Journal of the Korea Convergence Society
Vol. 8. No. 9, pp. 41-47, 2017
https://doi.org/10.15207/JKCS.2017.8.9.041

해킹에 따른 로보어드바이저의 시세조종 행위와 운용사의 법적 책임

김동주[1], 권헌영[2], 임종인[3*]
[1]고려대학교 정보보호대학원 정보보호학과,
[2,3]고려대학교 정보보호대학원 교수

Legal liability of the management firm on hacked Robo-Advisor's stock price manipulation

Dong Ju Kim[1], Hun Yeong Kwon[2], Jong In Lim[3*]
[1]Dept. of Information Security, Graduate School of Information Security, Korea University
[2,3]Prof. of Graduate School of Information Security, Korea University

요 약 본 연구에서는 제4차 산업혁명의 핵심 요소인 인공지능 기술의 발전에 불가피하게 수반될 수 있는 부작용을 최소화하기 위한 제도적 보완점을 도출하기 위한 선행 연구로서, 인공지능 기술 적용의 대표적인 유형에 해당하는 로보어드바이저가 해킹되어 시세조종 행위를 범하는 구체적인 경우에 있어서 현행 법체계에 따른 책임관계가 어떠한지 검토하고자 하였다. 현행 법체계가 기본적으로 해킹 행위 및 시세조종 행위를 엄격히 금지하는 입장을 취하고 있으나, 로보어드바이저 운용사는 평소 해킹 방지를 위한 보호조치 의무를 준수할 경우 해킹에 따른 시세조종 행위로 일반 투자자들에게 대규모 피해가 발생하여도 이에 대한 법적 책임을 면할 수 있는 등 피해자 보호에 미흡한 것으로 확인되었다. 본 연구를 바탕으로 이러한 문제를 극복하기 위한 제도적 보완점 도출에 관한 후속 연구가 필요하다.

• 주제어 : 인공지능, 로보어드바이저, 해킹, 시세조종, 법적 책임

Abstract This study is a preceding research designed to deduct an institutional supplementary measure that minimizes any inevitable side effects from the improvement of artificial intelligence (AI) technology, which is the core element of the Fourth Industrial Revolution. In this specific case in which the Robo-Advisor, the representative type of AI-applied technology, was hacked by a third party and ended up manipulating prices, the study was intended to examine the responsibility relationship of the current legal framework. Although the current legal framework strictly prohibits acts such as hacking and manipulation, it was confirmed that if the Robo-Advisor management firm acts in compliance with protection measures regarding hacking, the firm is free from any legal liabilities and there is insufficient legal protection available for ordinary investors with grand-scale damage from price manipulation
Based on this study, further studies are needed to derive more institutional supplementary measures on overcoming these problems.

• Key Words : Artificial Intelligence, Robo-Advisor, Hacking, Stock Price Manipulation, Legal Accountability.

*Corresponding Author : 임종인(jilim@korea.ac.kr)
Received August 7, 2017 Revised September 2, 2017
Accepted September 20, 2017 Published September 28, 2017

1. 서론

최근 주목받고 있는 제4차 산업혁명은 디지털 초연결 사회, 인공지능과 기계학습의 범용화 등을 주요 특징으로 하고 있으나, 기계가 인간을 완전히 대체하는 단계에는 이르지 못하고 있기 때문에 아직은 초기 단계라고 볼 수 있다. 그러나 가까운 미래에 과학기술의 진보에 따라 본격적인 제4차 산업혁명이 이루어짐으로써 진정한 '포스트휴먼 사회'로 진입할 것으로 예상되고 있다[1].

이러한 과학기술의 눈부신 발전은 이전에 누려보지 못한 많은 혜택을 인류에게 가져다줌과 동시에 부정적인 변화 또한 초래할 것으로 예상된다. 대표적으로, 고용과 노동 환경의 급격한 변화가 예상되는데, 세계경제포럼은 2020년까지 사회 각 분야에서 전체적으로 500만개 이상의 일자리가 줄어들 것으로 전망하고 있다[2]. 제4차 산업혁명의 본질적인 내용이 기계가 인간을 완전히 대체 가능하게 된다는 것이므로 이러한 결과는 필연적일 수밖에 없을 것이며, 따라서 제4차 산업혁명의 도래에 따른 사회환경의 급격한 변화에 미리 대비하지 아니할 경우 긍정적인 효과 못지않게 부작용에 따른 큰 혼란을 겪을 가능성이 농후하다.

최근 우리나라에서도 인공지능 기술 발전의 사회적 영향에 관한 연구들이 활발히 진행되고 있는데,[1] 이러한 선행 연구들은 쟁점을 정리하여 나름의 해결방안을 제시하거나, 지능정보사회에 대응하기 위한 체계적인 거버넌스 구축의 필요성을 제시하는 등으로 큰 의미가 있는 반면, 고도의 자율성을 갖지 못한 초기 단계의 인공지능을 상정하여 현행 법체계의 확장적인 해석을 통해 문제해결을 시도하거나, 일반론적인 관점에서 포괄적으로 접근함으로써 구체적인 대안 제시가 부족하다는 등의 한계가 있어 보인다.

따라서 본 논문에서는 최근 인공지능 기술 적용의 대표적인 유형에 해당하는 로보어드바이저가 해킹되어 시세조종 행위를 범하는 구체적이면서도 이종 학문 간의 융합적인 경우를 상정하고, 그러한 상황에서의 법적인 책임관계가 어떠한지 검토함으로써, 전자금융 관련 사고에 있어서의 쟁점을 보안 측면에서 금융 실체법 측면으로 확대하여 연구의 폭을 넓히는 한편 고도의 자율성을 지닌 인공지능 시대에 대비하기 위한 구체적인 제도적 보완점 도출의 기반을 제시하고자 한다.

아래에서는 로보어드바이저의 활용 현황, 로보어드바이저에 대한 해킹 가능성, 시세조종 행위에 대한 법적 규율을 살펴보고, 이어서 로보어드바이저 운용사의 법적 책임을 검토하고, 결론으로 마무리 짓는다.

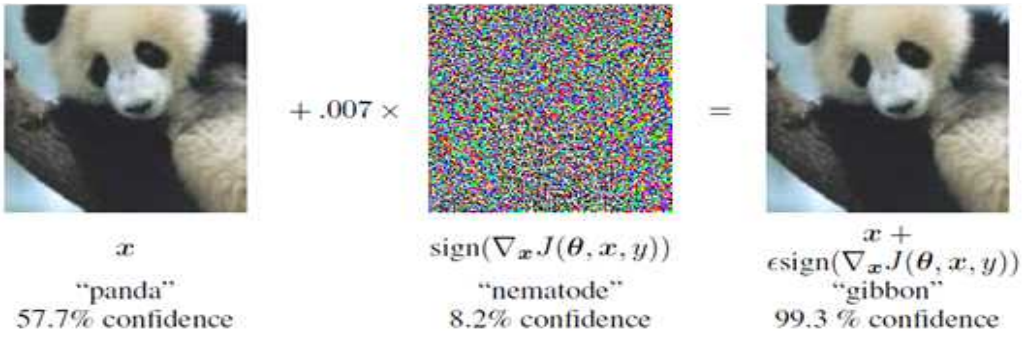
2. 로보어드바이저의 활용 현황

Robot과 Advisor의 합성어인 로보어드바이저(Robo-Advisor)는 2002년 미국 언론에서 처음 사용되었는데, 여기서 Robo는 자동화(automated)의 의미로 사용되었다[3]. 현재 로보어드바이저는 다양한 형태로 정의되고 있으나, 대체로 다음과 같은 요소들을 담고 있는 것으로 언급되고 있다. 먼저, 1) 미리 짜여진 알고리즘을 이용하여 투자자문 및 자산관리 서비스를 제공하여야 하고, 2) 투자자 유형 파악, 자산배분, 주문집행, 리밸런싱 등 모든 자산관리 과정에서 사람의 개입을 최소화하는 자동화를 추구하여야 하며, 3) 최소 투자한도와 자문 보수를 대폭 낮추어 투자자문 및 자산관리 서비스의 대중화를 추구하여야 한다는 것이다[4].

로보어드바이저의 유형은 1) 로보어드바이저가 자산배분 및 리밸런싱을 위한 거래 실행까지 전담하는 운용형(Fully-automated Platform), 2) 로보어드바이저가 자문을 하면 거래를 고객이 스스로 하는 자문형(Self-executed Trades), 3) 로보어드바이저가 산출한 자산배분 및 리밸런싱 결과를 사람인 전문가가 검증하는 하이브리드 유형(Advisor-executed Trades)의 3가지로 구분되고 있다[5].

독일의 시장조사기관 스타티스타(Statista)에 따르면 전 세계 로보어드바이저의 운용자산 규모가 2015년 약 660억 달러에서 2021년 1조 달러 이상으로 증가하고, 이용자 수는 2015년 약 280만 명에서 2021년 9,500만 명을

1) 의미있는 선행 연구로, 최경진(지능형 신기술에 관한 민사법적 검토, 정보법학 제19권 제3호, 2015년), 고윤승(우리나라 로보어드바이저 도입을 위한 활성화 방안 탐색, 한국과학예술포럼 제25권, 2016년), 김범준・엄윤경(로보어드바이저의 활용과 금융투자자 보호, 법학연구 제17권 제1호, 2017년), 심우민(지능정보사회 입법 동향과 과제, 연세 공공거버넌스와 법 제8권 제1호, 2017년), 안수현(Automated Investment Tool을 둘러싼 법적 쟁점과 과제, 상사판례연구 제29권 제2호, 2016년), 양종모(인공지능의 위험의 특성과 법적 규제방안, 홍익법학 제17권 제4호, 2016년), 이상용(인공지능과 계약법, 비교사법 제23권 제4호, 2016년), 이시직(4차 산업혁명 시대, 지능정보기술의 사회적 영향과 법적 과제, 연세 공공거버넌스와 법 제8권 제1호, 2017년), 이원태 외 4명(지능정보사회의 규범체계 정립을 위한 법・제도 연구, 정보통신정책연구원, 2016년), 이중기(인공지능을 가진 로봇의 법적 취급, 홍익법학 제17권 제3호, 2016년) 등이 있다.



상회할 것으로 전망되고 있다[6]. 그러한 급성장의 배경으로는, 1) 자동화를 통해 비용을 절감함으로써 자문 수수료를 기존의 인력에 의한 서비스 수수료에 비하여 1/3 내지 1/10 수준으로 낮출 수 있는 점, 2) 기계학습과 빅데이터를 기반으로 투자환경의 다양한 변수들을 종합적으로 고려하여 과학화되고 체계적인 서비스를 제공할 수 있는 점, 3) 시장 상황의 변화에 신속히 반응할 수 있는 점, 4) 모바일 및 온라인을 통한 서비스 접근이 용이하여 투자자의 편의성이 뛰어난 점 등이 언급되고 있으며, 향후 자산관리 서비스의 대중화에 크게 기여할 것으로 기대되고 있다[7,8].

한편, 로보어드바이저가 이처럼 혁신적인 가치를 지닐 수 있게 된 기술적인 배경으로는 인공지능 딥러닝 기술과 빅데이터 기술을 꼽을 수 있을 것이다. 딥러닝 기술은 생물학적 신경망을 응용하여 기존의 인공신경망 기술을 심화시킨 것으로, 답보 상태를 보이던 인공지능 기술의 발전에 중대한 모멘텀으로 작용하고 있으며[9], 여기에 빅데이터 기술이 결합되어 방대한 분량의 정보를 수집・분석・실행하고, 그 결과로 생성되는 정보를 다시 수집하여 분석하는 거대한 정보 흐름의 선순환 구조를 만들어냄으로써 산업 생태계의 경쟁력을 획기적으로 향상시켜 주는 것이다[10].

반면, 로보어드바이저에 대한 의존도가 높아질수록 그 부작용 또한 그만큼 클 수밖에 없을 것이다. 금융시장의 규모와 역할이 과거와 비교할 수 없을 만큼 커지고 금융투자상품들이 고도로 구조화되어 긴밀한 상호작용을 하고 있는 현재의 상황에서 로보어드바이저에 의한 금융사고가 발생할 경우 그 충격은 매우 클 수밖에 없을 것이므로, 로보어드바이저의 장점을 최대한 활용함과 동시에 로보어드바이저에 의한 대형 금융사고의 발생 가능성을 최소화하려는 노력을 병행할 필요가 있다.

3. 로보어드바이저에 대한 해킹 가능성

최근 글로벌 사이버 보안기업 시만텍이 발표한 '인터넷 보안 위협 보고서'(ISTR)에 따르면, 스피어 피싱 이메일을 이용하는 송금 유도 이메일 사기(Business Email Compromise) 스캠에 의해 지난 3년간 전세계적으로 30억 달러 가량의 피해가 발생하는 등 컴퓨터 및 네트워크 기술 발전의 부작용으로서 해킹 범죄가 크게 증가하고 있을 뿐 아니라 기술적으로 고도화되고 있는 상황이다[11].

해킹은 인간 본성에 기인한 문제로서 해킹을 막으려는 자가 있으면 뚫으려고 하는 자도 있기 마련이며, 공격과 방어에 사용되는 기술들이 밀접한 상호작용을 하는 관계이므로 창과 방패의 관계처럼 끊임없는 대결이 펼쳐질 수밖에 없을 것이다. 언제든지 더욱 치명적인 공격 기법이 등장할 수 있으므로 현재 알려져 있는 해킹 기법에 대한 관계에서 안전하다는 것은 별다른 의미가 없으며, 항상 새로운 공격의 등장 가능성을 염두에 두고 정보보안의 수준을 강화하기 위해 노력할 필요가 있을 것이다.

고도로 발전된 형태의 인공지능에 있어서도 사람의 능력을 뛰어넘는 고차원적인 판단능력을 보유하고 있다는 것일 뿐 외부의 공격을 스스로 완벽히 방어할 수 있다는 것을 의미하지는 않는다. 기존의 전통적인 해킹 기법 가운에 1) 스푸핑 등의 중간자 공격(Man-in-the-middle)을 통해 인공지능 시스템의 입출력 데이터를 위변조 하는 방법, 2) 리버스 엔지니어링 등을 통해 알고리즘을 임의로 조작하는 방법 등은 인공지능에 대해서도 여전히 유효한 공격일 수 있다.

최근의 연구에 따르면 기계학습 프로그램에 대한 해킹 공격이 얼마든지 가능하며, 실제로 데이터의 패턴을 인식하는 성향을 파악하고 이를 바탕으로 기계학습 프로

그램을 조작할 수 있는 다양한 공격 기법들이 등장하고 있다. 자동차의 비전 시스템을 속여서 존재하지 않는 장애물이 존재하는 것처럼 보이게 할 수 있고, 음성 인식 알고리즘을 속여서 악성코드 다운로드와 같은 은밀한 공격 행위를 할 수도 있으며, 또한 스팸 메일 발신자들이 추후 인공지능 스팸 분류시스템을 속이기 위해 기계학습 단계에서 미리 학습 데이터에 허위 전자메일을 삽입해두는 행위 등 인공지능에 대한 해커의 공격이 현실화되고 있는 상황이다[12]. 구체적인 사례로서 위 예시 그림은 인공신경망에 의해 57.7%의 신뢰도로 판다(panda)로 인식되는 이미지에 8.2%의 신뢰도로 선충(nematode)으로 인식되는 미세한 대립정보(adversarial example)를 추가함으로써 육안으로는 정상적인 판다로 보임에도 인공신경망에 의해서는 99.3%의 신뢰도로 긴팔원숭이(gibbon)로 잘못 인식되도록 만들 수 있음을 보여준다[13].

다만, 본 논문은 해킹 기법 자체가 아니라 인공지능에 대한 해킹이 이루어진 이후의 문제에 초점을 맞추고 있으므로 해킹 가능성에 대해서는 위와 같이 원론적인 수준에서 언급하고, 아래에서는 인공지능에 대한 해킹이 성공하여 인공지능이 공격자의 의도에 따라 시세조종 행위를 하는 경우에 있어서의 법적 규율 문제에 관하여 살펴본다.

4. 시세조종 행위에 대한 법적 규율

주가조작이라는 용어로 더 잘 알려져 있는 시세조종 행위는 시장에서의 수요공급 원칙에 따라 정해져야 할 증권의 시세를 매도물량이나 매수물량을 쏟아내는 등의 의도적인 행위를 통해 인위적으로 조종하는 것을 의미한다[14]. 현행 자본시장과금융투자업에관한법률(이하 '자본시장법'이라고 함) 제176조에서 이를 금지하고 있으며, 내용만 조금씩 다를 뿐 거의 모든 국가에서 시세조종 행위에 대한 금지규정을 두고 있다.

시장에서 형성되는 증권의 가격은 기존의 모든 정보가 반영된 합리적 가격으로 인정되고, 투자자들의 주관적인 판단에 따른 순차적인 매매 행위에 따라 그 가격은 계속해서 조정될 것이다. 이와 같이 시세 형성은 객관적 정보와 투자자의 주관적 판단이 끊임없이 반영되어 가상의 균형가격을 향하여 지속적인 수렴이 이루어지는 동태적인 과정이다. 그 과정에서 완전한 균형 가격이 형성되기 위해서는 정보의 진실성이 담보되어야 하며, 이러한 집단적 의사의 수렴을 방해하는 인위적인 조작이 없어야 할 것이다. 공시제도가 정보의 진실성 담보를 위한 장치라면 시세조종 행위 규제는 집단적 의사의 자연적인 수렴을 방해하는 일체의 행위를 금지하는 장치라고 할 수 있다[15].

시세조종 행위의 유형은 크게 1) 위장매매, 2) 매매유인 목적 행위, 3) 시세의 고정•안정 행위, 4) 연계 시세조종 등으로 분류할 수 있으며, 시세조종 행위의 동기는 보유중인 증권의 가격을 인위적으로 상승시킨 후 이를 장내에서 일반투자자들에게 매도하여 차익을 얻으려는 것이 가장 일반적이고, 그밖에 기존 주가를 바탕으로 산출되는 신주 또는 전환사채 등의 발행가격을 높이기 위한 경우, 담보로 제공한 증권의 가치가 하락하여 담보권자가 담보권을 실행하게 되는 것을 방지하기 위한 경우, 합병반대 주주의 주식매수청구권 행사를 억제하려는 경우 등으로 다양하다[16].

기본적으로 시세조종 행위는 일상적으로 이루어지는 수많은 거래에 묻혀 적발될 가능성이 낮은 반면, 성공했을 경우의 반대급부는 매우 크기 때문에 인간의 탐욕적인 본성을 고려할 때 아무리 엄중히 단속하더라도 끊임없이 계속 이루어질 것으로 예상된다[17]. 더구나, 인터넷 및 모바일 기술의 발전에 따라 허위정보를 더욱 빠르고 광범위하게 유포하여 정상적인 일반투자자들을 시세조종에 이용하는 등 신종 불공정거래 행위가 크게 증가하고 있을 뿐 아니라[18], 상대적으로 적발이 어려운 소량 주문을 이용한 초단기 시세조종 행위가 증가하는 현상 등으로 인해 단속의 어려움이 가중되고 있다[19].

이에 반하여, 현행 법체계는 피해자 보호 측면에 있어서 여전히 미흡한 상황인 것으로 보인다. 자본시장법 상의 손해배상청구권의 소멸시효가 지나치게 짧게 설정되어 있을 뿐 아니라[20], 시세조종 등으로 인한 피해자 보호를 강화하기 위해 도입된 증권관련 집단소송의 허가절차가 매우 까다롭고 장기간이 소요되는 탓에 도입 취지와 달리 그 효과가 매우 제한적이다[21,22].

향후 고도의 인공지능 로보어드바이저가 시세조종에 악용되어 자신이 관리하는 수많은 계좌를 활용하여 단기간에 치밀하게 시세조종을 진행할 경우 이를 적발하는 것 자체가 매우 어려울 것으로 예상되며, 현재와 같은 투자자 보호 체계로는 이에 제대로 대응하기 어려워 보이므로 피해자 보호 강화를 위한 추가적인 조치가 필요할 것으로 생각된다.

5. 로보어드바이저 운용사의 법적 책임[2)]

민사적인 관점에서, 로보어드바이저의 운용사는 이용자들에게 정보통신 서비스를 제공하는 지위에 있으므로 정보통신망의이용촉진및정보보호등에관한법률(이하 '정보통신망법'이라고 함) 제45조(정보통신망의 안정성 확보 등) 및 그 위임을 받아 미래창조과학부 장관이 정하는 정보보호지침에 따라 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 취하여야 하고, 여기에는 해킹을 방지하기 위한 기술적·물리적 보호조치를 취할 의무도 포함된다. 따라서 운용사가 해킹 방지 조치를 소홀히 한 경우에는 위 정보통신망법 제45조를 위반한 불법행위로 인한 민법 제750조의 손해배상책임 및 전항에서 설명한 자본시장법 제176조 위반에 따른 손해배상책임 등을 부담하게 된다.

한편, 금융회사 등은 전자금융거래법 제21조(안전성의 확보 의무) 및 그 위임을 받아 금융위원장이 정하는 고시에 따라 전자금융거래가 안전하게 처리될 수 있도록 하기 위한 선량한 관리자로서의 주의의무를 기울여야 하고, 전자금융거래의 안전성과 신뢰성을 확보할 수 있도록 전자적 전송이나 처리를 위한 인력, 시설, 전자적 장치 등에 관한 기준을 준수할 의무가 있다. 여기에는 해킹 방지를 위한 보호조치도 포함되므로 운용사가 이를 소홀히 한 경우에는 위 전자금융거래법 제21조 위반에 따른 불법행위 측면에서도 손해배상책임을 부담하게 된다.

다만, 일반적으로 불법행위에 따른 손해배상 책임에 있어서는 피해자가 가해자의 불법행위 사실을 입증하여야 하므로, 해킹 사고 발생시 정보통신 서비스 제공자가 보호조치 의무를 준수하지 아니하였다는 점은 피해자가 입증해야 한다. 그러나 정보통신 서비스에 활용되는 기술이 매우 전문적일 뿐만 아니라 관련 증거자료의 대부분이 정보통신 서비스 제공자의 지배 영역에 놓여 있으므로 일반 국민인 피해자가 그러한 사실을 입증하기는 매우 어렵고, 이러한 사정은 해킹 사고에 따른 손해배상 청구 소송에서 피해자가 승소하기 어렵게 만드는 요소로 작용하고 있다[23]. 여기에 전항에서 설명한 바와 같이 인공지능에 의한 시세조종 행위의 적발이 매우 어려울 것이라는 점과 시세조종 행위에 대한 법적 구제 절차가 미흡하다는 점이 더해짐으로써 피해자의 법적 지위는 더욱 취약해질 것으로 생각된다.

한편, 전자금융거래법 제9조(금융회사 또는 전자금융업자의 책임)에서는 이와 달리 입증책임의 전환에 관하여 규정하고 있으나, 동 규정은 그 요건 상 금융회사등과 직접적인 계약관계에 있는 '이용자'에 한하여 적용되고, 그러한 계약관계가 없는 제3자의 경우에는 적용되지 아니한다. 따라서 해킹에 따른 로보어드바이저의 시세조종 행위로 인하여 피해를 입은 일반 투자자들은 운용사가 해킹 방지를 위한 주의의무를 소홀히 하였다는 점에 대한 입증책임을 부담하게 되고, 결국 전자금융거래법에 따른 손해배상책임에 있어서도 운용사에 비하여 상대적으로 불리한 지위에 놓여 있다고 할 수 있다.

형사적으로는, 정보통신망법 및 전자금융거래법 등에 따른 해킹 방지를 위한 보호조치 의무 위반행위에 대해 과태료를 부과하도록 되어 있을 뿐 형사처벌 규정은 존재하지 아니한다. 따라서 방조에 이르지 않는 단순 보호조치 의무 위반에 대해서는 운용사에 대해 형사책임의 문제는 발생하지 아니한다.

참고로, 인공지능 기술 수준의 고도화 및 이에 대한 전문적인 해킹기법의 개발이 최근에서야 비로소 의미있게 진행되는 이유로 전 세계적으로 인공지능 해킹에 따른 법적인 책임문제를 논함에 있어서 참고할 사례는 아직 알려지지 않고 있으나, 현재의 발전 추세를 고려할 때 조만간 유의미한 실제 분쟁 사례가 발생할 것으로 전망된다.

6. 결론

정리하면, 운용사는 평소 해킹 방지를 위한 법규상의 보호조치 의무를 준수하고 직원들의 불법행위 방지에 상당한 주의를 기울였을 경우에는 해킹에 따른 시세조종 행위로 인해 일반 투자자들에게 대규모 피해가 발생하더라도 이에 대한 민사·형사상의 법적 책임을 면할 수 있다. 더군다나 운용사가 법규상의 보호조치 의무를 위반한 사실이 있는 경우에 있어서도 이에 대한 입증책임을 피해자인 원고가 부담하는 이유로 인해 운용사는 손해배상 소송에서 상대적으로 유리한 입장에 있다고 할 수 있다.

그러나, 로보어드바이저 운용사의 경우 인공지능을 활

2) 해킹범이 엄정한 법적 책임을 부담해야 한다는 점은 명백하나, 해킹범은 그 신원을 파악하기 어려울 뿐 아니라 신원이 밝혀지더라도 변제자력이 부족한 경우가 대부분이고, 따라서 실제 사건에 있어서는 변제자력이 있는 운용사의 손해배상책임 여부가 주로 문제될 것이므로, 본 논문에서는 운용사의 법적 책임에 국한하여 검토한다.

용함으로써 비용 절감 및 고객 증가 등의 많은 이익을 향유하는 반면, 시세조종의 피해자에 해당하는 일반 투자자들은 그러한 이익을 누리지 못하는 상태에서 일방적으로 피해를 입게 되는 구조인 점을 고려하면 이러한 결과가 합당한 것이라고 보기는 어렵다.

현행 법체계가 고도의 자율성을 지닌 본격적인 인공지능의 출현을 예상하지 못한 상태에서 만들어진 것인 만큼 위와 같은 사각지대가 존재할 수밖에 없을 것이며, 본 논문은 현행 법체계의 그러한 한계를 확인하는 한편 전자금융 관련 사고에 있어서의 쟁점을 보안 측면에서 금융 실체법 측면으로 확대하였다는 점에서 의미가 있다. 향후 본 연구를 기반으로 이러한 한계를 극복하기 위한 제도적 보완점 도출에 관한 후속 연구가 이루어지기를 기대한다.

REFERENCES

[1] J. H. Paek, “The Fourth Industrial Revolution and Posthuman Society”, Conference of The Korean Association for Posthuman Society, 2016.

[2] World Economic Forum, “The Future of Jobs”, 2016.

[3] S. B. Lee, “The Effect of Robo-Advisor to the Korean capital market”, KRX Market, Vol. 2016 Summer, 2016.

[4] Y. S. Ko, “A Study on the Measures to activate the Introduction of the Robo-Advisor in Korea”, Korea Science & Art Forum, Vol. 25, 2016.

[5] S.H. Ahn, “A Study on the Trends and Regulation of Robo-Advisor Services Internationally and its Implication to Korea”, Journal of Korea Commercial Cases Association, Vol. 29, No. 2, 2016.

[6] G. S. Lee, “US Wellsfargo’s Robo-Advisor Service Providing Strategy”, KIF(Knowledge, Insight and Frontier), Vol. 26, No. 12, 2017.

[7] S. B. Lee, “The Effect of Robo-Advisor to the Korean capital market”, KRX Market, Vol. 2016 Summer, 2016.

[8] S. H. Ahn, “A Study on the Trends and Regulation of Robo-Advisor Services Internationally and its Implication to Korea”, Journal of Korea Commercial Cases Association, Vol. 29, No. 2, 2016.

[9] Michael Negnevitsky, Artificial Intelligence, Trans. Y. H. Kim, Hanbit academy, 2016.

[10] K. S. Bock and J. S. Yoo, “Big Data in the Fourth Industrial Revolution”, Communications of the Korean Institute of Information Scientists and Engineer, Vol. 35 No. 6, 2017.

[11] Symantec, “Internet Security Threat Report”, Vol. 22, 2017.

[12] Will Knight, “How Long Before AI Systems Are Hacked in Creative New Ways?”, MIT Technology Review, 2016.

[13] I. J. Goodfellow, J. Shlens and C Szegedy, “Explaining and harnessing adversarial examples”, ICLR, 2015.

[14] B. Y. Kim, J. Y. Kwon and K. J. Yang, Capital Market Law, 3rd ed., PYbook, 2017.

[15] KSLA(Korea Securities Law Association), Capital Market Law Annotation Book(1), PYbook, 2015.

[16] J.Y Lim, Capital Market Law and Unfair Trading Practices, PYbook, 2014.

[17] KSLA(Korea Securities Law Association), Capital Market Law Annotation Book(1), PYbook, 2015.

[18] FSS(Financial Supervisory Service), “The Current State of Stock Unfair Trading Practices by SNS circulation and The Countermeasures”, News Release, 2017.

[19] KRX(Korea Exchange), “Observance Strengthening for Ultrashort-period Stock Price Manipulation using Small Order”, News Release, 2013.

[20] K. S. Kim and S. S. Jung, Capital Market Law, 2nd ed., Dusung Publishing, 2010.

[21] H. K. Kim, “A Study on Improvement of Class Action Suit System for the Financial Consumer Protection in Korea”, Commercial Law Review,

Vol. 33, No. 2, 2014.
[22] Y. J. Jeon, “Study to Improve The Securities Class Action Act”, Economic Reform Issue, Vol. 2016-5, 2016.
[23] H. S. Park, “Smart Society and Liability for Damages in the Civil Law”, The Legal Studies Institute of Chosun University, Vol. 23, No. 2, 2016.

저자소개

김 동 주(Dong-Ju Kim) [정회원]

- 1996년 : 서울대학교 전산학 전공 (구 계산통계학과)
- 2009년 : 영국 런던대학교 킹스칼리지 법학석사
- 2016년 : 고려대학교 정보보호대학원 박사과정 수료
- 2001 ~ 2014년 : 법무부 검찰국, 서울중앙지검 등 검사
- 2015년 : 금융위원회 법률자문관 (창원지검 부부장검사)
- 2016년 ~ 현재 : 김·장 법률사무소 변호사
- 2016년 ~ 현재 : 한국블록체인학회 운영위원
- 2017년 ~ 현재 : 한국주택금융공사 비상임이사
- 2017년 ~ 현재 : 한국거래소 시장감시위원

<관심분야> : 인공지능, 빅데이터, 개인정보보호, 금융, 형사법

권 헌 영(Hun-Yeong Kwon) [정회원]

- 2008년 ~ 2015년 : 광운대학교 법과대학 교수
- 2010년 ~ 현재 : 한국정보보호학회 이사
- 2014년 ~ 현재 : 총리소속 공공데이터 법제도분야전문위원회 위원장
- 2015년 ~ 현재 : 고려대학교 정보보호대학원 교수
- 2015년 ~ 현재 : 방송통신위원회 규제심사위원회 위원
- 2016년 ~ 현재 : 개인정보분쟁조정위원회 위원
- 2016년 ~ 현재 : 사이버커뮤니케이션학회 부회장
- 2017년 ~ 현재 : 한국교육학술정보원 이사
- 2017년 ~ 현재 : 한국인터넷윤리학회 회장

<관심분야> : 개인정보보호, 전자정부, 인터넷 윤리, 보안정책, 행정법

임 종 인(Jong-In Lim) [정회원]

- 2006년 ~ 2015년 : 고려대학교 정보보호대학원 원장
- 2010년 : 한국정보보호학회 회장
- 2012 ~ 2014년 : 대통령 직속 개인정보보호위원회 위원
- 2012년 ~ 현재 : 고려대학교 사이버국방학과 교수
- 2012년 ~ 현재 : 행정안전부 국가정보화포럼
- 2013년 ~ 현재 : 안전행정부 정부3.0 민간자문단 자문위원
- 2015년 ~ 현재 : 금융보안원 금융보안자문위원회 자문위원장
- 2015년 : 대통령 안보 특별보좌관
- 2016년 ~ 현재 : 한국 CISO협회 회장
- 2016년 ~ 현재 : 사이버보안정책센터 센터장

<관심분야> : 정보보호 거버넌스, 개인정보보호, 전자정부, 금융보안, 인공지능