

Intellectual property / New technologies / Media Department

Topic of the month: PRODUCT PLACEMENT:

The French Audiovisual Media Commission publishes its long-awaited recommendation.

Product placement is an advertising method consisting of directly or indirectly promoting products, services or brands in exchange for payment or other consideration by the advertiser.

Neither Community nor national laws specifically dealt with the issue of the presence of brands in audiovisual works of fiction or animation.

Therefore, television service providers needed to ensure that works programmed did not give excessive visual or verbal prominence to any good, service or brand. Otherwise, the placement of products could be considered surreptitious advertising, which is liable to sanctions.

The European directive of 11 December 2007, the "Audiovisual Media Services" (AMS) directive, which was transposed into French law by the Act of 5 March 2009, seeks to modernise the legal framework governing audiovisual contents.

This new legislative scheme authorises *inter alia* legislation concerning product placement in linear or on-demand audiovisual media services.

The AMS directive states the principle that this type of advertising is prohibited in all audiovisual media services. However, this general prohibition is moderated because, by derogation, Member States may authorise product placement in certain exhaustively listed cases. The French parliament opted to use this right and assigned to the French Audiovisual Commission (*Conseil Supérieur de l'Audiovisuel* or "CSA") the task of establishing the procedures applicable to this new advertising technique.

One year after the law transposing the directive into French law was published, the CSA's Recommendation with respect to product placement, for consideration, in television programmes was at last published on 5 March 2010.

Accordingly, products and services may be placed in audiovisual programmes for which production begins after March 6th 2010, provided a certain number of conditions are met.

■ **Products may be placed in certain types of programmes only**

The CSA has adopted a restrictive interpretation of the scope of possible uses of product placement.

This new source of financing is not available to all types of programmes. Only cinematographic works, audiovisual works of fictions and music videos, except if intended for children, will be allowed to show products, services or brands.

Any other use, for example, in talk shows, entertainment programmes, reality shows, news magazines or sports programmes, is therefore forbidden.

■ **Exclusion of certain types of products**

For ethical reasons, certain types of products cannot be placed in programmes. These include beverages with an alcohol content exceeding 1.2 percent, tobacco products, drugs, whether or not a medical prescription is required, firearms and munitions, as well as baby formula.

Also for ethical reasons, broadcasts of gambling and betting will not be able to use product placement. Despite the fact they will be legally entitled to do so by the upcoming Act authorising online gambling and betting, the prohibition on product placement will remain in place until a specific decision establishes the legal framework therefor.

Furthermore, if a programme is sponsored, the sponsor's products or services cannot be placed.

■ **The pictogram**

The CSA has adopted the same policy as for advertising, where there is an obligation to clearly distinguish in the minds of television viewers between advertising and programmes themselves. Accordingly, the placement of a product or service in a broadcast must be clearly indicated by a pictogram.

This pictogram must appear for one minute at the start of the programme, for one minute after each commercial break and during the entire closing credits.

However, in the case of music videos in which products are placed, the pictogram must appear during the entire broadcast.

In order to familiarise television viewers with these new symbols, the obligation to inform the public will be heightened during the first two months after it is introduced. In addition to the pictogram, a banner stating "This programme includes product placements" must be broadcasted for five seconds at the start of the programme.

■ **Safeguards surrounding product placements**

The placement of a product or service must be governed by a contract signed by the broadcaster, the producer of the programme and the television service provider. In general, the parties must ensure that the content and programming of programmes including product placements are not influenced in such a way as to affect the responsibility and editorial independence of the television service provider. The intent is to prohibit cases of fraud. For example, advertising a product should not be the sole purpose of a programme, which could be demonstrated if the product appears onscreen too often.

Furthermore, it is important that product placement be clearly distinct from advertising. Therefore, the product should not be given unjustified prominence given the programme in question nor directly encourage the purchase or rental of the product. The television service provider must refrain from including any promotional references to the products or services.

■ **HADOPI decree on the “system for managing measures to protect works on the internet”**

The HADOPI II Act of 28 October 2009 set up a graduated response system [for copyright infringement over the internet]. To implement this system, new Article L.331-29 of the Intellectual Property Code authorises electronic processing of personal data concerning persons subject to this procedure.

This data processing system should enable the HADOPI (*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* = High Authority for the distribution of works and protection of rights on the internet) to correlate IP addresses collected from copyright holders with identification data provided by internet users to internet service providers (ISPs).

The decree setting forth the procedures for applying this system, which is essential to the Act's operation, was at last published on March 7th and enables to define the types of data that will be available to the HADOPI.

The following data will be collected from copyright holders: date and time of occurrences [of infringement], IP addresses of the internet subscribers concerned, the peer-to-peer software protocol used, the pseudonym used, information concerning protected works or items affected by the occurrences [of infringement], the file name as it appears on the internet subscriber's computer, the complete identity of the sworn agent who collected the information and the ISPs with which subscriptions for internet service are held.

When this data has been recorded, ISPs will be required to provide the High Authority with the following information to identify the internet subscriber: last name, first name, telephone number, postal address and e-mail addresses.

A third type of data will also be processed electronically: any previous warnings already sent to the internet subscriber.

The data processed will be retained for a maximum period of two (2) months if no warning has been sent to the internet subscriber. This period is extended to fourteen (14) months if a first warning has been sent to the internet user, and to twenty (20) months if a recorded delivery letter has been sent.

For what the guarantees are worth, the decree provides that information concerning consultations of the data processed electronically will be recorded and retained for one year.

Internet users will have a right to access and correct this data (pursuant to the French Data Protection Act of 6 January 1978), but they will no longer be entitled to oppose that such data be retained.

Although the publication of this decree means that the first warning e-mails are imminent, it also confirms that the scope of the HADOPI Acts' anti-piracy efforts will be limited to users of illicit peer-to-peer networks. What about sites that host and stream pirated videos? Also, what about their financing? To be continued...

■ **IP addresses are not personal data**

A decision rendered on 1 February 2010 by the Paris Court of Appeal confirms a principle laid down by the French Supreme Court (*Cour de Cassation*) in a previous case (Supreme Court, criminal chamber, 13 January 2009): although an IP address may allow proving that an offence has occurred, it is insufficient to identify the perpetrator of the offence.

In that case, a sworn agent of SACEM (a royalties collection society) had observed that internet users, using peer-to-peer software, had made available to the public a certain number of musical works that were part of its catalogue. The agent collected several pieces of information, such as the number of works made available, the ISP, the country of origin, as well as the IP address. Based on this information, SACEM filed suit and the ISP was served with an order requiring it to identify the internet subscriber who used that IP address. The perpetrator was found and convicted.

The Court of Appeal reiterated the legality of an affidavit documenting illegal downloading of musical files as observed by sworn agents of SACEM. The procedure for collecting such information does not constitute electronic processing of personal data and, therefore, prior authorisation of the French Data Protection Commission (*Commission Informatique et Libertés* or “CNIL”) is not mandatory.

The Court also held that an IP address, by itself, is insufficient to identify the perpetrator of an offence. In many cases, IP addresses have been diverted, modified by pirates or simply used by persons who are not the owners of the internet connection. To hold otherwise would mean that the person convicted would be the subscriber to an online communication service, rather than the actual perpetrator of the offence.

Therefore, an enquiry must be initiated before a conviction because an IP address is only a lead that may allow successful completion of the enquiry, but is not proof of the identity of the perpetrator. The facts of this case confirmed this conclusion because the holder of the IP address was not in fact the perpetrator of the acts at issue.

■ **The offence of use of a third party's identity**

On 16 February 2010, the National Assembly adopted at first reading the proposed Basic Internal Security Act (*Loi d'Orientation et de Programmation pour la Performance de la Sécurité Intérieure*, known as LOPPSI 2), which creates the offence of identity usurpation, punishable by one year's imprisonment and a fine of €15,000.

Identity usurpation on the internet has become increasingly frequent, especially on social networking sites (Facebook, Twitter, etc.) and the usurpers have multiple motivations. This may be done as a hoax, to remain prudently anonymous in a discussion forum, but also to commit an offence (such as defamation or fraud) or to spread a virus. Before the adoption of the proposed Internal Security Act, the law did not provide any definition of, or specific penalty for, the offence of digital identity usurpation.

○ Criminalising the use of a third party's identity

The Act applies to the use of a third party's identity. This term is broader than usurpation, and means that the offence may cover various situations, in particular press offences (e.g., defamation), thereby allowing the period of prescription for acting against such offences to be avoided (three months from the time the content is put online).

○ Two offences created

The Act distinguishes two offences: the act of using, on an electronic communications network, a third party's identity or data of any type allowing a third party to be identified for the purpose of:

- Disturbing the tranquillity of such person or any other person; or
- Infringing such person's honour or lowering the esteem in which he is held.

There are therefore now two separate offences that are subject to the same penalties.

○ No definition of digital identity

However, the components of digital identity are not defined; the Act simply states that it applies to data “of any type allowing [a third party] to be identified”. However, digital identity is quite different from identity in the physical world and is based on e-mail addresses, pseudonyms, passwords, IP addresses, videos, photographs, etc. It therefore appears necessary that the definition of digital identity be more precise.

In this regard, a reading of the parliamentary debates shows just how difficult it is to define the limits of digital identity. Nevertheless, the position adopted by Parliament, i.e., creating a potentially broad offence, seems the most appropriate solution for this environment. It will therefore be up to the courts to define the limits of what constitutes truly fraudulent uses of a third party's identity based on possibly exaggerated claims made by claimants whose name or image has been used on the internet. To be continued...

P.D.G.B. Law Firm
174 Avenue Victor Hugo
75116 Paris
Tel.: 00 (33) 01.44.05.21.21
www.pdgb.com
Julie Jacob - Benjamin Jacob
Sandy Herve – Elodie Perier