Digital technology and the protection of intellectual property rights on the Internet

Anna Butlen,
Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits sur Internet (HADOPI)

Abstract:
It has been argued that technological advances, by themselves, offer an alternative to the protection by the law of intellectual property and suffice to fight against piracy on the Internet; but this argument soon met its limits. Problems due to the dependance on technology and its domination have sparked lively debates. Cyberpiracy by parties under rival legal systems and the fight against it have aroused strong concerns about the protection of basic freedoms and the social acceptability of the measures to be adopted. Debates on the introduction of digital technology in the legal realm must both set the conditions for authorizing and regulating the uses of these new tools and show how they can better protect fundamental rights.

The question of changes in the legal professions stemming from changes in technology is normally approached from the angles of security or the simplification of procedures. This approach leads to the quest to find the optimal articulation between the work of jurists and of robots. No one, in penal procedures, objects to the advances made by science and technology for solving crimes, or regrets the time when the determination of descent involved a complicated fabrication in the courtroom, the latter now replaced with the simplicity of a DNA test.[1] Given the emergence of digital technology and the spread of cyberpiracy, the playing board has been turned around, and businesses in the culture and entertainment industry are forced to use new tools of protection and content recognition. A simple postulate has been formulated for intellectual property law: the idea developed in the mid-1990s that cyberpiracy results from advances in technology. Therefore, fighting against it implies developing tools for protecting contents and detecting illegal sources. This is summarized by the saying, "*The answer is in the machine*."[2]

We can qualify the many techniques for fighting against cyberpiracy as being either defensive (measures for protecting, blocking, etc.), or cooperative (means for cybernauts to secure their operating systems, payment agreements with platforms, etc.). Despite the many tools available, there is still, nevertheless, a multitude of illegal websites with illegal cultural contents. In France, 45% of the consumers of goods and services on line have admitted to illegal practices on the Internet. For the audiovisual industry, such practices amount to 2.5 billion illegal viewings of films or series on line.[3]

[1] This article, including quotations from French sources, has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.

[2] Charles Clark, representative of international publishing houses, to the World Intellectual Property Organization (WIPO) in 1995. BENHAMOU F. & FARCHY J. (2014) *Droit d'auteur et copyright* (Paris: La Découverte).

[3] EY FRANCE (2017) "Piratage en France. Estimation du manque à gagner lié à la consommation illégale de contenus audiovisuels", February, available at: http://www.ey.com/Publication/vwLUAssets/ey-piratage-de-contenus-audiovisuels/%24FILE/ey-piratage-de-contenus-audiovisuels.pdf.

This paradoxical situation can be set down to several factors. The use of digital technology by legitimate users generates major costs owing to the volume of works of culture and the number of websites. As for public authorities, they are historically wary of intervening lest their interventions overreach and overprotect.

At the center of the debate about the new technology, apart from the question of its efficiency (especially for countering cyberpirates' strategies to circumvent the law) is a question about how much protection is needed whenever most illegal uses are apparently concentrated on a limited part of the contents. The tools indispensable for fighting against massive cyberpiracy are raising questions about the fundamental equilibrium to be found between the law and technology. For more than fifteen years, these tools are at the core of problems related to regulations and regulatory actions at the sectoral and national levels, as the pendulum swings back and forth between recognizing what is at stake in protecting intellectual property and establishing a legal framework for the cultural and entertainment industry.

Protecting intellectual property

Techniques for protecting works of culture

Technical measures control the access to intellectual property or the use of the contents. Some techniques are protective. They preventively stop certain uses by applying a code or procedures (such as encryption, jamming or software for transforming the protected work or object) or by for controlling the copies made. Other technical measures are information-centered (*e.g.*, the tools related to authorizations, consent and the management of rights). Given the rapid development of both these sorts of techniques — grouped under the phrase "digital rights management" (DRM) — in line with a very closed rationale of ownership (given the investments at stake), European and then national lawmakers were soon led to intervene. Technical measures were defined by the EU directive 2001/29/CE of 22 May 2001 and transposed, in France, into the DADVSI Act of 2006 on authors' rights in the information society.[4]

While these tools benefit from legal protection and breaches of the law are sanctioned, the law has also recognized the risks of overly protecting contents. Technical measures are deemed legitimate if they are effective and do not infringe on the exceptions existing under copyright law. Judges or national regulatory authorities are responsible for overseeing this equilibrium. French lawmakers, when transposing the EU directive and setting up a regulatory authority (the forerunner of HADOPI),[5] went farther by including an additional requirement about interoperability to the benefit of service-providers and the makers of software and operating systems.

[4] Article L.331-5 of the Intellectual Property Code (CPI): Loi n°2006-961 du 1er août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information (NOR : MCCX0300082L). Texts of French law are available at: https://www.legifrance.gouv.fr/Droit-francais.
Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society available via: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001L0029&from=EN.

[5] HADOPI: Haute Autorité pour la Diffusion des Oeuvres et la Protection des Droits d'Auteur sur Internet (High Authority for the Distribution and Protection of Intellectual Property on the Internet), the regulatory authority instituted by the so-called HADOPI I Act: Loi n°2009-669 of 12 June 2009 on the diffusion and protection of creations on the Internet.

Techniques in the fight against cyberpiracy

As of 2007, the Olivennes report[6] emphasized that the technical solutions examined by experts were not all practicable for reasons having to do with the law or with acceptance by society. It pointed to two limits: the risks of setting up procedures for a private justice that would infringe on basic freedoms (in particular, the freedom of communications), and the indispensable guarantees needed to protect cybernauts' personal data.

Besides imposing an obligation of security on cybernauts and outlining a graduated response to offences, the aforementioned DADVSI and HADOPI I acts have also:

- provided for penal sanctions for editing, knowingly making available or communicating to the public software that is clearly intended to give unauthorized access to protected intellectual property (Article 335-2-1 of the Intellectual Property Code, CPI).
- introduced the possibility for rightful owners to undertake legal action against Internet access-providers or search engines so as to make them block the access to, or referencing of, illegal websites (Article L.336-2 of the CPI).
- assigned HADOPI, the regulatory authority, the job of evaluating experiments in filtering or content recognition technology and reporting on the major trends observed, in particular on the effectiveness of these forms of technology (Article L. 331-23 du CPI).

Various tools now exist for detecting works of culture on peer-to-peer networks. They scan the websites and services for streaming or downloading illicit copies. Many businesses in this field, including platforms, have developed techniques for recognizing protected contents. Among these techniques are:[7]

- hashing, which matches each file with a unique string of alphanumerical characters, thus permitting the identification of exactly identical files.
- watermarking, which incorporates in the work of culture a sort of invisible code for identifying (by using a tool capable of detecting it) the original and the copies made from it.
- fingerprinting (or automatic content recognition, ACR), which uses a unique digital fingerprint of the contents (that is not incorporated in the work but is mapped to part of its contents) and compares the contents of works on line with a database of references (under agreements for this purpose with the rightful owners).

Experiments are also being conducted with other techniques. For example, searches can be targeted by using the metadata (*e.g.*, a song's title or the singer's name) provided by the user or by using artificial intelligence to recognize contents (such as faces).

The fight against cyberpiracy…

…On peer-to-peer networks

Intellectual property holders in the music business have tried, since the turn of the century, to use digital fingerprint recognition technology to collect the IP addresses of users who share works of music on peer-to-peer networks.

By a decision on 29 July 2004 about an act of law on information technology and freedoms, the French Constitutional Council ruled in favor of the procedures allowing these property holders

[6] OLIVENNES D. (2007) "Le développement et la protection des oeuvres culturelles sur les nouveaux réseaux", 23 November, 43p. Available via http://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/074000726.pdf.

[7] "La protection du droit d'auteur sur les plateformes numériques: les outils existants, les bonnes pratiques et leurs limites", report by Olivier Japiot (chef de mission) to the Conseil Supérieur de la Propriété Littéraire et Artistique (CSPLA), 19 December 2017, 27p.. Available via https://shareslides.org/philosophy-of-money.html?utm_source=la-protection-du-droit-d-auteur-sur-les-plateformes-numeriques-les-outils-existants-les-bonnes-pratiques-et-leurs-limites&utm_campaign=download.

to collect and process personal data related to infringements of copyright law on the Internet.[8] In a decision of 23 May 2007,[9] the Council of State declared that, under condition of satisfying the finalities set in the law (CPCE), the data-processing of "*10,000 titles of pieces of music, of which 10% were updated weekly*" was legitimate given "*on the one hand, the number of titles [millions of titles] that the claimant companies have the assignment of protecting and, on the other hand, the volume of exchanges of music files on the internet*" — hundreds of thousands of exchanges per day compared with the number of IP addresses collected, of which the upper limit was set at 25,000/day. In 2009, this setup was completed to allow the transmission of the reports and IP addresses by the property holders to HADOPI (and no longer simply to judicial authorities).

Every day, HADOPI receives tens of thousands of reports and IP addresses. Using them under the conditions set by the law on protecting personal data, it sends queries to Internet access-providers as part of a "graduated response" during a prepenal procedure. The detection of IP addresses and illicit contents is not done by HADOPI itself but by a private firm commissioned by the organizations representing intellectual property holders (music and cinema) within the aforementioned limit and following the technical procedures for processing this sort of data laid down by the National Commission on Informatics and Liberty (CNIL).

During these proceedings prior to prosecution, there is a harmonious articulation of: detection tools, information systems, the verification work done by certified civil servants, and the expertise of the members of HADOPI's committee for protecting rights.

…With content recognition technology

YouTube, Dailymotion and Facebook have voluntarily adopted automatic content recognition software to verify whether protected contents have been posted on their platforms. These programs automatically compare a new post by a cybernaut with a database of digital fingerprints that is, under agreements with property holders, updated with the information they provide. If a match is found, the property holder has two choices: have the work of music deleted from the website or obtain a payment (a share of the advertising revenue related to the work posted on line). This use of content recognition technology is a stride forward, since intellectual property holders are no longer forced to continually demand platforms to eliminate posted works of music. Furthermore, the obligation to use content recognition technology helps distinguish between the "lawful" platforms and the platforms that, abetting counterfeiting, will be the target of lawsuits by intellectual property holders and public authorities.

However this voluntary, contractual approach, which lies outside any legal framework, has limits. Intellectual property holders have criticized, in particular, the lack of transparency about the actual operations performed by the content recognition software. They also complain that they depend so much on these platforms that they are forced to sign agreements with them.

[8] Conseil Constitutionnel referring to Article 34-1 of the Code des Postes and Communications Électroniques (CPCE) and Article L.331-1 of the Code de Propriété Intellectuel (CPI): Décision 2004-499 DC - 29 juillet 2004 - Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés - Non conformité partielle. Available at https://www.legifrance.gouv.fr/affichJuriConst.do?oldAction=rechJuriConst&idTexte=CONSTEXT000017664802&fastReqId=190382022&fastPos=1.

[9] Conseil d'État décision n°288149 available at: https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000018259508&fastReqId=963831298&fastPos=1.

During the process of modifying the aforementioned Directive 2001/29/CE, debate has arisen at the EU level about the generalized use of content recognition technology by the platforms that diffuse the cultural contents posted by their users, in particular about the platform's obligation of due care for detecting and deleting unlawful contents. For the critics, a first issue is how to articulate this modified directive with the system of limited liability granted to access-providers under the directive on electronic commerce.[10] The latter forbids imposing on access-providers measures for the generalized surveillance and filtering of the contents hosted on their sites. Furthermore, some EU MPs have emphasized the risk of robots making mistakes, and fear lest this technology lead to "overblocking" contents, an action that would require the intervention of a judge or regulatory authority.

These EU debates draw attention, once again, to the complexity of adopting legal measures for the future given that digital technology is evolving and that the modalities for implementing legal measures have to be "appropriate and proportional" to the issues at stake.

[10] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce'). Available via https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32000L0031.