기획

방송프로그램의 해외저작권 침해 현황 및 대응방안

김성주
법무법인 덕수 변호사

목차

1 들어가며
2 방송프로그램의 해외저작권 침해 관련 온라인 서비스 사업자의 유형분석
3 불법 사이트가 활용 중인 온라인 서비스의 조사 및 분석
4 현행 법, 제도 상황에서의 대응 가능성 및 개선방안

요약

본 원고에서는 방송프로그램의 해외저작권 침해 문제에 대한 해결방안을 모색함에 있어서, '침해자'에 집중되어 있는 침해대응 방안의 시선을 보다 다각화 시켜보고자 했다. 특히 침해자가 불법 침해 과정에서 단계별로 이용하는 각종 서비스가 무엇인지 면밀히 분석하고, 침해자들의 서버 생성, 저작물 불법 복제와 전송, 수익 달성 등의 과정에서 어떻게 사용되는지 파악하여, 이러한 서비스 제공행위가 저작권 침해에 어떤 영향을 미치는지 검토한다. 이를 위해 대규모 불법 유통 사이트 111개를 선별하고, 위 불법 사이트들이 침해 과정에서 주로 이용하는 서비스 업체를 조사하였다. 주요 분석 대상 서비스 업체로는 ① 도메인/레지스트라, ② SSL 발급업체, ③ CDN, ④ 광고 네트워크가 있다. 나아가 위 서비스 업체들에 대한 해외의 선진 대응 사례를 소개하고, 이를 바탕으로 현행 법 · 제도를 이용한 국내외 대응방안을 제안하고자 한다.

1. 들어가며

방송 분야에서 해외저작권 침해에 대한 대응 방안을 모색함에 있어서 핵심은 '침해자'(방송 콘텐츠 관련 불법 사이트의 운영자, 이하 '침해자'로 통일하여 서술함)의 관련 정보를 파악하는 데 집중되어 있었다. 즉 침해자들의 소재지나 서버 운영지를 파악하고, 이들에 대한 수사를 통해 검거하는 것이 대응의 핵심이었다. 불법 사이트를 근절하고 피해를 최소화하기 위해서는 침해자 검거가 필수적이라는 점에서, 침해자들의 정보를 파악하는 것이 여전히 가장 중요한 부분임에는 이견이 없을 것이다.

그러나 방송 콘텐츠 저작권을 대규모로 침해하는 불법 사이트의 운영자들을 검거하는 것은 그 절차와 성과 양면에서 상당한 어려움을 겪을 수밖에 없다. 불법 콘텐츠가 유통되는 과정에 다양한 웹 서버 운용 기술과 보안 서비스들이 결합되어 있기 때문이다. 특히 불법 사이트들은 이른바 'CDN(Content Delivery Network)'으로 대표되는 클라우드 서버 제공 서비스를 이용하여 자신의 본 서버를 CDN 서버 안에 숨겨두고 있다. 설사 CDN으로부터 관련 서버 정보를 얻게되더라도, 워낙 많은 국가에 침해 사이트 서버가 산재해 있다는 문제가 있다. 때문에 침해자의 소재 등이 파악된다고 하더라도 현지 수사당국의 적극적인 협조 없이는 검거가 불가능하다. 침해자들은 수사망이 좁혀오면 검거에 시간이 걸리는 점을 이용하여 서버 자체를 이전하여 CDN 서버 망에 숨긴 채 불법 침해를 계속 이어나간다.

이러한 난점을 고려해 볼 때, 보다 효과적인 불법 침해 대응방안을 모색할 필요가 있다. 필자는 무엇보다도 '침해자'에 집중되어 있는 침해대응 방안의 시선을 보다 다각화 시켜볼 것을 제안한다. 구체적으로는 침해자가 불법 침해 과정에서 단계별로 이용하는 각종 서비스가 무엇인지를 면밀히 분석해보자는 것이다. 온라인 서비스가 침해자들의 서버 생성, 저작물 불법 복제와 전송, 수익 달성 등의 과정에 어떻게 사용되는지 파악하고, 이러한 서비스 제공행위가 저작권 침해에 어떻게 기여하는지를 검토해보는 것이다.

이를 통해 비록 침해자가 특정되지 않더라도, 그들이 이용하는 각종 서비스를 제한함으로써 실질적으로 불법 침해를 차단하는 효과를 기대할 수 있다. 본 연구는 이러한 가능성에 주목하면서 권리자들이 보다 효과적인 침해 대응을 할 수 있도록 정보를 제공하고 침해 대응방안을 제시하고자 한다.

관련하여 필자가 소속되어 있는 '법무법인 덕수'는 2024년 12월, 저작권해외진흥협회(Copyright Overseas promotion Association, 이하 'COA')의 의뢰를 받아 <2024 해외저작권 특정침해 실태조사> 연구 용역을 수행하였다. 이 과정에서 'COA'로부터 국내 권리자들의 방송 영상 저작물들을 대규모로 불법 유통하는 사이트 111개에 대한 정보를 제공받았고, 이들 불법 사이트들이 침해 과정에서 주로 이용하는 서비스 업체를 조사하였다. 주요 분석 대상 서비스 업체로는 ① 도메인/레지스트라, ② SSL 발급업체, ③ CDN, ④ 광고 네트워크가 있다. 본 원고는 위 연구 용역의 결과보고서에 담겨 있는 조사결과 및 핵심 분석 내용 등을 발췌·인용하고 있음을 밝힌다.

2. 방송프로그램의 해외저작권 침해 관련 온라인 서비스 사업자의 유형분석

1) 불법사이트 구축 과정에서 확인되는 온라인 서비스 사업자의 유형

(1) ISP(Internet Service Provider, 인터넷 접속 서비스 업체)

침해자들은 저작물을 복제·전송하는 과정에서 불법 사이트를 구축한 후 침해 저작물을 게재한다. 이 과정에서 모든 침해자들은 인터넷 접속 서비스(Internet Service Provider, 이하 'ISP')를 이용하게 된다.

ISP 사업자는 인터넷 접속 수단을 제공하는 서비스 업체들을 일컫는데, 이들은 웹사이트 구축과 웹호스팅 서비스 등을 제공한다. 또한 '웹호스팅'(Web Hosting) 서비스는 웹사이트에 업로드 되는 이미지, 동영상, 텍스트 등을 저장하는 서버를 제공하는 서비스이다. 침해자들은 이렇듯 ISP 사업자들을 통해 웹사이트와 웹호스팅을 구축하고, 불법 사이트의 외관과 운영구조를 만든다.

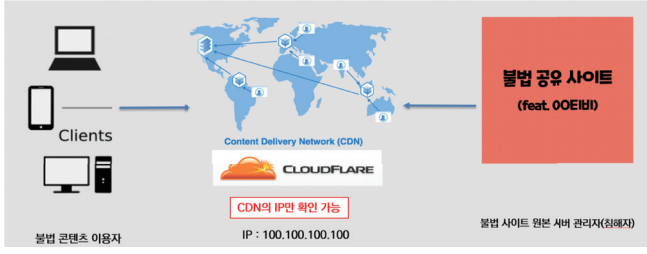
(2) CDN(Content Delivery Network)

많은 ISP 업체들이 'CDN(Content Delivery Network, 이하 CDN)'서비스를 이용하고 있다. CDN 서비스는 본래 인터넷을 통해 전송되는 파일이 트래픽 증가로 속도가 느

려지거나, 디도스 공격 등으로 인해 이용에 불편을 겪는 상황을 방지하기 위해 만들어진 서비스다(홍범석 외, 2008).

그런데 이러한 CDN 서비스는 불법 사이트의 운영자 서버 정보와 신원 등을 숨기는 데 결정적인 역할을 하고 있다. 즉 CDN 서비스를 이용하면 본래 IP를 드러내지 않기 때문에, 실제 IP를 추적해도 CDN 서비스 제공자의 IP만 공개된다. 아래 그림에서 보는 바와 같이, 영상 불법 해외 사이트의 IP를 추적하면 해당 서버의 본래 IP가 아닌 해당 운영자 또는 ISP가 이용하는 CDN 서비스 업체의 IP가 확인된다.

[그림 1] CDN 서비스를 통한 저작권 침해 구조



[그림 2] 불법사이트 IP 추적 시 확인되는 CDN 업체의 IP 정보

(3) 도메인 관련: 도메인 레지스트라, 레지스트리, SSL 인증 발급업체 등

웹사이트를 구축하려면 도메인(Domain)을 구입해야 한다. 도메인은 IP를 대신하여 이용자들이 쉽게 기억하고 이용할 수 있도록 만든 인터넷 주소를 의미한다.

또한 도메인은 인터넷 상에 '등록'(Registration)이 필요하다. 이때 도메인 이름 등록을 대행하는 업체를 '도메인 레지스트라(Registrar)'라고 일컫는다. 이들 업체는 고객으로부터 도메인 이름등록 신청을 접수받은 후, 도메인 레지스트리(도메인 명칭의 데이터베이스를 유지 및 관리하는 업체)의 데이터베이스에 이를 등록한다.

이 과정에서 도메인은 보안 인증을 받아야 하는데, 이를 따로 관리하고 인증을 대행해주는 업체들이 있다. 이들을 도메인 SSL(Secure Sockets Layer, 이하 'SSL')이라고 한다.

2) 불법사이트의 수익 창출 과정에서 확인되는 온라인 서비스 사업자의 유형

(1) 광고 네트워크(애드네트워크)

침해자들은 방송 영상 유료 콘텐츠들을 불법적으로 복제하고 이를 불법사이트를 통해 이용자들에게 무료로 제공하면서, 그 대가로 불법 도박 사이트와 성인 사이트 등으로부터 광고료를 받아서 수익을 올리고 있다.

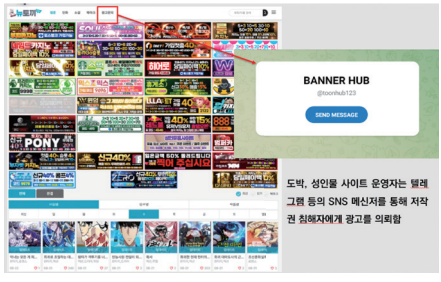
이때 불법 사이트에서는 광고 네트워크 업체(이하, '애드네트워크')와 광고 중개 계약을 체결하고, 위 업체들은 광고주와 불법사이트를 연결해주는(Networking) 역할을 한다.

(2) 광고 직계약을 연결해주는 SNS 업체

또한 침해자들은 도박, 성인물 사이트의 광고주와 직접 계약을 체결하기도 한다. 이 경우, 광고주는 텔레그램 등의 SNS 메신저를 이용하여 침해자에게 광고를 의뢰한다.

[그림 3] 불법 사이트 도박 광고 링크 예시

[그림 4] 불법사이트 광고 문의를 위한 SNS 배너



3. 불법 사이트가 활용 중인 온라인 서비스의 조사 및 분석[1]

1) 조사 및 분석 대상 서비스의 분류

앞서 밝혔다시피, 필자는 COA의 의뢰에 따라 방송 저작권을 침해하는 주요 불법 사이트 111개를 선별한 후, 이들이 활용 중인 온라인 서비스 유형을 조사하였다. 불법사이트 침해자들이 침해 단계 별로 이용하는 주요 서비스 업체는 크게 ① 도메인 레지스트라, ② SSL 발급업체, ③ CDN, ④ 광고 네트워크로 구분할 수 있다.

2) 조사 결과

조사 결과, 도메인 레지스트라의 경우 전체 111개 불법 침해 사이트 중에서 Namecheap을 이용하는 사이트가 27개, Godaddy.com을 이용하는 사이트가 15개, Namesilo를 이용하는 사이트가 6개, TUCOWS를 이용하는 사이트가 5개, Sarek Oy를 이용하는 사이트가 4개, Name.com을 이용하는 사이트가 3개, 그리고 응답을 거절한 사이트가 21개로 조사되었다.

SSL 인증 발급 업체의 경우, 전체 111개 불법 침해 사이트 중에서 Google Trust Service를 이용하는 사이트가 99개, Cloudflare를 이용하는 사이트가 3개, Let's Encrypt를 이용하는 사이트가 3개, Amazon을 이용하는 사이트가 1개, Sectigo Limited를 이용하는 사이트가 1개, 그리고 인증서가 없는 경우가 11개로 조사되었다.

CDN 업체의 경우, 전체 111개 불법 침해 사이트 중에서 Cloudflare를 이용하는 사이트가 105개, Firstcolo GmbH 1개, Akamai Technologies 1개, Cloud Builders 1개, IWS NETWORKS 1개, 사이트 폐쇄로 인한 응답 거절이 2개로 조사되었다.

그리고 광고 네트워크 업체의 경우, 전체 111개 불법 침해 사이트 중에서 Viglink를 이용하는 사이트가 17개, Bidgear를 이용하는 사이트가 9개, Ajax 9개, Yandex 5개, 기타 48개, 그리고 응답 거절 23개로 각 조사되었다.

---

1) 이하 원고는 저작권해외진흥협회, 〈2024년 해외저작권 특정침해 실태조사〉(2024. 12.), 8쪽 이하 부분을 인용하였음.

[표 1] 도메인 서비스업체 이용 현황

회사명	사이트 수
NAMECHEAP INC	27
GoDaddy.com, LLC	15
NameSilo, LLC	6
TUCOWS, INC.	5
Sarek Oy	4
Name.com, Inc.	3
응답거절	21

[표 2] SSL 인증 발급업체 이용 현황

회사명	사이트 수
Google Trust Service	99
Cloudflare Inc.	3
Let's Encrypt	3
Amazon	1
Sectigo Litmited	1
인증서 없음	11

[표 3] CDN 업체 이용 현황

회사명	사이트 수
Cloudflare, Inc.	105
Firstcolo GmbH	1
Akamai Technologies	1
Cloud Builders	1
IWS NETWORKS	1
정보없음(사이트 폐쇄)	2

[표 4] 광고 네트워크 업체 이용 현황

회사명	사이트 수
Viglink	17
Bidgear	9
ajax	9
yandex	5
기타	48
응답 거절	23

3) 주요 서비스업자들의 이용 약관 분석

위 조사 결과를 보면, 불법 사이트를 운영하는 침해자들이 주로 어떤 서비스를 이용하고 있는지 확인할 수 있다. 이러한 결과가 유의미하려면, 위 서비스 업체들이 침해자들과 어떤 방식으로 계약 관계를 맺고 있는지 살펴보아야 한다. 특히 위 업체들이 제공하는 서비스가 불법적인 방식으로 이용되고 있을 경우, 해당 업체들이 어떤 조치를 취할 수 있는지(또는 취해야 하는지)를 분석할 필요가 있다.

(1) 도메인 업체들의 침해자 정보 제공 권한, 도메인의 차단 혹은 폐쇄 권한

주요 도메인 서비스 업체들은 해당 이용약관에 근거하여 도메인 이용자들에 대한 정보 제공이나 도메인의 차단, 폐쇄 등을 요구할 수 있는 권한을 자체적으로 설정해두고 있다.

예컨대 도메인 업체 'NameSilo'의 경우, 고객은 지적재산권을 침해하는 서비스를 제공하지 않는다고 진술하고 보증해야 하며, 이를 위배할 경우 NameSilo는 단독 재량으로 개인정보를 공개(Disclose)할 수 있는 권한을 가진다. 이는 문리 해석 상, 법원의 명령 등 법적 절차 없이 개인정보 제공을 요청할 수 있는 여지를 제공한다(이용자 정보제공).[2]

또한 도메인 업체 'Godaddy'의 경우, 사이트에 지적재산권을 침해하지 않을 계약상 의무를 부과하고, 계약상 의무를 이행하지 않는 경우 당사의 재량(may)에 따라 사용 중지 혹은 사이트 폐쇄 조치가 가능하다.[3]

(2) SSL 업체의 인증 취소 권한

주요 SSL 업체들은 자신의 이용약관에서 불법 사이트에 자신들의 서비스가 이용될 경우 SSL 인증을 취소할 수 있도록 하고 있다. 위 조사 대상 111개의 사이트 중 99개 업체가 SSL 서비스를 이용하고 있는 구글의 경우, 해당 인증서가 범죄나 악의적인 활동에 사용되고 있음을 발견할 경우 인증서를 취소할 수 있도록 하고 있다.[4]

---

2) "4.c.viii. We reserve the right in our sole judgment to suspend, terminate and/or disclose your personal information in the event that any of the following occur: (d) If we believe you have not completely abided by your representations and warranties listed in this Agreement. 3.b.ii. You represent and warrant that the statements in your application are true and that no Services are being procured for any unlawful purpose, including but not limited to the infringement of any intellectual property right, the unauthorized transfer to yourself or any other party of any domain name or Services, or the violation of any laws, rules, or regulations (the"Illegal Uses")."

3) "5.iii. You will not use this Site or the Services in a manner (as determined by GoDaddy in its sole and absolute discretion) that infringes on the intellectual property rights of another User or any other person or entity; (생략) 10. GoDaddy may remove any item of User Content (whether posted to a website hosted by GoDaddy or posted to this Site) and/or suspend or terminate a User's access to this Site or the Services found at this Site for posting or publishing any material in violation of this Agreement, or for otherwise violating this Agreement (as determined by GoDaddy in its sole and absolute discretion), at any time and without prior notice."

4) "5. Revocation. Google will revoke Subscriber's Certificate for the reasons and within the applicable timeframes stated in the section of the CPS referring to reasons for Revoking a Subscriber Certificate. Google may revoke Subscriber's Certificate immediately if Subscriber violates the terms of this Agreement or Google discovers that the Certificate is being used to enable criminal or other malicious activities, such as phishing attacks, fraud, or the distribution of malware. Google may also revoke Subscriber's Certificate within a commercially reasonable period under the following circumstances: (a) Subscriber requests revocation of the Certificate; (b) Subscriber is added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of Google's jurisdiction of operation; (c) Google determines that use of the Certificate may compromise the security, reputation or trust status of the Google PKI or Google; (d) Google reissues a Certificate (in which case, Google may revoke the previously issued Certificate); (e) a licensing agreement affecting the Certificate terminates or expires; or (f) Google determines that use of the Certificate is otherwise harmful to the business or reputation of Google or third parties, considering, among other things: (i) the nature and number of complaints received; (ii) the identity of the complainant; (iii) relevant legislation in force; and, (iv) Subscriber's response to the alleged harmful use."

(3) CDN 업체의 콘텐츠 삭제 권한

조사 대상 111개의 사이트 중 105개의 업체가 CDN 서비스로 이용하고 있는 'Cloudflare'의 경우, 미국 법원의 서피나(subpoena, 소환장) 또는 명령, 기타 법적 절차를 통해 정보를 제공하고 있다. 뿐만 아니라, 'Cloudflare'는 자체적으로 불법 활동, 이용약관 위반 행위 등을 조사, 방지, 조치가 필요하다고 인정하는 경우에도 정보를 제공할 수 있도록 하고 있다.[5]

4) 주요 서비스 업체들에 대한 선진 대응 사례 분석

한편, 해외에서 방송 지적재산권 보호를 위하여 행하여진 조치들을 분석함으로써 국내에도 적용 가능한 제도나 조치방안들을 살펴볼 수 있을 것이다. 아래 몇 가지 주요 대응 사례를 소개한다.

(1) ISP에 대한 조치

가. Warner Bros, Records Inc. v. Doe (2007) - 미국

미국 유타주 연방지방법원은 Warner Bros.가 BitTorrent를 통한 저작권 침해 혐의자의 신원 확인을 위해 ISP에게 가입자 정보 공개를 요청한 사안에서, ISP가 해당 정보를 제공해야 한다고 판단했다. 특히 법원은 저작권 침해의 개연성이 충분히 입증된 경우, 익명의 인터넷 이용자의 신원 정보를 얻기 위한 조기 증거 수집 절차(Immediate Discovery)를 허용했다. 다만 법원은 ISP가 가입자들에게 정보 공개 사실을 미리 통지하고, 이의를 제기할 수 있는 기회를 제공해야 한다는 조건을 부과했다.

---

5) "Cloudflare Privacy Policy""[5. INFORMATION SHARING] In addition to sharing with Service Providers as described above, we also may share your information with others in the following circumstances: When we are required to disclose personal information to respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims. Where we have a good–faith belief sharing is necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or violations of our Website Terms of Use, Self–Serve Subscription Agreement, and/or Enterprise Subscription Terms of Service; or as otherwise required to comply with our legal obligations;"

나. SNE(전국 출판 조합)의 Z-Library에 대한 액세스 차단 명령 신청(2022)[6,7] - 프랑스

전국 출판 조합(SNE : Le Syndicat National de l'Edition)은 파리 법원에 전자책 불법 유통 웹사이트인 Z-Library의 프랑스의 5개 인터넷 접속 서비스 제공자에 대한 액세스 차단명령을 신청하였다. SNE는 프랑스 지식재산권법 L.336-2.[8]에 따라 '동적 가처분 명령'을 청구하여 209개의 도메인과 신속 사법 절차를 통해 식별될 모든 미러 웹사이트까지도 차단할 것을 구하였고, 이에 파리 법원은 위 제공자들에 대하여 '동적 금지 명령(Dynamic Injunction)'을 내렸다.

다. 라리가 등의 신청에 기한 ISP에 대한 불법 IPTV 사이트 차단 명령(2021)[9,10] - 스페인

스페인 축구 리그 라리가와 IPTV 플랫폼 Movistar+는 Telefonica와 협력하여 41개의 해적 IPTV 및 ISP에 대하여 차단 조치를 요청하였다. 이 사건 이전에도 라리가 경기를 중계하는 Telefónica Audiovisual Digital은 44개의 침해자 사이트에 대하여 플랫폼 차단을 요구하였고, 바르셀로나 법원은 동적 금지명령(Dynamic Injunction)을 승인하였던 바 있다. 바르셀로나 법원은 이번에도 유사하게 동적 금지명령을 내렸다.

동적 금지명령(Dynamic Injunction)이란 침해자가 계속해서 도메인이나 IP 주소 등을 이동해가며 침해 사이트를 제작하는 경우에 대응하기 위한 방안으로서, 법원이 도메인 차단 등의 조치를 명할 때에, 최초 신청 범위에 들어가지 않는 경우라고 하더라도 차단 대상인 도메인이나 URL 등이 유사하거나 거의 동일한 사이트에 대하여서도 별도로 법원이 명령을 내리는 일 없이 이동한 도메인 등을 차단할 수 있게끔 권한을 부여하는 것이다.

---

6) https://www.euipo.europa.eu/en/law/recent-case-law/a-dynamic-blocking-injunction-targeting-z-library-website-in-france-proportionality-and-balancing-of-rights

7) https://www.kcopa.or.kr/lay1/bbs/S1T11C330/A/54/view.do?article_seq=3934&cpage=1&rows=10&condition=A.TITLE&keyword=z-library

8) 온라인 대중 커뮤니케이션 서비스의 내용으로 인한 저작권 또는 이웃 권리의 침해가 발생한 경우, 법원장은 실질적인 신속한 절차에 따라 저작물 및 보호 대상에 대한 권리 소유자의 요청에 따라 권리 소유자의 권리를 명령할 수 있다. 제3권 제2호에 의거하여 관리되는 집단 관리 기관 또는 L. 331-1조에 언급된 전문 방어 기관은 저작권 또는 인접한 권리의 침해를 예방하거나 중단하는 데 도움이 될 수 있는 모든 조치를 취한다. 신청은 국립영화영상센터를 통해서도 할 수 있다.

9) https://torrentfreak.com/laliga-wins-dynamic-injunction-to-block-40-pirate-iptv-platforms-211230/

10) https://www.kcopa.or.kr/lay1/bbs/S1T11C330/A/54/view.do?article_seq=3933&cpage=1&rows=10&condition=A.TITLE&keyword=%EB%9D%BC%EB%A6%AC%EA%B0%80

(2) CDN에 대한 조치

가. ALS Scan, Inc. v. Cloudflare, Inc., et al. (2018) - 미국

미국 캘리포니아 중부지방법원은 ALS Scan, Inc.가 Cloudflare, Inc.와 기타 피고들을 상대로 제기한 저작권 침해 소송에서 Cloudflare의 서비스가 캐시 서버에 이미지 복사본을 생성하고 사용자에게 제공하는 과정을 통해 직접적인 침해를 지원할 가능성이 있다는 점에서 ALS Scan의 주장이 충분히 입증되었다고 판단했다. 특히 Cloudflare의 콘텐츠 전송 네트워크(CDN)는 고객 사이트가 저작권 침해 이미지를 더 빠르고 효율적으로 배포할 수 있게 함으로써 실질적인 기여를 했을 수 있다는 점을 지적했다.

그러나 법원은 ALS Scan이 Cloudflare의 고객 사이트에서 발생한 특정 저작권 침해 사례에 대한 명백한 증거를 완전히 입증하지 못했다고 보아, 기여적 저작권 침해 책임 여부를 배심원이 판단해야 한다고 결정했다. 다만, Cloudflare의 CDN 네트워크가 실질적으로 기여했음을 법리적으로 인정했다.

나. Universal Music Publishing GmbH v. Cloudflare, Inc. (2019) - 독일

독일 쾰른 고등법원은 Universal Music Publishing GmbH가 Cloudflare, Inc.를 상대로 제기한 저작권 침해 소송에서 일부 원고의 주장을 받아들였다. 원고는 Cloudflare가 제공하는 콘텐츠 배포 네트워크(CDN)와 DNS 리졸버 서비스가 불법 다운로드를 가능하게 해 저작권을 침해했다고 주장했는데, 법원은 CDN 서비스가 불법 링크를 통한 저작권 침해에 중요한 역할을 했다고 판단했다. 따라서 법원은 CDN 관련 금지 명령을 내렸고, DNS 리졸버 서비스는 법적 책임이 없다고 보아 이 부분은 기각했다.

다. 주식회사 슈에이샤(集英社), 카도카와(KADOKAWA), 고단샤(講談社),
쇼가쿠칸(小学館) vs Cloudflare (2018) - 일본

일본의 주요 출판사인 슈에이샤(集英社), 카도카와(KADOKAWA), 고단샤(講談社), 쇼가쿠칸(小学館)은 2019년 미국의 콘텐츠 전송 네트워크(CDN) 서비스 제공업체인 Cloudflare를 상대로 도쿄 지방법원에 소송을 제기했다.

일본 도쿄 지방법원은 Cloudflare가 해적판 사이트에 대한 캐시 서비스를 제공함으로써, 불법 복제된 만화 콘텐츠의 전송과 접근을 용이하게 했다는 점에서 저작권 침해 방조

책임이 있다고 판단했다. 또한 Cloudflare에 특정 사이트에 대한 캐시 삭제와 서비스 제공 중지를 명령했다.

(3) 도메인 서비스업체에 대한 조치

가. Stichting Brein v Ziggo (2017) - 유럽 연합

유럽연합사법재판소(CJEU)는 Stichting Brein 대 Ziggo 사건에서 불법 파일 공유 사이트인 The Pirate Bay에 대한 법적 조치를 다루면서, 사이트 운영자와 도메인 등록기관에 대한 책임을 논의했다. 이 사건에서 저작권자는 The Pirate Bay의 불법 콘텐츠 배포에 대해 도메인 등록기관에 서비스 중단 요청과 사이트 차단을 요구하였으며, 법원은 도메인 등록기관과 호스팅 업체가 저작권 침해를 알고 있음에도 불구하고 이를 방치하면 법적 책임을 질 수 있다고 판단했다.

나. Sony Music Entertainment v. Quad9 (2023) - 독일

독일 함부르크 지방법원은 DNS 리졸버 서비스 Quad9에 대해 Sony Music의 저작권을 침해하는 웹사이트 접속을 차단하라는 명령을 내렸다. 이 명령은 DNS 리졸버가 도메인 이름을 IP 주소로 변환하지 않음으로써 해당 웹사이트에 접근하지 못하게 하는 내용이다. 이 판결은 독일에서 선례가 될 만한 사례로, DNS 서비스 제공자에게 처음으로 저작권 침해에 대한 적극적 차단 의무를 부과했다는 점에서 의미가 있다.

(4) 직접침해자·ISP·도메인 등록자·금융기관에 대한 조치

가. UNITED KING FILM DISTRIBUTION LTD et al. v. Does 1-10 (2022) - 미국

미국 뉴욕 남부지방법원에서 United King Film Distribution Ltd 등 이스라엘의 영화, 텔레비전, 스포츠 및 뉴스 저작물 제작자가 3개의 침해 사이트를 운영하는 피고의 운영 사이트에 대해 법원의 차단 명령을 요청했다.

법원은 피고들이 원고들의 저작권을 직접적으로, 대리적으로 그리고 기여적으로 침해했으며, DMCA의 기술적 보호 조치를 무력화한 반(反)우회 조항을 위반했다고 판단했다. 이에 따라 법원은 피고들 및 관련 서비스 제공업체(ISP, 도메인 등록기관 등)에게 Sdarot.tv와 관련된 모든 활동을 영구적으로 중단하도록 명령하는 영구금지명령을 내렸다. 결과적으로 피고들의 웹사이트에 대한 접근이 차단되었으며, 관련 도메인은 원고들에게 이전되었다.

4. 현행 법, 제도 상황에서의 대응 가능성 및 개선방안

1) 국내에서의 대응방안

(1) 국내 저작권법에 따른 불법복제물등의 삭제명령 및 시정권고 등 조치

「저작권법」 제133조의2 제1항에 따르면, 문화체육관광부장관은 정보통신망을 통하여 저작권이나 그 밖에 이 법에 따라 보호되는 권리를 침해하는 복제물 또는 정보, 기술적 보호조치를 무력하게 하는 프로그램 또는 정보(이하 "불법복제물등"이라 한다)가 전송되는 경우, 저작권보호심의위원회의 심의를 거쳐 불법복제물등의 복제·전송자에 대한 경고(제1호), 불법복제물등의 삭제 또는 전송 중단(제2호) 조치를 명할 수 있다.

또한 「저작권법」 제133조의3 제1항에 따르면, 한국저작권보호원은 온라인서비스제공자의 정보통신망을 조사하여 불법복제물등이 전송된 사실을 발견한 경우에는 심의위원회의 심의를 거쳐 온라인서비스제공자에 대하여 불법복제물등의 복제·전송자에 대한 경고(제1호), 불법복제물등의 삭제 또는 전송 중단(제2호), 반복적으로 불법복제물등을 전송한 복제·전송자의 계정 정지(제3호) 조치에 대한 시정권고를 할 수 있다.

위 저작권법 제133조의2, 제133조의3에 따르면 '온라인서비스제공자'는 불법복제물등에 대하여 저작권보호심의위원회의 심의가 있으면 이에 따라 이를 삭제, 전송 중단 하는 등의 조치를 취하도록 되어 있다. 그리고 저작권법 제2조 제30호에서는 '온라인서비스제공자'를 아래와 같이 정의하고 있다.

「저작권법」 제2조 제30호

"온라인서비스제공자"란 다음 각 목의 어느 하나에 해당하는 자를 말한다.

가. 이용자가 선택한 저작물등을 그 내용의 수정 없이 이용자가 지정한 지점 사이에서 정보통신망(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항 제1호의 정보통신망을 말한다. 이하 같다)을 통하여 전달하기 위하여 송신하거나 경로를 지정하거나 연결을 제공하는 자

나. 이용자들이 정보통신망에 접속하거나 정보통신망을 통하여 저작물등을 복제 · 전송할 수 있도록 서비스를 제공하거나 그를 위한 설비를 제공 또는 운영하는 자

CDN(Content Delivery Network)은 저작물 등의 원본 내용을 복제하여 네트워크 상에 복수설치하고 접근을 분산시킴으로써 이용자들이 콘텐츠에 더 효율적으로 접근할 수 있도록 도와주는 서비스다. 침해자들은 이러한 CDN 서비스를 이용하여 저작물 등이 이용자들에게 복제, 전송되도록 한다. CDN 업체들은 이를 가능하게 하는 서비스를 제공하고, 분산서버 등을 통해 설비 또한 제공하는 역할을 한다. 따라서 적어도 국내에 법인을 설립하고 운영 중인 CDN 업체들은 저작권법 상의 '온라인서비스제공자'에 해당된다고 볼 여지가 상당하다.

그렇다면 문화체육관광부장관은 저작권법 제122조의6에 따라 구성되는 저작권보호심의위원회에서 CDN 서비스를 이용하여 국내에서 접속 가능한 불법 사이트들에 대한 불법복제물등의 삭제, 전송중단 등의 조치 의결을 할 경우, CDN 업체들에게 해당 조치를 이행할 것을 명령할 수 있다(저작권법 제133조의2 제1항). 저작권보호원 역시 저작권보호심의위원회의 의결이 있을 경우 위 CDN 업체들을 상대로 불법복제물등의 삭제, 전송중단 등의 시정 조치를 권고할 수 있다고 판단된다.

이러한 저작권법에 따른 절차를 통해 '온라인서비스제공자'에 해당하는 CDN 업체들이 직접 불법사이트에 대한 삭제, 전송중단 등의 조치를 이행할 수 있도록 강제하고, 만일 이러한 조치에도 불구하고 CDN 업체들이 이를 이행하지 않는다면, 저작권법 위반에 따른 법적 책임을 묻는 방안 또한 강구할 수 있을 것으로 보인다.

(2) CDN을 상대로 국내에서 저작권 침해의 방조책임을 묻는 방안

앞서 검토한 해외 사례에서 확인되었듯이, 최근 미국, 독일, 일본 등지에서 CDN 사업자를 상대로 저작권 침해에 대한 책임을 묻는 소송이 발생하고 있다. 침해자들의 신원을 특정하더라도 이들에 대한 책임을 묻는 과정에 상당한 제약이 따르다보니, CDN이 침해자들의 저작권 침해 행위를 방조하거나, 침해 행위에 기여하고 있다는 취지의 법리를 제시하며 CDN에게 법적 책임을 묻기 시작한 것이다.

만일 CDN이 콘텐츠의 불법 복제 및 전송 과정에 핵심적인 역할을 하는 서비스를 제공하고 있고, 권리자들의 침해 방지 요청 등을 통해 저작권 침해 사실을 알고 있음에도 불구하고 적절한 조치를 하지 아니할 경우, CDN 사업자에게도 저작권 침해의 방조 책임을 추궁해 볼 가능성이 있을 것이다(김우균, 2024).

2) 해외에서의 대응방안

불법 사이트의 운영자 및 운영 서버가 해외에 소재할 가능성이 높은 이상, 국내에서의 사법 절차를 이용하는 데에는 물리적, 시간적 한계가 상당할 수밖에 없다. 이에 권리자들이 해외에서의 법·제도 및 관련 서비스업자들의 이용약관 정책 등에 근거하여 취할 수 있는 조치들을 정리해 볼 필요가 있다. 특히 침해자들이 주로 이용하는 서비스 업체들(도메인 레지스트라, CDN, SSL 인증)이 대부분 미국에 소재하고 있는 만큼, 미국 저작권법 등 관련 법령과 제도에 따른 조치를 중심으로 정리하였다.

우선 조치 유형별로 분류하면, ①콘텐츠의 유통이나 게재를 직접적으로 제한하는 조치(서비스 차단과 게시물 삭제 등)와, ②침해자의 정보 제공을 구하는 조치로 나눌 수 있을 것이다.

콘텐츠 제한 조치의 경우, ISP, 도메인, CDN 등 각 OSP를 상대로 해당 업체의 소재지 관할 법원에 현지 저작권법에 따른 서비스 중단, 차단 등의 금지명령, 침해 물품의 압수 및 파기 등의 처분, 손해배상, 형사 처벌 등의 청구를 진행할 수 있다.

특히 미국의 경우 저작권자 등은 OSP에 DMCA법에 따른 '저작권 침해 주장 통지'를 통해 저작권 침해 사실 등에 대한 소명과 함께 콘텐츠제한 조치를 요청할 수 있으며, 각 OSP는 이러한 요청을 받아들여서 콘텐츠에 대한 이용이나 접근을 제한하게 될 것이다.

이용자 정보 제공 조치의 경우, 업체가 소재하는 미국 관할 법원에 '정보제공명령(Subpoenas)'을 신청하여 침해자에 대한 이용 정보를 제공받을 수 있고, 이외에도 형사사법공조조약에 따른 대한민국 수사기관을 통한 정보 제공 협조 요청 절차를 거치는 방안, 'CLOUD' 행정협정에 따라 자국의 법적 절차를 근거로 직접적으로 각 업체에 정보 제공을 요구하는 방안 등이 있다.

[표 5] 조치 유형별 구체적 대응 방안 및 난이도

조치 유형	상세 조치 유형	난이도	세부사항
국내에서의 대응방안			
콘텐츠 제한 조치	저작권법 제133조의2, 3에 따른 삭제, 전송중단 명령·시정권고	하	권리자들이 문화체육관광부 또는 저작권보호원에 불법복제물등에 대한 제한 조치를 요구하는 민원을 제기 후, 저작권보호심의위원회의 심의·의결을 거쳐 CDN에 대한 불법복제물등의 삭제, 전송중단 등을 조치
	CDN 소재 관할 법원에 대한 소제기	중	위 저작권법 제133조의 2, 3에 따른 조치 미이행 시 국내 법원에 불법복제물등의 삭제, 전송중단을 명하고, 저작권법 위반에 따른 손해배상을 청구하는 소송을 제기하는 방안
	CDN 소재 관할 수사기관에 대한 형사고소	중	국내에 소재한 CDN 등 서비스업체들에 대하여 저작권 침해의 방조책임을 물어 고소하는 방안
해외에서의 대응방안			
콘텐츠 제한 조치 (서비스 차단, 게시물 삭제 등)	OSP 소재 관할 법적 절차	상	ISP, 도메인, CDN 등의 각 OSP를 상대로 해당 업체의 소재지 관할 법원에 현지 저작권법에 따른 서비스 중단, 차단 등의 금지명령, 침해 물품의 압수 및 파기 등의 처분, 손해배상, 형사 처벌 등의 청구(해당 국가의 저작권법 등 관련 법령 근거)
	OSP의 재량 조치 (이용약관 등)	중	미국의 경우 저작권자 등이 OSP에 DMCA법에 따른 '저작권 침해 주장 통지 ' 를 통해 저작권 침해 사실 등에 대한 소명과 함께 콘텐츠제한 조치를 요청하여(각 OSP 사이트별 양식 존재하는 경우 해당 양식에 따라, 별도 양식이 존재하지 않을 경우 요청자의 임의 요청 방식에 따라), 각 OSP에서 소명되었음을 재량 판단하여 제한 조치
이용자 정보제공	업체 소재지 관할 법적 절차	상	침해사이트에 대한 일정 서비스를 제공하는 ISP, 도메인, CDN 등의 각 OSP를 상대로 해당 업체 소재지 관할 법원에 '정보제공명령(Subpoenas)'를 신청하여 침해자에 대한 이용 정보 제공 요청
	형사사법공조조약(MLAT) 이용 절차	중	OSP 소재지 국가가 대한민국과 형사사법공조조약(MLAT)을 체결한 국가인 경우 대한민국 수사기관이 수사공조 요청 등의 방법으로 해당 국가의 법원에 이용자 정보 제공 등을 요청
	OSP의 재량 조치 (미국 Subpoenas에 준하는 절차)	중	OSP 소재지 법원 절차를 통하지 않고도 그 외 국가의 미국 '정보제공명령(Subpoenas)' 절차에 준하는 법적 절차를 근거로 침해사이트 및 OSP에 침해자 정보제공을 요청하고, OSP의 재량 판단에 따라 이용자 정보제공 가능(업체 의무 아님)
	CLOUD법 이용 절차	하	미국의 경우 CLOUD법에 따라 행정협정을 체결한 국가는 자국의 법적 절차를 근거로 직접적으로 각 업체에 정보 제공 요구 가능(업체의 의무). 다만 대한민국은 미국과 행정협정 체결하지 않은 상태

3) 보론 - 동적 금지명령의 도입 검토

현재 침해자들은 침해 사이트에 대한 접속이 차단될 때마다 계속해서 도메인 등을 이동하여 새로운 사이트를 서비스하는 방식으로 저작권 침해행위를 이어가고 있다. 이러한 문제에 대응하기 위한 방안으로서 해외 대응사례에서도 확인되는 '동적 금지 명령(Dynamic Injunction, 모색적 금지 명령 혹은 동적 차단 명령이라고도 함)'의 도입을 검토할 필요성 또한 제기되고 있다.

'동적 금지 명령'은 기본적으로 침해 사이트에 대한 접속 차단을 명령함과 동시에, 해당 사이트와 사실상 동일한 서비스를 제공하는 새로운 도메인, URL, IP 주소에 대해 추가적인 법원의 명령 등 법적 절차를 거치지 않고도 예방적 차원에서 함께 차단이 가능하게끔 허용하는 방식이다. 권리자들의 입장에서는 현재 불법 침해가 이루어지고 있는 사이트 등을 소송 등을 통해 접속 차단한다고 하더라도, 그 시점에서 이미 새로운 도메인을 통해 저작물 침해가 이루어지고 있을 개연성이 상당하기 때문에, 장래의 침해를 예방할 수 있도록 하는 '동적 금지 명령'과 같은 방식이 상당히 유용할 것으로 보인다.

다만, 이러한 조치는 인터넷 서비스 제공자의 권리를 과도하게 제한하지 않는 선에서 침해되고 있는 저작권의 비교형량을 통하거나 비례성을 확보하여 이루어짐이 바람직하다. 향후 '동적 금지 명령'을 가능케 하기 위하여 '동적 금지 명령' 및 역외적용 조항의 신설을 비롯하여 현행 저작권법의 개정이 필요할 것으로 생각되며, 싱가포르, 스페인, 멕시코, 스웨덴, 호주 등 '동적 금지 명령'을 발한 해외 사례를 참고하여 국내 저작권 침해 구제 환경에 적합한 방식을 모색해 볼 필요성이 있다.

참고문헌

김우균 (2024). CDN 사업자의 저작권 침해 책임에 대한 소고. 한국저작권보호원 C STORY.

이규호 (2022). 온라인상 저작권 침해에 대한 대응방안으로서 모색적 금지명령(dynamic injunction)의 도입연구. 한국저작권위원회 계간저작권

저작권해외진흥협회 (2024). 〈2024년 해외저작권 특정침해 실태조사〉.

홍범석 외 (2008). CDN 서비스의 현황 및 이슈. 정보통신정책.