문제에 관해서는 김병기, "정보보호 거버넌스 현황과 지능정보사회의 정보보호 거버넌스 개편 試論", 『행정법연구』 제51호, 행정법이론실무학회, 2017, 73-108쪽 참고.

9) 미국의 「사이버보안 정보공유법」에 관해서는 양천수 · 지유미, "미국 사이버보안법의 최근 동향: 「사이버보안 정보공유법」을 중심으로 하여", 『법제연구』 제54호, 한국법제연구원, 2018, 155-192쪽 참고.

10) 이에 관해서는 양천수, "정보보호를 위한 정보공유 법정책: 현황과 개선방안", 『인권이론과 실천』 제23호, 영남대학교 인권교육연구센터, 2018, 33-47쪽 참고.

II. 독일의 사이버 보안 관련 정책 방향

먼저 논의의 출발점으로서 독일이 사이버 보안에 관한 어떤 정책을 마련 및 추진하고 있는지 살펴본다. 여기에서는 크게 네 가지를 언급하고자 한다. '독일을 위한 사이버 보안전략 2016', '디지털 아젠다 2014-2017', '디지털 전략 2025', '「네트워크 및 정보보안 지침」의 독일법 전환'이 그것이다.

1. 독일을 위한 사이버 보안전략 2016

2000년대 이후 '정보화 사회'(information society)가 대두하면서 정보보호에 대한 중요성이 높아졌고, 이에 독일 연방정부는 물리적 주요기반시설 외에 사이버 공간에 대한 보안정책도 마련하여 발전시켜왔다.[11] 그 첫 단계에 해당하는 정책으로 2011년 2월 '독일 연방내무부'(Bundesministerium des Innern: BMI)는 '독일을 위한 사이버 보안전략'(Cyber-Sicherheitsstrategie für Deutschland)을 발표한 바 있다.[12] 이 보안전략은 미래지향적인 사이버 보안정책에 관한 주요 결정사항을 포함하고 있는데, 2016년 11월 새로운 내용으로 업데이트되었다.[13] 이러한 업데이트에서는 크게 두 가지 특징을 읽어낼 수 있다. 먼저 종래의 IT 시스템 및 시설 등 '하드웨어 중심의 보호조치'에서 IT 보호대상의 주체가 되는 '개인 및 기업 중심의 보호조치'로 기조가 변화했다는 것이다. 말하자면 인터넷에 참여하는 참여자의 측면을 강화한 것이다. 다음으로 사이버 공간에서 진행되는 점진적 변화에 따라 등장하는 새로운 사이버 위협 및 공격에 대응하기 위해 보안전략을 마련했다는 것이다.

2016년의 새로운 사이버 보안전략은 다음과 같이 4대 활동 영역을 중심으로 하여 구성된다. 첫째, 디지털 환경에서 안전하고 독립적으로 행동할 수 있도록 하는 것으로 이

11) 독일의 사이버 보안정책 및 문제에 관해서는 우선 Hans-Jürgen Lange/Astrid Bötticher (Hrsg.), *Cyber-Sicherheit*, Springer VS, 2014 참고. 사이버 보안에 관한 기본권적 문제, 특히 '기본권으로서 안전권' 문제에 관해서는 Sebastian Leuschner, *Sicherheit als Grundsatz: Eine grundrechtsdogmatische Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit*, Tübingen, 2018 참고.

12) 이는 '독일 연방정보기술보안청'(Bundesamt für Sicherheit in der Informationstechnik)의 전자정부 및 IT에 의한 주요기반시설의 보호업무에 따라 마련된 2005년 '정보기반시설의 보호를 위한 국가계획'(Nationaler Plan zum Schutz der Informationsinfrastrukturen)을 대체하는 정책이다. 이러한 '독일을 위한 사이버 보안전략'을 소개하는 문헌으로는 Alexander Silhavy, *Cyber-Sicherheitsstrategie für Deutschland: Neue Bedrohungen? Neue Lösungen?*, Norderstedt, 2013 참고.

13) Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016, 2016, S. 3 ff. '독일을 위한 사이버 보안전략' 홈페이지 (http://www.bmi.bund.de/cybersicherheitsstrategie/)에서 그 자료를 확인할 수 있다.

는 사이버 보안의 핵심초석이 된다. 시민은 정보기술을 사용하면서 기회와 위험을 이해하고 평가하며 행동할 수 있는 위치에 있어야 한다. 이를 위해서는 신뢰 가능한 기술 및 '프레임워크'(framework)와 같은 조건이 필요하다. 둘째, 높은 수준의 사이버 보안을 위해서는 국가와 경제 간에 신뢰 있는 협력과 긴밀한 교류를 해야 할 필요가 있다. '협력적 접근'이라는 의미에서 새로운 길을 찾아야 한다. 셋째, 국가는 사이버 공간을 포함하여 안보, 정의, 자유를 보장해야 한다. 이를 위해서는 연방 차원의 효율적이고 지속가능한 국가 사이버 보안아키텍처가 필요하다. 넷째, 디지털화된 세계에서 이루어지는 다국적 네트워킹을 고려하여 유럽 및 국제 사이버 보안정책을 마련할 때 독일이 적극적인 역할을 해야 한다는 것이다. 각 활동 영역의 조치는 개괄적 성질을 지니며, 사회의 모든 영역에 영향을 미친다. 각각의 활동 영역에 대한 세부 전략은 아래 <표 1>과 같다.

<표 1> 독일을 위한 사이버 보안전략의 세부내용

활동 영역	세부 전략
디지털 환경에서 안전하고 독립적인 행동	- 모든 사용자들의 디지털 역량 제고 - 디지털 부주의에 대응 - 안전한 전자 통신과 웹사이트를 위한 조건 생성 - 안전한 전자 신원증명 - 인증 및 허가 강화: IT 보안 품질보증 도입 - 안전한 디지털화 형성 - IT 보안 연구 추진
국가와 경제 간의 협력	- 주요기반시설 안전조치 - 독일 내 기업 보호 - 독일 IT 경제 강화 - 제공자와 협력 - IT 보안서비스 제공자 고려 - 신뢰할 수 있는 정보교환플랫폼 구축
효율적이고 지속가능한 국가 사이버 보안아키텍처	- 국가사이버방어센터의 발전 - 분석 및 대응을 위한 현장능력 강화 - 사이버 공간에서 형사처벌 강화 - 사이버 스파이/사보타지(sabotage)의 효과적 퇴치 - 해외 사이버 공격에 대한 조기경보시스템 - 보안영역 중앙정보기술기관(ZITiS) 설립 - 사이버 보안의 국방 측면 강화 - 독일의 컴퓨터긴급대응팀(CERT) 구조 강화 - 연방행정의 안전 확보 - 연방정부와 주정부 간의 긴밀한 협력 - 자원 활용, 인력 확보 및 개발
유럽 및 국제 사이버 보안정책에서 독일의 적극적 역할	- 효과적인 유럽 사이버 보안정책을 적극 수립 - NATO의 사이버 방위정책 발전 - 사이버 보안을 위한 국제전선 적극 형성 - 사이버 역량 구축을 위한 양자 간 및 지역별 지원 및 협력 - 국제적 형사처벌 강화

※ 자료: Cyber-Sicherheitsstrategie für Deutschland 2016.

2. 디지털 아젠다 2014-2017

두 번째로 '디지털 아젠다 2014-2017'(Digitale Agenda 2014-2017)을 언급할 필요가 있다.[14] 다만 여기서 주의해야 할 점은, '독일을 위한 사이버 보안 전략 2016'이 사이버 보안을 정면으로 다루는 전략으로서 연방내무부가 마련한 것이라면, '디지털 아젠다 2014-2017'은 사이버 보안을 직접적인 대상으로 하기보다는 이를 포괄하는 '디지털 경제'를 활성화시키는 것을 주된 목표로 삼고 있다는 것이다. 달리 말하면, '디지털 아젠다 2014-2017'은 'ICT 정책을 위한 프레임워크(Framework)'에 해당한다. 이를 증명하듯 '디지털 아젠다 2014-2017'은 연방내부무가 아닌 '연방경제에너지부'(Bundesministerium für Wirtschaft und Energie)가 2014년 8월에 발표하였다. 물론 여기에는 사이버 보안에 관한 내용 역시 포함되어 있다. 이를테면 독일 연방정부는 디지털 커뮤니케이션, 전자거래 등 IT 시스템을 기반으로 하는 비즈니스 모델을 성공시키기 위해서는 IT 보안문제 해결이 필수적이라는 점을 인식하였고, 이를 달성하기 위해 독일 정부는 사이버 보안 규제 강화, 전자상거래 등 비즈니스 섹터 감시 강화, 데이터 보호, IT 보안체계 확립 등 IT 보안수위를 높이는 데 주력해왔다.[15]

3. 디지털 전략 2025

세 번째로 독일 연방경제에너지부가 2016년 4월에 발표한 '디지털 전략 2025'(Digitale Strategie 2025)를 들 수 있다.[16] 이는 '디지털 아젠다 2014-2017'을 보완하기 위해 제시된 것이다. 독일 연방정부는 특히 '디지털 아젠다 2014-2017'에서 강조한 'Industrie 4.0'이 중소기업 차원에서는 제대로 실현되지 못하고 있다는 점을 고려하여 이를 보완하기 위해 새롭게 '디지털 전략 2025'를 마련한 것이다.[17] 그 점에서 '디지털 전략 2025' 역시 사이버 보안을 정면에서 다루고 있는 것

14) 이에 관한 보다 자세한 내용은 독일연방정부 디지털 아젠다 홈페이지 (https://www.digitale-agenda.de/Webs/DA/DE/Home/home_node.html) 참고.

15) 코트라 해외시장뉴스, "독일, IT · 통신분야 보안정책 강력 추진", 2015. 7. 29. (https://news.kotra.or.kr/user/globalBbs/kotranews/5/globalBbsDataView.do?setIdx=244&dataIdx=153603).

16) 이에 관한 구체적인 내용은 (https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-strategie-2025.pdf?__blob=publicationFile&v=8)에서 확인할 수 있다. 이를 소개하는 국내 문헌으로는 한국정보화진흥원, NIA Hot Issue Report 2017-13: 2016년 다포스포럼 4차 산업혁명 발표 전후 주요국 국가정보화 전략 분석 및 시사점, 2017 참고.

17) 'Industrie 4.0'에 관해서는 Thomas Schulz (Hrsg.), *Industrie 4.0: Potenziale erkennen und*

은 아니다. 다만 '디지털 아젠다 2014-2017'처럼 '디지털 전략 2025'도 사이버 보안 강화에 관한 내용을 담고 있다. 이와 더불어 '개인정보 자기통제권'에 관한 내용도 담고 있다.

4. 「네트워크 및 정보보안 지침」의 독일법 전환

마지막으로 유럽연합 지침인 「네트워크 및 정보보안 지침」을 독일법으로 전환한 것을 들 수 있다. 2013년 12월 EU집행위원회는 EU회원국에 공통적으로 적용되는 사이버 보안 규범 마련을 지원하기 위해 보안조치를 실행하도록 의무화하고 그 기준을 제시하는 「네트워크 및 정보보안 지침」(Directive on Network and Information Security, 이하 'NIS지침'이라고 함)을 발표하였다. 2014년 3월 EU의회에서 동 지침 초안을 채택하였으며, 2016년 5월 EU이사회가 이를 승인하고, 같은 해 7월 EU의회가 이를 최종적으로 통과시킴으로써 같은 해 8월부터 발효되었다.[18]

NIS지침은 사이버 보안과 관련하여 EU 전체에 적용되는 최초의 법적 규범으로, 국가 네트워크 정보보안 체계, 관할기관 간 협력, 공공행정 및 기업의 정보보안 등의 내용으로 구성되어 있으며, 이에 관한 국가 및 민간기업 그리고 국가 간의 의무 등을 모두 규정하고 있다.[19] 또한 NIS지침은 EU회원국 내 컴퓨터 긴급대응팀(CERT-EU) 설치, 회원국 간 사이버 보안 정보공유 체계 구축, 주요 사업자들에 대한 보안요건 준수의무 부과 등을 명시함으로써 실질적인 보안강화 요건을 제시하고 있다.[20] 한 국가의 디지털 정보 시스템에서 야기되는 혼란은 국경을 넘어 다른 국가 및 EU 전체에 영향을 줄 수 있기에 이에 대응하기 위한 조치가 필요한 것이다.

NIS지침이 특징적인 것은 국가 및 행정기관 관계자뿐만 아니라 전자상거래, 소셜 네트워크, 통신 사업자 등 주요 인프라 서비스 운영자 및 교통, 금융, 보건의료 등 일반적인 서비스 제공자에게도 의무를 부과함으로써 디지털 환경을 보장하고자 한다는 점이다. 이러한 NIS지침은 EU회원국에게 다음과 같은 점을 요구하였다. 먼저

---

umsetzen, Vogel Business Media, 2017 참고.

18) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, COM(2013) 48 final-2013/0027(COD).

19) 네트워크 및 정보보안 지침의 주요내용은 양천수 외, 사이버 보안 강화를 위한 정보통신망법 체계 개선방안 연구, 미래창조과학부, 2015, 210쪽 아래 참고.

20) COM(2013) 48 final-2013/0027(COD), p. 2; 배병환 · 송은지, "주요국 사이버 보안 전략 비교 · 분석 및 시사점: 미국, EU, 영국의 사이버 보안 전략을 중심으로", 『정보통신방송정책』 제26권 21호, 정보통신정책연구원, 2014, 6쪽.

EU회원국은 2017년 상반기 중으로 동 지침을 채택해야 한다. 다음으로 사이버 보안에 대한 위험과 침해사고를 방지하고 대응하며 이를 관리하기 위해 상당한 인적·물적 자원을 승인할 수 있는 국가별 네트워크 및 정보보안 관할기관을 지정해야 한다. 나아가 EU회원국과 유럽집행위원회 간의 협력체계를 구축하기 위해 보안체계와 협력하고, 정기적인 상원의원 재검토를 통하여 위험과 침해사고에 대한 조기경보를 확보해야 한다. 그 밖에 금융, 교통, 에너지, 보건 등 중요 분야의 인프라, 앱스토어, 전자 상거래 플랫폼, 인터넷 결제, 클라우드 컴퓨팅, 검색 엔진, 소셜 미디어 등 정보사회 서비스 제공자 및 공공 행정기관은 위험관리기법을 도입하고 핵심 서비스의 주요 보안사건을 보고해야 한다.

각 EU회원국은 21개월 안에 자국 국내법에 NIS지침의 내용을 반영한 후 6개월 안에 기반서비스 운영기관을 선정해야 했다.[21] 독일은 2017년 6월 29일 NIS지침을 자국법으로 전환하는 법률을 공포하였다.[22] 동 법률은 독일의 사이버 보안 관련 주요 조직의 새로운 업무를 규율하고, 사이버 보안 관련 법률의 개정내용을 담고 있다.[23] 이에 관해서 아래 III.에서 구체적으로 살펴보기로 한다.

III. 독일의 사이버 보안 관련 주요 조직

독일에서 사이버 보안은 연방정부 차원에서 수행해야 하는 중요한 업무로 이해된다. 이러한 이유에서 사이버 보안은 독일 연방내무부를 중심으로 하여 경제에너지부, 교육연구부, 국방부 등이 분담하고 있다. 각 주(州)의 자치단체는 각자의 관할 영역에

21) 글로벌 과학기술정책정보 서비스, 해외정책동향, 2016. 8. 1. (http://www.now.go.kr/ur/poliTrnd/UrPoliTrndSelect.do?screenType=V&poliTrndId=TRND0000000000029617&pageType=008&currentHeadMenu=1&currentMenu=12).

22) 한편 영국은 "NIS 규정"(The Network and Information Systems Regulations 2018, Electronic Communications, 2018 No. 506)을 2018년 5월 10일 발효하였으며 (https://www.legislation.gov.uk/uksi/2018/506/made), 프랑스는 총리실 주도 아래 "French National Digital Security Strategy 2015" 및 "Digital France 2020" 전략을 세우고 이러한 지침의 내용을 디지털공화국법, 군사계획법, 정보처리법 등에 반영하였다. 그러나 벨기에, 스페인, 포르투갈, 덴마크, 스웨덴, 네덜란드 등은 자국법 전환 기간 안에 자국법 전환을 마무리 짓지 못한 상황이다. 각국이 처한 상황에 따라 동지침의 내용을 반영한 사이버 보안 관련 법제를 구축 및 운용해갈 것으로 예상된다.

23) Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewähr - leistung eines hohen gemeinsamen Sicherheits - niveaus von Netz- und Informations - systemen in der Union (ABl. L 194 vom 19. Juli 2016, S. 1).

서 사이버 보안을 책임진다. 독일 연방정부는 특히 사이버 보안을 전담하는 기관으로서 '연방정보기술보안청'과 '연방망관리청'을 설치하고 있는데, 이들 조직을 규율하기 위한 법률을 독자적으로 마련하고 있다. 아래에서는 이 두 조직을 중심으로 하여 살펴본다.

1. 연방정보기술보안청

(1) 의의 및 연혁

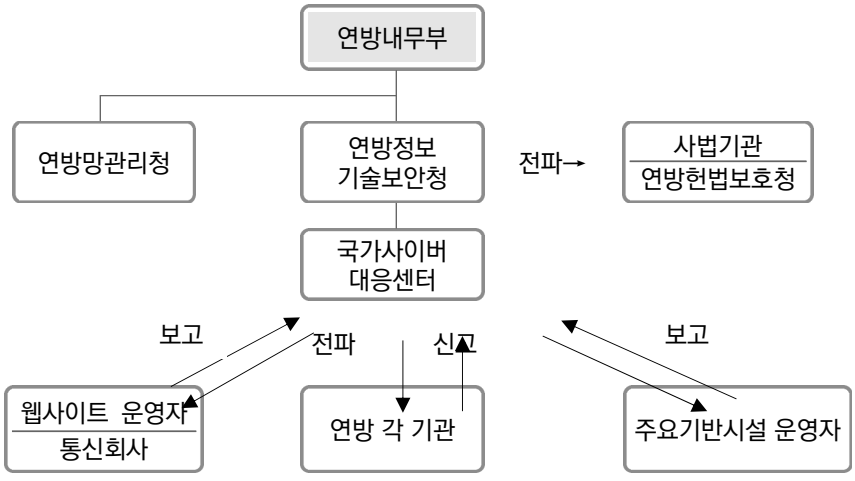
1991년 1월 1일에 설립된 '독일 연방정보기술보안청'(Bundesamt für Sicherheit in der Informationstechnik: BSI)은 독일 연방내무부 산하의 국가기관으로서, 정보화 사회에서 등장하는 컴퓨터 및 통신 등 IT 보안 관리에 관한 문제를 다루는 독립적·중립적인 연방상급기관이다.[24] 구성원은 컴퓨터과학자, 물리학자, 수학자 등 다양한 분야의 전공자를 포괄한다. 현재 700명이 넘는 인원이 근무하고 있고, 본(Bonn)에 본사를 두고 있다. 연방정보기술보안청은 유럽연합 차원에서 IT 보안 문제를 담당하는 '유럽 네트워크·정보보안청'(European Network and Information Security Agency: ENISA)이 설립되는 데 표본이 되기도 하였다.

연방정보기술보안청은 1957년에 설립된 연방정보부 소속의 '중앙암호제도실'(Zentralstelle für das Chiffrierwesen: ZfCH)에서 출발한다. 중앙암호제도실은 연방행정 정보의 안정성과 고유직무, 국외 비밀정보를 수집하고 분석하는 업무를 수행하였다. 1980년대 중반 이후 컴퓨터 기술이 급속하게 발전하면서 컴퓨터의 안전성과 관련한 업무로 범위를 확대하여 1989년에 '중앙정보기술안전실'로 명칭을 변경하고 정보기술의 사법적 적용 및 안전성 업무까지 담당하게 되었다.[25] 이후 1991년 시행된 「연방정보기술보안청 설립에 관한 법률」에 따라 연방내무부 산하의 연방상급관청으로서 현재까지 기능하고 있다.

---

24) 연방정보기술보안청은 연구기관으로서 다양한 연구물을 간행하기도 한다. 이에 관해서는 BSI, *IT-Grundschutz Arbeitshandbuch: DIN ISO/IEC 27001, DIN ISO/IEC 27002*, Bonn, 2017; BSI, *IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung: Tagungsband zum 16. IT-Sicherheitskongress des BSI*, Bonn, 2019; BSI, *Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis: Tagungsband des 15. Deutschen IT-Sicherheitskongresses des BSI*, Bonn, 2017 등 참고.

25) 권현준 외, 『사이버 보안법제 선진화 방안 연구』, 방송통신위원회, 2011, 68쪽 아래 참고.



[그림 1] 독일의 정보보안 및 공유 기관 체계

(2) 기능

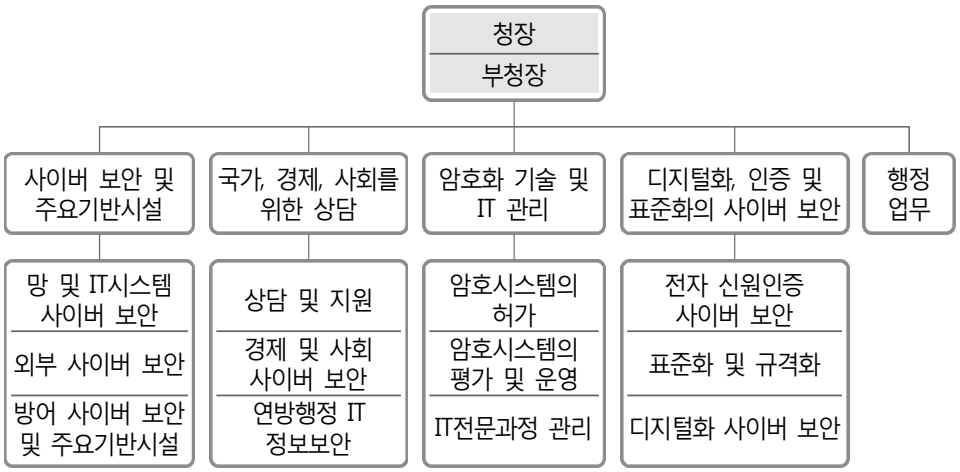
연방정보기술보안청의 핵심과제는 정부 네트워크를 보호하는 것으로 기술적 업무뿐만 아니라 사법적 임무수행 지원, 테러정보 수집 및 평가, 정보보안 관련 자문 등 광범위한 사이버 보안업무를 총괄 · 집행하고 있다.[26] 구체적으로 IT 제품 및 서비스의 검사 및 인증, IT 제품 및 서비스의 유해프로그램 또는 보안결함에 대한 경고, 연방정부 및 기타 그룹을 위한 IT 보안 컨설팅, IT 보안 및 인터넷 보안에 대한 시민의 정보 및 인식 제고, 통일적이고 구속력 있는 IT 보안표준 개발, 연방정부 IT를 위한 암호 시스템 개발, 연방정부의 정보보고기관 및 주요기반시설의 정보기술보안센터 등과 같은 역할을 수행한다.

(3) 조직

현재 연방정보기술보안청은 아래 [그림 2]가 보여주는 것처럼 5개의 국(Abteilung)으로 구성된다. 첫째, '사이버 보안 및 주요기반시설국'(Abteilung CK), 둘째, '국가 · 경제 · 사회를 위한 상담국'(Abteilung B), 셋째, '증가하는 보안수요를 위한 암호화 기술 및 IT 관리국'(Abteilung KT), 넷째, '디지털화, 인증 및 표준화의 사이버

26) 김상배, "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각", 『국제지역연구』 제26권제3호, 서울대학교 국제학연구소, 2017, 97쪽. 우리나라 조직으로서는 그나마 '한국인터넷진흥원'이 이와 유사한 기능을 수행한다고 말할 수 있다. 그러나 한국인터넷진흥원은 행정안전부 소속이 아닌 과학기술정보통신부 소속으로 되어 있다. 행정안전부 소속의 조직으로는 '한국정보화진흥원'을 들 수 있다.

보안국'(Abteilung D), 다섯째, 행정업무를 담당하는 '행정업무국'(Abteilung Z)이 그것이다. 행정업무국을 제외한 각 국은 각각 세 개의 부(총 12개)로 구성되며, 국 및 부 아래에 다섯 내지 여섯 개의 과(총 145개)가 배치된다.[27]



※ 자료: 연방정보기술보안청 홈페이지(2019년 1월 현재)

[그림 2] 독일 연방정보기술보안청의 조직도(국, 부)

2. 연방망관리청

(1) 의의 및 연혁

연방정보기술보안청 외에 독일의 정보보호 관련 기관으로는 전기통신망과 관련된 업무를 담당하는 '연방망관리청'(Bundesnetzagentur: BNetzA)이 있다.[28] 통신소비자를 보호하는 데 주된 목적이 있으며, 주로 통신서비스 제공자의 변경, 통신업체 간의 분쟁 해결, 전화 남용 내지 광고 등 불법행위의 차단, 전파간섭의 방지, 특정 무선시스템으로부터 안전유지와 같은 업무를 수행한다. 연방망관리청은 통신 외에도 전기 및 가스, 우편, 철도 관련 '망' 업무를 통합적으로 관리하는 규제행정청의 기능을 수행한다.[29]

27) 더욱 자세한 조직도는 연방정보기술보안청 홈페이지 참고 (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/BSI/Organisationsplan_IFG_pdf.pdf?__blob=publicationFile&v=11).

28) 이를 소개하는 문헌으로는 Marcus Lobedann, *Die neue Rolle der Bundesnetzagentur*, Norderstedt, 2012 참고.

29) 이는 연방망관리청의 정식명칭이 '연방전기 · 가스 · 전기통신 · 우편 · 철도망청'(Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn)에서도 확인할 수 있다. 우리나라

연방망관리청의 전신은 경제 분야, 특히 통신 및 우편의 총괄 관리를 위해 1996년에 설립된 '통신우편관리청'(Regulierungsbehörde für Telekommunikation und Post: RegTP)이다. '통신우편관리청'이 연방망관리청으로 확대 개편된 것이다. 이렇게 관할범위가 확장된 배경에는 모든 시장에서 기회 균등한 경쟁기능을 담보하기 위해 민영화 추진경과의 실효성 확보 차원에서 연방망관리청이 자신이 관할하는 사무영역에 대해 직접 고권적 규제를 할 필요가 있다는 입법자의 강한 요청이 있었다.[30]

(2) 사무와 권능

연방망관리청의 사무와 권능은 '각 직무에 관련된 법적 근거'에서 도출된다. 연방망관리청이 설립되었다고 해서 통신 분야의 규제에 대해 특별히 달리 적용되는 사항은 없으며, 다만 기존의 '통신우편관리청'에서 '연방망관리청'으로 그 명칭이 변경된 것 정도만이 문제될 뿐이었다.[31] 연방망관리청이 설치되면서 신설된 「통신법」(Telekommunikationsgesetz: TKG) 제116조는 연방망관리청의 사무와 권능을 명확하게 규정하고 있다.[32] 이에 따르면, "연방전기 · 가스 · 통신 · 우편 · 철도망청은 이 법률 소정의 규제행정청이며, 이 법률에 따라 동 규제행정청에 속한 사무와 권능을 수행한다." 이에 관해서는 전신인 통신우편규제청과 비교할 때 '행정조직체계'를 변경한 정도에 그쳤다는 평가가 일반적이다.

(3) 조직구성

2019년 1월 현재 연방망관리청은 '중앙국'(Abteilung Z), '정보기술 및 보안'(Abteilung IS), '통신규제의 경제문제'(Abteilung 1), '통신 및 주파수 규제의 법률문제'(Abteilung 2), '국제 업무 및 우편 규제'(Abteilung 3), '통신에 대한 기술적 규제'(Abteilung 4), '섭외 및 전화번호오용'(Abteilung 5), '에너지 규제'(Abteilung

---

에는 이러한 연방망관리청과 같은 국가조직이 없다. 방송통신 영역에서 이와 유사한 기능을 수행하는 조직으로서 '방송통신위원회'가 있을 뿐이다.

30) 정보통신 영역에서 중요한 규제 및 경영판단의 자본시장지향적 평가에 대해서는 Lutz Johanning/Ernst-Olav Ruhle, "Sind Regulierungsbehörden die besseren Manager? Eine kapitalmarktorientierte Bewertung von wichtigen Regulierungs- und Managemententscheidungen", in: *K&R* (2003), S. 369 ff.

31) 신봉기, "독일 연방통신망청에 관한 연구: 망(網) 관련 통합 규제관청으로서의 지위와 절차를 중심으로", 『공법연구』 제35권제3호, 한국공법학회, 2007, 342쪽.

32) 독일 통신법에 관해서는 류지태 외, 독일 통신법, 법원사, 2007 참고.

6), '철도 규제'(Abteilung 7), '망 확장'(Abteilung 8)과 같은 10개의 국(Abteilung)으로 조직되어 있으며, 국 아래 각각 세부조직으로 소속되어 있다.[33]

그리고 연방망관리청에 소속된 이른바 결정위원회(Beschlußkammern)가 있으며, '행정행위'의 형식으로 행정절차 영역에서 제반 결정(Entscheidungen)을 한다. 결정위원회는 2019년 1월 현재 11개가 있으며, 각 담당영역은 다음과 같다. '의장단위원회'(BK 1), '통신소비자시장, 유무선통신, 참여자정보, 요금징수 등 규제'(BK 2), '통신 사전급부 시장, 유무선통신 규제'(BK 3), '신재생에너지 분담금, 투자조치, 망이용 등 규제'(BK 4), '우편시장에서 비용규제 및 특별 권한남용감독'(BK 5), '전력망 규제'(BK 6), '가스망 규제'(BK 7), '전력망 비용규제'(BK 8), '가스망 비용규제'(BK 9), '철도'(BK 10), '국제분쟁조정기관'(BK 11)이 그것이다. 이외에도 연방하원과 연방상원에 소속된 위원으로 구성되는 자문위원회(Beirat) 및 결정의 준비 및 규제에 관해 전문적인 자문을 담당하는 학술위원회를 두고 있다.

Ⅳ. 독일의 사이버 보안 관련 법률의 최근 동향

1. 「정보기술 시스템 보안 증진에 관한 법률」 제정

(1) 제정배경 및 의의

독일 연방정부는 2015년 7월부터 「정보기술 시스템 보안 증진에 관한 법률」(이하 'IT 보안법'이라고 함)을 시행하고 있다.[34] 2014년 7월 독일 연방내무부는 내각 합의를 거쳐 「IT 보안법 초안」을 작성해 의회에 상정하였다. 이는 2015년 6월 12일 독일 연방의회(Bundestag)를 통과하였고, 같은 해 7월 10일 연방참사원(Bundesrat)에서도 통과되어 7월 25일부터 발효되었다. 동법은 이른바 '조항법률' (Artikelgesetz)로서,[35] IT 보안과 관련하여 독일의 연방정보기술보안청 설치법, 에너지관리법, 텔

33) 더욱 자세한 조직도는 연방망관리청 홈페이지 참고 (https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/UeberdieAgentur/Organigramm/OrganigrammMitNamen.pdf?__blob=publicationFile&v=19).

34) Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015, Bundesgesetzblatt(BGBl) Jahrgang 2015 Teil I Nr. 31, ausgegeben am 24. 7. 2015, S. 1324.

35) 독일에서 '조항법률'(Artikelgesetz)은 동시에 여러 개의 법률을 변경하는 법률을 말하는데, 독일의 독특한 입법형식이라고 볼 수 있다. 이에 관해서는 우선 Thomas M. Lachner, *Das Artikelgesetz*, Berlin, 2007 참고.

레미디어법, 전기통신법, 연방범죄수사청법 등 관련 법률을 변경하고 보충하는 법률이다.[36] 독일에서 사이버 보안을 보장하기 위한 포괄적인 법적 틀을 처음으로 고안하고 시행한 것이다.

앞서 살펴본 것처럼, 독일은 정보보호 정책 방안과 관련하여 2011년 초에 '독일을 위한 사이버 보안전략'을 구상함으로써 사이버 공간에서 더욱 강화된 보안정책의 기반을 마련한 바 있다. 그리고 이러한 보안전략의 목표는 2014년에 채택된 독일 연방정부의 '디지털 아젠다 2014-2017'을 통해 계속적으로 추구되었다. 이러한 정책방안의 흐름에 따라 IT 시스템 및 서비스의 보안강화 및 보호개선을 주요 목표로 하는 아젠다의 첫 번째 결과물로서 IT 보안법이 도출된 것이다.

(2) 목적 및 적용대상

IT 보안법은 독일의 IT 시스템과 디지털 인프라를 세계에서 가장 안전하게 조성하고자 하는 일환으로 시행되었다. 특히 전기, 수도, 의료, 금융, 교통, 식품 등과 연관된 사회의 '주요기반시설'(Kritische Infrastrukturen: KRITIS)은 이미 IT 분야와 결합되어 있고, 이러한 기반시설의 불안전성 내지 이용중단은 국가 경제 및 사회에 극심한 혼란을 초래할 수 있기에, IT 시스템의 안전과 가용성 확보는 주요 기반시설의 기능과 관련해서도 매우 중요한 역할을 한다. 독일 연방정부는 IT 시스템 또는 디지털 세계의 안전과 무결성에 대한 신뢰 없이는 경제적, 사회적 잠재력을 성장시킬 수 없다는 믿음을 바탕으로 하여 국가가 인터넷에서 발생하는 위험과 범죄를 효과적으로 방어할 책임을 지고 있다고 강조하였다.[37] IT 보안법의 주된 목적은 기업 및 연방행정의 IT 보안 수준을 향상시키고, 인터넷 안에서 시민을 더욱 효과적으로 보호하는 것이다. 따라서 IT 보안법의 주된 적용대상은 국가의 경제와 사회에 긴밀하게 연결된 주요기반시설을 관리하는 운영자 및 IT 시스템에 대해 더 높은 요구를 충족시켜야 하는 운영자로서 영리를 추구하는 웹사이트 운영자 등이다.

1) 주요기반시설 운영자

우선 주요기반시설 운영자에 대해 IT 보안법이 적용된다. 여기서 IT 보안법의 의미에서 볼 때 주요기반시설 운영자란 「주요기반시설 확정에 관한 규정」에 따라 사회

36) BSI, *Das IT-Sicherheitsgesetz*, Bonn, 2016, S. 5.
37) 김상배, 앞의 글, 96쪽.

구성원 다수에게 필수적인 서비스를 제공하는 단체 및 설비를 운영하는 자를 말한다.[38] 이에 해당하는 분야로는 에너지, 정보기술, 통신, 식품, 수도 분야뿐만 아니라 현재는 금융, 보험, 보건, 운송, 교통 분야까지도 언급할 수 있다.[39] 주요기반시설 운영자는 중요한 IT 서비스를 제공할 때 현재의 기술수준에 따라 적절하게 IT 보안 안전장치를 마련해야 한다. 이러한 안전성은 최소한 2년마다 검증되어야 한다. 또한 주요기반시설 운영자는 심각한 IT 보안 사고를 연방정보기술보안청에 보고해야 한다. 연방정보기술보안청은 이러한 보고내용과 다양한 기타 정보에서 획득한 인지정보를 모든 주요기반시설 운영자에게 제공함으로써 운영자의 IT 시스템을 적절하게 보호할 수 있도록 해야 한다.

2) 웹사이트 운영자

다음으로 웹사이트 운영자는 자신들의 웹사이트 고객 데이터와 웹사이트 운영에 필요한 IT 시스템을 보호하기 위해 기술적 조치 및 조직적 대책을 강구해야 한다. 이러한 조치는 충분히 보호되지 않은 웹서버를 통해 이루어지는 바이러스 프로그램의 확산을 방지하는 것을 목적으로 한다.

3) 통신회사

나아가 통신회사도 IT 보안법의 적용대상이 된다. 통신회사는 통신연결상 오용이 확인되는 경우 고객들에게 이를 고지하고 해결책을 제시해야 한다.

2. 연방정보기술보안청 관련 법률

한편 그 동안 통신회사를 감독하는 관청은 연방망관리청이었다. 여기에 IT 보안법의 목적을 실현하기 위해 연방정보기술보안청의 임무와 권한이 확대되었다. 아래에서는 IT 보안법에 따라 개정된 연방정보기술보안청 관련 법률의 주요내용을 살펴보기로 한다.

---

38) Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), die durch Artikel 1 der Verordnung vom 21. Juni 2017 (BGBl. I S. 1903) geändert worden ist.

39) 「주요기반시설 확정에 관한 규정」에는 운영자가 규율범위에 속하는지 여부를 확인할 수 있는 측정 가능하고 이해하기 쉬운 기준이 규정되어 있다. 적용범위는 각 분야의 각 자산 범주에 대한 임계값을 기준으로 결정된다. 표준 임계값은 500,000명의 사람을 돌보는 것이다. 연방정보기술보안청 홈페이지(https://www.bsi.bund.de/DE/Service/FAQ/IT-Sicherheitsgesetz/faq_node.html#faq6636762) 참고.

(1) 연방정보기술보안 강화를 위한 법률

연방정보기술보안청의 첫 번째 법적 근거는「연방정보기술보안청 설립에 관한 법률」이다.[40] 동법은 1991년 1월 1일부터 2009년 8월 19일까지 시행되었다. 동법은 평가 · 인증업무와 함께 정보통신기술 시스템의 연구개발, 정보통신 시스템 안전성 검사, 동 시스템과 내용심사를 통한 안전성 위험 조사, 평가서 및 인증서 발급, 정보통신 시스템의 허가를 비롯한 국가기관 및 민간기관에 대한 기술지원과 자문제공을 규정하고 있다.[41]

이후 2009년 8월 20일부터 발효된「연방정보기술보안 강화를 위한 법률」(이하 '연방정보기술보안청법'이라고 함)이 현재 적용되는 연방정보기술보안청의 법적 근거가 되고 있다.[42] 동법은 정보통신기술의 중요성이 점점 증대되는 현실에 대응하고, 그에 따른 새로운 위협에 대처하기 위해 연방정보기술보안청에 더욱 광범위한 책임과 권한을 부여하였다. 이에 관해서는 다음과 같은 사항을 언급할 수 있다.

우선 연방정보기술보안청법 제4조에 따르면, 연방정보기술보안청은 IT 보안에 대한 중앙신고기관으로서 정보기술 보안에 대한 새로운 침입방식과 보안결함에 대한 정보를 수집하고 이를 평가한다. 이로써 사이버 공간을 신뢰할 수 있는 상태로 만들어내고, 외부의 공격을 일찍 발견하여 이에 대한 대책을 취할 수 있는 것이다.

또한 연방정보기술보안청은 연방정보기술보안청법 제5조에 따라 프로토콜 데이터 및 연방통신기술 인터페이스에서 생성된 데이터를 수집, 평가, 저장, 사용 및 처리할 수 있는 권한을 갖게 되었다. 이를 통해 IT 공격 징후를 사전에 탐지하고 타겟 목표에 대처할 수 있게 되었다. 요컨대, 예방적 조치에 관한 권한을 강화한 것이다.

한편 연방정보기술보안청법 제7조에 따르면, 연방정보기술보안청은 정보기술 제품과 서비스의 안전성 결함, 바이러스 프로그램에 대한 정보내용 및 경고 메시지 등을 관련 기관이나 공중에 알려야 한다. 이때 우선적으로 사전에 제조자에게 알릴 의무가 있고, 이어서 공중에게 공개해야 한다.

그리고 연방정보기술보안청은 연방정보기술보안청법 제8조에 따라 연방행정에 대한 통일적이고 엄격한 보안표준을 정의하고, 필요한 경우에는 적절한 제품을 개발하거나 입찰을 제공할 수 있는 권한을 갖게 되었다. 이렇게 함으로써 적합하지 않은

40) Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Errichtungsgesetz) vom 17. Dezember 1990 (BGBl. I S. 2834), zuletzt geändert durch Artikel 11 der Verordnung vom 25. November 2003 (BGBl. I S. 2304).

41) 강석구 외, 사이버안전체계 구축에 관한 연구, 한국형사정책연구원, 2010, 190쪽.

42) Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821).

곳에 부적절한 제품이 사용되거나 조작된 IT 구성요소가 연방행정 및 정부망에서 사용되는 것을 방지할 수 있게 되었다.

(2) IT 보안법에 따라 개정된 연방정보기술보안청법

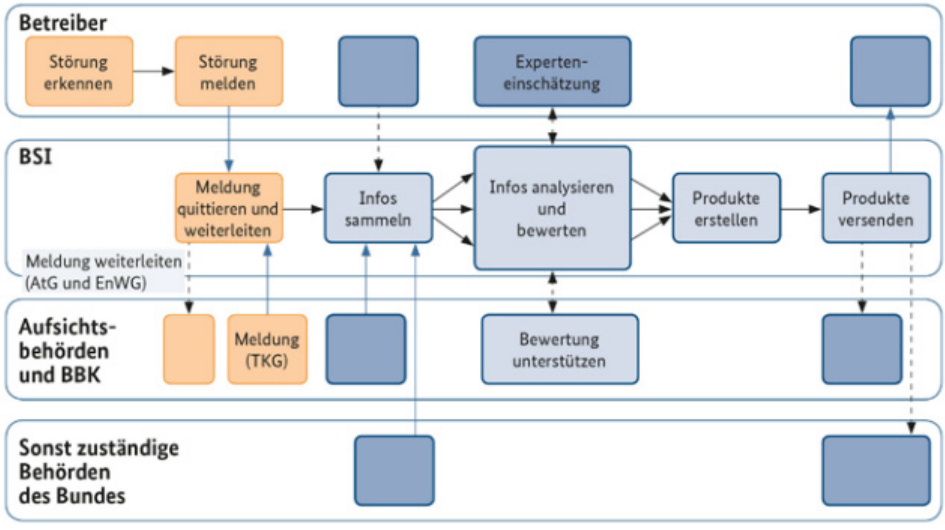
연방정보기술보안청법은 이후 몇 차례 변화를 겪어 오다가, 2015년 7월 25일에 발효된 IT 보안법이 적용되면서 사이버 보안에 관한 규율내용을 한층 강화하였다. 먼저 연방정보기술보안청법 제7조에 따라 연방정보기술보안청은 IT 제품의 안전성 결함 및 바이러스 프로그램에 대한 경고를 알리는 것 이외에도 데이터 손실 또는 데이터에 대한 무단 접근이 있었을 경우 이에 대한 경고를 발할 수 있게 되었다. 또한 연방정보기술보안청은 연방정보기술보안청법 제7조a에 따라 판매중이거나 판매 예정인 IT 제품 및 정보 시스템의 안전성을 검사할 수 있게 되었다. 이 경우 연방정보기술보안청은 검사를 제3자에게 위탁할 수 있다. 이로써 사이버 보안에 관한 연방정보기술보안청의 권한이 더욱 강화되었다.

그리고 연방정보기술보안청법 제8조a에 따르면, 주요기반시설 운영자는 정보 시스템의 오류를 방지하기 위해 현재의 기술수준을 준수하고 기술적 · 관리적 조치를 강구해야 한다. 주요기반시설 운영자는 이렇게 현재의 기술수준에 따라 IT 보안을 구현하는 대책을 강구하고 있음을 연방정보기술보안청에 정기적으로 보고해야 하고 2년마다 인증을 받아야 한다. 보안결함이 발견되는 경우에는 연방정보기술보안청은 감독당국과 합의하여 결함을 해결할 것을 명령할 수 있다.

연방정보기술보안청은 연방정보기술보안청법 제8조b에 따라 주요기반시설의 IT 보안을 실현하기 위한 중앙신고기관 역할도 담당한다. IT 보안에 관한 심각한 장애요소가 중요한 서비스의 가용성에 영향을 끼칠 수 있는 경우에는, 주요기반시설 운영자는 연방정보기술보안청에 당해 IT 장애사항을 신고해야 한다. 반대로 연방정보기술보안청은 주요기반시설의 IT 보안에 대한 공격을 방어하는 데 필요한 모든 관련 데이터를 수집 · 평가하고, 여기서 획득한 정보를 다른 주요기반시설 운영자와 관할당국 및 감독당국에 제공해야 한다. 말하자면 '정보공유'를 해야 하는 것이다. 그리고 IT 장애사항이 신고의무가 있는 주요기반시설 운영자에게 발생하는 경우에는 연방정보기술보안청은 연방정보기술보안청법 제8조b에 따라 필요한 경우 해당 IT 제품 및 정보 시스템의 제조자에게 협력하도록 요청할 수 있다.[43] 아래 [그림 3]

43) 다만 연방정보기술보안청법 제8조c에 따라 주요기반시설의 정보 시스템에 관한 규정은 종업원 10명 미만 및 연간 매출액이 200만 유로 미만의 기반시설 운영자에게는 적용되지 않는다. 또한 통신법, 에너지관리법, 원자력법 등 유사한 규정이 적용되는 운영자에게는 적용되지 않는다.

은 연방정보기술보안청법 제8조b가 규정하는 IT 보안정보 신고절차의 흐름을 보여준다.[44]



[그림 3] 연방정보기술보안청법 제8조b에 따른 IT 보안정보 신고절차

그밖에 연방정보기술보안청은 연방정보기술보안청법 제7조a에 따라 연방정보기술보안청법 제3조가 부여하는 임무를 수행하기 위해 보안과 관련한 IT 제품을 조사할 권한을 갖게 되었다. 더불어 연방행정망의 인터페이스 데이터와 프로토콜 데이터를 분석할 수 있도록 규정하는 연방정보기술보안청법 제5조에 따라 연방정보기술보안청의 권한은 확대되었다. 이에 따라 연방당국은 연방정보기술보안청의 임무를 지원해야 한다. 요컨대, 연방정보기술보안청은 사이버 보안에 관한 일체의 정보를 수

44) 이 자료는 BSI, *Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS*, Bonn, 2017, S. 25에서 인용하였다. 이 자료는 (https://www.bsi.bund.de/SharedDocs/ Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7)에서 확인할 수 있다. 한편 여기서 말하는 "UP KRITIS"는 "주요기반시설 운영자 및 그 연합체 그리고 관할 국가조직 사이에서 이루어지는 공적-사적 협력을 말한다." (Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen). BSI, a.a.O., S. 19 참고. 한편 위 그림에서 표시하는 'Betreiber'는 '주요기반시설 운영자'를, 'BSI'는 '연방정보기술보안청'을, 'Aufsichtsbehörden'는 '감독관청'을, 'BBK'는 '연방국민보호재난지원청'(Bundesamt für Bevölkerungsschutz und Katastrophenhilfe)을, 'Sonst zuständige Behörden des Bundes'는 '그 밖의 연방관할관청'을 뜻한다.

집 및 분석할 수 있는 권한을 확보한 것이다.

이외에도 연방정보기술보안청은 연방행정의 IT 보안을 강화하기 위해 연방행정 IT 부서의 최소기준을 개발해야 한다. 아울러 연방정보기술보안청은 연간백서 발행 등을 통해 IT 보안에 대한 현재의 위협을 시민에게 알리고, 시민이 IT 보안에 대한 인식을 높일 수 있도록 노력해야 한다.

(3) NIS지침에 따라 개정된 연방정보기술보안청법

연방정보기술보안청법은 최근 유럽연합이 마련한 NIS지침을 독일법으로 전환함으로써 한 차례 더 개정되었다. 무엇보다도 법률 명칭이 「연방정보기술보안청에 관한 법률」(이하 '개정 연방정보기술보안청법'이라고 함)로 변경되었으며,[45] 유럽연합 NIS지침의 내용이 다수 반영되었다.

우선 정보기술 시스템의 보안 및 기능성 복원에 관한 법적 임무를 부여하는 개정 연방정보기술보안청법 제5조a에 따라 연방정보기술보안청에 '모바일사고 대응팀'(Mobile Incident Response Teams: MIRTs)을 설치할 수 있는 법적 근거를 확보하였다.

다음으로 개정 연방정보기술보안청법은 제8조c에 따라 기존의 주요기반시설 운영자뿐만 아니라 독일에 있는 디지털 서비스 제공자, 독일 안에서 임명된 디지털 서비스 제공자 대표, 독일 안에서 디지털 서비스 제공을 위해 네트워크 및 정보 시스템을 운용하는 업체들까지 적용대상으로 삼게 되었다. 적용대상이 되는 주체가 확장된 것이다. 따라서 이들은 사이버 보안 요구사항이 포함된 디지털 서비스 의무를 준수해야 한다.

개정 연방정보기술보안청법은 2018년 5월 10일부터 시행되고 있다. 이에 따라 주요기반시설 운영자와 디지털 서비스를 제공하는 업체는 자신이 사용하는 네트워크 및 정보 시스템을 보호하기 위해 동법에 따른 조치를 취해야 하고, 보안사고가 디지털 서비스 제공에 중요한 영향을 미칠 수 있는 경우에는 즉시 연방정보기술보안청에 신고해야 한다. 디지털 서비스 제공자가 개정 연방정보기술보안청법 기준을 충족하지 못하는 경우에는 최고 5만 유로에 달하는 과태료가 부과된다. 또한 주요기반시설 운영자가 보안과 관련된 감사, 점검, 인증과정에서 발견된 결함을 제거하지 않는 경우에는 최고 10만 유로의 과태료가 부과된다.

45) Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885).

3. 통신법

(1) 연방망관리청의 권한에 관한 규율

앞서 독일의 정보보호 관련 기관으로서 연방망관리청을 살펴보았다. 이러한 연방망관리청 설립의 근거가 되는 법률이 바로 「통신법」(Telekommunikationsgesetz: TKG, 이하 '통신법'이라고 함)이다.[46] 통신법은 제8장(Teil 8)에서 연방망관리청과 관련한 내용을 규율한다. 특히 통신법은 연방망관리청의 책무를 효과적으로 현실화시키기 위해 제126조와 제127조에서 정보통신기업에 대한 일련의 개입 권한과 절차를 부여하고 있다.

먼저 통신법 제126조 제1항 따르면, 연방망관리청은 사업자가 동법 등에 근거한 의무를 이행하지 않는다고 판단되는 경우에는 일정한 기한을 정하여 사업자가 사유서를 제시하고 문제를 해결하도록 요청할 수 있다. 사업자가 특정한 기간 안에 의무를 이행하지 못하면, 연방망관리청은 일정한 기한을 정하여 의무를 이행하는 데 필요한 조치를 명령할 수 있다(제2항). 이 경우 명령을 집행하기 위해 연방망관리청은 최대 50만 유로까지 벌금을 부과할 수 있다. 그리고 사업자의 의무위반이 중대하거나 반복적인 방식으로 의무를 위반하는 경우에는 연방망관리청은 통신망 운영자 또는 통신서비스 제공자의 활동을 금지할 수 있다(제3항).

통신법 제127조 제1항에서는 일반 공중을 위해 통신망 운영자 및 통신서비스 제공자로 하여금 연방망관리청에 정보를 제공하도록 하는 의무를 부과하고 있다. 또한 동조 제2항에 따라 연방망관리청은 사업자의 경제적 관계에 관한 정보 및 일상적인 운영 · 영업시간 안에서 영업 관련 서류를 열람하고 심사할 수 있다. 동조 제6항 및 제7항에서는 압류명령 및 조사명령에 관한 권한도 규율한다.

이러한 규정에서 다음과 같은 내용을 도출할 수 있다. 통신법은 정부기관의 기밀누설을 방지하고, 데이터의 안정성 확보 및 네트워크 침해사고를 방지하기 위해 연방망관리청이 통신망 운영자 및 통신서비스 제공자가 보유하는 고객정보에 직접 접근할 수 있도록 규정하고 있으며, 이 경우 통신망 운영자와 통신서비스 제공자는 이를 지원하도록 하고 있다는 것이다.

이외에도 통신법은 연방망관리청에 소속되어 있는 결정위원회의 권한에 관해 규

46) Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 10 Absatz 12 des Gesetzes vom 30. Oktober 2017 (BGBl. I S. 3618). 이에 관해서는 우선 Klaus-Dieter Scheurle/Thomas Mayen (Hrsg.), *Telekommunikationsgesetz*, 3. Aufl., München, 2018 참고.

율한다. 이에 따르면, 결정위원회는 첫째, 통신법 제2장에 의한 시장규제(그 밖에 진입규제와 요금규제, 특별한 권한남용의 감독 및 그 밖의 의무), 둘째, 주파수 부족 시 그 교부절차에 관한 결정(제55조 제9항) 및 그 교부절차의 형성(제61조), 셋째, '주파수거래'의 형성(제62조), 넷째, 보편적 서비스 의무의 부담(제81조), 다섯째, 통신법 또는 동법에 따른 의무와 관련하여 공공통신망을 운영하는 주체 또는 공공에 대한 정보통신서비스 제공자들 간에 각종 분쟁이 발생하는 경우(제133조) 등의 사안을 결정한다.[47]

(2) 통신비밀, 데이터보호, 공공안전에 관한 규율

통신법은 제2조에서 규제목표를 설정하고 있다.[48] 특히 제2조 제2항 제9호에서 '공공안전'의 이익이 보장되어야 함을 명백히 하고 있다. 사이버 보안을 위해서는 때때로 개개인의 권리가 제한되기도 하지만, 다른 한편으로는 국가이익도 보장해야 하기에 공공안전의 이익을 강조하되, 가능한 한 개인에 대한 규제를 최소화하여 통신비밀, 데이터보호, 공공안전에 관한 규정이 이러한 목적에 기여하도록 균형을 유지하고 있다.[49] 이와 관련하여 통신법은 제7장에서 통신비밀(제1절), 데이터보호(제2절), 공공안전(제3절)을 규율함으로써 사이버 보안에 대비한다. 공공안전을 위해 사업자들이 긴급전화를 할 수 있도록 하고, 기술적 보호대책 및 감시가 가능한 방법을 마련하도록 하고 있다. 그리고 사업자 등에 대한 자료요청 권한 및 사업자 시설에 대한 지원의무 등을 구체화하고 있다.

그 중에서 통신법 제111조에 주목할 필요가 있다. 통신법 제111조는 최근 수사기관의 정보제공요청을 거부한 사건들과 관련하여 입법된 조항이다. 통신법은 아날로그 방식의 전화 통신에만 적용되는 것이 아니다. 다른 개별법에서 사이버상 정보제공에 관한 규정을 갖추고 있지 않은 경우에도 통신법 제111조 제1항이 규정하는 "기타 연결정보" 또는 "고정된 네트워크 주소 또는 추측으로 식별 가능한 네트워크 주소"를 근거로 하여 통신법이 사이버 통신에도 적용될 수 있도록 하고 있다. 통신

47) 신봉기, 앞의 글, 347쪽.

48) 「통신법」 제2조 제2항은 다음과 같은 규제목표를 규정한다. ① 통신 영역에서 이용자의 이익, 특히 소비자의 보호 및 통신비밀의 보장, ② 공정한 경쟁의 담보와 통신서비스와 통신망의 영역 및 그에 속한 시설과 서비스, 모든 지역의 영역에서 지속적으로 경쟁지향적 통신시장의 지원, ③ 효과적인 기간시설투자의 지원 및 혁신의 지원, ④ EU 역내시장 발전의 지원, ⑤ 모든 지역에서 적정한 가격에 의한 기본적 통신서비스(보편적 서비스 급부) 공급의 보장, ⑥ 공공시설에서 통신서비스의 지원, ⑦ 주파수의 효과적이고 방해 없는 이용의 담보, 방송의 이해도 고려, ⑧ 번호부여 수단의 효과적 이용 보장, ⑨ 공공안전 이익의 보장이 그것이다.

49) 이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구", 『국가정보연구』 제1권제2호, 한국국가정보학회, 2009, 82쪽.

법 제111조 제1항에 따르면, 보안관청으로부터 정보제공을 요청받아 통신서비스에서 식별 가능한 정보를 제공하는 경우에는 '정보제공요청'과 관련하여 통신법 제112조 및 제113조가 규정하는 고지절차 등을 준수할 책임이 있다. 고지대상이 되는 정보내용으로는 전화번호 및 기타 연결정보, 성명과 추측으로 식별 가능한 주소, 자연인의 생일, 고정된 네트워크 주소 또는 추측으로 식별 가능한 네트워크 주소, 이동단말기의 접속과 제공으로 이동단말기의 번호 식별이 가능한 경우의 단말기 사용계약 개시정보 등이 포함된다. 요컨대, 보안관청은 통신법 제112조 및 제113조가 규정하는 절차를 준수하는 경우에는 제111조에 따라 고객의 데이터를 확보할 수 있는 것이다. 그만큼 보안관청의 권한이 강화된 것이다.

(3) IT 보안법에 따라 개정된 통신법

IT 보안법은 시민을 더욱 안전하게 보호하기 위해 통신법상 통신사업자에게 다음과 같은 의무를 부여한다. 먼저 통신법 제109조 제1항과 제2항에 따르면, 통신사업자는 개인정보보호뿐만 아니라 허가되지 않은 침입으로부터 기반시설을 보호하기 위해 현재의 기술수준에 따른 IT 보안조치(기술적 · 관리적 조치)를 취하고 유지해야 한다. 이때 IT 보안책임자를 임명하여 IT 보안대책을 수립해야 한다. 그리고 통신법 제109조a 제4항에 따라 통신서비스 제공자는 이용자에게 유해한 프로그램에 관한 정보와 당해 프로그램에 대한 장애 발견 및 제거에 관한 정보를 제공해야 한다. 아울러 중대한 IT 장애사항은 연방망관리청뿐만 아니라 연방정보기술보안청에도 신고해야 한다(제109조 제5항). 여기서 연방정보기술보안청의 역할이 확대되었음을 알 수 있다.

(4) NIS지침에 따라 개정된 통신법

IT 보안법에 의해 개정된 통신법 제109조 제5항은 NIS지침의 독일법 전환 법률에 의해 연방정보기술보안청의 역할을 재차 확대하는 내용으로 개정되었다. 이에 따라 통신 네트워크 및 서비스의 결함 등은 연방망관리청뿐만 아니라 연방정보기술보안청에도 보고되어야 한다. 이를 위해 공공 통신 네트워크를 운영하거나 공개적으로 이용 가능한 통신서비스를 제공하는 자는 연방정보기술보안청에 등록을 하도록 하였다. 이를 통해 연방정보기술보안청은 공공 통신 네트워크를 운영하거나 공개적으로 이용 가능한 통신서비스를 제공하는 자가 정확한 신고를 하도록 보장할 수 있고, 이들 통신서비스 제공자는 연방정보기술보안청의 상황정보 및 경고정

보를 수신 받는 그룹에 포함되어 일련의 정보를 공유할 수 있게 되었다. 또한 통신서비스 제공자는 등록을 함으로써 시설을 보호하는 데 도움이 되는 제품을 제공받을 수 있다.

4. 텔레미디어법

(1) 텔레미디어법의 적용범위

이외에도 사이버 보안 관련 법률로서 「텔레미디어법」(Telemediengesetz: TMG)을 언급할 수 있다.[50] 텔레미디어법은 제1조에서 적용범위를 규정한다. 이에 따르면, 통신법의 적용영역을 제외한 모든 전자적 정보와 통신서비스에 대해 텔레미디어법이 적용된다. 조세 영역은 적용에서 제외되지만, 언론방송법이나 기타 법률의 적용을 배제하지는 않는다. 그리고 「방송과 텔레미디어에 관한 협약」(Rundfunkstaatsvertrag)에서 방송과 텔레미디어를 포함하는 특별요건들이 편입되었다.[51]

방송법은 전파를 이용한 프로그램의 제작과 전송을 대상으로 하는 데 반해, 통신서비스는 네트워크를 이용하는 것을 대상으로 한다는 점에서 차이가 있다. 그런데 텔레미디어법은 적용범위를 '모든 전자적 정보와 통신서비스'(alle elektronischen Informations-und Kommunikationsdienste)라고 규정함으로써 방송과 통신 네트워크뿐만 아니라 모든 융합서비스를 포괄한다. 인적 적용범위도 공영방송을 포함한 모든 서비스 제공자들을 포괄한다. 방송이면 유료방송이든 무료방송이든 불문하고 적용된다.

(2) 텔레미디어 이용에 대한 법률관계와 정보보호

텔레미디어법은 서비스 제공자와 이용자의 관계를 규율할 때 '서비스 제공자가 일방향으로 방송하던 시대에서 쌍방향으로 방송하는 시대로 전환되는 변화'를 배경으로 하여 법률관계를 설명한다. 여기서 '정보보호의 기본원칙'을 선언하면서, 서비스

50) Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), zuletzt geändert durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530). 이에 관해서는 Gerald Spindler/Peter Schmitz (Hrsg.), *Telemediengesetz: mit Netzwerkdurchsetzungsgesetz*, 2. Aufl., München, 2018 참고.

51) 「방송과 텔레미디어에 관한 협약」(Rundfunkstaatsvertrag)은 독일 연방의 16개 주들이 방송과 텔레미디어에 관해 체결한 협약을 말한다. 이에 관해서는 Alexandra Wagler, *Die Auswirkungen der Konvergenz der Medien auf den öffentlich-rechtlichen Rundfunk, insbesondere auf die Regelungen im Rundfunkstaatsvertrag*, Berlin, 2018 참고.

제공자는 법령에서 명시적으로 허용하는 규정을 두고 있거나 이용자가 동의하는 경우에만 텔레미디어에 관한 정보를 사용할 수 있다고 한다. 이때 서비스 제공자에게는 정보는 특별히 정해진 목적을 위해서만 수집 · 처리 · 이용되어야 한다는 '목적구속성 원칙'이 적용된다.[52] 예외적으로 텔레미디어에 대해 법령의 명시적인 규정이 있거나 이용자가 동의하는 경우에만 목적 외의 사용이 허용된다. 이러한 원칙은 해당 정보가 자동적으로 처리되는 정보인지 여부와 상관없이 적용된다.

(3) IT 보안법에 따라 개정된 텔레미디어법

IT 보안법은 텔레미디어법에 대한 개정 내용도 일부 포함하고 있다. 이에 따르면, 텔레미디어법 제13조 제7항을 신설하여 서비스 제공자에게 기술적 · 관리적 조치를 이행하는 것을 의무화하였다. 텔레미디어 서비스 제공자는 개인정보보호뿐만 아니라 허가되지 않은 침입으로부터 기반시설을 보호하기 위해 현재의 기술수준에 따른 IT 보안조치를 취하고 유지해야 한다. 또한 사이버 공격을 발견하고 차단할 수 있는 가능성이 확대되었다. 이는 통신법에서 이루어진 개정내용과 기본적으로 같다. 그 이유는 통신법과 텔레미디어법의 적용영역이 다르기 때문이다.

Ⅴ. 시사점 – 결론을 대신하여

지금까지 독일이 추진하는 사이버 보안 관련 법정책을 '정책, 거버넌스, 법률'이라는 견지에서 살펴보았다. 이제 아래에서는 결론을 대신하여 독일의 사이버 보안법에 관한 논의에서 우리의 사이버 보안 법정책과 관련하여 어떤 시사점을 도출할 수 있는지 분석하도록 한다.

1. 독자적인 사이버 보안 관련 거버넌스

먼저 독일은 연방정보기술보안청이라는 독자적인 사이버 보안 관련 거버넌스를 구축하고 있다는 점을 언급할 필요가 있다. 연방정보기술보안청이 사이버 보안에 관

52) '목적구속성(Zweckbindung) 원칙'은 정보보호법의 보편적인 원칙으로서, 독일은 연방정보보호법 제28조에서 관련 내용을 규정하고 있다. 목적구속성의 원칙에 관해서는 김중길, "빅데이터(Big Data)와 정보인권에 관한 최근 독일의 논의와 시사: 개인정보보호를 중심으로", 『법학논총』 제21권제2호, 조선대학교 법학연구소, 2014, 238쪽 아래 참고.

한 모든 문제를 총괄하도록 하고 있는 것이다. 이에 따라 연방정보기술보안청은 연방 차원에서 사이버 보안 위험에 대응하는 것뿐만 아니라 사이버 보안과 관련을 맺는 다른 분야의 문제 그리고 국제적인 차원에서 대두하는 사이버 보안 문제도 관할한다. 사이버 보안 문제를 총체적으로 관할하는 전문 거버넌스를 아직 갖추고 있지 않은 우리에게는 이러한 독일의 거버넌스가 좋은 참고가 된다. 이를테면 우리는 사이버 보안 문제를 공공부문은 국가정보원이 민간부문은 과학기술정보통신부가 분담하여 관할하고, 이외에도 방송통신위원회, 행정안전부, 금융위원회, 개인정보보호위원회 등이 각각의 개별 영역에서 근거법령에 따라 관련 업무를 수행하고 있다. 이와 같은 구조는 한편으로는 유기적으로 조직되어 있는 듯하지만, 그 실질은 국가정보원이 주도하는 사이버 보안 체계가 한정적으로 작용하는 것으로 볼 수 있다. 이는 국가안보 차원에서 발생하는 침해에 대응하기 위한 전형적인 구조에 해당한다. 따라서 제4차 산업혁명이 야기하는 사회구조의 변화에 적절하게 대응할 수 있는 사이버 보안 거버넌스가 되기는 어렵다. 특히 독일에서 이루어지는 논의 및 정책을 참고하면 이는 적절하지 않아 보인다. 이에 각 영역별로 존재하는 정보공유 및 분석센터를 총괄하는 독자적인 거버넌스를 구축할 필요가 있다. 이는 크게 두 가지 방안으로 실현할 수 있다. 첫째는 독일의 경우처럼 사이버 보안 업무를 총괄하는 독자적인 사이버 보안청을 신설하여 각 정보공유·분석센터를 총괄하도록 하는 것이다. 둘째는 과학기술정보통신부장관 소속으로 사이버 보안을 위한 정보공유·분석센터를 설치하여 이를 통해 각 정보공유·분석센터를 총괄하도록 하는 것이다.

2. 사이버 보안에 관한 강력한 권한

다음으로 사이버 보안에 관한 강력한 권한을 연방정보기술보안청에 부여하고 있다는 점에 주목해야 한다. 이에 대한 근거로 크게 세 가지를 언급할 수 있다. 먼저 사이버 보안에 대한 침해를 사전에 적절하게 예방할 수 있도록 연방정보기술보안청이 이에 관한 데이터를 광범위하게 수집·분석할 수 있도록 하고 있다는 것이다. 특히 정보통신서비스 이용자의 데이터에도 직접 접근할 수 있도록 하고 있다는 점이 눈에 띈다. 이에 관해서는 개인정보침해 문제가 대두할 수 있는데, 독일은 이에 대한 법적 근거를 마련함으로써 이 문제를 풀어가고 있는 것이다. 현재 우리 정보통신망법은 이에 관한 법적 근거를 명확하게 갖추고 있지 않은데, 이러한 점에서 독일 연방정보기술보안청의 사례는 우리에게 시사하는 바가 크다. 다음으로 정보통신 관련제품의 사이버 보안 정도를 연방정보기술보안청이 직접 검사할 수 있도록 한 것이다. 현대

초연결사회에서는 사물인터넷을 해킹함으로써 손쉽게 전체 사이버 보안을 위협할 수 있다는 점에서 이러한 권한을 연방정보기술보안청에 부여한 것은 적절하다고 평가할 수 있다. 이외에도 연방정보기술보안청이 중심이 되어 정부와 주요기반시설의 사이버 보안을 통합적으로 추진하도록 함으로써 사이버 보안과 관련된 각 기관의 기능을 서로 연결하고 이를 효율적으로 통합하도록 한 것도 좋은 근거가 된다.

3. 공적 영역과 사적 영역의 상호협력

나아가 사이버 보안을 실현하기 위해 공적 영역과 사적 영역이 적극적으로 상호협력을 추구한다는 점을 고려해야 한다. 이는 앞의 [그림 3]이 보여주는 연방정보기술보안청법 제8조b에 따른 IT 보안정보 신고절차에서 확인할 수 있다. 여기에서 특히 'UP KRITIS'가 눈에 띄는데, 이는 "주요기반시설 운영자 및 그 연합체 그리고 관할 국가조직 사이에서 이루어지는 공적-사적 협력"을 말하기 때문이다.[53] 이를 예증하듯, 연방정보기술보안청법 제8조b에 따라 진행되는 IT 보안정보 신고절차에서는 '주요기반시설 운영자'(Betreiber), '연방정보기술보안청'(BSI), '감독관청'(Aufsichtsbehörden), '연방국민보호재난지원청'(BBK), '그 밖의 연방관할관청'(Sonst zuständige Behörden des Bundes)이 상호협력을 해야 한다.[54] 상호성 원칙과 자발성 원칙을 기반으로 하여 공공기관이 사이버 보안 관련 정보를 적극적으로 민간에 전파 · 제공하고, 민간은 사이버 보안에 관해 획득한 노하우를 공공기관에 제공 및 위협정보를 보고 · 신고하도록 해야 한다. 이는 어찌 보면 현대 초연결사회에서 사이버 보안을 실현하기 위해서는 당연한 일이라 할 수 있다.

4. 정보공유

이어서 연방정보기술보안청이 보유하고 있는 정보를 다른 기관과 공유하도록 하고 있다는 점을 언급할 필요가 있다. 이는 위에서 말한 공적 영역과 사적 영역의 상호협력을 예증하는 또 다른 중요한 예에 해당한다. 이를 통해 사이버 공격에 관해 연

53) BSI, *Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS*, Bonn, 2017, S. 25

54) BBK는 독일 연방내무부에 소속되어 있는 재난 관련 전문연방관청으로서, 국가적으로 중요한 위험시설로부터 국민을 보호하고, 연방의 재난정책 수행 및 각 주의 재난대응에 대한 권한을 단일화함으로써 위기관리에 대응하고 조율하는 기관이다. 이에 관해서는 연방국민보호재난지원청 홈페이지 참고(https://www.bbk.bund.de/DE/Home/home_node.html).

방정보기술보안청이 보유하는 정보를 다른 감독기관 및 주요기반시설 운영자가 공유하도록 하고 있다. 이는 정보공유가 사이버 보안을 실현하는 데 매우 중요한 역할을 한다는 점을 잘 보여준다.

현재 우리 법체계는 독자적인 법률로써 정보공유를 규율하고 있지는 않다. 「공공기관의 정보공개에 관한 법률」, 「전자정부법」, 「정보통신기반 보호법」 등에서 단편적으로 이를 규율하고 있을 뿐이다. 이러한 상황에서 2017년 1월 3일 정부가 제안한 「국가사이버안보법안」은 정보공유에 관해 상당히 의미 있는 규정을 두고 있다.[55] 이를테면 「국가사이버안보법안」 제12조는 "사이버위협정보의 공유"라는 표제 아래 모두 여섯 항으로 구성된 비교적 상세한 규정을 두고 있다.[56] 이 규정에서는 크게 세 가지 의미 있는 사항을 발견할 수 있다. 첫째, 독자적인 사이버위협정보 공유센터를 설치한다는 것이다. 둘째, 이러한 사이버위협정보 공유센터를 국가정보원장 소속으로 설치한다는 것이다. 셋째, 사이버위협정보 공유센터와 책임기관 사이에 상호적인 정보공유를 인정한다는 것이다. 이렇게 볼 때, 「국가사이버안보법안」이 마련하고 있는 정보공유 규정은 꽤 진일보한 것이라고 평가할 수 있다. 다만 이 법안은 아직 법률로 제정되지 못하고 있다는 점, 사이버위협정보 공유센터는 '국가안보를 위협하는 사이버공격'에 관한 정보를 대상으로 한다는 점에서 정보공유에 관한 원칙적인 규정이 될 수는 없다.

5. 기술적 · 관리적 조치 강화

이뿐만 아니라 독일의 사이버 보안법은 최근 사이버 보안을 강화하기 위해 기술적

55) 이에 관해서는 양천수, "정보보호를 위한 정보공유 법정책: 현황과 개선방안", 「인권이론과 실천」 제23호, 영남대학교 인권교육센터, 2018, 33-47쪽 참고.

56) 「국가사이버안보법안」 ① 다음 각 호의 정보를 공유하기 위하여 국가정보원장 소속으로 사이버위협정보 공유센터를 둔다. 1. 사이버공격 방법에 관한 정보 2. 악성프로그램 및 이와 관련된 정보 3. 정보통신망, 정보통신기기 및 소프트웨어의 보안상 취약점에 관한 정보 4. 그 밖에 사이버공격의 예방을 위한 정보 ② 책임기관의 장은 소관 사이버공간의 제1항에 따른 정보(이하 "위협정보"라 한다)가 다른 책임기관의 사이버안보를 위하여 필요하다고 인정하는 경우 대통령령으로 정하는 바에 따라 소관 사이버공간의 위협정보를 제1항에 따른 사이버위협정보 공유센터(이하 "공유센터"라 한다)의 장에게 제공할 수 있다. 이 경우 공유센터의 장은 사이버안보를 위하여 위협정보의 공유가 필요하다고 판단되는 책임기관의 장에게 위협정보를 제공하여야 한다. ③ 누구든지 제2항에 따라 공유된 위협정보를 사용할 때에는 사이버안보 목적에 필요한 최소한의 범위에서 사용·관리하여야 한다. ④ 공유센터의 장은 위협정보를 공유하는 경우 국민의 권리가 침해되지 아니하도록 기술적·관리적 또는 물리적 보호조치를 마련하여야 한다. ⑤ 공유센터의 장은 제4항에 따른 기술적·관리적 또는 물리적 보호조치에 관한 사항을 심의하기 위하여 책임기관 및 민간 전문가 등이 참여하는 사이버위협정보 공유협의회를 구성·운영하여야 한다. ⑥ 제1항부터 제5항까지의 규정에 따른 공유센터의 설치·운영, 공유센터의 장에게 제공하는 위협정보의 범위 등에 필요한 사항은 대통령령으로 정한다.

· 관리적 조치에 대한 의무를 강조하고 있다는 점에 주목해야 한다. 규제체계의 관점에서 보면, 기술적 · 관리적 조치는 두 가지 의미를 갖는다. 첫째, 기술적 · 관리적 조치는 사후적 조치가 아니라 사전예방적 조치라는 것이다. 이는 현대 초연결사회에서 사이버 보안을 실현하기 위해서는 사이버 침해가 발생하였을 때 비로소 이에 대응하는 현재적 · 사후적 조치보다 사전예방적 조치가 더욱 중요하다는 점을 보여준다. 둘째, 기술적 · 관리적 조치 중에서 특히 기술적 조치는 현대사회에서 새로운 규제수단으로 주목받고 있는 '아키텍처 규제'(architectural regulation)의 대표적인 예에 속한다는 점이다.[57] 독일 사이버 보안법이 최근 이러한 기술적 · 관리적 조치를 강화하고 있는 점은 우리에게도 시사하는 바가 없지 않다.

6. 독자적인 망 관리 거버넌스

이외에도 독자적인 망 관리 거버넌스로 연방망관리청을 두고 있다는 점도 우리가 눈여겨 볼 필요가 있다. 예전과는 달리 오늘날에는 ICT가 모든 분야에서 사용되고 있다는 점을 고려하면, 우리도 정보통신과 관련을 맺는 국가의 기간 소통망을 총괄적으로 관리하는 거버넌스 설립을 모색할 필요가 있다.

57) '아키텍처 규제'에 관해서는 심우민, "사업장 전자감시 규제입법의 성격", 『인권법평론』 제12호, 전남대학교 공익인권법센터, 2014, 157-183쪽 참고.

참고문헌

I. 국내문헌

강석구 외, 『사이버안전체계 구축에 관한 연구』, 한국형사정책연구원, 2010.

권현준 외, 『사이버 보안법제 선진화 방안 연구』, 방송통신위원회, 2011.

김대근, "안전 개념의 분화와 혼융에 대한 법체계의 대응방안", 『법과 사회』 제47호, 법과사회이론학회, 2014.

김병기, "정보보호 거버넌스 현황과 지능정보사회의 정보보호 거버넌스 개편 試論", 『행정법연구』 제51호, 행정법이론실무학회, 2017.

김상배, "세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각", 『국제·지역연구』 제26권제3호, 서울대학교 국제학연구소, 2017.

김재광, "사이버안보 위협에 대한 법제적 대응방안", 『법학논고』 제58집, 경북대학교 법학연구원, 2017.

김중길, "빅데이터(Big Data)와 정보인권에 관한 최근 독일의 논의와 시사: 개인정보보호를 중심으로", 『법학논총』 제21권제2호, 조선대학교 법학연구소, 2014.

류지태 외, 독일 통신법, 법원사, 2007.

배병환 · 송은지, "주요국 사이버 보안 전략 비교·분석 및 시사점: 미국, EU, 영국의 사이버 보안 전략을 중심으로", 『정보통신방송정책』 제26권 21호, 정보통신정책연구원, 2014.

신봉기, "독일 연방통신망청에 관한 연구: 망(網) 관련 통합 규제관청으로서의 지위와 절차를 중심으로", 『공법연구』 제35권제3호, 한국공법학회, 2007.

심우민, "사업장 전자감시 규제입법의 성격", 『인권법평론』 제12호, 전남대학교 공익인권법센터, 2014.

양천수, "현대 초연결사회와 새로운 인격권 보호체계", 『영남법학』 제43집, 영남대학교 법학연구소, 2016.

양천수, "제4차 산업혁명과 정보보호 법정책의 방향", 『공법학연구』 제18권제4호, 한국비교공법학회, 2017.

양천수, "정보보호를 위한 정보공유 법정책: 현황과 개선방안", 『인권이론과 실천』 제23호, 영남대학교 인권교육연구센터, 2018.

양천수 외, 『사이버 보안 강화를 위한 정보통신망법 체계 개선방안 연구』, 미래창조과학부, 2015.

양천수 · 지유미, "미국 사이버보안법의 최근 동향: 「사이버보안 정보공유법」을 중심으로 하여", 『법제연구』 제54호, 한국법제연구원, 2018.

이연수 외, "주요국의 사이버안전관련 법·조직체계 비교 및 발전방안 연구", 『국가정보연구』 제1권제2호, 한국국가정보학회, 2009.

정필운, "사이버보안이란 개념 사용의 유용성 및 한계", 『연세 의료 · 과학기술과 법』 제2권제2호, 연세대학교 법학연구원 의료 · 과학기술과 법센터, 2011.

한국정보화진흥원, NIA Hot Issue Report 2017-13: 2016년 다포스포럼 4차 산업혁명 발표 전후 주요국 국가정보화 전략 분석 및 시사점, 2017.

II. 외국문헌

Bundesamt für Sicherheit in der Informationstechnik, Das IT-Sicherheitsgesetz, Bonn, 2016.

Bundesamt für Sicherheit in der Informationstechnik, Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS, Bonn, 2017.

Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz Arbeitshandbuch: DIN ISO/IEC 27001, DIN ISO/IEC 27002, Bonn, 2017.

Bundesamt für Sicherheit in der Informationstechnik, Digitale Gesellschaft zwischen Risikobereitschaft und Sicherheitsbedürfnis: Tagungsband des 15. Deutschen IT-Sicherheitskongresses des BSI, Bonn, 2017.

Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung: Tagungsband zum 16. IT-Sicherheitskongress des BSI, Bonn, 2019.

Bundesministerium des Innern, Cyber-Sicherheitsstrategie für Deutschland 2016, 2016.

Lutz Johanning/Ernst-Olav Ruhle, "Sind Regulierungsbehörden die besseren Manager? Eine kapitalmarktorientierte Bewertung von wichtigen Regulierungs-und Managemententscheidungen", in: K&R, 2003.

Hans-Jürgen Lange/Astrid Bötticher (Hrsg.), Cyber-Sicherheit, Springer VS, 2014.

Thomas M. Lachner, Das Artikelgesetz, Berlin, 2007.

Sebastian Leuschner, Sicherheit als Grundsatz: Eine grundrechtsdogmatische Rekonstruktion im Unionsrecht am Beispiel der Cybersicherheit, Tübingen, 2018.

Marcus Lobedann, Die neue Rolle der Bundesnetzagentur, Norderstedt, 2012.

Thomas Schulz (Hrsg.), Industrie 4.0: Potenziale erkennen und umsetzen, Vogel Business Media, 2017.

Klaus-Dieter Scheurle/Thomas Mayen (Hrsg.), Telekommunikationsgesetz, 3. Aufl., München, 2018.

Alexander Silhavy, Cyber-Sicherheitsstrategie für Deutschland: Neue Bedrohungen? Neue Lösungen?, Norderstedt, 2013.

Gerald Spindler/Peter Schmitz (Hrsg.), Telemediengesetz: mit Netzwerkdurchsetzungsgesetz, 2. Aufl., München, 2018.

Alexandra Wagler, Die Auswirkungen der Konvergenz der Medien auf den öffentlich-rechtlichen Rundfunk, insbesondere auf die Regelungen im Rundfunkstaatsvertrag, Berlin, 2018.

논문 투고일: 2019. 04. 15
심사 완료일: 2019. 05. 31
게재 확정일: 2019. 06. 11

[Abstract]

The Cyber-Security Laws in Germany - Policy, Governance, Law -

Chun-Soo Yang* · Jung-Gil Kim**

As modern society is being transformed into a 'hyper-connected society', new legal problems are emerging. Cyber security is one of the most important examples. As for cyber security, the following problems are arising: Is a new integrated legal regulation for cyber security necessary, how to build a governance system for cyber security, how to strengthen information sharing on cyber security, and how to prepare preventive measures for cyber security? There have been various discussions on those problems, but still fail to find a satisfactory solution. In this context, this article looks at what kind of law policy is being pursued by Germany, which has had a great impact on our legal system. At this point, this article focuses on policy, governance and law. First, this article examines the cyber security strategies in Germany (II), and next, analyzes the major organizations related to cyber security (III). The 'Bundesamt für Sicherheit in der Informationstechnik' and 'Bundesnetzagentur' are the main subjects of the analyzing. Then, this article analyzes the current status of Cyber Security Act in Germany (IV): "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz), "Directive on Network and Information Security" (NIS Directive), "Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes", "Gesetz über das Bundesamt für Sicherheit in der Informationstechnik", "Telekommunikationsgesetz" and "Telemediengesetz" are analyzed here. From these discussions, finally, this article provides meaningful implications for our cyber security law policy (V). This article draws the following implications: First, Germany has its own governance system dedicated to cyber security. This is the 'Bundesamt für Sicherheit in der Informationstechnik'. Second, Germany gives 'Bundesamt für Sicherheit in der Informationstechnik' strong authority on cyber security. Third, Germany intensifies interactive cooperation between public and private sectors for cyber security. Fourth, 'information sharing' and 'technical and managerial measures' are being strengthened for cyber security.

Key Words: Cyber-Security Laws in Germany, Bundesamt für Sicherheit in der Informationstechnik, Bundesnetzagentur, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, IT-Sicherheitsgesetz, NIS Directive

* Professor at Yeungnam University Law School, Dr. jur. (Lead author)

** Lecturer at Yeungnam University Chunma Honors School, Dr. jur. (Corresponding author)