논문 2022-2-6 http://dx.doi.org/10.29056/jsav.2022.12.06

징벌적 손해배상 제도 활성화를 위한 디지털 포렌식 활용방안 연구
- 지식재산 침해 사건을 중심으로 -

김종성*, 정세희**, 이선경**†

A Study on the Utilization of Digital Forensic System for the Activation of Punitive Damage System
- Based on the case of Intellectual Property infringement -

JongSeong Kim*, SeHee Jung**, SunKyung Lee**†

요 약

현재 지식재산 침해 범죄의 경우 주로 온라인 환경에서 범죄가 발생하며 이 때 온라인 데이터는 위법행위에 대한 사실관계를 증명하기 위한 중요한 요소로 작용한다. 한편, 징벌적 손해배상제도는 가해자가 불법행위로 인한 손해를 배상할 때 실제 손해액 그 이상의 배상금을 지급하도록 하여 유사한 불법행위를 반복하지 않도록 하는데 목적을 둔다. 징벌적 손해배상이 성립되기 위해서는 고의성 및 위법성 등 위법행위에 대한 인과관계가 구분되어야 한다. 그러나 온라인 데이터의 특성상 손쉽게 위·변조될 수 있어 위법성에 대한 사실관계를 증명하기에 어려움이 존재하고 있다. 따라서 변화하는 지식재산 침해 유형 중 디지털 기기를 활용한 범죄를 중심으로 징벌적 손배해상제도 활성화를 위해 고의 판단 시 디지털 포렌식 결과의 직접 활용 및 관련 제도 개편 방안 등을 제시한다. 이를 통해 디지털 포렌식 활용범위 확대를 통해 징벌적 손해배상제도의 객관적 고의성 판단기준에 기여하고자 한다.

Abstract

Currently, in the case of intellectual property infringement crimes, crimes occur mainly in the online environment, and at this time, online data acts as an important factor to prove the facts about illegal acts. On the other hand, the punitive damage compensation system aims to prevent repeating of similar illegal acts by requiring the perpetrator to pay more than the actual amount of damage when the perpetrator compensates for the damage caused by the tort. In order for punitive damages to be established, the causal relationship between intentional and illegal acts must be distinguished. However, due to the nature of online data, it can be easily forged or falsified, making it difficult to prove the facts about illegality. Therefore, we suggested direct utilization of digital forensic results for intentionality judgment and related institutional reform measures, focusing on crimes using digital devices. So, we want to contribute to the objective judgment standard of the punitive damages system by expanding the scope of digital forensic utilization.

한글키워드 : 징벌적 손해배상, 디지털 포렌식, 디지털 범죄, 지식재산 침해, 온라인 범죄, 고의성 판단

keywords : Punitive Damages, Digital Forensics, Digital Crime, Intellectual Property Infringement, Online Crime, Judgment of Intent

* 한국저작권보호원 과학수사지원부
** 중앙대학교 일반대학원 융합보안학과
† 교신저자: 이선경(email: cjsk3630@gmail.com)

접수일자: 2022.11.18. 심사완료: 2022.12.06.
게재확정: 2022.12.20.

1. 서 론

디지털 대전환시대, 4차 산업혁명과 과학기술 발전 등에 따라 IoT(Internet of Things), 모바일, 클라우드, 인공지능 등의 기술들이 등장하며 데이터 기반 산업구조로 전환되고 있다. 산업에서의 새로운 가치를 찾는 핵심요소로 신기술이 사용되는 반면 복합적인 유형의 범죄의 수단으로 활용되고 있다.

최근 온라인을 통한 지식재산 침해 범죄는 주로 온라인과 데이터를 기반으로 침해 범죄가 나타나고 있다. 과거와 달리 지식재산 침해 범죄는 단순한 기술유출 등의 침해행위가 아닌 불법도박, 불법정보 등과 결합되며 복합적인 범죄로 변질되고 있다. 그로 인해 범죄행위에 대한 사실관계 및 손해배상 등을 위해 사실관계 및 고의성 등을 입증하기에는 어려움이 존재하고 있다.

요컨대 저작재산권 침해의 주관적 요건인 의거성은 직접증거보다는 주로 사건 전후의 정황 등 간접사실에 의한 추정의 방식으로 입증하는 경우가 대부분이다. 이에 법원이 가지고 있는 경험치나 주관적 판단 등이 판결에 영향을 미치는 경우가 있다[1]. 실제로 같은 사건에 대하여 거의 동일한 사실관계를 인정하고 있음에도 불구하고 상반된 결론에 이른 판결 또한 있어 객관적인 판단 기준이 필요한 것이 현실이다.

한편 징벌적 손해배상에서 손해배상의 인정 여부가 가해자의 주관적 심리상태가 중요한 기준으로 작용한다. 이러한 이유들로 현행 법률은 징벌적 손해배상을 인정하는 데 모두 가해자의 주관적 요건을 규정하고 있다[2].

결론적으로 지식재산 침해 범죄에 사실관계 및 고의성 등을 입증하기 위한 한계가 커짐에 따라 징벌적 손해배상제도 활용의 어려움이 존재하고 있다.

따라서 본 고에서는 지식재산 침해 범죄의 유형 등을 살펴보며 국내 징벌적 손해배상제도를 활성화하기 위해 디지털 포렌식을 활용한 고의성 판단 여부 등을 중심으로 디지털 포렌식 활용범위 및 제도적 개선 방향을 살펴본다.

2. 디지털 범죄 현황과 징벌적 손해배상 제도

2.1 디지털 범죄 유형 및 현황과 지식재산 침해 범죄

초연결 기술과 기존 전 산업들이 융합하며 산업 생태계 등을 새롭게 맞이하고 있다. 하지만 과학기술의 영역이 확대됨에 이에 대한 양면성 또한 존재한다. 편리함을 누리기 위해 사용되는 여러 디지털 기기가 다양한 범죄에 활용되고 있기 때문이다. 초연결 시대 과학기술이 산업과 융합되며 발생되는 범죄의 유형을 분류하면 아래의 그림 1과 같다.

그림 1. 디지털 범죄 유형 분류 다이어그램
Fig. 1. Digital Crime Type Classification Diagram

그림 1 에 대해 설명하면 다음과 같다. 먼저 가장 큰 범위인 범죄는 디지털 기기를 활용하는 범죄 뿐만 아니라 디지털 기기를 활용하지 않는 폭행이나 절도 등과 같은 범죄를 포함한 모든 범죄를 의미한다. 다음으로 범죄를 좀 더 세부적으로 보면 “디지털 기기를 활용하는 범죄”가 있다. 예를 들어 모바일 기기로 범죄 방법을 검색하여

수행하는 계획범죄나 몰래카메라 촬영 등이 있다. 더 나아가 디지털 기기를 활용하는 범죄 내에서 범죄 발생환경을 기준으로 다시 분류할 수 있는데 이때 디지털 환경 내에서 일어나는 범죄를 사이버 범죄로 정의한다. 예를 들어 사이버 불링, 보이스피싱, 불법 성인물 유통, 해킹 등이 있다. 해당 분류로 미루어보아 오프라인에서"만" 일어나는 범죄를 제외한 대부분의 범죄가 디지털 범죄 유형에 모두 포함되는 것을 알 수 있다.

본 고에서는 특히 다양한 디지털 범죄 중 지식재산 침해 범죄를 주로 다루고자 한다. 그렇다면 디지털범죄 유형 분류에서 지식재산 침해 범죄는 어디에 해당하는지 짚고 넘어갈 필요가 있다. 먼저 지식재산 침해 범죄란 특허나 상표, 저작권 등 지식재산권법상 보호하는 창작물을 무단으로 활용 및 불법수익 창출 등의 불법행위를 의미한다[3]. 이를 디지털 기기를 활용하는 범죄 관점에서 구체적인 예를 들자면 다음과 같다.

먼저 디지털 환경 외에서 진행되는 지식재산 침해 범죄에는 USB 등을 활용하여 지식재산을 저장 및 전달하는 범죄 등이 있다. 즉 디지털 기기를 사용하되 범죄가 일어나는 것은 디지털 환경 외인 오프라인에서 발생하는 범죄를 말한다. 반면 디지털 환경 내에서 발생하는 지식재산 침해 범죄로는 타인의 지식재산(IP)을 불법으로 메일 등을 통해 유출하거나[4], 창작자의 저작물을 불법으로 복제하여 유통하여 불법수익 취득[5] 등이 있다.

최근 코로나 19로 인해 전통적인 TV, 영화 등의 콘텐츠 소비 대신 정보통신망을 통한 OTT(Over-The-Top)서비스 이용이 늘어나고 있다. 다수의 콘텐츠를 소비할 수 있는 온라인 대전환은 저작물을 무단으로 복제 및 인터넷 공간에서 게시가 매우 수월해져 무단으로 저작권 침해 문제가 대두되고 있다[6]. 또한 업무환경 변화로 인해 과거와 달리 기술유출도 클라우드 악용, 보안 시스템 무력화 등 비대면으로 바뀌고 있다[7].

고도화되는 과학기술과 환경의 변화로 인해 복합적인 유형의 지식재산 침해로 인해 창작자와 기업들은 경제활동에 심각한 폐해를 일으키고 있다. 기술진보와 문화발전을 위한 지식재산의 창출은 국가 경제의 밑거름이라 할 수 있지만 이에 대한 보호가 전혀 이뤄지지 않는다면 새로운 지식재산을 창출에 대한 유인이 줄어들며 경제적 가치가 있는 지식재산이 제3자로부터 부당하게 이용될 수 있다. 따라서 본 고에서는 디지털 환경에서 발생하는 지식재산 침해 범죄로 인한 피해를 최소화하기 위한 제도인 징벌적 손해배상제도에 대해 살펴보고자 한다.

2.2 징벌적 손해배상제도 개관

위의 2.1에서 디지털 환경 내에서 발생하는 지식재산침해 범죄를 정의했다. 한편, 본 저자들은 해당 범죄들의 처벌을 위한 여러 방안 중 징벌적 손해배상제도에 대해 중점적으로 다루고자 한다. 이에 본 문단에서는 징벌적 손해배상제도의 정의 및 의의, 그리고 각각의 법률에서 확인할 수 있는 징벌적 손해배상제도의 내용을 살펴본다.

2.2.1 징벌적 손해배상제도의 의의

징벌적 손해배상(Punitive Damages)이란 가해자가 불법행위 등으로 인해 손해를 배상함에 있어 특정한 사유 등이 존재할 경우 가해자로부터 실제 손해액 이상의 배상금을 지급하도록 명하는 제도를 말한다[8]. 가해자의 의도적 또는 악의적 등 불법행위로 인해 발생되는 피해자의 실제 손해액 이상의 손해액을 지급하는 제도로서 유사한 불법행위를 반복하지 않도록 예방하는 것을 목적으로 한다[9][10]. 징벌적 손해배상은 최초 영국에서 징벌적 손해배상제도가 정립되며, 이후 영미법계 국가인 미국, 호주 등에서 동 제도가 활성화되어 있다[11]. 이후 대륙법계 국가에서도 도

입되는 추세이다[12].

우리 법원의 태도에 따르면 징벌적 배상이란 가해자에게 특히 고의 등의 주관적인 사정이 있는 경우에 보상적 손해배상에 덧붙여 위법행위에 대한 징벌과 동종행위의 억지를 주목적으로 하여 과하여지는 손해배상으로 코몬로(common law)상 인정되고 있는 구제방법으로 보고 있다[13].

동 제도는 주로 소비자 보호 관련 법률 등에서 규정되었지만 최근 지식재산 분야에도 도입되고 있다. 따라서 징벌적 손해배상제도는 비재산적 손해의 전보적 기능을 가지고 있으며 특정 영역에서 징벌적 손해배상제도의 도입은 악의적 불법행위에 대한 강한 제재 등의 기능을 수행될 수 있다[14].

2.2.1.1 징벌적 손해배상제도 성립요건

징벌적 손해배상이 인정되기 위해서는 불법행위에 대한 판단이 필요하다. 따라서 민사상 불법행위 손해배상이 적용되기 위해 「민법」상 불법행위와 요건을 살펴보아야 한다. 불법행위의 요건으로 i) 고의성 또는 과실, ii) 위법성, iii) 책임성, iv) 위법행위에 대한 인과관계로 구분할 수 있다[15]. 위의 요건에 대해 손해배상을 청구하는 피해자는 해당 불법행위에 대해 직접 입증해야 한다. 따라서 손해배상에 대한 요건의 해당 여부에 대한 구체적인 판단기준도 기본적인 민사상 불법행위 손해배상과 동일하다[16]. 징벌적 손해배상은 「민법」상 불법행위와 차이점으로 i) 불법행위 손해배상은 위법행위의 종류를 판단하지 않고 위법행위에 대해서 손해를 모두 인정하는 반면 징벌적 손해배상의 경우 해당 분야에 대한 한정된 위법행위에 대한 손해를 인정하며, ii) 불법행위의 성립요건 중 고의·과실의 경우 민법상 불법행위는 피해자가 해당 존재를 입증해야 하지만, 징벌적 손해배상은 해당 부분에 대해 피해자가 그 부존재를 입증해야 한다[16].

2.2.1.2 국내 징벌적 손해배상제도 현황

국내에서 처음으로 징벌적 손해배상제도를 도입한 것은 2011년 「하도급 공정화에 관한 법률」개정을 통해 원사업자가 수급 사업자의 기술자료를 유용하는 행위에 대해 배상하게 한 것이었다. 이후 「개인정보보호법」 및 「특허법」등 다수 법령에 도입하게 되었다. 징벌적 손해배상제도에 대해 각 개별 법령에서는 해당 산업분야에 대한 불법행위 등에 대한 징벌적 손해배상제도의 규정을 두고 있다. 현재까지 도입된 징벌적 손해배상은 가해행위의 악의성을 전제로 전보배상제도로 불법행위 억제가 어렵거나 특별한 보호 필요성이 있는 영역을 대상으로 예외적으로 도입되고 있는 것을 파악할 수 있다[17].

2.2.2 지식재산 침해범죄 관련 법률 내 징벌적 손해배상제도 비교분석

본 고에서는 앞서 언급한 것처럼 지식재산 침해 범죄를 중점으로 다루고자 한다. 이에 특히 지식재산 침해 범죄와 관련 법률들은 「산업기술의 유출방지 및 보호에 관한 법률」(이하 산업기술보호법), 「부정경쟁방지 및 영업비밀보호에 관한 법률」(이하 부정경쟁방지법), 『저작권법」으로 선정한 후 해당 법률 내 징벌적 손해배상 조항을 살펴보고자 한다.

먼저 「산업기술보호법」에서 언급하고 있는 손해배상제도 내용은 다음과 같다. 「산업기술보호법』에서는 제22조의2(산업기술의 유출 및 침해행위에 대한 손해배상책임), 제22조의3(자료의 제출)에서 손해배상을 언급하고 있다. 해당 법률에서는 특허법과는 다르게 산업기술침해행위가 고의적인 것으로 인정되는 경우에만 손해액의 3배를 넘지 않는 범위에서 배상액을 산정한다.

다음으로 「부정경쟁방지법」에서는 제5조(부정경쟁행위 등에 대한 손해배상책임), 제6조(부정경쟁행위 등으로 실추된 신용의 회복), 제14조의

2(손해액의 추정 등)에서 손해배상제도를 언급하고 있다. 고의 또는 과실에 의한 타인의 영업상 이익을 침해하여 손해를 입힌 자에게 손해를 배상할 책임을 진다. 법원은 침해 행위가 고의적인 것으로 인정되는 경우에는 손해로 인정된 금액의 3배를 넘지 아니하는 범위에서 배상액을 정할 수 있다.

마지막으로 「저작권법」에서는 제125조(손해배상의 청구), 제125조의2(법정손해배상의 청구), 제126조(손해액의 인정)에서 손해배상제도를 언급하고 있다. 고의 또는 과실로 권리를 침해한 자에 대하여 저작재산권자 등이 손해배상을 청구할 수 있다. 침해자가 침해행위로 인해 이익을 얻은 경우, 그 이익의 액을 손해액으로 추정한다. 권리의 행사로 통상 받을 수 있는 금액에 상응하는 금액을 손해액으로 손해배상을 청구할 수 있다. 권리행사로 통상 받을 수 있는 금액보다 손해액이 많을 경우, 초과액에 대해서도 손해배상을 청구할 수 있다. 각각의 법률 내에 별도로 있는 조항으로 징벌적 손해배상제도가 도입되었지만, 조항의 내용은 매우 유사하며, 정보유출 범죄, 환경범죄, 기타 경제범죄 산업별로 별도 특이사항을 적용하지 않음을 알 수 있다. 앞선 내용을 정리한 결과는 표 1과 같다.

표 1. 지식재산 침해 범죄 관련 법률과 징벌적 손해배상제도

Table 1. Laws related to intellectual property infringement crimes and punitive damages system

구분 (법령)	조문	위법행위	배상액 고려사항
산업기술보호법	제22조의2제2항	산업기술 침해행위	(1)침해행위를 한 자의 우월적 지위 여부, (2)고의 또는 손해 발생의 우려를 인식한 정도, (3)침해행위로 인하여 영업비밀 보유자가 입은 피해규모, (4)침해행위로 인하여 침해한 자가 얻은 경제적 이익, (5)침해행위의 기간·횟수 등, (6)침해행위에 따른 벌금, (7)침해행위를 한 자의 재산상태, (8)침해행위를 한 자의 피해구제 노력의 정도
부정경쟁방지법	제14조의2제6항	아이디어 및 영업비밀 침해행위	
저작권법	제125조	저작권 및 해당 권리자에 대한 권리 침해행위	

2.3 우리나라의 도입 시 문제점

징벌적 손해배상제도의 목적 및 기능은 처벌과 억제이다. 즉, 불법행위를 자행한 가해자를 처벌함으로써 범죄자의 불법행위를 예방하고 나아가 일반사회에 대해 본보기를 보여줌으로써 유사한 불법행위의 재발을 방지하는 억제기능을 수행하게 된다[18]. 징벌적 손해배상제도를 도입함으로써 범죄 억제 효과를 기대한다. 하지만 법원이 징벌적 배상을 실제로 명한 사례는 극히 드물며, 그로 인해 징벌적 손해배상제도는 조문으로만 존재하는 제도가 될 우려가 있다[19]. 징벌적 손해배상은 손해액 산정에서 법관의 재량을 지나치게 넓혀 판결의 예측 가능성을 떨어뜨리는 문제가 있다고 지적받는다[20].

따라서 우리나라 현행법상 도입된 징벌적 손해배상제도에 대한 이러한 한계점과 실효성에 대한 문제가 대두되고 있다. 이에 본 저자들은 징벌적 손해배상이 판결 등에 활용되고 있지 않는 이유에 대해 논의해보고자 한다.

2.3.1 온라인 IP 범죄와 고의입증의 한계

온라인을 통한 지식재산(IP)범죄는 기존 일반적 범죄와 달리 온라인 환경의 특징인 하나의 데이터를 복제 및 전송, 삭제 등을 할 수 있어 범죄 관련 디지털 증거물을 조작할 수 있다[21]. 특히 지식재산(IP)은 무형자산으로서 물리적 형체가 없어 제3자로부터 손쉽게 침해될 수 있다. 최근

데이터 등을 부정하게 사용하는 행위를 근절하기 위해 「부정경쟁방지 및 영업비밀보호에 관한 법률」(시행 2022. 4. 20.)개정을 했다.

경찰청의 사이버 범죄 발생 현황 자료에 따르면 불법콘텐츠 범죄는 2019년 24,945건, 2022년 30,160건으로 매년 증가하고 있다. 이러한 불법행위에 대해 우리나라 지식재산권법에는 징벌적 손해배상제도 등이 도입되었다. 하지만 온라인 환경에서 발생하는 범죄행위에 대한 사실관계 등을 파악하기에는 어려움이 존재한다.

온라인을 통한 지식재산 침해 범죄에서는 범죄사실을 확인하기 위해 디지털 증거 확보 및 객관적 분석 등을 통해 고의성 및 사실관계 파악이 중요하다. 또한 앞서 언급한 바 지식재산 침해와 같은 불법행위에 대해 징벌적 손해배상제도를 활용하기 위해 “고의성” 및 불법행위에 대한 사실관계 등이 증명되어야 한다. 우리나라 특허법 또한 증액손해배상을 획득하려는 원고에게 피고의 고의를 증명하도록 요구하고 있으며(동법 제128조 제1항), 상표법 등 이외 지식재산권법들에서도 동일한 입법형식을 취하고 있다. 하지만 온라인을 통해 침해된 지식재산 범죄의 경우 디지털 증거를 확보하지 못할 시 불법행위에 대한 손해배상 등이 권리자에 대한 IP 침해 구제방법이 어려워질 수 있다.

또한 특허권 침해에 대해 고의성이 있을 경우 이는 형사처벌의 대상이다. 서울고등법원 2007. 8. 16. 선고 2007노929 판결에 따르면 피고 측은 검찰 측 포렌식 조사관 혼자만의 디지털 증거 분석・처리 결과에 대한 신뢰를 인정하기 어려움을 나타내었다.

서울남부지방법원 2012.2.2 선고 2010가합1884 판결과 항소심인 서울고등법원 2012나17150 판결이 상반된 판결이 발생했다. 본 사건의 1심에서는 저작권 침해와 아이디어 무단이용에 관한 책임을 모두 부정하며 항소심에서는 저작권 침해와 일반 불법행위 책임을 모두 인정했다[1]. 해당 판결에서 1심과 항소심의 견해가 달랐던 이유로는 바로 주관적 요건(의거성) 부분의 해석에 대한 차이이다. 의거 관계는 피고가 원고 저작물에 대한 접근 가능성과 양 저작물 사이의 유사성 등의 간접사실이 인정되면 추정될 수 있다[22]. 항소심에서는 의거관계를 인정하는 데 필요한 유사성 판단을 위한 자료에는 ’아이디어’나 ‘주제’가 포함될 수 있다고 판시하고 있다. 따라서 본 사건에서 ‘현저한 유사성’이 존재함을 근거로 하여 주관적 요건인 의거성을 추정한 것으로 판단된다[1]. 이처럼 주관적 요건에 대해 법원에 해석에 따라 판결이 달라질 수 있기 때문에 주관적 요건을 최대한 객관적인 데이터로 제시하는 것이 필요하다.

앞선 이유들로 본 저자들은 징벌적 손해배상 제도 활용성이 낮은 이유로 고의성 여부 판단 시 객관성 부족을 주장하고자 한다. 징벌적 손해배상의 손해액 산정을 결정하는 주된 요인으로 작용하는 것은 고의성 여부에 대한 판단이다. 하지만 이 고의성을 입증할 때 증거나 자료들이 누구나에게 그렇다고 인정할만한 객관성 부여되기 어렵다.

손해배상액 산정이 법원 재량에 맡겨져 있는 지금 고의성 여부를 증빙하는 자료에 객관성이 부족하다면 법원마다 각자 중점적으로 고려하는 상황에 따라서 다양한 결론이 나올 수 있다. 결론적으로 징벌적 손해배상제도가 활성화되기 위해서는 제3자가 보았을 시 객관적 판단에 용이할 수 있는 자료가 필요하다.

2.3.2 지식재산 관련 감정과 디지털포렌식

소송법상 감정이란 특별한 학식·경험 등이 있는 제3자의 보고를 요구하는 증거조사를 의미한다(민사소송법 제333조 이하, 형사소송법 169조). 우리나라 지식재산권법에는 지식재산 분쟁이 발

생할 경우 법원 및 수사기관 등으로부터 재판 또는 수사를 위해 지식재산 침해 등에 관한 감정을 할 수 있다(저작권법 제119조, 특허법 제128조의2). 이는 법관의 사건에 대한 판단능력을 보충하기 위한 목적이다. 현행법에 따르면 지식재산 침해 관련 감정의 범위는 크게 i) 실질적 유사성 판단을 통해 침해 여부 및 ii) 지식재산 손해액 판단 등으로 구분될 수 있다. 한국저작권위원회의 감정 제도 소개에 따르면 감정 분야에는 일반저작물과 컴퓨터프로그램저작물이 있다. 일반저작물은 저작물의 실질적 유사성 여부를 감정해주고, 컴퓨터프로그램저작물의 경우에는 동일(복제) 유사성 여부, 완성도(하자) 여부, 개발에 소요된 비용 및 단가 판단 등을 수행하고 있는 것으로 확인된다[23].

또한 「특허법」 제128조의2에 따르면 특허권 또는 전용실시권 침해소송에서 법원이 침해로 인한 손해액의 산정을 위하여 감정을 명한 때에는 당사자는 감정인에게 감정에 필요한 사항을 설명하여야 한다. 이는 특허침해 소송에 있어 손해액을 산정하기 위한 수단으로 감정업무를 수행하고 있다.

「형사소송법」 제313조제2항에 따르면 법원 또는 수사기관은 제3자로부터 디지털포렌식 기술을 활용한 감정을 할 수 있다. 하지만 현재 지식재산 분야에서 수행하는 감정은 (1) 저작물에 대한 실질성 유사성 여부를 판단 및 (2) 침해소송에서의 피해액 등을 산정할 경우에만 활용되고 있다. 특히 소프트웨어 저작권 침해 감정의 경우 파일 시스템의 유형, 개발자의 컴퓨터프로그램 소스코드 패턴 등 고유의 특징점을 포렌식 정보로 활용할 수 있다[24]. 하지만 해당 포렌식 활용은 저작물에 대한 실질적 유사성 판단을 위해 저작물 침해 여부만 판단할 수 있다.

따라서 지식재산 침해 관련 감정은 저작물에 대한 실질적 유사성만을 판단하며 지식재산 범죄 행위에 대한 고의성 여부 등의 판단은 수행하지 않는다.

본 고에서는 지식재산 침해에 있어 고의성 판단이라는 주관적 요건은 지식재산권의 실질적 유사성뿐만이 아니라 피고의 범죄 인지 여부 또한 중요한 판단 요소이다. 따라서 다음 장에서 해당 지식재산 침해 범죄의 전주기적 과정에 대한 실제 사례를 기반으로 제작된 시나리오 과정에서 디지털 증거를 확보 및 법원에서의 법적 증거능력을 담보할 수 있는 방안 등에 대해 제시하고자 한다.

3. 디지털 포렌식과 고의성 입증 사례

2장에서 현재 발생하고 있는 디지털 기술 관련 지식재산 침해 범죄 및 해당 범죄 처벌을 위한 징벌적 손해배상 제도를 검토한 결과, 해당 제도가 활성화되기 위해서는 고의성 여부를 객관적으로 판단할 수 있도록 지원해야 함을 밝혔다.

특히 온라인 공간 등을 활용한 지식재산 침해 범죄에서는 범죄사실을 확인하기 위해 디지털 증거 확보 및 객관적 분석 등이 필요하다. 객관적인 증거의 확보가 어려워진다면, 법원에서 징벌적 손해배상 판결을 위해 고려해야 하는 사항들의 검토가 어려워질 수 있다. 따라서 본 저자들은 다양한 데이터 증거를 확보할 수 있으며 고의성 여부에 대한 객관성 마련을 위한 지원방안으로 디지털 포렌식을 제시하고자 한다.

3.1 디지털 포렌식 개념과 특징

디지털 포렌식(Digital Forensic Science)란 컴퓨터 범죄와 관련하여 디지털 장치에서 발견되는 자료(Data)를 복구하고 조사하는 법과학의 한 분야이다[25]. 디지털 기기에 남아 있는 자료(Data)를 통해 일련의 사실관계 등을 파악하여 수사에

활용하고 법정에서 증거로 활용될 수 있게 한다. 따라서 디지털 포렌식은 디지털 데이터에 대한 조사결과가 법정에서 증거로 채택되는 것을 목표로 하며 디지털 증거물에 대해 수집에서의 과정에서 적법한 절차가 지켜져야 한다[26].

디지털포렌식 기술의 핵심은 디지털 데이터를 기반한 행위기반의 범죄행위를 파악할 수 있다. 하지만 데이터로 구성된 디지털 증거는 표 2와 같은 특징이 있어 다루기 위한 전문적인 디지털 포렌식 기술이 필요하다.

표 2. 디지털 증거 특징[27]
Table 2. Digital Evidence Features

특징	설명
매체 독립성	데이터 내용이 생성, 삭제에 영향을 미치지 않는다면 데이터의 정보 값이 같다면 어느 매체에 있든 정보 값이 같음
대량성	디지털 증거는 무형의 형태로 방대한 분량의 정보를 하나의 저장매체로 저장이 용이하며, 다양한 정보와 혼합될 수 있음
취약성	컴퓨터 등의 데이터는 쉽게 정보를 삭제, 변경 등을 할 수 있어 증거 훼손 및 위·변조행위가 발생할 수 있음
비가시성 · 비가독성	디지털 증거는 데이터로 표현되며 하나의 결과값이 무형의 형태로 사람이 인식하도록 출력하는 절차변환과정 등이 필요함
전문성	디지털 증거에 대한 법적 증거능력을 위해 디지털 증거의 수집 과정에서 분석까지 일련의 절차와 전문적인 기술이 사용됨

3.2 디지털 포렌식과 고의입증 관련 사례

다양한 기술의 발전으로 기존 물리 공간에서 발생하던 불법행위는 사이버 공간을 활용한 불법행위로 발전되었다. 그로 인해 사이버 공간에서 발생되는 불법행위에 대해 대응할 수 있는 새로운 방식이 필요하다. 특히 온라인 공간 등을 활용한 지식재산 침해 범죄에서는 책임소재 등을 확인하기 위해 고의성 판단 여부가 처벌의 중요한 요소이다. 따라서 본 절에서는 주요국의 디지털 증거물을 바탕한 불법행위 고의성 판단에 관한 사례분석을 검토하고자 한다.

3.2.1 21ST CENTURY SYSTEMS INC v. PEROT SYSTEMS GOVERNMENT SERVICES INC(2012)[28]

소프트웨어 개발업체인 PEROT(원고)가 과거 직원들과 21ST CENTURY SYSTEMS 기업(피고)를 대상으로 영업비밀 침해 등을 주장하며 이에 대한 손해배상 소송을 청구했다. 당시 원심에서는 법원은 컴퓨터 포렌식 등을 통해 확인한 바 원고가 주장하는 피고의 영업비밀 및 비경쟁 및 계약위반 등에 대한 주장을 받아들였다. 이에 피고로부터 징벌적 손해배상과 컴퓨터 포렌식 조사 비용 등을 청구했다. 이후 피고는 해당 판결에 대해 항소를 제출하며 원고가 컴퓨터 포렌식 조사를 위한 지불 비용을 보상할 필요가 없다고 주장했다.

당시 컴퓨터 포렌식 조사관인 Shannon Perkins("Perkins")는 원고를 위해 컴퓨터 포렌식 분석 전문가로 증언한 내용은 아래와 같다. Perkins는 피고가 원고에 있는 데스크탑 컴퓨터에서 외장 하드 드라이브로 수천 개의 파일을 복사했으며 수많은 파일이 원고의 데스크탑 컴퓨터에 있는 파일과 일치하며 해당 파일들은 과거 원고의 직원이 퇴직한 이후 피고의 회사에 있는 컴퓨터에 복사되었다고 증언했다. 이에 법원은 디지털 포렌식 전문가인 Perkins의 컴퓨터 포렌식 분석결과와 증언 등을 기초하여 해당 영업비밀이 침해된 행위를 인정하며 고의적으로 해당 영업비밀을 침해한 행위에 대해 징벌적 손해배상액 및 디지털 포렌식 조사 비용 등을 보상해야 한다고 판결했다. 동 사건에서 살펴볼 수 있듯 내부 직원들에 의해 고의적이고 악의적인 방법을 통해 기술 유출한 행위를 원고가 제시한 디지털 포렌식 분석을 통해 밝혀냈다. 따라서 영업비밀 유출 행위에 대한 고의성 여부 판단 시 디지털 포렌식이 활용된 사건이다.

3.2.2 Klipsch Group, Inc. v. ePRO E-Commerce Ltd. (2018)[29]

2012년 헤드폰 및 음향기기 등을 제조하는 Klipsch(원고)는 ePRO(피고)의 자회사인 DealExtreme.com가 원고의 제품을 위조하여 판매했다고 주장하며 소송을 청구했다. 이에 피고는 일부 원고의 제품이 침해되어 판매되었다는 점에 대해 이의를 제기하지 않았지만, 원고가 제기한 피해 규모와 달리 다른 피해액 등을 주장했다. 원고는 피고가 불법으로 제작한 위조품에 대해 최소 500만 달러에 판매했다고 주장하며 피고는 전 세계적으로 관련 제품의 매출이 8,000달러 미만이라고 주장했다. 이에 법원은 처음 주장한 피고의 증거가 설득력이 있다고 판단했으며 원고의 조사관이 2017년 1월에 판매되고 있는 두 개의 다른 위조 원고의 제품을 발견한 후에도 사건의 가치에 대한 견해를 크게 수정하지 않았다. 그러나 사건이 진행됨에 따라 피고는 소송 절차 등을 준수하지 않았다. 해당 준수 사항을 보완하기 위해 판사는 원고가 피고의 컴퓨터 시스템에 대한 독립적인 법의학 검사를 수행하도록 승인했다.

원고는 Daniel Regard가 이끄는 iDiscovery Services("iDS")를 고용하여 조사를 실시했다. Regard는 피고의 직원이 파일, 이메일 및 기타 사건과 관련 가능성이 있는 데이터를 삭제했다고 진술했다. 피고는 재해 복구 목적으로 데이터베이스의 백업 복사본을 보존하지 않았기 때문에 데이터 기록이 없다고 진술했다. 이와 관련하여 Regard는 관리인이 수천 개의 파일과 이메일을 수동으로 삭제하는 등 다양한 형태의 약탈에 가담했다는 사실을 발견했다. 이에 법원은 피고가 의도적으로 일부 파일을 복구할 수 없게 하였음을 인정했다. 이에 법원은 피고가 해당 문서를 보관할 의무가 시작된 후 관련 파일을 폐기했음을 배심원단에게 확인하도록 요구하며 배심원단이 파기된 증거와 원고에게 유리할 것이라고 추정하도록 하며 불법행위에 대한 합리적인 비용 및 수수료 등에 대해 원고의 3배 손해배상을 부과했다. 동 사건은 법원이 원고의 디지털 포렌식 결과를 증거로 채택하며 피고의 의도적인 파일 삭제 등에 대한 행위를 인정한 사건이다. 당초 피고가 주장한 피해액을 인정하였으나 원고가 추가로 진행한 디지털 포렌식 결과로 인해 손해액이 변경된 사례이다.

3.2.3 東京地方裁判所 平成25(ワ)30447 平成28年4月27日[30]

원고는 1980년에 창업한 이래 광학 측정기의 설계, 제조, 판매 및 오토 포커스 기술 등 개발하며 제품의 도면 및 부품표 등을 디지털 데이터로 제작하여 사내 서버에 보관하고 있었다. 원고의 직원인 피고는 원고의 영업비밀인 기술, 제품 도면인 전자 데이터가 보관된 시스템에 접근하여 무단 다량의 데이터를 취득하고 USB 메모리 등에 저장했다. 이에 원고는 피고가 무단으로 획득한 영업비밀인 전자 데이터 및 인쇄된 도면 자료 등에 대해 폐기를 요청하며 피고의 행위에 대해 원고는 취업 규칙상 징계해고 사유에 해당하여 피고에게 지급될 퇴직금에 대해 피고가 불법으로 취득한 정보로 인한 손실이 발생했다고 주장하며 부당 이득 반환 청구 소송을 청구했다. 반면 피고는 원고의 제조 및 판매하는 제품은 광학 기술, 기계 기술, 소프트웨어 기술 등 고객 수요에 맞게 적용한 것으로 기본적인 광학계 이론 등과 기술자 개개인의 기술 능력과 경험으로 바탕으로 재현이 가능하며 이는 도면과 모든 기술정보는 유용한 것이 아니므로 본 전자 데이터는 영업비밀이 아니라고 주장했다. 이에 법원은 ① 본건 데이터는, 광학 측정기의 설계, 제조, 판매 등을 업으로 하는 원고의 최근의 주력 제품인 2 라인 센서 방식의 오토 포커스 현미경, 자동식 마이크로 스캐닝 스테이지 및 레이저 오토 콜리메이터

의 조립도, 부품도 및 부품표인 것, ② 원고에 있어서, 조립도, 부품도 등의 도면이나 부품표는, 과거에 제작한 제품의 도면을 그대로 사용하거나, 혹은 CAD 소프트웨어로 수정을 하거나 설계, 개발에 필요한 기간을 단축하는 목적 등에 사용하기 위해 보관되어 있는 것, ③ 도면이나 부품표의 디지털 데이터는 사내 서버에 저장된 후, 사내 문서 관리 시스템 인 아크 스위트를 사용하여 관리되며 원고 직원이 데이터를 검색, 열람, 인쇄하려면 소정의 이용 등록을 받아야하며, 서버에 축적된 데이터 개별적으로 또는 일괄적으로 다운로드하여 기록 매체에 저장할 수 있는 권한을 부여받은 것은 기술 부서의 일부 직원에게 제한되어 있었기 때문에 이 데이터는 모두 원고에서 비밀로서 관리되고 있는 생산방법 그 밖의 사업활동에 유용한 기술상의 정보로서, 공개적으로 알려지지 않은 것이므로 이는 영업비밀에 해당하는 것으로 인정되었다. 또한 피고는 2010년 6월부터 10월까지 5개월 간 아크 스위트 시스템을 통해 4만 8964건의 디지털 데이터를 다운로드한 것에 대해 보면 원고가 동 시스템에 보관하고 있는 모든 설계 데이터에 상당하며 상기 기간 중에 동 데이터를 다운로드한 행위는 부정경쟁방지법 제2조제1항4호의 부정의 수단에 의해 영업비밀을 취득한 행위로 추인했다. 이에 법원은 피고는 원고의 영업비밀을 불법으로 취득한 것에 대해 인정하는 것으로 판결했다.

3.3 시사점

주요국들의 사례 등을 통해 확인한 결과, 사이버 공간을 활용한 디지털 데이터를 통해 불법행위, 범죄행위의 사실관계 확인에 디지털포렌식 분석결과가 사용되고 있다. 특히 Klipsch Group과 ePRO E-Commerce 사의 사례에서 볼 수 있듯이 디지털포렌식 분석 결과가 재판 결과까지 변경하는 중요한 역할을 하는 것을 볼 수 있었다. 피고가 의도적으로 재판 관련 파일을 삭제하는 등의 디지털포렌식 분석은 범죄사실의 사실관계 및 고의성 판단에 활용되는 것을 알 수 있다. 즉, 디지털 데이터를 활용한 불법행위에 대한 인과관계를 확인하고 이에 대한 위법행위를 확인하기 위한 핵심증거로 활용되고 있다.

실제로 2021년 특허청 영업비밀 소송 판결문을 분석한 결과 대부분 소송의 75% 이상에서 이메일이 중요한 증거로 활용되는 등 디지털 증거가 실제 재판에서 영업비밀 침해 입증에 결정적인 역할을 하고 있다는 것으로 나타났다[31]. 이에 우리나라의 판결에도 디지털 포렌식이 활용되고 있으나 징벌적 손해배상 제도에서의 적용은 미비하다. 따라서 다음 4장에서 디지털 포렌식이 특히 징벌적 손해배상 제도에 활용될 수 있도록 방안을 제시하고자 한다.

4. 디지털 포렌식 활용방안 제언

앞서 3장을 통해 본 저자들은 실제 법원에서 징벌적 손해배상 판결을 내릴 때 디지털 포렌식을 활용한 사례를 분석했다. 또한 우리나라에서도 영업비밀 관련 판례에서 디지털 포렌식이 사용되고 있음을 알 수 있었다. 이에 본 저자들은 징벌적 손해배상 제도에서 디지털 포렌식 기술을 활용한 개선방안을 아래와 같이 제언하고자 한다.

4.1 고의판단에의 디지털 포렌식 결과 활용

본 저자들은 디지털 포렌식 기술을 활용하여 법원에서의 징벌적 손해배상 객관적인 판단을 돕고자 한다. 고의 또는 손해발생의 우려를 인식한 정도를 판단하기 위해 객관적인 증거가 필요하며 이를 디지털 포렌식 분석으로 가능할 것임을 아래 시나리오를 통해 제언한다. 해당 시나리오는 실제 사례를 각색했다.

시나리오 1.
신고자 C는 자신의 지적재산물을 피의자 B가 무단 사용하고 있는 것을 인지했다. 피의자 B를 대상으로 경찰이 수사한 결과, A가 최초유포자임을 알게 되었으며 A와 B가 고의적으로 C의 지적재산물을 침해했다는 것을 확인하기 위하여 A의 디지털 기기(PC, 모바일)를 디지털 포렌식 전문가에게 감정을 맡겼다.

다음의 표 3은 디지털 포렌식 분석을 통해 알 수 있는 정보들의 예시이다. 시나리오를 아래의 증거 예시를 기반으로 범죄행위를 객관적으로 입증해나가는 과정을 설명하고자 한다.

표 3. 징벌적 손해배상 고의판단 디지털 증거 및 시나리오
Table 3. Digital Evidence Analysis Scenarios for Punitive Damages Determination of Intentionality

디지털 증거 유형(예시)	설명 및 시나리오
파일 삭제 정보	파일 삭제 여부 및 내역 등 관련 정보
	삭제된 파일 현황 파악 및 복구 등 관련 내용 확인 가능
디지털 파일 메타데이터	파일의 수정 여부를 확인할 수 있는 정보 (파일 생성, 수정, 접근 날짜, 생성자 등)
	디지털 파일의 위·변조 내역을 확인해 고의성 여부 판단 가능
브라우저 검색기록	Chrome, Internet Explore 등 검색엔진을 통한 검색 히스토리 등 관련 정보
	브라우저 검색 기록 확인을 통해 계획범죄 여부 등 고의성 여부 판단 가능
통신내역	문자, 전화, 카카오톡 메신저 등 통신내역 및 내용을 확인할 수 있는 정보
	연락 내역 및 내용 확인을 확인해 공범 및 계획범죄 여부 등 고의성 여부 판단 가능
위치정보	디지털 기기를 사용한 시점의 사용자 위치를 확인할 수 있는 정보
	범죄 행위를 할 당시의 사용자 위치 파악을 통해 본인을 숨기려는 의도 등 고의성 여부 판단 가능

case 1. A의 PC 분석결과 2022년 11월 10일 오전 8시경, n개의 파일 및 실행 파일, 브라우저 검색기록 삭제 등의 작업이 이루어진 것을 확인하고, 해당 파일 및 내역을 디지털 포렌식으로 복구했다.

case 2. 복구된 파일의 메타데이터를 확인한 결과, n개의 파일은 모두 생성일시가 2022.11.9. 오후 9시인것으로 확인되었고, 수정일시는 생성일시보다 빠른 것을 확인했다. 이는 해당 컴퓨터에 n개의 파일을 복사한 것으로 해석할 수 있다. 또한 컴퓨터 연결 기기 내역 확인 결과, 2022.11.9. 오후 10시경 외부저장장치(USB) 연결 흔적을 발견했다.

case 3. 자동저장된 브라우저 히스토리 로그 파일 확인 결과, A는 2022.11.1.부터 2022.11.5.까지 구글 검색엔진을 통하여 '저작권법', '지식재산권 유출', '파일완전삭제' 등을 검색한 흔적을 발견했다.

case 4. A의 모바일 분석결과, 2022.11.9. 오후 9부터 2022.11.10. 오후 8시까지 B와 총 11건의 통화 및 5건의 메일을 주고받은 흔적을 찾을 수 있음. 카카오톡 내역 확인 결과, 2022.11.10. 오후 4시에 A카페에서 약속한 기록을 확인할 수 있다.

case 5. 2022.11.10. 오후 3시경, A의 거주지와 5시간 거리에 있는 A카페 네비게이션 검색 결과와, 2022.11.10. 오후 5시경, 모바일과 연결된 와이파이 위치가 네비게이션 결과와 동일함을 확인할 수 있다.

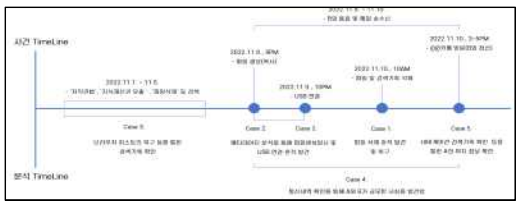

그림 2. 사건 및 디지털 포렌식 분석 타임라인
Fig. 2. Incident and Digital forensic Analysis Timeline

결론적으로 해당 사건의 타임라인을 정리하면 그림 2와 같다. 또한 각 시나리오와 앞서 언급한 데이터 증거물을 연관지어 표 4와 같이 고의성 판단의 근거를 제시했다.

표 4. 시나리오 케이스별 데이터 유형을 반영한 고의성 판단
Table 4. Determination of Intentionality by reflecting Digital Evidence by Cases

구분	데이터 유형	고의성 판단 예시
Case 1	파일 등 삭제 데이터	피의자가 고의로 관련 증거 삭제 등을 했다고 해석할 수 있는 데이터
Case 2	생성일시 등 메타데이터	사건의 타임라인(파일 생성, 복사, 삭제 등) 확인 가능하여 case3. 4.5와 결합하여 사건의 고의성 여부 판단에 기여할 수 있는 데이터
Case 3	검색기록 등	해당 행위가 범죄임을 인지하고 있는지 등을 확인할 수 있는 데이터
Case 4	통신 데이터	공모 사실 및 범죄 행위 동기 등을 파악할 수 있는 데이터
Case 5	위치 데이터	피의자가 사내 보안 시스템 등을 우회하여 유출하였는지 확인 가능한 데이터

디지털 포렌식을 통해 A의 디지털 기기를 분석한 결과, A와 B가 공모하여 C의 창작물을 불법유통했다는 사실을 발견했다. 특히 A는 해당 행위가 범법행위임을 인지하고 관련 내용을 검색했고, 범죄사실을 숨기기 위해 파일을 삭제하는 등의 행위를 한 것을 확인할 수 있었다. 위 시나리오에서 제안한 것처럼 디지털 포렌식 분석 결과를 징벌적 손해배상 고려사항에의 고의성 판단에 직접적 증거로 활용하는 것이 가능해진다면 보다 객관적이고, 공정한 판결을 낼 수 있을 것으로 기대한다.

4.2 디지털 포렌식 활용 제고를 위한 제도 개편 방안

앞서 살펴본 바 디지털 포렌식 분석 결과가 재판에 직접 활용되기 위해서는 추가적으로 제도적인 측면이 변화해야 한다. 현재 디지털 포렌식 기술의 활용은 주로 법무법인 등에서 증거로 제출하거나 형사사건의 경우, 경찰 등에서 직접 분석하여 증거로 제출하고 있다.

증거로 활용되기 위해 전문가의 디지털 포렌식 분석 결과에 대한 객관성을 부여하는 것이 중요하다. 하지만 디지털 포렌식 분석을 수행하는 주체, 즉 전문가에 대한 기준이 모호하다. 이런 현황을 개선하기 위해 본 저자들은 디지털 포렌식 전문가 국가공인제도가 필요하다고 주장하는 바이다.

현재 해외에서 발급하는 디지털포렌식 전문가 관련 자격증은 총 9개가 존재하고 있다. EnCE, ACE 등 대부분의 디지털포렌식 자격증은 민간기관인 디지털포렌식 기업 등에서 디지털포렌식 자격증을 발급하고 있다. 따라서 해외에서는 주로 국가공인 자격증이 아닌 민간 포렌식 솔루션 기업에서 발급하는 포렌식 전문자격증만 존재하고 있다. 따라서 검사기관 공인인증제도 및 전문가 국가공인제가 실시된다면 공인받은 전문기관 및 전문가로부터 분석한 디지털 포렌식 결과가 증거로 활용될 가능성이 올라갈 것이다.

결론적으로 디지털 포렌식 활용이 확대되기 위해서는 디지털 포렌식 활용 제도 개편을 통해 기반을 마련해야 한다. 이를 통한 디지털 기기 등을 활용한 불법행위에 대해 객관적인 사실관계, 고의성 입증 등으로 징벌적 손해배상제도 활성화에 기여할 수 있을 것으로 예상된다.

5. 결 론

과거와 달리 현재의 지식재산(IP)은 디지털로

변화되고 보관 및 활용되고 있다. 특히 과학기술이 발전하며 지식재산(IP)을 디지털로 보관하거나, 데이터를 기반한 새로운 지식재산 등을 창출하고 있다. 하지만 온라인을 기반한 지식재산 창출-보호 등의 지식재산 생태계 환경 속에서 새로운 유형의 범죄들 또한 발생하고 있다.

한편 징벌적 손해배상제도는 비재산적 손해의 전보적 기능을 가지고 있으며 특정영역에서의 징벌적 손해배상제도의 도입은 악의적 불법행위에 대한 강한 제재 등의 기능을 수행하고 있다. 해외에서는 해당 제도를 지식재산 침해 범죄에서도 활용하고 있다.

하지만 현재 우리나라에서 징벌적 손해배상제도는 활용되고 있지 못하다. 징벌적 손해배상제도는 사실관계 및 피해액 등을 상정하기 위한 여러 요건 중 고의성・과실은 원고와 피고의 진술만으로 법원이 결정하기에 어려운 부분이 있기 때문이다.

따라서 본 저자들은 징벌적 손해배상제도 활성화를 위한 객관적인 고의성・과실에 대한 법원의 판단을 지원하기 위해 디지털 포렌식을 활용을 주장하고자 한다. 이를 위해 실제 징벌적 손해배상 판결 판례에서 디지털 포렌식이 활용된 사례를 분석했다. 이후 디지털 증거 예시를 기반으로 시나리오 기반의 실제 활용방안 및 디지털 포렌식 활용이 활성화되기 위한 공인인증제도 같은 제도적 개선방안에 대해 제시했다. 본 연구를 기반으로 징벌적 손해배상제도가 바람직한 지식재산권의 활용 및 보호를 위해 잘 적용되는 것에 기여하고자 한다.

본 논문은 다음과 같은 한계점을 가진다. 해당 논문은 징벌적 손해배상 제도에서의 디지털 포렌식 기술 관련 판례 분석 사례가 적고 구체적이지 못했다. 구체적이고 정량적인 판례 분석을 통해 “고의적”에 대한 법원의 판단 기준 해석이 필요하다. 향후 디지털 포렌식 분석 결과는 개개인의 디지털 포렌식 분석관의 역량에 영향을 받는 한계점을 개선하기 위한 기술 활용 관련 가이드라인 구축 연구가 필요할 것으로 사료된다.

본 논문은 교육부 및 한국연구재단의 BK21 4단계(사이버-물리공간 청정화 연구사업단)로 지원된 연구임(5199990314137)

참 고 문 헌

[1] S.J. OH. (2022). [Judicial precedent commentary] Determination of validity in copyright infringement and establishment of general tort Seoul High Court 2012.12.20. Sentencing 2012 Na 17150 Judgment. The Korean Legal News. http://news.koreanbar.or.kr/news/articleView.html?idxno=9415

[2] W.Y. Jung. (2022). [First half of 2020 Ministry of Justice research report] Analysis of precedents on punitive damages in Korea and limitations and improvement measures in application. Seoul : Korea Law School

[3] W.S. WOO. (2013). [legislative debate] A Study on Support for Victims in Crimes of Infringement of Intellectual Property Rights. Ministry of Government Legislation. https://www.moleg.go.kr/mpbleg/mpblegInfo.mo?mid=a10402020000&mpb_leg_pst_seq=133263

[4] Industrial Policy Team. (2012). Investigation of domestic companies' intellectual property leakage damage and policy tasks. Korea Chamber of Commerce and Industry. http://www.korcham.net/nCham/Service/Economy/appl/KcciReportDetail.asp?SEQ_NO_C010=20120925607&CHAM_CD=B001

[5] T.H. KO; H.S. YANG. [Planning] 'Content = Free'... Illegal site sharing is a 'criminal'. (2021). Gyeonggi Newspaper. https://www.kgnews.co.kr/news/article.html?no=681317
[6] J. H. LEE. (2021). 3,500 music creators "OTT copyright infringement, please punish". (2021). NEWSIS. https://newsis.com/view/?id=NISX20211206_0001677503.
[7] G.J. LEE. (2021). 71% of technology leaks were done by insiders... Techniques such as cloud abuse are also evolving. Asia Econom,y. https://www.asiae.co.kr/article/2021111610002962132
[8] J.M. LEE. (2006). A Study on Necessity and Possibility on the Introduction of Punitive Damages. Dong-A University Law Research Institute, DONG-A LAW REVIEW, (38), 187-243. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE01204745
[9] H.S. JUNG. (2004). A Comparative Study on Punitive Damages with the Theory of Punitive Damages in Korean Civil Law. CHUNG_ANG LAW REVIEW, 6(4), 241-254. https://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE06591635
[10] Roddy, N. E. (1981). Punitive Damages in Strict Products Liability Litigation. Wm. & Mary L. Rev., 23, 333. https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=2269&context=wmlr
[11] J.K. LEE; S. G. PARK. (2019). Measures to improve the effectiveness of the punitive damages system. Seoul : Ricon(Korea Construction Policy Institute). ISBN 9791159530654
[12] S.S. WOO; Y.S. CHO; H.J. LIM; S.H. Hong; H.J. LEE; H.J. LEE; J.H. JANG; S.S. AHN.(2021) Industrial Security law. Seoul : Keduai.
[13] Seoul Eastern District Court 1995. 2. 10. Decision 93-19069.
[14] I. H. KWON. (2012). Possibility to Award Punitive Damages on Patent Infringement Cases - at the Time of Introduction of Punitive Damages to Fair Subcontract Transactions Act. Journal of Law Studies. 27, 27-43.
[15] M.J. Kim. (1996). Tort and Intention/Fault Theory. The 'GOSHIGYE' a monthly law journal, 41(8), 14-25.
[16] D.H. YANG. (2015). Triple Damage Compensation System under the Subcontracting Act. Korea Ministry of Government Legislation. https://www.moleg.go.kr/mpbleg/mpblegInfo.mo?mid=a10402020000&mpb_leg_pst_seq=133503.
[17] S.H. Yang. (2019). Discussion on introduction of punitive damages system and review of current status of legislation. KIRI report (focus). 468, 1-7.
[18] J.I. LEE. (2017). A Critical Study on the Punitive Damages under the Korean Legal System, DONG-A LAW REVIEW. (74), 43-86.
[19] J.Y. KIM. (2021). Beware of the spread of punitive damages. Hankookilbo. https://www.hankookilbo.com/News/Read/A2021081711000003675
[20] Legal newspaper opinion. (2021). Legislation for punitive damages should be prudent. Lawtimes. https://www.lawtimes.co.kr/Legal-Opinion/Legal-Opinion-View?serial=172348
[21] S.H. HAN. (2015). Study on the Improvement of Seizure and Seizure of Digital Evidence. Journal of hongik law review. 16(3). 343-370. DOI: 10.16960/jhlr.16.3.201509.343
[22] Supreme Court Decision 2005Da35707 delivered on December 13, 2007.
[23] Korea Copyright Commission. Appraisal, Korea Copyright Commission, https://www.copyright.or.kr/business/appraisal/index.do
[24] K.Y. LEE. (2013). Digital Forensics on the

Handheld Devices. Journal of Software Assessment and Valuation. 9(1), 15-19.
[25] Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of digital evidence, 1(3), 1-12.
[26] S.J. LEE. (2015). Introduction to Digital Forensics (Revised Edition). Gyeonggi : ilun.
[27] B.R. RYU. & M.S. JEON. & O.C. NA.& H.B CHANG. (2017). A Study on Analysis of Digital Forensics Research Trends. Korea Information Processing Society 2017 Spring Conference, 24(1), 306-308.
[28] 21ST CENTURY SYSTEMS INC v. PEROT SYSTEMS GOVERNMENT SERVICES INC, 2012.
[29] Klipsch Group.(2018) Inc. v. ePRO E-Commerce Ltd. 880 F.3d 620 (2d Cir. 2018), 2018.
[30] Tokyo District Court 2013 (wa). 30447 April 27. 2016.
[31] M.Y. Park. (2021). Korean Intellectual Property Office, New promotion of digital forensic support business for companies affected by trade secret leakage. Boannews, https://www.boannews.com/media/view.asp?idx=95911&page=1&kind=2

저 자 소 개

김종성(JongSeong Kim)

2021.2. 중앙대학교 대학원 융합보안학 석사
2021.3-현재: 중앙대학교 대학원 융합보안학과 박사과정
2019.3-2020.11: (사)지식일자리포럼 연구원
2020.11-현재: 한국저작권보호원 주임
<주관심분야> 지식재산권, 디지털포렌식, 산업보안, 융합보안

정세희(SeHee Jung)

2019.2. 중앙대학교 산업보안학과 졸업
2021.2. 중앙대학교 대학원 융합보안학 석사
2021.3-현재: 중앙대학교 대학원 융합보안학과 박사과정
<주관심분야> 산업보안, 인간중심 보안, 보안범죄, NFT

이선경(SunKyung Lee)

2021.3-현재: 중앙대학교 대학원 융합보안학과 석사과정
2019.6-2019.11 소상공인시장진흥공단 주임
2019.11-2022.11: 한국저작권보호원 주임
<주관심분야> 디지털포렌식, 개인정보보호, 산업보안