FIDAL
AVOCATS

# Newsletter

PROPRIÉTÉ INTELLECTUELLE /
NUMÉRIQUE, TECH ET DONNÉES



## NEWSLETTER #171
## *September-October 2026*

**INTELLECTUAL PROPERTY**

**DIGITAL, TECH AND DATA**

# CONTENTS


*HEADLINE* ..... 3

*The ambitious "Digital Omnibus" reform on Artificial Intelligence: a review of the key points* ..... 3

*ARTICLES* ..... 7

*Deceptive trademark at filing, deceptive trademark through use: the Cour de cassation's double sanction* ..... 7

*Cybersecurity: the institutions are making progress in supporting operators regulated by the Cyber Resilience Regulation* ..... 8

*Patentability exclusion of a flight-path data display system: a second difficult landing* ..... 9

*Protection of the integrity of a mural: the difficult duty of preservation borne by municipalities* ..... 10

*Algorithmic personalization: placing trackers remains subject to internet users' consent* ..... 11

FIDAL
AVOCATS

# HEADLINE

**The ambitious "Digital Omnibus" reform on Artificial Intelligence: a review of the key points**

*Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as regards the simplification of the implementation of the harmonised rules on artificial intelligence (Digital Omnibus on AI)*

## I. Background to the reform

The "Digital Omnibus on AI" reform, and more generally the "Digital Omnibus" package, results from a new political direction adopted by the European Commission, formalised in its "Commission's political guidelines for 2024-2029", which makes regulatory simplification a genuine objective in support of economic growth and competitiveness in the EU.

Drawing on various works including:

- the Draghi Report "The Future of European Competitiveness" (2024);
- the Letta Report "Much More than a Market" (2024);
- the Commission Communication "A Competitiveness Compass for the EU" (29 January 2025);
- the Commission Communication "A Simpler and Faster Europe" (11 February 2025);

the European institutions agree in particular on the need to carry out a "stress test" of recently drafted digital legislation, having regard notably to the compliance burden borne by regulated operators and, ultimately, to the competitiveness of European businesses.

These works concluded that, without compromising "predictability, strategic objectives and high standards", it was necessary to put forward measures simplifying the digital regulatory framework.

In this context, on 19 November 2025 the European Commission published a "Digital Omnibus" package (or digital omnibus) which also includes a text specific to artificial intelligence. That text, adopted on 8 July 2026 and published in the OJEU of 24 July 2026, amends Regulation No. 2024/1689 on artificial intelligence.

## II. The points addressed by the reform

### Additional time for compliance

In view of the delay by the European institutions in adopting standards, guidelines or recommendations to support the compliance work of regulated operators, the Commission decides to postpone the entry into application:

- of the obligations concerning high-risk artificial intelligence systems ("AIS"), initially applicable from 2 August 2026, which will become mandatory on 2 December 2027 for systems falling under Annex III and on 2 August 2028 for systems falling under Annex I;

- of the obligation to mark generative AI systems (Art. 50(2) of the AI Act), originally scheduled for 2 August 2026, which is postponed to 2 December 2026 insofar as the system was placed on the market before 2 August 2026.

The obligation on Member States to set up a national regulatory sandbox (Art. 57 of the AI Act) is also postponed from 2 August 2026 to 2 August 2027, in view of the technical difficulties observed.

### Changes concerning the scope of the AI Act

The Digital Omnibus adds ***two new categories of "prohibited practices"*** within the meaning of Article 5 of the AI Act (the list of which cannot be amended directly by delegated act of the European Commission):

- AI practices that generate non-consensual sexual or intimate content (see in particular recital 12, which provides a full list of the prohibited "practices");
- AI practices that produce child sexual abuse material.

The reform also seeks to ***limit the risks of regulatory overlap***. To that end, it revises in particular the applicability of the AI Act to high-risk AIS falling under Annex I, that is, AIS already regulated by other sectoral instruments (toy safety, medical devices, etc.), provided that they include an equivalent level of safeguards regarding risks to health, safety or fundamental rights. As a result, only those AIS under Annex I that are intended to be used as "safety components of a product", in accordance with the new definition given in Article 3, will be subject to the obligations of the AI Act, that is, only products in respect of which:

- 1) the use of AI serves a purpose of safety of persons or property; or
- 2) the failure or malfunction "endangers the safety of persons or property".

Products that serve other purposes, such as optimising the product's performance, are therefore excluded from the scope of high-risk AIS. This clarification effort will be elaborated by the European Commission, which undertakes to determine, by 2 August 2027, which high-risk AIS are affected by this measure.

The Commission decides to ***formally exclude from the scope of the AI Act***, and in particular from the obligations on high-risk AIS, ***AIS that correspond to products or safety components of a product falling under the "Machinery" legislation*** (defined by Regulation No. 2023/1230 of 14 June 2023, which has an extremely broad scope), as lex specialis. The integration of the compliance rules for AIS in the field of machinery will have to be implemented by delegated acts of the European Commission by August 2028.

### Simplification measures for SMEs

The text expressly introduces the category of ***small mid-cap companies*** as provided for by Recommendation No. 2003/361/EC and the annex to the Commission's Recommendation No. 2025/1099. This category of entity benefits from the same relaxed compliance rules as those applying to SMEs and start-ups.

SMEs, including start-ups and small mid-cap companies, now have ***privileged access to the regulatory sandboxes*** run by the AI Office (Art. 57(3a)), but must also receive particular consideration both from the AI Office or the Member States when drawing up codes of conduct (new paragraph 4 of Art. 95), and from the European Commission when adopting guidelines (revised Art. 96(1) of the AI Act).

In the event of infringements of the AI Act, these same SMEs are subject to ***adapted penalties which must take account of their "economic viability"*** (new paragraph 1 of Art. 99).
All SMEs that deploy or use a high-risk AIS now benefit from the ***simplified mechanism for establishing a quality management system*** (internal compliance obligations), as provided for in Article 17 of the AI Act, which was initially limited to microenterprises (Art. 63). However, this simplified system is to be specified by European Commission guidelines.

The Digital Omnibus ***significantly eases the reporting obligations of providers who consider that their AIS is not high-risk*** with respect to the information required under the obligation to register AIS in the European database (Article 49). The following mandatory entries provided for in Annex VIII, point b), are removed:

- the brief summary of the reasons why the AI system is considered not to be high-risk, and
- the designation of the Member State in which the AIS was placed on the market.

The reform amends Article 60 of the AI Act on ***"testing" of high-risk AIS in real-world conditions*** (outside regulatory sandboxes) to extend it, in addition to high-risk AIS under Annex III, to high-risk AIS covered by Annex I, Section A. High-risk AIS listed in Annex I, Section B may also be covered by this authorisation of real-world testing, subject to national legislative reform by the Member States. This option is specified by a new Article 60a inserted in the AI Act.

**Cybersecurity measures**

Article 5 of the Digital Omnibus on AI seeks to simplify certain obligations of providers and deployers of AIS regarding ***internal staff training and, more generally, AI literacy itself*** among those who deploy and use it, by amending Article 4 of the AI Act (already applicable since February 2025) and shifting from a logic of mandatory training to recommended training: *"take measures to encourage a sufficient level of AI literacy for persons dealing with the operation and use of AI systems"*.

In addition, the Digital Omnibus on AI incorporates into Article 42 of the AI Act a rule on the interaction between the AI Act and Regulation No. 2024/2847 "Cyber Resilience" (or "CRA"). The latter expressly provides in its Article 12 that where a product with digital elements (connected product) contains a high-risk AIS, such a product is deemed to comply with the ***cybersecurity obligations contained in the CRA***. The amendment to the AI Act thus aligns this cross-reference with Article 12 of the CRA.

**Measures to align the processing of personal data by AIS**

The initial text of the AI Act placed on providers of high-risk AIS the obligation to ***correct any biases in their AIS liable to have "a negative impact on fundamental rights"***. Yet such a bias-correction requirement may involve processing sensitive data, which is prohibited in principle by Article 9 of the GDPR, subject to strictly framed exceptions. The Digital Omnibus on AI accordingly introduces a special derogatory legal basis for the sole purposes of detecting and correcting biases liable to have negative consequences on fundamental rights, subject to the safeguards laid down in a new Article 4a, which notably entails the implementation of reinforced technical and organisational measures (IT security, pseudonymisation, etc.). It should be noted that the reform opts to extend this legal basis to all providers and deployers of AIS and no longer only to providers and deployers falling within the category of high-risk AIS.

**Institutional measures**

The ***responsibilities of the AI Office*** are clarified as regards its now exclusive role as supervisory authority for:

- general-purpose AI models, excluding in particular high-risk AIS listed in Annex I or point 2 of Annex III;
- AIS that constitute, or are integrated into, a very large online platform or very large online search engine regulated by the DSA.

For the performance of its tasks, the AI Office has the powers granted to "market surveillance authorities" (requests for information, on-site investigation powers, seizure or copying of documents, etc.) within the meaning of Regulation No. 2019/1020, notably as regards monitoring and sanctioning powers (new Arts. 75a to 75e of the AI Act).

The powers of the AI Office are also extended by the introduction of a paragraph 3a in Article 57 on regulatory sandboxes, entrusting it with setting up and supervising such a sandbox at EU level for AIS within its supervisory competence (Art. 75(1)), in addition to national initiatives.

As part of the relaxation of the training and AI literacy obligation, the text requires the European Commission and the Member States to support regulated operators in this process and ***gives the AI Office the task of publishing recommendations to promote AI literacy***.

The text also seeks to ***streamline the procedures for designating the "notified bodies"*** competent for the conformity assessment of high-risk AIS falling under Annex I, by introducing a simplified procedure operated through the single window of the national supervisory authorities.

# ARTICLES

## Deceptive trademark at filing, deceptive trademark through use: the Cour de cassation's double sanction

*Cass. Com., 23 September 2026, No. 22-23.833*
*Cass. Com., 23 September 2026, No. 22-11.499*

The deceptive character of a trademark creates a risk at several stages of its life: at filing, a sign liable to mislead the public is likely to be refused, and then during its use, through the revocation of the rights of a proprietor whose mark has become deceptive because of the use made of it. Two judgments handed down on the same day by the Commercial Chamber of the Cour de cassation, both following a preliminary reference to the Court of Justice, each illustrate one of these mechanisms, in settings where the mark rests on a narrative: that of a historic house and that of an artist.

In the first case, the house of Fauré Le Page, founded in 1716 and active in gunsmithing and leather goods, had ceased trading in 1992. Its mark, filed in 1989 and transferred to a third party, was recovered in 2009 by a newly formed company, Fauré Le Page, before being supplemented in 2011 by two further filings of "Fauré Le Page Paris 1717" marks covering, in particular, leather goods. Goyard challenged these two marks, arguing that the use of the founding year of the historic house was a term misleading consumers.

Relying on the recent guidance of the Court of Justice of the EU, the French supreme court decides the dispute in Goyard's favour. Finding that the words "Paris 1717" evoked the place and date of the company's creation and suggested continuity of operation and a transmission of know-how, whereas the former house had disappeared in 1992 and the proprietor, created in 2009 to acquire and exploit marks, had not carried it on, the judges hold that this use was, from the time of filing, liable to mislead the public.

The second case concerns deceptiveness arising from the use of the mark. An artist had seen the assets of the company he founded in 1978, including his name-based marks, taken over in 2012 by PMJC in insolvency proceedings. During an initial phase and until 2015, the artist had entered into a commercial partnership with the acquiring company. Sued for trademark infringement and unfair competition after continuing his activity in collaboration with another company, he sought revocation of PMJC's rights in the two word marks bearing his surname.

The difficulty in this dispute was that the Court of Justice of the EU had held in its 2006 *Emanuel* judgment that the proprietor of a mark corresponding to the name of the designer may not, by reason of that feature alone, be revoked, in particular where the goodwill was assigned together with the business. Yet, at the request of the French Cour de cassation, that same Luxembourg court clarified in its judgment of 18 December 2025 that revocation of such a mark may be ordered, even where it was lawfully acquired by the third party, if the use he makes of it leads the average consumer wrongly to believe that the artist took part in designing the products.

Upholding the solution of the Court of Appeal, the Cour de cassation endorses the argument that the use made of the two marks by PMJC was liable to mislead the public insofar as it suggested the artist's collaboration or authorisation. The judges noted in particular that the company had been irrevocably convicted twice for infringing the artist's copyright in his recent unassigned works, notably by affixing the marks to products bearing infringing designs, presented as original creations of the assignor.

The Cour de cassation, under Article L. 714-6, b) of the Intellectual Property Code in its version prior to the Ordinance of 13 November 2019, accordingly dismisses the ground, which assumed the opposite.

**Cybersecurity: the institutions are making progress in supporting operators regulated by the Cyber Resilience Regulation**

*Regulation (EU) 2024/2847 of 23 October 2024 (Cyber Resilience Act)*
*Decree No. 2026-944 of 9 October 2026 on the notification of conformity assessment bodies for products with digital elements*
*Commission guidance on the application of Regulation (EU) 2024/2847*

Regulation No. 2024/2847, known as the "Cyber Resilience Act" ("CRA"), imposes cybersecurity requirements on all products with digital elements placed on the Union market, throughout their life cycle. Although it will be fully applicable from 11 December 2027, two waves of application have already been passed, on 11 June 2026 (concerning the obligation for Member States to designate "notified bodies") and then on 11 September 2026, concerning Article 14 on the notification of actively exploited vulnerabilities and severe incidents.

As to the first aspect, a French decree of 9 October 2026 designates ANSSI as the notifying authority, entrusting it with the oversight of notified bodies. Operators wishing to assess the conformity of regulated connected products therefore send it a written application accompanied by the documents provided for in Article 42(2) of the Regulation, after obtaining an accreditation certificate from the French Accreditation Committee (COFRAC). The decree nevertheless opens an alternative: a body whose accreditation application is admissible may be notified solely on the basis of evidence of its compliance with the requirements of Article 39, but it may then issue only twenty-five conformity certificates over a maximum period of twelve months, and ANSSI may put an end to this if accreditation is refused. ANSSI has two months from the filing of a complete file to notify the body to the Commission and the Member States, or to inform it of the grounds for refusal.

As to the second aspect, the European Commission has, for its part, published non-binding guidance as early as summer 2026 for regulated operators to support their compliance work. This guidance clarifies a number of points.

On scope, it recalls that the CRA covers only products supplied in the course of a commercial activity. Applied to free and open-source software, this requirement leads to a distinction between the project's "maintainer", who publishes it and controls its development and distribution, and the mere "contributor", who is not subject to the Regulation. The maintainer places the software on the market when it charges a price for the software itself, monetises other products or services, or requires as a condition of use the processing of personal data unrelated to the security, compatibility or interoperability of the software. By contrast, a free, non-monetised version is not regarded as placed on the market, even where a paid version coexists, and the provision of paid support services is not in itself sufficient to establish a commercial activity.

The guidance gives other useful clarifications to manufacturers. The support period, during which vulnerabilities must be handled effectively, must be at least five years unless the expected use time of the product is shorter, and must not be regarded as a default duration: it is determined case by case, in light of users' reasonable expectations and the nature of the product, and its end date must be indicated at the time of purchase.

As regards software updates, a modification is substantial only if it alters the cybersecurity risk level in a way that the initial risk assessment had not envisaged, which requires publishers to assess, case by case, the impact of each functional change.

**Patentability exclusion of a flight-path data display system: a second difficult landing**
*Cass. Com., 7 October 2026, No. 25-15.279*

The Intellectual Property Code excludes "presentations of information" from patentability (Article L. 611-10, 2, d). A substantial body of litigation has notably revisited the delicate boundary of the validity, in terms of patentability, of human-machine interfaces.

At issue was a patent application for a "Method for the temporal display of an aircraft's mission", filed by Thales and rejected in 2018 by the Director General of INPI on the ground that its subject matter concerned only a presentation of information associated with a mathematical method.

Indeed, claim 1 concerned a method of displaying on a screen the stages (waypoints) of a flight plan, in a graphical window comprising a time-graduated scale ("timeline") longer than the window, so that the user views only the portion he selects. The dependent claims provided in particular for automatic re-centring on the current time, a "magnifier" function and a second, map window.

The Cour de cassation had already ruled on 11 January 2023 in favour of rejecting this application on the ground that it made no "technical contribution" beyond the mere presentation of information.

The judgment of 7 October 2026 therefore comes in a second appeal, brought against the judgment of the court of appeal on remand of 26 March 2025, which had applied the solution of the quashing decision.

This time, the judges propose a more precise definition than the one adopted at the first intervention, where the reasoning already focused on the technical effect before even questioning the existence of an invention.

According to the Court, *"a claim that is limited to describing the information presented and various forms of presentation does not constitute an invention and is not patentable, unless it mentions a technical device or means that produces a technical effect making a technical contribution to the problem set out in the patent application"*. That effect is regarded as established "where there is objectively a reliable causal link" between the claimed feature and the assistance given to the user in performing the technical task, a link that is lacking where the alleged effect depends on the user's subjective interests or preferences.

More specifically, the supreme court clarifies the point criticised by part of academic opinion by recalling that the technical character of a claim is assessed at the patentability stage and is distinct from the invention's contribution to the state of the art, which falls under inventive step.

Applying this criterion, the Court upholds the reasoning of the appeal judgment:

- claim 1 relates only to a presentation of information along a timeline,
- the mere mention of a screen does not characterise a technical means,
- the application does not explain how the partial display of the timeline during the flight solves a technical problem distinct from the mere presentation of information, and no technical means of interaction allowing the view to be zoomed or re-centred is disclosed, nor any technical effect resulting from human-machine interaction.

**Protection of the integrity of a mural: the difficult duty of preservation borne by municipalities**
*Paris Court of First Instance, 1 October 2026, No. 25/00171*

Litigation concerning the defence of an artist's copyright in an architectural work or a mural commissioned by a public body continues to feature in case law every year. These particular works raise a difficulty with regard to the ordinary rules of the author's moral right, and more specifically respect for the integrity of the work. Being freely accessible in a public place, these works are liable to be damaged or defaced by third parties.

Many decisions have had to strike, in the past, a balance between strict respect for the artist's copyright and a principle of reality that makes absolute preservation of the work impossible in practice, given the legitimate constraints weighing on the owner, including, for a municipality, the neutrality of the public service, the prevention of public disorder, and the need to adapt, modify or renovate the place or facility housing the work.

In this case, a municipality had entered into a commission contract with an artist for the participatory creation of a mural in a car-parking area in return for the payment of EUR 1,000. The municipality, however, noticed that the work, measuring approximately 23 metres, bore an inscription "Justice pour…" in tribute to a victim whose widely reported death had sparked riots. It asked a third-party company to erase this graffiti, three days after the mural's inauguration. However, as this intervention led the contractor to cover the entire mural with white paint, the artist sued the municipality for infringement of her moral right.

In fact, covering the mural entirely amounted to a destruction of the work not authorised by the artist. The court therefore decides to reject the municipality's arguments, such as the principle of neutrality of the public service and the prevention of a disturbance of public order. Even assuming the aim to be legitimate, the court finds the interference disproportionate: the inscription, a minor element of a few square centimetres on a work about 23 metres long, could at least temporarily be masked or removed without altering the remainder. In this respect, the decision recalls the solution established by case law: the measure chosen by the owner must be the least detrimental possible to the work.

The decision is more surprising as regards the compensation awarded to the artist. The claims made in the pleadings (EUR 50,000 for loss of a chance to contribute to the author's reputation and EUR 20,000 for lost royalties) are dismissed in favour of a sum mentioned by the parties in an attempt at amicable settlement. The judges therefore award in total EUR 1,000 plus 10% for the moral prejudice suffered by the artist. This second aspect highlights the difficulty of valuing a work and its exploitation.

**Algorithmic personalization: placing trackers remains subject to internet users' consent**
*CNIL, 22 October 2026, Deliberation SAN-2026-015*

The placing of trackers or cookies on the terminal of an internet user visiting a website is governed by the "ePrivacy" Directive which, like the GDPR, requires the site operator to obtain the consent of the individual, unless the sole purpose of the operation is to enable or facilitate electronic communication or it is strictly necessary for the provision of a service expressly requested by the user. This technical measure indeed allows the operator of that same site to collect a certain amount of information about the user, which is then used for various purposes, such as optimising the recommendation of a given product or service in light of the profile drawn.

While the Digital Omnibus reform projects put forward by the European Commission note a phenomenon of "consent fatigue" among internet users constantly asked to accept or refuse the processing of their personal data, a recent CNIL deliberation addresses a case in which the site operator disregarded the choices expressed by the internet user, and in particular their refusal of trackers.

Following a complaint from the association None Of Your Business (NOYB) of 15 September 2023, the CNIL found that the mobile application of Fnac Darty automatically carried out read and write operations on users' terminals via an application programming interface (API), including where users had clicked "Continue without accepting". An identifier was assigned to the user while information on their activity, such as the products viewed, was collected, notably in order to train the recommendation algorithm for the display of personalised, similar or complementary products.

Contrary to the position suggested by Fnac, which argued that these operations amounted to a navigation aid, strictly necessary and expressly requested by the user who downloads and uses the application, the CNIL rejects the argument.

Recalling now well-established rules, the CNIL explains that personalisation of the products displayed and commercial targeting do not fall within the exceptions of Article 82 of the e-Privacy Directive. Accordingly, offering complementary products to the internet user or training the recommendation algorithm are not purposes strictly necessary for the operation of the service. It follows that the placing of trackers was indeed subject to the user's consent for each of the purposes pursued.

Consequently, the Fnac Darty group is fined EUR 6 million in view of the group's turnover (over EUR 10 billion in 2025), the seriousness of the breach (over 1.5 million downloads in France between March 2023 and March 2024), negligence, given the CNIL's recommendations published as early as 2013 and an established enforcement doctrine, and the group's lack of particular cooperation during the investigation.

FIDAL
AVOCATS

## Fidal est le plus grand cabinet d'avocats d'affaires français indépendant.

Partenaires stratégiques des entreprises, des institutions et des organisations, nous nous attachons à faire du droit un levier de leur performance et de leur croissance, en France et à l'international. Tout autant experts dans leur discipline que transverses dans leur approche, nos talents parlent le même langage que nos clients et comprennent leurs enjeux. Nous encourageons le partage de la connaissance et de l'expérience. C'est notre manière d'offrir à nos clients - quelles que soient leur taille, leur activité, leur implantation géographique ou les problématiques qu'ils nous soumettent- des conseils engagés, éclairés et avisés. Des conseils opérationnels qui les protègent et contribuent activement à leur développement stratégique et commercial.

Plus d'infos sur fidal.com
Suivez-nous sur les réseaux sociaux

contact@fidal.com

FIDAL - Société d'avocats • Société d'exercice libéral par actions simplifiée à directoire et conseil de surveillance. Capital : 6 000 000 Euros • 525 031 522 RCS Nanterre
TVA Union Européenne - FR 42 525 031 522 - NAF 6910Z • Siège social : 4-6 avenue d'Alsace - 92400 Courbevoie - France • T : 01 46 24 30 30 • Barreau des Hauts-de-Seine

MEMBER OF Unyer GLOBAL ADVISORS AND wts global