영남대학교 법학연구소 인권교육연구센터
「인권이론과 실천」
제32호 (2022.12.) pp.1~24.

디지털 시대에 인격권 보호*

이 부 하**

Ⅰ. 서론

디지털 시대[1]에 법 해석과 적용은 과학기술의 발전 정도와 밀접하게 연관되어 있다. 디지털 시대에는 과학기술 발전이 획기적으로 이루어지기 때문에 법은 과학기술의 발전 정도에 발맞추어 개선되어야 한다. 디지털 기술로는 사물인터넷(IOT: Internet of Things), 블록체인, 온디맨드 경제(공유경제, 플랫폼 비즈니스, 디지털 플랫폼), 인공지능(Artificial Intelligence) 등이 있다. 특히 IOT(사물인터넷) 환경에서 데이터의 수집, 저장, 관리를 통한 빅 데이터(Big Data)로 인해 개인정보 침해 가능성이 높아졌다. 미디어 분야에서 유튜브(YouTube), Facebook, 넷플릭스, Apple TV+ 등 다양한 미디어 서비스는 놀라운 속도로 기존 방송의 중앙 집중식 보급 방식을 뒤집고 전 세계를 매체를 통해 하나로 연결하고 있다. '빅 데이터'는 1초에 수조 비트의 정보를 분석한다. 현재 디지털 사회에서는 데이터 흐름이 24시간 내내 제3자에게 유통되는 대규모 자체 감시 체제가 만들어졌다. 특히 사이버안전과 관련하여, 디지털 시대에 대량의 감시가 만연한 것은 다양한 유형의 디지털 기술 발전에 따른 것이다.

본 논문에서는 먼저 독일 연방헌법재판소의 온라인 수색 판결에 대해 살

---

* 이 논문은 「미디어와 인격권」 제8권 제3호(2022. 12.)에 게재된 저자의 논문 "일반적 인격권에 대한 헌법적 고찰"의 일부분을 활용하여 수정한 논문임.

** 영남대학교 법학전문대학원 교수.

1) 디지털 시대에 공법적 대응에 관하여는 김정수 · 엄주희, "디지털 시대의 소외와 포용, 그리고 공법적 대응", 「법과 사회」 제71호, 법과사회이론학회, 2022. 10., 227면 이하.

펴보고, 헌법적으로 검토·분석해 본다(이하 II). 다음으로 디지털 시대에 공익인 사이버안전과 기본권인 인격권 보호 간의 관계를 연구해 본다(이하 III). 결론에서는 본론에서 서술한 연구 내용을 정리해 본다(이하 IV).

Ⅱ. 독일 연방헌법재판소의 온라인 수색 판결

1. 사건의 개요

독일 연방헌법재판소에 2개의 헌법소원심판이 청구되었다.[2] 1 BvR 370/07 헌법소원심판 청구인들은 1a, 1b가 있었고, 1 BvR 595/07 헌법소원심판 청구인들은 2a, 2b, 2c가 있었다. 헌법소원심판 청구인 1a는 여성 언론인이며, 주로 온라인 출판물에 기사를 쓰고 있었다. 청구인 1a는 직업 활동의 일환으로 헌법에 적대적인 개인과 단체가 운영하는 인터넷-프레젠첸(Internet-Präsenzen) 사이트에 자주 방문하였다. 또한 청구인 1a는 정보보호법 관련 업무에도 관여하였고, www.stop1984.com 홈페이지를 다른 사람들과 함께 운영하고 있었다. 이 홈페이지에 접속하여 자주 채팅에 참여했다. 청구인 1a는 사적·직업적으로 사용하는 컴퓨터 하드 드라이브에 극우주의자들에 관한 정보를 저장해 왔다. 헌법소원심판 청구인 1b는 노르트라인-베스트팔렌 주(州) 헌법수호청에 의해 감시당하는 좌파당(DIE LINKE)의 노르트라인-베스트팔렌 주(州) 협회의 진성당원이다. 청구인 1b는 정치적 활동을 위해 인터넷이 연결된 자신의 컴퓨터를 사용했다. 청구인 1b도 사적인 통신을 위해 그리고 은행 지로계좌(Girokonto)를 통해 거래를 위해 인터넷에 접속하곤 했다.[3]

헌법소원심판 청구인 2a와 2b는 변호사 사무실의 파트너 변호사였다. 변

2) BVerfGE 120, 274 ff.
3) 1 BvR 370/07, 116-117.

호사로서 청구인 2a는 특히 망명 신청자들을 돌보고 있었다. 망명 신청자들 중에는 노르트라인-베스트팔렌 주 헌법수호청의 감시를 받고 있는 쿠르드 노동자당(PKK)의 지도당원이 있었다. 그는 집과 변호사 사무실에 인터넷이 연결되어 있는 컴퓨터 네트워크를 사용했다. 변호사 사무실 네트워크는 청구인 2b와 변호사 사무실에서 프리랜서로 일하는 청구인 2c도 함께 사용하고 있었다.[4)]

헌법소원심판의 대상은 한편으로는 정보통신시스템에서 다양한 정보를 수집할 수 있는 헌법보호기관의 권한을 규율하고 있고, 다른 한편으로는 수집된 정보의 처리를 규율하고 있는 노르트라인-베스트팔렌 주(州) 헌법보호법(VerfSchutzG NRW)의 조항이었다. 헌법소원심판의 대상이 된 법조항은 2006년 12월 20일자 노르트라인-베스트팔렌 주(州) 헌법보호법 개정법률에 의해 추가되거나 개정된 법조항이었다. 2개의 헌법소원심판에서 청구인들은 노르트라인-베스트팔렌 주(州) 헌법보호법 제5조 제2항 제11호와 제5c조 제4항 제1호의 위헌성을 주장하였다.

2. 판결요지

독일 기본법 제1조 제1항과 관련된 독일 기본법 제2조 제1항에 근거하고 있는 일반적 인격권에서는 정보통신시스템의 기밀성과 완결성을 보장하는 기본권이 포함되어 있다.[5)] 정보통신시스템에의 비밀리 접근은 독일 기본법 제10조 제1항(통신의 비밀 보장)에 근거하지 않는다. 정보통신시스템에의 정보 수집에 대해 보장하는 기본권이 존재하지 않는다. 이는 기본권 보장에 있어서 흠결 상태이다. 이러한 흠결로 인해 정보통신시스템의 기밀성과 완결성의 보호로서 일반적 인격권을 새로이 형성하였다.[6)]

---

4) 1 BvR 595/07, 118. 이부하, "일반적 인격권에 대한 헌법적 고찰", 「미디어와 인격권」 제8권 제3호, 언론중재위원회, 2022. 12., 152-153면.

5) 1 BvR 370/07, 166.

정보통신시스템의 사용을 모니터링하고 저장매체에 접근하여 가독할 수 있는 정보통신시스템에의 비밀리 접근은 상당히 중대한 법익에 대한 구체적 위험의 실제 징후가 있는 경우에만 헌법에 근거하여 허용된다. 개인의 신체, 생명, 자유 또는 국가의 존속이나 인간 존재의 토대에 영향을 미치는 공익이 존재해야 한다. 정보통신시스템에의 비밀리 접근조치는 가까운 장래에 위험이 발생할 확률로 결정할 수 없더라도, 특정 사실이 개별 사건에서 특정인이 제기하는 가장 중요한 법익에 대한 위험을 야기하는 경우에는 정당화될 수 있다.

정보통신망에서 행한 통신 내용과 통신 상황을 수집하거나 관련 정보를 조사하는 국가의 조치에 관한 법률 규정은 독일 기본법 제10조 제1항의 통신의 비밀 보장 조항에 의거하여 판단해야 한다.[7] 국가가 온라인 수사 목적을 위해 기술적 방식으로 인터넷상 통신 내용을 인지하게 되는 경우, 국가기관이 통신 참여자들의 정보를 지득할 권한이 없는 경우에만 독일 기본법 제10조 제1항의 통신의 자유를 침해하게 된다.[8]

3. 온라인 수색 판결의 분석 및 평가

(1) 판례의 의의

독일 연방헌법재판소의 온라인 수색 판결을 살펴보았다. 위 연방헌법재판소 판결의 주요 대상은 정보통신시스템에의 비밀리 접근과 인터넷 비밀 수사 그리고 은행계좌의 내용 및 계좌의 입출금 상태의 수집이었다. 이에 대해 독일 연방헌법재판소는 정보통신시스템에의 침입에 대한 보호는 독일 기본법 제10조 또는 제13조 및 사생활 보호나 및 개인정보자기결정권을 통해 보장되지 않는다고 하면서 '정보통신시스템의 기밀성 및 무결성 보장'에 관한

6) 1 BvR 370/07, 187.
7) 1 BvR 370/07, 184.
8) 1 BvR 370/07, 178.

기본권이라는 새로운 기본권을 형성해냈다. 독일 연방헌법재판소는 헌법소원심판 대상 법규정인 노르트라인-베스트팔렌 헌법보호법 제5조 제2항 11호 1문은 법규범의 명확성 원칙을 충족하지 못하고 있고, 비례성 원칙도 준수하지 못하고 있으며, 사적 생활 형성의 핵심영역을 보호하기 위한 충분한 장치도 규정하고 있지 않기 때문에 무효라고 판단하였다. 또한 인터넷 비밀 수사를 규정하고 있는 노르트라인-베스트팔렌 헌법보호법 제5조 제2항 11호 1문은 독일 기본법 제10조 제1항의 통신의 비밀을 침해할 뿐 아니라, 독일 기본법 제19조 제1항 2문의 적시의무(이유제시의무)도 위반하였으므로 무효라고 판단했다. 다만, 인터넷 수사를 위한 그 밖의 조치가 기본권 침해로 간주되지 않는 경우에는 인터넷 비밀 수사는 할 수 있다고 했다. 노르트라인-베스트팔렌 헌법보호법 제5a조 1항에서 규정하고 있는 은행계좌의 내용과 계좌의 입출금 상태의 수집은 개인정보자기결정권으로서 형성되는 일반적 인격권을 침해한다고 판결하였다.

독일 연방헌법재판소는 이 판결을 통해 정보통신시스템의 기밀성 및 무결성 보장에 관한 기본권을 형성함으로써 온라인 수색에 대한 헌법적 근거를 마련하였다. 이는 노르트라인-베스트팔렌 주 헌법보호법 규정을 무효로 한 것이지만, 온라인 수색 자체는 합헌적인 것으로 인정한 점에 의의가 있다. 위 연방헌법재판소 판결은 형사소송법에서 온라인 수색을 허용하고 있지 않다고 한 지난 2007년 1월 31일 연방대법원 판결 이후, 학계, 법조계, 정치계 등에서 많은 논란이 있었던 것에 대한 헌법적 판단을 내린 것이다. 결국 연방 및 각 주에서는 정보통신시스템에의 비밀 접근과 관련한 법률을 제정하였다.

(2) 판례의 분석

1) 제한되는 기본권: IT 기본권

독일 연방헌법재판소는 온라인 수색 판결에서 '정보통신시스템의 기밀성

과 완결성을 보장'하는 새로운 기본권, 즉 '컴퓨터 기본권'(소위 'IT 기본권')을 창설해냈다. 이러한 '컴퓨터 기본권'(소위 'IT 기본권')은 일반적 인격권에 근거하고 있다. 일반적 인격권 보호영역은 사적 영역의 보호, 의료정보, 일기장 기록 등과 같은 개인 사생활의 기밀성 등 자기보호(自己保護)에 있다. '자기보호'란 '프라이버시권'(privacy right)에서 나오는 '혼자 있을 권리'라는 사생활 보호다. 독일 연방헌법재판소는 온라인 수색 판결에서 일반적 인격권의 요소로서 '자기보호권'을 그 보호내용으로 제시하고 있다.[9)]

위 헌법소원심판에서는 인터넷 감시(Beobachten)와 비밀 수사(Aufklären)와 관련된 헌법적 쟁점이 있고, 또한 정보통신시스템에의 비밀리 접근이라는 헌법적 문제가 되었다. 노르트라인-베스트팔렌 주 헌법보호법 제5조 제2항 제11호에 규정된 '기술적 침입을 통한 정보통신시스템에의 비밀리 접근'은 '정보통신시스템의 기밀성과 완결성 보장'에 관한 기본권으로서 헌법상 '일반적 인격권'을 제한하고 있다. 일반적 인격권은 특별한 기본권은 아니지만, 인격을 구성하고 있다는 점에서 인격의 구성요소를 보장하고 있다.[10)] 특히 과학기술의 발전과 생활환경의 변화과정에서 발생할 수 있는 새로운 형태의 리스크에 대비하기 위해서 이러한 흠결을 해소해 주는 새로운 기본권이 필요하다.[11)] 일반적 인격권의 다양한 측면에서 법적 보호 요구는 무엇보다도 인격권에 대한 위험의 유형에 따라 달라지게 된다.[12)]

정보통신시스템이 서로 네트워크로 연결되어 있는 경우, 개인의 인격 발현은 그 중요성이 커진다.[13)] 정보통신시스템이 생활 전반에 광범위하게 확대됨에 따라 이 시스템을 활용하여 개인의 인격 발현의 새로운 기회가 생겼을 뿐만 아니라 인격권 침해에 대한 위험이 새롭게 발생하게 되었다. 개인정보

9) BVerfGE 120, 274 - Online-Durchsuchungen
10) BVerfGE 99, 185 (193); BVerfGE 114, 339 (346).
11) BVerfGE 54, 148 (153); BVerfGE 65, 1 (41); BVerfGE 118, 168 (183).
12) BVerfGE 101, 361 (380); BVerfGE 106, 28 (39).
13) 권형둔, "디지털 전환의 시대 언론의 자유 보장과 인격권 보호 사이의 균형모색",「미디어와 인격권」 제7권 제3호, 언론중재위원회, 2021, 16면.

처리과정과 관련하여 정보통신시스템의 저장매체에는 개인의 정보, 그 개인의 사회적 관계, 개인이 행한 활동과 관련하여 다량의 정보가 저장되어 있다. 이러한 정보들을 제3자가 수집하여 활용한다면, 이는 이용자의 인격을 충분히 추론할 수 있게 되고 이용자의 인격을 인식할 수 있게 된다. 만일 제3자가 개인정보가 수집되어 있는 정보통신시스템에 침입하게 되면, 이용자의 개인정보 보호는 불가능해진다. 위 헌법보호법은 정보통신기술의 발전을 통해 발생하는 위험으로부터 일반적 인격권의 핵심인 개인정보 보호를 충분히 고려하지 못했다.[14]

2) 헌법적 쟁점

독일 연방헌법재판소는 소위 트로이 목마와 같은 침투성 정보통신시스템의 도움으로 심각한 범죄행위의 혐의가 있을 때, 국가가 용의자의 컴퓨터 저장매체를 비밀리에 염탐하는 것이 허용되는지 여부가 문제되었다. 독일 연방헌법재판소는 노르트라인-베스트팔렌 주(州)의 헌법보호법(VerfSchutzG NRW) 제5c조 제4항 1호[15]에서 이러한 국가행위의 법적 근거를 찾았다. 독일 연방헌법재판관들은 독일 기본법 제10조(서신, 우편 및 전신의 비밀)[16]와 제13조(주거의 불가침)[17]의 기본권이 정보통신기술의 진보적인 발전에 따른 위험 상황을 적절하게 반영하지 못하고 있다고 판단했다.

독일 기본법 제10조 제1항의 '서신의 비밀과 우편 및 전신의 비밀은 불가침'은 무선 또는 유선 전자파를 매개로 한 공간적 원거리 통신의 위험성을 방지하기 위한 것이다. 즉, 원거리의 사생활을 보호하고 있다.[18] 그러나 '온

14) 이부하, 앞의 논문, 155면.
15) Verfassungsschutzgesetz Nordrhein-Westfalen § 5c (4) 1. 형사 범죄를 예방하거나 조사하기 위해
16) 독일 기본법 제10조 (서신, 우편 및 전신의 비밀)
17) 독일 기본법 제13조 (주거의 불가침)
18) BVerfGE 115, 166 (183 ff.).

라인 수색'은 반드시 통신 매체를 통한 교신과 관련된 것은 아니다. 또한 독일 기본법 제13조 제1항의 '주거의 불가침' 조항은 정보통신시스템 상에 인격권의 중요한 영역에 대한 감시를 효과적이고 포괄적으로 보호하지 못하고 있다. 온라인 수색은 예를 들어, 노트북에 와이파이 연결을 통해 주거지의 공간적 관계 등 그 주거지의 위치와 독립적인 상태에서 가능하다. 독일 기본법 제13조 제1항에서 의미하는 '주거'에서 '주거지'와 매개하는 공간 영역은 정보 수집에 어떠한 영향도 받지 않는다.

디지털 시대에 통신의 비밀은 중요한 기본권이다. 통신의 비밀 보장의 중요한 목적은 개인이 사적인 의사소통을 통해 인격의 자유로운 발현을 보장하는 동시에 … 인간의 존엄성을 보장하기 위함이다.[19] '온라인 수색' 사례에서 독일 기본법 제13조(주거의 불가침)의 적용을 반대하는 것은 컴퓨터 사용자가 인터넷 트래픽에 참여하여 개인의 정보통신시스템을 고의적으로 열어 인터넷 영역에 진입한다는 것에 있다.[20] 이러한 생각은 개인용 컴퓨터를 사용할 때 일반적인 행위태양을 잘못 생각하고 있다. 인터넷에서 이메일이나 정보 '서핑'을 하는 사용자는 하드 드라이브에 저장된 개인정보를 다른 사람에게 공개하는 것을 원하지 않는다.[21] 오히려 해커의 공격으로부터 자신의 개인정보를 보호하기를 원하며 소위 방화벽을 설치하여 외부의 공격으로부터 자신의 개인정보를 보호하려고 한다.

독일 기본법 제2조 제1항의 '일반적 인격권'은 인격권 발현의 수단으로서 정보통신기술을 차별 없이 사용하도록 기본권 보호의 흠결을 보충하고 있다. 독일 연방헌법재판소는 온라인 수색 판결에서 '컴퓨터 기본권'(IT 기본권)이라고 알려진 '정보통신기술시스템의 기밀성과 완결성 보장의 기본권'이라는

19) BVerfGE 110, 33 (53).

20) M. Hofmann, Die Online-Durchsuchung? staatliches Hacken oder zulässige Ermittlungsmaβnahme? NStZ 2005, S. 121 (124).

21) M. Kutscha, Verdeckte „Online-Durchsuchung" und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169 (1170).

일반적 인격권의 새로운 구성요소를 형성하였다.[22] 정보통신기술시스템의 기밀성과 완결성 보장의 기본권은 개인의 생활형성의 필수적인 부분에 대한 개인적 조망과 인격을 의미 있게 설계하도록 하기 위해 정보통신기술시스템 상에 국가에 의한 개인정보 수집으로부터 개인을 보호한다.[23] 그러나 독일 연방헌법재판소는 일반적 인격권의 구성요소로서 자기보호권을 개인정보자기결정권과 별도의 기본권으로 창설하고 있는데, 개인정보자기결정권과 구별되는 자기보호권의 독자적인 존재가치가 있는지는 살펴보아야 한다.[24]

(3) 비례성 원칙 위반 여부

노르트라인-베스트팔렌 주 헌법보호법 제5조 제2항 제11호 1문은 비례성 원칙을 충족하지 못하고 있다. 비례성 원칙은 기본권 침해가 정당한 목적을 달성하여야 하며, 이러한 목적 달성에 적합하고 필요한 수단을 사용해야 한다.

헌법보호법에 규정하고 있는 정보 수집은 헌법보호기관이 헌법보호법 제3조 제1항에 근거한 자신들의 업무 수행에 기여하고, 구체적 위험의 전 단계에서 자유민주적 기본질서와, 연방과 주의 존립 및 외국과의 관계에서 독일 연방공화국의 특정한 이익을 확보하는 데 기여한다. 동시에 헌법보호법 입법이유에 의하면, 헌법보호법의 개정으로 인해 입법목적을 추구하고 있는데, 인터넷 통신과 연결된 위험을 고려하여 헌법보호기관을 통한 효과적인 테러척결을 위한 것이다.[25]

헌법상의 평화유지 권력 및 질서유지 권력으로써 국가의 안전과 국가로부터 보호되는 시민의 생명, 신체 및 자유의 위험에 대한 안전은 헌법상의 가

22) BVerfGE 120, 274; Martin Kutscha, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042 ff.
23) BVerfGE 120, 274 (279).
24) Martin Eifert, Informationelle Selbstbestimmung im Internet - Das BVerfG und die Online- Durchsuchungen, NVwZ 2008, S. 521 ff.
25) LT-Drucks 14/2211, S. 1.

치이다. 이러한 헌법상 가치는 고도의 가치를 지닌 법익이다.[26] 국가의 기본권보호의무는 독일 기본법 제2조 제2항 1문뿐만 아니라, 독일 기본법 제1조 제1항 2문에서도 도출된다.[27] 국가는 테러 계획이나 그 밖의 계획들로 인한 위험에 대처함으로써 국가 자신의 헌법상의 과제를 수행한다. 전자적 또는 디지털 통신수단의 이용이 늘어나고 이러한 수단들이 거의 모든 생활영역에 확산됨에 따라 헌법보호기관이 그들의 업무를 효과적으로 인지하는 것이 어렵게 되었다. 또한 현대의 정보기술은 근본주의자와 테러주의자들의 테러에 밀접하게 관계되어 있고 이러한 관계를 유지하거나 범죄를 계획ㆍ예비하거나 이를 실행하기 위한 수많은 가능성이 상존하고 있다. 국가가 수사활동을 위해 정보통신기술을 이용하게 하는 입법자의 조치에는 특히 전통적인 통신형태의 무게 중심에서 전자적 통신으로 이전하려는 배경과 이러한 테러 집단들이 정보를 암호화하고 은닉할 가능성이 있다는 배경이 깔려 있다.

정보통신기술 시스템에의 비밀리에 접근은 이러한 목적을 이용하기에 적합한 수단이다. 이를 통하여 헌법보호기관이 위협적인 상황을 수사할 가능성이 존재한다. 수단의 적합성 판단에 있어서 입법자에게 상당한 평가의 여지가 허용된다. 이 사건에서 이러한 평가여지를 벗어났는지는 명확하지 않다.[28]

헌법보호법 제5조 제2항 제11호 1문에 포함되는 권한[29]은 구두변론에서 정보 전문가들에 의한 평가에 의하면 피청구인이 접근 소프트웨어의 도움으로 대상 정보통신시스템에 침입하여 접근한 경우, 이러한 접근을 효과적으로 저지하기 위한 기술적 가능성이 있는가에 따라 수단의 적합성이 인정되는 것은 아니다. 수단의 적합성 심사와 관련하여, 헌법소원심판 대상인 헌법보

26) BVerfGE 49, 24 (56 f.); 115, 320 (346).
27) BVerfGE 115, 118 (152).
28) BVerfGE 77, 84 (106); 90, 145 (173); 109, 279 (336).
29) Buermeyer, HRRS 2007, S. 154 (165 f.); Gercke, CR 2007, S. 245 (253); Hornung, DuD 2007, S. 575 (579).

호법이 허용하고 있는 조치가 통상적인 경우에만 결과 기대를 요구하지는 않는다. 헌법보호법에 규정된 수단인 접근이 특별한 경우 다른 결과를 가져올 수 있다는 입법자의 판단은 명백한 결함이 있는 것은 아니다. 또한 정보통신기술이 더욱 발전해 가는 과정에서 헌법보호기관을 위해 기술적으로 더 이상 이러한 접근을 저지할 수 없거나 저지하는데 과도한 비용을 지불해야만 한다면 정보통신시스템에 접근 가능성은 열려있다고 판단할 수 있다.

따라서 헌법보호법에 규정된 권한의 수단 적합성은 부정되지 않는다. 왜냐하면 접근의 수단으로 취득한 증거가치는 인식 가능한 수단에 한정되기 때문이다. 수집된 정보의 진정성을 기술적으로 증명하는 것은 원칙적으로 문제되는 시점에 대상 정보통신시스템의 배타적인 통제를 전제로 한다.[30] 그러나 이러한 증거 확보의 어려움이 수집된 정보에 정보가치를 부여하지 않다는 것을 의미하지는 않는다. 더욱이 헌법보호법에 규정된 조항들에 따른 온라인 접근은 형사소송을 위해 확실한 증거를 직접 획득하는 것이 아니라, 헌법보호기관이 인식해야 하는 것이다.

정보통신시스템에의 비밀리에 접근은 필요성 원칙을 위반한다. 입법자의 평가특권과 관련하여 입법자는 정보통신시스템에 있는 정보 수집과는 동일한 정도로 효과적인 수단이 되지는 않지만, 청구인에게 기본권 제한이 덜 되는 수단이어야 한다. 원칙적으로 헌법보호법에서 규정하고 있지 않은 정보통신시스템에의 비밀리에 접근과는 달리, 정보통신시스템에의 공개적인 수색은 경미한 수단으로 간주된다.[31] 그러나 헌법보호기관이 자신의 업무 수행과 관련하여 정보통신시스템의 저장매체에 있는 포괄적으로 암호화된 정보를 포함한 정보를 충분한 근거로 볼 수 있고, 장시간 동안 변경을 시도하거나 정보통신시스템의 사용을 감시할 수 있는 충분한 근거로 볼 수 있다면, 이러한 목적을 달성하는데 더 완화된 수단은 찾아보기 어렵다. 암호화된 정보 통

30) Hansen/Pfitzmann, DRiZ 2007, S. 225 (228).
31) Hornung, DuD 2007, S. 575 (580).

신의 내용에 접근하는 경우에도 전달 범위에의 접근이 성공할 가망이 없는 경우에 한하여 동일하게 해석된다.

헌법보호법 제5조 제2항 제11호 1문은 협의의 비례성 원칙도 준수하지 못하고 있다. 협의의 비례성 원칙이 요구하는 것은 전체적 평가에 있어서 기본권 침해의 중요성이 이를 정당화하는 근거의 중요성과 밀접한 관계에 있다.[32] 입법자는 기본권 제한을 통해 제한되는 개인적 법익과 그러한 제한을 통해 달성하려는 공익 간을 비교형량해야 한다. 이러한 협의의 비례성 원칙 심사에 있어서 어떠한 수단은 공익을 달성하기 위해 사용되어서는 안될 수도 있다. 왜냐하면, 이러한 수단의 투입으로 인해 제한되는 기본권이 추구하는 공익보다 더 중요하기 때문이다.[33]

헌법보호법 제5조 제2항 제11호 1문은 이러한 측면에서 법익의 균형성을 충족하지 못하고 있다. 헌법보호법에서 규정하고 있는 조치(수단)는 중대한 기본권 침해를 야기한다. 이는 헌법보호법에 규정된 침해의 근거로부터 나오는 공적인 수사이익과는 관계가 없다. 또한 기본법에서 보호되는 청구인의 이익을 고려하기 위해 절차법적인 규정도 필요하다. 이러한 법규정도 없다.

(4) 판례에 대한 평가

위 헌법소원심판은 하나는 인터넷 감시(Beobachten)와 비밀 수사(Aufklären)가 헌법적으로 정당화되는지 여부와 관련된 것이고, 또 다른 하나는 정보통신시스템에의 비밀리 접근이 헌법적으로 허용되는지의 문제이다. 노르트라인-베스트팔렌 주 헌법보호법 제5조 제2항 제11호에 규정된 '기술적 침입을 통한 정보통신시스템에의 비밀리 접근'은 '정보통신시스템의 기밀성과 완결성 보장'에 관한 기본권으로서 '일반적 인격권'을 제한하고 있다고 판시하였다. 일반적 인격권은 헌법상 인격을 구성하는 의미에서 인격의 구성요소를

32) BVerfGE 90, 145 (173); 109, 279 (349 ff.); 113, 348 (382); st. Rspr.
33) BVerfGE 115, 320 (345 f.).

보장하고 있다.[34] 특히 과학기술의 발전과 생활여건의 변화 과정에서 발생할 수 있는 새로운 형태의 위험 또는 리스크에 대비하기 위하여 기존 기본권으로 보장되지 않는 기본권의 흠결을 해소하기 위해 새로운 기본권인 '정보통신시스템의 기밀성과 완결성 보장'에 관한 기본권을 형성한 것이다.[35]

독일 연방헌법재판소는 온라인 수색 판결에서 '정보통신시스템의 기밀성과 완결성을 보장'하는 새로운 기본권, 즉 '컴퓨터 기본권'을 창설했다. 이 판례는 일반적 인격권 중에 '자기보호권'과 관련된 것이다. 독일 기본법 제1조 제1항과 관련된 기본법 제2조 제1항에서 도출된 일반적 인격권은 과학기술 발전과 변화하는 생활여건에서 발생할 수 있는 새로운 위험이나 리스크로부터 보호하는 기본권이다.[36] 온라인 수색의 경우, 기존 개인정보자기결정권, 통신의 비밀 보호, 주거의 보호 등의 기본권으로는 이 문제를 해결할 수 없다.[37] 정보통신시스템이 점점 일상생활의 중심이 되고 개인의 인터넷 사용 의존도가 높아짐에 따라 개인정보를 정보통신시스템에 위탁하거나 사용을 위해 불가피하게 개인정보를 시스템에 제공한다.[38] 기본권의 보호영역은 이러한 목적을 위해 개인이 사용하는 정보통신시스템을 포함하게 된다. 정보통신시스템에서 개인정보 수집의 필요성을 능가하는 정보주체의 인격권 비중이 큰 반면, 잠재적으로 상당히 중요하고 의미 있는 데이터 베이스(database) 구축의 필요성이 있을 때 문제는 복잡해진다.[39] 정보통신시스템은 그 자체를 보호하는 것이 아니라 인격권 발현과 관련된 범위에서만 보호된다.[40] 여

34) BVerfGE 99, 185 (193); BVerfGE 114, 339 (346).
35) BVerfGE 54, 148 (153); BVerfGE 65, 1 (41); BVerfGE 118, 168 (183).
36) BVerfGE 54, 148 (153); 65, 1 (41); 118, 168 (183); 120, 274 (303). Roβnagel/Schnabel, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534.
37) Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informtionstechnischer Systeme, JZ 2008, S. 1009 (1015 f).
38) BVerfGE 120, 274 (312 f).
39) BVerfGE 120, 274 (312 f).
40) Hoffmann-Riem, JZ 2008, S. 1009 (1012); Eifert, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 (522).

기서 정보통신시스템이 처리하고 저장하는 정보는 사용자의 특성과 행동을 재식별할 수 있는 개인정보를 말한다.[41]

온라인 수색 판결에서 독일 연방헌법재판소가 판시하고 있는 '정보통신시스템의 기밀성과 완결성 보장'이라는 '컴퓨터 기본권'을 새롭게 형성할 필요가 없다는 견해가 있다.[42] 컴퓨터 기본권이라는 새로운 기본권을 창설할 필요 없이 개인정보자기결정권의 보호영역을 확장하게 되면, 이러한 기본권의 흠결을 보충하게 된다는 것이다. 또한 '컴퓨터 기본권'이라는 기본권 창설은 헌법소원심판에서 '기본권 침해성' 여부를 충족(독일 기본법 제93조 제1항 제4a호)하기 위한 헌법소원심판의 적법요건을 충족하기 위한 '절차적 의미' 밖에 없다는 견해도 있다.[43] 독일 연방헌법재판소는 위 헌법소원심판에서 기본권 침해를 판단하기 위해 새로운 기본권인 컴퓨터 기본권(IT 기본권)을 형성해야만 했던 '절차적 의미'만 있을 뿐, 컴퓨터 기본권(IT 기본권)으로부터 '실체법적 의미'는 도출되지 않는다는 것이다.[44]

Ⅲ. 사이버안전과 인격권 보호

1. 사이버안전 보장

(1) 사이버안전을 위한 국가의 의무

오늘날 인터넷상 발생하는 개인의 인격권이나 개인정보자기결정권 침해의 위험이나 리스크를 제어ㆍ감소시키기 위해 법적 조치가 강구되어야 한다.

41) BVerfGE 120, 274 (314).

42) W. Hoffmann-Riem, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, AöR 134 (2009), S. 532.

43) O. Lepsius, Das Computer-Grundrecht: Herleitung-Funktion-Überzeugungskraft, Online-Durchsuchung, Berlin, 2008, S. 21 ff. (36 f.).

44) 김태오, "사이버안전의 공법적 기초",「행정법연구」 제45권, 행정법이론실무학회, 2016. 6., 119면; 이부하, 앞의 논문, 157면.

그러나 인터넷이나 정보통신시스템에서 발생하는 위험이나 리스크는 그 발생을 예측하기 어려운 측면이 있다. 사이버안전 사고가 발생하면 그 사고에 대한 책임을 지는 사람은 두려움으로 인해 발생한 사고를 공개하지 않으려 한다. 따라서 사이버안전 사고 발생에 대한 인지를 신속하게 할 수 있는 법적 규율이 중요하다. 또한 국가 차원에서 국민의 안전권이나 기본권 보호를 위해 정보통신시스템을 관리할 의무도 있다.

위 독일 연방헌법재판소의 헌법소원심판처럼 인터넷이나 정보통신시스템에서 발생하는 위험이나 리스크를 관리하기 위한 법규범은 명확성 원칙과 비례성 원칙을 준수해야 한다. 사이버안전을 위해 법 규정시 개인정보(특히 민감정보)와 관련하여 사후 통지절차 규정 마련, 사전 통제수단 확보가 중요하다.[45] 사이버안전과 관련한 법적 규율은 사이버공격과 위협이라는 일종의 불확실성에 대응하는 리스크 관리라는 특징이 있다. 이에 대하여 국민의 안전 보호를 위해 헌법 제37조 제2항의 국가안전보장이나 질서유지의 목적으로 법률로써 제한해야 한다.

(2) IT 기본권과 IT 시스템 보호

독일 연방헌법재판소는 'IT 시스템의 기밀성 및 완결성 보장에 대한 기본권'(Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnicher System)을 인정하였다. 독일 연방헌법재판소에 의하면, 이른바 IT 기본권은 추가적인 정보 수집이나 가공조치 없이도, 잠재적으로 대규모 정보가 조달될 수 있는 상황에서 개인정보자기결정권으로 이러한 위협에 대처할 수 없으므로, 독일 기본법 제2조 제1항에 근거하고 있는 일반적 인격권으로부터 나오는 정보통신시스템의 기밀성과 완결성을 보장하는 기본권을 도출하고 있다. IT 기본권의 내용은 IT 시스템이 생산하고 처리하

45) 헌재 2022. 7. 21. 선고 2016헌마388, 2022헌마126(병합), 2022헌마105, 110(병합).

며 저장한 정보의 기밀이 유지되기를 바라고 이를 신뢰하고 이용하는 IT 시스템 이용자의 이익을 보호하는 것이다. 더불어 IT 기본권의 보장은 개인정보자기결정권과 밀접한 관계에 있지만, 개인정보자기결정권을 넘어서서 개인정보의 수집으로 인한 기본권 침해를 넘어서는 IT 시스템에 높은 의존도로 인한 기본권에 대한 잠재적인 위험이나 리스크로부터 보호하려는 것이다. 즉, 개인정보자기결정권을 넘어서는 IT 시스템의 안전성을 확보하려는 것이다.[46]

2. 사이버안전을 위한 조치

정보통신시스템상에서 위험이나 리스크를 관리한다고 하더라도, 개인이나 기업이 스스로 자율적으로 관리하고 이에 대해 정부의 권고 수준을 상회하는 정부개입이 가능하다. 디지털 시대에는 사전적 통제나 현재적 통제를 우선시할 필요가 있다. 디지털 시대에 내재하는 위험이나 리스크가 현실화되지 않도록 예방적인 조치가 필요하다. 예를 들어, 과학기술윤리제도를 도입하여 자율 규제를 하거나 영향평가제도를 사전에 도입하여 관리하는 방식이다.[47]

침해사고 발생시 정보통신서비스 제공자는 정보보호 최고책임자를 구성원으로 하는 '정보보호 최고책임자 협의회'를 구성ㆍ운영할 수 있다고 규정하고 있다. 이는 재량규정으로 만약 이를 구성ㆍ운영하지 않는다면 이를 강제할 방법이 없다. 현재 정보통신망법상의 이러한 자율적 조치만으로는 효과적인 사이버안전을 달성하기 어렵다. 사이버안전을 위해 실질적이고 실효성있는 법률 규정이 필요하다.

---

46) 박재윤, "사이버보안법의 공법적 체계에 관한 소고", 「경찰법연구」 제16권 제2호, 한국경찰법학회, 2018, 126면.

47) 양천수, "지능정보기술의 위험과 법적 대응 방안 - 알고리즘에 대한 대응을 중심으로 하여 -", 「법학연구」 제32권 제1호, 충북대학교 법학연구소, 2021. 6., 373면.

3. 디지털 시대에 인격권 보호

일반적 인격권은 독일 기본법 제2조 제1항과 관련한 '인격의 발현을 존중할 권리'로서 나타나며, 다른 기본권보다 특별한 기본권이다.[48] 일반적 인격권은 '헌법에 규정되지 않은 기본권'[49]으로서 과학기술의 발전과 생활환경의 변화 속에서 나타나는 새로운 유형의 위험이나 리스크에 대처하는 명문 기본권의 흠결을 보충해 주는 특별한 기본권이다.[50] 독일 연방헌법재판소는 과학기술의 발전 속에서 일반적 인격권의 중요성을 강조하고 있다. 디지털 대전환(digital transformation) 시대에 일반적 인격권은 과학기술의 발전에 따라 발생하는 새로운 유형의 위험이나 리스크에 대비한 기본권 흠결을 보충해 주는 보충적 기본권이다.[51] 개인의 인격 발현을 위해서 개인은 정보통신시스템 사용에 의존할 수밖에 없는 상황에서 헌법이나 법률에서 인격에 대한 위험이나 리스크를 보호할 적절한 조치를 취하지 않는다면, 이는 국가가 국민의 기본권 보장의무를 해태하는 것이다. 따라서 정보통신시스템의 완결성과 기밀성을 보장하고, 개인의 인격 발현을 보장하기 위해 일반적 인격권은 기본권으로 보장된다.[52]

Ⅳ. 결 론

디지털 시대에는 인격권 침해나 개인정보의 침해 등 위험이나 리스크가

48) Dreier, in: Ders. (Hrsg.), GG, Bd. 1, Art. 2 Abs. 1 Rn. 64; H. Kube, Persönlichkeitsrecht, in: Isensee/Kirchhof (Hrsg.), HStR VII, § 148 Rn. 35.
49) BVerfGE 54, 148 (153).
50) BVerfGE 118, 168 (183); 120, 274 (303).
51) BVerfGE 114, 339 - Mehrdeutige Meinungsäusserungen; BVerfGE 120, 274 - Online-Durchsuchungen; BVerfGE 120, 378 - Automatisierte Kennzeichenerfassung; BVerfGE 138, 377 - Mutmaßlicher Vater; BVerfGE 153, 182 - Zuizidhilfe
52) BVerfGE 120, 274 (313).

크게 증가하고 있다. 독일 연방헌법재판소는 온라인 수색 판결을 통해 정보통신시스템에의 비밀리 접근과 인터넷 비밀 수사 그리고 은행계좌의 내용 및 계좌의 입출금 상태의 수집에 대한 헌법적 판단을 하였다. 독일 연방헌법재판소는 이 사건에서 기존에 독일 기본법상의 사생활 보호, 개인정보자기결정권, 통신의 비밀에 의해 보장되지 않으며, '정보통신시스템의 기밀성 및 무결성 보장'이라는 새로운 기본권을 형성해냈다. 독일 연방헌법재판소는 일반적 인격권에서 자기보호권, 자화상의 권리, 자기결정권이 파생된다고 판시하고 있다. 일반적 인격권 중 자기보호권과 관련하여 '정보통신시스템의 기밀성과 완결성 보장'에 관한 기본권이 도출된다고 말한다.

IT 기본권은 IT 시스템이 생산하고 처리하며 저장한 정보의 기밀이 유지되기를 바라고 이를 신뢰하고 이용하는 IT 시스템 이용자의 이익을 보호하고자 하는 것이다. IT 기본권 보장은 개인정보자기결정권과 밀접한 관계에 있지만, 개인정보자기결정권을 넘어서서 개별적인 개인정보의 수집으로부터 발생하는 피해를 상회하는 IT 시스템에 대한 높은 의존도로 인하여 발생하는 기본권 주체에 대한 잠재적인 위협에 따른 기본권의 침해를 보호하는 것이고, 개별적인 개인정보 보호를 넘어서 'IT 시스템 자체'에 대한 보호를 하는 것이다.

인터넷이나 정보통신시스템에서 발생하는 위험이나 리스크 발생으로 인한 기본권 침해를 방지하기 위해 국가는 입법적 조치를 취하여야 한다. 그러한 입법은 인터넷이나 정보통신시스템에서 발생하는 위험이나 리스크를 방지하기 위한 수단을 담고 있어야 한다. 이러한 법규범상의 수단은 헌법상 명확성 원칙과 비례성 원칙을 준수해야 한다.

〈참고문헌〉

권형둔, “디지털 전환의 시대 언론의 자유 보장과 인격권 보호 사이의 균형 모색”, 「미디어와 인격권」 제7권 제3호, 언론중재위원회, 2021.

김정수 · 엄주희, “디지털 시대의 소외와 포용, 그리고 공법적 대응”, 「법과 사회」 제71호, 법과사회이론학회, 2022.

김태오, “사이버안전의 공법적 기초”, - 독일의 IT 기본권과 사이버안전법을 중심으로 -”, 「행정법연구」 제45권, 행정법이론실무학회, 2016.

박재윤, “사이버보안법의 공법적 체계에 관한 소고”, 「경찰법연구」 제16권 제2호, 한국경찰법학회, 2018.

양천수, “지능정보기술의 위험과 법적 대응 방안 - 알고리즘에 대한 대응을 중심으로 하여 -”, 「법학연구」 제32권 제1호, 충북대학교 법학연구소, 2021.

이부하, “일반적 인격권에 대한 헌법적 고찰”, 「미디어와 인격권」 제8권 제3호, 언론중재위원회, 2022.

M. Eifert, Informationelle Selbstbestimmung im Internet, NVwZ 2008, S. 521 ff.

W. Hoffmann-Riem, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informtionstechnischer Systeme, JZ 2008, S. 1009 ff.

W. Hoffmann-Riem, Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation, AöR 134 (2009), S. 532 ff.

M. Hofmann, Die Online-Durchsuchung? staatliches Hacken oder zulässige Ermittlungsmaβnahme? NStZ 2005, S. 121 ff.

M. Kutscha, Verdeckte „Online-Durchsuchung” und Unverletzlichkeit der Wohnung, NJW 2007, S. 1169 ff.

M. Kutscha, Mehr Schutz von Computerdaten durch ein neues Grundrecht?, NJW 2008, S. 1042 ff.

O. Lepsius, Das Computer-Grundrecht: Herleitung-Funktion-Überzeugungskraft, in: Fedrik Roggan (Hrsg.), Online-Durchsuchung, Berlin, 2008, S. 21 ff.

Roßnagel/Schnabel, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme und sein Einfluss auf das Privatrecht, NJW 2008, S. 3534 ff.

Sachs/Krings, Das neue Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, JuS 2008, S. 481 ff.

【국문초록】

디지털 시대에 인격권 보호

이 부 하*

독일 연방헌법재판소의 온라인 수색 판결은 정보통신시스템에서 다양한 정보를 수집할 수 있는 헌법보호기관의 권한을 규율하고 있고, 수집된 정보 처리를 규율하고 있는 노르트라인-베스트팔렌 주(州) 헌법보호법(VerfSchutzG NRW)의 조항에 대한 헌법소원심판 사건이었다. 독일 연방헌법재판소는 온라인 수색 판결에서 '정보통신시스템의 기밀성과 완결성을 보장'하는 새로운 기본권, 즉 '컴퓨터 기본권'(소위 'IT 기본권')을 창설해냈다. 이러한 '컴퓨터 기본권'(소위 'IT 기본권')은 일반적 인격권에 근거하고 있다. 일반적 인격권 보호영역 중 자기보호(自己保護)가 있다. '자기보호'란 '프라이버시권'(privacy right)에서 나오는 '혼자 있을 권리'라는 사생활 보호다. 독일 연방헌법재판소는 온라인 수색 판결에서 컴퓨터 기본권은 일반적 인격권 중 자기보호권에서 도출된다고 한다.

독일 연방헌법재판소의 온라인 수색 판결에서처럼 인터넷이나 정보통신시스템에서 국가의 행위를 규율하는 법규범은 비례성 원칙을 준수해야 한다. 정보통신시스템에의 비밀리에 접근은 필요성 원칙(침해의 최소성 원칙)을 위반한다. 또한 헌법보호법 제5조 제2항 제11호 1문은 법익의 균형성도 충족하지 못하고 있다. 헌법보호법에서 규정하고 있는 수단은 중대한 기본권 침해를 야기하는 반면, 헌법보호법에 규정된 수단에 의해 제한되는 사익 보다 공적인 수사이익은 적기 때문이다.

IT 기본권의 내용은 IT 시스템이 생산하고 처리하며 저장한 정보의 기밀이

* 영남대학교 법학전문대학원 교수.

유지되기를 바라고 이를 신뢰하고 이용하는 IT 시스템 이용자의 이익을 보호하는 것이다. IT 기본권 보장은 개인정보자기결정권과 밀접한 관계에 있지만, 개인정보자기결정권을 넘어서서 개별적인 개인정보의 수집으로부터 발생하는 피해를 상회하는 IT 시스템에 대한 높은 의존도로 인하여 발생하는 기본권 주체에 대한 잠재적인 위협에 따른 기본권의 침해를 보호하는 것이다. 또한 개별적인 개인정보 보호를 넘어서 'IT 시스템 자체'에 대한 보호를 하는 것이다.

주제어: 디지털 시대, 인격권, 정보통신시스템, 사이버안전, 리스크

【ABSTRACT】

Protection of Personal Rights in the Digital Age

Lee, Boo-Ha*

The German Federal Constitutional Court's online search ruling governs the authority of the constitutional protection body to collect various information from information and communication systems, and the North Rhine-Westphalia State Constitutional Protection Act, which regulates the processing of collected information. (VerfSchutzG NRW) was a constitutional complaint case. The German Federal Constitutional Court created a new fundamental right, namely 'computer fundamental rights' (so-called 'IT fundamental rights'), which 'guarantees the confidentiality and integrity of information and communication systems' in its ruling on online search. These 'fundamental rights to computers' (so-called 'fundamental rights to IT') are based on general personal rights. Among the areas of protection of general personal rights, there is self-protection. 'Self-protection' is the protection of privacy, which is the 'right to be alone' that comes from the 'privacy right'. The German Federal Constitutional Court said in its ruling on online search that the basic computer right derives from the right to self-protection among general personality rights.

As in the ruling of the German Federal Constitutional Court on online search, the legal norms governing state behavior on the Internet or information and communication systems must comply with the principle of proportionality. Covert access to information and communication systems violates the principle of necessity (the principle of least infringement). In addition, Article 5, Section 2, Number 11, Sentence 1 of the Constitutional

* Professor, Yeungnam University Law School.

Protection Act does not satisfy the balance of legal interests. The methods stipulated in the Constitutional Protection Act cause serious violations of fundamental rights, but the public investigative interest is less than the private interests that are limited.

The content of the fundamental rights of IT is to protect the interests of IT system users who trust and use the information that the IT system produces, processes, and stores in hopes that the confidentiality will be maintained. Although the guarantee of the IT fundamental rights is closely related to the right to self-determination of personal information, it protects against infringement of fundamental rights beyond the right to self-determination of personal information to the potential threat to the subject of fundamental rights arising from the high dependence on the IT system that exceeds the damage caused by the collection of individual personal information. In addition, it is to protect the 'IT system itself' beyond individual personal information protection.

Keywords : digital age, personal rights, information communication system, cyber safety, risk