N° 626

SÉNAT

SESSION ORDINAIRE DE 2025-2026

Enregistré à la Présidence du Sénat le 13 mai 2026

RAPPORT D'INFORMATION

FAIT

au nom de la commission des affaires européennes (1)
*sur l'***omnibus numérique européen : un risque pour la protection des droits numériques des citoyens***,*

Par Mmes Catherine MORIN-DESAILLY et Karine DANIEL,

Sénatrices

(1) Cette commission est composée de : M. Jean-François Rapin*, président ;* MM. Alain Cadec, Ronan Le Gleut, Mme Gisèle Jourda, MM. Didier Marie, Claude Kern, Mme Catherine Morin-Desailly, M. Teva Rohfritsch, Mme Cathy Apourceau-Poly, MM. Cyril Pellevat, Louis Vogel, Mme Mathilde Ollivier, M. Ahmed Laouedj*, vice-présidents ;* Mme Marta de Cidrac, M. Daniel Gremillet, Mmes Florence Blatrix Contat, Amel Gacquerre*, secrétaires ;* MM. Georges Patient, Pascal Allizard, Jean-Michel Arnaud, Bruno Belin, François Bonneau, Mmes Valérie Boyer, Sophie Briante Guillemont, M. Pierre Cuypers, Mmes Karine Daniel, Brigitte Devésa, MM. Jacques Fernique, Christophe-André Frassa, Mmes Pascale Gruny, Nadège Havet, MM. Olivier Henno, Bernard Jomier, Mme Christine Lavarde, M. Dominique de Legge, Mme Audrey Linkenheld, MM. Vincent Louault, Louis-Jean de Nicolaÿ, Mmes Elsa Schalck, Silvana Silvani, M. Michaël Weber.

SOMMAIRE

L'ESSENTIEL

Le 11 novembre 2025, la Commission européenne a présenté **un paquet omnibus de simplification relatif au numérique**. Composé de deux volets, – l'un portant spécifiquement sur l'intelligence artificielle (IA), l'autre couvrant plus largement le champ du numérique et des données –, l'omnibus numérique est **un ensemble très dense qui modifie plusieurs textes formant l'arsenal juridique européen du numérique**.

Face à des retards pris dans l'élaboration de normes harmonisées, le **volet sur l'IA a fait l'objet de négociations au pas de course** afin de permettre le report de certaines obligations du règlement sur l'IA de 2024, qui devaient sinon s'appliquer au 2 août 2026.

Concernant le **volet « données »**, présenté par la Commission européenne comme un paquet de mesures de simplification « ciblées », il appelle plusieurs observations, notamment concernant la **réduction du niveau de protection des droits numériques garantis par le standard international qu'est le RGPD**.

Alors que la très grande majorité des plateformes en ligne et des systèmes d'IA dominant le marché européen sont américains et chinois, **l'Union européenne, tout en veillant à mener une politique industrielle offensive pour le secteur et à soutenir ses propres entreprises, ne doit ni trembler ni transiger dans l'application de l'arsenal juridique novateur et ambitieux qu'elle a commencé à construire pour encadrer le secteur numérique et l'IA**.

Les principales recommandations

1. **S'opposer à la modification de la définition de « données à caractère personnel » dans le RGPD, au risque d'en bouleverser l'équilibre protecteur** : dans un univers numérique de plus en plus complexe, l'Union européenne doit demeurer une boussole pour la protection des données personnelles.

2. **Refuser tout privilège pour l'IA dans le traitement des données sensibles, notamment biométriques ou de santé, en l'absence de garanties de protection suffisantes pour les droits et libertés numériques** : en dépit de l'importance de l'exploitation des données pour la compétitivité européenne, l'utilisation sans contrôle par l'IA de données sur le genre, l'origine ethnique, l'âge ou encore la religion est une source potentielle de discriminations.

3. **Interdire au niveau européen toute pratique en matière d'IA capable d'exploiter les éventuelles vulnérabilités économiques, personnelles ou sociales** et de causer préjudice aux personnes concernées. Cette interdiction ne saurait se limiter aux hypertrucages sexuels ; il convient d'**interdire les contenus générés ou manipulés par l'IA à caractère pédocriminel**, et plus largement toute pratique en matière d'IA de nature à **porter atteinte à la dignité de la personne humaine**.

4. **S'employer sérieusement au niveau européen à réduire la fatigue du consentement aux *cookies***, mais toute solution consistant à déplacer les règles en matière de cookies de la directive e-Privacy vers le RGPD créerait un double régime juridique dangereux pour le contrôle de ces traceurs, sans répondre à l'enjeu de diminution de la lassitude des citoyens européens face aux bannières de gestion des *cookies*.

5. **Ne pas concentrer les déclarations d'incidents en matière de cybersécurité au sein d'un point d'entrée unique géré par l'Agence de l'Union européenne pour la cybersécurité (ENISA)** : celui-ci pourrait en effet devenir un point de faille unique, concentrant des risques cyber nombreux et critiques, avec des implications potentielles pour la sécurité nationale, laquelle demeure une compétence exclusive des États membres.

I. LE VOLET IA DE L'OMNIBUS NUMÉRIQUE : UN TEXTE PRÉSENTÉ COMME ESSENTIELLEMENT TECHNIQUE, NÉGOCIÉ AU PAS DE COURSE ET QUI SOULÈVE DES QUESTIONS DE FOND POUR L'AVENIR DE L'IA EN EUROPE

A. L'ARRÊT DU CHRONO POUR LES OBLIGATIONS FAITES AUX IA À « HAUT RISQUE » : UN RÉVÉLATEUR DE LA DIFFICULTÉ À ENCADRER L'IA ET D'UN ÉCHEC RELATIF DU PROCESSUS DÉCISIONNEL EUROPÉEN

Le règlement sur l'IA est entré en vigueur le 1er août 2024. Depuis lors, ses dispositions entrent en application de manière échelonnée, la date butoir théorique étant le 2 août 2027. Toutefois, compte tenu des **retards pris dans l'élaboration de normes européennes harmonisées**, il est **apparu nécessaire de reporter cette échéance**. On parle de « **l'arrêt du chrono** » ou *stop the clock*.

Si un report à dates fixes est jugé nécessaire du point de vue de la sécurité juridique pour les entreprises du secteur, **il apparaît cependant révélateur de la difficulté rencontrée par la Commission européenne à anticiper pour encadrer un secteur complexe et au rythme d'innovation rapide**. L'évolution des règles ne doit pas se faire au pas de course, sous la pression du lobby des grandes plateformes, au risque de nuire à leur clarté et de déstabiliser les entreprises européennes et notamment les plus petites, et les citoyens, contribuant ainsi **au décrochage démocratique**.

B. DES PROPOSITIONS D'AJUSTEMENTS PAS SI « CIBLÉES » POUR FAVORISER L'INNOVATION : LA TENTATION PLUTÔT DE DÉRÉGULER L'IA

Des ajustements décrits par la Commission européenne comme « ciblés » sont proposés au règlement sur l'IA pour favoriser l'innovation.

Certains aménagements apparaissent bienvenus, comme l'**élargissement aux petites entreprises à moyenne capitalisation (PEMC) des simplifications existantes** (documentation technique allégée, sanctions proportionnées) pour les PME innovantes du numérique. En revanche, d'autres, comme l'élargissement des possibilités d'utilisation de données sensibles par l'IA, **introduisent des assouplissements dangereux aux règles destinées à protéger les droits et libertés numériques des citoyens européens**.

La commission des affaires européennes considère ainsi que **l'IA ne devrait pas avoir de privilège pour le traitement de données sensibles, en l'absence de garanties suffisantes quant aux mésusages que cette technologie pourrait en faire**.

Deux grands sujets sont en outre oubliés dans le **train de mesures proposé par la Commission européenne et validé en trilogue. Tout d'abord, en matière d'environnement**, le texte ne prévoit aucunement d'assortir les obligations déclaratives existantes, d'objectifs de réduction de ces consommations d'énergie et d'eau. De même, **l'examen de ce texte a écarté la nécessité de clarifier le régime juridique du droit d'auteur en matière d'IA**, comme cela avait été pourtant demandé par les rapporteures dans leur avis politique du 14 mai 2025 sur le code de bonnes pratiques en matière d'IA, alors que des solutions juridiques ont depuis été identifiées pour **veiller à la rémunération des contenus culturels utilisés par les systèmes d'IA**, en particulier la proposition de loi relative à l'instauration d'une présomption d'utilisation des contenus culturels par les fournisseurs d'intelligence artificielle, adoptée par le Sénat le 8 avril 2026, à laquelle les deux rapporteures se sont associées.

C. L'INTERDICTION DE LA NUDIFICATION PAR LES SYSTÈMES D'IA : UNE MESURE À COMPLÉTER POUR D'AUTRES USAGES PROBLÉMATIQUES

Lors des négociations, le Conseil, à l'initiative notamment de la France, a souhaité ainsi **amender la liste des systèmes d'IA interdits pour y ajouter les systèmes d'IA capables de produire des contenus de « nudification »** ainsi que des **contenus pédocriminels**. Seule l'interdiction de la nudification a abouti lors du trilogue conclusif du 7 mai 2026.

Cette étape est à saluer mais cette logique devrait être élargie aux atteintes à la « dignité humaine » (article 3 de la Charte des droits fondamentaux de l'Union européenne), bien que la proportionnalité d'une telle interdiction doive faire l'objet d'une évaluation attentive.

II. LE VOLET « DONNÉES » DE L'OMNIBUS NUMÉRIQUE : UNE REVISITE DU RGPD PRÉOCCUPANTE POUR LA PROTECTION DES DONNÉES PERSONNELLES EN EUROPE

A. CERTAINES « VRAIES » MESURES DE SIMPLIFICATION JUGÉES BIENVENUES

Outre des mesures techniques qui relèvent d'une codification à droit constant de dispositions relatives aux données, plusieurs propositions présentées par la Commission sont de **vraies mesures de simplification pour les entreprises**. Il en va ainsi de l'**allongement du délai de notification des incidents de sécurité** par les délégués à la protection des données aux autorités nationales compétentes, qui passe de 72 heures à 96 heures, permettant aux organisations concernées de parer à l'urgence puis de remplir, dans des délais demeurant raisonnables, leurs obligations de notification.

B. UN CUMUL DE MODIFICATIONS QUI POURRAIT VIDER LE RGPD DE SA SUBSTANCE, AU DÉTRIMENT DE LA PROTECTION DES DROITS ET LIBERTÉS NUMÉRIQUES

Le volet « données » de l'omnibus numérique modifie de manière substantielle le règlement général sur la protection des données (RGPD) de 2016. Or ce texte est devenu un étalon-or mondial de la protection des données personnelles, d'autant plus protecteur pour les citoyens européens que sa portée est extraterritoriale.

Dès lors, la commission des affaires européennes invite à la plus grande précaution dans la modification du RGPD :

• il apparaît **contreproductif et dangereux de modifier la définition de « données à caractère personnel »**, pour en écarter les données pseudonymisées ;

• les **dérogations supplémentaires envisagées pour le traitement de données à caractère personnel** (aux fins d'entraînement de l'IA, pour la recherche scientifique, y compris à des fins commerciales, au motif d'intérêt légitime…) apparaissent de nature à fragiliser les garanties existantes pour la protection des données sensibles (notamment de santé), avec des risques induits pour les libertés fondamentales.

À la différence du train de mesures sur l'IA qui a donné lieu à un accord en trilogue, le volet « données » de l'omnibus numérique en est encore au stade des négociations inter-institutionnelles, les premières réunions de trilogue ne devant pas avoir lieu avant l'été 2026.

La commission des affaires européennes invite le Gouvernement à veiller scrupuleusement au **maintien d'un niveau de protection suffisant des données à caractère personnel**, eu égard aux risques nouveaux que fait peser l'IA en la matière.

L'union européenne ne doit ni trembler ni transiger dans l'application de l'arsenal juridique novateur et ambitieux qu'elle a commencé à construire pour encadrer l'IA. Au contraire, elle devrait avoir l'ambition de faire du règlement sur l'IA un standard international en la matière, à l'instar du RGPD il y a huit ans, en matière de protection des données personnelles.

AVANT-PROPOS

La proposition d'omnibus numérique, objet de ce rapport d'information, intervient dans un cadre juridique européen dense et qui présente un rythme d'évolution particulièrement soutenu ces dernières années.

Ainsi, le cadre juridique européen du numérique, déjà complexe car composé de textes épars couvrant différents aspects et champs de régulation du secteur numérique (économie et concurrence, gestion des données, cybersécurité…) a été agrémenté depuis 2022 de plusieurs ajouts majeurs, dont notamment :

- en matière de cybersécurité : le règlement sur la résilience cyber de 2022[1] et le règlement sur la cyber-solidarité de 2023[2], destinés à améliorer la préparation, la détection et la réaction aux incidents de cybersécurité dans l'ensemble de l'UE ;

- en matière d'encadrement du secteur numérique : le règlement sur les services numériques (DSA) de 2022[3] qui encadre les activités des plateformes, en particulier celles des GAFAM, et le règlement sur les marchés numériques (DMA) de 2022[4] également, qui prévoit des obligations et interdictions opposables aux géants du numérique dans l'objectif de lutter contre les pratiques anticoncurrentielles dans ce secteur ;

- en matière d'IA : le règlement sur l'IA de 2024[5] ;

- de manière générale, concernant l'industrie numérique : le règlement sur les infrastructures gigabit de 2024[6] et le règlement européen sur les semi-conducteurs (Chips Act) de 2023[7].

---

[1] *Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).*

[2] *Règlement (UE) 2025/38 visant à renforcer la solidarité et les capacités dans l'Union afin de détecter les cybermenaces et incidents, de s'y préparer et d'y réagir (règlement sur la cybersolidarité).*

[3] *Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques).*

[4] *Règlement (UE) 2022/1925 relatif aux marchés contestables et équitables dans le secteur numérique (règlement sur les marchés numériques).*

[5] *Règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle).*

[6] *Règlement (UE) 2024/1309 du Parlement européen et du Conseil du 29 avril 2024 relatif à des mesures visant à réduire le coût du déploiement de réseaux gigabit de communications électroniques, modifiant le règlement (UE) 2015/2120 et abrogeant la directive 2014/61/UE (règlement sur les infrastructures gigabit).*

[7] *Règlement (UE) 2023/1781 du Parlement européen et du Conseil du 13 septembre 2023 établissant un cadre de mesures pour renforcer l'écosystème européen des semi-conducteurs et modifiant le règlement (UE) 2021/694 (règlement sur les puces).*

Malgré leur complexité et leur prolifération, il convient de souligner que la commission des affaires européennes du Sénat s'est efforcée d'analyser de manière systématique et approfondie l'ensemble des propositions de la Commission européenne ayant abouti à ces règlements.

S'agissant de règlements, ces textes trouvent à s'appliquer directement en droit français. Sur le plan national, le cadre européen a par ailleurs été conforté et complété par l'adoption le 21 mai 2024 de la loi n° 2024-449 visant à sécuriser et à réguler l'espace numérique (dite « loi SREN »).

C'est dans cet écosystème normatif foisonnant que s'inscrit la nouvelle proposition de la Commission européenne dite « omnibus numérique », présentée le 11 novembre 2025, dans un objectif affiché de simplification et d'harmonisation. Il s'agit d'un ensemble dense qui balaie une large portion de l'arsenal juridique européen du numérique. Il est ainsi composé de deux volets : le premier portant spécifiquement sur l'intelligence artificielle (IA) et modifiant le règlement sur l'IA de 2024, et le second, couvrant dans une approche plus extensive, les données et la cybersécurité.

I. LE VOLET IA DE L'OMNIBUS NUMÉRIQUE : UN TEXTE PRÉSENTÉ COMME ESSENTIELLEMENT TECHNIQUE, NÉGOCIÉ AU PAS DE COURSE ET QUI SOULÈVE POURTANT DES QUESTIONS DE FOND

La proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2024/1689[1] et (UE) 2018/1139[2] en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l'intelligence artificielle (ci-après « **train de mesures omnibus numérique sur l'IA** ») vise deux objectifs principaux :

- le **report dans le temps de certaines obligations prévues par le règlement sur l'IA de 2024**, d'une part ;
- des **ajustements décrits par la Commission européenne comme « ciblés » pour favoriser l'innovation** en matière d'IA en Europe, d'autre part.

[1] *Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) no 300/2008, (UE) no 167/2013, (UE) no 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle).*

[2] *Règlement (UE) 2018/1139 du Parlement européen et du Conseil du 4 juillet 2018 concernant des règles communes dans le domaine de l'aviation civile et instituant une Agence de l'Union européenne pour la sécurité aérienne, et modifiant les règlements (CE) n° 2111/2005, (CE) n° 1008/2008, (UE) n° 996/2010, (UE) n° 376/2014 et les directives 2014/30/UE et 2014/53/UE du Parlement européen et du Conseil, et abrogeant les règlements (CE) n° 552/2004 et (CE) n° 216/2008 du Parlement européen et du Conseil ainsi que le règlement (CEE) n° 3922/91 du Conseil.*

L'objectif de simplification apparaît légitime pour alléger certaines charges administratives pour les entreprises, notamment lorsqu'elles apparaissent disproportionnées au vu de leur taille. C'est un enjeu clé pour favoriser le développement de startups innovantes et leur passage à l'échelle (*scale-up*), face à la concurrence des géants américains et chinois.

En outre, le train de mesures omnibus numérique sur l'IA vise à renforcer la cohérence du cadre législatif européen du numérique. Ainsi, un rapport de la commission de l'industrie, de la recherche et de l'énergie (ITRE) du Parlement européen du 30 octobre 2025 (*Interplay between the AI Act and the EU digital legislative framework*, PE 778.575), avait souligné la nécessité d'améliorer la coordination du règlement sur l'IA avec les nombreux autres textes européens sur le numérique.

Pour autant, les rapporteures estiment que la proposition de la Commission européenne excède pour partie ces seuls objectifs d'harmonisation et de simplification. Elles soulignent ainsi la nécessité qu'il y aurait à enfin « mieux légiférer » au niveau européen[1], ce qui est fondamental dans un contexte géopolitique incertain.

1. L'arrêt du chrono pour certaines obligations faites aux systèmes d'IA : un aveu d'échec pour l'UE ?

a) Le choix d'un report à date fixe : la meilleure option du point de vue de la sécurité juridique pour les entreprises du secteur

Le règlement sur l'IA est entré en vigueur le 1er août 2024. Depuis lors, ses dispositions entrent en application de manière échelonnée, avec pour date butoir théorique le 2 août 2027.

En particulier, les obligations pour les systèmes d'intelligences artificielles dits « à haut risque », la mise en place des bacs à sable réglementaires en matière d'IA ou de systèmes d'évaluation de conformité, **devaient théoriquement entrer en application le 2 août 2026**.

[1] *Voir à cet égard le rapport d'information n° 190 (2024-2025), déposé le 4 décembre 2024, présenté par MM. Jean-François RAPIN et Didier MARIE et Mme Catherine MORIN-DESAILLY*

Qu'est-ce qu'une IA à haut risque ?

Le règlement sur l'IA de 2024 se fonde sur **une approche par niveau de risque des systèmes d'IA** pour définir les modalités de régulation et obligations qui incombent aux fournisseurs et déployeurs.

Un système d'IA est considéré comme à haut risque s'il est **utilisé comme composant de sécurité d'un produit**, ou s'il s'agit d'un produit lui-même, qui est couvert par la législation européenne de l'annexe I du règlement sur l'IA. Cette annexe couvre notamment les secteurs suivants : machines, jouets, ascenseurs, dispositifs médicaux, véhicules de transport…

Outre les systèmes d'IA de l'annexe I, des systèmes d'IA sont considérés à haut risque s'ils entrent dans des **domaines d'utilisation « cruciaux »**, tels l'éducation, la biométrie, les autorités répressives, l'administration de la justice… Ces domaines sont listés à l'annexe III du règlement sur l'IA.

De façon générale, un système d'IA n'est **pas considéré à haut risque s'il ne présente pas de risque significatif pour la santé, la sécurité ou les droits des personnes**.

Or, compte tenu des **retards pris dans l'élaboration de normes harmonisées sur l'IA**[1] rédigées par l'organisme européen de normalisation, il est **apparu nécessaire de reporter cette échéance**, en réponse notamment aux plaintes de nombreux acteurs, industrie numérique en tête. On parle en conséquence de « **l'arrêt du chrono** » ou « *stop the clock* », en anglais.

Dans sa proposition initiale, la Commission européenne envisageait un report de l'entrée en application des règles pour les systèmes à haut risque conditionné à la disponibilité des normes, orientations ou lignes directrices, précisant toutefois des dates butoirs :

- le 2 décembre 2027 (soit un report de 18 mois) pour les systèmes d'IA de l'annexe III (les systèmes d'IA à haut risque utilisés dans certains secteurs, comme l'éducation, les prestations sociales ou le contrôle des frontières) ;

- le 2 août 2028 (soit un report de 24 mois) pour les systèmes d'IA de l'annexe I (les systèmes d'IA à haut risque intégré dans un produit, par exemple, de l'imagerie médicale).

Alors qu'a été débattue la pertinence du choix d'un report à dates fixes ou de son conditionnement à la publication des normes de références, les colégislateurs se sont accordés dans leurs négociations sur un report à dates fixes. Cette approche est **en ligne avec la position défendue par la France** au Conseil, dans un objectif de clarté et de sécurité juridique.

[1] *Il s'agit des normes harmonisées du JTC 21 du CEN-CENELEC.*

Ainsi, le trilogue conclusif du 7 mai 2026 a supprimé le mécanisme de flexibilité proposé par la Commission européenne et **retenu uniquement les dates de report d'entrée en application** du 2 décembre 2027 pour les systèmes d'IA de l'annexe III et du 2 août 2028 pour les systèmes d'IA de l'annexe I.

Tout en déplorant le retard pris dans l'édiction des normes harmonisées, les rapporteures estiment qu'un report à date fixe et à relativement brève échéance est la meilleure option en termes de sécurité juridique et de prévisibilité pour les entreprises du secteur.

- En outre, les rapporteures saluent la position qui a été défendue par la France de n'appliquer **aucun report dans le temps des obligations de transparence pour les fournisseurs et les déployeurs de certains systèmes d'IA** (article 50 du règlement sur l'IA), qui visent le marquage des contenus générés artificiellement. Cet article du règlement sur l'IA va ainsi dans le sens d'une **première couche de protection des contenus protégés par le droit d'auteur**, comme le soulignait déjà la commission des affaires européennes dans son avis politique relatif au code de bonnes pratiques en matière d'intelligence artificielle à usage général, du 14 mai 2025[1].

- **À l'issue du trilogue conclusif du 7 mai 2026, un report de 6 mois des obligations de marquage au titre de l'article 50 du règlement sur l'IA aurait été acté[2] (soit le 2 décembre 2026 au lieu du 2 août 2026). Les rapporteures regrettent ce report qu'elles estiment dommageable tant du point de vue de la protection du droit d'auteur que de la transparence pour les citoyens dans leur utilisation de l'IA.**

b) Un report certes nécessaire mais révélateur de la difficulté à encadrer l'IA et d'un échec relatif du processus décisionnel européen

À l'issue d'une série d'auditions, les rapporteures de la commission des affaires européennes estiment que le report des obligations faites à certains systèmes d'IA était devenu nécessaire, eu égard à l'incertitude de l'application des normes, en l'absence de guides et outils de conformité à destination des entreprises. **Ce report apparaît ainsi justifié du point de vue de la compétitivité des entreprises européennes et pour éviter toute entrave à l'innovation dans le secteur de l'IA**, critique pour la compétitivité des systèmes d'IA européens.

Pour autant, alors que le **règlement sur l'IA a été adopté il y a à peine deux ans**, les rapporteures **jugent ce report révélateur des maux qui frappent la législation européenne du numérique** : une forme de « capture du régulateur » face un écosystème numérique complexe et rapide, d'une part, et un certain dysfonctionnement des processus européens, d'autre part.

---

[1] *Avis politique relatif au code de bonnes pratiques en matière d'intelligence artificielle à usage général, présenté par Mmes Karine DANIEL et Catherine MORIN-DESAILLY, adopté par la commission des affaires européennes du Sénat le 14 mai 2025.*

[2] *À la date du présent rapport, le texte du compromis issu du trilogue du 7 mai 2026 n'est pas paru.*

Ainsi, **confronté à une industrie numérique au rythme d'innovation soutenu et aux évolutions techniques particulièrement complexes**, ce report intervient sans suffisamment de recul pour pouvoir expertiser les effets des règles proposées par le règlement sur l'IA de 2024, qui n'est pas totalement implémenté. D'ailleurs, **la Commission européenne n'a pas soumis d'étude d'impact pour sa proposition d'omnibus numérique**, indiquant que le « document de travail des services » (« *staff working document* ») était suffisant.

Les rapporteures **déplorent l'absence d'étude d'impact**, qui – dans un environnement législatif européen du numérique dense, foisonnant et rapidement renouvelé – nuit à la bonne compréhension des propositions formulées et de leur insertion dans le droit de l'Union européenne. Elles soulignent que cette situation tend à démontrer que la Commission européenne a privilégié dans la période récente les effets d'annonce politique, au détriment d'un travail de fond abouti, qui certes prend du temps, mais s'avère nécessaire dans l'environnement numérique actuel.

Cette situation **soulève un sujet d'ordre plus général sur la clarté du droit européen**. En contradiction avec l'objectif affiché de simplification, des révisions rapides et peu expertisées du règlement sur l'IA peuvent paraître difficilement compréhensibles pour les entreprises, mais aussi pour les citoyens européens. Elles posent question quant à leur acceptabilité, qui en l'absence d'effort de pédagogie suffisant, participe au phénomène de décrochage démocratique.

Dès lors, les rapporteures s'interrogent sur le calendrier de cet « arrêt du chrono » : doit-il être perçu comme un aveu d'échec de la Commission européenne, confrontée à l'impossibilité de tenir les délais qu'elle s'était elle-même fixée pour l'édiction des normes de références harmonisées sur l'IA ?

La France, dans les négociations inter-institutionnelles menées en 2024 et 2025 sur le règlement sur l'IA, avait déjà identifié que le calendrier proposé était difficilement tenable au vu de la complexité d'aboutir à des normes techniques dans les délais prescrits, sur des sujets de droit aussi novateurs et complexes, l'UE étant en effet la première puissance à proposer une régulation systématique de l'IA.

Comme l'avait déjà soulignée la commission des affaires européennes dans son rapport d'information « Législation européenne : Peut mieux faire ! »[1], **le volontarisme européen alimente une dérive normative au risque de fragiliser l'UE**. **C'est particulièrement vrai dans le cas de la législation européenne du numérique et de l'IA, qui frappe par sa fragmentation.** Ainsi, près d'une dizaine de textes européens ont été adoptés entre 2022 et 2025 spécifiquement dans le secteur du numérique[2], sans compter les textes sectoriels ou connexes intéressant ces questions de près ou de loin. À titre d'exemple, les rapporteures estiment qu'un seul texte européen aurait pu utilement couvrir les mesures comprises dans le règlement sur l'IA, le règlement sur les services numériques (DSA) et le règlement sur les marchés numériques (DMA), tous trois adoptés ou mis en œuvre en 2024.

Face au cadre réglementaire européen du numérique très vaste posé par la précédente mandature, force est de constater qu'il faudra du temps à l'ensemble des acteurs de l'écosystème numérique – agences nationales de régulation, entreprises et administrations – pour mettre en œuvre et appliquer les règles. En conséquence, l'omnibus IA – comme les autres paquets omnibus – doit veiller à respecter une approche strictement circonscrite aux objectifs de simplification, de clarification et d'harmonisation. Il s'agit donc de limiter les nouvelles mesures ou les modifications profondes de textes récents.

Dans ce contexte, les rapporteures rappellent l'importance d'une **association pleine et entière des parties prenantes dans la préparation des projets de législation européenne**, y compris des Parlements nationaux. De même, l'effort de pédagogie et de communication auprès des entreprises et des citoyens européens doit être poursuivi et renforcé.

2. Des propositions pas si « ciblées » pour favoriser l'innovation : la tentation de déréguler l'IA

Outre l'enjeu du report dans le temps des obligations faites à certains systèmes d'IA, **le train de mesures omnibus numérique sur l'IA comprend plusieurs ajustements présentés par la Commission européenne comme « ciblés » au règlement sur l'IA** de 2024.

Destinés à favoriser l'innovation au sein de l'UE, en réduisant les coûts administratifs induits pour les entreprises, certaines mesures sont jugées positives par l'industrie numérique comme par les rapporteures ; d'autres soulèvent, par leur ampleur ou leurs effets cumulés, des questions quant aux risques potentiels, notamment du point de vue de la protection des données à caractère personnel.

---

[1] *Rapport d'information n° 190 (2024-2025), déposé le 4 décembre 2024, présenté par MM. Jean-François RAPIN et Didier MARIE et Mme Catherine MORIN-DESAILLY.*

[2] *En 2022 : cyber resilience act, DSA, DMA, Chips act ; en 2023 : cyber solidarity act ; en 2024 : règlement sur l'IA, GIA, managed security services act.*

a) Une série de mesures de simplification favorables aux startups et aux « scaleups »

Les rapporteures considèrent que **plusieurs mesures vont dans le bon sens**, c'est-à-dire dans le sens d'une simplification effective et de la réduction des charges induites pour les entreprises du secteur.

Plusieurs mesures visent ainsi la simplification des obligations administratives pour les petites et moyennes entreprises (PME) et les **petites entreprises à moyenne capitalisation (PEMC)**, dont les définitions sont clarifiées (paragraphe 3 de l'article 1 du train de mesures omnibus numérique sur l'IA).

La nouvelle catégorie européenne des petites entreprises à moyenne capitalisation (PEMC)

Introduite par l'omnibus IV de mai 2025 sur le marché unique, la catégorie petites entreprises à moyenne capitalisation (PEMC) correspond aux entreprises qui comptent plus de 249 salariés (PME), mais moins de 750 salariés, et qui ont soit un chiffre d'affaires n'excédant pas 150 millions d'euros, soit des actifs totaux n'excédant pas 129 millions d'euros.

L'omnibus numérique propose de faire bénéficier la logique de simplification à destination des PEMC, issue de l'omnibus IV, aux entreprises du numérique qui ont dépassé le stade de la startup et rejoignent le stade de la « *scaleup* ».

Les simplifications existantes (documentation technique allégée, sanctions proportionnées, etc.) et **les mesures de soutien à l'innovation ouvertes aux PME sont élargies aux PEMC**. Concrètement les mesures de simplification des startups seraient ouvertes aux *scaleups*, c'est-à-dire aux entreprises innovantes du numérique ayant atteint une certaine taille critique (paragraphes 1, 8 et 9 de l'article 1 du train de mesures omnibus numérique sur l'IA). D'autres mesures de simplification administrative de nature technique, à destination des micro-entreprises, PME et PEMC, sont également jugées favorablement par les rapporteures (notamment celles figurant aux paragraphes 21, 23, 27, 28 et 29 de l'article 1 du train de mesures omnibus numérique sur l'IA).

Alors que – comme le rappelle Arthur Mensch, co-fondateur et CEO de Mistral AI[1], **près d'un tiers des licornes européennes ont délocalisé leur siège à l'étranger, notamment vers les Etats-Unis**, toute mesure destinée à faciliter le développement des *scaleups* contribue effectivement à une stratégie européenne intégrée visant à faire de l'UE un acteur souverain et compétitif dans l'IA. Les mesures destinées à faciliter la conformité réglementaire des *scaleups* sont de nature à les encourager à demeurer implantées dans l'UE pour la suite de leur croissance. Elles viennent en complément des mesures destinées à améliorer leur accès au financement, projetées par ailleurs par la Commission européenne et des perspectives ouvertes par le 28e régime (« EU Inc. »), présenté le 18 mars 2026.

Les mesures visant **l'harmonisation et la simplification en matière de documentation technique et de système de gestion de la qualité**, avec un formulaire simplifié pour les PME/PEMC, sont également jugées favorablement. Elles rejoignent la proposition de Mistral AI de faire bénéficier les entreprises de documentations unifiées et standardisées pour réduire les coûts de conformité réglementaire.

Auditionnée le 29 avril 2026, l'association France digitale, qui regroupe 2 000 entreprises françaises et européennes du numérique, a confirmé que ces mesures sont jugées favorablement par ses adhérents. France digitale a néanmoins indiqué que les entreprises de son réseau ne s'attendaient pas particulièrement à de nouvelles mesures en matière d'IA (outre le report dans le temps des obligations faites à certains systèmes à haut risque, compte tenu de l'absence de normes harmonisées publiées dans les temps), ayant même déjà commencé à travailler à leur mise en conformité au règlement sur l'IA de 2024.

b) Les bacs à sable réglementaires : des dispositifs pas si enfantins en matière d'IA ?

En matière d'IA, les bacs à sable règlementaires, créés par le règlement sur l'IA de 2024, permettent aux entreprises, startups et développeurs de tester des systèmes d'intelligence artificielle innovants dans un environnement contrôlé, sous la supervision des autorités réglementaires. Le Sénat s'était déjà prononcé en faveur de la création des bacs à sable règlementaires en matière d'IA, tout en soulignant la nécessité d'un fonctionnement le plus homogène possible de ces bacs à sable, à travers les États membres[2]. Entendue le 29 avril 2026, France digitale confirme que les bacs à sable règlementaire en matière d'IA sont très appréciés par leurs adhérents pour permettre le test de nouvelles solutions, tout en bénéficiant, pour la France, d'un accompagnement de la Cnil.

---

[1] *Rapport « European AI : A playbook to own it », Arthur Mensch, Mistral AI (avril 2026).*

[2] *Voir la résolution européenne du Sénat n° 100 (2022-2023) relative à la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle et modifiant certains actes législatifs de l'Union, COM(2021) 206 final.*

Que sont les bacs à sable réglementaires ?

Les bacs à sable réglementaires sont des lieux d'expérimentation ouverts aux entreprises afin de leur permettre de tester leur technologie ou service innovant sans devoir nécessairement respecter l'ensemble du cadre réglementaire qui s'appliquerait normalement.

Ils sont opérés pour une durée donnée, sous la supervision d'agences nationales ou européennes, afin d'assurer une surveillance et de mitiger les risques.

L'omnibus IA propose plusieurs amendements concernant les bacs à sacs réglementaires de l'article 57 du règlement sur l'IA.

D'une part, le Bureau de l'IA (Commission européenne) deviendrait compétent pour mettre en place un **bac à sable réglementaire européen,** dès 2028, en plus des bacs nationaux, avec accès prioritaire pour les PME. Les rapporteures sont favorables à cette mesure qui apparaît de nature à renforcer la capacité des startups à atteindre une taille critique suffisante pour s'ouvrir au marché européen, bien qu'elles soulignent la nécessité pour les États membres de conserver des marges de manœuvre quant aux modalités de leur participation.

D'autre part, les bacs à sable, initialement réservés aux PME, seraient étendus aux **petites entreprises à moyenne capitalisation (PEMC)** et aux entreprises de taille intermédiaire (ETI).

Enfin, les bacs à sable pourront désormais inclure des **essais en conditions réelles** pour les systèmes d'IA à haut risque couverts par la législation sectorielle (ex : dispositifs médicaux, machines), sous supervision stricte.

Ces mesures sont jugées plutôt favorablement par les rapporteures, qui **soulignent néanmoins l'absence de recul suffisant pour déterminer réellement la pertinence de ces amendements, notamment en l'absence d'étude d'impact. Elles considèrent en outre comme potentiellement risqués les essais en conditions réelles pour les systèmes d'IA à haut risque dans certains secteurs (santé, industries critiques, …)**, ce qui plaide pour une supervision très stricte des autorités nationales, notamment en termes de sécurité des produits et de protection des données personnelles (notamment les données de santé).

Enfin, des questions restent ouvertes quant aux bacs à sable réglementaires pour l'IA, relativement à leur opérationnalité du point de vue des acteurs privés du numériques et aux perspectives de leur contrôle par les États-membres et le Bureau de l'IA, s'agissant du nouveau bac à sable paneuropéen.

Ainsi, dans ces environnements de tests, libérés des contraintes réglementaires, ou tout est virtuellement permis, les risques sont nombreux : risque de faille cyber, risque du point de vue de la gestion des données… ce qui fait de ces bacs à sable des terrains de jeu pas si enfantins à ce stade…

c) Les risques d'une gouvernance trop centralisée pour la surveillance de l'IA

La Commission européenne propose de renforcer les pouvoirs du Bureau de l'IA (le Bureau de l'IA étant pour mémoire intégré à la Commission européenne) dans une démarche de centralisation de la surveillance des systèmes d'IA, en vue de réduire la fragmentation de la gouvernance.

Ainsi, la **compétence du bureau de l'IA serait renforcée** s'agissant de la surveillance et de l'application du règlement pour certains systèmes d'IA basés sur un modèle d'IA à usage général, lorsque le modèle et le système sont fournis par le même prestataire. La supervision et le contrôle de la conformité des systèmes d'IA intégrés dans des plateformes en ligne ou des moteurs de recherche en ligne de très grande taille relèveraient également de la compétence exclusive du Bureau de l'IA.

Entendue le 28 avril 2026 en audition, la **Commission nationale Informatique et Libertés (CNIL) a insisté sur l'importance d'une bonne articulation entre les prérogatives du Bureau de l'IA et des autorités nationales de surveillance de marché**. Le renforcement des compétences du Bureau de l'IA et notamment le caractère exclusif de sa compétence dans les cas listés *supra*, conduiraient potentiellement à réduire la quantité et/ou la qualité des contrôles opérés, en empêchant les autorités nationales de se saisir d'un dossier, alors même que le Bureau de l'IA n'a pas souhaité se saisir.

Les rapporteures **estiment ainsi qu'une logique de dessaisissement serait préférable**. Selon une telle logique, les autorités nationales seraient tenues de se dessaisir dès lors que le Bureau de l'IA souhaite opérer un contrôle dans les secteurs concernés. Cette logique est **favorable à une meilleure coordination entre agences nationales, tout en renforçant la gouvernance du Bureau de l'IA, pour les contrôles transfrontaliers**.

Dans le cadre des négociations en cours, le Conseil et le Parlement européen ont souhaité réduire la portée des compétences techniques du Bureau de l'IA, notamment afin d'assurer un partage des compétences avec les autorités nationales concernées. Il conviendra de voir ce qu'il advient de ces propositions au prisme des résultats du trilogue conclusif du 7 mai 2026, dont les conclusions restent à paraître à la date de ce rapport.

d) L'extension des systèmes d'IA interdits (nudification, pédopornographie, …) : quel cadre pour quelles interdictions ?

Deux points qui ne faisaient pas partie de la proposition initiale de la Commission européenne ont été ajoutés par le Conseil, à l'initiative de la France et d'autres États-membres, afin de compléter la liste des systèmes d'IA interdits (article 5 du règlement sur l'IA).

Considérant que le cadre juridique existant est insuffisant pour responsabiliser et sanctionner les fournisseurs de systèmes d'IA[1], la France a porté au Conseil une **logique d'élargissement de la liste des pratiques interdites en matière d'IA** (article 5 RIA). Elle a proposé d'y ajouter de manière ciblée deux interdictions concernant d'une part, les systèmes d'IA capables de produire ou générer des hypertrucages sexuels sans consentement (« nudification »), et d'autre part, les contenus pédocriminels.

Dans son mandat de négociation, le Conseil a suggéré d'**interdire les systèmes d'IA** capables de générer, manipuler ou reproduire des contenus (image, vidéo, audio) **« représentant les parties intimes ou des activités sexuellement explicites d'une personne », sans son consentement** (« nudification »). De même, le Conseil a retenu l'**interdiction des contenus pédopornographiques générés par IA** (« *child sex abuse materials* »). Les systèmes qui, dans leur conception, entraînement, architecture ou fonctionnalité, permettent de produire ces contenus « sans nécessiter de modification technique » et qui n'ont pas de « mesures de sécurité techniques efficaces » pour lutter contre seraient aussi interdits, dans une logique conforme au principe de sécurité dès la conception (« *safety by design* »).

Pour sa part, dans son mandat de négociation, le **Parlement européen a repris uniquement l'interdiction de la nudification** (considérant 5 bis), tout en nuançant cette interdiction qui « *ne devrait pas empêcher les fournisseurs d'IA de développer leurs capacités techniques à modifier, manipuler ou produire artificiellement des images ou des vidéos.* »

Si l'interdiction des contenus de nudification a abouti lors du trilogue conclusif du 7 mai 2026, les rapporteures regrettent que tel ne soit pas le cas de l'interdiction des contenus pédopornographiques

Concernant le périmètre des interdictions de nudification, une approche listant les parties du corps concernées a été retenue, ce qui pourrait permettre de couvrir les contenus de nudification partielle. Cette extension des interdictions à la nudité partielle, en ligne avec la position du Gouvernement français, est effectivement jugée souhaitable par les rapporteures.

---

[1] *Le règlement sur les services digitaux prévoit bien l'interdiction de la diffusion de tels contenus, mais le règlement sur l'IA n'interdit pas aux fournisseurs des systèmes d'IA que ces systèmes puissent proposer de telles options.*

De façon principielle, les rapporteures estiment qu'une **approche plus extensive pourrait viser toutes les atteintes à la personne ou à la dignité humaines** (article 3 de la Charte des droits fondamentaux de l'UE). Toutefois, se poserait alors la question de la formulation juridique des interdictions listées à l'article 5 du règlement sur l'IA. Une extension systémique à tous contenus dégradants pour la dignité humaine pourrait en effet **se heurter à des difficultés de proportionnalité** (articles 11 et 49 de la Charte) **et de prévisibilité**, ce qui plaide pour une analyse au cas par cas, à travers des dispositions sectorielles le cas échéant, qui trouveraient leur place à l'annexe III, article 7 du règlement sur l'IA.

Les rapporteures notent en outre que **l'effectivité des recours en cas de violation constatée est déjà garantie**. Ainsi, l'article 226-8-1 du code pénal, créé par l'article 21 de la loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (loi SREN), sanctionne déjà de 2 ans et 60 000 euros d'amende, la mise à la connaissance du public ou d'un tiers d'un montage à caractère sexuel non consenti, y compris généré algorithmiquement. De plus, la directive (UE) 2024/1385 du 14 mai 2024 sur la lutte contre la violence à l'égard des femmes et la violence domestique fournit un socle juridique au niveau européen et le règlement sur l'IA permet la saisine de l'autorité de surveillance du marché (article 85[1]), étant précisé que le retrait des contenus relève principalement du règlement sur les services numériques (DSA) de 2024.

Concernant l'interdiction des contenus de nudification, lors du trilogue conclusif du 7 mai 2026 aurait été ajouté un considérant dans le dispositif afin de préciser que « les interdictions sont sans préjudice des voies de recours offertes par le droit national », notamment en cas de non-respect de la dignité humaine. Cette disposition de principe va dans le sens de la position défendue par les rapporteures.

En revanche, les rapporteures considèrent que **doit être renforcée la littératie de l'IA pour les citoyens européens** – c'est-à-dire leur capacité à lire, comprendre et traiter l'information produite par l'IA –, y compris la connaissance de leurs droits et libertés et des voies de recours en cas d'abus. Au vu des usages émergents des IA, des risques nouveaux (cyberharcèlement, manipulation par l'IA, …) pourraient émerger ou s'amplifier pour les citoyens européens et notamment les plus jeunes. L'éducation et la formation continue au numérique et à l'IA apparaissent critiques pour garantir des usages éclairés de ces outils.

[1] *Des amendes sont en outre prévues à l'article 99, paragraphe 3 du règlement sur l'IA, mais sans droit subjectif à indemnisation des victimes.*

e) Faut-il modifier l'annexe I du règlement sur l'IA, comme le propose le Parlement européen ?

Non prévu dans la proposition initiale de la Commission européenne, **la fusion des deux sections de l'annexe I du règlement sur l'IA** a été proposée par le Parlement européen (notamment par le groupe du parti populaire européen, PPE). Cette fusion conduirait à ce que, pour les produits intégrant de l'IA, les législations sectorielles (comme le règlement sur les dispositifs médicaux *in vitro* ou encore sur les jouets) priment sur le règlement sur l'IA, réduisant les obligations et besoins de documentation.

Cette proposition est **le point de blocage principal dans les discussions entre les colégislateurs**. La proposition de compromis de la Présidence chypriote n'a ainsi pas permis de faire aboutir le trilogue du 28 avril 2026, pourtant souhaité conclusif.

Souhaitée par les acteurs de l'industrie[1], la fusion des deux sections de l'annexe I du règlement sur l'IA est au contraire jugée défavorablement par plusieurs associations de la société civile[2], qui défendent qu'elle pourrait avoir des conséquences néfastes pour la protection des consommateurs, car elle reviendrait à « *exclure un large éventail de systèmes d'IA industriels et grand public du champ d'application direct du règlement sur l'IA* » notamment en matière de technologie de la santé où elle serait donc contraire à l'objectif de sécurité des patients.

L'enjeu est donc de savoir si, secteur par secteur, les réglementations sectorielles apportent des garanties équivalentes au règlement sur l'IA quant aux risques spécifiques des systèmes d'IA pour le secteur concerné.

Au sein du Conseil, plusieurs États membres (la Belgique, la Bulgarie, la République tchèque, la Grèce, l'Espagne, la Lettonie, le Luxembourg, la Hongrie, Malte, l'Autriche et la Slovaquie) s'opposent à la fusion des deux sections de l'annexe I du règlement sur l'IA, la Slovénie et la République tchèque ayant même fait de ce point une ligne rouge des négociations.

Entendue par les rapporteures le 28 avril 2026, le SGAE a indiqué que la France a, elle, estimé que cette proposition de fusion aurait mérité une analyse approfondie. La France appelle ainsi à une clarification des chevauchements éventuels entre le règlement sur l'IA et les régulations sectorielles, eu égard aux effets de bords potentiels pour la protection de la santé, de la sécurité et des droits fondamentaux.

---

[1] *Voir notamment la déclaration conjointe d'acteurs de l'industrie numérique sur le train de mesures omnibus sur l'IA : appel à un accord rapide axé sur la simplification (« Joint Industry Statement on the Digital Omnibus on AI calling for a swift agreement with simplification at its core ») du 10 avril 2026.*

[2] *Voir la lettre ouverte de plusieurs organisations de la société civile, sur le train de mesures omnibus sur l'IA « préserver le périmètre et l'intégrité du règlement sur l'IA » (Open Joint Letter on the Digital Omnibus on AI, Preserving the Scope and Integrity of the AI Act), du 8 avril 2026.*

Pour sa part, la Commission européenne estime que la fusion des deux sections de l'annexe I du règlement sur l'IA risquerait de « fragmenter » les règles européennes et d'« abaisser les exigences et les niveaux de sécurité ».

Les rapporteures soutiennent la position française et soulignent en outre l'importance, notamment dans certains secteurs « cruciaux » (jouets, équipements médicaux, etc.), de favoriser une approche de sécurité dès la conception ou « *safety by design* », qui est conforme à l'esprit du règlement sur l'IA avec son approche par niveau de risque.

Le trilogue conclusif du 7 mai 2026 a abouti à un accord interinstitutionnel sur ce point, conformément à la proposition de compromis présenté par la présidence chypriote du Conseil. Ce compromis reprend la proposition allemande de transférer uniquement le règlement sur les machines[1] de la section A à la section B de l'annexe I. Ce règlement encadre une large gamme de machines et équipements de natures et d'importances diverses, allant des outils de bricolage aux machines et robots industriel. En pratique, cela signifie que le règlement sur l'IA ne s'appliquera plus directement aux systèmes d'IA intégrés dans des produits couverts par le règlement sur les machines.

Les rapporteures prennent acte de ce compromis qui a permis le déblocage des négociations interinstitutionnelles, mais regrettent qu'en l'absence d'étude d'impact, il soit difficile d'apprécier si le règlement sur les machines présente un niveau de garanties équivalent à celui du règlement sur l'IA pour les produits embarquant de l'IA, couverts par cette réglementation.

f) Des premières évolutions jugées sensibles de l'approche protectrice du traitement des données à caractère personnel aux fins de correction des biais des IA

La proposition initiale de la Commission européenne entendait élargir **la possibilité de traitement de catégories particulières de données personnelles (sur l'origine, les convictions politiques ou religieuses, sur la santé, la sexualité, l'identification) aux fins de détection et correction des biais des systèmes d'IA**, aux « fournisseurs et aux déployeurs d'autres systèmes et modèles d'IA ».

Dans le cadre des négociations inter-institutionnelles, le Conseil comme le Parlement européen ont souhaité **conditionner cette extension pour qu'elle soit accordée « à titre exceptionnel, et lorsque cela est strictement nécessaire »**, aux systèmes d'IA qui ne sont pas considérés à haut risque, eu égard aux risques pour les droits fondamentaux.

---

[1] *Règlement (UE) 2023/1230 du Parlement européen et du Conseil du 14 juin 2023 sur les machines, abrogeant la directive 2006/42/CE du Parlement européen et du Conseil et la directive 73/361/CEE du Conseil.*

Cette formulation reprend la recommandation de l'avis conjoint (n° 2/2026) du Comité européen de la protection des données (CEDP) et du Contrôleur européen de la protection des données (EDPS) sur la proposition de règlement omnibus numérique en date du 10 février 2026.

Les rapporteures soutiennent la formulation de compromis du Conseil et du Parlement qui s'appuie sur le standard de la jurisprudence issue de l'arrêt Schrems II (CJUE, 16 juillet 2020, C-311/18) en matière de nécessité du traitement.

Cependant, notant que ces traitements sont par principe interdits aux humains au titre du règlement général sur la protection des données (RGPD), les rapporteures considèrent que **des garde-fous additionnels pourraient être utiles pour veiller au développement d'IA alignées avec les valeurs européennes**. Ces garanties supplémentaires pourraient passer par la circonscription du champ d'application de la dérogation à la correction des biais affectant la santé, la sécurité ou des discriminations expressément prohibées et par une obligation explicite de documentation soumise au contrôle des autorités de surveillance, démontrant l'impossibilité d'une alternative moins intrusive (par exemple en utilisant des données synthétiques ou anonymisées).

3. Un avis en demi-teinte sur le volet IA

Tout en prenant acte des évolutions apportées, les rapporteures **dénoncent la rapidité des négociations sur le volet IA et s'interrogent sur la réalité de l'association des parties prenantes et des États-membres**, dans un calendrier aussi contraint. Ce constat est d'autant plus vrai que l'IA était particulièrement peu réglementée avant l'introduction du règlement sur l'IA en 2024. Alors que ce règlement n'est pas encore totalement mis en œuvre, les amendements qui lui sont proposés peuvent être perçus comme des atténuations du cadre envisagé en 2024 pour le développement de l'IA dans une logique d'alignement avec les valeurs européennes. Cette situation apparaît à rebours de certaines orientations stratégiques qu'avait défendues la commission des affaires européennes du Sénat en 2023[1].

Si la simplification est nécessaire pour répondre aux défis de la compétitivité des entreprises européennes œuvrant dans le secteur de l'IA, les rapporteures rappellent que les règles ainsi définies s'appliquent indifféremment à elles et aux géants américains et chinois, conformément au principe d'extraterritorialité.

---

[1] *Voir le rapport d'information n° 483 (2022-2023), déposé le 30 mars 2023, « Pour un déploiement de l'intelligence artificielle conforme aux valeurs européennes ».*

Dès lors, certaines mesures, telles l'autorisation du traitement de catégories particulières de données personnelles (sur l'origine, les convictions politiques ou religieuses, sur la santé, la sexualité, l'identification) aux fins de détection et correction des biais des systèmes d'IA posent question quant à la protection des droits numériques des citoyens européens, d'où la nécessité de garde-fous et garanties suffisants.

4. L'environnement, grand oublié du train de mesures omnibus sur l'IA

Si le règlement sur l'IA invoque un **objectif de protection de l'environnement** « contre les effets néfastes de l'IA », à travers des règles harmonisées (considérants n° 1 et 8 du RIA), il ne prévoit aucune contrainte en la matière. Seules sont prévues des obligations déclaratives portant sur les systèmes d'IA, notamment concernant la consommation d'énergie. Néanmoins, ces obligations déclaratives ne sont pas assorties d'un objectif de réduction de la consommation énergétique des systèmes d'IA.

En outre, comme le rappelle le programme pour l'environnement des Nations Unis (PNUE), l'IA soulèvent d'autres enjeux pour l'environnement que la seule consommation énergétique en termes de puissance de calcul : l'IA implique une utilisation importante de matières premières et d'eau. Le PNUE suggère ainsi que « les gouvernements peuvent élaborer des réglementations obligeant les entreprises à divulguer les conséquences environnementales directes des produits et services basés sur l'IA ».

Les rapporteures déplorent par conséquent **l'insuffisante prise en compte des aspects environnementaux de l'IA**, qu'un train de mesures aussi large que l'omnibus numérique aurait pu facilement intégrer. Elles considèrent en outre qu'il serait utile d'assortir les obligations déclaratives existantes en matière de consommation énergétique, d'obligations en termes d'objectifs de réduction de ces consommations. Pourrait également être envisagée l'introduction d'obligations déclaratives en matière environnementale pour les grands fournisseurs d'IA, à l'échelle de l'ensemble du cycle de vie des systèmes d'IA.

Sur ce point, il convient de noter que la commission de l'aménagement du territoire et du développement durable du Sénat a lancé, le 10 décembre 2025, une mission d'information sur l'empreinte environnementale de l'intelligence artificielle.

5. Le rappel de la nécessité de concilier protection du droit d'auteur et IA

Les rapporteures **regrettent également l'absence de toute disposition sur le droit d'auteur et l'IA** dans le projet de la Commission européenne et dans les négociations en cours entre les colégislateurs.

Les rapporteures considèrent cette absence comme une omission dommageable, alors même que les juridictions commencent à se prononcer en la matière[1] et que des solutions juridiques ont été identifiées pour concilier protection du droit d'auteur et développement de l'IA, comme le souligne d'ailleurs l'**adoption par le Sénat de la proposition de loi n° 220 (2025-2026) relative à l'instauration d'une présomption d'utilisation des contenus culturels par les fournisseurs d'intelligence artificielle le 8 avril 2026** et pour laquelle le Conseil d'État avait rendu un avis favorable le 19 mars 2026.

II. LA PROPOSITION DE RÈGLEMENT OMNIBUS NUMÉRIQUE MODIFIANT « L'ACQUIS NUMÉRIQUE » ET LES MODIFICATIONS AU RGPD : QUEL AVENIR POUR LA PROTECTION DES DONNÉES PERSONNELLES ?

1. Des propositions de la Commission européenne qui balaient un large champ de l'arsenal juridique européen sur le numérique

La proposition de règlement du Parlement européen et du Conseil COM(2025)837 modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024, dite « **règlement omnibus numérique** », entend simplifier le cadre législatif numérique, en modifiant neuf textes de « l'acquis numérique » et en abrogeant quatre autres textes.

Ce texte comprend plusieurs aspects, dont les dispositions principales sont présentées ci-après, ainsi que la position des rapporteures sur chacun des volets, eu égard aux points de vigilance soulevés par les personnes entendues et l'analyse juridique et contextuelle des propositions.

À la différence du train de mesures omnibus numérique sur l'IA, pour lequel les négociations ont abouti à l'occasion du trilogue conclusif du 7 mai 2026 et présagent d'une suite favorable et rapide pour la proposition de règlement en la matière, la proposition de « règlement omnibus numérique » n'a à ce stade fait l'objet que de premières réunions techniques au sein du Conseil de l'UE. Les trilogues pourraient ne débuter qu'à compter de l'ouverture de la prochaine présidence tournante, par l'Irlande, à compter du 1er juillet 2026.

[1] *Voir notamment la décision du Tribunal régional de Munich I, 11 novembre 2025, n° 42 O 14139/24, GEMA c/ OpenAI et la décision pendante de la CJUE C-250/25 Like Company c/ Google Ireland.*

La présente proposition de résolution entend donc présenter l'avis du Sénat quant à cette proposition de règlement, en vue de sa prise en compte pour la conduite des négociations inter-institutionnelles en cours et à venir.

a) Un volet « données non sensibles » jugé essentiellement technique et qui n'appelle pas de vigilance particulière

Le **volet « données non sensibles »** du « règlement omnibus numérique » opère pour l'essentiel une codification à droit constant de dispositions figurant dans divers textes, avec l'objectif d'harmoniser et d'améliorer la coordination des textes entre eux et de supprimer les redondances.

Dans ce contexte, les mesures envisagées sur ce point n'appellent pas de réaction particulière de la part des rapporteures, qui soulignent leur pertinence dans un objectif de clarté et d'intelligibilité du droit européen du numérique. Par exemple, la proposition **améliore la cohérence et l'articulation entre les différentes dispositions portant sur la gestion et l'utilisation des données, notamment en abrogeant le règlement sur le libre flux des données à caractère non personnel**[1], rendu obsolète par l'adoption du règlement sur les données[2] (ou « data act »), tout en conservant ce principe fondamental qui s'exprime notamment au travers de l'interdiction d'imposer la localisation des données. Il en va de même de l'abrogation de la directive « données ouvertes[3] », devenue obsolète.

Par ailleurs, concernant les données non sensibles, les amendements aux règles existantes sont largement perçus comme des améliorations techniques, avec par exemple le **renforcement de la protection du secret des affaires en matière de données**. Il s'agit ainsi d'élargir la possibilité de s'opposer à la divulgation de données qui constituent un secret des affaires, lorsqu'il existe un risque élevé d'obtention ou d'utilisation illicites ou de divulgation illicite à des pays tiers, ou à des entités placées sous leur contrôle.

b) Le volet « cyber » : la création d'un point d'entrée unique pour la déclaration des incidents ou le risque d'un point de faille unique

Le **volet « cyber »** du « règlement omnibus numérique » consiste principalement en **la création d'un point d'entrée unique** (dit « single entry point » ou « SEP »), pour la déclaration des incidents de cybersécurité dans l'UE. Ce point d'entrée unique serait géré par l'Agence de l'Union européenne pour la cybersécurité (ENISA).

---

[1] *Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne.*

[2] *Règlement (UE) 2023/2854 du Parlement européen et du Conseil du 13 décembre 2023 concernant des règles harmonisées portant sur l'équité de l'accès aux données et de l'utilisation des données et modifiant le règlement (UE) 2017/2394 et la directive (UE) 2020/1828 (règlement sur les données)*

[3] *Directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public.*

Cette proposition répond à une problématique concrète issu du cadre régulatoire actuel : un même incident peut aujourd'hui nécessiter plusieurs notifications, selon des formulaires différents avec des informations différentes à fournir et dans des délais différents. Cette situation crée une lourdeur et une complexité administrative non négligeable pour les entités concernées.

La création du point d'entrée unique ne modifierait pas les destinataires finaux des signalements (selon les obligations imposées par les directives NIS2[1] pour la résilience cyber, REC[2] pour la résilience physique, le RGPD, le règlement eIDAS[3], mais aussi les textes sectoriels applicables pour le secteur bancaire et financier, le secteur de l'énergie, ou encore celui des transports aériens). La création du point d'entrée unique ne modifierait pas non plus le contenu des obligations déclaratives des incidents.

Dans une contribution écrite qu'elle a souhaité transmettre aux rapporteures, l'Afep indique accueillir favorablement la proposition de la Commission européenne visant à mettre en place un point d'entrée unique pour répondre aux obligations de déclaration des entreprises soumises à des obligations en matière de cybersécurité, mais que cette mesure soulève néanmoins des questions et des incertitudes quant à sa mise en œuvre pratique. Les rapporteures **déplorent en effet l'absence de détails opérationnels quant à l'organisation concrète que pourrait prendre le point d'entrée unique**, notamment en l'absence d'étude d'impact, qui là encore fait défaut.

Auditionnée le 29 avril 2026, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) considère même que – de par la concentration en un même lieu de l'ensemble des informations sur les failles de cybersécurité européennes – **le point d'entrée unique pourrait se transformer en un point de faille unique (« single point of failure »)**, qu'il pourrait par ailleurs être très compliqué pour l'ENISA de sécuriser de manière robuste. En effet, la logique du SEP est contraire aux bonnes pratiques de la résilience cyber, fondées notamment sur l'idée de redondance. Le système de gouvernance actuel, fondé sur la possibilité pour les États membres de mettre en place des guichets régionaux ou sectoriels, participe de la création de relais locaux de confiance pour les entreprises et entités confrontées à des incidents

---

[1] Directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

[2] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

[3] Règlement (UE) 90/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

de cybersécurité. La centralisation de la notification vers un point central distant ne va pas dans le sens du renforcement de la confiance.

Pour répondre aux complexités administratives existantes, une **solution alternative fondée sur l'harmonisation des obligations de notification des incidents cyber, issues de différents textes** (NIS2, cyber resilience act, cybersecurity act[1], eIDAS, etc.) **apparaît préférable**. Elle passerait une retouche à la marge des textes concernés pour assurer que sont demandés pour les mêmes incidents des informations identiques dans des calendriers identiques, aux fins d'harmonisation des formulaires.

En complément, avec la création du SEP, le renforcement des prérogatives de l'ENISA et la centralisation des déclarations d'incident apparaissent **contraires aux principes de subsidiarité et de proportionnalité**, eu égard aux enjeux de sécurité nationale sous-jacents en matière d'incidents cyber. En déplaçant le centre de gravité des États membres vers l'ENISA, les États membres perdent le droit de filtrage dont ils disposent aujourd'hui pour partager ou non, à l'échelon européen, des informations sur les failles de cybersécurité d'infrastructures critiques nationales.

Les rapporteures invitent donc le Gouvernement à s'opposer fermement à la proposition de la Commission européenne et à soumettre au Conseil une solution alternative fondée sur une harmonisation des exigences déclaratives figurant dans les différents textes européens.

Dans le cadre des premières négociations techniques, le Gouvernement français – en phase avec plusieurs autres États-membres (Allemagne, Italie, Suède…) – s'est indiqué très réservé concernant la proposition de ce point d'entrée unique, notamment en l'absence de détails sur les modalités techniques de sa mise en œuvre.

c) La fausse bonne idée pour réduire la lassitude du consentement aux cookies

Si les rapporteures partagent largement **l'objectif de réduire la lassitude face à la prolifération des bannières de consentement aux traceurs (cookies),** il apparaît que plusieurs mesures du nouveau régime de consentement aux cookies pourraient soulever des difficultés d'application sérieuses.

Le bouton de refus en un clic, l'interdiction de re-sollicitation pendant six mois et la consécration des signaux automatisés (article 88 ter) pourraient constituer des avancées concrètes. Toutefois, en l'absence d'étude d'impact, les rapporteures estiment que ces mesures créent des zones d'incertitude qu'il convient de lever en amont de l'adoption du texte.

---

[1] *Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) no 526/2013 (règlement sur la cybersécurité).*

En outre, les rapporteures rappellent que beaucoup de secteurs économiques utilisent les cookies pour proposer des contenus « gratuits », notamment culturels ou informatifs. L'incidence du nouveau régime des cookies serait dès lors très fortement néfaste pour les médias en ligne.

Par ailleurs, la centralisation des décisions de consentement ou de rejet au niveau des navigateurs web risquerait d'avantager indument les grandes plateformes américaines, qui exploitent les principaux navigateurs.

Enfin, **un point de vigilance majeur est à souligner sous l'effet du déplacement proposé des règles en la matière, de la directive e-Privacy[1] vers le RGPD**, en matière de sanction des manquements aux règles applicables aux cookies. Un tel déplacement créerait un double régime juridique pour ces traceurs (les traceurs adossés à des données à caractère personnel seraient soumis au RGPD, les autres, à la directive e-Privacy). Or, comme l'a rappelé la Cnil lors de son audition du 28 avril 2026, le RGPD et la directive e-Privacy relèvent de logiques très distinctes. Le RGDP prévoit un mécanisme de guichet unique dans le lieu d'établissement principal du responsable de traitement (souvent l'Irlande ou les Pays-Bas s'agissant des grandes plateformes américaines). Quant à elle, la directive e-Privacy prévoit que chaque autorité nationale est compétente pour sanctionner les manquements sur son propre sol. Par conséquent, le nouveau régime pourrait conduire à rendre compétentes dans les faits presque uniquement les autorités nationales irlandaise et néerlandaise. Cette situation réduirait l'effectivité des recours, face au risque d'embolie de ces autorités qui centraliseraient la quasi-totalité des plaintes.

La directive e-Privacy et le RGPD

Le règlement général sur la protection des données (RGPD), entré en vigueur en 2018, et la directive e-Privacy, en application depuis 2002, sont deux textes européens majeurs dans le domaine de la confidentialité et de la protection des données personnelles.

Ils présentent toutefois des différences en matière de champs et de modalités d'application.

S'agissant d'une directive, e-Privacy fixe des objectifs aux États membres en matière de protection de la vie privée sur Internet. Elle s'applique notamment aux traceurs (*cookies*) et à l'envoi de communications à des fins commerciales ou de *marketing*.

À la différence de la directive e-Privacy qui concerne la communication électronique même si elle concerne des données non personnelles, le RGPD réglemente strictement la protection des données à caractère personnel et définit les règles en la matière dans toute l'Union européenne.

[1] *Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).*

En complément, cette mesure créerait un manque à gagner important pour les finances publiques françaises. Le produit des amendes issues de ce champ régulatoire s'élèverait ainsi pour la France à près d'un milliard d'euros depuis 2020, pour une cinquantaine de sanctions décidées dans cette période. Sur ce montant, la Cnil estime que – si le système envisagé dans l'omnibus numérique s'était appliqué – la France aurait connu un manque à gagner de l'ordre 90 %, soit près de 900 millions d'euros en moins.

Les rapporteures invitent donc le Gouvernement à continuer de défendre une position ferme de suppression de cette proposition, tout en soulignant que lassitude du consentement doit être effectivement prise en compte et soulagée à brève échéance, au bénéfice des citoyens européens.

d) Des révisions du RGPD trop substantielles et trop risquées

Le dernier volet du « règlement omnibus numérique » porte sur des révisions décrites comme « ciblées » du règlement général sur la protection des données (RGPD).

Face à la marchandisation croissante et aux risques inhérents à la manipulation des données, sous l'influence de la législation pionnière de la France dite « Informatique et libertés » du 6 janvier 1978, l'Union européenne avait reconnu les droits d'une personne à garder la maîtrise de ses données en adoptant en 2016 **le règlement général sur la protection des données (RGPD)**[1].

Un temps critiqué par le secteur privé comme un frein à l'innovation, ce texte est devenu **un étalon-or mondial** de la protection des données personnelles au niveau international. Il est **d'autant plus protecteur pour les citoyens européens que sa portée est extraterritoriale**. À la différence d'autres textes européens, il est marqué par une cohérence interne forte entre les principes qu'il pose et les droits et les limites qu'il établit.

Comme le souligne la Commission européenne dans son document de travail sur l'omnibus : « *Les parties prenantes partagent globalement l'avis que le RGPD représente un cadre juridique équilibré et solide en matière de protection des données personnelles* [2] ». Cependant, **certaines modifications qu'elle se propose d'y apporter sont jugées par de nombreux acteurs comme entrainant une réduction effective de la protection offerte actuellement par le RGPD** (notamment dans l'IA, le marketing programmatique, la recherche privée) voire vectrices d'instabilité juridique. Les conséquences seraient

[1] *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*

[2] *Traduction libre du document de travail pour les services, accompagnant les propositions de règlements de l'omnibus numérique, publié exclusivement en anglais par la Commission européenne, le 19 novembre 2025.*

l'affaiblissement du RGPD comme standard international et l'introduction d'incertitudes juridiques.

Il demeure que certaines modifications proposées sont jugées favorablement, y compris par les professionnels du secteur de la protection des données. Ainsi, l'association Française des Correspondants à la Protection des Données (AFCDP), auditionnée le 16 avril 2026, a présenté les résultats d'une enquête réalisée par le CEDPO (*Confederation of European Data Protection Organisations*), sur l'Omnibus numérique, à laquelle ont répondu 672 professionnels de la protection des données dans les 27 États membres de l'UE. De manière générale, les professionnels de la protection des données accueillent ainsi favorablement la création de méthodologies et modèles communs pour les analyses d'impact pour la protection des données (AIPD), lesquels ne sont actuellement pas harmonisés au niveau européen, ce qui crée des incohérences pour les organismes installés dans plusieurs États membres.

Sur ce point, les rapporteures soulignent toutefois que la Commission européenne demande à se faire attribuer le droit de prendre des actes d'exécution relativement aux documents harmonisés d'AIPD. Or, comme pour d'autres points où la Commission européenne se propose de prendre des actes d'exécution, il apparaît que les autorités européennes sectorielles compétentes, plus proches du terrain, sont plus à même pour proposer des normes d'exécution. En matière d'AIPD, il en va ainsi des autorités de protection des données, réunies au niveau européen, avec le comité européen de la protection des données (CEPD) et le Contrôleur européen de la protection des données (EDPS).

De même, l'allongement du délai de notification des alertes de sécurité par les délégués à la protection des données aux autorités nationales compétentes (de 72 heures à 96 heures) est perçu favorablement ; il apparaît de nature à permettre aux délégués à la protection des données de parer à l'urgence de sécurité puis de remplir dans des délais raisonnables leurs obligations de notification. Entendue par les rapporteures le 28 avril 2026, la Cnil partage également cette analyse favorable sur ce point.

En revanche, plusieurs amendements au RGPD semblent loin d'être anodins ; ils sont assez peu « ciblés » et leurs conséquences potentiellement très dangereuses pour la protection des données sensibles.

Ainsi, outre l'ajout de diverses définitions d'ordre technique (par exemple, pour les termes « équipement terminal »), la Commission européenne entend proposer des **modifications importantes de certaines définitions, notamment la définition canonique de « données à caractère personnel »** (article 4, point 1 du RGPD), mais aussi celle de « recherche scientifique », élargie à toute recherche soutenant l'innovation, y compris à un intérêt commercial.

Des dérogations supplémentaires au traitement portant sur des catégories particulières de données à caractère personnel – c'est-à-dire les données « sensibles » (telles les données biométriques, les données de santé, les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, etc.) – seraient par ailleurs ajoutées au RGPD :

- une exception pour l'entraînement et le développement de l'IA, en permettant le recours à la base légale de l'intérêt légitime (article 88 e), d'une part ;

- un assouplissement concernant l'utilisation des données biométriques concernant la vérification d'identité, sous conditions.

En contrepoint, à l'issue des auditions, les rapporteures estiment que la proposition de la Commission européenne **aurait pu aller plus loin dans l'encadrement du droit d'accès, dans les cas de demandes manifestement infondées ou excessives**, notamment lorsque la demande porte sur un volume important de données. En effet, le droit d'accès est de plus en plus détourné de sa vocation première de protection des données personnelles, en décalage avec l'intention du législateur européen rappelée au considérant 63 du RGPD, lequel suggère que les personnes concernées doivent pouvoir accéder à leurs données à titre d'information, pour vérifier la licéïté du traitement et la nature des données qui les concernent.

Ainsi, entendu par les rapporteures, l'AFCDP indique que, dans le cadre de démarches administratives, le droit d'accès est détourné à des fins autres que la protection des données, par exemple pour modifier ou corriger incidemment un dossier administratif, voire pour contourner les délais ou retirer des informations désavantageuses.

Dans une contribution écrite qu'elle a transmise aux rapporteures, l'Association des grandes entreprises françaises (Afep) estime que le droit d'accès – préoccupation importante pour les grandes entreprises françaises – doit être fortement encadré, dans les situations litigieuses, par exemple dans le cas de litiges entre un employé et un employeur. De même, l'Afep souligne qu'il aurait été utile d'amender cette disposition pour indiquer que le droit d'accès ne peut porter que sur des données personnelles et non sur des documents dans leur intégralité.

2. Face aux risques potentiels pour la protection des droits et libertés numériques, les rapporteures appellent à la plus grande précaution dans la modification du RGPD

En ligne avec l'objectif affiché par la Commission européenne, les rapporteures considèrent que **toute modification du RGPD doit être strictement proportionnée et finement équilibrée** pour ne pas « *compromettre les objectifs politiques du RGPD, notamment le niveau élevé de protection des données*[1] » qu'il assure.

Ainsi que le souligne l'association Française des Correspondants à la Protection des Données (AFCDP), **si certaines propositions semblent acceptables individuellement, une fois cumulées, elles pourraient affaiblir le cadre du RGPD**. Ce cumul pourrait « vider le RGPD de sa substance » et affaiblir la place du RGPD comme standard international.

a) La modification de la définition de « données à caractère personnel » : une proposition contreproductive et dangereuse

Dans son document de travail pour les services en date du 19 novembre 2025, qui en l'absence de véritable analyse d'impact fait référence, la Commission européenne souligne que la conformité au RGPD implique à la fois des avantages et des coûts pour les entreprises, notamment les plus petites, et que « *des difficultés ont été identifiées, notamment en ce qui concerne l'interprétation et l'application cohérentes du RGPD par les autorités de contrôle. Les parties prenantes ont souligné la nécessité de renforcer la sécurité juridique en introduisant des mesures visant à réduire la fragmentation du droit et à améliorer l'application cohérente du RGPD*[2] ».

En particulier, la Commission européenne souhaite proposer « *une plus grande clarté sur certains aspects clés essentiels à l'interprétation du RGPD, tels que la définition des données personnelles à la lumière de la jurisprudence récente de la Cour de justice de l'Union européenne (CJUE), afin de garantir une compréhension commune et harmonisée de ce concept fondamental dans toute l'UE*[3] ».

---

[1] *Traduction libre du document de travail pour les services, accompagnant les propositions de règlements de l'omnibus numérique, publié exclusivement en anglais par la Commission européenne, le 19 novembre 2025.*

[2] *Traduction libre du document de travail pour les services, accompagnant les propositions de règlements de l'omnibus numérique, publié exclusivement en anglais par la Commission européenne, le 19 novembre 2025.*

[3] *Ibid.*

La Commission européenne propose donc de « codifier » les arrêts Breyer (CJUE, 19 octobre 2016, C-582/14) et EDPS c/ SRB (CJUE, 4 septembre 2025, C-413/23 P) sur l'approche relative de l'identifiabilité, dans l'idée de préciser la portée de la notion de « donnée à caractère personnel » dans le contexte d'un transfert de **données pseudonymisées** à des tiers. La proposition introduit ainsi une **modification de l'article 4, point 1, du RGPD pour disposer que des informations relatives à une personne physique ne sont pas nécessairement des données personnelles pour toute entité, dès lors que cette entité ne dispose pas des moyens raisonnablement susceptibles d'identifier la personne**.

Quelle est la différence entre les données pseudonymisées et les données anonymisées ?

La pseudonymisation consiste à transformer des données personnelles afin qu'elles ne puissent plus être attribuées à une personne spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles visant à garantir que les données ne sont pas attribuées à des personnes physiques. Dans la pratique, il peut s'agir de remplacer les données personnelles (nom, prénom, numéro personnel, numéro de téléphone, etc.) par des données d'identification indirecte (alias ou pseudonyme, numéro séquentiel, etc.) dans un ensemble de données. Selon le cadre réglementaire en vigueur, les données pseudonymisées sont bien des données personnelles et sont soumises au RGPD.

A contrario, les données anonymisées sont des données qui ont été rendues anonymes, de telle sorte que l'individu n'est pas ou plus identifiable par tout moyen raisonnablement susceptible d'être utilisé. Comme le rappelle Comité européen de la protection des données (CEPD), lorsque l'anonymisation est correctement mise en œuvre, le RGPD ne s'applique plus aux données anonymisées.

Néanmoins, dans un communiqué de presse en date du 4 décembre 2025, **le Comité européen de la protection des données (CEDP) estime que la modification de la définition des données personnelles proposée par la Commission européenne « semble aller au-delà de la jurisprudence récente de la CJUE et d'une modification ciblée du RGPD »**.

Dans leur avis conjoint (n° 2/2026) sur la proposition de règlement omnibus numérique en date du 10 février 2026, le Comité européen de la protection des données (CEDP) et le Contrôleur européen de la protection des données (EDPS) considèrent la proposition de la Commission européenne comme une régression et porterait atteinte au droit fondamental à la protection des données.

Entendue le 28 avril 2026, la Cnil a indiqué rejoindre l'analyse très ferme du CEDP sur ce point.

En effet, la rédaction projetée crée une zone grise : un opérateur pourrait soutenir que, ne « visant » pas l'identification, les données qu'il traite ne relèvent pas du RGPD, alors même que des moyens techniques d'identification existent dans son système d'information ou dans son écosystème. **Il y a donc un risque réel de contournement des obligations par des acteurs déclarant ne pas « viser » l'identification des personnes**.

Cette proposition apparaît dès lors contreproductive. Elle est en effet contradictoire avec la logique objective et contextuelle que retenait la jurisprudence jusque-là : ce sont les moyens raisonnablement disponibles, non l'intention déclarée de l'opérateur de traitement des données, qui doivent fonder la qualification de données à caractère personnel.

L'effet serait amplifié par l'habilitation qui serait donnée à la Commission européenne de prendre des actes d'exécution pour spécifier les moyens et les critères permettant de déterminer si des données issues de la pseudonymisation constituent encore ou pas des données personnelles (nouvel article 41 *bis*). **Les rapporteures estiment ainsi que la combinaison des modifications proposées réduirait significativement le champ matériel du RGPD par voie réglementaire, sans contrôle effectif des législateurs européens et nationaux**.

En conséquence, à l'issue des auditions, notamment de la CNIL et de l'Association française des correspondants à la protection des données (AFCDP), **les rapporteures jugent que la modification proposée par la Commission européenne à la définition canonique du RGPD de « données à caractère personnel » est dangereuse**, pour plusieurs raisons :

- elle **conduirait à une réduction du champ d'application du RGPD** en proposant une définition négative (« ce qui n'est pas une donnée à caractère personnel », après pseudonymisation), risquant de « générer de nouvelles incertitudes juridiques », contrariant donc l'objectif affiché par la Commission européenne ;

- la **classification d'une donnée comme à caractère personnel ou non deviendrait incertaine** car elle dépendrait des capacités techniques du destinataire à identifier une personne, créant une fragmentation de l'interprétation. Elle reposerait donc sur une interprétation subjective ;

- la **perte du caractère personnel d'une donnée pseudonymisée est potentiellement réversible**. En effet, une donnée pseudonymisée peut ne pas permettre l'identification d'une personne à un instant donné, mais le permettre ultérieurement au moyen de recoupement de jeux de données devenus entre temps disponibles. En outre, une entité qui n'a pas les moyens d'identifier une personne est susceptible de transférer les données pseudonymisées (qui ne bénéficient plus d'aucune protection particulière puisqu'elles ne sont plus des données à caractère personnel) à une entité qui, elle, détient ces moyens ;

- elle serait **partiellement en contradiction avec la jurisprudence de la CJUE** qui rappelle que des données anonymes pour une entité peuvent devenir personnelles si un destinataire ultérieur dispose des moyens de réidentification. Or, en affirmant que la transmission à une tierce partie ne rend pas les données personnelles pour l'entité initiale, la proposition de la Commission européenne ne semble pas tenir compte de ce principe.

Ainsi que le résume l'Association française des correspondants à la protection des données (AFCDP) : « *En basant la définition sur les moyens qu'un acteur peut ''raisonnablement'' utiliser, la proposition ouvre la porte à ce que des organisations classent des données identifiables comme « non personnelles » au motif qu'elles (ou leurs destinataires) n'ont pas l'intention ou les capacités techniques immédiates de viser l'identification. Il est craint que les données ne finissent par être considérées comme non personnelles par défaut, affaiblissant ainsi toute la chaîne de responsabilité et laissant circuler des données personnelles (même sensibles) sans supervision légale adéquate* ».

En somme, les rapporteures estiment que cette modification nuirait aux droits fondamentaux eu égard à la protection des données personnelles des citoyens français et européens, sans pour autant apporter de clarté juridique pour les entreprises et responsables de traitement. Au contraire, elles considèrent comme non nul le risque d'exploitation de cette flexibilité pour contourner le RGPD par des acteurs mal intentionnés.

Les rapporteures invitent le Gouvernement français à continuer de tenir fermement la position de suppression de la modification de la définition de données à caractère personnel, laquelle est majoritaire au sein du Conseil européen. En outre, les rapporteures jugent préférable de rechercher une clarification de cette définition par des lignes directrices (en cours d'élaboration), plutôt qu'une révision de la réglementation européenne.

En complément, les rapporteures soulignent que la disposition visant à permettre à la Commission européenne de prendre des actes d'exécution relativement aux critères de définition des données pseudonymisées, ne leur apparaît pas justifiée. Là encore, elles **appellent la Commission européenne à davantage de mesure et à en référer aux autorités européennes et nationales compétentes, plutôt que de viser une démarche centralisatrice qui présente des limites.**

Ces réserves semblent partagées par le Conseil de l'UE, qui dans son deuxième compromis sur le volet « RGPD », en date du 15 avril 2026, a proposé d'amender le projet de la Commission européenne sur la question de la pseudonymisation, afin de détailler que « les données à caractère personnel ayant fait l'objet d'une pseudonymisation, qui pourraient être attribuées à une personne physique grâce à l'utilisation d'informations supplémentaires, doivent être considérées comme des informations relatives à une personne physique identifiable ». En outre, le Conseil souhaite que le CEDP puisse rendre un avis au plus tard douze mois après l'entrée en vigueur du règlement, portant sur « l'application de la pseudonymisation et de

l'anonymisation, y compris les mesures techniques et organisationnelles connexes, et précisant les moyens et les critères permettant de **déterminer si l'application de la pseudonymisation aux données à caractère personnel est de nature à empêcher efficacement des personnes autres que le responsable du traitement d'identifier une personne concernée, de telle sorte que, pour ces personnes, la personne concernée ne soit pas ou ne soit plus identifiable »**.

b) Une modification hasardeuse de la définition de recherche scientifique pour y inclure toute recherche soutenant l'innovation, y compris dans un intérêt commercial

Dans ses lignes directrices 03/2020 sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19, le Comité européen de la protection des données (EDPB) rappelle que l'article 4 actuel du RGPD ne contient pas de définition explicite du « traitement à des fins de recherche scientifique » et que le considérant 159 indique que « le traitement de données à caractère personnel à des fins de recherche scientifique devrait être interprété au sens large et couvrir, par exemple, le développement et la démonstration de technologies, la recherche fondamentale, la recherche appliquée et la recherche financée par le secteur privé ». Néanmoins, il suggère des difficultés d'application liée à l'imprécision de cette définition.

Dès lors, une définition harmonisée de la « recherche scientifique » apparaît bienvenue. Selon la proposition de la Commission européenne, **la définition de « recherche scientifique » serait élargie à toute recherche menée pour générer de nouvelles connaissance ou soutenant l'innovation, y compris la recherche privée**. Elle pourrait donc dès lors englober des activités essentiellement commerciales présentées comme de la R&D. Une telle définition est souhaitée par les grandes entreprises, car elle est favorable à l'innovation, comme le souligne l'Association des grandes entreprises françaises (Afep), dans la contribution écrite qu'elle a transmise aux rapporteures le 27 avril 2026.

Or, comme le rapporte l'Association française des correspondants à la protection des données (AFCDP) dans le cadre de son audition, l'élargissement de la notion de « recherche scientifique » pour préciser qu'elle peut poursuivre un intérêt commercial associé à la proposition de considérer la réutilisation de données pour la recherche comme automatiquement compatible avec la finalité initiale est perçue par certains délégués à la protection des données, comme une atteinte aux principes fondamentaux du RGPD, et notamment en raison du caractère automatique de cette autorisation. Selon l'AFCDP, **il est à craindre que l'inclusion de l'intérêt commercial ne serve de « prétexte » à certaines entreprises pour contourner les garde-fous posés par l'article 9 du RGPD**. Pour les données de santé ou biométriques, la réutilisation de ces données sans évaluation de compatibilité au cas par cas

peut mener à des risques élevés de stigmatisation, de profilage ou d'inférences.

Ainsi, des professionnels de la protection des données recommandent de **maintenir un test approfondi de compatibilité des finalités**. Selon l'AFCDP, ces mesures, couplées à la réduction de l'obligation d'information des personnes dans le contexte de la recherche scientifique aboutissent à une atteinte directe au principe de transparence et sont perçues comme venant limiter les possibilités de contrôle des individus sur leurs propres données, notamment lorsque la recherche scientifique a un but commercial.

Conjuguée aux assouplissements de certains traitements à cette fin, **l'élargissement de l'acception de la « recherche scientifique » soulève un risque potentiel pour la protection de certaines données sensibles**. Le **risque pour les données de santé est ainsi particulièrement aigu** : un acteur privé pourrait invoquer la qualification de « recherche scientifique » pour justifier le traitement de ces données dans un cadre purement marchand. La présomption de compatibilité avec la finalité initiale (article 5, paragraphe 1, point b), modifié) accentue ce risque.

Dans son deuxième compromis sur le volet « données » en date du 15 avril 2026, le Conseil a à ce stade rejeté l'inclusion de la recherche avec des « intérêts commerciaux » du champ de la « recherche scientifique ».

Eu égard aux risques pour la protection des données sensibles, notamment les données de santé, les rapporteures rejoignent la position portée par le Conseil de ne pas étendre de manière trop large la définition de « recherche scientifique » au risque d'y inclure des activités de R&D menées à des fins purement marchandes.

Si la promotion de la recherche est un objectif important pour l'UE et que l'utilisation de l'IA et des jeux de données européens notamment de santé ouvrent des perspectives prometteuses pour l'amélioration des diagnostics cliniques[1], l'automaticité de la compatibilité du traitement de données sensibles aux fins de recherche interroge les rapporteures. Elles considèrent ainsi que la compatibilité des traitements ultérieurs avec la finalité initiale doit demeurer réfragable et subordonnée à des garanties concrètes en matière de sécurité des données et de mode de gouvernance. Il apparaît dès lors que **des garanties supplémentaires sont nécessaires pour assurer le caractère véritablement « scientifique » du traitement** de données et garantir un certain niveau de standard éthiques, à travers des modalités pratiques à définir. À titre d'exemple, pour les traitements à grande échelle de données de santé à des fins de recherches, une autorisation préalable des traitements par un comité d'experts indépendant pourrait être souhaitable.

[1] *Des applications récentes sont à noter pour la détection précoce de la septicémie ou l'amélioration de la détection de certains cancers.*

Comme le suggère la Cnil, les rapporteures **plaident pour l'ajout des notions de vérifiabilité, de transparence et d'objectifs de la recherche scientifique à la définition**, afin de veiller au caractère véritablement scientifique des recherches ainsi couvertes par le règlement sur l'IA et des assouplissements induits.

c) Des nouvelles dérogations au traitement sur des catégories particulières de données sensibles qui ouvrent des privilèges à l'IA, sans garanties suffisantes

Deux **dérogations supplémentaires au traitement portant sur des catégories particulières de données à caractère personnel** – c'est-à-dire les données « sensibles » (ex : données biométriques, données de santé, données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, etc.) – seraient ajoutées au RGPD :

- une exception **pour l'entraînement et le développement de l'IA** (Article 3, paragraphe 2), sous certaines conditions. Serait ainsi autorisé le traitement résiduel par les systèmes d'IA de telles données : si celles-ci sont présentes de manière accidentelle ou résiduelle dans les jeux de données malgré les mesures techniques et organisationnelles prises pour l'éviter, et si leur suppression est impossible ou exige des efforts disproportionnés, elles devront être protégées pour éviter un usage abusif (par exemple, via du chiffrement). Cette dérogation ne s'applique pas si le traitement de ces données est nécessaire à la finalité de principe (par exemple, relativement à un système d'IA conçu pour analyser des données de santé) ;

- une **clarification concernant les données biométriques** : si leur utilisation reste soumise à des restrictions très strictes en matière d'identification des personnes, une dérogation est proposée concernant le traitement des données biométriques pour la vérification d'identité, sous deux conditions : 1) la personne concernée a le contrôle exclusif du processus (par exemple, s'agissant de données stockées uniquement sur son appareil personnel) et 2) des garanties appropriées sont prises pour éviter les abus.

Dans le cadre des discussions interinstitutionnelles en cours, ces propositions sont à ce stade refusées par le Conseil de l'UE. Dans son deuxième compromis sur le volet « données » en date du 15 avril 2026, le Conseil a écarté l'ajout d'un nouvel article 88 c dans le RGPD, qui autoriserait l'utilisation des données à caractère personnel pour l'entrainement des modèles d'IA dans le cas d'un « intérêt légitime » ; cet ajout apparaît effectivement superfétatoire, un tel traitement étant déjà possible (voir points 39 à 45 de l'avis 2/2026 du comité européen de la protection des données et du Contrôleur européen de la protection des données sur la proposition de règlement omnibus numérique[1]).

[1] *Dans son avis 28/2024 du 17 décembre 2024 sur les modèles d'IA, le Contrôleur européen de la protection des données (EDPS) a ainsi déjà confirmé que l'intérêt légitime pouvait être utilisé, dans*

En complément, la proposition de règlement de la Commission européenne entend assouplir les conditions du traitement de données sensibles aux fins de recherche scientifique. Outre la clarification de la définition de « recherche scientifique » (cf. supra), les modifications suivantes sont proposées :

- le **traitement ultérieur** de données à des fins scientifiques est considéré comme **licite** s'il est compatible avec la finalité initiale de la collecte ;

- la **recherche scientifique est reconnue comme un intérêt légitime** au sens de l'article 6(1)f du RGPD, à condition que 1) les droits des personnes concernées soient protégés et 2) les données utilisées soient uniquement celle strictement nécessaires à la recherche ;

- des **exceptions sont apportées à l'obligation d'information individuelle des personnes concernées**, si cette information est impossible ou disproportionnées, à condition de rendre les informations publiquement disponibles.

En somme, les possibilités pour les responsables de traitement d'utiliser des données sensibles sont étendues **à différents motifs** (intérêt légitime, aux fins de recherche, y compris à des fins commerciales, entrainement d'IA, détection et correction des biais algorithmiques, y compris discriminatoires des IA).

Or, dans les faits, les responsables de traitement sont seuls responsables de l'analyse du bien-fondé et de la légalité des traitements de données qu'ils entendent opérer. Ainsi, en élargissant les possibilités de traitement, on risque donc un effet de bord possible consistant à élargir également les mésusages de données sensibles, soit en raison d'une erreur de jugement, soit par des responsables de traitement négligeant ou malintentionnés.

*

Les rapporteures considèrent en somme que **les modifications proposées au RGPD sont loin d'être cosmétiques ou mineures** et appellent donc le gouvernement français à la plus grande vigilance sur ce sujet. Il s'agit en effet de veiller à ce que l'équilibre protecteur du RGPD, reconnu internationalement, ne soit pas remis en cause.

En outre, en permettant à l'IA de traiter sans garanties suffisantes des données sensibles, les rapporteures considèrent qu'on ouvre la porte à des traitements potentiellement contraires aux valeurs européennes.

---

certains cas, comme base légale pour le développement et l'entrainement des modèles ou systèmes d'IA. L'ajout de cette base légale dans le règlement sur l'IA est donc jugé superfétatoire, d'autant que la rédaction (« peut »*) n'apporte aucune clarification comparativement à l'avis 28/2024.*

Enfin, **les rapporteures appellent l'Union européenne à avoir l'ambition de faire du règlement sur l'IA un standard international de régulation de l'IA, sur le modèle du RGPD, qui en huit ans, est devenu un étalon-or mondial en matière de protection des données.**

*

La proposition de résolution européenne qui suit présente ainsi les observations de la commission des affaires européennes sur le volet IA, ainsi que les principales orientations et point de vigilance qu'elle souhaite soumettre au Gouvernement dans le cadre des négociations en cours et à venir sur le volet « données », notamment relativement aux évolutions proposées du RGPD.

PROPOSITION DE RÉSOLUTION EUROPÉENNE SUR LA PROPOSITION DE RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL MODIFIANT LES RÈGLEMENTS (UE) 2024/1689 ET (UE) 2018/1139 EN CE QUI CONCERNE LA SIMPLIFICATION DE LA MISE EN ŒUVRE DES RÈGLES HARMONISÉES CONCERNANT L'INTELLIGENCE ARTIFICIELLE - COM(2025) 836 FINAL ET SUR LA PROPOSITION DE RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL MODIFIANT LES RÈGLEMENTS (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 ET (UE) 2023/2854 AINSI QUE LES DIRECTIVES 2002/58/CE, (UE) 2022/2555 ET (UE) 2022/2557 EN CE QUI CONCERNE LA SIMPLIFICATION DU CADRE LÉGISLATIF NUMÉRIQUE, ET ABROGEANT LES RÈGLEMENTS (UE) 2018/1807, (UE) 2019/1150 ET (UE) 2022/868 AINSI QUE LA DIRECTIVE (UE) 2019/1024 (RÈGLEMENT OMNIBUS NUMÉRIQUE) - COM(2025) 837 FINAL

(1) Le Sénat,

(2) Vu l'article 88-4 de la Constitution,

(3) Vu le traité sur le fonctionnement de l'Union européenne, notamment son article 114,

(4) Vu la charte des droits fondamentaux de l'Union européenne,

(5) Vu la convention de sauvegarde des droits de l'homme et des libertés fondamentales,

(6) Vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), dit « RGPD »,

(7) Vu le livre blanc du 19 février 2020 intitulé « Intelligence artificielle. Une approche européenne axée sur l'excellence et la confiance », COM(2020) 65,

(8) Vu le rapport de Mario Draghi du 9 septembre 2024 sur le futur de la compétitivité européenne,

(9) Vu la stratégie de la Commission européenne pour l'Union des données du 19 novembre 2025, COM(2025) 835 final,

(10) Vu le plan d'action pour le continent de l'IA, présenté par la Commission européenne le 9 avril 2025, COM(2025) 165,

(11) Vu la proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 et (UE) 2023/2854 ainsi que les directives 2002/58/CE, (UE) 2022/2555 et (UE) 2022/2557 en ce qui concerne la simplification du cadre législatif numérique, et abrogeant les règlements (UE) 2018/1807, (UE) 2019/1150 et (UE) 2022/868 ainsi que la directive (UE) 2019/1024,

(12) Vu la proposition de règlement du Parlement européen et du Conseil modifiant les règlements (UE) 2024/1689 et (UE) 2018/1139 en ce qui concerne la simplification de la mise en œuvre des règles harmonisées concernant l'intelligence artificielle,

(13) Vu la proposition de règlement du Parlement européen et du Conseil relatif à la création de portefeuilles européens d'identité numérique pour les entreprises, COM(2025) 838 final,

(14) Vu l'avis conjoint (n° 2/2026) du Comité européen de la protection des données (CEDP) et du Contrôleur européen de la protection des données (EDPS) sur la proposition de règlement omnibus numérique, du 10 février 2026,

(15) Vu le rapport d'Arthur Mensch, Mistral AI, « European AI: A playbook to own it », d'avril 2026,

(16) Vu le rapport « Pour un déploiement de l'intelligence artificielle conforme aux valeurs européennes », n° 483 (2022-2023) de M. André GATTOLIN, Mme Catherine MORIN-DESAILLY, M. Cyril PELLEVAT et Mme Elsa SCHALK au nom de la commission des affaires européennes, ainsi que la résolution européenne n° 100 (2022-2023),

(17) Vu le rapport n° 444 (2024-2025) de Mmes Catherine MORIN-DESAILLY et Florence BLATRIX CONTAT, déposé le 13 mars 2025, ainsi que la résolution n° 106 (2024-2025) visant à l'application stricte du cadre réglementaire numérique de l'Union européenne et appelant au renforcement des conditions d'une réelle souveraineté numérique européenne, devenue résolution du Sénat le 18 avril 2025,

(18) Vu le rapport d'information du Sénat n° 279 (2018-2019) de MM. André GATTOLIN, Claude KERN, Cyril PELLEVAT et Pierre OUZOULIAS, fait au nom de la commission des affaires européennes, intitulé « Intelligence artificielle : l'urgence d'une ambition européenne », déposé le 31 janvier 2019,

(19) Vu le rapport d'information du Sénat n° 627 (2021-2022) de MM. Marc-Philippe DAUBRESSE, Arnaud de BELENET et Jérôme DURAIN, fait au nom de la commission des lois, intitulé « La reconnaissance biométrique dans l'espace public : 30 propositions pour écarter le risque d'une société de surveillance », déposé le 10 mai 2022,

(20) Vu le rapport « L'Europe, colonie du monde numérique ? » n° 443 (2011-2012) de Mme Catherine MORIN-DESAILLY au nom de la commission des affaires européennes,

(21) Vu le rapport d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet » n° 696 (2013-2014) de Mme Catherine MORIN-DESAILLY, au nom de la mission commune d'information du Sénat sur la gouvernance de l'Internet, ainsi que la résolution européenne n°122 (2014-2015),

(22) Vu les conclusions du rapport du Sénat n° 7 (2019-2020) du 1er octobre 2019, intitulé « Le devoir de souveraineté numérique : ni résignation, ni naïveté », fait au nom de la commission d'enquête sur la souveraineté numérique,

(23) Vu la proposition de loi n° 220 (2025-2026) relative à l'instauration d'une présomption d'utilisation des contenus culturels par les fournisseurs d'intelligence artificielle, adoptée par le Sénat le 8 avril 2026,

(24) Considérant la centralité des technologies numériques dans nos société sur les plans socio-économiques, sociétaux et environnementaux ;

(25) Considérant la place grandissante des technologies d'intelligence artificielle (IA) et les opportunités comme les risques que soulèvent ces technologies pour nos sociétés et nos économies et notamment pour la compétitivité des entreprises européennes, mais aussi pour l'efficacité des services publics, la sécurité et le bien-être de nos sociétés ;

(26) Considérant que ce processus de diffusion de l'IA ne doit en aucun cas amoindrir la protection des droits fondamentaux, y compris le haut niveau de protection des données à caractère personnel dont les Européens jouissent actuellement, et que ces technologies doivent être au service des personnes et soumises aux valeurs, principes et droits fondamentaux de l'Union européenne ;

(27) Considérant les risques que posent les technologies d'intelligence artificielle pour le respect la dignité et de la personne humaine, pour le respect de la vie privée et la protection des données à caractère personnel, la sécurité des données et la non-discrimination au regard au regard du genre, de l'origine ethnique, de l'âge, de la religion, mais aussi du statut économique ;

(28) Considérant que pour que l'Europe puisse tirer pleinement parti des potentialités économiques et sociétales de l'IA, il est nécessaire d'assurer une meilleure sécurité juridique, ce qui passe par l'élaboration de règles claires, précises, compréhensibles par tous et suffisamment stable dans le temps ;

(29) Considérant le risque élevé de capture du régulateur auquel sont confrontés les institutions publiques nationales et européennes dans le secteur numérique et en particulier l'IA, au vu de la complexité et du rythme des évolutions techniques et des asymétries d'informations entre ces acteurs publics et les acteurs privés, notamment les grandes plateformes extra-européennes ;

(30) Considérant les risques hybrides et systémiques que l'IA tend à créer pour les États membres dans un contexte géopolitique mouvant ;

(31) Sur le principe de l'omnibus :

(32) Appelle l'Union européenne à ne pas trembler ni transiger dans l'application de l'arsenal juridique novateur et ambitieux qu'elle a commencé à construire pour encadrer l'IA et le secteur numérique ;

(33) Accueille favorablement la volonté de la Commission européenne de simplifier le cadre applicable et de réduire la charge administrative et les coûts de conformité, notamment pour les petites et moyennes entreprises (PME) et les petites entreprises à moyenne capitalisation (PEMC), en vue d'améliorer leur compétitivité ;

(34) Se réjouit des mesures techniques destinées à améliorer la coordination des différentes normes européennes dans le secteur numérique, aux fins de clarté et de sécurité juridique ;

(35) Déplore que la proposition dépasse pour partie le seul objectif de simplification, tendant à complexifier un cadre régulatoire déjà complexe et dense, au risque de nuire à sa clarté et à son acceptation par les entreprises et les citoyens ;

(36) Regrette l'absence d'étude d'impact, ce qui nuit à la bonne compréhension des propositions formulées par la Commission européenne et de leur insertion dans le droit de l'Union européenne ;

(37) Souligne que les évolutions de la régulation en matière numérique ne doivent pas être menées avec une précipitation excessive, au risque d'être dictées par l'industrie numérique ;

(38) Regrette le calendrier très resserré des négociations du volet sur l'IA, qui n'a pas permis la pleine association de toutes les parties prenantes et des États membres ;

(39) Regrette l'absence de clarification du régime juridique du droit d'auteur en matière d'IA, alors que les juridictions commencent à se prononcer sur des cas d'espèce et que des solutions juridiques ont été identifiées pour veiller à la rémunération des contenus culturels utilisés par les systèmes d'IA, en particulier la proposition de loi relative à l'instauration d'une présomption d'utilisation des contenus culturels par les fournisseurs d'intelligence artificielle, adoptée par le Sénat le 8 avril 2026 ;

(40) Déplore que le train de mesures omnibus numérique sur l'IA n'ait pas été l'occasion d'assurer une meilleure prise en compte de l'empreinte environnementale de l'IA, notamment eu égard à l'utilisation importante qu'elle entraine en termes d'eau et de matière premières ;

(41) Invite la Commission européenne à envisager d'assortir les obligations déclaratives existantes en matière de consommation énergétique d'obligations en termes d'objectifs de réduction de ces consommations, ainsi qu'à envisager de futures obligations déclaratives en matière environnementale pour l'ensemble du cycle de vie des systèmes d'IA applicable aux grands fournisseurs d'IA ;

(42) Sur le report des obligations faites à certains systèmes d'IA :

(43) Prend acte du report des obligations faites à certains systèmes d'IA à haut risque décidé lors du trilogue du 7 mai 2026, estimant qu'un report à date fixe va dans le sens d'une meilleure sécurité juridique et d'une prévisibilité renforcée pour les entreprises du secteur ;

(44) Regrettent que ce report ait été étendu aux obligations de transparence figurant à l'article 50 du règlement sur l'IA, repoussant de six mois le marquage des contenus générés par l'IA, au détriment des bénéfices attendus par cette mesure tant du point de vue de la protection du droit d'auteur que pour la transparence vis-à-vis des utilisateurs d'IA ;

(45) Juge cependant ce report révélateur tant de la difficulté à réguler et réglementer un secteur technique aux évolutions si rapides, que des limites du processus décisionnel européen pour allier agilité et stabilité des normes ;

(46) Sur les efforts de simplification du cadre règlementaire de l'IA :

(47) Salue les efforts de simplification des obligations administratives pour les petites et moyennes entreprises (PME) et les petites entreprises à moyenne capitalisation (PEMC) du secteur de l'IA ;

(48) Regrette l'insuffisante simplification de l'articulation entre les exigences en matière de cybersécurité pour les fournisseurs de services d'IA, portées par le règlement sur l'IA et celles issues du cadre existant, notamment le règlement sur la cyberrésilience ;

(49) Sur l'élargissement des usages interdits de l'IA :

(50) Soutient la proposition d'interdiction des systèmes d'IA capables de générer, manipuler ou reproduire des contenus représentant les parties intimes ou des activités sexuellement explicites d'une personne, sans son consentement (« nudification ») ;

(51) Regrette que l'interdiction des systèmes d'IA capables de générer, manipuler ou reproduire des contenus (image, vidéo, audio) pédopornographiques n'ait pas abouti ;

(52) Souhaite de façon générale l'interdiction de toute pratique en matière d'intelligence artificielle susceptible d'exploiter les éventuelles vulnérabilités économiques, personnelles ou sociales d'une personne ou d'un groupe de personnes donné, de manière à causer ou étant susceptible de cause un préjudice à cette personne, à ce groupe ou à un tiers, et notamment de toute pratiques en matière d'IA de nature à porter atteinte à la dignité de la personne humaine ;

(53) Estime que doit être renforcée l'éducation et la formation continue au numérique et à l'IA en vue d'améliorer la littératie des citoyens européens en la matière, y compris la connaissance de leurs droits et libertés et des voies de recours en cas d'abus ;

(54) Sur les bacs à sable réglementaires en matière d'IA :

(55) Prend acte de la mise en place de bacs à sable réglementaires, y compris transfrontaliers, afin d'encourager l'innovation européenne et de favoriser le passage à l'échelle des startups européennes de l'IA ;

(56) Appelle à la vigilance concernant les essais en conditions réelles pour les systèmes d'IA à haut risque dans certains secteurs critiques (santé, industries critiques, …) ;

(57) Estime particulièrement souhaitable que les autorités nationales de protection des données à caractère personnel soient systématiquement impliquées dans le fonctionnement desdits bacs à sable, notamment dans ces secteurs critiques, y compris concernant le bac à sable transfrontalier ;

(58) Sur la gouvernance et le contrôle du respect du cadre normatif de l'IA :

(59) Rappelle qu'une répartition équilibrée des prérogatives entre la Commission européenne et les autorités nationales de contrôle constitue un prérequis indispensable à une régulation efficace du secteur numérique et de l'IA ;

(60) Appelle la Commission européenne à renforcer son Bureau de l'IA aux seules fins d'amélioration des capacités d'expertise et d'anticipation des évolutions du secteur, en rendant possible le recrutement d'experts techniques et juridiques, sans pour autant nuire aux capacités nationales ;

(61) Estime ainsi que le Bureau de l'IA ne doit pas supplanter les prérogatives des États membres et de leurs agences nationales de supervision dans leurs champs de compétences respectifs et que, de manière générale, toute expérimentation en matière d'IA doit être placée sous le contrôle d'agences indépendantes de la Commission européenne ;

(62) Considère que le renforcement des compétences exclusives du Bureau de l'IA pour certains systèmes d'IA, notamment ceux basés sur un modèle d'IA à usage général, est contraire aux principes de subsidiarité et de proportionnalité, en privant les autorités nationales de surveillance de marché de la possibilité de se saisir, y compris dans les cas où le Bureau de l'IA n'a pas souhaité se saisir ;

(63) Considère donc que pour les systèmes d'IA concernés, une logique de dessaisissement, selon laquelle les autorités nationales seraient tenues de se dessaisir dès lors que le Bureau de l'IA souhaite opérer un contrôle dans les secteurs concernés, aurait été préférable et de surcroît favorable à une meilleure coordination entre agences nationales, tout en renforçant la gouvernance du Bureau de l'IA, pour les contrôles transfrontaliers ;

(64) Sur la modification de l'annexe I du règlement sur l'IA :

(65) Regrette le transfert du règlement sur les machines de la section A à la section B de l'annexe I du règlement sur l'IA, qui a pour effet de l'exclure du champ d'application du règlement sur l'IA, notant qu'en l'absence d'étude d'impact, il n'est pas possible d'apprécier utilement si ce règlement présente un niveau de garanties équivalent à celui du règlement sur l'IA pour les produits concernés embarquant de l'IA ;

(66) Souligne l'importance, notamment dans les secteurs critiques couverts par l'annexe I du règlement sur l'IA, de favoriser une approche de sécurité dès la conception ou « safety by design », qui soit conforme à l'esprit du règlement sur l'IA reposant sur une approche par niveau de risque ;

(67) Sur les mesures de simplification et de clarification portant sur les différents textes européens relatifs aux données :

(68) Salue l'effort de la Commission européenne visant à harmoniser et à améliorer la coordination des textes entre eux et de supprimer les redondances ;

(69) Soutient l'élargissement de la possibilité de s'opposer à la divulgation de données qui constituent un secret des affaires, lorsqu'il existe un risque élevé d'obtention ou d'utilisation illicites ou de divulgation illicite à des pays tiers, ou à des entités placées sous leur contrôle ;

(70) Sur la création d'un point d'entrée unique pour la déclaration des incidents cyber :

(71) S'oppose fermement à la proposition de la création d'un point d'entrée unique pour la déclaration des incidents de cybersécurité, eu égard au risque d'en faire un point de faille unique ;

(72) Doute de la capacité technique de l'ENISA à sécuriser ce point d'entrée unique de manière suffisante pour en assurer la résilience ;

(73) Considère la création d'un point d'entrée unique comme étant contraire aux principes de subsidiarité et de proportionnalité eu égard aux enjeux de sécurité nationale sous-jacents en matière d'incidents cyber et à l'importance stratégique pour les États membres de conserver le droit de filtrage dont ils disposent aujourd'hui pour partager ou non des informations sur les failles de cybersécurité d'infrastructures critiques nationales à l'échelon européen ;

(74) Sur le déplacement des règles en matière de cookies de la directive e-Privacy vers le RGPD :

(75) Considère que le déplacement des règles en matière de cookies de la directive e-Privacy vers le RGPD créerait un double régime dangereux pour le contrôle de ces cookies, sans répondre à l'enjeu de réduction de la fatigue du consentement aux traceurs ;

(76) Sur les amendements au règlement général sur la protection des données (RGPD) :

(77) Rappelle que l'objet du RGPD n'est pas en soi la protection des données, mais la protection des libertés et droits des personnes qui sont concernées par ces données ;

(78) Considère que les révisions proposées au RGPD sont trop substantielles et potentiellement dangereuses, eu égard à un texte devenu une référence mondiale en matière de protection des données à caractère personnel ;

(79) Accueille néanmoins favorablement les propositions d'harmonisation des cadres et documents relatifs aux analyses d'impact pour la protection des données (AIPD) ;

(80) Soutient la proposition d'allongement du délai de notification des incidents relatifs aux données personnelles de 72 heures à 96 heures, laissant davantage de temps aux délégués à la protection des données pour gérer l'urgence avant de remplir, dans des délais raisonnables leurs obligations de notification ;

(81) Estime que la modification de la définition de donnée à caractère personnel, en allant au-delà des contours définis par la jurisprudence récente de la CJUE en matière de pseudonymisation, ouvre la porte à des dérives potentiellement graves et nuirait au droit fondamental à la protection des données personnelles des citoyens français et européens, sans pour autant apporter la clarté juridique attendue par les entreprises et responsables de traitement ;

(82) Juge par conséquent qu'il n'est pas opportun de modifier la définition de « données à caractère personnel » figurant dans le RGPD ;

(83) S'oppose à la modification de la définition de « recherche scientifique » dans le RGPD, pour l'élargir à toute recherche soutenant l'innovation, y compris dans un intérêt purement marchant ;

(84) Estime que des garanties supplémentaires sont nécessaires pour assurer le caractère véritablement « scientifique » du traitement de données à caractère personnel aux fins de recherches scientifiques, par l'ajout à la définition de notions de vérifiabilité, de transparence et d'objectifs de la recherche scientifique ;

(85) Considère que l'IA ne doit pas bénéficier de privilèges en matière de traitement des données personnelles, sans que des garanties de protection suffisantes soient assurées ;

(86) Appelle de ses vœux la recherche de la préservation de l'équilibre fragile entre innovation et protection des droits fondamentaux qui découlent de la protection des données à caractère personnel ;

(87) Sur la possibilité ouverte à la Commission européenne de prendre des actes d'exécution :

(88) Juge disproportionnées les dispositions visant à permettre à la Commission européenne de prendre des actes d'exécution dans plusieurs domaines (relativement aux critères de définition des données pseudonymisées, aux listes et documents harmonisés relatifs aux AIPD, etc.) et estime que les institutions sectorielles européennes compétentes sont mieux placées pour émettre les lignes directrices qui s'imposent, le cas échéant ;

(89) Demande donc la suppression de cette disposition ;

(90) Invite le Gouvernement à faire valoir cette position dans les négociations au Conseil.

LISTE DES PERSONNES ENTENDUES

Services de l'État

Secrétariat général aux Affaires européennes (SGAE)

- M. Maxence BRISCHOUX, Secrétaire général adjoint
- M. Alexandre BORDES, chef du bureau Marché intérieur, Industrie, Recherche et innovation, Numérique et espace
- M. Harold MAGNAN, adjoint bureau Justice pénale et civile
- Mme Lena WALLENDORF, bureau Parlements (Parlement national, Parlement européen)

Représentation permanente de la France auprès de l'Union européenne

- M. Nicolas THERVET, conseiller
- Mme Marie DUGRÉ, conseillère justice, adjointe au chef de service JAI
- Mme Marie Léa ROLS, conseillère télécommunications, numérique et postes

Autorités de régulation

Commission nationale de l'informatique et des libertés (CNIL)

- M. Vincent VILLETTE, Secrétaire général
- Mme Nacera BEKHAT, cheffe du service de l'économie numérique et du secteur financier
- Mme Najma BICHARA, juriste au service des affaires européennes et internationales
- Mme Chirine BERRICHI, conseillère pour les questions parlementaires et institutionnelles

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- M. Vincent STRUBEL, Directeur général
- Mme Juliette PÉRON, conseillère
- M. Robin MASSON, chargé de mission affaires politiques européennes et internationales

Autorité de régulation de la communication audiovisuelle et du numérique (Arcom)

- M. Frédéric BOKOBZA, Directeur général adjoint

Société civile

Association française des correspondants à la protection des données (AFCDP)

- M. Fabrice MATTATIA, Délégué général
- Me Florence GAULLIER, membre du Conseil d'administration

Syndicats professionnels

France Digitale

- Mme Clotilde HOCQUARD, responsable des affaires réglementaires
- M. Edgar BERTHELIER, chargé d'affaires publiques

L'Association française des grandes entreprises (Afep)

- Mme Amina TARMIL, responsable des Affaires parlementaires
- M. Jocelyn GOUBET, Directeur Droit économique et politique numérique

Experte

- Mme Alexandra BENSAMOUN, professeure de droit à l'Université Paris-Saclay, spécialiste en régulation du numérique et en droit de la propriété intellectuelle, Personnalité qualifiée au ministère de la Culture (CSPLA, France)