해킹으로 인한 자율주행자동차 사고 관련 책임 법제에 관한 연구 -민사상, 형사상, 행정책임 중심으로-

안 명 구*, 박 용 석**

요 약

최근 4차 산업혁명이 화두로 등장하면서 자율주행자동차의 중요성과 관심이 높아지고 있다. 전 세계적으로 시험 운행이 늘어나면서 자율주행자동차와 관련된 사고도 발생하고 있으며, 이에 대한 사이버 해킹 위협 가능성도 높아지고 있다. 미국, 영국, 독일을 포함한 여러 국가들은 이러한 추세를 반영하여 자율주행자동차의 사이버 해킹에 대응하기 위한 가이드라인을 만들거나 기존의 법률을 개정하고 있다. 국내의 경우 자율주행자동차의 제한적인 임시운행이 이루어지고 있으나, 자율주행자동차 해킹으로 인한 사고 발생 시 적용할 법제가 미흡한 상태이다. 본고에서는 기존의 관련 법률 체계를 분석하고 이를 바탕으로 자율주행자동차 사이버 해킹으로 인한 민사, 형사, 행정 책임 문제를 살펴보면서, 자율주행자동차 특성에 맞는 사고 책임 관련 법률체계를 제안하고 각 법제의 구성요소에 대해서 분석하여 이슈사항을 도출하며, 추가적으로 간략한 개선방안도 제시한다.

Civil liability and criminal liability of accidents caused by autonomous vehicle hacking

Myeonggu An*, Yongsuk Park**

ABSTRACT

As the 4th industrial revolution has recently become a hot topic, the importance of autonomous vehicles has increased and interest has been increasing worldwide, and accidents involving autonomous vehicles have also occurred. With the development of autonomous vehicles, the possibility of a cyber-hacking threat to the car network is increasing. Various countries, including the US, UK and Germany, have developed guidelines to counter cyber-hacking of autonomous vehicles, In the case of Korea, limited temporary operation of autonomous vehicles is being carried out, but the legal system to be applied in case of accidents caused by vehicle network hacking is insufficient. In this paper, based on the existing legal system, we examine the civil liability caused by the cyber hacking of the autonomous driving car, while we propose a law amendment suited to the characteristics of autonomous driving car and a legal system improvement plan that can give sustainable trust to autonomous driving car.

Keywords : Automatic Vehicle Accident, Hacking, Vehicle Network, Cyber Security Threats

접수일(2018년 11월 28일), 수정일(1차: 2019년 12월 24일, 2차: 2019년 3월 26일), 게재확정일(2019년 3월 29일)

*세종사이버대학교 정보보호대학원
**세종사이버대학교 정보보호대학원(교신저자)

1. 서 론

자율주행자동차의 기술발전이 이루어질수록 사이버 보안 위협에 노출될 가능성이 커지는 만큼 해킹에 의한 자율주행자동차 사고 발생에 대비한 책임법제에 대한 새로운 법리와 기존 법제에 대한 개정이 필요하다. 구체적으로는 해킹으로 인한 자동차 공격에 따른 책임 분석이 필요하며, 이와 함께 기존 법리에 대한 분석이 요구되며, 또한 개선사항 분석도 필요하다. 따라서 본고에서는 주요 관계법인 민사법, 형사법, 행정법을 중심으로 책임법제를 분석하고 또한 자율주행자동차의 특성에 맞는 새로운 법리 및 법제를 추가적으로 간략히 제안하여 자율주행자동차 해킹으로 인한 사고 발생 시 피해자에 대한 신속한 손해배상과 사고 발생을 방지하기 위한 목표로 국민의 기본권 보호와 지속가능한 자율주행자동차 사고 책임 관련 법률체계에 일조함으로써 자율주행자동차 상용화에 기여하고자 한다. 구체적으로는 해킹으로 인한 자동차 공격에 따른 책임을 분석하고 국내외 자율주행자동차 사고 책임을 비교하였고, 해킹에 의한 자동차 사고의 민사법적 규율, 형사법적 규율, 행정 책임 및 예방수단에 대한 간략한 개선방안을 제시하였다. 추가적으로 자율주행자동차와 일반 자동차 교통사고에 대한 비교를 하였고, 해킹에 의한 자율주행자동차 사고에 따른 책임 소재에 관한 소결을 하였다.

2. 선행연구

해킹에 의한 사고 발생 시 손해배상책임에 관한 연구로는 전자금융사기를 중심으로 한 은행의 손해배상책임에 관한 연구를 한 논문[1]과 개인정보 유출에 관한 SK컴즈 사건을 중심으로 손해배상책임에 관한 연구를 한 논문[2]이 있다. 사이버 보안 단계별 법제도에 대해 미국과 한국을 비교한 연구[3]가 있으며, 핀테크 활성화를 위한 보안과 법제도에 관한 연구[4]가 있다. 국내외 자율주행자동차 법률체계를 비교 분석하여 해외 법률 체계에 대한 연구가 이루어졌으며, 해외 선진국가의 특장점을 도출한 논문이 있다.[5] 본 연구에서는 해당 논문[5]을 바탕으로 해킹에 의한 자율주행자동차 사고 시 책임법제에 대한 연구를 진행하고자 한다. 다만 자율주행자동차 사고에 따른 민사책임과 관련된 문제를 현행 민사법 중심으로 어떻게 적용할지에 대해서 연구한 논문[6]과 형사책임과 관련된 문제를 현행 형사법을 중심으로 어떻게 적용할지에 대해서 연구한 논문[7]을 통해 자율주행자동차 사고에 대한 책임 법제에 대한 연구가 진행되었고 자율주행자동차 교통사고 발생 시 어떤 식으로 보험 제도를 적용할지에 대한 연구[8]가 진행되었지만 자율주행자동차 해킹에 의한 사고의 책임법제에 대한 연구는 진행되지 않았다.

본 연구에서는 자율주행자동차 해킹 사고에 대한 책임법제를 제안하며 특히 국민의 기본권이 보호되면서 자율주행자동차의 활성화를 목적으로 한다.

3. 해킹으로 인한 자동차 공격에 따른 책임 분석

해킹으로 인한 자동차 공격의 경우 다양한 원인을 통해 일어날 수 있다. <표1>에서는 참고문헌[9]에서 대표적인 사례를 기반으로 재구성하였다. <표1>의 예시와 같이 자동차 해킹 사례는 다양하다.

<표2>에서는 해킹으로 인한 자동차 공격의 유형을 여섯 가지로 나누어 각 유형별로 형사책임과 민사책임 그리고 행정처분 대상자에 대한 분석을 하였다. 첫 번째로 운전자의 고의 또는 과실로 인한 사고유형이다. 자율주행시스템을 임의로 조작하거나 변경하는 경우에 새로운 보안 취약점이 발견되어 해킹이 발생할 수 있는 유형이다. 두 번째로 차량의 하드웨어 결함에 의한 유형이다.

<표1> 자동차 공격 사례

개요(년도)	공격방법	대상
테슬라 원격 해킹(2016)	차량용 웹브라우저 취약점 이용 악의적 AP에 접속 및 악성코드 설치 유도차량 원격 제어	CAN-Top roof, seat, wiper and break system
Jeep 해킹(2016)	OBD II를 통하여 변조된 FW를 타겟 ECU에 주입	OBD-II
미스비씨 아웃랜더 PHEV 해킹 (2016)	차량 Wi-Fi 접속 구간에서 PSK 크래킹, 바이너리프로토콜 분석, MITM 등을 통한 차량 제어권 획득	프라이버시 (위치정보), 헤드라이트, 원격 잠금/해제, 공조장치 조작, 경보
앱 리패키징 공격(2015)	스마트폰용 텔레매틱스 앱을 위변조, 변조된 앱을 통한 차량 도어락 임의 제어	CAN-도어락
GM Onstar 해킹(2015)	OwnStar라는 도청장치를 부착, 도청정보를 분석하여 원격 제어 메시지 전송	Infotainment system
도요타 프리우스 해킹 (2013)	CAN 버스 리버스 엔지니어링OBD-II 포트를 통한 통신데이터 모니터링 및 분석 (DARPA 프로젝트)	CAN
TPMS 취약점 공격 (2010)	TPMS 통신 데이터 수집 프로토콜 분석 TPMS 센서와 ECU간의 통신 도청 차량의 움직임 추적, ECU 전송 데이터 변조	TPMS(Tire pressure monitoring system)

자율주행자동차의 경우 하드웨어와 소프트웨어 시스템이 연결된 상태인 만큼 하드웨어의 결함이 소프트웨어에 영향을 주어 해킹이 발생할 수 있다.

<표2> 해킹으로 인한 대표 사고발생 유형 예시와 책임

대표 사고유형	사고원인요소	민사책임	형사책임	행정처분 대상
운전자의 고의 또는 과실	자율주행시스템 미 관리 혹은 임의변경	운전자 혹은 운행자	운전자	운전자
차량의 하드웨어 결함 혹은 오류	차량의 하드웨어 결함	차량 제조사	차량 제조사 혹은 관련 임직원	차량 제조사 혹은 관련 임직원
차량의 소프트웨어 오류 혹은 오작동	차량의 소프트웨어 결함 혹은 오류	차량 소프트웨어 개발사	차량 소프트웨어 개발사 혹은 관련 임직원	차량 소프트웨어 개발사 혹은 관련 임직원
통신망 시스템 결함 또는 오류	통신망 시스템 결함 혹은 오류	통신회사 (ITS회사 포함)	통신회사 (ITS회사 포함) 혹은 관련 임직원	통신회사 (ITS회사포함) 혹은 관련 임직원
인증 또는 표준 취약점	인증체계 또는 인증기준의 보안 취약점	국가 혹은 인증기관	인증기관 혹은 인증심사원	인증기관 혹은 인증심사원
지능형 교통시스템 결함 또는 오류	지능형 교통시스템의 결함 혹은 오류	국가 혹은 도로 관련 공기업 (민자 사업자 포함)	도로 관련 공기업 (민자 사업자 포함) 혹은 관련 임직원	도로 관련 공기업 (민자사업자 포함) 혹은 관련 임직원

(*<표2>는 참고문헌[9]의 내용 중 11페이지 그림 13의 자동차 사고원인 유형분석과 12페이지 그림 14의 자동차 보안 위협에 대한 공격 경로를 바탕으로 재구성함)

세 번째로 소프트웨어 결함에 관한 유형이다. 소프트웨어 결함이나 오류로 인해 취약점으로 인해 해킹이 발생할 수 있는 유형이다. 네 번째로 통신망 시스템 결함에 관한 유형이다. 자율주행자동차는 통신망을 이용하여 차량 간의 통신을 하게 된다. 통신망에 대한 오류나 결함으로 인해 해킹으로 인하여 사고가 일어날 수 있는 유형이다. 다섯 번째로 인증 또는 표준의 취약점으로 인한 유형이다. 자율주행시스템 정보보안에 대한 인증기준 또는 표준의 취약점으로 인하여 해킹이 발생할 수 있는 유형이다. 여섯 번째로 지능형 교통 시스템의 결함에 관한 유형이다. 자율주행자동차의 경우 도로에 설치되어 있는 지능형 교통시스템의 정보를 바탕으로 시스템이 판단을 내리는데 지능형 교통시스템의 결함이나 오류로 인한 해킹으로 인해 사고가 일어날 수 있는 유형이다.

<표1>에서 보듯이 해킹은 다양하게 벌어 질 수 있으며, <표1> 외에도 더 많은 해킹 사례는 나올 수 있다. <표2>는 참고문헌[9] 내용을 바탕으로 재구성하였으며, 이는 더 많은 해킹사례로 추가 또는 업데이트 될 수 있다. 또한 법리나 법률해석에 따라 달라질 수 있으나 자율주행자동차가 상용화되었을 경우 대표적으로 일어날 수 있는 사고발생 유형에 대해서 우선적으로 정리하여 <표2>가 재구성되었다.

4. 국내외 자율주행자동차 사고 책임에 관한 비교

먼저 현행 국내 법률체계와 해외 법률체계의 비교를 통해 자율주행자동차 사고 원인에 따른 책임에 관한 차이점을 미국, 영국, 독일, 한국으로 나누어 각 나라의 법률체계를 정리하여 아래의 같은 <표3>으로 간략 비교하였다.

<표3> 국내외 자율주행자동차 사고 책임 법률적 해석 비교

	한국	미국	영국	독일
일반사고	운행자 혹은 운전자 책임	운행자 혹은 운전자 책임	운행자 혹은 운전자 책임	운행자 혹은 운전자 책임
결함에 의한 사고	명확한 규정 없음	차량 제조업체 책임	차량 제조업체 책임	차량 제조업체 책임
해킹에 의한 사고	명확한 규정 없음	해커 / 차량 제조업체 책임(조건부)	해커 / 차량 제조업체 책임(조건부)	해커 / 차량 제조업체 책임(조건부)
제조물 책임의 입증	운행자 혹은 운전자	차량 제조업체	차량 제조업체 책임	차량 제조업체 책임
제조물 책임 보험가입 규정	없음	있음(자율적)	있음(의무적)	있음(자율적)
제조물 책임에 따른 형사책임	민사책임으로 대체	민사책임으로 대체	민사책임으로 대체	민사책임으로 대체
일반 교통사고의 형사처벌	12대 중과실만 처벌	중대한 법규 위반만 처벌	교통법규 위반 여부에 따라 처벌	친고죄인 형법상 과실상해죄로 처벌

<표3>에서 보듯이 (해킹에 의한 사고를 포함하여) 우리나라의 경우 아직 자율주행자동차의 결함이나 해킹으로 인한 사고에 대한 책임에 관한 명확한 규정이 없으며 미국, 영국, 독일의 경우 차량 제조업체에게 많은 책임을 부여하는 규정이 존재한다. 제조물 책임의 경우 미국, 영국, 독일 모두 형사 처벌은 하고 있지 않지만 민사상 손해배상책임을 적용하는 것으로 대체하고 있다. 제조물 책임 보험의 경우 미국이나 독일의 경우 의무화되어 있지 않으나 책임 발생 시 손해배상액이 크고 과실인정의 범위가 넓어 자율적으로 보험에 가입하고 있다. 영국의 경우 자율주행자동차에 한해서는

차량 제조업체의 책임을 담보하기 위해서 보험에 가입하도록 하고 있다. 따라서 우리나라의 경우도 운행자 또는 운전자 책임으로 되어 있는 교통사고 책임을 특히 해킹에 의한 사고 유형에 따라 차량 제조업체, 차량 소프트웨어 개발사, 국가, 공공기관, 인증기관에게 책임을 부여하고 차량 제조업체의 보험 가입을 의무화시켜야 한다.(관련 조항 : 자동차손해배상보장법 제5조)

5. 자율주행자동차 해킹 사고의 민사법적 규율

5.1 민사상 손해배상책임의 주체

현재 인신사고의 경우에는 자동차손해배상보장법 제3조에 의해 자동차손해배상보장법상의 손해배상책임을 부담하고 물적 사고의 경우 자동차손해배상보장법 제4조에 의하여 민법상의 불법행위책임을 부담한다. 하지만 사이버 해킹으로 인하여 자율주행자동차의 인신사고(사망 또는 부상)와 물적 사고가 발생할 경우 운행자의 의지가 아닌 외부의 위협으로 인한 사고이므로 운행자의 요건 중에 하나인 운행지배가 해킹 이후부터는 사라진다. 따라서 자율주행시스템을 만든 차량 제조업체가 운전자를 비롯한 피해자의 손해에 대해 배상책임을 부담하여야 한다. 물론 자율주행시스템 자체를 1개의 회사가 아닌 여러 회사가 협력하여 개발하였을 경우 그 책임 소재를 가리기 힘든 만큼 최종적으로 만든 차량 제조업체에게 1차적인 손해배상책임 의무를 부여하여 피해자와 운전자의 손해에 대해서 신속한 손해배상이 이루어지도록 해야 한다. 차량 제조업체가 아닌 협력업체의 과실이 인정될 경우 과실 비율에 따라 2차적인 책임을 부여하여야 한다.

다만 운행자가 임의로 차량 소프트웨어를 변경하였거나 필수적이고 중요한 업데이트를 하지 않았을 경우와 해킹에 대한 공모나 방조 같은 고의가 있는 경우에는 차량 제조업체의 책임을 감경 또는 면책해 주고, 운행자에게 전자의 경우 자동차손해보장법상의 손해배상책임을 부담하도록 하고 후자의 경우 민법상의 불법행위 책임을 부담하도록 해야 한다.(관련 조항 : 자동차손해배상보장법 제4조)

5.2 차량제조업체의 입증책임 전환

현행 자동차손해배상보장법은 제3조 단서규정에 규정된 면책사유를 제외하고는 가해자에게 책임을 부여하는 조건부 무과실책임을 부여하고 있다. 해킹으로 인한 자율주행자동차 사고의 경우 해커에게 직접적인 책임이 있는 만큼 간접적인 책임이 있는 차량 제조업체에게 조건부 무과실책임을 부여할 수는 없고 과실이 있는 경우에만 책임을 인정해야 한다. 해킹으로 인한 인신사고와 물적 사고가 발생할 경우 운행자에게 제조업체의 과실에 대해 입증하도록 하면 개인의 입장에서 기업의 과실을 입증하기 어려워 실질적인 손해배상책임을 운행자가 부담하는 경우가 발생하게 된다.

해킹에 의한 사고 발생에 대해 제조물 책임법을 적용할 경우에도 정상적인 상태가 아닌 외부의 위협에 의한 비정상적인 상태에 의한 사고이므로 현행 제조물 책임법 제3조의 2 규정을 적용하기 어렵다. 또한 운행자 혹은 피해자가 차량 제조업체를 상대로 제조물 책임을 입증해야 하는 부담이 있으며 소프트웨어에 대한 명확한 규정이 없어 자율주행시스템에 대한 제조물 책임법 적용이 어려울 수 있으므로 해당 관련 제2조와 제3조의 2 조항의 개정을 통해 명확한 기준이 필요하다. 현재 소프트웨어를 제조물의 정의(제조물 책임법 제2조)에 포함하는 제조물 책임법 개정안이 국회에 계류 중이다.[10] 해킹으로 인한 자율주행자동차로 인한 사고가 발생한 경우 개인이 자율주행시스템에 대한 지식이 부족한 상태에서 차량 제조업체의 과실을 입증하기가 사실상 어려운 만큼 개인정보보호법 제39조의 손해배상책임 조항처럼 차량 제조업체가 고의 또는 중과실이 없음을 입증하도록 입증 책임의 전환이 필요하다. 다만 해킹에 의한 자율주행자동차 사고

의 경우 인신사고가 일어날 수 있는 만큼 과실 인정의 범위가 넓어야 하고 기준이 명확해야 한다.

5.3 차량 제조업체의 손해배상책임 한도

독일의 개정 도로교통법은 자율주행자동차 사고 피해자의 보호를 강화하기 위하여 독일의 경우 손해가 “고도의 혹은 전면 자율주행기능의 사용에 기하여” 발생한 경우 기존의 책임한도액을 2배로 증액하였다. (제12조 제1항 제2문)[11] 국내의 경우에도 자율주행자동차 상용화가 이루어지는 초창기에 소비자에게 지속가능한 신뢰를 주기 위해서 독일처럼 자율주행자동차 사고의 경우 예를 들어 자동차손해배상보장법 시행령 제3조를 개정하여 책임한도액을 한시적으로 올리는 방안을 고려해야 한다.

자율주행자동차 사고의 경우 산업의 발전과 경쟁력을 보호하기 위해서 과도한 징벌적손해배상책임은 도입하지 않아야 한다. 다만 해킹에 의한 자율주행자동차 사고에 차량제조업체가 공모하거나 방조, 교사하는 고의가 있거나 중과실이 있을 경우에는 민법상의 불법행위에 의한 손해배상책임을 부여하고 경과실의 경우에는 자동차손해보장법상의 손해배상책임을 부담하도록 하여 현행 일반 자동차 교통사고처럼 손해배상책임 한도액 내에서만 책임지는 유한책임으로 부담하도록 해야 한다.(관련 조항 : 자동차손해배상보장법 시행령 제3조)

유한책임으로 인한 한계를 극복하기 위해 현재 교통안전공단에서 시행하고 있는 자동차사고 피해지원 기금의 적용을 자율주행자동차 사고에도 확대 적용하는 동시에 자율주행자동차의 상용화 시기에는 차량 제조업체에게도 일정한 액수의 기금출연을 의무화하여 지원대상의 범위와 지원액을 늘리는 것이 필요하다.(관련조항 : 자동차 손해배상보장법 제30조부터 제39조의13)

5.4 차량제조업체의 사이버 보험 가입 의무화

차량 제조업체에게 자동차손해배상보장법상의 손해배상책임을 부여한다고 해도 실질적인 손해를 보상받기 위해서는 법원에 민사소송을 제기해야 한다. 피해 보상을 받기 위해 민사소송을 제기 하려면 변호사를 선임하거나 법정에 출석해야 하는 등 별도의 비용과 시간이 투입되어야 한다. 이러한 부담은 피해자에게 불리하게 작용하여 손해배상 자체가 지연되거나 정당한 손해배상액 보다 적은 금액에 합의를 하는 경우가 생길 수 있다. 피해자의 기본권 보호와 신속한 손해배상을 보장하기 위해서 차량 제조업체에게 해킹으로 인한 사고로 인한 피해를 담보하기 위한 사이버 보험 가입을 의무화해야 한다. 1차적으로 보험사가 운전자를 포함한 피해자에게 보상을 하도록 하고 차량 제조업체나 제3자의 고의 또는 중과실이 있는 경우에 보험사가 해당 업체나 제3자에게 구상금을 청구하도록 해야 한다.(관련조항 : 자동차손해배상보장법 제5조)

6. 자율주행자동차 해킹 사고의 형사법적 규율

6.1 형사책임의 주체

현행 형법에서는 형사책임을 부여할 수 있는 주체로 태어날 때부터 자연인이거나 법으로 인격을 부여한 법인이어야 한다. 따라서 자율주행시스템의 경우 사람이 개발한 하나의 소프트웨어 혹은 임베디드 시스템에 해당 되므로 해킹이 일어났다고 하더라도 자율주행시스템에 형사책임을 부여할 수 있는 주체가 될 수는 없다.

차량 제조업체의 경우 민법상 법인에 해당되는데 법인이 단독적으로 형사 책임의 주체가 될 수 있는지에 대해서는 우리나라의 통설과 판례는 부정설을 취하고 있다. 따라서 법인을 처벌하는 규정은 대부분 양벌규정의 방식에 의하고 있다. 법인의 경우 자유형 아닌 벌금형만 부과할 수 있으므로 실질적인 형사 책임의 수준이 낮다.

차량 제조업체 대표 혹은 자율주행시스템에 대한 사이버 보안을 담당하거나 시스템 개발을 총괄

하는 임원의 경우 자연인으로서 형사책임의 주체가 된다. 예를 들어 교통사고처리특례법 제2조의 개정을 통해서 자율주행시스템을 가진 차량에 대한 정의를 명확히 하여 형사 처벌이 가능하도록 하는 것이 필요하다.

6.2 형사책임의 범위

고의범의 처벌을 원칙으로 하되 과실범의 경우 특별한 규정이 있는 경우에만 처벌한다는 형법 제14조의 규정에 의해 과실이 없는 경우에는 형사책임이 면책된다. 완전무결한 정보보안이 현실적으로 불가능한 상태에서 해킹으로 인한 자율주행자동차 사고에 과실이 있다는 이유로 모든 사고에 대해서 형사 처벌을 할 경우 차량 제조업체나 법인 대표자 혹은 사이버 안전 관련 책임자에게 과도한 부담을 줄 수 있다. 이러한 부담이 소극적인 의사결정행위로 이어져 자율주행자동차 산업 발전이 저해되어 4차 산업 경쟁력이 약화될 수 있다. 따라서 과실에 의한 사망사고에 한해서 차량 제조업체 대표자 혹은 사이버 안전 관련 책임자에게 형사 책임을 부담하도록 하되 법인도 같이 책임지도록 하는 양벌규정이 필요하다. 과실이 있지만 형사 처벌을 하지 않는 경우에는 행정 처분을 통하여 차량 제조업체나 법인 대표자 혹은 사이버 안전 관련 임직원에게 과징금 혹은 과태료 처분을 내리도록 해야 한다.

예를 들어 일정 수준의 징계를 받게 되면 관련 임직원이 자율주행자동차 제조업체에 일정 기간 등기임원으로 취업할 수 없도록 하여 행정처분을 통한 형사책임의 비 범죄화를 통해 과도한 부담을 줄이는 방향으로 나아가야 한다. (관련 조항 : 교통사고처리특례법 제3조, 제4조에는 형사 처벌만 규정되어 있으므로 예를 들어 대통령령을 신설하여 행정 처분에 관한 규정의 신설이 필요함)

6.3 형법상의 업무상 과실

차량 제조업체 대표나 혹은 사이버 안전 담당 임직원의 경우 사이버 보안에 대한 업무를 수행한다고 볼 수 있으므로 일정한 업무에 해당된다. 따라서 자율주행자동차가 해킹으로 인하여 사고가 발생된다면 업무상 과실이 있다고 볼 수 있다.

현행 교통사고처리특례법의 경우 운전자에 의한 교통사고 발생 시 형법 제268조에 의한 업무상 과실 치상죄와 중과실치상죄가 적용되어야 함에도 불구하고 특별법을 통하여 교통사고처리특례법 제4조 제1항 각 호의 경우를 제외하고 보험 또는 공제에 가입한 경우 형사 책임을 면제해 주고 있다.

해킹에 의한 자율주행자동차의 사고도 원칙적으로 형법 제268조를 적용하여 차량 제조업체 대표나 사이버 보안 관련 임직원을 처벌할 수 있으나 직접적인 원인이 해커에게 있는 만큼 사이버 보안 담당 임직원에게 과도한 형사책임을 부여하는 것이 적절치 않다. 가령 교통사고처리특례법에 사망 또는 피해자가 사고로 인해 생명의 위협을 느끼거나 불구 혹은 불치, 또는 난치의 질병이 생기는 경우에 한해서만 형사 처벌 규정을 신설하여 자율주행자동차 산업이 활성화하는데 초점을 맞추어야 한다.

7. 자율주행자동차 해킹 사고에 대한 행정 책임 및 예방수단

7.1 자율주행자동차 사고기록장치 설치 의무화

자율주행자동차의 사고가 일어날 경우 사고 원인이 다양하기 때문에 명확한 원인을 파악하기 위해서는 자율주행자동차의 정확한 운행기록이 필요하다. 현재 교통안전법 제55조에 규정되어 있는 자동차 사고기록 장치의 수준을 넘어서 선박에 설치되는 항해 기록 장치 수준의 자율주행자동차 사고기록장치 설치가 필요하다. 또한 사업용 차량에 한해 사고기록장치를 설치하도록 의무화한 교통안전법 제55조를 개정하여 모든 자율주행자동차에 설치를 의무화하여야 한다. 구체적으로 날짜 및 시간, 차량의 위치, 주행상황, 주행코스, 자율주행자동차 모드 사용 및 변경에 관한 기록, 차량의 속력, 자율

주행시스템의 작동여부 등에 관한 기록이 들어가야 하며 운전자가 스마트 디바이스를 이용하여 차량 내 소프트웨어와 연결하여 식별한 기록이 사고 기록 장치에 저장되어야 한다. 더불어 현재 카메라 형식의 블랙박스인 대시캠 기능도 자율주행자동차 사고 기록 장치에 포함되어 차량 안과 밖을 촬영하여 사고 발생 시 참고 되어야 할 것이며 차량 안에서 이루어지는 대화 내용도 녹음되어야 한다.

자율주행자동차 사고 기록 장치는 안전한 보호 용기 내에 보관되어야 할 것이며 그 안에 들어가 있는 사고 기록 장치는 사고 후 자료를 입수할 수 있으면서 내용을 변조할 수 없어야 한다. 어떤 사고에도 최종 기록 자료 손상이 없어야 하며 손상이 되면 그 내용이 최대한 복구가 되어야 하며 누구나 쉽게 찾을 수 있도록 눈에 잘 띄는 곳에 눈에 잘 띄는 색상으로 설치되어야 한다.

자율주행자동차 사고 기록 장치 성능 요건으로는 정상적인 상태에서 자동으로 작동되어야 하며 비정상적인 상태에서도 기록 중단이 최소화 되어야 한다. 사고 후 최소 12시간 이상 저장된 내용을 유지해야 하며 외부컴퓨터에 연결이 가능하면서 해당 자료의 내용을 다운받거나 볼 수 있어야 한다. 사고 기록 장치의 설치나 오류로 인하여 차량 소프트웨어나 하드웨어의 기능이 저하되거나 오류가 발생되지 않아야 한다.

현재 일반 자동차 사고 기록 장치로 개발되어 있는 는 EDR(Event Data Recorder)[9]의 경우 자율주행자동차에 그대로 적용하기에는 무리가 있다. 이를 대체하기 위해 자율주행자동차 사고 기록 장치인 ADR(Accident Data Recorder)[9]이 개발되었으나 현재 성능으로는 해킹에 의한 사고 여부에 대해서 명확히 구분할 수 없는 한계점이 있다.[9] 향후 ADR(Accident Data Recorder)[9]의 성능이 해킹에 의한 사고를 분별할 수 있는 수준까지 개발되고 도입 기준이 만들어지는 동시에 공신력 있는 제3의 기관(예를 들어 한국인터넷진흥원)에서 ADR(Accident Data Recorder)[9]에 대한 인증심사를 진행하여야 한다.

7.2 자율주행자동차 교통사고 조사위원회 설치

자율주행자동차 교통사고의 경우 일반 자동차의 교통사고에 비해 다양하고 복잡한 원인으로 발생하는 경우가 빈번할 가능성이 높고 이해관계 당사자가 개입할 경우 사고 조사의 공정성에 문제가 생길 수 있다. 따라서 공신력 있는 제3의 기관에서 자율주행자동차 교통사고에 대한 원인을 조사하고 분석할 필요성이 있다.

국토교통부 산하에 자율주행자동차 교통사고 조사위원회를 설치하여 필요 시 사고 원인 조사 할 수 있도록 하여 차량 제조업체나 제3자의 고의가 발견될 경우 형사 고발 할 수 있는 권한을 주어야 한다. 사이버 보안 부분에 대해서는 해킹에 관한 조사를 담당하고 있는 한국인터넷진흥원(KISA)이 자율주행자동차 교통사고 조사위원회와 협력하여 차량 제조업체의 사이버 보안 조치 준수여부와 해킹 원인에 대한 조사를 담당하고 하드웨어나 임베디드 시스템에 대한 조사는 교통안전공단이 자율주행자동차 교통사고 조사위원회와 협력하여 진행해야 한다.

이를 위해 자동차손해배상보장법에 자율주행자동차 교통사고 조사위원회에 관한 새로운 규정을 신설하여 신속한 교통사고 조사가 이루어질 수 있도록 하는 동시에 민·형사상 책임규명을 위한 소송이나 행정처분의 증거로서 사용될 수 있도록 규정하는 것이 필요하다.

7.3 자율주행자동차 인증기준 제도 도입

자율주행자동차의 경우 주변 사물을 인식하려는 첨단센서, 그래픽 처리장치, 네트워크에 자동차를 연결하는 IoT 기술 등 다양한 기술이 들어가야 한다. 자율주행자동차의 경우 인신사고가 일어났을 수 있으므로 차량에 대한 하드웨어의 안전성과 소프트웨어의 사이버 보안에 대한 중요성이 크다고 할 수 있다. 따라서 자율주행자동차를 제조하는 업체의 경우 인증기준을 통과한 경우에만 판매를 할 수 있도록 하여야 한다. 자율주행자동차의 경우 하드웨어의 안전성 검사는 현재 자동차관리법에 규정

되어 있는 자기인증적합조사를 대행하는 교통안전공단이 가진 경험과 인력을 활용하여 담당하여야 한다. 사이버 보안의 경우 현재 ISMS(정보보호관리체계 인증)를 담당하고 있는 한국인터넷진흥원(KISA)이 관련 경험과 인력을 활용하여 심사 인증을 진행하고 심사원 양성을 담당하여야 한다.

자율주행자동차의 인증 부분은 국민의 생명권과 직결된 문제이므로 국내 업체뿐만 아니라 외국 업체에게도 똑같이 적용하여 하드웨어 안전성 검사와 사이버 안전 인증을 통과한 경우에만 판매하도록 하는 것이 필요하다. 향후 자율주행자동차 관련 사업을 진행하는 네트워크, 서버, 통신망 관리 업체에게도 자율주행자동차 사이버 보안 인증을 의무화하여야 한다.

자율주행자동차의 인증 부분은 국민의 생명권과 직결된 문제이므로 인증기관과 심사원이 뇌물 등을 수령하고 고의로 부실심사를 하거나 과실로 인한 부실심사로 인하여 사고가 발생할 경우 형사 처벌과 함께 차량 소비자에 대한 민사책임도 부담하도록 해야 하며 차량 제조업체나 차량 소프트웨어 업체와 공모했을 경우 해당 업체나 관계자도 같은 책임을 부담하도록 해야 한다.

ISMS(정보보호관리체계 인증)에 대한 주무부처로 과기정통부가 규정 되어 있어 자율주행자동차 사이버 보안에 관한 사항은 과기정통부가 담당하고 교통에 관한 사항은 국토교통부가 담당하게 된다. 하지만 자율주행자동차의 경우 궁극적으로 자동차에 관한 사항이고 하드웨어 부분과 사이버 보안 부분에 대해 주무부처를 이원화할 경우 차량 제조업체의 행정업무가 과중될 수 있고 관련 규제가 중복될 수 있으므로 자율주행자동차에 관한 사항은 힘들더라도 정부 부처를 일원화하는 것이 필요하다. (예를 들어 국토교통부)

이를 위해 자동차관리법에 자율주행자동차 인증기준에 관한 새로운 규정을 신설과 인증기관과 심사원의 과실 또는 고의로 인한 부실심사가 진행될 경우 형사 처벌 규정 신설을 통해 자동차 소비자의 권익과 기본권을 보호하도록 하는 것이 필요하다.

7.4 자율주행자동차 분쟁조정 위원회 도입

자율주행자동차 해킹으로 인하여 인신사고가 발생될 경우 직접적인 육체에 대한 피해뿐만 아니라 경제적인 피해가 발생될 수 있기 때문에 신속하고 간편한 구제가 필요하다. 따라서 비용이 많이 들고 시간이 오래 걸리는 소송 제도 대신 신속한 구제를 위한 분쟁 조정 제도가 필요하다.

자율주행자동차 분쟁조정 제도의 경우 당사자 일방이 신청할 경우 조사를 개시할 수 있도록 하며 신청자와 상대방이 조정에 대해서 수락할 경우 조정서를 작성하도록 하며 조정서의 효력은 민법상의 재판상 화해와 동일한 효력을 가지도록 하여야 한다.

자율주행자동차 분쟁조정 위원회의 경우 분쟁조정에 따른 손해배상 결정뿐만 아니라 관련 업체에 대한 시정권고 조치, 사고 피해 예방을 위한 활동을 할 수 있도록 규정하여 국민의 기본권을 보호할 뿐만 아니라 자율주행자동차 산업이 발전할 수 있는 토대를 마련하여야 한다.

현재 교통사고 분쟁이 생길 경우 금융회사와 금융 이용자 간의 분쟁으로 인정되어 금융위원회의 설치 등에 관한 법률 제5절 금융 분쟁의 조정(제51조에서 제57조 적용)에 의해 금융분쟁조정위원회 관할로 되어 있다. 하지만 자율주행자동차 교통사고의 경우 다양한 원인으로 인해 일어날 수 있으므로 법조인과 금융기관 경력자, 의사 등으로 구성되어 있는 현재 금융분쟁조정위원회의 기능으로는 자율주행자동차 분쟁조정이 쉽지 않다.

따라서 자동차손해배상보장법에 자율주행자동차 교통사고 분쟁조정위원회에 관한 새로운 규정을 신설하여 자동차, 전자, IT 관련 경력자 및 교수 등을 조정위원으로 선임하여 분쟁조정을 하도록 하되 분쟁이 성립할 경우 재판상 화해와 동일한 효력을 갖도록 규정하는 것이 필요하다.

8. 자율주행자동차와 일반자동차 사고 책임에 관한 비교

자율주행자동차와 일반 자동차의 경우 사고 원인에 대해서 여러 가지 차이점이 있으므로 해킹에 의한 자율주행자동차 사고의 개선방안과 현재 일반 자동차 사고의 책임법제에 대한 예상되는 차이점을 아래와 같은 <표4>로 정리하여 비교하였다.(*법리나 법률해석에 따라 상이 할 수 있으며, 세부 해킹 원인에 따라 ITS, 통신회사, 인증기관 등도 포함될 수 있음)

일반 교통사고 대비해서 자율주행자동차 사고의 경우 차량 제조업체의 책임이 커져야 한다. 그러므로 해킹에 의한 사고에 대해서 차량 제조업체의 대비책이 필요하며 지속적인 보안 취약점에 대한 연구와 더불어 중요 소프트웨어에 대한 업데이트를 지속적으로 제공하여 해킹으로 인한 자율주행자동차 사고에 대해서 대비하여야 한다.

<표4> 해킹에 의한 자율주행자동차 사고와 일반자동차 사고의 예상되는 우선적 대상 차이

우선적 대상 차이	*해킹에 의한 자율주행자동차 사고	일반 자동차 사고
손해배상책임	차량 제조업체 혹은 운행자 혹은 운전자	운행자 혹은 운전자
형사 책임 주체	차량 제조업체 담당 임직원	운행자 혹은 운전자
형사 책임 범위	사망 혹은 뇌사	12대 중과실
제조물 책임 주체	차량 제조업체	차량 제조업체
제조물 책임입증	차량 제조업체	운행자 혹은 운전자
보험가입의무	차량 제조업체	차량 소유주
행정처분 대상	차량 제조업체 담당 임직원	운전자

9. 해킹에 의한 자율주행자동차 사고에 따른 책임 소재에 대한 소결

<표5> 해킹에 의한 자율주행자동차 사고의 책임 소재 개선 방안

구분	민사 책임	형사 책임	행정 책임
해킹에 의한 자율주행자동차 사고의 책임 소재 개선 방안	①손해배상 책임 명확화 (자동차 손해배상보장법 제4조 개정) ②제조물 책임 명확화 (제조물 책임법 제3조의 2 개정) ③손해배상 책임 한도 (자동차 손해배상보장법 시행령 제3조 개정) ④자동차 사고 피해지원 기금(자동차 손해배상보장법 제30조부터 제39조의13 개정) ⑤사이버보험 가입 의무화 (자동차 손해보장법 제5조 개정)	⑥자율주행 자동차 형사 책임 명확화 (교통사고 처리특례법 제2조 개정) ⑦자율주행 자동차 사고 형사처벌 명확화 (교통사고 처리특례법 제4조 제1항 개정)	⑧사고기록 장치 의무화 (교통안전법 제55조 개정) ⑨자율주행 자동차 사고조사위원회 신설 (자동차 손해배상보장법에 관련 법규 신설) ⑩자율주행 자동차 인증 기준 마련 (자동차 관리법에 관련 법규신설) ⑪자율주행 자동차 교통사고 분쟁조정위원회 신설 (자동차 손해배상보장법에 관련 법규 신설)

해킹에 의한 자율주행자동차 사고의 경우 다양한 원인에 의해서 이루어질 수 있다. 해킹의 원인에 따라 차량 제조업체, 협력 업체, 차량 소유주, 인증기관, 국가, 도로 관련 기업에 대한 책임 기준을 다르게 해야 하며, 인증 심사 부분에서 문제가 생길 경우 인증기관과 인증 심사원에게 일정한 책임을 부여해야 한다.

해킹에 의한 자율주행자동차 사고에 있어서 차량 제조업체나 인증기관, 인증 심사원, 협력 업체, 관련 임직원의 불법행위가 있을 경우 형사 처벌과 함께 민사 책임을 부여해야 한다.

따라서 각 원인에 따라서 책임이 있는 부분을 규명하고 과실에 따른 명확한 기준을 통해서 국가, 차량 제조업체, 협력업체, 차량 소유주, 인증기관, 인증 심사원, 도로 관련 기업에게 책임을 부여함으로써 자율주행자동차 산업 발전에기여하고 우리나라가 4차 산업혁명을 선도해 나갈 수 있는 국가가 될 수 있도록 책임 법제에 대한 개선이 필요하다. <표5>는 앞서 논의한 민사책임, 형사책임, 행정책임으로 나누어 각 책임 소재별 개선사항을 정리한 것이다.

10. 결 론

본고에서는 자율주행자동차 주행 시 일어날 수 있는 사이버 해킹에 의한 사고가 일어날 경우 어떤 식으로 책임 법제를 적용할 것인지에 대해 기존 법제를 중심으로 점검하면서 개정이 필요한 부분에 대해 제안하였다. 본 연구에서 전체적인 여러 가지 법률의 연계성을 연구한다는 것은 어려운 일이고 우선적으로 핵심 또는 가장 연계성 있는 연구가 먼저 되어야 하는 민법, 형법, 행정법의 연관성 중심으로 유기적인 관계성에 대해서 살펴보았다. 구체적으로는 자율주행자동차에 맞는 민사책임의 주체와 범위를 정하고 책임 보험 제도를 통해 뒷받침하고 형사책임의 주체와 범위를 정해 사후적 책임을 명확히 하여 책임 법제에 대한 개선방안을 제시하였다. 해킹을 방지하기 위한 사이버 보안 인증제도와 자율주행자동차 분쟁조정 제도 도입을 통한 정책적 예방 수단을 도입을 통해 행정책임에 대한 개선방안을 제시하였다. 자율주행자동차 시험 운행이나 상용화되는 시점에 해킹에 의한 사고가 발생할 경우 법률의 부재로 인해 국민의 기본권이 침해되지 않아야 한다.

전문가를 대상으로 델파이 방법 등을 통해 자율주행자동차 책임 소재에 관한 개선 사항에 대한 더 성숙한 검증은 아쉬운 부분이며 다음 연구로 진행 예정이다.

자율주행자동차 책임 법제를 정비하여 향후 자율주행자동차가 문제없이 사회에 받아들여져 자율주행자동차의 신속한 보급이 이루어진다면 우리나라의 4차 산업혁명 경쟁력을 확보하는 계기가 될 것이고 이를 통해 세계를 선도해 나가는 국가로 나아가야 한다. 본 논문에서는 자율주행자동차 해킹으로 인한 사고에 대한 책임 법제에 대한 연구만 다루었으나 향후 다양한 자율주행자동차 사고 원인에 대한 책임 법제에 대한 후속 연구가 진행되어야 할 것이다.

참고문헌

[1] 박지선, “전자금융사기로 인한 손해 발생시 은행의 배상책임에 관한 연구 : 「전자금융거래법」 제9조에 대한 검토를 중심으로”, 은행법 연구, 제6권 제2호., 331-355, 2013

[2] 최호진, “해킹에 의한 개인정보유출과 정보통신서비스제공자에 대한 손해배상책임에 관한 고찰:sk컴즈 사건을 중심으로”, 법조, 63권 2호., 123-159, 2014

[3] 박상돈, 김인중, “한국과 미국의 사이버보안 단계별 법제도 비교연구”, 융합보안논문지, 제12권 제4호., 33-40, 2012

[4] 한세진, “전자상거래 지급결제의 핀테크 활성화를 위한 보안 및 법제도적 과제”, 융합보안논문지, 제15권 제2호., 25-31, 2015

[5] 안명구, 박용석, “자율주행자동차의 법률체계와 국내외 자율주행자동차 법제 현황,” 융합보안논문지, 제18권 제4호., 53-61, 2018

[6] 권영준, 이소은, “자율주행자동차 사고와 민사책임”, 민사법학, (75), 449-495, 2016

[7] 김형준, “자율주행자동차 교통사고의 형사책임”, 중앙법학, 19(4), 47-82, 2017

[8] 지광운, “자율주행차의 발전에 따른 자동차보험관련 법제의 개선방안에 관한 연구”, 법학논문집, 제41집 제2호., 105-145, 2017

[9] 과학기술정보통신부와 정보통신기술진흥센터의 “지능형 자동차 보안 위협 및 대응 방안 보고서(2017)”

[10] 제조물책임법일부개정법률안(원유철의원등10인), 국회의안정보시스템, 2009568번, 2017-09-22

[11] 윤진아, 김상태 “독일에서의 자율주행자동차에 관한 법적 논의”, 법학논총 제34권 제1호., 59-77, 2017

〔저자소개〕

안 명 구 (Myeonggu An)

2014년 2월 인제대학교 법학과 학사
2018년 3월 ~ 현재 세종사이버대학교 정보보호대학원 석사과정
email : amg1227@naver.com

박 용 석 (Yongsuk Park)

서강대학교 컴퓨터학 (학사)
뉴욕(POLY)대 (석사, 박사)
AT&T (Bell) Labs, 삼성전자
현재 세종사이버대학교 정보보호대학원 주임교수
현재 세종사이버대학교 IT학부 교수
email : yongspark@sjcu.ac.kr