CONSEIL D'ÉTAT

Paris, 30 April 2026

PRESS RELEASE

[Legal decision]

Protecting copyright from piracy: personal data processing must be reviewed

After consulting the Court of Justice of the European Union, the Conseil d'État today ruled that the 'graduated response' mechanism used to combat online piracy of protected works does not comply with European law as it does not require internet service providers to retain the data used by Arcom in a segregated manner and permits Arcom to carry out more than two instances of data cross-referencing without prior authorisation from a judge, even though such cross-referencing may infringe privacy rights. It ordered the Government to bring the mechanism into compliance.

The French Intellectual Property Code requires all internet users to ensure that their connection is not used for the purpose of pirating protected works.

To ensure compliance with this obligation, Arcom, which succeeded Hadopi on 1 January 2022, implements a mechanism known as the graduated response procedure, comprising three stages: at the first recorded infringement, a warning is issued to the subscriber; at the second, a further warning is issued; and at the third, the case is referred to the public prosecutor.

To identify subscribers, Arcom is authorised (based on reports submitted by professional bodies or public authorities) to request that internet service providers link the IP addresses used to illegally download works to personal identity details. Once this link has been established by the operators, Arcom can then identify the individuals concerned and apply the graduated response. The terms and conditions governing this personal data processing, known as the management system for measures to protect online works, are set out in the Decree of 5 March 2010.

The organisation La Quadrature du Net and three other organisations, which oppose the measure in principle, brought the matter before the Conseil d'État seeking the annulment of the decree and arguing that it contravenes EU law. Before issuing a ruling on the legality of the existing scheme, the Conseil d'État referred the matter to the Court of Justice of the European Union (CJEU) on 5 July 2021, asking it to clarify the correct interpretation of the ePrivacy Directive of 12 July 2002.

Limits determined by the CJEU

On 30 April 2024, the CJEU specified that a Member State may require internet service providers to retain, on a generalised basis, data relating to civil identity and the corresponding IP addresses, including for the purpose of prosecuting minor criminal offences. However, in such cases, the relevant data must be retained in a segregated manner to prevent the risk of serious interference with individuals' privacy through cross-referencing with other retained data.

Furthermore, regardless of the gravity of the offence, if a national public authority is authorised to access the personal data of individuals suspected of having committed criminal offences, it must not be able to draw precise conclusions about the private lives of internet users. For this reason, if the public authority has already linked the identity details of the same subscriber with information regarding the content of

works that they are alleged to have pirated twice, it may not make a third such link without first obtaining authorisation from a court or an independent administrative body.

Personal data processing must be reviewed to ensure compliance with EU law

In consideration of the implications of the CJEU's judgment, and in light of the arguments advanced by the applicant organisations, the Conseil d'État today ruled that the decree of 5 March 2010 setting out rules on data processing does not comply with EU law.

The system does not prevent Arcom from receiving identity data from internet service providers that has not been retained in a segregated manner, as required by European law in relation to tackling minor criminal offences. It also authorises Arcom to link subscriber identification data with information relating to pirated content for a third time concerning the same individual, without this link being subject to authorisation by a court or an independent administrative authority.

It, therefore, ordered the Government to review the decree to bring it into compliance with these requirements

A transitional monitoring framework

Pending the possible adoption of a new decree, the Conseil d'État specified that, in relation to minor criminal offences, Arcom may only request that operators identify a subscriber based on their IP address if it is established that such personal data has been retained in compliance with the conditions laid down by the CJEU.

If serious criminal offences (such as counterfeiting) are reported to it, Arcom may request identification from electronic communications operators without having to verify that the data is retained separately.

Lastly, regardless of the seriousness of the offence, Arcom may continue to cross-reference data on the content of works with internet users' personal details, but only for the purpose of sending them the first two warnings under the graduated response system.

Decision No. 433539, La Quadrature du Net et al., 30 April 2026

For more information on the graduated response procedure and the court's ruling, see page 3

The graduated response procedure for copyright protection

Anyone with internet access is required to ensure that their connection is not used to reproduce, display or make available works protected by copyright or related rights without the authorisation of the holders of those rights (article L. 336-3 of the French Intellectual Property Code). To ensure compliance with this obligation, the law entrusts Arcom (the French regulatory authority for audiovisual and digital communication) with the implementation of a mechanism known as the graduated response procedure, consisting of three successive stages.

Stage 1: Simple recommendation

When Arcom is notified of an alleged infringement - by a professional defence body, a collective management organisation, the Centre national du cinéma et de l'image animée (CNC) or through judicial channels - it requests the data enabling the identification of the subscriber from the relevant electronic communications operator. It then issues an initial warning to the subscriber, reminding them of their legal obligations and warning them of the possible penalties.

Stage 2: Recommendation with acknowledgement of receipt

If the same offences reoccur within six months, Arcom may issue a further recommendation, this time served by registered letter or by any other means that provides proof of receipt.

Stage 3: Referral to the public prosecutor's office

If further infringements are identified within one year of the second recommendation, Arcom informs the subscriber that the matter may be subject to legal proceedings and, where appropriate, refers the case to the relevant public prosecutor's office. Such acts may constitute gross negligence (article R. 335-5 of the French Intellectual Property Code) or counterfeiting (articles L. 335-2 to L. 335-4 of that code).

To carry out their mission, Arcom is authorised to operate automated processing of personal data, the management system for measures for the protection of online works, the terms and conditions of which are set out in a Decree of the Conseil d'État of 5 March 2010 adopted pursuant to article L. 331-23 of the Intellectual Property Code.

CJEU ruling of 30 April 2024

Following an application for a preliminary ruling from the Conseil d'État, the Court of Justice of the European Union specified the conditions under which the graduated response mechanism is compatible with the ePrivacy Directive of 12 July 2002.

Retention of IP addresses

The Court acknowledged that a Member State may require operators to retain their users' IP addresses in a generalised manner to combat minor criminal offences. However, such data retention is only lawful if it is effectively segregated; i.e., it must under no circumstances be combined with traffic or location data that could reveal sensitive aspects of the private lives of the data subjects.

Access to civil identity data

The Court ruled that a public authority responsible for copyright protection may, in principle, access data enabling the identification of a subscriber based on their IP address without systematic prior review. Indeed, the mere knowledge of a subscriber's civil identity does not, in itself, constitute a serious breach of privacy.

Limit after a third instance of cross-referencing

The situation is different when that authority links a subscriber's identity details with information relating to the content of works made available illegally. Such cross-referencing is likely to shed light on sensitive aspects of the individual's private life. The Court concluded that, since such a procedure has already been implemented twice in relation to the same person, it cannot take place a third time without the prior authorisation of a court or an independent administrative body. This check, which cannot be fully automated, must in principle be carried out before any data is accessed, except in duly justified emergencies. It is up to the supervisory body to refuse such access where the available evidence does not provide grounds for suspecting serious criminal offences.